Abstract – Deutsch

Mit der zunehmenden Kommerzialisierung des Internets wurde auch seine Einsatzmöglichkeit als Werbeträger entdeckt. Durch die Möglichkeit, mit geringem Aufwand auf sehr einfache Art und Weise eine große Anzahl an Personen zu erreichen, wird die Form der Werbung mittels Internet immer stärker eingesetzt.

Diese Arten der Werbung sind einerseits die bekannte Bannerwerbung, andererseits Internet-Werbung mittels Spam-Mails und Spam-Postings in Newsgroups, welche zu Werbezwecken für Privatpersonen als auch kommerzielle Organisationen eingesetzt werden.

Durch die immer stärker werdende Werbetätigkeit im Internet werden die damit verbundenen Probleme immer größer.
Diese Probleme reichen von Downloadkosten für unerwünschte Mails über Zeitvergeudung für das Lesen und Löschen – was wiederum einen Kostenfaktor darstellt, da in kommerziellen Unternehmen Produktivzeit von Arbeitnehmern benötigt wird – bis hin zur persönlichen Belästigung, da oftmals der übermittelte Inhalt von den Empfängern subjektiv als Ärgernis empfunden wird.

Ziel dieser Arbeit ist, die Arten der Internetwerbung zu erklären und wie man entsprechende Nachrichten als unerwünscht identifizieren kann. Ebenso werden Abwehrmaßnahmen vorgestellt und der rechtliche Aspekt betrachtet.

Abstract – English

The increasing commercialization of the internet encouraged its use for advertising purposes. As it can reach many people in a convenient and practical way with little expenses this kind of advertising will be used more and more.

Internet advertising is banner-advertising on the one hand and spam-advertising – divided into spam-mails and spam-postings in newsgroups - on the other. It adresses private persons as well as commercial organizations.

The increasing exploitation of the internet as an advertising medium causes, however, some problems.
These problems are e.g. download costs for spam-mails, a certain waste of time when reading and deleting these mails – which causes additional expenses. In this case you have to bear in mind that the working hours of employees are used to do this job.
Sometimes, receivers are even annoyed about the contents of certain mails.

The goal of this paper is to explain the different kinds of internet-advertising and how to identify messages not asked for. Just so defence mechanisms are explained in this paper and the legal aspects are introduced.

0 Einleitung

Mit der immer stärker werdenden Nutzung des Internets wurde auch dessen Einsatz für Geschäftabwicklungen, dem E-Commerce, immer beliebter. Doch damit verbunden steigt jedoch auch seine Verwendung für Werbezwecke. Diese Werbung im Internet – im Fachjargon als Spam bezeichnet - und die damit verbundenen Auswirkungen auf den Internet-User wurden zunehmend zu einem Problem, da die eingesetzten Mittel wie Banner oder Spam für den User unangenehme Effekte wie etwa Downloadkosten oder Zeitaufwand für den Download verursachen.
Das Hauptproblem bei Werbung im Internet ist zweifelsfrei Spam. Spam-Mails ermöglichen das einfache Versenden von Nachrichten in großer Menge und auf billige Art und Weise, was mittlerweile für die Empfänger einen beachtlichen Kostenaufwand (Download, Lesen und Löschen der Mails) sowie auch eine inhaltliche Belästigung darstellt.
Doch nicht nur für den Empfänger selbst, sondern auch für den Sender bringen Spam-Mails negative Auswirkungen, da sich die Adressaten durch den immer stärker werdenden Spam-Einsatz belästigt fühlen und ablehnende Einstellungen gegenüber den Spammern aufbauen.

Es ist daher Ziel dieser Arbeit, Bannerwerbung sowie Spam zu erklären sowie Maßnahmen zur Identifikationen und zur Abwehr dieser unerwünschten Nachrichten aufzuzeigen.
Den Mittelpunkt der Betrachtungen wird das Thema Spam einnehmen, da diese Thematik ein weitaus größeres Problem darstellt als oberflächlich vermutet wird und nahezu jeder Internet-User davon betroffen ist, denn Spam ist nicht nur kommerzieller E-Mail-Versand, sondern tritt auch in Form sinnloser Virenwarnungen oder Kettenbriefe auf (Hoax).

Neben einer Systematisierung dieser Nachrichten werden in dieser Arbeit auch Identifikationsmechanismen und –kriterien sowie Abwehrmaßnahmen und ein abschließende Betrachtung aus rechtlicher Situation sowie eine Umfrage zum Thema Spam dargestellt.

Da im deutschsprachigen Raum noch keine umfassende Dokumentation zu diesem wichtigen Thema existiert, war der Anreiz sehr groß, diese Arbeit zu erstellen und betroffenen Usern damit einen Leitfaden und eine Hilfestellung für diese Problematik zu anzubieten.

1 Werbung im Internet

Durch das rasante Wachstum des Internets wuchs auch seine Bedeutung als Marktplatz und damit verbunden seine Bedeutung als Absatzmittel (Online-Shops) und als Werbemittel sehr rasch an.

1.1 Aufgaben

Der wesentliche Unterschied der Internetwerbung im Vergleich zu konventioneller Werbung sind nicht die Aufgaben, sondern vielmehr die Werbemittel, auf welche im folgenden etwas näher eingegangen wird.
Die eigentlichen Aufgaben der Internetwerbung unterscheiden sich im Prinzip nicht von den Aufgaben normaler Werbung und dienen ebenso der Gewinnmaximierung des Unternehmens. Diese Aufgaben wären:

- Intensivierung der Werbung
- Sicherung vorhandener Märkte
- Erschließung neuer Märkte
- Bildung eines positiven Images

Neben diese alten Aufgaben treten jedoch auch neue Aspekte wie etwa

- Verbesserung des Informations- und Kommunikationsflusses im Unternehmen
- Kostensenkung im Unternehmen

1.2 Werbearten

Werbung im Internet geschieht gegenwärtig fast ausschließlich über die Schaltung von Anzeigen, das Versenden von Werbe-E-Mails oder die sogenannten Interstitials, d.h. Werbeeinblendungen auf dem Weg von einer Web-Site zur anderen. Als mehr oder weniger etablierte Werbeform gilt jedoch nur das Werben per Anzeige.
Elektronische Anzeigen im WWW haben verschiedene Bezeichnungen: Ads, Buttons, Banner, u.a. Die gebräuchliste Bezeichnung für Anzeigen ist jedoch Banner.

Dabei handelt es sich zumeist um Grafiken (Logo oder Werbeslogan), die als GIF- oder JPG-Datei in die HTML-Dokumente eingebunden werden und mittels Hyperlinks zu den Seiten des beworbenen Produkts oder des Unternehmens führen. Relativ neu sind Banner, die als Java-Applets realisiert wurden. Der Benutzer kann dabei mit den Java-Applets interaktiv agieren.

1.2.1 Site-Promotion

Unter Site-Promotion sind im wesentlichen die Maßnahmen zur Erhöhung der Attraktivität einer Internet-Site zu verstehen. Im folgenden Abschnitt wird dieser Begriff dargestellt und näher erläutert.

1.2.1.1 Definition von Site-Promotion

Es existiert noch keine verbindliche, allgemein akzeptierte Definition, was Site-Promotion ist, wo die Unterschiede zu anderen Werbeformen liegen und wo die Grenzen zu anderen Formen der Unternehmenskommunikation verlaufen.
Site-Promotion ist *„alles was hilft, ein Internet-Angebot interessanter zu machen“*.
[BÜRLIMANN 1999]
Site-Promotion hat grundsätzlich zwei Aufgaben: Die erste Aufgabe besteht darin, das Zielpublikum darauf aufmerksam zu machen, dass das Unternehmen mit ihrer Web-Site im Internet vertreten ist. Die zweite Aufgabe der Site-Promotion besteht darin, das Zielpublikum darüber zu informieren, wo sich diese Web-Site befindet. Die beiden Aufgaben sind, verglichen mit der Aufgabenpalette anderer klassischer Werbeformen, einfach zu bewerkstelligen. Die Einfachheit der Aufgabe – „Sag‘ den Leuten dass wir im Internet sind und nenne ihnen unsere Adresse“ – verleitet dazu anzunehmen, dass die Umsetzung ebenfalls sehr einfach ist.
Site-Promotion findet entweder im Internet oder außerhalb des Internets statt. Vernünftig scheint die Unterteilung der Mittel, Träger und Instrumente der Site-Promtion bezüglich der medialen Schnittstelle: Das Hauptinstrument der Site-Promotion im Internet ist die Bannerwerbung. Außerhalb des Internets gibt es eine breite Palette von Instrumenten, die zur Verfügung stehen. Diese Instrumente können Zeitschrifteninserate, TV-Werbespots (z.B. Lycos oder Yahoo) oder ähnliches sein. Das Unterscheidungskriterium ist das Medium selbst.

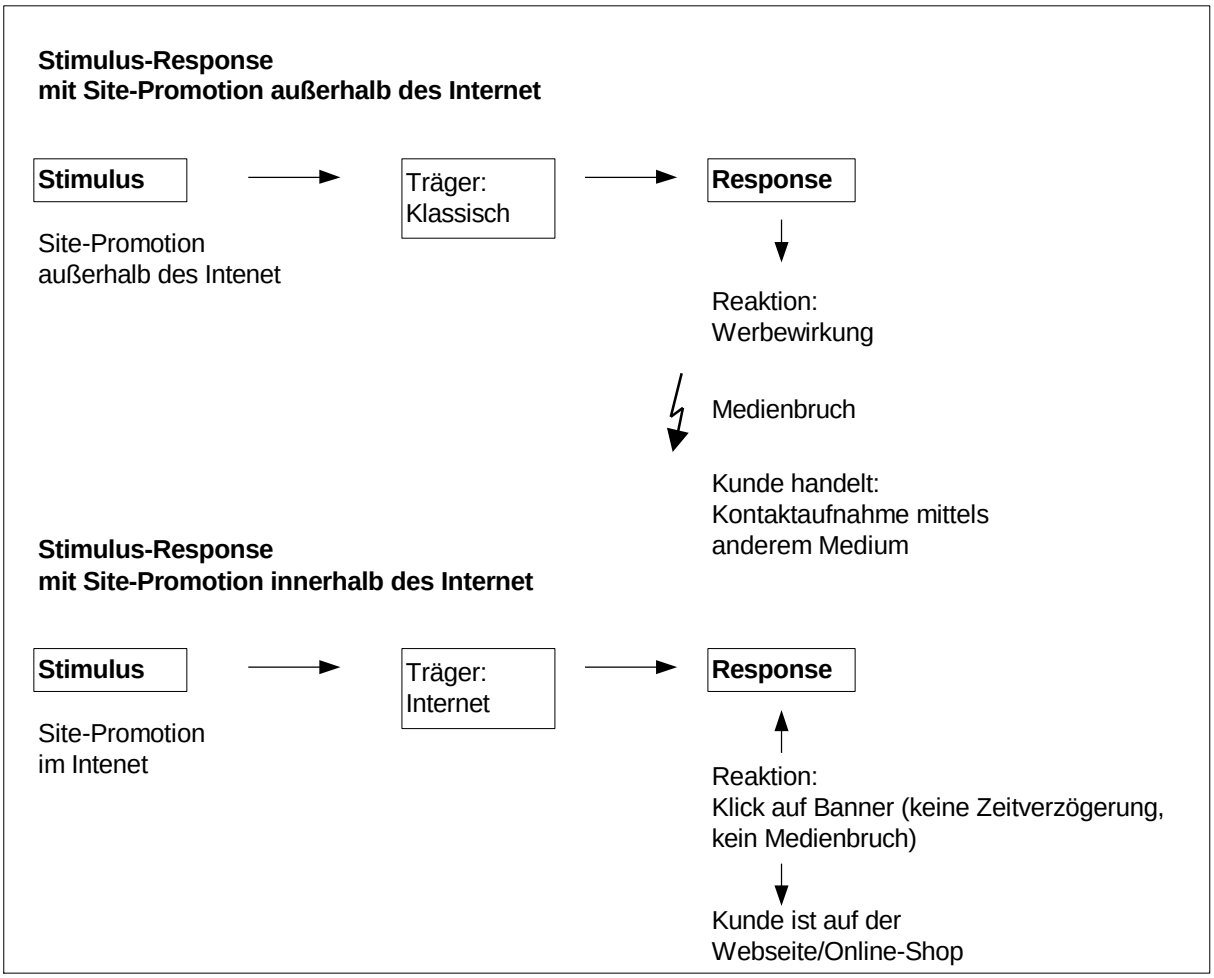


Abbildung 1: Stimulus-Response-Modell der Site-Promotion nach *„ionos GmbH“* in Bürlimann 1999

Die Mechanismen der Stimulus-Response (Reiz-Reaktion) der Site-Promotion außerhalb des Internet sind die gleichen wie in klassischen Medien. Der Stimulus geht vom Werbeträger aus, z.B. vom Werbemittel (Inserat) in einem Träger (Zeitung). Der Response stammt von einer Werbewirkung. Es gibt einen Medienbruch, der Kunde handelt und nimmt über ein anderes Medium Kontakt mit dem Unternehmen auf, z.B. er schickt den Bestellschein des Inserats per Post zurück.
Stimulus-Response bei Site-Promotion im Internet ist sehr direkt: Der Stimulus geht vom Werbemittel (Banner) auf dem Werbeträger (andere Web-Site) aus. [BÜRLIMANN 99]

1.2.1.2 Klassische Werbung für die Web-Site

Die naheliegendste Form von Site-Promotion ist die klassische Werbung, die darauf hinzielt, dem Publikum das Online-Angebot bekannt zu machen. Noch 1997 war in Europa nur ganz vereinzelt Site-Promotion in Form gezielter klassischer Werbung zu sehen. Professionell geführte Werbekampagnen, die auf einen Mediaplan aufbauten, waren praktisch nicht existent. Der offensichtliche Nutzen dieser Werbeform sorgt dafür, dass Site-Promotion seit 1998 rasant wächst.
Weder die Werbepraxis noch die betriebswirtschaftliche Literatur haben das Thema bis heute umfassend bearbeitet. Es sollen hier nur Anstöße gegeben werden, in welche Richtung sich die Werbetätigkeit bewegen könnte, um mit klassischer Werbung effiziente Site-Promotion zu bewerkstelligen.
Die Kernaufgabe ist für jedes Werbemittel und jeden Werbeträger in der klassischen Werbung dieselbe. Bezüglich der neuen Aufgabe der Site-Promotion ergeben sich für die Werbemittel und Werbeträger keine Änderungen.

Ausweitung der Werbebotschaft
Das Unternehmen transportiert auf allen ihren bisherigen Werbeträgern ergänzend zur bisherigen Werbebotschaft die Information, wo sich welches Internet-Angebot der Firma befindet. Zentral ist, dass die Site-Promotion auf klassischen Werbeträgern nicht isoliert erscheinen darf, sondern nahtlos in die bisherige Werbung des Unternehmens eingebettet sein muss. Das könnte dadurch geschehen, indem man am Ende eines Werbespots die Web-Adresse einblendet oder zu Zeitungsinseraten und auf Produktverpackungen die Web-Adresse abdruckt.

Klassische Werbung für das Online-Angebot
Als Träger der Botschaft kommen natürlich sämtliche bekannten Werbeinstrumente in Frage: Möglich sind einfache Flyer, Plakate, Annoncen, Kleininserate, Spots, CD-ROM und weitere. Das Thema ist äußerst vielseitig und berührt die Werbebranche fundamental. Aus diesem Grund soll hier nicht näher auf diese Thematik eingegangen werden. [BÜRLIMANN 99]

1.2.1.3 Angewandte Site-Promotion

Neben der Verwendung klassischer Werbemedien existieren einige zusätzliche Möglichkeiten für Site-Promotion, die kostengünstig sind und gute Resultate erzielen. Der Eintrag in Suchmaschinen und Verzeichnisse gehört ebenso dazu, wie dafür zu sorgen, dass möglichst viele Links auf die eigene Seite verweisen. Nicht zu vernachlässigen sind zudem Pressearbeit und geschickter Einsatz von E-Mail.

Domainname

Der Anfang aller Site-Promotion ist ein gut gewählter Domain-Name. Für jede im Handelsregister eingetragene Firma muss die entsprechende Domain registriert werden. Auch für jedes eingetragene Warenzeichen empfiehlt es sich, die Domain registrieren zu lassen.
Es war im Internet praktisch nicht möglich, sich einen Markennamen auf juristischem Weg zurückzuholen. Die Gesetzgebung hinkte der Entwicklung in diesem neuen Medium enorm hinterher.
Der Handel mit Domain-Namen, das sogenannte „Domain-Grabbing“, welcher in den Anfängen des Internets sehr verbreitet war, wurde dadurch unterbunden, indem die Gerichte begannen, dem Domain-Namen eine kennzeichnende Funktion zuzuschreiben. Unternehmen können heute ihre Domain unter Berufung auf bestehende Kennzeichenrechte relativ problemlos einklagen.
Einer der ersten Präzedenzfälle war das Urteil bezüglich der Domain „www.epson.de“, in welchem der Firma „Epson“ die Rechte an dieser Domain, welche sich eine Privatperson sichern ließ, zugesprochen wurden.

Eintrag in Suchmaschinen und Verzeichnisse

Das naheliegendste ist, die eigene Web-Site in möglichst viele Suchmaschinen und Verzeichnisse einzutragen. In den Suchmaschinen im eigenen Land und in regionalen und thematisch begrenzten Suchmaschinen sollte der Eintrag von Hand aus geschehen. Für den automatischen Eintrag in weltweite Suchmaschinen und nationale Suchmaschinen im Ausland stehen verschiedene Dienste zur Verfügung, wobei einige davon kostenlos sind.
An den Eintrag in Suchmaschinen sind meist Stichworte geknüpft, nach welchen die Suchmaschinen die Suchergebnisse auswerten. Die Web-Site des Unternehmens erschient dann in der Trefferliste weiter oben, wenn ein Benutzer nach diesem Stichwort sucht.

Eintrag in thematische Verzeichnisse

Thematische Verzeichnisse - beispielsweise ein Verzeichnis von Maschinenbaufirmen in Deutschland - nehmen immer stärker an Bedeutung zu, da man dadurch schneller und gezielter auf gewünschte Informationen zugreifen kann.

Eintrag in geographische Verzeichnisse

Einen regelrechten Boom erleben die geographischen, lokalen Verzeichnisse und Plattformen, die eine Gemeinde oder eine Stadt darstellen und touristische Möglichkeiten zeigen oder Dienstleistungen wie Ausgehtipps oder das Kinoprogramm anbieten. Fast jede Stadt hat bereits eine oder mehrere solcher Plattformen. In größeren Städten existieren meist mehrere Plattformen mit verschiedenen Schwerpunkten nebeneinander.
Einträge in geographische Plattformen sind in der Regel kostenlos, sie sollten aber einen lokalen Bezug zu dieser Plattform haben, da ansonsten die falsche Zielgruppe angesprochen wird und andererseits, bei globaleren Einschaltungen, der regionale bzw. lokale Charakter verloren geht.

Links auf die eigene Web-Site generieren

Die mit Abstand beste Site-Promotion sind Links im Internet, die auf die eigene Site verweisen. Normalerweise bezahlt man für solche Links nichts. Das Unternehmen kann auf der eigenen Site Gegenlinks anführen, beispielsweise unter dem Titel "our friends" oder "Andere interessante Seiten". Dies ist allerdings bereits etwas antiquiert und erinnert an die Anfänge des Internets. Heute ist es eher üblich, solche Links durch Banner darzustellen.

Newsgroups

Newsgroups sind für die Site-Promotion weniger bedeutungsvoll als allgemein angenommen. Die Newsgroups sind aus zwei Gründen nicht besonders wichtig für Site-Promotion-Zwecke: Die Diskussionen sind oft privat und eine Werbemeldung ist störend. Der zweite Grund ist die Masse an neuen Internetangeboten : Es gibt Schätzungen, wonach pro Tag weltweit 10000 neue Internetangebote aufgeschaltet werden. Wer eine kleine Firmenpräsentation in den Newsgroups als große Neuheit ankündigt, läuft Gefahr, sich lächerlich zu machen. [BÜRLIMANN 1999]
Neben diesen zwei Gründen ist weiters zu bemerken, dass diese Art der Werbung eine Form von Spamming darstellt (siehe Kapitel3) und gegen die Usenet-Netiquette verstößt.

Pressearbeit

Mittelgroße Unternehmen sind meist mindestens einmal im Jahr in den Medien präsent, wenn sie ihre Umsatzzahlen bekannt geben. Das Internetangebot des Unternehmens ist ein idealer Anknüpfungspunkt die Medienpräsenz zu erhöhen. Journalistische Erfahrung ist von Vorteil; Pressearbeit eignet sich jedoch auch für Unternehmen, die sich keine Agentur leisten können oder wollen.

Gute Pressearbeit ist für Klein- und Kleinstunternehmen perfekt geeignet, im geographischen Einzugsgebiet Publizität zu schaffen. Regionale Zeitungen oder Gratisblätter haben zwar ein eher schlechtes Image, sie werden aber in der Regel sehr gut gelesen. Wenn ein Fachgeschäft oder ein Unternehmen, welches in der Gemeinde bekannt ist, ihre Internetpräsenz startet, muss es damit unbedingt in der lokalen Presse erscheinen. Insbesonders für kleine Firmen ist ein Zeitungsartikel die beste Werbung.

E-Mails

Der Versand von E-Mails für Werbezwecke ist sehr heikel. Massenversand von Mails, ein sogenannter Spam (siehe Kapitel 3), ist unnütz und gefährlich. Es kann wüste Beschimpfungen auslösen und die Absender können Gefahr laufen, auch den treuesten Kunden zu verlieren. Der Gratisversand von Mails mittels Tools, die auch Anfänger bedienen können, verlocken dazu, Mails in Massen abzuschicken. Das Unternehmen muss darauf achten, dass kein Spam betrieben wird. E-Mails sind nur dann sinnvoll, wenn sie analog wie ein Brief an Empfänger gerichtet sind, die sich auch tatsächlich für den Inhalt interessieren. In Frage kommen Presse-Mailings, Mailings an Branchenverbände, Mailings an die eigenen Kunden oder ähnliches. [BÜRLIMANN 99]

Durch den Eintrag in Opt-In-Listen von Unternehmen erklärt sich ein User bereit, von dieser Firma Werbe-E-Mails zu erhalten

1.2.1.4 Nebenformen der Site-Promotion

Site-Promotion ist jung. Eine ganze Reihe von möglichen Maßnahmen ist nicht ausgereift und nur wenige Agenturen und Unternehmen verfügen über das Know-How, diese Werbemöglichkeiten anzuwenden. An dieser Stelle werden vier Möglichkeiten der Site-Promotion angeführt, deren Bedeutung wächst. Es sind dies Event-Marketing im Internet,

Sponsoring im Internet, Durchführung von klassischen Events für Interent-Angebote und das Erstellen von eigenen Plattformen.
Diese Werbeformen sind nicht für Experimente geeignet. Das Unternehmen muss sich solche Maßnahmen sehr gut überlegen, die Maßnahmen müssen perfekt konzipiert sein und von Fachleuten umgesetzt werden. Bedingung für solche oder ähnliche Formen von Site-Promotion ist auch, dass die Angestellten mindestens ein Jahr Internet-Erfahrung aufweisen. Diese Werbemittel können nur Erfolg aufweisen, wenn sie von Profis durchgeführt werden. Das Unternehmen muss sich auch bewusst sein, dass solche Werbeformen größere Budgetdimensionen aufweisen können.

Event-Marketing im Internet

Die schwierigste und teuerste Form von Site-Promotion ist Event-Marketing im Internet. Durch die Eigenschaften des Mediums sind Online-Events komplett anders geartet als in der realen Welt. Insbesondere gibt es im Internet keine kollektiven Erlebnisse, da jeder Besucher einer Seite alleine vor dem Bildschirm sitzt. Gruppenerlebnisse beschränken sich real gesehen auf kleine Gruppen, die gemeinsam vor dem PC sitzen oder Anlässe in einem Internet-Cafe, was jedoch mit einem Gruppenerlebnis nicht vergleichbar ist. Das Erlebnis eines realen Events ist der "Ich-war-dabei-Effekt", Events im Internet beschränkt sich auf den "Ich-hab's-auch-gesehen-Effekt".
Unternehmen können mit der Durchführung von eigentlichen Internet-Events warten, bis klar ist, was der eigentliche Nutzen einer solchen Aktion ist. Wenn das Budget zur Verfügung steht ist es möglich, ein Experiment zu wagen. Man kann auf diesem Gebiet Ersterfolge erzielen, die hohe Wellen werfen und Beachtung finden. Allerdings sind Internet-Events Unternehmen vorbehalten, die große Budgets zur Verfügung haben. Die Durchführung obliegt absoluten Spezialisten.
Ein Hauptgrund, weshalb solche Events durchgeführt werden, beruht darauf, dass damit der Einsatz neuer Technologien verbunden ist und die Veranstalter zu den Ersten gehören möchten, die diese Technologien verwenden.
Ein Beispiel für solche Internet-Events wären Fragestunden mit Politikern oder auch Übertragungen von Pop-Konzerten live im Internet.

Sponsoring im Internet

Eine naheliegendere Form von Site-Promotion als die Durchführung von Online-Events ist Sponsoring im Internet. Obwohl mit Sponsoring bereits spektakuläre Erfolge erzielt wurden, ist diese Form von Site-Promotion erstaunlicherweise kaum zu beobachten. Im folgenden wird vor allem auf das Sponsoring von geographischen Plattformen und das Sponsoring von Anbietern in Form von Hardware eingegangen. Es sind prinzipiell weitere Formen von Sponsoring denkbar, allerdings sind die Erfahrungen auf diesem Gebiet noch sehr bescheiden.

Sponsoring von geographischen Plattformen

Geographische Plattformen sind Web-Sites, welche sich auf einen geographisch eingegrenzten Bereich beschränken und aktuelle Informationen über diesen Bereich anbieten. Als Beispiel wären hier Web-Sites von Städten, Gemeinden oder Regionen (z.B. Ennstal-Region, Nationalpark Hohe Tauern) zu erwähnen, welche Ausflug-, Ausgeh-, Kulturtipps oder ähnliche Informationen bereitstellen.
Lokale geographische Internet-Plattformen haben eine ganz große Zukunft.
Für ein Unternehmen, das auf eine lokale Präsenz angewiesen ist, könnte es langfristig äußerst wertvoll sein, eine solche lokale Internet-Plattform zu sponsern. Die Betreiber sind meist Jungunternehmer voller Enthusiasmus, die viele Ideen und wenig Geld haben. Die Unternehmen, die als Sponsoren in Frage kommen - wie führende Lokalzeitungen oder tiefverwurzelte Industriebetriebe in einer Region - können enormen Imagegewinn erzielen, wenn sie eine solche Plattform unterstützen.

Sponsoring in Form von Hardware

Die heute am weitesten verbreitete Art von Sponsoring im Internet ist die Unterstützung von Betreibern eines Internet-Angebotes in Form von Hardware. Meist sind es Informatik-Unternehmen, welche die eigenen Produkte in günstiges Licht setzen. Die häufigste Form von Sachsponsoring ist es, Server, Leistungen und Administrationen zu übernehmen. Die Gegenleistung ist meist, dass das eigene Firmenlogo prominent platziert wird.

Klassische Events

Prinzipiell sind zwei Formen von klassischen Events für Site-Promotion denkbar: Einerseits können klassische Events für ein Internet-Angebot durchgeführt werden, andererseits ist die Darstellung von klassischen Events im Internet möglich.

Klassische Events für eine Site

Genauso wie eine Firma einen Event durchführt, um den Bekanntheitsgrad zu erhöhen, kann der Betreiber eines Internetangebots einen Event durchführen, um die Adresse und den Inhalt der Web-Site dem Zielpublikum näher zu bringen.
Fundierte Internet-Kenntnisse sind nicht notwendig, da ein realer Event durchgeführt wird.

Darstellung von klassischen Events im Internet

Darstellung von Groß-Events im Internet weisen unglaublich hohe Abfragezahlen aus. Die bekanntesten Beispiele sind die Fußballweltmeisterschaft 1998 in Frankreich und die Übertragungen der Marssonde 1997. Die schier unglaublichen Abfragezahlen - über 1,1 Milliarden Zugriffe auf den WM-Server - sind das deutlichste Indiz, dass sich das Internet längst zu einem Medium entwickelt hat, das mit klassischen Informationsvermittlern wie Fernsehen und Zeitung ernsthaft konkurriert. Das Internet gehört schon heute zu den wichtigsten Zusatzinformations-Medien. [BÜRLIMANN 99]
Durch neue Techniken wie ADSL („Asynchron Data Subscriber Line“) oder Internetverbindungen über Kabel-TV-Anschlüsse sind Bild- und Tonübertragungen ohne oder mit lediglich sehr geringen Qualitätsverlusten möglich. Dadurch könnte das Internet in absehbarer Zeit eine ernsthafte Konkurrenz zu Liveübertragungen im Fernsehen darstellen.
Da das Internet nicht durch regionale Reichweiten und eine begrenzte Anzahl von Übertragungskanälen wie im TV beschränkt ist, können sehr viele klassische Events im Internet parallel dargestellt werden. Eine Beschränkung erfolgt lediglich durch die begrenzte Bandbreite.

1.2.2 Werbung mittels Banner

Die mit Abstand wichtigste Werbeform im Internet ist die Bannerwerbung.
Ein Banner als Werbemittel verweist nach dem Prinzip eines Links auf ein beworbenes Internetangebot. Der größte Unterschied zu klassischen Werbemitteln ist, dass kein Medienbruch stattfindet: Der Transfer der Werbebotschaft, die Reaktion des Zielpublikums, Bestellung im Online-Shop und Bezahlung finden im gleichen Medium statt (siehe Abbildung 1). Das Banner selbst kann verschiedene Ausprägungen annehmen. Als Werbeträger kommt prinzipiell jede Internet-Seite in Betracht, die typischen Werbeträger sind jedoch Suchmaschinen und Seiten mit hohem Bekanntheitsgrad und hohen Abfragezahlen. Die Schaltung kann nach verschiedenen Kriterien erfolgen.
Die wichtigste Wirkung von Bannerwerbung ist die Abfragesteigerung auf dem beworbenen Internetangebot.

1.2.3 Spamming

Spam im weiteren Sinne ist eine Sammelbezeichnung für unerwünschte, belästigende Nachrichten in Form von E-Mail oder Beiträgen (Postings) in Newsgroups. Bei E-Mail spricht man auch von Junk-Mail ("Junk" = wertloser Mist). Begleiterscheinung ist meist, dass diese Nachrichten nur geringen inhaltlichen oder ästhetischen Wert haben.

Die Absender wollen durch Versenden solcher Nachrichten den Effekt einer großen Postwurfsendung erzielen, erreichen aber durch die Belästigung der Empfänger fast immer das Gegenteil.

Da das Versenden von Nachrichten in großer Menge einfach und billig ist, ist es zu einem ernsthaften Problem geworden. Spam und Junk-Mail werden von fast allen Netzbenutzern abgelehnt und als schwerer Missbrauch angesehen. Uneinsichtigen Versendern von Spam wird in letzter Konsequenz durch den ISP der Internet-Zugang gesperrt, was aber durch einen Wechsel zu einem anderen Provider für den Spammer kein ernst zu nehmendes Problem darstellt.

So verständlich es ist, dass jeder Mensch sein eigenes Anliegen möglichst vielen anderen Menschen mitteilen will, so entstehen dadurch beim Empfänger gravierende Probleme. Wenn man täglich Spendenaufrufe von allen möglichen Organisationen, Angebote von Versicherungen, Vermögensberatern, Pizzaservice, Installateur etc. aus der ganzen Welt bekommt, ist das sehr lästig und mit Zeitaufwand zum Lesen und Löschen verbunden. Durch viele technische und organisatorische Maßnahmen kann das unterbunden werden. Letztlich helfen auch alle Internet-Benutzer mit, welche sich engagiert und massiv gegen Spam einsetzen.

Da inhaltliche Zensur im großteils selbstverwalteten Internet abgelehnt wird, kann Spam auch nicht über den Inhalt definiert werden. Inhalt ist immer Wertung. Wertungen sind subjektiv oder kulturell unterschiedlich. Was für den einen gut ist, ist in den Augen des anderen schlecht. Auf der Basis von inhaltlichen Wertungen kann weltweite Kommunikation nicht reguliert werden. Spam wird deshalb ausschließlich über objektiv messbare Kriterien definiert. Es gibt daher keinen "guten" oder "bösen" Spam - entweder ist es Spam oder nicht. [VIBE 99]

Tatsache aber ist, dass Spam generell negativ gesehen wird und zu unterlassen ist (siehe Kapitel 3).

1.3 Negative Auswirkungen der Internetwerbung

Wie auch bei der konventionellen Werbung treten auch bei der Werbung im Internet negative Auswirkungen auf. Diese Auswirkungen beziehen sich in der Regel immer auf den Werbeberührten, der sich von der Art der Werbung, ihrer Inhalte oder auch anderen Aspekten gestört sind.
Im Internetbereich kommt im Gegensatz zu herkömmlicher Werbung der Zeitfaktor für den Download der Werbung sowie die dafür anfallenden Kosten dazu.

1.3.1 Bannerwerbung

Ein Nachteil der Bannerwerbung ist, dass für den Werbeberührten immer Kosten anfallen, Diese Kosten setzen sich zusammen aus Telephongebühren, Providerkosten und fallweise auch Mengengebühren. Weiters ist die Zeit des Werbekontakts im Internet im Vergleich zum Fernsehen oder Radio jeweils unterschiedlich. Ein Radiospot dauert in etwa ca. 15 Sekunden, Im Internet kommt es auf die Ladezeit an, die je nach Tageszeit und Auslastung des Internets und verschiedener Modemgeschwindigkeiten sehr verschieden sein kann. Je mehr Banner enthalten sind, desto mehr Graphiken müssen geladen werden. Das bedeutet dass die Ladezeit erheblich erhöht wird und der Benutzer länger auf den Aufbau der Seite warten muss und höhere Kosten entstehen, was mitunter öfters zur Beendigung des Besuchs der Webpage seitens des Users führt. Andererseits haben viele Internet-User in ihrem Browser die Graphiken ausgeschalten, um diese langen Ladezeiten zu vermeiden, was wiederum für die Werbebetreiber nachteilig ist, da einerseits die Banner nicht eingeblendet werden und andererseits die Web-Seite in ihrem Aussehen verunstaltet wird.
Mit den Abbildungen der Suchmaschine "Lycos-Schweiz" auf der folgenden Seite soll ein Beispiel gegeben werden, wie sich das Ausschalten der Graphiken negativ auf das Aussehen einer Web-Seite auswirken kann:

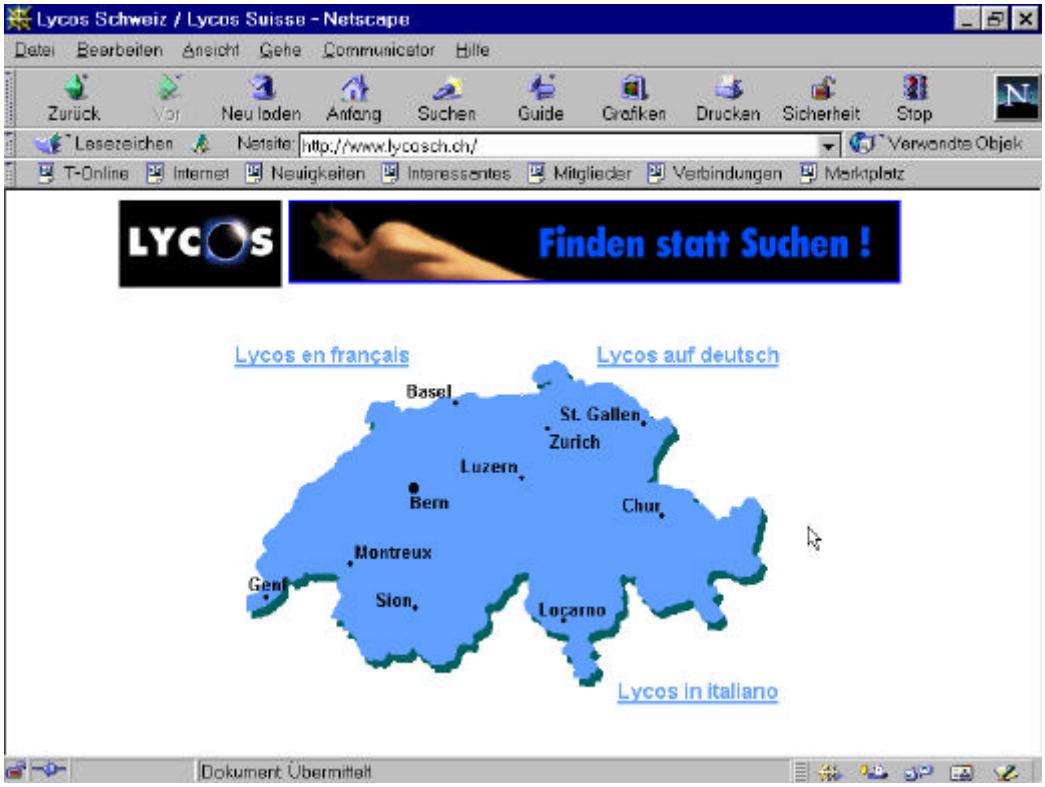


Abbildung 2: Lycos-Schweiz mit eingeschalteter Graphikanzeige

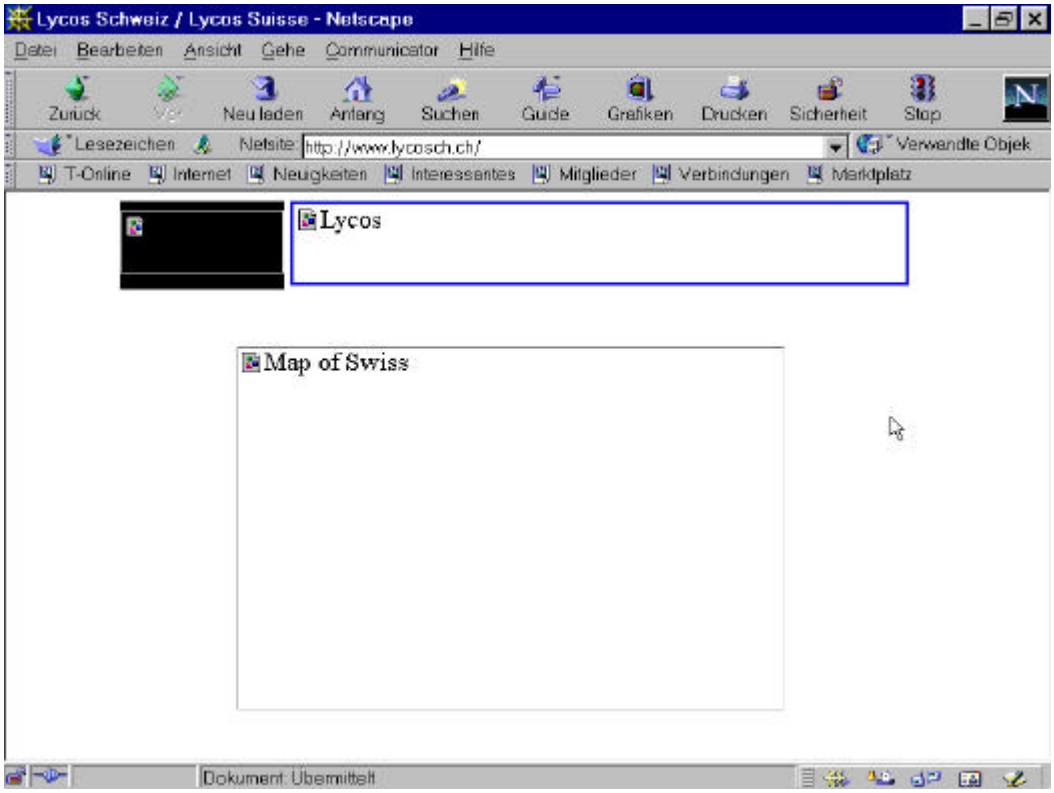


Abbildung 3: Lycos-Schweiz mit ausgeschalteter Graphikanzeige

1.3.2 Spamming (E-Mail-Werbung)

Durch massenhaftes versenden von E-Mails oder Mitteilungen in Diskussionsgruppen werden diverse Server - der eigene Mailserver sowie die Mail- bzw. Newsserver der Empfänger - unnötig belastet und das Internet wird dadurch langsamer. Es wird dadurch wertvolle Bandbreite verschwendet.
Weiters werden Empfänger von Spam-Mail sowie Teilnehmer an Newsgroups, in denen Werbemitteilungen bzw. unpassende Beiträge gepostet werden, verärgert. Dieser Ärger kann wiederum zu einer Beschwerde per E-Mail beim Postmaster des entsprechenden Providers, von welchem das Spam bzw. die Newsgroup-Mitteilung gepostet wurde, führen. Dadurch wird wiederum Bandbreite vergeudet und bereitet dem Postmaster zusätzliche und unangenehme Arbeit.
Ebenso werden Teilnehmer aus Newsgroups vertrieben, in welchen sinnlose und ärgerliche Beiträge stehen, da dadurch niemand mehr Interesse hat, an einer solchen Diskussion teilzunehmen.

2 Bannerwerbung

Wie bereits in Kapitel 1.2.2 erwähnt, ist Bannerwerbung die mit Abstand wichtigste Form der Internetwerbung.

Aus dem Englischen übersetzt heißt Banner Flagge, Wimpel, Transparent oder Fahne. Das Wort stammt ursprünglich aus dem Altfranzösichen „la bannière“ und einer romanischen Vorform „bandiere“, welche als militärischer Ausdruck den Ort bezeichnet, wo in der schlacht die Fahne steht. Davon übriggeblieben ist das „Panier“, ein etwas antiquierter Ausdruck für eine Fahne. Das altfranzösiche Verb dazu heißt „banir“ und bedeutet verkünden. [BÜRLIMANN 99]

Von dieser Namensgebung und der Bedeutung ist Banner ein gut gewählter Name für diese Form der Werbung, da man einerseits eine Werbebotschaft verkünden will und andererseits im Kampf um Marktanteile bestehen will.

Im folgenden Abschnitt soll daher etwas näher auf die Aufgaben und die Gestaltung von Bannern sowie auf die Durchführung der Bannerwerbung eingegangen werden.

2.1 Funktionsweise (Push-Pull-Effekt)

Die Funktionsweise eines Banners ist im Prinzip zu vergleichen mit der Funktionsweise eines normalen Hyperlinks. Da es das Ziel der Bannerwerbung ist, einen User durch anklicken auf eine bestimmte Internetseite zu bringen, verbirgt sich hinter einem Banner lediglich ein Link zu einer anderen Web-Site.

Der „Push-Effekt“

Der „Push-Effekt“ bei der Bannerwerbung ist zu vergleichen mit der Funktionsweise einer normalen Anzeige in Zeitschriften, Plakaten oder ähnlichem. Das bedeutet, dass der Surfer das Banner sieht und das Unternehmen bzw. das Produkt bekannt wird. Ein Anklicken und weiterverbinden zu der Web-Site, welche hinter dem Banner steht erfolgt hier nicht.

Der „Pull-Effekt“

Als „Pull-Effekt“ wird bezeichnet, wenn der User sofort auf das Banner klickt und ohne Umwege auf die durch das Banner beworbene Web-Site gelangt. Weiters entsteht beim „Pull-Effekt“ zuerst der „Push-Effekt“, da der Surfer das Banner wahrnimmt und es auch die Aufgaben einer normalen Werbung übernimmt (siehe oben).

2.2 Banneraufbau

Der Aufbau eines Banners bezüglich Größe und Gestaltung bzw. seiner Inhalte ist ein wesentliches Kriterium, um erfolgreich Bannerwerbung zu betreiben. Man sollte daher bei der Gestaltung von Bannern gewisse Richtlinien einhalten, um die Erfolgsaussichten zu steigern.

2.2.1 Größe

Nach dem IAB-Standard[1] (Internet Advertising Bureau) sind folgende gängige Bannergrößen zu unterscheiden:

- 468 X 60 Pixel (Full Banner)
- 392 x 72 Pixel (Full Banner with Vertical Navigation Bar)
- 234 x 60 Pixel (Half Banner)
- 120 x 240 Pixel (Vertical Banner)
- 120 x 90 Pixel (Button 1)
- 120 x 60 Pixel (Button 2)
- 125 x 125 Pixel (Square Button)
- 88 x 31 Pixel (Micro Button)

Neben diesen standardisierten Bannerformaten sind noch folgende Formate gebräuchlich:

- 450 x 50 Pixel
- 75 x 75 Pixel
- 156 x 60 Pixel
- 130 x 80 Pixel
- 137 x 60 Pixel

[ABSEITS 99/1]

[1] Das IAB ist eine US-amerikanische NON-Profit-Organisation mit dem Ziel, den Gebrauch und die Effektivität der Internetwerbung zu erhöhen. Homepage: http://www.iab.net

2.2.2 Inhalt eines Banners

Da sich die Internet-User an Bannerwerbung bereits gewöhnt haben, sinkt dadurch auch die Effizienz der Bannerwerbung. Immer weniger User klicken einen Banner tatsächlich an, um dadurch die vom Banner verbundenen Web-Seiten zu erreichen. Deshalb muss Werbung mittels Banner immer attraktiver werden. Um das zu erreichen, sollte auf die Einhaltung gewisser Standards geachtet werden.

Mauszeiger

Benutzer schauen eher in die Mitte einer Seite oder rechts neben ihren Mauszeiger am Scrollbalken und klicken. Einige Anzeigen beinhalten einen animierten Mauszeiger. Es existieren jedoch noch keine Aussagen über die Wirkung solcher Anzeigen, allerdings ist davon auszugehen, dass diese deutliche Steigerungsraten zur Folge haben. Ob diese Steigerung aber auf erhöhte und bewusste Aufmerksamkeit des Benutzers oder eher auf eine Verwechslung mit seinem "realen" Mauszeiger zurückzuführen ist, ist nicht geklärt.

Anzeigen des Markennamens

Wenn der Marken- bzw. Produktname in der Anzeige nicht erscheint, erhöht sich die Ad Click Rate. Wenn aber die Marke gezeigt wird, beeinflusst die Anzeige auch Personen, die nicht auf die Anzeige klicken. Bei Anzeigen, die für ein neues Produkt oder eine Dienstleistung werben, sollte der Markenname zunächst nicht angezeigt werden, da bei einem potentiellen Benutzer schnell der Eindruck entsteht, er sei bereits über das entsprechende Produkt informiert bzw. hätte kein Interesse an weiterführenden Informationen.

Farben

Bei der Gestaltung der Banner führen helle, glänzende, leuchtende, strahlende Farben zu den besten Ergebnissen. Helle leuchtende Farben ziehen die Blicke des Benutzers auf sich, wodurch sich auch höhere Ad Click Raten ergeben. Untersuchungen haben aufgezeigt, dass Farben wie Blau, Grün und Gelb die nachhaltigsten Eindrücke hervorrufen, während Rot, Weiß und Schwarz weniger effektiv sind.

Außerdem sollten die Farben für Texte und Hintergründe so aufeinander abgestimmt sein, dass sich eine Kontrastwirkung ergibt und damit Texte gut lesbar erscheinen.
Sind bestimmte Markenfarbe auch in der normalen Werbung bzw. bei der Firmenrepräsentation in Verwendung, sollte man eine Verwendung dieser Farben ebenfalls überlegen, um sich im Sinne einer „Corporate Identity“ einheitlich zu präsentieren.

Gestaltung der Texte

Fragen auf einer Anzeige erhöhen die Ad Click Rate um 16 %. Fragen wie "Suchen Sie nach kostenloser Software?" wirken unmittelbar auf den Benutzer und rufen eine Reaktion hervor. Aufrufe zur einer Aktion erhöhen die Ad Click Rate um 15 %. Die Ad Click Rate erhöht sich beispielsweise, wenn man dem Benutzer eine Erklärung gibt, was er tun soll. Einfache Aufrufe wie "Klicken Sie hier!" oder "Besuchen Sie uns jetzt!" führen dazu, dass die Benutzer eher auf die Anzeige klicken. Sätze dieser Art sollten strategisch in der Anzeige platziert werden, wobei eine Positionierung auf der rechten Seite zu den besten Ergebnissen führt. Verschlüsselte Botschaften erhöhen die Ad Click Rate um 18 %. Verschlüsselte Botschaften sollen dazu beitragen, das Interesse des Benutzers für die Anzeige zu steigern. Der Benutzer fragt sich: "Was bedeutet das?", "Was soll das heißen?".
Bei verschlüsselten Botschaften sollte die Marke in den Hintergrund rücken oder ganz weggelassen werden, da andernfalls möglicherweise die Zielgruppe nicht erreicht wird. Da das zu verkaufende Produkt für die Botschaft nicht wichtig ist, können Botschaften dieser Art sehr interessant gestaltet werden. Andererseits veralten solche Anzeigen schneller. Wenn allerdings die Anzeige ohnehin nur kurz gezeigt werden soll, kommt der potentiellen Lebensdauer keine große Bedeutung zu.

2.2.3 Bannerarten

Durch den Umstand, dass Bannerwerbung die klassische Form der Internetwerbung ist und eine dementsprechende Verbreitung gefunden hat, entwickelten sich im Laufe der Zeit verschiedene Bannerformen, die nicht nur von den Gestaltungsrichtlinien her variieren, sondern sich auch von ihrem Aufbau und ihren Eigenschaften unterscheiden.

2.2.3.1 Statische Banner

Die einfachste Form des Banners ist statisch. Ein statischer Banner besteht aus einer Datei, die Bild und Text enthält. Das statische Banner ist das Grundmodell der Bannerwerbung. Jedes Unternehmen sollte für seinen Firmenauftritt, seinen Online-Shop oder seine anderen Internetangebote ein paar statische Banner in Reserve haben. Professionelle Internet-Anbieter liefern bei der Erstellung des Firmenauftritts ein statisches Banner gleich mit.
Das statische Banner hat eine Reihe von Vorteilen. Es ist leicht - in Kilobyte ausgedrückt - und somit beim Benutzer schnell geladen. Die Herstellung ist technisch recht einfach. Grafiker, Texter und Werber können ihre gewohnten Arbeitsinstrumente verwenden und die Arbeitsmethoden beibehalten, um ein statisches Banner zu gestalten. [BÜRLIMANN 99]

2.2.3.2 Animierte Banner

Animierte Banner, auch Living Banner und Moving Banner genannt, sind Werbeflächen im Internet, die Bewegung enthalten. Es gibt zwei Arten von Animationen, bewegte Bilder und bewegte Elemente. Die bewegten Bilder sind keine Sequenzen im Sinne eines Kurzfilms sondern meist eine Reihe aneinandergekoppelter Einzelbilder. Animationen sind bewegte Elemente, die in dem Banner integriert sind. [BÜRLIMANN 99]

2.2.3.3 Applikatorische Banner

Applikatorische Banner sind Werbemittel im Internet, die eine Anwendung aufweisen oder eine solche vortäuschen, wobei die Anwendung jedoch meist vorgetäuscht ist. Typische Elemente sind Pull-Down-Menüs zum Anklicken oder Kästchen mit "Stop", "OK", "Cancel"

oder ähnlichem. Die applikatorischen Banner wollen mit graphischen Elementen die Click-Through-Rate (siehe Kapitel 2.5.2) erhöhen. Ein typisches Beispiel um die Internet-Benutzer zu überlisten, ist ein Banner, das wie eine Fehlermeldung aussieht. Manchmal sind die Banner versteckt, so dass sie vom Besucher der Seite gar nicht als Werbung erkannt werden können. Eine Unterform von applikatorischen Bannern sind zusätzliche Browserfenster, die sich öffnen oder Kästchen, in denen die Werbefläche erscheint. Ein analoges applikatorisches Element ist, wenn beim Klick auf das Back- oder Forward-Button des Browsers ein neues Fenster geöffnet wird.

Abbildung 4: Applikatorisches Banner

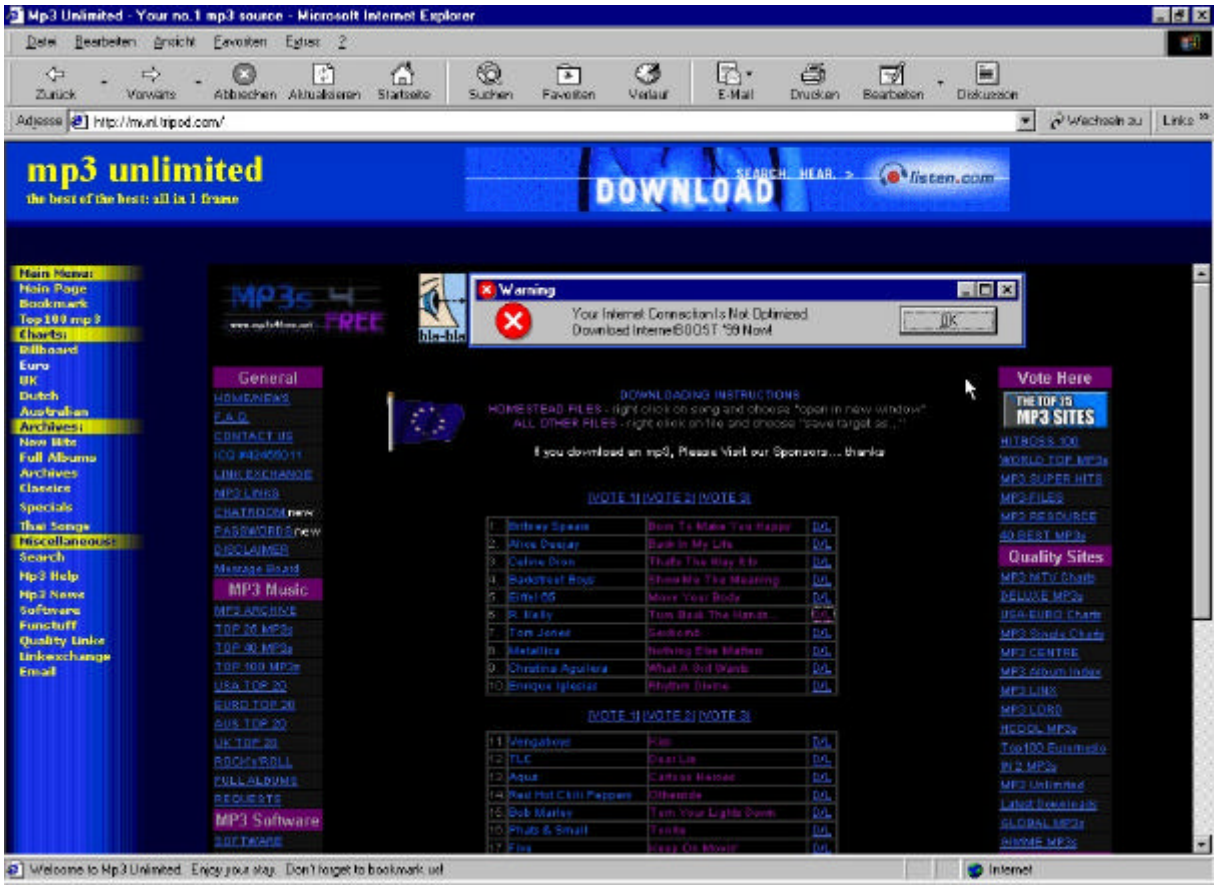


Abbildung 5: Applikatorisches Banner in einer Web-Seite

2.2.3.4 Narrative Banner

Narrative Banner sind Werbemittel im Internet in Form einer Bildfolge. "Narrativ" bedeutet sinngemäß "eine Geschichte erzählend". Ein narratives Banner ist eine Folge von einigen Bildern, die eine Handlung zum Inhalt hat. Ein narratives Banner ist das Pendant im Internet zu einem Spot im Fernsehen. Sie haben gegenüber animierten und vertonten Bannern den Vorteil, dass sie durch die technischen Gegebenheiten weniger eingeschränkt sind. Jeder Browser, der ein statisches Banner laden kann, bewältigt auch kleine Bild- und Textfolgen. Die Hauptgefahr des narrativen Banners ist, dass die Möglichkeiten überstrapaziert werden und die kleine Bildfolge zu einem ermüdenden Geflacker oder einem unendlichen Märchen ausartet.
Die Herstellung eines narrativen Banners ist auf ihre Weise ebenso komplex wie die Herstellung eines Werbespots. Die Grundlage ist ein Drehbuch mit Screenplay. Das Konzept erfordert viel Verständnis für das Internet als Medium, die Umsetzung ist Handwerk und gehört in die Hände einer spezialisierten Agentur. [BÜRLIMANN 99]

2.2.3.5 Site-in-the-Site

Eine komplett andere Form von Bannern ist die " Site-in-the-Site" - wörtlich "Eine-Seite-in-der-Seite", dem Sinn nach aber eher eine "Anwendung-in-der-Seite". Es handelt sich um Java-Anwendungen, die in ein Banner eingebaut sind. Die typische Anwendung bei der " Site-in-the-Site" ist eine direkte, einfache Einkaufsmöglichkeit.
Bei einer " Site-in-the-Site" ist eine Anwendung im Banner versteckt, respektive die Anwendung wird per Mausklick aktiviert. Die Grundidee ist, dem interessierten Besucher eine Anwendung zu bieten, die er unmittelbar ausführen kann. Damit bleiben die Werbeberührten auch nach dem Klick auf das Banner auf dem Werbeträger. Dies ist mit keiner anderen Bannerform möglich. Die " Site-in-the-Site" ist somit nicht ein Link auf eine andere Seite, wie es alle anderen Bannerformen sind, sondern die Anwendung ist direkt in den Werbeträger integriert.
Zu beachten ist, dass diese Werbeform noch nicht ausgereift ist und dass die Anwender somit mit unerwarteten Folgekosten rechnen müssen. Die Anwendungsform erscheint jedoch äußerst interessant, so dass es sich für größere Unternehmen lohnen könnte, Zeit und Geld in

diese neue Werbeform zu integrieren. Ideal ist eine Kombination von "Site-in-the-Site" mit digitalem Geld. Die Grundidee der "Site-in-the-Site"-Banner ist extrem vielversprechend, auch wenn die technischen Restriktionen heute noch viele Ideen im Keim ersticken. [BÜRLIMANN 99]

2.3 Platzierung des Banners auf der Web-Seite

In einer Studie („Banner Ad Placement Study von Kim Doyle, Anastasia Minor und Carolin Weynrich)[2] wurde der Zusammenhang zwischen der Platzierung eines Banners und seiner Ad Click Rate (d.h. wie oft ein Banner angeklickt wurde und somit wie erfolgreich die Bannerschaltung ist) untersucht und lieferte folgende Ergebnisse:

- Anzeigen neben dem Scroll-Balken erzeugen eine höhere Ad Click Rate. Benutzer klicken eher neben dem Scrollbalken, da ihre Augen schon auf den entsprechenden Bildschirmbereich fixiert sind.

- Die Ad Click Rate steigt, wenn die Anzeige um ein Drittel tiefer auf der Seite positioniert wird. Der Benutzer nimmt diesen Teil der Seite eher wahr.

- Zwei Anzeigen für das gleiche Produkt auf einer Seite erhöhen die Ad Click Rate. Für den Benutzer ist es bequemer (günstiger), auf die zweite Anzeige zu klicken, nachdem er die Seite gelesen hat.

2.4 Erhöhung der Trefferquote durch Bannerexchange

Folgende Beispiele sollen verdeutlichen, wie die Click-Rate durch Banneraustausch gesteigert werden kann.

Um die Steigerung der Hitrate zu demonstrieren, werden folgende Annahmen zum Bannerexchange getroffen:

[2] Die Studie ist ersichtlich unter http://www.webreference.com/dev/banners/index.html

- Annahme 1: Auf der Hauptseite sind 600 Besucher im Monat und auf zwei Nebenseiten auch noch je 200 Besucher
- Annahme 2: Die erste Banner-Version wird bei etwa jeder 50. Sichtung angeklickt
- Annahme 3: Man nimmt bei 2 Bannertausch-Anbietern teil, die je ein Verhältnis von 2:1 (für 2 gezeigte Seiten wird eine eigene ausgestrahlt) anbieten und mittels Subcodes werden auf den Nebenseiten andere Banner ausgestrahlt (statt dem Bild, das der Besucher bereits im Cache hat) und voll gezählt.
- Annahme 4: Man strahlt auf jeder der 3 Seiten je 2 Banner aus (je 1 pro Banner-Tausch-Anbieter)
- Annahme 5: Es finden keine Tricks statt, durch die Banner öfter angezeigt werden.

Dadurch ergibt sich:

- (600+200+200)* 1/2= 500 mal wird der Banner im Monat bei jedem der beiden Anbieter ausgestrahlt
- (500)*2% = 10 zusätzliche Besucher durch einen Banner-Tausch-Anbieter
- 10 * 2 = 20 zusätzliche Besucher im ersten Monat durch zwei Banner-Tausch-Anbieter (insgesamt 6 Fremd-Bannerplätze auf den 3 Seiten)

Diese Quote ist zwar nicht sehr hoch, stellt jedoch zunächst einen zufriedenstellenden Anfang dar.

Können viele der neu gewonnenen Besucher gehalten werden, kann man bei den späteren Berechnungen dann stets von einem höheren Wert ausgehen, wodurch auch wieder mehr neue Besucher gewonnen werden können.

Es gibt natürlich weitere Möglichkeiten, den Wert zu erhöhen. Um das zu erreichen, ist allerdings mehr Aufwand erforderlich!
[SOFTSURF 98]

Erhöhung der Hitrate beim Banneraustauschdienst *A-SITE BannerXchange*

A-SITE BannerXchange funktioniert nach einem einfachen Prinzip.
Auf der Site werden durch einmalige Installation eines HTML-Codes automatisch abwechselnd verschiedene Banner eingeblendet, dafür wird der eigene Banner kostenlos auf Seiten anderer Mitglieder des Banner-Exchange-Dienstes angezeigt. Für 2 Einblendungen auf der eigenen Seite wird der eigene Banner einmal auf einer anderen Seite angezeigt. Wenn man mehr als 200 Bannereinblendungen pro Woche auf der eigenen Site verzeichnen kann, beträgt das Verhältnis sogar 10:7.
Der HTML-Code, den man nach der Anmeldung bekommt und auf der eigenen Web-Site integriert wird, sorgt dafür, dass jedes Mal, wenn die Site aufgerufen wird, ein Banner eines anderen Mitgliedes zu sehen ist.
Klickt man auf ein Banner, kommt man auf die Seite des Mitgliedes mit diesem Banner

Vorteile des *A-SITE BannerXchange*
Angenommen, man hat auf der Hauptsite derzeit 600 Besucher/Monat und auf 2 weiteren Unterseiten je 200 Besucher/Monat. Man meldet sich beim *A-SITE Banner-Exchange* an und platziert auf jeder Seite 2 Subcodes (beim *A-SITE Banner-Exchange* erlaubt).
Somit ergeben sich (600+200+200)*2= 2000 Bannereinblendungen auf der Site und somit 1000 Einblendungen des eigenen Banners auf anderen Seiten. [A-SITE]

Weitere Möglichkeiten, um die Hitrate zu erhöhen

- Kostenlose Einblendungen
  Kurzfristig sind kostenlose Einblendungen eines Banners eine gute Hilfe. Diese gibt es bei manchen Anbietern als Starthilfe und auch bei Gewinnspielen zu gewinnen. Hier ist jedoch nicht mit einer hohen Steigerungsrate zu rechnen, denn 100 Gratiseinblendungen bringen bei einem durchschnittlich gutem Banner einmalig 2 Besucher.

- Höhere Einblendraten
  Die meisten Anbieter bieten bereits bessere Einblendeverhältnisse als das Verhältnis 1:2. Bei Doppelbanner-Einblendungen mit dem Verhältnis 1:1 ist allerdings anzumerken, dass dadurch das Verhältnis wieder auf 1:2 reduziert wird, da 2 Banner eingeblendet werden.

Statt dessen könnte man auch 2 Banner von verschiedenen Anbietern einblenden und ein höheres Verhältnis erzielen.

- Das Angebot attraktiv gestalten
  Indem man das Angebot attraktiv gestaltet bleiben mehr Stammbesucher und diese bringen wiederum mehr Einblendungen.

- Mehr Seiten statt längere Seiten
  Indem man die Quantität - die Seitenanzahl - des Angebots erhöht und auch dort Banner einsetzt, kann die Hitquote ebenfalls erhöht werden. Man muss jedoch darauf achten, dass das Verhältnis Information/Banner in einem vernünftigen Rahmen bleibt, so dass die Seite nicht von Bannern regelrecht überschwemmt wird.

- Bei mehreren Anbietern teilzunehmen ist auf jeden Fall empfehlenswert. Dadurch werden die Banner weiter gestreut, werden einem breiterem Publikum zugänglich und bleiben dadurch auch etwas länger aktuell. Ein wichtiger Faktor ist hier auch, dass man dadurch mehrere Banner auf einer Seite anbieten kann (vom selben Anbieter darf eigentlich immer nur 1 Banner pro Seite eingeblendet werden) und das eigene Banner wiederum auf mehreren Seiten aufscheinen - sofern keine Überladung mit Bannern entsteht und die Besucher das dulden (sonst würde sich dieses Vorgehen ad absurdum führen, da man dadurch vielleicht sogar mehr Besucher verlieren kann als gewinnen).

- Mehrere kostenlose Einblendungen nutzen und an Gewinnspielen teilnehmen.

- Mehrere Möglichkeiten nutzen in die beliebten Top 10 zu kommen und zusätzlich gesehen zu werden.

- Weiters kann man vergleichen, welcher Dienst einem unter welchen Umständen mehr Hits bringt oder persönlich mehr zusagt. Auch kann man entsprechend auf den eigenen Seiten umschichten.

- Die Attraktivität des Banners
  Durch attraktive gestaltete Banner kann die Click-Through-Rate ebenfalls beträchtlich erhöht werden

Welcher Anbieter bringt mehr?

Grundsätzlich ist die Anmeldung bei mehreren Bannertausch-Anbietern empfehlenswert. Anhand der Statistiken und Einblendeverhältnisse kann man umrechnen, wie viele neue Besucher pro Einblendungen durch jeden der Anbieter gekommen sind.
Wie wertvoll der Anbieter ist, ist dadurch ersichtlich, indem man die Click-Rate des Banners beim jeweiligen Anbieter mit dessen Einblendeverhältnis multipliziert.
Wenn man 100 Banner des Anbieters auf den eigenen Seiten einblendet und dieser aber nur 50 des eigenen Banners präsentierte, bei dem man ein Anklickverhältnis von 4% erreicht, dann hat man lediglich einen Nutzen von nur 2%, bei einem 4:3 Anbieter mit derselben Click-Rate des Banners wären es 3%.

Es sollten allerdings insgesamt zumindest mehrere hundert Einblendungen stattfinden, damit man eine erste Abschätzung des Einblendeverhältnisses machen kann. Denn auch bei der Click-Rate besteht ein großer Unterschied, ob von 100 Einblendungen 1x (1%) oder 3x (3%) das Banner angeklickt wurde, wobei die Situation bei den nächsten 100 Einblendungen wieder ganz anders aussehen kann.

Wenn man unschlüssig ist, welche Dienste man zuerst in Anspruch nehmen soll oder nur für wenige Anbieter Platz auf der Homepage zur Verfügung hat, sollte man die mit dem Banner-Exchange-Award ausgezeichneten Anbieter wählen. [SOFTSURF 98]

2.5 Abrechnung

Die Abrechnung der Bannerwerbung kann über verschiedene Abrechnungsmodelle erfolgen, wobei der Werbetreibende das für ihn günstigste Abrechnungsmodell ermitteln sollte, da dadurch ein erheblicher Kostenvorteil entstehen kann.

2.5.1 Werbung auf "befreundeten"-Web-Sites - Linkexchange

Linkexchange bzw. Verweisaustausch ist eine Art Ehrenkodex im Internet, der aber bestimmten ungeschriebenen Regeln unterliegt. Die meisten Webmaster sind einem gegenseitigen Tausch der Links auf das eigene Angebot zugeneigt. Besonders dann, wenn eine Artverwandtheit der Angebote vorliegt, also eine ähnliche Zielgruppe angesprochen wird. [NETCOLOGNE]

Diese Art der Werbung ist sehr zu empfehlen, da hier im Optimalfall überhaupt keine Kosten anfallen.

Folgende Regeln sollten jedoch beachtet werden [HAB8]:

- Es soll mit dem gleichen Banner, wie mit dem Banner des Bannertauschdienstes geworben werden. Einheitlichkeit ist ein Muss und der Wiedererkennungseffekt ein wichtiges Moment für die Werbung.

- Es soll nicht auf Seiten geworben werden, die das Gleiche anbieten wie das, für das geworben werden soll. Es besteht dadurch die Gefahr, dass man sich gegenseitig konkurriert.

- Es soll ein Verzeichnis mit den Orten, wo der Banner eingebunden wurde, erstellt werden. Bei einer Banneränderung erreicht man dadurch, dass die Einheitlichkeit der Werbung gewahrt bleibt.

- Es soll versucht werden, eine Statistik zur Einblendung des eigenen Banners zu bekommen.

2.5.2 CTR

CTR bezeichnet die Click-Trough-Rate. Hier wird der Prozentsatz der Besucher einer Web-Site ermittelt, die auf ein bestimmtes Banner klicken.
Die CTR berechnet sich nach folgender Formel: 100 * Bannerklicks / Anzahl der Bannereinblendungen gegenüber den Besuchern.

2.5.3 Zeitablauf

Hier wird das Banner über einen bestimmten Zeitraum eingeblendet, unabhängig von der Anzahl der tatsächlich eingeblendeten oder angeklickten Banner. (z.B. eine Woche oder ein Monat, oder nur den 27.2. und den 28.2., oder MO-FR von 12:00-13:00 Uhr)
Die Vorteile bei Zeitablauf sind, dass bei hoher CTR der Preis pro Click günstiger wird. Auch der Preis pro Page-View kann wesentlich günstiger ausfallen, wenn hohe Abrufzahlen vorhanden sind. Als Nachteil ist jedoch zu erwähnen, dass bei geringen Abrufzahlen und niedriger CTR Zeitablauf unverhältnismäßig teuer ist.
Man sollte sich daher für eine Abrechnung mittels Zeitablauf erst dann entschließen, wenn man sicher gehen kann, dass sich diese Abrechnungsform auch rentiert.

2.5.4 AdClicks

AdClicks sind besonders bei Bannertauschdiensten eine überlegenswerte Abrechnungsform. Hier wird nicht nach Anzahl der Einblendungen, sondern nach Anzahl der Klicks auf das Banner bezahlt. Man bezahlt hier daher nur für die Banner, die tatsächlich eingeblendet und auch angeklickt wurden. Die Bezahlung mittels AdClicks ist auch mit zeitlicher Beschränkung, etwa nur Montage von 13:00-15:00 Uhr, möglich.

Ein Nachteil besteht jedoch darin, dass dieses Abrechnungssystem bei einer hohen CTR sehr teuer wird.

Beim Banneraustauschdienst „Link4Link®“ kostet ein 500er-Paket "AdClicks" 2030.-DM inkl. MwSt. (ca. öS 14210,-- bzw. ca. 1032,7 Euro). Somit kostet jeder Klick auf das Banner 4,06 DM inkl. Mwst. (ca. öS 28,4 bzw. ca. 2,07 Euro).

Besuchen 50 Surfer die beworbene Web-Site ergeben sich daher Kosten in der Höhe von 203 DM (ca. öS 1421,-- bzw. ca. 103,3 Euro).
Bei der Annahme, dass 5 % der Besucher (guter Schnitt) zu Kunden werden, ergeben sich Kosten in der Höhe von ca. 81,2 DM (ca. öS 568,4 bzw. ca. 41,3 Euro) pro Neukunden. Diese Kosten können mit einer Erstbestellung kaum eingespielt werden, es sei denn es handelt sich um hochpreisige Produkte wie Autos. Bei einem Internet-Vertrieb von Niedrigpreisprodukten wie z.B. CDs wird sich diese Abrechnungsform daher kaum rentieren. Diese Art der Abrechnung rentiert sich nur, wenn der Neukunde zu einem Stammkunden wird und ist daher sehr riskant.

Diese Art der Abrechnung ist bei neuen Web-Sites interessant, wenn die Besucherrate noch gering ist, also eine niedrige CTR besteht. Will ein Banneraustauchdienst eine Bezahlung mittels AdClicks nicht akzeptieren, sollte man am besten einen zeitlich begrenzten Test vorschlagen: Man bezahlt, was einem ein AdClick wert ist, mindestens aber einen vereinbarten Mindestbetrag. Am Ende der Testzeit kann man ermitteln ob das Geschäft lohnend war und diese Art der Abrechnung fortsetzen oder zu einer anderen Abrechnungsart wechseln.

2.5.5 TKP

TKP ist die Abkürzung für den sogenannten Tausender-Kontakt-Preis für Banner. Mit diesem Begriff findet sich eine Richtgröße, welcher die eigene Analyse der Bannerwerbung erleichtert.

Beispiel:
Das Banner wird 2000 mal eingeblendet und 40 Surfer haben auf das Banner geklickt.

- (Klicks / Einblendungen * 100 = Klickrate) 100 * 40 / 2000 = 2% Klickrate
- Beim Einkauf von 20.000 Bannern für 812.- DM (ca. öS 5684 bzw. ca. 413,1 Euro) beträgt der TKP (inkl. Mwst.): 40,60 DM (ca. öS 284,2 bzw. ca. 20,65 Euro)

- 2.000 Bannereinblendungen haben somit 81,20 DM (ca. öS 568,4 bzw. 41,31 Euro) gekostet. Jeder Click kostete 2,03 DM (ca. öS 14,2 bzw. 1,03 Euro). [HAB8]

Werden von diesen Besuchern 5 % Neukunden (guter Schnitt), entstehen Kosten von 40,60 DM (ca. öS 284,2 bzw. ca. 20,65 Euro) pro Kunde. Nur wenn das Angebot sehr hochpreisig ist und man eine gute Gewinnspanne hat, bzw. wenn der Neukunde zu einem Stammkunden wird, können die Kosten pro gewonnenem Kunden auch wieder abgedeckt werden.

2.5.6 Konversionsrate

Die Konversions-Rate ist die wichtigste Größe zur Abrechnung der Bannerwerbung. Mit dieser, jedoch schwer zu ermittelnden, Größe sind jene Besucher der Web-Site gemeint, die tatsächlich zu Käufern werden. Realistisch gesehen liegt eine gute Konversions-Rate zwischen 1 % und 5 %. Höhere Konversionsraten sind eher die Ausnahme.

Die Bannerwerbung sollte immer nur als Teil einer erfolgreichen Site-Bewerbung betrachtet werden. Denn selbst bei 10% Konversionsrate ist Bannerwerbung immer noch teuer.
Es sollte daher von vornherein für einen positiven Kundenkontakt gesorgt werden. Nur so können die Kosten wieder eingespielt werden.
Es wäre daher falsch zu glauben, durch Bannerwerbung massive Neukundenzuwächse verzeichnen zu können. Was man mit Bannerwerbung bewirken kann ist, dass potentielle Neukunden auf die Web-Site aufmerksam gemacht werden. Erst durch die Kombination von Werbeformen externer und interner Werbung werden Käuferschichten angesprochen. Es ist daher die Summe der Werbungaktivitäten, die zum Erfolg führt.
Bannerwerbung ist lediglich ein wichtiger Baustein dieser Aktivitäten. [HAB8]

2.5.7 Abrechnungsvergleich mit Printinseraten

Vorsicht ist geboten bei enthusiastischen Versprechungen und Vergleichen mit Print-Inseraten:

1. Werden Banner zu weit gestreut, etwa in Search-Engines oder General-Interest-Onlinemedien, ist der TKP wesentlich höher als bei vergleichbaren Printmedien wie der

"Kronen-Zeitung", "News", etc. Man sollte deshalb „Äpfel mit Äpfel vergleichen“, indem die Streuung der Print- und Onlinemedien berücksichtigt werden.

2. Print-Inserate können von mehreren Personen gelesen werden. Fachzeitschriften etwa haben pro Exemplar 4 oder mehr Leser. Eine Banneranzeige hingegen wird in der Regel immer nur von einer Person gesehen, da der Internetsurfer meistens alleine vor dem PC sitzt. Bewegt sich ein Surfer in einem Online-Angebot, ruft er das Banner öfter auf, da durch die „Back“, „Forward“ und „Reload“ – Buttons eine Seite öfters aufgerufen wird. Da die Banner zumeist über CGI abgerufen werden, und somit nicht in einem Proxy-Server gespeichert sind, sollte man auf diese Punkte bei Verhandlungen hinweisen und weniger für die Bannerwerbung bezahlen.

3. Print-Inserate sind größer, und ziehen somit größere Aufmerksamkeit auf sich. Banner sind bei einer durchschnittlichen Bildschirmauflösung von 800x600 Punkten maximal 15x2cm groß. Man sollte deshalb bestenfalls das bezahlen, was man in einer vergleichbaren Zeitschrift für diese Größe bezahlen müsste.

4. Der "Vorteil" der Interaktivität: Surfer kommen oft durch Gewinnversprechungen oder sensationelle Lockangebote auf die Homepage und wandern dann genauso schnell ab, wie sie gekommen sind. "Printleser" von Fachzeitschriften hingegen, speziell Abonnenten, widmen den Anzeigen wesentlich mehr Aufmerksamkeit, weil sie nach interessanten Angeboten suchen und/oder Marktforschung betreiben. Man sollte deshalb die "Leser/Blattbindung" des für die Bannerwerbung verwendeten Onlinemediums bewerten.

   Man sollte hier außerdem beachten, wie hoch die Wiederbesuchsrate oder die Anzahl der elektronischen Newsletter-Abonnenten ist. Typische in Österreich vertretene Online-Medien wären etwa "NEWS" (http://www.news.at), die "Kronen-Zeitung" (http://www.krone.at) oder der "KURIER" (http://www.kurier.at).

5. Vorsicht ist auch bei Vergleichen mit Direct-Mailings geboten: 2 % Erfolgsrate bei Direkt-Mailings bedeutet 2 % neue Adressen von Interessenten, während 2 % CTR bedeutet, dass sich 2% der Angesprochenen das Angebot kurz angesehen haben. Sie werden dadurch noch nicht zu Kunden und man erhält auch keine Kontaktadresse. Man

sollte deshalb solche Vergleiche zurückweisen und weniger zahlen sowie Registrierungen bei Folgeseiten von Bannern einbauen, um Kundendaten zu sammeln.

Generell sollte man das Banner auf jeden Fall testen bevor man es schaltet und möglicherweise zu hohe Kosten bezahlen muss. Bannertausch bietet eine billige Möglichkeit, die CTR zu erheben und bei Bedarf zu verbessern.

Kostenbeispiele pro 1.000 PageViews bei Bannertausch:

Stern Online: 60-130 DM,
Focus-Online: 80-100 DM

[HEIM 98]

2.6 Bannerabwehr

Da mit Bannern überladene Web-Sites für viele Surfer durch die erhöhten Ladezeiten und die damit verbundene Vergeudung wertvoller Bandbreite ein immer größer werdendes Ärgernis darstellen, wurde von der Softwareindustrie darauf reagiert und entsprechende bannerfilternde Programme entwickelt.

Angesichts des Erfolgs von diesen bannerabwehrenden Programmen machte sich bei den Online-Medien sehr rasch Nervosität breit. Einige Anbieter denken schon laut über die Einführung von Nutzungsgebühren nach, da sie ihre Werbeeinnahmen schwinden sehen. Dass es dazu kommen wird, ist jedoch eher unwahrscheinlich, da in den USA Werbeblocker wie beispielsweise der Junkbuster (http://internet.junkbuster.com) schon sehr lange populär sind. Dennoch zeichnet sich dort kein Trend zu gebührenpflichtigen Angeboten ab, sondern im Gegenteil dazu kehrt Microsoft mit seinem sogenannten „Slate“-Angebot (http://www.slate.com) eben erst wieder vom Abonnementmodell zur Werbefinanzierung zurück.

Langfristig können nur die Werbetreibenden dieses Dilemma selbst lösen indem sie vom praktizierten „Belästigungsmodell“, welche die User generell mit Bannerwerbung überhäuft, Abstand nehmen und zu einer individualisierten Zielgruppenwerbung übergehen, wie dies

zum Beispiel bei Freemailaccounts wie etwa „gmx“ der Fall ist. Ein solcher Paradigmenwechsel würde aber auch die Mitwirkung der potentiellen Kunden voraussetzen. Solange es aus falsch verstandenem Datenschutz und übertriebenem Sicherheitsdenken auch von Anwendern, die Werbung wünschen, keine Nutzerprofile gibt, muss sich die Reklamebranche an die herkömmliche Massenwerbung halten.

2.6.1 WebWasher

Die von der Firma Siemens entwickelte Software „WebWasher“ ist ein Tool, welches Werbung aus Web-Seiten sehr wirkungsvoll herausfiltert. Der dadurch für den Anwender entstehende Vorteil ist, dass beim Öffnen einer Web-Seite kürzere Ladezeiten entstehen, andererseits bangen die Anbieter von Seiten mit kostenlosen Inhalten (z.B. Download-Sites) um ihre Werbeeinnahmen.

Siemens verzeichnet rund 7000 Downloads pro Tag, was von der Popularität diese Hilfsmittels zeugt und andererseits wiederum aufzeigt, dass mit der derzeitigen Form der Internetwerbung vielleicht ein falscher Weg beschritten wird. Ebenso wird das Programm auf diversen anderen Web-Sites angeboten.

Funktionsweise des „WebWasher“s

Der „WebWasher“ arbeitet als HTTP-Proxy, dessen Adresse man in der Konfiguration des Browsers einstellen muss. Dieser fordert Daten dann nicht direkt aus dem Internet an, sondern schickt zuerst eine Anfrage an den „WebWasher“, der leitet diese Anfrage ins Netz weiter, empfängt anschließend die Daten aus dem Netz filtert die Werbung aus und liefert das Ergebnis an den Browser zurück.

Das Programm läuft unter Windows 95/98/Me/2000, NT 4.0, Linux und Mac. Dank der Einbindung als Proxy funktioniert es mit jedem Browser, der diese Technik unterstützt, also zum Beispiel mit dem Netscape Navigator und dem Microsoft Internet Explorer ab Version 2.0. Da „WebWasher“ die Daten auf Wunsch über einen weiteren Proxy beziehen kann, fügt er sich auch nahtlos in Intranets ein. Zudem kann er auch von anderen Rechnern im lokalen Netz genutzt werden. Der „WebWasher“ lädt die Werbebanner nicht vom Server und spart dadurch Online-Zeit beziehungsweise Bandbreite. Er nutzt zwei Methoden, um Banner zu

erkennen: Eine Liste mit typischen Größen und eine mit bestimmten URLs. Die Werbebranche hat sich nämlich auf bestimmte Standardgrößen für Banner geeinigt. Allerdings filtert der „WebWasher“ auch andere Bilder mit banner-typischen Abmessungen aus und lässt Werbung durch, die davon abweicht. Das tritt in der Praxis jedoch sehr selten auf. Außerdem kann man die Liste der Bildgrößen, die ausgefiltert werden, editieren.

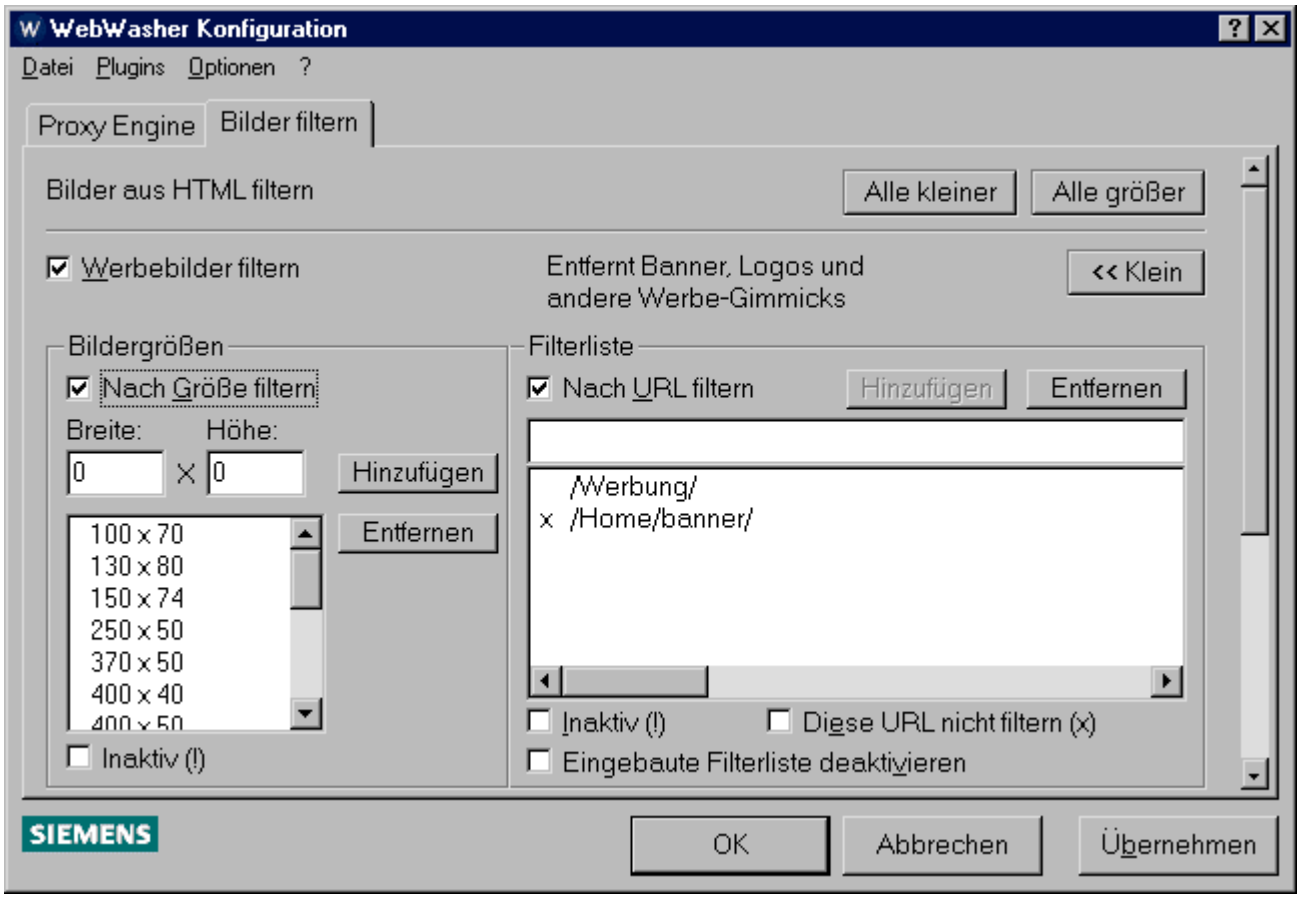


Abbildung 6: „WebWasher“ Konfiguration

Die Liste der gesperrten URL-Muster ist nicht einsehbar. Sie lässt sich aber ebenfalls erweitern; man kann Adressmuster, die in der Voreinstellung gesperrt werden, auch wieder freigeben. Um den „WebWasher“ kurzfristig zu deaktivieren, genügt ein Mausklick auf das Icon in der Tas-Leiste. Neben den Bannern kann der „WebWasher“ auch Pop-Up-Fenster abwehren, wie sie häufig benutzt werden, um Werbung einzublenden.

Die Installation funktioniert äußerst einfach durch das Ausführen der Datei „setup.exe“ und anschließender dialoggesteuerter Installation wie es von herkömmlichen Windows-Programmen bekannt ist. Nach erfolgreicher Installation muss lediglich nur noch der Proxy-Eintrag des Browsers angepasst werden. Eine ausführliche Anleitung dazu wird automatisch

angezeigt. Zur Zeit stehen die Versionen 3.0 (1021 kB) und 2.2.1 (1013 kB) zum Download zur Verfügung.

Laut Angaben der Fa. Siemens könne der „WebWasher“ bis zu 45 Prozent Bandbreite sparen, wobei jedoch anzunehmen ist, dass es sich hierbei um eine sehr optimistische Schätzung handelt. Erfahrungswerten aus der Praxis zufolge liegt die tatsächliche Einsparung eher zwischen 20 und 30 Prozent. [3]

2.6.2 Junkbuster

Der Internet Junkbuster ist technisch gesehen ein „nicht-cachender“ HTTP Proxy-Server, wobei mit „nicht-cachend“ gemeint ist, dass der Junkbuster keine Daten lokal speichert.

In der Praxis bedeutet dies, dass der Junkbuster verwendet werden kann, um

- Werbebanner auszublenden
- Die Privatsphäre der User zu schützen (Ausblenden von sog. „*cookies*“ und anderer Informationen, z.B. „*referer*“ und „*user-agent*“)
- Bestimmte Web-Sites zu sperren: ausgewählte URLs lassen sich mithilfe sog. „Regulärer Ausdrücke“ (*regular expressions*) „blocken“

Der Junkbuster (ijb) eignet sich hervorragend dafür, Werbemüll aus dem Internet herauszufiltern. Es kann sich dabei um Werbebanner handeln, oder auch, wie oben erwähnt, um Cookies.

Dieses Programm klinkt sich in den Internet-Datenstrom als "Proxy" ein und verhindert den Eingang von Inhalten beliebig definierter Quellen. Dadurch kann es sowohl auf dem Rechner des ISPs als auch auf dem des Surfers betrieben werden. Beispiel: Beim Einwählen in die Suchmaschine Altavista wird am Anfang der Seite immer ein Werbebanner angezeigt. Dieses stammt von der Internetadresse "ad.se.doubleclick.net". Wird JunkBuster diese Adresse mitgeteilt, werden zukünftig Inhalte von dort nicht geladen und das Werbebanner nicht mehr angezeigt. Natürlich kann auch die Anzeige von Daten spezifischer Web-Sites grundsätzlich

[3] Die Shareware „WebWasher“ kann man von http://www.webwasher.com/de/index.htm. Sie ist für nicht-kommerzielle Anwender kostenlos, Firmen zahlen nach 30 Tagen Lizenzgebühr.

blockiert, das Übertragen von Cookies oder der Eingang von Spam-E-Mail verhindert werden. Der Nachteil ist, dass bestimmte Angebote im WWW nicht mehr funktionieren - z.B. gibt der Webserver von Microsoft keine Seiten mehr heraus, wenn kein Cookie beim User deponiert werden darf.

Ein großer Vorteil des Programms ist jedoch, dass es für alle Rechnerplattformen verwendbar ist.

3 Spamming

Mit der zunehmenden Anzahl an elektronisch ausgetauschten Nachrichten (E-Mails) steigt leider auch die Zahl der unerwünschten E-Mails. Meist handelt es sich dabei um Werbe-E-Mails, in denen Produkte, Dienstleistungen oder WWW-Seiten angepriesen werden, an denen die Empfänger in der Regel keinerlei Interesse haben.
Massen-E-Mails, sogenannte Spam-Mails, sind nicht nur für den Empfänger störend, sondern können auch erhebliche Probleme für Datenschutz- und Sicherheit verursachen:

- häufig sind die E-Mail-Adressen aller angeschriebenen Empfänger im Header der E-Mail erkennbar und werden damit verteilt.
- durch den Absturz bzw. Ausfall eines Mailservers durch den Versand solcher Massen-E-Mails können wichtige E-Mails verloren gehen und auch erhebliche Kosten entstehen.

Darüber hinaus verursachen Spam-Mails auch erhebliche Kosten auf Seiten des Empfängers, denn dieser finanziert die Bandbreite, vergeudet Zeit beim Download und hat darüber hinaus auch noch die Aufgabe den Werbemüll zu löschen. [CERT 99]

Spam ist schnell zu einem der großen Probleme im Internet geworden. Während der Ärger der User über unverlangte Werbe-E-Mails wächst, steigt auch die Aggressivität der Spammer.

3.1 Definition

„Spam“ ist zunächst ein Produkt der Firma „Hormel Foods Corporation“, USA. Es handelt sich hier um gewürztes Schweinefleisch und Schinken in Dosen. Es ist ein Kunstwort aus den Anfangsbuchstaben „spiced pork and ham“.
Der nächste Schritt in der Entwicklung des Wortes stammt von der englischen Komiker-Gruppe „Monty Python's Flying Circus“'. In einem Sketch dieser Gruppe wird der Begriff „Spam“ in wenigen Minuten mehr als 120 mal wiederholt.
Aus dieser massenhaften Wiederholung desselben Begriffes in kurzer Zeit übernahmen Usenet-Benutzer das Wort auch für ihr Medium: Das massenhafte Verbreiten desselben Artikels in den Newsgroups wurde ebenfalls „Spam“ bzw. das zugehörige Verb „spamming“

genannt. Von dort wurde der Begriff später auf andere Internet-Medien wie E-Mail und WWW übernommen. [BRAUNSCHWEIG 98]

Die englische Originalversion dieses Sketches ist ersichtlich unter *http://www.ironworks.com/comedy/python/spam.htm*

Unabhängig von dieser kuriosen Bezeichnung steht Spam für die Abkürzung von „Send Phenomenal Amounts of Mail“.

Eine andere, wenn auch nicht so ernst zu nehmende Interpretation ist, dass Spam für "*Stupid Person's AdvertiseMent*" steht.

Spam ist im weitesten Sinne eine Sammelbezeichnung für unerwünschte, belästigende Nachrichten in Form von E-Mail oder Usenet-Beiträgen. Bei E-Mail-Spamming spricht man auch von Junk-E-Mail.
Im folgenden ist ein solches Junk-E-Mail, welches der Autor dieser Arbeit selbst erhalten hat, abgebildet (die im E-Mail enthaltenen Artikel wurden vom Autor tw. gekürzt):

```
Betreff: laser printer toner advertisement
Datum:   Mon, 24 Apr 2000 05:42:09
Von:     benchmark@conok.com

BENCHMARK SUPPLY
5334 LAKE VIEW CLUB
ATLANTA GA 30338

***LASER PRINTER TONER CARTRIDGES***
***FAX AND COPIER TONER***

WE ACCEPT GOVERNMENT, SCHOOL & UNIVERSITY PURCHASE ORDERS
JUST LEAVE YOUR PO # WITH CORRECT BILLING & SHIPPING ADDRESS

CHECK OUT OUR NEW CARTRIDGE PRICES :

APPLE

  LASER WRITER  PRO 600 OR 16/600         $69
  LASER WRITER SELECT 300,310.360         $69
  LASER WRITER 300, 320                   $54
  LASER WRITER LS,NT,2NTX,2F,2G & 2SC     $54
  LASER WRITER 12/640                     $79
```

HEWLETT PACKARD

LASERJET SERIES 2,3 & 3D (95A)	$49
LASERJET SERIES 2P AND 3P (75A)	$54
LASERJET SERIES 3SI AND 4SI (91A)	$75
LASERJET SERIES 4L AND 4P	$49

HP LASERFAX

LASERFAX 500, 700, FX1,	$59
LASERFAX 5000, 7000, FX2,	$59
LASERFAX FX3	$69
LASERFAX FX4	$79

LEXMARK

OPTRA 4019, 4029 HIGH YIELD	$135
OPTRA R, 4039, 4049 HIGH YIELD	$135
OPTRA S 4059 HIGH YIELD	$135
OPTRA E	$59
OPTRA N	$115

EPSON

EPL-7000, 8000	$105
EPL-1000, 1500	$105

CANON

LBP-430	$49
LBP-460, 465	$59
LBP-8 II	$54
CANON FAX L700 THRU L790 FX1	$59
CANONFAX L5000 L70000 FX2	$59

CANON COPIERS

PC 20, 25 ETC....	$89
PC 3, 6RE, 7, 11 (A30)	$69
PC 320 THRU 780 (E40)	$89

NEC

SERIES 2 LASER MODEL 90,95	$105

PLEASE NOTE:

1) ALL OUR CARTRIDGES ARE GENUINE OEM CARTRIDGES.
2) WE DO NOT SEND OUT CATALOGS OR PRICE LISTS
3) WE DO NOT FAX QUOTES OR PRICE LISTS.
4) WE DO NOT SELL TO RESELLERS OR BUY FROM DISTRIBUTERS
5) WE DO NOT CARRY: BROTHER-MINOLTA-KYOSERA-PANASONIC PRODUCTS
6) WE DO NOT CARRY: XEROX-FUJITSU-OKIDATA OR SHARP PRODUCTS
7) WE DO NOT CARRY ANY COLOR PRINTER SUPPLIES
8) WE DO NOT CARRY DESKJET/INKJET OR BUBBLEJET SUPPLIES
9) WE DO NOT BUY FROM OR SELL TO RECYCLERS OR REMANUFACTURERS

****OUR ORDER LINE IS 770-399-0953 ****

****OUR CUSTOMER SERVICE LINE IS 800-586-0540****
****OUR E-MAIL REMOVAL AND COMPLAINT LINE IS 888-494-8597****

****PLACE YOUR ORDER AS FOLLOWS**** :

BY PHONE   770-399-0953

BY FAX: 770-698-9700
BY MAIL: BENCHMARK PRINT SUPPLY
           7540 BRIDGEGATE COURT
,   ATLANTA GA 30350

MAKE SURE YOU INCLUDE THE FOLLOWING INFORMATION IN YOUR ORDER:

1) YOUR PHONE NUMBER
2) COMPANY NAME
3) SHIPPING ADDRESS
4) YOUR NAME
5) ITEMS NEEDED WITH QUANTITIES
6) METHOD OF PAYMENT. (COD OR CREDIT CARD)
7) CREDIT CARD NUMBER WITH EXPIRATION DATE

1) WE SHIP UPS GROUND. ADD $4.5 FOR SHIPPING AND HANDLING.
2) COD CHECK ORDERS ADD $3.5 TO YOUR SHIPPING COST.
2) WE ACCEPT ALL MAJOR CREDIT CARD OR "COD" ORDERS.
3) OUR STANDARD MERCHANDISE REFUND POLICY IS NET 30 DAYS
4) OUR STANDARD MERCHANDISE REPLCAMENT POLICY IS NET 90 DAYS.

NOTE NUMBER (1):

PLEASE DO NOT CALL OUR ORDER LINE TO REMOVE YOUR E-MAIL ADDRESS OR COMPLAIN. OUR ORDER LINE IS NOT SETUP TO FORWARD YOUR E-MAIL ADDRESS REMOVAL REQUESTS OR PROCESS YOUR COMPLAINTS..IT WOULD BE A WASTED PHONE CALL.YOUR ADDRESS WOULD NOT BE REMOVED AND YOUR COMPLAINTS WOULD NOT BE

```
HANDLED.PLEASE CALL OUR TOLL FREE E-MAIL REMOVAL AND
COMPLAINT LINE TO DO THAT.

NOTE NUMBER (2):

OUR E-MAIL RETURN ADDRESS IS NOT SETUP TO ANSWER ANY
QUESTIONS YOU MIGHT HAVE REGARDING OUR PRODUCTS. OUR E-MAIL
RETURN ADDRESS IS ALSO NOT SETUP TO TAKE ANY ORDERS AT
THIS TIME. PLEASE CALL THE ORDER LINE TO PLACE YOUR ORDER
OR HAVE ANY QUESTIONS ANSWERED. OTHERWISE PLEASE CALL OUR
CUSTOMER SERCICE LINE.
```

(Der zu diesem Spam-Mail dazugehörige Header ist im Kapitel 3.5 ersichtlich)

3.2 Entwicklung von Spam

Die Ursache von Spam ist die Tatsache, dass die Medien wie Usenet und E-Mail es ermöglichen, mit sehr geringen eigenen Kosten eine große Menge von Empfängern zu erreichen.

Spamming ist somit zu einem ernsten Problem in Internet geworden. Bereits im Frühjahr 1994 waren die digitalen Postwurfsendungen ein Thema in Newsgroups. Hintergrund der Diskussion war eine Werbe-Aktion der Anwaltskanzlei "Canter and Siegel", die ein "U.S. Green Card Lottery"-Angebot an über 8000 Newsgroups geschickt hatte. Der Protest gegen diese Aktion äußerte sich in Form einer Flut von Mailbomben, die den Provider der Kanzlei schließlich dazu zwangen, den E-Mail-Zugang der Kanzlei zu schließen. [AKADEMIE 98]

3.2.1.1 Usenet

Usenet wurde als erstes befallen, z.B. durch den "Canter&Siegel-Greencard-Spam".
Dort wird das Phänomen durch halbautomatisches (Fremd-)Canceln (siehe Kapitel 3.8.2) von Artikeln nach formalen Kriterien bekämpft.

3.2.1.2 Native E-Mail

In weiterer Folge gingen die "Werber" dazu über, sich Listen von E-Mail-Adressen zu besorgen, und sie auf Ihren Rechnern abzuarbeiten.

Das führte natürlich schnell zu Beschwerden bei den Absendern, und wenn diese ignoriert wurden, zu Beschwerden bei deren Providern.
Nachdem diese sich nicht vor den Beschwerden verschließen konnten, ohne ihren guten Ruf zu verlieren, griffen sie zu technischen und rechtlichen Maßnahmen.
Teilweise wird die Mailversendungsrate über den Server des Providers begrenzt.
In den TOS (Terms of Service) oder der AUP (Acceptable Use Policy) wird das Spammen verboten und teilweise mit hohen Vertragsstrafen bis zu 1000$ pro Fall geahndet, was jedoch nicht sehr wirksam ist.

3.2.1.3 E-Mail Relaying

Die Reaktion auf die in Punkt 3.2.1.2 erwähnten Vertragsstrafen war, nicht den Server des Providers zu benutzen, sondern über andere Mailserver zu relayen, die dann auch das Vervielfältigen der E-Mail erledigen.

Technische Realisierung:

Nur in den seltensten Fällen wird eine E-Mail vom sendenden System direkt zum Mail-Server des Empfängers transportiert. In der Regel wird die zu transportierende E-Mail über mehrere dafür vorgesehene Transportsysteme (Message Transfer Agents, MTA) geleitet, die z.B. folgende Aufgaben erledigen:

- Auswahl des geeigneten Übertragungsweges (insbesondere dann, wenn das sendende System dazu nicht fähig ist)
- Zwischenspeicherung bei Ausfall von Übertragungswegen
- Ausgangs- bzw. Eingangspostamt der Einrichtung (z.B. in Verbindung mit einer Firewall)
- Mailbearbeitung, z.B. Adressumsetzungen, Filterungen, ...

Als Mail-Relaying wird das Entgegennehmen und anschließende Weiterleiten einer E-Mail durch ein Rechnersystem bezeichnet. Der dafür genutzte Rechner ist dann ein Mailrelay-Rechner, kurz auch Mailrelay genannt.

Ein Missbrauch liegt vor, wenn ohne Notwendigkeit (oder ohne Berechtigung) ein fremder Rechner zum Mailtransport/Mail-Relaying benutzt wird.
Wichtig ist das Verhältnis *absendender Rechner* → *nächster Mailserver*.
Auf den benutzten Übertragungsweg hat der normale Mail-Nutzer im allgemeinen keinen Einfluss. Entsprechende Steueranweisungen in den zentralen Mail- und Internet-Systemen weltweit enthalten alle notwendigen Informationen.

In jüngerer Vergangenheit werden nun bisher weltoffene Mailserver - insbesondere auch Mailsysteme von Universitäten und Hochschulen - von verantwortungslosen Firmen, Einrichtungen und Einzelpersonen immer wieder zur Verbreitung unerwünschter Massenmails (Werbung, Verbreitung von Computerviren, ...) missbraucht (der Transport über Fremdsysteme erfolgt z.B. auch, um Spuren zu verwischen). Neben dem Verbrauch wichtiger rechentechnischer Ressourcen (bis hin zum Ausfall des Rechners wegen Überlastung - mehrere tausend E-Mails je Stunde überfordern viele Systeme) entsteht auch für die so missbrauchte Einrichtung ein nicht unbeträchtlicher Schaden.
Deshalb gehen immer mehr Einrichtungen dazu über, ihre vorhandenen Mailsysteme durch Zugriffsbeschränkungen und andere Konfigurationsmaßnahmen gegen einen solchen Missbrauch zu schützen bzw. zentral sogar zusätzliche Rechner für diesen Zweck einzusetzen. Dabei ist dennoch klar, dass es einen sicheren und vollständigen Schutz mit vernünftigem Aufwand nicht geben kann. [UNI-HALLE 98]

Gleichzeitig hat sich ein Markt für Software gebildet, die Mail-Relaying automatisiert, welche wiederum über Spam vertrieben werden.

Solche Software versucht (mehr oder weniger erfolgreich), den wirklichen Einspeisepunkt zu verheimlichen, indem gezielt im Internet nach schlechten SMTP-Serverimplementierungen gesucht wird, die kein korrektes Log-In in den Received-Zeilen durchführen.

3.3 E-Mail-Grundlagen

E-Mail ist wahrscheinlich der einfachste Internetdienst, da er lediglich aus dem Senden einfacher Textnachrichten zwischen zwei Computern besteht.
Um E-Mail nutzen zu können, benötigt man einen Internetzugang sowie eine Mailbox auf einem mit dem Internet verbundenen Rechner.
Diese Mailbox ist gekennzeichnet durch eine eindeutige Adresse (E-Mail-Adresse), welche sich aus der Benutzeradresse und der Rechneradresse des für die E-Mail-Konto zuständigen Rechners zusammensetzt, wobei beide Teile durch das "@"-Zeichen getrennt sind.
Die Benutzeradresse ist normalerweise die Login-Kennung des Benutzers oder ein Aliasname, der auf die Login-Kennung zeigt. Die Rechneradresse ist die eindeutige Internetadresse (IP-Adresse) des für die Mailbox zuständigen Rechners.
Bei der E-Mail-Adresse `hans.wurst@jk.uni-linz.ac.at` wäre `hans.wurst` der Aliasname, der auf die Login-Kennung k0000e0 des Benutzers Hans Wurst zeigt. Die auf dem Rechner verwaltete E-Mail-Adresse lautet daher tatsächlich k0000e0@jk.uni-linz.ac.at.

3.3.1 Versenden von E-Mail

Wird ein E-Mail versendet, versucht der sendende Rechner eine Verbindung zum Zielrechner aufzubauen. Kommt es beim Verbindungsaufbau zu Verzögerungen, wird die E-Mail in einer Warteschlange zwischengespeichert. Der Senderrechner versucht nun in voreingestellten Zeitintervallen eine Verbindung zum Zielrechner aufzubauen. Gelingt der Verbindungsaufbau nach einer definierten Anzahl von Verbindungsversuchen nicht, geht der Senderrechner davon aus, dass die E-Mail nicht zugestellt werden kann und die E-Mail wird mit einer Fehlermeldung an den Absender zurückgeschickt. Wurde die Verbindung erfolgreich aufgebaut, versucht der Senderrechner festzustellen, ob die E-Mail-Adresse am Empfängerrechner bekannt ist. Verläuft diese Überprüfung positiv, wird die E-Mail an die Empfänger-Mailbox ausgeliefert, ansonsten wird der Vorgang abgebrochen und die E-Mail wiederum mit einer entsprechenden Fehlermeldung an den Senderrechner zurückgeschickt.

Das zum Versenden von E-Mail-Nachrichten verwendete Protokoll ist das Simple Mail Transport Protocol (SMTP) nach Internet "Request For Comments" RFC 821, welches weltweit den größten Teil des E-Mail-Verkehrs regelt (falls nicht durch IMAP 4 geregelt). Um zu einem Rechner E-Mail schicken zu können, muss dieser einen sogenannten SMTP-Server betreiben. Wird ein E-Mail von einem Rechner zum anderen versendet, nehmen beide eine SMTP Verbindung auf. Der Sender setzt einen Befehl ab (sendet die E-Mail) und der Empfänger antwortet mit einer Bestätigung (Confirmation), einer Fehlermeldung (error message) oder der angeforderten Information. Die Antwort vom Empfängerrechner besteht immer aus einem 3-stelligen Zahlencode (Reply Code) und Text.

3.3.2 Empfangen von E-Mail – POP 3

Das Empfangen von E-Mail wird großteils über das POP3-Protokoll (Post Office Protokoll Version 3) nach Internet RFC 1460 geregelt. Voraussetzung zum Empfang von E-Mail ist wiederum, dass auf dem Mail-Server ein POP3-Server läuft.
Das POP3-Protokoll wurde speziell dafür entwickelt, um es einem Mailprogramm zu ermöglichen, Mails von einem Server abzuholen, wobei das abholende Programm sich mit Kennung und Passwort ausweisen muss.
Die Vorteile von POP3 sind, dass das Mailprogramm alle E-Mails vom Server abholt, sobald es gestartet wurde und eine Verbindung zum Internet besteht (die Option „Leave messages on server“ muss deaktiviert sein). Bricht während der Übertragung die Verbindung ab, sind die E-Mails auf der lokalen Festplatte des Rechners, auf welchem das Mailprogramm läuft, gespeichert. Noch nicht heruntergeladene Mails verbleiben auf dem Mailserver und können zu einem späteren Zeitpunkt heruntergeladen werden.

3.3.3 Empfangen von E-Mail – IMAP 4

IMAP4 (Interactive Mail Access Protocol Version 4) verfolgt einen ähnlichen Ansatz wie POP3, es werden hier jedoch komplexere Funktionen implementiert und ein größerer Teil der Last auf den Mailserver verlegt. Auch hier ist Voraussetzung, dass auf dem Mailserver ein IMAP4-Server läuft.
Der Vorteil von IMAP4 ist, dass alle Nachrichten auf dem Server bleiben und bei einer Sitzung nur die Header ohne Message-Body und MIME-Anteil (Multipurpose Internet Mail

Extension; Protokoll, welches im Internet eine Binärdatei beliebigen Inhalts in eine Textdatei einbindet. MIME-Typen werden bei der Kommunikation zwischen WWW-Server und WWW-Browser eingesetzt. Sowohl der WWW-Server als auch der WWW-Browser unterhält eine Liste mit ihm bekannten Dateitypen. In vielen WWW-Browsern (z.B. bei Netscape) ist das die Liste der sogenannten "Helper Applications". Beim Übertragen vom Server zum Browser wird über das HTTP-Protokoll der MIME-Type mit übertragen. Aufgrund seiner Liste mit MIME-Typen weiß der WWW-Browser, wie er die Datei zu behandeln hat) übertragen werden. Es wird dadurch ein vorselektieren der enthaltenen Nachrichten erlaubt. Dieser selektive Mailtransfer wird mittels serverseitigen Suchalgorithmen ermöglicht.
Wird eine Nachricht zur Bearbeitung ausgewählt, wird eine Kopie zur Bearbeitung auf den Rechner übertragen. Dadurch wird Zeit beim Hochlaufen erspart und die Synchronisation der Mailboxen zwischen Rechner und Mailserver entfällt. Markiert der Benutzer eine Nachricht als gelesen, werden alle Änderungen der Mailbox auf dem Server gespeichert und dem Benutzer steht immer eine aktuelle Mailbox zur Verfügung. Weiters kann simultan auf Mailboxen verschiedener Server zugegriffen werden.

IMAP konnte sich bisher jedoch vermutlich deshalb noch nicht als Internetstandard etablieren, da die serverseitigen Operationen den Providern zu ressourcenintensiv sind. Weitere Nachteile sind, dass eine Dauerverbindung zum Internet erforderlich ist und kein Batch-Betrieb möglich ist.

3.4 Sammlung von Adressen

In diesem Kapitel soll dargestellt werden, wie Spammer zu den E-Mailadressen der betroffenen User gelangen um diese mittels Spam zu bewerben.

3.4.1 Newsgroup-Beiträge mit Angabe der E-Mailadresse

Spammer durchsuchen regelmäßig die Newsgroups mittels eigenen Programmen nach E-Mailadressen. Einige dieser Programme durchsuchen lediglich den Header eines Artikels (*From*:, *Reply-To*: etc.), während andere Programme den ganzen Artikel nach dem "@"-Zeichen durchsuchen und dadurch versuchen, E-Mailadressen zu entdecken.

Personen, welche häufig gespammt wurden, berichteten, dass nach einer gewissen Zeit, in der sie an keiner Newsgroup-Diskussion teilgenommen haben, die Häufigkeit erhaltener Spam-Mails stark abgenommen hat.
Es wird deshalb auch vermutet, dass Newsgroups die primäre Quelle für Spammer sind, um gültige E-Mailadressen zu sammeln.

3.4.2 Mailinglisten

Spammer versuchen regelmäßig Listen von eingetragenen Mitgliedern in Mailinglisten zu erhalten, da manche Mailserver diese Listen auf Anfrage freigeben. Der Vorteil bei der Adressensammlung von Mailinglisten ist, dass nur wenige ungültige Adressen eingetragen sind.

Wenn ein Mailserver auf Anfrage die Liste der Mitglieder nicht freigibt, wenden Spammer einen anderen Trick an; Sie senden ein E-Mail an die Mailingliste mit dem `Header Return-Receipt-To: <E-Mailadresse>` oder `X-Confirm-Reading-To: <E-Mailadresse>.` Diese Header bewirken, dass bestimmte Mail-Transfer-Agenten oder bestimmte Leseprogramme eine E-Mail an die im Header unter `<E-Mailadresse>` spezifizierte E-Mailadresse zurückschicken. Diese E-Mails beinhalten Informationen, an welche E-Mailadressen dieses Mail übermittelt wurde und gibt Spammern somit wiederum die E-Mailadressen der in die Mailingliste eingetragenen Mitglieder bekannt.

Eine weitere von Spammern angewandte Technik ist, eine Abfrage um Übermittlung einer Liste aller Mailinglisten, welche der Server verwaltet, an einen Mailserver zu stellen. Diese Möglichkeit ist bei manchen Mailservern zur Userlegitimation vorhanden. An die vom Mailserver übermittelten Adressen werden dann von Spammern E-Mails geschickt, wobei in der Regel dem Mailserver, von welchem die Adressen gesammelt wurden, die Arbeit überlassen wird, an jedes Mailinglistenmitglied eine Kopie des Spam-Mails zu forwarden.

3.4.3 Webseiten

Spammer benutzen spezielle Programme, welche Webseiten nach E-Mailadressen durchsuchen bzw. nach E-Mail-Adressen welche im *"mailto:"*-Tag enthalten sind. Viele

Spammer durchsuchen Suchmaschinen nach neuen Web-Seiten und spammen die Besitzer der in diesen Seiten enthaltenen E-Mailadressen.
Eine weit verbreitete Maßnahme um dieser Technik der Adressensammlung entgegenzuwirken ist das sogenannte "*poison*"-CGI-Skript. Dieses Skript erstellt eine Web-Seite mit falschen E-Mailadressen und einen Link zu der generierten Seite. Durchsucht nun ein Spammer mittels Software eine Web-Site mit diesem Skript, sammelt der Spammer nur falsche E-Mail-Adressen und folgt immer dem Link auf die Seite mit den falschen Adressen. Da bei jedem Seitenaufruf eine neue Seite generiert wird, gerät der Spammer in eine Art Endlosschleife.

3.4.4 Internet-Gästebücher und Online-Listen

Über Gästebücher, dessen Einträge auf der entsprechenden Web-Seite veröffentlicht werden, können Spammer sehr leicht an die E-Mailadressen eingetragener Personen kommen, da diese in der Regel bei einem Gästebucheintrag angegeben werden. Hier hat der Spammer jedoch den Nachteil, dass oftmals veraltete Adressen enthalten sind oder dass beim Eintrag in das Gästebuch ungültige oder keine Adressen angegeben werden.
Weiters haben viele Provider auf ihrer Homepage eine Liste ihrer Teilnehmer bzw. jener Personen, welche bei diesem Provider eine Homepage haben. In der Regel wird hier auch die E-Mail-Adresse des Kunden angeführt und somit öffentlich zugänglich gemacht, da dieses Service für viele Internet-Teilnehmer sehr nützlich ist.

3.4.5 Ident-Dämon

Auf vielen Unix-Systemen läuft ein Ident-Dämon, welcher anderen Computern erlaubt Leute zu identifizieren, welche mit dem Unix-System gerade verbunden sind.
Surft nun jemand auf einem solchen Computer und verbindet sich zu bestimmten Web-Sites oder News-Servern, kann diese Seite oder der News-Server seinerseits wieder eine Verbindung zurück zum Computer des Surfers herstellen und mittels Dämon die E-Mailadresse ermitteln.
Manche Chat-Clients auf PCs weisen ein ähnliches Verhalten auf, so dass die Teilnahme an IRCs die E-Mailadresse des Teilnehmers preisgeben kann.

3.4.6 Webbrowser

Manche Web-Seiten verwenden raffinierte Techniken um die E-Mailadresse eines Surfers, welcher sich gerade auf dieser Seite befindet, zu ermitteln, wobei der Surfer dies oftmals gar nicht bemerkt.

Diese Techniken sind:

- Manche Web-Seiten versuchen, dass der Browser eine Graphik der besuchten Seite mittels einer Anonymous-FTP-Verbindung herunterlädt. Manche Browser leiten dadurch die E-Mailadresse des Surfers, wenn sie bei den Grundkonfigurationen des Browsers als Passwort für Anonymous-FTP-Verbindungen angegeben wurde, an den FTP-Server weiter, ohne dass der Surfer etwas davon bemerkt. Im *"Netscape Communicator 4.5"* zum Beispiel ist diese Einstellung unter *Bearbeiten/Erweitert/Einstellungen* zu finden.

- Durch verwenden eines geeigneten Java-Scripts in der Web-Seite kann bewirkt werden, dass die im Browser konfigurierte E-Mailadresse an eine im Java-Script angegebene E-Mail-Adresse weitergeleitet wird.

- Manche Browser verschicken einen Header (HTTP_FROM-Header) mit der E-Mail-Adresse des Users an den Server einer jeden besuchten Web-Seite. Die in diesem Header enthaltene Adresse können sich Spammer wiederum zunutze machen.[4]

3.4.7 IRC und Chat-Rooms

Manche IRC-Clients geben E-Mail-Adressen auf Anfrage weiter. Diesen Umstand machen sich Spammer zunutze und sammeln in diesen IRCs Adressen mit der Gewissheit, dass diese gültig sind, da die User im IRC aktiv eingeloggt sind.

[4] Um zu überprüfen, ob der in Verwendung befindliche Browser einen solchen HTTP_FROM-Header an den Server einer besuchten Web-Seite weiterleitet, kann man unter der Adresse http://www.helie.com/BrowserCheck einen Test durchführen.

Neben dieser Methode machen sich Spammer den Umstand zunutze, dass IRCbots interaktiv Nachrichten an IRCs und Chat-Rooms versenden, in denen E-Mailadressen enthalten sind, ohne darauf Rücksicht zu nehmen, wer am Chat teilnimmt. Vor allem Internetneulinge, bei denen eine der ersten Aktivitäten das Chatten ist und welche noch keine Erfahrung mit Spammern haben und daher in IRCs und Chat-Rooms ihre E-Mail-Adresse preisgeben, sind dadurch potentielle Opfer von Spammern. Der Vorteil den Spammer hier haben ist, dass die meisten der Adressen noch relativ jung sind und eine entsprechend lange Gültigkeit haben werden.

3.4.8 Finger-Dämons

Bei manchen Finger-Dämons ist es möglich, Abfragen der Form <*name*>@<*host*> abzusetzen. Als Ergebnis dieser Abfrage wird übermittelt, ob der User mit dem Namen <*name*> auf dem Host <*host*> eingeloggt ist.
Eine Abfrage mit der Form @<*host*> liefert eine Liste aller eingeloggten User auf dem Host <*host*>.
Spammer machen sich diese Möglichkeit zunutze um auf diese Art extensive Listen von Usern bestimmter Hosts zu erstellen und an diese Spam-Mails zu versenden.
Da hier Adressen von eben eingeloggten Personen gesammelt werden, wissen Spammer, dass es sich hier um gültige Adressen handelt.
Diese Option ist auf den meisten Hosts jedoch deaktiviert, da sie in der Regel nicht benötigt wird.

3.4.9 AOL-Profile

Spammer sammeln häufig E-Mailadressen von AOL-Mitgliedern über Listen von User-Profilen, falls sie darauf zugreifen können. Da AOL ein von Internetneulingen häufig gewählter ISP ist, sind diese beliebte Opfer von Spammern, da sie im Umgang mit Spam-Mails keine Erfahrung haben.

3.4.10 Domain-Contact-Points

Jede Domain hat einen bis drei Contact-Points. Diese Contact-Points sind in der Regel die Administration, der technische Support und die Verrechnung. Diese Contact-Points beinhalten die E-Mailadresse der entsprechenden Kontaktperson.
Da die meisten dieser Contact-Points frei zugänglich sind, z.B. mit dem "*whois*"-Kommando, sammeln Spammer die E-Mailadressen dieser Kontaktpersonen für ganze Listen von Domains (diese Domainlisten sind normalerweise bei Domainregistrierungsstellen frei erhältlich). Bei diesen Adressen haben Spammer den Vorteil, dass es sich hier normalerweise um gültige E-Mailadressen handelt und dass die an diese Contact-Points verschickten E-Mails auch gelesen werden. Weiters ist auch die Zielgruppe genau bekannt und kann gezielt beworben werden.

3.4.11 Guessing and Cleaning

Guessing basiert auf der Annahme von Spammern, dass die E-Mailadressen bei den ISPs nach dem System `vorname.nachname@domain` aufgebaut sind.
Manche Spammer senden an E-Mailadressen, von welchen sie vermuten dass sie existieren, Test-Mails oder sofort Spam-Mails. Anschließend warten sie auf eine Rückmeldung, dass die E-Mailadresse ungültig ist oder um eine Bestätigung, dass die Nachricht erfolgreich übermittelt wurde.
Ein Beispiel dafür wäre die Johannes-Kepler-Universität Linz, an der die E-Mail-Adressen der Studenten nach diesem Prinzip aufgebaut sind (vorname.nachname@jk.uni-linz.ac.at). So wäre es für einen Spammer möglich, Anmeldelisten zu diversen Lehrveranstaltungen zu kopieren und zu versuchen die darin eingetragenen Studenten zu spammen.

Oft werden bestimmte Mail-Header verwendet, um zu erreichen, dass der Mail-Client eine Empfangs- oder Lesebestätigung retour sendet.
Diese Mail-Header sind generell:

`Return-Receipt-To: <E-Mailadresse>`	Sendet eine Empfangsbestätigung
`X-Confirm-Reading-To: <E-Mailadresse>`	Sendet eine Lesebestätigung

Die genauen Einstellungen sind jedoch immer vom verwendeten Mail-Tool abhängig.

3.4.12 Gelbe Seiten

Da in den "Gelben Seiten" der Telephonbücher nun auch die E-Mailadressen eingetragen werden, können Spammer auch auf diesem Weg zu E-Mail-Adressen gelangen. Durch Verwendung der "Gelben Seiten" im Internet (z.B. http://www.gelbeseiten.at) oder auf CD-ROM haben Spammer diese Adressen bereits in elektronischer Form vorliegen und können diese direkt übernehmen.

3.4.13 Mittels Zugang zum selben Computer

Haben Spammer Zugang zu einem Computer, haben sie auch die Möglichkeit eine Liste von gültigen Usernamen zu erhalten. Auf UNIX-Systemen können diese Usernamen mittels dem Kommando *`/etc/passwd`* abgerufen werden. Eine Liste der gerade eingeloggten User kann mittels dem Kommando *`who`* abgerufen werden.

3.4.14 Adressenkauf

Es gibt auch im E-Mail-Bereich Unternehmen welche den Handel und Verkauf mit E-Mail-Adressen anbieten. Gegen einen bestimmten Geldbetrag kann man eine bestimmte Anzahl von E-Mail-Adressen käuflich erwerben. Viele Adressenhändler bieten eine Einteilung der Adressen nach bestimmten Zielgruppen an. Diese Kriterien können sich unterscheiden nach Kaufkraft, Interessen, Aktivitäten oder ähnlichem, so dass ein Spammer gezielt eine Gruppe von Personen bewerben kann.

3.5 Identifizierung von Spam-Mails

Der zur Identifizierung von Spam-Mails wichtigste Anhaltspunkt ist der Header der eingelangten E-Mail. Als Beispiel werden im folgenden zwei Netscape-Mail-Header angeführt, wobei der erste von einem normalen E-Mail stammt und der zweite von einem Spam-Mail.

```
Received: from mail.fim.uni-linz.ac.at (mail.fim.uni-
linz.ac.at [140.78.100.3])
```

```
        by alijku04.edvz.uni-linz.ac.at (8.8.8/8.8.8) with
ESMTP id LAA111700
        for <b.s@jk.uni-linz.ac.at>; Thu, 29 Jun 2000 11:02:20
+0200
Received: from s.fim.uni-linz.ac.at (m.fim.uni-linz.ac.at
[140.78.100.25]) by mail.fim.uni-linz.ac.at with SMTP
(Microsoft Exchange Internet Mail Service Version 5.5.2650.21)
        id NVYG5YGP; Thu, 29 Jun 2000 11:03:16 +0200
Message-Id: <4.3.2.7.2.20000629110050.00b0f868@mail.fim.uni-
linz.ac.at>
X-Sender: s@mail.fim.uni-linz.ac.at
X-Mailer: QUALCOMM Windows Eudora Version 4.3.2
Date: Thu, 29 Jun 2000 11:02:22 +0200
To: b.s@jk.uni-linz.ac.at
From: M. S. <s@fim.uni-linz.ac.at>
Subject: Re: Diplomarbeit
In-Reply-To: <395B0D30.52ED38EE@jk.uni-linz.ac.at>
References: <4.3.2.7.2.20000629082433.00b0f868@mail.fim.uni-
linz.ac.at>
Mime-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"; format=flowed
Content-Transfer-Encoding: 8bit
X-MIME-Autoconverted: from quoted-printable to 8bit by
alijku04.edvz.uni-linz.ac.at id LAA111700
X-Mozilla-Status: 8011
X-Mozilla-Status2: 00000000
X-UIDL: g;_"!X+m"!pQn!!#(E!!


Received: from unknown (ip150.atlanta14.ga.pub-ip.psi.net
[38.30.162.150])
        by alijku04.edvz.uni-linz.ac.at (8.8.8/8.8.8) with
SMTP id DAA80540;
        Mon, 24 Apr 2000 03:17:59 +0200
From: benchmark@conok.com
Subject: laser printer toner advertisement
Date: Mon, 24 Apr 2000 05:42:09
Message-Id: <841.130454.715899@>
Status: U
X-Mozilla-Status: 8001
X-Mozilla-Status2: 00000000
X-UIDL: 2bf1b39475880f56981608a5aab2f99b
```

3.5.1 Programmgestützte Identifikation

Da Spamming in den letzten Jahren zu einem immer größeren Problem geworden ist, hat sich auch die Software-Industrie dieses Themas angenommen und so stehen mittlerweile bereits

eine Vielzahl an Softwareprodukten zur Identifikation und Bekämpfung von Spam-Mail zur Verfügung. Es handelt sich bei diesen Produkten in der Regel um sogenannte Filterprogramme, die nach bestimmten, frei definierbaren Regeln (z.B. Schlüsselwörter im Betreff oder bestimmte Absenderadressen), Spam-Mails identifizieren und einer entsprechenden Weiterverarbeitung zuführen (Löschen, Verschieben in einen bestimmten Mailordner).
Diese Spam-Filter können einerseits clientseitig ablaufen, was den Nachteil hat, dass zuerst die E-Mails bzw. zumindest die Mail-Header auf den lokalen Rechner geladen werden müssen, oder andererseits bereits auf dem Server des entsprechenden Providers eingehende oder auch ausgehende E-Mails als Spam identifizieren.
Ein weitere Art von serverseitigen Filtern wären etwa Spam-Filter für Newsgroups zur Identifikation unerwünschter Postings. Ein solches Programm wäre z.B. „NoCeM-on-Spool“.

3.5.1.1 Text in der Subject-Zeile

Um Spam-Mails über den Inhalt der „Subject:“-Zeile zu identifizieren, werden in den Filterprogrammen mögliche Inhalte der „Subject:“-Zeile definiert, die Spammer beim Versenden von Spam-Mails verwenden könnten.
Da es sich bei dieser Zeile jedoch um eine Textzeile handelt, können die Inhalte von Fall zu Fall sehr stark variieren und es ist besser, wenn man sich auf Stichworte beschränkt.
Um diese Methode als wirkungsvollen Filteransatz zu verwenden, muss man die im Filterprogramm definierten Einträge regelmäßig pflegen, was mitunter sehr aufwendig werden kann.
Mögliche Schlagworte, welche in der „Subject:“-Zeile vorkommen könnten, wären z.B. „Gewinnspiel“, „Urlaub“, „Angebot“, „Sensation“, „sensationell“, „einmalig“, „Gelegenheit“ oder ähnliches.

3.5.1.2 Absenderadresse

Die Identifikation von Spam-Mails über die Absenderadresse wird verwendet, um bekannte Spammer zu identifizieren und die von ihnen versendeten E-Mails mittels Filterprogrammen aus den eingehenden E-Mails auszufiltern. Um diese Methode sinnvoll einsetzen zu können,

wird in den verwendeten Filterprogrammen eine Liste mit den E-Mail-Adressen jener Personen verwaltet, von denen man keine E-Mails erhalten möchte.
Da viele Spammer häufig ihre E-Mail-Adresse wechseln bzw. in den von ihnen verfassten Spam-Mails keine Absenderadresse angeben, bzw. diese nur im Mailtext angeben um von Filterprogrammen nicht entdeckt zu werden, ist diese Methode nur sehr eingeschränkt erfolgreich.
Weiters kann die Identifikation von Spammern über die E-Mail-Adresse als kooperativer Filteransatz (Zusammenarbeit zwischen Spammern und Empfängern bzw. ISPs - siehe Kapitel 3.8.3.2) verwendet werden.

3.5.1.3 Domainname und IP-Adresse überprüfen

Das Überprüfen des Provider-Domain-Namen bzw. der Provider-IP-Adresse des Verfassers einer E-Mail durch serverseitige Programme am Mailserver ist nicht direkt eine Maßnahme gegen Spamming sondern vielmehr eine Maßnahme gegen E-Mail-Relaying.
Da Spammer jedoch sehr oft ihre Spam-Mails mittels E-Mail-Relaying verbreiten, ist dieser Vergleich indirekt auch ein Schutz gegen den Missbrauch des Mailservers durch Spammer. Die potentiellen Empfänger von Spam-Mails werden durch diese Maßnahme jedoch nicht vor dem Empfang dieser unerwünschten E-Mails verschont, da ein Spammer vermutlich mehrere Relay-Versuche unternehmen wird, bis ein Mail-Server die Versendung der Spam-Mails akzeptiert bzw. ein Spammer im – für ihn – schlimmsten Fall über den Mailserver seines eigenen Providers versendet und ein Sperren seines Internetzuganges riskiert.

3.5.1.4 Adressierung der E-Mail

Ist eine E-Mail nicht persönlich an den Empfänger adressiert (bzw. ist der Empfänger nicht in der „CC:“-Zeile (Carbon-Copy) oder der „BCC:“-Zeile (Blind Carbon Copy) angeführt) sondern wird z.B. direkt der Mailserver des Providers adressiert, handelt es sich mit hoher Wahrscheinlichkeit um den Versand von Spam-Mails. Dies ist ein sehr guter Ansatzpunkt für Anti-Spam-Programme zur Identifikation, da es sich hier um einen sehr stichhaltigen Hinweis für den Versand von Spam-Mail handelt, da der Empfänger nicht direkt angeschrieben wird.

Verwendet man diesen Ansatzpunkt zur Identifikation von Spam-Mail ist jedoch Vorsicht geboten, dass nicht auch erwünschte E-Mails aus einer Mailing-Liste vom Filterprogramm gelöscht werden, da hier ebenfalls nicht der Name des Empfängers aufscheint.
Als Beispiel sind im folgenden die Header-Daten einer E-Mail aus einer Mailing-Liste angeführt. Diese Header-Daten enthalten meist die Schlüsselwörter „Subscriber“ bzw. „Listserv“, da hier in der Regel die Teilnehmer in einer Subscriberliste auf einem Listserver verwaltet werden. Man sollte daher die Filterregeln dementsprechend aufbauen, dass E-Mails, welche diese oder ähnliche Wörter enthalten, nicht gelöscht werden.

```
Received: from VM230.AKH-WIEN.AC.AT (VM230.AKH-Wien.ac.at
[149.148.150.3])
     by alijku04.edvz.uni-linz.ac.at (8.8.8/8.8.8) with SMTP id
XAA136856;
     Fri, 19 Jan 2001 23:08:25 +0100
Received:  by VM230.AKH-WIEN.AC.AT (IBM VM SMTP Level 310) via
spool with SMTP id 8939 ; Fri, 19 Jan 2001 22:39:43 MEZ
Received: from AKH-WIEN.AC.AT (NJE origin LISTSERV@AWIIMC12)
by AKH-WIEN.AC.AT (LMail V1.2d/1.8d) with BSMTP id 5008; Fri,
19 Jan 2001 22:39:35 +0100
Received: from LISTSERV.EARTHWEB.COM by LISTSERV.EARTHWEB.COM
(LISTSERV-TCP/IP
          release 1.8d) with spool id 1623708 for
          SUBSCRIBERS-JAVASCRIPTS-COM@LISTSERV.EARTHWEB.COM;
Fri, 19 Jan 2001
          15:53:12 -0500
Approved-By: bradleyj@EARTHWEB.COM
Received: from sblexch001.earthweb.com
(connies.microhouse.com) by
          listserv.earthweb.com (LSMTP for Windows NT v1.1b)
with SMTP id
          <4.00041D4E@listserv.earthweb.com>; Fri, 19 Jan 2001
15:40:02 -0500
Received: by connies.microhouse.com with Internet Mail Service
(5.5.2650.21) id
          <C5V1JFHL>; Fri, 19 Jan 2001 13:54:50 -0700
MIME-Version: 1.0
X-Mailer: Internet Mail Service (5.5.2650.21)
Content-Type: text/plain; charset="iso-8859-1"
Message-ID:
<FBAB9F4BF38BD41188910004ACE39061586E1E@connies.microhouse.com
>
Date:         Fri, 19 Jan 2001 13:54:46 -0700
Sender: "Javascripts.com Info"              <SUBSCRIBERS-
JAVASCRIPTS-COM@LISTSERV.EARTHWEB.COM>
From: JS News <JSNews3@EARTHWEB.COM>
```

```
Subject:      JavaScripts Update (1-19-2001)
To: SUBSCRIBERS-JAVASCRIPTS-COM@LISTSERV.EARTHWEB.COM
X-UIDL: #NL"!pHB"!3]U"!_d5"!
```

3.5.2 Kriterienkatalog zur programmgestützten Identifikation

Im folgenden Abschnitt erfolgt eine Gegenüberstellung von für Spam-Mail und für normale Mailsendungen typischen Merkmalen. Anhand der Bedeutung eines jeden Merkmales wird eine gewisse Punkteanzahl addiert (bei Merkmalen für Spam) bzw. eine gewisse Punkteanzahl wieder abgezogen (bei Merkmalen für normales Mail). Wird ein gewisser Punktewert überschritten, so kann man mit hoher Wahrscheinlichkeit davon ausgehen, dass es sich bei dem untersuchten E-Mail um Spam handelt.
Dieser Kriterienkatalog ist lediglich als Richtlinie zur programmgestützten Identifikation von Spam gedacht und soll als Hilfestellung zur Identifikation dienen.
Die im folgenden genannten Kriterien können vom Anwender aufgrund seiner persönlichen Erfahrungen mit Spam natürlich entsprechend erweitert, abgeändert oder anders bewertet werden.

- **Absenderadresse:**

  Hotmail-, GMX- oder andere Freemail-Adressen:
  Diese Adressen sind sehr leicht zu wechseln und werden deshalb von Spammern gerne verwendet. Außerdem ist es bei diesen Adressen auch möglich, sich unter Phantasienamen anzumelden, da keine Verifikation der User erfolgt. Viele Spam-Mails haben als Absenderadresse eine Freemailadresse.

  Punkte: + 1

- **Adressierung**:

  Keine persönliche Adressierung

  Ist eine E-Mail im Header nicht persönlich oder gar nicht adressiert, handelt es sich auf jeden Fall um ein Massenmail. Es ist hier jedoch noch zu unterscheiden, ob das E-Mail von einem Mailverteiler kommt, an dem man freiwillig Mitglied ist.

  Punkte: + 5

  Persönlich adressiert

  Ist eine E-Mail persönlich adressiert, handelt es sich nur in solchen Fällen um Spam-Mail, wenn ein Spammer Zugang zur adressierten E-Mailadresse hat und diese für seine Zwecke nützt.

  Sind im Adreßfeld weitere Empfänger angeführt:

  Punkte: je weiterem Empfänger + 0,3

  Erfolgt die Adressierung nur an die Empfängeradresse und an keine weiteren E-Mailadressen, handelt es sich aller Wahrscheinlichkeit nach um kein Spam.

  Punkte: - 5

- **CC**

  Pro CC + 0,5 Punkte

- **Vorname oder Familienname in Anrede**

  Enthält die E-Mail eine persönliche Anrede, ist davon auszugehen, dass es sich um eine normale E-Mail handelt, da Spammer fast nie den Namen der Person wissen, die hinter der E-Mail-Adresse steht und es andererseits ein zu großer Aufwand wäre, für alle Empfänger der E-Mail eine persönliche Anrede zu generieren.

  Punkte: - 5

- **Subject:**
  Enthält die E-Mail kein Subject, handelt es sich meist um normales E-Mail, da Spammer dazu neigen, in der Subject-Zeile ihre Botschaft anzukündigen

  Punkte: - 1

  Enthält die E-Mail einen groß geschriebenen Subject-Text, ist Vorsicht geboten, da diese plakative Schreibweise des Subjects für Spammer typisch ist.

  Punkte: + 0,5

- **Wörter im Mailtext oder in der Subject-Zeile**
  Ebenfalls ein guter Ansatz zum Erstellen von Filterregeln ist das Vorkommen bestimmter Wörter in der Subjectzeile bzw. im Mailtext, welche für Spam charakteristisch sind.

  Solche Wörter können z.B. folgende sein:
  - Gewinn
  - Urlaub
  - Glücklich
  - Reich
  - Sensationell
  - Gelegenheit

  oder ähnliche. Diese Liste kann individuell ergänzt und abgeändert werden.

  Punkte pro enthaltenem Wort: + 2

Kriterium	**Punkte**
Absenderadresse als Hotmail, GMX oder andere Freemail-Adresse	+ 1
Keine persönliche Adressierung	+ 5
Persönlich adressiert und im Adressfeld weitere Empfänger angeführt:	+ 0,3 je weiterer Adresse

nur persönlich adressiert	- 5
CC	pro CC + 0,5
Vorname oder Familienname in Anrede	- 5
kein Subject	- 1
plakatives Subject	+ 0,5
Wörter im Mailtext oder in der Subject-Zeile	

Abbildung 7: Punktekatalog zur E-Mail-Bewertung bezüglich Spam

Nach folgender Tabelle lassen sich E-Mails bezüglich ihrer Spam-Wahrscheinlichkeit kategorisieren:

Punkte	**Spamwahrscheinlichkeit**
< 1,5	sicher kein Spam
1,5 – 3	wahrscheinlich Spam
> 3	höchst wahrscheinlich Spam

Abbildung 8: Punktebewertung einer E-Mail bezüglich ihrer Spam-Wahrscheinlichkeit

3.5.3 Subjektive Identifikation durch den User

Eine subjektive Identifikation von Spam-Mails erfolgt clientseitig direkt durch den User. Durch Betrachtung des Inhalts der E-Mail ist für den User erkennbar, ob es sich um ein normales E-Mail oder ein Spam-Mail handelt (typische Inhalte für solche Spam-Mails sind im Kapitel 3.6.2 ersichtlich).
Von dieser Methode ist jedoch eher abzuraten, da einerseits Zeit und Ressourcen durch den Download sowie die Betrachtung des Inhalts der Spam-Mails vergeudet werden und andererseits der Spammer sein Ziel – nämlich dass der gespammte User die E-Mail liest – erreicht. Um einen wirksamen Schutz vor Spam-Mails zu erreichen, sollten eher Filterprogramme verwendet werden.

3.6 Klassifizierung von Spam-Mails

In diesem Kapitel soll ein Überblick über die Arten von Spam-Mails und die am häufigsten verschickten Spam-Mails gegeben werden.

3.6.1 Die zwei Hauptarten von Spam

Grundsätzlich lassen sich zwei Hauptarten von Spam unterscheiden. Diese beiden Hauptarten sind Usenet-Spam und E-Mail-Spam.

3.6.1.1 Usenet Spam

Unter Usenet-Spam versteht man das Überschwemmen einer Newsgruppe mit einem Artikel. Die Zielgruppe dieser Art des Spam sind zwar Personen die Newsgruppen lesen, selbst aber keine Artikel verfassen. Dadurch bleibt ihre E-Mail-Adresse unbekannt und sie können nicht direkt mittels E-Mail-Spam angesprochen werden. Durch diese Art von Spam wird versucht, diese Zielgruppe ebenfalls zu erreichen.

Usenet-Spam lässt sich in ECP und EMP unterscheiden.

3.6.1.1.1 ECP (Excessive Cross Posting)

Hier wird ein Artikel in verschiedenen Newsgroups gepostet. Es werden hier in der „Newsgroup:“-Headerzeile mehrere Newsgoups angegeben. Ein Artikel mit folgender „Newsgroup:“-Headerzeile

„Newsgroups:
rec.games.mud.admin,rec.games.mud.tiny,rec.games.mud.misc“

wird an drei Newsgoups cross-posted.
Der Artikel wird allerdings nur einmal versandt und ist daher auf dem News-Server physikalisch nur einmal vorhanden.
Versendet man eine Newsgroup-Artikel lediglich an einige Newsgroups, ist dagegen nichts einzuwenden. Wird der Artikel jedoch an z.B. hunderte Newsgroups versandt ist dies ein Missbrauch des Usenets.

ECP wird manchmal auch als „velveeta“ bezeichnet.

3.6.1.1.2 EMP (Excessive Multiple Posting)

Hier werden identische Exemplare von Newsgroup-Artikeln in vielen Newsgroups gepostet. Der Unterschied zu ECP besteht darin, dass der Artikel nicht nur einmal, sondern gleich mehrfach physikalisch auf dem News-Server vorhanden ist. Das liegt daran, dass beim ECP alle Newsgroups, in die gepostet werden soll, in der Newsgroups-Zeile angegeben werden und der Artikel somit nur einmal in eine lange Newsgroup-Liste gepostet wird. Beim EMP hingegen wird in jede Newsgroup einzeln gepostet. EMP beansprucht die Netzbandbreite somit wesentlich mehr als ECP.

3.6.1.1.3 Weitere Arten von Usenet-Spam

Neben den beiden bereits erwähnten Arten von Usenet-Spam lassen sich noch folgende Kategorien unterscheiden:

Spew
Ein Spew tritt auf, wenn ein schlecht bzw. falsch konfiguriertes News-Programm ein und den selben Artikel in der selben Newsgroup immer wieder veröffentlicht.

Off-topic-postings
Unter Off-topic-postings versteht man Newsgroup-Artikel, mit einem unpassenden Inhalt für die Newsgroup, in welcher sie veröffentlicht werden.

Binaries
Binaries sind Newsgroup-Artikel mit verschlüsselten Binärfiles wir z.B. Image-Files, Programme, Musik- oder Videofiles. Binaries sind für Newsgroups, welche nicht ausdrücklich Binärfiles zulassen, ungeeignet.

Commercial-Postings
Hier handelt es sich um Newsgroup-Artikel, welche ein Produkt oder eine Dienstleistung zum Verkauf anbieten. Solche Angebote sind in manchen Newsgroups willkommen, in manchen werden sie toleriert und in anderen wiederum sind sie unerwünscht bzw. verboten.

3.6.1.2 E-Mail Spam

Unter E-Mail-Spam wird das versenden einer ungebetenen E-Mail-Nachricht an eine große Zahl von Adressaten verstanden (in der Regel 25 oder mehr Adressaten binnen 24 Stunden). Die Zielgruppe sind individuelle Personen. Genau genommen handelt es sich bei dieser Art des E-Mail Missbrauchs nicht um Spam im eigentlichen Sinne. Ursprünglich wurde unter Spam nur die Usenet-Variante verstanden. Da Begriffsinhalte aber niemals statisch gesehen werden können (besonders in einem dynamischen Medium wie dem Internet), wird heute der Begriff „Spam“ auf verschiedene Arten des E-Mail-Missbrauchs angewandt. [AOL]

3.6.1.2.1 UBE (Unsolicited Bulk E-Mail)

Darunter sind E-Mail-Sendungen mit Großteils identem Inhalt zu verstehen, die unaufgefordert an viele Adressen versandt werden. Fast immer ist UBE von kommerzieller Art und daher auch als ein UCE (siehe Kapitel 3.6.1.2.2) zu betrachten. Andere Zwecke von UBE wären z.B. politisches Lobbying bzw. Wahlwerbung. UBE stellt die heute problematischste Form des E-Mail-Missbrauchs dar. Mit entsprechenden E-Mail-Programmen lassen sich Millionen von Nachrichten innerhalb kürzester Zeit senden. Dadurch wird die Netzbandbreite, die Speicherkapazität und die Zeit der Empfänger enorm beansprucht.

3.6.1.2.2 UCE (Unsolicited Commercial E-Mail)

Ein UCE ist ein E-Mail, das kommerzielle Informationen enthält und dem Empfänger unaufgefordert zugeschickt wird. Die Anzahl der versandten E-Mails ist dabei nicht von Bedeutung um eine E-Mail-Sendung mit entsprechendem Inhalt als UCE klassifizieren zu können.
Diese Art von Spam-Mails wird auch als Junk-Mail bezeichnet.

3.6.1.2.3 MMF (Make Money Fast) und MLM (Multi Level Marketing)

Unter diesem Begriff sind E-Mail-Sendungen zu verstehen, die hohe Gewinne versprechen, nachdem man eine „Anfangsinvestition“ übermittelt und andere Personen rekrutiert hat. Ein typisches Beispiel wären Pyramidenspiele. Es wird dabei eine Liste mit Namen übermittelt wobei man an den Namen der auf der Liste ganz oben steht einen gewissen Geldbetrag

überweist, diesen Namen streicht und den eigenen unten an der Liste dazu fügt. Anschließend muss man die Listen an eine bestimmte Anzahl von Personen weiterschicken.
Bei MLM versuchen die Betreiber zum Unterschied zu MMF (1.1.2.3) durch Einsatz von hochtrabenden Begriffen, wie eben z.B. „Multi-Level-Marketing“ oder ähnlichen, über mangelnde Seriosität (und meist auch mangelnde Legalität wie z.B. in Österreich) ihrer Angebote hinweg zu täuschen. [SCHWARTZ 98]
Ein Beispiel dafür wären Kettenbriefe.

3.6.1.2.4 Reputation Attack

Reputation Attacks sind Mails, bei denen angegeben wird, dass sie von einer bestimmten Person bzw. von einer bestimmten Organisation stammen, tatsächlich aber von jemand anderem gesandt wurden. Der Zweck eines solchen Mails ist nicht ein bestimmtes Produkt oder eine bestimmte Dienstleistung zu verkaufen, sondern vielmehr die Empfänger auf den vermeintlichen Absender verärgert zu machen. [SCHWARTZ 98]

3.6.2 Die häufigsten Spam-Mails

In diesem Kapitel werden die zwölf am häufigsten auftretenden Spam-Mails beschrieben. Im Spam-Jargon werden sie auch als „das dreckige Dutzend“ bezeichnet.

3.6.2.1 Möglichkeiten sich Selbständig zu machen

In dieser Art von Mails wird die Möglichkeit offeriert, sich auf einfache Art und Weise bei sehr hohen Verdiensten selbständig zu machen. Außerdem wird versprochen, dass der Arbeitsaufwand und die zu erwartenden Ausgaben für das zukünftige Unternehmen gering sind und dass es sich nicht um Verkaufstätigkeit oder Tätigkeit mit anderen Personen handelt. Viele dieser Möglichkeiten zur Selbständigkeit enthalten internetbezogene Tätigkeiten. Im Mail wird jedoch nicht sehr auf Details eingegangen, dafür werden aber umso mehr Versprechungen gemacht.
Oft wird eine kostenpflichtige Telephonnummer (sogenannte Mehrwertnummer) angegeben, bei der man genauere Angaben erhält. Bei Anruf dieser Nummer wird man dann gebeten seinen Namen und seine Telephonnummer zu hinterlassen, um zurückgerufen zu werden.

Es handelt sich bei diesen Angeboten jedoch oft um illegale Pyramidenspiele, welche nur als Geschäftsmail getarnt sind.

3.6.2.2 Kommerzielle Versendung von Massenmails

In diesen Mails werden Listen mit E-Mail-Adressen zum Kauf offeriert, um eigene Massenmailsendungen verschicken zu können.
Oft wird auch eine Software zum Kauf angeboten (Spamprogramme), welche die Versendung von Massenmails zu Tausenden von Empfängern vollautomatisch übernimmt. In anderen Fällen wird angeboten, die Sendung von Massenmails im Namen des Auftraggebers zu übernehmen. In einigen dieser Angebote wird außerdem suggeriert, dass man bei Verwendung dieser Marketingmethode sehr viel Geld verdienen kann.
Das Problem bei diesen Angeboten ist, dass Massenmails oft die Kapazität der Internet-provider überschreiten und gegen deren Geschäftsbedingungen verstoßen. Bei Benutzung solcher Spamprogramme zum Versenden von Massenmails, kann es durchaus sein, dass man vom Provider gesperrt wird. Benutzt man die von Spamprogrammen angebotene Möglichkeit eine falsche Antwortadresse anzugeben, kann man sehr leicht in Konflikt mit dem Eigentümer der Domain in der falschen Adresse kommen.

3.6.2.3 Kettenbriefe

Bei dieser Art von Spam-Mail geht es darum, einen gewissen Geldbetrag (5 – 20 Dollar) an vier oder fünf Personen einer dem Mail beigelegten Liste weiterzuschicken, einen Namen auf der Liste durch den eigenen zu ersetzen und anschließend dieses Mail mittels Bulk-Mail weiterzusenden.
Es wird in dieser Art von Mails oft angeführt, dass es sich um eine legale Aktion handelt oder von einem Rechtsanwalt begutachtet wird. Tatsache aber ist, dass Kettenbriefe, egal ob traditionell auf Papier oder via E-Mail, in Österreich auf jeden Fall illegal sind. Fast alle der beteiligten Personen verlieren das investierte Geld, da nur diejenigen, die an der Spitze sitzen, etwas verdienen können, Personen, welche sich in der Hierarchie weiter unten befinden, in der Regel aber immer ihr investiertes Geld verlieren.

3.6.2.4 Heimarbeitsangebote

Ein häufiges Angebot ist das Verpacken von Schriftstücken in Kuverts. Es wird ein ständiges Einkommen mit minimalem Arbeitsaufwand garantiert. So werden zum Beispiel oft bis zu 2 $ für jedes in ein Kuvert verpacktes Schriftstück geboten.
Handwerks- oder Montagearbeiten, welche auch des öfteren angeboten werden, erfordern Investitionen in der Höhe von oft ein paar Hundert Dollar für Ausrüstung oder Zubehör – natürlich zu Kaufen beim Sender des Mails. Es soll dann anschließend für eine Firma produziert werden, welche auch eine Abnahmegarantie verspricht.
Für das Verpacken von Schriftstücken in Kuverts ist es üblich, dass ein gewisser Startbetrag an den Auftraggeber, den Sender des Spam-Mails, bezahlt werden müssen um mit dieser Tätigkeit beginnen zu können. Nach der Bezahlung dieser Gebühr erfährt man, dass der „Auftraggeber“ gar keine Arbeit anbietet, sondern lediglich Anweisungen, wie man selbst ein gleiches Spam-Mail an andere versendet. Sollte man auf diese Art und Weise jemals Geld verdienen, dann kommt es lediglich von anderen Teilnehmern, welche auf das weiterverbreitete Spam-Mail ebenso hereingefallen sind.
Bei Handwerks- oder Montagearbeiten verhält es sich so, dass, nachdem die benötigte Ausrüstung besorgt wurde, die produzierten Produkte vom Abnehmer wegen zu geringer Qualität abgelehnt werden.

3.6.2.5 Gesundheits- und Diätangebote

Pillen die zu Gewichtsverlust ohne Diät oder Umstellung der Ernährungsgewohnheiten führen, pflanzliche Wirkstoffe, welche das Fettgewebe verflüssigen, so dass es vom Körper absorbiert wird und Kuren gegen Impotenz und Haarausfall sind die Inhalte dieser Art von Spam-Mails.
Oft sind auch überaus positive Erfahrungsberichte von früheren Anwendern und Zertifikate von angeblich bekannten Ärzten oder Experten beigefügt. Von den genannten Ärzten und Experten hat aber noch niemand etwas gehört. Sie sind entweder erfunden oder gänzlich unbekannt.
Es wird meistens weiters angeführt, dass das erwähnte Produkt nur über einen bestimmten Zeitraum und nur bei einer bestimmten Verkaufsquelle erhältlich ist.

Auch werden Phrasen wie „wissenschaftlicher Durchbruch“, „Wunderkur“, „exklusives Produkt“, „Geheimformel“ oder „alte, wiederentdeckte Zutaten“ verwendet.

3.6.2.6 Zusatzeinkommen ohne große Anstrengungen

Der am häufigsten verwendete Tipp um schnell und mühelos reich zu werden ist, auf internationalen Märkten durch Geldwechselgeschäfte Geld zu verdienen. In dieser Art von Mails werden jedoch noch viele andere Möglichkeiten angeboten, um auf einfache Art und Weise rasch viel Geld zu verdienen. Es stellt sich jedoch die Frage: wenn es funktionieren täte, würden es dann nicht alle machen? Weiters stellt sich die Frage, ob die Versender es überhaupt noch nötig haben solche E-Mails zu versenden, wenn diese Methoden tatsächlich funktionieren würden.

3.6.2.7 Gratisprodukte

In vielen Werbe-E-Mails werden teure Produkte wie etwa Computer, Stereoanlagen oder andere ähnliche Produkte gratis angeboten. Man wird aufgefordert eine gewisse Grundgebühr zu bezahlen um einem Klub beizutreten. Nachdem man das getan hat, wird man aufgefordert eine bestimmte Anzahl an Personen zum Beitritt für diesem Klub zu werben, um die eingangs erwähnten Produkte tatsächlich zu erhalten.
Diese Vorgangsweise ist sehr ident mit Pyramidenspielen, nur dass hier keine Geldbeträge sondern diese in Form von bestimmten Produkten ausbezahlt werden.
Die meisten Erträge erhält der Initiator dieses Schreibens, nur einen kleinen Teil oder auch gar nichts erhalten die Teilnehmer. Das System wird, wie jedes andere Pyramidenspiel auch, früher oder später kollabieren.

3.6.2.8 Investitionsgelegenheiten

Per Mail übermittelte Investitionsangebote versprechen außergewöhnlich hohe Gewinne ohne Risiko. Bei einer Art dieser „profitablen“ Investitionen werden Investoren für eine Überseebank gesucht, bei anderen Angeboten ist die Form der Investitionen sehr verschwommen dargestellt und es wird hauptsächlich auf den zu erwartenden Gewinn hingewiesen. Viele dieser Angebote funktionieren nach dem sogenannten Ponzi-Schema, bei

denen Investoren, welche bereits früher eingezahlt haben, mit dem Geld von späteren Investoren ausbezahlt werden. Dadurch glauben die früheren Investoren dass das System tatsächlich funktioniert und werden dadurch angeregt noch mehr einzuzahlen.
Betreiber solcher betrügerischen Kapitalanlagen bieten diese nur kurze Zeit an, verbrauchen das Geld das sie eingenommen haben und ziehen sich aus dem Geschäft zurück, bevor sie entdeckt werden können. Oft betreiben sie später unter anderem Namen wieder ähnliche Kapitalanlageformen.
Im Mail wird garantiert, dass der Veranstalter sehr einflussreiche Beziehungen im Finanzsektor besitzt und er für das investierte Kapital garantiert bzw. es nach einer bestimmten Zeit wieder zurückzahlt.
Um mit potentiellen Kunden ein Geschäft abzuschließen werden Statistiken aus Telefonumfragen aufgetischt, der Sachverhalt von gegenwärtigen wirtschaftlichen Situationen verdreht (z.B. Pensionsvorsorge oder Währungsinstabilität) oder es wird die Einzigartigkeit des Angebots hervorgehoben.
Solche eingangs erwähnten Ponzi-Schematas brechen früher oder später zusammen, da durch Neuinvestoren nicht genug Geld eingenommen wird, um weitere Gewinne und Auszahlungen vortäuschen zu können. Diese Schematas sind nur gewinnbringend für denjenigen der sie initiiert, nicht aber für die Investoren.

3.6.2.9 Decoder für Satellitenprogramme

Hier wird angeboten, dass man für einen geringen Betrag ein Decoder-Kit zum Entschlüsseln von Satellitenprogrammen, ohne für diese eine Gebühr bezahlen zu müssen, kaufen kann.
Das Problem aber ist, dass das Set, welches hier zum Kauf angeboten wird, möglicherweise nicht funktionieren wird. Für die meisten verschlüsselten Satellitenprogramme werden Technologien verwendet, welche dieses Set nicht entschlüsseln kann. Sollte es dennoch funktionieren ist es aber Betrug an den Sendebetreibern.

3.6.2.10 Garantierte Darlehen und Kredite zu günstigen Konditionen

In einigen E-Mails werden Wohnbaudarlehen und Kreditkarten angeboten, ohne dafür eine Sicherheit zu verlangen und ohne dass auf die Kreditwürdigkeit des potentiellen „Kunden" näher eingegangen wird.
Diese Angebote werden in der Regel von ausländischen Banken offeriert. Öfters sind diese Angebote auch mit einem Pyramidenspiel kombiniert, welche Verdienstmöglichkeiten bei Anwerbung neuer Mitglieder versprechen.
Die versprochenen Kredite bzw. Kreditkarten werden jedoch nicht übermittelt und das Pyramidensystem bricht immer zusammen.

3.6.2.11 Steigern bzw. Herstellen der Kreditwürdigkeit und Kreditauskünfte

Bei diesen Mails wird angeboten, negative Kundeninformationen aus dem EDV-System einer Bank zu löschen, so dass man leichter zu Krediten, Kreditkarten oder Leasingangeboten kommt. Diese Angebote sind für Personen mit nicht ausreichender Kreditwürdigkeit gedacht. Diese Vorgehensweise ist illegal und man macht sich bei Annahme eines solchen Angebots strafbar.
Oft werden auch Kreditauskünfte und Bonitätsprüfungen von über dem Empfänger bekannten Personen angeboten, was aber auch oft nicht möglich ist und zu keinem Ergebnis führt.

3.6.2.12 Gewinn eines Urlaubs

Bei dieser Art von Spam-Mails wird dem Empfänger mittels eines elektronischen Zertifikats mitgeteilt, dass er einen hervorragenden Urlaub zu sehr günstigen Konditionen „gewonnen" hat. Oft wird noch angefügt, dass man persönlich für diese Möglichkeit ausgewählt wurde. Diese Mails gehen aber zu Tausenden, wenn nicht zu Millionen, von Empfängern zum gleichen Zeitpunkt.
Sollten diese Urlaube tatsächlich gebucht werden, entsprechen die gebotenen Leistungen häufig nicht dem angebotenen Standard und bessere Unterkünfte werden nur gegen

dementsprechende Mehrzahlungen zur Verfügung gestellt. Weiters erweist es sich oft als sehr schwierig, den Urlaub auch zum gewünschten Zeitpunkt antreten zu können.

3.6.3 Hoaxes

“Hoax”, was übersetzt etwa schlechter Scherz bedeutet, hat sich im Internet als Bezeichnung für die zahlreichen falschen Warnungen vor angeblich bösartigen Viren oder andere unwahre Meldungen eingebürgert. [ZDF 99]
Genau wie es Leute gibt, welche echte Viren entwickeln, gibt es auch solche, die via e-Mail Lügen und Gerüchte über Viren verbreiten, die gar nicht existieren. In solchen Warnungen stehen oft die abenteuerlichsten Sprüche. [SALVIE 99]
Es werden dem Empfänger regelrechte Schreckensszenarien vorgespielt: Beim Öffnen der E-Mails würden Festplatten gelöscht, Daten ausspioniert oder ähnliches. Insbesondere Internet-Neulinge geraten durch solche Meldungen in Panik, aber auch in Newsgroups sorgen sie regelmäßig für Aufregung.
Die meisten Hoaxes sind nach dem gleichen Schema aufgebaut: Sie erläutern die angebliche Bedrohung und fordern die Empfänger der Warnmeldungen auf, eine E-Mail, die als Betreff einen der genannten Begriffe enthält, vor dem Lesen zu löschen, da sonst der Virus aktiv wird. Wie Kettenbriefe verbreiten sich diese Hoaxes im Schneeball-System durch das Internet. Dabei ist der einzige Schaden, den sie anrichten, lediglich Verunsicherung beim Empfänger und nutzloser Datenverkehr im Netz. [ZDF 99]

Hoaxes enthalten praktisch immer folgenden Merkmale, an denen man sie ziemlich eindeutig erkennt:

1. Die Aufforderung, das Mail an möglichst viele Bekannten E-Mail-Adressen weiterzuleiten
2. Die Behauptung, die Information käme von namhaften Firmen, um die Glaubwürdigkeit zu verbessern.
3. Die (falsche) Information über einen furchtbar gefährlichen (aber in der Realität nicht existierenden) Computer-Virus
4. Das Subject (Betreff) enthält oft den Begriff "Virus Warnung" oder sinnverwandtes.

5. Die Wirkung des Virus wird sehr drastisch dargestellt und beinhaltet Dinge, die ein Computer-Virus gar nicht kann (z.B. Hardware beschädigen).

Keine der in solchen E-Mails genannten Firmen hat aber tatsächlich jemals Warnungen dieser Art publiziert. Es werden generell nie echte Virus-Warnungen auf diese Weise in Umlauf gebracht, da diese Art der Verbreitung nicht seriös ist. Solche Virenwarnungen sind immer Hoaxes.

Wer eine Virenwarnung in seiner Mailbox findet, sollte diese nicht beachten und sofort löschen, keinesfalls aber weiterleiten. Dadurch wird am wenigsten Arbeit und Web-Traffic verursacht. Es soll nämlich nicht die Aufgabe von Endbenutzern sein, solche Warnungen weiterzuleiten, denn dafür sind sie grundsätzlich nicht zuständig, da tatsächliche Virenwarnungen generell über seriöse Fachmedien erfolgen.
Sollte jemand beim Erhalt einer Virenwarnung unsicher sein, kann er sich auf der Webseite der „Datafellows“ umsehen. Auf dieser Seite stehen alphabetisch geordnet die bekannten Hoaxes und der Empfänger kann sich überzeugen ob es sich um einen Hoax handelt.[5]
Meist strotzen Hoaxes geradezu vor Ausrufezeichen und deren Urheber malen in schillerndsten Farben aus, was durch den angeblichen Virus alles passieren könne, begonnen beim simplen Disk-Crash bis fast zum Weltuntergang.
Anhand von drei klassischen Beispielen von Hoaxes soll dass Problem etwas veranschaulicht werden:

Budweiser Frog (Hoax Beispiel 1)

DANGER! VIRUS ALERT! THIS IS A NEW TWIST. SOME CREEPOID SCAM-ARTIST IS SENDING OUT A VERY DESIRABLE SCREEN-SAVER {{THE BUD FROGS}}. IF YOU DOWN-LOAD IT, YOU'LL LOSE EVERYTHING!!!! YOUR HARD DRIVE WILL <<>> CRASH!! DON'T DOWNLOAD THIS UNDER ANY CIRCUMSTANCES!!! IT JUST WENT INTO CIRCULATION ON 05/13/97, AS FAR AS I KNOW!! PLEASE DISTRIBUTE THIS WARNING TO AS MANY PEOPLE AS POSSIBLE...

Budweiser Frog (Hoax Beispiel 2)

Someone is sending out a very desirable screen-saver . The Budweiser Frogs.
If you download it, you will lose everything on your hard drive. It will crash, and someone from the internet will get your name and password!
DO NOT DOWNLOAD THIS UNDER ANY CIRCUMSTANCES !!!!!!!!!!
IT JUST WENT INTO CIRCULATION YESTERDAY.
This is a new, very malicious virus and not many people know about it yet. This information was announced yesterday morning from MICROSOFT.
Please share this information with everyone that might access the internet.
Once again, pass this along to EVERYONE in your address book so that this may be stopped. Also do not open or even look at any mail that says RETURNED or UNABLE TO DELIVER. This virus will attach itself to your computer components and render them useless. Immediately delete mail items that say this.
AOL (America on Line) has said that this is a very dangerous virus and that there is no known remedy for it at this time.
regards,
helpdesk.
Administrator-Harsha

Join the Crew (oder "Club") (Hoax Beispiel 3)

Hey, just to let you guys know one of my friends received an E-Mail called "Join the Crew," and it erased her entire hard drive. This is that new virus that is going around. Just be careful of what mail you read. Just trying to be helpful...

"Budweiser Frogs" existiert tatsächlich schon seit Jahren als sehr gut gemachter Screensaver, ist jedoch absolut ungefährlich.
Wie die Beispiele 1 und 2 zeigen, kann der selbe Hoax in verschiedenen Wortlauten auftreten. In Beispiel 2 erfolgt die typische Erwähnung gleich zweier namhafter Firmen (Microsoft und AOL). Wer beim Lesen solcher Mails über den Inhalt nachdenkt, wird von selbst merken,

[5] http://www.europe.datafellows.com/news/hoax.htm.

dass es die darin erwähnten, sehr gefährlichen, Viren nicht geben kann. Wie in Beispiel 1 erwähnt, sei der Virus bereits seit 1997 im Umlauf. Wenn dem so wäre, hätten sämtliche Hersteller von Antivirus-Programmen schon längst ein wirksames Abwehrinstrument dagegen entwickelt.

"Budweiser Frogs" ist kein Programm von Microsoft. Weshalb sollte deshalb ausgerechnet Microsoft über einen allfällig darin enthaltenen Virus informieren und so sein Ansehen gefährden? (Beispiel 2). Interessanterweise enthalten solche Hoaxes niemals Web-Links zu seriösen Informationen, was natürlich auch nicht möglich ist, da diese nicht existieren.

Beispiel 3 "Join the Club" oder auch "Join the Crew" warnt vor verseuchten E-Mails. Beim derzeitigen technischen Stand kann ein reiner Mail-Text niemals Viren enthalten. Es sind ausschließlich den Mails beigefügte Dateien (auch Beilagen oder Attachements genannt), welche mit einem Virus infiziert sein und eventuell auf dem System Schaden anrichten könnten.
Die E-Mail selbst besteht dagegen aus reinem ASCII-Text - welcher nicht mit einem Virus infiziert sein kann. Das reine Lesen einer Mail kann daher keine Schäden verursachen. Vorsicht ist jedoch bei solchen E-Mail-Clients angebracht, die Attachements einer E-Mail automatisch öffnen bzw. ausführen (z. B. Outlook). In diesen Binärdateien ist es nämlich wiederum möglich, einen Virus zu verstecken. Es sollte daher ein Attachement niemals ausgeführt oder geöffnet werden, wenn man über eine eventuelle Vireninfektion unsicher ist.

Verhalten bei Erhalt eines Hoax:

Es sind zwei Fälle zu unterscheiden:

1. Man erhält ein E-Mail mit einer Warnung vor einem Virus

Ein solches E-Mail soll man auf keinen Fall weiterleiten. Man sollte es löschen oder speichern, falls man Kuriositäten sammelt und danach dieses E-Mail vergessen und keine wertvolle Zeit verschwenden.

2. Man erhält ein E-Mail, vor dem man gewarnt wurde

Lautet das Subject "Returned or undeliverable mail" oder ähnlich, handelt es sich wahrscheinlich um eine normale E-Mail, die man lesen kann.
Enthält das Betreff dagegen einen der oben genannten Begriffe, erlaubt sich wahrscheinlich jemand einen schlechten Scherz, da die Mails, vor denen gewarnt wird, eigentlich nicht existieren. Auch hier gilt: Löschen und vergessen. [KRONACH]

Zu unterscheiden sind jedoch Warnungen von tatsächlichen existenten Viren, wie z.B. das „Love-Letter-Virus“. In solchen Fällen ist das Virus aber meistens äußerst populär und man hat in der Regel schon genug Informationen aus allgemeinen Informationsmedien (wie z.B. Tageszeitungen) erhalten. Außerdem fühlen sich bei solchen bekannten Viren viele Personen als wertvoller Informationsträger und man erhält die Virenwarnung wahrscheinlich sehr oft, was wiederum äußerst lästig ist.

Neben den erwähnten Virenwarnungen werden weiters sinnlose Kettenbriefe in Umlauf gebracht.
Kettenbriefe zählen ebenso zu den Hoaxes, denn auch hier existiert kein realer Hintergrund, der eine Weiterleitung an andere rechtfertigen könnte. Darüber hinaus fallen sie auch in die gleiche Kategorie wie Werbe-E-Mails: Sie sind unverlangte Massenmails.

Es gibt mehrere Varianten von Kettenbriefen:

- **Pyramiden-Systeme** (Schneeball-Systeme, 'Make Money Fast')
  Eine genauere Behandlung dieses Themas erfolgt unter Punkt 3.6.2.3

- **Gewinnspiele und Artverwandtes**
  Microsoft schenkt jedem $1000,- oder eine Windows98-CD, Nike verschenkt Sportartikel, Disney World zahlt jedem $5000,- oder eine All-Inclusive-Reise nach Disney World ist ein sehr häufig vorkommender Inhalt von dieser Art von Hoaxes.
  Es ist jedoch sehr leicht ersichtlich, dass dies keine realen Versprechungen sind. Es wird z.B. angegeben, Microsoft habe ein System entwickelt, dass man jede weitergeleitete Mail registrieren könne (das 'Microsoft E-Mail Tracking System'), welches man gerade testen

und als Belohnung dafür eine Windows98-CD erhalten würde. Das ist natürlich nicht richtig, ein solches System existiert nicht.

- **Glücksbriefe**
  Diese an sich harmlos erscheinenden Kettenbriefe stellen durch ihre Zahl und Häufigkeit eine Belastung der Netzressourcen und eine Belästigung der meisten Empfänger dar. Es wird wohl kein vernünftiger Mensch ernsthaft annehmen, dass diese Briefe (welche es seit Jahrhunderten auch in handschriftlicher Form gibt), irgendeine andere Wirkung als die eben genannte haben. Viele finden es einfach lustig oder meinen, sie würden jemandem damit zumindest eine Freude machen. Tenor: "Schaden kann's ja nicht!"
  Einige dieser Glücksbriefe drohen jedoch auch mit ernsten Konsequenzen für den Fall, dass sie nicht weitergeleitet werden. Dies kann abergläubische Menschen durchaus verunsichern; sie leiten sie dann lieber weiter, womit das Ziel wiederum erreicht wäre.

- **Mitleids-Briefe**
  Ein typischer Inhalt eines solchen E-Mails wäre, dass ein Kind an Krebs oder einer anderen Krankheit leidet und bald sterben wird und sein letzter Wunsch es wäre, dass dieser Kettenbrief um die Welt geht oder es mögen ihm möglichst viele Personen schreiben. Da die entsprechende E-Mail einem guten Zweck dient und außerdem die jeweilige Klinik von einer bestimmten Stiftung für jede Weiterleitung einen bestimmten Geldbetrag erhält, wie oft angefügt wird, sind viele Leute dazu geneigt, diese E-Mail weiterzuleiten.
  Es stellt sich jedoch die Frage, wer die Mails eigentlich zählt, wenn sie nicht alle an eine bestimmte Adresse geschickt werden. Weiters ist unklar wer an wen Geld zahlt und ob diese Zahlungen dann auch tatsächlich erfolgen. Schließlich könnte ja auch ein Spammer der Urheber dieser E-Mail sein, der auf diese Art an viele gültige E-Mail-Adressen gelangt und diese selbst verwenden oder weiterverkaufen kann.
  Die vor einigen Jahren durch die Presse gegangene Postkarten-Aktion für ein todkrankes Kind in England ist ein Beispiel für diese Art von E-Mails, nur dass es sich in diesem Fall um tatsächliche Postsendungen handelte. Dieses Kind wurde jedoch noch lange Zeit später mit Unmengen an Post überhäuft, die es gar nicht haben wollte, da die Idee dazu nicht von dem Kind selbst sondern von jemand anderem kam.

- **Sinnlose Petitionen**

  In diese Kategorie fallen Kettenbriefaktionen, die dazu aufrufen, sich für oder gegen bestimmte Anliegen einzusetzen. Diese Anliegen mögen zwar gut gemeint und die Ziele auch sinnvoll sein, jedoch sind Kettenbriefe kein adäquates Medium, um über seriöse Anliegen zu kommunizieren.
  Ein Beispiele für solche Aktionen sind der von Medien gewürdigten Kettenbriefe "Taliban's War on Women" und diverse Filmboykotte. Ein weiteres Beispiel kursierte 1999: Das „TIME-Magazin“ suchte den Menschen, der das 20. Jahrhundert am meisten geprägt hat ('Man of the Century'). Es wurde befürchtet, dass dazu Adolf Hitler gewählt werden könnte und man versuchte diese Wahl per E-Mail-Petition zu beeinflussen.
  Hinzu kommt, dass solche Aufrufe häufig aus USA stammen und - wenn überhaupt - auch nur dort ein Zusammenhang zur Realität hergestellt werden könnte. Diese in Europa weiterzuleiten, hätte nur geringen oder gar keinen Sinn.

Abschließend kann angemerkt werden, dass man Kettenbriefe auf keinen Fall unterstützen sollte. Soweit sie nicht ohnehin illegal sind, handelt es sich bestenfalls um schlechte Scherze, die man ignorieren sollte.

Eine Ausnahme spezieller Art stellen tatsächliche Hilferufe dar, die allerdings sorgfältig auf Aktualität und Seriosität geprüft werden müssen. Allgemein ist ein Kettenbrief jedoch, wie bereits erwähnt, kein geeignetes Mittel, um seriöse Hilferufe zu verbreiten.
Als Beispiel wird folgendes E-Mail aus dem Jahr 1999 angeführt, welches ein tatsächlicher Hilferuf war:

> ACHTUNG AN ALLE! SENDET DIESE NACHRICHT AN ALLE; DIE IHR KENNT
> Gesucht wird: Ein Knochenmarkspender mit der Blutgruppe B
> positiv, der so selbstlos ist , dass er die Risiken einer
> Transplantation auf sich nimmt. Wer ein Leben retten mochte, der maile
> mir bitte. XXXXXX@on-luebeck.de Weitere Informationen wurde man dann
> von den Eltern des betroffenen Madchens erhalten. DANKE!!!!!

Die Angabe der E-Mailadresse lässt in diesem Fall darauf schließen, dass es sich um einen echten Hilferuf handelte was durch eine Rückfrage an die angegebene E-Mailadresse auch überprüft werden konnte.

3.7 Auswirkungen von Spam-Mails

Die Auswirkungen von Spam-Mails können sehr vielfältig sein. Spam-Mails können sich einerseits im technischen Bereich, das sind der Senderrechner, der Empfangsrechner sowie das Internet selbst, als auch im persönlichen Bereich bezüglich Arbeitsaufwand bis hin zu psychologischen Problemen auswirken. Neben diesen Auswirkungen sind die Übertragungskosten zum Herunterladen von Spam-Mails nicht unbeträchtlich.
Einer Studie des britischen Marktforschungsunternehmen "Benchmark Research" zufolge (Stand: Frühjahr 1998) verursachte die Unzahl an Werbe-E-Mails alleine in Großbritannien und Irland Kosten in der Höhe von etwa 98 Milliarden Schilling (etwa 7,12 Milliarden EURO). Diese Kosten setzen sich aus den Kosten für die Übertragung, das Lesen, Löschen sowie einer eventuellen Beantwortung dieser Werbe-E-Mails zusammen.

3.7.1 Beim Empfänger

Neben der belästigenden Wirkung sind die größten negativen Auswirkungen die der Empfänger tragen muss, die Kosten welche für das Herunterladen, Lesen und Löschen von Spam-Mails entstehen. Diese Kosten setzen sich aus der Netzbenutzung sowie der aufgewendeten Zeit zusammen.
Setzt man den durchschnittlichen Zeitaufwand für das Herunterladen, Lesen und Löschen eines Spam-Mails mit 10 Sekunden an und rechnet man eine Arbeitsstunde des mit Spam-Mail konfrontierten Mitarbeiters inklusive Steuern und Lohnnebenkosten mit 800 Schilling (ca. 58,14 EURO), so ergeben sich Kosten von 2,2 Schilling (ca. 0,16 EURO) pro erhaltenem Spam-Mail. Geht man davon aus, dass ein Unternehmen im Durchschnitt etwa 30 Spam-Mails (Annahme) pro Tag erhält, belaufen sich die Kosten pro Jahr (angesetzt mit 220 Arbeitstagen) auf ca. 14520 Schilling (ca. 1055,22 EURO). Nicht berücksichtigt sind in dieser Rechnung die Kosten für die Netzbenutzung, da sich diese aufgrund der unterschiedlichen Provider und deren unterschiedlichen Tarifen schwer ermitteln lassen.

Neben diesen Kosten können beim Empfänger von Spam-Mail aufgrund beleidigender, obszöner oder aggressiver Inhalte auch psychologische Probleme entstehen.

3.7.2 Beim Empfangsrechner

Beim Empfangsrechner kann es durch Erhalt von Massenmails zu einer Überfüllung der betroffenen Mailbox oder des gesamten Mailserver kommen. Durch diesen Speicherplatzmangel besteht die Gefahr, dass normale E-Mails verloren gehen, weil sie auf dem Server nicht mehr gespeichert werden können.

3.7.3 Beim Sender

Durch die negative Einstellung der Internet-User gegenüber Spam kann es passieren, dass der Spammer statt des gewünschten Werbeerfolgs genau das Gegenteil erreicht. Es ist durchaus denkbar, dass Internet-User die Geschäftsaktivitäten des Spammers boykottieren und andere Firmen bevorzugen.
Neben diesem denkbaren Geschäftsentgang leidet auch das Image von Unternehmungen, welche mittels Spam Werbung betreiben.
Neben dieser passiven Boykottmaßnahme greifen User immer häufiger zu aktiven Maßnahmen. Diese Maßnahmen können einerseits eine Beschwerde beim Provider des Spammers sein, andererseits können die User mit Mailbombs reagieren. Dies geschieht dadurch, indem dem Spammer eine Vielzahl von Mails oder einige von der Datenmenge her sehr große E-Mails geschickt werden. Diese Mailbombs (siehe Kapitel 3.10.3) führen zu einer Überfüllung der Mailbox des Spammers und können zum Verlust anderer erhaltener Mailnachrichten führen. Weiters kostet es dem Spammer hohe Online-Ressourcen um die Mailbox abzurufen, da aufgrund der Überfüllung ein sehr hoher Datentransfer zwischen Mailserver und Rechner besteht. Benutzt er jedoch den IMAP 4 – Standard, stellen diese Mailbombs jedoch kein Problem für ihn dar.
Auch der Einsatz von sogenannten „Teergruben“ (engl. „tar pits“) ist eine stark verbreitete Abwehrmaßnahme gegen Spammer. Die Verwendung von Teergruben hat zur Folge, dass der Host des Spammers verlangsamt oder sogar gänzlich sendeunfähig wird (siehe Kapitel 3.8.7). Gelangen bei einem Provider eines Spammers häufige Beschwerden von Spam-Opfern ein, bzw. leiden die Ressourcen des Providers aufgrund von Attacken mit Mailbombs bzw.

Teergruben, hat das sehr häufig zur Folge, dass der Internetzugang des Spammers gesperrt wird.
Immer häufiger ist im deutschsprachigen Raum auch zu beobachten, dass gespammte User dem Spammer mit einer Gerichtsklage drohen. Grundlage dafür sind exemplarische Gerichtsurteile in der Bundesrepublik Deutschland, welche Spammern unter Androhung hoher Geldstrafen eine Weiterführung ihrer Tätigkeit untersagt haben (siehe Kapitel 3.8.1.1 und 3.11).[6]

3.7.4 Beim Senderechner

Ein großes Problem ist, dass durch das Versenden von Spam-Mails die Ressourcen des Senderechners sehr stark beansprucht werden. Das hat natürlich zur Folge, dass auch andere Kunden des Providers unter dem Ressourcenverbrauch der Spam-Sendungen, welche oft zigtausende Mails beinhalten, in Mitleidenschaft gezogen werden.
Darüber hinaus werde - wie in Kapitel 3.7.3 erwähnt - Spammer häufig mit Mailbombs oder Teergruben attackiert, was wiederum zu einer Ressourcenbelastung führt.
Häufig werden Spam-Mails jedoch nicht über den Mailserver des eigenen Providers versendet, sondern mittels E-Mail-Relaying (siehe Kapitel 3.2.1.3) über fremde Server, welche durch eine schlechte SMTP-Implementierung den Absender des Spammers eventuell geheim halten können. Diese leiden dann ebenso unter Ressourcenverschwendung und Überlastung wie die eingangs erwähnten Server.

3.7.5 Im Internet

Durch den Massenversand von E-Mails mittels Spamming wird wertvolle Bandbreite des Internets verschwendet. Das Internet wird insgesamt langsamer und diverse Server sowie der Mailserver des Senders und die Mail- und News-Server der Empfänger werden unnötig belastet.
Dadurch, dass Spammer Mailinglisten verwenden, in denen häufig nicht mehr gültige E-Mail-Adressen enthalten sind, werden viele Nachrichten mit einer Fehlermeldung an den Spammer

[6] In der CNN-Onlineausgabe vom 28. Oktober 1999 wird berichtet, dass zwei US-Amerikaner, welche Werbung mittels E-Mail-Spam betrieben haben, von Unbekannten wegen ihrer Spam-Tätigkeit ermordet wurden. http://www.cnn.com/US/9910/28/businessmen.killed.02.ap/index.html

zurückgeschickt, was wiederum zu einer weiteren Verschwendung wertvoller Bandbreite des Internets führt.
Darüber hinaus leidet - wie in Kapitel 3.7.6 erwähnt wird - die Effektivität von Newsgroups, da viele User aufgrund nicht zum Thema gehörender Artikel eine Nutzung von Newsgroups unterlassen. Ein weiterer Grund für die geringere Nutzung des Usenets ist die Gefahr, dass die E-Mail-Adresse der User von Spammern gesammelt wird, da das Usenet die größte Quelle zur Sammlung von E-Mail-Adressen ist.

3.7.6 Soziale Auswirkungen

Diese Art von Auswirkungen sind von nichtmonetärer Natur. Es handelt sich hier vielmehr um die Schädigung des Usenets in seiner ursprünglichen Art der vorgesehenen Verwendung.
Aufgrund der immer häufiger werdenden Werbepostings in Newsgroups sinkt das Interesse der User an Newsgroups teilzunehmen, da es immer schwieriger wird, die relevanten Nachrichten zu finden. Damit verbunden sinkt die Verwendung und Effektivität von Newsgroups als Diskussionsforen und als Informationsquellen zur Problemlösung.
Da Newsgroups für Spammer als große Quelle zur Adressensammlung dienen, haben darüber hinaus Internet-Neulinge immer häufiger Hemmungen an Newsgroups teilzunehmen.
Weiters ist anzumerken, dass als Konsequenz eines zu hoch werdenden Traffics in Newsgroups, aufgrund von Werbepostings, ISPs häufig gezwungen sind die Anzahl der Newsgroups zu reduzieren. Daraus resultiert wiederum eine verringerte Nutzungsmöglichkeit des Usenets.
Wie in Kapitel 3.8.1.1 erwähnt, ändern viele Usenet-User ihre E-Mail-Adresse entsprechend, um nicht von Adresssammelprogrammen von Spammern aufgenommen zu werden. Dieser Umstand erschwert jedoch das Antworten auf Usenet-Artikel, da die E-Mail-Adresse mühsam von Hand aus geändert werden muss und dadurch entsprechend Zeit kostet. Viele User unterlassen deshalb häufig eine Beantwortung eines Artikel mit geänderter E-Mail-Adresse, was wiederum die Effektivität des Mediums Usenet verringert bzw. zerstört.
Es gilt im Usenet außerdem als unhöflich, Leuten, mit denen man diskutieren will oder von denen man Hilfe erwartet, zuzumuten, den Artikel auf Änderungshinweise für die E-Mail-Adresse zu durchsuchen.

3.8 Maßnahmen gegen Spamming

In diesem Kapitel werden sowohl Maßnahmen beim Userverhalten als auch technische und administrative Maßnahmen gegen Spamming beschrieben.

3.8.1 Maßnahmen seitens des Users

Hier wird beschrieben, wie sich ein User verhalten soll, falls er gespammt wird bzw. welche Maßnahmen er setzen kann, um nicht potentielles Opfer eines Spammers zu werden oder um Spam-Mails abzublocken.

3.8.1.1 Verhalten des Users

- Erhält man eine Spam-E-Mail, sollte man nie auf den Inhalt antworten. Es wird bei Spam-Mails oft die Möglichkeit angeboten, durch ein entsprechendes Reply-Mail sich von der Mail-Liste entfernen zu lassen. Geht man jedoch auf diese Angebot ein, wird man zwar von dieser Mail-Liste entfernt, der Spammer weiß aber, dass es sich um eine gültige Adresse handelt und wird diese wahrscheinlich weiterverkaufen.

- Bei deutschsprachigen Spam-Mails kann es durchaus Sinn haben, auf dieses Mail zu reagieren um bekannt zu geben, dass man keine weiteren Werbesendung mehr wünscht. [GOLDMANN 99]
  Eine angemessene Reaktion auf Spam sollte sachlich und bestimmt sein. Gleichzeitig sollte sie nicht allzu viel Zeit kosten. Mit folgender Standard-Reply-E-Mail wurden bereits gute Erfahrungen gemacht. Weit mehr als 90% der mit dieser Mail bedachten Spammer haben weitere Mails unterlassen.

```
At 21:14 16.04.99 +0200, you wrote:
>Wir sind ein innovatives Unternehmen, dass sich mit seinem
Produkt
>ganz klar an dem Bedarf der Anleger nach aktuellen und
präzisen Daten
>und Fakten über US-amerikanische Aktien und Optionswerte
orientiert.
```

```
>...

Folgenden Text zur Kenntnisnahme.
```

Hier kann nun z.B. der Beschluss Geschäftsnummer 16 O 201/98 des Landgerichts Berlin eingefügt werden (siehe Kapitel 3.11).

```
Mit freundlichen Grüßen
```

[WALDNER]

Gegenüber Usenet-Spam mag ein ähnliches Vorgehen richtig sein. Leider fehlt eine entsprechende Gerichtsentscheidung für Usenet-Spam bis dato. Man könnte darauf hinweisen, dass die Sachlage ähnlich wie bei E-Mail zu beurteilen ist, jedoch muss die Reaktion direkt an denjenigen gesendet werden, der gespammt hat und nicht in die Newsgroup gepostet werden, da es sich sonst seinerseits wiederum um Spam handeln würde.

Viele Spammer unterlassen ihren Spam in Newsgroups bereits dann, wenn sie einmal öffentlich darauf hingewiesen werden, dass Spam in der betreffenden Newsgroup unerwünscht ist. Solche Hinweise sind schließlich schon peinlich genug.

Bei häufigerem Erhalt von Spam-Mails von verschiedenen Absendern ist es durchaus sinnvoll, wenn der User Kontakt zum Postmaster seines ISPs aufnimmt, um Abwehrmaßnahmen zu besprechen und einzuführen. Sendet ein einzelner Absender häufig Spam-Mails und ist dieser eindeutig identifizierbar, ist eine Beschwerde beim Administrator der Absender-Domain durchaus sinnvoll [TU-CHEMNITZ 97]. Fast alle Provider verbieten es in ihren AGB ausdrücklich, über ihren Netzwerkzugang rechtswidrige Handlungen vorzunehmen. Die meisten Provider verpflichten ihre Kunden zusätzlich in der einen oder anderen Form zur Einhaltung der Netiquette. Um einen Spammer eindeutig zu identifizieren, sind die "`Path:`"-Header von besonderem Interesse, da hier steht, welche Wege eine Mail genommen hat. Jedoch ist hier auch Vorsicht geboten, da die angegebenen Rechnernamen nicht unbedingt stimmen müssen.

Man sollte daher immer die IP-Adressen der angegebenen Rechner ansehen, da die Gültigkeit dieser Angaben nämlich vom empfangenden Mailserver garantiert werden. Ein Aufruf von *nslookup* mit dem Rechnernamen oder der IP-Adresse als Parameter zeigt an, ob der Rechnername wirklich zur IP-Adresse gehört. Stimmt die Angabe nicht, dann hat man mit der IP-Adresse denjenigen gefunden, der die Mail versendet hat. Sind alle Angaben korrekt, dann ist der letzte Sender der korrekte Absender.

Als Beispiel wird hier mit *nslookup* der Server *web.williams.edu* des "Williams College" gesucht:

```
Non-authoritative answer:
web.williams.edu      internet address = 137.165.4.29

Authoritative answer can be found from:
williams.EDUnameserver = lee.williams.EDU
williams.EDUnameserver = lenox.williams.EDU
williams.EDUnameserver = nic.near.net
lee.williams.EDU      internet address = 137.165.4.2
lenox.williams.EDU    internet address = 137.165.4.21
nic.near.net     internet address = 192.52.71.4
```

In zwei Fällen ist die IP-Adresse nicht ersichtlich.
Der erste Fall ist, wenn der erste Host den man sucht kein realer Host ist sondern lediglich ein alternativer Name für einen tatsächlich existierenden Host. Sucht man z.B. *www.williams.edu* wird folgende Meldung ausgegeben:

```
www.williams.edu canoncial name = web.williams.edu
```

So erfährt man den tatsächlichen Hostnamen mit welchem man nun die IP-Adresse ermitteln kann.

Der zweite Fall ist jener, wenn der Host, nach welchem man sucht, seine eigenen E-Mails nicht selbst verwaltet. Ein Beispiel dafür wäre:

```
sjdm.org preference = 10, mail exchanger = mail.sjdm.org
```

Wird ein Mail zum Host *sjdm.org* gesendet, wird es nicht von diesem Host verwaltet, sondern vom Host *mail.sjdm.org*. Von diesem Host kann man nun wiederum die IP-Adresse ermitteln.

- Hat man die Absenderdomain ermittelt, dann erfährt man mit `whois-<Domain>` mehr über diese Domain. Die whois-Abfrage wird bereits von einigen Web-Seiten unterstützt, welche auf eine existierende Domain umfangreiche Informationen liefert. So liefert die Abfrage nach *aon.at* (Austria Online) auf der Web-*Seite "http://www.ripe.net/cgi-bin/whois"* folgende Informationen (Abfrage durchgeführt am 99-09-29):

```
Whois aon.at

% Rights restricted by copyright. See
http://www.ripe.net/db/dbcopyright.html

domain:      aon.at
descr:       [organization]: PTA TG4
descr:       [name]: Hr. P.
descr:       [street address]: Postgasse 8
descr:       [postal code]: A-1010
descr:       [city]: Wien
descr:       [country]: Austria
descr:       [phone]: +43 1 515 51 0
descr:       [fax-no]: +43 1 798 29 88
descr:       [e-mail]: h.p@pta.at
descr:       Austria-ONLINE Dienst
admin-c:     GP159-RIPE
tech-c:      WC82-RIPE
tech-c:      VM404-RIPE
zone-c:      WC82-RIPE
```

```
nserver:     ws01is01.highway.telekom.at
nserver:     ws01is02.highway.telekom.at
remarks:     195.3.96.67
remarks:     195.3.96.68
mnt-by:      AT-DOM-MNT
changed:     domain-admin@univie.ac.at 19980928
source:      RIPE

person:      Gottfried P.
address:     Post und Telekom Austria Aktiengesellschaft (PTA)
address:     Technical Engineering Centre (FZA)
address:     Arsenal Obj. 22
address:     A-1103 Vienna, P.O.Box 111
address:     AUSTRIA
phone:       +43 1 79711 0
fax-no:      +43 1 79711 1608
e-mail:      gpieler@aon.at
nic-hdl:     GP159-RIPE
notify:      r@highway.telekom.at
changed:     g@aon.at 19970521
changed:     g@aon.at 19980929
source:      RIPE

person:      Wolfgang C.
address:     Telekom Dienste Wien
address:     Highway 194
address:     FZG Arsenal Objekt 24
address:     A-1103 Wien
address:     Austria
phone:       +43 1 79744 3291
fax-no:      +43 1 7982667
e-mail:      domain-admin@highway.telekom.at
nic-hdl:     WC82-RIPE
notify:      domain-admin@highway.telekom.at
```

```
notify:      domain-admin@highway.telekom.at
changed:     domain-admin@univie.ac.at 19980420
changed:     at-dom.admin@nic.at 19990623
source:      RIPE

person:      V. Martin
address:     Telekom Austria Aktiengesellschaft
address:     Technical Engineering Centre
address:     Arsenal Obj. 22
address:     A-1103 Vienna, P.O.Box 111
address:     AUSTRIA
phone:       +43 1 79711 1625
fax-no:      +43 1 79711 1608
e-mail:      mv@highway.telekom.at
nic-hdl:     VM404-RIPE
notify:      mv@highway.telekom.at
changed:     gp@aon.at 19980515
changed:     mv@highway.telekom.at 19980619
changed:     mv@highway.telekom.at 19990519
source:      RIPE
```

- Ein `tracert` (auf WinNT) oder `traceroute` (auf Unix) mit dem Mailserver des Absender als Parameter zeigt an, über welche Rechner der Mailserver des Absenders mit dem Internet verbunden ist. Sieht man sich die letzten Ausgabezeilen an, dann kann man daran auch den ISP des Absenders ersehen. Heute gibt es unter Windows bereits sehr gute Programme, mit denen man solche Abfragen bewerkstelligen kann. Hat man diese Angaben ermittelt, steht einer Beschwerde beim Absenderdomain oder beim ISP nichts mehr im Wege. Viele Domains haben für solche Beschwerden extra einen User `abuse` eingerichtet. Existiert dieser nicht, kann man sich beim `postmaster` beschweren. [TU-BERLIN 2/99] Diese Suche nach dem Spammer wird jedoch sehr oft erschwert, da Spammer durch Verwendung von Testangeboten häufig den ISP wechseln.

- Findet man eine Werbe-E-Mail erstmals im Maileingang, sollte man einen Hinweis mit der E-Mailadresse des Absender an die Betreiber von Robinsonlisten schicken. Die Betreiber werden den Absender der Werbe-E-Mail auf die Robinsonliste hinweisen, bzw. wenn er ihnen schon bekannt ist, entsprechend deutlicher werden.

- Der User sollte darauf verzichten allzu häufig oder überhaupt keine Nachrichten in Newsgroups zu posten, da Newsgroups die größten Quellen für Spammer sind, um E-Mailadressen zu erhalten (siehe Kapitel 3.4.1).

- Beim Posten von Nachrichten in Newsgroups kann man versuchen, potentielle Spammer zu täuschen, indem man die E-Mailadresse so ändert, dass sie von automatischen Adresssammelprogrammen nicht erkannt wird. Eine Möglichkeit z.B. wäre der Einbau von Unterstrichen beim "@"-Zeichen. So würde etwa aus `hans.wurst@jk.uni-linz.ac.at` dann `hans.wurst_@_jk.uni-linz.ac.at`. Wer dann ein E-Mail an diese Adresse schreiben will, muss lediglich die Unterstriche entfernen. Diese Maßnahme ist im Usenet jedoch umstritten, da sie das Antworten auf Beiträge erschwert. Oft ist auch zu beobachten, dass nicht existente E-Mailadressen wie etwa `absender@nospam.at` angegeben werden, um damit darauf hinzuweisen, dass man mit dieser Adressen damit vorbeugen will, ein potentielles Opfer von Spammern zu werden. Diese Methode wiederum hat den Nachteil, dass man eventuell erwünschte Reaktionen auf das Posting nicht erhält und eventuelle Reaktionen an den Postmaster der tatsächlich existierenden Domain `nospam.de` fehlgeleitet werden. Um dies zu umgehen ändern manche Benutzer von Newsgroups ihre E-Mailadresse so ab, indem sie am Ende der Adresse den Zusatz `.nospam` anhängen und in der Signatur darauf hinweisen, dass man bei Antworten diesen Zusatz entfernen soll. Dieses Verfahren hat jedoch zwei entscheidende Schwachpunkte. Der erste Schwachpunkt ist die Effektivität. Verwendet man für die Absenderänderung eine einfache Methode wie das Anhängen von `.nospsam`, kann ein Spammer diese Methode auch maschinell implementieren. Wenn er die Absender scannt, probiert er einfach aus, ob die Adresse auf `nospam` endet, entfernt gegebenenfalls diesen Zusatz und erhält somit wiederum die richtige E-Mail-Adresse. Um dies zu vermeiden, ist es erforderlich, die E-Mail-Adresse komplexer zu verschlüsseln. Dies hat jedoch wiederum den Nachteil, dass es jemandem, der antworten will, schwierig gemacht wird die korrekte Absenderadresse zu ermitteln und dadurch oft auf eine Antwort

verzichtet. Da man in Newsgroups jedoch häufig als Fragesteller auftritt, sollte man es möglichst einfach machen Antworten zu senden, was wiederum Spammern zugute kommt.

3.8.1.2 Maßnahmen beim Webdesign

- Ebenso kann man modifizierte Adressen mit "_@_" oder ähnlichem auf der eigenen Homepage verwenden, da viele Spammer auch Homepages mit Suchprogrammen nach E-Mailadressen durchsuchen (siehe oben und Kapitel 3.3.3).

- Eine andere Möglichkeit wäre, Teile der E-Mail-Adresse oder der Domain im HTML-Quelltext fett oder in *italic* darzustellen, da viele Adressen-Harvester auf diese Art dargestellte E-Mail-Adressen nicht erkennen. Ein Beispiel für einen solchen HTML-Quellcode wäre: b.s@<I>jk.uni-linz.ac.at</I>.

- Die *"Multimedia Marketing Group"* (http://www.mmgco.com/nospam) schlägt vor, ein `%20` vor der E-Mail-Adresse einzufügen, wenn sie in einem "`mailto:`"-Link vorkommt.

  Ein Beispiel wäre:
  ```
  <A HREF=mailto:%20bernhard.schoberberger@jk.uni-
  linz.ac.at>Mail me!</A>
  ```

  Web-Browser übersetzen `%20` beim Anklicken in ein Leerzeichen, so dass diese Methode auf Web-Browsern funktioniert, Adressen-Harvester jedoch eine falsche E-Mail-Adresse bekommen. Spammer jedoch können wiederum eine Methode implementieren, dass der Harvester beim Scannen der E-Mail-Adressen überprüft, ob am Beginn der Adresse %20 steht und dieses automatisch entfernen lassen, was die Effizienz dieses Verfahrens sinken lässt.

- Man sollte auf den Besuch von WWW-Seiten verzichten, welche eine Registrierung erfordern. Lässt man sich doch registrieren, sollte man nicht die richtige E-Mailadresse angeben, außer man vertraut dem Betreiber der Web-Seite.

- Beim Design von Web-Seiten kann man statt einem "`mailto:`"-Link auch eine Graphik verwenden, welche die E-Mail-Adresse beinhaltet. Diese Vorgangsweise hat jedoch zwei entscheidende Nachteile. Zum einen muss jemand, der ein Mail schicken will zuerst ein Mailprogramm öffnen und die Adresse händisch eintippen, zum anderen wird die Graphik mit der E-Mail-Adresse in Browsern, bei welchen die Anzeige von Graphiken ausgeschalten ist, nicht angezeigt.

- Beim Auslesen von Daten aus Web-Formularen sollte man CGI-Skripts anstatt des "`mailto:`"-URLs verwenden, da dadurch die Sicherheit der übermittelten Daten am ehesten gewährleistet ist.

3.8.1.3 Einschalten von Mailfiltern in Mailreadern

Ein guter Mailreader hat meist die Möglichkeit, Mails beim Empfang automatisch in Ordner zu verschieben. Durch geeignete Wahl dieser Mailfilter können sehr viele Spam-Mails gelöscht oder in einen eigenen Ordner verschoben werden. Diese Verfahren haben jedoch den Nachteil, dass alle Mails heruntergeladen werden müssen, da sie erst auf dem eigenen Rechner aussortiert werden. Besser wäre es, einen Mailfilter auf dem Server des Providers zu benutzen, da dadurch die Spam-Mails nicht mehr heruntergeladen werden müssen.

3.8.1.4 Eintrag in Robinsonlisten bzw. Opt-In und Opt-Out

Nach der Robinson-Liste gegen Werbebriefe gibt es nun auch die sogenannte "eRobinson"-Liste gegen die unerwünschte Flut aus dem Datennetz. Durch einen Eintrag in eine Robinson-Liste erklärt man, dass man keine Werbe-Mails erhalten will. Unter der Adresse *www.eRobinson.com* können sich Internet-User kostenlos eintragen lassen. Wie bei dem schon 1982 eingerichteten Vorbild respektieren - zumindest nach Angaben der deutschen Verbraucherschutz-Initiative - alle großen Versandhäuser auch die elektronische Robinson-Liste und verschonen die eingetragenen E-Mail-Adressen mit ihren Sendungen.
Zur Kontrolle hat die deutsche Verbraucherschutz-Initiative 30 getarnte E-Mail-Adressen selbst eingerichtet. Ob sich jedoch die einschlägigen Versandhäusern in den USA, die beim Werbe-E-Mailing besonders aktiv sind, sich an den Wunsch der Nutzer halten, ist wohl mehr als fraglich. [MORGENPOST 97]

Das Problem dabei ist, dass das Internet ein internationales Medium ist, wobei selbst oft nationale Regelungen kaum geklärt sind.

Aktivitäten der Betreiber von Robinson-Listen:

- Es werden Listen mit den eingetragenen E-Mail-Adressen interessierten Mailversendern (Spammern) zur Verfügung gestellt, damit diese ihre Adresslisten abgleichen können. Seriöse Anbieter - sofern man bei Spammern überhaupt von seriös sprechen kann - werden davon Gebrauch machen.

- Bei bekannt werden eines neuen Mailversenders wird dieser über die Robinson-Liste informiert und ebenfalls die Liste mit den Adressen zum Adressabgleich gesendet.

- Sollte ein Werbe-E-Mail-Versender wiederholt und trotz entsprechender Hinweise an Mitglieder von Robinsonlisten Werbe-E-Mails senden, behalten sich die Betreiber von Robinsonlisten rechtliche Schritte vor. Die Problematik jedoch ist, dass die rechtliche Situation in vielen Ländern zur Zeit noch ungeklärt ist, vom internationalen Aspekt ganz zu schweigen.

- Spammer werden darauf hingewiesen, dass ein Versand von Werbe-E-Mails an Mitglieder einer Robinsonliste kontraproduktiv ist. Ziel einer Werbung ist ja, aus potentiellen Kunden Neukunden zu machen. Da jedoch die in eine Robinsonliste eingetragenen Personen pauschal erklärt haben, keine Werbung zu wünschen, finden die Werbe-E-Mails keine Akzeptanz und das Image des Versenders leidet.

Eine Robinsonliste funktioniert nach dem sogenannten Opt-Out-Verfahren. Jeder, der keine Werbe-E-Mails erhalten will, muss sich in eine Robinsonliste eintragen, was dem Briefkastenaufkleber "*Keine Postsendungen ohne persönliche Anschrift"* entspricht.
Beim Opt-In-Verfahren hingegen wird unverlangte E-Mail-Werbung generell verboten. Das Verschicken von Werbe-E-Mails ist nur mehr zulässig, wenn sich der Empfänger in eine Mailing-Liste eingetragen hat, und er somit explizit sein Zuverständnis zum Erhalt von E-Mail-Werbung gibt. Es muss jedoch gewährleistet sein, dass er sich jederzeit wieder aus dieser Liste austragen kann. Damit wäre gewährleistet, dass jeder, welcher Informationen

oder Werbung über ein bestimmtes Produkt oder Thema wünscht, diese auch bekommt und andere User davon verschont bleiben. [VIBE 99]

3.8.2 Fremdcancel

Fremdcancel bietet Systemadministratoren im Usenet die Möglichkeit, bereits abgeschickte Artikel nachträglich zu löschen.
Die heute zur Verbreitung von Newsgroup-Artikeln verwendeten Programme werten sogenannte "Cancel-Messages" (Cancel-Steuernachrichten) aus. Es handelt sich hier um zusätzliche Nachrichten, in der Informationen darüber enthalten sind, welche Artikel zu löschen sind. Die Cancel-Steuernachricht ist dazu gedacht, dass Benutzer fehlerhafte oder unüberlegte Artikel später wieder zurückziehen können. Empfängt ein System eine Cancel-Nachricht, löscht es lokal den entsprechenden Artikel und leitet ihn nicht mehr weiter. Ist der Artikel nicht vorhanden, wird er zur Löschung vorgemerkt. Er wird dann im Falle eines späteren Eintreffens nicht mehr akzeptiert.
Unter einem Fremdcancel versteht man nun eine Cancel-Mitteilung, die nicht vom Autor des gecancelten Artikels verschickt wurde. Diese Möglichkeit von Fremdcancel ist sehr effektiv, da man gezielt gegen einen Verursacher von Spam-Postings vorgehen kann, ohne dabei fremde Ressourcen zu belasten. Das Problem, das der Fremdcancel jedoch verursacht ist, dass im Prinzip jeder einen Fremdcancel durchführen und somit beliebige fremde Artikel löschen kann. Dadurch ist das Usenet-Prinzip der freien Nachrichtenverteilung gefährdet und das Usenet könnte unbrauchbar werden. Das Canceln fremder Nachrichten ist daher im Prinzip nicht erwünscht und wird nur in bestimmten Fällen geduldet.

Im RFC 1036, dem derzeit gültigen Newsstandard ist zu Cancel-Mitteilungen angemerkt:

Nur der Autor und eines Artikels oder der lokale News-Administrator dürfen eine solche Steuernachricht versenden. Der verifizierte Absender einer Mitteilung ist der "Sender"-Zeile zu entnehmen, oder, wenn keine solche Zeile vorhanden ist, der "From"-Zeile. Der verifizierte Absender der Löschmitteilung muss mit der "Sender"- oder der "From"-Zeile des ursprünglichen Artikels übereinstimmen. Insbesondere reicht es hin, wenn der verifizierte Absender der Löschmitteilung mit dem unverifizierten Absender , der der "From"-Zeile der ursprünglichen Nachricht zu entnehmen ist, übereinstimmt.

Durch das Überhandnehmen von Spam in Newsgroups wird dieses Prinzip seit einiger Zeit nicht mehr strikt befolgt und Fremdcancel von Dritten bezüglich Spam akzeptiert.

Als Kriterium, wann ein Artikel gecancelt werden soll, dient der *Breitbard-Index*.
Dieser ist definiert als die Summe der Quadratwurzeln der Anzahl der Newsgroups, in die die Inkarnation des Artikels gepostet wurde.

$$BI = \frac{\sum Inkarnationen}{\sqrt{Anzahl\ an\ Newsgoups}}$$

Erreicht dieser Index einen bestimmten Wert, kann man davon ausgehen, dass ein Artikel als Spam gepostet wurde und ein Fremdcancel wird vertretbar. Z.B. In der *.de-Newsgroup-Hierarchie liegt dieser Index bei 10, bei den großen internationalen Hierarchien (comp, misc, rec, talk, news, sci, humanities, soc) liegt die Toleranzschwelle bei 20. [UNI-GIESSEN 98]

Da jedoch auch häufig ungerechtfertigte Fremdcancels auftreten, hat dies dazu geführt, dass auf bestimmten Systemen die Cancel-Verarbeitung deaktiviert wurde und somit eintreffende Cancel-Nachrichten ignoriert werden. Dadurch wird einerseits den Nutzern die Möglichkeit genommen eigene Artikel zu löschen, andererseits geht ein wichtiges Instrument zur Regulierung des Usenets verloren.

3.8.3 Filter

Filter sind die am weitesten verbreitete Methode um gegen Spam anzukämpfen. Die Filterarten können einerseits nach ihrer Wirkungsweise in heuristische und kooperative Filter und andererseits nach dem Wirkungsbereich in client- und serverseitige Filter unterteilt werden.

3.8.3.1 Heuristische Filter

Die meisten der existierenden Ansätze zur Filterung von Spam beruhen auf der Annahme, dass mit dem Spammer keine Kooperation besteht (siehe Punkt 3.8.3.2). Es muss also versucht werden, Spam nach gewissen Regeln bzw. Richtlinien zu identifizieren. Kommerzielle Filtersoftware beinhaltet bereits eine sehr hohe Anzahl von Filterregeln, die der Benutzer individuell anpassen und erweitern kann. Spammer jedoch werden gegenüber diesen Filterprogrammen immer einfallsreicher und tarnen Spam-Mails immer geschickter, so dass sie von den Filterprogrammen nicht als solche erkannt und an den Empfänger weitergeleitet werden.
Bei heuristischen Filtern sind clientseitige und serverseitige Filterprogramme zu unterscheiden.

3.8.3.1.1 Clientseitige Filter

Clientseitige Mailfilter sind Filter, die entweder im Mailprogramm eingebaut sind oder lokal am PC installiert werden um Spam-Mail zu filtern.
Mit solchen Filtern kann sich der User zwar vor unerwünschten Werbe-E-Mails schützen, der Nachteil dieser clientseitigen Filter ist jedoch, dass die Mails für eine Filterung weiterhin vom Server auf den PC geladen werden müssen und somit weiterhin Kosten und Wartezeit für die Übertragung dieser Mails zum eigenen Rechner entstehen.

3.8.3.1.2 Serverseitige Filter

Um Spam-Mails nicht vom Server herunterladen zu müssen um sie lokal mit einem E-Mail-Filter zu untersuchen, bieten sich serverseitige Filter an. Diese Filter laufen beim Provider auf

dem Mailserver und filtern Spam-Mail sofort aus, ohne dass diese an den Adressaten geliefert werden. Es bieten jedoch die wenigsten Provider den Usern die Möglichkeit serverseitige Mailfilter zu nutzen.
Da die gefilterten Mails bereits auf dem Server gelöscht werden, erspart sich der User die Online-Gebühren für das Herunterladen von Spam-Mails. Es ist jedoch nicht auszuschließen, dass das Filterprogramm E-Mails falsch filtert und diese löscht. Da der User, wie es bei clientseitigen Filtern möglich ist, die Mails, welche gelöscht werden, nicht kontrollieren kann, besteht die Gefahr, dass auch normale E-Mails gelöscht werden.

Das Filtern von Spam erfolgt nach folgenden vier Methoden:

1. IP-Verbindungen zum Server von bekannten Spammern abweisen
2. TCP-Verbindungen von bekannten Spammern im SMTP-Server (Mailserver) abweisen
3. Mail-Nachrichten abweisen, wenn im „From:“-Header die Adresse eines bekannten Spammers steht
4. Mail-Nachrichten abweisen, wenn die Domain des Absenders nicht mit der IP-Adresse übereinstimmt

ad 1)
Diese Technik beruht darauf, dass die Router des Servers so eingestellt werden, dass sie von bestimmten Domains, von welchen aus Spam verbreitet wird, keine IP-Pakete annehmen.

ad 2)
Viele Mailserver können so konfiguriert werden, dass sie die Domain oder die IP-Adresse, von welcher Daten empfangen werden, überprüfen, ob sie auf einer Liste unerwünschter Absender steht. Ist dies der Fall, wird die Annahme dieser Daten nicht zugelassen.

ad 3)
Der Mail-Server wird so konfiguriert, dass der „`From:`“-Header mit einer Liste unerwünschter Absenderadressen verglichen wird. Steht der Absender auf der Liste, wird die E-Mail gelöscht.

ad 4)
Bei dieser Methode wird die IP-Adresse der Domain ermittelt, von welcher die E-Mail geschickt wurde. Anschließend wird diese IP-Adresse mit der IP-Adresse der TCP-Verbindung über welche die E-Mail empfangen wurde, verglichen. Stimmen diese beiden IP-Adressen nicht überein, kann der Mailserver den Empfang dieser E-Mail ablehnen.

3.8.3.2 Kooperative Filter

Kooperative Filter beruhen auf einer Zusammenarbeit zwischen den Verfassern von Spam sowie den Empfängern dieser Nachrichten. Diese Methode ist jedoch nur dann sinnvoll, wenn die Urheber von Spam auch zu einer Zusammenarbeit bereit sind.
Bei dieser Art von Filterung werden zwei verschiedene Vorgehensweisen unterschieden:

- Identifikation des Mails als Spam seitens des Urhebers
- User-Registrierung

Identifikation des Mails als Spam seitens des Urhebers
Der Urheber eines Spam-Mails fügt in die E-Mail zusätzliche Informationen ein, so dass dieses von Filterprogrammen auch als Spam-Mail erkannt wird. Diese Informationen können zusätzliche Textinformationen - z.B. das Wort „Spam“ in der „Betreff“-Zeile - sein oder der Spammer identifiziert sich z.B. durch die Angabe seiner E-Mail-Adresse in der „From“-Zeile, sofern es sich um bekannte Spammer handelt, dessen E-Mail-Adresse den Usern auch geläufig ist.
Der Nachteil dieser Methode ist, dass das Spam-Mail auf jeden Fall zum User geschickt wird und dort clientseitig von einem Filterprogramm identifiziert und einer entsprechenden Bearbeitung zugeführt wird. Dadurch wird wiederum wertvolle Bandbreite des Internets verschwendet

User-Registrierung
Diese Filtermethode funktioniert ähnlich den in Kapitel 3.8.1.4 erwähnten Robinsonlisten, nur dass hier die User, welche keine Werbemails erhalten wollen, direkt beim Spammer registriert sind.

Der Vorteil dieser Methode ist, dass an registrierte User keine Spam-Mails gesendet werden und somit wertvolle Bandbreite des Internets gespart wird.
Die Gefahr, die bei dieser Methode besteht, ist, dass der Spammer die beim ihm registrierten E-Mail-Adressen zum Adressenhandel weiterverwendet und man durch eine Registrierung beim Spammer genau das Gegenteil erreicht. Es empfiehlt sich daher, diese Methode der Zusammenarbeit nur bei „seriösen“ Spammer (wenn man davon überhaupt sprechen kann) anzuwenden, noch besser wäre allerdings ein Eintrag in eine Robinsonliste (siehe Kapitel 3.8.1.4).

3.8.4 Firewalls

Eine Firewall ist eine Netzwerksoftware auf einem Computer, der zwischen das LAN und das Internet geschaltet wird. Über diesen Rechner wird der gesamte TCP/IP-Verkehr vom Internet in das LAN sowie vom internen LAN in das Internet abgewickelt.

Jedes Mal, wenn ein externer Server angesprochen wird, wird der komplette TCP/IP-Verkehr über die Firewall umgeleitet (bei Kommunikation zwischen zwei Servern in einem internen Netzwerk kann die Kommunikation auch direkt erfolgen). Dementsprechend werden ebenso alle IP-Pakete, welche vom Internet in das interne Netzwerk gelangen, über die Firewall umgeleitet, die sie nach Prüfung entweder an den tatsächlichen Empfänger weiterleitet, an den Absender zurückschickt oder verwirft.

Eine Firewall ist gewissermaßen eine Schwelle zwischen zwei Netzwerken, die überwunden werden muss, um Systeme im jeweils anderen Netz zu erreichen.
Es wird dafür gesorgt, dass jede Kommunikation zwischen den beiden Netzen über die Firewall geführt werden muss. Die Firewall sorgt durch Zugriffskontrolle und Audit dafür, dass das Prinzip der geringsten Berechtigung durchgesetzt wird und potentielle Angriffe schnellstmöglich erkannt werden. [DFN_CERT 97]

Je nach Konfiguration und gewünschtem Schutzniveau kann eine Firewall alle externen IP-Pakete, nur solche von definierten Servern oder die für bestimmte Internet-Protokolle bzw. Port-Nummern herausfiltern. Dadurch enthält eine Firewall die Wirkung eines zentralen Filters, welcher auch Mails von bestimmten Absendern filtern kann.

Weiters ist eine korrekt konfigurierte Firewall ein wirksamer Schutz gegen unautorisierte Versuche von außen auf das interne Netz zuzugreifen.

Bei der Konfiguration einer Firewall bestehen zwei unterschiedliche Ansätze:

- **Bestimmte Dienste erlauben**
  Bei diesem Ansatz werden bestimmte Dienste erlaubt, die genutzt werden können. Die restlichen Dienste stehen nicht zur Verfügung.
- **Bestimmte Dienste verbieten**
  Bestimmte Dienste werden verboten und können nicht genutzt werden. Alle anderen Dienste, die nicht ausdrücklich verboten sind, können genutzt werden.

Neben dieser Grobeinteilung können Firewalls nach Ihrer Konfiguration in 4 Klassen eingeteilt werden:

1. Packet Filter
Zwischen LAN und dem Internet wird ein Router so konfiguriert, dass er nur bestimmte Pakete durchlässt und die anderen Pakete abblockt.

2. Gateways
Ein Gateway ist ein Host, der eine Verbindung zu zwei verschiedenen Netzwerken hat und diese Verbindungen auf Applikations-Ebene realisiert werden. Durch Erweiterung dieser Applikationen um Access Control mit eigenem Audit und Aktivierung eines ausführlichen Audits auf dem Host ist die Nutzung eines Gateways als Firewall möglich. Einen Firewall auf Basis eines Gateways zu errichten, bietet sich besonders für kleinere LANs an.

3. Kombinationen von Packet Filter und Bastion
Bei diesem Konzept wird ein spezieller Host eingeführt, der als Bastion bezeichnet wird. Aufgabe dieser Bastion ist, ein ausführliches Audit der Netzaktivitäten zu ermöglichen und die Access Control zu verfeinern.
Der Packet Filter sorgt dafür, dass alle Verbindungen zwischen LAN und Internet immer über diese Bastion geführt werden müssen.

Je nach Position der Bastion werden drei verschiedene Konzepte unterschieden:

- 1.Bastion innen: Die Bastion liegt im LAN und ist von diesem leicht zu erreichen. Der Router beschränkt den Zugriff vom Internet auf diesen Host.
- 2.Bastion mitte: Die Bastion ist an einem eigenen Netzstrang angeschlossen, zu dem der Zugang sowohl vom Internet als auch vom LAN aus durch einen Router beschränkt wird.
- 3.Bastion außen: Die Bastion ist an einem eigenen Netzstrang angeschlossen, der vom Internet aus unbeschränkt erreichbar ist. Die Hosts des LAN können im Internet nur die Bastion erreichen

4. Mischtechniken

Firewalls mit einer Mischtechnik sind in ihrer Architektur den bereits beschriebenen Techniken sehr ähnlich, ihre Sicherheit hängt aber zu einem großen Teil von der Benutzung anderer Vernetzungstechniken ab.

3.8.5 Köderadressen

Dieser neue Ansatz von der Firma "Bright Light Technologies" (http://www.brightlight.com) macht sich den Umstand zunutze, dass Spammer häufig Programme zum Sammeln von E-Mail-Adressen verwenden. Es werden spezielle E-Mail-Adressen, sogenannte "Köderadressen", verstreut, die nur dazu verwendet werden, um von Spammer gesammelt zu werden.
Wird eine solche E-Mail-Adresse in einer Aussendung verwendet, handelt es sich aller Wahrscheinlichkeit nach um eine Spam-Aussendung, die bereits beim Provider durch einen entsprechenden serverseitigen Filter erkannt und gelöscht werden kann.
Dieser Ansatz hat den Vorteil, dass, im Gegensatz zu den herkömmlichen Filterprogrammen, keine Informationen über Spammer bekannt sein und damit keine Filterregeln definiert werden müssen. Spammer werden aufgrund der Köderadressen automatisch erkannt, was im schnelllebigen Medium Internet sehr von Vorteil ist.
Eine weitere Variante wäre auf der Web-Seite ein Verweis auf ein Script, welches automatisch Mengen an ungültigen E-Mail-Adressen produziert.

3.8.6 Blockieren von Port 25

Um dem Missbrauch des eigenen Mail-Servers zum E-Mail-Relaying zu verhindern, blockieren Mail-Administratoren häufig den Port 25 am Mail-Server, was jedoch auch zur Folge hat, dass das Eintreffen von jeglicher E-Mail von außerhalb verhindert wird.
Um jedoch weiterhin E-Mail empfangen zu können, müssen einige Rechner von diesem Block ausgenommen werden. Um die Auslieferung von E-Mail an Adressen dieses Mail-Servers zu ermöglichen, ist es erforderlich, dass zu jeder Domain-Adresse, an die E-Mail ausgeliefert werden soll, mindestens zwei sogenannte MX-records im DNS existieren. Ein primärer, der den Zielrechner selbst bezeichnet sowie ein sekundärer für die vom Block freigegebenen Rechner. Versucht ein Spammer von außerhalb diesen Mailserver zum Relaying zu verwenden, wird zuerst versucht die E-Mails über den primären Server zu versenden, was jedoch nicht funktionieren wird. Durch ansprechen des sekundären Servers wäre es jedoch wiederum möglich, die Spam-Mails zu versenden. Da dann der angesprochene Rechner in der Relay-Mail aber gar nicht vorkommt, ist ein Relaying nicht möglich.

3.8.7 Teergruben (tar-pits)

„Tar Pits“ (dt. Teergruben) sind ursprünglich Kampfutilities im Cyberpunk/Darkfuture – Computerspiel „Shadowrun“. Ein tar-pit-utility verlangsamt in diesem Spiel den Gegner bis zur Bewegungsunfähigkeit.
Da eine Teergrube bei Spammern eine ähnlich Wirkung hat, nämlich den Host des Senders von Spam-Mail zu verlangsamen bzw. - wenn möglich - gänzlich sendeunfähig zu machen, wurde diese Bezeichnung für den Internetbereich übernommen. [NETZSERVICE]

Eine Teergrube bezeichnet eine ergänzte Posttransportsoftware, die im Kampf gegen die Belästigung durch unerwünschte Werbung per E-Mail zum Einsatz kommt.

Die numerischen Adressen der Internet-Rechner, von denen regelmäßig UCE kommt, sind bekannt. Sollte sich nun ein Posttransportprogramm (MTA = Mail Transfer Agent) von einer solchen Adresse bei einer Teergrube melden, wird die Verbindung so lange offen gehalten, bis die Verbindung vom Sender wieder abgebrochen wird. „Im Prinzip geht es darum, dem Postboten solange die Hand zu schütteln, bis er sich endlich losreißt“.

Ein Rechner kann allerdings eine ganze Reihe von Verbindungen zu anderen Netzknoten unterhalten. Trifft er dabei auf weitere Teergruben, bleibt er dort auch kleben, während an anderen Stellen der Werbemüll normal ausgeliefert wird. Der gewünschte Effekt wird trotzdem erzielt: Die Postauslieferung des Senders wird deutlich verlangsamt, und damit werden die Kosten für Spam erhöht. [FITUG 98]

Eine Teergrube ist ein Mailer, der Spam im SMTP-Dialog erkennen kann und die Datenübertragung künstlich extrem verlangsamt. Der Werbeversender wird dadurch im Absetzen seiner Nachrichten behindert, denn er wird gezwungen eine Vielzahl von Verbindungen parallel aufzubauen und kann diese nicht wieder schließen, bis die Übertragung abgeschlossen ist. Ähnlich wie ein Mammut in einer eiszeitlichen Teergrube ertrinkt der Werbeversender langsam, aber sicher in der schieren Anzahl von Verbindungen, die er aufbaut und nicht wieder los wird. Dadurch entstehen ihm extreme Onlinezeiten und Transportmengen, die das Senden für ihn unwirtschaftlich werden lassen.

Wirkungsweise einer Teergrube:
E-Mail Versand erfolgt über SMTP. Dabei wird eine TCP/IP Verbindung zum MX Host des betreffenden Empfängers hergestellt. Üblicherweise kann ein Rechner max. 65500 TCP/IP Verbindung gleichzeitig offen halten, in der Regel sind es weniger (Ressourcenlimit, z.B. MAX_SOCKET, MAX_FILE_DESCRIPTOR).

Wenn es gelingt, einen Port bei der Mailauslieferung offen zu halten, bspw. über mehrere Stunden, so reduziert sich die Leistungsfähigkeit des UBE Senders. SMTP bietet dazu die Fortsetzungszeilen, mit denen die SMTP Session offengehalten werden kann, ohne dass ein Timeout zuschlägt.

Was eine Teergrube nun macht ist, einen genauso präparierten MTA dazu zu bewegen, dass er eben (in Abhängigkeit vom SMTP-Absender) den Prozess auflaufen lässt.
Dem Spammer werden somit seine Arbeitsmittel zerstört.

Fortsetzungszeilen

Ein SMTP Host sendet als Antwort auf die Kommandos des Clients Zeilen, die aus einem Fehlercode, einem Leerzeichen und einem lesbaren Text bestehen. Wird das Leerzeichen durch ein Minuszeichen ersetzt, so bedeutet das, dass der Host noch nicht mit der Antwort fertig ist. Folgendes Aussehen ist vorstellbar:

```
help
214-This is Sendmail version 8.8.5
214-Topics:
214-    HELO    EHLO    MAIL    RCPT    DATA
214-    RSET    NOOP    QUIT    HELP    VRFY
214-    EXPN    VERB    ETRN    DSN
214-For more info use "HELP <topic>".
214-To report bugs in the implementation send E-Mail to
214-    sendmail-bugs@sendmail.org.
214-For local information send E-Mail to Postmaster at your
site.
214 End of HELP info
```

Sendet man nun derartige Fortsetzungszeilen im Abstand von Minuten, so verbraucht das fast keine Bandbreite und stoppt den UBE-Versenderhost wirksam. [FITUG 99]
Der Nachteil dabei ist, dass Rechner von großen Firmen, welche viele E-Mails versenden, davon genau so betroffen sind.

3.9 Anti-Spam-Programme

Um die immer stärker werdenden Flut von Spam-Mails in den Griff zu bekommen, wurden bereits eine Vielzahl von Programmen zur Bekämpfung von Spam entwickelt.
Die Wirkungsweise solcher Programme besteht darin, dass Mails aufgrund benutzerdefinierter Regeln als Spam identifiziert und einer entsprechenden Bearbeitung (Löschen, entsprechend markieren oder in einen bestimmten Ordner verschieben) zugeführt werden.
Bei diesen Programmen kann es sich einerseits um serverseitige Filterprogramme (laufen serverseitig) oder andererseits um clientseitige Programme (laufen auf dem Clientrechner des Benutzers) handeln.

3.9.1 Serverseitig

Bei serverseitigen Filtern handelt es sich um Filterprogramme, welche direkt auf dem Mailserver laufen und dort das Filtern von Spam-Mails erledigen (siehe Punkt 3.8.3.1.2).

3.9.1.1 Procmail

Procmail ist ein Programm auf Unix-Systemen, welches einkommende Mails anhand von benutzerdefinierten Regeln serverseitig sofort nach Einlangen bestimmten Aktionen unterwerfen kann (z.B. Mails automatisch in einen bestimmten Mail-Folder einsortieren, bestimmte Mails an andere Accounts weiterleite, unerwünschte Mails verwerfen).
Bei einem starken Mail-Traffic stellt dieses Programm für den User eine wesentliche Arbeitserleichterung dar, da er die Mails nicht selbst überprüfen muss, ob es sich um Spam handelt und spart außerdem wertvolle Bandbreite des Internets, da Spam-Mails nicht zum Client weitergeleitet werden.

3.9.1.1.1 Funktionsweise von Procmail

Bei einer eingehenden Mail wird die Datei `.forward` gelesen und die Nachrichten z.B. an eine vordefinierte Adresse weitergeleitet (Autoforward) oder an ein Programm zur Weiterbearbeitung der Nachricht übergeben (zB. `procmail` oder `vacation`).
Existiert keine `.forward`-Datei werden die Nachrichten standardmäßig in der Inbox des Benutzers abgelegt.
Alle `.forward`-Einstellungen wie `procmail`, `vacation` oder ein `autoforward` können bequem über das Mailmenü unter "Erweiterte Funktionen" aktiviert, konfiguriert und auch wieder deaktiviert werden.

Recipes

Ein Recipe (Rezept) definiert eine Bedingung (Text im Feld Empfänger, Subject oder Absender) und eine Aktion (Weiterleiten, Löschen etc.), welche ausgeführt wird, wenn die Bedingung erfüllt ist. Wenn die Bedingung eines Recipes „Wahr“ ergibt, werden die nachfolgenden Recipes ignoriert und das entsprechende Mail mit diesen Recipes nicht mehr überprüft.
Recipes müssen exakt geschrieben werden, da auch nur ein syntaktisch fehlerhaftes Recipe zu unerwünschten Ergebnissen in der Mail-Sortierung führen kann.
Die Aktionszeilen in einem Recipe dürfen empfangene Mails auf keinen Fall wieder an die eigene Adresse weiterleiten, da dadurch ein endloser Mail-Loop entstehen kann.

Funktionsweise eines Recipes

Die einzelnen Recipes in der Datei `.procmailrc` werden durch das Programm `procmail` sequentiell von oben nach unten abgearbeitet. Dabei wird bei jedem Recipe überprüft, ob die Bedingung erfüllt ist.
Ist eine Bedingung „Wahr“, so wird die definierte Aktion ausgeführt und der Durchlauf ist beendet, ansonsten prüft `procmail` das nächste Recipe auf „Wahr/Falsch“. Wenn kein Recipe „Wahr“ ergeben hat, wird die Mail in die INBOX gelegt.
Die einzelnen Recipes beginnen immer mit einer Zeile `:0`, anschließend folgen eine oder mehrere Bedingungszeilen (beginnen immer mit *) und zum Abschluss eine einzelne

Aktionszeile.
Kommentare oder Leerzeilen sollten nicht innerhalb eines Rezeptes stehen.

Festlegen von Regeln für ein Recipe

In der Datei `.procmailrc` wird die Behandlung eingehender Nachrichten verwaltet.

Format eines `procmail-Recipes`: (Bedingung und Aktion)

Eine Regel hat folgenden Aufbau:

```
1. :0 [method]
2. [rule]
3. [action]
```

- 1. Zeile: Beginn des Recipes

0:w → Zeigt den Beginn eines Recipes an (unbedingt erforderlich, da das Recipe ansonsten nicht als solches erkannt wird).
Das Flag „w“ bei den Procmail-Regeln bewirkt, dass Procmail den Returncode von `dmail` auch auswertet und an das Mailempfängerprogramm `dmail` weitergibt. Dieses kann dann den Sender der Nachricht über die gescheiterte Aktion benachrichtigen.
Das Flag sollte deshalb bei Aktionen mit „|DELIVER“ und „|FORMAIL“ verwendet werden, da ansonsten Nachrichten bei Problemen verloren gehen können.

- 2. Zeile: Filter-Bedingung (→ Ergebnis ist Wahr oder Falsch):

In der Filter-Zeile wird definiert, nach welchen Stichwörtern gesucht werden soll.

Beispiele für Regeln:

- `^To: .*HansWurst` → alle Mails an Hans Wurst
- `^From: .*(absender1|absender2|absender3)` → alle Mails von *absender1* oder *absender2* oder *absender3*
- `^From: .*hans.wurst@hanswurst.at` → ein bestimmter Absender
- `^From: .*alijku.ac.at` → alle Mails einer bestimmten Domain, hier z.B. Uni Linz

- `^Subject: *.Gewinn` → alle Mails, die in der Subject-Zeile das Wort „Gewinn“ enthalten

Um genauere Informationen zu den „Regular Expressions“ (Filterbedingungen) zu erhalten, kann man dies durch Eingabe der Befehle „`man egrep`“ und „`man regexp`“ auf der Shell erreichen.

➢ 3. Zeile: auszuführende Aktion (genau eine Zeile)

Die Aktion wird ausgeführt, wenn die voranstehende Filter-Bedingung wahr ist.

Beispiele für Aktionen:

- `! hans.wurst@hanswurst.at` → Weiterleitung an angegebene Adresse
- `! hans.wurst@hanswurst.at,max.wurst@hanswurst.at` → Weiterleitung an mehrere Adressen
- `! $DELIVER +Privat` → Speichern in Ordner Privat
- `/dev/null` → endgültiges Löschen
- .....

3.9.1.1.2 Ausgewählte Aktionen in ProcMail

Die Datei `.procmailrc` muss folgende Zeilen enthalten, um das Verschieben von Nachrichten in bestimmte Ordner zu ermöglichen:

```
DELIVER=/usr/local/sbin/dmail
```

Die Nachrichten werden dann mit

```
| $DELIVER +Folder
```

in den Mailfolder „*Folder*“ abgelegt. Der Folder muss beim Eintreffen der Nachricht bereits existieren. Ansonsten landen die Nachrichten trotzdem in der INBOX.
Wichtig ist weiters, dass die folgenden Zeilen am Ende des Filters stehen:

```
:0 w
*
| $DELIVER +INBOX
```

Diese Anweisung bewirkt, dass alle Mails, die nicht herausgefiltert wurden, in der „Inbox“ abgelegt werden.

Sortierung nach Betreff (Subject)

```
:0 w
* ^Subject:.*Termin
| $DELIVER +Termin
```

Hiermit wird eine Mail, in deren Betreffzeile irgendwo die Zeichenkette „Termin“ vorkommt, im Ordner „Termin“ abgelegt.

Verwerfen von Nachrichten

Möchte man, dass bestimmte Mails gar nicht gespeichert werden, so gibt man als Aktion einfach `/dev/null` an. Durch diese Anweisung werden Mails automatisch und unwiderruflich gelöscht, wenn sie ankommen.

```
:0
* ^Subject:.*Gewinn
/dev/null
```

In diesem Beispiel werden alle eingehenden Mails, bei denen in der Subject-Zeile an irgendeiner Stelle das Wort „Gewinn“ vorkommt, automatisch gelöscht.

Sortierung nach Absender (From-Zeile)

```
:0 w
* ^From:.*HansWurst
| $DELIVER +Privat
```

Hiermit wird eine Mail, die von „Hans Wurst“ (Absendername) kommt, im Ordner „Privat“ abgespeichert.

Sortierung nach Empfänger (To)

```
:0 w
* ^TO.*HansWurst
| $DELIVER +Privat
```

Durch diese Anweisung werden alle Mails, die an „Hans Wurst“ geschickt wurden, im Ordner „Privat“ abgespeichert (TO ist eine Klasse, die für alle möglichen Adressierungsfelder steht (To:, Cc:,Bcc)).

Weiterleiten von Mails an eine Adresse

```
:0
* ^From:.*HansWurst
!Max.Wurst@uni-linz.ac.at
```

Alle Mails, die vom Absender Hans Wurst kommen, werden an die Adresse `max.wurst@uni-linz.ac.at` weitergeleitet. Um eine Kopie auf dem Mail-Server zu behalten, wird folgende Modifikation der ersten Anweisungszeile verwendet:

```
:0 c
* ^From:.*HansWurst
!Max.Wurst@uni-linz.ac.at
```

Weiterleiten von Mails an mehrere Adressen

Möchten man E-Mails an mehrere Empfänger weiterleiten, kann man dies durch ausführen der Aktion

```
:0 w
* ^From:.*HansWurst
! `cat adressen.txt`
```

erreichen. Die Datei „`adressen.txt`“ enthält dabei die Empfängeradressen, wobei in jeder Zeile eine Adresse steht.
Diese Anweisungsmöglichkeit ist insofern problematisch, da sie wiederum für Spamming missbraucht werden kann!

Negative Bedingung für ein Recipe

```
:0
* ! From:.*alijku04.ac.at
| $DELIVER +Extern
```

Bei diesem Beispiel werden alle Mails, die nicht von der Domain `alijku04.ac.at` geschickt werden, in den Ordner „Extern“ verschoben.

Verschiedene Bedingungen für ein Recipe

```
:0 w
* ^Subject:.*Gewinn
|^To:.* alijku04.edvz.uni-linz.ac.at
|^From:.*uibk.ac.at
! $DELIVER +Spam
```

Bei diesem Beispiel werden alle Mails, die das Wort „Gewinn“ in der Subject-Zeile enthalten oder an die Adresse „`alijku04.edvz.uni-linz.ac.at`“ (generelle Adressierung des Mailservers der Johannes Kepler Universität Linz – Hinweis auf Spam) geschickt wurden oder von der Domain „spam.com“ gesendet wurden, in den Ordner „Spam“ verschoben.

Verschiedene Aktionen für eine Mail

Um verschiedene Aktionen auf eine Mail anwenden zu können, besteht die einfachste Möglichkeit darin, die E-Mail zu kopieren und auf die angelegten Kopien anschließend verschiedene Recipes auszuführen:

```
# Weiterleitung an Adresse1
:0 c
* ^From:.*Dagobert
! Adresse1@uibk.ac.at
```

```
# Abspeichern im Ordner Privat
:0 w
* ^From:.*Dagobert
| $DELIVER +Privat
```

Die elegantere und übersichtlichere Methode besteht darin, geschwungene Klammern zu verwenden:

```
:0 w
* ^From:.*Dagobert
{
:0 w
| $DELIVER +Privat
:0
! Adresse1@uibk.ac.at
}
```

Mails von bestimmten Absendern löschen

Dieses Recipe bewirkt, dass alle Mails, welche von in der „rule“-Zeile angegebenen Domains stammen, automatisch gelöscht werden. Diese Funktion ist in ProcMail äußerst wichtig, um dieses Programm sinnvoll zur Bekämpfung von Spam einzusetzen.

```
:0
* ^From:.*@(spam.com|spamworld.de|spammer.at)
/dev/null
```

Textkörper durchsuchen

ProcMail durchsucht standardmäßig lediglich den Header der Mail-Nachrichten. Um auch den Textkörper zu durchsuchen, kann auch ein Recipe verwendet werden, welches jedoch folgendes Aussehen haben muss:

```
:0 bw
* ^.*Gewinn
| $DELIVER +Spam
```

Nun werden alle Mails, die den Begriff „Gewinn“ enthalten in den Ordner „Spam“ verschoben.
Auch diese Funktion ist, so wie die vorher beschriebene, sehr wichtig, um mittels Procmail Spam wirkungsvoll zu bekämpfen.

3.9.1.2 Sendmail

Mailprogramme wie das im Internet weit verbreitete „S*endmail“* für UNIX-Rechner bieten in ihren aktuellen Versionen zahlreiche Optionen, um die Behandlung von Spam-Mails deutlich zu vereinfachen. Am Beispiel von „*Sendmail“* ist es jedoch wichtig, in jedem Fall die aktuellste Versionen (> 8.8.x) einzusetzen, da ältere Implementierungen noch nicht über diese zusätzlichen Funktionen verfügen. Idealerweise sollte gleich die derzeit aktuellste „*Sendmail“*-Version (8.9.3 – Stand 24.11. 1999) installiert werden, die von ihren Autoren auch als "The Spam Control Release" bezeichnet wird. Bei dieser Version ist das "Mail relaying" standardmäßig abgeschaltet, ferner enthält „*Sendmail“* 8.9.3 zahlreiche weitere Optionen zur Kontrolle der E-Mail-Header auf Korrektheit. So können beispielsweise ungültige E-Mail-Adressen oder nicht-existente Domainnamen automatisch zurückgewiesen werden.
Bereits ab „*Sendmail“* 8.8 wurden einige neue Regeln eingeführt, die es erlauben, die Annahme von E-Mails aufgrund der Absenderadresse zu verweigern. Dabei kann nach Host- oder Domainnamen, aber auch nach einzelnen E-Mail-Adressen gefiltert werden. Kommen von bestimmten Adressen immer wieder Spam-Mails an, werden diese in eine sogenannte "Schwarze Liste" eingetragen, die von „*sendmail“* bei jeder hereinkommenden Nachricht geprüft wird. Findet „*sendmail“* einen Absender in dieser Liste, wird die E-Mail nicht angenommen; der Absender erhält stattdessen eine frei konfigurierbare Fehlermeldung.
Der Nachteil von derartigen schwarzen Listen besteht jedoch in der Tatsache, dass mit dem Eintrag einer Domain in die Liste alle E-Mails dieser Domain blockiert werden. Auch seriöse E-Mails können dann nicht mehr empfangen werden. Man sollte daher beim Sperren kompletter Domains sehr vorsichtig sein.
Einen Schritt weiter geht „*sendmail“* 8.9 mit der "Realtime Blackhole List". Diese Liste enthält eine große Anzahl an IP-Adressen, von denen bekannt ist, dass in der Vergangenheit Spam-Mails versendet wurden, bzw. die als Mail-Relay missbraucht wurden. „*Sendmail“* kann nun so konfiguriert werden, dass vor der Annahme einer E-Mail online geprüft wird, ob

die IP-Adresse des absendenden Mailhosts in dieser Liste geführt wird. Falls dies der Fall ist, wird die Annahme der Nachricht verweigert.
Auch andere Mailprogramme verfügen teilweise über ähnliche Funktionalitäten zur Abwehr von Spam-Mails bzw. Mail-Relaying. So hat beispielsweise *Procmail* (siehe Kapitel 3.9.1.1) diverse Filter-Optionen, die insbesondere im gemeinsamen Einsatz mit *„sendmail“* zum Tragen kommen.

3.9.1.3 NoCeM-on-spool

Nach neuesten Schätzungen von Fachleuten sind 40% aller News-Artikel Spam, weitere 40% SPAM-Cancels (um die Spam-Artikel wieder zu löschen) und nur 20% der Postings inhaltlich relevante Artikel.
Um diese Flut von inhaltlich nicht passenden Postings zu stoppen, ist auf vielen Newsserver „NoCem-on-spool“ installiert. Dieses Programm basiert auf „*NoCem*“ und entfernt alle Artikel die von einer Liste vertrauenswürdiger Personen nach objektiven Kriterien als Spam eingestuft werden, noch bevor sie überhaupt den News-Server erreichen. Es handelt sich demzufolge bei „NoCem-on-spool“ um eine Form des Fremdcancelns (siehe Kapitel 3.8.2). Es können mit diesem Verfahren mehrere Anweisungen auf einmal gelöscht werden und es ist im Gegensatz zu älteren Cancel-Anweisungen PGP-authentisiert.

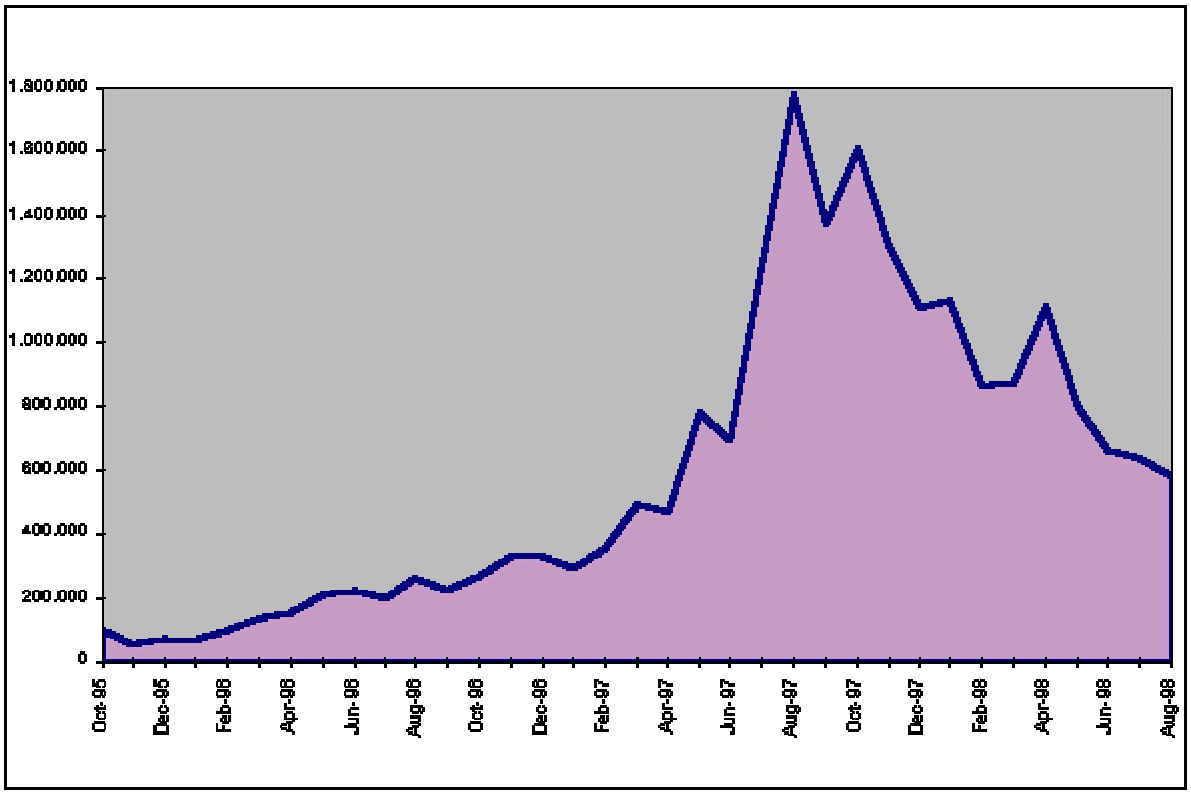


Abbildung 9: Reduktion von nicht relevanten Postings durch den Einsatz von „*NoCem-on-spool*“ (entnommen aus http://www.nocem.org)

Funktionsweise

Der Absender eines Postings hängt an dieses eine entsprechende *NoCeM*-Notiz an. Diese Notiz ist ein einfaches Posting an „`alt.nocem.misc`“ in einem speziellen Format. Diese Notizen sind mit dem PGP-Key desjenigen der das Posting veröffentlicht hat signiert.
Die Leser von Newsgroups können nun entscheiden, von welchen PGP-Keys sie Postings akzeptieren.
Der *NoCeM*-Client liest „`alt.nocem.misc`“ und findet die entsprechenden *NoCeM*-Notizen, in denen festgehalten ist, von welchen PGP-Keys der User Postings akzeptiert. Es wird in weiterer Folge der Newsreader instruiert, Nachrichten welche nicht akzeptiert werden, als gelesen zu markieren, so dass sie dem User nicht angezeigt werden.

NoCeM PGP-Key

```
Type Bits/KeyID    Date       User ID
pub  1024/FEAF0949 1999/01/18 M. B.

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i
```

```
mQCNAzajaAUAAAEEALLEmbrYbJNxXzok3w+56HlqXolc5DzPxHTjHP1bkN8HPU
pNKE6mn/Kawk15GQb0kGirX5+42XJjGqLXsodeYPRC23jd7G/0CtTnefVmPOZD
cl5tffW14quBZOKZxh6rNrgeo9ZY/4DwY6LB9pbmwp7lZ4ZGdxpaqJ/DyVb+rw
lJAAURtB5NYXJrIEJ1cmtsZXkgPG1idXJrbGV5QGlvbC5pZT6JAJUDBRA2o2gF
n8PJVv6vCUkBAfRPA/9sw2aej4GBo/Ube/hvYDHSDsc1ONlDv8XhcnwTk0i2v9
Sz9LQ7kxLE4hScEMGdm+vN0A+rwYUwanm+09pYVYCkXfQvolD7trC8TwtBeYdD
3FXZ9kLbn8HTzRgQ14AKCbiNM28smJw0jmmKXDVlpQTbYQ7D4j3L5zqucWfXCz
wG5Q===2DvN
-----END PGP PUBLIC KEY BLOCK-----
```

3.9.2 Clientseitig

Clientseitige Filter sind Filterprogramme die direkt am PC des Users installiert werden. Es wird hier unterschieden zwischen Programmen, welche sich mit der Mailbox auf dem Mailserver des Providers verbinden und die darin enthaltenen E-Mails überprüfen und erst nach positiver Prüfung auf den Client laden (z.B. „*SpamEater Pro*“) und Programmen, welche nur den Mail-Header laden und überprüfen (z.B. „ *E-Mail Remover*“ oder „*SpamBuster*“) sowie Programmen, welche die erhaltenen E-Mails zuerst auf den Client laden und erst dann überprüfen . Diese Methode hat jedoch den Nachteil, dass dadurch wieder Bandbreite des Internets und Online-Ressourcen verschwendet werden. Ein Beispiel für einen clientseitigen, in ein Mailprogramm integrierten Filter wäre der Filter im „ *Netscape Communicator 4.5*“

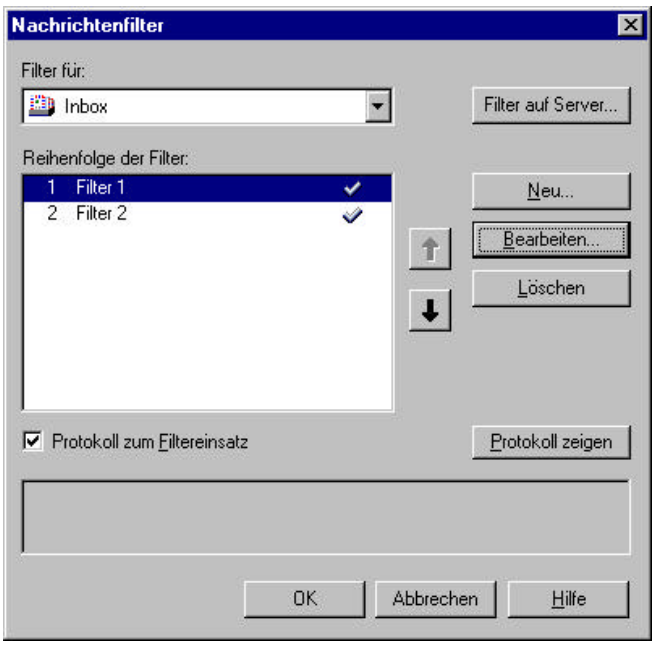


Abbildung 10: Filter in Netscape Messenger 4.5

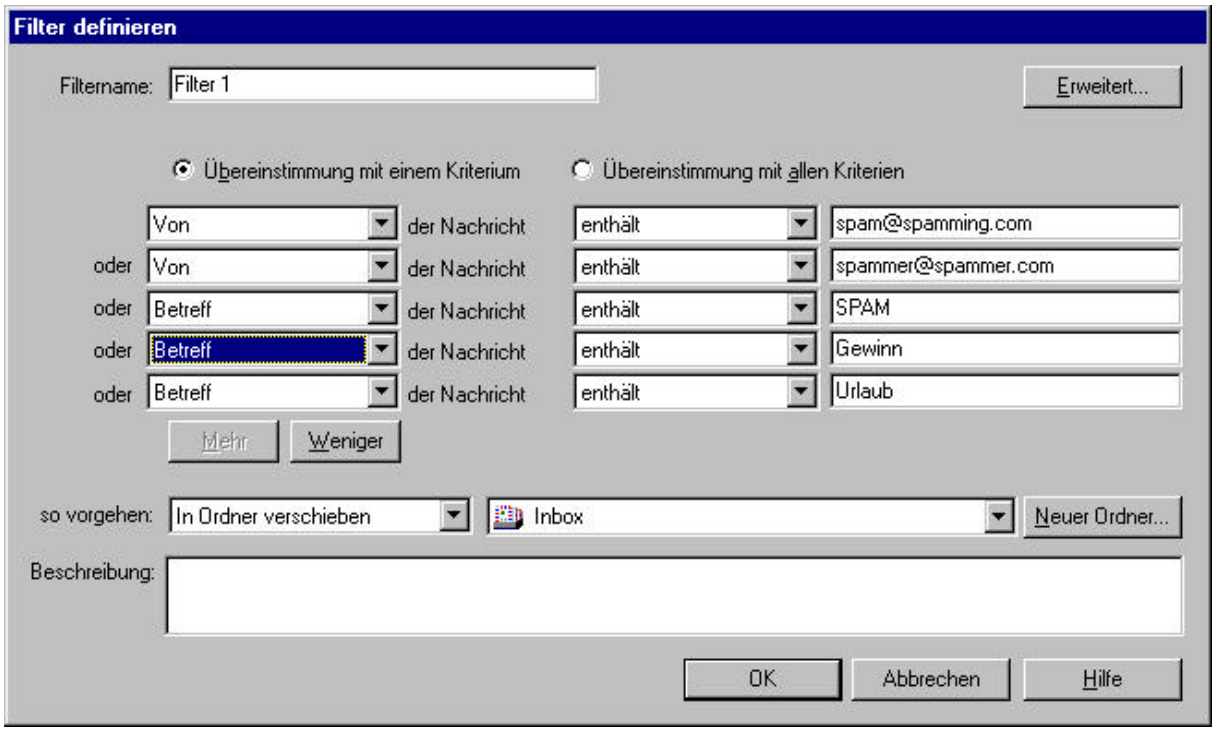


Abbildung 11: Filtereinstellungen in Netscape Messenger 4.5

Beim Netscape Messenger 4.5 besteht die Möglichkeit, mehrere benutzerdefinierte Filter einzustellen. Diese Filter können jeweils aus 5 Kriterien bestehen, nach denen gefiltert werden soll. Diese Filterkriterien können sich auf "Betreff, Von, Text, Datum, Priorität, Status, An, CC, An oder CC, Alter in Tagen" beziehen. Es kann für jedes dieser Kriterien eine Vergleichsoperation mit den Operatoren "enthält, enthält nicht, ist, ist nicht, beginnt mit, endet mit" auf einen frei wählbaren Text definiert werden.
Wird aufgrund dieser Filterkriterien eine Nachricht identifiziert, stehen folgende Möglichkeiten zur Verfügung: "In Ordner verschieben (es kann ein beliebiger Ordner definiert werden), Priorität ändern, Löschen, Als gelesen markieren, Thread ignorieren, Thread beobachten".

3.10 Rechtliche Situation

Da das Internet ein internationales Medium ist, ist die Rechtslage bezüglich Spamming noch sehr unklar. Oft ist nicht einmal im nationalen Recht die Rechtslage eindeutig geklärt. Generell ist jedoch anzumerken, dass bei bestehenden Geschäftsbeziehungen der Versand von Werbe-E-Mails zulässig ist.

3.10.1 Spamming per E-Mail

Die Meinung über die Rechtslage bei Werbung per E-Mail ist geteilt. Die Rechtsprechung hat sich in mehreren Entscheidungen inzwischen eindeutig auf den Standpunkt gestellt, dass unaufgefordert zugesandte Werbung per E-Mail unzulässig ist (vgl. LG Traunstein, MMR 1998, 53; LG Berlin, CR 1998, 499; LG Berlin, MMR 1998, 491).

Nach Rechtsprechung des dBGH ist eine Werbeart immer dann schon als unlauter zu beurteilen, d.h. sie verstößt gegen § 1 UWG, wenn sie den Keim zu einem immer weiteren Umgreifen in sich trägt und damit zu einer untragbaren Belästigung und zu einer Verwilderung der Wettbewerbssitten führt. Die Belästigung hat der BGH schon sehr früh für Werbung über Mitteilungen im BTX-System als gegeben angesehen, da das Sortieren der für den Nutzer interessanten und uninteressanten Nachrichten sehr zeitaufwendig sein kann.

Da Werbung per E-Mail so gut wie nichts kostet, besteht die Gefahr, dass diese Art der Werbung eine so starke Verbreitung findet, dass der Nutzer untragbar belästigt wird. Für einen Werbetreibenden, der einmal eine Empfängerliste zusammengestellt hat, ist es ein leichtes, eine Mail gleich an mehrere Tausend Empfänger zu schicken. Gleichzeitig kann er aufgrund der geringen Kosten auch in sehr kurzen Abständen Mails versenden.

Die wettbewerbsrechtliche Unzulässigkeit von E-Mail-Werbung mag für einen werbenden Unternehmer zwar ärgerlich sein. Der werbenden Wirtschaft ist letztlich auch nicht damit gedient, wenn die E-Mail-Accounts der Kunden vor Werbung überquellen und eine

Individualkommunikation über E-Mail stark erschwert wird.

Der Adressat von Werbe-Mails muss sich also mit der Zusendung von Werbung per E-Mail einverstanden erklärt haben. Eine Aufforderung zur Zusendung von Werbung wird man jedoch nicht darin sehen können, dass der Adressat auf einer Postkarte für ein Gewinnspiel oder auf einem Formular auf einer Web-Site für eine Support-Anfrage o.ä. seine E-Mail-Adresse verraten hat. Ebenso kann nicht davon ausgegangen werden, dass ein Teilnehmer einer Newsgroup damit einverstanden ist, unter seiner in der Newsgroup verwendeten E-Mail-Adresse Werbung zu empfangen, selbst wenn die Werbung inhaltlich zum Thema der Newsgroup passt. Die Angabe einer E-Mail-Adresse dient schließlich nur dazu, eine individuelle Diskussion zu Themen zu eröffnen, die nicht öffentlich diskutiert werden sollten.

Wer Werbung per E-Mail versenden will, muss also darauf achten, dass der Adressat sich ausdrücklich und eindeutig damit einverstanden erklärt, Werbung über diese E-Mail-Adresse zu empfangen. Es ist jedoch auch unzulässig, Werbung zunächst unaufgefordert zuzusenden mit dem Hinweis, dass der Adressat die Werbung mit einer einzigen Reply-Mail abbestellen kann.

Bei beabsichtigter Werbung per E-Mail sollte man sich vorher mit den AGB seines Providers vertraut machen. Viele Provider verbieten nämlich vertraglich den Versand von Werbe- oder Massenmailings. [WALDNER]

Zulässig kann Werbung per E-Mail aber ausnahmsweise sein, wenn der Adressat mit dem Erhalt von E-Mail-Werbeschreiben ausdrücklich oder konkludent einverstanden ist, oder sein Einverständnis zum Empfang vom Absender anhand konkreter Umstände vermutet werden kann.
Hierfür genügt aber nicht, dass sich der Empfänger z.B. in Newsgroups oder Diskussionsforen unter Angabe seiner E-Mailanschrift zu Wort gemeldet hat. Entgegen von einer von Spammern in Anspruch genommenen Rechtfertigung kann man nämlich nicht davon ausgehen, dass die nicht anonyme Teilnahme an einer Newsgroup ein Interesse des Betreffenden an Werbung begründen würde. [RUHLAND 97]

Während in der EU Bemühungen unternommen werden, um E-Mail-Werbung im EU-Raum zu erleichtern, wird in Österreich auf gemeinsamen Antrag aller Parlamentsparteien das Telekommunikationsgesetz novelliert, indem ein mit Strafe versehenes Verbot unbestellter Werbung per elektronischer Post eingefügt wird.

Der Justizausschuss hat folgende Änderungen beschlossen:

1.) §101 wird folgender Satz angefügt:

„Die Zusendung einer elektronischen Post als Massensendung oder zu Werbezwecken bedarf der vorherigen – jederzeit widerruflichen – Zustimmung des Empfängers.“

2.) §104 abs.3 Z.22 wird wie folgt abgeändert:

„entgegen dem §101 unerbetener Anrufe oder Zusendungen einer elektronischen Post als Massensendung oder zu Werbezwecken tätigt“.

d.h. Verwaltungsstrafe bis öS 50.000

Mit dieser Gesetzesänderung wird der gesamte deutschsprachige EU-Raum zur spamfreien Zone. In der Schweiz war zum Zeitpunkt der Erstellung der Arbeit keine entsprechende Gesetzesregelung ausgearbeitet.

3.10.2 Spamming in Newsgroups

Die Frage, ob es wettbewerbswidrig ist, Werbung in einer Newsgroup zu posten, ist in Deutschland noch nicht gerichtlich entschieden worden. Die Rechtsprechung zu Werbung per E-Mail lässt sich aber weitgehend auf Werbung per Newsgroups übertragen.
Der Dienst Newsgroups dient zur Diskussion bestimmter Themen innerhalb interessierter Gruppen. In den meisten Newsgroups sind die Teilnehmer an den individuellen Meinungen, Erfahrungen und Ratschlägen anderer Personen interessiert. Werbepostings tragen zu einem

solchen Meinungs- und Erfahrungsaustausch meist nichts bei sondern erhöhen nur den vom Teilnehmer zu sichtenden Datenwulst. Da die Postings fast nichts kosten, besteht die Gefahr, dass in Newsgroups mehr und mehr Werbepostings die eigentlich interessanten individuellen Postings überlagern und die Newsgroup so für die Teilnehmer wertlos wird.

Zu berücksichtigen ist freilich immer der Charakter einer Newsgroup. Werbung, die zum Thema der Newsgoup passt und die in sachlicher Form präsentiert wird, mag im Einzelfall wettbewerbsrechtlich zulässig sein. Z.B. mag in einer Newsgroup, in der Veranstaltungen in einer bestimmten Region angekündigt werden sollen, ein Werbeposting einer Disko der Region zu einem bestimmten Eventabend tolerabel sein und verstößt nicht gegen § 1 dUWG. Ebenso akzeptabel ist eine Werbe-E-Mail als Antwort auf eine konkrete Anfrage - wie dies oft über Anfrageseiten auf Web-Sites geschieht - eines Interessenten.

Stets als wettbewerbswidrig dürften jedoch Werbepostings einzustufen sein, die eindeutig off topic sind. Ebenfalls wettbewerbswidrig sind mehrfache Werbepostings mit demselben Inhalt unter einer anderen Subject-Zeile. Ein solches Verhalten trägt ganz besonders die Gefahr einer Verwilderung der Wettbewerbssitten in sich. Der erste Werbetreibende postet seine Message dreimal. Der nächste tut selbiges gleich vierunzwanzigmal. Letztlich könnte ganz schnell ein Wettbewerb darum entstehen, wer mehr Postings in der Newsgroup platziert. Die Newsgroup wäre ganz schnell für ihre Teilnehmer wertlos.

Eine richtungsweisende Entscheidung der Gerichte steht zwar noch aus, es ist jedoch vermutlich nur eine Frage der Zeit, bis Werbung in Newsgroups auch ausdrücklich durch die Rechtsprechung als rechtswidrig eingestuft wird.

3.10.3 Mailbombs

Mailbombing ist eine Methode, Spam und andere unerwünschte Verhaltensweisen im Internet zu ahnden. An den Mail-Account des Urhebers von unerwünschten Postings werden so viele Mail versandt, dass dieser Mail-Account faktisch unbrauchbar wird. Sofern der vom Provider für die Speicherung von Mails zur Verfügung gestellt Speicherplatz überschritten wird, kann es zum Verlust von Nachrichten führen.

Mailbombing kann daher den Straftatbestand der Datenveränderung nach § 303a dStGB in der Form der Unterdrückung von Daten erfüllen. Ein Unterdrücken von Daten ist dann gegeben,
wenn die Daten dem Zugriff durch den Berechtigten auf Dauer oder zeitweilig entzogen werden und er sie deshalb nicht mehr verwenden kann. Wird ein Mail-Account zum Überlaufen gebracht, so werden dem Inhaber die per E-Mails übersandten Daten entzogen, die der Provider entweder löscht oder nicht speichert. Sofern der E-Mail-Anschluss für einen Betrieb, ein Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, kommt sogar eine Computersabotage nach § 303b dStGB in Betracht.

Die genannten Tatbestände sind nur dann erfüllt, wenn der mutmaßliche Täter vorsätzlich handelt. Er muss also das Unterdrücken der E-Mails bewusst und gewollt herbeiführen. Es reicht aus, wenn er einen Datenverlust durch seine Handlungen billigend in Kauf nimmt, also ernsthaft damit rechnet. Vorsatz wird regelmäßig dann nicht vorliegen, wenn es zwar zu einem Datenverlust kommt, dieser aber durch eine Vielzahl kleiner Mails von unterschiedlichen Personen verursacht wird, es sei denn, diese Personen wirken bewusst und gewollt zusammen.
Wer also in einer Newsgroup Spam postet wird nicht durch die §§ 303a, 303b dStGB davor geschützt, dass ihm u.U. hunderte von Newsgroup-Teilnehmern erboste E-Mails schicken, die in ihrer Summe zu einer Verstopfung des Mail-Accounts und damit zu einem Datenverlust führen.

Sofern ein rechtswidriges Mailbombing vorliegt, hat das Opfer dieser Aktion auch zivilrechtliche Unterlassungs- und Schadensersatzansprüche gegen die Schädiger. Eine beliebte Racheaktion ist auch, große E-Mails zu senden, welche ebenso die Bandbreite belasten sowie den Zwischenrechner und den Mail-Account des Opfers füllen. Diese Vorgehensweise ist ebenso strafbar.

3.10.4 Beleidigung und Verleumdung

3.10.4.1 Deutschland

Wenn ein Streit eskaliert und zu härteren verbalen Bandagen gegriffen wird, kann es schnell passieren, dass sich die eine oder die andere Seite in ihrer Ehre verletzt sieht.

Durch eine Reihe von Straftatbeständen wird die Ehre von Personen oder Personengruppen geschützt. Die zentralen Vorschriften sind im dStGB:

§ 185 Beleidigung
§ 186 Üble Nachrede
§ 187 Verleumdung

Eine Beleidigung ist ein Angriff auf die Ehre eines anderen durch eine Kundgabe der Missachtung oder Nichtachtung. Wann eine solche Ehrverletzung vorliegt, kann nur im Einzelfall entschieden werden. Generell gilt dabei, dass derjenige, der kräftig austeilt, auch kräftiger einstecken können muss.

Behauptet jemand eine ehrverletzende Tatsache über einen anderen, so kann eine üble Nachrede vorliegen, wenn die Tatsache nicht erweislich wahr ist. Bei der Behauptung einer nachweislich wahren Tatsache liegt zwar keine üble Nachrede mehr vor, die Art und Weise der Behauptung oder die Umstände können jedoch dazu führen, dass eine Beleidigung gegeben ist. Eine Verleumdung liegt dann vor, wenn jemand wissentlich eine unwahre ehrenrührige Tatsache über einen anderen behauptet.

Bei Behauptungen in E-Mail oder News über andere Personen ist daher immer zu überlegen, ob sich diese andere Person in ihrer Ehre gekränkt fühlen kann. Falls ja, ist zu überlegen, ob die Behauptung Missachtung oder Nichtachtung ausdrückt. In einem sachlich geführten fachlichen Diskurs kann sich daher zwar einer der Diskussionspartner in seiner Ehre gekränkt

fühlen, wenn der andere seine Meinung für falsch hält. Sofern der andere Diskussionspartner jedoch nicht seine Missachtung oder Nichtachtung ausdrückt, begeht er dabei schwerlich eine Beleidigung. Eine Beleidigung kommt jedoch dann in Betracht, wenn der Diskurs die sachliche Ebene verlässt und sich auf der persönlichen Ebene fortsetzt.

Auch sachliche Behauptungen können jedoch eine üble Nachrede oder Verleumdung darstellen. Das ist z.B. dann der Fall, wenn eine sachliche Behauptung gleichzeitig die fachliche Kompetenz einer anderen Person in Frage stellt. Bei sachlichen Behauptungen, die jemand anderen in seiner Ehre verletzen könnten, ist daher darauf zu achten, dass diese den Tatsachen entsprechen. Eine Strafbarkeit wegen übler Nachrede entfällt, wenn eine behauptete Tatsache nachweislich wahr ist. Kann der Richter also nicht mehr herausfinden, ob die Tatsache wahr oder falsch war, wird er den Täter verurteilen. Bei Tatsachenbehauptungen, die das Ansehen einer anderen Person beeinträchtigen könnten, muss also besonders sorgfältig recherchiert werden.

Anzumerken ist noch, dass der Geschädigte wegen einer Beleidigung, übler Nachrede oder Verleumdung Schadensersatz- und Unterlassungsansprüche geltend machen kann.

3.10.4.2 Österreich

Im österreichischen Recht werden Beleidigung in § 115 StGB und Üble Nachrede in § 111 StGB geregelt. Verleumdung existiert nicht als eigener Paragraph, da sie in Übler Nachrede enthalten ist.

Unter Beleidigung wird in Österreich die Demütigung oder Kränkung einer Person vor anderen verstanden. Um den Tatbestand der Beleidigung zu erfüllen bedarf es eines Täters, eines Opfers und 3 Personen die diese Beleidigung tatsächlich wahrgenommen haben.
Auf das Internet umgelegt bedeutet das, dass Beleidigungen am häufigsten in Newsgroups verbreitet sind, da die hier veröffentlichten Postings allen Teilnehmern der Newsgroup frei zugänglich sind. Im E-Mail-Verkehr kann dieser Tatbestand nur erfüllt werden, wenn eine E-Mail mit beleidigendem Inhalt an mindestens 3 weitere E-Mail-Adressen außer dem ursprünglichen Adressaten (beleidigte Person) weitergeleitet wird.

Unter Übler Nachrede wird die ehrenrührige Zuschreibung von Charakter- oder Verhaltensmängel verstanden. Der Tatbestand von Übler Nachrede ist dann erfüllt, wenn die Möglichkeit besteht, dass ein Dritter diese wahrnehmen kann, sie aber nicht unbedingt wahrgenommen haben muss.
Wird eine E-Mail mit Inhalten über ehrenrührigen Charakter- oder Verhaltensmängel nicht nur an das Opfer, sondern auch an einen Dritten weitergeleitet, ist dieser Tatbestand im E-Mail-Verkehr erfüllt, auch wenn der Dritte diese E-Mail nicht gelesen hat. Wird ein Artikel mit solchen Inhalten in einer Newsgroup gepostet, ist dieser Tatbestand immer gegeben.
Wird eine E-Mail mit solchen Inhalten lediglich an das Opfer gesendet, handelt es sich nicht um Üble Nachrede sondern um Ehrenkränkung, was nach Landesrecht geregelt ist und Verwaltungsstrafen nach sich ziehen kann.

3.10.5 Gefälschte E-Mails oder Postings

Besonders übel kann einem Kommunikationspartner mit gefälschten E-Mails oder News-Postings mitgespielt werden. Das Vorgehen ist dabei meist sehr einfach und plump. Der Täter trägt in sein E-Mail- oder News-Programm lediglich den Namen und die E-Mail-Adresse einer anderen Person als Absender ein. Derartige plumpe Fälschungen sind leicht zu entlarven, da der Mail-Header der gefälschten Mails mit dem Header der tatsächlich vom Opfer stammenden Mails in der Regel nicht übereinstimmt. Der nichtsahnende Leser, der normalerweise aber keine Fälschung vermuten wird, wird durch derartige Mails oder Postings tatsächlich getäuscht. Gefälschte E-Mails oder Postings sind juristisch sehr schwierig zu handhaben.

3.10.5.1 Deutschland

Verleumdung
Zunächst kann durch ein gefälschtes Posting der Straftatbestand der Verleumdung erfüllt werden.
Durch das Absenden des gefälschten Postings wird die unwahre Tatsache verbreitet, der vermeintliche Absender hätte dieses Posting geschrieben. Wenn das Ansehen des vermeintlichen Absenders dadurch Schaden nehmen kann, dass andere Leute meinen, das Posting sei von ihm, so ist der Tatbestand der Verleumdung erfüllt. Handelt es sich um ein

Posting in einer Newsgroup, so ist die Tat öffentlich begangen. Es gilt dann der nach § 187 dStGB verschärfte Strafrahmen, der Freiheitsstrafe von bis zu fünf Jahren vorsieht.

Verletzung des Namensrechtes

Gleichzeitig stehen dem Verletzten eine ganze Reihe zivilrechtlicher Ansprüche gegen den Fälscher auf Unterlassung und Schadensersatz zu. Zunächst ist das Namensrecht aus § 12 dBGB verletzt. Nur der Namensträger ist zur Führung seines Namens berechtigt. Schadensersatzansprüche ergeben sich aus § 823 f. dBGB.

Urkundenfälschung

Man könnte auf die Idee kommen, in der Fälschung einer Mail eine Urkundenfälschung zu sehen.

Regelmäßig dürfte eine Urkundenfälschung jedoch nicht vorliegen, da diese mit dem Begriff der Urkunde zusammenhängt. Eine Urkunde ist eine verkörperte Gedankenerklärung, die im Rechtsverkehr zum Beweis geeignet und bestimmt ist und den Aussteller erkennen lässt. E-Mails und Postings sind zweifellos Gedankenerklärungen, die - so sie nicht anonym erfolgen - auch den Aussteller erkennen lassen. Man kann jedoch schon darüber streiten, ob E-Mails und News-Postings verkörpert sind. Es reicht dazu nicht aus, dass man eine Mail ausdrucken kann. Druckt der Empfänger eine Mail aus, so erfolgt diese Verkörperung der Mail nicht durch den Aussteller.

Mails und Postings werden jedoch auf einen Datenspeicher beim Provider und auch beim Empfänger gebannt, so dass man u.U. eine Verkörperung begründen kann. (Näher liegt jedoch eine Fälschung beweiserheblicher Daten nach § 269 I dStGB.)

Die meisten Mails und Postings sind jedoch nicht zum Beweis im Rechtsverkehr bestimmt. In der Regel wird über Mail und Postings ein Gedankenaustausch gepflegt. Etwas anderes mag gelten für eine Bestellung bei einem Internet-Shop. Bei einer Bestellung unter falschem Namen mag man über eine Urkundenfälschung und vor allem über eine Fälschung beweis-erheblicher Daten nachdenken können.

Falsche Verdächtigung

Erfüllt ein gefälschtes Posting in einer Newsgroup zusätzlich einen Straftatbestand, so kann sich der Fälscher gleichzeitig wegen einer falschen Verdächtigung nach § 164 II dStGB

strafbar gemacht haben. Nach dieser Vorschrift macht sich derjenige strafbar, der öffentlich über einen anderen wider besseres Wissens eine Behauptung aufstellt, die dazu geeignet ist, gegen diesen anderen ein behördliches Verfahren einzuleiten.

3.10.5.2 Österreich

Urkundenfälschung

Schriftliche Urkunden sind in Österreich Dokumente welche mit freiem Auge lesbar und dauerhaft festgehalten sind.

In Österreich gelten elektronische Daten nie als Urkunden, egal wo und wie dauerhaft sie gespeichert sind. Auch wenn E-Mails oder Newsgroup-Postings mittels elektronischer Signatur unterzeichnet sind gelten sie nicht als Urkunde. Urkundendelikte im Internet sind in Österreich daher nicht möglich.

Wird eine E-Mail vom Autor ausgedruckt, anschließend unterzeichnet und auf dem Postweg an den Empfänger gesendet, handelt es sich wiederum um ein Schriftstück und kann die Merkmale einer Urkunde erfüllen. Das Ausdrucken eines E-Mails durch den Empfänger reicht nicht aus, da in diesem Fall die Unterschrift des Absenders fehlt.

Mails und Postings sind zwar keine Urkunden, können jedoch als Beweismittel verwendet werden.

3.11 Gerichtsbeschlüsse

Landgericht Traunstein

Beschluß

Az: 2HK O 3755/97
18. Dezember 1997

In Sachen

(...)

gegen

Internetagentur (...)

wegen einstweiliger Verfügung

Der Antragsgegnerin wird Prozeßkostenhilfe versagt.

Gründe

I.

Die Antragstellerin, die Serviceleistungen rund um die EDV anbietet, will der Antragsgegnerin, die eben solche Leistungen anbietet und einen Anzeigenservice für das Internet betreibt, im Wege der einstweiligen Verfügung verbieten lassen, Werbung an Privatleute über e-mail ohne vorherige Zustimmung zu versenden. Die Antragsgegnerin hatte unverlangt an einen privaten Anschluß ein kurzes e-mail versandt, in dem sie für ihren Anzeigenservice warb. Das Landgericht hat ihr solche Versendungen durch einstweilige Verfügung ohne mündliche Verhandlung verboten. Die Antragsgegnerin beabsichtigt, hiergegen Widerspruch einzuleben und beantragt, ihr zur Rechtsverteidigung Prozeßkostenhilfe zu bewilligen. Der Antrag war abzulehnen, weil der Rechtsverteidigung die hinreichende Erfolgsaussicht fehlt (§ 114 ZPO).

II.

Die Antragstellerin ist gemäß § 13 Abs. 2 Nr. 1 UWG zur Geltendmachung des Unterlassungs-Anspruchs berechtigt, weil sie gewerbliche Leistungen gleicher oder verwandter Art anbietet wie die Antragsgegnerin. Wiederholungsgefahr ist gegeben, weil sich die Antragsgegnerin nicht zur Änderung ihres Verhaltens verpflichtet. Gemäß §§ 25 UWG, 935 ZPO kann die Antragstellerin Unterlassungsansprüche aus § 1 UWG mit Hilfe einer einstweiligen Verfügung durchsetzen.

III.

Die unverlangte Versendung von Werbung an private e-mail-Anschlüsse ist wettbewerbswidrig (§ 1 UWG).

Soweit ersichtlich, fehlt Rechtsprechung zur Wettbewerbswidrigkeit von e-mail-Werbung. Die juristische Literatur teilt überwiegend die vorstehende Rechtsauffassung (s. Ernst NJW CoR 97, 494). Ob ein gegen die guten Sitten des lauteren Wettbewerbs verstoßendes Verhalten (§ 1 UWG) vorliegt, ist unter Berücksichtigung der Rechtsprechung zur Werbung in vergleichbaren Medien zu beurteilen, das ist Briefkasten-, Telefon-, Telex-, Teletex-, Telefax- und BTX-Werbung (s. dazu die Übersichten bei Baumbach-Hefermehl Wettbewerbsrecht 19. Aufl., Rn. 67-71 c zu § 1 UWG, Reichelsdorfer-GRUR 97, 191, Schrey-Westerwelle, Supplement Kommunikation und Recht S. 17, Beilage zu Betriebsberater, Heft 43, 1997).

1. Briefkastenwerbung ist grundsätzlich zulässig, weil weite Bevölkerungskreise ein Interesse an informativer Werbung haben (BGH GRUR 73, 552). Ob das auch bei Tarnung als Privatbrief heute noch gelten kann, erscheint zweifelhaft, nachdem die Werbeflut in allen Medien erheblich zugenommen hat, Adressaten sich zunehmend gegen Werbung zur Wehr setzen und die technischen Möglichkeiten der Tarnung zugenommen haben.Durch e-mail-Werbung ist jedoch eine weitaus größere Belästigung zu erwarten als durch Briefkasten-werbung, weil e-mail unvergleichlich billiger, schneller, arbeitssparender und gezielter an eine Vielzahl von Adressaten verschickt werden kann und überdies stärker in den Betriebs-ablauf eindringt bzw. auf den Schreibtisch vordringt. Die begrenzte Zahl von e-mail-usern, deren erwartete wirtschaftliche Potenz und die leichte und preiswerte Verschickungs-möglichkeit lassen ein weiteres Anschwellen der Werbeflut erwarten. Dass die Antrags-gegnerin ihre Adressaten - wie sie behauptet - gewissermaßen per Hand auswählt, prüft, ob sie in der Robinsonliste von T-online enthalten sind, ihre Zahl gering hält und dass sie durch die Absenderbezeichnung "Anzeigenboerse.com" als gewerbliche Versenderin erkennbar ist, ändert daran nichts. Es ist nämlich ein Sogeffekt nachahmender Konkurrenten zu erwarten, welche sich an solche Beschränkungen nicht halten. Auch wenn erkennbar ist, dass die Sendung von einem kommerziellen Versender stammt, entbindet dies den Empfänger nicht von der Mühe zu prüfen, ob die Sendung für ihn von Interesse ist.
Ob es sich um Werbung oder anderes handelt, läßt sich ohne Studium des Inhalts regelmäßig nicht sicher beurteilen. Auch auf Filterprogramme, die Werbesendungen herausfiltern sollen, ist kein Verlaß. Einerseits ist nicht auszuschließen, dass dadurch auch andere Geschäftspost herausgefiltert wird, insbesondere wenn sie Waren- und Leistungsbezeichnungen enthält, andererseits ist zu erwarten, dass die Filterwirkung dadurch umgangen wird, dass die Formulierung der Werbetexte den Besonderheiten dieser Programme Rechnung trägt.
Auch das Ausfiltern erwünschter, ausdrücklich angeforderter Werbung musste befürchtet werden.

2. Unverlangte Telefonwerbung ist wegen des damit verbundenen Eingriffs in die Individualsphäre wettbewerbswidrig (s. BGHZ 54, 188; NJW 89, 2820). Ein solcher Eingriff liegt bei e-mail jedoch nicht vor.

3. Unverlangte Telexwerbung ist wettbewerbswidrig, weil die Anlage zeitweise blockiert wird und zusätzliche Arbeit und Kosten entstehen, zumal wegen des Nachahmungseffekts (s. BGH GRUR 73, 211). Die Rechtsprechung ist auf die vorliegende Sache insoweit nicht übertragbar, als sie sich auf den geschäftlichen Verkehr bezieht und schon das vermutete Interesse des Empfängers die Wettbewerbswidrigkeit entfallen läßt. Im übrigen fehlen bei e-mail die Blockierung der Anlage und Empfangskosten in vergleichbarem Umfang. Die kurzen Übertragungszeiten schließen eine Blockierung bei der Übertragung auf den Surfer und von diesem auf den PC weitgehend aus, ebenso erheblich Kosten für die Übertragung sowie Gerätekosten. Papierkosten entfallen, weil ein Ausdruck entbehrlich ist. Es ist jedoch zusätzliche Arbeit beim Adressaten zu erwarten, weil dieser mit einer Überschwemmung mit Werbung rechnen muss.
Insoweit ist Telexwerbung mit e-mail-Werbung vergleichbar.

4. Die Teletexwerbung ist wie die Telexwerbung zu behandeln mit der Maßgabe, dass die stärkere Belastung wegen beschränkter Speicherkapazität und höherer Kosten zu berücksichtigen ist. Eine Erschöpfung der Speicherkapazität ist jedoch bei e-mail wenig wahrscheinlich angesichts der hohen Kapazitäten, die für die Surfer zur Verfügung gestellt werden können. Erhebliche Mehrkosten fehlen.

5. Unverlangte BTX-Werbung sieht die Rechtssprechung als unzumutbare Belästigung wegen der Blockierung des Anschlusses und des erforderlichen Aufwands an Zeit und Mühe zum Aussortieren an. Dabei sei zu berücksichtigen der Zeitbedarf des Bildaufbaus von 8 bis 30 Sekunden pro Seite. Gäbe es die Möglichkeit, Werbemitteilungen ohne Bildaufbau zu erkennen und zu löschen, entfielen die Bedenken zur Wettbewerbswidrigkeit (s. BGHZ 103, 201 ff.). Die uneingeschränkte Anwendung dieser Rechtsprechung auf e-mail könnte zur Zulässigkeit unverlangter e-mail-Werbung führen. Sie ist jedoch abzulehnen. Einerseits ist davon auszugehen, dass der Zeitbedarf für den Bildaufbau entfällt und Möglichkeiten zur Erkennung von Werbung schon aufgrund des Inhaltsverzeichnisses und der Löschung ohne Bildaufbau vorhanden sind. Andererseits ist zu berücksichtigen, dass in den fast zehn Jahren seit der BTX-Entscheidung tiefgreifende Veränderungen eingetreten sind. Zahl der Anschlußinhaber und Häufigkeit der Nutzung sind beim e-mail ungleich größer als sie es beim BTX waren. Die technischen Möglichkeiten zur schnellen und billigen Übertragung an

eine Vielzahl von Adressaten wurden erheblich ausgeweitet. Der verstärkte Einsatz von e-mail auch für wichtige Korrespondenz birgt auch bei Aussonderung von Werbung ohne Lesen des Textes die Gefahr, dass auch erwünschte Sendungen vernichtet werden. Die enorm angewachsene Werbeflut ließ das Interesse der Bevölkerung an unverlangter Werbung sinken. Der Umfang von Arbeit und Mühen für die Aussonderung kann bei e-mail weit größer sein
wegen steigender Werbeflut, wobei auch der zu erwartende Sog- und Nachahmungseffekt zu berücksichtigen ist. Es kann deshalb heute nicht davon ausgegangen werden, dass große Teile der privaten e-mail-Empfänger unverlangte Werbung als erwünschte Sendungen oder allenfalls als geringfügige, akzeptable Belästigung ansehen.

6. Durch europäische Rechtsvorschriften ist das Gericht nicht daran gehindert, die Wettbewerbswidrigkeit zu bejahen. Art. 10 Abs. 2 der EU-Fernabsatzrichtlinie sieht zwar vor, dass e-mail-Dienste zu kommerziellen Zwecken verwendet werden dürfen, wenn der Verbraucher sie nicht offenkundig ablehnt, jedoch läßt Art. 14 strengere Bestimmungen einzelner Mitgliedsstaaten zu, so auch die - durch die Rechtsprechung ausgestattete - Regelung des § 1 UWG (vgl. Hoeren WRP 97, 993, 995).

7. Eine zusammenfassende Bewertung ergibt, dass die beanstandete Werbung wettbewerbswidrig im Sinne des § 1 UWG ist und ihre Unterlassung verlangt werden kann.

a) e-mail-Werbung ist angeschwollen. Weiteres Anschwellen ist zu erwarten, weil sie für die Werbenden besonders attraktiv ist und billig, schnell, gezielt und massenhaft in Wohnungen und Büros gebracht werden kann und dabei auch bewegte Bilder, Sprache und Ton einsetzen kann.

b) Das Anschwellen der Werbung in allen Medien hat das Interesse des Bürgers an weiterer Werbung sinken lassen.

(So im Ergebnis auch Schrey-Westerwelle a.a.O.; aA Reichelsdorfer, a.a.0.)

8. Über die Zulässigkeit unverlangter Versendung von Werbung an kommerzielle e-mail-Anschlüsse war im vorliegenden Fall nicht zu entscheiden.

Ob die wirtschaftlichen Voraussetzungen für die Gewährung von Prozeßkostenhilfe vorliegen, kann dahinstehen. Vorsorglich wird darauf hingewiesen, dass die Angaben über das Bruttoeinkommen aus nichtselbständiger Arbeit im Prozeßkostenhilfeantrag und der dazugehörigen Bescheinigung nicht übereinstimmen, auch wenn das Weihnachtsgeld berücksichtigt wird und dass die Angaben über das Bruttoeinkommen aus selbständiger Arbeit und die Werbekosten in keiner Weise substantiiert sind.

Weinzierl
Vors. Richter am LG

[NETLAW 99]

Landgericht Berlin

Beschluß

Geschäftsnummer: 16 O 201/98
Beschluß vom 2. April 1998

In Sachen

(...)

wird im Wege der einstweiligen Verfügung - wegen Dringlichkeit ohne mündliche Verhandlung - angeordnet (§§ 1, 25 UWG, § 823 BGB, §§ 935 ff., 91, 890 ZPO):

1. Dem Antragsgegner wird bei Vermeidung eines vom Gericht für jeden Fall der Zuwiderhandlung festzusetzenden Ordnungsgeldes bis zu 500.000,00 DM, ersatzweise Ordnungshaft, oder Ordnungshaft bis zu sechs Monaten untersagt, künftig im Wege der

e-mail-Werbung an den Antragsteller heranzutreten, es sei denn, der Antragsteller hat der jeweiligen Sendung zuvor zugestimmt oder das Einverständnis kann wegen bereits bestehender Geschäftsverbindungen vermutet werden.

2. Die Kosten des Verfahrens trägt der Antragsgegner.

3. Der Wert des Streitgegenstandes wird auf 10.000,00 DM festgesetzt.

Gründe

Der Antragsteller hat glaubhaft gemacht, dass er per e-mail eine Werbung der (...) Agentur der (...) erhalten hat, ohne mit ihr in Geschäftsverbindung zu stehen. Er hat ferner glaubhaft gemacht, dass es sich bei der in dieser Werbung genannten Telefonnummer um die Telefonnummer des Antragsgegners handelt.

Die unaufgeforderte Zusendung von E-Mails verstößt aber gegen § 1 UWG, § 823 Abs. 1 BGB. In der Rechtsprechung ist es anerkannt, dass die unerbetene Zusendung von Werbung und Prospekten durch Telefax gegen § 1 UWG verstößt, sofern der Empfänger nicht damit einverstanden ist oder sein Einverständnis im Rahmen einer bereits bestehenden Geschäftsverbindung vermutet werden kann. Aus den gleichen Gründen ist auch die Zusendung von E-Mails ohne vorheriges Einverständnis oder in den Fällen, in denen nicht bereits eine Geschäftsverbindung besteht, wettbewerbswidrig.

Denn auch wenn der Empfang einer E-Mail selber - im Gegensatz zum Empfang eines Telefaxes - noch keine direkten Kosten beim Empfänger verursacht, so kann der Empfänger die E-Mail dennoch nur unter Verursachung von eigenen Kosten lesen und überhaupt als Werbung erkennen. Denn die E-Mail kann nur gelesen werden, während der Empfänger "online" ist. Auf diese Weise entstehen dem Empfänger einerseits Telefongebühren für die Verbindung des eigenen Computers mit dem externen Computer des Providers. Darüber hinaus stellt der Provider dem Empfänger die Kosten für die Nutzung seines Servers in Rechnung, die anteilmäßig auch auf die Zeit entfällt, in denen die Werbe-E-Mails gelesen werden.

Zudem läßt es sich im "E-Mail Briefkasten" nicht ohne weiteres identifizieren, welche E-Mails Werbung enthalten und welche E-Mails sonstige Nachrichten enthalten, so dass der Empfänger beim Leeren seines "E-Mail Briefkasten" die unverlangte Werbung unter Aufwand von Zeit und Mühe erst aussortieren muss, indem er die einzelnen Sendungen abruft. Aus denselben Gründen verstößt die Werbung auch gegen § 823 BGB.

Der Tenor wurde in Anwendung des § 938 ZPO präzisiert.

[WALDNER]

3.12 Spamming im internationalen Rechtsvergleich

Durch die Internationalität sowie die schwer feststellbare Menge der Benutzer und die Größe des Mediums Internet ist es für Gesetzgeber schwierig, Rechtsverstöße zu entdecken und eine entsprechende Verfolgung der Täter zu veranlassen. Eine weitere Schwierigkeit besteht darin, dass durch den länderübergreifenden Charakter des Internets es sich als sehr schwierig gestaltet, nationale Rechtsgebungen anzuwenden. Die Verwendung international gültiger Regelungen wird dadurch erschwert, dass die Entwicklung dieser mit der rasanten Entwicklung des Internets nicht mithalten konnten und entsprechende Regelungen und Richtlinien daher weitgehend fehlen.

3.12.1 Beteiligte juristische Personen

Da im Internet keine zentrale Administration und Kontrolle existiert, gibt es somit niemanden, der die Verantwortung für das Gesamtsystem übernimmt und als kompetenter Ansprechpartner für alle Bereiche des Internets dienen könnte. Die Gesetzgebungen differenzieren daher folgende Gruppen:

- **Internet Service Provider (ISPs):**

  Betreiber, welche die serverseitige Hard- und Software für eine Verbindung ins Internet zur Verfügung stellen.
  Die Tätigkeiten der ISPs sind nach Funktionsgesichtspunkten differenziert (Content-Provider, Moderation von Newsgroups, Betreiben eines FTP-Servers, Betreiben eines Mail-Servers, reines Hosting) und bietet dadurch die Möglichkeit, die strafrechtliche Verantwortlichkeit der beteiligten Personen im Einklang mit klassischen vergleichbaren Fällen zu regeln.

- **Content Provider:**

  Anbieter, welche Inhalte (Web-Sites, Usegroups, Chatrooms) im Internet präsentieren.
  Der Content-Provider ist für strafbare Inhalte einer Web-Site primär verantwortlich, da er der Urheber der jeweiligen präsentierten Information ist.

Postet jemand einen Artikel in einer Newsgroup, wird er damit zum Content-Provider und ist für den dargestellten Inhalt mit all den entsprechenden Konsequenzen voll verantwortlich.

- **User:**

nutzen die im Internet präsenten Dienste und Angebote

3.12.2 Ort der Tat

Eine grundlegende Eigenschaft des Internets ist seine Internationalität. Es ist mit Rechnern aus den verschiedensten Ländern verbunden und man kann über das Internet Daten von diesen Rechner abrufen bzw. Daten an diese Rechner senden. Es unterliegt außerdem durch Anschluss neuer Rechner und Netzte sowie Inbetriebnahme neuer Dienste ständigen Veränderungen.
Es ist daher für nationale Rechtsgebungen nicht möglich die Größe des Internets und dessen rechtliche Konsequenzen abzudecken.
Rechtlich ist jedoch nach dem Territorialitätsprinzip für eine begangene Straftat im Internet jeweils das nationale Recht anzuwenden, das für den Tatort Gültigkeit hat, d.h. jenes nationale Recht, auf dessen Territorium die Straftat über Internet begangen wurde.
In Österreich ist diese Regelung im § 67 StGB zu finden:

```
§ 67 Zeit und Ort der Tat

(1) Eine mit Strafe bedrohte Handlung hat der Täter zu der
Zeit begangen, da er gehandelt hat oder hätte handeln sollen;
wann der Erfolg eintritt, ist nicht maßgebend.

(2) Eine mit Strafe bedrohte Handlung hat der Täter an jedem
Ort begangen, an dem er gehandelt hat oder hätte handeln
sollen oder ein dem Tatbild entsprechender Erfolg ganz oder
zum Teil eingetreten ist oder nach der Vorstellung des Täters
hätte eintreten sollen.
```

Ein Spammer, der Spam über mehrere Zwischenstationen – angenommen von Österreich ausgehend über einen Server in Finnland und einen weiteren in England – an deutsche Internet-User versendet, handelt demnach eigentlich an vier verschiedenen Orten bzw. in vier verschiedenen Ländern, was die Frage, welches Recht anzuwenden ist, äußerst kompliziert gestaltet.
Durch das Routing im Internet ist auch kaum transparent, durch welche Länder eine E-Mail bei seiner Versendung geleitet wird und welche nationalen Gesetzgebungen anzuwenden sind.

Es ist jedoch nicht nur die Frage interessant, wo das Delikt begangen wurde, sondern auch, wo die Folgen des Delikts wirksam werden. So ist es möglich, dass es sich in einem Land um kein Delikt handelt, in einem anderen jedoch schon.
Folgendes Beispiel (leicht abgeändert) aus [LOEWENHEIM 98] soll dies verdeutlichen:

Ein deutsches und ein englisches Unternehmen sind starke Konkurrenten im deutschen und englischen Markt. Der englische Konkurrent verschickt an deutsche Internet-User Spam-Mails mit vergleichender Werbung als Inhalt, was nach dem englischen Recht zugelassen, nach deutschem aber verboten ist. Es erhebt sich nun die Frage, ob das deutsche Unternehmen gegen die Werbung des englischen Konkurrenten vorgehen kann und nach welchem Recht eine eventuelle Vorgehensweise judiziert wird.
Diese Zuständigkeiten und Vorgehensweisen können nach den sogenannten „Kollisionsregeln des internationalen Privatrechts“ – es handelt sich hier um Regeln in nationalen Rechtsgebungen für Fälle mit Auslandsbezug – behandelt werden.

3.12.3 Strafverfolgung

Ein besonderes Problem ergibt sich bei der Strafverfolgung eines Täters, da es im Internet sehr leicht möglich ist, Straftaten zu begehen ohne Spuren zu hinterlassen. Da ein Spammer sich sehr leicht als andere Person ausgeben kann, muss technisch sichergestellt sein, das dies nicht der Fall ist. Durch Anonymisierung des Absendernamens und der Absenderadresse sowie durch E-Mail-Relaying (siehe Kapitel 3.2.1.3) ist dies jedoch sehr oft nicht möglich. Durch Verwendung von Pseudo-Anonymous-Remailern, welche die Verwendung von Pseudonymen für E-Mail und News erlauben, lässt sich die Herkunft einer Nachricht auch sehr leicht verbergen. Bei dieser Form der Anonymisierung wird jedoch nur die versandte

Nachricht anonymisiert. Es wird jedem Absender ein Pseudonym zugeordnet, über welche der Absender wieder, wenn auch mit mehr Aufwand, identifiziert werden kann, da Strafverfolgungsbehörden berechtigt sind, auf die Pseudonym-Zuordnungstabellen dieser Remailer zuzugreifen. Diesem Zugriff entziehen sich jedoch wiederum viele Spammer, indem sie ihre Nachrichten über mehrere Pseudo-Remailer in verschiedenen Ländern laufen lassen. Darüber hinaus existieren auch Remailer mit einer noch stärkeren Form der Anonymisierung,. Hier wird den Absendern kein Pseudonym zugewiesen, was eine Identifizierung unmöglich macht.

Anders geartet ist die Situation bei Versendern von kommerziellem Spam. Hier gibt es sehr wohl Anhaltspunkte, um den Spammer zu identifizieren, da es bei kommerziellen Spam-Mails ja notwendig ist, eine Kontaktadresse oder Kontakttelefonnummer zu hinterlassen, um mit potentiellen Kunden in Kontakt zu kommen.

Gelingt es, Täter zu identifizieren, ist eine Strafverfolgung nicht immer gewährleistet, da Spamming bzw. dessen Inhalte, von Nation zu Nation unterschiedlich, entweder legal oder illegal sein können. Die zuständigen nationalen Behörden dürfen jedoch nur auf ihrem Staatsgebiet tätig werden.

3.13 Organisationen gegen Spam

Aus dem weltweiten Kampf gegen Spam entwickelten sich Zusammenschlüsse von Interessensgruppen, welche gezielt gegen Spam vorgehen. Es ist jedem Internet-User möglich, Mitglied dieser Organisationen zu werden und dadurch aktiv zur Bekämpfung von Spam beizutragen.

3.13.1 CAUCE

Coalition against Unsolicited E-Mail[7]

„CAUCE“ ist keine körperliche Institution sondern existiert lediglich im WWW mit einer Web-Site sowie im Usenet.
CAUCE entwickelte sich 1997 in den USA aus der Usenet-Diskussionsgruppe „SPAM-LAW“, welche sich wiederum aus der Diskussionsgruppe „SPAM-L“ entwickelte. Da in der Gruppe „SPAM-L“ das Thema Spam nicht mit der gewünschten Aufmerksamkeit behandelt wurde, entschlossen sich Teilnehmer dieser Gruppe die Diskussionsgruppe „SPAM-LAW“ zu gründen, um das Thema Spam ausführlicher behandeln zu können. Der Kern dieser neuen Diskussionsgruppe gründete schließlich „CAUCE“, von der später auch die europäische „CAUCE“-Institution „EURO-CAUCE“ gegründet wurde.
Weiters wurden von „EURO-CAUCE“ länderspezifische Seiten eingerichtet, welche aktuelle Informationen bezüglich Spam für das entsprechende Land bereitstellen.[8]
„CAUCE“ selbst bietet keine Abwehrmaßnahmen gegen Spam sondern versucht durch eine hohe, ständig anwachsende Mitgliederzahl ein entsprechendes Gewicht und Mitsprache bei legislativen Regelungen bezüglich Spam zu erreichen. Weiters werden auf der Web-Site weiterführende Links angeboten, die bezüglich der Bekämpfung von Spam sehr hilfreich sein können.

[7] http://www.cauce.org bzw. http://www.euro.cauce.org
[8] Für Österreich ist diese Seite ersichtlich unter: http://www.euro.cauce.org/en/countries/c_at.html

3.13.2 FREE

Forum for Responsible and Ethical E-Mail[9]

"FREE" geht von der Grundeinstellung aus, dass es ethisch nicht vertretbar ist, dass ISPs und Internet-User den größten Teil der von Spam verursachten Kosten übernehmen müssen.
Aus diesen Gründen engagiert sich „FREE" in folgenden Punkten:

- ISPs mittels Wissenstransfer bei der Bekämpfung von Spam zu unterstützen
- Die Internet-User über Spam und Abwehrmaßnahmen zu informieren
- Versuchen, zuständige Politiker und politische Institutionen aktiv zu beeinflussen, um Gesetzgebungen gegen Spam unter Strafandrohung gegen die Spammer zu erlassen.

Um diese Ziele verwirklichen zu können, betreibt „FREE" eine Web-Site, welche reichhaltige Informationen und weiterführende Links zum Thema Spam enthält.
Weiters wird ein Diskussionsforum sowie eine Mailing-Liste angeboten.

3.13.3 VIBE!AT

Verein für Internetbenutzer in Österreich[10]

"VIBE!AT" ist ein österreichischer, anonymer Remailer, welcher das anonyme Versenden von E-Mail und Newsgroup-Postings ermöglicht, ohne dass die Adresse des Absenders ersichtlich ist und er dadurch gegen Adressensammlung von Spammern geschützt ist.
„VIBE!AT" hat seine Zielsetzungen in folgender Grundsatzerklärung festgelegt:

[9] http://www.spamfree.org
[10] http://www.vibe.at

Grundsatzerklärung

Der "Verein für Internet-Benutzer Österreichs (VIBE.AT)" wurde Anfang 1999 infolge von Diskussionen im Usenet gegründet, um die Interessen der Benutzer gegenüber Behörden, Internet-Service-Providern (ISPs) und anderen Organisationen zu vertreten.

VIBE setzt sich ein

- *für eine Zusammenarbeit von Behörden, Interessensvertretungen, Wirtschaft und Privatpersonen mit dem Ziel, die intensive und freie Nutzung des Internet zu fördern*
- *für die Förderung der Verbreitung und des Einsatzes von Verschlüsselung und elektronischen Unterschriften (Signaturen) zum Schutz und zur Sicherheit des privaten und geschäftlichen Nachrichtenaustausches ohne Zwang zur Schlüsselhinterlegung bei staatlichen Stellen oder Dritten und ohne Einschränkung der Eigenschaften von Verschlüsselungssystemen*
- *für gesetzliche Regelungen gegen den Netzmissbrauch (z.B. Belästigung durch unverlangte Werbezusendungen - SPAM)*
- *für den Schutz der Privatsphäre - E-Mail und jede andere nicht öffentliche Kommunikation im Internet soll als vertraulich gelten und den gleichen Schutz genießen, wie schon jetzt Briefe und Telefonate*
- *für freien Meinungsaustausch und freie Meinungsäußerung im Internet sowie Schutz dieser Freiheit zumindest im Ausmaß von konventionellen Medien (wie Zeitung, Rundfunk)*
- *für gesetzliche Regelungen, welche lediglich einem unabhängigen Gericht Eingriffe in den Schutz der freien Meinungsäußerung und der Privatsphäre erlauben*
- *für die nachdrückliche Forderung, dass die freie elektronische Meinungsäußerung nicht durch indirekte Maßnahmen wie staatliche oder private Regulative von Hard- und Software, der Telekommunikations-Infrastruktur oder anderer wesentlicher Komponenten des Internet eingeschränkt werden darf*
- *für gesetzliche Regelungen, welche bei der Verantwortung für Inhalte deutlich zwischen inhaltlich Verantwortlichen ("content providers") und bloßen Netzbetreibern ("service providers") unterscheiden*

- *für die Anerkennung des Internet als Medium und eigene gesetzliche Regelungen, wo die bestehenden Gesetze nicht ausreichen, um die Besonderheiten des Internet zu berücksichtigen*

Diese Ziele will VIBE mittels Information der Öffentlichkeit über aktuelle Entwicklungen und durch internationalen Meinungsaustausch umsetzen. [VIBE 99]

3.13.4 Anti-Spam-Kampagne von „c't Magazin“ und „politik-digital“[11]

Die Computerzeitschrift „c’t Magazin“ sowie die parteiunabhängige Kommunikations- und Informationsplattform „politik-digital“ haben im EU-Raum eine mehrsprachige Internetkampagne gegen die Legalisierung von Spam gestartet. Die Initiatoren wollen sich mit dieser Online-Petition, bei der jeder Internet-User gegen Spam mitstimmen kann, an die Abgeordneten des Europäischen Parlaments sowie an die Abgeordneten der nationalen Parlamente richten, um ein EU-weites Spamverbot durchzusetzen bzw. um gegen eine Legalisierung von Spam zu protestieren.

3.13.5 Robinsonlisten

Robinson-Listen arbeiten mit Spammern zusammen, indem sie bekannten Spammern Listen mit eingetragenen Mitgliedern veröffentlichen, welche keine Werbe-E-Mails empfangen möchten (Opt-Out) bzw. welche ausdrücklich erklären, Werbe-E-Mails empfangen zu wollen (Opt-In) (siehe Kapitel 3.8.1.4).

Zwei im deutschsprachigen Raum populäre Robinsonlisten sind

- „eRobinson“ (http://www.erobinson.com) und
- „Die Freitag-Liste“ (http://www.de/freitag/info.html)

[11] http://www.politik-digital.de/spam

Gegenüber den Betreibern solcher Listen bestehen keine Rechtsansprüche seitens der eingetragenen Mitglieder, falls diese dennoch Spam-E-Mails bekommen, da keine Rechtsverbindlichkeiten eingegangen werden.
Die Teilnahme erfolgt kostenlos und anonym. Internet-User, welche an diesen Listen teilnehmen, geben lediglich ihre E-Mail-Adresse bekannt.
Die Finanzierung von „Robinson-Listen“ erfolgt über Bannerwerbung.

Das Problem von Robinsonlisten ist, wie gut die Betreiber mit den Spammern zusammenarbeiten und inwieweit sich diese an die Vereinbarungen halten.

4 Zusammenfassung

Mit der immer stärker werdenden Durchdringung von Unternehmen und Privathaushalten mit dem Internet wurde auch zunehmend seiner Einsatzmöglichkeit als Werbeträger ein immer größer werdendes Augenmerk geschenkt.

Durch die kostengünstige und einfache Art und Weise, viele Personen zu erreichen, wird das Internet nun schlussendlich auch immer stärker für Werbezwecke eingesetzt.
Beginnend mit der ersten Werbeaktion im Internet – dem „Canter & Siegel Greencard Spam" – entwickelte sich die Werbung per E-Mail in die Richtung normaler Postwurfsendungen. Beinahe täglich finden sich im Maileingang kommerzielle E-Mails.

Neben dieser Form der E-Mailwerbung wird auch sehr stark die Bannerwerbung eingesetzt. Bannerwerbung ist Werbung mittels sogenannter Banner, das eine bestimmte Werbebotschaft enthält und auf beinahe allen Web-Sites bereits zu finden sind.

Durch die immer stärker werdende Benutzung von Newsgroups wurde auch diese Internetplattform als Werbemedium entdeckt. Hier werden einfach Werbepostings in zum beworbenen Produkt passenden Newsgroups, oder auch themenfremden, gepostet.

Neben diesen drei erwähnten Formen unerwünschter Nachrichten tritt noch eine vierte Form, nämlich die Form sinnloser E-Mails. Als sinnlose E-Mails kann man Kettenbriefe, Virenwarnungen über Viren, welche gar nicht existent sind (sog. Hoax wie z.B. die Warnung vor dem Internetvirus „Budweiser Frogs") oder Hilfeaufrufe für Personen, die ebenso nicht existent sind, bzw. deren Problem sich bereits erledigt hat (durch die schneeballartige Verbreitung dieser Hilfeaufrufe sind die Internetuser über die geänderten Umstände jedoch nicht informiert und versenden erhaltene Hilferufe weiter) bezeichnen.

Aus diesem Grund ist es auch erforderlich, Spam zu klassifizieren, was in dieser Arbeit auch erfolgt.

Nicht nur, dass solche unerwünschte Nachrichten äußerst lästig sind – man denke z.B. an eine Postkasten, der vor Werbesendungen überquillt – stellt diese Problematik auch einen enormen Kostenfaktor dar. Es wird neben wertvoller Internetbandbreite auch viel Zeit von den Empfängern zum Lesen und Löschen dieser Nachrichten verschwendet. Besonders in kommerziellen Organisationen ist diese dafür eingesetzte Aufwand ein beträchtlicher Kostenfaktor, da die unternehmensweit dafür eingesetzte Zeit auch bezahlt werden muss und dadurch jährlich enorme wirtschaftliche Verluste entstehen können.

Es wird in dieser Arbeit außerdem erläutert, wie Spammer zu den Adressen ihrer potentiellen Opfer gelangen, da die Adressensammlung über verschiedenste Methoden erfolgt.
Denn nur wenn man weiß, wie Spammer Adressen sammeln, kann man wirksam vorbeugen, dass die eigene E-Mail-Adresse von Spammern benutzt wird.

Ist man jedoch bereits Opfer von Spammern geworden, gibt es verschiedene Möglichkeiten, dagegen vorzugehen.
Es wird daher erläutert, wie man Spam identifiziert und ein umfassender Überblick über Abwehrmethoden geboten, die einerseits technischer, andererseits administrativer Natur sein können.
Bei den technischen Abwehrmethoden werden sowohl serverseitige als auch clientseitige Filterprogramme erklärt, welche einen wirksamen Schutz bieten. Weiters wird auf eigene Anti-Spam-Tools eingegangen, welche wiederum server- bzw. clientseitig eingesetzt werden können.
Zu den administrativen Maßnahmen, die erläutert werden, zählen z.B. Beschwerden beim Provider oder Eintrag in Robinsonlisten bzw. Opt-In/Opt-Out-Listen.

Da das Internet ein sehr junges und vor allem internationales Medium ist, ist in diesem Bereich die Rechtslage äußerst kompliziert, in manchen Bereichen sogar noch ungeklärt.
Da ein Werbemail beispielsweise von einem Land in eine anderes über den Umweg eines Dritt- oder auch Viertlandes gesendet werden kann, ist die Legalität dieser Vorgehensweise schwer zu eruieren, da auch nationale Gesetzgebungen (wie z.B. das Werberecht) in die Überlegungen miteinbezogen werden müssen.
Es wird deshalb die rechtliche Situation im Bereich Spam gründlich ausgearbeitet und eine Darstellung von Spam im internationalen Rechtsvergleich gegeben.

Um die Spam-Problematik in den Griff zu bekommen, gibt es bereits veschiedenste nationale und internationale Organisationen gegen Spam, von denen die wichtigsten vorgestellt werden, da sie betroffenen Internet-Usern wertvolle Hilfestellung bieten können.

Um die theoretische Abhandlung dieses Themas zu ergänzen, wird im Anhang weiters die Auswertung einer im Zuge dieser Diplomarbeit durchgeführten Online-Umfrage zum Thema Spam vorgestellt.

Durch den immer stärker werdenden Einsatz des Internets wird sich voraussichtlich auch die Spam-Aktivität erhöhen. Es wird durch die Auswertung des Fragebogens ersichtlich, dass Spam als ein doch wesentliches Ärgernis empfunden wird und die sich die befragten User entsprechend mit dem Thema befassen. Diese Arbeit dient als Leitfaden zur erfolgreichen Bekämpfung gegen Spam und soll betroffenen Usern eine entsprechende Hilfestellung bieten, um Werbung im Internet auf einem erträglichen Niveau zu halten.

5 Abbildungsverzeichnis

6 Literaturverzeichnis

6.1 Bücher

[BÜRLIMANN 99] Bürlimann Martin: Webpromotion – Professionelle Werbung im Internet, Midas Management Verlag, 1999.

[SCHWARTZ 98] Schwartz Alan, Garfinkel Simson: Stopping Spam, O'Reilly, 1998.

[RUHLAND 97] Ruhland Jochen: Internet für Anbieter - Strategische Planung und Umsetzung der WWW-Präsenz, Hanser, 1997.

[MULLIGAN 99] Mulligan Geoff: Removing the Spam - E-Mail Processing and Filtering, Addison-Wesley, 1999.

6.2 Internetartikel

[A-SITE] http://www.a-site.at/bannerexchange/faq.htm
„Die wichtigsten und am häufigsten gestellten Fragen rund um den A-SITE BannerXchange“
01-05-24

[ABSEITS] http://www.abseits.de/webringe.htm
„Webringe und Banneraustauschdienste“
01-05-24

[ABSEITS 99/1] http://www.abseits.de/bannertips.htm
„Tipps für die Gestaltung von Bannerwerbung“
01-05-24

[ABUSE] http://spam.abuse.net/spam/whatisspam.html
“What is spam?”
01-05-24

[AOL] http://members.aol.com/E-Mailfaq/E-Mailfaq.html
“The E-Mail Abuse FAQ “
99-09-30

[BRAUNSCHWEIG 98] http://www.tu-bs.de/rz/doku/mitteilungen/mitt149/node3.html
1998
„Spam-Mails und kein Ende!?“
01-05-24

[CERT 99] http://www.cert.dfn.de/infoserv/dib/dib-9901.html 1999
„Technische Maßnahmen gegen Spam - Was tun gegen unerwünschte E-Mails? „
01-05-24

[CYBERNOTHING 99] http://www.cybernothing.org/faqs/net-abuse-faq.html 1998
“The Net Abuse FAQ”
01-05-24

[DFN-CERT 97] http://www.cert.dfn.de/infoserv/dib/dib-9502.html
„Informationen zum Thema Firewalls - Informationsbulletin DIB-95:02“
1997
01-05-24

[EANTC 99] http://www.eantc.de/~amk/dni/glossar
01-05-29

[FITUG1] http://www.fitug.de/netpol/97/5.html 1998
„Digest "Netz und Politik" (NETPOL-Digest) 5“
01-05-24

[FITUG2] http://www.fitug.de/debate/9901/msg00266.html 1999
„Einige Anmerkungen zum Thema Spam“
01-05-24

[FTC] http://www.ftc.gov/bcp/online/pubs/alerts/doznalrt.htm
99-09-30

[GOLDMANN 98] http://www.goldmann.de/stupid/junk.html
„Junk-Mail“
01-05-24

[HAB8] http://www.hab8.de
„Interne & externe Webseitenbewerbung“
01-05-24

[HEIM 98] http://meine.heim.at/webpromotion 1998
„The Web-Promotion-Site - Tipps und Tricks um den Traffic zu erhöhen“
99-09-30

[IAB 99] http://iab.net/iab_banner_standards/bannersizes.html
“IAB/CASIE Advertising Banner Sizes”
99-10-03

[KRONACH] http://www.kronach.baynet.de/bnv/faq/hoaxes.htm
99-09-30

[MORGENPOST 97] http://www.berliner-morgenpost.de/bm/bits_bytes/up2date/online/robinson.html 1997
„Robinson-Liste: Endlich Schluss mit E-Mail-Werbung?“
99-09-30

[NETCOLOGNE] http://www.netcologne.de/~nc-abendrca/promo.htm
01-05-24

[NETZSERVICE] http://www.netzservice.de/Home/kk/inkomploehntopp/02323.html
99-09-30

[NETLAW 99] http://www.netlaw.de 1999
„Online und Multimediarecht“
01-05-24

[PUBLIC-ZU 98] http://www-public.tu-bs.de:8080/~y0003361/spam.html 1998
„Unerwünschte E-Mail“
99-09-30

[QUINTESSENZ] http://quintessenz.at/campaign/justizausschuss.txt
01-05-24

[REWI 96] http://www.rewi.hu-berlin.de/~matze/rdi/selbstregulierung2.html 1996
„Selbstregulierung im Internet, Teil 1“
99-11-25

[RUHR-UNI] http://www.ruhr-uni-bochum.de/www-rz/kriegjcb/vortrag/Spam_Relay/all.html
„Werbe-E-Mail und E-Mail-Relaying“
01-05-24

[SALVIE] http://www.salvie.ch/hoaxinfo.htm 1999
„Spam und Hoax Informationen“
01-05-24

[SOFTSURF] http://www.softsurf.com/bannerexchanges
„Bannerwerbung, Bannertausch und Banner-Exchanges im deutschsprachigen Raum“
01-05-24

[TU-CHEMNITZ 97] http://archiv.tu-chemnitz.de/pub/1997/0048/spam.html
„Unerwünschte Botschaften: E-Mail-Spams“
01-05-24

[TU-BERLIN 1/99] http://www.tu-berlin.de/www/software/hoax.shtml 1999
„Computer-Viren, die keine sind (sog. "Hoaxes")"
01-05-24

[TU-BERLIN 2/99] http://users.cs.tu-berlin.de/~beinhart/AntiSpamWehren.html
99-09-30

[TU-BERLIN 3/99] http://www.tu-berlin.de/www/software/hoax/jana.shtml
1999
01-05-24

[UNI-GIESSEN 98] http://www.hrz.uni-giessen.de/faq/archiv/de-net-abuse.fremdcancel-faq/msg00000.html 1998
“Fremdcancel-FAQ”
01-05-24

[UNI-HALLE 98] http://www.uni-halle.de/urz/mailrelay2.html
„Was ist Mail-Relaying und was ist Missbrauch?“
1998
01-05-24

[VIBE 99] http://www.vibe.at 1999
„Spam und Belästigung durch E-Mail“
01-05-24

[WALDNER] http://www.uwe.waldner.com
„Cyberrecht und Telekommunikationsrecht“
99-09-30

[ZDF] http://www.zdf.msnbc.de/news/21643.asp 1999
“Hoaxes”: Viren, die es nicht gibt
01-05-29

6.3 Zeitschriftenartikel

[COMP 37/98] „Unerwünschte E-Mails verursachen hohe Kosten“
Computerwoche 37/98, S. 25 f

[COMP 40/98] „Mittelständler entdecken den Nutzen der Internetwerbung“
Computerwoche 40/98, S. 31

[COMP 49/98] „E-Mail-Falschmeldungen bescheren Unternehmen Produktivitätsverluste“
Computerwoche 49/98, S. 27

Anhang A) Fragebogen zu Spam

Folgender Fragebogen war Bestandteil einer Online-Umfrage zum Thema Spam und der damit verbundenen Auswirkungen:

1. Welche Internetverbindung haben Sie?
(Gilt für privaten und beruflichen Internetanschluss - bitte machen Sie die Angaben für die Verbindung, die Sie am häufigsten benutzen)

- Standleitung
- ADSL
- ISDN-Verbindung
- 2x64 kbit (ISDN-Basisanschluss)
- >128000 (ISDN-Multianschluss)
- Wählverbindung mittels Modem
- <28800
- >=28000

2. Wie oft erhalten Sie durchschnittlich Spam-Mail?

- mehrmals pro Tag
- 1 mal pro Tag
- alle paar Tage
- 1 mal pro Woche
- selten
- nie

3. Wenn Sie bereits Spam-Mail erhalten, aus welcher Kategorie war es?

(mehrere Antworten möglich)

- Möglichkeiten sich selbständig zu machen
- Angebot für kommerzielle Versendung von Massenmails
- Kettenbriefe
- Heimarbeitsangebote
- Gesundheits- und Diätangebote
- Zusatzeinkommen
- Gratisprodukte
- Investitionsgelegenheiten
- Angebote für Decoder von Satellitenprogrammen
- Darlehen und Kredite zu günstigen Konditionen
- Steigern bzw. Herstellen der Kreditwürdigkeit und Kreditauskünfte
- Gewinn eines Urlaubs
- Virenwarnungen
- Hard- und Softwareangebote
- sexbezogene Angebote
- andere

4. Wieviel Zeit benötigen Sie ungefähr um diese Spam-Mails herunterzuladen, zu lesen und zu löschen?

- < 5 min. / Tag
- 5-15 min. / Tag
- 15-30 min. / Tag
- 30-45 min. / Tag
- 45-60 min. / Tag
- 1 Std. / Tag

5. Haben Sie einen Mail-Filter in Verwendung

Server-seitig - wenn ja, welchen Filter

- ProcMail
- SendMail
- Firewall
- NoCeM-on-spool
- andere
- unbekannt
- nein

Client-seitig - wenn ja, welchen Filter

- DL MailFilter
- E-Mail-Remover
- Mail-Shield
- MailTalkX
- SpamBuster
- SpamEaterPro
- SpamKiller
- sonstige
- unbekannt
- nein

6. Sind sie in eine Robinsonliste gegen den Erhalt von Spam-Mail eingetragen? Wenn ja, in welche?

- eRobinson
- Freitag-Liste
- sonstige
- unbekannt
- nein

6. a Falls sie in eine Robinsonliste eingetragen sind, hat sich ab dem Zeitpunkt des Eintrags die Spam-Frequenz vermindert?

- nein
- etwas
- stark
- sehr stark
- kein Spam mehr

7. Falls sie keinen eigenen Server haben, wurde sie von Ihrem Provider über Maßnahmen bzw. über richtiges Verhalten gegenüber Spammern informiert?

- ja
- nein

8. Falls Sie einen Provider haben, hat Ihr Provider Maßnahmen gegen Erhalt von Spam-Mails getätigt?

- ja
- nein
- unbekannt

9. Nehmen Sie an Newsgroups teil?

Wenn ja, an welchen?
(mehrere Antworten möglich)

- comp Computer, Hard- und Softwarethemen

- news Neuigkeiten
- rec Unterhaltung zum Thema Freizeit, Sport und Entertainment
- sci natur- und geisteswissenschaftliche Themen
- soc soziale, gesellschaftliche und politische Themen
- talk allgemeine Diskussionen und Talkrunden
- misc verschiedene Themen
- sonstige

Wurden Sie in diesen Newsgroups mit nicht zum Thema gehörenden Postings bzw. Werbepostings konfrontiert?

- ja
- nein

Wenn ja, welche Postings waren das?
(mehrere Antworten möglich)

- Möglichkeiten sich selbständig zu machen
- Angebot für kommerzielle Versendung von Massenmails
- Kettenbriefe
- Heimarbeitsangebote
- Gesundheits- und Diätangebote
- Zusatzeinkommen
- Gratisprodukte
- Investitionsgelegenheiten
- Angebote für Decoder von Satellitenprogrammen
- Darlehen und Kredite zu günstigen Konditionen
- Steigern bzw. Herstellen der Kreditwürdigkeit und Kreditauskünfte
- Gewinn eines Urlaubs
- Virenwarnungen
- Hard- und Softwareangebote
- sexbezogene Angebote

- andere

10. Haben Sie bereits einmal Schritte gegen Spammer eingeleitet, wenn ja, welche?
(mehrere Antworten möglich)

- noch nie
- Beschwerde beim Spammer
- Beschwerde beim Provider des Spammers
- Beschwerde beim eigenen Provider
- Eintrag in Robinsonlisten
- Mailbombs
- Teergruben (tar pits)
- unsubscribe aus Mailtext
- sonstiges

11. Empfinden Sie Spam-Mails generell als belästigend?
(mehrere Antworten möglich)

- nein, weil .....
- ja, wegen
- Kosten 1 2 3 4 5
- Ressourcenverschwendung 1 2 3 4 5
    - Zeit 1 2 3 4 5
    - Speicher 1 2 3 4 5
    - Downloadkosten 1 2 3 4 5
- ärgerliche bzw. belästigende Inhalte 1 2 3 4 5

Bitte beurteilen Sie die Punkte mit 1 (eher egal) bis 5 (sehr belästigend)

12. Bitte machen Sie noch einige statistische Angaben zu Ihrer Person:

Wie hoch ist Ihre durchschnittliche Verweildauer im Internet?

- < 1 Stunde/Tag
- 1 – 3 Stunden/Tag
- 3 – 5 Stunden/Tag
- 5 Stunden/Tag

In welcher Weise nutzen sie das Internet? (mehrere Antworten möglich)

- Lesen/Senden von E-Mails
- Informationssuche im WWW
- Produktsuche/-kauf im WWW
- Netbanking / ELBA
- Teilnahme an Newsgroups
- Chat / ICQ

EDV-Nutzung (mehrere Antworten möglich)

- Systemadministrator
- Mailadministrator
- EDV-Leiter
- EDV-Nutzer
- Private Nutzung
- andere

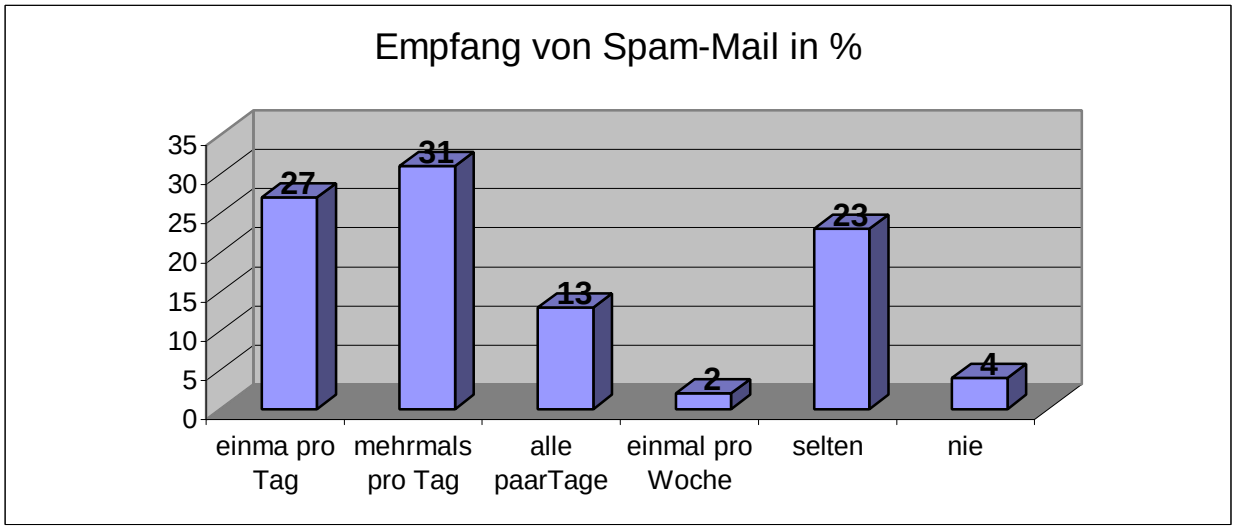
Anhang B) Fragebogen zu Spam – Auswertung

1. Welche Internetverbindung haben Sie

Da mehr als ¾ der befragten Personen eine Standleitung oder eine bessere Verbindung zur Verfügung steht, kann man von der befragten Personengruppe annehmen, dass es sich um sogenannte „Power-User“ handelt.

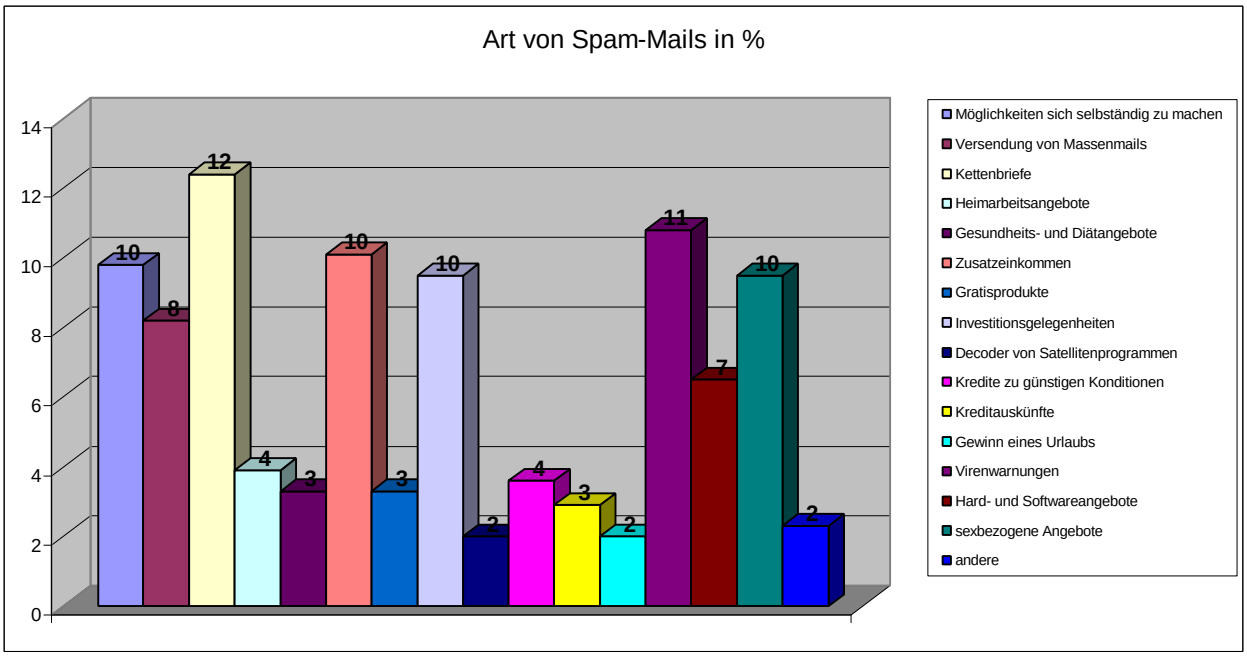
2. Wie oft erhalten Sie durchschnittlich Spam-Mail ?

Mehr als die Hälfte der befragten Personen erhält mindestens einmal pro Tag Spam-Mail. Fast ¾ der befragten Personen erhält alle paar Tage Spam und lediglich etwa ¼ erhält selten oder nie Spam:



3. Wenn Sie bereits Spam-Mail erhalten haben, aus welcher Kategorie war es?

Wie aus der folgenden Abbildung ersichtlich ist, dominieren bei der Art von Spam-Mails finanzbezogene Themen (Zusatzeinkommen, Investitionsgelegenheiten) sowie Kettenbriefe, zu denen im weiteren Sinn auch Virenwarnungen zu zählen sind. Ebenfalls sehr stark vertreten sind sexbezogene Themen. Da die Häufigkeit der versandten Spam-Mails noch vor Hard- und Softwareangeboten liegt, kann daraus geschlossen werden, dass Spamming nicht zielgruppenorientiert eingesetzt wird, da der mit diesem Fragebogen adressierte Personenkreis aufgrund seiner Tätigkeit (es wurden Personen aus dem IT-Bereich adressiert) an solchen Mails eher (wenn überhaupt) Interesse hätte:

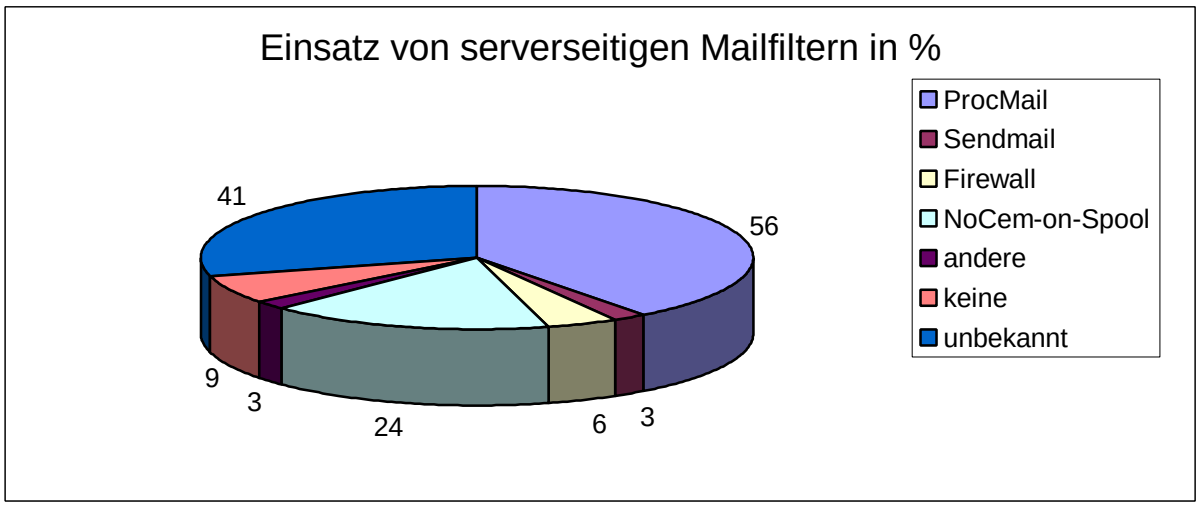


4. Wieviel Zeit benötigen Sie ungefähr um diese Spam-Mails herunterzuladen, zu lesen und zu löschen?

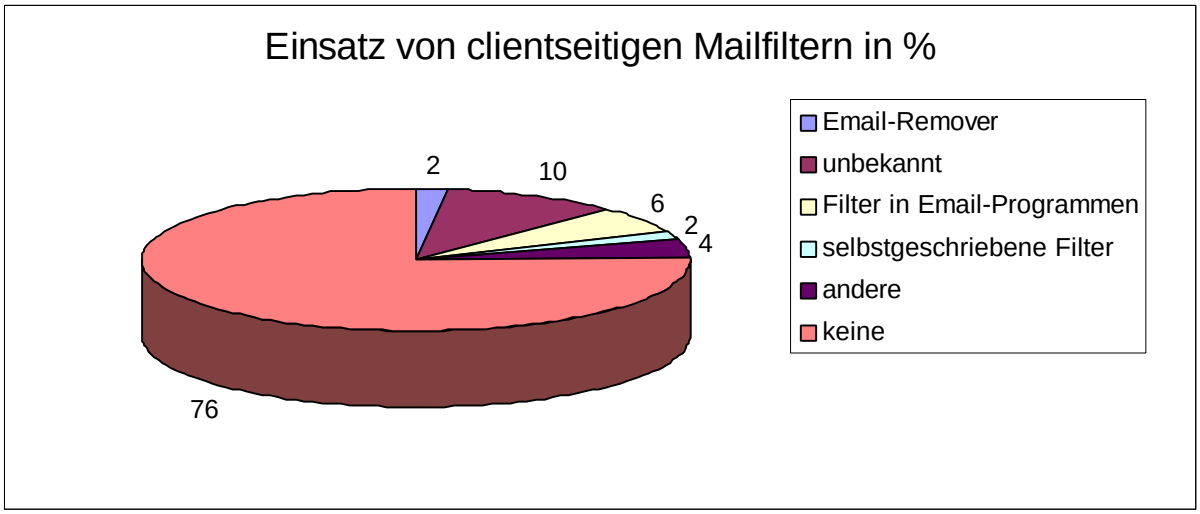
87 % der befragten Personen benötigen täglich durchschnittlich 5 Minuten, 13 % benötigen 5-15 Minuten.

5. Haben Sie einen Mail-Filter in Verwendung?

Mehr als die Hälfte der befragten Personengruppe ist nicht über serverseitig eingesetzte Filter informiert. Hier wäre seitens der Internetprovider verstärkte Aufklärungsarbeit bezüglich Spam sicherlich wünschenswert bzw. erforderlich:

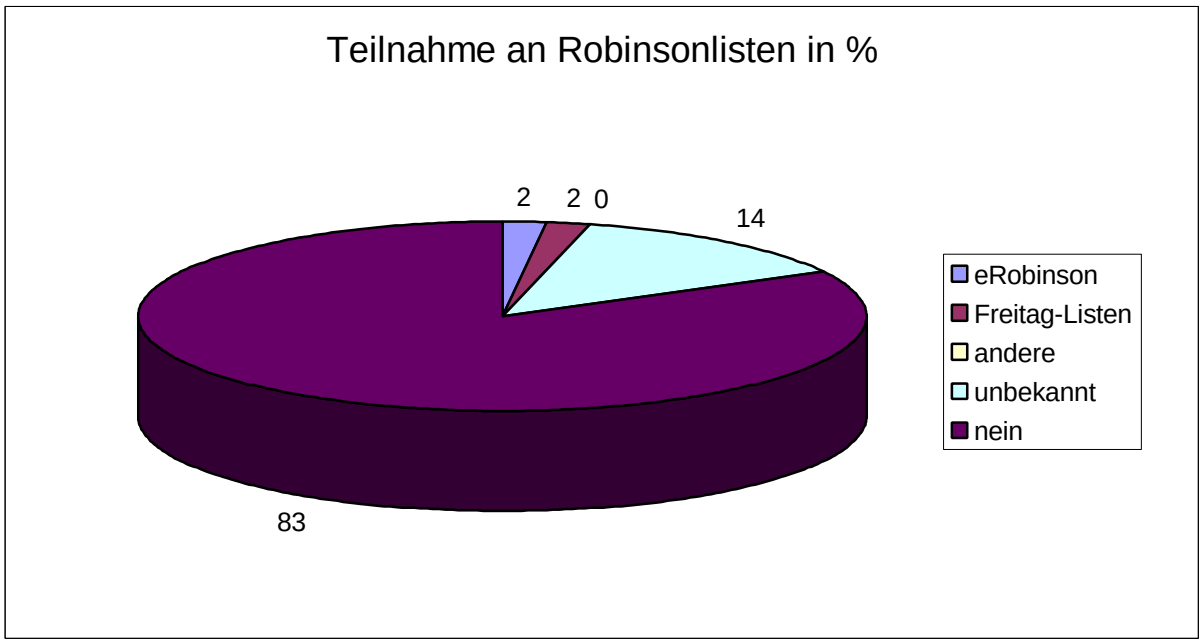


Da mehr als 75 % der User keine clientseitigen Filter verwenden und nur etwas mehr als 10 % die in E-Mail-Programmen integrierten Filter einsetzen, lässt diese Tatsache vermuten, dass die User sich mit der Problematik Spam noch nicht wirklich ernsthaft auseinandergesetzt haben. Um dieses Informationsmanko zu verkleinern, wäre seitens der Internetprovider verstärkte Aufklärungsarbeit erforderlich, um den Usern dieses Problem vor Augen zu führen:



6. Sind Sie in eine Robinsonliste gegen den Erhalt von Spam eingetragen? Wenn ja, in welche?

Da ebenfalls nur sehr wenige User an Robinsonlisten teilnehmen, wird durch die folgende Grafik die Aussage, welche bei den clientseitigen Filtern getroffen wurde, bekräftigt:



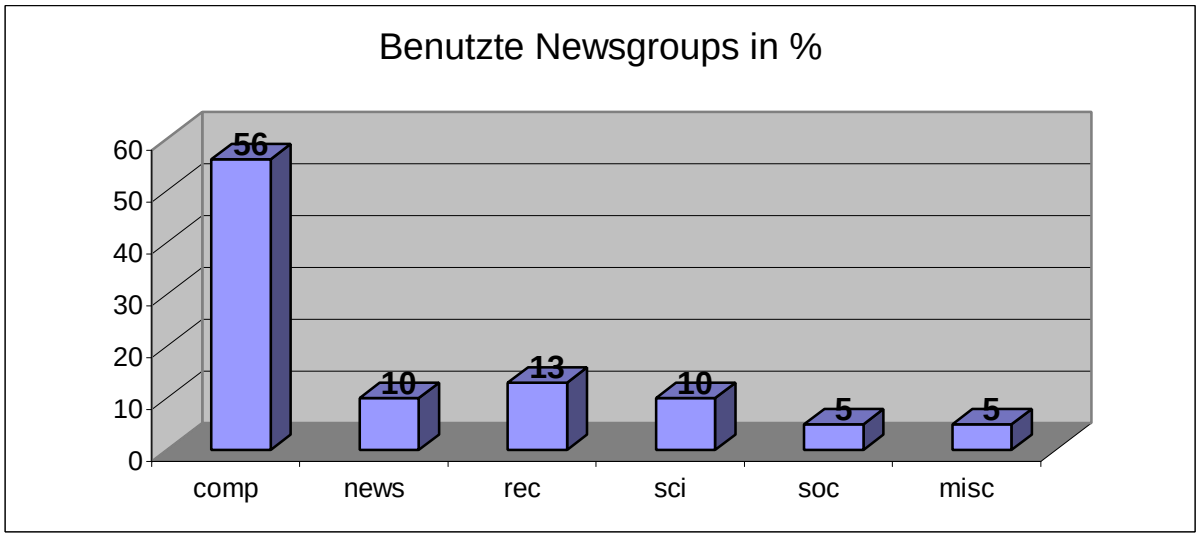
Fragen 7 u. 8:

Wie bei den Grafiken für clientseitige Filter bzw. der Teilnahme an Robinsonlisten bereits angesprochen wird, wird durch diese Frage bestätigt, dass die Aufklärungsarbeit der Internetprovider bezüglich Spam sehr dürftig ist:

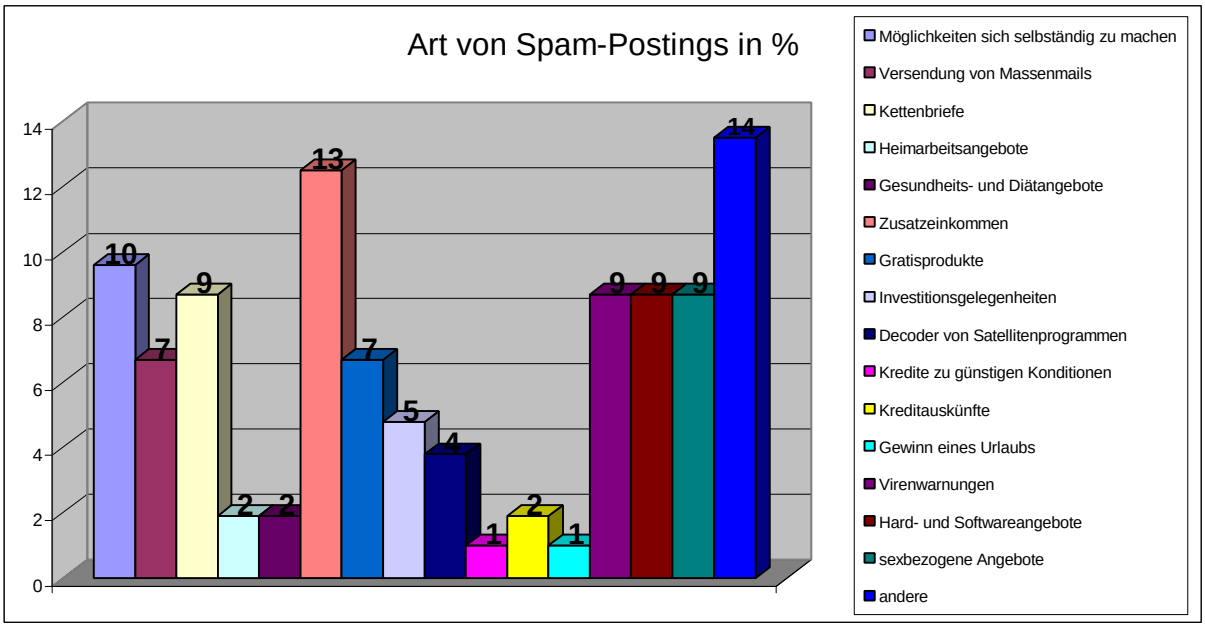
	nein	ja	unbekannt
Maßnahmeninformation vom Internetprovider	76	24	-
Getätigte Maßnahmen vom Provider	10	23	67

Angaben in %

9. Nehmen Sie an Newsgroups teil?



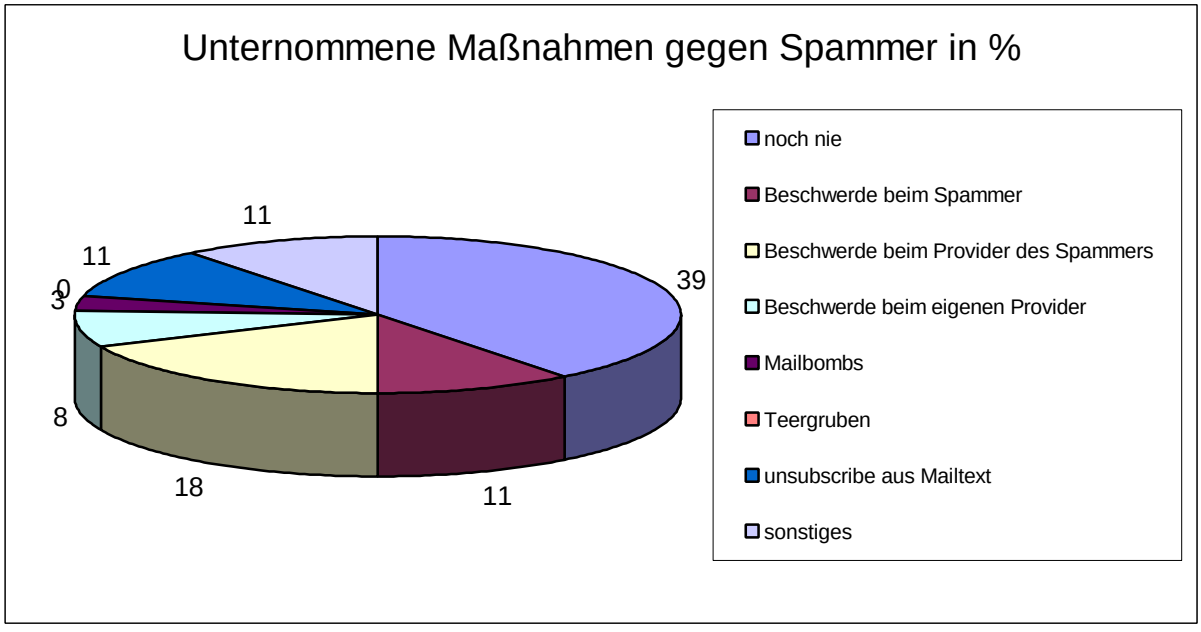
Zusatzeinkommen, Gratisprodukte, Hard- u. Software sowie diverse andere Postings haben in Newsgroups einen höheren Prozentwert erreicht als bei E-Mail-Spam. Diese Tatsache ist vermutlich darauf zurückzuführen, dass in Newsgroups eher eine zielgruppenorientierte Werbung möglich ist. Da die Newsgroup "comp" mit 56 % die vom befragten Personenkreis am häufigsten benutze Newsgroup ist, ist auch nachzuvollziehen, dass Hard- und Softwareangebote steigen. Da Fachkräfte in der IT-Branche seht stark nachgefragt sind, wäre eine mögliche Erklärung für den Anstieg von Spam-Postings jene, dass einfach Jobangebote gepostet werden (z.B. auf eine gepostete Antwort auf ein gepostetes Web-Problem wird wiederum ein Jobangebot als Webdesigner gepostet):



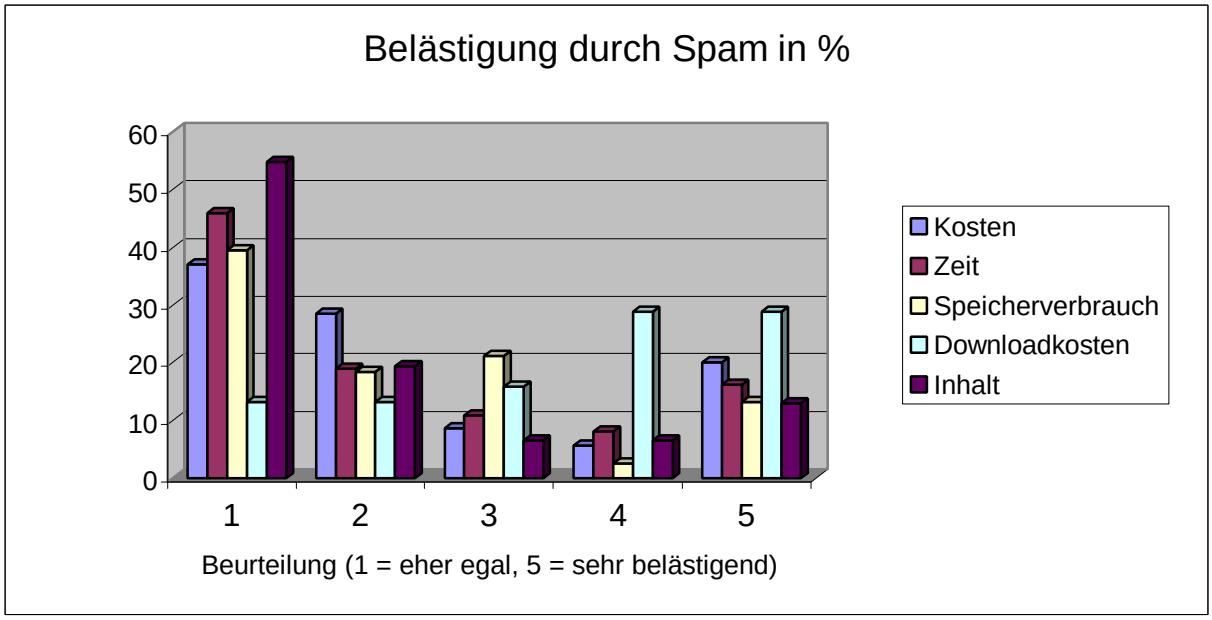
10. Haben Sie bereits einmal Schritte gegen Spammer eingeleitet, wenn ja, welche?

Obwohl 76 % der befragten Personengruppe angibt, keine Clientfilter zu verwenden bzw. 83 % angeben, an keiner Robinsonliste teilzunehmen, haben fast 60 % Maßnahmen gegen Spam getätigt, was darauf schließen lässt, dass Spam als sehr lästig empfunden wird.

Diese Vermutung wird in der übernächsten Grafik auch bestätigt.



11. Empfinden Sie Spam generell als belästigend?



Für den Großteil der befragten Personen ist der Aspekt der Downloadkosten (z.B. Onlinekosten) der am meisten störende Aspekt bei Spam. Erst danach folgen Kosten für die eingesetzte Arbeitszeit.

Wenn man jedoch bedenkt, dass die Mehrheit der Leute, welche mehrmals pro Tag Spam-Mails erhalten, 5-15 Minuten zum Aussortieren und Löschen benötigen, ergibt das ungefähr folgende Kosten (Zahlen sind nur ungefähre Richtwerte):

> Bei ca. 10 min. Arbeitszeit pro Tag, welche für das Lesen und Löschen von Spam benötigt werden, ergibt das bei einer Anzahl von 220 Arbeitstagen pro Jahr einen Gesamtzeitaufwand von ca. 37 Stunden. Wenn man nun Bruttogehaltskosten incl. Lohnnebenkosten von ATS 800,-- (ca. 58,14 Euro) pro Stunde ansetzt, ergibt das Kosten von **ATS 29600 ,--** (ca. 2151 Euro) pro Mitarbeiter und Jahr nur für das Beseitigen von Spam.

Dieses Rechenbeispiel führt meines Erachtens deutlich vor Augen, dass Spam nicht nur, wie aus der Befragung hervorgeht, für den Internet-User subjektiv als belästigend empfunden wird, sondern in Unternehmen auch enorme Kosten verursacht.
Aus diesem Grund sind sowohl User als auch Provider gefordert, Spam zu bekämpfen und dadurch eine Eindämmung der damit verbundenen Kosten zu erreichen.