Association for Information Systems
AIS Electronic Library (AISeL)

Wirtschaftsinformatik Proceedings 2003 | Wirtschaftsinformatik

September 2003

"Sie haben schon wieder Post": Spam Forschungsgebiet der Wirtschaftsinformatik

Christopher Peter Lueg
University of Technology Sydney, Australia, lueg@it.uts.edu.au

In: Uhr, Wolfgang, Esswein, Werner & Schoop, Eric (Hg.) 2003. *Wirtschaftsinformatik 2003: Medien - Märkte - Mobilität*, 2 Bde. Heidelberg: Physica-Verlag

ISBN: 3-7908-0111-9 (Band 1)
ISBN: 3-7908-0116-X (Band 2)

„Sie haben *schon wieder* Post“: Spam als Forschungsgebiet der Wirtschaftsinformatik

Christopher Peter Lueg
University of Technology Sydney, Australia

Zusammenfassung: Spam hat sich in den letzten Jahren von einem „Ärgernis“ zu einem wirtschaftlich bedeutenden Problem entwickelt. In diesem Beitrag werde ich aufzeigen, daß zur Erforschung der Probleme, die durch Spam verursacht werden, und der Maßnahmen, die gegen Spam ergriffen werden können, eine interdisziplinäre „Brille“ notwendig ist, da neben eher technischen Aspekten auch wirtschaftliche und juristische Aspekte berücksichtigt werden müssen. Damit ist die Wirtschaftsinformatik als Forschungsrichtung prädestiniert für den Aufbau eines umfassenden und vielschichtigen Verständnisses des Spam-Phänomens und seiner technischen, unternehmerischen und nicht zuletzt auch gesellschaftlichen Auswirkungen.

Schlüsselworte: Internet, Email, Spam, Informationsverbreitung, Informationsfilterung, Betriebskosten, betriebliche Kommunikationssysteme

1 Einleitung

Der immer leichter werdende Zugriff auf das Internet und Dienste wie Email und das World Wide Web hat zu großen Erleichterungen in der Informationsbeschaffung und -verbreitung geführt. Die dadurch entstandenen neuen Möglichkeiten von Digitalen Bibliotheken bis hin zu E-Business sind sowohl wirtschaftlich als auch kulturell von enormer Bedeutung. Neben diesen Errungenschaften haben sich allerdings Nebenwirkungen manifestiert, deren Schadenpotential erst langsam wahrgenommen wird: die Rede ist insbesondere von dem ungefragten Zusenden von Email mit typischerweise kommerziellem Hintergrund -- besser bekannt als „Spam“.

Über viele Jahre wurde Spam in erster Linie als „persönliches Ärgernis“ betrachtet, da man davon ausging, daß das Löschen einzelner Spam-Emails (genauer: das Drücken der Lösch-Taste im Email-Programm) nur wenige Sekunden dauert und ein paar Spam-Emails auch keine nennenswerten Übertragungskosten verursachen.

Wirtschaftlich orientierte Studien zum Thema Spam gab es entsprechend kaum. Nahezu unbemerkt hat sich Spam allerdings in der vergangenen Jahren zu einem

Phänomen entwickelt, das Unternehmen Kosten in Milliardenhöhe verursacht und Kommunikation per Email zu gefährden droht.

Maßnahmen gegen Spam sind bisher nur auf der technischen Kommunikationsebene effektiv einsetzbar und auch einigermaßen gut verstanden. Andere Maßnahmen wie gesetzliche Einschränkungen oder auch Selbstregulierung der Werbenden kranken daran, daß Spam ein internationales Problem ist, während gesetzliche Einschränkungen und auch Selbstregulierung typischerweise lediglich nationale oder wie im Fall einer einheitlichen Regelung in Staatenbunden wie der EU regionale Auswirkungen haben. Entsprechend kommentiert auch [Heid03] des Juristen Heidrich zu dem Entwurf zur Neuregelung des deutschen Gesetzes gegen den unlauteren Wettbewerb (UWG):

> „Am Spam-Aufkommen wird das neue Gesetz ohnehin nicht viel ändern -- schließlich kommt ein Großteil des Werbemülls aus dem Ausland, und Spammer aus Tuvalu, den Bahamas oder den USA kümmern sich erfahrungsgemäß wenig um deutsches Wettbewerbsrecht. Immerhin gelten aber nun in den Mitgliedsstaaten der EU weitgehend einheitliche gesetzliche Regelungen."

Eine Diskussion von juristischen Aspekten findet sich bei [Wend02].

Die bisher effektivsten (Selbst-)Schutzmaßnahmen gegen Spam, wie z.B. das Filtern eingehender Email aufgrund des Vorkommens Spam-typischer Begriffe („Warez", „Free Porn") oder auch das Ablehnen von Emails, die über Mail-Server von als Spam-freundlich bekannten Internet Service Providern (ISP) verschickt wurden, sind daher technischer Natur. Auch die erste internationale Spam-Konferenz im Januar 2003 [MIT03] war eine „conference on spam filtering" und damit auf technische Ansätze zur Spam-Bekämpfung ausgerichtet. Der erste deutsche Kongress zum Thema Spam beschäftigt sich schwerpunktmäßig auch mit technischen Lösungsansätzen. Daneben werden allerdings auch noch juristische Aspekte und Maßnahmen der Gesetzgebung behandelt, wobei diese vermutlich nur für Deutschland relevant sein dürften.

Auch wenn technisch orientierte Anti-Spam-Maßnahmen durchaus effektiv sind in der Reduzierung der Spam-Menge, so kommen sie den spezifischen Bedürfnissen von Firmen trotzdem nur unter Einschränkungen entgegen. Maßnahmen wie das Filtern oder Blocken von Email weisen einige unschöne Eigenschaften auf, die sich beim Einsatz im Unternehmen negativ bemerkbar machen können. Für Privatpersonen mögen solche Nachteile tragbar sein, aber für Unternehmen können sich diese Eigenschaften der Anti-Spam-Maßnahmen geschäftsschädigend auswirken.

Im weiteren Verlauf des Beitrages werde ich aufzeigen, daß zur Erforschung der Probleme, die durch Spam verursacht werden, als auch der Maßnahmen, die gegen Spam ergriffen werden können, eine interdisziplinäre Brille notwendig ist, da neben technischen Aspekten auch wirtschaftliche und juristische Aspekte berücksichtigt werden müssen. Damit ist die Wirtschaftsinformatik als Forschungsrichtung prädestiniert für den Aufbau eines umfassenden und

vielschichtigen Verständnisses des Spam-Phänomens und seiner technischen, unternehmerischen und nicht zuletzt auch gesellschaftlichen Auswirkungen. Aufgrund der Komplexität des Themas und den Platzbeschränkungen bei Konferenzbeiträgen kann ich allerdings lediglich die aus Sicht der Wirtschaftsinformatik interessantesten Gebiete aufzeigen sowie mögliche Forschungsrichtungen andiskutieren.

Der weitere Aufbau dieses Beitrages ist wie folgt: Zuerst werde ich kurz anreißen, was in Fachkreisen unter Spam verstanden wird, da der Begriff häufig auch für lediglich unerwünschte Email verwendet wird. Dann werde ich diskutieren, was prinzipiell an technischen Maßnahmen gegen Spam ergriffen werden kann. Dabei werde ich mich aus den weiter oben genannten Gründen auf technische Maßnahmen beschränken. Darauf aufbauend werde ich durch Spam verursachte Kosten diskutieren. Von Anti-Spam-Maßnahmen (mit-)verursachte Kosten nehme ich dann zum Anlaß, Vor- und Nachteile von Anti-Spam Maßnahmen aus betrieblicher Sicht zu diskutieren sowie weitere Forschungsrichtungen zu erörtern.

2 Hintergrund: Spam/UBE/UCE

Wie von [Base03] in der Email Abuse FAQ („Frequently Asked Questions“ sowie dazu passende Antworten) ausgeführt, ist der Begriff Spam historisch gesehen eine Bezeichnung für eine bestimmte Art von Usenet (NetNews) Beitrag und hat im Grunde genommen nichts mit Email zu tun. SPAM (in Großbuchstaben geschrieben) wiederum ist eine geschützte Markenbezeichnung für eine in den U.S.A. weit verbreitete Fleischkonserve, wobei der Markeninhaber die Verwendung des Markennamens im Email-Kontext zu tolerieren scheint, solange es sich um die „Spam“ Schreibweise handelt. Gerüchten zufolge geht die Verwendung des Wortes Spam für Usenet Beiträge auf einen Monty Python Sketch zurück; für Details siehe die von [Falk03] unterhaltene Net Abuse FAQ.

Auf der Web Site des Anti-Spam-Dienstes abuse.net gibt [Muel03] eine etwas weiter gefaßte Definition von Spam, die sowohl Usenet Beiträge als auch Email umfaßt:

> „Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products, get-rich- quick schemes, or quasi-legal services.“

Das australische National Office for the Information Economy (NOIE) begreift Spam wie folgt [NOIE02, S. 6]:

> „Spam is the term now generally used to refer to unsolicited messages, usually transmitted to a large number of recipients. They usually, but not necessarily, have a commercial focus, promoting or selling products or services [...]“

[Base03] geht näher auf den Unterschied zwischen „solicited email“ und „unsolicited email“ ein. „Solicited email“ ist etwa Email im inhaltlichen Zusammenhang mit einem vorherigen Usenet Beitrag oder Werbung, deren Zusendung man beim Ausfüllen eines Web Formulars explizit zugestimmt hat; auch Kontaktversuche von Bekannten und Arbeitskollegen fallen darunter. „Unsolicited email“ ist Email, bei der der Empfänger dem Empfang in keiner Weise zugestimmt hat. Des weiteren unterscheidet [Base03] zwischen UCE (Unsolicited Commercial Email) und UBE (Unsolicited Bulk Email), wobei UBE im allgemeinen auch UCE ist: *„UBE is undoubtedly the single largest form of email abuse today“*. Besonders bekannte UBEs haben ihre eigenen Kürzel, wie etwa MMF (Make Money Fast) sowie MLM (Multi-Level Marketing).

CAUCE, eine Non-Government Organisation (NGO), die sich seit Jahren mit Anti-Spam-Maßnahmen beschäftigt, faßt die verschiedenen Typen unter „junk mail“ zusammen und nennt typische Beispiele für die von CAUCE beobachteten Spams [CAUCE03]:

„[...] the most commonly seen UCEs advertise:

- Chain letters
- Pyramid schemes (including Multilevel Marketing, or MLM)
- Other 'Get Rich Quick' or 'Make Money Fast' (MMF) schemes
- Offers of phone sex lines and ads for pornographic web sites
- Offers of software for collecting e-mail addresses and sending UCE
- Offers of bulk e-mailing services for sending UCE
- Stock offerings for unknown start-up corporations
- Quack health products and remedies
- Illegally pirated software ('Warez')“

Brightmail, ein Entwickler von Anti-Spam Produkten, stellt mittels Tausender von Test-Accounts jeweils die „Top 10“ Spams eines Jahres fest. [Brig02] zufolge sind im Jahr 2002 unter den am meisten verschickten Spams ein „Credit Card Scam“ (Platz 2), der auch in Deutschland bekannte „Nigeria Scam“ (Platz 9), sowie Werbung für eine Porno Web Site (Platz 10). Brightmail betont, daß die Porno-Werbung auch an Postfächer von Kindern geschickt wurde (manche Mail Provider erlauben per Web Formular das Erstellen von Eigentümer-Beschreibungen, die u.a. das Alter des Eigentümers festhalten. Solche Beschreibungen sind allerdings i.allg. extern nicht verfügbar).

Die beworbenen Email Adressen sind in der Regel ohne Zustimmung der Betroffenen aus Usenet Beiträgen und von Web Sites entnommen worden: *„Email spam lists are often created by scanning Usenet postings, stealing Internet mailing lists, or searching the Web for addresses.“* [Muel03]. CDs mit 100 Millionen

Email Adressen sind laut [SL02] schon für 2000 USD zu haben, wobei der Autor dieses Beitrags schon verschiedentlich (Spam-)Werbung für wesentlich günstigere Angebote gesehen hat.

Neben den verschiedenen Sammelmethoden verwenden Spammer auch „brut force“ Methoden, wie das systematische Durchtesten automatisch generierter und formal korrekter Email Adressen oder sogenannte „dictionary attacks“ [TSP03a], bei denen Spammer ähnlich wie beim „Password“-Knacken mit Hilfe von Wörterbüchern mögliche Email-Adressen erzeugen. Solche Methoden um so erfolgversprechender, desto mehr Postfächer bei einem Provider existieren. Große Email-Provider wie AOL oder hotmail.com sind entsprechend besonders anfällig.

[CAUCE03] faßt Vermutungen zusammen, warum sich „Junk Mail“ überhaupt zu einem Problem entwickeln konnte. Die Punkte stimmen weitgehend mit den Erkenntnissen anderer Organisationen wie NOIE oder der U.S. Federal Trade Commission (FTC) überein. Die drei wichtigsten Punkte sind:

1. „Cost-Shifting“

   Die wahren Kosten für Transport und Empfang der Spam-Nachrichten werden nicht vom Versender, sondern von Anderen (vom Dienstleister bis zum Empfänger) getragen (siehe auch [Muel03]).

   Dieser Eindruck wird von [NOIE02, S. 2] geteilt: *„The biggest single factor leading to spam growth is the low cost of sending such material.“*

2. „Fraud“

   Man kann davon ausgehen, daß Spammer im Allgemeinen wissen, daß ihre Junk Mails unerwünscht sind. Von daher versuchen sie häufig, den Empfänger über den wahren Inhalt von Junk Mail zu täuschen. Oft sehen Junk Mails so aus, als wären sie keine kommerziellen Angebote, sondern etwa Tips von Freunden. Häufig geben Mails auch vor, eine Antwort auf eine Anfrage oder gar auf eine vorhergegangene Konversation zu sein.

3. „Disguise origin“

   Insbesondere professionelle Spammer wissen, daß ihre Mail Server geblockt und Mails mit ihren Absendern gefiltert werden (für Details siehe „Maßnahmen gegen Spam“ weiter unten). Von daher versuchen sie, die Herkunft ihrer Junk Mail zu verschleiern.

   Beliebt ist unter Spammern das Fälschen des Absenders, d.h. etwa das Angeben eines Yahoo Absenders, obwohl der Spammer dort kein Postfach hat. Der gefälschte Absender soll Anwender und Spam-Filter täuschen, und führt neben der eigentlichen Täuschung auch noch dazu, daß Beschwerden über das Spamming bei unbeteiligten Dritten landen.

   Ein weiterer beliebter Spammer-Trick ist „third party relaying“, d.h. der Spammer sucht sich einen sogenannten „offenen“ Mail Server, der es erlaubt,

> Mail an Dritte zu verschicken. Der Effekt von Relaying ist, daß die Junk Mail scheinbar von einem harmlosen Server kommt und „akzeptiert“ wird. Zudem ändert sich auch die rechtliche Situation, wenn Spam über einen Server verschickt wird, der in einem Land steht, in dem Spamming toleriert wird.

Punkte 2 und 3 werden auch von einer von der U.S. Federal Trade Commission (FTC) durchgeführten Untersuchung unterstützt:

> „FTC staff found that UCE for Investment/ Business Opportunity, Financial, and Adult offers accounted for over half of all messages. When analyzing the prevalence of false claims, FTC staff found indicators of falsity in the 'From' lines, 'Subject' lines, or content of two-thirds of the messages.“ [FTC 2003, S. 14].

Es wird von Spammern gerne argumentiert, Spamming wäre eine schützenswerte Meinungsäußerung (die dann etwa von dem 'First Amendment' in den U.S.A. gedeckt würde) geschützt und Anti-Spam-Maßnahmen damit versteckte Zensurversuche. Ohne hier auf die Details eingehen zu wollen, kann man festhalten, daß es Spammern selbstredend frei steht, ihre Angebote „unzensiert“ auf ihren eigenen Web Sites oder auch in Zeitschrifteninseraten zu verbreiten.

3 Maßnahmen gegen Spam

In diesem Abschnitt werde ich einige der wichtigsten Anti-Spam-Maßnahmen ansprechen. Die Übersicht soll lediglich einen Eindruck der in Frage kommenden Techniken geben, da ich einige Details zur Verdeutlichung von Sachverhalten in späteren Abschnitten des Beitrages benötige. Eine detaillierte Darstellung ist im Kontext dieses Beitrages weder notwendig noch sinnvoll.

3.1 Vorbeugende Maßnahmen

Die scheinbar naheliegendste Maßnahme gegen Spam ist das Nicht-Erwähnen von Email Adressen an jedwelchen Stellen im „Cyberspace“, die von Spammern und ihren Such-Programmen abgegrast werden könnten. Dazu gehört auch das Angeben von Email Adressen bei Anmeldungen auf Web Sites, da solche Adressen gerne an „Partnerprogramme“ weitergereicht werden. Nicht selten gehören Kundenadreßbestände auch bei Web Sites mit restriktiver „Privacy Policy“ beim Konkurs der Betreiberfirma zu den wertvollsten „Assets“ und werden ganz regulär weiterverkauft.

Erfahrene Internet-Benutzer halten es schon seit Jahren so, daß sie jedesmal, wenn eine Email Adresse für eine Registrierung o.ä. benötigt wird, eine neue Adresse bei einem „Freemailer“ wie hotmail.com oder gmx.de anlegen, und diese dann nur für die Anmeldung verwenden. Sollte die Adresse in die Hände von Spammern

gelangen, würde sich der Schaden in Grenzen halten. Für „Freemailer“ stellt sich dagegen die Frage, wieviele ihrer Email Adressen tatsächlich genutzt werden und nicht nur Anti-Spam-Postfächer sind.

Für Firmen ist die „Vogel Strauß“ Strategie aus verschiedenen Gründen kaum praktikabel. Zum einen gehört „Erreichbarkeit“ zu den Erfordernissen des modernen Geschäftslebens. Typische Adressen wie info@firma sollten immer existieren und sind dementsprechend Spam-anfällig. Zum anderen zeigt das Aufkommen von Wörterbuch-basierenden Angriffen die Grenzen einer solchen Email Politik auf.

3.2 Abwehrende Maßnahmen

Die derzeit üblichen technischen Maßnahmen gegen Spam sind „Filtern“ und „Blocken“. Die Idee ist jeweils, daß man den Großteil des Spams unterdrückt, bevor er zu den Mitarbeitern gelangt. Des weiteren können solche Filter auch noch zum Beseitigen von „Malware“ wie Viren und Trojanischen Pferden benutzt werden.

3.2.1 Filtern

Beim Filtern kann man wiederum grob zwei Ansätze unterscheiden, die häufig zum Erreichen größtmöglicher Effektivität kombiniert werden:

Inhaltsorientiertes Filtern („content-based filtering“)

Da ein Großteil des Spams immer wieder die gleichen Produkte bewirbt (s.o.) ist es einfach, diesen Teil des Spams aufgrund von Schlüsselwörtern zu erkennen und zu filtern. Begriffe wie „Free porn“, „XXX“, „Warez“ oder auch „Get rich quick“ usw. kommen in der regulären Geschäftspost vermutlich selten vor. „Lernende“ Spam-Filter können zudem mit von Mitarbeitern identifiziertem Spam gefüttert werden, um auf diese Weise die „Spam Profile“ auf dem neusten Stand zu halten.

Viele erfahrene Email-Benutzer filtern seit Jahren auch auf die Verwendung von HTML, Javascript oder elektronischen Visitenkarten in Emails, da solche proprietären Zusätze häufig sowieso unerwünscht sind und überproportional häufig in Spam vorkommen. Manche gehen so weit, daß sie auf den in einer Email verwendeten Zeichensatz filtern. Ein guter Teil des Spams aus China und Korea kann z.B. aufgrund der Deklaration asiatischer Zeichensätze im Email Header identifiziert werden (natürlich nur empfehlenswert, so man keine elektronische Post aus den betreffenden Ländern erwartet).

Eine der neueren Entwicklungen im „content-based filtering“ ist „SpamNet“ [Clou03], ein verteilt operierendes Spam-Erkennungsnetz. Wo immer Spam innerhalb des P2P Netzes identifiziert wird, wird eine charakteristische Beschreibung des Spams erzeugt und durch das SpamNet propagiert. Anhand

dieser Beschreibung können andere Teilnehmer die bei ihnen ankommenden Instanzen des Spams identifizieren und ggf. filtern.

Herkunftsorientiertes Filtern („origin-based filtering“)

Häufig wird der Ursprung von Emails zum Bekämpfen von Spam genutzt. Viele Mail Server sind via DNS einer markanten Domain zugeordnet, die im Header von Email hinterlegt wird, oder sie verwenden bestimmte „HELO“ Zeichenketten beim Kontaktieren anderer Mail Server. „HELO“ dient eigentlich der Identifikation eines Mail Servers gegenüber einem anderen Server. Spammer nutzen gerne aus, daß diese Information leicht gefälscht werden kann.

Das folgende Beispiel eines nahezu zweifelsfrei von einem AOL Host verschickten Porno-Spams zeigt die angesprochenen Merkmale:

From: "hallo unbekannter" <lust_auf_mich2000@yahoo.de>
From lust_auf_mich2000@yahoo.de Tue Jan 14 16:42:11 2003
Return-Path: <lust_auf_mich2000@yahoo.de>
Subject: Betreff
Received: from mx0.gmx.de (HELO mx0.gmx.net) (213.165.64.100)
by [eigener Mail-Server] *with SMTP; 14 Jan 2003 16:42:10 -0000*
Received: from acb84c8a.ipt.aol.com (HELO mail.mailer.de)
(172.184.76.138)
by mx0.gmx.net (mx029-rz3) with SMTP; 14 Jan 2003 16:42:51 -0000
[Header gekürzt, Body gelöscht, relevante Stellen unterstrichen]

Dieser Spam ist ein Beispiel aus einer Serie von etwa tausend (1000) Spams, die den Header Daten nach allesamt über AOL Hosts verschickt wurden und dann von gmx.de an den eigentlichen Mail Account des Autors weitergeleitet wurden. AOL „Abuse“-Mitarbeiter und „Lotsen“ verneinten zwar regelmässig den AOL Ursprung, konnten aber auf Nachfrage keine Begründung liefern; gmx.de lies wiederholte Anfragen hinsichtlich einer Verifizierung des AOL Ursprungs unbeantwortet. Aufgrund der markanten HELO und „Betreff“ Zeichenketten sowie aufgrund des Versendens über Hosts der ebenfalls markanten Domain „ipt.aol.com“ hätte man diese Spams leicht filtern können. Lernende statistische Filter hätten vermutlich schnell einen Zusammenhang zwischen der Zeichenkette „HELO mail.mailer.de“ und Spam gefunden; die Stärke der Korrelation zwischen der Zeichenkette „ipt.aol.com“ und Spam würde insbesondere auch davon abhängen, wieviel reguläre Email via AOL empfangen wird (in diesem speziellen Fall sehr wenige im Vergleich zu der Spam Menge) und ob man ggf. das Risiko eingehen möchte, über AOL verschickte Email zu „verpassen“.

3.2.2 Blocken

Blocken bedeutet, daß der Betreiber einen Mail Server so konfiguriert, daß in Zukunft die Annahme jeglicher elektronischer Post von bestimmten anderen Mail-Servern verweigert. Typischerweise wird Blocken bei Mail-Servern angewendet,

die sich wiederholt als Quelle von Spam-Emails herausgestellt haben. Blocken kann noch verschärft werden, indem der eigene Mail Server den Spam Server bei der Kontaktaufnahme möglichst lange beschäftigt, obwohl die Mail-Annahme sowieso abgelehnt werden wird. Die Idee hinter einer solchen „Teergrube“ [Donn03] ist, daß (Übertragungs-)Zeit für Spammer eine äußerst wichtige und zudem leicht angreifbare Ressource ist.

Das Blocken von Mails von bestimmten Servern kann heutzutage vollautomatisch erfolgen, da Internet-Dienste wie die Spamhaus Block List (SBL) in Echtzeit abgefragt werden können. Die Betreiber der SBL fassen die Technik auf ihrer Web Site wie folgt zusammen [TSP03b]:

> „What does the SBL contain?
>
> The Spamhaus Block List (SBL) is a realtime database of IP addresses of static spam-sources, including known spammers, spam operations and spam support services. SBL listings are based in part on Spamhaus' Register of Known Spam Operations (ROKSO) database, spammers which Spamhaus believes are responsible for 90% of all American and European spam.“

4 Spam als Kostenfrage

Aus wirtschaftlicher Sicht sind bei Spam in erster Linie Kosten interessant. In den vergangenen Jahren gab es jedoch kaum wirtschaftliche Studien zum Thema Spam. Einer der Hauptgründe dürfte gewesen sein, daß Spam lange Zeit als „persönliches Ärgernis“ betrachtet wurde: das Löschen einzelner Spams (genauer: das Drücken der Lösch-Taste im Email-Programm), so nahm man an, würde ja nur Sekunden dauern. Aufgrund der schieren Menge des heutzutage verschickten Spams muß diese Kostenannahme allerdings verworfen werden.

4.1 Spam-Menge

Die Spam-Menge ist in den vergangen Jahren dramatisch angestiegen. Newsweek berichtete kürzlich [SL02], daß Spam 30-50% des gesamten Email Verkehrs ausmacht. Die Schätzung von 30% Spam wird auch von der Email Security Firma MessageLabs angegeben. Gemäß Heise [Heis03a] schätzt die Marktforschungs-firma zudem, daß Verbraucher im Jahre 2006 mit 206 Milliarden Junk Mails zugeschüttet werden. Pro Kopf bedeutet das etwa 1.400 Junk Mails pro Person (gegenüber 700 im Jahr 2002), wobei allerdings schon heute das Empfangen von etwa 100 Junk Mails pro Tag nicht ungewöhnlich ist.

Bei Firmen sah die Lage noch vor wenigen Jahren nicht ganz so dramatisch aus. In einer im Jahr 1998 veröffentlichten Studie von AT&T und Lucent Subdomains wurde befunden, daß im April des Jahres 2.5% aller Mails an die Domains als

Spam befunden wurden. Aufgrund dieser Zahlen schlußfolgerten sie, daß die damals aktuellen AOL Zahlen von 30% Spam mit Vorsicht zu genießen wären, da AOL Nutzer möglicherweise überdurchschnittlich viel Spam empfangen würden. Bis zum August des gleichen Jahres, dem Ende der Studie, hatte sich der Spam-Anteil allerdings auch bei den beobachteten AT&T und Lucent Subdomains auf 5% verdoppelt.

Inzwischen hat sich die Situation allerdings auch bei Firmen nachhaltig geändert. Marktforscher der Aberdeen Group [Aber02] schätzen, daß Spam in Firmen-Netzwerken von geschätzten 25% aller Emails im Jahr 2002 noch innerhalb des Jahres 2003 auf 50% steigen wird.

4.2 Spam-Kosten

In einer Studie von Ferris Research wird aufzeigt, daß die finanziellen Folgen der Spam-Flut alles andere als harmlos sind [Jesd03]: Ferris Research schätzt den durch Spam entstandenen Schaden auf 8.9 Milliarden USD für U.S.-amerikanische Firmen und auf weitere 2.5 Milliarden USD für europäische Firmen. Der Schaden für U.S.-amerikanische und europäische ISPs (Internet Service Provider) wird auf weitere 500 Millionen USD geschätzt. Ferris-Research-Mitarbeiter Marten Nelson hatte dabei angenommen, daß sich einzelne Spam-Mails normalerweise innerhalb einer Sekunde löschen lassen; dazu kommt Zeit für Spams, die nicht sofort als solche erkannt wurden, sowie Zeit für die Suche nach Emails, die irrtümlich als Spam klassifiziert worden sind und in Spam-Archiven gesucht werden müssen. Bei einer Gesamtschätzung von 4.4 Sekunden Arbeitsaufwand pro Spam-Mail kam Nelson für U.S.-amerikanische Firmen auf Produktivitätsverluste im Gegenwert von 4 Milliarden USD pro Jahr.

Ein nützlicher Ansatz ist, Kosten für Infrastruktur-Betreiber und Endbenutzer (sowohl Privatpersonen als auch Firmen) zu unterscheiden. Dabei sollte man allerdings nicht vergessen, daß Kosten zu Lasten derer, die die Netz-Infrastruktur betreiben, mittelbar an (End-)Benutzer weitergegeben werden. Kosten können z.B. durch höhere Mietpreise für Standleitungen und höhere Gebühren für Online-Zeit / Menge der übertragenen Daten weitergegeben werden.

4.2.1 Durch Spam verursachte Kosten (ISPs)

Wie bereits erwähnt schätzt Ferris Research den Schaden für U.S.-amerikanische und europäische ISPs (Internet Service Provider) auf 500 Millionen USD. [CAUCE03] schlüsselt Kosten für Internet Service Provider (ISP) auf:

> „For example, for an Internet Service Provider, „time“ includes the load on the processor in their mail servers; „CPU time“ is a precious commodity and processor performance is a critical issue for ISPs. When their CPUs are tied up processing spam, it creates a drag on all of the mail in that queue-- wanted and unwanted alike. This is

> also a problem with „filtering“ schemes; filtering email consumes vast amounts of CPU time and is the primary reason most ISPs cannot implement it as a strategy for eliminating junk email.
>
> The problem is also compounded by the fact that ISPs purchase bandwidth -- their connection to the rest of the Internet -- based on their projected usage by their prospective user base. For most small to mid-sized ISPs, bandwidth costs are among one of the greatest portions of their budget and contributes to the reason why many ISPs have a tiny profit margin. Without junk email, greater consumption of bandwidth would normally track with increased numbers of customers. However, when an outside entity (e.g., the junk emailer) begins to consume an ISP's bandwidth, the ISP has few choices: 1) let the paying customers cope with slower internet access, 2) eat the costs of increasing bandwidth, or 3) raise rates. In short, the recipients are still forced to bear costs that the advertiser has avoided.“

Die wichtigsten Punkte sind, daß Spam bei ISPs sowohl bei der Rechnerausstattung als auch bei der Anbindung ans Internet durch Spam verursachte Kosten anfallen. Dazu kommen typischerweise weitere Kosten wie Installationskosten, weitere/teurere Wartungsverträge und neue Software.

4.2.2 Durch Spam verursachte Kosten (Endbenutzer)

In diesem Beitrag betrachte ich lediglich Kosten für Firmen. Die Kosten für Privatpersonen werde ich von daher im folgenden vernachlässigen.

Aufgrund der deutlich erhöhten Datenmenge (wie bereits erwähnt, macht Spam bereits im Jahre 2002 geschätzte 25% aller Firmen-Email aus und es wird erwartet, daß der Anteil noch innerhalb des Jahres 2003 auf 50% steigen wird) erfordert Spam wie bei den ISPs leistungsfähigere Rechner und „dickere“ Leitungen zum Internet. Dazu kommen ebenfalls weitere Kosten wie Installationskosten, weitere/teurere Wartungsverträge und neue Software.

Maßnahmen zum Schutz gegen Spam verursachen weitere Kosten wie etwa Kosten für Produkte wie das von dem Viren-Spezialisten McAfee angekündigte „SpamKiller Enterprise“ oder auch Cloudmarks „Authority“ (SpamNet). Der Einsatz von Anti-Spam Software wie z.B. Filter-Software erfordert häufig leistungsfähigere Hardware/Software (Filtern ist Rechenzeit-intensiv) mit entsprechenden Installations- und Wartungskosten. Bei größeren Firmen mit eigenen Mail Servern können zudem Kosten anfallen für das „Abdichten“ der Server gegen Wörterbuch-basierte Angriffe (i.allg. durch Blocken von Servern, die zu viele nicht-existierende Mail Adressen innerhalb einer bestimmten Zeitspanne ansprechen).

Finanziell gesehen haben inhaltsorientierte Filter-Ansätze den Nachteil, daß die zu überprüfenden Emails --und damit auch der Spam-- erst einmal ins Firmennetz übertragen werden müssen, damit überhaupt eine Überprüfung vorgenommen werden kann. Die Datenübertragungsmenge verringert sich also üblicherweise nicht.

Die von Ferris Research geschätzten Kosten von 8.9 Milliarden USD für U.S.-amerikanische Firmen wurden bereits erwähnt. In [Cran98] wird zudem der Zeitaufwand für das Pflegen von Filtern mit 4-20 Administrator-Stunden pro Woche angegeben.

Maßnahmen wie etwa das Blocken von Spam-verdächtigen Mail Servern aufgrund von Realtime Blacklists wie der SBL [TSP03b] erfordern erhebliches technisches Fachwissen. Der Einsatz solcher Mittel sollte auch nicht ohne entsprechende Richtlinien und „Policies“ geschehen, und sollte in passende Reporting Prozesse eingebunden sein, so daß das Management ggf. richtungweisend eingreifen kann.

4.2.3 Weitere Kosten

Die beiden wichtigsten Anti-Spam-Maßnahmen, „content-based filtering“ und „origin-based filtering“, könnten den diskutierten Spam zwar komplett verhindern, aber der Schaden wäre möglicherweise nicht unerheblich. Eine Reduktion ist allerdings durchaus machbar: „Content-based filtering“ kann z.B. Begriffe wie 0190-Nummern und pornographische Begriffe zur Spam-Identifikation benutzen. 0190-Nummern können allerdings auch Service-Nummern von Kunden sein. Pornographische Begriffe oder Schimpfwörter scheinen ein sicheres Maß zu sein, aber längst nicht alle angesprochenen Spams enthalten solche Begriffe. Abgesehen davon zeigt die betriebliche Realität, daß gewisse Begriffe auch so in der Mitarbeiter-Post vorkommen können. Filtern solcher Emails könnte das wichtige „Socializing“ negativ beeinflussen.

„Origin-based filtering“ wäre noch problematischer. Filtern auf den AOL Ursprung bzw. auf die Zeichenkette „ipt.aol.com“ des schon diskutierten Spam-Beispiels würde zwar den Großteil dieser Spam-Welle erwischen, aber es kann kaum eine Firma ausschließen, daß einer ihrer Kunden oder Mitarbeiter Email über einen der weltweit größten ISPs verschickt.

Bei Maßnahmen wie dem Blocken von externen Mail Servern aufgrund von Eintragungen in Real Time Blacklists verringert sich die Netzlast, da Spam gar nicht erst übertragen wird. Der große Nachteil dieser Block-Ansätze ist, daß unter Umständen auch legitime Geschäftspost, die über Spam-freundliche ISPs verschickt wurde, nicht mehr zugestellt werden kann. Häufig sind sich Geschäftskunden nicht über den „Ruf“ ihres ISPs im Klaren. Das unerwartete Blocken kann insbesondere dann passieren, wenn der besseren Handhabbarkeit wegen ganze Teilnetze großer Spam-freundlicher ISPs geblockt werden und kleinere ISPs in einem dieser Teilnetze angesiedelt sind.

Die Betreiber der SBL [TSP03b] thematisieren das Problem wie folgt:

> „Can the SBL block legitimate email?
>
> The SBL's primary objective is to avoid 'collateral damage' while blocking as much spam as possible. However, like any system used to filter email, the SBL has the

> potential to block items of legitimate email if they are sent from an IP under the control of a spammer or via IPs belonging to spam support services. The chances of legitimate email coming from such IPs are slim, but need to be acknowledged."

Des weiteren kann es aus den eben geschilderten Gründen auch ohne firmeneigene aktive Nutzung von Real Time Blacklists zu Mail-Verlusten kommen, da Mail auf dem Weg zwischen dem Kunden-Mail Server und dem eigenen Mail Server auf sogenannten Relay-Servern geblockt werden kann.

Realistisch betrachtet muß man auch davon ausgehen, daß bei Anti-Spam-Maßnahmen Fehler auftreten können. Bei der inhaltsorientierten Überprüfung von Emails muß z.B. mit „Falsch-Richtigen" gerechnet werden. Falsch-richtig bedeutet in diesem Fall, daß eine Email als Spam behandelt wird, obwohl es in Wirklichkeit kein Spam ist. [Heis03b] hatte z.B. berichtet, daß ein E-Mail-Filter, der Abgeordnete des britischen Unterhauses vor Porno-Spam schützen sollte, Diskussionspapiere zum so genannten Sexual Offences Bill blockiert habe. Diese Vorfälle zeigen, daß es betriebsinterne Prozesse geben sollte, die die Auswirkungen auch jenseits der Falsch-positiv/negativ Ratio von Anti-Spam-Maßnahmen regelmäßig überprüfen. Die in dem Heise Artikel zitierte Lösung, „ein Anruf würde genügen, um eine versehentlich blockierte Mail weiterzuleiten", ist sicherlich untragbar im Geschäftsbetrieb.

5 Forschungsrichtung: Spezifische Auswirkungen von Anti-Spam-Maßnahmen

Bei genauerer Betrachtung von (traditionellen) Anti-Spam-Maßnahmen im vorausgehenden Abschnitt hat sich gezeigt, daß es beim Einsatz solcher Maßnahmen keinen „free ride" gibt. Gewisse Vorteile werden immer mit gewissen Nachteilen erkauft.

Während Fehler bei Privatpersonen eine persönliche Ermessensfrage sind, setzen geschäftliche Interessen häufig andere Schwerpunkte: Das Blocken der Email eines Geschäftspartners oder einer Anfrage eines potentiellen Kunden aufgrund falsch-positiver Erkennung als Spam dürfte in den meisten Fällen geschäftsschädigend sein.

Ein bisher in der Literatur wenig thematisiertes Problem ist die Konfrontation von Mitarbeitern mit Pornographie, die per Spam zugestellt wurde. Falls eine Firma Spam-Filter einsetzt, könnte das möglicherweise so interpretiert werden, daß die Firma als Herausgeber gilt und für Inhalte haftbar gemacht werden kann (im Gegensatz zu ISPs, die Daten lediglich „durchschleusen"). Da hier wiederum national gültige Gesetze zur Anwendung kommen, müßte diese Problematik länderspezifisch diskutiert werden.

Angesichts der in diesem Beitrag wiederholt deutlich gewordenen Nachteile von Anti-Spam-Maßnahmen stellt sich zum einen die Frage, wie die Nebeneffekte solcher Maßnahmen im betrieblichen Alltag behandelt werden. Zudem stellt sich die Frage nach Alternativen zu den „traditionellen“ Anti-Spam-Maßnahmen.

5.1 Traditionelle Anti-Spam-Maßnahmen

Firmen müssen sich darüber im Klaren sein, daß der Einsatz von Anti-Spam-Maßnahmen unmittelbar den „Lebenssaft“ von Unternehmen betrifft, da heutzutage ein bedeutender Teil der (externen) Unternehmenskommunikation über Email abgewickelt wird. Das bedeutet, daß es sich kein Unternehmen leisten kann, Anti-Spam-Maßnahmen einzusetzen, ohne daß die verantwortlichen Mitarbeiter genauestens im Bilde sind über Nutzbarkeit, Verläßlichkeit, sowie Vor- und Nachteile. Der Einsatz solcher Mittel sollte auch nicht ohne entsprechende Richtlinien und „Policies“ geschehen, und sollte in passende Reporting Prozesse eingebunden sein, so daß das Management ggf. richtungsweisend eingreifen kann. Hier ist es wichtig zu erwähnen, daß [LS00] in einer Studie zum Thema Sicherheit beobachtet haben, daß Sicherheits-relevantes Wissen auf unteren Hierarchie vorhanden sein kann, aber trotzdem nicht zu den Führungsebenen gelangt. Solche Blockaden müssen sowohl im Bereich Sicherheit als auch im Bereich Anti-Spam-Maßnahmen verhindert werden.

Mir sind bisher weder an den betrieblichen Bedürfnissen orientierte Aufstellungen über die Nutzbarkeit, Verläßlichkeit sowie die spezifischen Vor- und Nachteile von Anti-Spam-Maßnahmen bekannt, noch scheint es Literatur zu geben, die den Einsatz von Anti-Spam-Maßnahmen im Kontext von Richtlinien, „Policies“ und „Reporting“ Prozessen diskutiert. Hier besteht sicherlich Nachholbedarf sowohl aus der Sicht der Betriebe als auch aus der Sicht der Wirtschaftsinformatik.

5.2 Alternative Ansätze

In der einschlägigen Literatur gibt es eine Reihe von alternativen Ansätzen zur Bekämpfung des Spam-Problems:

- „Kostenverrechnung“ für Unterbrechungen

  [Fahl02] diskutiert ein allgemeines Modell, bei dem die Versender von Botschaften (Email, Fax, Telephon etc.) „Unterbrechungsrechte“ erwerben müssen. Spamming dürfte aufgrund der entstehenden Kosten abnehmen.

- Unterbrechungen gegen Rechenleistung

  [DwNa93] diskutieren einen Ansatz, bei dem Versender von Nachrichten hinreichend komplizierte „pricing“ Funktionen berechnen müssen, um ein Token zu erhalten, das sie für den erfolgreichen Aufbau der Kommunikation

benötigen. Spammern dürfte es an den erforderlichen Rechenkapazitäten fehlen. [DwNa93] geben keine anderweitig sinnvolle Verwendung der Rechenzeit an, aber man könnte sich das Berechnen einer Einheit bei einem verteilten gemeinnützigen Rechennetz ähnlich SETI@Home vorstellen. SETI@Home ist ein Projekt, das massiv verteiltes Rechnen zur Analyse von Radiosignalen aus dem Weltraum nutzt.

- „Communication Channels“

  [Hall98] diskutiert ein Konzept, bei dem Benutzer eine Vielzahl von Kommunikationskanälen einrichten und diese mit unterschiedlichen Prioritäten versehen.

All diesen Ansätzen ist gemeinsam, daß sie zwar theoretisch interessant, aber für den Einsatz im Unternehmen (noch) ungeeignet sind, da sie noch nicht unter realistischen Bedingungen überprüft worden sind und zudem von der Existenz einer speziellen technischen Infrastruktur abhängen (z.B. Verfügbarkeit von Email-Programmen, die den Erwerb von „Unterbrechungsrechten“ ermöglichen).

Eine alternative Herangehensweise zur Minderung des Spam-Problems wäre das Verleihen eines „Gütesiegels“ für geschäftstaugliche ISPs. Hier ergibt sich allerdings wieder das Problem, daß Spammer sich typischerweise als respektable Geschäftskunden ausgeben. Zudem ergäben sich weitere Probleme wie das kontinuierliche Überprüfen der Geschäftstauglichkeit, das Behandeln geschäftstauglicher ISPs, die in als „unbekannt“ oder gar „unzuverlässig“ eingestuften Teilnetzen größerer Netz-Betreiber liegen.

5.3 Gesellschaftliche Auswirkungen von Anti-Spam Maßnahmen

Wie bereits erwähnt, ist es bei Spammern nicht unüblich, daß sie ihren Firmensitz in Drittländer wie Gibraltar verlagern und ihren Spam über Mail-Server verschicken, die in Ländern stehen, die entweder nicht willens oder nicht in der Lage sind, effektiv gegen Spam vorzugehen. Des weiteren gibt es Anzeichen („anecdotal evidence“ aus den Usenet Diskussionsgruppen zum Thema Email-Mißbrauch) dafür, daß zumindest erfahrene Email-Benutzer schon seit Jahren auf den in einer Email verwendeten Zeichensatz und andere regionale Kennzeichen filtern, da ein erheblicher Teil des Spams aus China und Korea kommt und Mails aus diesen Ländern kommt. Die Deklaration asiatischer Zeichensätze im Email Header ist ein relativ verläßlicher Weg, Email aus China und Korea als solche zu identifizieren. Während das Filtern ganzer Länder oder Regionen auf der Ebene des Individuums harmlos zu sein scheint, solange es eher die Ausnahme als die Regel ist, stellt sich die Frage, wie es sich verhält, wenn größere Firmen, Organisationen oder sogar ISPs Länder-orientiert filtern würden.

Eine länderspezifische Aufschlüsselung von Einträgen in Real Time Blacklists liegt bisher nicht vor, aber es gibt neben „anecdotal evidence“ auch deutlichere Anzeichen dafür, daß diese Filterpraxis bereits Realität sein könnte. Der U.S.-basierte Spam-Filter-Dienst SpamStopsHere etwa erwähnt auf seiner Web Site als besondere Stärke, daß der Dienst ganze Länder blocken kann: „[b]locks entire countries notorious for sending spam, e.g. China and Brazil.“ [SSH03]. Auf einer anderen Seite der Web Site empfiehlt SpamStopsHere das Blocken von Argentinien, Brasilien, Hongkong, Malaysia, Nigeria, Russland, Thailand, and Singapur. Das Blocken von China, Korea und Taiwan ist sogar „Highly recommended“.

Das Blocken Spam-freundlicher ISPs ist nicht ungewöhnlich, aber das Blocken ganzer Länder oder Regionen stellt die Frage nach einem weiteren „Digital Divide“, der diesmal von Anti-Spam-Maßnahmen (mit-)verursacht würde [Lueg03]. Nach [Cast01, S. 248] ist „Digital Divide“ ist ein Begriff, der Ungleichheiten beim Zugriff auf das Internet beschreibt. Während sich der „traditionelle” Digital Divide eher auf wirtschaftlich und gesellschaftlich bedingte Zugangsbeschränkungen bezieht, könnte sich der neue Digital Divide dadurch manifestieren, daß gewisse Länder und Regionen zwar über den für die Teilnahme am weltweitem Email-Verkehr notwendigen Internet-Zugang verfügen, aber faktisch dennoch nicht teilnehmen können, da ein Großteil ihrer ihrer Emails in den Industrieländern geblockt oder gefiltert würde. Hier ist sicherlich die internationale Politik gefordert, auch wenn wohl kurzfristig keine Lösungen zu erwarten sind angesichts der Beobachtung, daß sogar Industrieländer wie Australien, Deutschland und die U.S.A. Jahre gebraucht haben für erste Schritte in Richtung legislativer Maßnahmen gegen Spam. In diesen Ländern dürfte der wirtschaftliche Schaden eine treibende Kraft darstellen, während das Tolerieren oder Erlauben von Spamming für wirtschaftlich schwache Länder eine leicht erreichbare Einnahmequelle darstellen könnte.

6 Schlußfolgerungen

Firmen müssen sich darüber im Klaren sein, daß der Einsatz von Anti-Spam-Maßnahmen unmittelbar den „Lebenssaft“ von Unternehmen betrifft, da in der heutigen Zeit ein bedeutender Teil der Unternehmenskommunikation über Email abgewickelt wird. Das bedeutet, daß es sich kein Unternehmen leisten kann, Anti-Spam-Maßnahmen einzusetzen, ohne daß die verantwortlichen Mitarbeiter genauestens im Bilde sind über Nutzbarkeit, Verläßlichkeit sowie andere spezifische Vor- und Nachteile. Der Einsatz solcher Mittel sollte auch nicht ohne entsprechende Richtlinien und „Policies“ geschehen, und sollte in passende Berichterstattungsprozesse eingebunden sein, so daß das Management ggf.

richtungweisend eingreifen kann. Anti-Spam-Maßnahmen sollten nicht nur auf der Ebene von Technikern entschieden werden.

Auch wenn der Schwerpunkt dieses Beitrages auf technischen Aspekten von Anti-Spam-Maßnahmen lag, dürfte dennoch deutlich geworden sein, daß das Verstehen von Spam und Anti-Spam-Maßnahmen Wissen aus einer Vielzahl von Disziplinen von Informatik zu Wirtschaftswissenschaften und Jura betrifft. Damit ist die Wirtschaftsinformatik als stark interdisziplinäre Forschungsrichtung prädestiniert für den Aufbau eines umfassenden und vielschichtigen Verständnisses der notwendigen und betrieblich vertretbaren Maßnahmen.

Das Andiskutieren möglicher gesellschaftlicher Folgen des großflächigen Einsatzes von Anti-Spam-Maßnahmen deutet darauf hin, daß Bemühungen um das Verstehen von Anti-Spam-Maßnahmen weit über wirtschaftliche Aspekte hinausgehen sollten. Auch hier könnte die Wirtschaftsinformatik wiederum eine Brückenfunktion zwischen den verschiedenen Disziplinen einnehmen.

7 Danksagungen

Die detaillierten Kommentare der anonymen Gutachter waren außerordentlich hilfreich bei der Überarbeitung dieses Beitrages. Beiträge in den Usenet Diskussionsgruppen zum Thema Netz-Mißbrauch, insbesondere de.admin.net-abuse.mail und de.admin.net-abuse.news, haben mir nicht nur einmal beim Verständnis aktueller Entwicklungen und Hintergründe im Bereich Spamming geholfen.

Literatur

[Aber02] Aberdeen Group 2002: 2003: Predictions for Security and Privacy. Artikel verfügbar unter URL http://www.aberdeen.com/ab%5Fcompany/researchareas/security2003.htm, Abruf am 2003-01-13.

[Base03] Baseley, W. D.: The Email Abuse FAQ (last updated June 25, 1998) Artikel verfügbar unter URL http://members.aol.com/emailfaq/emailfaq.html, Abruf am 2003-01-13, oder in den Usenet newsgroups news.admin.net-abuse.email, news.answers.

[Brig02] Press Release: Brightmail Reveals Annual Top 10 Spam Messages for 2002. Artikel verfügbar unter URL http://www.brightmail.com/pressreleases/121202_top_spam.html, Abruf am 2003-01-10.

[Cast01] Castells, M.: *The Internet galaxy. Reflections on the Internet, Business and Society*. Oxford University Press, Oxford, UK.

[CAUCE03] Coalition Against Unsolicited Commercial Email (CAUCE). The Problem. Artikel verfügbar unter URL http://www.cauce.org/about/problem.shtml, Abruf am 2003-01-10.

[Clou03] SpamNet http://www.cloudmark.com/products/spamnet/, Abruf am 2003-01-10.

[Cran98] Cranor, L.F., LaMacchia, B.A. Spam! *Communications of the ACM* Volume 41, No 8, S. 74-83.

[Donn03] Donnerhacke, L. Teergruben FAQ. Artikel verfügbar unter URL http://www.iks-jena.de/mitarb/lutz/usenet/teergrube.html, Abruf am 2003-01-10.

[DwNa93] Dwork, C., Naor, K.: Pricing via processing: combatting junk mail. *Advances in Cryptology - 1992. Lecture Notes in Computer Science 740, Springer-Verlag, S. 139-147.*

[Fahl02] Fahlman, S. E.: Selling interrupt rights: a way to control unwanted e-mail and telephone calls. *IBM Systems Journal* Vol 41, No 4, 2002, S. 759-766.

[Falk03] Falk, J.D.: The Net Abuse FAQ. Artikel verfügbar unter URL http://www.cybernothing.org/faqs/net-abuse-faq.html, Abruf am 2003-01-13.

[FTC03] U.S. Federal Trade Commission: False claims in spam. A report by the FTC's division of marketing practices. Released April 30, 2003. Available at http://www.ftc.gov/reports/spam/030429spamreport.pdf, Abruf am 2003-03-05.

[Hall98] Hall, R. Channels: avoiding unwanted electronic mail. *Communications of the ACM* Volume 41, No 3.

[Heid03] Heidrich, J.: Gesetzes-Novelle mit Schwachstellen beim Spam-Schutz. *c't aktuell* - Meldung vom 08.05.2003. Artikel verfügbar unter URL http://www.heise.de/ct/aktuell/data/jo-08.05.03-000/, Abruf am 2003-05-12.

[Heis03a] Heise Online News vom 04.01.2003: Spam belastet Europas Unternehmen. Artikel verfügbar unter URL http://www.heise.de/newsticker/data/ae-04.01.03-003/, Abruf am 2003-01-13.

[Heis03b] Heise Online News vom 09.02.2003: Spam-Filter verärgert britische Abgeordnete. Artikel verfügbar unter URL http://www.heise.de/newsticker/data/wst-09.02.03-003/, Abruf am 2003-02-09.

[Jesd03] Jesdanun, A.: Study Says Spam Costs U.S. Businesses $8.9 Billion. *InformationWeek* Jan. 3, 2003. Artikel verfügbar unter URL http://www.information week.com/story/IWK20030103S0004, Abruf am 2003-01-10.

[LS00] Lichtenstein, S. und Swatman, P.: Issues in e-business security management and policy. In *Proceedings of the 1st Australian Information Security Management Workshop*, 2000.

[Lueg03] Lueg, C.: A look at wider impacts of spam and anti-spam measures. Zur Veröffentlichung einreicht.

[Muel03] Mueller, S. H.: What is Spam? http://spam.abuse.net/overview/whatis spam.shtml, Abruf am 2003-01-13.

[MIT03] Spam Conference http://spamconference.org/, Abruf am 2003-01-13.

[NOIE02] Australian National Office for the Information Economy: Final report of the NOIE review of the spam problem and how it can be countered. Report available at http://www.noie.gov.au/projects/confidence/Improving/Spam/Interim_Report/contents.htm, Abruf am 2003-05-03.

[SL02] Stone, B. and Lin, J: Spamming the World. *Newsweek* August 19, S. 40-42.

[SSH03] SpamStopsHere http://www.spamstopshere.com/, Abruf am 2003-05-03.

[TSP03a] The Spamhaus Project: Spammers Grab Hotmail and MSN addresses. Artikel verfügbar unter URL http://www.spamhaus.org/newsdog.lasso?article=114, Abruf am 2003-01-13.

[TSP03b] The Spamhaus Project. The Spamhaus Block List (SBL) Advisory Frequently Asked Questions. Artikel verfügbar unter URL http://www.spamhaus.org/sbl/sbl-faqs.lasso, Abruf am 2003-01-13.

[Wend02] Wendlandt, B.: Cybersquatting, Metatags und Spam. Beck Juristischer Verlag. ISBN 3406489176.