Anti-Spam Technologie

Prof. Dr. Norbert Pohlmann
Fachhochschule Gelsenkirchen
Fachbereich Informatik
Neidenburger Straße 43
45877 Gelsenkirchen

norbert.pohlmann@informatik.fh-gelsenkirchen.de

Zusammenfassung

E-Mail, die elektronische Post, ist die am häufigsten genutzte Anwendung im Internet und von daher für die Informationsgesellschaft ein nicht mehr wegzudenkender Service. SPAM-Mails, unerwünschte Werbe-Mails, sind ein ernsthaftes Problem mit hohem Schaden. Die positive Nutzung von E-Mails und damit die Informationsgesellschaft sind gefährdet. In diesem Artikel wird das Problem von SPAM-Mails und die möglichen unterschiedlichen Maßnahmen, das Problem zu bewältigen, beschrieben und deren Wirkung diskutiert.

1 Definition und Hintergründe von SPAM-Mails

SPAM-Mails sind "unerwünscht" oder "unverlangt" zugesandte E-Mails. Die E-Mails können als "Massenware" - Unsolicited Bulk E-Mail (UBE) - oder als personalisierte Werbemails auftreten. Die im Internetjargon als SPAM (SPiced HAM - weitverbreitetes amerikanisches Frühstücksfleich in Dosen, welches den Empfängern massenhaft unverlangt zugesandt wurde) oder offiziell als "unsoliceted commercial e-mail" (UCE, unerwünschte Werbemails) bezeichnet werden, stellen für die Verwendung des Internets, insbesondere im Geschäftsbereich, ein ernsthaftes Problem dar. Von derzeit ca. 30 Milliarden E-Mails pro Tag werden ein sehr hoher Prozentsatz als SPAM-Mails eingestuft [Grou03]. Prognosen zeigen auf, dass sich der Anteil von SPAM-Mails zukünftig noch weiter erhöhen wird (siehe Tabelle IDC-Studie) [Herr03].

	1996	1999	2002	2006
Geschäftlich	130 Mrd.	920 Mrd.	3.330 Mrd.	5.580 Mrd.
Privat	100 Mrd.	660 Mrd.	2.150 Mrd.	3.570 Mrd.
Gesamt	230 Mrd.	1.580 Mrd.	5.480 Mrd.	9.150 Mrd.
Davon SPAM	50 Mrd.	290 Mrd.	1.500 Mrd.	2.920 Mrd.

Tab. 1: IDC E-Mail Usage Forcast 2002-2006

Die unternehmensspezifische "Belästigungsrate" kann jedoch individuell sehr viel höher sein. Trotz aller Versuche, die Werbemail-Flut mit juristischen Mitteln in den Griff zu bekommen, wird der Einsatz von Anti-SPAM Technologie angeraten, um SPAM-Mails schnell und wirksam zu blockieren, da die rechtlichen Grundlagen für den Versand von E-Mail-Werbung international nicht einheitlich geregelt sind. In Deutschland und anderen EU-Ländern werden verschiedene Gesetze und Verordnungen berührt. Hierzu gehören die Telekommunikations- und Datenschutzgesetze sowie das Wettbewerbs- und das Medienrecht. Von den Gerichten wird unerwünschte Werbung per Fax, E-Mail oder per SMS auf das Handy als Verletzung der Persönlichkeitsrechte des Empfängers eingestuft. Kunden müssen demnach ausdrücklich zustimmen, dass sie die Werbung erhalten möchten. Da jedoch fast 60 Prozent der SPAM-Mails aus den USA kommen, lässt sich das Problem auf diese Weise z.Z. nur unzureichend lösen [Pohl03].

Abb. 1: Die SPAM-Flut

Motivation von SPAM-Mails

Im Gegensatz zur normalen Werbepost werden bei SPAM die Kosten vom Anbieter zum Empfänger verschoben. Im Vergleich zur Werbepost im Briefkasten ist der Versand von Millionen von E-Mails mit geringen Kosten für den Absender machbar.

Selbst wenn nur jeder zehntausendste Adressat einer SPAM-Mail Kunde wird, sind das 100 erfolgreiche Geschäftsabschlüsse pro Million versandter SPAM-Mails - da der Versand von Mails nahezu nichts kostet, lohnt das Geschäft also immer noch.

Zahlenbeispiel: SPAM-Mails - Papierwerbung

SPAM-Mails: kosten ca. 250 € pro Million Mails mit einer Erfolgsrate von 0,1 %

Eine Antwort auf eine SPAM kostet ca. €250/1000 = 0.25 €

Papierwerbung: kostet etwa 0.25 € pro Stück und hat eine Erfolgsrate von 5%.

Eine Antwort auf Papierwerbung kostet ca. €0.25/0.05 = 5 €

Diese Zahlenbeispiel zeigt auf, dass Werbung per E-Mail zur Zeit sehr viel Preisgünstiger ist als Papierwerbung!

E-Mail-Adressen für SPAM-Mails

Die Versender von SPAM-Mails nutzen verschiedene Wege, um an ihre Adressen zu gelangen. So gibt es international einen lebhaften Handel mit Adresslisten oder es werden sogenannte Robots als Suchprogramme eingesetzt, die aus News-Groups, Foren und Webseiten das Adressmaterial sammeln. Weitere beliebte Quellen sind Online-Gewinnspiele, Nachrichtendienstabonnements oder Mailing-Listen für Newsletter-Versand.

Besondere Probleme des Internets bezüglich SPAM-Mails

- Das Internet ist ein offenes System, jeder kann jedem etwas senden.
- Der Dienst E-Mail muss nicht besonders bezahlt werden.
- Das Internet geht über alle geographischen und politischen Grenzen, Gesetze und Kulturen hinaus und stellt somit eine neue und ungewohnte Herausforderung für die internationale Gesellschaft dar.
- Die Herkunft der SPAM-Mails ist schwer identifizierbar, da die Adressen, mit denen Spammer arbeiten, oftmals nicht existent oder gefälscht sind.

2 Schäden, die durch SPAM-Mails auftreten

Die durch SPAM-Mails entstehenden Schäden sind zum Teil nicht exakt bezifferbar. Sie lassen sich jedoch in folgende Bereiche grob unterteilen:

- Arbeitszeitverlust
  Zum Erkennen von SPAM-Mails müssen die Mitarbeiter eine E-Mail zumindest kurz anlesen. Besonders bei professionell gestalteten Werbemails entsteht ein höherer Zeitaufwand für die manuelle Erkennung, da die Werbung oft nicht leicht zu erkennen ist. Verbunden mit der Echtzeitsignalisierung moderner E-Mail-Clients wie Outlook oder Notes kommt es zu permanenter Ablenkung und Zeitverlusten. Außerdem müssen die E-Mails noch aussortiert und/oder gelöscht werden. Der Zeitaufwand zum Trennen relevanter (gewollter) E-Mail von SPAM-Mail ist erheblich und birgt zusätzlich die Gefahr, dass wichtige E-Mails im Müllberg untergehen.
- Speicherverbrauch
  Die Speicherkapazitäten von E-Mail-Servern und Archivierungssystemen werden durch SPAM-Mails massiv beansprucht. Durch die große Anzahl von Werbemails verbunden mit vielen Empfängern kommt es zu einer hohen Auslastung der Speicherkapazitäten mit eigentlich unerwünschten Daten (SPAM-Mails).
- Bandbreitenverbrauch
  Dadurch, dass mehr E-Mails übertragen werden "müssen", ist es erforderlich, für eine entsprechende höhere Bandbreite für E-Mails zu sorgen, die letztendlich höhere Kosten verursacht. Mobile Benutzer, die oft nur über eine schmalbandige und volumenbegrenzte Verbindung verfügen, erfahren die Auswirkungen von SPAM-Mails am deutlichsten.

- Sicherheitsprobleme
  Durch SPAM-Mails drohen in erhöhtem Maße Schäden durch Computerviren, Würmer und Trojaner.
- Mail-Server lahmlegen
  Spammer nutzen immer häufiger frei erfundene Absenderadressen aus existierenden Domains. In der Folge verstopfen Rückläufer wie Fehlermeldungen von anderen Mailservern die Postfächer des absichtlich fälschlich angegebenen Absenders. Im Extremfall kann die Zahl der eintreffenden Rückläufer an einem Tag in die Hunderttausende gehen und z.B. den eigenen Mailserver, der vom Spammer als Absender verwendet wird, lahmlegen.
- Reputation
  Wenn die Adresse des eigenen Mail-Servers von einem fremden Spammer angegeben wird und z.B. SPAM-Mail Artikel bewerben, die dem eigenen Ruf schaden können (z.B. Pornographie, Gewalt, usw.), kann ein nicht unerheblicher Schaden auftreten.
- Nutzbarkeit
  Falls das Problem SPAM-Mails nicht eingeschränkt werden kann, wird die Verwendung von E-Mails über das Internet nicht mehr sinnvoll möglich sein, und dadurch ein nicht unerheblicher Schaden für die meisten Unternehmen auftreten.

Wirtschaftlicher Schaden durch SPAM-Mails

Die negativen Auswirkungen durch SPAM-Werbemüll auf die Wirtschaft sind beträchtlich.

In amerikanischen Unternehmen und bei Internet-Serviceprovidern beläuft sich der durchschnittliche SPAM-Anteil auf rund 30 Prozent aller E-Mails. Die Kosten, die der US-Wirtschaft in diesem Jahr durch die unerwünschte Post entstehen, werden auf ca. zehn Milliarden Dollar geschätzt. Bei europäischen Unternehmen verursachen SPAM-Mails Produktivitätseinbußen in Höhe von mehr als 2,5 Milliarden Euro.

In Deutschland ergab eine kürzlich von der IDC-Marktforschung durchgeführte Umfrage unter IT-Verantwortlichen, dass der SPAM-Anteil an den erhaltenen E-Mails bei einem Drittel der IT-Verantwortlichen mehr als die Hälfte ausmacht. Für ein Unternehmen mit 500 E-Mail-Accounts und täglich durchschnittlich vier SPAM-Mails pro Empfänger wurden Produktivitätsverluste durch die elektronische Werbepost mit einem finanziellen Schaden von mehr als 60.000 Euro pro Monat errechnet (1 € pro SPAM-Mail).

3 Verfahren zur Erkennung und Verhinderung von SPAM-Mails

Im folgenden Abschnitt werden grundsätzliche Methoden dargestellt, mit denen SPAM-Mails erkannt und/oder verhindert werden können.

Abb. 2: Das Produkt, welches den Namen gab (siehe www.spam.com)

Generell lassen sich SPAM-Mails mit modernen Filtertechnologien (Inhaltsfilter, regelbasierte Filter sowie verteilte Prüfsummenfilter), Adressvalidierung und Protokollmodifikationen (Verwendung von inverse DNS, AUTH, usw.) erkennen und verhindern.

3.1 Mechanismen zum Erkennen von SPAM-Mails

Bei der Erkennung von SPAM-Mails ist im Detail zu entscheiden, ob SPAM-Mails bereits am Mailserver oder erst am Client herausgefiltert oder blockiert werden sollen. Für mittlere und größere Unternehmen ist eine zentrale Server- oder Gatewaylösung meistens die einzige pragmatische Alternative. Kleinunternehmen, welche keine eigene E-Mail-Infrastruktur betreiben, sind mit Clientlösungen oder Services von E-Mail-Dienstleistern (z.B. GMX) gut gerüstet.

Modernste Anti-SPAM Technologien realisieren die SPAM-Abwehr durch einen mehrstufigen Prozess. Im Kern werden die folgenden technischen Mechanismen unterschieden, die auch in Kombination und gestaffelt verwendet werden können:

- E-Mail-Kopfzeilen Analyse und Strukturanalyse.

Jede E-Mail enthält neben den sichtbaren Informationen eine Vielzahl von Kontroll- und Steuerungsfeldern für das E-Mail-Routing durch das Internet, die im E-Mail-Kopf enthalten sind. Anhand dieser Informationen lässt sich z.B. die Route einer E-Mail vom Absender bis zum Empfänger nachvollziehen. Versender von SPAM-Mails manipulieren die Kontrollfelder, um sich der Verfolgung zu entziehen. So werden beispielsweise Informationen zum Quell-Mailserver verändert, um die Rückverfolgung zum Absender zu erschweren.

Verfahren zur E-Mail-Kopfzeilen Analyse untersuchen die Kontrollinformationen auf Konsistenz und Vollständigkeit. Die Prüfung von erweiterten Informationen in den E-Mail-Kopfzeilen (Header) auf Konsistenz erlaubt das gezielte Erkennen von E-Mails, welche nicht von Standard E-Mail-Systemen wie Microsoft Exchange, Lotus Domino, usw. versendet wurden. Wird eine oder mehrere Unregelmäßigkeiten erkannt, so werden diese mit einem Rating versehen. Voraussetzung für eine hohe Erkennungsrate ist ein feinabgestimmtes Rating der einzelnen Merkmale.

Bei der Strukturanalyse wird überprüft, ob der E-Mail-Nachrichtentext (Body) eine Kombination von unerwünschten HTML-Tags und Skripten enthält.

- Textanalyse durch gewichtete Wortlisten in Betreff und Nachrichtentext.

Die Wirksamkeit dieser Methode hängt im Wesentlichen von den Wortlisten und dem Gewichtungsalgorithmus ab. Gewichtete Wortlisten sind eine effektive Technologie für Inhaltsprüfung. Dazu werden Wortlisten (z.B. Sex) und Phrasen (z.B. "Werden Sie reich") eines Themengebietes in einer Kategorie zusammengefasst. Ein Gewichtungsalgorithmus sorgt dafür, dass nicht ein einmaliges Auftreten eines Wortes zur Schwellwertüberschreitung führt, sondern eine Kombination oder ein Mehrfachauftreten den Ausschlag geben. Spezielle Wortlisten für Anti-SPAM-Funktionen erlauben eine differenzierte Konfiguration mit hohem Filtergrad. Entscheidend für die Wirksamkeit ist der verwendete Gewichtungsalgorithmus, weshalb einige Anbieter in diesem Zusammenhang von Heuristik sprechen.

- Textanalyse mit statistischen Verfahren wie z.B. Content Recognition Engine (CORE).

Hierbei handelt es sich um ein sehr flexibles Verfahren zur systematischen Erkennung von Inhalten nach frei definierbaren Kategorien wie SPAM-Mails, Newsletter, Business etc. Die Wirksamkeit dieses Verfahrens ist sehr hoch. In Kombination mit den oben genannten Filtermethoden sind sehr hohe Erkennungsraten möglich.

- Distributed Checksum Clearinghouse (DCC)

Eine neuartige Methode stellt das Distributed Checksum Clearinghouse (DCC - verteilte Prüfsummenfilter) dar. Das Verfahren erzeugt für jede empfangene E-Mail eine Prüfsumme, welche an ein verteiltes Netzwerk von Checksummen-Server weitergeleitet wird. Im Checksummen-Server wird ermittelt, wie oft diese Prüfsumme bereits registriert wurde und erhöht gleichzeitig den entsprechenden Zählerstand. Wird ein bestimmter Schwellwert überschritten und ist diese E-Mail nicht in einer Positivliste gemeldet, so wird die Nachricht als SPAM-Mail klassifiziert.

Das Prinzip weist auch einige Lücken auf: Newsletter werden in der Regel auch als Massenmail versendet, ein SPAM-Versender kann das System durch personalisierte Einzelmails (z.B. ist die Anrede in jeder E-Mail leicht verändert) oder durch Einfügen zufälliger Zeichenketten (z.B. eine Kategorisierung) umgehen. Bei sich schnell ausbreitenden E-Mails existiert noch kein Datenbankeintrag, es besteht große Abhängigkeit von der Community und von der Verbreitung des Systems.

- SpamNet

Ein alternatives und kommerzielles Verfahren ist SpamNet. Ähnlich wie bei DCC werden Prüfsummen für jede E-Mail berechnet. Im Unterschied zu DCC erhält SpamNet die SPAM-Mails jedoch durch eine individuelle Klassifikation durch Endbenutzer zugestellt.

Hierdurch entsteht unter Umständen ein erheblicher Zeitversatz, da eine E-Mail erst ab einem bestimmten Schwellwert an Meldungen als SPAM-Mail in die Datenbank aufgenommen wird. Der monatliche Beitrag beträgt z.Z. 3,99 US$.

Bewertung von Erkennungsmechanismen

Für die Bewertung der Anti-SPAM-Technologien gibt es im Prinzip zwei Kenngrößen.

Die Filterrate von Anti-SPAM Technologie wird als Verhältnis von erkannten SPAM-Mails zu den insgesamt erhaltenen SPAM-Mails ausgedrückt.

Eine weitere wichtige Kenngröße sind die sogenannten "False Positives". Damit sind E-Mails gemeint, die fälschlicherweise als SPAM-Mails eingeordnet, herausgefiltert und meist in Quarantäne gestellt worden sind. Dies kann in der Praxis zu Problemen führen, wenn wichtige E-Mails dort landen und nicht rechtzeitig den Empfänger erreichen oder sogar gelöscht werden.

Die Trefferquoten der Anbieter solcher Programme und Services liegen in der Regel bei 90% und mehr.

Eingehende Mails, die den Anforderungen einer SPAM-Mail des Filters entsprechen, werden z.B. direkt in einen SPAM-Ordner verschoben. Der Vorteil ist, dass E-Mails nicht automatisch gelöscht werden und eine abschließende Kontrolle durch den Nutzer möglich bleibt.

Es wird in der Zukunft nie Erkennungssysteme geben, die SPAM-Mails automatisch löschen können (False Positive Rate)! Aus diesem Grund wird der Aufwand für den Anwender immer "zu groß" sein!

Nachteile der SPAM-Erkennungsverfahren

- Die SPAM-Mails werden nach wie vor zum Zielsystem übertragen, wodurch Bandbreitenverbrauch, Speicherverbrauch, Arbeitszeitverlust (zwar weniger!) und damit auch Kosten entstehen.
- Auf dem Zielsystem werden sie dann z.B. im Betreff als SPAM gekennzeichnet oder in "SPAM"-Ordner einsortiert, dürfen meist aber aus rechtlichen Gründen nicht automatisch gelöscht werden.
- Ein weiteres Problem bei einer Löschung wäre die "False Positive Rate", bei denen gewollte und möglicherweise sehr wichtige E-Mails gelöscht werden, nur weil sie fälschlicherweise als SPAM deklariert worden sind.
- Da es nicht möglich ist, die "False Positive Rate" auf praktisch null zu bekommen, müssen immer auch die gekennzeichneten oder aussortierten E-Mails betrachtet werden, um gewollte und wichtige E-Mails wieder herauszuholen.
- Ein weiteres Problem bei den Lösungen von SPAM-Erkennungsverfahren ist, dass sie in der Regel keinen Feedback-Mechanismus haben. D.h. der Benutzer informiert das Erkennungssystem nicht direkt über die Trefferrate, damit kann das Erkennungssystem sich auch nicht mit Hilfe dieser Informationen bezüglich der verwendeten Heuristik optimieren.
- Damit sich aus Kostengründen die SPAM-Mails nicht mehr lohnen, müssten die Erkennungsraten über 99,9 % sein, was nicht realistisch ist.

3.2 Mechanismen zur Vermeidung von SPAM-Mails

Im folgenden werden technische Mechanismen zur Vermeidung von SPAM-Mails beschrieben und bewertet.

- Absendererkennung und Blockierung der Absender per IP-Adresse und Name.

Die Wirksamkeit dieser Methode ist unterdurchschnittlich, da viele Adresslisten im Internet nicht dem aktuellen Stand entsprechen und die SPAM-Versender die Adressen häufig wechseln. Die Methode kann unter Umständen zusätzlich zu einer hohen False Positive Rate führen, wenn der Kommunikationspartner ungewollt auf eine derartige Sperrliste geraten ist. In Kombination mit anderen Verfahren und richtig eingesetzt kann die Absendererkennung aber ein einfaches und sehr hilfreiches zusätzliches Mittel sein.

- Nutzung von Domain Name System zur Namensauflösung

Reverse DNS ist Teil des Domain Name System im Internet. Es beruht auf einem Rückfrageverfahren, bei dem Name und IP-Adresse des anrufenden Mailservers durch einen Reverse Lookup (Abfrage der IP-Adresse anhand des Domänennamens bei einem DNS-Server) auf Konsistenz geprüft wird. Treten Abweichungen auf, wird die Verbindungsaufnahme abgebrochen. Die meisten Realisierungen haben dieses Verfahren implementiert. Die Wirksamkeit gegen SPAM-Mails ist stark umstritten, da SPAM-Versender sehr häufig fremde (Echt) Systeme für den Versand nutzen oder sogar eigene E-Mail-Versandsysteme betreiben.

- Authentifikation vor dem Versand

Die Idee ist, dass SMTP, POP, usw. nur dann aktiv werden, wenn der Client vorher mittels eines Authentikationsverfahren als berechtigt verifiziert wird. Dadurch kann ein Mißbrauch reduziert werden, wenn die Mailserver die Berechtigungen pflegen und überprüfen. Dieser Mechanismus ist auf jeden Fall zu empfehlen. Die meisten Realisierungen haben Authentikationsverfahren implementiert.

- Realtime Blackhole List (RBL)

Realtime Blackhole List (RBL) ist eine Sperrliste im Internet, welche im Rahmen des Mail Abuse Prevention Systems (MAPS) zur Verfügung gestellt wird. Die Liste enthält alle ungeschützten Mailserver (z.B. die Mailserver, die "mail relaying" - weiterleiten jeglicher E-Mail - konfiguriert haben), welche von SPAM-Versendern zum Versand der unerwünschten E-Mails verwendet werden. Ein Mailserver, der RBL nutzt, kann die Aufnahme der Kommunikation mit dem ungeschützten System, noch in der SMTP Session vor dem Empfang der eigentlichen E-Mail, verweigern. Die Wirksamkeit von RBL sank in letzter Zeit stark, da immer mehr offene Clientsysteme mit wechselnden IP-Adressen nichtsahnender Internetbenutzer zum Versand vom SPAM-Mails missbraucht werden.

- Whitelist

Bei dieser Methode wird eine Liste aller legitimen Versender geführt. Im einfachsten Fall kann die Eintragung der Versender durch den Empfänger selbst vorgenommen werden. Dazu wird jeder erwünschte Kontakt in diese Liste aufgenommen, die entsprechenden E-Mails direkt zugestellt und alle anderen E-Mails werden vom Zusteller in einem niedrig priorisierten Postfach des Benutzers abgelegt. Das Whitelist-Verfahren kann verbessert werden, indem die Einträge dynamisch über ein Versenderverifkationssystem vorgenommen werden. Dazu wird einem unbekannten Versender zunächst eine E-Mail als Bestätigung zugesendet. Wenn eine

zweite E-Mail eintritt - und der Versender sich somit als antwortfähig herausstellt hat - wird die E-Mail zugestellt.

- Sender Permitted From

Mit SMTP+SPF ist derzeit ein weiterer Vorschlag in der Diskussion, der helfen soll, SPAM-Mails weiter zu verhindern. Mit der Angabe "Sender Permitted From" sollen Betreiber von Mail-Servern die IP-Adresse ihrer Mail-Server veröffentlichen, über die E-Mails mit Absender unter ihren Domains versendet werden. Empfänger haben so noch vor Annahme der E-Mail die Möglichkeit zu überprüfen, ob der Absender der E-Mail auch über einen Server versendet wurde, dessen Betreiber die entsprechende Domain hält. Nutzt ein Spammer einen anderen Mail-Server als vom Domain-Inhaber angegeben, wird dies so sichtbar. Zwar kann auf diesem Weg nicht verhindert werden, dass E-Mails mit gefälschten Absenderadressen versendet werden, wohl aber, dass diese nicht zu erkennen sind. Wer SMTP+SPF verwendet, kann so entsprechende Mails direkt abblocken. SMTP+SPF ist derzeit noch in der Entwicklung, einige Implementierungen für verschiedene Mail-Transfer-Agenten (MTAs) sind bereits verfügbar. Eine entsprechendes RFC liegt als Draft vor [Golm03].

Bewertung der technischen Mechanismen zur Vermeidung vom SPAM-Mails

Mit den technischen Mechanismen zur Vermeidung von SPAM-Mails kann ein großer Effekt gegen SPAM-Mails erzielt werden. Aus diesem Grund sollen alle Unternehmen und Provider die beschriebenen technischen Mechanismen sinnvoll nutzen. Eine vertrauenswürdige E-Mail-Infrastruktur würde SPAM-Mails deutlich reduzieren.

4 Weitere Methoden zur Verhinderung von SPAM-Mails

Im folgendem Abschnitt werden weitere Methoden beschrieben, die helfen SPAM-Mails zu bekämpfen.

4.1 Mechanismen, die jeder Anwender zur Verfügung hat

Zwar gibt es keine hundertprozentig sichere Methode, die eigene E-Mail-Adresse vor Versendern zu bewahren, doch gibt es eine ganze Reihe von Dingen, die jeder tun kann - ebenso einiges, was jeder unterlassen sollte - um es SPAM-Versendern so schwer wie möglich zu machen, an E-Mail-Adressen heranzukommen. Im folgenden werden einige der wichtigsten Punkte aufgeführt [Curt03]:

- Jeder sollte eine sehr große Zurückhaltung bei der Weitergabe der eigenen E-Mail-Adresse haben. Geben Sie Ihre E-Mail-Adresse nur Personen, die Sie kennen und/oder vertrauen.
- Verwenden Sie eine E-Mail-Adresse für den geschäftlichen (privaten) Mailverkehr, und eine zweite (dritte, ...) Adresse für Newsletter-Abonnements, E-Commerce-Transaktionen und sonstigen Web-Aktivitäten. Erstere Adresse erhalten die im vorherigen Punkt erwähnten Vertrauenspersonen, letztere Adressen erhalten alle anderen.

- Viele Websites verlangen vor dem Download einer Datei oder dem Betrachten einer Seite die Angabe einer E-Mail-Adresse. Sofern nicht ausdrücklich eine gültige Adresse vonnöten ist - weil etwa ein Zugangs-Code an die Adresse geschickt wird - empfiehlt es sich, einfach eine Dummy-Adresse wie beispielsweise "1234@zyxwv.com" anzugeben.
- Wenn Sie Online-Services wie Webmail, Messenger oder Chat benutzen, stellen Sie in Ihren Konto-Optionen sicher, dass Ihr Mitgliedsname in keinem öffentlich zugänglichen Verzeichnis gelistet wird.
- Nur E-Mail-Adressen verwenden, die lang genug sind. Viele Spammer senden SPAM-Mails an bekannte Provider, wie z.B. GMX, in dem sie alle Buchstabenkombinationen als E-Mail-Adressen annehmen. Dieser Mechanismus funktioniert nur bei kurzen E-Mail-Adressen vor dem @.
- Indirekte Darstellung von E-Mail-Adressen auf Web-Seiten. Hier können z.B. die gesamte E-Mail-Adresse oder nur das "@"-Zeichen als GIF-Bild wiedergegeben werden. Der Nachteil dabei ist, dass die E-Mail-Adresse nicht mehr durch Anklicken oder Kopieren in das Mail-Programm übernommen werden kann, sondern mühsam von Hand eingegeben werden muss.
- Wenn Sie eine E-Mail gleichzeitig an mehrere, einander unbekannte Empfänger versenden, setzen Sie alle auf Blindkopie (BCC), so dass die E-Mail-Adressen verborgen und privat bleiben. Dies gilt insbesondere für geschäftliche Korrespondenz. Ihre Empfänger werden es Ihnen danken.
- Wenn Sie E-Mail-Newsletter abonnieren, oder sonstige Online-Services, die eine Registrierung voraussetzen, nutzen möchten, nehmen Sie sich die paar Minuten Zeit, um die Nutzungsbedingungen und/oder Datenschutzrichtlinien (Privacy Policy) durchzulesen. In der heutigen Wirtschaftslage versuchen nicht wenige Firmen mit allen nur erdenklichen Mitteln Geld zu verdienen - inklusive der Weitergabe Ihrer persönlichen Daten und Kontaktinformationen.
- Öffnen Sie keine empfangenen SPAM-Mails. Neben dem Risiko, dass Sie sich einen Virus, Würmer, Trojaner oder Dialer einfangen, nutzen SPAM-Versender oft HTML-formatierte Mails, um die Gültigkeit Ihrer Adresse zu überprüfen. Spezielle IMG-Tags für die eingebetteten Grafiken können Ihre E-Mail-Adresse in kodierter Form enthalten. Wenn diese Grafiken vom Server abgerufen werden, ist das für den SPAM-Versender der Beweis, dass die Mail ihren Empfänger erreicht hat und auch gelesen wurde. Die Folge: Noch mehr SPAM-Mails. Dies gilt übrigens auch für die in Mail-Programmen wie Outlook integrierte "Voransicht "-Funktion.
- Sollten Sie versehentlich eine SPAM-Mail öffnen, widerstehen Sie der Versuchung, auf die oft angebotene Möglichkeit des "Abmeldens" (Unsubscribe) einzugehen. Mit Ihrer E-Mail-Adresse verdienen SPAM-Versender ihren Lebensunterhalt - niemals würden sie Sie aus ihrer Liste austragen. Auch hier gilt: Ein Klick auf den Link "Abmelden" dient in aller Regel ausschließlich zum Verifizieren Ihrer E-Mail-Adresse.
- Ein weiterer und sehr wichtiger Punkt ist: Kaufen Sie keine Ware oder Dienstleistung, die mittels SPAM-Mails beworben wird. Dank der extrem niedrigen Kosten des SPAM-Versands ist eine Kampagne auch bei nur einem verkauften Produkt von 10.000 ein Erfolg. Wenn niemand die Produkte kauft, die durch SPAM-Mails beworben werden, dann

hören Hersteller und Dienstleister eines Tages auf, SPAM-Mails als Vertriebsweg zu nutzen.

Bewertung der Mechanismen, die jeder Anwender zur Verfügung hat

Durch diese Maßnahmen können SPAM-Mails für jedes Individuum (E-Mail-Adresse) sehr gut reduziert werden. Außerdem wird es den Spammern schwer gemacht, daraus ein lohneswertes Geschäft zu machten!

4.2 Rechtliche Mechanismen

Die rechtliche Situation greift zur Zeit nicht genug, um SPAM-Mails wirkungsvoll zu verhindern. Was nützen uns Gesetze, wenn Sie nicht konsequent umgesetzt werden.

Dennoch sind in der jüngsten Zeit einige wichtige und richtige Schritte durchgeführt worden.

US-Präsident unterzeichnet Gesetz gegen SPAM

Im Dezember 03 hat George W. Bush das Gesetz "Controlling the Assault of Non-Solicited Pornography and Marketing Act" unterzeichnet, das die Flut unerwünschter Reklame-E-Mails eindämmen soll. Internet-Nutzer sollen sich damit gegen Reklame wehren und Absender bestraft werden können. Zudem wird es illegal, in der Absenderzeile falsche Angaben zu machen. Das Gesetz sieht Haftstrafen von fünf Jahren und Geldstrafen bis zu 6 Millionen US-Dollar vor [Heis03a].

Gericht bestätigt Haftung des Subdomain-Vermieters für Spam

Das Landgericht bestätigte die Auffassung der Vorinstanz, wonach unverlangte E-Mail-Werbung einen Eingriff in das allgemeine Persönlichkeitsrecht sowie das Recht am eingerichteten und ausgeübten Gewerbebetrieb darstellt. Dabei käme es nicht darauf an, ob der Subdomain-Betreiber die Werbe-Mails selbst versandt habe oder nicht. Vielmehr hafte er in seiner Eigenschaft als Host-Provider als so genannter "Zustandsstörer" neben dem nicht zu ermittelnden Subdomain-Inhaber. Dies gelte zumindest dann, wenn der Anbieter bei der Vergabe der Subdomains seine Prüfungspflichten über die Identität seines Kunden verletze und dieser dadurch nicht zu ermitteln ist. Ließe er vielmehr eine anonyme Nutzung des Angebots zu, so wäre nach Ansicht des Gerichts dem "Rechtsbruch im Internet völlig freie Hand gelassen" [Heis03b].

Bewertung der rechtlichen Mechanismen

Gesetze sind ein sehr wichtiger Mechanismus. Wichtiger als die Gesetze selber, ist aber deren internationale Umsetzung. Wenn jedem Spammer bewußt ist, dass die Wahrscheinlichkeit sehr groß ist, dass er Strafe zahlen muss oder ins Gefängnis kommt, werden sich die SPAM-Mails auch nachhaltig reduzieren.

5 Ausblick und Bewertung

SPAM-Mails sind ein ernsthaftes Problem, welches die positive Nutzung von E-Mails und damit die Informations- und Wissensgesellschaft gefährden könnte.

SPAM-Mails sind ein gesellschaftliches Problem, welches wir nur gemeinsam über alle geographischen und politischen Grenzen, Gesetze und Kulturen hinaus lösen können. Damit stellen SPAM-Mails eine neue und ungewohnte Herausforderung für die internationale Gesellschaft dar.

Gegen SPAM-Mails sollte auf allen Ebenen in der aufgeführten Priorität etwas getan werden!

1. Erkennen von SPAM-E-Mails, aber nicht um jeden Preis

Mit dem Einsatz von Anti-SPAM-Technologien können SPAM-Mails erkannt werden, was möglicherweise helfen kann, mit dem Umgang besser klar zu kommen. Dazu müssen aber in Zukunft vermehrt Feedbackmechansimen berücksichtigt werden, um viel bessere Ergebnisse zu erzielen.

2. Verhinderung von SPAM in der Infrastruktur

Die Unternehmen und Provider sollen alles tun, um ihre MTAs und Mail-Clients gegen Missbrauch zu schützen, damit die SPAM-Mails so stark wie nur möglich in der Infrastruktur verhindert werden.

3. Bestrafung vorantreiben

Die Versendung von SPAM-Mails muss international sehr hoch bestraft werden.

4. E-Mails sollten etwas kosten!

Wenn das Versenden von E-Mails Geld kosten würde, ging die Anzahl von SPAM-Mails sofort zurück, da die Motivation fehlt! Ein andere Möglichkeit wäre ein Fonds zur gründen. Hier ist die Idee X % von den Internetkosten dafür zu nutzen, damit rechtliche Schritte gegen Spammer realisiert werden können!

5. SPAM-Mails dürfen sich nicht lohnen!

Eine weitere effektive Hilfe gegen SPAM-Mails ist dann besonders geeignet, wenn es sich für den Absender nicht mehr lohnt, diese in Umlauf zu bringen. Das Versenden von SPAM-Mails müsste mit finanziellen Nachteilen verbunden sein, die größer sind, als die evtl. zu erzielenden Gewinne durch Rückläufe. Aus diesem Grund müssen alle Maßnahmen, die getroffen werden, dafür sorgen, dass sich SPAM-Mails nicht mehr lohnen. Solche Maßnahmen sind z.B.: sehr hohe Strafen, nie auf SPAM-Mails reagieren und eine hohe gesellschaftliche Ächtung. Möglicherweise sollte auch ein Verrechnungssystem von E-Mails eingeführt werden, sodass dem Spammer (aber auch allen anderen) Kosten entstehen.

Literatur

[BlPo04] H. Blumberg, N. Pohlmann: "Der IT-Sicherheitsleitfaden“, ISBN 3-8266-0940-9, MITP-Verlag, Bonn 2004

[Curt03] J. Curtis: "Spam-Flut außer Kontrolle: Wie Sei den Kampf gewinnen", ZDNet-Security-Special

[DCC03] "Distributed Checksum Clearinghouses" über www.brightmail.com

[Golm03] "Sender Permitted From soll Spam vermeiden" über www.glom.de (06.10.2003)

[Grou03] "Schwerpunkt: Anti-Spam", Group-Technogies über www.group-technologies.com/de/produkte/faq/antispam.php

[Heis03a] "US-Präsident unterzeichnet Gesetz gegen Spam" über www.heise.de (16.10.2003)

[Heis03b] "Gericht bestätigt Haftung des Subdomain-Vermieters für Spam" über www.heise.de (12.10.2003)

[Klau03] P. Klau: "Perfekt geschützt vor Spam&Spy", bhv, 2003

[Herr03] F. Herrmann: "Ein Internetdienst zur Vermeidung von unerwünschter Reklamepost", Diplomarbeit, Technische Universität Dresden, Fakultät Informatik, Institut für Systemarchitektur, 2003

[Pohl03] N. Pohlmann: "Kampf dem Müll - Unerwünschte Werbe-Mails sind ein ernstes volkswirtschaftliches Problem”, Frankfurter Allgemeinen Zeitung – FAZ, Dienstag, 21. Oktober 2003

[ScGa00] A. Schwartz, S. Garfinkel: "Stopp Spam", O´Reilly, 2000