



Bundesamt  
für Sicherheit in der  
Informationstechnik

## Antispam - Strategien

Unerwünschte E-Mails erkennen und abwehren



Stand: März 2005

Autoren

**Jochen Topf**, Jochen Topf Internet Consulting

**Matthias Etrich**, T-Systems International GmbH

**Joerg Heidrich**, Heise Zeitschriften Verlag

**Leslie Romeo**, WEB.DE AG

**Marco Thorbrügge**, DFN-CERT

**Bert Ungerer**, Heise Zeitschriften Verlag

---

## Vorwort

E-Mail ist neben dem World Wide Web der wichtigste Dienst des Internets. Kein Wunder: schnell, zuverlässig, kostengünstig – die Vorteile von E-Mail liegen auf der Hand.

Genau diese Vorteile werden jedoch immer häufiger missbraucht. Inzwischen machen unverlangt zugeschickte Massen-E-Mails den Großteil des E-Mail-Verkehrs aus und gefährden so die Zuverlässigkeit des Dienstes. Es wird immer schwieriger, eine wichtige Nachricht in Hunderten von Spammails zu finden, wenn keine Gegenmaßnahmen ergriffen werden. Doch nicht nur das: Ungeschützte Computer werden für den Spam-Versand von Angreifern ferngesteuert zweckentfremdet. Ohne technische Hilfen, wie Viren Schutzprogramme und Firewalls, fällt der Missbrauch kaum auf. Das dadurch entstehende Bedrohungspotenzial reicht von finanziellen Verlusten Einzelner bis hin zur Gefährdung der IT-Sicherheit ganzer Organisationen.

Das Problem Spam wird derzeit öffentlich stark diskutiert, denn wir brauchen geeignete Strategien um das Bedrohungspotenzial zu verringern. Derzeit sind zwar viele Informationen zu technischen, rechtlichen und organisatorischen Aspekten verfügbar, doch es fehlt die Bündelung des Wissens. Aus diesem Grund hat das BSI die vorliegende Studie initiiert. Sie gibt IT-Verantwortlichen einen Überblick über alle Aspekte zur Entwicklung einer individuellen Antispam-Strategie. Unser Ziel muss es sein, Antispam-Strategien flächendeckend umzusetzen – nur so können wir das Problem weltweit lösen.



Dr. Udo Helmbrecht, Präsident des BSI

## Danksagung

Wir bedanken uns bei allen, die Vorversionen dieses Textes (teilweise mehrfach) gelesen und uns wertvolle Hinweise und Korrekturen geliefert haben:

- Holger Bleich, Heise Zeitschriften Verlag
- Michael Dyrna, GMX
- Prof. Dr. Nikolaus Forgó, Universität Hannover
- Anders Henke, Schlund+Partner
- Stefan Kelm, securvo
- Klaus-Peter Kossakowski, DFN-CERT
- Frederik Ramm, limiting factor GmbH
- René Schönfeldt, dpunkt. verlag
- Martin Sellmann, T-Systems International GmbH

## Inhaltsverzeichnis

|   |    |
|---|----|
| Vorwort   | 3  |
| Danksagung  | 4  |
| 1 Einleitung                                      | 8  |
| 2 Management Summary                              | 10 |
| 3 Was ist Spam?                                   | 13 |
| 3.1 Definition von Spam                           | 13 |
| 3.2 Spam und ähnliche Phänomene                   | 14 |
| 3.2.1 Kommerzielle Werbung                        | 14 |
| 3.2.2 Nicht-kommerzielle Werbung                  | 14 |
| 3.2.3 Malware                                     | 15 |
| 3.2.4 Betrug und Phishing                         | 15 |
| 3.2.5 Rufschädigung und Provokation von Angriffen | 15 |
| 3.2.6 Kettenbriefe                                | 16 |
| 3.2.7 Kollateraler Spam                           | 16 |
| 3.3 Warum ist Spam ein Problem?                   | 17 |
| 3.3.1 Wirtschaftliche Schäden                     | 17 |
| 3.3.2 Die Spammer                                 | 18 |
| 4 Wie Spam funktioniert                           | 20 |
| 4.1 Technische Grundlagen                         | 20 |
| 4.1.1 Simple Mail Transfer Protocol (SMTP)        | 20 |
| 4.1.2 Envelope, Header und Fälschungen            | 21 |
| 4.1.3 Fehlermeldungen                             | 22 |
| 4.1.4 Der Weg einer E-Mail                        | 23 |
| 4.2 Spamversand                                   | 24 |
| 4.2.1 Spam-Server                                 | 24 |
| 4.2.2 Open Relays                                 | 24 |
| 4.2.3 Open Proxies                                | 25 |

---

|  |    |
|--|----|
| 4.2.4 Unsichere CGI-Skripte  | 25 |
| 4.2.5 Zombie-PCs und Botnetze  | 25 |
| 4.2.6 Mailserver des Providers                                       | 26 |
| 4.3 Wie Spammer an die Mailadressen gelangen                         | 26 |
| 4.3.1 Offline-Datensammlungen  | 27 |
| 4.3.2 Webseiten und Newsgruppen                                      | 27 |
| 4.3.4 Externe Inhalte in HTML-Mails                                  | 28 |
| 4.3.5 Automatische Antworten   | 28 |
| 4.3.6 Whois-Datenbanken  | 28 |
| 4.3.7 Lokal gespeicherte Adressen                                    | 28 |
| 5 Kosten von Spam und Antispam-Maßnahmen                             | 30 |
| 5.1 Durch Spam verursachte Kosten                                    | 30 |
| 5.2 Kosten von Antispam-Maßnahmen                                    | 30 |
| 5.3 Fallbeispiele  | 30 |
| 5.3.1 Beispiel Großprovider  | 31 |
| 5.3.2 Beispiel Provider  | 32 |
| 5.3.3 Beispiel Großunternehmen                                       | 33 |
| 5.3.4 Beispiel mittelständisches Unternehmen                         | 34 |
| 5.3.5 Beispiel Einzelunternehmer/Kleinunternehmen                    | 35 |
| 5.3.6 Zusammenfassung  | 36 |
| 5.4 Einkauf oder Eigenleistung?                                      | 36 |
| 6 Rechtliche Aspekte von Spam  | 38 |
| 6.1 Rechtslage   | 38 |
| 6.1.1 Spam im juristischen Sinn                                      | 38 |
| 6.1.2 Spam und die Gerichte  | 39 |
| 6.1.3 Maßnahmen des Gesetzgebers                                     | 41 |
| 6.2 Zivilrechtliche Maßnahmen gegen Spam                             | 42 |
| 6.2.1 Wer haftet für Spam?   | 43 |
| 6.2.2 Schadensersatz und Gewinnabschöpfung                           | 43 |
| 6.2.3 Abmahnung  | 44 |
| 6.2.4 Einstweilige Verfügung   | 45 |
| 6.2.5 Hauptsacheverfahren  | 46 |
| 6.2.6 Erfolgsaussichten und typische Probleme in Spam-Verfahren      | 46 |
| 6.2.7 Kosten für rechtliche Maßnahmen                                | 46 |
| 6.2.8 Datenschutzrechtlicher Auskunftsanspruch                       | 47 |
| 6.3 Spam und Strafrecht  | 48 |
| 6.3.1 Strafbarkeit des Versands von Spam                             | 48 |
| 6.3.2 Strafbare Inhalte in Spam-Mails                                | 49 |
| 6.3.3 Fälschung der Absenderadresse                                  | 49 |
| 6.3.4 Vorsätzliche Schädigung durch Absenderfälschung                | 49 |
| 6.3.5 Selbsthilfemaßnahmen gegen Spammer                             | 50 |
| 6.4 Viren, Würmer und Trojaner rechtlich betrachtet                  | 50 |
| 6.4.1 Vorsätzliches Verbreiten von Malware                           | 50 |
| 6.4.2 Haftung für die Weiterverbreitung über virenverseuchte Rechner | 51 |
| 6.4.3 Haftung der Provider   | 52 |
| 6.4.4 Sind Bounces und Viren-Warnungen Spam?                         | 52 |
| 6.5 Rechtliche Beurteilung von Filtermaßnahmen                       | 53 |
| 6.5.1 Strafbarkeit nach § 206 StGB                                   | 53 |
| 6.5.2 Strafbarkeit nach § 303a StGB                                  | 55 |
| 6.5.3 Filterung ausgehender Mail                                     | 56 |
| 6.5.4 Tipps für rechtskonforme Mailfilterung                         | 56 |
| 6.5.5 Reaktionsmöglichkeiten im Notfallbetrieb                       | 57 |

|   |    |
|---|----|
| 6.5.6 Besonderheiten bei der Filterung auf Malware        | 57 |
| 6.6 Zulässiges E-Mail-Marketing                           | 58 |
| 7 Vermeiden von Spam                                      | 60 |
| 7.1 Sichere Konfiguration eigener Systeme                 | 60 |
| 7.1.1 Mailserver  | 60 |
| 7.1.2 HTTP(S) und SOCKS-Proxies                           | 61 |
| 7.1.3 Formmail-Skripte                                    | 61 |
| 7.2 Umgang mit Mailadressen                               | 62 |
| 7.2.1 Auswahl der eigenen Mailadresse                     | 62 |
| 7.2.2 Verschleiern und Geheimhalten der Adresse           | 63 |
| 7.2.3 Anzahl eigener Mailadressen begrenzen               | 64 |
| 7.2.4 Zusatzinformationen in den eigenen E-Mails mitgeben | 64 |
| 7.2.5 Zusatzinformationen im mailto:-Link                 | 65 |
| 7.2.6 Häufiger Adresswechsel und Wegwerfadressen          | 65 |
| 8 Antispam-Maßnahmen: Grundlagen                          | 67 |
| 8.1 Ansatzpunkte für eine Filterung                       | 67 |
| 8.1.1 IP-Adresse  | 67 |
| 8.1.2 Absenderadresse und -domain                         | 68 |
| 8.1.3 Inhalt  | 68 |
| 8.1.4 Verhalten des Absenders                             | 70 |
| 8.1.5 Menge und Frequenz                                  | 70 |
| 8.2 Absenderauthentifizierung                             | 71 |
| 8.3 Accreditation und Reputation                          | 72 |
| 8.3.1 Accreditation                                       | 72 |
| 8.3.2 Reputation  | 72 |
| 8.4 Ort der Maßnahme                                      | 73 |
| 8.4 Ort der Maßnahme                                      | 73 |
| 8.4.1 Im Server beim Versand                              | 73 |
| 8.4.2 Im Server vor Annahme der E-Mail                    | 74 |
| 8.4.3 Im Server nach Annahme der E-Mail                   | 75 |
| 8.4.4 Im Client vor Abholung der E-Mail                   | 75 |
| 8.4.5 Im Client nach Abholung der E-Mail                  | 75 |
| 8.5 Bewertung   | 76 |
| 8.5.1 Vergleichbarkeit                                    | 76 |
| 8.5.2 Zusammenwirken von Maßnahmen                        | 77 |
| 8.5.3 Einfluss durch den Anwender                         | 79 |
| 8.6 Behandlung nach der Bewertung                         | 80 |
| 8.6.1 Zustellen   | 80 |
| 8.6.2 Abweisen  | 80 |
| 8.6.3 Löschen   | 81 |
| 8.6.4 Markieren   | 81 |
| 8.6.5 Unter Quarantäne stellen                            | 82 |
| 8.6.6 Auswahl des Verfahrens                              | 82 |
| 9 Antispam-Maßnahmen: Einzelne Verfahren                  | 84 |
| 9.1 Filterung durch Personen                              | 86 |
| 9.2 Protokollbasierte Maßnahmen                           | 86 |
| 9.3 White- und Blacklists                                 | 88 |
| 9.4 DNS-basierte Blacklists (DNSBLs)                      | 89 |
| 9.4.1 Technik der DNSBLs                                  | 89 |
| 9.4.2 Policies  | 90 |

---

|   |     |
|---|-----|
| 9.4.3 Typen von DNSBLs  | 91  |
| 9.4.4 Probleme mit DNSBLs   | 92  |
| 9.4.5 Rechtliche Aspekte von DNSBLs                               | 93  |
| 9.5 IP-Blacklisting durch Frequenzanalyse                         | 93  |
| 9.6 Sperre des SMTP-Ports   | 96  |
| 9.7 MTAMARK   | 97  |
| 9.8 Existenzprüfung der Absenderadresse                           | 97  |
| 9.9 MARID-Verfahren: SPF und SenderID                             | 98  |
| 9.9.1 DNS-Einträge  | 99  |
| 9.10 S/MIME und PGP   | 100 |
| 9.11 MASS-Verfahren: DomainKeys und IIM                           | 100 |
| 9.12 RHSBLs   | 102 |
| 9.13 Greylisting  | 102 |
| 9.14 Heuristische Inhaltsanalyse                                  | 103 |
| 9.15 Statistische Inhaltsanalyse                                  | 104 |
| 9.16 Prüfsummenvergleich  | 106 |
| 9.17 URIDNSBLs  | 108 |
| 9.18 Tokenbasierte und Challenge-Response-Verfahren               | 108 |
| 9.19 Proof-of-Work-Verfahren                                      | 110 |
| 9.20 E-Mail-Briefmarken   | 110 |
| 9.21 Bounce Address Tag Validation (BATV)                         | 111 |
| 10 Empfehlungen   | 113 |
| 10.1 Grundlegende Überlegungen                                    | 113 |
| 10.2 Aufstellen einer Antispam-Policy                             | 115 |
| 10.2.1 Organisatorische Aspekte                                   | 115 |
| 10.2.2 Technische Aspekte   | 116 |
| 10.2.3 Notfall-Policy   | 117 |
| 10.3 Allgemeine Empfehlungen                                      | 118 |
| 10.3.1 Sichere Konfiguration                                      | 118 |
| 10.3.2 Eigene Mail-Infrastruktur                                  | 118 |
| 10.3.3 Gestaltung von Webanwendungen                              | 119 |
| 10.3.4 Verhalten des Endanwenders                                 | 119 |
| 10.4 Maßnahmenempfehlungen  | 120 |
| 10.4.1 Empfehlenswerte Maßnahmen                                  | 120 |
| 10.4.2 Eingeschränkt empfehlenswerte Maßnahmen                    | 123 |
| 10.4.3 Maßnahmen, die nicht genutzt werden sollten                | 124 |
| 10.4.4 Experimentelle Maßnahmen                                   | 124 |
| 10.5 Fallbeispiele  | 124 |
| 10.5.1 Privatanwender, Selbständige und Kleinunternehmer          | 125 |
| 10.5.2 Mittelständische Unternehmen und Ämter                     | 126 |
| 10.5.3 Großunternehmen und Ministerien mit nachgeordnetem Bereich | 127 |
| 10.5.4 Universitäten und Hochschulen                              | 128 |
| 10.5.5 Intern et-Provi der  | 129 |
| 10.6 Hinweise zur Produktauswahl                                  | 130 |
| Schlusswort   | 133 |
| Glossar   | 134 |
| Literatur und Links   | 144 |

# 1 Einleitung

Das Medium E-Mail wird jeden Tag von Millionen Menschen in der ganzen Welt genutzt. Kein Internet-Dienst ist erfolgreicher. E-Mail ist aus der privaten Kommunikation und dem Geschäftsleben nicht mehr wegzudenken.

Mit dem Siegeszug der E-Mail in den letzten zehn Jahren ging aber eine steigende Zahl von Missbrauchsfällen einher. Was als kleines Ärgernis begann, ist heute ein großes und sehr teures Problem, das die Verfügbarkeit dieses Dienstes gefährdet. Werbemail und andere unerwünschte E-Mails, kurz „Spam“, kosten jeden einzelnen Zeit und die Gesellschaft jedes Jahr viele Milliarden Euro. Das tägliche Spam-Aufkommen hat die Zahl der erwünschten E-Mails bei weitem überschritten; manche Studien schätzen bereits, dass 90 % des Mailaufkommens im Internet aus Spam besteht. Zum Versand von Spam werden Hunderttausende infizierter Rechner missbraucht – was für sich genommen bereits ein gigantisches Sicherheitsproblem darstellt.

In den letzten Jahren hat die Internet-Gemeinde viele Verfahren entwickelt, die helfen, Spam zu vermeiden oder zumindest den Empfänger davor zu schützen. Umfangreiche Filtersysteme untersuchen eingehende E-Mail und trennen Unerwünschtes von Erwünschtem. Die Kosten dafür sind enorm, aber ohne Maßnahmen gegen Spam wäre E-Mail für viele nicht mehr nutzbar.

Wegen der Komplexität des weltweiten Mailsystems und der immer neuen Tricks der Spammer gibt es eine große Anzahl sehr verschiedener Antispam-Maßnahmen. Es ist daher nicht leicht, die Funktion und Effizienz der Verfahren und ihre Vor- und Nachteile einzuschätzen. Diese Studie hat vor allem das Ziel, technische Maßnahmen gegen Spam in ihrer ganzen Bandbreite ausführlich zu beschreiben, um eine Entscheidungshilfe für Auswahl und Einsatz eines oder mehrerer Verfahren zu geben. Dabei werden auch die juristischen Rahmenbedingungen erklärt, weil gerade hier häufig große Unsicherheiten bei den Betreibern von Antispam-Systemen bestehen.

Zielgruppe dieser Studie sind in erster Linie IT-Verantwortliche, Systemadministratoren und Postmaster. Daneben richtet sich die Studie an alle, die sich eingehender mit dem Thema Spam und seiner Bekämpfung beschäftigen möchten.

Vor der Erläuterung der Maßnahmen müssen die Grundlagen geklärt werden. Das beginnt mit Kapitel 3, das Begriffe wie „Spam“ definiert und genauer aufzeigt, wo das Problem liegt. Kapitel 4 geht auf die Methoden der Spammer ein, ohne deren Kenntnis man die Antispam-Maßnahmen nicht verstehen kann. Die beispielhaften Kostenbetrachtungen im Kapitel 5 geben einen Überblick über die Kosten von Spam und Antispam-Maßnahmen und sollen dem Leser Orientierungshilfen bieten, wie er die entstehenden Kosten für seine eigene Organisation erfassen kann.

Neben dem finanziellen und technischen steht der juristische Aspekt, dem sich Kapitel 6 widmet. Darauf folgt in Kapitel 7 eine Diskussion der vorbeugenden Maßnahmen – Spam, der gar nicht erst entsteht, muss auch später nicht ausgefiltert werden. Kapitel 8 geht auf die grundlegenden Eigenschaften und Parameter der Antispam-Maßnahmen ein, während Kapitel 9 einen Katalog von Maßnahmen aufführt und erklärt. Das Kapitel 10 fasst alles Vorhergehende in allgemeinen Empfehlungen zusammen. Es geht auf verschiedene Fallbeispiele ein, um es dem Leser einfacher zu machen, die Empfehlungen in seiner Organisation anzuwenden und eine entsprechende Policy zu entwickeln. Ein Glossar und ein Literaturverzeichnis mit Hinweisen zu weiterführenden Informationen schließen sich an.

Die Methoden der Spammer und damit auch die Antispam-Verfahren sind einem ständigen Wandel unterworfen. Dabei ändern sich viele Details, aber die grundsätzlichen Fragen und Techniken bleiben oft gleich. Die Studie gibt den Stand Anfang 2005 wieder; viele Details können und werden sich ändern. Überall dort, wo große Veränderungen zu erwarten sind, gibt es entsprechende Hinweise. In jedem Fall ist es empfehlenswert, sich im Internet über aktuelle Entwicklungen weiter zu informieren. Startpunkte dazu finden sich in den Fußnoten und im Literaturverzeichnis.

Für viele Fachwörter gibt es keine deutschen Übersetzungen, sie stehen deshalb im englischen Original und sind durch *Kursivdruck* gekennzeichnet. Wichtige Wörter werden gelegentlich **fett**

---

gedruckt, beispielsweise Definitionen im Kapitel 3 und wichtige Empfehlungen in Kapitel 10. Protokollbefehle, Header-Zeilen und andere Computeraus- und -eingaben sind in der Schriftart Letter Gothic gedruckt. Viele weiterführende Informationen und Anmerkungen finden sich in umrahmten und grau hinterlegten Kästen.

## 2 Management Summary

### Das Problem

Der Erfolg des Mediums E-Mail ist unbestreitbar. Aber niemand nutzt es intensiver als die Spammer. Untersuchungen ergeben, dass 60 % bis 90 % aller E-Mails Spam sind. Spam kostet den Privatanwender Zeit und Nerven, mittelständische Unternehmen Zehntausende, große Internet-Provider viele Millionen Euro pro Jahr. Eine Spam-Aussendung kann sich an eine Million Empfänger richten. Kämen keine Spamfilter zum Einsatz und würde jeder Empfänger im Durchschnitt nur 10 Sekunden für das Anschauen und Löschen der E-Mail aufwenden, entstünde (bei angenommenen 50 € Arbeitskosten pro Stunde) bereits ein Schaden von fast 140.000 €. Der Schaden für die weltweite Volkswirtschaft geht Jahr für Jahr in die Milliarden, die Verfügbarkeit des Mediums E-Mail ist bedroht. Und die Spammer verdienen nicht schlecht: Zwar sind typische Rücklaufquoten winzig und jeder so gewonnene Kunde bringt meist nur zweistellige Einnahmen, aber bei Millionen von Spam-Mails, die sich mit sehr geringem Aufwand und nahezu kostenlos versenden lassen, ergeben sich erhebliche Beträge.

Neben dem kommerziellen Werbe-Spam kann E-Mail Viren, Würmer und andere Schädlinge verbreiten. Sie infizieren die Rechner von Privatanwendern und Arbeitsplatz-PCs in vielen Unternehmen. Die Angreifer fassen dann Tausende bis Hunderttausende dieser Rechner in so genannten Botnetzen zusammen, die sie nach Belieben fernsteuern, und schaffen damit ein riesiges Sicherheitsproblem. Dynamische Updates der Bot-Software erlauben es ihnen, die Rechner zur Verbreitung von Spam oder zu Angriffen auf andere Rechner zu verwenden oder die Anwender auszuspionieren. Große Teile des Spams werden heute nicht von Gelegenheitsspammern verteilt, sondern von Profis, die mit Kriminellen in einer regelrechten Untergrundwirtschaft verbunden sind, in der unter anderem Mailadressen, Listen von infizierten Rechnern und Kreditkartennummern gehandelt werden.

### Juristische Fragen

In Deutschland und innerhalb der EU ist Spam mit kommerziellem Hintergrund verboten, international ist die Lage uneinheitlich. Viele Länder haben Gesetze gegen Spam, die aber häufig ungeeignet sind, Spammer abzuschrecken oder wesentlich einzuschränken. Da der überwiegende Teil des Spams aus dem Ausland kommt, ist den Spammern von Deutschland aus mit juristischen Mitteln kaum beizukommen. Dazu kommt, dass sie sich tarnen und der Ermittlungsaufwand damit erheblich ist. Daher muss jeder sich selbst schützen, etwa durch die gezielte Filterung von derartigen E-Mails. Dabei sind vor allem das Fernmeldegeheimnis und der Datenschutz zu beachten. Unternehmen, Behörden und Internet-Provider sollten daher vor Aufnahme der Filterung mit den Betroffenen klare Regelungen treffen, etwa in Form von Betriebsvereinbarungen, Dienstanweisungen oder Hinweisen in den AGB.

Spam ist auch eine Folge von schlecht gesicherten Systemen in Unternehmen und bei Privatanwendern. Erste Maßnahme gegen Spam ist also zu verhindern, dass eigene Systeme zur Verteilung von Spam missbraucht werden. Dies ist nicht nur hilfreich für die Allgemeinheit, sondern es verhindert auch, dass das infizierte eigene Netzwerk auf schwarzen Listen landet, die andere zum Filtern und Blockieren von E-Mails verwenden. Auch aus juristischer Sicht ist eine Absicherung erforderlich, da es insbesondere für Unternehmen gesetzliche Mindestanforderungen an die IT-Sicherheit gibt, deren Missachtung unter Umständen zu einer Haftung für die Verbreitung von Spam führen kann.

---

## Maßnahmen gegen Spam

Es gibt einige Methoden, die eigene Mailadresse zu schützen oder zu verschleiern. Die Erfahrung zeigt jedoch, dass Spammer sie früher oder später herausbekommen, sei es durch „Ernten“ der (versehentlich) in einem öffentlichen Forum genutzten Adresse, durch Ausspähen von Adressbuchdaten oder Ähnliches.

Als einzig praktikable Lösung bleibt die Filterung der ankommenden E-Mails. Dazu gibt es eine ganze Reihe von Verfahren, die über die Jahre entwickelt und immer weiter verbessert und an die Tricks der Spammer angepasst wurden. Wegen der Komplexität des weltweiten Mailsystems, der Gegenmaßnahmen der Spammer und weil die zum Mail-Austausch verwendeten Protokolle für ein „friedlicheres“ Internet entwickelt wurden, gibt es kein perfektes Verfahren. Durch die Kombination mehrerer technischer Verfahren ist es aber heute möglich, das Spamproblem auf ein erträgliches Maß zu reduzieren, ohne dabei den Empfang erwünschter E-Mails über Gebühr zu gefährden.

## Filterverfahren

Die Verfahren unterscheiden sich vor allem darin, welche Merkmale sie zur Filterung heranziehen. Da ist zuerst die IP-Adresse des Absenders, das einzige Datum, das der Spammer nicht ohne weiteres fälschen kann. White- und Blacklists können die „guten“ und „schlechten“ IP-Adressen erfassen, die sich zur Filterung nutzen lassen. Da Spammer aber in großem Stil fremde Rechner missbrauchen, können sie in sehr kurzen Abständen ihre IP-Adressen wechseln. Eine schnelle und automatisierte Reaktion und die Zusammenarbeit vieler Mailempfänger über zentrale Datenbanken mit IP-Adressen (so genannte DNSBLs) ist trotzdem erfolversprechend, da von den meisten darin erfassten IP-Adressen stunden- oder tagelang Spam ausgeht. Vorteil der IP-basierten Verfahren ist vor allem, dass sie einfach und günstig zu implementieren sind und große Mengen an E-Mails schnell bewerten können.

Inhaltsbasierte Verfahren dagegen sind meist wesentlich aufwendiger, weil sie erhebliche Rechenzeit erfordern, dafür ist aber die Qualität der Filterung oft besser. Man unterscheidet Verfahren, die mittels „handgefertigter“ Muster (Heuristik) bekannte Spaminhalte erfassen, und statistische (wie das populäre Bayes-Verfahren), die laufend durch die Vorlage von E-Mails trainiert werden und selbständig typische Kennzeichen von Spam erlernen.

Spam tritt immer in großen Mengen auf. Der einzelne Empfänger sieht das nicht unbedingt, aber in großen Unternehmen, bei Internet-Providern und durch Zusammenarbeit zwischen mehreren Empfängern kann man mit Ähnlichkeits- und Frequenzanalysen sehr zuverlässig erkennen, ob eine E-Mail an viele Empfänger geht und damit wahrscheinlich Spam ist. Natürlich gibt es auch legitime Versender von Massenmail, die notfalls durch Whitelisting von solchen Verfahren ausgenommen werden müssen.

Die dem weltweiten Mailsystem zugrunde liegenden Protokolle erlauben – wie auch das klassische Postsystem – keine eindeutige Authentifizierung des Absenders; jeder kann unter beliebigem Namen E-Mails versenden. In letzter Zeit sind Verfahren wie SPF, SenderID und DomainKeys im Gespräch, die zumindest die Authentifizierung der Domain (in der Regel also der Firma oder des Internet-Provider) ermöglichen sollen. Da sie aber nicht frei von Nebenwirkungen sind und auch Spammer beliebig Domains registrieren können, sind diese Verfahren sehr umstritten. Erst in Verbindung mit Reputations-Verfahren, die etwas über die bisherige Verwendung dieser Domain zum Versand von Ham oder Spam aussagen, sind sie effektiv einsetzbar.

## Policy

Jede Organisation sollte eine E-Mail-Policy entwickeln, die ihrem Sicherheitsbedürfnis, ihrem Umgang mit dem Medium E-Mail und dem vorhandenen technischen Wissen und der Kapazität der IT-Abteilung gerecht wird. Diese Policy wird in die allgemeine Sicherheitspolicy eingebunden. Neben Anweisungen an die Mitarbeiter, wie sie mit ihrer Mailadresse und empfangenem Spam umzugehen haben, enthält die Policy grundsätzliche Entscheidungen zum Betrieb von Antispam-Lösungen (eigene Entwicklung, Einkauf einer Softwarelösung oder externen Dienstleistung). Sie bildet die Grundlage für Betriebsvereinbarungen, AGB und Service-Level-Agreements.

Die Policy legt auch fest, an welcher Stelle die Filterung erfolgen soll. Grundsätzlich gibt es dabei die Unterscheidung zwischen der serverbasierten Filterung und der Filterung im Mailprogramm des Endanwenders. Wegen der riesigen Mengen an Spam und der besseren Administrierbarkeit ist die Filterung durch einen zentralen Server meist sinnvoller, als die Filterung allein dem Empfänger zu überlassen. Eine vielversprechende Alternative ist die Kombination aus zentraler Vorfilterung und weiterer Filterung beim Endanwender.

Vor allem bei der zentralen Filterung stellt sich immer die Frage, wie erkannter Spam zu handhaben ist. Praktische Alternativen sind hier die Nicht-Akzeptanz oder die Markierung und Zustellung der E-Mail. Häufig unterscheidet man dabei drei Fälle: Sehr sicher als Spam erkannte E-Mails werden abgelehnt und sehr sicher als erwünscht erkannte E-Mails angenommen, alles dazwischen in einen speziellen Spam-Ordner oder ein Quarantänepostfach zugestellt.

Für größere Unternehmen und Internet-Provider gilt heutzutage, dass sie eventuell auch am Ausgang ihres Netzes einen Spamfilter einsetzen sollten, um Spam zu erkennen und zu blockieren, den die Rechner ihrer Mitarbeiter oder Kunden (meist ohne deren Wissen) versenden.

Teil einer Policy müssen auch vorbeugende Maßnahmen für eine Notfallsituation sein, wie sie bei einer neuen Spam- oder Virenwelle auftreten kann, die die Mailserver völlig überlastet. Auch dann soll deren Verfügbarkeit (zumindest eingeschränkt) erhalten bleiben.

Die technischen Möglichkeiten zur Spambekämpfung sind heute vorhanden. Deren konsequente Nutzung beseitigt das Problem zwar nicht, mildert aber die Folgen so weit ab, dass E-Mail effektiv einsetzbar bleibt.

## 3 Was ist Spam?

Während das Wort „Spam“ als Synonym für unerwünschte Inhalte erst dem Zeitalter weltweiter Computernetze entstammt, beschreibt der Begriff doch ein Grundproblem aller Kommunikationsformen: Jedes Medium dient früher oder später dazu, Nachrichten zu verbreiten, die aus Sicht der Mehrheit der Benutzer unerwünscht, lästig oder sogar gefährlich sind.

### Spam – Lovely Spam!

Der Begriff SPAM („Spiced Ham“) ist einer Markenbezeichnung der amerikanischen Firma Hormel Foods<sup>1</sup> für Frühstücksfleisch in Dosen entliehen. Zur Bezeichnung für unerwünschte E-Mail wurde Spam auf dem Umweg über einen Sketch der britischen Komiker-Truppe Monty Python [MPFC93]. In diesem Sketch preist eine Gruppe Wikin-ger laut singend den SPAM und unterdrückt damit jedwede sinnvolle Unterhaltung in einem kleinen Restaurant – genau der Effekt, den Spam-Nachrichten auf ein betroffene-nes Medium haben.

Der vorliegende Text konzentriert sich auf das besonders betroffene Medium E-Mail. Andere elektronische Verbreitungswege wie Instant Messaging, der Nachrichtendienst des Windows-Betriebssystems oder Newsforen des Usenet und deren Absicherung sind nicht zentraler Inhalt des Textes. Ebenso wenig geht er auf per Fax oder SMS verbreitete unerwünschte Nachrichten ein. Einige der vorgestellten Maßnahmen zur Bekämpfung von Spam sind allerdings auch geeignet, den Versand unerwünschter Nachrichten auf anderen Verbreitungswegen und in anderen Medien zu verhindern oder zu erschweren.

### 3.1 Definition von Spam

Die vorliegende Studie verwendet die folgende Definition:

*Der Begriff **Spam** bezeichnet **unverlangt zugesandte Massen-E-Mail**.<sup>2</sup>*

***Unverlangt** ist eine E-Mail dann, wenn das Einverständnis des Empfängers zum Empfang der Nachricht nicht vorliegt und nicht zu erwarten ist.*

***Massen-E-Mail** bedeutet, dass der Empfänger die Nachricht nur als einer von vielen erhält.*

Auf englisch bezeichnet man das als **UBE (Unsolicited Bulk Email, Unverlangte Massenmail)**.

Es reicht nicht, dass eine E-Mail unverlangt **oder** Massenmail ist. Zur Definition von Spam gehören beide Aspekte: Unverlangte, aber persönliche E-Mail ( z. B. von einem lange aus den Augen verlorenen Schulkameraden) ist nicht als Spam einzustufen, wie auch Massenmail dann kein Spam ist, wenn man mit dem Empfang einverstanden ist ( z. B. bei einem explizit abonnierten Newsletter).

Ein Newsletter, den ein Empfänger abonniert hat, wird nicht zu unverlangter E-Mail, nur weil der Empfänger es sich inzwischen anders überlegt hat und er den Newsletter nicht mehr erhalten möchte. Erst wenn der Empfänger seinen Wunsch, den Newsletter nicht mehr zu erhalten, gegenüber dem Absender ausgedrückt hat, wird der Newsletter bei weiterem Versand zu Spam.

1 [http://www.spam.com/ci/ci\\_in.htm](http://www.spam.com/ci/ci_in.htm)

2 Für weitere Definitionen siehe: <http://www.spamhaus.org/definition.html>, [http://www.mail-abuse.com/spam\\_def.html](http://www.mail-abuse.com/spam_def.html), <http://www.imec.org/ubef.html>

Als Abgrenzung von Spam dient häufig der Begriff **Ham** (englisches Wort für „Schinken“) zur Bezeichnung erwünschter E-Mails.

Bei der Beurteilung der Frage, ob eine Spam-Mail vorliegt, spielt es auch eine Rolle, ob sich Empfänger und Absender kennen. Bei Spam ist das praktisch nie der Fall, bei Ham besteht aber in der Regel eine Bekanntschaft oder Geschäftsbeziehung. Allein die Tatsache, dass sich Absender und Empfänger nicht kennen, ist aber noch keine hinreichende Voraussetzung für das Vorliegen von Spam.

Massenmail (*bulk email*) bedeutet, dass viele Empfänger eine Nachricht mit substantiell gleichem Inhalt per E-Mail erhalten. Massenmails können auch personalisiert sein (z. B. durch den Namen des Empfängers in der Anrede); das bedeutet aber nicht, dass eine E-Mail kein Spam ist, da sie sich trotzdem in gleicher Weise an viele Empfänger richtet und nicht auf die persönlichen Umstände des Einzelnen eingeht. Es kommt auch nicht darauf an, dass ein einzelner Empfänger mehr als eine E-Mail bekommt, sondern darauf, dass insgesamt viele E-Mails versandt wurden.

Der Inhalt einer E-Mail eignet sich weniger als Kriterium zur Definition des Begriffes „Spam“. Sicher gibt es typische Spam-Inhalte, aber hier wird die Entscheidung schnell subjektiv. Es sind Spam-Nachrichten im Umlauf, die so formuliert sind, dass ihr Inhalt durchaus eine gewöhnliche private Nachricht zwischen Bekannten darstellen könnte.

In der Regel hängt die Einschätzung, ob eine bestimmte E-Mail unerwünscht und damit als Spam zu klassifizieren ist, von der Wahrnehmung und den Einstellungen des Empfängers ab. Spam ist also immer auch subjektiv, die gleiche E-Mail kann der eine als Spam und der andere als Ham einordnen. Trotzdem sind die Kategorisierungen und Begriffserklärungen in diesem Kapitel allgemein akzeptiert.

Die juristische Definition von Spam unterscheidet sich von der hier verwendeten. In der EU ist zurzeit nur der kommerzielle Spam verboten (siehe Kapitel 6).

### 3.2 Spam und ähnliche Phänomene

Es gibt eine ganze Reihe verschiedener Arten von Spam und Spam-ähnlicher E-Mails, die sich unter anderem nach Intention des Spammers, Wirkung oder Verbreitungswegen unterscheiden lassen. Bei den meisten Spam-Mails, die heute in den Postfächern der Anwender landen, handelt es sich um kommerzielle Werbung, daneben gibt es aber viele weitere Kategorien von Spam und anderen „Problem-E-Mails“.

#### 3.2.1 Kommerzielle Werbung

Ein Versender geschäftlichen Werbe-Spams, formal auch als **UCE** bezeichnet (**U**nsolicited **C**ommercial **E**mail, übersetzbar mit „unverlangter kommerzieller E-Mail“), hat die Absicht, den Empfänger zur Bestellung eines Produktes oder einer Dienstleistung zu animieren. Der Versand von UCE ist in Deutschland in der Regel unzulässig, mehr Informationen dazu folgen in Kapitel 6. Kommerzielle Werbung durch Spam wird heute kaum noch von seriösen Firmen betrieben. Die Spammer bewerben typischerweise pornographische Webseiten, potenzsteigernde Mittel, fragwürdige Diätpillen oder ähnliche Produkte. Viele Spams gehen nicht direkt von den Betreibern einer Webseite aus, sondern von Spammern, die für die Vermittlung neuer Kunden Prämien erhalten.

#### 3.2.2 Nicht-kommerzielle Werbung

Werbung muss nicht unbedingt kommerzieller Natur sein. Auch die Übermittlung religiöser, weltanschaulicher oder politischer Ideen wie das Anpreisen eines Kandidaten während Wahlperioden

mit dem Zweck, den Wähler zu beeinflussen, oder die Verbreitung extremistischer Propaganda kann im weitesten Sinne als Werbe-Spam eingestuft werden.

### 3.2.3 Malware

Ebenfalls im elektronischen Postkasten der Opfer landen verschiedene Formen von **Malware** (Schadsoftware). **Viren** und **Würmer**, die sich über Schwachstellen im PC, aber auch per E-Mail verbreiten, gehören in diese Kategorie, ebenso **Trojaner**<sup>3</sup> (Schadprogramme, die sich als harmloses Programm tarnen) und **Spyware**, die den Benutzer und sein System ausspähen.

Die Erkennung und Bekämpfung dieser Art von Computer-Schädlingen erfolgt häufig mit recht ähnlichen Methoden wie die sonstige Spam-Bekämpfung. Die Art, wie sie programmiert sind (beispielsweise die Mechanismen zur Selbstverbreitung) und ihre Schadroutinen (*payload*) machen diese Form der Schadsoftware jedoch zu einem grundlegend anderen Untersuchungsgegenstand als Spam. Außerdem verfolgt Malware meist das Ziel, das Computersystem eines Opfers zu attackieren. Sonstiger Spam dagegen zielt typischerweise auf den Menschen, der das System bedient, und buhlt um seine Aufmerksamkeit.

In der vorliegenden Studie wird Malware lediglich am Rande betrachtet. Die Funktionsweise, Erkennung und Bekämpfung von Malware sind nicht Thema dieser Studie.

### 3.2.4 Betrug und Phishing

Auch Betrüger benutzen das Medium E-Mail, um potentielle Opfer zu erreichen. Die Absender bauen auf die Gutgläubigkeit und Gewinnsucht der Menschen. Bekanntestes Beispiel: der **Nigeria-Scam**<sup>4</sup> (wobei „Scam“ übersetzbar ist mit „Betrug“ oder „Masche“). E-Mails mit Betreffzeilen wie „Confidential Business Proposal“ versprechen dem Empfänger meist sehr große Geldsummen. Beißt das Opfer an, wird es aufgefordert, mit einer kleineren Summe in Vorleistung zu treten, etwa um die „Überweisungsgebühren“ zu tragen. Die versprochenen Millionen kommen natürlich nie an, und das Opfer bleibt auf seinem Verlust sitzen. Ähnliches versuchen Kriminelle, die dem Empfängereinen großen Lotteriegewinn in Aussicht stellen, für dessen Übermittlung sie eine „Bearbeitungsgebühr“ fordern.

**Phishing**-Mails (hergeleitet von engl. *fishing*, also dem „Fischen“ mit einem Köder) sind eine Masche von Internet-Betrügern, die das Opfer zur Preisgabe sensibler Daten wie Kreditkartennummern, PINs, TANs oder Passwörtern verleiten soll. Dazu nehmen die Kriminellen die Identität einer Online-Einrichtung an (Bank, Auktionshaus, Web-Shop o. Ä.), oft mit täuschend echt nachgemachten E-Mail-Designs und Webseiten. Das Opfer wird in der E-Mail aufgefordert, die (gefälschte) Website aufzurufen und dort beispielsweise ein Passwort zu ändern oder die persönlichen Daten nach PIN-Eingabe zu aktualisieren.<sup>5</sup>

### 3.2.5 Rufschädigung und Provokation von Angriffen

Eine besonders perfide Variante von Spam nutzt die leichte Fälschbarkeit von E-Mails dazu aus, Spam in fremdem Namen zu verschicken, in der Erwartung, dass viele Empfänger sich beim vermeintlichen Absender oder dessen Firma oder Internet-Provider beschweren oder ihn sogar aus Rache angreifen werden.

3 Ursprünglich wurde für solche Programme der Begriff „Trojanisches Pferd“ verwendet, der historisch korrekter ist [Vergil]. Inzwischen hat sich aber allgemein der kürzere Begriff „Trojaner“ (trojan) durchgesetzt.

4 <http://www.tu-berlin.de/www/software/hoax/419.shtml>

5 <http://www.antiphishing.org/>

Im März 1997 wurde der Amerikaner Joe Doll Opfer einer solchen Aktion.<sup>6</sup> Er hatte einen Spammer aus seinem System verbannt, der sich so an ihm rächte. In Folge einer wahren Flut von Beschwerden, E-Mail-Fehlermeldungen und anderen Angriffen war das System von Joe Doll für zehn Tage nicht erreichbar, der Effekt war also ein verteilter Denial-of-Service-Angriff (*DDoS attack*) auf das Opfer. Seither wird das gezielte Fälschen von E-Mails zur Rufschädigung als **Joe Job** bezeichnet. Vor allem Antispam-Aktivisten werden immer wieder das Ziel solcher Aktionen.

#### 3.2.6 Kettenbriefe

Immer wieder kommt es vor, dass Anwender auf **Hoaxes** (Falschmeldungen, Scherze) und **Kettenbriefe** hereinfließen und sie in gutem Glauben weiterschicken. Initiatoren von Kettenbriefen setzen auf die Gutgläubigkeit der Empfänger und appellieren an deren Gewinnstreben oder ihr gutes Herz. Das Besondere bei dieser Art der Spam-Verteilung ist, dass Spammer ihre Nachrichten nicht durch Lücken oder Schwachstellen in technischen Systemen verteilen, sondern die „Schwachstelle Mensch“ ausnutzen.

Hoaxes können in vielen Formen vorkommen. Ein Beispiel sind fingierte Meldungen namhafter Unternehmen wie Microsoft oder AOL, die vor einer bisher unbekanntem Schwachstelle in einem ihrer Produkte warnen. Verbunden mit der Aufforderung, die Nachricht an andere Personen zu verteilen, raten die Verfasser dazu, bestimmte Veränderungen am System wie das Löschen von Systemdateien vorzunehmen.<sup>7</sup> Wer den Rat befolgt, fügt in den meisten Fällen seinem System Schaden zu.

Mehr auf die Gutgläubigkeit und Warmherzigkeit der Empfänger zielen fingierte Spendenaufrufe, meist in Verbindung mit einer rührseligen Geschichte, bevorzugt über ein todkrankes Kind. Auch nach dem Tsunami in Südostasien Ende 2004 gab es wieder eine Welle von E-Mails mit Bildern von verletzten Kindern, die angeblich ihre Eltern suchen. Solche E-Mails fordern den Empfänger auf, sie weiter zu verbreiten. Viele kursieren seit Jahren im Internet. Der ursprüngliche Anlass ist vielleicht längst vergessen oder erledigt, und trotzdem werden die E-Mails wieder und wieder weitergegeben. Statt die Falschmeldungen weiter zu verbreiten, sollte man sich auf einschlägigen Webseiten<sup>8</sup> über den Wahrheitsgehalt informieren.

Eine weitere Variante sind illegale **Schneeball-** oder **Pyramidensysteme**, bei denen der Empfänger an den Absender einen Geldbetrag entrichten soll und die Kettenmail dann in der Hoffnung weiterversendet, dadurch in die Position des Geldempfängers zu gelangen.

#### 3.2.7 Kollateraler Spam

In eine ganz andere Kategorie als die direkt versandten Nachrichten fällt kollateraler Spam. Bevor eine E-Mail den Empfänger erreicht, wandert sie über mehrere Systeme, die für ihre Verarbeitung oder Weiterleitung zuständig sind: MTAs (Mail Transfer Agents), aber auch virenschneidende *relays* gehören dazu. Tritt ein Fehler auf, etwa weil die E-Mail nicht ausgeliefert werden kann oder weil sie einen Virus enthält, senden diese Systeme oft **Fehlermeldungen** (*bounces*) an den vermeintlichen Absender zurück. Da Spam und Viren aber häufig eine gefälschte Absenderadresse tragen, erreichen viele dieser Fehlermeldungen unschuldige Opfer. Solcher Spam wird als **kollateraler Spam** (*colateral spam*) bezeichnet.

---

<sup>6</sup> <http://www.joes.com/spammed.html>

<sup>7</sup> <http://www.tu-berlin.de/www/software/hoax/jdbgmgr.shtml>

<sup>8</sup> <http://www.tu-berlin.de/www/software/hoax.shtml>, <http://www.snopes.com/>

### 3.3 Warum ist Spam ein Problem?

Das Internet ermöglicht den vollautomatischen Versand von Nachrichten. Dadurch ist der Mailversand sehr billig und schnell. Der Absender trägt nur einen geringen Teil der Kosten, den anderen Teil trägt der Empfänger oder die Allgemeinheit. Wenn Spammer fremde Rechner und Netze illegal mitbenutzen, können sie ihren Teil der Kosten weiter minimieren.

#### 3.3.1 Wirtschaftliche Schäden

Auch unter der Annahme, dass nur ein Prozent der Spam-Mails überhaupt wahrgenommen wird und wiederum ein Prozent davon zu Umsatz führt, handelt es sich bei Spams um eine extrem erfolgreiche Werbeform mit einer sonst unerreichbaren Gewinnspanne, wie eine Beispielrechnung zeigt:

| Spammer-Profit versus betriebswirtschaftlicher und persönlicher Schaden bei den Empfängern |                                    |  |  |
|--|------------------------------------|--|--|
|  | Spammer                            | Spam-Auftraggeber                          | Empfänger-Kosten (ohne Filter)   |
| 1.000.000 Spams versenden bzw. empfangen   | Kosten: 100 €                      | -  | 140.000 € (nur Arbeitszeit, bei 10 s Bearbeitungszeit pro Spam-E-Mail und 50 € Arbeitskosten pro Stunde) |
| Lesen von 1,00% der Spams  | -                                  | -  | 8.000 € (nur Arbeitszeit, bei weiteren 60 s für Lesen + WWW)   |
| Kundengewinnung durch 0,01 % der Spams   | -                                  | -  | 400 € (nur Arbeitszeit, bei weiteren 300 s für die Bestellung)   |
| Umsatz bei 100 erfolgreichen Spams und 50 € pro Bestellung                                 | Einnahmen: 1.500 € (30% Provision) | 5.000 € - 1.500 € Provision an den Spammer | Ausgaben: 5.000 € für ein oft illegales oder nutzloses Produkt   |
| Ergebnis   | 1.400 €                            | 3.500 €                                    | <b>-153.400 € Schaden</b>  |

Tabelle 3.1: Beispielrechnung für einen Spam-Lauf

Der bei allen Empfängern summierte betriebswirtschaftliche Schaden durch Spam liegt um Größenordnungen über dem Gewinn auf Seiten des Absenders. Wenn nur zwei Kunden anbeißen, sind bereits die Kosten für den Versand gedeckt. Die Tabelle führt die Zahlen für den Spammer und seinen Auftraggeber getrennt auf, weil Spammer oft im Auftrag Dritter arbeiten.

Spam kostet nicht nur Arbeitszeit beim Löschen, sondern kann darüber hinaus auch die Netzinfrastruktur einer Firma oder eines ISP (Internet Service Provider) gefährden.

Laut einer Studie von Nucleus Research aus dem Jahre 2004 kostet Spam in den USA ein Unternehmen im Durchschnitt 1.934 \$ pro Mitarbeiter und Jahr.<sup>9</sup> Ferris Research beziffert den

<sup>9</sup> <http://www.nucleusresearch.com/research/e50.pdf>

Gesamtschaden durch Spam auf 10 Mrd. \$ jährlich in den USA.<sup>10</sup> Für Europa errechnet diese Studie einen Schaden von 3 Mrd. \$.

Derartige Kosten und Schätzungen ergeben sich, wenn man die Zusammensetzung des gesamten Mailaufkommens betrachtet. Zurzeit geben verschiedene Studien unterschiedliche Spamanteile im Mailaufkommen an. Die Werte schwanken zwischen 60 % und 90 %.<sup>11</sup> Damit ist sowohl die absolute Zahl von Spam-Mails in den letzten Jahren starkgestiegen als auch deren relativer Anteil im Vergleich zu Ham. Darüber hinaus ist der Anteil der Viren-Mails am gesamten Mailaufkommen mit 2% bis 10 % beziffert.

Das Medium E-Mail ist demnach ohne geeignete Schutzmaßnahmen zumindest stark beeinträchtigt, in einigen Fällen sogar lahm gelegt. In jedem Fall wäre dieses Medium ohne Spamschutzmaßnahmen nicht mehr sinnvoll nutzbar. Das von Spammern oft vorgebrachte Argument, dass man unerwünschte E-Mail ja einfach löschen könne, greift also deutlich zu kurz.

## Mehr Spam durch mehr Filter?

Die Anwender von E-Mail sind derzeit die Leidtragenden in einem sich selbst verstärkenden Prozess: Mit der Ausbreitung von Mailfiltern wächst für die Spamversender die Notwendigkeit, den Ausstoß unerwünschter E-Mails zu erhöhen, damit die gewünschte Zahl von Aussendungen bis zu den Empfängern durchdringt. Damit sehen sich wiederum mehr Anwender gezwungen, Filtersysteme einzusetzen, da sie sonst das Medium angesichts des stark wachsenden Spam-Anteils gar nicht mehr nutzen können. So gut technische Lösungen funktionieren mögen, die Spirale kommt erst dann zu einem Ende, wenn nicht die Auswirkung (Spam im Posteingang), sondern die Ursache (das Versenden von Spam) behoben ist.

### 3.3.2 Die Spammer

Der Versand von Spam bringt mit wenig Aufwand viel Geld ein [McWi04], und das bei geringem Risiko. Es gibt seit geraumer Zeit in vielen Ländern Gesetze gegen Spam, doch Spammern wird so selten das Handwerk gelegt, dass die wenigen Fälle bis heute für Schlagzeilen sorgen.

Professionelle Spammer, von denen es nach Schätzungen des Spamhaus Project<sup>12</sup> nur rund 200 weltweit gibt, sind für den weitaus größten Teil des Spams verantwortlich. Tatsächlich zeigt ein Blick in einen durchschnittlichen Spam-Ordner, dass mindestens 90 % der unerwünschten E-Mails immer wieder ähnliche Inhalte haben. Die Spamversender bieten die beworbenen – meist dubiosen – Produkte und Dienstleistungen oft nicht selbst an, sondern im Auftrag der eigentlichen Anbieter oder weiterer Mittelsmänner. Rücklauf und Abschlussquote lassen sich mit heutiger Internet-Technik leicht ermitteln, da die späteren Kunden in der Regel über URLs mit entsprechenden Tracking-Informationen auf die Seiten der Anbieter gelangen.

Während Mitte der 90er Jahre der typische Spammer meist nur gelegentlich Spam versandte, um zum Beispiel für ein eigenes Produkt zu werben, sind die meisten Spammer heute Profis, die sehr genau wissen, was sie tun. Immer öfter arbeiten Spammer auch mit eindeutig kriminellen Methoden. Sie stehlen Adressdaten und nutzen Würmer und Trojaner, um fremde Rechner zu infizieren, die sie dann wiederum zum Spamversand benutzen. Es gibt einen regelrechten Untergrundhandel mit Mailadressen

---

<sup>10</sup> <http://www.heise.de/newsticker/meldung/33417>

<sup>11</sup> siehe z. B. <http://www.spamhaus.org/news.lasso?article=156>, <http://www.message-labs.com/emailthreats/default.asp>

<sup>12</sup> <http://www.spamhaus.org/>

und Listen von offenen Proxy-Servern<sup>13</sup> (siehe Kapitel 4.2.3). Selbst die Kontrolle über ganze „Botnetze“ (siehe Kapitel 4.2.5) wird vermietet oder verkauft [Fern04].

---

<sup>13</sup> [http://matthias.leisi.net/archives/80\\_Spam\\_Biz.html](http://matthias.leisi.net/archives/80_Spam_Biz.html)

## 4 Wie Spam funktioniert

Vor einer Klärung der Frage, wie Spam bekämpft werden kann, sind einige Erläuterungen zur Funktionsweise von E-Mail notwendig.

### 4.1 Technische Grundlagen

Dieses Kapitel erklärt im Schnelldurchlauf einige technische Grundlagen des weltweiten Mailsystems, ohne die die Funktionsweise von Spam nicht zu verstehen ist. Es kann aber eine Einführung für den Anfänger nicht ersetzen. Wer sich näher mit der Materie auseinandersetzen möchte, findet Einführungen in [John99] und [Wood99].

#### 4.1.1 Simple Mail Transfer Protocol (SMTP)

Praktisch jede E-Mail im Internet wird per Simple Mail Transfer Protocol (SMTP, [RFC2821]) auf den Weg gebracht. Die Eigenheiten dieses Protokolls wirken sich daher erheblich auf die Art und Weise aus, wie E-Mail (und damit auch Spam) im Internet technisch funktioniert.

SMTP stammt aus den frühen 1980er Jahren und damit aus einer Zeit, als noch nicht jeder Rechner mit einer Mailclient-Software ausgestattet war und als sich alle Betreiber von Internet-Servern gegenseitig mehr oder weniger vertrauen konnten. Es ist im wahrsten Sinne des Wortes möglichst „simple“ gehalten, so dass jeder – zwecks Fehlersuche – mit einem einfachen Terminal-Programm E-Mails versenden kann, von jedem ans Internet angeschlossenen Rechner und mit wenigen Zeilen Klartext [RFC2821].

---

**220 mail.example.com ESMTP**

EHLO mail.example.org

**250-mail.example.com Hello mail.example.org [192.0.2.17] 250-SIZE**

**250 PIPELINING**

MAIL FROM:<absender@example.org>

**250 OK**

RCPT TO:<empfaenger@example.com>

**250 Accepted**

RCPT TO:<person@example.com>

**250 Accepted**

DATA

**354 Enter message, ending with „.“ on a line by itself**

*...header und body... .*

**220 OK**

QUIT

**221 mail.example.com closing connection**

---

*Beispiel für eine SMTP-Sitzung: Zu keinem Zeitpunkt wird hier die Echtheit des Absenders oder anderer Daten, die der Absender liefert, überprüft. Den wirklichen Absender zu verschleiern ist also trivial.*

Bei SMTP treten der sendende Rechner (Client) und der empfangende Rechner (Server) in einen Dialog. Nach einer Begrüßung durch den Server und Anmeldung durch den Client (HELO/EHLO) schickt der Client zunächst die Absenderadresse (MAIL FROM) und die Liste der Empfängeradressen (RCPT TO) einer E-Mail. Nach dem DATA-Befehl kommen die Kopfzeilen (*header*) und der eigentliche Inhalt der E-Mail (*body*). Der Server hat in jedem Schritt die Möglichkeit, den Empfang der E-Mail abzulehnen und kann dazu einen permanenten (5xx) oder temporären (4xx) Fehlercode erzeugen. Temporäre Fehlercodes kommen z. B. beim Greylisting (siehe Kapitel 9.13) zum Einsatz.

Dieses mehrstufige Verfahren ermöglicht es, den Empfang einer E-Mail auch dann abzulehnen, wenn der Inhalt noch nicht übertragen ist. Dadurch lässt sich ein erheblicher Aufwand auf Empfängerseite sparen.

Ebenso lässt sich der Empfang einer E-Mail für einzelne Empfänger ablehnen, für andere akzeptieren. Das geht allerdings nur vor Übertragung des Inhalts der E-Mail. Diese Eigenschaft von SMTP erschwert die Einrichtung benutzerkonfigurierbarer Spamfilter an zentraler Stelle auf den Mailservern.

### 4.1.2 Envelope, Header und Fälschungen

Versand, Transport und Zustellung von E-Mails im Internet sind mit den Vorgängen bei der Papierpost vergleichbar. Auch wenn E-Mails häufig mit Postkarten verglichen werden<sup>1</sup>, liegt technisch gesehen der Vergleich mit Briefen näher. So hat eine E-Mail einen für die transportierende Organisation entscheidenden Umschlag (*envelope*) mit der Empfängeradresse (Envelope-To) und einen größeren Teil im Umschlag, der mit dem Transport nichts weiter zu tun hat: einen Briefkopf (*header*) und die eigentliche Nachricht (*body*). Die Envelope-Adressen bekommt der Adressat in der Regel gar nicht zu Gesicht, denn es handelt sich lediglich um Parameter des SMTP-Dialogs, und dem MTA-Administrator steht es frei, ob und in welcher Form diese Parameter im *header* erscheinen sollen. In aller Regel ist zumindest die Envelope-From-Adresse in der Header-Zeile Return-Path: angegeben.

Es gibt lediglich einen SMTP-Parameter, der für den Mail-Transport notwendig ist und den ein Spammer daher nicht nach Belieben angeben kann: Die Envelope-Adresse des Empfängers. Außerdem ist die IP-Adresse des absendenden Computers nicht fälschbar, da sonst die zugrunde liegende TCP-Verbindung nicht zu Stande kommen kann.<sup>2</sup> Diese IP-Adresse schreibt der empfangende MTA in eine Received:-Zeile im *header* (Received: from ... [IP-Adresse]), gefolgt von einem Zeitstempel. Nichts hindert den Spammer daran, nach Belieben eigene Received:-Zeilen hinzuzufügen, um die Spam-Herkunft zu verschleiern, was in der Praxis häufig passiert. Auch alle anderen Daten sind praktisch frei wählbar, insbesondere die Envelope-Adresse des Absenders. Die Header-Informationen, die der Adressat zu Gesicht bekommt, beschränken sich meist auf die From:-, To:- und Subject:-Zeilen. Bei diesen handelt es sich jedoch aus Sicht von SMTP lediglich um Nutzdaten (nach dem DATA-Befehl) ohne jegliche Relevanz für Transport und Zustellung der E-Mail.

Dem Spamproblem recht nahe kommt die folgende Analogie zur Papierpost: Jeder Absender darf anonym und unkontrolliert beliebige Sendungen in beliebiger Menge in beliebige Postkästen stopfen. Die Post ist durch Gesetze und Richtlinien (bei E-Mail: in RFCs festgelegte Protokolle) gezwungen, alles unbesehen zum Adressaten zu transportieren, solange eine gültige Empfängeradresse auf dem Brief steht. Nur ein paar Mindestvoraussetzungen wie die Einhaltung von Maßen und Gewichten

<sup>1</sup> Weil E-Mail in der Regel unverschlüsselt übertragen wird, ist der Inhalt für jeden, der die E-Mail transportiert, einsehbar. Der *envelope* im Sinne des SMTP dient nur der Adressierung der E-Mail. Er hat nicht die schützende Funktion wie der Umschlag eines Papierbriefes.

<sup>2</sup> Genauer: Der Aufwand, eine IP-Adresse zu fälschen, ist so erheblich, dass es in der Praxis kaum vorkommt. Jemand, der IP-Adressen fälschen kann, wird mit dieser Möglichkeit „besseres“ anfangen, als nur Spam zu verbreiten.

sowie die korrekte Frankierung muss der Absender erfüllen. Allerdings ist hier die Analogie auch schon zu Ende: Es gibt keine Briefmarken für E-Mails. Der Versand von E-Mails ist so viel billiger und schneller als derjenige von Papierpost, dass sich anders als bei Briefwerbung der Versand von Spam auch dann lohnt, wenn sehr wenige der Angeschriebenen im Sinne des Spammers reagieren.

Die IP-Adresse des Absenders hat ebenfalls kein Pendant: Eine Protokollierung, welchen Postkasten der Absender zu welchem Zeitpunkt benutzt hat, findet bei der gelben Post nicht statt. Diese eindeutige Information ist Spamversendern natürlich ein Dorn im Auge, und ironischerweise hat das mit dazu geführt, dass es heute derart viele Spam-Quellen gibt.

| Papierpost („Snail Mail“)   | E-Mail-/SMTP-Entsprechung  |
|---|--|
| Gelber Postkasten (unbewacht)   | Absender-Gateway ( <i>open relay, proxy, ...</i> )   |
| Öffnen der Klappe   | HELO ... (ein regulärer SMTP-Client lässt meist seinen DNS-Namen folgen)   |
| Absender-Adresse<br>(reine Formsache)   | MAIL FROM: <...@...> (Envelope-From-Adresse, beliebig, wird meist nicht geprüft und kann sogar leer sein)  |
| Empfänger-Adresse (für die Zustellung unabdingbar)                              | RCPT TO: <. ..@. .> (Envelope-To-Adresse, notwendig für die Zustellung. Im Unterschied zur Papierpost sind mehrere Empfänger möglich, die vom Empfänger-Gateway angefertigte, identische Kopien erhalten.) |
| Inhalt des Briefs   | DATA (vollkommen beliebig und fälschbar, inklusive Header-Bestandteilen wie From:- und weiterer Received:-Zeilen)  |
| Schließen der Klappe  | .  |
| Ort und Zeitpunkt des Einwerfens werden bei der Papierpost nicht protokolliert. | Recei ved: from .. . IP-Adresse .. . Zeitstempel (die einzigen nicht fälschbaren Anhaltspunkte in einer vom Empfänger-MTA selbst erzeugten zusätzlichen Header-Zeile)                                      |
| Die Post bringt den Brief vom gelben Postkasten zum Briefkasten des Empfängers. | Ein oder mehrere Relays reichen die E-Mail bis zum Mailbox-Server des Adressaten weiter.   |
| Briefkasten öffnen und Post entnehmen   | Der Mailclient des Empfängers ruft E-Mails per Internet Mail Access Protocol (IMAP) oder Post Office Protocol (POP) vom Mailbox-Server ab.   |

Tabelle 4.1: Analogien zwischen Papierpost und E-Mail

### 4.1.3 Fehlermeldungen

Wenn eine E-Mail nicht zustellbar ist, hat die Empfängerseite zwei Möglichkeiten, den Absender darauf hinzuweisen: Entweder lehnt der Mailserver bereits im SMTP-Dialog die Übernahme der E-Mail mit einem Fehlercode ab oder er nimmt sie zunächst an und erzeugt später eine neue E-Mail (*bounce*) mit einer Fehlermeldung. E-Mails gelangen häufig durch mehrere Mailserver an ihren Bestimmungsort. Jeder von ihnen kann die E-Mail annehmen und weiterleiten, ablehnen oder eine Fehlermeldung zurückschicken.

Die Ablehnung der E-Mail mit einem SMTP-Fehlercode ist dabei in jedem Falle vorzuziehen. Das benötigt weniger Ressourcen und vermeidet vor allem den Versand von Fehlermails an Anwender, deren Adresse ein Spammer unerlaubt benutzt und die gar nichts mit dem Spamversand zu tun haben. Falls eine E-Mail nicht zustellbar ist, wird der MTA oder der MUA auf Seiten des Absenders mit Hilfe des Fehlercodes den Absender darüber informieren.

Leider gibt es aber auch heute noch viele Mailsysteme, die trotzdem E-Mails annehmen und erst später eine Fehlermeldung zurücksenden, weil sie zur Zeit der Annahme der E-Mail noch nicht erkannt haben, dass eine spätere Zustellung nicht möglich ist. Dadurch landen viele E-Mails mit Fehlermeldungen zu Spam und Viren-Mails in den Postfächern der vermeintlichen Absender. Insbesondere bei Weiterleitungen (*forward*) von E-Mails gibt es leider Fälle, in denen es sich nicht vermeiden lässt, eine *bounce* statt einer direkten Fehlermeldung zu erzeugen, da zum Zeitpunkt der Annahme der E-Mail noch nicht feststeht, ob die Weiterleitung funktionieren wird.

#### 4.1.4 Der Weg einer E-Mail

Typischerweise erzeugt der Mailclient des Absenders eine E-Mail und versendet sie über den MTA des Providers oder des eigenen Unternehmens an den Mailserver des Empfängers. Der nimmt die E-Mail entgegen und stellt sie in die Mailbox des Adressaten zu.

SMTP dient sowohl der Auslieferung der E-Mail vom Kunden zum Provider als auch der Weiterleitung zwischen den Providern. Der Mailserver des Providers muss die E-Mail weiterleiten (*relay*). Früher waren alle SMTP-Server als „offene Relays“ (*open relay*) konfiguriert. Jeder konnte jeden SMTP-Server verwenden, um E-Mails an Dritte zu senden. Weil Spammer diese Offenheit aber ausnutzten, um die Herkunft des Spam zu verschleiern und die Last bei anderen abzuladen, ist das heute nicht mehr üblich (siehe 4.2.2).

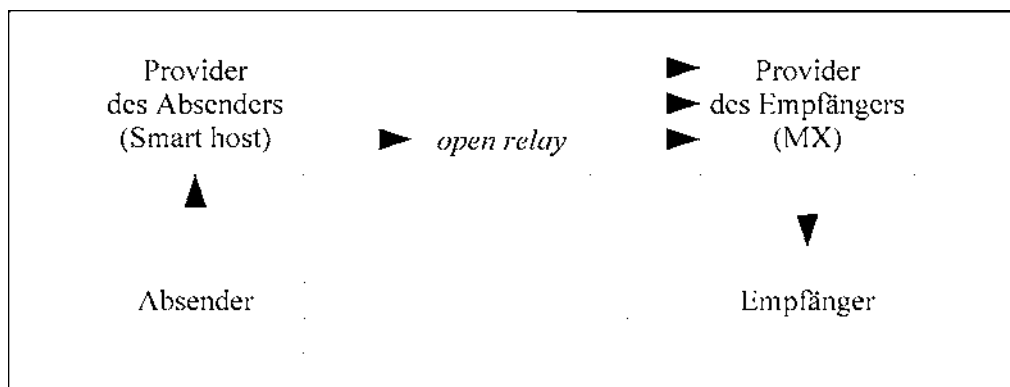


Abb. 4.1: Zustellung einer E-Mail über verschiedene Wege

Theoretisch kann ein Kunde seine E-Mail auch direkt an den MX des Empfängers senden. Da aber gerade Spammer und Wurmprogramme diese Art des direkten Versands nutzen, schränken die Provider diese Möglichkeit immer weiter ein. Das passiert einerseits durch Sperren des SMTP-Ports auf Seiten des Zugangsproviders, andererseits durch den Eintrag von (dynamischen) IP-Adressen, die typischerweise von Endkunden genutzt werden, in Blacklists. Diese Blacklists kommen auf vielen Mailservern für das Filtern zum Einsatz.

Die Folge davon ist, dass Spammer anfangen, die Authentifizierungsdaten von Benutzern auf kompromittierten Rechnern auszulesen und zum Versand von Spam über den Mailserver des Providers zu nutzen. Es wird damit verstärkt zur Aufgabe der Provider, nicht nur eingehende, sondern auch ausgehende E-Mails auf Spam zu überprüfen (*egress* oder *outbound filtering*).

## 4.2 Spamversand

Über die letzten Jahre haben sich die Methoden des Spamversands mehrfach geändert. Spammer versuchen immer wieder neue und wirksamere Methoden zu benutzen, wenn ihnen die alten Wege durch Filtermaßnahmen verbaut werden.

Schon 1978 verschickte ein Hersteller von Minicomputern Werbung für seine Systeme über das Arpanet (den Vorgänger des Internet) per E-Mail an zahlreiche Empfänger<sup>3</sup>. Den Begriff „Spam“ gab es damals in diesem Zusammenhang aber noch nicht. Im Internet-Newsgruppensystem Usenet kam eine US-Anwaltskanzlei<sup>4</sup> Anfang der 1990er Jahre zu zweifelhafter Berühmtheit, als sie per Massen-Posting für eine Greencard-Verlosung warb. In diese Zeit fällt die erstmalige Benutzung von „Spam“ als Beschreibung unerwünschter Internet-Inhalte, damals vor allem kommerziell orientierter Usenet-Beiträge. Diese Bezeichnung war jedoch nicht zuerst im Internet, sondern schon in den 80er Jahren in Mailbox-Systemen (BBS) gebräuchlich und bezeichnete störende Beiträge in digitalen Foren.

### Usenet-Spam

Schon die Nutzung des Usenet zur Verbreitung von Spam Anfang der 1990er Jahre hatte einen prinzipiellen Wandel des Sendeverfahrens markiert: Die Nutzung fremder Infrastruktur (hier die der Usenet-Teilnehmer) zur Verteilung der unerwünschten Nachrichten. Spammer brauchten nicht mehr jeden einzelnen Empfänger selbst zu beschriften, sondern nur noch ein einziges Dokument zu „posten“, das die Usenet-Teilnehmer innerhalb kurzer Zeit an beliebig viele Leser beliebiger Newsgruppen verteilten. Der Missbrauch fremder Infrastrukturen ist heute typisch für den Großteil des Spams und hat im Laufe eines Jahrzehnts eine bedrohliche Eigendynamik entwickelt.

#### 4.2.1 Spam-Server

Der technisch nahe liegendste und in den 1990er Jahren häufig genutzte Weg, Spam zu versenden, ist der Betrieb eigener Mailserver. Noch heute stammt ein nennenswerter Teil des Spams aus festen IP-Adressbereichen. Allerdings ist dieses Phänomen rückläufig, weil einerseits die Empfänger über einfaches Blacklisting der Spammer-Netzbereiche viel Spam vorab aussortieren können und andererseits der Missbrauch fremder Infrastruktur weniger kostet als die Verwendung eigener Server.

#### 4.2.2 Open Relays

Bis in die 1990er Jahre war es üblich, dass Mailserver nicht nur E-Mails von und an die eigene Domain zustellten, sondern als *open relay* auch aus beliebigen Domains in beliebige andere. Das war kein Konfigurationsfehler, sondern entsprach dem Gedanken der Fehlertoleranz: Funktionierte der eigene Mailserver einmal nicht, konnte der Absender einfach auf einen anderen Mailserver ausweichen, der sich nicht unbedingt im eigenen Netz befinden musste. Dieses System war so offensichtlich missbrauchs anfällig, dass es mittlerweile keine nennenswerte Zahl von *open relays* mehr gibt. Es gibt aber immer wieder fehlerhafte Konfigurationen, die dann doch wieder zu *open relays* führen.

Damit Kunden eines Providers weiterhin E-Mails über den Server des Providers versenden können, hat sich inzwischen die SMTP-Erweiterung SMTP AUTH durchgesetzt. Dazu muss sich der Kunde (genauer gesagt sein Mailprogramm) beim Provider mit einem Passwort authentifizieren, bevor der

---

<sup>3</sup> <http://www.templetons.com/brad/spamreact.html>

<sup>4</sup> <http://www.templetons.com/brad/spamterm.html>

Mailserver die Mail annimmt und weiterleitet.<sup>5</sup> Ein älteres Verfahren namens SMTP-after-POP wird auch gelegentlich verwendet: Für eine gewisse Zeitspanne, typischerweise zehn Minuten, geht das Relay davon aus, dass ein Anwender, der gerade seine POP-Mailbox per User-ID und Passwort abgefragt hat, E-Mails versenden darf. Die Zuordnung findet dabei über die IP-Adresse des Clients statt.

### 4.2.3 Open Proxies

Anders als offene Mailrelays lassen sich *open proxies* für die Vermittlung und letztlich Verstärkung nahezu beliebigen Internet-Datenverkehrs einsetzen und missbrauchen.

Proxies sind an sich ein regulärer Bestandteil vieler Internet-Installationen. Sie dienen zum Beispiel zum Überwinden von Firewall-Grenzen und (in Verbindung mit Caches) dazu, WWW-Datenverkehr auf der teuren Standleitung zum Provider zu reduzieren, indem sie Web-Inhalte zwischenspeichern und den Anwendern des lokalen Netzes direkt zur Verfügung stellen. Fehlkonfigurierte Proxies, die eine Nutzung von außerhalb des eigenen LAN erlauben, sind dankbare Opfer von Spammern, die E-Mails über diese Zwischenstationen absenden können, meist ohne Wissen des Proxy-Betreibers. Die eigentlichen Spam-Quellen tauchen anders als bei der Nutzung offener Relays nicht in den Received-Zeilen auf, und bestenfalls gäbe eine Logdatei des offenen Proxy darüber Auskunft. Doch Spammer auf diese Weise dingfest machen zu können, ist illusorisch: Wer einen Proxy falsch konfiguriert, wird meist auch keine Logdateien zur Verfügung stellen können. Zudem können Spammer die Spuren nahezu perfekt verwischen, indem sie ihre E-Mails über ganze Proxy-Ketten lenken.

### 4.2.4 Unsichere CGI-Skripte

Auf vielen interaktiv gestalteten Webseiten (Grußkarten, Blogs, Gästebücher, ...) können Websurfer per Submit-Knopf E-Mails in alle Welt in Gang setzen, ohne dass sie dafür einen eigenen MUA oder MTA benötigen. Berüchtigt sind die unzähligen Varianten des Formmail-Skripts, von denen viele es erlauben, E-Mails an beliebige Empfänger zu senden. Unsichere CGI-Skripte, mit deren Hilfe sich E-Mails an beliebige Empfänger senden lassen, spielen zwar heutzutage kaum noch eine Rolle im Vergleich zum enormen Volumen, das durch die anderen Verfahren auf den Weg kommt. Dennoch kann es für den Verantwortlichen der Webseite extrem unangenehm sein, wenn Spammer seinen Webserver missbrauchen. Schlimmstenfalls ist er binnen kurzer Zeit für Millionen von Spams mitverantwortlich.

### 4.2.5 Zombie-PCs und Botnetze

Die große Attraktivität offener Proxies hat im Verbund mit der Verwundbarkeit vieler PCs dazu geführt, dass Spammer sie inzwischen fast nach Belieben selbst installieren (lassen) [Fern04]. Meist sind offene Proxies daher mittlerweile wurm- oder trojanerbefallene PCs, von denen es weltweit mehrere 100.000 gibt<sup>6</sup> und von denen zu jedem Zeitpunkt eine mindestens fünfstellige Zahl online zur Verfügung steht, die sich ferngesteuert zum Mailversand missbrauchen lässt.

Für solche Rechner, die außerhalb der Kontrolle des eigentlichen Besitzers und ohne dessen Wissen agieren, hat sich der Begriff „Zombie-PC“ eingebürgert. Zombies werden in so genannten Botnetzen

---

<sup>5</sup> Wenn der Kunde nun sein System nicht richtig gesichert hat und ein offenes Relay betreibt, können Spam-Mails über den Mailserver des Kunden und von dort über die authentifizierte Verbindung zum ISP ins Internet gelangen. ISPs sollten auf die-sen Fall achten und eventuell selbst Relaytests bei ihren Kunden vornehmen.

<sup>6</sup> <http://www.spamhaus.org/news.lasso?article=158>

(*botnets*) zusammengefasst. Nach Schätzungen<sup>7</sup> werden zwischenzeitlich 70 bis 80 % des weltweiten Spam-Aufkommens über solche fremdgesteuerten Botnetze verschickt. Heutige Netzanschlüsse und PC-Hardware bieten derartige Leistungsreserven, dass eine gelegentliche „Mitnutzung“ durch einen Botnetz-Betreiber gar nicht auffällt. Die einzigen Mittel dagegen sind der regelmäßige Einsatz aktueller Antiviren-Programme und die laufende Aktualisierung der installierten Software.

Da offene Proxies anders als dedizierte Mailrelays nicht nur Verkehr auf dem SMTP-Port generieren können, sind sie geeignet, verteilte DoS-Angriffe gegen fast alle Internet-Anwendungen zu starten, etwa zum Zwecke der Erpressung gegen Webserver zahlungskräftiger Unternehmen [Brau04].

Der Hauptzweck der Botnetze scheint es aber derzeit zu sein, Spam über so viele IP-Adressen rasch in alle Welt zu verteilen, dass IP-Blacklists keinen ausreichenden Teil aller verwendeten Adressen auflisten können. Endanwender (oder Filterprogramme), die Received:-Header-Zeilen prüfen, können Spam aus Botnetzen daran erkennen, dass gleichartige E-Mails ihren Ursprung in Netzbereichen haben, die scheinbar gar nichts miteinander zu tun haben. Außerdem ist die auf Zombie-PCs installierte Spam-Software oft noch darauf angewiesen, E-Mails direkt zum Mailserver der Opfer zu senden. Das ist in den Received:-Zeilen häufig daran zu erkennen, dass der sendende „Mailserver“ (wenn er überhaupt einen rückwärts auflösbaren Namen hat) einen Begriff wie „adsl“, „dialup“ oder „cable“ oder seine eigene IP-Adresse als Namensbestandteil trägt – ein untrügliches Zeichen dafür, dass das Gegenüber nicht den üblichen Versandweg über eine dedizierte Mail-Infrastruktur nutzt.

Betreiber von MTAs können darüber hinaus erkennen, ob die mit der Mail-Zustellung einhergehenden DNS-Anfragen nach dem MX, dem im DNS eingetragenen Mail-EXchanger des Empfängers vom sendenden Rechner oder womöglich aus einem ganz anderen Netzbereich kommen. In Botnetzen sind die Aufgaben häufig klar getrennt, so kann ein *master* (in der Regel unter direkter Kontrolle des Spammers) die DNS-Formalitäten erledigen, während die *slaves*, also die Hintertür-verseuchten PCs, weltweit verteilt allein mit der Spam-Zustellung beschäftigt sind. Deren Mailsoftware ist (noch) recht primitiv.

### 4.2.6 Mailserver des Providers

In letzter Zeit immer häufiger zu beobachten ist, dass Spammer ihre E-Mails über die legitimen Mailserver von Providern absetzen. Von Zombie-PCs (siehe Kapitel 4.2.5) aus versenden sie den Spam nicht mehr direkt an den MX des Empfängers, sondern über den Provider des Anwenders, dessen Rechner sie missbrauchen.<sup>8</sup> Offenbar greifen die Spammer zu dieser neuen Methode, weil der direkte Versand nicht mehr gut genug funktioniert. Infolgedessen sind viele Filtermaßnahmen, etwa DNSBLs (siehe Kapitel 9.4), nicht mehr wirksam. Allerdings hat diese Methode des Spamversands den Vorteil, dass der Absenderprovider die E-Mail möglicherweise schon filtern kann, bevor der Spam sein Netz verlässt (*egress* oder *outbound filter*, siehe Kapitel 8.4.1).

## 4.3 Wie Spammer an die Mailadressen gelangen

Web und Newsgruppen sind die prominentesten Verbreitungswege für Mailadressen. Daher gehört es zu den am häufigsten zitierten Tipps zur Vermeidung von Spam, die eigene Adresse möglichst gar nicht zu veröffentlichen. Doch der Besitzer einer Mailadresse kann deren Verbreitung zwar verzögern, aber nicht verhindern und schon gar nicht steuern. Viele Anwender wissen aus leidvoller Erfahrung, dass auch „praktisch geheime“ Mailadressen in die Hände von Spammern geraten können

---

<sup>7</sup> Während die BBC von einem Anteil von 70 % ausgeht, vgl. [http://news.bbc.co.uk/1/hi/programmes/click\\_online/3618944.stm](http://news.bbc.co.uk/1/hi/programmes/click_online/3618944.stm), kommt eine Studie aus dem Sommer 2004 gar auf einem Anteil von 80 %, vgl. [http://www.theregister.co.uk/2004/06/04/trojan\\_spa\\_m\\_study/](http://www.theregister.co.uk/2004/06/04/trojan_spa_m_study/)

<sup>8</sup> The Spamhaus Project: Increasing Spam Threat from Proxy Hijackers, <http://www.spamhaus.org/news.lasso?article=156>

– zum Beispiel durch Erraten. Es kann daher vorkommen, dass Spam an Mailadressen geht, die noch nie zum Einsatz kamen.

### 4.3.1 Offline-Datensammlungen

Wer Internet-Anwender mit Spam beschicken will, benötigt eine große Zahl von Mailadressen. Am naheliegendsten ist der einfache Ankauf von Daten auf CDs, die natürlich auch per Spam beworben werden. Für weit unter einen Cent pro Adresse – typischerweise gehen CDs mit vielen Millionen Adressen für unter 100 US-Dollar in den Versand – erhalten Neu-Spammer die Daten von ihren Kollegen gegen Zahlung per Kreditkarte. Ein Massenmailer-Werkzeug<sup>9</sup> wird in der Regel mitgeliefert, damit sich die Opfer sogleich beschicken lassen [BaBH02].

Gekaufte Adress-CDs sind von zweifelhafter Herkunft und Aktualität und kommen daher für professionelle Spammer vielleicht als zu bewerbende Vertriebsobjekte in Frage, nicht aber als alleinige Grundlage für eigene Spam-Attacken.

### 4.3.2 Webseiten und Newsgruppen

Wesentlich mehr und aktuellere Adressen stehen online auf vielen verschiedenen Wegen zur Verfügung; letztlich sind auch die auf CD-ROMs erhältlichen Adressensammlungen lediglich Produkte der „Adress-Ernte“ (*harvesting*) im Web und im Usenet – dafür gibt es sogar kommerzielle „Erntewerkzeuge“ zum „Spammen für jedermann“.<sup>10</sup> Das Web ist voll von Mailadressen. Die meisten Homepages und Kontakt- oder Impressumseiten von Firmen und Privatpersonen enthalten sie. Dazu gibt es Archive unzähliger Mailinglisten und Newsgruppen voller Mailadressen und viele andere Quellen.

### 4.3.3 Raten und Durchprobieren

Um Mailadressen zu sammeln, bedienen sich Spammer auch so genannter Wörterbuchangriffe (*dictionary attacks*). Dabei generieren sie Listen möglicher Mailadressen mit Hilfe eines Wörterbuches (oder z. B. einer Liste von Vornamen), oder sie verwenden einfach jede mögliche Zeichenkombination (*brute force attack*). Diese Adressen präsentieren sie dann einem Mailserver und merken sich, welche funktioniert haben. Besonders Domains großer Firmen oder von Freemail-Providern, in denen es sehr viele Adressen gibt, sind anfällig für ein solches Vorgehen.

## Technische Maßnahmen gegen Wörterbuchangriffe

SMTP [RFC2821] sieht die Befehle VRFY und EXPN für die Prüfung von Mailadressen vor. In der Regel ist diese Funktion heutzutage deaktiviert, damit Spammer nicht mehr erfahren als nötig (siehe RFC 2821, Abschnitt 7.3). Trotzdem kann der Spammer einfach per RCPT TO versuchen, eine E-Mail abzusenden. Wenn es klappt, ist die Adresse entweder gültig oder der Server nimmt E-Mails für alle Adressen an und generiert später eine *bounce*, wenn sie nicht existieren.

Um *dictionary attacks* zu begegnen, kann man versuchen zu erkennen, dass besonders viele Anfragen für ungültige Adressen vom gleichen Client kommen, und dann die SMTP-Verbindung abbrechen oder verlangsamen. Natürlich könnte man auch alle E-Mails grundsätzlich annehmen, um dem Spammer nicht zu verraten, welche Mailadressen gültig sind. Damit würde man aber über das Ziel hinausschießen und durch die vielen *bounces* selbst zum Spammer werden (siehe Kapitel 3.2.7).

---

<sup>9</sup> z.B. Dark Mailer (<http://www.dark-mailer.com/>) oder Send-Safe (<http://www.send-safe.com/>)

<sup>10</sup> <http://www.bestextractor.com/>

Besonders erfolgreich sind *dictionary attacks*, wenn man E-Mail an alle Adressen in der eigenen Domain annimmt. In diesem Fall führt jeder Versuch zu einer gültigen Adresse (*catch all*). Früher war es üblich, solche Adressen zu verwenden, um E-Mails auch dann noch zu erhalten, wenn sich der Absender vertippt haben sollte; heute sieht man in aller Regel davon ab.

### 4.3.4 Externe Inhalte in HTML-Mails

Spammer müssen gar nicht selbst aktiv werden, um an aktuelle Adressdaten zu kommen oder ihren Datenbestand zu verifizieren: Mit Aus- und Eintragungs-Links und -Formularen auf von ihnen kontrollierten Webseiten sorgen sie dafür, dass E-Mail-Anwender von sich aus ihre Adressen preisgeben, etwa angelockt von einem Gewinnspiel oder Gutschein – oder auch vom Versprechen in einer Spam-Mail, dass sich durch eine Eintragung der Adresse in einem Opt-Out-Formular künftig Spam vermeiden lässt.

Durch die Integration von Mailclients mit Web-Browsern gibt es darüber hinaus mehrere Möglichkeiten, über entsprechend präparierte Webseiten an Mailadressen der Anwender zu gelangen oder sich die Existenz der Adressen bestätigen zu lassen. Eine verbreitete Methode ist der Versand von HTML-Mails, die externe Inhalte wie Bilder oder Stylesheets (oder auch kleine, nicht sichtbare Grafikelemente, so genannte Web-Bugs) referenzieren: Die E-Mail enthält eine ganz normale Webseite, die der Mailclient ohne weiteres Zutun des Anwenders öffnet. Da der in den Mailclient integrierte Browser Inhalte von einem im Spammer-Umfeld betriebenen Webserver lädt, hinterlässt der Client dort verräterische Spuren – sogar eventuelle E-Mail-Weiterleitungen lassen sich auf diese Weise von außen feststellen.

Darüber hinaus ist es üblich, dass anonyme FTP-Sitzungen mit der Übertragung der Mailadresse als FTP-Passwort beginnen. FTP gehört zum gängigen Funktionsumfang heutiger Web-Browser, auch wenn es wenige Anwender benötigen. Da Webbrowser FTP-Sitzungen auf genauso einfache Weise initiieren können wie das Laden von Webseiten, kann der Anwender bereits durch einfaches Laden präparierter Seiten seine Mailadresse preisgeben, ohne es zu merken.

### 4.3.5 Automatische Antworten

E-Mails – insbesondere automatisch generierte Urlaubsantworten (*autoreply*) – der Opfer an die Spammer enthalten oft wertvolle Informationen, und nicht alle Absenderadressen von Spams sind gefälscht. Besonders die E-Mails der „Nigeria-Connection“ gehen häufig von gültigen Freemailer-Adressen aus. Mittels automatischer Antwort können Kriminelle an Telefonnummern, Abwesenheitszeiten und weitere persönliche Daten gelangen – die Einrichtung einer automatischen Antwort (*autoresponder*) will daher gut überlegt sein.

### 4.3.6 Whois-Datenbanken

Jeder Inhaber oder Administrator einer Domain ist in einer so genannten Whois-Datenbank eingetragen, die von den Domain-Vergabestellen gepflegt werden. Diese Datenbanken sind öffentlich und enthalten auch die Mailadressen der Ansprechpartner. Ähnliches gilt für die Datenbanken zur Zuteilung von IP-Adressräumen. Zwar erlauben es deren Nutzungsbedingungen nicht, die Daten massenweise auszulesen, was aber noch keinen Spammer davon abgehalten hat, genau das zu tun.

### 4.3.7 Lokal gespeicherte Adressen

Die Allianz zwischen Spammern und Hackern hat neben der Tatsache, dass ein Großteil der Spams heute von Rechnern Unschuldiger ausgeht, den Effekt, dass Spammer Zugriff auf den Inhalt der Adressbücher missbrauchter Rechner erlangen können. Diese Adressen sind hoch relevant, da der

Benutzer sie ja auf dem aktuellen Stand hält. Und nicht nur Adressbücher, sondern auch andere Datenbereiche lokaler Festplatten können aus Sicht der Spammer interessante Daten enthalten. Der Browser-Cache etwa kann nicht nur Mailadressen der vom Anwender besuchten Webseiten preisgeben, sondern auch Zugangsinformationen der letzten Homebanking-Sitzung.

## 5 Kosten von Spam und Antispam-Maßnahmen

Dieses Kapitel gibt einen Überblick über die durch Spam verursachten und die durch Antispam-Maßnahmen entstehenden Kosten. Die Berechnungen beruhen auf Schätzungen und Erfahrungswerten, alle Zahlenangaben sind als Circa-Angaben zu verstehen. Sie sind sicher nicht für jeden Fall zutreffend und sind nur als Grundlage für eigene Berechnungen und Überlegungen aufgeführt.

### 5.1 Durch Spam verursachte Kosten

**Unmittelbare Kosten** werden durch Traffic, die Nutzung der Mailserver- und Storage-Infrastruktur sowie das zusätzliche Personal für die Bearbeitung von Missbrauchsfällen (Abuse-Management) und die Administration verursacht.

Die **mittelbaren Kosten** setzen sich zusammen aus dem Produktivitätsverlust der Mailempfänger aufgrund der Zeitverschwendung durch den Umgang mit Spam, den Kosten durch die eingeschränkte oder nicht vorhandene Erreichbarkeit und Verfügbarkeit und den Kosten für die Reparatur beschädigter oder überlasteter Systeme.

Hinzu kommen **sonstige Kosten**. Dazu gehören Verluste durch Imageschaden, z. B. wegen des unwissentlichen eigenen Versands von Spam und Viren aufgrund einer Virenverseuchung, und die Kosten für Werbung und Marketing, um den Imageschaden wieder auszugleichen. Ebenfalls dazu gehören die Kosten, die durch den Wettbewerbsdruck entstehen.

### 5.2 Kosten von Antispam-Maßnahmen

Die **unmittelbaren Kosten** der Spamschutzmaßnahmen ergeben sich aus der zusätzlich benötigten Hardware zum Betrieb sowie eventuell aus der Lizenzierung von Antispam-Produkten. Im Fall der Eigenleistung fallen Entwicklungskosten an. Zusätzliche Personalkosten entstehen durch die Notwendigkeit zur Administration der Spamfilter, den Support und das Abuse-Management.

Die Schulung der Mitarbeiter im Umgang mit der Spamschutztechnik, der Bearbeitungsaufwand zur Fehlerkorrektur der falsch bewerteten E-Mails auf Seiten der Mitarbeiter oder der Systemadministration und die Verdienstauffälle durch eine etwaige falsche Filterung wichtiger E-Mails bilden die **mittelbaren Kosten** des Spamschutzes.

**Sonstige Kosten** entstehen im Umfeld des Spamschutzes nur bei Anbietern von Mailedienstleistungen, die den Spamschutz in das Marketingportfolio aufnehmen, durch Marketing und Öffentlichkeitsarbeit in Bezug auf den Spamschutz und das Produktmanagement.

Ausgaben für den Spamschutz können die durch Spam entstehenden Kosten verringern, aber nicht vollständig vermeiden.

### 5.3 Fallbeispiele

Die Höhe der durch Spam verursachten Kosten und der Umfang der Maßnahmen gegen Spam hängen stark vom Einsatzbereich ab. Zur Veranschaulichung ist die Kostenbetrachtung hier beispielhaft für fünf typische Umgebungen gezeigt, wobei die Darstellung notwendigerweise stark vereinfachend ist. Der Leser sollte die Beispiele auf seine Organisation übertragen und, soweit bekannt, Zahlen aus dem eigenen Betrieb einsetzen.

Um die Fälle vergleichbar zu gestalten, sind in den folgenden Beispielen jeweils die gleichen Voraussetzungen zugrunde gelegt. Der durchschnittliche Spamanteil im Normalfall fließt mit ca. 65 % des Mailaufkommens ein, während dieser Anteil im Fall einer akuten Spamwelle ca. 85 % beträgt.

Für die durchschnittliche Größe einer Spam-Mail werden hier 25 KByte<sup>11</sup> als Berechnungsgrundlage verwendet.

Für die fünf beispielhaften Umgebungen sind folgende Werte angenommen:

|  | <b>Groß-provider</b> | <b>Provider</b> | <b>Großunter-nehmen</b> | <b>Mittelständi-sches Unter-nehmen</b> | <b>Kleinunter-nehmen/<br/>Einzelunter-nehmer</b> |
|--|----------------------|-----------------|-------------------------|--|--|
| <b>Anzahl aktive Postfächer</b>                            | 3 Mio.               | 50.000          | 5.000                   | 500                                    | 5  |
| <b>Anzahl Spam-Mails pro Tag im Normalfall<sup>2</sup></b> | 15 Mio.              | 250.000         | 25.000                  | 2.500                                  | 25   |
| <b>IT- Umgebung</b>  | –                    | –               | eigene IT-Abteilung     | keine IT-Abteilung                     | keine IT-erfahrenen Mitarbeiter                  |

Tabelle 5.1: Beschreibung der Fallbeispiele

### 5.3.1 Beispiel Großprovider

Das Anbieten von Spamschutzmaßnahmen ist für den Großprovider nicht nur eine reine Kostenfrage. Allein der Wettbewerb verpflichtet ihn, in diesem Bereich aktiv zu sein. Daher spielen gerade in diesem Beispiel die unmittelbaren und die sonstigen Kosten eine wichtige Rolle. Große Provider werden in der Regel mehrstufige, serverbasierte Filtersysteme einsetzen, um den verschiedenen Merkmalen von Spam Rechnung zu tragen und die Performance zu optimieren. Da die Filtersysteme stark an die Eigenheiten der jeweiligen Provider-Infrastruktur angepasst sein müssen, werden Eigenentwicklungen oder stark angepasste Lizenzprodukte verwendet.

#### Durch Spam verursachte Kosten

Unmittelbare Kosten treten in den verschiedenen Bereichen der Infrastruktur auf. Der zusätzliche Traffic beläuft sich auf 128 TByte<sup>3</sup> pro Jahr, die Anbindung muss eine doppelte Bandbreite aufweisen. Allein der Spam benötigt während eines Peaks 150 MBit/s<sup>4</sup>. Bei einer mittleren Verweildauer der Spam-Mails in der Mailbox bis zur Löschung durch den Nutzer von acht Tagen entsteht zusätzlicher Speicherbedarf von drei TByte<sup>5</sup>. Die Mailer-Infrastruktur muss ebenfalls die doppelte Kapazität bieten. Da ein Großprovider selten blockt, sondern die Spam-Mails markiert

<sup>1</sup> Eine typische Spam-Mail ist kleiner als 10 KByte. Wenn man aber Viren, Würmer, bounces und den SMTP- und TCP/IP-Over-head mit einbezieht, also den Traffic betrachtet, der letztendlich auf der Leitung entsteht, dann ergibt das einen Erfahrungswert von 25 KByte im Durchschnitt.

<sup>2</sup> Der Wert von 5 Spams pro Account und Tag ist ein Durchschnitt. Es gibt bei einzelnen Postfächern extreme Abweichungen davon. So gibt es Postfächer ohne Spam und solche mit Hunderten von Spams pro Tag.

<sup>3</sup> 15 Mio. Spam- & Viren-Mails x 365 Tage x 25 KByte durchschnittl. Größe entspricht 127,475 TByte (gerechnet wurde mit 1 KByte = 1024 Bytes)

<sup>4</sup> Eingang von 500 bis 1.000 Spam- & Viren-Mails pro Sekunde mit einer Durchschnittsgröße von 25 KByte

<sup>5</sup> 15 Mio. Spam- & Viren-Mails x 8 Tage x 25 KByte durchschnittliche Größe

zustellt, bleiben diese Kosten auch mit geeigneten Spamschutzmaßnahmen zumindest zu 75 %<sup>6</sup> erhalten. Dieses Paket verursacht jährliche Abschreibungskosten in einer Höhe von 300.000 €<sup>7</sup>.

Der Kostenblock der mittelbaren Kosten ist bei einem großen Provider vergleichsweise gering, da diese Kosten auf der Seite des Kunden entstehen.

Sonstige Kosten durch Imageverlust bzw. die Gegenmaßnahmen in Form von Werbung und Marketing sind nicht zu beziffern. Tatsächlich würde der Verzicht auf Sicherungsmaßnahmen für den Provider ungeheure direkte und indirekte Verdienstaussfälle bedeuten, da seine Kundenbasis nicht zu halten wäre. Daher ist es nicht möglich, die Gesamtsumme der durch Spam verursachten Kosten für den Großprovider konkret zu beziffern. Es ist jedoch sicher, dass diese Summe die Gesamtsumme der Kosten mit etablierten Spamschutzmaßnahmen übersteigen würde.

### Kosten von Antispam-Maßnahmen

Als unmittelbare Kosten entstehen Personalkosten durch die Summe der Mitarbeiter im Bereich Forschung und Entwicklung, Systemadministration, Support, Abuse-Management, Marketing und dedizierte Stellen im Bereich Spamschutz. Hier kann ein Wert von 50.000 € pro Monat angesetzt werden. Je nach Strategie und Ausrichtung hin zur Eigenleistung und -entwicklung oder Softwarelizenzierung können weiter rund 30.000 € pro Monat an Softwarekosten kalkuliert werden. Im Falle der Fokussierung auf die Eigenleistung oder -entwicklung fällt dieser Betrag in Form von zusätzlichen Personalkosten an. In diesem Beispiel kann erfahrungsgemäß eine Infrastruktur von ca. zehn PC-basierten Servern rein als Träger für die Spam- und Virenschutzmaßnahmen gerechnet werden und zusätzlich eine Verdoppelung der Mailserverinfrastruktur, des Storagevolumens und der Leitungskapazität. Somit entstehen jährliche Abschreibungskosten für die Hardware in Höhe von 260.000 € Daraus resultieren jährliche Kosten durch den Spamschutz von 1,22 Mio. €<sup>8</sup>.

Auch bei den Schutzmaßnahmen sind die mittelbaren Kosten bei einem Provider vergleichsweise gering, da die Ausgaben für eine Fehlerkorrektur und etwaige Verdienstaussfälle auf Seiten des Kunden entstehen. Umso wichtiger ist hier eine rechtliche Absicherung gegen eventuelle Schadensersatzforderungen des Kunden. Auch bei umfassender und sorgfältiger Planung wird es vereinzelt zu rechtlichen Auseinandersetzungen mit Kunden kommen; ferner kann sich der Provider gezwungen sehen, selbst auf dem Rechtswege gegen Spammer vorzugehen. Die Kosten für Rechtsberatung und Rechtsbeistand sind stark vom Einzelfall abhängig, sollen hier aber pauschal mit 60.000 € pro Jahr angenommen werden.

Auch die sonstigen Kosten sind nur schwer pauschal zu beziffern. Presse- und Marketingaktivitäten sind natürlich Kostenträger und spielen im Umfeld des großen Providers zur Abgrenzung gegen den Wettbewerb eine erhebliche Rolle. Im Beispiel sollen (Mehr-)Kosten von 150.000 € pro Jahr durch mit der Spam-Bekämpfung zusammenhängende Maßnahmen angenommen werden.

Das ergibt eine gemittelte Belastung von 1,43 Mio. € pro Jahr oder **0,026 Cent** pro Spam-Mail.

### 5.3.2 Beispiel Provider

Auch kleinere Provider fühlen inzwischen den Wettbewerb, der den Einsatz von Schutzmaßnahmen notwendig erscheinen lässt. Der Hauptunterschied zum großen Provider ist der Skalierungsgrad. Je nach Größe, Infrastruktur und Kundenstruktur des Providers befinden sich auch hier vornehmlich Eigenentwicklungen, angepasste Open-Source-Lösungen und angepasste Lizenzprodukte im Einsatz.

---

<sup>6</sup> 75 % der E-Mails werden weitergeleitet und 25 % geblockt, weil es sich z. B. um eindeutige Wurm-Mails handelt.

<sup>7</sup> Kostenschätzung für Netztraffic, Storage, Mailserver, Datenbanken, Backup, usw. inkl. RZ-Infrastruktur unter Berücksichtigung der Abschreibung.

<sup>8</sup>  $50.000 \text{ €} \times 12 \text{ Monate (Personal)} + 30.000 \text{ €} \times 12 \text{ Monate (Software)} + 260.000 \text{ € (Hardware-Abschreibung)}$

<sup>9</sup>  $50.000 \text{ €} \times 12 \text{ Monate (Personal)} + 30.000 \text{ €} \times 12 \text{ Monate (Software)} + 260.000 \text{ € (Hardware-Abschreibung)} + 60.000 \text{ € (Rechtsberatung)} + 150.000 \text{ € (PR)}$

Zusätzlich tritt der Provider oft als Wiederverkäufer oder Full-Service-Provider für Fertiglösungen zum Einsatz in der Infrastruktur seines Kunden auf. Da dieser Aspekt nicht direkt in die Kostenbetrachtung zu Spam eingeht, ist er in dem folgenden Beispiel vernachlässigt.

### Durch Spam verursachte Kosten

Die unmittelbaren und mittelbaren Kosten des Providers setzen sich aus den gleichen Kostenbestandteilen wie beim Großprovider zusammen. Die Anforderungen an Redundanz und Sicherheit der Infrastruktur sind ebenfalls gleich. Daher können die Kosten zum Teil proportional skaliert werden. Ausnahmen bilden der Personalaufwand und die Storage-Infrastruktur, da bei dieser Größenordnung des Speicherplatzbedarfs erheblich günstigere Lösungen angewendet werden können. Im Beispiel belaufen sich die unmittelbaren Kosten auf 5.000 € pro Monat für Personal, und jährlich 30.000 € für Hardware/Software und zusätzlich jährlich 40.000 € für Leitung und Traffic. Auch hier bewirkt der Spam zumindest eine Verdoppelung der Kosten im Bereich des Mailsystems.

Analog zum großen Provider entstehen die mittelbaren Kosten auf der Seite der Kunden.

Die Bezifferung der sonstigen Kosten ist für den Fall des Providers, aus den gleichen Gründen wie im Fall des Großproviders, nicht möglich. Auch für den Provider kann allerdings vorausgesetzt werden, dass ein Fehlen von Spamschutzmaßnahmen mittelfristig zu einem Imageverlust und Verdienstausschlag führt, dessen Höhe die zusätzlichen Kosten durch Antispam-Maßnahmen übersteigt.

### Kosten von Antispam-Maßnahmen

Ein Provider muss seinen Kunden unabhängig von seiner Größe immer den gleichen Service in der gleichen Qualität bieten. Bei kleineren Providern ist die Möglichkeit der Bandbreiten- und Storage-Ersparnis wegen des unterschiedlichen Kundenprofils noch geringer als bei den großen. Die durch Spam verursachten Kosten werden demnach auch bei dem Einsatz von Spamschutzmaßnahmen nahezu komplett übernommen. Die Kosten durch zusätzliche Hardware dahingegen sind weniger hoch, da die vorhandene Hardware für den Einsatz der Schutzmaßnahmen mitgenutzt werden kann. Das führt im Ergebnis zu einer leichten Verringerung der Kosten für Hardware und Traffic und einer deutlichen Steigerung der Personalkosten. Die unmittelbaren Kosten betragen für Personal 10.000 € pro Monat, für Hardware/Software zusätzlich 25.000 € jährliche Abschreibungskosten, sowie Leitung und Traffic 35.000 € pro Jahr.

Mittelbare Kosten entstehen bei den Kunden.

Die sonstigen Kosten sind mit 10.000 € pro Jahr angesetzt.

Das ergibt eine gemittelte Belastung von 190.000 €<sup>10</sup> pro Jahr oder **0,2 Cent** pro Spam-Mail – im Vergleich mit einem größeren Provider also eine wesentlich stärkere Belastung.

### 5.3.3 Beispiel Großunternehmen

Ganz anders stellt sich die Situation in einem Unternehmen dar. Die Verteilung der Kosten verschiebt sich stark innerhalb der Kostengruppen. In der Regel verfügt das Mailsystem eines Unternehmens über genügend Ressourcen, um die Mehrbelastung durch Spam und Viren ohne Erweiterung verarbeiten zu können. Ein Unternehmen dieser Größenordnung mit eigener IT-Abteilung wird eine zentrale kommerzielle Lösung am Mailserver einsetzen, die den Spam- und Virenschutz gewährleistet. Somit bleiben bei den unmittelbaren Kosten nur die Lizenz- und Personalkosten. Auch die sonstigen Kosten sind hier gänzlich zu vernachlässigen. Die mittelbaren Kosten dahingegen fallen in Unternehmen viel deutlicher ins Gewicht.

<sup>10</sup> 10.000 € x 12 Monate (Personal) + 35.000 € (Leitung & Traffic) + 10.000 € (sonstige Kosten) + 25.000 € (Hardware-Abschreibung)

### Durch Spam verursachte Kosten

Unmittelbare Kosten begründen sich in der Umgebung des Unternehmens nur aus dem gesteigerten Traffic. Sie belaufen sich in diesem Beispiel auf 1.300 €<sup>11</sup> pro Jahr. Die mittelbaren Kosten des Produktivitätsausfalls belaufen sich in diesem Beispiel auf 1,6 Mio. €<sup>12</sup> pro Jahr bei einem Personentagesatz von 500 € und einer Arbeitsverzögerung von im Durchschnitt 10 Sekunden pro Spam-Mail durch manuelle Sortierung oder Ablenkung von der Arbeit. In diesem ungeschützten Umfeld ist mit einem häufigen Virenbefall zu rechnen, zu dessen Beseitigung auch Kosten entstehen. Daneben entstünden sicher auch sonstige Kosten durch Imageschaden und rechtliche Auseinandersetzungen. Diese Kosten werden in diesem Beispiel in einer Höhe von 100.000 € berücksichtigt.

Die durch Spam verursachten Kosten, ohne Schutzmaßnahmen, belaufen sich in Summe auf 1,7 Mio. €<sup>13</sup> pro Jahr, das entspricht **18 Cent** pro Spam-Mail.

### Kosten von Antispam-Maßnahmen

Eine Antispam-Software kann für ca. 10 bis 20 € pro Nutzer lizenziert werden. Für eine 5.000-Nutzer-Lizenz entstehen damit Kosten von durchschnittlich 75.000 € pro Jahr. Sonstige Hardwarekosten für die benötigte Infrastruktur belaufen sich auf 10.000 € pro Jahr. Die Personalkosten zur Administration des Systems betragen zusätzlich 150.000 € pro Jahr. Dadurch wird der Produktivitätsausfall um sicher 95 % verringert, wenn der realistische Wert einer Trefferquote von 95 % des Spamfilters vorausgesetzt wird.

Danach ist der Summe der Kosten, mit Schutzmaßnahmen, 320.000 €<sup>14</sup> pro Jahr und entspricht einem Betrag von **4 Cent** pro Spam-Mail.

## 5.3.4 Beispiel mittelständisches Unternehmen

Die Kostenverteilung ist bei einem Unternehmen dieser Größenordnung die gleiche wie im vorigen Beispiel. Nicht selten jedoch werden solche Unternehmen die Fixkosten von Administratoren in Festanstellung scheuen und eher auf freie Mitarbeiter oder externe Dienstleister zurückgreifen, die das IT-System betreuen. Kleinere IT-bezogene Arbeiten werden in der Regel von Mitarbeitern mit mehr oder weniger IT-Erfahrung erledigt.

### Durch Spam verursachte Kosten

Die unmittelbaren und mittelbaren Kosten entsprechen proportional skaliert denen eines größeren Unternehmens. Allein die Beauftragung eines externen Dienstleisters zur Administration und Reparatur der Infrastruktur kann eine leichte Erhöhung dieser Kosten bewirken. Wegen der geringen Auswirkung auf die Gesamtsumme braucht das hier allerdings nicht berücksichtigt zu werden.

In diesem Beispiel entstehen ohne Schutzmaßnahmen Gesamtkosten in Höhe von 170.000 €<sup>15</sup> pro Jahr, das entspricht ebenfalls **18 Cent** pro Spam-Mail.

### Kosten von Antispam-Maßnahmen

Auch diese Kosten lassen sich übertragen. Hier muss jedoch für die Einrichtung, Pflege und Wartung des Mailsystems und der Spamschutzmaßnahmen mit höheren Kosten gerechnet werden, da diese Leistungen durch einen externen Dienstleister erbracht werden.

---

<sup>11</sup> 25.000 Spam- und Viren-Mails x 365 Tage x 25 KByte durchschnittl. Größe x 6€ pro GByte

<sup>12</sup> ((25.000 Spam- und Viren-Mails x 365 Tage x 10 Sek.) / (8 Std. x 60 Min. x 60 Sek.)) x 500 €

<sup>13</sup> 1,6 Mio € + 100.000 €

<sup>14</sup> 75.000 € + 10.000 € + 150.000 € + 5% von 1,7 Mio

<sup>15</sup> Skaliert vom Beispiel der Großunternehmen

Die Lizenzgebühren betragen 10.000 € pro Jahr. Die Schulungs- und Supportkosten sind mit 15.000 € pro Jahr berechnet. Der Wartungs- und Pflegeaufwand beläuft sich (bei mindestens 50 Personentagen) auf 25.000 € pro Jahr.

Somit ist die Summe der Kosten, mit Schutzmaßnahmen, 59.000 €<sup>16</sup> pro Jahr und entspricht einem Betrag von **6 Cent** pro Spam-Mail.

### 5.3.5 Beispiel Einzelunternehmer/Kleinunternehmen

Kleine Unternehmen wie in diesem Beispiel sind vom Mail-Verhalten und der eingesetzten Technik mit privaten Endanwendern vergleichbar. Meist besteht keine eigene Mail-Infrastruktur und kein dauerhafter Zugang zum Internet. Hier ist demnach das gesamte beeinflussbare System im Client angesiedelt.

#### Durch Spam verursachte Kosten

Die unmittelbaren Kosten entstehen typischerweise aus verlängerten Downloadzeiten der E-Mails und erhöhtem Traffic. Mittelbar entstehen Kosten durch den Zeitaufwand zur Sortierung und Verarbeitung der E-Mails. Sonstige Kosten können durch einen Virusbefall der Rechner und zusätzlich durch eine daraus folgende Nutzung des Rechners als Spamplattform entstehen. Im Beispiel kann der zusätzliche Download von 750 E-Mails pro Monat und der daraus folgende zusätzliche Traffic von 18 MByte vernachlässigt werden. Am stärksten wirkt sich der Produktivitätsausfall aus. Wenn die manuelle Bearbeitung bzw. die Ablenkung pro Spam-Mail durchschnittlich 10 Sekunden kostet, summiert sich das in diesem Beispiel zu einem Produktivitätsverlust von zwei Stunden pro Monat. Ein Virenbefall kann zur Desinfektion im Einzelfall auch einen halben bis ganzen Personentag kosten und passiert, ohne Schutzmaßnahmen, sicher einmal pro Monat. Der Gesamtaufwand beläuft sich demnach auf ca. einen Personentag.

Bei einem Personentagesatz von 500 € entspricht das **66 Cent** pro Spam-Mail.

Damit ist die relative Höhe der Kosten für Endanwender ohne Schutzmaßnahmen die höchste.

#### Kosten von Antispam-Maßnahmen

In dieser Umgebung sind die Kosten für die Schutzmaßnahmen sehr überschaubar. Der Großteil der Provider bietet zu den Mailaccounts einen kostenlosen serverbasierten Spamschutz an. Dieser Spamschutz ist grundsätzlich sehr wirksam und unterscheidet sich vor allem im Funktionsumfang und der Konfigurierbarkeit. Daher kann es unter Umständen notwendig sein, weitere lokale Spamschutzmaßnahmen zu ergreifen. Hier reicht die Palette von kommerziellen Produkten zu einem Lizenzpreis von z. B. 25 € pro Jahr und Client über Programme zu einem einmaligen Preis von 20 € pro Client bis hin zu kostenlosen Filtern in den jeweiligen Mailclients.<sup>17</sup>

Diese Schutzmaßnahmen können die Belastung nahezu komplett beseitigen und damit den Produktivitätsverlust um sicher 95 % verringern. Die Gesamtkosten betragen 325 €<sup>18</sup> pro Jahr, das entspricht einem Betrag von **4 Cent** pro Spam-Mail.

<sup>16</sup> 10.000 € + 15.000 € + 25.000 € + 5% von 170.000

<sup>17</sup> Außerdem sollte ebenfalls pro Client ein Virens Scanner mit Firewall installiert sein, der mit 45 € jährlich zu berücksichtigen ist.

<sup>18</sup> 5% von (500 € (Arbeitszeit) x 12 Monate) + 25 € Lizenzkosten

### 5.3.6 Zusammenfassung

|  | Groß-provider   | Provider        | Großunter-nehmen | Mittel-ständisches Unternehmen | Kleinunter-nehmen / Einzelunter-nehmer |
|--|-----------------|-----------------|------------------|--------------------------------|--|
| Unmittelbare Kosten p. a.                    | 1 Mio. €        | 120.000 €       | 150.000 €        | 35.000 €                       | 25 €                                   |
| Mittelbare Kosten p. a.                      | 60.000 €        | –               | 85.000 €         | 15.000 €                       | –                                      |
| Sonstige Kosten p. a.                        | 150.000 €       | 10.000 €        | –                | –                              | –                                      |
| <b>Kosten durch Spam<sup>19</sup></b>        | 225.000 €       | 60.000 €        | 85.000 €         | 9.000 €                        | 300 €                                  |
| <b>p. a.</b>                                 |                 |                 |                  |                                |  |
| Gesamtkosten p. a.                           | 1,43 Mio. €     | 190.000 €       | 320.000 €        | 59.000 €                       | 325 €                                  |
| Kosten pro Spam-Mail                         | 0,026 Cent      | 0,2 Cent        | 4 Cent           | 6 Cent                         | 4 Cent                                 |
| Kosten pro Spam-Mail ohne Antispam-Maßnahmen | – <sup>20</sup> | – <sup>20</sup> | 18 Cent          | 18 Cent                        | 66 Cent                                |

Tabelle 5.2: Kosten von Spamschutzmaßnahmen für die Fallbeispiele

Es ist deutlich zu sehen, dass Spam- und Viren-Mails eine hohe finanzielle Belastung für die betroffenen Teilnehmer am Mailverkehr darstellen. Im Extremfall können die Kosten des Mailsystems seinen Nutzen übersteigen und das Medium insgesamt für ein Unternehmen unattraktiv machen. Der deutliche Unterschied bei den auf die einzelne Spam-Mail umgelegten Kosten zeigt, dass die Hauptlast bei den kommerziellen Nutzern des Mediums, also den Unternehmen, entsteht. Die absoluten Kosten sind jedoch wegen der Massen an Spam auch bei den Providern sehr hoch und stellen durchaus eine relevante wirtschaftliche Last dar. Allein der Einzelanwender und Privatnutzer hat heute schon die Möglichkeit, sich ohne hohe Kosten vor Spam zu schützen.

## 5.4 Einkauf oder Eigenleistung?

Bei allen Spamschutzmaßnahmen hat man heute die Wahl zwischen dem Kauf einer fertigen Software und dem Einsatz einer Eigenentwicklung oder der Nutzung von Open Source-Software. Neben den Anschaffungskosten sind die Wartungskosten bzw. die Kosten für einen Service- und Supportvertrag zu berücksichtigen.

Die entscheidende Fragestellung ist dabei nicht „Open Source oder kommerzielle Software?“, sondern „Einkauf oder Eigenleistung?“. Die richtige Entscheidung kann z. B. anhand der Verfügbarkeit von qualifizierten Mitarbeitern im Unternehmen, der Größenordnung des Systems, dem angestrebten SLA (Service Level Agreement) und vorherigen Erfahrungen mit IT-Produkten getroffen werden.

Am Markt ist heute eine große Bandbreite von Antispam-Produkten zu haben. Darunter finden sich fertig konfigurierte Blackbox-Lösungen, die man vor einen bestehenden Mailserver setzen kann, ebenso wie Softwarelösungen, die auf bestehenden Mailservern installiert werden. Häufig werden

<sup>19</sup> Verbleibenden Kosten durch Spam, nach der Einführung von Spamschutzmaßnahmen

<sup>20</sup> Da die Gesamtsumme der Kosten ohne Spamschutzmaßnahmen nicht gebildet werden kann, ist es nicht möglich diesen Wert zu beziffern. Die Kosten würden jedoch, genau wie in den anderen Fallbeispielen, mittelfristig die Kosten mit Spamschutz übersteigen.

<sup>20</sup> Da die Gesamtsumme der Kosten ohne Spamschutzmaßnahmen nicht gebildet werden kann, ist es nicht möglich diesen Wert zu beziffern. Die Kosten würden jedoch, genau wie in den anderen Fallbeispielen, mittelfristig die Kosten mit Spamschutz übersteigen.

diese Produkte auch in Kombination mit klassischer Mailsoftware, Virenschutzlösungen oder Firewalls angeboten. Typische Blackbox- oder softwarebasierte Komplettlösungen sind zu Preisen von 5.000 € bis 10.000 € pro 500-Nutzer-Lizenz pro Jahr erhältlich. Im Normalfall ist der Service und Support in diesen Preisen inbegriffen.

Der Administrationsaufwand bei Produkten mit Servicevertrag ist in der Regel nicht sehr hoch und durch die gegebenen Update- und Supportmöglichkeiten wenig zeitaufwendig. Ein 500-Nutzer-System kann mit maximal einer halben, wenig qualifizierten Stelle betreut werden.

Eigenentwicklungen bewirken andere Kostenfaktoren. Die Installation und Integration in das bestehende System erfordert einen viel höheren Kenntnisstand des Administrators, ist zeitaufwendiger und häufig komplizierter. Updates, Wartung und Support werden in der Regel durch einen angestellten Administrator erledigt. Dabei entstehen höhere Personalkosten. Zur Einrichtung und dauernden Betreuung und Optimierung eines 500-Nutzer-Systems ist mindestens eine halbe hoch qualifizierte Stelle zu rechnen. Unter Umständen ist auch eine Vollzeitstelle notwendig.

## 6 Rechtliche Aspekte von Spam

Die Problematik der unerwünschten Werbung per E-Mail ist auch für Juristen nicht neu. Das erste veröffentlichte Urteil zu diesem Thema stammt bereits vom Dezember 1997.<sup>1</sup> Seit dieser Zeit hat sich eine weitgehend einheitliche Rechtsprechung entwickelt, die ein Urteil des Bundesgerichtshofs inzwischen bestätigt hat. Mitte 2004 schließlich wurde das Verbot von Werbemail im Rahmen des Wettbewerbsrechts nach einer Vorgabe der EU auch gesetzlich normiert.

Auf Basis dieser Rechtslage ergeben sich aussichtsreiche Möglichkeiten, gegen Spam zumindest innerhalb von Deutschland und der EU auch ergänzend auf juristischer Ebene vorzugehen. Rechtliche Mittel können aber nur ein Teilaspekt der Bewältigung dieses internationalen Problems sein und scheitern häufig an den Grenzen der einzelnen Staaten, die Versender der Werbemails dagegen problemlos überwinden können.

Dieses Kapitel behandelt die allgemeinen rechtlichen Aspekte von Spam. Wenn sich zu einzelnen Antispam-Maßnahmen besondere rechtliche Gesichtspunkte ergeben, sind sie in den Kapiteln 8 oder 9 erwähnt.

### 6.1 Rechtslage

#### 6.1.1 Spam im juristischen Sinn

Die rechtliche Definition von unerwünschter E-Mail-Werbung unterscheidet sich von der von Seiten der Technik verwendeten Begrifflichkeit, was zwischen beiden Gruppen regelmäßig für Konflikte sorgt.

Umgangssprachlich bezeichnet „Spam“ jegliche Art von unverlangt zugesandten Nachrichten. Rechtlich verboten sind – mit wenigen, später behandelten Ausnahmen – nur die Zusendung von Nachrichten mit werbendem, also kommerziellen Inhalt. Daher sind diese in einem rechtlichen Kontext scharf von solchen Nachrichten ohne kommerziellem Inhalt, wie etwa Viren-Mails, karitative Inhalte oder *bounces* aufgrund von nicht zustellbaren Nachrichten zu trennen. Der Grund für diese Trennung liegt darin, dass aus rechtlicher Sicht nicht die massenhafte Versendung von E-Mails als solche, sondern lediglich der Missbrauch dieser Technik für Werbezwecke auf Kosten der Empfänger unterbunden werden soll.

#### **Juristische Definition von „Spam“**

- Werbender Inhalt mit kommerziellem Hintergrund Nichtkommerzielle E-Mails für karitative Zwecke sind in der Regel zulässig
- Unverlangte Zusendung Keine vorherige Anforderung von Informationen durch den Empfänger
- Kein bereits bestehender geschäftlicher Kontakt zwischen Versender und Empfänger

Spam im juristischen Sinne sind also nicht solche E-Mails, bei denen bereits ein geschäftlicher Kontakt zu dem Versender besteht oder solche Fälle, bei denen der Empfänger sich ausdrücklich oder konkludent, also durch schlüssiges Verhalten, mit dem Empfang von Werbenachrichten einverstanden erklärt hat. Dabei reicht es bereits aus, wenn der Benutzer einer Mailadresse gegenüber dem Versender diese an irgendeiner Stelle angegeben hat. Dagegen stellt die Angabe der eigenen Adresse auf der eigenen Website oder in Web-Verzeichnissen keinen „Freibrief“ für die Zusendung von elektronischer Werbung dar.

---

<sup>1</sup> LG Traunstein, MMR 1998, 53

Wichtigster Fall für zulässiges Online-Marketing, häufig auch als *permission marketing* bezeichnet, sind die regelmäßigen Kundeninformationen von Free-Mail-Anbietern oder Online-Versandhäusern. Sofern solche Nachrichten an einen Kunden des Unternehmens gehen, sind sie rechtlich ebenso zulässig wie Sendungen an solche Personen, die derartige Informationen angefordert haben.<sup>2</sup> Dies gilt natürlich nur so lange, wie der Betroffene seine Zustimmung zum Empfang derartiger E-Mails nicht widerrufen hat, was ihm jederzeit einfach möglich sein muss. Zu beachten ist weiterhin, dass eine einmal erteilte Einwilligung zur Übersendung von Werbung nicht uneingeschränkt gilt. Erfolgt die Zusendung beispielsweise erst zwei Jahre später, ist sie nach Ansicht des Landgerichts Berlin nicht mehr von der Zustimmung des Werbeadressaten gedeckt.<sup>3</sup>

Das in Deutschland und inzwischen auch in den anderen EU-Staaten herrschende Verfahren wird als Opt-In-Regelung bezeichnet. Danach ist die Übersendung von Werbung per E-Mail nur bei vorheriger Einwilligung des Empfängers rechtlich einwandfrei. Im Gegensatz dazu verlangt das bisher in den USA gängige Opt-Out-Verfahren vom Empfänger, dass er nach Erhalt der E-Mail selbst die Initiative ergreifen muss, um eine weitere Belästigung mit elektronischer Post zu unterbinden. Diese Regelung lehnte das europäische Parlament jedoch trotz enormer Lobby-Arbeit nach langem Ringen zu Gunsten der verbraucherfreundlichen jetzigen Regelung ab.

Im Zusammenhang mit Opt-Out-Verfahren stehen die so genannten „Robinson-Listen“. Darunter versteht man Verzeichnisse, in denen Nutzer ihre Mailadressen eintragen können und damit ihren ausdrücklichen Willen angeben, an diese Adressen keine E-Mail-Werbung ohne Zustimmung zu erhalten. Da die Kundgabe eines solchen Willens nach deutschem Recht aber nie erforderlich war, konnten sich derartige Listen in Deutschland nie durchsetzen. Ohnehin haben sich professionelle Spammer nie an derartige Listen gehalten und seriöse Versender von Anfang an auf die explizite Zustimmung der Empfänger gesetzt.<sup>4</sup>

### 6.1.2 Spam und die Gerichte

Als die ersten Klagen aus den Bereichen Internet und E-Mail ab 1996 die deutschen Gerichte erreichten, fehlte es den Richtern nicht nur an speziellen Gesetzen und einschlägiger juristischer Literatur zu der neuen Technik, sondern nicht zuletzt auch an elementaren Kenntnissen der Materie. Während es bei Sachverhalten aus dem Bereich des World Wide Web vor allem in diesen Anfangsjahren häufig zu fragwürdigen Urteilen vor allem in den unteren Instanzen kam, entwickelte sich in der Rechtsprechung zum Thema Spam schnell eine einheitliche und lebensnahe Linie, die sich im Prinzip in dieser Form bis heute durchgesetzt hat. Dies lag sicher auch daran, dass die Richter im Bereich der E-Mail-Werbung auf eine bereits bestehende und ausführliche Rechtsprechung zu verwandten Gebieten zurückgreifen konnten: den Urteilen zu Brief-, BTX-, Fax- und Telefonwerbung.

Elektronische Post lässt sich aus juristischer Perspektive nur auf den ersten Blick mit der althergebrachten Form der Kommunikation auf dem Postweg vergleichen. Die Zusendung von Briefen ist ohne vorherige Einwilligung des Betroffenen zulässig, da weite Bevölkerungskreise – zumindest nach Ansicht der Gerichte – ein Interesse an informativer Werbung haben.<sup>5</sup> Diese Ansicht wird damit begründet, dass die Zustellung von unerwünschter Briefwerbung zwar belästigend sein könne, aber nur eine relativ geringe Beeinträchtigung des persönlichen Bereichs zur Folge habe. Der werbende Inhalt des Prospekts werde vom Verbraucher sofort erkannt und könne gegebenenfalls einfach ent-

---

<sup>2</sup> vgl. zu den Details: Christian Schmoll, E-Mail-Werbung an bestehende Kundenkontakte, JurPC Web-Dok. 283/2004, <http://www.jurpc.de/aufsatz/20040283.htm>

<sup>3</sup> LG Berlin MMR 2004, S. 688

<sup>4</sup> <http://www.ftc.gov/reports/dneregistry/report.pdf>

<sup>5</sup> BGH, Entscheidung vom 30.04.1992, Az. I ZR 287/90

sorgt werden. Im Gegensatz zu Briefen kostet der Versand einer E-Mail jedoch kein Porto und die Kosten liegen überwiegend auf Seiten der Empfänger und der Provider.<sup>6</sup>

Näher liegend ist daher der Vergleich mit der – verbotenen – Werbung per Telefonanruf<sup>7</sup>, per BTX<sup>8</sup> oder insbesondere per Telefax.<sup>9</sup> Während sich der Vergleich mit *cold calls*, also dem unangeforderten Telefonmarketing, vor allem auf den Grad der Belästigung durch das Eindringen in die Persönlichkeitssphäre des Adressaten beschränkt, liegen die Parallelen zur Telefax-Werbung auf der Hand. Der Bundesgerichtshof argumentiert in seinen Entscheidungen zu diesem Thema vor allem mit der Störung des Betriebsablaufs, den Kosten der Inanspruchnahme des Gerätes sowie der Tatsache, dass der Anschluss während der Übermittlung der ungewollten Nachrichten blockiert ist. Diese Punkte lassen sich zumindest teilweise auch auf unerwünschte Werbung per E-Mail übertragen.

Ausgehend von der oben genannten Entscheidung des LG Traunstein und einem richtungsweisenden Urteil<sup>10</sup> des LG Berlin aus dem Jahr 1998 entwickelte sich in den folgenden Jahren eine weitgehend einheitliche Rechtsprechung der Instanzgerichte zum Thema Spam mit einer Fülle von Entscheidungen<sup>11</sup>, unter denen sich nur wenige abweichende Urteile befinden. Dabei gingen die Gerichte ganz überwiegend von der Rechtswidrigkeit der unerwünschten E-Mail-Werbung aus.

Die Rechtsgrundlage für die Unzulässigkeit von Spam liegt bei Gewerbetreibenden in dem Recht am eingerichteten und ausgeübten Gewerbebetrieb sowie bei Privatpersonen im allgemeinen Persönlichkeitsrecht nach den §§ 823, 1004 BGB. Begründet wird dies damit, dass eine unverlangte Werbemail die Aufmerksamkeit des Betroffenen über Gebühr in Anspruch nimmt und zu einer unzumutbaren Belastung des Privat- oder Arbeitsbereiches führt. Darüber hinaus fallen durch den Abruf von E-Mails für den Empfänger Kosten an, während der Versender bei dieser Vertriebsart seine Kosten gleichermaßen zu Lasten des Empfängers reduzieren kann. Wird der Beworbene am Arbeitsplatz mit Spam konfrontiert, so entsteht dem Unternehmen zudem ein Schaden durch verlorene Arbeitszeit und betriebliche Systemressourcen.

Während auf Basis dieser Regelungen nur die Empfänger von Spam gegen den Versender vorgehen und diesem eine zukünftige Belästigung ausschließlich der eigenen Mailadressen verbieten können, bietet das Wettbewerbsrecht ein weitaus schärferes Schwert gegen unerwünschte E-Mail-Werbung. Spam ist eine unerlaubte Werbeform und als unzumutbare Belästigung rechtswidrig. Aus diesem Grunde können auf Basis des Gesetzes gegen den unlauteren Wettbewerb (UWG) Mitbewerber des Spam-Versenders sowie Verbände wie Verbraucher- und Wettbewerbszentralen direkt gegen diesen vorgehen und von ihm bei Androhung einer Strafe verlangen, jegliche unerwünschte E-Mail-Werbung generell zu unterlassen.

Diese bislang herrschende Rechtsprechung wurde im März 2004 durch eine Grundsatzentscheidung des Bundesgerichtshofs bestätigt.<sup>12</sup> Danach ist die Zusendung einer unverlangten E-Mail zu Werbezwecken grundsätzlich als Verstoß gegen die guten Sitten im Wettbewerb anzusehen. Eine solche Werbung sei nur dann ausnahmsweise zulässig, wenn der Empfänger sein Einverständnis zu der Übersendung erklärt habe. Der Werbende habe durch geeignete Maßnahmen sicherzustellen, dass es nicht zu einer fehlerhaften Zusendung einer E-Mail zu Werbezwecken aufgrund des Schreibversehens eines Dritten komme. Schließlich habe der Versender auch das die

---

<sup>6</sup> Vergleiche dazu auch die Gegenüberstellung zwischen Briefpost und E-Mail in Tabelle 4.1 sowie die beispielhafte Kostenrechnung zu Spam in Tabelle 3.1

<sup>7</sup> BGHZ 54, 188; BGH NJW 1989, 2820; BGH GRUR 1990, 280; BGHZ 113, 282

<sup>8</sup> BGH NJW 1988, 1670

<sup>9</sup> BGH NJW 1996, 660

<sup>10</sup> LG Berlin MMR 99, 43

<sup>11</sup> Eine Sammlung von Urteilen findet sich unter <http://www.recht-im-internet.de/themen/spam/>

<sup>12</sup> BGH NJW 2004, 1655

Wettbewerbswidrigkeit ausschließende Einverständnis des Empfängers der E-Mail darzulegen und gegebenenfalls zu beweisen.

### 6.1.3 Maßnahmen des Gesetzgebers

Obwohl in der Rechtsprechung und der juristischen Literatur bereits früh der Ruf nach einer verbindlichen gesetzlichen Regelung der Problematik rund um unerwünschte Werbemails laut wurde, brauchte der Gesetzgeber bis Juli 2004, um eine derartige Regelung im nationalen Recht einzuführen.

Im Rahmen der Reform des Gesetzes gegen den unlauteren Wettbewerb (UWG) wurde in Form des neuen § 7 UWG eine Vorschrift ergänzt, die bestimmte Formen der Direktwerbung, darunter auch das E-Mail-Marketing, nunmehr eindeutig reglementiert.

#### § 7 Unzumutbare Belästigungen

- (1) Unlauter im Sinne von § 3 handelt, wer einen Marktteilnehmer in unzumutbarer Weise belästigt.
- (2) Eine unzumutbare Belästigung ist insbesondere anzunehmen
  - bei einer Werbung, obwohl erkennbar ist, dass der Empfänger diese Werbung nicht wünscht;
  - (...)
  - bei einer Werbung unter Verwendung von automatischen Anrufmaschinen, Faxgeräten oder elektronischer Post, ohne dass eine Einwilligung der Adressaten vorliegt;
  - bei einer Werbung mit Nachrichten, bei der die Identität des Absenders, in dessen Auftrag die Nachricht übermittelt wird, verschleiert oder verheimlicht wird oder bei der keine gültige Adresse vorhanden ist, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.
- (3) Abweichend von Absatz 2 Nr. 3 ist eine unzumutbare Belästigung bei einer Werbung unter Verwendung elektronischer Post nicht anzunehmen, wenn
  - ein Unternehmer im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat,
  - der Unternehmer die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet,
  - der Kunde der Verwendung nicht widersprochen hat und
  - der Kunde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann.

*§ 7 des Gesetzes gegen den unlauteren Wettbewerb in der Form vom Juli 2004 normiert erstmals die Rechtslage bei unerwünschter E-Mail-Werbung*

Die neue Regelung bestätigt die bisherige Rechtsprechung und sorgt für eine eindeutige Rechtslage zumindest im Bereich des Wettbewerbsrechts. Danach gilt in Deutschland das Opt-In-Prinzip, wonach nur derjenige im Rahmen von E-Mail-Werbung angeschrieben werden darf, der hierzu seine Einwilligung erteilt hat oder zu dem der Versender bereits eine Geschäftsbeziehung unterhält. Gleichzeitig besteht für den Empfänger jederzeit das Recht, einer zukünftigen Verwendung seiner Adresse zu widersprechen.

Diese Lösung der Problematik des E-Mail-Marketings beruht in wesentlichen Punkten auf Vorgaben von Seiten der EU. Diese hatte bereits im Jahr 2002 eine Richtlinie<sup>13</sup> erlassen, die von den Mitgliedsstaaten eine Umsetzung des Opt-In-Prinzips in nationales Recht verlangte und wesentliche Punkte der nunmehr beschlossenen Lösung vorgab. Eine entsprechende Umsetzung der Richtlinie wurde inzwischen von allen Staaten der EU vorgenommen, so dass nunmehr von einer vergleichbaren Rechtslage in allen Mitgliedsstaaten ausgegangen werden kann.<sup>14</sup>

Die von Spam betroffenen Verbraucher und Unternehmen können allerdings aus der Regelung im UWG kein eigenes Klagerecht gegen die Versender unerwünschter Werbung herleiten. Klagebefugt auf Basis des Wettbewerbsrechts ist nur der direkte Mitbewerber des Spam-Versenders sowie Verbraucher- und Wettbewerbsverbände oder die Handelskammern, nicht dagegen die unmittelbar von der Spam-Sendung Betroffenen. Diese müssten sich, sofern sie auf Basis des UWG gegen den Werbeversender vorgehen wollen, zunächst an einen der Verbände wenden und diesen um Unterstützung bitten.

Ungeachtet dieser Problematik bleiben die Empfänger von E-Mail-Werbung auch nach der Reform des UWG nicht schutzlos. Wie oben dargelegt, steht ihnen im Rahmen der §§ 823, 1004 BGB aus dem Recht am eingerichteten und ausgeübten Gewerbebetrieb bzw. dem allgemeinen Persönlichkeitsrecht bei Privatpersonen gegen den Versender ein Unterlassungsanspruch zu, der auch jederzeit gerichtlich durchsetzbar ist, sofern natürlich der Spammer zu ermitteln ist.

Der BGH ist in seinem Urteil, welches auf der Rechtslage vor der Reform des UWG beruht, noch davon ausgegangen, dass E-Mail-Werbung auch dann ausnahmsweise zulässig sei, wenn bei der Werbung gegenüber Gewerbetreibenden aufgrund konkreter tatsächlicher Umstände ein sachliches Interesse des Empfängers vermutet werden könne. Dies ist mit den neuen Regelungen des § 7 UWG inzwischen nicht mehr vereinbar. Die Vorschrift verbietet nunmehr generell jede „unzumutbare Belästigung“ von Marktteilnehmern, also sowohl von Gewerbetreibenden als auch von Privatpersonen.<sup>15</sup>

Insgesamt kann man spätestens nach den jüngsten Gesetzesänderungen sowie dem Grundsatzurteil des BGH in Deutschland von einer eindeutigen Rechtslage sprechen, wonach der Versand von E-Mail-Werbung ohne vorherige Zustimmung durch den Empfänger oder vorherigen Geschäftskontakt nicht zulässig ist.

## 6.2 Zivilrechtliche Maßnahmen gegen Spam

Aufgrund der dargelegten klaren Rechtslage und der inzwischen durch zahlreiche Urteile gefestigten Rechtsprechung ist die Durchsetzung von rechtlichen Maßnahmen gegen Spammer möglich. Dies gilt in dieser Form jedoch nur für Spam, der eindeutig und gerichtsfest nachweisbar aus Deutschland versandt wurde oder für eine Website wirbt, für die ein Deutscher rechtlich verantwortlich ist. Die Durchsetzung von rechtlichen Ansprüchen gegen Versender außerhalb der Bundesrepublik und insbesondere außerhalb der EU ist dagegen schwierig und in der Praxis meist schon aufgrund des hohen finanziellen Risikos wenig empfehlenswert. Die nachfolgenden Betrachtungen beschränken sich daher auf den Bereich der Bundesrepublik.

---

<sup>13</sup> Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), online abrufbar unter [http://www.bfd.bund.de/aktuelles/eurili\\_ekommun.pdf](http://www.bfd.bund.de/aktuelles/eurili_ekommun.pdf)

<sup>14</sup> Eine Übersicht über die Umsetzung der EU-Richtlinie in einzelnen Staaten findet sich unter <http://www.antispam.de/download/antispam-gesetze.pdf>

<sup>15</sup> Vgl. zur neuen Rechtslage auch: Dieselhorst/Schreiber, Computer und Recht (CR) 2004, S. 680

### 6.2.1 Wer haftet für Spam?

Grundsätzlich steht dem Empfänger einer unerwünschten und rechtlich unzulässigen Werbemail nach deutschem Recht gegen den Versender ein Anspruch auf Unterlassung zu. Doch die Haftung für den Versand von Spam beschränkt sich nicht allein auf den Absender.

Nach den Grundsätzen der Störerhaftung können auch Mitwirkende zur Unterlassung verpflichtet werden. Störer ist nach der Definition des Bundesgerichtshofs<sup>16</sup> derjenige, der an der rechtswidrigen Handlung eines eigenverantwortlichen Dritten willentlich und adäquat kausal mitwirkt, wobei es auf ein Verschulden nicht ankommt. Als Mitwirkung genügt auch die Unterstützung oder das Ausnutzen des Handelns eines eigenverantwortlichen Dritten, sofern der Störer die rechtliche Möglichkeit zur Verhinderung dieser Handlung hatte. Die Störerhaftung trifft also auch denjenigen, der vom Versand einer unerwünschten Werbemail Vorteile hat, also etwa den Betreiber der beworbenen Website oder Inhaber der genannten 0190er-Nummer.

Die Rechtsprechung legt diese Grenze in Einzelfällen noch weiter aus. So haftet regelmäßig der Anbieter von *e-cards*, also elektronisch versandten Grußkarten, für unerwünschte Nachrichten, die über seine Applikation verschickt werden.<sup>17</sup> Der Anbieter ist nach Meinung der Rechtsprechung schon durch das Bereithalten der Versandfunktion als Mitstörer für die Rechtsverletzung verantwortlich. Er müsse insbesondere auch damit rechnen, dass ein solcher Dienst durch Dritte missbraucht werde und gegebenenfalls Filter verwenden, um einen solchen Missbrauch zu unterbinden.

Nicht verantwortlich für Spam-Sendungen sind dagegen die Zugangs-Provider. Hier sieht § 9 des Teledienstegesetzes (TDG) eine Privilegierung der Diensteanbieter vor, die lediglich fremde Informationen an Dritte vermitteln, ohne deren Inhalt zu kennen. Eine Grenze findet diese Haftungsfreistellung jedoch, wenn Access-Provider mit ihren Kunden zusammenarbeiten oder die Übermittlung selbst veranlassen. Eine eigene Haftung des Providers käme also allenfalls dann in Betracht, wenn er gezielt und gerichtlich nachweisbar mit einem Spamversender kooperiert. Seriöse Anbieter werden ohnehin in ihren AGB eine Klausel aufnehmen, welche die Versendung unerwünschter E-Mail-Werbung unter Nutzung der eigenen Infrastruktur verbietet und jedem dagegen verstoßenden Kunden unverzüglich kündigen.

In Einzelfällen kann die Störerhaftung für Spamversand allerdings den Hosting-Provider umfassen. So stellte das Landgericht Leipzig in einem Berufungsurteil<sup>18</sup> fest, dass ein solcher Anbieter als so genannter „Zustandsstörer“ neben einem nicht zu ermittelnden Subdomain-Inhaber für darüber versandten Spam selber hafte. Dies gelte zumindest dann, wenn der Provider bei der Vergabe einer Subdomain seine Prüfungspflichten über die Identität seines Kunden verletze und der dadurch nicht zu ermitteln sei. Dabei käme es nicht darauf an, ob der Hoster der Subdomain die Werbemails selbst versandt habe oder nicht.

### 6.2.2 Schadensersatz und Gewinnabschöpfung

Nach dem Gesetzeswortlaut steht dem Empfänger einer unerwünschten Werbemail gegen den Sender neben dem Anspruch auf Unterlassung auch ein Schadensersatzanspruch zu. Als Schaden kommen neben den Kosten für Abruf und Lesen der E-Mails auch die Belastung der Ressourcen des Betroffenen in Frage. Der Anspruch dürfte jedoch in den allermeisten Fällen theoretischer Art sein. Dies liegt vor allem daran, dass vor Gericht der Nachweis eines konkret zu beziffernden Schadens notwendig ist, der faktisch nur schwer zu leisten ist. Ohnehin dürfte der für den Empfänger durch die Übersendung einer Spam-Mail entstehende Schaden in Euro-Cent zu bemessen sein, was eine

---

<sup>16</sup> BGH GRUR 1991, 769

<sup>17</sup> OLG München, MMR 2004, 324 m.w.N.

<sup>18</sup> LG Leipzig, JurPC Web-Dok. 66/2004

Verfolgung eines solchen Anspruchs unwirtschaftlich erscheinen lässt. Folglich gibt es auch kaum Urteile, die sich mit der Problematik der Schadensersatzforderung gegen Spammer beschäftigen.

In dem einzig bekannten und wenig repräsentativen Fall<sup>19</sup> im Bereich der unerwünschten E-Mail-Werbung wurde ein entsprechender Antrag abgewiesen. Bei Fax-Werbung dagegen wurde bereits Schadensersatz zugesprochen.<sup>20</sup> Der Kläger erhielt 290 DM für den Zeitaufwand und die Kosten, die ihm beim Ermitteln des Absenders und für die Durchsetzung seiner Ansprüche entstanden sind.

Ganz andere Beträge könnten – zumindest theoretisch – in Verfahren anfallen, die auf dem Wettbewerbsrecht basieren. Nach § 9 UWG ist derjenige, der vorsätzlich oder fahrlässig unlautere Wettbewerbshandlungen vornimmt, darunter fällt auch der Versand unerwünschter E-Mail-Werbung, dem Mitbewerber zum Ersatz des daraus entstandenen Schadens verpflichtet. Doch auch hier stellt sich die Frage nach der Nachweisbarkeit eines Schadens, den ein Konkurrent dadurch erleidet, dass ein Mitbewerber Spam verschickt. Er dürfte kaum zu beziffern und vor Gericht einzuklagen sein.

Auch um diesem Problem zu begegnen, hat der Gesetzgeber bei der Reform des Wettbewerbsrechts im Sommer 2004 mit § 10 UWG ein neues Instrument kreiert: den Gewinnabschöpfungsanspruch. Bei vorsätzlichem Wettbewerbsverstoß zu Lasten einer Vielzahl von Abnehmern kann der Verursacher von Verbänden, Industrie- und Handelskammern, Wettbewerbs- und Verbraucherschutzvereinen auf Herausgabe des dadurch erzielten Gewinns in Anspruch genommen werden. Dieser wird dann nach Abzug der Kosten für die Rechtsverfolgung von den Vereinigungen dem Bundeshaushalt zugeführt.

In der Praxis bleibt abzuwarten, wie sich dieses neue Instrument bewährt. Urteile sind derzeit noch nicht bekannt. Gerade gegenüber dem massenhaften Versand von Spam oder auch dem Missbrauch von 0190/0900er-Nummern könnte es sich aber als wirksames Werkzeug erweisen.

### 6.2.3 Abmahnung

Wie kann der Empfänger einer Spam-Mail also gegen den Versender juristisch vorgehen? Mittel ist zunächst die Abmahnung. Hierunter versteht man die formale Aufforderung einer Person an einen potentiellen Rechtsverletzer, ein bestimmtes Verhalten künftig zu unterlassen.

Sinn und Zweck einer Abmahnung ist es, schon im Rahmen eines außergerichtlichen Verfahrens einen Streitfall zu klären. Dies kann dadurch erreicht werden, dass der Abgemahnte dem Gegner vertraglich zusichert, in Zukunft den gerügten Rechtsbruch nicht mehr zu begehen oder diesen zu unterbinden. Da der Abmahnende auf eine bloße Zusicherung allein nicht vertrauen muss, ist nach der Rechtsprechung ein so genanntes Vertragsstrafversprechen erforderlich. Damit verpflichtet sich der Abgemahnte, im Falle eines erneuten Verstoßes einen festgelegten oder von einem Gericht festzusetzenden Betrag an den Abmahnenden zu zahlen. Die Höhe der Vertragsstrafe ist variabel und richtet sich nach dem Einzelfall. Es gilt die Regel, dass die zu zahlende Summe so schmerzhaft sein muss, dass er den Verstoß sicher nicht wiederholt. Daher reichen Strafen im Bereich von 100 € nur in wenigen Fällen aus, in der Praxis üblich sind Vertragsstrafen ab 2500 € aufwärts.

Die Einschaltung eines Rechtsanwalts zur Versendung einer Abmahnung ist zwar formal nicht erforderlich, in den meisten Fällen jedoch empfehlenswert, da ein solches Schriftstück eine Reihe von formalen Voraussetzungen hat, die es einzuhalten gilt. Wird die Abmahnung durch einen Anwalt geschrieben, entstehen hierdurch noch näher darzulegende Kosten, die der Gegner zu erstatten hat, sofern er tatsächlich einen Rechtsverstoß begangen hat. Diese Pflicht zu Erstattung der Kosten wird als „Geschäftsführung ohne Auftrag“ damit begründet, dass der Anwalt durch die Abmahnung quasi im Willen des Empfängers handelt und es diesem dadurch ermöglicht, die weitaus höheren Kosten eines Gerichtsverfahrens zu vermeiden.

---

<sup>19</sup> AG Dachau CR 2002, 455

<sup>20</sup> AG Frankfurt/M., MMR 2002, 490

Gibt der Verursacher von unerwünschten Werbemails aufgrund einer Abmahnung eine strafbewehrte Unterlassungserklärung ab und übernimmt ggf. die Anwaltskosten, so ist die Angelegenheit damit erledigt. Eine solche Erklärung enthält typischerweise die Verpflichtung dazu, es zu unterlassen, an Mailadressen des Empfängers zukünftig „bei Meidung einer Vertragsstrafe in Höhe von 5.001,00 €“ ohne vorherige Zustimmung oder Aufforderung E-Mail-Werbung zu versenden oder durch Dritte versenden zu lassen. Der krumme Betrag von 5.001 € erklärt sich damit, dass ab dieser Höhe ein eventueller Rechtsstreit in den Zuständigkeitsbereich der Landgerichte fällt.

#### 6.2.4 Einstweilige Verfügung

Wird dagegen die Abgabe einer strafbewehrten Unterlassungserklärung durch den Spam-Versender verweigert oder die Angelegenheit schlicht ignoriert, so bleibt juristisch nur noch der Weg vor die Gerichte. Hierbei stehen dem Kläger zwei Möglichkeiten offen: das Hauptsache- oder das Verfügungsverfahren.

Die Vorteile des Verfügungsverfahrens liegen auf der Hand. Es handelt sich dabei um ein juristisches „Eilverfahren“, bei dem eine gerichtliche Entscheidung in der Regel innerhalb von wenigen Tagen oder Wochen erlangt werden kann. Ausgangspunkt ist das Stellen eines „Antrags auf Erlass einer einstweiligen Verfügung“ vor dem zuständigen Gericht, in der Regel das für den Ort des Spam-Empfangs zuständige Landgericht. Ein solcher Antrag muss allerdings – schon aufgrund der Eilbedürftigkeit – innerhalb einer vergleichsweise kurzen Frist nach Zugang der unerlaubten Werbemail eingereicht werden. Als Faustregel gelten hier vier Wochen nach Empfang. Gleichzeitig sind die Beweismittel eingeschränkt, da z. B. eine langwierige Zeugenvernehmung im Rahmen einer Eilentscheidung kaum möglich ist.

Erscheinen dem zuständigen Gericht die vorgelegten Beweise glaubhaft und der geltend gemachte Anspruch juristisch schlüssig, so wird es ohne mündliche Verhandlung – also ohne Anhörung des Gegners – einen Beschluss erlassen. Der Antragsgegner wird also in den meisten Fällen erst durch den Gerichtsvollzieher, der ihm den Beschluss zustellt, von dem Verfahren Kenntnis erlangen. Dem Betroffenen bleibt nun die Möglichkeit, gegen die Verfügung Widerspruch einzulegen und somit eine Verhandlung über die Sache zu erreichen. Gegen das hieraus resultierende Urteil kann Berufung eingelegt werden. Unabhängig davon kann der Betroffene auch ein Hauptsacheverfahren einleiten.

In der Praxis wird in vielen Fällen schon durch das Verfügungsverfahren eine abschließende Klärung des Streitfalls erreicht. Das liegt vor allem daran, dass das Gericht zwar die dem Verfahren zugrunde liegenden Tatsachen nur summarisch prüft, die Rechtsfragen aber in vollem Umfang klärt. Zudem sind sowohl im einstweiligen Rechtsschutz als auch im Hauptsacheverfahren die gleichen Gerichte und Kammern zuständig.

Das Verfügungsverfahren hat für den Antragsteller jedoch auch Nachteile. Zwar erhält er innerhalb von kurzer Zeit eine gerichtliche Entscheidung, die auch vollstreckbar ist. Trotzdem regelt diese den Rechtsstreit schon ihrer Natur nach nur „einstweilig“. Es bleibt das Risiko, noch einmal das gesamte Verfahren im Rahmen der Hauptsacheklage durchstehen zu müssen – und selbstverständlich auch das Risiko der dadurch entstehenden Kosten.

Hinzu kommt ein spezielles Problem im Bereich von Spam. Zwar ist die Beantragung einer einstweiligen Verfügung wegen unerlaubter E-Mail-Werbung im Bereich der meisten Gerichte unproblematisch möglich. Einige wenige Entscheidungen<sup>21</sup> lehnten jedoch bei E-Mail-Werbung den Erlass einer Verfügung ab, da die Gerichte – insbesondere bei einzeln übersandten Nachrichten – keine Eilbedürftigkeit annehmen wollten. Diese Auffassung steht allerdings im Widerspruch zu der gängigen Rechtsprechung der meisten deutschen Gerichte.

---

<sup>21</sup> OLG Düsseldorf, Beschluss vom 26. März 2003, Az. I-15 W 25/03 und OLG Koblenz MMR 2003, 590

### 6.2.5 Hauptsacheverfahren

Wer die Risiken einer einstweiligen Verfügung meiden will, sollte das „normale“ gerichtliche Verfahren wählen und eine Unterlassungsklage im Hauptsacheverfahren anstreben. Nach dem Einreichen der Klageschrift und der Überweisung der Gerichtskosten erhält in solchen Verfahren der Gegner die Gelegenheit, zu der Klage Stellung zu nehmen. Nach einiger Zeit kommt es dann in der Regel zu einer mündlichen Verhandlung, in der die Parteien die Anträge stellen und den Sachverhalt mit dem Gericht erörtern. Am Ende steht nach einigen Monaten ein Urteil des Gerichts, gegen das Berufung und Revision zulässig sind.

Das Hauptsacheverfahren ist zwar meist der „sicherere Weg“, hat aber zugleich den erheblichen Nachteil, dass während der Dauer des Verfahrens der Spammer ungestört mit der Zusendung weiterer Werbemails fortfahren kann. Frühestens nach Zustellung der Urteilsbegründung an den Kläger kann dieser aus dem Urteil vollstrecken und dem Spammer juristisch Einhalt gebieten. Häufig wird bis dahin ein Jahr ins Land gegangen sein.

### 6.2.6 Erfolgsaussichten und typische Probleme in Spam-Verfahren

Wie bereits dargelegt, sind die Erfolgsaussichten für Gerichtsverfahren gegen Spammer aus Deutschland angesichts der klaren Rechtslage vergleichsweise gut.

In einem Verfahren gilt es primär, gegenüber den Richtern nachzuweisen, dass der Beklagte auch tatsächlich der Versender der unerwünschten Werbung war. Dieser wird im Zweifelsfall stets behaupten, seinerseits die Nachrichten nicht versandt zu haben oder gar Opfer eines so genannten *Joe Jobs* zu sein.

Gegen diese Behauptung hilft häufig schon ein Blick in den *header* der streitgegenständlichen E-Mail, der nicht selten bereits das Gegenteil beweist. Auch ist es schon aufgrund der allgemeinen Lebenserfahrung in den allermeisten Fällen kaum glaubhaft, dass sich ein in fremden Diensten stehender und daran verdienender Spammer die Mühe macht, Zeit und Energie in die Bewerbung der Online-Präsenz eines Dritten zu investieren.

Ein weiteres Problemfeld bei der gerichtlichen Durchsetzung von Ansprüchen gegen Versender unerwünschter Werbemails war bislang die Frage der mutmaßlichen Einwilligung des Empfängers. Während bei Werbung gegenüber Privatpersonen keine E-Mail ohne vorheriges und eindeutig geäußertes Einverständnis versandt werden darf, kann bei Geschäftskunden noch nach Ansicht des BGH in seinem Spam-Urteil ein „vermutetes Einverständnis“ ausreichen.

Die bisherige Rechtsprechung ist jedoch mit der Neuformulierung des § 7 UWG nF nicht länger vereinbar. Diese Regelung bezieht sich mangels einer entsprechenden Differenzierung eindeutig sowohl auf natürliche als auch auf juristische Personen. Damit reicht auch ein mutmaßliches Interesse von gewerblichen Empfängern künftig nicht mehr aus, um diesem E-Mail-Werbung zu übersenden.<sup>22</sup>

### 6.2.7 Kosten für rechtliche Maßnahmen

Nach deutschem Recht trifft die gesamte Kostenlast eines Gerichtsverfahrens immer denjenigen, der unterliegt. Daher muss auch in einem Verfahren wegen unerwünschter E-Mail-Werbung der Spammer bei einem Urteil zu seinen Lasten die Anwalts- und Gerichtskosten beider Seiten übernehmen. Es bleibt jedoch in jedem Verfahren ein gewisses Restrisiko für den Kläger. Denn auch im Falle des Obsiegens kann dieser in Ausnahmefällen auf seinen Kosten „sitzen bleiben“; nämlich dann, wenn die Gegenseite – etwa durch Insolvenz – zahlungsunfähig und daher nicht in der Lage ist, die per Gerichtsbeschluss auferlegten Zahlungen zu leisten.

---

<sup>22</sup> dazu ausführlich: Dieselhorst/Schreiber, Computer und Recht (CR) 2004, S. 680

Die Höhe der Anwalts- und Gerichtskosten bemessen sich in Deutschland in der Regel nach dem Rechtsanwaltsvergütungsgesetz (RVG) bzw. dem Gerichtskostengesetz (GKG) und werden anhand des Werts einer Sache bemessen. Üblicherweise werden in Verfahren rund um unerwünschte E-Mail-Werbung von den Gerichten Streitwerte zwischen 2.500 und 15.000 € angesetzt.

In der Praxis fallen für eine anwaltliche Abmahnung eines Spammers bei einem angemessenen Gegenstandswert von 7.500 € Anwaltskosten von insgesamt rund 645 € an. Auch diese Summe hat ein Spammer im Falle einer gerechtfertigten Abmahnung voll zu ersetzen. Die Kosten für ein Gerichtsverfahren in der Hauptsache liegen bei gleichem Streitwert bei rund 2.436 € in der ersten Instanz und bei 3.387 € für ein Verfahren über zwei Instanzen. Geht dem Hauptsacheverfahren noch ein Verfügungsverfahren voraus, so kann sich der Gesamtbetrag für Anwalts- und Gerichtskosten also auf weit über 6.000 € als maximales Prozessrisiko summieren.

### 6.2.8 Datenschutzrechtlicher Auskunftsanspruch

Wer das Risiko einer gerichtlichen Auseinandersetzung scheut oder ganz einfach wissen will, woher ein Versender von E-Mail- oder sonstiger Werbung die eigenen Daten erhalten hat, dem bleibt ungeachtet der oben beschriebenen Vorgehensweisen noch die Möglichkeit, von dem Versender eine datenschutzrechtliche Auskunft zu verlangen. Dieser ist gemäß § 34 des Bundesdatenschutzgesetzes verpflichtet, Auskunft darüber zu erteilen, welche personenbezogenen Daten des Betroffenen er speichert, zu welchem Zweck dies geschieht, an wen er diese übermittelt und woher er die Angaben bekommen hat.

#### **Musterschreiben: Datenschutzrechtliche Auskunft**<sup>23</sup>

Betr.: Auskunftsverlangen nach § 34 BDSG Sehr geehrte Damen und Herren,

Sie haben mir am [Datum] Werbematerialien der Firma XY zugesandt, welche ich nicht angefordert habe. Somit besteht ein konkreter Hinweis darauf, dass Sie von mir personenbezogene Daten gespeichert haben.

- 1 Ich fordere Sie daher unter Hinweis auf § 34 BDSG auf, mir unentgeltlich Auskunft zu erteilen über die bei Ihnen über mich gespeicherten Daten, den Zweck der Speicherung, die Personen und Stellen, an die meine Daten übermittelt werden, sowie insbesondere die Herkunft und weitere Empfänger.
2. Gleichzeitig widerspreche ich mit sofortiger Wirkung der Nutzung und Übermittlung meiner Daten insbesondere zum Zwecke der Werbung und der Markt- und Meinungsforschung soweit diese aufgrund gesetzlicher Regelungen nicht ausnahmsweise zulässig ist.

Für die Erledigung dieser Angelegenheit setze ich Ihnen eine Frist bis zum ... [zwei Wochen].

Bei Nichteinhaltung dieser Frist sehe ich mich gezwungen, mein Auskunftsrecht gerichtlich geltend zu machen und eine Auskunftsklage gegen Sie zu erheben, wodurch Ihnen erhebliche Kosten entstehen können. Weiterhin werde ich in diesem Fall die für Sie zuständige Aufsichtsbehörde nach § 38 BDSG einschalten.

Mit freundlichen Grüßen

Der Vorteil des Auskunftersuchens nach BDSG liegt vor allem darin, dass sie für den Betroffenen im Normalfall keine Kosten nach sich zieht. Allerdings sind die Antworten der speichernden Unternehmen in der Praxis für den Fragenden nicht immer sehr aussagekräftig.

<sup>23</sup> Eine Sammlung von Mustern für Auskunftsansprüche hält das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) online bereit: <http://www.datenschutzzentrum.de/selbstdatenschutz/checkheft/index.htm>

## 6.3 Spam und Strafrecht

Entgegen einer in der Öffentlichkeit weit verbreiteten Meinung ist der Versand von unerwünschter E-Mail-Werbung als solches nach derzeitigem Recht nicht strafbar. Dies gilt zumindest dann, wenn der Spammer für den Versand der Nachrichten auf eine eigene Infrastruktur zurückgreift. Anders sieht die Rechtslage in den Fällen aus, in denen er sich dazu der Rechner von Dritten bedient, also etwa im Rahmen von Botnetzen. Zudem kann sich in Einzelfällen eine Strafbarkeit durch die Fälschung der Absenderadressen ergeben.

### 6.3.1 Strafbarkeit des Versands von Spam

Hinsichtlich einer möglichen Strafbarkeit des Versands von unerwünschter E-Mail-Werbung werden in der juristischen Diskussion<sup>24</sup> überwiegend die Straftatbestände des Erschleichens von Leistungen, § 265a StGB, der Datenveränderung, § 303a StGB, der Computersabotage, § 303b StGB sowie der Störung von Telekommunikationsanlagen, § 317 StGB, genannt.

Eine Strafbarkeit nach § 265a StGB für das Erschleichen von Leistungen scheidet auch in den Fällen aus, in denen die Spam-Mails über fremde Rechner verschickt werden. Diese Vorschrift setzt voraus, dass jemand die Leistung eines öffentlichen Zwecken dienenden Telekommunikationsnetzes in der Absicht erschleicht, das für die Nutzung normalerweise fällige Entgelt nicht zu entrichten. Zwar ist es durchaus möglich, dass ein Spam-Versender bestimmte Kontrollen oder Sicherheitssysteme auf dem von ihm benutzten Server umgeht. Das geschieht jedoch primär in der Absicht, die effektive und weitgehend anonyme Verteilung seiner Werbenachrichten per Zombie-PC (siehe Kapitel 4.2.5) oder über offene Relays zu ermöglichen. Es fehlt also an der für § 265a StGB als so genanntes „Vermögensdelikt“ notwendigen Absicht, eine üblicherweise entgeltspflichtige Leistung ausnahmsweise ohne Gegenleistung zu nutzen, dies ist allenfalls eine Nebenfolge des Handelns. Die bloße Nutzung eines fremden Rechners ohne dessen Beeinträchtigung ist ohnehin nicht strafbar und wird allgemein nur als folgenloser „Zeitdiebstahl“ behandelt.

Diskutiert als möglicherweise einschlägige Strafrechtsnorm bei der Versendung von Spam wurde in der Vergangenheit weiterhin der § 303a des Strafgesetzbuches (StGB), die Datenveränderung bzw. Datenunterdrückung. Im strafrechtlichen Sinne „unterdrückt“ werden Daten, wenn sie dem Zugriff des Verfügungsberechtigten auch nur vorübergehend entzogen werden und dieser deshalb nicht mehr auf sie zugreifen kann. Damit fallen unter diese Norm wie auch unter § 317 StGB vor allem die Fälle, in denen es aufgrund von massivem Spam-Aufkommen auf Seiten des Mailservers zu erheblichen Performance-Problemen kommt oder der Speicherplatz des betroffenen Users durch Spam ausgereizt ist und daher eine Zustellung von regulären E-Mails nicht mehr stattfindet. Allerdings ist eine derartige Argumentation heute angesichts des beständig wachsenden Speicherangebots auch bei E-Mail-Postfächern kaum noch relevant. Auch zu Server-Blockaden wird es im normalen Betrieb allein durch den Zugang von Spam-Mail kaum kommen. Erfasst werden daher von den §§ 303a, 303b, 317 StGB allenfalls Sonderfälle wie die noch zu behandelnden *Mail-Bombings* oder *Joe Jobs*.

Schließlich scheidet auch eine Anwendung von § 269 StGB auf die Versendung von unerwünschter Werbemail. Zwar sind in fast allen Spam-Sendungen die Angaben über den Absender vorsätzlich gefälscht. Da es aber zumindest E-Mails ohne digitaler Signatur üblicherweise an der Urkundeseigenschaft fehlt, kommt weder eine Strafbarkeit aufgrund der Fälschung beweisbarer Daten nach § 269 StGB noch auf Basis von Urkundenfälschung nach § 267 StGB in Frage.

---

<sup>24</sup> Zur Strafbarkeit von Werbemails: Thomas Frank, „You've got (Spam-)Mail“ – Zur Strafbarkeit von E-Mail-Werbung, CR 2004, S. 123

### 6.3.2 Strafbare Inhalte in Spam-Mails

Darüber hinaus kann sich eine Strafbarkeit auch aus den Inhalten der versandten Spam-Mails ergeben. Häufigster Fall dürfte das Verbreiten pornographischer Schriften nach § 184 StGB sein. Diese Vorschrift ist unter anderem dann erfüllt, wenn harte Pornographie Personen unter 18 Jahren zugänglich gemacht wird. Versendet also ein Spammer eine E-Mail mit derartigen Bildern, so macht er sich strafbar. Gleiches gilt selbstverständlich auch für die Verbreitung von kinderpornographischen Inhalten als Bild, Text oder auch nur mit entsprechenden Links. Hier spielt es keine Rolle, ob die Nachricht an Minderjährige oder Erwachsene geht.

Je nach Formulierung der E-Mail können in Einzelfällen die Tatbestände des Betrugs nach § 263, der Beleidigung oder Verleumdung nach §§ 185 ff. und der unerlaubten Veranstaltung eines Glücksspiels nach § 284 StGB verwirklicht sein.

### 6.3.3 Fälschung der Absenderadresse

Da die Absenderangaben bedingt durch die Unzulänglichkeiten des SMTP beliebig ausgefüllt werden können, nutzen Spam-Versender frei erfundene Absenderadressen aus existierenden Domains zur Versendung ihrer Nachrichten. Grund dafür ist, dass immer mehr Mailhosts beim Eingehen der E-Mail überprüfen, ob die Domain existiert – wenn nicht, wird die E-Mail als Spam klassifiziert. Für die Domaininhaber als Leidtragende dieser Kollateralschäden des Wettrüstens zwischen Spammern und Mailserver-Betreibern hat das häufig sehr unangenehme Folgen: Rückläufer wie Fehlermeldungen von Mailservern verstopfen die Postfächer der vermeintlichen Absender. Im Extremfall kann die Zahl der eintreffenden Rückläufer an einem Tag in die Hunderttausende gehen und die Verfügbarkeit des Mailservers gefährden.

Ohnehin werden die Versender in den allermeisten Fällen ihr Unwesen in außereuropäischen Ländern treiben und so für die deutsche Justiz kaum greifbar sein. Aber auch bei Tätern in Deutschland offenbart die bestehende Rechtslage eine Regelungslücke. Dies gilt insbesondere für private User, deren Domains missbraucht werden. Bei dieser Form der Manipulation handelt es sich weder um Betrug noch um Computerbetrug, auch Urkundenfälschung liegt nicht vor.

Gewerblichen Anbietern, deren Domain als Absender missbraucht wird, kann dagegen das Markenrecht helfen, das in § 143 MarkenG die „strafbare Kennzeichenrechtsverletzung“ verbietet. Danach ist es bei einer Strafandrohung von maximal fünf Jahren verboten, vorsätzlich eine eingetragene Marke oder ein Geschäftskennzeichen ohne Zustimmung des Inhabers im geschäftlichen Verkehr in verwechslungsfähiger Art und Weise zu nutzen. Da die Rechtsprechung davon ausgeht, dass eine im geschäftlichen Verkehr verwendete Domain ein Unternehmenskennzeichen ist, wäre danach die Verwendung einer derartigen Adresse als Absenderangaben in Spam eine strafbare Handlung. Urteile zu diesem Bereich bestehen jedoch trotz einer Reihe von Strafanzeigen nicht.

In dem Fall, dass enorme Mengen an Spam-Mails verschickt werden und die Anzahl der *bounces* (Rückläufer) so hoch ist, dass der Mailserver vorübergehend ausfällt, greift der eigentlich für Hacker-Angriffe konzipierte § 303b StGB, die Computersabotage. Diese Vorschrift schützt allerdings wiederum nur essenzielle Infrastruktur von Unternehmen oder Behörden, nicht dagegen die Anlagen von Privatpersonen. Betroffenen Privatleuten bleibt nur der Weg, den Spammer zivilrechtlich auf Unterlassung und Schadensersatz zu verklagen. Das Prozesskostenrisiko ist dabei hoch, die Beweislast liegt beim Kläger.

### 6.3.4 Vorsätzliche Schädigung durch Absenderfälschung

Der Missbrauch von E-Mails mit dem Ziel, durch den Versand von Spam den Unmut der Empfänger, ISPs und Hosters auf den vermeintlichen Absender und dessen Online-Präsenz zu lenken, wird als *Joe*

*Job* bezeichnet. Hier werden häufig nicht nur die Absenderadressen gefälscht, sondern der Inhalt der E-Mail wird darüber hinaus so gestaltet, als ob er für den angeblichen Absender werben würde.

Eine rechtliche Beurteilung solcher Angriffe in Literatur und Rechtsprechung steht derzeit noch aus. Es spricht aber viel dafür, dass zumindest auf der strafrechtlichen Ebene ein Verweis auf die Ausführungen zur Adressfälschung möglich ist. Auch bei *Joe Jobs* dürfte danach eine Strafbarkeit nur in Ausnahmefällen anzunehmen sein, etwa bei gezielten Attacken auf den Mailserver oder beim Missbrauch von geschützten Kennzeichen. Das liegt auch daran, dass E-Mails keine Urkunden im Rechtssinne sind und damit eine Strafbarkeit hinsichtlich Urkundenfälschung und verwandter Delikte ausscheidet. Wie im oben genannten Fall bleibt den Geschädigten nur ein zivilrechtliches Vorgehen, etwa aus § 826 BGB im Rahmen der vorsätzlichen sittenwidrigen Schädigung.

### 6.3.5 Selbsthilfemaßnahmen gegen Spammer

Unter rechtlichen Gesichtspunkten ähnlich zu behandeln sind die von der „Antispam-Szene“ eingesetzten Mittel. Häufig wird hier neben legalen Mitteln wie Beschwerden bei Mail- und Hosting-Providern auch auf solche Handlungsweisen zurückgegriffen, die sich in einer rechtlichen Grauzone befinden, z. B. das so genannte „Server-Streicheln“ (siehe Kasten).

#### „Server-Streicheln“

Unter dem „Streicheln“ von Servern versteht man das massenhafte Abrufen von per Spam beworbenen Webseiten, letztendlich also nicht anderes als einen DDoS-Angriff. Der dadurch entstehende Traffic führt in vielen Fällen auf Seiten der Spammer zu erheblichen Mehrkosten. Verwendet wird dazu meist das Linux-Tool wget, das per Skriptsteuerung komplette Webseiten oder größere Grafiken herunterlädt.

Auch hier ist die Grenze der Strafbarkeit entsprechend der obigen Ausführungen wohl erst dann erreicht, wenn aufgrund der Angriffe der betroffene Server funktionsunfähig oder zumindest unbrauchbar wird. Eine Strafbarkeit kann sich also wie oben beschrieben aus §§ 303a, 303b, 317 StGB ergeben. Allerdings fehlt es auch in diesem Bereich noch an relevanten gerichtlichen Entscheidungen.

## 6.4 Viren, Würmer und Trojaner rechtlich betrachtet

Wie bereits ausgeführt, unterfällt der durch Malware verursachte Mail-Traffic zwar der technischen, nicht aber der juristischen Definition von Spam. Allerdings ist die vorsätzliche Verbreitung von Viren, Würmern und Trojanern strafbar, und unter Umständen machen sich auch diejenigen schadensersatzpflichtig, die ohne eigene Kenntnis Malware weiterverbreiten.

### 6.4.1 Vorsätzliches Verbreiten von Malware

Das Gefährdungspotential von Malware hat sich in den letzten Jahren entscheidend verschärft. Bisher wurde vor allem der infizierte Rechner manipuliert und schlimmstenfalls unbrauchbar gemacht. Inzwischen jedoch werden elektronische Schädlinge, die sich massiv und automatisiert weiterverbreiten, häufig für kriminelle Aktionen gegenüber Dritten eingesetzt. So entstehen wahre Heere von fremdkontrollierten Rechnern, über die DDoS-Attacken<sup>25</sup> ausgeführt oder Spam-Mails versandt werden.

---

<sup>25</sup> Etwa im Rahmen der Erpressung eines Wettbüros mit der Androhung einer DDoS-Attacke, vgl. <http://www.heise.de/security/news/meldung/48613>

Hinsichtlich der Haftung für dadurch verursachte Schäden juristisch unumstritten ist vor allem die Haftung desjenigen, der in Schädigungsabsicht Malware herstellt und verbreitet. Abhängig von der Schadensroutine des Virus, Wurms oder Trojaners wird sich der Versender des Ausspähens von Daten nach § 202 des Strafgesetzbuches (StGB), des Computerbetrugs nach § 263a, der Datenveränderung nach § 303a oder der Computersabotage nach § 303b StGB strafbar machen. Daneben haftet er zivilrechtlich aus § 826 des Bürgerlichen Gesetzbuches (BGB) und weiteren Vorschriften auf Schadensersatz.

Allerdings ist ein Vorsatz in den meisten Fällen nur schwer nachzuweisen, und in vielen Fällen sitzen die Verbreiter der Schädlinge nicht greifbar oder unerkant im Ausland.

#### 6.4.2 Haftung für die Weiterverbreitung über virenverseuchte Rechner

Einmal in die Online-Welt gesetzt, verbreitet sich ein Virus moderner Prägung vollkommen selbständig und nutzt dabei nicht nur das Unwissen vieler Nutzer, sondern vor allem auch die Schwächen der durch Windows geprägten Betriebssystem-Monokultur. Hauptquelle für die Verteilung von Viren sind damit in der Regel ahnungslose Nutzer von Privat- und Unternehmensrechnern, auf denen die Schädlinge ohne Wissen der Besitzer ihr Werk verrichten. Bislang hat sich die Rechtsprechung noch nicht mit der Frage nach einer Haftung für ein solches Verhalten befassen müssen.

Eine Strafbarkeit der Weiterverbreiter scheidet bereits mangels eines entsprechenden Vorsatzes aus. Doch auch wer fahrlässig handelt, also die „im Verkehr erforderliche Sorgfalt außer Acht lässt“, haftet zivilrechtlich unter bestimmten Umständen für dadurch von ihm verursachte Schäden. Ein Anspruch auf Schadensersatz kommt aber nur dann in Betracht, wenn für PC-Nutzer eine Verpflichtung besteht, Rechner und Netzwerke gegen die Verbreitung von Malware abzusichern. Anspruchsgrundlage wäre in diesem Fall der § 823 Abs. 1 BGB. Umstritten ist allerdings, aus welchen Vorschriften sich gegebenenfalls solche Verpflichtungen zur Gewährleistung der IT-Sicherheit, der Jurist spricht von so genannten „Verkehrssicherungspflichten“, ergeben könnten.<sup>26</sup>

Für Unternehmen finden sich eine Reihe von Vorschriften, die auch einen wirksamen Schutz gegen Viren, Trojaner & Co. vorsehen. Insbesondere das „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich“ (KonTraG), das praktisch alle größeren Firmen betrifft, verpflichtet Unternehmen unter anderem zu einem IT-Risikomanagement und zur Schaffung sicherer Netzwerkinfrastrukturen. Ähnlich weitgehende Verpflichtungen enthält auch § 109 des Telekommunikationsgesetzes (TKG). Darüber hinaus fordern vielfältige Vorschriften im Datenschutzbereich einen gesonderten Schutz rund um die Speicherung personenbezogener Daten.

Was genau ein Unternehmen gewährleisten muss, um diesen Ansprüchen zu genügen, ist letztlich eine Frage des Einzelfalles. Zumindest für größere Firmen dürfte es im Gegensatz zu einem kleinen Handwerksbetrieb mit drei Mitarbeitern kaum ausreichen, für einen stets aktualisierten Virenschutz und Firewalls zu sorgen. Vielmehr bedarf es in diesen Fällen auch organisatorischer Maßnahmen, um eine gut informierte EDV-Abteilung ebenso zu garantieren wie eine Instruktion der Mitarbeiter in Bezug auf die mit der Internetnutzung verbundenen Sicherheitsrisiken. Erfüllt allerdings ein Unternehmen diese Vorgaben, so entfällt mit dem Vorwurf der Fahrlässigkeit auch die Haftung für die Verbreitung virtueller Schädlinge. Ohnehin kann man niemandem einen rechtlichen Vorwurf hinsichtlich Viren oder Würmern machen, die erst neu in Umlauf gebracht werden und für die es unter Umständen noch keine Erkennung von Seiten der Antiviren-Anbieter gibt.

Anders sieht dagegen die rechtliche Lage bei Privatpersonen aus. Hier gibt es keine juristischen Vorschriften, die zur Einhaltung der Gebote der IT-Sicherheit verpflichten. So hat etwa der BGH in

---

<sup>26</sup> vgl. zu den Details: Koch, Haftung für die Weiterverbreitung von Viren durch E-Mails, NJW 2004, 801; Heidrich, Unwissenheit schützt vor Strafe nicht – Zur Haftung für die Verbreitung von Viren, Würmern und Trojanern, c't 19/2004, S. 168

einem Urteil aus März 2004 zu Mehrwertdienste-Dialern<sup>27</sup> (Az. III ZR 96/ 03) noch einmal ausdrücklich bestätigt, dass keine übermäßige technische Sorgfaltspflicht bei privaten Nutzern besteht. Daher ist für diese Gruppe allenfalls in Ausnahmefällen eine Haftung für die nicht vorsätzliche Verbreitung von Viren anzunehmen.

Aus dem Vergleich der IT-Sicherheitsanforderungen an Unternehmen auf der einen und Privatpersonen auf der anderen Seite ergibt sich ein erhebliches Erwartungsgefälle. Nimmt man für Firmen derartige, je nach Größe und Produktionsgebiet mehr oder weniger ausgeprägte Verpflichtungen an und für Endnutzer dagegen nicht, so ergibt sich daraus, dass ein Unternehmen für die Verbreitung von Viren, Würmern und Trojanern an Privatpersonen zivilrechtlich haftet. Angesichts des Ungleichgewichts gilt das im umgekehrten Verhältnis allerdings nicht. Noch schwieriger zu beurteilen ist die Rechtslage im Verhältnis von Unternehmen oder Nutzern untereinander. Da an beide Seiten die gleichen Anforderungen hinsichtlich der Schutzvorkehrungen zu stellen sind, dürfte eine Haftung beidseitig ausscheiden. Das ergibt sich daraus, dass der Empfänger im gleichen Maße wie der Absender zu Sicherungsvorkehrungen verpflichtet ist, die seinerseits eine Infektion verhindern müssen. Kommt er dem nicht nach, so trifft ihn eine entsprechendes Mitverschulden.

Allerdings gibt es auch hinsichtlich der Haftungsfragen für die Verbreitung von Malware über das Internet soweit ersichtlich noch keine gerichtlichen Entscheidungen.

### 6.4.3 Haftung der Provider

Die Access- und Mail-Provider haften grundsätzlich nicht für die Verbreitung von Viren. Diensteanbieter sind nach § 9 des Telediensteegesetzes (TDG) für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie die Übermittlung nicht veranlassen, den Adressaten der übermittelten Informationen nicht ausgewählt und die übermittelten Informationen nicht ausgewählt oder verändert haben.

Das gilt zumindest so lange, wie ihnen die Handlungen ihrer Kunden nicht bekannt sind, aber natürlich auf keinen Fall, wenn der Provider mit dem Nutzer gemeinsam handelt. Ungeklärt ist in diesem Zusammenhang noch die Frage, ob ein Zugangsdienstleister den Rechner eines Kunden vom Netz nehmen muss, sobald ihm bekannt ist, dass er als „Virenschleuder“ fungiert und Malware verbreitet. Diese Frage ist wohl zumindest ab Kenntnis des Providers zu bejahen. Eine entsprechende Handlungsgrundlage dürfte sich in jeder AGB eines Diensteanbieters finden. Auch zu diesem Bereich gibt es derzeit noch keinerlei Urteile.

### 6.4.4 Sind Bounces und Viren-Warnungen Spam?

Jede neue Viren-Epidemie belastet die Infrastruktur des Internet nicht nur durch die eigentliche Verbreitung der elektronische Schädlinge, sondern auch durch eine daraus resultierende Flut an meist völlig sinnlosen Virenwarnungen, die entsprechende Scanner automatisiert an die angeblichen Absender schicken. Für die Empfänger der Warnungen ist das höchst ärgerlich, sind sie in aller Regel doch nicht die Absender der monierten Viren-Mails, die oft mit aus Adressbüchern ausgelesenen Absenderangaben arbeiten.

Unter Umständen können solche Nachrichten wie auch *bounces* nach der oben genannten Definition als unerwünschte E-Mail-Werbung zu bewerten sein. Enthält die E-Mail lediglich einen kurzen Hinweis auf den angeblichen Viren-Befall, so passen die ausgeführten Kriterien sicherlich nicht. Wirbt die Nachricht dagegen massiv für ein Produkt des Versenders oder des Herstellers der

---

<sup>27</sup> BGH NJW 2004, 1590

Antivirus-Lösung, so kann man die E-Mails sehr wohl als rechtswidrigen Spam klassifizieren und dagegen vorgehen.

Ein Unternehmen, das trotz der angesichts von gefälschten Absenderadressen offensichtlichen Sinnlosigkeit weiter an derartigen Mitteilungen festhalten will, sollte die in den E-Mails enthaltenen Informationen also auf das notwendige Minimum beschränken und werbende Angaben in den Vorlagen entfernen.

## 6.5 Rechtliche Beurteilung von Filtermaßnahmen

Der Einsatz von Mailfiltern zum Aussortieren von Spam- und Viren-Mails ist inzwischen bei Privatpersonen ebenso wie bei Unternehmen, Behörden und Providern üblich. Viele Empfänger wären ohne derartige Sortiermechanismen kaum noch in der Lage, in der Mail-Flut im eigenen Posteingang relevante Dokumente zu erkennen. Die automatisierte Filterung von E-Mails bei Providern und im Betrieb ohne Kenntnis und Zustimmung der Empfänger kann jedoch rechtliche Probleme aufwerfen. Unter Umständen machen sich Mitarbeiter und Verantwortliche durch das Löschen von E-Mails sogar strafbar.

Diese Ansicht hat jüngst das OLG Karlsruhe bestätigt, das in einer Entscheidung das gezielte Filtern von E-Mail grundsätzlich als strafrechtlich relevant angesehen hat.<sup>28</sup> Ausgangslage der Entscheidung war die vorsätzliche Filterung von E-Mails sowohl von einem als auch an einen ehemaligen Mitarbeiter einer Universität.

### 6.5.1 Strafbarkeit nach § 206 StGB

Die juristische Diskussion über die Beurteilung von Mailfilterung steht noch weitgehend am Anfang.<sup>29</sup> Urteile zu diesem Bereich gibt es mit Ausnahme der genannten Entscheidung des OLG Karlsruhe nicht.

Weitgehende Einigkeit besteht jedoch darüber, dass E-Mails, ebenso wie Telefonate oder Faxe, dem Fernmeldegeheimnis unterliegen. Dieses erstreckt sich sowohl auf den Inhalt der Telekommunikation als auch auf ihre näheren Umstände und die daran Beteiligten. Demzufolge umfasst es jede Art der individuellen Nachrichtenübermittlung und damit auch die Kommunikation per E-Mail. Das Fernmeldegeheimnis schützt unter anderem § 206 des Strafgesetzbuches (StGB). Danach ist es Inhabern und Beschäftigten von Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen, verboten, ihnen zur Übermittlung anvertraute Sendungen unbefugt zu unterdrücken. Bis zu fünf Jahren Freiheitsstrafe oder eine Geldstrafe drohen bei einer Verletzung dieser Vorschrift.

#### **Verletzung des Post- oder Fernmeldegeheimnisses, § 206 StGB**

- (1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekannt geworden sind, das geschäftsmäßig Postoder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
- (2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt

<sup>28</sup> OLG Karlsruhe, Az 1 Ws 152/04; Beschluss vom 10. Januar 2005, vgl. dazu <http://www.heise.de/newsticker/meldung/55201>

<sup>29</sup> Vgl. dazu Heidrich/Tschoepe, Rechtsprobleme der E-Mail-Filterung, MMR 2004, S. 75; Hoeren, Virenscreening und Spamfilter, Rechtliche Möglichkeiten im Kampf gegen Viren, Spams & Co, NJW 2004, S. 3513; Spindler/Ernst, Vertragsgestaltung für den Einsatz von E-Mail-Filtern, CR 2004, 437

1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,
2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder
3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) Die Absätze 1 und 2 gelten auch für Personen, die

1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen,
2. von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder
3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

Voraussetzung für die Anwendung der Vorschrift ist zunächst das Erbringen eines „geschäftsmäßigen Telekommunikationsdienstes“. Darunter versteht das Telekommunikationsgesetz (TKG) ein „nachhaltiges Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte mit oder ohne Gewinnerzielungsabsicht“. Folglich ist weder eine Entgeltlichkeit noch ein gewerbliches Handeln erforderlich. Zum Kreis der Verpflichteten gehören daher neben Access- auch Internet-Service-Provider, die Mailedienste anbieten. Diese Voraussetzung wird aber auch von Unternehmen und Behörden erfüllt, die ihren Mitarbeitern einen Online-Zugang bereitstellen und die private Nutzung des Internet gestatten oder dies zumindest tolerieren. „Dritter“ im Sinne des § 206 StGB ist in diesen Fällen der Mitarbeiter. Nach der Entscheidung des OLG Karlsruhe fallen auch Hochschulen unter diese Vorschrift. Diese genehmigten nicht nur den Mitarbeitern und Studenten die zumindest auch private Nutzung der Mailaccounts, sondern handelten durch zunehmend engere Kontakte zwischen den Bildungseinrichtungen und Unternehmen zunehmend auch im wirtschaftlichen Bereich.

Keine Dienste für Dritte erbringen dagegen solche Unternehmen und Betriebe, die eine private Nutzung verboten haben. Diese unterfallen folglich auch nicht dem Anwendungsbereich des § 206 StGB. Möglich ist jedoch auch in diesen Fällen eine Strafbarkeit nach § 303a StGB, wie nachstehend dargelegt.

Weiterhin muss die E-Mail dem übermittelnden Server „zur Übermittlung anvertraut“ sein. Nach Ansicht des OLG Karlsruhe ist dies zumindest dann eindeutig der Fall, wenn die Anfrage zur Übermittlung von Daten den Mailserver des Unternehmens erreicht hat und der versendende Rechner die Daten dem empfangenden Server übermittelt hat. In dem zu beurteilenden Sachverhalt wurden die E-Mails ordnungsgemäß vom Mailserver der Fakultät „angenommen und quittiert“ und erst dann fakultätsintern ausgefiltert.

Die Sichtweise des OLG entspricht der technischen Betrachtung der Problematik. Danach liegt ein Wechsel der Verantwortung für den Mail-Transport vor, sobald der empfangende Server dem Absender-Client den Erhalt der E-Mail bestätigt, damit also im Rahmen des *Simple Mail Transfer Protocol* am Ende der so genannten DATA-Phase nach Übertragung der Kopfzeilen (*header*) und des eigentlichen Inhalts der E-Mail (*body*).<sup>30</sup> Es scheint folgerichtig, sich in der juristischen Beurteilung dieser Frage der technischen Sichtweise anzuschließen.

Die folgerichtige Beschränkung des Tatbestandsmerkmals „zur Übertragung anvertraut“ des § 206 Abs. 2 Nr. 2 StGB auf den Zeitpunkt nach der vollständigen Übertragung der Nachricht, technisch

---

<sup>30</sup> Zum genauen technischen Ablauf bei dem Eingang einer E-Mail siehe Kapitel 4.1

also nach Ende der DATA-Phase, hat zur Folge, dass eine ganze Reihe praxisrelevanter Filtermaßnahmen, die schon vor diesem Zeitpunkt ansetzen, strafrechtlich nicht relevant sind. Gerade im Bereich der Filterung von E-Mail-Werbung ist eine Blockierung von Nachrichten bereits vor Übertragung der Inhalte üblich, da dadurch ein erheblicher Aufwand auf Empfängerseite vermieden werden kann. So basiert beispielsweise die Filterung auf Basis so genannter Blacklists darauf, dass eingehende E-Mails bereits anhand der IP-Adresse oder der Mailadresse des Absenders abgelehnt werden, ohne dass es zu einer Übertragung von *header* oder *body* der Nachricht kommt.

Die Tatsache, dass eine derartige Filterung nicht unter den Straftatbestand des § 206 StGB fällt, stellt allerdings keinen „Freibrief“ zum Blockieren von E-Mails ohne Zustimmung der Empfänger dar. Zumindest bei Providern kann sich allerdings eine Verpflichtung der Zustellung auch derartiger E-Mails aus dem Vertragsverhältnis zu dem betroffenen Kunden ergeben.<sup>31</sup> Eine ähnliche Verpflichtung wird auch bei Mitarbeitern anzunehmen sein, denen die Privatnutzung von E-Mail am Arbeitsplatz erlaubt ist. Ein „Unterdrücken“ der E-Mails ist schließlich dann anzunehmen, wenn Eingriffe in den technischen Vorgang des Aussendens, Übermittels oder Empfangens von Nachrichten mittels Telekommunikationsanlagen verhindern, dass die Nachricht ihr Ziel vollständig und ohne Änderungen erreicht. Dieses Tatbestandsmerkmal wird sowohl durch das Blockieren der E-Mails als auch durch ihre Filterung verwirklicht. Im ersten Fall wird bereits das Empfangen der Nachricht unterbunden, während im zweiten Fall die Weiterleitung, also das Übermitteln, der eingehenden E-Mail vom empfangenden Mailserver an den einzelnen Anwender nicht stattfindet. In jeder Alternative ist daher ein Unterdrücken der E-Mail anzunehmen.

Da diese Maßnahmen auch vorsätzlich, also mit Wissen und Wollen der jeweils Befugten geschehen, ist der Tatbestand des § 206 StGB durch die Filterung von E-Mail unter den genannten Voraussetzungen regelmäßig erfüllt. Darüber hinaus sind ungeachtet der strafrechtlichen Bewertung Provider und solche Unternehmen und Behörden, die eine Privatnutzung von E-Mail erlauben, auch auf zivilrechtlicher Basis zu einer Weiterleitung der eingehenden Nachrichten an den Nutzer verpflichtet.

### 6.5.2 Strafbarkeit nach § 303a StGB

Neben einer Strafbarkeit nach § 206 Abs. 2 Nr. 2 StGB kommt durch die Filterung von Spam- und Viren-Mails ohne vorherige Einwilligung auch eine Verletzung des § 303a StGB in Betracht. Der Tatbestand setzt voraus, dass rechtswidrig Daten gelöscht oder unterdrückt werden. Anders als der zuvor behandelte § 206 StGB schützt § 303a StGB das Interesse des Verfügungsberechtigten an der unversehrten Verwendbarkeit der gespeicherten Daten. Eine Einschränkung auf Unternehmen, die geschäftsmäßig Postoder Telekommunikationsdienste erbringen, gibt es nicht. Daher ist § 303a StGB uneingeschränkt auf alle Provider, Unternehmen und Behörden anwendbar.

#### Datenveränderung, § 303a StGB

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

Unter Daten versteht man Inhalte, die „elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden“, also auch E-Mails. Die Daten brauchen mangels einer entsprechenden Eingrenzung in der Vorschrift nicht fremd zu sein. Dennoch ist der Tatbestand auf solche Daten beschränkt, an denen und an deren Unversehrtheit ein Dritter ein unmittelbares Interesse besitzt oder besitzen könnte. Ein potentiell Interesse des Empfängers auch bei Spam-Mails ist grundsätzlich angesichts der auch subjektiven Bewertung von Werbemails nicht auszuschließen. Grundsätzlich müssen die Provider und Arbeitgeber bei allen E-Mails zunächst davon

<sup>31</sup> Vgl. dazu Hoeren, Virens scanning und Spamfilter, Rechtliche Möglichkeiten im Kampf gegen Viren, Spams & Co, NJW 2004, S. 3513, 3515

ausgehen, dass ihre Kunden oder Arbeitnehmer jede an sie adressierte E-Mail auch erhalten oder es sich selbst vorbehalten wollen, die Nachricht als Spam zu löschen. Eine Ausnahme ist hier allenfalls bei den noch zu behandelnden Fällen von Viren-infizierten E-Mails anzunehmen.

Werden E-Mails also vorsätzlich gelöscht oder entsprechend der oberen Darstellung unterdrückt, so ist regelmäßig auch der Straftatbestand des § 303a StGB bereits erfüllt. Die ungenehmigte Filterung von E-Mails wird also auch durch diese Vorschrift erfasst.

### 6.5.3 Filterung ausgehender Mail

Auch das *egress filtering*, also das Filtern der ausgehenden Mail, verstößt unter den oben genannten Voraussetzungen gegen die § 206 und § 303a StGB. Das hat inzwischen auch das OLG Karlsruhe in der oben genannten Entscheidung bestätigt, die ausdrücklich auch die Filterung ausgehender E-Mails grundsätzlich als strafrechtlich relevant ansieht.

Unzweifelhaft ist eine ausgesandte E-Mail dem jeweiligen Provider anvertraut. Ihre Löschung ohne Kenntnis und Zustimmung des Versenders erfüllt damit den Tatbestand der Verletzung des Fernmeldegeheimnisses nach § 206 Abs. 2 StGB bei Providern und solchen Unternehmen oder Behörden, die eine Privatnutzung elektronischer Nachrichten am Arbeitsplatz erlauben. Ohne diese Einschränkung verstößt das selbstbestimmte *egress filtering* auch gegen § 303a StGB, da in rechtswidriger Weise fremde Daten gelöscht werden.

### 6.5.4 Tipps für rechtskonforme Mailfilterung

Allein das Vorliegen der Tatbestandsmerkmale sagt juristisch allerdings noch nichts darüber aus, ob letztlich auch eine Strafbarkeit vorliegt.

So schließt das Einverständnis des Empfängers in die Filtermaßnahmen bereits die Tatbestandsmäßigkeit der §§ 206 und 303a StGB und damit auch die Strafbarkeit aus. Äußert der Empfänger seine Zustimmung zum Löschen der Mails, so wird das Vertrauen der Allgemeinheit in die Wahrung des Post- und Fernmeldegeheimnisses nicht mehr berührt. Dieses Einverständnis muss allerdings ausdrücklich und insbesondere vor Beginn der Filterung von allen Betroffenen erteilt werden.

Eine mutmaßliche Einwilligung der Empfänger ist zumindest bei Spam nicht anzunehmen. Grundsätzlich darf und muss jeder Kunde damit rechnen, dass die an ihn adressierten Sendungen ohne eigenmächtige Handlungen des Vermittlers an ihn zugestellt werden und eine von ihm versandte E-Mail auch den Adressaten erreicht. Dies gilt insbesondere auch aufgrund der Tatsache, dass die Beurteilung einer E-Mail als „Spam“ aus der Perspektive des Empfängers eine subjektive Angelegenheit ist. Was für den einen unerwünschter Werbe-Müll ist, ist für den anderen eine wertvolle Information. Es ist bei persönlich adressierten E-Mails nicht Sache des Providers oder Arbeitgebers, zu beurteilen, wann was der Fall ist. In der Regel wird der auch gar nicht beurteilen können, ob zum Beispiel ein Newsletter dem Empfänger gewollt oder ungefragt zugeht.

Daher bleibt den Anbietern in juristischer Hinsicht nur der Weg, im Vorfeld von den Nutzern die ausdrückliche Zustimmung zur Spamfilterung sowohl beim Empfang als auch bei der Versendung einzuholen. Bei Providern empfiehlt sich dies durch Aufnahme entsprechender Klauseln in ihre allgemeinen Geschäftsbedingungen, denen jeder Kunde bei Vertragsbeginn zustimmen muss. Alternativ dazu bietet sich ein durch den User konfigurierbares Menü zur Spamfilterung an, das der Nutzer selbst aktivieren muss.

Das Gleiche gilt im Prinzip für Unternehmen und Behörden. Juristisch unbedenklich ist eine Filterung im betrieblichen Bereich nur, wenn zuvor eine Betriebsvereinbarung abgeschlossen wurde, die die Löschung von E-Mails ausdrücklich vorsieht. Derartige Regelungen empfehlen sich ohnehin für jedes Unternehmen, um eine klare und für alle Seiten transparente Nutzung der elektronischen Medien am Arbeitsplatz zu ermöglichen. Zu beachten ist allerdings, dass die Zustimmung des

Betriebsrats gemäß § 87 des Betriebsverfassungsgesetzes (BetrVG) zu der Einrichtung der Filter erforderlich ist, da sie potentiell zur Überwachung der Mitarbeiter geeignet sind. Alternativ zu einer Betriebsvereinbarung kann von jedem Mitarbeiter individuell die Zustimmung eingeholt oder diesem die volle Konfiguration des Filters übertragen werden. Behörden sollten entsprechende klare Dienstanweisungen zur Nutzung von E-Mail und Internet vorgeben.

Ebenfalls unbedenklich sowohl im betrieblichen Einsatz als auch bei Providern ist die Quarantänelösung, bei der als Spam erkannte E-Mails nicht gelöscht, sondern in separate Eingangsordner verschoben werden. In diesem Falle ist auch keine Einwilligung des Empfängers erforderlich.

### 6.5.5 Reaktionsmöglichkeiten im Notfallbetrieb

Besonderheiten kann es allerdings in diesem Bereich im so genannten „Notfallbetrieb“ geben. Während der Dauer eines Angriffes auf die IT-Infrastruktur eines Providers, Unternehmens oder einer Behörde, etwa durch ein Mail-Bombing oder eine DDoS-Attacke, können sich erweiterte Befugnisse der Betroffenen ergeben.

So kann es in derartigen Fällen ausnahmsweise auch zulässig sein, eindeutig als Spam erkannte Nachrichten schon vor Zustellung auch ohne Zustimmung des Betroffenen zu filtern oder die Zustellung zu verzögern, um die Funktionsfähigkeit des gesamten Netzwerkes zu bewahren. In diesen Fällen überwiegt eindeutig das Sicherheitsinteresse des Betreibers das des Empfängers der E-Mail. Eine entsprechende gesetzliche Grundlage für ein solches Handeln „im Notfallbetrieb“ kann sich etwa aus § 109 TKG sowie aus anderen Rechtfertigungsgründen ableiten lassen.

Wie weit die Befugnisse reichen, bleibt jedoch immer eine Frage des Einzelfalles und ist abhängig insbesondere von der Intensität des Angriffs. So kann es bei besonders heftigen Attacken sogar erlaubt sein, die Zustellung von E-Mail gänzlich zu stoppen. Andererseits rechtfertigen geringfügige Beeinträchtigungen solche Maßnahmen kaum.

### 6.5.6 Besonderheiten bei der Filterung auf Malware

Grundsätzlich erfüllt auch das Löschen von virenbehafteten E-Mails ohne Zustimmung des Empfängers die Tatbestände der §§ 206 Abs. 2 und 303a StGB. Eine Strafbarkeit dürfte dagegen nur in ganz wenigen Ausnahmefällen anzunehmen sein, da in diesem Fall diverse Rechtfertigungsgründe zugunsten des Filternden greifen. Das gilt sowohl für eine Filterung bei ankommenden als auch im Rahmen des *egress filtering* bei abgehenden E-Mails. Auch das OLG Karlsruhe geht in seiner bereits genannten Entscheidung zur Spamfilterung davon aus, dass bei der Abwehr drohender Virenangriffe ein solcher Rechtfertigungsgrund anzunehmen ist.

So verpflichten etwa § 109 und andere Vorschriften des Telekommunikationsgesetzes (TKG) die Betreiber von Telekommunikationsanlagen zum Ergreifen von Schutzmaßnahmen für ihre Anlagen gegen unerlaubte Zugriffe. Derartige Störungen können unzweifelhaft aus Viren oder Würmern entstehen, die sich per E-Mail verbreiten. Ob dies allerdings auch für Werbemails gilt, erscheint angesichts der klar formulierten Schutzziele des § 109 TKG und der hieraus resultierenden Pflichten, die wegen des mit ihnen verbundenen Eingriffs in das Fernmeldegeheimnis eng auszulegen sind, zweifelhaft.

Daher ist das automatisierte Scannen von E-Mails auf Viren und Trojaner sowie deren Entfernung rechtlich grundsätzlich unbedenklich. Selbstverständlich ist dabei aber sicherzustellen, dass es nicht zu „Kollateralschäden“ kommt, also nur solche E-Mails aussortiert werden, die elektronische Schädlinge enthalten.

## 6.6 Zulässiges E-Mail-Marketing

Ungeachtet der Spam-Problematik gehört der Versand von E-Mail-Newslettern an eigene Kunden oder interessierte Käufer zweifellos zu den wirksamsten Mitteln des Marketings. Wer seinen Geschäftspartnern darin interessante Informationen bietet und sie über Neuigkeiten im Unternehmen informiert, erhält und stärkt die Kundenbindung zu einem unvergleichlich günstigen Preis. Um die enorme Rufschädigung ebenso wie die potentiellen juristischen Folgen eines Spam-Verdachts zu vermeiden, gilt es einige rechtliche Spielregeln zu beachten.

Der Versand von Werbemails ist insbesondere hinsichtlich der Auswahl der Angesprochenen und der Herkunft der Adressen eine sensible Angelegenheit. Eindeutig zulässig ist diese Art der Werbung auf Basis des geltenden Opt-In-Modells nur in den Fällen, in denen der Empfänger in die Übersendung ausdrücklich eingewilligt hat, sich also zum Beispiel explizit für einen Newsletter angemeldet hat. Darüber hinaus regelt § 7 Abs. 3 UWG den Fall, dass der Werbende eine Mailadresse im Zusammenhang mit dem Kauf einer Ware oder Dienstleistung erhalten hat. Nutzt er sie ohne einen vorherigen Widerspruch durch den Kunden im Rahmen von Direktmarketing für ähnliche Angebote, so ist die Werbesendung rechtmäßig, sofern der Betroffene „bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen“. Eine Unterscheidung zwischen gewerblich tätigen und privaten Empfängern sieht diese Vorschrift nicht vor.

Da die Einwilligung des Empfängers im Regelfall Voraussetzung für das Zusenden von Werbemails ist, verbietet sich schon aus diesem Grund die Nutzung von gekauften Adressen, die häufig aus dubiosen Quellen stammen und in aller Regel gegen den Willen der E-Mail-Benutzer gesammelt wurden. Die „sauberste“ Methode ist es ohnehin, nur diejenigen in den Verteiler aufzunehmen, der den Newsletter tatsächlich angefordert hat. Bei der Anmeldeprozedur sind ebenfalls datenschutzrechtliche Grundsätze zu beachten. So muss der Empfänger über die Speicherung seiner Daten aufgeklärt werden und die Erlaubnis dazu sowie zum Versand der E-Mails an ihn ausdrücklich bestätigen. Zu diesem Zweck empfiehlt es sich, eine Checkbox einzubauen, durch deren Aktivierung der Interessent dies bekräftigt.

Im Rahmen des Opt-In-Verfahrens sollte der Nutzer seine Anmeldung noch einmal ausdrücklich bestätigen. Üblicherweise geschieht das durch den Versand einer E-Mail an die angegebene Adresse, die der Empfänger durch ein Reply oder die Aktivierung eines Links bestätigen muss, das so genannte „*double-opt-in*“ oder „*verified opt-in*“. Der Grund für die doppelte Absicherung liegt in der Tatsache, dass die erste Bestellung nicht eindeutig einer Person zugeordnet werden kann, da ein beliebiger Dritter problemlos fremde Mailadressen eintragen kann. Dieses Verfahren wird allerdings von den Vertretern des Direktmarketings häufig als zu umständlich abgelehnt. Fakt ist, dass auf diesem Wege häufig nicht nur die weniger motivierten Interessenten auf der Strecke bleiben, sondern oft auch solche, die den gesamten Opt-In-Prozess nicht verstehen und daher nicht auf die Bestätigungs-Mail antworten.

Als Mittelweg hat sich daher bei vielen Versendern das so genannte „*confirmed opt-in*“ durchgesetzt. Dabei erhält der Newsletter-Abonnent vor dem Zusenden des ersten Newsletters eine schriftliche Bestätigung des Abonnements mit einer sofortigen Kündigungsmöglichkeit.<sup>32</sup> Diese vermeintlich einfache Prozedur hat jedoch aus juristischer Sicht entscheidende Nachteile. Im Streitfall trägt nämlich nach der Rechtsprechung der Versender der Werbemail die Beweislast dafür, dass ein Interessent sich tatsächlich bei ihm angemeldet hat. Diesen Nachweis wird er im Rahmen des *confirmed opt-in* kaum führen können. Insbesondere kann ein Schweigen des Empfängers auf die versandte Bestätigungs-Mail rechtlich kaum als Einwilligung in die Übersendung zukünftiger Werbenachrichten interpretiert werden. Um derartigem Beweisnotstand vorzubeugen, empfiehlt sich

<sup>32</sup> Diese Definition von „*confirmed opt-in*“ ist in Deutschland üblich, manchmal wird „*confirmed opt-in*“ aber auch mit „*double-opt-in*“ gleichgesetzt.

zumindest aus juristischer Sicht der Prozess des *double-opt-in*. Auch sollte die Aktivierungs-Mail allenfalls eine Kurzvorstellung der angebotenen Inhalte beinhalten, im Übrigen aber auf Werbung verzichten. Ebenfalls in jeder E-Mail sollte die Möglichkeit zum Abbestellen der Sendungen, etwa durch Aktivierung eines Links, vorhanden sein. Seriöse Geschäftsleute versehen ihre E-Mails überdies mit einer Anbieterkennzeichnung und nennen Ansprechpartner für den Fall des Missbrauchs.

Schließlich steht und fällt der Erfolg eines Newsletters mit den dort angebotenen Inhalten. Wer seinen Kunden neben Informationen über die eigenen Produkte einen Mehrwert bietet, sichert den Erfolg seiner Mailing-Aktionen. Er muss jedoch dafür sorgen, dass die dort publizierten Beiträge urheberrechtlich unbedenklich sind. Oft finden sich beispielsweise in solchen Nachrichten von anderen Websites übernommene Ticker-Meldungen oder sonstige Beiträge. Das ist ein eindeutiger Verstoß gegen das Urheberrechtsgesetz (UrhG) und kann den Versender teuer zu stehen kommen. Wer also keine eigenen Artikel anzubieten hat, sollte fremde Beiträge nur mit eindeutiger Zustimmung des Verfassers oder mit einer entsprechenden Lizenz verwenden.

### **Zehn Regeln für gesetzeskonformes und akzeptables E-Mail-Marketing**

1. Nur explizit selbst angeforderte oder gestattete Werbung
2. Nur vom Empfänger gestattete oder angeforderte Inhalte in den Newslettern
3. Die Häufigkeit der Aussendungen ist dem Empfänger bekannt oder wird von ihm vorgegeben
4. Anmeldung über Web-Frontend oder E-Mail nur per „double opt-in“
5. Verwendung von Adressen nur zum angegebenen Zweck
6. Empfänger können sich selbst vom Verteiler streichen
7. Kündigungsmöglichkeit in jeder E-Mail
8. Keine Adressweitergabe ohne Zustimmung
9. Erläuterung des Umgangs mit personenbezogenen Daten durch verständliche Privacy Policy
10. Führen einer internen „Blacklist“ mit Adressaten, die keinen weiteren Kontakt wünschen

## 7 Vermeiden von Spam

Spam bekommt nur derjenige, dessen Adresse der Spammer kennt – so einfach es klingt, so schwierig ist es, genau das zu verhindern. Schließlich können Mailadressen ihrer Bestimmung, der freien Kommunikation im Internet, nur dienen, wenn man sie nicht versteckt. So liegt es in der Natur der Sache, dass Spam praktisch alle existierenden Mailadressen irgendwann einmal trifft. Damit das möglichst spät und möglichst selten geschieht, können die Empfänger jedoch einige Vorsorgemaßnahmen treffen, die im Folgenden beschrieben sind.

Neben den vielfältigen Antispam-Maßnahmen darf keinesfalls in Vergessenheit geraten, dass viele E-Mails erwünscht sind und heutzutage durch diverse Filter hinweg zum Adressaten gelangen müssen. Die Vorsorge sollte daher auch dem Hauptzweck des Mediums E-Mail gelten: der erwünschten Kommunikation zwischen den Anwendern.

### 7.1 Sichere Konfiguration eigener Systeme

Den meisten Spam verteilen heute Systeme, die einem Virus oder Wurm zum Opfer gefallen sind. Ein ungesicherter Rechner „überlebt“ im Internet nur Minuten, bis er angegriffen und gecrackt wird.

Die wichtigste präventive Maßnahme gegen Spam ist es daher, eigene Rechner zu schützen und sämtliche Software (Systemsoftware, Anwendungen, Virentfilter, Firewalls, ...) laufend auf dem neuesten Stand zu halten [GSHB04].

#### 7.1.1 Mailserver

Früher waren Mailserver oft so konfiguriert, dass sie E-Mail von jedem beliebigen Absender im Internet an jeden beliebigen Empfänger im Internet weiterleiteten (*open relay*). Heute gibt es keinen Grund mehr, ein solches offenes Relay zu betreiben. Kein Mailserver sollte E-Mails von Fremden annehmen, die nicht für die eigene Domain bestimmt sind. Arbeitet der Mailserver auch als MSA (Mail Submission Agent), nimmt er also E-Mail von eigenen Mitarbeitern oder Kunden an und leitet sie ins Internet weiter, muss er in jedem Fall prüfen, ob die Weiterleitung erlaubt ist. Dazu kann er die IP-Adresse des Absenders ( z. B. in lokalen Netzen) heranziehen oder SMTP AUTH [RFC2554] verwenden (siehe Kapitel 4.2.2).

Ein komplexes Mailsystem gegen Relaying abzusichern ist nicht einfach. Nach jeder Konfigurationsänderung sollte der Administrator das eigene System erneut daraufhin abklopfen, zum Beispiel mit dem öffentlichen Relay-Tester unter <http://www.abuse.net/relay.html>.<sup>1</sup>

Sein besonderes Augenmerk sollte dabei so genannten Multi-Hop-Relays gelten. Mailsysteme bestehen häufig aus mehreren Rechnern, die sich gegenseitig vertrauen. Bei einer Fehlkonfiguration kann es passieren, dass zwar jeder Rechner für sich sicher konfiguriert ist, sie zusammen jedoch als Relay fungieren.

---

<sup>1</sup> Es gibt auch eine Telnet-Variante für Tests vom eigenen Mailserver aus: „telnet relay-test.mail-abuse.org“.

### 7.1.2 HTTP(S) und SOCKS-Proxies

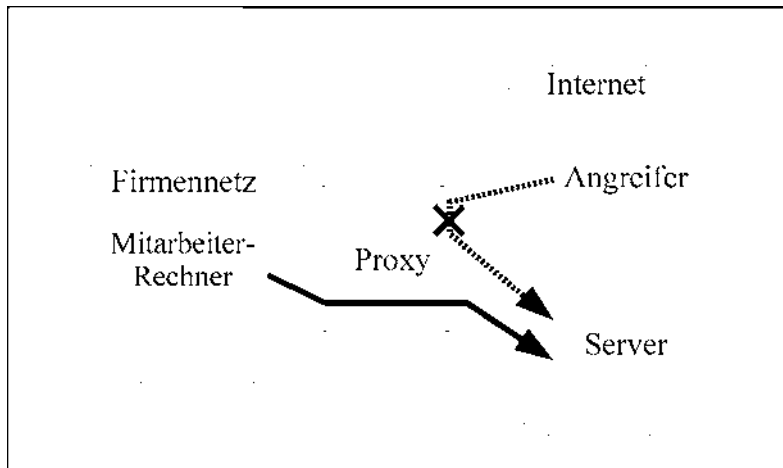


Abb. 7.1: Proxies dürfen keine unauthentifizierten Verbindungen schaffen.

Oft ist der Zugang ins Internet oder zu einzelnen Diensten im Internet aus Firmen- oder anderen lokalen Netzen heraus nicht direkt möglich, etwa weil Firewalls eingesetzt werden. HTTP(S)- und SOCKS-Proxies<sup>2</sup> [RFC1928] dienen dazu, solche Restriktionen im Netz zu umgehen. Sie sollten grundsätzlich so konfiguriert sein, dass sie nicht allgemein nutzbar sind (*open proxy*), sondern nur aus dem lokalen Netz oder nach einer Authentifizierung, damit ein Angreifer sie nicht ausnutzen kann. Eine Verbindung zum SMTP-Port sollten die Proxies grundsätzlich nicht zulassen. Der Administrator sollte den Netzverkehr überwachen und bei ungewöhnlicher Aktivität eingreifen.

Während SOCKS-Proxies generell Verbindungen an beliebige Ports weiterleiten, dienen HTTP-Proxies in erster Linie der Weiterleitung von HTTP-Anfragen, also zur Nutzung des World Wide Web. Da viele HTTP-Proxies aber auch Verbindungen zu beliebigen Ports herstellen können (z. B. mit der CONNECT-Methode, siehe [RFC2616] Abschnitt 9.9), können sie unter Umständen auch zum Versand von E-Mails missbraucht werden.

### 7.1.3 Formmail-Skripte

Viele Webseitenbetreiber bieten auf ihren Webseiten Formulare an, mit denen man E-Mails versenden kann (siehe auch Kapitel 4.2.4). In vielen Fällen sind sie nur dazu gedacht, an wenige definierte Adressen E-Mails zu versenden („Ihre Nachricht an uns“). Leider beschränken aber viele der dahinterliegenden so genannten Formmail-Skripte den Versand nicht auf konfigurierte Adressen. Stattdessen kann sie der Spammer nutzen, um E-Mails an beliebige Adressen zu versenden. Eine Festlegung der Mailadresse in einem Hidden-Feld im Webformular reicht zur Sicherung nicht aus. Die Adressen müssen stattdessen im Skript oder seiner Konfiguration festgelegt und vor dem Versand überprüft werden.

Besonders anfällig sind Webserver, die E-Mails an beliebige Adressen schicken können („Schicken Sie eine Web-Postkarte“). Hier ist zwar häufig der Inhalt der E-Mail festgelegt, aber dennoch gibt es manchmal die Möglichkeit für einen Angreifer, die Festlegung zu umgehen. In jedem Fall sollte man die Benutzung solcher Skripte überwachen, um bei einem Missbrauch schnell eingreifen zu können.

Hiermit nicht zu verwechseln sind mailto:-Links im HTML-Dokument, da die E-Mail in diesem Fall durch den lokalen Mailclient des Anwenders versandt wird und nicht durch den Webserver.

<sup>2</sup> <http://www.socks.permeo.com/>

## 7.2 Umgang mit Mailadressen

Für den Versand von E-Mails benötigen Spammer umfangreiche Listen gültiger Empfängeradressen, an die sie auf den in Kapitel 4.3 genannten Wegen gelangen. Mit präventiven Maßnahmen können die potenziellen Opfer versuchen, den Spam-Versendern die eigene Mailadresse vorzuenthalten. Neben der ausschließlich nicht-öffentlichen Verwendung sowie der Verschleierung von Mailadressen auf Webseiten und in News-Beiträgen zählt der häufige Adresswechsel – bis hin zur Verwendung von Einmaladressen (auch „Wegwerfadressen“ genannt) – zu den häufig genannten Vorschlägen.

Leider haben einige der denkbaren Gegenmaßnahmen schwer wiegende Nachteile, insbesondere erschweren sie die Kommunikation mit erwünschten Partnern. Darüber hinaus gibt es Wege, an Empfängeradressen zu gelangen, die deren Besitzer gar nicht beeinflussen können. In allen Fällen ist daher zu berücksichtigen, dass sich das Spamproblem durch Prävention höchstens mildern, aber nicht beheben lässt.

### Niemals auf Spam antworten

Es versteht sich von selbst, dass Spammer Adressen, die zu einer Reaktion der Empfänger führen, als besonders wertvoll erachten, da diese Empfänger offenbar Spam lesen und sogar bereit sind, sich aktiv damit zu befassen. Wer also Links in Spam-Mails anklickt, die etwa zum beworbenen Inhalt oder vermeintlich zu einer Austragung der eigenen Adresse führen, muss mit einem Anstieg des Spamvolumens rechnen. Insbesondere Spams, deren Absender ganz offensichtlich jenseits der Legalität operieren, indem sie zum Beispiel Header-Informationen frei erfinden und Absenderadressen Dritter missbrauchen, sind daher konsequent zu ignorieren. Dadurch schützt man sich auch vor Malware, die sich häufig auf den beworbenen Webseiten verbirgt und den eigenen Rechner infizieren kann.

Etwas anders verhält es sich bei unerwartet eingehenden Newslettern von an sich offenbar seriösen Organisationen. Eine einfache Antwort an die Absenderadresse oder ein Klick auf den Unsubscribe-Link sollte genügen, das Missverständnis zu klären und die Empfängeradresse vom Verteiler zu nehmen – allerdings nur, wenn die E-Mail authentisch und nicht gefälscht ist (*phishing*). Die Kontaktaufnahme mit dem Absender oder dessen Provider wegen einer Beschwerde empfiehlt sich daher nur erfahrenen Anwendern. Im Zweifelsfall ist der eigene Postmaster die erste Anlaufstelle.

Manche Antispam-Systeme bieten auch eine so genannte Auto-Whitelist, auf die alle Empfängeradressen aus eigenen E-Mails gesetzt werden. Wer auf Spam antwortet, setzt damit die Mailadresse des Spammers automatisch auf die Whitelist – nicht gerade erstrebenswert.

Da Spammer auch Web-Bugs und andere per HTTP nachladbare Inhalte (siehe Kapitel 4.3.4) in ihren E-Mails einsetzen, um eine (automatische) Rückmeldung über gelesenen Spam zu bekommen, sollten E-Mail-Clients immer so eingestellt sein, dass sie bei der Anzeige von HTML-Mails keine externen Inhalte wie Bilder und Stylesheets laden.

### 7.2.1 Auswahl der eigenen Mailadresse

Schon die bloße Beschaffenheit der eigenen Mailadresse hat großen Einfluss darauf, ob und wie schnell sie sich in Spammerkreisen verbreitet, denn häufig lassen sich Adressen durch einfaches Durchprobieren aller möglichen Zeichenkombinationen erraten. Erst ab einer gewissen Mindestlänge der Mailadresse (genauer des *local-part*) schiebt die Kombinatorik den Spammern einen Riegel vor. Erfahrungsgemäß genügen acht Zeichen lange Zeichenketten zum Schutz vor *brute force attacks* auf die Adresse. Die so gebildeten *local-parts* sollten allerdings nicht in Wörterbüchern vorkommen, damit sie Schutz vor Wörterbuchangriffen (*dictionary attacks*, siehe Kapitel 4.3.3) bieten. Ein *local-part* wie *mmusterm* lässt sich durch Ausprobieren praktisch nicht herausfinden, während *mi chael*

.mustermann deutlich mehr Spam auf sich zieht, sofern Vor- und Nachname in öffentlich zugänglichen Verzeichnissen zur Verfügung stehen. Der Punkt zwischen Vor- und Nachnamen ist ein gängiges Trennzeichen, das Spammer beim Durchprobieren von Adressen berücksichtigen und das daher keinen Schutz bietet.

Vorsicht ist jedoch vor allzu ungewöhnlichen Zeichenketten geboten. Wer zum Beispiel Ziffern oder willkürliche Kombinationen wie asdfg in seine Adresse einbaut, könnte bei vielen Spamfiltern selbst in Verdacht geraten, da derlei häufig in Spams vorkommt.

Exotische Zeichen, etwa ein + oder gar ein @ im *local-part* können Absender vor eine unnötig hohe Hürde stellen, da viele MUAs sich nicht ganz standardkonform verhalten und sich in solchen Fällen gelegentlich weigern, E-Mails an die entsprechenden Empfänger zu versenden.

Andererseits lassen sich auf diese Weise Adressen einrichten, die auch Spam-Werkzeuge offenbar überfordern. Ein Test mit dem *local-part* pl ease+remove während der Arbeiten an dieser Studie führte zwar zu viel Spam an remove, aber zu keiner einzigen unerwünschten E-Mail an die vollständige Adresse. Offenbar hatten die Spammer das pl ease+ als nicht zur Adresse gehörend verworfen.

### Namen in Mailadressen und der Datenschutz

Im Vergleich etwa mit einer Rufnummer geben Internet-Anwender mit ihren Mailadressen mehr Informationen über sich preis, häufig ihren Namen und den der Firma, in der sie arbeiten. Mailadressen sind häufig sehr lange gültig, vielleicht sogar ein ganzes Leben lang. Bei der Vergabe der Mailadressen sollte man sich überlegen, ob man im Sinne des Datenschutzes und der Datensparsamkeit Adressen mit seinem vollen Namen verwenden möchte. Manch einer, der solche Adressen verwendet, hat sich schon über Spam mit einer persönlichen Anrede gewundert.

## 7.2.2 Verschleiern und Geheimhalten der Adresse

Auf den eigenen Webseiten lassen sich die Mailadressen relativ bequem mittels HTML-Tricks oder Javascript verschleiern, um Spammern deren Auffinden zu erschweren. Nicht empfehlenswert sind dagegen Texte oder gar Bilddateien ohne jeden Link, da sie die Benutzung der Webseiten unnötig verkomplizieren und nicht den anerkannten Richtlinien zur Barrierefreiheit<sup>3</sup> entsprechen. Ebenfalls fragwürdig ist das absichtliche Unbrauchbarmachen von Mailadressen, etwa in Form von ci ndy-at-company-dot-com oder mi chael .mustermann@fi rma.nospam.de. (Die Domain nospam.de ist eine ganz normale Domain, die dem Besitzer viel „fehlgeleiteten“ Spam einbringt.) Potenzielle Versender einer E-Mail müssen in solchen Fällen erraten, welche funktionierende Mailadresse sich hinter derlei Konstrukten verbergen mag. Nicht wenige verweigern einfach die Benutzung solcher Adressen – eine nahe liegende Reaktion. Interessanterweise führte ein Test mit dem *local-part* spamtest sowohl zu Spam an genau diese Adresse als auch an test – ein deutlicher Hinweis darauf, dass Spammer solch einfachen Verschleierungen mit eigenen Filtern begegnen.<sup>4</sup>

### Verschleiern der Mailadresse auf Webseiten

Mittels verschiedener Kodierungen kann man die eigene Adresse auf Webseiten so gestalten, dass sie nur schwer mit automatischen Werkzeugen auslesbar ist. Auf der anderen Seite bleibt sie mit den üblichen, von Lesern der Webseite genutzten Werkzeugen Browser und Mailclient transparent und ohne Zusatzaufwand nutzbar. Ironischerweise sind das Verschleierungsmethoden, die Spammer selbst in ihren E-Mails einsetzen, um Filterprogramme zu täuschen.

<sup>3</sup> Web Accessibility Initiative (<http://www.w3.org/WAI/>), Aktionsbündnis für barrierefreie Informationstechnik (<http://www.abi-projekt.de/>)

<sup>4</sup> <http://www.antispam.de/encoder.php>

In URLs können beliebige Zeichen hexadezimal kodiert werden. (Das Leerzeichen wird z. B. zu %20.) Damit sind sie im HTML-Quelltext nicht ohne weiteres als solche erkennbar. Das gilt insbesondere auch für Programme, die Adressen automatisch sammeln sollen (*harvester*).

Die Adresse

<mailto:test@nixspam.org>

lässt sich in einer URL z. B. in der folgenden Weise hexadezimal kodieren:

`mailto:%74%65%73%74%40%6E%69%78%73%70%61%6D%2E%6F%72%67`

Intelligentere *harvester* stören sich daran allerdings nicht. Ein bleibender Erfolg ist nicht zu erwarten.

Da die meisten Webbrowser Javascript unterstützen, kann man damit E-Mail-Links auch vor dem einfachen *harvesting* schützen. Man baut ein regelrechtes Programm in seine Webseite ein, das auf dem Rechner des Besuchers läuft und dort die eigentliche Adresse erzeugt. Ein gewöhnlicher *harvester* sucht lediglich nach reinem Text oder bestenfalls nach HTML-Feinheiten, aber die Interpretation von Javascript ist ihm kaum möglich. Allerdings sollte man hier an die Accessibility denken, die durch allzu tiefgreifende Verschleierungsverfahren<sup>2</sup> eingeschränkt sein kann, etwa wenn der Anwender die Nutzung von Javascript aus Sicherheitsgründen abgeschaltet hat, was sehr zu empfehlen ist.

### 7.2.3 Anzahl eigener Mailadressen begrenzen

Je mehr Mailadressen ein Anwender hat und je älter sie sind, desto mehr Spam bekommt er. Ein Unternehmen sollte daher jeden Mitarbeiter mit nur einer einzigen Mailadresse ausstatten. Es gibt sogar Konstellationen, in denen sich mehrere Mitarbeiter eine einzige, funktionsgebundene Mailadresse teilen können. Funktions- statt personengebundene Adressen wie `info@firma.de` oder `sales@company.com` sind im Geschäftsverkehr üblich.

### 7.2.4 Zusatzinformationen in den eigenen E-Mails mitgeben

Ein Großteil aller Mails ist für Bekannte, Kollegen oder Geschäftspartner bestimmt. Die dazu notwendigen Informationen geben die Absender so gut wie nie von Hand ein, sondern holen sich die Empfängerdaten aus dem (oft automatisch generierten) Adressbuch ihres Mailclients oder verwenden einfach dessen Antwortfunktion.

Gibt der Absender einer E-Mail neben seiner Mailadresse weitere Informationen in der Absenderzeile an (z. B. seinen kompletten Namen und die Firmenzugehörigkeit):

From: Gustav Meier, Example GmbH <[gmeier@example.com](mailto:gmeier@example.com)>

so werden diese Informationen auch mit im Adressbuch des Empfängers gespeichert und in der Regel auch wieder in einer Antwort enthalten sein:

To: Gustav Meier, Example GmbH <[gmeier@example.com](mailto:gmeier@example.com)>

Gustav Meier kann nun alle E-Mails, die diese Zusatzinformationen enthalten, bevorzugt behandeln. Spammer haben diese Zusatzinformationen meistens nicht und würden die E-Mail nur an

To: [gmeier@example.com](mailto:gmeier@example.com) versenden.

### 7.2.5 Zusatzinformationen im mailto:-Link

In der Regel findet ein Erstkontakt per E-Mail mit Hilfe von Informationen statt, die der Absender auf einer Webseite des Angeschriebenen gefunden hat. Der spätere Empfänger kann schon bei der Gestaltung seiner Webseiten darauf achten, dem Absender auf diesem Weg außer der Mailadresse zusätzliche Informationen mitzugeben, die dem Empfänger (oder meist dessen Mailfilter) das Klassifizieren der eingehenden Mail erleichtert. Es reicht bereits die Ergänzung des eigenen Vor- und Nachnamens in der To:-Zeile, damit sich die erwünschte E-Mail von den meisten unerwünschten eindeutig unterscheiden lässt. Der mailto:-Link ist aber auch geeignet, viele weitere Informationen in der später ausgehenden Mail unterzubringen, bis hin zu einem vorab ausgefüllten *body*.

#### HTML-mailto: ausnutzen

Das *HTML anchor tag* `<a href=„...“>` dient dazu, Links auf andere Webseiten zu erzeugen, ist aber auch durch Nutzung des `mailto:-URL-Formats` für den Versand von E-Mails verwendbar: Beim Klick auf entsprechend unterlegte Texte oder Bilder startet der Mailclient des Anwenders. Üblicherweise lässt der Gestalter der Webseite auf das `mailto:` nur die Mailadresse folgen, die der Mailclient direkt in die To:-Zeile übernimmt.

Weitergehende Informationen kommen selten zum Einsatz, dabei gibt es kaum einen bequemeren Weg, E-Mails vorab in eine Form zu bringen, die ihnen beim Empfänger (oder zunächst bei dessen Filter) die nötige Aufmerksamkeit verschafft.

Mit dem HTML-Code

```
<a href=„mailto:Michael      Mustermann      &lt;mmusterm@nix-
spam.org&gt;?subject=
```

```
Wichtige%20Anfrage&body=Sehr%20geehrter%20Herr%20Mustermann,“>Kontakt</a>
```

erreicht man nicht nur, dass die E-Mail per Mausklick vorab teilweise ausgefüllt ist. Der Link enthält auch weitaus mehr Informationen, als ein typischer Adressensammler verarbeiten kann – insbesondere wenn der Gestalter der Webseite dieses Verfahren mit der HTML-Umkodierung verbindet, die der vorangegangene Kasten beschreibt. Ein Tutorium <sup>5</sup>

<sup>6</sup> gibt es im WWW.

### 7.2.6 Häufiger Adresswechsel und Wegwerfadressen

Einige Anwender setzen darauf, dass sie weniger Spam erhalten, wenn sie ihre Mailadresse häufig wechseln. Manche lassen sich sogar Adressen mit „Verfallsdatum“ monatlich neu zuteilen. Ein häufiger Wechsel der Adresse verhindert nicht prinzipiell deren Verbreitung bei Spammern. Aber dadurch, dass jede Adresse anfangs nur selten zum Spam-Ziel wird und dass der Adressat sie schon vor einem deutlichen Anstieg des Spam-Volumens wieder für ungültig erklärt, geht insgesamt weniger Spam ein als bei einer dauerhaft verwendeten Adresse. Er bedeutet aber mehr Aufwand für reguläre Absender, da beispielsweise die Adressbucheinträge und gesammelten Visitenkarten der Kommunikationspartner schnell nutzlos werden. Manche trennen deshalb ihre „normale“ Mailadresse, die sie im Kontakt mit Bekannten oder Geschäftspartnern nutzen, von Adressen, die sie in öffentlichen Foren wie dem Usenet verwenden.

Im Extremfall benutzt man Einmal- oder Wegwerfadressen (*disposable email address*). Das bietet sich an, wenn ein Anwender sich online für eine Software oder einen Web-Dienst registrieren will. Für diesen und ähnliche Vorgänge ist meist eine funktionsfähige Mailadresse nötig. Bei einem

<sup>5</sup> <http://eduweb.brandonu.ca/~edtech/class/notes/mailto.htm>

<sup>6</sup> <http://pnahay.home.sprynet.com/mailtogenerated.htm>

einmaligen Vorgang wäre es ein unnötiges Risiko, die offizielle Mailadresse einzusetzen, besonders wenn die Vertrauenswürdigkeit des Anbieters noch unklar ist.

Wegwerfadressen lassen sich auch von Dienstleistern wie Spam Gourmet<sup>7</sup> oder Spammotel<sup>8</sup> beziehen. Ob eine solche Adresse eines Tages in die Hände von Spammern gerät, spielt für den Anwender keine Rolle, da sie dann schon nicht mehr gültig ist. Auch wer keine speziellen Einmal-Adressen, sondern etwa eine normale, unbegrenzt gültige Webmailer-Adresse für Registrierungszwecke nutzt, muss sich wenig vom dort eingegangenen Spam stören lassen, denn die erwünschte E-Mail ist nur in einem eng begrenzten Zeitraum zu erwarten, ein langwieriges Aussortieren entfällt.

Der Einsatz solcher Alternativen wirkt zwar einer unkontrollierten Verbreitung der offiziellen Mailadresse entgegen, doch der Anwender muss sich darüber im Klaren sein, dass er einen gewissen Zusatzaufwand betreiben muss (etwa für das Besuchen der Webmailer-Sites) und dass er einen Teil der persönlichen E-Mails Dritten anvertraut, wenn er externe Dienste nutzt.

---

<sup>7</sup> <http://www.spamgourmet.com/>

<sup>8</sup> <http://www.spammotel.com/>

## 8 Antispam-Maßnahmen: Grundlagen

Dieses Kapitel untersucht die Ansatzpunkte für Antispam-Verfahren und beschreibt, aus welchen grundlegenden Bausteinen die Verfahren bestehen können. Dabei findet auch der Ort der Maßnahme Berücksichtigung, ebenso wie die Bewertung und anschließende Aktionen. Mit dem Wissen aus diesem Kapitel sind die spezifischen Maßnahmen, die Kapitel 9 aufführt, besser einzuordnen und zu verstehen.

### 8.1 Ansatzpunkte für eine Filterung

Zur Unterscheidung von Spam und Ham und damit als Ansatzpunkte für eine Filterung stehen mehrere Merkmale zur Verfügung. Neben der IP-Adresse des sendenden Rechners (und den IP-Adressen in den `Received`-Zeilen) sind das die Absenderadresse (oder auch nur die Absenderdomain) und der Inhalt der E-Mail. Aber auch das Verhalten des Absenders bei deren Zustellung kann Hinweise darauf geben, ob die Kommunikation mit einem regulären MTA oder mit einem Spammer stattfindet. Daneben ist die Tatsache, dass Spam immer in Massen auftritt, ein gutes Kriterium. Die verschiedenen Ansatzpunkte werden im Folgenden näher erläutert.

Die Abbildungen in den folgenden Kapiteln weisen auf die einzelnen Maßnahmen in Kapitel 9 hin. Der Ansatzpunkt für die Filterung wird dabei als Basis in einem grauen Kasten dargestellt. Darauf bauen verschiedene Verfahren auf, die getrennt werden in solche, die Accreditation und Reputation (siehe Kapitel 8.3) verwenden, sowie alle anderen. Für die absenderbasierten Verfahren gibt es als zusätzlichen Block die Absenderauthentifizierung (siehe Kapitel 8.2), die für sich genommen keine Antispam-Maßnahme ist, sondern nur ein Baustein in einem größeren System.

#### 8.1.1 IP-Adresse

Das einzige nicht fälschbare Datum bei der Einlieferung einer E-Mail ist die IP-Adresse des sendenden MTA<sup>1</sup>. Der empfangende MTA kann sie folglich zur Filterung einsetzen. Niemand kann eine Liste aller „guten“ und „bösen“ IP-Adressen führen, zumal sie sich ständig ändern. Für Teilbereiche ist das aber durchaus möglich: Die Erfahrung zeigt, dass IP-Adressen, von denen aus vor kurzem Spam versandt wurde,

wahrscheinlich weiterhin als Spam-Quellen in Erscheinung treten werden. Umgekehrt kommen aus Adressbereichen, von denen erwünschte E-Mails ausgingen, mit hoher Wahrscheinlichkeit auch in nächster Zeit ausschließlich Ham-Mails. Aufgrund dieser Erfahrungen ist es eine gängige Maßnahme, Black- und Whitelists von IP-Adressen zu führen, die als Ausgangspunkte entweder von Spam oder von Ham bekannt sind.

Außerdem stellt jeder Mailserver, den eine E-Mail passiert, dem bestehenden *header* der E-Mail eine `Received`-Zeile voran, die unter anderem die IP-Adresse des sendenden Rechners enthält. Der Weg einer E-Mail ist damit im *header* von unten nach oben nachvollziehbar.

Eine typische `Received`-Zeile sieht wie folgt aus<sup>2</sup>:

```
Received: from client.example.com (client.example.com [192.0.2.4]) by mailserver.example.org
(Postfix) with ESMTP id A35FA69ED8 for <empfaenger@example.org>; Mon, 2 Nov 2004
13:44:14 +0100 (MET)
```

<sup>1</sup> Auch die IP-Adresse kann im Prinzip gefälscht werden, der Aufwand ist aber so hoch, dass dieser Fall in der Praxis keine Rolle spielt. Wenn jemand IP-Adressen fälschen kann, kann er außerdem noch ganz anderen Schaden anrichten.

<sup>2</sup> Hier vom MTA Postfix erzeugt. `Received`-Zeilen unterscheiden sich etwas je nach MTA-Software.

Das Beispiel zeigt in der ersten Zeile die IP-Adresse und den Hostnamen des zustellenden, in der zweiten Zeile den Hostnamen des empfangenden MTA.

Ein Spammer kann natürlich in eine von ihm versandte E-Mail beliebige Received-Header eintragen, um irgendeinen Versandweg vorzutäuschen. Erst wenn die E-Mail in den eigenen Verantwortungsbereich übergegangen ist, kann man sich auf die danach eingetragenen Informationen verlassen. Ist der empfangende MTA vertrauenswürdig, weil es sich bei ihm zum Beispiel um ein eigenes System oder den Mailserver des eigenen Providers handelt, so ist davon auszugehen, dass die IP-Adresse des zustellenden MTA authentisch ist. Kennt man mehrere MTAs in ununterbrochener Kette von oben nach unten, kann man all diesen Informationen vertrauen.

### 8.1.2 Absenderadresse und -domain

Einige Verfahren benutzen die Absenderdomain als Kriterium für die Spamfilterung und vergleichen diesen Teil rechts des At-Zeichens „@“ in der Envelope-From-Adresse oder in einem oder mehreren Header-Adressfeldern mit entsprechenden Listen.

Da der Spammer diese Angaben jedoch beliebig fälschen kann, ist die Absenderdomain allein kein ausreichendes Filterkriterium. Damit es sich stärker gewichten lässt, gibt es Verfahren zur Absenderauthentifizierung (siehe Kapitel 8.2).

Ein spezieller Fall liegt vor, wenn die Absenderdomain überhaupt nicht existiert, denn dann sollten von dort auch keine E-Mails kommen. Leider passiert so etwas aber gelegentlich bei erwünschten E-Mails, wenn das Mailprogramm des Absenders fehlerhaft konfiguriert ist.

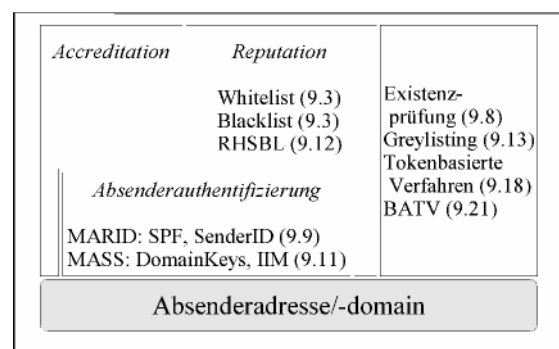


Abb. 8.2: Absenderbasierte Verfahren

Wie die Absenderdomain lässt sich auch die gesamte Absenderadresse zur Filterung heranziehen. Da Spammer Absenderadressen fälschen und ständig neue verwenden, sind sie für die Verwendung in Blacklists schlecht geeignet. „Gute“ Adressen sind dagegen in lokalen Whitelists gut aufgehoben, da es sehr unwahrscheinlich ist, dass der Spammer sie errät.

### 8.1.3 Inhalt

Für den Menschen eignet sich der Inhalt einer E-Mail am besten zur Erkennung von Spam. Für den Computer ist das etwas schwieriger und aufwendiger. Trotzdem gibt es viele Verfahren, die auf der Analyse des Inhalts beruhen. Manche Verfahren untersuchen dabei nur den *header*, manche nur den *body*, am besten ist aber die kombinierte Sicht. Neben

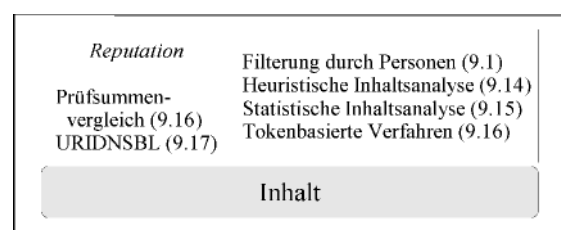


Abb. 8.3: Inhaltsbasierte Verfahren

heuristischen Filtern mit fest konfigurierten Regeln sind immer mehr Filterprogramme erfolgreich im Einsatz, die den Text der E-Mails (und meist auch den *header*) anhand statistischer Analysen bewerten.

Gut zur Unterscheidung eignet sich auch die Sprache einer E-Mail.<sup>3</sup> Spam ist meist englisch. Bekommt ein Empfänger selten Ham-Mails auf englisch, kann das ein sinnvolles Kriterium sein. Und Europäer können meist wenig mit einer koreanischen oder japanischen E-Mail anfangen. Hier sieht man aber besonders deutlich, wie subjektiv solche Einschätzungen sind, denn natürlich gibt es Empfänger, die Korrespondenzpartner im Ausland haben.

Häufig enthält Spam wechselnde Nonsens-Inhalte, die den eigentlichen Inhalt (*payload*, oft nur wenige Worte Text und ein Web-Link oder eine Rufnummer) vor Filtersystemen abschirmen sollen, die den Inhalt der E-Mails analysieren. Gegen die automatisierte Inhaltsanalyse helfen sollen auch Methoden wie die absichtliche Falsch-Schreibung<sup>4</sup> („V1 agr@“) oder die Tarnung mit Hilfe von fremden Texten zum Beispiel aus News-Seiten. Das Einstreuen vollkommen sinn- und zusammenhangloser Worte soll darüber hinaus die statistische Analyse und die Wiedererkennbarkeit mittels Prüfsummenverfahren erschweren – um den Preis der Tatsache, dass ein menschlicher Leser derartige E-Mails umso leichter als Spam erkennt.<sup>5</sup>

Aufgrund der Web-Fähigkeit der meisten Mailclients steht den Spammern in Form von HTML ein großes Betätigungsfeld zur Verfügung, die eigentlichen Inhalte der E-Mail zu verschleiern, um einerseits den Zugriff durch Filter zu erschweren, andererseits dem „Anwender“ den erwünschten Klartext zukommen zu lassen. So ignorieren Web-Browser zum Beispiel unbekannte HTML-Tags wie `<unsinn>` genauso wie `<!--HTML-Kommentare-->`. Das Einstreuen solcher Tags ist eine relativ alte, aber immer noch beliebte Verschleierungsmethode, ebenso das Verstecken sinnloser Füllwörter und -zeichen durch kleine Schriftgröße oder unlesbare Farbe. Derlei Verfahren kann ein Filter leicht erkennen und als verdächtig einstufen.

Es ist allerdings ein Mehraufwand für den Filter, wenn er nicht nur die Verschleierung an sich erkennen soll, sondern auch die verschleierte Schlüsselwörter, da er dann ein komplettes HTML-Parsing durchführen muss. Besonders trickreiche Spams enthalten Javascript-Code, der erst per Interpretation durch den Mailclient zu lesbarem Text wird. Ein Filter kann sich in solchen Härtefällen damit begnügen, die Existenz dieser Verschleierungsmethode als verdächtig anzusehen, ohne selbst Javascript beherrschen zu müssen.

Ähnliches gilt für die Transportkodierung Base64<sup>6</sup>, die meist zum Einsatz kommt (nicht nur bei Spammern), wenn E-Mails binäre Inhalte transportieren. Sie eignet sich auch zur Verschleierung von Klartext: Da es einen Mehraufwand für Filter bedeutet, zunächst den Klartext zu extrahieren, setzen Spammer gerne die Base64-Kodierung ein, auch wenn sie nur Text versenden. Einige Filter „übersetzen“ deshalb den Inhalt der E-Mail erst in eine Form, die dem ähnelt, was der Nutzer zu sehen bekommen würde, bevor sie die eigentliche Filterung durchführen, andere begnügen sich auch an dieser Stelle damit, etwa die Existenz Base64-kodierten Klartextes als ein Verdachtsmoment (von vielen möglichen) anzusehen. Außer der Transportkodierung gibt es viele weitere Datenformate, die ein umfassender Filter heute berücksichtigen muss. E-Mail ist mittels des Standards Multipurpose Internet Mail Extension (MIME, [RFC2045-RFC2049]) zu einem Medium geworden, das den Austausch beliebiger binärer Inhalte ermöglicht, darunter eben auch Viren und Würmer und verschleierter Spam.

Zur Vermeidung von *false positives* untersuchen wirksame Filter die E-Mails nicht nur auf unerwünschte, sondern auch auf erwünschte Merkmale. Spammer kennen den Empfänger in der Regel nicht einmal namentlich. Allein ein Test auf das Vorhandensein des vollständigen Namens etwa in einer Anrede im *body* oder in der To:-Header-Zeile kann mit hoher Trefferquote erwünschte E-Mails erkennen. Umgekehrt ist es leider nicht so einfach, da viele erwünschte E-Mails relativ

<sup>3</sup> Die Sprache eines Textes lässt sich z. B. über charakteristische Häufigkeiten von Buchstabenkombinationen automatisch ermitteln. Nicht auf die Sprache, sondern auf den verwendeten Zeichensatz bezieht sich die Charset-Definition in einer Content-Type:-Header-Zeile, aber auch dieser eignet sich unter Umständen zur Filterung.

<sup>4</sup> <http://cockeyed.com/lessons/viagra/viagra.html>

<sup>5</sup> Viele Beispiele gibt es unter <http://www.jgc.org/tsc/> und <http://www.jgc.org/pdf/jgc-march-2004-hackin9.pdf>

<sup>6</sup> siehe <http://de.wikipedia.org/wiki/Base64> und in [RFC2045] Abschnitt 6.8

unpersönlich gestaltet sind. Nicht nur Massensendungen wie Newslettern mangelt es häufig an derlei persönlichen Elementen, sondern auch geschäftlichen oder privaten E-Mails, die oft betont salopp aufgemacht sind, etwa lediglich ein „hi!“ als Anrede enthalten. Erwünschte Newsletter und Mailinglisten-Beiträge können aus diesem Grunde gelegentlich zu *false positives* führen und erfordern manchmal gesonderte Filterregeln.

Spams sind in der Regel recht klein (meist deutlich unter 10 kByte<sup>7</sup>), vor allem damit die Aussendung von Millionen von E-Mails schnell erledigt ist und der Versand von einem Zombie-PC aus nicht durch einen abnormen Ressourcenbedarf auffällt. Auch wenn Anwender eigentlich darauf achten sollten, dass die Eingangsbox ihres Gegenübers nicht überläuft, sind dagegen E-Mails mit einem Umfang von 100 kByte und mehr wahrscheinlich kein Spam. Erwünschte E-Mails tragen oft Anhänge mit PDF- oder Office-Dateien, und das ist bisher bei Spam selten zu beobachten. Spamfilter untersuchen aus diesem Grund oft nur kleinere E-Mails.

Ein Sonderfall sind verschlüsselte E-Mails. Hier kann eine Inhaltsanalyse erst nach der Entschlüsselung erfolgen. In der Praxis spielt das aber keine große Rolle, weil Ham selten verschlüsselt ist und Spam noch seltener. (Anders allerdings bei Viren, die sich manchmal in verschlüsselten ZIP-Files verbergen, um eine Erkennung durch Virencanner zu erschweren. Das Passwort für die Entschlüsselung findet sich dann meist im *body* der E-Mail.)

Juristisch ist die automatisierte Inhaltsanalyse auf Viren oder Spam unbedenklich, soweit nicht zusätzliche Informationen mit Hilfe der Analyse gewonnen werden, etwa über die Arbeitsleistung eines Beschäftigten oder Ähnliches.

#### 8.1.4 Verhalten des Absenders

Spammern geht es immer darum, möglichst viele E-Mails in möglichst kurzer Zeit zu versenden. Zu diesem Zweck verwenden sie spezielle Programme, die vom standardkonformen Verhalten von MUAs oder MTAs abweichen können. Beliebte Beispiele sind das Auslassen der *HELO/ EHLO*-Sequenz bei der Verbindungsaufnahme oder das Absetzen der kompletten Daten einer E-Mail, ohne auf Antworten des empfangenden Mailserver zu warten. Auch Timeouts beim Protokollablauf, die sehr viel kürzer sind als bei MTAs üblich, können ein Indiz für die Aktivität einer Spam-Software sein. Ein Spam-Programm wird auch selten ein zweites Mal versuchen, eine E-Mail abzusetzen, wenn der erste Versuch fehlgeschlagen ist.

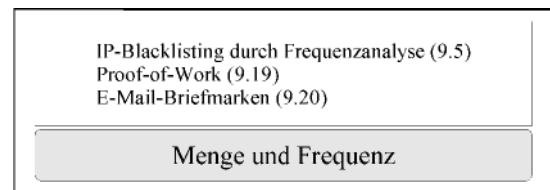


Abb. 8.5: Mengen-/Frequenz-basierte Verfahren

#### 8.1.5 Menge und Frequenz

Ausgesprochen charakteristisch für Spam ist der Massenversand. Dem einzelnen Empfänger wird dieses Charakteristikum natürlich nicht viel helfen, aber insbesondere große Provider können sehr wohl erkennen, dass aus einer Quelle besonders viele gleiche oder ähnliche E-Mails kommen. Besonders wenn gleiche oder ähnli-

che E-Mails aus ganz verschiedenen Quellen kommen, ist ein deutlicher Hinweis auf Spam oder Viren gegeben. Ebenso typisch für Spam ist eine hohe Fehlerquote bei der Zustellung wegen ungültiger Mailadressen, da die Adresslisten der Spammer häufig schlechter „gewartet“ sind als die Adresslisten von legitimer Massenmail.

Große Provider oder auch Organisationen und Firmen, die sich zusammenschließen, um auf entsprechend breiter Basis zu operieren, können durch eine Frequenzanalyse Rückschlüsse auf den

<sup>7</sup> anders bei Viren oder Würmern, die oft deutlich größer sind

Spam- oder Ham-Gehalt einer E-Mail ziehen. Die Frequenzanalyse kann sich auf mehrere der vorgenannten anderen Spam-Merkmale beziehen.

Solche Verfahren sind relativ aufwendig, aber außerordentlich wirksam. Und da es ja gerade das wesentliche Ziel des Spammers ist, viele E-Mails zu verschicken, greifen sie genau an der richtigen Stelle an. Es gibt aber auch viele legitime Versender von Massenmails, und ein Mailserver, von dem gestern noch wenige E-Mails ausgingen, kann heute plötzlich viel mehr abliefern. Daher sind solche Verfahren entsprechend vorsichtig umzusetzen, etwa in Kombination mit Whitelisting.

## 8.2 Absenderauthentifizierung

Wer bei einer Antispam-Maßnahme die Absenderadresse oder -domain als Merkmal zur Filterung einsetzen will, muss bedenken, dass diese Angabe beliebig fälschbar ist. Insoweit liegt hier eine andere Situation als bei der Filterung auf Basis der IP-Adresse vor, die sich nicht einfach fälschen lässt.

Da es viele Millionen Absenderadressen von ebenso vielen Endanwendern gibt, ist es schwierig, ein System einzuführen, das jeden Absender authentifizieren kann. Statt die komplette Absenderadresse zu authentifizieren, wäre aber auch schon die Authentifizierung der Domain ein Schritt in die richtige Richtung, weil man dann den Domaininhaber verantwortlich machen oder über ihn an den eigentlich Schuldigen herankommen kann. Deswegen sind solche Verfahren in letzter Zeit oft im Gespräch.

Bei jeder Art von Absenderauthentifizierung ist zu bedenken, dass sie für sich genommen vielleicht gegen *phishing*, *Joe Jobs* und *bounces* helfen kann, nicht aber gegen „gewöhnlichen“ Spam. Einem professionellen Spammer bereitet es keine Schwierigkeit, authentifizierte Absenderadressen zu verwenden.<sup>8</sup> Erst wenn die Absenderauthentifizierung mit einem *reputation system* (siehe Kapitel 8.3) kombiniert wird, ist ein Antispam-Effekt zu erwarten. Bei einer Implementierung muss dieser Zusatzaufwand also berücksichtigt werden. Zurzeit gibt es noch keine verbreitete Lösung, die sowohl die Absenderauthentifizierung als auch ein *reputation system* umfasst.

Ob die diversen Methoden zur Absenderauthentifizierung sich durchsetzen, ist ungewiss. Alle Verfahren sind zu neu und zu komplex, als dass sich ihre zukünftige Effektivität abschließend bewerten ließe. Dass sie heute teilweise recht gut wirken, ist auch darauf zurückzuführen, dass die Spammer noch wenig Gelegenheit (und wegen der geringen Verbreitung wenig Anlass) hatten, sich auf die Verfahren einzustellen.

Manche dieser Verfahren haben so gravierende Nebenwirkungen (insbesondere bei Mail-Weiterleitungen), dass ihr Einsatz umstritten ist. Ein weiteres Problem bei der Einführung ist die unklare Lage bezüglich der Urheber- und Patentrechte. Für viele Verfahren haben sich Firmen Schutzrechte gesichert, die einer allgemeinen Implementierung (z. B. in Open-Source-Produkten) im Wege stehen könnten.

Obwohl es weder bei der DNS-basierten (siehe Kapitel 9.9) noch bei der kryptographischen Absenderauthentifizierung (siehe Kapitel 9.11) einen offiziellen Standard gibt, schreitet die Entwicklung schnell voran. Mehrere große Provider haben schon ihre Unterstützung für das eine oder andere Verfahren erklärt. Die Firma Sendmail<sup>9</sup>, die die im Internet am weitesten verbreitete MTA-Software herstellt, hat bereits eine Empfehlung zur Nutzung der Verfahren zur Absenderauthentifizierung herausgegeben [Send04].

Auch wenn viele Fragen offen bleiben, kann kein Administrator die Existenz der Verfahren ignorieren. Er sollte die Entwicklung verfolgen und zumindest darauf hinarbeiten, E-Mails aus dem eigenen System nur über definierte Mailserver zu verschicken, damit er entsprechende Verfahren dort umsetzen kann.

---

<sup>8</sup> [http://www.ciphertrust.com/company/press\\_and\\_events/article.html?id=0000362](http://www.ciphertrust.com/company/press_and_events/article.html?id=0000362)

<sup>9</sup> <http://www.sendmail.com/>

Keines dieser Verfahren ist ein Antispam-Verfahren im eigentlichen Sinne. Sie wenden sich gegen Adressfälschungen und damit in erster Linie gegen *bounces*, *phishing* und *Joe Jobs*. Sie können allerdings Antispam-Verfahren verbessern, die auf eine verlässliche Absenderadresse angewiesen sind.

## 8.3 Accreditation und Reputation

Wenn der Absender einer E-Mail ziemlich sicher identifizierbar ist (zum Beispiel anhand seiner IP-Adresse oder durch eine Absenderauthentifizierung), bleibt immer noch die Frage, ob es sich um einen Spammer oder einen Absender regulärer E-Mail handelt. Die Authentifizierung verrät nur, wer jemand ist, sie verrät nichts über seine Absichten.

### 8.3.1 Accreditation

Bei so genannten *accreditation systems* („Systeme zur Beglaubigung“) beglaubigt eine Organisation, dass ein bestimmter Absender nur lautere Absichten verfolgt. Wer der beglaubigenden Organisation vertraut, kann unbesorgt E-Mails von diesem Absender annehmen. In der Praxis betreibt die beglaubigende Organisation eine Whitelist, gegen die man ankommende E-Mail prüfen kann. Technisch ist das z. B. über eine DNSBL (siehe Kapitel 9.4) realisierbar.

*Accreditation systems* nützen vor allem den Absendern legitimer Massenmails, deren E-Mails sonst häufig in Spamfiltern hängen bleiben. Der Vorteil für den Empfänger besteht darin, dass er eine (hoffentlich verlässliche) Whitelist benutzen kann, um legitimen Massenversand zu gestatten und seine Filtersysteme zu entlasten. Zurzeit basieren die meisten solcher Whitelists auf der IP-Adresse des Absenders, es ist aber zu erwarten, dass domainbasierte Whitelists eine größere Verbreitung erfahren, wenn sich Systeme zur Absenderauthentifizierung (siehe Kapitel 8.2) durchsetzen.

Die Sicherheit dieser Verfahren beruht darauf, dass ein Mailversender, der beglaubigt werden möchte, mit der beglaubigenden Organisation einen Vertrag schließt, der mehr oder weniger strikte Regeln enthält, an die er sich zu halten hat. Beschwerden nimmt die beglaubigende Organisation entgegen, prüft sie und verhängt falls nötig Sanktionen. In Deutschland wurde ein solches System im Herbst 2004 vom Verband der Internetwirtschaft (eco) e. V.<sup>10</sup> in Zusammenarbeit mit dem Deutschen Direktmarketing Verband (DDV) e. V.<sup>11</sup> unter dem Namen Certified Senders Alliance<sup>12</sup> aus der Taufe gehoben.

Bei manchen *accreditation systems* verlangt die beglaubigende Organisation vom Mailversender eine Garantiesumme (*bond*), die bei Fehlverhalten des Absenders verfällt. Das schafft einen finanziellen Anreiz, sich an die Regeln zu halten.<sup>13</sup>

Eine wesentliche Kritik an diesem Verfahren ist, dass damit nur finanzkräftige Organisationen legitim Massenmails versenden können, während als Hobby betriebene Mailinglisten das Nachsehen haben.

### 8.3.2 Reputation

Einen etwas anderen Ansatz verfolgen so genannte *reputation systems*. Auch hier geht es um den guten Ruf (*reputation*) der Absender. Statt aber potentielle Absender im Vorfeld zu testen, werden

---

<sup>10</sup> <http://www.eco.de/>

<sup>11</sup> <http://www.ddv.de/>

<sup>12</sup> <http://www.eco.de/servlet/PB/menu/1446034/index.html>

<sup>13</sup> Das am weitesten verbreitete System ist „Bonded Sender“ (<http://www.bondedsender.com/>) von der Firma IronPort (<http://www.ironport.com/>).

die Erfahrungen mit bestehenden Absendern erfasst und bei einer Filterentscheidung berücksichtigt. Das Ganze funktioniert also ähnlich wie bei Kredit-Rating-Agenturen in der Finanzwelt, die aus historischen Daten zu Bankkonten und Krediten die Kreditwürdigkeit eines Antragstellers schätzen.

Je nach System kann die Information über den Leumund eines Absenders zentral<sup>14</sup> oder verteilt<sup>15</sup> vorliegen. Viele DNSBLs (siehe Kapitel 9.4) und kollaborative Inhaltsfilter (siehe Kapitel 9.16) sind auch der Kategorie *reputation systems* zuzuordnen. Wie bei den *accreditation systems* stellt sich wieder die Frage, ob die Betreiber des *reputation systems* vertrauenswürdig sind. Bei dezentralisierten Systemen ist das Vertrauen in Einzelne nicht so wichtig, dafür wird es schwieriger, einen Verantwortlichen zu finden, wenn man ihn braucht.

Zu bedenken ist auch, dass man sowohl bei *accreditation* als auch bei *reputation systems* Informationen über den eigenen Mailverkehr weitergibt.

## 8.4 Ort der Maßnahme

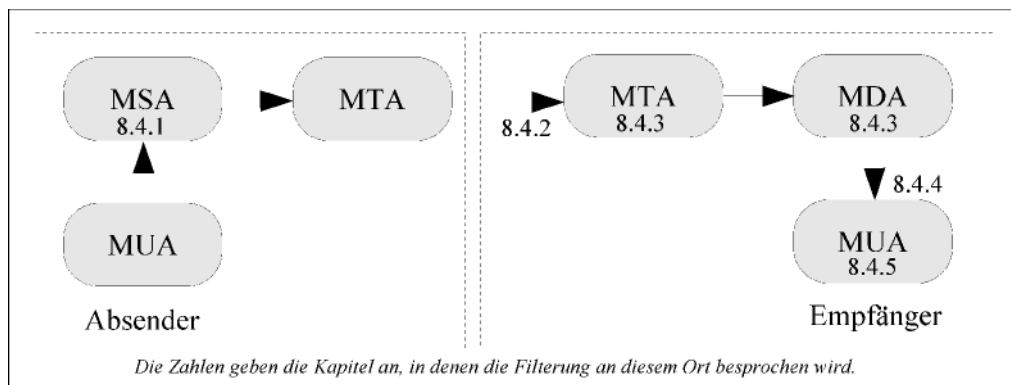


Abb. 8.6: Vereinfachte Darstellung des Weges einer E-Mail

Jede E-Mail gelangt über mehrere Stationen vom Absender zum Empfänger. Daher gibt es mehrere Stellen, an denen eine Antispam-Maßnahme greifen kann. Manche Maßnahmen sind nur an einigen Stellen möglich oder sinnvoll, manche überall einsetzbar. Vom Einsatzort der Maßnahme hängt es erheblich ab, wie viele Ressourcen eine Spam-Mail benötigt. Je mehr Stufen eine E-Mail durchläuft, desto mehr Ressourcen benötigt sie. Ein möglichst früher Einsatzort ist deshalb wünschenswert. In der Praxis werden häufig mehrere Verfahren kombiniert, die an verschiedenen Stellen greifen.

## 8.4 Ort der Maßnahme

### 8.4.1 Im Server beim Versand

Wenn der Spammer den Mailserver eines Providers nutzt, um Spam zu versenden, ist dort die erste Stelle, an der sich die E-Mails abfangen lassen (Ausgangsfilterung, *outbound* oder *egress filtering*). Die meisten Spammer umgehen die Mail-Infrastruktur des eigenen Providers und stellen den Spam direkt zu, doch SMTP-Port-Sperren (siehe Kapitel 9.6) und Verfahren zur Absenderauthentifizierung (siehe Kapitel 8.2) beschränken den direkten Versand mehr und mehr. Es ist also damit zu rechnen, dass die Zustellversuche über die MTAs der Provider zunehmen werden.

<sup>14</sup> Z. B. beim SenderBase-System: <http://www.senderbase.org/>, ebenfalls von der Firma IronPort

<sup>15</sup> Z. B. beim GOSSIP Project: <http://gossip-project.sourceforge.net/>

Der Vorteil der Spambekämpfung beim Absender-Provider ist, dass die E-Mail niemals beim Mailserver des vom Spammer vorgesehenen Empfängers ankommt. Außerdem kann der Provider auf Absenderseite den Spam eventuell leichter erkennen, weil er mehr davon transportiert. Der Empfänger erhält zu einem Zeitpunkt aus einer Quelle in der Regel nur eine einzelne Spam-Mail, der Absender-Provider sieht aber die E-Mails an alle Empfänger. Die Filterverfahren unterscheiden sich dort kaum von den Verfahren für ankommende E-Mails.

Stellt sich ein Kunde eines Providers als Spammer heraus, kann der Provider ihn besser identifizieren und er hat mehr Möglichkeiten, auf ihn Einfluss zu nehmen, beispielsweise über die AGB. Und selbst wenn der Spammer fremde Systeme für den Spamversand missbraucht, kann der Provider seinen Kunden, der dem Spammer hilft, ohne es zu wissen, den Internetzugang sperren und darauf hinwirken, dass der sein System bereinigt. Analog gilt das für Betriebe und ihre Mitarbeiter.

In einer ähnlichen Situation sind Webmail-Provider, deren Web-Interface missbraucht werden kann, um große Mengen an Spams zu versenden. Auch hier ist es nötig, mit Heuristiken und Filtern einzugreifen, um die Massenmails zu erkennen und „an der Quelle“ abzustellen.

Nachteil dieses Verfahrens ist, dass der Empfänger keinerlei Einfluss darauf hat, welche E-Mails ihm zugehen. Der Provider des Spammers entscheidet, was ausgeliefert wird und was nicht.

### 8.4.2 Im Server vor Annahme der E-Mail

Wenn Spam direkt zugestellt wird oder die Hürde des absendenden Mailsystems genommen hat, erreicht er den Mailserver des Empfängers. Absender- und Empfängersystem treten in einen Dialog (SMTP, siehe Kapitel 4.1.1), über den sie Absender- und Empfängeradressen und weitere Informationen austauschen und schließlich die eigentliche E-Mail transportieren. Solange der Empfänger den korrekten Empfang der E-Mail nicht bestätigt hat, ist sie in technischem Sinne noch nicht übertragen worden. Bis dahin hat er also Zeit, den Empfang der E-Mail abzulehnen (siehe [RFC2821], Abschnitt 3.3).

Im SMTP-Dialog lassen sich mehrere Phasen unterscheiden. Die Ablehnung kann

- durch Nicht-Akzeptanz der TCP-Verbindung ( z. B. durch IP-Level-Filter),
- nach dem TCP-Connect, vor dem *HELO* (statt des Banners),
- nach dem Kommando *HELO*,
- nach dem Kommando *MAIL FROM*,
- nach dem Kommando *RCPT TO*, oder
- nach dem Kommando *DATA*, gefolgt von `<CRLF>.<CRLF>`

erfolgen.

Der Mailserver kann den Empfang im Prinzip in jeder Phase ablehnen, häufig hat er aber erst nach dem Kommando *RCPT TO* oder nach der *DATA*-Phase genug Informationen für eine Entscheidung.

Da der sendende Server das *RCPT-TO*-Kommando (mit der Empfängeradresse) mehrfach angeben kann, ist hier eine Ablehnung oder Annahme der E-Mail in Abhängigkeit von der angegebenen Empfängeradresse möglich.

Vorteil der Ablehnung nach der *DATA*-Phase ist, dass jetzt die komplette E-Mail vorliegt, also sämtliche Prüfungen möglich sind, die auf dem Inhalt basieren.

Nachteil einer Ablehnung nach der *DATA*-Phase ist, dass die Ablehnung nicht mehr für einzelne, sondern nur für alle Adressaten gemeinsam erfolgen kann. Wenn man erst in diesem Schritt erkennt, dass die E-Mail für einen Empfänger abgelehnt, für den anderen aber angenommen werden soll, beispielsweise aufgrund unterschiedlicher Konfiguration der persönlichen Spamfilter, dann muss der MTA die E-Mail annehmen und für den ablehnenden Empfänger weiter verfahren wie im nächsten

Abschnitt beschrieben. Daneben benötigt die komplette Übertragung der E-Mail auch mehr (teure) Bandbreite.

Je nach Architektur der MTA-Software kann es sein, dass selbst nach dem *RCPT TO* oder nach der *DATA*-Phase noch nicht feststeht, in welche Mailbox eine Mail schließlich gelangen wird. Zwar steht die Empfängeradresse fest, aber der MTA kann sie noch umschreiben. Eventuell können benutzerdefinierte Filter an dieser Stelle also noch nicht zum Einsatz kommen.

### 8.4.3 Im Server nach Annahme der E-Mail

Hat der Server eine E-Mail angenommen (durch eine Bestätigung nach Abschluss der *DATA*-Phase), muss er sie auch weiter bearbeiten. Der Server muss die E-Mail entweder zustellen oder eine Fehlermail (*bounce*) an den Absender senden.

Viele Spamfilter, die nicht direkt in den MTA integriert sind, arbeiten an dieser Stelle. Der MTA ruft dazu ein externes Filterprogramm auf und übergibt ihm die E-Mail. Bevor Mailprogramme eine direkte Interaktion mit Mailfiltern unterstützten, war das häufig die einzige Möglichkeit der Filterung. Und auch heute gibt es noch viele Mailserver, die erst an dieser Stelle den kompletten Inhalt der E-Mail zur Filterung zur Verfügung stellen können.

Ganz wesentlicher Nachteil dieser Methode ist, dass sie *bounces* und damit viel kollateralen Spam (siehe Kapitel 3.2.7) erzeugt. Und da diese *bounces* häufig nicht zustellbar sind, verstopfen sie die Versand-Queue auf dem Server.

### 8.4.4 Im Client vor Abholung der E-Mail

Auch nachdem eine E-Mail zugestellt, also im Postfach des Empfängers abgelegt wurde, kann gefiltert werden. Der Client kann über das POP3- oder IMAP-Protokoll den *header* der E-Mail anfordern, darauf basierend die Unterscheidung in Spam und Ham treffen und dann direkt ein Löschkommando für jede Spam-Mail zum Server schicken. Er muss den Inhalt der E-Mail dann nicht mehr übertragen. Falls der vom Anwender verwendete Client diese Vorgehensweise nicht unterstützt, kann er dafür spezielle Software benutzen.

### 8.4.5 Im Client nach Abholung der E-Mail

Die letzte Gelegenheit für eine Filterung, bevor der Anwender den Spam sieht, bietet dessen Mailclient. Der Spam hat dann die ganze Kette der Server durchlaufen und überall

Ressourcen verbraucht, aber vielleicht kann noch die kostbarste Ressource, nämlich die Zeit des Anwenders, geschützt werden.

Vorteil solcher Filter ist, dass der Anwender hier den größten Einfluss auf deren Funktion hat: Er kann beliebige Software einsetzen, die ihm geeignet erscheint, und er kann einen Filter beliebig konfigurieren und im Extremfall auch ganz deaktivieren. Dadurch ist also seine subjektive Definition von Spam umsetzbar. Einige Filterverfahren lernen (entweder selbständig oder mit Hilfe des Anwenders) mit der Zeit immer besser, was Spam und was Ham ist. Der Anwender hat hier den größten und direktesten Einfluss auf den Lernfortschritt.

Daneben ist von Vorteil, dass das System des Anwenders in der Regel schnell genug ist, um auch umfangreiche und komplexe Tests des Inhalts der E-Mail durchzuführen. Jeder Anwender sieht für sich genommen wesentlich weniger Spam als der Server, der für viele Mailadressen zuständig ist, und damit häufig durch komplexere Filterverfahren überlastet wäre.

Nachteil ist, dass die E-Mail den ganzen Weg bis zum Client durchlaufen muss, was besonders für Anwender langsamer Modemverbindungen sehr unangenehm sein kann.

Falls dem Client keine dauerhafte Internet-Verbindung zur Verfügung steht, sind ihm alle Filterverfahren verwehrt, die auf Datenbanken im Internet zugreifen müssen ( z. B. SPF, SenderID, DNSBLs, Prüfsummenvergleich, siehe Kapitel 9). Diese Einschränkung kann man umgehen, wenn der Server bereits entsprechende Abfragen durchführt und dem Client die dadurch erlangten Informationen in speziellen Header-Zeilen zur Verfügung stellt.

## 8.5 Bewertung

Jedes Antispam-System muss am Ende eine Bewertung in Spam und Ham vornehmen. Sie kann richtig oder falsch sein. Dadurch sind vier Ergebnisse möglich:

|              |      | E-Mail ist tatsächlich ... |                       |
|--------------|------|----------------------------|-----------------------|
|              |      | Spam                       | Ham                   |
| E-Mail wurde | Spam | <i>true positive</i>       | <i>false positive</i> |
|              | Ham  | <i>false negative</i>      | <i>true negative</i>  |

Wünschenswert sind eine möglichst große True-Positive- und True-Negative-Rate sowie möglichst kleine Werte für *false negatives* und *false positives*.<sup>16</sup> Die False-Positive-Rate, also die Anzahl der E-Mails, die fälschlicherweise als Spam erkannt wurden, ist dabei in der Regel das wichtigste Kriterium. Schließlich soll keine erwünschte E-Mail verloren gehen.

Kein Verfahren zur Erkennung von Spam ist perfekt, alle haben ihre charakteristischen Werte für die vier möglichen Ergebnisse. Der Administrator kann Verfahren unterschiedlich gewichten und dadurch beschränkt Einfluss auf die False-Negative- und False-Positive-Raten ausüben. Fehler ganz ausschließen kann er jedoch nicht. Zu bedenken ist dabei, dass auch sehr kleine Fehlerraten bei einem großen Mailumsatz zu einer spürbaren Anzahl fehlerhaft klassifizierter E-Mails führen.

Die Effektivität von Maßnahmen kann über die Zeit erheblich schwanken, weil sich die Methoden der Spammer verändern. Viele Maßnahmen sind nur deshalb so effektiv, weil sie neu oder nur bei wenigen Anwendern im Einsatz sind. Die Spammer haben so keinen Anlass, ihre Methoden zu ändern. Sobald sich aber ein Verfahren allgemein durchsetzt, werden die Spammer sich darauf einrichten. Auch deshalb ist es in der Regel sinnvoll, eine Kombination von Maßnahmen zu verwenden. Bei der Auswahl der Verfahren sollte man also auch die zu erwartende Nachhaltigkeit berücksichtigen. Seit Jahren erfolgreiche Antispam-Maßnahmen werden nicht von heute auf morgen völlig wirkungslos.

### 8.5.1 Vergleichbarkeit

Die Beurteilung der Effektivität von Antispam-Maßnahmen ist schwierig. Es gibt keine standardisierten Tests, ja nicht einmal eine Übereinkunft, was denn überhaupt zu messen ist. Die Schwierigkeiten kommen vor allem daher, dass zum Test viele Ham- und Spam-Nachrichten vorhanden sein müssen, die man als Grundlage verwenden kann. Sie müssten aber ständig auf dem neuesten Stand gehalten werden, da nur dann eine aussagekräftige Bewertung möglich ist.

Erschwerend kommt hinzu, dass viele Verfahren dynamisch sind. Sie werten aktuelle Datenbanken und Statistiken aus, die bei einem „Labortest“ nicht zur Verfügung stehen. Daneben ist das E-Mail-Aufkommen unterschiedlicher Firmen und Anwender so verschieden, dass nicht jedes Verfahren

<sup>16</sup> <http://www.nwfusion.com/reviews/2004/122004spamside3.html>

überall gleich gut passt. Bei einem Vergleichstest muss man also gezwungenermaßen auf aktuelle und subjektive Daten zurückgreifen, die keine perfekten, aber doch hilfreiche Antworten liefern können.<sup>17</sup>

### 8.5.2 Zusammenwirken von Maßnahmen

Keine Antispam-Maßnahme kann für sich allein erfolgreich sein. Deswegen verbinden Spamfilter verschiedene Maßnahmen auf geeignete Weise miteinander.

Verschiedene Maßnahmen sind entweder nacheinander oder parallel anwendbar. Werden sie nacheinander angewendet, entscheidet jede Filterstufe, ob sie die E-Mail annimmt, ablehnt oder an den nächsten Filter weiterleitet. Bei der parallelen Anwendung werden alle Kriterien gleichzeitig überprüft, um zu einer gemeinsamen Entscheidung zu gelangen. Auf die Kombinationsmöglichkeiten geht das Folgende näher ein.

#### Serielle Anwendung

Bei der seriellen Anwendung kommen mehrere Antispam-Verfahren nacheinander zum Einsatz. Jede Maßnahme kann „sicher“ erkannten Spam oder Ham aussondern und den Rest an die nächste Stufe weiterleiten. Typischerweise wird man billigere (also einfachere Verfahren) zuerst ausführen. Nur E-Mails, die durch die einfacheren Verfahren nicht eindeutig bewertbar sind, gelangen zu aufwendigeren Verfahren.

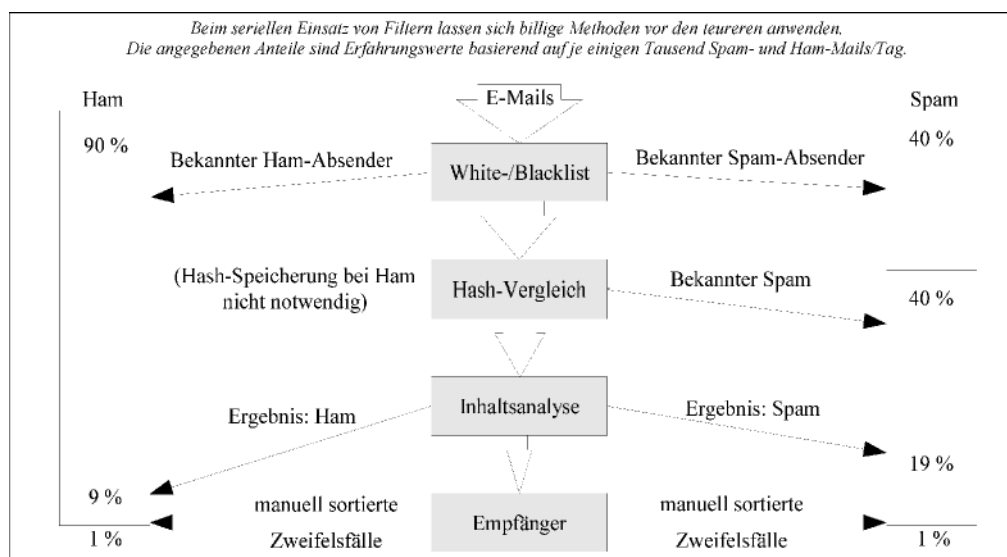


Abb. 8.7: Serieller Einsatz von Filtern

In der Praxis sieht die Aufteilung häufig so aus, dass ein Verfahren einige E-Mails ziemlich sicher als Spam und einige ziemlich sicher als Ham erkennt. Es bleibt eine Grauzone dazwischen. Ziel ist es, diese Grauzone möglichst klein zu halten, ohne *false positives* und *false negatives* zu erzeugen.

Vorteil der seriellen Anwendung ist der niedrige Ressourcenbedarf, da sich viele E-Mails schon mit sehr einfachen und schnellen Verfahren kategorisieren lassen. Nachteil ist die geringere Zuverlässigkeit, da eine spätere Stufe eine E-Mail eventuell nicht mehr zu Gesicht bekommt und deswegen ihre Einschätzung nicht in die Bewertung einfließen kann. Als Folge steigt die False-Positive-Rate.

<sup>17</sup> <http://www.nwfusion.com/reviews/2004/122004spampkg.html>

## Scoring-Verfahren

Bei der parallelen Anwendung wird eine E-Mail nach vielen (manchmal Hunderten) von Kriterien überprüft. Jede Prüfung ergibt eine Punktzahl (*score*). Wenn nach der Prüfung aller Kriterien die aufsummierte Punktzahl größer ist als ein festgelegter Wert, gilt die E-Mail als Spam, sonst als Ham. Dabei können auch Kriterien, die gegen Spam sprechen, mit negativer Punktwertung eingehen.

Der Nachteil des Scoring ist, dass selbst bei offensichtlichem Spam viel Aufwand nötig ist, da alle Kriterien überprüft werden, bevor das endgültige Ergebnis feststeht. Für das Scoring spricht, dass die Filterung aufgrund vieler Kriterien gemeinsam zuverlässiger funktioniert als beim Einsatz weniger Kriterien. Typischerweise wird der Score in eine spezielle Header-Zeile eingetragen (siehe auch Kapitel 8.6.4), was es dem Client ermöglicht, seinen eigenen Schwellwert für die Filterung festzulegen.

In den ersten Antispam-Programmen nahm der Entwickler der Software die Verteilung der Punkte auf die verschiedenen Kriterien noch manuell vor, inzwischen geschieht dies (halb-) automatisch. Aus einer großen Menge von Spam- und Ham-Mails errechnet die Software, wie gut jedes Kriterium zur endgültigen Entscheidung beiträgt und weist ihm einen passenden Score zu. Der zugrunde liegenden Menge an Test-Mails kommt daher eine besondere Bedeutung zu; insbesondere Spam sollte bei der Filterjustierung nicht älter als einige Wochen sein.

## Ressourcenbedarf

Antispam-Maßnahmen verursachen Kosten, insbesondere durch den hohen Bedarf an CPU-Leistung und Festplattenplatz. Aufwendige Tests sind auf ausgelasteten Mailservern häufig nicht durchführbar. Bei nur wenigen hundert E-Mails pro Tag sind alle Tests mit heutiger Hard- und Software problemlos zu leisten. Bei Millionen von E-Mails täglich lassen sich in der Regel nur die effizienteren Verfahren einsetzen.

In vielen Fällen ist es daher sinnvoll, schnelle und effiziente Verfahren vorzuschalten, um nur wenige nicht eindeutig erkannte E-Mails einem aufwendigerem Verfahren zu unterwerfen.

## Rückkopplung

Wurde eine E-Mail als Spam erkannt, so steigt die Wahrscheinlichkeit, dass ähnliche E-Mails ebenfalls Spam sind. Hat ein Rechner viel Spam und wenig Ham versandt, so ist die Wahrscheinlichkeit groß, dass auch weitere E-Mails vom gleichen Rechner Spam sein werden. Diese Tatsachen sind für eine Rückkopplung (*feedback*) der Antispam-Methoden nutzbar.

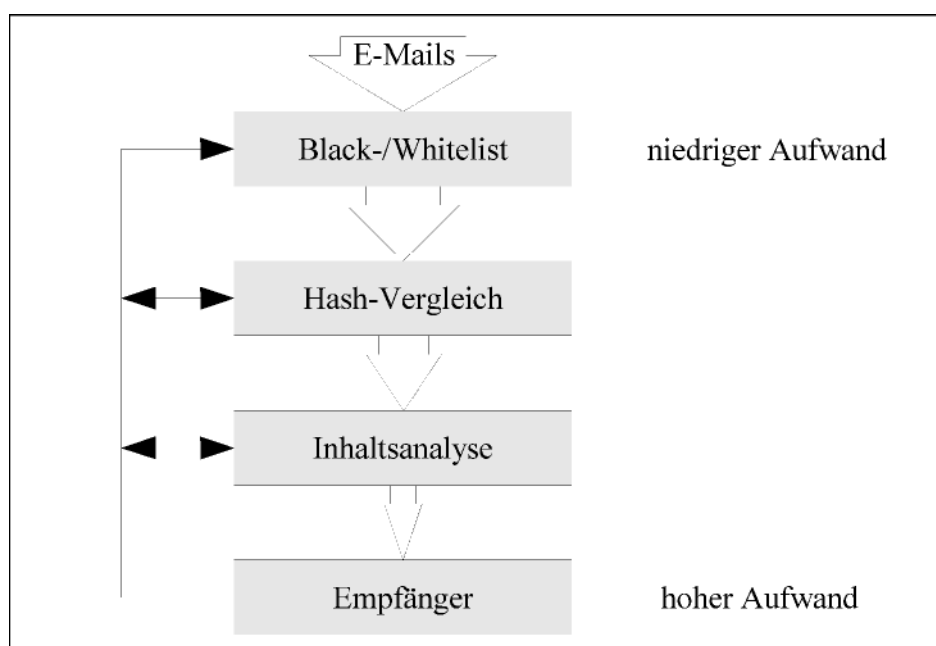


Abb. 8.8: Serielle Filterung mit Rückkopplung

Wenn inhaltsbasierte Filter einen Rechner als Spamquelle erfasst haben, können sie ihn in eine Blacklist eintragen. In Zukunft ist es dann einfacher und schneller möglich, E-Mails von diesem System abzulehnen. Ebenso ist erkannter Spam zum automatischen Training beispielsweise von Bayes-Filtern (siehe Kapitel 9.15) verwendbar. Dieses Verfahren geht von der Annahme aus, dass sich die Spam-Inhalte nur allmählich ändern, und soll die statistischen Filter nach und nach anpassen.

Der Wert der Rückkopplung besteht vor allem darin, dass ein aufwendiges, teures Verfahren in Zukunft durch einfachere, billigere Tests ersetzt werden kann. Man muss hier allerdings mit der nötigen Sorgfalt vorgehen, weil eine Rückkopplung falsche Einschätzungen verstärken kann. Typischerweise wird die Rückkopplung nur anwenden, wer sich seiner Entscheidung sehr sicher ist.

### Zusammenfassung

In der Praxis kommt meist eine komplexe Kombination der beschriebenen Verfahren zum Einsatz, die in der Kombination eine gute Erkennungsrate bei niedrigem Ressourcenbedarf verspricht. Grundsätzlich sinnvoll ist die Kombination von Verfahren, die auf verschiedenen Merkmalen (siehe Kapitel 8.1) beruhen.

Beispielsweise kann man als erste Stufe protokollbasierte Verfahren (siehe Kapitel 9.2) einsetzen, danach eine oder mehrere Blacklists (siehe Kapitel 9.3) abfragen und dann die Ergebnisse einer Inhaltsanalyse (siehe Kapitel 9.14 und 9.15) zu einem Scoring zusammenfassen. Das Ergebnis davon kann wiederum in die Blacklists der zweiten Stufe einfließen. Viele andere Kombinationen sind möglich, für ein weiteres Beispiel siehe [SCKL04].

#### Ein Kombinationsbeispiel

Spamversender benutzen heute massenhaft verseuchte PCs mit dynamischen IP-Adressen. Aus diesem Grund kommen viele gleiche oder ähnliche E-Mails einer Spam-Attacke aus vollkommen unterschiedlichen Netzbereichen. Das lässt sich als Filterkriterium an zentraler Stelle heranziehen:

- Ist der Inhalt der E-Mail bekannt, die IP-Adresse des Absenders jedoch nicht, handelt es sich wahrscheinlich um Spam.
- Genau anders herum verhält es sich bei Ham: Erwünschte E-Mails sind meistens noch nicht bekannt und entstammen immer wieder vorkommenden IP-Adressen. Da letzteres Kriterium auch für erwünschte Massensendungen wie Newsletter gilt, unterscheiden auch sie sich deutlich zumindest von denjenigen Spams, die von Zombies mit wechselnden IP-Adressen kommen.

Die Kombination von IP-Adresse mit einem Prüfsummen-Verfahren zur Wiedererkennung bekannter E-Mails ergibt also deutliche Hinweise für bestimmte Klassen von Spams [Unge04].

### 8.5.3 Einfluss durch den Anwender

Viele Verfahren unterscheiden sich darin, inwieweit der Mailempfänger auf die Filterung Einfluss nehmen kann. Manche Verfahren erlauben nur die Entscheidung für oder gegen den Einsatz, bei anderen kann der Anwender im Prinzip feinere Einstellungen vornehmen. In den meisten Fällen wird der Administrator aber die Verfahren vorgeben, da eine Einflussnahme durch den Anwender oft schwierig umsetzbar ist.

Aus rechtlicher Sicht ist zu bedenken, dass Filtereinstellungen der Empfänger personenbezogene Daten enthalten können und deshalb dem Datenschutz unterliegen.

## 8.6 Behandlung nach der Bewertung

Prinzipiell gibt es mehrere Möglichkeiten mit einer als Spam oder Ham bewerteten E-Mail zu verfahren. Sie kann – möglicherweise mit einer **Markierung** versehen – **zugestellt** werden. Wenn der MTA sich noch im SMTP-Dialog befindet, kann er sie **abweisen**. Außerdem kann er die E-Mail kommentarlos **löschen**. Eine erkannte Spam-Mail zu löschen und dem Absender eine **Fehlermeldung** (*bounce*) zu senden, ist in keinem Fall zu empfehlen, da nahezu alle Spam-Mails eine gefälschte Absenderadresse tragen und die *bounces* somit nicht zustellbar sind oder den Falschen erreichen (siehe auch [RFC3834]). Eine Sonderform ist die Zustellung in eine **Quarantänemailbox**.

### 8.6.1 Zustellen

Als Ham bewertete E-Mails müssen auf jeden Fall normal zugestellt werden. Schwieriger ist es, mit E-Mails umzugehen, die mit mehr oder weniger großer Sicherheit als Spam erkannt wurden. In vielen Fällen wird man sie aber auch dann zustellen, schon um die E-Mail nicht möglicherweise rechtswidrig zu unterdrücken.

Soll die Bewertung überhaupt einen Sinn haben, muss spamverdächtige E-Mail entweder in einen anderen Ordner oder in irgendeiner Weise markiert zugestellt werden (siehe unten).

### 8.6.2 Abweisen

Der MTA geht am sparsamsten mit den eigenen Ressourcen um, wenn er E-Mails möglichst frühzeitig ablehnt, denn er muss die E-Mail dann nicht auf Festplatte speichern und nicht weiterleiten. In vielen Fällen ist das die beste Lösung. Sie setzt allerdings voraus, dass der verwendete MTA eine E-Mail schon während des SMTP-Dialogs als Spam erkennen kann. Ältere Software ist dazu häufig nicht in der Lage. Inzwischen unterstützen aber fast alle Produkte ein entsprechendes Vorgehen oder bieten zumindest die Möglichkeit, eine solche Funktion einzubauen.

Vorteil dieser Lösung ist, dass der Absender im Falle eines *false positive*, also der irrtümlichen Abweisung einer Ham-Mail, erfährt, dass seine Nachricht nicht zugestellt wurde.

Nachteil dieser Methode ist, dass sie in der Regel keine benutzerspezifischen Kriterien für die Filterung verwenden kann. Das liegt einerseits an der Architektur der MTAs, die zum Zeitpunkt der Annahme der E-Mail häufig noch nicht wissen, in welche Mailbox eine E-Mail am Ende zuzustellen ist. Andererseits gibt es auch ein Problem mit dem SMTP. Der Absender einer E-Mail kann mehrere Empfänger für eine E-Mail angeben, die im SMTPDialog als mehrere *RCPT-TO*-Kommandos erscheinen. Zwar kann der Empfänger-MTA die E-Mail für einzelne Empfänger annehmen und für andere ablehnen, aber zu diesem Zeitpunkt im SMTP-Dialog hat er den Inhalt der E-Mail noch nicht gesehen, alle Verfahren, die eine Inhaltsanalyse erfordern, können also nicht greifen.

Vorsicht bei dieser Methode ist auch angebracht, wenn Mailinglisten im Spiel sind. Die Mailinglisten-Software löscht einen Benutzer häufig automatisch aus der Abonnentenliste, wenn sie eine E-Mail nicht zustellen kann. Sie nimmt fälschlicherweise an, dass die Mailadresse nicht mehr existiert.

Statt einer endgültigen Fehlermeldung (*permanent negative completion reply*) kann der MTA auch eine temporäre Fehlermeldung (*transient negative completion reply*) zurückgeben.<sup>18</sup> Der Provider des Absenders hat so eventuell die Chance, eine fehlerhafte Filterung zu erkennen und korrigierend einzugreifen, ohne dass der Endanwender etwas davon merkt. Sollte etwa ein legitimer Mailserver auf eine Blacklist geraten sein, kann der Betreiber des Mailservers eine Löschung veranlassen und

---

<sup>18</sup> Also eine Fehlermeldung mit einem 4xx- statt 5xx-Code, siehe [RFC2821], Abschnitt 4.2.1

dann eine erneute Zustellung versuchen. Spammer unternehmen hingegen meist keinen weiteren Zustellversuch (siehe auch das Greylisting-Verfahren in Kapitel 9.13).

### 8.6.3 Löschen

E-Mails kommentarlos zu löschen kommt kaum in Betracht. Niemand bekommt etwas davon mit, fehlerhafte Klassifizierungen sind nicht erkennbar und es gibt keine Möglichkeit, eine E-Mail nachträglich wiederzubeschaffen. Zudem verbietet der Mailstandard RFC 2821 [RFC2821] das Löschen der E-Mail.<sup>19</sup>

Ganz anders ist die Situation bei erkannten Viren und Würmern. Hier ist es durchaus sinnvoll, die E-Mail nicht zuzustellen, da die Wahrscheinlichkeit, dass eine E-Mail fälschlicherweise als Virus klassifiziert wurde, viel niedriger ist als die Wahrscheinlichkeit einer Fehlklassifizierung als Spam. Darüber hinaus ist der Schaden, den ein Virus oder Wurm anrichten kann, viel größer als der potentielle Schaden durch Spam.

### 8.6.4 Markieren

Als Spam oder Ham bewertete E-Mails sollten vor der Zustellung entsprechend markiert werden. Typischerweise bringt Antispam-Software sowohl bei Spam als auch bei Ham eine Markierung an, die häufig die Wahrscheinlichkeit der Einschätzung als Spam enthält und weitere Details über die Kriterien der Bewertung. Dem MUA oder dem Anwender stehen damit genug Informationen für eine eigene Entscheidung zur Verfügung. Der MDA oder der MUA kann die „spamverdächtige“ E-Mail in eine spezielle Spam-Mailbox einstellen, die der Benutzer von Zeit zu Zeit durchsieht.

Die Markierung der E-Mails kann mit speziellen Header-Zeilen oder in der Subject:-Zeile erfolgen. Viele MUAs können eingehende E-Mails nach diesen Zeilen filtern und dem Benutzer in anderer Form präsentieren.

### Beispiel für Header-Zeilen, wie sie „SpamAssassin“ erzeugt

X-Spam-Level: \*\*\*\*\*

X-Spam-Checker-Version: SpamAssassin 2.60 (1.212-2003-09-23-exp) on [host.example.com](http://host.example.com)

X-Spam-Status: Yes, hits=6.7 required=4.6 tests=BAYES\_00, BIZ\_TLD, FROM\_ENDS\_IN\_NUMS, MISSING\_MIMEOLE, MISSING\_OUTLOOK\_NAME, URI OFFERS, USERPASS, X\_PRIORITY HIGH, X\_PRI MISMATCH HI

X-Spam-flag: YES

Nachteil dieser Methode ist der hohe Ressourcenbedarf. Unter Umständen müssen große Mengen von E-Mails weitergeleitet werden, obwohl die weitere Verwendbarkeit fraglich ist. Probleme sind absehbar, wenn der Endnutzer über eine langsame Modemleitung an das Internet angebunden ist, denn dann kann das Herunterladen aller E-Mails sehr lange dauern.

Auch Markierungen im *header* einer E-Mail sind fälschbar. Ein Spammer kann seine E-Mails vor dem Versenden als „sauber“ markieren, wenn er das Format der Markierung kennt. Der MDA oder MUA sollte daher zuerst nach einer Spam-Markierung und nur bei deren Fehlen nach einem Ham-Hinweis suchen. Eventuell kann man im MTA auch alle Markierungen, die das gleiche Format wie die eigene haben, löschen, bevor er seine eigene anbringt. Es gibt auch die Möglichkeit, die

---

<sup>19</sup> „In sending a positive completion reply to the end of data indication, the receiver takes full responsibility for the message (see section 6.1). Errors that are diagnosed subsequently MUST be reported in a mail message, as discussed in section 4.4.”

Markierung durch digitale Signaturen oder ähnliche Verfahren abzusichern. Zurzeit verwendet jede Software eine andere (meist konfigurierbare) Methode der Markierung. Es gibt aber bereits Bestrebungen zu einer Vereinheitlichung.

Markieren und Zustellen in einen Spamfolder kommt bei Anwendern mit hoher Spam-Belastung praktisch einem verzögerten Löschen gleich. Erfahrungsgemäß suchen sie im Spamfolder nur dann etwas, wenn eine erwartete E-Mail nicht im normalen Eingangsordner auftaucht, und beschränken sich sonst verständlicherweise auf ein gelegentliches grobes Durchsehen.

### Die Filtersprache Sieve

Manche Software unterstützt die standardisierte Mailfilter-Sprache Sieve<sup>20</sup> [RFC3028], mit der ein Anwender (in eingeschränkter Weise) einen persönlichen Mailfilter implementieren kann. Ihm stehen Optionen offen wie die Zuordnung von E-Mails in Mailboxen anhand der Informationen im *header* und dergleichen. Sieve ist begrenzt für die Spamfilterung selbst geeignet, aber sehr gut, um von Antispam-Software geschriebene Header-Zeilen auszuwerten und danach zu handeln:

```
if header :contains „Subject“ „[Spam]“ { fileinto „spamfolder“ }
```

In diesem Beispiel würde jede E-Mail, die im Betreff den Text „[Spam]“ enthält (den vielleicht der zentrale Mailfilter eingefügt hat), in einen speziellen Spamfolder zugestellt.

### 8.6.5 Unter Quarantäne stellen

Es gibt Antispam-Software, die spamverdächtige E-Mails unter Quarantäne stellen kann. Der Anwender prüft sie mit einem speziellen Client oder über ein Webinterface und gibt sie frei oder löscht sie endgültig.

Im Prinzip ist eine Quarantäne nicht viel mehr als ein spezielles Postfach. Durch die Trennung sind aber einige Funktionen einfacher oder übersichtlicher implementierbar. So kann man in der Quarantäne-Box die E-Mails nach ihrer Spamwahrscheinlichkeit sortieren. E-Mails, die möglicherweise kein Spam sind, erscheinen dann in der Übersicht zuerst. Für manche Firmen kann es sinnvoll sein, eine Quarantäne-Box pro Abteilung oder sogar nur eine Box für die ganze Firma einzurichten. Ein Mitarbeiter kann die Vorfilterung übernehmen, um die Kollegen zu entlasten.

Die Quarantänemailbox sollte bei Anzeige der spamverdächtigen E-Mails keine externen Bilder oder andere Inhalte laden und Links in E-Mails abschalten, um zu verhindern, dass ein Anwender (un)absichtlich dem Spammer die Auslieferung der E-Mail anzeigt (siehe Kap. 4.3.4).

Schließlich kann die Quarantäne-Box auch die Spamfilterung verbessern, indem die Antispam-Software die Ergebnisse der manuellen Filterung direkt zum Trainieren ihres Filters benutzt. Die Handhabung ist hier viel einfacher als bei getrennten Mailboxen im Client des Anwenders.

### 8.6.6 Auswahl des Verfahrens

Die Anwendung eines Verfahrens oder einer Kombination von Verfahren hängt von den Umständen ab. In vielen Fällen ist eine Kombination sinnvoll. E-Mails, die mit hoher Wahrscheinlichkeit oder aus formalen Gründen als Spam erkannt wurden, werden direkt abgelehnt, andere in einen Spamordner zugestellt.

Ein mobiler Benutzer mit einer langsamen Verbindung wird dann nur E-Mails in seiner regulären Inbox lesen. Sobald er wieder in der Firma ist, kann er dort auch seinen Spamordner prüfen.

---

<sup>20</sup> <http://www.cyrusoft.com/sieve/>

### **8.6.7 Ausnahmen**

Für die Postmaster-Adresse (siehe RFC 2821, Abschnitt 4.5.1) und für Adressen, über die ein Abuse-Helpdesk erreichbar ist ([abuse@example.com](mailto:abuse@example.com)), sind meist Ausnahmen bei der Spamfilterung erforderlich. Sonst wird es für Anwender und andere Postmaster in vielen Fällen schwierig sein, sich zu beschweren, wenn sie z. B. eine Spam-Mail im Anhang als Beweis anfügen und dadurch die Beschwerde im Spamfilter hängen bleibt.

## 9 Antispam-Maßnahmen: Einzelne Verfahren

Dieses Kapitel listet die meisten derzeit bekannten Antispam-Maßnahmen und ihre Funktion auf. Es erklärt, welche Merkmale diese Methoden zur Unterscheidung zwischen Ham und Spam heranziehen und beleuchtet die Maßnahmen nach verschiedenen Kriterien. Die Verfahren sind über die Jahre entstanden und häufig geändert und ausgebaut worden. Sie müssen Rücksicht nehmen auf bestehende Protokolle und gewachsene Strukturen im weltweiten Mailsystem und sich immer wieder an neue Methoden der Spammer anpassen.

| Kap. | Maßnahme                              | Aufwand | Effektivität | Kap. | Maßnahme                                       | Aufwand | Effektivität |
|------|---------------------------------------|---------|--------------|------|--|---------|--------------|
| 9.1  | Filterung durch Personen              | -       | +            | 9.12 | RHSBLs   | O       | -            |
| 9.2  | Protokollbasierte Verfahren           | *1      |              | 9.13 | Greylisting                                    | O       | +            |
| 9.3  | White- und Blacklists                 | +       | O            | 9.14 | Heuristische Inhaltsanalyse                    | O       | +            |
| 9.4  | DNS-basierte Blacklists (DNSBLs)      | O       | +            | 9.15 | Statistische Inhaltsanalyse                    | -       | +            |
| 9.5  | IP-Blacklisting durch Frequenzanalyse | O       | O            | 9.16 | Prüfsummenvergleich                            | -       | +            |
| 9.6  | Sperre des SMTP-Ports                 | *3      |              | 9.17 | URIDNSBLs                                      | O       | +            |
| 9.7  | MTAMARK                               | +       | *2           | 9.18 | Tokenbasierte und Challenge-Response-Verfahren | -       | +            |
| 9.8  | Existenzprüfung der Absenderadresse   | -       | O            | 9.19 | Proof-of-Work-Verfahren                        | -       | *2           |
| 9.9  | MARID-Verfahren: SPF und SenderID     | +       | -            | 9.20 | E-Mail-Briefmarken                             | -       | *2           |
| 9.10 | S/MIME und PGP                        | -       | O            | 9.21 | Bounce Address Tag Validation (BATV)           | O       | O            |
| 9.11 | MASS-Verfahren: DomainKeys und IIM    | O       | -            | 9.22 | Spamfallen                                     |         | *3           |

Aufwand: -: hoch O: mittel +: niedrig  
 Effektivität: -: niedrig O: mittel +: hoch

\*1 Einzelne Verfahren sehr verschieden  
 \*2 Keine Aussage, da nicht/kaum verbreitet  
 \*3 Nicht zur Filterung eingehender E-Mail

Tabelle 9.1: Aufwand und Effektivität von Filter-Maßnahmen beim Empfänger

Den Anfang macht die klassische **Filterung durch einen Menschen (9.1)**, die auch in Zukunft als letzte Maßnahme nötig bleiben wird. Danach geht es um **Verfahren, die Eigenheiten in der Benutzung von SMTP nutzen (9.2)** und IP-basierte Verfahren: **White- und Blacklists allgemein (9.3)**, **DNS-basierte Blacklists (9.4)** sowie um **IPBlacklisting durch Frequenzanalyse (9.5)**. Hier lassen sich auch die **SMTP-Port-Sperre (9.6)** und **MTAMARK (9.7)** einordnen.

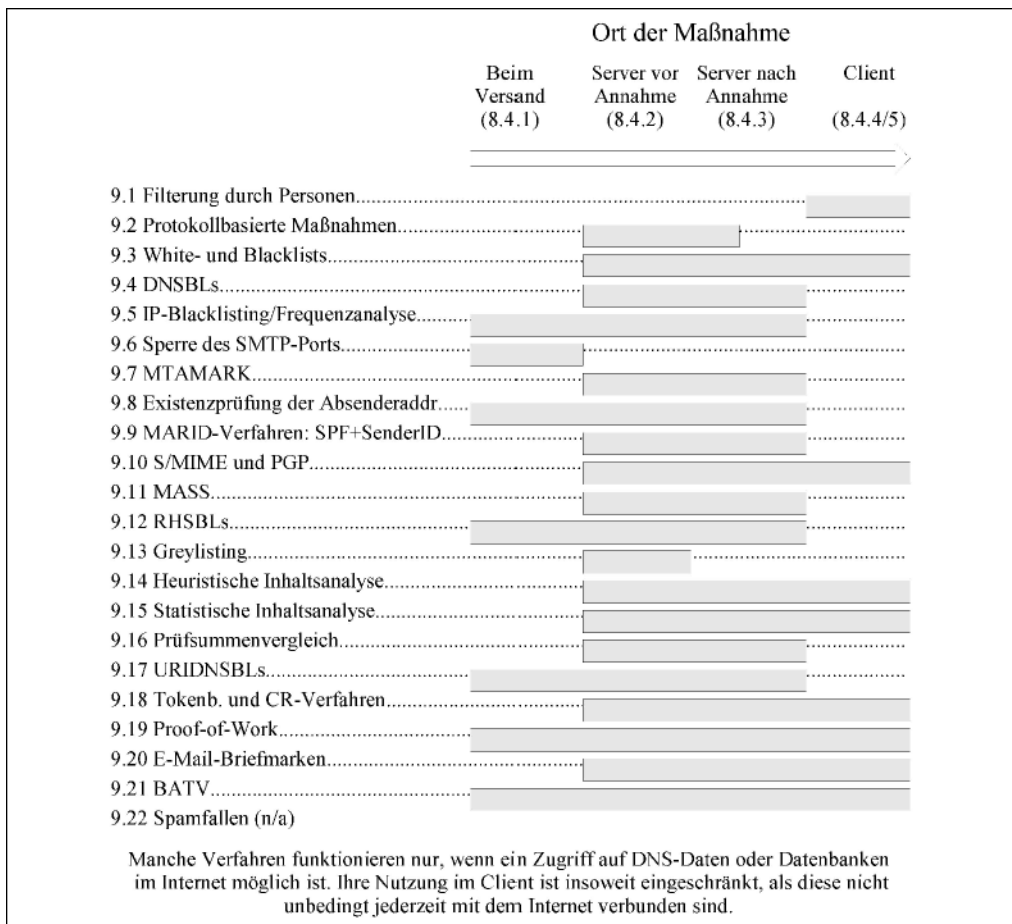


Abb. 9.1: Zuordnung der Maßnahmen zum Ort der Filterung

Die folgenden Verfahren basieren auf der Absenderadresse oder -domain. Dazu gehören die **Existenzprüfung der Absenderadresse (9.8)** und die Verfahren zur Absenderauthentifizierung in ihren vielfältigen Varianten: Die DNS-basierten **MARID-Verfahren SPF und SenderID (9.9)**, die kryptographische Authentifizierung mit **S/MIME und PGP (9.10)** und die **MASS-Verfahren (9.11)**. Daran schließt sich die Beschreibung von **RHSBL (9.12)** an, ein domainbasiertes Reputationsverfahren.

Spammer unternehmen selten einen zweiten Zustellversuch, wenn der erste misslingt. Das **Greylisting (9.13)** macht sich diese Tatsache zunutze und lehnt alle E-Mails beim ersten Versuch ab – in der berechtigten Annahme, dass fast nur noch Ham durchkommt.

Das nächste Thema ist die Inhaltsanalyse, die in **heuristischen (9.14)**, **statistischen (9.15)** (deren bekanntester Vertreter die Bayes-Filterung ist) und **kollaborativen Verfahren (9.16)** zum Einsatz kommt. **URIDNSBLs (9.17)** sind ein Sonderfall inhaltsbasierter Reputationsverfahren.

Es folgen einige weitere „vermischte“ Verfahren, die sich nicht ohne weiteres einem Schema unterordnen lassen. **Tokenbasierte Verfahren (9.18)** erwarten bestimmte Zeichenketten in einer E-Mail oder in einer Mailadresse, um die E-Mail durchzulassen. Sind die Token nicht vorhanden, wird der Absender aufgefordert, eines nachzuliefern oder sich anderweitig (*out of band*) zu melden (**Challenge-Response (9.18)**).

Bei **Proof-of-Work-Verfahren (9.19)** muss der Absender beweisen, dass er einen gewissen Rechenaufwand getrieben hat, bevor er eine E-Mail versenden darf. Ein Spammer, der große Mengen an E-Mails versendet, muss dafür viel CPU-Leistung vorhalten.

Für die Zukunft immer wieder vorgeschlagen, aber noch nirgends umgesetzt, ist die Nutzung von **Briefmarken (9.20)** für E-Mails. Der Versand kostet dann Geld, das der Spammer ungern aufbringt.

Zur Erkennung von *bounces*, die nicht von eigenen E-Mails ausgelöst wurden, dient schließlich das **BATV-Verfahren (9.21)** (Bounce Address Tag Validation).

Ganz aus dem Rahmen fällt die Einrichtung von **Spamfallen (9.22)**, die nicht direkt der Filterung dienen, sondern der Optimierung der Filtermaßnahmen.

## 9.1 Filterung durch Personen

Das Ziel jeder Antispam-Maßnahme ist die möglichst weitgehende Vermeidung der manuellen Spamfilterung. Da aber kein automatischer Filter perfekt arbeitet, wird der Anwender auch in Zukunft gelegentlich Spams selbst löschen müssen.

Die manuelle Filterung oder zumindest die Durchsicht ist besonders dann notwendig, wenn man E-Mails weiterleitet und keinesfalls selbst Spams weiterverbreiten möchte: Viele Betreiber von Mailinglisten erlauben beispielsweise nur E-Mails von bekannten Absendern auf ihrer Liste. E-Mails von Unbekannten prüft der Listenverwalter manuell, bevor er sie akzeptiert.

Bei der manuellen Filterung werden Spam-Mails entweder gelöscht oder in einen Spamordner verschoben. Zusätzlich kann erkannter Spam auch zum Trainieren verwendet (siehe Kapitel 9.15) oder gemeldet werden, z. B. an eine zentrale Blacklist oder an eine Prüfsummendatenbank (siehe Kapitel 9.16). Die manuelle Filterung wird in der Regel im MUA durchgeführt, alternativ kann sie auch mittels spezieller Software in einer Quarantänebox erfolgen (siehe Kapitel 8.6.5).

Bei manueller Filterung ist außerdem zu bedenken, dass auch Menschen nicht perfekt sind und ab und zu eine E-Mail zuviel löschen. Automatische Filterverfahren können durchaus kleinere False-Positive-Raten erreichen als die manuelle Filterung. William S. Yerazunis, der Autor des Filterprogrammes CRM114, schreibt dazu:

„I measured my own accuracy to be around 99.84 %, by classifying the same set of about 3000 messages twice over a period of about a week, reading each message from the top until I feel „confident“ of the message status, (one message per screen unless I want more than one screen to decide on a message.) and doing the classification in small batches with plenty of breaks and other office tasks to avoid fatigue. Then I diff()ed the two passes to generate a result. Assuming I never duplicate the same mistake, I, as an unassisted human, under nearly optimal conditions, am 99.84 % accurate.“<sup>1</sup>

Aus juristischer Sicht berührt die manuelle Mailfilterung in besonderem Maße die Belange des Datenschutzes, wenn sie über den eigenen Posteingang hinaus für mehrere Anwender zentral stattfindet. Da bei diesem Verfahren nicht auszuschließen ist, dass der Filternde vertrauliche oder private E-Mails in Augenschein nimmt, ist die manuelle Einsichtnahme im Rahmen der Filterung ausschließlich bei vorheriger, am besten schriftlicher Zustimmung der Betroffenen möglich. Diese Maßnahme erfordert gerade beim Einsatz in Unternehmen, bei Providern oder Behörden besondere Vorsicht, um einem Missbrauch vorzubeugen. Rechtlich unbedenklich ist dagegen die manuelle Filterung durch den Empfänger der Nachricht.

## 9.2 Protokollbasierte Maßnahmen

Der Übertragung von E-Mail liegt in der Regel das Protokoll SMTP zugrunde. Viele seiner Details lassen sich mehr oder weniger streng auslegen. Die meisten MTAs halten sich recht gut an die Regeln, während Spam-Software häufig laxer damit umgeht oder etwas andere Charakteristika zeigt. Eine strengere Auslegung der Regeln kann daher einen Teil des Spams abfangen. Da auch legitime Mailsoftware oft nicht perfekt ist, müssen solche Systeme durch ein Whitelisting von der Filterung ausgenommen werden.

---

<sup>1</sup> <http://crm114.sourceforge.net/>

Außerdem lassen sich diverse Domain- und Hostnamen sowie Mailadressen, die der Absender angibt, auf Gültigkeit oder zumindest Plausibilität prüfen.

Es folgt eine Auflistung verschiedener Verfahren, die im MTA einsetzbar sind:

a) EHLO/HELO-Check

Nach der Begrüßung durch den Server schickt der Client im SMTP-Dialog eine *EHLO*-oder *HELO*-Zeile mit seinem Hostnamen (siehe [RFC2821], Abschnitt 4.1.1.1). Versucht der Client eine E-Mail abzusetzen, ohne ein *EHLO/HELO* zu schicken (RFC2821, Abschnitt 4.1.1.1, Absatz 2) oder gibt er einen syntaktisch falschen Hostnamen an, liegt ein Protokollverstoß vor. Viele Spammer verwenden die IP-Adresse (gelegentlich auch den Hostnamen) des Rechners, dem sie die E-Mail schicken (oder eine Localhost-Adresse, 127.0.0.0/8), auch darauf kann gefiltert werden (wobei man bei lokaler Zustellung – vom eigenen Rechner zum eigenen Rechner – aufpassen muss). Zudem ist über einen Reverse-Lookup auch der angegebene Name überprüfbar (RFC 2821, Abschnitt 4.1.4, Absatz 5), allerdings darf darauf streng genommen wohl nicht gefiltert werden (RFC 2821, Abschnitt 4.1.4, Absatz 6). Manche MTAs tragen in der *Received*:-Zeile sowohl den *HELO*-Namen als auch den echten Hostnamen ein, so dass der *HELO*-Check nicht nur dem MTA vorbehalten ist. Verdächtig sind auch Rechner, die ihren *HELO*-Namen häufig ändern.

b) SMTP-Pipelining

Beim SMTP treten Absender und Empfänger in einen Dialog. Jede Seite muss auf die Antwort der anderen Seite warten, bevor sie neue Kommandos oder Daten schicken darf. Viele Spammer halten sich nicht daran und senden alle Kommandos auf einmal, weil es schneller und einfacher ist. Die Eindeutigkeit dieses Kriteriums ist allerdings dadurch eingeschränkt, dass die meisten Mailserver heute ESMTP mit der PIPELINING-Erweiterung [RFC2920] verwenden, die es dem Client erlaubt, die Kommandos auf einmal zu versenden, ohne auf die Antwort des Servers zu warten. Diese Erweiterung lässt sich aber im Server-MTA abstellen. In jedem Fall wartet aber ein korrekt implementierter MTA nach dem HELO/EHLO und DATA die Antworten ab (RFC 2920, Abschnitt 3.1, Absatz 1).

c) Nutzung von TLS (Transport Layer Security)

TLS dient zur Verschlüsselung der SMTP-Verbindung. Für Spammer ist TLS unattraktiv, da der Aufwand dazu recht hoch ist. Die Nutzung von TLS ist also (zurzeit) ein Hinweis auf Ham. Da sie aber auf den Mailservern zu deutlich mehr Last führt, kommt sie selten zum Einsatz. Aus Gründen der Vertraulichkeit sollte TLS jedoch möglichst aktiviert sein.

d) Filterung auf leeres MAIL FROM

Eine leere MAIL-FROM-Adresse kennzeichnet *bounces*. Eine Filterung auf leere Adressen kann viele *bounces* (siehe Kapitel 3.2.7) unterdrücken, darunter allerdings auch legitime bounces, was die Zuverlässigkeit und Funktionsfähigkeit des Mailsystems gefährdet. Dieses Verfahren sollte deshalb im Normalbetrieb nie eingesetzt werden. Gegen „echten“ Spam ist das Verfahren ohnehin unwirksam, da er selten mit leerer MAIL-FROM-Adresse versandt wird. Etwas anders sieht es aus, wenn eine E-Mail mit leerem Envelope-From an mehrere Empfänger geht. Bei einer bounce kann das nie vorkommen, die Wahrscheinlichkeit, dass es sich hier um Spam handelt, liegt also deutlich höher. Wenn ein Spammer unter der Mailadresse eines Dritten große Mengen an Spam verschickt und derjenige daraufhin sehr viele bounces bekommt, kann er eventuell vorübergehend auch auf ein leeres MAIL FROM filtern, wenn sein Mailserver sonst unter der Last zusammenbrechen würde.

e) Besondere Filterregeln auf dem Secondary MX

MTAs verwenden *DNS MX (mail exchanger) records*, um zu entscheiden, wohin sie E-Mails für eine bestimmte Domain senden sollen. Neben dem Hostnamen enthalten *MX records* auch eine Priorität. Der (oder die) Mailserver mit der höchsten Priorität heißt *primary MX*, alle weiteren *secondary MX*. Spammer senden gerne an den *secondary MX*, weil er häufig schlechter geschützt ist als der Haupt-MTA, z. B. wenn es sich um einen Backup-MX handelt, den ein Dritter betreibt.

Das kann man sich bei der Filterung zunutze machen. Es ist allerdings Vorsicht geboten, da auch legitime MTAs E-Mails an den *secondary MX* versenden können, obwohl der *primary MX* online ist. Das kann z. B. passieren, wenn die Netzwerkverbindung kurzzeitig gestört war. Sollte der *primary MX* wegen eines Ausfalls nicht erreichbar sein, so muss man den *secondary MX* bei Einsatz dieses Verfahrens eventuell umkonfigurieren, um die Verfügbarkeit des Mailsystems zu gewährleisten.

f) Ausnutzen von Timeouts

RFC 2821 schlägt für verschiedene Phasen und Kommandos im SMTP verschiedene Timeouts vor (Abschnitt 4.5.3.2). Da Spamssoftware es immer eilig hat, nutzt sie vielleicht kürzere Timeouts und bricht die Übertragung ab. Reguläre Mailsoftware hält sich dagegen meist an die vorgeschlagenen Timeouts. Ein Nachteil ist die verzögerte Auslieferung regulärer E-Mails, die sowohl im Server als auch im Client Ressourcen bindet.

### Teergruben

Teergruben<sup>2</sup> (engl. *tar pits*) dienen dazu, beim Spammer Ressourcen zu binden und ihn möglichst lange hinzuhalten, damit er weniger E-Mails ausliefern kann. Technisch gesehen werden dazu die Antworten in einer SMTP-Verbindung Zeile für Zeile mit großem zeitlichen Abstand geschickt (zu mehrzeiligen Antworten siehe [RFC2821], Abschnitt 4.2.1). Nachteil des Verfahrens ist, dass auch der Empfänger die Verbindung geöffnet lassen muss, der Ressourcenbedarf also steigt.

Solange nur wenige Teergruben anwenden, ist deren Wirksamkeit sehr fraglich, da erst die Masse einen spürbaren Erfolg erreichen würde.<sup>3</sup> Außerdem tritt der Erfolg weniger beim Betreiber selbst auf als bei anderen Empfängern. Die wenigsten werden also zu diesem Verfahren greifen.

Für das Verfahren sind die Namen *teergrubing* und *tarpitting* in Gebrauch.

Wunder kann man von keinem dieser Verfahren erwarten, viel Spam bleibt unerkannt. Die meisten sind jedoch relativ einfach und kostengünstig umzusetzen, brauchen in der Regel, außer zur Definition seltener Ausnahmen, keine Administration und stoppen den Spam schon sehr früh. Zudem sind sie in der Regel juristisch unbedenklich. Deshalb kann sich ihr Einsatz trotzdem lohnen. Insbesondere für große Mailsysteme kann der Aufwand für die Pflege der Ausnahmelisten den Nutzen jedoch überschreiten.

Alle Verfahren sind von Spammern im Prinzip ohne erheblichen Aufwand zu umgehen, es ist also damit zu rechnen, dass die Effektivität laufend sinkt. Dafür wird es künftig wahrscheinlich mehr und mehr dieser Tricks geben, die auch immer komplexer werden. Spam, der von Botnetzen ausgeht, verrät sich z. B. manchmal dadurch, dass die DNS-MXAnfrage aus einem ganz anderen Netz kommt als die dann folgende SMTP-Verbindung. Durch ein Zusammenwirken von DNS-Server und Mailserver ergäbe sich also eine weitere Klassifizierungsmöglichkeit.

## 9.3 White- und Blacklists

White- und Blacklists enthalten Adressen, von denen nur Ham oder nur Spam zu erwarten ist. Je nach Art der Liste können sie entweder die IP-Adresse des sendenden Rechners oder die Absenderadresse oder Absenderdomain speichern und lassen sich sowohl im MTA als auch im MUA einfach einrichten. Sie müssen ständig auf dem aktuellen Stand sein, um Fehlklassifizierungen zu vermeiden.

---

<sup>2</sup> <http://www.iks-jena.de/mitarb/lutz/usenet/teergrube.html>

<sup>3</sup> Da Spammer heute oft Botnetze zum Spamversand benutzen, haben sie so große Ressourcen, dass der Erfolg noch unwahrscheinlicher wird.

In der Frühzeit der Spamfilterung war es üblich, Listen erwünschter oder unerwünschter Absenderadressen zu führen. Mailadressen sind jedoch anders als IP-Adressen beliebig fälschbar. Weil Spammer davon reichlich Gebrauch machen, hat es praktisch keinen Sinn mehr, Absenderadressen eingehender E-Mails mit denen bekannter Spams zu vergleichen. Etwas nützlicher sind Whitelists der Mailadressen bekannter Absender, doch diese bedürfen eines erheblich höheren Pflegeaufwands als etwa Listen von IP-Adressen und lassen sich wegen der einfachen Fälschbarkeit der From-Adresse relativ einfach unterlaufen.

Insbesondere Whitelists werden heute noch häufig manuell mitgeführt. Versender von legitimer Massenmail, z. B. große Versandhäuser, und Mailinglistenserver müssen häufig auf Whitelists eingetragen werden, weil sie sonst einer automatischen Spamererkennung zum Opfer fallen können. Lokale, manuell gepflegte White- und Blacklists sind deswegen auch heute noch notwendig, um (kurzfristig) Fehlklassifizierungen anderer Verfahren zu korrigieren.

## 9.4 DNS-basierte Blacklists (DNSBLs)

Erfahrungsgemäß kommt in sehr vielen Fällen von einer IP-Adresse entweder nur Spam oder nur Ham. Schon früh entstand deshalb die Idee, Listen von IP-Adressen der Spammer anzulegen und öffentlich zu verbreiten.

Für einen schnellen und einfachen Zugriff auf die Listen wurde das Domain Name System zweckentfremdet. Über eine bestimmte DNS-Anfrage kann man feststellen, ob eine IP-Adresse unter Spamverdacht steht oder nicht. Mit der Zeit haben sich immer mehr Listen etabliert, die alle die gleiche zugrunde liegende DNS-Technik benutzen, sich aber darin unterscheiden, welche IP-Adressen sie aufnehmen.

Als Oberbegriff für all diese Listen dient der Name DNSBL (Domain Name System Blacklist / Blackhole List / Blocklist / Blocking List). Die häufig verwendete Bezeichnung RBL (wobei das „R“ für „Realtime“ steht) bezieht sich streng genommen auf eine spezielle Art der DNSBL, die Kelkea Inc. (früher MAPS<sup>4</sup>) anbietet.

Viele DNSBLs werden von Hobbyisten und kleinen Antispam-Organisationen betrieben und sind meist kostenlos nutzbar. Andere sind erst nach Zahlung einer Lizenzgebühr zugänglich.

Die Nutzung von DNSBLs ist relativ einfach möglich. Sie können (je nach Policy des Betreibers) mehr oder weniger effektiv sein und werden es wahrscheinlich in Zukunft auch bleiben. DNSBLs fragt in der Regel der MTA ab, der die IP-Adresse des einliefernden Rechners überprüft und die Annahme der Spam-Mail unmittelbar verweigern kann. Für die Nutzung im MUA eignet sich die Abfrage von DNSBLs weniger, da man dort nicht unbedingt über einen ständigen Internet-Zugang verfügt, der für DNSBL-Abfragen notwendig ist.

Die meisten DNSBLs verzeichnen, wie beschrieben, IP-Adressen. Der gleiche DNS-Mechanismus ist aber durchaus auch für andere Daten, etwa die Absenderdomain (RHSBLs, siehe Kapitel 9.12), und im Inhalt vorkommende URLs (URIDNSBLs, siehe Kapitel 9.17) verwendbar.

### 9.4.1 Technik der DNSBLs

Die Abfrage einer DNSBL funktioniert ähnlich wie der IP-Reverse-Lookup im DNS. Wenn ein MTA eine IP-Adresse bei einer DNSBL überprüfen will, nimmt er die vier Zahlen der IP-Adresse in der umgekehrten Reihenfolge, hängt den Zonen-Namen der DNSBL an und löst diesen Namen per DNS auf. Will er beispielsweise die IP-Adresse 192.0.2.1 in der DNSBL dnsbl.example.com überprüfen, so ergibt sich 1.2.0.192.dnsbl.example . com. Ergebnis der DNS-Abfrage ist zumeist ein Pseudo-Adress-

<sup>4</sup> <http://www.mail-abuse.com/>

Eintrag im Bereich 127.0.0.0/8, in dem das Ergebnis kodiert ist (oder eine Fehlermeldung, wenn kein Eintrag vorliegt).

Einfachere Listen geben ausschließlich 127.0.0.2 zurück, wenn der Eintrag existiert. Manche Listen haben aber mehrere Rückgabewerte, in denen z. B. der Grund der Auflistung kodiert ist. Deren Bedeutung ist von Liste zu Liste unterschiedlich und der jeweiligen Anleitung zu entnehmen.

Einige Listen enthalten zusätzlich TXT-Records zur Beschreibung, die für eine SMTP-Fehleroder Logmeldung geeignet sind.

Zur Abfrage von DNSBLs lassen sich die üblichen DNS-Clients und -Bibliotheken nutzen. MTAs und Antispam-Software haben diese Funktion heute meist bereits eingebaut. Auch serverseitig kann man traditionelle DNS-Software ( z. B. BIND<sup>5</sup>) einsetzen. Es gibt auch spezielle Software<sup>6</sup>, die für den Betrieb von DNSBLs optimiert ist. Sie ist einfacher zu konfigurieren und vor allem performanter und ressourcenschonender.

Um nicht jedesmal eine DNS-Abfrage über das Internet durchführen zu müssen, stehen manche DNSBLs auch komplett zum Herunterladen zur Verfügung.<sup>7</sup> Die Daten werden dann lokal zwischengespeichert und abgefragt, was die Geschwindigkeit, Verfügbarkeit und Vertraulichkeit erhöht. Manche Systeme unterstützen das Rsync-Verfahren<sup>8</sup>, das nur die laufenden Änderungen und nicht jedesmal die komplette Datenbank überträgt.

#### 9.4.2 Policies

Jede DNSBL hat eine Policy, die angibt, welche IP-Adressen auf der Liste eingetragen werden und welche nicht. In manchen Fällen ist die Policy auf den Webseiten des Betreibers genau erklärt, in anderen nicht.

Es gibt eine ganze Reihe von Fragen, die eine Policy klären sollte:

- **Welche IP-Adressen werden aufgenommen?** Sind es die IP-Adressen von bekannten Spammern? Oder solche, von denen jemand in letzter Zeit Spam bekommen hat? Rechner, die als offene Relays oder offene Proxies erkannt wurden? Dynamische IP-Adressen? Werden nur einzelne IP-Adressen oder sogar ganze IP-Netze aufgenommen? Manche Listen nehmen bei wiederholten Verstößen nicht nur einzelne IP-Adressen, sondern ganze Netze auf. Das kann vor allem bei dynamischen IP-Adressen sinnvoll sein, aber auch zu mehr *false positives* führen.
- **Wer kann einen Eintrag vornehmen?** Manche Listen werden von einem Administrator verwaltet, und nur er kann Einträge vornehmen. Manche erlauben jedem, IP-Adressen vorzuschlagen, die dann direkt oder nach einer automatischen oder manuellen Prüfung eingetragen werden. Und manche Listen sind vollautomatisch, sie tragen z. B. alle IP-Adressen ein, von denen eine Spamfalle (*spam trap*) E-Mails erhält.
- **Wie wird ein Eintrag von der Liste gelöscht?** Manche Listen erlauben es jedem, jede Adresse einfach zu löschen. Bei anderen kann man einen Test anstoßen, der die IP-Adresse erneut überprüft und danach ggf. löscht. Wieder andere Listen erfordern es, dass man den Administrator überzeugen muss, Einträge von der Liste zu löschen. Manche Betreiber verlangen sogar Geld für eine Löschung oder löschen überhaupt nicht.

---

<sup>5</sup> BIND (Berkeley Internet Name Domain): <http://www.isc.org/sw/bind/>

<sup>6</sup> rblndsd: <http://www.corpit.ru/mjt/rblndsd.html>, rbldns: <http://cr.yip.to/djbdns/rbldns.html>

<sup>7</sup> z. B. über einen DNS Zone Transfer

<sup>8</sup> <http://samba.anu.edu.au/rsync/>

**Werden Einträge automatisch gelöscht?** Manche Listen löschen Einträge automatisch, die ein gewisses Alter erreicht haben. Das ist insbesondere für Listen mit nicht sehr sorgfältig geprüften Einträgen wichtig. Ist eine IP-Adresse fehlerhaft klassifiziert worden, ist der dadurch angerichtete Schaden zumindest zeitlich begrenzt. Vor allem bei dynamisch vergebenen IP-Adressen sind lange Haltezeiten nicht sinnvoll, da sie ja jederzeit einer neuen Maschine zugeordnet werden können.

Vor dem Einsatz einer Liste sollte der Administrator überprüfen, ob die Policy der Liste mit der eigenen Policy vereinbar ist. Es versteht sich von selbst, dass man mit Listen ohne klare Policy sehr vorsichtig umgehen sollte.

Früher wurden die meisten DNSBLs noch manuell gepflegt, und Einträge hatten eine unbegrenzte Lebensdauer. Da die Spammer heute aber mobiler geworden sind und die genutzten Rechner, genauer IP-Adressen schnell wechseln (vor allem durch die Nutzung von Botnetzen), werden Listen heute mehr und mehr automatisiert zusammengestellt und deren Einträge schneller wieder gelöscht.

### 9.4.3 Typen von DNSBLs

Wie der vorangehende Abschnitt zeigt, gibt es viele Möglichkeiten, die Policy einer Liste zu gestalten. Neben IP-Adressen, die erwiesenermaßen Spamquellen sind, werden häufig solche von Systemen aufgenommen, die als offenes Relay (*open relay*, OR) oder als offener Proxy (*open proxy*, OP) aufgefallen sind. Daneben gibt es etliche Listen von Einwahlloder dynamischen IP-Adressen (*dialup users list*, DUL).

**Hier sind ein paar Beispiele:**

|   |  |
|---|--|
| Spamhaus Block List (SBL)<br><a href="http://www.spamhaus.org/">http://www.spamhaus.org/</a>              | Listet nur manuell geprüfte IP-Adressen, die mit Spammern assoziiert werden.   |
| Composite Blocking List (CBL)<br><a href="http://cbl.abuseat.org/">http://cbl.abuseat.org/</a>            | Listet <i>open proxies</i> sowie viren- und wurminfizierte Rechner, die vollautomatisch mittels Spamfallen (siehe Kapitel 9.22) erkannt wurden.                |
| Blitzed Open Proxy Monitor (OPM)<br><a href="http://opm.blitzed.org/info">http://opm.blitzed.org/info</a> | Handverlesene <i>open proxies</i> , die als Spammer oder als Störer im Internet Relay Chat (IRC) aufgefallen sind.   |
| Spam and Open Relay Blocking System (SORBS)<br><a href="http://www.sorbs.net/">http://www.sorbs.net/</a>  | Mehrere Listen offener Relays, offener Proxies und dynamischer IP-Adressen.  |
| SpamCop Blocking List (SCBL)<br><a href="http://www.spamcop.net/">http://www.spamcop.net/</a>             | Wird über automatisierte Reports und (ungeprüfte) Meldungen von SpamCop-Benutzern gefüttert.   |
| Open Relay Database (ORDB)<br><a href="http://www.ordb.org/">http://www.ordb.org/</a>                     | Liste mit offenen Relays   |
| Distributed Server Boycott List (DSBL)<br><a href="http://dsbl.org/">http://dsbl.org/</a>                 | Rechner, die als <i>open proxy</i> oder <i>open relay</i> fungieren. Die DSBL wertet dazu automatisch alle E-Mails aus, die sie über solche Rechner erreichen. |
| <a href="http://countries.nerd.dk">countries.nerd.dk</a>  | Listen mit IP-Adressen, die bestimmten Ländern zugeordnet sind. Diese Listen sind nicht sehr zuverlässig, weil es in der Regel nicht einfach                   |

|  |  |
|--|--|
| <a href="http://countries.nerd.dk/">http://countries.nerd.dk/</a>  | festzustellen (und auch vielfach nicht eindeutig) ist, in welchem Land eine IP-Adresse beheimatet ist.<br><br>Außerdem ist der Zusammenhang zwischen dem Absenderland und der Spamwahrscheinlichkeit nicht zwingend. |
| <a href="http://www.rfc-ignorant.org/">RFC-Ignorant.Org</a><br><a href="http://www.rfc-ignorant.org/">http://www.rfc-ignorant.org/</a> | Mehrere sehr umstrittene Listen von Systemen, die gegen RFCs verstoßen. Ist somit eigentlich keine Antispam-Liste.   |

Tabelle 9.2: Beispiele für DNSBLs

Die Liste ist wegen der großen Zahl verfügbarer DNSBLs notwendigerweise unvollständig und soll nur erste Anhaltspunkte und einen Einblick in die Bandbreite der Möglichkeiten geben. Weitere Listen finden sich im Internet.<sup>9</sup>

Manche Listen aggregieren Informationen von mehreren Listen, damit weniger Abfragen nötig sind. Beispielsweise nutzt die Spamhaus Exploits Block List (XBL<sup>10</sup>) Daten der CBL und OPM.

#### 9.4.4 Probleme mit DNSBLs

DNSBLs stehen bei vielen in schlechtem Ruf, weil sie in der Vergangenheit häufig unzuverlässig waren und zu viele „unschuldige“ Rechner auflisteten.<sup>11</sup> Manchmal sind DNSBLs auch schon für persönliche Vendettas verwendet worden. Dennoch sind DNSBLs heute eine so wichtige Antispam-Maßnahme, dass man sie nicht ignorieren kann.

Bevor man sich für eine (oder mehrere) Listen entscheidet, sollte man sich also den Betreiber der Liste sehr genau ansehen und entsprechende Informationen über die Liste einholen. Und hier wie auch anderswo gilt die Regel, dass eine Liste allein in den meisten Fällen für eine zuverlässige Entscheidung nicht ausreicht.

Grundsätzlich ist vor dem Einsatz einer DNSBL auch zu bedenken, dass man eine wichtige Entscheidung sozusagen „außer Haus“ gibt. Und auch wenn der Betreiber der Liste heute zuverlässig ist, heißt das noch lange nicht, dass er es auch morgen sein wird.<sup>12</sup> Daneben ist das DNS schlecht gegen Manipulationen Dritter gesichert.

#### **Auch DNSBLs haben Vorurteile**

*Bei DNSBLs gilt es immer die Anwenderbasis zu berücksichtigen, denn manchmal haben auch DNSBLs Vorurteile: Angenommen, ein Spammer benutzt die Rechner eines großen deutschen Webmail-Providers, um seinen Spam abzusetzen. Zwar kümmern sich die Admins darum, sobald sie das Problem erkennen, aber bis dahin kann schon einiges an Spam versandt sein. Auf einem*

<sup>9</sup> Umfangreiche Listen von DNSBLs mit Zusatzinformationen gibt es unter <http://rbld.org/>, <http://www.moensted.dk/spam/> und <http://www.decl ude.com/Articles.asp?ID=97>

<sup>10</sup> <http://www.spamhaus.org/xbl/index.lasso>

<sup>11</sup> Ein ausführliches, wenn auch nicht mehr ganz aktuelles Traktat gegen DNSBLs findet sich unter <http://theory.whirlycott.com/%7Ephil/antispa m/rbl-bad/rbl-bad. html>

<sup>12</sup> Berüchtigt ist der Fall der Osirusoft-DNSBL, deren Betrieb eingestellt wurde und die danach auf alle Anfragen eine positive Antwort zurückgegeben hat (siehe <http://slashdot.org/article.pl?sid=03/08/27/0214238>).

*anderen deutschen System wird dieser Spam kaum auffallen, da er in der Menge der Ham-Mails untergeht, die von diesem deutschen Webmail-Provider kommen.*

*Es gibt allerdings viel weniger Ham-Mails von diesem Webmail-Provider, die in die USA versandt werden. Eine DNSBL, die in den USA betrieben und hauptsächlich von amerikanischen Anwendern mit Daten gefüttert wird, sieht mehr Spam als Ham von diesem deutschen Provider und setzt ihn deswegen auf die schwarze Liste.*

*In diesem Szenario ist niemandem ein Vorwurf zu machen. Die DNSBL macht genau das, was sie soll: Sie schützt ihre amerikanischen Kunden vor Spam. Ein deutscher Kunde wäre damit aber wohl nicht zufrieden.*

In vielen Fällen hat sich gezeigt, dass eine Kommunikation mit dem Betreiber einer DNSBL schwierig sein kann. Das ist vor allem für jene problematisch, deren Adresse unverschuldet auf eine DNSBL geraten ist und kann den sorgfältigsten Admins passieren. Wenn ein ISP Millionen von Kunden hat, ist auch gelegentlich ein Spammer dabei. Häufig erfährt ein Administrator erst dann von der Eintragung in einer DNSBL, wenn eigene Kunden sich beschwerten, weil sie ihre E-Mails nicht mehr versenden können. Aufgrund der großen Menge an DNSBLs, die es weltweit gibt, ist es keinem Administrator möglich, immer auf dem Laufenden zu bleiben. Betreiber großer Mailsysteme sollten jedoch regelmäßig die wichtigsten DNSBLs daraufhin prüfen, ob ihre eigenen Mailserver dort eingetragen sind.<sup>13</sup>

#### 9.4.5 Rechtliche Aspekte von DNSBLs

DNSBLs sind zwar in der Praxis weit verbreitet, rechtlich jedoch nicht ganz unbedenklich. Nach einer weit verbreiteten, in der Praxis allerdings wenig beachteten Ansicht unter Juristen und Datenschützern unterfallen auch IP-Adressen als personenbezogene oder -beziehbare Daten dem Datenschutz. Begründet wird dies unter anderem damit, dass es unter den statischen IP-Adressen auch solche gibt, die unmittelbar einer natürlichen Person zugeordnet sind. Die Weitergabe und Speicherung dieser Daten ohne die ausdrückliche Zustimmung der Betroffenen ist grundsätzlich ein Verstoß gegen einschlägige Rechtsvorschriften des Datenschutzes. Nach dieser Meinung dürfen DNSBLs weder betrieben noch abgefragt werden.

Zulässig ist eine Speicherung von personenbezogenen Daten aufgrund des allgemeinen Gebots der Datensparsamkeit nur dann, wenn sie zu Abrechnungszwecken erfolgt, der Betroffene der Speicherung zustimmt oder als Maßnahme zur Gewährleistung der Datensicherheit nach § 9 BDSG und § 109 TKG. Unter dieser Prämisse könnte man die Speicherung von IP-Adressen im Rahmen von DNSBLs als Maßnahme sehen, die zum Schutz der eigenen Daten erforderlich ist. Schließlich können derartige Listen einen wichtigen Beitrag dazu leisten, die eigene Mail-Infrastruktur weiter funktionsfähig zu halten und den Zugriff auf gespeicherte Daten weiter zu ermöglichen. Dafür ist es allerdings auch erforderlich, dass der Betreiber die Gewinnung der verwendeten Daten so weit wie möglich transparent gestaltet. Die Speicherung der IP-Adressen würde demnach zumindest auch der Datensicherheit dienen.

Neben datenschutzrechtlichen setzt sich der Betreiber einer derartigen Liste auch anderen Risiken aus. So muss er im Zweifelsfall nachweisen, dass die gelisteten IP-Adressen tatsächlich im Zusammenhang mit der Versendung von Spam stehen. Derjenige, dessen Dienste unberechtigt auf dem Index landen und dem dadurch Nachteile entstehen, kann in diesem Fall Unterlassung und Schadensersatz vom DNSBL-Betreiber beanspruchen.

## 9.5 IP-Blacklisting durch Frequenzanalyse

Die Bewertung einer E-Mail anhand der IP-Adresse der Gegenstelle oder der IP-Adressen im *header* der E-Mail ist eine gute und günstige Möglichkeit zur Spamererkennung. Dazu müssen zuerst die IP-

Adressen erkannt und kategorisiert werden. Eine Möglichkeit ist die Frequenzanalyse der eingehenden Verbindungen pro IP-Adresse.

Diese Methode ist je nach Einsatzgebiet und Größe des Mailsystems mehr oder weniger aufwendig. In jedem Fall sollte zur Minimierung der *false positives* und aus Gründen der Performance eine Whitelist vorgeschaltet sein, die bestimmte Adressbereiche von der Prüfung ausnimmt.

Grundsätzlich werden für eine definierte Zeitspanne bei allen ankommenden E-Mails die Merkmale gezählt, auf deren Basis eine spätere Beurteilung erfolgt. Die maßgebliche Information ist die IP-Adresse, von der aus die Verbindung aufgebaut wird. Weitere Merkmale sind die Anzahl der bekannten und unbekanntem Empfänger (Spam ist häufig durch fehlerhafte Empfängeradressen gekennzeichnet) und die Absenderadresse während des SMTP-Dialogs. Die Zählung und Ermittlung dieser Werte erfolgt im MTA während des SMTP-Dialogs. Auch andere Merkmale können analysiert werden und weiteren Aufschluss über die Spamwahrscheinlichkeit der E-Mails von einer IP-Adresse geben.

Diese statistischen Werte können einzeln oder in Kombination zur Beurteilung der IP-Adresse des sendenden Hosts genutzt werden. Eine einfachere Variante besteht in der Definition absoluter Schwellwerte für einzelne oder die Kombination mehrerer Merkmale. Aufwendiger, aber auch treffsicherer, ist die Betrachtung der Abweichung dieser Messwerte vom Normalwert für den betreffenden Host. Die ideale Variante ist die Kombination beider Verfahren: Die einfachen Frequenzregeln bilden die Basis der Bewertung, die eine Whitelist falls nötig korrigiert. Die Betrachtung der Abweichung im E-Mail-Traffic von einer IP-Adresse korrigiert daraufhin die Whitelist, wenn der Verdacht des Missbrauchs einer dort aufgeführten IP-Adresse besteht.

Anhand eines definierten Regelwerks können somit bei Erreichung der Schwellwerte für zukünftige E-Mails und Verbindungen von dieser IP-Adresse die geeigneten Maßnahmen ergriffen werden. Da dieses System komplett automatisiert funktioniert und die Zählungszeiträume frei definiert werden können, steht eine sehr schnelle Reaktionsmöglichkeit auf einen beginnenden Spamversand zur Verfügung. Diese automatisch erzeugten Spam-Einträge sollten regelmäßig manuell überprüft werden, um *false positives* zu minimieren.

Die ermittelten Messwerte sind für jeden einzelnen Einsatzbereich verschieden. Die Schwellwerte sind also reine Erfahrungswerte für das einzelne Mailsystem und müssen während der Vorbereitung zum Einsatz dieser Methode sorgfältig ermittelt werden. Das Mailprofil eines mittelständischen Unternehmens in der Bauindustrie unterscheidet sich beispielsweise stark von dem einer multinationalen Werbeagentur. Zur Ermittlung der Anfangswerte lassen sich die aktuellen Mailserver-Logdateien der vergangenen Wochen heranziehen.

### **Beispielhaftes Anwendungsmodell eines frequenzbasierten Filters**

Für die einfache Variante eines Regelwerks werden zunächst drei Stufen der Spamwahrscheinlichkeit definiert: Warnung, Spamverdacht, Spam. Die „Warnung“ bewirkt z. B., dass diese E-Mails in Zukunft zur weiteren Analyse an andere Spamfilter-Module übergeben der E-Mails von dieser IP-Adresse. Für die Zeitspanne von 15 Minuten werden die Merkmale E-Mails in das nächste System zugestellt. Die Bewertung „Spam“ bewirkt eine Nichtannahme

IP-Adresse, bekannte Empfänger und unbekanntem Empfänger genutzt.

| <b>Anzahl<br/>Mails</b> | <b>Anteil<br/>unbe-<br/>kannter<br/>Empfänge<br/>r</b> | <b>Stufe</b> | <b>Gültig-<br/>keit</b> | <b>Kommentar</b> |
|-------------------------|--|--------------|-------------------------|------------------|
|                         |  |              |                         |                  |

|     |      |              |         |   |
|-----|------|--------------|---------|---|
| 200 | –    | Warnung      | 5 Tage  | Wenn im Zeitraum von 15 Minuten von einer IP-Adresse E-Mails an 200 Empfänger eingehen, dann warne vor dieser IP für den Zeitraum von 5 Tagen.  |
| 100 | 10 % | Spamverdacht | 30 Tage | Wenn im Zeitraum von 15 Minuten von einer IP-Adresse E-Mails an 100 Empfänger eingehen, von denen 10% unbekannt sind, dann stelle die Mails von dieser IP-Adresse für 30 Tage als Spam markiert zu.           |
| 50  | 80 % | Spam         | 4 Std.  | Wenn im Zeitraum von 15 Minuten von einer IP-Adresse E-Mails an 50 Empfänger eingehen, von denen 80% unbekannt sind, dann nimm von dieser IP-Adresse für 4 Stunden keine Mails mehr an.                       |
| 800 | –    | Spam         | 1 Std.  | Wenn im Zeitraum von 15 Minuten von einer IP-Adresse E-Mails an 800 Empfänger eingehen, unabhängig davon, ob diese bekannt sind oder nicht, dann nimm von dieser IP-Adresse für 1 Stunde keine Mails mehr an. |

Dieser Regelsatz würde in einem Umfeld mit ca. einer Million E-Mails am Tag und einem gemischten privaten Maileingangsprofil ca. 25 % des Spam nahezu ohne *false positives* bewerten. Ausnahmen von diesen Regeln sind in Form einer Whitelist zu berücksichtigen, da diese Regeln selbstverständlich auch von den Mailservern großer Provider ausgelöst werden würden. Damit käme ein Versender legitimer Massenmails schnell auf eine Blacklist.

Es kommt aber bisweilen vor, dass auch große seriöse Versender unfreiwillig Spam versenden oder vormals „gute“ IP-Adressen nun zum Spamversand benutzt werden. Der bedingungslose Einsatz einer Whitelist würde das Spam-Risiko erhöhen. Das gleiche Regelwerk lässt sich nach entsprechender Datensammlung jedoch erweitern, um den Einfluss der Whitelist zu relativieren. Im Laufe der Zeit wird sich die typische Frequenz einer IP-Adresse herausstellen. Diese Frequenz bewegt sich erfahrungsgemäß in einer Bandbreite von ca. 30 % Abweichung. Bei einem plötzlichen Spamversand, z. B. durch eine Virusinfektion im betroffenen Netz, würde sich diese Abweichung vergrößern. Folgende Regeln in einem komplexeren frequenzbasierten System können diesen Effekt ermitteln und die geeigneten Maßnahmen automatisch durchführen.

| Abweichung | Anteil unbekannter Empfänger | Stufe   | Kommentar  |
|------------|------------------------------|---------|--|
| 30 %       | –                            | Warnung | Wenn für den Zeitraum von 1 Stunde von einer IP-Adresse auf der Whitelist 30% mehr E-Mails eingehen, dann warne vor dieser IP-Adresse. |

| Abweichung | Anteil unbekannter Empfänger | Stufe        | Kommentar   |
|------------|------------------------------|--------------|---|
| 30 %       | 40 %                         | Spamverdacht | Wenn für den Zeitraum von 1 Stunde von einer IP-Adresse auf der Whitelist 30% mehr E-Mails eingehen, wovon 40% an unbekannte Empfänger gehen, dann stelle die Mails von dieser IP-Adresse als Spam markiert zu. |
| 100 %      | 10 %                         | Spam         | Wenn für den Zeitraum von 1 Stunde von einer IP-Adresse auf der Whitelist 100% mehr E-Mails eingehen, wovon 10% an unbekannte Empfänger gehen, dann nimm keine Mails von dieser IP-Adresse mehr an.             |

Wie in den Beispielen zu sehen ist, können die verschiedenen Merkmale genutzt werden, müssen es aber nicht. Die einzelnen Regeln und deren genauer Inhalt werden sich im Laufe der Zeit durch die regelmäßige Pflege immer weiter verbessern, bis sich ein optimaler Regelsatz für den eigenen Einsatzbereich entwickelt hat. Der benötigte Pflegeaufwand leitet sich nur aus der selbst gewählten Komplexität des Regelwerks ab und kann damit auch an alle Situationen angepasst werden.

Der Einsatz dieser Technik verlangt eine gewisse Grundlast im Mailverkehr, anderenfalls ist eine Frequenzanalyse auf den eigenen Mailservern nicht sinnvoll. Diese oder eine sehr ähnliche Technik kommt auch in kommerziellen Antispam-Produkten zum Einsatz, wobei die gesammelten Daten der Anwender des jeweiligen Systems der Frequenzmessung zugrunde liegen. Die Mailserver der Kunden liefern die bei ihnen anfallenden Daten zur Auswertung an ein zentrales System. Die fertig ausgewerteten Daten werden daraufhin zur weiteren Erkennung an die verteilten Installationen übermittelt.

Eine weitere im Einsatz befindliche Variante ist die lokale Pufferung und Vorab-Auswertung der gesammelten Frequenzdaten, die im Folgenden in festen Zeitabständen an die zentrale Instanz des Systems übermittelt werden. Das hat zwar den Nachteil der langsameren Reaktion, aber den Vorteil, weniger Bandbreite zu beanspruchen. Im kommerziellen Umfeld heißen solche und andere Frequenzmessungen auch *time patterns*.

## 9.6 Sperre des SMTP-Ports

E-Mails werden über SMTP [RFC2821] versandt. Dazu ist eine Verbindung zum SMTP-Server nötig, der auf dem TCP-Port 25 auf Anfragen wartet. Sperrt eine Firewall den SMTPPort für einen Rechner ausgehend, kann er keine E-Mail mehr versenden.

Besonders in Firmennetzen ist es sinnvoll, allen Rechnern (außer dem eigenen Mailserver) auf der Firewall den Zugriff auf den SMTP-Port externer Rechner zu verbieten.<sup>14</sup> Die einzelnen Rechner der Mitarbeiter sollen ja in der Regel ihre E-Mail nicht direkt ins Internet versenden, sondern über den Mailserver der Firma. Sollte ein Rechner in der Firma kompromittiert werden, kann er trotzdem nicht dem Spamversand dienen. Außerdem kann man so auch effektiv verhindern, dass ein fehlkonfigurierter Firmenrechner am eigenen Mailserver vorbei E-Mails versendet. Mit der

<sup>14</sup> Vor allem für Funk-Netze (WLAN) sollte der SMTP-Port ausgehend gesperrt werden, damit sie nicht von „vorbeikommenden“ Spammern missbraucht werden können.

Verbreitung von Maßnahmen zur Absenderauthentifizierung (siehe Kapitel 8.2) steigt die Notwendigkeit für Organisationen, möglichst wenige Mailserver nach außen sichtbar zu betreiben.

Auch einige Internet-Provider haben für ihre Kunden den SMTP-Port bereits gesperrt. Das betrifft hauptsächlich DSL- und Kabelmodem-Provider, deren Kunden Leitungen mit großer Übertragungskapazität verwenden und die damit bevorzugt zu unfreiwilligen „Helfershelfern“ der Spammer werden.<sup>15</sup> Die Kunden sind dadurch gezwungen, die Mail-Infrastruktur des Providers zu nutzen, was für die meisten Endanwender kein Problem ist. Größere Kunden wollen allerdings häufig einen eigenen Mailserver betreiben.

Damit die Kunden auch bei gesperrtem SMTP-Port weiterhin den Mailserver ihres eigenen Providers erreichen können, um über diesen ihre E-Mail zu versenden, muss dieser entweder von der Sperre ausgenommen werden, oder es muss stattdessen der Message-Submission-Port 587 [RFC2476] verwendet werden. Auch auf der Verbindung über diesen Port wird SMTP „gesprochen“, der Absender kann dort aber nur den Mailserver des eigenen Providers erreichen, der in der Regel eine Authentifizierung per SMTP AUTH verlangt. Eine Auslieferung direkt an den MX des Empfängers ist nicht möglich. Viele Provider bieten ihren Kunden bereits die Nutzung des Submission-Port an, aber manche ältere Client-Software kommt damit nicht zurecht.

## 9.7 MTAMARK

Weniger direkt als eine SMTP-Port-Sperre (siehe Kapitel 9.6), aber auf den gleichen Effekt aus, ist das Verfahren MTAMARK [StHo04]. Jeder „Besitzer“ einer IP-Adresse (in der Regel ein Internet-Provider) kann festlegen, ob von dieser IP-Adresse aus E-Mail versandt werden darf oder nicht. Dazu legt er in der DNS-Reverse-Zone, die zu dieser IP-Adresse gehört, einen entsprechenden Eintrag an. Der empfangende MTA kann diesen Eintrag überprüfen und danach filtern.

Der Vorteil dieses Verfahrens gegenüber der SMTP-Port-Sperre liegt darin, dass der Empfänger entscheidet, von wem er E-Mails annehmen will. Er kann also durchaus „liberaler“ sein, als es der Internet-Provider des Absenders vorgesehen hat.

Zurzeit ist das Verfahren noch im Versuchsstadium und kaum verbreitet. Es wird manchmal als Ersatz für die DNS-basierte Absenderauthentifizierung (siehe Kapitel 9.9) vorgeschlagen und bindet die „Erlaubnis zum Mailversand“ nicht an die Kombination aus IP-Adresse und Domain, sondern nur an eine IP-Adresse. Das Verfahren ist dadurch wesentlich einfacher umzusetzen, kann aber nicht so gut differenzieren. Da erfahrungsgemäß von den meisten IP-Adressen entweder nur Ham oder nur Spam ausgeht, dürften die Verfahren in der Praxis aber von vergleichbarer Wirksamkeit sein.

## 9.8 Existenzprüfung der Absenderadresse

Spam benutzt häufig zufällig generierte Absenderadressen im *MAIL FROM*. Diese Adressen sind ohne Funktion und E-Mail an diese Adressen ist daher nicht zustellbar. Zwei Tests sind möglich, um die Nichtexistenz einer Adresse festzustellen. Der einfachere und schnellere ist die Prüfung der Absenderdomain durch eine DNS-Anfrage. Etwas aufwendiger ist die Prüfung der kompletten Absenderadresse durch eine Anfrage beim MX der Absenderdomain. Dazu muss der MTA während des SMTP-Dialogs eine weitere SMTP-Verbindung in Gegenrichtung aufbauen. Das Verfahren kann effektiv sein, braucht aber erhebliche Ressourcen und mit einigen *false positives* ist zu rechnen. Zudem ist sicherzustellen, dass keine Endlosschleife<sup>16</sup> entsteht und dass das eigene System weiter funktioniert, wenn die Gegenstelle nicht in vernünftiger Zeit erreichbar ist. Dieses Verfahren

---

<sup>15</sup> In den USA bereits verbreitet, hat AOL es in Deutschland im Februar 2005 eingeführt: <http://www.heise.de/newsticker/meldung/56418>

<sup>16</sup> Die Anfrage in Gegenrichtung erfolgt meist mit einem leeren MAIL FROM, das sich nicht wieder prüfen lässt.

ist in manchen MTAs unter Namen wie Sender-Address-Verification, Sender-Verify oder Sender-Callout implementiert.

Das Verfahren kann nicht mit absoluter Sicherheit feststellen, ob eine Mailadresse existiert (der Mailserver kann eine E-Mail ja annehmen und später erst eine *bounce* erzeugen). Wenn der Server eine Fehlermeldung zurückgibt, dann existiert die Adresse entweder nicht oder die andere Seite hat auch einen Spamfilter, der den Empfang verhindert ( z. B. bei der Verwendung von BATV, siehe Kapitel 9.21). Nur durch die Auswertung erweiterter Fehlermeldungen (siehe [RFC2034] und [RFC3463]) ließe sich das genauer feststellen. Mit zusätzlichen *false positives* durch fehlerhaft konfigurierte Mailsysteme, die falsche Absenderadressen verwenden, ist zu rechnen.<sup>17</sup>

## 9.9 MARID-Verfahren: SPF und SenderID

Die ersten Vorschläge zur Authentifizierung von Absender-Mailservern per DNS-Eintrag gab es bereits 1998. Bis heute hat sich aber kein Verfahren durchgesetzt. Die Idee ist auf den ersten Blick bestechend einfach: Für jede ankommende E-Mail überprüft der MTA, ob der Rechner, der ihm diese E-Mail anbietet, überhaupt berechtigt ist, für diese Absenderdomain E-Mails zu versenden. Dazu nutzt er das Domain Name System (DNS), das um spezielle Einträge erweitert wird. Leider hat das Verfahren im heutigen weltweiten Mailsystem das Problem, dass es z. B. bei der Nutzung von Weiterleitungen und Mailinglisten ganz normal ist, dass E-Mails von fast beliebigen Rechnern mit fast beliebiger Absenderdomain stammen können. Daneben gibt es noch einige weitere Probleme.<sup>18</sup> Beispielsweise fällt es Spammern nicht schwer, große Mengen von „Wegwerfdomains“ zu registrieren und für sie passende DNS-Einträge anzulegen.

Diskutiert wurden und werden eine ganze Reihe von Verfahren, die sich alle recht ähnlich sind. Am bekanntesten sind SPF<sup>19</sup> (Sender Policy Framework), das z. B. GMX und AOL einsetzen, und das von Microsoft vorgeschlagene CallerID, die zum SenderID<sup>20</sup>-Vorschlag vereinigt wurden.

Von Frühjahr bis Herbst 2004 beschäftigte sich die MARID-Arbeitsgruppe<sup>21</sup> der IETF (Internet Engineering Task Force) mit diesem Thema und scheiterte schließlich daran, dass kein Konsens in Bezug auf die zu verwendenden Methoden herzustellen war. Neben der Komplexität des Problems und den daraus folgenden technischen Schwierigkeiten war dafür vor allem die unklare Lage bezüglich der Patentrechte verantwortlich.<sup>22</sup>

Die Verfahren unterscheiden sich vor allem in zwei Punkten: Welche Absenderadresse zur Authentifizierung herangezogen wird und wie die DNS-Einträge, mit denen die Authentifizierung durchgeführt wird, genau aussehen. SPF verwendet als Absender-Adresse die Adresse im *envelope* der E-Mail, SenderID verwendet die „Purported Responsible Address“ (PRA), die weiter unten erklärt wird.

---

<sup>17</sup> Das Verfahren eignet sich auch zur Überprüfung ausgehender E-Mail beim Provider. Er kann so verhindern, dass der Absender ungültige E-Mailadressen verwendet. Das ist allerdings weniger eine Antispam-Maßnahme als eine Hilfe für den Kunden.

<sup>18</sup> <http://www.advogato.org/article/816.html>

<sup>19</sup> <http://spf.pobox.com/>

<sup>20</sup> <http://www.microsoft.com/senderid/>

<sup>21</sup> MTA Authorization Records in DNS. <http://www.ietf.org/html.charters/OLD/marid-charter.html>

<sup>22</sup> [http://www.circleid.com/article/855\\_0\\_1\\_0\\_C/](http://www.circleid.com/article/855_0_1_0_C/)

### 9.9.1 DNS-Einträge

Die DNS-Einträge für die verschiedenen Verfahren sind alle etwas unterschiedlich. In der Regel wird kein neuer Typ von DNS Resource Record (DNS RR) verwendet, sondern der TXT-Record zweckentfremdet. Damit kann die bestehende DNS-Software auch für diese Einträge verwendet werden, ein Upgrade ist nicht notwendig.

Das zurzeit am meisten verbreitete Format ist das von SPF. Es sieht vor, dass (zusätzlich zu anderen DNS-Records für eine Domain) ein TXT-Eintrag verwendet wird, der beispielsweise für die Domain example.com so aussehen könnte:

```
example.com IN TXT „v=spf1 +a:mailout.example.com -all“
```

Der erste Eintrag ist immer die Versionsbezeichnung. Für das klassische SPF ist das `v=spf1`, für SenderID wird `spf2.0/pr` verwendet. Danach kann es diverse Einträge geben, die angeben, welche Server E-Mail von der Domain exampl e.com versenden dürfen. In diesem Fall ist das der Rechner mit dem Namen (dem DNS-Adress-Eintrag) `mailout`.

example.com. Alle anderen Rechner dürfen keine E-Mails für diese Domain versenden (`-al l`).

Das Format erlaubt sehr flexible Einstellungen. Eine genaue Beschreibung findet sich in [LeWo04].

### 9.9.2 Purported Responsible Address (PRA)

Die meisten Verfahren zur Absenderauthentifizierung setzen auf die Überprüfung der Envelope-From-Adresse. Das hat den Nachteil, dass die Überprüfung nicht mehr im MUA stattfinden kann, da er diese Adresse (anders als der MTA) in der Regel nicht mehr zu Gesicht bekommt.<sup>23</sup> Auch der Anwender sieht diese Adresse nie, stattdessen wird er die Header-From-Adresse sehen. Soll das Verfahren gegen *phishing* und *Joe Jobs* schützen, wäre es sinnvoller, die Adresse im *header* zur Authentifizierung heranzuziehen. Dazu dient das PRA-Verfahren.

Purported Responsible Address (PRA) heißt soviel wie „angeblich verantwortliche Adresse“. Es ist ein Verfahren, mit dem der Empfänger die Mailadresse des Absenders aus dem *header* einer E-Mail ermitteln kann. Wurde eine E-Mail über mehrere MTAs weitergeleitet, so ist die PRA die Adresse des letzten Absenders in der Kette. Da Header-Zeilen beliebig fälschbar sind, kann die Adresse nicht mit Sicherheit bestimmt werden, daher das „angeblich“ im Namen.

Das PRA-Verfahren verwendet (in dieser Reihenfolge) aus dem *header* die erste Resent-Sender:-Zeile, die erste Resent-From:-Zeile, die Sender:-Zeile oder die From:-Zeile (jeweils falls vorhanden). Im typischen Fall einer direkt zugestellten E-Mail ist das also die From:-Zeile. Eine detaillierte Beschreibung des Verfahrens findet sich in [Lyon04].

Leitet ein MTA eine E-Mail weiter, so soll er gemäß diesem Verfahren passende Resent-From:- oder Resent-Sender:-Zeilen einfügen. Die damit veränderte E-Mail könnte aber unter Umständen ein Verfahren nicht mehr als gültig erkennen, das auf einer kryptographischen Signatur der E-Mail inklusive der *header* beruht (siehe Kapitel 9.11).

### 9.9.3 Sender Rewriting Scheme (SRS)

Wie schon erwähnt ist eines der größten Probleme dieser Verfahren, dass E-Mail, die durch eine Mailingliste oder auf eine andere Weise weitergeleitet wurde, keinen passenden DNS-Eintrag mehr haben kann. Die einfache Antwort darauf ist, alle Mailinglistenrechner und andere, die einem E-Mails weiterleiten, in eine Whitelist einzutragen. Der damit verbundene Aufwand macht diesen Vorschlag aber unpraktikabel.

<sup>23</sup> Bei der Zustellung der E-Mail in eine Mailbox ergänzt der MTA häufig eine Return-Path: -Header-Zeile, die das Envelope-From enthält. Nach RFC2822, Abschnitt 3.6.7 ist das aber optional.

Als Alternative wird das Sender Rewriting Scheme<sup>24</sup> vorgeschlagen: Der weiterleitende Mailserver ändert die Absenderadresse, so dass sie seine eigene Domain enthält und kodiert die ursprüngliche Adresse im *local-part* so, dass sie sich wiederherstellen lässt.

Am einfachsten lässt sich das an einem Beispiel erläutern:

Der Absender einer E-Mail sei `user@example.com`. Die E-Mail wird über den Mailserver `mail.forward.com` weitergeleitet, der nicht für die Domain `exampl e.com`, sondern nur für die Domain `forward.com` zuständig ist. Er ändert die Absenderadresse jetzt in `user=example.com@forward.com`. Damit eine Antwort (z. B. eine Fehlermeldung) weiterhin funktionieren kann, muss diese Adresse nun gültig sein, `mail.forward.com` muss also E-Mails für diese Adresse annehmen und an `user@example.com` weiterleiten.

Das Ganze hat noch diverse Haken. Es muss verhindert werden, dass ein Spammer das Verfahren verwendet, um sich zu verstecken und unter fremdem Namen E-Mails zu verschicken. In der Praxis ist das Verfahren also noch etwas komplizierter, und die erzeugten Adressen sind umständlicher.<sup>25</sup>

Da sich bei diesem Verfahren die Envelope-From-Adresse bei jeder Weiterleitung ändert, könnte es Systeme stören, die diese in eine kryptographische Sicherung (siehe 9.9.4) einbeziehen.

## 9.10 S/MIME und PGP

Schon seit Jahren gibt es S/MIME [RFC3850, RFC3851] und PGP<sup>26</sup> [RFC2440], zwei miteinander konkurrierende Verfahren zur Mail-Verschlüsselung. Im Prinzip eignen sich diese Verfahren auch zur Spambekämpfung, allerdings wird nur der *body* der E-Mail geschützt, nicht der *header* und *envelope*. Leider sind all diese Verfahren zu selten im Einsatz.

Da Spam-Mail sehr selten im S/MIME oder PGP-Format verschickt wird, ist allein die Tatsache, dass entsprechende S/MIME- oder PGP-Angaben in der E-Mail vorkommen, ein Hinweis für Ham, der sich bei der Filterung berücksichtigen lässt. Es sind aber auch schon PGP-signierte Spam-Mails aufgetaucht. Als nächsten Schritt sollte man daher die Signaturen überprüfen. Damit ist zumindest die Kommunikation mit bekannten Absendern abgesichert. Statt einer Whitelist muss man eventuell nur eine Liste weniger Zertifikate pflegen.

Und letztendlich kann man sich durch konsequente Verwendung signierter E-Mails vor den Folgen von *Joe Jobs* und *phishing* schützen, solange die Empfänger Bescheid wissen und solche Signaturen erwarten.

## 9.11 MASS-Verfahren: DomainKeys und IIM

S/MIME- und PGP-Signaturen werden von MUAs erzeugt und geprüft. Für den Spamschutz geeigneter ist eine Überprüfung durch den oder die MTAs, die an der Weiterleitung der E-Mail beteiligt sind. Es liegen verschiedene Vorschläge vor; der bekannteste davon ist DomainKeys. Die IETF will eventuell eine Arbeitsgruppe namens „Message Authentication Signature Service (MASS)“<sup>27</sup> einrichten, die sich mit den Vorschlägen befasst und einen gemeinsamen Standard erarbeitet (Stand Anfang 2005).

---

<sup>24</sup> <http://spf.pobox.com/srs.html>

<sup>25</sup> <http://www.libsrs2.org/srs/srs.pdf>

<sup>26</sup> <http://www.openpgp.org/>

<sup>27</sup> <http://mipassoc.org/mass/>

Die Vorschläge unterscheiden sich in vielen Details, haben aber auch viele Gemeinsamkeiten.<sup>28</sup> Grundlage ist jeweils eine kryptographische Signatur von Teilen einer E-Mail (*header* oder Teile davon, *body*), die entweder in einer speziellen Header-Zeile oder als MIME-Teil an die E-Mail angefügt wird. Jeder MTA kann die Signatur des Absender-MTA (bei manchen Vorschlägen die aller MTAs in der Kette) überprüfen, indem er per DNS oder mit einer anderen Methode das passende Zertifikat anfordert.

Durch die Verwendung kryptographischer Routinen sind diese Verfahren aufwendig umzusetzen und CPU-intensiv. Die Sicherheit der Verfahren ist noch in der Diskussion [Hous05].

Die wichtigsten zur Zeit diskutierten Verfahren sind „DomainKeys“, „Identified Internet Mail (IIM)“ und „META Signatures“.

Das von Yahoo vorgestellte und seit Dezember 2004 dort im Einsatz befindliche Domain-Keys-Verfahren<sup>29</sup> [Dela04] ist von allen kryptographischen Verfahren zur Absenderauthentifizierung zurzeit am weitesten verbreitet. Außer bei Yahoo ist es unter anderem bei Google Mail (GMail) im Einsatz. Eine von GMail eingefügte DomainKeys-Header-Zeile sieht beispielsweise so aus:

```
DomainKey-Signature: a=rsa-sha1; q=dns; c=noaws; s=beta; d=gmail.com; h=received:message-id:date:from:reply-to:to:subject:mime-version:content-type:content-transfer-encoding;
b=PgrMY1Veeg+r0/ 7IOAXI6tKvmmGS/EH+//+47qAsEhhrd+pktJ3E2Od6rVCZKGyNzJpiFy/
nv8K0trRGIV1rEnfs6nqhjpP2GwEkbktfNTRggOp2G+4RJ0y6ssurjFqYqGid571hm
WQZMFw+n/mFjgmdwfX8ZyUxHuGbAbgRLBo=
```

Darin enthalten sind der Bezeichner des verwendeten Krypto-Algorithmus (a=rsasha1), die Information, wie der Empfänger den Signaturschlüssel abfragen kann (zurzeit nur per DNS, q=dns), die Art der Vorbehandlung des Inhalts (c=noaws), ein Key-Subtyp (s=beta), die Absenderdomain (d=gmail.com), die Liste der signierten Header-Zeilen (h=received. ..) und die Signatur selbst (b=..) im Base64-Format.

Die Vorbehandlung des Inhalts ist notwendig, weil sich E-Mails beim Versand manchmal leicht verändern, z. B. können sich Zeilenumbrüche verschieben. Errechnet der Empfänger nun die Signatur einer veränderten E-Mail, stimmt sie nicht mit der Signatur in der E-Mail überein. Eine Vorbehandlung (*canonicalization*) bringt die E-Mail in eine Standardform (*canonical form*), von der die Signatur berechnet wird. Es gibt zwei verschiedene *canonicalization algorithms*: „simple“ erlaubt kaum Änderungen, während „noaws“ einige typische Änderungen erlaubt.

Im DNS findet man im TXT-Record beta.\_domainkey.gmail.com<sup>30</sup> den folgenden Eintrag:

```
beta._domainkey.gmail.com.      300      IN      TXT      „t=y;      k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC69TURXN3oNfz+G/
m3g5rt4P6nsKmVgU1D6cw2X6BnxKJNlQKml0f8tMx6P6bN7juTR1BeD8ubaGqztm2rWK4
LiMJqhoQcwQziGbK1zp/MkdXZEWMcfiLY6oUITrivK7JNOLXtZbdxJG2y/
RAHGswKKyVhSP9niRsZF/IBr5p8uQIDAQAB“
```

Darin bezeichnet t=y den Test-Modus, k=rsa den Key-Type und p=MIG. ..QAB die Daten des öffentlichen Schlüssels im Base64-Format. Mit diesen Daten und dem Eintrag im *header* der E-Mail kann der Empfänger die Signatur der E-Mail überprüfen.

Die Firma Cisco hat ebenfalls im Jahre 2004 das Verfahren „Identified Internet Mail“ (IIM)<sup>31</sup> vorgestellt [FeTh04], das dem DomainKeys-Verfahren sehr ähnelt. IIM wird zur Zeit noch nicht oder kaum genutzt.

<sup>28</sup> [http://www.elan.net/~william/emailsecurity/emails\\_signatures-comparisonmatrix.htm](http://www.elan.net/~william/emailsecurity/emails_signatures-comparisonmatrix.htm) und <http://mipassoc.org/mass/crocker-featu-res-iim-dkeys-06dc.htm>

<sup>29</sup> <http://antispam.yahoo.com/domainkeys>

<sup>30</sup> Der Name des Eintrags setzt sich aus dem Key-Subtyp („beta“), der festen Bezeichnung „\_domainkey“ und der Domain („gmail.com“) zusammen.

Ein weiteres derzeit entstehendes Verfahren, das die besten Aspekte verschiedener Verfahren zusammenzufassen versucht, läuft unter dem Namen „META Signatures“<sup>32</sup> (Mail Enhancements for Transmission Authorization).

## 9.12 RHSBLs

So genannte RHSBLs (*Right Hand Side Blacklists*) sind eine Variante der DNSBLs (siehe Kapitel 9.4). Es handelt sich also auch um ein Reputationssystem. Statt der IP-Adresse des Absenders speichern sie jedoch den Teil der Absenderadressen, der sich auf der rechten Seite des At-Zeichens (@) in einer Mailadresse befindet. Das erlaubt also eine Filterung basierend auf der Absenderdomain. Da ein Spammer die Absenderdomain beliebig fälschen kann, ist der Nutzen einer solchen Liste aber begrenzt, solange kein Verfahren zur Absenderauthentifizierung benutzt wird. Sinnvoll sind allenfalls Listen, die nur Domains enthalten, die Spammern gehören. Möglich wäre auch ein Vergleich des HELO-Namens oder von Domains, die in URLs benutzt werden (siehe Kapitel 9.17), mit einer solchen Liste.

Wie bei anderen DNSBLs sind die juristischen Aspekte zum Datenschutz zu berücksichtigen (siehe Kapitel 9.4).

## 9.13 Greylisting

Der empfangende MTA kann in einer SMTP-Verbindung die Annahme einer E-Mail temporär ablehnen, wenn er beispielsweise vorübergehend nicht genug Ressourcen hat. Der Absender wird dann nach einer Wartezeit eine erneute Zustellung versuchen. Beim so genannten Greylisting<sup>33</sup> kommt diese Funktion zum Einsatz, um die Annahme einer spamverdächtigen E-Mail erst einmal abzulehnen. Spamssoftware ist üblicherweise auf möglichst hohen Durchsatz getrimmt und macht sich nicht die Mühe, eine erneute Auslieferung zu versuchen, während reguläre E-Mail dann beim zweiten Versuch ausgeliefert wird.

Damit der MTA den ersten und zweiten Zustellversuch voneinander unterscheiden kann, legt er in einer Datenbank mehrere Informationen darüber ab, in der Regel das Tripel aus Envelope-Adressen von Empfänger und Absender sowie der IP-Adresse des sendenden Mailservers.<sup>34</sup>

Nach einer gewissen „Karenzzeit“ von typischerweise einer halben bis ganzen Stunde stellt das Empfänger-Gateway weitere Mails genau dann unverzüglich zu, wenn sie dieselbe Kombination von Adressdaten tragen, wie sie bereits in der Datenbank gespeichert ist. Ab dieser erfolgreichen Zustellung bleibt der Datensatz für eine längere Zeit (mehrere Wochen) „freigeschaltet“. Bleiben weitere Zustellversuche aus, verfällt der Datensatz innerhalb weniger Tage, und die nächste Mail von diesem Absender durchläuft die gesamte Prozedur erneut. Die Karenzzeit verhindert, dass einem Spammer die Zustellung gelingt, indem er einfach zwei Sendeversuche in kurzer Folge unternimmt.

Da ein Mailserver, der eine E-Mail wiederholt eingeliefert hat, das wahrscheinlich auch in Zukunft tun wird, kann die IP-Adresse dieses Servers in einer Whitelist gespeichert werden. Man spart sich damit die Speicherung des ganzen Tripels.

Typische Greylisting-Systeme antworten im SMTP-Dialog nach dem *RCPT TO* mit einem temporären Fehler. Da es aber ältere MTA-Software gibt, die dann einen endgültigen Fehler erkennt, kann der temporäre Fehler stattdessen auch erst nach der *DATA*-Phase übermittelt werden. Nachteil

---

<sup>31</sup> <http://www.identifiedmail.com/>

<sup>32</sup> <http://www.metasignatures.org/>

<sup>33</sup> <http://projects.puremagic.com/greylisting/> und <http://greylisting.org/>

<sup>34</sup> Hat eine Domain mehrere MX-Rechner, sollten sie eine gemeinsame Datenbank verwenden.

ist, dass dadurch unnötiger Datenverkehr erzeugt wird. Vorteil ist, dass der Empfänger dann den Inhalt der E-Mail kennt. Wenn keine zweite Zustellung versucht wird, kann er den Inhalt analysieren und beispielsweise zum Training eines Bayes-Filters einsetzen.

Juristisch ist das Greylisting-Verfahren weitgehend unbedenklich. Zwar sieht etwa § 303a StGB ein „Unterdrücken“ auch schon bei einem vorübergehenden Entziehen von Daten als ausreichend zur Verwirklichung dieses Tatbestandsmerkmals an, ausgenommen sind jedoch solche Zeitspannen, die für den Berechtigten keine oder eine sehr geringfügige Beeinträchtigung bedeuten. Eine Verzögerung der Zustellung einer E-Mail um eine halbe Stunde fällt daher kaum in den strafbaren Bereich.

Nachteilig ist, dass Greylisting beim Empfänger und bei regulären Absendern zusätzliche Ressourcen bindet. Benutzt der Absender ein großes Mailsystem, das mehrere Mailserver für ausgehende E-Mail hat, und wird die gleiche E-Mail nicht bei jedem Zustellversuch vom selben Rechner (und damit derselben IP-Adresse) kommen, so kann der Empfänger nicht erkennen, dass er diese E-Mail schon gesehen hat. Darüber hinaus gibt es Probleme mit Einmal-Adressen, wie sie zum Beispiel beim Betrieb von Mailinglisten (bei der Nutzung von VERP<sup>35</sup>) vorkommen, die gesondert behandelt werden müssen (siehe auch Kapitel 9.21). Und bei weitem nicht jeder Absender-MTA ist RFC-konform. Ein Verlust von E-Mails ist daher nicht auszuschließen. Eine Whitelist ist aus diesen Gründen nebenher zu pflegen. Da jeder einzelne Zustellversuch zu Speicher- und Vergleichsoperationen in einer dem Empfänger-MTA nachgeschalteten Datenbank führt, sind die entsprechenden Systeme redundant und besonders leistungsfähig auszuliegen.

Derzeit kann Greylisting den Spam-Anteil in der eingehenden E-Mail deutlich reduzieren [Völk04]. Es steht jedoch zu befürchten, dass sich die Spam-Versender darauf einstellen, indem sie einfach jedwede Aussendung nach einer Zeitspanne wiederholen, die bei den meisten Greylisting-geschützten Systemen schließlich doch zu einer Zustellung führt. Darunter leiden dürften alle anderen Systeme, die dann ein Mehrfaches des bisherigen Mailvolumens erhalten würden, da bei ihnen nicht erst der wiederholte, sondern bereits der erste Zustellversuch zum „Erfolg“ führt. Außerdem ist Greylisting unwirksam, wenn Spammer die offiziellen Mailsysteme der ISPs missbrauchen.

Greylisting kann auch automatisch generierte IP-Blacklists und kollaborative Filter unterstützen und ihnen Zeit geben, sich auf neue Spammer oder neue Spam-Inhalte einzustellen.

## 9.14 Heuristische Inhaltsanalyse

Ein heuristischer Filter verfügt über ein festes Regelwerk, das die Unterschiede zwischen Ham und Spam herausarbeitet und nach dem Durchlaufen meist mehrerer, sehr unterschiedlicher Regeln eine Entscheidung trifft, wie die E-Mail zu klassifizieren ist (*rule based filtering*). Die Regeln können sich auf den *header* und den *body* der E-Mail beziehen, die Prüfung kann an jeder Stelle erfolgen, findet jedoch meist im MTA oder MDA statt.

Typische Filterregeln für Betreff (*subject*) und Inhalt der E-Mail erlauben z. B. die Filterung nach Wörtern oder Sätzen, die gewöhnlich nicht in Ham, aber vielfach in Spam vorkommen, etwa „Viagra“ und „Make Money Fast“, oder Wörter, die auf Pornografie usw. hindeuten. Natürlich gibt es auch Ham-Mails, die solche Wörter enthalten. Deswegen ist eine E-Mail erst dann als Spam zu klassifizieren, wenn mehrere solcher Tests die Wahrscheinlichkeit für Spam ausreichend erhöhen.

Andere typische Anzeichen für Spam sind viele Wörter in Großbuchstaben, Texte, die den Empfänger auffordern eine Webseite aufzurufen, oder Beschreibungen, wie man sich angeblich von der Verteilerliste streichen kann.

Neben dem Text sind auch die in einer E-Mail vorkommenden URLs sehr aussagekräftig. Der Spammer will ja häufig etwas verkaufen und verweist den Empfänger dazu auf eine Webseite, die

<sup>35</sup> Variable Envelope Return Path (<http://cr.yp.to/proto/verp.txt>). Methode zur Zuordnung von bounces durch Kodieren der Empfängeradresse einer E-Mail im Envelope-From.

speziell für diesen Spam angelegt wurde. Das Vorkommen dieser URL oder auch bestimmter Muster in der URL ist deshalb ein sehr spezifisches Filtermerkmal.

Spammer versuchen den Inhalt der E-Mail häufig vor den Filtern zu verschleiern, indem sie Wörter falsch schreiben ( z. B. „V1 @gra“ statt „Viagra“) oder HTML-Tricks<sup>36</sup> einsetzen. Doch gerade diese Tricks lassen sich wiederum zur Filterung heranziehen, weil sie – wenn man sie einmal kennt – deutlich auf Spam hinweisen.

Aber nicht nur der Inhalt, auch der *header* einer E-Mail kann eine Vielzahl von Hinweisen enthalten. Im *header* finden sich neben Absender (From:) und Empfänger (To:), dem Versand-Datum (Date:) und einer eindeutigen ID (Message-Id:) häufig noch eine Vielzahl weiterer Angaben. Beispielsweise verewigen viele MUAs ihren Namen und ihre Versionsnummer in Header-Zeilen wie User-Agent: oder X-Mailer:. Wenn dort beispielsweise eine Versionsnummer steht, die der Hersteller der Software sicher nie vergeben hat, so muss es sich um eine Fälschung handeln. Auch weiß man von bestimmten Message-Ids oder anderen Header-Zeilen, dass Spamssoftware solche Angaben in einem bestimmten Format erzeugt.

Zur Analyse können auch die Received:-Zeilen herangezogen werden, die MTAs in den header einfügen, wenn sie eine E-Mail weiterleiten. Allerdings fügen Spammer häufig gefälschte Zeilen ein, um zu verschleiern, woher der Spam tatsächlich kommt. In Einzelfällen kann man von Hand prüfen, ob die Received:-Zeilen eine ununterbrochene Kette von Systemen darstellen. Sehr große Sprünge bei den Zeitstempeln oder Lücken in den Systembezeichnungen zwischen zwei Received:-Zeilen deuten ziemlich sicher auf eine Manipulation der Kopfzeilen und somit auf eine Spam-E-Mail hin. Die Header-Zeilen sind aber leider nicht ausreichend standardisiert und verlässlich genug, als dass man diese Prüfung automatisieren könnte.<sup>37</sup>

Wer solche Muster für die Headeranalyse selbst anlegt, muss dabei sehr aufpassen. Oft erzeugen auch reguläre Mailprogramme fehlerhafte Header-Zeilen, weil sie falsch konfiguriert oder nicht sorgfältig genug programmiert sind. Auch hier darf also erst die Kombination mehrerer Spamhinweise zur Kategorisierung als Spam führen.

Die heuristische Inhaltsanalyse weist vor allem aus Sicht der Systemverwaltung einige Vorteile auf. Sie ist flexibel, technisch einfach und nachvollziehbar umzusetzen und funktioniert „aus dem Stand“ ohne Trainingsphase. Mit einem geeigneten Satz von Regeln ist die Methode sehr zuverlässig. Bei Problemen ist es dem Administrator einfach möglich, zweifelhafte Regeln zu identifizieren und zu modifizieren oder abzustellen. Dem gegenüber steht der Nachteil, dass die Regeln immer wieder auf den neuesten Stand gebracht werden müssen, sobald sich die Spammer neue Tricks ausgedacht haben, ähnlich wie die Signaturen bei einer Antiviren-Software.

Der Rechenaufwand für die Prüfung all dieser Regeln ist erheblich. Die weit verbreitete Software SpamAssassin<sup>38</sup> beispielsweise enthält mehr als 700 Body- und Header-Regeln, die sie für jede E-Mail prüft. Die Vergleiche basieren meistens auf *regular expressions* und sind dadurch erheblich aufwendiger als einfache Textvergleiche.

## 9.15 Statistische Inhaltsanalyse

Computer werden praktisch seit ihrer Erfindung dafür eingesetzt, die mit ihrer Hilfe angesammelten Datenmassen automatisch zu klassifizieren und zu sortieren, insbesondere um Wichtiges von

---

<sup>36</sup> Beispielsweise kann man die einzelnen Buchstaben in einem Wort durch HTML-Elemente und Füllbuchstaben trennen: V<font style="font-size: 1px">x</font>I<font style="font-size: 1px">x</font>AGRA.

<sup>37</sup> Siehe auch RFC 2821, Abschnitt 3.8.2

<sup>38</sup> <http://spamassassin.apache.org/>

Unwichtigem zu trennen – eben zu filtern. Eine Herausforderung ist die flexible, automatische Anpassung der Filter an sich laufend ändernden Input. Den mehr oder weniger erfolgreichen Lösungsbestrebungen sind Verfahren zu verdanken, die mit Begriffen wie künstliche Intelligenz (KI), neuronale Netze, maschinelles Lernen, *support vector machines* und Mustererkennung umschrieben werden. Von zentraler Bedeutung sind statistische Methoden für die Vorhersage zukünftiger Ergebnisse mit Hilfe von Daten aus vergangenen Erhebungen (etwa für Hochrechnungen von Wahlergebnissen).

Als unerwünschte E-Mails zu einem drängenden Problem wurden, fanden die statistischen Klassifizierungsverfahren fast zwangsläufig ihren Weg auch in die Spamfilterung. Der Artikel „A Plan for Spam“ von Paul Graham<sup>39</sup> aus dem Jahr 2000 gilt als Startschuss für die statistische Spamfilterung. Er widmet sich der relativ einfachen „naiven Bayes-Klassifizierung“<sup>40</sup> (siehe Kasten). Ein solcher Filter untersucht alle in einer E-Mail vorkommenden Zeichenketten darauf, wie signifikant ihr Auftreten bisher für Spam oder Ham war und ermittelt daraus für die vorliegende E-Mail, mit welcher Wahrscheinlichkeit sie unerwünscht ist. Schon wenige Wörter können für eine richtige Kategorisierung ausreichen.

### Naive“ Bayes-Filter und ihre Grenzen

Bayes-Filter verdanken ihren Namen den jahrhundertealten statistischen Methoden des Mathematikers Thomas Bayes. Ein naiver Bayes-Filter stellt keine Zusammenhänge innerhalb des E-Mail-Textes her, sondern bildet lediglich Statistiken über einzelne Wörter (genauer *tokens*) und sieht deren Auftreten als unabhängig voneinander an. Das ist nur eine sehr grobe Näherung der Realität. In der Praxis haben sich naive Bayes-Filter dennoch als sehr erfolgreich erwiesen. Sie erreichen False-Negative-Raten von unter 1% bei einer False-Positive-Rate unterhalb derjenigen, die bei manueller Sortierung zu erwarten ist.

Ein statistischer Filter erfordert anders als die heuristischen Filter mit ihrem festem Regelwerk zunächst eine Trainingsphase, während der er etliche Hundert Spam- und Ham-Mails vorgesetzt bekommt. Während der Trainingsphase muss der Anwender die als Spam erkannten E-Mails besonders gründlich nach *false positives* durchsuchen, die der Filter als Ham lernen muss, damit er nach und nach zuverlässiger arbeiten kann.

Auch nach der Trainingsphase muss ein statistischer Filter ständig weiter trainiert werden, damit er neue Muster lernt. Außerdem muss darauf geachtet werden, nicht auf falsche Merkmale, wie z. B. das Datum der E-Mails, zu trainieren. Bei laufendem Training ist die Effektivität sehr hoch, wenn zusätzliche Verfahren („Rauschunterdrückung“) zum Einsatz kommen, die gezielte Angriffe der Spammer auf statistische Filter (z. B. durch „unschuldige“ oder Nonsense-Worte) abwehren. Da der Inhalt der Trainingsdatenbank aus den Inhalten der eingehenden E-Mails generiert wurde, muss er entsprechend vertraulich behandelt werden, auch wenn ein Rückschluss auf den Inhalt der E-Mails kaum möglich ist.

Die Analyse von E-Mails mit statistischen Methoden erfordert nicht nur gelegentliche Eingriffe der Anwender, sondern ist zudem enorm ressourcenintensiv. Zunächst muss der MTA die E-Mails komplett empfangen, und die eigentliche Analyse erzeugt eine hohe CPU-Last. Da sich die statistische Analyse im Wesentlichen auf den Mail-Inhalt konzentriert, drohen insbesondere bei der Kommunikation bezüglich unerwünschter Inhalte *false positives*, etwa bei der Spam-Weiterleitung an Beschwerdeabteilungen von Internet-Providern. Warum der Filter eine E-Mail falsch einsortiert hat, ist nicht so einfach nachzuvollziehen wie bei heuristischen Filtern, da es kein festes Regelwerk gibt. Der Einsatz von Bayes und anderen statistischen Filtern kommt aus diesen Gründen häufig nur in Kombination mit anderen Verfahren in Frage.

<sup>39</sup> <http://www.paulgraham.com/spam.html>

<sup>40</sup> <http://www.mathpages.com/home/kmath267.htm>, <http://www.statsoft.com/textbook/stnaiveb.html>, [http://en.wikipedia.org/wiki/Naive\\_Bayesian\\_classification](http://en.wikipedia.org/wiki/Naive_Bayesian_classification)

Meistens sind Bayes-Filter MUA-basiert anzutreffen. Auf dem Rechner des Endanwenders sortieren sie am Ende der Zustellkette diejenigen Spams aus, die nicht bereits eines der vorgeschalteten, zentraler operierenden Verfahren erkannt hat. Die statistische Filterung ermöglicht es dem Endanwender, seine Vorstellungen von Spam und Ham zu definieren. Andererseits funktionieren Bayes-Filter umso besser, je größer die der Entscheidung zugrunde liegende Datenbasis ist. Bei einer homogenen Anwendergruppe ist daher eine zentrale Bayes-Filterung sinnvoll (und weniger aufwendig für den Einzelnen).

Obwohl allen Bayes-Spamfiltern die selben statistischen Prinzipien zugrunde liegen, können sie zu recht divergierenden Filterergebnissen führen. Zudem benötigen sie sehr unterschiedliche Mengen an Trainings-Spam und -Ham, bevor sie zufrieden stellend arbeiten. Dafür gibt es zweierlei Gründe: Zunächst bereiten die Filterprogramme eingehende E-Mails in unterschiedlicher Weise auf. Ein Filter, der nur Rohdaten aus dem Datenfluss verarbeitet, bekommt weniger signifikante *tokens* zu fassen als einer, der die Daten vor der statistischen Analyse praktisch so aufarbeitet wie ein ausgewachsener Mailclient, indem er die Transportkodierung auflöst. Selbst Filter, die prinzipiell HTML wie ein Webbrowser interpretieren („rendern“) können, müssen nicht zu gleichen Filterergebnissen kommen. Der eine fällt eventuell auf Zeichen in der Hintergrundfarbe herein, während der andere diese ausblendet, da sie der Anwender gar nicht wahrnehmen könnte.

Der zweite Grund für die unterschiedlichen Erfolgsquoten von Bayes-Filtern liegt in der Definition der *tokens* an sich und daran, wo der Filter sie überhaupt sucht. Einer, der außer dem *body* den gesamten *header* in die Bewertung einbezieht, kommt natürlich zu anderen Ergebnissen als einer, der sich auf Betreffzeile und *body* beschränkt. Außerdem ergeben sich je nachdem, welche Zeichen der Filter als Trennzeichen wertet und welche er als *token*-Bestandteile sieht, unterschiedliche Statistiken. Je nachdem, welcher Teil der E-Mail untersucht wird, kann es erforderlich sein, unterschiedliche Zeichen als Trennzeichen zuzulassen: IP- und Mailadressen sollte ein Filter komplett bewerten und nicht an den Punkten in mehrere *tokens* zerlegen, die für sich genommen statistisch kaum noch signifikant wären.

## 9.16 Prüfsummenvergleich

Das wichtigste Kennzeichen von Spam ist, dass er tausend- oder sogar millionenfach auftritt. Für den einzelnen Empfänger ist es allerdings nicht zu erkennen, ob auch andere die gleiche oder eine ähnliche E-Mail bekommen haben. Es gibt aber eine ganze Klasse von Filtern, die hier ansetzt. Ist der Spam einmal erkannt, wird er einer zentralen (in der Regel externen, d. h. nicht in der eigenen Organisation angesiedelten) Datenbank gemeldet. Ein Empfänger kann diese Datenbank nun bei jeder ankommenden E-Mail abfragen, ob sie die E-Mail schon kennt. Die Überprüfung muss in der Regel im MTA oder MDA stattfinden, da der MUA nicht unbedingt eine Internetverbindung zum Zugriff auf die zentrale Datenbank hat, deren ständige Verfügbarkeit und Zuverlässigkeit für dieses Verfahren unbedingt notwendig ist. Verfahren wie dieses, die sich auf eine gemeinsam geführte Datenbank stützen, heißen „kollaborativ“.

Zum Vergleich dient nicht die gesamte E-Mail, sondern nur eine Prüfsumme (*checksum* oder *digest*), aus der sich der Inhalt der E-Mail nicht rekonstruieren lässt. Damit muss also nicht der Inhalt jeder E-Mail einer zentralen Stelle gemeldet werden, was aus Datenschutzgesichtspunkten sicher unerwünscht wäre. Die Prüfsumme ist darüber hinaus deutlich kürzer als die E-Mail selbst.

Da Spammer ihre E-Mails häufig leicht verändern, kommen oft so genannte „unscharfe Prüfsummen“ (*fuzzy checksums*) zum Einsatz, die robust gegenüber kleinen Änderungen sind. Selbst wenn z. B. mehr oder weniger Leerzeichen zwischen Worten auftauchen, bleibt die Prüfsumme gleich. Wie die Algorithmen dieser Prüfsummen genau funktionieren, halten die Hersteller

proprietärer Software meist geheim, es gibt aber auch öffentlich bekannte Verfahren.<sup>41</sup> Auf jeden Fall ist die Berechnung der Prüfsumme aber deutlich effizienter als viele andere inhaltsbasierte Tests.

Beispiele für öffentliche und frei nutzbare Prüfsummendatenbanken sind das Distributed Checksum Clearinghouse (DCC<sup>42</sup>), Vipul's Razor<sup>43</sup> und Pyzor<sup>44</sup>. Auch die Redaktion der Zeitschrift iX bietet eine eigene Prüfsummenliste<sup>45</sup> an, die sie aus rund 3000 Spams pro Tag bildet. Bei deren internen Gebrauch ergibt sich eine Trefferquote von über 70 %, das heißt weniger als ein Drittel des eingehenden Spams muss der eigentliche Spamfilter überhaupt neu analysieren. Der Rest ist bereits durch Übereinstimmung der unscharfen Prüfsumme mit derjenigen einer zuvor als Spam erkannten E-Mail als unerwünscht erkennbar. Daneben gibt es viele Firmen, die ähnliche Verfahren in ihren kommerziellen Filterprogrammen nutzen.

Damit sich die zentrale Datenbank ohne großen Filteraufwand mit E-Mail-Mustern füllt, verwenden viele Betreiber so genannte Spamfallen (siehe Kapitel 9.22). Dabei handelt es sich in der Regel um Mailaccounts, die niemals für legitime E-Mails zum Einsatz kommen. Auch seit Jahren unbenutzte Adressen kommen als Spamfallen in Frage. Bei E-Mails, die an solche Adressen gehen, handelt es sich mit hoher Wahrscheinlichkeit um Spam, der sich direkt in die Datenbank aufnehmen lässt. Spamfallen werden z. B. auf Webseiten in einer Weise veröffentlicht, dass ein menschlicher Websurfer sie nicht finden würde, wohl aber die automatisierten Adressensucher der Spammer. Darüber hinaus gibt es in der Regel eine einfache Möglichkeit, wie auch der Anwender Prüfsummen an die Datenbank melden kann.

Mit Hilfe der Prüfsummen lassen sich auf einfache Weise Informationen über derzeit umlaufenden Spam austauschen, nicht nur im eigenen LAN, sondern im ganzen Internet. Anders als die meisten IP-Adressen, von denen aus Spam eingeht, ändern sich die Spam-Inhalte oft tage- oder gar wochenlang nicht wesentlich, sodass sich Prüfsummen-Blacklists wesentlich kompakter halten lassen als IP-Blacklists.

Ein Problem ist jedoch, dass es keine standardisierte Methode für die Prüfsummenbildung von E-Mails gibt. Und gäbe es die, würden Spammer ihre E-Mails so aufbauen, dass sie von dem Algorithmus nicht mehr als gleich erkannt werden. Wer einen Prüfsummendienst nutzt, ist darauf angewiesen, selbst die gleichen Algorithmen auf eingehende E-Mails anzuwenden wie der Prüfsummenlieferant, indem er dessen Software lokal installiert. Prüfsummenverfahren und damit die entsprechende Software sind ab und zu auf den neusten Stand zu bringen, um den Spammern kein fest stehendes Ziel zu bieten. Darüber hinaus fällt aber kein administrativer Aufwand an.

Die Schwierigkeit bei diesem Verfahren besteht darin, keine legitimen Newsletter und andere Ham-Mails in die Datenbank aufzunehmen. Anwender, die einen Newsletter nicht mehr haben wollen, kennzeichnen ihn häufig als Spam, weil es ihnen als einfachste Möglichkeit erscheint, die E-Mail loszuwerden. Machen das „genug“ Anwender, dann sieht der Algorithmus eine E-Mail, die von vielen als Spam abgelehnt wurde, und klassifiziert sie auch für alle anderen als Spam.

Datenschutzrechtlich sind diese Verfahren unbedenklich, da nur eine Prüfsumme der E-Mails gespeichert wird, aus der sich die E-Mail nicht rekonstruieren lässt.

---

<sup>41</sup> z. B. nilsimsa (siehe <http://ixazon.dynip.com/~cmeclax/nilsimsa.html>)

<sup>42</sup> <http://rhyolite.com/anti-spam/dcc/>

<sup>43</sup> <http://razor.sourceforge.net/>

<sup>44</sup> <http://pyzor.sourceforge.net/>

<sup>45</sup> <http://www.nixspam.org/>

## 9.17 URIDNSBLs

URIDNSBLs sind eine spezielle Form der DNSBLs (siehe Kapitel 9.4), die nicht die IP-Adressen von (potentiellen) Spammern speichern, sondern die IP-Adressen der von Spammern benutzten Web- oder Nameservern. In E-Mails vorkommende Webadressen (URLs) können gegen diese Listen geprüft werden. Sie gehören damit zu den sowohl IP-als auch inhaltsbasierten Reputationssystemen. Diese Idee basiert auf der Erkenntnis, dass es für Spammer einfacher ist, die Herkunft einer E-Mail zu verschleiern als den Ort der Webseiten, für die sie werben. In der Praxis können teilweise dieselben Listen sowohl zur Überprüfung der Absender-IP-Adresse als auch als URIDNSBL verwendet werden. Anders als rein IP-basierte DNSBLs erfordern URIDNSBLs eine Analyse des Inhaltes einer E-Mail. URIDNSBLs gibt es in verschiedenen Formen und unter verschiedenen Namen: URIBL, URIRHSBL, SURBL.<sup>46</sup> Eine Variante speichert nicht IP-Adressen, sondern direkt die in der URL vorkommende Domain (siehe auch RHSBLs in Kapitel 9.12).

Um zu verhindern, dass Spammer mit zufälligen Subdomains die URIDNSBL umgehen, wird nur die Basis-Domain überprüft. Kommt in einer URL beispielsweise die Adresse [abc.example.com](http://abc.example.com) vor, so wird nur [example.com](http://example.com) abgefragt. In einigen Toplevel-Domains (etwa in Großbritannien) stehen nur Third-Level-Domains wie [example.co.uk](http://example.co.uk) zur Verfügung. Das Verfahren muss darauf vorbereitet sein.

Manchmal verschleiern Spammer die verwendeten Webadressen, indem sie sie durch Redirect-Dienste wie TinyURL<sup>47</sup> schleusen. Vor Abfrage einer URIDNSBL sollten Redirects in einer URL deshalb rekursiv aufgelöst werden. Das automatisierte Aufnehmen von neuen Adressen in eine URIDNSBL ist problematisch, weil z. B. viele Freemail-Provider oder Mailinglisten alle durchlaufenden E-Mails automatisch mit einem Anhang versehen, der häufig eine URL enthält.

Wie bei anderen DNSBLs sind die juristischen Aspekte zum Datenschutz zu berücksichtigen (siehe Kapitel 9.4).

## 9.18 Tokenbasierte und Challenge-Response-Verfahren

Spammer kümmern sich selten um Antworten (*bounces*) auf ihre E-Mails, und sie geben sich auch nicht die Mühe, auf etwaige Besonderheiten bei einzelnen Empfängern einzugehen. Manche Verfahren machen sich das zunutze, indem sie verlangen, dass ein bestimmtes *token* (eine kurze Zeichenkette oder ein anderes Merkmal) in der Empfängeradresse kodiert oder in einer bestimmten Header-Zeile oder im *body* der E-Mail erscheinen muss. E-Mail, die den Empfänger ohne das *token* erreicht, wird – mit einem entsprechenden Hinweis versehen – automatisch zurückgesandt. Der ursprüngliche Absender muss nun seine E-Mail mit dem *token* erneut versenden (Abb. 9.2a).

---

<sup>46</sup> Spam URI Realtime Blocklists: <http://www.surbl.org/>

<sup>47</sup> <http://tinyurl.com/>

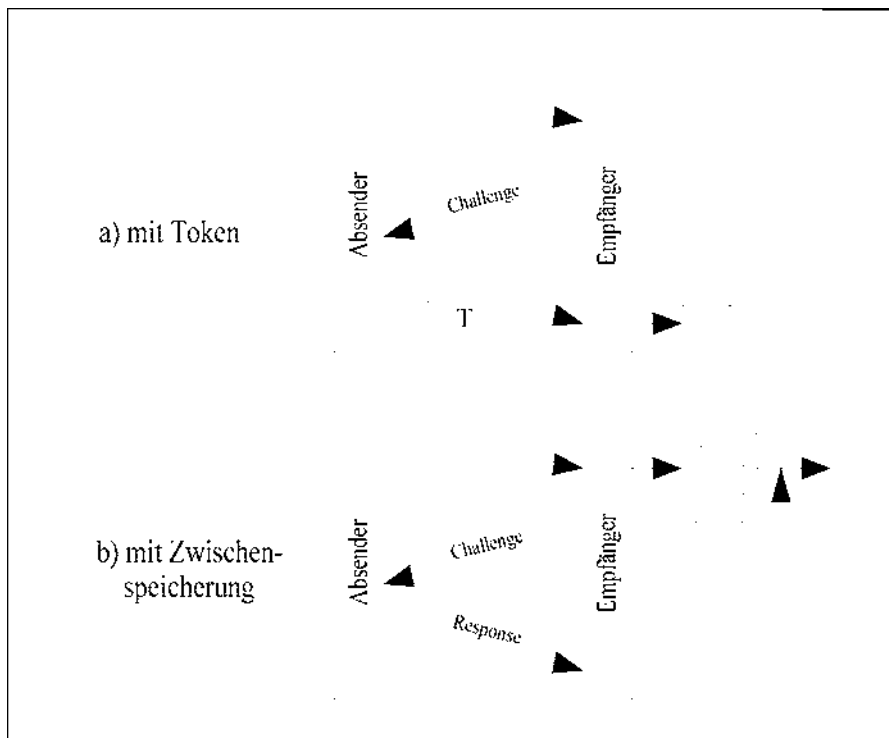


Abb. 9.2: Challenge-Response-Verfahren

Bei einem ähnlichen Verfahren erhält der vermeintliche Absender einer E-Mail eine *bounce*, die ihn dazu anhält, auf einem zusätzlichen, SMTP-unabhängigen Kanal (in der Regel per WWW) in Interaktion mit einem System des Empfängers zu treten, damit der die E-Mail erhält (Abb. 2b). Der Absender muss sie nicht erneut versenden, denn das Mailsystem des Empfängers hält sie für eine gewisse Zeit (einige Tage) vor, während es auf die Interaktion wartet. Um es einem Spammer besonders schwer zu machen, werden auf der Webseite manchmal auch so genannte CAPTCHA-Verfahren<sup>48</sup> eingesetzt, die es Menschen erlauben sollen, einfach zu antworten, nicht aber Computern.<sup>49</sup>

Verfahren, die den Absender zu einer zusätzlichen Aktion auffordern, werden als *challenge-response*-Verfahren (Aufforderung-Antwort-Verfahren), kurz CR-Verfahren, bezeichnet. In der Regel nehmen sie den Absender nach der Bestätigung in eine Whitelist auf, damit er das Prozedere nicht erneut durchlaufen muss. Alternativ können sie ihm auch ein *token* zuordnen, das er in Zukunft immer in die Mailadresse des Empfängers einbauen muss. Die Implementierung solcher Verfahren erfolgt in der Regel im MTA.

CR-Verfahren bringen mehrere Probleme<sup>50</sup> mit sich: Sie erschweren die gewünschte Kommunikation, und manche Absender werden eventuell die Kommunikation komplett aufgeben, weil sie das Verfahren als zu umständlich empfinden. Für Mailinglisten und andere seriöse Versender von Massenmail baut CR eine unüberwindliche Hürde auf, die durch Whitelists auf Seiten der Empfänger umgangen werden muss. In vielen Fällen wird das System versagen, wenn es sowohl beim Absender als auch beim Empfänger zum Einsatz kommt, weil beide Seiten sich gegenseitig blockieren.<sup>51</sup> Besonders umstritten sind CR-Systeme, weil sie *bounces* erzeugen können und damit kollateralen Spam, wenn ein gefälschter Absender verwendet wurde. Schließlich sind sie auch rechtlich dann kritisch, wenn im Rahmen des CR-Verfahrens wie auch bei der normalen Filterung Nachrichten ohne

<sup>48</sup> Completely Automated Public Turing Test to tell Computers and Humans Apart. <http://www.captcha.net/>

<sup>49</sup> Wobei die Accessibility, also die Zugänglichkeit für Behinderte, oft leidet.

<sup>50</sup> <http://kmsself.home.netcom.com/Rants/challenge-response.html>

<sup>51</sup> <http://www.freedom-to-tinker.com/archives/000389.html>

Kenntnis und Zustimmung des Berechtigten gelöscht werden. Ebenfalls unzulässig dürfte es auf Basis des Gebots der Datensparsamkeit sein, vom Absender zu verlangen, vor einer Zustellung seiner E-Mail personenbezogene Daten anzugeben.

Der Betrieb und die Nutzung von CR-Systemen ist also sehr aufwendig, die Zuverlässigkeit fraglich, aber dagegen steht der Vorteil, dass sie Spam quasi zu 100 % blockieren können, weil der Aufwand, sie zu umgehen, für die Spammer beträchtlich ist. Solange CR-Systeme wenig verbreitet sind, werden Spammer sich nicht die Mühe machen, Verfahren zu deren Umgehung zu entwickeln.

## 9.19 Proof-of-Work-Verfahren

Ähnlich wie Bezahlverfahren (siehe Kapitel 9.20) versuchen so genannte Proof-of-Work-Verfahren, den Versand von E-Mails teurer zu machen. Allerdings wird dazu kein echtes Geld verwendet, stattdessen muss der Absender dem Empfänger beweisen, dass er eine gewisse Menge an komplizierten Berechnungen durchgeführt hat. Da CPU-Leistung Geld kostet, ist der Effekt ein ähnlicher. Jede E-Mail kostet mehr Rechenleistung im Versand, und die Anzahl E-Mails, die ein einzelner Rechner versenden kann, ist erheblich eingeschränkt.

Ein wesentlicher Aspekt des Verfahrens ist, dass es für den Empfänger sehr einfach und billig sein muss, die Berechnung zu überprüfen. Es gibt diverse (kryptographische) Algorithmen, die diese Eigenschaft der Asymmetrie aufweisen, d. h. für den Absender ist der Aufwand groß, für den Empfänger gering.

Proof-of-Work-Verfahren benutzen in der Regel zusätzlich eine Whitelist, damit möglichst wenige legitime E-Mails die Mehrarbeit erfordern. Wichtig ist das vor allem auch für jene, die legitim viele E-Mails versenden. Das sind zum Beispiel Betreiber von Mailinglisten oder Webmail-Provider, die ihre Dienste häufig kostenlos anbieten und deshalb keine großen Rechnerfarmen betreiben können, um die aufwendigen Algorithmen zu berechnen.

Schon seit einigen Jahren gibt es das Hashcash-Verfahren<sup>52</sup>, das vom Camram<sup>53</sup>-Projekt und von SpamAssassin integriert wurde, es nutzt derzeit jedoch kaum jemand. Auch Microsoft beschäftigt sich im PennyBlack-Projekt<sup>54</sup> mit solchen Ideen.

Ob Proof-of-Work-Verfahren Spammer ausreichend einschränken können, ohne legitime Mailversender zu sehr zu behindern, ist unklar [LaCl04]. Hauptproblem ist hier, dass Spammer häufig nicht die eigenen Systeme zum Spammen verwenden, sondern Abertausende von Rechnern in Botnetzen, die zusammengenommen enorme Rechenkapazitäten haben.

## 9.20 E-Mail-Briefmarken

Die Kopplung von Bezahlssystemen an die Zustellung von E-Mails wird gelegentlich als mögliche Lösung des Spamproblems diskutiert.<sup>55</sup> Wenn man für jede E-Mail eine virtuelle Briefmarke kaufen muss, wird der Versand teurer, und der Spammer wird weniger E-Mail verteilen. Ein solches System würde aber erst einmal eine weltweite, zuverlässige und hochverfügbare Micropayment-Lösung erfordern, die mit extrem niedrigen Transaktionskosten auskommt. So etwas ist aber nicht in Sicht. Und selbst wenn ein solches System geschaffen werden könnte, ergäben sich wieder zahlreiche neue Missbrauchsmöglichkeiten, die das Opfer viel Geld kosten könnten, statt wie heute nur unangenehm

---

<sup>52</sup> <http://www.hashcash.org/>

<sup>53</sup> <http://www.camram.org/>

<sup>54</sup> <http://research.microsoft.com/research/sv/PennyBlack/>

<sup>55</sup> [http://fare.tunes.org/articles/stamps\\_vs\\_spam.html](http://fare.tunes.org/articles/stamps_vs_spam.html)

zu sein. Ungelöst ist auch die Frage, wie legitime Massenversender (etwa Betreiber von Mailinglisten) damit zurechtkommen sollen.

Es existiert noch eine weitere Variante dieser Idee: Statt an die Betreiber der Mailsysteme (also an die ISPs) geht die Bezahlung an den Empfänger. Bei erwünschten E-Mails kann er auf die Auszahlung verzichten, um den Absender nicht unnötig zu belasten. Der Effekt wäre, dass reguläre E-Mails nicht betroffen sind, das Lesen von Spam dem Empfänger aber Geld einbrächte. Aber so verlockend diese Idee klingt, die auch unter dem Namen *attention bonds* bekannt ist, so wenig wird sie in der Praxis umzusetzen sein.<sup>56</sup>

## 9.21 Bounce Address Tag Validation (BATV)

Die meisten Antispam-Verfahren wenden sich gegen „absichtlichen“ Spam, schützen aber nicht vor kollateralem Spam durch fehlgeleitete *bounces*. Eigentlich sollte es möglich sein, nur *bounces* auf E-Mails zu akzeptieren, die man auch selbst versandt hat. Unglücklicherweise ist es aber im SMTP nicht vorgesehen, Informationen mitzuliefern, die das ermöglichen.

Eine Fehlermail enthält meist eine Klartextfehlermeldung, die von einem Systemadministrator zu lesen und zu verstehen ist, aber von einem Computer schwer zu interpretieren, da sie keiner Standardisierung unterliegt. Insbesondere kann man sich nicht sicher sein, welche Informationen aus der ursprünglichen E-Mail noch in der Fehlermail vorhanden sind. Die Message-ID beispielsweise, die sich für eine Zuordnung eignen würde, ist nicht in allen *bounces* vorhanden.

Es gibt nur ein Datum, das sicher in der *bounce* zur Verfügung steht, und zwar das ursprüngliche Envelope-From. In der *bounce* taucht es als Envelope-To wieder auf. Wenn der eigene Mailserver statt der normalen Absenderadresse im Envelope-From einer ausgehenden E-Mail besondere Tracking-Informationen kodiert, dann kann er der *bounce* ansehen, ob sie echt ist. Finden sich die Tracking-Informationen im Envelope-To wieder und sind sie gültig, dann ist die *bounce* echt, sonst ist sie gefälscht oder von einer gefälschten E-Mail verursacht. Bei der Kodierung der Zusatzinformationen im *envelope* ist zu berücksichtigen, dass der *local-part* einer Mailadresse maximal 64 Zeichen lang sein sollte.<sup>57</sup>

Die Tracking-Information muss entweder kryptographisch abgesichert sein, damit sie ein Angreifer nicht fälschen kann, oder der MTA muss eine Datenbank führen, in der er sich die Informationen merkt und gegen die er eine eintreffende *bounce* abgleichen kann. Noch weiter zur Reduzierung des Traffic würde es beitragen, wenn auch jeder andere MTA die Gültigkeit einer solchen speziellen Mailadresse prüfen kann.

Bisher setzen nur wenige Mailsystem-Betreiber testweise solche Verfahren ein; ob sie sich in der Praxis bewähren, muss sich erst noch zeigen. Ohnehin wirken sie nur gegen kollateralen, nicht aber gegen den übrigen Spam.

Damit ein Angreifer eine abgehörte Tracking-Information nicht wieder verwenden kann, muss sie für jede E-Mail neu und einzigartig sein, z. B. indem man das Datum mit hineinkodiert. Beim Einsatz von Systemen, die die Envelope-From-Adresse interpretieren, ist daher mit Schwierigkeiten zu rechnen. Sie sehen bei gleichem Absender nicht mehr die immer gleiche Adresse, sondern jedesmal eine andere. Mailinglisten, die das Envelope-From zur Authentifizierung einsetzen, können dadurch verwirrt werden. Das Verfahren kann darüber hinaus mit dem Greylisting (siehe Kapitel 9.13) kollidieren.

---

<sup>56</sup> John R. Levine: An Overview of E-Postage. <http://www.taugh.com/epostage.pdf>

<sup>57</sup> RFC 2821, Abschnitt 4.5.3.1

Es gibt noch keinen Standard für diese Verfahren, aber es ist einer namens „Bounce Address Tag Validation (BATV)“<sup>58</sup> [LCSF04] in Arbeit.

## 9.22 Spamfallen

Spamfallen (engl. *spam traps*) dienen dazu, Spam anzulocken und einzufangen. Man kann dazu spezielle Mailadressen anlegen und z. B. auf seiner Webseite veröffentlichen oder man „recycelt“ nicht mehr benötigte Mailadressen.<sup>59</sup> Die Idee ist, dass diese Adressen nur Spam und keinen Ham auf sich ziehen. Der Inhalt der E-Mails ist also zum Trainieren von statistischen Filtern (siehe Kapitel 9.15) geeignet<sup>60</sup> oder kann in Prüfsummendatenbanken (siehe Kapitel 9.16) eingepflegt werden. Ebenso lässt sich die IP-Adresse des sendenden Rechners als Spamquelle in eine Blacklist eintragen.

Eine Variante ist es, offene Relays oder Proxies vorzutäuschen und damit große Mengen von Spam anzulocken<sup>61</sup>. Der für das System Verantwortliche muss aber unbedingt darauf achten, dass es tatsächlich keinen Spam verbreiten kann.

Besonders trickreiche Spamfallen generieren dynamische Mailadressen, die sich bei jedem Auslesen in Abhängigkeit von der IP-Adresse des *harvester* oder der Uhrzeit ändern. Auf diese Weise lässt das Log des Webservers oder auch die Adresse selbst Rückschlüsse auf den Spamverursacher zu.

Es existieren auch Webserver, die *harvester* geradezu in eine Falle locken (auch *honeypot* genannt), indem sie automatisch ganze Verzeichnisstrukturen voller Webseiten mit beliebig vielen Mailadressen generieren, die allesamt nicht existieren. Solche Maßnahmen erfordern viel Aufwand und Sorgfalt bei der Adressgenerierung, funktionierende Adressen dürfen nicht dabei sein. Solche Aktionen dienen dazu, den Spammer mit dem Versand großer Mengen von E-Mails zu beschäftigen, die nie einen menschlichen Empfänger erreichen werden.

Spamfallen erhöhen also die Effektivität von Filtermaßnahmen. Daneben können sie Spammer mit nutzloser Arbeit beschäftigen und unter Umständen Beweise für spätere Gerichtsverfahren gegen die Spammer sichern.

---

<sup>58</sup> <http://mipassoc.org/batv/>

<sup>59</sup> Dann kann es aber sein, dass auch Ham eingeht.

<sup>60</sup> Allerdings braucht man dann zusätzlich eine Quelle für Ham-Mails, weil statistische Filter mit Spam und Ham trainiert werden sollten.

<sup>61</sup> <http://www.lurhq.com/proxies.html> und <http://www.proxypot.org/>

## 10 Empfehlungen

Dieses Kapitel gibt dem Leser Hilfestellung zur Einführung einer Antispam-Lösung. Es konkretisiert die in den vorhergehenden Kapiteln dargestellten technischen, organisatorischen und rechtlichen Aspekte und stellt den Weg von den grundlegenden Überlegungen über die Aufstellung einer individuellen Policy bis zu Hinweisen zur Produktauswahl dar. Daneben gibt es allgemeine und Maßnahmen-Empfehlungen, die für einige Fallbeispiele näher aufgeschlüsselt werden.

### 10.1 Grundlegende Überlegungen

Vor der Einführung einer Antispam-Lösung sollte die bestehende Mail-Infrastruktur und -Policy untersucht und alle relevanten Details zusammengestellt werden. Basierend darauf werden dann die Maßnahmen passend zum individuellen Bedarf ausgewählt. Die Informationen sind auch Grundlage einer Anforderungsliste an Produkte.

- **Wer ist der Betreiber der Lösung?**  
Hier geht es um die Entscheidung, die Lösung selbst zu betreiben, von externen Anbietern einrichten und betreiben zu lassen oder komplett als externe Dienstleistung zu beziehen. Sie ist auch unter Sicherheitsaspekten zu fällen, insbesondere beim Einsatz von Dienstleistern für das eigene Mailsystem. So könnte die Vorgabe, Unternehmensdaten nur auf unternehmensinternen Massenspeichern abzulegen, den Einsatz eines von Dritten betriebenen Mailserverns verhindern.
- **Eigenbedarf oder Dienstleistung?** Antispam-Lösungen für den Eigenbedarf oder als Dienstleistung für Kunden unterscheiden sich oftmals beträchtlich voneinander.
- **Art und Bandbreite der Internetanbindung**  
Da der Mailverkehr über die Internetanbindung abgewickelt wird, ist deren Bandbreite und Art (ständige Verbindung oder temporäre Einwahl) wichtig. Wenn sehr viele Spam-Mails über diese Verbindung laufen, kann es neben hohen Kosten auch zu einer unbefriedigenden Übertragungsrate für andere Dienste kommen. Außerdem benötigen einige Antispam-Verfahren eine Internetanbindung für die Abfrage des DNS oder anderer Datenbanken. Der Betrieb eines SMTP-Servers setzt eine ständige Internetverbindung voraus, nur dann können protokollbasierte Verfahren eingesetzt werden.
- **E-Mail-Durchsatz**  
Die Menge der eingehenden E-Mails kann die Art der einzusetzenden Verfahren wesentlich beeinflussen. So bieten sich frequenzbasierte Blacklists erst bei einem nennenswerten Mailaufkommen an. Whitelists zur Vorfilterung von bekanntem Verkehr wiederum können bei hohem Mailaufkommen die Systemlast reduzieren.
- **Reaktionszeit / Geschwindigkeit**  
E-Mail ist ein asynchrones Medium. Absender und Empfänger wissen, dass eine E-Mail manchmal verzögert ankommt. Trotzdem erwarten heute viele Benutzer, dass ihre E-Mail nach sehr kurzer Zeit im Postfach des Empfängers landet. Manche Antispam-Maßnahmen führen zu Verzögerungen, die vielleicht nicht immer hinnehmbar sind.
- **Verfügbarkeit und Robustheit** Diese Aspekte stehen im engen Zusammenhang mit der Abhängigkeit vom Mailsystem. Dabei sollte hier an Ausfälle technischer Art ( z. B. defektes Serversystem), aber auch betrieblicher Art (Fehlkonfiguration) gedacht werden. Eine typische Überlegung sollte hier sein, welche Ausfallzeiten ( z. B. in Stunden pro Monat) hinnehmbar sind.
- **Anforderungen an Filtergenauigkeit und Effektivität**

Kein Antispam-System ist perfekt. Grundsätzlich ist abzuwägen, ob es wichtiger ist, dass möglichst viele Ham-Mails ankommen oder dass der Spam-Anteil möglichst gering ist.

- Blockieren vs. Quarantäne vs. Markieren

Hier sind Grundüberlegungen zum Umgang mit E-Mails notwendig. Insbesondere die drei grundsätzlichen Reaktionen auf Spam (Blockieren, Quarantäne, Markieren) sind sorgfältig abzuwägen (siehe Kapitel 8.6).

- Reporting

Je nach Art und Umfang des Reporting kann es Hinweise über die Effektivität der Spamfilter liefern. Typische Kenngrößen sind die Anzahl der E-Mails, erkannte Spam-Mails, Verteilung auf Tageszeiten und Wochentage, Beanstandungen der Filterung, Hotline-Anfragen, Anzahl der E-Mails je Art der Behandlung (Zustellen, Quarantäne, Markieren, Blockieren etc.), Aufwand für die Pflege der Lösung, Ressourcenbedarf oder Herkunft von Spam/Ham.

- Verfügbares technisches oder Bedien-Know-how

Das verfügbare Know-how für den Betrieb einer Antispam-Lösung kann bei der Entscheidung, ob das System selbst oder durch einen Dienstleister betrieben werden soll, eine wichtige Rolle spielen. Für den sinnvollen Betrieb einer größeren Antispam-Lösung ist ein breitgefächertes technisches Verständnis nötig. Neben der eigentlichen Lösung und dem Know-how zur sicheren Systemkonfiguration sind die technischen Prinzipien von Mailsystemen, Namensdiensten und manchmal Firewallsystemen wichtig.

- Technische Eingriffsmöglichkeit

Je nach technischer Platzierung des Systems ergeben sich unterschiedliche Eingriffsmöglichkeiten. Findet die Filterung auf dem Mailserver des Unternehmens statt, hat der Administrator naturgemäß viele Möglichkeiten der Einflussnahme, filtert bereits der Internet Service Provider, gibt es weniger Eingriffsmöglichkeiten.

- Administrierbarkeit und Regelabgleich

Wer viel Wert auf eine sehr fein abgestufte Justierung der Filtermechanismen legt, sollte passende Lösungen einsetzen. Bei sehr hohem Mail-Aufkommen führt manchmal kein Weg an einer detailliert konfigurierbaren Lösung vorbei. Sehr vielfältige Optionen erfordern oftmals ein tief gehendes Know-how.

- Unternehmensstrukturen und Bezugsbereiche

Filialen, Tochterunternehmen und Mehrheitsbeteiligungen können unter Umständen technische Architekturen (mehrere separate Mailserver-Farmen), aber auch die Verantwortlichkeiten beeinflussen. Der Bezugsbereich definiert die Mail-Empfänger, die die Antispam-Lösung bedienen soll. Hier ist zu überlegen, ob die Dienstleistung für alle Bereiche einheitlich organisiert ist oder z. B. die Filtermechanismen für jeden Bereich angepasst werden müssen. Beispielsweise müssen Hotline- oder Support-Abteilungen aufgrund ihrer intensiven Kundenkontakte eventuell mit anderen Mechanismen versorgt werden als die Personalabteilung.

- Kommunikationspartner

Sind die Kommunikationspartner eindeutig identifizierbar, können deren E-Mails mit einfacheren Maßnahmen behandelt werden als für unbekannte Teilnehmer. Das bedeutet eine Entlastung des Gesamtsystems.

- Rechtliche Rahmenbedingungen

Rechtliche Aspekte sind in Kapitel 6 im Allgemeinen und je nach Maßnahme in Kapitel 8 und 9 im Speziellen beschrieben. So kann zum Beispiel ein erhöhter Bedarf an Datenschutz die Konzeption der Antispam-Lösung beeinflussen: Viele Maßnahmen beruhen auf zentralen (und

oft von Dritten betriebenen) Datenbanken, die IP-Adressen, Mailadressen oder Mailinhalte speichern.

- Abrechnung/Kostenvergütung der Antispam-Maßnahmen

Die Verrechnung der Kosten ist ein wichtiger Punkt für einen Spamschutz-Dienstleister. Auch innerbetriebliche Kostenverrechnungen können notwendig sein. Hier sollte Klarheit bestehen, ob sie möglich und notwendig sind und welche Berechnungsparameter angesetzt werden können.

- Betriebswirtschaftliche Aspekte

Der Kostenrahmen für Planung, Anschaffung/Integration und Betrieb einer derartigen Lösung sollte definiert werden. Gleichzeitig sollten die durch Spam auftretenden Kosten (inkl. möglicher Systemausfälle durch Spam) berücksichtigt werden. Ansätze für die Kostenberechnung finden sich in Kapitel 5.

## 10.2 Aufstellen einer Antispam-Policy

Eine Antispam-Policy beschreibt die organisatorischen und technischen Aspekte einer Antispam-Lösung. Jede Policy muss individuell zu den lokalen Gegebenheiten passen. Für Selbständige und kleinere Firmen genügt häufig ein informeller Ansatz, größere Firmen sollten die Policy und darauf fußende Entscheidungen strukturierter angehen. Die Antispam-Policy wird in unternehmensweite Sicherheits-, Internet- und E-Mail-Policies integriert.

### 10.2.1 Organisatorische Aspekte

Dieses Kapitel beschreibt die organisatorischen Belange, die eine Antispam-Policy definieren sollte. Sie umfassen sowohl den Betrieb als auch Anweisungen für Endbenutzer von Mailsystemen.

#### Verantwortung

Die Verantwortung für das Antispam-System sollte klar geregelt sein, sie kann auch verteilt werden. Folgende Verantwortungsbereiche sollten klar definiert sein:

- Verantwortung für den technischen Betrieb
- Verantwortung für die Aktualität und Pflege der Filter
- Ansprechpartner für Kunden oder Mitarbeiter Einbindung in das Incident-Management

Sowohl für die Bewältigung von Sicherheitsproblemen mit dem Antispam-System als auch bei aktuell laufenden Spam-Attacken muss eine organisatorische Schnittstelle zum Incident-Management (Management von Sicherheitszwischenfällen) vorhanden sein. Es darf keine Unklarheit bezüglich der Ansprechpartner und Verantwortlichkeiten geben, da im Ernstfall keine Zeit für Klärungen organisatorischer Art besteht. Da die Bewältigung von Angriffen oftmals nur durch die Zusammenarbeit mehrerer organisatorischer Einheiten möglich ist, ist die koordinierende und steuernde Funktion des Incident-Managements hilfreich.

#### Einbindung in das Abuse-Management

Das Abuse-Management stellt den Ansprechpartner für Dritte dar. Diese organisatorische Schnittstelle ist zu definieren, um auch bei selbst verursachtem Spam auf die Beschwerden Dritter reagieren zu können. Üblicherweise sollte das Abuse-Management unter der Mailadresse `abuse@DOMAIN` erreichbar sein [RFC2142].

#### Einbindung in Hotlines und User-Helpdesks

Die Einführung und der Betrieb einer Antispam-Lösung verursachen zusätzliche Anrufe bei Hotlines oder User-Helpdesks (UHD). Treten *false positives* oder *false negatives* auf, müssen die damit

verbundenen Anfragen bearbeitet werden können. Für eine Akzeptanz der Antispam-Lösung ist die Einbindung in den Anwender-Support unbedingt notwendig.

### **Verhaltensregeln für Mitarbeiter oder Kunden**

Die Verhaltensregeln zum Umgang mit Spam legen fest, was mit als Spam erkannter E-Mail geschehen soll. Sie können einen Beitrag zur Spam-Vermeidung leisten. Die Verhaltensregeln sind typischerweise in einer *acceptable use policy* oder einem *code of behaviour* festgehalten, Dokumente, die die wesentlichen Punkte in kurzen, einprägsamen und einfach zu merkenden Schlagzeilen enthalten.

### **Kunden-AGB / Betriebsvereinbarung**

Als verbindliche Grundlage für den Einsatz einer Antispam-Lösung sind Allgemeine Geschäftsbedingungen (AGB) oder Betriebsvereinbarungen notwendig, die explizit in die Rechte der Endanwender eingreifende Maßnahmen gestatten. Sie sollten auch regeln, wie lange E-Mails in Quarantäneverzeichnissen vorgehalten werden. Sie sind außerdem geeignet, typische Verhaltensregeln zu vereinbaren und auf weitere verbindliche Dokumente ( z. B. *acceptable use policy*) hinzuweisen. AGB und Betriebsvereinbarungen können auch Maßnahmen im Fall von Zuwiderhandlungen definieren. Da Betriebsvereinbarungen nicht mit einzelnen Mitarbeitern, sondern mit deren Interessenvertretung abgeschlossen werden, müssen die Inhalte für alle Mitarbeiter zugänglich sein.

### **Betriebliche Prozesse**

Ein Betriebshandbuch beschreibt alle Schritte des Betriebs einer technischen Infrastruktur und der Pflege des Systems. Diese Prozesse sind unabdingbar für den professionellen Betrieb von IT-Systemen. Die Antispam-Policy sollte das Betriebshandbuch explizit ansprechen und als verbindliche Arbeitsgrundlage deklarieren.

## **10.2.2 Technische Aspekte**

Dieses Kapitel beschreibt die technischen Aspekte, die eine Antispam-Policy definieren sollte.

### **Technische Einbindung in bestehende Infrastrukturen**

Antispam-Maßnahmen sind eng mit der Mail-Infrastruktur verzahnt. Insbesondere bei umfangreicheren, aus mehreren Komponenten bestehenden Systemen ist die Beschreibung der Einbindung in die Mail-Infrastruktur wichtig. Zur Umsetzung eines effektiven und effizienten Spamschutzes sind unter Umständen grundsätzliche Änderungen an der bestehenden Mailserver-Struktur notwendig.

Antispam-Systeme sollten in bestehende Management-Systeme eingebunden sein. Das gewährleistet eine zeitnahe Reaktion auf Ausfälle oder sonstige Systemalarme und sichert die Verfügbarkeit des eigenen Mailsystems.

### **Technische Einbindung in bestehende Sicherheitsmaßnahmen**

Bestehende Sicherheitsmaßnahmen sollen alle Systeme schützen, auch die Antispam-Systeme.

- An Firewalls und Routern sind manchmal Filterregeln zu ändern und Verkehrsflüsse zu steuern.
- Die neuen Systeme sind bei der Angriffserkennung (*intrusion detection/prevention*) zu berücksichtigen.
- Antiviren-Systeme sind einzubeziehen.
- Auditmaßnahmen sind zu erweitern.
- Der Erfassungsbereich von Schwachstellen-Scannern sollte auch die Antispam-Systeme umfassen.
- Korrelierendes Sicherheitsmonitoring sollte für diese Systeme erweitert werden.

### Härtungsmaßnahmen für die technischen Antispam-Systeme

Antispam-Systeme können je nach Ausprägung an sehr exponierter und somit angreifbarer Stelle untergebracht sein. Oft sind sie sehr nah am Übergang zum Internet platziert. Daher spielt das Härten eine wichtige Rolle. Die Maßnahmen des BSI-Grundschutzhandbuches für Internet-nahe Serversysteme sollten immer umgesetzt sein.

### Wirkungsmechanismus der Antispam-Lösung

Wenn ein sehr komplexes Antispam-System etabliert werden soll, ist die Beschreibung des grundsätzlichen Zusammenwirkens der Komponenten eine wichtige Grundlage für den Betrieb, aber auch bei Notfall-Situationen oder Störungen.

Die Antispam-Policy sollte daher insbesondere die Einsatzorte der Antispam-Maßnahmen, die Kombination der Filterstufen und möglichen Rückkopplungswege (siehe Kapitel 8.5.2) und die nachfolgende Behandlung von Mails wie Quarantäne, Markierung, Zustellung etc. beschreiben (siehe Kapitel 8.6). Dazu gehören Information darüber, wie User auf ihre E-Mails in der Quarantänezone zugreifen können und über deren Inhalt informiert werden.

### Konfiguration der Antispam-Lösung

Wie jede andere technische Sicherheitsmaßnahme in der IT-Sicherheitspolicy festgehalten wird, sollte auch die Konfiguration der Antispam-Lösung in der Antispam-Policy beschrieben sein. Vergleichbar zur Beschreibung einer Firewall-Policy sollte auch diese detaillierte Konfigurationsbeschreibung nicht öffentlich zugänglich sein, sondern nur den Verantwortlichen für den Betrieb. Internet-Provider werden aber häufig ihre Kunden über Details der Konfiguration informieren müssen, da diese ein berechtigtes Interesse daran haben, zu erfahren, wie ihre E-Mail gefiltert wird.

## 10.2.3 Notfall-Policy

Das Internet ist unberechenbar. Ist im täglichen Betrieb die Spamflut noch in den Griff zu bekommen, kann ein neuartiger Virus, ein neuer Wurm oder eine Spamwelle ein Mailsystem sehr schnell überlasten. Entsprechend müssen die Maßnahmen in Krisenzeiten anders aussehen als im Normalbetrieb.

Der Administrator muss sich darauf vorbereiten und Notfallpläne ausarbeiten, die in das Betriebshandbuch integriert werden. Bei akuter Gefahr steht häufig nicht mehr die Frage nach *false negatives* und *false positives* im Vordergrund, sondern die Verfügbarkeit des Mailsystems an sich.

Daher ist zuerst der Begriff „Notfall“ für die eigenen Bedürfnisse zu definieren und festzulegen, wie und von wem ein Notfall erkannt wird.

Weiterhin sind die zu benachrichtigenden Personen festzulegen. Das können einerseits die Verantwortlichen sein, aber idealerweise auch das zuständige Computer-, Notfalloder ein vergleichbares Team.

Anschließend sollten die konkreten Notfallmaßnahmen beschrieben werden. Um die Verfügbarkeit des Systems sicherzustellen, ist es manchmal notwendig, härtere Maßnahmen als im Normalfall zu ergreifen, etwa sonst nur markierten Spam direkt abzulehnen. IP-Adressen lassen sich schon auf Netzwerkebene (im Router oder Firewall) filtern, verstopfte Mailqueues lassen sich deaktivieren und später in Ruhe bearbeiten.

Mailfilter können bei hohem Mailaufkommen überlastet werden. Für solche Fälle sollten Pläne, zum Beispiel zu Ausweichmöglichkeiten oder zum Deaktivieren einzelner Filter, bereitstehen. Der Ausfall von Filtern darf den Mailverkehr nicht komplett verhindern oder zum Löschen erwünschter E-Mails führen (*failsafe*).

## 10.3 Allgemeine Empfehlungen

Dieses Kapitel beschreibt die allgemeinen Empfehlungen im Zusammenhang mit Spam, während im nächsten Kapitel (10.4) dann die Empfehlungen für spezifische Antispam-Maßnahmen gegeben werden.

Empfehlungen für Versender legitimer Massenmail finden sich im Kasten am Ende von Kapitel 6.6.

### 10.3.1 Sichere Konfiguration

Für den Betrieb und die Konfiguration von IT-Systemen sollten immer die grundlegenden Schutzmechanismen umgesetzt werden, wie sie im BSI-Grundschutzhandbuch dargestellt sind [GSHB04].

Unzureichend gesicherte Proxies lassen sich als Mailrelays von Spammern missbrauchen. Daher sind HTTP(S)- und SOCKS-Proxies unbedingt gegen die missbräuchliche Nutzung abzusichern (siehe Kapitel 7.1.2).

Die Mailclients der Anwender sollten so konfiguriert werden, dass sie keine externen Inhalte laden (siehe Kapitel 4.3.4).

### 10.3.2 Eigene Mail-Infrastruktur

Der Transport aller aus- und eingehenden E-Mails sollte über ein zentrales Mailsystem erfolgen, das auch für die Filterung (*ingress* und *egress*) zuständig ist. Sinnvollerweise trennt man die Server für aus- und eingehende E-Mail, damit der Ausfall eines Systems, etwa während eines Virenangriffs, das andere nicht beeinflusst. Versender legitimer Massenmail sollten diese von einem anderen Server aus versenden als ihre normale E-Mail, um bei Filtermaßnahmen Dritter gegen den Massenmail-Server ihre normale E-Mail-Kommunikation zu erhalten.

Die eigenen Mailserver sollten nur die Annahme von E-Mails aus dem Internet für eigene Adressen gestatten und eigene ausgehende E-Mails in Richtung Internet zulassen (siehe Kapitel 7.1.1). Sofern für ausgehende E-Mail die Authentifizierung nicht über die IP-Adresse erfolgen kann, sollte SMTP AUTH verwendet werden. Im Mailserver sollten außerdem technische Maßnahmen gegen Wörterbuchangriffe zum Einsatz kommen (siehe Kasten im Kapitel 4.3.3).

Die Empfehlungen für Filtermaßnahmen für den ein- und ausgehenden Mailverkehr sind im Kapitel 10.4 aufgeführt. Grundsätzlich sollten Filtermaßnahmen so frühzeitig wie möglich ansetzen, da die durch Spam verursachten Kosten umso höher sind, je weiter er bis zum Endanwender vordringt.

Vom Filter erkannte Wurm-Mails sollten direkt abgelehnt werden. Erkannte Viren-Mails sollten abgelehnt oder in eine Quarantäne verschoben werden. Für sonstige Spam-Mails gibt es je nach Organisation verschiedene Erfordernisse, siehe dazu Kapitel 8.6.

Es kann trotz großer Sorgfalt passieren, dass aus dem eigenen Netz Spam verteilt wird, z. B. nach einer Vireninfection. Um so einen Fall frühzeitig zu erkennen, ist es sinnvoll, Statistiken über den Mailverkehr zu erheben und auf Anomalien zu achten. Die gängigen DNSBLs sollten regelmäßig daraufhin überprüft werden, ob eigene IP-Adressen dort gelistet sind. Als Ansprechadresse für Meldungen von Mitarbeitern, Kunden und Dritten sollte die Mailadresse `abuse@DOMAIN` eingerichtet werden, über die ein spezielles Abuse-Team, die technische Hotline oder der Postmaster erreichbar ist.

E-Mails an beliebige *local-parts* einer eigenen Domain, die sich keinem gültigen Empfänger zuordnen lassen, sollten abgewiesen werden, statt sie in das Admin- oder Postmaster-Postfach einzusortieren (*catch all*). Da Spammer häufig zufällig generierte Mailadressen verwenden, erspart man sich so große Mengen an Spam.

### 10.3.3 Gestaltung von Webanwendungen

Eine wichtige Maßnahme ist das Absichern von Formmail-Skripten (siehe Kapitel 7.1.3) innerhalb von Webseiten. Hier sollten alle Mailempfänger fest im Skript konfiguriert sein.

Auf Webseiten werden häufig auch Adressen per mailto:-Link öffentlich bereitgestellt. Neben einer sorgfältigen und sparsamen Auswahl der Adressen ermöglicht die Angabe von Zusatzinformationen im mailto: -Link (siehe Kapitel 7.2.5) das spätere Filtern im Rahmen einer Heuristik. Eine Verschleierung der Mailadresse (Kapitel 7.2.2) ist ebenfalls denkbar, jedoch meistens nur von begrenztem Nutzen.

### 10.3.4 Verhalten des Endanwenders

Das Verhalten des Endanwenders spielt eine wichtige Rolle bei der Vermeidung von Spam. Die wichtigste Grundregel ist, niemals auf Spam zu antworten (siehe Kasten in Kapitel 7.2). Spam-Mails sollten möglichst nicht einmal angeschaut werden, damit z. B. Web-Bugs (praktisch nicht sichtbare, von einem Webserver nachgeladene HTML-Elemente) ohne Wirkung bleiben, und auch die beworbenen Webseiten sollten nicht aufgerufen werden.

#### Antispam-Verhaltensregeln

- Spams immer ungelesen löschen
- Niemals auf Spam antworten
- Niemals Spam an andere weiterleiten
- Niemals Kettenbriefe weiterleiten
- Niemals auf E-Mails antworten, die ein „unsubscribe“ versprechen, und keine „Unsubscribe“-Links anklicken
- Keine Postings in Newsgroups mit der Firmen-Mailadresse
- Notwendige Registrierungen nur über anonyme Mailadressen

Eine Reduktion der Anzahl von Mailadressen (Kapitel 7.2.3) auf das unbedingt notwendige Maß reduziert auch die Anzahl von Spam-Mails. Das Einfügen von Zusatzinfos in eigenen E-Mails (Kapitel 7.2.4) kann die Spamfilterung erleichtern.

Da E-Mails in der Regel über öffentliche Netze übertragen werden, bietet die Mail-Verschlüsselung einen hohen Gewinn an Vertraulichkeit der Informationen. Für die Spamfilterung kann eine verschlüsselte Mail zusätzlich ein Indiz für Ham sein. Verschlüsselte E-Mails lassen sich an einer aufwendigen Inhaltsanalyse vorbeileiten.

Zusätzlich sollten die Mitarbeiter für die Phishing-Problematik sensibilisiert werden.

## 10.4 Maßnahmenempfehlungen

| Kap. | Maßnahme                              |           |           | Kap. | Maßnahme                                |           |           |
|------|---------------------------------------|-----------|-----------|------|---|-----------|-----------|
|      |                                       | Ausgehend | Eingehend |      |   | Ausgehend | Eingehend |
| 9.1  | Filterung durch Personen              | -         | O         | 9.12 | RHSBLs                                  | -         | O         |
| 9.2  | Protokollbasierte Verfahren           | O         | O         | 9.13 | Greylisting                             | -         | +         |
| 9.3  | White- und Blacklists                 | -         | +         | 9.14 | Heuristische Inhaltsanalyse             | +         | +         |
| 9.4  | DNS-basierte Blacklists (DNSBLs)      | -         | +         | 9.15 | Statistische Inhaltsanalyse             | +         | +         |
| 9.5  | IP-Blacklisting durch Frequenzanalyse | +         | +         | 9.16 | Prüfsummenvergleich                     | +         | +         |
| 9.6  | Sperre des SMTP-Ports                 | +         | n/a       | 9.17 | URIDNSBLs                               | +         | +         |
| 9.7  | MTAMARK                               | +         | +         | 9.18 | Token- und Challenge-Response-Verfahren | -         | -         |
| 9.8  | Existenzprüfung der Absenderadresse   | -         | O         | 9.19 | Proof-of-Work-Verfahren                 | -         | X         |
| 9.9  | MARID-Verfahren: SPF und SenderID     | -         | O         | 9.20 | E-Mail-Briefmarken                      | -         | X         |
| 9.10 | S/MIME und PGP                        | O         | O         | 9.21 | Bounce Address Tag Validation (BATV)    | -         | X         |
| 9.11 | MASS-Verfahren: DomainKeys und IIM    | -         | O         | 9.22 | Spamfallen                              | n/a       | n/a       |

+: empfehlenswert O: eingeschränkt empfehlenswert -: nicht verwenden X: experimentell

Tabelle 10.1: Maßnahmenempfehlungen für die Filterung ausgehender und eingehender E-Mail

Im Folgenden sind die in Kapitel 9 im Detail beschriebenen Maßnahmen in empfehlenswerte, eingeschränkt empfehlenswerte, nicht zu verwendende und experimentelle Maßnahmen für die Filterung eingehender E-Mail untergliedert. Diese sowie die Empfehlungen für die Filterung ausgehender E-Mail finden sich auch in der Tabelle 10.1.

### 10.4.1 Empfehlenswerte Maßnahmen

- Protokollbasierte Verfahren (siehe Kapitel 9.2)
  - EHLO/HELO-Check (siehe Kapitel 9.2 a)

Generell zu empfehlen ist die Ablehnung einer Verbindung von Servern, die beim EHLO/HELO-Dialog statt ihrer eigenen die IP-Adresse des empfangenden Servers (oder dessen Hostnamen) oder eine Localhost-Adresse (127.0.0.0/8) angeben. Sonst ist die Anwendung dieser Maßnahme aufgrund zu erwartender hoher Raten von *false positives* nicht zu empfehlen.

- SMTP-Pipelining (siehe Kapitel 9.2 b) Empfehlenswert. Vorsicht ist aber bei einem Smarhost geboten, weil viele Mailclients sich nicht standardkonform verhalten.
- Einsatz von TLS (siehe Kapitel 9.2 c)

Der Einsatz von TLS ist generell und nicht nur in Bezug auf Spam empfehlenswert, denn die Verschlüsselung des SMTP-Datenstroms stellt die Vertraulichkeit von E-Mails während der Übertragung sicher. Auch deutet die Verwendung von TLS darauf hin, dass die so übertragenen Mails erwünscht sind. Die Verwendung von TLS kann somit zumindest als ein „Ham-Aspekt“ in das Scoring von E-Mails einfließen. Das Ver- und Entschlüsseln der Daten kostet jedoch viel Rechenzeit, sodass es zu Ressourcen-Engpässen bei stark

ausgelasteten Systemen kommen kann. Der reibungslose Mailversand und -empfang beim Einsatz von TLS auch zu Stoßzeiten ist somit vor Einführung der Maßnahme durch Tests unter realen Einsatzbedingungen sicherzustellen. In Hochlastphasen lässt sich TLS notfalls ausschalten.

- White- und Blacklists (siehe Kapitel 9.3)

White- und Blacklists, die IP- und Mailadressen verzeichnen, von denen E-Mail generell erwünscht oder unerwünscht ist, sind ein einfaches und günstiges Basisverfahren. Der Einsatz dieser Maßnahme ist grundsätzlich zu empfehlen. Sind mehrere Antispam-Maßnahmen im Einsatz, sollten die White- und Blacklists zuerst überprüft werden, damit später ansetzende Maßnahmen keine fehlerhaften Entscheidungen treffen. Die Eintragung von IP-Adressen ist auf jeden Fall sinnvoll, Eintragungen von Mailadressen dagegen nur, wenn eine Absenderauthentifizierung damit verbunden ist. Ausnahmen sind Whitelists für einen kleinen Personenkreis, da es hier sehr unwahrscheinlich ist, dass ein Spammer die richtigen Einträge errät. Die Eintragungen in White- und Blacklists sind mit Datum und Grund des Eintrags sowie dem Namen des Eintragenden zu protokollieren. Vor allem bei Blacklists sollte der Eintragende jedem Eintrag ein Verfallsdatum mitgeben, nach dessen Ablauf der Eintrag automatisch ungültig wird.

- DNS-basierte Blacklists (DNSBLs) (siehe Kapitel 9.4)

DNS-basierte Blacklists sind sehr verbreitet und arbeiten ausgesprochen effizient, sollten wegen nicht zu vernachlässigender False-Negative- und False-Positive-Raten jedoch nicht als alleiniges Verfahren zum Einsatz kommen. Es sollten immer mehrere DNSBLs parallel verwendet werden, um die Zuverlässigkeit zu erhöhen. Nur wenn mehrere DNSBLs sich über das Ergebnis einig sind, ist das Ergebnis als ausreichend zuverlässig anzusehen. Da sich DNSBLs meist im Verantwortungsbereich Dritter befinden, ist eine ständige Kontrolle im Bezug auf rationales Verhalten notwendig. Dafür bieten sich laufend aktualisierte Statistiken über Trefferquoten an. Bei großen Mailsystemen lohnt es sich eventuell, eine lokale Kopie einer externen DNSBL einzurichten oder auch lokale Blacklists zu betreiben, die die DNSBL-Technik nutzen.

- IP-Blacklisting durch Frequenzanalyse (siehe Kapitel 9.5)

Das Blacklisting von IP-Adressen mit Hilfe der Frequenzanalyse braucht einen ausreichend hohen Mailedurchsatz, um statistisch signifikante Werte zu liefern. Es ist deshalb nur in großen Mailsystemen einsetzbar. Das Feintuning dieser Maßnahme und die Definition von Ausnahmeregeln erfordern einen hohen Administrationsaufwand. Organisationen mit geringerem Mailedurchsatz können eine fremdbetriebene, kommerzielle Lösung verwenden. Bei hohem Mailedurchsatz ist die Frequenzanalyse aufgrund der hohen Zuverlässigkeit sehr empfehlenswert.

- Sperre des SMTP-Ports (siehe Kapitel 9.6)

Das Sperren des SMTP-Ports ist eine grundsätzlich für alle nicht am Mailverkehr teilnehmenden Systeme zu empfehlende Maßnahme. Größere Einrichtungen stellen damit sicher, dass die Anwender E-Mails nur über die dafür vorgesehenen Mailserver versenden. Die Gefahr des Missbrauchs durch *open proxies* und *open relays* verringert sich dadurch erheblich.<sup>1</sup> Der administrative Aufwand beschränkt sich auf eine einmalige Konfigurierung der Router oder Firewalls, die Maßnahme ist somit auch ausgesprochen günstig. Internet-Provider können eine Sperrung nur mit Zustimmung des Kunden vornehmen.

- MTAMARK (siehe Kapitel 9.7)

Hier handelt es sich um ein neues, noch kaum verbreitetes Verfahren, das ähnlich der SMTP-Port-Sperre einem direkten Mailversand etwa durch *open proxies* vorbeugen soll. Es ist derzeit nicht abzusehen, ob es jemals eine große Verbreitung finden wird. Die passive Nutzung von MTAMARK ist allgemein zu empfehlen, also ein positiver Eintrag für eigene Mailserver und

---

<sup>1</sup> Ebenso verringert sich die Gefahr durch Viren und Würmer.

unter Umständen auch ein negativer Eintrag für Rechner, die keine E-Mail versenden dürfen. Provider brauchen für letzteres aber das Einverständnis des Kunden. Zur aktiven Filterung kann MTAMARK verwendet werden, allerdings ist aufgrund der geringen Verbreitung zur Zeit kein wesentlicher Erfolg zu erwarten. Dabei sollten positive Einträge zum Abschalten von Greylisting oder zu einem niedrigeren Spamscore führen, negative Einträge zu einem höheren Spamscore. Je mehr Spam von offiziellen Mailservern ausgeht, desto weniger wirksam ist MTAMARK. Die weitere Entwicklung sollte beobachtet werden.

- Greylisting (siehe Kapitel 9.13)

Greylisting bringt einerseits sehr gute Filterraten, führt aber andererseits zu einer Verzögerung bei der Zustellung einiger E-Mails. Die Nutzung von Greylisting ist in solchen Bereichen nicht empfehlenswert, in denen der Empfänger der E-Mails auf eine reibungslose und schnelle Kommunikation angewiesen ist und er es mit vielen neuen Kontakten zu tun hat. Vor allem im Rahmen der beruflichen Nutzung ist eine Verzögerung der Zustellung einer E-Mail um eine halbe Stunde und mehr oft störend. Die in Kapitel 9.13 angesprochenen Probleme beispielsweise mit Einmaladressen oder Mailinglisten sind durch eine zusätzliche Whitelist lösbar, die grundsätzlich für Greylisting-Systeme anzuraten ist. Das Verfahren bindet auf Empfänger- und Absenderseite zusätzliche Ressourcen. Sonst ist Greylisting mit den genannten Einschränkungen derzeit empfehlenswert. Zu berücksichtigen ist aber, dass die Spammer sich bei weiterer Verbreitung dieses Verfahrens anpassen werden; so geht der Trend zurzeit wieder zur Auslieferung von Spam über legitime Mailserver. Die Filterrate wird sich in Zukunft also verschlechtern.

- Heuristische Inhaltsanalyse (siehe Kapitel 9.14)

Die heuristische Inhaltsanalyse ist ein Standardverfahren, dessen Einsatz grundsätzlich empfehlenswert ist, denn es ist einfach und relativ günstig zu implementieren und liefert sehr gute Filterraten. Bei entsprechender Ausbildung kann der Administrator sehr schnell auf neu auftretende Spam-Muster reagieren. Wichtig ist es, die Konfiguration aktuell zu halten, meist über regelmäßige Software-Updates.

- Statistische Inhaltsanalyse (siehe Kapitel 9.15)

Auch die statistische Inhaltsanalyse hat sich als Standardverfahren etabliert. Sie ist ebenfalls einfach und günstig zu implementieren. Sie stützt sich auf eine Datenbank mit Spam- und Ham-Merkmalen, die sich durch Training im laufenden Betrieb füllt. Bei homogeneren Benutzergruppen kann der Administrator die Trainingsdaten aggregieren und an zentraler Stelle bereitstellen, anderenfalls führt der Endanwender eine eigene Trainingsbasis. Wegen der aufwendigen Algorithmen ist die statistische Inhaltsanalyse sehr rechenintensiv und daher nur in Verbindung mit einer Vorfilterung beispielsweise durch IP-basierte Verfahren zu empfehlen. Dieses Verfahren hält in mehr und mehr MUAs Einzug, steht in absehbarer Zeit gegebenenfalls als optionale Maßnahme für jeden Endanwender zur Verfügung.

- Prüfsummenvergleich (siehe Kapitel 9.16)

Der Prüfsummenvergleich kann bei ausreichender Datenbasis ausgesprochen effektiv sein, der Erfolg hängt aber von der Beteiligung möglichst vieler Organisationen ab, die Prüfsummen bilden und in die zentrale Datenbank einspeisen. Aufgrund seiner Effektivität und der einfachen Implementierung ist dieses Verfahren, das Bestandteil vieler kommerzieller Produkte ist, grundsätzlich zu empfehlen. Wie bei allen Verfahren, die eine von Dritten betriebene Datenbank benutzen, ist entsprechende Vorsicht angebracht: Man sollte sich nicht bedingungslos auf die Antworten verlassen.

- URIDNSBLs (siehe Kapitel 9.17)

In E-Mails vorkommende URLs können gegen URIDNSBLs geprüft werden. Das Verfahren ist sehr effektiv und allgemein zu empfehlen.

- Spamfallen (siehe Kapitel 9.22)

Bei Spamfallen handelt es sich nicht um ein Verfahren, das Spam direkt bekämpft. Vielmehr liefern die Spamfallen Daten für Blacklists und prüfsummenbasierte Filter und können für das Training statistischer Mailfilter verwendet werden. Spamfallen sind somit nur für größere Einrichtungen zu empfehlen, die genau das im Sinn haben und den Mehraufwand und die Kosten dafür rechtfertigen können.

### 10.4.2 Eingeschränkt empfehlenswerte Maßnahmen

- Filterung durch Personen (siehe Kapitel 9.1)

Die rein manuelle Filterung ist nur bei niedrigem Mailaufkommen umsetzbar, kann aber *false negatives* und *false positives* nahezu ausschließen. Wichtig ist dies beispielsweise für Abuse-Abteilungen, die häufig Beschwerden mit zitiertem Spam bearbeiten müssen. Steigt das Mailaufkommen jedoch, versagt der menschliche Filter immer häufiger und die Vorteile des Verfahrens verschwinden. Da Dritte jede E-Mail sichten, gibt es bei der Filterung durch Personen unter Umständen datenschutzrechtliche Probleme.

- Existenzprüfung der Absenderadresse (siehe Kapitel 9.8)

Auf jeden Fall verwendet werden sollte die Überprüfung der Domain, weil das schnell und einfach geht. Dieses Verfahren filtert zuverlässig E-Mails mit nicht existierenden Absenderadressen und somit einen erheblichen Anteil der Spam-Mails heraus. Aufgrund eines erhöhten Ressourcenbedarfs und wegen der Gefahr von *false positives* ist die Überprüfung der ganzen Adresse zurzeit dagegen als experimentell anzusehen.

- MARID-Verfahren: SPF und SenderID (siehe Kapitel 9.9)

Die MARID-Verfahren sind noch recht neu. Die weitere Entwicklung, insbesondere was eine Standardisierung angeht, sollte beobachtet werden. Zur Vorbereitung auf die Nutzung sollte jede E-Mail der eigenen Organisation über zentrale Mailserver gehen, für die passende SPF-DNS-Einträge vorhanden sind. Am Schluss des Eintrags sollte ein `?al 1` stehen, der ausdrückt, dass E-Mails nicht nur von den eingetragenen, sondern auch von anderen Servern kommen können. Für die Mailfilterung eignen sich diese Maßnahmen noch nicht. Für weitere Details siehe [Send04].

- S/MIME und PGP (siehe Kapitel 9.10) Ebenso wie TLS ist der Einsatz von S/MIME oder PGP auch abseits der Spam-Problematik empfehlenswert, da diese Verfahren Vertraulichkeit und Integrität von E-Mails sicherstellen. Der Absender ist bei bekanntem Schlüssel oder X.509-Zertifikat einwandfrei ermittelbar. Eine Filterung allein anhand der Tatsache, dass S/MIME- oder PGP-Informationen in der E-Mail vorhanden sind, ist nicht zu empfehlen, denn mit PGP signierte Spam-Mails sind bereits im Umlauf. Als ein Ham-Kriterium von vielen kann diese Tatsache zumindest in das Scoring von E-Mails eingehen. Weil S/MIME und PGP weltweit nicht sehr verbreitet sind, ist die Nutzung als Antispam-Maßnahme zurzeit nur eingeschränkt zu empfehlen.

- MASS-Verfahren: DomainKeys und IIM (siehe Kapitel 9.11)

Die MASS-Verfahren sind noch recht neu und nicht weit verbreitet, nur DomainKeys (siehe Kapitel 9.11.1) ist bei einer nennenswerten Anzahl an Organisationen im Einsatz. Die weitere Entwicklung, insbesondere was eine Standardisierung angeht, sollte beobachtet werden. Zur Vorbereitung auf die Nutzung sollten alle E-Mails der eigenen Organisation über zentrale Mailserver geleitet werden, die passende MASS-Einträge im *header* vornehmen. Für die Mailfilterung eignen sich diese Maßnahmen noch nicht. Für weitere Details siehe [Send04].

- RHSBLs (siehe Kapitel 9.12)

Da die Absenderdomain in einer E-Mail beliebig gefälscht werden kann, sind RHSBLs erst bei gleichzeitigem Einsatz von Verfahren zur Absenderauthentifizierung sinnvoll. Noch liegen nicht genug Erfahrungen mit der Kombination von Absenderauthentifizierung und RHSBLs vor, eine vorsichtige Nutzung ist aber zu empfehlen. Dabei gelten die gleichen Aspekte wie bei den

DNSBLs, RHSBLs, die nur Domains enthalten, die sich sicher Spammern zuordnen lassen, sind auch ohne Authentifizierung verwendbar.

### 10.4.3 Maßnahmen, die nicht genutzt werden sollten

- Filterung auf leeres MAIL FROM (siehe Kapitel 9.2 d)

Dieses Verfahren hat eine Reihe von Nachteilen und, zumindest im Hinblick auf die Spam-Bekämpfung, kaum einen Vorteil. Hauptnachteil, wie in Kapitel 9.2 d beschrieben, ist die Unterdrückung von legitimen *bounces*, was für einen MTA nicht hinnehmbar ist. Darüber hinaus versendet kaum ein Spammer Mails mit einem leeren Envelope-From. Dieses Verfahren ist somit nicht empfehlenswert.

- Tokenbasierte und Challenge-Response-Verfahren (siehe Kapitel 9.18)

Diese Verfahren verhindern die Zustellung von Spam zwar recht sicher, büren jedoch anderen Kommunikationsteilnehmern zusätzliche Arbeit auf, was nicht selten dazu führt, dass legitimer Mailverkehr überhaupt nicht zustande kommt. Solche Verfahren haben darüber hinaus mit Interoperabilitätsproblemen zu kämpfen. Von einem Einsatz ist daher abzuraten.

### 10.4.4 Experimentelle Maßnahmen

Einige der in dieser Studie aufgeführten Maßnahmen sind noch nicht ausgereift oder derzeit überhaupt nicht einsetzbar. Es liegen keine verlässlichen Zahlen zur Effektivität vor, und mögliche Nachteile sind noch nicht ausreichend untersucht. Die hier aufgeführten Verfahren sollte – wenn überhaupt – nur erfahrenes IT-Personal unter kontrollierten Bedingungen einsetzen:

- Besondere Filterregeln auf dem Secondary MX (siehe Kapitel 9.2 e)
- Ausnutzen von Timeouts (siehe Kapitel 9.2 f)
- Proof-of-Work-Verfahren (siehe Kapitel 9.19)
- E-Mail-Briefmarken (siehe Kapitel 9.20)
- Bounce Address Tag Validation (BATV) (siehe Kapitel 9.21)

## 10.5 Fallbeispiele

| Verhalten   | IP-Adresse       | Mailadresse      | Inhalt     |
|-------------|------------------|------------------|------------|
| TLS         | Black/Whitelists | Black/Whitelists | Manuell    |
| Pipelining  | DNSBLs           | Existenzprüfung  | Heuristik  |
| EHL0/HELO   | MTAMARK          | MARID            | Statistik  |
| Greylisting | Frequenzanalyse  | MASS             | Prüfsummen |
|             |                  | S/MIME, PGP      | URIDNSBLs  |
|             |                  | RHSBLs           |            |

Abb. 10.1: Generell und eingeschränkt empfehlenswerte Maßnahmen

Dieses Kapitel stellt die folgenden Fallbeispiele vor:<sup>2</sup>

- Privatanwender, Selbständige und Kleinunternehmer
- Mittelständische Unternehmen und Ämter
- Großunternehmen, Konzerne und Ministerien mit nachgeordneten Behörden
- Universitäten und Hochschulen
- Provider

Jedes Fallbeispiel enthält Annahmen, die als typische Merkmale für diesen Fall stehen. Basierend auf diesen Merkmalen wird die geeignete Auswahl an Maßnahmen beschrieben. Ein konkreter Fall mag sich davon unterscheiden. Allerdings bieten die Beschreibungen zusammen mit den Ausführungen in den vorhergehenden Kapiteln die notwendigen Informationen für die Zusammenstellung einer eigenen, individuellen Lösung.

Die Abbildung 10.1 enthält eine Aufstellung aller empfehlenswerten oder eingeschränkt empfehlenswerten Maßnahmen für die Filterung eingehender E-Mail. In den folgenden Kapiteln wird die Abbildung jeweils wiederholt und die für dieses Fallbeispiel anwendbaren Maßnahmen hervorgehoben. Die Grafik soll dem Überblick dienen, in Einzelfällen können sich Abweichungen ergeben, die der Text beschreibt.

### 10.5.1 Privatanwender, Selbständige und Kleinunternehmer

| Verhalten   | IP-Adresse       | Mailadresse      | Inhalt     |
|-------------|------------------|------------------|------------|
| TLS         | Black/Whitelists | Black/Whitelists | Manuell    |
| Pipelining  | DNSBLs           | Existenzprüfung  | Heuristik  |
| EHLO/HELO   | MTAMARK          | MARID            | Statistik  |
| Greylisting | Frequenzanalyse  | MASS             | Prüfsummen |
|             |                  | S/MIME, PGP      | URIDNSBLs  |
|             |                  | RHSBLs           |            |

Abb. 10.2: Maßnahmen für Privatanwender, Selbständige und Kleinunternehmer

Besonders typische Aspekte in diesem Fallbeispiel sind:

- langsame, nicht-ständige Internetanbindungen
- oftmals gering ausgeprägtes technisches Know-how zu Antispam- und Mailsystemen
- Hosting und Betrieb des Mailsdienstes beim ISP

Aufgrund der eingeschränkten Eingriffsmöglichkeiten in diesem Fallbeispiel bietet sich als Empfehlung an, einen **ISP zu verwenden, der Antispam-Maßnahmen für den Kunden bereitstellt**. Der ISP sollte Spam in einen **Spam-Ordner** zustellen.

Alternativ ist der Einsatz eines in den Mailclient integrierten Spamfilters denkbar. Diese Variante würde allerdings bedeuten, dass die ohnehin langsame Internetanbindung durch die unnötigen Spam-

<sup>2</sup> Die Fallbeispiele unterscheiden sich von denen im Kapitel 5 verwendeten, weil die Betonung hier nicht auf den Kosten, sondern auf den unterschiedlichen Maßnahmen liegt.

Mails belastet wird und der Anwender sich um die Konfiguration des lokalen Filters kümmern müsste.

Wenn der ISP einen Spamfilter nach aktuellem Stand der Technik anbietet, ist durch zusätzlichen Einsatz eines lokalen Filters keine signifikante Verbesserung des Filterergebnisses zu erwarten. Sollte die Filterung durch den ISP nicht ausreichend sein, ist ein **Mailclient mit eingebautem statistischem Filter**, der entsprechend trainiert wird, zu empfehlen. Darüber hinaus können Mailadressen, mit denen man in Kontakt steht, in eine Whitelist eingetragen werden.

Auch wenn der ISP die Spamfilterung vornimmt, gelten die Grundregeln für den Umgang mit Spam („Niemals auf Spam antworten“). Auch die sichere Konfiguration des Arbeitsplatzes („Aktuelles Betriebssystem und Virenschutz verwenden“, „Unbenutzte Rechner ausschalten“) sowie dessen gesicherte Anbindung an das Internet („Personal Firewall verwenden“, „Zugangsrouten mit Firewallfunktionen ausstatten“, etc.) sollte immer gewährleistet sein. Das BSI-Grundschutzhandbuch gibt entsprechende Hinweise.

Schulen sind technisch in einer ähnlichen Situation wie Kleinunternehmer. Hier ist aber besonders auf den Jugendschutz zu achten, z. B. durch den Einsatz entsprechender Filter.

### 10.5.2 Mittelständische Unternehmen und Ämter

| Verhalten   | IP-Adresse       | Mailadresse      | Inhalt     |
|-------------|------------------|------------------|------------|
| TLS         | Black/Whitelists | Black/Whitelists | Manuell    |
| Pipelining  | DNSBLs           | Existenzprüfung  | Heuristik  |
| EHLO/HELO   | MTAMARK          | MARID            | Statistik  |
| Greylisting | Frequenzanalyse  | MASS             | Prüfsummen |
|             |                  | S/MIME, PGP      | URIDNSBLs  |
|             |                  | RHSBLs           |            |

Abb. 10.3: Maßnahmen für mittelständische Unternehmen und Ämter

Die Bandbreite der Lösungen ist hier besonders groß, als typische Aspekte in diesem Fallbeispiel sind aber anzunehmen:

- Mangel an Know-how-Trägern und Zeit
- Mailserver werden häufig durch Dritte implementiert und betrieben
- technische Eingriffsmöglichkeiten aufgrund der Dienstleistung Dritter reduziert
- relativ schmalbandige Internetanbindung (~ 2 Mbit/s)

Aufgrund des Mangels an technischem Wissen über Mailsysteme kommen zwar für interne Zwecke Mailserver zum Einsatz, für den Übergang in das Internet jedoch oftmals von Dritten betriebene Systeme. Außerdem besteht ein hoher Kostendruck, der umfangreichen und pflegeintensiven Antispam-Maßnahmen mit signifikanten laufenden Kosten entgegensteht.

Als empfehlenswerte Antispam-Lösung bietet sich der Einsatz einer kommerziellen **All-in-One-Lösung** an, die entweder auf dem zentralen oder externen Mail- oder Antivirus-Server installiert wird oder als separates Gerät inklusive Software (Appliance). Diese Lösungen enthalten meist eine Kombination von **Blacklist- (DNSBLs)** mit inhaltsbasierten (oft auch **kollaborativen**) **Verfahren**. Diese Lösungen werden komplett vom Hersteller gepflegt, dadurch ergibt sich ein relativ niedriger Betriebsaufwand. Allerdings ist zu beachten, dass die Hersteller solcher Lösungen oftmals eine

Rückkopplung der Spamfilter beim Kunden auf ihre zentralen Listen und Datenbanken einsetzen. Dafür gelangen zumindest die Eckdaten der E-Mails zum Hersteller.

Aufgrund der typischerweise recht schmalbandigen Internetanbindung wäre es zusätzlich denkbar, mit dem ISP eine erste Spamfilterung auf Basis zuverlässiger Blacklists oder verhaltensbasierter Verfahren (siehe Kapitel 8.1.4) zu vereinbaren.

Selten ist eine umfangreiche IT-Sicherheitspolitik einschließlich detaillierter Sicherheitsmaßnahmen für alle Systeme vorhanden. Daher sei hier nochmals auf die grundsätzlichen Empfehlungen des BSI im **Grundschutzhandbuch** [GSHB04] verwiesen.

Unbedingt ist an die zugehörige **Betriebsvereinbarung** bezüglich der Spamfilterung und die **Information** aller Mitarbeiter zu denken.

### 10.5.3 Großunternehmen und Ministerien mit nachgeordnetem Bereich

| Verhalten   | IP-Adresse       | Mailadresse      | Inhalt     |
|-------------|------------------|------------------|------------|
| TLS         | Black/Whitelists | Black/Whitelists | Manuell    |
| Pipelining  | DNSBLs           | Existenzprüfung  | Heuristik  |
| EHLO/HELO   | MTAMARK          | MARID            | Statistik  |
| Greylisting | Frequenzanalyse  | MASS             | Prüfsummen |
|             |                  | S/MIME, PGP      | URIDNSBLs  |
|             |                  | RHSBLs           |            |

Abb. 10.4: Maßnahmen für Großunternehmen und Ministerien

Die nachstehenden Punkte sind besonders typisch für diese Fallgruppe:

- breitbandige, redundante Anbindung an das Internet mit statischen IP-Adressen
- hohes ein- und ausgehendes Mailvolumen
- unterschiedliche Bezugskreise an Mailempfängern
- bestehende Sicherheitspolitik und Sicherheitsregeln

Für den Betrieb der IT sind zwei gegensätzliche Aspekte zu finden: Outsourcing und Eigenbetrieb. Steht eine IT-Abteilungen mit gutem technischem Know-how zur Verfügung und will man sich mehr Einflussmöglichkeiten bewahren, wird man auf den Eigenbetrieb setzen. Beim Betrieb und Hosting der Mailserver durch Outsourcing-Partner bestehen dagegen nur reduzierte technische Eingriffsmöglichkeiten.

Aufgrund der unterschiedlichen Bezugskreise bietet sich die **Kombination mehrerer Verfahren** an, um ein den unterschiedlichen Bedürfnissen angepasstes Filterverhalten zu erreichen.

Das sowohl bei einem Outsourcing-Dienstleister als auch beim Eigenbetrieb zu unterstellende technische Know-how ermöglicht den Einsatz wirkungsvoller, aber auch technisch anspruchsvollerer Verfahren. Die bei diesen Verfahren unvermeidliche Pflege können die mit dem Betrieb der Lösung betrauten IT-Mitarbeiter übernehmen.

Als Basisverfahren sollten hier **White- und Blacklists** (siehe Kapitel 9.3) zum Einsatz kommen. Ein sehr hohes Mailaufkommen rechtfertigt den Einsatz von **Blacklists auf Basis der Frequenzanalyse** (siehe Kapitel 9.5). Blacklists auf Basis **mehrerer DNSBLs** (siehe Kapitel 9.4) sind ebenfalls sinnvoll, **Greylisting** (siehe Kapitel 9.13) kann eine gute Alternative sein.

Als zweite Filterstufe an zentraler Stelle eignen sich die relativ einfach umzusetzenden und zu pflegenden **heuristischen Verfahren** (siehe Kapitel 9.14), die jedoch ständig auf Aktualität geprüft werden müssen. Gleiches gilt für **kollaborative Verfahren** (siehe Kapitel 9.16), die beim Einsatz kommerzieller Produkte eine nennenswerte Filterleistung aufweisen können. Insbesondere für die zentralen inhaltsbasierten Filter sollten Umgehungswege für besondere Bezugsbereiche wie Abteilungen für das Abuse-Management definiert sein. Ebenfalls zentral oder am Arbeitsplatz der Mailempfänger können **statistische Verfahren wie Bayes-Filter** (siehe Kapitel 9.15) sinnvoll eingesetzt werden.

Auf jeden Fall sollten alle ausgehenden E-Mails über zentrale Mailserver geleitet werden, andere Rechner im Unternehmensnetz sollten keine E-Mail direkt ins Internet senden dürfen. Für Unternehmen sinnvoll ist auch das **Filtern ausgehender E-Mails**, z. B. durch eine Frequenzanalyse. Dabei sind die rechtlichen Aspekte zu prüfen.

Zeichnet für den IT-Betrieb ein Outsourcing-Partner verantwortlich, ist den reduzierten technischen Eingriffsmöglichkeiten über den Weg von Service Level Agreements (SLAs) Rechnung zu tragen. In den Verträgen sollte die Notwendigkeit von Anpassungen und Aktualisierungen in Abhängigkeit von den Bedürfnissen des Unternehmens festgelegt werden. Spezielle SLAs bezüglich der Wirksamkeit der Antispam-Maßnahmen steigern den Nutzen für das Unternehmen.

Unabhängig von den Verfahren ist der Aufwand für die vollständige Integration einer Antispam-Policy in die IT-Sicherheitspolicy einschließlich der notwendigen Abstimmungsprozesse und zu beachtender Mitbestimmungsrechte ein nicht zu unterschätzender Aufwand.

#### 10.5.4 Universitäten und Hochschulen

| Verhalten   | IP-Adresse       | Mailadresse      | Inhalt     |
|-------------|------------------|------------------|------------|
| TLS         | Black/Whitelists | Black/Whitelists | Manuell    |
| Pipelining  | DNSBLs           | Existenzprüfung  | Heuristik  |
| EHLO/HELO   | MTAMARK          | MARID            | Statistik  |
| Greylisting | Frequenzanalyse  | MASS             | Prüfsummen |
|             |                  | S/MIME, PGP      | URIDNSBLs  |
|             |                  | RHSBLs           |            |

Abb. 10.5: Maßnahmen für Universitäten und Hochschulen

Für Hochschulen sind die folgenden Gegebenheiten typisch:

- Mailservices werden sowohl für den Eigenbedarf als auch als Dienstleistung für Dritte angeboten.
- Ein hohes Niveau an technischer Kompetenz ist vorhanden.
- Vielfältige organisatorische Strukturen und Bezugsbereiche.
- Freizügige Handhabung von Sicherheitsvorgaben und -policies.

Aufgrund der unterschiedlichen Bezugskreise und insbesondere auch aufgrund der Bereitstellung von Mailservices für Dritte bietet sich die **Kombination mehrerer Verfahren** an, um ein den unterschiedlichen Bedürfnissen angepasstes Filterverhalten zu erreichen. Eine Vorfilterung kann z. B. durch **protokollbasierte Verfahren, DNSBLs** und **Greylisting** erfolgen, danach kann dann jede Abteilung weitere (z. B. **inhaltsbasierte**) Filtermaßnahmen treffen. Für eine effektive **Frequenzanalyse** wird das Mailaufkommen in vielen Fällen wohl nicht ausreichen.

Wegen der in den IT-Bereichen der Universitäten zu erwartenden hohen technischen Kompetenz bieten sich effektive, aber auch technisch anspruchsvolle Verfahren an. Dabei kann es durchaus auch im Sinne einer Hochschule sein, teilweise noch **experimentelle Verfahren** einzusetzen. Auch der Einsatz von **Spamfallen** ist bei großen Hochschulen eventuell sinnvoll.

Unbedingt ist an eine Filterung des ausgehenden Mailverkehrs zu denken, z. B. durch eine **SMTP-Port-Sperre** an den Netzgrenzen.

Besondere Aufmerksamkeit sollte auch den Nutzungsbedingungen gelten: Die Dienstleistung wird für viele relativ unabhängige Organisationseinheiten angeboten. Da eine einheitliche Sicherheitspolicy nicht zu erwarten ist, sollten die Nutzungsbedingungen für die angebotenen Mailservices diesem Umstand mit umfassenden, detaillierten Ausführungen begegnen.

### 10.5.5 Internet-Provider

| Verhalten   | IP-Adresse       | Mailadresse      | Inhalt     |
|-------------|------------------|------------------|------------|
| TLS         | Black/Whitelists | Black/Whitelists | Manuell    |
| Pipelining  | DNSBLs           | Existenzprüfung  | Heuristik  |
| EHLO/HELO   | MTAMARK          | MARID            | Statistik  |
| Greylisting | Frequenzanalyse  | MASS             | Prüfsummen |
|             |                  | S/MIME, PGP      | URIDNSBLs  |
|             |                  | RHSBLs           |            |

Abb. 10.6: Maßnahmen für Internet-Provider

Wegen des Grundsatzes der möglichst frühen Filterung und des vorhandenen technischen Know-hows sind Internet-Provider häufig gefragt, eine zentrale Spamfilterung anzubieten. Sie darf allerdings nur in Absprache mit den Kunden erfolgen oder wenn die AGB entsprechende Klauseln vorsehen. Dem Kunden sollte die Möglichkeit gegeben werden, Einfluss auf die Spamfilterung zu nehmen.

Die **Nutzungsbedingungen** oder **AGB** sollten verbindliche Passagen über das Verbot des Spamversandes enthalten. Provider, die anonyme oder leicht zu erlangende Accounts anbieten (z. B. Freemail-Provider oder Hosting-Provider) sollten durch geeignete Verfahren (CAPTCHA, telefonischer Rückruf oder dergl.) sicherstellen, dass nicht automatisiert große Mengen an Accounts angelegt werden können. Zugangsprovider für Endanwender können durch **SMTP-Port-Sperren** (siehe Kapitel 9.6) oder durch die Veröffentlichung von **MTAMARK-Einträgen** (siehe Kapitel 9.7) die Gefahr durch Spam aus dem eigenen Netz einschränken. Wichtig ist eine **Abuse-Abteilung**, die schnell auf Meldungen über Spam aus dem eigenen Netz reagiert.

Zugangsprovider, die ausschließlich Internet-Connectivity anbieten, benötigen keine technischen Maßnahmen zur Filterung eingehenden Spams. Die Verantwortung für die Abwehr und Vermeidung von Spam liegt vollständig bei den Kunden.

Für Service-Provider, die neben der Connectivity auch Mailsdienste für ihre Kunden anbieten, gilt – abhängig von der eigenen Größe und der der Kunden – im Prinzip das in den Kapiteln 10.5.2 und 10.5.3 Beschriebene. Provider werden dabei häufig als Outsourcing-Partner die gesamte Viren- und Spamfilterung für ihre Kunden übernehmen.

Vom Mailsystem des Providers aus versandte E-Mails sollten durch Methoden wie die Frequenzanalyse überwacht werden. Besondere Anforderungen bestehen bei Webmail-Anbietern, die ihr Web-Interface gegen Spamversuche absichern müssen. Webhosting-Provider sollten sicherstellen,

dass von den von ihnen gehosteten Systemen kein Spam ausgeht. Dazu sind Maßnahmen wie Tests auf *open relays*, *open proxies* und unsichere Formmail-Skripte sinnvoll.

Bei größeren Providern können inhaltsbasierte Verfahren häufig nicht oder erst in späteren Filterstufen zum Einsatz kommen, weil sie zu ressourcenintensiv sind. Dagegen sind lokal gepflegte **White- und Blacklists** (siehe Kapitel 9.3), **DNSBLs** (siehe Kapitel 9.4), die **Frequenzanalyse** (siehe Kapitel 9.5) und **Greylisting** (siehe Kapitel 9.13) sinnvoll einsetzbar.

Insbesondere Provider mit vielen Kunden in wenigen Domains sollten **SPF**-Einträge (siehe Kapitel 9.9) veröffentlichen und **DomainKeys** (siehe Kapitel 9.11) zur Kennzeichnung eigener E-Mails nutzen.

## 10.6 Hinweise zur Produktauswahl

Vor dem Einsatz einer Antispam-Lösung sollten die idealen Produkte und deren Kombinationen identifiziert sein. Dazu sollten die grundlegenden Überlegungen um konkrete technische und kommerzielle Details erweitert werden. Mit diesen Details können dann die in Frage kommenden Produkte gefunden werden. Zur konkreten Auswahl eignen sich Vergleichstests von Fachzeitschriften.<sup>3</sup>

Die nachfolgenden Evaluationspunkte teilen sich auf in

- die wesentlichen technischen Details,
- Fragen zur Leistungsfähigkeit des (Produkt-)Anbieters und
- kommerzielle Fragestellungen.

Jeder dieser Evaluationspunkte sollte nach Erhalt aller Informationen mit einer Gewichtung versehen werden. Zusätzlich können einzelne, besonders wichtige Eigenschaften als K.-o.-Kriterien gesetzt werden.

### Wesentliche technische Details sind unter anderem:

- Antispam-(Filter-)Methode:  
Hier sollten zumindest die in Frage kommenden Methoden verglichen werden. Sinnvoll ist es aber auch, alle vom Hersteller angebotenen Verfahren zu erfragen. Hersteller, die eine Kombination von Verfahren anbieten, sollten darüber Auskunft erteilen, welche Verfahren den wichtigsten Teil ausmachen.
- Wie hoch ist die False-Positive- und False-Negative-Rate? Die Angaben der Anbieter sind häufig übertrieben und selten direkt vergleichbar. Der Anbieter sollte in der Lage sein, die Basis seiner Angaben zu erklären.
- Konfiguration und Anpassung:  
Können die einzelnen Maßnahmen ausreichend konfiguriert werden? Gibt es geeignete Schnittstellen und Oberflächen zur Konfiguration und Anpassung durch Systemadministratoren und Abuse-Team-Mitarbeiter?
- Gewünschte Spam/Ham-Behandlungsverfahren:  
Die notwendigen Methoden sollten hier aufgelistet und alle bereitgestellten Verfahren abgefragt werden. Insbesondere für die Quarantäne-Verfahren sollten detaillierte Informationen zur Verfügung stehen.

---

<sup>3</sup> <http://www.nwfusion.com/reviews/2004/122004spampkg.html>

- Ausnahmen für Abuse-Adressen: Lassen sich einzelne Adressen oder Abteilungen von der Spamfilterung ausnehmen?
- Newsletter und Mailinglisten:  
Wie sind Ausnahmen für legitime Massenmails definierbar? Können einzelne Anwender, die sich von einem Newsletter „abmelden“, indem sie ihn als Spam klassifizieren, diesen Newsletter für andere Anwender blockieren?
- Zu bewältigender Durchsatz in E-Mails pro Stunde oder Tag:  
Die Hersteller und Dienstleister sollten die Durchsatz-Leistung des Systems beziffern. Dabei ist die Kombination aus Hardware und Software zu bewerten. Systeme müssen ausreichende Leistungsreserven für Hochlastzeiten haben.
- Hochverfügbarkeit und Loadbalancing: Besteht eine hochverfügbare Umgebung (eventuell an verteilten Standorten), sollte die Antispam-Lösung in dieses Konstrukt hineinpassen.
- Technische Daten der Netzwerkschnittstellen: Die verfügbaren Netzwerkschnittstellen sollten in Bezug auf Anschlüsse, Übertragungsverfahren und Durchsatz zu den Gegebenheiten passen.
- Ausführung (Software oder Appliance):  
Appliance-Lösungen versprechen einen relativ niedrigen eigenen Aufwand für die Installation, während Software-Lösungen oft die höhere Flexibilität bezüglich ihrer Integrationsfähigkeit bieten.
- Schnittstellen zum Systems-Management, Operating und Security-Monitoring: Sofern übergreifende Management-Systeme im Einsatz sind, sollte die Unterstützung entsprechender Agenten und Verfahren geprüft werden.
- Schnittstellen zum Reporting: Besteht Bedarf an automatischen Reportingverfahren, sind diese zu evaluieren. Auch die Abfrage einzelner Reports sollte möglich sein.
- Schnittstellen zum User-Helpdesk: Für Anfragen beim User-Helpdesk ist eine Schnittstelle zur Antispam-Lösung mit nichtadministrativen, eingeschränkten Rechten notwendig.

#### **Weitere Details zum Betrieb der Lösung und Leistungsfähigkeit des (Produkt-) Anbieters:**

- Betreibt der Anbieter ein Helpdesk (Hotline)? Ist er mittels Telefon, E-Mail und Fax erreichbar?
- Kann der Anbieter selbst oder durch entsprechende Partnerfirmen Installations- und Beratungsdienstleistungen vor Ort anbieten?
- Gibt es einen 7x24h-Support und ist er gewünscht?
- Kann der Anbieter eine Reaktionszeit für die Behebung von Störungen garantieren?
- Gibt der Hersteller/Lieferant Schwachstellen-Berichte zu seinem Produkt heraus?
- Werden Handbücher zur Installation und Administration in deutscher Sprache mitgeliefert?
- Geht die Spamfilterung auf die Besonderheiten der deutschen oder internationalen Umgebung ein?
- Wie häufig erfolgen Software- und Konfigurations-Updates? Einige Verfahren, etwa die heuristische Inhaltsanalyse, bedürfen der regelmäßigen Aktualisierung.

#### **Für eine betriebswirtschaftliche Bewertung kommen folgende Punkte in Betracht:**

- Einmaliger Preis der Software-Lizenzen bezogen auf die Anzahl der Anwender oder Mailadressen. Gelten andere Bezugsgrößen als die Useranzahl oder Mailadressen, sollten sie angegeben werden.
- Einmaliger Preis der Hardware für eine Installation, die den technischen Anforderungen genügt

- Jährlicher Basispreis für Support während der Bürozeiten, Aufpreis für 7x24h Support.
- Jährlicher Preis für Patches, Updates und Upgrades auf neue Major-Releases der Antispam-Software
- Jährlicher Preis für Wartung/Support der Hardware und des Betriebssystems
- Schulung der Administratoren (Installation und Administration, Schulungsdauer erfragen). Auch die Möglichkeit einer Vor-Ort-Schulung ist falls notwendig zu erfragen.
- Pauschalpreis für Installation durch Anbieter oder Hersteller
- Preis/Arbeitsstunde für die Beratung und Konfigurierung durch den Anbieter
- Aufwandsabschätzung für die Beratung und Konfigurierung

Beim Outsourcing des Betriebs gelten im Prinzip die gleichen Kriterien. Zusätzlich müssen, falls notwendig, Wartungsfenster vereinbart werden.

Der Einführung einer neuen Software sollte eine Testphase vorausgehen, in der die Antispam-Software für die Ermittlung der besten Konfiguration reale E-Mails unter realen Bedingungen filtert. In dieser Phase wird man E-Mails grundsätzlich nicht ablehnen, sondern nur markieren.

## Schlusswort

Die vorliegende Studie lässt erkennen, wie teuer und komplex das Spamproblem ist, aber auch, wie viele Mittel es gegen die Spamflut gibt. Spam ist kein Problem, das sich ausschließlich mit juristischen Mitteln lösen lässt, denn es handelt sich um ein internationales Phänomen, dem mit einer überwiegend nationalen Rechtsprechung und Gesetzgebung kaum beizukommen ist.

Bei der Entwicklung von technischen Maßnahmen zur Vermeidung und vor allem zur Filterung von Spam gab es in den letzten Jahren große Fortschritte. Dadurch steht heute eine beachtliche „Werkzeugkiste“ an Maßnahmen zur Verfügung, die sich an lokale Gegebenheiten und Anforderungen anpassen lässt. Der Einsatz von Filtern auf dem Stand der heutigen Technik kann das Problem so weit eingrenzen, dass einzelne Mitarbeiter oder Kunden nicht mehr wesentlich beeinträchtigt werden. Trotzdem bleibt Spam ein enormer Kostenfaktor und ein ständiges Sicherheitsproblem für jede Organisation.

Bei allen Problemen sollte nicht vergessen werden, wie nützlich und für viele unverzichtbar das Medium E-Mail in nur wenigen Jahren geworden ist. Die technischen und juristischen Grundlagen sowie die beispielhaften Kostenrechnungen und die Empfehlungen geben dem Leser hoffentlich eine gute Basis für die Planung und Umsetzung eigener Schritte zur Erhaltung der E-Mail als überaus praktisches Kommunikationsmittel.

## Glossar

### Adress-Harvesting

siehe **Harvesting**

### ASRG (Anti-Spam Research Group)

Gruppe in der IRTF (Internet Research Task Force) zur Erforschung des Spamproblems (<http://asrg.sp.am/>)

### Autoreply

Automatisch erzeugte Antwortmail

### Autoresponder

Programm, das automatisch auf eine E-Mail antwortet, z. B. um dem Absender mitzuteilen, dass der Empfänger in Urlaub ist.

### Backup-MX

Secondary **MX**, der nicht vom Besitzer einer Domain, sondern von jemand anderem betrieben wird. Der Backup-MX soll dann einspringen, wenn der Primary MX nicht erreichbar ist.

### BASE64-Kodierung

Eine Form der Kodierung einer E-Mail, bei der nicht übertragbare 8-Bit-Zeichen durch 6-Bit-Zeichen ersetzt werden. Wird häufig in **MIME**-Nachrichten verwendet.

### BATV (Bounce Address Tag Validation)

Verfahren zur Erkennung gültiger **Bounces** mithilfe von Zusatzinformationen im **Envelope-From** (siehe Kapitel 9.21)

### Bayes-Filter

siehe Kapitel 9.15

### Blacklist

(dt. schwarze Liste) Liste mit E-Mail- oder IP-Adressen, von denen keine E-Mail angenommen oder deren E-Mail als Spam bewertet wird. Gegenteil: **Whitelist**.

### Body

(dt. Körper) Inhalt einer E-Mail ohne die Kopfzeilen (**Header**), also der Teil, der den eigentlichen Text (und eventuell Anhänge) enthält (siehe auch **Header** und **Envelope**).

### Bot

(von *bot*, kurz für *robot*) Von Unbefugten ferngesteuerter Rechner, typischerweise PCs von Privatanwendern oder Arbeitsplatzrechner, die durch Viren oder Würmer infiziert wurden. Ein anderes Wort für Bot ist **Zombie**. Bots werden in **Botnetzen** zusammengefasst.

### Botnetz oder Botnet

Gruppe von Rechnern, die unter zentraler Kontrolle eines Angreifers stehen und von ihm z. B. für (DDoS-)Angriffe auf andere Rechner oder zum Spamversand benutzt werden. Die Rechner in einem Botnetz werden als **Bots** oder **Zombies** bezeichnet. Botnetze werden häufig über IRC-Server gesteuert, zu denen alle Bots automatisch eine Verbindung aufbauen und dort in speziellen Channels auf Befehle warten.

### Bounce

Fehlermail, die erzeugt wird, wenn ein **MTA** eine E-Mail angenommen hat und danach feststellt, dass er sie nicht zustellen kann. Die Fehlermail wird an den Absender (die Adresse im **Envelope-**

**From)** der ursprünglichen E-Mail versandt. Ist diese Angabe gefälscht, erreicht die Fehlermail nicht den tatsächlichen Absender, sondern einen unbeteiligten Dritten. Die technische Bezeichnung einer *bounce* ist *non-delivery notification* (NDN). *Bounces* haben immer ein leeres **Envelope-From**.

### **Brute force attack**

(dt. Angriff durch rohe Gewalt) Angriff, bei dem der Angreifer nicht besonders clever vorgeht, sondern einfach alle möglichen Zeichenkombinationen durchprobiert, um z.B. Passwörter oder Mailadressen zu erraten (siehe Kapitel 4.3.3).

### **CallerID**

Vorläufer des **SenderID**-Verfahrens (siehe Kapitel 9.9)

### **CGI (Common Gateway Interface)**

Definition einer Schnittstelle zwischen Webserver und Programmen, die Aktionen auf einem Webserver auslösen und dynamisch Webseiten generieren.

### **Challenge-Response-Verfahren**

(dt. Anforderung-Antwort) Verfahren, bei dem der Empfänger einer E-Mail den Absender auffordert, eine bestimmte Tätigkeit durchzuführen oder eine bestimmte Antwort zu liefern. Nur wer das richtig macht, darf E-Mail an diesen Empfänger versenden (siehe Kapitel 9.18).

### **Confirmed Opt-In**

Opt-In-Verfahren, bei dem der Abonnent eines Newsletters eine Mail bekommt, die ihm bestätigt, dass er sich gerade auf eine Liste eingetragen hat. Sollte ein Fehler vorliegen, kann er sich umgehend wieder austragen (siehe auch **Opt-In, Opt-Out, Double-Opt-In**).

### **DCC (Distributed Checksum Clearinghouse)**

siehe Kapitel 9.16

### **DDoS-Angriff**

Distributed-Denial-of-Service-Angriff (Verteilter Angriff auf die Verfügbarkeit von Diensten), **DoS-Angriff**, den viele im Internet verteilte Rechner zusammen ausführen. Häufig kommen dabei **Botnetze** zum Einsatz.

### **Dictionary attack**

**Brute force attack**, bei der sich der Angreifer auf Wörter aus einem Wörterbuch beschränkt (siehe Kapitel 4.3.3).

### **DNSBL (Domain Name System Blocking List)**

siehe Kapitel 9.4

### **DomainKeys**

Verfahren zur kryptographischen Authentifizierung der Absenderdomain (siehe Kapitel 9.11)

### **DoS-Angriff**

Denial-of-Service-Angriff (Angriff auf die Verfügbarkeit von Diensten). Angriff auf einen Rechner, der einen Dienst behindert oder den Zugriff darauf unterbindet.

### **Double-Opt-In (auch Verified Opt-In genannt)**

Opt-In-Verfahren, bei dem der Abonnent eines Newsletters eine Mail bekommt, die ihn zu einer zweiten Bestätigung auffordert. Die Bestätigung erfolgt meist entweder durch eine Antwortmail oder durch Aufruf einer bestimmten Webseite. Nur ein Double-Opt-In-Verfahren kann einigermaßen sicher verhindern, dass jeder jeden auf eine Liste eintragen kann (siehe auch **Opt-In, Opt-Out, Confirmed Opt-In**).

### **Egress-Filterung (auch: Outbound-Filterung)**

Ausgangsseitige Filterung beim Übergang von einem Netzwerk zu einem anderen, in der Regel von einem internen Netzwerk zum öffentlichen Internet.

### **Envelope**

(dt. Umschlag) Im **SMTP**-Dialog ausgetauschte Absender- und Empfänger-Daten einer E-Mail. Nur diese verwenden **MTAs** zur Zustellung der E-Mail (vgl. **Header**). (Vergleichbar den Daten auf einem Briefumschlag)

### **Envelope-From**

Absenderadresse im **Envelope**. Wird mit dem SMTP-Befehl **MAIL FROM** übertragen (siehe auch **Return path**).

### **Envelope-To**

Empfängeradresse im **Envelope**. Wird mit dem SMTP-Befehl **RCPT TO** übertragen.

### **ESMTP (Extended Simple Mail Transfer Protocol)**

Erweiterung von **SMTP**, die heute weitgehend anstelle des ursprünglichen SMTP verwendet wird. Definition in RFC2821. ESMTP erlaubt das Aushandeln von Erweiterungen zwischen Absender und Empfänger.

### **False negative**

Eine nicht als solche erkannte Spam-Mail (Gegenteil: **True negative**, siehe Kapitel 8.5)

### **False positive**

Eine als Spam erkannte, aber erwünschte E-Mail (Gegenteil: **True positive**, siehe Kapitel 8.5)

### **Forward**

Weiterleitung einer E-Mail an eine andere Adresse. Meist vom Empfänger eingerichtet, der unter mehreren Mailadressen erreichbar sein will.

### **FUSSP (Final Ultimate Solution to the Spam Problem)**

Die von vielen gesuchte aber niemals wirklich erreichbare „Letzte und endgültige Lösung für das Spamproblem“. Siehe <http://www.rhyolite.com/anti-spam/you-mightbe.html>

### **Greylisting**

Antispam-Verfahren, siehe 9.13

### **Ham**

Erwünschte E-Mail, Gegenteil von Spam

### **Harvesting**

(dt. Ernten) Automatisches Sammeln von Mailadressen auf Webseiten, in Newsgroups oder ähnlichen Medien zur Benutzung durch Spammer.

### **Header**

(dt. Kopf) Verwaltungsdaten am Anfang einer E-Mail. Die Daten werden in mehreren Header-Zeilen aufgelistet, die jeweils ein Schlüsselwort ( z. B. From, To, Date, Message-ID, ...), einen Doppelpunkt und dann den Inhalt enthalten. Der *header* ist vom *body* der E-Mail durch eine Leerzeile getrennt (siehe auch **Body**, **Envelope**).

### **Hoax**

Scherz, Falschmeldung. Häufig in Form eines Kettenbriefes versandt.

**Honeypot**

(dt. Honigtopf) Rechner, der dazu aufgestellt wird, Spammer oder Hacker anzulocken, um ihre Methoden zu studieren (siehe auch **Spamfalle**).

**Identified Internet Mail (IIM)**

siehe Kapitel 9.11

**IETF (Internet Engineering Task Force)**

Standardisierungsorganisation des Internet

**IMAP (Internet Message Access Protocol)**

Protokoll zum Zugriff auf das Postfach eines Anwenders. Bietet wesentlich mehr Funktionen als **POP**, z. B. die Verwaltung von Ordnern.

**Inbound-Filterung**

siehe Ingress-Filterung

**Inbox**

Postfach, das ankommende E-Mails aufnimmt

**Ingress-Filterung (auch Inbound-Filterung)**

Eingangsseitige Filterung beim Übergang vom öffentlichen Internet ins eigene Netzwerk

**Internet-Draft (I-D)**

Textentwurf für ein **RFC**. Internet-Drafts haben Namen nach dem Muster „draft-autorkurztitel-version.txt“. Die zweistellige Versionsnummer wird von 00 hochgezählt. Internet-Drafts laufen nach einem halben Jahr aus, wenn es keine neue Version gibt (siehe <http://www.rfc-editor.org/>).

**Joe Job**

Rufschädigung einer Person oder Firma durch Versand von E-Mails im Namen des Opfers (siehe Kapitel 3.2.5).

**Kollateraler Spam (collateral spam)**

Spam, der ohne böse Absicht von (oft falsch konfigurierten) Mailsystemen erzeugt wird (siehe 3.5.7).

**Local-part**

Teil einer Mailadresse links vom At-Zeichen „@“, den das Mailsystem lokal interpretiert. Rechts davon steht die Domain der Adresse.

**Mailclient**

Programm, das Anwender benutzen, um E-Mails zu schreiben und zu lesen. Die technische Bezeichnung ist **MUA**.

**Mailserver**

Programm oder Rechner, der E-Mails entgegennimmt. In der Regel ein **MTA** oder **MSA**.

**mailto:**

URL-Format zum Versenden von E-Mails aus dem Webbrowser, siehe Kapitel 7.2.5

**Malware**

Oberbegriff für „Schadsoftware“ wie **Viren, Würmer, Trojaner, Spyware** usw.

### **MARID (MTA Authorization Records in DNS)**

Inzwischen aufgelöste Arbeitsgruppe der IETF zur Standardisierung von Verfahren zur Absenderauthentifizierung (siehe Kapitel 9.9)

### **MASS (Message Authentication Signature Service)**

siehe Kapitel 9.11

### **MDA (Mail Delivery Agent)**

Programm, das E-Mails in das Postfach des Empfängers zustellt. Wird in der Regel vom **MTA** aufgerufen oder ist bereits im **MTA** enthalten.

### **META-Signatures (Mail Enhancements for Transmission Authorization)**

siehe Kapitel 9.11

### **MIME (Multipurpose Internet Mail Extensions)**

Standardisiertes Format, das den Versand von Multimedia-Anhängen per E-Mail erlaubt. Die ursprünglichen E-Mail-Standards sahen nur Textnachrichten vor (siehe auch **S/MIME**).

### **MSA (Mail Submission Agent)**

Programm, das E-Mails vom **MUA** entgegennimmt und über das Internet weiterverschickt. Häufig ist der **MSA** das gleiche Programm wie der **MTA**. Der Rechner, auf dem der **MSA** läuft, wird häufig als **Smarthost** bezeichnet. Siehe auch RFC 2476 und RFC 3888.

### **MTA (Mail Transfer Agent)**

Programm, das E-Mails von einem **MSA** oder **MUA** entgegennimmt und (in der Regel mittels **SMTP**) an einen anderen **MTA** weiterleitet. Der letzte **MTA** in der Kette gibt die E-Mails an einen **MDA** weiter oder stellt sie in die Mailbox zu.

### **MTAMARK**

siehe Kapitel 9.7

### **MUA (Mail User Agent)**

Mailprogramm beim Anwender, mit dem E-Mail geschrieben und gelesen wird.

### **MX-Record (Mail eXchanger)**

DNS-Eintrag für Mailserver. Zu jeder Domain gibt es in der Regel einen oder mehrere **MX**-Einträge, die angeben, welcher Rechner E-Mails für diese Domain annehmen kann. Jeder Eintrag ist mit einer Priorität (einem Zahlenwert zwischen 0 und 65535) versehen. Niedrigere Zahlen bedeuten eine höhere Priorität. **MTAs** sollten E-Mails bevorzugt an Rechner mit hoher Priorität senden. Kurz als „**MX**“ wird der Mailserver bezeichnet, für den ein **MX**-Eintrag existiert.

### **Netnews**

siehe Usenet

### **Open Proxy**

Rechner, auf dem ein **SOCKS**- oder **HTTP**-Proxy-Server läuft, der alle Verbindungen unauthentifiziert weiterleitet. Spammer missbrauchen gerne *open proxies*, um ihre Spuren zu verschleiern.

### **Open Relay**

Mailserver, der E-Mails von beliebigen Absendern an beliebige Empfänger weitergibt.

### **Opt-i n**

Verfahren zum Newsletter-Abonnement, bei dem der Empfänger sich aktiv eintragen muss (siehe auch **Opt-out**).

**Opt-out**

Verfahren zum Newsletter-Abonnement, bei dem der Empfänger automatisch eingetragen wird  
**in).**

**Outbound-Filterung**

siehe Egress-Filterung

**Permission(-based) Marketing**

E-Mail-Marketing mit Zustimmung des Empfängers

**PGP (Pretty Good Privacy)**

Programm (und inzwischen auch Standard) zur Verschlüsselung und Signierung von E-Mail.  
Meist als Erweiterung eines **MUA** verwendet (siehe auch **S/MIME**).

**Phishing**

Masche von Betrügern, die durch Vortäuschen einer fremden Identität mittels gefälschter E-Mails und Webseiten vertrauliche Daten ( z. B. Passwörter und PINs) erlangen (siehe Kapitel 3.2.4).

**Pipelining**

Verfahren, bei dem der Absender-MTA im SMTP-Dialog nicht auf die Antwort des Empfänger-MTA warten muss (siehe Kapitel 9.2).

**PKI (Public Key Infrastructure)**

(dt. Öffentliche Schlüssel-Infrastruktur) Organisationssystem für kryptographische Schlüssel und Zertifikate, das es Anwendern ermöglicht, eine kryptographische Signatur einer unbekannt Person zu überprüfen, von der nur die Zertifizierungsstelle des Schlüssels bekannt ist.

**POP (Post Office Protocol)**

Protokoll zur Abholung von E-Mail aus dem Postfach eines Anwenders

**POP-before-SMTP**

siehe SMTP-after-POP

**Postmaster**

Systemadministrator eines Mailsystems

**PRA (Purported Responsible Address)**

(dt. angeblich verantwortliche Adresse) Verfahren zur Bestimmung des letzten Absenders einer E-Mail. Wird beim SenderID-Verfahren verwendet (siehe Kapitel 9.9.2).

**Proof-of-Work**

(dt. Beweis, dass Arbeit geleistet wurde) Antispam-Verfahren (siehe Kapitel 9.19)

**Proxy**

(dt. Stellvertreter) Programm, das einem Client gegenüber als Server auftritt, den Dienst aber nicht selbst erbringt, sondern seinerseits eine Verbindung zum Server herstellt. **Proxies** gibt es in vielen Variationen, meist als Web-Proxy, der den Zugriff auf Seiten im World Wide Web ermöglicht. Problematisch im E-Mail-Umfeld sind die so genannten *open proxies*, die es dem Spammer ermöglichen, unerkant Spam zu versenden, da sie keine ausreichende Authentifizierung der Anwender verlangen.

### **Quarantänemailbox**

Spezielles Postfach für Spam oder Viren. Die E-Mails können dort überprüft und entweder freigegeben oder gelöscht werden (siehe Kapitel 8.6.5).

### **Quoted Printable**

Verfahren zur Kodierung von nicht druckbaren 8-Bit-Zeichen in E-Mails.

### **RBL**

siehe **DNSBL**

### **Relay**

Rechner, der eine E-Mail an einen anderen Rechner weitergibt. Problematisch sind die so genannten *open relays*, die jede E-Mail ohne Authentifizierung an beliebige Adressen weiterleiten.

### **Reply Antwort-E-Mail**

Return path (dt. Rückkehr-Pfad) Mailadresse, an die eine Fehlermeldung verschickt werden soll. Steht während des SMTP-Dialogs im Envelope-From. Viele Mailsysteme tragen eine Return-Path:-Header-Zeile in die E-Mail ein, wenn sie in das Postfach des Empfängers zugestellt wird. Bei Spam häufig gefälscht.

### **RFC (Request for Comments)**

Serie von Texten mit Standards und anderen Informationen zu Internet-Protokollen. Wird vom RFC-Editor (<http://www.rfc-editor.org/>) herausgegeben. Jedes RFC-Dokument hat eine eindeutige, fortlaufende Nummer. Ist eine Nummer vergeben, wird der Text nicht mehr geändert. RFCs beginnen ihr Leben als **Internet-Draft**.

### **RHSBL (Right Hand Side Blocking List)**

siehe **DNSBL**

### **Scam**

(dt. Betrug)

### **Scoring**

Punktezählverfahren zur Bewertung von E-Mail nach vielen Kriterien. Erreicht die Gesamtpunktzahl einen bestimmten Schwellwert, wird die E-Mail als Spam klassifiziert.

### **SenderID**

siehe Kapitel 9.9

### **Smarthost**

Server für den Mailversand. Er nimmt E-Mails vom Anwender (**MUA**) entgegen, interpretiert die Empfängeradresse und leitet die E-Mails an den richtigen Empfänger-Mailserver weiter.

### **S/MIME (Secure/ Multipurpose Internet Mail Extensions)**

Standard für den Austausch verschlüsselter und signierter E-Mail. Baut auf dem **MIME**-Format auf (siehe auch **PGP**).

### **SMTP (Simple Mail Transfer Protocol)**

Textbasiertes Protokoll, nach dem der weitaus größte Teil der E-Mail im Internet ausgetauscht wird. Heute wird meist die erweiterte Version **ESMTP** verwendet. Definiert in RFC 2821.

### **SMTP-after-POP**

Verfahren zur Pseudo-Authentifizierung einer SMTP-Verbindung mit Hilfe einer POP-Verbindung (auch manchmal unter dem Namen POP-before-SMTP zu finden). Wurde

verwendet, weil es ursprünglich keine Authentifizierung von SMTP-Verbindungen (**SMTP AUTH**) gab.

### **SMTP AUTH**

Protokoll zur Authentifizierung eines **SMTP**-Clients gegenüber dem SMTP-Server mit dem AUTH-Befehl von **ESMTP**

### **SOCKS**

Protokoll zur Weiterleitung von TCP-Verbindungen und UDP-Daten durch SOCKS-Proxies (z. B. auf Firewalls, siehe Kapitel 7.1.2)

### **Spam**

Unverlangt zugesandte Massen-E-Mail (siehe auch **UBE** und **UCE** sowie Kapitel 3.1)

### **Spamfalle (spam trap)**

Mailadresse, die nur Spam erhält und nicht der normalen Kommunikation dient. Wird zur verlässlichen Identifizierung von Spam verwendet (ähnlich den *honeypots* (dt. Honigtopf), die in anderem Zusammenhang zum Anlocken von Hackern verwendet werden, siehe Kapitel 9.22).

### **SPF (Sender Policy Framework)**

siehe Kapitel 9.9

### **Spywa re**

Software, die Aktionen des Anwenders belauscht (z. B. die Eingabe von PINs) oder den Inhalt des Rechners untersucht und die Informationen an einen Angreifer weiterleitet.

### **SRS (Sender Rewriting Scheme)**

Verfahren zum Umschreiben des Absenders bei weitergeleiteter E-Mail. Wird im Zusammenhang mit **SPF** verwendet (siehe 9.9.3).

### **SSL (Secure Socket Layer)**

siehe **TLS**

### **Subject**

Betreffzeile einer E-Mail, Teil des **Headers**

### **Tarpitting**

Verfahren zur Blockade von Spammern durch Verzögerung der Antworten im SMTPDialog (siehe Kasten im Kapitel 9.2)

### **Teergrube, teergrubing**

siehe Tarpitting

### **TLS (Transport Layer Security)**

Protokoll zur Verschlüsselung von Internet-Verbindungen. Kann auch für E-Mail verwendet werden. Frühere Versionen des Protokolls hießen **SSL**. Nicht zu verwechseln mit **PGP** und **S/MIME**, bei denen nicht die Verbindung, sondern die E-Mail verschlüsselt wird.

### **Trojaner**

Historisch inkorrekte, aber verbreitete Kurzform für **Trojanisches Pferd**

### **Trojanisches Pferd**

Programm, das vorgibt, einen nützlichen Zweck zu erfüllen, und deswegen vom Anwender installiert oder ausgeführt wird. In Wirklichkeit dient es aber anderen Zwecken (z. B. dem Ausspionieren des Anwenders).

### **True negative**

Eine E-Mail wurde korrekt als Ham erkannt (Gegenteil: **False negative**, siehe auch Kapitel 8.5).

### **True positive**

Eine E-Mail wurde korrekt als Spam erkannt (Gegenteil: **False positive**, siehe auch Kapitel 8.5).

### **UBE (Unsolicited Bulk E-Mail)**

Unverlangte Massen-E-Mail, **Spam** (siehe Kapitel 3.1)

### **UCE (Unsolicited Commercial E-Mail)**

Unverlangte kommerzielle E-Mail, **Spam** (siehe Kapitel 3.2.1)

### **Unschärfe Prüfsumme**

Prüfsumme über einen Text, die kleinere Änderungen toleriert (siehe Kapitel 9.16).

### **URIDNSBL**

siehe DNSBL

### **Usenet**

Verteiltes Diskussionsforen-System (auch **Netnews** genannt).

### **Vacation-Programm oder -Nachricht**

Programm, das eine automatische Antwort an den Absender verschickt, wenn der Empfänger der E-Mail in Urlaub ist. Im weiteren Sinne jede Art der automatischen Antwortmail (siehe auch **Autoreply** und **Autoresponder**).

### **Verified Opt-In**

siehe Double-Opt-In

### **VERP (Variable Envelope Return Path)**

Methode zur Zuordnung von *bounces* durch Kodieren der Empfängeradresse einer E-Mail im Envelope-From (vgl. **BATV**)

### **Virus**

Software, die sich in anderer Software versteckt und bei Ausführung weitere Programme infiziert (siehe auch **Wurm**).

### **Web-Bug**

Kleine, meist unsichtbare Grafik oder anderer externer Inhalt, der in eine Webseite oder HTML-Mail eingefügt wird. Fragt der Mailclient die zugehörige URL ab, kann der Spammer im Logfile sehen, wer die Spam-Mail gelesen hat.

### **Whitelist**

(dt. weiße Liste) Liste mit Mailadressen oder IP-Adressen, von denen auf jeden Fall E-Mail angenommen werden soll. Im weiteren Sinne kann eine Whitelist auch Einträge enthalten, für die eine weniger strikte Filterung notwendig ist. Gegenteil: **Blacklist**.

### **Wörterbuchangriff**

Verfahren, bei dem ein Angreifer Wörter aus einem Wörterbuch durchprobiert, um z. B. Passwörter oder Mailadressen zu erraten (siehe Kapitel 4.3.3).

### **Wurm**

Software, die sich unter Ausnutzung von Schwachstellen in der Software oder Konfiguration selbständig im Internet von Rechner zu Rechner verbreitet (siehe auch **Virus**).

**Zombie**

Ein unter Kontrolle eines Angreifers stehender Rechner in einem **Botnetz**, typischerweise ein PC in einem Haushalt oder in einer Firma.

## Literatur und Links

Allgemeine technische Grundlagen zu E-Mail finden sich in „Internet Email Protocols“ [John99] und „Programming Internet Email“ [Wood99]. Speziell mit dem Thema Spam beschäftigen sich „Degunking your Email, Spam, and Viruses“ [Dunt04] und „Spam bekämpfen für Dummies“ [LYEC04].

Einen (nicht-technischen) Blick hinter die Kulissen bringt das locker und spannend geschriebene „Spam Kings“ [McWi04], das abwechselnd von Spammern und Antispam-Aktivisten berichtet. Aus der Sicht eines Spammers geschrieben ist „Inside the SPAM Cartel“ [Spam04], das viele Tricks der Spammer verrät. Wer nur einen kleinen Überblick will, findet unter [http://matthias.leisi.net/archives/80\\_Spam\\_Biz.html](http://matthias.leisi.net/archives/80_Spam_Biz.html), was er sucht.

Die offizielle Heimat der RFC-Serie (Request for Comments, zitiert als [RFCxxx]) ist unter <http://www.rfc-editor.org/> zu finden. Dort kann man die Texte herunterladen und bekommt Informationen zum Status (Draft Standard, Standard, Informational, ...) der Texte.

Internet-Drafts sind Entwürfe von Texten, die später als RFC veröffentlicht werden sollen. Sie sind an einem Namen zu erkennen, der mit „draft-“ beginnt. Die offizielle Heimat ist ebenfalls beim RFC-Editor: <http://www.rfc-editor.org/>. Vorversionen erscheinen dort aber nicht immer sofort. Internet-Drafts laufen nach einem halben Jahr aus, wenn keine neue Version vorliegt.

Weiterführende Information zum Thema Spam gibt es unter folgenden Adressen:

- Ergiebiger Enzyklopädie-Artikel zu Geschichte, Etymologie, Kosten und mit vielen weiterführenden Links: <http://en.wikipedia.org/wiki/Spamming>
- Spam Links („*everything you didn't want to have to know about spam*“). Sehr umfangreiche Linksammlung zu allen Themen rund um Spam: <http://spamlinks.net/>
- Viele Informationen über Spam und was man dagegen tun kann: <http://spam.abuse.net/>
- Coalition Against Unsolicited Commercial Email (CAUCE): <http://www.cauce.org/>
- The European Coalition Against Unsolicited Commercial Email (EuroCAUCE): <http://www.euro.cauce.org/de/index.html>
- Anti-Spam Research Group der IETF: <http://asrg.sp.am/>
- Das Spamhaus-Projekt sammelt Informationen über Spammer: <http://www.spamhaus.org/>
- Rick's Spam Digest: <http://www.rickconner.net/spamweb/index.html>
- Popular Spammer Tricks: <http://www.rickconner.net/spamweb/tricks.html>

[ASTF04] Braun, Dietmar; Kocovski, Jan; Rickert, Thomas; Waldhauser, Béla: White Paper der Anti Spam Task Force (ASTF). eco-Verband, 21.09.2004. [http://www.eco.de/servlet/PB/men\\_u/1446039\\_11/index.htm](http://www.eco.de/servlet/PB/men_u/1446039_11/index.htm)

[BaBH02] Bager, Jo; Bleich, Holger; Heidrich, Joerg: Die Internet-Massenplage. Was tun gegen Spam-Mails? c't 22/2002, S. 150 ff.

[Brau04] Brauch, Patrick: Geld oder Netz! Kriminelle erpressen Online-Wettbüros mit DDoS-Attacken. c't 14/2004, S. 48.

[Dela04] Delany, Mark: Domain-based Email Authentication Using Public-Keys Advertised in the DNS (DomainKeys). August 2004. draft-delany-domainkeys-base-01

- [Dunt04] Duntemann, Jeff: Degunking your Email, Spam, and Viruses. Paraglyph Press, 2004. ISBN 1-93211193-X.
- [Fern04] Ferngesteuerte Spam-Armeen. Nachgewiesen: Virenschreiber lieferten Spam-Infrastruktur. c't 5/2004, S. 18 ff.
- [FeTh04] Fenton, J.; Thomas, M.: Identified Internet Mail. Oktober 2004. draft-fenton-identified-mai l-01.
- [FTC04] Federal Trade Commission (FTC): National Do Not Email Registry. A Report To Congress. Juni 2004. <http://www.ftc.gov/reports/dneregistry/report.pdf>
- [GSHB04] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch. Stand: 2004. <http://www.bsi.bund.de/gshb/deutsch/index.htm>
- [Hein04] Heinlein, Peer: Das Postfix-Buch. Sichere Mailserver mit Linux. Open Source Press, 2004. ISBN 3-937514-04-X.
- [Hous05] Housley, R: Security Review of Two MASS Proposals. Januar 2005. draft-housley-mass-sec-review-00.
- [John99] Johnson, Kevin: Internet Email Protocols. A Developer's Guide. Addison-Wesley, 1999. ISBN 0-201-43288-9.
- [LaCl04] Laurie, Ben; Clayton, Richard (2004): „Proof-of-Work“ Proves Not to Work. Presented at the Third Annual Workshop on Economics and Information Security (WEIS04). <http://www.cl.cam.ac.uk/~rnc1/proofwork.pdf> (Letzter Zugriff: 07.12.2004).
- [LCSF04] Levine, J.; Crocker, D.; Silberman, S.; Finch, T.: Bounce Address Tag Validation (BATV). September 2004. draft-levine-marid-batv-00; <http://www.bbiw.net/C/SV/draft-levine-mass-batv-00.html>
- [LeWo04] Lentzner, M.; Wong, M.: Sender Policy Framework: Authorizing Use of Domains in MAIL FROM. <http://www.ozonehouse.com/mark/spf/draftlentzner-spf-00.txt>; 12.10.2004.
- [LYEC04] Levine, John R.; Young, Margaret Levine; Everett-Church, Ray: Fighting Spam for Dummies. Wiley, 2004. ISBN 0-7645-5965-6 (Deutsche Übersetzung: Spam bekämpfen für Dummies. Mitp-Verlag, 2004. ISBN 3-826-63144-7).
- [Lyon04] Lyon, J.: Purported Responsible Address in E-Mail Messages. draft-lyon-senderid-pra-00.txt.
- [McWi04] McWilliams, Brian: Spam Kings. The Real Story Behind the High-Rolling Hucksters Pushing Porn, Pills, and @\*#?% Enlargements. O'Reilly Media, 2004. ISBN 0-596-00732-9.
- [MPFC93] Monty Python's Flying Circus: Sämtliche Worte (Band 2). Seite 42 ff.; Haffmanns Verlag, 1993. ISBN 3-251-00223-6.
- [RFC1928] Leech, M.; et al.: SOCKS Protocol Version 5. März 1996.
- [RFC2034] Freed, N.: SMTP Service Extension for Returning Enhanced Error Codes. Oktober 1996.
- [RFC2045] Freed, N.; Borenstein, N.: Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies. November 1996.

- [RFC2046] Freed, N.; Borenstein, N.: Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types. November 1996.
- [RFC2047] Moore, K.: Multipurpose Internet Mail Extensions (MIME) Part Three: Message Header Extensions for Non-ASCII Text. November 1996.
- [RFC2048] Freed, N.; Klensin, J.: Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures. November 1996.
- [RFC2049] Freed, N.; Borenstein, N.: Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples. November 1996.
- [RFC2142] Crocker, D.: Mailbox Names for Common Services, Roles and Functions. Mai 1997.
- [RFC2440] Callas, J.; Donnerhacke, L.; Finney, H.; Thayer, R.: OpenPGP Message Format. November 1998.
- [RFC2476] Gellens, R.; Klensin, J.: Message Submission. Dezember 1998.
- [RFC2505] Lindberg, G.: Anti-Spam Recommendations for SMTP MTAs. Februar 1999.
- [RFC2554] Myers, J.: SMTP Service Extension for Authentication. März 1999.
- [RFC2616] Fielding, R.; et al.: Hypertext Transfer Protocol – HTTP/1.1. Juni 1999.
- [RFC2635] Hambridge, S.; Lunde, A.: DON'T SPEW. A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam\*). Juni 1999.
- [RFC2821] Klensin, J. (Ed.): Simple Mail Transfer Protocol. April 2001.
- [RFC2822] Resnick, P. (Ed.): Internet Message Format. April 2001.
- [RFC2920] Freed, N.: SMTP Service Extension for Command Pipelining. September 2000.
- [RFC3028] Showalter, T.: Sieve: A Mail Filtering Language. Januar 2001.
- [RFC3098] Gavin, T.; Eastlake 3rd, D.; Hambridge, S.: How to Advertise Responsibly Using E-Mail and Newsgroups or – how NOT to \$\$\$\$\$ MAKE ENEMIES FAST! \$\$\$\$\$. April 2001.
- [RFC3463] Vaudreuil, G.: Enhanced Mail System Status Codes. Januar 2003.
- [RFC3834] Moore, K.: Recommendations for Automatic Responses to Electronic Mail. August 2004.
- [RFC3850] Ramsdell, B. (Ed.): Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1. Certificate Handling. Juli 2004.
- [RFC3851] Ramsdell, B. (Ed.): Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1. Message Specification. Juli 2004.
- [Schw04] Schwartz, Alan: SpamAssassin. O'Reilly Media, 2004. ISBN 0-596-00707-8.
- [SCKL04] Segal, Richard; Crawford, Jason; Kephart, Jeff; Leiba, Barry: SpamGuru: An Enterprise Anti-Spam Filtering System. Published in the Proceedings of CEAS 2004. <http://www.ceas.cc/papers-2004/126.pdf>
- [Send04] Sender Authentication Deployment Recommendations. November 2004. [http://www.sendmail.net/tools/Sendmail\\_Auth\\_Reco\\_wp.pdf](http://www.sendmail.net/tools/Sendmail_Auth_Reco_wp.pdf)

- [Spam04] Spammer-X: Inside the SPAM Cartel. Trade Secrets from the Dark Side. Syngress, 2004. ISBN 1-932266-86-0.
- [StHo04] Stumpf, M.; Hoehne, S.: Marking Mail Transfer Agents in Reverse DNS with TXT RRs. October 2004. draft-stumpf-dns-mtamark-03.
- [Unge04] Ungerer, Bert: Eingeengt. E-Mail zwischen unerwünscht und unverzichtbar. iX 4/2004, S. 118 ff.
- [Vergil] Vergil: Äneis. ca. 29 v. Chr.
- [Völk04] Völker, Roland: Moment bitte. Mit Greylisting gegen Spam vorgehen. iX 12/2004, S. 94 ff.
- [Wood99] Wood, David: Programming Internet Email. O'Reilly & Associates, 1999. ISBN 1-56592-479-7.