KAPITEL 2

Strategien gegen Spam und Viren

In diesem Kapitel werden die Strategien gegen Spam und E-Mail-Viren vorgestellt, die im Verlauf des Buchs detailliert thematisiert werden sollen. Dabei werden die Strategien hier zunächst ohne Bezug auf Implementierungen vorgestellt. Die folgenden Kapitel werden dann konkrete Software-Lösungen vorstellen, die jeweils eine oder mehrere der hier vorgestellten Techniken umsetzen. Außerdem werden in diesem Kapitel einige allgemeine Überlegungen zum Kampf gegen Spam und Viren angestellt, auf die im Verlauf des Buchs wiederholt Bezug genommen wird.

Spam-Erkennung versus Viren-Erkennung

Spam und Viren sind gleichermaßen Ärgernisse für E-Mail-Anwender. Um einen vernünftigen Betrieb zu gewährleisten, müssen Maßnahmen gegen beide dieser Arten von E-Mail-Missbrauch ergriffen werden. Trotzdem ist es sinnvoll, sie getrennt zu behandeln.

Zunächst sind Spam und Viren verschieden aufgebaut, deshalb müssen die technischen Maßnahmen gegen sie verschieden sein.

Spam ist, wie in Kapitel 1, *Einführung* definiert, unverlangte Werbe-E-Mail. Technische Maßnahmen zur Abwehr von Spam müssen also erkennen, ob die E-Mail Werbecharakter hat oder ob sie verlangt worden ist. Dies funktioniert vornehmlich durch Betrachtung des Textinhalts, des Absenders und des Versandwegs der E-Mail. Eine technische Herausforderung für Spam-Filtersysteme ist die Analyse der natürlichen Sprache im Text einer E-Mail, die die meisten aktuellen Systeme nur rudimentär beherrschen und die vermutlich nie von einem Computersystem perfekt gemeistert werden wird.

Ein Virus ist nach der Definition in Kapitel 1, *Einführung* eine Programmroutine mit Schadensabsichten. Dieses Buch behandelt freilich nur Viren, die über E-Mail versendet werden, was jedoch heutzutage die häufigste Verbreitungsform ist. Technische Maßnahmen zur Abwehr von Viren müssen also erkennen, ob eine E-Mail Programmcode enthält und insbesondere ob dieser Schadensabsichten hat. Es ist

mathematisch unmöglich, ein Programm zu analysieren und mit Sicherheit festzustellen, was es tun wird, ohne das Programm auszuführen. Abwehrmaßnahmen gegen Viren können daher nur besonders viele Viren erkennen, indem sie die zu prüfenden Objekte mit bekannten Exemplaren und verdächtigen Mustern vergleichen. Die meisten aktuellen Virenscanner-Programme funktionieren auf diese Weise und erkennen so sehr verlässlich alle aktuell existierenden Viren, aber sehr schlecht Viren, die zum Zeitpunkt der Herstellung noch nicht bekannt waren.

Spam und Viren haben aber auch einige gemeinsame Eigenschaften. So werden beide Arten von E-Mails normalerweise in großen Mengen und automatisiert versendet und nutzen dabei oft Konfigurationsfehler oder Sicherheitslücken in anderen Systemen aus. Auch diese Umstände können teilweise durch technische Maßnahmen erkannt werden, was somit zur Abwehr von Spam und Viren gleichermaßen beiträgt.

Aber auch im rechtlichen Status unterscheidet sich Spam von Viren, woraus sich unter anderem unterschiedliche Rechte und Pflichten für den Administrator ergeben. Auf die juristischen Aspekte wird im Einzelnen in Kapitel 14, *Juristische Aspekte beim Einsatz von Spam- und Virenfiltern* eingegangen.

Die meiste Software, egal ob sie Spam oder Viren oder beides zu filtern behauptet, differenziert daher in der Regel zwischen beiden Kategorien aus technischen, administrativen und rechtlichen Gründen.

Falsche Positive, falsche Negative

Technische Maßnahmen gegen Spam und Viren sind nicht hundertprozentig akkurat. Ansonsten würde man sie einfach installieren, und das Problem, oder zumindest das Symptom, wäre beseitigt. Technische Maßnahmen gegen Spam und Viren können dazu führen, dass legitime E-Mails nicht zugestellt werden können, und natürlich ebenso dazu, dass unerwünschte E-Mails trotzdem noch den Empfänger erreichen.

Falsche Positive (englisch: false positives) sind Exemplare von E-Mails, die von Filtersystemen als Spam beziehungsweise Virus eingestuft worden sind, obwohl sie es nicht sind. Falsche Positive sind natürlich extrem unerwünscht. Bei der Entwicklung eines Filtersystems, sowohl bei der Herstellung der Software als auch bei der Installation und Konfiguration, sollte stets die Vermeidung von falschen Positiven Priorität haben. Trotzdem können falsche Positive natürlich nicht gänzlich ausgeschlossen werden. Die Marketing-Materialien von kommerziellen Spam- und Virenerkennungssystemen geben regelmäßig Falsche-Positive-Raten von unter einem Prozent an. Es gibt aber auch Berichte von Raten im einstelligen Prozentbereich. Da das E-Mail-Aufkommen einer jeden Person und einer jeden Firma unterschiedlich ist, ist eine derartige Spanne durchaus möglich. Eigene Tests der eingesetzten Software mit dem eigenen E-Mail-Aufkommen sind in jedem Fall anzuraten.

Falsche Negative (englisch: false negatives) sind Exemplare von E-Mails, die von Filtersystemen nicht erkannt worden sind, obwohl sie Spam oder einen Virus enthalten. Ganz ohne Filtersysteme gäbe es natürlich jede Menge falscher Negative, aber in dem Fall wäre es auch nicht sinnvoll, diesen Begriff anzuwenden. Natürlich sind falsche Negative – noch viel mehr als falsche Positive – nicht zu verhindern. Obwohl die Reduzierung von falschen Negativen letztendlich ein Qualitätsmerkmal von Filtersystemen ist, ist der Vermeidung von falschen Positiven stets Vorrang zu geben. Aktuelle Spam-Erkennungssysteme können eine Falsche-Negative-Rate im einstelligen Prozentbereich erreichen. Bei Virenscannern ist die Anzahl der nicht erkannten Exemplare nahezu bei null, sofern sie ständig aktualisiert werden.

Die in diesem Buch vorgestellten Software-Lösungen haben in der Summe unzählige Konfigurationseinstellungen. Abgesehen von einigen, die die Software in das System und in das Netzwerk einpassen, sind die meisten Einstellungen dazu da, dem Anwender eigenverantwortlich die Möglichkeit zu geben, zwischen falschen Positiven und falschen Negativen abzuwägen.

Server- und clientbasierte Erkennung

Eine E-Mail durchläuft beim Versand normalerweise mehrere Rechner, im häufigsten Fall vier: den Arbeitsplatzrechner des Absenders, den Mailserver des Absenders, in der Regel vom Internet Service Provider (ISP) oder von der Firma gestellt, den Mailserver des Empfängers, in der Regel ebenfalls beim ISP oder in der Firma, und den Arbeitsplatzrechner des Empfängers. Je nach bestimmten Umständen können unterwegs auch weitere Mailserver involviert sein.

Spam- und Virenerkennung kann an verschiedenen Stellen in diesem Ablauf implementiert werden.

Die Abwehr von Spam und Viren auf der Absenderseite ist nicht Haupthema dieses Buchs. Sie erfordert eine ganze Reihe von anderen Maßnahmen; siehe Abschnitt »An der Quelle« unten. Dieses Buch behandelt die Abwehr von Spam und Viren auf der Empfängerseite, also auf dem Mailserver oder dem Arbeitsplatz des Empfängers.

Spam- und Virenerkennungssysteme könnten also zunächst auf dem Mailserver des Empfängers installiert werden. Der Mailserver ist hier der Rechner, auf dem der zuständige SMTP-Server läuft. Dies wird im Folgenden als serverbasierte Erkennung bezeichnet.

Alternativ könnten Spam- und Virenerkennungssysteme auf dem Arbeitsplatzrechner des Empfängers installiert werden. Sie könnten dabei in den E-Mail-Client eingebunden sein, beim Herunterladen der E-Mails über die Protokolle IMAP oder POP3 aktiviert werden oder anderweitig im Betriebssystem installiert sein. Dies wird im Folgenden als clientbasierte Erkennung bezeichnet.

Serverbasierte Erkennungssysteme haben mehrere Vorteile:

- Sie können zentral administriert werden. Dies spart Aufwand und Personal. Auch wird so erreicht, dass Anwender die Systeme nicht abschalten oder falsch konfigurieren können, sei es versehentlich oder absichtlich.
- Sie verhindern, dass Spam und Viren die Systeme der Empfänger erreichen. Dies ist wichtig, wenn die Empfänger unerfahren oder unvorsichtig im Umgang mit E-Mail sind. Viren nutzen außerdem oft Sicherheitslücken oder Konfigurationsfehler aus und sollten besser gar nicht auf anfällige Systeme gelangen, da so auch clientbasierte Filtersysteme infiziert oder abgeschaltet werden könnten.

Die Nachteile von serverbasierten Erkennungssystemen sind:

- Die Anpassung an die Wünsche und Bedürfnisse einzelner Nutzer ist schwieriger. Spezialkonfigurationen müssen, sofern sie technisch überhaupt machbar sind, entweder von den Administratoren vorgenommen werden, oder den Nutzern muss Zugriff auf den Mailserver gegeben werden. So oder so werden damit die Vorteile der zentralen Administration ausgehöhlt. Auf clientbasierten Systemen haben die Nutzer selbst die Kontrolle über die Konfiguration.
- Einige lernende Spam-Filtersysteme (siehe unten) funktionieren besser, wenn sie sich auf jeden Nutzer individuell einstellen können, statt auf eine ganze Organisation als Einheit. Benutzerspezifische Lerndatenbanken können nur mit einigen Schwierigkeiten auf serverbasierten Filtersystemen implementiert und gewartet werden. Auf clientbasierten Systemen ist dies wesentlich einfacher.

In der Praxis werden in vielen Fällen beide Systeme eingesetzt und kombiniert: Serverbasierte Systeme erledigen die Erkennung, clientbasierte Systeme das Aussortieren. Oder: Serverbasierte Systeme filtern mit allgemein verträglichen Einstellungen, clientbasierte Systeme werden von Nutzern mit schärferen Einstellungen nachgeschaltet. Welche Balance gefunden wird, hängt von den Wünschen der Nutzer und den Möglichkeiten der Administratoren ab.

Die in diesem Buch behandelte Software ist überwiegend primär für den Einsatz auf einem Mailserver konzipiert. Einige Hinweise zur Filterung von E-Mail auf Client-Systemen werden in Kapitel 11, *E-Mail-Clients* gegeben.

In vielen Fällen werden Spam- und Virenfiltersysteme vom eigentlichen Mailserver getrennt. Dabei wird dem Mailserver ein weiterer Server vorgeschaltet, der die Filterung übernimmt und die nicht abgelehnten E-Mails an den eigentlichen Mailserver weiterleitet, der dann die normale Auslieferung in die Postfächer der Nutzer übernimmt. Dies wird oft als E-Mail-Filter-Gateway oder ähnlich bezeichnet. Die Gründe für diese Trennung sind administrativer Natur: Man ist bei der Wahl der Filtersoftware und der Wartung des Filtersystems unabhängig von den anderen Umständen im E-Mail-System, also zum Beispiel wie der Zugriff auf die Postfächer

geregelt ist. Gleichzeitig sind Systeme, die nur eine Aufgabe erfüllen, also entweder E-Mail filtern oder E-Mail zustellen, einfacher zu warten und möglicherweise sicherer.

Der Nachteil eines Gateways ist, dass es die oben aufgezählten Probleme der serverbasierten Erkennung noch verschlimmert. Gateway-Systeme haben überhaupt keine Kenntnisse von lokalen Nutzern und schirmen aus Sicherheitsgründen den Zugriff durch normale Nutzer ab. Einige Software-Lösungen gehen auf diese Probleme ein, aber allgemein kann gesagt werden, dass die individuelle Behandlung einzelner Nutzer auf Gateway-Systemen eingeschränkt ist.

Trotzdem ist es heutzutage durchaus üblich und empfehlenswert, die Spam- und Virenerkennung auf separate Gateway-Systeme auszulagern.

Regelbasierte Erkennung

Die einfachsten und naivsten Spam-Erkennungssysteme suchen nach bestimmten Wörtern oder Phrasen in der E-Mail und löschen auf diese Art erkannte E-Mails. Beispielsweise könnte man E-Mails mit Phrasen wie »Earn extra cash« oder »Cheap medication« einfach wegwerfen. Dies sind Beispiele von statischen Regeln. Dieser einfache Ansatz führt natürlich zu vielen falschen Positiven und kann daher auch nicht in Software zur allgemeinen Verwendung eingebaut werden. Private Spam-Filter oder Ergänzungen davon sehen aber noch wie vor so aus.

Vielversprechender ist der Ansatz, eine E-Mail erst dann als Spam einzustufen, wenn mehrere verdächtige Phrasen gefunden worden sind. Außerdem sind einige Phrasen verdächtiger als andere. Derartige Systeme verwenden gewichtete Regelsätze und treffen daher ausgewogenere Entscheidungen.

Der Nachteil von Spam-Erkennungssystemen mit statischen Regeln ist, dass die Spammer diese Regeln früher oder später auch mitbekommen und ihre Software, Methoden und Texte so anpassen können, dass die Erkennungsregeln umgangen werden. Spam-Erkennung mit statischen Regeln ist also ein ständiges Wettrüsten.

Die Software SpamAssassin, die in Kapitel 4, *SpamAssassin* beschrieben wird, implementiert ein solches gewichtetes statisches Regelsystem. Eigene statische Regeln ohne Gewichtung können oft auch direkt im Mail Transport Agent (MTA) implementiert werden; dazu siehe Kapitel 3, *Spam- und Virenabwehr mit Postfix, Exim und Sendmail*. Procmail ist ebenfalls ein mächtiges Programm zur Analyse und Filterung von E-Mail auf Basis von Texterkennung. Hinweise zur Verwendung von Procmail zur Spam- und Virenfilterung und eine Reihe von vorgefertigten »Rezepten« finden sich in Kapitel 12, *Procmail*.

Virenerkennungssysteme verwenden ebenfalls statische Regeln, wobei dies dabei sogar die wichtigste Methode ist. Die »Regeln« sind in dem Fall so genannte Signaturdatenbanken, die typische Merkmale von bekannten Viren speichern. Virenscanner werden in Kapitel 7, *Virenscanner* behandelt.

Lernende Systeme

Um die offensichtlichen Angriffspunkte von statischen Regelsätzen zu umgehen, wurden lernende oder dynamische Erkennungssysteme entwickelt. Dynamische Erkennungssysteme ziehen ihre Schlussfolgerungen darüber, ob eine E-Mail Spam ist, aus Vergleichen mit früheren E-Mails, den Schlussfolgerungen aus den früheren E-Mails und Lerneingaben von Benutzern.

Lernende Spam-Erkennungssysteme können sich zum Beispiel merken, welche Wörter im Text der E-Mails eher in Spam oder eher in Nicht-Spam vorkommen. Der Inhalt einer bestimmten E-Mail kann dann mit diesen Datenbanken verglichen werden und durch stochastische Analysen als Spam oder Nicht-Spam eingestuft werden. Derartige Systeme sind insbesondere unter dem (mathematisch nicht korrekten) Namen »Bayes«-Filter bekannt geworden. Die Software SpamAssassin, die in Kapitel 4, *SpamAssassin* behandelt wird, bietet unter anderem ein solches System. Die Software CRM114 (Controllable Regex Mutilator, concept #114) ist ein weiteres lernendes E-Mail-Klassifizierungssystem, das verschiedene andere Algorithmen implementiert, aber nach eigenen Angaben noch experimentell ist.

Lernende Systeme müssen, wie der Name schon sagt, lernen, das heißt, sie müssen erfahren, welche E-Mails der Nutzer als erwünscht und als unerwünscht einstuft. Man sagt auch, das System muss »trainiert« werden. Training verlangt im Extremfall viel Handarbeit, wenn jede einzelne E-Mail von Hand klassifiziert werden muss. In anderen Fällen werden nur die Fehler, also falsche Positive und falsche Negative, trainiert. Oder man bezieht eine E-Mail nur dann ins Training ein, wenn andere Teile des Spam-Erkennungssystems sie bereits als Spam oder Nicht-Spam klassifiziert haben. Dies geht dann vollautomatisch, bietet aber nicht so gute Ergebnisse wie das manuelle Training. Letztendlich hängt es aber auch von der Software und dem verwendeten Algorithmus ab, was und wie trainiert werden muss.

Systeme, die von Rückmeldungen der Nutzer abhängen, stellen auch den Administrator vor ganz neue Herausforderungen. Rückmeldungen müssen empfangen und verarbeitet werden, Nutzer müssen über diese Möglichkeit informiert werden, und Missbrauch muss unterbunden werden. Das SpamAssassin-Kapitel geht auf diese Problematiken ein.

Ein anderes lernendes System ist das so genannte Autowhitelisting. Es merkt sich, wie oft von bestimmten Absendern Spam oder Nicht-Spam empfangen wird, und kann bei neuen E-Mails daraus Schlüsse ziehen. Dieses System dient hauptsächlich der Verhinderung von falschen Positiven. SpamAssassin hat dieses System ebenfalls eingebaut.

Lernende Systeme sind eine passende Ergänzung zu statischen Regeln, sind aber auch keine Wunderwaffe. Spammer können ihre E-Mails auch so anpassen, dass sie lernende Systeme umgehen, zum Beispiel indem eine E-Mail mit irrelevanten Wör-

tern gefüllt wird, die die Bayes-Analyse ablenken. Neue Abwehrmaßnahmen und eine verbesserte Textanalyse werden diesen Problemen in der Zukunft möglicherweise begegnen.

Verteilte Erkennung

Spam und Viren sind ein globales Problem. Spam und Viren, die auf dem lokalen Mailserver auflaufen, werden mit Sicherheit auch auf anderen Mailservern erscheinen. Dies liegt in der Natur von Spam und Computerviren. Aus diesem Umstand kann man Kapital schlagen und die weltweit verteilten Ressourcen bei der Spam- und Virenabwehr zusammenschließen:

- Es stellt sich heraus, dass bestimmte Hosts, IP-Adressen und Domainnamen oft in Verbindung mit Sendungen von Spam oder Viren auftreten. Dies liegt dann oft daran, dass diese Systeme unsicher konfiguriert sind und von Dritten missbraucht werden oder dass sich die Administratoren dieser Systeme nicht kümmern oder dass die Systeme gar Spammern gehören. Man wird geneigt sein, E-Mails von derartigen Systemen durch lokale Konfigurationseinstellungen abzulehnen. Effektiver ist es aber, eine Liste dieser Systeme zentral im Internet zu verwalten und allen zur Verfügung zu stellen, damit kompromittierte oder unsichere Systeme schnell erkannt werden können und jeder vor ihnen geschützt ist. Dieses Prinzip wird durch DNS-Blackhole-Lists (DNSBL) verwirklicht, die in Kapitel 5, *DNS-basierte Blackhole-Lists* behandelt werden.
- Wenn viele unabhängige Mailserver untereinander vergleichen könnten, welche E-Mails bei ihnen durchlaufen, könnte man E-Mails erkennen, die weltweit in großen Mengen in kurzer Zeit versendet werden. Solche E-Mails sind mit ziemlicher Sicherheit entweder Spam oder Viren. Dieses Prinzip wird durch das Distributed Checksum Clearinghouse (DCC) verwirklicht, das in Kapitel 6, *Zusätzliche Ansätze gegen Spam* behandelt wird.
- Alternativ können Mailserver auch die Ergebnisse ihrer Spam-Erkennungssysteme mit anderen teilen. Dazu werden als Spam erkannte E-Mails an eine zentrale Datenbank gesendet, bei der andere Mailserver dann ihrerseits nachfragen können, ob eine ihnen zugesendete E-Mail Spam ist. Dieses Verfahren spart zwar keine Ressourcen, aber man gewinnt zusätzliche Sicherheit bei den Erkennungssystemen durch Vergleiche mit anderen Systemen. Dieses Prinzip wird durch das Pyzor-System verwirklicht, das ebenfalls in Kapitel 6, *Zusätzliche Ansätze gegen Spam* behandelt wird.

Die Verwendung von verteilten Erkennungssystemen ist im Allgemeinen sehr effektiv und empfehlenswert. Sie stellt einen aber vor das Problem, sich dadurch auf Fremde und deren Einschätzungen verlassen zu müssen. Das ist normalerweise kein Problem, sonst gäbe es diese Systeme nicht mehr, mag aber gelegentlich aus Prinzip abgelehnt werden. Dies muss dann bei der Konfiguration berücksichtigt werden.

Andere Methoden

Die oben aufgeführten Methoden stellen im Allgemeinen das Grundgerüst jeder Strategie gegen Spam und E-Mail-Viren dar. Daneben gibt es noch mehrere andere Methoden, die als Ergänzungen dienen können. Einige von diesen werden in Kapitel 6, *Zusätzliche Ansätze gegen Spam* vorgestellt. Die MTA-Software selbst bietet auch verschiedenartige Einstellungen, die zur Abwehr von unerwünschter E-Mail dienen können. Dies wird in Kapitel 3, *Spam- und Virenabwehr mit Postfix, Exim und Sendmail* beschrieben. Bei diesen Maßnahmen handelt es sich zum Teil um verschiedene Tricksereien mit dem SMTP-Protokoll, um mangelhaft implementierte Clients, wie sie von Versendern von Spam und Viren oft verwendet werden, abzulehnen. Darüber hinaus unterstützt fast jede in diesem Buch behandelte Software Whitelists und Blacklists (weiße und schwarze Listen), also explizite Listen von Kommunikationspartnern, je nach Aufbau beispielsweise nach E-Mail-Adresse gelistet, die von der Filterung freigestellt beziehungsweise auf jeden Fall ausgefiltert werden.

Was tun mit erkannter E-Mail?

Wurde eine E-Mail von einer Software-Komponente als Spam oder Virus erkannt, gibt es mehrere Möglichkeiten, mit ihr zu verfahren. Dies hängt von den technischen Möglichkeiten der Software und den Anforderungen des Anwenders ab. Mögliche Verfahrensweisen sind:

Die E-Mail wird abgelehnt: Wenn die Erkennung von Spam oder Viren stattfindet, bevor die Annahme der E-Mail gegenüber dem absendenden Host bestätigt ist, kann die Annahme der E-Mail verweigert werden. Der Absender der E-Mail weiß dann, dass die E-Mail nicht zugestellt werden konnte. Versender von Spam und Viren werden jetzt in der Regel aufgeben und keine neuen Sendeversuche starten. Versender von legitimer E-Mail können auf die erhaltene Fehlermeldung hin eventuell versuchen, ihr E-Mail-System anders zu konfigurieren, die E-Mail nochmals in veränderter Form zu senden oder zumindest den beabsichtigten Empfänger auf andere Art zu kontaktieren. Auf jeden Fall geht so keine legitime E-Mail verloren.

Dieses Verfahren ist theoretisch das beste, weil es die E-Mail-Protokolle korrekt einsetzt, Fehler mit Fehlermeldungen beantwortet und System- und Netzwerkressourcen sinnvoll einsetzt. Es lässt sich aber in der Praxis oft nicht vollständig umsetzen, denn die Erkennung von Spam und Viren während der Annahme der E-Mail ist performancetechnisch problematisch. Daher werden die E-Mails oft bedingungslos angenommen und erst später geprüft, womit dieses Verfahren nicht mehr anwendbar ist. Beide Ansätze, Prüfung während des Empfangs und Prüfung nach dem Empfang, werden in der Praxis eingesetzt und oft in verschiedenen Graden kombiniert. In Kapitel 3, *Spam- und Virenabwehr mit Postfix, Exim und Sendmail* wird beschrieben, wie die verschiedenen Mailserver-Systeme dies umsetzen.

Die E-Mail wird angenommen, gelöscht, und eine Nachricht wird an den Absender geschickt: Dies ist die Alternative zum oben beschriebenen Ablehnen der E-Mail, wenn die Prüfung auf Spam oder Viren erst nach der Annahme der E-Mail stattfindet. Zu dem Zeitpunkt besteht keine Netzwerkverbindung mit dem absendenden Host mehr, und es ist daher auch nicht mehr direkt möglich, diesem eine Fehlermeldung zukommen zu lassen. Die einzige Möglichkeit, den Absender zu benachrichtigen, ist, die Absenderadresse aus dem Envelope oder aus dem E-Mail-Header zu verwenden und eine neue E-Mail mit der Fehlermeldung abzusetzen.

Das Problem bei diesem Verfahren ist, dass Absenderadressen in Spam- und Viren-E-Mails in den allermeisten Fällen gefälscht sind. Derartige Fehlermeldungen gelangen also an unbeteiligte Dritte, die erstens verwirrt und zweitens belästigt werden. Wenn Spam und Viren mit gefälschten Absenderadressen in Massen versendet werden, dann werden diese Dritten mit falschen Fehlermeldungen in Massen überflutet und haben ihrerseits eine Art Spam-Problem. Seit vor ein paar Jahren Spam- und Virenerkennungssysteme Verbreitung gefunden haben, sind derartige fehlgeleitete Fehlermeldungen zu einer ganz neuen Plage im Internet geworden und werden mittlerweile ihrerseits von Anti-Spam-Software bekämpft. Spam- und Virenfilter-Software sollte also, wenn sie diese Funktionalität überhaupt bietet, *auf keinen Fall* so konfiguriert werden, dass sie als Reaktion auf alle E-Mails, die sie als Spam oder Virus eingestuft hat, eine E-Mail an den angeblichen Absender dieser E-Mail sendet.

Die E-Mail wird verworfen: Dabei wird die E-Mail zum Schein für den absendenden Host angenommen, nach der positiven Erkennung als Spam oder Virus aber ohne Nachricht verworfen oder gelöscht. Der Absender kann dann, nach den gültigen E-Mail-Protokollen, davon ausgehen, dass die E-Mail zugestellt wird oder er, eventuell später, eine Fehlermeldung erhalten wird. Beides passiert hier nicht; dieses Vorgehen ist also streng genommen eine Protokollverletzung.

Dieses Verfahren ist natürlich gewissermaßen sehr ressourcenschonend und erspart Nutzern und Administratoren auch viele Umstände. Der Nachteil ist selbstverständlich, dass Fehler bei der E-Mail-Klassifizierung unerkannt bleiben. Als generell anwendbares Verfahren ist es daher ungeeignet. In bestimmten Fällen, bei besonders sicheren Erkennungsergebnissen, kann es aber durchaus eingesetzt werden.

Die E-Mail wird nur markiert und weitergeleitet: Zur Markierung wird zum Beispiel eine neue Header-Zeile eingefügt oder die Betreffzeile geändert. Anhand dieser Markierung kann der Benutzer mit Hilfe des E-Mail-Clients oder anderer zwischengeschalteter Software die E-Mail erkennen und mit ihr nach eigenem Wunsch verfahren. Dabei hat der Empfänger die Möglichkeit, die E-Mail zu löschen oder in ein getrenntes Postfach einzusortieren, oder je nach Software weitere Möglichkeiten.

Dieses Verfahren ist sinnvoll, wenn es nicht möglich erscheint, auf dem Mailserver eine Entscheidung zu treffen, die für alle Nutzer akzeptabel ist, oder wenn es nicht möglich ist, dass die Nutzer auf dem Mailserver ihre eigenen Einstellungen vornehmen können. Es ist auch sinnvoll, wenn die Nutzer im Grunde selbst erfahren genug sind, um die E-Mail-Filterung selbst durchzuführen und die Erkennungssoftware auf dem Mailserver nur aus Ressourcengründen gemeinsam verwendet wird. Insbesondere bei der Spam-Erkennung ist dieses Verfahren üblich. Bei der Virenerkennung ist dieses Verfahren dagegen weniger angebracht, da Viren gar nicht erst auf die Computer des Empfängers gelangen sollten, weil die Gefahr besteht, dass sie dort Sicherheitslücken ausnutzen oder der Nutzer die Virenfilterung ausgeschaltet hat.

Die E-Mail wird an eine andere Adresse umgeleitet: Dies kann eine sekundäre Adresse des Empfängers, die Adresse eines Administrators oder eine speziell für diesen Zweck eingerichtete Adresse sein. Im letzteren Fall wird dann oft von einer Quarantäne gesprochen, in Analogie zur Quarantäne bei der Einfuhr von potenziell infizierten Tieren und Pflanzen. (Der Begriff »Quarantäne« ist abgeleitet von »quaranta«, italienisch für vierzig, und bezieht sich eigentlich auf den zeitlich begrenzten Aufenthalt, 40 Tage, in Isolation. Das ist natürlich bei E-Mails so nicht sinnvoll.) Der Empfänger könnte die E-Mail dann in Einzelfällen, eventuell nur mit Hilfe eines Administrators, aus dem Quarantäne-Bereich beziehen, wenn sich herausstellt, dass die Viren- oder Spam-Erkennung einen Fehler gemacht hat.

Die Verwendung einer Quarantäne ist insbesondere bei der Virenfilterung eine sinnvolle Alternative zum bedingungslosen Verwerfen von E-Mails, insbesondere wenn die Erfahrung oder die Befürchtung besteht, dass der eingesetzte Virenscanner gelegentlich Fehler macht. Man muss allerdings bedenken, dass ein Quarantäne-Bereich nicht nur eingerichtet, sondern auch betreut werden muss, was zu erhöhtem Personal- und Arbeitsaufwand führt.

Die in diesem Buch vorgestellten Software-Lösungen unterstützen, insofern das im jeweiligen Fall sinnvoll und technisch möglich ist, alle diese Verfahrensweisen. Es ist eine der wichtigsten Aufgaben eines Administrators eines Spam- und Virenfiltersystems, auszuwählen, wie mit unerwünschten E-Mails verfahren werden soll. Dabei sollten folgende Faktoren mit bedacht werden:

- Welche Verfahren werden von der Software individuell und im Zusammenhang mit den anderen eingesetzten Software-Komponenten des Mailservers unterstützt?
- Wie gut sind die Erfahrungen mit der Spam- und Virenerkennungssoftware? Am Anfang sollte man sicher nur markieren lassen, später eventuell auf andere Verfahren umsteigen.
- Wenn eine Quarantäne eingerichtet wird: Sind Ressourcen da, um diese zu betreuen?

- Sind die Anwender erfahren genug, dass sie die Filterung selbst übernehmen können? Dann würde eine einfache Markierung ausreichen.
- Unter welchen Umständen ist es akzeptabel, erkannte E-Mails zu löschen?
- Inwiefern müssen verschiedene Benutzergruppen unterschiedlich behandelt werden?

Wie schon zuvor erwähnt, spielen neben diesen Überlegungen auch juristische Belange eine Rolle, siehe Kapitel 14, *Juristische Aspekte beim Einsatz von Spam- und Virenfiltern*. Zusammenfassend kann hier gesagt werden, dass die Filterung von Spam ohne Zustimmung des Anwenders bedenklich ist, die Filterung von Viren jedoch zwingend unter die Sorgfaltspflicht des Administrators fällt.

Ohne zu weit vorgreifen zu wollen, sind folgende Einstellungen, die aber bei weitem nicht überall in der Standardkonfiguration eingerichtet sind, in vielen Fällen angebracht sowie juristisch vertretbar:

- Wenn die Erkennung während der Annahme der E-Mail erledigt werden kann, können Spam und Viren vor der Annahme abgelehnt werden.
- Ansonsten wird Spam markiert und die Filterung dem Empfänger überlassen.
- Viren werden gelöscht oder in einer Quarantäne abgelegt.

Eingehende und ausgehende E-Mail

Bei der Einrichtung von Spam- und Virenfiltersoftware wird man vornehmlich darauf bedacht sein, E-Mails, die von Dritten an die eigene Organisation gesendet werden, zu prüfen. Es kann aber ebenso sinnvoll sein, E-Mails, die aus der eigenen Organisation heraus abgesendet werden, zu prüfen. Dies geht prinzipiell mit der gleichen Software; man muss es nur bei der Konfiguration bedenken.

Das Prüfen von ausgehender E-Mail sichert natürlich nicht das eigene Netzwerk, aber man tut dem Internet einen Gefallen. In großen Organisationen weiß man nie genau, ob nicht ein Benutzer das Netzwerk für den Versand von Spam verwendet. Und wenn ein Computer im eigenen Netzwerk ein Virus eingefangen hat, wäre es von Vorteil, dieses nicht an andere zu versenden. Und man erweist sich selbst einen Dienst: Wenn man als Absender von Spam oder Viren auftritt, schadet das dem Ansehen, und man landet möglicherweise anderswo auf schwarzen Listen.

Als ISP gar sollte man vielmehr davon ausgehen und darauf vorbereitet sein, dass irgendwann ein Kunde ein Spammer ist, Viren versendet oder durch eine Fehlkonfiguration das E-Mail-System stört. Neben entsprechenden technischen Vorkehrungen sind hier im Voraus geplante Verfahrensweisen mit solchen Kunden, gestützt durch die allgemeinen Geschäftsbedingungen, sowie ausreichend Versicherungsschutz (Haftpflicht, Rechtsschutz) zu empfehlen.

Die Reaktionen der Filtersoftware auf Spam oder Viren im ausgehenden E-Mail-Verkehr sollten allerdings anders eingestellt werden als für den eingehenden E-Mail-Verkehr. Es ist sicherlich nicht besonders elegant, Spam aus dem eigenen Netzwerk schon als Spam markiert an die externen Empfänger zu senden. In so einem Fall ist es sinnvoller, einfach den Administrator zu benachrichtigen, der sich dann von Fall zu Fall mit der Problemquelle befassen kann. Beim Versand von Viren sollte ebenfalls der Administrator benachrichtigt und die E-Mail natürlich nicht weitergeleitet werden.

Der menschliche Faktor

Das Problemfeld Spam und Viren hat allen technischen Überlegungen zum Trotz auch einen menschlichen Faktor. Anwender, die unerfahren, unvorsichtig, leichtgläubig, neugierig, fahrlässig oder destruktiv sind, machen die Verbreitung von Spam und Viren erst möglich. Als Administrator eines E-Mail-Systems hat man die Aufgabe, durch technische Mittel, wie die in diesem Buch beschriebenen, diese Nutzer zu schützen sowie das System vor diesen Nutzern zu schützen. Zusätzlich ist es jedoch auch notwendig, diese Anwender im Umgang mit E-Mail und Computern im Allgemeinen zu schulen und weiterzubilden. Im Hinblick darauf wurden in Kapitel 13, *Regeln für Nutzer im Umgang mit Spam und Viren* einige zu empfehlende Verhaltensweisen zusammengestellt.

An der Quelle

Dieses Buch behandelt die Abwehr von Spam und Viren, die bereits versendet worden sind. Ein ganz anderes Thema ist es, Spam und Viren an der Quelle, also beim Versand, zu verhindern, was, wenn man die Problematik als Ganzes betrachtet, natürlich viel sinnvoller ist. Der Versand vom Spam und Viren wird hauptsächlich begünstigt durch:

- als offene Relays konfigurierte Mailserver,
- allgemeiner formuliert, falsch konfigurierte Software,
- Sicherheitslücken aller Art sowie daraus resultierende kompromittierte Rechner (»Zombies«),
- unvorsichtige Anwender,
- mangelnde rechtliche Handhabe,
- Absender im Ausland sowie
- annähernde Anonymität als Kunde eines großen ISP.

Obwohl Bestrebungen existieren, gegen diese Probleme vorzugehen, kann man schon anhand der Formulierungen erahnen, dass hier gar keine abschließenden Lösungen existieren können. Die Notwendigkeit von Spam- und Virenfiltersystemen auf der Empfängerseite wird also fortbestehen.