In diesem Kapitel:

- SMTP und POP
- Absender
- Bösartiger Code
- Mailbomben
- Hoax
- Spam – Werbe- und Massenmails
- E-Mail-Maulwürfe
- Webmail
- Verschlüsselung mit GnuPG und PGP

KAPITEL 6

E-Mail – wer liest mit?

Die provokative Frage im Titel dieses Kapitels ist keineswegs als schlechter Scherz gemeint. Man könnte sie sogar noch zugespitzter formulieren und fragen: »Wie viele lesen mit?«. Dass elektronische Post mitgelesen wird, ist heutzutage kein Geheimnis mehr. Viel beunruhigender ist jedoch die Tatsache, dass es sich dabei nur in den wenigsten Fällen um Cracker, sondern hauptsächlich um Regierungen verschiedener Länder handelt. Mit dem Argument des »Schutzes der Allgemeinheit« werden immer wieder Rufe nach vollständiger Überwachung der elektronischen Kommunikation laut. Wie Sie in Kapitel 9, *Anonymität*, noch lesen werden, wird heutzutage ein Großteil des gesamten Datenverkehrs von den USA und einigen weiteren Staaten mit Hilfe des Abhörsystems »Echelon« überwacht. Dabei spielt es keine Rolle, ob Sie selbst Bürger der Vereinigten Staaten sind. Dass Ihre Daten in vielen Fällen entweder über in den USA stationierte Server und Router oder über amerikanische Kommunikationssatelliten wandern, ist für die dortige Regierung Grund genug, diese Daten zwischenzuspeichern und auszuwerten.

Vor einigen Jahren waren die Kapazitäten der EDV-Systeme noch so beschränkt, dass man mit der schier unendlichen Datenflut nicht zurande kam und die Informationen deshalb nicht flächendeckend ausgewertet werden konnten. Das hat sich in den letzten Jahren geändert. Die Behörden in den USA erwägen sogar, alle Telefonate zu protokollieren, da sie mittlerweile über die Technologien und Kapazitäten verfügen, um eindeutige Benutzerprofile anzulegen und aus dem Datenstrom herauszufiltern. Der Hamburger Heise-Verlag berichtet in seinem Newsticker unter *http://www.heise.de* sowie in der Netzkultur-Zeitung *Telepolis* und dem Computermagazin *c't* immer wieder über neue beunruhigende Entwicklungen in diesem Sektor. Im Verlauf dieses Kapitels werden wir daher eine weitere Anwendungsmöglichkeit von GnuPG kennen lernen, die Verschlüsselung von E-Mails.

In diesem Kapitel geht es weniger um die praktischen Aspekte als um die technischen Grundlagen des E-Mail-Dienstes, weshalb wir auf eine detaillierte Erläuterung einzelner Mail-Clients verzichten. Da die Konfiguration des Browsers in den

meisten Fällen auch für den Mail-Client gilt, haben wir die aus Sicherheitsperspektive wichtigsten Einstellungen für kombinierte Programme bereits in Kapitel 5, *Browser – einer für alles*, vorgenommen.

SMTP und POP

SMTP und *POP* sind die wichtigsten E-Mail-Protokolle.[1] Das Kürzel SMTP steht für *Simple Mail Transfer Protocol* und bezeichnet den Dienst, der für das Senden von E-Mails zuständig ist. SMTP-Server lauschen auf Port 25 auf Anfragen. Spezifiziert wurde SMTP im RFC 821.

Wenn Sie von Ihrem Mail-Client aus eine E-Mail abschicken, verpackt der Client die Mail entsprechend SMTP und schickt sie über TCP an Ihren Mailserver. Nachdem die Mail vom Server akzeptiert wurde, überprüft dieser zunächst die Adresse des Empfängers. Liegt diese Adresse in der eigenen Domain, wird die Nachricht gespeichert und kann vom Empfänger abgeholt werden. Liegt die Adresse in einer anderen Domain, leitet der SMTP-Server die E-Mail an den zuständigen Mailserver weiter. Auf diese Weise wandert die Nachricht auf ihrem Weg bis zum Ziel über mehrere Hosts, die sie jeweils temporär zwischenspeichern.

Leider ist SMTP das Alter von über 20 Jahren deutlich anzumerken, denn es sendet alle Daten im Klartext und verlangt in der Grundversion nicht einmal eine Authentifizierung per Passwort durch den Benutzer. Sie können also theoretisch jeden beliebigen SMTP-Server im Internet für dunkle Zwecke mißbrauchen. Im Zeitalter großen Wachstums von Netzwerken und besonders des Internets haben aber viele Provider und Hersteller Möglichkeiten gefunden, ihre SMTP-Server gegen unbefugte Benutzung abzusichern. Der Provider kann beispielsweise prüfen, ob die Absenderadresse aus seiner eigenen Domain stammt oder ob die dynamisch zugewiesene IP-Adresse des versendenden Rechners dem eigenen Bestand angehört. Ist das nicht der Fall, kann der Provider die Annahme und Weiterleitung der Mails verweigern. Auch Autentifizierungen (oft SMTP-Login genannt) oder das SMTP-after-POP-Verfahren, bei dem der SMTP-Dienst nur dann eine E-Mail annimmt, wenn der Benutzer sich zuvor beim POP-Dienst ausgewiesen hat, sorgen inzwischen für mehr Sicherheit. Allerdings gibt es nach wie vor genügend Server im Netz, die sich anonym zum Senden von Mailbomben, Spam oder Hoax missbrauchen lassen (siehe dazu die entsprechenden Abschnitte weiter hinten in diesem Kapitel). Die Zeit, in der Mailserver ein beliebtes Angriffsziel waren, ist jedoch vorbei, da Spam-

1 Das Internet Message Access Protocol (IMAP) ist das dritte bekannte Mail-Protokoll, dessen Einsatz vor allem aus Sicherheitsgründen empfehlenswert wäre. Zwar unterstützen die meisten bekannten E-Mail Clients IMAP mehr oder weniger gut, doch bieten nur wenige Provider und Mailboxanbieter IMAP (bei dem die E-Mails auf dem Server verbleiben) an. Daher verzichten wir hier auf eine ausführliche Besprechung und verweisen auf *http://www.imap.org*. Interessierten Lesern sei nach der Lektüre dieses Kapitels dennoch ein Blick auf IMAP empfohlen.

mer nun vielmehr die PCs von privaten Surfern zum Verschicken ihrer E-Mails benutzen (siehe Kapitel 10, *Viren, Würmer und Trojaner*).

Ebenfalls auf TCP basiert das *Post Office Protocol* (POP), das an Port 110 lauscht. Es bildet das Gegenstück zu SMTP und ist für den Empfang von E-Mails zuständig. Mittels POP und eines Mail-Clients können Sie Ihre Nachrichten vom Mailserver herunterladen. POP bedarf zwar einer Authentifizierung durch den Benutzer, übermittelt aber ebenfalls alle Daten, einschließlich Benutzername und Passwort, im Klartext. Auch an dieser Stelle könnten externe Angreifer und selbst beliebige Rechner, die im gleichen Netz stehen wie Ihr eigener PC, die Kommunikationsdaten abfangen und somit Zugriff auf Ihren Mail-Account erlangen.

Wie Sie sehen, lässt sich der gesamte E-Mail-Dienst nicht unbedingt als sicher bezeichnen. Sensible Daten sollten daher niemals unverschlüsselt per E-Mail übertragen werden. Um so unverständlicher ist es daher, dass es bei Providern und Internetanbietern (wie beispielsweise Online-Shops) oft an der Tagesordnung ist, Passwörter im Klartext per Mail zu verschicken. Sie sollten in einem solchen Fall beim Anbieter nachfragen, ob Sie das Kennwort selbst ändern können, und dies anschließend auch schnellstmöglich erledigen.

Absender

Wenn Sie eine E-Mail empfangen haben, sehen Sie in der Regel auf den ersten Blick im Header der Nachricht den Namen und die E-Mail-Adresse des Absenders. Haben Sie sich schon einmal Gedanken darüber gemacht, ob diese Angaben überhaupt stimmen müssen?

Tatsächlich ist es möglich, Mails mit einer fremden Absenderadresse zu verschicken. Dieses Problem liegt in der Konzeption des SMTP-Dienstes begründet. Wie Sie im letzten Abschnitt lesen konnten, verfügen viele SMTP-Server über keinerlei Sicherheits- oder Authentifizierungsmechanismen. Ein Angreifer kann als Absender in eine Mail eine beliebige Adresse und den dazu passenden Benutzernamen eingeben, ohne dass Sie den Betrug bemerken würden. Die gefälschte Nachricht ist von einer wirklich vom angegebenen Absender stammenden E-Mail nicht ohne Weiteres zu unterscheiden.

Diese Betrugsmethode wird gern verwendet, um in den Besitz von Account-Daten zu kommen. Cracker geben sich beispielsweise bevorzugt als Administratoren von Mailprovidern aus und erfragen von arglosen Benutzern deren Zugangsdaten, die diese dann per Mailantwort an den angeblichen Administrator zurückschicken sollen (Social Engineering-Attacke). Wenn Sie eine Mail mit dem ANTWORTEN-Button Ihres Mailprogramms beantworten, wird diese normalerweise an die Adresse verschickt, die auch als Absender angegeben ist. Dies muss jedoch nicht immer der Fall sein. Dem Cracker bleiben mindestens zwei Möglichkeiten, in den Besitz Ihrer Antwort zu kommen. Die erste Variante wäre, dass es ihm gelungen ist, einen der Rech-

ner, über den Ihre E-Mail auf dem Weg zum Adressaten wandert, zu unterminieren (also quasi in seine Gewalt zu bringen). Er kann dann in aller Ruhe eine Kopie der Nachricht anfertigen und sogar verhindern, dass diese den eigentlichen Empfänger erreicht. Dies dürfte aber der schwierigere Weg sein – es geht auch deutlich einfacher. Die zweite Möglichkeit basiert darauf, dass man in den meisten Programmen zu einer E-Mail auch eine Adresse angeben kann, an die eine mit dem ANTWORTEN-Button erzeugte E-Mail geschickt werden soll. Diese Adresse kann sich von der Absenderadresse unterscheiden und wird in den Standardeinstellungen der meisten Mail-Clients auf Empfängerseite nicht angezeigt. Der Angreifer kann z.B. die Antwortadresse auf einen kostenlosen Account im Internet setzen. Ohne es zu bemerken, schicken Sie die Antwort mitsamt Ihren Benutzerdaten dann direkt an das Postfach des Crackers. Um solchen Gefahren vorzubeugen, sollten Sie niemals wichtige persönliche Daten auf Anforderung unverschlüsselt per E-Mail verschicken. Bedenken Sie außerdem, dass ein echter Administrator Sie nie nach Ihren Benutzerdaten fragen wird oder Sie gar auffordern, Ihr Passwort in eine von ihm vorgegebene Kennung zu ändern.

Es gibt jedoch einen zuverlässigen Weg herauszufinden, ob es sich bei einer zweifelhaften Nachricht um eine gefälschte E-Mail handelt. Wie Sie im Abschnitt »SMTP und POP« gelesen haben, wird eine Nachricht meist über zahlreiche SMTP-Server durch das Internet geleitet, bis sie den Zielserver (von dem Sie dann Ihre elektronische Post abrufen) erreicht. Auch wenn diese Route nicht immer die gleiche ist, kann mit großer Gewissheit gesagt werden, dass zumindest der erste SMTP-Server, den ein bestimmter Absender verwendet, immer derselbe ist. Verschickt ein Freund seine E-Mails normalerweise über den Server *smtp.beispiel.de*, besteht kein Grund, dass ausgerechnet eine verdächtige Nachricht dieses Absenders eine völlig andere Route genommen haben sollte. Wie gelangt man aber zu dieser Information?

Eine E-Mail besteht aus weit mehr als nur dem für Sie sichtbaren Text. Ein Blick in den Quelltext der Nachricht (siehe Abbildung 6-1) verrät neben der Route unter anderem auch das vom Absender benutzte Mailtool. Schauen wir uns an, wie man zum Quelltext der Nachricht gelangt:

Thunderbird

Bei geöffneter Mail rufen Sie aus dem Menü ANSICHT den Befehl NACHRICHTEN-QUELLTEXT auf (oder drücken Strg-U) und gelangen so direkt in ein neues Fenster mit dem Quell-Code der betreffenden Nachricht.

Microsoft Outlook/Outlook Express[2]

Für Outlook wählen Sie im ANSICHT-Menü der geöffneten Nachricht den Befehl OPTIONEN und finden den Quelltext anschließend im unteren Bereich in

2 Microsoft ändert die Menüs beinahe in jeder Programmversion und folgt bei Outlook und Outlook Express einer anderen Logik in der Benutzeroberfläche. Daher kann es sein, dass die hier beschriebenen Menüs in verschiedenen Versionen anders benannt sind oder Befehle sich an einer anderen Stelle befinden. Das Vorgehen bleibt aber generell das gleiche.

Abbildung 6-1: Der Quelltext einer E-Mail

einer kleinen Box mit dem (verwirrenden) Namen INTERNETKOPFZEILE. Die Registerkarte DETAILS in dem daraufhin erscheinenden Dialogfeld enthält den Nachrichtenkopf. Im Falle von Outlook Express wählen Sie, wiederum bei geöffneter E-Mail, im Menü DATEI die EIGENSCHAFTEN und dort den Reiter DETAILS und anschließend den Button QUELLTEXT. Alternativ können Sie die Tastenkombination Strg-F3 benutzen.

Opera

Auch das Mailtool von Opera verfügt über einen Befehl zur Anzeige des E-Mail-Headers. Dazu markieren Sie die Nachricht und wählen den Befehl QUELLTEXT im Menü Ansicht. Bei geöffneter E-Mail können Sie auch die Tastenkombination Strg-F3 benutzen.

Eudora

Hier klicken Sie bei geöffneter Nachricht auf den etwas absurd benannten Button BLAHBLAHBLAH, der sich in der Shortcut-Leiste direkt über dem Nachrichtenfenster befindet. Im Nachrichtenfenster selbst wird dann über der eigentlichen Nachricht der komplette Header angezeigt.

WordPerfect Mail

Den vollständigen Nachrichten-Header erreichen Sie bei geöffneter Mail über das Menü ANSICHT und den Befehl QUELLTEXT.

Aus den so erhaltenen Daten kann man einige Schlüsse über den Absender ziehen. Das Feld X-MAILER gibt zum Beispiel das verwendete Mailprogramm preis. Jemand, der Ihnen bisher mit Thunderbird gemailt hat, wird wahrscheinlich nicht kurzerhand auf einen amerikanischen Webmail-Account umgestiegen sein. Aussagekräftiger sind jedoch die Informationen, die sich hinter dem Schlüsselwort RECEIVED verstecken. Jeder SMTP-Server, den die E-Mail auf ihrer Reise passiert hat, fügt sein eigenes RECEIVED-Feld in die Nachricht ein. Diesen Zeilen ist zu entnehmen, von wem der Server die Nachricht erhalten hat (FROM) und wer er selber ist (BY). Da jeder weitere Server die E-Mail neu verpackt, steht an erster Stelle im Header der Server, der die Nachricht zuletzt verschickt hat. Die unterste RECEIVED-Zeile gibt also den Ausgangsserver (und sogar den Client, der ihm die Daten übermittelt hat) an. Unter dem Eintrag RETURN PATH finden Sie die Adresse, an die Ihr Client Ihre Antwort schicken wird. Schauen Sie sich ruhig einige Mail-Header an, um ein Gefühl dafür zu bekommen, über welche Server Kollegen und Freunde ihre Nachrichten verschicken. Eine angeblich firmeninterne Nachricht wird beispielsweise niemals über die Hosts von Freemail-Services oder Universitäten geleitet. Zwar kann man mit Hilfe der Header-Informationen recht genau ausmachen, ob es sich um eine gefälschte E-Mail handelt, dies funktioniert aber natürlich nur dann zuverlässig, wenn der Angreifer einen anderen Server als der wirkliche Absender benutzt. Senden beide über den gleichen SMTP-Server (z.B. weil beide einen Account bei T-Online haben), kann der Betrug auf diese Weise nicht nachgewiesen werden.

Um zu verdeutlichen, dass es sich bei gefälschten E-Mails nicht nur um eine theoretische Gefahr, sondern um ein reales Problem handelt, soll folgendes Beispiel dienen: Ende Februar 2001 sorgte eine Social Engineering-Attacke auf GMX-Kunden für Aufsehen. GMX ist einer der führenden Webmail-Betreiber (die werden wir im Abschnitt »Webmail« noch einmal genauer betrachten). Von einem Absender mit der Adresse *anmeldeservice@hotmail.com* erhielten GMX-Kunden die Nachricht, dass GMX ab dem 15. März mit Microsoft Hotmail (einem weiteren Freemail-Dienst) verschmelzen werde. Die Empfänger wurden dazu aufgefordert, eine Nachricht mit dem Betreff »Angebotsverlängerung« an die oben genannte Adresse zu schicken, um auch weiterhin den Freemail-Dienst nutzen zu können. Als Inhalt sollten der Login-Name und das Passwort angegeben werden. Auf Anfrage von *heise online* dementierten sowohl GMX als auch Hotmail diesen Zusammenschluss. Zwar kündigte Microsoft als Betreiber von Hotmail an, den betrügerischen Account sofort zu sperren, wie viele Kunden in der Zwischenzeit ihre Daten preisgegeben hatten, bleibt jedoch ungeklärt.

Bösartiger Code

Unter bösartigem Code versteht man Programme oder Skripten, die, wenn sie ausgeführt werden, in der Lage sind, auf dem betroffenen Computer Schaden anzurichten. Im Fall des E-Mail-Dienstes kann man bösartigen Code in zwei Gruppen einteilen:

Bei der ersten Gruppe handelt es sich um *Attachments* (Mail-Anhänge), die ausführbaren Code enthalten. Beispiele hierfür sind die klassischen Viren, die meist in Form von *.vbs*- oder *.exe*-Dateien wie z.B. *happy99.exe* auftreten und nach dem Start dieser Dateien aktiv werden. Aber auch Viren (Würmer), die auf Skriptsprachen basieren, wie beispielsweise *I LOYE YOU*, zählen hierzu. Bösartigen Code dieser Art haben wir bereits ansatzweise in Kapitel 5, *Browser – einer für alles*, betrachtet und werden in Kapitel 10, *Viren, Würmer und Trojaner*, noch genauer darauf eingehen.

In diesem Abschnitt wollen wir uns mit der zweiten Gruppe, dem unmittelbar in der Mail enthaltenen Code, beschäftigen. Ursprünglich bestand eine elektronische Nachricht aus reinem Fließtext ohne die heute gängigen Formatierungen wie fett, kursiv oder verschiedenfarbiger Schrift. Inzwischen ist E-Mail der am häufigsten im Internet genutzte Dienst geworden, und aus den funktionsarmen Clients von früher sind komfortable Programme mit vielen grafischen Spielereien geworden. Da lag die Überlegung natürlich nahe, auch das langweilige Design der eigentlichen Nachrichten grundlegend zu erneuern. Wie auch beim WWW-Dienst stand man vor dem Problem der Heterogenität des Internets, d.h. der Tatsache, dass das Internet aus Maschinen mit vielen verschiedenen Betriebssystemen besteht, die alle eine andere Sprache sprechen (siehe hierzu Kapitel 4, *World Wide Web*). Es musste also ein betriebssystemunabhängiges Format zur Darstellung von E-Mail-Inhalten gefunden werden. Um das Rad nicht neu erfinden zu müssen, bediente man sich auch hier der Auszeichnungssprache HTML. Seitdem haben Sie als Benutzer die Möglichkeit, eine Nachricht wahlweise in reinem Textformat oder im HTML-Stil zu verfassen.

Abbildung 6-2: Eine E-Mail mit HTML-Inhalt

Schauen wir uns die in Abbildung 6-2 dargestellte Nachricht an. Das Mailtool generiert zu den von uns gewählten Formatierungseigenschaften automatisch den HTML-Quelltext. Für unser Beispiel sähe er (abhängig vom Programm) in etwa so aus:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<meta content="text/html;charset=ISO-8859-1"
http-equiv="Content-Type">
</head>
<body bgcolor="#ffffff" text="#000000">
<b><font color="#999999"><big><big>Testmail</big></big></font> </b>  <b
class="moz-txt-star">
<i><u><big><big><span class="moz-txt-tag"> </span>in</big></big></u></i>
<span class="moz-txt-tag"></span></b>HTML mit <b><big>verschiedenen </big></b><i>
Formatierungen</i>.<br>
</body>
</html>
```

Sie sehen, dass es sich tatsächlich um HTML-Code handelt. Nur in wenigen Fällen kann reines HTML Schwierigkeiten verursachen. Problematisch ist aber die Möglichkeit, in diesen HTML-Code Skriptsprachen wie JavaScript oder VBS einzubetten. Um zu vermeiden, dass beim Öffnen einer E-Mail Skripten automatisch ausgeführt werden, sollten Skriptsprachen in den Einstellungen des E-Mail-Programms generell unbedingt deaktiviert werden.

Aber auch reiner HTML-Code kann zu unerwünschten Effekten führen. Die Tatsache, dass Werbemails oft nur dann lesbar sind, wenn der Benutzer online ist, sollte zu denken geben. Öffnet man eine solche Nachricht, versucht das Mailtool sich mit dem Internet zu verbinden. Bei seriösen Anbietern kann man davon ausgehen, dass nur Bildmaterial aus dem Netz geladen wird, theoretisch könnte es sich dabei aber auch um andere Inhalte wie z.B. Viren handeln. Auf jeden Fall erfährt der Absender der Mail auf diese Weise, wann Sie Ihre Post gelesen haben. Da man beim Öffnen einer Nachricht also nicht genau weiß, wo die Reise hingeht, sollte man auch HTML deaktivieren. Wenn dies bei Ihrem Mail-Client nicht möglich ist, sollten Sie unseriöse Nachrichten direkt in den Papierkorb verfrachten oder den Spamfilter aktivieren. Wie das funktioniert, erfahren Sie im Abschnitt »Spam – Werbe- und Massenmails« später in diesem Kapitel.

Zu guter Letzt wollen wir einige Beispiele von bösartigem Code betrachten: Bei aktivierten Skriptsprachen kann das Öffnen einer E-Mail zum Systemabsturz führen, indem der Angreifer z.B. Code in seine Nachricht integriert, der den Browser anweist, in schneller Abfolge neue Fenster zu öffnen. Der Code wird ausgeführt, sobald der ahnungslose Empfänger die Mail liest. Der Schaden besteht darin, dass das Betriebssystem mit den immer neu aufpoppenden Browserfenstern irgendwann nicht mehr Schritt halten kann und abstürzt.

Andere Skripten können bei bestimmten Sicherheitslücken Dateien auf Ihrem PC lesen oder gar schreiben. Dem Opera-Mail-Client konnte man beispielweise bis zur Version 8.50 als Bild getarnte Skripten unterschieben, die anschließend unter lokalen (und somit vollständigen) Rechten ausgeführt wurden.

Besonders Würmer machen sich die Sicherheitslücken zunutze, die durch die Integration von immer mehr multimedialen Funktionen in Mail-Clients (allen voran Outlook und Outlook Express) entstehen. Wie wir in den folgenden Abschnitten sehen werden, reicht inzwischen unter Umständen das Anklicken einer E-Mail zur Infektion aus.

Mailbomben

Eine beliebte und häufig genutzte Möglichkeit, Unfrieden zu stiften, ist das Verschicken von so genannten *Mailbomben*. Dabei wird das Ziel mit einer großen Anzahl an (meist gleichen) Nachrichten regelrecht überflutet. Der Angreifer bedient sich dazu in der Regel spezieller Programme, die es ihm ermöglichen, anonym zu bleiben. Der Umfang einer solchen Attacke liegt je nach der Netzbandbreite, die dem Cracker zur Verfügung steht, zwischen einigen hundert und mehreren zehntausend Nachrichten. Von manchen Angriffen sind aber auch Größen von mehr als hunderttausend E-Mails bekannt. Unabhängig davon ist das Prinzip immer das gleiche: Der Angreifer missbraucht einen oder direkt mehrere ungesicherte SMTP-Gateways, um seine Nachrichten an das Opfer zu verschicken. Um sich nicht durch seine IP-Adresse zu verraten, wird diese mittels eines Programms oder eines Proxys maskiert und verweist daher nicht mehr auf den Ursprungsrechner. Inzwischen bedienen sich immer mehr Angreifer so genannter Bot-Netze, die wir im Laufe dieses Buches noch genauer unter die Lupe nehmen werden.

Die Auswirkungen für den Empfänger einer Mailbombe können vielfältig ausfallen. Bei einem klein dimensionierten Angriff ist lediglich mit einer längeren Online-Zeit für das Herunterladen der Nachrichten zu rechnen, größere Bomben können aber zu ernsthafteren Problemen führen. Dies liegt zum einen daran, dass POP-Server beim Herunterladen mehrerer hundert Nachrichten die Verbindung verlieren können und der Benutzer anschließend alle Nachrichten erneut herunterladen muss. Zum anderen kann es ohne Weiteres einige Stunden dauern, bis sämtliche Mails endlich auf dem heimischen PC angekommen sind. Bei einer langsamen Verbindung über ISDN oder ein analoges Modem kann es daher passieren, dass es partout nicht gelingen will, alle Nachrichten herunterzuladen, und der Benutzer so in einer Schleife festhängt. Die Verbindung zum POP-Server wird dann immer wieder abbrechen.

Ein weiteres Problem stellt der vom Mailprovider zur Verfügung gestellte Speicherplatz dar. Viele Anbieter beschränken die Größe der Accounts auf wenige MByte. Ist dieser Speicherplatz belegt, gehen weitere ankommende Nachrichten verloren. Da der Speicherplatz nach einer größeren Mailbombenattacke verbraucht ist, werden neue Nachrichten nicht mehr akzeptiert, sondern mit einem Hinweis auf die überfüllte Mailbox des Empfängers an den Absender zurückgeschickt. Besonders häufig tritt dieses Problem bei Webmail-Accounts von Freemail-Anbietern auf, aber auch

T-Online ist betroffen. Das Problem besteht meist darin, dass die Benutzer oft vergessen, die Mails wirklich vom Server auf die Festplatte zu laden, was dazu führt, dass der Posteingang langsam voll läuft. Es hat daher auch Vorteile sich die Nachrichten direkt auf dem Server anzuschauen, denn gefährliche Nachrichten können vor dem Herunterladen gegebenenfalls direkt dort gelöscht und der eigene PC auf diese Weise keiner Gefährdung ausgesetzt werden.

Angriffe im Umfang vieler tausend E-Mails bereiten aber noch ein anderes Problem. Nicht nur Outlook Express, sondern auch Thunderbird neigt dazu, bei einer großen Anzahl neuer Nachrichten am Ende des Downloads abzustürzen und möglicherweise einen Crash des Betriebssystems nach sich zu ziehen. Gerade im Fall von Outlook Express kann dies zudem zu einer frustrierenden Endlosschleife führen. Jedes Mal, wenn Sie wieder versuchen, den Posteingang zu öffnen, versucht Outlook, alle enthaltenen Nachrichten aufzulisten und stürzt anschließend wieder ab. Bei der aktuellen Version 6 tritt das Problem glücklicherweise nicht mehr so häufig auf. Sollten Sie wegen der großen Anzahl an Nachrichten Probleme beim Herunterladen haben, hat Ihr Provider die Möglichkeit, die E-Mails direkt auf dem Server zu löschen. Oftmals können Sie Ihre E-Mails aber auch online über eine Weboberfläche lesen und löschen.

Gegen einige zehntausend Mails ist aber fast jedes Programm machtlos und wird rasch instabil. Dies liegt daran, dass die meisten Mailtools die Nachrichten in einem eigenen datenbankähnlichen Format abspeichern, das neben den eigentlichen Nachrichten große Mengen an Metadaten enthält. Die bei einer Mailbombe entstehende Inbox-Datei wird unter Umständen einige hundert MByte groß und bringt daher den Speicher Ihres PCs in arge Bedrängnis. Ist diese Mail-Datenbank erst einmal beschädigt, gehen dadurch alle Nachrichten in dieser Datei verloren. Zwar legen einige Hersteller Reparaturtools bei, doch deren Leistung ist meist gering. Gerade Outlook hat hier einen zweifelhaften Ruhm erlangt, und zahlreiche Anbieter verdienen daher Geld damit, Reperaturtools zu vertreiben, die Microsoft selbst leider nicht anbietet. Betroffen sind vor allem Versionen bis Outlook XP.

Viel gefährlicher als für Privatanwender sind Mailbomben aber für die entsprechenden Server, die mit dieser Last umgehen müssen und bei großen Angriffen zusammenbrechen. Daher wenden sich solche Angriffe oft gezielt gegen einzelne Server und stellen dann eine Art DoS-Angriff dar.

Ein guter Tipp ist daher, Nachrichten möglichst stark auf verschiedene Ordner zu verteilen, da viele gängige Mail-Clients für jeden Ordner eine eigene, von den anderen Ordnern unabhängige Datei anlegen. Bei einem potenziellen Ausfall geht dann nicht mehr die gesamte Post verloren. In der Praxis hat sich, vor allem bei größerem Mailaufkommen, folgende Taktik bewährt: Legen Sie für jeden Bereich einen neuen Ordner in Ihrem Postfach an (z.B. Privat, Geschäftlich, Hobby, Sonstiges). Verschieben Sie nach dem Lesen die eingegangenen Nachrichten in die jeweiligen Ordner, so dass der eigentliche Posteingang am Ende wieder leer ist. Datenverlust kann

dann entweder nur in einem Bereich oder im fast immer leeren Posteingang auftreten. Dennoch sollten Sie natürlich darauf achten, Ihre Mails regelmäßig zu sichern.

Um gar nicht erst von Mailbomben belästigt zu werden, können Sie statt POP das bereits erwähnte *Internet Message Access Protocol* (IMAP) verwenden, da bei IMAP die Nachricht auf dem Server verbleibt und zunächst nur die Betreffzeile der einzelnen Mails angezeigt wird. Unverlangte Post kann man daher direkt vom Server löschen, ohne den Mail-Client mit der Mailbombe in Bedrängnis zu bringen. Leider wird IMAP bislang nicht von allen Providern angeboten, so dass nicht allen Benutzern diese Möglichkeit offen steht.

Kommen wir aber nun zurück zum eigentlichen Angriff. Wie soll man sich als Benutzer verhalten, wenn man von einer Mailbombe betroffen ist? Als bewährtes Mittel hat sich für kleinere Angriffe eine Mail an die Postmaster der beteiligten SMTP-Gateways[3] sowie den eigenen Provider erwiesen. Zwar sind diese nicht verpflichtet, in irgendeiner Weise zu reagieren, in den meisten Fällen werden sie jedoch selbstständig versuchen, Licht ins Dunkel zu bringen. Bei häufigeren Angriffen oder Dimensionen jenseits einiger hundert oder tausend E-Mails sollten Sie aber in Erwägung ziehen (insbesondere wenn der eigene Unternehmens-Account oder gar Server betroffen ist), auch rechtliche Schritte zu ergreifen. Dazu benötigen Sie aber unter Umständen ein dickes Fell, denn die Wahrscheinlichkeit, dass der Cracker tatsächlich gefasst wird, ist sehr gering. Das liegt vor allem daran, dass die Polizei in der Verfolgung solcher Delikte meist noch recht wenig Erfahrung hat und die Angreifer sich hinter anderen Rechnern tarnen. Wichtig ist eine Anzeige aber dennoch, um die eigenen rechtlichen Ansprüche zu wahren. Bei einem ausgewachsenen Mailbombenangriff auf eine Firmenadresse sollte man zusätzlich einen Security-Spezialisten zur Beratung heranziehen. Dieser ist in der Lage, die nötigen Maßnahmen zu treffen und gegebenenfalls das Firmennetz auf mögliche Schwachstellen zu prüfen, um einem potenziellen Crackerangriff vorzubeugen. Als Beispiel für eine größere Mailattacke sei der Angriff auf die Mailserver bei der großen WDR-Computer-Nacht zu nennen, der die dortigen Mail-Accounts für Stunden nahezu lahm legte.

Hoax

Der englische Begriff *Hoax* lässt sich in unserem Zusammenhang am besten mit »Falschmeldung« oder »blinder Alarm« übersetzen. Im Internet tauchen Hoaxes meist in Form von Kettenbriefen auf. Unabhängig vom Inhalt folgen sie immer demselben Prinzip: Der Empfänger soll die Nachricht möglichst schnell an möglichst viele Bekannte weiterleiten. Typische Themen für solche Kettenmails sind beispiels-

3 Die Adresse lautet meist *postmaster@smtp-gateway.de* (wobei für *smtp-gateway.de* natürlich der Name des entsprechenden Servers eingesetzt werden muss).

weise Viruswarnungen, die unbedingt schnell weitergeleitet werden sollen, oder angebliche Hilfe- und Spendenaufrufe.

Damit die Nachrichten auch tatsächlich weitergeleitet werden, überlegen sich deren Erfinder immer raffiniertere und erschütterndere Geschichten. Wir wollen uns an dieser Stelle einen besonders hartnäckigen Hoax anschauen, der sogar gleich zweimal zuschlug.

Der Betreff dieser Kettenmail lautete meist »Knochenmarkspende«. Angeblich suchte jemand Hilfe für seine an Leukämie erkrankte Freundin. Dazu sei dringend eine Knochenmarkspende nötig, da besagte Freundin nur noch einige Wochen zu leben habe. Als Kontaktperson wurde eine gewisse Julia Schmidt samt Arbeitsanschrift, Telefon- und Faxnummer aufgeführt. Zahlreiche gutmütige Benutzer haben diese E-Mail an alle in Ihrem Adressbuch verzeichneten Personen weitergeleitet und so eine erhebliche Mailflut verursacht. Einige Tage später bat besagte Frau Schmidt die Empfänger des Kettenbriefes, eine zweite E-Mail weiterzuleiten. Diese zweite Nachricht enthielt eine persönliche Stellungnahme zu der Leukämiespende. Frau Schmidt schrieb dort, dass sie nicht die Verfasserin der ersten Kettenmail gewesen sei und jemand sie böswillig als Kontaktperson eingetragen habe. Seit Tagen stehe ihr Telefon nicht mehr still, und die Mailbox laufe über. Weiter bat sie die Leser, die Knochenmark-Mail nicht mehr zu verbreiten, stattdessen aber ihre Stellungnahme publik zu machen, damit das Telefon endlich wieder ruhe. Unabhängig davon, ob diese zweite E-Mail wirklich ernst gemeint war oder nicht, verursachte sie jedoch wieder viel unnötigen Mailverkehr.

Als Empfänger eines solchen Kettenbriefs sollte man weder die erste noch die zweite E-Mail weiterleiten, sondern beide in den Papierkorb verschieben. Um besser beurteilen zu können, ob es sich bei einer E-Mail tatsächlich um einen Hilferuf oder nur um einen Hoax handelt, genügt ein Blick in die Hoax-Info (*http://www.tu-berlin.de/www/software/hoax.shtml*) der TU Berlin. Dort findet man eine Liste aller bekannten Hoaxes samt einer ausführlichen Beschreibung.

Machmal werden Hoaxes auch als »manuelle Viren« bezeichnet. Das ist eine Anspielung darauf, dass sie über keine eigene Schadensroutine verfügen, aber der Benutzer den Schaden dennoch eigenhändig verursachen kann. So gab es in den letzten Jahren immer wieder Kettenmails, die vor einem völlig neuartigen Virus warnten, der sich auf der heimischen Festplatte versteckt halte. In der E-Mail wurde auch der Name der Datei genannt, empfohlen sie sofort zu löschen und die Warnung zum Schutz von Freunden möglichst schnell weiterzuverbreiten. In Wirklichkeit handelte es sich dabei meist um Windows-Systemdateien, die man auf keinen Fall löschen sollte.

Da Systemdateien unter Windows (und anderen Betriebsystemen) kryptische Namen tragen und gelegentlich aus unverständlichen Gründen mit absurden Icons versehen sind, ist es entsprechend einfach, beim Benutzer Verunsicherung oder Misstrauen zu wecken. Als gutes Beispiel sei hierfür der *JDBGMGR.EXE*-Hoax von

Mitte 2002 genannt. Diese Datei gehörte zum Umfang des Internet Explorers und war völlig harmlos. Als Icon hatten die Entwickler bei Microsoft einen kleinen Teddybären gewählt. Daher leuchtete es den Empfängern der Falschmeldung ein, dass es sich bei *JDBGMGR.EXE* um den so genannten Teddybär-Virus handeln musste und nicht um eine Systemdatei. Einen solchen Virus hat es jedoch nie gegeben und dass die Benutzer die Datei dennoch löschten, macht diesen Hoax zu einer gelungenen Social Engineering-Attacke.

Spam – Werbe- und Massenmails

Ein weiteres Ärgernis im Internet sind Massen-E-Mails, auch *Spam* genannt. Dabei handelt es sich meistens um Werbemails, generell bezeichnet man mit Spam aber alle E-Mails, die unaufgefordert und in großen Mengen verschickt werden.

Neben dem Argument der unnötig hohen Netzauslastung spricht vor allem die Aufdringlichkeit dieser Art von Werbung gegen das Verschicken von Massenmails. Auch juristisch gesehen ist das »Spammen« (Verschicken von Spam) bedenklich, und die Versender riskieren empfindliche Geld- oder gar Haftstrafen. Zahlreiche Provider versuchen, ihre SMTP-Server vor Spammern zu schützen, trotzdem landet auch in Ihrem Briefkasten wahrscheinlich täglich unerwünschte Post. Der Anteil an Spam liegt in Deutschland Schätzungen zufolge bereits bei über 70%. Spam ist daher zu einem wirklich gewichtigen Faktor geworden, kostet es doch nicht zuletzt viel Zeit und Geld, in der Flut an Müll die wirklich wichtigen E-Mails zu finden. Inzwischen haben zahlreiche Konsortien und Behörden reagiert und Meldezentralen für Spam eingerichtet.

Da man solche Massenmails meist von den immer gleichen Anbietern erhält und auch die Betreffzeilen und Inhalte oft in typischer Weise formuliert sind, lassen sich unerwünschte Mails mit so genannten Spam- oder Junkfiltern relativ gut automatisch herausfiltern. Dazu gibt es verschiedene Ansatzpunkte und natürlich beliebige Kombinationen davon. Eine umfassende Beschreibung der Spamproblematik und mathematischer Verfahren würde ein ganzes Buch füllen, daher wollen wir hier nur einen kurzen Überblick geben.

Grob gesehen können Spamfilter an verschiedenen Punkten ansetzen: Auf dem Mailserver kann ein Filter installiert werden, der jede weiterzuleitende oder zu speichernde E-Mail untersucht und mit eine speziellen Spam-Flag kennzeichnet. Dieses Flag kann beispielsweise eine Zeichenkette in der Form »*****SPAM*****« sein, die in die Betreffzeile einer als unerwünscht eingestuften Mail integriert wird. Ein anderer Ansatz ist es eine komplett neue Mail zu generieren und in dieser die Kriterien zu beschreiben, nach denen die betreffende Mail als Spam klassifiziert wurde, und die eigentliche Mail als Anlage beizufügen. Diese Lösung ist besonders elegant, da der Benutzer anschließend nachvollziehen kann, warum der Filter die Spam-Flag gesetzt hat, und das Flaglevel eigenständig verändern kann. Dazu wird eine bestimmte

Anzahl an Punkten festgelegt, ab der eine Mail als Spam gilt. Eine Betreffzeile, die beispielsweise das Wort »Viagra« enthält, bekommt eine bestimmte Anzahl an Punkten, und die Aufforderung einem Link zu folgen, eine andere Anzahl an Punkten. Je nach Installation ist das Einstellen des Filters entweder dem Administrator vorbehalten oder jeder Benutzer, der über den Server Mails bezieht, kann eigene Konfigurationen vornehmen.

Die Spamanalyse einer solchen Trägermail könnte etwa folgendermaßen aussehen:

```
Content analysis details:  (11.8 points, 5.0 required)

 pts rule name              description
 ---------------------- --------------------------------------------
 1.9 MSGID_SPAM_CAPS        Spam tool Message-Id: (caps variant)
 2.8 MIME_BOUND_DD_DIGITS   Spam tool pattern in MIME boundary
 0.1 HTML_LINK_CLICK_HERE   BODY: HTML link text says "click here"
-0.9 BAYES_30               BODY: Bayesian spam prob. is 30 to 40%
 0.1 HTML_MESSAGE           BODY: HTML included in message
 0.3 MIME_HTML_ONLY         BODY: only has text/html MIME parts
 0.6 MIME_HTML_NO_CHARSET   RAW: Message text in HTML without charset
 1.0 URI_OFFERS             URI: Message has link to company offers
 1.2 HTML_MIME_NO_HTML_TAG HTML-only message, but no HTML tag
 1.9 RCVD_DOUBLE_IP_SPAM    Bulk email fingerprint (double IP) found
 1.1 MIME_HTML_ONLY_MULTI   Multipart message only has text/html MIME
 0.1 MISSING_OUTLOOK_NAME   Message looks like Outlook, but isn't
 1.6 MISSING_MIMEOLE        X-MSMail-Priority, but no X-MimeOLE
 0.1 CLICK_BELOW            Asks you to click below
```

Die Filtergrenze liegt in diesem Beispiel bei 5 Punkten und die eingestufte Mail bekommt mit 11,8 Punkten deutlich mehr. Wie Sie sehen, beziehen sich zahlreiche Prüfregeln auf HTML, was einmal mehr zeigt, dass Sie die HTML-Unterstützung Ihres Mail-Clients am besten ganz deaktivieren und Ihre eigenen E-Mails nur in Klartext (*plain text*) schreiben sollten.

Der zweite Punkt, an dem eine Spamfilterung ansetzen kann, ist die dem Firmennetz vorgeschaltete Sicherheitslösung, die aus Firewall, Antivirensystem und Spamfilter besteht. Da es sich dabei um professionelle Systeme handelt, mit denen Sie als gewöhnlicher Benutzer nicht in Kontakt kommen werden, wollen wir dieses Szenario auf das lokale Sicherheitsystem Ihres Computers übertragen. Die Personal Firewalls und Virenscanner, die wir im weiteren Verlauf dieses Buchs noch kennen lernen werden, verfügen teilweise (z.B. das System von Symantec) über eigene Spamfilter, die sich je nach Lösung in den Mail-Client integrieren oder diesem vorgeschaltet sind. Die Eingriffsmöglichkeiten entsprechen jedoch weit gehend denen, die wir von Filtern auf Mailservern kennen. Der große Unterschied liegt darin, dass die Filterung in diesem Fall auf Ihrem Computer stattfindet.

Der dritte und letzte Ansatzpunkt ist schließlich das Mailprogramm. Hier gibt es zwei Fälle zu unterscheiden. Im ersten Fall arbeitet ein Spamfilter selbstständig im Mailtool und verhält sich wie oben beschrieben. Im zweiten Fall können Sie als

Benutzer eine Spam-Flag manuell setzen. Dazu bietet der Client einen Button oder Menüpunkt an, über den Sie eine bestimmte E-Mail als Spam klassifizieren können. Der integrierte Spamfilter merkt sich diese E-Mail und flaggt automatisch jede weitere identische E-Mail. Das wäre aber immer noch mit sehr viel Arbeit verbunden, da es viele tausend verschiedene Spammails gibt und die Spammer immer neue Formulierungen und Inhalte versenden. Daher sind die Filter intelligent und analysieren die als Spam geflaggte Mail. Die Möglichkeiten, die dem Mail-Client hier zur Verfügung stehen, sind weitaus mächtiger und effizienter als bei den anderen Ansatzpunkten, denn der Filter kann hier gezielt die E-Mails untersuchen, die der betreffende User als Spam erachtet. In der Regel werden hierfür sowohl mit den anderen Filtersystemen vergleichbare Taktiken verwendet als auch Textanalysen und zahlreiche statistische Verfahren. So kann der Filter so genannte Blacklists abfragen,[4] aber auch anhand der vom User markierten Mails Schlussfolgerungen über unerwünschte Mails ziehen. Die Resultate sind in den meisten Fällen so gut, dass es ausreicht, den Filter mit Hilfe von 30-100 Mails zu trainieren, um etwa 95% des Spams automatisch zu filtern. Diese Zahlen unterliegen jedoch je nach Art des Spams und Mailaufkommen erheblichen Schwankungen. Natürlich liegt dies nicht zuletzt an der eingesetzen Filtersoftware.

Wie eingangs erwähnt, benutzen die meisten Systeme eine Kombination zahlreicher Verfahren, und so greifen Spamfilter auf Providerebene ebenfalls auf statistische und heuristische Methoden zurück. Ihnen steht nur schlicht und einfach ein ganz anderes Ausgangsmaterial zur Verfügung, und die Filterung ist daher zwangsläufig schlechter als bei einer Lösung, bei der der Benutzer den Mailfilter zunächst eigenhändig trainiert.

Dennoch führen Spamfilter zu einer ganzen Reihe von Problemen und haben daher bis vor kurzem alle verdächtigen E-Mails markiert, aber niemals eigenständig gelöscht oder geblockt. Dies hat sich leider in den letzten Monaten geändert, und Provider nehmen sich nun zunehmend das Recht heraus, Mails eigenständig abzuweisen. Das hat sich beispielsweise im Fall von AOL als fatal erwiesen, da nun auch zahlreiche Server gefiltert werden, die eine große Anzahl an Mails verschicken, ohne dabei zu spammen. In Online-Communities ist es die Regel, dass Benutzer bestimmte Themen abonnieren können und per E-Mail auf dem Laufenden gehalten werden, wenn sich dort etwas tut (also beispielsweise ein anderer Benutzer eine Nachricht zu einem abonnierten Thema schreibt). Die Server größerer Online-Com-

4 Dabei handelt es sich um Listen, die zentral von Anti-Spam-Konsortien gepflegt werden und sowohl spammende Mailserver als auch die zurzeit im Umlauf befindlichen Spammails enthalten. Solche Blacklists greifen auch auf Serverebene bevorzugt auf Spamfilter zurück. Dies hat zum Teil aber auch negative Folgen. Nicht selten ist es in der Vergangenheit vorgekommen, dass Angreifer Mailserver kleinerer Unternehmen unterminiert und anschließend über diese Spammails verschickt haben. Wurde der Mailserver dann erst einmal in eine Blacklist aufgenommen, wurden alle E-Mails des betroffenen Unternehmens, also auch Geschäftskorrespondenz, nicht mehr weitergeleitet. Es hat sich als sehr schwierig bis hoffnungslos erwiesen, seinen eigenen Server effizient aus allen gängigen Blacklists löschen zu lassen.

munities versenden daher nicht selten tausende E-Mails täglich, bei denen es sich aber keineswegs um Spam handelt. Wenn diese Server bei einigen Providern zu Unrecht auf den Blacklists landen und die Mails daher nicht mehr weitergeleitet werden, ist das für die Community-Betreiber ein wahres Desaster. Darüber hinaus werden beispielsweise AOL-Kunden nicht einmal darüber informiert, wenn Mails an sie vollautomatisch geblockt wurden. Es wäre nicht das erste Mal, dass selbst wichtige Geschäftskorrespondenz so im Nirvana landet. Der versendende Server bekommt vom Provider in der Regel zwar eine E-Mail, in der ihm mitgeteilt wird, dass eine Mail geblockt wurde, keinem Postmaster der Welt ist es aber zuzumuten, unter den tausenden eingehender Fehlermeldungen diejenigen herauszusuchen, die zu unrecht gefiltert wurden, und sie dann per Hand auf anderem Wege an den Empfänger zu leiten. In solchen Fällen hilft es dann nur noch, sich telefonisch mit dem Provider in Verbindung zu setzen. Die meisten großen Provider bieten dazu eine eigene Hotline an, die zum Teil sogar rund um die Uhr verfügbar ist.

Die angesprochenen Blacklists (die meist DNS-Einträge speichern) werden in Zukunft jedoch nur noch eine geringe Rolle spielen, da der größte Teil der unerwünschten E-Mails nicht mehr von offenen oder unterminierten Mailservern verschickt wird, sondern von so genannten *Bots* oder *Zombies*. Dabei handelt es sich um von Angreifern erbeutete Systeme, die anschließend ohne Wissen und Zutun des eigentlichen Benutzers ferngelenkt und zum Beispiel zum Spammen missbraucht werden. Wir werden uns mit diesen Zombies zu einem späteren Zeitpunkt genauer befassen und wollen hier daher nur ein paar Fakten nennen, um das Ausmaß des Problems zu beleuchten.

Schätzungen zufolge sind rund um die Uhr etwa deutlich mehr als 100.000 Zombies online und somit für Spammer verfügbar. Diese Zombies haben dynamische IP-Adressen – daher sind Versender, die über solche Zombienetze spammen, vor Blacklists geschützt.

Einen guten Überblick über die vorhandenen Zombies verschafft der ZombiMeter von CipherTrust unter *http://www.ciphertrust.com/resources/statistics/zombie.php* (siehe Abbildung 6-3). Wie Sie erkennen können, gibt es in Deutschland rund um die Uhr viele tausend Zombies, einer davon könnte auch Ihr heimischer PC sein.

Häufig kommt es vor, dass der Spammer Ihnen in der Werbemail anbietet, Sie aus seinem Adressbuch zu streichen. Dazu sei es nur nötig, eine Mail mit dem Betreff »unsubscribe« an den Anbieter zu mailen. In den meisten Fällen erweist sich das aber als Falle: Der Betreiber versucht mit solchen Aufforderungen nur sicherzustellen, dass die angeschriebene Adresse auch tatsächlich noch benutzt wird. Antworten Sie deshalb generell nicht auf Werbemails. Ein weiterer, gern verwendeter Trick, um den Empfänger von Spam aus der Reserve zu locken, besteht darin, ihm eine Mitgliedsbestätigung zu schicken. Darin steht beispielsweise, dass Sie sich angeblich als Mitglied eines Webclubs oder einer Shoppingsite angemeldet haben. Sollte es sich dabei jedoch um einen Fehler handeln, mögen Sie sich bitte per E-Mail an

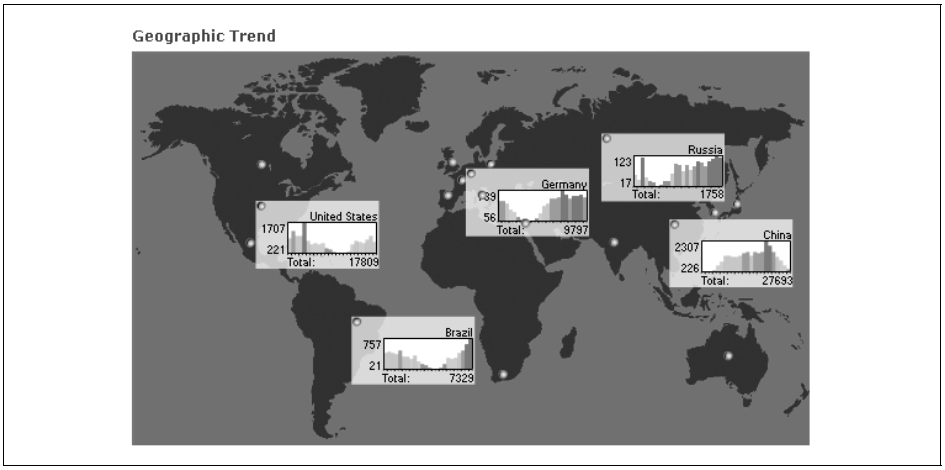

Abbildung 6-3: Der ZombiMeter von CipherTrust

den Anbieter wenden. Auch hier geht es meist um nichts anderes, als herauszufinden, ob die Mailadresse noch benutzt wird; daher sollten Sie auch hier auf eine Antwort verzichten.

Spamfilter im Mail-Client

Die in den Mail-Client integrierten Spamfilter sind alle mehr oder weniger ähnlich zu bedienen, daher wollen wir uns stellvertretend hier Thunderbird anschauen. Abbildung 6-4 zeigt den Trash-Ordner des Mailtools, in dem sich jede Menge als Spam gekennzeichnete Nachrichten befinden. Zu erkennen ist das an dem Papierkorb-Icon (*Spam-Flag*), das in jeder Zeile zu finden ist. Für jede einzelne erhaltene Mail kann man dieses Spam-Flag per Mausklick an- und wieder ausschalten und auf diese Weise die eingehenden Nachrichten filtern. Wählen Sie jedoch das Spam-Flag mit Bedacht: Markieren Sie beispielsweise eine Nachricht als Spam, die keine ist, wird Thunderbird eine ähnliche E-Mail in Zukunft automatisch wieder mit dem Papierkorb-Icon markieren.

Häufig liest man Anleitungen dazu, wie man als Spam markierte Nachrichten automatisch in den Papierkorb verfrachten kann. Seitdem mir auf diese Weise die E-Mail eines Reiseveranstalters über eine Änderung beim Abflugtermin abhanden gekommen ist, rate ich dringend davon ab. Ich hatte Monate zuvor den wöchentlichen Newsletter der Fluggesellschaft mehrfach genervt als Spam markiert, woraufhin Thunderbird auch wichtige Mails des Anbieters direkt in den virtuellen Papierkorb verschob. Es ist daher die bessere Lösung, den Spam zunächst in der Inbox zu lassen und dann im Schnelldurchlauf all das per Hand zu löschen, was unwichtig erscheint. Die Lösung, den Papierkorb regelmäßig nach fälschlich einsortierten Nachrichten zu durchsuchen, ist hingegen wenig ratsam, wenn es Ihnen – wie mir – an der Disziplin mangelt, dies nach jedem Mailabruf aufs Neue zu tun.

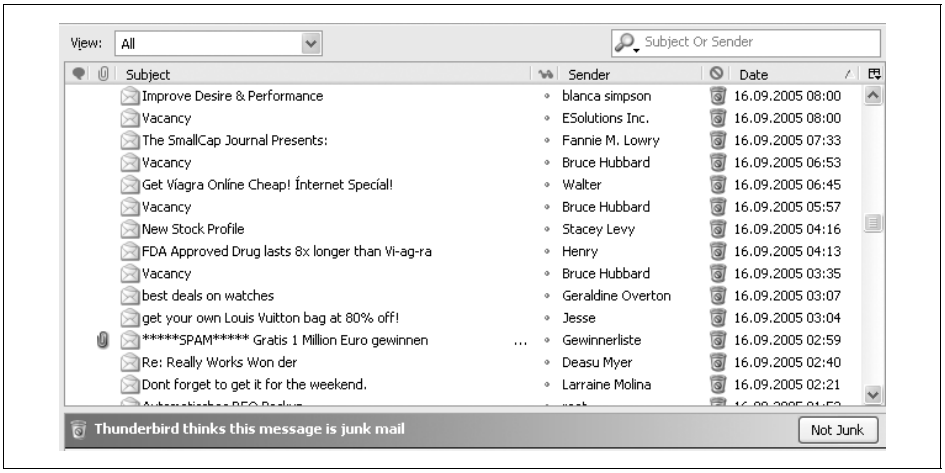

Abbildung 6-4: Spam-Flag in Thunderbird

E-Mail-Maulwürfe

In zunehmendem Maß gewinnen im Internet Kundendaten an Bedeutung. Im Gegensatz zur Bargeldzahlung im Geschäft hinterlassen Sie beim Online-Shopping immer einige Spuren, die Informationen über Sie preisgeben, so dass sich mittlerweile nahezu alle größeren Anbieter näher mit der Analyse dieser Daten beschäftigen.

Eine immer noch wenig bekannte Variante zur Datengewinnung stellen die so genannten E-Mail-Maulwürfe (*moles*) dar. Dabei handelt es sich auf den ersten Blick um gewöhnliche E-Mails, die Ihnen von den Betreibern eines Online-Shops zugeschickt werden. In der Nachricht ist aber ein Verweis auf eine nur einen Bildpunkt (Pixel) große Grafik enthalten. Der Trick dahinter ist ebenso einfach wie clever: Beim Öffnen der E-Mail fordert Ihr Mail-Client die Datei vom Server an und stellt damit eine Verbindung zu ihm her. Somit gelangt der Anbieter an Ihre zurzeit gültige IP-Adresse sowie an den Namen und die Version des von Ihnen benutzten Mail-Programms. Das mag auf den ersten Blick noch nicht so problematisch erscheinen, jedoch können bereits aus diesen Daten mehrere wichtige Erkenntnisse gezogen werden: So kann der Anbieter beispielsweise die Zeit zwischen dem Verschicken der E-Mail und dem Lesen ermitteln und auf diese Weise feststellen, wie häufig ein Mail-Account genutzt wird. Außerdem kann er den Inhalt der Mail so formulieren, dass Sie als Leser zum Weiterleiten der Nachricht an Ihre Bekannten oder Kollegen angeregt werden. Öffnen diese die Nachricht, erhält der Anbieter neben ihren Mail- und IP-Adressen auch eine Vorstellung darüber, für welche Produkte Sie sich interessieren – denn sonst hätten Sie die Mail wohl nicht weitergeleitet. Anhand der IP-Adresse kann zudem in den meisten Fällen Ihr Provider und damit oft auch der Wohnort ermittelt werden (besonders wenn der Provider nur eine Region oder Stadt betreut).

Die Möglichkeiten moderner Moles gehen aber noch weiter. So ist es beispielsweise möglich, alle auf Ihrer Festplatte gespeicherten Cookies auszulesen, die bei einem früheren Besuch des Online-Shops gesetzt wurden. Damit wird es erstmals möglich, eine Verbindung zwischen Ihnen als Surfer und als E-Mail-Nutzer herzustellen. Beim nächsten Besuch des Online-Shops kann der Anbieter Sie nicht mehr nur anhand der Cookies identifizieren, sondern dem aktuellen Surfverhalten auch eine E-Mail-Adresse zuordnen. Wenn Sie dann beispielsweise eine bestimmte Musik-CD auf der Seite des Anbieters angeschaut haben, brauchen Sie in Zukunft nicht überrascht zu sein, wenn Sie kurz darauf über Neuerscheinungen desselben Interpreten informiert werden. Abhilfe schafft hier leider nur ein nicht HTML-fähiger Mail-Client oder in einigen Fällen der Einsatz von Firewall-Software, wie wir sie im Kapitel 12, *Firewalls und erweiterte Sicherheitssysteme*, kennen lernen werden.

Einen interessanten Test zum Thema Moles finden Sie unter *http://www.mackraz.com/trickybit/readreceipt/*. Von hier aus können Sie sich einen Maulwurf schicken lassen und erfahren dann durch eine zweite Mail, welche Informationen der Betreiber der Seite über Sie sammeln konnte.

Webmail

Mit *Webmail* bezeichnet man die kostenlosen bzw. in Teilen kostenpflichtigen E-Mail-Dienste im Internet. In puncto Qualität und Umfang der gebotenen Leistungen unterscheiden sich die einzelnen Anbieter zum Teil erheblich voneinander. Für den deutschsprachigen Raum scheint sich *web.de* derzeit als interessantester Anbieter herauszukristallisieren.

Interessant sind für uns die sicherheitsrelevanten Aspekte solcher Webmail-Accounts. Als Vorteil ist allen Anbietern gemein, dass die Anmeldung meist »anonym« erfolgt, d.h., dass entweder gar keine persönlichen Daten abgefragt werden oder der Anbieter die Richtigkeit der Einträge nicht kontrolliert (zumindest verspricht er, sie nicht weiter zu benutzen). Die Anonymität hat zwar auch negative Aspekte, es kann aber von Vorteil sein, einen Mail-Account zu unterhalten, der nicht direkt auf den eigenen Namen schließen lässt. Der zweite, größere Vorteil dieser Art von Accounts liegt in der Resistenz gegen die meisten E-Mail-Würmer. *I LOVE YOU* und andere skriptbasierte Viren und Würmer können auf den Webmail-Accounts keinen Schaden anrichten, da sie ja meist auf einen bestimmten Mail-Client spezialisiert sind.[5]

5 Früher nannte man als weiteren Vorteil die Ausfallsicherheit und die Backup-Möglichkeiten des Anbieters. Inzwischen wissen wir aber durch etliche Pannen, dass E-Mails oder sogar ganze Accounts verloren gehen können. Der größte bekannt gewordene Ausfall ereignete sich beim Anbieter GMX, als Mitte 2000 einige tausend Nachrichten für immer im Datennirvana verschwanden.

Problematisch an Webmail-Accounts hingegen ist, dass der Anbieter die Sicherheit der Kennwörter nicht überprüft und jedes noch so unsinnige Passwort mit mehr als vier oder sechs Zeichen Länge akzeptiert. Inzwischen achten einige Anbieter immerhin darauf, dass Kennwort und Benutzername nicht identisch sind, doch dies ist natürlich noch zu wenig. Denn oft wählen arglose Nutzer Passwörter, die sich auf Anhieb erraten lassen. Besonders beliebt ist dabei das Rückwärtsschreiben des Benutzernamens oder das Wort »Passwort« oder »qwert«. Aus diesem Grund gelingt es Crackern immer wieder problemlos, in fremde Webmail-Accounts einzudringen und diese für eigene Mailings zu missbrauchen.

Im Vergleich zu Mail-Clients ist es extrem einfach für Angreifer, E-Mails auf einem Webmail-Account mitzulesen und zu kopieren. Das ist sogar automatisch mit Hilfe von Skripten möglich, so dass noch nicht einmal (z.B. über einen Trojaner) zusätzliche Software installiert werden muss. Sie reduzieren dieses Risiko, indem Sie das Angebot Ihres Webmail-Betreibers nutzen, E-Mails mittels POP auf einen gewöhnlichen Mail-Client herunterzuladen und dort zu archivieren. Allerdings gilt es hier zu bedenken, dass Sie sich gegebenenfalls auf diese Weise Viren direkt auf Ihr System laden. Sie sollten deshalb unbedingt mit einem aktuellen Virenscanner und am besten zusätzlich noch mit einer Firewall arbeiten.

Auch die freie Wahl der Benutzerkennung kann im Hinblick auf Webmail-Accounts ihre Nachteile haben. Da mit Hilfe der Kennung die E-Mail-Adresse bestimmt wird, kann ein Angreifer versuchen, Sie mittels eines geschickt gewählten Namens in die Irre zu führen. Er könnte beispielsweise eine Adresse erzeugen, die aus dem Vor- und Nachnamen eines Ihrer Bekannten besteht, und Ihnen eine E-Mail schicken, um auf diese Weise persönliche Informationen von Ihnen zu erhalten. Bedenken Sie daher, dass solche Freemail-Adressen nur bedingt als vertrauenswürdig angesehen werden können.

Zahlreiche Anbieter haben mittlerweile Virenscanner und Spamfilter in ihre Angebote integriert. In vielen Fällen kosten diese und weitere Extras einen geringen monatlichen Aufpreis, der sich jedoch meistens als lohnenswerte Investition erweist.

Verschlüsselung mit GnuPG und PGP

Zum Abschluss dieses Kapitels betrachten wir die beiden Verschlüsselungsprogramme *GNU Privacy Guard (GnuPG)* und *Pretty Good Privacy* (*PGP*), mit denen Sie Daten wie E-Mails ver- und entschlüsseln und darüber hinaus elektronische Signaturen erzeugen und prüfen können. Da sich sowohl die Lizenzpolitik als auch die Transparenz von PGP im Laufe der letzten Jahre zum Negativen entwickelt haben und die aktuelle Version 9.0 nicht mehr als Freeware vertrieben wird, beschreibt dieser Abschnitt die freie und weit verbreitete Software GnuPG. Sie ist kompatibel zu PGP und beruht auf dem gleichen Prinzip, so dass Sie die folgende Anleitung fast

eins zu eins für PGP übernehmen können, falls Sie sich für diese Software entscheiden.

Zunächst wollen wir das von GnuPG und PGP angewandte Verschlüsselungsverfahren genauer unter die Lupe nehmen.

Asymmetrische Verschlüsselung

GnuPG verwendet ein asymmetrisches Verschlüsselungsverfahren. Im Gegensatz zu symmetrischen Verfahren, bei denen derselbe Schlüssel sowohl für das Verschlüsseln als auch für das Entschlüsseln benutzt wird, gibt es beim asymmetrischen Verfahren zwei unterschiedliche Schlüssel.

Bei der Installation beziehungsweise ersten Inbetriebnahme von GnuPG werden diese beiden Schlüssel automatisch generiert. Dabei handelt es sich um einen so genannten »privaten« Schlüssel (*Private Key*) und einen »öffentlichen« (*Public Key*). Bei der Erstellung des ersten müssen Sie eine Passphrase eingeben. Bei dieser Passphrase handelt es sich um einen beliebigen Satz, den Sie später zum Signieren oder Entschlüsseln von Nachrichten immer wieder eingeben müssen. Es ist wichtig, dass Sie sich diesen Satz einprägen und nirgendwo aufschreiben, da von diesem das gesamte Sicherheitskonzept von GnuPG abhängt. Sollte er dennoch in fremde Hände geraten, müssen Sie schnellstmöglich einen neuen Schlüssel generieren und Ihren Bekannten mitteilen, dass der alte Schlüssel ungültig ist (dazu bieten sich so genannte Rückzugszertifikate oder Widerrufschlüssel an).

Schauen wir uns zunächst die Aufgabe Ihres Public Key genauer an: Diesen Schlüssel müssen Sie Ihren Bekannten mitteilen, damit diese die an Sie gerichteten Mails verschlüsseln können. Sie können den Schlüssel entweder per E-Mail verschicken, in einer Datei per Diskette transportieren oder an einen der zentralen Keyserver im Internet schicken. Diese Servern sind vergleichbar mit Telefonbüchern, nur dass dort anstatt der Telefonnummern öffentliche GnuPG-Schlüssel zu finden sind. Kennen Sie den Public Key eines Bekannten nicht, können Sie eine Suchanfrage an den Server stellen. Wenn dieser über die entsprechenden Daten verfügt, können diese direkt in Ihr GnuPG-Adressbuch importiert werden.

Sie fragen sich vielleicht, ob es nicht gefährlich, seinen Schlüssel öffentlich zur Verfügung zu stellen. Das Gegenteil ist der Fall, denn darauf beruht ja gerade das Sicherheitskonzept von GnuPG. Mit dem Public Key werden Nachrichten vom Absender verschlüsselt. Für die anschließende Entschlüsselung benötigen Sie als Empfänger Ihren Private Key. Beide Schlüssel bilden zusammen also ein Paar. Möchte Ihnen ein Arbeitskollege beispielsweise eine kodierte E-Mail zuschicken, benötigt er dazu Ihren öffentlichen Schlüssel, mit dem GnuPG die Nachricht verschlüsselt. Da zu jedem öffentlichen Schlüssel genau ein privater Schlüssel passt, sind nur Sie in der Lage, die E-Mail wieder zu entschlüsseln.

Zwar ist es theoretisch möglich, eine so kodierte Nachricht auch ohne den Private Key lesbar zu machen, die dafür nötigen Rechenkapazitäten sind jedoch enorm und überschreiten, will man die Rechendauer realistisch halten, selbst die Grenzen modernster Supercomputer.[6] In der Praxis können Sie also davon ausgehen, dass die transportierten Inhalte sogar vor der Einsicht des Staates sicher sind. Gerade deswegen wird in den entsprechenden Gremien diskutiert (allen voran in den US-amerikanischen), ob der Regierung nicht ein *Master Key* zur Verfügung gestellt werden müsste, um kodierte Nachrichten »notfalls« entschlüsseln zu können. In einigen Ländern sind beispielsweise nur sehr kurze und daher leicht zu knackende Schlüssel erlaubt. Als Beispiel für die amerikanischen Bemühungen zur E-Mail-Überwachung und -Entschlüsselung sei hier das heftig umstrittene Mailfiltersystem *Carnivore* des FBI genannt. Dieses wird wahrscheinlich seit dem 11.9.2001 in unbekanntem Umfang eingesetzt und ist nicht zuletzt deshalb umstritten, weil es – da das Internet keine Landesgrenzen kennt – auch E-Mails außerhalb der Vereinigten Staaten filtern und auswerten kann. Innerhalb der USA ist der Einsatz durch den *USA Patriot Act* von 2001 gedeckt.[7]

Selbst in Anbetracht der Tatsache, dass die Rechenleistung der PC-Systeme rasant zunimmt, müssen Sie sich vorerst keine Sorgen um die Sicherheit der Verschlüsselungstechnik an sich machen, denn mit GnuPG kann man sogar bis zu 4.096 Bit lange Schlüssel generieren. Beim derzeitigen Stand der Technik reichen Schlüssel mit einer Länge von 2.048 Bit jedoch völlig aus, um eine Nachricht sicher zu verschlüsseln.

Wie verhält es sich nun mit dem privaten Schlüssel? Dieser ist nur für Sie bestimmt und darf daher nicht weitergegeben werden. Er dient zur Entschlüsselung von Nachrichten, doch der private Schlüssel allein reicht noch nicht aus, um eine kodierte E-Mail wieder lesbar zu machen. Zusätzlich müssen Sie vor jeder Entschlüsselung noch Ihre Passphrase eingeben. Diese dient als zusätzliche Absicherung für den Fall, dass jemand in den Besitz Ihres privaten Schlüssels gekommen sein sollte.[8] Wie der Begriff »Phrase« schon andeutet, handelt es sich dabei nicht um ein einzelnes Wort, sondern um einen ganzen Satz. Beim Generieren der Phrase gelten prinzipiell die Tipps aus Kapitel 3, *Sicherheitsbewusstsein*. Generell sollte eine Passphrase nicht kürzer als neun Zeichen sein.

6 Zweifelsohne lässt sich jedoch jede verschlüsselte Nachricht knacken, die Frage ist nur, ob ein Betreiber eines Hochleistungsrechners dafür, je nach Schlüssellänge, einige Jahre oder Jahrzenhte opfern möchte. Ein Schlüssel mit einer Länge, die derzeit als sicher gilt, mag aber in einigen Jahren durchaus in realistischer Zeit zu knacken sein.

7 Gerüchten zufolge soll sich dies Werkzeug jedoch als nicht effektiv und unrentabel erwiesen haben, weshalb es wahrscheinlich nur noch eines unter mehreren benutzten Überwachungstools ist.

8 Trotz dieser Sicherheitsmaßnahme sollte man sehr sorgsam mit dem Schlüssel umgehen, denn im Gegensatz zu einer EC-Karte oder einem Online-Banking-Passwort hat ein Angreifer unendlich viele Versuche frei, um die Passphrase zu erraten, wenn er den Schlüssel erbeutet hat.

Man kann mit dem Private Key auch Nachrichten signieren. Dazu bildet GnuPG aus dem geschriebenen Klartext und dem Schlüssel eine Art Quersumme und hängt diese am Ende der E-Mail an. Mit dem dazu passenden öffentlichen Schlüssel kann der Empfänger der Nachricht nicht nur überprüfen, ob die Mail tatsächlich von Ihnen stammt, sondern auch, ob sie während des Transports verändert wurde. Es ist daher wichtig, nach dem Signieren der E-Mail keine Änderungen mehr am Text vorzunehmen. Bereits ein Leerzeichen oder ein Zeilenumbruch reichen aus, um die Signatur ungültig zu machen. Wissenschaftler suchen seit vielen Jahren Verfahren, mit denen man durch gezieltes Umformatieren eine geänderte Nachricht erzeugen kann, die jedoch die gleiche Signatur trägt. Würde dies einem Angreifer gelingen, könnte er im Nachhinein digital signierte Geschäftsunterlagen manipulieren und beispielsweise Kaufverträge zu seinen Gunsten ändern. Trotz einiger Fortschritte gilt dies bisher (und vermutlich auch in naher Zukunft) als unmöglich.[9]

GnuPG und die Thunderbird-Erweiterung Enigmail

GnuPG basiert auf dem OpenPGP-Standard und ist für sich genommen ein mächtiges, aber äußerst unkomfortables Tool.[10] Daher werden wir uns einer grafischen Oberfläche bedienen, um besser mit damit arbeiten zu können. Als Beispiel für die Verwaltung von Schlüsseln und das eigentliche Verschlüsseln von Nachrichten soll uns hier die Erweiterung *Enigmail OpenPGP* für Thunderbird dienen. Falls Sie hingegen Outlook Express oder Eudora als E-Mail-Client nutzen, empfiehlt es sich, die Erweiterung WinPT zu nutzen, die Sie unter *http://www.winpt.org* downloaden können. Die Bedienung entspricht in etwa der hier dargestellten Kombination von Thunderbird und Enigmail.

Da E-Mails, die von Ihnen verschlüsselt werden, an ihrem Zielort auch wieder entschlüsselt werden müssen, ist es natürlich notwendig, dass beide Kommunikationspartner GnuPG bzw. PGP auf ihrem Rechner installiert haben. Die Schritte, die nun beschrieben werden, müssen also auch Ihre künftigen Adressaten durchführen, mit denen Sie verschlüsselte E-Mails austauschen möchten.

Kommen wir nun zum Einsatz von Enigmail unter Thunderbird. Wir gehen davon aus, dass Sie GnuPG bereits heruntergeladen und installiert haben. Eine Konfiguration ist nicht nötig, sondern erfolgt direkt über die Enigmail-Erweiterung. Als Erstes müssen Sie die Erweiterung von einer seriösen Quelle wie der Mozilla-Update-Seite oder *http://www.thunderbird-mail.de/erweitern/erweiterungen/enigmail/* herunterladen.

---

9 Im August 2005 ist es gelungen, den Aufwand zur Kollisionsberechnung bei SHA-1 (dem Algorithmus, der auch für OpenPGP benutzt wird) von 2^{80} auf 2^{63} zu verkürzen. Mit diesen Kollisionen ist jedoch das Erzeugen einer beliebigen Nachricht mit gleicher Signatur gemeint. Dies hilft einem Angreifer jedoch nicht, da die falsche Nachricht ja eine sinnvolle und keine wirre Aneinanderreihung von Zeichen sein darf. Zudem ist selbst die genannte Zahl von 2^{63} Möglichkeiten weit außerhalb des heutzutage Machbaren.

10 Linux- und Windowsversionen finden Sie unter *http://www.gnupg.org/*.

Wählen Sie dann in Thunderbird das Menü EXTRAS → ERWEITERUNGEN... In dem aufspringenden Fenster klicken Sie auf den Button INSTALLIEREN (siehe Abbildung 6-5) und wählen das gespeicherte Enigmail aus. Starten Sie nun Thunderbird neu, und es erscheint ein zusätzliches Menü mit dem Namen der Erweiterung. Zudem wird die Icon-Leiste um das Icon VER-/ENTSCHLÜSSELN ergänzt. Bevor es losgehen kann, müssen Sie Enigmail noch über das Menü ENIGMAIL → EINSTELLUNGEN... auf dem Reiter ALLGEMEIN mitteilen, wo sich GnuPG auf Ihrer Festplatte befindet (»Pfad zur GnuPG-Anwendung«).

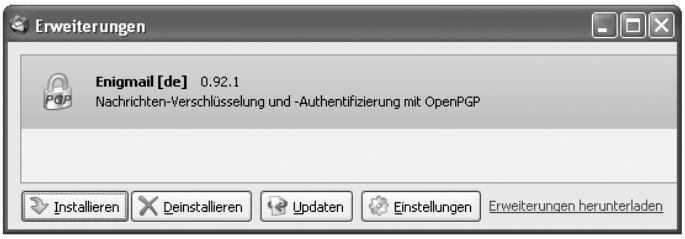

Abbildung 6-5: Das Dialogfenster Erweiterungen in Thunderbird

Klicken Sie nach dem Schreiben einer neuen E-Mail zum ersten Mal auf das Verschlüsseln-Icon oder das Schlüsselsymbol unten rechts, meldet sich Enigmail mit dem Hinweis, dass noch kein Schlüsselpaar vorliegt. Dieses können Sie anschließend mit wenigen Mausklicks unter Angabe der eigenen E-Mail-Adresse und einer Passphrase anlegen. Zudem werden Sie aufgefordert, für den Notfall einen Widerrufsschlüssel zu generieren. Weitere Schlüssel (z.B. für andere Mailkonten) können Sie zu einem späteren Zeitpunkt im Enigmail-Menü in der OpenPGP-Schlüsselverwaltung (und dort unter dem Eintrag ERZEUGEN) anlegen. Abbildung 6-6 zeigt das entsprechende Fenster, in dem neben der E-Mail-Adresse und der Passphrase auch Laufzeit und Länge des Schlüssels festgelegt werden

Danach kann es schon losgehen. Verschlüsseln Sie die eben geschriebene Nachricht und schicken Sie sie als Test an die eigene E-Mail-Adresse. Wenn Sie die Nachricht nun abrufen, erscheint sie bereits automatisch entschlüsselt (mitsamt einem Schlüsselsymbol) in Ihrem Mail-Client (siehe Abbildung 6-7).

Um zu sehen, wie die Nachricht ohne die Passphrase, also zum Beispiel für Dritte aussieht, wählen sie im Menü ENIGMAIL den Eintrag PASSPHRASE AUS CACHE LÖSCHEN aus. Wenn Sie die Nachricht nun erneut öffnen, sehen Sie statt einer lesbaren Botschaft nur Zeichensalat samt der Information, dass es sich dabei um eine verschlüsselte Mail handelt (siehe Abbildung 6-8).

Wie Sie sehen, bietet Ihnen Enigmail an, den Schlüssel für eine gewisse Zeit zwischenzuspeichern. Das ist praktisch, da es sehr lästig wäre, wenn man bei jeder Mail von Neuem manuell die lange Passphrase eingeben müsste, was auf Dauer die Nutzer dazu animieren würde, zu kurze und einfache Phrasen zu benutzen. Denken Sie

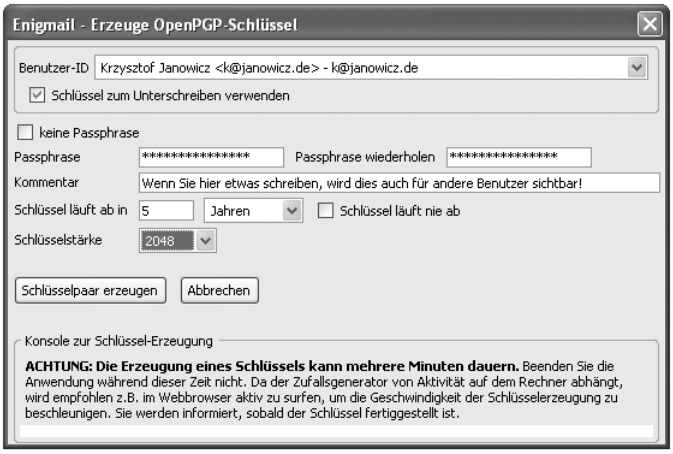

Abbildung 6-6: Schlüssel erzeugen mit Enigmail

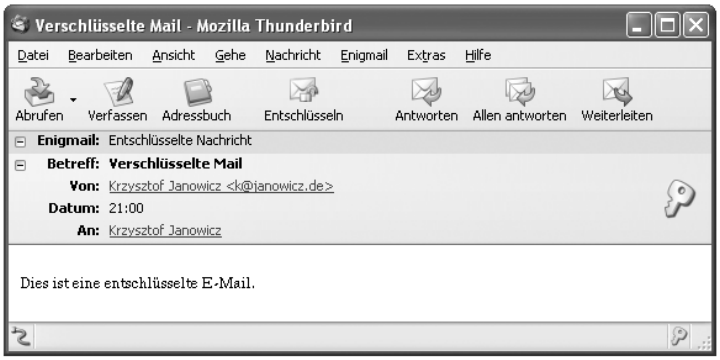

Abbildung 6-7: Eine entschlüsselte E-Mail in Thunderbird

jedoch unbedingt daran, den Cache zu leeren, bevor Sie Ihren Arbeitsplatz verlassen.

Zu guter Letzt werfen wir noch einen Blick auf die Veröffentlichung und Suche von Schlüsseln. Zum einen müssen Sie Ihren öffentlichen Schlüssel publik machen, damit andere Benutzer Ihnen überhaupt verschlüsselte Nachrichten schicken können, zum anderen möchten Sie wahrscheinlich die Schlüssel Ihrer Kollegen oder Bekannten nicht von Hand importieren, sondern bequem von einem Schlüsselserver laden. Dazu dient in Enigmail die bereits genannte OpenPGP-Schlüsselverwaltung. Wie Sie in Abbildung 6-9 sehen, kann man dort über das Menü SCHLÜSSEL-SERVER eigene Schlüssel hochladen oder nach anderen Schlüsseln suchen und diese importieren.

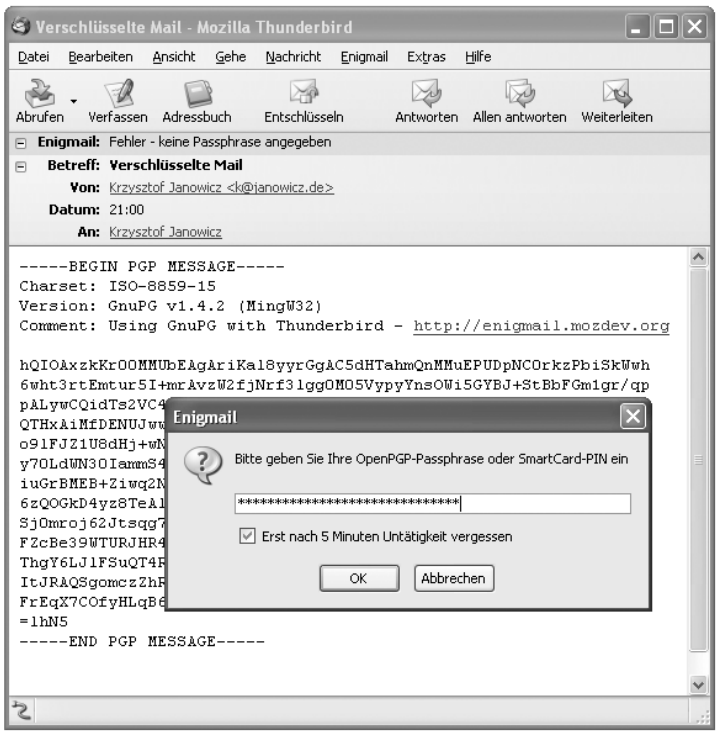

Abbildung 6-8: Eine verschlüsselte E-Mail in Thunderbird

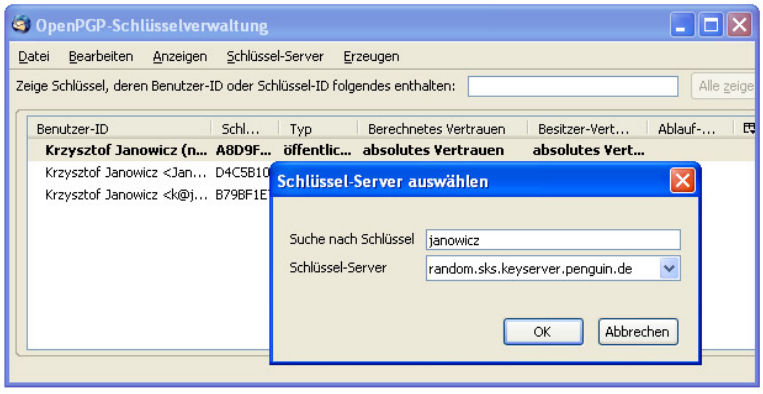

Abbildung 6-9: Schlüssel suchen und hochladen

Sicherheitshinweise

Wie bereits in früheren Kapiteln beschrieben, ist beim Einsatz von Programmen auch immer auf ihre Vorgeschichte im Hinblick auf Sicherheitslöcher zu achten. Gerade bei solch komplexen und multifunktionalen Tools wie Pretty Good Privacy und GnuPG ist dies besonders wichtig, um potenziell vorhandene Fehler der Software einschätzen zu können.

Von früheren PGP-Versionen sind zum Beispiel einige schwere Sicherheitslücken bekannt. Die aktuelle Version scheint aber frei von gröberen Schnitzern zu sein. Dennoch sollten Sie darauf achten, regelmäßig im Internet nach neuen Versionen Ausschau zu halten und sich über mögliche Fehler (*Bugs*) zu informieren. Besonders wichtig ist auch hier, dass Sie GnuPG und PGP nur von vertrauenswürdigen Seiten herunterladen. Ein manipuliertes GnuPG könnte immensen Schaden verursachen, da das Programm für viele sicherheitsrelevante Aufgaben benutzt wird.

Nicht unerwähnt bleiben sollen zwei schwere Bugs, die vor einigen Jahren für großes Aufsehen sorgten. Dabei handelt es sich um den so genannten »Klima-Rosa-Angriff« im März 2001 und die »ASCII Armor Parser Vulnerability«. Beim ersten dieser Angriffsszenarien, das von den tschechischen Kryptologen Vlastimil Klima und Tomas Rosa geplant und durchgeführt wurde, gelang es den Angreifern nach der geringfügigen Modifikation der privaten Schlüsseldatei des Opfers, mittels eines Programms aus der PGP-Signatur den Private Key der Zielperson zu errechnen. Auf diese Weise war es möglich, gefälschte Nachrichten mit dem privaten Schlüssel des Opfers authentisch zu verschlüsseln oder zu signieren. Voraussetzung für den Angriff ist allerdings der physische Zugriff auf den Rechner des Opfers. Die »ASCII Armor Parser Vulnerability« hingegen ist eine Schwachstelle des Windows-Betriebssystems. Der Angreifer maskiert hierbei beispielsweise ein Trojanisches Pferd als verschlüsselte E-Mail. Wenn PGP diese Datei entschlüsseln, also den Klartextinhalt generieren will, erzeugt es stattdessen den »entschlüsselten« Trojaner in Form einer *.dll*-Datei,[11] die dann z. B. beim nächsten Versuch, eine PGP-Datei zu entschlüsseln, geladen wird und das Betriebssystem kompromittiert. Eine genaue Erläuterung dieser Schwachstelle finden Sie unter *http://www.atstake.com/research/advisories/2001/a040901-1.txt*.

Auch GnuPG hat keine völlig saubere Weste: 2003 wurde eine Sicherheitslücke bekannt, durch die mit GnuPG erzeugte ElGamal-Schlüssel kompromittierbar wurden. Diese Art von Schlüsseln stand jedoch nur im so genannten Expertenmodus zur Verfügung.

Abgesehen von diesen implementierungsspezifischen Sicherheitslücken, die in jeder Software vorkommen, haben GnuPG und PGP aber auch designbedingte Schwach-

11 *.dll*-Dateien (*Dynamic Link Libraries*) sind Windows-Betriebssystemdateien, die einzelne Routinen enthalten und jeweils nur bei Bedarf geladen und ausgeführt werden.

stellen. Wie Sie anhand der sehr einfachen Suchmaske des Schlüsselmanagers erkennen können, ist nur die Suche per Schlüssel oder Teilen der E-Mail Adresse möglich. Wenn Sie nun bei der Eingabe des Suchwortes »Janowicz« auf die E-Mail-Adresse *Krzysztof.Janowicz@gmx.de* stoßen, den Schlüssel herunterladen und eine mit ihm verschlüsselte E-Mail mit wichtigen Daten an mich schicken würden, wären Sie der bekanntesten Designschwäche auf den Leim gegangen. Eine solche GMX-Adresse mag es zwar geben, und eine durchtriebene Person mag sogar einen Schlüssel dafür erzeugt und hochgeladen haben, sie gehört jedoch nicht zu meinen Mail-Accounts. Daher würde Ihre Nachricht in falsche Hände geraten. Nun werden Sie anmerken, dass Sie so wichtige Mails sicherlich nur an die Ihnen bereits bekannten E-Mail-Adressen schicken, doch auch dies löst das Problem nur teilweise. Genauso gut könnte ein Angreifer einen Schlüssel zu Ihrer echten E-Mail-Adresse generieren und hochladen. Wenn Ihnen nun jemand eine verschlüsselte Nachricht schicken möchte (und nicht weiß, dass Sie nie einen Schlüssel angefertigt haben), wird er den Schlüssel finden und ihn benutzen. Anschließend werden Sie (je nach Geschick des Angreifers) entweder eine für Sie unlesbare E-Mail erhalten oder gar keine. Dazu muss der Cracker jedoch im Besitz Ihrer Account-Daten, Ihres Systems (beispielsweise durch einen Trojaner) oder des benutzten Mailservers sein. Er fungiert dann quasi als Man-in-the-Middle und kann als einziger die Nachricht entschlüsseln.

Web of Trust

Um solchen Szenarien vorzubeugen, hat sich die Idee des *Web of Trust* (»Vertrauensnetzwerk«) etabliert. Mit den Optionen VERTRAUENSWÜRDIGKEIT FESTLEGEN... und UNTERSCHREIBEN... im Menü BEARBEITEN der Schlüsselverwaltung können Sie in Enigmail bzw. WinPT einstellen, zu welchem Grad Sie einem bestimmten Schlüssel vertrauen und vor allen Dingen die Schlüssel Ihrer Kollegen mit Ihrem eigenen Schlüssel unterschreiben. Dazu geben Sie zusätzlich an, wie detailliert Sie die Echtheit des fremden Schlüssels geprüft haben, und signieren diese Aussage mit Ihrem eigenen Schlüssel. Diese Unterschrift wird nun wiederum öffentlich gemacht, so dass es für Dritte ersichtlich ist, welcher Benutzer welchem Schlüssel traut. Auf diese Art und Weise entsteht ein Netzwerk von gegenseitigen Vertrauensbeziehungen. Wenn Sie einen Schlüssel nur unterschreiben, nachdem Sie wirklich sichergestellt haben, dass es der echte Schlüssel Ihres Kollegen oder Bekannten ist, bewirkt das – wenn es alle so machen – ein hohes Maß an Sicherheit. Selbst wenn der Angreifer seinen gefälschten Schlüssel unterschreibt, bleibt dennoch sichtbar, dass der Schlüssel von einer Ihnen nicht bekannten Person unterschrieben wurde, der Sie selber wenig trauen.

Durch jeden weiteren GnuPG-/PGP-Benutzer, der seinen öffentlichen Schlüssel auf einen Schlüssel-Server lädt, steigt die Akzeptanz und vor allem auch die Möglichkeit der flächendeckenden Nutzung der Kryptographie. Für die Wahrung der Privatsphäre ist es daher wichtig, dass Tools wie GnuPG oder PGP nicht nur von einem Kreis eingeweihter Spezialisten genutzt werden.