KAPITEL 1

Einführung

9,5 Millionen Dollar aus der Elfenbeinküste herausschaffen, gegen eine kleine Provision? 20.000 Paar Schuhe kaufen? Eine E-Card von Shelly? (Wer ist überhaupt Shelly?) 600 kg Gold aus Ghana herausbringen, natürlich auch gegen Provision? Jemand liebt mich mehr als alle Sterne und packt zum Beweis eine ZIP-Datei bei? Probleme im Schlafzimmer? Die Bank in Madrid braucht meine Zugangsdaten, um mein Konto zu schützen? Reklame im Internet schalten?

Dies sind einige der Geschäftsvorschläge, die den Autoren per E-Mail angetragen wurden, während sie dieses Kapitel schrieben. Natürlich sind es nicht alle, sondern nur die, die sie automatisch in den Ordner mit den interessantesten Geschäftsideen (*$HOME/Maildir/.spam*) einsortieren ließen. Die Aufzeichnungen zeigen, dass rund 500 weitere Geschäftsvorschläge vom Mailserver gleich wegen Implausibilität verworfen worden waren. Man kann sich schließlich nicht für jeden Zeit nehmen.

Ähnlich geht es vielen E-Mail-Anwendern. Jede zweite E-Mail im Internet ist Spam oder ein Virus! Dieses Buch handelt davon, wie man sie erkennt und aussortiert und sich wieder den realistischen Geschäften widmen kann.

Systemadministratoren kommt im Kampf gegen Spam und Viren eine Schlüsselrolle zu. Es liegt in ihrer Verantwortung, ihren Nutzern das Medium E-Mail als verlässliches und sicheres Medium zur Verfügung zu stellen. Sie müssen die Nutzer vor schädlichen Sendungen schützen, Hardware und Software gegen Angriffe absichern und dafür sorgen, dass E-Mails trotzdem schnell und zuverlässig zugestellt werden. Dieses Buch behandelt den Kampf gegen Spam und Viren daher hauptsächlich aus der Sicht der Administratoren von E-Mail-Systemen.

Was ist Spam?

Im weitesten Sinn ist Spam eine Bezeichnung für unerwünschte Werbe-E-Mails. Darüber hinaus variieren die Definitionen.

Spam trat zuerst Mitte der Neunzigerjahre des vorigen Jahrhunderts im Usenet auf, noch bevor E-Mail Verbreitung gefunden hatte. Im Usenet bezeichnete (und bezeichnet) der Begriff Spam Beiträge mit Werbeinhalt, die massenhaft in zahllose Newsgroups gepostet werden, ohne Bezug auf das Thema der Diskussion in diesen Gruppen zu nehmen. Während das Spam-Aufkommen im Usenet zunahm, wurden auch erste automatische Anti-Spam-Maßnahmen entwickelt, insbesondere so genannte Cancelbots, die automatisch massenhaft Spam-Postings canceln, also aus den Newsgroups entfernen. Dabei konnte durch die Arbeit einiger weniger das Spam-Problem im gesamten Usenet mehr oder weniger kontrolliert werden. Eine derartige Effizienz ist in anderen Medien leider nicht möglich.

Das erste Spam überhaupt war vermutlich das Posting von Clarence L. Thomas IV von der Andrews University am 19.1.1994 mit dem Titel »Global Alert For All: Jesus is Coming Soon« (*http://groups.google.com/groups?selm=9401191510.AA18576%40jse.stat.ncsu.edu*). Das erste Spam mit kommerziellem Inhalt war das Posting von Laurence Canter von der Anwaltskanzlei Canter & Siegel (USA) am 12.4.1994 mit dem Titel »Green Card Lottery - Final One?« (*http://groups.google.com/groups?selm=2odj9q%2425q%40herald.indirect.com*). Dieses Posting wird allgemein als Start der weltweiten kommerziellen Spam-Welle angesehen. Und es hatte auch ein weiteres Merkmal mit vielen heutigen Spams gemeinsam: Die angebotenen Dienste zur anwaltlichen Unterstützung bei der Teilnahme an der Green Card-Lotterie in den USA waren im Prinzip betrügerisch, weil für die Teilnahme überhaupt keine anwaltliche Hilfe nötig ist. Und die letzte Lotterie dieser Art war es selbstverständlich auch nicht.

Mit der Verbreitung neuer elektronischer Kommunikationsmedien und dem Rückgang des Usenets wurde der Begriff Spam auf die neuen Medien übertragen. Die meiste Aufmerksamkeit erhält heute der Spam-Versand über E-Mail, da Spam über E-Mail im Verhältnis besonders häufig auftritt und E-Mail heute schon als nahezu universelles Kommunikationsmedium gelten kann. Spam gibt es aber auch über Mobiltelefone, Instant-Messaging-Protokolle wie ICQ und IRC (Spam over Instant Messaging: SPIM) sowie über Internet-Telefone (Spam over Internet Telephony: SPIT). In diesem Buch geht es freilich nur um Spam über E-Mail.

Im Zusammenhang mit E-Mail wird statt »Spam« oft die Bezeichnung »Unsolicited Commercial Email« (unverlangte kommerzielle E-Mail), kurz UCE, verwendet. Dieser Begriff ist präziser und vermeidet die Assoziation mit dem Usenet, schließt aber scheinbar nur E-Mails mit kommerziellem Inhalt ein. Genauer treffen würde wohl die Bezeichnung »unverlangte Werbe-E-Mail«, womit auch Werbung ohne geschäftlichen Hintergrund eingeschlossen wäre. Der kommerzielle Hintergrund einer Werbe-E-Mail ist rechtlich allerdings von Bedeutung, da eine solche E-Mail zum Beispiel in Deutschland gegen das Gesetz gegen den unlauteren Wettbewerb verstoßen würde. Von technischer Seite wird das aber eher nicht beachtet, da das Ziel die Vermeidung von unerwünschter Werbe-E-Mail gleich welcher Art ist. Der Begriff UCE kann daher als Synonym für Spam gesehen werden.

Etwas allgemeiner ist der Begriff »Unsolicited Bulk Email« (unverlangte Massen-E-Mail), kurz UBE. Dieser Begriff schließt sowohl Spam als auch E-Mail-Viren ein. Sowohl technisch als auch rechtlich ist es sinnvoll, Spam und Viren unterschiedlich zu behandeln, daher wird dieser Begriff hier nicht verwendet.

In diesem Buch wird ausschließlich der Begriff »Spam« für unerwünschte Werbe-E-Mails verwendet. Die Rechtsprechung in Deutschland definiert Werbung im Übrigen als immer dann unerwünscht, wenn sie außerhalb einer bestehenden Geschäftsbeziehung versendet wird und keine Zustimmung des Empfängers vorlag oder zu mutmaßen war.

Das Gegenteil von Spam, also E-Mail, die erwünscht ist oder keine Werbung darstellt, wird gelegentlich als »Ham« bezeichnet. Diese Bezeichnung kommt in verschiedener Software vor, wird aber ansonsten in diesem Buch nicht verwendet.

Spam, Spam, Spam

SPAM ist die Bezeichnung einer Dosenfleischsorte der Firma Hormel Foods Inc. aus den USA. Der Name entstand aus »spiced ham« (gewürzter Schinken). In Mitteleuropa ist das Lebensmittel SPAM ziemlich unbekannt, aber es ist zum Beispiel in Großbritannien erhältlich.

Die Übertragung des Namens auf elektronische Kommunikationsmedien geht auf einen Sketch aus der bekannten britischen Comedyserie Monty Python's Flying Circus zurück. In einem Restaurant, in dem es ausschließlich Gerichte, die SPAM enthalten, gibt, fragt eine Besucherin nach einem Gericht ohne SPAM. Bei jeder Erwähnung von SPAM fällt ein Wikinger-Chor mit einem Loblied auf SPAM ein, bis das Gesinge jede Unterhaltung erstickt: »Spam, spam, spam, spam. Lovely spam! Wonderful spam! Spam, spa-a-a-a-a-am, spam, spa-a-a-a-a-am, spam. Lovely spam! Lovely spam! Lovely spam! Lovely spam! Spam, spam, spam, spam!«

Ähnlich würde es wohl auch um die Unterhaltungen im Usenet oder über E-Mail bestellt sein, wenn keine technischen Maßnahmen ergriffen worden wären.

Spam wird durch mehrere Umstände ermöglicht:

- Der Versand von E-Mails ist nahezu kostenlos. Es fällt nur eine geringe Grundgebühr für die Internetverbindung an.
- E-Mails können sehr schnell und in großen Mengen versendet werden.
- Der Versand von E-Mails kann automatisiert werden.
- E-Mails können anonym versendet werden.
- Durch Sicherheitslücken und Konfigurationsfehler können Anti-Spam-Maßnahmen regelmäßig umgangen werden.

Einige dieser Umstände sind wünschenswert und können nicht beseitigt werden. Vorschläge, die zum Beispiel mit dem Versand von E-Mails eine Stückgebühr verbinden wollen, werden stets zurückgewiesen. Andere Umstände, zum Beispiel der Massenversand und der anonyme Versand, können durch technische Maßnahmen erkannt werden und stellen Ansatzpunkte im Kampf gegen Spam dar. Da Spam aber hauptsächlich durch seinen Inhalt mit Werbecharakter und die Umstände, wie diese Werbung zum Empfänger kommt, definiert wird, ist eine automatische Erkennung eine besondere technische Herausforderung.

Die in Spam beworbenen Waren und Dienstleistungen sind fast immer gesellschaftlich tabuisiert, zum Beispiel Potenzmittel, »Erwachsenenunterhaltung« oder Kredite von dubiosen Quellen, und bewegen sich ebenso oft am Rande der Legalität. Obwohl davon auszugehen ist, dass einige der durch Spam verbreiteten Angebote zumindest real sind, sind sie sehr oft auch einfach Einladungen zum Betrug. Diese Umstände haben sich gewissermaßen gegenseitig bedingt. Da Werbung über E-Mail mittlerweile einen derartig schlechten Ruf hat, werden angesehene Unternehmen nur mit größter Sorgfalt überhaupt Werbung darüber betreiben. Übrig bleiben die zwielichtigen Gestalten.

Allerdings ist Spam auch nur deswegen möglich, weil die Spammer mit ihren Methoden anscheinend wirtschaftlichen Erfolg haben. Deswegen ist Spam auch ein gesellschaftliches Problem.

Die USA sind übrigens das Hauptursprungsland von Spam mit rund einem Drittel des weltweiten Aufkommens. Die üblichen Verdächtigen Korea und China folgen erst auf den Plätzen zwei und drei. Spam aus Deutschland soll nur mit rund einem Prozent zum weltweiten Aufkommen beitragen.

Was sind Viren?

Malware (»malicious software«) ist ein allgemeiner Begriff für Programmroutinen mit Schadensabsichten. Dabei werden mehrere Kategorien unterschieden, abhängig davon, wie sich die Schadensroutinen verbreiten. Die wichtigsten sind:

- Viren sind Programmroutinen, die nicht selbstständig aktiv werden können, sondern sich in andere Programme einbinden, um dort Schaden anzurichten und sich weiter zu verbreiten. Diese Definition ist analog zu biologischen Viren. Verglichen mit anderen Malware-Arten sind klassische Computerviren im E-Mail-Zeitalter eher rückläufig
- Würmer sind eigenständige Programme, die sich selbst verbreiten und Schaden anrichten. Würmer werden heutzutage bevorzugt per E-Mail-Anhang versendet und von unvorsichtigen Anwendern oder durch Sicherheitslücken oder Konfigurationsfehler aktiviert. Im Normalfall verbreiten sich die Würmer in der Form, dass sie sich selbst an alle Adressen im Adressbuch des befallenen Computers senden.

- Trojanische Pferde sind schädliche Programmteile, die in legitim erscheinenden Programmen oder Dokumenten versteckt sind. Sie replizieren sich nicht selbst, sondern werden von Anwendern verbreitet, die nichts von der Existenz des Trojaners wissen, indem sie jene Programme oder Dokumente weitergeben. Die Bezeichnung geht auf die Legende des Trojanischen Pferdes zurück, einem großen hölzernen Pferd, das bei der Belagerung des antiken Troja von den Griechen scheinbar als Geschenk vor den Toren der Stadt zurückgelassen worden war. Von den ahnungslosen Einwohnern in die Stadt gezogen, konnten die in dem Pferd verborgenen griechischen Soldaten die Stadt einnehmen. Oft wird diese Art von Malware verkürzt als Trojaner bezeichnet, was wohl etwas unangebracht ist, da sie dann richtiger Grieche heißen müsste.

Computerviren kamen Mitte der Achtzigerjahre des letzten Jahrhunderts auf und verbreiteten sich zu der Zeit häufig über illegal kopierte Software und auch über so genannte Mailbox-Systeme. Der Verbreitungsfaktor war dabei der Bedarf der Anwender, günstig an Software aus zwielichtigen Quellen heranzukommen – Software, die auf normalen Wegen vom Hersteller bezogen wird, enthält in der Regel keinen Virus. Mit steigender Vernetzung verbreitete sich Malware zunehmend über Netzwerkdienste, die Software-Bugs enthielten oder Konfigurationsfehler hatten. Da Firewalls und Netzwerke mit privaten IP-Adressen mittlerweile üblich sind, sind derartige Verbreitungsmethoden nicht mehr sehr effektiv. Üblicher ist daher heutzutage die Verbreitung über E-Mail, da quasi jeder Netzteilnehmer ein E-Mail-Postfach hat und so insbesondere auch unerfahrene und unvorsichtige Anwender erreicht werden können.

Die Verbreitung von Malware über E-Mail wird insbesondere ermöglicht durch:

- universellen Internetzugang durch unerfahrene, technisch nicht versierte Anwender
- E-Mail-Programme mit »hilfreichen«, aber unsicheren Standardkonfigurationen
- Sicherheitslücken in Software aller Art

Daneben tragen auch hier die schon oben erwähnten Eigenschaften des E-Mail-Systems bei: E-Mails können kostenlos, massenhaft, automatisiert und anonym versendet werden.

Auch hier gilt, dass einige dieser Umstände, zum Beispiel die Tatsache, dass sich jedermann relativ problemlos ins Internet einwählen kann, weithin wünschenswert und nicht zu verändern sind. Hauptmittel im Kampf gegen Malware sind daher einerseits Virenscanner-Programme, die Dateien, E-Mails und Computersysteme bezüglich Virenbefall überwachen und gegebenenfalls säubern, andererseits Bestrebungen, Software sicherer zu machen und Anwender zu belehren. Beide Arten von Maßnahmen können aber keine absolute Sicherheit versprechen.

Die Schadensroutinen von Malware können vielfältig sein. In den Anfangszeiten wurde gern einfach die Festplatte oder Diskette gelöscht. Im Netzwerkzeitalter wird Spyware installiert, die den Computer ausspioniert, oder es wird eine Backdoor auf dem Computer eingerichtet, damit er später für andere Machenschaften des Malware-Autors verwendet werden kann, etwa verteilte Denial-of-Service-Angriffe auf Dritte. In letzter Zeit sind Allianzen zwischen Virenautoren und Spammern zu beobachten, wobei die Viren die Adressen für die Spammer sammeln und/oder dafür sorgen, dass die befallenen Computersysteme für den anonymen Spam-Versand missbraucht werden können. Häufig ist es allerdings auch der Fall, dass keine nennenswerte Schadensroutine vorhanden ist und der Malware-Autor lediglich auf den Verbreitungsgrad seines Werks stolz sein möchte. Das bloße Vorhandensein und die Selbstreplikation von Malware kann allerdings auch schon als Schaden angesehen werden, weil so Computerressourcen belegt werden und Zeit zur Bereinigung der Systeme aufgewendet werden muss.

Für Hersteller von Antiviren-Software und die Administratoren von anfälligen Computersystemen, insbesondere Desktop-Systemen, sind die technischen Unterscheidungsmerkmale von Computerviren relevant, insbesondere bei der Reparatur von schon infizierten Systemen. Bei der Administration von E-Mail-Systemen dagegen ist es das Ziel, Computerviren gar nicht erst auf die anfälligen Systeme kommen zu lassen. In diesem Zusammenhang sind die unterschiedlichen Eigenschaften von Viren und Malware eher unerheblich. Daher wird in diesem Buch ausschließlich der Begriff Virus in Bezug auf alle Programmroutinen mit Schadensabsichten verwendet. Dieser Begriff wird auch überwiegend in der Öffentlichkeit und von der einschlägigen Software verwendet, insbesondere bei so genannten »Virenscannern«, die natürlich auch viele andere Arten von Malware erkennen.

Konsequenzen

E-Mail-Missbrauch durch Spam und Viren ist bekanntlich kein Randproblem. Die Konsequenzen für die Anwender, Betreiber, die Wirtschaft und das Medium E-Mail sind erheblich.

Ressourcenverschwendung

Regelmäßige Schätzungen von verschiedenen Stellen sagen aus, dass derzeit über 50% aller weltweit versendeten E-Mails Spam oder Viren sind. In einigen Untersuchungen ist die Zahl sogar weit höher angesiedelt.[1] Folglich müssen, allein um den Fluss der E-Mails aufrechtzuerhalten, doppelt so viele Ressourcen eingesetzt werden, wie eigentlich nötig wären. Das bedeutet mehr Computersysteme, Netzwerk-

1 Siehe zum Beispiel *http://www.absolit.de/eMail-Marketing/74-aller-E-Mails-Spam.html*, *http://www.clickz.com/stats/sectors/software/article.php/3364421*, *http://www.clickz.com/stats/sectors/email/article.php/3447341*, *http://internetweek.com/e-business/showArticle.jhtml?articleID=21100199*, *http://www.newsfactor.com/story.xhtml?story_id=30294*.

leitungen, Personal, Zeitaufwand. Dazu kommen Maßnahmen, um sich gegen Spam und Viren zu verteidigen: mehr Computersysteme, mehr Netzwerkverkehr, mehr Personal, mehr Zeitaufwand. Erheblich ist auch die Anzahl der durch Spam und Viren verursachten Rückläufer und Fehlermeldungen: noch mehr Netzwerkverkehr, noch mehr Aufwand für das Administrationspersonal. Die Abwehr von E-Mail-Missbrauch ist zur Materialschlacht geworden.

Aktuelle Schätzungen gehen übrigens davon aus, dass 50% des gesamten Internetverkehrs dem Download von Musik und Filmen zuzuschreiben sind. E-Mail-Missbrauch ist also zugegebenermaßen nicht das einzige Phänomen, das die Ressourcen des Internets strapaziert.

Vertrauensverlust

E-Mail hat sich in kurzer Zeit zu einem extrem populären Kommunikationsmittel entwickelt. Jeder kann mit jedem kostenlos und unbegrenzt kommunizieren und ist dabei nicht auf die sofortige Anwesenheit des Kommunikationspartners angewiesen. Diese Möglichkeiten haben zu ganz neuen Geschäftsmethoden und Lebensstilen geführt. Dadurch, dass E-Mail aber mehr und mehr missbraucht wird und in jeder E-Mail eine potenzielle Gefahr für das Computersystem und das Netzwerk steckt, sinkt das Vertrauen in das Medium.

Das E-Mail-Protokoll SMTP wurde ursprünglich so entwickelt, dass alles versucht wird, um eine E-Mail zuzustellen, und dass, wenn dies nicht möglich ist, eine Fehlermeldung an den Absender geschickt wird. Durch die Allgegenwart von Spam- und Virenfiltersystemen wird heute nicht mehr angenommen, dass jede E-Mail sicher ankommt und nicht einem Filter zum Opfer fällt. Und dadurch, dass Fehlermeldungen durch Rückläufer von Spam- und Viren-E-Mails überhand nehmen, werden wahre Probleme im E-Mail-System leicht übersehen. E-Mail ist heute ein unzuverlässiges Kommunikationsmittel.

Auf Grund der Gefahr, die Computerviren darstellen, wird die Vielfalt des Kommunikationsmittels E-Mail vielerorts künstlich eingeschränkt. Bestimmte Dateitypen dürfen nicht versendet werden oder werden herausgefiltert. Anhänge werden ganz verboten. E-Mail darf nur zu bestimmten Zwecken und mit bestimmten Kommunikationspartnern verwendet werden. E-Mail-Clients werden zur Gefahrenquelle und müssen in ihrer Funktionalität begrenzt werden. E-Mail ist heute oft ein unflexibles Kommunikationsmittel.

Obwohl es für E-Mail als Kommunikationsmedium zurzeit keine wirkliche Alternative zu geben scheint, ist vielerorts die Abkehr davon zu beobachten. Mobiltelefone, SMS und Instant-Messaging haben im gesellschaftlichen Bereich E-Mail weit zurückgedrängt. Das Telefax, das eigentlich durch E-Mail hätte abgelöst werden müssen (und selbst mit einem Spam-Problem zu kämpfen hat), gehört nach wie vor

zur Standardausstattung eines Büros. Und das papierlose Büro ist sowieso nie mehr als eine Utopie gewesen. All diese Umstände zeigen, dass die Spam- und Virenproblematik dem Medium E-Mail einen Vertrauensverlust beschert hat, der die Nützlichkeit dieses Mediums gefährdet.

Wirtschaftlicher Schaden

Aus der Ressourcenverschwendung und dem Vertrauensverlust entsteht natürlich auch ein wirtschaftlicher Schaden auf Grund des zusätzlichen zeitlichen und materiellen Aufwands zur Abwehr von Spam und Viren, ganz zu schweigen vom Schaden, den nicht abgefangene Viren anrichten.

Studien schätzen den durch Spam verursachten Schaden in Deutschland im Jahr 2005 auf bis zu 4 Milliarden Euro.[2] Bei rund 40 Millionen Internetnutzern in Deutschland kann man sich leicht selbst ausrechnen, welcher Schaden statistisch auf einen selbst oder die eigene Firma entfällt. Der Schaden weltweit wird auf bis zu 40 Milliarden Euro geschätzt. Diese Zahlen gelten aber nur, weil weithin Maßnahmen zur Abwehr von Spam und Viren ergriffen worden sind, ansonsten wäre der Schaden ungleich höher.

Open Source-Software

Dieses Buch behandelt die Bekämpfung von Spam und Viren mit Open Source-Tools. Open Source-Software ist Software, deren Lizenzbestimmungen den Anwendern der Software bestimmte Rechte einräumen. Dazu gehören insbesondere:

- Die Verwendung der Software ist nicht beschränkt.
- Die kostenlose Weitergabe der Software ist erlaubt.
- Der Quellcode der Software ist erhältlich.
- Der Anwender darf geänderte Versionen erstellen und weitergeben.

Die Idee hinter Open Source-Software ist diese: Wenn Software-Entwickler den Quellcode lesen und die Software an ihre Bedürfnisse anpassen können, dann kann Software schneller weiterentwickelt werden. Je mehr Entwickler auf diese Art mitwirken, desto schneller schreitet die Entwicklung fort, desto mehr Funktionalität entsteht, und desto eher werden Fehler berichtigt.

Die Anhänger von Open Source-Software sind der Meinung, dass dieser Entwicklungsprozess bessere Software produziert als der herkömmliche, »geschlossene« Prozess, in dem Software von wenigen Entwicklern produziert wird und die Anwender nur ein fertiges Produkt erhalten, das sie nicht prüfen oder anpassen können.

2 *http://www.at-mix.de/news/657.html*

Diese These wird gestützt durch die Tatsache, dass ein Großteil der Infrastruktur des Internets auf Open Source-Software läuft. Die meisten Webserver, Mailserver, DNS-Server laufen ausschließlich oder größtenteils mit Hilfe von Open Source-Software. So erscheint es auch folgerichtig, für technische Maßnahmen gegen Spam und Viren in E-Mail auf Open Source-Software zu setzen.

Da Open Source-Software von jedem, der sie erhalten hat, kostenlos weitergegeben werden kann, wird sie normalerweise nicht im herkömmlichen Sinne verkauft. Daher ist Open Source-Software in der Regel auch billiger in der Anschaffung als herkömmliche Software. Dies hat erheblich zu ihrem Erfolg beigetragen, ist allerdings nicht das primäre Ziel dieser Entwicklungsmethode; das primäre Ziel ist es, bessere Software zu produzieren. Beim Einsatz von Open Source-Software können auch Kosten entstehen durch Personalaufwand, Schulungen, Beratungsleistungen, Support oder zusätzliche Programmierleistungen. Oft erhält der Anwender am Ende aber ein besseres Produkt zu geringeren Kosten. Es ist jedoch falsch, Open Source-Software als Gegensatz zu »kommerzieller« Software zu verstehen. Geschäftlicher Erfolg lässt sich auch mit Open Source-Software erzielen.

Obwohl oft von der Open Source-Community die Rede ist, ist die Open Source-Landschaft in Wahrheit sehr vielfältig und nur lose verbunden. Gemeinsam ist allen das Vertrauen in den besseren Entwicklungsprozess. In dieser Vielfältigkeit sind eine ganze Reihe von Software-Lösungen entstanden, die beim Kampf gegen Spam und Viren behilflich sein können, und dieses Buch wird versuchen, diese Vielfalt zu sortieren.

Nicht unerwähnt bleiben soll neben der Open Source-Software auch die Freie Software. Diese Bewegung setzt sich ein für Software mit Lizenzbedingungen ähnlich den oben aufgeführten, aber im Sinne der »Freiheit« des Anwenders. Freie Software ermöglicht, dass Computerbenutzer prüfen und kontrollieren können, wie ihr Computer arbeitet, und ermöglicht, anderen dabei zu helfen, Selbiges zu tun.

Pragmatiker sehen in Open Source-Software und Freier Software zwei Seiten derselben Medaille. So wird es auch in diesem Buch gehalten. Puristen mögen es den Autoren vergeben.

Das Gegenteil von Open Source-Software ist Closed Source-Software. Der Gegensatz zu Freier Software ist proprietäre Software. Kommt derartige Software zur Sprache, wird in diesem Buch der letztere Begriff verwendet.

Weitere Informationen über Open Source Software gibt es unter anderem bei der Open Source Initiative (*http://www.opensource.org/*), weitere Informationen über Freie Software gibt es bei der Free Software Foundation (*http://www.fsf.org/*).