

MARTIN GOLDMANN

Dear Emily Postnews

Die Geschichte der Netikette

1. Wie die Netikette entstand

Wann genau die erste Netikette entwickelt wurde, ist nicht auszumachen. Sie entstand wahrscheinlich im Usenet, dem Vorläufer der heutigen Newsgroups. Zusammengesetzt aus »Net« und »Etikette« bildeten die Teilnehmer ein neues Kunstwort: »Netiquette«, zu Deutsch Netikette. Da im Internet Dokumente ständig auf den neuesten Stand gebracht werden, ist der genaue Werdegang der Netikette schwer nachzuvollziehen. Archivierte Dokumente fehlen, viele Server, auf denen früher wichtige Dokumente gespeichert waren, sind umgezogen oder existieren nicht mehr. Und wie so oft im Internet haben sich viele Instanzen an der Netikette beteiligt, sie kopiert, weiter entwickelt und wieder kopiert. Der Ursprung verliert sich im Dickicht der Kopien.

1.1 Netikette im Usenet: Emily Postnews

Ein frühes Dokument der Netikette ist das humoristische »Dear Emily Postnews«, das Brad Templeton nach eigenen Angaben zwischen 1986 und 1987 geschrieben hat.¹ Der Name Postnews lehnt sich an die amerikanische Autorin Emily Post (1873–1960) an. Ihr Buch »Etiquette« erschien 1922 und ist mit dem hier zu Lande bekanntesten Knigge vergleichbar.

»Dear Emily Postnews« fasst die Vergehen gegen die Netikette zusammen: Zu lange Signaturen, überflüssiges Zitieren von Antworten, massenhafter Versand von Texten. Geboren sind diese Benimmregeln aus technischer Notwendigkeit. Das Usenet war einst nicht Teil des Internet. Vielmehr riefen sich die Computer gegenseitig an und glichen die Nachrichten untereinander ab. All das lief noch über sehr langsame Modemleitungen. Jedes Byte zu viel verlängerte unnötig den Versand und den Empfang der Nachrichten. Denn auch die Leser mussten sich mit langsamen Modems auf den Usenet-Servern ihre Informationen abholen. Zwar sind die Leitungen

jetzt schneller. Aber das große Problem in den Newsgroups bleibt die weite Verbreitung und die massenhafte Nutzung: Ein zu viel geschriebenes Byte vermehrt sich hundert- und millionenfach im Internet und wird so zu nutzlosem Datenballast.

1.2 Netikette in E-Mail

Mit der massenhaften Nutzung des Internets und speziell der E-Mail ist der Bedarf nach Richtlinien beim elektronischen Postversand gestiegen. Also haben sich mit der Zeit die Netikette-Regeln auf E-Mails erweitert. Wieder ist die berechtigte Furcht um Ressourcen der Grund: Unternehmen oder Bildungseinrichtungen kann es teuer zu stehen kommen, wenn ihre Mitarbeiterinnen und Mitarbeiter megabyteweise Bilder oder Multimedia-Dateien versenden. Nicht nur die eigenen Server leiden darunter, auch die Leitungen nach draußen werden überlastet. Schlimmstenfalls müssen Administratoren eingreifen und den Mail-Server von Hand stoppen. Also verfassen auch Unternehmen Regeln für den Umgang mit Nachrichten oder sperren den Versand von allzu umfassenden E-Mails.

1.3 Höflichkeit

Die in den späten 1980ern formulierte Netikette »Emily Postnews« konzentrierte sich noch auf technische Aspekte der Internet-Nutzung. Immerhin drei Kapitel beschäftigen sich mit der Rücksichtnahme auf andere Teilnehmer: Bitter ironisch empfiehlt »Emily Postnews«, Frauen im Netz herablassend zu behandeln, Konflikte möglichst öffentlich auszutragen, in den Mails ausfallend und beleidigend zu werden. Später wurden allgemeine Regeln und ethische Grundsätze der Internet-Nutzung verfasst. Sie sind im Dokument RFC 1087 aus dem Jahr 1989 festgehalten: Niemand soll sich unbefugt Zugriff auf die Ressourcen anderer verschaffen, Ressourcen verschwenden oder in die Privatsphäre anderer eindringen.

Regeln, die unterschiedliche Kulturkreise, Sprachen oder Religionen unter einen Hut bringen, kamen erst später. Sie schienen unnötig in der Netz-Frühzeit, als das Internet ein rein akademisch genutztes Netzwerk war. Mit der massenhaften, weltweiten Verbreitung des Internets ist aber der Bedarf an genau solchen Regeln gewachsen. Ebenso bleibt die Notwendigkeit technischer Regeln erhalten. Mit der Zunahme technisch ungebildeter Benutzerinnen und Benutzer steigt der Bedarf an klaren und verständlichen Regeln für Mail und Newsgroups, denn nicht jeder Neuling im Netz kann sich vorstellen, welchen Ärger er mit einer hundertfach versandten Multimedia-Nachricht anrichtet.

1.4 Sanktionen

Bei Verstößen gegen diese Regeln der Netikette drohen nicht nur böse Anrufe oder Mail-Antworten. Der Diebstahl von Daten oder der wissentliche Versand von schädlichen Programmen sind Straftatbestände. Hackern in den USA wie Kevin Mitnick drohen harte Strafen: Mitnick hatte Systeme von großen Firmen wie Sun oder Fujitsu gehackt, wurde 1995 gefasst und ist 1999 zu fünf Jahren Haft verurteilt worden. Nach der langen Untersuchungshaft war die Strafe aber bereits im Januar 2000 abgesessen. Doch Bewährungsauflagen verbieten dem Hacker jede Nähe zu Computern und die Tätigkeit als Berater zu EDV-Themen.

Auch in Deutschland sind Computer-Delikte keine Bagatellen. Die Kölner Polizei meldete für das Jahr 2000 über 1 000 Internet-Betrugsfälle bundesweit: Die Betrüger stehlen mit Hilfe von Trojanischen Pferden Zugangsdaten von Rechnern anderer Nutzer. Dann loggen sie sich unter deren Kennung ein und verprassen Gebühren. Der Schaden läge, so die Polizei, zwischen einem Cent und mehreren Millionen Euro. Allerdings sei die Aufklärungsrate recht hoch, so die Kölner Polizei. Denn bei jeder Einwahl sähe man die Rufnummer des Kunden und könne anhand dieser auch den Aufenthaltsort des Hackers ermitteln. Den Betrügern drohen bis zu fünf Jahre Haft. Damit es erst gar nicht so weit kommt, rät die Polizei, keine Zugangsdaten auf der Festplatte zu speichern.

Internet-Kriminellen ist bald nicht mehr nur die Kölner Polizei auf den Fersen. Denn im November 2001 wurde die »Budapester Konvention« verabschiedet. In diesem internationalen Vertragswerk sind erstmals einheitlich Internet-Vergehen definiert. Dazu gehören das illegale Abhören, das Einbrechen in Computer und das Stören von Systemen. Auch das Stehlen, Manipulieren oder Löschen von Daten steht mit auf der Liste. Ebenfalls unter Strafe: Copyright-Vergehen, das Umgehen von Kopierschutzsystemen, das Herstellen, Verbreiten und Verfügbarmachen von Kinderpornografie sowie Verbrechen, die unter Ausnutzung von Computer-Netzwerken begangen werden können.² Das Cybercrime-Abkommen ist allerdings bei Datenschützern umstritten, da es den Behörden weit reichende Abhör- und Spionage-Befugnisse einräumt.³

Im Jahr 1998 rief die britische Datenschutzorganisation »Privacy International« den »Big Brother Award« ins Leben. Ausgezeichnet werden Personen oder Firmen, die in besonderer Weise die Privatsphäre von Menschen beeinträchtigen oder private Daten Dritten zugänglich machen. Rasch übernahmen Datenschutzorganisationen in Kanada, Österreich, den USA, Frankreich und Deutschland das Konzept, um mit dem Negativpreis eine breite Öffentlichkeit für Gefährdungen der Privatsphäre zu sensibilisieren. Federführend bei der Verleihung in Deutschland ist der »Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e. V.«, kurz FoeBuD. Mitglieder der Jury kommen aus dem »Chaos Computer Club«, dem FITUG, der Deutschen

Vereinigung für Datenschutz (DVD) sowie dem FIF (Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung).⁴

2. Die Grundregeln der Netikette

Die Grundregeln der Netikette im Internet lauten wie folgt:

- Beleidige niemanden.
- Stehe immer zu dem, was Du sagst.
- Äußere dich klar, knapp und präzise.
- Sei freundlich zu jedem.
- Spioniere niemanden aus.
- Spare mit Daten.
- Verschicke keine Nachrichten, die der andere nicht lesen kann.
- Sende keine schädlichen Programme, sprich: überprüfe jede Datei vor dem Versand auf Viren.
- Brich' nicht in Datenbestände von anderen ein.

Je nach Umgebung, ob World Wide Web, Chat-Foren, Newsgroups oder ob E-Mail, werden diese Grundregeln ausdifferenziert.

2.1 Netikette im Web

Wenn Sie im World Wide Web surfen, kommen Sie mit den Anstandsregeln des Netzes kaum in Konflikt. Denn beim Abrufen von Daten kann man nicht viel verkehrt machen. Wenn Sie allerdings gemeinsam mit anderen Benutzern und Benutzerinnen auf einen einzigen Netzzugang zugreifen, sollten Sie auf das Überspielen großer Datenmengen verzichten. Denn damit bremsen Sie den Zugriff anderer Benutzer auf das Internet.

Anders ist es, wenn Sie als Betreiber einer Internet-Seite auftreten. Hier sollten Sie Folgendes beachten:

- Halten Sie die Webseite so schlank wie möglich. Verzichteten Sie auf aufwendige Animationen. Und wenn Sie multimedial arbeiten müssen, gehen Sie sparsam vor. Das spart Zeit und Geld des Benutzers.
- Sammeln Sie nicht unnötig Daten. Wenn ein Besucher auf Ihre Seite kommt, verrät er noch nicht allzu viel über sich. Allenfalls der Internet-Anbieter, das Internet-Zugangsprogramm und die vorher besuchte Seite lassen sich herausfinden. Allerdings machen es einige Internet-Anbieter so: Sie lassen den Zugriff auf das Angebot nur zu, wenn sich der Besucher zu erkennen gibt. Das ist an sich noch nichts Böses – im Gegenteil: Bei frei verfügbaren Internet-E-Mail-Angeboten schützt das sogar vor Missbrauch. Neben Namen und Adresse müssen aber oft auch Vorlieben und andere persönliche Daten preisgegeben werden. Und die gehen niemanden et-

was an, dienen aber zum Erstellen von Kundenprofilen und zum Anpassen der Werbeangebote. Sie sollten das nicht tun. Verlangen Sie nur die Daten von einem Besucher, die Sie wirklich benötigen. Auf jeden Fall tabu ist die Weitergabe der Daten gegen das ausdrückliche Einverständnis des Benutzers.

Genauer regelt das Bundesdatenschutzgesetz (BDSG) das Erheben von Daten. Der Paragraph 3 a verlangt, nur die Daten zu erheben, die notwendig sind: »Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.« Die Anbieter von Internet-Angeboten werden sich mit diesem Gesetz auseinandersetzen müssen.

Allerdings ist es oft nicht einmal nötig, Daten zu erfassen. Denn meist liefern die Kunden freiwillig genügend Informationen. Besonders die beliebten Online-Kataloge und Suchmaschinen wie Yahoo oder Altavista setzen »Targeting« ein. So nennt sich das gezielte Platzieren von Werbebannern, passend zum Suchbegriff. Der Informationssuchende wundert sich vielleicht nicht einmal, dass zu seiner Suchanfrage »BMW 753i« gleich die passende Anzeige des Autohauses eingeblendet wird. Das ist an sich noch nichts Schlimmes. Allerdings lassen sich diese Informationen in einer Datenbank speichern. Über Cookies wird dann der Benutzer identifiziert. Sobald er sich auch noch mit seinem Namen anmeldet, hat der Anbieter schon ein genaues Bild von den Konsum-Gewohnheiten. »Profiling« nennen die Marketing-Experten das Gewinnen eines aussagekräftigen Kundenprofils. Sind genügend Informationen in der Datenbank gesammelt, sprechen Marketingexperten von einem »Data-Warehouse«. Jetzt tritt »Data-Mining« in Aktion: Per Computerprogramm werden Zusammenhänge aufgespürt, die vorher unbekannt waren. Data-Mining könnte beispielsweise entdecken, dass 30–35-jährige Väter von zwei Kindern und mit einem gewissen Mindesteinkommen häufig Bausparverträge in einer bestimmten Höhe abschließen. Und los geht's mit der gezielten Werbung – das spart eine Menge sonst verschwendeten Portos.

2.2 Netikette für den Chat

Chat-Programme erlauben ihren Benutzerinnen und Benutzern, sich per Tastatur zu unterhalten. In gemeinsamen Chat-Räumen treffen sich Teilnehmer aus aller Welt und tauschen sich aus. Das Niveau dieser Chats reicht vom spannenden »Geschnatter« bis hin zur Hilfe bei Computer-Problemen.

Der beste Weg, sich in einem Chat unbeliebt zu machen:

- Geben Sie sich einen möglichst aufregenden Namen, schreiben Sie ihn in VERSALIEN.

- Grüßen Sie nicht, wenn Sie den Chat-Raum betreten.
- Fangen Sie sofort an, mitzureden.
- Stellen Sie allen anderen Teilnehmern Fragen, die diese garantiert nicht interessieren.
- Nerven Sie die Chat-Teilnehmer mit bohrenden Nachfragen, sofern sie nicht innerhalb von Sekunden antworten.

In einem Chat ist erst einmal eines angesagt: Ruhig bleiben, zurückhalten. Wenn Sie einen virtuellen Plauderraum betreten, grüßen Sie höflich, zum Beispiel mit »hallo allerseits«. Und dann warten Sie ab. Lesen Sie erst einmal ein paar Minuten mit. Dann finden Sie heraus, um welches Thema es geht und können vielleicht mitreden. Wenn Ihnen ein anderer eine Frage stellt, antworten Sie freundlich und offen. Mit der Zeit wird es dann zum angenehmen Gespräch kommen.

Etwas anderes ist es, wenn Sie schon Stammgast in einem Chatraum sind. Dann können Sie sofort loslegen und sich mit ihren Freunden unterhalten. Kommt aber ein Neuer hinzu, begegnen Sie ihm mit Höflichkeit. Fragen Sie ihn, was er macht und wie es ihm geht. Und wenn Sie wollen, binden Sie ihn in die Diskussion mit ein. Wenn Sie kein Interesse haben an unbekanntem Mit-Chattern, dann sperren Sie Ihren Chatraum.

2.3 Netikette für Newsgroups im Usenet

Im Usenet diskutieren Tausende von Internet-Teilnehmern. Um den Daten- und Informationsstrom geregelt in Fluss zu halten, ersann die Netzgemeinde schon sehr bald eine eigene Netikette. Alle Teilnehmerinnen und Teilnehmer im Usenet sollte sich an diese Benimmregeln halten. Zwar drohen ihm weder Geld- noch Gefängnisstrafen. Doch wer gegen den guten Ton im Netz verstößt, dem drohen Rüffel und Sanktionen. Diese reichen von verbalen Attacken, Flames genannt, bis hin zum Löschen seiner Newsgroup-Beiträge. Auf die Durchsetzung der Regeln achtet im Allgemeinen die Usenet-Gemeinde selbst. In vielen Gruppen arbeiten zudem Moderatoren. Die lesen einen Beitrag, bevor er veröffentlicht wird.

Diese Grundregeln sollte jeder Usenet-Teilnehmer beherzigen:

Die richtige Newsgroup wählen. Überlegen Sie zuerst, was Sie schreiben wollen. Überlegen Sie dann eine griffige Überschrift, um den Text zusammenzufassen und prüfen Sie, in welche Newsgroup Ihr Beitrag passt. Es gehen nicht nur viele Nachrichten in den falschen Gruppen verloren, es ärgern sich auch Leser, wenn die Newsgroup voller Beiträge ist, die dort nichts zu suchen haben.

Crosspostings vermeiden. Eine Nachricht gehört immer nur in ein Usenet-Forum. Überlegen Sie, wo Sie Ihre Messages unterbringen. Wenn Sie partout der Ansicht sind, dass eine Nachricht in mehrere Foren passt, posten Sie diese

in einen Bereich und platzieren Sie in den anderen Newsgroups kurze Hinweise. Das sollte jedoch die Ausnahme bleiben.

Persönliche Angriffe vermeiden. Bleiben Sie höflich im Netz – verbale Ausfälle und Attacken bringen niemandem etwas und provozieren nur unnötige Auseinandersetzungen. Wenn Sie Streit suchen, nehmen Sie das passende Forum dafür, etwa de.alt.flame.

Ironie kennzeichnen. Die Kommunikation via Computer ist beschränkt – weder Tonfall noch Mimik oder Gestik stehen als zusätzliche Kanäle bereit. Das provoziert Missverständnisse. Verzichten Sie daher auf doppeldeutige oder ironische Formulierungen. Wenn sich diese nicht vermeiden lassen, nutzen Sie Emoticons, etwa das ;-) um Ironie zu unterstreichen.

Kurze Signaturen verwenden. Reduzieren Sie Ihre Signatur. Zwei oder drei Zeilen reichen, um alles in dieser digitalen Kennung unterzubringen.

Keine Werbung. Senden Sie keine Werbung in Newsgroups. Erstens bringt es nicht viel, zweitens ärgert sich die Netzgemeinde enorm darüber, drittens kann es Ihrem Unternehmen schaden, mit dem Bann des Usenet belegt zu werden.

Schreiben Sie unter Ihrem Namen. Adresssammler durchstöbern täglich die Newsgroups, um neue E-Mail-Anschriften zu sammeln. Viele Nutzer sind dazu übergegangen, ihre Adressen für diese Suchmaschinen unbrauchbar zu machen, indem Sie zusätzliche Namen oder Zeichen einfügen, etwa meier_@_foo.bar oder meier@remove.foo.bar. Doch diese Maßnahme schadet mehr als sie bringt. Denn sie erschwert, auf Ihre Beiträge zu antworten. Im Usenet ist dieses Adress-Faking nicht gerne gesehen.

FAQs nutzen. Zu praktisch jeder Newsgroup gibt es eine FAQ, eine Liste mit den meistgestellten Fragen. Diese FAQ-Liste wird regelmäßig aufs Netz geschickt und aktualisiert. Bevor Sie also eine Frage öffentlich in einer Newsgroup stellen, sehen Sie nach, ob diese nicht schon in der FAQ beantwortet ist.

Redundanz vermeiden, Neues sagen. Bevor Sie sich an einer Usenet-Diskussion beteiligen, lesen Sie genau die anderen Beiträge. Bringen Sie dann nur Meinungen oder Fakten, die dort nicht schon dargelegt wurden. Zitieren Sie nur die Passagen aus anderen Beiträgen, auf die Sie sich wirklich beziehen. Fassen Sie sich kurz und schreiben Sie nur dann, wenn Sie wirklich etwas Neues sagen wollen.

Formalia einhalten. Achten Sie auf das, was Sie schreiben. Lesen Sie jeden Text noch einmal durch, bevor Sie ihn posten. Achten Sie auf die Rechtschreibung und grammatikalische Richtigkeit.

Binärdateien nur in die richtigen Foren. Für Binärdateien, also Bilder oder Programme gibt es eigene Newsgroups, meist erkennbar am Kürzel »bin« oder an der Bezeichnung »binaries«. Nur hier haben Files etwas zu suchen.

Gutes Subject wählen. Das Subject ist wie die Überschrift in einer Zeitung: Nur wenn sie gut gewählt ist, wird man einen Beitrag lesen.

Nutzen Sie E-Mail. Nicht jede Antwort auf einen Newsgroup-Beitrag muss öffentlich sein. Antworten Sie per E-Mail, um das Netz zu entlasten. Wenn Sie selbst E-Mails als Antworten auf eine Frage bekommen, stellen Sie nach einigen Tagen eine Zusammenfassung dieser Antworten aufs Netz.

2.4 Netikette für E-Mail

Mit einer freundlichen E-Mail können Sie nicht viel verkehrt machen. Im Allgemeinen gelten hier dieselben Regeln wie auch in den Newsgroups. Also sind Höflichkeit, Kürze, Eindeutigkeit und wohl überlegtes Schreiben gefragt. Im Folgenden wird daher nur auf einige zusätzliche Aspekte eingegangen.

- Nicht an zu große Verteiler senden
E-Mail sollte man grundsätzlich nur an die senden, die es betrifft. Viele neigen dazu, Nachrichten an einen zu großen Verteiler zu schicken. Dazu gehören besonders Mitarbeiterinnen und Mitarbeiter in Unternehmen, die eine Nachricht an alle anderen Angestellten schreiben, nur weil sie ihre Kaffeetasche nicht finden. Inhalt der Nachricht dann: »Wer hat meine Kaffeetasche aus der Küche genommen?« Auch im Privaten gilt es: Nicht jeder will alles lesen. In der Informationsflut von heute stören unnütze E-Mails.
- Nicht zu große Mails schicken
Das kommt oft vor: Person A hat einen schnellen T-DSL-Anschluss oder eine Standleitung in das Internet, Person B nur ein Modem. Person A findet einen kleinen Videofilm im Internet und verschickt ihn an alle Freunde. Person B ist auch darunter. Und B ärgert sich, dass die sieben Megabyte ewig lang die Leitung verstopfen und dass letztlich dabei eine nutzlose Datei heraus kommt, die er sich schlimmstenfalls nicht einmal ansehen kann. Verzichten Sie deshalb auf den Versand von allzu großen Mails. Alles über 200 KByte ist schon kritisch.
- Private Mails nicht veröffentlichen
Nicht nur ein Verstoß gegen die Netikette ist es, E-Mail, die man privat erhalten hat, zu veröffentlichen oder an einen größeren Verteiler weiter zu leiten. Es ist auch ein Vertrauensbruch. Stellen Sie sich vor: Sie schreiben einem Kollegen oder einer Mitschülerin eine E-Mail und erzählen dort wie attraktiv Sie diesen oder jenen Menschen finden. Und der Empfänger leitet die Mail nicht nur an alle anderen Kollegen weiter, sondern auch noch an Ihren Partner (der dann wohl nicht mehr lange Ihr Partner ist).

2.5 Spam

Die weitaus lästigste Art der Mail verstopft jeden Tag unsere Briefkästen: Elektronische Werbesendungen versprechen Millionengewinne, preisen Hautcremes an, Versicherungen oder die neuesten Sonderangebote aus dem Supermarkt. Auf dem Internet haben diese lästigen Postwurfsendungen ein neues Refugium gefunden. Diese Werbemails sind auch als Spam bekannt, benannt nach dem Dosenfleisch der US-Firma Hormel. Das Fleisch spielte in vielen Monty-Python-Sketchen eine Rolle. In einem Film sang eine Wikingerhorde »Spam, Spam, Spam, . . .« und erstickte dadurch sämtliche Konversation im Raum.

Inhaltlich füllen die digitalen Nachrichten die gesamte Bandbreite menschlicher und wirtschaftlicher Bedürfnisse: »Ein WWW-Programm ist hervorragend dazu geeignet, Produkte und Dienstleistungen im Ausland zu verkaufen und das eigene Unternehmen weltweit in angemessener Form zu repräsentieren,« sinnierte Ende der 90er-Jahre ein Übersetzungsdienst. »Dieser Brief wurde zu Dir geschickt, um Dir Glueck zu bringen,« predigt ein Kettenbrief, und susan140@juno.com preist eine frivole 4-for-1-Dateline an.

Gegen Spam ist kein E-Mail-User gefeit. Ob in T-Online oder AOL – die Mails kommen früher oder später automatisch. Spams sind nicht nur lästig, sie kosten auch Geld. Viele Online-User werden nach übertragener Datenmenge zur Kasse gebeten. Spam-Opfer kommen schnell auf ein halbes Megabyte Datenmüll pro Woche. Außerdem fallen für den Download der Nachrichten Telefonkosten oder andere Leitungsgebühren an. Spam-Mail-Versender nehmen das in Kauf.

Nichts ist einfacher, als im Internet an E-Mail-Adressen zu kommen. Spam-Mail-Versender bedienen sich im Usenet oder im World Wide Web. Jeder, der sich online zeigt, wird zum potenziellen Opfer der Mailer. Denn in den News muss ein Spam-Mailer nur die Absenderfelder untersuchen und in eine Datenbank übernehmen. Im World Wide Web bedient man sich eines Robots, der ähnlich wie Altavista oder Lycos automatisch Homepages abklappert und dabei nach Adressen sucht. Auf einer Homepage sind Anschriften einfach zu erkennen, sie werden mit »mailto:« eingeleitet. Selbst für wenig talentierte Programmierer ist die Anschriftensuche leicht. Eine weitere Quelle sind die User selbst. Wer auf einer Webseite Infomaterial anfordert, gibt dabei seine Internet-Adresse preis und landet in einem Verteiler.

Um Spam-Mail zu vermeiden, sollten Sie im Netz so wenig auffallen wie nur möglich. Das bedeutet: Keine Beiträge in Newsgroups, keine eigene Homepage mit E-Mail-Adresse, keine Anforderung von Informationen auf Web-Seiten, keine E-Mails an Unternehmen. So einfach es klingt, so unsinnig ist dieses Verhalten, denn schließlich ist das Internet ein Kommunikationswerkzeug. Zumindest jedoch sollten Sie versuchen, mit Ihrer Adresse zu geizen, also nicht täglich eine Unzahl von Nachrichten in die Newsgroups zu schreiben oder tonnenweise Infos anzufordern.

Spam-Mail-Fallen lauern auf Registrierungsseiten von Software-Anbietern. Vor einem Download verlangt der Server eine E-Mail-Adresse. Und irgendwo auf dem Formular verbirgt sich eine Checkbox. Ist diese angekreuzt, wertet der Software-Anbieter dies als Einverständniserklärung für die Weitergabe der E-Mail-Adresse. Andere Server wiederum gehen den umgekehrten Weg. Hier muss der Downloader die Checkbox aktivieren, um den Spam-Empfang zu vermeiden. Lesen Sie also genau, was Sie anklicken, sehen Sie sich immer die komplette Formularseite an, bevor Sie den Submit-Button drücken. Einige User sind bei der Registrierung des Downloads dazu übergegangen, eine ungültige E-Mail-Anschrift anzugeben, etwa niemand@foo.bar. Doch das ist nicht unbedingt fair und ehrlich.

Ein ideales Mittel gegen unerwünschte Werbung ist ein Postfach (Account) bei einem Gratis-Mailanbieter. Wer mit einer solchen Adresse etwa in Newsgroups schreibt, dessen Ursprungs-Account bleibt vor unangenehmer Werbung verschont – erreichbar ist man für die Netzgemeinde trotzdem. Denn die Mailedienste im Internet filtern die Nachrichten von Spam-Mail-Versendern so weit wie möglich heraus. Anbieter wie Yahoo oder der deutschsprachige GMX verfügen über ausufernde Listen mit Absendeadressen, die sie von vornherein sperren. Darüber hinaus bieten einige Dienste persönliche Blockade-Listen für ihre Kunden.

Mail-Anbieter haben selbst großen Ärger mit Spam-Versendern. So kommt es immer wieder vor, dass Teilnehmer eines Dienstes diesen für Werbesendungen missbrauchen. Dafür haben die Gratis-Services allerdings rigide Regeln: Wer Werbung versendet, fliegt raus. Die meisten Spam-Versender gehen aber raffinierter vor. Sie schicken die Werbepostkarten mit gefälschten Absendern durch das Internet. Häufig werden dabei große Mail-Anbieter als Absendeadressen verwendet. Dann steht hinter dem @ meist der Domain-Name eines Anbieters wie Bigfoot oder Yahoo. Die Folge sind Tausende erboster Rückantworten an den schuldlosen Mail-Anbieter. Das belastet wiederum die Server und lässt den Anbieter in einem schlechten Licht erscheinen. Deshalb gehen Mail-Anbieter auch gerichtlich gegen Spammer vor. So klagte Bigfoot 1997 erfolgreich den selbst ernannten Spam-König Sanford Wallace und seine Firma Cyber Promotions aus dem Geschäft.⁵

Oft nutzen die Spam-Sender auch Sicherheitslücken, die unerfahrene Computer-Verwalter offen lassen. Wer beispielsweise einen Server im Internet betreibt und sein Mail-Versandprogramm nicht ausreichend absichert, kann sicher sein, binnen einer Woche zum unfreiwilligen Aussender von Werbemail zu werden.

Wenn Sie von Spam belästigt werden, sollten Sie nicht die Ruhe verlieren. Kommt die Mail aus den USA, dann halten Sie still. Jede Antwort ist nutzlos. Nutzen Sie keinesfalls das Angebot, sich aus dem Werbeverteiler auszutragen. Denn falls die dort angegebene Adresse überhaupt stimmt, bestätigen Sie mit einer Nachricht dorthin nur, dass es Ihre Mail-Anschrift wirklich gibt. Und damit steigt der Verkaufswert Ihrer Adresse gleich wieder.

Kommt die Werbemail aus deutschen Landen, sollten Sie den Absendern mit einem freundlichen aber deutlichen Hinweis klar machen, dass Sie keine Mail mehr wünschen. Wunder wirkt bisweilen eine Kopie der Mail und Ihrer Antwort an den Postmaster der betreffenden Domain. Denn die Systembetreuer eines Absenders sind nicht unbedingt mit dem Treiben ihres Kunden einverstanden. Um den Systembetreuer eines Providers zu erreichen, setzen Sie statt des Absendernamens einfach »postmaster« ein und belassen die Adresse ab »@«. Aus »Spamie@foo.bar« wird also »postmaster@foo.bar«. Häufig haben Provider auch eine spezielle Adresse, um Missbrauch zu melden. Die lautet »abuse@. . .«. Damit der Provider mit der Spam-Mail etwas anfangen kann, müssen sie diese als Quelltext schicken. Mit Outlook Express

erhalten Sie den Quelltext per Tastendruck auf [Strg]-[F3]. Wenn Sie auf Ihrem PC ausreichend Platz finden, archivieren Sie die Spam-Mails. So machen Sie Wiederholungstäter auffindig und können gegebenenfalls geballtes Beweismaterial an einen Postmaster schicken.

Wenig Nutzen bringt der Eintrag auf einer Robinson-Liste. Denn die wenigsten Versender sehen zuvor in einer solchen Liste nach, bevor sie ihre Botschaften los schicken. Im Gegenteil: Viele sehen in den Listen eher noch eine Gefahr. So gerieten sich im Herbst 2001 der »Interessenverband Deutsches Internet IDI« und die anderen Verbände DDV, DMMV und eco in die Haare. Grund waren die von IDI betreuten eRobinson-Listen. Die IT-Branchenverbände warnten in einer Pressemitteilung vor dem Eintrag in die Listen. Die Verbände befürchteten unter anderem, dass die Listen Ziel von Hackerangriffen werden könnten. Und diese Befürchtungen haben sich schnell bestätigt. Die Liste wurde Ziel eines Angriffs, bei dem der Zugangsschutz gehackt wurde. Als Reaktion auf den Zwischenfall hat der IDI die Listen auf einen vom Internet aus nicht zugänglichen Server transferiert und wird die Liste in Zukunft den Berechtigten nur noch per Mail verschlüsselt zuschicken.

Ein weiterer Weg, ungeliebten Nachrichten aus dem Weg zu gehen, sind Mail-Clients mit Rules, zu Deutsch »Regeln«. Anhand dieser Regeln sortiert ein Client einkommende Nachrichten und wirft Werbe-Messages gleich weg.

Die meisten aktuellen Mail-Clients verfügen über Rule-Systeme. Sie untersuchen Betreff oder Absender einer Nachricht und verschieben verdächtige Messages in einen eigenen Ordner oder in den digitalen Reißwolf. Einige Clients recherchieren sogar in der Nachricht selbst nach verdächtigen Schlüsselwörtern. Welche Begriffe der Mailer sucht und welche Maßnahmen er ergreift, bestimmen Sie. Wenn Ihr Client Rules nicht beherrscht, verwenden Sie einen Online-Filter wie Mail Guard oder E-Filter. Diese Programme durchsuchen die Nachrichten auf dem Server nach Schlüsselbegriffen und ergreifen entsprechende Aktionen. Doch Rules sind kein Allheilmittel: Allzu restriktive Einschränkungen bergen die Gefahr, dass ihnen wichtige persönliche Nachrichten zum Opfer fallen. Zu lasche Regelungen dagegen lassen zu viel Unrat durch. Mit Rules kurieren Sie außerdem nur an den Symptomen herum. Die Nachrichten landen trotzdem in Ihrem Postfach, Übertragungs- und Online-Kosten lassen sich mit Rule-fähigen Clients nicht eindämmen.

2.6 Das müssen Sie beachten, wenn Sie selbst Werbe-Mail versenden wollen

Viele Unternehmen versenden Informationen via E-Mail und sind dennoch keine Spam-Mailer. Wenn Sie selbst Informationen digital versenden wollen, sollten Sie folgende Regeln beachten:

- Die Empfängerin und der Empfänger müssen mit dem Empfang der Werbesendungen einverstanden sein. Das bedeutet: Er muss aktiv die News an-

fordern. Dies kann er per Formular auf Ihrer Homepage oder per E-Mail tun. Senden Sie keinesfalls unerwünschte Werbenachrichten an unbekannte Mail-Teilnehmer.

- Versenden Sie Ihre Nachrichten am besten über einen Listserver. Ihr Internet-Provider sagt Ihnen, ob sie einen solchen Server verwenden können. Wenn das nicht klappt, setzen Sie die Adressen keinesfalls alle in das Adressfeld. Nutzen Sie das Blind-Copy-Feld.
- Teilen Sie am Anfang und Ende jeder Mail mit, wie man sich von der Mailing-Liste löschen lassen kann.
- Halten Sie Häufigkeit und Umfang Ihrer Werbesendungen in Grenzen.
- Schicken Sie nur Mails ab, wenn Sie wirklich etwas Neues zu sagen haben.

Anmerkungen

1 Valentina Djordjevic, <http://duplox.wz-berlin.de/texte/vali>

2 <http://www.heise.de/newsticker/data/hod-23.11.01-001/>

3 Vgl. Telepolis, <http://www.heise.de/tp/deutsch/inhalt/te/7239/1.html>

4 Vgl. Big Brother Awards, <http://www.bigbrotherawards.de/>

5 Vgl. The John Marshall Law School, <http://www.jmls.edu/cyber/cases/spam.html>