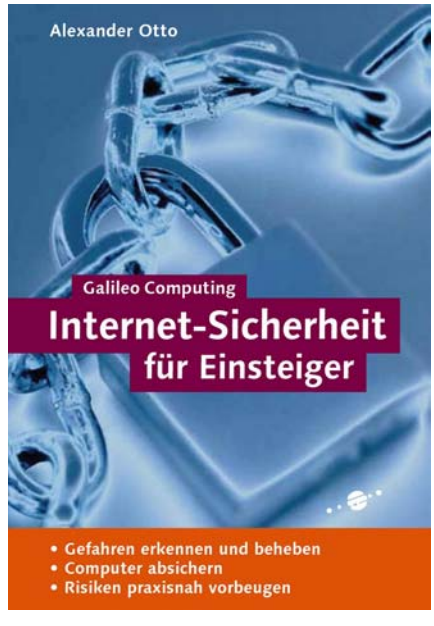
Alexander Otto

Internet-Sicherheit für Einsteiger



Galileo Computing

Inhalt

1 Einleitung

Moderne Informationssysteme und Kommunikationstechniken haben in den letzten Jahren eine unglaublich rasante Entwicklung erlebt. Die globale und länderübergreifende Vernetzung moderner Kommunikationsinfrastrukturen hat dazu geführt, dass die Welt näher zusammengerückt und das viel zitierte »globale Dorf« Realität geworden ist.

Wegen des exponentiellen Wachstums des Internet verlagern sich gesellschaftliche Aktivitäten und Geschäftsprozesse zunehmend ins Internet. Dazu zählen Kommunikation, Einkauf, Handel, Auktionen, Zahlungsverkehr, Unterhaltung und Informationsbeschaffung aller Art.

Immer mehr Menschen entdecken das Internet und gehen in virtuellen Einkaufsmeilen auf Shopping-Tour, koordinieren ihre Finanzen mittels Online-Banking von zu Hause aus oder unterhalten sich mit Gleichgesinnten im virtuellen Chat-Café. Allein in Deutschland sind bereits über 50 Prozent aller Haushalte ans Internet angeschlossen. In vielen Haushalten hat mittlerweile sogar jedes Familienmitglied seinen eigenen PC. Was liegt da näher, als die einzelnen Rechner zu Hause miteinander zu verbinden, um Ressourcen, wie Festplatten, Drucker, Dateien oder einen Internet-Zugang, über das heimische Netzwerk gemeinsam zu nutzen?

Insbesondere das Thema Computer- und Internet-Sicherheit ist in den vergangenen Jahren immer stärker in den Mittelpunkt des öffentlichen Interesses gerückt. Seit dem Internet-Boom Mitte der 90er Jahre vergeht kaum ein Tag, an dem in den Medien nicht über neue Computerviren, E-Mail-Würmer und vermeintlich gefährliche Trojanische Pferde berichtet wird.

Anstelle sachlicher und kompetenter Informationen werden der Öffentlichkeit jedoch meistens nur übertriebene und beängstigende Gruselgeschichten präsentiert, die bei dem unbedarften Anwender nicht selten Panik, Verwirrung und Verunsicherung auslösen. Die Folgen sind übertriebene Reaktionen des Benutzers, die von der Installation mehrerer Antivirus-Programme über die Vermeidung bestimmter Dienstleistungen z. B. Homebanking, bis hin zur völligen Abneigung gegenüber dem Medium Internet reichen.

Sicherlich stimmt es, dass bei der Nutzung des Internet eine Reihe von Risiken und Gefahren für die Privatsphäre des Einzelnen und für die auf dem PC gespeicherten Daten besteht, sonst wäre dieses Buch auch überflüssig.

Die Angst und die Unsicherheit vieler User beruhen aber nur auf einer Sache: auf dem Mangel an richtigen Informationen. Andere Nutzer hingegen verfügen zwar über genügend Informationen, können diese jedoch nur schwer interpretieren und in die Praxis umsetzen. Andere wiederum beschäftigen sich erst gar nicht mit

dem Thema Internet-Sicherheit und verhalten sich entsprechend leichtsinnig, wenn es um den Umgang mit ihren persönlichen Daten oder um den Schutz ihrer Privatsphäre geht.

Für den Anwender ist es daher wichtig, sich sachlich und umfassend über die mit der Nutzung des Internet einhergehenden Gefahrenpotenziale zu informieren, um sich daraufhin in angemessener Form und wirkungsvoll schützen zu können. Einen ersten Schritt haben Sie, liebe Leser, bereits getan, indem Sie sich ein Buch über Internet-Sicherheit angeschafft haben.

Das primäre Ziel dieses Buches ist es, Sie für die Thematik zu sensibilisieren und Ihnen das notwendige Wissen zu vermitteln. So lernen Sie, die mit der Nutzung des Internet verknüpften Gefahren und Risiken realistisch einzuschätzen und zu bewerten, und können dadurch geeignete und sinnvolle Maßnahmen ergreifen, um den PC oder das Heimnetzwerk abzusichern, ohne sich dabei in Ihrem Bewegungsspielraum einschränken zu müssen.

Es ist wichtig zu verstehen, dass alle durch die Nutzung des Internet vorhandenen Risiken im Grunde genommen auf menschliche Schwächen zurückzuführen sind, die ihrerseits wiederum von anderen Menschen ausgenutzt werden müssen, damit ein Risiko zu einer echten Bedrohung wird.

Die allgemein als **Hacker** bezeichneten Zeitgenossen sind anderen Anwendern in der Regel immer einen Schritt voraus und verfügen über ein weit reichendes technisches Know-how. Dieser Informationsvorsprung ist u.a. auch der Grund für die unzähligen Angriffe auf Websites von Regierungen, Unternehmen und anderen öffentlichen Organisationen in den vergangenen Jahren.

Um ein System zu infiltrieren, nutzen Hacker in der Regel eine oder mehrere Schwachstelle(n) auf dem Zielsystem aus.

Dies kann zum Beispiel ein Programmierfehler (so genannter *Bug*) oder aber ein Konfigurationsfehler einer Software sein. Hacker nutzen Bugs in Programmen wie Serversoftware oder Browsern aus, um in entfernte Systeme einzudringen.

E-Mail-Würmer hingegen machen sich die Standardeinstellungen des beliebten E-Mail-Programms Outlook (Express) von Microsoft (und den Umstand, dass der unbedarfte Anwender diese unsicheren Einstellungen beibehält) zu Nutze, um sich in möglichst kurzer Zeit auf so vielen (vernetzten) Rechnern wie möglich ausbreiten zu können. Ein weiteres Beispiel sind Anbieter illegaler Dialer-Programme, die oftmals die Standardeinstellungen des Microsoft Internet Explorer ausnutzen, um sich heimlich auf den Rechner des Anwenders zu kopieren, der sich bei seiner nächsten Einwahl ins Internet unwissentlich mit einer teuren 0190-Nummer verbindet.

Im Verlaufe dieses Buches werden Sie detaillierte Informationen zu den angesprochenen Themen, Techniken und Risiken erfahren und vor allem lernen, wie Sie sich effektiv vor den Gefahren aus dem Internet schützen können.

1.1 Für wen dieses Buch geeignet ist

Dieses Buch richtet sich sowohl an Internet-Einsteiger als auch an Anwender, die mit dem Medium Internet schon Erfahrungen gesammelt haben und/oder ihren Rechner für professionelle Zwecke nutzen. In erster Linie wendet sich das Buch an private Benutzer, die über einen oder mehrere vernetzte Windows-PC(s) mit Internet-Anschluss verfügen. Ich habe mich sehr darum bemüht, das Buch so verständlich und interessant wie möglich zu schreiben, sodass der Inhalt auch für Laien und Neulinge gut verständlich und nachvollziehbar sein sollte. Wenn Sie anderer Meinung sein sollten, wäre ich für Ihr Feedback sehr dankbar. Meine E-Mail-Adresse finden Sie am Ende dieses Kapitels.

Da der Trend im privaten Bereich immer mehr in Richtung lokale Vernetzung und breitbandiger Highspeed-Internet-Zugänge geht, profitieren auch anspruchsvolle Anwender mit einem Heimnetzwerk (mit DSL- oder ISDN-Zugang) von dem hier vermittelten Wissen.

Darüber hinaus haben viele Menschen ihr Büro zu Hause und arbeiten am heimischen Arbeitsplatz mit einem oder mehreren ans Internet angeschlossenen PC(s), auf dem bzw. denen sich geschäftliche und andere sensible Daten befinden, deren Schutz höchste Priorität haben sollte. Aus diesem Grunde sind viele der hier enthaltenen Informationen auch für professionelle Anwender im SoHo-(SmallOffice/HomeOffice-)Bereich, wie Freelancer, Telearbeiter und/oder Selbstständige relevant.

1.2 Wie Sie mit diesem Buch arbeiten können

Dieses Buch ist in zwölf Kapitel gegliedert, bei deren Strukturierung ich mich um einen gewissen didaktischen Aufbau bemüht habe. Sie können das Buch natürlich von der ersten bis zu letzten Seite durcharbeiten, um sich ein detailliertes Bild über die Thematik zu verschaffen. Sie können sich aber auch einzelne Kapitel, die Sie besonders interessieren, gezielt heraussuchen.

Auch als Nachschlagewerk sollte dieses Buch gut geeignet sein.

Fachbegriffe, deren Bedeutung Sie nicht sofort verstehen, können Sie im Glossar nachschlagen, das sich im Anhang des Buches befindet.

Neue Begriffe, die erstmals im Buch auftauchen, sind fett formatiert dargestellt und werden im Glossar ausführlich beschrieben.

Zudem kann Ihnen ein Blick in den Index weiterhelfen, wenn Sie die benötigten Informationen nicht im Glossar finden sollten.

Am Ende eines jeden Kapitels finden Sie zudem einige ausgewählte Internet-Adressen und WWW-Links, über die Sie weitere Informationen zu diesem Thema aus dem World Wide Web beziehen können.

1.3 Inhalt der Kapitel

Kapitel 2: Grundlagen der Datenübertragung im Internet
Um besser nachvollziehen zu können, wie Hacker in fremde Systeme eindringen, wie Trojaner funktionieren oder wie Firewall-Systeme Angriffe aus dem Internet abwehren, ist es hilfreich zu wissen, wie die verschiedenen Mechanismen und Techniken bei der Datenübertragung im Internet zusammenwirken. Sie erhalten zunächst grundlegende Informationen zur Struktur, Funktionsweise und Adressierung des Internet.

Kapitel 3: Gefahren im Internet
In diesem Kapitel werden alle Gefahren und möglichen Bedrohungen, die mit der Benutzung des Internet in Verbindung gebracht werden, ausführlich dargestellt, ohne dabei zunächst zu sehr ins Detail zu gehen, wie man sich davor schützen kann. Themen sind unter anderem Computerviren, Trojaner, Sicherheitslücken in Software-Produkten, Spyware, 0190-Dialer und dergleichen.

Kapitel 4: Datenschutz und Privatsphäre im Internet
Welche Daten gibt der Webbrowser preis? Was sind eigentlich Cookies, und wie funktionieren diese? Wie gehen Internet-Anbieter mit persönlichen Daten ihrer User um? Ist Anonymität im Internet eine Illusion? Wie kann man die Privatsphäre im Internet wahren und sich vor unerwünschten Werbe-E-Mails schützen? Diese und viele andere Fragen werden in diesem Kapitel beantwortet.

Kapitel 5: Schutz- und Abwehrmaßnahmen
Dieses Kapitel beschreibt, welche Möglichkeiten dem Anwender zur Verfügung stehen, um sich vor den in Kapitel 3 aufgezeigten Gefahren zu schützen und die Risiken zu minimieren. Hier wird gezeigt, wie Sie sich verhalten sollten, wenn Sie beispielsweise eine E-Mail mit Anhang erhalten, und wie Sie Ihren Webbrowser und Ihr E-Mail-Programm sicher einstellen, ohne dabei allzu große Einbußen in Bezug auf die komfortable Nutzung hinnehmen zu müssen.

Darüber hinaus wird ausführlich die Funktionsweise von Antiviren-Programmen, Personal-Firewalls und Intrusion-Detection-Systemen beschrieben. Einige dieser Programme werden hier vorgestellt. Sie erhalten wichtige Informationen über ihre Arbeitsweise und Konfigurierbarkeit und erfahren, welche Strategien zur Absicherung Ihres Systems am sinnvollsten sind.

Kapitel 6: Sicherheit im Bereich der Internet-Programmierung
Hier werden Sicherheitsaspekte der wichtigsten Technologien erläutert, die bei der Entwicklung von WWW-Seiten eingesetzt werden. Sie finden Informationen über die Funktionsweise und Risiken von Webtechnologien, die für interaktive Websites benötigt werden, wie ActiveX, JavaScript, Java und PHP.

Kapitel 7: Windows-Sicherheit
Da sich dieses Buch ausschließlich an Windows-User wendet, werden hier spezielle Gefahren dargestellt, die im Zusammenhang mit vernetzten Windows-PCs bestehen. Mit »vernetzt« ist einerseits der einzelne Windows-Rechner mit Internet-Zugang und andererseits der durch ein LAN mit anderen PCs lokal verbundene Windows-PC mit Zugang zum Internet gemeint.

In diesem Kapitel Kapitel beschreibe ich für alle gängigen Windows-Plattformen (Windows 95/98/98SE/NT/2000/XP), wie Sie Schwachstellen und Sicherheitslücken schließen, Ihr Betriebssystem für den Einsatz im Internet härten und damit für mehr Sicherheit Ihrer Daten sorgen.

Kapitel 8: Kryptographie und Datenverschlüsselung
Da ein gewisses Risiko besteht, dass der Inhalt einer E-Mail auf dem Weg vom Sender zum Empfänger ausspioniert wird, beschäftigt sich dieses Kapitel u.a. damit, wie man den Inhalt von E-Mails für unbefugte Personen unleserlich machen kann. Es werden verschiedene symmetrische und asymmetrische Verschlüsselungsverfahren und -algorithmen vorgestellt sowie einige Tools, die diese Verfahren einsetzen. Dabei werden die Funktionen des Verschlüsselungsprogramms PGP erläutert, und u.a. wird auch die Frage beantwortet, warum die US-Regierung immer wieder versucht hat, die Veröffentlichung von PGP zu verhindern.

Kapitel 9: Sicherheit beim Homebanking
In Kapitel 9 werden verschiedene Zugangsverfahren wie PIN/TAN und HBCI vorgestellt und die Vor- und Nachteile bezüglich der Sicherheit aufgezeigt. Sie erhalten nützliche Praxis-Tipps zur sicheren Abwicklung Ihrer Finanztransaktionen über das Internet.

Kapitel 10: Sicherheit beim Online-Shopping
Dieses Kapitel beschreibt, wie (un)sicher das Zahlen mit Kreditkarte im Internet ist und welche Verfahren eingesetzt werden, um Transaktionen abzusichern. Außerdem wird hier beschrieben, was einen guten Online-Shop auszeichnet und was es mit Gütesiegeln auf sich hat.

Kapitel 11: Sicherheit im Heimnetzwerk
In diesem Kapitel zeige ich Ihnen Möglichkeiten auf, wie Sie ein kleines lokales Heimnetzwerk vor Angriffen aus dem Internet schützen können. Es werden verschiedene Firewall-Konzepte vorgestellt, mit denen ein für den Heimanwender angemessener und wirkungsvoller hard- und softwarebasierter Schutz ohne großen Aufwand und Kosten realisiert werden kann.

Kapitel 12: Virtual Private Networks
Virtual Private Networks (VPN) ermöglichen eine gesicherte Datenübertragung zwischen zwei Kommunikationspartnern, wobei die Informationen verschlüsselt über das Internet gesendet werden. Die Daten werden bei diesem Verfahren sozusagen durch einen Tunnel geschleust. Auf diese Weise wird die Integrität der übertragenen Daten gewährleistet.

Auch für private Anwender nimmt der Einsatz dieser Technologie einen immer höheren Stellenwert ein. In diesem Kapitel wird beschrieben, wie Sie in kürzester Zeit ein VPN zwischen einem Sender und einem Empfänger einer Nachricht aufbauen können.

1.4 Noch eine Bitte

Auf Grund der Komplexität und Vielfalt der Thematik ist es trotz sorgfältiger Recherchen und gewissenhafter Überarbeitungen der einzelnen Kapitel durchaus möglich, dass an der einen oder anderen Stelle noch Unstimmigkeiten herrschen. Sollte Ihnen also etwas negativ auffallen oder sollten Sie vielleicht das eine oder andere Thema vermissen, dann lassen Sie es mich bitte wissen. Ihre Anregungen und konstruktive Kritik liegen mir sehr am Herzen und tragen erheblich dazu bei, dieses Buch ständig zu verbessern und aktuell zu halten.

Ich wünsche Ihnen viel Spaß beim Lesen.

Alexander Otto

Vielbach, im Januar 2003
alex0909@t-online.de

4 Datenschutz und Privatsphäre im Internet

Das globale Dorf ist eine Welt, in der man notwendigerweise keine Ruhe und Harmonie findet und in der jeder extrem um die Angelegenheiten des anderen besorgt ist. Das globale Dorf erlaubt tiefe Einblicke in das Leben des anderen. Zwar ist es so riesig wie ein Planet, aber auch so klein wie das Dorf-Postamt.
– frei nach M. McLuhan

Viele Internet-Nutzer unterliegen dem Irrtum, dass sie sich völlig frei und anonym durchs Internet bewegen.

Der Grund für diese Annahme hängt zum einen damit zusammen, dass beim Chatten oder in Newsgroups die eigene Identität vor anderen Teilnehmern verborgen bleibt, zumal man mit anderen Nutzern unter einem Nickname (dt. *Spitzname*) kommuniziert, der keine Rückschlüsse auf die eigene Person zulässt.

Zum anderen sind viele Menschen der Meinung, in der breiten Masse des Internet unterzugehen, weil sie meinen, schließlich nur einer unter vielen Millionen Nutzern zu sein, der sich im Schutz seiner eigenen vier Wände, verborgen hinter seinem Computer, durch das Netz bewegt.

Doch der Schein trügt. Denn das Internet ist eine riesige Informationsquelle, die nicht nur Websites und HTML-Dokumente über Suchmaschinen findet, sondern die auch über einzelne Personen Auskunft geben kann. Wenn Sie einen Beitrag in ein Forum stellen, kann dieser noch über Jahre im Internet gefunden werden.

Vielen Usern ist nicht bewusst, dass sie mit jedem Schritt im Internet Spuren hinterlassen. Spätestens dann, wenn sich die Anzahl unerwünschter Werbe-E-Mails häuft, beginnt man sich Gedanken zu machen.

Tatsache ist: Wer keine Initiative ergreift und nicht selbst für den Schutz seiner Privatsphäre sorgt, der wird sich auch niemals anonym im Internet bewegen können.

Zwar gibt es viele Organisationen, Vereine und Initiativen im Web, die sich für den Datenschutz und die Rechte der Bürger im Internet einsetzen, doch der Weg dorthin will erst einmal gefunden werden.

Bereits Ihr Provider, über den Sie sich ins Internet einwählen, kann herausfinden, welche Websites Sie in einem bestimmten Zeitraum besucht haben, da schließlich alle Anfragen über die Server des Providers laufen. Ein genaues Protokollieren von User-Aktivitäten war bis vor kurzem lediglich zu Abrechnungszwecken erlaubt.

Mittlerweile sind Internet Service Provider in Deutschland gesetzlich dazu verpflichtet, sämtliche Online-Aktivitäten ihrer Kunden zu protokollieren und langfristig zu archivieren.

Anonymität im Internet existiert nicht wirklich und ist lediglich eine trügerische Illusion.

Warum das so ist und wie Sie Ihre Privatsphäre im Internet wahren, wird in diesem Kapitel behandelt.

4.1 User-Tracking

Viele Unternehmen haben ein Interesse daran zu erfahren, woher ihre Besucher kommen und wie oft ihre Website innerhalb eines bestimmten Zeitraums angeklickt wurde.

Die Betreiber kommerzieller Angebote beobachten daher das Nutzungsverhalten ihrer Besucher. Dadurch können umfangreiche Statistiken darüber geführt werden, wie häufig die Website am Tag, pro Woche oder im Monat besucht wurde, welche Seiten durchschnittlich am häufigsten angeklickt wurden, wie lange die Seiten angeschaut wurden und über welchen Link ein Besucher zu einer bestimmten Website gefunden hat.

Eine solche Quellenanalyse, ob ein Besucher nun über eine Suchmaschine oder einen bestimmten Link zu einem Webangebot gefunden hat, ist für das Online-Marketing wichtig.

Mit Hilfe unterschiedlicher Tracking-Technologien wird auf diese Weise ein bedarfs- und bedürfnisorientiertes Online-Marketing möglich, wodurch der Betreiber einer Website sein Angebot gezielter auf die Interessen der Benutzer abstimmen kann.

Solange die gesammelten Daten nicht mit einer bestimmten Person assoziiert werden, ist dagegen auch nichts einzuwenden. Allerdings geht ein solches **User-Tracking** in den meisten Fällen zu Lasten der Anonymität und der Privatsphäre, insbesondere dann, wenn folgende Tracking-Instrumente eingesetzt werden:

- Session-IDs (Cookies)
- Webwanzen
- Spyware

4.2 Cookies

Cookies (dt. *Kekse*) sind kleine Textdateien, die viele Webserver auf dem Rechners des Besuchers einrichten, um den Anwender beim nächsten Besuch wiedererkennen zu können, ohne dass sich der Anwender mit Benutzername und Passwort

authentifizieren muss. Ohne Cookies kann ein Anwender vom Betreiber eines Online-Angebotes zwar anhand der IP-Adresse identifiziert werden, allerdings nur für die Dauer der Online-Sitzung. Wählt sich der User zu einem anderen Zeitpunkt ins Internet ein, erhält er in der Regel eine neue IP-Adresse und kann beim erneuten Besuch einer bestimmten Website nicht wiedererkannt werden.

Durch Cookies ist es möglich, dass Sie beim Besuch einer Website persönlich begrüßt werden oder dass die Einstellungen, die Sie dort in einer vorherigen Sitzung vorgenommen haben, nicht verloren gehen und damit beim nächsten Besuch wieder zur Verfügung stehen. Ein Beispiel für den sinnvollen Einsatz eines Cookies wäre ein Web-Portal, bei dem sich der Besucher für ihn interessante Themengebiete auswählen kann. Diese Informationen werden an den Browser gesendet, der die übermittelten Daten in einer Cookie-Datei auf dem lokalen Rechner des Anwenders speichert. Jedes Mal, wenn der User diese Website besucht, liest der Webserver den Inhalt des Cookies von der lokalen Festplatte des Anwenders und generiert anhand dieser Informationen eine individuelle Willkommensseite, auf der dem Besucher aktuelle Nachrichten, Informationen oder Angebote zu seinen Interessengebieten angezeigt werden.

Vielleicht waren Sie schon einmal auf den Seiten des Online-Buchhändlers Amazon.de. Alle Produkte, die Sie dort kaufen, legen Sie zunächst in einen virtuellen Einkaufskorb. Der Inhalt dieses Warenkorbs wird in Form eines Cookies auf Ihrem PC gespeichert.

Abbildung 4.1 Die Warenkorb-Funktion von Amazon.de

Sobald Sie alle Artikel im Einkaufswagen abgelegt und Ihre persönlichen Daten (Name, Anschrift, E-Mail-Adresse etc.) eingegeben haben, können Sie die Bestellung absenden. Sollten Sie Ihre virtuelle Einkaufstour aus irgendeinem Grund

unterbrechen, können Sie Ihren Einkauf zu einem späteren Zeitpunkt fortsetzen, ohne dabei alle zuvor ausgesuchten Produkte noch einmal auswählen und in den Warenkorb legen zu müssen.

So gesehen sind die kleinen digitalen Kekse eine sehr nützliche und praktische Sache, die dem Anwender das Leben im Web versüßen kann. Die Kehrseite der Medaille ist aber, dass alle Schritte des Users überwacht und individuelle Interessen ausgewertet werden können. Ein solches Benutzerprofil kann dann für zielgerichtete Werbung verwendet oder für teures Geld an Dritte weiterverkauft werden. Zudem müssen Sie vor der ersten Bestellung in einem Online-Shop persönliche Angaben, wie Name, Adresse, Bankdaten, E-Mail-Adresse etc., machen. Wenn Sie bestimmte Produkte kaufen oder sich für bestimmte Artikel interessieren, kann der Shop-Betreiber ein umfangreiches Benutzerprofil erstellen. Die gesammelten Informationen können dann zusammen mit Ihren Stammdaten weiterverkauft werden. Dies ist jedoch nur mit der ausdrücklichen Zustimmung des Betroffenen erlaubt.

Hinweis Personenbezogene Daten dürfen grundsätzlich nur dann erhoben, verarbeitet und genutzt werden, wenn dies rechtlich erlaubt ist oder der Anwender explizit zugestimmt hat. Wenn Daten dafür verwendet werden, einen Vertrag zu erfüllen, handelt es sich um eine vom Vertragszweck abgedeckte Übermittlung. Sollen Daten aber zweckentfremdet eingesetzt werden, bedarf es einer gesonderten Einwilligung der betroffenen Person. Eine Verlinkung auf eine Datenschutzerklärung oder ein einfacher Hinweis reicht für eine Zustimmung des Anwenders nicht aus. Laut § 4 Abs. 2 des Teledienste-Datenschutzgesetzes (TDDSG) müssen folgende Voraussetzungen für eine elektronische Einwilligung gegeben sein:

- Eine Einwilligung kann nur durch eine bewusste und eindeutige Handlung des Anwenders erfolgen.
- Die Einwilligung muss protokolliert werden
- Der Anwender muss die Einwilligung jederzeit inhaltlich einsehen können.

Verzweifelte User müssen sich tagtäglich mit einem Wust an Werbe-E-Mails herumschlagen, sodass es ihnen schwer fällt, die wirklich wichtigen Nachrichten herauszusuchen, die unter dem Berg an Datenmüll begraben sind.

Aus diesem Grunde sollte man als Anwender darauf achten, dass man seine Spuren im Netz verwischt oder das Einrichten von Cookies nur bestimmten Websites erlaubt.

Wie Sie diese Vorhaben in die Praxis umsetzen können, ohne dabei auf die Vorzüge von Cookies verzichten zu müssen, erfahren Sie in den folgenden Abschnitten.

4.2.1 So werden Cookies missbraucht

Werbefirmen wie Doubleclick platzieren Werbegrafiken (so genannte **Banner**) gegen Bezahlung auf unterschiedlichen kommerziellen Websites und bei Online-Diensten.

Das Ziel der Werbestrategen besteht darin, für Produkte zu werben, die den User auch tatsächlich interessieren. Dazu muss der Besucher einer Website jedoch aus seiner Anonymität herausgerissen und transparent gemacht werden.

Wenn Sie eine Site im World Wide Web besuchen, die einen Vertrag mit einer Werbefirma geschlossen hat, wird neben dem gewünschten Inhalt das Werbebanner vom Server der Werbefirma geladen und gleichzeitig ein Cookie auf Ihrem Rechner eingerichtet. In diesem Cookie sind z. B. Informationen darüber enthalten, welche Seiten Sie wann und wie oft angeklickt haben. Wenn Sie eine andere Website aufrufen, die ebenfalls ein Vertragspartner eines Werbenetzwerkes ist, werden die im Cookie enthaltenen Informationen an den Server der Werbefirma übertragen und ein weiterer Cookie auf Ihrem Rechner eingerichtet.

Wenn Sie sich beispielsweise für Börsenberichte, Fußball und Computerspiele interessieren und regelmäßig entsprechende WWW-Angebote zu diesen Themen besuchen, kristallisiert sich ein immer feineres Profil Ihrer persönlichen Interessen heraus. Wenn ein Werbeunternehmen also weiß, welche Webseiten Sie besuchen, können aus diesen Informationen Ihre Vorlieben und Bedürfnisse abgeleitet werden.

Werbefirmen können auf diese Weise gezielte Werbebanner auf Webseiten einblenden, um sich an den individuellen Bedürfnissen des Besuchers zu orientieren. Je mehr Sie also im Web unterwegs sind, desto mehr Werbung werden Sie im Web entdecken, die Sie tatsächlich interessiert. Das mag vielleicht nicht schlecht sein – immer noch besser als Werbung, die Sie überhaupt nicht tangiert. Viele User empfinden Werbung im Internet jedoch allgemein als störend und möchten in erster Linie informiert und unterhalten werden. Zudem können sich durch die zahlreichen Werbegrafiken auch die Ladezeiten von Websites erheblich erhöhen, was die Nerven vieler Modem- und ISDN-Nutzer überstrapaziert. DSL-User dürfte dies zwar wenig interessieren, aber (noch) längst nicht jeder hat einen solchen Highspeed-Internetzugang.

Solange die Informationen, die über Sie im Web gesammelt werden, nicht mit Ihrer Person unmittelbar in Verbindung gebracht werden, sind Cookies völlig harmlos. Wenn jedoch die E-Mail-Adresse mit ins Spiel kommt, wird es ernst.

Denn falls ein User in einem Online-Formular seine E-Mail-Adresse einträgt und abschickt, werden auch diese Informationen in einem Cookie gespeichert. Die Werbefirma kennt also nicht nur irgendeinen User und dessen Vorlieben und Interessen, sondern auch seine E-Mail-Adresse, die zusammen mit Informationen über Benutzerinteressen an Dritte verkauft werden kann.

Der Käufer kann damit gezielte Werbe-E-Mails an Internet-Anwender senden. Viele Anwender fühlen sich durch Werbe-E-Mails jedoch belästigt, auch wenn es sich um Produkte handelt, an denen sie im Grunde genommen interessiert sind. Ärgerlich ist, wenn man beim Abrufen seines Postfaches, E-Mails von Freunden, Bekannten und Geschäftspartnern nicht auf Anhieb findet, weil man sich zunächst durch einen Berg voller **Junk**-Mails (engl. Junk = *unbrauchbares Material Krempel, Müll*) durcharbeiten muss.

Darüber hinaus funktioniert das oben beschriebene Prinzip natürlich nicht nur bei Websites, sondern auch bei HTML-formatierten E-Mails. E-Mail-Programme wie Outlook (Express) können ohne Probleme HTML-formatierte E-Mails verarbeiten. Outlook Express greift hierzu auf die Funktionen des Internet Explorer zurück. Wenn der Internet Explorer also so eingestellt ist, dass er alle Cookies akzeptiert, dann gelten diese Einstellungen auch für Outlook (Express).

Eine E-Mail kann so präpariert werden, dass die E-Mail-Adresse des Empfängers eindeutig der vom Webserver eingebundenen Bannergrafik zugeordnet werden kann. Die im Cookie enthaltenen Benutzerinformationen, können damit nicht mehr länger nur mit einem anonymen Benutzer, sondern auch mit einer E-Mail-Adresse assoziiert werden.

Die Möglichkeit, Cookies zusätzlich per E-Mail einzurichten, führt zu einem regelrechten Teufelskreis:

Sie surfen im World Wide Web, füllen hier und da ein Online-Formular aus, hinterlassen hier und da Ihre E-Mail-Adresse und erhalten dadurch immer mehr E-Mail-Werbung. Viele dieser Werbe-E-Mails richten wiederum selbst Cookies auf Ihrem Rechner ein, was zu einem exponentiellen Anstieg von Werbe-E-Mails führt usw.

Wenn Ihnen ein solches Szenario erspart bleiben soll, dann sollten Sie Abschnitt 4.2.3 lesen, in dem beschrieben wird, wie Sie durch gezieltes Cookie-Management Ihre Privatsphäre wahren, ohne dabei gänzlich auf Cookies verzichten zu müssen, die für das Funktionieren vieler Websites zwingend erforderlich sind.

4.2.2 Cookie-FAQs

Viele Internet-User äußern immer wieder Bedenken, dass Cookies nicht nur die Privatsphäre gefährden, sondern auch noch andere Risiken bergen.

In den folgenden Abschnitten werden häufig gestellte Fragen (FAQ – Frequently Asked Questions) von Anwendern zu diesem Thema beantwortet.

Frage 1: Können durch Cookies Viren übertragen werden?

Da Cookies keine ausführbaren Programme, sondern lediglich einfache Textdateien sind, kann innerhalb eines Cookies kein (schädlicher) Code ausgeführt werden. Ein Computervirus könnte zwar über ein Cookie übertragen und auf dem Rechner des Anwenders gespeichert werden. Ausgeführt werden könnte der Virus jedoch nicht.

Allerdings kann nicht völlig ausgeschlossen werden, dass eine Cookie-Datei auf Grund eines Bugs im Browser oder eines Fehlers im Betriebssystem auf dem Rechner des Anwenders ausgeführt wird. Bei älteren Netscape-Versionen (Netscape Navigator 2 und 3) sind derartige Bugs in der Tat schon aufgetreten. Diese wurden jedoch unmittelbar nachdem sie entdeckt wurden, von Netscape mit der Veröffentlichung eines Sicherheits-Patches behoben. Der Fall, dass ein Cookie einen Virus enthält, der auf Grund eines Browserbugs tatsächlich ausgeführt wird, ist zwar extrem unwahrscheinlich, trotzdem sollten Netscape-Anhänger, die noch mit älteren Netscape-Versionen ins Web gehen, entweder ein Update auf Netscape 7 vornehmen oder auf den Open-Source-Browser Mozilla umsteigen, zumal ältere Browser-Versionen im Allgemeinen eine Reihe weiterer sicherheitskritischer Fehler enthalten.

Frage 2: Können die in Cookies gespeicherten Informationen einer Person zugeordnet werden?

In der Regel werden an den Server, der den Cookie erzeugt hat, keine Benutzernamen übertragen, sodass die in Cookies enthaltenen Daten nur einer IP-Adresse (einem Rechner) zugeordnet werden können – es sei denn, der Cookie wird dazu verwendet, Benutzernamen und Passwort zu speichern, über die man sich bei einem Online-Dienst einloggen kann. Dies ist beispielsweise beim Online-Auktionshändler eBay.de der Fall. Da das Risiko besteht, dass Cookies während der Datenübertragung von Unbefugten mitgelesen werden könnten, werden Cookies häufig mittels SSL verschlüsselt übermittelt.

Frage 3: Ist es möglich, dass Cookies in falsche Hände geraten?

Da Cookies für gewöhnlich nicht verschlüsselt, sondern im Klartext übertragen werden, können Cookies, die während des Datentransfers abgehört werden, von unberechtigten Personen gelesen werden.

Außerdem wäre es möglich, den Domainnamen des Servers, der berechtigt ist, einen Cookie einzurichten und von einem Client zu empfangen, durch DNS-Spoofing zu verfälschen. Dies hätte zur Folge, dass ein Cookie auch an einen Server übertragen werden könnte, der den Cookie gar nicht eingerichtet hat.

4.2.3 Cookie-Management im Browser

Um einen Cookie von einem Server empfangen zu können, muss Ihr Browser in der Lage sein, Cookies zu akzeptieren. Fast alle Webbrowser wie Netscape, Mozilla oder der MS Internet Explorer sind standardmäßig so konfiguriert, dass alle Cookies zugelassen sind. Wenn Sie diese Einstellungen beibehalten, werden Cookies von allen Websites akzeptiert, die versuchen, einen Cookie einzurichten.

In RFC 2901 werden unter dem Aspekt des Schutzes der Privatsphäre vor Cookies unter anderem folgende Forderungen an die Hersteller von Webbrowsern gestellt, die bisher nur teilweise in die Praxis umgesetzt wurden:

- Der Browser sollte eine Option bieten, mit der der Versand und der Empfang von Cookies verhindert wird.
- Der Anwender sollte über das Einrichten eines Cookies informiert werden.
- Der Browser sollte sicherstellen, dass ein Server auch tatsächlich die Berechtigung hat, einen Cookie anzufordern.
- Der Browser sollte die Möglichkeit bieten, eine Warnmeldung herauszugeben, wenn beim Besuch einer Website ein Cookie auf dem Rechner des Anwenders eingerichtet werden soll, dessen Ursprung ein anderer ist als der aufgerufene Domainname.
- Der Browser sollte dem User anzeigen, wenn ein Cookie am Ende einer Sitzung gespeichert wird.
- Der Anwender sollte jederzeit die Inhalte aller gespeicherten Cookies einsehen können.

4.2.4 Cookie-Management mit Netscape 7 und Mozilla

Die Verwaltung und Konfiguration von Cookies sind bei Netscape 7 und Mozilla 1.1 schon recht zufrieden stellend und bieten dem Anwender gute Kontrollmöglichkeiten zur Behandlung von Cookies. Hierzu hat Netscape einen hervorragenden Cookie-Manager in die neueste Version 7 des Webbrowsers integriert, mit dem Cookies übersichtlich und komfortabel verwaltet werden können.

Die umfangreichen Cookie-Kontrollfunktionen sind bei Netscape 7 mittlerweile besser als beim Internet Explorer 6. Beispielsweise ist es beim Netscape-Browser nun möglich, einzelne Cookies auszuwählen und zu löschen. Beim IE 6 hingegen können nur alle Cookies auf einmal gelöscht werden.

Zu den Cookie-Optionen gelangen Sie über die Menüleiste **Bearbeiten · Einstellungen · Privatsphäre & Sicherheit · Cookies** beziehungsweise **Edit · Preferences · Privacy & Security · Cookies**

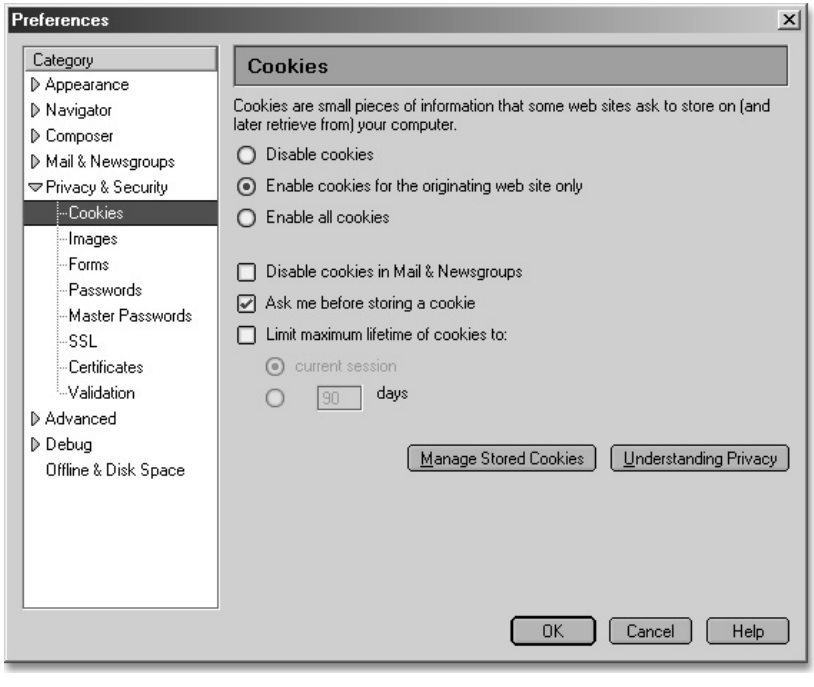


Abbildung 4.2 Cookie-Einstellungen von Mozilla

Sie können nun entscheiden, ob Sie alle Cookies oder gar keinen akzeptieren wollen. Zusätzlich dazu können Sie festlegen, dass nur Cookies an denjenigen Server übermittelt werden dürfen, der die Sitzung eröffnet beziehungsweise der den Cookie bei Ihnen eingerichtet hat. Wenn Sie Letzteres möchten, klicken Sie einfach auf den Radio-Button »Nur an die ursprüngliche Seite gesendete Cookies akzeptieren« (»Enable cookies for the originating web site only«).

Für den Fall, dass Sie erst während des Surfens entscheiden wollen, welche Website einen Cookie setzen darf und welche nicht, können Sie Netscape 7/Mozilla anweisen, Sie vor jeder Annahme eines Cookies um Erlaubnis zu bitten. Jedes Mal wenn Sie eine Website aufrufen, die einen Cookie einrichten will, öffnet der Browser bei dieser Vorgabe einen Dialog, den Sie entweder mit Ja oder Nein

bestätigen müssen. Es kann zwar lästig sein, wenn Sie während des Surfens permanent danach gefragt werden; auf der anderen Seite wird Ihnen dadurch erst bewusst, wie viele Websites tatsächlich versuchen, einen Cookie auf Ihrem Rechner zu platzieren.

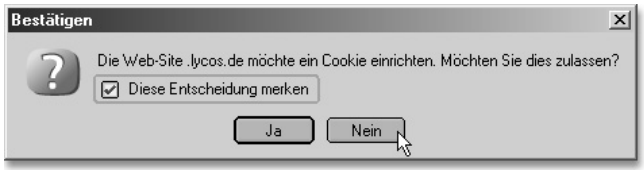


Abbildung 4.3 Der Bestätigungsdialog von Netscape 7

Bei Websites, die Sie häufig und regelmäßig besuchen, wäre es natürlich unsinnig, wenn Sie jedes Mal bestätigen müssten, ob ein Cookie gespeichert werden darf oder nicht, da Ihre Entscheidung bei ein und derselben Website stets die gleiche sein wird.

Damit Sie während einer Online-Sitzung nicht ununterbrochen von Ihrem Browser mit Fragen zur Behandlung von Cookies gestört werden, können Sie Ihrem Browser mitteilen, dass er sich diejenigen Websites dauerhaft merken soll, von denen Sie Cookies akzeptieren oder nicht akzeptieren. Wenn Ihr Browser also einen Dialog wie in Abbildung 4.3 anzeigt und Sie beispielsweise möchten, dass der Cookie weder zum derzeitigen Zeitpunkt noch zukünftig von dieser Website eingerichtet werden soll, dann setzen Sie zunächst ein Häkchen in das Kontrollkästchen »Diese Entscheidung merken« (»Remember this Decision«) und klicken anschließend auf **Nein**. Wenn Sie nun die Website zu einem späteren Zeitpunkt erneut aufrufen, wird der Cookie automatisch von Ihrem Browser abgelehnt.

Der Cookie Manager

Es kann vorkommen, dass man, anstatt einen Cookie dauerhaft abzulehnen, den Browser versehentlich angewiesen hat, das Speichern von Cookies dauerhaft zuzulassen. Wenn Sie in unter **Bearbeiten · Einstellungen · Privatsphäre & Sicherheit · Cookies** auf die Schaltfläche **Gespeicherte Cookies verwalten** (**Manage Stored Cookies**) klicken, öffnet sich der Cookie-Manager von Netscape 7 bzw. Mozilla.

Im Register **Gespeicherte Cookies** (**Stored Cookies**) sind sämtliche Cookies, die sich in der Datei `cookies.txt` befinden, aufgeführt.

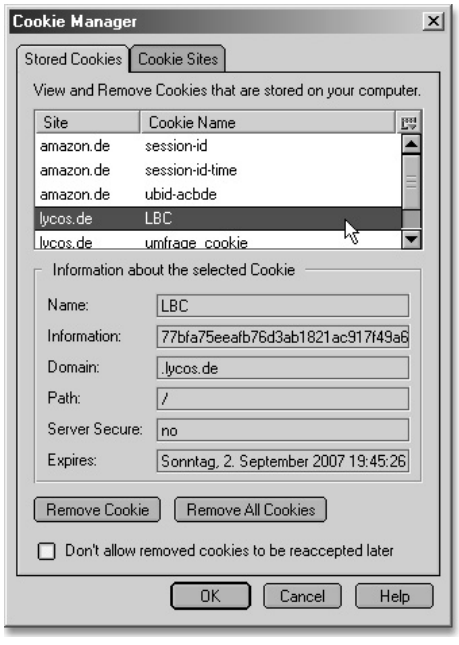


Abbildung 4.4 Der Cookie Manager von Mozilla 1.1

Hier erkennen Sie außerdem, welche Werte den Umgebungsvariablen `NAME` (»Name«), `domain` (»Host«), `path` (»Pfad«), `server secure` (»Server, sicher«) und `expires` (»Läuft ab«) zugewiesen wurden. Abbildung 4.4 zeigt diese Attribute unter Mozilla 1.1 (englische Version). Diese Attribute werden im Cookie Manager angezeigt, wenn Sie einen dort gespeicherten Cookie auswählen.

Sie können einzelne Cookies oder aber auch alle Cookies im Cookie Manager manuell löschen. Zudem können Sie hier festlegen, dass einmal gelöschte Cookies zukünftig nicht mehr akzeptiert werden dürfen (»Don't allow removed cookies to be reaccepted later«), was jedoch nicht bedeutet, dass gleichzeitig auch der Server, der der von Ihnen gelöschte Cookie zuvor eingerichtet hat, überhaupt keine Cookies mehr an Ihren Browser senden darf. Das Verbot bezieht sich lediglich auf einen einzelnen, universellen Cookie, unabhängig davon von welchem Server er eingerichtet wurde.

Neben dem Register **Stored Cookies** befindet sich der Reiter **Cookie Sites**. Hier werden jene Websites angezeigt, die befugt sind, Cookies einzurichten, und solche, die keine Berechtigung haben, Cookies an Ihren Browser zu senden. Diese Regeln wurden vom Anwender während des Surfens im Web festgelegt.

Unter »Sites« befindet sich eine Website, die mit Cookies arbeitet. Daneben befindet sich unter »Status« entweder der Eintrag »Web-Site kann keine Cookies einrichten« (»site cannot set cookie«) oder »Web-Site kann Cookies einrichten« (»site can set cookie«)

Sie können die von Ihnen festgelegte Regel wieder aufheben, indem Sie eine bestimmte Seite aus der Liste auswählen, die Sie entfernen möchten (siehe Abbildung 4.5), und anschließend auf die Schaltfläche **Web-Site entfernen** (**Remove Site**) klicken.

Sie können aber auch alle Einträge auf einmal löschen, indem Sie den Button **Alle Web-Sites löschen** (**Remove All Sites**) anklicken.

Wünschenswert wäre hier noch die Möglichkeit, nur den einer Website zugewiesenen Cookie-Status verändern zu können, ohne dabei den gesamten Eintrag komplett löschen zu müssen.

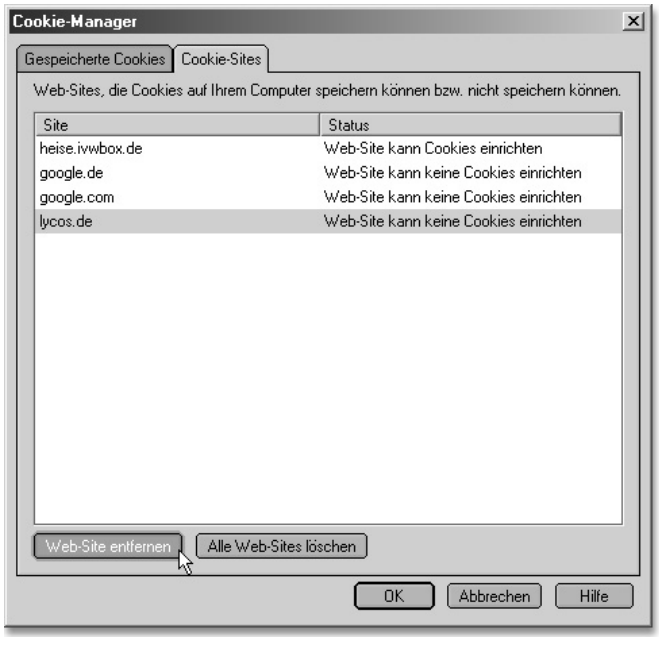


Abbildung 4.5 Der Cookie-Manager von Netscape 7

Privatsphären-Stufen mit P3P

Eine weitere Option zur Behandlung von Cookies in Netscape 7 heißt »Cookies auf der Grundlage von Privatsphären-Stufen aktivieren«.

Damit ermöglicht Netscape 7 ein Cookie-Management, das auf dem so genannten **P3P**-Standard basiert. P3P (Platform for Personal Privacy Preferences Project) ist ein Protokoll, das vom **W3C** (World Wide Web Consortium) speziell für die Übertragung benutzerspezifischer Daten konzipiert wurde, um die Privatsphäre des Anwenders besser zu schützen. Eine Datenübertragung über P3P kommt nur dann zustande, wenn der Anbieter einer Website in einer so genannten **Privacy Policy** (Privatsphärenrichtlinie, Datenschutzrichtlinie) erklärt, welche Daten ermittelt werden und zu welchem Zweck dies geschieht. Der Anwender muss dieser Datenschutzerklärung explizit zustimmen.

In Abbildung 4.6 ist dargestellt, welche Möglichkeiten Netscape 7-User haben, Cookies auf der Grundlage von Privatsphären-Stufen zu akzeptieren.

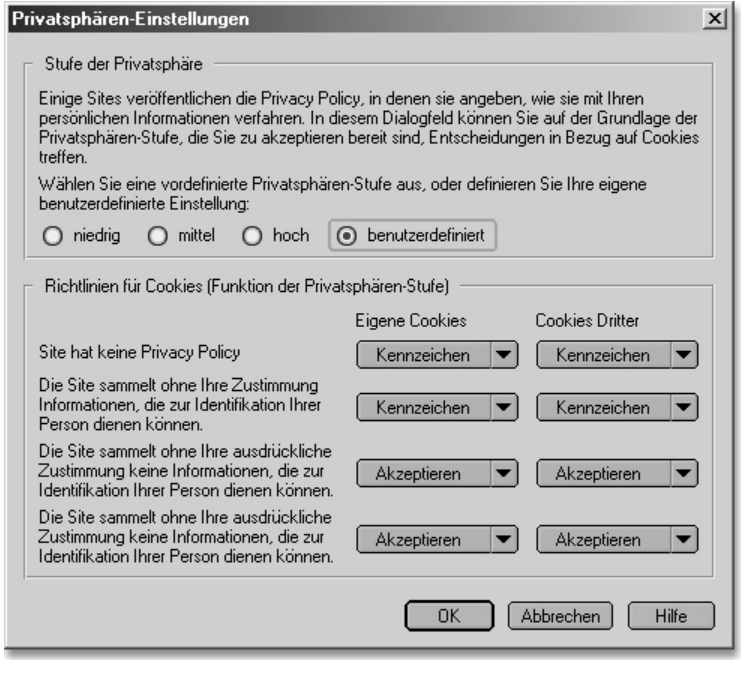


Abbildung 4.6 Privatsphären-Stufen in Netscape 7

Mit der hier festgelegten Privatsphären-Stufe können Sie darüber entscheiden, wie der Browser Cookies gemäß den P3P-Richtlinien, die von manchen Websites veröffentlicht werden, behandeln soll. Sie können dabei Richtlinien für »Eigene Cookies« und Richtlinien für »Cookies Dritter« festlegen.

Unter »Eigene Cookies« sind solche Cookies zu verstehen, die von der Website eingerichtet werden, die Sie besuchen. »Cookies Dritter« sind fremde Cookies, die von anderen Websites als der besuchten Website eingerichtet werden.

Ihnen stehen die in Tabelle 4.1 aufgeführten Privatsphären-Stufen zur Auswahl.

Privatsphären-Stufe	Beschreibung
Niedrig	Wählen Sie diese Option, wenn Sie alle Cookies ungeachtet der Privatsphärenrichtlinien einer Website akzeptieren möchten. Der Browser akzeptiert alle eigenen Cookies und alle Cookies Dritter, wobei fremde Cookies von Websites gekennzeichnet werden, die darauf hinweisen, dass sie persönliche Informationen ohne Ihre Zustimmung sammeln. Alle gekennzeichneten Cookies werden im Cookie-Manager im Register »Gespeicherte Cookies« in der Statusspalte als gekennzeichnet angezeigt. Um sich den Cookie-Status anzeigen zu lassen, klicken Sie im Cookie-Manager auf das entsprechende Symbol oben rechts und machen einen Haken bei »Status«. Wenn ein Cookie gekennzeichnet wird, zeigt der Cookie-Manager das Cookie-Benachrichtigungssymbol in der rechten unteren Ecke des Browserfensters an. Um sich ausführlichere Informationen zu den gekennzeichneten Cookies anzeigen zu lassen, klicken Sie einfach darauf.
Mittel	Wählen Sie diese Option, wenn Sie sowohl eigene Cookies als auch fremde Cookies akzeptieren und kennzeichnen möchten, die von Websites übertragen werden, die möglicherweise persönliche Informationen ohne Ihre Zustimmung sammeln. Dies ist die Standardeinstellung.
Hoch	Diese Option entspricht der Standardeinstellung mit der Ausnahme, dass Cookies Dritter dann abgelehnt werden, wenn sie von Websites übertragen werden, die Informationen ohne Ihre ausdrückliche Zustimmung sammeln. Außerdem werden Cookies Dritter, die ohne Ihre Zustimmung persönliche Informationen an die fremde Website übertragen, nach Beendigung der Sitzung wieder gelöscht.
Benutzer-definiert	Wählen Sie diese Option, wenn Sie Ihre eigenen benutzerdefinierten Richtlinien für Cookies festlegen möchten. Um diese zu ändern, wählen Sie in den Dropdown-Menüs des Dialogfeldes im Bereich »Richtlinien für Cookies« die gewünschten Optionen aus. Die zur Verfügung stehenden Richtlinien werden im Folgenden beschrieben.

Tabelle 4.1 Netscape 7, Privatsphären-Stufen

Wenn Sie unter »Stufe der Privatsphäre« die Option »benutzerdefiniert« auswählen, stehen Ihnen acht Kategorien zur Verfügung, in denen Sie über eine Dropdown-Liste jeweils zwischen vier Einstellungen wählen können:

- **Akzeptieren** – Alle Cookies in der Kategorie akzeptieren.
- **Sitzung** – Alle Cookies in der Kategorie nur für die aktuelle Sitzung akzeptieren, das heißt so lange, bis Sie den Browser schließen.
- **Ablehnen** – Alle Cookies in der Kategorie ablehnen.

- **Kennzeichen** – Der Cookie-Status wird auf der Registerkarte **Gespeicherte Cookies** des Cookie-Managers in der Statusspalte als »gekennzeichnet« aufgeführt, und das Cookie-Benachrichtigungssymbol wird angezeigt.

Diese Richtlinien können Sie sowohl für eigene Cookies als auch für Cookies von Drittanbietern festlegen.

Dabei stehen Ihnen für jeden Cookie-Typ jeweils vier Kategorien zur Verfügung, bei denen Sie die oben genannten Parameter »Akzeptieren«, »Sitzung«, »Ablehnen« oder »Kennzeichen« auswählen können:

- **Site hat keine Privacy Policy** – Hier legen Sie fest, wie Sie mit Cookies verfahren wollen, die von Websites übertragen werden, die über keine Datenschutzrichtlinien verfügen. Da Sie bei Websites ohne Privacy Policy keine Möglichkeit haben festzustellen, welche Informationen sie sammeln, empfiehlt es sich, solche Cookies abzulehnen.
- **Die Site sammelt ohne Ihre Zustimmung Informationen, die zur Identifikation Ihrer Person dienen können** – Die Website veröffentlicht zwar eine Privatsphärenrichtlinie, bittet allerdings nicht um Ihre Erlaubnis, um persönliche Informationen zu sammeln.
- **Die Site sammelt ohne Ihre ausdrückliche Zustimmung keine Informationen, die zur Identifikation Ihrer Person dienen können** – Die Website sammelt immer persönliche Informationen über Sie, außer Sie lehnen dies ausdrücklich ab und verweigern Ihre Zustimmung.
- **Die Site sammelt ohne Ihre ausdrückliche Zustimmung keine Informationen, die zur Identifikation Ihrer Person dienen können** – Die Website sammelt nur dann persönliche Informationen, wenn Sie explizit Ihre Zustimmung dazu geben.

Etwas verwirrend ist, dass die beiden zuletzt aufgeführten Kategorien vom Wortlaut her völlig identisch sind, obwohl beide Kategorien unterschiedliche Bedeutungen haben. Der Unterschied ist, dass sich die erstgenannte Kategorie auf Websites bezieht, die bei einem Besuch automatisch einen Cookie auf Ihrem Rechner ablegen, solange Sie dies nicht ausdrücklich untersagen.

Die zuletzt aufgeführte Kategorie bezieht sich hingegen auf Websites, die erst dann einen Cookie auf dem Rechner des Anwenders ablegen, wenn der Anwender ausdrücklich zugestimmt hat.

4.2.5 Cookie-Verwaltung mit dem Internet Explorer 6

Der Internet Explorer 6 verfügt gegenüber älteren Versionen über eine weiterentwickelte Cookie-Filterung, die wie bei Netscape 7 auf dem P3P-Standard basiert, sodass auch Website-Anbieter, die über eine Privacy Policy verfügen, vom IE 6

erkannt werden. Wenn eine aufgerufene Website nicht den von Ihnen vorgenommenen Datenschutzeinstellungen entspricht, dann informiert der Microsoft-Browser Sie darüber.

Zu den Cookie-Einstellungen des Internet Explorer 6 gelangen Sie, indem Sie aus der Menüleiste **Extras · Internetoptionen** wählen und anschließend auf die Registerkarte **Datenschutz** klicken. Hier können Sie über einen Schieberegler zwischen sechs verschiedenen Stufen wählen, mit denen Sie bestimmen können, wie der IE 6 Cookies behandeln soll. Tabelle 4.2 zeigt, zwischen welchen Datenschutzeinstellungen Sie wählen können. Wie Netscape 7 und Mozilla unterscheidet auch der Internet Explorer 6 zwischen eigenen Cookies und denen von Drittanbietern.

Sicherheitsstufe	Beschreibung
Alle Cookies sperren	Alle Cookies werden gesperrt. Auf Ihrem Computer vorhandene Cookies können nicht von den Websites gelesen werden, die sie erstellt haben.
Hoch	Gesperrt werden Cookies ▶ von Anbietern ohne Datenschutzrichtlinie ▶ von Anbietern mit einer Datenschutzrichtlinie, die angibt, dass persönliche Daten gesammelt werden, ohne dass Ihre ausdrückliche Zustimmung notwendig ist Cookies, die vor der Installation des IE 6 auf Ihrem Computer vorhanden waren, werden so eingeschränkt, dass sie von Erstanbietern gelesen werden können.
Mittelhoch	Gesperrt werden Cookies ▶ von Drittanbietern ohne Datenschutzrichtlinie ▶ von Drittanbietern, die persönliche Daten ohne Ihre ausdrückliche Zustimmung sammeln ▶ Von Erstanbietern mit einer Datenschutzrichtlinie, die angibt, dass persönliche Daten immer gesammelt werden – es sei denn, der Anwender ist ausdrücklich dagegen (stillschweigende Zustimmung) Cookies von Erstanbietern, die nicht über eine Datenschutzrichtlinie verfügen, und Cookies, die vor der Installation des IE 6 auf Ihrem Computer vorhanden waren, werden so eingeschränkt, dass sie nur im Erstanbieter-Kontext gelesen werden können.
Mittel (Standardstufe)	Gesperrt werden Cookies ▶ von Drittanbietern ohne Datenschutzrichtlinie ▶ von Drittanbietern mit einer Datenschutzrichtlinie, die angibt, dass persönliche Daten immer gesammelt werden – es sei denn, der Anwender ist ausdrücklich dagegen.

Tabelle 4.2 Optionen zur automatischen Behandlung von Cookies

Sicherheitsstufe	Beschreibung
	Cookies von Erstanbietern mit einer Datenschutzrichtlinie, die angibt, dass persönliche Daten nur mit Ihrer ausdrücklichen Zustimmung gesammelt werden, werden heruntergestuft (gelöscht, wenn Sie den Internet Explorer schließen). Cookies von Erstanbietern ohne Datenschutzrichtlinie werden so eingeschränkt, dass sie nur vom Erstanbieter gelesen werden können. Cookies, die vor der Installation des IE 6 auf Ihrem Computer gespeichert waren, werden ebenfalls eingeschränkt.
Niedrig	Cookies von Erstanbietern ohne Datenschutzrichtlinie werden so eingeschränkt, dass sie nur vom Erstanbieter gelesen werden können. Cookies, die vor der Installation des IE 6 auf Ihrem Computer vorhanden waren, werden ebenfalls eingeschränkt. Cookies von Drittanbietern ohne Datenschutzrichtlinie oder mit einer Datenschutzrichtlinie, die angibt, dass persönliche Daten ohne Ihre stillschweigende Zustimmung verwendet werden, werden heruntergestuft (gelöscht, wenn Sie den Internet Explorer schließen).
Alle Cookies annehmen	Alle Cookies werden auf Ihrem Computer gespeichert, und auf Ihrem Computer vorhandene Cookies können von den Websites gelesen werden, die sie erstellt haben.

Tabelle 4.2 Optionen zur automatischen Behandlung von Cookies (Forts.)

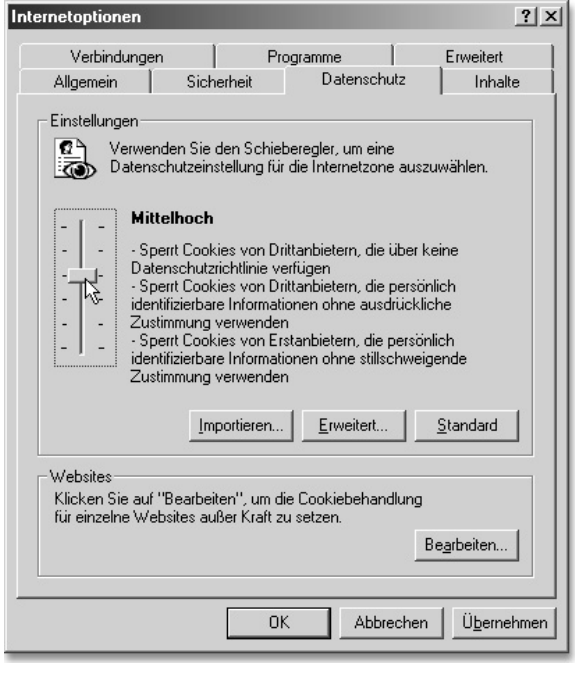


Abbildung 4.7 Cookie-Einstellungen des Internet Explorer 6

Hinweis Der Schieberegler im Register **Datenschutz** gilt nur für die Zone »Internet«. Von Websites in den Zonen »Lokales Intranet« und »Vertrauenswürdige Sites« werden alle Cookies automatisch angenommen. Alle Cookies von Websites, die in der Zone »eingeschränkte Sites« aufgenommen wurden, werden automatisch gesperrt.

Datenschutzaktionen pro Site

Die Richtlinien zur Verwaltung und Behandlung von Cookies, die durch die Position des Schiebereglers im Register **Datenschutz** festgesetzt werden, gelten allgemein für alle Websites. Darüber hinaus können Sie bestimmen, für welche Websites diese allgemeinen Regeln und Datenschutzrichtlinien nicht angewandt werden sollen. Dazu müssen Sie die entsprechende URL der Website im Dialogfeld »Datenschutzaktionen pro Site« eingeben.

Um dorthin zu gelangen, klicken Sie im Register **Datenschutz** auf **Bearbeiten...**. Die Schaltfläche **Bearbeiten...** steht Ihnen allerdings nur dann zur Verfügung, wenn Sie den Regler nicht auf »Alle Cookies annehmen« oder »Alle Cookies sperren« verschoben haben. Bei diesen Einstellungen werden Datenschutzaktionen pro Site ignoriert, da entweder alle Cookies ausnahmslos gesperrt oder ausnahmslos zugelassen sind und damit auch keine Ausnahme von dieser Regel gebildet werden kann.

Bei allen anderen Reglereinstellungen können einzelne Websites mit der Richtlinie »Sperren« oder »Zulassen« belegt werden.

Benutzerdefinierte Datenschutzeinstellungen

Wenn Sie möchten, können Sie die automatische Behandlung von Cookies für alle Websites in der Zone »Internet« auch völlig aufheben und eigene, benutzerdefinierte Richtlinien festsetzen. Hierzu klicken Sie im Register **Datenschutz** auf die Schaltfläche **Erweitert**.

Im Dialogfeld **Erweiterte Datenschutzeinstellungen** können Sie definieren, ob Sie Cookies von Erstanbietern und Drittanbietern »Annehmen«, »Sperren« oder erst nach Bestätigung einer »Eingabeaufforderung« zulassen wollen. Durch einen Klick auf das Kontrollkästchen »Sitzungscookies immer zulassen« bestimmen Sie, dass temporäre (kurzzeitige) Cookies, deren Gültigkeit sich auf die Dauer der aktuellen HTTP-Sitzung beschränkt (und die folglich nicht auf Ihrer Festplatte gespeichert werden), immer zugelassen werden dürfen. Die im Dialogfeld **Datenschutzaktionen pro Site** aufgeführten Websites bleiben auch von diesen benutzerdefinierten Regeln weiterhin unberührt.

Importieren von benutzerdefinierten Datenschutzeinstellungen

Wenn Sie sich nicht sicher sind, wie Sie Ihren Internet Explorer 6 am besten einstellen sollen, haben Sie die Möglichkeit, definierte Datenschutzeinstellungen zu importieren. So kann man die Empfehlungen von Datenschutzbeauftragten und Sicherheitsexperten auf einfache Weise in den IE importieren. Definierte Datenschutzeinstellungen können Sie sich unter **http://anon.inf.tu-dresden.de/ie6_privacy.html** herunterladen. Laden Sie die Datei `ie_privacy_file.xml` einfach auf Ihren Rechner, und übergeben Sie die dort enthaltenen Datenschutzeinstellungen an den IE6, indem Sie auf die Schaltfläche **Importieren** klicken.

Diese Datei optimiert die Datenschutzeinstellungen des IE6 und korrigiert zudem einige Nachlässigkeiten, die sich Microsoft bei den Grundeinstellungen von Cookies erlaubt hat. So werden in der Sicherheitsstufe »Hoch« standardmäßig immer noch Cookies von Werbefirmen wie Doubleclick durchgelassen. Wenn Sie Datenschutzeinstellungen, die in der oben genannten Datei enthalten sind, importieren, nimmt der IE6 auch solche Cookies nicht mehr an.

4.3 Webbug – Der Spion im Pixel

Da viele Internet-Nutzer Cookies mittlerweile meiden, weil sie dahinter gekommen sind, dass Cookies durch ihre Spionagemöglichkeiten eine Gefahr für die Privatsphäre darstellen, haben sich Anbieter kommerzieller Internet-Angebote etwas Neues einfallen lassen, um Benutzer fortlaufend zu identifizieren.

So genannte Webbugs (auch Webwanzen genannt) sind mikroskopisch kleine, transparente GIF-Bilder mit einer Größe von einem Pixel (ein einziger Bildpunkt also), die in Websites und HTML-E-Mails versteckt werden und beim Betrachten der Website nicht auffallen.

So unauffällig und unscheinbar die kleinen Winzlinge sind, so gefährlich sind sie auch.

In eine Website oder HTML-E-Mail integriert, ermittelt ein Webbug folgende Informationen:

- IP-Adresse des Users
- URL der Website
- URL des Webbug-GIFs
- Zeitpunkt, zu dem die Website aufgerufen wurde
- Browsertyp und Betriebssystem des Anwenders
- Cookie-Informationen (falls vorhanden)
- HTTP-Referer (Wie hat der User zu der Seite gefunden?)

Wenn Sie sich auf einer solchen Seite registrieren lassen oder persönliche Angaben machen, werden diese zusammen mit einer so genannten Bug-ID gespeichert, anhand derer Sie eindeutig identifiziert und in Zusammenhang mit Ihren Interessen gebracht werden können.

Mit Hilfe von Webbugs können sehr präzise Benutzerprofile erstellt werden, die es erlauben, maßgeschneiderte und zielgruppenorientierte Werbeangebote zu erstellen.

Funktionsweise von Webbugs

Webbugs werden in eine HTML-Datei als Bilder mit dem **HTML-Tag** `<img>` eingebunden. `<img>` ist eine reguläre HTML-Anweisung, mit der üblicherweise Bilder (engl. *images*) in HTML-Seiten integriert werden können. Mit dem Parameter `<scr>` gibt man die Quelle des Bildes an.

Beispiel: `<img scr="http://www.galleria.com/bilder/ballon.gif">`

Im Beispiel wird die Bilddatei `ballon.gif`, die sich im Verzeichnis `/bilder` auf dem Server `www.galleria.com` befindet, in den Browser geladen und angezeigt.

Beim Erstellen eines Webbugs wird anstelle eines Bildes eine Scriptdatei als Quelle angegeben.

Beispiel: `<img scr="http://www.datenspione.de/cgi-bin/webbug?">`

Beim Aufruf der Website würde der Browser die Scriptdatei `webbug` starten, die sich im `CGI-Bin`-Verzeichnis des Webservers `www.datenspione.de` befindet.

Da es sich um ein **CGI-Script** handelt, das auf dem Server und nicht auf dem Client des Anwenders ausgeführt wird, sind auch die Sicherheitseinstellungen des Browsers irrelevant. Selbst wenn sämtliche Sicherheitseinstellungen des Internet Explorer auf der höchsten Stufe stünden, würde das Script uneingeschränkt ausgeführt.

Hinweis Webbugs können sich heutzutage nicht nur in Webseiten oder E-Mails versteckt halten, sondern auch in MS Office-Dokumenten wie Word oder Excel. Denn inzwischen können auch Bilder aus einer Online-Quelle in ein Word-Dokument geladen werden. Wenn Sie ein solches Dokument bei einer bestehenden Internetverbindung öffnen, geschieht genau dasselbe wie beim Öffnen einer verwanzten Webseite. Dadurch kann man genau ermitteln, wer zu welchem Zeitpunkt das Dokument geöffnet hat.

Webwanzen in E-Mails und Foren-Beiträgen

Seitdem die Möglichkeit besteht, E-Mails im HTML-Format zu verfassen, werden auch Webbugs immer häufiger in E-Mails integriert.

Webwanzen können hierbei verschiedene Zwecke erfüllen:

- Wenn ein Anwender anonyme Informationen zu einem bestimmten Produkt anfordert und hierzu eine anonyme E-Mail-Adresse verwendet, können Werbe- und Marketingfirmen eine solche Adresse mit keiner Person in Verbindung bringen. Wenn nun in der Antwort-E-Mail ein Webbug versteckt ist, der die IP-Adresse des Empfängers ermittelt, erkennt die Werbefirma am Netzwerkanteil der IP-Adresse zumindest, bei welchem Internet-Provider der Benutzer registriert ist.
- Marketingunternehmen verfügen über umfangreiche Listen von E-Mail-Empfängern. Um die Aktualität ihrer Adresslisten zu überprüfen, werden Werbe-E-Mails häufig mit Webbugs versehen, die diese Aufgabe wahrnehmen können. Ist eine E-Mail-Adresse noch aktuell, kann der Empfänger weiterhin mit Werbung versorgt werden bzw. dessen Adresse weiterverkauft werden.
- In werbefinanzierten Newslettern werden Webbugs als Lesebestätigung verwendet, um zu überprüfen, ob ein Abonnent den Inhalt auch tatsächlich liest und die Nachricht nach dem Empfang nicht sofort löscht.
- Sobald ein Abonnent die E-Mail öffnet, wird auch der Webbug aktiviert. Wenn man die Anzahl der Aktivierungen summiert, ergibt sich daraus automatisch die Anzahl der Leser.

Neben E-Mails können natürlich auch Foren-Beiträge Webbugs erhalten. Da viele E-Mail-Programme auch die Möglichkeit bieten, Newsgroups zu abonnieren sowie Beiträge zu lesen und zu verfassen, gilt technisch das Gleiche wie bei E-Mail-Nachrichten. Jeder Benutzer, der einen News-Beitrag liest, kann mit Hilfe eines Webbugs erfasst werden. Damit wird die Anonymität von Newsgroups aufgehoben.

4.3.1 Schutz vor spionierenden Bannern und Webbugs

Verschiedene Tools, die im Internet zum kostenlosen Download angeboten werden, bieten eine Vielzahl von Filtermöglichkeiten, mit denen Sie Banner, Popup-Fenster, Webbugs, Skripten und natürlich auch Cookies abblocken und filtern können. Viele dieser nützlichen Programme können zudem als anonyme **Proxy**-Server eingesetzt werden. Was es damit auf sich, können Sie in Abschnitt 4.4, *Anonym surfen und mailen*, lesen.

Auf der Website von Bugnosis finden Sie neben vielfältigen Informationen zum Thema Webwanzen den »Web bug detector«, ein Tool, das in den Internet Explorer eingebunden wird und Webwanzen aufspürt und sichtbar macht. Das Tool durchsucht den Quelltext einer Website nach typischen Merkmalen von Webbugs. Wurde ein Webbug gefunden, ertönt ein Alarmsignal und es wird angezeigt, an welcher Stelle der Webseite sich der Spion befindet. Am unteren Rand des Browserfensters blendet Bugnosis zusätzlich Informationen über Herkunft des Webbugs ein und gibt an, welche Daten übermittelt wurden.

Das Tool eignet sich hervorragend zum Aufspüren von Webbugs, kann diese jedoch nicht entfernen oder blockieren.

Auf der Bugnosis Website **http://www.bugnosis.org** können Sie sich dieses Tool herunterladen.

Ein weiteres hervorragendes Programm ist Webwasher, das neben einer Vielzahl von Filtermöglichkeiten (z. B. Filterung von Werbebannern oder Cookies) auch über einen Webbug-Filter verfügt. Der Filter sorgt dafür, dass alle Bilder, die nicht von der aufgerufenen Website selbst kommen, nicht vom Server geladen werden. Anders als bei Bugnosis werden sämtliche Spionagemöglichkeiten, die in Zusammenhang mit den Webwanzen stehen, von vornherein unterbunden.

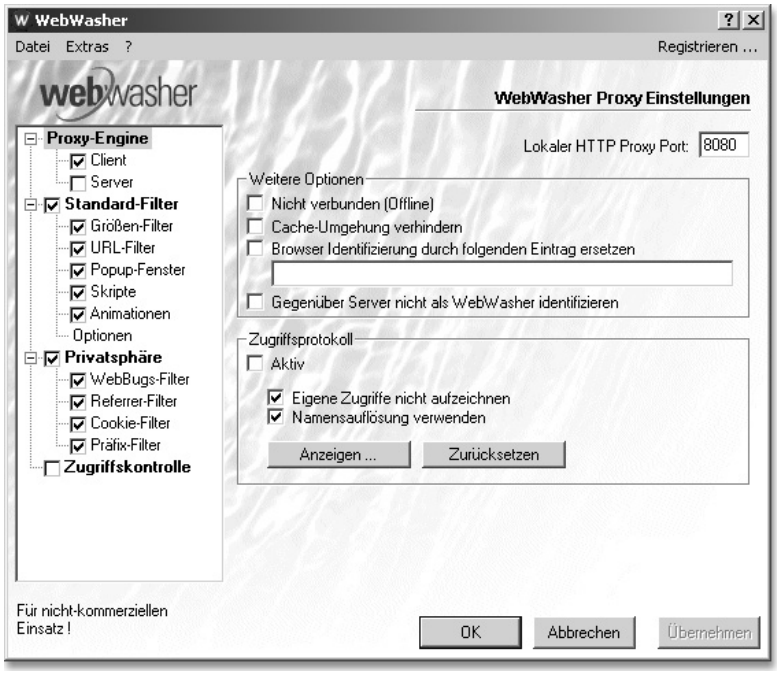


Abbildung 4.8 Webwasher

Sie aktivieren den Webbug-Filter, indem Sie im Programm unter der Rubrik »Privatsphäre« das Kontrollkästchen »Webbugs-Filter« anhaken.

Das universelle Filter-Tool können Sie sich unter **http://www.webwasher.com/de** herunterladen.

Eine sehr empfehlenswerte Website ist **http://www.junkbuster.com**, die die erste Anlaufstelle für all jene sein sollte, denen ihre Privatsphäre am Herzen liegt. Hier können Sie sich auch den »Internet Junkbuster-Proxy« herunterladen, der sämtliche Werbebanner, Cookies und Webwanzen abblockt.

Ein weiteres Tool namens Guidescope erfüllt vom Prinzip her den gleichen Zweck wie der Junkbuster, ist aber leichter zu installieren und zu bedienen. Unter **http://www.guidescope.com** können Sie sich dieses Tool besorgen.

4.4 Anonym surfen und mailen

Eine Methode, um anonym durch das World Wide Web zu surfen, ist die Benutzung von Anonymisierungsdiensten wie **http://www.anonymizer.com** oder **http://rewebber.de**

Rufen Sie einfach die Website eines Anonymisierungsdienstes auf, und tragen dort die Adresse der Website ein, die Sie anonym besuchen möchten.

Allerdings ist es bei manchen dieser Dienste zwingend erforderlich, dass Sie sich vorher anmelden und Ihre persönlichen Daten hinterlegen, was voraussetzt, dass Sie dem Betreiber des Anonymisierungsdienstes vertrauen. Denn schließlich könnte dieser Ihre Daten auch missbrauchen. Bei Anonymisierungsdiensten, bei denen Sie persönliche Angaben machen müssen, handelt es sich also mehr um eine Pseudoanonymität.

Eine weitaus bessere Möglichkeit, Ihre Privatsphäre zu schützen, besteht darin, über einen anonymen Proxy-Server durch das Web zu surfen. Der Proxy (engl. *Stellvertreter*) tritt praktisch stellvertretend für Ihren PC im WWW auf und leitet alle HTTP-Anfragen Ihres Browsers ins Internet weiter. Der Webserver, von dem die Information angefordert wurde, sendet seine Antwort an den Proxy, der das HTML-Dokument an den HTTP-Client des Anwenders weiterleitet.

Der Vorteil für den Anwender besteht darin, dass die IP-Adresse seines Rechners vor dem Webserver verborgen bleibt. Somit kann der Webserver auch keinen Cookie auf dem Rechner des Anwenders einrichten.

Die Benutzung eines Proxys bringt jedoch einige Nachteile mit sich. Je nachdem in welchem Land sich der Proxy befindet, kann er sich negativ auf die Surf-Geschwindigkeit auswirken. Zudem findet man nicht immer auf Anhieb einen

funktionierenden Proxy-Server, da einerseits die Listen, auf denen Proxy-Server-Adressen im Internet aufgeführt sind, schnell veralten und andererseits viele Proxy-Server nur zu bestimmten Zeiten oder nur vorübergehend online sind.

Wenn Sie nach Proxy-Servern suchen wollen, geben Sie in einer Suchmaschine wie Google.de einfach Schlüsselbegriffe wie »Proxy list« ein, und Sie werden eine Vielzahl von WWW-Dokumenten zu diesem Thema finden.

Webtipp Eine aktuelle Liste anonymer Proxy-Server finden Sie unter: **http://www.multiproxy.org/anon_list.htm**

4.4.1 Proxy-Einstellungen beim Internet Explorer

Um den Microsoft Internet Explorer für die Verbindung über einen anonymen Proxy-Server zu konfigurieren, öffnen Sie den Internet Explorer und klicken in der Menüleiste unter **Extras** auf **Internetoptionen**.

Nachdem Sie auf den Karteireiter **Verbindungen** geklickt und eine Verbindung ausgewählt haben, klicken Sie auf **Einstellungen**. Setzen Sie ein Häkchen in das Kästchen vor »Proxyserver für diese Verbindung verwenden«, und tragen Sie dort die IP-Adresse des anonymen Proxys nebst dem Server-Port ein, die Sie aus einer Proxy-Liste entnommen haben. Anschließend bestätigen Sie mit **OK**.

Abbildung 4.9 Die Proxy-Einstellungen im Internet Explorer

Sollte der von Ihnen eingetragene Proxy nicht funktionieren, nehmen Sie sich Ihre Liste vor und suchen sich den nächsten Proxy heraus.

Stellen Sie eine Verbindung zum Internet her, öffnen Sie die Eingabeaufforderung (**Start · (Alle) Programme · Zubehör**) und geben Sie den Befehl `ping` gefolgt von der IP-Nummer des Proxys ein. Sollte dieser antworten, können Sie die Adresse in den Browser eintragen.

Hinweis Einige Proxy-Adressen sind nur temporär verfügbar, weshalb es von Zeit zu Zeit notwendig ist, den Proxy-Server zu wechseln.

4.4.2 Proxy-Einstellungen bei Netscape-Browsern

Verwenden Sie hingegen einen Netscape-Browser, gehen Sie folgendermaßen vor: Klicken Sie auf **Bearbeiten · Einstellungen · Erweitert · Proxies,** und wählen Sie den Radio-Button **Manuelle Proxy-Konfiguration**. Unter »HTTP-Proxy« geben Sie nun die IP-Adresse des Proxys sowie die Portnummer ein.

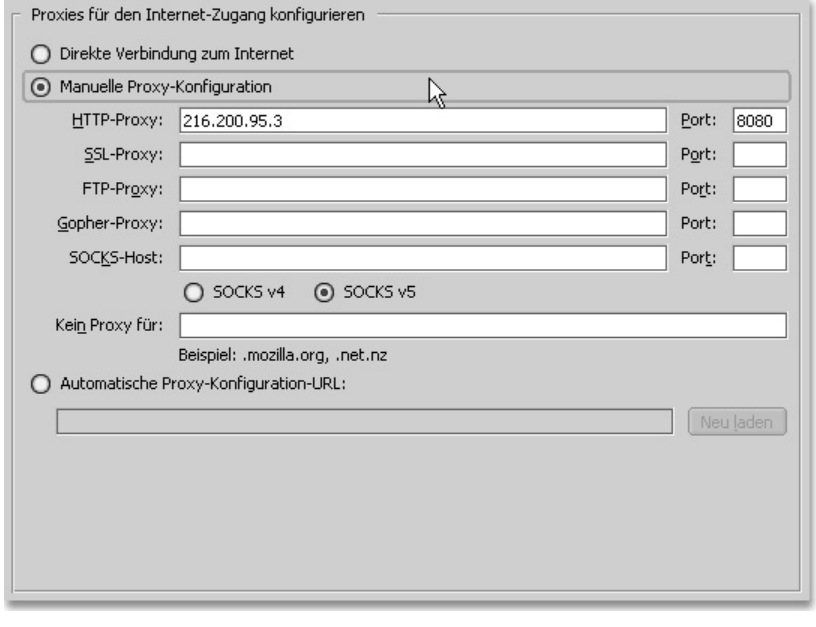


Abbildung 4.10 Manuelle Proxy-Konfiguration unter Netscape

4.4.3 Proxy-Tools

Wesentlich komplexere und umfangreichere Möglichkeiten bieten Proxy-Tools wie Junkbuster, Java Anon Proxy, Proxomitron oder Webwasher.

Sie können diese nicht nur als Proxy-Server verwenden, sondern auch eine Reihe weiterer Parameter festlegen, um Inhalte wie JavaScript-Code, HTTP-Header oder GIF-Animation aus Webseiten in vielfältiger Weise herauszufiltern. Positiv ist, dass der durch einen Proxy-Server verursachte Geschwindigkeitsverlust durch die Filterung von Werbegrafiken und Bannern kompensiert werden kann.

Eine weitere interessante Funktion bietet Proxomitron. Mit diesem Tool können Sie nämlich gleich mehrere Proxy-Server verwenden, die, während Sie im Internet surfen, in bestimmten Abständen oder zufällig ausgetauscht werden. Somit ist es nahezu unmöglich, Ihre Spuren im Web zu verfolgen.

Abbildung 4.11 The Proxomitron

Alle Webadressen zu den genannten Tools finden Sie am Ende dieses Kapitels.

4.4.4 Browser-Cache löschen

Ein triviales und ganz offensichtliches Verfahren, um Ihre Spuren im Netz zu verwischen, wurde hier noch gar nicht angesprochen: nämlich das einfache Löschen von Cookies und der von Ihnen besuchten Webseiten von Ihrer Festplatte.

Wenn Sie eine Website zum ersten Mal aufrufen, speichert Ihr Browser bestimmte Elemente der Seite in einem Ordner auf Ihrer Festplatte. Wenn Sie die gleiche Seite erneut aufrufen, wird diese nicht aus dem Web geladen, sondern kann von Ihrer lokalen Festplatte aufgerufen werden. Der Vorteil besteht darin, dass die Netzlast reduziert wird und Webseiten wesentlich schneller angezeigt werden. Einen solchen Zwischenspeicher bezeichnet man als Cache.

Beim Internet Explorer werden Cookies und Inhalte von besuchten Webseiten wie Bilder im Ordner **Temporary Internet Files** (Temporäre Internetdateien) gespeichert. Wenn Sie im Menü **Favoriten · Zu Favoriten hinzufügen** das Kontrollkästchen »Inhalte offline zugänglich machen« aktiviert haben, werden von

allen besuchten Webseiten lokale Kopien angefertigt. Hierdurch können nicht nur Sie, sondern auch andere Anwender, die Ihren PC mitbenutzen, schneller auf Webseiten zugreifen. Jeder Benutzer kann damit aber auch nachvollziehen, welche Webseiten Sie wann besucht haben. Außerdem ist es möglich, dass der Inhalt des Browser-Caches von einem Webserver abgefragt und an diesen übermittelt wird.

Aus diesem Grunde ist es ratsam, den Cache Ihres Browser hin und wieder zu löschen.

Um temporäre Internetdateien zu löschen öffnen Sie den Internet Explorer und wählen im Menü **Extras · Internetoptionen** aus. Im Register **Allgemein** klicken Sie auf die Schaltfläche **Dateien löschen** (siehe Abbildung 4.12).

Wenn Sie zusätzlich alle Offline-Inhalte in den Favoriten löschen möchten, setzen Sie einen Haken im Kontrollkästchen »Alle Offline-Inhalte löschen« der Dialog-Box.

Abbildung 4.12 Die Internetoptionen im Internet Explorer

Wenn Sie temporäre Internetdateien nicht immer wieder manuell löschen wollen, können Sie Ihren Internet Explorer so einstellen, dass alle im Cache abgelegten Dateien unmittelbar nach Beendigung einer Online-Sitzung automatisch gelöscht werden.

Hierzu wechseln Sie in den Internetoptionen zum Register **Erweitert** und aktivieren unter der Kategorie »Sicherheit« den Punkt »Leeren des Ordners Temporary Internet Files beim Schließen des Browsers«.

Der Ordner Verlauf

Eine weitere Funktion, die in Zusammenhang mit der Speicherung von temporären Internetdateien steht, ist der so genannte Verlauf. Hierbei werden die Elemente einer Webseite nicht als Datei abgelegt, sondern es werden lediglich die Webadressen (URLs) von besuchten Seiten gespeichert.

Wenn Sie eine bestimmte Webseite erneut aufrufen wollen, die Adresse aber vielleicht vergessen haben, können Sie diese einfach aus der Verlaufsliste auswählen, ohne die Adresse mühsam nachschlagen und von Hand eingeben zu müssen.

Wenn Sie in der Symbolleiste des Internet Explorer auf die Schaltfläche **Verlauf** klicken, wird auf der linken Seite des Browserfensters die Verlaufsliste eingeblendet, wo alle von Ihnen aufgerufenen URLs nach Wochentagen geordnet aufgeführt sind.

Dieselben Bedenken bezüglich temporär gespeicherter Internetdateien sind auch bei der lokalen Speicherung von URLs angebracht.

Wenn Sie in der Verlaufsfunktion eine Verletzung Ihrer Privatsphäre sehen, weil auch andere Benutzer Ihres PCs erkennen können, welche Seiten Sie in den letzten 20 Tagen besucht haben (so lange werden URLs im Verlauf standardmäßig gespeichert), sollten Sie den Verlauf löschen.

Wählen Sie im Internet Explorer-Menü **Extras · Internetoptionen,** und klicken Sie im Register **Allgemein** auf die Schaltfläche **Verlauf löschen**.

Wenn Sie möchten, können Sie hier auch festlegen, nach wie vielen Tagen der Verlaufsordner automatisch gelöscht werden soll.

4.4.5 Peekabooty

Die Hackergruppe »Cult oft the dead Cow« (Kult der toten Kuh), kurz cDc, die mit ihren Trojaner-Programmen Back Orifice und BO2k bereits für Furore sorgte, hat einen speziellen Browser namens Peekabooty entwickelt, der mehr Bewegungsspielraum und Anonymität im Internet ermöglichen soll.

Der Browser wurde im Juli 2001 erstmals auf der jährlichen Hacker-Konferenz DefCon in Las Vegas vorgestellt und sorgte für wahre Begeisterungsstürme bei den Zuschauern.

Genau genommen ist Peekabooty jedoch ein Produkt von *Paul Baranowski*, der einst Mitglied eines Projekts gegen Zensur und Diskriminierung namens »Hacktivismo« war, das vom cDc-Leader *Oxblood Ruffin* ins Leben gerufen wurde.

Da *Baranowski* mittlerweile weder etwas mit cDc noch mit Hacktivismo zu tun hat, obliegt ihm nun die alleinige Verantwortung für das PAB-Projekt.

Doch egal, wer die Lorbeeren für dieses Projekt erntet, für Behörden, Unternehmen und Regierungen dürfte Peekabooty jedenfalls ein schlimmer Alptraum sein, da für diese Institutionen die Kontrolle und Überwachung sämtlicher Netzaktivitäten der Inbegriff für ein »sicheres Internet« ist.

Wenn Sie Peekabooty auf Ihrem Rechner starten, stellt Ihr Browser zunächst eine Verbindung zum Peekabooty-Netz her, das als zentraler Proxy fungiert.

Ähnlich dem **Peer-to-Peer**-Prinzip nehmen Peekabooty-Rechner HTTP-Anfragen von Internet-Usern aus aller Welt entgegen, holen die Information von der entsprechenden Website und liefern diese an den anfragenden Rechner zurück.

Da der gesamte Datentransfer zwischen Server und Browser verschlüsselt wird, können auf diese Weise auch Firewalls umgangen werden.

Für Menschen, die in Ländern leben, wo die Nutzung des Internet zensiert oder stark eingeschränkt ist, bedeutet Peekabooty den Ausbruch aus einem virtuellen Käfig, mit dem viele Staaten ihre Bürger am Zugang zu bestimmten Inhalten im Web hindern und verschiedene Websites sperren. Für diese Menschen ist Peekabooty quasi die Befreiung aus ihrer virtuellen Gefangenschaft. Internet-Anwender müssen lediglich einen aktiven Peekabooty-Proxy in ihrem Browser eintragen.

Lauschangriffe, Datenfilterungen und Zensur könnten somit endgültig der Vergangenheit angehören.

Der einzige Nachteil ist, dass Peekabooty erst am Anfang seiner Entwicklung steht. Denn Peekabooty basiert auf dem Gemeinschaftsprinzip: Je mehr Anwender diese Technologie verwenden und je mehr Peekabooty-Knotenpunkte existieren, desto besser funktioniert unzensiertes und anonymes Surfen im Internet. Derzeit ist es noch etwas schwierig, einen aktiven Peekabooty-Knoten zu finden.

Peekabooty ist selbstverständlich Open-Source und wird unter der GNU General Public Licence (GNU-GPL) vertrieben.

Wussten Sie schon, dass ... in 45 Ländern dieser Erde Webinhalte entweder staatlich zensiert werden oder die Regierung den Zugang zum Internet völlig verbietet?

Eine Untersuchung der Journalistenvereinigung »Sans Frontières« hat ergeben, dass viele Staaten den Internetzugang in irgendeiner Form behindern. Viele dieser Regierungen begründen eine Kontrolle damit, dass man die Bürger des eigenen Landes vor »subversiven Ideen« schützen müsse. Zu den zensierenden Staaten gehört beispielsweise der Iran, wo sexuelle, religiöse und medizinisch-anatomische Inhalte genauso verboten sind wie Websites, in denen die USA oder Israel erwähnt werden. Auch in China werden Webinhalte zensiert, die eine Gefahr für die Staatsicherheit darstellen könnten und der kommunistischen Ideologie zuwiderlaufen. Glücksspiele und pornographische Inhalte sind ebenfalls nicht erlaubt.

Durch Peekabooty besteht zwar die Gefahr, dass es Menschen mit krimineller Energie leichter gemacht wird, illegale Aktivitäten im Netz auszuüben. Andererseits muss man aber sagen, dass Kriminelle so oder so einen Weg finden werden, um ihre Spuren im Netz zu verwischen – auch ohne Peekabooty.

Den Browser gibt es für UNIX/Linux sowie für alle gängigen Windows-Plattformen.

Unter **http://sourceforge.net/projects/peekabooty** können Sie Peekabooty kostenlos herunterladen.

Weitere Informationen zu Peekabooty finden Sie auf der Website von *Paul Baranowski* unter **http://paulbaranowski.org** und auf der offiziellen PAB-Homepage unter **http://paulbaranowski.org/phpnuke/html/index.php**.

Neben Peekabooty gibt es eine Reihe weiterer, ähnlicher Projekte wie Crowds, Freenet oder AN.ON.

4.4.6 Anonyme Remailer

Damit Sie Ihre Anonymität nicht nur beim Surfen im World Wide Web, sondern auch bei der E-Mail-Kommunikation erhalten, wurden so genannte Remailer-Dienste ins Leben gerufen.

Auf der Website eines Remailer-Dienstes tragen Sie einfach den Empfänger, die Betreffzeile und die Nachricht ein und schicken diese an einen Mailserver. Eine Software entfernt aus der E-Mail sämtliche Absenderdaten und ersetzt diese durch falsche Informationen. Diese Technik, die als **Cloaking** (dt. *Vermummen*)

bezeichnet wird, sorgt dafür, dass niemand nachvollziehen kann, wer die E-Mail tatsächlich abgeschickt hat. Insbesondere in Newsgroups, in denen Sie Ihre Meinung zu kontroversen und heiklen Themen äußern, kann es sinnvoll sein, Ihre Identität durch Cloaking zu verschleiern.

Grundsätzlich unterscheidet man zwischen echten Remailern und so genannten pseudoanonymen Remailern.

Der Unterschied besteht darin, dass bei letzterer Variante der Dienstanbieter Ihre wahre Identität kennt, was bei echten anonymen Remailer-Diensten nicht der Fall ist. Dafür sind pseudoanonyme Remailer aber leichter zu nutzen. Wenn Sie wirklich anonym bleiben wollen, sollten Sie auf pseudoanonyme Remailer verzichten.

Webtipp Auf folgendenen Websites können Sie E-Mails völlig anonym senden:

- Riot – **http://riot.eu.org/anon/**
- AnonWWW – **http://nonymouse.com/anonwww_de.html**
- COTSE – **http://webmail.cotse.com/servicedetails.html**

4.5 Spamming – Datenmüll im Postfach

Wenn die hohe Anzahl von Werbe-E-Mails für den Anwender zur nervlichen Belastung wird und Werbebotschaften per E-Mail nur noch als belästigend empfunden werden, spricht man von **Spam**-Mails. Im ursprünglichen Sinne bezeichnet der Engländer mit dem Begriff Spam in Dosen abgefülltes Frühstücksfleisch (**S**piced **P**ork an H**am**). Im Zeitalter des Internet werden auch Werbe-E-Mails, denen man zwangsläufig ausgeliefert ist, als Spam bezeichnet. Dies wiederum basiert auf einem Sketch der englischen Komikertruppe Monty Python, in dem eine Gruppe Wikinger in einem Restaurant sitzt und permanent »Spam, Spam, Spam!« schreit, sodass eine vernünftige Unterhaltung nicht mehr möglich ist. Im Zusammenhang mit unerwünschten Werbe-E-Mails steht Spam für die Abkürzung »**S**end **P**henomenal **A**mounts oft **M**ails«.

Unter **Spamming** versteht man also die Überflutung von Mailboxen mit unerwünschter Massenwerbung. Dieses auch unter dem Begriff Junk-Mail bekannte Phänomen ist oft das Ergebnis der weiter oben erläuterten Tracking-Praktiken von Website-Betreibern.

Es gibt aber auch andere Wege, wie Werbefirmen und unseriöse Geschäftemacher an Ihre E-Mail-Adressen gelangen können:

- über Mitgliederverzeichnisse von Internet Service Providern wie AOL und T-Online
- über E-Mail-Adressverzeichnisse wie bigfoot.com und MESA
- über Mailinglisten und Newsgroups
- durch das Erraten von E-Mail-Adressen

Hinter dem Spamming stecken in erster Linie kleine, dubiose Geschäftemacher, die dem Empfänger zweifelhafte Angebote unterbreiten, um schnell Kasse zu machen.

Folgende Schwindeleien werden tagtäglich an unzählige Internet-Nutzer per E-Mail versendet:

- Heimarbeitsangebote, die Geld für Eintüt- oder Handarbeiten anbieten, bei denen die Opfer niemals Geld für Ihre Arbeit erhalten
- Schwindeleien über Gesundheitsprodukte (Diätpillen, Wunderheilmittel etc.)
- Kettenbriefe
- Ungesetzliche Devisengeschäfte
- Betrügereien, die Einkünfte durch Spam-Aktivitäten versprechen
- Schwindel durch Pyramiden- und Schneeballsysteme, die große Gewinne versprechen, ohne großen Aufwand betreiben zu müssen.
- Kreditbetrügereien, bei denen die Not hoch verschuldeter Menschen ausgenutzt wird. Gegen Zahlung eines bestimmten Betrages sollen die Opfer angeblich wieder kreditwürdig werden.
- Besonders günstige Luxusferienangebote zu Tiefstpreisen. Den Opfern wird dabei verschwiegen, dass die Unterkunft keineswegs zur Luxusklasse gehört.

Ist Ihre E-Mail-Adresse erst einmal auf eine Spamliste geraten, besteht kaum eine Chance, dort wieder ausgetragen zu werden. Spammer tauschen solche Listen meist mit ihresgleichen, sodass die Wahrscheinlichkeit zunimmt, noch mehr lästige Werbung per E-Mail zu erhalten. Sie sollten daher präventive Maßnahmen treffen, mit denen Sie die Wahrscheinlichkeit verringern, dass Spammer überhaupt an Ihre E-Mail-Adresse gelangen.

Sollte es bereits zu spät sein, haben Sie die Möglichkeit, Filterprogramme zu verwenden, die automatisch die wirklich wichtigen Nachrichten vom täglichen E-Mail-Datenmüll trennen.

In Abschnitt 4.5.2, *Kampf gegen Spam – So schützen Sie sich*, werden diese Möglichkeiten näher beschrieben.

Webtipp Die Robinsonliste ist eine gemeinnützige Einrichtung, die sich dafür einsetzt, Belästigungen beim E-Mail-Verkehr zu vermeiden. Jeder, der sich in die Mail-Schutzliste einträgt, erhöht damit die Wahrscheinlichkeit, dass sich sein Aufkommen an unerwünschten Werbe-E-Mails zumindest reduziert. Die Website finden Sie unter: **http://www.robinsonliste.de**

4.5.1 Problematik und Gefahren von Junk-Mails

Insbesondere für Systemadministratoren stellt das Spamming ein sehr großes Problem dar. Wenn eine E-Mail-Adresse zufällig von einer Software erzeugt oder erraten wird, heißt das natürlich noch lange nicht, dass die Adresse auch tatsächlich existiert.

Sendet der Spammer nun eine Werbe-E-Mail an einen nicht vorhandenen Mail-Account, wird die E-Mail automatisch an den Absender zurückgesendet, vorausgesetzt, die Adresse des Absenders ist gültig. Da Spammer ihre Adresse jedoch fälschen oder nach dem Senden sofort wieder löschen, schlägt dieser Versuch fehl.

In einem solchen Fall bleibt alles am Postmaster des Mailservers hängen. Der Postmaster muss nämlich überprüfen, was bei der Datenkommunikation schief gelaufen ist. So kann es vorkommen, dass beispielsweise unter 2000 E-Mails 1800 nicht zustellbare Junk-Mails sind, die er alle einzeln überprüfen muss. Das kostet Zeit und Nerven.

Ein weiteres Problem von Spamming besteht darin, dass es den Gemeinschaftsgeist des Usenet zunichte machen, da Junk-Mails auch massenhaft an Newsgroups versendet werden. Die Folge ist, dass immer weniger Leute die Beiträge lesen und der Provider die Anzahl legitimer Diskussionsgruppen immer mehr einschränkt, wodurch der Nutzen der »schwarzen Bretter« zunehmend sinkt.

Spamming sorgt außerdem auch dafür, dass der massenhaft versendete Datenmüll, der täglich über den Äther läuft, zu einer regelrechten elektronischen Sintflut führt, in der der wirklich wichtige Datenverkehr einfach untergeht.

4.5.2 Kampf gegen Spam – So schützen Sie sich

Das einfachste und naheliegendste Verfahren, sich vor Junk-Mails zu schützen, besteht sicherlich darin, seine eigene E-Mail-Adresse vor Spammern zu verbergen. Das hört sich jedoch einfacher an, als es in Wirklichkeit ist. Denn selbst wenn Spammer Ihre E-Mail-Adresse nicht kennen oder herausfinden können, bleibt immer noch ein kleines Risiko, dass diese erraten oder per Software automatisch generiert wird.

Hier einige Tipps, wie Sie es Spammern erschweren können, an Ihre E-Mail-Adresse zu gelangen:

- Tragen Sie sich nicht in öffentliche E-Mail-Verzeichnisse wie bigfoot.com ein.
- Weisen Sie Ihren Provider an, Ihren Namen aus dem Mitgliederverzeichnis zu entfernen. Insbesondere AOL- und T-Online-Nutzer sollten von dieser Möglichkeit Gebrauch machen.
- Verwenden Sie zwei oder mehrere E-Mail-Accounts.

  Ihre erste E-Mail-Adresse geben Sie ausschließlich an Freunde, Bekannte, Verwandte oder Geschäftspartner weiter, von denen Sie über diesen Account legitim Post erhalten möchten.

  Die zweite Adresse verwenden Sie dann, wenn Sie sich auf einer Website registrieren lassen, persönliche Daten beim Online-Shopping hinterlassen, an Gewinnspielen teilnehmen, sich in eine öffentliche Mailingliste eintragen oder Beiträge in Newsgroups posten.

  Viele Anbieter wie Web.de, Yahoo!, Hotmail, GMX etc. bieten die Möglichkeit, eine kostenlose und providerunabhängige E-Mail-Adresse einzurichten.

Tarnung von E-Mail-Adressen

Aus Zeit- und Kostengründen lassen Spammer das Internet automatisch von einer Software nach E-Mail-Adressen durchsuchen. Diese Suchagenten suchen nach bestimmten, für E-Mail-Adressen typischen Mustern.

Wenn der Suchagent einen Text mit dem @-Zeichen findet, geht er davon aus, dass es sich um eine E-Mail-Adresse handelt. Da ein Mensch flexibler ist als ein stupider Suchroboter, kann man einige Tricks anwenden, um seine E-Mail-Adresse vor Suchagenten zu verbergen.

Wenn Sie in einem öffentlichen Forum Ihre E-Mail-Adresse hinterlassen, kann diese von einem Suchagenten einfach aufgespürt werden.

Üblicherweise haben E-Mail-Adressen folgende Form: donaldduck@entenhausen.de

Um einen Suchagenten auszutricksen, müssen Sie lediglich die E-Mail-Adresse ein wenig abwandeln.

Beispiele:

- donaldduck_@_entenhausen.de
- donald!duck@enten!hausen.de!
- donaldduck at entenhausen.de
- entenhausen.de@donaldduck

Ein Mensch erkennt natürlich auf Anhieb, dass die oben aufgeführten Varianten nicht der Form einer E-Mail-Adresse entsprechen, und ändert die Adresse entsprechend um, wenn er Kontakt mit Ihnen aufnehmen möchte. Es kann auch sinnvoll sein, wenn Sie im Forum kurz einen Hinweis wie »at durch @ ersetzen« oder »alle Ausrufezeichen entfernen« geben.

Auf diese Weise können Sie mit einfachen und effektiven Mitteln verhindern, dass Ihre E-Mail-Adresse nicht auf eine Spammer-Adressliste gelangt.

Was Sie beim Eintrag in Mailinglisten beachten sollten

Insbesondere öffentliche E-Mail-Listen dienen Spammern als Informationsquelle, um nach E-Mail-Adressen zu fahnden.

Die Verwaltung von E-Mail-Verteilerlisten wird häufig von Programmen wie Listserv, Listproc, Majordomo oder Mailbase übernommen, deren Aufgabe darin besteht, ankommende Beiträge an alle Mitglieder weiterzuleiten und die eintreffenden Anfragen und Befehle auszuführen.

Mit Hilfe des `who`-Befehls fragen Spammer häufig Mailinglisten-Server, um sich die E-Mail-Adressen einer bestimmten Liste anzeigen zu lassen.

Wenn Sie sich in eine Mailingliste eintragen, sollten Sie daher den Listenmanager bitten, die `who`-Option zu deaktivieren – falls dies nicht schon geschehen ist.

Sollte dies nicht möglich sein, können Sie Ihre E-Mail-Adresse anderweitig vor `who`-Anfragen verbergen.

Wenn es sich um eine Listproc-Liste handelt, in die Sie sich eingetragen haben, geben Sie in den Body (Textkörper) Ihres E-Mail-Clients folgendes ein: `SET listname CONCEAL YES`.

Bei einer Listserv-Liste lassen Sie `Yes` einfach weg.

Spam-Filter

Ein probates Mittel, Werbe-E-Mails von Ihrem elektronischen Postfach fernzuhalten, sind so genannte Spam- oder Junk-Mail-Filter.

Mit Hilfe einer solchen Filtersoftware können Sie Regeln erstellen, nach denen bestimmte E-Mails gelöscht werden, noch bevor sie in Ihrem Posteingang landen. Je nach Flexibilität und Funktionsumfang der Software können Sie komplexe Filtertechniken und Filterstrategien festlegen, die Sie vor Datenmüll in Ihrem E-Mail-Postfach bewahren. Dabei wird jede eingehende E-Mail der Reihe nach überprüft und in einer logischen Abfolge nach bestimmten Kriterien und Bedingungen (Wenn ..., dann ...) gefiltert.

Beispiel Eine Filterregel könnte folgendermaßen aussehen:

1. Speichere alle Nachrichten meines Chefs im Ordner »geschäftlich«.
3. Lösche alle Nachrichten, die das Wort »Abmahnung« in der Betreffzeile enthalten.
4. Alle anderen E-Mails sollen im Posteingang bleiben.

In dem Beispiel überprüft der Spam-Filter zunächst, ob es sich um eine Nachricht Ihres Chefs handelt. Ist dies der Fall, wird die Mail in einem Ordner namens »geschäftlich« abgelegt. Wenn es sich nicht um eine Nachricht Ihres Chefs handelt, springt der Filter zu Punkt 2 und sucht nach dem Begriff »Abmahnung« in der Betreffzeile. Wird die Software fündig, so wird die E-Mail unverzüglich gelöscht. Ansonsten lässt der Filter die E-Mail zum Posteingangsordner passieren.

Beachten Sie hierbei, dass die Reihenfolge der Filter eine sehr wichtige Rolle spielt. Denn wenn Sie beispielsweise Punkt 1 und 2 miteinander vertauschen, würde der Filter nach folgendem Schema arbeiten:

- Als Erstes überprüft der Filter, ob die Betreffzeile einer eingegangenen E-Mail-Nachricht das Wort »Abmahnung« beinhaltet.
- Wenn dies der Fall sein sollte, wird die E-Mail auf jeden Fall gelöscht, selbst dann wenn die Nachricht von Ihrem Chef sein sollte.

Hätte der Filter, wie im obigen Beispiel, eine Nachricht zunächst daraufhin überprüft, ob diese von Ihrem Chef stammt, wäre diese unverzüglich gespeichert worden, einschließlich einer Nachricht Ihres Chefs, in deren Betreffzeile ausnahmsweise einmal das Wort »Abmahnung« vorkommt.

Wie Sie sehen, spielt die Filter-Reihenfolge bei der Festlegung von Filterregeln deswegen eine so entscheidende Rolle, weil durch fehlerhafte Filter-Konfigurationen für Sie wichtige E-Mails gelöscht werden könnten.

Um Nachrichten effektiv filtern zu können, benötigen Sie nicht unbedingt eine zusätzliche Software, da viele E-Mail-Clients wie Eudora, Outlook Express oder Netscape Messenger bereits einige Möglichkeiten zur Filterung von Spam zur Verfügung stellen.

In Outlook Express gelangen Sie zu den E-Mail-Filtern über **Extras · Nachrichtenregeln · E-Mail**.

Wie Sie in Abbildung 4.13 erkennen können, vollzieht sich eine Filter-Definition in mehreren Schritten. Als Erstes müssen Sie eine allgemeine Bedingung sowie eine allgemeine Aktion festlegen, also beispielsweise »Enthält den Absender...«

und »Nachricht löschen«. In einem dritten Schritt können Sie diese Aktion detaillierter beschreiben.

Zusätzlich dazu haben Sie noch die Möglichkeit, einzelne E-Mail-Adressen oder Adressen, die einen bestimmten Domainnamen (z.B. @cash.de oder @xxx.de) enthalten, komplett zu blockieren.

Abbildung 4.13 Filterregeln in Outlook Express festlegen

4.5.3 Anti-Spam Tools (Spam-Filter)

Zum Abschluss dieses Abschnitts werden noch einige Hilfsprogramme vorgestellt, mit denen Sie gezielt gegen Spamming vorgehen können und die Sie vor unerwünschten Werbe-E-Mails bewahren:

- **Spam-Eater Pro** – Dieses Tool überprüft Ihren POP-Account auf bekannte Spam-Absenderadressen, von denen Spam Eater mittlerweile etwa 15.000 erkennen kann.

  Download: **http://www.hms.com/downloads.asp**

- **SuperSpamkiller Pro** – Dieses Tool schützt Sie nicht nur vor Spam, sondern auch vor in E-Mails enthaltenen Viren, Würmern und 0190-Dialern.

  Download: **http://www.super-spamkiller.de/**

- **McAfee SpamKiller** – Dieses Programm enthält einen umfangreichen Spam-Filter mit Tausenden bereits vordefinierten Filter-Regeln. Mit dem Filter-

Wizard können Sie jederzeit neue Regeln und Filter hinzufügen und an die gegebene Situation anpassen.

Anhand umfangreicher Spammer-Listen können Junk-Mails wirkungsvoll abgeblockt werden.

Download: **http://www.spamkiller.com**

- **Simons SpamKiller** – Simons SpamKiller spürt nicht nur Spam-E-Mails auf, sondern lokalisiert auch zuverlässig E-Mail-Viren und Würmer. Auch mit den umfangreichen Filtermöglichkeiten, die das Tool bietet, kann Microsofts Outlook Express bei weitem nicht mithalten.

  Das Programm kann beliebig viele Mailkonten abfragen und die dort vorhandenen Nachrichten nach verschiedenen Regeln untersuchen. Unerwünschte Mails werden erst gar nicht an den E-Mail-Client gesendet, sondern sofort vom POP-Server gelöscht.

  Download: **http://www.picsoft.de/swspam.htm**

- **Spam Hater** – Auch Spam Hater macht Schluss mit lästigen Junk-Mails. Das Tool arbeitet mit vielen beliebten E-Mail-Clients wie Eudora, Netscape oder Pegasus Mail zusammen. Das Besondere an Spam Hater ist, dass das Programm den Ursprung einer E-Mail exakt zurückverfolgen kann und automatische Beschwerdebriefe an den Provider des Spam-Versenders oder an den entsprechenden Online-Dienst senden kann. So müssen Sie sich nicht um die zeitaufwändige Aufgabe kümmern, den Header einer Spam-E-Mail zu analysieren.

  Download unter: **http://web.conferencing.co.uk/**

Hinweis Große Internet-Provider wie AOL und T-Online verwenden so genannte Spam-Filter, um die elektronischen Wurfsendungen von ihren Mitgliedern und Kunden fernzuhalten. Die Effektivität dieser Filter ist jedoch sehr zu bezweifeln. Denn in den Listen der Provider sind nur große und hinreichend bekannte Spam-Versender eingetragen. Das weit größere Problem entsteht aber durch die kleinen Spammer, die sehr flexibel sind und permanent ihre Absenderadressen wechseln oder diese gar fälschen. Aus diesem Grunde sollten auch AOL- oder T-Online-Kunden auf ein eigenes Anti-Spam-Tool zurückgreifen und sich nicht darauf verlassen, dass der Provider das komplette Spam-Aufkommen abblockt.

4.6 Spyware

Viele Free- u. Shareware-Programme finanzieren sich durch Werbung und können vom Anwender daher kostenlos genutzt werden.

Während der Arbeit mit einem solchen Programm werden permanent verschiedene Werbebanner eingeblendet, die über das Internet geladen werden. Von vielen Anwendern wird das zwar als störend empfunden, dennoch ist Bannerwerbung völlig legitim und absolut harmlos.

Zu einer echten Bedrohung der Privatsphäre werden diese Programme jedoch, wenn sie heimlich Daten über den Anwender sammeln und bei der nächsten Internetverbindung an den Hersteller oder Vertreiber der Software senden, ohne dass der ahnungslose User etwas davon mitbekommt. Dies ist ein Eingriff in die Privatsphäre des Einzelnen. Denn schließlich geht es niemanden außer Ihnen etwas an, wann und zu welcher Uhrzeit Sie welche Website wie lange besucht haben, welche Software Sie verwenden oder wie Ihr Betriebssystem konfiguriert ist.

Solche Programme, die Benutzerprofile erstellen und persönliche User-Daten heimlich über das Internet versenden, bezeichnet man als **Spyware** oder **Adware** im Sinne von »Advertising Spyware«.

Der Grund für die Datensammelwut ist, dass Werbestrategen ein Interesse daran haben zu wissen, wie effektiv ihre Werbung ist und wie viele Menschen ihre Werbung überhaupt wahrnehmen. Zudem wollen sie so viele Informationen wie möglich über ihre potenziellen Kunden sammeln, um Benutzerprofile zu erstellen, die für die Werbeindustrie von hohem Wert sind.

Inzwischen ist es gang und gäbe, dass Softwarefirmen insgeheim das Nutzerverhalten von Privatpersonen auf diese Weise ausspionieren.

Zu den Vertretern dieser Spezies gehören Firmen wie Adware, Alexa, Cydoor, Gator, OnFlow, Radiate (früher Aureate) oder Web3000.

Bereits 1996 hatte die Firma Aureate (heute Radiate) die Idee, Werbebanner nicht nur in Websites, sondern auch in kleine Software-Applikationen zu integrieren. In Form eines Frage-Antwort-Spiels wurde ein Benutzerprofil erstellt, das werbetreibenden Firmen Informationen darüber liefern sollte, wann (Tag, Datum, Uhrzeit) und wie oft welche URLs und Links aufgerufen wurden. Diese Daten wurden dann bei der nächsten Gelegenheit an ein Werbeunternehmen weitergeleitet, das die gesammelten Informationen auswertete, um schließlich die betreffende Person mit gezielten Werbebotschaften zu bombardieren.

Mittlerweile gibt es massenhaft durch Werbung finanzierte Programme, die die oben genannten Praktiken ausüben.

Da die Spionage-Komponenten als Plug-In in einer Software implementiert sind und sich wie Trojaner und 0190-Dialer in der Registry eintragen, werden Sie den Spion nicht ohne weiteres los.

Es gibt jedoch nützliche Hilfsprogramme, wie **Ad-aware**, die Spyware-Komponenten aufspüren und wirkungsvoll beseitigen können.

Wenn Sie ein durch Werbung finanziertes Freeware-Programm weiterhin nutzen möchten, aber die entsprechende Spyware-Komponente entfernen, kommt es nicht selten vor, dass das Programm nicht mehr einwandfrei funktioniert. Wenn Sie auf das Programm dennoch nicht verzichten wollen, bleibt als Alternative nur noch die kostenpflichtige Registrierung. Das bedeutet aber dann noch lange nicht, dass Ihr Rechner frei von Datenspionen ist oder Ihr Benutzerprofil aus den Datenbanken des Shareware-Anbieters gelöscht wurde.

Folgende Informationen werden von Spyware gesammelt und an den Betreiber übertragen:

- Vom Anwender aufgerufene Webseiten
- Zu welchen Zeiten und wie lange der User online ist
- Verweildauer des Benutzers auf einer Website – Das gibt Aufschluss darüber, für welche Themen sich der Anwender besonders interessiert.
- Suchbegriffe, die der Anwender bei Suchmaschinen eingibt – Das verrät viel über die Interessen und Vorlieben des Anwenders und hilft, Werbung zielgerichtet anzuwenden.
- Welche Software auf dem Rechner des Nutzers installiert ist

4.6.1 So spionieren Softwarefirmen Sie aus

So genannte **Spymodule**, die als Plug-Ins in Freeware-Programme eingebettet wurden, nehmen während einer Online-Session Kontakt zum Hersteller oder einem Werbenetzwerk wie Doubleclick oder Web3000 auf und senden ohne Wissen des Anwenders verschiedene persönliche Informationen an den entsprechenden Server.

Genau wie Trojanische Pferde nutzen sie zur Datenübertragung eine frei-definierbare Portnummer zwischen 1024 und 65.535.

Die Spionageprogramme lesen beispielsweise den Browser-Cache, vorhandene Cookie-Dateien oder die Registry aus, in der alle Systemkonfigurationen von Windows enthalten sind. Die Spymodule scannen gezielt bestimmte Registry-Schlüs-

sel, fassen die gefilterten Daten zusammen und senden sie bei der nächsten Internetverbindung an einen Server.

Damit die Spymodule auch dann noch ihre Aufgabe wahrnehmen können, wenn das eigentliche Programm bereits entfernt wurde, nisten sich die hartnäckigen Plagegeister selbst in der Registrierungsdatenbank ein und sitzen damit quasi direkt an der Quelle – schon wieder eine Gemeinsamkeit mit Trojanern (und vielen 0190-Dialern).

Die am weitesten verbreiteten Spionage-Komponenten sind die beiden Aureate-Dateien `advert.dll` und `amcis.dll`. Hierbei handelt es sich um so genannte Dynamic Link Libraries (DLL), die bei der Programminstallation ins Windows-Systemverzeichnis (**C:\Windows\System**) kopiert werden.

Durch Firewall-Protokolle wurde festgestellt, dass die `advert.dll` während einer bestehenden Internetverbindung den Usernamen, die IP-Adresse, die vom Benutzer zuletzt aufgerufenen URLs (durch das Auslesen der History bzw. des Verlauf-Ordners aus dem Browser), die Verweildauer sowie die Software-Registrierungsschlüssel an einen Internet-Server sendet. Hierfür nutzt sie den TCP-Port 1749.

Die Datei `amcis.dll` scant die Registry und überträgt Softwareschlüssel von Browsern und anderen Programmen.

Spyware = Trojaner?

Wie oben erläutert wurde, haben Spyware und Trojaner viele Gemeinsamkeiten

- Ausspähen von Daten
- Client-Server-Kommunikation über Ports
- Manipulation der Registry

Auch wenn Spyware dieselben Methoden wie Trojaner anwendet, gibt es dennoch einige Unterschiede:

- Trojaner spähen persönliche Benutzerdaten wie Passwörter, Kreditkartennummern etc. heimlich aus, wohingegen Spyware marketing-relevante Benutzerprofile erstellt.
- Trojaner werden heimlich ins System des Anwenders eingeschleust; Softwarehersteller weisen den Anwender bei der Programminstallation hingegen darauf hin, dass ihre Software bestimmte Funktionen zur Datenerfassung beinhaltet. Leider sind solche Hinweise nicht auf Anhieb zu erkennen

und oft missverständlich formuliert. Zudem wird kaum ein Anwender sich die Mühe machen, bei jeder Installation einer neuen Software die meist ellenlangen Lizenzbedingungen komplett durchzulesen. Auf diese Weise installiert man ein Programm, bei dem man sich nicht darüber im Klaren ist, dass es persönliche Daten ausspäht.

Eine Spyware, die den Benutzer nicht über ihre Spionagefunktionen informiert, kann man in jedem Fall als Trojaner bezeichnen.

4.6.2 Welche Programme übertragen Daten an einen Internet-Server?

In Tabelle 4.3 finden Sie eine alphabetische Auflistung bekannter Programme, die entweder Spymodule enthalten oder bei denen vermutet wird, dass sie System- und Benutzerdaten ins Internet senden. Bei den meisten Produkten lässt sich dies jedoch durch Firewall- oder Sandboxprotokolle nachweisen.

Die meisten Hersteller überprüfen dabei lediglich die Seriennummer von installierten Programmen, um festzustellen, ob der Anwender das Original oder eine Raubkopie verwendet. Darüber hinaus beinhalten einige Programme noch Funktionen, die das System gezielt nach der Konfiguration oder bereits installierter Software (beispielsweise konkurrierender Unternehmen) durchsuchen und nach Daten des Benutzers Ausschau halten, um diese bei bestehender Internetverbindung an einen Webserver zu senden.

Tipp Wenn Sie ein Update auf Windows XP durchführen, sollten Sie Ihren Rechner anschließend von Spyware befreien. Denn mit Windows XP wird gleichzeitig auch der Internet Explorer 6 mitinstalliert, der Spionage-Plug-Ins von der Firma Alexa enthält. Das Gleiche gilt natürlich bei einem Update von IE 5.5 auf IE 6. Das hierfür nötige Tool können Sie sich unter **http://www.xp-antispy.de** kostenlos aus dem Internet herunterladen.

Software-Hersteller/Produkt	Beschreibung
Abe`s MP3 Finder	sendet Daten über den User und die Systemkonfiguration
ACDsee V3.1e	übermittelt Seriennummer und Produkt-ID, sowie Benutzer- und Betriebssysteminformationen
CD MP3 Studio	enthält Cydoor-Spy-Programme
ChrystelFTP Freeware	enthält den »TimeSink Advertising Bot«

Tabelle 4.3 Software mit Spionage-Plug-Ins

Software-Hersteller/Produkt	Beschreibung
CuteFTP	installiert Radiate-Dateien auf den Rechner
Macromedia Dreamweaver	stellt eine Verbindung zum Hersteller her und sendet Registry-Daten und die Seriennummer an Macromedia
Download Accelerator Plus	liest die Seriennummer des Programms während einer Online-Session
Eudora 5	sendet unbekannte Daten über das Internet
FlashGet	enthält Aureate- und Cydoor-Spione
Getright	übermittelt heimlich Daten an den Hersteller
Hypersnap	enthält Radiate Spy-Module
ICQ 2000a	überträgt bei einer Internetverbindung Daten aus der System-Registry
Namo Webeditor 4.02	überträgt unbekannte Daten ins Internet
Microsoft Internet Explorer 6	enthält Spyware von Alexa
Neoplanet	beinhaltet Werbebanner der Firma Doubleclick und übermittelt vermutlich User- und Systemdaten
Opera Browser	enthält Cydoor-Spy-Module
Partition Magic 5	sendet über das Internet Daten an den Hersteller
Planet MP3.find	beinhaltet Komponenten von Radiate
Printshop	enthält einen DSSAgent von Broadcast, der zur Übermittlung von Benutzerprofilen eingesetzt wird
Winace	überprüft die Programm-Seriennummer und überträgt den Usernamen an einen Internet-Server
Windows Media Player 7 bis 9	generiert einen so genannten GUID (Global Unique Identifier), der Streaming-Anbietern die eindeutige Identifizierung des Users ermöglicht

Tabelle 4.3 Software mit Spionage-Plug-Ins (Forts.)

Webtipp Die Website **http://www.tom-cat.com/spybase/index.html** enthält eine Liste mit mehr als 850 Programmen, die eindeutig als Spyware eingestuft werden können.

4.6.3 Erkennung und Beseitigung von Spionage-Modulen

Nun möchten Sie sicher gern wissen, ob sich auf Ihrem Rechner Spionage-Software befindet.

Es gibt mehrere Möglichkeiten, wie Sie dies herausfinden können und wie Sie verhindern können, dass Datenspione Ihre persönlichen Daten insgeheim versenden:

1. **Einsatz einer Sandbox** – Hiermit können Sie jeder Anwendung, die sich auf Ihrem Rechner befindet, Zugriffsrechte auf bestimmte Rechner-Ressourcen zuteilen. Diese Rechte können Sie individuell nach Ihren eigenen Bedürfnissen festlegen. Der Einsatz einer Sandbox setzt allerdings ein wenig Erfahrung voraus. Einige Sandbox-Programme sind in Kapitel 6 aufgeführt.
2. **Firewalls** – Firewalls schützen den PC nicht nur vor unbefugten Zugriffen aus dem Internet, sondern überwachen die Ports, über die Daten ins Internet gesendet und aus dem Internet empfangen werden. Sie eignen sich daher hervorragend, um Datenspionen auf die Schliche zu kommen und um Datenübertragungen zu protokollieren. Wie beim Aufspüren von Trojanern können Sie mit Hilfe eines Portscanners feststellen, ob verdächtige TCP-Ports auf Ihrem Rechner offen sind. Wenn Sie einen von einer Spyware verwendeten Port gefunden haben, können Sie diesen mit einer Firewall blockieren, um eine Datenübertragung über diesen Port zu unterbinden. Manche Sypware-Module verwenden für den Datentransfer jedoch den TCP-Port 80, der für die HTTP-basierte Kommunikation von Ihrem Browser benötigt wird. Diesen Port können Sie natürlich nicht mit einer Firewall schließen, da Sie ansonsten keine Webseiten mehr aufrufen können.
3. **Anti-Spyware-Tools** – Diese Hilfsprogramme suchen gezielt nach Spy-Modulen und entfernen diese bei Bedarf aus Ihrem System:
   - **Ad-aware** – Dieses kostenlose Programm vom Hersteller Lavasoft durchsucht den Arbeitsspeicher, die Registrierungsdatenbank und die gesamte Festplatte nach Spionagekomponenten, wie sie in Adware und Bannerware enthalten sind. Die bekanntesten Spyware-Module werden dabei aufgespürt und dauerhaft aus dem System entfernt. Das Tool findet unter anderem Module von Aureate, Doubleclick, DSSAgent, TimeSink, Web3000 und Webhancer.

     Als Ergänzung zu Ad-aware ist das Monitorprogramm Ad Watch zu empfehlen, das im Hintergrund die Registry permanent überwacht. Sobald eine Spyware einen Eintrag in der Registrierungsdatenbank vornehmen will, schlägt Ad Watch Alarm und verhindert, dass das Werbe-Plug-In sich im System einnistet.

     Ad-aware können Sie unter **http://www.lavasoft.de** herunterladen.

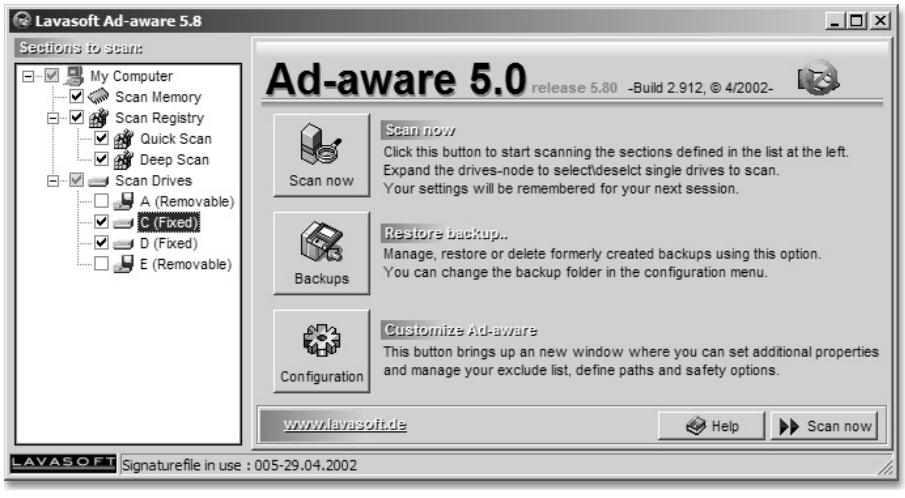


Abbildung 4.14 Ad-aware von Lavasoft

- **Spybot Search and Destroy** – Ein Tool zum Auffinden und Entfernen von so genannten Spybots. Dies sind kleine Zusatzprogramme, die in unregistrierten Software-Applikationen automatisch Werbung einblenden.

  Viele dieser Werberoboter enthalten zudem Spionagefunktionen, um bei aktiver Internetverbindung Informationen über den User oder installierte Software an einen Webserver zu senden. Das Tool entfernt die für die Werbung und Spionage zuständigen Programmteile, ohne dabei die Funktionstüchtigkeit der Software zu beeinträchtigen.

  Download und Info: **http://spybot.eon.net.au**

- **PestPatrol** – Dieses Programm macht das System nach einem Port-Crash, der durch die Datenübermittlung von Adware verursacht wurde, wieder stabil und hält nach Trojanern und Spy-Modulen Ausschau.

  Download und Info: **http://www.pestpatrol.com/**

4.7 Quellen im Internet

Beschreibung	URL
Anonym im Internet	**http://easy.to/privacy**
Electronic Privacy Information Center	**http://www.epic.org**
Anonymizer.com	**http://www.anonymizer.com/**
Rewebber	**http://www.rewebber.de**
Webwasher	**http://www.webwasher.de**

Beschreibung	URL
Junkbuster	http://www.junkbuster.com
Stay Invisible	http://www.stayinvisible.com/index.html
Proxyliste	http://www.proxylist.com/
allproxy.com	http://www.allproxy.com/
Proxys4all	http://proxys4all.cgi.net
Multiproxy	http://www.multiproxy.org
Datenschutz Berlin	http://www.datenschutz-berlin.de/
Datenschutz-Informationen der juristischen Fakultät der Humboldt-Universität Berlin	http://www.rewi.hu-berlin.de/index.php?path=./jura/proj/dsi/
Der Bundesbeauftragte für den Datenschutz	http://www.bfd.bund.de
Deutsche Vereinigung für den Datenschutz e.V.	http://www.aktiv.org/DVD
DuD – Datenschutz und Datensicherheit	http://www.dud.de/
Cookie Cruncher	http://www.RBAworld.com/Programs/Cookie-Cruncher
Cookiecentral	www.cookiecentral.com
Cookies und deren Gefahren	http://www.techfak.uni-bielefeld.de/rechner/cookies.html
Computec: Cookies	http://www.computec.ch/mruef/texte/cookies.html
Der Hirnbrauser	http://www.hirnbrauser.de
Robinsonliste	http://www.robinsonliste.de/