In diesem Kapitel:

- Passwörter und Benutzer-Accounts
- Wireless LAN
- Umgang mit wichtigen Daten
- Sicherheitsrelevante Windows-Optionen
- Bewusster Surfen

KAPITEL 3

Sicherheitsbewusstsein

Während in Kapitel 1, *Gefahren und Akteure im Internet*, eher theoretische Vorüberlegungen zur Sicherheit im Internet im Vordergrund standen, werden in diesem Kapitel einige praktische Probleme aufgegriffen und näher erläutert. Im Einzelnen werden wir uns mit folgenden Themenbereichen beschäftigen:

- Passwörter: Welche Rolle spielen Passwörter, wie wählt man ein sicheres aus und wie lassen sich unsichere Passwörter erbeuten?
- Wireless LAN: Wie lassen sich drahtlose Netzwerke absichern, damit keine unerwünschten Gäste mitsurfen oder Daten ausspionieren?
- Datenverlust: Was können Sie dagegen unternehmen? Wie sichern Sie Ihre sensiblen Dokumente?
- Software und Betriebssystem: Was gehört auf die Festplatte und was nicht? Wie können Sie sich vor Einbrechern schützen?
- Vertrauenswürdigkeit: Woran können Sie seriöse Service-Anbieter und Websites erkennen, und in welche Fallen sollten Sie nicht tappen?

Passwörter und Benutzer-Accounts

Passwörter sind ein zentraler Sicherungsmechanismus im Internet. Zusammen mit dem Benutzernamen bilden sie einen so genannten *Benutzer-Account*. Dabei handelt es sich um eine Art Konto, über das die Profildaten und die (Kunden-)Historie des Benutzers verwaltet werden. Wenn Sie sich beispielsweise bei Ihrem Provider einwählen, müssen Sie diese Informationen übermitteln, um sich als rechtmäßiger Benutzer ausweisen zu können. Anhand dieser Daten kann der Provider dann feststellen, welcher Benutzer wann und wie lange im Internet war. Dabei spielt der Ort der Einwahl für den Anbieter keine Rolle. Ob sich ein Benutzer von zu Hause, aus einem Hotel oder per Notebook aus dem Ferienhaus einwählt: Es sind seine Zu-

gangsdaten, die ihn einwandfrei ausweisen.[1] Für die sichere Aufbewahrung dieser Zugangsdaten sind Sie als Benutzer voll verantwortlich, und man wird Sie bei Missbrauch zur Verantwortung ziehen.

Gelingt es beispielsweise einem Fremden, an Ihren Benutzernamen und das dazugehörige Passwort zu gelangen, kann er anschließend auf Ihre Kosten surfen. Selbst wenn man einwandfrei nachweisen kann, dass die Kosten nicht durch das eigene Surfverhalten entstanden sind, wird der Provider nur in wenigen Fällen so kulant sein, nicht auf das Begleichen der Rechnung zu bestehen.

Besonders beliebt ist auch das Cracken von eBay-Accounts. Der Angreifer kauft anschließend Ware für tausende oder gar hunderttausende von Euros und freut sich über den Schaden, den er damit anrichtet. 2005 wurden auch in Deutschland viele Fälle dieser Art bekannt. Teilweise hatten Angreifer mehrere hundert Artikel, darunter auch Autos oder Schiffe, innerhalb weniger Tage bestellt. eBay reagiert in diesen Fällen glücklicherweise sehr kulant und schnell, dennoch bleibt die Situation für den Geschädigten unangenehm.

Nach einem solchen Angriff ist immerhin klar, dass jemand mit Ihren Daten Unfug getrieben hat, und Sie können das Passwort ändern und den Angreifer somit aussperren. Viel häufiger kommt es jedoch vor, dass sich der Cracker unauffällig verhält und im Hintergrund bleibt.

Um die Gefahr zu verringern, beim Cracken erwischt zu werden, bedienen sich geschickte Angreifer gern fremder Zugangsdaten, um bei einem fehlgeschlagenen Einbruch in einem fremden System anonym zu bleiben. Auch in diesem Fall wird sich das betroffene Unternehmen an Sie wenden, da die Spuren des Angreifers in Ihre Richtung deuten. Wählt sich ein Cracker beispielsweise mit Ihren Zugangsdaten beim Provider ein, erhält er, wie in Kapitel 2, *Technische Hintergründe*, erläutert, eine dynamische IP-Adresse. Da der Provider aber die Zuordnung von IP-Adresse und Benutzernamen speichert, werden Sie anschließend mit dem Einbruch in Zusammenhang gebracht. Da es für einen Cracker nicht ohne Weiteres möglich ist, Ihr Passwort auszuspionieren, ohne dass beispielsweise Trojaner auf Ihrem System installiert sind, begnügen sich viele Angreifer damit, andere Zugangsdaten zu erbeuten.

Besonders hoch im Kurs stehen dabei Passwörter von Freemail-Accounts. Da der Benutzer hier sowohl Benutzernamen als auch Passwort frei wählen kann, ist dies für Cracker in der Regel ein leichtes Spiel. Trotz zahlreicher Berichte im Fernsehen und im Internet wählen immer noch sehr viele Benutzer die Passwörter so leichtsinnig, dass nicht einmal drei Versuche nötig sind, um Zugriff auf einen Account zu bekommen. Hat der Cracker erst einmal die Daten, kann er den dazugehörigen

1 Bei Internet-by-Call-Verbindungen ist dies nicht der Fall, hier erfolgt die Zuordnung von IP-Adresse und Benutzer über die Telefonnummer. Die Account-Daten sind hierbei für alle Benutzer gleich, z.B. als Account-Name der Name des Anbieters und als Passwort das Wort »Internet«.

Benutzer ausspionieren, indem er seine Mails liest und selbst Mails schreibt. Die Empfänger dieser Nachrichten glauben natürlich, mit dem echten Benutzer zu kommunizieren.

Je aktiver Sie sich im Internet bewegen, desto mehr Accounts werden Sie auf Dauer besitzen. Da wäre beispielsweise der Account beim Provider, auf dem Mailserver, der Zugang zur eigenen Webseite, die Einwahl in das Firmennetzwerk und zahlreiche weitere Konten bei Online-Shops, Chats, Foren, Blogs und Online-Spielen. Der Einfachheit halber können Sie für alle Accounts einen identischen Benutzernamen wählen.[2] Dies gilt jedoch nicht für die Passwörter! Jeder Account sollte unbedingt ein eigenes, einmaliges Passwort erhalten. Wegen der oft unterschätzten Bedrohung, die aus unsicheren Zugangsdaten resultiert, wollen wir uns näher ansehen, welche Aspekte für die Sicherheit eines Passworts relevant sind.

Unsichere Passwörter

Je weniger Zeichen ein Kennwort hat, desto leichter ist es durch Zufall zu erraten. Benutzen Sie daher möglichst Passwörter, die mindestens sechs, besser acht, Zeichen enthalten. Natürlich darf das Kennwort nicht identisch mit dem Benutzernamen sein. Ebenfalls sollte es nicht Ihr Vor- oder Nachname oder der eines Familienmitglieds sein.

Ungeeignet sind außerdem Geburtsdaten sowie Namen der Lieblingsländer, -städte, Freizeitaktivitäten o.Ä. Solche Passwörter sind nicht sicher, da es ausreicht, den Benutzer ein wenig zu kennen, um zu erahnen, welches Passwort er wählen könnte. Ein Musikfan sollte also nicht den Namen der Lieblingsband als Kennwort wählen. Besonders hoch ist die Trefferquote bei »Passwort«, »123456« oder »qwert«. Es gibt im Internet tausende von Accounts, in die man mit einem dieser drei Passwörter einbrechen kann. Als unsicher gelten im Prinzip alle rein lexikalischen Wörter.

Sichere Passwörter

Wie bereits erwähnt, sollte das Passwort nicht kürzer als sechs Zeichen sein. Benutzen Sie dabei sowohl Groß- und Kleinbuchstaben als auch Zahlen und Sonderzeichen. Ein Passwort wie »IlCQ13!« kann im Gegensatz zu »security« als sicher gelten. Doch wie soll man sich diese komplizierten alphanumerischen Kennwörter merken?

Eines sollten Sie auf keinen Fall machen: Ihr Passwort in einer Textdatei auf dem Computer speichern oder gar als Post-it-Notiz an den Monitor kleben!

2 Dennoch sollten Sie beachten, dass es bei gleich bleibendem Benutzernamen und/oder E-Mailadresse für Dritte leichter wird, eine Verbindung zwischen den einzelnen Accounts herzustellen. Ist dies unerwünscht, sollten Sie verschiedene Benutezrnamen wählen.

Folgender Trick hilft Ihnen, sichere Passwörter zu generieren und sie sich dennoch gut einzuprägen: Überlegen Sie sich einen Satz, der zu dem Account passen könnte, und wählen Sie nun die Anfangsbuchstaben der Wörter dieses Satzes als Passwort. Das Kennwort ist dann meist lang und sicher genug, aber auch leicht zu merken. Aus »Dies ist mein Passwort für den Provider!« entstünde so das Kennwort »DimPfdP!«. Vielleicht findet sich dann noch eine Zahl, die Sie unterbringen können, und fertig ist ein sicheres Passwort. Vorraussetzung ist natürlich, dass der Satz nicht zu kurz oder zu leicht zu erraten ist.

Wenn Sie mit der Zeit so viele Accounts einrichten, dass Sie sich diese nicht mehr merken können, gibt es im Internet zahlreiche kostenlose Programme zum Passwortmanagement. Da solche Programme ihrerseits Sicherheitslücken aufweisen können und es sehr schwierig werden dürfte, die Entwickler für Fehler haftbar zu machen, ist von der Verwendung dieser Software eigentlich abzuraten. Ob Sie in gewissen Situationen eine Ausnahme machen, hängt vom persönlichen Sicherheitsbedarf und dem Grad der Gefährdung ab. Daher kann es durchaus in Frage kommen, weniger kritische Account-Daten (wie z.B. diejenigen zu einem Chat oder Forum) in der Passwortverwaltung Ihres Bowsers zu hinterlegen. Achten Sie in solchen Fällen jedoch unbedingt auf eine zusätzliche Sicherung per Master-Passwort.[3] Programme zur Passwortverwaltung basieren im Prinzip alle auf der gleichen Idee: Das Programm speichert alle Ihre Account-Daten samt einer kurzen Info zum Verwendungszweck. Ein Master-Passwort schützt dabei vor unbefugtem Zugriff auf die eigentliche Datenbank. Die dort gespeicherten Passwörter sind stark verschlüsselt und liegen nicht im Klartext auf der Festplatte.

BIOS- und Supervisor-Passwort

Ein Kennwort wird immer nur für einen bestimmten Bereich des Computers oder einen bestimmten Dienst vergeben. Das Passwort zur Einwahl beim Provider schützt also nur den Internetzugang. Befindet man sich bereits im Internet, ist es nutzlos. Man muss sich daher stets klar machen, was genau durch das Kennwort geschützt wird. So schützt das Passwort, das Sie in Ihrem E-Mail-Client eingeben, weder vor dem Lesen Ihrer bereits empfangenen Post noch vor dem Schreiben von Mails über Ihren Account. Der Schutz beschränkt sich hier überraschenderweise auf das Herunterladen neuer E-Mails. Es ist also nicht immer ersichtlich, was durch das Passwort geschützt wird. Warum das so ist, werden wir in Kapitel 6, *E-Mail – wer liest mit?*, näher erläutern.

Besonders deutlich wird dieses Problem beim Betriebssystem. Unter Windows 2000 oder XP sowie beim Einsatz von Zusatzsoftware unter Windows 95, 98 und ME schützt der Benutzer-Account nur vor illegalem Zugang zum Betriebssystem selbst.

3 Beachten Sie dazu auch die entsprechenden Absätze in Kapitel 5, *Browser – einer für alles*.

Der Schutz gilt weder für das Dateisystem des Computers[4] noch für eventuell im Hintergrund arbeitende Dienste. Dies bedeutet, dass die Sicherheitsmaßnahmen erst dann greifen, wenn das Betriebssystem bereits geladen ist. In ähnlicher Form gilt das übrigens für alle Systeme, also auch für Linux, Unix und MacOS. Gelingt es nun einem Angreifer, Zugang zum Computer zu bekommen, bevor das Betriebssystem geladen ist, kann er den Passwortschutz umgehen. In der Praxis ist dies durch einfaches Neustarten per Reset-Taste möglich. Mit einer Boot-Diskette oder -CD kann der Angreifer ein eigenes Betriebssystem booten und alle auf der Festplatte enthaltenen Daten auslesen, ohne sich per Passwort ausweisen zu müssen. Auf zahlreichen Windows-Einzelplatzsystemen bedarf es je nach Windows-Version hierzu nicht einmal einer Diskette, da man mit der F8-Taste das System umgehen und unter DOS booten kann.

Zu einer wirkungsvollen Absicherung ist also ein Kennwort nötig, das auf einer früheren Ebene einsetzt und nicht umgangen werden kann. Es gibt bei jedem Computer die Möglichkeit, ein so genanntes *Supervisor-Passwort* zu vergeben, ohne das der PC schon beim Starten abbricht. Um dieses Passwort festzulegen, müssen Sie Ihren Computer neu starten und anschließend sofort ins BIOS (*Basic In- and Output-System*) wechseln. Bei den meisten PCs gelangt man über die Entf- oder die F2-Taste ins BIOS. Da einige Hersteller von diesen typischen Tasten abweichen und das BIOS je nach Modell und Hersteller unterschiedlich aufgebaut ist, ist gegebenenfalls ein Blick ins Handbuch erforderlich.

Interessant sind für uns nur die Einträge SUPERVISOR PASSWORD und BIOS PASSWORD. Die genauen Bezeichnungen können dabei jedoch variieren. Das BIOS-Passwort sichert nur den Zugang zum eigentlichen BIOS, während das Supervisor-Kennwort bei jedem Start abgefragt wird. Da die Abfrage noch vor dem Bootvorgang liegt, ist es auch nicht möglich, ohne Kennwort von Diskette oder CD zu booten.[5] Da das BIOS eine zentrale Schaltstelle ist und direkten Einfluss auf die Hardware hat, sollten Sie aber unter keinen Umständen Änderungen an anderen Einstellungen vornehmen, wenn Sie nicht genau wissen, was Sie tun. Dies könnte im Extremfall sogar zur Beschädigung Ihrer Hardware oder zumindest zu starken Performance-Verlusten führen. Wenn Sie an einem Computer innerhalb eines Firmennetzwerks arbeiten, sollten Sie vor der Einrichtung von Passwörtern auf BIOS-Ebene unbedingt Ihren Systemadministrator zu Rate ziehen.

Hat ein Angreifer ungestört physischen Zugang zu einem Computer, kann er zudem auf vielfache Weise BIOS-Passwörter umgehen oder Daten direkt von der Festplatte lesen. Gestohlene Notebooks mit internen Unternehmensdaten sind daher ein

4 Bei NTFS-Partitionen sieht dies hingegen anders aus und daher sollten Sie Ihre Partitionen, wenn möglich, nicht mehr als FAT-Partitionen anlegen

5 Leider ist auch dieser Schutz nicht unumgänglich, denn es existieren für die meisten Modelle so genannte Master-Passwörter, mit denen man den Kennwortschutz aushebeln kann. Unter *http://www.bios-info.de* finden Sie bei Interesse eine umfangreiche Liste mit Master-Passwörtern.

ernsthaftes Problem, das nur durch die Verschlüsselung des Dateisystems oder einzelner senibler Bereiche zu lösen ist. Selbst große Unternehmen nehmen diese Gefahr jedoch anscheinend kaum ernst.

Wie Passwörter erraten werden

Warum sollten Sie eigentlich keine lexikalischen Ausdrücke als Passwörter wählen? Der Angreifer kann doch ein Kennwort wie »Vulkan« unmöglich erraten? Stimmt, bei der nahezu unbegrenzten Menge an möglichen Wörtern dürfte der arme Cracker wohl bis an sein Lebensende damit beschäftigt sein, das passende Wort zu ermitteln. Doch in der Realität braucht sich der Angreifer nur einige Minuten zurückzulehnen und zu warten, bis der Computer diese Aufgabe für ihn erledigt hat.

Die dafür geeigneten Methoden fasst man unter dem Begriff *Wörterbuchangriffe* zusammen, die wiederum zu den Brute-Force-Angriffen zählen, also solchen, die nicht auf Effizienz, sondern auf pure Gewalt (hier im Sinne von Rechengeschwindigkeit) setzen. Dabei spielen zwei Komponenten eine wichtige Rolle: Die eine Seite besteht aus einem Wörterbuch der häufigsten Passwörter wie beispielsweise Namen und typische Zahlenkombinationen. Diese Wortsammlungen stehen im Internet frei zur Verfügung und können von Benutzern immer wieder um neue Wörter ergänzt werden. Ist das Repertoire dieses Wörterbuchs erschöpft, werden weitere Ausdrücke generiert, indem beispielsweise Zahlenreihen durchlaufen werden. Die zweite Komponente besteht aus dem Programm, das die Passwortabfrage mit dem Dienst koordiniert. Ein bekanntes Beispiel für ein solches Programm ist das unter Linux verfügbare *Jack*. Das Programm liest Begriffe aus dem Wörterbuch ein, verschlüsselt sie und vergleicht sie mit der Datei *.../etc/shadow* (dort befinden sich bei zahlreichen Linux-Distributionen die verschlüsselten Passwörter). Kennwörter wie »Vulkan« oder »Antigone« werden von *Jack* je nach Kapazität des Computers innerhalb von Sekunden entschlüsselt und im Klartext angezeigt. *Jack* ist in der Lage, nahezu alle lexikalischen Passwörter innerhalb einer halben Stunde zu knacken.

Bei gut gewählten Passwörtern mit einer Länge von mehr als sechs Zeichen sind solche Wörterbuchangriffe glücklicherweise fast aussichtslos. Zudem muss man beachten, dass die meisten Angreifer nach kurzer Zeit die Geduld verlieren und versuchen, einen der vielen anderen Accounts zu knacken. Die Passwörter vieler Freemail-Benutzer sind wie beschrieben jedoch so simpel, dass es nicht einmal eines Programms bedarf, um hier einen Zugang zu erlangen.

Grundsätzlich muss man zwischen dem Angriff auf passwortverschlüsselte Inhalte in Form von Dateien und dem Angriff auf Account-Daten im Internet unterscheiden. Nehmen wir an, dass ein Cracker eine DVD oder ein Notebook mitsamt durch ein Sicherheitsprogramm verschüsselten Inhalten erbeutet hat. Fordert ihn das Programm bei jedem Zugriffsversuch auf, ein Passwort einzugeben, und blockiert den Zugriff nicht nach einer bestimmten Anzahl von Fehleingaben für längere Zeit, so stehen dem Angreifer unendlich viele Versuche offen. Da die Kommunikation zwi-

schen Angriffswerkzeug und Sicherheitstool schnell erfolgt, kann er innerhalb weniger Minuten viele tausend oder gar zehntausend Wörterbuchanfragen durchführen.

Versucht der Angreifer hingegen einen Account auf einem Server zu knacken, dauert es jeweils einige Millisekunden oder gar Sekunden, bis eine Antwort vom Server kommt. Die Geschwindigkeit des Angriffs wird damit massiv herabgesetzt. Der Angreifer muss sich daher in der Regel mit wenigen hundert Anfragen pro Minute begnügen, teilweise können es sogar noch deutlich weniger sein. Selbst wenn der Server entsprechend schnell reagiert, wäre es eine große Dummheit, zu viele Versuche auf einmal zu unternehmen. Sicherheitsbewusste Serverbetreiber stellen die Software auf ihren Servern so ein, dass sie bei typischen Brute-Force-Angriffswellen Alarm schlägt, die IP-Adresse des Angreifers speichert[6] und den angegriffenen Account vorsichtshalber für eine Zeit sperrt. Daher wird ein professioneller Angreifer gezielt nach Informationen über den Account suchen, um mit mehr Hintergrundwissen effizient und mit wenigen Versuchen erfolgreich angreifen zu können. Das soll jedoch nicht bedeuten, dass es im Internet nicht täglich viele tausend erfolgreiche Angriffe durch massive Brute-Force-Techniken gibt, die Frage ist nur, ob der Serverbetreiber in solchen Fällen seine Hausaufgaben richtig gemacht hat.

Ihnen als Benutzer sollte nach dem Lesen dieses Abschnitts Folgendes im Gedächtnis bleiben: Die Sicherung von Daten mit Hilfe von Passwörtern ist sehr wirkungsvoll und im Moment de facto konkurrenzlos. Falsch konfigurierte Server, fehlende Sicherheitsmaßnahmen, Programmierfehler und vor allen Dingen schlecht gewählte Passwörter liefern Angreifern aber immer wieder genügend Ansatzpunkte.

Passwörter speichern

Neben den Passwortmanagern bieten Ihnen zahlreiche weitere Programme an, Ihre Zugangsdaten zu speichern. Abbildung 3-1 zeigt das Dialogfenster VERBINDUNG MIT in Windows XP. Auch hier wird Ihnen angeboten, das Kennwort zu speichern. Aus Sicherheitsgründen sollte diese Option jedoch nur mit Bedacht aktiviert werden.

Es gibt, wie bereits angesprochen, zwei Gründe, generell keine Passwörter von Anwendungen speichern zu lassen: Erstens kann dadurch jeder Fremde, der vor Ihrem Computer sitzt, direkt Zugriff zum Internet oder anderen passwortgeschützten Bereichen erlangen. Da das Kennwort fest eingegeben ist, können Sie nicht einmal nachvollziehen, ob jemand an Ihrem Computer gearbeitet hat. Der zweite Grund besteht in der Möglichkeit, auf Datenträgern gespeicherte Passwörter auszulesen. Die Zusicherung der Hersteller, dass diese mit starker Kryptografie geschützt seien, ist in der Regel nicht viel wert, da Tools wie *Jack* in Dateien abgelegte Kennwörter ermitteln können. Die heutigen Verschlüsselungsverfahren sind so konzipiert, dass eine Entschlüsselung im Prinzip nicht möglich ist; daher benutzen die

6 Gerade deswegen versuchen Angreifer, von anderen Rechnern aus anzugreifen oder Ihre IP-Adresse zu manipulieren (IP-Spoofing).

Abbildung 3-1: Das Dialogfenster »Verbindung mit« in Windows XP

Angriffswerkzeuge das bereits erläuterte Vergleichsverfahren, um an die Zugangsdaten zu gelangen. Dennoch darf auch hier nicht vergessen werden, dass Programmierfehler in den für die Verschlüsselung zuständigen Programmen den gesamten Schutz aushebeln können. Wenn Sie sich den Arbeitsplatz mit mehreren Benutzern teilen, sollten Sie Passwörter generell nicht abspeichern.

Passwörter auf dem Server

Für Account-Daten, die Sie auf ihrem lokalen System verwalten, tragen Sie die Verantwortung und haben es somit selbst in der Hand, wie gut diese Daten geschützt werden. Im Fall von Internet-Accounts (wie etwa Ihren Zugangsdaten zu einem Online-Shop) gibt es aber noch eine zweite Partei, die Datensicherheit gewährleisten muss.

In der weit verbreiteten Forensoftware *phpBB2* wurde beispielsweise 2005 eine Lücke gefunden, durch die es möglich war, sich ohne das richtige Passwort mit jedem beliebigen Account einzuloggen. Ein Angreifer konnte also Ihre privaten Nachrichten lesen und Ihr Profil einsehen und verändern. Ebenso war es möglich, sich als Administrator anzumelden und Forenbeiträge oder Benutzer zu löschen. Nur wenige Wochen nach Bekanntwerden der Sicherheitslücke brachten Cracker einen Wurm in Umlauf, der viele tausend Foren erfolgreich kompromittierte.

Auf ähnliche Art und Weise gelangen Angreifer immer wieder in den Besitz vertraulicher Informationen oder gar Passwörter. Als Benutzer eines betroffenen Systems erfahren Sie meist nichts über den Vorfall und über die Art der erbeuteten Daten.

Die einzige Lösung ist daher, verschiedene Passwörter für jeden Account zu benutzen und in Profilformulare nur die allernötigsten Daten einzugeben. Ebenso empfiehlt es sich, einen E-Mail-Account anzugeben, bei dem Sie verschmerzen können, wenn er massiv mit Spam bombardiert wird.

Benutzer- und Gruppenprofile in der Windows-Welt

Echte Multi-User-Betriebssysteme wie etwa Linux erlauben eine separate Verwaltung von Benutzern eines einzelnen PCs und ihren Dateien. Das kann so weit gehen, dass eine von Person A gespeicherte Datei (auf Wunsch) von Person B nicht einmal geöffnet oder gelesen werden kann. Jeder Benutzer und alle seine Dateien sowie von ihm installierten Programme sind völlig unabhängig von den anderen User-Accounts auf demselben PC. Zudem kann man Benutzer in Gruppen zusammenfassen und diesen Gruppen bestimmte Rechte erteilen.

Ein Beispiel dafür ist die Finanzabteilung eines Unternehmens. In der Abteilung arbeiten fünf Angestellte, von denen jeder der Gruppe »Finanzen« angehört. Die Dateirechte sind so gesetzt, dass jeder Benutzer die Daten der anderen Mitglieder zwar lesen, aber nicht verändern kann. Benutzer, die nicht zur Gruppe »Finanzen« gehören, haben gar keinen Zugriff auf die Daten. Auch könnte man festlegen, wer Zugang zum Internet erhalten darf und wer nur den E-Mail-Dienst nutzen soll. Einzig der Superuser (z.B. unter Unix/Linux der Benutzer *root*), also der Systemadministrator, hat alle Rechte. Fängt sich einer der Benutzer einen Virus ein, kann dieser nur innerhalb des befallenen Accounts aktiv werden. Dem Schädling stehen also keine Systemdateien zur Verfügung. Nur wenn der Virus den Benutzer *root* befällt, besteht Gefahr für das System. Solche echten Mehrbenutzersysteme sind aus sicherheitstechnischer Sicht natürlich empfehlenswert. Auch bei Windows 2000 und Windows XP handelt es sich zwar um Multi-User-Systeme, diese sind aber, im Bezug auf ihr Mehrbenutzerverhalten, noch nicht so ausgereift wie etwa Linux.

Abbildung 3-2: Der Anmeldebildschirm in Windows XP

Bei älteren Windows-Versionen wie etwa Windows 95, 98 oder ME wird zwar der Eindruck eines Multi-User-Systems erweckt, jedoch völlig ohne die oben genannten Differenzierungen und die sich daraus ergebenden Vorzüge. Diese Systeme sind mittlerweile deutlich veraltet und sollten, wenn irgend möglich, nicht mehr eingesetzt werden.

Bei den modernen Windows-Versionen 2000 und XP gilt es zwischen drei Aspekten zu trennen: Den Möglichkeiten des Betriebssystems, den Fähigkeiten und der Userverwaltung einzelner Applikationen sowie dem typischen Verhalten eines Windows-Benutzers.

Mit Windows 2000 und XP hat Microsoft die eigene Produktlinie vereinheitlicht und das Prinzip der Multi-User-Betriebssysteme auch auf den heimischen Computer gebracht. Von Haus aus verfügt Windows also über die meisten Vorteile dieser Systeme und die damit einhergehende erhöhte Sicherheit. Um zu erläutern, an welchen Stellen es Windows noch fehlt, müssten wir einen ausgiebigen Exkurs in die Themen System-Accounts und erweitertes Rechtemanagement machen.

Daher wollen wir den ersten Aspekt beiseite lassen und stattdessen einen kurzen Blick auf die Applikationen und das typische Userverhalten werfen. Als einzige Anmerkung zu den Defiziten von Windows (besonders XP Home Edition) sei erwähnt, dass bei der Standardinstallation die zu Beginn eingerichteten Benutzerkonten Administratorrechte erhalten. Genau das führt das Prinzip der Multibenutzersysteme aber ad absurdum, wie wir später sehen werden.

Mit dem Schritt zum echten Multi-User-System hat sich Microsoft deutlich zu viel Zeit gelassen. Zwar existierte mit Windows NT bereits seit den 90ern ein Mehrbenutzersystem, es war jedoch bezüglich seiner Multimedia-Fähigkeiten stark beschränkt. Zudem wurde wenig Wert auf die Kompatibilität mit moderner Hardware gelegt und stattdessen ein stabiles, aber sehr konservatives System für Unternehmen angestrebt. Für den privaten Endbenutzer wurde die Linie Windows 95, 98 und ME entwickelt. Bei diesen Systemen lag der Focus auf Computerspielen, Multimedia und der Fähigkeit, mit möglichst viel verschiedener Hardware zusammenzuarbeiten. Leider hatte Microsoft die Entwicklung (oder die eigenen Fähigkeiten, diese zu lenken) falsch eingeschätzt und konzipierte diese Versionen als reine Einzelbenutzersysteme. Mit Windows 2000 wollte man beide Produktlinien zusammenführen und damit auch auf die Situation reagieren, dass der private PC auf gleiche Weise von mehreren Benutzern geteilt wird wie der Computer in Unternehmen. Letztendlich fehlte Microsoft aber der Mut, und man brachte mit Windows 2000 zwar ein voll multimediafähiges System auf den Markt, entschloss sich aber, mit Windows ME noch eine weitere Einzelbenutzerversion für den privaten Bereich nachzuschieben. Da diese aber sehr fehlerbehaftet war (ähnlich wie Jahre zuvor die erste Version von Windows 98, der daher kurze Zeit später 98SE folgte), wechselten zahlreiche Nutzer auf Windows 2000. Mit Windows XP Home und Professional gibt es inzwischen aber nur noch eine gemeinsame Multi-User-Produktlinie. Aufgrund zahlrei-

cher Defizite der Home Edition ist es ratsam, die Preofessional Edition auch für den privaten Gebrauch zu nutzen.

Durch diese verschleppte und – nicht zuletzt wegen Windows ME – teils verunglückte Entwicklung hatte man aber vergessen, die Entwickler und Benutzer auf die Reise zum neuen Systemparadigma mitzunehmen. Der Wechel vom Einzelplatz- zum Mehrbenutzersystem bringt nämlich, wie Sie in diesem und allen folgenden Kapiteln immer wieder sehen können, viel mehr Veränderungen mit sich als erhöhten Komfort beim Gebrauch durch mehrere Nutzer.

Noch Jahre nach der Einführung von Windows 2000 und sogar XP entwickelten Hersteller Software, die offensichtlich noch nicht in der neuen Welt angekommen war. Stellvertretend für dieses Problem wollen wir uns Computerspiele ansehen; die Situation lässt sich jedoch auf viele andere Applikationstypen übertragen. Der eigentliche Sinn von Mehrbenutzersystemen ist es, die Daten einzelner Benutzer voneinander zu separieren. Ein Benutzer soll also keinen Zugriff auf private Daten (wie etwa Spielstände oder E-Mails) eines anderen Benutzers haben. Alle privaten Einstellungen und Daten sollen sich daher in den jeweiligen Home-Verzeichnissen (unter Windows liegen diese in *C:\Dokumente und Einstellungen*) der entsprechenden Nutzer befinden. Diese Verzeichnisse bilden quasi die Profile (Accounts) jedes einzelnen Users ab und sind daher eine Art Zuhause für dessen Daten. Viele Spiele fragten den Benutzer bei der Installation jedoch gar nicht erst, ob nur er Zugiff auf das Spiel haben wollte oder ob es auch für alle anderen Nutzer verfügbar sein sollte. Zudem kopierten sie alle zentralen Einstellungen und Spielstände in den Programmordner. Somit konnte jeder nicht nur das Spiel starten und die Spielstände der anderen benutzen oder überschreiben, sondern auch die Konfiguration, wie etwa die Tastaturbelegung, ändern. Anschließend war diese für alle nachfolgenden Spieler gültig, unabhängig davon, ob sie ein anders Benutzerkonto hatten.

Im Fall von Computerspielen mag dies unerheblich sein, bei E-Mails und Banking-Applikationen ist es das aber nicht. Eine Software sollte den Benutzer während der Installation fragen, ob sie nur für ihn zugänglich sein sollte, und selbst für den Fall, dass die Applikation für alle Benutzer zugänglich ist, für jeden Anwender einzelne (nur für diesen lesbare) Profildaten anlegen. So wäre es ohne Weiteres möglich, dass jeder Nutzer des Computers das gleiche Banking-Tool benutzt und dennoch nichts von den Einstellungen und Kontendaten der anderen zu Gesicht bekommt.

Inzwischen legen jedoch die meisten Programme anwenderspezifische Daten in die entsprechenden Home-Verzeichnisse. Die Nachfrage, ob das Programm anderen überhaupt zur Verfügung stehen soll, unterbleibt hingegen in vielen Fällen.[7]

7 Bei Computerspielen wäre dies zum Beispiel für Spiele sinnvoll, die einer bestimmten Altersbeschränkung unterliegen und daher nicht von allen Familienmitgliedern gespielt werden sollen bzw. dürfen.

Dennoch gibt es immer wieder Negativbeispiele wie etwa Kamerasoftware, die heruntergeladene Bilder in den eigenen Programmordner und nicht den Ordner *Eigene Bilder* des entsprechenden Nutzers legt.

Die Schuld liegt hier jedoch nur zum Teil bei den Herstellern: Über Jahre hinweg hat Microsoft ein solches Verhalten forciert, und es dauert eben seine Zeit, bis das Umdenken auch bei Spieleentwicklern, für die Mehrbenutzersysteme immer ein Fremdwort waren, angekommen ist.

Gleiches gilt, in deutlich verschärftem Maß, für die Anwender. Die meisten Leser dieses Buchs werden nicht erst seit Windows XP, sondern schon seit einigen Jahren mit dem Computer arbeiten. Wenn es aber über Jahre hinweg nie einen Grund gab, sich mit verschiedenen Benutzerkonten und Zugriffsrechten zu befassen, fällt der große Paradigmenwechsel im alltäglichen Umgang mit dem System wahrscheinlich nicht einmal besonders auf. Entgegen anders lautenden Behauptungen arbeitet die große Mehrheit mit dem Konto, das bei der Installtion definiert wurde, und somit meist mit Administratorrechten. Noch dazu nutzen viele Familien und Lebensgemeinschaften die Möglichkeit, mehrere Konten zu führen, überhaupt nicht. Es ist also keineswegs so, dass es überall für jedes Familienmitglied einen eigenen Benutzer-Account gibt. Dies wird (teils zurecht) als zu umständlich empfunden. In der überwiegenden Zahl der Fälle gibt es einen einzigen gemeinsamen Zugang, den jeder benutzt.

Der Grund dafür liegt aber nicht nur darin, dass die Idee hinter den neuen Betriebsystemen und den damit verbundenen Vorteilen (und davon gibt es auch neben der reinen Sicherheit viele) nicht vermittelt wurde, sondern dass es an der praktischen Umsetzung hapert. Eine gezielte Informationskampagne von Microsoft hätte hier viel bewirken können, letztendlich muss das Umdenken jedoch bei allen Teilnehmern stattfinden.

Stellen Sie sich einmal vor, dass Sie mit Ihrem Partner oder Ihrer Partnerin in den Urlaub fahren und dort Fotos mit der Digitalkamera machen. Der Hersteller der beigefügten Software hat seine Hausaufgaben erledigt und nach Ihrem Urlaub wandern die Bilder von der Kamera direkt in Ihr persönliches Album im richtigen Home-Verzeichnis. Nur: Welches Home-Verzeichnis ist das »richtige«? Wenn Sie das Prinzip der Multi-User-Systeme wirklich ernst nehmen und getrennte Benutzerkonten führen, wird nur einer von Ihnen Zugriff auf die gemeinsamen Bilder haben. Natürlich könnten Sie sich nach dem Herunterladen der Bilder ausloggen, den zweiten Account wählen und die Bilder auch dorthin übertragen. Viel schöner, zeit- und festplattenplatzsparender wäre es jedoch, wenn man die Bilder so ablegen könnte, dass Sie für beide Benutzer zugänglich sind. Windows bietet, genau wie jedes Multi-User-System mit Gruppen, das dafür nötige Werkzeug. So wäre es beispielsweise denkbar, dass Sie für bestimmte Teile Ihres Home-Verzeichnisses Leserechte für die Gruppe »Familie« definieren. Jeder Benutzer, der Mitglied dieser Gruppe ist, könnte die Fotos ansehen (aber nicht löschen). Es könnte genauso gut auch ein zentrales

Bilderverzeichnis geben, in dem für jedes Urlaubsalbum eigene Zugriffsrechte gesetzt werden können.

Das Setzen von detaillierten Zugriffsrechten, z.B. nur Lesen (Ansehen), Lesen und Schreiben usw., ist in Windows nicht weiter schwierig; es ist den allermeisten Nutzern jedoch schlichtweg unbekannt, und die Entwickler geben sich nicht unbedingt Mühe, diese Situation zu ändern. Darum bleibt dem Einsteiger in die Windows-Welt oft nur die pragmatische Lösung, sich einen Account zu teilen.[8]

Nutzt man ein gemeinsames Konto, bedeutet ein Virenbefall jedoch nicht nur für die eigenen Daten eine Gefahr, sondern ist zugleich auch für alle anderen Benutzer problematisch. Arbeitet man mit Administratorrechten, kann ein Virus sogar Systemdateien löschen. Zahlreiche Trojaner können beim Fehlen der entsprechenden Rechte nicht einmal auf ihrem PC Fuß fassen.

Sowohl aus Gründen der Privatsphäre als auch aus Sicherheitsüberlegungen heraus sollten Sie mehrere Accounts anlegen und diese nicht mit Administratorrechten ausstatten. Weitere Überlegungen und eine Schritt-für-Schritt-Anleitung finden Sie in Kapitel 13, *Erste Hilfe*.

Wireless LAN

Zunehmend ersetzt der Funk das Kabel, und so wundert es nicht, dass drahtlose Netzwerke (Wireless-LANs oder WLANs) und miteinander interagierende Funkkomponenten (Bluetooth) einen wahren Boom erleben. So kann man mit letztgenannter Technologie beispielsweise das eigene Handy blitzschnell an einen drahtlosen Kopfhörer koppeln oder über Funk einen Drucker im Nebenraum dazu bewegen, die eben mit der integrierten Handykamera geschossenen Bilder auf Papier zu bannen. Vor allem aber lassen sich E-Mails und Geschäftskontakte drahtlos und daher besonders bequem zwischen Notebook und Personal Digital Assistant (PDA) abgleichen.

Während man im Fall von Bluetooth nur darauf achten muss, die Kontrolle über diese Verbindungen nicht zu verlieren, da die eigenen Daten sonst versehentlich am Flughafen einem Datendieb zugefunkt werden könnten,[9] ist die Lage beim drahtlosen Netz etwas komplizierter. Das Problem bei einem WLAN liegt darin, dass die Reichweite durchaus ausreicht, um ungebetene Gäste anzulocken. Mittlerweile hat sich sogar eine ganze Szene um das so genannte *Wardriving* etabliert. Dabei fahren

8 Ebenso ist das Wissen nicht weit verbreitet, dass man bei Windows XP mittels der Tastenkombination Windows-Taste+L blitzschnell von Benutzer zu Benutzer wechseln und somit auch praktisch mit Multi-User-Systemen arbeiten kann. Dazu ist es, im Gegensatz zum Ab- und wieder Anmelden, nicht einmal nötig, die laufenden Programme zu schließen.

9 Dazu ist es wichtig, die Einstellungen so restriktiv zu setzen, dass das Handy oder der PDA vor jedem Verbindungsaufbau nachfragen muss, ob die Verbindung auch erwünscht ist. Am besten ist es, Bluetooth gleich ganz zu deaktivieren und nur bei Bedarf einzuschalten. Viele Handys bieten genau dafür Shortcuts an oder aktivieren Bluetooth auf Wunsch nur für einige Minuten.

Cracker mit dem Auto ganze Straßenzüge ab auf der Suche nach ungesicherten drahtlosen Netzwerken und kennzeichnen diese oft mit Kreidezeichen an den Häuserwänden für eventuelle Nachfolger. Diese können anschließend umsonst über Ihre Leitung surfen, im schlimmsten Fall aber genauso gut Daten ausspionieren oder Passwörter mitlesen. Daher sollte ein WLAN niemals unverschlüsselt betrieben werden.

Grob gesagt unterscheidet man zwischen der alten WEP- und der neuen WPA- (bzw. WPA2-)Verschlüsselung. Beide Verschlüsselungsverfahren sorgen dafür, dass die Kommunikation zwischen den WLAN-Komponenten und dem Access Point (dem drahtlosen Zugangspunkt ins Netzwerk) nicht mitgelesen werden kann, denn ohne den passenden Schlüssel lassen sich keine sinnvollen Informationen abfangen. Im Fall von WEP lässt sich der Schlüssel jedoch mittels geschickter Verfahren aus dem Datenstrom herausrechnen und somit der Schutz aushebeln. Diese Möglichkeit ist nicht neu, wurde aber von den meisten WLAN-Herstellern zu lange als rein theoretisches Szenario eingeschätzt. Seit April 2005 hat sich dies jedoch schlagartig geändert: Neue, verbesserte Verfahren erlauben es inzwischen, innerhalb weniger Minuten mit Hilfe von Werkzeugen wie *airsnort* oder *aircrack* WEP-verschlüsselte Netzwerke zu knacken. Im Gegensatz zu früheren Techniken ist es dazu nicht einmal mehr nötig, große Datenmengen mitzuhören; die Angriffe funktionieren sogar dann, wenn keine Kommunikation im Netzwerk stattfindet. Da der Großteil der WLAN-Access Points oder -Router rund um die Uhr läuft, kann der Angreifer problemlos in den Besitz des Schüssels gelangen und anschließend unbemerkt ins Netzwerk gelangen – mit allen Konsequenzen, die dies nach sich ziehen kann.

Der einzige sichere Schutz vor Angriffen dieser Art ist der Einsatz der neuen Verschlüsselungstechnik WPA in Verbindung mit einer langen und nicht trivialen Passphrase. Die Konfiguration ist in den meisten Fällen spielend einfach und dauert nicht einmal fünf Minuten. Dazu ist es jedoch nötig, dass sowohl der WLAN-Router als auch die WLAN-Karte oder der Stick im PC den neuen Standard unterstützen. Dies sollte eigentlich bei allen seit Ende 2004 gekauften Geräten der Fall sein, allerdings ist dies, wie wir im nächsten Abschnitt sehen werden, nicht immer der Fall. Empfehlenswert wäre zudem sicherzustellen, dass auf dem System das zweite Service Pack von Windows XP installiert ist.

Als die Hersteller erkannten, dass die WEP-Verschlüsselung nicht mehr sicher war, nahmen die meisten ihre Produkte nicht etwa vom Markt, sondern versuchten, ihre Bestände noch schnell abzusetzen. Als Folge gab es im Frühsommer 2005 eine wahre Flut günstiger WLAN-Produkte. Besonders kritisch sind hier die Bundle-Angebote zu bewerten: Dabei handelt es sich um die Kombination aus Gerät und Anschluss, bei der der DSL-Provider dem Kunden zu einem kleinen Aufpreis den WLAN-Router zum DSL-Vertrag dazugibt. Diese Gelegenheit wollten sich viele Nutzer natürlich nicht entgehen lassen und kauften somit Geräte, für die mit einer »sicheren Verschlüsselung« in Form von WEP geworben wurde, lange nachdem der Standard sich als unsicher erwiesen hatte.

Zudem liefern viele Hersteller ihre Geräte immer noch mit WEP als Standardverschlüsselung aus, selbst wenn diese bereits WPA unterstützen. Der ahnungslose Kunde sieht keinen Grund, von der vom Router empfohlenen Verschlüsselungsart auf eine andere zu wechseln, und begibt sich somit in Gefahr. Vereinzelt gibt es sogar noch Geräte, die den Kunden bei der Konfiguration nicht auffordern, überhaupt Verschlüsselung einzusetzen. Dies ist insbesondere deswegen so gefährlich, da es kaum festzustellen ist, ob gerade eine unerwünschte Person mit im Funknetz hängt oder nicht.

Wenn Sie WLAN einsetzen, sollten Sie daher unbedingt prüfen, ob WPA oder WPA2 als Verschlüsselungsverfahren eingesetzt wird. Im besten Fall brauchen Sie dazu lediglich die Konfiguration Ihres Routers und Ihres PCs von WEP auf den neuen Standard umzustellen. Bieten die Komponenten kein WPA an, gibt es immer noch die Möglichkeit, eine neue Firmware bzw. neue Treiber von der Webseite des Herstellers herunterzuladen. In vielen Fällen kann man seine älteren Geräte so noch auf den neuesten Stand der Technik bringen. Gibt es ein solches Angebot jedoch nicht, sollten Sie dringend in Erwägung ziehen, entweder auf Wireless LAN zu verzichten oder zeitgemäße Komponenten zu kaufen. Die Gefahr, Opfer eines Angriffs zu werden, ist nicht zu unterschätzen.

Umgang mit wichtigen Daten

Wenn Ihr Computer an das Internet angeschlossen ist, erhöht sich die Gefahr eines Befalls durch Würmer und Trojaner erheblich. Es ist daher wichtig, einige Maßnahmen für den Schutz der eigenen Daten zu treffen. Den selbstverständlich nötigen Virenscanner wollen wir hier außen vor lassen und uns mit dem Sichern und Löschen privater Inhalte sowie mit dem Spiegeln des gesamten Systems befassen. Informationen rund um das Thema Virenscanner finden Sie in Kapitel 10, *Viren, Würmer und Trojaner*.

Backups und Spiegelungen

Neben einem aktuellen Virusscanner und einer Personal Firewall gehört zu jedem gut ausgestatteten Computer auch ein Backup-Gerät und die dazugehörige Software. Neben der Gefahr durch Viren (die man sich auch ohne Internetzugang per Diskette oder CD einfangen kann), Trojaner, Cracker und sonstige Eindringlinge sollte man sich bewusst sein, dass auch Festplatten einmal den Geist aufgeben können und alle Ihre Daten damit verloren gehen. Besonders Ihre privaten Dateien (etwa Bilder oder Office-Dokumente) und E-Mails sollten regelmäßig auf ein geschütztes Medium kopiert werden. Dazu eignen sich externe USB-Festplatten, USB-Sticks oder CDs und DVDs besonders gut.

Externe Festplatten gibt es in verschiedenen Größen und Formen, manche haben die Größe einer Zigarettenschachtel, während andere eher das Format einer Videokassette haben. Die richtige Wahl hängt hier nur von den persönlichen Vorlieben ab und inwieweit Sie die Festplatte regelmäßig transportieren möchten. Kleine Gehäuse sind komfortabler, jedoch auch deutlich teurer, und die darin enthaltenen Festplatten teils weniger leistungsfähig (etwa um weniger Abwärme zu erzeugen).

Entscheidender als das Design sind die Kapazität des Datenträgers und die Anbindung an Ihren Computer. Dabei gilt als Faustregel, dass die externe Festplatte mindestens halb so groß sein sollte wie der interne Datenträger. Natürlich wäre es ideal, wenn die Sicherungsplatte genauso groß oder gar größer wäre, in den meisten Fällen ist dies jedoch nicht zwingend erforderlich und bei großen Kapazitäten zudem kostspielig. Den Großteil des Speicherplatzes verbrauchen nämlich nicht Ihre eigentlichen Daten, sondern die installierten Programme wie das Betriebssystem, das Office-Paket, Grafikprogramme und vor allem Computerspiele. Diese brauchen Sie (von Konfigurationsdateien und Spielständen abgesehen) jedoch nicht zu sichern, da Sie die Datenträger im Original zu Hause haben. Eine Kapazität ab 60 GByte reicht für den Heimgebrauch selbst dann noch völlig aus, wenn Sie viele tausend Musikdateien und Fotos sichern möchten. Viel interessanter ist daher die Anbindung an Ihren Computer; dabei sollten Sie unbedingt auf einen USB2-Anschluss anstelle einer veralteten und deutlich langsameren USB1-Verbindung achten. Dies gilt selbst dann, wenn Ihr Computer über keine USB-2-Schnittstelle verfügt, da der neue Standard abwärtskompatibel ist und die externe Festplatte wahrscheinlich Ihren aktuellen Computer überdauern wird. Anstatt einer Fertiglösung empfiehlt es sich, das Gehäuse und die Festplatte separat zu kaufen. Ein stabiles, leise gekühltes Gehäuse mit einem An/Aus-Schalter überlebt nicht nur manch einen Sturz, sondern schont auch deutlich Ihre Nerven, im Gegensatz zu einem Gerät mit einem deutlichen Summen im Hintergrund. Sollte Ihnen der Datenträger einmal zu klein werden, stellt der Austausch gegen eine größere Festplatte kein Problem dar. Von Produkten, die ihren Energiebedarf nicht durch ein externes Netzteil, sondern direkt über den USB-Anschluss beziehen, ist abzuraten, falls es der erhöhten Mobilität wegen nicht zwingend notwendig ist. Wenn Sie mehrere USB-Geräte betreiben, kann es ansonsten zu Engpässen und kurzfristigen Ausfällen kommen. Der Preis für externe Festplatten liegt, je nach Art und Ausstattung, zwischen 80 und 200 Euro. Externe Festplatten gelten als sehr sicher und verfügen meist über eine relativ lange Lebenszeit. Besonders bequem sind Lösungen mit integrierter Backup-Funkion. Per Druck auf einen Knopf am Gehäuse startet automatisch das Sicherungsprogramm, das meist auch über eine Zeitplanungsfunktion verfügt.

CD/DVD-Brenner sind erheblich günstiger und vielseitiger als eine externe Festplatte, verfügen jedoch über deutlich weniger Speicherplatz. Je nach Brenner und verwendetem Medium (CD oder DVD) finden einige hundert oder tausend MByte Platz auf dem Datenträger. Zwar besteht inzwischen die Möglichkeit, die Laufwerke genauso wie eine Festplatte zu benutzen und somit Dokumente ad hoc sichern zu

können, in der Regel wird man sich jedoch eines Brennprogramms bedienen und die CD oder DVD dort zusammenstellen und brennen. Auch wieder beschreibbare Medien bringen weniger Komfort, als man vielleicht erwarten könnte. Darunter leidet meist auch die Regelmäßigkeit, in der die Daten gesichert werden. Zudem müsste man für Komplettsicherungen jeweils mehrere Datenträger und deutlich mehr Zeit opfern. Der Vorteil eines CD- oder DVD-Brenners liegt darin, dass das entsprechende Medium von jedem Computer, teils auch von externen Geräten wie etwa DVD-Playern, gelesen werden kann. Gespeicherte Bilder lassen sich so etwa auf dem Fernseher anschauen. Zudem verfügt jeder moderne PC von Haus aus über einen Brenner. Achten Sie beim Kauf darauf, möglichst ein Komplettpaket inklusive der nötigen Software zu kaufen. Als besonders empfehlenswert haben sich die Programme *Nero Burning Rom* und *WinOnCD* erwiesen. Als kostenlose und annährend gleichwertige Alternative kann man sich DeepBurner (*http://www.deepburner.com*) aus dem Internet herunterladen. Die Haltbarkeit einer CD bzw. DVD beträgt mindestens einige Jahre, jedoch sind die Medien teils kratzempfindlich, wodurch es zu Datenverlust kommen kann. Der Preis für einen DVD-Brenner liegt bei etwa 50 bis 100 Euro.

Für Firmenbereiche, in denen größere Datenmengen anfallen und die Ausfallsicherheit im Vordergrund steht, eignen sich beide Lösungen nur bedingt. In diesem Fall sollten Sie auf so genannte *Streamer* zurückgreifen. Diese Laufwerke sichern je nach Modell zwischen einige dutzend oder gar tausend GByte in kürzester Zeit auf speziellen Sicherungsbändern.[10] Die Kosten für ein günstiges Modell liegen hier allerdings zwischen 300 und 1.000 Euro. Zudem ist ein direkter Zugriff auf einzelne Dateien oftmals nicht oder nur umständlich möglich, da Bänder nur sequentiell ausgelesen werden können und der Streamer außerdem die Daten in der Regel komprimiert zu Archiven zusammenfasst.

Unabhängig von der eingesetzten Hardware sollten Sie natürlich auch über die entsprechende, auf Ihre Ausstattung zugeschnittene Backup-Software verfügen. Dazu können sich sowohl die mitgelieferte Software als auch Programme von Drittanbietern eignen. Für den Home-Office-Bereich liegen die Kosten hier meist unter 50 Euro, für den Unternehmenseinsatz sollten Sie mit einem Vielfachen davon rechnen. Mit einem Brenner oder externen Laufwerk können Sie, unabhängig von der Kapazität, jedoch nicht Ihr ganzes Betriebssystem sichern. Besonders wenn Sie neben der üblichen Standardsoftware, wie zum Beispiel dem Office-Paket, noch zahlreiche andere Programme auf Ihrem Computer installiert haben, ist eine eventuelle Neuinstallation des Betriebssystems enorm zeitaufwändig und mühevoll.

Aus diesem Grund gibt es spezielle Software, die eine Partition Ihrer Festplatte spiegeln kann. Diese Spiegelung kann entweder auf eine CD, eine DVD oder auf eine

10 Wobei die »kürzeste Zeit« natürlich von der Datenmenge abhängig ist und daher auch mehrere Stunden betragen kann.

andere Partition der Festplatte erfolgen. In jedem Fall wird dabei der Ist-Zustand aller enthaltenen Daten eingefroren und in einem komprimierten Archiv gespeichert. Bei Bedarf können Sie dann innerhalb weniger Minuten das komplette System restaurieren. Als empfehlenswert hat sich das Programm *Ghost* der Firma Symantec erwiesen.

Wie auch immer Sie Ihre Daten und Programme sichern, wichtig ist vor allem, dass es regelmäßig geschieht. Nichts ist ärgerlicher, als im Notfall nur ein Backup aus dem letzten Jahr zur Hand zu haben. Sollten Sie Ihr System nicht regelmäßig spiegeln, müssen Sie zudem daran denken, nach der Neuinstallation des Systems auch Ihre Programm- und System-Updates aus dem Internet wieder einzuspielen. Während es beispielsweise bei Bildern und Musikstücken ausreicht, eine einmalige Sicherung anzulegen, müssen die Ordner mit den eigenen Profileinstellungen und E-Mail-Konten wöchentlich oder sogar täglich gesichert werden.

Sichere Aufbewahrung persönlicher Daten

Im Hinblick auf einen Cracker-Angriff (beispielsweise mit Hilfe eines Trojanischen Pferds) oder bei mehreren Benutzern, die sich einen Computer teilen, stellt sich natürlich die Frage, wo und wie man seine Daten sicher aufbewahren kann. Die Windows-Bordmittel reichen nicht aus, um die Sicherheit Ihrer privaten Inhalte nachhaltig zu gewährleisten. Einem unprofessionellen oder sehr hastig agierenden Eindringling können diese Maßnahmen das Leben aber ausreichend schwer machen. Wie bereits erwähnt, kommt es beim effektiven Schutz nicht darauf an, einen Angriff unmöglich zu machen, sondern vielmehr darauf, kein bequemes Ziel zu sein. Viel häufiger als professionelle Cracker sind ohnehin verärgerte Arbeitskollegen oder Bekannte am Werk. Diese Personen arbeiten nicht mit spezieller Software, sondern werden versuchen, während Ihrer Kaffeepause schnell und unbemerkt Schaden anzurichten.

Wie bereits erläutert, ist es in den modernen Windows-Versionen möglich, einzelne Dateien oder ganze Verzeichnisse durch Verschlüsselung zu schützen. Prinzipiell ist es deutlich sinnvoller, ganze Ordner zu verschlüsseln, da man anschließend nicht bei jeder neu angelegten Datei die Verschlüsselung wieder einschalten muss. Alle Dateien, die sich in dem entsprechenden Ordner befinden, werden so automatisch verschlüsselt. Viele Programme, wie etwa Word, erstellen temporäre Versionen von bearbeiteten Dokumenten. Würden Sie nur das eigentliche Ursprungsdokument verschlüsseln, wären diese Versionen unter Umständen lesbar. Dies ist vor allem dann ein Problem, wenn die temporären Dateien in anderen Ordnern abgelegt werden. Beachten Sie zudem, dass Sie verschlüsselte Datein vor der Weitergabe (z.B. auf CD) wieder entschlüsseln müssen. Zwei wichtige Aspekte gilt es bei dieser Art der Verschlüsselung zu beachten: Zum einen bleiben die Verzeichnisse und Dateien weiterhin für andere Personen sichtbar (wenn auch nicht zugreifbar), zum anderen greift der Schutz nur außerhalb Ihres Benutzerprofils. Wenn Sie sich also vor der

Kaffeepause nicht am System abmelden oder den Desktop sperren (beides über Strg+Alt+Entf), ist der Schutz wirkungslos, denn der lokale Angreifer arbeitet dann unter Ihrem Account. Das Gleiche gilt natürlich auch für Trojaner. Ein Cracker, der Kontrolle über Ihren Account erlangt hat, ist durchaus in der Lage, die Entschlüsselung temporär zu deaktivieren und die Daten auf seinen Computer zu laden.

Um Ordner zu verschlüsseln, müssen Sie diese im Explorer (Windows-Taste+E) markieren und per Rechtsklick den Dialog EIGENSCHAFTEN auswählen (siehe Abbildung 3-3). Im Reiter ALLGEMEIN öffnen Sie anschließend die erweiterte Auswahl und setzen ein Häckchen bei INHALT VERSCHLÜSSELN, UM DATEN ZU SCHÜTZEN.

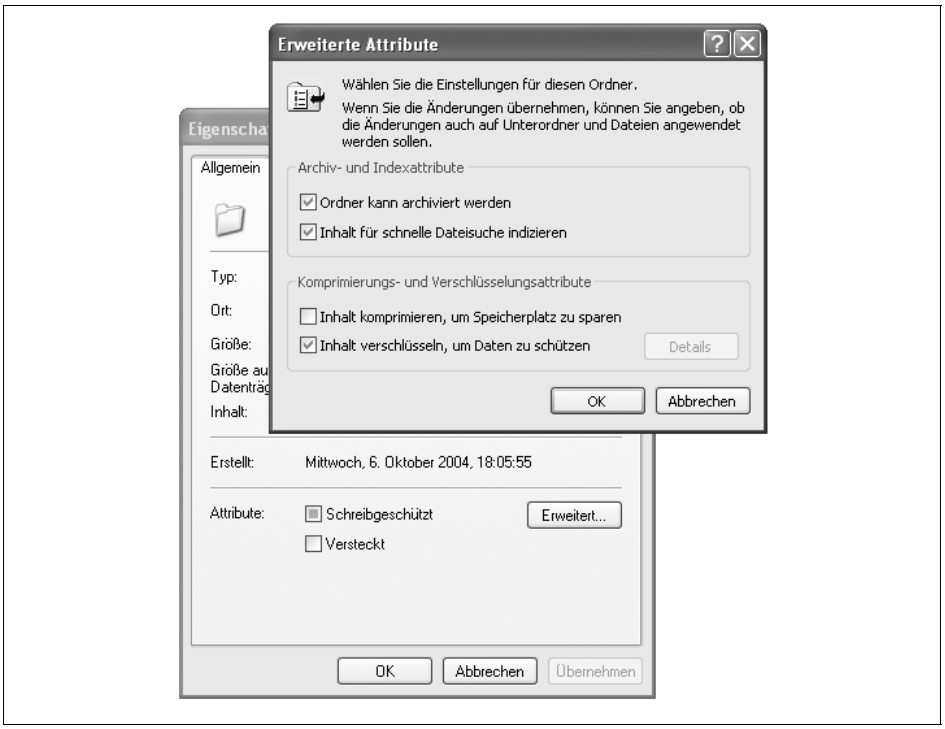

Abbildung 3-3: Ordner verschlüsseln unter Windows XP

Anschließend erscheinen verschlüsselte Ordner und Dateien in anderer Schriftfarbe. Das ist zwar für die Übersichtlichkeit eine gut gemeinte Idee, sollte jedoch im Fall höherer Sicherheitsanforderungen unbedingt deaktiviert werden, da es die Aufmerksamkeit eines lokalen Angreifers unnötigerweise auf die schutzbedürftigen Daten lenkt. Um diese Funktion auszuschalten, müssen Sie im Explorer das Menü EXTRAS und dort die ORDNEROPTIONEN... öffnen. Im Reiter ANSICHT können Sie dann die Funktion VERSCHLÜSSELTE ODER KOMPRIMIERTE NTFS-DATEIEN IN ANDERER FARBE ANZEIGEN deaktivieren.

Bedenken Sie zudem, dass Sie die erreichte Sicherheit wieder aufgeben, wenn Sie die Daten vor der Sicherung auf einem externen Medium wieder entschlüsseln. Jeder, der in den Besitz der Sicherungskopie gelangt, kann so frei auf die Daten zugreifen. Sind die Daten verschlüsselt und somit sicher, können Sie das Sicherungsmedium, z.B. die CD, allerdings nicht einfach in einen anderen Computer einlegen und benutzen. Dies wird vor allem dann zum Problem, wenn Sie Ihr Betriebssystem neu installieren müssen oder einen anderen Account benutzen wollen. Windows legt einen Schlüssel (ein Zertifikat) für Ihre verschlüsselten Dateien an. Dieser Schlüssel ist einmalig. Löschen Sie Ihre Windows-Partition, den entsprechenden Benutzer-Account oder die Schlüsseldatei, sind Ihre Daten für niemanden mehr lesbar. Es gibt einige komplizierte Tricks, einen solchen Schlüssel zu retten, eine Erfolgsgarantie gibt es jedoch nicht. Daher sollten Sie den Schlüssel unbedingt durch Export sichern. Nähere Informationen und Schritt-für-Schritt-Anleitungen dazu finden Sie sowohl in der Windows-Hilfe als auch an zahlreichen Stellen im Internet.

Ein zweiter Schritt hin zu mehr Sicherheit – der sich übrigens hervorragend mit der Verschlüsselung kombinieren lässt – besteht darin, die Dateien auf der Festplatte zu »verstecken«. Dazu markiert man das gewünschte Dokument und drückt die rechte Maustaste. In dem daraufhin erscheinenden Menü wählt man EIGENSCHAFTEN. Anschließend kann man per Häkchen im Bereich ALLGEMEIN die Option VERSTECKT aktivieren. Verlässt man nun das Fenster, ist die gewählte Datei nicht mehr sichtbar. Dieses Verfahren hat natürlich den Vorteil, dass ein Eindringling das Dokument weder sehen noch per Suchfunktion finden kann. Für Sie als rechtmäßigen Benutzer gelten jedoch die gleichen Einschränkungen. Das Arbeiten mit solchen versteckten Dateien erweist sich als unkomfortabel, da man stets den genauen Pfad (Standort) des Dokuments kennen muss. Zudem kann man diesen Schutz ganz einfach umgehen, indem man im Menü EXTRAS → ORDNEROPTIONEN die Registerkarte ANSICHT und dort die Option ALLE DATEIEN UND ORDNER ANZEIGEN wählt, so dass man alle versteckten Dateien dennoch sehen kann. Wie Sie weiter unten lesen werden, kann das Verstecken von Dateien auch von Nachteil sein.

Eine weitere Möglichkeit ist, die Dokumente per Passwort vor unbefugtem Zugriff zu schützen. Das funktioniert jedoch nur mit Office-Dokumenten (und solchen, in denen der Hersteller diese Option explizit vorgesehen hat) und ist zudem nicht besonders sicher.

Entscheidend für die Wahl der Sicherheitsvorkehrungen ist auch die Frage, wie sensibel Ihre Daten sind. Ein privater Brief an einen Freund braucht sicherlich weniger Schutz als die Zugangsdaten zu Ihrem Online-Banking-Account.

Zum Abschluss wollen wir uns noch ein weiteres, plattformunabhängiges und freies Verschlüsselungsprogramm anschauen. *GnuPG*, mit dem wir uns ausführlich in Kapitel 6, *E-Mail – wer liest mit?* beschäftigen werden, ist die freie Version des, mittlerweile nicht mehr kostenlosen, *Pretty Good Privacy* (*PGP*). PGP ist gewissermaßen das Urmodell aller modernen Verschlüsselungs- und Cleaning-Tools mit Schwer-

punkt auf Clientsystemen. Die Software hat eine bewegte und spannende Geschichte hinter sich, die allein ein ganzes Kapitel wert wäre[11] und verkörpert einen Teil des Community-Geistes im Internet. Durch Aufkäufe und Lizenzänderungen hat das Tool jedoch Teile seiner Attraktivität eingebüßt. Daher werden wir uns hier nur auf das freie GnuPG konzentrieren. Es sei jedoch durchaus empfohlen, die (kostenlose) Testversion von Pretty Good Privacy aus dem Netz zu laden und für ein paar Tage unter die Lupe zu nehmen. Nutzer mit hohen Anforderungen an Sicherheit,[12] kommerziellen Support und vor allem Bedienungskomfort sollten die ca. 100 Euro teure Anschaffung durchaus in Betracht ziehen.

GnuPG können Sie unter *http://www.gnupg.org* herunterladen. Die Installation gestaltet sich einfach und bedarf keiner weiteren Erläuterung. Da GnuPG aber ein reines Kommandozeilentool ist, wollen wir zusätzlich eine grafische Oberfläche benutzen, in diesem Fall beispielhaft WinPT (*http://www.winpt.org*).

Nach der Installation der Programme erscheint ein kleines graues Schlüsselsymbol in der Taskleiste. Per Doppelklick gelangen Sie in die Oberfläche von WinPT, mit der Sie alle GnuPG-Befehle bequem nutzen können. Als Erstes gilt es jedoch einen Schlüssel zu generieren. Dazu rufen Sie im Menü KEY den Eintrag ERSTELLE... auf und legen, der Abbildung 3-4 folgend, einen neuen Schlüssel an.

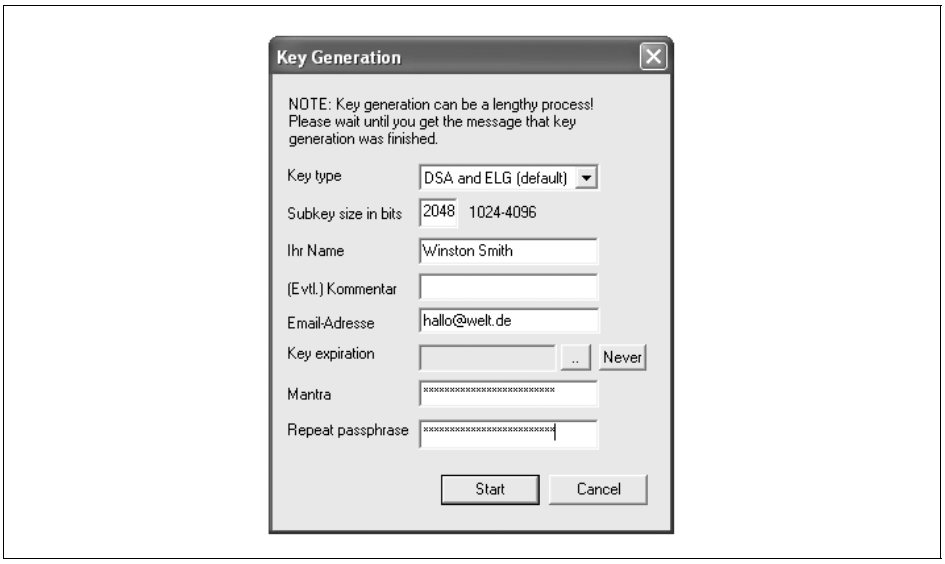

Abbildung 3-4: Der Schlüsseldialog in WinPT

11 Interessant ist unter anderem, wie das Programm nach Europa gelangte. Bei Interesse finden sie im Internet zahlreiche gute Zusammenfassungen rund um die Entwicklung von PGP.

12 Das bedeutet keineswegs, dass GnuPG weniger sicher ist, es ist nur etwas funktionsärmer und weniger komfortabel.

Im Kontextmenü des Windows-Explorers steht Ihnen ab sofort die Möglichkeit zur Verfügung, einzelne Dateien mit dem soeben erstellten Schlüssel zu verschlüsseln oder zu signieren. Dazu wählen Sie den Eintrag WINPT und dort die Option ENCRYPT. Daraufhin wird eine neue, verschüsselte Datei mit der Endung *.gpg* und einem Tresorsymbol angelegt. Die alte, unverschlüsselte Datei bleibt weiterhin erhalten. Sie müssen diese also manuell löschen oder im ENCRYPT-Fenster die Option WIPE ORIGINAL aktivieren. Diese arbeitet manchmal etwas ungründlich, kontrollieren Sie also in jedem Fall, ob die unverschlüsselte Version tatsächlich gelöscht wurde. Mit einem Doppelklick können Sie die verschlüsselten Dateien wieder benutzbar machen, müssen zuvor aber den Schlüssel (in Form der zuvor definierten Passphrase) eingeben. Im Gegensatz zur NTFS-Verschlüsselung von Windows funktioniert die GnuPG-Verschlüsselung auch bei FAT-Partitionen und Windows-Versionen vor Windows 2000. Darüber hinaus ist die Angabe der Passphrase bei jedem Zugriff erforderlich, gleich mit welchem Account Sie angemeldet sind. Daher brauchen Sie sich nicht vor Angreifern oder neugierigen Kollegen zu fürchten, büßen aber ein wenig Komfort ein. Sollte ein Cracker über einen so genannten Keylogger jedoch alle Tastenanschläge mitprotokollieren können, wird er die Passphrase in Erfahrung bringen und nutzen können. Verschlüsselung ersetzt also keinesfalls einen Virenscanner!

Sollten Sie mehrere verschlüsselte Dateien verwalten, eignet sich dazu der File-Manager von WinPT, den Sie über einen Rechtsklick auf das Schlüsselsymbol in der Taskleiste erreichen können.

Weitere Informationen zu Schlüsseln und Verschlüsselungsmechanismen sowie zum Umgang mit GnuPG entnehmen Sie bitte dem Kapitel 6, *E-Mail – wer liest mit?*

Löschen ist nicht gleich Löschen

Neben dem sicheren Aufbewahren Ihrer Daten ist auch das Löschen von Dateien nicht ganz trivial. Viele Programme, wie zum Beispiel der Browser, sammeln entweder Informationen über Ihr Verhalten oder speichern Ihre Daten temporär. Das Thema Browser wird in Kapitel 5, *Browser – einer für alles*, genauer betrachtet und soll deshalb hier nur am Rand erwähnt werden. Wichtig ist für uns erst einmal zu wissen, dass von vielen Dokumenten und anderen Daten im Hintergrund temporäre Abbilder angelegt werden. Nach dem automatischen Löschen dieser Dateien, aber auch wenn Sie etwas (z.B. Office-Dokumente oder Bilder) von Hand löschen, verschwindet die Information nicht wirklich von der Festplatte. Eine vermeintlich gelöschte Datei wird nicht spurlos »ausradiert«, sondern eher »vergessen«.

Wie soll man sich das vorstellen? Sehr vereinfacht erklärt, werden Daten anhand von *Pointern*, sozusagen Ortsangaben, identifiziert. Diese zeigen auf die Position der eigentlichen Datei. Beim Löschen wird nun einfach der Pointer entfernt und nicht die Daten selbst. Wirklich gelöscht werden die Dateien erst, wenn sie mit neuen überschrieben werden. Das Problem besteht nun darin, dass diese vermeintlich gelöschten Daten mit spezieller Software problemlos wiederhergestellt werden können.

Auch hier können uns die oben vorgestellten Programme GnuPG *und* PGP weiterhelfen.[13] Mit Hilfe des File-Managers kann man nämlich nicht nur Daten verschlüsseln und signieren, sondern auch gezielt so löschen, dass eine Wiederherstellung unmöglich wird. Dazu ziehen Sie einfach die gewünschte Datei mit der Maus aus dem Windows-Explorer in den File-Managervon WinPT und wählen dort im Menü FILE den Eintrag WIPE aus. Alternativ erreichen Sie die Funktion auch im Windows-Explorer über das Kontextmenü unter WINPT → WIPE.

Dies funktioniert jedoch nur mit Dateien, die Sie für immer von der Festplatte entfernen wollen. Die bereits angesprochenen äußerst problematischen temporären Dateien bekommen Sie so nicht zu fassen, da es keine Datei gibt, die Sie zum Säubern auswählen könnten. Auch hier hilft ihnen der File-Manager von WinPT mit der Option WIPE FREE SPACE im Menü FILE weiter. Mit ihr werden auch die nur scheinbar leeren Stellen der Festplatte überschrieben und so verhindert, dass Dritte sinnvolle Informationen daraus gewinnen können.

Zahlreiche kommerzielle Privacy-Toolkits bieten diese und zum Teil noch weitere Funktionen und sind bei Bedarf einen detaillierteren Blick wert. Nicht unerwähnt bleiben soll auch das Kommandozeilentool *Cipher* von Microsoft, das seit Windows 2000 zum Standardumfang gehört, aber wegen des fehlenden Komforts eher unbekannt ist. Mittels Cipher können Sie zahlreiche Datenschutzeinstellungen ändern sowie das Verschlüsseln und Löschen per Befehlszeile vornehmen. Eine kurze aber informative Anleitung finden Sie in der Windows-Hilfe (Windows-Taste+F1) unter dem Stichwort »Cipher«.

Allen Tools ist gemeinsam, dass Sie sehr langsam arbeiten und verständlicherweise massiv auf die Festplatte zugreifen müssen. Daher sollte man das Säubern der Festplatte am besten zeitlich mit einem guten Spielfilm abstimmen.

Sicherheitsrelevante Windows-Optionen

Während wir uns in den folgenden Kapiteln mit der Sicherheitsproblematik in Hinblick auf einzelne Dienste – beispielsweise das WWW – und Programmen zum Schutz vor Viren und Einbrechern beschäftigen werden, wollen wir uns in diesem Abschnitt zunächst mit einigen Einstellungen vertraut machen, die uns im Allgemeinen dabei helfen, das Windows-Betriebssystem sicherer zu gestalten. Auch hier gilt es auch hier, einen Kompromiss zwischen Sicherheit und Komfort zu finden, weswegen wir uns nur auf einige wichtige Einstellungen konzentrieren möchten. Im Vergleich zu den stark eingeschränkten Einzelbenutzersystemen wie etwa Windows 98 bieten Windows 2000 und XP eine große Fülle an erweiterten Optionen und

13 Erweiterte Verschlüsselungsmöglichkeiten ganzer Partitionen und Ordner bietet auch die freie und quelloffene Software TrueCrypt 4.0 (*http://www.truecrypt.org*). Auch die Verschlüsselung von USB-Sticks ist möglich, was besonders hilfreich ist, weil Sticks leicht verloren gehen und vertrauliche Informationen auf diese Weise in falsche Hände geraten können.

Hintergrunddiensten. Diese sind zu großen Teilen nützlich, stellen aber auch oft genug Eingriffe in die Privatsphäre oder ernsthafte Sicherheitslücken dar – von aufspringenden Net-Send-Fenstern mit Werbeinhalten[14] bis hin zur unerwünschten Fernsteuerung des Systems durch Dritte.

Die jeweiligen Funktionen dieser Dienste und Einstellungen ausführlich zu erklären, würde den Umfang dieses Kapitels sprengen. Die höhere Komplexität ist der Preis für die Vereinigung eines professionellen Betriebssystems mit einer möglichst einfach zu bedienenden Multimedia-Plattform. Interessierten Lesern sei ein Einblick auf die Seiten *http://dingens.org* und *www.ntsvcfg.de* als Ausgangspunkt ans Herz gelegt.

Versteckte Dateien

Wie im Abschnitt »Sichere Aufbewahrung persönlicher Daten« zu lesen war, können Dateien oder sogar ganze Verzeichnisse versteckt werden, so dass sie für Anwendungen nicht mehr sichtbar sind. In Windows wird diese Option häufig vom System dazu verwendet, interne Daten und Ordner vor dem Benutzer zu tarnen. Microsoft erhofft sich dadurch wohl einen gesteigerten Bedienungskomfort. Der Kunde sieht nur die Inhalte, die für ihn relevant sind, und kann dadurch auch nichts versehentlich löschen oder beschädigen. Angreifer nutzen diese Einstellung jedoch gern aus und verstecken so ihre Trojaner oder illegalen Inhalte. Da die meisten Windows-Benutzer nichts von der Existenz solcher unsichtbaren Dateien wissen, werden die getarnten Programme nicht entdeckt. Es gibt zwar einige Tricks, mit denen man Dateien auf spezielle Art und Weise komplett verschwinden lassen kann, viele Angreifer bedienen sich jedoch des hier beschriebenen *Versteckt*-Attributs von Windows. Neben getarnten Trojanern sind auch zahlreiche Fälle bekannt geworden, in denen Cracker (zu ihrem eigenen Schutz) illegale Inhalte auf den PCs ihrer Opfer ablegten. In besonders drastischen Fällen mussten die ahnungslosen Benutzer viel Zeit, Geld und Energie aufbringen, um die Staatsanwaltschaft davon zu überzeugen (was nicht immer gelang), dass die Daten dort ohne ihr eigenes Wissen gelagert wurden. Aus diesem Grund sollten Sie sich als Benutzer stets alle Dateien vom System anzeigen lassen (siehe oben).

Dateiendungen anzeigen

In der Windows-Welt besteht jede Datei aus einem Namen und einer festgelegten Dateiendung. Diese Endung ist aus historischen Gründen meist drei Zeichen lang und gibt dem System zu verstehen, um welche Art von Daten es sich handelt. Die Endung *.exe* bedeutet beispielsweise *executable* (engl. für »ausführbar«) und zeigt

14 Der Net-Send-Befehl konnte ursprünglich dazu genutzt werden, kurze Nachrichten zwischen den Benutzern eines Netzwerks zu verschicken. Da der Dienst aber aus dem Internet erreichbar war, wurde er massiv für Spam missbraucht.

somit an, dass es sich um ein Programm handelt. Word-Dokumente hingegen haben die Endung *.doc* (*Document*). Jeder Dateiendung ist eine Anwendung zugeordnet, die als Standardprogramm zur Ausgabe des jeweiligen Formats dient. Nur deshalb ist es überhaupt möglich, dass zum Beispiel ein Doppelklick auf eine *.avi*-Datei den Videoplayer öffnet. Aus unverständlichen Gründen unterdrückt Windows allerdings per Voreinstellung die Anzeige von Dateiendungen, die dem System bekannt sind. Dies soll vermutlich den Bedienkomfort steigern, führt aber dazu, dass man nur anhand der Symbole erkennen kann, um welche Art von Dokument es sich handelt. Leider sind diese Symbole nicht immer eindeutig und ändern sich zudem, sobald man ein neues Programm installiert, das für diese Dateien zuständig sein soll.

Die Informationen über den Typ der Datei sind aber gerade deshalb so wichtig, da sie uns abschätzen helfen, ob das Öffnen ein Risiko darstellen könnte. Die wenigsten Nutzer würden eine per E-Mail zugeschickte Datei mit dem Namen *MeinFoto.exe* öffnen, da es offensichtlich ist, dass es sich dabei um ein ausführbares Programm handelt. Wie Sie in Kapitel 10, *Viren, Würmer und Trojaner*, noch lesen werden, können solche Programme Viren oder Trojaner enthalten. Dasselbe gilt für eine Datei mit der Endung *.vbs*. Dies ist die Abkürzung für Microsofts Skriptsprache *Visual Basic Script*, die häufig für E-Mail- und Makro-Viren missbraucht wurde. Neben vielen anderen basierte auch der berühmte *I LOVE YOU*-Virus auf dieser Programmiersprache. Da Windows aber die Anzeige der Dateiendung unterdrückt, weiß der Benutzer nicht, was er gerade öffnet. Anstelle des verräterischen Namens *Bild_von_mir.vbs* ist nur *Bild_von_mir* zu sehen, und der Betroffene wird aller Wahrscheinlichkeit nach auf die Datei klicken, im Glauben, dass es sich um ein Bilddokument handelt.

Die meisten Virenprogrammierer verhalten sich noch geschickter und taufen ihre Dateien wie folgt: Da der Dateiname in Windows nahezu beliebig gewählt werden kann und nur das letzte *.xxx* als Dateiendung gilt, ist es möglich, Dokumente in der Art von *Bild_von_mir.jpg.vbs* zu benennen. Ohne die unterdrückte *.vbs*-Endung lautet der Name der Datei *Bild_von_mir.jpg*. Die vermeintliche Endung *.jpg* steht für ein im Internet sehr verbreitetes Bildformat und bestätigt den Benutzer in der Meinung, dass es sich tatsächlich um ein Foto handelt.

Sie sehen also, dass die Dateiendung wichtig ist und daher immer angezeigt werden sollte. Im Windows-Explorer oder im Arbeitsplatz können Sie die Anzeige der Endungen erzwingen, indem Sie im Menü EXTRAS → ORDNEROPTIONEN... auswählen. In dem dann erscheinenden Dialogfeld wählen Sie die Registerkarte ANSICHT und deaktivieren dort die Option ERWEITERUNG BEI BEKANNTEN DATEITYPEN AUSBLENDEN.

Zuordnungen ändern

Wie erwähnt, verfügt das Betriebssystem über eine Tabelle, in der den verschiedenen Dateitypen die jeweilige Anwendung zugeordnet wird. Aus Sicherheitsgründen macht es durchaus Sinn, bestimmte Zuordnungen zu ändern und damit zu verhindern, dass bestimmte Datein per Doppelklick automatisch gestartet werden. Besonders empfehlenswert ist dies bei den Endungen *.vbe* und *.vbs* (*Visual Basic Script*), *.wsf* (*Windows Script File*) sowie *.jse* und *.js* (*JavaScript*). In der Standardeinstellung von Windows werden diese Dateien direkt ausgeführt und können so, wie am Beispiel des *I LOVE YOU*-Virus deutlich wurde, immensen Schaden anrichten.

Um das zu verhindern, können Sie die Dateitypen beispielsweise an den Texteditor binden, der daraufhin für das gefahrlose Öffnen per Doppelklick zuständig sein wird. Dazu wählen Sie im Windows-Explorer oder im Arbeitsplatz EXTRAS → ORDNEROPTIONEN... aus dem Menü. In dem dann erscheinenden Dialogfeld wechseln Sie auf die Registerkarte DATEITYPEN und gelangen so zur Zuordnungstabelle (siehe Abbildung 3-5). Im Feld REGISTRIERTE DATEITYPEN scrollen Sie bis zu den entsprechenden Dateiendungen (»Erweiterungen«), markieren diese und drücken anschließend auf ÄNDERN.... Nun erscheint ein neues Fenster, in dem Sie unter ANDERE PROGRAMME den Editor wählen und mit OK bestätigen.

Abbildung 3-5: Die Zuordnungstabelle von Windows XP

Alternativ zu dieser Lösung besteht auch die Möglichkeit, den gesamten *Windows Script Host* zu deinstallieren. Das ist inzwischen jedoch nicht mehr auf komfortablem Wege möglich und daher nicht empfehlenswert.

Dokumentleiste löschen

Wir zählen zum Sicherheitsbewusstsein nicht nur den Schutz vor Cracker-Angriffen, sondern auch den der Privatsphäre. Windows legt in der so genannten *Dokumentleiste* einen Verweis auf die von Ihnen zuletzt benutzten Dateien ab. Dabei kann es sich neben Office-Dokumenten auch um Bilder, Videos und vieles mehr handeln. Sie finden diese Shortcuts in der Startleiste unter dem Eintrag ZULETZT VERWENDETE DOKUMENTE. Ein Angreifer – aber auch ein Kollege – kann daraus folgern, an welchen Dokumenten Sie zurzeit arbeiten oder welche Bilder Sie zuletzt betrachtet haben und wo diese sich auf der Festplatte befinden. Darum sollten Sie diese Informationen regelmäßig löschen. Dazu klicken Sie mit der rechten Maustaste auf die Taskleiste und wählen den Eintrag EINSTELLUNGEN. Anschließend wechseln Sie auf die Registerkarte STARTMENÜ und drücken die Schaltfläche ANPASSEN im unteren Teil des Fensters. Im daraufhin erscheinenden Fenster wählen Sie den Reiter ERWEITERT und können dort die Liste löschen oder ganz deaktivieren.[15] Wenn Sie nun in der Startleiste die Dokumentübersicht aufrufen, wird sie nur noch den Eintrag (LEER) enthalten.

Unterschätzen Sie die Wichtigkeit der Informationen nicht, die potenzielle Angreifer aus der Dokumentleiste ziehen können. Als Beispiel soll uns hier wiederum das Tool GnuPG dienen. Wie Sie im Abschnitt »Sichere Aufbewahrung persönlicher Daten« gelesen haben, können Sie Ihre persönlichen Dokumente sicher in *.gpg*-Dateien aufbewahren, dennoch ist es ohne Weiteres möglich, diese Dateien zu kopieren oder gar zu löschen. Daher sollten sie an einem sicheren Ort auf der Festplatte aufbewahrt werden. Öffnet man eine verschlüsselte Datei jedoch per Doppelklick, erscheint daraufhin ein Eintrag in der Dokumentleiste (siehe Abbildung 3-6), und ein Angreifer kann die Datei sofort finden und eventuell zerstören. Löschen Sie die Leiste also unbedingt, nachdem Sie sicherheitskritische Dateien bearbeitet haben!

Netzwerkoptionen

Der Versuch, die nötigen Sicherungseinstellungen in einem Netzwerk zu beschreiben, würde den Rahmen dieses Buches bei Weitem sprengen. Daher wollen wir hier nur einige typische Fehlkonfigurationen in privaten oder sehr kleinen Firmennetzwerken ansprechen.

15 Ob Sie das möchten, hängt natürlich davon ab, ob Sie die Dokumentleiste als sinnvoll erachten und bisher ausgiebig genutzt haben. Sollte das nicht der Fall sein, können Sie die Option komplett deaktivieren und erhöhen damit Ihre eigene Sicherheit.

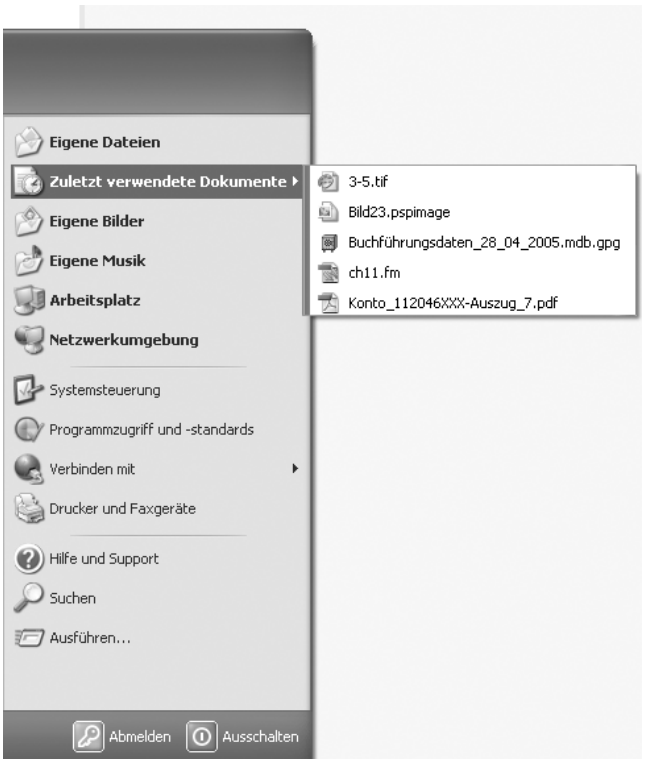

Abbildung 3-6: Eine verschlüsselte .gpg-Datei in der Dokumentleiste

Als Erstes ist es wichtig, in der Netzwerkumgebung alle unnötigen Protokolle zu entfernen, da von ihnen mögliche Angriffe ausgehen könnten. In typischen Windows-Netzwerken können Sie zum Beispiel getrost auf das IPX-Protokoll und inzwischen sogar auf NetBEUI verzichten. Nötig ist meist nur TCP/IP. Zusätzlich sollten Sie die Datei- und Druckerfreigabe nicht auf die leichte Schulter nehmen und nur dann aktivieren, wenn Sie wirklich Dateien oder Drucker freigeben wollen. Mittels der so genannten Windows-Freigabe können Benutzer von Computern, die an ein Netzwerk angeschlossen sind, angeben, welche Ressourcen sie mit anderen Rechnern teilen möchten. Freigegebene Windows-Ordner erkennen Sie daran, dass eine offene blaue Hand am Ordner angezeigt wird. Zwar können Freigaben mittels Passwort geschützt werden, dieser Schutz kann jedoch leicht ausgehebelt werden. Wenn Sie sich dazu entschlossen haben, Daten über das Netzwerk zugänglich zu machen, sollten diese Freigaben dennoch stets mit Passwörtern geschützt sein. Ebenfalls ist darauf zu achten, dass nach Möglichkeit nur Lese- und keine Schreibrechte gesetzt werden. Seien Sie mit der Freigabe nicht zu großzügig, und geben Sie keinesfalls die gesamte Partition oder komplette Systemverzeichnisse frei. Die aktuellen Windows-Versionen geben jede Partition über so genannte »verstecke Freigaben« frei. Diese

dienen nur administrativen Zwecken, stellen unter Umständen aber dennoch eine Gefahr dar. Es ist zwar möglich, diese Freigaben zu deaktiveren, die Einstellung hält jedoch nur bis zum nächsten Neustart. Eine endgültige Lösung ist nur über einen Eingriff in die Registry möglich. Weitere Informationen und eine Schritt-für-Schritt-Anleitung finden Sie beispielweise unter *http://support.microsoft.com/default.aspx?scid=kb;de;314984*.

Bei Fehlkonfigurationen ist es für Angreifer aus dem Internet problemlos möglich, Dateien von Ihrem Computer herunterzuladen oder sogar zu verändern. Diese Gefahr besteht keineswegs nur in der Theorie.

Ebenso unterschätzt werden die Sicherheitsrisiken beim Online-Spielen. Bedenken Sie daher, dass auf einem PC mit sensiblen Daten keine Netzwerk- oder Internetspiele betrieben werden sollten. So war es bei *Quake III*, einem der damals beliebtesten Online-Spiele, bis Mitte 2000 möglich, Daten von den Festplatten der Spieler zu lesen und zu verändern oder sogar Programme auf den Rechnern zu installieren. Die Spieler bemerkten von all dem nichts.

Bewusster Surfen

Nachdem wir uns in den letzten Abschnitten mit der Optimierung von Passwörtern und des Betriebssystems unter Sicherheitsaspekten beschäftigt haben, wenden wir uns nun dem Surfen im Internet zu.

Um sich wirklich sicher im Internet zu bewegen, bedarf es einiger Vorkehrungen. Zunächst sollte man über das nötige Hintergrundwissen verfügen, um mögliche Sicherheitsrisiken bereits im Vorfeld abschätzen zu können. In Kapitel 2, *Technische Hintergründe*, haben Sie dazu die wichtigsten Fakten kennen gelernt. Zweitens müssen natürlich das Betriebssystem und alle Client-Programme wie beispielsweise der Browser so konfiguriert sein, dass keine leicht vermeidbaren Sicherheitslücken entstehen. Damit befassen sich schwerpunktmäßig die Kapitel 5, *Browser – einer für alles*, Kapitel 6, *E-Mail – wer liest mit?*, und Kapitel 8, *Weitere Internetdienste*. Der dritte Aspekt, mit dem wir uns in diesem Abschntt näher beschäftigen wollen, ist das umsichtige Verhalten beim Surfen. Es soll dabei weder um technische Details noch um Einstellungen in Programmen gehen, sondern darum herauszufinden, wo man sicher surfen, einkaufen und downloaden kann. Dem Thema E-Commerce und Online-Banking ist ein eigenes Kapitel gewidmet (Kapitel 8), einige Aspekte werden wir jedoch hier schon aufgreifen.

Vertrauenswürdigkeit prüfen

Bevor man sich dazu entschließt, etwas online zu kaufen, sollte man sich natürlich darüber informieren, wie seriös der Anbieter ist. Dies gilt auch für das Surfen im Allgemeinen. Hat sich beispielsweise eine Website als vertrauenswürdig erwiesen,

kann man speziell für diese die Sicherheitseinstellungen des Browsers lockern und z.B. JavaScript zulassen. Um herauszufinden, ob ein Anbieter seriös ist, gibt es natürlich zahlreiche Möglichkeiten; drei davon haben sich aber als besonders schnell durchführbar und recht treffsicher erwiesen.

Die wahrscheinlich sicherste Möglichkeit nachzuvollziehen, ob ein Anbieter wirklich seriös ist, ist ein Blick in eines der zahlreichen Internetmagazine. Dort werden regelmäßig E-Shops und bekannte Websites auf Ihre Qualität hin untersucht. Mit anonymen Testbestellungen prüfen die Magazine, ob, wann und wie die bestellte Ware beim Kunden ankommt und wie vertraulich der Anbieter mit den Kundendaten umgeht. Auch aus technischer Sicht werden die Seiten gründlich unter die Lupe genommen.

Als zweites sollten Sie versuchen herauszufinden, wer überhaupt hinter einer Website steckt. Dazu kann man sich des Angebots auf *http://www.denic.de* bedienen. Bei DENIC handelt es sich um den deutschen Ableger der weltweiten Vergabestelle für Domainnamen, das Network Information Center (NIC). Unter dem Link WHOIS können Sie Domains prüfen und herausfinden, wer diese beantragt hat und welcher Provider dafür zuständig ist. Dazu geben Sie in das Formularfeld einfach den Domainnamen ein, über den Sie nähere Informationen wünschen. Beachten Sie, dass die DENIC nur zwei Level einer Domain unterscheidet: den gewählten Namen (Second Level) und die Top-Level-Domain. Hosts oder Subdomains dürfen nicht in die DENIC-Maske eingegeben werden. Die Eingabe *oreilly.de* kann also verarbeitet werden, wohingegen *www.oreilly.de* einen Fehler erzeugen wird. DENIC ist nur für *.de*-Domains zuständig. Sollte es sich bei der fraglichen Adresse um eine *.com*-Domain handeln, können Sie Ihr Glück auf der NIC-Seite unter *http://www.nic.com* versuchen.

Wenn Sie das Formular korrekt abgeschickt und die Nutzungsbedingungen akzeptiert haben, erscheint eine Seite mit den wichtigsten Informationen über den Betreiber der Website. Abbildung 3-7 zeigt einen Ausschnitt aus dem Ergebnis einer Datenbankabfrage für »oreilly«.

Den Daten kann man zum Beispiel entnehmen, ob es sich um eine Gesellschaft oder um eine Privatperson handelt. Auch den technischen und administrativen Ansprechpartner kann man hier finden. Diese Daten erlauben bereits einige Rückschlüsse auf die Seriosität des Anbieters.

Inzwischen sind alle kommerziellen Anbieter dazu verpflichtet, auf ihrer Seite ein eigenes Impressum zu führen. Die Informationen überschneiden sich aber nur zum Teil mit denen der DENIC und können sich daher gut ergänzen. Ein fehlendes oder unvollständiges Impressum deutet auf einen nicht seriösen oder laienhaften Anbieter hin.

Ein weiteres Kriterium ist der *Webhoster*, der für die Website verantwortlich ist. Als Webhoster bezeichnet man eine Firma, die Webseiten auf Ihren Servern unterbringt, also Festplattenplatz und Domainnamen im Internet vermietet. Steht der

Domaindaten

Domain:	oreilly.de
Letzte Aktualisierung:	29.06.2005

Domaininhaber

Der Domaininhaber ist der Vertragspartner der DENIC und damit der an der Domain materiell Berechtigte.

Name und Adresse:	O'Reilly Verlag GmbH & Co. KG Balthasarstr. 81 DE-50670 Koeln

Administrativer Ansprechpartner

Der administrative Ansprechpartner (admin-c) ist die vom Domaininhaber benannte natürliche Person, die als sein Bevollmächtigter berechtigt und gegenüber DENIC auch verpflichtet ist, sämtliche die Domain oreilly.de betreffenden Angelegenheiten verbindlich zu entscheiden.

Name:	Elke Hansel
Kontakttyp:	PERSON
Adresse:	O'Reilly Verlag GmbH & Co. KG Balthasarstr. 81
PLZ:	50670
Stadt:	Koeln
Land:	DE

Technischer Ansprechpartner, Zonenverwalter

Abbildung 3-7: Ausschnitt aus der Whois-Datenbankabfrage für oreilly.de

Server samt Standleitung beim Besitzer des Domainnamens selbst, kann man in der Regel davon ausgehen, dass es sich um einen größeren Anbieter handelt. Befindet sich das Angebot hingegen auf dem Server eines Webhosters, lohnt auch ein Blick auf diesen. E-Shops, die bei kostenlosen Hostern liegen, können generell nicht als seriös angesehen werden; dies gilt auch für Seiten, die bei einem so genannten Low-Budget-Hoster liegen. Gerade kostenlose Hoster stellen häufig den Plattenplatz zur Verfügung, ohne persönliche Informationen über den Kunden zu erfragen. Sie können in solchen Fällen also nur schwer oder gar nicht nachvollziehen, wer überhaupt für die Webseite verantwortlich ist.

Ein seriöser Webseiten- oder E-Commerce-Betreiber wird bestrebt sein, eine möglichst große Bandbreite auf einem starken Server zu erhalten, um den Kunden einen schnellen Zugang zu seinem Angebot zu gewährleisten. Er wird auch auf Ausfallsicherheit und die nötige Kompetenz seitens des Webhosters achten. Daher ist Zweifel angebracht, wenn die Website bei einem Low-Budget-Anbieter gehostet wird. Die Informationen über den Seiteninhaber sind leichter zu deuten als die über den Hoster, denn bei Letzterem bedarf es etwas mehr Marktübersicht, um abschätzen zu können, wie dieser einzuordnen ist.

Wichtig ist zudem zu prüfen, in welchem Land sich das Angebot wirklich befindet. Eine *.de*-Domain muss weder in Deutschland liegen noch in deutscher Sprache verfasst sein. Die *.de*-Endung sagt lediglich aus, welche Organisation und damit welcher Top-Level-Nameserver für diese Domain verantwortlich ist. Eine *.de*-Domain

kann also auch einem Unternehmen aus Spanien gehören, das diese in Amerika hosten lässt. So etwas ist keineswegs selten.

Leider ist das Internet- und besonders das Fernverkaufsrecht in den verschiedenen Ländern unterschiedlich. Die in Deutschland gesetzlich festgelegte Rückgabemöglichkeit für jegliche per Telefon, Fax oder Internet bestellte Ware gilt nicht unbedingt in anderen Ländern. Gerade in Osteuropa und Asien sind die gesetzlichen Regelungen noch nicht so ausgereift wie in der EU oder den Vereinigten Staaten. Wenn Sie also beispielsweise über einen Online-Shop, der in Russland gehostet wird, etwas bestellen, können Sie im Notfall nicht mit EU-Gesetzen argumentieren. Selbst die Zuordnung von Anbieter und Hoster ist in einigen Staaten nicht genau geregelt. So kann es durchaus passieren, dass nicht die Gesetze des Landes gelten, in dem der Anbieter ansässig ist, sondern die des Landes, in dem sich der Hoster befindet.

Was passiert zum Beispiel, wenn wegen einer fahrlässigen Sicherheitslücke Ihre Kreditkarteninformationen von einem Server gestohlen werden? Ist nun der Website-Betreiber oder der Webhoster zuständig? In der Regel, wenn überhaupt sinnvoll und möglich, werden Sie natürlich Klage gegen den Betreiber einreichen, der diese dann wahrscheinlich an den Hoster weitergibt. Wie dort aber »Fahrlässigkeit« ausgelegt wird, ist für Sie als Kunde nicht mehr nachzuvollziehen. Generell kann ein Webhoster für Schäden, die durch Sicherheitslücken entstanden sind, nur dann zur Verantwortung gezogen werden, wenn nachgewiesen werden kann, dass es sich um ein grobes Versäumnis seitens des Hosters gehandelt hat.

Natürlich müssen Sie diesen Aufwand nicht vor dem Besuch jeder einzelnen Internetseite auf sich nehmen. Bevor Sie jedoch persönliche Daten oder gar Kreditkarteninformationen auf einer Website hinterlassen, sollten Sie sich über den Anbieter informieren, denn die Anzahl an schwarzen Schafen im Internet nimmt leider drastisch zu. Vor allem, wenn es sich um Zahlungsdaten (insbesondere solche von Kreditkarten) handelt, ist Vorsicht geboten. Vor allem bei den Power-Sellern von eBay sei erhöhte Wachsamkeit angeraten. Man kann dort wirklich ein gutes Schnäppchen machen, die Anbieter können in puncto Zuverlässigkeit und Sicherheit jedoch nicht mit großen Plattformen mithalten. Zudem ist meist völlig undurchsichtig wer sich genau hinter einem Angebot verbirgt, woher die Ware stammt und wie Ihre persönlichen Daten gelagert und verwaltet werden. AGBs fehlen in der Regel ebenso.

Um Ihnen aber nicht den Spaß am Einkaufen im Internet zu nehmen, sei noch gesagt, dass man vor allem bei größeren und bekannteren Anbietern (wie etwa *http://www.libri.de*, *http://www.computeruniverse.net*, *http://www.apple.com/de/itunes/music/* und vielen anderen) bedenkenlos einkaufen kann.

Sichere Download-Quellen

Häufiger als zum Einkaufen wird das Internet dazu benutzt, Dateien herunterzuladen. Dabei kann es sich um Musikstücke (z.B. *mp3*), Videos (*avi*, *mpg* u.a.), Bilder (z.B. *jpg*, *gif*, *tiff*, *png*, *bmp*), Text, Programme oder vieles andere handeln. Sogar ganze Kinofilme kann man sich aus dem Internet herunterladen, oft bereits vor der Premiere in Deutschland.[16]

Wenn Sie Bilder, Musik, Texte oder Ähnliches aus dem Internet laden, gehen Sie in der Regel kein Sicherheitsrisiko ein. Vorsicht ist jedoch angebracht, wenn es sich um Programme handelt. Diese liegen im Internet meist in binärer Form vor, das heißt, der in einer Programmiersprache verfasste Quell-Code wurde bereits in maschinenlesbaren Code aus Einsen und Nullen umgewandelt (*kompiliert*). Sie können also nicht in das Programm »hineinschauen«.[17] Rein theoretisch ist es möglich, den Quell-Code eines Programms vor dem Kompilieren so zu ändern, dass es neben seiner eigentlichen Funktion noch ganz andere Dinge im Hintergrund durchführt. Dazu könnte zum Beispiel das Protokollieren der gedrückten Tasten oder das heimliche Austauschen von Daten mit dem Internet zählen. Der Benutzer merkt von all diesem Geschehen im Hintergrund nichts!

Umso wichtiger ist es, das sensible Daten nicht auf dem Computer zu speichern und damit solchen Programmen Tür und Tor zu öffnen. Viele der berühmten Trojaner, die wir in Kapitel 10, *Viren, Würmer und Trojaner*, genauer betrachten werden, tarnen sich als harmlose Programme. Besonders beliebt sind dabei Bildschirmschoner, die man von einem angeblichen Freund per E-Mail zugeschickt bekommt (siehe Kapitel 6, *E-Mail – wer liest mit?*) oder selbst aus dem Internet herunterlädt. Geeignet für die Unterbringung von Trojanern sind natürlich auch Programme, die zurzeit besonders populär sind. So wurde zum Beispiel per E-Mail eine verseuchte Version des Mittagspausenfüllers Pinguin-Weitschießen in Umlauf gebracht. Da die Programme nicht im Klartext vorliegen, kann der Angreifer davon ausgehen, dass die heimlichen Aktivitäten des Programms nicht entdeckt werden. Natürlich sollte man deswegen nicht gleich auf das Downloaden verzichten oder alle Bildschirm-

16 Vor dem Download ist aber stets zu prüfen, ob dadurch keine Urheberrechte tangiert werden. Das Herunterladen eines Kinofilms ist natürlich strafbar! Genauso verhält es sich mit den Musikstücken, die Sie im Internet finden. Es ist natürlich eine feine Sache, sich den neuesten Titel der Lieblingsband einfach aus dem Internet zu besorgen, doch könnten Sie den Künstlern damit auf Dauer schaden. Selbst wenn man alle moralischen Bedenken ignoriert, sollte man zumindest wissen, dass es sich dabei um keine Bagatelle, sondern um ein ernsthaftes Vergehen handelt. Dies kann je nach Umfang auch mit mehr als nur einer Geldstrafe geahndet werden.

17 Als Linux-/Unix-Benutzer sind Sie auch hier wieder auf der sicheren Seite, denn für diese Systeme werden fast alle Programme auch im Quelltext angeboten. Sie können diesen Code herunterladen und anschließend auf Ihrem Rechner kompilieren. Sollten Sie also die Möglichkeit haben, Quelltext herunterzuladen, ist dieser stets der Vorzug gegenüber bereits kompilierten Dateien zu geben. Ein solches Vorgehen wäre im Prinzip auch für quelltextoffene Software unter Windows möglich, aus verschiedenen Gründen hat sich jedoch nie eine entsprechende Kultur des Selbstkompilierens etablieren können.

schoner von seinem System entfernen. Es gibt auch hier zwei einfache Möglichkeiten, sich vor solch bösen Überraschungen effektiv zu schützen.

Schauen wir uns zuerst an, wo man keinesfalls Programme herunterladen sollte. Im Internet gibt es eine große Anzahl an privaten Homepages, auf denen die Betreiber Programme, Bildschirmschoner oder einfach nützliche Tools zum Download anbieten. Es ist keinesfalls meine Intention, die Betreiber (zum Teil sehr guter und informativer) kostenloser Webseiten in Misskredit zu bringen, aus Sicherheitsgründen sind in solchen Fällen aber immer Zweifel angebracht. Von solchen Quellen sollten Sie daher lieber keine Software herunterladen. Die berühmten DDoS-Angriffe (*Distributed Denial of Service*) auf eBay, CNN und andere große Firmen im Sommer 2000 sind auf genau solche Benutzerfehler zurückzuführen. Damals hatten tausende Internetnutzer Trojaner auf Ihren Systemen installiert oder sie sich per Wurm eingefangen, die dann auf den Befehl des Crackers hin einen DDoS-Angriff auf Unternehmensserver starteten. Die Server brachen dann auf Grund der Last dieses verteilten Angriffs zusammen und waren nicht mehr für gewöhnliche Benutzer erreichbar. Da die Cracker nur dann Kontrolle über ein System erlangen können, wenn der Computer online ist, hält sich die Zahl solcher verteilten Angriffe derzeit noch in Grenzen, sie nimmt aber rapide zu. Beim zunehmenden Trend zu DSL-Flatrate und Standleitung kann man sich aber ausrechnen, dass in naher Zukunft viel mehr Computer für solche Angriffe zur Verfügung stehen werden. Es sind bereits jetzt Angriffe mit mehreren zehntausend Rechnern bekannt geworden.[18]

Der sicherste Ort, um ein Programm aus dem Internet zu laden, ist natürlich die Website bzw. der FTP-Server des Herstellers. Dort muss man sich zwar manchmal registrieren lassen, kann dafür aber auch davon ausgehen, dass die Programme »sauber« sind. Kennt man nur den Namen des Produkts, kann man schnell über eine Suchmaschine den Hersteller samt Internetseite ausfindig machen.

Schwieriger wird es hingegen, wenn man nur eine grobe Ahnung vom gewünschten Produkt hat. Ähnlich wie bei den Suchmaschinen für Webinhalte gibt es auch die Möglichkeit, in speziellen Archiven nach Programmen zu suchen. Man kann auf einer solchen Seite in der Regel die Rubrik, einen Teil des Namens oder der Produktbeschreibung und das gewünschte Betriebssystem angeben und bekommt eine Liste möglicher Programme. Besonders beliebte Archive sind *http://www.download.com* und *http://www.tucows.com* (bzw. *http://www.tucows.de*). Für Open Source-Projekte sei vor allem Sourceforge *(http://sourceforge.net/)* empfohlen. Neben Testversionen bekannter Produkte werden dort auch viele günstige oder sogar kostenlose Programme (*Freeware*) zum Download angeboten. Kurzbeschreibungen und Bewertungen ergänzen das Angebot und helfen Ihnen, schneller ein passendes Produkt zu

18 Die vielen Millionen Internetnutzer Osteuropas und Asiens benutzen derzeit noch hauptsächlich langsame analoge Verbindungen. Man kann davon ausgehen, dass mit steigender Verbreitung von digitalen Verbindungen in diesen Regionen eine Vervielfachung der Zahl schwerer DDoS-Angriffe einhergen wird.

finden. Es hat sich herausgestellt, dass gerade die kleineren, kostenlosen (oder -günstigen) Programme für einen bestimmten Zweck oft besser geeignet sind als die umfangreichen kommerziellen Produkte großer Hersteller. Viele bekanntere Archive testen die angebotenen Programme sogar auf eventuell versteckte Viren oder Trojaner.

Adware und Spyware

Mit dem Begriff *Adware* bezeichnet man die so genannte *Advertising Supported Software*. Dabei handelt es sich um Programme, die durch Werbeeinblendungen finanziert werden. Die Idee dahinter ist, dass ein Produkt, wenn es für den Konsumenten kostenlos sein soll, durch Werbung finanziert werden muss. Beispiele dafür sind zahlreiche Filesharing-Tools mit Werbeeinblendungen in der oberen Programmleiste. Findet man an der Software Gefallen und möchte die Banner nicht mehr sehen, kann man anschließend häufig eine werbelose Version käuflich erwerben. Das Konzept der Adware an sich ist also nichts Negatives, sondern gibt uns ganz im Gegenteil die Möglichkeit, eine Vielzahl zum Teil sehr guter Tools kostenlos zu nutzen.

Etwas anders verhält es sich, wenn von *Spyware* die Rede ist. Im Gegensatz zur Adware werden dabei nicht nur Werbeeinblendungen, sondern auf dem umgekehrten Weg auch zahlreiche persönliche Daten übertragen. Den Namen verdankt die Spyware vor allem der Tatsache, dass dieser Vorgang ohne das Wissen des Benutzers geschieht und somit mit Spionage gleichgesetzt werden kann. Verantwortlich für diesen Verlust an Privatsphäre ist in den meisten Fällen nicht die kostenlose Software an sich, sondern zusätzliche Programme, die beim Installieren des gewünschten Tools einfach mitgeladen werden. Diese unerwünschte Zusatzsoftware nistet sich in Ihrem System ein und sammelt heimlich Informationen über Ihr Surfverhalten. Anschließend übermittelt sie diese Informationen an den Server des Werbepartners. Während eher harmlose Tools »nur« Ihre Online-Zeiten oder Ähnliches mitprotokollieren, existieren auch Versionen, die das gesamte Surfverhalten einschließlich der besuchten Webseiten und bestellten Produkte überwachen und somit die Erstellung sehr detaillierter Benutzerprofile erlauben.

Einige Produkte gehen über das reine Protokollieren hinaus und ändern sogar die Darstellung von Webseiten in Ihrem Browser. Das Programm *KaZaA* der Firma eZula enthielt zum Beispiel ein zusätzliches Programm namens *TopText*, das nach der Installation von nun an alle von Ihnen aufgerufenen Internetseiten nach bestimmten Wörtern aus dem Musikbereich durchsuchte und diese im Browser als gelben Link darstellte. Ein Klick auf diesen Link führte direkt zu einem passenden Online-Shop, der einen Vertrag mit eZula abgeschlossen hatte. Besonders problematisch ist diese Art der Werbung deshalb, weil damit die Originalseite im Browser des Betrachters verändert wird. Der jeweilige Webdesigner oder Betreiber ist aber mit Sicherheit nicht damit einverstanden, dass seine Webseite für Werbezwecke

missbraucht wird. So kann man sich kaum vorstellen, dass der Anbieter eines Musik-Online-Shops sonderlich begeistert davon ist, dass seine Besucher möglicherweise lauter gelbe Links auf seiner Seite vorfinden, die direkt zur Konkurrenz führen. Nähere Informationen über TopText finden Sie auf den Seiten der damals als Gegenreaktion ins Leben gerufenen Aktion *Fighting eZula*, zum Beispiel unter *http://www.whirlywiryweb.com/q/ezula.asp*.

Die Frage, ob Spyware illegal ist, lässt sich nicht eindeutig beantworten, da meist in einer Klausel der Lizenzbedingungen auf die entsprechenden Softwarekomponenten hingewiesen wird. Dennoch ist es höchst fraglich, ob solch ein Hinweis ausreichend ist, denn immerhin weiß der Benutzer nicht, welche Daten aufgezeichnet und übermittelt werden. Detaillierte Informationen zum Thema Spyware finden Sie beispielsweise unter *http://www.virenschutz.info/spyware.html*. Zudem existieren mit Programmen wie etwa *Ad-aware* (*http://www.lavasoftusa.com/*) und *Webroot Spy Sweeper* (*http://www.webroot.com/*) hilfreiche Tools, die Spyware auf Ihrem System ausfindig machen und bei Bedarf entfernen können. Weitere Informationen zu Spyware finden Sie in Kapitel 10, *Viren, Würmer und Trojaner*.

Was nicht auf Ihre Festplatte gehört

Es gibt einige Kategorien von Software, die definitiv nicht auf den heimischen Rechner und erst recht nicht auf einen vernetzten PC im Büro gehören, selbst wenn Sie der Download-Quelle vertrauen und einen Virenscanner benutzen. Dazu zählen in erster Linie alle Arten von Hacker-Tools und Trojanern, die man »einfach mal so« ausprobieren will. Der lieb gemeinte Ratschlag einiger »Sicherheitsexperten«, man solle sich diese Software mal anschauen, um die Risiken besser abschätzen zu können, hat oft unüberschaubare Folgen.[19] Vor einigen Jahren ist beispielsweise ein Fall bekannt geworden, in dem ein Angestellter ein Hacker-Tool auf seinem Büro-PC ausprobieren wollte. Dieser kleine Zeitvertreib kostete ihn schließlich den Arbeitsplatz, denn er konnte den Systemadministrator, der das Tool entdeckt hatte, nicht davon überzeugen, dass er mit einem so gefährlichen Programm nur »ein bisschen herumexperimentieren« wollte. Da die Mehrzahl aller Angriffe in Firmennetzen von Innen kommt, nehmen Administratoren solche vermeintlichen Experimente sehr ernst. Aber auch zu Hause können diese Programme sehr viel Schaden anrichten. Wenn Sie nicht genau über die Funktionsweise des Tools Bescheid wissen, könnten Sie es versehentlich »scharf« machen und somit nicht nur sich, sondern auch andere Rechner im Internet gefährden. Diese Tools wurden von Sicherheitsspezialisten oder Hackern entworfen und sind keine Spielzeuge. Möglicherweise machen Sie sich durch den Einsatz und Besitz dieser Produkte sogar versehentlich strafbar. Auch wenn Sie der Meinung sind, diese Programme unter Kontrolle zu haben,

19 Theoretisches Wissen über die Funktion von Angriffswerkzeugen ist sehr wohl auch für Privatpersonen interessant und sinnvoll – das Testen solcher Applikationen sollte man jedoch getrost den Sicherheitsexperten überlassen.

bedenken Sie bitte, dass Sie einem potenziellen Angreifer sein Werkzeug gleich mitliefern und ihm das Leben somit unnötig leicht machen.

Die zweite Kategorie von Programmen, die nicht auf Ihre Festplatte gehören, sind jegliche Programme, die im Hintergrund arbeiten und nicht zu den essenziellen Bestandteilen des Betriebssystems gehören. Dazu zählen Produkte wie Hintergrundbildwechsler und andere Programme, die sich unaufgefordert mit dem Internet verbinden. Bei den erstgenannten handelt es sich um Tools, die nach jedem Neustart des Betriebssystems ein neues Hintergrundbild auf den Desktop zaubern. Diese Bilder werden, während Sie im Internet surfen, aus dem Netz geladen und auf Vorrat auf der Festplatte gespeichert. Was diese Programme nebenbei sonst noch anstellen, können Sie als Benutzer nicht nachvollziehen. Auch ein Virenscanner hilft nicht weiter, denn er schöpft keinen Verdacht, wenn neben den Bildern auch Word- oder Excel-Dokumente übertragen werden. Das beliebte *SETI@home*-Programm, mit dem Sie in Radioteleskopaufnahmen aus dem All nach Anzeichen außerirdischer Intelligenz suchen können, verbindet sich zwar auch im Hintergrund mit einem Server im Internet, kann aber (wenn von der offiziellen Website heruntergeladen) ohne Sicherheitsbedenken benutzt werden. Dennoch sollten Sie in den PREFERENCES des Programms einstellen, dass Sie um Erlaubnis gefragt werden, bevor neue Daten aus dem Netz geladen werden. Eine mögliche Absicherung gegen unerwünschte Aktivitäten von Hintergrundprogrammen ist eine Personal Firewall, wie wir sie in Kapitel 12, *Firewalls und erweiterte Sicherheitssysteme*, betrachten wollen.

Die letzte Kategorie unerwünschter Programme bilden alle unaufgefordert zugesendeten Programme in E-Mail-Anhängen. Wenn Ihr Virenscanner nicht auf dem aktuellsten Stand ist oder ein ganz neuer Virus auftaucht, geht von solchen Attachments eine große Gefahr aus.

Keine unnötigen Spuren hinterlassen

Bevor wir das Thema »Bewusster Surfen« abschließen, wollen wir uns noch einem wichtigen Punkt bei der Vermeidung von Unannehmlichkeiten widmen: Je aktiver und auffälliger Sie sich im Internet verhalten, desto größer ist natürlich die Gefahr, zum potenziellen Opfer zu werden. Wenn Sie also an jedem möglichen Gewinnspiel im Netz teilnehmen oder sich auf vielen Webseiten als Mitglied eintragen, sollte es Sie nicht wundern, wenn Sie sich vor Spam-Mails kaum retten können.

Generell ist es ratsam, sich an die Netiquette (eine Art Kodex für richtiges Verhalten im Internet) zu halten. Wer sich zum Beispiel in Newsgroups anständig verhält, braucht keine Angst vor möglichen Mailbomben zu haben. Dies gilt auch für ICQ und andere Chatsysteme. In älteren Windows-Versionen gab es beispielsweise eine Möglichkeit, Systeme durch so genannte *Nuke'em-Angriffe*[20] zum Absturz zu brin-

20 Dabei handelt es sich um einen Angriff, bei dem mit einem speziellen Programm ein einzelnes mit dem URG-Flag ausgezeichnetes TCP-Paket an einen Rechner geschickt wird und diesen zum Absturz bringt.

gen. Fiel ein Chatter durch sein unverschämtes Verhalten auf, wurde er des Öfteren zum Opfer einer solchen Attacke. Diese Sicherheitslücke wurde zwar in späteren Windows-Versionen gestopft, es gibt jedoch nach wie vor eine Vielzahl von Möglichkeiten, PCs aus dem Internet heraus anzugreifen und eventuell zum Absturz zu bringen.

Möchten Sie in Internetforen nicht belässtigt werden, hilft es sicherlich nicht die persönlichen Kontaktdaten (E-Mail-Adresse, Messenger-Nickname, etc.) oder Bilder von sich selbst dort zu veröffentlichen. Gerade in Foren bekommen die Benutzer untereinander oft das Gefühl, sich schon lange und gut zu kennen, nur weil sie ab und an in der gleichen Community Beiträge verfassen.