In diesem Kapitel:

- Telnet/SSH
- File Transfer Protocol (FTP)
- News
- Instant Messaging (IM)
- Online-Gaming
- Tauschbörsen

KAPITEL 8

Weitere Internetdienste

In diesem Kapitel wollen wir uns einigen weiteren Internetdiensten widmen, denen Sie möglicherweise einmal begegnen werden oder bereits begegnet sind. Dazu zählen neben Terminal und Dateidiensten auch solche für den Feierabend, wie etwa Online-Spiele oder Tauschbörsen. Dabei wollen wir kurz deren technischen Hintergrund beleuchten und anschließend mögliche Sicherheitsrisiken ansprechen.

Telnet/SSH

Um Serversysteme auch von entfernten Computern aus bedienen zu können, wurde das Telnet-Protokoll erfunden. Es ermöglicht einem Client, über Port 23 Kontakt zum Server aufzunehmen und nach der Eingabe der Account-Daten so auf dem Gerät arbeiten zu können, als säße man direkt davor. Der User arbeitet an einer so genannten *Shell* (ein Eingabefenster), in die er Kommandos eingeben kann, die dann auf dem Server ausgeführt werden.[1]

Wenn ein Angreifer an die Account-Daten gelangt und eine Telnet-Verbindung zum Server aufbauen kann, wird es in den meisten Fällen nicht mehr allzu lange dauern, bis er das gesamte System unter seine Kontrolle gebracht hat. Bei sicher gewählten Passwörtern sollte man nun meinen, dass es eigentlich keinen Grund zur Sorge gebe, doch das Problem mit Telnet besteht vor allem darin, dass es die Kommunikations- und auch die Account-Daten im Klartext überträgt. Computer im selben Netz oder Zwischenstationen auf der Route können daher alle Informationen in Echtzeit mitprotokollieren.

1 Wenn Sie sich als Windowsnutzer nichts unter einer Shell vorstellen können, tippen Sie den Befehl `cmd` in das Windows-Fenster AUSFÜHREN (im Startmenü) ein. Diese Kommandozeile ist zwar im Vergleich zu Unix/Linux stark unterentwickelt, gibt Ihnen aber einen ersten Eindruck, worum es geht. Mit dem Kommando `help` erhalten Sie innerhalb der Windows-Shell eine Liste verfügbarer Befehle.

Aus diesen Gründen gilt Telnet bereits seit einigen Jahren als hohes Sicherheitsrisiko. Umso verwunderlicher ist es, dass es trotz zahlreicher Warnungen immer noch auf sehr vielen Servern und Routern zum Einsatz kommt. Der Grund dafür liegt wohl in der Tatsache, dass Telnet standardmäßig auf nahezu allen Netzwerkgeräten installiert ist und der Einsatz von Verschlüsselungen in den USA streng limitiert wird.

Als wesentlich sicherere Alternative bietet sich hingegen die *Secure Shell* (SSH, Port 22) an, bei der der gesamte Datenverkehr stark verschlüsselt übertragen wird. SSH hat und wird Telnet daher zunehmend verdrängen. Zwar sind in der Vergangenheit auch Sicherheitslücken in verschiedenen SSH-Implementierungen aufgetaucht; aktuelle Versionen gelten jedoch als sehr zuverlässig. Voraussetzung ist aber auch hier, dass man stets die neuesten Patches aufspielt. So wurde beispielsweise eine kritische Sicherheitslücke bei der Version 3.0 der Firma SSH Communication Security bekannt, bei der ein Angreifer unter Umständen sogar an *root*-Rechte (Superuser) gelangen kann und somit die volle Kontrolle über den Rechner erhält. Der Fehler lag darin, dass bei Passwörtern mit einer Länge von einem oder zwei Zeichen der Zugang auch bei der Eingabe eines beliebigen anderen Passworts erfolgt, der Passwortschutz also versagt. Das eigentliche Problem liegt nun nicht darin begründet, dass ein SSH-Benutzer leichtsinnigerweise ein so kurzes Passwort wählen würde, sondern darin, dass unter dem Betriebssystem Solaris wichtige administrative Accounts durch das Kürzel NP (»no password«) als gesperrt gesetzt werden. So laufen z.B. einige ganz bestimmte Systemprogramme unter den Benutzerrechten *bin* oder *adm*. Diese Accounts sind nicht für Anwender gedacht, sondern werden nur vom Betriebssystem genutzt. Es ist deshalb nicht wünschenswert, dass sich jemand mit diesen Accounts anmelden kann. Um dies zu verhindern, wählt das Betriebssystem ein Passwort, das nie erraten werden kann, und diese Sperrung wird bei Solaris eben mit NP abgekürzt. Ein NP im Passwortfeld bedeutet also eigentlich, dass ein vom Benutzer eingegebenes Passwort nie stimmt. Die SSH-Implementierung der fehlerhaften Version interpretiert dies jedoch als Passwort aus zwei Zeichen und gestattet daher ungehinderten Zugang zu den Accounts.

Die Konsequenz aus den beschriebenen Schwächen von Telnet sollte für Sie als Benutzer daher lauten, Telnet nur so selten wie nötig zu benutzen und ansonsten auf die jeweils aktuellsten Versionen von SSH zurückzugreifen. Ein kostenloser Telnet- und SSH-Client für Windows ist z.B. Putty, das Sie unter *http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html* finden (siehe Abbildung 8-1).

File Transfer Protocol (FTP)

Obwohl HTTP(S) auch beim Datentransfer stark an Bedeutung gewinnt, ist FTP nach wie vor die Nummer Eins, wenn es um das Up- und Downloaden von Dateien im Internet geht. Im Gegensatz zu den meisten Diensten baut FTP zwei verschie-

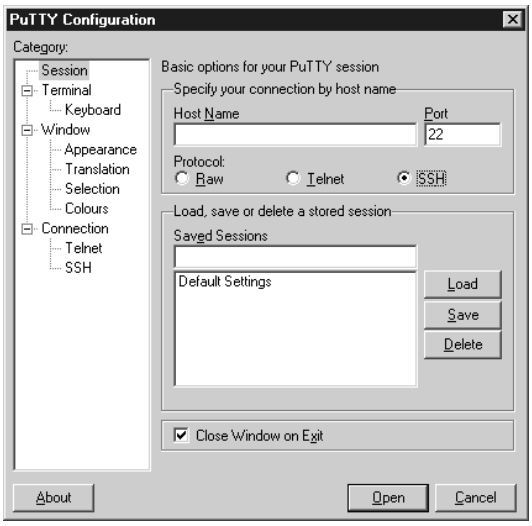

Abbildung 8-1: Der PuTTY-Client in der Windows-Version

dene Kanäle zwischen den Kommunikationspartnern auf: Über Port 21 wird eine Verbindung aufgebaut, über die Server und Client Kommandos untereinander austauschen. Port 20 hingegen dient der Auflistung der Verzeichnisstruktur und der eigentlichen Datenübertragung. Dabei unterscheidet man zwischen dem älteren aktiven und dem passiven Modus.

Beim aktiven Modus wird der Kommunikationskanal vom Client aufgebaut, der Datenkanal jedoch vom Server initialisiert. Diese ungewöhnliche Kombination ist für Firewalls ganz besonders schwer zu handhaben, da es nicht ohne weiteres möglich ist, auf Paketfilterebene festzustellen, ob der aufzubauende Datenkanal auch tatsächlich von dem angefragten FTP-Server stammt oder aber von einem Angreifer.

Beim passiven Modus hingegen initialisiert der Client beide Verbindungen selbst. FTP-Sicherheit ist vor allem aus Serversicht ein wichtiges Thema, da fehlerhafte FTP-Implementierungen in der Vergangenheit eine der häufigsten Einbruchsstellen dargestellt haben. Für Serverbetreiber ist es daher sehr wichtig, stets aktuelle Softwareversionen zu benutzen.

Ähnlich wie beim Schritt von Telnet zu SSH gibt es auch verschlüsselte FTP-Verbindungen, und wann immer möglich sollten Sie von dieser erweiterten Möglichkeit Gebrauch machen.

Aus Benutzersicht sei noch zu erwähnen, dass Sie auf die Rechtevergabe achten sollten. Dabei kann man für jede Datei und jeden Ordner festlegen, wer Zugriff darauf haben soll und wie dieser Zugriff auszusehen hat. Damit jeder beliebige Internetuser Ihre Dateien (z.B. Webseiten) ansehen kann, muss die Rechtevergabe so eingestellt

sein, dass das Anzeigen für alle User (auch unbekannte) erlaubt ist. Hingegen sollte das bei Schreibrechten nicht der Fall sein. Dies ist im Bereich privater Homepages ein häufig gemachter Fehler.[2]

News

Unter dem News-Dienst versteht man den Zugang zu der weiten Welt der *Newsgroups*. Dabei handelt es sich um Interessensgruppen zu fast allen erdenklichen Themen, an denen jeder nach Belieben teilnehmen kann, sobald er die Newsgroup abonniert hat. Aus Clientsicht ist der News-Dienst, der meist über den Browser, aber auch über spezielle *Newsreader* bezogen werden kann, wenig kritisch, weswegen wir ihn hier nur kurz in Bezug auf seine Eignung zur Verbreitung von bösartigem Code oder Social Engineering-Attacken ansprechen wollen. Da vor allem die größeren Newsgroups täglich von hunderttausenden interessierter Benutzer gelesen werden, fällt es Angreifern hier besonders leicht, ein geeigentes Opfer zu finden. Hat er beispielsweise einen Trojaner in einem Musikprogramm versteckt, wird er nirgendwo mehr Erfolg haben, als wenn er seine neue Musiksoftware zum Abspielen beliebiger Audiodateien in einer Gruppe zu genau diesem Thema anpreist. Daher sollten Sie den von Newsgroup-Mitgliedern ausgesprochenen Softwareempfehlungen nicht blind vertrauen. Auch wenn es in solchen Gruppen üblich ist, sich mit vollem Namen zu erkennen zu geben, gibt es keine Garantie dafür, dass diese Person auch wirklich existiert. Ebenso ist dringend davon abzuraten, persönliche Details oder Sicherheitsproblematiken des eigenen Systems öffentlich zu diskutieren. Selbstverständlich sind die meisten Newsgroup-Teilnehmer keine schwarzen Schafe, aber Sie würden im realen Leben ja auch nicht auf dem Marktplatz bekannt geben, wo Sie Ihr Geld verstecken oder dass Ihr Haustürschlüssel unter der Fußmatte liegt. Als letzte Anmerkung zum News-Dienst sei noch erwähnt, dass bei den meisten Groups Archive geführt werden, die auch noch nach Jahren vom Internet aus durchsucht werden können. Schreiben Sie daher mit Bedacht, man wird Sie danach bewerten. Da fast alle erdenklichen Fragen schon einmal gestellt wurden, lohnt ein Blick auf das Archiv unter *http://www.deja.com* (inzwischen Teil von Google).

Instant Messaging (IM)

Dem Schlagwort *Instant Messaging* (IM) begegnet man zurzeit an jeder Ecke des Internets. Dabei handelt es sich um die wohl innovativste und zukunftsträchtigste Dienstkombination der letzten Jahre. Allein eine Beschreibung der verschiedenen Clients und Optionen könnte schon ein ganzes Buch füllen, weshalb wir uns hier nur auf einige sehr grundsätzliche Fakten konzentrieren wollen.

2 Selbstverständlich tritt dieses Problem in seltenen Fällen auch bei kommerziellen Webauftritten auf.

Die Erfolgsgeschichte von IM beginnt bei der israelischen Firma Mirabilis und deren einzigem Produkt *ICQ* (gesprochen »I seek you«). Ziel war es, einen Dienst zu schaffen, der die Kommunikation im Internet in Echtzeit erlauben sollte. Im Gegensatz zur herkömmlichen E-Mail, bei der die Nachricht auf einem Server gespeichert wird und auf den Benutzer wartet, erfolgt der Nachrichtenaustausch bei IM nur dann, wenn die Kommunikationspartner online sind. Der IM-Client zeigt dem Benutzer an, wenn ein Freund oder Kollege online ist und erlaubt dann den sofortigen Nachrichtenaustausch (*Chat*).

Der Erfolg von ICQ war so groß, dass man schnell auf die Firma aufmerksam wurde und AOL sie kurzerhand für eine nicht unbeträchtliche Summe kaufte. Da der Markt für Instant Messaging ein großes Wachstum versprach, traten schnell zahlreiche große Anbieter auf den Plan. Darunter waren neben AOL mit seinem eigenen *AOL Instant Messenger* (*AIM*) und *ICQ* auch Microsoft mit dem *MSN Messenger* und Yahoo! mit dem *Yahoo! Messenger*. Wie so oft wurde auch hier bewusst nicht auf Kompatibilität geachtet, so dass ein AIM- oder ICQ-Benutzer nicht mit einem User des MSN Messenger kommunizieren kann. Das technische Prinzip ist aber bei allen IM-Clients dasselbe: Der Benutzer installiert die jeweilige kostenlose Software auf seinem PC und meldet sich dann beim Dienstbetreiber mit einem Login-Namen und einem Passwort an. In so genannten *Buddy-Listen* kann man im Client eingeben, wen man als Freund, Geschäftspartner usw. einstuft. Ist derjenige dann online, erhält man eine Meldung vom eigenen IM-Client und kann anfangen zu chatten.

Neben diesem rudimentären Dienst bieten inzwischen fast alle Instant Messenger auch die Möglichkeit, Dateien wie zum Beispiel Bilder auszutauschen oder im Video-Chat miteinander zu kommunizieren.[3] Schätzungen gehen daher davon aus, dass einerseits die Anzahl an IM-Nutzern weiterhin stark wachsen wird und andererseits immer mehr Funktionen und Internetdienste innerhalb der Clients untergebracht werden. Schon heute erinnert manches IM-Tool mehr an eine Kommunikationszentrale samt Spionagefunktionen als an ein einfaches Chat-Tool. Besonders hervorgehoben sei hier noch einmal die Rolle des mit Abstand am weitesten verbreiteten ICQ, mit dem man sogar SMS verschicken und empfangen kann. ICQ zu benutzen, ist im Internet schon fast eine Lebenseinstellung geworden, und so ist es nicht weiter verwunderlich, dass dieses Tool die meisten Funktionen aufweist. Übersichtlicher sind für den Einsteiger der AIM oder das Äquivalent von Microsoft. Zudem gibt es einige kleinere Clients, die sich vor allem dadurch von den übrigen unterscheiden, dass man mit ihrer Hilfe auch mit Benutzern anderer Produkte kommunizieren kann (z. B. *Jabber Instant Messenger*, JIM). Für Linux-User kann man neben JIM und dem Yahoo! Messenger vor allem das AIM-kompatible *Gaim* empfehlen, Macintosh-User werden wohl am häufigsten zum Produkt von Yahoo! greifen. Während die Kommunikation zwischen Fremdprodukten und AIM noch teilweise funktioniert, hat sich

3 Zahlreiche Messenger erlauben es inzwsichen, auch Nachrichten an User zu schreiben, die gerade offline sind; gehen die Benutzer schließlich online, erhalten sie die Nachricht.

der MSN Messenger erfolgreich abgeschottet und gestattet eigentlich keine Kommunikation mit anderen Produkten. Dennoch gelingt es einigen Messengern immer wieder, Verbindungen zum MSN Messenger aufzubauen. Microsoft ändert es jedoch anschließend immer wieder das eigene Protokoll so, dass eine Kommunikation mit anderen Produkten wieder unmöglich wird. Dieses Vorgehen erinnert stark an den Browserkrieg Mitte der 90er Jahre, als Microsoft seinen Internet Explorer gegen Netscape in den Ring schickte.

Sicherheitsrisiken

Nach diesem kurzen Einblick in die Produktvielfalt des Instant Messaging wollen wir uns jetzt den Sicherheitsrisiken zuwenden. Dabei werden wir uns bis auf wenige Ausnahmen nicht auf die Implementierungsfehler und Sicherheitslücken der einzelnen Produkte, sondern auf Gefahren in der Konzeption von IM im Allgemeinen konzentrieren.

Ein immer wieder angesprochenes Problem ist die IP-Adresse, die beim Messaging mitübertragen wird. Damit ist es theoretisch möglich, einen Benutzer entweder per DoS-Attacke oder über bekannte Sicherheitslücken in der Software oder innerhalb des Betriebssystems lahmzulegen. Dabei müssen Sie bedenken, dass Sie bei aktiviertem Messenger-Client für alle Benutzer erkennbar, also auch erreichbar sind. Um dieses Problem zu entschärfen, verfügen fast alle Tools über Control-Listen, in denen man eintragen kann, für wen man erreichbar sein will und für wen nicht. Dabei sollte man immer nach der Devise vorgehen, nur diejenigen Benutzer zuzulassen, die explizit in der Buddy-Liste erwähnt sind, und alle anderen zu sperren (siehe Abbildung 8-2).

Die Konfigurationsmenüs der einzelnen Clients sind sehr unterschiedlich, Sie sollten jedoch bei der Auswahl Ihres Clients darauf achten, dass eine solche Control-Liste als Funktionalität zur Verfügung steht. Ebenso sollte es die Möglichkeit geben, die Übertragung der IP-Adresse zu unterdrücken (glücklicherweise setzen viele Anbieter dies bereits als Standardwert). Um interessante Personen leichter im System finden zu können, verfügen fast alle IM-Tools über so genannte Profile, in denen Sie neben Ihrem Namen auch persönliche Daten wie Telefonnummer und Hobbys angeben können. In Abbildung 8-3 sehen Sie das entsprechende Dialogfeld von AIM. Von der Eingabe solcher Daten ist jedoch abzuraten, da das Internet nicht nur aus gut gesinnten Mitbürgern besteht und Sie ja auch sonst nicht jedermann Ihre Privatanschrift samt persönlichen Vorlieben mitteilen. Die Angabe der Daten erfolgt ohnehin auf freiwilliger Basis, daher können Sie sich entscheiden, welche Informationen Sie über sich preisgeben möchten.[4]

4 Einige Messenger (z.B. AIM) weisen darauf hin, dass man mit den hier eingegebenen Daten vorsichtig sein sollte.

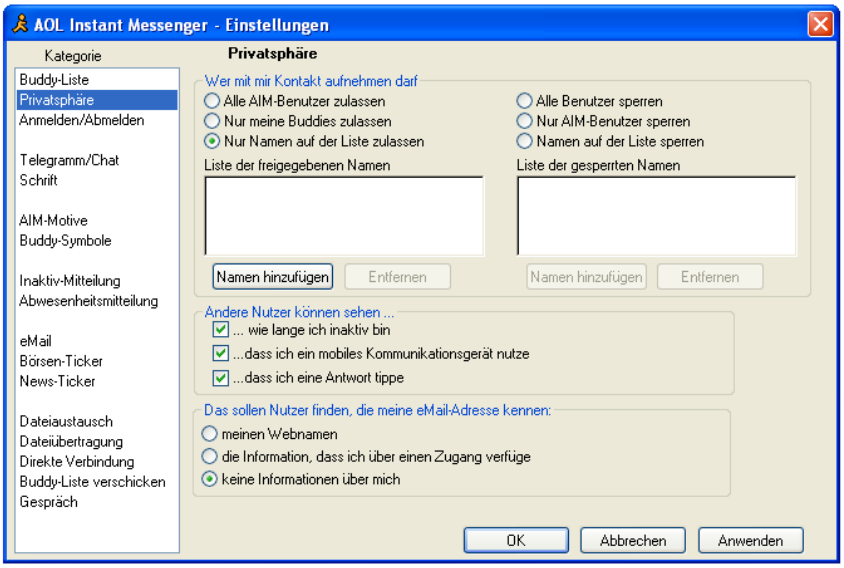

Abbildung 8-2: Für welche Benutzer will man sichtbar sein, für welche nicht?

Abbildung 8-3: Alle hier gemachten Angaben sind öffentlich

Alle IM-Tools leiden zudem an einer weiteren Sicherheitslücke: dem Mangel an Verschlüsselung. Daher sollten Sie daran denken, keine wichtigen, sensiblen Daten per Instant Messaging übers Netz zu schicken. Abhilfe gibt es hier in Form von seperaten Verschlüsselungs-Plugins (z.B. PGP-ICQ), die Sie in Ihren Messenger integrieren können.

Bevor wir uns einer neuen, Besorgnis erregenden Entwicklung im IM-Sektor widmen, wollen wir noch kurz die Spannweite von implementierungsseitigen Sicher-

heitslücken der einzelnen Produkte anreißen. Die bisher bekannt gewordenen Probleme älterer Versionen reichen vom Ausspähen fremder Login-Daten über DoS-Attacken bis hin zur Manipulation der Datenströme durch Dritte. Aber auch typische Mail-Angriffsvarianten gewinnen bei IM zunehmend an Bedeutung. Besonders oft wird von Social Engineering und von Trojanern berichtet, die an Nachrichten angehängt werden. Daher gilt auch hier das bereits im Kapitel 3, *Sicherheitsbewusstsein*, und Kapitel 6, *E-Mail – wer liest mit?*, Gesagte: Da die Wahl des Login-Namens frei ist, sollten Sie keinem angeblichen Administrator oder ähnlichen Personen trauen und Ihre Zugangsdaten sicher aufbewahren.

Spionage

Da die IM-Tools immer ausgefeilter werden, schleichen sich auch immer mehr Sicherheitslücken in die Clients ein. Darüber hinaus versuchen die Hersteller, mit immer neuen Spielereien den User an sich zu binden und damit Geld zu verdienen. Daher gibt es inzwischen auch sehr Besorgnis erregende Entwicklungen am Instant Messaging-Markt. Besonders deutlich wird dies am Beispiel des IM-Client *Odigo*: Bereits in den Lizenzbedingungen wird dem Benutzer mitgeteilt, dass der Hersteller sich vorbehält, alle nicht persönlichen Daten an Dritte weiterzugeben. Da Lizenzbedingungen aber zum einen oft seitenlange Texte sind und zum anderen meist ähnliche Inhalte haben, akzeptiert man sie gern, ohne den Text genau gelesen zu haben. Im Fall von Odigo begibt man sich damit aus den oben genannten Gründen in eine gewisse Gefahr.

Damit nicht genug: Als besonderes Gimmick bietet Odigo auch ein so genanntes *Site-Radar*. Damit bekommt der User angezeigt, wer gerade auf derselben Webseite surft wie man selbst. Dazu fängt das IM-Tool die HTTP-Verbindungsdaten des eigenen PCs ab und leitet sie an den Odigo-Server weiter. Befinden sich noch andere Personen auf der gleichen Seite, werden sie im Radar angezeigt (siehe Abbildung 8-4). Zwar gibt man dem Benutzer glücklicherweise die Möglichkeit, sich auf »unsichtbar« zu schalten und somit nicht mehr für andere Nutzer sichtbar zu sein, das Programm überträgt die Daten aber dennoch weiterhin an den Odigo-Server.

Als letzter Ausweg bleibt nur, den Client jedes Mal zu deaktivieren, wenn man seinen Browser benutzen möchte. Solche Spielereien gehen eindeutig in die falsche Richtung und liefern dem Hersteller nebenbei Nutzerprofildaten, die er für teures Geld verkaufen kann.

Online-Gaming

Immer mehr Computerspiele bieten Ihnen die Möglichkeit, auch gegen menschliche Gegner zu spielen, oder sind gar ganz auf das Spielen im Internet (mit und gegen tausende anderer Spieler) ausgelegt. Dazu ist das Internet als Trägernetz geradezu

Abbildung 8-4: Mit dem Radar kann man sehen, wer sich auf derselben Webseite aufhält wie man selbst.

prädestiniert, da man dort zu jeder Uhrzeit Benutzer aus aller Welt antreffen kann und sich dazu nicht einmal aus der eigenen Wohnung zu bewegen braucht. Dabei sind vor allem zwei Problemtypen bekannt.

Im Fall der Spieleplattform *Battle.net* änderte z.B. der Hersteller kurzerhand die Nutzungsbedingungen auf seinem Server mit dem Ziel, die Verbindungsdaten samt eines eindeutigen Schlüssels aus der Hardware aufzuzeichnen. Trotz eines gewaltigen Proteststurms seitens der Benutzer und eines Hacks auf die Homepage des Anbieters wurden die Änderungen in den Nutzungsbedingungen nur teilweise zurückgenommen, und so muss man damit rechnen, dass dieses Modell auch von anderen Unternehmen übernommen wird. Die Konsequenz daraus ist, dass es für immer mehr Firmen möglich ist, Zugang zu den Daten ihrer Kunden zu erhalten.

Die zweite und größere Gefahr liegt in Spielen, bei denen die Kommunikation nicht über einen zentralen Server, sondern direkt über die Computer der einzelnen Spieler läuft. Dabei übernimmt einer der User die Rolle des Servers und wartet, bis sich genügend Spieler bei ihm angemeldet haben. Während des anschließenden Spiels ist

der Server dafür zuständig, die Daten über den Spielverlauf möglichst zügig an alle beteiligten Clients zu schicken. Dazu muss er diesen Kommunikationsendpunkte anbieten, über die der Datenaustausch möglich wird. In den meisten Fällen kommt dabei das typische Client-Server-Prinzip mit den uns schon bekannten Ports zum Einsatz.

Oftmals sind sich die Betreiber solcher Kurzzeitserver nicht im Klaren darüber, welche Konsequenzen diese Kommunikation mit sich bringt. Genau wie bei jedem anderen Server auch sind die Ports offen und warten auf eingehende Verbindungen. Wer nun aber versucht, eine solche Verbindung herzustellen, ist für den Spieler, der den Server betreibt, nicht ersichtlich. Meist kann er zwar im Notfall einen Benutzer vom Server verbannen, dies ist aber kaum ein Schutz gegen gezielte Angriffe auf diese offenen Ports.

Damit sind solche Server zum einen sehr anfällig gegen DoS-Angriffe, denn sie verfügen über keine oder nur schwache Sicherheitsmaßnahmen gegen ein Bombardement mit sinnlosen Anfragen. Zum anderen werden immer wieder Möglichkeiten bekannt, mit denen ein beliebiger Client den Computer, auf dem der Server läuft, vollständig in seine Gewalt bringen oder zumindest Systemabstürze verursachen kann. Da viele Hersteller der Spiele davon ausgehen, dass über die offenen Ports nur die spielinternen Daten übertragen werden, kommen Sicherheitslücken zustande. In der Realität kann man aber nahezu beliebige sinnvolle und sinnlose Daten an den Server senden. Dieser muss dann versuchen, mit dem Datenmüll umzugehen, und ist damit oftmals überfordert. Erwartet er zum Beispiel von einem Client als Anmeldung die IP-Adresse samt Benutzernamen und erhält stattdessen eine sehr lange Zahlenkolonne, kann dies dazu führen, dass der für den Namen reservierte Speicherbereich überläuft und einen Programmfehler bewirkt (ein so genannter *Buffer Overflow*). Mehr dazu erfahren Sie in Kapitel 10, *Viren, Würmer und Trojaner*.

Genauso kann man bei einigen Spielen den Server bereits damit ausreichend beschäftigen, dass man ihm seine eigene IP-Adresse als Antwortadresse vorgaukelt. Der Server interpretiert die Anfrage und antwortet sich sozusagen anschließend selbst. Da die Anzahl der gleichzeitigen Verbindungen oftmals beschränkt ist, führt das unter Umständen dazu, dass der Server für andere nicht mehr erreichbar ist. Meist ist es bei den heutigen Spielen nicht mehr mit solch rudimentären Mitteln möglich, ernsthaften Schaden anzurichten. Ausgefeiltere Angriffstaktiken führen jedoch nach wie vor fast immer zum Erfolg.

Machen Sie sich daher immer klar, dass ein offener Port eine ernsthafte Gefahr für Ihre Datensicherheit darstellt. Ohne dass man sich dessen bewusst ist, verhält es sich mit den Spiele-Clients oft ähnlich wie mit den Servern. Auch diese müssen ja einen Port öffnen, um die Kommunikation aufzubauen. Da der Spieler von der Datenübertragung zwischen seinem Programm und dem Server nichts mitbekommt, kann er nicht feststellen, welche Inhalte überhaupt ausgetauscht werden. Ein bösartiger Server könnte anstelle der regulären Spieldaten auch andere Dinge in

den Datenstrom einfließen lassen und so eventuell an Dateien oder auch Zugangsmöglichkeiten zu anderen Diensten gelangen.

Dies alles wäre nicht so dramatisch, wenn die Hersteller nicht eine »Alles oder Nichts«-Taktik im Hinblick auf Personal Firewalls, Router und Proxys verfolgen würden. Wer daher versucht, solche Sicherheitsmaßnahmen zu nutzen, bleibt bei vielen Spielen immer noch außen vor.[5] Als Beispiel soll hier das weit verbreitete Spiel Quake III dienen, bei dem es bis zur Version 1.17 für den Betreiber eines Servers möglich war, beliebige Dateien auf den Rechnern der Clients zu löschen. Die Gefahr ist zwar in neueren Versionen gebannt, es zeigt aber deutlich die Problematik solcher Spiele auf.

Man muss sich zudem bewusst machen, dass die meisten Sicherheitslücken in Softwareprodukten von der Öffentlichkeit unentdeckt bleiben, da sie vom Hersteller nicht veröffentlicht werden (dies gilt nicht nur für Spiele, sondern für jede Art von Software). Entweder schließt der Hersteller die Sicherheitslücke unauffällig in einem späteren Patch, oder das Problem bleibt weitgehend unbekannt.

Tauschbörsen

Seit Jahren sind Internet-Tauschbörsen das Streitthema schlechthin im Netz. Wir wollen uns hier nicht mit der Frage auseinander setzen, ob die Software an sich strafbar ist oder nur das Tauschen Copyright-geschützter Daten.

Bei Internet-Tauschbörsen handelt es sich in den allermeisten Fällen um so genannte *Peer-to-Peer-Software* (*P2P*), also um Programme, die im Prinzip ohne das Client-Server-Modell auskommen oder einen zentralen Server nur als Listenverwalter für angeschlossene Tauschbörsenmitglieder benötigen. Genau genommen fungieren Rechner, auf denen Tauschbörsenprogramme installiert sind, immer als Client und Server zugleich. Jeder Benutzer bietet Dateien (meist Filme, Musik oder kommerzielle Software wie etwa Computerspiele) zum Tausch an, sucht aber im Gegenzug selbst nach neuen Inhalten und lädt diese von fremden Computern herunter. Im ersten Fall dient sein Rechner also als Server, im zweiten als Client. Um das Herunterladen (den Download) zu beschleunigen, ist es zudem in den meisten Fällen möglich, eine Datei von mehreren Quellen gleichzeitig herunterzuladen. Dazu wird die Datei in einzelne Segmente aufgeteilt, und diese werden getrennt downgeloadet und anschließend wieder auf dem eigenen Computer zusammengefügt. Dies ist bei großen Dateien wie etwa Filmen besonders wichtig, da hier mehrere hundert MByte herunterzuladen sind und die Wahrscheinlichkeit, dass ein Tauchbörsenbenutzer, von dessen PC man gerade downloadet, offline geht, entsprechend groß ist. Zudem benutzen die allermeisten Tauschbörsennutzer (A)DSL-

5 Wobei hier lobend gesagt werden muss, dass immer mehr Spiele mit Personal Firewalls und Routern umgehen können.

Anschlüsse und können damit zwar sehr schnell Daten herunterladen, aber nur verhältnismäßig langsam anbieten. Das Verhältnis liegt je nach DSL-Anbieter und Tarif etwa zwischen 5:1 und 10:1. Im letzteren Fall kann man also Daten zehnmal schneller aus dem Internet »ziehen« (downloaden), als man andere hinaufladen (uploaden) kann. Fordern sie verschiedene Segmente der Datei von unterschiedlichen Computern an, nutzen Sie Ihre Leitung folglich viel effektiver.

Wie bereits angeklungen, sind 99% aller angebotenen Inhalte gesetzlich ausdrücklich nicht dafür vorgesehen getauscht zu werden. Wer also beispielsweise den neuesten Kinofilm aus dem Internet lädt, macht sich strafbar.[6] Da es viele hunderttausend Tauschbörsennutzer gibt und diese noch dazu in mehreren unabhängigen Tauschbörsennetzen agieren, ist es für die Copyrightinhaber jedoch kaum möglich, dagegen vorzugehen. Inzwischen gibt es zwar erste Klagen gegen Massentauscher, dies ist jedoch mehr ein symbolischer Akt. Nachdem die Industrie jahrelang versucht hat, Tauschbörsen zu verteufeln und den Benutzern Angst zu machen, hat man jetzt ein deutlich besseres Mittel gegen Tauschbörsen gefunden: Anstatt die eigenen potenziellen Käufer zu kriminalisieren und zu verklagen, bietet man einfach Musik titelweise und gegen eine wirklich vertretbare Gebühr im Internet zum legalen Download an. Apples *iTunes Music Store*, der etwa 60% der weltweiten Marktanteile an diesem noch sehr jungen Markt hält, gab im Sommer 2005 bekannt, binnen weniger als zwei Jahren schon mehr als 500 Millionen Musikstücke verkauft zu haben. In der gleichen Zeit stellte man übrigens erstmals Anzeichen für das Schrumpfen der illegalen Tauschbörsen fest.

Bevor wir nun zur eigentlichen Sicherheitsproblematik kommen, sei noch ein kurzer persönlicher Kommentar zum Thema Tauschbörsen, Industrie und Rechtssystem erlaubt (weitere Ausführungen zur Rechtslage im Allgemeinen finden Sie im nächsten Kapitel): Wenn es etwas gibt, das ich als größte Errungenschaft des Internets bezeichnen würde, dann sind es die unglaubliche Geschwindigkeit und Intensität, mit der sich dort neue Ideen verbreiten, und der unüberhörbare Ruf nach Informationsfreiheit und Kommunikationswille. Das Tauschen von Copyright-geschützten Daten im Internet ist ein ernsthaftes Problem und ganz eindeutig nicht legal. Es stellt die Musik- und Filmindustrie, vor allen Dingen aber die Künstler, vor ernsthafte Schwierigkeiten und soll hier in keinster Weise beschönigt werden. Das virtuelle Stehlen von Musikstücken und Filmen ist aber nur die eine Seite der Medaille, während die andere gern möglichst unter den Teppich gekehrt wird: Tauschbörsen wären ohne so genannte Komprimierungsformate gar nicht denkbar. Diese Formate (im Musikbereich ist das bekannteste sicherlich MP3) verkleinern die Datenmenge, die eine Musikdatei oder ein Film auf der heimischen Festplatte einnimmt, grob

6 Übrigens ist es längst eine Frage der Ehre geworden, wer welche Datei zuerst und in guter Qualität anbieten kann. Teilweise gibt es daher den neuesten Hollywood-Streifen schon einen Tag nach oder gar vor der Premiere in guter Qualität als Download. Wie dies gelingt und welche Motive diese gigantische Community antreiben, wäre sicherlich ein eigenes Buch wert.

gesagt um das Zehnfache nahezu verlustfrei. Ohne diese Komprimierung wären die Dateien viel zu groß, um sie per Internet zu verschicken, und ließen sich kaum auf mobile Datenträger speichern. Die überwältigende Mehrheit dieser Komprimierungsformate dient eben dem Zweck des illegalen Tauschens und weit über 90% aller so gebündelten Daten werden nicht Copyright-gerecht genutzt. Warum hat dann aber die Industrie,[7] lange bevor der erste Gedanke an legale Musikportale überhaupt ins Auge gefasst wurde, Geräte zum Abspielen von MP3-Dateien auf den Markt gebracht und viele Millionen dieser Geräte verkauft? Das Gleiche gilt ebenso für DVD-Player, die spezielle Funktionen besitzen, um selbst gebrannte und komprimierte CDs abspielen zu können, und für renommierte Softwarehersteller, die Programme auf den Markt bringen, mit denen man halbautomatisch große Mengen an Musik-CDs im MP3-Format auf die Festplatte bannen kann. Der heimische PC eignet sich nur sehr bedingt als Multimediazentrale, und Tauschbörsen hätten nie den derzeitigen Stellenwert erreicht, wenn die Industrie nicht allzu gerne daran mitverdient hätte. Zusätzlich hat man sich anscheinend nie die Frage gestellt, warum die eigenen Kunden plötzlich im großen Stil anfangen, Musik und Filme zu stehlen, anstatt ins Kino zu gehen oder CDs zu kaufen. Stattdessen hat man die Preise weiter erhöht und die Tauschbörsennutzer verklagt und kriminalisiert. Einem 16-jährigen Tauschbörsennutzer wäre aber sicherlich viel eher damit gedient gewesen, wenn er das Musikstück seiner Wahl für 99 Cent hätte herunterladen können, anstelle die ganze (mäßige) CD für 16 Euro kaufen zu müssen. Gerichtlich mit hohen Strafen gegen diese Benutzer vorzugehen und somit seine eigene Kundschaft zu verklagen und zu verteufeln, ist aber sicherlich nicht der richtige Schritt. Glücklicherweise hat nach Jahren das Umdenken in der Industrie begonnen, und zahlreiche legale Plattformen haben sich im Internet etabliert. Die eigentlich tolle Idee, einzelne Musikstücke zu jeder Zeit aus dem Internet beziehen zu können, wurde also aufgegriffen und in legale Bahnen gelenkt.

Kommen wir nach diesen Überlegungen zurück zum Thema Sicherheit. Bei Tauschbörsen gibt es vor allem drei wichtige Punkte zu beachten: Die Sicherheit der Software, die wahre Natur der getauschten Daten und unerwünschte Inhalte.

Der Sinn der Tauschbörsensoftware ist es, Dateien auf Ihrem Computer für den Rest der Welt zugänglich zu machen (und zwar in den meisten Fällen so, dass Sie keinen Einfluss darauf haben, wer diese von Ihrem PC anfordert). Aber wie stellen Sie sicher, dass nur die von Ihnen gewünschten Dateien getauscht werden können und nicht der gesamte Inhalt Ihrer Festplatte? Die Tauschbörsenprogramme erlauben, hierfür spezielle Ordner zu benennen, die nach außen sichtbar sind, während der Rest verborgen bleibt. In der Vergangenheit haben sich aber immer wieder Fehler eingeschlichen, mit denen diese Einschränkungen umgangen werden konnten. Unter Umständen stellen Sie also sämtliche privaten Dokumente und Bilder offen

7 Darunter fallen übrigens auch die eigentlichen Copyright-Träger.

im Netz zur Verfügung. Mittels einiger Sicherheitlücken war es darüber hinaus sogar möglich, beliebige Dateien auf dem Computer des Tauschbörsennutzers abzulegen. Dies können beispielsweise Trojaner sein, aber auch illegale Inhalte. Es ist natürlich allzu verständlich, dass ein Angreifer solch gefährliche Daten ungern auf seinem eigenen Computer liegen hat, wenn er sie auch mit Hilfe fremder Systeme verteilen kann. Im Ernstfall wird es Ihnen als ahnungslosem Benutzer überaus schwer fallen, der Polizei zu erklären woher dieses Material kommt und dass Sie nichts damit zu tun haben. Diese Gefahr ist übrigens keineswegs nur theoretischer Natur. Es ist nicht selten, dass Cracker illegale Daten auf fremden Servern und PCs lagern. Sicherheitslücken dieser Art werden immer wieder in Tauschbörsenprogrammen auftauchen, und es ist nicht klar, wie schnell (und ob) der Hersteller diese beseitigen kann.

Die Natur der getauschten Daten und unerwünschter Inhalte sind oftmals eng miteinander verbunden, wir wollen sie dennoch getrennt betrachten. Es ist verwunderlich, dass man in manchen Tauschbörsennetzen wirklich alles findet, was man in die Suchmaske eingibt, und es dabei keine Rolle spielt, ob und wie stark man sich bei der Eingabe vertippt hat. Bei einem nicht unerheblichen Teil[8] der angebotenen Dateien handelt es sich nämlich nicht um die erhofften Inhalte, sondern um Trojaner; und einige dieser Trojaner sind so programmiert, dass sie stets so heißen wie die gesuchte Datei. Lädt man sich im Glauben, dem Dateinamen blind vertrauen zu können, den Trojaner herunter (und startet ihn, weil man die Datei für Musik hält), gerät der eigene Computer in die Hände des Angreifers. Es gibt inzwischen sogar Trojaner, die speziell auf einige Tauschbörsen optimiert wurden. In der Regel kann man den Betrug jedoch an der Dateigröße, dem Windowssymbol oder der Dateiendung festmachen und sollte solche Dateien niemals herunterladen oder zumindest nicht starten.

Die Suche in Tauschbörsen basiert neben anderen Angaben vor allem auf den Dateinamen. Da diese aber frei wählbar sind, können Sie nicht davon ausgehen, dass sich hinter einem angegebenen Titel auch tatsächlich der gesuchte Film oder Song verbirgt. Es muss nicht gleich ein Trojaner sein, oft ist die Überraschung schon groß, wenn man sich nach tagelangem Download eine völlig andere und unerwünschte Art Film auf den Rechner geladen hat. Einige Tauschbörsennutzer machen sich sogar ein Spaß daraus, lauter skurrile Inhalte mit beliebten Schlagwörtern zu tarnen. Dies ist vielleicht keine Sicherheitslücke im klassischen Sinn, unschön ist es allemal.

Verzichten Sie daher lieber generell auf die Nutzung von Tauschbörsen, oder tauschen Sie ausschließlich dazu bestimmte Inhalte. Die Künstler, deren Musik man gern hört, sollte man nicht um Ihren Lohn bringen.

8 Man munkelt sogar, dass es Anzeichen gibt, einige Trojane seien im Auftrag der Musikindustrie eingeschleust worden, um die Tauschbörsen zu schädigen bzw. zu zerschlagen.