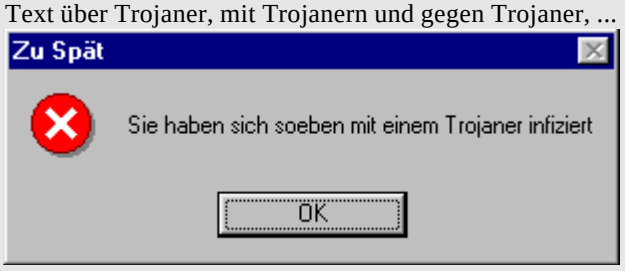
Trojaner
Kompendium

-- Medium Edition --

Geschrieben von:
Megaman IV

Text über Trojaner, mit Trojanern und gegen Trojaner, ...



damit Ihnen DAS nicht passiert!

Inhalt

Rache ist süß
Rausfinden, wer der Angreifer ist und Wege ihn in Schwierigkeiten zu bringen

Nachwort
Das letzte Wort / Das Wort zum Sonntag

Vorwort

Ich schreibe dieses Dokument um meinen Teil dazu beizutragen, dass das Internet nicht aus einer Masse von dummen Usern besteht, die keine Ahnung von Computern, Internet und Sicherheit haben.
Ich will allgemeine Sicherheit alle User im Internet, indem ich Wissen anbiete, dass nur Leute haben, die sich mit dem Thema beschäftigt haben oder selbst Trojaner nutzen. Wer nicht auf Securityseiten oder Hackerseiten surft, der weiß eventuell nicht einmal, was alles möglich ist. Dazu will ich echte Informationen zum Thema „Hacking mit Trojanern“ bieten und erwähnen, dass das „Hackers Blackbook“ der letzte Müll ist, den es gibt. Wer sich davon Überzeugen will, kann es von mir als E-Book haben. „Hackers CD“ würde ich mir auch nicht hohlen, denn es ist vom selben Anbieter.
Ich bin mir im Klaren, dass dieses Wissen auch zu illegalen Zwecken genutzt werden kann, aber das ist mit egal, denn ihr seit selbst dafür verantwortlich, was ihr mit dem Wissen macht.

>Wissen ist Macht<

Was sind Trojaner und was machen die ?

Trojaner (genauer gesagt Trojanische Pferde) sind Programme, die unbemerkt im Hintergrund nicht autorisierte und/oder unerwünschte Aktionen ausführen. Dabei werden sie stets von einem Angreifer gesteuert. Daher auch der Name nach dem Trojanischen Pferd, mit dem (in der griechischen Mythologie) sich die Griechen bei der Schlacht um Troja in Troja einschlichen und die Trojaner dumm aus der Wäsche guckte, als das Tor für die Griechen plötzlich offen stand (ich hoffe, jeder kennt es). Je nach Machart des Trojaners kann der Angreifer beinahe alles tun, was ihm beliebt, da er die volle Kontrolle hat.

Trojaner können:

- Dateien hochladen (einschleusen) und runterladen (stehlen)
- Informationen sammeln
- Passwörter ausspionieren
- Maus und Tastatur beeinflussen
- Programme starten und beenden
- Monitorbild beobachten und verstellen
- Und viele andere (für den Angreifer) lustige Dinge

Dies waren nur die wesentlichsten und allgemeinsten Punkte. In der Praxis äußert sich das so, dass er mit einem Keylogger auch alle nichtgespeicherten Passwörter findet und zum Beispiel auch deine ICQ Nummer (UIN) inklusive der Einstellungen und der Contact List übernimmt, alle Mails mitlesen kann und von dem infizierten Rechner aus weitere Angriffe auf andere Rechner starten kann, ohne dabei entdeckt werden zu können. Was jetzt noch relativ harmlos klingt, kann schlimme Folgen haben.

Trojaner sind also in der Hand von Profis ein sehr gefährliches Werkzeug. Im Normalfall werden sie aber nur zum stehlen von Passwörtern und zum Ärgern benutzt.

Wer ist der Angreifer ?

In der „Szene“ gibt es ganz unterschiedliche Ansichten über Trojaner und deren Benutzer. Es ist erst mal sinnvoll einige Begriffe zu klären. Das Problem ist, dass viele andere Definitionen zu den Gruppen haben. Meine lauten so:

Ein Hacker : macht sich Sicherheitslücken und sein Wissen zunutze um in fremde Computersysteme einzudringen. Dabei richtet er keinen Schaden, außer um seine Spuren zu verwischen (Logfiles löschen) und hinterlässt hin und wieder eine Visitenkarte. Er tut dies um Daten zu stehlen, zu zeigen, dass es in dem Bereich eine Sicherheitslücke gibt oder um einfach nur sein Ego zu stärken. Auch ein richtiger Hacker kommt ohne Trojaner nicht aus, behauptet aber stets seine selbstprogrammierten Trojaner zu nutzen. Ohne Hacker als Helden darstellen zu wollen, können wir Ihnen, dank vieler Angriffe nun sehr ausgeklügelte Sicherheitssysteme verdanken, die das digitale Verbrechen sehr schwer machen.

Ein Cracker : Es gibt zwei Definitionen für einen Cracker:
Nr.1) Ein Cracker hat mit hacken wenig tun. Ein Cracker macht sich lieber über Programme her und knackt z.B. mittels Kenntnisse in Assembler Kopierschutz-Mechanismen, snifft Serialkeys und erstellt Keygenerators und Cracks.
Nr.2) Ein Cracker ist ein „böser“ Hacker, der hackt, um zu zerstören.

Script Kiddi : „Script Kiddi“ ist ein Schimpfwort für Leute, die nur Trojaner nutzen. Es wird benutzt, weil man mit Trojanern schnell gute Erfolge haben kann, ohne hacken zu können. (Ähnlich verhält es sich mit dem Schimpfwort „Camper“, oder „Cheater“).

User : Ein Computerbenutzer ohne fortgeschrittene Kenntnissen. Die am häufigsten anzutreffende Benutzergruppe.

DaU : **D**ümmste **a**nzunehmende **U**ser. Gerade Anfängern droht die Gefahr als ein DaU durchzugehen. Um die Anzahl der DaUs zu verringern ist z.B. auch deses Dokument geschrieben.

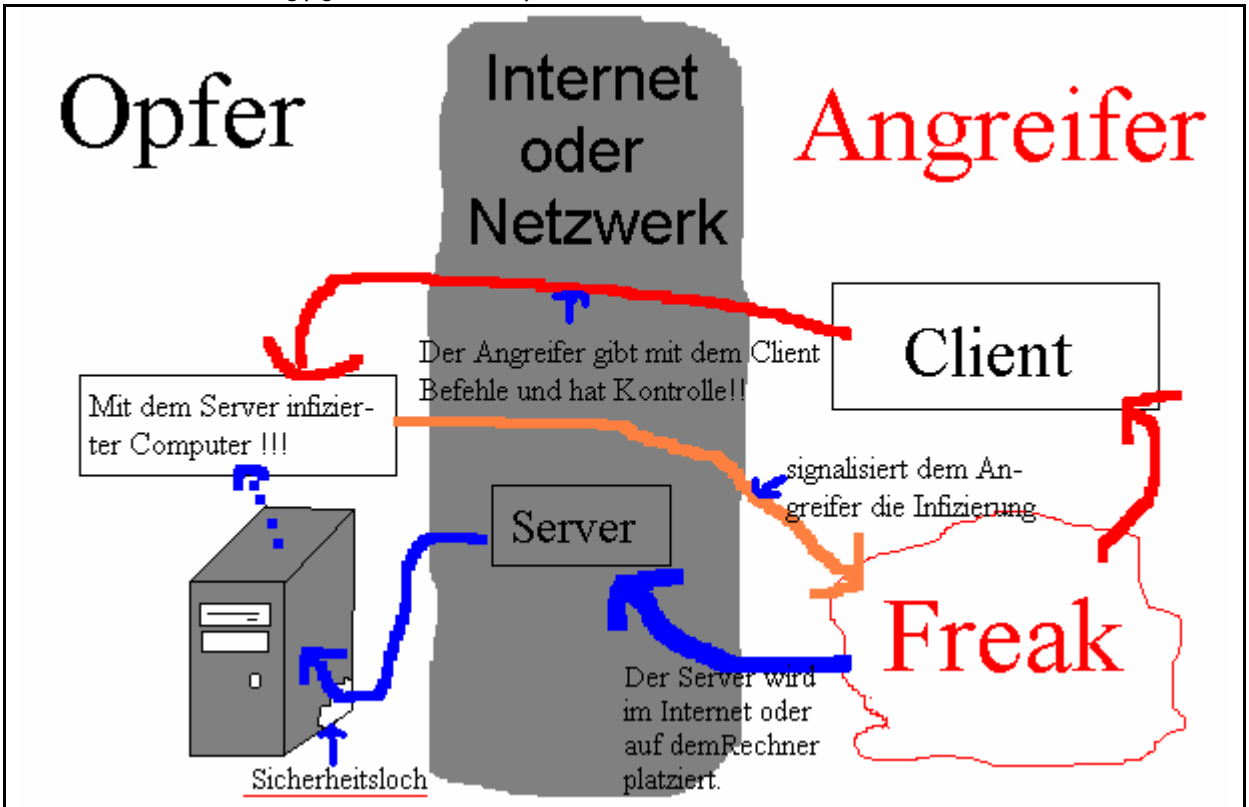
Lamer : Ein Vollidiot, der keine Ahnung von Computern hat, aber meint viel von Computern und Hacken zu verstehen. Wird gerne und oft als Schimpfwort benutzt, hat aber daher an ursprüngliche Gewichtung verloren. Einfach nicht ernst nehmen.

Da in der „Szene“ mit den Begriffen nur so um sich geworfen wird, ist ein „Hacker“ oder sonst was im folgenden nur noch ein „Angreifer“.

Wie funktioniert ein Trojaner ?

Der Trojaner besteht in der Regel aus zwei, manchmal auch drei Teilen. Aus einem Server (= Diener. Das ist der eigentliche Trojaner), dem Client (=Der „Bediente“) und manchmal aus einem „EditServer“ (Mit dem man Einstellungen an dem Server vornehmen kann).
Ziel des Angreifers ist es, dass das Opfer den Trojaner (also den Server) ausführt. Falls dies geschehen ist, verbindet sich der Angreifer unter Benutzung des Clients mit dem Server. Dabei kann der Server Hilfestellung geben, indem er über ICQ oder per Mail die IP des Opfers schickt und damit gleichzeitig signalisiert, dass das Opfer online ist. Selbige Einstellungen werden dann per Knopfdruck mit dem „EditServer“ vorgenommen. Ein Angreifer kann aber auch einen IP Bereich abscannen, ob auf einem Computer eventuell einen Trojaner läuft. Wenn man zum Beispiel weiß, dass IPs von T-Online User meistens zwischen 62 .150.0.0 - 62 .255.255.255 liegen, kann man den Bereich scannen und hoffen, dass irgendein Script Kiddi einen Trojaner mit Standart Port und ohne Passwort

hinterlassen hat. Dann verbindet man sich mit dem Server und stiehlt die Passwörter und schon hat man eine kostenlose T-Online Flatrate.
Aber zuerst muss der Angreifer dem Opfer den Server erst mal unterjubeln. Entweder er macht es selbst, indem er sich an den PC des Opfers setzt oder er schickt es getarnt per Mail oder bietet es unter falschem Namen zum Download an (beliebt sind: "Sex.exe", "Pamela_Anderson.jpg.exe" usw. ...).



Erklärung zum Bild: Der Angreifer (Freak), platziert den **Server** und dieser gelangt entweder durch eine Sicherheitslücke oder durch die Dummheit des Benutzers in ein System und infiziert es. Nun schickt der Server meist Signale zum Angreifer, um zu zeigen, dass er online ist, was allerdings nicht zwingend ist. Auf jeden Fall wird der Freak sich mit Hilfe des **Clients** mit dem Server verbinden und hat nun volle Kontrolle.

Dann muss der Angreifer nur noch erreichen, dass das Opfer den Server auch ausführt. Gerade Internet Neulinge fallen auf die billigsten Tricks rein. Es gibt eine Menge Tricks um jemanden dazuzubringen den Server auszuführen. Einer ist z.B. einen sehr langen Dateinamen zu wählen und zu versuchen den Server über ICQ an irgendwelche Leute zu verschicken und sagt es wäre ein Bild. Das Opfer kann aufgrund der Länge des Namen die Endung nicht erkennen und denkt es wäre ein Bild und lässt die Datei eventuell von ICQ ausführen. Gerade bei ICQ sollte man aufpassen, was man geschickt bekommt. Ebenfalls, kann der Angreifer das Icon der Datei so ändern, sodass sie wie ein Bild aussieht. Wenn das Opfer nicht auf die Endung achtet oder das Anzeigen aller Dateiendungen deaktiviert hat (oder besser gesagt nicht aktiviert hat) kann man getäuscht werden. Ich möchte nun nicht weiter auf die vielen Tricks eingehen, wie man andere User bescheißt.
Hat das Opfer den Trojaner, egal wie, ausgeführt dann sorgt der Server automatisch dafür, dass er beim nächsten Start des Computers auch garantiert wieder gestartet wird. Die Palette reicht von Manipulation wichtiger Systemdateien über Einträge in Startdateien bis hin zu Einträgen in die Registry. Dabei können mehrere Dateien eingetragen werden, die sich gegenseitig Schreibschützen und eventuell neu kopieren und Einträge wiederherstellen.
Nun muss der Server und hauptsächlich der Angreifer dafür sorgen, dass der Server nicht von Firewalls, Virenscannern und Benutzer entdeckt wird. Dazu kann er die

Virendefinitionen der Virenscanner löschen oder modifizieren oder das Programm komplett löschen um eine Erkennung zu verhindern. Der Server kann verhindern, dass Firewalls u.ä. beim nächsten Systemstart gestartet werden und meldet sich erst dann beim Angreifer. Eine weitere interessante Taktik ist das sogenannte „joinen“. Dabei wird eine Datei mit einer anderen „gejoint“, sodass eine Datei entsteht, die beide Ursprungsprogramme enthält und auch beide startet. Dies hilft um Trojaner vor Virenscannern zu verstecken. Am meisten Probleme bereitet dem Angreifer das Überwinden einer Firewall. Dort kann nur das Wissen über Fehler in einem Programm oder das joinen mit einem „Killer“ helfen. Ja, auch Firewalls haben Fehler. Die Firewall „Lockdown 2000“(Lockdown 7.0) kann im Haupttextfeld nur 61000 Zeichen darstellen. Wenn sich ein Angreifer verbinden will, dann werden etwa 300 Zeichen für die Logfile dargestellt. Nun muss man nur genügend Angriffe vortäuschen (Programme gibt’s genug, ansonsten selbst schreiben) und Lockdown stürzt kommentarlos ab. Der Weg wäre nun frei. Ein anderer gemeiner Trick ist es den Server mit einem „Killer“ zu joinen. Ein Killer schafft es alle speicherresistenten Programme trotz dieses Schutzes zu beenden. Wird die Datei ausgeführt verabschieden sich Firewall und Virenscanner. Der Weg ist abermals frei. Am besten ist es für den Angreifer allerdings, wenn das Opfer keinen im Hintergrund laufenden Virenscanner und keine Firewall hat.
Wenn der Trojaner also am Laufen ist, kann sich der Angreifer mit seinem Client mit dem Server verbinden und dem Server Befehle erteilen. Der Server kann dabei mindestens genauso viel, wie das Betriebsystem kann. Gerade unter Windows™ 9x ist es für „Visual Basic“ Trojaner ein leichtes die verschiedensten Aktionen auszuführen. Verschiedene Trojaner haben je nach Zweck verschiedene Fähigkeiten. Einige Trojaner sind nur zum Ärgern oder nur zum chatten da. Gerade die sind schwer zu erkennen, weil es sehr viele gibt und es für Software schwer wird zwischen einem gutartigem Programm und einem Trojaner zu unterscheiden. Die meisten Programme können daher nur bekannte Programme entdecken. Jeder Trojaner bietet dem Angreifer die Möglichkeit, sich selbst wieder von Rechner eines Opfers zu entfernen, also kann es sein, dass man auch bei regelmäßigen Tests einen Trojaner nicht bemerkt, weil er nämlich schon gar nicht mehr da ist.

Welche Gefahr geht von Trojanern aus?

Wie ich in dem vorherigen Kapitel bereits angedeutet habe, geht, wenn es um Spionage geht, von Trojanern eine sehr große Gefahr aus. Ich schweife nun etwas vom Thema ab und schreibe etwas über die allgemeine Sicherheitssituation. Ist aber trotzdem Interessant!

Stichwort Verschlüsselung: Was war das doch für eine große Enddeckung, als endlich die RSA Verschlüsselung erfunden wurde und einen vollkommen neuartigen Weg in der Verschlüsselung ging. Früher gingen noch ziemlich James Bond mäßig die Geheimagenten mit einem an der Hand geketteten Koffer zu einem Treffpunkt. In diesem Koffer befanden sich nicht etwa geheime Pläne zum Aufenthaltsort aller Spione im anderen Land, nein, dort befand sich nur der Schlüssel (Ent- und Verschlüsselungscode), um diese Pläne wieder in Klartext zu verwandeln. Es handelte sich immer um äußerst starke konventionelle Verschlüsselungen, die aber alle mit bekannt werden des Verschlüsselungsalgorithmus und des Codes leicht wieder entschlüsselt werden konnten. Im zweiten Weltkrieg konnten die Engländer den ENIGMA-Code nur knacken, weil sie das nötige Entschlüsselungsgerät erbeutet hatten (Nebenbei erwähnt: Nach Ende des Zweiten Weltkrieges hatte die US Amerikanische Regierung reihenweise ENIGMA Maschinen nach Afrika verkauft und die Käufer nicht darüber informiert, dass der Entschlüsselungscode bereits bekannt war). Mit der Erfindung des Computers wurde die Entschlüsselung sehr einfach. Dies konnte nur ausgeglichen werden, indem die Verschlüsselungen äußerst kompliziert und die Schlüssel äußerst lang waren. Anders bei RSA. Man denkt sich einfach eine (Prim)Zahl aus, so mit etwa 1 Million Stellen. Das ist der Entschlüsselungscode. Aus dieser Zahl lässt dann recht schnell ein Verschlüsselungscode errechnen, den man öffentlich, sprich für alle frei zugänglich

macht. Der Clou dabei ist, dass man von diesem öffentlichen Code, durch nicht umkehrbare mathematische Funktionen nicht auf den privaten Entschlüsselungscode umrechnen kann. Alle, die einem eine verschlüsselte Nachricht zukommen lassen wollen, verschlüsseln mit dem öffentlichen Schlüssel und nur Du kannst mit deinem privaten Schlüssel entschlüsseln. Aus reiner Menschenliebe erspare ich euch die mir bekannten mathematischen Algorithmen. Die RSA -Verschlüsselung ist ein Mechanismus, der sowie Internet als auch in der beliebten Software „PGP“ angewandt wird. Über mögliche Verschwörungstheorien und andere Vermutungen, dass die US Amerikanische Geheimdienst bereits schnelle Algorithmen zur sicheren Rückrechnung hätte lasse ich mich auch nicht weiter aus. Aber nun zum Kern der Angelegenheit, denn was nützt der längste Schlüssel und die kompliziertesten Algorithmen, wenn der private Code von einem Trojaner ausspioniert wird? Garnichts! Über Echelon möchte ich auch nichts weiter sagen, aber man sollte sehr auf seine eigenen Schlüssel acht geben, obwohl nicht immer deutlich ist, dass welche benutzt werden.

Stichwort Spionage: Sie arbeiten an einem Projekt oder einem Liebesbrief, in dem sie Ihre Liebe zu einem der Netzwerkadministratoren gestehen und wollen sich der Spionage der anderen Netzwerkadministratoren oder anderer Unternehmen erwehren. Sie können dies nun mit einer Verschlüsselungssoftware (z.B. PGP) verschlüsseln, oder begnügen sich im Falle des Liebesbriefes an einen der Netzwerkadministratoren damit die Datei einzuzippen und ein Passwort zu setzten. Während man bei der zip-Datei bei einem sechsstelligem Passwort nur wenige Stunden braucht um das richtige durch Durchprobieren rauszufinden („Brute Force Hacking“) hat man bei einem neunstelligem Passwort mit Sonderzeichen schon mit ein paar Monaten zu rechnen (Mein Tipp: rar Dateien haben eine deutlich stärkere Verschlüsselung und halten dadurch länger stand). Bei einem richtigen Schlüssel ist die Spionage des Passwortes bzw. Schlüssels deutlich leichter als ein Dekodierversuch („Kryptoanalytischer Angriff“). Während man das Passwort zum Liebesbrief sehr leicht mit einem Keylogger, einem Programm, dass alle Tastatureinschläge aufzeichnet und dem Angreifer übermittelt (neuerdings baut man sogar Keylogger in Form von Chips in das Kabel zwischen Tastatur und PC) ausspionieren lässt, ist die Sache mit dem Projekt durch intensives Schnüffeln und Kramen und eventuellem Abhören des Netzwerkverkehrs („Sniffing“) ebenfalls zu lösen. Dies ist nicht alles. Stellen Sie sich vor, sie haben beispielsweise mit „Quicken“ Ihren Steuerrückzahlungsantrag fertiggestellt, in dem sie praktisch alle Ihre Finanzen dargelegt haben und jemand stiehlt Ihr Passwort. Das war noch lange nicht alles!

Stichwort Betrug: Spätestens jetzt wird’s extrem Illegal. Nehmen wir mal an Sie betreiben Homebanking und sind nebenbei noch Mitglied in einigen verschiedenen Clubs. Wenn jemand nun Ihre Passwörter und Schlüssel kennt, kann der Angreifer sich auch Ihre Signaturen beschaffen und sich als Sie Selbst ausgeben („Spoofing“). Er kann denn in Ihrem Namen Überweisungen und Abbuchungen vornehmen und kennt zumindest Ihre Finanzen. Er kann auch Ihre Verdienste bei Paid4Surf angeboten einkassieren. Ebenso ist ein Trojaner die beste Möglichkeit an heißbegehrte gültige Kreditkartennummern und deren Ablaufdaten zu kommen.

Stichwort Mailbox: Ein Angreifer kann mit Hilfe eines Trojaner Ihr Mailboxpasswort rausfinden und alle Ihre Mails lesen. Viele meinen, dass das eh Nichts ausmacht, aber denken sie noch mal was ich in den vorherigen Abschnitten alles geschrieben habe! Man kann erstaunlich viel erfahren, denn nahezu alle Clubs bieten an sich Passwörter erneut zuschicken zu lassen. Ich erwähne extra, dass dabei auch ein mehr oder weniger großer Teil Ihrer Privatsphäre flöten geht und sie eventuell erpressbar sind.

Wie ich schon vorher erwähnt hatte geht von einem Trojaner, der von professioneller Hand (Einen echten Hacker) gelenkt wird eine sehr große Gefahr aus. Allein das Bekannt werden des Mailboxpasswortes ist ein großes Sicherheitsrisiko.
Wenn man merkt, dass man sich mit einem Trojaner infiziert hat sollte man auf jeden Fall SOFORT ALLE, ABSOLUT ALLE Passwörter ändern!

PS: Es gibt immer noch Leute, die für alles ein und das selbe Passwort nutzen und wenn dieses, wie ich es mal erlebt habe, aus einer vierstelligen Zahlenkombination besteht („1429“), die dann reinzufällig noch die Geheimnummer für sein Konto ist, dann kann man sich in ungefähr vorstellen, dass diese Person, nennen wir sie mal „Nils“ mit einem großen Risiko lebt.

Wie bekomme ich einen Trojaner ?

Glücklicherweise ist der einzige Weg sich mit einem Trojaner zu infizieren das Ausführen (Ein normaler Doppelklick!!) des Servers oder eines Scripts, das den Server startet. Trojaner sind ausschließlich ausführbare Dateien mit den Endungen „.com“ und „.exe“ . Scripts, die Trojaner ausführen haben verschiedenste z.B. die Endungen „.vbs“ und „.bat“.
Schreckensmeldungen, dass allein das Lesen einer Mail oder das Surfen zu einer Seite einen Trojaner ins System einschleusen kann zum Glück nicht ganz so schlimm, wenn man mit bedacht surft und seine Software richtig konfiguriert.
Daher ist es auch wichtig, dass sie „Dateiendungen für bekannte Dateitypen ausblenden“ deaktiviert (Anleitung weiter unten) haben, denn ausführbare Dateien (.exe) können sich selbst ein Icon (Bildchen) geben und sehen auf einmal aus, wie Bilddateien. Der Benutzer kann dadurch äußerst schnell getäuscht werden.
Es gibt dabei verschiedenste Tricks andere dazu zu bewegen den Server auszuführen, daher sollten Sie ein natürliches Misstrauen gegen ausführbare Dateien entwickeln. Auch, wenn ein Freund/Freundin versucht Sie eine Datei ausführen zulassen, um sich dann ein paar Scherze zu erlauben, so ist die Gefahr groß, dass ihm die Gelegenheit an sich dazu veranlasst Passwörter oder Dateien zu stehlen oder dass ein ganz anderer Angreifer sich mit dem Server verbindet.
Wenn sie sich nicht bewusst sind, dass sie gerade eine Trojaner ausgeführt haben und sie an einem ungeschützten Computer sitzen, dann ist es tatsächlich zu spät. Der Server schickt er dem Angreifer die IP des Opfers (also Ihre). Port und Passwort kennt der Angreifer ja noch und schon oder sind nicht gesetzt und schon hat er Kontrolle über Ihren Rechner.
Wenn Sie nicht wissen, dass Sie sich mit einem Trojaner infiziert haben, dann wird es Ihnen auch nie auffallen.

Wie erkenne ich einen Angriff ?

Wenn es der Angreifer nicht will ist es an einem ungeschützten System nicht möglich einen Angriff zu erkennen. Sicher gibt es Tricks, die aber viel aufwendiger sind, als sich gleich durch eine Firewall oder ähnliches zu schützen.
Allerdings kann es sein, dass sich der Angreifer einen Fehltritt oder einen Spaß erlaubt. Dies ist die einzige Möglichkeit zu erkennen, dass sich da jemand Zugriff zu ihrem System verschafft hat. Anzeichen sind:

- Ihre Maus macht ungewöhnliche Bewegungen.
- Der PC wird langsamer und hat Traffic, obwohl sie nicht surfen.
- Die Bildschirmeinstellungen verändern sich oder das Bild wird gar gespiegelt
- Applikationen starten oder beenden sich, ohne ihr zutun oder führen nicht angeordnete Funktionen aus
- Merkwürdige Fehlermeldungen erscheinen (z.B. : „Ihr Computer läuft schon seit 13h und 43 m. Microsoft erlaubt nicht, das Windows solange läuft“).
- Der Angreifer interagiert mit ihnen (via Chat oder ähnlichem)

Dies wird auch wichtig, wenn Sie in einem Netzwerk arbeiten und den Admins mal wieder langweilig wird oder sie vermuten, von ihrem Chef oder Lehrer ausspioniert und / oder überwacht werden. Ein versierter Angreifer wird nach seinem Angriff seine Spuren vernichten, sprich Applikationen wieder starten, Logfiles, falls vorhanden löschen und den Trojaner an sich entfernen.
Wenn sie keine Möglichkeit haben ihren PC zu schützen, dann können sie bestehende Verbindungen so erkennen:

Erkennen von bestehenden Verbindungen:
Gehen sie auf „START“ → „Ausführen“ und geben sie dann „command“ ein, um die DOS Konsole zu starten. In dem folgenden Fenster geben sie nun „netstat –a“ ein, um alle aktiven Verbindungen auflisten zu lassen. Dies kann unter umständen eine Weile dauern. Wenn die Liste Länger ist als die Konsole anzeigen kann, dann können sie die Auslistung mit STRG-C (Cancel) abbrechen. Die Ausgabe sieht dann etwa so aus:

```
C:\WINDOWS\Desktop>netstat -a

Aktive Verbindungen

  Proto  Lokale Adresse          Remote-Adresse            Status
  TCP    megaman-iv:1029         MEGAMAN:0                 LISTENING
  TCP    megaman-iv:6174         MEGAMAN:0                 LISTENING
  TCP    megaman-iv:137          MEGAMAN:0                 LISTENING
  TCP    megaman-iv:138          MEGAMAN:0                 LISTENING
  TCP    megaman-iv:1029         205.188.8.180:5190        ESTABLISHED
  TCP    megaman-iv:nbsession    MEGAMAN:0                 LISTENING
  TCP    megaman-iv:1224         imedia5.imedia-online.de:80  CLOSE_WAIT
  UDP    megaman-iv:1195         *:*
  UDP    megaman-iv:nbname       *:*
  UDP    megaman-iv:nbdatagram   *:*
```

Die Ausgabe liest man so:
In der ersten Spalte steht das Protokoll, welches meistens TCP/IP oder UDP ist. In der zweiten Spalte sehen sie Ihren Computernamen und hinter dem Doppelpunkt den lokalen Port. Der Rest ist nicht von Bedeutung.
Jeder Computer stellt 65535 Ports zur Verfügung. Programme verbinden sich meistens über ganz typische Ports mit dem eigenen Rechner. http (normales Internet) läuft über Port 80. FTP über 20 und 21. Und Trojaner verbinden sich auch über für sie typische Ports. Angreifer können den Port aber verändern um nicht zu auffällig zu sein. Wenn der Angreifer allerdings ein Anfänger ist, hat er den Port nicht verändert.
Um zu erkennen, ob es sich um einen Trojaner handelt müssen sie sich den Port anschauen. Generell sind alle komisch aussehenden Ports z.B. 12345 oder 55555 oder 321 verdächtig, denn Trojaner haben ja verstellbare Ports. Eine sehr umfangreiche, aber für den Hausgebrauch zu große Liste finden sie bei Trojaner-Info(Direktlink zur Liste). In der vierten Spalte können sie sehen, ob an dem Port nur gelauscht wird (LISTENING) oder ob schon eine Verbindung besteht (ESTABLISHED). In diesem Fall können sie in der dritten Spalte den Computernamen oder die IP des Anderen ablesen.

Wenn sie an einem durch Firewall oder ähnlich geschütztem PC sitzen, dann wird zumindest der Angriff von bekannten Trojanern erkannt und abgeblockt. Virenscanner, die im Hintergrund laufen können den Start oder das Aktivwerden eines Trojaners (falls bekannt) erkennen, warnen Sie ebenfalls und bieten das entfernen des Trojaners an. Sie sind dann relativ sicher.

Wie schütze ich mich ?

Am besten ist es natürlich sich erst gar keinen Trojaner einzufangen. Schwerer als man denkt, weil sich Trojaner auch sehr gut verstecken können. Der Angreifer kann seinen Trojaner auch an die Installationsdatei der neuesten Moorhuhnversion oder irgendeines anderen interessanten Spiels hängen und schon kann ein Benutzer getäuscht werden.
Was also tun, wenn man erst gar keinen bekommen möchte? Ich habe hier ein paar Vorschläge zusammengestellt, die ebenso gut gegen Viren helfen können:

- Seien Sie misstrauisch : Wenn sie Daten bekommen, gehen Sie immer davon aus, dass sie eventuell verseucht sind und prüfen Sie Disketten vorher.
- Prüfen sie regelmäßig ihren Computer: Vielleicht hat einer Ihrer Kollegen, Geschwister oder Freunde den Computer(unbeabsichtigt oder beabsichtigt) infiziert.
- Erst denken, dann klicken : Führen Sie nie einfach so eine interessant aussehende Datei aus. Nicht ausführbare Dateien können auch mit einem Virus infiziert sein.
- Dateiendungen anzeigen lassen (Anleitung weiter unten): Wenn sie alle Dateiendungen anzeigen lassen, dann erkennen sie auch, wenn ein Trojaner sich z.B. für ein Bild ausgibt (`laracroft_naked.jpg.exe`).
- Auf Dateigrößen achten : Die Server der Trojaner haben charakteristische Größen. Wenn eine Datei genauso groß ist wie einer der Server, dann passen sie auf (Größen siehe Serverliste).
- Nur von offiziellen Quellen downloaden : Laden sie Programme und Dateien nur von offiziellen und vertraulichen Quellen runter. Gerade bei dem Spiel „Moorhuhnjagd“ ist es oft vorgekommen, dass die Installationsdatei mit einem Trojaner „gejoint“ oder mit einem Virus infiziert und zum Download von einer privaten Seite angeboten wurde.
- Installieren sie, falls möglich zwei Virenscanner und bestenfalls auch zwei Firewalls : 100%igen Schutz gibt es nicht, aber doppelt hält bekanntlich besser. Also, wenn ihr Rechner schnell genug ist und genug RAM hat, dann spricht nichts dagegen.

Wer diesen Vorschlägen(!) Folge leistet, der ist relativ sicher und eine regelmäßige Prüfung des eigenen Rechners verhindert, dass Trojaner unbemerkt von anderen Personen ausgeführt werden.

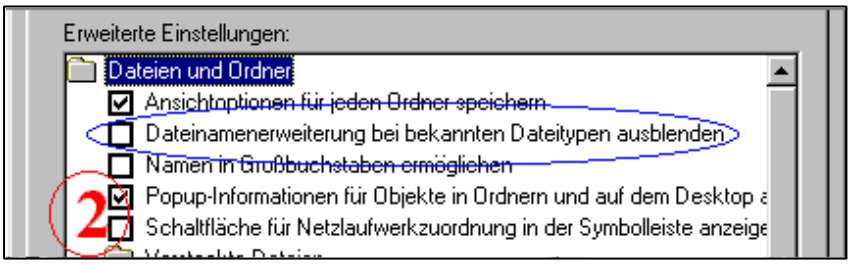
Aber was ist, wenn der Angriff bereits vonstatten geht, oder bereits vorüber ist? Dann lesen Sie dieses Dokument von vorne bis zu dieser Stelle noch mal durch und suchen nach Informationen, was denn ein Trojaner kann.
Aber hier nun die heiß ersehnten Tipps, wenn sie an Ihrem eigenen Computer sitzen und gerade surfen:

- Trennen Sie die Verbindung mit dem Internet, oder schalten sie ihn aus wenn sich in einem Netzwerk befinden (Stecker ziehen und beschweren)!
- Danach sollten sie (möglichst schnell)den Trojaner entfernen
- Dann sollten Sie so schnell wie möglich WIRKLICH ALLE Passwörter ändern. Es sei denn der Trojaner wird von den Admins genutzt, denn denen kann man meistens vertrauen und wenn nicht, dann wissen Sie wer schult hat.

Anders ist die Sache natürlich, wenn sie an einem Multiusersystem sitzen. Ich empfehle daher privates und berufliches (bzw. schulisches) zu trennen und hin und wieder mal die Passwörter zu wechseln.

Wie gesagt, am besten ist es sich erst gar keinen einzufangen.

Anleitung zum anzeigen aller Dateiendungen:
Windows 95: Siehe „Windows 98 SE“
Windows 98 SE: Öffnen Sie den Explorer oder ein beliebiges Fenster. Wählen Sie dann das Menü „Ansicht“ (ALT+A) aus. Wählen Sie dann den Menüpunkt „Ordneroptionen“ (O) aus. Im folgenden Fenster (1) wählen sie die Zweite Kartei „Ansicht“. Nun können Sie verschiedene Einstellungen vornehmen, die sie sich alle mal angucken sollten. Prüfen sie in der zweiten Kartei (2), ob der Menüpunkt „Dateinamenerweiterung bei bekannten Dateitypen ausblenden“ nicht aktiviert ist. Wenn doch, dann entfernen Sie das Häkchen.



Windows XP: Bei Windows XP finden sie die Ordneroptionen im Menüpunkt „Extras“

Nun zur nötigen Software um sich richtig zu schützen:
Ziel ist es eine Softwarezusammenstellung zu finden, die Ihnen maximalen Schutz vor vielen Gefahren bei möglichst geringem Aufwand bietet.
Vorerst noch ein Wort zu Virenscanner. Virenscanner heißen Virenscanner, weil sie Viren finden und nicht weil sie Trojaner finden! Früher war dies ein Problem, da Virenscanner keinen einzigen Trojaner gekannt haben und auch nicht erkannt haben, wenn einer gestartet wurde. Die Lage hat sich etwas zugunsten des Users geändert und die Hersteller von Antivirensoftware haben einige Trojanerdefinitionen mit in ihre Software gepackt. Heute (Jahr 2001) ist es selbstverständlich, dass Virenscanner auch Trojaner finden, aber nochlange nicht alle! Es gibt mindestens 600 Trojaner und nicht zu vergessen die Self-made-Trojaner der vielen Hackergruppen und Jungprogrammierer, die sich immer wieder neue Verfahren zum verstecken und verschlüsseln ihrer Server finden, um sich gegen Firewalls zu wehren. Virenscanner schaffen es einfach nicht.
Jetzt noch was zu Firewalls. Firewalls bieten in der Regel auch einen Schutz der im Hintergrund nach Trojanern sucht, aber die Anzahl der dem Programm bekannten Trojanern ist von Firewall zu Firewall sehr unterschiedlich, sodass man sich nicht darauf verlassen sollte, zudem auch Firewalls das selbe Problem haben wie Virenscanner.
Und nun noch was zu Trojanerscannern. Trojanerscanner haben mit Trojanern das Problem, was Virenscanner mit Viren haben. Ein Trojaner kann den Trojanerscanner manipulieren und sich z.B. aus den Definitionen löschen, sodass er nicht mehr erkannt wird, wobei Trojaner noch mehr Macht haben als Viren.

Also, was tun? Eine Firewall ist das wichtigste. Zwei sind auch nicht schlecht, denn die können sich gegenseitig ergänzen. Firewalls sind im Allgemeinen sehr selbstständig und sie brauchen sich nicht immer um sie zu kümmern. Sie sollten zudem Firewalls auch vor „Nuke“-Attacken schützen lassen. Aus Gründen der Performance können sie das Suchen von Trojanern abschalten und die Firewall nur den Datenverkehr beobachten lassen.
Ein Virenscanner gehört zur Pflichtsoftware schlechthin. Wenn sie gute Virenscanner haben wollen kommen sie kaum darum herum Geld auszugeben. Tests von Virenscanner gibt es immer mal wieder in der „ComputerBILD“, „Chip“, „PC Welt“ und in der „ct“, die in der Regel sehr sorgfältig testen. Virenscanner scannen dann im Hintergrund nach Viren und auch nach einigen (aber nicht allen!) Trojanern. Sie sollten darauf achten, dass diese Funktion auch aktiviert wurde und, falls sie die Funktion aus Performancegründen nicht aktivieren wollen, Sie alle Dateien regelmäßig manuell prüfen.
Ein Trojanerscanner ist nicht immer sinnvoll, aber sollte langsam aber sicher auch zur Sandartausrüstung eines Users gehören. Sie können regelmäßig Ihren Computer

überprüfen oder auch im Hintergrund suchen lassen. Einige können auch Trojaner finden, die sich gut versteckt haben.

Wie bei jeder Software ist es absolut notwendig immer die aktuellen Definitionen zu haben, denn was nützt die teuerste Software, wenn sie veraltet ist. Alle kommerziellen Programme bieten auf deren Homepages die aktuellsten Definitionen zum Download an. Wenn sie Freeware benutzen, dann stellen sie sich darauf ein, dass sie hin und weder die Software wechseln, wenn von einem anderen Programm von ungefähr gleicher oder höherer Qualität eine neue Version rauskommt. Bei Firewalls ist das Problem nicht ganz so groß, aber sie sollten auf keinen Fall veraltete Software einsetzen.

Firewalls

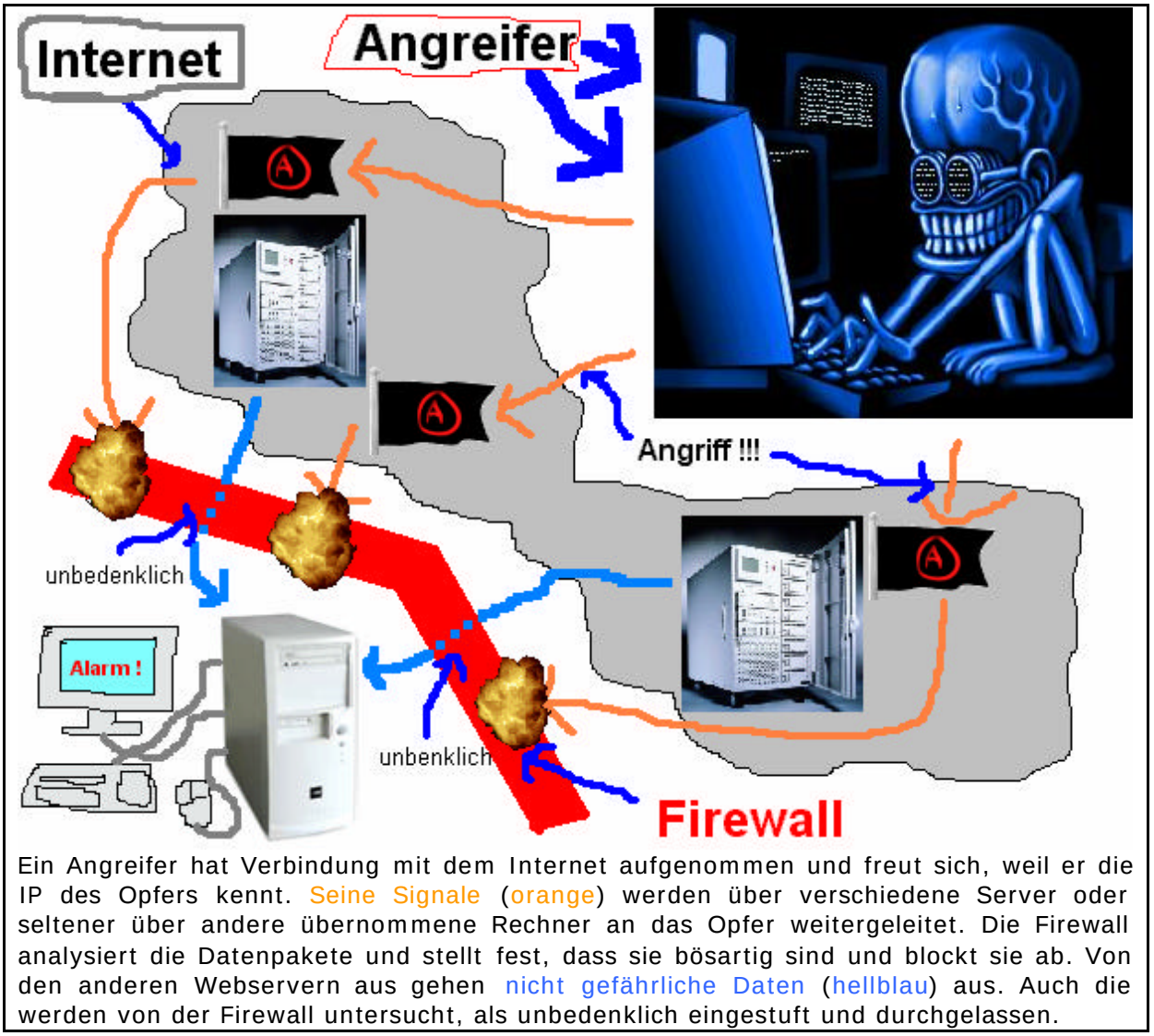
Früher wurden Firewalls im militärischen Bereich eingesetzt, doch mit Fortschreiten der Technik konnten sich auch Banken und Universitäten Firewalls zulegen. Heute ist die Technik so weit entwickelt, dass man keinen extra Rechner als Firewall braucht, sondern die Firewall als Software lokal auf einem Computer installieren kann.
Wenn sie sich im Internet bewegen und keine Firewall haben, dann ist das so, als ob sie in der Nacht nackt durch die Innenstadt gehen. Relativ unbemerkt, aber immer in Gefahr! Firewalls erkennen, wenn auf dem Computer laufende Programme Daten nach draußen schicken, oder ein Angreifer versucht sich mit einem Server eines Trojaners zu verbinden. Dazu schützen sie den PC vor Nuke- und DoS-Attacken. So wird auch die Benutzung von ICQ kein Wagnis mehr. Heutzutage funktionieren viele Programme, die eine Internetverbindung aufbauen (z.B. ICQ oder mIRC u.v.a.) auch trotz einer Firewall und müssen gegebenenfalls noch konfiguriert werden. Es spricht nichts gegen den Einsatz einer Firewall.

Eine Firewall (eng. = Feuerwand) untersucht alle rausgehenden und ankommenden Datenpakete und lässt nur die durch, die in ungefährlich sind oder als unbedenklich eingestuft wurden. Sollte allerdings ein Datenpaket gefährlich sein, dann schlägt die Firewall Alarm. Der Absender wird ermittelt, zurückverfolgt und der Angriff geblockt.
Für alle, die es interessiert gibt es nun eine kleine und sehr zusammengefasste Beschreibung der vier verschiedenen Arten der Datenkontrolle:

1) Paket Filter: Ein Paket Filter untersucht nur alle Datenpakete nach deren Header. Ein Paketfilter ist sehr komfortabel und schnell, allerdings untersucht ein Paket Filter nicht den Inhalt (schützt also nicht vor Cookies), entdeckt keine versteckten Datenströme (welche von Trojanern genutzt werden können) und bietet kaum Möglichkeit einer genauen Protokollierung (was aber eh nur fortgeschrittene User interessant ist). Bei einem Paket Filter gibt es trotzdem viele Möglichkeiten eines Angriffs. Bekannte Sequenzen können aber sicher erkannt werden.
2) Application Level Gateways: Für jede Verbindung wird eine neue Firewall aufgebaut. Wenn ein Programm mit einem anderen Kontakt aufnimmt fungiert die Firewall als Vermittler. Dies bietet insofern mehr Schutz, dass die Firewall nun den Inhalt des Datenstromes untersuchen kann und auch bei bestimmten Verbindungen nach Wahl mehr oder weniger Sicherheitsbestimmungen gibt. Auf anderen Protokollebenen können Angriffe nicht erkannt werden.
3) Lokale Paket Filter und Application Level Gateways auf einem Rechner: Die Kombination beider Techniken schein am sinnvollsten zu sein. Bietet aber für den Normalanwender vernachlässigbare aber im Netzwerk wichtige Sicherheitsrisiken.
4) Statefull Inspection Filter: Auf der Basis der Paket Filter wurden Statefull Inspection Filter entwickelt, die, grob gesagt, in der Lage sind sich die Zusammenhänge zwischen einzelnen Datenpaketen zu merken. Zudem wird auch für jeden Datenstrom ein eigener Überwachungsprozess gestartet. Das Verfahren benötigt keine aufwendige Konfiguration und ist ordentlich schnell.

(Quelle: E-Book von Thomas Veit auf der Cebit 2000)

Wie eine Firewall in ungefähr arbeitet lässt sich im folgenden hochwissenschaftlichen Schaubild erkennen:



Ein Angreifer hat Verbindung mit dem Internet aufgenommen und freut sich, weil er die IP des Opfers kennt. Seine Signale (orange) werden über verschiedene Server oder seltener über andere übernommene Rechner an das Opfer weitergeleitet. Die Firewall analysiert die Datenpakete und stellt fest, dass sie bösartig sind und blockt sie ab. Von den anderen Webservern aus gehen nicht gefährliche Daten (hellblau) aus. Auch die werden von der Firewall untersucht, als unbedenklich eingestuft und durchgelassen.

Nun dürfte die Funktionsweise einer Firewall deutlich sein ;)

Andere Software

Firewalls, Viren- und Trojanerscanner sind nicht die einzige Software, die man gegen Trojaner einsetzen kann. Einige Programme sind speziell für den Einsatz gegen Trojaner programmiert. Darunter befinden sich Fakeserver und Programme gegen einzelne Trojaner.

Fakeserver: Fakeserver sind gerade für fortgeschrittene Benutzer interessant. Sie werden vom Benutzer absichtlich gestartet und geben sich als echte Trojaner aus (Fake = Fälschung). Wenn sich ein Angreifer nun mit dem Fakeserver verbindet, wird ihm ein echter Server vorgetäuscht. Das „Opfer“ kann entscheiden, welche Informationen der Angreifer bekommt.
Software gegen bestimmte Trojaner: Diese Programme sind gegen bestimmte Trojaner. Wenn man also weiß, welchen man sich eingefangen hat, kann man ihn damit entfernen lassen. Der Vorteil dieser Software ist, dass sie sehr klein ist und also leicht per E-Mail

oder Diskette in andere Systeme (Büro, Schule) eingeschleust und aufbewahrt werden kann.

Fakeserver sind gerade dann nützlich, wenn man soeben über ICQ o.ä. eine verdächtige Datei zugeschickt bekommen hat. Auch auf einer Netzwerksession gibt es immer Leute die alle Rechner nach Trojanern scannen. Wenn man also weiß, dass sich in Kürze ein Angreifer versucht zu hacken, dann kann es äußerst amüsant sein, wenn man ihm mit dem Fakeserver einen 1,4 GHz Rechner, mit 86 GB Platte und 512 MB RAM vorgaukelt und ihm statt alle gespeicherten Passwörter nur „Fuck You“ (schwer zu übersetzten, aber das heißt soviel wie: „Verzieh dich du Landstreicher!“) sendet. Wenn der Angreifer auf die Idee kommt mal zu gucken, was denn auf dem Bildschirm so im Gange ist, werden dem Angreifer nur vorgefertigte Bilder gesendet, die ihm weiß machen man hätte schon Kontakt mit seinem Provider und mit der Polizei aufgenommen. Leider sind Fakeserver selten und auch nicht für alle Trojaner verfügbar. WARNUNG: Gerade bei Fakeservern kann man sich nicht sicher sein, ob sie selbst gutartig sind und nicht ein Trojaner des Programmierers sind. Vertraue nie einer Software, die du nicht selbst programmiert hast!! Diese Art von Software bietet keinerlei Schutz und ist auch eher zum Spaß da.
Software gegen einzelne Trojaner gibt es auch nicht für alle Trojaner, doch kann man sich da schon sicherer sein. Diese Programme gibt es meistens für die bekanntesten und am einfachsten zu bedienenden Trojaner, da die sehr weit verbreitet sind und von Anfängern genutzt werden können. Auch erfahrene Administratoren setzten diese der Einfachheit wegen ein, um ihr System zu überwachen (beliebt ist zum Beispiel Back Orifice). Wenn also der Server bekannt ist und man keinen Bock hat ausspioniert, überwacht oder geärgert zu werden, dann kann man sich ein Programm gegen diesen Trojaner besorgen und den Trojaner regelmäßig entfernen. Aufgrund des geringen Verbrauchs von Speicherplatz lässt er sich leicht per Diskette oder E-Mail überall hin mitnehmen und speichern.
Tests werden folgen.

Windows XP Firewall

Tut mir leid euch berichten zu müssen, dass die Firewall von MS Windows XP überhaupt nichts wert ist und keinen Schutz vor Trojanern bietet und schon lange nicht verhindert, dass XP nach Hause telefoniert. Die Firewall behindert sie bloß beim Betrieb eines FTP Servers oder Filesharing Programmen. Schaltet diese Also ab!

Warentest : Firewalls

In meinem Test über Firewall beschränke ich mich auf die am häufigst gekauften und beliebtesten Firewalls. Dabei berufe ich meine technischen Informationen aus PC Zeitschriften, die ich in den Quellen erwähne. Die Reihenfolge der getesteten Software steht nicht im direkten Zusammenhang mit deren Platzierung!
Leider bot keine der Zeitschriften eine Angabe über die Testmethoden und Bewertungskriterien.

Norton Personal Firewall 2001.
Wie man am Namen unschwer erkennen kann ist diese Firewall schon seit letztem Jahr erhältlich, aber die Updatefunktion sorgt dafür, dass das Produkt auf dem Allerneuesten Stand gebracht wird. Diese Firewall ist die am meisten gekaufte.
Mein Urteil ist:
Die Installation der Firewall verlief problemlos und es konnten Firewall Regeln eingestellt werden. Die Firewall blockt alles Unerwünschte ab und beschränkt den Zugriff von ActiveX Controls und Applets. Nach Wunsch können auch Cookies geblockt werden. Wenn ein Programm versucht ohne vordefinierte Regeln Daten zu übertragen wird ein leicht zu

bedienender Assistent gestartet. Die Filterregeln für die Firewall sind individuell konfigurierbar.
Online-Updates: Ein Jahr kostenlos per Internet.
Preis: ca. 100 Mark (unv. Preisempfehlung)
Info: www.symantec.de

Persönlicher Kommentar:
Die Firma Norton ist für qualitativ Hochwertige Produkte bekannt, also spricht alle mal der etwas hohe Preis dagegen dieses Programm oder einen seiner Nachfolger zu erwerben. Die 2000 Version könnten sie als Schnäppchen bekommen

Norton Personal Firewall 2002.

Das ist die aktuelle Version von Norton Personal Firewall. Diese Firewall ist die am meisten gekaufte.
Mein Urteil ist:
Die Installation der Firewall verlief problemlos. Das Setup ist etwas langwierig, aber erfahrene Anwender haben die Konfiguration schnell gemacht. Die Firewallregeln können wieder individuell eingestellt werden, was aber wesentlich unintuitiver ausfällt als bei der Version 2001. Die Firewall blockt wieder alles Unerwünschte ab und beschränkt den Zugriff von ActiveX Controls und Applets. Nach Wunsch können auch Cookies geblockt werden. Wenn ein Programm versucht ohne vordefinierte Regeln Daten zu übertragen wird ein Assistent ein Assistent gestartet, der umständlicher ist als bei der Version 2001. Die Filterregeln für die Firewall sind individuell konfigurierbar.
Online-Updates: Ein Jahr kostenlos per Internet.
Preis: ca. 100 Mark
Info: www.symantec.de

Persönlicher Kommentar:
Die Firewall ist zuverlässig, doch die Bedienung ist irgendwie viel schlimmer geworden. Ich empfehle jedem sich die Version 2001 zuzulegen, und das Update zu nutzen solange es geht.

ZoneLabs Zone Alarm: (getestet 2001)

Eine gute und leicht zu bedienende und kostenlose Firewall.
Die Zeitschrift Chip urteilte wie folgt (sinngemäß zusammengefasst):
Das Sicherheit nicht teuer sein muss, zeigt ZoneAlarm von der Firma Zone Labs. Das Programm gibt es für Privatanwender kostenlos auf der Webseite und neben dieser Version auch eine mit 20 US$ zu Buche schlagende erweiterte Version.
Nach dem Start aktiviert die Software dann eine Grundkonfiguration für den Schutz der Daten. Bei den Einstellungen unterscheidet sie zwischen dem lokalen Netzwerk und dem Internet. Ein Schieberegler bestimmt, welche Zugriffe aus dem jeweiligen Netz zulässig sind. Das Programm bietet als einziger die Möglichkeit den Zugang zum Internet nach voreingestellten Zeiten zu blockieren oder wenn der Bildschirmschoner aktiv ist. Wenn ein Programm auf das Internet zugreifen will erscheint ein Dialogfeld, dessen Einstellungen gespeichert werden. Den Testangriff erkante die Software und werte ihn gut ab. Alles in Allem fehlt der Software allerdings viele Einstellungsmöglichkeiten.
Platz: Platz zwei und Preis/Leistungssieger bei Chip
Preis: Für Privatanwender kostenlos. Erweiterte Version für 20 US $
Info: www.zonealarm.de
Quelle: www.chip.de (direkter Link zum Test hier)

Persönlicher Kommentar:
ZoneAlarm bietet einen anständigen Grundschutz für Neulinge, dürfte aber für anspruchsvollere Benutzer eher weniger interessant sein. Ich habe schon viel gutes, aber

hin und wieder auch schlechtes über dieses Programm gehört, aber der Preis von 0 DM dürfte die meisten User wohl zum „kauf“ bewegen. Urteilt selbst.

Network Associates McAfee Firewall: (getestet 2001)

Die Zeitschrift Chip urteilte wie folgt (sinngemäß zusammengefasst):
Die Firewall fragt nach der Installation nach einem Sicherheitslevel und startet dann die Firewall. Die Firewall erkennt, wenn beliebige Programme auf das Internet zugreifen wollen und fragt den Benutzer. Laut Chip soll diese Firewall über eine gute Technik verfügen und einen sehr guten Paketfilter verfügen der leider nicht frei konfigurierbar ist. Die Firewall soll für viele Netzwerkinterfaces Optionen zur Verfügung stellen. Allerdings bietet die Firewall keinen Schutz vor Cookies. Updates werden via Internet kostenlos und nur für registrierte Benutzer zu Verfügung stehen.
Preis: 30 US $
Info: www.mcafee-at-home.com
Direktlink: Test von Chip

Persönlicher Kommentar:
Diese Software scheint wohl für fortgeschrittene Anwender eine echte Alternative zu Norton Personal Firewall zu sein und ist mit einem Preis von 30 US$ auch billiger.

Kurztests (von Chip ausführlich getestet) (2001)

PGP Desktop Security 7.0

Diese Firewall bietet laut Chip ein reichhaltiges Angebot an Funktionen und dürfte mit einem stolzen Preis von 130 US $ für Privatpersonen eher weniger in Frage kommen. Profis wird allerdings ein sehr guter und frei konfigurierbarer Schutz geboten.
Direktlink zum Test von Chip

Norman Personal Firewall

Diese Firewall erwähne ich nur, da sie leicht mit der von “Norton” zu verwechseln ist. Diese Software hier bietet laut Chip nur einen eingeschränkten Schutz und sei umständlich zu bedienen. Laut PC Welt würde die Software stark an Norton Personal Firewall erinnern. Zudem soll sie als Zusatz auch einen Werbeblocker enthalten.
Direktlink zum Test von Chip

Nicht erwähnte, aber von Chip getestete Firewalls

Sandbox Security Secure 4U

Direktlink zum Test von Chip

Aladdin e Save Desktop 3.0

Direktlink zum Test von Chip

Fazit:
Firewalls gibt’s viele und für Privatanwender gibt es schon gute Produkte. Norton Personal Firewall 2000 und McAfee Firewall sind wohl gute Firewalls für den Hausgebrauch und wer kein Geld ausgeben möchte oder wem die Software zu teuer ist, der hat mit Zone Alarm ebenfalls eine gute Firewall auf der Platte. Die anderen Firewalls kommen teilweise auch als Paket mit einem (nicht getesteten) Virenscanner und können unter Umständen auch lohnend sein. Ich empfehle da mal die Testberichte zu lesen.
In dem von Chip durchgeführten Test vermisste ich allerdings die Firewall Lockdown 2000 (v 7.0). Ich habe auch schon viel Schlechtes über die Firewall gehört, sodass ich diese wohl nicht mehr einsetzten werde.

Hinweis: Symantec bietet an eine Sicherheitscheck vom Internet aus durchzuführen, um zu prüfen, wie sicher ihr Rechner ist.
Der Check ist unter: http://security1.norton.com/ssc/ zu finden. Lassen sie während des Testes alle ActiveX Steuerelemente usw. zu.

Warentest : Trojanerscanner

Die Trojanerscanner bieten einen unfassenden und leicht zu bedienenden Schutz vor Trojanern. Gerade auf einer Netzwerksession ist es ratsam mit solch einem Programm alles zu scannen, was die anderen haben, denn mitunter kann das recht viel sein. Wie bei Virenscannern sollte man sich auch bei Trojanerscannern immer aktuelle Trojanerdefinitionen besorgen, damit man auch gegen die neuesten Trojaner (bzw. Viren) geschützt ist.
Nun gibt es ein paar Softwaretests zu den Trojanerscanner, welche sich, wie der Name schon sagt auf Trojaner spezialisiert haben. Die Software, die hier aufgeführt ist habe ich selbst getestet. Ein paar Informationen habe ich von den Herstellerseiten und aus den Programmen selbst entnommen.

Anti Trojan 4.0.98

Dieses Programm ist von Februar 2000 und mittlerweile veraltet. Er ist optisch ganz gut und erkennt (nur) 93 Trojaner. Die Suche ist auch nicht unbedingt schnell, aber erträglich. Dazu kann der Scanner die Festplatte nach verdächtigen Dateien durchsuchen. Der Grund, warum ich das Programm erwähne ist, dass diese Version noch Freeware ist. Alle Neueren (ab 5.0) sind Shareware.
Hersteller: http://www.anti-trojan.net (kein Download mehr)
Download: <keiner>

Anti Trojan 5.5.337

Die aktuellste Version von Anti Trojan (eventuell muss von der Downloadversion ein update durchgeführt werden) erkennt etwa 6937 Trojaner ist ist seinem Freewarevorgänger weit überlegen. Er bietet verschiedene Suchoptionen, die insgesamt recht schnell ablaufen. Im Test erkannte die Software auch die neuesten Versionen von verschiedenen und auch seltenen Trojanern, bietet dazu noch das suchen nach offenen Ports (und findet zum Beispiel den ICQ Port) und deren Schließung. Im test stürzte die Software stellenweise aber nie während der Suche ab. Einen Trojanerwächter, der im Hintergrund lauscht gibt es inklusive und ein Update kann bequem online und ohne Neustart durchgeführt werden.
Hersteller: www.anti-trojan.net
Preis: Shareware (14 Tage) und danach 25 € (Euro)
Download: Von der Herstellerseite und ohne Registrierung

Trojan Check 5.0 final

TrojanCheck ist ein Programm, dass sich eher an fortgeschrittene User richtet. Nach eigenen Aussagen ist das Programm darauf spezialisiert den Start eines Trojaners zu verhindern. Dies geschieht, indem dem Benutzer sehr leicht alle Registry und Win.ini Einträge gezeigt werden. Die Suchoptionen sind eher umständlich über den Menüpunkt „Extras“ und „Suchen nach“ zu erreichen, sind aber angenehm schnell. Updates sind ebenfalls online möglich. Im großen und ganzen macht die Software einen professionellen Eindruck. Auf jeden Fall mal antesten.

Hersteller: www.TrojanCheck.de
Preis: Für Privatpersonen kostenlos
Download: Von der Herstellerseite und ohne Registrierung

Fazit:
Diese drei Produkte sind die einzigen, die ich bisher ohne großen Aufwand ausfindig machen konnte. Anti Trojan 4.0 ist viel zu veraltet, um noch nützlich zu sein. Anti Trojan 5.5 ist zwar mit einem preis von 25 € (Euro) für meinen Geschmack ziemlich teuer, kann aber auch die meisten Trojaner erkennen und ist sehr einfach zu bedienen. Trojan Check würde ich jedem etwas fortgeschrittenen User wärmstens ans Herz legen. Die Hilfe von TrojanCheck bietet zum Glück reichliche Informationen für Anfänger. Man muss sie nur lesen. Weitere Tests werden folgen.

Rache ist süß (abuse@provider.de)

Es hat also gerade jemand versucht sich mit ihnen zu verbinden, hat aber Dank Firewall und einem aufmerksamen Auge keinen Erfolg gehabt. Was nun? Den Angreifer einfach ziehen lassen? Vielleicht! Vielleicht aber auch nicht!

Ich gehen davon aus, dass soeben eine Firewall per Alarmsignal aus den langweiligen Computeralltag gerissen hat und brav die IP des Angreifers liefert. Nun haben wir also die IP. Schön!
Hinweis für alle blutigen Anfänger unter euch: Leider gibt es keine Methode von der IP einer Person auf die E-Mailadresse zu schließen, denn das ist technisch unmöglich! Leider kenne ich auch keine Möglichkeit anhand der IP herauszufinden, ob der Angreifer ICQ hat, um ihn eventuell über ICQ anzuscheißen.
Theoretisch reicht es schon die IP des Angreifers zu kennen. Praktisch wäre es noch den Rechnernamen (Hostname), der ihm von seinem Provider zugewiesen wurde zu kennen. In der Regel liefern Firewalls über die eingebaute trace-Funktion auch den Rechnernamen. Wenn sie das nicht tut (z.B. Lockdown), sollten sie eine andere nehmen. Andernfalls ist es ein kleines bisschen komplizierter. Nun üben wir also Rache und zwar auf völlig legalem Wege. Wir beschweren uns einfach bei seinem Provider, denn mit seinem Handeln, hat er bestimmt gegen die AGB (**A**llgemeine **G**eschäfts**b**edingung) verstoßen, denn kein Provider kann und darf so ein Treiben dulden. Jeder Provider ist dazu verpflichtet für einen Zeitraum von 60 bis 80 Tagen zu speichern, welcher Kunde wann mit welcher IP online war.
Ich gehe mal davon aus, dass der Rechnername (Hostname) des Angreifers bekannt ist. Er könnte beispielsweise so aussehen:
pd9552e69.dip.t-dailin.net
Dieser Name repräsentiert den Computer, der die Daten aus dem Internet durch die Telefonleitung zum Rechner des Surfers (in diesem Falle den des Angreifers). Dieser Rechner gehört seinem Provider. Aber zu welchem Provider gehört dieser Rechner? Dies lässt sich an der Endung des Namen erkennen. In diesem Falle „t-dailin.net“. Das richt schon förmlich nach T-Online. Beschweren wir uns also bei T-Online, indem wir eine E-Mail an abuse@t-online.de schicken (Musterbrief folgt später). Alle Provider haben charakteristische Endungen (Suffix) in den Hostnamen an denen sie sich eindeutig identifizieren lassen.
Falls sie nicht über den Hostnamen verfügen, können sie seinen Provider auch an der IP Adresse erkennen. Alle Provider haben einen bestimmten IP Bereich. Dieser Bereich wird von den Computern des Providers besetzt und ist immer gleich.

Um herauszufinden zu welchem Provider oder Server eine IP gehört können sie den Dienst „ripe.net“ verwenden.
Dieser Dienst steht unter: http://www.ripe.net/perl/whois kostenlos zur Verfügung und spuckt nach Eingabe einer IP alle wichtigen Daten aus (testen sie mal ihre Eigene IP!)

Meist erhält man mehrere Einträge, aber ein Blick auf die Einträge „descr:“ und „Adress:“ verrät ihnen wer der richtige ist. Irgendwo (meistens bei „remarks“ oder „notify“) ist noch eine Information an wen im Falle eines Hackangriffes o. ä. Eine Beschwerdewail geschickt werden soll.

Nur so nebenbei mal gesagt:

132.96.x.x	DOD Network Information Center, The Pentagon, Washington, DC 20310

Nachdem wir also seine Provider kennen, können wir uns nun Beschweren, da der Provider ja abgespeichert hat, wer mit dieser IP gerade online ist oder war. Nun folgt eine Liste mit allem, was in dieser Mail drinstehen sollte:

- Formale Anrede („Sehr geehrte Damen und Herren“)
- Sachliche Beschreibung des Tatbestandes inklusive Datum und Zeit des Angriffs
- Ganz kurze Erklärung, woher Sie wissen, dass es deren Kunde war.
- Komplette (!) Logfile der Firewall (wirklich wichtig)

Das sollte drinstehen. In der Praxis könnte das z.B. so aussehen:
(Das ist mein erste Beschwerdebrief, den ich abgeschickt habe, als ich noch „Lockdown“ hatte)

```
Sehr geehrte Damen und Herren

Hiermit möchte ich Sie darauf aufmerksam machen, dass einer Ihrer Kunden
versucht hat sich mittels des Trojanischen Pferdes „NetBus“ unerlaubt
Zugang zu meinem Computer zu verschaffen. Ich bitte Sie dafür zu sorgen,
dass dies nicht mehr passiert.

Datum : 04.03.2001
Zeit  : 20:40 MEZ
IP    : 217.85.46.105

Mittels der Software „Neo Trace Pro“ ermittelte ich seinen Hostname und Sie
als seinen Provider.

-- Auszug aus der Logfile --
** LockDown 2000 v7.0.0.1 initialized at Mo, Jun 4, 2001, at 09:47 AM (MEZ)
Mitteleuropäische Zeit **
:: Trojan network connectivity check enabled.
:: Auto Trojan scan has been disabled.
:: Nuke protection enabled.
:: ICQ Nuke protection enabled.
[04.06.01 20:40:46] Incoming hack attempt from IP Address: 217.85.46.105
[04.06.01 20:40:46] Hacker is attempting to gain access using the Netbus
trojan on port 12345.
[04.06.01 20:40:46] Hacker's connection was terminated by Lockdown 2000.
[04.06.01 20:40:46] Log auto-saved to: 06042001.LOG
-- Ende des Auszuges --
```

Man bekommt in den meisten Fällen zwar eine Standartantwort, aber ich kenne Leute, die schon mal von ihrem Provider abgemahnt. Eine solche Beschwerde bringt keinen Angreifer in echte Schwierigkeiten, doch sollten sich die Beschwerden häufen, oder ein Opfer mit einer Klage drohen gibt’s schon mal ne Verwarnung und im schlimmsten Fall eine Vertragskündigung. Ich spreche da aus Erfahrung. Also, wenn man es nicht übertreibt, kann man durchaus Spaß dabei empfinden.

Nachwort

Ich bin nun nach einigen Wochen der Recherche und Schreiberei glücklich euch diese Dokumentation bieten zu können. Wie ihr alle sehen könnt habe ich wohl ziemlich viel geschrieben. Mehr als ich gedacht habe. Ich hoffe, dass dieses Dokument seinen Zweck erfüllt, nicht langweilig ist und auch nicht schwergängig zu lesen ist. Man berichtete mir meine Texte seien weniger flüssig zu lesen. Nächstes Jahr kommt noch eine Version und die wird noch umfangreicher.