4.5 Spione im Hintergrund: Trojanische Pferde

Nachdem sich inzwischen fast jeder der Gefahr durch Viren bewusst ist, taucht vermehrt eine neue Bedrohung in den Netzwerken auf, die oft eine noch größere Gefahr darstellt. Trojanische Pferde – kurz als Trojaner bezeichnet – sind eine besondere Form von Eindringlingen. Sie haben meist keine zerstörerische Absicht, sondern sind darauf aus, vertrauliche Informationen auszuspähen. Dazu nisten sie sich ähnlich wie Viren auf Rechnern ein und spionieren versteckt im Hintergrund. So können Sie beispielsweise wichtige Dateien auslesen oder manipulieren oder etwa die Tastendrücke der Benutzer protokollieren, um Passwörter auszuspähen.

INFO

Was heißt eigentlich Trojanisches Pferd?

Die Bezeichnung „Trojanisches Pferd" geht auf die Sage vom Kampf um die antike griechische Stadt Troja zurück, die schließlich durch eine List erobert wurde: Die Belagerer schenkten den Trojanern ein riesiges hölzernes Pferd als „Versöhnungsgeschenk". Die Bewohner zogen es in die Stadt und feierten den vermeintlichen Sieg. Im Holzpferd hatten sich aber Soldaten versteckt, die im Schutz der Dunkelheit herauskamen und die Stadttore öffneten, um ihre Kameraden einzulassen. Gemeinsam besiegte man die vom Fest berauschten Bewohner mit Leichtigkeit. Von dieser Legende leitet sich bis heute der Name für eine List ab, mit der man sich unerlaubt Zugang verschaffen kann.

Workshop: PC-Fernsteuerung mit einem Trojaner

Von Trojanern ist in letzter Zeit viel die Rede. Dabei heißt es immer, dass Trojaner gefährlich seien, weil sie einen infiltrierten PC ausspionieren und fernsteuern könnten. Die Erfahrung zeigt aber, dass viele Benutzer nur eine sehr ungenaue Vorstellung davon haben, was ein Trojaner tatsächlich genau anstellen kann. Deshalb wird die Gefahr von vielen nicht wirklich ernst genommen. Damit Sie sich selbst ein Bild davon machen können, was mit einem Trojaner alles möglich ist, wollen wir Ihnen in diesem Workshop ein solches Programm vorstellen. Wir benutzen dazu das Produkt NetBus Pro. Es ist insofern bemerkenswert, als es ursprünglich als Trojaner entstanden ist, sich inzwischen aber zu einem professionellen Fernwartungstool entwickelt hat. Dies zeigt mal wieder, wie schmal der Grat zwischen hilfreichen und gefährlichen Programmen ist. Es hängt immer davon ab, wer sie bedient.

NetBus: Ein „gereifter" Trojaner

NetBus besteht aus zwei Komponenten. Das eine ist der Server, ein Modul, das auf dem angegriffenen Rechner installiert werden muss. Dieser Server läuft dort im Hintergrund, nimmt die Befehle des Angreifers entgegen und führt sie aus. Die andere Komponente ist der Client, das Programm, das der Angreifer auf seinem PC benutzt, um mit dem Server auf einem anderen Rechner zu kommuni-

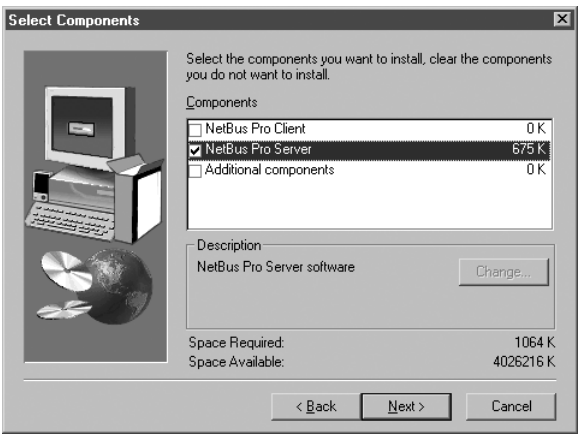
zieren. Zur Kommunikation zwischen den beiden Modulen auf unterschiedlichen Rechnern wird das TCP/IP-Protokoll eingesetzt. Sobald also beide Rechner mit dem Internet verbunden oder Teil eines lokalen Netzwerks mit TCP/IP-Unterstützung sind, ist eine Fernsteuerung möglich.

Das folgende Beispiel können Sie selbstverständlich auch selbst nachvollziehen. NetBus Pro steht unter *http://www.netbus.org* in einer Testversion zum Download zur Verfügung. Darüber hinaus benötigen Sie zwei PCs. Einer simuliert den angegriffenen Rechner, vom anderen aus erfolgt der Angriff. Beide PCs müssen vernetzt sein. Am einfachsten geht es, wenn Sie selbst über ein kleines Windows-Netzwerk verfügen, das das TCP/IP-Protokoll unterstützt. Alternativ können Sie auch zwei PCs verwenden, die sich beide ins Internet einwählen. Selbst wenn Sie selbst nur einen PC haben, können Sie sich für diesen Test mit einem Bekannten zusammentun und NetBus auf dessen PC installieren. Sie müssen dann nur beide zur gleichen Zeit ins Internet eingewählt sein und einige Funktionen werden relativ langsam ablaufen.

Ganz wichtig: Wenn Sie den Test mit NetBus selbst ausprobieren, müssen Sie darauf achten, den Server anschließend wieder zu deaktivieren oder besser ganz zu deinstallieren. Andernfalls kann jeder andere NetBus-Benutzer Zugriff auf Ihren PC erlangen, wenn dieser mit dem Internet verbunden ist.

NetBus installieren und konfigurieren

1. Zunächst muss NetBus auf beiden Rechnern installiert werden. Dabei reicht es, wenn Sie den Installations-Assistenten auf einem (dem angegriffenen) PC nur den *NetBus Pro Server* und auf dem anderen nur den *NetBus Pro Client* aufspielen lassen.

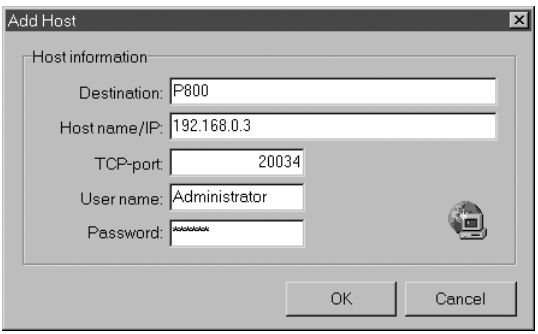


Auf einem PC wird der Server, auf dem anderen der Client installiert

2. Anschließend muss der Server aktiviert werden. Aus Sicherheitsgründen ist er nach der Installation zunächst nicht aktiv. Starten Sie dazu auf dem potenziellen Zielrechner mit *Start/Programme/NetBus Pro/NetBus Server* den Server und öffnen Sie mit einem Klick auf *Settings* die Einstellungen. Hier aktivieren Sie in der Kategorie *General* die Option *Accept connections*. Aus Sicherheitsgründen sollten Sie außerdem unbedingt ein Passwort eingeben, damit wirklich niemand außer Ihnen den Fernwartungszugang benutzen kann.

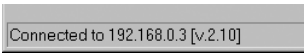
Aktivieren Sie den NetBus-Server auf dem Zielrechner

3. Damit ist der Zielrechner für den simulierten Angriff vorbereitet. Nun können Sie zum Angriffsrechner wechseln und dort mit *Start/Programme/Net Bus Pro/NetBus* den Client starten. Hier sollten Sie zunächst mit *Host/New* eine Verbindung zum Zielrechner anlegen. Geben Sie dazu im nachfolgenden Menü einen Namen für die Verbindung (Destination) sowie die IP-Nummer des Zielrechners, auf dem der Server läuft, an. Wenn Sie den Server mit einem Passwort konfiguriert haben, sollten Sie dieses hier ebenfalls im entsprechenden Feld angeben.



Erstellen Sie zunächst eine Verbindung für den Zielrechner

4. Daraufhin wird der neue Eintrag in der Liste der potenziellen Ziele im Hauptfenster geführt. Wenn Sie diesen markieren und *Host/Connect* aufrufen, wird die Verbindung zum Server hergestellt. Die Bestätigung dafür finden Sie in der Statuszeile unten im Hauptfenster, wo nach kurzer Zeit die Meldung *Connected to ...* angezeigt werden sollte.

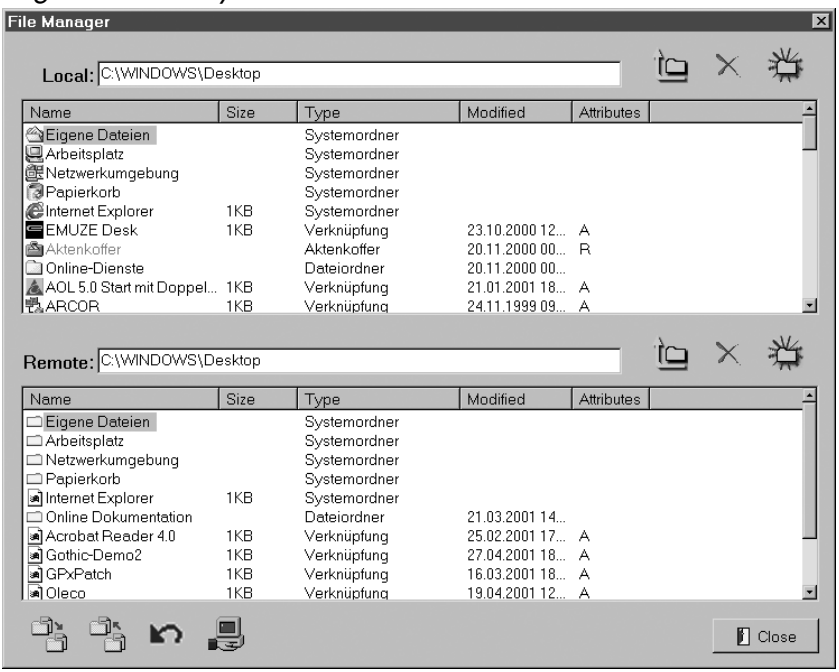


Die Verbindung zum Server-Modul ist hergestellt und der Spaß kann beginnen

Fernsteuerung mit NetBus

Nachdem die Verbindung zum NetBus-Server auf dem anderen PC hergestellt ist, können Sie sich an das Austesten der Zugriffsmöglichkeiten machen. Sie befinden sich alle im vollgepackten *Control*-Menü des NetBus-Clients. Alle Funktionen können wir hier aus Platzgründen nicht vorstellen. Deshalb beschränken wir uns auf einige besonders interessante, die hoffentlich die Gefahr gut verdeutlichen, die von diesem Trojaner ausgeht.

Zugriff aufs Dateisystem



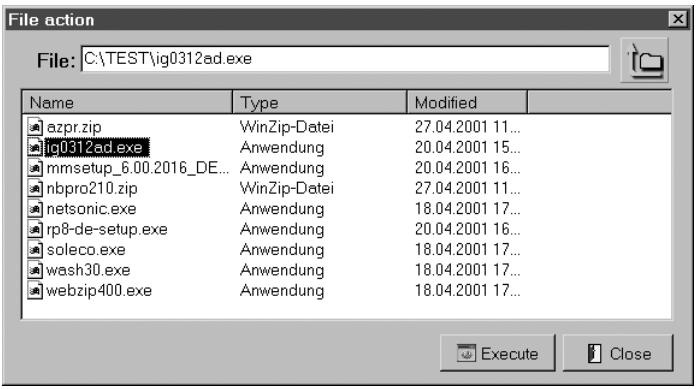
Mit dem File-Manager erlangen Sie vollen Zugriff auf die Dateien des Zielrechners

Eine der mächtigsten Funktionen von NetBus verbirgt sich unter *Control/Filemanager*. Damit öffnen Sie einen Dateimanager, der aber nicht nur den Dateibestand Ihres eigenen PCs, sondern auch den des anderen anzeigt und ganz komfortabel bearbeiten lässt. Oben sehen Sie unter *Local* Ihren eigenen Rechner, unten wird unter *Remote* der Zielrechner angezeigt. Wie Sie feststellen werden, haben Sie auf beide Dateisysteme vollen Zugriff, d. h., Sie können sämtliche Ordner durchsuchen und auf alle Dateien zugreifen. Auch das Löschen einzelner oder mehrerer Dateien oder Ordner ist möglich. Dazu brauchen Sie die Kandidaten nur zu markieren und auf die Schaltfläche *Delete file/folder* für das jeweilige Dateisystem zu klicken.

Sehr interessant sind außerdem die Symbole ganz unten links im File-Manager. Damit können Sie Dateien vom oberen (Angriffs-)Rechner auf den unteren (Ziel-)Rechner übertragen und umgekehrt. So kann man wichtige Dokumente unbemerkt vom Zielrechner kopieren oder eigene Programme dort installieren.

Programme ausführen

Auch das Ausführen von beliebigen Programmen ist mit NetBus ein Kinderspiel. Besonders in Verbindung mit dem File-Manager kann man sehr effektiv vorgehen, indem man mit diesem zunächst ein eigenes Programm auf den Zielrechner überträgt und es dann dort ausführt. Um ein Programm auf dem Zielrechner auszuführen, rufen Sie einfach die Menüfunktion *Control/File actions/Execute file* auf. Damit öffnen Sie einen Dateiauswahldialog auf dem Zielrechner, in dem Sie das auszuführende Programm angeben und mit einem Klick auf *Execute* starten lassen.



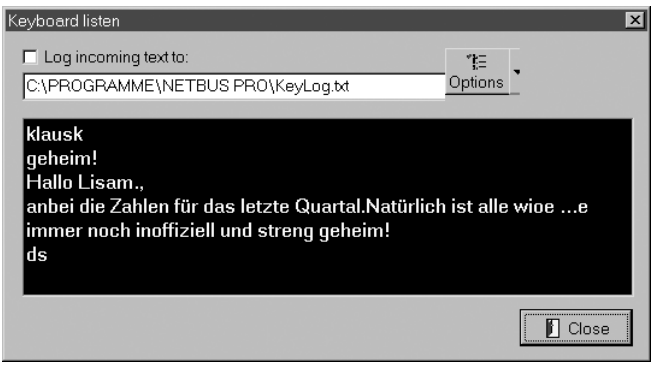
Wählen Sie ein Programm zur Ausführung auf dem Zielrechner aus

NetBus veranlasst daraufhin die Ausführung des Programms. Dabei wird wohlgemerkt das auf dem Zielrechner vorhandene Programm von diesem ausgeführt, d. h., alles läuft genauso ab, als ob der lokale Benutzer des Zielrechners das Programm eigenhändig aktiviert hätte. Damit werden also auch eventuell vorhandene Sicherheitsfunktionen, die den Zugriff auf das Programm oder dessen Dokumente über das Netzwerk verhindern sollen, einfach ausgehebelt.

Spionage-Funktionen

Auch für Spione ist NetBus eine prima Hilfe. Im Untermenü *Control/Spy functions* finden Sie gleich mehrere verschiedene Funktionen:

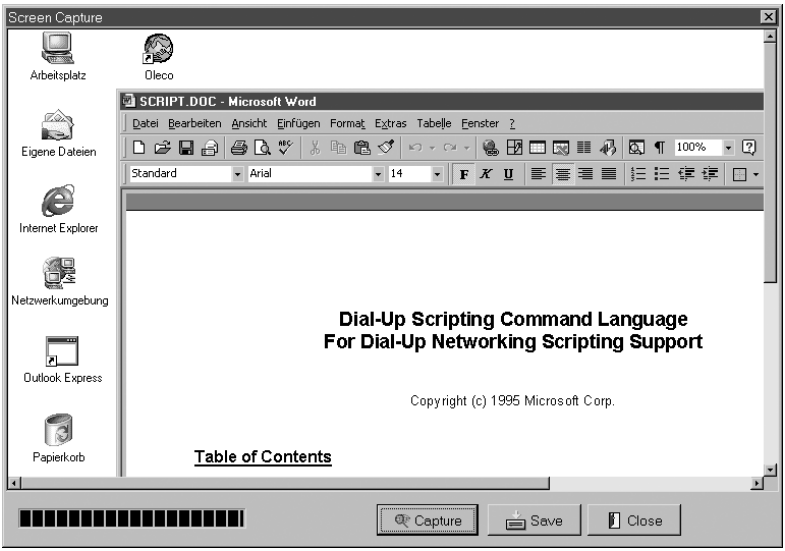
- Mit *Keyboard listen* können Sie die Tastatur des Zielrechners „belauschen". In diesem Modus übermittelt der Server alle eingegebenen Zeichen an den Client. Dieser stellt sie in einem Textfenster dar. Wenn am Zielrechner ein längerer Text (z. B. ein Brief oder eine E-Mail) eingegeben wird, können Sie diesen also komplett mitlesen. Ist diese Funktion während der Eingabe eines Passworts aktiv, wird auch dieses im Klartext übermittelt. Die Spionagefunktion setzt direkt im Kern des Betriebssystems an und ist deshalb völlig unabhängig davon, in welchem Programm die Eingabe erfolgt. Auch wenn der Benutzer in ein Passwortfeld tippt und am Bildschirm nur Sternchen angezeigt werden, übermittelt NetBus trotzdem die richtigen Zeichen. Das Lesen der übermittelten Texte ist etwas gewöhnungsbedürftig, da z. B. auch Tippfehler und Steuerzeichen (z. B. für Menüs) mitgeschickt werden.



NetBus kann die am Zielrechner eingegebenen Zeichen und Texte übermitteln

- Eine andere Möglichkeit ist das Anfertigen eines Screenshots vom Zielrechner. Dazu benutzen Sie die Spionagefunktion *Capture sceen image* und klicken im anschließenden Menü auf *Capture*. Nach kurzer Wartepause (für das Übermitteln der Grafikdaten) betrachten Sie auf Ihrem Bildschirm, was auf dem Monitor des Zielrechners gerade noch zu sehen war. Wenn das

Bild interessante Details enthält, können Sie es mit *Save* dauerhaft speichern. Andernfalls können Sie die Aufnahme beliebig oft wiederholen.



Auch ein Abbild des Bildschirms vom Zielrechner kann jederzeit abgerufen werden

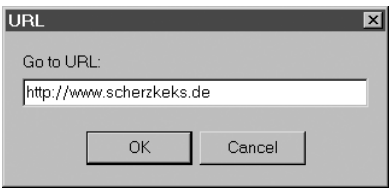
- Wenn am Zielrechner eine Webcam oder ein Mikrofon angeschlossen sind, kann die Spionage noch weitergehen. NetBus kann diese Eingabegeräte ansteuern und die Daten an Sie übermitteln. So können Sie z. B. Gespräche vor dem Zielrechner über das Mikrofon belauschen oder den Benutzer mit der Webcam beobachten. Bei der Webcam sollte man allerdings bedenken, dass manche Modelle mit einem kleinen Kontrolllämpchen signalisieren, wann sie aufnehmen. Dadurch könnte ein heimlicher Lauschangriff bemerkt werden. Die Funktionen für solche Lauschangriffe finden Sie ebenfalls *im Spy functions*-Untermenü.

Sabotage-Funktionen

Einige weitere Fernsteuerungsfunktionen fasst NetBus unter dem Stichwort *Cool functions* zusammen, was wohl andeuten soll, dass es sich dabei eher um Spaßfunktionen handelt, mit denen man andere ärgern kann. Allerdings kann man nach dem Motto „kleines Mittel, große Wirkung“ die Benutzung des Zielrechners damit massiv behindern.

- Im Untermenü *CD-ROM* etwa findet man Funktionen zum Öffnen und Schließen eines im Zielrechner eingebauten CD-Laufwerks. Dies gehört nun sicherlich zu den harmloseren Scherzen, der allerdings einiges an Verwirrung beim ahnungslosen Opfer auslösen kann.

- Weniger lustig sind unter Umständen die Funktionen zum Manipulieren der Tastatur im Untermenü *Keyboard*. Hier kann man die Tastatur des Zielrechners ganz deaktivieren oder mit einem lästigen Klickton versehen, der bei jedem Tastendruck abgespielt wird.
- Auch die Maus lässt sich beeinflussen. Hier bietet NetBus die Möglichkeit, die Maustasten zu vertauschen. Dies kann die Arbeit am Zielrechner nun wirklich empfindlich stören, insbesondere bis der Benutzer das Problem erkannt hat.
- Wenn man es mit einem abergläubischen Benutzer zu tun hat, kann man ihn mit den Funktionen *Go to URL* und *Send text* leicht glauben lassen, es mit einem Spuk-PC zu tun zu haben. Erstere öffnet eine beliebige Webadresse im Standardbrowser des Zielrechners. Wenn der Browser noch nicht läuft, wird er dazu automatisch gestartet. Die zweite Funktion sendet einen frei wählbaren Text in das momentan benutzte Fenster auf dem Zielrechner. Wenn dessen Benutzer also z. B. gerade einen Text eingibt, können Sie ihm damit etwas „zur Hand gehen".



Wie von „Geisterhand" kann man eine beliebige Webadresse auf dem Bildschirm erscheinen lassen

Diese Beispiele haben hoffentlich gezeigt, dass ein Trojaner die absolute Kontrolle über einen infiltrierten Rechner erlaubt. Man hat auf alles Zugriff, ganz so, als ob man selbst vor dem Rechner sitzen würde. Solange man sich nicht zu erkennen gibt, stehen einem außerdem umfangreiche Spionagefunktionen zur Verfügung. Nun können Sie natürlich einwenden, dass man für das Beispiel ja erst einen Server auf dem Zielrechner installieren musste. Schon richtig, aber NetBus gibt es auch in anderen Versionen. So werden z. B. einige als Freeware-Spiele getarnte NetBus-Dateien im Internet zum Download angeboten. Installiert man das Spiel, wird der NetBus-Server heimlich aufgespielt und so eingerichtet, dass er in Zukunft bei jedem Rechnerstart aktiv ist. Der NetBus-Client wiederum verfügt über eine Scan-Funktion. Mit der kann man in einem lokalen Netzwerk oder auch in einem bestimmten Bereich des Internets nach Rechnern suchen, auf denen ein solcher NetBus-Server aktiv ist. Da diese Trojaner in der Regel ohne Passwortschutz eingerichtet werden, kann jeder mit einem NetBus-Client auf jeden PC mit einem NetBus-Server zugreifen und alle hier beschriebenen Funktionen durchführen. Die Gefahr ist also allgegenwärtig. Im nachfolgenden Abschnitt beschreiben wir deshalb, wie Sie heimlich eingeschleppte Trojaner auf Ihrem PC erkennen und entfernen können.