The Hackers Blackbook

Cover Design:
The13th

THE HACKERS BLACKBOOK – RIPPED BY The13th of the DTP

Dieser Report ist in zweierlei Hinsicht hilfreich. Er soll Menschen, die ihr Passwort verloren haben, die Möglichkeit geben, es durch Anwendung einfacher Techniken ohne lange Wartezeiten zurückzubekommen und Besitzern von Websites mit geschütztem Inhalt ermöglichen, diese Inhalte zu schützen.
Webmaster, die die in diesem Report beschriebenen Techniken kennen, haben wesentlich bessere Aussichten, Ihre Website sicher gegen Eindringlinge zu schützen.

(Anm. v. The13th:
Die hier besprochene Software findet sich fast ausnahmslos auf: http://www.warmaster.de .
Solltet ihr UNIX software suchen, so schaut doch mal auf http://www.rootshell.com nach.)

THE HACKERS BLACKBOOK – RIPPED BY The13th of the DTP

Inhaltsverzeichnis

JavaScript-Passwortschutzsysteme

Die einfachste Art von Passwortschutzsystemen ist der sogenannte JavaScript-Schutz. Dabei wird der Benutzer beim Betreten einer Seite oder beim Anklicken eines bestimmten Links dazu aufgefordert ein Passwort einzugeben. Diese Art von Schutz ist sehr einfach und bietet nur ein Minimum an Schutz.

Beim Betrachten des HTML-Quellcodes der Seite findet sich dann oftmals ein JavaScript-Code ähnlich dem folgenden:

```
<head><title> Website-Titel </title> <script>
function jprot() { pass=prompt("Enter your password","password");
if (pass == "foo") {
document.location.href="http://protectedserver.com/index.html";
} else {
alert( "Password incorrect!" );
}
</script> </head>
```

Wie man sieht, wird das eingegebene Passwort verglichen und bei Korrektheit an eine angegebene URL gesprungen. Nun sieht man, wie das Passwort zu heißen hat und kann es einfach eingeben oder direkt die Ziel-URL wählen.
Oft wird auch das Passwort benutzt, um eine Ziel-URL zu generieren. Beispielsweise könnte die geheime Ziel-URL http://members.protectedserver.com/members/hu8621s.html derart geschützt werden: das Passwort „hu8621s" würde als Teil der URL kodiert. Die entsprechende Schutz-Funktion im HTML-Code der Seite sähe dann folgendermaßen aus:

```
function jprot() {
pass=prompt("Enter your password","password");
document.location.href="http://members.protectedserver. com/members/"+pass-+-".html" ;
```

Hier besteht mehr Schutz als in der ersten Variante, allerdings sind die Verzeichnisse mittels des HTTP-Servers oft nicht gegen unerlaubtes listen des Verzeichnisses geschützt. Wählt man mittels des Browsers die URL
http://members,Drotectedserver.com/members/ direkt in den Browser, so erhält man oftmals eine Auflistung aller HTML-Seiten in diesem Verzeichnis, also auch die Seite, die über den JavaScript-Passwortschutz angesprungen wird.

(ANMERKUNG >1< VON The13th BEACHTEN)

HTACCESS-Passwortschutzsysteme

Fast alle heute eingesetzten Webserver beherrschen den sogenannten HTACCESS-Passwortschutz. Zuerst wurde er vom Apache-Webserver eingesetzt, mittlerweile sind jedoch viele andere Webserver zum HTACCESS-Standard kompatibel. Daher wird er auch sehr häufig von sogenannten Paysites eingesetzt. Die Websites www.playgal.com oder www.hotsex.com setzen z.B. diesen Schutzmechanismus ein.
Eine Website, die HTACCESS einsetzt, ist daran zu erkennen, dass bei betreten des Mitgliedsbereichs ein Popup-Dialog erscheint (NICHT JavaScript-generiert), der folgendermaßen aussieht:

BILD FEHLT (SORRY!)

Um die Arbeitsweise dieses Schutzes zu verstehen, sollte man einige Grundlagen des Unix-Betriebssystems kennen. Unter Unix (bzw. Linux, BSD etc.) und auch unter Windows-Webservern wie dem Microsoft US sind die HTML-Dokumente wie auch bei einem normalen PC hierarchisch in Verzeichnisstrukturen angeordnet und abgelegt. Man spricht hier insbesondere von einer „Baumstruktur". Die Wurzel des Baumes (engl. „Root") ist die Domain selber ohne weitere Informationen. Zum Beispiel www.ibm.com ist die Domain und diese ist das Root der Verzeichnisstruktur.

```
|-|..#root
   |    |-|..#members     |    |..#secure     |....#public
```

Wenn in dem Verzeichnis "secure" nun die zu schützenden HTML-Dokumente und Grafiken liegen würden, so müsste in diesem Verzeichnis nun ein HTACCESS-File abgelegt werden. Das File muss den Namen ".htaccess" (mit Punkt davor) tragen. Das HTACCESS-File legt fest in welcher Datei die Passwörter liegen und aufweiche Art das Verzeichnis zu schützen ist. Das HTACCESS-File sieht folgendermaßen aus:

```
AuthUserFile /usr/home/myhomedir/passes AuthName MyProtectedSite AuthType Basic.
<Limit GET POST PUT> require valid-user </Limit>
```

Diese HTACCESS-Datei legt fest, dass das Passwortfile die Datei /usr/home/myhomedir/passes auf dem Server ist.

Sinnvoller Weise sollte die Passwort-Datei nicht im Bereich der HTML-Dokumente liegen, also nicht via WWW zugehbar sein.
Die Optionen "AuthName" gibt an, welche Bezeichnung im PopUp-Dialog erscheinen soll (im Dialog oben beispielsweise "playgal").

Das interessante am HTACCESS-Schutz ist, dass durch das HTACCESS-File auch alle Unterverzeichnisse unterhalb des Verzeichnisses, in dem sich die HTACCESS-Datei befindet, mitgeschützt sind. Und dies bis zu einer beliebigen Tiefe.
In unserem Beispiel könnte man also unterhalb des Verzeichnisses "secure" beliebig viele weitere Verzeichnisse anlegen. Diese wären alle geschützt.
Wie sieht nun die Passwort-Datei selber aus? Im Folgenden eine beispielhafte Passwort-Datei:

```
robert:$l$4A$JRLOVdCRzYtbpekrLBYzl/
manfred:$l$30$ddEyRldHykHUo654KE01i/
thomas:$l$sa$09grRUELps.nkqkRIWLA/Ge/
```

Für jedes Mitglied enthält die Passwortdatei eine Zeile, die aus zwei Teilen besteht, die durch einen Doppelpunkt getrennt sind.
Der erste Teil ist der Login-Name, der zweite Teil enthält das Passwort in verschlüsselter Form. Diese Verschlüsselung ist sehr sicher. Sie ist maschinenspezifisch. Das heißt, dass selbst wenn man diese Passwortdatei in die Finger bekommen würde, könnte man aus den verschlüsselten Passwörtern nicht die wirklichen Passwörter zurückberechnen. Bei der Passworteingabe wird das Passwort durch die Unix-Systemfünktion "crypt()" kodiert und mit dem in der Passwortdatei abgelegten verschlüsselten Passwort verglichen. Ist es gleich, so ist der Login OK.
Wie man also erkennen kann, ist es sehr schwierig, in Websites, die mittels HTACCESS geschützt sind, zu gelangen. Allerdings sind manche Webmaster einfach zu dumm, den HTACCESS Schutz richtig einzusetzen, und bieten so dem Angreifer einige Möglichkeiten.

Schwache Passwörter

Ein schwaches Passwort ist ein Passwort, dass leicht erraten werden kann. Hier einige der am häufigsten eingesetzten Username/Passwort Kombinationen:

asdf/asdf
123456/123456
fuck/me
qwertz/qwertz
qwerty/qwerty
qlw2e3
abcl23

Besonders die großen Pay-Websites, die einige tausend Mitglieder haben, ist es sehr wahrscheinlich, dass solche „schwachen" Passwörter dabei sind. Außerdem muss man sich vorstellen, dass einige Mitglieder in vielen verschiedenen Websites Mitglied sind und sich nicht alle möglichen Passwörter merken wollen. Daher wird auch oft der Name der jeweiligen Website von den Mitgliedern als Passwort gewählt.
Beispiel:

www.hotsex.com: username: hot, password: sex www.hotbabes.com: username: hot, password: babes

Oder die Mitglieder benutzen einfach nur ihren Namen. Dabei sind natürlich die am häufigsten vorkommenden Namen besonders interessant:
Im amerikanischen zum Beispiel

john/smith
john/john
miller/miller
rick/rick
frank/frank

und weitere mehr. Im Deutschen sind natürlich andere Namen interessanter.

Der einfach zu merkende Login bestehend aus „Username/password", so wie er auch im Passwort-Dialog gefragt wird, kommt auch häufig vor.
Das schwächste von allen Passwörtern ist allerdings das sogenannte „ENTER" - Passwort. Dabei kann beim erscheinen des Passwort-Dialogs einfach bestätigt werden, ohne überhaupt etwas einzugeben. Hat nämlich der Webmaster beim Erzeugen neuer Mitglieds-Daten einfach ohne Eingabe irgendwelcher Daten aus versehen einmal unbemerkt sein Tool gestartet, so befindet sich im Passwort-File ein eben solcher „leerer" Eintrag.

An den engagierten Webmaster richten sich folgende Sicherheitstipps:
• Das Erzeugen „leerer" Passwörter verhindern und kontrollieren
• Die Mitglieder nicht die Passwörter selber wählen lassen, sondern eines per Zufall generieren (z.B. „kd823joq")
• Falls die Kunden ihre Username/Passwort-Kombination selber wählen dürfen, nicht zulassen, dass der Username gleich dem Passwort ist.

Direktes Hacken der Passwort-Datei

Normalerweise sollte es nicht möglich sein, an das Passwort-File zu gelangen. In einigen Fällen ist es jedoch möglich, daran zu kommen, und zwar in folgenden Fällen:

> Die Passwort-Datei liegt im public_html-Bereich des Webservers,

also in den Verzeichnissen, in denen auch die via WWW zugänglichen HTML-Dokumente liegen

> Auf dem Webserver haben viele User einen eigenen virtuellen Webserver.

Der zweite Fall tritt dann auf, wenn der Website-Betreiber seinen Webserver bei einem großen Webspaceprovider mietet, der auf einem Rechner viele weitere Webserver betreibt (z.B. www.webspace-service.de, www.webspace-discount.de, www.simplenet.com etc.).

Dann ist es möglich, an die Passwortdatei zu kommen, falls man auf dem gleichen Rechner einen Account hat und die Passwortdatei öffentlich lesbar ist. Dann kann man mittels FTP oder TELNET in das Verzeichnis wechseln, indem derjenige seine Passwortdatei aufbewahrt und diese lesen. Mittels eines Brute-Force-Passwort-Crackers wie „Crack V5.0" lassen sich dann die Passwörter zurückberechnen. Das Programm braucht allerdings oft viele Stunden dazu und es führt nicht immer zum Erfolg.
Für einen absolut sicheren Schutz sollte also der Webmaster seine Paysite nicht auf einem Webserver betreiben, den er sich mit anderen Websites teilen muss.

Die Admin-Tools

Viele Webmaster der Paysites haben einen sogenannten „Admin-Bereich", der nur für sie selber gedacht ist. Dort erzeugen Sie neue Passwörter oder löschen alte Passwörter etc. Oft liegen diese Admin-Bereiche jedoch nicht in einem Passwortgeschützten Bereich. Die Webmaster denken nämlich, es würde ja keiner die URL ihres Admin-Tools kennen. Aber die URL ist manchmal einfach zu erraten. Oft heißt die URL www.thepaysite.com/admin.htm www.thepaysite.com/admin.html oder www.thepaysite.com/admin/

Man sollte auch weitere Namensmöglichkeiten austesten. Denn gelingt es, an die Admin-Seite zu kommen, so ist man natürlich am allerbesten bedient: Man kann selber so viele neue Passwörter hinzufügen, wie man möchte!

Phreaken

Unter „Phreaken" versteht man den Einsatz von falschen Informationen, um sich bei einer Paysite als neues Mitglied zu registrieren. Das ist natürlich verboten und diese Hinweise hier sollen in erster Linie den Webmastern dienen, damit sie sich vor solchem Missbrauch schützen können.
Wir wollen hier den am weitesten verbreiteten Fall beschreiben, bei dem die Mitgliedschaft online via Kreditkarte bezahlt wird und danach sofortiger Zugang erteilt wird.
Phreaker benutzen dazu einen anonymen Internetzugang. Dazu wird oft der Test-Zugang von AOL missbraucht. Test-Mitgliedschaften finden sich nahezu in jeder Computerzeitung. Aber auch okay.net bietet sofortigen Zugang nach Angabe aller Daten. Dabei meldet man sich mit Phantasienamen und irgendeiner Kontoverbindung an, die man aus irgendeiner Rechnung oder sonst wo her kennt. Schon ist man einen Monat lang anonym via AOL oder okay.net im Internet unterwegs.
Des weiteren benötigt man eine „gültige" Kreditkarten-Nummer (vorzugsweise VISA oder Mastercard - in Deutschland Eurocard). An diese zu kommen, ist schon etwas schwieriger. Eine gängige Methode ist es, einen sogenannten „Credit-Card-Generator" wie z.B. „Credit Wizard" oder „Cardpro" oder „Creditmaster" einzusetzen. Ein Suchern mittels „metacrawler.com" und den Begriffen „Credit Card Generator" o.a. bringt oft schon die gewünschten Programme.
Dazu sollte man wissen, dass die Online-Transaktionszentren nicht genau überprüfen können, ob eine Kreditkartennummer wirklich existiert und wem sie gehört. Es gibt lediglich bestimmte Algorithmen, um die Nummer und die Gültigkeitsdaten einer Kreditkarte auf eine gültige Struktur hin zu überprüfen. Daher kann man bei der Anmeldung beliebige Namen und Adresse angeben und eine der generierten Nummern. Allerdings liefern die Generatoren nicht das dazugehörige Gültigkeitsdatum.
Jedoch gibt es einen einfachen aber recht wirksamen Trick, um Kartennummern mit richtigem Gültigkeitsdatum zu erhalten: Die meisten der obengenannten Programme bieten die Möglichkeit, aus einer real existierenden Kreditkarten-Nummer neue Nummern zu generieren. Dieses Verfahren wird „Extrapolation" genannt. Die generierten Nummern unterscheiden sich meist nur in den letzten Stellen und da die Kartennummern bei den Kreditkarten-Herausgebern in der Regel in aufsteigender Reihenfolge vergeben werden, haben die so generierten Kartennummern meistens das Gültigkeitsdatum der Karte, von der aus extrapoliert wurde. Folgender Bildschirmauszug zeig den Extrapolationsvorgang:

BILD FEHLT (Sorry !)

Dabei kann man seine eigene, realexistierende Kreditkarte nehmen und aus ihrer Nummer neue Kartennummern berechnen. Das Gültigkeitsdatum ist dann mit größter Wahrscheinlichkeit bei den extrapolierten Nummern identisch mit dem Gültigkeitsdatum der eigenen, realen Kreditkarte.
Dabei braucht der Benutzer dieser Techniken keine Angst zu haben, dass man ihn zurückverfolgen kann. Der Zugang mittels anonymer AOL-Testzugänge bietet maximalen Schutz. Steht kein solcher Zugang zur Verfügung, sollte ein "Anonymizer" benutzt werden. Einen solchen findet man beispielsweise unter www.anonymizer.com. Surfman über den Anonymizer, ist die IP-Adresse nicht zurückverfolgbar. Eine etwas schwächere Variante, seine IP-Adresse zu verstecken ist die, einen Proxy-Server zu benutzen. Die meisten Internet-Zugangsprovider bieten die Möglichkeit an, über einen Proxy zu surfen.
Aber Achtung: Benutzen man seinen eigenen Internet-Zugang, also keinen anonymen AOL-Zugang oder Anonymizer oder Proxy, so kann der Betreiber der Website, bei dem man sich mittels der falschen Kreditkartendaten anmeldet, mittels der IP-Adresse, die der Server protokolliert, herausfinden, wer ihn betrogen hat bzw. es versucht hat. Dazu braucht er lediglich Ihren Zugangsprovider zu kontaktieren und ihm die IP-Adresse mitzuteilen. Die Provider führen i.d.R. über die letzten 80 Tage ein Protokoll, wann wer mit welcher IP-Adresse online war.

Login-Name Checker

Manche Pay-Sites geben möglichen neuen Mitgliedern während der Anmeldungsprozedur bereits vor der eigentlichen Zahlung die Möglichkeit, einen Mitgliedsnamen zu wählen. Ist der gewünschte Name bereits vergeben, wird dies mitgeteilt und man soll einen anderen Namen wählen. Gibt man beispielsweise „John" als Mitgliedsnamen ein, so sagt der Server meistens, dass der Name bereits vergeben ist. Das ist natürlich eine prima Vorraussetzung für die oben genannten Tricks zum Erraten von Passwörtern. Denn nun weiß man, dass es zumindest den Namen „John" schon gibt, somit muss nur noch das entsprechende Passwort erraten werden. Das ist eine wesentliche bessere Ausgangslage. als wenn man Passwörter zu Usernamen erraten muss, von denen man gar nicht weiß, ob sie überhaupt existieren!
Als Webmaster einer Paysite sollte man also darauf achten, dass das Neumitglied erst nach verifizierter Zahlung seinen Usernamen wählen kann!

Login-Generator nicht sicher

Oftmals ist es so, dass das Neumitglied zur Zahlung von der Paysite zu einem Kreditkarten-Service geschickt wird (z.B. www.ibill.com). Nach Verifizierung der Zahlung kommt der Neukunde dann wieder zu den Seiten der Paysite und wird dort entsprechend weiterbehandelt. In der Regel wird er nach erfolgreicher Zahlung zu einem Formular geschickt, mit dem die Login-Daten erzeugt werden. Das Neumitglied kann einen Usernamen und ein Passwort wählen und erhält nach wähl derer sofortigen Zugang. Das Formular fügt die Daten automatisch in die Passwort-Datei ein. Hier liegt jedoch ein oft gemachter Fehler:
Geht man nach Erzeugung eines Username/Passwort-Paares einfach mittels des „Back"-Buttons des Browsers zurück zum Formular, so kann man auf einfache und legale Weise ein weiteres Username/Passwort-Paar erzeugen und das immer wieder.
Als Webmaster sollte man folgende zwei Schutzmechanismen einsetzen:

- Das Kreditkarten-Unternehmen sollte nach erfolgreicher Prüfung einen einmaligen PIN-Code übermitteln, den man dann aus der liste der noch gültigen PIN-Codes streicht und so das Formular zur Username/Passwort-Erzeugung bei jeder Zahlung nur genau EINMAL eingesetzt werden kann. Dieses Verfahren wird von den meisten Kreditkarten-Unternehmen auch als „One-Time PIN-Hardcoding" bezeichnet.
- Das Script, dass die Usernamen/Passwörter erzeugt, sollte auch mittels der HTTP_REFERRER-Servervariablen überprüfen, ob der User auch vom Kreditkartenunternehmen kommt. Sonst kann ein gewiefter Hacker ein Script schreiben, das von seinem Rechner aus einfach solange verschiedene PIN-Nummern ausprobiert, bis es eine noch gültige findet. Sind die PIN z.B. siebenstellig, so dauert es im statistischen Mittel nur 5000 Sekunden, bis man eine gültige PIN findet, wenn das Script jede Sekunde eine PIN testet. Bei einer schnellen Internetverbindung sind jedoch auch mehrere Tests pro Sekunde möglich!

Bilder nicht in geschützten Verzeichnissen

Dieser Fehler ist einer der häufigsten, da er leicht übersehen wird:
Wie bereits erwähnt, sind mittels des HTACCESS-Schutzes immer das jeweilige Verzeichnis und alle Unterverzeichnisse geschützt. Befinden sich die Bilder der Mitgliederseiten jedoch in einem Verzeichnis, das nicht in dieser geschützten „Baumstruktur" enthalten ist, so kann dieses Verzeichnis und die Bilder darin ohne Eingabe von Username/Passwort angesehen werden. Besonders einfach ist es dann, wenn das Bilder-Verzeichnis auch nicht gegen auflisten geschützt ist. Dann genügt das Eingeben des Pfades um alle Bilder aufzulisten. Diese Bilderverzeichnisse haben oft den Namen „Images" oder „gfx", „pics", „pix", „Pictures", „pic", „Graphics". Ein einfaches Durchprobieren mit etwas Phantasie führt hier bereits oft zum Erfolg.
Beispiel:

```
|-|...#root        |...#images
       |...#members
```

Das .htaccess-File liegt im Geschützten Verzeichnis "members". Dort liegen auch die HTML-Dokumente für die Mitglieder. Die dazugehörigen Bilder liegen jedoch in diesem Beispiel im Verzeichnis "Images", welches nicht in der members-Hierarchie ist und somit nicht passwortgeschützt ist. Handelt es sich beispielsweise um www.pornsite.com als root dieser Paysite, so kann im Browser einfach die URL www.pornsite.com/images eingegeben werden, und man erhält eine Liste der gesammelten Bilder (vorrausgesetzt, das Directory-Browsing ist nicht serverseitig ausgeschaltet)

Packet Sniffing

Diese Möglichkeit ist etwas komplizierter als die anderen beschriebenen, denn es müssen einige Vorraussetzungen getroffen werden: Sie müssen in einem LAN (Ethemet-Netwerk) an einem Rechner sitzen und Root-Access haben. Dann kann man einen sogenannten „Packet-Sniffer" wie beispielsweise „SNOOP" einsetzen. Packet-Sniffer findet man meist als C-Sourcecode im Internet. Diese kurzen Sourcecodes muss man dann nur noch mittels gcc auf der UNIX-Shell kompilieren und schon ist es möglich, die Pakete, die zu und von anderen Rechner im LAN gesendet werden, abzuhören. Denn Ethernet-Netzwerke setzen die sogenannte „Broadcast-Technologie ein. Ein Paket, dass für einen Rechner in einem LAN bestimmt ist, wird im Prinzip an alle Rechner im LAN ausgesandt. Packet-Sniffing ist also wiederum besonders in den Fällen gefährlich, bei denen man bei einem Webspaceprovider seinen Webserver mietet und sich dort naturgemäß mit vielen anderen Kunden in einem LAN befindet. Ein Beispiel ist www.pair.com. einer der größten kommerziellen Webspaceprovider in den USA. Dort befinden sich über 70 Webserver in einem LAN, auf dem z.Zt. über 30.000 Kunden einen virtuellen Webserver betreiben!
Als Schutz gegen Packet-Sniffing bietet sich der Einsatz eines „Segmented Networks" an. Bei einem solchen Netzwerk wird nicht die Broadcast-Technologie benutzt, sondern die Pakete werden direkt mittels Routing-Tabellen zu dem Ziel-Rechner geroutet. Eine besonders für Web-Server geeignete Lösung ist der Einsatz von SSL (Secure Sockets Layer). Dies Protokoll verschlüsselt alle Pakete, die somit zwar noch abgefangen werden können, aber nicht mehr gelesen werden können. SSL wird von den meisten Webhosting-Unternehmen gegen geringen Aufpreis angeboten. SSL-Verschlüsselte Webinhalte sind am Protokoll-Prefix „https://" zu erkennen.
Zum Betrieb einer SSL-geschützten Website muss man eine SSL-ID haben, die es beispielsweise bei www.verisign.com gibt. Ein kleiner Nachteil ist jedoch, dass HTTPS-Verbindungen etwas langsamer sind als gewöhnliche HTTP-Verbindungen, da ein relativ hoher Verschlüsselungs-Overhead existiert.

Trojanische Pferde
Back Orifice und NetBus

Back Orifice

Die amerikanische Hackergruppe Cult of the dead Cow (http://www.cultdeadcow.com) veröffentlichte ein Programm mit dem Namen "Back Orifice", das sie als "Fernwartungswerkzeug für Netzwerke" bezeichnet. Dass die Intention eine andere ist, ergibt sich schon aus dem Namen: Back Orifice (hintere Öffnung) übersetzt man hier am besten mit "Hintertür", denn das Programm macht es fast zum Kinderspiel, Schindluder mit Windows-PC`s zu treiben. Witzig die Anspielung auf MicroSchuft's "Back Office"-System.
Das nur 124 KByte große "Server-Modul" lässt sich nämlich an ein beliebiges Windows-EXE-Programm koppeln, um es nichtsahnenden Anwendern unterzuschieben. Wird die Datei unter Windows 95 oder 98 ausgeführt, klinkt sich der Server quasi unsichtbar im System ein. Von diesem Moment an wartet das trojanische Pferd nur noch darauf, über das UDP-Protokoll geweckt zu werden.
Mit dem Client lässt sich bequem auf den befallen Rechner zugreifen. Unter anderem kann man das Dateisystem manipulieren (Dateien runterladen, hochspielen etc.), Tasks beenden, um. Die Funktionsweise des Back Orifice ist schon aus anderen Hacker-Tools bekannt; neu ist in erster Linie der Bedienungskomfort der grafischen "Wartungskomponente" - wenige Eingaben und Mausklicks genügen, um Prozesse zu beenden. Tastatureingaben zu protokollieren, die Windows-Registry zu manipulieren oder IP-Adressen umzuleiten.
Einen interessanten Praxisbericht findet man unter der deutschen Adresse
http://www.puk.de/BackOrifice/default.html oder http://www.bubis.com/glaser/backorifice.htm
Um Ihr System auf ein vorhandenes Back-Office zu untersuchen, gibt es Programme wie BoDetect
(http://www.spiritone.com/~cbenson/current_projects/backorifice/backorifice.htm)
oder das Programm BORED
(http://www.st-andrews.ac.uk/~sjs/bored/bored.html)
Es ist aber auch manuell sehr einfach. Back Orifice zu entfernen:
Öffnen Sie die Registry (regedit.exe ausrühren) und schauen unter dem Schlüssel
"HKEY_LQCAL_MACHINE\SOFTWARE\Microsoft\Windows\CuiTentVersion\RunServices"
nach einem Eintrag mit dem Namen "<blank>.exe" (Default-Filename) bzw. mit einem Eintrag der Länge 124,928 (+/- 30 Bytes). Löschen Sie diesen Eintrag; er bewirkt, dass der "Back Orifice"-Server bei jedem Windows-Start automatisch aktiviert wird.
Das Programm selbst liegt im allgemeinen im Verzeichnis "\Windows\System" und ist daran erkennbar, dass es kein Programm-Icon hat und eine Größe von 122 KByte (oder geringfügig mehr) besitzt. Sollten Sie die Datei aus irgendwelchen Gründen nicht finden, kann es Ihnen helfen, dass verschiedene Informationen als ASCII-String im Programm-Code zu finden sind; so ist mit großer Wahrscheinlichkeit die Zeichenkette "bofilemappingcon" enthalten, die Sie über Suche im Explorer finden werden.
Zusätzlich zur "Back Orifice-Programm-Datei" wird im selben Verzeichnis noch die "WINDLL.DLL" zum mitloggen von Tastatureingaben installiert, die Sie auch sinnvoller Weise löschen, die aber alleine keinen Schaden anrichten kann.
Das Problem bei Back-Orifice ist, dass es schwierig ist, die IP-Adresse des Hosts zu erkunden, da diese sich ja bei jedem Einwählen des befallenen Rechners ändert.
Dieses Problem gelöst und eine noch mächtigere Lösung geschaffen hat Carl-Fredrik Neikter mit seinem Programm "NetBus", welches recht ähnlich ist. Es bietet noch weitgehendere Funktionen und ist einfacher zu installieren.

NetBus

Nachdem Sie sich die entsprechende Datei heruntergeladen haben, sollten Sie diese entpacken. Nun erhalten Sie drei Dateien:
NETBUS.EXE, NETBUS.RTF und PATCH.EXE
Bei PATCH.EXE handelt es sich um das gefährliche Infizierungsprogramm, das eigentliche Trojanische Pferd. Starten Sie diese Datei also nicht! Die Datei NETBUS.RTF enthält eine kurze englische Anleitung des Autors. Die Datei NETBUS.EXE ist der „dient" mit dem Sie auf infizierte Server zugreifen können. Diese können Sie ohne Sorgen starten. Starten Sie zum Testen den Server auf Ihrem eigenen Rechner, indem Sie eine DOS-Eingabeaufforderung öffnen und im Verzeichnis von NetBus den Server mit dem Parameter ,,/noadd" starten, also

PATCH.EXE /noadd [RETURN]

Nun läuft der Server. Jetzt können Sie den Dienst starten (NETBUS.EXE doppelclicken) und auf Ihren eigenen Rechner zugreifen. Wählen Sie dazu als Adresse „localhost" oder „ 127.0.0.1". Wenn Sie den Server beenden wollen, wählen Sie im Client „Server Admin" und dann „close Server".

Außerdem kann das Infizierungsprogramm so geändert werden, dass es die IP-Adresse automatisch an eine von Ihnen gewählt Email-Adresse schickt, sobald jemand mit einem von NetBus infizierten Rechner in das Internet geht. Dies ist der gewaltige Vorteil gegenüber Back Orifice. Dazu wählt man im NetBus-Client den Button "Server Setup" und gibt die entsprechenden Informationen ein. Schwierig ist es lediglich, einen freien Mail-Server zu finden, der Mails von jeder IP-Adresse akzeptiert. Dann wählt man "Patch Srvr" und wählt die zu patchende Infizierungsdatei (standardmäßig "patch.exe").
Wer versucht, einen anderen Rechner zu infizieren, kann die Datei PATCH.EXE nun einfach per Email an einen anderen Internetnutzer schicken und die Datei als „Windows-Update" oder als irgendeine tolle lustige Animation bezeichnen. Die Datei kann dazu beliebig umbenannt werden (z.B. Win98update.exe oder siedler2patch.exe
etc.).
Wird die Datei nun gestartet, passiert optisch gar nichts. Jedoch hat sich der NetBus-Server bereits auf dem Rechner versteckt installiert und wird von nun an jedes Mal automatisch gestartet, wenn der Rechner gebootet wird.
Hat man obige Veränderungen am Infizierungsprogramm vorgenommen, bekommt man nun immer automatisch eine Email mit der IP-Adresse des infizierten Rechners, sobald dieser online ins Internet geht. Diese IP-Adresse können Sie nun im NetBus-Client eingeben und den Rechner manipulieren.
Hacker benutzen sicherheitshalber anonyme Email-Adressen, die es beispielsweise bei hotmail.com oder mail.com gibt.

Um Ihr System zu schützen, empfiehlt sich Norton Antivirus http://www.symantec.de/region/de/avcenter/ welches neben NetBus auch Back Orifice erkennt. Sie können auch wiederum manuell arbeiten. Der automatische NetBus-Start ist in der Registry unter
"\HKEY_LOCAL_MACHINESOFTWARE\Microsoft\Windows\CurrentVersion\Run"
eingetragen und sollte entfernt werden. Allerdings kann der Dateiname variieren (patch.exe, sysedit.exe oder explore.exe sind einige bekannte Namen)
Weiterführende Info finden Sie unter http://www.bubis.com/glaser/netbus.htm

Tip des Autors

Sollten Sie beabsichtigen, einen Passwortgeschützten Internetservice zu betreiben, so kommen Sie nie auf die Idee, einen Microsoft NT-Webserver einzusetzen! Windows NT hat ein Sicherheitssystem, das mehr Löcher hat, als ein Schweizer Käse. Statt dessen sollten Sie ein Unix-System wählen. Leider bieten deutsche Webspaceprovider größtenteils NT-Lösungen an. Hier heißt es also, Ausschau halten und ggf. konkret bei einem Webspaceprovider nach einem Unix-Server
fragen! Ein wesentlicher Vorteil eines Unix-Servers ist neben der Sicherheit der Vorteil, dass man sich dort auch per TELNET einloggen kann und so wesentlich mehr Kontroller über den Server hat. Bei NT-Servern ist dies nicht möglich! Empfehlenswert und preiswert sind besonders unter BSDI oder Linux laufende Webserver. Wie jeder weiß, ist Linux sogar kostenlos und Apache, einer der besten Webserver, ist ebenfalls kostenlos erhältlich. Außerdem sollte man auch die Performance-Vorteile eines Unix-Systems nicht unterschätzen. Besonders im Bereich Traffic-starker Webangebote wird fast ausschließlich Unix eingesetzt. Sollten Sie also beispielsweise ein Erwachsenen-Angebot mit vielen tausend Bildern etc. planen, so lege ich Ihnen den Einsatz eines Unix-Server wärmstens ans Herz. Eine interessante Website zum Thema „Unix vs. NT" findet sich unter http://www.lot-germany.com/magazin/unix-nt.htm !

Anmerkungen von The13th

Anmerkung zum Auflisten von Verzeichnissen über das angeben eines Verzeichnisses:
Dies kann man weitetgehend dadurch verhindern, in dem in dem Verzeichniss , in dem die „versteckten“ Dateien liegen, eine „index.html“ , „default.html“ oder „start.html“ gelegt wird (einfach nachsehen, was für eine Datei der webspace-provider automatisch anzeigt).
Dadurch wird beim auflisten des Verzeichnisses immer die angegebene HTML Datei angezeigt.

Ich habe mir dieses Buch aus der Bücherei ausgeliehen, und bin froh das ich es nicht gekauft habe-es mag zwar ganz interessant für absolute Anfänger sein, doch wenn man ein wenig weiter fortgeschritten ist, kann man sich das Buch auch gut sparen – oder als Notizblätter benutzen *g*.)