DOMINIQUE DEWITT

HIER STEHT, WAS IM HANDBUCH NICHT STEHT …

FESTNETZ, HANDY, INTERNET

DAS INOFFIZIELLE BUCH

MIT BELIEBIGER ABSENDERRUFNUMMER TELEFONIEREN

ANRUFMONITORE · ECHTE RUFNUMMERN NERVIGER CALLCENTER SEHEN

MIT DEM HANDY ZUM FESTNETZTARIF GÜNSTIG TELEFONIEREN

ANONYME SMS · OVER-THE-AIR-ANGRIFFE · ZWANGSPROXY UMGEHEN

SSH-TUNNEL · VPN-SERVER UND -CLIENT · OPEN-DNS MIT DER FRITZ!BOX

FRANZIS

Einleitung

Moderne Kommunikation bedeutet heutzutage weit mehr, als sich untereinander auszutauschen oder Daten zu übertragen: Festnetztelefon und Handy besitzt fast jeder Bürger, doch die wenigsten wissen, was diese Kommunikationsmittel für ein Potenzial außerhalb ihres ursprünglichen Einsatzgebiets bergen.

Wollten Sie schon immer wissen, wie Callcenter mit einer Servicenummer bei Ihnen anrufen, ohne dabei die echte Absenderrufnummer preiszugeben? Oder interessiert Sie vielmehr, wie Sie das selbst ebenfalls tun können?

Dieses Buch lüftet viele Fragen zum Thema Telekommunikation und zeigt die Möglichkeiten von Festnetz, Mobilfunk und Internet auf – egal ob Sie nur kostengünstiger mit Ihrem Handy telefonieren wollen oder wissen möchten, wie es um die Sicherheit moderner Mobiltelefone bestellt ist oder wie Sie Webfilter umgehen können.

Kunden von Telekommunikationsverträgen bekommen neben den angebotenen Leistungen mehr, als sie ahnen. Im Bereich Festnetz ist der ISDN-Anschluss hierfür das beste Beispiel. Neben den zwei frei nutzbaren B-Kanälen, die für Sprache und Daten verwendet werden können, verfügt der ISDN-Anschluss auch über einen D-Kanal, auf dem alle Steuerinformationen für die ISDN-Endgeräte übertragen werden.

HINWEIS!

Einige der hier im Buch behandelten Themen nutzen rechtliche Grauzonen. Grundsätzlich ist das Manipulieren von Telekommunikationseinrichtungen strafbar! Alle Informationen zum Thema »Hacking« dienen lediglich Informationszwecken und sind nicht dafür gedacht, irgendjemandem in irgendeiner Weise zu schaden! Autor und Verlag übernehmen keine Verantwortung für die hier gebotenen Informationen und deren Auswirkungen!

Wenige ISDN-Telefone sind in der Lage, neben den Standardinformationen, wie z. B. der übertragenen Rufnummer des Anrufers oder dem Zeitpunkt des Anrufs, auch andere nützliche Informationen auszuwerten, beispielsweise die »echte« Rufnummer eines Callcenters, die zusätzlich zu der übertragenen Service-Hotline im D-Kanal übertragen wird.

Das wichtigste Hilfsmittel ist neben einem Telefon und/oder einem Handy der Computer. Idealerweise sollten Sie über eine ISDN-Karte oder über einen Router mit integriertem ISDN-Controller (wie z. B. der AVM FRITZ!Box Fon-Reihe) verfügen, um alle hier erwähnten Szenarien nachstellen zu können. Ein Handy mit Symbian OS-Betriebssystem oder mit Windows Phone ist empfehlenswert.

Wir wünschen Ihnen viel Spaß mit und vor allem viel Nutzen mit diesem Buch.

Autor und Verlag

Auswertung der Protokollinformationen

Dieser kurze Protokollauszug beinhaltet jede Menge Informationen: Folgende Zeile gibt zum Beispiel an, um welche Art von Kommunikation es sich handelt:

```
DD320  Information transfer capability: speech
```

Hier handelt es sich bei *speech* um Sprache. Die Diensterkennung *speech* deutet darauf hin, dass der Gesprächspartner über ISDN verfügt.

3.1 kHz audio würde zum Beispiel auf einen Gesprächspartner mit einem analogen Anschluss hindeuten. Die Verkehrsausscheidungsziffer *0* spielt im D-Kanal keine Rolle, da durch die Zeile

```
DD320  Type of number: national number
```

angegeben wird, dass es sich um eine nationale Nummer handelt, der eine *0* vorangestellt werden muss. Aus diesem Grund fehlt die führende *0* bei allen Telefonnummern der eingehenden Anrufe im Logfile.

Folgende Zeile zeigt die Rufnummer, die auf dem Display des Angerufenen zu sehen ist (user provided):

```
DD320  Calling party number: 8001013449
```

Einige Absätze darunter lässt sich nun die »echte« Rufnummer (network provided) des Anrufers sehen:

```
DD320  Calling party number: 305900270
```

Schlussendlich wird in der letzten Zeile die Rufnummer dargestellt, für die der Anruf bestimmt ist:

```
DD320  Called party number: 123456
```

Nun wissen Sie, dass der Anrufer mit der auf dem Telefondisplay angezeigten Rufnummer *08001013449* in Wahrheit aus Berlin stammt und die echte Rufnummer *0305900270* ist.

1.4 Mit dem Handy zum Festnetztarif telefonieren

Handys der neusten Generation sind zusätzlich zu den immer beliebter werdenden Multimedia-Funktionen mehr und mehr für die Nutzung des mobilen

Internets ausgerüstet. Aus diesem Grund gibt es beim Abschluss vieler neuer Mobilfunkverträge entsprechende Datenoptionen, die ein gewisses Datenkontinent beinhalten – meist sogar ohne Aufpreis.

Weil UMTS genau die richtige Geschwindigkeit bietet, um Telefonate über das Internet in guter Qualität führen zu können, ist es eine gute Möglichkeit, bares Geld beim mobilen Telefonieren zu sparen. Auch wenn viele Netzbetreiber eine Nutzung von Internettelefonie über das UMTS-Netz untersagen, wird es dennoch toleriert.

TIPP!

Voraussetzung UMTS-Handy

Um dieses Feature nutzen zu können, müssen Sie über ein UMTS-fähiges Mobiltelefon verfügen, das einen integrierten VoIP-Client hat (z. B. viele Geräte der Nokia E-Serie). Auch ist es dringend angeraten, über einen Datentarif mit genug Inklusivvolumen oder, besser, eine mobile Internetflatrate zu verfügen.

Beachten Sie, dass durch die Nutzung von VoIP ohne Datentarif oder mobile Internetflatrate sehr hohe Kosten anfallen können.

Neben einem UMTS-fähigen Mobiltelefon, das mit einem VoIP-Client ausgerüstet ist, müssen Sie über ein Benutzerkonto für Internettelefonie verfügen. Sofern Sie sich, wie im vorherigen Kapitel beschrieben, ein Benutzerkonto bei Sipgate angelegt haben, können Sie dieses natürlich auch auf Ihrem Handy nutzen.

Im folgenden Beispiel werden die nötigen Schritte anhand des integrierten Nokia SIP-Clients (Internettelefon) aufgezeigt, der bei vielen Modellen identisch oder nur wenig unterschiedlich ist. Die dazugehörigen Bildschirmabbildungen vom SIP-Client zeigen die Version, die auf dem Nokia E90 Communicator zu finden ist.

Außerdem erhalten Sie im nächsten Abschnitt eine Musterkonfiguration für den VoIP-Anbieter Sipgate, sodass die Konfiguration Schritt für Schritt auf einfachste Weise vorgenommen werden kann.

Mobiltelefon für Internettelefonie fit machen

Um einen VoIP-Account auf dem Mobiltelefon nutzen zu können, müssen Sie folgende Schritte gehen:

1. Öffnen Sie das Menü auf dem Handy und wählen Sie *System/Einstellungen/ Verbindung* aus.

Bild 1.21 Funktionen im Menü *Verbindung*.

2. In diesem Menüabschnitt wählen Sie zunächst *SIP-Einstellungen* aus, im darauffolgenden Menü *Optionen/Neues Profil* und anschließend *Stand.-profil verwenden*.

Bild 1.22 Ein neues SIP-Profil anlegen.

3. Für *Profilname* können Sie *Sipgate* oder alternativ auch einen beliebigen anderen Namen verwenden. Für die folgenden Auswahlfelder verwenden Sie für eine reibungslose Konfiguration am besten diese Daten:

```
Dienstprofil:           IETF
Standard-Zug.-Punkt:    Ihr WLAN oder Ihre UMTS-
Internetverbindung
```

```
Öff-Benutzername:       Ihre Sipgate-Kundennummer @sipgate.de
                        (z. B. 12345@sipgate.de)
Komprimier. verwend.:   Nein
Anmeldung:              Bei Bedarf
Sicherh.-mech. verw.:   Nein
Öffnen Sie das Untermenü "Proxyserver", um dort folgende
Einstellungen einzutragen:

Proxyserver-Adresse:    sip:sipgate.de
Gebiet:                 (frei lassen)
Benutzername:           Ihre Sipgate-Kundennummer (z. B. 12345)
Passwort:               Ihr SIP-Passwort (zu finden bei: https://
                        secure.sipgate.de/user/settins.php)
Loose Routing erlauben: Ja
Transporttyp:           UDP
Port                    5060
```

4. Anschließend wechseln Sie in das vorherige Menü zurück und wählen den Eintrag *Anmeldeserver*. Dort tragen Sie dann folgende Daten ein:

```
Anmeldeserver-Adresse:  sip:sipgate.de
Gebiet:                 sipgate.de
Benutzername:           Ihre Sipgate-Kundennummer
Passwort:               Ihr SIP-Passwort
Transporttyp:           UDP
Port:                   5060
```

5. Nun können Sie auch dieses Menü verlassen und zu *System/Einstellungen/Verbindungen* zurückwechseln. Hier wählen Sie den Eintrag *Web-Tel.* aus, um den internen VoIP-Client für die SIP-Telefonie mit den zuvor festgelegten Daten nutzen zu können.

Bild 1.23 Funktion *Web-Tel.* auswählen.

6. Gehen Sie in diesem Menü wie folgt vor: Wählen Sie *Optionen/Neues Profil* aus. Sie können dem neu angelegten Profil wieder den Namen *Sipgate* geben. Bei *SIP-Profil* wählen Sie das unter *SIP-Einstellungen* eingerichtete Profil aus

Bild 1.24 Neu angelegtes Profil.

7. Wenn Sie diesen Schritt abgeschlossen haben, können Sie den VoIP-Client starten, den Sie im Hauptmenü unter *Verbindung/Internet-Tel.* finden.

8. Nach dem Start der Anwendung wählen Sie *Optionen/Einstellungen*, um zu kontrollieren, ob bei *Standard-Anrufart* die Auswahl *Internetanruf* gesetzt ist. Wenn ja, können Sie über *Zurück* in die Anwendung zurückkehren. Andernfalls korrigieren Sie die Auswahl, indem Sie *Internetanruf* als *Standard-Anrufart* auswählen, und kehren dann zur Anwendung zurück.

TIPP!

Einige Sekunden Verzögerung

Wenn Sie das UMTS-Netz für Internettelefonie nutzen, kann es – bedingt durch eine lange Signallaufzeit – vorkommen, dass Ihr Gesprächspartner Sie mit einigen Sekunden Verzögerung hört.

9. Die *Internet-Telefon*-Anwendung sucht in einem bestimmten Intervall immer nach verfügbaren Zugangspunkten – entweder nach einem WLAN-Zugangspunkt oder bei verfügbarem UMTS-Netz einem UMTS-Zugangspunkt.

Bild 1.25 Zugangspunkte werden gesucht.

10. Wählen Sie den Zugangspunkt aus, den Sie für die Internettelefonie nutzen möchten. Wurde die Verbindung erfolgreich hergestellt, können Sie die Anwendung schließen.

11. Auf dem Display erscheint nun in der rechten oberen Ecke eine Weltkugel mit Telefon. Um zu testen, ob die Verbindung stabil ist, können Sie die Rufnummer *10000* oder *10005* wählen.

Sofern Sie ausreichend Guthaben auf Ihrem Sipgate-Konto haben, können Sie nun zum Festnetztarif mit Ihrem Handy telefonieren. Haben Sie eine UMTS-Internetflatrate, können Sie dauerhaft im Netz eingebucht bleiben und sind fortan nun auch unter Ihrer von Sipgate vergebenen Festnetzrufnummer erreichbar.

1.5 Anonym SMS-Nachrichten versenden

Ein Thema, das für viele Anbieter eine eigene Geschäftsidee darstellt, ist das anonyme Versenden von SMS-Nachrichten. Dabei müssen Anwender, die anonym Kurzmitteilungen versenden wollen, für die Dienste des Anbieters meist einen happigen Aufpreis zu den eigentlichen SMS-Gebühren hinblättern.

Was viele Nutzer nicht wissen: Das Versenden von anonymen Mitteilungen geht ganz ohne Aufpreis vom eigenen Handy aus! Dafür müssen Sie allerdings einige Dinge beachten. Welche das sind, erfahren Sie jetzt.

- Sie sollten unter anderem schon vorab wissen, welches Gerät derjenige besitzt, dem Sie eine anonyme SMS senden möchten. Auch müssen Sie beachten, dass Sie nicht von jedem Gerät aus eine anonyme SMS versenden können.

2 Sicherheitslücken moderner Handys

Ob iPhone oder No-Name-Gerät mit Schwarz-Weiß-Display: Das, was einmal den Platz eines ganzen Raums in Anspruch nahm, passt heute in jede Hosentasche. Die Entwicklung schreitet immer schneller voran, und die immer schneller erscheinenden Handymodelle bieten schon wieder ein paar Funktionen mehr als die Modelle der vorangegangenen Generation.

Weil bei der kurzen Entwicklungszeit mitunter nur wirkliche Sorgfalt auf die später in der Werbung angepriesenen Funktionen verwandt wird, passiert es häufiger, dass sich Mängel in der Architektur des Systems zeigen oder Sicherheitslücken mit eingeschleust werden.

Doch nicht nur Hersteller sind für die Sicherheit ihrer Geräte verantwortlich, oft sind es auch die Nutzer, die ihr Gerät und somit die darauf befindlichen Daten angreifbar machen. Im Verlauf dieses Kapitels erfahren Sie ebenfalls, wie unterschiedlich die jeweiligen Gerätehersteller auf Sicherheitslücken reagieren und wie sie die Lösung solcher Probleme priorisieren.

HINWEIS!

Dieses Buch ist keine Anleitung zum Manipulieren oder unberechtigten Eindringen in fremde Systeme, aber das Thema »Sicherheit« sollte in einem Buch über Telekommunikation nicht fehlen. Es vermittelt das Wissen darüber, welche Möglichkeiten und Sicherheitsaspekte die modernen Telekommunikationsgeräte bieten und wie man sich vor Schwachstellen schützen kann. Aus diesem Grund kann an einigen Punkten dieses Kapitels nicht genauer auf spezifische Einzelheiten eingegangen werden.

2.1 Potenzielle Angriffsmöglichkeiten

Die erste Hürde bei einem Angriff besteht darin, die gewünschten Befehle oder Daten auf dem anzugreifenden Handy ausführen zu können. Hierzu muss zunächst ein Weg gefunden werden, wie man den entsprechenden Content

auf das »Zielgerät« bekommt. Die Möglichkeiten, die sich bieten, um Zugriff auf ein Handy oder Smartphone zu erhalten, sind vielfältig.

Während um die Jahrtausendwende das GSM-Netz die einzige Möglichkeit war, Kontakt zu einem Mobiltelefon aufzunehmen, und man somit nur mit dem Senden modifizierter SMS die Software eines Handys verändern konnte, so eröffnet sich einem heute ein viel breiteres Spektrum an Möglichkeiten: Ob Bluetooth oder offene Ports, eine geöffnete Hintertür ist nicht selten und stets das Ziel der Suche eines Hackers.

Aktivierte Bluetooth-Schnittstelle

Eine sehr populäre Technik, die heutzutage wohl in jedem Mobiltelefon integriert ist, ist Bluetooth. Dass eine solche Technik praktisch überall verfügbare Angriffsziele bietet, veranlasste Hacker und Gruppen, die sich auf das Auffinden von Sicherheitslücken spezialisiert haben, immer wieder dazu, auf die Einzelheiten der Protokolle und Verbindungstypen von Bluetooth einzugehen.

Am Anfang war das Bluesnarfing

Als eine der ersten Sicherheitslücken der Bluetooth-Technik wurde das »Bluesnarfing« bekannt, das die Möglichkeit bietet, ein Mobiltelefon mithilfe eines Computers bzw. Notebooks oder auch eines Smartphones anzugreifen und sich so Zugang zum Kalender, dem Adressbuch, zu E-Mails und Textmitteilungen zu verschaffen.

Als Studie zum Bluesnarfing wurde von der Entwicklergruppe trifinite.group das in J2ME geschriebene Programm »Blooover« vorgestellt, das die Möglichkeiten und Gefahren von Bluesnarfing aufzeigt.

Als weitere Lücke der früheren Tage präsentierte sich der sogenannte »Bluebug«, der der Öffentlichkeit erstmals im März 2004 auf der CeBIT in Hannover vorgeführt wurde. Mobiltelefone der ersten Generationen (darunter z. B. Nokia 6310 bzw. Nokia 6310i und Sony Ericsson T610) sind hiervon besonders betroffen.

Befindet sich ein solches Gerät mit aktivierter Bluetooth-Funktion in der näheren Umgebung (d. h. in einem Umkreis von 10 Metern, bei Nutzung von Spezialequipment auch mehreren Kilometern), erhält der Angreifer durch den Einsatz eines Notebooks mit Bluetooth-Dongle und der entsprechenden Software Zugriff auf fast alle relevanten Funktionen eines Mobiltelefons.

Das heißt, dass ein Angreifer, der sich dank des Ausnutzens der Bluebug-Lücke unbemerkt vom Besitzer des angegriffenen Handys Zugriff auf dieses verschafft hat, nun in der Lage ist, neben dem Versenden und Lesen von SMS Anrufe zu tätigen oder mitzuhören.

Dass der Zugriff auf die damaligen Geräte so einfach war, entwickelte sich zu einem Skandal, da Informationen darüber veröffentlicht wurden, dass viele Regierungsmitglieder der Bundesrepublik Deutschland ein Mobiltelefon mit entsprechend aktivierter Bluetooth-Funktion besaßen und man somit mitunter auch an vertrauliche Informationen gelangen konnte, wenn man sich in deren Umkreis aufhielt und mittels einer Software Daten von deren Handys ohne größeren Aufwand auslesen konnte.

Einige Hersteller reagierten sofort und stellten ein Firmwareupdate bereit, das die Lücken (Bluesnarfing und Bluebug) schloss. Bei neueren Geräten funktionieren beide Angriffsarten nicht mehr.

Die Situation heute

Die Frage, ob man heutzutage noch Handys per Bluetooth hacken kann, muss mit »Jein« beantwortet werden. Die Möglichkeiten der Machbarkeit sind zwar vorhanden, aber sehr gering. Momentan existieren keine bekannten Sicherheitslücken in der Bluetooth-Technik, die sich ohne erheblichen Aufwand nutzen ließen.

Aus diesem Grund konzentriert man sich bei der Suche nach Schwachstellen eher auf die Gerätesoftware anstatt auf die Übertragungstechnik allein. Der Zugriff auf Daten bzw. Gerätefunktionen ist, da keinerlei vergleichbare Angriffsmöglichkeiten wie Bluebug & Co. vorhanden sind, nicht mehr ohne die Zustimmung des anderen Handys bzw. ohne Kopplung möglich.

Sollten allerdings beide Geräte (durch Kopplung) einander bekannt sein und eine Autorisierung bestehen, eine Verbindung ohne vorherige Bestätigung herzustellen, ermöglicht z. B. das Handytool »BT Info« das Verwalten der Systemfunktionen sowie das Auslesen von Telefonbuch, Mitteilungen etc. direkt von einem anderen Handy aus. Allerdings kann das nicht mehr als hacken bezeichnet werden, da im Voraus die Einwilligung zur Verbindung durch Kopplung erteilt werden muss.

Hacken im eigentlichen Sinn ist somit nur auf Umwegen möglich. Die Methoden dafür beschränken sich im Prinzip auf zwei Wege:

- **Hacken vom eigenen Handy aus**: Verschicken von manipulierten GIF-Bildern per MMS, manipulierter Bluetooth-Name.
- **Hacken vom Laptop bzw. PC aus**: Bluetooth DoS, Exploits per Shell ausführen, Schwachstellen von Handys per Internet ausnutzen.

Doch bevor man sich Gedanken über den produktiven bzw. eher destruktiven Einsatz solcher Möglichkeiten macht, sollte man lieber an folgende Weisheit denken: »Was du nicht willst, dass man dir tu, das füg auch keinem anderen zu!«

Programme zum Thema Bluetooth

Eher als Spielerei oder Demonstration des Machbaren anzusehen sind die nun vorgestellten Programme zum Thema Bluetooth, die in der heutigen Zeit eine mehr oder weniger wichtige Rolle spielen:

Blooover

Einst als Studie zum Bluesnarfing gedacht, wurde das Programm Blooover vom Entwicklerteam trifinite.group entwickelt. Heute findet es aufgrund nicht mehr vorhandener Sicherheitslücken kaum mehr Anwendung. Sie können Blooover von der Herstellerseite herunterladen:

⊡ LESEZEICHEN

http://bit.ly/c4rz8d

Blooover: Laden Sie Blooover von der Herstellerseite herunter.

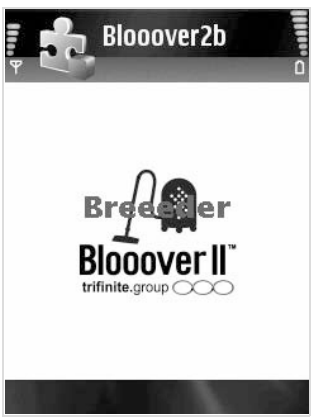

Bild 2.1 Die Breeeder-Edition von Blooover in der Version 2b.

BT Info

BT Info spiegelt die eigentlichen Funktionen im Sinne eines Hacks wider. Es vereint die Komponente des Systemzugriffs mit der Funktion, eigene Befehle auf dem entfernten Handy auszuführen. Realisiert wird das durch AT-Befehle, die an das verbundene Gerät gesendet und auf diesem ausgeführt werden. AT-Befehle werden von fast allen gängigen Gerätetypen unterstützt, daher ist dieses Programm weit verbreitet.

Im Gegensatz zu einem richtigen Hack bedarf es allerdings der Kopplung beider Geräte bzw. der einmaligen Bestätigung der Verbindung. Die neueste Version von BT Info in deutscher Sprache ist auf *www.bt-info.de* zu finden.

Bild 2.2 BT Info zeigt seinen Funktionsumfang.

BT TeRoR

Ein völlig anderes Ziel als die letzten beiden Programme verfolgt BT TeRoR. Anstatt Sicherheitslücken auszunutzen oder sich der Systembefehle zu bedienen, versucht BT TeRoR, den Besitzer des via Bluetooth ausgewählten Geräts mit Verbindungsbestätigungen zu nerven.

Auf dem eigenen Gerät, auf dem BT TeRoR ausgeführt wird, wird eine Datei ausgewählt, die das Programm im nächsten Schritt permanent an ein zuvor ausgewähltes Gerät aus der Umgebung schickt. Wird die Verbindungsaufforderung abgelehnt, schickt BT TeRoR prompt die nächste, sodass das verbundene Gerät blockiert wird. Wird der Dateitransfer angenommen, schickt BT TeRoR nach dem Übertragen sofort wieder eine Verbindungsaufforderung.

⊡ LESEZEICHEN

http://bit.ly/9jJ2tM

BT TeRoR: Die Installationsdateien sowie eine ausführliche Anleitung für BT TeRoR finden Sie hier.

Bild 2.3 BT TeRoR terrorisiert ein anderes Bluetooth-Gerät.

BlueDoS

Das Skript BlueDoS, das unter Linux ausgeführt wird, nutzt im eigentlichen Sinn keine Sicherheitslücke aus, sondern bedient sich einer Technik, die in kürzester Zeit extrem viele Anfragen an ein System schickt, womit dieses überlastet wird und schließlich abstürzt. Das funktioniert bei fast allen Mobiltelefonen, die über Bluetooth verfügen.

⊡ LESEZEICHEN

http://bit.ly/a8uN0f

BT TeRoR: Hier finden Sie den Quellcode für BlueDoS.

Over-the-air-Angriff

Hinter dem Sammelbegriff »Over-the-air-Angriff« (zu Deutsch Angriff aus der Luft) verbergen sich mehrere Arten von Angriffsformen, die allesamt aus der Ferne über das Mobilfunknetz ausgeführt werden. Im Gegensatz zu den Attacken via Bluetooth bieten diese Angriffsformen mitunter den kompletten Systemzugriff und ermöglichen somit echtes Hacken.

3 Internetrestriktionen nein, danke!

Das Internet: Unbegrenzter Zugang zu Informationen aller Art ist in erster Linie das, was das weltweite Netz auszeichnet. Doch diese Freiheit wird leider häufig durch den Einsatz von Filtersoftware oder transparenten Zwangsproxys am Arbeitsplatz oder in Schulen eingeschränkt. Auch Anonymität ist im Internet nicht gegeben, obwohl das häufig angenommen wird. Wie Sie sich anonym im Internet bewegen und wie Sie Filtersoftware am Arbeitsplatz bzw. in der Schule umgehen können, erfahren Sie in diesem Kapitel.

3.1 Filtersoftware und Zwangsproxys umgehen

Nicht selten kommt es vor, dass man am Arbeitsplatz oder in der Schule auf eine Webseite zugreifen möchte, die durch eine lokale Filtersoftware blockiert wird. Sinn solcher Sperren ist es, Webseiten oder bestimmte Webinhalte zu blockieren, um die Arbeitnehmer bzw. Schüler vom privaten Surfen abzuhalten und das Internet nur zur reinen Informationsrecherche oder dem Nachgehen der geforderten Aufgaben bereitzustellen.

Mit etwas technischem Geschick und mehr oder weniger Aufwand lassen sich diese Restriktionen umgehen. Man kann durch den Einsatz bestimmter Software (sofern das Ausführen von Software auf dem Rechner möglich ist) sogar die Protokollierung der eigenen Internetaktivität komplett umgehen.

TIPP!

Riskieren Sie nicht Ihren Arbeitsplatz!

Wenn Ihr Arbeitgeber es Ihnen untersagt, den Internetzugang am Arbeitsplatz zum privaten Surfen zu nutzen und Sie es dennoch tun, riskieren Sie Ihren Arbeitsplatz! Viele Unternehmen protokollieren die Webaktivitäten und können damit feststellen, zu welchem Zweck der Internetzugang genutzt wurde.

3.2 Einen Webproxy nutzen

Die einfachste Art, beispielsweise einen transparenten Zwangsproxy – also eine Software, durch die alle Webanfragen geleitet werden – zu umgehen, ist es, einen Webproxy zu benutzen. Das ist ein Skript, das auf einem Webserver ausgeführt wird und es ermöglicht, Anfragen (in diesem Fall: die Eingabe einer URL) entgegenzunehmen, zu verarbeiten und das Ergebnis an den Benutzer zurückzugeben.

Somit werden die über einen Webproxy aufgerufenen Webseiten nicht von dem Zwangsproxy im lokalen Netzwerk verarbeitet, und die sonst blockierten Webseiten können uneingeschränkt aufgerufen werden, da der Browser die Anfrage nach der gewünschten Website nicht mehr direkt an den Webserver, auf dem diese Website gehostet ist, stellt, sondern an den Webproxy.

Der Vorteil solcher Webproxys ist es, dass man sie direkt nutzen kann, ohne Veränderungen an den Einstellungen des genutzten Computers bzw. dessen Browser vornehmen zu müssen.

Natürlich wissen auch die Administratoren von den Möglichkeiten der Nutzung von Webproxys, um die eigens eingerichteten Blockaden des Webfilters zu umgehen. Deshalb werden kurzerhand bekannte öffentliche Webproxys mit in die Filterlisten aufgenommen, sodass der Zugriff darauf nicht mehr möglich wird.

Doch mithilfe der folgenden Tricks sollte auch das kein Problem sein:

1. Ersetzen Sie das führende *http://* der URL des Webproxys durch *https://*.

   Solche verschlüsselten SSL-Verbindungen können von einem lokalen Proxy nicht kontrolliert und deshalb nicht ohne Weiteres geblockt werden.

2. Ersetzen Sie die URL durch die IP-Adresse des Webproxys.

   Hierfür können Sie unter Windows einfach über *Start/Ausführen/cmd* und der Eingabe von *ping,* gefolgt von einem Leerzeichen sowie dem Domainnamen des Webproxys die dazugehörige IP-Adresse herausfinden, z. B. *ping vtunnel.com* (siehe Abbildung)

   Sollte das nicht zum gewünschten Erfolg führen, versuchen Sie auch hier, das führende *http://* vor der IP-Adresse des Webproxys durch *https://* zu ersetzen.

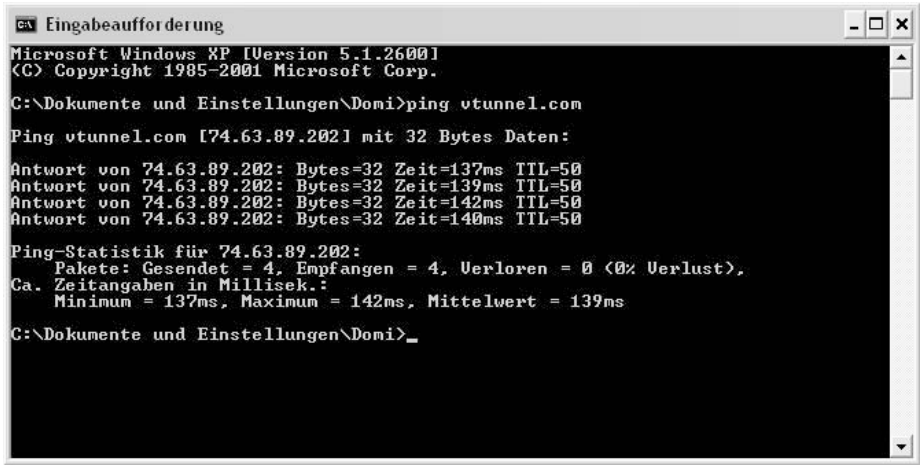

Bild 3.1 Durch das Anpingen der Domain eines Webproxys können Sie die IP-Adresse in Erfahrung bringen.

⊡ LESEZEICHEN

http://www.proxyliste.com/
http://proxy.org/

Öffentliche Webproxys: Hier finden Sie eine Liste, die genau beinhaltet, welche öffentlichen Webproxys Sie nutzen können.

Als dauerhafte Alternativen haben sich die Webproxys Anonymouse (*http://anonymouse.org*) sowie Vtunnel (*www.vtunnel.com*) etabliert. Vtunnel unterstützt alle genannten Möglichkeiten, einen lokalen Zwangsproxy zu umgehen (SSL-Verschlüsselung und Aufrufen über die IP-Adresse).

Nachteil öffentlicher Webproxys

Der Nachteil solcher öffentlichen Webproxys ist allerdings, dass sie die Anfragen gerade zu Stoßzeiten sehr schleppend verarbeiten und deshalb den gewünschten Inhalt nur sehr langsam laden. Ein weiterer Kritikpunkt ist, dass Sie sich nie sicher sein können, was mit Ihren Daten passiert, die Sie durch den Webproxy schicken.

Einen eigenen Webproxy einrichten

Sollten Sie ein Webhostingpaket Ihr Eigen nennen, das mindestens PHP 4.2.0 unterstützt, können Sie einige Nachteile der öffentlichen Webproxys umgehen, indem Sie Ihren eigenen Webproxy einrichten.

Hierzu ist es allerdings notwendig, dass Ihr Hostingprovider die Einstellung *safe_mode turned off* gesetzt oder die *fsockopen()*-Option nicht deaktiviert hat. Für die Realisierung eignet sich am besten das kostenlose Skript »PHProxy«, das Sie auf folgender Webseite herunterladen können:

⊡ LESEZEICHEN

http://sourceforge.net/projects/proxy/

Skript: Speichern und entpacken Sie die ZIP-Datei in einen Ordner z. B. auf Ihrem Desktop.

Anschließend können Sie diesen Ordner per FTP auf Ihren Webspace laden, z. B. mit dem bereits vorgestellten kostenlosen FTP-Programm FileZilla. Das ist alles, was von Ihrer Seite zu tun ist. Das Webproxyskript PHProxy ist nun unter Ihrer zugeteilten Domain und dem entsprechenden Ordner über einen Webbrowser erreichbar.

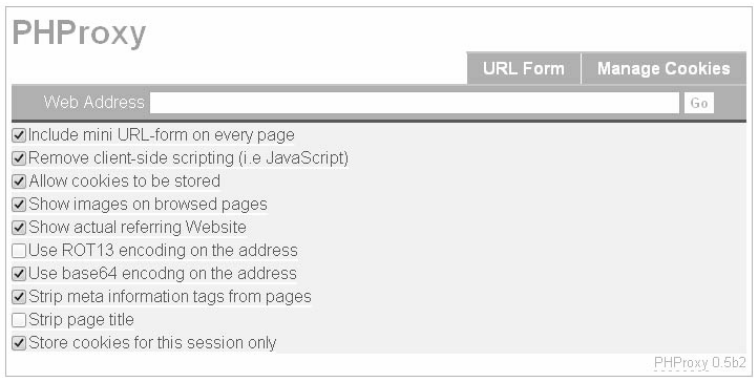

Bild 3.2 So begrüßt PHProxy Sie beim Aufruf mit dem Webbrowser.

Rufen Sie Ihren Webproxy nun auf, können Sie in die Adressleiste des Skripts die gewünschte URL eingeben, die durch den Proxy aufgerufen werden soll.

Im Gegensatz zu öffentlichen Webproxys können Sie jetzt sicher sein, dass niemand Ihre Daten mitlesen oder abfangen kann. Solange Sie niemandem die URL zu Ihrem Webproxy mitteilen, können Sie damit rechnen, dass Ihnen keine Performanceprobleme entstehen und die durch den Webproxy geladenen Webseiten rasch geladen werden.

Damit kein anderer Ihren Webproxy benutzen kann, ist es sinnvoll, den Zugriff auf das Proxyskript durch ein Passwort zu schützen. Dieses können Sie entweder über einen ».htaccess-Generator« im Internet erstellen lassen oder, besser noch, über das Kundenmenü Ihres Webhosters.

⊡ LESEZEICHEN

http://bit.ly/9Yly9l

.htaccess-Generator: Hier finden Sie einen .htaccess-Generator.

Einen Webproxy transparent nutzen

Wesentlich bequemer, als immer erst die URL des Webproxys aufrufen zu müssen, ist es, wenn Sie den Webproxy (PHProxy) transparent in Ihren Browser einbinden, indem Sie das Plug-in »Phzilla« für Mozilla Firefox installieren«.

Damit können Sie durch nur einen Klick entscheiden, ob die gewünschte Webseite über den Internetgateway des lokalen Netzwerks oder über den Webproxy geladen werden soll.

Ein kleiner Tipp hierzu: Es ist empfehlenswert, die Portable-Version von Mozilla Firefox einzusetzen, falls Ihr Arbeitgeber bzw. der Administrator des Netzwerks, in dem Sie das Plug-in nutzen möchten, die Installation von Drittsoftware verbietet.

Firefox Portable können Sie beispielsweise von Ihrem USB-Stick aus ausführen und haben so auch stets Ihre persönlichen Lesezeichen, Plug-ins und individuellen Einstellungen dabei.

⊡ LESEZEICHEN

http://bit.ly/5WTmg

Mozilla Firefox: Die portable deutsche Version Mozilla Firefox herunterladen.

1. Um PHProxy transparent nutzen zu können, müssen Sie zuerst das Plug-in Phzilla downloaden und installieren. Öffnen Sie dazu den Firefox-Browser und rufen Sie folgende URL auf:

   https://addons.mozilla.org/de/firefox/addon/3239

   Klicken Sie auf den Button *Zu Firefox hinzufügen*.

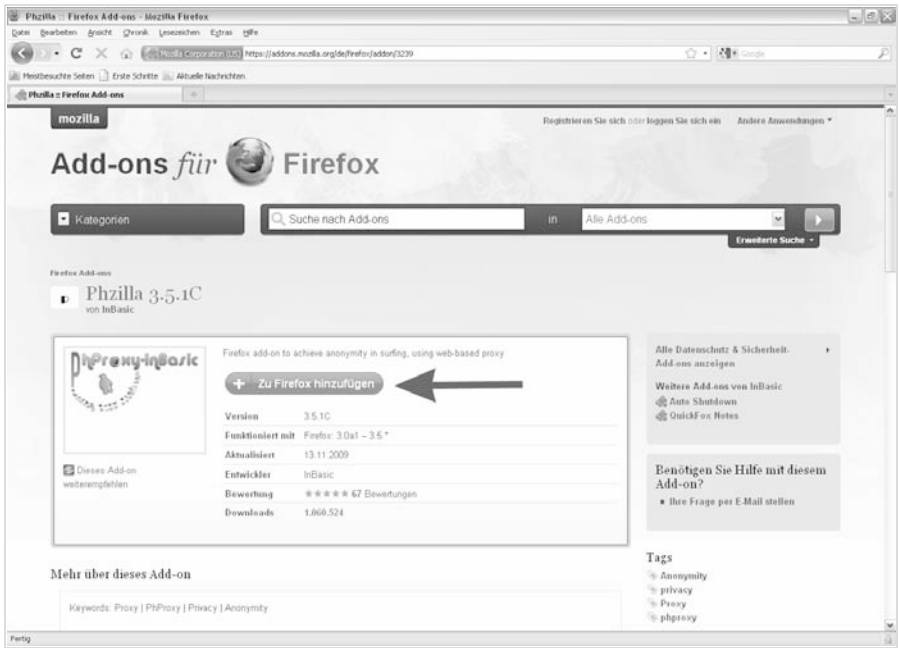

Bild 3.3 Das Phzilla-Plug-in herunterladen ...

2. Anschließend öffnet sich folgendes Fenster, in dem Sie ca. drei Sekunden warten müssen, bis Sie auf die Schaltfläche *Jetzt installieren* klicken können.

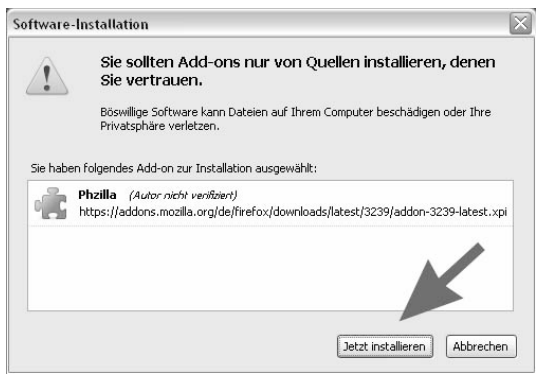

Bild 3.4 … und anschließend installieren.

3. Nach der Installation des Plug-ins müssen Sie Firefox neu starten, woraufhin das *Add-ons*-Fenster erscheint und meldet, dass das Plug-in erfolgreich installiert wurde. Klicken Sie in diesem Fenster im Abschnitt des Plug-ins Phzilla auf die Schaltfläche *Einstellungen*.

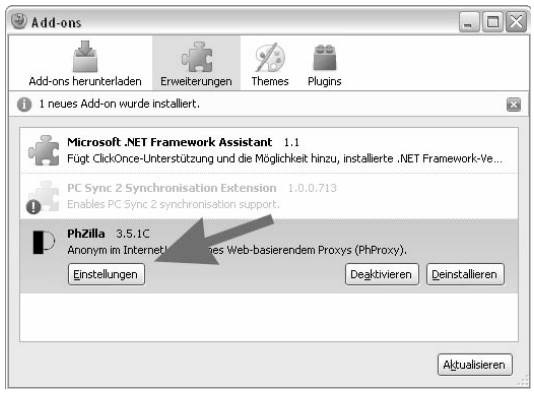

Bild 3.5 Das *Add-ons*-Fenster zeigt das neu installierte Plug-in an.

4. Im Fenster *PhProxy Einstellungen* können Sie nun entweder in der ersten Zeile die Adresse zu Ihrem eigenen PHProxy-Skript auf Ihrem Webserver eintragen oder aus der zweiten Zeile einen öffentlichen Proxy auswählen.

Bild 3.6 PHProxy-Einstellungen.

5. Haben Sie die entsprechende URL eingetragen bzw. einen öffentlichen Proxy ausgewählt, klicken Sie gegebenenfalls auf *Test starten* oder direkt auf *Übernehmen*, um die Einstellungen zu sichern.

6. Über die Registerkarte *Server* können Sie Ihren eigenen PHProxy als Server hinzufügen, sodass er als Standardserver eingerichtet ist.

7. Haben Sie alle Einstellungen vorgenommen, schließen Sie das Fenster durch einen Klick auf den *OK*-Button.

8. Möchten Sie nun eine Webseite über den Proxy laden, können Sie am rechten unteren Bildschirmrand auf das *P*-Symbol in Firefox klicken.

Bild 3.7 Durch einen Klick auf dieses Symbol wird die aktuell aufgerufene Webseite durch den Webproxy aufgerufen.

9. Um zu überprüfen, ob Sie eine Seite über einen Webproxy aufrufen können, empfiehlt es sich, eine Webseite, die Ihre IP-Adresse preisgibt, zu starten.

   Rufen Sie deshalb z. B. die URL *www.wieistmeineip.de* auf.

Bild 3.8 *www.wieistmeineip.de:* direkt und ohne Proxy aufgerufen.

Index

E

F

G

H

I

J

K

M

N

O

P

R

S

T

U

V

W

Z

Dominique Dewitt

FESTNETZ, HANDY, INTERNET
DAS INOFFIZIELLE BUCH

Festnetztelefon, Handy und Internetzugang besitzt fast jeder, doch kaum jemand weiß, was für ein Potenzial diese Kommunikationsmittel außerhalb ihres ursprünglichen Einsatzgebiets bieten. Wollten Sie schon immer einmal wissen, wie Callcenter mit einer Servicenummer bei Ihnen anrufen, ohne dabei die echte Absenderrufnummer preiszugeben? Oder interessiert Sie vielmehr, wie Sie das selbst ebenfalls tun können?

Dieses Buch lüftet viele Fragen zum Thema Telekommunikation und zeigt die Möglichkeiten von Festnetz, Mobilfunk und Internet auf – egal ob Sie nur kostengünstiger mit Ihrem Handy telefonieren wollen oder wissen möchten, wie es um die Sicherheit moderner Mobiltelefone bestellt ist und wie Sie Webfilter umgehen können. Übrigens – besitzen Sie einen Festnetz-ISDN-Anschluss? Dann sollten Sie wissen, dass Sie neben den zwei frei nutzbaren B-Kanälen, die für Sprache und Daten verwendet werden können, auch über einen D-Kanal verfügen, auf dem alle Steuerinformationen für die ISDN-Endgeräte übertragen werden. Wenige Telefone sind in der Lage, neben den Standardinformationen, wie z. B. der übertragenen Rufnummer des Anrufers oder dem Zeitpunkt des Anrufs, auch andere nützliche Informationen auszuwerten, beispielsweise die „echte" Rufnummer eines Callcenters, die zusätzlich zu der übertragenen Service-Hotline im D-Kanal übertragen wird.

Auch Anonymität ist im Internet nicht gegeben, obwohl das häufig angenommen wird. Wie Sie sich unerkannt im Internet bewegen und wie Sie Filtersoftware umgehen können, erfahren Sie ebenfalls hier. Mit etwas technischem Geschick und mehr oder weniger Aufwand lassen sich Restriktionen umgehen. Sie können durch den Einsatz bestimmter Software sogar die Protokollierung der eigenen Internetaktivität komplett verhindern. Wenn Sie immer schon wissen wollten, was wirklich in Ihren Kommunikationsmitteln steckt, liegen Sie mit diesem Buch genau richtig.

Aus dem Inhalt:

ISBN 978-3-645-65015-1

Euro 16,95 [D]

Besuchen Sie unsere Website

www.franzis.de