In diesem Kapitel:

- Phishing
- JavaScript als Einfallstor für Trojaner
- Dialer

KAPITEL 11

Angriffsszenarien

Im Verlauf dieses Buchs haben wir uns stets bemüht, die einzelnen Sicherheitsaspekte und Gefahren vor einem realen Hintergrund zu schildern und zahlreiche Angriffe und Angriffswerkzeuge der jüngsten Vergangenheit zu beleuchten. Um die klassische Buchform mit einzelnen Kapiteln zu zentralen Aspekten der Internetsicherheit zu wahren, haben wir jedoch immer nur einzelne Fragmente eines kompletten Angriffs betrachtet. Nachdem Sie nun mit dem nötigen Rüstzeug ausgestattet sind, soll dieses Kapitel anhand dreier Szenarien die Fragmente zu komplexen Angriffen zusammenfügen und aufzeigen, wie Cracker tatsächlich agieren.

Sie können beim Lesen das bereits erworbene Wissen Revue passieren lassen und überlegen, an welcher Stelle des Angriffs welche Gegenmaßnahmen möglich und effektiv wären.

Phishing

Phishing ist seit dem Jahr 2004 die wohl am häufigsten diskutierte Angriffsform im Internet und wird dies auch auf absehbare Zeit bleiben. Dabei ist Phishing weder eine neue Idee, noch basiert es auf bis dato unbekannten revolutionären Techniken. Im Grunde genommen ist Phishing hauptsächlich eine Social Engineering-Attacke, die als solche leicht zu erkennen und bereits im Keim zu verhindern ist.[1] Der immense Erfolg von Phishing beruht einerseits auf einer allgemeinen Verunsicherung und fehlendem Sicherheitsbewusstsein der Benutzer und zweitens auf den veralteten Sicherheitsstandards der Dienstleister (in diesem Fall meist der Banken). Als dritten Aspekt könnte man noch hinzufügen, dass die Struktur des WWW von Haus aus nicht für Anwendungen wie Online-Banking konzipiert wurde und sich, der enormen Größe und der damit verbundenen Standards wegen, nur langsam zu einer digitale Geschäftsmodelle unterstützenden Plattform entwickelt.

1 Dies gilt leider nicht für eine sich stark ausbreitende Sonderform des Phishings, die über Trojaner arbeitet.

Zur Drucklegung dieses Buches lag das gemessene Aufkommen an Phishing-Mails (siehe unten) allein in Deutschland bei mehreren zehntausend täglich. Die tatsächliche Anzahl erfolgreicher Angiffe lässt sich nicht messen, muss jedoch erschreckend hoch liegen, da bereits viele hundert Fälle zur Anzeige gebracht wurden. Schätzungen gehen davon aus, dass allein in Deutschland 2004/05 ein Schaden von etwa 4,5 Mio. Euro entsteht. Erbeutet werden in der Regel Beträge zwischen mehreren hundert und etwa zehntausend Euro (ab 12.500 Euro greift das Geldwäschegesetz). Auf Kulanz seitens der Bank brauchen Geschädigte nicht mehr zu hoffen – was in Anbetracht der Tatsache, dass ein Gutteil der Schuld für einen erfolgreichen Angriff auf Seiten der Banken liegt, vollkommen unverständlich ist – und sollten sich daher direkt an die Polizei wenden.

Wir wollen uns nun einen typischen Phishing-Angriff vereinfacht in vier Phasen ansehen und später einige Ergänzungen zu den verwendeten Angriffstechniken vornehmen.

Phase 1: Die Vorbereitungen

Je nach Art des Phishings fallen die nötigen Vorbereitungen unterschiedlich aus, sind jedoch meist aufwändiger als bei anderen automatisierten Angriffen, da es beispielsweise keine fertigen Bausätze (Construction Kits) gibt. Zunächst einmal gilt es, ein geeignetes Ziel zu finden. Dies muss nicht zwangsläufig eine Online-Banking-Plattform sein, je nach Motivation des Angreifers kommen auch Online-Shops oder Webmail-Anbieter in Frage, besonders hoch im Kurs steht auch eBay. Da Phishing besonders häufig im Bankenumfeld vorkommt, sehen wir uns ein Betrugsszenario beim Online-Banking an.

Phisher agieren meist nicht gezielt gegen einzelne Opfer, sondern versuchen ein Angebot zu fälschen, das von so vielen Anwendern genutzt wird, dass sie diese bequem mit ungezielten Massenmails erreichen können. Die Website einer bestimmten Bank mit deutlichem regionalen Touch eignet sich daher deutlich weniger gut als das zentrale Internetportal der Deutschen Bank oder der Postbank, die zurzeit am häufigsten von Phishern ins Visier genommen werden. Ist ein geeignetes Ziel ausgemacht, versucht der Phisher, die Anmeldeseite der Bank so gut wie möglich zu fälschen. Das ist eigentlich kein Problem, da er den Quell-Code des Originals samt Bildern herunterladen kann und nur die Links (beispielsweise zu den Bildern) umzusetzen braucht.

Auf der gefälschten Webseite wird nun der Bankkunde aufgefordert, seine Login-Daten fürs Online-Banking samt einer (oder mehrerer) gültigen TAN einzugeben. Als Vorwand für die Abfrage dieser sensiblen Daten dient die Behauptung, dass der Bankkunde nur so ein neues, sicheres System nutzen könne, mit dem die Bank in Zukunft Phishing verhindern möchte.

Um seiner Seite zusätzliche Glaubwürdigkeit zu verleihen, setzt der Angreifer nun noch einen Link zu der tatsächlichen Sicherheitsseite der angegriffenen Bank. Die

Phisher sind sich ihrer selbst dabei so sicher, dass es sie nicht weiter stört, dass auf der entsprechenden Seite der Bank vor genau solchen Tricks gewarnt wird – der Erfolg gibt ihnen recht!

Anspruchsvolle Angreifer versuchen, auch das Verhalten eines echten Logins möglichst getreu nachzubilden, um ihre Opfer in Sicherheit zu wiegen. Nachdem sie die Zugangsdaten zum Online-Banking sowie die TANs erbeutet haben, nutzen sie diese Informationen dazu, ihr Opfer auf die Website der Bank weiterzuleiten und es dort einzuloggen. Auf diese Weise gelangt der Bankkunde in seinen Account und schöpft keinen Verdacht. Weniger ambitionierte Phisher machen sich das Leben allerdings leichter: Nach der Eingabe der Bankdaten leiten sie ihre Opfer nur auf eine Seite, wo ihnen mitgeteilt wird, dass die Umstellung auf die neue Sicherheitssoftware erfolgreich verlaufen sei. Manchmal führt von dort aus ein Link auf die echte Login-Seite der Bank oder der Benutzer wird nach wenigen Sekunden automatisch auf die Homepage des Bankportals geleitet. Unmittelbar nachdem das Opfer also in die Falle getappt ist, wird ihm die echte Seite vorgelegt, auf der es nun keinerlei Spuren oder verdächtige Elemente finden kann.

Nachdem die Webseite fertig gestellt ist, braucht der Phisher einen Server auf den er das Plagiat laden kann. Nun sind die Domains *postbank.de* und *deutsche-bank.de* (beide Institute zählen in Deutschland derzeit zu den Hauptzielen von Phishern) natürlich schon vergeben, und so muss sich der Angreifer etwas anderes einfallen lassen. Die einfachste Variante ist es, sich gar nicht erst darum zu kümmern und darauf zu hoffen, dass das Opfer nicht auf die Adressleiste des Browsers achten wird. Dies funktioniert sogar erstaunlich gut, denn nicht umsonst findet man immer noch Adressen, die nur aus der IP-Adresse und eventuell einem Verzeichnis mit dem Namen der bank das der Bank bestehen (z.B. *http://198.4.23.7/postbank/*). Viel kritischer hingegen wird es, wenn der Phisher einfach für bestimmte Buchstaben einen anderen Zeichensatz nutzt. In solchen Fällen können Sie die Domain nicht von der echten unterscheiden. Diese Angriffe sind zum Glück sehr selten, da bei modernen Browsern, wie etwa Opera und Firefox die Verwendung solcher Zeichensätze standardmäßig deaktiviert ist.

Es gibt jedoch noch zwei weitere sehr elegante Tricks. Schauen Sie sich die Adressleiste in Abbildung 11-1 genauer an und erinnern Sie sich daran, was Sie über den Aufbau von Domains und Computernamen in Kapitel 2, *Technische Hintergründe*, gelesen haben. Scheinbar liegt die abgebildete Seite unter *www.deutsche-bank.de*. Bei genauerem Hinsehen wird jedoch klar, dass der Domainname in Wahrheit *backupserver11.com* ist – der gehört sicherlich nicht der Deutschen Bank.

Um diesen Trick zu entlarven, braucht es schon ein geübtes Auge und vor allen Dingen das nötige Maß an Misstrauen. Hauptsächlich könnte es den Besucher stutzig machen, dass die Bank entgegen aller Regeln der Vernunft keine Verschlüsselung, d.h. *http* anstelle von *https* benutzt. Der Angreifer könnte ein eigenes Zertifikat erstellen, das dann aber nicht gültig wäre und vom Browser moniert würde. Auch

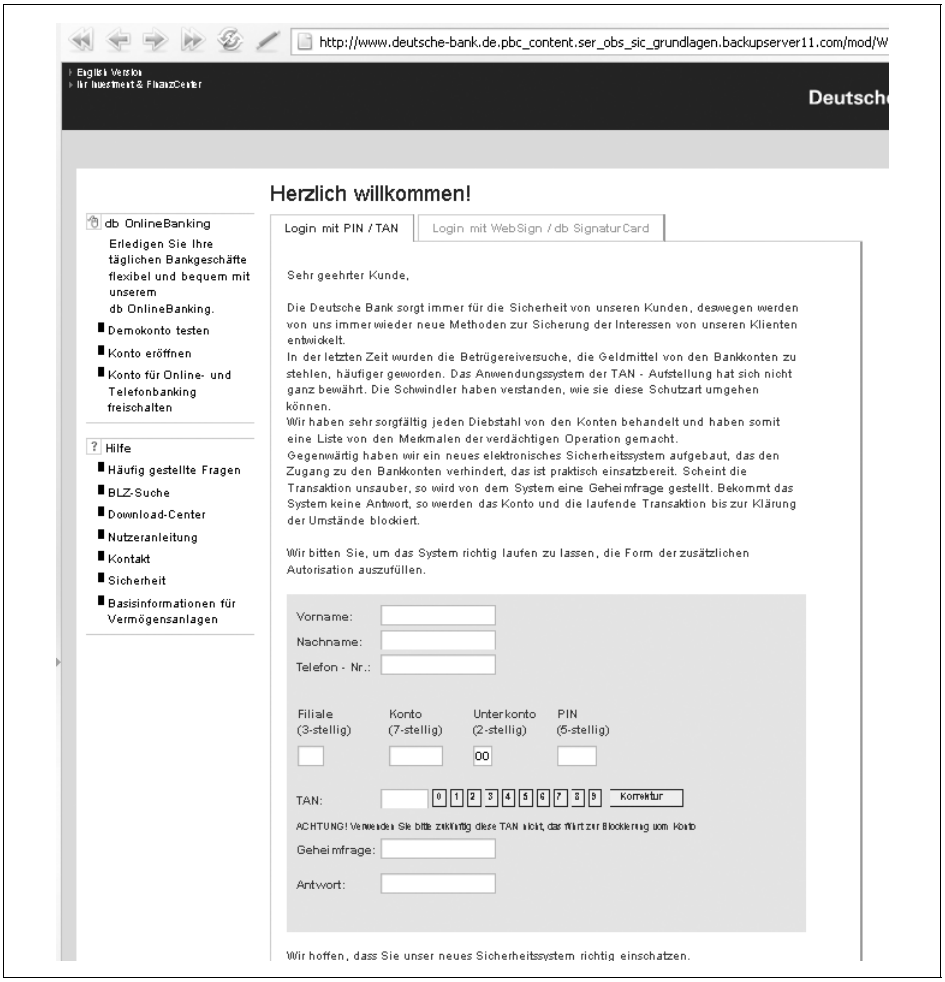

Abbildung 11-1: Phishing-Webseite

hier stellt sich wieder die Frage, ob der Anwender die Browsermeldung überhaupt liest oder nur rasch wegklickt. Es geht jedoch noch viel geschickter ...

In modernen Browsern können Sie mit Hilfe von JavaScript das Aussehen des Browsers an die Bedürfnisse Ihrer Seite anpassen. So lässt sich beispielsweise die Größe eines Browserfensters festlegen oder einzelne Leisten unterdrücken.[2] Ziel ist es, Adress- und Statusleiste des Browsers zu unterdrücken und in der gefälschten Webseite durch vorgefertigte Grafiken zu ersetzen. Dazu muss man im Grunde genommen nur einen Screenshot der echten Seite der Bank machen und aus diesem

2 Sie können dies beispielsweise beim Internet Explorer gern manuell nachvollziehen, indem Sie im Menü ANSICHT auf SYMBOLLEISTEN klicken und dort den Haken bei ADRESSLEISTE entfernen.

die entsprechenden Leisten ausschneiden. Da die Seite dann nur bei einer bestimmten Auflösung richtig angezeigt würde, erstellt man die Leistengrafik aus zwei verschiedenen Grafiken, von denen die eine auf den jeweils verbleibenden Platz skaliert wird (das ist beispielsweise mit unsichtbaren HTML-Tabellen problemlos möglich). Da es sich bei den Leisten nur noch um Bilder handelt, ist es nicht weiter schwierig, sie so aussehen zu lassen wie man möchte. Der Betrug wäre jedoch schnell entlarvt, wenn der Benutzer, nachdem er das Formular abgeschickt hat, die Adressleiste benutzen möchte, um eine weitere Internetseite zu besuchen. Um das zu verhindern, leitet man das Opfer also auf die echte Seite der Bank um, auf der die Leisten natürlich wieder wie gewohnt funktionieren).

Aufmerksame Anwender würden auch hier den Schwindel möglicherweise bemerken. Das setzt aber voraus, dass sie sich die Zeit nehmen, die Seite genau unter die Lupe zu nehmen. Aber jemand, der leichtgläubig genug war, dem Link aus einer Phishing-Mail zu folgen, wird wohl kaum so misstrauisch sein. Damit kommen wir auch zur zweiten Phase, dem eigentlichen Social Engineering.

Phase 2: Der Angriff

Nachdem die gefälschte Seite sich auf dem entsprechenden Server befindet, geht es nun darum, mögliche Opfer zu finden. Dabei geht der Phisher völlig wahllos vor und versendet einfach eine Massenmail an alle Adressen, die er im Vorfeld gesammelt hat. Um dabei selbst keine Spuren zu hinterlassen und gleichzeitig glaubwürdig zu wirken, fälscht er erstens die Absenderadresse (siehe dazu Kapitel 6, *E-Mail – wer liest mit?*) und benutzt zweitens ein Botnet (siehe dazu Kapitel 10, *Viren, Würmer und Trojaner*), durch das er ausreichend schnell genügend E-Mails versenden kann. Verfügt er nicht über eine große Anzahl aktueller E-Mail-Adressen, besteht für ihn die Möglichkeit, diese beim Anbieter des Botnets ebenfalls einzukaufen. Die Kunden anderer Banken werden die E-Mail ignorieren, doch die Trefferquote liegt immer noch hoch genug, da allein die Postbank und die Deutsche Bank zusammen mehrere Millionen Online-Banking-Kunden haben.

Natürlich muss sich auch die E-Mail nahtlos in das Design des entsprechenden Kreditinstituts einfügen, weshalb sie meist mit HTML und CSS gestaltet wird. Abbildung 11-2 zeigt eine solche E-Mail. Wie Sie sehen, warnt der Phisher in der Nachricht quasi vor sich selbst. Während die hier gezeigte Mail noch Schwächen aufweist und daher auf den zweiten Blick wenig überzeugend wirken mag, fügen die Phisher inzwischen noch einzelne Textpassagen hinzu, in denen der Bankkunde unter Druck gesetzt wird. Da heißt es dann z.B., dass die Bank im Fall eines Einbruchs keine Haftung übernehme oder das Konto deaktiviert werde, falls man sich nicht binnen 24 Stunden beim »neuen Sicherheitssystem« anmelde. Einerseits möchte der Angreifer seinen Argumenten und Aufforderungen dadurch mehr Gewicht verleihen und den Bank-kunden dazu bringen, übereilt zu handeln; andererseits arbeiten Phisher mittlerweile selbst unter enormem Zeitdruck, denn schon

kurz nachdem die ersten E-Mails versendet wurden, reagieren die ersten Provider, Betreiber von Mailservern oder auch die Banken.[3] Bis die Phishing-Seite offline ist – weil beispielsweise der Hoster bemerkt hat, was sein Kunde da treibt –, vergehen oft nur wenige Tage oder gar Stunden. Die Seite ist zwar schnell auf einem anderen Server untergebracht, doch die Mails gehen fortan ins Leere.

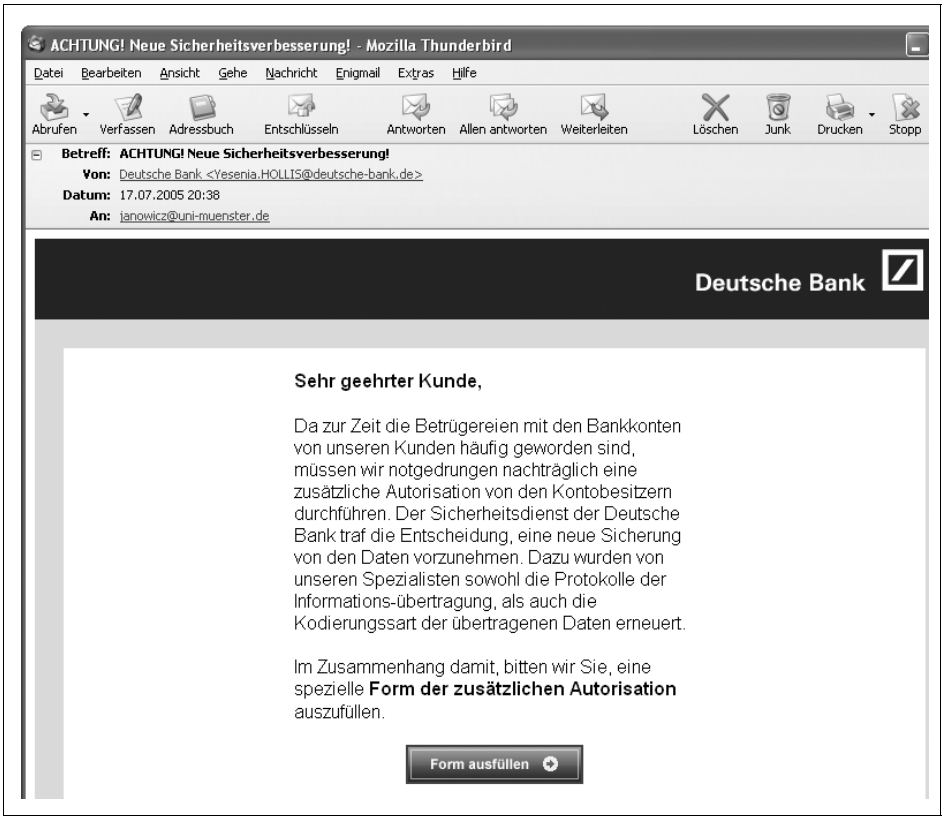

Abbildung 11-2: Phishing-E-Mail

Damit der Anwender nicht sofort sieht, dass der Link in der E-Mail zu einem dubiosen Ziel führt, benennt ihn der Angreifer nach dem eigentlichen Ziel, nämlich der angegriffenen Bank. Wie Sie in Kapitel 4, *World Wide Web*, gelesen haben, gilt es grundsätzlich zwischen dem (sichtbaren) Namen des Links und dem Zielort zu unterscheiden. Da ein Textlink weniger eindrucksvoll aussieht und die ersten Anti-Phishing-Tools, die derzeit auf den Markt kommen, solche Tricks erkennen, bindet er den Link wahlweise in Form einer Grafik ein. Es gibt auch Phishing-Varianten, in

3 So berichtete der Sicherheitsspezialist F-Secure, dass die Nordea-Bank in Schweden am 4.10.2005 kurzzeitig ihr komplettes Online-Banking-Angebot nach einer massiven Phishing-Mail-Welle vom Netz nahm, um ihre vier Millionen Kunden vor eventuellem Missbrauch zu schützen (siehe dazu *http://www.f-secure.com/weblog/archives/archive-102005.html#00000668*).

denen das Formular zur Eingabe der Zugangsdaten zum Konto sowie der TANs direkt in der E-Mail enthalten sind, diese sind jedoch weitaus seltener. Es lässt sich derzeit jedoch nicht sagen, ob das daran liegt, dass diese Versionen weniger erfolgreich sind. Zu vermuten wäre es jedoch, da Phisher sehr schnell auf neue Situationen reagieren und so das erfolgreichste Konzept schon nach kurzer Zeit die weiteste Verbreitung findet. Der Vorteil einer solchen integrierten Lösung liegt jedoch darin, dass der Nutzer keinerlei Domainnamen zu Gesicht bekommt.

Hat das potenzielle Opfer die Mail erhalten und folgt dem angegebenen Link, landet es auf der gefälschten Seite. Sofort nachdem die Daten eingegeben und abgesendet wurden, gelangen sie in die Hände des Phishers. Früher gaben sich Phisher in der Regel mit *einer* TAN zufrieden und führten damit eine einzelne Überweisung aus. Inzwischen versuchen die Angreifer, gleich an mehrere TANs zu gelangen. Es soll sogar Phisher geben, die gleich zehn TANs auf einmal zu erbeuten versuchen – allerdings mag man kaum glauben, dass jemand ernsthaft so viele TANs eingibt, ohne skeptisch zu werden. Da vielen Online-Banking-Kunden schon die Eingabe zweier TANs ungewöhnlich erscheinen mag, greifen Phisher häufig ein weiteres Mal in die psychologische Trickkiste: Jeder Computernutzer hat sich schon einmal bei der Eingabe eines Passworts vertippt und kennt die entsprechenden Aufforderungen, das Passwort erneut einzugeben. Dieses Wissen machen sich Phisher zunutze: Unabhängig davon, ob nun richtige oder falsche TAN eingegeben wurde, meldet die gefälschte Seite einen Tippfehler und fordert den Bankkunden auf, eine zweite TAN einzugeben.

Mit dieser zweiten TAN kann der Angreifer entweder eine weitere Überweisung vornehmen (das ist für ihn von Vorteil, da er mit mehreren kleinen Überweisungen die erwähnte Grenze von 12.500 Euro nicht überschreitet) oder aber die PIN des Opfers verändern. Da Kunden Ihre PINs aus Sicherheitsgründen regelmäßig ändern sollen, bieten die Banken ein spezielles Online-Formular dafür an. Nach der Eingabe der neuen PIN muss diese durch eine TAN abgesichert werden. Ändert nun der Angreifer die PIN, so verhindert er, dass sich der Kunde in seinen Account einloggen und den Betrug bemerken kann. Allerdings wird ein solches Vorgehen wohl eher die Ausnahme bilden, denn es gibt gleich zwei Gründe, warum das Ändern der PIN für den Angreifer problematisch ist. Zum Ersten wird der Kunde, nachdem er sich nicht mehr einloggen kann, mit Sicherheit die Bank verständigen, und zum Zweiten sperren viele Kreditinstitute den Online-Banking-Account, wenn drei Mal eine falsche PIN eingegeben wurde. Da das Opfer sich seiner PIN aber sehr sicher ist, stehen die Chancen nicht schlecht, dass es zu eben so einer Sperrung kommt und der Phisher seine erbeutete TAN nicht nutzen kann. Viel erfolgversprechender ist hier ein Angriff mit Social Engineering. Wie Sie unmittelbar unter dem TAN-Eingabefeld in Abbildung 11-1 sehen können, fordert der Phisher den Nutzer auf, die eingegebene TAN auf keinen Fall noch einmal zu benutzen, da dies zur Sperrung des Kontos führen werde.

Mit den so erbeuteten TANs und Zugangsdaten kann der Phisher nun Überweisungen tätigen.

Phase 3: Die Beute

Natürlich kann ein Phisher es sich nicht leisten, die ergaunerten Überweisungen auf sein eigenes Konto zu buchen. Um die Spuren zu ihm zu verwischen, muss er noch einen weiteren Schachzug machen. Dazu fälscht er nicht nur die Seite der angegriffenen Bank, sondern erstellt zusätzlich die Internetpräsenz eines Unternehmens aus dem Finanzdienstleistungssektor. Dieses Unternehmen gibt es natürlich nicht wirklich, aber das spielt keine Rolle. Auf der, meist seriös wirkenden, Seite des Unternehmens wird die Geschäftsidee vorgestellt und aufgezeigt, wie man als Finanzkurier dort eigenständig bis zu 15.000 Euro im Monat verdienen kann. Anschließend wird der Webauftritt um einige Seiten mit eindrucksvollen Zahlen und vor allem Erfolgsgeschichten beteiligter Finanzkuriere erweitert. Über ein weiteres Massenmailing verschickt der Angreifer nun Jobgesuche dieser virtuellen Firma an tausende von Empfängern. In der Mail werden der vermeintliche Traumjob beschrieben und auf die Webseite des erfolgreichen Unternehmens verwiesen. Ein Beispiel einer solchen Seite sehen Sie in Abbildung 11-3 – verlassen Sie sich jedoch nicht darauf, dass die Deutschkenntnisse der Angreifer stets so schlecht sind.

Abbildung 11-3: Webseite eines dubiosen Finanzdienstleisters

Abgesehen von einigen Variationen ist das Prinzip immer das gleiche: Der gesuchte Finanzkurier soll als Vertreter der Firma in Deutschland agieren. Diese sei bereits seit Jahren international tätig und versuche nun, auch in Deutschland Fuß zu fassen. Wer jetzt beim Aufbau einer funktionierenden Infrastruktur helfe, könne damit viel Geld verdienen. Meistens agiert die angepriesene Firma entweder als Dienstleister für Internetunternehmen oder wickelt selbst direkt Käufe über das Internet ab. Da man aber in Deutschland derzeit noch kein eigenes Konto unterhalten und niemanden mit der eventuell anfallenden Kommunikation mit deutschen Kunden

betrauen könne, suche man eine verantwortungsvolle Person, die das eigene Konto als Zwischenstation zur Verfügung stellt. Kunden besagter Firma würden daher das Geld an den frisch gebackenen Finanzkurier überweisen und dieser brauche nichts weiter zu tun, als das eingegangene Geld per Bargeldtransfer dem betrügerischen Finanzdienstleister zukommen zu lassen. Als Gegenleistung soll der Kurier in der Regel 7-10% des Betrags erhalten, die er direkt für sich behalten könne.

Für den Bargeldtransfer bedient sich der Phisher meist eines renommierten Anbieters auf diesem Sektor, nämlich Western Union. Der Geldtransfer an und für sich ist vollkommen legal und wird insbesondere von Personen genutzt, die sich im Ausland befinden und dort kein Konto haben. Das ist für Reisende enorm praktisch: Sie können z.B. einen Freund oder Verwandten in ihrer Heimat bitten, eine bestimmte Summe bei Western Union für sie einzuzahlen. Diese bekommen als Bestätigung für die Einzahlung einen Auszahlungscode, den sie dem Empfänger der Geldes nun telefonisch mitteilen sollen. Gegen Vorlage dieses Auszahlungscodes, kann der Empfänger das Bargeld in einer der vielen Western Union-Filialen einfach abholen. Dieser Service ist jedoch ausschließlich für Personen gedacht, die sich persönlich kennen, worauf Western Union auf seiner Webseite auch deutlich hinweist. Außerdem sollte man um keinen Preis den Auszahlungscode per E-Mail verschicken, weil dieser leicht abgefangen werden kann. Hält man sich nicht an diese Regeln, läuft man Gefahr, dass das Geld in falsche Hände gerät.

Genau dies ist beim Phishing der Fall. Ist der Bargeldtransfer erfolgt, braucht der Phisher nur zu einer Western Union-Filiale (und die gibt es in fast jedem Land der Welt) zu fahren und das Geld bar abzuheben; Spuren hinterlässt er dabei nicht. Alle vorhandenen Spuren führen zum Finanzkurier, und der Besuch von Bank und Polizei lässt nicht lange auf sich warten. Die Chancen, ohne Anzeige aus dieser Geschichte herauszukommen, stehen für ihn sehr schlecht. Dennoch scheinen sich immer wieder genügend leichtsinnige oder kriminelle Personen zu finden. Die Möglichkeiten, die wahren Hintermänner im Ausland (derzeit oft Russland) zu fassen, sind hingegen sehr gering, die Lebensdauer einer solchen Firma beträgt meist nicht länger als wenige Wochen.

Phishing-Trojaner und Pharming

Das hier besprochene Angriffsszenario zeigt den derzeit am weitesten verbreiteten Weg des Phishing im Bereich der Kreditinstitute. Die Zukunft gehört aber dem Phishing über Trojaner, erste Anzeichen dieser Zukunft zeichnen sich bereits ab. So berichtet Symantec in einem aktuellen Sicherheitsbericht, dass es mehr als 100 bekannte Varianten dieser speziellen Trojaner gibt, die bereits zu Angriffen genutzt werden.

Auch in diesem Fall ist die scheinbare Verwunderung der Banken und einiger Sicherheitsdienstleister nicht recht glaubwürdig, hat doch der CCC solche Angriffe nicht nur vor Jahren vorhergesagt, sondern auch ausführlich demonstriert (siehe

dazu Kapitel 7, *E-Commerce und Online-Banking*). Die Angriffsdemonstrationen des CCC sind zwar nicht identisch mit der jetzigen Umsetzung durch Phisher, ähneln ihr aber in erstaunlich vielen Punkten bis ins Detail. Bei diesen Szenarien werden die Tastatureingaben eines Opfers per Trojaner aufgezeichnet und der Browser des Benutzers in exakt dem Moment zum Absturz gebracht, in dem dieser (nach Eingabe der TAN) die Überweisung tätigen will. Während das Opfer erneut den Browser öffnet, bleibt dem Angreifer genug Zeit, um mit der TAN eine eigene Überweisung vorzunehmen. Mit dem gleichen Verfahren lassen sich auch die Überweisungsinformationen selbst manipulieren. Der Trojaner könnte so beispielsweise die Kontonummer ändern, nachdem der Benutzer das Überweisungsformular abgeschickt hat, da er frei in den Datenstrom des befallenen PCs eingreifen kann. Bevor die Antwortseite der Bank auf dem Browser erscheint, muss die Nummer nur noch wiederhergestellt werden, und die Illusion ist perfekt. Der Anwender führt in diesem Fall also selbst eine, von ihm gewollte, Überweisung aus – nur das Ziel ist ein anderes.

Als Pharming bezeichnet man verschiedene Arten von DNS-Angriffen, im Zusammenhang mit Phishing jedoch vor allem das Umschreiben der *hosts*-Datei, wie wir es in Kapitel 12, *Firewalls und erweiterte Sicherheitssysteme*, beschreiben. Dazu verändert der Angreifer mit Hilfe eines Trojaners die *hosts*-Datei des Opfers und braucht sich nunmehr nicht länger um möglichst authentisch aussehende Internetadressen für seine Phishingseite zu kümmern, da der Domainname des echten Kreditinstituts mit der IP-Adresse der Website des Angreifers verbunden wird. Einen solchen Angriff aufzudecken ist daher weitaus schwieriger, verlangt aber auch mehr Aufwand von Seiten des Angreifers, da sein Server, will er die Illusion aufrecht erhalten, als Man-in-the-Middle agieren und Anfragen weiterleiten muss. Einen zuverlässigen Schutz gegen Pharming gibt es zurzeit nicht. Die einzige Chance, eine Pharming-Seite überhaupt zu erkennen, besteht darin, beim Login zunächst eine falsche PIN einzugeben. Wird diese PIN vom Server akzeptiert, handelt es sich mit Sicherheit um eine Pharming-Seite. Wird die PIN hingegen zurückgewiesen, ist die Seite vermutlich echt. Ein Restrisiko bleibt allerdings bestehen, denn der Pharmer könnte als Man-in-the-Middle agieren und die PIN vom Server des Geldinstituts prüfen lassen.

Schutz vor Phishing beim Online-Banking

Im Prinzip haben Sie alles Nötige, um sich vor Phishing effektiv schützen zu können, bereits in den vorigen Kapiteln gelesen; einen hundertprozentigen Schutz gibt es bekanntlich dennoch nicht.[4] Sie brauchen aber keine Angst vor dem Online-Banking zu haben, wenn Sie sich an folgende Regeln halten:

4 Wenn der Angriff beispielsweise in Form eines Trojaners stattfindet, der von Ihrem Virenscanner noch nicht erkannt wird.

Folgen Sie niemals (und zwar ohne Ausnahmen) Links in E-Mails, wenn diese in irgendeinem Zusammenhang mit Online-Banking stehen. Im Grunde genommen gilt das auch für alle Online-Dienstleister wie etwa eBay oder Amazon, die aber leider täglich Nachrichten mit Links verschicken und es dem Benutzer dadurch nicht unbedingt einfacher machen. Während dies aber aus Gründen der Werbung einerseits und des Komforts andererseits noch in einem gewissen Kosten-Nutzen-Verhältnis steht, ist das beim Online-Banking sicherlich nicht der Fall. Zu keinem Zeitpunkt wird ein Kreditinstitut oder ein seriöser Online-Shop Sie per E-Mail, Telefon oder Fax dazu auffordern, Account-Daten oder gar TANs zu nennen. Wenn Sie solchen Links gar nicht erst folgen, sind Sie vor den üblichen Angriffen geschützt.

Darüber hinaus sollten Sie unbedingt einen tauglichen, immer auf dem neuesten Stand gehaltenen Virenscanner benutzen: An der falschen Stelle einige Euro zu sparen, kostet Sie womöglich später tausende. Achten Sie darauf, dass der Scanner zuverlässig Trojaner erkennt und dauerhaft im Hintergrund arbeitet. Gleiches gilt auch für eine Personal Firewall, die auf dem heimischen PC nicht fehlen sollte; zur Not tut es auch die in Windows XP (SP2) integrierte Microsoft-Firewall.

Zusätzliche Sicherheit erhalten Sie durch Nutzung spezieller (und zudem sehr komfortabler) Home-Banking-Software wie etwa *Quicken* oder *Mein Geld* (von *Wiso*). Auch hier sind Angriffe natürlich möglich, das klassische Phishing aber nicht.

Der wichtigste Schritt ist jedoch der Wechel von PIN/TAN auf HBCI und einen Kartenleser der Klasse 2 oder besser 3. Bietet Ihr Kreditinstitut kein HBCI an (was allerdings unwahrscheinlich ist), nimmt die Bank das Thema Sicherheit nicht sonderlich ernst und ist kein vertrauenswürdiger Partner für Online-Banking. Das gilt insbesondere dann, wenn Banken gegenüber Phishing-Opfern jegliche Schuld von sich weisen.

Seit dem Sommer 2005 gibt es erste mehr oder weniger hilfreiche Anti-Phishing-Tools. Diese lassen sich jedoch einerseits leicht austricksen und helfen andererseits keineswegs gegen Phishing-Trojaner. Wir werden daher bewusst keines dieser Programme oder Plugins besprechen, da sie Sicherheit vorgaukeln und dem Benutzer so möglicherweise das nötige Misstrauen gegenüber kritischen Links nehmen. Wenn der Phishing-Blocker im eigenen Mailtool oder Browser keinen Alarm schlägt, sollte dies nicht als Zeichen für eine saubere Nachricht oder Internetseite gewertet werden!

JavaScript als Einfallstor für Trojaner

Die meisten kritischen Sicherheitslücken gehen von ActiveX-Komponenten oder der Kombination Outlook (Express) und Internet Explorer aus. Häufig wird dabei übersehen, dass auch JavaScript ein gefährliches Einfallstor für Trojaner ist und massive Sicherheitslücken kein reines Microsoft-Problem sind. Der Fairness halber und um die Wichtigkeit regelmäßiger Updates bei allen Produkten hervorzuheben, werden

wir uns im Folgenden eine Sicherheitslücke in Firefox und nicht dem Internet Explorer genauer ansehen.

Der Angriff funktionierte nur mit den älteren Firefox-Browsern vor der Version 1.0.3. Diese und ähnliche Lücken werden innerhalb der letzten Versionen stets sehr zügig und zuverlässig beseitigt, so dass von diesem Szenario keine akute Gefahr mehr ausgeht. Dennoch verdeutlicht es sehr gut, wie Angreifer arbeiten, und aus diesem Grund sehen wir uns den Angriff etwas genauer an.

Phase 1: Die Vorbereitungen

Der Angreifer erstellt als erstes eine Webseite, die bei potenziellen Opfern Neugier wecken soll. Dabei kann es sich um eine Download-Möglichkeit für aktuelle Spieledemos, Bilder, Filme oder andere, teils illegale Angebote handeln. Wichtig ist nur, dass der Besucher der Seite am Ende auf einen bestimmten Link klickt. Hat man ein Opfer erst einmal auf die eigene Seite gelockt, stehen die Chancen meist sehr gut, dass der Link angeklickt wird und die Falle zuschnappt.

Bewerben kann man die eigene Webseite in zahlreichen Internetforen oder über Massenmailings, wie wir sie schon im Phishing-Angriff kennen gelernt haben. Auch in diesem Fall braucht der Angreifer sich nicht um eine zielorientierte Werbung zu sorgen, denn es gibt viele Millionen Firefox-Nutzer weltweit. Alle anderen Besucher der Seite werden von dem gescheiterten Angriff auf Ihren Browser nichts merken und können daher weitere potenzielle Opfer nicht warnen. Der Angreifer wird jedoch sehr genau darauf achten, dass auch bei erfolgreichem Angriff nichts Verdächtiges passiert, so dass sich die Opfer auch weiterhin sicher fühlen.

Die Firefox-Sicherheitslücke erlaubt, Dateien auf dem Rechner des Besuchers abzulegen und auszuführen. Das geschieht mit Hilfe eines Trojaners, den sich der Angreifer selbst erstellt. Sollte sein Fachwissen nicht dazu ausreichen oder sollte er nicht genau wissen, wie die Sicherheitslücke in Firefox zu nutzen ist, kann er Code-Fragmente, genaue Anleitungen oder komplette Angriffswerkzeuge bei Cracker-Gruppen käuflich erwerben. Da Programmierer von Schad-Code oft eher auf Masse als auf ausgewählte Kunden setzen, sind die Code-Fragmente nicht sonderlich teuer. Der Preis hängt vor allem davon ab, wie lange die Sicherheitslücke schon bekannt ist. Besonders gefragt und teuer sind sogenannte *0-Day-Exploits*, also Schad-Code, der bis dahin unbekannte oder vor wenigen Stunden veröffentlichte Sicherheitslücken nutzt, für die es noch keinen Gegenmaßnahmen gibt.

Nachdem ein passender Trojaner bereitsteht und entsprechend konfiguriert wurde, kann der Angriff beginnen.

Phase 2: Der Angriff

Der JavaScript-Angriff beruht auf einem falschen Umgang mit so genannten Favicons (auch Shortcut-Icons genannt).[5] Dabei handelt es sich um kleine Grafiken, die auf dem besuchten Server liegen und in die Adressleiste eingebettet werden. Viele Webseiten benutzen als Favicon das eigene (Unternehmens-)Logo, darüber hinaus haben die Icons jedoch keinerlei Funktion. Ursprünglich wurden Favicons von Microsoft im Internet Explorer eingeführt, werden inzwischen aber von fast allen Browsern unterstützt. Die eigentliche Gefahr liegt nicht in der Grafik an sich, sondern darin, dass Firefox nicht prüft, ob es sich dabei tatsächlich um eine solche harmlose Grafik handelt. Schiebt man dem Browser stattdessen JavaScript unter, wird dieses unter lokalen Rechten ausgeführt. Dadurch ist es dem Script möglich, auf eine Vielzahl mächtiger Befehle zuzugreifen, die einem gewöhnlichen externen JavaScript nicht zur Verfügung stehen. Dazu gehört beispielsweise auch das Lesen und Schreiben von Dateien auf der Festplatte des Benutzers.

Wir werden den Angriff nun anhand der Web-Demo unter *http://www.mikx.de/firelinking/* nachvollziehen. Es ist zwar auf den ersten Blick gefahrlos möglich, diese Demo selbst auszuprobieren, dazu müssten Sie sich aber eine ältere Firefox-Version aus dem Netz herunterladen und sie installieren. Dabei wird Ihre aktuelle und sichere Version überschrieben. Das stellt ein erhebliches Sicherheitsrisiko dar, weshalb von derartigen Experimenten abgeraten sei, wenn Sie nicht sehr sicher sind, dass Sie wirklich wissen, was Sie da tun, und nach dem Test zügig eine aktuelle Firefox-Version aufspielen. Abbildung 11-4 zeigt die Demonstration.

Ohne zu detailliert in die Programmierung mit JavaScript eintauchen zu wollen, werden wir uns anhand des folgenden Skript-Code-Ausschnitts anschauen, was genau in der Demo passiert:[6]

```
<textarea id="clearhtml" style="display:none">
<link rel="SHORTCUT ICON" href="favicon.ico"></textarea>
<textarea id="linkhtml_win" style="display:none">
<link rel="SHORTCUT ICON" href="javascript:delayedOpenWindow('javascript:netscape.
security.PrivilegeManager.enablePrivilege(\'UniversalXPConnect\');file=Components.
classes[\'@mozilla.org/file/local;1\'].createInstance(Components.interfaces.
nsILocalFile);file.initWithPath(\'c:\\\\booom.bat\');file.createUnique(Components.
interfaces.nsIFile.NORMAL_FILE_TYPE,420);outputStream=Components.classes[\
'@mozilla.org/network/file-output-stream;1\'].createInstance(Components.interfaces.
nsIFileOutputStream);outputStream.init(file,0x04|0x08|0x20,420,0);output=\'@ECHO
OFF\\n:BEGIN\\nCLS\\nDIR\\nPAUSE\\n:END\';outputStream.write(output,output.
length);outputStream.close();file.launch();','','')">
</textarea>
```

5 Das entspricht übrigens der typischen Situation, in deren Kontext die meisten Sicherheitslücken durch (eigentlich unntötige) Spielereien entstehen.

6 Es ist keineswegs erforderlich, dass Sie den Quelltext verstehen – vielmehr sollen Sie sich die einzelnen Schritte des Angriffs bewusst machen.

Abbildung 11-4: Erfolgreicher JavaScript-Favicon-Angriff gegen Firefox 1.0.2

Der restliche, hier nicht abgedruckte Quelltext sorgt nur für die Gestaltung der Seite, den Text sowie dafür, dass die Lücke auch unter Mac und Linux nutzbar wird. Außerdem bewirkt er, dass beim Laden zunächst das echte Favicon angezeigt wird und erst der Klick auf den Link die Falle zuschnappen lässt. Dies ist aber im Prinzip nicht nötig, denn bereits das Laden der Seite würde ausreichen, um den Angriff einzuleiten. In diesem Fall wäre der Effekt einer Demonstration aber nicht gegeben, und der Besucher könnte nicht selber entscheiden, ob er die Lücke testen will oder nicht. Das Testen von Sicherheitslücken ist insofern problematisch, als ein geschickter Angreifer seine bösartige Seite als genau so eine Testseite tarnen könnte.

Beim Betreten der Demoseite kommt der erste Teil des Quell-Codes zum Tragen:

```
<textarea id="clearhtml" style="display:none">
<link rel="SHORTCUT ICON" href="favicon.ico"></textarea>
```

Er stellt die unter *favicon.ico* gespeicherte Grafik dar. Bis dahin verläuft also alles, wie es sollte. Drückt man jedoch auf den Test-Link, wird durch ein kleines Skript die jeweils zum Betriebssystem des Besuchers passende Sektion (`inkhtml_win`) aktiviert. Wie Sie anhand des Quelltexts erkennen können, zeigt `SHORTCUT ICON` jedoch nicht mehr auf eine Grafik, sondern auf den eingebetteten JavaScript-Code (`href="javascript....`). Dieser erstellt eine neue Datei (`file...`) mit dem Namen *booom.bat*[7] und legt sie unter C:\, also im Wurzelverzeichnis Ihrer Systempartition, ab (`file.initWithPath(\'c:\\\\booom.bat\');`). Anschließend wird die Datei über

7 .bat steht für »batch file«, es handelt sich dabei um die Bezeichnung für Stapelverarbeitungsdateien in Windows, mit denen wiederkehrende Aufgaben automatisiert werden können.

einen so genannten Stream mit Inhalt gefüllt (`output=\'@ECHO OFF\\n:BEGIN\\nCLS\\nDIR\\nPAUSE\\n:END\';`) und anschließend gestartet (`file.launch();`).

Werfen wir abschließend noch einen Blick auf den Inhalt von *booom.bat*. Die Zeichenfolge `\n` bedeutet nichts anderes als einen Zeilenumbruch und spielt für die eigentliche Funktion des Programms keine Rolle. Auch `ECHO OFF` ist nur eine Schönheitskorrektur, die die Ausgabe der folgenden Befehle unterdrückt; bleibt `ECHO` angeschaltet, sind die folgenden Befehle in der Kommandozeile zu sehen, ist `ECHO` hingegen ausgeschaltet, sieht man nur ihre Auswirkungen. Der Name Echo rührt also daher, dass die Kommandozeile die Befehle quasi zurückwirft. Der nun folgende Befehl `CLS` löscht den bisherigen Inhalt der Kommandozeile, während `DIR` den Inhalt des aktuellen Verzeichnisses ausgibt. Mittels `PAUSE` bleibt das Kommandozeilenfenster so lange im Wartemodus, bis der Benutzer eine beliebige Taste drückt. Das Ergebnis ist in Abbildung 11-4 dargestellt. Wie Sie sehen, ist es völlig harmlos.

Kommen wir nun zurück zu unserem Angreifer, denn dieser möchte nicht einfach den Inhalt eines Verzeichnisses ausgeben, sondern einen Schädling installieren. Je nach Art der Sicherheitslücke, bevorzugter Taktik des Angreifers und gewünschtem Ergebnis kann der Trojaner entweder direkt in den JavaScript-Code eingebettet oder über einen so genannten Dropper geladen werden. Der letztgenannte Weg ist deutlich eleganter und oft auch der technisch einzig mögliche. Als Dropper bezeichnet man ein meist winzig kleines Programm, dessen einzige Funktion es ist, den eigentlichen Wurm, Virus oder Trojaner nachzuladen (siehe dazu Kapitel 10, *Viren, Würmer und Trojaner*). Nachdem der Dropper auf die gleiche Art und Weise wie *booom.bat* auf das System gelangt ist und ausgeführt wurde, lädt er den Trojaner des Angreifers und startet ihn.

Der Trojaner wird im ersten Schritt dafür sorgen, dass er von nun an bei jedem Systemstart geladen wird. Dazu legt er sich in das Autostart-Verzeichnis ab oder erstellt entsprechende Starteinstellungen in der Windows-Registry, dem Herzen von Windows. Anschließend durchsucht er den befallenen Computer nach Antivirensoftware oder einer Personal Firewall und versucht, sie zu deaktivieren oder zumindest an Updates zu hindern. Wenn möglich, wird der Trojaner nun versuchen, die Sicherheitslücke, über die er selbst in das System eingebrochen ist, zu schließen, denn Cracker teilen Ihre Zombie-PCs ungern mit der Konkurrenz.

Nach diesen Schritten darf sich das bösartige Programm zurecht in seinem neuen Wirt wohl fühlen und entfaltet die eigentliche Schadfunktion. Da der Trojaner vor dem Angriff konfiguriert wurde, weiß er, mit wem er sich nun in Verbindung setzten muss. Dazu öffnet er eine Verbindung zu einem geschlossenen Chatroom im Internet Relay Chat (IRC), dessen Passwort ihm sein Entwickler natürlich mit auf die Reise gegeben hat, und meldet dort, dass er einsatzbereit ist. Über den Chat kann der Angreifer dem Trojaner nun Anweisungen zukommen lassen. Dazu gibt er einfach die entsprechenden Befehle in das Chatfenster ein. Das kann man sich in etwa wie bei einem sprachgestützten Roboter vorstellen, der alles Gesagte nach ihm bekannten Befehlen analysiert und diese ausführt. Auf dem gleichen Wege kann der

Angreifer seinem Trojaner auch befehlen, sich weitere Programm-Updates von einem bestimmten Server zu laden.

In unserem Szenario ist der Trojaner mit einem Keylogger ausgestattet, der jeden Tastenanschlag samt des gerade aktiven Windows-Fensters protokolliert.

Phase 3: Die Beute

Um den Kreis zu schließen, nehmen wir an, dass es sich bei dem Angreifer um einen Phisher handelt und dieser, wie im ersten Szenario beschrieben, nun auf Bankdaten und TANs wartet. Tätigt das Opfer über den befallenen Rechner eine Online-Überweisung, friert der Trojaner den Browser des Benutzers ein, und der Angreifer benutzt die erbeutete Kontonummer samt PIN und einer gültigen TAN für eine Überweisung an einen Strohmann. Den weiteren Verlauf können sie sich nach der Lektüre des ersten Szenarios ausmalen.

Schutz vor Browserlücken

Auch hier gilt das bereits mehrfach Gesagte: Benutzen Sie stets eine aktuelle Version des Browsers und deaktivieren Sie alle unnötigen Einstellungen und Komponenten. Ist Ihnen bekannt, dass derzeit eine JavaScript-Lücke für Ihren Browser existiert, sollten Sie die JavaScript-Unterstützung komplett deaktivieren. Achten Sie zudem darauf, dass der Virenscanner aktuell ist und auch tatsächlich im Hintergrund arbeitet. Dies können Sie anhand des Symbols in der Taskleiste erkennen.

In 90% der Fälle genügt es aber schon, dubiose Seiten zu meiden und unseriöse E-Mails direkt zu löschen. Die beiden Szenarien haben Ihnen deutlich gezeigt, dass die Angreifer wahllos agieren, da sich stets genug Opfer finden. Wenn Sie kein leichtes Ziel bieten, hat kaum ein Angreifer Interesse an Ihnen (siehe dazu auch den Abschnitt »Wie viel Sicherheit ist notwendig?« in Kapitel 1, *Gefahren und Akteure im Internet*).

Dialer

Ursprünglich wurde mit dem Begriff Dialer eine unerwünschte Einwahlsoftware bezeichnet, über die der Internetzugang schnell zu einer sehr teuren Angelegenheit werden konnte. Dank deutlich verschärften Gesetzen und dem Siegeszug von DSL ist die Ausbreitung der Dialer jedoch in den letzten Monaten stark zurückgegangen. Zudem trennen sich zahlreiche Service-Provider blitzschnell von Kunden, die sich als Internetbetrüger erweisen. Inzwischen fasst man unter dem Begriff Dialer jedoch häufig verschiedene Arten von Trickbetrügereien zusammen, die einen bestimmten Dienst für einen hohen Minuten- oder SMS-Preis anbieten. Früher waren dies meist Anbieter von pornografischen Inhalten, inzwischen finden sich solche unseriösen

Geschäftsideen aber auch in zahlreichen anderen Bereichen, wie etwa bei Gewinnspielen, Tauschbörsen und Download-Plattformen.

Zum einen ist die Anzahl dieser Angebote und der verwendeten Techniken unüberschaubar groß geworden, zum anderen haben viele davon nicht direkt etwas mit Internetsicherheit zu tun. Darüber hinaus handelt es sich nach geltendem Recht nicht etwa um Angreifer, sondern um legale Geschäftsleute, die einfach jedes Gefühl für Ethik verloren zu haben scheinen. Daher wollen wir hier auf die Einteilung in Angriffsphasen verzichten und stattdessen einige unseriöse Tricks beleuchten.

Das Anbieten von Bezahldiensten auf Minutenbasis ist sicherlich rein rechtlich unproblematisch und für bestimmte Anwendungen sinnvoll; Minutenpreise, bei denen man schnell auf Kosten von mehreren hundert Euro kommt, sind jedoch inakzeptabel. Der Verpflichtung, die Minuten- bzw. SMS-Preise auf der Homepage zu nennen, kommen die Anbieter zwar nach, verstecken diese Informationen aber so geschickt, dass man sie leicht übersehen kann. Zudem wird der Kunde oft im Unklaren darüber gelassen, für was und wie lange er eigentlich zahlt.

Am besten, wir betrachten die Funktionsweise eines Dialers anhand eines Beispiels. Um einen Film aus dem Internet laden und anschauen zu können, sollen ein Anruf und das dort erhaltene Passwort ausreichen, könnte man meinen. Der Film wäre dann beispielsweise mit 1,99 Euro pro Minute vergleichsweise günstig. Sicherlich dauert es einige Minuten, bis man sich durch das absichtlich verschachtelte Menü gehangelt hat und am Telefon das Passwort zu hören bekommt. Tatsächlich sieht die Geschäftsidee jedoch völlig anders aus. Das Passwort ist eigentlich völlig überflüssig und dient nur dazu, schon zu Beginn Geld aus dem Kunden zu pressen. Gibt man das Passwort nämlich ein, gelangt man zwar zu einer Seite, auf der man die entsprechenden Videos auswählen kann, bekommt aber gleichzeitig die Meldung, dass man den Telefonhörer nicht auflegen dürfe, da sonst das Angebot abgebrochen werde. Bis das Opfer soweit gekommen ist, sind sicher schon fünf oder gar zehn Minuten vergangen. Wer jetzt aber glaubt, dank schnellem DSL den Film binnen kürzester Zeit auf die Festplatte laden zu können, hat sich getäuscht. In Wirklichkeit bekommt man den gewählten Film als Live-Stream aus dem Internet zu sehen und kann dabei oftmals nicht einmal vor oder zurück spulen. Würde man einen Spielfilm tatsächlich auf diese Art und Weise zu Ende sehen wollen, wäre das sicherlich teurer, als sich den Film direkt zu kaufen und noch einen guten DVD-Spieler mit nach Hause zu nehmen. In der Blütezeit der Dialer, vor der Einführung gesetzlicher Regelungen und spezieller Anti-Dialer-Software, lagen die Minutenpreise teilweise bei 300 Euro!

Abschließend sei noch eine andere Dialer-Variante erwähnt, bei der es sich um eine skurrile Art von Internet-Provider handelt. Betritt ein Besucher eine bestimmte Internetseite, wird ihm ein Programm untergeschoben, das von nun an die Einwahl ins Internet übernimmt. Dies kann einmalig für den Besuch der Seite gelten oder im schlimmsten Fall dazu führen, dass man dauerhaft über einen stark überteuerten

Tarif surft. Anstelle mit der Telefonnummer des eigenen Providers und den jeweiligen Account-Daten verbindet sich der Dialer mit der Gegenstelle des dubiosen Unternehmens und benutzt diese als Internetzugang. Selbst wenn der Kunde ausreichend darüber informiert wurde und den Dialer wissentlich installiert, um ein bestimmtes Angebot gegen Gebühr nutzen zu können, so erwartet er doch, dass die Verbindung mit dem Verlassen der Internetseite getrennt wird. Tatsächlich ist aber genau das nicht der Fall, und der Benutzer surft vielleicht noch eine halbe Stunde auf völlig anderen Webseiten weiter, zahlt dabei aber die Gebühren des Dialer-Anbieters. Auch hier liegen die Minutenpreise bei einem Vielfachen des Marktüblichen. Betroffen sind jedoch nur Nutzer von analogen oder ISDN-Modems, da es im Fall von DSL keine Einwahlnummern gibt, die manipuliert werden könnten.

Schutz vor Dialern

Mehr als in allen anderen Fällen hilft es bei Dialern bereits, aufmerksam zu sein und keinerlei kostenpflichtige Dienste mit Minutenpreisen zu nutzen. Im Internet gibt es gleich mehrere seriöse und komfortable Bezahlsysteme, die auch ohne Kreditkarte nutzbar sind (z.B. Firstgate). Desweiteren kann man die Dailer-Einstellungen oft in den DFÜ-Netzwerkeinstellungen von Windows rückgängig machen. Ist das manuell nicht möglich, sollte man zu einer Anti-Dialer-Software greifen. Viele interessante Informationen, Links und Softwarebewertungen sowie Tipps zum Erkennen der neuesten Tricks der Dialer-Anbieter finden Sie etwa auf den Seiten *http://www.dialerschutz.de*, *http://www.dialerhilfe.de* und *http://www.trojaner-info.de/dialer*.