Digitale Forensik

Dipl-Ing. Thomas Käfer

1. Ausgabe

Social Engineering und Phishing
am Beispiel von Facebook & Paypal

www.KaeferLive.de

DigiFor Inside 1. Ausgabe

Social Engineering und Phishing am Beispiel von Facebook & PayPal.

Impressum

Herausgeber: KäferLive - Dipl.-Inf. Thomas Käfer
Elchenrather Weide 20
52146 Würselen
Tel. 02405/47949-0

Autor: Dipl.-Ing. Thomas Käfer
Öffentlich bestellter und vereidigter Sachverständiger
für Systeme und Anwendungen der Informationsverarbeitung

Website: http://www.KaeferLive.de
E-Mail: service@KaeferLive.de

Bildnachweis: Quelle Fotolia.com bzw. eigene Aufnahmen/Grafiken

Bezug und weitere Informationen und Artikel siehe:
http://www.KaeferLive.de

ISBN-Nr.: 978-3-944632-10-0 (Apple iBook®-Format)
978-3-944632-01-8 (ePub)
978-3-944632-02-5 (PDF)

Erscheinungsdatum 04.03.2013

Inhalt

DigiFor Inside

Was ist DigiFor Inside? DigiFor ist die Kurzform für den Begriff „Digitale Forensik“, einem Spezialgebiet der IT, welches sich mit der Analyse und Aufdeckung von Sicherheitsvorfällen (sogenannten Incidents) und missbräuchlicher Nutzung von Computern im Rahmen von Straftaten und zivilrechtlichen Auseinandersetzungen beschäftigt. DigiFor Inside ist eine neue Reihe von Fachaufsätzen und Veröffentlichungen, bei denen der Autor Thomas Käfer aus dem IT-Nähkästchen plaudert und Angriffskonzepte und Maßnahmen zu deren Erkennung bzw. Abwehr offen legt.

Weitere Artikel siehe http://www.KaeferLive.de/digifor-inside

About Social Engineering und Phishing

Was kümmert mich Social-Engineering und Phishing bzw. was ist das überhaupt?

Jeder, der sich heutzutage durch Surfen auf Webseiten, Nutzung von Online-Shops und -Bezahlsystemen, Social-Media-Netzwerken oder ganz simpel per E-Mail im Internet bewegt, ist praktisch ständig Angriffsversuchen Dritter ausgesetzt, die versuchen, an die persönlichen Daten des Nutzers heran zu kommen oder ihm auf dubiose und illegale Weise das Geld aus der Tasche zu ziehen.

Als Social-Engineering bezeichnet man Mechanismen und Vorgehensweisen, bei denen man als Angreifer versucht, über verschiedene Kanäle und Quellen Informationen über das potentielle Opfer zu sammeln bzw. sich durch Vorspielen gefälschter Tatsachenbehauptungen und geschickter Ausnutzung menschlicher Schwächen das Vertrauen der Zielperson zu erschleichen.

„Phishing“ ist ein Kunstwort aus „Passwort“ und „Fishing“ (fischen) und beschreibt Angriffsszenarien, bei denen man versucht, aus einem Datenstrom gezielt Passwörter bzw. Zugangskennungen herauszufischen bzw. abzugreifen, um sie anschließend für eigene (illegale) Zwecke zu nutzen.

Der Artikel beschäftigt sich im Schwerpunkt mit den Wegen und Werkzeugen mit denen versucht wird, Daten zu stehlen, wie diese funktionieren und wie man sich gegen derartige Angriffe schützen kann. Am Beispiel von Facebook, PayPal & Co wird gezeigt, wie derzeit gängige Phishing-Attacken ablaufen und wie man sie erkennen kann. Hierbei werden zum einen Angriffe im Internet gezeigt und zum anderen – wesentlich gefährlichere und schwerer abzuwehrende – Kompromittierungsversuche im lokalen Netzwerk (LAN[i]/WLAN[ii]) besprochen.

Hinweis zu Marken- bzw. Firmennamen

Die im Artikel verwendeten Namen wie PayPal, Facebook, UPS, DHL, Visa, MasterCard usw. sind allesamt eingetragene Marken der jeweiligen Eigentümer. Deren Nennung erfolgt exemplarisch, u.a. weil die Beispiele dadurch nicht nur plastischer werden, sondern weil diese Systeme und Firmen tatsächlich beliebte Angriffsziele der Hacker sind.

Das wiederum heißt nicht, dass diese Systeme besonders unsicher sind. Vielfach können die Unternehmen gar nichts für die Attacken und sind selber Opfer der teilweise systembedingten Angriffsszenarien.

Das bedeutet andererseits natürlich auch nicht, dass gerade diese Firmen ihre Anstrengungen nicht noch verstärken könnten, ihre Systeme sicherer zu machen bzw. die Angriffsmöglichkeiten einzuschränken. Da gibt es viel zu tun, denn im Internet herrscht bereits Krieg (neudeutsch CyberWar).

Zielgruppe

Dieser Artikel richtet sich gleichermaßen an Computer-Anwender als auch an IT-Sicherheitsbeauftragte und Administratoren und bietet in der täglichen Praxis anwendbare Sicherheitshinweise und empfohlene Verhaltensweisen, um sich und seine Computer vor einer missbräuchlichen Nutzung durch Dritte zu schützen und Gefahren durch Identitätsdiebstahl bzw. Kompromittierung von persönlichen Daten zu vermindern. Der interessierte Leser findet in den vertiefenden Kapiteln fachlich fundierte Informationen zur Funktionsweise der behandelten Angriffsszenarien mit dem Ziel, sich und andere gegen Gefahren durch Identitäts- bzw. Datendiebstahls wirksam zu schützen.

Abgrenzung

Die im vorliegenden Dokument beschriebenen Mechanismen und Konzepte können natürlich auch von der „dunklen Seite der IT“ als Anleitung verstanden oder benutzt werden, wie man einen Angriff auf fremde Daten konzipiert. Dies ist nicht die Intention des Autors bzw. des Fachaufsatzes und mutmaßlich für erfahrene Hacker überflüssig. Jeder, der dieses oder vergleichbares Wissen dazu nutzt, sich unbefugt Daten Dritter zu bemächtigen, sollte sich jedoch bewusst machen, dass jede konkrete Aktion zum Überwinden von fremden Schutzmaßnahmen, ein Eindringen in IT-Systeme anderer oder das Abschöpfen von persönlichen Daten bereits eine strafbare Handlung darstellt. Datendiebstahl oder gar das Ausnutzen der gestohlenen Daten, um sich zu bereichern, ist kein Kavaliersdelikt und auch kein Sport!

Der Autor

Der Autor - Dipl.-Ing. Thomas Käfer - beschäftigt sich seit mehr als zwei Jahrzehnten professionell mit dem Werkzeug „Computer“ und hier seit geraumer Zeit mit dem Aspekt der IT-Sicherheit und der Digitalen Forensik. Seit dem Wintersemester 2012 bildet er sich nebenberuflich im Rahmen des Masterstudiengangs Digitale Forensik an der Hochschule Albstadt-Sigmaringen in diesem Bereich aktiv und intensiv weiter. Im Studium und bei der täglichen Arbeit als öffentlich bestellter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung bzw. IT-Consultant wird er regelmäßig mit unterschiedlichen Aspekten der missbräuchlichen Nutzung der EDV konfrontiert. Kernaufgabe als Sachverständiger bzw. Forensiker ist die Aufdeckung von Delikten, bei dem der Computer zur Waffe bzw. Ziel eines Angriffes geworden ist.

Grundlagen

Das Kapitel Grundlagen behandelt das Grundprinzip des Social-Engineerings sowie des Phishings und welche Maßnahmen vermeiden helfen, Opfer einer entsprechenden Attacke zu werden.

Grundprinzip des Phishings

Eine Phishing-Attacke zielt immer darauf ab, in den Besitz persönlicher Daten des Opfers zu gelangen. Das kann z.B. dadurch erfolgen, dass Daten mitgelesen werden, während sie vom Opfer an das Zielsystem gesendet werden oder dass der Angreifer versucht, die Dateneingabe bzw. das Senden der Daten auf ein System des Angreifers umzuleiten. Je nach Art des Angriffs erhält der Täter direkt die Nutzdaten oder „nur“ die Zugangsdaten, um sich in einem zweiten Schritt durch Einloggen in das Zielsystem der Nutzdaten zu bemächtigen und entsprechenden Schaden anzurichten.

Motivation und Ziel des Angreifers

Der oder die Angreifer verfolgen bei einer Phishing-Attacke unterschiedliche Ziele. Die „harmloseste“ Sorte ist diejenige, die aus „sportlichen“ Gründen versucht, in fremde Systeme einzudringen, um sich zu profilieren oder im besten Fall Schwachstellen von Systemen und Anwendungen mit dem Ziel aufzudecken, diese Sicherheitslücken zu schließen. Sofern keine ausdrückliche Erlaubnis bzw. gar ein Auftrag für einen sogenannten Pentest vorliegt, ist dieser jedoch genauso illegal wie ein Angriff, der auf die missbräuchliche Nutzung der Daten ausgerichtet ist. Man kann davon ausgehen, dass der aktive Versuch, eine offensichtlich vorhandene Schutzmaßnahme zu überwinden, bereits eine strafbare Handlung darstellt.

Beispiel: Ist ein Funknetzwerk (WLAN) durch eine wie auch immer geartete Verschlüsselung gesichert, so ist bereits der Versuch, diese Verschlüsselung bzw. das Login ins Netzwerk zu überwinden, eine unzulässige Handlung.

Die meisten Hackversuche zielen jedoch darauf ab, Daten zu verändern (z.B. Postings in Facebook), Daten heimlich mitzulesen (zum Ausspähen von Personen) oder für eigene Zwecke zu missbrauchen (wirtschaftlicher Schaden durch Warenbestellung unter fremden Namen oder Diebstahl von Geld in Online-Bezahlsystemen).

Hat ein Hacker, z.B. im Rahmen einer Phishing-Attacke, den Benutzernamen und das Passwort zu einem fremden System erhalten, so kann er i.d.R. dieselben Aktionen durchführen, wie der Eigentümer des Accounts. D.h., er kann zum Beispiel auf alle Daten in sozialen Netzwerken zugreifen und Nachrichten bzw. Postings im Namen und mit der Identität des Eigentümers verfassen. Das ist im günstigen Fall peinlich für das Opfer, kann aber auch schwerwiegende Folgen haben (man denke zum Beispiel an rufschädigende Aussagen).

Sind die Zugangsdaten von einem Online-Shop (Ebay, Amazon o.ä.) in fremde Hände gelangt, so kann der Täter Ware im Auftrag und auf Rechnung des Opfers ordern und bei geschickter Manipulation der Lieferadresse zu sich umleiten.

Hat er erst einmal Zugriff auf das Shop-Konto des Opfers, so wird er die Benachrichtigung über Transaktionen (i.d.R. per E-Mail) abschalten bzw. auf eigene E-Mail-Adressen umleiten, damit das Opfer nicht sofort über verdächtige Aktionen informiert wird.

Die weitreichendsten Folgen hat die Kompromittierung eines Online-Banking-Kontos (Bank, Kreditkarte oder Bezahlsysteme wie z.B. PayPal). Sind Überweisungen (Transaktionen) in einem solchen System nicht durch wirksame zusätzliche Schutzmechanismen abgesichert, auf die nur das Opfer Zugriff hat, so kann ein Angreifer leicht kleine und große Beträge auf Konten überweisen, auf die er Zugriff hat.

Bei Transaktionen mittels Kreditkarte oder PayPal werden i.d.R. keine sekundären Bestätigungsmechanismen (z.B. TAN[iii]-Listen bzw. Generatoren oder Two-Factor-Authentifizierung[iv]) eingesetzt, sodass allein die Kenntnis der Karten- bzw. Kontodaten eine Überweisung auslösen kann. Als Geschädigter ist man dann erst einmal in der Pflicht zum Nachweis, dass die Transaktion von einem fremden Dritten vorgenommen wurde und nicht durch einen selbst und man ist auf die Kulanz des Payment-Dienstleisters angewiesen.

Phishing im Internet

In diesem Kapitel wird erklärt, wie eine Phishing-Attacke abläuft, wenn der Angreifer nicht im lokalen Netzwerk, sondern „draußen“ im Internet lauert.

Funktionsweise

Beim Passwort-Fischen oder neudeutsch „Phishing“ versucht ein Angreifer durch Mitlesen des Datenstromes oder Umleiten der Benutzereingabe an die Login-Daten (Benutzerkennung und Passwort) eines potentiellen Opfers zu gelangen.

Wesentlich häufiger als eine personalisierte Phishing-Attacke, bei dem der Angreifer ein bestimmtes Opfer im Visier hat, sind massenweise versandte Phishing-Attacken anzutreffen. Das liegt vor allem daran, dass es technisch viel aufwändiger ist, eine bestimmte Person im Datenverkehr des Internets zu finden und zu belauschen, als einfach massenweise Fallen aufzustellen und sich überraschen zu lassen, wer in selbige tappt.

Daher wird sich ein Angreifer in der Regel (zumindest im Internet) kaum die Mühe machen, eine Datenkommunikation zwischen einem konkreten Opfer und einem Zielsystem abzuhören (weil er das meistens gar nicht kann), sondern automatisiert Da-

ten über seine Fallen zu sammeln und diese anschließend (offline bzw. zeitversetzt) auszuwerten und zu nutzen.

Konkrete Beispiele

Es gibt eine Vielzahl von Angriffs- und Missbrauchsszenarien im Kontext des Phishings. Exemplarisch seien einige beliebte und gebräuchliche Methoden nachfolgend erläutert.

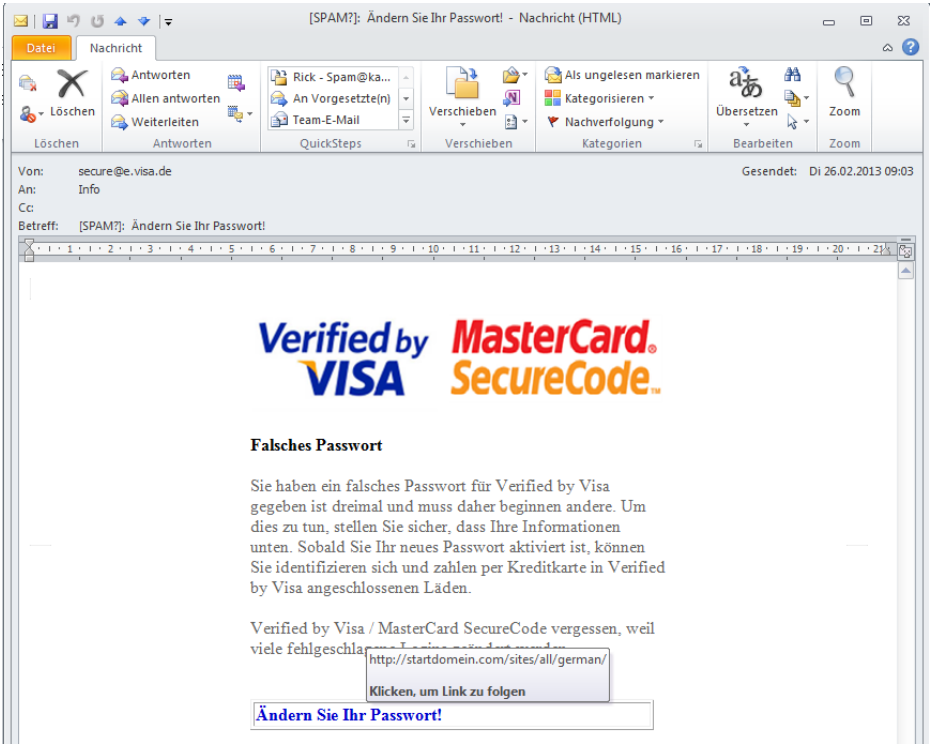
Kreditkarten

Der missbräuchliche Zugriff auf Kreditkarten-Informationen ist schon fast ein Klassiker. Das liegt daran, dass Kreditkarten als Zahlungsmittel international eine breite Akzeptanz und hohe Verbreitung besitzen und vergleichsweise schlecht gegen eine missbräuchliche Nutzung gesichert sind. Die für die Bezahlung mittels Kreditkarte nötigen Informationen stehen im Klartext lesbar auf Vorder- und Rückseite der Karte und werden im Online-Zahlungsverkehr über Webbrowser i.d.R. nicht elektronisch ausgelesen (Magnetstreifen), sondern müssen vom Menschen per Hand eingetippt werden. Bei der Online-Zahlung erfolgt nun lediglich eine Plausibilitätsabfrage beim Kartendienstleister, ob die Daten valide (gültig) sind und der dreistellige „Sicherheitscode“ auf der Rückseite korrekt eingegeben wurde. Danach erfolgt die Freigabe der Zahlung. Manchmal wird eine zusätzliche Freigabe über ein Online-Passwort erwartet, was jedoch auch keinen wesentlichen Schutz darstellt, wenn die Benutzerdaten über eine Phishing-Attacke mitgelesen wurden.

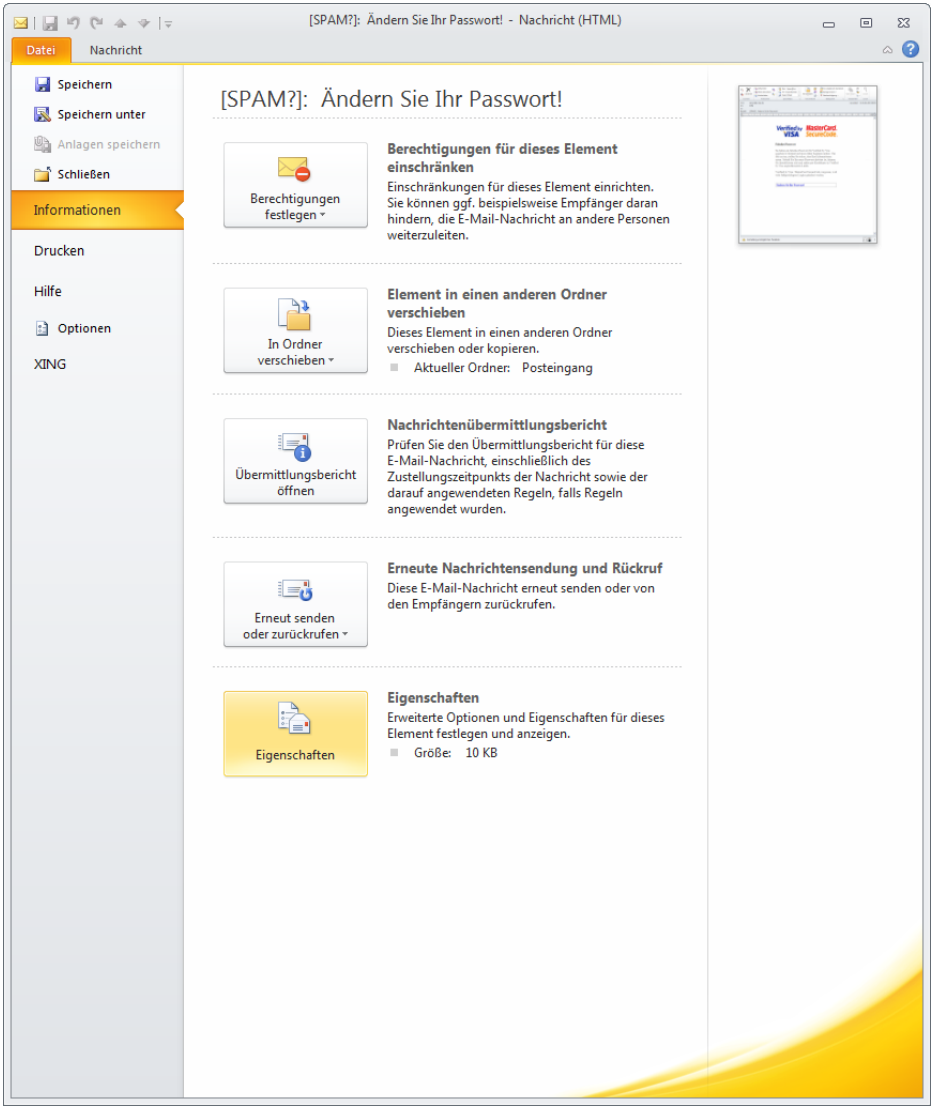
Der Angriff auf Kreditkartendaten wird meistens durch massenweise versendete E-Mails eingeleitet, bei dem die Opfer angeblich aus Sicherheitsgründen ihre Kartendaten überprüfen sollen (z.B. weil angeblich ein Missbrauch der Kartendaten festgestellt wurde). Die Attacke funktioniert trotz Streuverlusten deshalb gut, weil eben viele Menschen eine Kreditkarte eines gängigen Kreditkartenanbieters besitzen.

Eine solche E-Mail sieht dann z.B. so aus:

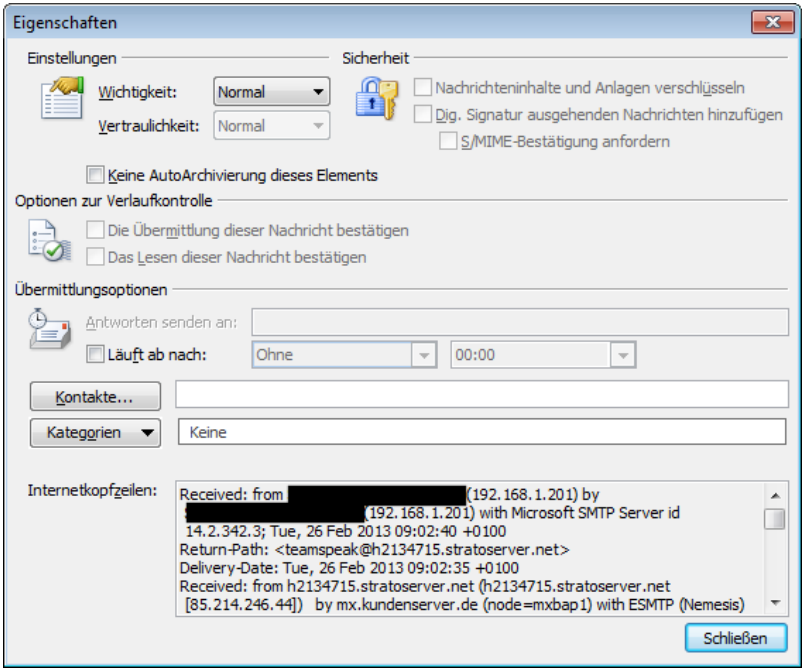
Was fällt hierbei alles auf? Zum einen hat offenbar der SPAM[v]-Filter angeschlagen und die Nachricht bereits als SPAM klassifiziert (1). Auch die Absender-Adresse sollte stutzig machen (Domain e.visa.de (2)). Spätestens das schlechte Deutsch und die katastrophale Satzstellung sollte das potentielle Opfer nun warnen (3). Und wenn das nicht reicht, dann hilft ein Blick auf die URL[vi] (4), die hinter dem Text „Ändern Sie Ihr Passwort“ liegt (Mauszeiger darüber halten, aber nicht darauf klicken). Die hier im Beispiel gezeigt URL „startdomein.com/sites/all/german“ hat sicherlich nichts mit den Kartenunternehmen VISA oder MasterCard zu tun.



Man kann bei weniger offensichtlichen Hinweisen auch genauer nachschauen, was es mit der E-Mail im Detail auf sich hat. Jedes E-Mail-Programm bietet die Möglichkeit, den sogenannten Header der Nachricht anzuzeigen (in Outlook 2010 z.B. über Datei/Informationen/Eigenschaften:



Im Feld „Internetkopfzeilen“ findet man nun detaillierte Informationen über den Absender und den Übertragungsweg:



Ob Visa wohl seine Kommunikation über

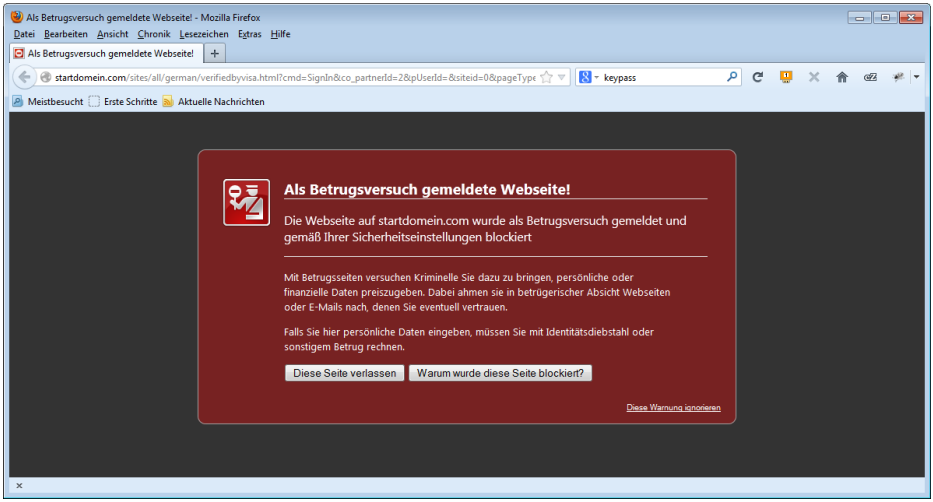
```
Return-Path:
<teamspeak@h2134715.stratoserver.net
```

abwickelt? Wohl kaum.

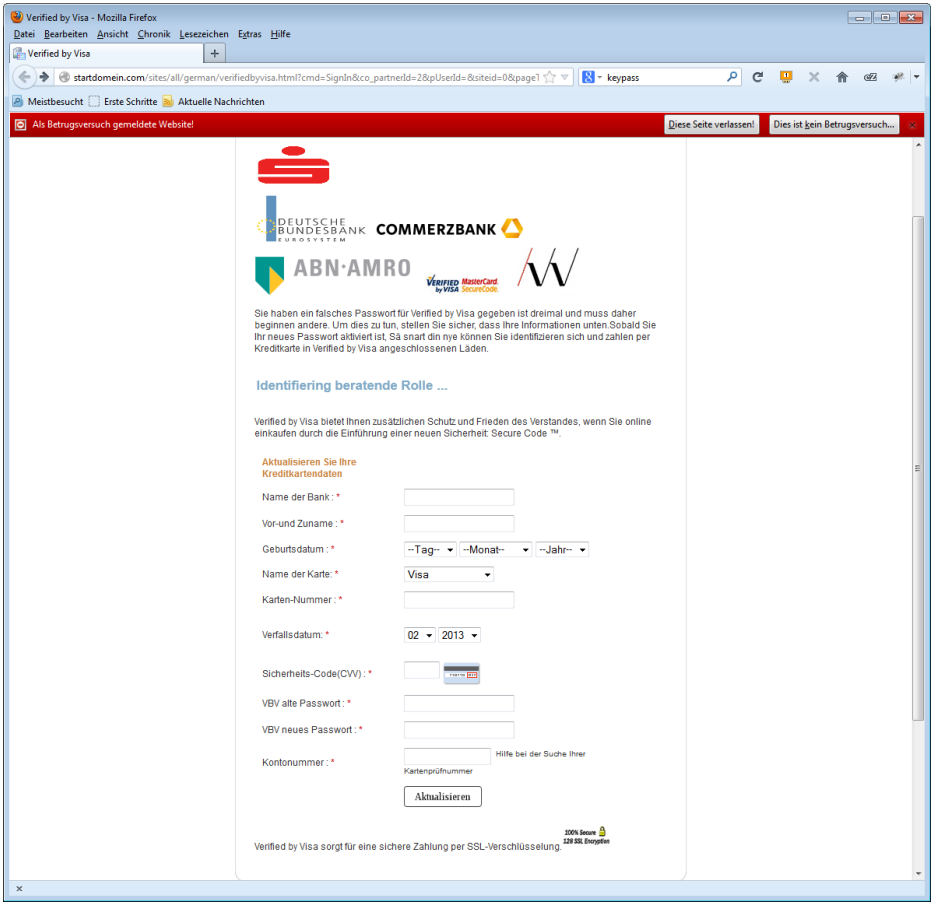
Wer jetzt immer noch glaubt, dass es sich um eine offizielle und wahre Warnung des Kreditkartenanbieters handelt, der sollte die echte URL von Visa oder MasterCard (z.B. über eine Suchmaschine wie Google ermittelt) aufrufen und sich tatsächlich einloggen. Wobei – auch hier lohnt sich ein Nachdenken: Kann man sich eigentlich sinnvoll direkt bei MasterCard & Co auf sein Kreditkartenkonto einloggen und müsste man dort seine gesamten Kartendaten eingeben? Wohl kaum!

Meist ist die Kreditkarte mit einem Girokonto der Hausbank gekoppelt und man muss sich bei der Hausbank einloggen, um die eigenen Kreditkartenumsätze abrufen zu können.

Wer den Link dann doch anklickt und nicht gerade zu den ersten Opfern gehört, wird ggf. wenigstens gewarnt (meist nach 1-2 Tagen, nachdem die Massenmail in Umlauf kam):



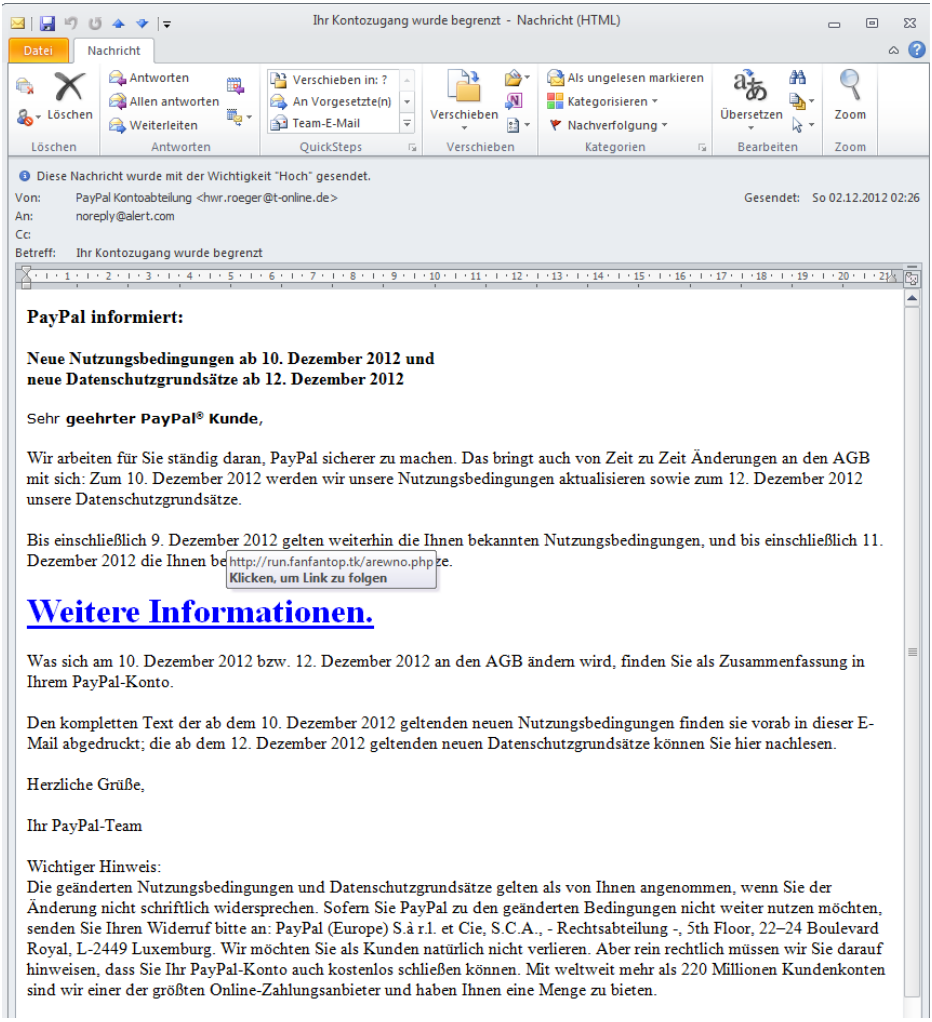
Wer jetzt (trotz Warnung und radebrechendem Deutsch auf der Zielseite) dennoch seine gesamten Kreditkarten eingibt (die Visa doch kennt…), dem ist nicht mehr zu helfen. Glückwunsch jedoch an den Täter. Er besitzt nun alle Kreditkartendaten incl. „Sicherheits-Code“ und kann nun auf Kosten des Opfers shoppen gehen:



PayPal

Sehr beliebt sind auch Phishing-Versuche auf PayPal-Accounts, weil dieses Zahlungssystem ebenfalls einen hohen Verbreitungsgrad hat.

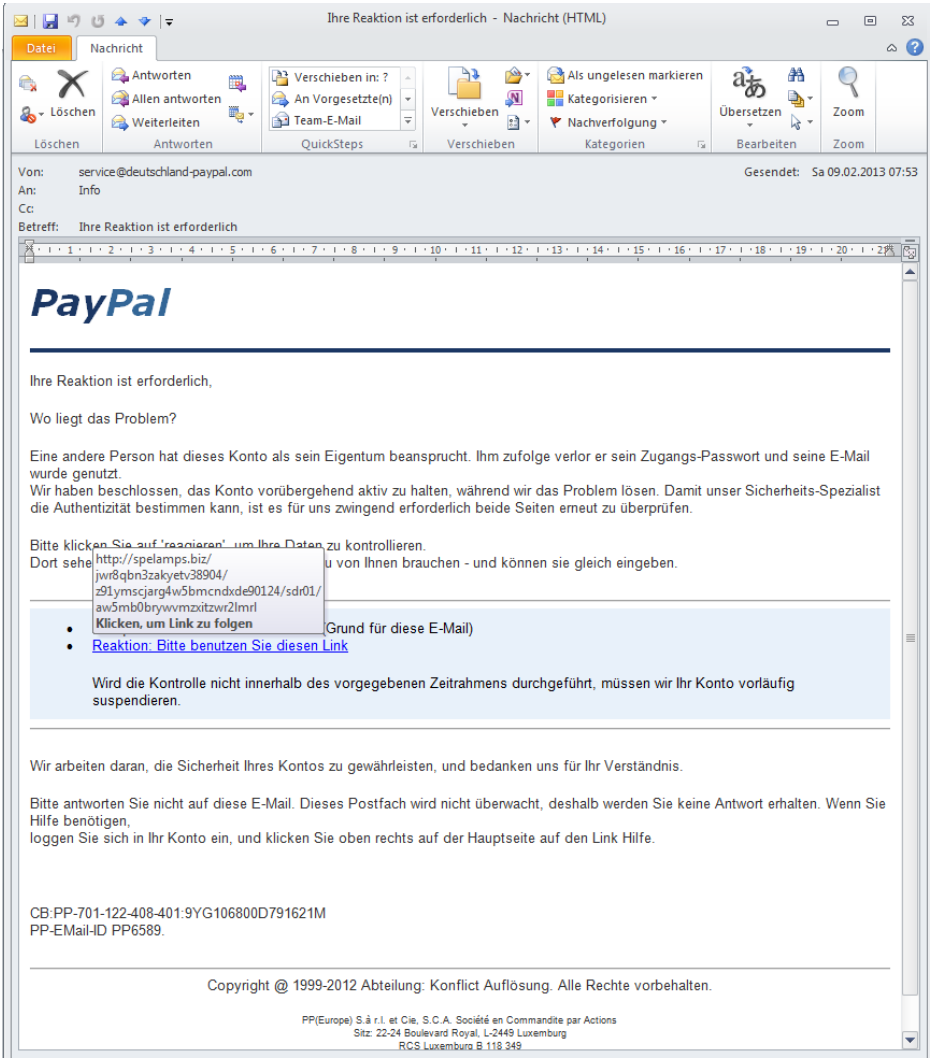
Eine Version sieht z.B. so aus und scheint total harmlos zu sein, enthält sie doch nur einen Link zu (angeblich) weiteren Informationen:



Aber wird PayPal wohl seine Kunden über eine E-Mail-Adresse hwr.roeger@t-online.de informieren und warum steht im Feld „An“ norepoly@alert.com?

Auch im nächsten Beispiel erhält das Opfer i.d.R. eine mehr oder weniger gut gemachte E-Mail mit der Aufforderung, sein PayPal-Konto wegen illegaler Aktivitäten umgehend zu prüfen.

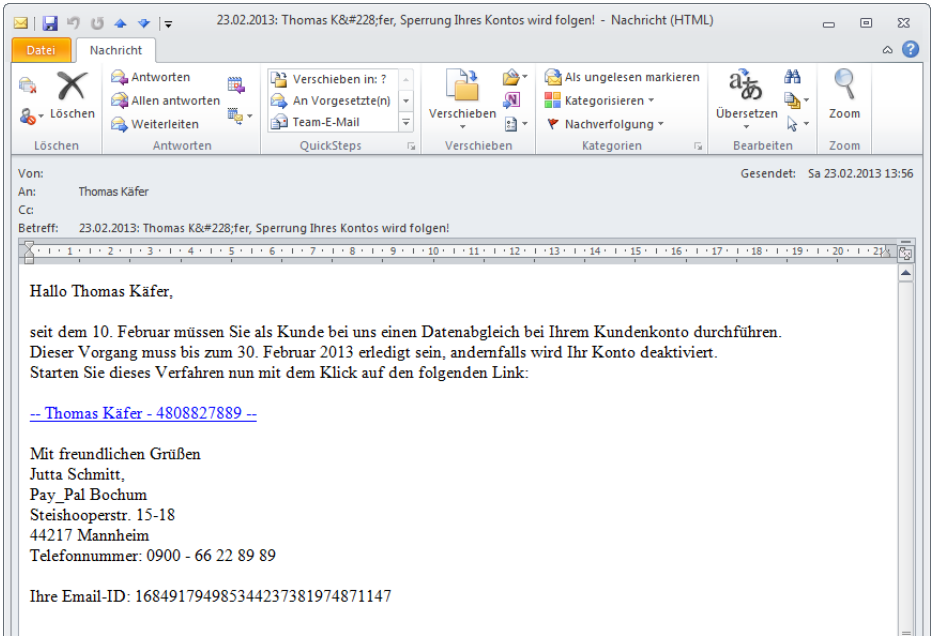
Meist wird der Aufforderung mit einer Drohung Nachdruck verliehen, dass das Konto ansonsten umgehend gesperrt wird.



Hier war der Täter wenigstens einigermaßen der deutschen Sprache mächtig und hat sich mehr Mühe gegeben, der Nachricht ein offizielles Aussehen zu geben.

Aber auch hier ist die Absender-Adresse service@deutschland-paypal.com genauso verdächtig, wie der hinter den Text hinterlegte Link http://spelamps.biz...

Manchmal bekommt man auch solche E-Mails:



In diesem Beispiel fällt neben der unprofessionellen Aufmachung auf, dass Umlaute teilweise nicht korrekt codiert wurden (siehe Betreff-Zeile) und dass offenbar bewusst nicht das Wort „PayPal“, sondern „Pay_Pal“ verwendet wurde, damit SPAM-Filter nicht anschlagen.

Die Adresse Pay_Pal Bochum, die dann doch in Mannheim liegt, sollte auch stutzig machen, denn PayPal sitzt bekanntermaßen in Luxemburg. Am schönsten ist jedoch die gesetzte Frist:

Manche Hacker sind so doof, dass sie noch nicht einmal den Kalender richtig lesen können oder haben Sie auf Ihrem Kalender schon einmal einen 30. Februar gefunden?

Sollte man nun triumphierend auf eine solche Mail antworten und dem Angreifer mal so richtig die Meinung sagen oder bei unverlangt zugesendeten SPAM-Werbe-Mails auf einen Link „Vom Newsletter abbestellen“ klicken?

Nein! Lassen Sie es bleiben. Sie bestätigen dem Versender damit allenfalls, dass die E-Mail-Adresse tatsächlich genutzt wird und Sie bekommen noch mehr solcher SPAM-Mails. Meist ist die Absender-Adresse sowieso gefälscht bzw. die Nachricht landet bei einem anderen Opfer, nämlich dem über dessen E-Mail-Konto die Nachrichten (illegal) versendet worden sind.

Was passiert nun aber, wenn man dem Link folgt, der tatsächlich etwas anderes enthält, als der Titel glauben machen will?

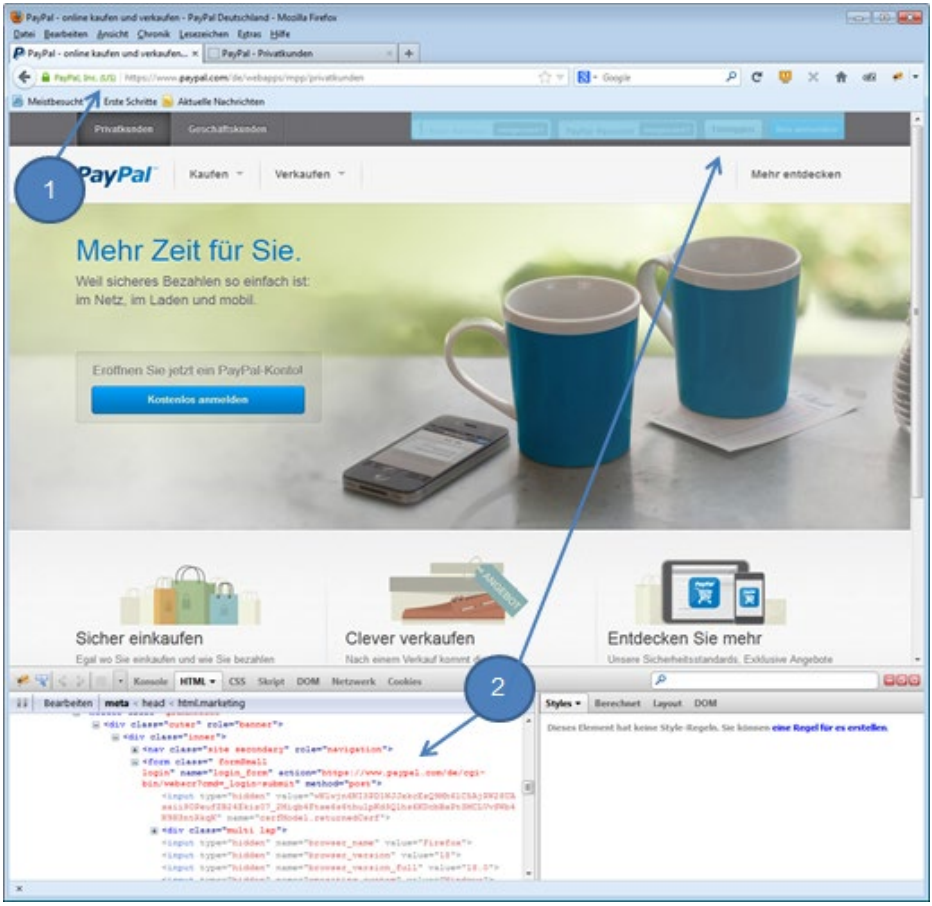
Der Link -- Thomas Käfer - 4808827889 – führt zu
http://www.pllove.de/components/7623039635/3853935958353/ .

Man gelangt (scheinbar) auf die Anmeldeseite von PayPal:

Auf den ersten Blick könnte es sich um die offizielle PayPal-Seite handeln. Tatsächlich ist diese Seite eine nur leicht modifizierte Kopie der echten Seite. Allein die URL muss stutzig machen: Was hat www.pllove.de mit PayPal zu tun? Nichts! Was würde nun passieren, wenn man in das Feld „E-Mail-Adresse“ und „PayPal-Passwort“ seine echten User-Credentials eingeben würde? Die Daten würden vom Angreifer gespeichert und man würde anschließend möglicherweise sogar zur echten PayPal-Seite durchgereicht. Dort würde man nichts Verdächtiges feststellen (Was auch?) und die Seite wieder verlassen.

Der Angreifer loggt sich nun ebenfalls mit Ihren Daten ein und überweist sich ein nettes Sümmchen auf ein Konto auf den Cayman Islands. Besonders perfide ist, dass viele der auf der gefakten Seite enthaltenen Links tatsächlich auf die echte PayPal-Seite führen. Diese Links wurden vom Angreifer nicht ausgetauscht.

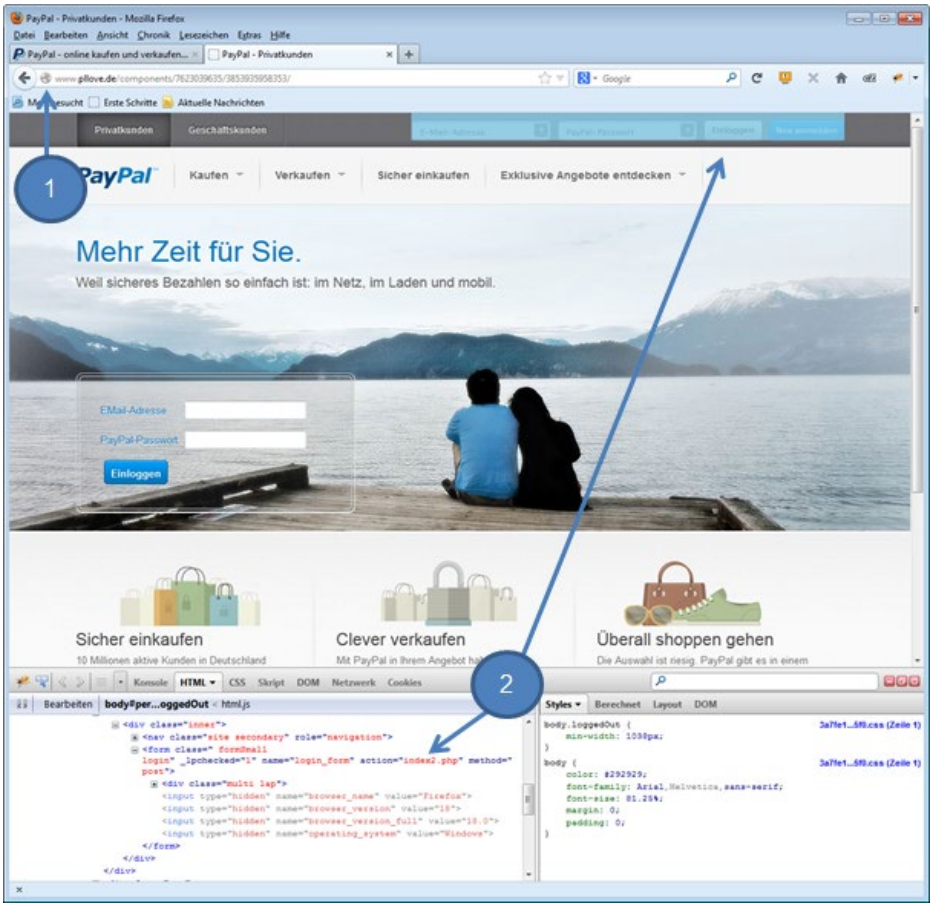
Er hat lediglich die Methoden rund um die Passworteingaben (das Login) verbogen, wie ein Blick in den Seitenquelltext der gefälschten Seite beim Vergleich zur echten Seite zeigt. Schauen wir uns zunächst die echte PayPal-Seite an. Auffällig ist schon einmal der erste Unterschied in der Adresszeile. Die echte PayPal-Seite ist SSL[vii]-verschlüsselt, was der Browser auch durch das grün hinterlegte Schloss und den Zusatz „https“ vor der Adresse entsprechend anzeigt (1).



Dass hier unterschiedliche Bilder und Inhalte in der Body-Section der Seite angezeigt werden, ist übrigens normal, da PayPal die Keyvisuals regelmäßig ändert und die PayPal-Seite heute schon wieder anders aussehen kann. Analysiert man nun z.B. mit dem Add-On Firebug (für den Firefox-Browser) die einzelnen DIV-Container der Seite, so erkennt man den Unterschied bei der sogenannten POST-Methode (2).

Auf der echten Seite wird nach Betätigen des Buttons „Einloggen“ die absolute URL „https://www.paypal.com/de/cgi-

bin/webscr?cmd=_login-submit“ aufgerufen (2). Auf der gefälschten Seite wird hingegen relativ zur aktuellen URL auf die Seite "index2.php" verwiesen.



Was passiert nun also im Detail? Der Login-Mechanismus ist in einem Formular gekapselt, welches u.a. die beiden Eingabefelder „E-Mail-Adresse“ und „Passwort“ und den Button „Einloggen“ beinhaltet.

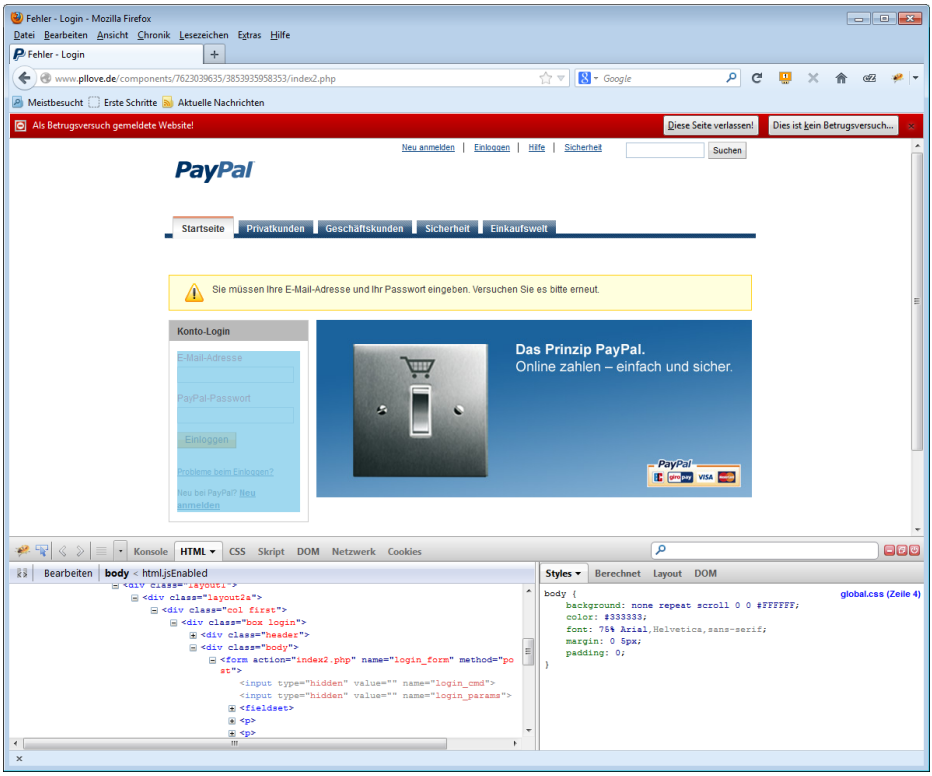
Mit dem Betätigen des Buttons „Einloggen“ wird nun die POST-Methode ausgelöst. Diese überträgt die Werte der Formularfelder als eigene Nachricht (für den Benutzer unsichtbar) an die aufgerufene Seite und die Werte können so Server-seitig ausgewertet werden. Bei der echten Seite führt das dazu, dass E-Mail-Adresse und Passwort mit den bei PayPal gespeicherten Daten verglichen werden und für den Fall einer Übereinstimmung der User Zugriff auf seine Daten erhält (eingeloggt ist). PayPal hat hier ein paar Sicherheitsmaßnahmen eingebaut.

So ist die URL der aufzurufenden Zielseite vollständig incl. HTTPS-Protokoll und Hostname www.paypal.com angegeben, um eine Umleitung zu erschweren. Zudem sind offenbar weitere teilweise versteckte bzw. codierte Felder und Werte enthalten, die ebenfalls übertragen werden. Der Server von PayPal überprüft auch diese Daten, die per POST-Methode übertragen werden und erkennt so, dass ein Login tatsächlich (bzw. wahrscheinlich) von einer der eigenen Seiten erfolgt ist.

Das Fälschen einer PayPal-Seite (und ähnlich aufgebauter Websites/Login-Mechanismen) und der Umbau zu einer Phishing-Seite ist jedoch trotzdem sehr einfach. Man ruft dazu einfach die originale Webseite auf und speichert diese als lokale Webseite auf dem eigenen Rechner ab (im Browser „Seite speichern unter“ / „als Webseite speichern“). Nun modifiziert man das Login-Formular. Im vorliegenden Beispiel hat der Angreifer die URL für die POST-Methode auf „index2.php“ geändert. Es handelt sich um eine relative Adresse, was man an dem fehlenden http://www... erkennt. Zudem ist hier nun keine SSL-Verschlüsselung aktiv. Der Webbrowser interpretiert die relative URL nun so, dass er einfach den aktuellen Hostnamen vor die URL setzt und daraus die gesamte Adresse aufbaut.

Da der Aufruf der gefakten Seite von der Basis-URL http://www.pllove.de/components/7623039635/385393 5958353/ erfolgte, wird nun die Zieladresse zu

http://www.pllove.de/components/7623039635/3853935958353/index2.php zusammengebaut. Diese führt jetzt auf eine (nun) ebenfalls als Betrugsversuch gemeldete Webseite:



Die Seite „index2.php“ ist ebenfalls von einer originalen PayPal-Seite abgeleitet und sorgt bei Eingabe des Benutzernamens / Passworts in der Box „Konto-Login“ für eine Endlos-Schleife, die immer wieder auf diese Seite verweist. Im Hintergrund werden dabei jedes Mal E-Mail-Adresse und Passwort protokolliert und der User wundert sich ggf. nur, warum seine Kontodaten nicht zu einem erfolgreichen Login führen.

Baut der Angreifer nun auch noch die versteckten Informationen der originalen PayPal-Seite in seine Phishing-Seite ein, so kann

er es ggf. sogar schaffen, nach dem Abgreifen der Daten den User erfolgreich an PayPal durchzureichen. Das scheint PayPal mittlerweile dadurch zu erschweren, dass die Seite Prüfsummen und eine bestimmte Anzahl von Leerzeichen im Seitenquelltext enthält, die beim Login ebenfalls überprüft werden. Damit wird das 100% Fälschen der Seite erschwert (aber nicht unmöglich gemacht).

Der Domain-Inhaber bzw. Betreiber (hier www.pllove.de) hat übrigens i.d.R. nichts mit einem solchen Angriff zu tun. Er dient nur als Hoster für die Phishing-Seiten und ist meist ebenfalls Opfer der Attacke (mindestens hinsichtlich seiner Reputation).

Wie einfach man die mittels POST übertragenen Variablen-Werte auswerten kann, wird später noch ausführlicher gezeigt.

Facebook

Ein weiteres beliebtes Angriffsziel ist Facebook. Warum? Weil derzeit allein ca. 25 Millionen Deutsche ein Facebook-Konto haben und ein Großteil davon dieses mehrfach am Tag nutzt. Weltweit ist etwa jeder 7. bis 8. Erdenbürger über Facebook vernetzt. Die Chance, per Massenmail einen potentiellen Facebook-Nutzer zu erreichen, geht damit in Richtung 50:50 (also minimale Streuverluste).

Auch hier verläuft ein Angriff ähnlich wie im Beispiel von PayPal. Dem Opfer wird eine gefälschte Facebook-Anmeldeseite untergeschoben und sein Passwort nach der Eingabe zwischengespeichert, bevor er auf die echte Webseite weitergeleitet wird. Der Angreifer hat nun eine gültige Kombination von E-Mail und Passwort für Facebook. Er könnte nun das Facebook-Konto übernehmen, was aber i.d.R. vollkommen uninteressant ist. Vielmehr wird er versuchen, mit demselben Benutzernamen/Passwort nun ein Login auf Ebay, PayPal oder einem sonstigen gängigen System in der Hoffnung versuchen, dass das Opfer zu faul war, verschiedene Logins zu benutzen.

Wie gefährlich und wie schwer zu erkennen eine solche Attacke z.B. auf eine Facebook-Seite im lokalen Netzwerk ist, wird in einem späteren Kapitel detailliert gezeigt.

Phishing im lokalen Netzwerk

Bisher haben wir nur Attacken betrachtet, bei dem der Angreifer (anonym) im Internet lauert und das potentielle Opfer erst dann zum tatsächlichen Opfer wird, wenn es sich im World Wide Web „bewegt“. Das Opfer genießt dadurch schon einmal eine gewisse Anonymität und verschiedene technische Mechanismen verhindern, dass ein Angreifer seine Attacke noch gezielter ausführen und perfekter tarnen kann.

Was ist aber, wenn der Täter bereits im eigenen Netzwerk sitzt?

Wir gehen bei der nachfolgenden Betrachtung davon aus, dass das Opfer ein wie auch immer geartetes Netzwerk betreibt, in dem ein oder mehrere Rechner über einen Router ans Internet angebunden sind.

Sie glauben, Sie haben kein Netzwerk? Haben Sie einen PC (oder ein Tablet) und ist dieses Gerät per LAN-Kabel oder via WLAN (Funknetzwerk) mit einem Router (das ist so eine kleine Kiste mit ein paar blinkenden LEDs in der Nähe Ihres Telefonanschlusses) verbunden? Dann haben Sie ein Netzwerk, denn bereits ein Endgerät, welches mit einem Router verbunden ist, spannt ein LAN auf und wird gerade dann, wenn es sich um eine Funkverbindung handelt, für Angreifer besonders interessant. Und wenn Sie so etwas tatsächlich nicht haben, nehmen Sie jedoch vielleicht mit Ihrem Smartphone oder Tablet-Computer an einem öffentlichen WLAN teil, nämlich dann, wenn Sie bzw. Ihr Gerät sich in einen öffentlichen HotSpot einloggen. Auch dann befinden Sie sich in einem lokalen Netzwerk. Ganz offensichtlich

nimmt Ihr Endgerät an einem LAN teil, wenn Sie sich in der Firma per Kabel oder Funk ins Netz „einklinken“.

Warum reiten wir nun auf dieser Sache herum? Ein Netzwerk besteht aus zwei oder mehreren Teilnehmern und die Anzahl der Teilnehmer ist i.d.R. zwar technisch limitiert, wer jedoch außer Ihnen noch im LAN aktiv ist, bekommen Sie üblicherweise gar nicht mit. Was ist, wenn es nun ein Angreifer geschafft hat, sich per WLAN in Ihr Netz einzuwählen oder per LAN-Kabel (legitimer) Netzteilnehmer ist? Dann ist Holland in Not!

Funktionsweise

Wie bekommt ein Angreifer Zugriff auf Ihr Netzwerk? Hier gibt es prinzipiell drei Wege:

1. Der Angreifer nutzt eine Schwachstelle Ihres Routers/Ihrer Firewall aus und stellt von außen (aus dem Internet) eine Verbindung zu Ihrem Netzwerk her. Wir gehen davon aus, dass er noch keinen Zugriff auf einen der Rechner, jedoch auf TCP/IP[viii]-Protokoll-Ebene genügend Rechte hat, den Netzwerkverkehr abzuhören (z.B. mittels Einbindung seines PC via VPN[ix] oder einem geöffneten Port und Vergabe einer gültigen IP-Adresse an sein Gerät).

Besonders gefährlich wird es, wenn der Angreifer bereits einen Rechner im Netz (z.B. mit einem Trojaner) übernommen hat und fernsteuern kann.

2. Der Angreifer hat sein Endgerät per LAN-Kabel mit Ihrem Netzwerk verbunden und ist gleichberechtigter Netzteilnehmer. Dazu muss er physikalisch in Ihrem Netzwerk (gleichbedeutend mit Ihrem Gebäude) „sitzen“. In einem großen Netzwerk mit frei zugänglichen Netzwerkdosen kein utopischer Gedanke.

3. Der Angreifer ist per WLAN mit Ihrem Netz gekoppelt bzw. Sie nutzen zusammen mit dem Angreifer ein öffentliches WLAN (z.B. am Flughafen, im Schnellrestaurant oder im Rahmen von Open-WLAN-Projekten).

Im Fall 1) erfolgt die Infizierung meist über einen eingeschleusten Trojaner, der z.B. per E-Mail-Anhang auf das Opfer-System gelangt ist und von dort aus eine Verbindung nach außen zum Täter aufgebaut hat. Der Täter kann sich irgendwo auf der Welt weit weg vom physikalischen Zugriff (auch der Strafverfolgungsbehörden) befinden und ist schwer zu fassen.

Bei 2) geht der Täter ein deutlich höheres Risiko ein, da er sich physikalisch im Gebäude befinden muss und es eine (mit Aufwand) nachvollziehbare physikalische Verbindung zwischen seinem Endgerät und dem Netzwerk gibt. Seine Risikobereitschaft wird jedoch mit extrem hoher Performance und den weitreichendsten Möglichkeiten bei seinen Hackattacken belohnt.

Die interessanteste Version des Angriffes ist in Fall 3) dargestellt. Der Angreifer muss sich nur in räumlicher Nähe des Netzwerkes befinden. Hier reicht es, den Angriff z.B. aus dem Auto im Abstand von 100m bis 300m vom WLAN-Router zu starten. Aber vielleicht sitzt der Hacker auch im Großraumabteil zwei Reihen hinter Ihnen.

Ein Wireless LAN hat eben den Vorteil, dass man keine physikalische Verbindung in Form eines Kabels braucht und man sich nur in Funkreichweite des Netzes befinden muss. Welche Hürden man wie zum Eindringen in ein privates bzw. gesichertes WLAN überwinden muss bzw. welche Gegenmaßnahmen es gibt, wird in Kapitel 0 noch genauer beschrieben.

Konkrete Beispiele

Für die nachfolgenden Beispiele gehen wir davon aus, dass der Angreifer in irgendeiner Form (siehe vorheriges Kapitel 0 (1)-(3) Zugriff auf das lokale Netzwerk erlangen konnte und nun mit seinem Endgerät „legitimer“ Teilnehmer im LAN ist.

Grundlage der meisten heute im Einsatz befindlichen Netzwerke ist das sogenannte TCP/IP-Protokoll oft noch im gebräuchlichen IPv4-Format. Es liegt im ISO/OSI-Referenzmodell[x] auf Schicht 4 bzw. 3 und im TCP-Modell auf Schicht 3 bzw. 2.

OSI-Schichtenmodell	TCP-Modell	Beispiel
Anwendung (7)	Anwendung (4)	HTTP/HTTPS, SMTP, FTP, LDAP u.a.
Darstellung (6)		
Sitzung (5)		
Transport (4)	Transport (3)	TCP, UDP u.a.
Vermittlung (3)	Internet (2)	IP, ICMP, IPSec u.a.
Sicherung (2)	Netzzugang (1)	Ethernet, MAC-Adressen u.a.
Bitübertragung (1)		

Die zu übertragenden Nutzdaten werden in Datenpakete verpackt und erhalten in jeder Schicht zusätzliche Header-Informationen. So wird beispielsweise in der Internet-Schicht dem Paket die IP-Adresse des Absenders und des Empfängers hinzugefügt. In der Netzzugangsschicht (im OSI-Modell in der Sicherungssicht) erfolgt dann das Zuordnen der sogenannten MAC-Adresse zum Paket bzw. der IP-Adressen. Die MAC-Adresse ist eine eigentlich weltweit eindeutige und nur einmal vergebene Hardware-Adresse, die der Netzwerkkarte eines Gerätes zugeordnet ist. Leider lässt sich auch die MAC-Adresse leicht fälschen. Sie besteht aus sechs Bytes (48 Bit), die i.d.R. hexadezimal durch einen Bindestrich oder Doppelpunkt getrennt notiert wird[xi] (Beispiel 00-0c-29-9e-3c-84).

Die Adressierung bzw. Versendung eines Datenpaketes im Netzwerk erfolgt letztlich über diese MAC-Adresse, auch wenn

der Anwender die Datenpakete mit DNS[xii]-Namen bzw. IP-Adressen versieht.

Damit die Netzteilnehmer wissen, welche IP-Adresse zu welcher MAC-Adresse gehört, gibt es das sogenannte ARP[xiii]-Protokoll mit entsprechenden ARP-Tabellen.

Meldet sich ein Rechner neu im Netzwerk an, so sendet er per Broadcast[xiv] (Senden an alle Netzteilnehmer des Segmentes) ein sogenanntes Gratuitous-ARP-Paket, also ein „gratis“ bzw. unaufgefordertes ARP-Paket mit seiner IP-Adresse und seiner MAC-Adresse. Alle Netzwerkteilnehmer, die diesen ARP-Broadcast „gehört“ haben, merken sich nun in ihrer lokalen ARP-Tabelle diese Zuordnung, falls sie zukünftig Daten mit diesem Teilnehmer austauschen müssen.

„Weiß“ ein Teilnehmer mal nicht, wie die MAC-Adresse zu einer IP-Adresse lautet, an die er ein Paket schicken soll, so „fragt“ er per Broadcast (u.a. den Router im Segment) nach dem entsprechenden Eintrag. Welcher Rechner diese Antwort liefert, ist nicht festgelegt (was ja der Angreifer beim ARP-Spoofing ausnutzt). Ist ein solcher Eintrag auch beim Standard-Gateway nicht vorhanden, so fragt das Standard-Gateway seinen nächsten Kommunikationspartner (Hop, z.B. der Internet Service Provider) nach der entsprechenden Information und leitet diese nachher an den anfragenden Netzteilnehmer zurück.

Sehr ähnlich verhält es sich mit DNS-Anfragen. Der Mensch kann sich Namen wie z.B. www.paypal.com besser merken, als die IP-Adresse (z.B. 23.53.178.234), abgesehen davon, dass es aufgrund von Load-Balancing-Mechanismen mehrere IP-Adressen für einen Host-Eintrag geben kann. Das Übertragen von Datenpaketen funktioniert aber, wie voran erläutert, nicht über die Host-Namen, sondern über IP-Adressen und dann letztlich über die zugehörigen MAC-Adressen.

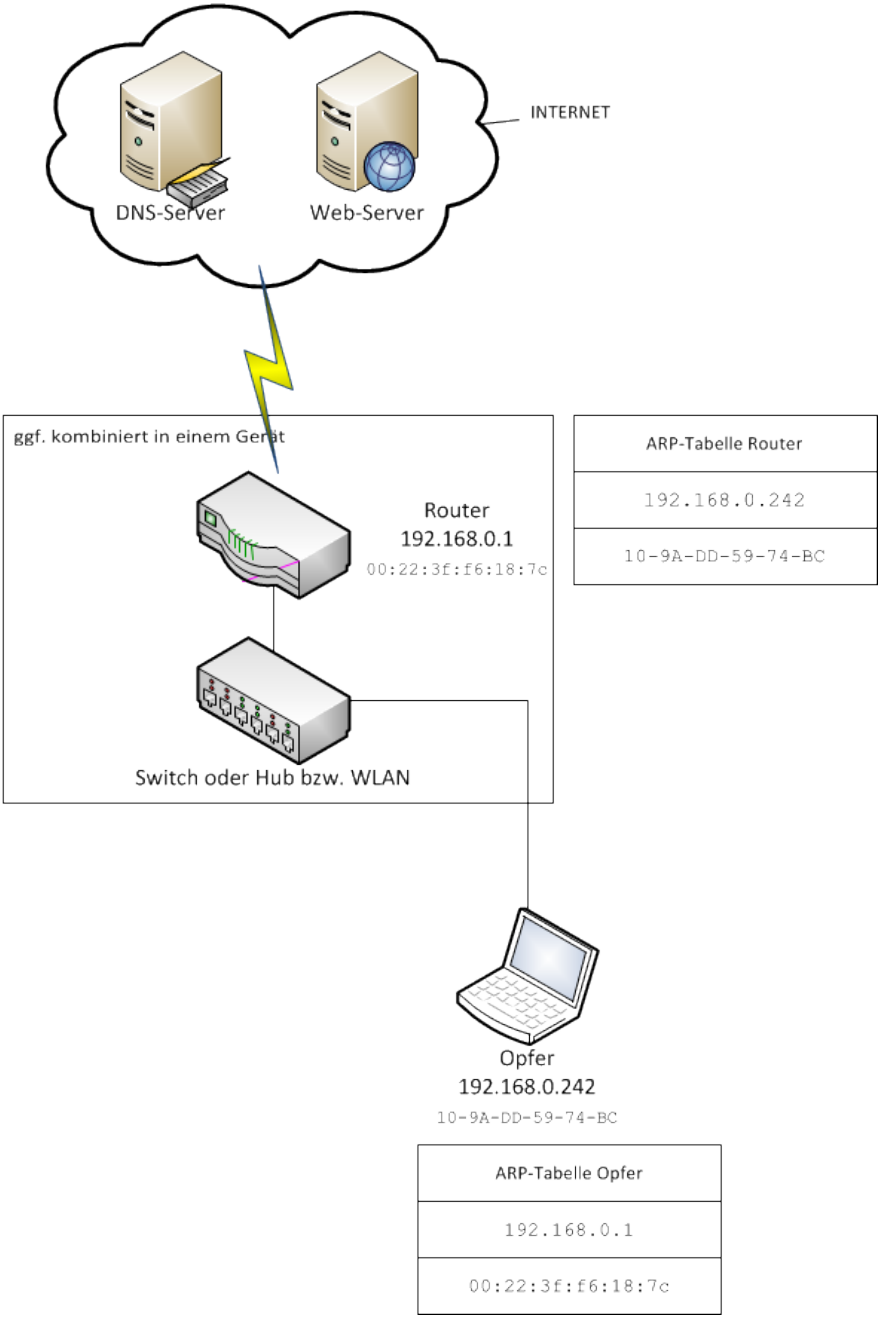
Per DNS-Zuordnung wird nun also www.paypal.com in die IP-Adresse 23.53.178.234 umgesetzt. Das erledigt ein lokaler DNS-Server (z.B. der Router, also das Standard-Gateway) oder dieser fragt solange bei den nächsten Hops nach, bis einer der DNS-Server im Internet die benötigte Information auflösen kann.

Weder das DNS- noch das ARP-Protokoll besitzen Sicherungsmechanismen, die sicherstellen, dass die Information, die gerade übertragen wurde, auch valide (unverfälscht) ist. Während man wenigstens beim DNS noch angeben kann, welcher Server die Namensauflösung übernehmen soll, ist das ARP-Protokoll vollkommen ungerichtet. Hier darf jeder Netzwerkteilnehmer die Antwort auf einen ARP-Request liefern und wer hierbei der schnellste ist, der „malt zuerst“. Das öffnet Angreifern natürlich Tür und Tor und wie einfach eine solche Attacke zu realisieren ist, zeigt das nächste Kapitel.

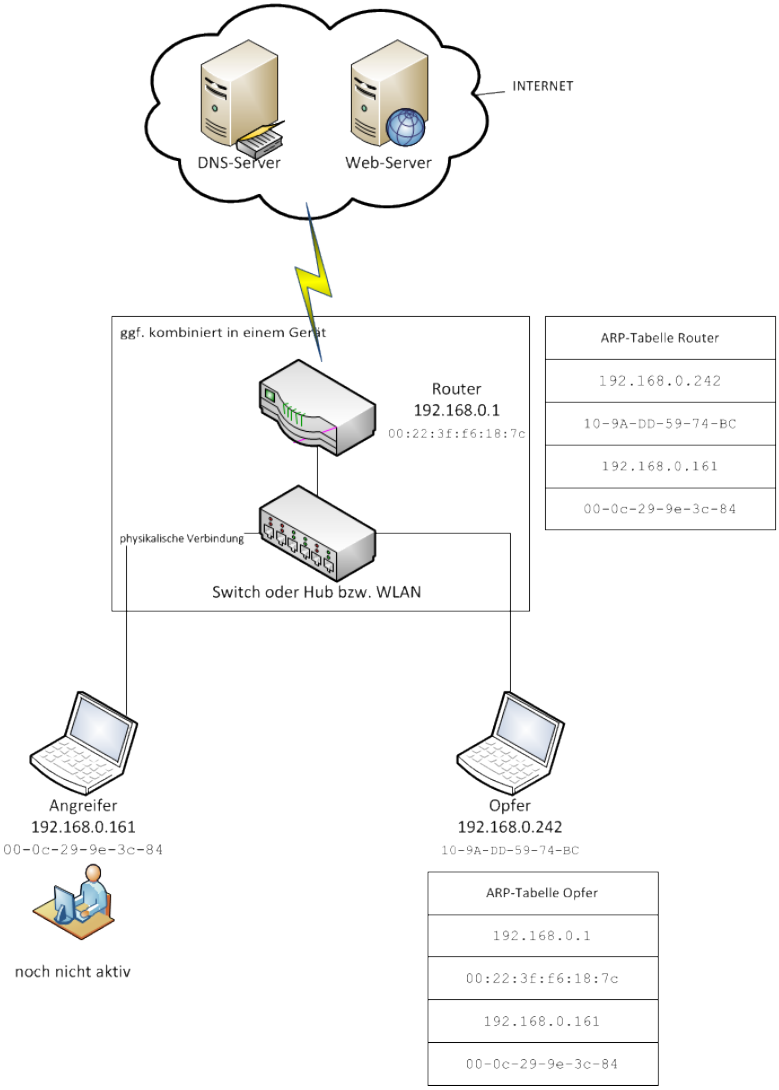
ARP- und DNS-Spoofing

Zunächst schauen wir uns die Ausgangssituation für ein ARP- und DNS-Spoofing[xv] an. Es handelt sich um ein einfaches Netzwerk mit einem Router (ggf. WLAN), der mit dem Internet verbunden ist und eine lokale DNS-Auflösung bereitstellt. Er verteilt die IP-Adressen an die lokalen Netzwerkteilnehmer per DHCP[xvi].

Die ARP-Tabelle des Routers enthält (neben weiteren Informationen) die korrekte MAC-Adresse und IP-Adresse des (späteren) Opfer-PC. Der Opfer-PC kennt die korrekte MAC-Adresse des Routers und dessen IP-Adresse. Alles ist gut.


INTERNET
DNS-Server
Web-Server
ggf. kombiniert in einem Gerät
Router
192.168.0.1
00:22:3f:f6:18:7c
Switch oder Hub bzw. WLAN
ARP-Tabelle Router
192.168.0.242
10-9A-DD-59-74-BC
Opfer
192.168.0.242
10-9A-DD-59-74-BC
ARP-Tabelle Opfer
192.168.0.1
00:22:3f:f6:18:7c

Nun verbindet sich der Angreifer mit dem Netzwerk und teilt seine MAC- und die per DHCP erhaltene IP-Adresse per Broadcast alle anderen Teilnehmern mit, die nun ihre ARP-Tabellen aktualisieren:



Jetzt beginnt der eigentliche Angriff. Der Angreifer verseucht nun die ARP-Tabellen des Opfer-PCs und des Routers so, dass die gesamte Kommunikation zwischen Opfer und Router über den PC des Angreifers erfolgt. Das erreicht er dadurch, dass er dem Opfer unaufgefordert ein Gratuitous-ARP-Paket sendet, in dem zur IP-Adresse des Routers die MAC-Adresse des Angreifers steht. Der Opfer-PC aktualisiert ungeprüft seine ARP-Tabelle und trägt zur IP-Adresse des Routers nun die falsche MAC-Adresse ein (nämlich die des Angreifers). Fortan verschickt das Opfer Datenpakte mit Ziel Router an den Angreifer-PC.

Dasselbe macht der Angreifer mit dem Router. Dem Router schickt er ein Gratuitous-ARP-Paket angeblich vom Opfer-PC mit der IP-Adresse des Opfers und der MAC-Adresse des Angreifers. Auch der Router aktualisiert nun seine ARP-Tabelle und wird Pakete für das Opfer ab sofort an den Angreifer schicken.

Da die ARP-Tabellen nach wenigen Minuten wieder automatisch aktualisiert werden, muss der Angreifer diesen Mechanismus ständig wiederholen, damit er die so genannten Race-Condition „gewinnt“. Er muss verhindern, dass die Netzteilnehmer wieder die Gelegenheit haben, ihre eigenen (echten) Daten im Netz zu übertragen. Solange er unentdeckt im Netzwerk sein Unwesen treiben kann, wird ihm das aber meist gelingen, es sei denn, die Manipulation der ARP-Tabellen bzw. die häufigen ARP-Broadcasts werden durch ein Intrusion Detection System (IDS) entdeckt. Besonders pfiffig ist der Angriff, wenn der Angreifer zunächst im Netzwerk die echten ARP-Broadcasts belauscht und auf diese Weise Informationen über die Teilnehmer sammelt. Er verzichtet hierbei auf das Senden der Gratuitous-Pakete, da das ja auffallen könnte. Stattdessen beantwortet er nach kurzer Zeit des Mithörens die Aktualisierungsabfragen der Teilnehmer in der Hoffnung, schneller zu sein als die eigentliche Quelle. Gewinnt der Angreifer diese Race Condition, so hat er gute Chancen, längere Zeit unentdeckt sein Unwesen zu treiben.

Technisch realisiert ein Angreifer dies z.B. mit einem frei erhältlichen Tool namens „arpspoof“. Dieses „Werkzeug“, welches unter LINUX arbeitet, wird über die folgenden drei Befehle aktiviert:

1. ARP-Tabelle des Angriffsziels manipulieren:

```
arpspoof -i eth0 -t 192.168.0.242 192.168.0.1
```

2. ARP-Tabelle des Standard-Gateways manipulieren:

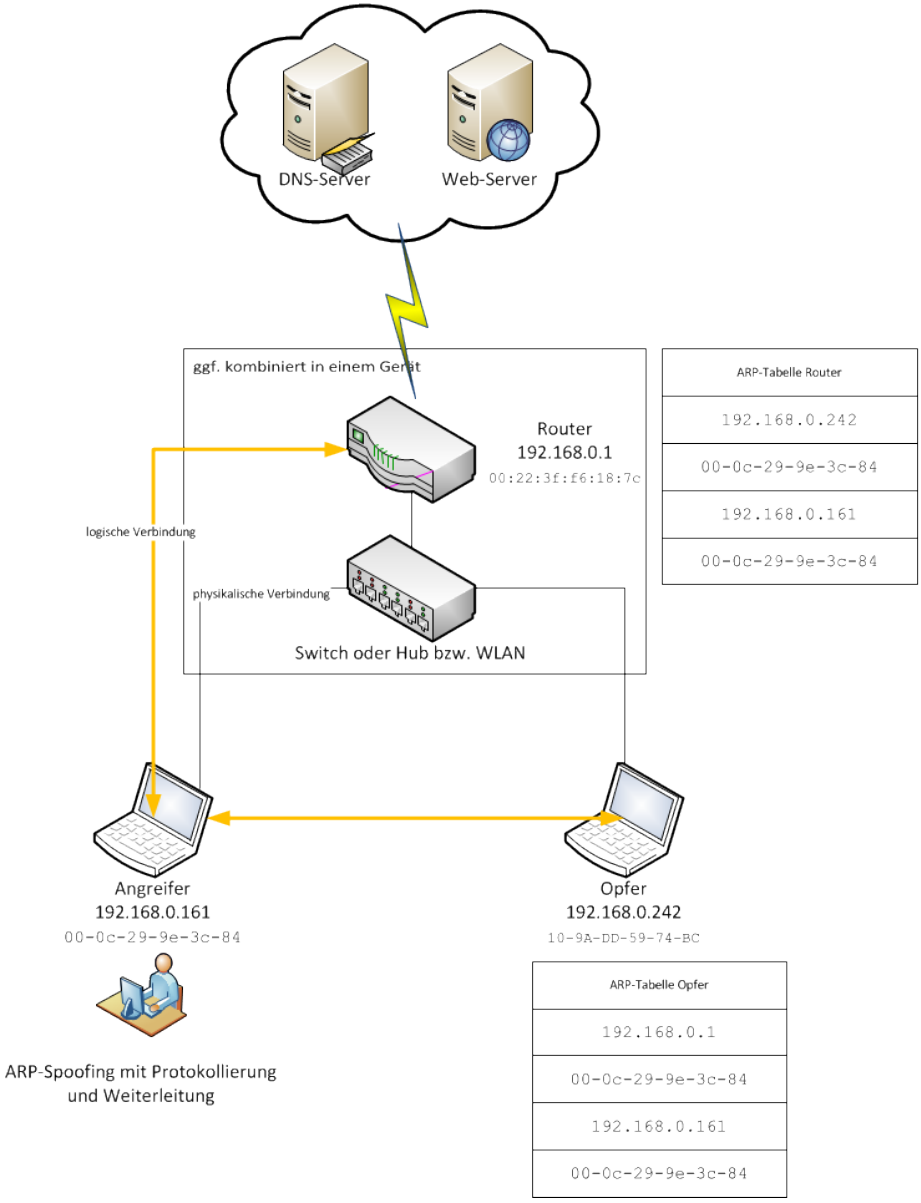
```
arpspoof -i eth0 -t 192.168.0.1 192.168.0.242
```

3. IP-Forwarding aktivieren:

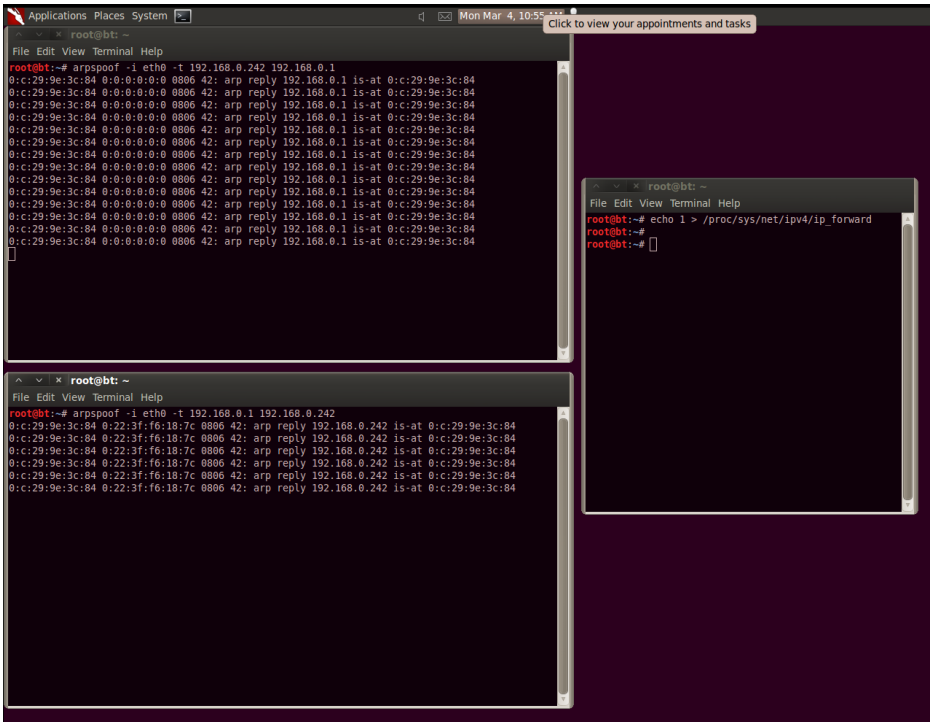
```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Das IP-Forwarding sorgt nun dafür, dass die Pakete, die vom Opfer-PC an den Router geschickt werden (und umgekehrt die Antworten), über den PC des Angreifers weitergeleitet werden. So kann der Angreifer alles mitlesen (und Daten manipulieren). Router und Opfer „merken“ jedoch nichts davon, da die Anfragen ja „korrekt“ durchgereicht werden.

Die ARP-Tabellen und der logische Datenfluss sehen jetzt so aus, wie in nachfolgender Abbildung gezeigt.


DNS-Server
Web-Server
ggf. kombiniert in einem Gerät
Router
192.168.0.1
00:22:3f:f6:18:7c
logische Verbindung
physikalische Verbindung
Switch oder Hub bzw. WLAN
ARP-Tabelle Router
192.168.0.242
00-0c-29-9e-3c-84
192.168.0.161
00-0c-29-9e-3c-84
Angreifer
192.168.0.161
00-0c-29-9e-3c-84
Opfer
192.168.0.242
10-9A-DD-59-74-BC
ARP-Spoofing mit Protokollierung
und Weiterleitung
ARP-Tabelle Opfer
192.168.0.1
00-0c-29-9e-3c-84
192.168.0.161
00-0c-29-9e-3c-84

Technisch erfolgt das Ganze auf einer LINUX-Maschine, die als Angreifer-PC dient. man erkennt die regelmäßigen ARP-Replies, die für das Verbiegen der Adressen notwendig sind und ständig wiederholt werden müssen und das Einschalten des IP-Forwarding:



Die Modifikation der ARP-Tabellen lässt sich auf einfache Weise mit einer Abfrage (ARP –a) der ARP-Tabelle auf dem Opfer-PC überprüfen. Die ARP-Tabelle (hier im Auszug) weist für zwei verschiedene IP-Adressen dieselbe MAC-Adresse auf (was eigentlich nicht sein dürfte).

```
  Internetadresse        Physische Adresse      Typ
  192.168.0.1            00-0c-29-9e-3c-84      dynamisch
  192.168.0.161          00-0c-29-9e-3c-84      dynamisch
```

Das Überprüfen der ARP-Tabellen stellt somit also schon einmal eine Möglichkeit dar, einen Verdacht des ARP-Spoofings zu erhärten.

Nun stellt sich die Frage, was der Angreifer mit diesem erfolgreich eingerichteten Szenario anstellen kann. Es handelt sich faktisch um eine klassische Man-In-The-Middle-Attacke, bei dem der gesamte Datenstrom zwischen Sender und Empfänger nicht nur mitgelesen, sondern auch modifiziert oder umgeleitet werden kann. Versuchen wir also einmal, an die Facebook-Login-Daten des Opfers zu gelangen. Dazu verfeinern wir den Angriff wie im Folgenden dargestellt.

Sniffen des Datenstroms

Zunächst könnte der Angreifer den Datenstrom mit einem Netzwerkscanner, wie beispielsweise Wireshark, im Klartext und bis auf Protokollebene mitlesen. Das funktioniert jedoch nur bei unverschlüsselter Datenübertragung. Sind die Datenpakete also z.B. mit SSL verschlüsselt und erfolgt ein Zugriff auf die Login-Maske einer Webseite mittels HTTPS-Protokoll, so sieht der Angreifer nur „Maumänner“. Solange der Angreifer sich nicht bereits in die Aushandlung des Schlüssels für die verschlüsselte Übertragung einklinken konnte, kennt er den zur Entschlüsselung nötigen Key nicht und sieht statt Klartext nur kryptischen Zeichencode, eben die besagten Maumänner.

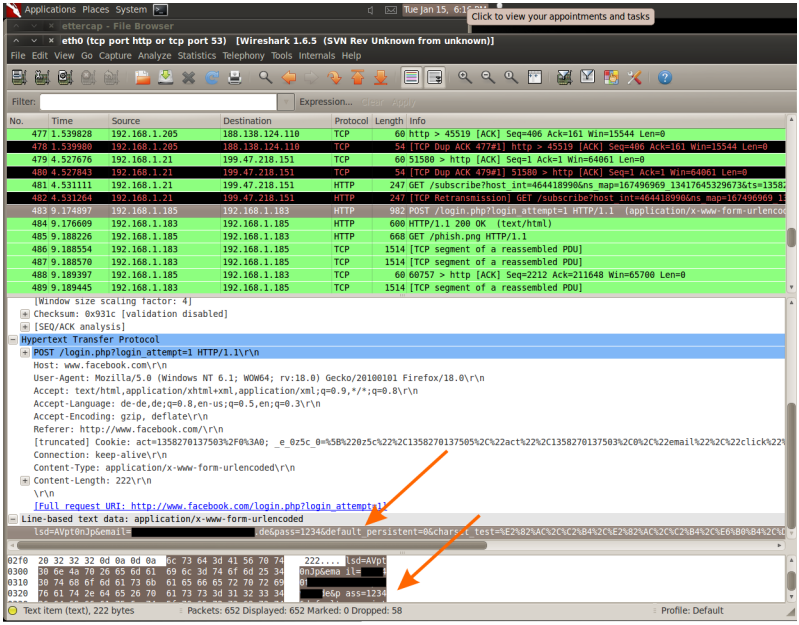
Nun gibt es dummerweise auch Möglichkeiten, die verschlüsselte Übertragung zu kompromittieren. In unserem Szenario wäre der Ansatz dazu, das ARP- bzw. DNS-Spoofing zu einem Zeitpunkt einzurichten, bevor das Opfer erstmalig auf die Ziel-Webseite zugegriffen hat. Dann würde der Angreifer sowohl mit dem Zielsystem als auch mit dem Opfer verschlüsselt kommunizieren. Dazu benutzt der Angreifer dann das originale SSL Zertifikat des Zielsystems und kommuniziert mit diesem ganz regulär über HTTPS.

Die für das Opfer bestimmten Daten verschlüsselt der Angreifer nun mit einem gefälschten SSL-Zertifikat im Namen des Zielsystems und je nach „Intelligenz“ des Opfer-PCs erkennt dieser die Modifikation nicht (oder zeigt sie zumindest nicht deutlich an).

Viele Systeme im Internet sind mittlerweile durchgängig auf HTTPS umgestellt worden und das Mithören damit deutlich erschwert. So ist z.B. die Facebook-Seite seit etwa November 2012 durchgängig per HTTPS erreichbar. Als das noch nicht der Fall war, bzw. bei Systemen, die Passwörter per HTTP transportieren, funktioniert ein Mit-Sniffen von Daten ganz hervorragend, wie folgendes Beispiel zeigt.

Es wurde hierbei der unverschlüsselte Datenverkehr beim Login in Facebook mitgelesen und nach dem Begriff „pass“ gesucht. Gezeigt wird ein Datenpaket, welches den Zugriff auf die Login-Seite und die Eingabe der Daten in die Felder E-Mail und Pass (für Passwort) beinhaltet. Das Feld „email“ enthält den Wert für die Benutzerkennung (im Bild unkenntlich gemacht) und das Passwort lautet offenbar „1234“.

Damit jetzt kein Leser auf die Idee kommt, die Credentials auszuprobieren, wurden die Angaben geschwärzt bzw. stimmen nicht mit dem echten Daten überein. Wer hierbei der Umrechnung von Hexcodes in ASCII-Zeichen mächtig ist, darf an diese Adresse natürlich gerne eine nette Nachricht schicken…



Verfeinerung des Angriffs mit ettercap

So ein Mit-Sniffen des Netzwerkverkehrs ist jedoch schlecht zu automatisieren und man erhält schon nach kurzer Zeit riesige Datenmengen. Deshalb wird ein Angreifer versuchen, nur die Quintessenz (nämlich die User-Credentials) abzugreifen und das Ganze zu automatisieren. Hierbei hilft ihm das ebenfalls frei erhältliche Tool „ettercap“, welches ebenfalls unter LINUX auf dem Angreifer-PC ausgeführt wird.

Ettercap erledigt das gesamte ARP- bzw. DNS-Spoofing und noch einiges mehr mit einer einzigen Befehlszeile:

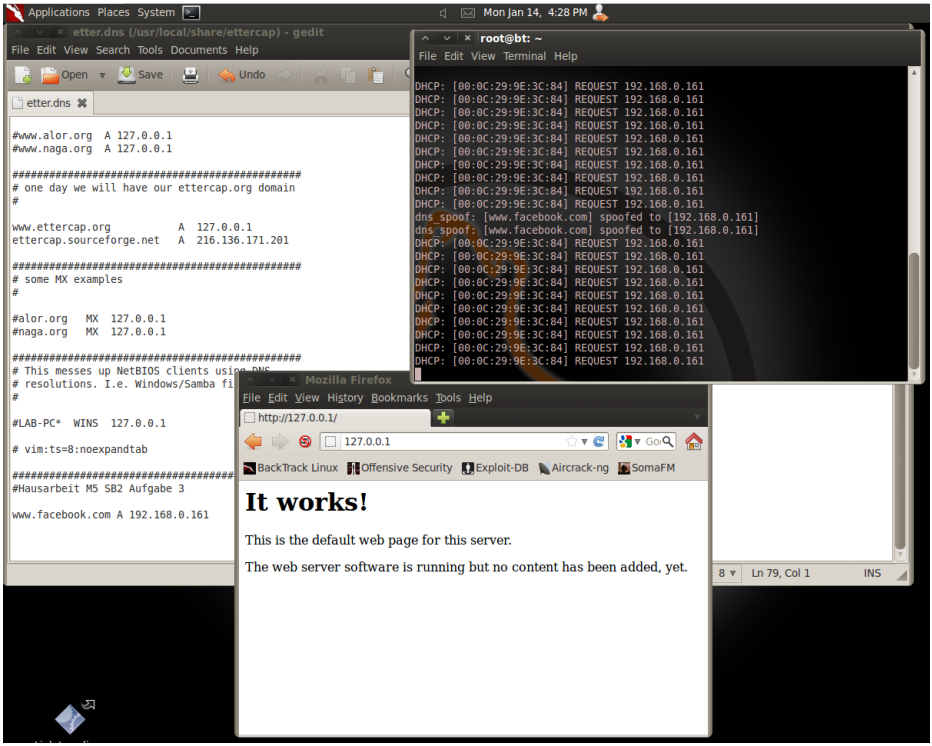
```
ettercap -T -q -P dns_spoof -i eth0 -M ARP // //
```

Ab sofort läuft der gesamte Netzwerkverkehr im LAN-Segment über den Angreifer-PC und auf der Console werden als „Abfallprodukt“ alle Passörter ausgegeben, die ettercap im Datenstrom zweifelsfrei ermitteln konnte. Ist z.B. ein E-Mail-Client aktiv, der

regelmäßig beim Internet Provider bzw. Mailserver E-Mails abruft, so werden die Passwörter zu den E-Mail-Konten im Klartext ausgegeben (sofern der E-Mail-Abruf nicht verschlüsselt erfolgt).

Aber das ist noch nicht alles. Der Angreifer pflegt nur die Konfigurationsdatei von ettercap (etter.dns) und trägt dort für die Adressen, die er im Rahmen einer Man-In-The-Middle-Attacke verbiegen will eine Kombination aus Hostnamen und IP-Adresse ein. Für eine Attacke auf die Facebook-Seite trägt er also die IP-Adresse des Angreifers ein: www.facebook.com A 192.168.0.161

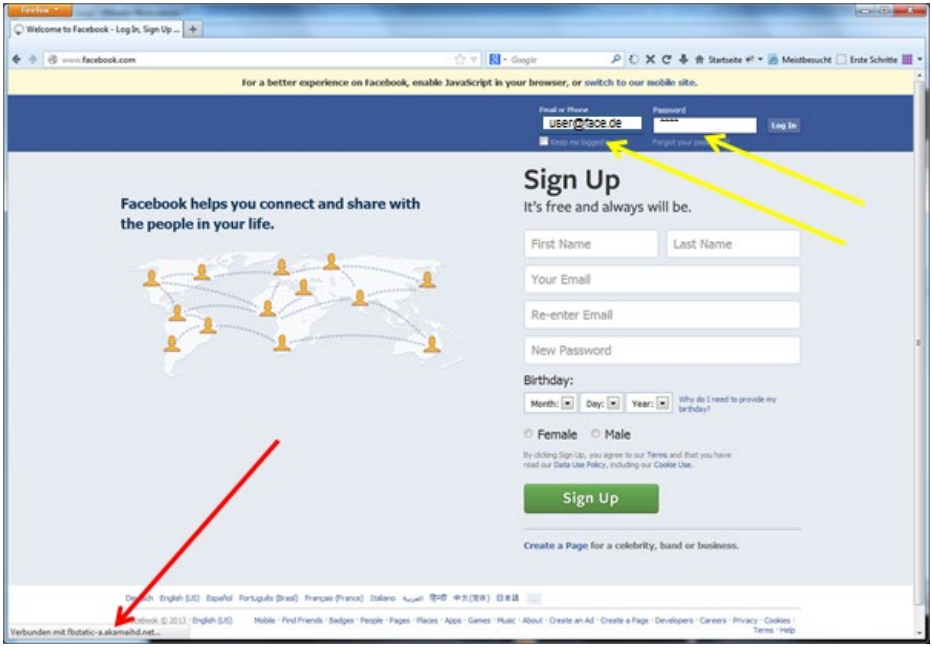
Ab sofort werden alle Anfragen des Opfers (bzw. aller Netzwerkteilnehmer im Segment) z.B. via Webbrowser an http://www.facebook.com oder https://www.facebook.com an den Angreifer gesendet. Dieser muss nun noch einen Webserver bereitstellen, der auf die Ports 80 (http) und 443 (https) antwortet. Auf einer Linux-Maschine kann man das durch Installation z.B. des gängigen Apache-Webservers erreichen.



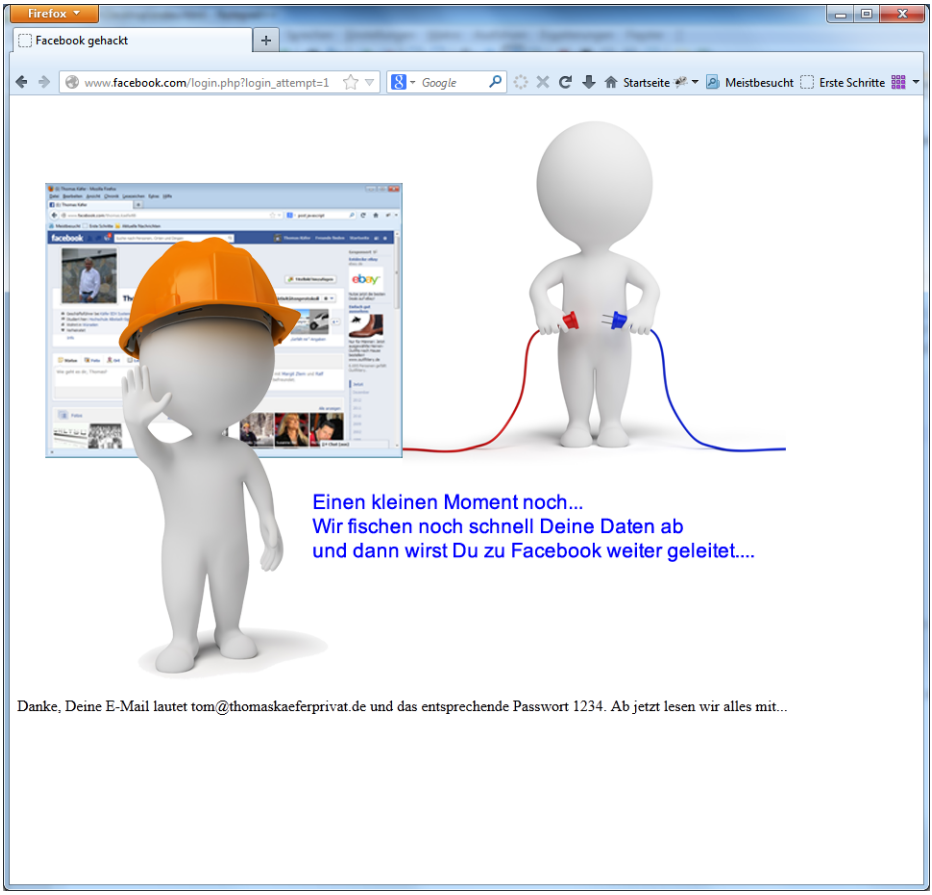
Der Apache-Server (unteres Fenster) ist offenbar noch nicht konfiguriert und diese Seite würde nun auch dem Opfer bei Aufruf von www.facebook.com angezeigt. Hier muss sich der Angreifer also noch etwas Mühe geben. Er wird dazu zunächst einmal einfach die originale Facebook-Seite in das Verzeichnis des Apache-Servers als index.html (/www/var) abspeichern und geringfügig modifizieren. In dieser Datei kann der Aufruf für die Übergabe des Passwortes sehr leicht identifiziert werden:

```
acion="https://www.facebook.com/login.php?login_
attempt=1" method="post" onsubmit="return win-
dow.Event […]
```

Wenn man sich nun die SSL-Konfiguration in Apache sparen will, stellt man einfach alle Links in der Seite, die mit „https“ beginnen, auf „http“ um und man erhält eine komplett unverschlüsselte Kommunikation. Nebeneffekt: Der Browser des Opfer-PCs meldet so auch keine Mismatches bei den SSL-Zertifikaten mehr und warnt somit nicht. Nun wird eine Seite `login.php` erstellt, die die per POST-Methode übergebenen Parameter (u.a. die Felder `email` und `pass`) ausliest und (hier) zu Demo-Zwecken anzeigt. In einem echten Szenario würde der Angreifer nicht so nett warnen wie in der Abbildung mit dem „Bauarbeiter“, sondern die so „gephishten“ Daten heimlich auf seinem Angreifer-PC in einer Datei speichern. Der nächste Screenshot zeigt die nachgebaute und lokal auf dem Angreifer-PC gespeicherte Facebook-Kopie mit Eingabe von E-Mail-Adresse (Login-Name) und Password im Feld pass (siehe gelbe Pfeile; Die User-Daten sind nicht echt!):



Der rote Pfeil zeigt das dynamische Nachladen von Inhalten bzw. Plugins (typische und oft kritisierte Unart von Facebook – By the way: in der Datei sind 73 https-Request/Reloads enthalten). Durch Betätigen des Buttons „Log In“ wird nun die nachgebaute Seite `login.php` aufgerufen, die sich ebenfalls auf dem Server des Angreifers befindet:



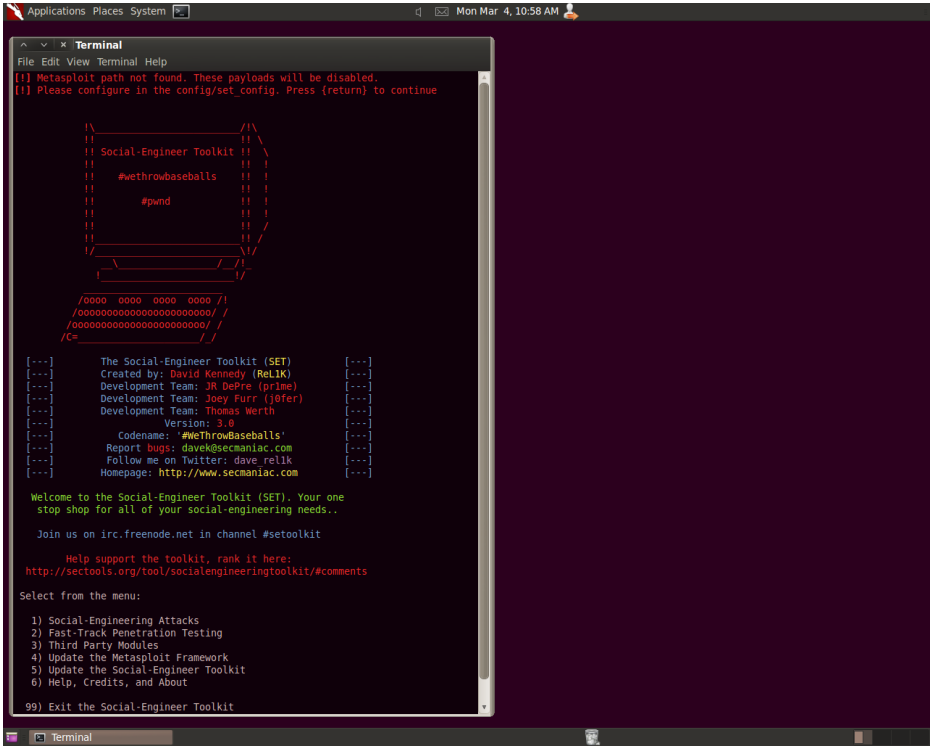
Der Code der Seite ist recht kompakt und besteht teilweise aus HTML und teilweise aus PHP-Syntax (die Server-seitig interpretiert wird):

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; char-
set=windows-1252">
<title>Facebook gehackt</title>
</head>
<body>
<p><img border="0" src="phish.png" width="800"
height="600"></p>
</body>
</html>
<?PHP
echo "Danke, Deine E-Mail lautet $_POST[email] und das
entsprechende Passwort $_POST[pass]. Ab jetzt lesen wir
alles mit...";?>
```

Da die PHP-Seite Server-seitig ausgeführt wird, wäre es jetzt einfach, die Daten der Felder „`email`“ und „`pass`“ in eine Datei auf dem Server (Angreifer-PC) zu schreiben und den User sofort auf die echte Facebook-Seite weiterzuleiten (z.B. mit refresh). Damit der User nicht bemerkt, dass seine Eingabe von Benutzernamen und Passwort nicht zu einem Login bei Facebook geführt hat, könnte man nun die POST-Methode der originalen Facebook-Datei erneut mit den zwischengespeicherten Werten aufrufen und das Login tatsächlich durchführen. Nun könnte der Angriff beendet werden (um später das Facebook-Konto zu übernehmen) oder sogar ein Live-Mitschnitt der aktuellen Facebook-Session erfolgen (optional mit Verändern der Daten). Im Gegensatz zu den in Kapitel 0 und 0 dargestellten Phishing-Attacken, die auf externen Servern mit einer mehr oder weniger sichtbaren Umleitung der Adresse ablaufen, ist eine Phishing-Attacke mit Werkzeugen wie ettercap bzw. DNS- und ARP-Spoofing sehr schwer zu erkennen. Bei den externen Attacken reicht es schon, von Hand die echte URL der Webseite einzugeben, was bei der internen Attacke nichts bringt. Man hat ja als Opfer die echte Adresse www.facebook.com eingegeben und wurde durch Verbiegen der IP- bzw. MAC-Adressen ohne Möglichkeit der Gegenwehr auf den Angreifer-PC geleitet und dort „abgefrühstückt“.

Social Engineering mit SET

Wem (als Hacker) diese manuelle Arbeit zu „aufwändig“ ist (oder wer die technischen Hintergründe nicht verstanden hat), der findet fertige Toolkits im Internet, die einen Angriff per Menüauswahl erledigen. Der bekannteste Vertreter ist das sogenannte Social Engineering Toolkit – kurz SET und findet sich z.B. auch als Bestandteil in der Forensic Suite BackTrack.

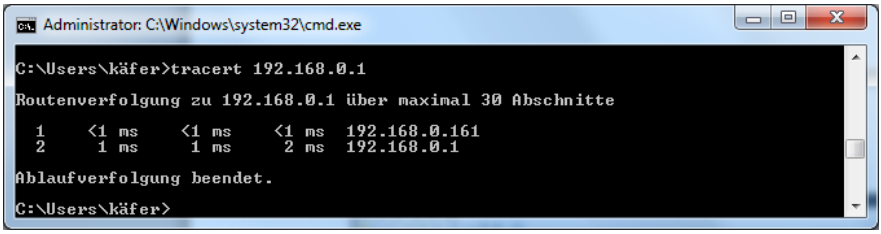


Das Tool ist nicht per se schlecht oder böse, dient es doch dem Forensiker zum Aufdecken von Schwachstellen mittels sogenannter Pentests. Aber wie so oft im Leben gibt es auch eine dunkle Seite.

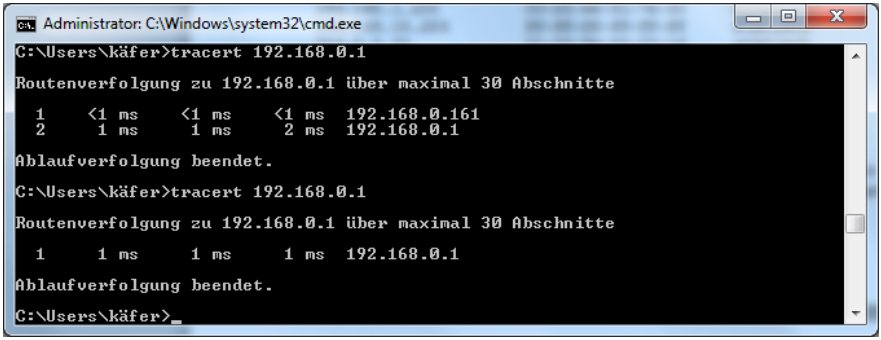
Lord Voldemort und Darth Vader würden SET eben zum Angriff nutzen (vielleicht ohne wirklich zu verstehen, was da genau passiert). Deshalb sind solche Zauberstäbe oder Lichtschwerter in der Hand von Script-Kiddies echte Waffen!

Indizien zu Erkennung

Dennoch ist man nicht gänzlich schutzlos. Vor allem, wenn man einen Verdacht hat, kann man überprüfen, ob zwischen eigener Adresse und Router (bzw. Ziel) noch ein weiterer Hop liegt, der da nicht hingehört. Aufgedeckt werden kann das ARP-Spoofing in diesem Fall über den Tracert-Befehl (bei Linux traceroute), der eine Routenverfolgung eines ICMP[xvii]-Paketes auf dem Weg vom Opfer zum Router (IP-Adresse 192.168.0.1) anzeigt und hier die IP-Adresse des Angreifers als Zwischenstation ausgibt (die es im Normalfall nicht geben würde):



Sobald das ARP-Spoofing beendet wird, reduziert sich die Route wieder (erwartungskonform) auf einen Hop:



Auch ein Monitoring-System oder ein IDS leistet gute Dienste. Solche Systeme erkennen anhand von veränderten Betriebsparametern (Verlängerung der Antwort-Zeiten auf ICMP-Requests, Flooding von ARP-Tabellen), dass es möglicherweise unzulässige Betriebszustände gibt oder ein Angriff versucht wird und schlagen Alarm.

Somit kann man natürlich auch ein Traceroute auf die Zieladresse im Internet absetzen. Ist ein ARP-Spoofing aktiv, wird auch bei Eingabe des Befehls „tracert www.facebook.com“ der zusätzliche Hop über den Angreifer-PC ausgeben (also hier 192.168.0.161). Die Analyse setzt natürlich schon Grundkenntnisse über die eigene Netzwerkstruktur voraus.

Gegenmaßnahmen

Grundlegende Gegenmaßnahmen

Es gibt eine Reihe von Verhaltensregeln und technischen Maßnahmen, die dazu beitragen, das Risiko, Opfer einer Phishing- oder Hackattacke zu werden, zu reduzieren bzw. auf ein akzeptables Maß zu minimieren. Einen vollständigen Schutz gegen solche Attacken gibt es – wenn man aktiv an den Diensten des Internets teilnimmt – nicht. Hier würde allein das „Einmauern“ des Systems ohne Schnittstellen nach außen einen wirksamen Schutz darstellen, wobei natürlich die Nutzbarkeit eines solchen isolierten Computers in Frage zu stellen wäre.

Menschliche Intelligenz

Die mächtigste Waffe gegen Angriffe aus dem Netz ist der Mensch, denn die Intelligenz sitzt (i.d.R.) vor dem Computer zwischen Monitor und Rückenlehne! Der Einsatz des eigenen Gehirns hilft erstaunlicherweise ungemein dabei, einen Großteil der Angriffe schon im Keim zu ersticken und abzuwehren.

Eine Vielzahl der heutzutage im Internet verschickten E-Mails ist SPAM und als solcher oft sehr einfach zu identifizieren. Das Aussortieren dubioser Angebote für diverse Pillen, Aktienoptionen auf Schweinehälften oder vermeintlicher Schnäppchen stellt einen Großteil der Computernutzer meist vor keine unlösbare Aufgabe (wenn nicht gar ein SPAM-Filter des E-Mail-Systems bereits eine Vorselektion durchgeführt hat).

Schwieriger wird es, wenn die E-Mail nicht sofort als gefährlich eingestuft werden kann, weil das Opfer gezielt angesprochen wird und dabei bewusst und meist mit Hilfe von Social Engineering Ängste oder Wünsche angesprochen werden, bei denen das rationelle Denken aussetzt und das Unterbewusstsein gezielt manipuliert wird.

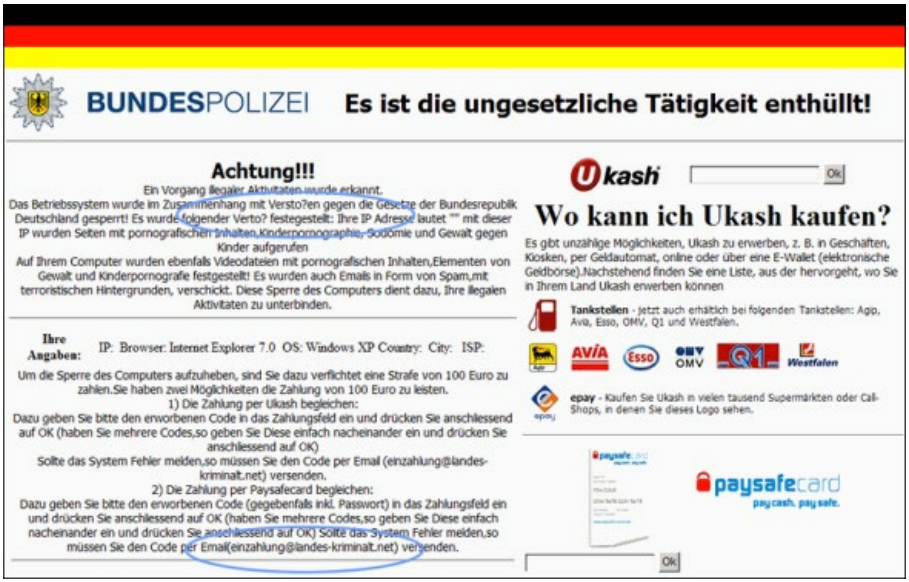
Hier gibt es mehrere Ansätze. Oft wird versucht, das Vertrauen des Opfers dadurch zu erlangen, dass bekannte und gelernte Mechanismen und Indizien eingesetzt werden, sodass man glaubt, dass die Nachricht echt und authentisch ist (z.B. Verwendung von Logos, offiziellem Layout usw.). Die Angreifer nehmen Streuverluste bewusst in Kauf und senden z.B. an Millionen von E-Mail-Empfängern eine echt aussehende E-Mail beispielsweise der Postbank (ohne zu wissen, ob der jeweilige Kunde überhaupt ein Postbank-Konto hat). Wie viele User, die tatsächlich Postbank-Kunde sind, werden nun den Anweisungen in der E-Mail folgen? Wenn nur ein Promille der Empfänger darauf reagiert, dann sind das bei einer Million Adressaten schon Tausend potentielle Opfer.

Die einfachste Regel zur Gefahrenabwehr lautet daher schon einmal: Prüfen Sie, ob Sie überhaupt zur angesprochenen Kundengruppe gehören. Warum sollten Sie auf eine E-Mail der Postbank reagieren, wenn Sie nur ein Konto bei der Sparkasse haben? Warum sollten Sie auf eine E-Mail von UPS antworten, wenn Ihre Lieferung per DHL versendet wird bzw. sie gar keine Lieferung erwarten? Sendet Ihnen UPS oder DHL überhaupt Lieferbenachrichtigungen per E-Mail? Warum sollten Sie eine Rechnung von einem Online-Shop bekommen, bei dem Sie gar nichts bestellt haben?

Warnt Ihr Bauch, dass da etwas komisch ist, dann nehmen Sie das Warnsignal ernst und gehen Sie mit besonders offenen Augen durch Internet und Ihr E-Mail-Postfach und seien Sie skeptisch. Öffnen Sie keine E-Mail-Anhänge aus dubiosen Quellen oder wenn Sie die Nachricht nicht explizit angefordert haben. Haben Sie zur angeblichen letzten Mahnung überhaupt schon eine Rechnung oder eine erste Mahnung erhalten? Haben Sie überhaupt etwas bestellt? Nein? Warum wollen Sie dann den Anhang in der E-Mail öffnen? Neugier?

Gut, dann machen Sie es und seien Sie später aber bitte nicht überrascht, wenn Ihr Rechner kurze Zeit später fremdbestimmt ist und Sie das System nicht mehr nutzen können.

So funktioniert z.B. der u.a. als BKA-Trojaner bekannte Schadcode. Das Opfer erhält eine E-Mail mit einer angeblich wichtigen Nachricht im Anhang (Rechnung, Mahnung, Gewinnankündigung, Lieferankündigung). Der Anhang enthält jedoch nicht das angekündigte Dokument, sondern (oder zusätzlich) Schadcode, der nun durch Ihre Freigabe (Anklicken einer ausführbaren Datei) auf Ihrem Computer aktiv wird. Der Schadcode nistet sich so in das System ein, dass er bei jedem Start des Rechners aktiv werden kann. Beim nächsten Neustart des PC wird er wieder geladen und treibt sein Unwesen. Das ist dann z.B. eine bildschirmfüllende Warnung, dass Sie bei einer illegalen Handlung erwischt worden sind (z.B. Laden von urheberrechtlich geschützten Werken aus einer Tauschbörse oder gar Austausch von Kinderpornografie) und nun seitens des BKA oder einer anderen Polizeibehörde gegen Sie ermittelt wird.



Ihr Rechner wurde „vorsorglich“ gesperrt und kann gegen Zahlung einer „Strafe“ von z.B. 100,- € wieder entsperrt werden.

Zur Zahlung sollen Sie dann zur nächsten Tankstelle oder zum Drogeriemarkt laufen und eine Ukash- oder Paysafe-Wertkarte (o.ä.) kaufen und die 100,- € damit überweisen.

Besonders perfide: Manche Versionen eines solchen Trojaners machen zusätzlich mit der eingebauten Webcam Ihres Notebooks noch ein Foto von Ihnen und untermalen die Forderung ganz subtil mit dem Hinweis, dass „man“ ja nun weiß, wer Sie sind und wie Sie aussehen. Die Überraschung ist dann groß, wenn die Freischaltung des Rechners nach Zahlung der Strafe unterbleibt. Geben Sie die 100,- € lieber direkt einem Fachmann, der Ihr System vom Trojaner befreit und investieren Sie für die Zukunft in einen aktuell gehaltenen Virenscanner, der meist Alarm schlägt, wenn ein Schadcode in einem E-Mail-Attachement enthalten ist.

Auch hier kann man an einigen Indizien wieder feststellen, dass die Hacker nicht 100% „sauber“ gearbeitet haben. Im Text (siehe Markierung) fehlen ein paar Umlaute. Und in der sicherlich falschen E-Mail-Adresse ist ein Tippfehler enthalten: „… landeskriminalt.net“ statt … „landes-kriminalamt…“.

Aber natürlich hilft auch hier wieder das Nachdenken durch den Benutzer: Würde eine deutsche Polizei-Behörde solch einen „Bußgeldbescheid“ in dieser Form und dann auch noch per E-Mail verschicken? Müsste das nicht an – um strafrechtlich relevant zu sein – an eine konkret benannte Person förmlich zugestellt werden? Kämen Sie mutmaßlich bei dieser Fülle angeblicher Verstöße (Straftaten) mit eine vergleichsweise niedrigen Buße in Höhe von 100,- € davon und warum können Sie das „Bußgeld“ nicht – wie jedes „Knöllchen“ z.B. für eine Geschwindigkeitsübertretung – per Banküberweisung bezahlen?

Weitere Informationen zu den verschiedenen Versionen des Trojaners finden Sie u.a. auf der Website http://www.bka-trojaner.de/ oder http://www.bundespolizei.de.

Mitte Februar 2013 meldete die spanische Polizei übrigens einen Ermittlungserfolg und konnte 11 mutmaßliche Hintermänner des sogenannten BKA-Trojaners festnehmen. Ihnen wird vorgeworfen, in 22 Ländern insgesamt rund eine Million jährlich mit dieser Masche erbeutet zu haben. Darauf vertrauen, dass damit dieser Angriff Geschichte ist, sollte man nicht. Es wird sicher bald schon die nächsten Nachahmer geben.

Sie lachen jetzt, weil Sie sich nicht vorstellen können, dass jemand auf solch eine Masche hereinfällt? Nun – offenbar schon, denn wenn die rund 1. Mio. € Umsatz p.a. stimmen, dann hat die nun zur Strecke gebrachte Bande rund 10.000 Opfer pro Jahr gefunden.

Indizien zu Erkennung von Phishing-E-Mails

Wie die vorangegangenen Kapitel gezeigt haben, kann man an einer Reihe von Indizien erkennen, ob eine Nachricht authentisch ist oder ob sie zum Ausspähen von Daten oder Einschleusen von Schadcode dient.

Die wichtigsten Faktoren sind Zeit und menschliche Intelligenz: Wer ohne richtig nachzudenken hektisch und nachlässig auf alles klickt, was er so tagtäglich in seinem Posteingang findet, der muss sich nicht wundern, wenn er Opfer einer Phishing-Attacke wird. Überlegen Sie immer, ob sie überhaupt an einem Gewinnspiel teilgenommen haben, für dass Sie nun eine Gewinnbenachrichtigung vorfinden. Haben Sie beim Anbieter XY überhaupt etwas bestellt oder ist es schon eigenartig, dass sie von ihm jetzt eine Rechnung (oder gar eine letzte Mahnung) als Datei-Anhang bekommen? Erwarten Sie eine Lieferung oder ist es eher seltsam, dass UPS oder DHL sich per E-Mail bei Ihnen melden?

Ein wenig paranoid sollte man schon sein und ruhig einmal zu viel als zu wenig nachdenken, ob man tatsächlich einen Vorgang initiiert hat, über den man nun benachrichtigt wird. Achten Sie im Detail immer auf die Aufmachung der Nachricht oder Webseite, die angezeigten Adressen (URL, Absender, Domain-Namen) und ob die Seite mit einem gültigen SSL-Zertifikat via HTTPS übertragen wird. Je formaler und korrekter die Formulierungen sind und je professioneller das Erscheinungsbild der Nachricht oder Webseite ist, umso höher ist die Wahrscheinlichkeit, dass sie echt ist. Achten Sie aber auch auf Kleinigkeiten. Nicht korrekt dargestellte Umlaute oder kleinere Fehler sind meist schon ein gutes Zeichen, dass etwas nicht stimmt.

Prüfen Sie die Angaben auf Plausibilität. PayPal sitzt nicht in Bochum und den 30.Februar gibt es in keinem Kalender. Auch wenn das kein Garant ist:
Viele Hacker sind nicht besonders schlau und haben in der Schule nicht gut aufgepasst (oder sie gehen sogar noch zur Schule), sonst müssten sie diesen „Job“ nicht machen. Seien Sie schlauer als die Hacker!

Übrigens: Extrem schlechtes Deutsch (oder Englisch) in E-Mails zu verwenden, kann durchaus eine gewollte Masche sein. Die sogenannte Nigeria-Connection nutzt diesen Mechanismus, um einen SPAM-Filter in eigener Sache zu installieren. Der Aufhänger ist immer derselbe. Irgendein entfernter Verwandter oder jemand, den Sie gar nicht kennen, hat angeblich ein riesiges Vermögen hinterlassen, welches zu verfallen droht. Sie sollen das Erbe annehmen und der Vermittler (Absender der E-Mail) bekommt dann von Ihnen eine Provision.

Jetzt könnte man meinen, dass die Initiatoren dieser E-Mails langsam genug Erfahrung (und Geld) gesammelt haben, um sich einen professionellen Übersetzer leisten zu können und die Anschreiben in einem formalen und formvollendeten Deutsch zu

verfassen. Damit aber würden nun auch Empfänger reagieren, die vorher noch von den schlechten Formulierungen abgeschreckt wurden. Unterstellen wir einmal, dass nun auch ein Arzt, Lehrer oder Rechtsanwalt auf eine solche Mail reagiert. Spätestens dann, wenn die Nigeria-Connection dann Vorkasse für eine Provision verlangt, springen diese doch ab und der Aufwand für die Täter war für die Katz‘. Wer sich aber auch von haarsträubenden Rechtschreibfehlern nicht abschrecken lässt, gehört zur Zielgruppe. Er wird mutmaßlich auch nicht misstrauisch, wenn er ein paar hundert Euro oder Dollar überweisen soll, damit die Sache in Gang kommt.

Natürlich gibt es auch schlaue Hacker bzw. Kandidaten, die sich richtig Mühe geben.

Da es möglich ist, praktisch jede Angabe in einer E-Mail zu fälschen oder Inhalte einer Web-Seite zu verschleiern, ist es nur eine Frage des Aufwandes, eine fast perfekte Phishing-Attacke zu konstruieren, bei der die in den Beispielen gemachten Fehler unterbleiben. Dann muss auch der Fachmann genauer hinschauen.Technische Gegenmaßnahmen.

Der Einsatz eines SPAM-Filters (ggf. mehrstufig beim Provider und im lokalen Netzwerk) bewirkt i.d.R. schon einmal eine gute Vorselektion und kennzeichnet (tagged) verdächtige E-Mails z.B. mit dem Schlagwort SPAM und/oder verschiebt sie in einen SPAM-Ordner. E-Mails, die so getagged worden sind, sollte man dann schon einmal mit besonderer Vorsicht „genießen“.

Ein funktionierender Virenscanner leistet ebenfalls gute Dienste, kann er doch meist Schadcode in Form von Dateianhängen oder verseuchten Webseiten erkennen und herausfiltern.

Eine Firewall sowohl im Router als auch im lokalen Computer (z.B. die Windows-Firewall) hilft dabei, direkte Angriffe abzuwehren und Schadcode im Datenstrom zu identifizieren.

Durch Verwendung verschiedener Passwörter für unterschiedliche Dienste kann man den Schaden bei Kompromittierung einer Zugangskennung deutlich begrenzen. Hat man den Verdacht, dass ein Zugang nicht mehr sicher ist, sollte man die Passwörter sofort ändern. Unabhängig von einem konkreten Verdacht sollte man Passwörter regelmäßig ändern. Um nicht den Überblick zu verlieren, hilft eine zentrale gesicherte Passwortdatenbank. Bei besonders gefährdeten Systemen (Online-Banking) sollte man ggf. angebotene zusätzliche Sicherungsmechanismen nutzen (Smart-Token, HBCI[xviii]-Karten, Two-Factor-Authentifizierung, Validierung per SMS usw.).

Sicherung von lokalen (Funk-)Netzwerken vor unbefugtem Zugriff

Während es in der Regel relativ einfach ist, ein kabelgebundenes LAN davor zu schützen, dass sich ein Fremder hier durch Einstecken seines Computers einklinken kann, ist dies bei einem Funknetzwerk schon etwas schwieriger. Hierbei entfällt nämlich die Notwendigkeit, dass der Angreifer eine physikalische Verbindung herstellen muss (als Person in das Netzwerk/Gebäude einbrechen muss). Es reicht, sich innerhalb der Funkreichweite des WLANs zu befinden.

Nun gibt es verschiedene Mechanismen, wie man ein WLAN absichern kann. Die schlechteste Idee ist es, ein offenes WLAN zu betreiben oder zu nutzen (auch wenn der sozialistisch angehauchte Grundgedanke eines offenen WLAN-Verbundes zur Nutzung für jedermann auch seinen Charme hat). Ein offenes WLAN lädt geradezu zum Missbrauch ein, braucht ein Angreifer doch gar keine technischen Hürden zu überwinden und macht sich allein durch Nutzung des offenen (ungesicherten) WLANs nach allgemeiner Rechtsauffassung erst einmal nicht strafbar.

Und auch als Nutzer eines offenen WLANs ist man Angriffen Dritter praktisch schutzlos ausgeliefert. So ein offenes WLAN findet

man häufiger, als Sie vielleicht denken: z.B. in ICE-Zügen, Reisebussen, Schnellrestaurants, Flughäfen, Bahnhöfen und natürlich im privaten Umfeld. Man schätzt, dass derzeit in Deutschland jedes 5. WLAN noch vollkommen ungeschützt ist bzw. mit einem ungeeigneten Schutzmechanismus betrieben wird. Fahren Sie doch mal in langsamer Fahrt mit einem WLAN-Sniffer durch Ihre Stadt…

Besser ist es also, sein WLAN zu verschlüsseln und den Zugriff mit einem Passwort zu schützen. Vollkommen ungeeignet sind Maßnahmen wie das Verstecken/Unterdrücken der sogenannten SSID[xix] oder der Einsatz der WEP[xx]-Verschlüsselung.
Das Unterdrücken der SSID hält einen WLAN-Sniffer nicht davon ab, das WLAN trotzdem zu finden und für das maschinelle Knacken der WEP-Verschlüsselung gibt es fertige Toolkits, die wenige Sekunden bis Minuten brauchen, um den Zugang zum WLAN zu ermöglichen.

Auch die MAC-Authentifizierung, bei der die MAC-Adressen legitimer Netzwerkgeräte zuerst in eine MAC-Adressliste eingetragen werden müssen, bietet nur bedingt Schutz, da ein Angreifer die MAC-Adressen mitlesen und seine Adresse dann in einer der zulässigen Adressen fälschen kann.

WPA[xxi] ist auch keine gute Idee, da auch dieses Verfahren, welches immerhin schon sicherer als WEP ist, seit 2004 aber auch als „gehackt“ gilt.

Derzeit praktisch sicher ist hingegen die WPA2-Verschlüsselung, die nur mit sehr viel Aufwand kompromittiert werden kann (vgl.[xxii]).

Mit WPA2 ist Ihr WLAN daher nach derzeitigem Stand ausreichend gut geschützt. Die Nutzung von VPN (wenn möglich) erhöht diese Sicherheit noch einmal zusätzlich. Lassen Sie Ihren Router daher im Zweifel lieber von einem wirklichen Fachmann

einrichten. Dass Ihr WLAN auf Anhieb bei der Einrichtung funktioniert hat, ist kein Grund zum Freuen und vor allem kein Indiz dafür, dass es sicher ist – im Gegenteil: Wenn Sie in Ihren Endgerät keinen Preshared Key zur Authentifizierung eingeben müssen/mussten (oder Ihnen dieser Begriff noch nie bei der Konfiguration Ihres WLANs begegnet ist), dann ist das ein gutes Zeichen dafür, dass Sie keine Verschlüsselung einsetzen! Bedenken Sie zudem immer, dass Sie sich gegen Fremde wirksam nur im eigenen Netzwerk schützen können. Nutzen Sie ein fremdes Netzwerk (egal, ob gesichert oder ungesichert), so wissen Sie i.d.R. nie, wer dort sein Unwesen treibt. Ein ARP- oder DNS-Spoofing ist dann für Sie nur sehr schwer zu erkennen!

Prüfen der URLs

Besondere Vorsicht ist bei in Texten enthaltenen Hyperlinks geboten. In der Seitenbeschreibungssprache HTML ist ein Hyperlink durch einen Namen (Titel) und die eigentliche Adresse (URL) definiert. Der Name ist das, was der User oberflächlich sieht (angezeigt bekommt) und dieser muss nicht mit der dahinter liegenden URL übereinstimmen.

Beispiel (funktioniert nur im Word-Dokument bzw. auf einer HTML-Seite[xxiii]):

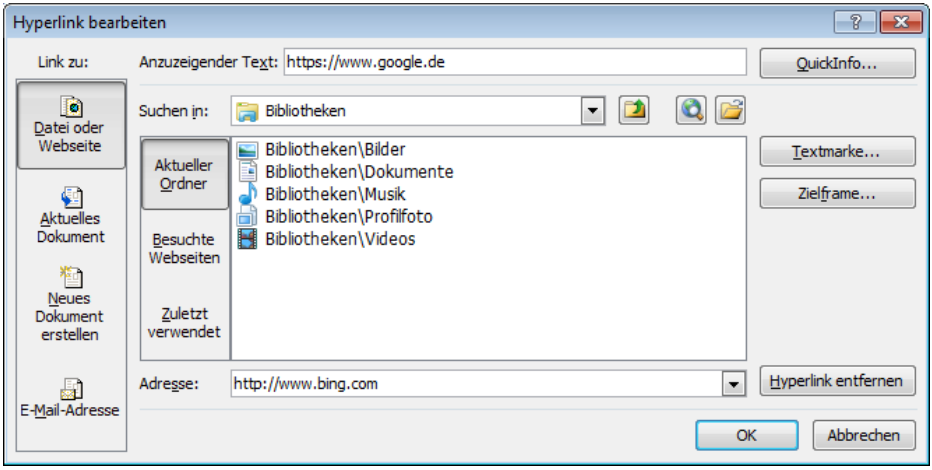
Der Link https://www.google.de führt in diesem Beispiel zur URL: http://www.bing.com.

Das können Sie z.B. dadurch nachvollziehen, dass Sie den Mauszeiger über den Link platzieren und nicht darauf klicken. Ein sogenanntes Pop-Up-Fenster zeigt, wohin die URL tatsächlich zeigt:

Beispiel:

Der Link https://www.google.de führt in diesem Beispiel http://www.bing.com

Wie einfach es ist, einen Hyperlink zu fälschen, sehen Sie an folgendem Dialogfeld zum Einfügen eines Hyperlinks:



Misstrauen Sie daher allen Hyperlinks in Dokumenten oder Webseiten dubioser Herkunft (Warum sollten Sie übrigens den Hyperlinks in diesem Dokument trauen?) und prüfen Sie vor einem Klick auf einen Link, wohin dieser tatsächlich führt.

Ist es plausibel, dass ein angeblicher Link zur PayPal-Seite zu einer URL hgf1.fgh2.com/442gg6dsh führt? Nein!

Am besten ist es, sie tippen die URLs immer von Hand in Ihren Browser ein und folgen nicht dem Hyperlink im Quelldokument, auch wenn es so schön bequem ist.

Nutzung von Verschlüsselung (HTTPS/SSL)

Im Beispiel des umgeleiteten Hyperlinks ist eine weitere Gemeinheit eingebaut. Anstatt mittels SSL-Verschlüsselung und HTTPS-Protokoll verschlüsselt auf die URL www.google.de zuzugreifen, wird unverschlüsselt mittels http auf www.bing.com zugegriffen.

Achten Sie darauf, möglichst immer verschlüsselt zu kommunizieren. Das gilt für den Zugriff auf URLs im Webbrowser genauso wie bei jeder anderen Kommunikation im unsicheren Internet oder lokalen Netzwerk (z.B. E-Mail-Abruf).

Bedenken Sie, dass ohne SSL-Verschlüsselung jedes Datenpaket vollkommen unverschlüsselt übertragen wird und von jedem mitgelesen werden kann, der Zugriff auf den Datenstrom hat. Werden hingegen das HTTPS-Protokoll bzw. eine Verschlüsselung wie z.B. SSL oder Mechanismen wie VPN eingesetzt, so ist das Mitlesen der Kommunikation (also z.B. der Passwörter) deutlich erschwert bis unmöglich.

Passwortkonzept

Unabhängig vom Ausspähen von Benutzerzugängen und Passwörtern gilt es natürlich auch, ein sinnvolles und durchgängiges Passwortkonzept aufzustellen und zu verfolgen.

Ist das Passwort durch Mitlesen oder Phishing dem Angreifer bekannt, ist es unerheblich, wie komplex es aufgebaut ist: Der Angreifer hat es so oder so. Damit Dritte ein Passwort möglichst nicht erraten oder mittels Brute-Force-Attacke durch Ausprobieren ermitteln können, muss dieses eine gewisse Komplexität aufweisen. Nach heutigen Maßstäben und den technischen Möglichkeiten zum maschinellen Knacken von Zugangskennungen muss ein Passwort mindestens zehn Zeichen haben, aus Buchstaben (Groß-/Kleinschreibung), Zahlen und Sonderzeichen bestehen und darf in keinem Wörterbuch zu finden sein. Je größer

der Zeichenvorrat ist, aus dem ein Passwort aufgebaut ist (werden kann), umso größer ist die Anzahl der möglichen Kombinationen und damit die benötigte Zeit, um diese alle durchzuprobieren. Mit der heutzutage (i.d.R.) verfügbaren Rechenleistung liegt die Grenze, bei der mit einer Brute-Force-Attacke ein Passwort entschlüsselt werden kann, zwischen 8 und 9 Zeichen.
Das liegt daran, dass mit jedem zusätzlichen Zeichen der Rechenaufwand für die hinzukommenden Möglichkeiten ab etwa der 8. Stelle exponentiell anwächst. Passwörter ab 10 Zeichen Länge gelten daher derzeit als sicher, sofern sie nicht (in Teilen) in einem Wörterbuch vorkommen.

Der Begriff „Wörterbuch“ ist hierbei nicht eng auf ein Nachschlagewerk wie etwa der Duden anzuwenden, sondern beinhaltet alle bekannten Phrasen und Zeichenkombinationen (u.a. umgangssprachliche Verfremdungen, Abkürzungen, Akronyme, Muster auf der Tastatur), die in einem mehr oder weniger breiten Verwendungsraum bekannt sind. Illegal abgegriffene Passwortlisten werden hierbei ebenso als Wörterbuchattacke genutzt wie alle offiziell bekannten Quellen und Sprachen.

Ein gutes Passwort ist vollkommen willkürlich aus möglichst vielen Zeichen ohne jegliche Systematik zusammengesetzt. Des Weiteren sollte man für jeden Dienst ein eigenes Passwort verwenden. Damit verhindert man, dass ein Angreifer mit Kenntnis eines Passwortes auch auf andere Systeme des gleichen Opfers zugreifen kann. Beispiel: Nutzt man für Facebook und Ebay dasselbe Passwort und geht bei Facebook relativ sorglos mit diesen Zugangsdaten um und ein Angreifer kann das Passwort dort bzw. in diesem Kontext abgreifen, so versucht er möglicherweise mit der ihm ebenfalls bekannten E-Mail-Adresse des Opfers nun ein Login bei Ebay. Hier ist der Schaden dann ggf. deutlich größer.

Nun stößt man als Mensch sehr schnell an natürliche Grenzen der Merkfähigkeit. Mehrere komplexe und unstrukturierte Pass-

wörter kann sich kaum jemand im Kopf merken. Er braucht eine Stelle, an der er seine Passwörter sicher abspeichern kann. Eine praktikable Lösung sieht so aus, dass man eine verschlüsselte Passwortdatenbank nutzt, in der alle Passwörter und Zugangskennungen gesichert gespeichert sind.

Diese Datei verwahrt man an sicherer Stelle (idealerweise auf einem USB-Stick offline und getrennt vom Rechner) und sichert die Passwortdatenbank mit einem sehr sicheren Masterpasswort ab. Man muss sich fortan nur noch ein Masterpasswort merken und kopiert die spezifischen Passwörter dann bei Bedarf per Copy & Paste aus der Datenbank in die Anmeldemasken der jeweiligen Systeme.

Ein gutes System ist Keypass, welches nach allgemeiner Auffassung noch nicht erfolgreich gehackt werden konnte (Quelle: http://keepass.info/).

Verwendung von Virenscannern

Ein weiterer wichtiger Baustein zur Verhinderung solcher Angriffe ist ein funktionierender und regelmäßig aktualisierter Virenscanner. Ein Virenscanner erkennt an bestimmten Bitmustern, Dateieigenschaften und Inhalten, ob es sich um Schadsoftware handelt und blockiert dann den Zugriff auf die Datei bzw. filtert den Anhang aus.

Wichtig ist, dass der Virenscanner regelmäßig mit Updates der Virensignaturen versorgt wird, damit er auch neue Bedrohungen erkennt. Es gibt praktisch keinen Virenscanner, der bei unabhängigen Tests immer und 100% zuverlässig jede Form von Schadsoftware erkannt hat und daher bleibt immer ein Rest-Risiko, dass Malware nicht identifiziert wird. Es ist dennoch keine gute Idee, zwei Virenscanner einzusetzen, die sich dann nämlich gegenseitig das Leben schwer machen. Am besten, man orientiert sich an aussagekräftigen Tests namhafter Fachzeitschriften und kauft (!) sich einen der Testsieger (meist als Jahresabonnement).

Kostenfreie Virenscanner sind besser als kein Virenscanner, bleiben oft aber hinter der Leistung der guten Kaufprogramme zurück.

An seine Grenzen kommt ein Virenscanner i.d.R. dann, wenn keine Schadsoftware heruntergeladen oder installiert wird, sondern mittels Phishing reine Nutzerdaten abgegriffen werden. Eine solche unzulässige Handlung kann von einem Virenscanner meist nicht erkannt werden. Hier ist der Mensch als Intelligenz gefordert!

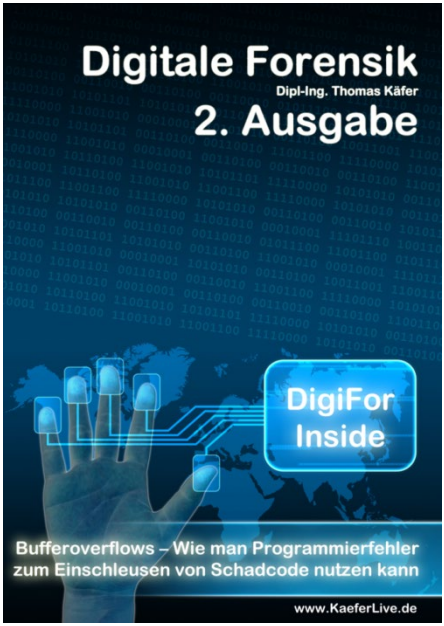
Fazit

Es ist selbst für den Fachmann manchmal erschreckend, wie einfach es ist, als Hacker an vermeintlich vertrauliche Daten und Passwörter zu gelangen. Gehen Sie mit offenen Augen durch das Internet und setzen Sie das Werkzeug Computer mit Bedacht und Augenmaß ein. Seien Sie immer dann auf der Hut, wenn Sie persönliche Daten und Zugangskennungen eingeben sollen. Macht die Aufforderung dazu Sinn und ist das System, in das Sie die Daten eingeben, tatsächlich vertrauenswürdig bzw. überhaupt echt? Wenn nicht oder Sie sich nicht sicher sind: Finger weg!

Auf der anderen Seite brauchen Sie vor Internet und Computern auch keine Angst zu haben. Beides ist nicht per se schlecht und die guten Nutzungsmöglichkeiten überwiegen bei weitem die Gefahren – Genauso, wie man vor einem Messer keine Angst haben muss, weil man damit täglich in der Küche hantiert und das Essen zubereitet.

Man sollte immer den nötigen Respekt davor haben, sonst sind die Finger ab! Und natürlich kann man ein Messer auch als Waffe einsetzen.

Deshalb immer wachsam sein (nicht nur in der Küche, sondern auch am Computer).



Lesen Sie in der nächsten Ausgabe von DigiFor Inside „Buffero-verflows – Wie man Programmierfehler zum Einschleusen von Schadcode nutzen kann“.

Hyperlink: http://www.KaeferLive.de/digifor-inside (und immer daran denken: Vor dem Klicken: Gucken!)

Ihr

Thomas Käfer

P.S. Und wenn Sie ein echtes Sicherheitsproblem haben oder dieses für die Zukunft vermeiden möchten, dann kontaktieren Sie uns. Wir kümmern uns darum: Tel. 02405/479490 oder E-Mail service@KaeferLive.de.

Glossar

[i] LAN: Local Area Network – Lokales Netzwerk
[ii] WLAN: Wireless Local Area Network – Funk-Netzwerk
[iii] TAN: Transaktions-Nummer – Einmal verwendbares Authentifizierungs-Token
[iv] Two-Factor-Authentication – Der Nutzer des Dienstes weist sich über die Angabe von zwei Dingen aus: etwas, das er weiß und etwas, das er besitzt.
[v] SPAM: Synonym für massenhaft unverlangt versendete Nachrichten (Mails); entstanden aus einem Monty-Python Sketch: Spam! Spam! Spam! Spam! Lovely Spam!
[vi] URL: Uniform Resource Locator – identifiziert und lokalisiert eine Ressource im Internet (z.B. Website)
[vii] SSL: Secure Socket Layer
[viii] TCP/IP: Transmission Control Protocol / Internet Protocol
[ix] VPN: Virtual Private Network – Virtuelles privates Netzwerk zum verschlüsselten Übertragen von Daten in einem ungesicherten Medium
[x] Weitere Information siehe z.B. http://de.wikipedia.org/wiki/OSI-Modell
[xi] Weitere Information siehe z.B. http://de.wikipedia.org/wiki/MAC-Adresse
[xii] DNS: Domain Name Systeme – sorgt für eine Auflösung von Hostnamen (wie z.B. www.ebay.com) in IP-Adressen wie z.B. 80.34.56.123
[xiii] ARP: Address Resolution Protocol
[xiv] Broadcast: Senden eines Datenpakets an alle Netzteilnehmer
[xv] Spoofing: Verschleiern
[xvi] DHCP: Dynamic Host Configuration Protocol – dient zur zentralen Vergabe von IP-Adressen im LAN
[xvii] ICMP: Internet Control Message Protocol – dient zum Austausch von Informations- und Fehlermeldungen in IP-Netzwerken
[xviii] HBCI: Homebanking Computer Interface – Standard im Bereich Homebanking
[xix] SSID: Service Set Identifier – Name des WLANs / des WLAN-Routers
[xx] WEP: Wired Equivalent Privacy – als extrem unsicher geltender, überholter Verschlüsselungsstandard für WLANs
[xxi] WPA: Wi-Fi Protected Access – Mittlerweile als unsicher geltender Verschlüsselungsstandard für WLANs
[xxii] siehe http://www.heise.de/netze/meldung/WPA2-Luecke-ARP-Spoofing-im-WLAN-1048568.html
[xxiii] Je nachdem, mit welchem Werkzeug das vorliegende Dokument erstellt wurde bzw. dargestellt wird, funktioniert das Beispiel mit dem verschleierten Link (z.B. aus Word heraus mit der Funktion PDF erstellen) oder eben nicht (z.B. beim Druck mittels PDF-Druckertreiber – dieser öffnet dankenswerter-

weise den Link https://www.google .de, so wie er angezeigt wird – was schlecht für die Demonstration ist ;-)).