Phishing

Thomas Prinz

27.04.2010

1. Einleitung

Petri Heil! Ein Fischergruß, der zum guten Fang wünscht, wird allzu gern mit einem *Petri Dank!* erwidert, nicht nur in der Fischerwelt, sondern auch in der Phisherwelt. *Phishing* ist eine Form des Computerbetrugs und ließ gerade in den letzten Jahren Schlagzeilen von sich machen. Die Phishing-Methoden werden immer besser und immer noch tappen viele Benutzer in die oft plumpen Versuche der Phisher. Aktuelle Zahlen von Opfern sind nicht bekannt und werden auch in bekannten Phishing-Berichten nicht erwähnt.

Die folgende Ausarbeitung soll einen Überblick über das Thema Phishing bieten. Es werden nach der Einleitung (1. Einleitung) neben der Kategorisierung und dem Begriff (2. Phishing und seine Spielarten) auch Beispiele (3. Zahlen, Fakten und Beispiele), Schutzmaßnahmen (6. Ursachen für einfaches Phishing und Schutzmöglichkeiten), rechtliche Konsequenzen (7. Was tun, wenn Phisher erfolgreich?), Folgen (5. Das Opfer und die Folgen), Unterarten (2. Phishing und seine Spielarten), Motive, Szenarien (4. Die Phisher, Motive und Methoden) und Ursachen (6. Ursachen für einfaches Phishing und Schutzmöglichkeiten) erläutert. Dabei spielt gerade der Umgang mit dem Internet und den Phishing-Fallen eine große Rolle und kann als Anleitung zur Prävention vor Phishing-Betrügern helfen. Im Anschluss folgen noch die Bildquellen (9. Bildquellen) und das Literaturverzeichnis (10. Literaturverzeichnis).

2. Phishing und seine Spielarten

Phishing ist ein Kunstwort, welches sich aus den englischen Wörtern *Password* (Passwort) und *Fishing* (Fischen) zusammensetzt. Es beschreibt die Täuschung eines Anwenders durch gefälschte E-Mails, Telefonanrufe, Internetseiten und SMS und das damit verbundene *Abfischen* von Passwörtern, TANs, Bankverbindungen und persönlichen Daten. Mit diesen Daten ist es dem *Phisher* (der Angreifer) dann möglich, mittels einer geklauten Identität Geschäfte zu tätigen.[1]

Das Phishing ordnet sich in eine mögliche Kategorisierung von Attacken als eine *Social Engineering* Attacke ein. Social Engineering beschreibt den Versuch eines Angreifers sein Opfer zu Tätigkeiten zu bewegen, welche dieser dann zu jedweder Art ausnutzen kann. Meist erfolgt dies unter einer Tarnung, wie als Systemadministrator. Telefone, täuschende

[1] Müller, Klaus-Rainer: IT-Sicherheit mit System, S. 451f;
Deutsche Polizei: Polizeiliche Kriminalprävention – passwort + fishing = phishing, http://www.polizei-beratung.de/vorbeugung/gefahren_im_internet/phishing/begriff/, Abgerufen am 13.04.2010;
c't: c't – 21.06.09 – Mehr Rechte für Phishing-Opfer, http://www.heise.de/ct/meldung/Mehr-Rechte-fuer-Phishing-Opfer-184249.html, Abgerufen am 13.04.2010

Internetseiten und E-Mails sind die häufigsten Angriffsversuche.[2] Ein weiterer Versuch der Kategorisierung könnte Phishing als eine Unterart von Spam definieren.[3]

Phishing ist nicht gleich Phishing. Es unterscheidet sich in Vorgehensweise und Zielgruppe. Je nachdem kann Phishing in weitere Unterarten unterteilt und verschiedene Phishing-Angriffe als eine davon oder in eine weitere, hier nicht erwähnte Art, eingeordnet werden. Die bekanntesten Unterarten von Phishing sind *Spear Phishing, SMiShing, Pharming* und *Vishing*.

Spear Phishing (Speer-Phishing oder gezieltes Phishing) richtet sich lediglich an eine kleine vorher genau ausgewählte Zielgruppe. Diese sind niemals Privatpersonen sondern immer Unternehmensmitarbeiter, Manager, Chefs, etc. Der Täter tarnt den Absender, als wäre die Nachricht vom Chef oder Systemadministrator des Unternehmens und fordert dann persönliche oder unternehmensrelevante Daten an. Beim Spear Phishing bedarf der Täter einer großen Vorbereitungszeit, denn er muss gezielt das Opfer aussuchen und seinen Angriff perfekt auf dieses ausrichten, um zum Erfolg zu kommen. Meist sind die Täter in diesem Fall Industriespione oder ähnliches.[4]

SMiShing bezeichnet das Phishing per SMS. Dabei werden häufig SMS über ein gebuchtes Abo verschickt, wobei das Opfer auf eine Internetseite umgeleitet wird, auf der ein spezieller Trojaner platziert wurde.[5] Wenn DNS-Anfragen von Internetseiten gefälscht werden und ein Opfer somit bei korrekter Eingabe einer Internetadresse dennoch auf eine gefährliche Homepage gelangt, so nennt man diesen Phishing-Versuch auch Pharming.[6] Auch das Vishing (Voice Phishing) ist lediglich ein Synonym für Phishing per Telefon.[7]

3. Zahlen, Fakten und Beispiele

Obwohl Phishing in dieser Zeit aus den Schlagzeilen der Medienwelt verschwunden ist, ist es so präsent, wie zuvor. Dies bestätigt ein aktueller Fall vom achten Oktober 2009, wo 10.000 E-Mail-Postfächer von Microsofts E-Mail-Diensten *Hotmail, MSN* und *Live* im Internet für alle Internetbenutzer veröffentlicht wurde. Dabei wurden viele Konten mit den Anfangsbuchstaben A und B bestätigt durch Phishing ausgespäht und die somit erworbenen Daten auf eine Homepage umgeleitet. Microsoft geht aber nicht davon aus, dass es ein

[2] Müller, Klaus-Rainer: IT-Sicherheit mit System, S. 461f
[3] Friedmann, Katharina: Was tun? – Das Risiko durch Phishing steigt – computerwoche.de, http://www.computerwoche.de/security/578008/index5.html, Abgerufen am 14.04.2010
[4] Microsoft: Spear Phishing: gezielte Phishingangriffe, http://www.microsoft.com/germany/protect/yourself/phishing/spear.mspx, Abgerufen am 14.04.2010
[5] Wikipedia: Phishing – Wikipedia: http://de.wikipedia.org/wiki/Phishing#SMS_.28SMiShing.29, Abgerufen am 14.04.2010
[6] Müller, Klaus-Rainer: IT-Sicherheit mit System, S. 451
[7] Feser Frank: Phishing – EDV- und IT-Recht, http://www.informationstechnologie.undrecht.info/phishing_und_recht.html, Abgerufen am 14.04.2010

gezielter Angriff gewesen war.[8] Es zeigt sich, dass selbst große Konzerne, die wohl mit den Angriffen aus dem Internet vertraut sind, nichts gegen Phishing unternehmen können, denn Phishing ist schwer als Spam-Mail zu identifizieren. Selbst in der kurzen Zeit, in der diese Ausarbeitung erstellt wurde, gingen aktuelle Phishing-Mails bei E-Mail-Konten ein, wie in Abbildung 1: Aktuelle Phishing-Mail als angebliche PayPal-Kontobestätigung zu sehen ist.

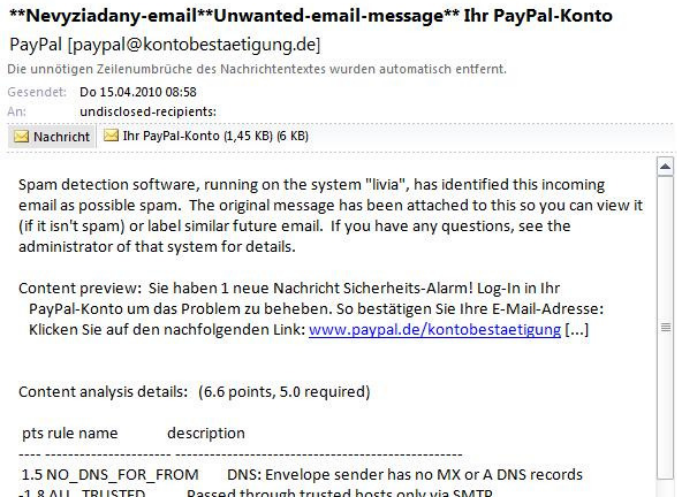

Abbildung 1: Aktuelle Phishing-Mail als angebliche PayPal-Kontobestätigung

Wie deutlich zu sehen ist, weißt die E-Mail auf einen angeblichen Sicherheitsalarm und die Vertrauenswürdigkeit der E-Mail hin. Es zeichnen sich immer die gleichen Muster ab. Die Täter sind meist so geschickt, dass sie in ihren Phishing-Mails auf gefährliche Phishing-Mails hinweisen und dass zum Schutz die Daten noch einmal abgeglichen werden müssen. Und wie sich zeigt, ist es eine erfolgreiche Masche.

Die Verbreitung von Phishing weltweit beschränkt sich vor allen Dingen auf die führenden Industrienationen. Dabei gibt es anscheinend mehr und weniger lohnenswerte Länder, wie eine Statistik über die Verbreitung von Phishing weltweit zeigt.[9] Dabei wurden in den letzten 12 Monaten vor allen Dingen die USA mit 67 % und Schweden mit 14 % von Phishing-Attacken heimgesucht. Deutschland liegt dabei mit 1,24 % im Mittel der restlichen Industrienationen. Werden aber lediglich die letzten 90 Tage betrachtet, fällt Schweden mit unter 0,1 % heraus und in Deutschland haben sich die Attacken auf 2,13 % fast verdoppelt. Dies zeigt, dass Phisher einmal mehr oder weniger stark auf bestimmte Länder fixiert sind oder das bestimmte Staaten sich erfolgreicher gegen Phishing-Attacken wären können als andere. Das Phisher mit Schwerpunkt in Industrienationen am Werk sind, liegt am höheren Profit und an lohnenderen Spionagezielen. Abbildung 2: Attacken in einem gewählten Zeitraum in Deutschland prozentual zur Welt gesehen zeigt deutlich, dass in den letzten

[8] Konsumo: 10.000 E-Mail Postfächer ausgespäht – Phishing-Angriff ist die Ursache, http://www.konsumo.de/news/3395-email-phishing-microsoft-postfach-passwort-mehrfach-verwendet-online-betrug, Abgerufen am 13.04.2010

[9] APWG: APWG: Crimeware Map, http://www.antiphishing.org/crimeware.html, Abgerufen am 16.04.2010

Wochen bzw. Monaten die Zahl der Phishing-Versuche gestiegen ist. In Deutschland brachte es den Angreifern alleine in den Jahren 2004/2005 4,5 Millionen Euro ein.[10]

Eine Statistik des Phishingberichts des ersten Halbjahres 2009 der APWG (Antiphishing Organisation)[11] zeigt deutlich, dass die Phisher gerade in den Industrienationen ihre Server positionieren. Dabei sind die USA, China, Schweden, Kanada und Deutschland meist unter den Top 5 der Ländern mit am meisten gehosteten Internetseiten von Phishing-Betrügern. Jedoch bildet die USA mit häufig mehr als 50 % das Zentrum.

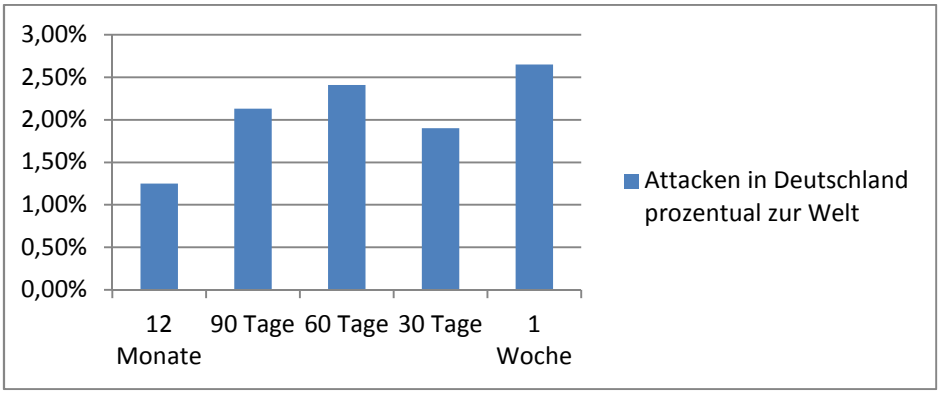

Abbildung 2: Attacken in einem gewählten Zeitraum in Deutschland prozentual zur Welt gesehen

Generell ist ein stetiger Zuwachs von Phishing-Attacken zu Verzeichnen. Die Methoden ändern sich von Zeit zu Zeit, es wird unauffälliger und noch perfekter Datenklau betrieben. So gab es in Deutschland vom Januar 2004 bis Dezember 2004 einen Zuwachs von 1200%[12], d. h. um das Zwölffach höhere Opferzahlen. Wird dieser Zuwachs mit dem Profit verrechnet, ergibt sich ebenso eine Erhöhung um das Zwölffache und zeigt, dass es sich um ein lohnendes Geschäft handelt.

4. Die Phisher, Motive und Methoden

Der Profit ist das grundsätzliche Motiv eines Phishers. Andere Motive sind lediglich die vorausgehenden Motive. So kann ein Angreifer neben Geld auch die Daten von Benutzern oder speziellen Personen in Besitz bringen, um damit einer Personengruppen oder Privatperson erheblich zu schädigen. Auch der Identitätsdiebstahl ist ein oft erwähntes Motiv, denn der Täter kann sich dann unter entsprechenden Umständen leicht als eine andere ihm oftmals unbekannte Person ausgeben. In der Wirtschaft werden außerdem Phishing-Attacken eingesetzt, um Betriebsgeheimnisse anderer Firmen oder brisante Informationen zu erlangen. Die Betriebsgeheimnisse können Forschungsergebnisse, noch nicht angemeldete Patente oder neue Ideen/Konzepte sein. Ganze Branchen könnten durch die Bekanntgabe von gefährlichen Informationen einen Image- und somit einen

[10] Janowicz, Krzysztof: Sicherheit im Internet, S. 244
[11] APWG: APWG: Phishing Activity Trends Report 1st Half 2009, S. 7
[12] Redaktion beck-aktuell: Nachrichten, Pressemitteilungen, Fachnews, becklink 132157

Produktionsverlust erleiden. Somit steht auch das Motiv des Wettbewerbsvorteils und der Spionage.[13] Die Motive offenbaren somit auch die Täter als gewöhnliche Kriminelle oder Firmen.[14]

Das Prinzip des Phishings und die Methoden der Täter sind sehr einfach. Sie folgen immer einem allgemeinen Szenario und unterscheiden sich oft nur in dem Medium der Weitergabe und der Zielgruppe.

Zunächst bereitet sich ein Phisher stets auf seinen Phishing-Angriff vor. Hat er seine Vorbereitungen abgeschlossen, versucht er über ein bestimmtes Medium ein gefälschtes Dokument an potentielle Opfer zu übermitteln. War dies erfolgreich und ein Opfer hat das Dokument unwissentlich ausgefüllt, kann der Angreifer mit Hilfe der Eingaben des Opfers seine vorher überlegte Absicht ausführen. In neueren Varianten dieses Schemas werden statt Dokumenten auch sogenannte Trojaner übermittelt. Bei einem Trojaner (oder Trojanisches Pferd) handelt es sich um ein Programm, dass neben seiner bekannten ebenfalls eine versteckte Funktion besitzt. Diese versteckte Funktion kann dann von innen heraus Schaden anrichten, z. B. Passwörter lesen, Tasteneingaben protokollieren, etc.[15] Ein solcher Trojaner würde im Phishing-Fall den Benutzer unbemerkt auf eine andere Internetseite umleiten, obwohl er die korrekte Internetadresse in seinen Browser eingegeben hat.[16] Diese Form des Phishings ist wesentlich gefährlicher und selbst für sicherheitsbewusste Benutzer sehr schwer auszumachen.

Ein Beispielszenario, sozusagen zum Nachmachen, würde für Internetseiten wie folgt aussehen. Der Betrüger sucht sich zunächst seine Zielgruppe aus. Diese kann aus den Kunden einer speziellen Bank, von E-Bay, von E-Mail-Diensten, etc. bestehen. Dann erstellt er eine täuschend echte Kopie der Internetpräsenz des Anbieters. Die Kopie einer Internetseite erstellt sich durch die *Seite speichern*-Funktion eines Browser leicht. Dabei ändert der Täter lediglich die Felder oder das auszuführende Skript um. Professionelle Betrüger leiden bei einem Login das Opfer wieder auf die korrekte Homepage zurück, um weniger Aufsehen zu erregen. Auch weisen besonders dreiste Datendiebe auf ihren Internetkopien auf die Gefahr von Phishing-Mails hin. Hat der Betrüger einmal die Homepage erstellt, benötigt er nur noch einen geeigneten Server, um sie auch im Internet verfügbar zu machen. Dabei achtet er darauf, dass möglichst keine persönlichen Informationen angegeben werden müssen bzw. diese nicht überprüft werden und pro-forma sind. Jede Internetpräsenz besitzt eine IP-Adresse, über die diese abzurufen ist. Damit der Betrug nicht offensichtlich scheint, maskiert ein Phisher diese durch einen anderen Zeichensatz (alt, da häufig nicht mehr angezeigt), durch einen Trojaner oder ähnlichem. Um

[13] Friedmann, Katharina: Was tun? – Das Risiko durch Phishing steigt – computerwoche.de, http://www.computerwoche.de/security/578008/index5.html, Abgerufen am 14.04.2010
[14] Friedmann, Katharina: Was tun? – Das Risiko durch Phishing steigt – computerwoche.de, http://www.computerwoche.de/security/578008/index5.html, Abgerufen am 14.04.2010
[15] ITWissen: Trojaner :: trojan :: ITWissen.info, http://www.itwissen.info/definition/lexikon/Trojaner-trojan.html, Abgerufen am 16.04.2010;
Schulze, Hans Herbert: Computerlexikon – Fachbegriffe schlüssig erklärt, S. 201f
[16] Redaktion beck-aktuell: Nachrichten, Pressemitteilungen, Fachnews, becklink 132157

später im aktuellen Land lange unerkannt zu bleiben, richtet sich der Täter ein Bankkonto im Ausland ein, worauf das geklaute Geld später überwiesen wird. Über ein Spam-Programm werden dann Kopien einer glaubhaft scheinenden E-Mail verschickt, diese sind oft so gut ausgearbeitet, dass sie von normalen Spam-Filtern nicht als dieses erkannt werden. Ab diesem Zeitpunkt braucht der Betrüger nur noch zu warten, bis ihm genügend Opfer in die Falle gegangen sind. Dadurch erhält er persönliche Daten oder Geld auf seinem Konto. Die persönlichen Daten verwendet er wiederrum, um Überweisungen oder Einkäufe zu tätigen. Um nicht zu viel Aufsehen zu erregen, werden nach kurzer Zeit alle Spuren gelöscht, d. h. die Internetpräsenz gelöscht und das Auslandskonto aufgelöst. Danach kann der Täter auf eine neue Zielgruppe übergehen.[17]

5. Das Opfer und die Folgen

Das Opfer hingegen bekommt vom eigentlichen Phishing-Betrug kaum etwas mit. Es erhält beispielsweise eine unauffällige E-Mail seiner Bank, worin auf eine angebliche Kontoschließung nach einigen Tagen hingewiesen wird, wenn die Kontodaten mit dem Opfer bis zu diesem Zeitpunkt nicht verglichen werden. Dann klickt das Opfer auf einen Internetlink und wird auf eine Kopie der Internetpräsenz seiner Bank umgeleitet. Dort meldet er sich unter seinen Daten an, befindet sich auf der richtigen Seite der Bank wieder, loggt sich aus, um nach einigen Wochen einen Geldabzug von 100-10.000 Euro[18] auf seinem Kontoauszug zu entdecken. Ein höherer Betrag wird von einem Konto nicht abgebucht, um einerseits nicht das Abbuchungslimit zu überschreiten und andererseits nicht ab 12.500 Euro in das Geldwäschergesetz in Kraft zu fallen.[19]

Weitere Folgen eines solchen Phishing-Angriffs können auch rechtliche Konsequenzen wegen der Umleitung auf strafrechtlich-relevanten Internetseiten[20] sein oder den Zugriffsverlust auf E-Mail-Konten und anderer Konten bedeuten, wo Passwörter via E-Mail angefordert werden.[21] Über den möglichen Image- oder Produktverlust wurde bereits berichtet.[22]

[17] Janowicz, Krzysztof: Sicherheit im Internet, S. 244ff
[18] Janowicz, Krzysztof: Sicherheit im Internet, S. 244
[19] Janowicz, Krzysztof: Sicherheit im Internet, S. 244
[20] Redaktion beck-aktuell: Nachrichten, Pressemitteilungen, Fachnews, becklink 282477
[21] Konsumo: 10.000 E-Mail Postfächer ausgespäht – Phishing-Angriff ist die Ursache, http://www.konsumo.de/news/3395-email-phishing-microsoft-postfach-passwort-mehrfach-verwendet-online-betrug, Abgerufen am 13.04.2010
[22] Friedmann, Katharina: Was tun? – Das Risiko durch Phishing steigt – computerwoche.de, http://www.computerwoche.de/security/578008/index5.html, Abgerufen am 14.04.2010

6. Ursachen für einfaches Phishing und Schutzmöglichkeiten

Doch warum haben Phisher so einen hohen Erfolg? Dies hat mehrere Ursachen. Zum einen sind Internetbenutzer oft zu unsicher im Umgang mit dem Computer und dadurch auch im Umgang mit dem Internet. Diese fehlende Sicherheit geht auch häufig mit fehlendem Sicherheitsbewusstsein einher und in den Zeiten sehr guter Firewalls, Antivirenprogramme und ständig erreichbarer Produktupdates sind einige Benutzer immer noch vollkommen ungesichert im weltweiten Netz. Zum anderen herrschen bei vielen Online-Banking-Homepages und Online-Kaufhäusern veraltete Sicherheitsstandards.[23] Eine weitere Ursache ist die Professionalität der Betrüger, denn welcher Benutzer achtet stets auf die vollkommen korrekte Internetadresse oder eine gesicherte Verbindung mittels *https*? Die Betrüger gestalten mittlerweile die E-Mails und Internetseiten auffallend gut und seriös, so dass lediglich Feinheiten über die Echtheit der Internetpräsenz Auskunft geben.[24] Ein Hauptgrund für den Erfolg von Phishing-Attacken ist das Internet selbst. Es wurde zur Gründungs- und Entwicklungszeit nicht für moderne Internetanwendungen, wie Online-Banking oder Online-Shops, konzipiert und muss sich erst langsam auf eine digitale, geschäftliche Welt ausbauen. Dabei sind die Anwendungen aber schneller im Umlauf, als sich das Internet in Punkto Sicherheit verbessert.[25]

Es gibt jedoch einfache Regeln, um die Anzahl von erfolgreichen Phishing-Attacken zu minimieren und somit die Gefahr eines jeden einzelnen zu verringern. Grundsätzlich gilt der Satz *Misstrauisch sein!*, denn oft reicht ein kritischer Blick, um einen Phishing-Betrug zu erkennen. Allgemein sollte jeder Benutzer von Online-Banking-Diensten in regelmäßigen Zeitabständen seinen Kontostand kontrollieren und auf etwaige, seltsame Abbuchungen sofort reagieren. Außerdem sollte jede Art von Online-Dienst an sicher geglaubten Computern und nicht in einem Internetcafé vorgenommen werden. Für jedes Benutzerkonto im Internet gilt, dass das Passwort für jeden Account anders lauten und ausreichend sicher sein sollte. Häufig kann ein Phisher mit einer E-Mail-Adresse und dazugehörigem Passwort nicht nur die E-Mails eines Opfers lesen, sondern gleichzeitig auch bei Amazon Einkäufe tätigen, da dort beispielsweise die E-Mail-Adresse auch der Nutzername ist. Weiterhin sollten niemals vertrauliche Daten ungesichert auf einem Computer abgespeichert werden, da diese einfach durch Spionagesoftware ausgespäht werden können. Abhilfe verschafft Software, die eine Anzahl an Daten passwortgeschützt verschlüsselt. Ein Computer muss mindestens eine Firewall und Antivirensoftware besitzen, die auf dem neuesten Stand sind. Auf dem neuesten Stand sollten auch alle anderen Produkte, wie das Betriebssystem, der Internet-Browser und andere Programme mit Verbindung zum Internet sein.[26] Weitere

[23] Janowicz, Krzysztof: Sicherheit im Internet, S. 243
[24] Microsoft: Erkennen von Phishingbetrug, betrügerischen E-Mails und Hoaxes, http://www.microsoft.com/germany/protect/yourself/phishing/identify.mspx, Abgerufen am 14.04.2010
[25] Janowicz, Krzysztof: Sicherheit im Internet, S. 244
[26] Deutsche Polizei: Polizeiliche Kriminalprävention – Vertrauen ist gut, Kontrolle ist besser, http://www.polizei-beratung.de/vorbeugung/gefahren_im_internet/phishing/tipps_und_verhaltenshinweise/, Abgerufen am 13.04.2010

Software, wie die *Windows Live Toolbar,* schützen zusätzlich vor Phishing-Betrügern.[27] Wichtig für unerfahrene Benutzer ist sich mit den Gefahren aus dem Internet vertraut zu machen. Dafür helfen Phishing-Erkennungslehrgänge, wie sie von einigen Organisationen angeboten werden. Diese müssen kostenlos sein, da sonst ebenfalls Betrug vorliegen kann. Ein Beispiel für einen solchen Lehrgang wäre der, der *Anti Phishing Organisation*.[28] Auch bieten Kreditinstitute häufig auf ihren Internetpräsenzen Informationen über die Gefahren von Online-Banking an. Als gutes Beispiel wäre da die Sparkasse zu erwähnen. Sie bieten neben einigen Informationen auch beispielhafte Phishing-Mails und geklonte Internetseiten an. Eine Phishing-Mail, welche sich als eine offizielle der Sparkasse ausgibt, sieht beispielsweise, wie in Abbildung 3: Als Sparkassen-E-Mail ausgebende Phishing-Mail zu sehen, aus. Der Link verweist auf eine geklonte Internetseite (Abbildung 4: Geklonte Internetpräsenz der Sparkasse).

Abbildung 3: Als Sparkassen-E-Mail ausgebende Phishing-Mail

Abbildung 4: Geklonte Internetpräsenz der Sparkasse

[27] Microsoft: Spear Phishing: gezielte Phishingangriffe, http://www.microsoft.com/germany/protect/yourself/phishing/spear.mspx, Abgerufen am 14.04.2010

[28] APWG: APWG CMU Phishing Education Landing Page Program, http://education.apwg.org/r/about.html, Abgerufen am 13.04.2010

Neben Kreditinstituten versuchen auch große Unternehmen, wie Microsoft, auf das Thema aufmerksam zu machen. Auf den Internetseiten von Microsoft lassen sich auch beispielhafte Phishing-Mails und kopierte Internetpräsenzen finden. Abbildung 5: Kopierte Internetseite einer amerikanischen Bank zeigt eine solche kopierte Internetseite einer amerikanischen Bank.

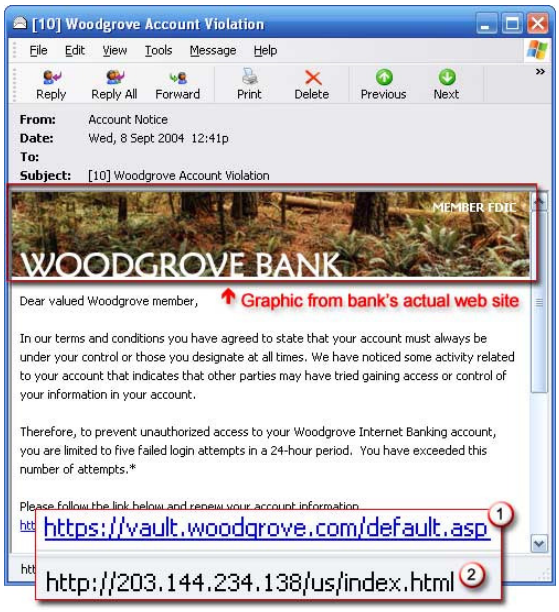

Abbildung 5: Kopierte Internetseite einer amerikanischen Bank

Eine weitere Vorgehensweise, wie sich ein Benutzer und eine Bank gegen Phishing schützen können, liegt in der Verantwortung von den Banken selbst. Diese sollten stets das neueste TAN-Verfahren anbieten. Neben dem normalen TAN-Verfahren, was ursprünglich aus einer Liste aus TANs bestand, wovon eine beliebige verwendet werden konnte, ist gerade das iTAN-Verfahren bei den Banken aktuell. Bei dem iTAN-Verfahren bekommt der Benutzer eine Liste von nummerierten TANs. Beim Online-Banking muss eine spezielle zufällige TAN eingegeben werden. Dies muss außerdem innerhalb von sieben Minuten geschehen, da ansonsten die Gültigkeit der TAN verfällt.[29] Die neueste Methode mTAN hat sich bisher noch nicht durchgesetzt. Es funktioniert analog dem iTAN-Verfahren, jedoch wird bei jeder getätigten Überweisung eine SMS mit den Daten als Gegencheck an ein Handy geschickt. So kann ein möglicher Betrug sofort erkannt und somit reagiert werden.[30]

Wichtig ist auch, dass jeder Benutzer, der eine E-Mail mit Verdacht auf Phishing-Mail erhält, diese an das Unternehmen weiterleitet, gegen den dieser Phishing-Versuch ausgerichtet ist, so dass diese Konzerne stets auf dem aktuellen Stand sind.

Bei E-Mails allgemein ist es wichtig, sich deutlich zu machen, dass ein Kreditinstitut niemals vertrauliche Daten per E-Mail oder Telefon anfordert. Daher sollten solche E-Mails

[29] Sparkasse: www.sparkasse.de: iTAN statt nur TAN, http://www.sparkasse.de/privatkunden/sicherheit-im-internet/itan.html, Abgerufen am 14.04.2010
[30] c't: c't – 21.06.09 – Mehr Rechte für Phishing-Opfer, http://www.heise.de/ct/meldung/Mehr-Rechte-fuer-Phishing-Opfer-184249.html, Abgerufen am 13.04.2010

geringsten Falls ignoriert und gelöscht werden. Außerdem dürfen niemals vertrauliche Daten allgemein über E-Mail verschickt werden, da diese zu leicht abgefangen werden können. Das Öffnen von E-Mail-Anhängen ist erst ungefährlich, wenn der Absender persönlich bekannt und eine Virensuche vergeblich ist. Ansonsten sollten Programme in E-Mail-Anhängen, wenn möglich, direkt auf der Internetseite heruntergeladen werden, wo es angeboten wird.[31] Gefährliche Anhänge besitzen häufig eine Dateiendung, wie *bat* für eine Batch-Datei oder auch eine verdeckte (Abbildung 6). Generell sollten Phrasen, wie *„Ihr Zugang zum Online-Banking wird geschlossen.“*, *„Überprüfung/Authentifizierung Ihres Online-Banking-Zugangs“*, *„Kontenauthentifizierung erforderlich.“*[32], *„Aktualisieren Sie die Daten Ihres Kontos.“*, *„Sie haben in der Lotterie gewonnen.“* und *„Sollten Sie innerhalb von 48 Stunden nicht antworten, wird Ihr Konto gesperrt.“*[33] ignoriert und die E-Mails nicht geöffnet werden.

Abbildung 6: Gefährliche Dateiendungen (links) und verdeckte Dateiendungen (rechts)

Im Internet sollte ein Benutzer stets mit der aktuellsten Version des Browser surfen. Der Browser *Mozilla Firefox* besitzt bereits ab Version 2.0[34] und der *Microsoft Internet Explorer* ab Version 7[35] einen integrierten Phishing-Schutz. Auch bietet die Homepage des Firefox Browsers auch eine Beispielseite, die zeigt, wie ein solcher Phishing-Schutz in Aktion aussieht (Abbildung 7). Dieser Schutz basiert allgemein auf einer Anzahl von registrierten, unsicheren Internetseiten. Wenn der Benutzer versucht auf solch eine zu gelangen, wird er darauf hingewiesen.

[31] Deutsche Polizei: Polizeiliche Kriminalprävention – Vertrauen ist gut, Kontrolle ist besser, http://www.polizei-beratung.de/vorbeugung/gefahren_im_internet/phishing/tipps_und_verhaltenshinweise/, Abgerufen am 13.04.2010

[32] Sparkasse: Phishing – so reagieren Sie richtig, http://www.sparkasse.de/privatkunden/sicherheit-im-internet/phishing-was-tun.html, Abgerufen am 13.04.2010

[33] Microsoft: Erkennen von Phishingbetrug, betrügerischen E-Mails und Hoaxes, http://www.microsoft.com/germany/protect/yourself/phishing/identify.mspx, Abgerufen am 14.04.2010

[34] Mozilla: Phishing-Schutz – FirefoxWiki, http://www.firefox-browser.de/wiki/Phishing-Schutz, Abgerufen am 13.04.2010

[35] Microsoft: Erkennen von Phishingbetrug, betrügerischen E-Mails und Hoaxes, http://www.microsoft.com/germany/protect/yourself/phishing/identify.mspx, Abgerufen am 14.04.2010

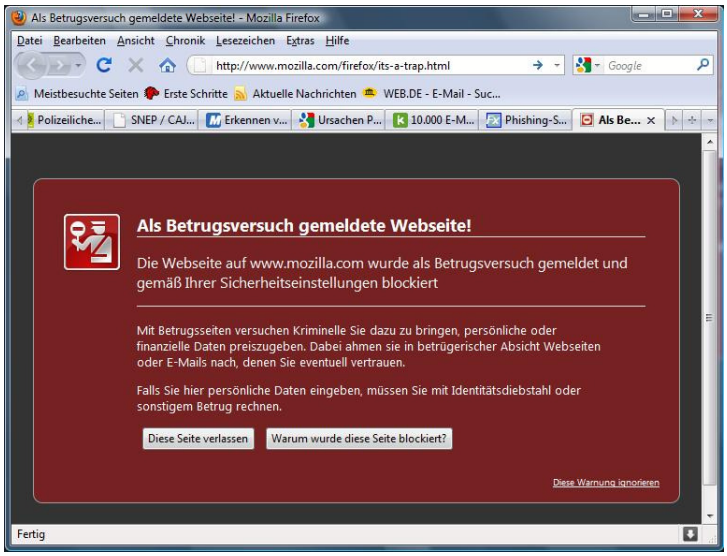

Abbildung 7: Phishing-Schutz im Mozilla Firefox

Das Surfen im Internet sollte sich außerdem nur auf vertrauenswürdige Seiten beschränken und häufig benutzte Internetseiten als Favorit, Tag, etc. abgespeichert werden. Die Internetadresse ist auch regelmäßig bei der Eingabe und bei einem Verweis mittels Link zu kontrollieren. Bei jedweder Unregelmäßigkeit in einem ansonsten häufig genutzten Internet-Dienst misstrauisch sein und im Zweifel lieber keine persönlichen Daten eingeben. Auf gesicherte *https*-Verbindung achten und immer über die Startseite einer Homepage gehen.[36] Außerdem ist das Achten auf das Schlosssymbol im Browser[37] genauso wichtig, wie das Ablehnen von Internetseiten mit ungültigem SSL-Zertifikat[38].

Das Benutzen von Handy- oder Smartphone-Applikationen sollte ausschließlich über offizielle Software laufen. Das heißt eine Online-Banking-Applikation sollte direkt von der jeweiligen Bank stammen, ansonsten können Daten ohne Verdacht zu erregen auf dem Weg zum Online-Banking-Dienst mitgeschrieben werden.[39]

7. Was tun, wenn Phisher erfolgreich?

Ist eine Person trotz aller Vorsichtsmaßnahmen dennoch Opfer einer Phishing-Attacke, bleibt nur noch der Weg zur Bank und zur Polizei. Gegen den Täter kann und muss strafrechtlich vorgegangen werden. Dies hat bezüglich des Opfers keine Auswirkung, denn

[36] Deutsche Polizei: Polizeiliche Kriminalprävention – Vertrauen ist gut, Kontrolle ist besser, http://www.polizei-beratung.de/vorbeugung/gefahren_im_internet/phishing/tipps_und_verhaltenshinweise/, Abgerufen am 13.04.2010
[37] Sparkasse: www.sparkasse.de: Vorsicht Phishing, http://www.sparkasse.de/privatkunden/sicherheit-im-internet/phishing.html, Abgerufen am 14.04.2010
[38] Microsoft: Erkennen von Phishingbetrug, betrügerischen E-Mails und Hoaxes, http://www.microsoft.com/germany/protect/yourself/phishing/identify.mspx, Abgerufen am 14.04.2010
[39] Deutsche Polizei: Polizeiliche Kriminalprävention – Vertrauen ist gut, Kontrolle ist besser, http://www.polizei-beratung.de/vorbeugung/gefahren_im_internet/phishing/tipps_und_verhaltenshinweise/, Abgerufen am 13.04.2010

dieses kann lediglich von der Bank zivilrechtlich die Rückerstattung des Betrages fordern. Die Bank ihrerseits fordert den Betrag, wenn möglich, zivilrechtlich vom Betrüger.

Allgemein ist jede Bank verpflichtet, einen Verlustbetrag dem Opfer zurückzuerstatten, wenn bezüglich des Opfers keine Fahrlässigkeit vorlag und er für die Sicherheit seines Computers sorgt. Dazu reichen meist ein aktuelles Betriebssystem, eine aktuelle Antivirensoftware und eine aktuelle Firewall aus.[40] Rein rechtlich trägt die Bank stets das Fälschungsrisiko.[41] Bevor dies galt, war es schwierig für ein Opfer vor Gericht Recht zu bekommen und oft wurden Phishing-Fälle außergerichtlich zwischen Bank und Opfer geklärt.[42] Generell gilt, dass umso raffinierter der Phishing-Betrug war, umso leichter eine Rückerstattung von der Bank.[43] Das Verfahren ist juristisch kompliziert, da dies ein Fall ist, bei dem drei Parteien involviert sind und die Bank nicht unmittelbar betroffen war.

Der Täter muss seinerseits mit schweren strafrechtlichen Konsequenzen rechnen, falls er gefasst wird. Nach dem Landesgericht Darmstadt machen sich die Betrüger bei Phishing mit anschließendem Auslandstransfer nach einem Urteil vom 11. Januar 2006 (212 Ls 360 Js 33848/05) der gewerbsmäßigen Geldwäsche nach § 216 IV StGB strafbar. Außerdem ist auch mit einem Urteil wegen Computerbetruges nach § 263a StGB und des Ausspähens von Daten nach § 202a StGB zu rechnen.[44] Fälscht der Phisher dabei noch Internetseiten, E-Mails, Telefonanrufe, SMS, etc. macht er sich auch wegen Fälschung beweiserheblicher Daten nach $ 269 Abs. 1 Variante 1 StGB strafbar.[45]

Da es seitens der Banken oft lediglich eine unzureichende AGB gibt, die keinerlei Regeln und Voraussetzungen für Online-Banking vorschreiben, werden auch in Zukunft viele Prozesse geführt werden. Banken fühlen sich oft im Recht, da sie in ihren AGBs den Hinweis auf vertraulichen Umgang mit persönlichen Daten verankert haben.

---

[40] Dr. Schulte, Thomas: Dr. Thomas Schulte | Phishing: Die Rechte der Opfer, http://anwaltzentrale.de/rechtsanwalt_fachartikel/fachartikel_detail.php?id=238&Fachgebiet_id=17, Abgerufen am 14.04.2010

[41] c't: c't – 21.06.09 – Mehr Rechte für Phishing-Opfer, http://www.heise.de/ct/meldung/Mehr-Rechte-fuer-Phishing-Opfer-184249.html, Abgerufen am 13.04.2010

[42] c't: c't – 21.06.09 – Mehr Rechte für Phishing-Opfer, http://www.heise.de/ct/meldung/Mehr-Rechte-fuer-Phishing-Opfer-184249.html, Abgerufen am 13.04.2010

[43] Dr. Schulte, Thomas: Dr. Thomas Schulte | Phishing: Die Rechte der Opfer, http://anwaltzentrale.de/rechtsanwalt_fachartikel/fachartikel_detail.php?id=238&Fachgebiet_id=17, Abgerufen am 14.04.2010

[44] Dr. Schulte, Thomas: Dr. Thomas Schulte | Phishing: Die Rechte der Opfer, http://anwaltzentrale.de/rechtsanwalt_fachartikel/fachartikel_detail.php?id=238&Fachgebiet_id=17, Abgerufen am 14.04.2010

[45] Feser Frank: Phishing – EDV- und IT-Recht, http://www.informationstechnologie.undrecht.info/phishing_und_recht.html, Abgerufen am 14.04.2010

8. Fazit

Auch nach langer Zeit des Phishings haben die Betrüger immer noch genug Chancen und Umsätze, um ihren betrügerischen Vorhaben nachzugehen. Leider tappen viele Benutzer noch in plumpe Phishing-Angriffe und verspielen sich damit auch das Recht den Verlust von Kreditinstituten zurückzuerstatten. Es reichen oft ein natürliches Maß an Misstrauen, ein wenig Informationen über Online-Banking und der Minimalschutz von Computern aus, um Phishing-Attacken vorzubeugen. Zwar werden Phishing-Betrüger in den letzten Jahren immer ausgefeilter und sind manchmal nur schwer oder gar nicht auszumachen, doch haben die Opfer dann das Recht den Verlust von den Kreditinstituten zurück zu bekommen. Es ist zu hoffen, dass auch gegen die neueren Methoden nicht der einzige Schutz die Rückerstattung von Beträgen bleibt, sondern dass sich auch die Sicherheitstechnologien weiter den Phishing-Angriffen anpassen.

So ist den Phishern nur zu wünschen, dass immer weniger Menschen den frohen Fischergruß *Petri Heil!* zurufen und das Echo *Petri Dank!* immer leiser im Ozean des Internets verhallt.

9. Bildquellen

10. Literaturverzeichnis

APWG. (18. Oktober 2009): *APWG CMU Phishing Education Landing Page Program*. Abgerufen am 13. April 2010 von http://education.apwg.org/r/about.html

APWG. (8. Juli 2009): *APWG: Crimeware Map*. Abgerufen am 13. April 2010 von http://www.antiphishing.org/crimeware.html

APWG: Phishing Activity Trends Report 1st Half 2009. http://www.antiphishing.org/reports/apwg_report_h1_2009.pdf

c't. (21. Juni 2009): *c't - 21.06.09 - Mehr Rechte für Phishing-Opfer*. Abgerufen am 13. April 2010 von http://www.heise.de/ct/meldung/Mehr-Rechte-fuer-Phishing-Opfer-184249.html

Deutsche Polizei: *Polizeiliche Kriminalprävention – passwort + fishing = phishing*. Abgerufen am 13. April 2010 von http://www.polizei-beratung.de/vorbeugung/gefahren_im_internet/phishing/begriff/

Deutsche Polizei: *Polizeiliche Kriminalprävention – Vertrauen ist gut, Kontrolle ist besser*. Abgerufen am 13. April 2010 von http://www.polizei-beratung.de/vorbeugung/gefahren_im_internet/phishing/tipps_und_verhaltenshinweise/

Feser, F: *Phishing - EDV- und IT-Recht*. Abgerufen am 14. April 2010 von http://www.informationstechnologie.undrecht.info/phishing_und_recht.html

Friedmann, K. (27. Juni 2006): *Was tun? - Das Risiko durch Phishing steigt - computerwoche.de*. Abgerufen am 14. April 2010 von http://www.computerwoche.de/security/578008/index5.html

ITWissen: *Trojaner :: trojan :: ITWissen.info*. Abgerufen am 16. April 2010 von http://www.itwissen.info/definition/lexikon/Trojaner-trojan.html

Konsumo. (8. Oktober 2009): *Konsumo, 10.000 E-Mail Postfächer ausgespäht - Phishing-Angriff ist die Ursache*. Abgerufen am 13. April 2010 von http://www.konsumo.de/news/3395-email-phishing-microsoft-postfach-passwort-mehrfach-verwendet-online-betrug

Krzysztof, J.: *Sicherheit im Internet.* 2. Auflage Köln 2006

Microsoft. (30. Januar 2009): *Erkennen von Phishingbetrug, betrügerischen E-Mails und Hoaxes*. Abgerufen am 13. April 2010 von http://www.microsoft.com/germany/protect/yourself/phishing/identify.mspx

Microsoft. (30. Januar 2009): *Spear Phishing: gezielte Phishingangriffe*. Abgerufen am 13. April 2010 von http://www.microsoft.com/germany/protect/yourself/phishing/spear.mspx

Mozilla. (12. September 2008): *Phishing-Schutz - FirefoxWiki*. Abgerufen am 13. April 2010 von http://www.firefox-browser.de/wiki/Phishing-Schutz

Müller, K.-R.: *IT-Sicherheit mit System: Sicherheitspyramide; Sicherheits-, Kontinuitäts- und Risikomanagement; Normen und Practices; SOA und Softwareentwicklung.* 3. Auflage Wiesbaden 2007

Redaktion beck-aktuell. (6. Dezember 2004): Nachrichten, Pressemitteilungen, Fachnews, becklink 132157

Redaktion beck-aktuell. (28. Mai 2009): Nachrichten, Pressemitteilungen, Fachnews, becklink 282477

Schulte, D. T. (30. November 2006): *Dr. Thomas Schulte | Phishing: Die Rechte der Opfer*. Abgerufen am 14. April 2010 von http://anwaltzentrale.de/rechtsanwalt_fachartikel/fachartikel_detail.php?id=238&Fachgebiet_id=17

Schulze, H. H.: *Computerlexikon - Fachbegriffe schlüssig erklärt.* 1. Auflage Reinbek bei Hamburg 2003

Sparkasse: *www.sparkasse.de: iTAN statt nur TAN*. Abgerufen am 13. April 2010 von http://www.sparkasse.de/privatkunden/sicherheit-im-internet/itan.html

Sparkasse: *www.sparkasse.de: Phishing - so reagieren Sie richtig*. Abgerufen am 13. April 2010 von http://www.sparkasse.de/privatkunden/sicherheit-im-internet/phishing-was-tun.html

Sparkasse: *www.sparkasse.de: Vorsicht Phishing*. Abgerufen am 13. April 2010 von http://www.sparkasse.de/privatkunden/sicherheit-im-internet/phishing.html

Wikipedia: *Phishing - Wikipedia*. Abgerufen am 14. April 2010 von http://de.wikipedia.org/wiki/Phishing#SMS_.28SMiShing.29