Ralph Lehmann
IT-Sicherheitsanalyse
und Beratung

Ralph Lehmann • IT-Sicherheitsanalyse und Beratung • Kochstraße 34 • 04275 Leipzig

Kochstraße 34
04275 Leipzig

Tel.: (03 41) 3 06 99 05
Fax: (03 41) 3 08 10 31
mobil: (01 70) 3 11 37 35

e-mail: info@ralph-lehmann.de
Web: www.ralph-lehmann.de

Wie funktioniert eigentlich Phishing? Die Maus erklärt!

Eine Satire von Dr. Andreas Beck (becka@uni-duesseldorf.de), überarbeitet und mit einem Glossar versehen von Ralph Lehmann (info@ralph-lehmann.de)

Das Original ist z.B. bei Google – Groups unter der Message-ID slrndop13l.c5v.becka-news-nospam-2005-11@xeon.mcs.acs.uni-duesseldorf.de zu finden.

Hallo, das ist der Peter. Der Peter ist ein böser Mensch, der gutgläubigen ~~Trott~~ äh Leuten das Geld vom Konto klauen will. Man nennt so was einen Phisher[1)].

Dazu sucht er sich erst mal eine Bank aus, deren Kunden er ausnehmen will. Am besten eine mit einer möglichst bunten und unübersichtlichen Website.

Diese Website baut er jetzt nach. Natürlich nur fast. Er baut eine Seite, die genauso aussieht, die aber nach Kontonummer, PIN, TAN, Kreditkartendaten, Schuhgröße der Ehefrau und sexuellen Vorlieben des Haustieres fragt.

Die muss er jetzt irgendwie ins Internet stellen. Die Bank wird er wohl nicht dazu überredet kriegen. Also mietet er entweder irgendwo Webspace[2)] mit einer geklauten Kreditkarte an, verwendet einen Freehoster[3)], oder er knackt einfach eine der vielen bunten, beschissen gewarteten Websites, auf denen irgendein PHP[4)]-~~Kot~~ äh -Code sein Unwesen treibt. Bevorzugt in Asien, weil dort das Abusemanagement[5)] oft grauenhaft ist.

So. Jetzt muss der Peter nur warten, dass genug Leute die Fragen auf seiner Seite ausfüllen. Wenn das einer tut, schickt ihm der Server eine Mail, oder er holt die Dateien ab und zu, oder der Server leitet das alles in irgendeinen IRC-Channel weiter, oder ... hach – die Möglichkeiten des Internet sind einfach herrlich ...

Nur: Es kommt niemand auf seine Seite. Das ist natürlich schlecht. Also fragt er seinen Kumpel Stefan Spammer[6)], ob er nicht ein paar ~~Idio~~ äh Besucher für seine Seite finden kann. "Nichts einfacher als das!", sagt Stefan, "Ich schicke einfach ein paar hundert Millionen Mails raus – da sind immer ein paar Volltrottel dabei."

Gesagt getan. Alsbald landet eine solche Mail in der Mailbox von Achim Ahnungslos. Sie verkündet großes Unheil – sein Konto würde gesperrt und die Katze wegen Steuerhinterziehung verklagt, wenn er nicht sofort seine Kontodaten bestätige. Das alles mit der krass sicheren neuen Spezialsicherungsmethode von der Bank gegen die Missetäter.

Entsetzt klickt Achim auf den Link und findet seine bunt blinkende Bankseite vor – denkt er. Schließlich guckt er nicht in die Adressleiste, in der http://192.168.45.87/phishing/enter.php steht und auch nicht auf das offen rumhängende Schloss rechts unten, welches anzeigt, dass die Verbindung nicht sicher[7)] ist. Und außerdem nutzt er sowieso den IE[8)], der ja bekanntlich auch ohne so Zeug voll sicher ist!

Besonders weil er auch die neueste Version von Schlangenöl 2006[9)] auf seinem Rechner hat. Da kann im Internet eh gar nix mehr passieren. Sagt sein Kumpel, der Sackmann[10)].

Auf der Seite soll er sich erst mal einloggen – das ist schnell passiert. (Warum hat eigentlich der Browser die Felder nicht selbst ausgefüllt, wie sonst immer? Muss wohl an der neuen Sicherheit liegen!)[11] Sooo – nächste Seite ... Was wollen die wissen? Ach ja: den Namen, und dann soll man 3 bis 23 noch unverbrauchte TANs eintragen. Die Liste rausgekramt und alles eingehackt – schnell, bevor der Katze was passiert!

"Weiter" ... was denn jetzt noch? Kreditkarte? Aber die ist doch gar nicht von denen?! Na, wenn's der Sicherheit dient, ... **klacker klacker** ...

"Weiter" – aahh - Sicherheitsüberprüfung abgeschlossen. Sie werden zur Startseite der Bank weitergeleitet. PUUHH – da haben wir aber noch mal Schwein gehabt!

Auf der anderen Seite der Leitung freut sich Peter Phisher. Er hat gerade via IRC die gewünschten Daten von Achim gekriegt. Jetzt mal schnell, bevor der noch auf die Idee kommt, mal bei der Bank nachzufragen!

Damit er nicht so leicht zu verfolgen ist, schnappt er sich schnell einen anonymen Proxy[12] – die Liste hat er günstig von Charlie Cracker gekauft - und macht eine Überweisung. Bloß an wen???

Seine eigenen Konten wären irgendwie unpraktisch. Außerdem sind Auslandüberweisungen den Banken eh suspekt ... nee, das muss anders gehen.

Er fragt wieder seinen Kumpel Stefan Spammer. Und der weiß wieder Rat. Er schickt eine neue Mail. Mit einer rührseligen Geschichte von russischen Programmierern, die nur 40% von dem verdienen, was sie kriegen würden, wenn sie Deutsche wären. Und ob der geneigte Empfänger nicht für 15% bereit wäre, ein bisschen Geld über sein Konto fließen zu lassen. Er müsste ja fast nix tun, und 15% für ihn wären dafür nicht schlecht und 85% für den Programmierer besser als 40%. Das Geld würde dann am einfachsten per irgendwelchen postalischen Bargeldanweisungen weitergeleitet, weil das ja am schnellsten ginge.

Auch dafür finden sich schnell einige ~~Gierschlü~~ äh nette Mitbürger. Zum Beispiel Rudolph Raffzahn.

Jetzt kann's losgehen. Peter besucht die Bankseite – diesmal die echte – wieder per anonymem Proxy und gibt brav alles ein, was ihm Achim ins Formular getippt hat. Hey – er hat sich nicht mal vertippt! Und er ist auch keiner dieser asozialen Spielverderber, die Unsinn eingeben[13].

Sooo – schnell eine Überweisung von EUR 1000 an Rudolph Raffzahn. Und morgen dann eines der Straßenkids kurz zur Post schicken, um die 850 EUR von Rudolph abzuholen.

In der Zwischenzeit hat aber auch Hans Helle so eine Mail[14)] gekriegt – und gemerkt, dass er da übers Ohr gehauen werden soll. Also leitet er die Nachricht an seine Bank weiter.

Die versucht jetzt erst mal, die andere Seite vom Netz zu kriegen. Theoretisch hat sie dazu sogar zumeist eine Handhabe – schließlich wird dort ja mit deren Warenzeichen, Logos etc. rumgeaast. Bloß – bis Walter Webforum, der Betreiber des wegen antikem Patchstand[15)] des darauf abgeladenen PHP-Sondermülls gehackten Webservers, gefunden und dazu veranlasst wurde, den Rechner abzuschalten, das dauert.

Inzwischen finden sich fröhlich weitere Achims.

Einige Tage später holt Achim seine Kontoauszüge – und staunt nicht schlecht: "Wer ist Rudolph Raffzahn, und warum soll ich dem 1000 EUR überwiesen haben?”

Er fragt seine Bank, und die erklärt ihm, er habe das online veranlasst. "Quatsch – einen Scheiß hab ich! Betrüger! Ich geh zur Polizei!"

Dort erklärt man ihm, dass seine Katze nie in Gefahr war und er einem Betrüger seine Kontodaten gegeben habe. "Quatsch, das war die Seite meiner Bank! Da war überall das Logo und sogar die Warnung vor solchen Verbrechern, und ein dickes fettes Schloss war da auch, und da stand, alles wäre jetzt noch sicherer! Und mein Schlangenöl 2006 hat auch nicht gemeckert."

Und überhaupt will er wissen, wer denn dieser Rudolph Raffzahn wäre. Das, sagen ihm die Beamten, würde gerade ermittelt.

Und in der Tat – schon am nächsten Tag stehen einige freundliche Beamte vor Rudolph Raffzahns Tür und eröffnen ihm, dass sie wegen Verdacht auf Geldwäsche gegen ihn ermitteln. Rudolph fällt aus allen Wolken und zeigt den Herren seine Mailkorrespondenz und alle Belege seiner ordentlichen Weiterleitungen für die netten Programmierer aus Russland.

"Schade", denkt sich Peter, als keine Anweisungen von Rudolph mehr kommen, "da muss ich mir wohl einen neuen Mitarbeiter suchen. Und eine neue Webseite brauche ich auch, die letzte ist ja inzwischen offline."

Aus, die Maus.

<u>Glossar</u>

1) jemand, der versucht, sich unberechtigt Passwörter und andere Zugangsdaten zu verschaffen
2) Speicherplatz für Webseiten
3) jemand, der Speicherplatz für Webseiten unentgeltlich zur Verfügung stellt
4) in der Vergangenheit oft durch Sicherheitsmängel aufgefallene, aber trotzdem außerordentlich beliebte Scriptsprache

5) Handhabung von Beschwerden
6) Versender unerwünschter Werbung
7) eigentlich nicht verschlüsselt – viele Pisher verzichten darauf, die Übertragung zu verschlüsseln und sollten so vom Benutzer leicht von der echten Bankseite unterschieden werden können
8) Internet Explorer – von Microsoft zum Betriebsystem mitgelieferter Webbrowser, hat derzeit sicherheitstechnisch nicht den besten Ruf genießt
9) spielt auf so genannte Sicherheitssoftware an, die dem Benutzer Sicherheit lediglich vorgaukeln
10) Johannes Sackmann ist ein Nutzer des Usenets, dem oft vorgeworfen wird, dieses für kommerzielle Zwecke zu missbrauchen und inkompetente Ratschläge zu erteilen
11) auf der originalen Webseite der Bank hätte der Browser dies in diesem Falle getan
12) greift stellvertretend für den Benutzer auf eine Webseite zu und erschwert die Zurückverfolgung zum eigentlichen Benutzer
13) einige Empfänger von Pishing – Mails versuchen gewöhnlich, durch Eingabe ungültiger Daten dem Pisher zu schaden
14) die erste Version der Mail
15) die Software wurde nicht aktualisiert, bekannte Schwachstellen wurden nicht beseitigt