Phishers-Guide

Zum Phishers-Guide

Was Sie hier lesen, ist eine kleine Einführung zum Thema Phishing. Ich werde versuchen, Sie ausführlich in das Thema einzuführen ohne jedoch zu sehr ins Detail zu gehen oder Ihnen unnötige Fachwörter an den Kopf zu werfen. Geeignet ist das Paper eigentlich für jeden, der sich mit dem Thema auseinandersetzen möchte, egal ob Sie nun Abwehrmassnahmen gegen Phishing entwickeln oder sich einfach nur ein wenig sicherer fühlen wollen im Zeitalter des Internets.
So nun wünsche ich Ihnen viel Spass beim lesen und hoffe, Sie mit diesem Paper ein wenig für beziehungsweise gegen Phishing sensibilisiert zu haben.

PS: Natürlich gibt es noch viele weitere Techniken und auch viele Ausnahmen in diesem spannenden Bereich, die hier nicht behandelt werden, aber wie schon erwähnt, es handelt sich hier um eine Einführung und nicht um ein Fachbuch.

Was ist Phishing?

Phishing lässt sich in die Kategorie “Social Engineering“ einstufen, was soviel heisst wie „nicht einen Computer zu manipulieren, sondern den User, der davor sitzt“. Das besondere an Phishing ist jedoch, dass der Angreifer zum einen nicht direkt mit dem Opfer in Kontakt tritt und zum anderen, dass Phishing immer eine Reaktion vom Opfer abverlangt, sei es das Besuchen einer Webseite über einen Link aus einem Phishing-Mail oder zum Beispiel die Eingabe von Daten über sich auf einer gefälschten Webseite.
Warum das ganze Phishing heisst, möchte ich nicht selbst nochmals erläutern, da dies auf Wikipedia bereits sehr treffend und kurz erklärt wird: „Die Bezeichnung Phishing leitet sich vom Fischen (engl.: fishing) nach persönlichen Daten ab. Die Ersetzung von F durch Ph ist dabei eine im Insider-Jargon (Leetspeak) häufig verwendete Verfremdung. Es könnte unter Umständen sein, dass der Ausdruck auch auf **p**assword **h**arvesting f**ishing** zurückführbar ist.“

Ziele von Phishing

Phishing ist eine der wenigen Tätigkeiten, im Bereich der IT-Sicherheit, die nie gemacht werden, um zum Beispiel von der Community anerkannt zu werden, denn Spammer und Phisher sind nur auf eines aus nämlich Geld. Doch wie soll ein Phisher zu Geld kommen mit seiner “Arbeit“? Dazu gibt es verschiedene Methoden, die häufigste ist jedoch die, sich Onlinebanking-Zugangsdaten zu beschaffen. Hierzu werden Sie auf eine gefälschte Webseite Ihrer Bank gelockt und wollen sich anmelden. Wie gesagt, befinden Sie sich nur auf einer Nachgebauten Seite und diese wird Ihnen den Zugang verweigern. Während Sie sich nun wundern, warum Sie keinen Zugang erhalten, sitzt irgendwo auf der Welt ein Phisher oder

sogar ein automatisiertes System, dass mit Ihrer Daten, die auf der falschen Seite geloggt wurden eine grössere Überweisung auf ein Konto im Ausland tätigt. Somit, lässt es sich als Phisher sehr gut leben, wenn man es richtig macht.

1. Phishing im E-Mail

Das normale Phishing beginnt mit einer E-Mail, die zum Beispiel von Ihrer Bank stammt. Viele Leute wissen leider gar nicht, wie einfach es ist, eine E-Mail zu versenden, die für einen Laien unverkennbar von einer bestimmten Adresse kommt, also dem Absender, den Ihnen Ihr Mailprogramm anzeigt. Für eine Person, die auch nur ein bisschen programmieren kann, ist dies ein Aufwand von wenigen Minuten. Also glauben Sie bitte nicht, wenn sie eine E-Mail erhalten von name.eines.freundes@gmail.com, dass diese auch sicher von dieser Person ist. Zudem ist es auch ein Trend unter Phishern, sich mit Spammern und Wurm-Autoren zu verbünden, um dann wirklich nur gültige Mailadressen anzuschreiben oder auch um einen Pharmin-Angriff zu starten (siehe dazu Zusatz/Pharming – Wenn lokal gefischt wird). Nun zum eigentlichen Angriff, auch wenn dies eigentlich nicht wirklich der richtige Ausdruck dafür ist, da wie schon erwähnt, bei einem klassischen Phishing nichts passieren kann, wenn der User nicht auf den Phishingversuch eingeht.

Der Aufbau eines Phishing-Angriffs ist eigentlich immer gleich:

- Sie erhalten eine E-Mail von einem gefälschten Absender, den Sie bestenfalls sogar kennen.
- Im E-Mail finden Sie Werbung für etwas, dies können Medikamente, bis zu Aktien sein.
- Die E-Mail beinhaltet einen Link und Sie werden aufgefordert, diesen zu besuchen.

Dies sind die Grundmerkmale eines Phishing-Mails. Sollten Sie also einen Aufbau wie oben bemerken, zögern Sie nicht lange sondern löschen Sie die E-Mail. Denken Sie sich immer, wenn Sie aus Versehen eine Nachricht löschen, die doch kein Phishingversuch war, wird der Absender Sie bestimmt wieder kontaktieren.

2. Phishing auf Webseiten

Als wenn die Masche mit den gefälschten E-Mails nicht schon genügen würde, gehen die Phisher noch einen Schritt weiter, denn nur das anklicken eines Links bringt dem Phisher ja noch keinen Gewinn. Hier gibt es mehrere Vorgehensweisen der Phisher, doch möchte ich mich auf möglichst wenige beschränken, da es immer neue Methoden gibt diese jedoch meist immer auf früheren Techniken beruhen und dieses Paper in sagen wir drei Jahren zudem völlig veraltet wäre. Zum einen wären hier die Folgen vom Besuchen eines Links aus einem Phishing-Mail zu erwähnen, wobei dazu muss ich ja wohl nichts mehr schreiben, denn diesen Ablauf habe ich Ihnen schon unter dem Punkt “Ziele von Phishing“

näher gebracht. Es geht einfach darum, eine Webseite nachzubauen, um den User glauben zu machen, er befinde sich auf der richtigen Seite, obwohl dem nicht so ist. Des Weiteren werden die Phisher auch immer "kreativer" und gehen mit der Zeit, so ist es nicht verwunderlich, dass Trends aus der Hackerszene, nicht selten auch von Phishern übernommen werden. Gutes Beispiel hierfür ist zurzeit gerade das so genannte XSS oder Cross-Site Scripting oder auch Trojanische Pferde, die die Host-Datei auf einem lokalen System verändert haben, doch darauf möchte ich jetzt nicht näher eingehen, denn darüber könnte man ganze Bücher schreiben.

Sie sehen, es gibt unglaublich viele Möglichkeiten einen Phishing-Angriff durchzuführen aber es ist möglich einen Grossteil problemlos als Phishing zu enttarnen, wenn man sich darüber im Klaren ist, wo Gefahren lauern können.

Wie schütze ich mich gegen Phishing?
Nun stellt sich die Frage, wie man sich denn gegen Phishing-Angriffe schützen kann. Diese Frage kann leider nicht so einfach beantwortet werden, denn wie bereits gezeigt, gibt es Unmengen von Techniken im Bereich Phishing und es kommen auch immer wieder neue dazu. Faste jeder Angriffsversuch muss anders abgewehrt werden. Doch dem zu trotz gebe ich Ihnen hier eine kleine Checkliste mit, wie Sie sich vor einem Grossteil an Phishingversuchen schützen können.

- Löschen Sie E-Mails, deren Absender sie nicht kennen sofort.
- Klicken Sie keine Links (in E-Mails sowie im Internet) an, von denen Sie nicht genau wissen, wohin sie führen.
  Zum Beispiel:
  http://www.verdaechtig.com/sad29ehsdosjfk20rjdsfi9f398ef sollten Sie nie anklicken, wenn Sie sich dennoch für den Inhalt der Webseite interessieren gehen Sie zuerst auf die Seite http://www.verdaechtig.com und suchen dort nach dem richtigen Link, sollte Ihnen dies nicht gelingen, können Sie davon ausgehen, das es sich um einen Phishingversuch gehandelt hat.
- Löschen Sie E-Mails, die in einer Sprache geschrieben sind, die Sie entweder nicht beherrschen oder in der Sie mit niemandem per E-Mail Kontakt haben.

Zusatz
Hier finden Interessierte nun noch eine weitere Technik, die mit dem Phishing verwandt ist: Das Pharming. Leider ist zu sagen, das Pharming momentan einen regelrechten Trend erfährt und man sich als Durchschnitts-User nur sehr schwer dagegen wehren kann.

Pharming – Wenn lokal gefischt wird
Pharming nennt sich ein neuer Trend unter den Phishern, die leider auch zunehmend immer mehr mit Viren- und Wurm-Programmieren zusammenarbeiten. Hierbei wird nicht wie beim Phishing versucht, den

User auf eine bestimmte Webseite zu locken um ihm dann zum Beispiel Benutzerdaten für seine Bankverbindung zu entlocken sondern hier wird zu extremeren Mitteln gegriffen. Wie schon erwähnt in der Checkliste, sollten Sie gewisse Links nicht besuchen, doch was ist nun wenn Sie eine E-Mail erhalten, die Ihrer Bank als Absender hat und einen Link auf http://www.ihre-bank.com/login angibt, den Sie doch ab sofort benutzen sollen, um Ihre Onlinebanking Tätigkeiten durchzuführen. Was dann? Es gibt keinen Punkt in der Checkliste, der nun sagen würde “Achtung“, dies könnte ein Phishingversuch sein. Ja das ist wohl so und darum lässt sich Pharming auch nicht mit Phishing gleichsetzen. Denn wenn Sie diese E-Mail bekommen, ist schon ein Virus oder Wurm auf Ihrem System, der Ihre sogenannte Host-Datei bearbeitet hat. Nun was heisst das: Die Host-Datei kann die Aufgabe eines DNS-Servers übernehmen, dass heisst, es können Einträge gemacht werden, die dann nicht über einen Server nach der IP-Adresse aufgelöst werden müssen, sondern dies wird bereits lokal über die Host-Datei erledigt. Nun die Folgen sind recht einfach zu erkennen: Sie geben http://www.ihre-bank.com/login ein, beziehungsweise klicken Sie den Link in der besagten E-Mail an und kommen auf eine Webseite, die genau so aussieht, wie die Ihrer Bank aber eigentlich befinden Sie sich auf der Seite http://www.falsche-bank.com/login, denn Ihre Host-Datei hat Sie automatisch durch Ihre Anfrage dorthin geleitet. Einen wirklichen Schutz gegen Pharming gibt es zurzeit noch nicht, das einzige was Sie dagegen tun können, ist sich eine Antiviren-Software zuzulegen, die verhindert, dass Viren und Würmer Ihre Hostdatei verändern.

Zum Schluss

Zu guter letzt, möchte ich mich bei Ihnen bedanken, dass sie sich die Zeit genommen haben, dieses Paper zu lesen. Ich hoffe es hat Ihnen Spass gemacht und Sie können von Ihrem neuen Wissen profitieren.

Wer Rechtschreibefehler findet, darf sie behalten.

Sollten Sie Fragen oder Anregungen haben, stehe ich Ihnen gerne zur Verfügung.

admin@disenchant.ch
http://www.disenchant.ch

Mit freundlichen Grüssen
Sven Vetsch