Phishing im Zentrum von Penetration-Tests

Marc Ruef, scip AG, maru-at-scip.ch

Penetration Tests, das zielgerichtete und „aggressive“ Überprüfen der Sicherheit von Systemen, wird auch zunehmends in unseren Breitengraden in Sicherheitsprozesse eingebunden. Dass dabei die technologische Angriffsfläche bei weitem nicht das meiste Gefahrenpotential in sich birgt, wird oft vergessen oder schlicht nicht wahrgenommen.

Bei Penetration Tests (Abk. PenTest oder PT) wird versucht, zielgerichtet die Sicherheit eines Systems zu untergraben, um in der Praxis die bestehenden Sicherheitslücken und die realen Gefahren dieser zu bestimmen. Als Erweiterung zu einem breitflächigen Security Audit können so die letzten Schlupflöcher ausgemacht und vermeintliche Sicherheitslücken zweifelsfrei festgestellt werden.

Penetration Testing ist dabei für viele Sicherheitsdienstleister und Kunden eine rein technische Disziplin: Security Scanner und Exploits sollen innert kürzester Zeit für Erfolge sorgen, in Systeme einbrechen und sensitive Daten zusammentragen. Dabei wird übersehen, dass die Sicherheit einer Umgebung eben auch und vor allem ganz besonders von menschlichen Faktoren abhängt. Falsches Verhalten von Administratoren, Benutzern und Kunden kann fatale Folgen für ein System haben – Nicht selten haben ein kleiner Fauxpas viel mehr Durchschlagskraft, weder der hundertste Remote-Exploit zu einer Webserver-Sicherheitslücke.

Die Gefahren von Social Engineering

Die Geschichte der Computerkriminalität lehrt uns, dass eine Vielzahl an Einbrüchen durch psychologische Tricks initiiert oder gar umgesetzt wurden. Kevin Mitnick, er galt als einer von Amerikas Superhackern, gelang mitunter durch einige simple Telefonanrufe der Einbruch in „hochsichere Computernetze“ bekannter Firmen: Oftmals wurde einfach nach den sensitiven Informationen „gefragt“.

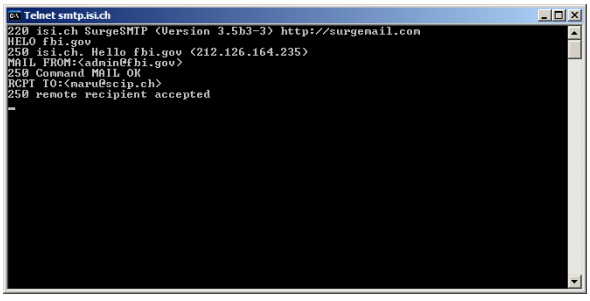

Abbildung 1: Der Versand von gefälschten Emails ist hinlänglich bekannt und gut dokumentiert. Durch das Umsetzen manueller SMTP-Kommunikationen lassen sich Absender oftmals nach Belieben setzen.

Nachdem er 1995 inhaftiert (eine erste Anhörung wurde ihm jedoch erst zwei Jahre später zuteil!) und im Januar 2002 vorzeitig entlassen wurde, publizierte er ein Buch mit dem Titel „The Art of Deception: Controlling the Human Element of Security“ – Eine ausgezeichnete Abhandlung darüber, wie effizient Social Hacking sein kann und wie sich derlei Angriffe umsetzen lassen. Der Erfolg des Buches in der Fachwelt und das noch dieses Jahr erscheinen sollende Nachfolgewerk „The Art Of Intrusion: The Real Stories Behind The Exploits Of Hackers, Intruders, And Deceivers“ (11. Februar 2005) geben Mitnick Recht.

„Kevin Mitnick gelang mitunter durch einige simple Telefonanrufe der Einbruch in hochsichere Netzwerke.“

Ein praxisorientiertes Fallbeispiel

Kann man den Kunden vom Nutzen von Social Engineering in einem Penetration Test-Projekt überzeugen, gilt es natürlich einen entsprechenden und vor allem realistischen Fall zu konstruieren. Ich möchte hier eine Phishing-Attacke, die wir für einen unserer Kunden umgesetzt haben, kurz dokumentieren.
Im Rahmen des regulären Penetration Tests, bei dem nach wie vor die technischen Aspekte im Mittelpunkt standen, wurden in einer ersten Footprinting-Phase durch verschiedene Medien die Mailadressen der Mitarbeiter der Organisation zusammengetragen. Eine Vielzahl an Adressen waren öffentlich auf der Unternehmens-Webseite zugänglich. Aber auch klassische Abfragen bei Google (z.B. @scip.ch) liessen die Liste der Mitarbeiter und ihrer Mailadressen anwachsen. Diese Daten sind die grundlegende Ausgangslage für einen entsprechenden Social Hacking-Angriff via Email (sie können jedoch auch bei einem Telefonat Verwendung finden).

Der Honigtopf lockt

Unsere Absicht eines Phishing-Angriffs war es, sämtlichen Mitarbeitern ein Email mit gefälschter Absenderadresse von der IT-Administration zu schicken. In unserem Schreiben wiesen wir

darauf hin, dass eine Erweiterung der Kommunikationsplattform im Unternehmen geplant sei. Unter anderem sei eine Messageing-Lösung samt Webcams geplant. Die Test-Phasen seien am Anlaufen und wer Interesse an einer Teilnahme habe, der solle seine Kontaktdaten auf einem extra dafür eingerichteten Webserver eingeben, damit die entsprechenden administrativen und technischen Schritte eingeleitet werden können.

Der Trick bestand nun darin, dass der vermeintlich interne Webserver gar nicht zur Firma gehörte, sondern unabhängig von dieser aufgesetzt wurde. Die Benutzer, die also dort ihre Namen, Mailadressen, Benutzernamen und Passwörter eingaben, stellten eben diese Daten externen Personen – unserem Auditoren-Team - zur Verfügung. Als Begründung, warum die sensitiven Kontoinformationen übertragen werden müssen, können verschiedene herhalten. So hat sich der Benutzer auf dem Formular zweifelsfrei zu identifizieren – Oder die Installation der Webcam soll ausserhalb der Arbeitszeiten durch das IT-Personal umgesetzt werden. Viele Anwender werden sich sowieso nicht darum kümmern ob und inwiefern sie nun ihre Passwörter angeben müssen.

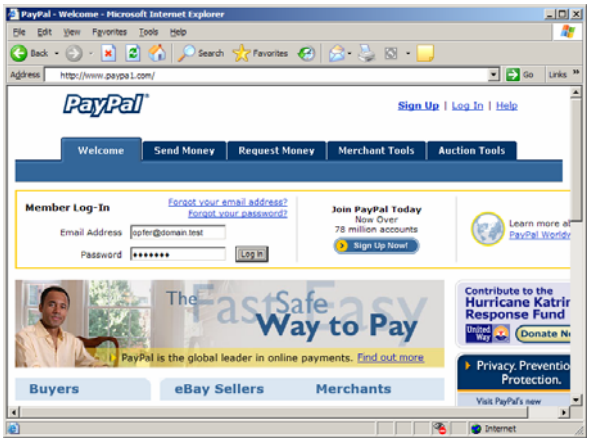

Abbildung 2: Gefälschte Webseiten, die auf einer vermeintlich authentischen URL angeboten werden - in diesem Beispiel paypa1.com anstatt paypal.com -, können die Eingaben der Benutzer abfangen und dem Angreifer zukommen lassen.

Es galt nun also, eine Webseite mit Formular im Stil des Zielunternehmens zu erstellen. Dabei wurde sich eng an die Aufmachung der öffentlich zugänglichen Homepage der Organisation gehalten. Das HTML-Gerüst und die Bilder wurden übernommen und nur geringfügig den eigenen Zwecken angepasst. Auf den ersten Blick sah es also wirklich so aus, als handle es sich um eine offizielle Intranet-Seite.

Die vermeintlich echte Nachricht

Der Kommunikationsaustausch, der das Opfer zu einer (ersten) Aktion bewegen soll, will gut überlegt und mindestens so akribisch vorbereitet sein. So muss die Nachricht – in unserem Fall ein Email – ein Maximum an Authentizität aufweisen. Dies beginnt beim Wortlaut des Schreibens, das höflich aber bestimmend auszufallen hat. Der Mitarbeiter soll schon allein am Klang der Worte das Gefühl haben, als sei das Vorgehen durch das oberste Management bewilligt und unterstützt.

„Es vergingen nur wenige Minuten, bis uns die ersten sensitiven Benutzerdaten zugeschickt wurden."

Zusätze wie eine griffige Betreffzeile und eine echt erscheinende Signatur sind ebenfalls von enormer Wichtigkeit. Ein Email erscheint automatisch vertrauenswürdiger, wenn an diesem eine Disclaimer- oder Antiviren-Nachricht angefügt wird.

Ebenfalls gilt es eine Nachricht technisch so authentisch wie möglich erscheinen zu lassen. Das in RFC 821 spezifizierte Simple Mail Transport Protocol zur Übermittlung von Emails kann sehr einfach zur Fälschung von Absenderadressen bewegt werden. Die wahre Herkunft eines Schreibens kann nur mit erweiterten technischen Kenntnissen, die eine Vielzahl der normalen Computerbenutzer nicht mitbringen, herausgefunden werden.

„Thanks for all the Fish..."

Nachdem die Mailadressen zusammengetragen, eine gefälschte Webseite aufgesetzt und das vermeintliche echte Email an die Mitarbeiter verschickt wurde, heisst es nun nur noch: Abwarten und Tee trinken, bis ein Fisch ins Netz geht...
Es verging nur wenige Minuten, bis ein erster Benutzer, sich eben für die Webcam interessierend, seine Daten auf dem gefälschten Web-Formular eingegeben hat - Benutzername und Kennwort inklusive! Der Beweis war erbracht: Die Mitarbeiter des Unternehmens sind sich der fehlenden Authentizität von elektronischen Nachrichten nicht bewusst. Das Anstreben von entsprechenden Awareness-Schulungen sollte ein zentraler Punkt bei der Verbesserung der Unternehmenssicherheit sein.

Fazit

Phishing war in den letzten Monaten einer der gern genutzten Mode-Begriffe der Massenmedien. Social Hacking ist aber

mindestens so alt wie die Menschheit selbst. Doch nur weil eine Angriffsform längst bekannt ist, heisst es noch lange nicht, dass wir sie akzeptieren oder gar ignorieren dürfen. Gerade in unserer technokratischen Gesellschaft sind psychologische Tricks, die durch die schillernde Technik imposant in Szene gesetzt wurden, das mitunter grösste Risiko für Dienstleister und Nutzer.

Der Autor

Marc Ruef arbeitet als Security Consultant bei der schweizer Firma scip AG (http://www.scip.ch), welche sich auf Sicherheitsberatungen im Bankenumfeld spezialisiert hat. Er hat eine Vielzahl an Artikeln, Büchern und Übersetzungen im Bereich Computersicherheit publiziert, betreut einige namhafte internationale Projekte auf diesem Gebiet und unterrichtet an diversen Fachhochschulen sowie Universitäten.

Impressum

scip AG
Technoparkstrasse 1
CH-8005 Zürich
T +41 44 445 1818
mailto:info-at-scip.ch
http://www.scip.ch

scip AG ist eine unabhängige Aktiengesellschaft mit Sitz in Zürich. Seit der Gründung im September 2002 fokussiert sich die scip AG auf Dienstleistungen im Bereich IT-Security. Unsere Kernkompetenz liegt dabei in der Überprüfung der implementierten Sicherheitsmassnahmen mittels **Penetration Tests** und **Security Audits** und der Sicherstellung zur Nachvollziehbarkeit möglicher Eingriffsversuche und Attacken (**Log-Management** und **forensische Analysen**). Vor dem Zusammenschluss unseres spezialisierten Teams im Jahre 2002 waren die meisten Mitarbeiter mit der Implementierung von Sicherheitsinfrastrukturen beschäftigen. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, Okena, Finjan, TrendMicro, Symantec etc.), welche den Grundstein für unsere Projekte bilden. Den kleinsten Teil des Wissens über Penetration Test und Log-Management lernt man jedoch an Schulen – nur jahrelange Erfahrung kann ein lückenloses Aufdecken von Schwachstellen und die Nachvollziehbarkeit von Angriffsversuchen garantieren.