Phishing und Social Engineering

Simon Lang

28. April 2015
Version 1.0.0

Studiengang	Informatik 5 Ba 2012
Seminar	Sicherheitsanwendungen/PKI
Dozent	Peter Stadlin
Schule	ZHAW - School of Engineering

Kurzfassung

Schlagwörter: Phishing, Social Engineering, Public Key Infrastructure, Fachhochschule, ZHAW School of Engineering

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Akronyme

Bezeichnung	Beschreibung
PKI	Public Key Infrastructure
ZHAW	Zürcher Hochschule für Angewandte Wissenschaften

Glossar

Ausfallsicherheit

Mit der Ausfallsicherheit wird die minimale zeitliche Erreichbarkeit (resp. maximale Ausfallzeit) eines Systems angegeben. Ist diese Ausfallzeit sehr gering spricht man von Hochverfügbarkeit (High Availability), dazu ist mindestens eine Verfügbarkeit von 99.9 % nötig. Die Verfügbarkeit berechnet man wie folgt:

$$\text{Verfügbarkeit} = (1 - \frac{\text{Ausfallzeit}}{\text{Periode}}) * 100$$
$$\text{Ausfallzeit} = (1 - \frac{\text{Verfügbarkeit}}{100}) * \text{Periode}$$

Cloud

Der Begriff *Cloud* ist im **??** definiert.

DMZ

Die Demilitarized Zone (DMZ) ist ein logisches oder physikaliches Subnetzwerk, welches interne Server zu einem grösseren, nicht vertrauenswürdigen Netzwerk verbindet. Es bietet eine zusätzliche Schicht Sicherheit und gibt den Administratoren mehr Kontrollmöglichkeiten, wer Zugriff auf Netzwerkressourcen hat.

Home Office

Mit Home Office wird das Arbeiten von zu Hause bezeichnet. Dabei wird oft eine sichere Verbindung von zu Hause auf die Infrastruktur der Firma erzeugt.

HTTPS

Das Hypertext Transfer Protocol Secure (HTTPS) ist ein Internet-Protokoll für eine verschlüsselte Kommunikation über ein Compunternetzwerk.

I/O-Device

Input/Output (I/O) Devices sind Geräte, welche für die Kommunikation zwischen Mensch und Maschine notwendig sind. (Bsp.: Bildschirm, Tastatur, Drucker,...)

LDAP

Das Lightweight Directory Access Protocol (LDAP) ist ein offenes, Anbieter unspezifisches Applikations-Protokoll um ein verteilter Verzeichnissdienst über das Netzwerk auszutauschen. Darüber können Informationen über Benutzer, Systeme, Netzwerke, Services und Applikationen abgefragt werden.

Load Balancing

Load Balancing verteilt die Arbeitsbelastung auf verschiedene Systeme. Damit kann die Antwortzeit reduziert werden. Wenn ein System ausfällt, hat es immer noch weitere die funktionieren. Dies steigert die Ausfallsicherheit des Gesamtsystems.

on-premise

On-premise Software bezeichnet jegliche Ausführung von Software die vorwiegend auf dem Endgerät selbst läuft. Alternativ existiert das Cloud Modell, bei dem der Grossteil der Software auf einem Server ausgeführt wird.

PUE

Mit der Power usage effectiveness (PUE) wird der Stromverbrauch eines Datenzenters berechnet. Dieser setzt sich folgendermassen zusammen:

$$\text{PUE} = \frac{\text{Total Stromkosten}}{\text{Stromkosten der IT}}$$

Thin Client

Ein Thin Client ist ein günstiger, rechen-schwacher Computer. Er wird dazu verwendet, um Arbeiten zu erledigen die auf einem rechen-starken Server statt finden. Ein Thin Client übernimmt hauptsächlich die Bereitstellung von I/O-Devices.

Virtual Private Netzwork

Ein Virtual Private Netzwork wird zwischen einem Teilnehmer und dem Server aufgebaut. Dabei wird innerhalb eines öffentlichen Netzwerkes, wie dem Internet, ein privates und sicheres Netzwerk erstellt.

KAPITEL 1

Einleitung

1.1 Ziele

Es soll eine detaillierte Einführung in das Gebiet des Social Engineering sowie Phishing erarbeitet werden. Es werden beide Bereiche erklärt, Unterschiede hervorgehoben sowie Attacken und Abwehrstrategien vorgestellt.

1.2 Begründung

Informationssysteme entwickeln sich rasant weiter, und auch das Sicherheitsbewusstsein vieler Firmen ist heute höher denn je. Um in ausgewählte Netzwerke einzudringen braucht es heutzutage mehr als nur einen Computer und fortgeschrittene EDV-Kenntnisse. Angreifer versuchen die am schwersten zu sichernde Schwachstelle auszunutzen: Den Menschen.

KAPITEL 2

Beschreibung der Aufgabe

2.1 Aufgabenstellung

2.1.1 Ausgangslage

Im Fach Public Key Infrastructure (PKI) wird der sichere Austausch von Nachrichten und Schlüsseln behandelt. Diese Seminararbeit bezieht sich auf das PKI Fach. Es wurden verschiedene Angriffszenarien in Bezug auf die Sicherheit vorgestellt. Dieses Seminar befasst sich mit Phishing und Social Engineering. Phishing und Social Engineering sind keine typischen Angriffszenarien, wie man sie sich vorstellt. Normalerweise werden Angriffe von einem weit entfernten Computer durchgeführt. Bei diesem Thema tritt der Angreifer direkt in Erscheinung. Er interagiert mit dem Angegriffenen und versucht durch geschickte Techniken an Daten oder Zugriffsrechte zu gelangen.

2.1.2 Ziele der Arbeit

Ziel der Arbeit ist es, Social Engineering sowie die unterart Phishing vorzustellen. Es werden Techniken erläutert, sowie Massnahmen wie man sich dagegen schützen kann. Es gibt auch diverse Interessante Beispiele die in der Arbeit aufgezeigt werden.

2.1.3 Aufgabenstellung

Es soll eine Arbeit im Umfang von ca. 15-30 Seiten erstellt werden. Das Thema ist Phishing und Social Engineering. Das Papier soll die beiden Themen erläutern und die Unterschiede aufzeigen. Zum Schluss gibt es noch eine Präsentation die den Inhalt der Arbeit für den Dozenten sowie den Rest der Klasse anschaulich zusammenfasst.

2.1.4 Erwartete Resultate

Das erwartete Resultat der Arbeit ist eine Einführung in das grosse Thema des Social Engineering sowie Phishing. Die Arbeit soll aufzeigen, was diese Antriffstechniken sind, welche Techniken verwendet werden und was die Gefahr dabei ist. Auch Teil der Arbeit sind Verteidigungsmassnahmen gegen die Techniken. Die Präsentation soll die Arbeit für die Mitstudenten sowie den Dozenten anschaulich und unterhaltsam zusammenfassen.

KAPITEL 3

Einführung

3.1 Aufbau

Dieses Kapitel stellt den Autoren vor und gibt eine Einführung in das Thema. Die folgenden Passagen stellen danach das Gebiet des Social Engineering und Phishing vor. Zum Schluss gibt es noch ein Abschlusswort.

3.2 Über den Autor

Mein Name ist Simon Lang. Als gelernter Informatiker arbeite ich seit 2006 in der Webentwicklungsbranche. Seit 2012 studiere ich Informatik an der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW). Da in der Webentwicklung die Sicherheit sehr wichtig ist habe ich das Fach Informationssicherheit und Kryptografie mit der Vertiefung Sicherheitsanwendungen und Public Key Infrastructure gewählt. Phishing und Social Engineering arbeitet stark mit dem Internet zusammen weshalb dieses Thema für die Arbeit gewählt wurde.

3.3 Über dieses Dokument

In dieser Arbeit werden die beiden Themen Social Engineering und Phishing vorgestellt. Das Dokument soll auch von Lesern ausserhalb der Informatik verstanden werden, obwohl grundlegende Kenntnisse von Computern und dem Internet vorausgesetzt werden.

3.4 Phishing und Social Engineering

Sicherheit ist ein relativer Begriff. Hacker und Sicherheitsexperten liefern sich einen stetigen Kampf. Die eine Seite versucht durch Angriff oder Viren in geschützte Netzwerke einzudringen, die andere Seite versucht dies zu verhindern. Sicherheit ist dabei nur die Schwierigkeit um einen Angriff erfolgreich durchzuführen. Denn einen Weg um in einen geschützten Bereich einzudringen gibt es immer. Zu Beginn der EDV Ära war ein unbefugtes Eindringen zum Teil sehr einfach. Das Sicherheitsbewusstsein von Personen und Firmen wurde jedoch immer höher, und so wurde auch das Hacken immer schwieriger. Deshalb suchten Angreifer andere Wege für einen Einbruch. Maschinen machen keine Fehler. Sind sie sicher Programmiert ist ein Hack schwierig. Dagegen ist das irren Menschlich. Diese Tatsache versucht man sich beim Social Engineering und Phishing zu seinem Gunsten zu

nutzen. Beim Social Engineering tritt der Hacker aus dem Keller hervor und tritt mit dem Angriffziel, einem Benutzer, Administrator, etc., direkt in Kontakt. Es wird versucht durch einen Fehler des Menschen eine Sicherheitslücke zu finden welche Angegriffen werden kann. Das Phishing ist eine Unterkategorie des Social Engineering. Durch gefälschte E-Mails oder Kurznachrichten wird das Opfer meistens auf eine Webseite geleitet wo versucht wird persönliche Informationen zu erschleichen.

KAPITEL 4

Social Engineering

4.1 Begriffserklärung

Zur Erklärung des Begriffs des Social Engineering zeigt man am besten Beispiele auf:

> Hallo! Ich bin neu hier, wie komme ich nochmal ins Wifi?[1]

So einfach kann ein Angriff durch ein Social Engineer aussehen. In dem Beispiel wird versucht sich eine Dienstleistung zu erschleichen. Es gibt keine „Hacks“ im eigentlichen Sinne. Niemand hängt sich ins Wireless rein, analysiert den Datenverkehr und versucht das Passwort zu knacken.

Angriffe können auch komplexer sein. Man stelle sich ein Unternehmen in Zürich vor, in welches Lastwagen einfahren. Oft haben Lastwagenfahrer ihren Namen auf einem Schild an der Frontscheibe aufgeschrieben. Sobald sich das Tor öffnet und der LKW einfährt, kann man dem Lastwagen nachrennen und den Namen des Fahrers rufen. So kommt man an den Sicherheitsbeamten am Tor vorbei. Der Angreifer möchte nun in die Abteilung Forschung & Entwicklung. Er fragt eine Mitarbeiterin nach dem Weg, mit der Begründung, dass er von einer Tochterfirma in Basel kommt und die Wegbeschreibung am Empfang wohl falsch verstanden hätte. Die Mitarbeiterin gibt bereitwillig Auskunft. Beim Gebäude der Abteilung Forschung & Entwicklung ist die Türe abgeschlossen. Nun wartet der Angreifer mit Sicht auf die Türe, bis ein Mitarbeiter dort eintritt. Mit diesem zusammen betritt er das Gebäude. Der Angriff lässt sich nun beliebig weiterführen. Vielleicht hängt irgendwo eine Liste mit Telefonnummern oder ein Mitarbeiter hat Notizen an seinem Bildschirm angeklebt mit welchen der Angreifer weiterarbeiten kann.[2]

Dieser Angriff nutzt verschiedene Schwachstellen aus. Allen gemein ist dass sie nichts direkt mit Informatik zu tun haben und deshalb in der Kategorie des Social Engineering

1 *Social Engineering: Wenn die Gefahr im Anzug kommt | t3n.* URL: http://t3n.de/news/social-engineering-529713/ (besucht am 26. 04. 2015).

2 *Beispiel für einen Social Engineering Angriff | Social Engineering - Manipulation.* URL: http://socialengineering24.de/social-engineering/social-engineering-angriffe/beispiel-fur-einen-social-engineering-angriff/ (besucht am 26. 04. 2015).

anzusiedeln sind. Dies wäre der Name an der Windschutzscheibe des LKW's, die Hilfsbereitschaft der Mitarbeiter oder dass offenhalten einer abgeschlossenen Türe für einen Kollegen.

Social Engineering muss nicht immer krimineller Natur sein. das nächste Kapitel setzt sich mit dieser Thematik auseinander.

4.2 Typen von Social Engineers

Social Engineering kann verschiedene Formen annehmen. Diese können bös- oder gutwillig sein. Folgend eine nicht abschliessende Liste von Aktivitäten[1] welche mit Social Engineering in Bezug gebracht werden kann:

- Hacker
- Spione
- Identitätsdiebe
- Verärgerte Angestellte
- Penetrationstester
- Regierungen
- Ärzte, Psychologen, Rechtsanwälte
- Personalvermittler
- Verkaufspersonal

Gemeinsam haben diese Jobs, dass sie sich mit der Domäne, in welchen sie agieren, auskennen müssen, viele Informationen zu sammeln haben und ein geschickter Umgang mit Kommunikation besitzen müssen.

Spione und *Identitätsdiebe* müssen Informationen über das Ziel sammeln, sich in eine Rolle hineinversetzten und auch Kommunizieren wie diese.

Verärgerte Angestellte können grossen Schaden anrichten. Mister X wird entlassen. Beim Gespräch mit dem Chef zeigt er sich verständnisvoll. Sobald er am Arbeitsplatz zurückkehrt beginnt er wichtige Daten zu löschen oder gibt diese weiter. Mister X darf sich nichts anmerken lassen. Muss Kommunizieren wie er es immer tut und den anderen Mitarbeitern etwas vortäuschen. *Penetrationstester* untersuchen Software auf Fehler. Dabei müssen sie sich in die Lage eines Hackers versetzen, so denken und handeln, wie dieser es tut. Dies umfasst deshalb die gleichen Kompetenzen eines Hackers.

Regierungen, *Ärzte*, *Psychologen* und *Rechtsanwälte* haben eines gemeinsam haben. Eine gute Kommunikation. Wie verkaufe ich etwas? Wie vermittle ich dem Volk etwas damit es nicht falsch verstanden wird? Wie überbringe ich eine schlechte Botschaft möglichst sanft? All diese Fragen bedienen sich dem Arsenal des Social Engineerings.

Personalvermittler und *Verkaufspersonal* müssen über ihre Produkte und die Kunden wichtige Informationen besitzen, sowie gutes Verhandlungsgeschick besitzen.

1 Christopher Hadnagy, Hrsg. *Die Kunst des Human Hacking*. mitp-Verlag, 2011.

Es wurde an Beispielen gezeigt, dass Informationen sammeln und eine geschickte Kommunikation zwei Schlüsselaspekten des Social Engineerings darstellen. Das erste Thema welches nun genauer betrachtet wird ist das Sammeln von Informationen.

4.3 Informationssammlung

Informationen sind das Fundament des Social Engineering. Ist die Basis schief, kann man keine geschickte Angriffe durchführen. Die Aufgabe der Informationssammlung gliedert sich dabei in zwei Bereiche. Die Beschaffung und die Organisation der Daten. Jede erdenkliche Quelle von Informationen sollte dabei durchsucht werden. Ein Haufen von undurchsuchbaren Daten nützt jedoch dem besten Social Engineer nichts. Deshalb müssen diese geordnet und durchsuchbar gegliedert werden.

4.3.1 Quellen

Ein Social Engineer ist nicht wählerisch in der Auswahl seiner Informationsquellen. Webseiten, Blogs, Suchmaschinen, Whois-Abfragen, Öffentliche Server, Social Media und öffentliche Berichte ist eine nicht abschliessende Liste von verlässlichen Datenquellen.

Man muss sich jedoch nicht nur auf online Medien beschränken. Durch Observation von Personen, Fahrzeugen oder Gebäuden können wertvolle Informationen gewonnen werden. Zu guter letzt darf sich ein Social Engineer auch nicht zu schade sein Abfälle zu durchwühlen. Diese Aktivität wird auch liebevoll Dumpster-Diving oder Garbage-Picking genannt.

Es ist verblüffend, wie viele Wertvolle Informationen im Müll landen. Checks, Gehaltslisten, Telefonnummern, Namen oder sogar Passwörter werden oft im Abfall entsorgt. Auch wenn sich die Opfer mühe geben und die Unterlagen zuerst durch einen Dokumentenschredder unkenntlich machen nützt dies nichts. Nach ein paar Stunden kann man die Streifen zu einem ganzen Papier zusammenfügen.

(a) Geschreddertes Dokument

(b) Zusammengesetztes Dokument

Abbildung 4.1: Schreddern eines Dokumentes

Das einzig verlässliche ist ein Zwei-Wege-Schredder. Solch unkenntlich gemachte Informationen lassen sich nicht mehr zusammenfügen.

Abbildung 4.2: Zwei-Wege geschreddertes Dokument

4.3.2 Datenorganisation

Beim der Sammlung können schnell ein paar Hundert Megabytes an Daten angehäuft werden. Dann stellt sich die Frage wie diese in eine ordentliche Form gebracht werden können.

Hier gibt es Tool die einen Social Engineer in seiner Sammelwut unterstützen. Wichtige Aspekte einer solchen Software ist es, dass sie einfach zu bedienen und übersichtlich ist. Denn man wird viel Zeit mit ihr verbringen. Natürlich muss sie auch mit grossen Datenmengen umgehen können und jegliche Formen von Daten unterstützen. Dies geht über Text, Bildern bis zu PDF und weiteren Dateien.

Ein einfaches Tool stellt BasKet dar. Es ist ein OpenSource Tool welches unter der GNU GPL v2 Lizenz betrieben wird und läuft mit Windows, Mac und Linux. Wie der Name bereits aussagt ist es ein Korb für die Ablage von jeglichen Daten.

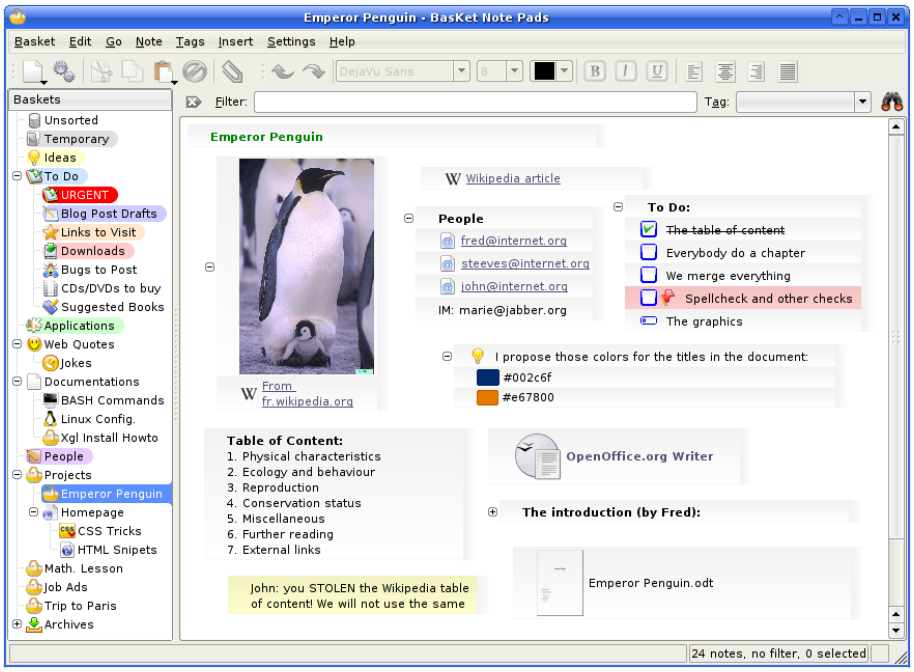

Abbildung 4.3: BasKet ermöglicht die einfache Ablage von jeglichen Informationen

Wenn man in einem Team arbeitet, muss eine gemeinsame Ablage der Daten möglich sein. Hier schafft das Programm Dradis abhilfe. Es läuft unter der gleichen Opensource Lizenz wie BasKet und ist auch für die selben Betriebsysteme verfügbar.

Bei Dradis handelt es sich um ein Webapplikation. Das ganze Team kann dabei auf einer Webseite kollaborieren.

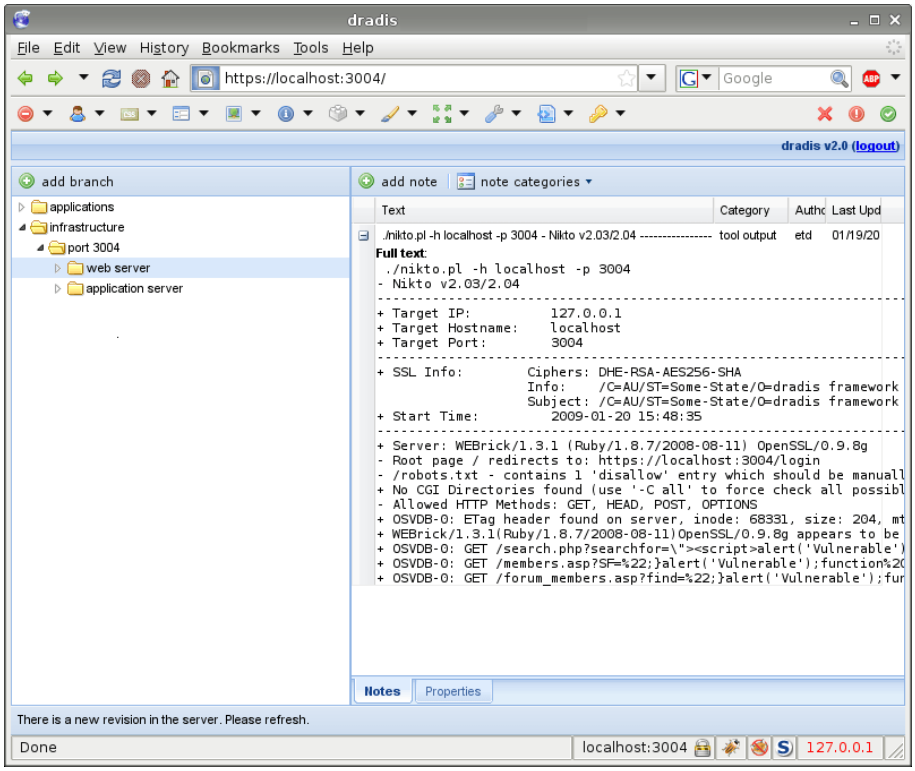

Abbildung 4.4: Mit Dradis können Teams zusammen arbeiten

4.4 Kommunikation

Kommunikation ist eine wichtige Waffe für einen Social Engineer.

KAPITEL 5

Diskussion

KAPITEL 6

Schlussfolgerung

Quellenverzeichnis

[1] *Beispiel für einen Social Engineering Angriff | Social Engineering - Manipulation.* URL: http://socialengineering24.de/social-engineering/social-engineering-angriffe/beispiel-fur-einen-social-engineering-angriff/ (besucht am 26. 04. 2015) (siehe S. 5).

[2] Christopher Hadnagy, Hrsg. *Die Kunst des Human Hacking.* mitp-Verlag, 2011 (siehe S. 6).

[3] *Social Engineering: Wenn die Gefahr im Anzug kommt | t3n.* URL: http://t3n.de/news/social-engineering-529713/ (besucht am 26. 04. 2015) (siehe S. 5).