

PHISHING UND SOCIAL ENGINEERING

Simon Lang

23. Mai 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

1 Einleitung	1
1.1 Ziele	1
1.2 Begründung	1
2 Beschreibung der Aufgabe	2
2.1 Aufgabenstellung	2
2.1.1 Ausgangslage	2
2.1.2 Ziele der Arbeit	2
2.1.3 Aufgabenstellung	2
2.1.4 Erwartete Resultate	2
3 Einführung	3
3.1 Aufbau	3
3.2 Über den Autor	3
3.3 Über dieses Dokument	3
3.4 Phishing und Social Engineering	3
4 Social Engineering	5
4.1 Begriffserklärung	5
4.2 Typen von Social Engineers	6
4.3 Informationssammlung	7
4.3.1 Quellen	7
4.3.2 Datenorganisation	8
4.4 Kommunikation	9
4.4.1 Kommunikationsmodell	9
4.4.2 Einsatzzweck im Social Engineering	10
4.5 Elizitieren	11
4.5.1 Angriff auf die Firma XY Computing	11
4.5.2 Techniken	12
4.5.3 Grundsätzliches	13
4.6 Pretexting	13
4.7 Weitere Techniken	14
4.7.1 Mikroexpressionen	15

4.7.2 Körpersprache	15
4.7.3 Framing	16
4.8 Technische Aspekte	17
4.8.1 ID Spoofing	17
5 Phishing	22
5.1 Informationssammlung und Zielgruppe	22
5.2 Kommunikationsmodell	23
5.3 Angriff vorbereiten	23
5.3.1 Angriffsvektoren	23
5.3.2 Nachricht ausarbeiten	27
5.4 Angriff durchführen	28
5.5 Beispiele	28
5.5.1 Facebook	29
5.5.2 Inkasso Firma	29
5.5.3 Paypal (einfach)	30
5.5.4 Paypal (fortgeschritten)	32
6 Schlussfolgerung	34
Quellenverzeichnis	35

Abbildungsverzeichnis

4.1 Schreddern eines Dokumentes	7
4.2 Zwei-Wege geschreddertes Dokument	8
4.3 BasKet ermöglicht die einfache Ablage von jeglichen Informationen	8
4.4 Mit Dradis können Teams zusammen arbeitent	9
4.5 Kommunikationsmodell nach Shannon und Weaver	10
4.6 Schreddern eines Dokumentes	15
4.7 Schreddern eines Dokumentes	16
5.1 Man-in-the-Middle Attackte	24
5.2 Entstehung und Verwendung eines Bot-Netzes ¹	28
5.3 Facebook Phishing E-Mail	29
5.4 Inkasso Phishing E-Mail	29
5.5 Einfaches PayPal Phishing E-Mail	30
5.6 Formular des PayPal Phishing E-Mails	31
5.7 Fortgeschrittenes PayPal Phishing E-Mail	32
5.8 Gefälschte PayPal Webseite	33

¹ *Botnet – Wikipedia*. URL: <https://de.wikipedia.org/wiki/Botnet> (besucht am 22.05.2015).

Tabellenverzeichnis

Akronyme

Bezeichnung	Beschreibung
CFO	Chief Financial Officer
CSO	Chief Security Officer
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Authentication, Reporting and Conformance
PKI	Public Key Infrastructure
SIP	Session Initiation Protocol
SPF	Sender Policy Framework
URL	Uniform Resource Locator
XSS	Cross-Site-Scripting
ZHAW	Zürcher Hochschule für Angewandte Wissenschaften

Glossar**DNS**

Domain Name Service (DNS) ist zuständig für die Beantwortung von Anfragen zur Namensauflösung in IP-basierten Netzwerken.

Firewall

Eine Firewall sichert einen Computer oder ein Rechnernetz vor unerwünschten Netzwerkzugriffen.

IRC

Internet Relay Chat (IRC) ist ein rein textbasiertes Chat-System. Es ermöglicht Chat-Rooms mit einer unbeschränkter Anzahl an Teilnehmern, sowie private Chats zwischen zwei Personen.

RFID

RFID (engl. radio-frequency identification) bezeichnet eine Technologie für Sender-Empfänger-Systeme zum automatischen und berührungslosen Identifizieren und Lokalisieren von Objekten und Lebewesen mit Radiowellen.

SMTP

Simple Mail Transfer Protocol (SMTP) ist ein E-Mail Protokoll zum Einspeisen und Weiterleiten von E-Mails. Traditionell wird der Port 25 verwendet.

VOIP

Voice over IP (VOIP) steht für Internet-Telefonie. Dabei ist das Telefonieren über Computernetzwerke gemeint. Anrufe auf weitere VOIP Telefone ist meistens gratis. Gegen Aufpreis können auf Anrufe auf das reguläre Telefonnetz getätigter werden.

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-für-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 Aktivitäten¹ 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 hineinversetzen 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 vermittele 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 Schlüsselaspekte 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 einzige 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.

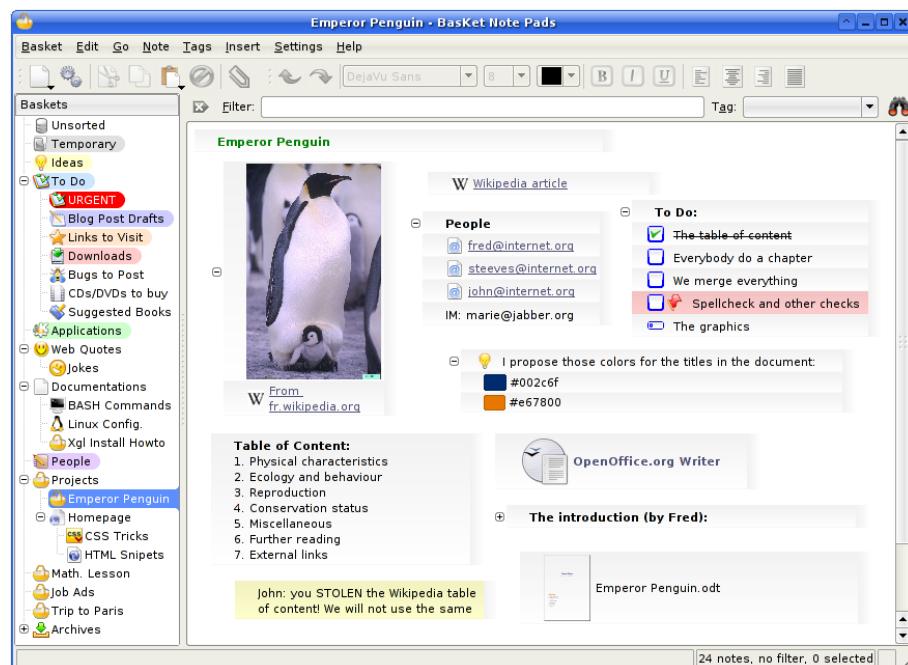


Abbildung 4.3: BasKet ermöglicht die einfache Ablage von jeglichen Informationen

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 Betriebssysteme verfügbar.

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

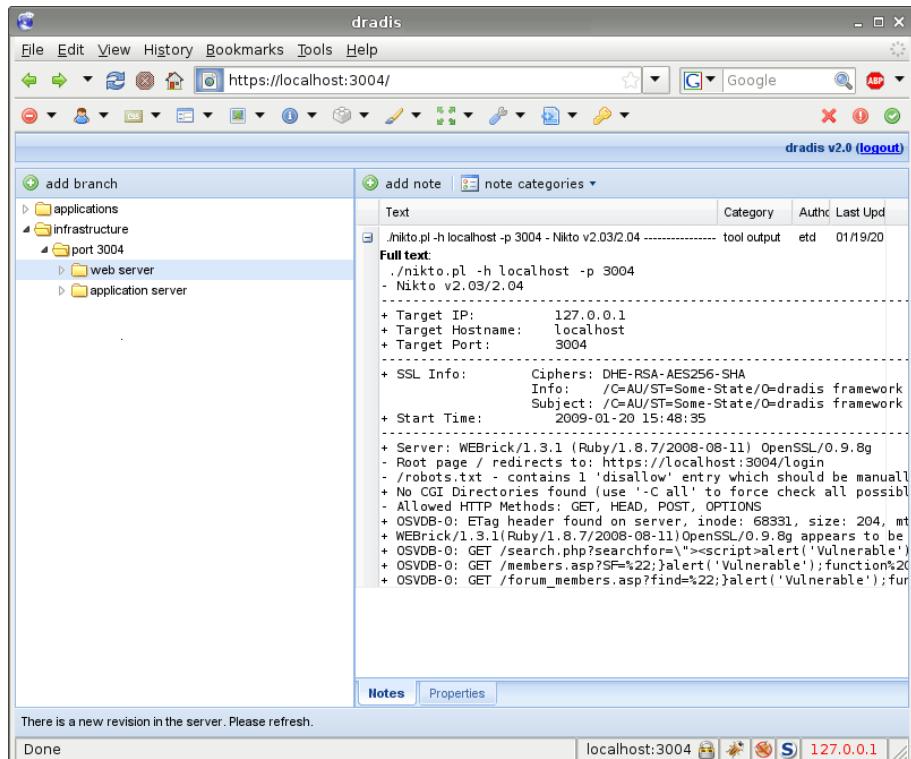


Abbildung 4.4: Mit Dradis können Teams zusammen arbeiten

4.4 Kommunikation

Kommunikation ist eine wichtige Waffe für einen Social Engineer. Dabei geht es darum, Informationen von einer Person zur nächsten zu transferieren. Dies kann verbal, oder über visuelle Effekte, Berührungen, Gerüche oder digital sein. Für den Social Engineer ist es dabei wichtig, wie die Informationen übermittelt werden, und zwar so, wie seine Absichten sind. Ein Arzt muss eine schlechte Nachricht möglichst sanft übermitteln. Möchte man hingegen einem Opfer Informationen entlocken, muss man Sympathien aufbauen.

Die Schwierigkeit bei der Kommunikation liegt darin, das Gegenüber richtig zu lesen und die Botschaft so zu überbringen, dass sie die richtige Wirkung erzielt. Dies wird versucht über Kommunikationsmodelle zu beschreiben.

4.4.1 Kommunikationsmodell

Kommunikationsmodelle versuchen die Kommunikation zu beschreiben. Also was Kommunikation ist und wie sie funktioniert.

Ein Gesprächspartner hat immer seine eigene Realität und Ansichtsweisen. Dies kann dazu führen, dass das Gesagte nicht immer gleich interpretiert wird.

Im Jahre 1947 entwickelten Claude Shannon und Warren Weaver das Shannon-Weaver-Modell, welches auch „Mutter aller Modelle“ genannt wird.

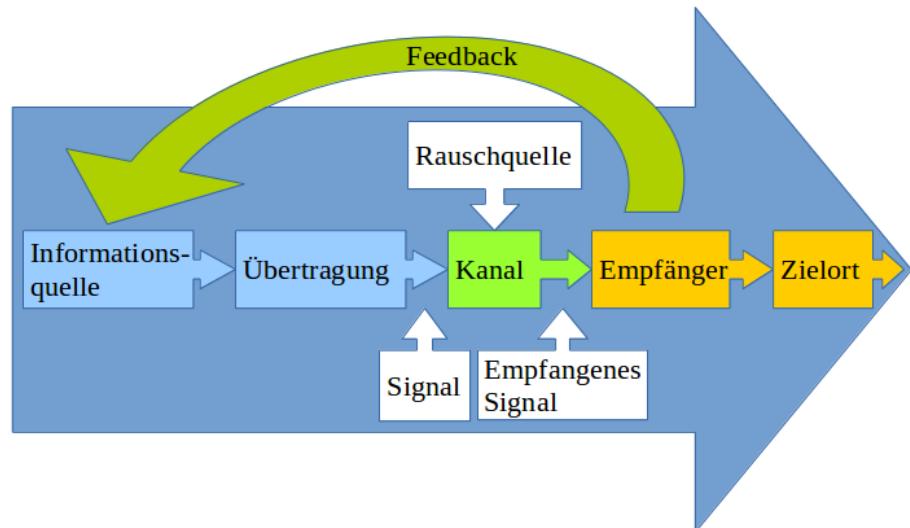


Abbildung 4.5: Kommunikationsmodell nach Shannon und Weaver

Der Ablauf einer Kommunikation lässt sich folgendermassen beschreiben:

- Informationsquelle: Quelle, welche eine Botschaft generiert.
- Übertragung: Übermittler, der die Botschaft in Signale umsetzt.
- Kanal: Ein Kanal, über den die Botschaft übermittelt wird. Dies kann über die sechs Sinne (sehen, hören, fühlen riechen oder schmecken) geschehen, oder über non-verbale Wege, wie zum Beispiel die Körpersprache.
- Empfänger: Empfänger der Botschaft.
- Feedback: Der Empfänger gibt der Quelle ein Feedback.
- Zielort: Eventuell ist der Empfänger noch nicht die Endstation der Botschaft. Deshalb kann sie von ihm noch an einen Zielort weitergetragen werden.

Zusätzlich gibt es eine Rauschquelle, welche den Kanal stören kann. Das Signal ist dabei die Nachricht, wie sie von der Informationsquelle gedacht ist und das empfangene Signal ist die Botschaft, wie sie vom Empfänger interpretiert wird.

4.4.2 Einsatzzweck im Social Engineering

Für jeden Angriff muss sich ein Social Engineer sein Kommunikationsmodell festlegen.

Um dies an einem praktischen Beispiel zu Zeigen stellt man sich ein Empfang vor. Durch Nachforschung hat man herausgefunden, dass der die PC's der Empfangsdame kein rechte Besitzt, somit für einen Angriff uninteressant ist. Der PC des Chefs jedoch hat erhöhte

privilegien wodurch sich eine Schwachstelle offenbart. Der Chef hat auch einen Drucker, die Empfangsdame nicht.

Nun bereitet man einen USB-Stick vor, welcher ein Virus in das System einspeist, sobald er an den PC angeschlossen wird. Zusätzlich kopiert man noch ein PDF File mit einem Lebenslauf auf den Stick.

Mit dieser Vorbereitung betritt man die Firma, geht zum Empfang und teilt der Dame mit, dass man soeben den Lebenslauf mit Kaffee bekleckert hat. Man fragt, ob sie ihn nicht nochmals vom USB-Stick ausdrucken könne. Bereitwillig nimmt die Empfangsdame den Stick entgegen, geht zum Chef und fragt ihn, ob er den Lebenslauf ausdrucken kann. Dieser willigt ein und der Angriff ist erfolgreich.

Analysiert man das Kommunikationsmodell zu diesem Angriff, so sieht dies folgendermassen aus:

- Informationsquelle: Beobachtung und die Informationssammlung des Social Engineers.
- Übertragung: Der Angreifer
- Kanal: Verbal
- Empfänger: Die Empfangsdame
- Feedback: Bereitwillige Einwilligung der Empfangsdame.
- Zielort: Chef des Empfangs.

4.5 Elizitieren

Elizitieren steht dafür, jemandem etwas zu entlocken. Es versteht sich von selbst dass dies für jeden Social Engineer eine wichtige Angelegenheit darstellt. Man muss in der Lage sein, Fragen so zu gestalten, dass Menschen aus sich herauskommen und so stimuliert werden, dass sie ein gewünschtes Verhalten einschlagen.

Einsetzen können diese Fähigkeit zum Beispiel Projektleiter, wenn sie mit Kunden kommunizieren, Polizisten, wenn sie verdächtige Verhören oder Hacker, wenn sie Informationen von Opfern erhalten möchten.

4.5.1 Angriff auf die Firma XY Computing

Dieser Abschnitt zeigt ein Beispiel eines Angriffes auf¹. Man möchte mehr über eine Firma in Erfahrung bringen. Zu Beginn muss man Informationen sammeln. Auf der Webseite findet man heraus welche Produkte vertrieben werden und für was diese eingesetzt werden können. Ein Produkt wird in einem Magazin sehr gelobt. In dem Bericht wird der Mitarbeiter John Smith interviewt. Er ist der **Chief Financial Officer (CFO)** der Firma und verantwortlich für dieses Produkt. Für sich selber legt man ein Pseudonym zu. Man wählt den Namen „Paul Parker“ und bestellt ein paar fiktive Visitenkarten im Internet. Mit diesen Vorkehrungen geht man zu einem offenen Fest der Handelskammer in einer Bar. Dort sieht man John Smith wie er mit einigen Reportern spricht. Als er sich aufmacht zur Bar zu gehen, schaut man dass man gleichzeitig dort ankommt.

¹ Hadnagy, *Die Kunst des Human Hacking*.

Paul: „Na, auch den Geiern entkommen?“

John schmunzelt: „Sie sagen es, ich brauche einen Drink.“

Paul zieht eine Visitenkarte hervor: „Ich arbeite bei einer kleinen Importfirma als Einkaufsleiter“

John überreicht seiner Seitens eine Vistenkarte: „Ich bin John Smith, **CFO** von XY Computing.“

Paul: „Ah, sie sind der Typ mit den Taschen voller Geld ... darum sind alle hinter Ihnen her. Was macht Ihre Firma eigentlich?“

John beginnt über die Produkte zu sprechen. Als er über das zuvor recherchierte zu sprechen beginnt fällt man ihm ins Wort.

Paul: „Ach ja, dieses Produkt kommt ja von *Ihrer* Firma. Ich liebe das Teil. Ich habe im XYZ-Magazin gelesen, dass Sie damit einen absoluten Verkaufshit gelandet haben.“

John drückt den Rücken etwas durch: „Wussten Sie, dass wir dieses Gerät im ersten Monat mehr verkauft haben als das davor und die nächsten fünf Produkte zusammen?“

Paul: „Oha - tja, und ich weiss auch warum. Ich habe nämlich selbst fünf Stück davon gekauft.“

Nach einigen weiteren Minuten findet man heraus, welche neue Buchhaltungssoftware die Firma soeben gekauft hat, dass der John soeben in den Ferien war und dass auch der **Chief Security Officer (CSO)** gleich für ein paar Tage in die Bahamas fliegt. Was bringen diese Infos einem Social Engineer? Für die Planung eines Angriffes können vertiefte Informationen über Produkte, Leute und Urlaubstermine entscheidend sein. Das Gespräch geht noch weiter.

Paul: „Ich weiss, dass das vielleicht eine komische Frage ist, aber wir sind eine kleine Firma, und mein Chef hat mich beauftragt, mal Recherchen anzustellen und ein Sicherheitssystem für die Türen zu kaufen. Aktuell haben wir nur Schlüssel, aber er fand, dass so was wie **RFID** vielleicht ganz gut ist. Sie wissen bestimmt, was bei Ihnen verwendet wird!“

John: „Ich habe keine Ahnung, ich habe dafür nur die Rechnungen gegengezeichnet. Ich weiss nur, dass wir diese schicke kleine Karte haben ...“

Mit diesen Worten zog er seine Geldbörse heraus und zieht eine Karte heraus.

John: „Ich glaube, das ist so ein **RFID**-Ding, aber sonst weiss ich nur, dass ich mit meinem Portemonnaie vor dem kleinen Kasten rumwedeln muss, um die Tür geht auf.“

Einem normalen Menschen erscheinen die erhaltenen Informationen nutzlos. Ein Social Engineer kann sich daraus jedoch wesentliche Vorteile ziehen. Es wurden eine Liste an Details über Software, Leute und Urlaubstermine gesammelt sowie Informationen über die Sicherheitssysteme der Firma. Möchte man sich Zutritt zum Gebäude verschaffen geht man zum Empfang und sagt dort, dass man eine **RFID**-Box defekt ist und dass der **CSO** einem beauftragt hätte, bevor er in die Bahamas flog.

4.5.2 Techniken

Im vorhergegangen Kapitel wurde ein Angriffszenario aufgezeigt, welches verschiedene Techniken des Social Engineering enthält. Zu Begin ist eine gute Vorbereitung nötig. Im Gespräch mit dem **CSO** kam das Elizitieren zum Einsatz.

Als John (der **CSO**) von seinem besten Produkt zu erzählen beginnt, zeigt Paul, dass er davon begeistert ist und unterschreicht dessen Genialität. Dadurch **appelliert** Paul (der Social Engineer) **ans Ego** von John, welcher sofort drauf einsteigt und weitere Informationen nachreicht.

Mit dem Satz „Ach ja, dieses Produkt kommt ja von Ihrer firma. Ichliebe das Teil“ bekundet Paul ein **gegenseitiges Interesse**. Dieses ist ein wichtiger Aspekt des Elizitieren, da es sogar noch wirkungsvoller ist als das Ego des gegenüber anzukraulen.

Später im Gespräch nutzt Paul eine weitere Technik, indem er dem Gesprächspartner **Kenntnisse unterstellt**. „Sie wissen bestimmt, was bei Ihnen verwendet wird!“ ist dabei der Schlüsselteil des Satzes. John weiss zwar die Antwort auf die Frage nicht, versucht jedoch trotzdem noch weiterzuhelfen, indem er seine **RFID**-Karte hervorholt.

Die der ganze Angriff war deshalb so erfolgreich, da **Alkohol** mit im Spiel war. Nichts lockert die Lippen besser als Ethanol.

In der aufgeführten Attacke nicht verwendet, jedoch auch ziemlich erfolgreich ist es, wenn man seinerseits **Informationen freiwillig anbietet**. Dadurch nötigt man seinem Gegenüber, eine ähnlich wertvolle Angabe zu machen.

Die letzte Waffe, die das Elizitieren bietet ist es, wenn man selbst eine **absichtlich falsche Aussage trifft**. Dies regt den Stolz des Anderen an, da er die Aussage berichtigen kann, wodurch oft geheime Informationen weitergegeben werden.

4.5.3 Grundsätzliches

Beim Elizitieren gibt es drei Grundregeln: **Seien Sie natürlich, Schulen Sie sich selbst und seien Sie nicht gierig**.

Wenn man nicht natürlich ist, kann das Gespräch schneller vorbei sein als es begonnen hat.

Mit „Schulen Sie sich selbst“ ist eine gute Vorbereitung gemeint. Man muss Informationen sammeln und deren Wert für das Gegenüber kennen. Es ist auch wichtig, dass man sich nie für mehr ausgibt, als man mit den gesammelten Informationen darstellen kann. Wenn das Opfer merkt, dass man etwas vorspielt, gibt er sicher keine weiteren Informationen frei.

Natürlich hat man stets das Ziel, möglichst viele Informationen zu ergattern. Ist man jedoch zu gierig, kann es schnell gefährlich werden, da der Gesprächspartner den Angriff möglicherweise bemerkt.

Der grosse Vorteil der erwähnten Techniken ist, dass es oft nicht auffällt wenn man Opfer einer Attacke wird. Die Hürde ist zwar hoch, da man zum Teil direkt in Kontakt mit dem Opfer trifft, jedoch kann ein Meister des Elizitieren viele wertvolle Informationen ergattern, ohne entdeckt zu werden.

4.6 Pretexting

Die nächste Disziplin eines Sociala Engineers ist das Pretexting. Dabei schlüpft man in die Haut einer anderen Person und gibt sich für diejenige aus.

Im Kapitel Abschnitt [4.1](#) wurde ein Angriffsszenario aufgezeigt. Der Pretext besteht in dem Fall daraus, dass sich der Eindringling als Mitarbeiter der Tochterfirma ausgibt. Als Vorbereitung ist hier eine ausführliche Recherche vor dem Angriff notwendig. Verstärkt werden kann der Pretext wenn der Social Engineer sich auch noch entsprechend kleidet.

Man kann sich zum Beispiel mit einem grauen Overall und einem Schraubenziehen in der Tasche verkleidet als Supportmitarbeiter ausgeben.

Als wichtigste Regel gibt es zu beachten, dass der Pretext **so einfach wie möglich** gehalten werden soll. Muss man sich zu viel einprägen kann man auf Fragen in einem Gespräch keine konsistente Antworten geben. Dies merkt man als Gegenüber rasch und gibt somit keine Informationen mehr preis. Verschiedene Pretexte erfordern auch mehr Wissen als andere. Es ist einfacher sich als Briefmarkensammler auszugeben verglichen mit einem Atomforscher.

Zusätzlich sollte der Pretext **sponatan wirken**. Wenn man zu viel nachdenken muss wird man innerlich unruhig. Zu vergleichen ist dies wie ein Sprung vom 10 Meter Sprungbrett in einen Pool. Wenn man oben steht und zu lange nachdenkt bekommt man Angst und springt nicht mehr.

Am Ende eines Angriffes ist es stets ratsam, einen **logischen Schluss oder Folgeauftrag zu erteilen**. Die Menschen mögen es, wenn sie Aufträge erteilt bekommen. Ein Arzt sagt nach der Behandlung nicht „Wir sehen uns in vier Wochen wieder“. Man zieht einen Schluss über das Gespräch und sagt dem gegenüber wie man verbleibt. Allfällige Aufträge müssen jedoch stets zum Pretext passen. Ist der Folgeauftrag wichtig für den Erfolg eines Angriffes ist es ratsam, wenn der Social Engineer selber Aktiv wird. Zum Beispiel wenn der Angegriffene Informationen an den Angreifer weitergeben soll ist es nicht ratsam zu sagen: „Melden Sie sich am Montag bei mir“. Besser ist es „Ich melde mich am Montag bei Ihnen, wenn das recht ist“. Dann läuft man nicht Gefahr, dass der Auftrag vergessen geht.

Hilfreich ist es, wenn man lokale **Dialekte und Redensarten** verwendet. In der Schweiz stösst man oft auf Abneigung, wenn man in Hochdeutsch spricht. In Amerika finden es viele Menschen sympathischer, wenn jemand einen britischen Akzent besitzt. Der Akzent muss dabei authentisch verkörpert werden können. Ist dies nicht möglich sollte er besser vergessen werden, da der Gesprächspartner merkt dass ihm etwas vorgespielt wird. Es gibt diverse Studien die belegen, dass der Akzent einen wesentlichen Einfluss auf das Verhalten des Zuhörers hat^{1, 2}.

Schlussendlich muss der Pretext vorher ausgiebig geübt werden. Dies kann vor dem Spiegel getan werden, oder man nimmt sich dabei auf. Auch ratsam ist es, wenn man mit fremden Leuten spricht und deren Reaktion beobachtet.

4.7 Weitere Techniken

Social Engineering ist, mehr als jede andere Angriffsart, eine sehr psychologische Angelegenheit. Es gibt deshalb noch viele andere Techniken, welche man sich zu nutzen machen kann. Nachfolgend noch eine nicht abschliessende Liste von weniger wichtigen, jedoch hilfreichen

¹ *Journal of Targeting, Measurement and Analysis for Marketing - The varying influence of spokesperson's accent in communication effectiveness: A comparative study in two different regions of Mexico.* URL: <http://www.palgrave-journals.com/jt/journal/v19/n1/full/jt20115a.html> (besucht am 14.05.2015).

² *PLOS ONE: The Effect of Perceived Regional Accents on Individual Economic Behavior: A Lab Experiment on Linguistic Performance, Cognitive Ratings and Economic Decisions.* URL: <http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0113475> (besucht am 14.05.2015).

Fertigkeiten.

4.7.1 Mikroexpressionen

Vieles lässt sich an dem Gesicht des Gegenübers ablesen. Diese Mikroexpressionen zu deuten ist wichtig um weitere Schritte im Social Engineering zu planen. Folgend einige Beispiele von Gesichtsausdrücken^{1, 2, 3}.

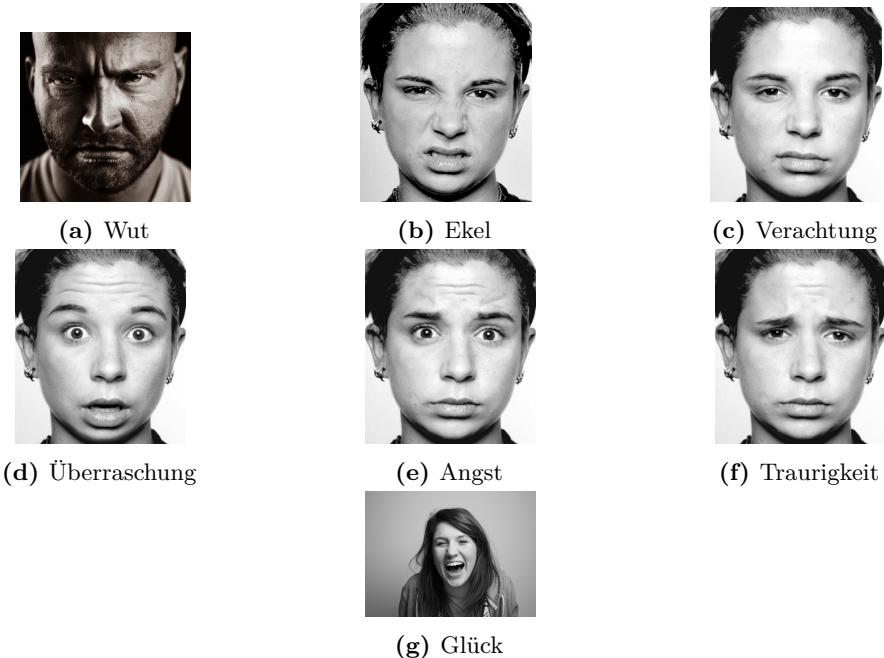


Abbildung 4.6: Schreddern eines Dokumentes

Zu beachten sind die Veränderungen der Augen, Stirn, Nase und den Mund.

4.7.2 Körpersprache

Ähnlich den Mikroexpressionen lassen sich wichtige Informationen aus der Körpersprache des Opfers ablesen. Zum Beispiel kann man durch genaue Beobachtung erfahren, wann man durch graben weitere Informationen erhalten kann oder man zu weit gegangen ist und das Gespräch besser abbricht.

Es sollte auf die Veränderung folgender Bereiche geachtet werden⁴:

- **Körperhaltung:** aufrecht, zusammengesackt, zurückgelehnt, auf Abstand bedacht
- **Hautfarbe:** blass, rötlich, weiss, Wechsel der Hautfarbe

1 *Anger by kwerfeldein on DeviantArt*. URL: <http://kwerfeldein.deviantart.com/art/Anger-102986132> (besucht am 16.05.2015).

2 *Ekman - Facial Expressions Foreign Language Flashcards - Cram.com*. URL: <http://www.cram.com/flashcards/ekman-facial-expressions-2447700> (besucht am 16.05.2015).

3 *Facial expression project - laughing girls / Flickr - Photo Sharing!* URL: <https://www.flickr.com/photos/daisykeeling/5462251889> (besucht am 16.05.2015).

4 Hadnagy, *Die Kunst des Human Hacking*.

- **Kopfhaltung** aufrecht, seitwärts geneigt, nach vorne oder hinten geneigt
- **Augen:** Blickrichtung, Offenheit
- **Hände/Füsse:** Bewegung, Position, Hautfarbe
- **Arme:** Gestiken, verschränkt, hängend, Hautfarbe
- **Mund/Lippen:** Position, Farbe, hoch- oder herabgezogen
- **Stimme:** Tonhöhe, Sprechgeschwindigkeit, Veränderungen
- **Worte:** kurz, lang, Anzahl der Silben, Störungen, Pausen

4.7.3 Framing

Beim Framing wird manipuliert, wie eine Person oder Gruppe eine Nachricht wahrnimmt. In der Lebensmittelindustrie schreibt man besser, ein Stück Fleisch ist *75% mager*, anstelle von *25% fett*. Oder in der Politik wird es eher akzeptiert, wenn man von *wirtschaftlichem Impuls* spricht anstelle von *Schuldenübernahme*. Es ist die jeweils die gleiche oder ähnliche Nachricht, die Wahrnehmung ist jedoch unterschiedlich.

In Firmenlogos wird Framing oft eingesetzt, um unterschwellige Nachrichten zu kommunizieren. Einige Beispiele¹:



(a) Federal Express



(b) Amazon



(c) Toblerone



(d) Yoga Australia

Abbildung 4.7: Schreddern eines Dokumentes

Federal Express: Ein Pfeil im Freiraum zwischen dem E und dem X steht für Schnelligkeit und Präzision.

Amazon: Zum einen stellt der Pfeil durch seine Form ein Lächeln dar und zeigt somit einen zufriedenen Kunden. Zum anderen zeigt der Pfeil vom A zum Z und sagt so aus, dass man alles über die Platform einkaufen kann.

Toblerone: Der Berg steht für ein schweizerisches Produkt. Im Berg selber ist ein Bär zu sehen und steht damit für die Hauptstadt Bern.

¹ Versteckte Botschaften in Logos. URL: <http://www.logoprofi.com/blog/2012/06/versteckte-botschaften-in-logos/> (besucht am 16.05.2015).

Yoga Australia: Der Freiram zwischen dem rechten Arm und dem Bein hat die Form vom Land Australien.

4.8 Technische Aspekte

Social Engineering umfasst nicht nur soziale Aspekte, sondern auch technische. Das wichtigste Hilfsmittel ist der **Computer**. Zielpersonen können über E-Mail, soziale Plattformen, Kurznachrichten, etc. angegriffen werden. Viele der vorhergegangenen Techniken lassen sich auch digital anwenden.

Ein Social Engineer sollte sich nicht scheuen, auch das **Telefon** für einen Angriff zu verwenden. Im Gegensatz zu E-Mail oder Kurznachrichten ist das entgegen gebrachte Vertrauen viel höher am Telefon als am Computer, wodurch oft mehr Informationen gewonnen werden können.

Auch kleinere Hilfsmittel können den Social Engineer unterstützen. Da wären zum Beispiel **Knopfkameras**, die sich in der Krawatte verstecken lassen oder **Aufzeichnungsgeräte**, damit man die gewonnenen Informationen an einem sicheren Ort nochmals durchgehen und archivieren kann.

Hilfreich können auch **GPS-Tracker** sein. Ist ein solcher bei einer Person oder Fahrzeug positioniert, kann man auf einer Karte nachvollziehen, wo sich hinbewegt. So können Positionen für nachfolgende Angriffe herausgefunden werden.

4.8.1 ID Spoofing

Bei der Kommunikation über das Telefon oder Computer ist es wichtig, vertrauen aufzubauen. Dies lässt sich gut über ID Spoofing erreichen. Dabei wird die Erkennung des Angreifers auf Seiten des Opfers so verändert, dass dieser meint er kenne den Angreifer. Beim Telefon kann die Rufnummer so verändert werden, dass zum Beispiel diejenige des Supports erscheint oder die einer Bank.

4.8.1.1 SpoofCard

In den USA gibt es SpoofCards. Darauf ist eine 800-Nummer notiert welche man anrufen kann. Dann gibt man die Telefonnummer ein, welche beim Opfer auf dem Display erscheint und danach die Nummer welche man anrufen möchte. Moderne SpoofCard's ermöglichen eine Aufzeichnung des Gesprächs sowie die Verfälschung der Stimme, sodass diese männlich oder weiblich klinkt.

4.8.1.2 SpoofApp

SpoofApp's sind für moderne Smartphones konzipiert und funktionieren vom Prinzip gleich wie eine SpoofCard. Die zu erscheinende und anzurufende Nummer werden in der Applikation angegeben und man ruft über einen Knopfdruck das Opfer an.

4.8.1.3 Asterisk

Bei Asterisk handelt es sich um einen **VOIP**-Server, mit welchem die eigene ID gespoofed werden kann. Der Vorteil zu den SpoofCards und SpoofApps wird ein eigenständig betriebener Server verwendet. Dazu wird folgendes benötigt:

- Computer (z.B. Intel P4 box mit 1GB RAM)

- Ubuntu Server
- Asterisk Software
- VOIP-Service

Der Ubuntu Server und Asterisk werden auf dem Computer installiert. Die Telefonate werden mit der Asterisk Software getätigt und über den VOIP-Service in das Telefonnetzwerk eingespielen.

Als erstes muss der VOIP-Service konfiguriert werden. Dazu wird die `/etc/asterisk/iax.conf` Datei angepasst.

```
[VoicePulse]
type=peer
host=server.example.oicepulse.com
username=SomeuSer
secret=PaSsWorD
```

type definiert den Typ der Verbindung. *host*, *username* und *secret* werden vom VOIP-Service zur Verfügung gestellt.

Als nächstes wird das Session Initiation Protocol (SIP) für Asterisk in der Datei `/etc/asterisk/sip.conf` konfiguriert:

```
[sipuser]
type=peer
host=dynamic
username=allan
secret=1234
context=outgoing
```

Der *type* definiert, welche Verbindungstyp verwendet werden soll.

host gibt die Adresse des SIP-Server oder -Service an. Es kann eine SIP, IP-Adresse, oder den Fixwert *dynamic* sein. Dynamic ist zu verwenden wenn der Server, wie in diesem Beispiel, eine dynamische IP-Adresse besitzt.

username und *secret* sind für die Authentifizierung am SIP-Server.

context gibt die Extension aus der `extension.conf` an, welche verwendet werden soll. Diese muss als letztes auch noch definiert werden:

```
[outgoing]
exten => _0NXXNXXXXXX,1,SetCallerID(0443344020)
exten => _0NXXNXXXXXX,n,Dial(IAX2/VoicePulse/${EXTEN})
```

Der Wert *0NXXNXXXXXX* ist ein Matching auf die eingegebene Telefonnummer. Die Nummer beginnt mit einer 0 und hat 9 folgende Zahlen. Dies passt auf alle schweizer Festnetz- und Mobil-Nummern ohne Landesvorwahl.

SetCallerID ist die Telefonnummer, welche gespoofed werden soll. Hier ist die Telefonnummer einer Credit Suisse Filiale angegeben.

Der Wert in *Dial* gibt an, dass das *IAX2* Protokoll verwendet werden soll in der *VoicePulse*-Verbindung, welche weiter oben definiert wurde. *\${EXTEN}* ist ein Platzhalter für die gewählte Telefonnummer.

Mit diesem Setup kann nun über Asterisk ein Telefonat gestartet werden über die Telefonnummer der Credit Suisse. Moderne Telefone gehen direkt ins Internet und zeigen an, dass der Absender die Credit Suisse ist¹.

4.8.1.4 E-Mail Absender

Zum versenden von E-Mails wird das **SMTP**-Protokoll verwendet. Die Schwachstelle besteht darin, dass keine Überprüfung der Absenderadresse vorgesehen ist. Eine gespoofde E-Mail kann vorlgendermassen versendet werden:

¹ *Caller ID Spoofing w/ Asterisk / Allan Feid.* URL: <http://allanfeid.com/content/caller-id-spoofing-w-asterisk> (besucht am 18.05.2015).

Client	Server	Kommentar
telnet mail.example.com 25		Client stellt Verbindung zum Server her
	220 service ready	Server ist bereit
HELO foobar.example.net		Client nennt seinen Namen
	250 OK	Server bestätigt
MAIL FROM:<sender@example.org>		Client gibt Absenderadresse an. Diese wird dem Empfänger nicht angezeigt, die Antwort geht jedoch hierhin.
	250 OK	Server bestätigt
RCPT TO:<receiver@example.com>		Client gibt Empfängeradresse an. Diese wird dem Empfänger nicht angezeigt.
	250 OK	Server bestätigt
DATA		Client gibt an, dass nun der Inhalt der E-Mail folgt
	354 start mail input	Server bestätigt
From: <sender@example.org> To: <receiver@example.com> Subject: Testmail Date: Thu, 26 Oct 2006 13:10:50 +0200 Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed eiusmod tempor incididunt ut labore et dolore magna aliqua. .		<i>From:</i> Absenderadresse, welche dem Empfänger angezeigt wird. <i>To:</i> Empfängeradresse, welche dem Empfänger angezeigt wird. <i>Subject:</i> Betreff der E-Mail <i>Date:</i> Datum Inhalt der Nachricht Der Punkt am Ende zeigt an, dass die Nachricht fertig ist.
	250 OK	Server bestätigt
QUIT		Client zeigt dass er fertig ist.
	221 closing channel	Server kündigt Trennung an.

Quelle: Wikipedia¹

Die Problematik besteht darin, dass die Adressen in *MAIL FROM* und *RCPT To* für das versenden benutzt werden, jedoch *From* und *To* dem Benutzer angezeigt werden. Das Protokoll lässt diese Diskrepanz standardmäßig zu.

¹ Simple Mail Transfer Protocol – Wikipedia. URL: https://de.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol (besucht am 18.05.2015).

Es gibt durchaus Einsatzgebiete, wo diese verhalten erwünscht ist. Zum Beispiel wenn man in der Universität einen einheitlichen Mailserver verwendet, jedoch verschiedene E-Mail-Adressen darüber verarbeitet werden.

Es gibt diverse Massnahmen um dies entgegenzuwirken. Die effektivste ist die Signierung der E-Mail mittels Zertifikaten. Dies benötigt jedoch eine Interaktion von den Usern weshalb sie nicht sehr verbreitet ist. Öfters benutzt werden Systeme, welche auf den Mailservern eingerichtet werden. Unter anderem folgende:

- **Sender Policy Framework (SPF):** Über zusätzliche **DNS**-Einträge (sogenannten TXT-Records) werden Computer definiert, welche für das versenden von E-Mails autorisiert sind.
- **DomainKeys Identified Mail (DKIM):** Die E-Mails werden mit dem private Key des senders versehen. Der Empfänger verifiziert die Signatur mit einem public Key aus dem **DNS**-Eintrag (TXT-Records) der Domain. Ist die verifzierung der Signatur nicht möglich kann die E-Mail verworfen werden.
- **Domain-based Message Authentication, Reporting and Conformance (DMARC):** Ist eine Verbindung von **SPF** und **DKIM**. Zusätzlich ist ein Modus, welcher vorgibt, dass die Domain der Absenderadresse exakt übereinstimmen muss, oder auch eine Subdomain enthalten darf. Es kann auch noch angegeben werden, wie mit einer E-Mail umgegangen werden muss, wenn die Überprüfung fehlschlägt. Es kann *none*, *quarantine* oder *reject* definiert werden.

KAPITEL 5

Phishing

Bei Phishing handelt es sich um eine Unterart des Social Engineerings. Bislang wurden stets einzelne, ausgewählte Opfer angegriffen. Phishing versucht über Spam E-Mails, [IRC](#) Chats oder soziale Plattformen eine grosse Anzahl an Opfer anzuschreiben in der Hoffnung, dass einige dem Angriff zum Opfer fallen. Es wird versucht, die Angegriffenen auf präparierte Webseiten zu locken, etwas zu verkaufen oder eine sicherheitstechnische Schwachstelle auszunutzen.

Den Ablauf eines Angriffes kann in folgende Schritte aufgeteilt werden:

- Informationssammlung und Festlegung der Zielgruppe
- Kommunikationsmodell ausarbeiten
- Angriff vorbereiten und durchführen

Auch wenn man eine Gruppe als Ziel hat und nicht eine ausgewählte Person, können die selben Techniken wie im Kapitel [4 Social Engineering](#) beschrieben verwendet werden.

5.1 Informationssammlung und Zielgruppe

Möchte man ein Angriff vorbereiten muss man wissen, wer seine Zielgruppe ist. Eine Einteilung ist in folgende Bereiche möglich:

- Geschlecht
- Alter
- Interessen
- Branche
- etc.

Mit einer Phishing-Nachricht muss das Interesse des Opfers geweckt werden, so dass er/sie auf die Nachricht antwortet oder auf einen weiterführenden Link klickt. Dazu müssen Informationen gesammelt werden, was die Interessen, stärken und schwächen der Zielgruppe ist. Diese Informationen werden nachher weiter verwendet um ein geeignetes Kommunikationsmodell auszuarbeiten.

Alternativ kann Gier oder Angst verwendet werden um das Interesse zu wecken. Dann kommen die Nachrichten meistens von reichen Ölscheichen oder Inkasso Unternehmen.

5.2 Kommunikationsmodell

Wie im Abschnitt [4.4.1](#) beschrieben besteht ein Kommunikationsmodell aus folgenden Teilen:

- Informationsquelle
- Übertragung
- Kanal
- Empfänger
- Feedback
- Zielort

Die *Informationsquelle* ist normalerweise der Angreifer selber oder ein Auftraggeber für den Angriff.

Die *Übertragung* wird vom Angreifer durchgeführt, da er die zu versendenden Nachrichten vorbereitet.

Der *Kanal* ist üblicherweise eine Auswahl aus E-Mail, [IRC](#) Chats oder soziale Plattformen, da darüber eine grosse Menge von Zielen angesprochen werden können. Die Wahl ist abhängig von der zuvor gewählten Zielgruppe. Junge Leute trifft man eher in Chatrooms an. Technisch versierte Personen sind eher in E-Mail Listen zu finden.

Empfänger ist die festgelegte Zielgruppe und der *Zielort* ist oft eine präparierte Webseite, ein Download welcher getätigter werden soll, etc.

5.3 Angriff vorbereiten

Der Angriff besteht daraus, das Opfer aus einer Nachricht heraus auf ein gewünschtes Ziel zu manövrieren und eine der folgenden Attacken auszuführen:

- Man-in-the-Middle Attacke
- URL-Obfuscation
- Cross-Site-Scripting Attacke
- Preset Session Attacke
- Hidden Attacke
- Observing Customer Data
- Client-side vulnerability

Die Verschiedenen Attacken werden nun genauer beschrieben.

5.3.1 Angriffsvektoren

5.3.1.1 Man-in-the-Middle Attacke

Bei der *Man-in-the-Middle Attacke* wird der User auf einen Proxy geleitet, welcher unter der Kontrolle des Angreifers steht. Dabei handelt es sich um einen Computer, welche alle Anfragen an das eigentliche Ziel des Opfers weiterleitet. Auf dem Proxy-Server kann danach die ganze Kommunikation mitgeschnitten und falls gewünscht, verändert werden.

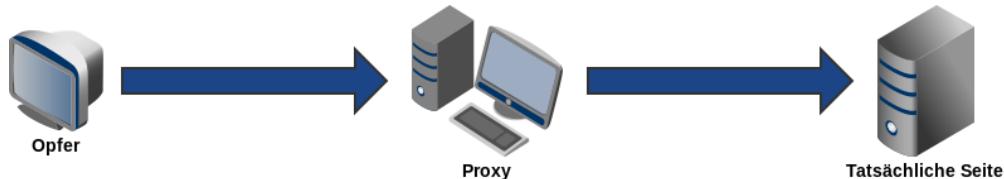


Abbildung 5.1: Man-in-the-Middle Attacke

Um den Benutzer auf den Proxy zu bugsieren gibt es mehrere Methoden:

- Transparent Proxy
- DNS Cache Poisoning
- URL Obfuscation
- Browser Proxy Configuration

Der **Transparent Proxy** verbindet den Proxy-Server mit dem Gateway des Computers vom Opfer. Sprich wenn der User über seinen Gateway ins Netzwerk geht, wird er automatisch über den Proxy-Server geleitet. Der Vorteil an dieser Attacke ist es, dass nichts am PC des Users manipuliert werden muss.

Bei **DNS Cache Poisoning** werden falsche **DNS**-Einträge auf dem Computer des Users oder auf der Netzwerk-**Firewall** generiert. Das führt dazu, dass wenn der Benutzer auf die Adresse www.meinebank.ch möchte, er auf dem Proxy-Server landet.

URL Obfuscation beschreibt das Maskieren von **Uniform Resource Locators (URLs)**. Es wird zum Beispiel auf die Seite www.meinebank.ch.cx verlinkt anstelle von www.meinebank.ch. Die Methode wird im Abschnitt [5.3.1.2](#) näher umschrieben.

Im Gegensatz zu den anderen Angriffen, muss der Angreifer bei **Browser Proxy Configuration** vor dem Angriff aktiv werden. Dazu wird im Webbrowser des Opfers der eigene Proxyserver eingetragen, sodass die ganze Kommunikation abgehört werden kann. Der Nutzer merkt dabei nichts, solange er nicht in den Einstellungen des Programms nachschauen geht.

5.3.1.2 URL-Obfuscation

Bei der URL-Obfuscation Attacke wird der User auf eine **URL** gelockt, die der originalen **URL** zum Verwechseln ähnlich sieht. Es gibt verschiedene Möglichkeiten dies zu bewerkstelligen.

- Ähnliche Domainname
- Freundliche Login Namen
- Domainname verschleiern
- Domainname verschleiern durch Drittanbieter

Bei den **ähnlichen Domainnamen** wird versucht die **URL** minimal zu verändern so dass der User nichts merkt. Wenn er zum Beispiel auf die Seite www.ebanking.meinebank.ch möchte, können folgende Adressen vorgetäuscht werden:

- www.ebanking.meinebank.ch.**cx**
- www.**meinebank.ebanking.ch**
- www.ebanking.meinebonk.ch
- www.ebanking.meineb**à**nk.ch
- www.ebanking.meinebank.**secure**.ch

Moderne Browser erlauben es, **Login-Daten** in der **URL** einzubetten, um. Diese **URLs** haben folgende Form: `http://[username]:[password]@[domainname]/[path]`. Damit kann zum Beispiel eine folgende **URL** generiert werden:

`http://meinebank.ch:ebanking@hack.ch/sicherheit/ebanking/loginseite.html`

Die Adresse ist absichtlich möglichst lange, damit der falsche Domainname nicht auffällt.

Eine weitere Möglichkeit ist die **verschleierung des Domainnamens**. Ist die das Ziel die Adresse `http://meinebank.ch:ebanking@hack.ch/loginseite.html`, kann anstelle von `hack.ch` die IP-Adresse verwendet werden. Zum Beispiel `210.134.161.35`. Diese kann noch weiter verschleiert werden, indem die decimalzahlen in das octal- oder hexadezimal-System konvertiert werden. Nachvollgend die Beispiele:

- Dezimal: `http://meinebank.ch:ebanking@210.134.161.35/loginseite.html`
- Octal: `http://meinebank.ch:ebanking@0322.0206.0241.0043/loginseite.html`
- Hexadezimal: `http://meinebank.ch:ebanking@0xD2.0x86.0xA1.0x23/loginseite.html`

Die letzte hier vorgestellte Methode ist die **verschleierung durch Drittanbieter**. Es gibt Anbieter, welche eine Linkverkürzung anbieten. Als Beispiele können hier `http://tinyurl.com/` oder Googles Service `http://goo.gl` genannt werden. Aus der Adresse `www.hacker.com` kann folgendes werden:

- `http://tinyurl.com/38gyas`
- `http://goo.gl/BNlbFj`

5.3.1.3 Cross-Site-Scripting Attacke

Das **URL** nutzt Sicherheitslücken auf Webseiten aus, die es erlauben Schadcode auszuführen, welche über die **URL** mitgegeben werden. Ein Beispiel ist `www.meinebank.ch?url=www.hacker.ch`. Der Benutzer geht dabei wirklich auf die Seite `www.meinebank.ch`. Wird jedoch auf `www.hacker.ch` weitergeleitet, da dies ein Fehler der Webseite ist. Es könnte auch sein, dass ein Code ausgeführt wird, welcher im Hintergrund die Benutzernamen und Passwörter mitschneidet und, ohne das der Benutzer etwas merkt, diese an einen Server weiterleitet.

Solche Adressen sind verdächtig, können jedoch mit den zuvor vorgestellten Techniken unkenntlich gemacht werden.

5.3.1.4 Preset Session Attacke

Um diese Attacke zu erläutern, muss zuerst etwas ausgeholt werden.

Im Internet werden die Protokolle meistens http und https verwendet. Beide sind statless, was so viel bedeutet, dass zwischen zwei Seitenaufrufen keine Verbindung besteht. Hat

man sich auf der ersten Seite eingeloggt, weiss das der Server auf der zweiten Seite nicht mehr. Um eine Verbindung zwischen den beiden aufrufen zu schaffen werden heute Sessions verwendet. Dazu wird dem Client (dem Computer des Benutzers) eine SessionID übergeben, die er bei jeder Anfrage mitsendet.

Bei der Attacke nutzt der Angreifer ein schlechtes Session Handling einer Webseite aus, indem zum Beispiel eine SessionID über die **URL** mitgegeben werden kann. Dies kann so aussehen: www.meinebank.ch?sessionid=3V1L5e5510N. Wenn der Benutzer auf den Link klickt und sich auf der Webseite in sein E-Banking einloggt, kann der Angreifer mit einem Aufruf der selben **URL** die Session übernehmen und hat damit Zugriff auf die Bankgeschäfte des Opfers.

Ein Server des Angreifers kann automatisiert stetig Anfragen an www.meinebank.ch stellen und eine Meldung bekommen, sobald sich ein Opfer eingeloggt hat.

5.3.1.5 Hidden Attacke

Hidden Attacken führen JavaScript Code auf einer Seite aus, um unbemerkt eine Attacke auszuführen. Der JavaScript Code wird mittels **URL** oder Man-in-the-Middle eingeschleust. Es gibt verschiedene Gruppen von dieser Attacke.

- Versteckte Frames
- Seiteninhalt überschreiben

Versteckte Frames zeigen auf eine andere Webseite (diejenige des Hackers) und führen diese aus. Es muss damit ein kleines Codestück in die Webseite eingeschleust werden, um viel Code auszuführen. Die Frames sind 0 Pixel gross und deshalb für den Benutzer unsichtbar.

Wenn **Seiteninhalte überschrieben** werden, kann das Verhalten der Seite so angepasst werden, dass zum Beispiel Benutzernamen und Passwörter nicht an die gewünschte Stelle, sondern an den Server des Phishers übermittelt werden. Dabei wird darauf geachtet, dass das Aussehen und das Verhalten der Ursprungsseite genau imitiert wird. Somit ist auch dieser Angriff für einen Benutzer nicht sichtbar.

5.3.1.6 Observing Customer Data

5.3.1.7 Client-side vulnerability

Oft ist das Ziel einer Attacke eine Sicherheitslücke eines Browsers. Moderne Browsers können Flash, Java-Programme, Filme, etc. direkt abspielen. Dazu verwenden sie Programme welche auf dem Computer des Opfers installiert sind. Angreifer können sich Schwachstellen im Browsern oder den installierten Programmen zunutze machen um zum Beispiel weiteren Schadcode auf dem Rechner zu installieren.

Internet Explorer hatte die Sicherheitslücke, dass er **URLs**, welche die Zeichenfolge %01 enthielten einfach abschnitt. Besucht der Benutzer die Seite <http://meinebank.ch:ebanking%01@hack.ch>, wurde die ganze **URL** ausgeführt, jedoch nur der Teil vor dem %01 angezeigt.

Eine weitere Sicherheitslücke bestand im Programm Media Player von Microsoft. Über folgenden Code konnte ein Skin für den Player heruntergeladen werden:

```
"C:/Program files/Windows Media Player/Skins/SKIN.WMZ": <IFRAME  
SRC="wmp2.wmz"></IFRAME>
```

Die Datei *wmp2.wmz* konnte dabei ein Java Applet sein. Das ist ein Java Code, welcher vom Browser ausgeführt werden kann. Mit folgendem Stück Code auf einer Webseite konnte der schadhafte Datei ausgeführt werden

```
<APPLET  
CODEBASE="file:///c:/"  
ARCHIVE="Program files/Windows Media  
Player/SKINS/wmp2.wmz"  
CODE="gjavacodebase.class"  
WIDTH=700  
HEIGHT=300>  
<PARAM NAME="URL" VALUE="file:///c:/test.txt" x > </APPLET>
```

Damit kann jeglicher Schadcode ausgeführt werden. Sprich ein Hacker kann volle Kontrolle über einen Computer erlagen.

Die gezeigten Sicherheitslücken sind mittlerweile behoben. Jedoch werden stetig neue Fehler in Programmen gefunden, welche zur ausführung von Schadcode verwendet werden kann.

5.3.2 Nachricht ausarbeiten

Abhängig vom gewählten Kommunikationskanal muss eine Nachricht ausgearbeitet werden, welche die ausgewählte Zielgruppe möglichst stark anspricht. Es können die Techniken des Elizitieren, welche im Abschnitt [4.5.2](#) besprochen wurden, angewendet werden um vertrauen mit dem Opfer herzustellen.

Ein oft verwendetes Thema für ein Phishing E-Mail ist zum Beispiel Kreditkarten-Daten. Das gefälschten Nachrichten kommen im Namen von E-Bay, PayPal, MasterCard oder einer anderen Anbieter. Es wird dabei druck gemacht, dass die Kreditkarte bald abläuft oder bereits abgelaufen ist und der Account gesperrt werden kann wenn nichts unternommen wird.

Andere Phishing Angriffe fälschen Sociale Plattformen wie Facebook, Twitter oder Instagram. Darin wird auf eine Nachricht eines Freundes verwiesen oder es wird mitgeteilt, dass eine eigene Nachricht an einen Freund nicht übermittelt werden konnte. Dazu hat es einen betrügerischen Link, der auf eine gefälschte Seite der Platform führt.

Wieder andere Phishing E-Mails versuchen die Gier der Menschen anzusprechen, indem sie schnelles Geld versprechen. Es wird von einem Bankkonto gesprochen das im Ausland liegt und der Besitzer hat keine Möglichkeit auf dieses zuzugreifen. Er bräuchte CHF 100 oder CHF 1000 und das Opfer bekäme CHF 100'000 zurückbezahlt. Oder die Nachricht kommt von einem Inkasso Unternehmen und es wird mit Verzeigungen oder Schadensersatzforderungen gedroht.

Es wird auch versucht, der Benutzer zum herunterladen einer Datei zu bewegen. Diese ist entweder über einen Link zu erreichen oder direkt dem E-Mail angehängt. Meistens handelt es sich dabei um einen Virus, Trojanisches Pferd oder ähnliches.

5.4 Angriff durchführen

Um eine grosse Masse an Nachrichten zu versenden reicht es nicht aus wenn der Angreifer sie selber versendet. Um viele Mitteilungen zu versenden verwenden die Phishers Bot-Netze. Das ist eine Ansammlung von Computern von ahnungslosen Personen. Die Computer sind virenversäucht und können ferngesteuert verwendet werden um Nachrichten zu versenden.



Abbildung 5.2: Entstehung und Verwendung eines Bot-Netzes^b

^b Botnet – Wikipedia. URL: <https://de.wikipedia.org/wiki/Botnet> (besucht am 22.05.2015).

Das Bot-Netz wird über Viren aufgebaut. Wenn das Netz steht, erteilt der Besitzer des Netzes auf Anfrage und Bezahlung eines Phishers den Auftrag, massenhaft E-Mails, IRC-Nachrichten oder Kurznachrichten zu versenden. Diese Methode wird *Command & Control* genannt, da eine Person die verseuchten Computer fernsteuert.

Benötigt für den Angriff werden noch die Adressen der Zielpersonen. Riesige Listen mit E-Mail Adressen können im Internet heruntergeladen oder gekauft werden. Dazu gibt es einschlägige Internetseiten und Foren.

Wenn man eine klare Zielgruppe hat, eignen sich die Sozialen Plattformen als Angriffsplattform. Es gibt gehackte Gruppen und Fanseiten, deren Abonnenten man, wiederum gegen Bezahlung, anschreiben kann. Der Vorteil daran ist, dass diese Gruppen ein gemeinsames Interesse haben und so gegen eine passende Phishing Nachricht sehr anfällig sind.

5.5 Beispiele

In diesem Abschnitt werden einige Beispiele für Phishing Nachrichten und betrügerischen Webseiten gezeigt¹.

¹ Was sind Phishing emails - Alles über Phishing mails / Computerfuzzy.de. URL: <http://www.computerfuzzy.de/phishing-mails-beispiele/> (besucht am 22.05.2015).

5.5.1 Facebook

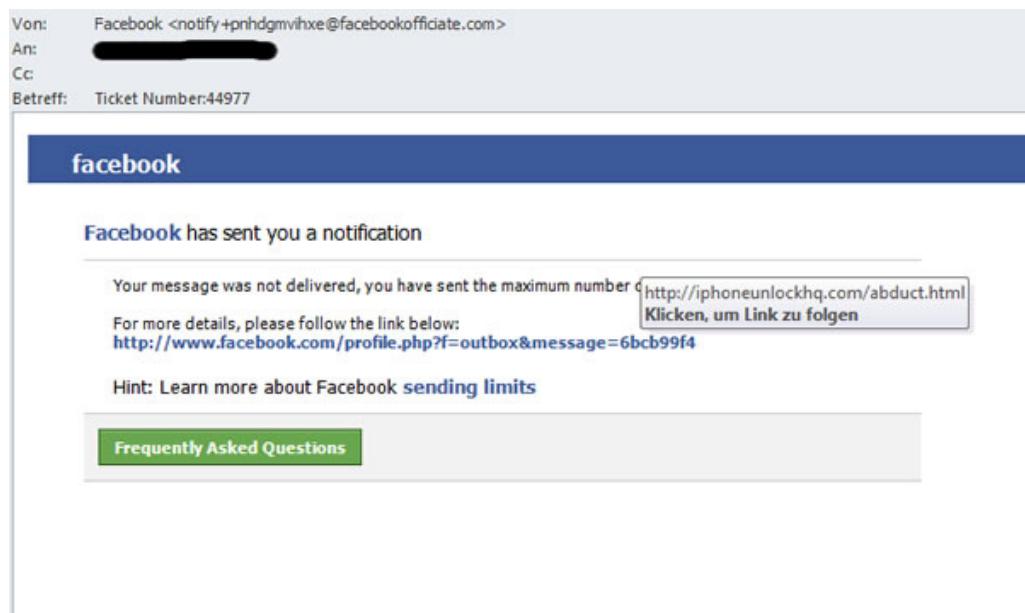


Abbildung 5.3: Facebook Phishing E-Mail

Die Nachricht informiert den Benutzer über eine unzustellbare Facebook Nachricht. Der Link sieht aus, als zeige er auf tatsächlich auf Facebook, führt jedoch auf eine ganz andere Seite.

5.5.2 Inkasso Firma



Abbildung 5.4: Inkasso Phishing E-Mail

Die Opfer werden mit einem 100 € Gutschrift angelockt. Fährt man mit der Maus über den Link ist nicht ersichtlich, wo der klick hinführt, da das Ziel unkenntlich gemacht wurde durch eine **URL** welche den User auf eine weitere Seite weitergeleitet.

5.5.3 Paypal (einfach)

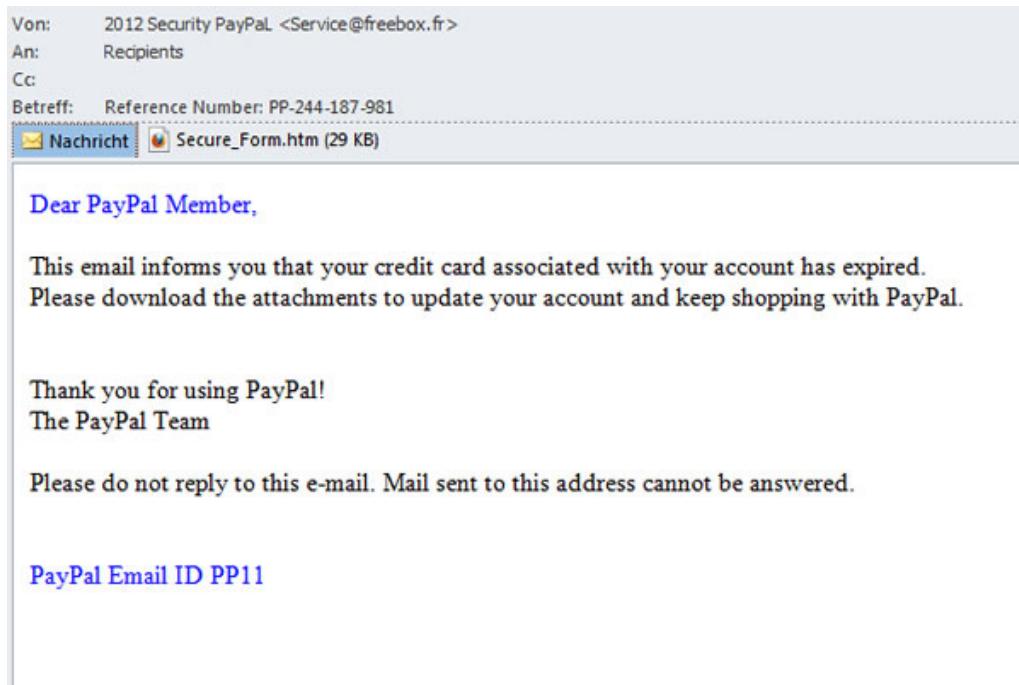


Abbildung 5.5: Einfaches PayPal Phishing E-Mail

Dieses Phishing E-Mail ist sehr einfach gemacht. Der Inhalt ist sehr schlicht und anstelle eines verweises auf eine Webseite ist ein Formular angehängt. Dadurch muss nicht noch ein Webserver betrieben. Das Formular kann in jedem Webbrowser geöffnet werden und sieht folgendermassen aus:

The screenshot shows a仿冒的PayPal登录界面。顶部有一个蓝色的横幅，中间是“PayPal”字样。下方是一个表单，标题为“Verify your Account”。表单包含以下字段：

- Email Address:
- PayPal Password:
- Full Name:
- Bank Name:
- Card Type: Card Type:
- Card Number:
- Expiration Date: Month: / Year: (Ex: 01/2011)
- Card Verification Number (CVV2):
- Password Verified By visa:
- Internet Banking ID :
- Internet Banking Password :
- Street:

右侧有三个信息块：

- Protect Your Account Info**: 建议用户不要向欺诈者提供密码。
- SSL Encryption**: 描述PayPal使用SSL协议加密敏感信息。
- Security Tips**: 提供保护自己免受欺诈的建议。

Abbildung 5.6: Formular des PayPal Phishing E-Mails

Das Formular fragt persönliche Daten ab und sendet es an den Angreifer.

5.5.4 Paypal (fortgeschritten)

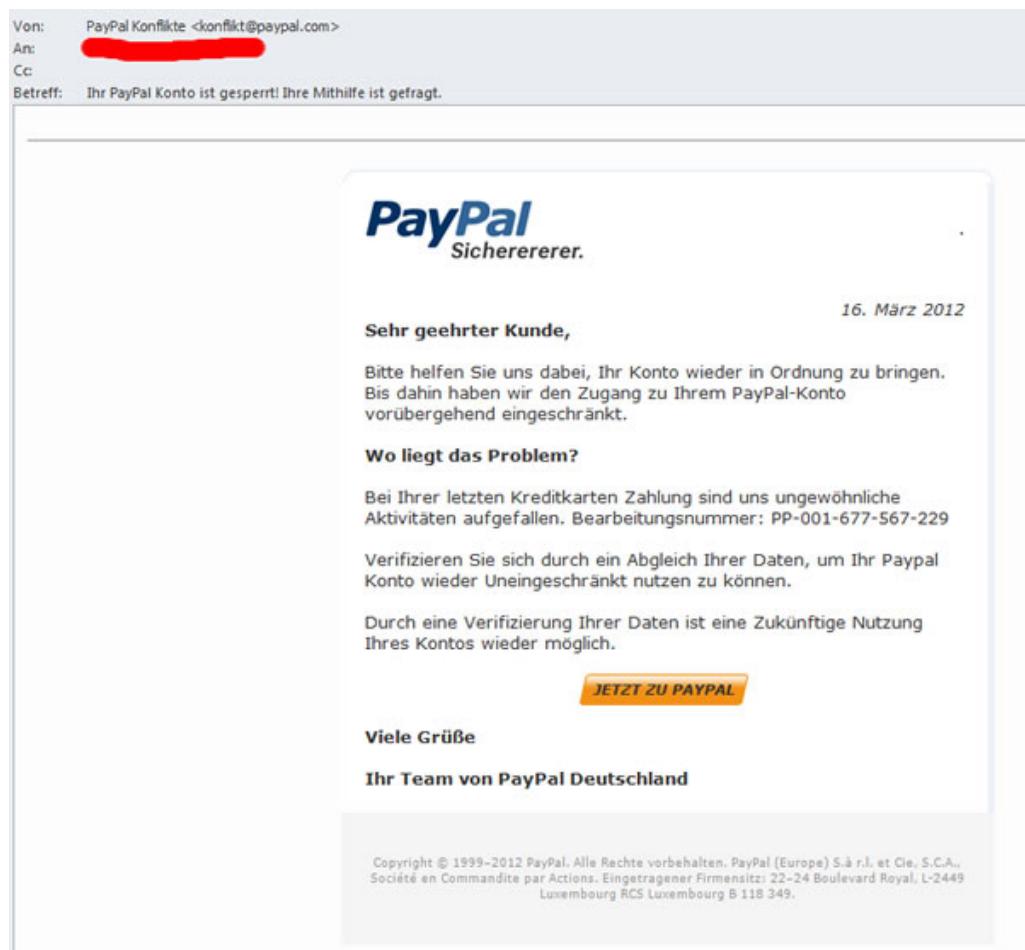


Abbildung 5.7: Fortgeschrittenes PayPal Phishing E-Mail

Dieses E-Mail ist wesentlich besser gemacht als jenes aus dem vorhergegangenen Abschnitt. Es beinhaltet das Logo und wirkt vertrauenswürdiger. Die Absenderadresse *konflikt@paypal.com* ist gespoofed (siehe Abschnitt 4.8.1 ID Spoofing)

Beim klick auf *JETZT ZU PAYPAL* sollte der Angriff jedoch erkannt werden.

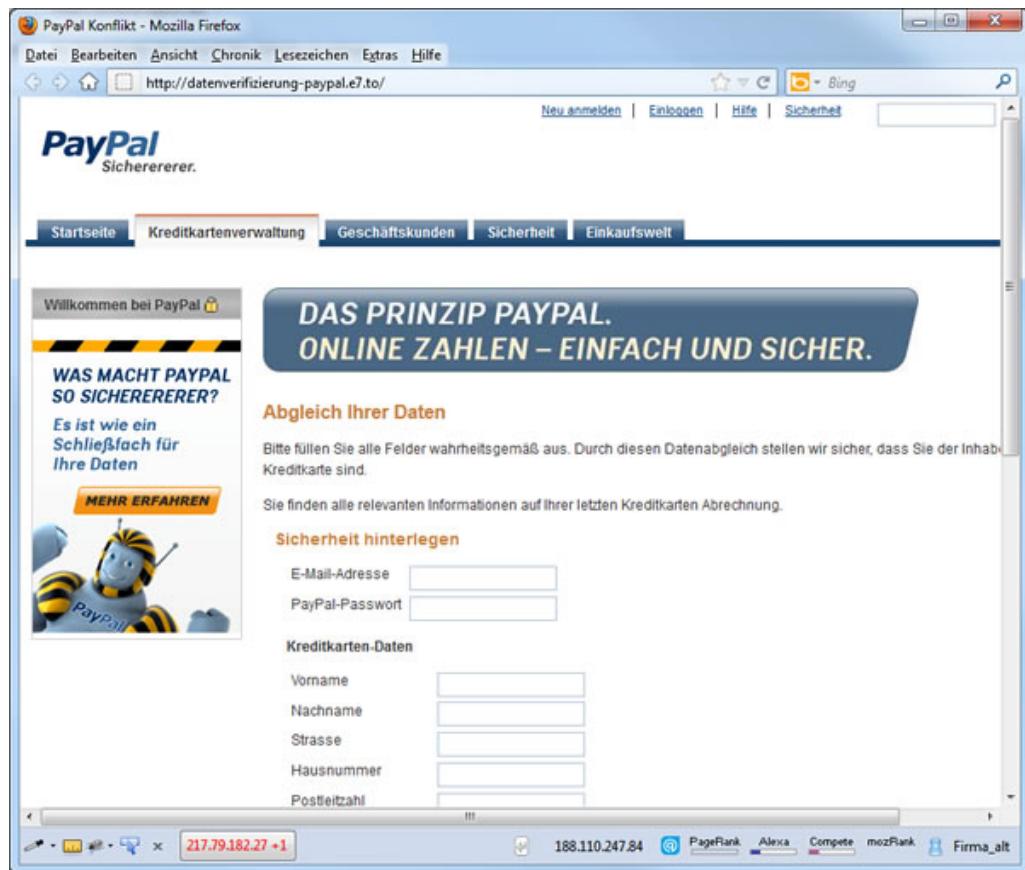


Abbildung 5.8: Gefälschte PayPal Webseite

Die Aufmachung der Seite imitiert genau diejenige von Paypal. Durch einen Blick auf die [URL](#) sollte der Angriff jedoch auffliegen.

KAPITEL 6

Schlussfolgerung

Quellenverzeichnis

- [1] *5 Ways to Tell Your Man is Lying*. URL: <http://www.kfm.co.za/Articles/2014/06/24/5-ways-to-tell-your-man-is-lying> (besucht am 16.05.2015).
- [2] *Anger* by kwerfeldein on DeviantArt. URL: <http://kwerfeldein.deviantart.com/art/Anger-102986132> (besucht am 16.05.2015) (siehe S. 15).
- [3] *Beispiel für einen Social Engineering Angriff / Social Engineering - Manipulation*. URL: <http://socialengineering24.de/social-engineering/social-engineering-angriffe/beispiel-für-einen-social-engineering-angriff/> (besucht am 26.04.2015) (siehe S. 5).
- [4] *Botnet – Wikipedia*. URL: <https://de.wikipedia.org/wiki/Botnet> (besucht am 22.05.2015) (siehe S. 28).
- [5] *Caller ID Spoofing w/ Asterisk / Allan Feid*. URL: <http://allanfeid.com/content/caller-id-spoofing-w-asterisk> (besucht am 18.05.2015) (siehe S. 19).
- [6] *Ekman - Facial Expressions Foreign Language Flashcards - Cram.com*. URL: <http://www.cram.com/flashcards/ekman-facial-expressions-2447700> (besucht am 16.05.2015) (siehe S. 15).
- [7] *Facial expression project - laughing girls / Flickr - Photo Sharing!* URL: <https://www.flickr.com/photos/daisykeeling/5462251889> (besucht am 16.05.2015) (siehe S. 15).
- [8] Christopher Hadnagy, Hrsg. *Die Kunst des Human Hacking*. mitp-Verlag, 2011 (siehe S. 6, 11, 15).
- [9] *Journal of Targeting, Measurement and Analysis for Marketing - The varying influence of spokesperson's accent in communication effectiveness: A comparative study in two different regions of Mexico*. URL: <http://www.palgrave-journals.com/jt/journal/v19/n1/full/jt20115a.html> (besucht am 14.05.2015) (siehe S. 14).
- [10] *Mimik: Gesichtserkennung, Spiegelneuron und Amygdala*. URL: <https://www.dasgehirn.info/handeln/mimik-gestik-koerpersprache/gesichter-lesen-4124> (besucht am 16.05.2015).
- [11] *PLOS ONE: The Effect of Perceived Regional Accents on Individual Economic Behavior: A Lab Experiment on Linguistic Performance, Cognitive Ratings and Economic Decisions*. URL: <http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0113475> (besucht am 14.05.2015) (siehe S. 14).

- [12] *Simple Mail Transfer Protocol – Wikipedia*. URL: https://de.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol (besucht am 18.05.2015) (siehe S. 20).
- [13] *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).
- [14] *Versteckte Botschaften in Logos*. URL: <http://www.logoprofi.com/blog/2012/06/versteckte-botschaften-in-logos/> (besucht am 16.05.2015) (siehe S. 16).
- [15] *Was sind Phishing emails - Alles über Phishing mails / Computerfuzzy.de*. URL: <http://www.computerfuzzy.de/phishing-mails-beispiele/> (besucht am 22.05.2015) (siehe S. 28).