# Seminar Datensicherheit

Verwaltungsinformatik

# Vortragsreihe der Studenten

**Prof. Dr. Thomas Waas**
**Alfons-Goppel-Platz 1**
**95028 Hof/Saale**

**Raum: FB 131**
**Tel.: 09281/409-489**
**Fax: 09281/409-400**
**Email: thomas.waas@fh-hof.de**

**Sprechstunde: Wintersemester 2005**
**Donnerstag: $10^{00}$ Uhr – $11^{00}$ Uhr**

# Social Engineering

über die Gefahren der psychologischen Verwirrung
bei der Informationsbeschaffung
und die Sicherheitskultur

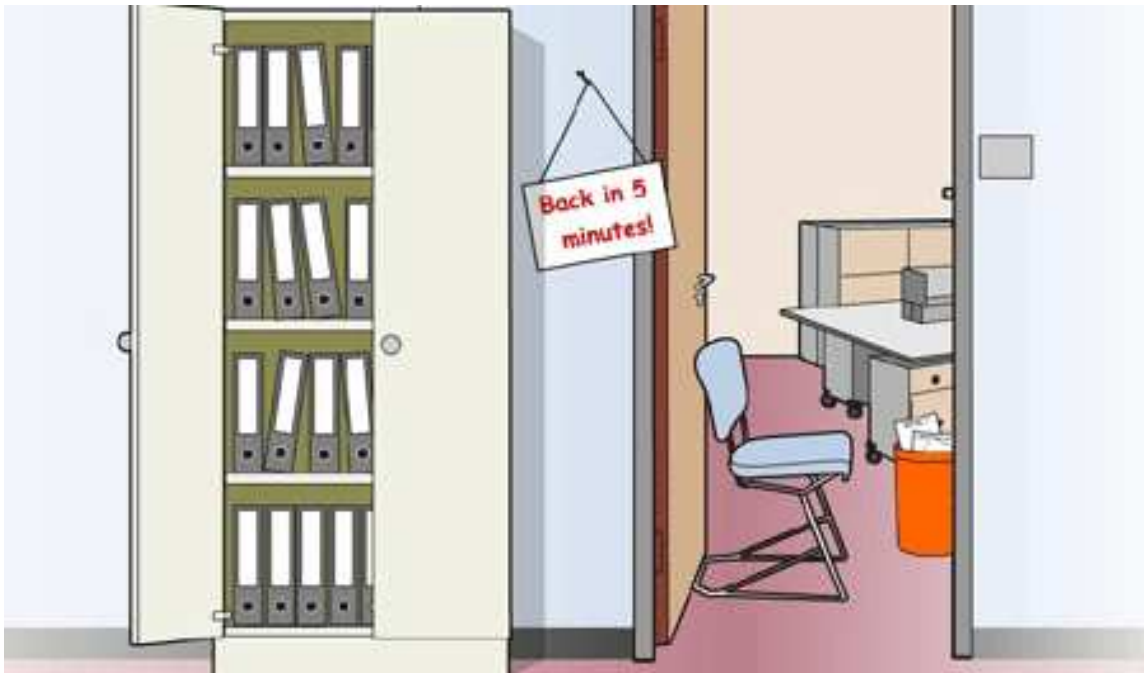

Abbildung 1.: Was versteht man unter Sicherheitskultur

©Christian Grafe
WS 06 / 07
Seminararbeit

# Inhaltsverzeichnis

Social Engineering ..... 1

Inhaltsverzeichnis (wird automatisch generiert) ..... 2

1. Grundlagen zum Social Engineering ..... 3
1.1. Versuch einer Definition ..... 3
1.2. Warum hat Social Engineering Erfolg ..... 3
1.3. Motivation von Social Engineers ..... 3

2. Unterschiedliche Arten von Social Engineering ..... 4
2.1. Computer Based Social Engineering ..... 4
2.2. Human Based Social Engineering ..... 5
2.3. Reverse Social Engineering ..... 5

3. Konkretes Vorgehen bei einem Angriff ..... 6
3.1 Informationsbeschaffung ..... 6
3.2 Aufbauen von Kontakten / Identität fälschen ..... 6
3.3 Informationen über das Ziel erarbeiten ..... 6
3.4 Mit den Informationen ..... 7
3.5 Informationen logisch zusammensetzen ..... 7

4. Schutzmaßnahmen ..... 7
4.1. Grundlegende Schutzmaßnahmen ..... 8
4.2. Secure Awareness ..... 8

5. Anhang ..... 9
Literaturverzeichnis: ..... 9

Abbildungsverzeichnis ..... 9

Definitionsverzeichnis ..... 9

# 1. Grundlagen zum Social Engineering

In diesem Script geht es grundlegend um den Begriff des Social Engineering oder auch Social Hackings. Es entstand im Rahmen des Wintersemesters 06/07 im Seminar Netzwerksicherheit bei Prof. Dr. Thomas Waas.

## 1.1. Versuch einer Definition

**Definition 1 – Social Engineering:**

**Der Begriff Sozialkonstruktion bzw. Social Engineering (auch Social Hacking) bezeichnet in der Informatik das Erlangen vertraulicher Informationen durch Annäherung an Geheimnisträger mittels gesellschaftlicher oder gespielter Kontakte.**

## 1.2. Warum hat Social Engineering Erfolg

Der Erfolg vom Social Engineering bzw . Social Hacking lässt sich eigentlich relativ leicht erklären:
Menschen sind manipulierbar und generell das schwächste Glied in einer Kette. Egal ob in der IT oder irgendwo anders – der Mensch selber ist der größte Risikofaktor.
Eine Vertrauensbasis ist schnell aufgebaut beziehungsweise vorgetäuscht und so können Menschen relativ leicht manipuliert werden. Ausserdem haben viele Mitarbeiter Angst sich gegen jemanden aufzulehnen, der Ihnen gegenüber vorgibt eine höhere Stellung zu haben.
Somit sind alle Soft- und Hardwaremäßigen Mechanismen zur Abwehr von Hackern und zur Verhinderung von Informationsdiebstahl nutzlos. Jeder Mensch der die Authorität hat diese zu umgehen ist potienziell eine Gefahr für die Sicherheit.
Deswegen wird Social Engineering von vielen Sicherheitsbeauftragten als die gefährlichste Form des Informationsdiebstahls angesehen.

## 1.3. Motivation von Social Engineers

Die Motivation einen Social Angriff durchzuführen ist keine andere als bei einem „normalen“ technischen Angriff auf Informationen.

Meistens geht es um einen der folgenden Punkte:

- Industriespionage
- Identitätsdiebstahl
- Spass oder Macht
- Finanzielle Gründe
- Soziale Gründe (ExPartner)

Vor allem der soziale Aspekt spielt hier häufig eine Rolle. Es liegt ziemlich auch ziemlich nahe, da hier die sozialen Bindungen meisten schon vorhanden sind. Zum Beispiel um an Kontodaten etc. von Ex-Partnern oder Kollegen zu gelangen. Manche Engineers gehen sogar soweit Freundschaften vorzutäuschen.

# 2. Unterschiedliche Arten von Social Engineering

Generell unterscheidet man zwischen drei großen Formen von Social Engineering. Allerdings kann man nicht genau unterscheiden, da es immer wieder neue Formen gibt und man nicht jeden Angriff generell ein- oder zuordnen kann. Aber die drei generellen Schubladen werden hier vorgestellt.

## 2.1. Computer Based Social Engineering

Das Computer Based Social Engineering ist eigentlich kein richtiger Social-Hack. Allerdings wird er trotzdem hinzugezählt, da hier wie bei einem normalen Angriff (siehe Punkt 2.2) eine Identität vorgetäuscht oder eine falsche Vertrauensbasis ausgenutzt wird.

Hierbei werden technische Mittel (Email, Webseiten) genutzt, um Identitäten (Bsp. Ebay oder die Hausbank) vorzutäuschen und schlussendlich um die gewünschten Informationen zu erlangen.

Ein besonders „prominentes“ Beispiel hierfür sind sogenannte Phishing Seiten oder Phishing Emails. Beide Maßnahmen können mit relativ leichten Mitteln und ohne großes technisches Wissen erstellt und somit ausgenutzt werden.

**Definition 2 – Phishing:**

**Phishing ist eine Form des Trickbetruges mit Methoden des Social Engineerings.Es ist der Oberbegriff für illegale Versuche, weitgestreut Anwendern Zugangsdaten (Loginnamen plus Passwörter) für sicherheitsrelevante Bereiche zu entlocken.**


Abbildung 2.: Beispiel einer Phishingseite – Hier Ebay.de

## 2.2. Human Based Social Engineering

Unter diese Kategorie fällt der eigentliche Social Engineering Angriff. Hierbei werden Informationen über einen konkreten Kontakt zwischen Täter und Opfer beschafft.
Meistens gibt sich der Täter als Autoritätsperson oder Vertrauensperson aus. Das Opfer gibt daraufhin (meist unwissend) Informationen preis beziehungsweise lässt sich zu Aktionen verleiten.

Meistens gelingt dies dadurch, dass ein Social Engineer sich sehr wortgewandt verhält. So benutzen sie unternehmensinternen Wortschatz oder Fach-Slang und täuschen meist Situationen vor, welche gewisse Stimmungen vorraussetzen.

Beispiele:

- Ein Serverausfall mit sofort notwendigen Maßnahmen
- Passwörter wurden gelöscht
- Probleme durch Hacker erfordern Zugriff auf Accounts

Dadurch wirkt die Situation hektisch oder chaotisch was bei den meisten Mitarbeitern oder Angestellten dazu führt, dass sie unüberlegt auf Anforderungen oder Befehle eingehen, wenn sie unter Stress stehen oder Angst haben.

Eine weitere Form, die mit unter diese Kategorie fällt ist das sogenannte Müllwühlen, bzw. „Dumpster Diving“. Rechtlich gesehen sind den Unternehmen hierbei die Hände gebunden, da es gesetzlich erlaubt ist.
Müll ist nämlich weder Privat noch das Eigentum von dem ehemaligen Besitzer. Lediglich Hausfriedensbruch darf der SE bei dieser Aktion nicht begehen.
Beim Dumpster Diving durchsucht ein Social Engineer den Müll eines Unternehmens nach Akten, Passwortdateien, Fotos oder jedwilligen Informationen ab. Auch unwichtige Informationen können wichtig sein, denn etwa fünf dieser Informationen ergeben eine sensible.

## 2.3. Reverse Social Engineering

Bei dieser Methode wird ein Problem erfunden oder vorgetäuscht und anschließend Hilfe angeboten, dieses Problem zu beseitigen.
Dadurch sieht das Opfer den Angreifer als Helfer in der Not und denkt meistens nicht über negative Folgen oder die Sicherheit nach.

Da ein gemeinsamer Feind vorgetäuscht wird gehen die meisten Anwender ohne große Bedenken auf die Anfrage ein.
Als Beispiele hierfür dienen folgende Aussagen:

- „Die im Rechenzentrum haben ein Problem gemacht“
- „Der Emailserver funktioniert schon wieder nicht.“
- „Ach, die Microsoft Software spinnt mal wieder..“

# 3. Konkretes Vorgehen bei einem Angriff

Ein Social Engineering Angriff läuft meistens in folgenden sechs Schritten ab. Natürlich gibt es auch Abwandlungen aber grundlegend kann man einen Angriff so beschreiben.

## 3.1 Informationsbeschaffung

Alles beginnt mit einem Anruf, Vorsprechen, Müllwühlen, Brief oder mit schlichten Surfen auf der Homepage des Opfers. Die ersten Informationen kann man sich unscheinbar und meist unaufällig beschaffen, jedoch ist es unabdingbar grundlegende Informationen über seine Opfer zu haben.

## 3.2 Aufbauen von Kontakten / Identität fälschen

Man muss in eine andere Rolle schlüpfen. Hierfür bietet es sich an jemanden zu nehmen, der im Unternehmen höher gestellt oder eine Stelle die Extern mit einem Problem betraut ist.
Welche Rollen man spielen kann, beziehungsweise mit welchen Informationen man sich an die Zielinformationen ranarbeitet, findet man schon im Schritt 3.1 heraus.

Beispiele:

- Telefonumfrage
- Anfrage vom Endanwender
- Internetprovider ruft an
- Gespräch mit dem Abteilungsleiter

## 3.3 Informationen über das Ziel erarbeiten

Hierbei muss man sich mit geschickten Fragen und Verschachtelungen an die eigentliche Information herantasten.
Jedoch muss man größte Vorsicht walten lassen, so dass es nicht zu offensichtlich ist, welche (evtl. bösen) Ziele man verfolgt.
Die meisten Social Engineer arbeiten sich mit geschickten Zwischenfragen an das Ziel heran:

=> Wie gehen sie bei einer Anfrage vor? -> Ach so und was machen sie mit den Daten? -> Sie benutzen also auch eine Oracle Datenbank?

! So hat man über Umwege die Information erlangt, welche Speicherstruktur bzw. Datenbank ein Unternehmen verwendet.

## 3.4 Mit den Informationen

Sollten alle bisherigen Schritte geklappt haben, so sollte man zwei Dinge im Nachhinein unbedingt sicherstellen:

- Den Kontakt nicht verlieren, er könnte sich später noch einmal als nützlich erweisen.
- Es darf niemand merken, dass man Daten/Informationen erarbeitet oder ein böses Ziel verfolgt hat.

## 3.5 Informationen logisch zusammensetzen

Meistens kommt man nicht direkt an die eigentlichen Informationen, sondern nur an kleinere Teilschritte. Aber je banaler die Information erscheint, umso wichtiger kann sie sich später herausstellen.

Beispiel:
Man hat von einer Liste den Benutzernamen eines Studenten der FH Hof erlangt. Sollte man jetzt noch sein Geburtsdatum (eigentlich triviale Information) erlangen, so kann man das Email-Passwort selbst erstellen. Man braucht nur die Information, dass die Passwörter aus Namen und Geburtsdatum zusammengestelllt sind. Und so erweisen sich selbst unwichtige Informationen als brisante Sicherheitslücken.

# 4. Schutzmaßnahmen

Grundlegend gibt es keinerlei Schutzmaßnahme, welche sich alleinig als effektiv gegen Social Engineering erwiesen hat. Man kann sich nicht mit dem Einspielen von Software oder durch das Einbauen von Hardware dagegen schützen.

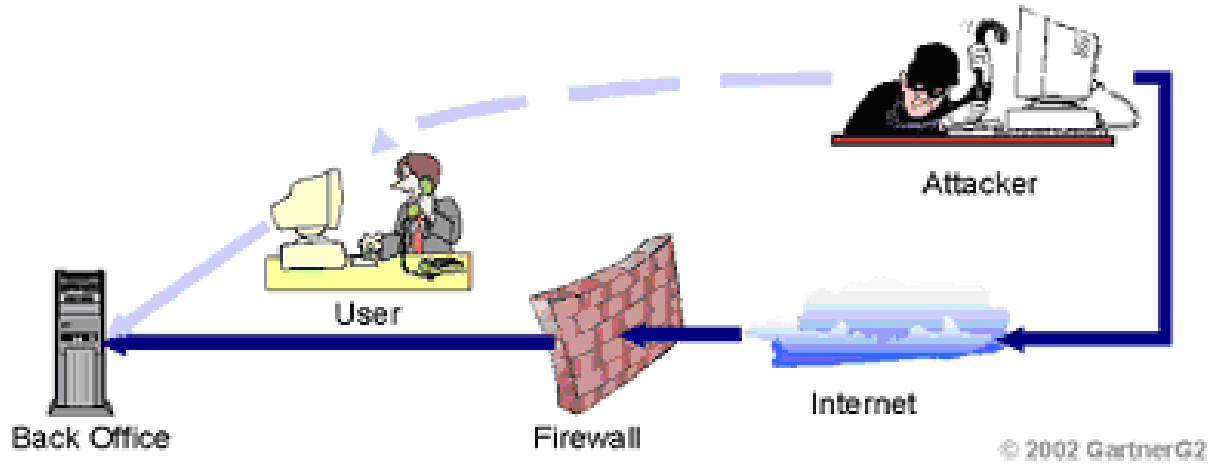


Abbildung 3.: Der Weg eines Social Engineer

## 4.1. Grundlegende Schutzmaßnahmen

Es gibt allerdings einige Bausteine, auf die man setzen kann, wenn man sich gegen Social Engineering schützen möchte:

- Schulung aller betroffenen Mitarbeiter in regelmäßigen Abständen
- Poster, Aufkleber, Warnhinweise
- Authorisierungen möglichst gering halten und die Leute mit Authorisierung besonders intensiv schulen
- Alte Dateien, Papiere, Festplatten und sensible Dokumente zerschreddern
- Keine Standardisierung von UserAccounts bspw. Logins, Passwörter und Anmeldungen mittels Perlscripten etc.
- Versuchen keine sensiblen Daten an die Öffentlichkeit dringen zu lassen, zum Beispiel durch Einträge in Telefonbücher, Broschüren..

## 4.2. Secure Awareness

**Definition 3 – Secure Awareness:**
**Bewusstsein bzw. Sensibilität der IT-Nutzer für Belange der Informationssicherheit.**

Das Wichtigste ist generell auch das Schwierigste. Es geht um das Sicherheitsbewusstsein an sich. Dieses zu entwickeln oder zu verbreiten kann aber nicht nur die Aufgabe eines Sicherheitsbeauftragten sein. Es geht um viele Faktoren: Die Corporate Identity, das Gemeinschaftsgefühl in der Firma und wie die Gesellschaft generell über Sicherheit in der IT aufgeklärt ist.

Möglichkeiten zur Steigerung des Bewusstseins:

- Es muss generell in der Gesellschaft selbstverständlich sein, dass Daten sensibel sind und sie geschützt werden müssen.
- Jeder Mitarbeiter muss logisch verstehen, warum er etwas tun darf oder muss.
- Es muss klar und informativ über die Sicherheit und die Möglichkeit von Firewall und anderen Sicherheitssystemen informiert werden.

Aber auch wenn es schwer fällt, sollte ein solches Bewusstsein in der Firma oder dem Unternehmen Normalität sein, so ist es ein riesen Vorteil für die IT-Sicherheit in Unternehmen oder der Behörde.

# 5. Anhang

## Literaturverzeichnis:


/Mitnick-02/ Mitnick, S., William L. S.:
The Art of Deception: Controlling the Human Element of Security., Wiley Publishing Inc., 2002

/Wikipedia-06/ http://de.wikipedia.org/wiki/Social_Engineering (Sicherheit)

/Christian-06/ http://social.christian-grafe.de/Sicherheitsbewusstsein.pdf

/Christian2-06/ http://social.christian-grafe.de/


## Abbildungsverzeichnis


Abbildung 1.: Was versteht man unter Sicherheitskultur ..... 1
Abbildung 2.: Beispiel einer Phishingseite – Hier Ebay.de ..... 4
Abbildung 3.: Der Weg eines Social Engineer ..... 7


## Definitionsverzeichnis


Definition 1 – Social Engineering: ..... 3
Definition 2 – Phishing: ..... 4
Definition 3 – Secure Awareness: ..... 8