INSTITUT FÜR INFORMATIK
DER LUDWIG–MAXIMILIANS–UNIVERSITÄT MÜNCHEN


**Bachelorarbeit**

# Kategorisierung von Social-Engineering-Angriffen im Hochschulumfeld und Gegenmaßnahmen

Martin Fröhlich

INSTITUT FÜR INFORMATIK
DER LUDWIG–MAXIMILIANS–UNIVERSITÄT MÜNCHEN


**Bachelorarbeit**

# Kategorisierung von Social-Engineering-Angriffen im Hochschulumfeld und Gegenmaßnahmen

Martin Fröhlich

| | |
|---|---|
| Aufgabensteller: | Priv. Doz. Dr. Wolfgang Hommel |
| Betreuer: | Stefan Metzger |
| Abgabetermin: | 15. November 2013 |

Hiermit versichere ich, dass ich die vorliegende Bachelorarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den 15. November 2013

.....
*(Unterschrift des Kandidaten)*

**Abstract**

Neben klassischer Schadsoftware, wie Viren, Würmern, Trojanischen Pferden oder auf Systemen installierte Rootkits, konzentrieren sich Angriffe, die unter dem Oberbegriff Social Engineering zusammengefasst werden, auf die menschliche Beeinflussung. Sie haben das Ziel, bei Personen ein bestimmtes Verhalten hervorzurufen, um beispielsweise vertrauliche Informationen zu erhalten.

Anhand einer selbständig durchgeführten Literaturrecherche wurden zunächst möglichst viele verschiedene Social-Engineering-Angriffsvarianten identifiziert und zusammengestellt. Neben einer allgemeinen Beschreibung der jeweiligen Attacke sind fiktive, aber dennoch realistische Beispiele konstruiert worden, wie die entsprechenden Angriffe auch im Hochschulumfeld ablaufen könnten. Dazu wurden im Speziellen auch die vom LRZ erbrachten Dienste herangezogen.

Die verschiedenen Angriffsvarianten wurden anschließend in Form einer Kategorisierung aufbereitet. Das dabei entstandene Schema ist dahingehend überprüft worden, ob eine hochschulspezifische Kategorisierung nötig ist und es den Anforderungen einer Taxonomie genügt. Die erarbeitete Kategorisierung erhebt den Anspruch, dass auch zukünftig neu identifizierte Angriffsvarianten eindeutig eingeordnet werden können. Für das Schema sind anschließend verschiedene Darstellungsmöglichkeiten behandelt und anhand ausgewählter Gesichtspunkte miteinander verglichen worden.

Für die konzipierten Kategorien mit ihren jeweiligen Angriffsvarianten wurden Gegenmaßnahmen vorgestellt, die beispielsweise in Security-Einweisungen und -Schulungen einfließen oder als technische Sicherheitsmaßnahme angeboten werden könnten.

# Inhaltsverzeichnis

# 1 Einleitung

In der heutigen Zeit werden immer mehr sensible Daten, seien es personenbezogene Informationen wie der eigene Name, Fotos, Geburtsdatum, Bankverbindungen oder auch jegliche Form vertraulicher Dokumente, Computern und dem Internet anvertraut. Dieser Umstand und die Angst davor, Fremde könnten sich an ihren Daten vergreifen, bringt bei allen Nutzern dieselbe Frage hervor: „Sind meine Daten sicher?“

Diese Problematik ist in der Öffentlichkeit zum fortwährenden Diskussionsthema geworden. Dennoch ist eine Antwort auf diese Frage eigentlich schnell gegeben: Wird ein angemessenes Passwort oder eine ausreichende Verschlüsselung verwendet, was ein anderer Computer nicht oder nur in utopischer Zeit umgehen kann, so lautet sie ja, ansonsten nein.

Die Sicherheit von Computern beziehungsweise Daten ist aufgrund der Möglichkeiten, die das Internet bietet, heutzutage von so großer Bedeutung, dass das Leistungsvermögen der zum Schutz beitragenden Mechanismen stetig gewachsen ist. Mittlerweile können sie dem Nutzer ein Höchstmaß bieten, sodass Informationen vor automatisierten, technischen Angriffen relativ sicher sind. Dieser Umstand erforderte ein Umdenken auf Seiten der Angreifer, denn der Risikofaktor und das schwächste Glied für die Sicherheit der Daten heißt nun meist nicht mehr Technik, sondern Mensch.

## 1.1 Motivation und Zielsetzung

Der Begriff für menschenbezogene Angriffe im Computer-Umfeld ist „Social Engineering“. *Social Engineering* beschreibt die Kunst, einen Menschen oder sein Umfeld so zu „benutzen“, dass geheime Informationen mehr oder weniger freiwillig preisgegeben werden. Mit Hilfe dieser Techniken kann ein Angreifer die Schwierigkeiten, die Schutzmechanismen am Computer möglicherweise darstellen, überwinden, um sein eigentliches Ziel ohne weitere Probleme und Hilfsmittel zu erreichen, was Abbildung 1.1 schematisch zeigt. „Human Hacking“(vgl. [Had11]) ist ein weiterer treffender Begriff für diese (nicht immer rechtmäßige) Art der Informationsbeschaffung. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert *Social Engineering* folgendermaßen:

> Social Engineering ist eine Methode, um unberechtigten Zugang zu Informationen oder IT-Systemen durch “Aushorchen“ zu erlangen. Beim Social Engineering werden menschliche Eigenschaften wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt. Dadurch können Mitarbeiter so manipuliert werden, dass sie unzulässig handeln. (siehe [Bun])

Als aktuelles Beispiel kann die NSA[1]-Affäre genannt werden, die von Whistleblower Edward Snowden ins Rollen gebracht wurde. Laut der Website *golem.de* soll er sich Passwörter von rund 20 NSA-Mitarbeitern besorgt haben, indem er vorgab, diese für seine damalige Tätigkeit als Systemadministrator zu benötigen. Mit den Zugangsdaten war er in der Lage geheime Dokumente herunterzuladen, die Informationen über die Arbeit des amerikanischen Geheimdienstes NSA und des britischen GCHQ[2] enthalten (vergleiche [Gre13]). Snowden gab also fälschlicherweise vor, die Passwörter seiner früheren Kollegen für seine Arbeit zu benötigen, obwohl er lediglich an geheime Informationen gelangen wollte. Dazu erfand er wahrscheinlich eine Geschichte, die es den NSA-Mitarbeitern plausibel erklärte, warum er ihre Zugangsdaten benötige. Snowden verwendete zu seiner Informationsbeschaffung demnach eine Art von *Social Engineering*. Dass selbst eine so stark abgesicherte Behörde wie die NSA von *Human-Hacking-Angriffen* betroffen sein kann, zeigt die Brisanz und Gefährlichkeit solcher Attacken.

Da bereits eine weitaus größere Anzahl unterschiedlicher Arten solcher Angriffe vorhanden ist und diese in Zukunft mit hoher Wahrscheinlichkeit weiter wachsen wird, ist Unübersichtlichkeit ob der Fülle kaum vermeidbar. Demnach wäre es wünschenswert, Bezeichnungen für Gruppen von Attacken zu haben, um relativ schnell deren spezifische Eigenschaften herauszufinden. Diese Kategorien gilt es im Rahmen dieser Bachelorarbeit zu identifizieren und in eine geordnete Struktur einzusortieren.

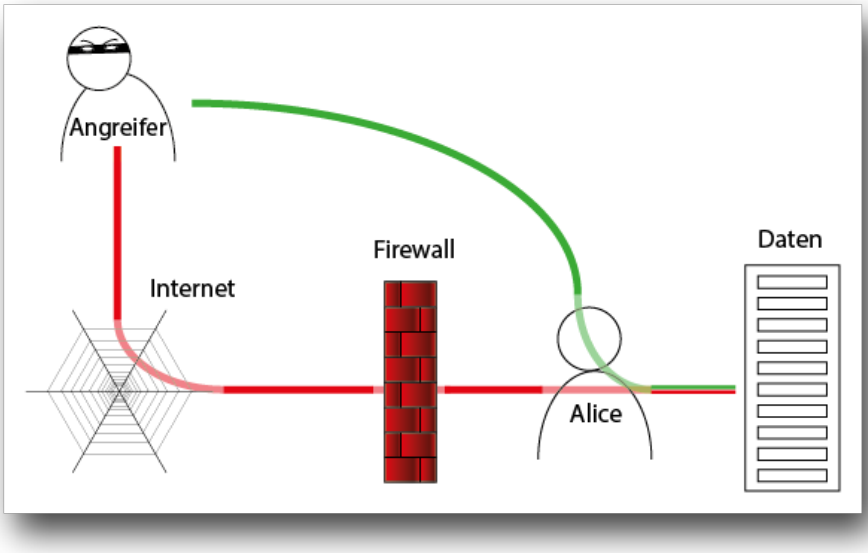



Abbildung 1.1: schematische Darstellung des Unterschiedes von gängigem Hacking (rote Route) und einer Social-Engineering-Variante (grüne Route)

Alle *Social-Engineering-Angriffe* werden gesondert in Bezug auf die angebotenen Hochschuldienste des Leibniz-Rechenzentrums (folgend als LRZ bezeichnet) betrachtet. Das LRZ bietet Kennungen für Studenten und Hochschulmitarbeiter an, welche den Zugriff auf einen Online-Speicher, einen Mailserver und den Zugang zum Münchner Wissenschaftsnetz (fol-

[1] NSA – National Security Agency
[2] GCHQ – Government Communications Headquarters

gend als MWN bezeichnet)[3] ermöglichen. Des Weiteren sind damit die in den Computer-Investitions-Programm-Pools (folgend als CIP-Pools bezeichnet) deponierten Rechner an der Ludwig-Maximilians-Universität München (folgend als LMU bezeichnet) zugänglich und die Nutzung der zentralen TUM[4]–Lernplattform `www.moodle.tum.de` möglich. Für Hochschulmitarbeiter bietet das LRZ optional die Verwendung von Hoch- und Höchstleistungsrechnern für wissenschaftliche Zwecke an.
Über den VPN-Zugang zum MWN haben Nutzer die Möglichkeit und die Berechtigung auf die LAN-Steckdosen[5] und die Wireless LAN's[6] in den Hochschulen Münchens zuzugreifen. Mit der Kennung sind außerdem eine Ferneinwahl in das MWN, die Nutzung MWN-interner Dienste und der Zugriff auf das IT-Portal von Gartner[7] möglich.
Neben dem SSID „lrz“ bietet das LRZ das Netz mit dem SSID „eduroam“ an, auf das der Nutzer einer LRZ-Kennung ebenfalls zugreifen kann. Die Vorteile des Zugangs sind vor allem die internationale Verbreitung und dass kein VPN-Client zum Verbindungsaufbau benötigt wird.
Abseits dieser technischen Angebote hat das LRZ einen Servicedesk, der durchgehend erreichbar ist. Zu den Kernzeiten des Servicedesks ist auch eine persönliche Präsenzberatung direkt im LRZ-Gebäude in Garching vorhanden (siehe [LRZ13]).

## 1.2 Aufgabenstellung

In dieser Bachelorarbeit soll eine möglichst monohierarchische Klassifikation für *Social-Engineering-Angriffe* unter Betrachtung der Attacken im Hochschulumfeld erstellt werden. Zudem soll geprüft werden, ob das resultierende Schema eine Taxonomie darstellt, also die unstrittige, eindeutige Einsortierung von Angriffen möglich ist. Das verstärkt das Bestreben, vage Klassengrenzen bei der Erstellung zu vermeiden.

Um die Angriffe im MWN beziehungsweise dem allgemeinen Hochschulumfeld darzustellen, wird der mögliche Ablauf einer solchen Attacke beispielhaft beschrieben. Dabei soll analysiert werden, wie gefährlich ein solcher Angriff werden kann und inwiefern dieser eine Einschränkung der Services nach sich zieht. Ergänzend soll die entstandene Kategorisierung dahingehend überprüft werden, ob die Klassierung eines Angriffs möglich ist, der nicht das Hochschulumfeld gefährdet, soweit eine solche Attacke in Betracht gezogen werden kann. Des Weiteren soll eine passende visuelle Darstellung der Klassifikation herausgearbeitet werden.

Anschließend sind mögliche Gegenmaßnahmen für die einzelnen Klassen auszuarbeiten. Daraus soll ersichtlich sein, ob die genannten *Social-Engineering-Angriffe* in irgendeiner Form zu verhindern sind. Gegenmaßnahmen können hierbei sowohl technischer Art, wie zum Beispiel bessere Sicherheitsvorkehrungen, als auch organisatorischer Art sein, nämlich Schulungen oder andere Methoden zur Sensibilisierung potentieller Opfer. Außerdem soll eine Analyse stattfinden, ob diese Gegenmaßnahmen auch im Hochschulumfeld wirksam

[3] wird vom LRZ angeboten und betrieben – ist über den Service Set Identifier (folgend als SSID bezeichnet) „lrz“ und Verbindung via Virtual Private Network Client (folgend als VPN bezeichnet) erreichbar
[4] ausgeschrieben Technische Universität München, folgend als TUM bezeichnet
[5] ausgeschreiben Local Area Network, folgend als LAN bezeichnet
[6] folgend als WLAN bezeichnet
[7] zu finden unter: `https://www.lrz.de/services/sonstiges/gartner/`

und in der beschriebenen Art umsetzbar wären. Die aufgelisteten Sicherheitsmechanismen sind dabei in eine bereits existente, auf Gegenmaßnahmen spezialisierte Kategorisierung einzusortieren. Deren Belegung ist mit der des hier entstandenen Schemas im Hinblick auf Zusammenhänge und Unterschiede zu vergleichen.

Insbesondere sollen jedoch nicht nur aktuell bestehende, sondern auch eventuell in Zukunft entwickelte Vorgehensweisen bei der Ausarbeitung der unterschiedlichen Klassen in Betracht gezogen werden. Damit soll sichergestellt werden, dass auch diese – bestenfalls eindeutig – klassifiziert werden können. Müsste man für jeden künftigen Angriff die Kategorisierung ein weiteres Mal überarbeiten, so verfehlt das hier entwickelte Schema seinen Zweck.

## 1.3 Struktur der Arbeit

Im nächsten Kapitel werden die verschiedenen Angriffsvarianten des *Social Engineering* vorgestellt. Die Stoffsammlung soll einen Überblick über das weite Feld des *Human Hacking* schaffen und jede Attacke mit einer genauen Definition, sowie einem Beispiel erläutern. Bereits in diesem Kapitel werden die Angriffe in ein in der Literatur häufig genanntes Schema eingeordnet. Diese erste Einteilung bringt die Knoten mit niedrigem Level, sprich die Knoten nahe der Wurzel, welche in unserem Fall „Social-Engineering-Angriffe“ heißt, für die Klassifizierung hervor. Danach wird das Hochschulumfeld definiert und die Angriffe exemplarisch in den universitären Alltag übertragen.

Im darauffolgenden Kapitel werden für die unterschiedlichen Attacken charakteristische Eigenschaften bestimmt und tabellarisch zusammengefasst. Mit Hilfe dieser Darstellung wird eine grobe Einteilung vorgenommen. Danach werden die verschiedenen Klassen und deren Merkmale identifiziert und passende Bezeichnungen herausgearbeitet. Sobald die Klassifikation ihren endgültigen Zustand erreicht hat, sollen die aufgeführten Angriffsvarianten des *Social Engineering* eindeutig einer Kategorie der Systematik zugeordnet werden. Nachdem dies geschehen ist, werden unterschiedliche Darstellungsmöglichkeiten vorgestellt und nach bestimmten Kriterien bewertet.

Anschließend werden zu jedem Angriff passende Gegenmaßnahmen genannt, welche ihrerseits wiederum in eine bereits vorhandene Kategorisierung einsortiert werden. Hierbei soll sowohl analysiert werden, inwiefern sich die Sicherheitsmechanismen der unterschiedlichen Attacken gleichen und welche Rückschlüsse daraus gezogen werden können, als auch Zusammenhänge dieser Kategorisierung mit dem im vorherigen Kapitel entstandenen Schema betrachtet werden.

Nachdem die aktuellen Attacken in der Arbeit ausreichend behandelt wurden, werden die Ergebnisse zusammengefasst. Abschließend wird ein Ausblick auf mögliche weiterführende Arbeiten und die Zukunft des *Social Engineering* gegeben, sowie das entwickelte Schema in Hinblick auf die Klassierung kommender Übergriffe bewertet.

# 2 Social-Engineering-Angriffe

In diesem Kapitel werden die verschiedenen *Social-Engineering-Angriffe* und ihre Varianten im Einzelnen definiert und erklärt. Für die anfängliche Einteilung der Attacken wird die Art der Informationsbeschaffung verwendet. Hierfür werden in der Literatur die drei Teilbereiche *Human Based Social Engineering* und *Computer Based Social Engineering* sowie *Reverse Social Engineering* unterschieden (siehe [Eic08]). Die letztgenannte Variante (*Reverse*) ist komplett losgelöst und als ein einzelner Angriff zu behandeln, da es keine bekannten, unterschiedlich aufgebauten Attacken dieser Art gibt.
Neben der Einsortierung in eine der beiden übrigen Oberkategorien wird jeder Angriff durch ein repräsentatives Beispiel genauer veranschaulicht.

## 2.1 Human Based Social Engineering

*Human Based Social Engineering* umfasst all jene Angriffe, bei denen die „Informationen auf nicht-technischem Weg über die soziale Annäherung an Personen beschafft“ ([Eic08]) werden.
Im Großen und Ganzen zielen Attacken dieser Kategorie auf die Naivität und Unvorsichtigkeit von Menschen ab. Nachdem bei einigen Übergriffen dieser Kategorie direkter Kontakt zwischen Opfer und Täter besteht, achtet der Täter besonders auf sein Verhalten, um seinen Angriff nicht zu offensichtlich durchzuführen. Die einzelnen Attacken dieser Rubrik werden im Folgenden erklärt.

### 2.1.1 Dumpster Diving

Kevin Mitnick, einer der renommiertesten *Social Engineers*, beschreibt als *Dumpster Diving*[1] das „Durchwühlen von Abfall einer Firma [oder einer Zielperson (Anm. d. Verf.)](oft in Mülltonnen, die außerhalb der Gebäude leicht zugänglich sind), um ausrangierte Informationen zu finden, die entweder selbst von Wert sind oder die man als Werkzeug bei einem Social-Engineering-Angriff einsetzen kann“ ([Mit06]).
*Dumpster Diving* ist vielleicht nicht die eleganteste Art der Informationsbeschaffung, in ihrer Effektivität jedoch nicht zu unterschätzen. Hinzu kommt, dass diese Attacke legal ist, sobald sie auf öffentlichem Gelände stattfindet. Das ist besonders in Firmen brisant, bei denen sich die Müllcontainer nicht auf dem Betriebsgelände befinden. Außerdem sollten die Mitarbeiter darin unterrichtet werden, wie sensible Dokumente entsorgt werden müssen. Hierzu gibt es in den meisten Unternehmen auch eine Policy[2], die genau diese Problematik behandelt.

[1] *engl.:* dumpster – Müllcontainer , *engl.:* to dive – tauchen, hechten
[2] Richtlinie, in der verschiedene Vorgehensweisen und Routinen beschrieben werden

Beim *Dumpster Diving* versucht der Angreifer sich Zugang zu den Mülltonnen seines ausgewählten Ziels zu verschaffen, was je nach Vorkehrungen des Unternehmens unterschiedlich schwer sein kann. Relativ einfach könnte er, getarnt als Mitarbeiter einer Reinigungsfirma, die Container, Abfalleimer oder auch die Schreibtische von Beschäftigten seines Zielobjekts durchsuchen. Um schnell an interessante Dokumente zu gelangen, achtet er auf auffällige Überschriften, Umschläge oder Markierungen der Papiere. Dabei sind für ihn Schreiben von Banken, Versicherungen, Ärzten und Behörden sowie Kontoauszüge, Kreditkartenabrechnungen, Ausdrucke firmeninterner Dokumente und Rechnungen von besonderem Interesse.

### 2.1.2 Shoulder Surfing

*Shoulder Surfing*[3] ist ein klassisches, effektives, einfach und schnell durchführbares Verfahren, um an zu schützende Werte zu gelangen, da es ohne jegliche Vorbereitungszeit angewandt werden kann.
Es ist der „Vorgang, eine Person beim Tippen am Computerkeyboard zu beobachten, um sein Passwort und andere User-Informationen ausfindig zu machen und zu stehlen."([Mit06])
Es ist ebenfalls möglich, mit einer Kamera über die Schulter eines Mitarbeiters zu fotografieren oder zu filmen, um das ausspionierte Material jederzeit zur Verfügung zu haben. Situationen für die Verwendung von *Shoulder Surfing* sind all jene, bei denen der Geschädigte personenbezogene, vertrauliche oder gar sensible Daten in sein Gerät eintippt oder diese bearbeitet.

Die Auswahl eines Ziels kann geplant, aber auch spontan geschehen. Ein unvermittelter Zugriff kann sich durch das zufällige Erscheinen eines Mitarbeiters einer für den Angreifer interessanten Firma ergeben und wird durch die Einfachheit der Attacke begünstigt. Anhand von Aufklebern, die von Geschäften oder Behörden gerne auf Reiselaptops angebracht werden, oder der Art des Laptops (Konzerne verwenden oft hochwertige Notebooks, wie Lenovo ThinkPads, vormals IBM) ist für den Angreifer schnell zu erkennen, ob es sich um ein potentielles Opfer handelt (siehe hierzu Abschnitt 2.1.7) (vgl. [Lon08]).

Die Geheimzahl für die Bankkarte am Geldautomaten oder an der Kasse eines Supermarktes, der Versand vertraulicher E-Mails, das Passwort für den Zugang auf Server oder den eigenen Computer und Post-It's, die an Bildschirmen haften, sind für den Angreifer interessante Ziele und jederzeit einen Blick wert. Auch das Bild des Desktops kann viel über den Benutzer des Computers verraten, denn die Verknüpfungen dort offenbaren einiges über die Tätigkeit und lassen den Angreifer schnell entscheiden, ob sich ein weiterer Zugriff lohnt. Nicht nur der Inhalt des Desktops, sondern auch das Hintergrundbild kann beispielsweise über den Familienstand oder andere Präferenzen des Opfers Aufschluss geben. Die gerade erwähnten Post-It's halten ebenfalls oft sensible Daten, wie Aufgaben, die der Besitzer zu erledigen hat, oder – in nicht all zu seltenen Fällen – sogar das Passwort für den Computer an dem sie sich befinden. Nicht nur die kleinen gelben Klebezettel, sondern auch auf dem Schreibtisch verteilte Dokumente können für den Täter interessant sein (vgl. [Lon08]).

[3] *engl.:* shoulder – Schulter , *engl.:* to surf – surfen

### 2.1.3 Tailgating

*Tailgating*[4] ist eine sehr einfache und zielführende Methode, sich unautorisiert Zutritt zu einem der Öffentlichkeit verschlossenen Gebäude oder Raum zu verschaffen. Der Angreifer wartet dabei vor einer verschlossenen oder gesicherten Tür, bis eine oder mehrere zugangsberechtigte Personen jene entriegeln und folgt ihnen (siehe [Kor12]).

Dabei gibt es mehrere Szenarien, wie eine solche Situation aussehen kann. Der Angreifer wartet unauffällig in einem Versteck, bis sich die Möglichkeit bietet, das Gebäude zu betreten. Öffnet ein Zutrittsberechtigter die Tür, folgt ihm der Angreifer unauffällig hindurch, bevor sie sich wieder schließt. Ebenso kann er durch einen großen Gegenstand in den Händen provozieren, dass ihm die Tür bereitwillig aufgehalten wird oder verkleidet als auswärtiger Service-Mitarbeiter außerhalb des Gebäudes warten, bis er sich zusammen mit Angestellten in das Objekt begeben kann. Dabei ist neben einer eloquenten Ausdrucksweise auch die überzeugende und passende Bekleidung Schlüsselelement. Zudem kann hierbei eine vorhergehende Observierung einer zu kopierenden Person, ihrer Arbeitskleidung sowie *Badge Surveillance* (siehe Abschnitt 2.1.4), die Kopie eines Dienstausweises, zum Einsatz kommen (vgl. [Lon08]).

Ergänzend sei erwähnt, dass *Tailgating* begrifflich auch das Verhalten von Stadionbesuchern (weit) vor Beginn einer sportlichen Veranstaltung umfasst. Bei einer sogenannten Tailgate-Party verkürzen sich die Zuschauer das Warten, indem sie sich auf dem Parkplatz der Arena zusammenfinden, um gemeinsam auf den Einlass zu warten. *Tailgate* bezeichnet als Nomen die Heckklappe eines Autos, welche namensgebend für diese Zusammenkunft ist. Nachdem bei der Attacke aber das dichte Folgen (siehe Fußnote 4) einer autorisierten Person und nicht der Vorgang des Wartens bezeichnend ist, ist ein derartiger Zusammenhang auszuschließen.

### 2.1.4 Badge Surveillance

*Badge Surveillance*[5] beschreibt die Tätigkeit eines Angreifers, Zutrittsausweise von Mitarbeitern der zu attackierenden Firma zu beobachten. Wie bereits im vorherigen Abschnitt 2.1.3 erwähnt, kann das passende Outfit eine vermeintliche Zugangsberechtigung vortäuschen. Ein zusätzlich vorgezeigter, offiziell aussehender Ausweis vermindert das Misstrauen der Menschen drastisch, selbst wenn es an sich nur ein kleines Accessoire ist. *Badge Surveillance* unterstützt das Kopieren eines solchen Identifikationsnachweises. Da viele Mitarbeiter auch abseits des Firmengeländes ihre Zutrittsausweise sichtbar mit sich tragen, erhält der Angreifer leicht die Gelegenheit, diese zu beobachten und eventuell zu fotografieren, um anschließend eine gute Vorlage für seine Kopie zu haben.

Abbildung 2.1 zeigt die gefälschte Version eines Zutrittsausweises für die Niederlassung eines japanischen Unternehmens der Foto- und Optikindustrie in Deutschland. Es bedarf nur einer zweckdienlichen Online-Recherche, um auf Fotos von Mitarbeitern mit Dienstmarke der Firma zu stoßen. Das passende Schlüsselband ist im Online-Shop des Betriebs bestellbar,

[4] *engl.:* to tailgate – (dicht) auffahren
[5] *engl.:* badge – Ausweis, Abzeichen , *engl.:* surveillance – Beobachtung, Observation

nach 20 minütigem Aufwand ist das Badge einsatzbereit und sieht auf den ersten Blick offiziell aus, was einem Angreifer zum unerlaubten Eindringen in ein Gebäude ausreichen kann.


Abbildung 2.1: Beispiel der Fälschung eines Angestelltennachweises der Niederlassung des Unternehmens in Deutschland

### 2.1.5 Pretexting


Beim sogenannten *Pretexting*[6] kreiert der Angreifer ein falsches Szenario und gibt vor, eine dem Opfer gegenüber autoritäre, vertraute, höhergestellte oder geschultere Person zu sein. Dadurch erhofft sich der Täter größeren Einfluss auf das Opfer und auf diese Weise sensible Daten zu bekommen. Eine solche Vertrauensperson kann ein höherer Angestellter (Vorgesetzter), ein Bankier, ein Versicherungsberater oder auch ein Mitarbeiter des IT-Supports sein (vgl. [Mis11]).

> Pretexting is the ability to create a false scenario that would make a targeted victim feel comfortable giving you information. It is more than simple lying. Often it is impersonating an individual that the targeted victim perceives has the right to know the information. It could be a police officer, bank personnel, tax authorities, or insurance investigators. Sometimes all that is needed is an authoritative and earnest sounding voice. [Mis11]

[6] *engl.:* pretext – Vorwand, Schein

Diese Art von Angriff kann prinzipiell über jede Kommunikationsplattform erfolgen, geschieht jedoch meist telefonisch. Mit einigen zielgerichteten Fragen oder Anweisungen wird so versucht, an die Informationen zu gelangen, welche das Opfer entweder wegen der vermeintlich hierarchisch höheren Position, Naivität oder des geschaffenen Vertrauens durch die Kompetenzdifferenz preisgeben wird.

Um die geheuchelte Identität zu keinem Zeitpunkt der Durchführung in Gefahr zu bringen, wird sich der Angreifer vorher überlegen, wie seine Tarnung auszusehen hat. Dazu gehört möglicherweise auch eine vorhergehende Observation der zu kopierenden Person. Selbstredend entfällt dieser Part, wenn es sich um eine nicht existente oder dem Opfer unbekannte Person handelt. Der Täter wird sich bestmöglich in seine Rolle hineinversetzen, um der Ausdrucksweise und dem Auftreten seiner gefälschten Identität gerecht zu werden. Dementsprechend würde er beispielsweise als Support-Mitarbeiter hauptsächlich ins Detail gehende Fachsprache verwenden.

Ein gefälschtes Szenario könnte der Anruf bei einem Mitarbeiter eines Krankenhauses sein. Der Angreifer gibt sich als Arzt der Intensivstation aus und bittet den Mittelsmann, unter dem Vorwand es ginge um Leben und Tod, einige Patientenakten an eine vom Täter kontrollierte E-Mail-Adresse zu verschicken. Gibt der Angreifer glaubhaft zu verstehen, dass er höherrangig ist und die Dringlichkeit der Sache keine längere Diskussion zulässt, wird das Opfer in den meisten Fällen die entsprechenden Maßnahmen einleiten und dem „Arzt“ die vertraulichen Patientendaten zukommen lassen.

### 2.1.6 Quid pro Quo

*Quid pro quo*[7] beschreibt einen Angriff, bei dem der Täter direkten Kontakt mit seinem Opfer aufnimmt und ihm, wie der Name der Attacke schon sagt, eine Gegenleistung für die Offenbarung interessanter Informationen anbietet (vgl. [Mis11]).

> Quid pro quo is simply “something for something“, in other words the social engineer calls the targeted victim and offers something, maybe money, chocolates, merchandise for password or other personal information. Surprisingly, large numbers of victims readily give this information believing they are getting something in return. ([Mis11])

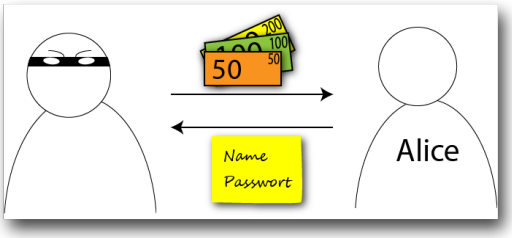



Abbildung 2.2: Zugangsdaten sind in vielen Fällen käuflich

Überraschend häufig werden bei einem Angriff dieser Art die vom Angreifer gewünschten Auskünfte tatsächlich preisgegeben. Auch hier kann die Kontaktaufnahme mit dem Geschädigten über jedes erdenkliche Kommunikationsmedium erfolgen.

Zur Vorbereitung hat der Täter über seine Methode, das Medium und die Gegenleistung zu entscheiden. So können beispielsweise im Rahmen einer vorgetäuschten telefonischen oder

[7] *lat.:* quid pro quo – etwas für etwas

Online-Umfrage relevante Hinweise gesammelt werden. Meist kann neben Name, Alter, Hobbys und sonstigen Angaben auch explizit nach den einzelnen, eigentlich schützenswerten Informationen gefragt werden. Als Entschädigung kann dem Opfer zum Beispiel ein Präsent in Form eines Kugelschreibers oder eines Gutscheins versprochen werden. Selbst für ein geringwertiges Geschenk sind viele Benutzer gewillt, ihre persönlichen Informationen offenzulegen.

### 2.1.7 People Watching

Auch wenn der Angriff mit der Bezeichnung *People Watching*[8] banal klingen mag, so erfordert er Routine und Erfahrung des Angreifers. Dieser tritt nicht in direkten Kontakt mit seiner Zielperson, sondern beobachtet diese nur. Hierbei wird auf Besonderheiten der Kleidung, des Verhaltens und auch auf mögliche Begleitpersonen geachtet. Aufschriften auf der Garderobe oder den Accessoires verraten Vorlieben oder die Tätigkeit des Gemusterten, welche, wenn nötig, mit der Hilfe einer Suchmaschine genauer bestimmt werden können. Sind alle Eigenheiten analysiert und in einen gemeinsamen Kontext gebracht, kann der sachverständige Täter ein Profil erstellen und entscheiden, ob eine weitere Observation oder die Anwendung eines anderen Angriffs lohnenswert ist (vgl. [Lon08]).

Abbildung 2.3: man kann jederzeit beobachtet werden

### 2.1.8 Diversion Theft

*Diversion Theft*[9] wird meist nur von erfahrenen *Social Engineers* durchgeführt, da es Fingerspitzengefühl und eine gute Informationsgrundlage verlangt. Ein solcher Angriff besteht darin, den Administrator oder das Personal einer Transportfirma zu überreden, dem Fahrer eines Werttransportes eine neue, geänderte Zieladresse zukommen zu lassen. Am falschen Ort angekommen, übergibt der Lieferant anschließend die Ware fälschlicherweise dem Täter und nicht dem eigentlichen Empfänger (siehe [Mis11]).

Als Beispiel sei ein Geldtransfer zwischen zwei Banken geplant. Das Transportunternehmen veranlasst, dass ein Fahrer das Geld mit einem Geldtransporter abholt und sich anschließend ohne Umwege zur Zieladresse begibt. Sobald der Lieferant die Wertpapiere im gesicherten Lastwagen deponiert und sich auf den Weg gemacht hat, ruft der Angreifer als angeblicher Mitarbeiter der zu beliefernden Bank beim Transporteur an und erklärt, dass sich die Lieferadresse aus einem wichtigen Grund geändert habe. Daraufhin bewirkt der Kontaktierte die Umleitung des Wagens. Ist der Lieferant dann an der anderen Position angekommen, erklärt ihm der *Social Engineer*, dass der Safe zur Aufbewahrung von Banknoten aktuell außer Betrieb sei und das Geld zwischenzeitlich in den „bankeigenen“ (eigentlich dem Angreifer gehörenden) Geldtransporter verfrachtet werden soll.

[8] *engl.:* people – Menschen, Leute , *engl.:* to watch – beobachten
[9] *engl.:* diversion – Ablenkung, Umleitung , *engl.:* theft – Diebstahl

## 2.2 Computer Based Social Engineering

> Bei dieser Variante wird der Computer als Täuschungs- und Kontaktwerkzeug verwendet. Sie ist gerade in Zeiten des Internet ein beliebtes Mittel, um schnell viele Personen anzugreifen. Der Social Engineer kann den Computer dazu benutzen, Kontakt herzustellen oder eine Täuschung durchzuführen. ([HZ09])

Ein direkter Kontakt von Geschädigtem und Täter ist allerdings nicht zwingend notwendig. Dadurch ist es für den Angreifer einfacher, seine Identität und somit auch die Attacke zu verschleiern. Nichtsdestotrotz werden weiterhin menschliche Schwächen ausgenutzt, um an die sensiblen Daten der Opfer zu gelangen.

### 2.2.1 Phishing

> Phishing refers to the practice of corresponding with a large number of people under the guise of a known entity (business or government agency) in an attempt to extract personal information such as social security numbers or passwords. Some of those people will inevitably believe that the correspondence is real and respond accordingly, with personal information. ([Gaz13])

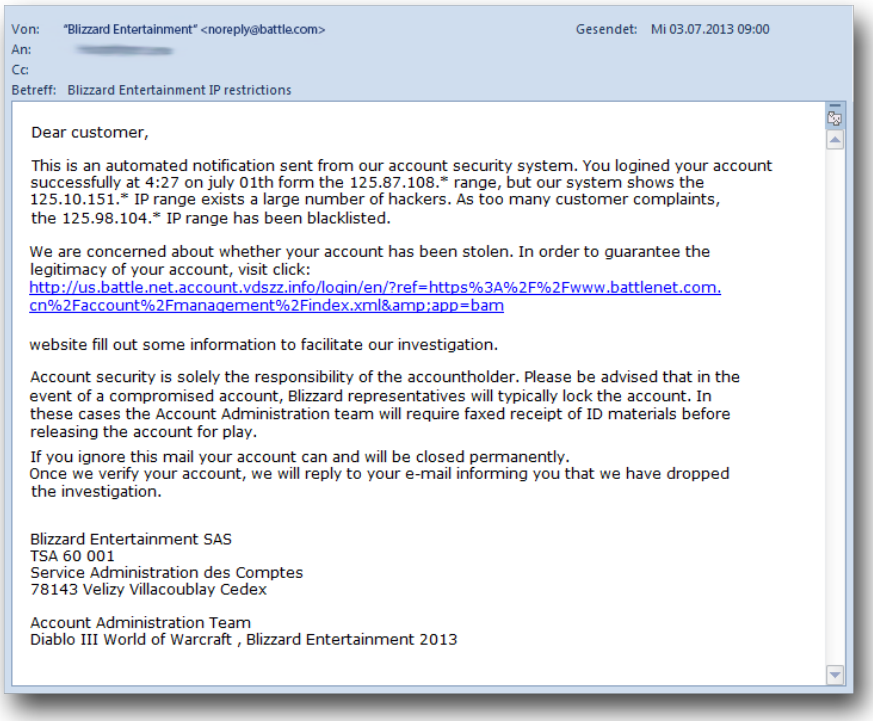
Als *Phishing*[10] bezeichnet man Attacken, mit denen der Angreifer – unter Missbrauch des Namens einer seriösen Einrichtung – an Daten des Opfers gelangen will, um Identitätsklau[11] zu begehen. Üblicherweise wird *Phishing* gegen mehrere Personen gleichzeitig ausgeübt, um die Chance eines „Treffers“ zu erhöhen. Bis dato ist keiner der auf dem Internet aufbauenden Kommunikationskanäle vor *Phishing* sicher (siehe [Gaz13]).
In den folgenden Absätzen werden einzelne *Phishing-Angriffe* genauer erläutert und die Unterschiede herausgearbeitet.

#### Phishing-E-Mails

Bei dieser Form des *Phishings* werden elektronische Nachrichten an viele, möglicherweise sogar alle Kunden eines Unternehmens versandt. Um bei einer *Phishing-E-Mail* ein möglichst authentisches Anschreiben zu generieren, wird sie meist im HTML-Format verschickt, womit die Nachricht die grafischen Möglichkeiten einer normalen Website aufweist und flexibel an die zu kopierende Firma sowie ihr Corporate Design angepasst werden kann. Üblicherweise enthält eine solche Mitteilung einen warnenden Text, der auf Sicherheitslücken aufmerksam macht, oder die Reaktivierung eines Kontos verlangt. Meist wird dabei die E-Mail-Adresse des Absenders so verändert, dass sie von einem offiziellen Schreiben noch schwerer zu unterscheiden ist, was bei E-Mails mit geringem Aufwand und sogenanntem *Spoofing*[12] möglich ist. Das Opfer wird aufgefordert, einem in der E-Mail angegebenen Link zu folgen, um die notwendigen Schritte zur Verbesserung der Dienste oder Reaktivierung des vermeintlich gesperrten Accounts durchzuführen. Allerdings erfolgt nach Aktivierung die automatische

[10] zusammengesetzter Kunstbegriff aus *password* (engl. für Passwort) und *fishing* (engl. für Angeln)
[11] werden auch *Identity-Theft-Attacken* (aus dem Englischen) genannt
[12] *engl.:* spoof – Schwindel

Weiterleitung auf eine gefälschte Website, welche vom Angreifer nach dem Vorbild der Homepage des Unternehmens zum Verwechseln ähnlich gestaltet wurde. Dort werden mithilfe eines Formulars weitere persönliche Informationen und geheime Angaben abgefragt, die nach Vervollständigung und Bestätigung dem Angreifer zugeschickt werden. In diesem Bereich des *Phishings* gibt es unterschiedliche Taktiken zur Distribution der E-Mails, welche nun im Einzelnen vorgestellt werden.


Von: "Blizzard Entertainment" <noreply@battle.com> Gesendet: Mi 03.07.2013 09:00
An:
Cc:
Betreff: Blizzard Entertainment IP restrictions

Dear customer,

This is an automated notification sent from our account security system. You logined your account successfully at 4:27 on july 01th form the 125.87.108.* range, but our system shows the 125.10.151.* IP range exists a large number of hackers. As too many customer complaints, the 125.98.104.* IP range has been blacklisted.

We are concerned about whether your account has been stolen. In order to guarantee the legitimacy of your account, visit click:
http://us.battle.net.account.vdszz.info/login/en/?ref=https%3A%2F%2Fwww.battlenet.com.cn%2Faccount%2Fmanagement%2Findex.xml&app=bam

website fill out some information to facilitate our investigation.

Account security is solely the responsibility of the accountholder. Please be advised that in the event of a compromised account, Blizzard representatives will typically lock the account. In these cases the Account Administration team will require faxed receipt of ID materials before releasing the account for play.

If you ignore this mail your account can and will be closed permanently.
Once we verify your account, we will reply to your e-mail informing you that we have dropped the investigation.

Blizzard Entertainment SAS
TSA 60 001
Service Administration des Comptes
78143 Velizy Villacoublay Cedex

Account Administration Team
Diablo III World of Warcraft , Blizzard Entertainment 2013

Abbildung 2.4: typische *Phishing-Mail*, angeblich von Blizzard Entertainment

**Clone Phishing** bedeutet, dass eine bereits vorher vom echten Unternehmen versandte E-Mail inklusive Link oder Anhang vom Angreifer kopiert wird. Dabei ersetzt er die zusätzlichen Informationen der originalen Mail durch eine schadhafte Version und schickt die Nachricht ein weiteres Mal an alle Empfänger. Um den Absender zu fälschen, wird vom Täter eine gespoofte E-Mail-Adresse verwendet und zusätzlich eine Art „Update-Hinweis“ gegeben, sodass die Nutzer nur die neuere E-Mail beachten (vgl. [Jac12]).

**Spear Phishing** nennt man einen personalisierten *Phishing-Angriff*. Der Angreifer täuscht vor, Vertrauter oder Freund des Opfers zu sein. Denkbar ist auch eine Rundmail an eine gesamte Gruppe von Leuten, die einen gemeinsamen Bekannten haben (zum Beispiel alle Mitarbeiter einer Abteilung). In beiden Fällen sammelt der Täter im Vorfeld Informationen, um eine plausible E-Mail verfassen zu können. Der Inhalt der Nachricht wird personalisiert und enthält wiederum einen Link oder ein wichtiges Dokument im Anhang, den der Leidtragende klicken oder das er öffnen soll. Davon ausgehend, die E-Mail sei von einer Vertrauensperson (auch hier ist eine gespoofte E-Mail-Adresse notwendig), kommt das Opfer der Bitte meist auch nach (siehe [Jac12]).

**Whaling** unterscheidet sich vom „normalen“ *Phishing* dadurch, dass hier ausschließlich hochrangige Mitarbeiter eines Unternehmens Empfänger und Angriffsziel der *Phishing-Mails* sind. Der Term *Whaling* kommt von der Redewendung „einen großen Fang machen“. Der Täter verspricht sich aufgrund der weitreichenden Entscheidungskompetenzen (u.a. bezüglich der Verwendung finanzieller Mittel) und der meist uneingeschränkten Zugriffsberechtigungen eines führenden Mitarbeiters großen Erfolg für seinen Angriff (vgl. [Jac12]).

### Vishing

*Vishing*[13] bezeichnet eine Attacke, bei der das Opfer in einer E-Mail aufgefordert wird, eine bestimmte Telefonnummer zu wählen. Dort wird es entweder von einer automatischen Ansage, wie Abbildung 2.5 darstellt, oder dem Angreifer, der sich als Service-Mitarbeiter ausgibt, empfangen und aufgefordert, Kontoinformationen oder Passwörter preiszugeben. Weitere Bezeichnungen für *Vishing* sind *Phone Phishing* oder passenderweise *IVR*[14] (vgl. [Mis11]).

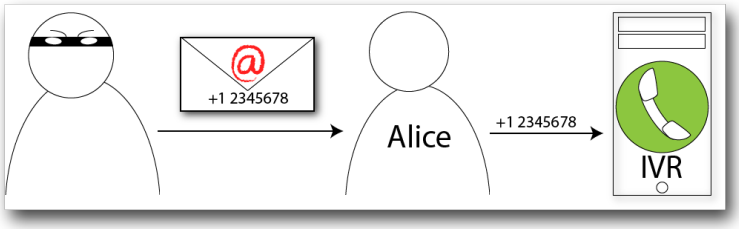



Abbildung 2.5: Variante eines Vishing-Angriffs

Beispielsweise sendet der Angreifer seinen Opfern eine gefälschte und gespoofte *Phishing-Mail* ihrer Bank, in der zur Reaktivierung ihres Kontos ein Telefonat mit dem Service-Desk gefordert wird. Ruft man dort an, wird man von einer automatischen Ansage oder dem *Social Engineer* persönlich empfangen und gebeten, Informationen wie Geburtsdatum, Ablaufdatum und Nummer der Kreditkarte, PINs oder Sozialversicherungsnummer preiszugeben. Um die vermeintliche Deaktivierung seines Kontos zu verhindern, wird das Opfer dem Angreifer bereitwillig seine Daten zur Verfügung stellen.

### Evil Twin

Ein *Evil Twin Angriff* benutzt nicht wie die bisherigen *Phishing-Angriffe* das Kommunikationsmedium E-Mail. Bei dieser Attacke generiert der Täter ein WLAN mit demselben SSID, wie eines, das an diesem Ort tatsächlich verfügbar ist (siehe Abbildung 3.2). Auch alle weiteren Einstellungen des zu kopierenden Zugangs übernimmt der Angreifer in seinen Access Point[15]. Loggt sich ein Nutzer fälschlicherweise in das vom Täter kontrollierte Netzwerk ein (auch automatisch möglich), kann der Täter bereits hier Log-In-Daten (Passphrase

[13] Voice phishing
[14] IVR – Interactive Voice Response
[15] folgend als AP bezeichnet

des eigentlichen Netzwerkes, IP/MAC-Adresse des Nutzers) abgreifen. Des Weiteren kann er über Veränderungen des DNS[16]-Caches den Nutzer auf gefälschte Internetseiten weiterleiten. Diese *Phishing-Websites* sind wiederum nach dem Vorbild jener Unternehmens-Seiten gebaut, von welchen der Täter die Nutzerinformationen stehlen möchte. Im Wesentlichen kann so die Bewegung des Opfers im Internet beliebig gesteuert werden, da der Angreifer die Kontrolle über die drahtlose Internetverbindung besitzt (siehe [Jam06]).

Ein solcher gefälschter Internetzugang ist vor allem für Laien sehr schwer auszumachen, da bei richtiger Durchführung alle Spezifikationen, Funktionalitäten und Eigenheiten der üblichen Internetverbindung kopiert werden. Ein *Evil Twin Angriff* wird meist von einem DoS (Denial of Service) des „Good Twin“, wie zum Beispiel mit SYN-Flooding[17], begleitet, sodass nur noch das schadhafte Netzwerk verwendbar ist. Die Gefahr einer solchen Attacke in der Öffentlichkeit ist unbestritten, da immer häufiger kostenlose AP's auf allgemein zugänglichen Plätzen oder in Cafés angeboten werden und eine große Menge an Opfern verfügbar ist.

### 2.2.2 Baiting

Als *Baiting*[18] bezeichnet man das Liegenlassen infizierter Datenträger (USB-Stick, CD/DVD, oder Diskette) an Orten, an denen der *Social Engineer* vermutet, dass Personen sie aufgrund von Neugierde oder Habgier aufsammeln könnten. Mit dem Speichermedium ködert er sein Opfer, das „Trojanische Pferd“ anzunehmen. Um den Anreiz zur Mitnahme zu vergrößern, werden die Datenträger mit Firmenlogos oder attraktiven Begrifflichkeiten versehen. Liest der Leidtragende dann später das Medium am Heim- oder gar dem Firmencomputer aus, installiert es im Hintergrund eine Schadsoftware, die dem Angreifer uneingeschränkten Zugriff auf die Daten und Funktionen des infizierten Rechners gewährt (vgl. [Mis11]).

> This technique requires the engineer to make a malware infected floppy disk, CD rom, or usb flash drive in a place an intended target(s) might pick it up out of curiosity or greed. The titles may be corporate information that would appear to allow the target information that would give financial gain. However presented, once the disk is inserted the users installs malware giving the engineer unfettered access to the targets pc or a company's internal computer network. ([Mis11])

Zur Vorbereitung einer *Baiting-Attacke* wird ein Datenträger mit der sich automatisch installierenden Schadsoftware bespielt und mit einer möglichst attraktiven Beschriftung an einem geeigneten Platz, wie zum Beispiel der Lobby, dem Parkplatz oder der Cafeteria des Zielunternehmens abgelegt. Das Medium könnte etwa das Logo einer Konkurrenzfirma mit der Überschrift „Jahresabschluss 2012“ tragen. Nach dem Deponieren liegt es an den Angestellten und deren Neugierde, den Angriff wirksam werden zu lassen.

[16] Domain Name System, folgend als DNS bezeichnet
[17] Angreifer stellt halboffene TCP-Verbindungen mit Server her, womit dieser ausgelastet wird und für andere Nutzer nicht mehr erreichbar ist
[18] *engl.:* bait – Köder

### 2.2.3 Forensic Analysis

*Forensic Analysis*[19] hat einen direkten Bezug zum *Dumpster Diving* (Abschnitt 2.1.1), da es sich ebenfalls auf entsorgtes Material konzentriert. Demzufolge wird auch bei dieser Attacke im „Müll getaucht“. Die auf ausrangierten Speichermedien enthaltenen Daten werden wiederhergestellt und anschließend analysiert, um dadurch sensible Informationen herauszufinden, die nicht in ausgedruckter Form vorhanden sind (vgl. [Oos08]).
Ebenfalls denkbar ist bei dieser Methode der gezielte Kauf von Datenträgern über Online-Auktionen oder andere Angebote. Die ausrangierten Medien sind oftmals noch mit Daten (wenn auch nicht auf den ersten Blick erkennbar) der Vorbesitzer beschrieben, wodurch der Täter einige interessante Informationen erhalten kann.

### 2.2.4 Badge Surveillance – Electronic Badges

Neben ausgedruckten und laminierten Zugangsberechtigungen sind elektronische Zugangsgeräte mit RFID (radio frequency identification) oder NFC (near field communication) entwickelt worden. Diese können die Form eines Chips (Abbildung 2.6) oder einer Karte (Abbildung 2.7) haben und werden von einer kleinen Apparatur neben einer Tür gelesen, die nach erfolgreicher Authentifizierung die Entriegelung des Schlosses bewirkt. Somit wird nur autorisierten Personen Zutritt zu einem Gebäude oder Raum gewährt. Um sich als unberechtigte Person Zutritt zu verschaffen, wird versucht, die Kommunikation der Zutrittsapparaturen abzufangen und zu kopieren.


Abbildung 2.6: RFID-Chip


Abbildung 2.7: RFID-Karte

Das Auslesen solcher Identifikationsmedien ist schon mit einem Mobiltelefon via NFC möglich. Hat der Angreifer die genannten Geräte frei zur Verfügung oder ist mit einem NFC-fähigen Smartphone in der Reichweite der Technologie, kann deren Speicher ausgelesen werden. Dazu genügt bereits eine kurze Annäherung auf dem Gang oder der Treppe, der Täter bewegt sein Gerät in die Nähe des RFID-Chips und die Daten sind übertragen. Ausgehend von einer unzureichenden Verschlüsselung der Information, ist anschließend die Kopie mit einem passenden Schreibgerät möglich.
Aus der beim Angriff ausgelesenen XML-Datei ist ersichtlich, welche Technik zur Verschlüsselung, beziehungsweise Programmierung des Chips verwendet wurde, welche Eigenschaften das Medium hat (Seriennummer, Produktionsdatum, Hersteller von Hardware und Software,

[19] *engl.:* forensic – gerichtsmedizinisch , *engl.:* analysis – Auswertung, Untersuchung

Speicherplatz, Anzahl der Blöcke und Sektoren, sowie Typen des Chips) und teilweise sogar welchen Inhalt die verschiedenen Sektoren haben. Ein Experte auf diesem Bereich kann dann bereits einige der Informationen entziffern und gegebenenfalls mit der Kopie eines solchen Chips beginnen.

```
13  ...
14  <MemoryTag type="Mifare Classic 1K">
15  <GeneralInformation>
16  <Value name="memorySize" description="Memory size"> 1024 Byte </Value>
17  <Value name="blockSize" description="Block size"> 16 Byte </Value>
18  <Value name="numberOfBlocks" description="Number of blocks"> 64 </Value>
19  <Value name="numberOfSectors" description="Number of sectors"> 16 </Value>
20  </GeneralInformation>
21  <Data unit="sector:block">
22  <Sector index="0">
23  <Block index="0" accessRead="keyA" accessWrite="never" accessIncrement="never"
        accessDecrementTransferRestore="never"> 723c09e8af880400c201000000000012 </Block>
24  <Block index="1" accessRead="keyA" accessWrite="keyA" accessIncrement="keyA" accessDecrementTransferRestore
        ="keyA"> 00000000000000000000000000000000 </Block>
25  <Block index="2" accessRead="keyA" accessWrite="keyA" accessIncrement="keyA" accessDecrementTransferRestore
        ="keyA"> 00000000000000000000000000000000 </Block>
26  <Block index="3" accessReadAccessBits="keyA" accessWriteAccessBits="keyA" accessReadKeyA="never"
        accessWriteKeyA="keyA" accessReadKeyB="keyA" accessWriteKeyB="keyA"> ffffffffffff078069ffffffffffff
        </Block>
27  </Sector>
28  ...
```

Code 2.1: Ausschnitt aus der XML-Datei der gelesenen RFID-Karte

```
17  ...
18  <MemoryTag type="Mifare DESFire EV1 (MF3ICD81)">
19  <GeneralInformation>
20  <Value name="serialNumber" description="Serial number"> 04853599C12580 </Value>
21  <Value name="batchNumber" description="Batch number"> CFB4176170 </Value>
22  <Value name="productionDate" description="Production date"> 45/2008 </Value>
23  <Value name="hardwareVendor" description="Hardware vendor"> NXP Semiconductors (Germany) </Value>
24  <Value name="hardwareVersion" description="Hardware version"> 1.0 </Value>
25  <Value name="hardwareType" description="Hardware type"> 0x0101(t504C) </Value>
26  <Value name="hardwareCommProtocol" description="Hardware communication protocol"> 0x05 </Value>
27  <Value name="hardwareMemorySize" description="Hardware memory size"> 8192 Byte </Value>
28  <Value name="softwareVendor" description="Software vendor"> NXP Semiconductors (Germany) </Value>
29  <Value name="softwareVersion" description="Software version"> 1.3 </Value>
30  <Value name="softwareType" description="Software type"> 0x0101 </Value>
31  <Value name="softwareCommProtocol" description="Software communication protocol"> 0x05 </Value>
32  <Value name="softwareMemorySize" description="Software memory size"> 8192 Byte </Value>
33  </GeneralInformation>
34  ...
```

Code 2.2: Ausschnitt aus der XML-Datei des gelesenen RFID-Chips

Neben der eben beschriebenen kontaktlosen Aktivierung gibt es noch die Möglichkeit von Durchzugskarten. Die Authentifikation läuft ähnlich ab, aber zum Kopieren der Karte muss sie im Gegensatz zu den RFID-Chips entweder zwingend im Besitz des Angreifers sein, da sie ein Empfangen der Daten ohne direkten Kontakt mit dem Lesegerät nicht unterstützen, oder der Angreifer sich eine Strategie überlegen, wie er seine potentiellen Opfer dazu bringt, ihre Karten durch sein Lesegerät zu ziehen (siehe [Lon08]).

## 2.3 Reverse Social Engineering

Als letzte Kategorie von Angriffen sei *Reverse Social Engineering* genannt. Diese Rubrik beinhaltet Attacken, die sowohl mit, als auch ohne technische Hilfsmittel auskommen.

> Ziel des Angreifers ist es hier, sich die gewünschten Informationen über das Opfer nicht selbst zu beschaffen, sondern einen Anwender dazu zu bringen, die Informationen freiwillig und aktiv an den Angreifer zu übermitteln. ([Eic08])

Oft verschafft sich der Angreifer dadurch den direkten Zugriff auf den Rechner oder das Netzwerk des Geschädigten. Gefährlich an einer solchen Vorgehensweise ist das geringe Misstrauen des Opfers, da der Täter von ihm selbst kontaktiert wurde.
Einzelne, explizit benannte Angriffe sind in dieser Kategorie nicht bekannt, da sich das Schema der Attacken nicht unterscheidet.

Als Beispiel kann sich der Angreifer in einem solchen Szenario als neuer Supportmitarbeiter beim Opfer vorstellen und seine Telefonnummer für den Fall eines Problems hinterlassen. Danach verursacht der Täter eine Dysfunktion am Rechner seines Ziels und bewirkt damit, dass das Opfer direkt ihn anstatt der zuständigen Hotline kontaktiert und um Hilfe bittet. Nachdem der Geschädigte dem „Support“ bei der Lösung des Problems behilflich sein möchte und dem Helfer vertraut, werden selbst sensible Daten freiwillig und aktiv übermittelt. Der Täter muss daher nur die richtigen Fragen stellen, um an die gewünschten Informationen zu gelangen.

# 3 Social Engineering im Hochschulumfeld

Nachdem nun das facettenreiche Feld des *Social Engineering* erfasst und die derzeit bekannten Attacken definiert sowie beispielhaft dargestellt wurden, stellt dieses Kapitel den Transfer in das Hochschulumfeld dar. Neben einer Definition des Hochschulumfeldes werden die Angriffe mit Hilfe plausibler Szenarien in den universitären Alltag eingegliedert.

## 3.1 Das Hochschulumfeld und das Münchener Wissenschaftsnetz

Um die verschiedenen *Human-Hacking-Attacken* nicht nur auf das MWN, sondern auch auf das allgemeine und internationale Hochschulumfeld projizieren zu können, muss dies vorher genau definiert werden. Denkbar sind drei Bereiche, bei denen ein *Social-Engineering-Angriff* ansetzen und durchgeführt werden könnte.

Zum Einen sind das Menschen, die an einer Universität einer Beschäftigung nachgehen. Explizit genannt seien hier Studenten, Hochschulmitarbeiter, Dozenten und Professoren. Bei allen Personen ist ein Angriff an der Uni und zu Hause (soweit dem Täter bekannt) möglich. Im Fall der Studenten ist auch ein Übergriff am Ort eines Nebenjobs denkbar. Interessant ist eine Betrachtung der unterschiedlichen Berechtigungen und Informationen, welche ein Angreifer eventuell über einen erfolgreichen Angriff je nach Position des Opfers erlangen kann.

Als Zweites sind die Einrichtungen der Universität und deren Organisation zu nennen. Hier kann man beispielsweise die Sekretariate der Lehrstühle oder der Prüfungsämter, die einzelnen Rechnerbetriebsgruppen, allgemein zugängliche Bibliotheken und die Fakultäten erwähnen. Vor allem die Auswahl der entsprechenden Fakultät ermöglicht dem Angreifer seine Opfer gezielt nach Themenbereich zu selektieren. Meist hält jedes Ressort seine eigenen Bibliotheken, Mensen, Lernräume (zum Beispiel die CIP-Pools an der LMU) sowie Mitarbeiterbüros. Im Gegensatz dazu kann bei Bibliotheken ohne spezifisches Fachgebiet allerdings eine größere Menge an potentiellen Zielen angesprochen werden. Ähnlich ist die Situation für einen Angriff über die Hörsäle der Universität. Hier können Täter sowohl wahllos, als auch gezielt Studierende, beziehungsweise Dozenten einer bestimmten Fachrichtung ansprechen, indem je nach Bedarf die Belegung des Saals beachtet wird.

Zuletzt kann *Social Engineering* im Hochschulumfeld auch bei grundsätzlich studienfernen Unternehmen ansetzen, welche mit der Universität kooperativ in Verbindung stehen. Nicht selten arbeiten einzelne Lehrstühle der Hochschulen mit Unternehmen der freien Wirtschaft zusammen. Speziell im MWN gibt es eine solche Konstellation sowohl lehrstuhl- als auch hochschulübergreifend. Das LRZ stellt im Wissenschaftsnetz insgesamt über 70 Dienste für die Hochschulen Münchens zur Verfügung. Um den Umfang der Auswertung nicht zu spren-

gen, werden Einzelne daraus gewählt, welche möglichst nicht nur für das MWN, sondern auch für andere Hochschulstandorte repräsentativ sind. Aus dieser Auswahl lässt sich allerdings nicht folgern, dass die restlichen, hier nicht berücksichtigten Dienste keine Angriffsfläche für einen *Social Engineer* darstellen. Die folgenden Leistungen wurden aufgrund der Menge an Betroffenen, ihrem Verbreitungsgrad oder ihrer möglichen Verwandtschaft zu Diensten an anderen Hochschulen ausgewählt.
Das LRZ stellt Kennungen zur Verfügung, mit denen die registrierten Nutzer verschiedene Services nutzen können. So ist damit beispielsweise der Zugriff auf eine persönliche Mailbox und die Netze „lrz“ (lokal im Raum München) und „eduroam“ (international an verschiedenen Hochschulen) gewährleistet. Durch die Internationalität des eduroam-Netzes und die dadurch sehr große Anzahl der Nutzer ist die Beurteilung der Gefährdung durch einen Angriff für Verwender dieses Netzes nicht nur im Falle des MWN von Relevanz. Da die meisten Universitäten außerhalb Münchens ihren Studierenden ebenfalls Hochschulkennungen und einen kostenfreien Internetzugang über den Login anbieten, ist die Betrachtung dieser Sparte für alle Hochschulen von Interesse. Angriffsgefährdet sind also Nutzerkennungen, die vom LRZ verwaltet werden.
Nicht nur die Benutzerkonten, sondern auch die Netze selbst können das Ziel von *Social Engineering* sein. Neben der Berechtigung zum Zugriff auf die beiden vorher erwähnten Netze fällt deren Betrieb in den Aufgabenbereich des LRZ. Eine erfolgreiche Attacke, die dem Angreifer die Gewalt über die Netzwerke verschafft, betrifft somit viele, bis alle Nutzer.
Auch die Betreuung und Unterstützung bei Incidents oder Service Requests zählt zu den Angeboten des LRZ. Der Servicedesk kümmert sich um Anliegen der Studenten und Hochschulmitarbeiter. Da dies meist mit persönlichem Kontakt geschieht, bietet auch dieser Bereich eine Angriffsfläche für *Social-Engineering-Angriffe*, wobei meist nur einzelne Benutzerkonten betroffen sind. Da aber die meisten Hochschulen ebenso über einen IT-Support oder eine Hotline verfügen und dieser Aspekt ein typisches Szenario für *Social Engineering* ist, ist die Betrachtung dieses Services auch im Hochschulumfeld von Relevanz.
Neben den Diensten des LRZ für Internet und Problem-Solving sind einige LRZ-Mitarbeiter auch Privatdozenten oder Übungsleiter an den Hochschulen Münchens. Naheliegend ist, dass auch dieses Feld, die Lehre, ein mögliches Ziel für *Social-Engineering-Angriffe* darstellt.

## 3.2 Anwendungsbeispiele für Social Engineering im Hochschulumfeld

Im Folgenden werden die verschiedenen *Social-Engineering-Angriffe* anhand eines musterhaften Beispiels im universitären Alltag reflektiert. Insbesondere soll hierbei auch auf die im Hochschulumfeld relevanten Dienste des LRZ Bezug genommen werden. Die nachfolgende Ausführung ist zur besseren Übersichtlichkeit in derselben Reihenfolge wie das vorhergehende Kapitel gehalten.

**Dumpster Diving**
Direkt an den Hochschulen, also in den öffentlich zugänglichen Mülleimern der Mensen, der Hörsäle oder der Gänge gestaltet sich die Anwendung von *Dumpster Diving* für einen Angreifer wenig Erfolg versprechend. Wichtige Dokumente werden meist an die Heimadressen der Studenten verschickt und anschließend auch nur in den seltensten Fällen mit in die Universität genommen, geschweige denn nur dort entsorgt. Vorstellbar wäre allerdings das Auffinden von Lösungen zu gestellten Aufgaben, die noch in der Universität bearbeitet wurden.
Differenziert zu betrachten ist die Situation für Mülleimer und -container der Hochschulmitarbeiter. Hier könnten durchaus sensible Daten im Abfall aufzustöbern sein. Vorstellbar sind verworfene Studienpapiere oder diverse andere Informationen über Studenten oder Anschreiben mit Adresse des Empfängers, bei denen Rechtschreibfehler aufgetreten sind. Auch sind fehlerhafte Schreiben wie Einladungen zu Kongressen, Ehrungen und Mitteilungen an kooperierende Firmen, die über den aktuellen Fortschritt eines Projekts informiert werden, eventuell aufzufinden. Besonders kritisch ist das unvorsichtige Wegwerfen von Klausuren oder derer Lösungen, die beispielsweise aufgrund von Papierstau oder Fehldruck unbrauchbar geworden, aber dennoch lesbar sind.
Dies kann nicht nur an den Universitäten, sondern auch bei den Arbeitsstellen von Privatdozenten der Fall sein. Oft haben diese keine Büros an den Hochschulen oder die Möglichkeit, Klausuren und Übungen, sowie die dazu gehörenden Lösungsvorschläge vor Ort auszudrucken. Demnach werden auch die Fehldrucke nicht in Mülleimern der Uni, sondern am Ort des Drucks entsorgt. So oder so würde ein Entdecken dieser Dokumente die Chancengleichheit aller Studenten beeinflussen.
Ebenso gefährlich kann das unsachgemäße Entsorgen von Passwortnotizen neuer Mitarbeiter oder geänderter Zugangsdaten einer Person sein. Hierbei ist darauf zu achten, nur weitestgehend unlesbare Kombinationen wegzuwerfen. Selbiges gilt für Notizen, die beispielsweise während eines vertraulichen Telefonats mit dem Service Desk entstehen. Der Anrufer sollte aus Eigeninteresse seine Bemerkungen zerstören und der Bearbeiter die ihm zugetragene Verantwortung nicht missbrauchen und ebenfalls die Notizzettel nur unkenntlich beseitigen.

**Shoulder Surfing**
*Shoulder Surfing* ist auch im MWN und Hochschulumfeld eine Gefahr. Grundsätzlich ist ein solcher Angriff an allen Plätzen der Universität möglich, an denen der Angreifer hinter einem Studenten Platz finden kann. Besonders einfach gestaltet sich ein Zugriff dieser Art bei großen Hörsälen, die treppenartig aufsteigen, um den Studenten der hinteren Reihen einen guten Blick Richtung Dozent zu ermöglichen. Der Aufbau eines solchen Auditoriums fördert *Shoulder Surfing* in großem Maße und verleitet den Hintermann geradezu zum Be-

obachten des Bildschirms des vor ihm Sitzenden. Denkbare Daten an die ein Angreifer im Hochschulumfeld per *Shoulder Surfing* gelangen will, können das Passwort für den Zugriff auf das MWN und die sich daraus eröffnenden Möglichkeiten, die Lösung für Aufgaben eines Übungsblattes oder sonstige Zugangsdaten für bestimmte Webseiten oder den Computer selbst sein.
Abbildung 3.1 zeigt einen Studenten, der seine Zugangsdaten auf der Login-Seite seines Bankinstituts eintippt.

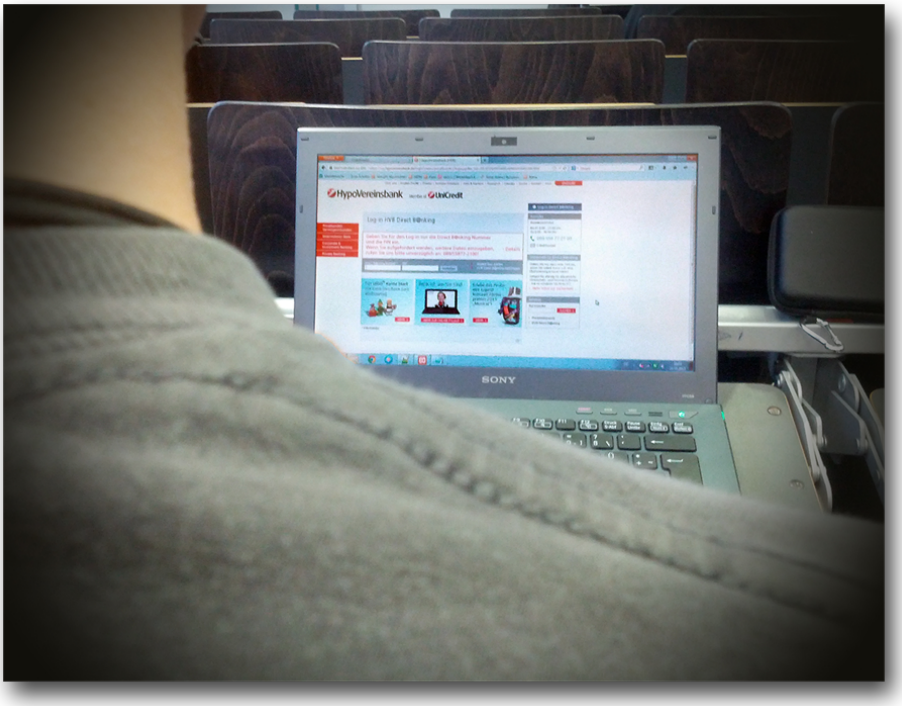



Abbildung 3.1: Shoulder Surfing im Hörsaal

**Tailgating**
Als Beispiel zu *Tailgating* im Hochschulumfeld ist hier die Zugangsbeschränkung der CIP-Pools der LMU für Studierende der Informatik zu nennen, konkret der CIP-Pool in der Amalienstraße. Dieser ist nur für Studierende der Medieninformatik zugänglich, da der Eingang mit einer Apparatur ausgestattet ist, die die Eingabe der richtigen Geheimzahl erfordert. Diese PIN[1] wird ausschließlich unter Studenten dieses Studiengangs kommuniziert. Trotz dieser Sicherheitsmaßnahme lassen sich immer wieder Studierende anderer Studiengänge identifizieren. Ihre Unkenntnis des PINs lässt darauf schließen, dass sie sich auf irgendeine andere Art und Weise Zutritt verschafft haben müssen. Augenscheinlich lässt sich dieser Umstand mit einer Art von *Tailgating* erklären. Nichtsdestotrotz kann hierbei von reinem *Tailgating* wohl nicht die Rede sein, da Medieninformatiker und Informatiker viele Lehrveranstaltungen gemeinsam haben und jene Medieninformatiker ihre unautorisierten Kommilitonen der Informatik wohlwissentlich mit in den Raum geleiten. Wesentlich gefährlicher wäre ein solcher Angriff bei Ermöglichung des Zutritts zu einem Gebäude mit deutlich interessanterem Inhalt,

[1] PIN – Persönliche Identifikationsnummer

wie beispielsweise dem Rechnergebäude des LRZ. Der dort ansässige Höchstleistungsrechner SuperMUC ist aufgrund seiner Möglichkeiten, potenter Ausstattung und des enormen (Geld-)Wertes ein weitaus schützenswerterer Gegenstand (Asset), als die Geräte der CIP-Pools. Dennoch ist *Tailgating* an den Computerräumen durchaus vorstellbar, da lediglich eine elektronische Authentifizierung am Eingang zur Sicherheit beiträgt. Auch andere Angriffe, wie zum Beispiel *Badge Surveillance* für *Electronic Badges* (siehe Kapitel 2.2.4) sind hierfür durchaus denkbar.

**Badge Surveillance**
Im Hochschulumfeld sind die Studentenausweise vor einer Kopie nicht gefeit. Damit könnte der Täter die Identität eines Studenten annehmen und für ihn beispielsweise Prüfungen absolvieren. Des Weiteren könnte er damit im Sekretariat möglicherweise neue Log-In-Daten oder gar die Exmatrikulation beantragen. Eine Vorlage kann sich der Angreifer entweder während einer Prüfung oder durch *Dumpster Diving* nach einem veralteten Ausweis aneignen. Dann hat er lediglich die Fachsemesteranzahl sowie das aktuelle Semester auf dem nachgemachten Dokument zu aktualisieren.

**Pretexting**
Auch im MWN ist ein solcher Angriff ernst zu nehmen. Der Täter könnte sich im direkten Kontakt mit dem Opfer als Netzwerkadministrator ausgeben und dessen Zugangsdaten verlangen, um angebliche Wartungsarbeiten am Postfach durchführen zu können. Ist sein Ziel ein Student, so kann er unter Vorwand der Exmatrikulation ein geeignetes Druckmittel schaffen, um die gewünschten Informationen zu erhalten.
Eine weitere denkbare Umsetzung von *Pretexting* ist ein Anruf beim Service Desk des LRZ unter Vorgabe einer falschen Identität. Hier kann der Angreifer durch geschickte Gesprächsführung Informationen über sein Ziel oder andere sensible Daten in Erfahrung bringen.

**Quid pro quo**
Ein derartiger Angriff ist im Hochschulumfeld recht leicht umzusetzen. Hier ist von größerer Relevanz, welche Informationen vom Angreifer als interessant angesehen werden. Insbesondere Lösungen zu Übungsblättern, Hochschulkennung und -passwort, folglich der Zugang zum MWN, PIN-Code der CIP-Pools und persönliche Informationen gilt es in Erfahrung zu bringen. Als Gegenleistung könnten umgekehrt auch bereits ausgefüllte Blätter zu Hausarbeiten angeboten werden.

**People Watching**
Eine solche Attacke ist im Hochschulumfeld jederzeit zu befürchten. Zunächst wird der Täter versuchen, bei den beobachteten Personen zwischen Studenten und Mitarbeitern der Universität zu unterscheiden. Dies lässt sich entweder anhand der Einschätzung des Alters, der Kleidung oder durch Verfolgung des Objekts herausfinden. Sollte sich die Person etwa in ein Büro begeben, weiß man im Anschluss aufgrund des Türschilds höchstwahrscheinlich sogar den Namen. Eine Internetsuche mit Angabe des Namens könnte anschließend Aufschluss über den Ausbildungsstand, die Fachrichtung und die Forschungsarbeiten geben. Sollte sich die Person allerdings in einem Hörsaal einen Platz suchen, so lässt sich durch die Analyse des Vorlesungsplans vor der Räumlichkeit der Name des Professors und nach einer Recherche dessen Fachbereich und somit das Studienfach des Ziels ausmachen. Mit diesen Informationen kann der Täter entscheiden, ob sich die Anwendung eines weiteren Angriffs lohnt.

**Diversion Theft**
Dieser *Social-Engineering-Angriff* eignet sich weniger für Computerdaten, sondern eher für handfeste Wertgüter. Alleinstehend ist ein solcher Übergriff deshalb für das Hochschulumfeld nicht direkt gefährdend. Denkbar wäre hier, dass veraltete Geräte der Hochschule von einer Spedition abgeholt werden und nach dem Beladen vom Angreifer umgeleitet werden. Nachdem sich der Täter die Computer, Drucker oder ähnliche Gegenstände verschafft hat, kann er allerdings weitere Angriffe (zum Beispiel *Forensic Analysis*, 2.2.3) zur Auswertung der eventuell noch vorhandenen Daten verwenden, was dann eine unvergleichbar größere Gefährdung darstellt.

**Phishing E-Mail**
All die verschiedenen *Phishing-Angriffe* sind auch im MWN denkbar. Derartige E-Mails lassen sich aber mit Hilfe von Spamfiltern[2] entdecken und blockieren, wodurch ein Großteil unter anderem durch die Filterung des LRZ nicht bis zu den Endanwendern, den Hochschulmitarbeitern und Studenten weitergeleitet wird. Bedauerlicherweise gibt es dennoch genügend Nachrichten, die ihren Weg bis zum Ziel schaffen. Der Angreifer kann hier sein Augenmerk beispielsweise speziell auf die Bankdaten von Professoren richten und eine *Phishing-Mail* im Namen einer Stiftung versenden, welche dem Dozenten eine Auszeichnung und Preisgeld zukommen lassen möchte. Hierzu fordert er den Lehrenden auf, seine Daten anzugeben. Ein weiteres lohnendes Ziel können bei einem solchen Angriff die LRZ-Kennungen von Studenten oder Hochschulmitarbeitern sein. Unter dem Vorwand, es hätten Angriffe auf Benutzerkonten stattgefunden und alle wären als Vorsichtsmaßnahme abgeschaltet worden, erbittet der Angreifer die Angabe von Kennung und Passwort, um die Identität des Nutzers kontrollieren und die Reaktivierung vornehmen zu können.

**Vishing**
Zur Umsetzung von *Vishing* im Hochschulumfeld sei folgendes Szenario gegeben:
Um die Gesamtzahl der Studenten zu erfassen, verlangt der Angreifer im Namen des Hochschulsekretariats in einer Mail Rückmeldung und droht mit einer Exmatrikulation, sollte diese nicht binnen einer vorgeschriebenen Frist erfolgen. Als Nummer hinterlegt er den Anschluss eines *IVR*. Ruft ein Student dort an, wird er nach Geburtsdatum, Matrikelnummer, Studienfach und -semester sowie seiner Hochschulkennung und dem passenden Kennwort gefragt. Folgen die Studenten dem Aufruf, so hat der Angreifer anschließend meist genug Informationen, um sich als einer von ihnen auszugeben. Die Kombination aus Hochschulkennung und dem zugehörigen Passwort ist für den Täter auch der Schlüssel zum MWN, wo er auf weitere Ressourcen zugreifen kann, was sowohl für den Studierenden, als auch für die Hochschule negative Folgen haben kann.

**Evil Twin**
Im MWN gibt es, wie bereits erwähnt die beiden SSID's „eduroam“und „lrz“. Auch bei diesen zwei WLAN's ist ein *Evil Twin Angriff* denkbar. Einfacher gestaltet sich eine Attacke auf das Eduroam-Netz, da kein VPN-Client für den Internetzugang notwendig ist und somit auch problemlos alle internetfähigen Mobilgeräte angegriffen werden können. Ebenfalls ist die Erstellung eines *Evil Twin* für diese Verbindung lukrativer, da dieser international wiederverwendet werden kann und mehr Nutzer als das lokale LRZ-Netz betrifft. Der Angreifer muss sich dazu in das Verbreitungsgebiet des entsprechenden Netzes begeben und

[2] Spam – unerwünschte (Werbe-)Mails

danach sein falsches Netz in Betrieb nehmen. Da schon bei der Authentifizierung Benutzername und Kennwort des Studenten angefordert werden, können sowohl diese Daten, als auch der spätere Internetverlauf (mit eventuellen Logins) als Angriffsziel gesehen werden. Abbildung 3.2 zeigt die Übersicht verfügbarer Drahtlosnetzwerke, wenn ein *Evil Twin* für das Eduroam-Netz erstellt wurde.

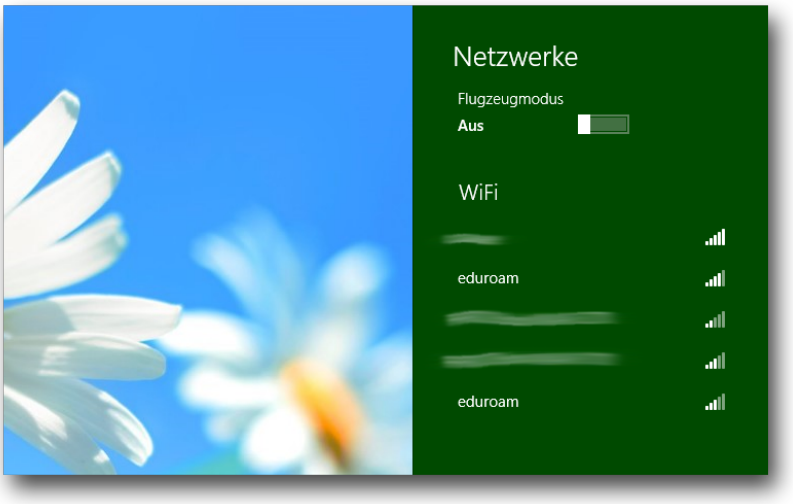



Abbildung 3.2: Auf den ersten Blick ist nur die Empfangsqualität als Unterschied erkennbar

**Baiting**

Im Hochschulumfeld ist ein solcher Angriff zweifellos durchführbar. Studenten würden den kostenlosen, an geeigneter Stelle platzierten USB-Stick oder ein ähnliches Speichermedium mit nach Hause nehmen und dort auch verwenden. Mögliche Orte für die Platzierung der Speichermedien sind die Bibliotheken, Cafeterien, Hörsäle und sonstige Räumlichkeiten der Universitäten. Der Vorteil dieser Lokalitäten ist, dass sie meist fakultativ unterscheidbar sind und die Schadsoftware gezielt unter einer bestimmten Zielgruppe verbreitet werden kann. Auch die Tische und Sitzgelegenheiten in den Gängen eignen sich hervorragend, allerdings ist dort eine kontrollierte Aufnahme durch Studenten bestimmter Fachrichtungen nahezu unmöglich. Der Einfluss auf die gewünschte Zielgruppe ist aufgrund der in Erfahrung zu bringenden Informationen sehr wichtig. So wird der Computer eines Professors interessantere Dateien und Zugriffsrechte enthalten, als der eines Studenten. Dementsprechend erscheint es für den Angreifer zweckmäßiger, das Speichermedium eher auf dem Schreibtisch oder dem Sprechpult des Dozenten zu platzieren, als auf den Hörsaalrängen.

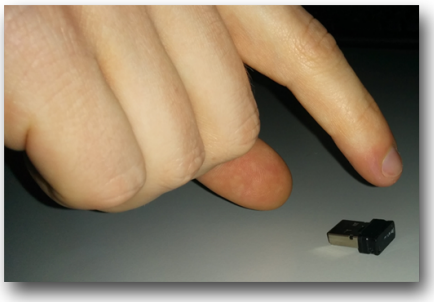


Abbildung 3.3: die unüberlegte Mitnahme eines USB-Sticks aus den CIP-Pools kann verheerende Folgen haben

**Forensic Analysis**
Auch im Hochschulumfeld können nicht mehr verwendete und abzugebende Geräte zur Gefahr werden. Beispielsweise speichern Drucker abgegebene Druckbefehle und deren Umfang im internen Speicher. Bei einem Verkauf kann es daher ohne vorherige Löschung der hinterlassenen Daten zu Problemen bei der Geheimhaltung sensibler Dokumente kommen. Dies gilt auch für ehemals benutzte PC's, CD's und andere Speichermedien.

**Electronic Badges**
Hier sei das Szenario eines Studenten mit Nebenerwerb betrachtet. Gerne werden in Firmen oder Behörden *Electronic Badges* zur Authentifizierung und Zutrittsberechtigung verwendet und deswegen auch an den dort angestellten Studenten ausgegeben. Meist lassen sich Arbeit und Studium am selben Tag vereinbaren, was dazu führt, dass der Studierende seinen Zugangsschlüssel auch bei Veranstaltungen an der Hochschule bei sich hat. Der Angreifer kann nun im Hörsaal, in der Mensa oder auf den Gängen der Universität, je nachdem, wo sich die Möglichkeit bietet, den Tag auslesen.

**Reverse Social Engineering**
Eine Umsetzung von *Reverse Social Engineering* in das Hochschulumfeld bedarf keiner großen Veränderung des allgemeinen Beispiels. Der Angreifer kann sich am Campus der Universität als Service-Desk-Mitarbeiter des LRZ oder einer betreuenden Organisation vorstellen und Visitenkarten mit seinen Kontaktdaten verteilen. Ebenso könnte er seine Dienste im Forum „die-informatiker.net“ anbieten. In beiden Fällen weist er explizit auf seine Spezialkenntnisse hin, die bei dem später von ihm initiierten Problem gefragt sind. Nachdem er eine Dysfunktion an den Rechnern der Studenten herbeigeführt hat, kann er ihnen nach Kontaktaufnahme ihrerseits sensible Informationen, die angeblich zur Lösung des Problems beitragen, entlocken.

Wie in den vorhergehenden Ausführungen beschrieben, kann jeder in Kapitel 2 erläuterte Angriff in einer beliebigen Form im universitären Alltag stattfinden. Nachdem nun alle Angriffe sowohl allgemein, als auch speziell für das Hochschulumfeld ausreichend erklärt wurden, wird im nächsten Kapitel die Kategorisierung des *Social Engineering* behandelt.

# 4 Kategorisierung – Klassifizierung

Dieses Kapitel widmet sich der Erstellung einer Kategorisierung für *Social-Engineering-Angriffe* im Hochschulumfeld. Hierzu müssen zunächst charakteristische Merkmale und deren Ausprägungen bestimmt werden. Danach folgt die Erklärung des Namensschemas und die Klassierung aller Angriffe. Anschließend wird überprüft, ob die entstandene Kategorisierung den Ansprüchen einer Taxonomie genügt und was eventuell dafür getan werden muss. Nach Klärung dieser Frage werden – sofern vorhanden – die unbelegten Klassen der Kategorisierung hinsichtlich ihrer Notwendigkeit begutachtet. Zuletzt werden verschiedene Visualisierungen für die Klassifizierung entworfen und miteinander verglichen.

## 4.1 Merkmalsbestimmung

In diesem Abschnitt werden relevante Merkmale der Angriffe und deren Wertebereiche identifiziert. Dabei soll sich vor allem herausstellen, welche der beschriebenen Attacken Ähnlichkeiten in gewissen Bereichen aufweisen. Dadurch wird ein Überblick über den Zusammenhang des *Social-Engineering-Feldes* geschaffen, der die anschließende Erstellung der Kategorisierung unterstützen soll. Die Ergebnisse werden zum Schluss anschaulich in Form einer Tabelle aufbereitet. Durch das Zusammenspiel der gewählten Merkmale entsteht für jeden Angriff ein charakteristischer Stempel, der die eindeutige Zuordnung in eine Klasse zulässt.

### 4.1.1 Merkmale

Bei einer Kategorisierung soll möglichst die Verwandtschaft unterschiedlicher Angriffe anhand gleicher Eigenschaften ersichtlich sein. Jeder *Social-Engineering-Angriff* besitzt eine Vielzahl an Merkmalen, die seinen Charakter bestimmen. Deren Kombination ist meist einzigartig und stellt den Angriff in seinen elementaren Teilen dar. Um die Merkmale identifizieren zu können stellt man einige Fragen an die Angriffsbeschreibung:

| | |
|---|---|
| Welcher Gattung gehört der Angriff an? | *Art* |
| Ist zwischenmenschlicher Kontakt nötig? | *Kontakt* |
| Was soll beschafft oder erreicht werden? | *Ziel* |
| Wer soll geschädigt werden? | *Opfer* |
| Wo findet die Attacke statt? | *Ort* |
| Wie auffällig ist der Angriff? | *Auffälligkeit* |
| Was muss der Angreifer vorher wissen? | *Vorkenntnisse* |
| Wie bereitet sich der Angreifer vor? | *Informationsbeschaffung* |
| Wie aufwändig ist die Vorbereitung? | *Vorbereitungsaufwand* |
| Ist der Angreifer aktiv beteiligt? | *Beteiligung* |

| | |
|---|---|
| Welche menschliche Schwäche wird ausgenutzt? | *Schwäche* |
| Welche Hilfsmittel werden verwendet? | *Hilfsmittel* |
| Ist der Angriff im Hochschulumfeld umsetzbar? | *Umsetzbarkeit* |
| Wie gefährdet ist das Hochschulumfeld? | *Gefährdungsgrad* |

Um in den kommenden Abschnitten die Verwandtschaft von Attacken feststellen zu können, ist es sinnvoll, die ausschlaggebenden Eigenschaften auf einige wenige zu reduzieren und deren Menge an Ausprägungen so klein wie möglich zu halten. Beispielsweise können Merkmale, die von anderen Merkmalsausprägungen abhängig sind, wie die Auffälligkeit (abhängig von Kontakt), der Vorbereitungsaufwand und die Informationsbeschaffung (beide abhängig von Vorkenntnisse) oder der Gefährdungsgrad (abhängig von Umsetzbarkeit) eingespart werden. Die Beteiligung eines Angreifers bei einer Attacke ist von der Ausprägung des Kontaktes abhängig. Besteht Kontakt mit dem Opfer, so greift der Angreifer unweigerlich in das Geschehen ein und wird somit aktiv. Wie Kapitel 3.2 zeigt, ist jeder der betrachteten Angriffe im Hochschulumfeld umsetzbar, weswegen auch der Gefährdungsgrad für die Kategorisierung keine Bedeutung hat. Ebenfalls uninteressant in Bezug auf die Klassifikation ist ein eventuell verwendetes Hilfsmittel, da für computerbasierte Angriffe generell eine Recheneinheit verwendet wird und die anderen Angriffsarten gegebenenfalls nur kleinere Gadgets zu Hilfe nehmen, welche allerdings für die einzelnen Angriffe nicht charakteristisch sind. Zudem ist die ausgenutzte Schwäche wenig aussagekräftig, da alle Attacken in irgendeiner Form die Gutgläubigkeit oder die Naivität eines Menschen missbrauchen. Irrelevant sind außerdem die Vorkenntnisse eines Angreifers, die er für eine bestimmte *Social-Engineering-Technik* benötigt, da diese nicht bezeichnend für die Attacke sind.
Abbildung 4.1 zeigt den kompletten Umfang der hier identifizierten Eigenschaften eines Angriffs, sowie die bisher genannten Abhängigkeiten (grün markiert) und die für die Kategorisierung irrelevanten Merkmale (rot markiert). Eingehende Pfeile zum Angriff symbolisieren, dass die Ausprägungen jener Merkmale zur Ausführung der Attacke von Nöten sind. Ausgehende Pfeile erschließen die Eigenschaften, die von der Ausführung eines Angriffs bestimmt werden. Merkmale, auf die eingehende Pfeile zeigen, sind von der Ausprägung des Merkmals am anderen Ende abhängig.

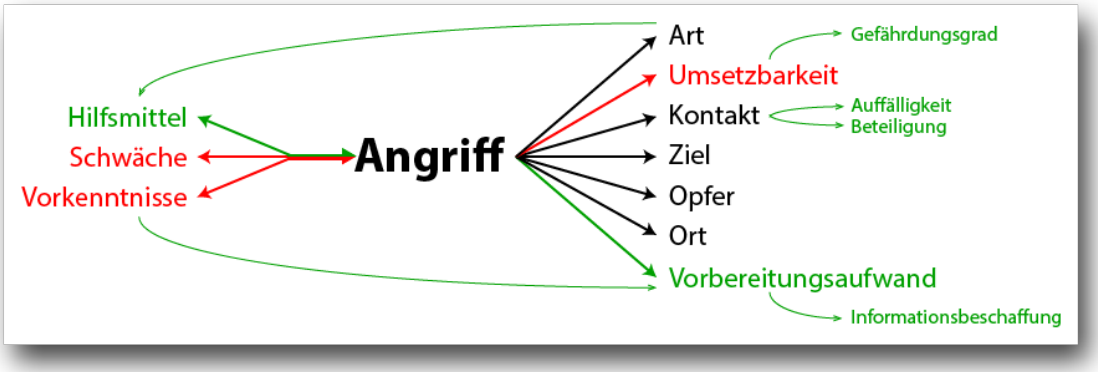
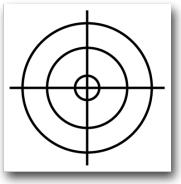



Abbildung 4.1: Beziehungen zwischen Angriff und Merkmalen mit genannten Abhängigkeiten (grün) und für die Kategorisierung unbedeutenden Eigenschaften (rot)

Die übrigen Eigenschaften der Angriffe charakterisieren die Durchführung einer Attacke und sollen daher der Erstellung der Kategorisierung zu Grunde liegen. Nachfolgend werden sie genauer erläutert und ihre möglichen Ausprägungen erklärt.

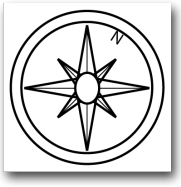
**Art:**
Bei der *Art* eines *Social-Engineering-Angriffs* sind folgende Ausprägungen möglich: *Human Based*, *Computer Based* oder *Reverse*. Die Unterschiede der Arten sowie die korrekte Einteilung der Attacken wurde bereits in Kapitel 2 geklärt.

**Kontakt:**
Als *Kontakt* wird jede Form von Kommunikation zwischen Täter und Opfer bezeichnet. Für die Einsortierung in die Kategorisierung wird dabei allerdings keine Unterscheidung von direktem, persönlichem oder Kontakt über ein Medium wie Internet oder Telefon beachtet. Die Berücksichtigung dieses Gesichtspunktes ist zwar essentiell für die Erklärung und Differenzierung verschiedener Angriffe, was jedoch die Klassierung von Attacken erschwert, da zu viele unterschiedliche Ausprägungen vorhanden sind. Als Werte sind demnach lediglich „Voraussetzung“ oder „unnötig“ sinnvoll.



**Ziel:**
*Ziele* sind Informationen, Gegenstände oder Angaben, auf die es der Täter durch seinen Angriff abgesehen hat. Mögliche Ausprägungen für dieses Merkmal sind einerseits sensible Daten und andererseits Zugriff oder Zutritt zu einem gesperrten Bereich. Sensible Daten sind beispielsweise persönliche oder firmeninterne Dokumente sowie vertrauliche E-Mails. Unter Zugriff oder Zutritt zu einem gesperrten Bereich versteht man die Zutrittsberechtigung zu einer Lokalität und unter anderem Login-Daten, da dadurch der Zugriff auf sensible Daten möglich wird.


**Opfer:**
*Opfer* sind Personen oder Unternehmen, denen der Angriff gilt und die durch einen Angriff geschädigt werden sollen. Im hier betrachteten Rahmen kann dies entweder eine Privatperson oder die Universität als Ganzes sein.



**Ort:**
Das selbsterklärende Merkmal, der *Ort* zeigt auf, wo eine Attacke meist stattfindet. Als Werte sind „spezieller Platz“ , oder „irrelevant“ festgelegt. Dies soll eine mögliche weite Streuung dieses Merkmals vermeiden. Unter „spezieller Platz“ ist entweder das Unigelände, der Arbeitsplatz oder ähnliches, wie beispielsweise die Nähe zum Opfer, auch wenn dies in der Öffentlichkeit wäre, zu verstehen. Die Ausprägung „irrelevant“ trifft genau dann zu, wenn der Täter an keinen Ort gebunden ist, was zum Beispiel beim Senden einer *Phishing-Mail* oder bei einem Übergriff via Telefon der Fall ist.

### 4.1.2 Tabellarischer Überblick

Nachdem nun die verschiedenen Merkmale der *Social-Engineering-Attacken* erklärt wurden, werden die einzelnen Angriffe beurteilt und das Resultat in Form einer Tabelle dargestellt. Die einzelnen Ausprägungen der Merkmale werden abstrahiert mit Farben dargestellt, um die Übersichtlichkeit der Tabelle zu wahren. Die Erklärung der Bedeutung der einzelnen Farben findet sich hier:

| Farbe | Art | Kontakt | Ziel | Opfer | Ort |
|---|---|---|---|---|---|
| Grün | Human Based | Voraussetzung | Zugriff/Zutritt | Privatperson | spezieller Ort |
| Gelb | Computer Based | – | – | – | – |
| Rot | Reverse | unnötig | sensible Daten | Universität | irrelevant |

Tabelle 4.1: Erklärung der Farbgebung

| Angriff | Art | Kontakt | Ziel | Opfer | Ort |
|---|---|---|---|---|---|
| Dumpster Diving | | | | | |
| Shoulder Surfing | | | | | |
| Tailgating | | | | | |
| Badge Surveillance | | | | | |
| Pretexting | | | | | |
| Quid pro quo | | | | | |
| People Watching | | | | | |
| Diversion Theft | | | | | |
| Phishing-E-Mails | | | | | |
| Vishing | | | | | |
| Evil Twin | | | | | |
| Baiting | | | | | |
| Forensic Analysis | | | | | |
| BS – Electronic Badges | | | | | |
| Reverse Social Engineering | | | | | |

Tabelle 4.2: anschauliche Darstellung der einzelnen Merkmalsausprägungen der *Social-Engineering-Angriffe*

Wie in Tabelle 4.2 zu sehen ist, gibt es bei beinahe jedem Angriff für einzelne Merkmale mehrere Ausprägungen. Dieser Umstand rührt daher, dass ein und dieselbe Attacke verschiedenste Ausführungsmöglichkeiten bietet, aber durch die gleichen Grundcharakteristika eine Einheit darstellt. Dadurch kann bei der Klassenidentifikation und der anschließenden Einsortierung der Angriffe das Problem entstehen, dass eine Attacke mehreren Klassen zugeordnet werden kann. Um dies zu vermeiden und eine eindeutige Klassierung zu gewährleisten, wird jede Attacke, bei der unterschiedliche Ausführungen vorhanden sind, in entsprechend viele Möglichkeiten unterteilt.

Bei den meisten Angriffen ist vor allem das Opfer nicht genauer definiert, da sie sowohl einer Privatperson als auch der Universität gelten können. Die Vorgehensweise bleibt weitestgehend gleich, mit dem Unterschied, dass die Attacke auf eine Hochschule über die Schwäche

eines Mitarbeiters oder Studenten erfolgt, da eine Einrichtung selbst nicht direkt angreifbar ist. Problematisch ist hierbei, dass keine Konkretisierung des Merkmals möglich ist, außer ein Angriff gilt ausschließlich einer Universität. Generell kann man sagen, dass der Schaden eines Angriffs immer für oder durch eine Person entsteht. So ist eine weitere Betrachtung dieses Merkmals unnötig, da die Ausprägung für die Kategorisierung nicht relevant ist. Die Auswirkungen dieses Schrittes werden in Abschnitt 4.1.3 genauer behandelt.

Beim *Baiting* (Abschnitt 2.2.2) kann neben dem Opfer auch der Ort differieren. Richtet sich der Angriff gegen eine bestimmte Person, so ist der Ort speziell. Gleiches gilt für den Fall, wenn *Baiting* gegen eine Hochschule oder eine Einrichtung verwendet wird. Ansonsten kann es passieren, dass das eigentliche Opfer nicht „getroffen“ wird. Ist dem Angreifer aber das Ziel wichtiger als ein ausgewähltes Opfer, ist der Ort nicht mehr entscheidend, da die Attacke demnach überall stattfinden kann. Das heißt, *Baiting* wird in zwei Teilbereiche aufgespalten, welche entsprechend mit „an speziellem/beliebigem Ort“ erweitert werden.

| | |
|---|---|
| Baiting | Baiting an speziellem Ort |
| | Baiting an beliebigem Ort |

Da *Baiting* jedoch sowohl zum Ausspähen sensibler Daten als auch zum Herausfinden von Zugangsdaten verwendet werden kann, werden die soeben neu entstandenen Angriffsvarianten weiter gesplittet. Selbiges gilt für *Vishing* (Abschnitt 2.2.1) und *Evil Twin* (Abschnitt 2.2.1). Auch *Pretexting* (Abschnitt 2.1.5) und *Quid pro quo* (Abschnitt 2.1.6) lassen sich deswegen jeweils in zwei weitere Möglichkeiten aufteilen. So ist es möglich, bei einer Privatperson, egal ob diese gezielt angegriffen wurde oder nicht, an Zugriffsdaten, wie beispielsweise den MWN-Zugang oder Online-Dienste und sensible Daten, wie Dokumente oder Klausurergebnisse, zu gelangen. Bei Organisationen des Hochschulumfelds sind der Zutritt zu gesperrten Bereichen und die Studentendaten durch solche Attacken gefährdet. Der Unterschied zu den Angriffsvarianten von *Baiting*, *Vishing* und *Evil Twin* liegt darin, dass kein Computer zur Durchführung der Attacke benötigt wird. Es wird direkt mit dem Opfer kommuniziert, was zur Folge hat, dass nicht wie bei den computerbasierten Angriffen weitere Schritte zur eigentlichen Informationsgewinnung durchgeführt werden müssen. Die jeweiligen Bezeichnungen werden um die Zusätze „zugriffsgerichtet“ und „datengerichtet“ erweitert.

| | |
|---|---|
| Pretexting | zugriffsgerichtetes Pretexting |
| | datengerichtetes Pretexting |
| Quid pro quo | zugriffsgerichtetes Quid pro quo |
| | datengerichtetes Quid pro quo |
| Vishing | zugriffsgerichtetes Vishing |
| | datengerichtetes Vishing |
| Evil Twin | zugriffsgerichteter Evil Twin |
| | datengerichteter Evil Twin |
| Baiting an speziellem Ort | zugriffsgerichtetes Baiting an speziellem Ort |
| | datengerichtetes Baiting an speziellem Ort |
| Baiting an beliebigem Ort | zugriffsgerichtetes Baiting an beliebigem Ort |
| | datengerichtetes Baiting an beliebigem Ort |

Des Weiteren ist *Tailgating* (Abschnitt 2.1.3) in zwei Teilbereiche aufzuspalten, da in diesem Fall der zwischenmenschliche Kontakt nicht zwingend ist. Dieser Angriff wird daher entweder als „aktiv“ bei bestehendem Kontakt oder „passiv“ bei *Tailgating* ohne Kontakt bezeichnet.

| | |
|---|---|
| Tailgating | aktives Tailgating |
| | passives Tailgating |

### 4.1.3 Generalisation der Kategorisierung

Ziel dieser Arbeit soll sein, eine Kategorisierung von *Social-Engineering-Angriffen* im Hochschulumfeld zu erstellen. Durch die in Abschnitt 4.1.1 und 4.1.2 begründete Konzentration auf die Merkmale *Art*, *Kontakt*, *Ziel* und *Ort* entfällt allerdings die Konkretisierung des Schemas auf das Hochschulumfeld. Demnach gilt es zu prüfen, ob und wie sich das hier definierte Hochschulumfeld von normalen Unternehmen unterscheidet. Wird ein solches Verhalten festgestellt, so muss eine genauere Differenzierung dieser beiden Bereiche in der Kategorisierung ersichtlich gemacht werden.

Die Definition in Kapitel 3.1 stützt sich auf die drei Bereiche Menschen, Einrichtungen und Partnerunternehmen der Universitäten. Als angreifbare Individuen werden Studenten und Mitarbeiter aufgeführt, welche auch bei normalen Firmen so genannt werden können. Auch bei einem Unternehmen in der freien Wirtschaft dient das Personal als Ansatzpunkt eines *Social-Engineering-Angriffs*. Ebenso haben die einzelnen Mitarbeiter je nach Hierarchiestufe oder Abteilung unterschiedliche Zugriffs- und Zutrittsberechtigungen. Daneben besitzen, wie die Hochschulen, auch die meisten Betriebe Räumlichkeiten und Einrichtungen wie Sekretariate, Kantinen oder Besprechungsräume, die als Ort für einen Übergriff dienen können. Genauso ist hier die Konzentration auf eine Abteilung möglich, was mit den Fachrichtungen der Hochschulen vergleichbar ist. Der dritte angreifbare Bereich, die Partnerunternehmen, sind auch bei Firmen der freien Wirtschaft zu finden. Beispielsweise seien hier Zulieferer-, Reinigungs- oder Wartungsunternehmen genannt.

Die Ausführung zeigt, dass sich das Hochschulumfeld ohne weitere Probleme mit einem Unternehmen der freien Wirtschaft vergleichen lässt und beide, bezogen auf *Social Engineering*, dieselben Angriffspunkte besitzen. Demnach ist die entstandene allgemeine Kategorisierung durchaus auf das Hochschulumfeld zugeschnitten, aufgrund der Ähnlichkeit von einer Universität zur normalen Firma aber keine weitere Spezifikation notwendig.

## 4.2 Identifikation der Klassen

Im vorherigen Abschnitt wurden die ausschlaggebenden Merkmale sowohl erklärt, als auch für die verschiedenen Angriffe interpretiert. Weitergehend wurden die unterschiedlichen *Social-Engineering-Techniken* in eine Form gebracht, mit der die Erstellung einer Kategorisierung möglichst intuitiv durchführbar ist. Da alle Techniken hinsichtlich ihrer unterschiedlichen Merkmalsausprägungen aufgeteilt wurden, sind insgesamt 23 *Social-Engineering-Angriffe* entstanden. In den folgenden Absätzen werden die Zusammensetzung der Klassennamen beschrieben und, aufbauend auf Kapitel 4.1, die Angriffe in ihre Oberkategorien einsortiert.

### 4.2.1 Namensschema

Um die Klassennamen verständlich, aber nicht unverhältnismäßig kompliziert oder lang werden zu lassen, werden abstrakte Namen für das Schema erstellt. Diese bauen auf Abkürzungen der einzelnen Merkmalsausprägungen auf, welche in den Namen durch einen Unterstrich getrennt werden.
Die Reihenfolge der Charakteristika in den Klassennamen wird aufgrund folgender Beweggründe festgelegt: Als erstes wird die *Art* eines Angriffes bestimmt, da dieses Merkmal drei Ausprägungen besitzt und jeder Angriff eindeutig einer Kategorie zugeordnet werden kann, womit eine gute Vorsortierung möglich ist. Bei den weiteren Merkmalen ist zu erkennen, dass die Ausprägungen sowohl von *Kontakt* als auch von *Ort* gegensätzliche Spezifikationen haben. Dadurch ist das *Ziel* eines Angriffs weniger bestimmend und wird an die letzte Stelle gesetzt. Die beiden anderen Merkmale werden alphabetisch auf die zweite und dritte Position verteilt. Dadurch ergibt sich das folgende Musterbeispiel, welches als Vorlage für das Namensschema der einzelnen Kategorien dienen wird:

$$Klassenname = ART\_KONTAKT\_ORT\_ZIEL$$

Die Abkürzungen für die einzelnen Ausprägungen lauten wie folgt:

| | | |
|---|---|---|
| Art: | HB, CB, RE | – stehen je für Human Based, Computer Based oder Reverse |
| Kontakt: | VOR, UNN | – stehen je für Voraussetzung oder unnötig |
| Ort: | SPEZ, IRLV | – stehen je für spezieller Ort oder irrelevant |
| Ziel: | ZU, SD | – stehen je für Zutritt/Zugriff oder sensible Daten |

### 4.2.2 Klassierung der Angriffe

Nachdem nun das Schema der Klassennamen erklärt wurde, folgt die Einsortierung der *Social-Engineering-Angriffe* in die zutreffenden Kategorien. Daraus wird ersichtlich, welche Klassen für die Klassifikation zur Zeit von Nöten sind. Anschließend nicht belegte Klassen sind dahingehend zu untersuchen, ob sie für die zukunftssichere Gestaltung der Kategorisierung beibehalten werden, oder ihre Spezifikation unvereinbare Merkmale verlangt und sie somit komplett ausgeschlossen werden können.

Um die Klasse einer Attacke herauszufinden, wird jede mit Hilfe von Tabelle 4.2 und des gerade entstandenen Namensschemas einer Kategorie zugeteilt und aufgelistet.

| **Schema**: Angriff | → | `Klassenname` |
|---|---|---|
| Dumpster Diving | → | `HB_UNN_SPEZ_SD` |
| Shoulder Surfing | → | `HB_UNN_SPEZ_SD` |
| aktives Tailgating | → | `HB_VOR_SPEZ_ZU` |
| passives Tailgating | → | `HB_UNN_SPEZ_ZU` |
| Badge Surveillance | → | `HB_UNN_SPEZ_ZU` |
| zugriffsgerichtetes Pretexting | → | `HB_VOR_IRLV_ZU` |
| datengerichtetes Pretexting | → | `HB_VOR_IRLV_SD` |
| zugriffsgerichtetes Quid pro quo | → | `HB_VOR_IRLV_ZU` |
| datengerichtetes Quid pro quo | → | `HB_VOR_IRLV_SD` |
| People Watching | → | `HB_UNN_SPEZ_SD` |
| Diversion Theft | → | `HB_VOR_IRLV_ZU` |
| Phishing-E-Mails | → | `CB_VOR_IRLV_ZU` |
| zugriffsgerichtetes Vishing | → | `CB_VOR_IRLV_ZU` |
| datengerichtetes Vishing | → | `CB_VOR_IRLV_SD` |
| zugriffsgerichteter Evil Twin | → | `CB_UNN_SPEZ_ZU` |
| datengerichteter Evil Twin | → | `CB_UNN_SPEZ_SD` |
| zug. Baiting an speziellem Ort | → | `CB_UNN_SPEZ_ZU` |
| dat. Baiting an speziellem Ort | → | `CB_UNN_SPEZ_SD` |
| zug. Baiting an beliebigem Ort | → | `CB_UNN_IRLV_ZU` |
| dat. Baiting an beliebigem Ort | → | `CB_UNN_IRLV_SD` |
| Forensic Analysis | → | `CB_UNN_SPEZ_SD` |
| BS – Electronic Badges | → | `CB_UNN_SPEZ_ZU` |
| Reverse Social Engineering | → | `RE_VOR_IRLV_ZU` |

Berechnet man das *Reverse Social Engineering* mit nur einer Klasse, da es ja nur eine einzige Ausprägung gibt und dieses Teilfeld somit keiner weiteren Verfeinerung bedarf, entstehen durch das in Abschnitt 4.2.1 beschriebene Schema insgesamt 17 Klassen.

**Berechnung:** $2^N + 1 = 17$ *, mit N=Anzahl der Merkmale=4*

### 4.2.3 Untersuchung auf Taxonomie

Nachdem alle Angriffe bereits eindeutig einsortiert wurden, soll überprüft werden, ob diese Eindeutigkeit der Zuordnung eines Angriffs zu einer Klasse immer gewährleistet sein kann. Dieser Umstand ist die Spezifikation einer Kategorisierung, welche bei Erfüllung als Taxonomie bezeichnet werden kann. Bei einer Taxonomie muss sichergestellt sein, dass ein Angriff zweifellos in eine der gegebenen Klassen einzusortieren ist. Kann eine Attacke nicht eindeutig einer Kategorie zugeordnet werden und wird somit zwei oder mehreren zugewiesen, so ist das Schema keine Taxonomie. Um dies bei allen hier betrachteten *Social-Engineering-Techniken* zu verhindern, wurden Attacken, bei denen mehrere Merkmalsausprägungen vorhanden sind

und somit mehrere Klassen zuträfen, vorausschauend in einzelne Teilangriffe aufgesplittet. Dadurch konnten sie eindeutig einer Klasse zugeordnet werden. Wäre dieser „Sichtweisen-Trick“ nicht verwendet worden, so hätte ein Angriff nicht zwingend eindeutig einer einzigen Klasse zugeordnet werden können. Nur durch diese formelle Änderung stellt die hier entwickelte Kategorisierung auch eine Taxonomie dar, die in Zukunft so beibehalten werden kann.

Bei der Einsortierung der 23 *Social-Engineering-Angriffe* werden allerdings nur 12 der 17 entstandenen Klassen belegt, da manche davon mehrere Attacken beinhalten. Fünf der Klassen sind also ohne Angriff und es ist von Interesse, die Ursache dafür genauer zu untersuchen.

### 4.2.4 Analyse unbelegter Klassen

Folgende fünf Klassen werden von keinem der in den vorhergehenden Kapiteln identifizierten Angriffe belegt:

| | HUMAN BASED | | COMPUTER BASED |
|---|---|---|---|
| 1 | | | CB_VOR_SPEZ_ZU |
| 2 | HB_VOR_SPEZ_SD | | CB_VOR_SPEZ_SD |
| 3 | | HB_UNN_IRLV_ZU | |
| 4 | | HB_UNN_IRLV_SD | |

Tabelle 4.3: nicht belegte Klassen

Die sortierte Tabelle 4.3 zeigt sehr gut, welche Merkmale möglicherweise nicht zusammenpassen, was die Nicht-Existenz eines Angriffes mit dieser Kombination von Ausprägungen erklären könnte. Zusammenhängend betrachtet sind Zeile 1 und 2 der *Computer-Based-Techniken*, sowie 3 und 4 der *Human-Based-Techniken* interessant, da hier jeweils für keine der beiden Ausprägungen des Merkmals „Ziel“ Angriffe vorhanden sind. Separat ist Zeile 2 ein weiteres Mal zu analysieren, da hier weder bei *Human Based* noch bei *Computer Based Social Engineering* diese Kombination der Merkmale vorhanden ist. Die Analyse der in der Tabelle enthaltenen Klassen soll zeigen, ob sie für die Kategorisierung entbehrlich wären. Speziell wird versucht, bereits behandelte *Social-Engineering-Techniken* zu adaptieren und damit die Beibehaltung der Kategorien, unter anderem zur Zukunftssicherung der entstandenen Klassifikation, zu rechtfertigen.

Um die beiden unbesetzten Klassen der *Computer-Based-Techniken* mit einem bestimmten Angriff zu besetzen, muss dieser sowohl an einem speziellen Ort stattfinden, als auch der Täter bei der Ausführung mit dem Opfer in Kontakt stehen. Da das Ziel bei der Besetzung dieser Kategorien scheinbar irrelevant ist, da weder für Zutrittsinformationen noch für sensible Daten hier behandelte Angriffe vorhanden sind, wird dies in der Analyse nicht weiter betrachtet. Der Täter hat mit dem Opfer bei den betrachteten computerbasierenden Attacken meist in Form von E-Mail-Verkehr Kontakt. Da in Zeiten von Smartphones und Tablets das Schreiben der elektronischen Briefe von nahezu jedem Punkt der Erde möglich ist, spielt der Ort kaum eine

| COMPUTER BASED |
|---|
| CB_VOR_SPEZ_ZU |
| CB_VOR_SPEZ_SD |

Tabelle 4.4: betrachteter Abschnitt aus Tabelle 4.3

tragende Rolle und es gibt somit in diesem Betrachtungsraum keinen Angriff, der in die Klassen passt. Dies heißt allerdings nicht, dass keine solche Attacke denkbar ist. Die Überlegung, computerbasierende Techniken mit den Kontaktmedien Internet oder Telefon hier in Betracht zu ziehen, scheitert aufgrund der eben genannten Gegebenheiten. Demnach ist direkter, zwischenmenschlicher Kontakt von Nöten, um einen Beispielangriff zu skizzieren, der in die beiden Kategorien passt.
Für einen Angriff der Kategorie `CB_VOR_SPEZ_ZU` sei folgendes Szenario im Hochschulumfeld für das Erringen von Zutrittsinformationen gegeben: Der offiziell gekleidete Angreifer begibt sich mit einem Tablet oder einem ähnlichen Gerät auf eine Hochschulmesse. Er bietet dort ein angebliches Gewinnspiel an, für das man sich lediglich auf dem Gerät mit seinem Hochschulzugang anmelden muss. Das Gerät speichert jedoch neben dem Benutzernamen im Hintergrund auch das Passwort des „Teilnehmers“. Das Gewinnspiel kann hierbei sowohl fiktiv, als auch reell sein, was allerdings unnötigen Zusatzaufwand bedeuten würde. Die zweite Klasse wird im nächsten Absatz genauer betrachtet.

Eine weitere unbesetzte Klassengattung ist in Zeile `2` von Tabelle 4.3 zu finden. Auf Unstimmigkeiten zu überprüfen ist die Kombination der Merkmalsausprägungen Voraussetzung von Kontakt, sensible Daten als Ziel und ein spezieller Ort. Da diese Zusammenstellung sowohl bei menschenbasierenden, als auch bei computerbasierenden Angriffen keiner Attacke entspricht, sind diese Ausprägungen augenscheinlich auf keinen Nenner zu bringen. Auf der Seite von *Human Based* ist es denkbar, dass eine Attacke auf sensible Daten abzielt und mit zwischenmenschlichem Kontakt an einem speziellen Ort stattfindet. Für Attacken der Art *Computer Based* gelten weiterhin die zuvor genannten Probleme.
Um dennoch die Klassen füllen zu können, könnte eine Art von *datengerichtetem Pretexing* verwendet werden, soweit es an einem speziellen Ort stattfindet. Allerdings ist diese Attacke nicht ortsgebunden, da sie meist per Telefon durchgeführt wird. Eine Variante mit E-Mail aus dem Intranet oder einer internen Telefonnummer würde diesen Umstand verändern und somit die Kriterien der unbesetzten Klassen erfüllen. Eine frühere Aufteilung von *Pretexting* aufgrund der beiden möglichen Ausprägungen des Merkmals Ort ist nicht nötig, da die Ausführung dieses Angriffs in seiner üblichen Vorgehensweise keinen speziellen Platz benötigt.

| HUMAN BASED | COMPUTER BASED |
|---|---|
| HB_VOR_SPEZ_SD | CB_VOR_SPEZ_SD |

Tabelle 4.5: betrachteter Abschnitt aus Tabelle 4.3

Bereits die Analyse der ersten drei unbesetzten Klassen zeigt deutlich, dass durchaus Angriffe denkbar sind, die in die leeren Kategorien passen. Auch könnten zukünftige Angriffe oder auch Varianten bereits vorhandener Übergriffe in jene Kategorien einsortiert werden. Dies bedeutet, dass diese Klassen in der Kategorisierung bestehen bleiben müssen.

Zuletzt sind die *Human Based* Klassen zu analysieren, welche sich in Zeile `3` und `4` von Tabelle 4.3 befinden. Wie bei den vorherigen Abschnitten differiert auch hier nur eine Merkmalsausprägung. Somit besteht augenscheinlich eine Unstimmigkeit der Kombination von *Human Based*, keinem Kontakt und unbestimmtem Ort. Dieser Umstand lässt sich auch leicht nachvollziehen, da es für einen Angreifer sehr

| HUMAN BASED |
|---|
| HB_UNN_IRLV_ZU |
| HB_UNN_IRLV_SD |

Tabelle 4.6: betrachteter Abschnitt aus Tabelle 4.3

schwer sein wird, ohne technische Hilfsmittel und ohne Kontakt zum Opfer an einem beliebigen Ort sein Ziel zu erreichen. Naheliegend ist der Versuch, bereits einsortierte Angriffe derselben Klasse aus dem Computer-Based-Bereich zu übersetzen. Demnach soll eine Variation des *Baiting* ohne Computer oder USB-Stick gelingen, um die hier betrachteten Klassen zu füllen. Dies stellt sich allerdings ohne die Möglichkeiten elektronischer Geräte oder Kontakt als äußerst schwierig heraus. Als Szenario könnten Briefe, beziehungsweise Flugblätter vom Angreifer beliebig deponiert werden, die mit dem Empfänger „An alle Interessenten“ und einer auffälligen Aufschrift „100 %-ige Gewinnchance“, oder einem Äquivalent bedruckt sind. Um den versprochenen Preis zu erhalten, soll das Opfer einige Daten an den Angreifer auf dem Postweg zurückschicken. Dieses Beispiel beinhaltet jedoch eine Kontaktaufnahme in Form des Anschreibens und genügt daher nicht den Spezifikationen der zu belegenden Klassen. Auch die Übertragung von Angriffen ähnlicher Klassen in ein passendes Szenario ist nicht ohne Weiteres möglich. Die Beibehaltung dieser beiden unbelegten Klassen ist daher selbst hinsichtlich der Zukunftssicherheit nicht sinnvoll.

Nachdem nun der Ausschluss nicht besetzter Klassen von der Kategorisierung durch die Ausführungen lediglich teilweise vollzogen wurde, befinden sich noch 15 Klassen in der Kategorisierung. Im nächsten Kapitel soll nun eine passende Visualisierung der Klassifikation entstehen.

## 4.3 Visualisierung der Kategorisierung

Ziel dieses Kapitels ist es, eine gut leserliche und einfache Darstellung für die Kategorisierung zu finden. Vor allem wegen der großen Menge an Angriffen ist es sinnvoll, eine geeignete Visualisierung zur Übersicht zu entwickeln. Außerdem soll dadurch die Einsortierung zukünftiger Attacken oder neuer Angriffsvarianten unterstützt werden und intuitiv gelingen. Wie vorher berechnet sind insgesamt 15 Klassen in einer Grafik zu vereinen.

### 4.3.1 Baumstruktur

Die naheliegendste Variante der Darstellung ist ein Baum. Um einen noch nicht kategorisierten Angriff einzusortieren, bewegt man sich von Knoten zu Knoten, bis man an dem Blatt angekommen ist, an dem sich die dem Angriff entsprechende Klasse befindet. Als Wurzel für die hier entstandene Kategorisierung wird „Social Engineering“ gewählt. Die nachfolgenden Knoten beinhalten die jeweiligen Ausprägungen der Merkmale, zwischen welchen man sich bei der Klassierung eines Angriffs entscheiden muss. Das entstandene Diagramm zeigt Abbildung 4.3, wobei die unterschiedlichen Merkmale jeweils in einer einheitlichen Farbe dargestellt wurden, welche der Legende zu entnehmen ist.

Das Namensschema aus Abschnitt 4.2.1 hat in dieser Grafik keinen Platz gefunden, ein Muster ist in Form von Abbildung 4.2 zu sehen. Die einzelnen Attacken werden, wie ebenfalls Grafik 4.2 beispielhaft entnommen werden kann, als Blätter hinter der letzten Entscheidungsmöglichkeit eingefügt.

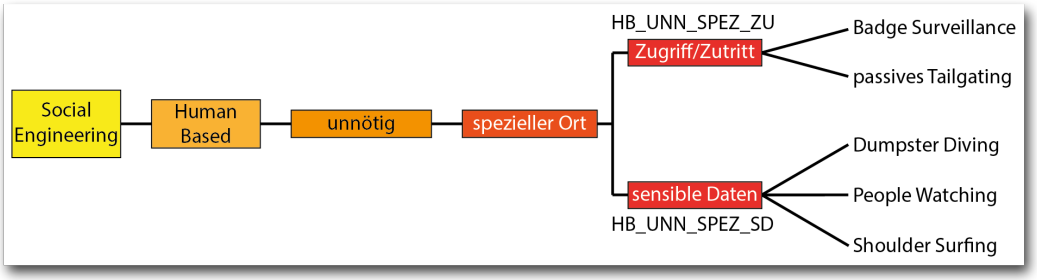



Abbildung 4.2: Teilast des Baumes
inkl. entsprechendem Namensschema und einsortierter Angriffe

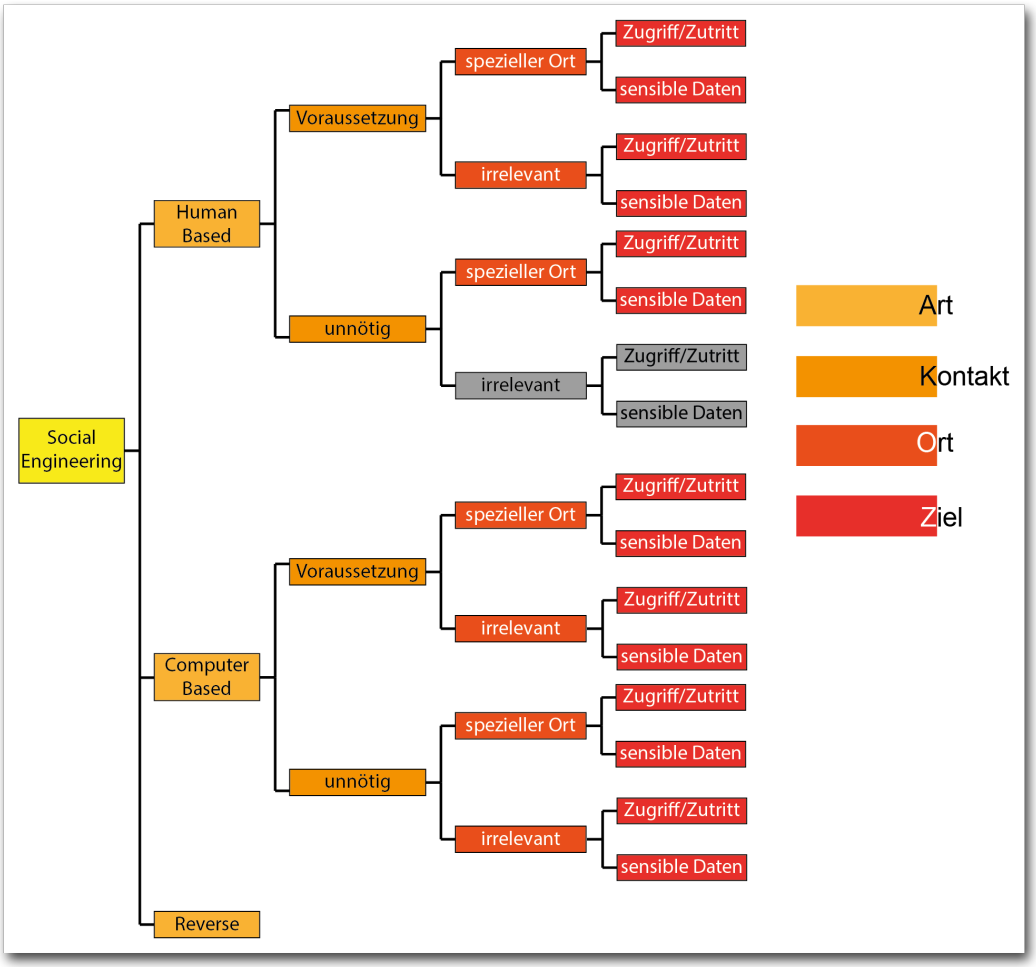



Abbildung 4.3: komplettes Baumdiagramm mit Legende rechterhand, ausgeschlossene Klassen sind nicht integriert

### 4.3.2 Kreisdiagramm

Als weitere Möglichkeit der Darstellung sei das Kreisdiagramm genannt. Um einer Entartung des Kreisdiagramms vorzubeugen, wird für jede Art des *Social Engineering* ein eigenes Diagramm gezeichnet, wodurch die Übersichtlichkeit der Darstellung gewährleistet wird.

Nachdem beim *Reverse Social Engineering* keine weitere Unterteilung vorgenommen wurde, gibt es auch im Diagramm lediglich einen einzigen Kreis, in den der Angriff einsortiert wird. Anders sieht es bei den beiden restlichen Ausprägungen des Merkmals *Art* aus. Sowohl für *Human Based*, als auch *Computer Based* gibt es einen Kreis je Merkmal. Somit enthalten die Diagramme für diese Arten drei Kreise, die sich überschneiden und damit die einzelnen Klassen formen. Befindet sich ein Angriff innerhalb eines Kreises oder einer Schnittmenge von Kreisen, so bedeutet das die „grüne“ Ausprägung eines Merkmals, wie sie in Tabelle 4.1 de-

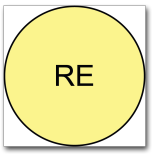



Abbildung 4.4: Kreis für den *Reverse-Angriff*

finiert wurde. Hat ein Angriff ausschließlich Ausprägungen, die nicht innerhalb eines Kreises festgelegt sind, so befindet sich diese Attacke außerhalb aller Kreise. Die genauen Positionen der einzelnen Klassen sind den Abbildungen 4.5 und 4.6 zu entnehmen. Um eine Vorstellung einer fertigen Darstellung zu bekommen, wurde das Diagramm der Art *Computer Based* mit den entsprechenden Angriffen gefüllt, was die Grafik 4.7 zeigt.

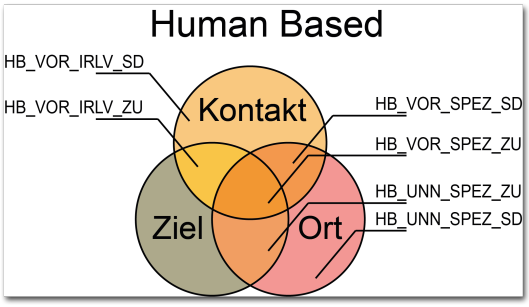



Abbildung 4.5: Kreisdiagramm für *Human-Based-Angriffe*, ausgeschlossene Klasse ist ausgegraut

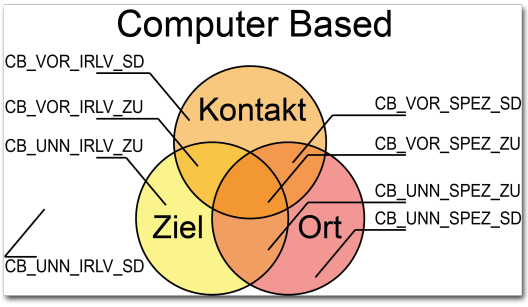



Abbildung 4.6: Kreisdiagramm für *Computer-Based-Angriffe*, keine ausgeschlossenen Klassen

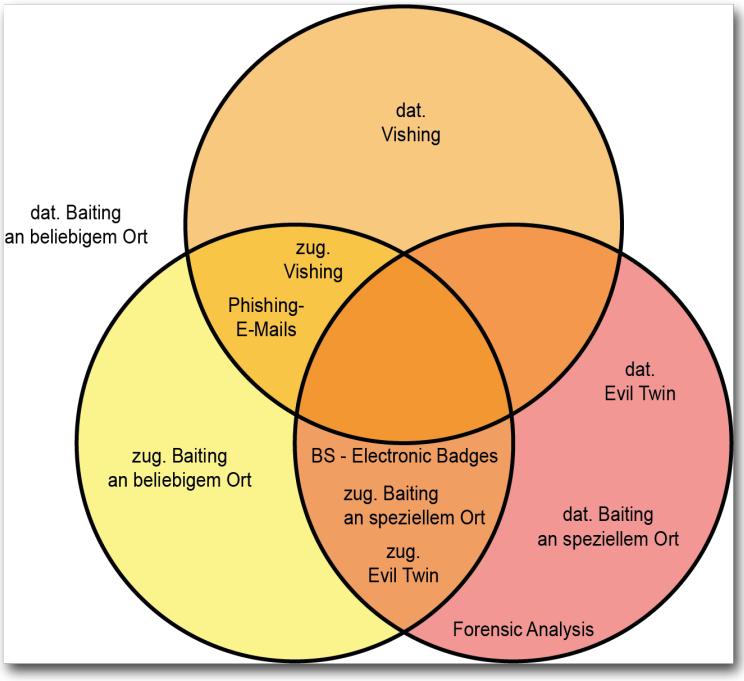



Abbildung 4.7: gefülltes Kreisdiagramm für *Computer-Based-Angriffe*

### 4.3.3 Netzstruktur

Eine Alternative zu den klassischen Diagrammen soll die folgende Ausführung zeigen, wobei sich jedoch die Vorgehensweise von den bereits vorgestellten Diagrammen etwas unterscheidet. Während man beim Baumdiagramm das Namensschema von links nach rechts abarbeitet und beim Kreisdiagramm nur darauf geachtet wird, dass nicht zu viele Kreise die Übersichtlichkeit stören, wird das Schema im Fall dieser Netzstruktur in umgekehrter Reihenfolge der Merkmale gelesen. Dadurch ist schlussendlich die richtige Anzahl an Unterscheidungs-Flächen für alle möglichen Klassen gewährleistet. Um die hier dargestellte Netzstruktur zu bekommen, folgt man einigen einfach aufgebauten Schritten, welche in Abbildung 4.8 zu sehen sind. Jedes Merkmal bekommt Achsen, die die einzelnen Ausprägungen voneinander trennen (Abb. 4.8/1-3). Abschnitt 1 der Grafik trennt den Kontakt, Abschnitt 2 den Ort und Abschnitt 3 das Ziel, wobei hier 2 Achsen notwendig werden, damit alle bereits entstandenen Klassen nach diesem Kriterium geteilt werden können. Bei dieser Kategorisierung ist es von Vorteil, dass nur das Merkmal *Art* mehr als zwei Ausprägungen besitzt, was sich am Ende mit Hilfe einer zusätzlichen Ebene anstatt einer weiteren Achse optimal realisieren lässt. Diese Dimension wird durch das Hinzufügen von Flächen dargestellt (Abb. 4.8/4). Abschnitt 5 der Grafik zeigt das leere, fertige Netz. Abbildung 4.9 stellt die für den darzustellenden Namensraum nötige Netzstruktur dar. Dort ist die innerste Fläche komplett für *Reverse Social Engineering* reserviert und wird daher nicht von den Achsen unterteilt.

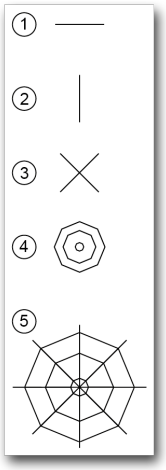



Abbildung 4.8: Evolution der Netzstruktur

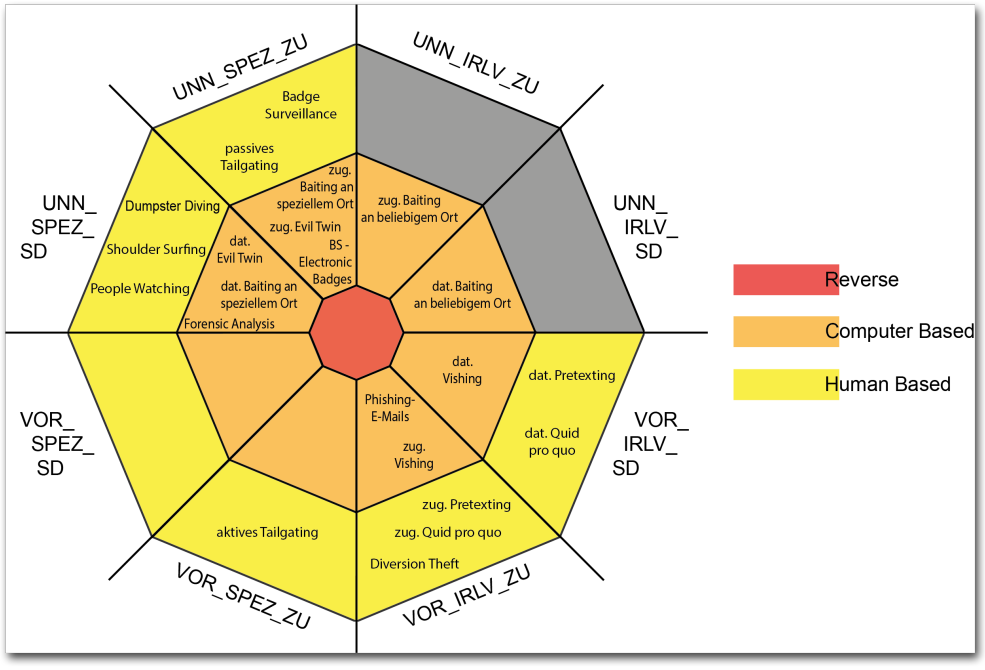



Abbildung 4.9: Darstellung der gefüllten Netzstruktur mit Legende rechterhand und an den Segmenten, ausgeschlossene Klassen sind ausgegraut

### 4.3.4 Binärcodierung

Bisher stützt sich jede Darstellung beziehungsweise die anschließende Einsortierung der Angriffe auf das hier entwickelte Namensschema. Um das gesamte Feld des *Social Engineering* erfassen zu können, wäre die internationale Verwendbarkeit der Kategorisierung wünschenswert. Da jede Attacke so aufgesplittet wurde, dass nur eine einzige Klasse auf sie zutrifft und drei der vier Merkmale ausschließlich zwei Ausprägungen haben, ist die Umsetzung der kompletten Kategorisierung in eine binäre Codierung zur Erreichung dieses Ziels denkbar. Durch die Darstellung der Klassen als Binärzahlen muss jede teilnehmende Nation lediglich einmalig die Merkmale und deren Ausprägungen korrekt übersetzen, sowie mit denselben binären Werten belegen. Die Codierung soll im folgenden Abschnitt geschehen.

Als Grundlage wird Tabelle 4.1 verwendet und die Farben mit Binärzahlen substituiert. Beim Merkmal *Art* tritt das Problem auf, dass mehr als zwei Ausprägungen vorhanden sind, was eine einstellige binäre Darstellung verhindert. Um diesen Konflikt aufzulösen, werden die ersten zwei Stellen der späteren Codierung für dieses Merkmal verwendet und zusätzlich mit einem Bindestrich von den anderen Ziffern getrennt. Außerdem wird das in der referenzierten Tabelle noch berücksichtigte Merkmal *Opfer* ebenfalls in der Binärcodierung nicht mehr betrachtet. Die fertige Übersetzung ist der folgenden Tabelle zu entnehmen:

| Merkmal | Ausprägung | Binärzahl |
|---|---|---|
| Art | Human Based | 00 |
| | Computer Based | 01 |
| | Reverse | 10 |
| Kontakt | Voraussetzung | 0 |
| | unnötig | 1 |
| Ort | spezieller Ort | 0 |
| | irrelevant | 1 |
| Ziel | Zutritt/Zugriff | 0 |
| | sensible Daten | 1 |

Tabelle 4.7: Übersetzung von Tabelle 4.1 in binäre Ziffern

Um sich die Darstellung in Binärcodierung vorstellen zu können wird aus jeder der drei Arten je ein Angriff exemplarisch in das neue Schema übersetzt.

| Art | Human Based | Computer Based | Reverse |
|---|---|---|---|
| Angriff | People Watching | Phishing-E-Mails | |
| Namensschema-Codierung | `HB_UNN_SPEZ_SD` | `CB_VOR_IRLV_ZU` | `RE(_VOR_IRLV_ZU)` |
| Binärcodierung | `00-101` | `01-010` | `10` |

### 4.3.5 Evaluierung der verschiedenen Darstellungsmöglichkeiten

Da es sich bei der Binärcodierung mehr um eine Alternative zum Namensschema handelt und daher jedes Diagramm damit versehen werden kann, ist diese Möglichkeit der Darstellung gesondert zu betrachten. Die binäre Zeichenfolge lässt sich leicht erweitern, was beim eventuellen Hinzufügen neuer Merkmale nötig wird. Ebenfalls vorteilhaft ist die bereits erwähnte internationale Verwendbarkeit dieses Schemas, eine vorhergehende exakte und abgestimmte Übersetzung in die Landessprache vorausgesetzt. Dadurch kann jeder Angriff von Landesgrenzen unabhängig katalogisiert und kommuniziert werden. Des Weiteren kann jede Zahlenfolge von einem Computer leichter analysiert werden als die vorher entwickelte Kürzelschreibweise. Damit kann ein Rechner sowohl die Übersetzung in eine normale Sprache, als auch die Einsortierung in ein bestimmtes Diagramm übernehmen. Allerdings ist diese Darstellung aufgrund der Abstraktion der Merkmalsausprägungen für den Menschen relativ unleserlich. Dennoch ist es grundsätzlich erstrebenswert, die Binärcodierung für die Klassierung der Angriffe zu verwenden.

Nun sollen die restlichen Diagramme auf Übersichtlichkeit oder Erweiterbarkeit untersucht werden. Diese Faktoren sollen zeigen, wie geeignet die verschiedenen Darstellungen für den aktuellen und den zukünftigen Umfang der Kategorisierung sind. Zu bedenken ist hierbei, dass in Zukunft sowohl mehr Angriffe vorhanden, als auch mehr Merkmale von Relevanz sein könnten. Die klassische Baumstruktur kann problemlos mit neuen Merkmalen versehen werden, wird allerdings durch mehr Knoten schnell unübersichtlich groß. Jedoch können ausgeschlossene Klassen einfach herausgenommen werden und müssen nicht extra ausgegraut werden, wie es bei Kreis- und Netzdiagramm der Fall ist. Die Einsortierung der Angriffe kann beim Baumdiagramm intuitiv vorgenommen werden, dauert aber mit jeder weiteren Verzweigung länger. Eine bessere Effizienz bieten hier die beiden anderen Diagramme. Die Kreisdarstellung bietet zwar eine schnelle Einsortierung, nachteilig hingegen sind die geringen Erweiterungsmöglichkeiten und die bei einer großen Anzahl von Angriffen mangelnde Übersichtlichkeit. Werden weitere Merkmale hinzufügt, so stößt das Kreisdiagramm bei fünf Eigenschaften an seine Grenzen. Ähnlich verhält sich die Netzstruktur. Auch hier ist eine hohe Effizienz bei der Klassierung der Angriffe gegeben und die Übersichtlichkeit bei vielen Angriffen in einer Klasse begrenzt. Nichtsdestotrotz lässt sich dieses Diagramm beliebig erweitern, was allerdings in einer unübersichtlichen Struktur endet. Ferner fällt bei der Darstellung als Netz die Einsortierung der Angriffe weitaus leichter als beim Kreisdiagramm, da keine Schnittmengen berücksichtigt, sondern lediglich der richtige Sektor gefunden werden muss. Letztendlich ist dennoch das Baumdiagramm vorzuziehen, da es aufgrund seiner leichten Anpassungsmöglichkeiten zukunftssicherer ist als die anderen Darstellungsmöglichkeiten. Würde die Kategorisierung um kein Merkmal erweitert, so ist die Netzstruktur als Alternative durchaus denkbar, da sie sowohl Informationen als auch Besonderheiten kompakter und übersichtlicher präsentiert.

# 5 Gegenmaßnahmen

Ein weiteres Ziel dieser Arbeit ist die Identifikation und Erklärung möglicher Gegenmaßnahmen für die in Kapitel 2 und 3 behandelten Angriffe. Dabei werden die gefundenen Gegenmaßnahmen in ein Schema für Sicherheitsmaßnahmen einsortiert, das im Rahmen der Vorlesung „IT–Sicherheit“ behandelt wurde. Zusätzlich wird analysiert, ob die Kategorien der gewählten Verfahren für alle Attacken der zugehörigen Klasse oder klassenübergreifend übereinstimmen. Aus den dabei erschlossenen Beziehungen sollen die noch unbesetzten Kategorien mit Klassen eventueller Sicherheitsmaßnahmen versorgt werden. Abschließend werden wirksame Methoden ausgewählt und überprüft, die *Social-Engineering-Angriffe* allgemein verhindern oder deren Ausübung erschweren können.

## 5.1 Methoden gegen einzelne Angriffe

Für die mit Angriffen oder Angriffsvariationen besetzten Klassen ist es besonders wichtig, Gegenmaßnahmen aufzuzeigen, da die darin enthaltenen Attacken bereits aktiv verwendet werden. Der folgende Abschnitt erläutert sowohl bewährte Schutzmechanismen als auch Überlegungen, wie die erwähnten Angriffe erfolgreich abgewehrt oder zumindest erschwert werden können. Anfangs werden die Klassen der hier entwickelten Kategorisierung nicht berücksichtigt, da die Konzentration auf den einzelnen Attacken liegt. Die Kategorien und eventuell vorhandene interne Überschneidungen oder klassenübergreifende Verbindungen der Gegenmaßnahmen werden im darauffolgenden Abschnitt behandelt.

Um eine starke Streuung der Sicherheitsmechanismen zu verhindern, werden die genannten Gegenmaßnahmen in eine Kategorisierung einsortiert, die in der Vorlesung „IT–Sicherheit“ behandelt wurde (siehe Abbildung 5.1). Die dabei herausgefundenen Klassen der einzelnen Gegenmaßnahmen werden anschließend zum Vergleich der klasseninternen und klassenübergreifenden Zusammenhänge verwendet. Die Klassierung kann intuitiv vorgenommen werden und wird jeweils anschaulich neben dem behandelten Angriff dargestellt.

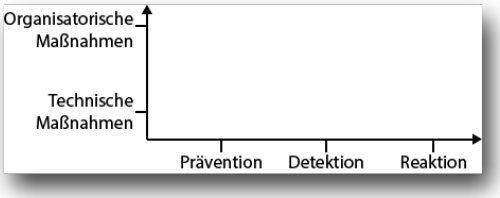
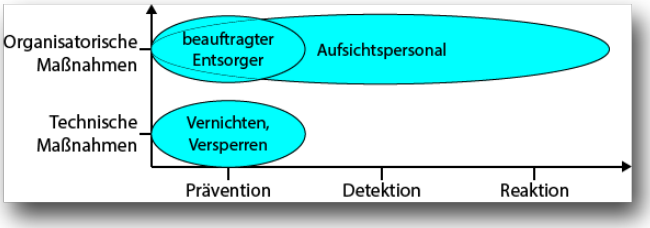



Abbildung 5.1: Kategorisierung von Sicherheitsmechanismen nach [HR12]

**Schema: Angriff** → *verallgemeinerte Gegenmaßnahme(n)*

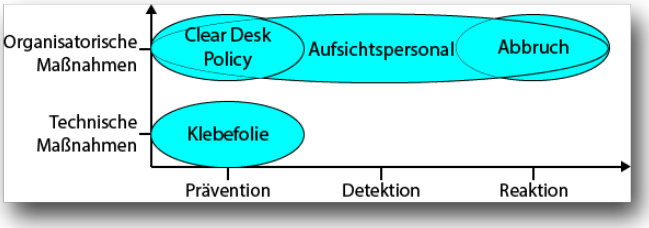
**Dumpster Diving** → *Versperren, Vernichtung, Aufsichtspersonal*




*Dumpster Diving* lässt sich im Allgemeinen recht einfach und vielseitig verhindern oder zumindest erschweren. Dies kann mit dem Schreddern zu entsorgender vertraulicher Dokumente (siehe Abbildung 5.2) und das anschließende Aufbewahren der Reste in einem abgeschlossenen Müllcontainer erreicht werden. Kommt das Abschließen des Abfallbehälters nicht in Betracht, kann ein umzäunter Bereich oder ein spezieller Raum im zugangsbeschränkten Gebäude dafür vorgesehen werden. Außerdem könnte das Abholen und Vernichten des Mülls von einer als vertrauenswürdig eingestuften Firma übernommen werden. Auch im privaten Bereich sollte auf die sichere Entsorgung von Dokumenten mit sensiblen Informationen, wie Kreditkartennummer oder Bankdaten, geachtet werden (siehe [Kee08]). Weitere Möglichkeiten zur Verhinderung oder Abschreckung von *Dumpster Diving* sind in der Nähe der Container angebrachte Kameras und Beleuchtung, zu deren Kontrolle Aufsichtspersonal benötigt wird (vgl. [Cen]).
Im Universitätsbereich ist das Aufstellen von Mülleimern an abgesperrten Orten nicht praktikabel, da jeder Student, Mitarbeiter oder Besucher Zutritt zu den Abfallbehältern benötigt. Alle vorhandenen Eimer mit einem Schloss zu versehen, ist sowohl zu kosten- als auch zu verwaltungsintensiv. Für die angriffsgefährdeten Container der Mitarbeiter ist jedoch eine der genannten Gegenmaßnahmen durchaus empfehlenswert und anwendbar.

Abbildung 5.2: geschredderte Dokumente sind nur mühsam zu rekonstruieren und Schrecken somit vor *Dumpster Diving* ab

**Shoulder Surfing** → *Abbruch, Klebefolie, Clear Desk Policy*



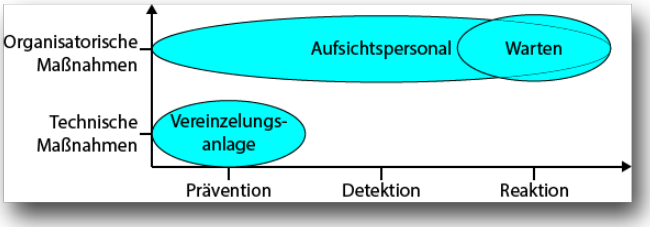

Die einfachste Methode, sich vor *Shoulder Surfing* zu schützen, ist die Wahl eines geeigneten Standortes, an dem niemand einen Blick über die Schulter auf das Notebook oder das Smartphone werfen kann. Am besten stellt man sich hierfür an eine Wand. Eine Reaktion auf einen derartigen Angriff ist der Abbruch der aktuellen Handlung, das heißt das Zuklappen des Notebooks oder das Wegstecken der gerade gelesenen Dokumente beziehungsweise des Handys (siehe [Lon08]). Sollte dies nicht möglich sein, kann eine blickwinkelabhängige Spiegel- oder Verdunkelungsfolie Abhilfe schaffen, die es dem Angreifer nicht erlaubt, etwas auf dem Bildschirm zu erkennen.

Da sich *Shoulder Surfing* jedoch nicht nur auf technische Geräte, sondern auch auf Dokumente in Papierform sowie den Schreibtisch am Arbeitsplatz konzentriert, kann eine sogenannte „Clear Desk Policy“ zum Verhindern einer solchen Attacke beitragen. Diese Richtlinie beinhaltet Anweisungen, dass ein Mitarbeiter bei temporärer Abwesenheit vertrauliche Dokumente stets verschlossen aufzubewahren hat. Computerausdrucke sollten nicht offen auf dem Schreibtisch liegen gelassen und Passwörter nicht schriftlich notiert werden dürfen. Des Weiteren sollte der Computer bei Abwesenheit heruntergefahren oder der Bildschirm gesperrt werden, um die Sicht auf offene Fenster und Dokumente und den kompletten Zugriff Unautorisierter nicht zuzulassen. Der Rechner sollte außerdem mit einem Passwort geschützt sein (vgl. [Onl09]). Die Einhaltung eines sauberen Schreibtisches wird durch einen abschließbaren Rollcontainer, wie ihn Abbildung 5.3 zeigt, erst sinnvoll, da dann die Dokumente verschlossen aufbewahrt werden können. Die Policy sollte von jedem Mitarbeiter bei Beginn des Beschäftigungsverhältnisses verpflichtend unterzeichnet werden. Auch *Shoulder Surfing* kann mit Überwachungskameras, die von Aufsichtspersonal kontrolliert werden, organisatorisch verhindert werden.

Abbildung 5.3: abschließbare Container dienen der sicheren Aufbewahrung von Dokumenten

Das hier behandelte Szenario im Hochschulumfeld lässt sich am einfachsten mit der blickwinkelabhängigen Folie bekämpfen, da selbst die hintersten Plätze im Vorlesungssaal aufgrund eines Ganges auch nicht zuverlässig vor *Shoulder Surfing* schützen. Eine Clear Desk Policy ist bezogen auf die Studenten nicht geeignet, bei Hochschulmitarbeitern allerdings empfehlenswert. Die Installation von Kameras und deren Kontrolle ist zu aufwändig, um einen Nutzen für die Universität darzustellen.

**Tailgating** → *Warten, Aufsichtspersonal, Vereinzelungsanlage*




Um *Tailgating* zu verhindern, reicht das Warten, bis die Tür in die Angel fällt, um sicher zu gehen, dass niemand unerlaubterweise in das Gebäude gelangt ist. Sollte sich beim Betreten eines Gebäudes eine unbekannte Person hinter jemandem befinden, so ist es zwar unfreundlich, aber effektiv, die Tür dennoch zu verschließen und zu warten, bis der Unbekannte (eventuell) von einem in Kenntnis gesetzten Kollegen abgeholt wird (siehe [Lon08]). Noch wirksamer wäre es, Pförtner zu beschäftigen, die Unbekannten den Zutritt verweigern. Des Weiteren sind Zugangskarten oder -chips in Kombination mit einer gesicherten Tür oder einem Drehkreuz ein probates Mittel, um *Tailgating* zu verhindern. Doch auch hier ist es für einen Angreifer möglich, die Maßnahmen zu umgehen. Deswegen ist eine Kombination aus Zutrittskontrolle und einer Pforte oder einer Vereinzelungsanlage, wie sie beispielsweise Abbildung 5.4 schematisch darstellt, zu empfehlen. Effektiv sind solche Maßnahmen allerdings nur, wenn sie an allen Ein- und Ausgängen des Gebäudes angebracht werden.

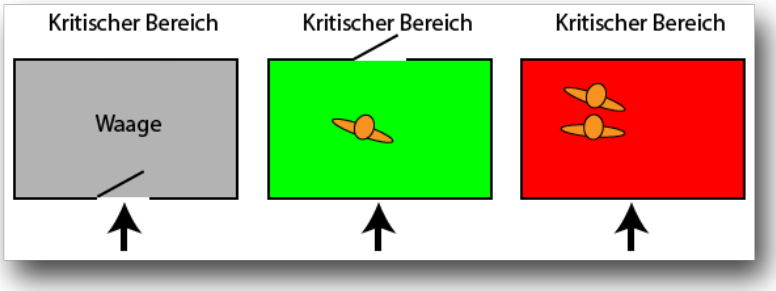
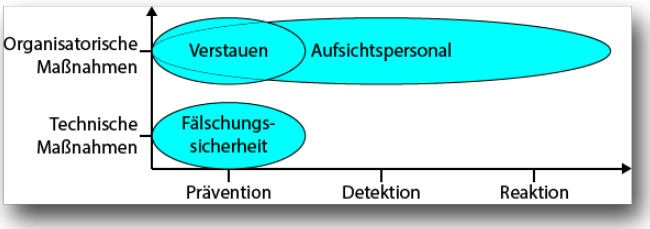



Abbildung 5.4: Vereinzelungsanlage mit Gewichtssensorik
links: Grundaufbau, mittig: einzelne Person, rechts: zwei Personen

Auch an den zugangsbeschränkten CIP-Pools kann eine Art Vereinzelungsanlage der bereits vorhandenen PIN-Eingabe kombiniert werden. Diese Vorgehensweise lässt sich jedoch relativ leicht durch Kommunizieren der richtigen Zahlenkombination vor dem Betreten außer Kraft setzen. Demnach müssten andere Authentifizierungsmethoden wie Zugangskarten eingesetzt werden, welche allerdings für diesen Zweck aufgrund des steigenden Verwaltungsaufwandes nicht praktikabel erscheinen.

**Badge Surveillance** → *Verstauen, Aufsichtspersonal, Fälschungssicherheit*




Badges sollen zur Identifikation von Mitarbeitern dienen und somit die Arbeit des Aufsichtspersonals und der eventuell vorhandenen Pforte erleichtern. Um die Kopie eines solchen Ausweises zu verhindern, sollte darauf

geachtet werden, dass bei repräsentativen Auftritten, auf Fotos und beim Verlassen des Firmengeländes die Badges nicht sichtbar sind (vgl. [Lon08]), oder einige fälschungssichere Elemente eingebaut werden. Außerdem sollten bei außerbetrieblichen Veranstaltungen temporäre Ausweise verwendet werden, sowie Besucher der Firma mit einem Besucherausweis eindeutig von normalen Mitarbeitern unterscheidbar sein, sodass neben dem Aufsichtspersonal jeder Kollege einen Gast als einen solchen erkennen kann.
Um der Kopie eines Studentenausweises vorzubeugen, genügt das Anbringen einiger Fälschungssicherungen, wie sie beispielsweise bei Banknoten oder dem Personalausweis (siehe Abbildung 5.5) eingesetzt werden. Dies sollte dem Angreifer die Erstellung eines Duplikats erheblich erschweren.

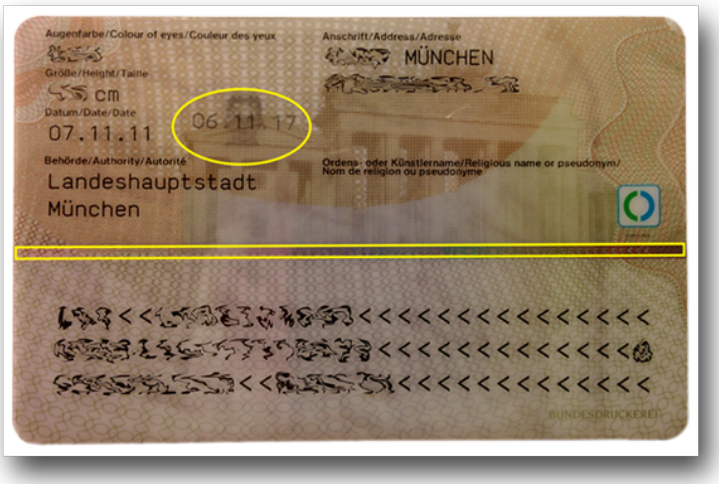
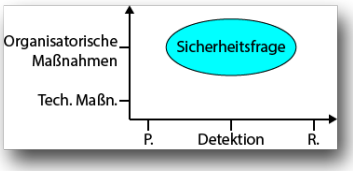


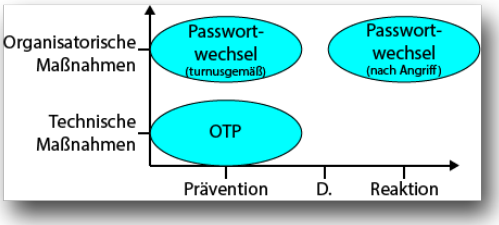

Abbildung 5.5: beim Personalausweis sorgen unter anderem der Sicherheitsfaden und ein Hologramm (beide gelb markiert) für erhöhte Fälschungssicherheit

**Pretexting** → *Sicherheitsfrage*




Damit *Pretexting* verhindert werden kann, sollte eine Verifikation des Gesprächspartners durchgeführt werden. Dies kann durch Passphrasen, bestimmte Fragen und Recherche des Namens im Intranet geschehen. Allerdings können auch diese Maßnahmen von einem gut informierten Angreifer relativ leicht umgangen werden. Es bleibt nur, die Mitarbeiter darauf hinzuweisen, keine sensiblen Daten an unbekannte Anrufer weiterzugeben (siehe [Kee08]).
Damit *Pretexting* im Hochschulumfeld verhindert werden kann, könnte bei der Immatrikulation die Rufnummer des Studenten abgefragt werden. Diese ist über ein Portal online leicht, aber nur mit Zugangsdaten änderbar. Ruft ein Student nun bei der Universität an, wird er aufgefordert seine Nummer anzugeben, da er für das Gespräch zurückgerufen werden soll. Die Rufnummer wird mit der Vorhandenen verglichen und der Student nach Übereinstimmung wieder kontaktiert. Für den anderen Fall, bei dem der Angreifer angibt vom Service-Desk zu sein, kann der Student dieselbe Vorgehensweise wählen und die Hotline selbst kontaktieren (vgl. [Ros10]).

**Quid pro quo** → *One-Time-Password (OTP), Passwortwechsel*




Bei *Quid pro quo* ist es relativ leicht, eine effektive Gegenmaßnahme zu finden. Zertifikatstoken, wie beispielsweise *SecurID* von RSA und OTP's sind hierfür die Mittel der Wahl, um solche Angriffe zu vereiteln. Ist eine derartige Ausstattung zu aufwändig, sollte das Passwort der Mitarbeiter zumindest im Monats-Turnus zurückgesetzt und geändert werden müssen. Generell hat aber jede Person solch offensichtlichen Angeboten eines Angreifers intuitiv auszuweichen und im Anschluss daran ihre Zutrittsdaten zu ändern. Die genannte Gegenmaßnahme der OTP's eignet sich aufgrund der

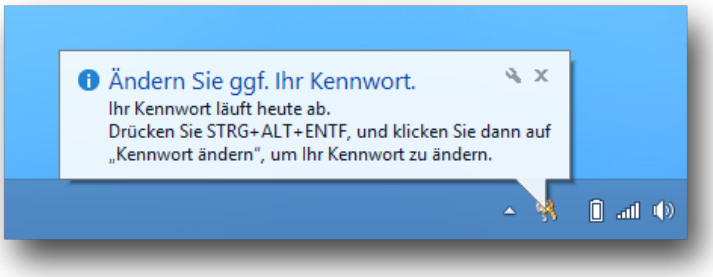


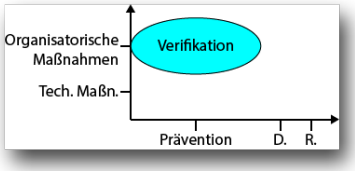

Abbildung 5.6: Erinnerung zum Ändern des Computerpasswortes

quantitativ hohen Anzahl an Studenten im Hochschulumfeld nicht, da dies zu kosten- und verwaltungsintensiv wäre. Allerdings ist eine solche Maßnahme für Mitarbeiter der Universität durchaus von Nutzen, da diese auch weitreichendere Zugriffsrechte besitzen. Die Verwendung der turnusgemäßen Änderung des Passwortes ist in beiden Fällen umsetzbar.

**People Watching** → /

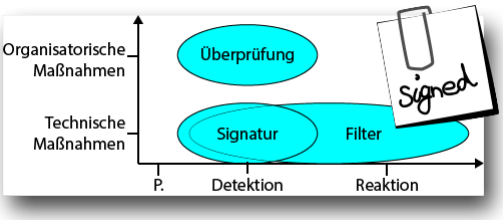
*People Watching* lässt sich kaum verhindern, da es jederzeit und unvermittelt geschehen kann. Des Weiteren werden durch die Beobachtungen meist nur andere Angriffe vorbereitet und nicht direkt vertrauliche Informationen preisgegeben, was eine Gegenmaßnahme für diesen Fall nicht unbedingt voraussetzt.

**Diversion Theft** → *Verifikation*




Um *Diversion Theft* zu verhindern, können einige Vorkehrungen getroffen werden. Bezugnehmend auf das Beispiel unter Abschnitt 2.1.8 sollten die Fahrer aus mehreren Händen die Zieladresse erfahren und während der Fahrt keine Änderung mehr annehmen. Des Weiteren kann eine bestimmte Person als Abnehmer der Ware gemeldet werden, die anschließend am Ort der Entladung mit Kontrolle des Personalausweises eindeutig zu identifizieren ist.
Da die Vorgehensweise eines solchen Angriffs im Hochschulumfeld sich kaum von einer generellen unterscheidet, ist die oben genannte Gegenmaßnahme auch im universitären Alltag voll gültig.

**Phishing E-Mails** → *Filter, Überprüfung, Signatur*

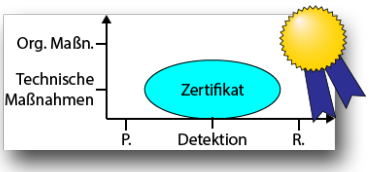



Als wirksame Gegenmaßnahme zu *Phishing-Mails* können Filter eingesetzt werden, die verdächtige E-Mails nicht zum Empfänger weiterleiten. Da diese Vorkehrung allerdings bei Weitem nicht alle gefährlichen Mails aussortiert, müssen ebenso andere Maßnahmen ergriffen werden. Da die meisten *Phishing-Versuche* an viele internationale Empfänger gehen und daher oft maschinell gefertigt sind, können Übersetzungsfehler oder sinnlose Wortzusammensetzungen ein klares Indiz für eine *Phishing-Mail* sein. Außerdem sollte man bei unbekannten Absendern besonders vorsichtig sein und bestenfalls die empfangene E-Mail ohne Berücksichtigung löschen, wenn auch der Betreff keinen Bezug zur Herkunft zeigt. Die genannten Indizien werden allerdings bei den Spezialfällen *Clone Phishing*, *Spear Phishing* und *Whaling* seltener anzutreffen sein, da sie meist professioneller gestaltet werden, als die *Phishing-Mails*, die an die breite Masse gerichtet sind. Daher wird es schwieriger, einen solchen Angriff zu identifizieren. Wird allerdings die Seriosität einer E-Mail angezweifelt, kann ein Anruf beim Absender für Klarheit sorgen. Um die Identität eines Absenders festzustellen, können auch Signaturen als technische Maßnahme gegen diesen Fall beziehungsweise generell gegen auf E-Mail basierende Angriffe verwendet werden.
Auch bei dieser Attacke besteht kein Unterschied der Vorgehensweise, was die genannte Vorsichtsmaßnahme auch im Hochschulumfeld gültig macht. Im behandelten Szenario eines Dozenten, der eine Auszeichnung bekommen soll, sollte er sich vor Übermittlung der Bankdaten telefonisch mit der Stiftung in Verbindung setzen.

**Vishing** → *Filter, Überprüfung, Signaturen*

Beim *Vishing* empfehlen sich ähnliche Abwehrmaßnahmen wie bei den *Phishing E-Mails*, da auch hier die Kontaktaufnahme per E-Mail geschieht. Wenn die angegebene Nummer gewählt wird und vom anderen Ende der Leitung sensible Daten verlangt werden, sollte man diese auf keinen Fall preisgeben. Auch hier kann zusätzlich sowohl darauf geachtet werden, ob das IVR-System ungewohnte Wörter oder falsche Grammatik verwendet, als auch durch Signaturen in den E-Mails der Sender verifiziert werden.
Wie beim *Phishing* gelten auch beim *Vishing* die genannten Gegenmaßnahmen für das Hochschulumfeld.

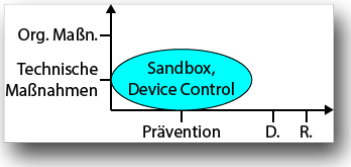
**Evil Twin** → *Zertifikat*




Zur Verhinderung eines *Evil Twin* kann eine Firma oder der entsprechende Betreiber eines WLAN's verschiedene Authentifizierungsoptionen anbieten, welche gewährleisten, dass der richtige Server kontaktiert wird. Ebenfalls sollten Programme zur Verbindungsherstellung verwendet werden, die eine verschlüsselte Übertragung der eingegebenen und angeforderten Daten garantieren. Außerdem ist die Verwendung von Zertifikaten zur (verschlüsselten) Kontrolle des kontaktierten Servers empfohlen (siehe [Phi]).
Im MWN hat das LRZ bereits durch die Verbindung per VPN-Client oder mit Zertifikat

die Authentizität der beiden vorhandenen Netze gewährleistet. Nichtsdestotrotz kann der Angreifer einen SSID mit identischem Namen anbieten. Stutzig werden sollte der Nutzer dann, wenn er nicht nach Benutzername und Passwort gefragt wird oder die Verbindung zum „Internet“ ohne VPN-Client funktionieren sollte.

**Baiting** → *Sandbox, Device Control*




*Baiting* ist schwer zu vereiteln, dennoch kann man seine Mitarbeiter darin unterrichten, keine aufgefundenen Datenträger mit dem Arbeitscomputer zu verbinden. Auch als Privatperson sollte man darauf achten, wie man diese Medien behandelt und sie beispielsweise nur mit dem Schutz einer Sandbox verwenden. Als weiterer kleiner Schritt kann die Autorun-Funktion deaktiviert werden, was allerdings die Ausführung einer anderen Datei des Datenträgers nicht beeinflusst. Dies sollte mit der Einstellung der USB-Sticks als „read-only“ gewährleistet werden. Als weitere Methode zur Verhinderung einer *Baiting-Attacke* kann auch eine Device-Control-Software (siehe Abbildung 5.7) verwendet werden, die es dem Administrator erlaubt, bestimmte Geräte über ihre Hardware-Identifikationsnummer oder die IMEI[1] für einen Benutzer freizugeben. Unregistrierte Speichermedien können dann wegen den entsprechenden Einstellungen nicht mehr verwendet werden.

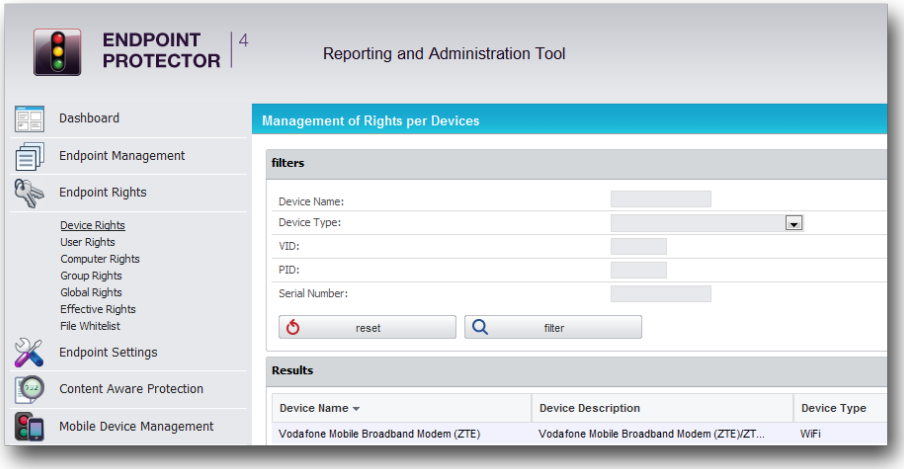
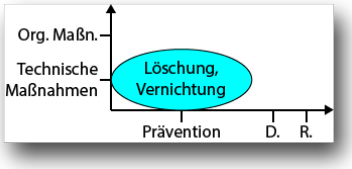



Abbildung 5.7: Ausschnitt eines Screenshots der Device-Control-Software „Endpoint Protector 4“ von CoSoSys Ltd. (siehe [CoS13])

Auch im Hochschulumfeld kann *Baiting* nicht vollständig verhindert werden. Da die Vorgehensweise ein weiteres Mal nicht zwischen Hochschulumfeld und normalem Angriffsfeld differiert, gelten wiederum die genannten Gegenmaßnahmen. Die Computer, die für Studenten bereitgestellt werden, sollten generell nur beschränkte Zugriffsrechte erhalten und die Mitarbeiter gesondert auf solche Attacken hingewiesen werden.

[1] International Mobile Equipment Identity

**Forensic Analysis** → *Löschung, Vernichtung*




Bereits in Kapitel 2 wurde die Verwandtschaft von *Forensic Analysis* und *Dumpster Diving* betont. Auch bei den Gegenmaßnahmen können ähnliche Vorgehensweisen angewendet werden. So sollte ein ausrangierter Datenträger mit professionellen Tools von seinen Inhalten bereinigt und gelöscht werden. Wenn eine weitere Verwendung des Mediums nicht vorgesehen ist, so ist eine sachgemäße Verschrottung, die auch von vertrauenswürdigen Dritten übernommen werden kann, als Sicherheitsmaßnahme angebracht. Ebenso sollten die entsorgten Speichermedien, wie beim *Dumpster Diving*, verschlossen verwahrt werden (siehe [Eic08]).
Weil sich auch bei dieser Attacke keine Unterschiede beim Hochschulumfeld feststellen lassen, ist die generelle Sicherheitsmaßnahme ebenfalls zulässig

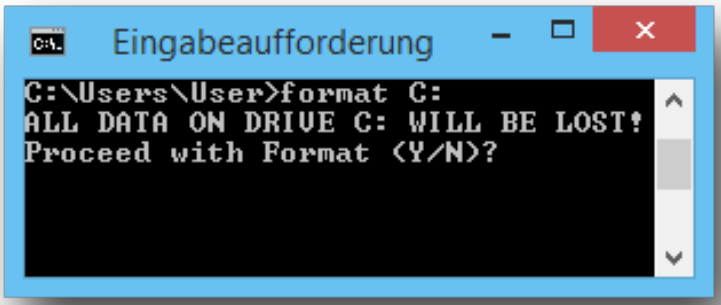
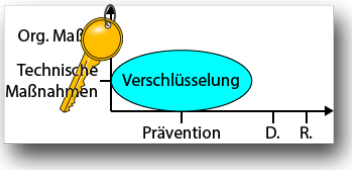


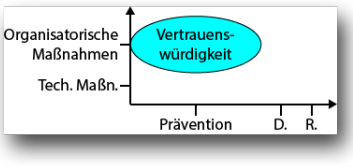

Abbildung 5.8: Formatieren des entsprechenden Datenträgers ist das Mindeste, um Forensic Analysis zu erschweren

**BS – Electronic Badges** → *Verschlüsselung*




Um die Kopie einer elektronischen Zugangskarte zu verhindern, sollten die darauf gespeicherten Informationen verschlüsselt werden. Dafür ist ein hinreichend gutes Kryptographie-Verfahren je nach Bedarf des Einsatzbereiches zu wählen.
Die Umsetzung dieses Angriffs in den universitären Alltag in Abschnitt 3.2 weist keinerlei Unterschiede zum normalen Einsatzbereich auf. Daher ist wiederum die gewählte Gegenmaßnahme uneingeschränkt einsetzbar.

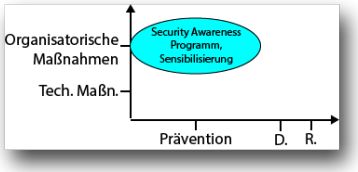
**Reverse Social Engineering** → *Vertrauenswürdigkeit*




*Reverse Social Engineering* ist schwer zu erkennen und daher ist auch die Zahl der möglichen Gegenmaßnahmen beschränkt. Es ist allerdings denkbar einfach, eine solche Attacke zu vereiteln, indem man nur vertrauenswürdige Administratoren oder Firmen kontaktiert. Hat man keine verifi-

zierten Kontakte zur Hand, sollte man sich mit vorher Kollegen oder Bekannten unterhalten, ob sie jemanden empfehlen können und nicht den kürzlich erst kennengelernten Fremden zu Hilfe rufen (vgl. [Kee08]).
Im Bereich der Hochschulen gibt es Rechnerbetriebsgruppen, die sich um die Funktionalität der vorhandenen Rechner, Drucker, Scanner und sonstigen technischen Ausstattung kümmern. Daher sollte bei auftretenden Problemen immer zuerst die RBG um Hilfe gebeten werden und kein externes Unternehmen.

## 5.2 Allgemeine Möglichkeiten




Als allgemeine Gegenmaßnahmen zu *Social-Engineering-Angriffen* werden in der einschlägigen Literatur einstimmig Security Awareness Programme genannt. Sie sollen Mitarbeiter auf die Möglichkeiten der Hacker hinweisen, sowohl alte als auch neue Attacken aufzeigen und somit das Personal sensibilisieren. Die nur einmalige Durchführung eines solchen Programms wird von den Autoren der Fachartikel einheitlich verneint, da wiederkehrende Hinweise auf die verschiedenen Angriffe essentiell sind und dadurch der Lerneffekt maximiert wird. Meist wird der Turnus von einem Jahr als optimale Frequenz derartiger Veranstaltungen angesehen. Auch die Durchführung von Live-Tests, wo die Mitarbeiter auf die Probe gestellt werden, hilft dabei, sie auf solche Attacken aufmerksam zu machen.
Für Privatpersonen ist es dagegen schwieriger, von der Existenz von *Social-Engineering-Angriffen* und vorgesehener Gegenmaßnahmen zu erfahren. Daher sollten auf diesen Anwenderbereich zugeschnittene Seminare angeboten werden. Zweifelhaft ist allerdings die Beteiligung der breiten Bevölkerung an solchen Programmen.

## 5.3 Besonderheiten

Nachdem nun explizit Beispiele für Gegenmaßnahmen genannt und deren Kategorisierung vorgenommen wurde, findet nun eine Analyse der dabei festgestellten Besonderheiten statt.

### 5.3.1 Zusammenhänge unterschiedlicher Klassen

Zunächst wird überprüft, ob und welche Zusammenhänge bei den Gegenmaßnahmen der Angriffe vorhanden sind. Zu diesem Zweck zeigt Abbildung 5.9 die Kategorisierung der Gegenmaßnahmen, in die anstatt der Sicherheitsmechanismen die entsprechenden Angriffsnamen einsortiert wurden. Die farbigen Markierungen vereinfachen die Zuordnung der Namen in die entsprechende Angriffsart.

Jede Attacke könnte durch die im vorherigen Abschnitt genannten allgemeinen Möglichkeiten präventiv organisatorisch behandelt werden. Allerdings würde eine Betrachtung der allgemeingültigen Gegenmaßnahmen die Analyse stark beeinträchtigen und daher wird dieser Punkt nicht weiter in Betracht gezogen.

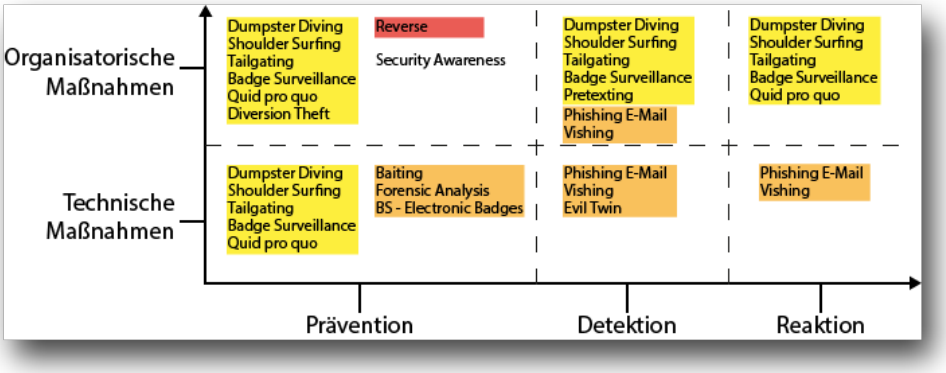



Abbildung 5.9: in die Kategorisierung der Sicherheitsmechanismen einsortierte Angriffsnamen anstelle entsprechender Gegenmaßnahmen

Es ist deutlich zu erkennen, dass viele der menschenbasierenden Attacken durch gezielte präventive Maßnahmen verhinderbar sind. Lediglich bei *Pretexting* kann kein vorbeugender Schutz gegeben werden. Es lässt sich jedoch feststellen, dass sich alle *Human Based* Angriffe durch organisatorische Maßnahmen verhindern lassen können, ungeachtet dessen, ob dies präventiv, detektierend oder reaktiv geschieht, da alle diese Kategorien bei der Verhinderung wirksam sein können. Ähnliches gilt für *Computer Based* Attacken, die alle mit Hilfe technischer Maßnahmen abwendbar sind. Außerdem kann man erkennen, dass sich das Gros unterschiedlicher computerbasierenden Angriffe durch präventive Mechanismen verhindern lässt, wobei auffällt, dass die Gegenmaßnahmen der gesamten Familie des *Phishing* (*Phishing E-Mail*, *Vishing*, *Evil Twin*) eine Ausnahme bilden. Diese Attacken sind entweder detektierend oder reaktiv abzuwehren. Die entstandene Gruppierung der gegen diese zusammenhängenden Techniken wirksamen Mechanismen ist durch das familiäre Verhältnis der Angriffe leicht nachzuvollziehen. Da allerdings *Phishing E-Mail* und *Vishing* dieselben Gegenmaßnahmen aufweisen, ist für diese beiden Attacken die Überschneidung der entsprechenden Kategorien keine Besonderheit. Ebenfalls auffällig ist die Tatsache, dass sich *Human Based* Attacken auf technische Weise ausschließlich präventiv bekämpfen lassen.

Bei genauerer Betrachtung der Kombination der Social-Engineering-Klassen mit den kategorisierten Gegenmaßnahmen können weitere Schlüsse gezogen werden. So sind folgende Klassen durch dieselbe Kategorie von Gegenmaßnahmen zu verhindern:

1. `HB_UNN_SPEZ_SD`
2. `HB_UNN_SPEZ_ZU`
3. `HB_VOR_SPEZ_ZU`
4. `CB_UNN_IRLV_ZU`
5. `CB_UNN_IRLV_SD`
6. `CB_VOR_IRLV_ZU`
7. `CB_VOR_IRLV_SD`

Die Klassen mit der Ziffer 3, 4, 5 und 6 stellen hierbei allerdings keine Besonderheit dar, da sie nur einen Angriff beinhalten und somit auch zwingend eine einheitliche Kategorie der Gegenmaßnahmen aufweisen. Die letzte computerbasierende Klasse auf Platz 7 ist ebenfalls keine Überraschung, da sie *Phishing E-Mail* und *Vishing* beinhaltet. Der Aufbau dieser beiden Attacken ähnelt sich stark, da beide eine Unterform des regulären *Phishings* darstellen. Weitaus interessanter sind die zwei übrigen Klassen der Art *Human Based* (Ziffer 1 und 2), da hier keine voneinander abgeleiteten Angriffe enthalten sind. `HB_UNN_SPEZ_SD` enthält neben *Dumpster Diving* und *Shoulder Surfing* auch *People Watching*, welches selbst nicht direkt zu verhindern ist und somit die Homogenität der Kategorie der Gegenmaßnahmen begünstigt. Ausschlaggebend kann hier die Möglichkeit sein, Aufsichtspersonal einsetzen zu können, um die beiden anderen Angriffe zu verhindern. Die Klasse `HB_UNN_SPEZ_ZU` beinhaltet die Angriffe *Tailgating* und *Badge Surveillance*. Beide zielen in ihrer Urform lediglich auf ein Unternehmen ab, was ein Grund für dieselben Kategorien ihrer Gegenmaßnahmen sein könnte. Auch hier kann in beiden Fällen eine besetzte Pforte Abhilfe schaffen.

Uneinigkeit herrscht dagegen bei den nachstehenden Klassen:

8. `HB_VOR_IRLV_ZU`
9. `HB_VOR_IRLV_SD`
10. `CB_UNN_SPEZ_ZU`
11. `CB_UNN_SPEZ_SD`

Bei den Klassen 8 und 9 erkennt man, dass die Attacken *Quid pro quo* und *Pretexting* der Grund für die jeweilige Unstimmigkeit sind. Bei Klasse Nummer 9 ist dies nichts besonderes, da sie lediglich diese beiden Angriffe enthält. In Klasse 8 hingegen besitzen wenigstens *Quid pro quo* und *Diversion Theft* eine gemeinsame Kategorie der Gegenmaßnahmen. Die computerbasierenden Klassen sind mit Ausnahme von *Evil Twin* durch identische Gegenmaßnahmen zu bekämpfen.
Eine weitere Auffälligkeit ist, dass der *Evil Twin* Angriff die Einigkeit aller kontaktlosen Attacken vereitelt. Wäre dem nicht so, könnten diese gemeinschaftlich mit Hilfe technisch präventiver Gegenmaßnahmen verhindert werden.

### 5.3.2 Unbelegte Klassen

Aufgrund der vorhergehenden Analyse in Kombination mit Abschnitt 4.2.4 können für die unbelegten Klassen zwar keine genauen Gegenmaßnahmen genannt werden, allerdings lässt sich dadurch eine Vermutung hinsichtlich der Art eines wirksamen Sicherheitsmechanismus treffen.
Die Kategorien `CB_VOR_SPEZ_SD` und `CB_VOR_SPEZ_ZU`, beide *Computer Based*, dürften mit Hilfe einer technisch präventiven Maßnahme zu verhindern sein. Dieser Schluss liegt nahe, da Hilfsmittel dieser Kategorie sowohl vor den meisten der computerbasierenden Human-Hacking-Attacken, als auch dem unter Punkt 4.2.4 beschriebenen Angriff Schutz bieten.
Die letzte unbelegte Klasse `HB_VOR_SPEZ_SD` wird, wie die meisten Attacken der Art *Human Based*, vorbeugend durch technische oder organisatorische Maßnahmen bekämpft werden können. Auch organisatorisch detektierende und reagierende Mechanismen wären hier

möglich. Da allerdings in Abschnitt 4.2.4 eine Variante des *Pretexting* als mögliche treffende Attacke genannt wurde, ist demnach im Speziellen ein organisatorisch detektierender Sicherheitsmechanismus für diese Kategorie naheliegend.

Auch wenn in diesem Fall für die unbesetzten Klassen keine direkten Gegenmaßnahmen gefunden werden konnten, sind zumindest die mutmaßlichen Kategorien identifiziert worden.

Für alle anderen Angriffe, mit Ausnahme von *People Watching* wurde jeweils mindestens eine effektive Gegenmaßnahme vorgestellt und in die entsprechende Kategorie einsortiert. Damit konnten verschiedene Auffälligkeiten festgestellt werden, die in die Analyse der möglichen Klassen für die Sicherheitsmechanismen der unbelegten Kategorien eingeflossen sind. Neben den spezifischen Ansätzen können alle *Social-Engineering-Angriffe* mit allgemeinen Möglichkeiten bekämpft werden, die vor allem auf Sensibilisierung der Zielgruppe aufbauen.

# 6 Zusammenfassung & Ausblick

## 6.1 Zusammenfassung der Erkenntnisse

Nach einer kurzen Einleitung in das *Social Engineering* sowie die für diese Arbeit relevanten Begrifflichkeiten, wurden die in der einschlägigen Literatur genannten *Social-Engineering-Angriffe* zunächst allgemein erklärt und bereits einer ersten Sortierung unterzogen. Diese schon bestehenden Kategorien halfen während der gesamten Arbeit, eine grobe Richtung in den folgenden Ausführungen einzuschlagen. Anschließend wurde der Begriff des hier behandelten Hochschulumfelds definiert und die einzelnen Attacken in diesem Bereich beispielhaft umgesetzt. Dabei zeigte sich, dass auch dieses Umfeld teilweise sehr stark durch *Social Engineering* gefährdet ist.

Über Fragen zur Vorgehensweise der Angriffe wurden charakteristische Merkmale herausgearbeitet und die für die Kategorisierung irrelevanten Eigenschaften aufgrund von Abhängigkeiten zu anderen aussortiert. Danach wurden die Wertebereiche der restlichen Attribute festgelegt und die *Social-Engineering-Techniken* bezüglich ihrer spezifischen Ausprägungen analysiert. Infolgedessen wurde das Merkmal *Opfer* ausgeschlossen, da herausgefunden wurde, dass sich in dieser Hinsicht eine Privatperson nicht von einer Universität unterscheidet, weil ein eventueller Schaden stets durch oder für eine Person entsteht. Danach wurden Angriffe aufgespalten, die bei der nachfolgenden Einsortierung wegen ihrer Merkmalsausprägungen in mehrere Klassen gepasst hätten.
Nachdem die Eigenschaften der Angriffe für die Kategorisierung festgelegt wurden, ist erkannt worden, dass sich aufgrund der vorhergehenden Entscheidungen eine spezielle Betrachtung des Hochschulumfeldes bei der Kategorisierung als unnötig erweist. Anschließend wurden die Klassen und deren abstrakte Namen definiert sowie alle Attacken in das dadurch entstandene Schema eindeutig einsortiert.
Dann ist überprüft worden, ob eine Taxonomie entstanden ist, was durch die Entscheidung, die Angriffe aufzuspalten, auch gelungen ist. Da zwar jede Attacke eindeutig einer Klasse zugeordnet werden kann, allerdings nicht alle Klassen besetzt wurden, sind die leeren Kategorien auf möglicherweise passende Angriffe untersucht worden. Dabei konnten für drei der fünf betroffenen Klassen denkbare Angriffsszenarien umgesetzt werden, was deren Beibehaltung nach sich zog. Die anderen beiden Kategorien wurden aus der Kategorisierung entfernt, da sie eine unvereinbare Kombination der Merkmale aufweisen.
Das Kapitel schloss mit der Entwicklung und Evaluierung verschiedener Darstellungsmöglichkeiten, aus welchen die Baumstruktur als intuitivste, die Netzstruktur als derzeit übersichtlichste und die Binärcodierung als internationalste erkannt wurden.

Zu guter Letzt wurden Gegenmaßnahmen für die einzelnen Angriffe sowie das gesamte *Social-Engineering-Feld* aufgezeigt. Durch die Verallgemeinerung und Kategorisierung der möglichen Abhilfen wurde versucht, Verwandtschaften zwischen den belegten Klassen her-

auszufinden, um dadurch auf Sicherheitsmaßnahmen für die unbelegten Kategorien schließen zu können, was leider nicht gelang. Die betrachteten allgemeinen Möglichkeiten zum Schutz vor *Social Engineering* sind jedoch sowohl für alle bestehenden Angriffe, als auch für noch nicht vorhandene als Alternative zu sehen.

## 6.2 Ausblick & weiterführende Themen

Die geschaffenen Kategorien mit den enthaltenen Angriffen können als Anhaltspunkt oder allgemeine Angriffsbeschreibung dienen, die in den verschiedenen Bereichen der Gegenmaßnahmen verwendet werden sollten. Durch die Übersichtlichkeit ist es für Laien verständlich und nachvollziehbar, wie solche Attacken funktionieren beziehungsweise ablaufen können und man darauf zu reagieren hat. *Social Engineering* wird auch in Zukunft weiterhin eine sehr große Gefahr für die Sicherheit aller Daten sein und das Entstehen neuer Angriffsvarianten ist dabei durchaus plausibel. Die hier entstandene Kategorisierung ist wegen des einfachen Namensschemas in dieser Hinsicht leicht erweiterbar. Lediglich die Wahl einer Visualisierung ist je nach Anzahl der Merkmale und Angriffe aufgrund der Übersichtlichkeit anzupassen.

Für auf dieser Arbeit aufbauende Ausführungen eignet sich beispielsweise die genauere Umsetzung der Binärcodierung. Hierbei würde sich sowohl die internationale Übersetzung als auch die Umsetzung in ein lauffähiges Programm als Möglichkeit anbieten. Dabei käme es vor allem auf eine fehlerfreie Implementierung eines Sortieralgorithmus und die übersichtliche grafische Darstellung der denkbar beträchtlichen Menge an Informationen an. Ein solcher Ansatz ist durchaus empfehlenswert, da dadurch die globale Kommunikation aller *Social-Engineering-Angriffe* und eine umfassende Sammlung unterstützt werden kann.
Ergänzend kann eine ebenfalls binäre Codierung der Kategorisierung der Gegenmaßnahmen entwickelt werden. Schön wäre es hierbei, diese beiden Darstellungen durch bestimmte Formeln oder Berechnungen zu verknüpfen, um direkt Vorschläge für Mechanismen zur Abwehr eines soeben eingefügten Angriffs zu bekommen. Dieser Entwicklung käme ebenfalls die mögliche internationale Verwendung zu Gute, die sämtliche Informationen zu vorhandenen Gegenmaßnahmen nicht nur sammeln sondern zusätzlich jedem zur Verfügung stellen kann.

Des Weiteren könnten weniger extensive Arbeiten in Zukunft die Einsortierung neuer Angriffe in das hier entstandene Schema übernehmen. Die Überarbeitung der Kategorisierung sollte dabei nicht notwendig werden.
Eine zukünftige Arbeit könnte auch die unterschiedlichen Klassen hinsichtlich ihrer Gefährdung für ein anderes Umfeld übernehmen. Ergänzend könnte die Anfälligkeit verschiedener Dienste für genannte Angriffe behandelt werden. Das entstandene Bewertungsschema mag anschließend für die Risikoanalyse eines Unternehmens von Nutzen sein, was ebenfalls exemplarisch ausgearbeitet werden kann.

# Abkürzungsverzeichnis

| | |
|---|---|
| AP | Access Point |
| CIP-Pools | Computer-Investitions-Programm-Pools |
| DNS | Domain Name System |
| LAN | Local Area Network |
| LMU | Ludwig-Maximilians-Universität München |
| LRZ | Leibniz-Rechenzentrum |
| MWN | Münchner Wissenschaftsnetz |
| SSID | Service Set Identifier |
| TUM | Technische Universität München |
| VPN | Virtual Private Network |
| WLAN | Wireless Local Area Network |

# Abbildungsverzeichnis

# Literaturverzeichnis


[Bun] Bundesamt für Sicherheit in der Informationstechnik: *G 5.42 Social Engineering.* https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05042.html. [aufger.: 07.10.2013], Stand: 12. EL Stand 2011.

[Cen] Center for Infrastructure Assurance and Security: *Dumpster Diving.* Technischer Bericht. frühestens 2008 verfasst.

[CoS13] CoSoSys Ltd: *Geräte Berechtigungen.* http://www.endpointprotector.de/products/endpoint_protector#screenshots, 2013. [aufger.: 18.10.2013].

[Eic08] Eichler, Jens: *Social Engineering: Hirngespinst paranoider Sicherheitsexperten oder reale Gefahr?* Gastvortrag beim Deutsche Telekom Chair of Mobile Business & Multilateral Security in Frankfurt, Juni 2008.

[Gaz13] Gazmuri, Pablo: *Social Engineering: Your Biggest Security Threat.* http://www.rdacorp.com/2013/04/social-engineering-your-biggest-security-threat/, April 2013. [aufger.: 06.07.2013].

[Gre13] Greis, Friedhelm: *Snowden soll Kollegen PasswÃ¶rter abgeluchst haben.* http://www.golem.de/news/nsa-affaere-snowden-soll-kollegen-passwoerter-abgeluchst-haben-1311-102636.html, 2013. [aufger.: 08.11.2013].

[Had11] Hadnagy, Christopher: *Die Kunst des Human Hacking: Social Engineering - Deutsche Ausgabe.* mitp Professional, 2. Auflage, 2011.

[HR12] Hommel, Wolfgang und Helmut Reiser: *IT-Sicherheit – Sicherheit vernetzter Systeme – Kapitel 2: Grundlagen.* Vorlesungsskript, Oktober 2012.

[HZ09] Hannebacher, Gerd und Markus Zinz: *Social Hacking.* Seminararbeit, Juni 2009.

[Jac12] Jackie: *What Is Phishing?* http://resources.avg.com.au/spam/what-is-phishing/, August 2012. [aufger.: 07.07.2013].

[Jam06] James, Lance: *Phishing Exposed.* Syngress Publishing, Inc., 1. Auflage, 2006.

[Kee08] Kee, Jared: *Social Engineering: Manipulating the Source.* Technischer Bericht, SANS Institute, 2008.

[Kor12] Kortschak, Gerald: *Social Engineering - Faktor Mensch als Sicherheitslücke.*

Vortrag beim E-Day 2012, 2012.

[Lon08] Long, Johnny: *No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*. Syngress Publishing, Inc., 1. Auflage, 2008.

[LRZ13] LRZ: *Unsere Servicepalette*. `http://www.lrz.de/services/`, Mai 2013. [aufger.: 02.07.2013].

[Mis11] Mishra, Aakash: *There's something „Human" to Social Engineering*. The Hacker News, Mai 2011.

[Mit06] Mitnick, Kevin: *Die Kunst der Täuschung: Risikofaktor Mensch*. mitp Professional, 1. Auflage, 2006.

[Onl09] Onlinesicherheit.at: *Clear Desk Policy*. `https://www.onlinesicherheit.gv.at/mitarbeiterinnen/computer_und_datensicherheit/clear_desk_policy/70950.html`, September 2009. [aufger.: 18.09.2013].

[Oos08] Oosterloo, Bernard: *Managing Social Engineering Risk*. Doktorarbeit, University of Twente, 2008.

[Phi] Phifer, Lisa: *Anatomy of a Wireless "Evil Twin" Attack*. `http://www.watchguard.com/infocenter/editorial/27079.asp`. [aufger.: 18.09.2013].

[Ros10] Ross, Michael: *Identity Theft Countermeasures*. `http://www.ross.ws/content/identity-theft-countermeasures`, Juli 2010. [aufger.: 09.10.2013].