Duale Hochschule Baden-Württemberg
- Karlsruhe -

Fakultät für Informatik

Große Studienarbeit

im Studiengang Informationstechnik

zur Erlangung des akademischen Grades
Bachelor of Engineering

Thema:	Social Engineering
Autor:	Mario Philipp Waxenegger <mariowaxenegger@gmail.de> MatNr. 3981981
Version vom:	2. Mai 2015
Betreuer:	Ralf Brune

Zusammenfassung

Abstract

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Listingverzeichnis

1 Einleitung

Social Engineering könnte man im Allgemeinen mit »gesellschaftliches Ingeniuerwesen« übersetzen. Jedoch trifft es die Bezeichnung »angewandte Sozialwissenschaften« wesentlich besser. Die Techniken hinter *Social Engineering* reichen schon sehr weit in die Vergangenheit zurück, wohingegen der Begriff selbst erst seit einigen Jahren durch verschiedene Hacker wie z.B. Kevin Mtnick geprägt wurde. Worum es sich bei *Social Engineering* handelt soll im Rahmen dieser Ausführung in erster Linie geklärt werden.

Vielmehr stellt sich allerdings die Frage, wie *Social Engineering* von der IT oder anderen Abteilungen gesehen und eingestuft wird. Da es sich um einen recht neuen Terminus handelt, ist dieser womöglich noch nicht vollends in den Unternehmen und Einrichtungen angekommen. Zwar kennt ein jeder die Rundmails eines nigerianischen Prinzen, der für sein Lebensglück noch schnell ein paar tausend Euro benötigt, jedoch handelt es sich bei solchen Maschen nur um die Spitze des Eisbergs *Social Engineering* - die tatsächlichen Möglichkeiten und Gefahren reichen viel weiter.

Um dieser Frage nachzugehen wird das Thema sowohl aus der Sicht des Angreifers als auch aus der Sicht der potenziellen Zielperson analysiert und ausgearbeitet. Dabei entpuppt sich *Social Engineering* als Vielkampf der angewandten Wissenschaften. Für einen Social Engineer gilt es oft die Bereiche Soziologie, Psychologie und einem gewissen Grad an schauspielerischem Können mit technischem Know-How zu verknüpfen.

1.1 Ziel der Arbeit

Im Rahmen dieser Arbeit sollen einige Aspekte zum Thema Social Engineering überprüft und näher untersucht werden. Der Kern der Ausarbeitung liegt im Ergebnis einer Umfrage. Anhand dieser soll zunächst festgestellt werden, wie stark die Gefahren solcher Angriffe wahrgenommen werden. Dabei gilt es außerdem herauszufinden, ob das Bewusstsein der Probanden für Social Engineering kontextabhängig ist. Außerdem soll untersucht werden, ob es diesbezüglich Auffälligkeiten gibt, die darauf hindeuten, dass bestimmte Personengruppen stärker und weniger anfällig sind. Ziel dieser Betrachtung ist es herauszufinden, ob bestimmte Personengruppen schlecht gegen Social Engineering Angriffe gewappnet sind, tatsächlich der Meinung sind für solche Angriffe keinen Nährboden bieten zu können. Des weiteren sollen Korrelationen zwischen Anfälligkeit und anderen Attributen wie Alter, Geschlecht oder ähnlichem hergestellt werden. Das Ziel dieser Ausarbeitung ist es, ein grundlegendes Verständnis von Social Engineering zu vermitteln und anhand der Untersuchungen die Gefährlichkeit einzustufen. Zudem sollen in Anbetracht der Ergebnisse Schutzmöglichkeiten eruiert werden.

Diese Ausarbeitung behandelt jedoch nicht die konkrete Vorgehensweise von Social Engineers. D.h. es werden weder Tools analysiert noch werden detaillierte Fallanalysen durchgeführt. Es werden lediglich dem Verständnis förderliche Beispiele erläutert.

Zudem sollen die beiden Kategorien telefonische und persönliche (direkte) Attacke nur theoretisch behandelt werden. Da die Arbeit ebenso auf zahlreiche psychologische Grundlagen zurückgreift, werden Themen wie *Nonverbale* Kommunikation ebenso kurz aufgegriffen.

1.2 Vorgehensweise

Zu Beginn der Arbeit steht eine umfangreiche Grundlagenrecherche. Dafür werden die Themen Vertrauen, Manipulation, Kommunikation, Risikomanagement und natürlich Social Engineering selbst analysiert. Aus den Ergebnissen dieser Recherche wird zum einen ein Fragebogen entworfen, welcher die Empfänglichkeit für Social Enginneering überprüfen soll, und zum anderen wird eine Phishing-Mail konstruiert. Dabei sollen aus der Theorie gewonnene Erkenntnisse vertieft und in der Anwendung geprüft werden.

Für die Recherche des Themas *Social Engineering* wird Literatur von auf diesem Gebiet wegweisenden Experten zu Rate gezogen. Darunter fallen die Autoren Kevin Mitnick, Christopher Hadnagy und Ian Mann. Das Thema »Vertrauen«, bei dem es sich um ein psychologisches wie soziologisches Phänomen handelt, wird zu Großen Teilen anhand der Autoren Niklas Luhmann und Bruce Schneier aufgearbeitet. Ausgangspunkt für die Recherche zum Thema Kommunikation und Kommunikationsmodelle bietet die Arbeit »Grundlagen der Kommunikation« von Markus Plate, welche unter anderem auf die grundlegenden Ergebnisse von Paul Watzlawick aufbauen. Das Werk »Die Psychologie des Überzeugens« von Robert Cialdini sowie die Arbeiten von Hadnagy bieten die Basis des Kapitels zum Thema *Manipulation. Risikomanagemt* wird anhand der Autoren Dan Borge und Ian Mann näher erläutert.

1.3 Leitfaden

Kapitel 2 stellt den Begriff Social Engineering und die Idee dahinter vor. Dabei werden auch Beispiele für mögliche Angriffe gegeben.

In Kapitel Kapitel 4 wird der Begriff Risiko näher erläutert. Da es sich bei Social Engineering ebenfalls um ein Risiko handelt werden die Analyse und die Handhabung von Risiken sowie damit verbundene Schwierigkeiten genannt.

Um Social Engineering zu verstehen, ist es wichtig die zu Grunde liegenden Prinzipien zu erläutern. In Kapitel 3 werden einige Verhaltensmuster vorgestellt und aufgezeigt wie diese gezielt ausgenutzt werden können. Zentrale Themen sind hierbei vor allem Vertrauen, das Zusammenspiel von Bewusstsein und Unterbewusstsein.

Kapitel Kapitel **??** befasst sich mit der Auswertung einer Umfrage, die im Rahmen der Studienarbeit durchgeführt worden ist.

Im darauf folgenden Kapitel **??** wird die praktische Anwendung einer Social Engineering Attacke

2 Social Engineering

Dieses Kapitel beschreibt den Begriff Social Engineering und grenzt die dazu gehörenden Techniken von üblichen Vorgehensweisen des Hackens ab. Dabei wird in Kapitel 2.1 zunächst eine Definition gegeben. In Kapitel 2.2 wird die Einfachheit solcher Angriffe gegenüber rein technischen Angriffen hervorgehoben. Zum Schluss werden in Kapitel 2.3 Beispiele für verschiedene Methoden gegeben.

2.1 Definition

Um den Begriff Social Engineering korrekt einordnen zu können müssen zunächst herkömmliche Aspekte der Informationssicherheit betrachtet werden. Bei diesen handelt es sich zum einen um physikalische Zugriffskontrolle (z.B. Identitätsprüfungen an Türen) und zum anderen um IT-Sicherheit (meistens wird allerdings bei IT-Sicherheit lediglich von „Sicherheit“ gesprochen). Diese beiden Sicherheitsaspekte haben zweifellos ihren Platz und ihre Berechtigung. In vielen Fällen werden aber nur diese Art Angriffe berücksichtigt, denen solche Systeme entgegenarbeiten sollen. Offensichtlich ist, dass sich IT-Sicherheit und physikalische Sicherheit ausschließlich auf ein Unternehmen beschränken, welches lediglich aus IT-Systemen und Gebäuden mit Türen und Fenstern besteht. Eine der essenziellsten Kernkomponenten des Unternehmens wird dabei gänzlich übersehen. Der Mitarbeiter stellt das größte Kapital des Unternehmens dar. Durch Social Engineering Techniken wird er jedoch zugleich zur größten Sicherheitslücke desselben Unternehmens. Dies liegt größtenteils an den mangelnden Gegenmaßnahmen, die zu Social Engineering Attacken ergriffen werden (Mann, 2008).

Nun stellt sich weiter die Frage, was einen solchen Angriff ausmacht. Social Engineering Attacken zielen darauf ab, bestimmte Personen dahingehend zu manipulieren bestimmte Informationen herauszugeben oder Handlungen auszuführen, für die der Eingreifer selbst keine Berechtigung besitzt. Um solche Handlung auszulösen werden verschiedenste Techniken zur Täuschung herangezogen, die alle auf psychologischen Erkenntnissen beruhen. Auf diese wird in Kapitel 3 Psychologische Grundlagen tiefer eingegangen.

2.2 Alternative zu technischen Methoden

In den letzten Jahren ist die Zahl von Social Engineering Angriffen, wie sie in (Mitnick and Simon, 2003) beschrieben sind, stark angestiegen. Diese Entwicklung ist nicht ohne Grund zu beobachten. Während seit Beginn des Informationszeitalters auch die Angriffe auf Datenbestände immer häufiger und vor allem gefährlicher geworden sind, wurden entsprechend starke Gegenmaßnahmen entwickelt. Diese beschränken sich bis heute auf die Apsekte der physikalischen Sicherheit und der IT-Sicherheit. Auch heute noch spielt vor allem die IT-Sicherheit in vielen Unternehmen sicherlich gerechtfer-

tigt eine übergeordnete Rolle. In jedem Unternehmen finden sehr wirkungsvolle jedoch ebenso kostenintensive Abwehrmechanismen ihre Anwendung. Diese stellen zwar kein unüberwindbares Hindernis dar, halten dennoch vielen Angriffen stand oder schrecken bereits vor einem Versuch ab. Während große Sicherheitsfirmen hierfür teure Software- und Hardwarelösungen anbieten, ist das Bewusstsein für das Angebot an Abwehr- und Präventaionsmaßnahmen, die der Prävention von manipulativen Angriffen auf die Mitarbeiter dienen, noch ausbaufähig (Mann, 2008).

Es liegt auf der Hand, dass immer mehr Angriffe nicht durch gewöhnliche Hacking-Techniken auf die IT-Systeme direkt gerichtet werden, sondern die dafür verantwortlichen Mitarbeiter als Ziel haben. Der zu konventionellen Methoden gesparte Aufwand ist größer als er erwartet wird. Im nächsten Kapitel werden einige gängige Methoden und deren Effizienz vorgestellt.

2.3 Typische Angriffsarten

In diesem Kapitel werden exemplarisch drei grundlegende Angriffstechniken vorgestellt und es wird zusammenfassend geklärt, warum diese Techniken besonders große Erfolgschancen bieten. Dabei werden einige psychologische Grundlagen vorweggenommen, welche in Kapitel 3 detailliert beschrieben werden. Zum Verständnis der folgenden Beispiele sind diese Grundlagen nicht notwendig, jedoch werden nach der Lektüre des Kapitels Psychologische Grundlagen die Vorgänge hinter diesen Beispielen noch sehr viel deutlicher erkennbar sein. Bei den im Folgenden vorgestellten Angriffskategorien handelt es sich um Phishing, Phone Elicitation und Identitätsbetrug. Diese Herangehensweisen haben viele Gemeinsamkeiten, unterscheiden sich jedoch in der Anonymität des Angreifers.

2.3.1 Phishing

Beim Phishing handelt es sich um die unpersönlichste Variante eines Social Engineering Angriffes. Bei einer Phishing-Attacke wird versucht, mittels einer E-Mail das Angriffsziel dazu zu bringen einen infizierten Anhang zu öffnen, oder einen bestimmten Link zu besuchen. Man unterscheidet hierbei zwischen dem gewöhnlichen Phishing (das Senden von Massenmails) und dem Spear-Phishing, bei dem die Mail(s) zielgerichtet versendet werden. Handelt es sich beim Opfer einer Spear-Phishing-Attacke um eine besonders einflussreiche Person, bezeichnet man dies als *Whaling* (Hadnagy, 2014). Das Phishing bietet durch den ausbleibenden persönlichen Kontakt mit der Zielperson ein besonders hohes Maß an Anonymität. Somit stellt ein Angriff dieser Art meist kein großes Risiko für den Social Engineer dar. Allerdings erschwert die Anonymität es dem Angreifer das Vertrauen der Zielperson zu erwecken (Mann, 2008).

Phishing-Mails zielen immer auf bestimmte Gefühle der Opfer ab. Dazu gehört bspw. Angst vor Diebstahl oder Verlust, wenn in der Mail beschrieben wird, dass der eigene

PC von Viren befallen ist oder man eine Mahnung für eine Rechnung erhält. Der Angreifer kann ebenso auf andere Emotionen wie Trauer (Hilfe-Aufrufe) oder Freude (»Sie haben gewonnen!«) abzielen. Der Angreifer versucht durch das Auslösen bestimmter Emotionen ein bestimmtes Verhalten zu triggern. Dabei handelt es sich um Automatismen, welche in Kapitel 3.3.1 genauer beschrieben werden (Hadnagy, 2014).

2.3.2 Phone Elicitation

Das Abhören per Telefon stellt für den Angreifer einen guten Kompromiss zwischen Anonymität und der Erlangung des Vertrauens der Zielperson dar. Das Opfer kann zwar die Identität des Anrufers nicht vollständig nachprüfen, es gibt allerdings trotzdem einige Indizien, die es möglich machen, die Zielperson von den guten Absichten und der Authentizität des Anrufers zu überzeugen. So erweckt es bspw. schnell Vertrauen, wenn die angezeigte Telefonnummer dem eigenen Unternehmen oder einem Partner-Unternehmen zugeordnet werden kann. Wenn die Zielperson zudem beiläufig eine Bemerkung macht, aus der man schließen kann, dass er zum Unternehmen gehört (Erwähnen eines anderen Mitarbeiters, Kenntnis von internen Termini).

Diese Indizien sind in der Praxis sehr leicht zu fälschen. Mittels *Spoofing* ist es mit besonders geringem Aufwand möglich, die auf dem Display angezeigte Rufnummer zu verfälschen. Anhaltspunkte für Randinformationen wie die Existenz eines bestimmten Mitarbeiters lassen sich durch vorbereitende Analyse ebenfalls mit überschaubarem Aufwand ermitteln. Beliebte Angriffsziele für Angriffe per Telefon sind vor allem Heimarbeiter und Mitarbeiter des IT-Helpdesks. Im Folgenden wird dieses Angriffsziel näher beleuchtet (Hadnagy, 2014).

2.3.3 Heimarbeit und Helpdesks

Ein beliebtes Ziel für Social Engineering Angriffe stellen Mitarbeiter dar, die vom Home-Office aus arbeiten. Dabei können die Mitarbeiter direkt als Ziel genommen werden. Angestellte, die zu großen Teilen von zu Hause aus arbeiten, wissen oftmals nicht über alle Kollegen Bescheid und können auf Anrufe eines Angreifers, der sich als vermeintlicher Arbeitskollege ausgibt, vertrauliche Informationen herausgeben. Dabei wird Distanz zum Unternehmen als Schwachstelle ausgenutzt. Dieses Angriffsziel ist zudem mit vertauschten Rollen denkbar. Somit wäre der Angreifer ein vermeintlicher Mitarbeiter im Home-Office und das Angriffsziel ist der IT-Helpdesk. Mitarbeiter eines solchen Helpdesks sind oft geschult darauf freundlich und zuvorkommend zu handeln. Da gegenüber Heimarbeitern eine besonders große Hilfsbereitschaft an den Tag gelegt wird, ist es eine beliebte Taktik sich als Heimarbeiter auszugeben und so gewünschte Informationen zu erhalten. Bei Angriffen auf Mitarbeiter des Helpdesks oder Heimarbeiter macht sich der Social Engineer die Rollen zu Nutze, die diese Personen im Arbeitsalltag spielen. Dazu gehört auch die Autorität durch Wissen des Helpdesk-

Mitarbeiters, die für den Angriff auf einen Mitarbeiter im Home-Office ausgenutzt werden kann (genauer beschrieben in Kapitel 3.3.5 Autorität und Befehle), sowie die grundsätzliche Hilfsbereitschaft, die für den umgekehrten Angriff genutzt werden können (Mann, 2008).

2.3.4 Identitätsbetrug

Beim Identitätsbetrug geht die Anonymität des Angreifers gegen null, da er der Zielperson direkt gegenübersteht. Wird der Angriff jedoch gekonnt durchgeführt, ist es die wirkungsvollste Art eines Social Engineering Angriffes, da mit dieser Methode sehr schnell Vertrauen aufgebaut werden kann. Ein passender Begriff hierfür wäre *Real Life Acting* oder *Angewandtes Schauspiel*. Mit verschiedenen Hilfsmitteln wie Kleidung, Sprache, Körperhaltung, gefälschten Identitätskarten und einem kongruenten Pretext überzeugt der Social Engineer seine Zielpersonen meist bereits ohne Worte von der Echtheit seines Auftretens (Hadnagy, 2014).

Die Dauer eines solchen Angriffes kann dabei stark variieren. Meist handelt es sich um eine kurze Infiltration, bei der Positionen von Überwachungskameras bestimmt oder mit Malware verseuchte USB-Sticks platziert werden. Wie solche Angriffe ablaufen können wird von (Hadnagy, 2014) und (Mann, 2008) erläutert erläutert. Desweiteren beschrieben sie eine weitere Dimension des Identitätsbetrugs, welche im Allgemeinen unter einem verdeckten Ermittler, Spion oder »Maulwurf« bekannt ist. Dies stellt eine sehr aufwändige und ebenso gefährliche Variante des Social Engineering dar und wird später im Abschnitt **??** anhand eines kurzen Beispiels erläutert.

Die zur Verfügung stehenden Mittel sind überraschend simpel. Ziel dieser Methoden ist es allerdings immer, unausgesprochene Fragen über die Person des Angreifers automatisch zu beantworten, so dass sich Zielpersonen keine weiteren Gedanken darüber machen, ob es sich bei dem Social Engineer um einen Betrüger handelt. Es haben sich hierbei vor allem drei charakteristische Muster bewährt: Dabei handelt es sich zum einen um unzureichend geschützte Bereiche eines Gebäudekomplexes. Gemeint sind damit insbesondere Raucherbereiche. Über solche Areale erhält man meist auch ohne Besitz einer Zugangskarte physischen Zugriff auf das Gebäude des Zielunternehmens. Die Herausforderung des Social Engineers liegt dabei in erster Linie darin, die Rolle des Mitarbeiters, der von einer Zigerettenpause zurückkehrt, überzeugend zu spielen. Eine weitere Methode um schnell Zugriff zu einem gesicherten Gebäude zu erhalten oder sich unbemerkt fort zu bewegen ist es, schwere Gegenstände oder einen großen Karton zu tragen. Mitarbeiter hinterfragen meist nicht, was transportiert wird oder um wen es sich bei der Person handelt. Im Gegenteil wird dem Social Engineer meist sogar die Türe aufgehalten. Die letzte nennenswerte Methode ist das Verwenden einer falschen Zugangskarte. Dafür genügt es, die Karte echt aussehen zu lassen. Versucht der Angreifer nun mehrmals vergeblich mit seiner falschen Karte Zugang zu erhalten,

kann er sich an den nächsten Mitarbeiter wenden und ihn darum beten, ihn einzulassen (Hadnagy, 2014). Die eben genannten Methoden machen sich ähnlich wie die unter Kapitel Heimarbeit und Helpdesks erwähnte Taktik dem im Allgemeinen als »Helferinstinkt« bekannten Phänomen zu Nutze. Dies geht stark mit dem Bedürfnis gemocht zu werden einher. In Kapitel 3 Psychologische Grundlagen wird dieses Prinzip nochmals aufgegriffen und genauer erklärt.

Eine weitere Möglichkeit ist es einen Maulwurf in das Unternehmen zu schleusen. Es kann sich dabei sowohl um einen neuen Angestellten als auch um einen langjährigen Mitarbeiter handeln, welcher sich aus verschiedenen Gründen motiviert fühlen kann, den Hacker mit Insiderwissen zu versorgen. Ebenso ist es denkbar, dass diese Rolle auch unwillentlich von einem Mitarbeiter eingenommen wird, z.B. durch Erpressung oder dass der Mitarbeiter gar unwissentlich in die Position eines *Insiders* gerät (Dhanjani et al., 2009). Dieses Szenario ist zwar etwas seltener anzutreffen jedoch nicht zu unterschätzen, da auf diese Weise bereits Zugriffsrechte auf bestimmte Bereiche des Unternehmens oder der Datenbasis gewährt wird. Auch in solchen Situationen wird die Hilfsbereitschaft von anderen Mitarbeitern ausgenutzt, denn gerade neue Mitarbeiter benötigen am Anfang viel Hilfe. Außerdem bringt man neuen Mitarbeitern mehr Nachsehen entgegen. In einer solchen Position ist es für einen Angreifer ein leichtes an eine Vielzahl wichtiger Informationen zu kommen oder zusätzliche Schwachstellen ausfindig zu machen. Wenn neue Mitarbeiter nach kurzer Zeit ohne plausiblen Grund Kündigen, kann dies ein Indiz dafür sein, dass es sich um einen Angriff gehandelt haben kann. Um solche Situationen zu verhindern, ist es angebracht für neue Mitarbeiter ausreichende Background-Checks vorzunehmen (Mann, 2008).

2.4 Wirkungsweise

Warum gerade solche Angriffe eine besonders gute Erfolgsquote haben, ergibt sich vor allem aus der allgemeinen Auffassung des Begriffs *Security*. In den meisten Unternehmen und Einrichtungen sind zumeist intensivst Sicherheitsvorkehrungen in Form von Soft- oder Hardwarelösungen getroffen. Sind lediglich Firewalls, Zugangskontrollen, Überwachungskameras o.ä. im Einsatz, werden damit jedoch nur zwei potenzielle Angriffsziele geschützt. Zum einen wird durch Firewalls und Antivirensoftware die Sicherheit vor reinen IT-Angriffen erhöht. Zum anderen erschweren Zugangskontrollen und Überwachungskameras den physischen Zugriff auf Systeme und Gebäudeabschnitte. Bei diesen herkömmlichen Maßnahmen wird jedoch eine gravierende Sicherheitslücke übersehen: Der Mensch (Mann, 2008).

Denn letztendlich werden sämtliche Sicherheitssysteme (bei denen es sich nur um Hard- und Software handelt) von menschlichen Mitarbeitern bedient, konfiguriert und gewartet. Sie stellen somit eine Schnittstelle zu den eigentlichen Sicherheitssystemen dar. Und genau darin liegt die Ursache für die hohe Effizienz von Social Engineering

Attacken. Denn der Mensch (an der direkten Schnittstelle) ist meist ungeschützt und das Gesamtsystem nicht auf solche Angriffe vorbereitet. Der Angreifer macht sich dabei verschiedene menschlicher Eigenschaften (man könnte sie in diesem Zusammenhang auch als »Sicherheitslücken« bezeichnen), wie sie später in Kapitel 3 auf der nächsten Seite erläutert werden, zu Nutze.

Aus den im vorigen Kapitel aufgeführten Angriffstypen ist jedoch ein grundsätzliche Schema herauszulesen. Alle Angriffe haben gemeinsam, dass zunächst ein Vertrauensverhältnis zwischen Angreifer und Ziel aufgebaut wird. Dabei ist vor allem die Glaubwürdigkeit des Angreifers ausschlaggebend. Zudem können bestimmte Manipulationswerkzeuge eingesetzt und Kommunikationsmodelle zu Hilfe genommen werden, um dieses Vertrauen gezielt aufzubauen. Damit diese Hauptbestandteile Vertrauen, Kommunikation und Manipulation verstanden werden, werden diese im folgenden Kapitel genauer erläutert.

3 Psychologische Grundlagen

In den beiden vorangegangen Kapiteln ist erklärt worden, worum es sich bei Social Engineering handelt und weshalb das damit einhergehende Risiko falsch bewertet wird. Nun sollen die psychologischen Grundlagen vermittelt werden, welche den Angriffstechniken eines Social Engineers zugrunde liegen. Der Kern ist dabei stets die zwischenmenschliche Kommunikation. Sie tritt in vielen verschiedenen Variationen auf. In Kapitel 3.2 werden daher zunächst wichtige Theorien und Modelle zum Thema Kommunikation vorgestellt. Im weiteren Verlauf befasst sich Kapitel 3.1 genauer mit dem Konzept des Vertrauens und wie sich Vertrauen entwickelt. Zuletzt werden in Kapitel 3.3 wichtige Methoden zur Manipulation mit kurzen Anwendungsbeispielen vorgestellt.

3.1 Vertrauen

Dieses Kapitel setzt sich genauer mit dem abstrakten Begriff Vertrauen auseinander. Dabei soll zunächst erklärt werden, worum es sich bei Vertrauen handelt und wie es aus der Entwicklungsgeschichte der Menschheit heraus entstanden ist, welchen Zweck es erfüllt und warum es für den gesellschaftlichen Umgang notwendig ist. Im weiteren Verlauf wird erläutert, welche Faktoren das Vertrauensgefühl verstärken oder hemmen.

3.1.1 Ursprung

Die Entstehung des Vertrauenskonzepts liegt weit zurück in der Evolutionsgeschichte der Menschheit. Wie bei anderen Lebewesen hat sich auch für den Menschen herausgestellt, dass die Kooperation mit anderen Artgenossen eine gute Überlebensstrategie darstellt. Dadurch sind kleine (soziale) Gruppen entstanden, die sich durch Zusammenarbeit ihre Existenz sicherten. Das Gesamtrisiko des Individuums wird durch diese funktionierende Kooperation geschmälert (Schneier, 2012).

Der Tatsache geschuldet, dass sich die menschliche Intelligenz stark von der eines Tieres unterscheidet, kommt es in gesellschaftlichen Gruppen vermehrt zu Täuschungsversuchen. Vereinfacht setzt sich eine Gruppe aus zwei Typen zusammen: *Tauben* und *Falken*. Die beiden Tiere sollen dabei zwei verschiedene Kampfstrategien in der Gesellschaft darstellen. Die *Falken* repräsentieren dabei für eine äußerst aggressive Strategie d.h. sie meiden einen Kampf nicht und ziehen sich erst zurück, wenn sie ernste körperliche Schäden erlitten haben. *Tauben* hingegen »kämpfen« lediglich mit konventionellen Mitteln z.B. durch Drohungen oder ähnliche Aktionen. Treffen zwei Tauben aufeinander, so gibt es keinen Verletzten, da es keine tatsächliche Auseinandersetzung gibt. Trifft eine Taube auf einen Falken, wird die Taube schnell die Flucht ergreifen und der Falke siegt. Bei eine Konfrontation zweier Falken wird jedoch so lange gekämpft bis einer der beiden kampfunfähig ist (schwer verletzt oder tot). Simuliert man dieses Modell wird man feststellen, dass die Anzahl der Tauben grundsätzlich sehr hoch ist,

da diese im Schnitt aus jeder zweiten Auseinandersetzung siegreich hervorgehen und kein Risiko tragen verletzt zu werden. Wird das System jedoch dahingehend aus dem Gleichgewicht gebracht, dass es lukrativ ist, die Kampfstrategie des Falken zu fahren, wird die Population der Tauben zurückgehen. Um die Anzahl der sozialen Ausreißer möglichst gering zu halten, ist es daher nötig, den Anreiz für ein solches Verhalten möglichst gering zu halten (Dawkins, 1976).

3.1.2 Notwendigkeit von Vertrauen

Überträgt man dieses abstrakte Spiel auf die gesellschaftlichen Gruppen wird klar, dass das Individuum großes Interesse daran hat, dass bspw. Täuschungsversuche durch Gruppenmitglieder (Falken-Strategie) für andere Mitglieder der Gruppe nicht lukrativ sind. Dies lässt sich mittels verschiedener Druckmechanismen realisieren, wie sie im Abschnitt Druckmechanismen näher beschrieben werden. Zusammenfassend ist festzustellen, dass sich durch Subtrahieren der Sicherheiten (Schutz der Gruppe, etc.) von allen potenziellen Gefahren ein Restrisiko (Täuschungsversuche o.ä.) bleibt. Dieses wird von menschlichen Individuen mit dem Vertrauen in die Mitmenschen und den Zusammenhalt der Gruppe überbrückt. Vertrauen ist demnach eine Erleichterung im alltäglichen gesellschaftlichen Leben und bietet dem Individuum sowie der Gruppe einen erheblichen Mehrwert. Es kann sich dabei auch um Vertrauen in verschiedene Institutionen (Polizei, Staat oder Justiz) oder uns fremden Personen handeln (Schneier, 2012). Der Soziologe und Gesellschaftstheoretiker Niklas Luhmann sieht in Vertrauen auch die Konsequenz der sozialen Komplexität (Luhmann, 2000).

Nachdem in diesem Abschnitt geklärt worden ist, worum es sich bei zwischenmenschlichen Vertrauen handelt, ist es nun an der Zeit sich Gedanken zu machen, durch welche konkreten Umstände sich Vertrauen entwickeln kann. Von Interesse ist für einen Social Engineer dabei vor allem wie und warum Vertrauen in fremde Personen entsteht. Der folgende Abschnitt beschäftigt sich mit den dafür verantwortlichen Faktoren.

3.1.3 Faktoren für erfolgreiche Vertrauensentwicklung

Die Entstehung von Vertrauen mit genetisch unverwandten Menschen ist auch als reziproker Altruismus bekannt. Unter einer altruistischen Verhaltensweise versteht man eine Handlung, die unmittelbar mehr Kosten als Nutzen für die ausübende Person trägt. In einer funktionierenden Gesellschaft ist es jedoch nötig, dass dieser Altruismus reziprok ausgeübt wird. Dadurch entsteht langfristig ein größerer Nutzen auf beiden Seiten. Die Frage ist dabei, wann dieses Vertrauen entsteht, um eine altruistische Verhaltensweise zu begünstigen.

Geht man von relativ kleinen Gruppen aus ist das altruistische Verhalten besonders stark ausgeprägt. Es bestehen nicht viele Möglichkeiten der unbemerkten Täuschung, was die Kooperation untereinander begünstigt. Die Gegebenheit des schwindenden Ver-

trauens ergibt sich mit wachsender Gruppengröße. Da die Bekanntschaften zunehmend oberflächlicher werden, wird es für das Individuum schwieriger Täuschungsversuche anderer Gruppenmitglieder zu erkennen. Damit scheint klar, dass das Ausmaß des Vertrauens proportional zur Gruppengröße ist. Der Antropologe Robin Dunbar erfasste, welche Gruppengröße ein Individuum im gesellschaftlichen Leben überschauen kann. Für eine einzelne Person ist es im Schnitt möglich mit bis zu 148 anderen Menschen soziale Beziehungen einzugehen, was ebenso grundsätzliches Misstrauen gegenüber fremden Personen mit sich bringt (Dunbar, 2010).

Bis vor ein paar tausend Jahren war diese Zahl noch mehr als ausreichend, denn selten hatte es der Mensch mit größeren Gruppen zu tun. Doch gerade in den letzten Jahrhunderten sind gesellschaftliche Interaktionen in größeren Gruppen an der Tagesordnung. Dadurch ist es für das Individuum unmöglich zu allen Gruppenmitgliedern (z.B. Großstadt) soziale Beziehungen zu entwickeln. Der Mensch zieht daher zur Beurteilung der Vertrauenswürdigkeit verschiedene Merkmale des Gegenübers heran. Bei fremden Personen können diese optischen und charakterlichen Merkmale entscheiden, ob ihr ein altruistisches Verhalten entgegengebracht wird. Dabei gilt zumeist das Prinzip *mirror and matching*. Es konnte in einigen Studien gezeigt werden, dass altruistische Verhaltensweisen verstärkt gegenüber Menschen, mit denen man sich identifizieren kann, an den Tag gelegt werden. Dies gilt nicht für anonyme Fremde. Beispiele für solche Merkmale sind

- Kleidung
- Herkunft
- Aussehen (Frisur, Hautfarbe, etc.)
- Sprache

Wie sehr die einzelnen Punkte ausschlaggebend sind variiert von Situation zu Situation. Vor allem in gewohnten Umgebungen spielen diese Faktoren eine zunehmend geringere Rolle, wohingegen der Faktor Herkunft an Bedeutung gewinnt, je weiter man sich von der eigenen Heimat entfernt befindet. Ebenso verhält es sich mit der Sprache (Schneier, 2012). Dies erklärt auch die hohen Erfolgschancen der in Kapitel 2.3 beschriebenen Angriffsmuster. Die größten Chancen auf Erfolg sind bei einem Angriff mit direkter Konfrontation gegeben. Das Opfer hat viele optische Merkmale, die es heranziehen kann, um den Angreifer einzuordnen. So genügt meist schon ähnliche Kleidung, um eine altruistische Verhaltensweise auszulösen (z.B. eine Tür aufhalten). Mit zunehmender Anonymität bzw. Distanz des Angreifers wird es schwieriger beim Opfer Vertrauen zu erwecken.

3.1.4 Druckmechanismen

Der Hauptgrund warum der Mensch davon ausgehen kann, dass Vertrauen grundsätzlich von seinen Mitmenschen nicht ausgenutzt wird, sind verschiedene Druckmechanismen, die einzelne Gruppenmitglieder einer Gesellschaft am Abweichen - etwa der Verhaltensweise eines Falken - hindern. Zweck dieser Druckmechanismen ist es, Täuschungsversuche so wenig lukrativ wie möglich zu gestalten bzw. deren Risiko so zu erhöhen, dass es sich nicht mehr mit dem Nutzen aufwiegen lässt. Im Folgenden werden verschiedene gesellschaftliche Druckmechanismen beschrieben: moralischer Druck, institutioneller Druck sowie Reputationsdruck.

Der moralische Druck hält das Individuum bspw. vom Stehlen ab, da es anhand der Moralvorstellungen als falsch eingestuft wird das Eigentum Anderer zu missachten. Bei institutionellen Druckmechanismen handelt sich um Regeln und Gesetze einer bestimmten Institution. Es kann sich bei dieser um ein Unternehmen, einen Verein oder einen Staat handeln. Abweichungen von diesen Regeln und Gesetzen gehen mit Bestrafung einher. Dieser Strafvollzug dient dabei als Abschreckung und lässt das Risiko für die von der gesellschaftlichen Norm abweichende Person steigen. Der Reputationsdruck hingegen bezieht sich auf die Reaktion anderer Personen auf die gewählte Handlungsweise. Dieser Druck hat die Ursache, dass ein Individuum durch Abweichung von der Gruppennorm einen Schaden am eigenen Ruf zu fürchten hat. Verteidigungssysteme dagegen sollen vor physischen Angriffen schützen. Dazu zählen allgemeine Sicherheitssysteme wie Türschlösser, Alarmanlagen oder Antivirus-Software. Diese Installationen sollen Menschen physisch davon abhalten einen Angriff zu unternehmen. Neben Verteidigungssystemen kommen auch andere präventive Maßnahmen zum Einsatz wie z.B. provisorische Polizeipräsenz oder Sicherheitspersonal. Durch bloße Anwesenheit von wird dadurch die Risikoeinschätzung direkt beeinflusst. Eine andere Art Sicherheitssysteme sind sog. Interventionen. Zu solchen zählen z.B. Wachpatrouillen, Überwachungskameras oder Authentifizierungssysteme. Um die Kooperation der Allgemeinheit diesbezüglich zu fördern werden Uniformen, Zugangskarten oder Ähnliches genutzt (Schneier, 2012).

Abschließend bleibt zu diesen Sicherheitssystemen zu sagen, dass es sich hierbei meist nicht um einen absoluten Schutz handelt, sondern vielmehr um eine Art Schadensreduzierung. Viele dieser Druckmittel greifen meist erst nach der Abweichung und nicht bereits davor (Ausnahme: Präventive Maßnahmen). Außerdem bieten diese »Sicherheiten« gleichzeitig auch gefährliche Angriffspotenziale. Oft genügt bereits das Tragen einer Uniform um unangebrachtes Vertrauen zu erwecken (s. Kapitel 3.3.5). Die zweifelhafte Nützlichkeit von Zugangskarten wurde bereits in Kapitel 2.3.4 Identitätsbetrug aufgezeigt.

3.2 Kommunikation

Der nun folgende Abschnitt behandelt das Thema Kommunikation. Im Zusammenhang mit Social Engineering nimmt die Art der Kommunikation eine tragende Rolle ein. Denn jeder Angriff ob per Mail oder durch persönlichen Kontakt läuft Kommunikation zweier Menschen (Ziel und Angreifer) ab. Grundsätzlich gilt es, das im vorigen Abschnitt beschriebene Vertrauen zu wecken. Damit ein Angreifer dieses Ziel erfolgreich erreichen kann, nutzt dieser verschiedene Modelle der Kommunikation. Auf den nun folgenden Seiten wird zunächst erklärt, welche Aspekte unter den Begriff Kommunikation fallen. Danach wird die sog. nonverbale Kommunikation genauer beleuchtet. Abschließend werden zwei Kommunikationsmodelle anhand kurzer Beispiele beschrieben.

3.2.1 Definition

(Duden, 2006) beschreibt den Begriff in diesem Zusammenhang *Kommunikation* treffender als »zwischenmenschlicher Verkehr besonders mithilfe von Sprache und Zeichen«. Eine eher technische, dafür jedoch sehr allgemeingültige Einordnung des Kommunikationsbegriffs verbirgt sich hinter dem Shannon-Weaver-Modell (s. Abbildung 1).

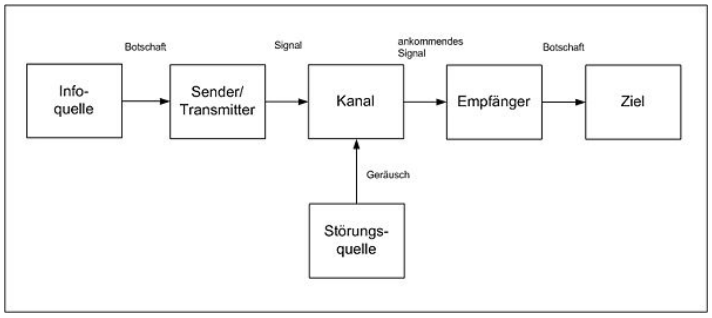

Abbildung 1: Shannon-Weaver-Modell

Dieses Modell verdeutlicht zunächst, dass an der Kommunikation stets zwei Instanzen beteiligt sind (Informationsquelle und Ziel). Die Informationsquelle erzeugt dabei eine Botschaft, welche für das Ziel bestimmt ist und von diesem interpretiert wird. Diese Kommunikationspartner Senden bzw. Empfangen mittels entsprechender Apparate, welche die zu sendende Botschaft in Signale umwandelt (und umgekehrt). Meist finden sich diese »Geräte« direkt in der Informationsquelle bzw. im Ziel integriert wieder (bei zwischenmenschlicher Kommunikation sind dies Mund und Ohren). Dieser Informationsaustausch geht immer über einen Kommunikationskanal (z.B. Kabel, Luft, Telefon oder E-Mail). Das darin übertragene Signal kann von Störquellen verfremdet werden. Kommunikation zeichnet sich in fast allen Fällen zudem durch einen bidirektionalen und wechselseitigen Informationsaustausch aus, d.h. jeder Sender ist gleichzeitig auch

Empfänger von Botschaften. Werden über diesen Weg zwei oder mehr Botschaften ausgetauscht spricht man von einer *Interaktion* (Hadnagy, 2011).

Um dieses allgemeine Modell für den praktischen Gebrauch nützlich zu machen, gilt es die relevanten Kommunikationskanäle zu definieren und näher zu studieren. Paul Watzlawick hat auf diesem Gebiet einige wertvolle Erkenntnisse gewonnen und die fünf *pragmatischen Axiome der Kommunikation* formuliert (Plate, 2013). Das erste und gleichzeitig Wichtigste dieser Axiome lautet »man kann nicht nicht kommunizieren« (Watzlawick et al., 2007, S. 53). Watzlawick setzt dabei Verhalten der Kommunikation gleich und da es keinen Gegensatz zu Verhalten gibt, ist es auch nicht möglich kein Verhalten zu zeigen ergo nicht zu kommunizieren. Somit hat jede Art von Verhalten, sofern sie über einen Übertragungskanal vermittelt wird, potenziell einen kommunikativen Charakter. Ferner hat nach Watzlawick Verhalten Mitteilungscharakter; somit sind Verhalten und Mitteilung nicht voneinander zu trennen und sollten für ein glaubwürdiges Auftreten kongruent sein. Diese Aspekte werden vor allem durch den Begriff *nonverbale Kommunikation* geprägt. In Abschnitt Kapitel 3.2.3 wird detaillierter auf diese Art der Kommunikation eingegangen (Plate, 2013). Ein weiteres von Watzlawick formuliertes Axiom besagt, dass »die Natur einer Beziehung durch die Interpunktion der Kommunikationsabläufe seitens der Partner bedingt« (Watzlawick et al., 2007, S. 61) ist. Diese Interpunktion von Ereignisfolgen kann mit der Klammersetzung eines mathematischen Terms verglichen werden. Durch unterschiedliche Positionierung der Klammern (d.h. durch unterschiedliche Interpunktion) entstehen verschiedene Ergebnisse. Im Bezug auf die Interaktion werden bei kommunikativen Abläufen somit Ursache und Wirkung markiert. Abbildung 2 zeigt beispielhaft wie durch Interpunktion Kausalzusammenhänge definiert werden. Durch das Zurückziehen des Ehemanns beginnt die Frau zu nörgeln, was wiederum das Verhalten des Ehemanns hervorruft. Gerade in diesem Beispiel ist die Kenntnis über die Interpunktion wichtig, denn genauso ist das Zurückziehen des Ehemanns nur eine Reaktion auf das nörgeln der Ehefrau (Plate, 2013).

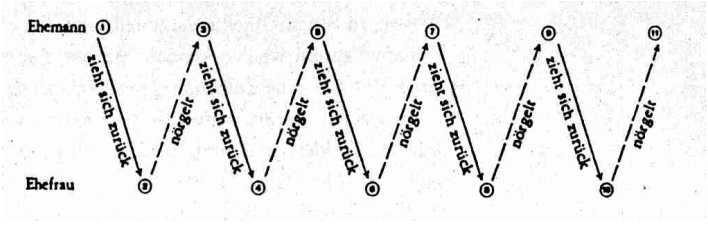

Abbildung 2: Interpunktion

Außerdem unterscheidet eines der in (Watzlawick et al., 2007, S. 56) aufgeführten Axiome zwischen *digitaler* und *analoger Kommunikation*. Damit sind zwei Ebenen gemeint. Die digitale Ebene beschreibt die zur Kommunikation verwendeten Worte einer Sprache. Diese sind dadurch digital, dass ein bestimmtes Wort einer bestimmten

Buchstabenfolge entspricht. Interessanter ist jedoch die analoge Kommunikationsebene. Darunter fallen sog. *paraverbale*, *extraverbale* und *nonverbale* Sprachanteile (Plate, 2013). Diese drei Aspekte werden in Kapitel Kapitel 3.2.3 Nonverbale Kommunikation gemeinsam beschrieben. Hinzu kommt ein weiteres Axiom, welches eine Aussage über den Beziehungs- und den Inhaltsaspekt (Watzlawick et al., 2007) der Nachrichten trifft. Watzlawick beschreibt den Zusammenhang dieser zwei Aspekte insofern, dass der Beziehungsaspekt den Inhaltsaspekt beeinflusst und es sich somit um eine *Metakommunikation* handelt. Diese Metainformation gibt dem Empfänger Aufschluss darüber, wie die eigentliche Information zu interpretieren ist. Ausdrücklich formuliert wird dieser Beziehungsaspekt der Nachricht jedoch nur in den seltensten Fällen (Plate, 2013). Das letzte von (Watzlawick et al., 2007, S. 50ff) formulierte Axiom unterteilt Interaktionen in *symmetrische* und *komplementäre* Interaktionen. Symmetrische Interaktionen zeichnen sich durch die Gleichheit beider Parteien aus. Die komplementäre Interaktionen hingegen basiert auf solchen Unterschieden. Bei dieser Art der Interaktion nimmt eine der Parteien eine übergeordnete Position ein (primäre Stellung), die andere befindet sich in der untergeordneten Position (sekundäre Stellung). Die übergeordnete Partei, welche die Art der Kommunikation bestimmt, ist dabei aktiv, während die Person in der untergeordneten Position lediglich akzeptiert (passiv) (Plate, 2013).

3.2.2 Berlos SMCR-Modell

Diese von Watzlawick genannten Axiome bilden eine gute Grundlage für erfolgreiches Social Engineering. Jedoch sind diese Axiome selbst nur schwer auf konkrete Situationen übertragbar. Aus diesem Grund bietet es sich an, sich verschiedenerer darauf aufbauender Modelle zu bedienen. In diesem Abschnitt wird dafür exemplarisch das SMCR-Modell von David Berlo vorgestellt. In der Einleitung des Kapitels Kommunikation wurde das Kommunikationsmodell nach Shannon und Weaver erwähnt. Dieses sehr allgemeine und eher technisch anmutende Modell wurde 1960 von David Berlo um einige Aspekte erweitert. Wie in Abbildung 3 zu sehen ist, werden die Hauptkategorien Quelle, Botschaft, Kanal und Empfänger wiederum konkreter definiert.

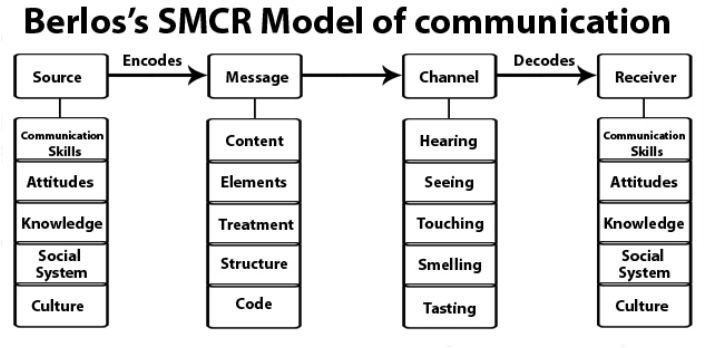

Abbildung 3: SMCR-Modell von Berlo

Bei Sender und Empfänger werden verschiedene individuelle Faktoren berücksichtigt wie z.B. Kultur, Wissen oder die eigenen Kommunikationskenntnisse. Auch die übermittelte Nachricht wird anhand verschiedener Merkmale analysiert. Wichtig ist jedoch vor allem die Einordnungsmöglichkeit der Kommunikationskanäle, welche über das Vorhandensein der fünf Sinne ermöglicht wird (Sehen, Hören, Fühlen, Geruchs- und Geschmackssinn). Abhängig vom gewählten Kanal fallen somit manche dieser Merkmale weg. Bspw. werden bei einer Videokonferrenz nur die beiden Merkmale Sehen und Hören berücksichtigt. Bei einer E-Mail wird der Kommunikationskanal zusätzlich auf lediglich das Sehen eingeengt bzw. bei einem gewöhnlichen Telefonat auf das Hören beschränkt (Hadnagy, 2011). Für einen Social Engineer sind dies wichtige Vorüberlegungen, denn die Aufmerksamkeit wird auf nur ein Merkmal der Botschaft verengt, sodass eine tiefere Verarbeitung derselben erfolgen kann. Dadurch fallen selbst kleinste Fehler leicht auf. Auch Christopher Hadnagy nutzt dieses Modell und erweitert es noch durch die Komponente *Feedback*, was die vom Angreifer erwartete Antwort im Falle einer korrekten Durchführung darstellt (Hadnagy, 2011).

3.2.3 Nonverbale Kommunikation

Die Nonverbale Kommunikation ist einer der wichtigsten Kommunikationskanäle. Schätzungen einiger Experten zufolge macht die Nonverbale Kommunikation ca. 55% des gesamten Informationsgehalts einer persönlich übermittelten Nachricht aus (Müller, 2007, S. 4). Dementsprechend ist die Deutung der Informationen dieses Kanals entsprechend komplex, denn zur Nonverbalen Kommunikation zählen alle körperlichen Gesten, Bewegungen und Haltungen sowie auch akustische Eigenschaften, d.h. neben dem tatsächlich Gesagten, wird der Art wie etwas gesagt wird, ebenfalls eine Bedeutung zugewiesen (Hadnagy, 2014).

Im einleitenden Abschnitt Definition war bereits die Rede von den durch Watzlawick definierten Axiomen der Kommunikation. Dabei wird insbesondere auf sog. *Analoge Kommunikation* eingegangen, die *extraverbalen*, *paraverbalen* und *nonverbalen* Eigenschaften. Als extraverbale Spracheigenschaften bezeichnet man individuelle Stimmeigenschaften, geschlechts- oder altersbedingte Eigenschaften sowie Dialekte und Akzente. Aus diesen lassen sich bereits Rückschlüsse auf die sprechende Person liefern, da sie jedoch im Laufe einer Kommunikation im Allgemeinen nicht variieren, werden sie hier außen vor gelassen (Plate, 2013). Interessanter sind die paraverbalen Sprecheigenschaften, zu denen Merkmale wie Lautheit, Tonhöhe, Sprechgeschwindigkeit und Sprachmelodie gehören. Diese Eigenschaften sind im englischsprachigen Raum auch durch RSVP abgekürzt (rythm, speed, volume, pitch). Über bestimmte Ausprägungen dieser Merkmale werden zu dem Gesprochen hinzu weitere Botschaften übermittelt. So kann eine laute Stimme die Wut über den Gesprächspartner vermitteln, schnelles Sprechen mit hoher Stimme kann ein Zeichen von Unsicherheit sein und lange Pausen

können signalisieren, dass der Sprecher nicht die Wahrheit spricht. Besonders wichtig ist hierbei das Wort »kann«. Die Bedeutung ist grundsätzlich situations- und personenabhängig (Plate, 2013). Die mitunter entscheidendsten Eigenschaften sind die eigentlichen nonverbalen Merkmale. Diese können in die Kategorien Mimik, Gestik und Körperhaltung unterteilt werden. Aus der Körperhaltung (z.B. Fußstellungen oder Armhaltungen) kann man den Status zwischenmenschlicher Beziehungen während einer Unterhaltung ableiten. Verschiedene Gesichtsausdrücke lassen außerdem eine solide Einordnung von Gefühlszuständen zu. Auch aus Arm- oder Handbewegungen können Rückschlüsse auf eine Person und ihren aktuellen Gefühlszustand gezogen werden. An dieser Stelle sei ein weiteres Mal betont, dass diese Merkmale nicht immer eine Bedeutung haben. Auch hier können bestimmte Merkmalsausprägungen zur *Baseline* der Person gehören und somit keine konkreten Aussagen zulassen (Plate, 2013).

Abschließend sei erwähnt, dass das Wissen über die nonverbale Kommunikation nicht nur zum Erkennen von Gefühlszuständen genutzt werden kann. Durch bewusste Kontrolle des Körpers oder der Stimme können gewünschte Stimmungen erzeugt werden. Dieses Können ist vor allem für den Aufbau eines Vertrauensverhältnisses nützlich. Weiß man solche Zeichen zu interpretieren und umzusetzen, ist es ein leichtes mittels »mirror and match« ein Vertrauensverhältnis aufzubauen (Hadnagy, 2014).

3.3 Instrumente der Manipulation

Bei Social Engineering geht es wie eingangs in Kapitel 2 bereits erwähnt vordergründig nicht darum, den Zugriff auf sensible Daten durch gezielte technische Angriffe gewährt zu bekommen. Vielmehr geht es darum andere Personen, welche für den Zugriff auf die gewünschten Informationen berechtigt sind, dahingehend zu beeinflussen, Aktionen durchzuführen, die dem Angreifer entweder diese Daten zuspielen oder ihn sogar selbst dafür autorisieren. Für solche Angriffe bieten sich einige bewährte Methoden an, wie sie unter anderem auch in der Werbebranche Verwendung finden. Dabei wird auf verschiedene Mechanismen und Automatismen des menschlichen Verhaltens abgezielt, wie sie ab Kapitel 3.3.2 erläutert werden sollen. Es wird dafür in jedem der folgenden Abschnitte eine kurze Erklärung des Prinzips gegeben sowie die Art und Intensität der Wirkung aufgezeigt und eine Angriffsmöglichkeit im Social Engineering erläutert. Diese Mechanismen liegen zunächst alle dem Prinzip der Automatismen zugrunde, welches in folgenden Kapitel beschrieben wird.

3.3.1 Automatismen

In der Psychologie versteht man unter einem Automatismus eine vom Bewusstsein kaum oder gar nicht kontrolliert ablaufende Tätigkeit (Duden, 2006). Bei Lebewesen handelt es sich dabei um fest verankerte Verhaltensmuster. Entwickelt haben sich diese Mechanismen im Laufe der Evolution und sind somit ein fester Bestandteil der Psyche

aller Lebewesen. Diese Automatismen bestehen im Wesentlichen aus zwei Teilen. Zunächst ist ein bestimmtes Ereignis nötig. Dabei kann es sich um einfache Reize aller Art handeln (visuell, akustisch, haptisch, etc.) oder auch um ein komplexes Zusammenspiel mehrerer solcher Reize. Dieses Ereignis kann leicht eine fest zugeordnete Reaktion triggern, welche den zweiten Teil des Automatismus darstellt. (Cialdini, 2006) führt dafür das Beispiel einer Truthenne an. Diese reagiert auf ein bestimmtes Geräusch, welches ihre Küken von sich geben (akustischer Reiz) damit, dass sie ihre Küken füttert. Auf den ersten Blick ist dieser Automatismus auch wirksam und hilfreich, denn er erlaubt das herausfiltern relevanter Informationen. Zwar erspart sich die Henne eine aufwändige Betrachtung der gesamten Informationen, jedoch ist sie dadurch bereits anfällig für eine Art Social Engineering, da Teil, die auf einen Täuschungsversuch hindeuten, können übersehen werden. Legt man der Henne einen Lautsprecher vor, der eben diese Geräusche von sich gibt, wird sie das gleiche Verhalten zeigen, als würde es sich um ein echtes Küken handeln.

Diese Verhaltensweisen sind bei Tieren zwar besonders stark ausgeprägt, machen allerdings bei uns Menschen nicht gänzlich halt. Denn auch Menschen benötigten in der Vergangenheit solche Automatismen um zu überleben und benötigen diese auch heute noch, für eine eingehende Betrachtung aller Informationen reicht die Gedächtniskapazität nicht aus. Der Unterschied zu den Tieren besteht allerdings darin, dass es Menschen leichter fällt diese Automatismen abzulegen. Nichtsdestoweniger bieten Automatismen auch beim Menschen Potenzial für Social Engineering Angriffe. In Anbetracht dessen ist es in der Praxis vielmehr das Zusammenspiel vieler Faktoren, die bestimmte Verhaltensweisen auslösen. Konkret sind damit Verhaltensmuster gemeint, welche erst durch die Bildung von Gemeinschaften entstanden sind. Dabei handelt es sich um erlernte Automatismen, die uns den Umgang mit Mitmenschen erleichtern. Aber auch diese Automatismen können ausgenutzt werden, um ein gewünschtes Verhalten auszulösen (Cialdini, 2006).

3.3.2 Reziprozität

Reziprozität leitet sich vom lateinischen Wort *reziprocus* ab, was mit »wechselseitig« zu übersetzen ist. Die Wechselseitigkeit tritt dergestalt auf, dass durch Leitungen, Gefälligkeiten o.ä. beim Empfänger derselben das Gefühl entsteht, sich dafür revanchieren zu wollen. Die Nützlichkeit dieses Mechanismus ist nicht bestreitbar. So ist es für uns selbstverständlich Dienstleistungen finanziell zu entlohnen, was für eine funktionierende Gesellschaft, wie wir sie kennen, unabdingbar ist. Das Gleiche gilt für Gefälligkeiten, welche nicht finanziell vergütet werden. Ein Beispiel hierfür ist es, das Anliegen eines Arbeitskollegen bevorzugt zu behandeln. Dadurch dass der anderen Person ein Gefallen erwiesen wird, entsteht bei ihr das Gefühl sich revanchieren zu wollen. Dieses Phänomen tritt in vielen verschiedenen Variationen auf, welche meist auf einer zuvorkommenden

Handlungsweise, einer Art Präsent oder auch einem eigenen Zugeständnis beruhen. Die Intensität der Auswirkung, die das Prinzip der Reziprozität mit sich bringt, hängt in jedem Fall vom Wert der erwiesenen Gefälligkeit bzw. des erbrachten Geschenks ab. Die bis hierhin beschriebenen Fakten lösen jedoch noch längst keinen Alarm aus, da sie uns Menschen in den meisten Fällen als logische Konsequenz erscheinen. Allerdings kann Reziprozität auch gegen die Interessen eines Menschen genutzt werden. Eine Vielzahl von Verkäufern machen sich die Macht der Reziprozität zu Nutze. Dabei wird bspw. mit einem kleinen Geschenk in Form eines »Kennenlernpakets« o.ä. der potenzielle Kunde dahingehend beeinflusst, einem späteren Kaufangebot zuzusagen, da er »in der Schuld« des Verkäufers steht (Cialdini, 2006).

Dieses Szenario ist nur ein Beispiel von vielen. Grundsätzlich ist jedoch zu erkennen, dass das Ausnutzen der Reziprozität immer das Ziel hat, bestimmte Handlungen beim Opfer auszulösen. Im Kontext des Social Engineering kann dies die Preisgabe kritischer Daten sein. Wie bei einem im vorigen Kapitel beschriebenen Automatismus, liegt die Gefahr der Reziprozität darin, dass Menschen im täglichen gesellschaftlichen Leben darauf angewiesen sind und demnach von ihrer Korrektheit überzeugt sind.

3.3.3 Konsistenz

Der Begriff *Konsistenz* bezieht sich im Kontext der Soziologie auf den logischen Zusammenhang von Worten, Meinungen und Taten einer Person. Menschen haben gesellschaftsbedingt das Bedürfnis in dem was sie tun, sagen und glauben konsistent zu sein. Der Grund dafür liegt darin, dass in unserer Gesellschaft ein hohes Ansehen genießt, wer erlässlich und grundsatztreu handelt. Menschen, die regelmäßig ihre Meinung ändern, gelten gemeinhin als unberechenbar und nicht vertrauenswürdig. Persönliche Konsistenz stellt zudem auch in der täglichen Entscheidungsfindung ein verlässliches Werkzeug dar. So lassen sich mit überschaubarem zeitlichen Aufwand Entscheidungen treffen. Die Zeitersparnis ergibt sich daraus, dass nicht mehr alle relevanten Informationen überprüft werden und genau an dieser Stelle liegt die Gefahr einer bedingungslos konsistenten oder auch konsequenten Handlungsweise. Diese können auch dazu genutzt werden, bestimmte Aktionen einer Person zu erzwingen (Cialdini, 2006).

Ein bekannter Überzeugungstrick ist es, die Zielperson zu einem Statement zu bringen. Durch diese Aussage nimmt sie eine Position ein. Das Prinzip der Konsistenz führt nun dazu, dass diese Person in folgenden Handlungen durch dieses Statement beeinflusst wird. Davon hängt letztlich auch ab, ob die Zielperson der Bitte des Angreifers nachkommt. Dabei ist das folgende Szenario vorstellbar:

Der Angreifer nähert sich einem Rezeptionisten in einem Krankenhaus, um Informationen (Zimmer, Zustand, etc.) über einen Patienten zu erhalten. Das Gespräch könnte wie folgt ablaufen:

Angreifer: "Guten Tag. Sie scheinen sehr gut darin zu sein, Leuten zu helfen."
Rezeptionist: "Ja, das ist mein Job."
Angreifer: "Wären Sie dann so freundlich und sagen mir in welchem Zimmer sich Patient XY aufählt?"
Rezeptionist: "Natürlich. Patient XY liegt in Zimmer 4711."

So oder so ähnlich kann sich ein solches Gespräch abspielen. Natürlich hängt der Erfolg eines Manövers dieser Art auch stark von den schauspielerischen Fähigkeiten des Angreifers ab, ob eine solche Aktion glückt. Die Essenz dieses Angriffs ist und bleibt jedoch das Konsistenz-Prinzip. Der Rezeptionist macht hierbei eine Aussage über seine Fähigkeit Menschen eine gewünschte Auskunft zu geben. Das Nicht-Preisgeben der Information würde demnach gegen das Konsistenz-Bewusstsein der Zielperson verstoßen. Wie stark dieses Bewusstsein ist, hängt wie im vorigen Kapitel zur Reziprozität beschrieben ebenfalls von der vorangegangenen Handlung ab. In diesem Fall handelt es sich dabei um die Intensität des gemachten Statements.

Faktoren, die die Auswirkungen eines solchen Statements verstärken, sind Aktivität des Opfers (wird das Statement selbst formuliert oder lediglich bestätigt?), Öffentlichkeit (hören andere Leute zu?) und auch die Ungezwungenheit (hat das Opfer das Gefühl zu einem Statement gedrängt worden zu sein?) (Cialdini, 2006). Anders als im bereits aufgeführten Beispiel, kann auch eine genaue Analyse der Zielperson Angriffspunkte offenlegen.

3.3.4 Sympathie

Die in den vorangegangenen Kapiteln beschriebenen Mechanismen lassen sich auch mit anderen »Techniken« kombinieren. Es ist allgemein bekannt, dass es besonders solchen Menschen leicht fällt uns zu Manipulieren, welche uns sympathisch sind. Sympathie wirkt wie ein sozialer Katalysator bei der Überzeugung anderer Menschen. An dieser Stelle soll zunächst erläutert werden, wie Sympathie entsteht und von welchen Faktoren sie abhängt.

Das ausschlaggebendste Kriterium, welches beeinflusst, ob wir eine Person sympathisch finden, ist tatsächlich die körperliche Attraktivität. Besonders bei gut aussehenden Menschen ist der sogenannte *Halo-Effekt* zu beobachten (dt. Heiligenschein-Effekt). Menschen schließen von der äußerlichen Schönheit einer Person direkt auf andere (davon unabhängige) Eigenschaften wie z.B. Kompetenz, Freundlichkeit oder Begabung. Neben körperlicher Attraktivität ist auch die Ähnlichkeit zur Zielperson selbst ausschlaggebend. Hierbei spielen sowohl äußerliche sowie charakterliche Merkmale und auch Ansichten eine wichtige Rolle. Sympathie kann zudem durch die wiederholte Kontaktaufnahme mit der Zielperson aufgebaut werden. Dabei ist es umso förderlicher, wenn mit dem Kontakt eine erfolgreiche Kooperation einhergeht (welcher Art auch im-

mer). Verstärken lässt sich der Effekt auch durch das Erteilen von Komplimenten. Denn durch das Erhalten eines Kompliments tritt zusätzlich der Effekt der Reziprozität in Kraft. Bei einem Kompliment handelt es um eine Art Geschenk, welches es zu erwidern gilt. So äußert die Zielperson bspw., dass sie eine bestimmte Eigenschaft der Person gegenüber schätzt. Somit ist außerdem ein Statement geäußert (»Mein Gegenüber ist nett«), was das Konsistenz-Bewusstsein anspricht (Cialdini, 2006).

Die Sympathie ist demnach bestens dafür geeignet mit anderen manipulativen Werkzeugen eingesetzt zu werden, da sie die Willfährigkeit anderer Menschen verstärkt. Die Sympathie ist gerade deshalb gefährlich, weil sie dem Menschen im Alltag ein bekannter jedoch oberflächlicher Ratgeber ist, welchen Personen man trauen kann bzw. welche man besser meidet.

3.3.5 Autorität und Befehle

Eine gegensätzliche und dennoch überraschend ähnliche Methode Menschen zu überzeugen ist die Macht der Autorität. In unserer Gesellschaft besteht ein starker Druck, was das befolgen von Anweisungen durch eine Autorität betrifft. Damit sind zunächst einmal nur echte Autoritäten gemeint. Gefährlich wird es, sobald Meinungen oder Befehle einer Autorität nur noch hingenommen und nicht mehr hinterfragt werden. Denn hinter solchen Befehlen kann sich ein Fehler verbergen oder eine falsche Autorität in Form eines Social Engineers. Es ist aus diesem Grund wichtig zu wissen, wann eine bestimmte Person für eine Autorität bzw. einen Experten gehalten wird. Meist wird nicht die eigentliche Autorität wahrgenommen sondern nur Symbole, die auf eine solche hindeuten. Bei solchen Symbolen handelt es sich im Speziellen um Kleidung (Arztkittel, Uniform, usw.), auch um Titel (Graf, Prof., Dr. med., etc.) oder andere äußerliche Merkmale wie die Körpergröße (Cialdini, 2006). Die Autoritätshörigkeit, wie wir sie kennen, ist deshalb so oft vorzufinden, da Menschen unserer Gesellschaft darauf gedrillt werden Anweisungen von Autoritäten zu folgen, da diese über mehr Wissen, Macht oder Erfahrung verfügen. Zusätzlich werden Autoritäten auch zur Vereinfachung der eigenen Entscheidungsfindung herangezogen (Mann, 2008).

4 Risikoanalyse und -management

In den vorigen Kapiteln ist das Prinzip von Social Engineering erläutert worden und somit aufgezeigt geworden, wie leicht solche Angriffe von statten gehen können und welche Gefahren im Vergleich zu herkömmlichen Angriffsmethoden bestehen. Dennoch wird das von Social Engineering herrührende Risiko oft unterschätzt. Um diesen Gefahren zielgerichtet entgegenzuwirken, ist es wichtig ein grundlegendes, allgemeines Verständnis von Risikofaktoren, deren Bewertungen und Handhabung zu bekommen. Dieses Kapitel vermittelt zunächst, wobei es sich bei dem Begriff Risiko im Allgemeinen handelt. Es wird außerdem geschildert, aus welchen Gründen meist kein angemessenes Risikomanagement zur Anwendung kommt. Abschließend werden diese allgemeinen Erkenntnisse auf den Bereich der speziellen Risikofaktoren durch Social Engineering Angriffe übertragen (s. Kapitel 4.4).

4.1 Risiken

Risiken im Allgemeinen und ihre Handhabung treten in nahezu allen Situationen des täglichen Lebens auf. Dabei kann es sich um solche trivialer Natur handeln wie der Wahl eines Getränks bis hin zur Entscheidung für oder gegen die Investition in eine Aktie. Auch wenn beide Situationen sehr unterschiedlich anmuten, haben sie sehr viel gemeinsam. Sowohl die Wahl eines Getränks als auch die Investition in eine Aktie bergen ein gewisses Risiko. Offensichtlich bieten die beiden Aktionen unterschiedlich große Risiken, weswegen es notwendig ist, solche Risiken korrekt einzustufen und zu bewerten. Ein wichtiges Merkmal für ein Risiko ist, dass eine jede Entscheidung mit einem Risiko verknüpft ist, wobei es sich dabei auch um die Entscheidung nichts zu tun handeln kann. In Bezug auf Informationssicherheit kann eine Gefahr bedeuten, dass geschäftskritische Daten für nicht-autorisierte Nutzer zugänglich gemacht werden. Trifft man in einem solchen Fall die Entscheidung nichts zu tun, ist das damit verbundene Risiko der Offenlegung kritischer Informationen entsprechend hoch. Die Auseinandersetzung mit Entscheidungen, den damit Verbunden Risiken und den Möglichkeiten des zweckmäßigen Umgangs ist vor allem wertvoll für die positive Beeinflussung zukünftiger Situationen. Die Analyse von Risiken sollte nicht dazu verwendet werden Ereignisse zu erklären welche der Vergangenheit angehören.

In Bezug auf den Umgang mit Risiken gibt es verschiedene Herangehensweisen, welche nicht in der Reinform auftreten, generell jedoch oft wiederzuerkennen sind. Die *fatalistische* Herangehensweise zeichnet sich besonders durch die damit verbundene Passivität aus. Dabei wird davon ausgegangen, dass zukünftige Ereignisse weder abwendbar noch voraussehbar sind. Auffällig ist, dass das Handeln ausschließlich aus Reaktionen besteht. Ein anderes Extrem ist der *fanatische* Ansatz. Hierbei wird von einer konkreten Zukunft ausgegangen, welche man in diesem Zusammenhang als Vision

bezeichnen kann. Abweichungen von dieser Vision in Form anderer Möglichkeiten werden gänzlich ignoriert und lösen auch keine notwendigen Reaktionen aus. Dass diese beiden Handlungsweisen nicht zielführend sind, ist offensichtlich. Allerdings ist auch eine rein wissenschaftliche Beurteilung von Risikosituationen nicht von Nutzen. Ein rein wissenschaftlicher Ansatz ist zwar unvoreingenommen, zeichnet sich jedoch durch die Notwendigkeit einer stichhaltigen Beweislage aus. Da diese für in der Zukunft liegende Ereignisse nicht vorhanden ist, würde der rein wissenschaftliche Ansatz nie zu einer endgültigen Entscheidung führen. Der *pragmatische* Ansatz geht von der Annahme aus, dass die Zukunft zwar ungewiss ist, allerdings nicht gänzlich unvorhersehbar ist. Dabei sollen die Chancen positiv verändert werden, während eine mangelnde Beweislage akzeptiert wird (Borge, 2002).

4.2 Risikomanagement

Der Umgang mit Risiken setzt sich aus mehreren Schritten zusammen. Der erste und wichtigste Schritt ist die Identifizierung von Risiken. Die Schwierigkeit besteht im Grunde darin, dass nicht klar ist, wonach überhaupt gesucht wird. Das liegt an der bislang noch spärlichen Kategorisierung von Risiken. In der Informationssicherheit sind jedoch viele Risiken bereits bekannt, obgleich sich die Methoden schnell weiterentwickeln. Ein Risiko stellt auch die Bedrohung durch Social Engineering Angriffe dar. (Borge, 2002) empfiehlt beim Umgang mit Risiken verschiedene Taktiken. Dabei wird beispielsweise die Vermeidung und Verteilen der Risiken vorgeschlagen. Im Falle von gespeicherten Informationen stellen diese Lösungsansätze allerdings keine brauchbaren Alternativen dar. Zwei Möglichkeiten für den Umgang mit Risiken solcher Art sind zum einen die Versicherung für den Fall, dass ein Schadensfall eintritt, zum anderen die gezielte Absicherung. Da mit dem Verlust solcher Daten an Dritte nicht nur finanzieller Schaden sondern auch ein immenser Imageschaden einhergeht, ist auch die Herangehensweise mit einer Versicherung nicht zweckgemäß. In aller Regel bildet nur ein gezielter Schutz vor Angriffen eine angemessene Art des Risikomanagements.

4.3 Ursachen für schlechtes Risikomanagement

Oft stehen dem korrekten Umgang mit Risiken allerdings einige Hürden im Weg. Zum einen sind es sicherlich Schätzungen und Vereinfachungen, die eine Fehlerquelle bilden. Viel gefährlicher sind jedoch Fehlerquellen menschlicher Natur. Diese Hindernisse zur rationalen Entscheidungsfindung gründen auf grundlegenden Eigenschaften der menschlichen Psyche (welche wiederum die Grundlage für die Techniken des Social Engineering bildet). Menschen neigen häufig dazu die eigenen Möglichkeiten zu überschätzen. Möglichkeiten, denen eine sehr geringe Wahrscheinlichkeit zugeordnet ist, werden oft ausgeblendet und als unmöglich bezeichnet. Die Tendenz bei Menschen geht allerdings dahin, dass dies stärker bei Risiken geschieht, als bei der Wahrnehmung von

Möglichkeiten (Borge, 2002). Die Ursache hierfür ist das Phänomen des menschlichen Optimismus. Negative Resultate werden vielmals unterschätzt und unverhältnismäßig hohe Risiken werden für Chancen mit geringer Aussicht auf Erfolg aufgenommen.

Zum anderen ist oft eine fälschliche Betrachtung vergangener Ereignisse zu beobachten. Im Detail bedeutet das, dass eingetretenen Ereignissen der Vergangenheit im Nachhinein nachgesagt wird, sie seien absehbar gewesen, auch wenn sie vor ihrem Eintreten als unwahrscheinlich eingeordnet worden sind. Mit dieser rückblickenden Betrachtung werden aus optimistischen Herangehensweise resultierende Fehlentscheidungen gerechtfertigt und beschönigt (Borge, 2002).

Vielen Menschen fällt es außerdem schwer an die Beliebigkeit und die Zufälligkeit von Ereignissen zu glauben. Tatsächlich neigen sie dazu nach Mustern zu suchen und Ereignisse in eine Ordnung zu bringen. So werden beispielsweise aus einer Entwicklung über eine relativ kurze Zeit Rückschlüsse für die Zukunft geschlossen. Ähnlich dem Suchen von Mustern geht die Kurzsichtigkeit bei der Beurteilung von Ereignissen einher. Dies kann unter anderem bei Fußballtrainern zu beobachten. Schon eine kurze Serie an Niederlagen, verleitet Fans und Vereinsvorstand die Ursache beim Trainer zu suchen. Viele Trainer werden schon nach kurzen Zeiträumen bereits entlassen, ohne dass eine solide Informationsbasis zur rationalen Entscheidungsfindung existiert hat. Einen Fußballtrainer nach einer Serie von Niederlagen zu entlassen, ist zwar eine harte Entscheidungsfindung, aus risikoanalytischen Gesichtspunkten jedoch immer noch sinnvoller als die Passivität. Die Ursache hierfür liegt darin, dass Menschen eine falsche Aktion negativer bewerten als das Unterlassen einer Aktion, auch wenn die Passivität das schlechtere Ergebnis liefert. Gerade in Bezug auf die Informationssicherheit ist es undenkbar keine Gegenmaßnahmen zu treffen oder im Falle eines Informationsverlustes in Tatenlosigkeit zu verharren.

Eine Bekannte Ursache für eine Fehleinschätzung von Risiken sind ironischerweise Sicherheitsmechanismen wie der Sicherheitsgurt im Auto oder ein verbesserter Algorithmus zur Berechnung des Risikos für Finanzanlagen. Eben diese risikominimierenden Algorithmen sorgen dafür, dass sich der Anwender in Sicherheit wähnt und damit in Summe ein größeres Risiko eingeht, als er ohne diese Absicherung eingegangen wäre.

Der letzte signifikante Punkt, welcher von (Borge, 2002) erwähnt wird, ist die Selbstzufriedenheit des Menschen. Darunter ist zu verstehen, dass dem Menschen bekannte Risiken weniger gefährlich erscheinen als solche, die über seine Gewohnheit hinausgehen. Gerade in Bezug auf Social Engineering ist dieser Punkt erwähnenswert, denn es ist dem Menschen in der Tat eine Gewohnheit, mit anderen Menschen zu interagieren. So fällt es Menschen schwer das Risiko zu erkennen, welches von einem Gespräch ausgehen kann. Grundsätzliche Skepsis ist allerdings ebenso kontraproduktiv und es muss abgeschätzt werden inwiefern Sicherheitsvorkehrungen bei internen und externen Gesprächen eines Unternehmens sinnvoll sind.

4.4 Risikofaktoren des Social Engineering

Bis zu diesem Kapitel wurde das Phänomen Social Engineering und die grundlegende Idee dahinter beschrieben sowie der Umgang mit Risikofaktoren und den Hindernissen der menschlichen Psyche. Social Engineering bildet unbestreitbar einen beachtenswerten Risikofaktor. Dabei gibt es eine Vielzahl an möglichen Szenarien, die beobachtet und analysiert werden können. Leider ist es zu oft der Fall, dass erfolgreiche Angriffe die auf Social Engineering basieren in den seltensten Fällen als solche identifiziert werden. Gerade weil Angriffe dieser Art oft in Kombination mit technischen Methoden angewandt werden, wird ein rein technischer Angriff dokumentiert. Aus diesem Grund und eines allgemein fahrlässigen Risikomanagements wegen wird in vielen Unternehmen die Gefahr von Social Engineering nicht angemessen ernst genommen. Zudem wird der Umgang mit Daten verschiedener Art nicht ausreichend kritisch beleuchtet. Viele Informationen werden oft fälschlicherweise als nicht-vertraulich eingestuft. In vielen Unternehmen besteht jedoch genau an diesem Punkt ein großer Irrtum. Denn aus der Sicht eines Social Engineers gibt es keine irrelevanten Informationen. Für einen Angreifer sind bereits kleine Details zu einzelnen Mitarbeitern hilfreich; auf der Grundlage des Vor- und Nachnamens lassen sich bereits viele weitere Informationen mittels Internetrecherche herausfinden. Auch branchen- oder firmeneigene Fachtermini sind für den Social Engineer von Nutzen. Zwar ist der Schutz vor solchen Auskünften freilich nur schwerlich zu verhindern, jedoch gerät man sehr schnell in eine Grauzone. Man denke dabei nur an Mitarbeiternummern, Nummer einer Kostenstelle oder ein internes Organigramm. Solche von den Mitarbeitern für harmlose Daten gehaltenen Informationen, sind für Social Engineering Attacken leicht gefundene Angriffsziele. Um diese Gefahren einzugrenzen ist es für Unternehmen wichtig den Mitarbeitern die verschiedenen Bedeutungen vermeintlich nicht-vertraulicher Informationen klar zu machen (Mitnick and Simon, 2006).

5 Umfrage

Bis hierhin ist geschildert worden, worum es sich bei Social Engineering handelt, welche Techniken dabei zum Einsatz kommen und wie das damit verbundene Risiko einzuschätzen ist. Um die tatsächlichen Anfälligkeiten zu überprüfen ist im Rahmen der Studienarbeit eine Umfrage durchgeführt worden, bei welcher verschiedene berufstätige Personen zu verschiedenen Themen befragt wurden. Die Umfrage mit dem Titel »Hilfsbereitschaft und Social Engineering« und die daraus gewonnenen Ergebnisse werden im folgenden vorgestellt, aufbereitet und diskutiert. Ebenfalls wird die Vorgehensweise skizziert.

5.1 Fragebogen

Für die Verteilung und Erstellung wurde das Web bzw. die Software Limesurvey verwendet. Die Umfrageergebnisse sind mittels einiger demographischer Daten kategorisiert. Bei den für diese Umfrage erhobenen Daten handelt es sich um das Alter, das Geschlecht, die Berufsgruppe, die Unternehmensgröße sowie die Anzahl der Standorte. Im weiteren Verlauf werden Fragen zu verschiedenen Themenschwerpunkten gestellt. Dabei handelt es sich konkret um Fragen zu Hilfsbereitschaft, Vertrauen, Aufmerksamkeit und einigen abschließenden Fragen zu Social Engineering selbst.

Im ersten Abschnitt (Hilfsbereitschaft) werden Fragen zu Situationen im Arbeitsalltag gestellt. Diese Szenarien sind maßgeblich an den in Kapitel 2.3 vorgestellten Angriffsmustern orientiert und sollen die Anfälligkeit der Probanden nachweisen. Bei den Fragen handelt es sich um Ja/Nein-Fragen, bei denen angegeben werden soll, ob man dazu tendiert die erwartete Handlung auszuführen oder diese zu unterlassen. Bei den ersten drei Fragen handelt es sich um direkte Angriffe bei denen eine gesamte Identität vorgetäuscht wird, die letzte Frage bezieht sich auf die Technik Phone Elicitation. Zudem überprüft die letzte Frage die Mitteilungsbereitschaft gegenüber den anderen Geschlecht.

Die darauf folgende Serie von insgesamt sechs Fragen bezieht sich auf das Vertrauen der Probanden. Dabei gibt es Fragen zu allen der drei Angriffskategorien: Identitätsbetrug, Phone Elicitation und E-Mail-Phishing. Dabei wird das Vertrauen in die Identität von angezeigten Telefonnummern und E-Mail-Adressen (und somit indirekt das bewusste Wissen über Spoofing-Techniken) überprüft. Damit ist die Problematik gemeint, dass eine Person tatsächlich über dieses Thema informiert ist, in der konkreten Situation jedoch nicht daran denkt. Die letzten beiden Fragen zeigen Bilder von jeweils einer Person und sollen prüfen inwiefern die Optik das Vertrauen beeinflusst. Innerhalb dieser Serie sollen Bewertungen des Vertrauens auf einer Skala von eins bis fünf angegeben werden. Dabei steht eins für »kein Vertrauen« und eine fünf für »volles Vertrauen«.

In der folgenden Kategorie werden dem Probanden drei Bilder gezeigt, welche jeweils verschiedene Personen darstellen. Zum einen wird eine Reinigungskraft gezeigt, welche gerade einen Fußboden wischt, zum anderen ein Techniker, der gerade an einer Art Verteilerkasten steht sowie eine Führungskraft. Dabei soll der Proband angeben wie sehr er diese Personen im Arbeitsalltag wahrnimmt. Wie in der vorangegangen Kategorie wird dies mittels einer Skala von eins bis fünf festgestellt. Abschließend werden Fragen zu Social Engineering gestellt. Der Proband wird dabei gefragt, ob er von Techniken wie Spoofing bereits gehört hat. Außerdem soll er eine persönliche Einschätzung des Risikos abgeben.

Die Umfrage selbst ist für den Zeitraum von ca. sechs Wochen öffentlich verfügbar gewesen und ist von freiwilligen Probanden durchgeführt worden. Verteilt wurde die Umfrage weitestgehend mittels sozialer Netze.

5.2 Nachträgliche Betrachtung

Im Rückblick vor allem jedoch durch die Betrachtung der Ergebnisse sind einige Punkte verdeutlicht worden, welche dem Fragebogen Aussagekraft entziehen bzw. Potenzial für weitere Aussagen entzogen haben. Innerhalb der demographischen Daten ist es wie den Ergebnissen des Fragebogens zu entnehmen ist, leider nicht gelungen, die Berufsgruppen sinnvoll abzudecken. Zwar können Kernaussagen darüber getroffen werden, inwiefern sich IT-affine Berufsgruppen von solchen Unterscheiden, die sich nicht näher damit beschäftigen, jedoch ist innerhalb letzterer keine Möglichkeit gegeben genauere Erkenntnisse zu gewinnen. Eine granulare Aufteilung ist an dieser Stelle sicherlich interessant und würde für verschiedene Bereiche in Unternehmen einen sinnvollen Aufschluss darüber geben, welche Abteilungen leichter anzugreifen sind als andere. Auch sind andere Merkmale gar nicht erfasst worden wie z.B. die Dauer der Berufstätigkeit oder wie viele verschiedene Berufsgruppen an einem Standort vertreten sind.

Die Fragen, welche Personen zeigen, haben seitens der Auswertung ein großes Potenzial, welches aufgrund der begrenzten Umfragedauer nicht vollständig ausgeschöpft werden konnte. So könnte man zur Fragegruppe Wahrnehmung wesentlich detailliertere Erkenntnisse gewinnen. Gerade in Kombination mit genaueren Angaben im Bereich der Berufsgruppe können hierbei sicherlich nützliche Hinweise herausgearbeitet werden.

Alldem ist hinzuzufügen, dass es sich bei den Ergebnissen letztlich nicht um eine Überprüfung des Ernstfalls handelt sondern lediglich eine theoretische Befragung vorliegt. Unterschiede zu einer Situation wie sie tatsächlich vorkommt liegen vor allem in der persönlichen Distanz der Person. Wird man auf einem Fragebogen mit einer solchen Situation konfrontiert ist es wesentlich besser möglich sich davon zu distanzieren und klarer darüber nachzudenken. Zudem ist dem Probanden dadurch mehr Zeit gegeben. Zwar sind die Probanden zum einen darauf hingewiesen worden, dass es sich um ein anonyme Umfrage handelt, zum anderen wurde darum gebeten die Fragen so zu beant-

worten, dass es dem eigenen Verhalten entspricht, jedoch ist nicht auszuschließen, dass ein kleiner Anteil der Anworten von der tatsächlichen Handlungsart des Probanden abweichen kann.

5.3 Auswertung

Für die Auswertung der Umfrageergebnisse bieten sich verschiedene Ansätze. Neben einem generellen Überblick ist vor allem der Vergleich zwischen Angehörigen der Berufsgruppen »EDV/IT« und anderen aussagekräftig.

5.3.1 Allgemeine Tendenzen

Aus den Umfrageergebnissen lässt sich gut ableiten, welche Art von Täuschungsversuchen bei den Probanden am effizientesten ist. Das angeführte Beispiel des Mitarbeiters mit dem Kuchenblech ist augenscheinlich besonders effizient. Ca. 84% aller Befragten würden eine solche Person in das Gebäude hereinlassen bzw. diesem sogar die Türe aufhalten. Paradoxerweise ist das Ergebnis weniger eindeutig, wenn ein Mitarbeiter lediglich seinen ID-Chip vergessen hat. Nur 33% der Befragten geben in diesem Szenario an, den fremden Mitarbeiter einzulassen. Die Gründe hierfür können verschiedene sein. Um weiterführende Antworten zu finden ist es wichtig zu wissen, womit sich die Probanden in einer solchen Situation beschäftigen, welche Fragen bei diesen aufkommen und vor allem wie diese beantwortet werden. Im zweiten Beispiel kommt durch die Feststellung des Offensichtlichen, dass die fremde Person keinen ID-Chip bei sich trägt, implizit die Frage auf, wo dieser ID-Chip sich befindet. Durch seine bloßes Erscheinungsbild liefert der Angreifer per se keine passende Antwort. Dies führt in vielen Fällen unwillkürlich zu der Frage, ob er oder sie tatsächlich eine Zugangskarte besitzt und zum Unternehmen gehört. Der vermeintliche Kollege mit dem Kuchenblech beantwortet aufkommende Fragen und somit aufkeimendes Misstrauen implizit durch sein Auftreten. Die Frage nach dem ID-Chip erübrigt sich, da der vermeintliche Mitarbeiter offensichtlich nicht in der Lage ist, seine Zugangskarte hervor zu holen bzw. dies nur mit großer Mühe möglich wäre. Er appelliert durch sein Auftreten implizit an der Hilfsbereitschaft der anwesenden Personen und dreht damit die Situation gewissermaßen um. Somit müssten die Anwesenden sich erklären, wenn sie der Person die Hilfe verwehren.

Sicherlich steht die Aktionsbereitschaft auch mit dem Gefahrenpotenzial des Angriffs in Verbindung. Im eben aufgeführten Beispiel ist die Gefahr, dass eine unbefugte Person in das Gebäude eindringt. Wesentlich heikler ist es, wenn fremde Geräte wie z.B. ein USB-Stick an einen Rechner innerhalb des Unternehmens angeschlossen werden. Die Hemmschwelle ist hierfür ist bereits etwas stärker ausgeprägt, wenn auch nicht deutlich. Etwa 54% geben an der Person den Gefallen zu tun.

Sehr deutlich ist das Ergebnis im Bezug auf telefonische Angriffe (Phone Elicitation) durch eine Person des anderen Geschlechts. Sowohl für Frauen als auch für Männer ist festzustellen, dass ein solcher Anruf schnell auf Mistrauen stößt. Ausschließlich 16% der Befragten gaben an Informationen wie z.B. die Mitarbeiternummer auf Anfrage herauszugeben. Dies lässt sich unter anderem durch den fehlenden Pretext der anrufenden Person erklären. Der angerufenen Person bieten sich wenige Möglichkeiten aufkommende Fragen zur Identität des Angreifers implizit zu beantworten. Durch die geringe Persönlichkeit des Anrufs ist auch die Basislinie an Misstrauen bereits wesentlich höher als bei einem tatsächlichen Identitätsbetrug.

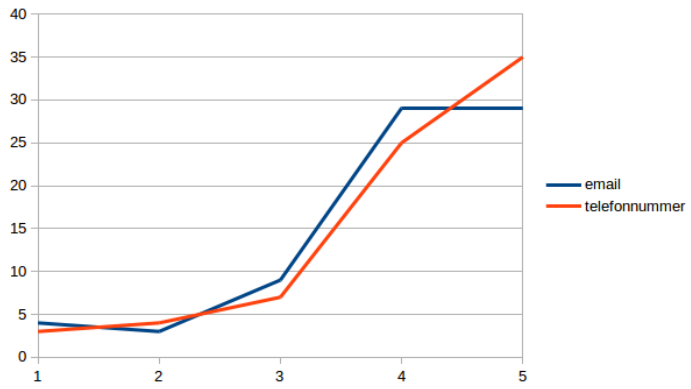

Abbildung 4: Vertrauen in bekannte E-Mail-Adressen und Telefonnummern

Überprüft man das Vertrauen in bekannte Mail-Adressen oder Telefonnummer kann man den Umfrageergebnissen eine deutliche Tendenz zum Vertrauen entnehmen. Abbildung 4 macht deutlich, dass eine signifikante Mehrheit der Mail voll bis bedingt Vertraut. Die Fragestellung selbst legt zwar noch keinen Fokus darauf, jedoch wird das Vertrauen in die Mail auch stark von deren Inhalt beeinflusst. Somit erklärt sich auch dass die Antworten zwischen vollem und bedingtem Vertrauen in etwa gleich gewichtet sind. Nebenbei ist im Ansatz zu erkennen, dass das Vertrauen in eine bekannte Rufnummer etwas stärker ausgeprägt ist als das in eine vertraute E-Mail-Adresse. Dies kann jedoch im Rahmen der Standardabweichung liegen. Um eine solche Hypothese zu untermauern müsste dies mit einer größeren Stichprobe überprüft werden.

Wenig überraschend ist die Aufmerksamkeit, welche bestimmten Personen-/Berufsgruppen im Alltag entgegengebracht wird. Wie aus Abbildung 5 zu entnehmen erfährt eine Putzkraft verglichen mit einer elegant gekleideten Person (Führungskraft oder gehobener Angestellter) weniger Aufmerksamkeit. Die Aufmerksamkeit, welche einem arbeitenden Techniker gilt, ist dazwischen vorzufinden. Aus diesen Ergebnissen ist direkt kein Rückschluss auf Gefahren für ein Unternehmen möglich, jedoch spiegelt es das Risiko für den Social Engineer wider. Je stärker der Angreifer im Fokus der Wahrnehmung anderer steht, desto glaubwürdiger muss sein Auftreten und somit auch die implizite Beantwortung von Fragen zur Identität sein. Für den Angreifer stellt sich natürlich auch die Frage, was er erreichen möchte, denn jeder der drei im

Beispiel aufgeführten Personengruppen stehen unterschiedliche Zugangsberechtigungen zur Verfügung.

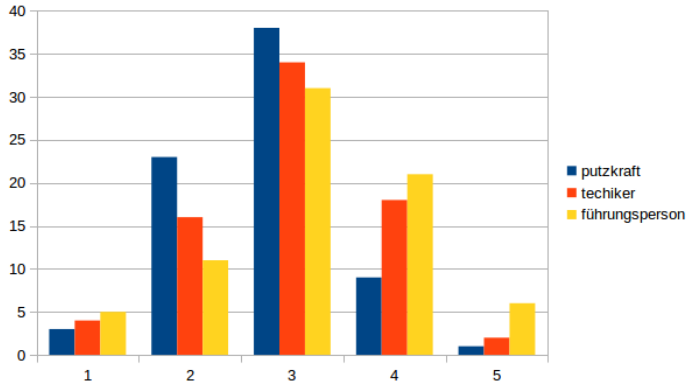

Abbildung 5: Aufmerksamkeit gegenüber verschiedenen Berufsgruppen

Abschließend kann anhand des Szenarios in dem der Hausmeister einige Kisten aus dem Bürokomplex trägt überprüft werden, wie sich das Verhalten seitens der Mitarbeiter bei einer funktionierenden Identität des Angreifers darstellt. Abbildung 6 zeigt deutlich, dass die Mehrheit der Befragten gar keine Reaktion zeigen würde. Nicht einmal 20% tauschen sich über das Gesehene mit ihren Kollegen aus. Aktiv werden lediglich 16% von denen 15% nachfragen, was der Hausmeister in den Kisten transportiert und nur 1% tatsächlich die Identität des Hausmeisters überprüft.

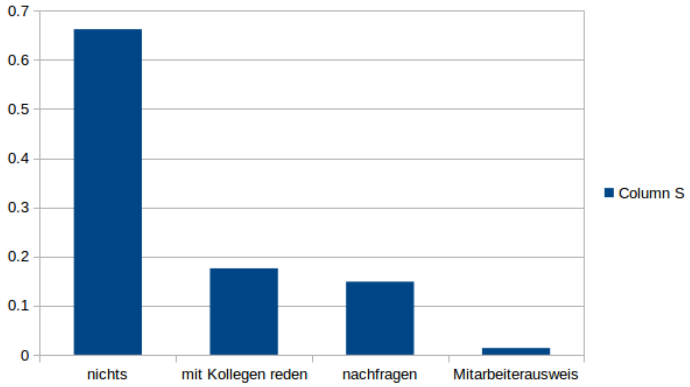

Abbildung 6: Reaktion auf verdächtiges Verhalten einer funktionierenden Identität

Zudem wurde das Wissen der befragten Personen zum Thema Social Engineering überprüft. Dabei wurde gefragt, ob der Begriff *Social Engineering* bekannt ist, die Person von Techniken wie Telefon-Spoofing weiß oder ob ihr klar ist, dass der angezeigte Linkname von der tatsächlichen Referenz abweichen kann. Anhand der Ergebnisse, wie sie in Abbildung 7 zu sehen sind, wird ersichtlich, dass die Mehrheit von diesen Techniken weiß. Dass dies jedoch vor Angriffen schützt ist in keiner Weise garantiert.

An dieser Stelle sei noch einmal betont, dass es sich hierbei um eine allgemeine Auswertung handelt. Ob sich zwischen verschiedenen Berufsgruppen die Wahrnehmungs-

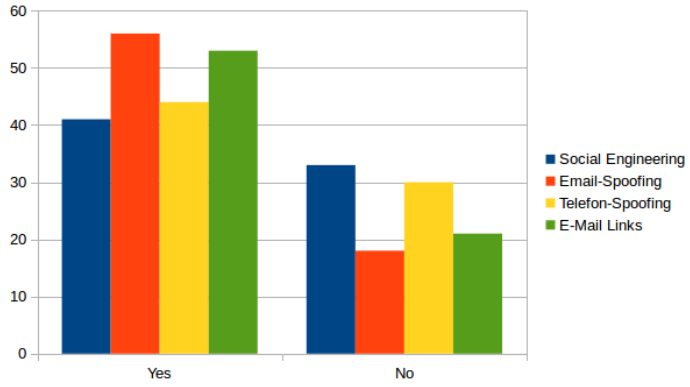

Abbildung 7: Wissen über Social Engineering und Techniken

verteilung ändert, ist zunächst nicht abzuleiten. Das nächste Kapitel zeigt Unterschiede zwischen den verschiedenen Berufsgruppen auf.

5.3.2 Berufsgruppenorientierte Auswertung

Von besonderem Interesse ist vor allem der Vergleich zwischen der Berufsgruppe der EDV/IT-Mitarbeiter mit IT-fremden Berufsgruppen. Im Vergleich zu anderen Berufsbildern haben Mitarbeiter der EDV/IT meist indirekt oder auch direkt mit der Sicherheit der Daten zu tun. Oft ist für den Datenschutz ein Team aus der EDV-Abteilung verantwortlich. Somit lässt sich vermuten, dass solche Personen sensibler für bestimmte Angriffstechniken sind und grundsätzlich wachsamer und informierter sind. Bei vielen Szenarien und Fragestellungen können jedoch keine signifikanten Unterschiede festgestellt werden. Das Vertrauen in bekannte E-Mail-Adressen und Rufnummern ist im Vergleich zur gesamten Stichprobe ähnlich verteilt. Ebenso gestaltet sich die Wahrnehmung verschiedener anderer Berufsgruppen übereinstimmend.

Kleinere Unterschiede ergeben sich unter anderem bei der Auswertung der Handlungsmuster. Während das Verhalten auf den Mitarbeiter mit dem Kuchenblech und dem ohne ID-Chip dem der allgemeinen Auswertung ähnelt, ist ein Unterschied bei dem Szenario mit dem USB-Stick einer unbekannten Person zu beobachten. Während Angehörige anderer Berufsgruppen zu ca. 60% dieser Person den Gefallen erweisen würden, sind unter den EDV-Mitarbeitern der Probanden lediglich 40% zu finden. Dies lässt sich sicherlich auf die Aufgeklärtheit des Personenkreises über die Gefahren eines harmlos erscheinenden USB-Speichers zurückführen. Nichtsdestotrotz birgt eine Erfolgsrate von 40% (aus der Sicht eines Angreifers) immer noch ein nicht zu unterschätzendes Potenzial für Angriffe.

5.3.3 Altersorientierte Auswertung

Das Alter betreffend wären verschiedene Argumentationen denkbar. Zum einen ließe sich behaupten altere Mitarbeiter, d.h. 30 Jahre oder älter, seien gegenüber Social

Engineering Angriffen besser gewappnet, da sie mit mehr Erfahrung ausgestattet sind und zudem weniger zu leichtsinnigen oder unüberlegten Handlungen tendieren. Dem entgegensetzen könnte man die Tatsache, dass die aus dieser Erfahrung resultierende Routine bei geschickt gestellten Anweisungen einem Social Engineer zu seinem Erfolg verhelfen kann. In Anbetracht der zugrunde liegenden Umfrageergebnisse kann jedoch keine dieser beiden Thesen untermauert werden. Zwar sind minimale Abweichungen innerhalb der Szenarien mit dem Mitarbeiter mit Kuchenblech, dem USB-Stick und dem fehlenden ID-Chip zu sehen, jedoch besitzen diese bei weitem keine Differenzen sie als signifikant bezeichnen zu können.

Bei einem Blick auf die Fragen bezüglich der Wahrnehmung gegenüber anderen Berufsgruppen ist bei den jüngeren Probanden eine Tendenz zu erkennen, Putzkräften überdurchschnittlich wenig Beachtung zu schenken. Dies könnte ein Anhaltspunkt für einen Social Engineer sein, der z.B. vor der Aufgabe steht die Räumlichkeiten eines Unternehmens mit vielen jungen Mitarbeitern auszukundschaften. Eine Ähnliche Tendenz ist bei der Berufsgruppe der Techniker zu erkennen.

Das Wissen um die technischen Möglichkeiten eine falsche Identität erfolgreich vorzutäuschen ist in den Köpfen der jungen Probanden präsenter. Dies lässt sich durch die geringere Distanz zu technischen Neuerungen und Möglichkeiten im Allgemeinen erklären. Dies wiederum könnte einen Angreifer zu der Überlegung bringen ein Unternehmen mit einem hohen Durchschnittsalter der Mitarbeiter per Phone Elicitation oder mittels gespoofter E-Mail-Adressen anzugreifen.

Am Rande sei noch erwähnt, dass junge Mitarbeiter nach eigenen Angaben Entscheidungen von ihnen nicht persönlich bekannten Führungspersonen kritischer Beäugen als ihre älteren Kollegen. Abbildung 8 zeigt deutlich, dass nur eine kleine Minderheit die Entscheidungen eines Vorgesetzten unkritisch entgegen nimmt. Der Großteil steht dieser Entscheidung bzw. neutral gegenüber. Bei älteren Mitarbeitern ist diese Ausprägung weniger deutlich.

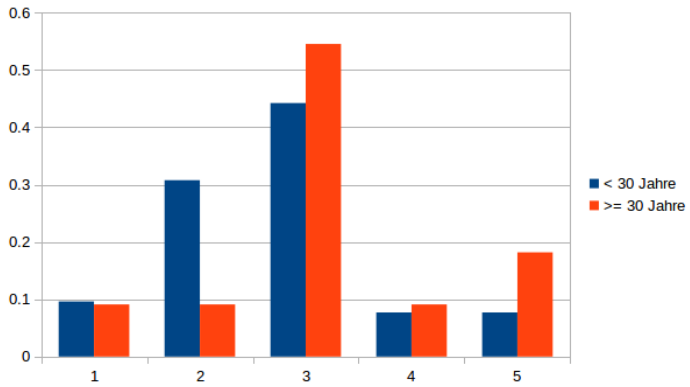

Abbildung 8: Kritische Beurteilung von Entscheidungen unbekannter Führungsperson

5.3.4 Unternehmensbezogene Auswertung

Unternehmen seien an dieser Stelle anhand zweier Ausprägungen zu unterscheiden. Zum einen lassen sich Unternehmen auf ihre Größe bezogen unterscheiden (messbar durch die Zahl der Mitarbeiter), zum anderen ist ein wichtiges Merkmal die Ausdehnung des Unternehmens (messbar durch die Zahl der Standorte). Um ein abgerundetes Bild der Umfrage zu erhalten, ist es wichtig neben den bisher aufgeführten Aspekten auch die unternehmensspezifischen Auswirkungen zu untersuchen.

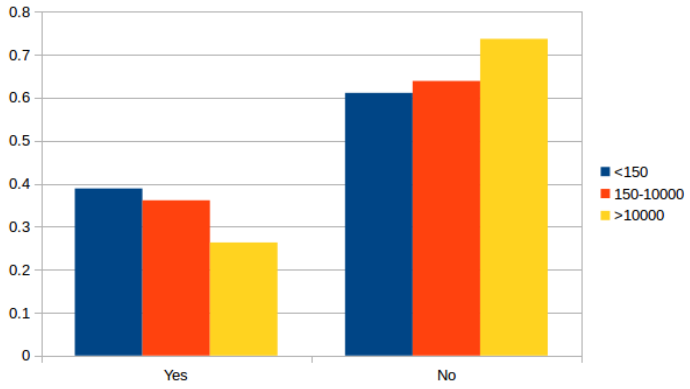

Abbildung 9: Reaktionen bezogen auf die Unternehmensgröße

Größtenteils sind die Tendenzen zwischen verschiedenen Unternehmensgrößen identisch und decken sich mit den bisher gewonnenen Erkenntnissen. Jedoch kann eine leichte Steigerung der Wachsamkeit mit wachsender Unternehmensgröße festgestellt werden. Abbildung 9 zeigt dies anhand des ID-Chip-Szenarios. Zwar neigen kleine, mittelständische und große Unternehmen alle dazu den vermeintlichen Mitarbeiter nicht ohne weiteres passieren zu lassen, jedoch steigt diese Ausprägung mit wachsender Mitarbeiterzahl.

Ähnliche Beobachtungen lassen sich auch bei Betrachtung der Ausbreitung machen. Eine mögliche Erklärung hierfür ist, dass es sich bei großen und verbreiteten Unternehmen etablierte Konzerne handelt, bei denen Informationssicherheit und Datenschutz einen enormen Stellenwert besitzt. Kleine oder mittelständische Unternehmen hingegen haben in der Regel noch kein ausgereiftes und vor allem kein ganzheitliches Sicherheitskonzept in Betrieb. Bei Großkonzernen sind viele der später in Kapitel 6 vorgestellten Gegenmaßnahmen bereits implementiert.

5.4 Anhaltspunkte für weitere Untersuchungen

Die aus der Umfrage gewonnenen Erkenntnisse geben bereits ein gutes allgemeines Bild wieder. Auch lassen sich anhand der spezifischen Auswertungen bereits genauere Rückschlüsse ziehen. In den auswertenden Kapiteln war jedoch zu erkennen, dass diese Untersuchungen nur der Oberfläche einiger Themen kratzen. Ein interessanter Anhaltspunkt für weitere Untersuchungen sind genauere Analysen einzelner Personengruppen.

Eine detaillierte Übersicht von verschiedenen Altersgruppen könnte Ausgangspunkt für eine weitere Untersuchung sein. Die Fragestellungen und Szenarien selbst können ebenfalls stärker fokussiert werden. Hierfür bietet es sich an Einbruchstechniken wie das Szenario mit dem Kuchen in vielen abgewandelten Formen zu überprüfen. Schwerpunkte können jedoch auch auf Themen wie die Wirkung der Körpersprache, einer E-Mail oder bestimmter Kleidung gelegt werden.

6 Human Hardening

Bislang wurden in der vorliegenden Arbeit ausschließlich die Gefahren diskutiert, die mit Social Engineering einhergehen. Es wurden die zugrunde liegenden Konzepte erklärt und auch eine konkrete stichprobenartige Analyse durchgeführt, um die Risiken besser einordnen zu können. An diesem Punkt besteht eine demütige Einstellung gegenüber den Gefahren des Social Engineering. Allerdings sind Unternehmen und auch Privatpersonen solchen Angriffsmethoden nicht gänzlich ausgeliefert. Es bestehen neben maßgeschneiderten Konzepten zum Schutz auch bereits viele Gegenmaßnahmen, welche größtenteils out-of-the-box ohne größere Anpassungen die Datensicherheit maßgeblich steigert. Diese Lösungsansätze bezeichnet man im Allgemeinen auch als *Human Hardening*. Der erste Schritt zum Schutz vor Social Engineering ist bereits getan, denn das Wissen um die Existenz und um die hierfür eingesetzten Werkzeuge und Kenntnisse bietet eine gute Grundlage für effektive Ansätze.

Es stellen sich in diesem Zusammenhang viele Fragen unter anderem wie man in einem Unternehmen Schwachstellen ausmacht, diese systematisch verbessert und die positiven Auswirkung dieser Verbesserungen sicherstellt. Hierfür werden bewährte Methodiken vorgestellt. Auch werden im Folgenden gängige Techniken und deren unmittelbare Einsetzbarkeit aufgezeigt.

6.1 Klassifizierung von Informationen

Die Leitfrage zur Absicherung gegen Social Engineering Angriffe ist neben der offensichtlichen Fragestellung, wie der Schutz letztlich gewährleistet wird, was geschützt werden soll. An dieser Stelle ist es sinnvoll sich klar zu machen, dass es sich bei Hacking-Angriffen aller Art um Kriegsführung handelt und nichts beschreibt eine solche Situation besser als folgendes Zitat von Napoleon: »War is 90 % Information.« (Jones, 2015) Und eben so bedacht sollte im Unternehmen mit Informationen jeder Art umgegangen werden. Denn unglücklicherweise gibt es für einen Angreifer prinzipiell keine nutzlosen Informationen. Genauso ist es für jedes Unternehmen absolut unmöglich keine Informationen über sich zu veröffentlichen. Im Kapitel 4 zur Risikoanalyse wurden bereits Anmerkungen dahingehend gemacht, dass der Wert und damit die Gefahr hinter vermeintlich uninteressanten Informationen oft unterschätzt wird und somit falsch mit ihnen umgegangen wird. (Mitnick and Simon, 2003) Im folgenden seien einige kritischen Informationen genannt:

- Adressen einzelner Standorte
- Telefonverzeichnisse und Durchwahlen
- Unternehmensstrukturen
- Firmeninterne Termini

- Informationen über einzelne Mitarbeiter
- Sitzungsprotokolle der Geschäftsleitung

Während es noch realistisch erscheint bestimmte Telefondurchwahlen oder ein Telefonverzeichnis geheim zu halten, so scheint es ein Ding der Unmöglichkeit zu sein, Informationen über Mitarbeiter oder gar die Adressen von Standorten geheim zu halten. Das Problem ist die Notwendigkeit Daten preiszugeben um sinnvoll mit Geschäftspartnern und Kunden zu arbeiten. Eine weitere Schwierigkeit ist die fehlende Kontrolle über diese Preisgabe. Zu Zeiten von Facebook, Twitter und anderen sozialen Netzwerken ist es für Social Engineers leichter denn je an Informationen von Mitarbeitern zu kommen und dies mit einem geringen Aufwand. Selbstverständlich gilt auch bei diesen Daten, dass keine Information für den Angreifer wertlos ist.

Es ist für eine effiziente Absicherung gegen Social Engineering nötig die im Unternehmen enthaltenen Informationen zu klassifizieren. Neben der Klassifikation ist außerdem zu definieren wie mit den verschiedenen Informationen umgegangen werden soll. (Mann, 2008) unterteilt die im Unternehmen befindlichen Daten zunächst in drei Klassen: geheim, vertraulich und öffentlich. Daten welche als *geheim* eingestuft werden, sollen nur ganz bestimmten Personen zugänglich gemacht werden, da sie von besonderem Wert sind. *Vertrauliche* Informationen sollen für Mitarbeiter des Unternehmens oder für vertrauenswürdige Partnerunternehmen verfügbar sein. *Öffentliche* Daten sind solche, deren Zugänglichkeit jedem beliebigen Menschen gewährt werden kann. Diese Abstufungen bieten zunächst eine gute Orientierung. In vielen Fällen kann es dennoch nötig sein die Aufteilung granularer zu definieren. Dabei sei allerdings zu bedenken, dass jede weitere Gruppe auch eine weitere Verhaltensregel mit sich bringt. Sollten zwischen zwei Gruppen nur geringe Unterschiede bestehen, ist es oft sinnvoller diese zu einer zu konsolidieren.

Sind solche Kategorien für die Informationen aufgestellt ist der nächste Schritt für alle denkbaren Aktionen zu formulieren und ob diese für die Informationen der entsprechenden Kategorie erlaubt, nicht erlaubt oder nur mit Einschränkungen genehmigt sind. Es ergeben sich daraus übersichtliche Tabellen wie z.B. folgende Übersicht für die Aktion per E-Mail versenden.

Klassifikation	**E-Mail-Versand**
Geheim	Nicht genehmigt
Vertraulich	Nur an bekannte Empfänger
Öffentlich	Genehmigt

Tabelle 1: Richtlinien für den E-Mail-Versand von Informationen

Mit Tabellen wie z.B. Tabelle 6.1 existieren bereits klar definierte Richtlinien, wie die Mitarbeiter mit den Informationen des Unternehmens umzugehen haben. Diese Listen bieten eine gute Ausgangssituation für erste provisorische Gegenmaßnahmen

indem sie an Mitarbeiter weitergeleitet werden. Bedenkt man allerdings die Mengen an E-Mails, die pro Tag bei einem Mitarbeiter eintreffen, relativiert sich die Wirksamkeit dieser Methode schnell. Wie sehr diese Regeln beachtet werden hängt von verschiedenen Faktoren ab, vor allem jedoch wie glaubwürdig und sinnvoll diese neuen Richtlinien präsentiert werden. Letzten Endes handelt es sich bei diesem Lösungsansatz nur um eine oberflächliche Schutzmaßnahme. Mitarbeiter wissen so nur welche Aktionen mit welchen Daten genehmigt sind, was per se bereits eine enorme Verbesserung ist, jedoch wissen die Mitarbeiter dies bereits. Ein geübter Social Engineer wird jedoch versuchen Angestellte zu eben solchen unerlaubten Aktionen verführen. Dabei spielt es letztlich keine Rolle mehr ob es schriftlich festgehalten ist. Um Mitarbeiter vor solchen Angriffen tatsächlich zu schützen hilft nachhaltig nur eine Methode.

6.2 Schulungen für Mitarbeiter

(Social-Engineer.Org, 2014) sowie (Mann, 2008) halten die Schulung von Mitarbeitern in Bezug auf Wissen über Social Engineering und Wachsamkeit im Arbeitsalltag für die nachhaltig effektivste Lösung. Denn wie bereits angedeutet sind Mitarbeiter nicht nur während der Arbeit potenzielle Angriffsziele sondern auch in ihrer Rolle als Privatperson eine wichtige Schnittstelle zum Unternehmen für einen Social Engineer. Um die Gefahr solcher unwissentlichen *Insider* zu mindern ist die Schulung ein besonders guter Ansatz, da es dem Mitarbeiter selbst die Fähigkeit verleiht Manipulationen zu erkennen. Da auch der Inhalt von Schulungen nur bedingt wahrgenommen wird und den Teilnehmern im Gedächtnis bleibt, sollte bereits bei der Gestaltung der Themen klar sein, worauf die Veranstaltung hinauslaufen soll. (Hadnagy, 2011) beschreibt folgende Ziele: Der Mitarbeiter soll

- Informationssicherheit bewusst ernst nehmen.
- wissen worauf er im Arbeitsalltag achten muss.

Hierfür bieten sich zwei Möglichkeiten an. Zum einen ist eine direkte Schulung denkbar, bei der die Mitarbeiter persönlich für die Thematik sensibilisiert werden. Eine weitere Methode stellt ein interaktives Online-Training dar. Auf den ersten Blick scheint die persönliche Unterweisung der Mitarbeiter die beste Variante zu sein. Sicherlich wird das Wissen am effektivsten in einem direkten Dialog vermittelt und es bleibt meist auch länger im Gedächtnis und erreicht eher das Unterbewusstsein. Doch diese Vorteile haben ihren Preis. Eine persönliche Schulung der Mitarbeiter ist äußerst ressourcenintensiv. Zum einen sind Angestellte für den Zeitraum der Schulung blockiert, zum anderen kostet jedoch auch die Vorbereitung eines solchen Seminars viel Zeit. In Bezug auf die Ressourceneinteilung bietet das interaktive Training am PC eine gute Alternative. Es besteht für den Mitarbeiter hierbei allerdings die Möglichkeit bei

Sicherheits-Stufe	Umfang der Schulung	Zugriffsberechtigungen
Hoch	Sehr umfangreich, möglichst häufig, spezielle Gegenmaßnahmen	Direkter Zugriff auf kritischen Informationen
Mittel	Initiale Einführung, regelmäßig über Sicherheitsmaßnahmen informieren	Möglicher Zugriff auf kritische Informationen
Niedrig	Stellenspezifische Anweisungen	Kein Zugriff auf kritische Informationen

Tabelle 2: Kategorisierung der Mitarbeiter zu Schulungszwecken nach (Mann, 2008)

der Abarbeitung der Übungen zu betrügen, womit der erwünschte Lerneffekt verloren ginge.

In Anbetracht der im vorigen Kapitel aufgeführten Kategorien ist festzustellen, dass auf hoch sensible Informationen nur wenige Mitarbeiter Zugriff haben. Es lassen sich demnach nicht nur Informationen in Kategorien unterteilen, sondern auch die Mitarbeiter in Gruppen unterteilen. Je heiklere Informationen ein Angestellter wahrt, desto intensiver sollte dieser gegen Social Engineering Techniken gerüstet sein. Liegt eine solche Kategorisierung vor, lassen sich die Schulungsmethoden effizienter planen und es werden allen Mitarbeitern keine überflüssigen Kenntnisse vermittelt. Tabelle 6.2 gibt hierfür eine beispielhafte Unterteilung an.

Wie ein solches Seminar strukturiert sein kann, würde den Rahmen der vorliegenden Ausarbeitung überschreiten. Es sei an dieser Stelle auf das Kapitel 3 Psychologische Grundlagen oder auf andere Quellen wie z.B. (Social-Engineer.Org, 2014) verwiesen. Die dort vorgestellten Prinzipien bilden einen guten Ausgangspunkt um Mitarbeiter an das Thema heranzuführen. Am naheliegendsten ist es dabei auf die Instrumente der Manipulation einzugehen, da diese zu dem offensichtlichsten Handwerkszeug eines Social Engineers gehören. Weiterhin sollte für Angestellten neben den sehr defensiven Gendanken und dem (berechtigten) Misstrauen auch das Prinzip des Vertrauens geklärt werden, denn ohne ein Mindestmaß an Vertrauen ist ein vernünftiges Agieren unmöglich.

7 Diskussion und Ausblick

Im Verlauf der vorliegenden Arbeit wurde zunächst an das Thema Social Engineering herangeführt und einige grundlegende Angriffsmuster beschrieben. Die mit solchen Angriffen erreichte Effizienz ist erschreckend und ist ein klares Zeichen für Unternehmen diese Bedrohung ernst zu nehmen. Vor allem die schwere Aufklärung solcher Methoden macht es schwer genaue Zahlen zu erfassen, denn oftmals stehen hinter scheinbar rein technischen Angriffen die Methoden eines Social Engineers am Anfang der Kausalkette. Zwar ist in sehr großen Konzernen die Gefahr bereits erkannt und korrekt eingeschätzt jedoch ist es vor allem in kleinen Unternehmen und vor allem von mittelständischen noch ernst genug genommenes Thema. Hacking Angriffe zielen zwar meist auf militärische Einrichtungen, Banken oder ähnliche Institutionen ab, jedoch liegt das Risiko für andere Branchen bei weitem nicht bei null. Wie das Kapitel über Risikoanalyse und -management gezeigt hat, werden viele Risiken wie Social Engineering oft nicht ernst genug genommen und zu oft darauf gehofft, dass ein negatives Ergebnis ausbleibt. Gewissenhafte Datenschutzbeauftragte in Firmen sollten demnach überlegen das Unternehmen und seine Mitarbeiter gegen Angriffe dieser Art zu schützen. Problematisch können an dieser Stelle selbstverständlich die aufkommenden Kosten für eine solide Implementierung von Abwehrmaßnahmen sein. Es kann jedoch aktiv ein Verständnis der Vertraulichkeit von Daten gelebt werden, was schon mit wenigen Mitteln stark verbessert werden kann.

Die Umfrage bestätigt in einigen Punkten die Dringlichkeit einer intensiveren Aufklärung. Zwar gaben nur wenige Probanden an einen Mitarbeiter mit defekten/fehlenden ID-Chip einzulassen, jedoch wurde auf Bitten anderer Szenarien weitaus freizügiger reagiert. Zwar gibt es leichte Schwankungen zwischen Berufsgruppen welche in der EDV angesiedelt sind und anderen Berufsgruppen, diese beziehen sich jedoch größtenteils auf Situationen in denen es konkret um Aktivitäten an IT-Geräten geht. Wenn es sich um Zugangskontrollen oder ähnliches handelt gleichen sich die Ergebnisse an. Sicherlich bietet das Grundprinzip solcher Umfragen noch weiteres Potenzial zur genaueren Untersuchung. Einzelne Zielgruppen können genauer analysiert werden, um somit genauere Vorstellungen von den Schwachstellen aufzudecken.

Literaturverzeichnis

Dan Borge. *Wenn sich der Löwe mit dem Lamm zum Schlafen legt : was Entscheider über Risikomanagement wissen müssen.* Wiley-VCH, Weinheim, 1. aufl. edition, 2002. ISBN 3-527-50028-6.

Robert B. Cialdini. *Die Psychologie des Überzeugens : ein Lehrbuch für alle, die ihren Mitmenschen und sich selbst auf die Schliche kommen wollen.* Psychologie Sachbuch. Huber, Bern, 4., korr. aufl. edition, 2006. ISBN 3-456-84327-5. URL `http://swbplus.bsz-bw.de/bsz251165922vlg.htm ; http://swbplus.bsz-bw.de/bsz251165922inh.htm`.

Richard Dawkins. *The Selfish Gene.* Oxford University Press, New York, 1976.

Nitesh Dhanjani, Billy Rios, and Brett Hardin. *Hacking - the next generation: bringing the attack to your network.* O'Reilly Media, Inc., Sebastopol, California, 2009. ISBN 978-0-596-15457-8.

Duden. *Duden – Deutsches Universalwörterbuch.* Bibliographisches Institut, Mannheim, 6 edition, October 2006. ISBN 3411055065. URL `http://www.duden.de/suche/detail.php?isbn=3-411-05506-5`.

R. I. M. Dunbar. *How many friends does one person need? : Dunbar's number and other evolutionary quirks.* Faber and Faber, London, 2010. ISBN 0571253423.

Christopher Hadnagy. *Social engineering : the art of human hacking.* John Wiley, Hoboken, N.J. Wiley Chichester, 2011. ISBN 978-0-470-63953-5. URL `http://opac.inria.fr/record=b1133491`.

Christopher Hadnagy. *Social Engineering enttarnt : [Sicherheitsrisiko Mensch].* mitp, Heidelberg, 1. aufl. edition, 2014. ISBN 978-3-8266-9664-0. URL `http://deposit.d-nb.de/cgi-bin/dokserv?id=4682812&prov=M&dok_var=1&dok_ext=htm`. 201408.

Blaire Jones. 45 more of the best data quotes, April 2015. URL `http://spinnakr.com/blog/data-2/2013/03/44-more-of-the-best-data-quotes/`.

N. Luhmann. *Vertrauen: ein Mechanismus der Reduktion sozialer Komplexität.* UTB Uni-Taschenbücher. UTB, 2000. ISBN 9783825221850. URL `http://books.google.de/books?id=8nL8q_8kcRUC`.

Ian Mann. *Hacking the human : social engineering techniques and security countermeasures.* Gower, Aldershot, 2008. ISBN 0-566-08773-1; 978-0-566-08773-8. URL `http://digitool.hbz-nrw.de:1801/webclient/DeliveryManager?pid=2663685&custom_att_2=simple_viewer`.

K.D. Mitnick and W.L. Simon. *Die Kunst der Täuschung: Risikofaktor Mensch.* mitp, 2006. ISBN 9783826615696. URL `http://books.google.de/books?id=MUK5AUvM3-8C`.

Kevin D. Mitnick and William L. Simon. *The Art of Deception: Controlling the Human Element of Security.* John Wiley & Sons, Inc., New York, NY, USA, 2003. ISBN 076454280X.

Prof. Dr. Stefan Müller. Verhaltensgrundlagen, 2007. URL http://tu-dresden.de/die_tu_dresden/fakultaeten/fakultaet_wirtschaftswissenschaften/bwl/marketing/lehre/lehre_pdfs/Mueller_IM_G1_Kommunikation.pdf.

M. Plate. *Grundlagen der Kommunikation: Gespräche effektiv gestalten*. Uni-Taschenbücher S. UTB GmbH, 2013. ISBN 9783825238551. URL http://books.google.de/books?id=jCFaLQG6cpcC.

Bruce Schneier. *Die Kunst des Vertrauens = Liars and outliers*. mitp, Heidelberg, dt. ausg., 1. aufl. edition, 2012. ISBN 978-3-8266-9216-1; 3-8266-9216-0. URL http://d-nb.info/1023999862/04.

Social-Engineer.Org. 45 more of the best data quotes, October 2014. URL http://www.social-engineer.org/how-tos/change-education-working/.

P. Watzlawick, J. H. Beavin, and D. D. Jackson. *Menschliche Kommunikation: Formen, Störungen, Paradoxien*. Bern: H. Huber, 11 edition, 2007. ISBN 3456834578. URL www.worldcat.org/search?q=isbn:3456834578.

Anhang

Fragebogen..

Eidesstattliche Erklärung

Eidesstattliche Erklärung zur <-Arbeit>

Ich versichere, die von mir vorgelegte Arbeit selbstständig verfasst zu haben. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder nicht veröffentlichten Arbeiten anderer entnommen sind, habe ich als entnommen kenntlich gemacht. Sämtliche Quellen und Hilfsmittel, die ich für die Arbeit benutzt habe, sind angegeben. Die Arbeit hat mit gleichem Inhalt bzw. in wesentlichen Teilen noch keiner anderen Prüfungsbehörde vorgelegen.

$Unterschrift$: $Ort, Datum$: