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:	21. Dezember 2014
Betreuer:	Ralf Brune

Sperrvermerk

Die vorliegende Arbeit beinhaltet interne und vertrauliche Informationen der Firma <Firmenname>. Die Weitergabe des Inhalts der Arbeit im Gesamten oder in Teilen sowie das Anfertigen von Kopien oder Abschriften - auch in digitaler Form - sind grundsätzlich untersagt. Ausnahmen bedürfen der schriftlichen Genehmigung der Firma <Firmenname>.

Zusammenfassung

Abstract

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Listingverzeichnis

Abkürzungsverzeichnis

CMS	Content Management System
CSS	Cascading Style Sheets
ERM	Entity Relationship Modell
GNU	GNU is not Unix
GPL	GNU General Public License
GUI	Graphical User Interface
HTML	Hypertext Markup Language
IM	Instant Message
JS	JavaScript
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
LGPL	GNU Lesser General Public License
OCR	Optical Character Recognition
RSS	Really Simple Syndication
SQL	Structured Query Language
TDD	Test-driven development
UGC	User Generated Content
WWW	World Wide Web
XMPP	Extensible Messaging and Presence Protocol

1 Einleitung

Diese Arbeit behandelt das Thema Social Engineering.

1.1 Aufbau der Arbeit

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

In Kapitel 3 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.

Die psychologischen Grundlagen zum Verständnis von Social Engineering werden in Kapitel 4 erklärt. Dabei sind verschiedene Kommunikationsmodelle, Neuro-Linguistische Programmierung, Transaktionsanalyse und das Zusammenspiel von Bewusstsein und Unterbewusstsein zentrale Themen.

Kapitel 5 stellt einige manipulative Techniken zur Anwendung vor.

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 ein Definition gegeben. Im darauf folgenden Kapitel wird die Einfachheit solche Angriffe gegenüber technischer Angriffe hervorgehoben. Kapitel 2.3 zählt die von Social Engineering herrührenden Risiken für Unternehmen mit kritischen Daten auf und bewertet diese. Zum Schluss (Kapitel 2.4) werden 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 bestehen. 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 eines

Unternehmens. Dies liegt größtenteils an den mangelnden Gegenmaßnahmen die es zu Social Engineering Attacken gibt.

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 Techiken 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 erfreuten sich Social Engineering Angriffe zunehmender Beliebtheit. 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 gerechtfertigt eine übergeordnete Rolle. In jedem Unternehmen finden sehr wirkungsvolle aber auch ebenso kostenintensive Abwehrmechanismen ihre Anwendung. Diese stellen zwar kein unüberwindbares Hindernis dar, halten aber dennoch vielen Angriffen stand oder schrecken bereits vor einem Versuch ab. Während große Sicherheitsfirmen hierfür teure Software- und Hardwarelösungen anbieten, gibt es derzeit kein besonders großes Angebot an Abwehrmaßnahmen, die der Prävention von manipulativen Angriffen auf die Mitarbeiter dienen.

Es liegt also auf der Hand, dass immer mehr Angriffe nicht mehr herkömmlich auf die IT-Systeme direkt gerichtet werden, sondern entsprechende 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 Gängige Angrifffe

In diesem Kapitel werden exemplarisch einige Angriffstechniken vorgestellt und es wird grob 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.

2.3.1 Heimarbeit und Helpdesks

Ein beliebtes Ziel für Social Engineering Angriffe stellen Mitarbeiter dar, die von zu Hause aus arbeiten. Dabei können die Mitarbeiter direkt als Ziel genommen werden. Mitarbeiter, 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 allerdings zweischneidiger Natur. Auch in die andere Richtung können Angriffe vollzogen werden. Dabei wird der IT-Helpdesk als Zielscheibe gewählt. 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.

2.3.2 Neue Angestellte

Dieses Szenario ist zwar etwas seltener anzutreffen aber durchaus 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, ist dies oft ein Indiz dafür, dass es sich um einen Angriff gehandelt haben kann. Um solche Situationen zu verhindern, ist es angebracht für neue Mitarbeiter ausreichende Background-Checks vorzunehmen.

2.3.3 Angriff auf Mitwisser

Manchmal stellt es den Angreifer vor große Probleme das Ziel direkt zu attakieren, da evtl. keine brauchbaren Sicherheitslücken ausfindig gemacht werden können oder das Risiko eines direkten Angriffes zu hoch wäre. Hier bietet es sich für den Angreifer an sich ein kooperierendes Unternehmen als Ziel zu wählen, welches größere Sicherheitslücken aufweist. Die Informationen die Dritte über das Zielunternehmen haben, können entscheidend für den tatsächlichen Angriff bieten. Auf ein solches drittes Unternehmen können dann Methoden wie bereits beschrieben angewendet werden.

2.3.4 Kombination sozialer und technischer Angriffe

Oft ist mit rein manipulativen Mitteln das gewünschte Ziel nicht erreichbar. Dabei nutzen Angreifer häufig eine Mischform von Social Engineering Techniken und herkömmlichen Angriffstechniken. Dafür kann ein Angreifer beispielsweise einen mit Malware infizierten USB-Stick in einer Büroetage liegen lassen. Die Neugier einiger Mitarbeiter wird dabei größer sein als die Vernunft und es ist keine seltenheit, dass ein solcher USB-Stick den Weg in die Buchse eines Mitarbeiter-PCs findet.

EIne sehr bekannte technsiche Methode, die sich Social Engineering Techniken bedient, ist das Senden von Phishing-Mails. Dabei werden an eine große Menge von Zielen E-Mails versendet, die sich verschiedene menschlichen Schwächen zu Nutze machen wie z.B. Leichtgläubigkeit, Kurzsichtigkeit oder Gier. Diese Technik findet allerdings weniger Anwendung bei Angriffen auf Unternehmen. Der Ausbeute eines solchen Angriffs ergibt sich nicht aus einem einzigen Angriff sondern vielmehr aus der Menge. Tatsächlich ist es eine Minderheit im Promillbereich, die auf solche Phishing-Mails reagiert. Sendet der Angreifer 1000000 Mails aus, bei denen pro Aktion 1000 € erbeutet werden können, genügt eine Erfolgsrate von 0,01% um 100 erfolgreiche Angriffe verbuchen zu können, was einem Gewinn von 100000 € entspricht.

3 Risikoanalyse und -management

In den vorigen Kapiteln ist das Prinzip von Social Engineering erläutert worden und somit klar 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 der Handhabung mit ihnen zu bekommen. Dieses Kapitel vermittelt zunächst wobei es sich bei dem Begriff Risiko im Allgemeinen handelt. Es wird außerdem geschildert wie man mit bereits erkannten Risiken umgehen kann (Kapitel 3.1.1) und aus welchen Gründen Risiken meist kein angemessenes Risikomanagement seine Anwendung findet. Abschließend werden diese allgemeinen Erkenntnisse auf den Bereich der speziellen Risikofaktoren durch Social Engineering Angriffe übertragen (Kapitel 3.2).

3.1 Allgemeines

Risiken im Allgemeinen und ihre Handhabung treten in nahezu allen Situationen des täglichen Lebens auf. Dabei kann es sich um solche Situationen trivialer Natur handeln wie der Wahl eines Getränks bis hin zur Entscheidung für oder gegen die Investition einer Aktie. Auch wenn beide Situationen sehr unterschiedlich anmuten, haben sie doch sehr viel gemeinsam. Sowohl die Wahl eines Getränks als auch die Investition in eine

Aktie bilden ein gewisses Risiko. Offensichtlich bieten die beiden Aktionen unterschiedliche große Risiken, weswegen es notwendig ist solche Risiken korrekt einzustufen und zu bewerten. Ein wichtiges Merkmal für ein Risiko ist, dass ein jedes Risiko mit einer Entscheidung 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 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 verschieden charakterisierte Herangehensweisen, welche freilich nicht in der Reinform auftreten, aber generell 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 aber 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, aber nicht gänzlich unvorhersehbar ist. Dabei sollen die Chancen positiv verändert werden, während eine mangelnde Beweislage akzeptiert wird.

Dan Borge S. 1-8, 21-39

3.2 Risikomanagement

Der Umgang mit Risiken setzt sich aus mehreren Schritten zusammen. Der erste aber auch schwierigste 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.

Gängige Werke zum Thema Risikomanagement empfehlen beim Umgang mit Risiken verschiedene Taktiken. Dabei wird beispielsweise die Vermeidung, das Verkaufen 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.

// to do: Vorgehensweise für Risk-Management in IT-Sec recherchieren
Dan Borge S. 45-58

3.3 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 solche 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 grundsätzlich 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. 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.

Des Weiteren 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.

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 ist 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 wieder entlassen, ohne dass eine solide Informationsbasis zur rationalen Entscheidungsfindung existiert.

Einen Fußballtrainer nach einer Serie von Niederlagen zu entlassen, ist zwar eine harte Entscheidungsfindung, aber aus risikoanalytischen Gesichtspunkten immer noch sinnvoller als die Trägheit des menschlichen Verhaltens. 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 fühlt und damit in Summe ein größeres Risiko eingeht, als er ohne diese Absicherung eingegangen wäre.

Der letzte signifikante Punkt 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 eine es muss abgeschätzt werden inwiefern Sicherheitsvorkehrungen bei internen und externen Gesprächen eines Unternehmens sinnvoll sind. Das Finden dieser Balance wird im Kapitel 10 Gegenmaßnahmen genauer erörtert.

// to do: weitere Recherche Tversky, Kahnemann

Dan Borge S. 61-72

3.4 Social Engineering als Risikofaktor

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 seltensteten 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.

4 Ausblick

5 Fazit

Literaturverzeichnis

Anhang

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.

$Unterschrift$: $Ort, Datum$: