



Social Engineering in sozialen Netzwerken

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

eingereicht von

Doris Herman
is101502

im Rahmen des
Studiengangs Information Security an der Fachhochschule St. Pölten

Betreuung
Betreuer: Mag. Simon Tjoa

St.Pölten, 22.06.2012

(Unterschrift Autor/Autorin)

(Unterschrift Betreuer/Betreuerin)

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.
- Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

St.Pölten, 22.06.2012

(Unterschrift Autor/Autorin)

Zusammenfassung

Soziale Netzwerke, die Teil des Web 2.0 sind und auch „Mitmachinternet“ genannt werden, gewinnen immer mehr an Beliebtheit und dadurch auch an Bedeutung. Mit dieser Entwicklung ergeben sich aber auch neue Gefahren durch weiterentwickelte Angriffsformen. Durch diese sozialen Netzwerke hat sich auch die Angriffsform Social Engineering weiterentwickelt und stellt eine Gefahr für die Nutzer dieser Dienste dar.

Diese Entwicklungen und neuen Möglichkeiten das soziale Netzwerk auszunützen werden in dieser Diplomarbeit näher erläutert. Für diese Arbeit wurden die derzeit populären sozialen Netzwerke Facebook und Twitter betrachtet.

Als weiterer Punkt der Arbeit werden die Arten der Informationssammlung näher beschrieben. Diese Informationssammlung wurde durch die sozialen Netzwerke weiterentwickelt und zum Teil auch sehr vereinfacht. Social Engineers haben es im jetzigen Zeitalter viel leichter an Informationen heranzukommen, als dies noch vor einigen Jahren der Fall war. Heute gibt es schon zahlreiche Möglichkeiten, nützliche persönliche Informationen aus dem Web herauszufinden und hier spielen die sozialen Netzwerke eine bedeutende Rolle. Es war noch nie so einfach wie in der heutigen Zeit, an so viele persönliche Informationen mit so einfachen Mitteln und in so kurzer Zeit zu kommen. Natürlich wurden auch hier Entwicklungen gemacht, solche Informationen automatisch zu bekommen oder zu „ergaunern“, denn nur weil es möglich ist heißt es nicht, dass es auch erlaubt ist. Es werden einige Möglichkeiten zur automatischen Datensammlung in dieser Arbeit vorgestellt, von einer Vollständigkeit kann keine Rede sein, zumal es auch hier sicher täglich neue Formen gibt.

Ein weiterer wichtiger Punkt der Arbeit ist die Darstellung, was die Nutzer wirklich in diesen Netzwerken eintragen und veröffentlichen. Hierfür werden Statistiken benutzt, die sehr gut veranschaulichen, welche Informationen veröffentlicht werden. Auch wenn viele Nutzer meinen die Informationen sind alle privat und können nur von den Freunden gesehen werden, so hat die Praxis schon oftmals bewiesen, dass dies nicht der Fall ist. Das Internet ist öffentlich und somit auch in gewisser Weise die Daten. Es gibt zahlreiche Möglichkeiten an die Informationen heranzukommen obwohl man nicht mit den Personen befreundet ist.

Anschließend werden die Angriffsszenarien vorgestellt die am häufigsten benutzt werden und auf Social Engineering basieren. Hier hat sich herausgestellt, dass Identitätsdiebstahl, Cyber Mobbing und Phishing die Hauptangriffsszenarien sind, welche Mithilfe von sozialen Netzwerken und innerhalb von sozialen Netzwerken häufig betrieben werden. Auch diese Formen werden mittels Statistiken veranschaulicht.

Auf diesen Ergebnissen basierend, wird anschließend ein Vorschlag für die Verwundbarkeitsdarstellung gemacht, um zu verdeutlichen, wie verwundbar die Nutzer sind, wenn sie persönliche Daten veröffentlichen. Auch wenn man die Nutzer nicht davon abbringen kann soziale Netzwerke zu nutzen, so sollte man wenigstens versuchen sie darauf hinzuweisen, mit diesen Medien behutsamer bzw. vorsichtiger umzugehen. Dieses Schulen bzw. Aufmerksam machen wird im letzten Kapitel „Maßnahmen“ dargestellt.

Die Ergebnisse dieser Forschungsarbeit zeigen, wie gefährlich soziale Netzwerke sein können und wo man besonders aufpassen muss. Weiters werden Maßnahmen vorgeschlagen um die Gefahren möglichst gering zu halten bzw. um die Angriffe nicht so leicht zu ermöglichen.

Die Kernaussage dieser Arbeit ist aber, dass man soziale Netzwerke sehr wohl nutzen kann, aber immer mit Vorsicht und zuerst überlegen was man schreibt

Abstract

Social networks are part of the Web 2.0, are also called "participatory web" are getting more popular, and therefore also more important. This development leads to new risks, arising from new advanced forms of attack. The use of these new social networks resulted in new forms of social engineering attacks developed and represent a threat for the user of the social networks.

These developments and new opportunities to capitalize the social network are explained in detail in this thesis. In this thesis the following popular social networks Facebook and Twitter are considered. An additional key aspect of this work is the detailed description of the types of information collection. This collection of information was further developed through the use of social networks and is getting much easier. For social engineers it is a lot easier to get information today, than it was a few years ago. Today there are many useful ways to find personal information in the Web and social networks play an important role. It was never as easy as it is today, to get so much personal information in such a short time. Also developments have been made to collect the information automatically or to grift the information, because that it is possible does not mean that it is allowed too. Part of this thesis is also the introduction of automated information collection. Due to the daily changing developments in this area the list is not exhaustive.

Another important point of this work is to present what information users add and publish on these networks. Statistics are used to demonstrate which information is published. While many users think that all the information is private and can only be seen by the friends, the practice has been proven different in many cases. The Internet is public and therefore also the data. There are many possibilities to get the personal information also if you aren't a friend of the person.

Afterward the most commonly used attack scenarios are presented based on social engineering. At this point it turned out that identity theft, phishing and cyber mobbing are the major attack scenarios operated with the help of social networks and within social networks.

Based on these results, the possible vulnerabilities are presented to illustrate how vulnerable the users are when they post personal information. Even if the users cannot be dissuaded to use social networks, they should be aware to handle social network with care and are careful with the information they provide.

The results of this research should show how dangerous social networks can be and where special care should be taken. Additionally, measures are proposed in order to minimize the dangers and to minimize the target. The central argument of this work is that you can use social networks very well, but always with caution and consider first what you'll write.

Inhaltsverzeichnis

1. EINLEITUNG	8
2. BEGRIFFSDEFINITIONEN UND THEORETISCHE GRUNDLAGEN	10
3. INFORMATIONSSAMMLUNG.....	21
3.1. INFORMATIONEN VON WEBSITES	21
3.2. SUCHMASCHINEN.....	21
3.3. SOCIAL MEDIA, USER SITES, BLOGS USW.....	24
3.4. INFORMATIONSQUELLEN UND FUNKTIONEN IN SOZIALEN NETZWERKEN	24
3.4.1. <i>Zur Verfügung gestellte persönliche Informationen in sozialen Netzwerken.....</i>	<i>28</i>
3.4.2. <i>Genutzte Funktionen in sozialen Netzwerken</i>	<i>33</i>
3.5. AUTOMATISIERTE INFORMATIONSGEWINNUNG.....	34
4. ANGRIFFSSZENARIOEN	48
4.1. IDENTITÄTSDIEBSTAHL.....	48
4.2. CYBER MOBBING BZW. STALKING	49
4.2.1. <i>Was ist Cyber Mobbing?</i>	<i>49</i>
4.2.1.1. <i>Unterschied - Cyber Mobbing und Cyber Stalking</i>	<i>49</i>
4.2.2. <i>Was ist neu an Cyber Mobbing?</i>	<i>50</i>
4.2.3. <i>Formen von Cyber-Mobbing</i>	<i>51</i>
4.2.4. <i>Wie werden die neuen Medien zum Mobben genutzt?</i>	<i>52</i>
4.2.5. <i>Relevante Gesetzespassagen für Cyber-Mobbing.....</i>	<i>53</i>
4.2.6. <i>Statistiken über Cyber - Mobbing.....</i>	<i>58</i>
4.3. PHISHING	62
4.3.1. <i>Spear Phishing.....</i>	<i>63</i>
4.3.2. <i>Social Phishing</i>	<i>63</i>
4.3.3. <i>Phishing über Soziale Netzwerke - Statistik</i>	<i>64</i>
4.4. VERBREITUNG VON SCHADSOFTWARE ÜBER SOZIALEN NETZWERKEN.....	67
5. VERWUNDBARKEIT IN SOZIALEN NETZWERKEN.....	69
5.1. VERWUNDBARKEITSDARSTELLUNG.....	75
5.1.1. <i>Zielgruppen</i>	<i>81</i>
5.1.2. <i>Verwundbarkeitsschlüssel:.....</i>	<i>83</i>
5.2. BEISPIELE FÜR EINE VERWUNDBARKEITSBERECHNUNG	85
6. MAßNAHMEN UND EMPFEHLUNGEN	87
6.1. DIE WICHTIGSTEN REGELN FÜR DIE BENUTZUNG VON SOZIALEN NETZWERKEN	87
6.2. TECHNISCHE MAßNAHMEN.....	88
6.3. VORSCHLÄGE AN FACEBOOK (MAßNAHMEN SEITENS FACEBOOK)	90
6.4. EMPFEHLUNGEN	91
7. SCHLUSSFOLGERUNGEN UND AUSBLICK	94
8. ANHANG (AUSWERTUNG DER BEFRAGUNG).....	96

Abbildungsverzeichnis

Abbildung 1: Nutzer von Social Networks (Jänner bis März 2011) [2] basierend auf [3]	8
Abbildung 2: Darstellung des Social Engineering Zyklus basierend auf Mitnick ([5], Seite 377)	12
Abbildung 3: Nutzungsmotivation von sozialen Netzwerken. [11]	14
Abbildung 4: Tägliche Nutzungsdauer - Facebook [2] basierend auf [13]	15
Abbildung 5: Am meisten genutzte Online Communities [15]	16
Abbildung 6: Derzeitige Facebook- Userzahlen in Österreich [16]	16
Abbildung 7: Derzeitige Twitter- Userzahlen in Österreich [16]	17
Abbildung 8: Google als Informationslieferant	22
Abbildung 9: Passwörter mittels Google finden	23
Abbildung 10: Ergebnis eines Beispiels	23
Abbildung 11: Freunde pro User [2] basierend auf ([25], Seite 6)	25
Abbildung 12: Durchschnittliche Anzahl der hochgeladenen Fotos [2] basierend auf [27]	27
Abbildung 13: Gesichtserkennungseinstellungen auf Facebook [28]	28
Abbildung 14: Bedenken beim Veröffentlichen von persönlichen Daten [2] basierend auf [30]	29
Abbildung 15: Persönliche Daten in sozialen Netzwerken [2] basierend auf [31]	30
Abbildung 16: Persönliche Daten in sozialen Netzwerken II [2] basierend auf ([25], Seite 7)	30
Abbildung 17: Persönliche Daten in sozialen Netzwerken, die für alle sichtbar sind [2] basierend auf [32]	31
Abbildung 18: Datensichtbarkeit [2] basierend auf ([25], Seite 8)	32
Abbildung 19: Schutz der Daten [2] basierend auf [32]	32
Abbildung 20: Aktivitäten in sozialen Netzwerken [2] basierend auf [30]	33
Abbildung 21: genutzte Funktionen in sozialen Netzwerken [2] basierend auf [33]	34
Abbildung 22: Twitter Suchfunktion	36
Abbildung 23: Friend-in-the-middle Attacke [34]	37
Abbildung 24: Maltego (Personensuche)	38
Abbildung 25: Maltego (E-Mail und Accounts)	39
Abbildung 26: Maltego – gezielte Accountsuche	39
Abbildung 27: Cree.py Personensuche	41
Abbildung 28: Facebook-Hacker Tool [36]	42
Abbildung 29: twitalyzer - Startseite	43
Abbildung 30: twitalyzer – Christina Stürmer Analyseergebniss	43
Abbildung 31: TwitterAnalyzer [38]	44
Abbildung 32: TweetPsych - Startseite	44
Abbildung 33: TweetPsych – Ergebnis 1 (Beispiel)	45
Abbildung 34: facebook search	45
Abbildung 35: facebook search – Christina Stürmer	46
Abbildung 36: pipl - Personensuche	46
Abbildung 37: Anzahl der gestohlenen Identitäten und Passwörter in 2010 [2] basierend auf [42]	48
Abbildung 38: Cyber Mobbing Erfahrungen in Deutschland [2] basierend auf ([48], Seite 8)	58
Abbildung 39: Verbreitung von Cybermobbing unter Jugendlichen [2] basierend auf [49]	59
Abbildung 40: Cyber Mobbing Täter [2] basierend auf ([48], Seite 6)	59
Abbildung 41: Jugendlichen, i. d. Bekanntenkreis schon gemobbt wurde [2] basierend auf ([15], Seite 40)	60
Abbildung 42: Länderstatistik über Cyber Mobbing [2] basierend auf [50]	61
Abbildung 43: Schlechte Erfahrungen in sozialen Netzwerken [2] basierend auf [51]	62
Abbildung 44: Entwicklung von Phishing über Soziale Netzwerke in 2010 ([59], Seite 58)	65
Abbildung 45: Phishing Angriffe nach Websites im 1.Halbjahr 2011 [2] basierend auf [60]	66
Abbildung 46: Angegriffene Organisationen durch Phishing in 2010 [2] basierend auf [61]	66
Abbildung 47: Vertrauenseinschätzung zu Informationsquellen in sozialen Netzwerken [2] basierend auf [62] ..	67
Abbildung 48: Infrastruktur - Proxy-basierter Echtzeit-Schutz-Mechanismus für Social Networking Sites [118] ..	89
Abbildung 49: Skizze des gesamten Verfahrens [118]	90

Tabellenverzeichnis

Tabelle 1: Social Engineering Zyklus (vgl. [5], Seite 377)	12
Tabelle 2: Neue Technologien im Überblick (vgl. [47], Seite 6-7)	52
Tabelle 3: Angriffsszenarien und Gefahren	70
Tabelle 4: Verwundbarkeitsmatrix	76
Tabelle 5: Beschreibung der Kritikalitätsstufen	76
Tabelle 6: gefährdete Zielgruppen	81
Tabelle 7: Beschreibung der Gewichtung der Gefährdung der Zielgruppen	81
Tabelle 8: Verwundbarkeitsschlüssel Identitätsdiebstahl	83
Tabelle 9: Verwundbarkeitsschlüssel Cyber - Mobbing	83
Tabelle 10: Verwundbarkeitsschlüssel Phishing	83
Tabelle 11: Verwundbarkeitsschlüssel Spear Phishing	83
Tabelle 12: Verwundbarkeitsschlüssel Social Phishing	84
Tabelle 13: Verwundbarkeitsschlüssel Schadsoftware	84
Tabelle 14: Verwundbarkeitsschlüssel Werbung	84
Tabelle 15: Verwundbarkeitsschlüssel Bewerbung	84
Tabelle 16: Verwundbarkeitsschlüssel Kündigung	84
Tabelle 17: Beispiel einer Verwundbarkeitsberechnung (viele Daten)	85
Tabelle 18: Beispiel einer Verwundbarkeitsberechnung (wenige Daten)	86
Tabelle 19: Auswertung Identitätsdiebstahl	97
Tabelle 20: Auswertung Cyber-Mobbing	98
Tabelle 21: Auswertung Phishing	99
Tabelle 22: Auswertung Spear-Phishing	100
Tabelle 23: Auswertung Social-Phishing	101
Tabelle 24: Auswertung Verbreitung von Schadsoftware	102
Tabelle 25: Auswertung Verkauf der Daten (Werbung)	103
Tabelle 26: Auswertung Bewerbung	104
Tabelle 27: Auswertung Kündigung	105

1. Einleitung

Dieses Kapitel gibt einen Überblick welche Ziele diese Arbeit verfolgt und wie geforscht wird. Weiters wird das Forschungsproblem kurz dargestellt.

Forschungsproblem und Zielsetzung

„In sozialen Netzwerken präsentieren sich Nutzer/innen in einem eigenen Profil mit möglichst vielen persönlichen Angaben, wie z.B. Hobbys, Interessen, aktuelle Aktivitäten, Fotos, Videos etc. Wenn zwei Nutzer/innen einwilligen, ‚verlinken‘ sie ihre Profile und werden zu ‚Freunden‘. Dadurch entsteht ein Netzwerk von Personen, die miteinander in Kontakt stehen. In sozialen Netzwerken kann man sich mit anderen austauschen, Fotos, Videos und Links teilen, Interessensgruppen bilden, gemeinsam Spiele spielen und neue Kontakte knüpfen. Andere Begriffe für ‚Soziales Netzwerk‘: Online-Community, Social Network, virtuelle Gemeinschaft.“ [1]

Die beliebtesten sozialen Netzwerke in Österreich sind (siehe Abbildung 1):

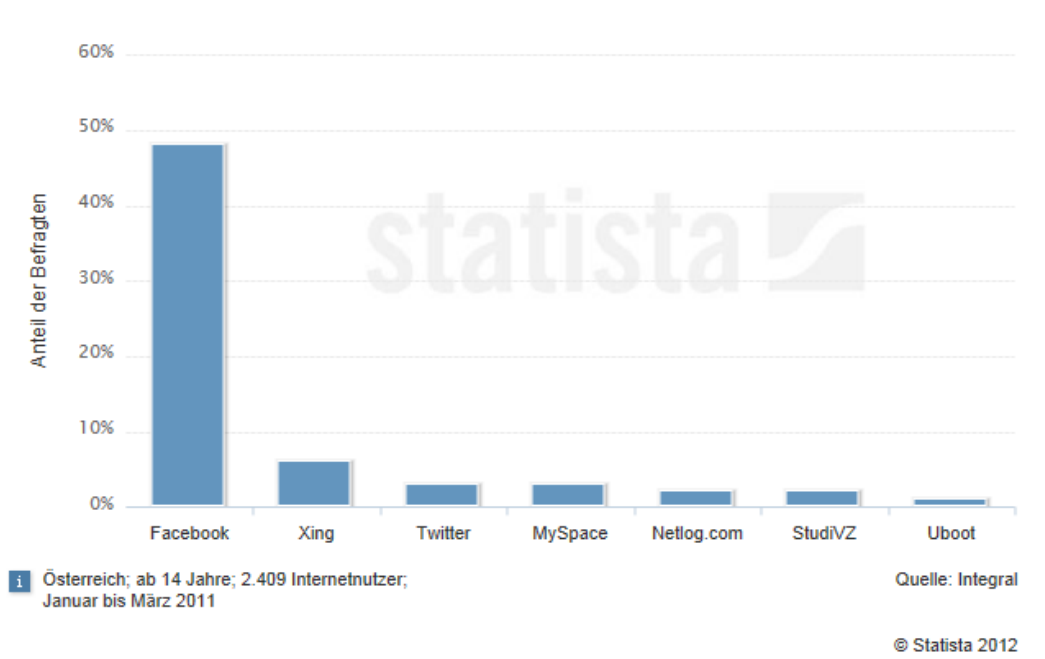


Abbildung 1: Nutzer von Social Networks (Jänner bis März 2011) [2] basierend auf [3]

Social Engineering ist eine extrem effiziente Methode um an Informationen zu kommen, denn beim Social Engineering werden natürliche menschliche Reaktionen und positive Eigenschaften wie Hilfsbereitschaft, Kundenfreundlichkeit, Dankbarkeit, Stolz auf die Arbeit oder weniger positive Aspekte wie Gutgläubigkeit, Respekt oder gar Bestechlichkeit, ausgenutzt. Social Engineering kann an sich schon im Gasthaus beginnen, wenn z.B. ein Mitarbeiter stolz über seine Arbeit erzählt. Meist sind Social Engineering Angriffe nur eine Vorstufe vom eigentlichen Angriff, wie einem Einbruch in das Firmennetz. Beim Social Engineering werden beispielsweise Benutzernamen und Passwörter erfragt bzw. erschlichen - der eigentliche Angriff passiert dann, wenn der Angreifer die Zugangsdaten schon besitzt. (vgl. [4])

Das Ziel dieser Diplomarbeit ist es herauszuarbeiten, welche neuen Methoden des Social Engineering es zurzeit gibt und welche Angriffsszenarien momentan in sozialen Netzwerken verwendet werden. Danach soll eine Verwundbarkeitsdarstellung erarbeitet werden, welche verdeutlichen soll, wie gefährlich soziale Netzwerke sein können. Daraus sollen anschließend Maßnahmen definiert werden, um die Risiken zu verringern.

In dieser Diplomarbeit werden hauptsächlich die sozialen Netzwerke Facebook und Twitter betrachtet, da diese momentan am populärsten sind.

Problemstellung und Forschungsleitende Fragestellung

Soziale Netzwerke werden immer öfter dazu benutzt um an Informationen zu kommen, um dann gezielte Angriffe zu starten. Häufig wird auch bewusst Schadsoftware oder ähnliches über soziale Netzwerke verteilt, weil hier die Vertrauensbasis sehr hoch ist. Daher sollen in dieser Diplomarbeit die am häufigsten verwendeten Angriffsszenarien, sowie die Gefahren von sozialen Netzwerken, dargestellt werden. In weiterer Folge soll dann mittels einer Verwundbarkeitsdarstellung erstellt werden, welche die Verwundbarkeit der Online-Profile darstellt und zeigt wie hoch sie unter bestimmten Bedingungen ist.

Daraus ergeben sich folgende Fragestellungen:

- Welche Social Engineering Angriffsszenarien sind in sozialen Netzwerken beliebt bzw. werden häufig angewendet?
- Wie kann eine Verwundbarkeitsdarstellung der Social Engineering Angriffsszenarien und Gefahren in sozialen Netzwerken getroffen werden?
- Mit welchen Maßnahmen kann man Risiken wie Identitätsdiebstahl, Phishing, Cyber Mobbing, usw. verringern?

Forschungsmethodik

Als Forschungsmethodik dient zum größten Teil die theoretische Analyse der Literatur aus Büchern und Online Quellen. Für den letzten Abschnitt wird eine kleine empirische Umfrage durchgeführt.

Es soll recherchiert werden, welche Angriffsszenarien momentan verwendet werden und wie sich das Social Engineering durch die sozialen Netzwerke verändert hat. Im Zuge dieser Literaturrecherche soll auch herausgefunden werden, welche Tools es zur automatischen Datensammlung gibt und wie erfolgreich diese sind. Danach wird eine Verwundbarkeitstabelle entwickelt die veranschaulichen soll, wie gefährlich die Veröffentlichung von sensiblen Daten in sozialen Online-Netzwerken ist. Aufgrund dieser Verwundbarkeitsdarstellung werden Maßnahmen erarbeitet.

2. Begriffsdefinitionen und Theoretische Grundlagen

Als Vorbereitung der Forschungsarbeit ist es wichtig Begriffe zu definieren und zu beschreiben. In folgendem Kapitel werden die wichtigsten Begriffe beschrieben und definiert.

Social Engineering

„Social Engineering benutzt Techniken der Beeinflussung und Überredungskunst zur Manipulation oder zur Vortäuschung falscher Tatsachen, über die sich ein Social Engineer eine gefälschte Identität aneignet. Damit kann der Social Engineer andere zu seinem Vorteil ausbeuten, um mit oder ohne Verwendung von technischen Hilfsmittel an Informationen zu gelangen.“ ([5], Seite 4)

Christopher Hadnagy geht in seinem Buch auch auf die Definition von Social Engineering ein. Er beginnt beide Begriffe einzeln zu definieren und sie danach wieder zusammenzuführen. „Social“ wird definiert als *„auf das Leben, Wohlergehen und die Beziehung von Menschen in einer Gemeinschaft bezogen.“ ([6], Seite 30)*

„Engineering“ wird definiert als *„die Kunst oder Wissenschaft wie Physik oder Chemie praktisch anzuwenden, z.B. in der Konstruktion von Motoren, Brücken, Gebäuden bzw. geschickte oder kunstvolle Erfindungen; kluges Taktieren.“ ([6], Seite 30)*

„Wenn man diese beiden Definitionen kombiniert, sieht man schnell, dass es beim Social Engineering um die Kunst oder besser noch Wissenschaft geht, wie man Menschen hinsichtlich bestimmter Aspekte ihres Lebens geschickt und umsichtig in Aktion bringt.“ ([6], Seite 30)

Beim Social Engineering werden menschlichen Eigenschaften wie Hilfsbereitschaft, Kundenfreundlichkeit oder Dankbarkeit, aber auch negative Aspekte, wie Gutgläubigkeit, Respekt oder Bestechlichkeit, ausgenützt. Daher ist Social Engineering eine sehr effiziente Methode zur Informationsbeschaffung. Als Vorbereitung für Social Engineering Angriffe steht immer eine gründliche Recherche im Vordergrund - ohne Recherche wird kein Social Engineering Angriff funktionieren, wobei wiederum die Social Engineering Angriffe meist nur die Vorstufe des eigentlichen Angriffes sind.

Will man zum Beispiel Firmendaten erfragen, so muss als Erstes die Firmenhomepage unter die Lupe genommen werden, anschließend wird über die Mitarbeiter recherchiert, da sie meist eine gute Quelle für weitere wichtige Informationen sind.

Für eine Recherche können soziale Netzwerke hervorragende Daten liefern, sowohl im Firmen - als auch im Privatbereich, anschließen können diese Netzwerke auch, für die eben genannten Angriffe, sehr gut genutzt werden. (vgl. [4])

Laut Christopher Hadnagy wird Social Engineering überall im täglichen Leben eingesetzt. Kinder nützen es, um die Eltern dazu zu bringen, das zu tun, das sie wollen. Auch Ärzte und Psychologen nutzen Social Engineering, um Informationen von ihren Klienten zu erhalten.

Laut Chrstopher Hadnagy ist *„mit der echten Definition des Social Engineering der Akt der Manipulation einer Person gemeint, eine Handlung auszuführen.“ ([6], Seite 30)* Damit kann die Erlangung von Informationen gemeint sein oder auch der Zugang in bestimmte Bereiche oder dass man die Zielperson dazu bewegt, eine bestimmte Aktion auszuführen. (vgl. [6], Seite 30)

Ärzte, Psychologen und Therapeuten nutzen oft Elemente des Social Engineerings, um ihre Patienten zu bestimmten Handlungen zu manipulieren, die gut für sie sind. Trickbetrüger nutzen diese Elemente, um ihre Zielperson zu Aktivitäten zu bringen, die zu einem Verlust führen. Obwohl die Absicht eine völlig andere ist, ist das Vorgehen doch sehr ähnlich. Der Psychologe arbeitet mit gut formulierten Fragen um den Patienten auf eine Schlussfolgerung zu bringen, während der Trickbetrüger die Fragen so formuliert, dass sein Ziel in eine angreifbare Position kommt. (vgl. [6], Seite 30)

Laut Kevin Mitnick ist ein Social Engineer ein „*skrupelloser Zauberer, der Ihre Aufmerksamkeit auf seine linke Hand zieht, während er mit rechts Ihre Geheimnisse klagt. Diese Type ist oft so freundlich, wortgewandt und entgegenkommend, dass es Ihnen eine Freude ist, ihm begegnet zu sein.*“ ([5], Seite 20)

Verschiedene Typen von Social Engineers

Laut Christopher Hadnagy gibt es mehrere Typen von Social Engineers, welche im folgenden Abschnitt näher beschrieben werden: (vgl. [6], Seite 39 -41)

■ **Hacker:**

Da die Softwarehersteller immer bessere Software schreiben und dadurch den Hackern das Leben maßgeblich erschwert wird, greifen diese immer wieder auf das Social Engineering zurück. Sie nutzen oft eine Mischung aus Hardware und persönlichen Skills, und setzen Social Engineering in aller Welt bei großen als auch bei kleineren Angriffen ein.

■ **Penetrationstester:**

Echte Penetrationstester lernen jene Skills, welche auch böswillige Hacker nutzen, und setzen diese ein, um die Sicherheit ihrer Kunden zu erhöhen. Penetrationstester sind Menschen, welche die gesammelten Informationen niemals zum eigenen Vorteil nutzen würden oder diese einsetzen, um das Ziel zu schädigen.

■ **Spione**

Spione nutzen Social Engineering sozusagen täglich. Sie lernen wie sie ihre Opfer so beschwindeln können, dass sie für jemanden gehalten werden, der sie in Wahrheit nicht sind.

■ **Identitätsdiebe:**

Identitätsdiebe haben es auf Informationen wie Name, Bankkontonummer und Sozialversicherungsnummer abgesehen, um diese dann, ohne Wissen des Eigentümers, zu verwenden.

■ **Trickbetrüger:**

Diese Gruppe von Personen hat sich meisterhaft die Fähigkeit angeeignet, andere zu „lesen“ und kleinste Hinweise zu erkennen, diesen Hinweisen entnehmen sie dann ob es sich um ein geeignetes Opfer handelt.

■ **Personalvermittler:**

Personalvermittler müssen viele psychologische Prinzipien des Social Engineering beherrschen, da sie Menschen durchschauen und verstehen müssen um sie dementsprechend zu vermitteln.

■ **Verkaufspersonal:**

In der Kunst des Verkaufens kommen viele Fähigkeiten und Fertigkeiten zusammen, z.B. Informationssammlung, Entlocken von persönlichen Angaben, usw.

■ **Regierungen:**

Regierungen nutzen ständig das Social Engineering, denn sie wollen die von ihnen ausgegebenen Botschaften kontrollieren.

■ Ärzte, Psychologen und Rechtsanwälte:

Die Gruppe von Personen, setzen genau die gleichen Methoden des Social Engineering ein, wie ein Angreifer. Sie nutzen die Methoden um Informationen von ihren Klienten zu erfragen, um sie dementsprechend behandeln bzw. „manipulieren“ zu können.

Zyklus eines Social Engineering Angriffes

Im folgenden Abschnitt wird der Social Engineering Zyklus dargestellt (Abbildung 2) und beschrieben (Tabelle 1). Dieser Zyklus veranschaulicht ein allgemeines Schema eines Social Engineering Angriffes.

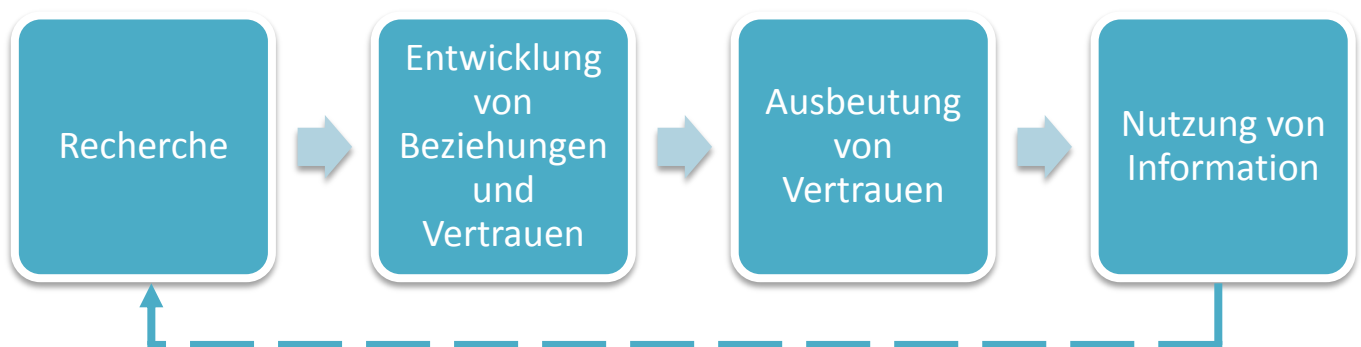


Abbildung 2: Darstellung des Social Engineering Zyklus basierend auf Mittnick ([5], Seite 377)

Aktion	Beschreibung
Recherche	Dazu gehört die Suche in öffentlich zugänglichen Quellen wie Inhalte von Websites, Social Network Sites, Zeitungsausschnitte, usw.
Entwicklung von Beziehung und Vertrauen	Nutzung von Insider-Informationen, falsche Darstellung von Identität, Verweise auf dem Opfer bekannte Personen, Hilfebedarf oder Autorität
Ausbeutung von Vertrauen	Bitte um Informationen oder Handlungen auf Seiten des Opfers.
Nutzung von Informationen	Wenn die gesammelten Informationen nur einen Schritt zum endgültigen Ziel darstellen, kehrt der Angreifer wieder zu früheren Schritten des Kreislaufes zurück.

Tabelle 1: Social Engineering Zyklus (vgl. [5], Seite 377)

Social Engineering in soziale Netzwerken

Social Engineering ist eine sehr beliebte Angriffsform, die schon verwendet wird, seit dem es Menschen gibt. Die Art und Weise des Social Engineerings wird immer wieder verändert und angepasst. Deswegen hat sich das Wesen des Social Engineerings in den letzten drei bis vier Jahren stark verändert, vor allem durch die sozialen Netzwerke. Diese bieten eine große Angriffsfläche und man kann hunderttausende Menschen mit einem Angriff anvisieren. Der wichtigste Punkt ist allerdings, dass in sozialen Netzwerken Informationen

preisgegeben werden, die für Angriffe optimal genutzt werden können, wie etwa der Name, das Geburtsdatum oder die Lieblingspizza. All diese Informationen können als Basis für Angriffe genutzt werden.

Soziale Netzwerke bauen sehr stark auf Vertrauen auf, und genau hier setzen Social Engineers an bzw. nutzen sie dieses Vertrauen aus. (vgl. [7])

Social Engineering ist bedeutend günstiger in der Durchführung geworden, als zur Ära des „Mülldurchsuchens“. Mittlerweile liegen durch die sozialen Netzwerke die Informationen unmittelbar in maschineller und automatisierter weiterverarbeitbarer Form vor, sodass Social Engineering auch durch Tools eigenständig betrieben werden kann. (vgl. [8], Seite 7)

Soziale Netzwerke

Der Begriff „Social Networking“ kommt aus dem soziologischen und beschreibt die Analyse der Qualität der zwischenmenschlichen Beziehungen. Die dialogischen Anwendungen, welche das Web heute zu bieten hat, ermöglichen es - einfacher denn je - Kontakte zu vertiefen und neue Netzwerke aufzubauen. (vgl. [9], Seite 64)

Soziale Netzwerke sind Teil des sogenannten „Mitmachwebs“ (auch Social Web oder Web 2.0 genannt). Früher brauchte man noch HTML Kenntnisse um etwas im Web zu veröffentlichen, doch mittels diesen Mitmachweb ist es kein großer Aufwand mehr, sich im Web zu präsentieren oder seine Meinung kund zu tun. (vgl. [10], Seite 15)

„Es gibt immer mehr Internetseiten, auf denen sich Menschen aus aller Welt treffen und sich über Hobbys, gemeinsame Interessen und vieles mehr unterhalten, tauschen, handeln, sich „daten“. Das fasziniert längst nicht nur Erwachsene, auch der Nachwuchs nutzt die Angebote mit Begeisterung“ [3]

In sozialen Netzwerken können User ihr eigenes Profil anlegen und sich so, mit möglichst vielen persönlichen Angaben, wie z.B. Name, Geburtsdatum, Hobbies, Interessen, Fotos, Videos, usw., präsentieren. Über die Suche in diesen Netzwerken kann man Freunde und Bekannte finden und mit ihnen in Kontakt treten. Dazu muss man eine Kontraktanfrage (Freundschaftsanfrage) senden, bestätigt man die Anfrage werden die beiden Profile miteinander verlinkt. So entsteht ein Netzwerk von Personen, die miteinander in Kontakt stehen.

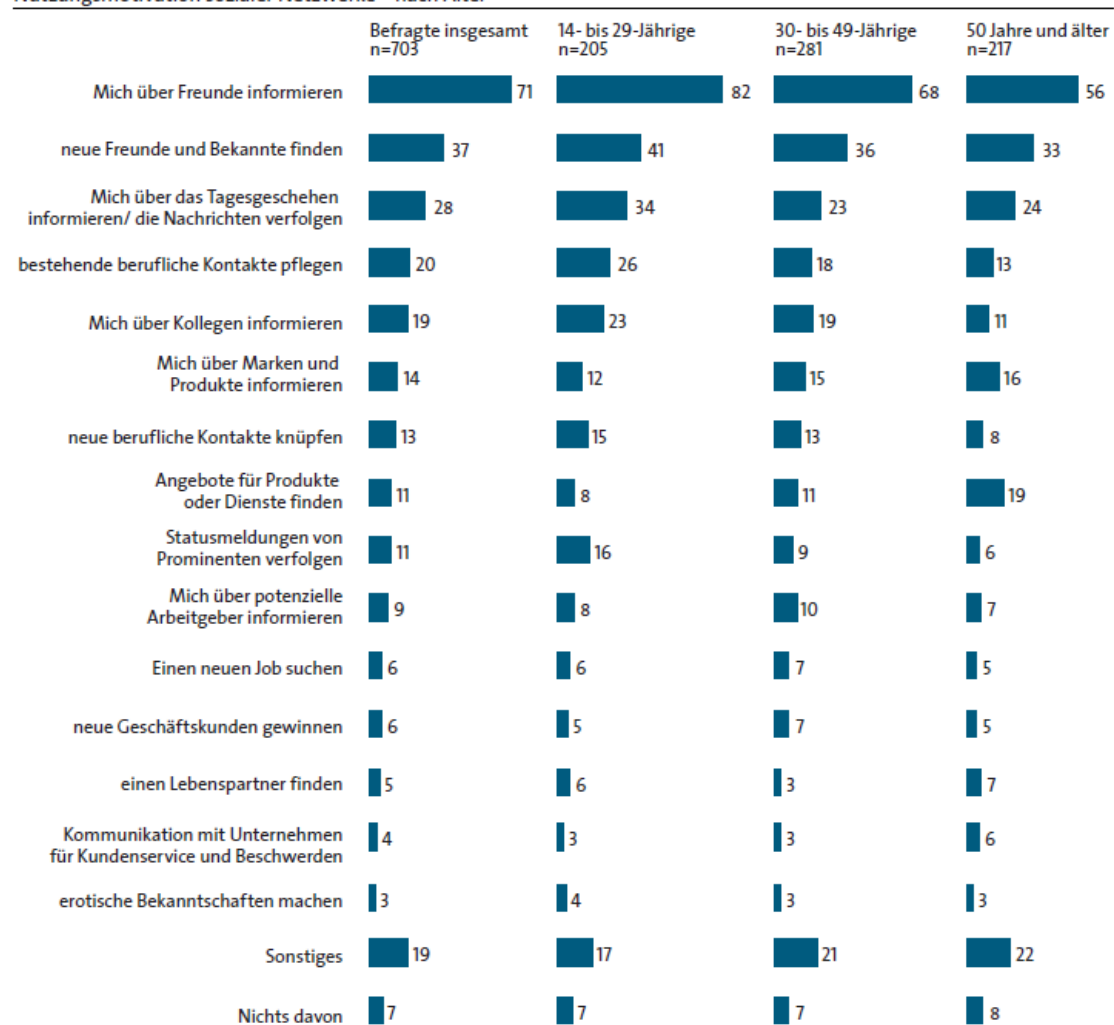
Diese Sozialen Netzwerke werden auch zum Austauschen von Fotos, Videos benutzt. Weiters können Gruppen erstellt werden, in denen diese Personen dann über gemeinsame Interessen diskutiert können.

Andere Begriffe für „Soziales Netzwerk“: Online-Community, Social Network, virtuelle Gemeinschaft. (vgl. [1])

Abbildung 3 zeigt, warum das Konzept der sozialen Netzwerke so gut funktioniert, denn die User haben das verlangen, mit anderen in Kontakt zu treten, sich über Freunde zu informieren, neue Bekanntschaften über das Netz zu finden und bestehende Freundschaften zu pflegen.

Die Hauptmotivation zur Nutzung sozialer Netzwerke ist auf die Vernetzung mit Freunden ausgerichtet. Denn hier kann man sich informieren, was die Freunde machen, welche Probleme sie haben und man kann sich auch mit ihnen per Chat oder Nachrichten unterhalten und austauschen.

Nutzungsmotivation sozialer Netzwerke – nach Alter



Basis: 703 Internetnutzer, die in mind. einem sozialen Netzwerk angemeldet sind. (Mehrfachnennungen möglich) Angaben in Prozent
Frage: „Wofür nutzen Sie die sozialen Online-Netzwerke? Bitte kreuzen Sie alles an, was zumindest gelegentlich auf Sie zutrifft.“

Abbildung 3: Nutzungsmotivation von sozialen Netzwerken. [11]

Herausforderungen von sozialen Netzwerken

Neue Technologien führen zu neuen Herausforderungen. Die massive Nutzung von sozialen Netzwerken auf der ganzen Welt hat zur Entstehung von vielen Herausforderungen geführt. Folgende Herausforderungen haben sich ergeben:

- Öffentliche Verfügbarkeit von persönlichen Daten
- Privatsphäre der Nutzer

Soziale Netzwerke sind eine der beliebtesten und zeitaufwändigsten Online-Aktivitäten. Ein durchschnittlicher Facebook User verbringt ca. 55 Minuten pro Tag in diesem sozialen Netzwerk. Für die User ist es sehr attraktiv, sich zu „sozialisieren“ und zwar auch mit Menschen die geografisch nicht in Reichweite sind. Ein durchschnittlicher Facebook User hat 130 Freunde, die meisten sind nur Online-Bekanntschaften und diese

„Online Bekanntschaften“ sehen alle persönlichen Informationen. Die meisten User sind sich der Gefahren der Preisgabe von Persönlichen Daten nicht bewusst, denn die meisten „Freunde“ haben sie im „realen“ Leben noch nie getroffen. (vgl. [12])

Wie lange nutzen Sie Facebook täglich?

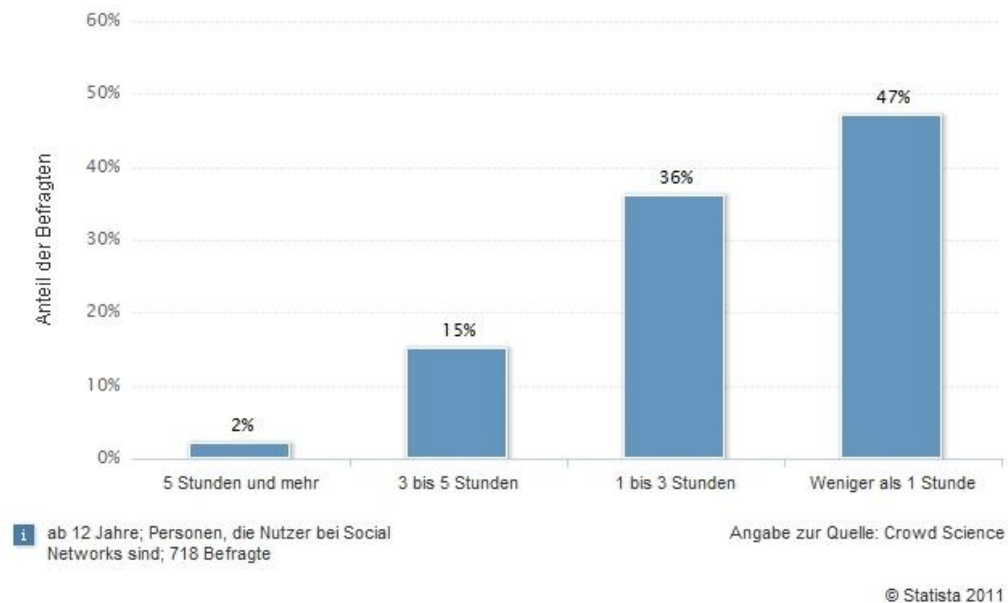


Abbildung 4: Tägliche Nutzungsdauer - Facebook [2] basierend auf [13]

Soziale Netzwerke bieten eine Fülle von persönlichen Informationen. Benutzer schreiben Berichte aus ihren täglichen Aktivitäten, politischen und religiösen Status, usw. auf ihre online Profile. Sie schauen sich Fotos oder Kommentare anderer User und vieles mehr an. Sobald ein Nutzer es geschafft hat, mit jemanden als „Freund“ zu gewinnen, kann er verschiedene Informationen extrahieren und für illegale Zwecke nutzen. (vgl. [12])

Während die Betreiber von sozialen Netzwerken gewisse Security-Mechanismen anbieten, um den Zugriff auf bestimmte persönliche Daten zu schützen, haben Studien ergeben, dass die Benutzer die Fragen der Online-Privatsphäre nicht verstehen. Daher ist es eine Herausforderung die Nutzer die Thematik der Online-Privatsphäre näherzubringen, damit sie begreifen, dass das Veröffentlichen von persönlichen Daten potenziell gefährlich ist. Doch selbst wenn es die Funktion gibt, dass man namentlich nicht gefunden werden kann, werden diese Funktion kaum User verwenden, denn wenn man nicht gefunden werden kann, hat das ganze soziale Netzwerk keinen Sinn mehr. (vgl. [12])

Facebook

„Facebook ist ein Web in Web geworden, ein Online-Netzwerk aus mehr als 500 Millionen Menschen, eine ultimative Kommunikationsplattform.“ ([14], Seite 12)

Facebook ist zu einem Kult geworden, an dem sehr viele Menschen teilnehmen. Es ist ein sozialer Druck entstanden, dabei sein zu müssen und seine Identität in einem eigenen Profil abzubilden. Mit Facebook ist eine neue Internet-Ära angebrochen, denn vom Netz der Informationen und Waren ist es nun zum Netz der

Menschen geworden. Plötzlich ist das eigene ICH in den Mittelpunkt gewandert. Mittlerweile gehört es schon zum Alltag, dass sich Paare trennen, weil der andere den Beziehungsstatus von „in einer Beziehung“ auf „Single“ geändert hat. Aber auch Scheidungsanwälte nutzen Facebook, um Beweise zu finden. Facebook ist das größte Mitmach-Netz der heutigen Zeit geworden, denn es enthält mit Abstand die größte digitale Fotosammlung der Welt. Weiters werden in dieses soziale Netzwerk mehr Buchstaben eingetippt als in allen Weblogs zusammen. (vgl. [14], Seite 12)

Facebook ist das bisher am meisten genutzte und beliebteste Soziale Netzwerk, wie folgende Statistik zeigt. Weltweit sind hier fast 510 Millionen Nutzer registriert und miteinander vernetzt.

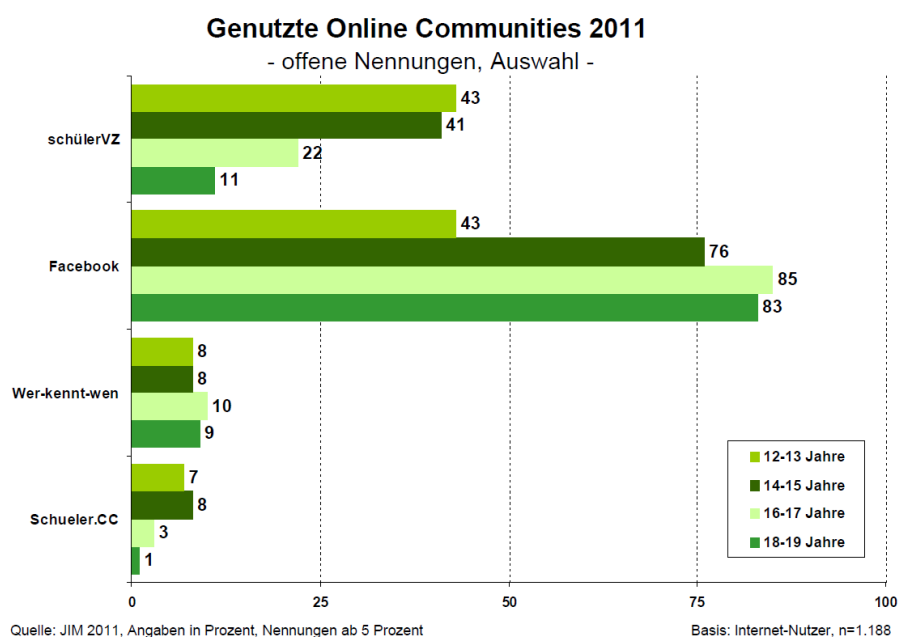


Abbildung 5: Am meisten genutzte Online Communities [15]

Derzeit sind circa gleich viele Frauen wie Männer bei Facebook registriert, mittlerweile sind es insgesamt ca. 2,7 Mio. österreichische User, die Facebook nutzen. Die Altersgruppe zwischen 20 – 29 nutzt Facebook am intensivsten.



Abbildung 6: Derzeitige Facebook- Userzahlen in Österreich [16]

Facebook ist mittlerweile zu einer „Plattform“ geworden, welche mit dem Chat, den Status-Updates, Fotos und Gruppen eine sehr mächtige Kommunikationsmaschine darstellt. Die Firma aus Palo Alto hat es geschafft eine „Plattform“ zu werden. Den Begriff Plattform hat Bill Gates in die Technik-Welt eingeführt. Bei einer Plattform handelt es sich um ein breites Fundament auf dem andere Firmen aufsetzen. (vgl. [14], Seite 27)

Hier noch ein paar Fakten über Facebook:

Facebook hat derzeit ca. 400 Millionen aktive User weltweit, davon nutzen ca. 100 Millionen User Facebook auch mobil. Jede Woche werden ca. 3,5 Milliarden Inhalte gepostet, ca. 2,5 Milliarden Fotos hochgeladen und 3,5 Milliarden Veranstaltungen angekündigt. Die User, die Facebook auch mobil benutzen sind dabei doppelt so aktiv wie andere Facebook Nutzer.

Durchschnittlich verbringt jeder Facebook Nutzer ca. eine Stunde täglich im sozialen Netz, ist mit 130 Freunden vernetzt und ist Mitglied von ca. 13 Gruppen. Weiters werden pro Nutzer und Monat ca. 8 Freundschaftsanfragen versendet, 25 Kommentare geschrieben und es wird neunmal auf den Button „Gefällt mir“ geklickt. (vgl. [10], Seite 17)

Twitter

Übersetzt man Twitter so heißt es eigentlich zwitschern oder schnattern. Dieser Name wurde bewusst gewählt, denn mit Twitter ist es möglich kurze Textnachrichten als Mikroblog per SMS, Instant Messaging oder Web-Oberfläche zu veröffentlichen. Andere Benutzer können diese Nachrichten dann mit ihrem Smartphone oder RSS-Reader verfolgen. Daher heißt der Dienst Twitter und die SMS-ähnlichen Nachrichten Tweets. (vgl. [17])

Twitter ist ein Kurznachrichtendienst, der sich auf 140 Zeichen lange Status-Updates spezialisiert hat. Weltweit nutzen mehr als 100 Millionen Nutzer diesen Dienst. Twitter hatte auch noch nie mit Privatsphäreneinstellungen Probleme, doch plagen Twitter immer wieder technische Schwierigkeiten, welche die Website schon oft lahm gelegt haben. (vgl. [14])

Derzeit besitzen ca. 71.684 Österreicher einen Twitter Account.



Abbildung 7: Derzeitige Twitter- Userzahlen in Österreich [16]

Schwachstellen

Durch eine Schwachstelle wird ein System erst anfällig auf Bedrohungen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird. (vgl. [18])

Typische Schwachstellen sind beispielsweise [19]

- Programmierfehler, die es z. B. erlauben Puffer-Überläufe (Buffer Overflows) auszunutzen,
- Konfigurationsfehler, die z. B. dazu führen, dass Passwörter im Klartext übertragen werden, obwohl sie eigentlich verschlüsselt sein sollten,
- Konzeptionsfehler in Programmiersprachen, die z. B. Programmen Zugriff auf Systemressourcen erlauben, die sie nicht benötigen,
- menschliches Fehlverhalten, wenn z. B. ein IT-Anwender aufgrund einer Phishing-Mail seine PIN und TAN in falsche Hände gibt.

Schwachstelle – der Menschliche Faktor

In dieser Diplomarbeit wird die Schwachstelle „Mensch“ behandelt. Denn mittels Social Engineering kann diese Schwachstelle hervorragend ausgenutzt werden, und anschließend für Angriffe verwendet werden, wobei in dieser Diplomarbeit nur die Angriffe behandelt werden, welche eben menschliche Schwachstellen ausnützen. Die Angriffe können zwar technisch unterstützt oder umgesetzt werden, jedoch helfen die Informationen enorm weiter um den technischen oder nicht technischen Angriff erfolgreich umzusetzen.

Die heutigen Technologien sind schon sehr weit fortgeschritten und immer mehr Unternehmen leisten sich sehr teure Sicherheitstechnologien. Die Angestellten werden zu Schulungen geschickt und gut ausgebildet, damit sie die Daten gut sichern und sehr aufmerksam damit umgehen können. Doch auch wenn all diese Faktoren sehr aufmerksam durchgeführt werden und die Daten immer „schön brav“ gesichert werden, bleibt das Unternehmen noch immer gefährdet! (vgl. [5], Seite 19)

„Warum? Weil der menschliche Faktor die eigentliche Schwachstelle der Sicherheitskette ist.

Sicherheit ist allzu oft nur eine Illusion, die häufig durch Leichtgläubigkeit, Arglosigkeit oder Ignoranz verschlimmert wird. Vom berühmtesten Wissenschaftler des 20. Jahrhunderts, Albert Einstein, stammt das Zitat: „Zwei Dinge sind unendlich: das Universum und die menschliche Dummheit. Aber bei dem Universum bin ich mir noch nicht ganz sicher.“ Letzten Endes können Angriffe durch Social Engineering erfolgreich sein, wenn Menschen dumm sind oder – was viel weiter verbreitet ist – einfach keine Ahnung von grundlegenden Sicherheitspraktiken haben. [...] Viele Profis aus der Informationsbranche halten an dem Irrtum fest, sie hätten ihre Firmen weitgehend gegen Angriffe abgeschirmt, weil sie Standard-Sicherheitsprodukte installiert haben: Firewalls, Zugangsbeschränkungssysteme oder widerstandsfähigere Authentifizierungsgeräte, wie zeitbasierte Tokens oder biometrische Smart Cards. Jeder der glaubt, dass allein die Anwendung von Sicherheitsprodukten ausreiche, echte Sicherheit zu gewährleisten, gibt sich mit der Illusion von Sicherheit zufrieden. [...] In dem Maße, wie Forscher immer bessere Sicherheitstechnologien entwickeln und damit die Möglichkeit verringern, dass technische Schwachstellen ausgenutzt werden können, werden Angreifer immer mehr den Hebel beim menschlichen Faktor ansetzen. Es ist oft ein Kinderspiel, die menschliche Firewall zu knacken. Das erfordert außer einem Telefonanruf keine Investitionen und beinhaltet nur ein minimales Risiko.“ ([5], Seite 20)

Cyberkriminelle versuchen häufig die menschliche Schwachstelle auszunutzen, da meistens der Mensch das schwächste Glied in einem Sicherheitssystem ist. Der Beweis dafür ist, dass Phishing Attacken großen Erfolg haben, denn mittels Phishing Attacken bringen die Cyberkriminellen die Anwender dazu ihre Benutzernamen, Passwörter oder PINs auf gefälschten Websites einzugeben. Der klassische Phishing Betrug ist also nach wie vor sehr beliebt.

Die neuen Entwicklungen wie Facebook, Twitter und co. ziehen viele Menschen an und so auch die Cyberkriminellen, die nun verstärkt die Mitglieder der sozialen Netzwerke ins Visier nehmen. So werden zum Beispiel über gehackte Facebook-Accounts Nachrichten mit Links auf schädliche Programme verschickt oder es werden „Tweets“ mit Links verschickt, die auf eine Betrüger Seite zeigen. Diese Links werden sehr oft mit URL-Kürzungsdiensten verschleiert.

Beispiel eines Facebook Betrugstrick: Oft geben sich die Betrüger als vermeintlicher Freund aus, der gerade im Ausland fest sitzt und nun dringend Geld braucht, damit er wieder nach Hause kommt. (vgl. [20])

„Allerdings ist der Mensch an sich nicht nur wegen seiner Unwissenheit angreifbar. Manchmal reicht schon ein angebliches Angebot über kostenlose Audio- oder Videodateien, damit Anwender auf einen verseuchten Link klicken“ [20]

Angriffe

Angriffe sind unerlaubte Tätigkeiten, die zum Schaden von Ressourcen, Dateien oder Programmen führen.

Es gibt aktive und passive Angriffe.

Bei **aktiven Angriffen** handelt es sich um Verfälschungen. Es werden Nachrichten, Komponenten oder die gesamte Kommunikation verfälscht. Zu aktiven Angriffen zählen DoS-Attacken (um Zugang zu Systemen zu erhalten), sowie das Übermitteln von schadhafte Codes (hier bringt der Angreifer das Opfer dazu geheime Daten, wie Passwörter einzugeben).

Bei **passiven Angriffen** handelt es sich um Angriffe, die die Vertraulichkeit bedrohen, aber die Kommunikation nicht stören. Sie zielen auf unerlaubte Informationsbeschaffung ab. Hier handelt es sich um Abhörmethoden. (vgl. [21])

Bedrohung, Gefahr und Risiko

Bedrohung

„Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann.“ [18]

Die Bedrohung kann alles (Objekt, Substanz, Mensch, ...) sein, dass einen Schaden verursachen kann. Weiters kann eine Bedrohung eine mögliche Ursache für ein unerwünschtes Ereignis sein. (vgl. [22])

Für die Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, dass die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Besitzer ein Schaden entstehen kann. (vgl. [18])

Gefahr

Die Gefahr ist zum Beispiel ein Datenverlust, der wiederum durch eine defekte Festplatte oder durch einen Dieb entstehen kann. (vgl. [18])

Risiko

Risiko ist die Kombination aus der Wahrscheinlichkeit eines Ereignisses und seiner Folgen. (vgl. [22])

Der Unterschied zur Gefahr ist hier, dass der Begriff „Risiko“ bereits eine Bewertung, inwieweit ein bestimmtes Schadensszenario relevant ist, beinhaltet. (vgl. [18])

Maßnahmen und Empfehlungen

Maßnahmen werden definiert, um die vorliegenden Risiken auf ein annehmbares Maß zu reduzieren. (vgl. [23], Seite 9)

Empfehlung wird in dieser Arbeit wie folgt definiert: Eine Empfehlung ist ein Vorschlag, wie man bestimmte Informationen besser schützen kann bzw. wie man Einstellungen verbessern kann damit man besser gegen Angriffe geschützt ist.

3. Informationssammlung

In diesem Kapitel widme ich mich der Informationsbeschaffung. Bei Social Engineering Attacks ist es sehr wichtig, sich vorher genauestens über sein Opfer zu informieren, denn umso mehr man über sein Opfer weiß, desto einfacher ist es, wichtige Informationen noch zusätzlich herauszufinden. Die neuen Medien, wie Websites, Blogs, Social Media (Soziale Netzwerke) bieten eine erstaunliche Fülle von Informationen. Folgend werden die einzelnen Quellen für Informationen vorgestellt und beschrieben.

3.1. Informationen von Websites

Die Firmen bzw. persönlichen Websites bieten Unmengen von Informationen. Hier beginnt ein Social Engineer mit seiner Suche nach wertvollen Informationen. (vgl. [6], Seite 58)

Folgende Informationen kann man auf Websites finden: (vgl. [6], Seite 58)

- Was macht jemand?
- Welche Produkte bzw. Dienstleistungen werden angeboten?
- Wo befindet sich geografisch gesehen das Gebäude?
- Stellenangebote
- Kontakttelefonnummern
- Biografien der Manager oder des Vorstandes
- Kundendienstforen
- Spezielle Wörter oder Formulierungen

Auf den persönlichen Websites kann man sehr oft sogar sehr persönliche Informationen, wie Angaben zu Kindern, Häuser, Arbeit usw. finden, meistens findet man mehrere Mitarbeiter einer Firma in den gleichen Foren oder Social Networks. So kann man sich ein gutes Bild von einer Firma verschaffen, da die Mitarbeiter auch sehr oft ihre Jobbezeichnung und ihre Abteilung online stellen. So kann ein Social Engineer sich sehr gut über die Abteilungsstruktur und die Jobbezeichnungen informieren. (vgl. [6], Seite 58)

3.2. Suchmaschinen

Über die Suchmaschinen bekommt man eine Menge Informationen, wenn man weiß, wie man die Fragen formuliert. Johnny Long hat dazu ein berühmtes Buch geschrieben namens „Google Hacking“. In diesem Buch hat er der Welt vor Augen geführt, dass man eine erstaunliche Menge an Informationen über Google herausfinden kann. (vgl. [6], Seite 59)

„Google vergibt, aber vergisst nie!“ ([6], Seite 59)

In diesem Buch zeigt Johnny Long, wie man über eine Zeichenfolge wertvolle Informationen einer Firma herausbekommen kann. Beispiel: `site:microsoft.com filetype:pdf` – hier bekommt man eine Liste aller PDF Dateien, die auf der Domäne microsoft.com liegen. (vgl. [6], Seite 59)

Ein äußerst wichtiger Teil der Informationsrecherche ist, sich mit diesen Themen zu befassen und sich die Operanden, die funktionieren, gut zu merken. Es gibt eine Reihe von Büchern, die sich mit dem Thema beschäftigen, wie man sich Daten über Suchmaschinen beschaffen kann. Erstaunlicherweise werden noch immer sehr viele Dateien von Mitarbeitern offen auf Servern liegen gelassen. (vgl. [6], Seite 59)

Hier der Funktionscheck des oben genannten Beispiels:

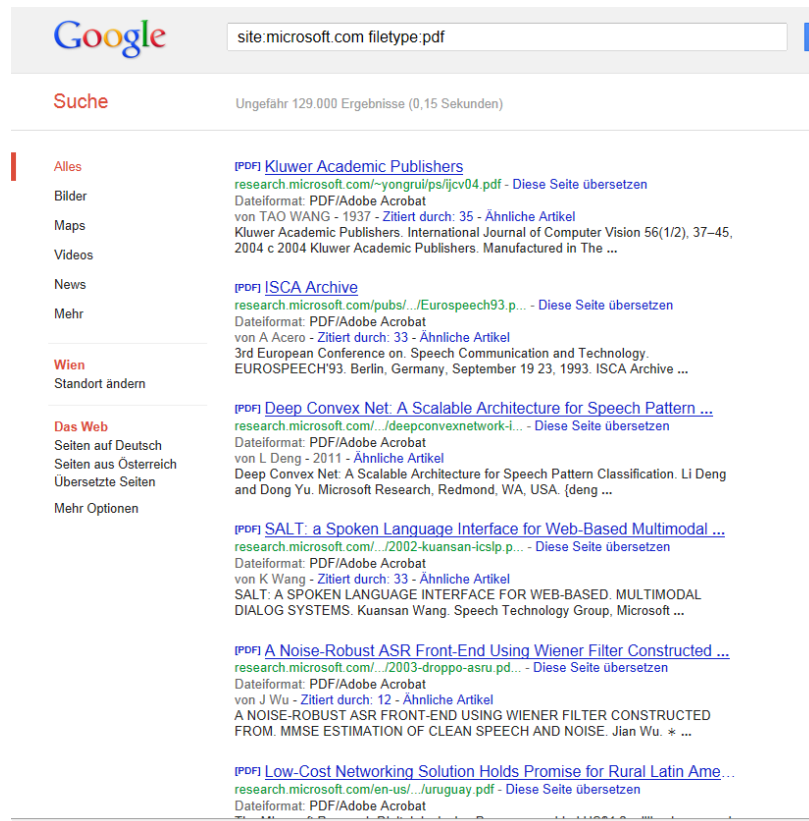


Abbildung 8: Google als Informationslieferant

Abbildung 9 zeigt, wie man Passwörter über Google herausfinden kann:

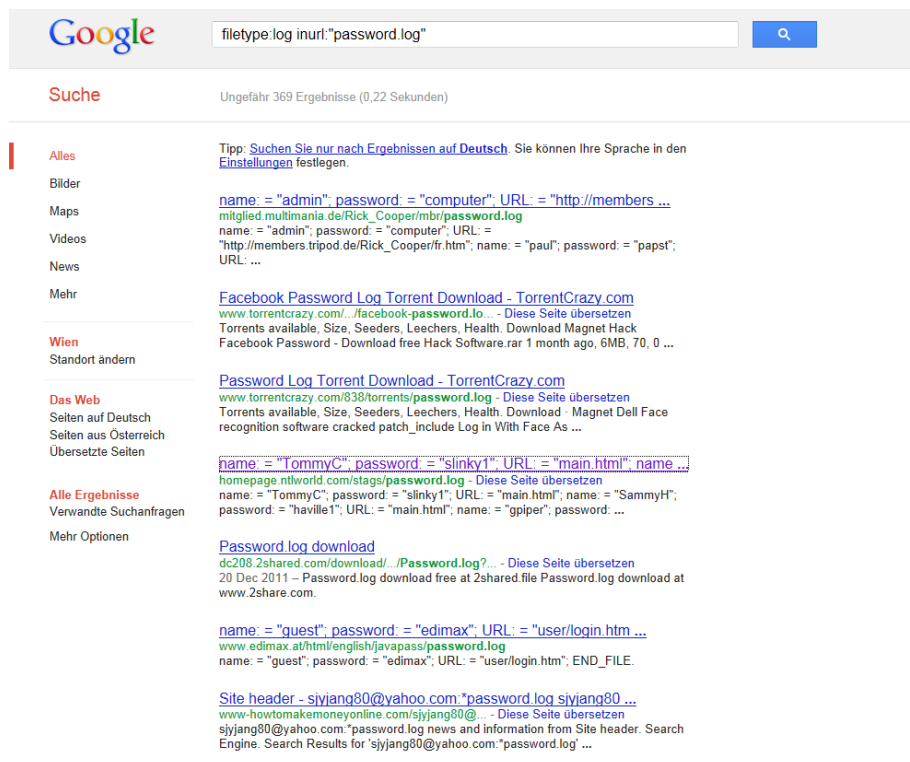


Abbildung 9: Passwörter mittels Google finden

Klickt man auf ein Suchergebnis kommt man zum Beispiel auf eine Liste der Passwörter (Abbildung 10):

```
name: = "TommyC";
password: = "slinky1";
URL: = "main.html";

name: = "SammyH";
password: = "haville1";
URL: = "main.html";

name: = "gpiper";
password: = "127612761";
URL: = "main.html";

name: = "admin";
password: = "pompeystage";
URL: = "main.html";

name: = "DjCabs";
password: = "Muddle";
URL: = "main.html";

name: = "legend";
password: = "shitmix";
URL: = "main.html";

name: = "daveh";
password: = "tripleh";
URL: = "main.html";

name: = "whiters";
password: = "mattw";
URL: = "main.html";

name: = "chrisvilkas";
password: = "qwerty";
URL: = "main.html";

name: = "tallpaul";
password: = "harold";
URL: = "main.html";

name: = "petef";
password: = "adidas";
URL: = "main.html";

name: = "mach";
password: = "justinp";
URL: = "main.html";

END_FILE
```

Abbildung 10: Ergebnis eines Beispiels

3.3. Social Media, User Sites, Blogs usw.

Social Media allgemein bietet eine weitere neue Informationsquelle für Social Engineering. In den letzten Jahren haben sich Soziale Netzwerke sehr stark entwickelt und sie sind zu einer richtigen Informationsdrehscheibe für Unternehmen, aber auch für Privat-Personen geworden. Firmen veröffentlichen Nachrichten über Events, neue Produkte, Pressemitteilungen und Storys, die sich mit aktuellen Ereignissen beschäftigen. In diesen Netzwerken (Facebook, Twitter, usw.) findet man frei verfügbare Informationen über das Leben und die Gegebenheiten anderer Menschen. Sie liefern eine erstaunliche Fülle umfassender Informationen. (vgl. [6], Seite 62)

Ein weiterer wichtiger Punkt der „neuen“ Medien sind User-Sites und Blogs. Denn in Blogs, Wikis usw. können User ihre Meinungen posten. So kann zum Beispiel ein verärgelter Mitarbeiter seine Probleme bloggen und er wird sicher jemanden finden, der ihm sein wohlwollendes Ohr schenkt. Ein weiteres Beispiel im Buch von Christopher Hadnagy ist, dass es auch Seiten gibt die nach Usern suchen, die Fotos per Smartphone ins Internet stellen. Dabei ist anzumerken, dass die meisten Smartphones die GPS Daten in das Foto einbetten und man so immer weiß, wo das Foto aufgenommen wurde. (vgl. [6], Seite 62)

„User posten immer ganz erstaunliche Datenmengen im Netz, die jeder sehen und lesen kann.“ ([6], Seite 62)

Mit all diesen Informationen kann man ein sehr gutes Profil der Zielperson erstellen. Denn die User lieben es, darüber zu twittern, wo sie sind, was sie machen und mit wem sie gerade zusammen sind. Wenn die Bilder die sie online stellen, dann auch noch Standortdaten enthalten und Sites, wie Facebook voller persönlicher Angaben stecken, weil sehr viele dort ihre Bilder, Storys und andere Infos veröffentlichen, dann sind das für einen Social Engineer paradiesische Zustände. Binnen kurzer Zeit kann man mit diesen Informationen ein vollständiges Profil zusammenstellen, in dem die Postanschrift, Angaben über Beruf, Bilder, Hobbys und vieles mehr enthalten ist. (vgl. [6], Seite 63)

3.4. Informationsquellen und Funktionen in sozialen Netzwerken

In diesem Kapitel werden einige Informationsquellen und Funktionen der sozialen Netzwerke beschrieben und anschließend werden Statistiken vorgestellt, die darstellen, welche Informationen preisgegeben werden und welche Funktionen genutzt werden. Daraus kann dann abgeleitet werden, welche Informationen und Funktionen für Angreifer besonders interessant sind.

Pinnwand

Die Pinnwand ist ein Ort zum Posten und Teilen von Inhalten mit Freunden. Es gibt verschiedene Möglichkeiten diese Inhalte den Freunden zur Verfügung zu stellen:

- **Teilen mit einem breiten Publikum:** Um die Informationen mit einem breiten Publikum zu teilen, kann man im „Teilen“ – Menü den Status aktualisieren und Fotos, Videos und Links mit anderen teilen. Diese Inhalte erscheinen als Beiträge auf dem Profil und können in den Neuigkeiten angezeigt werden. Damit diese Beiträge nur von bestimmten Personen angezeigt werden können, kann man für jeden geposteten Beitrag die Privatsphäre-Einstellungen ändern.

- **Teilen mit einer kleine Gruppe von Freunden:** Für diese Art der Informationsteilung eignet sich am besten die Gruppen-Funktion, hier kann man mit einer ausgewählten Gruppe von Personen seine Informationen teilen.
- **Teilen mit Einzelpersonen:** Man kann jederzeit Beiträge von Freunden „kommentieren“, d.h. man kann auf die Pinnwand eines Freundes schreiben und so Informationen austauschen. Diese Informationen können aber die anderen auch sehen. Will man seinem Freund etwas privates Mitteilen, so kann man eine private Nachricht senden. (vgl. [24])

Private Mitteilungen

Eine persönliche Nachricht kann man Freunden schicken, indem man auf den Button „Nachricht senden“ klickt. Die Person, der man eine Nachricht gesendet hat, wird entweder per E-Mail oder bei der nächsten Anmeldung bei Facebook über die Nachricht informiert. (vgl. [24])

Freunde

Freundschaftsanfragen, Freunde-Finder, als Freund hinzufügen – all das ist aus dem heutigen Leben nicht mehr wegzudenken. Facebook hat es geschafft das so emotional besetzte Wort „Freund“ zu vereinnahmen. Alle Funktionen der Website sind rund um diese Freundschaftsbeziehungen aufgebaut. Diese Freundschaftsbeziehungen bedeuten aber nichts anderes als eine Verbindung der beiden Profile. So eine Verbindung tritt in Kraft wenn beide die „Freundschaftsanfrage“ angenommen haben, wobei in der Regel von einem der beiden die Freundschaftsanfrage losgeschickt wird und vom anderen dann beantwortet wird. Mit der Bestätigung der Freundschaftsanfrage bekommen beide den Zugriff auf das Profil des Anderen. Das heißt ab diesen Zeitpunkt haben sie vollen Zugriff auf die Daten des anderen. Will man z.B. dass Arbeitskollegen oder Schulkollegen nicht dasselbe sehen, wie zum Beispiel „echte gute Freunde“ so kann man sie in Unterlisten zusammenfassen und diesen Listen unterschiedliche Berechtigungen geben. So kann man zwar „befreundet“ bleiben und es wird doch nicht alles preisgegeben.

Jedes Mitglied auf Facebook darf 5000 Freunde haben und im Durchschnitt hat jeder User ca. 130 „Freunde“. (vgl. [14], Seite 14 und 15)

Folgende Statistik (Abbildung 11) zeigt, dass die meisten User zwischen 50 und 200 Freunde haben:

Wie viele Personen haben Sie in den Kontaktlisten Ihrer sozialen Netzwerke insgesamt?

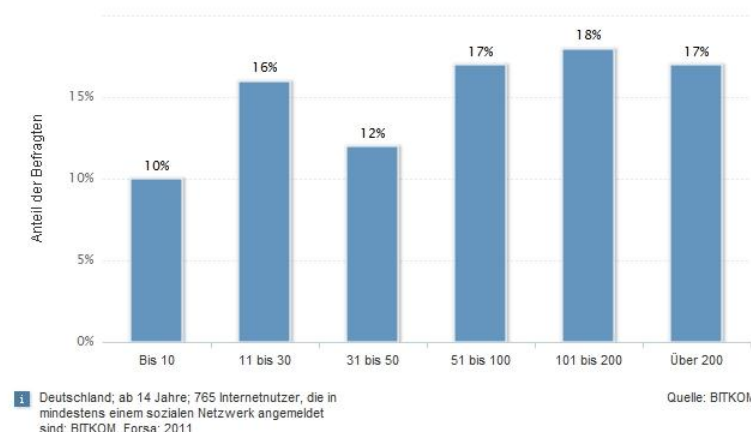


Abbildung 11: Freunde pro User [2] basierend auf ([25], Seite 6)

Der sogenannte „Freunde-Finder“ ist eine Software, die es ermöglicht die Freundeslisten zu vergleichen und dementsprechend dann Freunde vorschlägt. Außerdem ist es möglich auf Wunsch die eigenen E-Mail Kontakte zu importieren und abzugleichen ob es Facebook-Mitglieder gibt, denen man regelmäßig elektronische Post schickt.

Ein weiteres Problem der Facebook Freunde ist, dass die Freunde der Freunde automatisch Zugriff auf die Profile der anderen bekommen. Somit haben die Freunde der Freunde auch Zugriff auf Profile von Leuten die sie gar nicht kennen. (vgl. [14], Seite 14 – 16)

Veranstaltungen

Unter dem Punkt Veranstaltungen kann man Treffen organisieren, auf Einladungen antworten oder einfach auf dem Laufenden bleiben und sich informieren, was die Freunde so machen. (vgl. [24])

Gruppen, Seite und Communitys

Gruppen können von jedem Nutzer selbst gegründet werden oder man kann auch Gruppen beitreten. Es kann quasi zu jedem Thema eine neue Gruppe ins Leben gerufen werden. Diese Gruppen sind entweder geschlossen, so dass nur Nutzer Einblick haben, die eingeladen wurden oder sie können auch offen für alle Nutzer sein. (vgl. [9], Seite 121)

Bei Facebook gibt es noch weitere Typen von Seiten, nämlich die offiziellen Seiten (Pages), Gruppen sowie die Gemeinschaftsseiten (Communitys). Diese Seiten ermöglichen es Firmen, Interessensgruppen usw. auch am Facebook-Geschehen teilzunehmen. Die „offiziellen Seiten“ sind für Firmen, Marken, Produkte, Organisationen oder Personen, die im öffentlichen Leben stehen gedacht. Diese Seiten sind sozusagen vereinfachte Homepages, die sich in den Funktionalitäten von den Normalbenutzern unterscheiden. Ein wesentliches Merkmal dieser Seiten ist, dass die Nutzer diese Seiten „ liken“ können, das heißt sie können mit dem „Gefällt mir“-Button kennzeichnen, dass ihnen dieses Produkt, diese Firma usw. gefällt. Mittels diesen „Gefällt mir“-Button kennzeichnet man auch auf seinem Profil seine Interessen und Vorlieben. Diese Seiten bieten meistens Status-Updates, Fotos, Videos, Veranstaltungen und ein Diskussionsforum. Außerdem besteht die Möglichkeit sogenannte „Targeted-Updates“ an die Nutzer der Seite zu schicken, um so die „Fans“ „auf dem Laufenden zu halten“. Die Erstellung solcher Seiten ist ausschließlich dem rechtmäßigen Vertreter einer bestimmten Persönlichkeit oder Marke erlaubt. Erstellt eine Privatperson solch eine Seite, so riskiert sie gesperrt zu werden, denn Facebook kontrolliert diese Seiten. (vgl. [14], Seite 25 und 26)

Privatpersonen können aber sogenannte Communitys gründen um über gemeinsame Themen zu diskutieren. Diese Communitys besitzen eine Pinnwand, einen Video- und Foto- Bereich, Diskussionsforen und einen Veranstaltungskalender. Allerdings kann man diese Communitys nicht auf „geschlossen“ stellen - dies stellt auch den wesentlichen Unterschied zur Gruppe dar. Bei einer Gruppe kann der Gründer selbst entscheiden, welche Personen der Gruppe beitreten dürfen oder nicht. Bei den Communitys handelt es sich um öffentliche Informationen. (vgl. [14], Seite 26)

Fotos und Videos

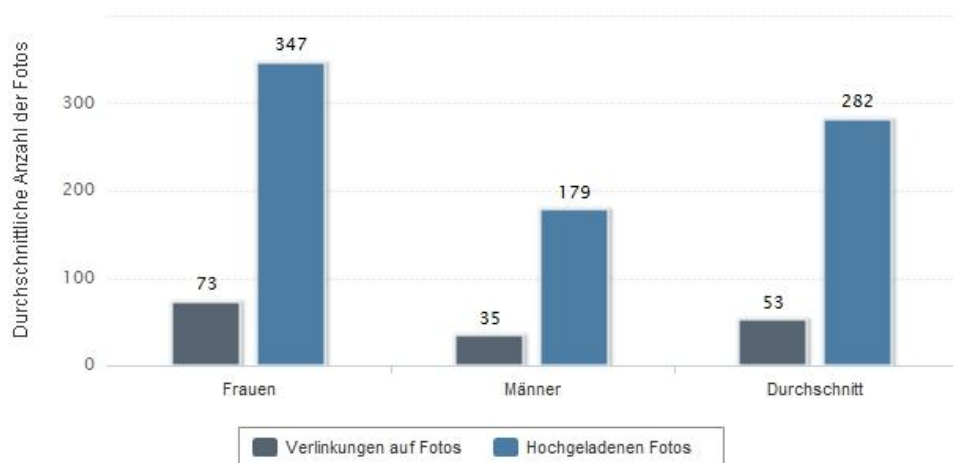
User lieben die Foto- und Video- Funktion in sozialen Netzwerken. Bis Ende 2009 waren auf Facebook-Server ca. 30 Milliarden Fotos gespeichert und es werden täglich mehr, denn im Durchschnitt lädt jeder Benutzer ca. sieben bis acht Fotos pro Woche hoch. Facebook setzt alles daran, den Benutzern das Hochladen der Fotos sehr einfach zu gestalten. So gibt es schon Kameras mit einer Funktion, die die Fotos gleich direkt ins

Facebook-Profil lädt. Dieser Trend wird sicher noch mehr werden und so wird sich bis 2013 das Volumen der Fotos auf Facebook versechsfachen. Für Videos gelten im Prinzip die gleichen Regeln wie für Fotos, man kann sie über die Website hochladen oder auch direkt vom Handy aus. (vgl. [14])

Markierung von Fotos

Mit Markierungen kann man Verknüpfungen zu Personen, Seiten oder Orten herstellen. So kann man zum Beispiel markieren, wer auf den Fotos zu sehen ist oder Statusmeldungen zu den Fotos schreiben, damit man den Freunden mehr zu den Fotos mitteilen kann. (vgl. [26])

Durchschnittliche Anzahl der hochgeladenen und verlinkten Fotos von Facebook-Nutzern weltweit nach Geschlecht (Stand: Januar 2011)



1 Weltweit; Pixable; Stand: Januar 2011

Quelle: Pixable

Abbildung 12: Durchschnittliche Anzahl der hochgeladenen Fotos [2] basierend auf [27]

Abbildung 12 zeigt die durchschnittliche Anzahl der hochgeladenen und verlinkten Fotos von Facebook-Nutzern, weltweit nach Geschlecht im Januar 2011, weibliche Facebook-Nutzer sind dabei im Durchschnitt auf 73 Fotos verlinkt.

Gesichtserkennung

Mitte 2011 hat Facebook die neue Funktion der Gesichtserkennung eingeführt. Bei der Einführung wurde die automatische Gesichtserkennung auf Fotos in Benutzerprofilen aktiviert. Mit diesem Dienst versucht Facebook die hochgeladenen Fotos mit Namen zu verlinken. Will man diese Funktion nicht nutzen, muss man in den benutzerdefinierten Einstellungen den Punkt „Freunden Fotos von mir vorschlagen“ bearbeiten. (vgl. [28])



Abbildung 13: Gesichtserkennungseinstellungen auf Facebook [28]

3.4.1. Zur Verfügung gestellte persönliche Informationen in sozialen Netzwerken

In diesem Kapitel werden einige Statistiken vorgestellt, die das veröffentlichen von persönlichen Daten betreffen.

Laut Datenschutzgesetz §4 gibt es folgende Definition zu „Daten“ bzw. „sensible Daten“:

„§ 4 „Daten“ („personenbezogene Daten“): Angaben über Betroffene (Z 3), deren Identität bestimmt oder bestimmbar ist; „nur indirekt personenbezogen“ sind Daten für einen Auftraggeber (Z 4), Dienstleister (Z 5) oder Empfänger einer Übermittlung (Z 12) dann, wenn der Personenbezug der Daten derart ist, daß dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann;

2. „sensible Daten“ („besonders schutzwürdige Daten“): Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben.“ [29]

Diese Daten gelten laut Datenschutzgesetz als schützenswert. Doch wie einige Statistiken im Folgenden zeigen werden, werden sowohl personenbezogene, als auch sensible Daten von den Benutzern in sozialen Netzwerken angegeben.

Abbildung 14 zeigt, dass 30,80% der Befragten starken Bedenken haben, wenn sie persönliche Daten, Fotos oder Videos online stellen. 53,80% haben leichte Bedenken und 15,40% haben überhaupt keine Bedenken.

Inwieweit haben Sie Bedenken, Persönliches (Daten, Fotos, Videos, etc.) auf Social Media Plattformen bzw. Web 2.0-Sites zu veröffentlichen?

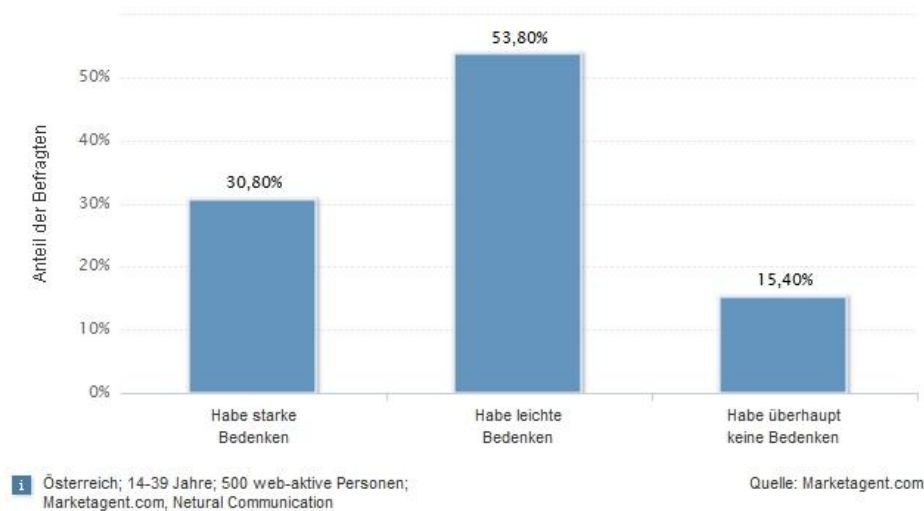


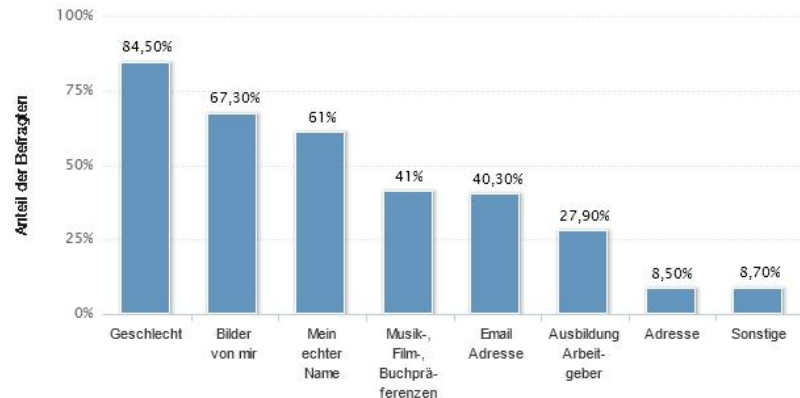
Abbildung 14: Bedenken beim Veröffentlichen von persönlichen Daten [2] basierend auf [30]

In den folgenden zwei Statistiken (Abbildung 15 und Abbildung 16) wird die Angabe, welche Daten veröffentlicht werden schon genauer.

Laut diesen Statistiken werden Vor – bzw. Nachname zu 77% angegeben, das Geschlecht wird sogar zu 84,50% veröffentlicht. Alter und Bilder folgen mit 76% und 67,30%. Etwas kritischer wird es meiner Meinung nach schon bei der Email Adresse, die zu 40,3% veröffentlicht wird und bei der Telefonnummer, die immerhin zu 8% online gestellt wird. Mit der Adresse (8,5%) und dem aktuellen Aufenthaltsort (5%) sollte auch sehr vorsichtig umgegangen werden. 7% der Befragten geben an, Fotos von anderen online zu stellen, ohne deren Erlaubnis – auch dies kann zu Problemen führen, denn laut Urheberrechtsgesetz § 78 ist die Veröffentlichung von Fotos ohne Zustimmung der Abgebildeten verboten.

„§ 78. Bildnisse von Personen dürfen weder öffentlich ausgestellt noch auf eine andere Art, wodurch sie der Öffentlichkeit zugänglich gemacht werden, verbreitet werden, wenn dadurch berechnigte Interessen des Abgebildeten oder, falls er gestorben ist, ohne die Veröffentlichung gestattet oder angeordnet zu haben, eines nahen Angehörigen verletzt würden.“ [29]

Welche der folgenden Informationen geben Sie in Social Media Plattformen über sich preis?



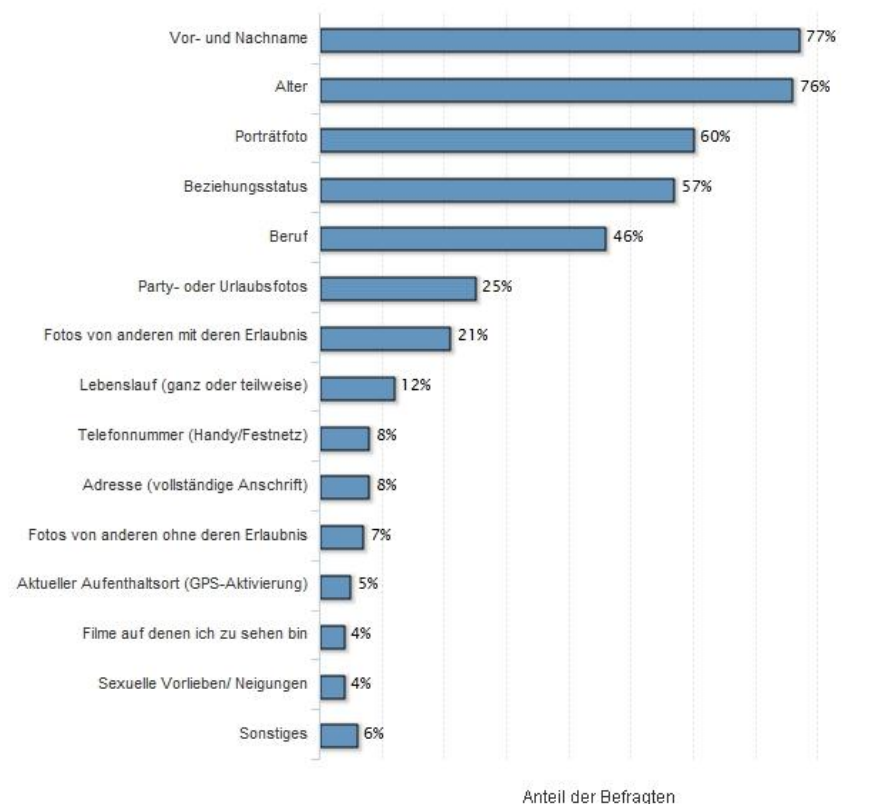
Deutschland; 1.099 Nutzer von Social Media Plattformen; Tomorrow Focus Media; Oktober 2010

Quelle: Tomorrow Focus Media

© Statista 2012

Abbildung 15: Persönliche Daten in sozialen Netzwerken [2] basierend auf [31]

Welche der folgenden persönlichen Daten und Infos haben Sie in mindestens einem sozialen Netzwerk angegeben?



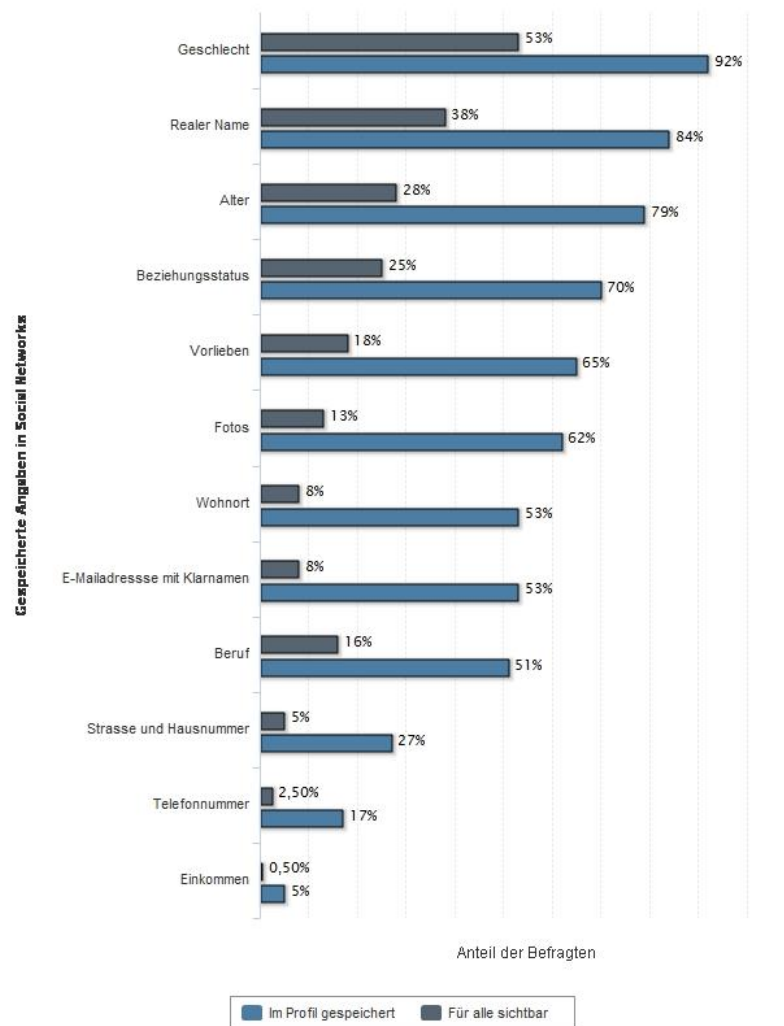
Deutschland; ab 14 Jahre; 765 Internetnutzer, die in mindestens einem sozialen Netzwerk angemeldet sind; BITKOM, Forsa; 2011

Quelle: BITKOM

Abbildung 16: Persönliche Daten in sozialen Netzwerken II [2] basierend auf ([25], Seite 7)

Abbildung 17 zeigt, welcher der angegebenen persönlichen Daten auch für alle Nutzer der sozialen Netzwerke sichtbar sind. 92% geben das Geschlecht an und 53% davon machen dieses öffentlich sichtbar, 84% geben den richtigen Namen in den sozialen Netzwerken an und davon machen 38% diesen öffentlich einsehbar. Sehr verblüffend ist, dass 17% ihre Telefonnummer angeben und sogar 2,5% diese öffentlich sichtbar machen. Bei der Wohnadresse sind es sogar 27% der Befragten die diese angeben und davon machen sie 5% öffentlich sichtbar. Hier sieht man sehr schön, dass sehr viele Nutzer die „Privatsphären Einstellungen“ nicht nutzen.

Welche Ihrer persönlichen Daten sind in Ihrem Social Network Profil gespeichert und welche sind für alle sichtbar?



i Deutschland; ab 14 Jahre; 1.604 Internetnutzer;
November 2010

Quelle: TNS Infratest

Abbildung 17: Persönliche Daten in sozialen Netzwerken, die für alle sichtbar sind [2] basierend auf [32]

Auch hier (Abbildung 18) sieht man sehr schön, dass schon sehr viele Nutzer der sozialen Netzwerke ihre Daten schützen, doch nicht alle. Und genau diejenigen, die ihre Daten nicht schützen, sind für Social Engineers sehr leicht zu erreichen.

Für wen sind Ihre Daten auf dem Profil sichtbar?

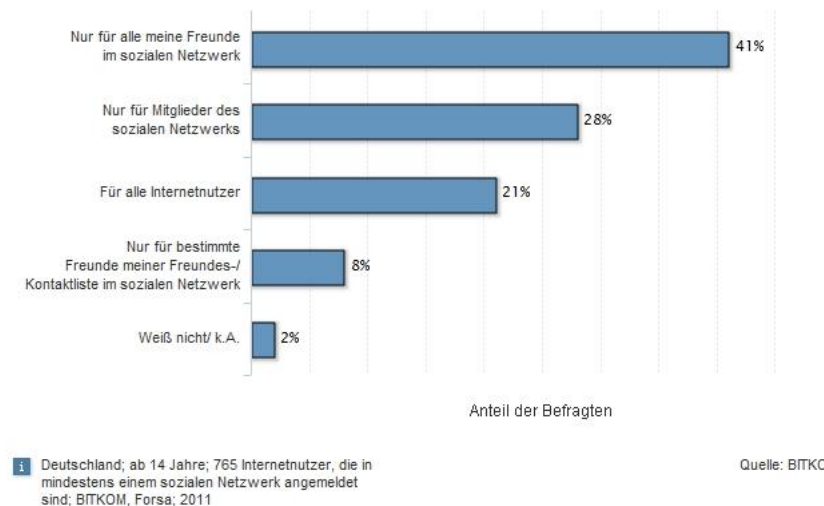


Abbildung 18: Datensichtbarkeit [2] basierend auf ([25], Seite 8)

Eine weitere Statistik (Abbildung 19) zeigt, wie wichtig der persönliche Schutz der Daten für die Benutzer ist. Hier wird verdeutlicht, dass die vielen Initiativen für den Schutz von persönlichen Daten in sozialen Netzwerken schon greifen und die User schon umdenken, doch sind es noch nicht alle die die Wichtigkeit des Datenschutzes erkannt haben.

Wie wichtig ist für Sie der persönliche Schutz Ihrer Privatsphäre im Internet?

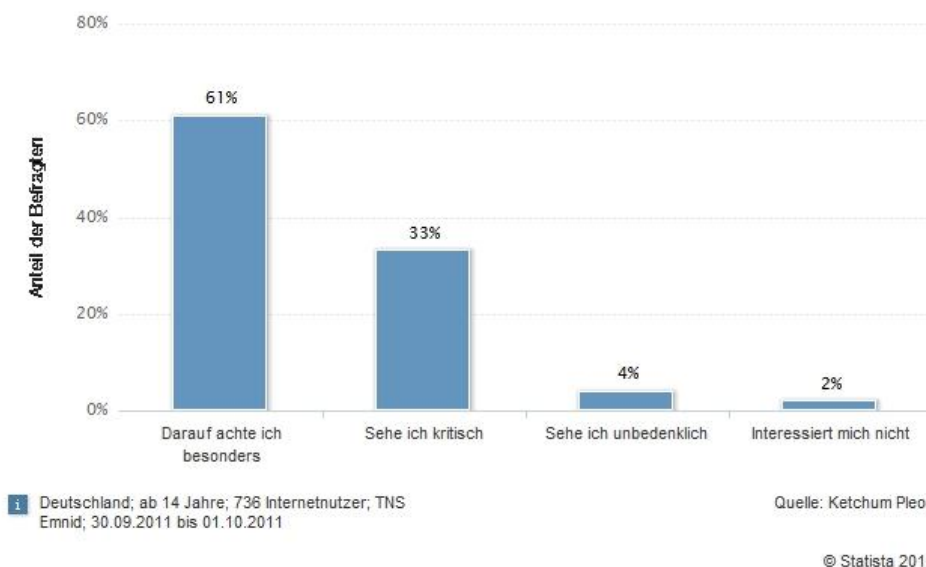
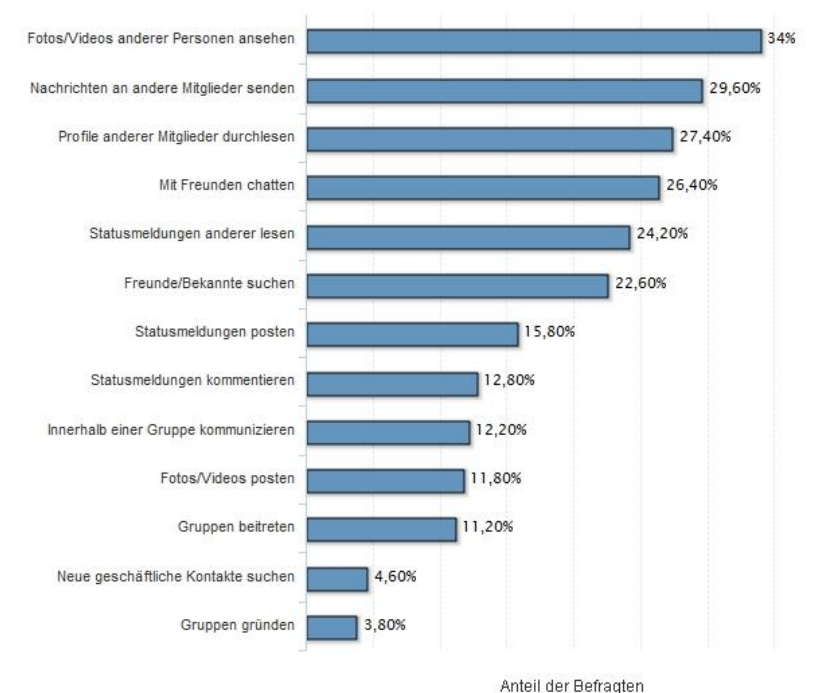


Abbildung 19: Schutz der Daten [2] basierend auf [32]

3.4.2. Genutzte Funktionen in sozialen Netzwerken

Die Funktionen in sozialen Netzwerken sind vielfältig und werden unterschiedlich häufig genutzt. Nachrichten schicken (29%), Fotos/Videos anderer anschauen (34%) und mit Freunden chatten (26%) sind die am häufigsten genutzten Funktionen. Aber auch Statusmeldungen lesen, posten und kommentieren, gehört zu den häufig genutzten Funktionen.

Aktivitäten, die auf Social Media Plattformen am häufigsten durchgeführt werden



1 Österreich; 14-39 Jahre; 500 web-aktive Personen;
Marketagent.com, Netural Communication

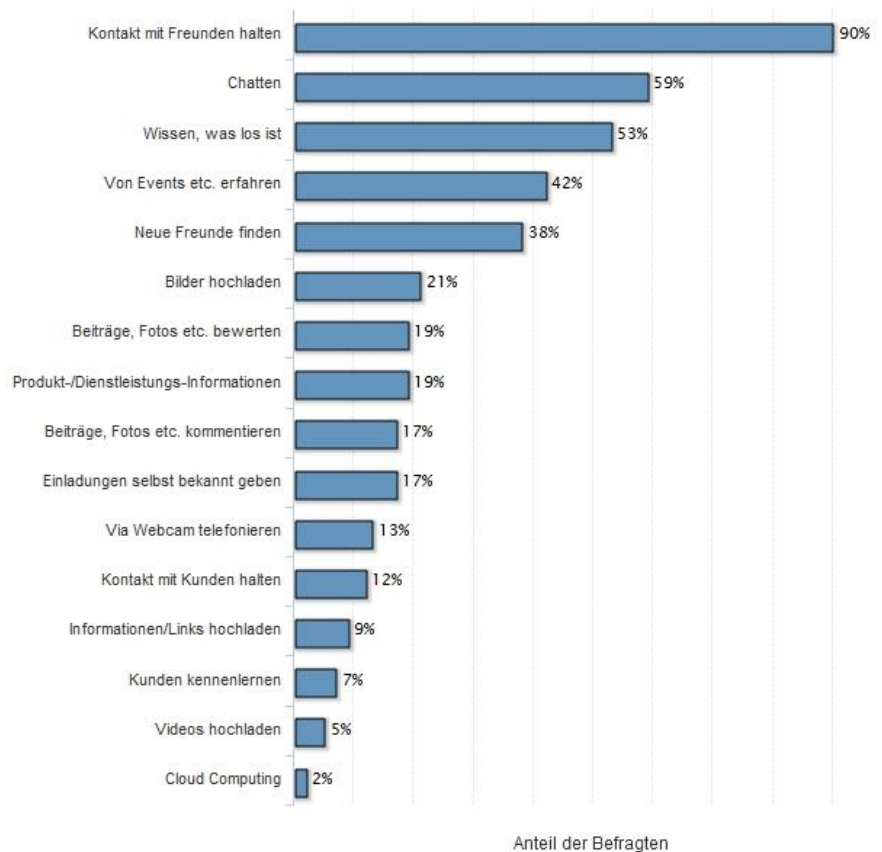
Quelle: Marketagent.com

Abbildung 20: Aktivitäten in sozialen Netzwerken [2] basierend auf [30]

All diese Funktionen können aber auch von Angreifern genutzt werden, um Schadsoftware oder ähnliches einzuschleusen bzw. können mittels diesen Funktionen User gezielt gemobbt oder beleidigt werden.

Eine weitere Statistik (Abbildung 21) zeigt, dass die Funktionen, wie Kontakt mit Freunden halten (90%), Chatten (59%), „Wissen, was los ist“ (53%) usw. sehr wichtig für die Nutzer der sozialen Netzwerke sind. Diese Statistik verdeutlicht, dass die sozialen Netzwerke ein Informationsaustausch-Medium geworden sind und viele dieses Medium auch dafür benutzen sehr persönliche Dinge preis zu geben bzw. mit anderen zu bereden.

Welche der folgenden Funktionen in sozialen Netzwerken sind für Sie persönlich wichtig?



i Deutschland; ab 14 Jahre; 637 Nutzer sozialer Netzwerke; SINUS-Institut Heidelberg

Quelle: Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)

© Statista 2012

Abbildung 21: genutzte Funktionen in sozialen Netzwerken [2] basierend auf [33]

3.5. Automatisierte Informationsgewinnung

Folgendes Kapitel beschäftigt sich mit Tools bzw. mit Möglichkeiten, wie man automatisiert oder auf ziemlich einfache Weise an sehr viele persönliche Daten kommt. Im Zeitalter des Web 2.0 ist es für Social Engineers oder Angreifer sehr einfach geworden die Angriffe auf Personengruppen zuzuschneiden, dadurch erhöht sich natürlich der Erfolgsfaktor dieser Angriffe.

Automatisiertes Sammeln von E-Mail Adressen

Mit den sozialen Netzen hat sich eine neue Möglichkeit ergeben, E-Mail Adressen zu sammeln. Da die sozialen Netzwerke von Millionen von Usern aus der ganzen Welt genutzt werden, haben sich Angreifer bereits jetzt auf diese Netzwerke spezialisiert und neue Techniken gefunden, um über diese Plattformen E-Mail Adressen herauszufinden. Schlussendlich ist es nämlich egal, wie sicher die Nutzer mit ihren Daten umgehen, denn es genügt schon alleine der Name, um Email Adressen zu sammeln. Der Name ist genug Information für den Angreifer, um nach der E-Mail Adresse zu suchen, dies ist viel effizienter als mit den traditionellen Methoden. (vgl. [12])

Folgend werden zwei neuen Techniken zum Sammeln von E-Mail Adressen beschrieben:

Blind harvesting

Diese Methode sucht blind nach E-Mail Adressen. Diese Methode gibt es schon sehr lange, aber mit den sozialen Netzwerken ist die Effizienz der Methode um einiges gestiegen, denn nun werden soziale Netzwerke in Verbindung mit Suchmaschinen wie Google benutzt.

Es werden die sozialen Netzwerke nach Namen durchsucht und anschließend können über Google E-Mailadressen herausgefunden werden. Ein sehr effizienter Weg, um auf Namen zu kommen, sind Fan-Seiten in Facebook, denn hier weiß man dann auch gleich welche Personen welche Interessen haben. (vgl. [12])

Target harvesting

Die Methode „Target harvesting“ geht gezielter vor, denn mit dieser Methode möchte man auch auf persönliche Informationen kommen, damit man gezielter Phishing Mails verschicken kann. Hier gibt es wiederum zwei Möglichkeiten, die eine Möglichkeit wird für Facebook und die andere für Twitter verwendet.

Reverse Lookup Emails auf Facebook

Hier wird die Facebook-Suche verwendet, um an E-Mail Adressen heranzukommen. Danach wird auch nach öffentlichen Informationen der User gesucht und hier kann natürlich auch die Freundschaftsanfrage sehr hilfreich sein, denn es gibt sehr viele Nutzer die Freundschaftsanfragen einfach nicht ablehnen. Laut einer wissenschaftlichen Publikation gab es eine Erfolgsquote von 30% bei den Freundschaftsanfragen. Ist man dann mit dem „Opfer“ als Freund verbunden, so kann man natürlich auf alle persönlichen Daten zugreifen. Bei dieser Methode wollen sich die Angreifer einfach die unnötigen E-Mails, die sowieso nie ankommen, ersparen und investieren dafür mehr Zeit in die Recherche. (vgl. [12])

Nickname based E-Mail harvesting

Bei dieser Methode handelt es sich um eine Twitter-Funktion, hier werden über Twitter-Nicknamen gesucht und anschließend über Google oder andere Suchmaschinen E-Mail Adressen herausgefunden. Hier wird auch damit spekuliert, dass die Nutzer den gleichen Nicknamen auf mehreren Websites verwenden. (vgl. [12])

Mit der Twitter-Suchfunktion (search.twitter.com) kann man auch zum Beispiel mittels „@hotmail.com“ nach E-Mail Adressen suchen. Abbildung 22 zeigt, wie das Ergebnis aussieht wenn man @hotmail.com in die Twitter Suchfunktion eingibt.



Abbildung 22: Twitter Suchfunktion

Friend-in-the-Middle Attacks – Ausnützung der Sozialen Netzwerke für Spam

Die Friend-in-the-Middle Attacke ist eine neue Art von Angriffen, die es ermöglicht, aus den sozialen Netzwerken wertvolle Informationen herauszubekommen. Mit der Beliebtheit der sozialen Netzwerke, ist auch die Beliebtheit der Angriffe auf soziale Netzwerke gestiegen. Mittlerweile haben sich Angreifer schon sehr stark darauf spezialisiert und entwickeln immer neue Methoden um an die Daten der sozialen Netzwerke zu kommen. Da es sehr viele unterschiedliche Privatsphären-Einstellungen gibt, ist es nicht so einfach auf die Daten der User zu kommen. An diesem Punkt setzt der Friend-in-the-Middle (FiTM) Angriff an, denn er überwindet dieses Hindernis durch Hijacking http Sitzungen.

Dieser Angriff ist auch für Social Engineering sehr interessant, da mit diesem automatisierten FiTM Angriff sehr ausgefeilte Angriffe geplant werden können. (vgl. [34])

Freund Ausnützung (Friend injection)

Die Vernetzung in den sozialen Netzwerken funktioniert über die „Freunde“, ist man mit jemanden eine Freundschaftsbeziehung eingegangen, so erlaubt man den anderen den Zugriff auf sein volles Profil. Diesen Punkt macht sich die FiTM Attacke zum Ziel, denn sie übernimmt eine „social network session“ und kann somit im Namen vom Opfer den Freundschaftsanfragen zusagen. Ab dem Zeitpunkt der Zusage kann der Angreifer auf alle Daten des Opfers zugreifen. (vgl. [34])

Ausnützung mittels Applikation (Application injection)

Sehr beliebt sind auch Applikationen wie Spiele. Mittels dieser Applikationen könnte ebenfalls ein Angriff gestartet werden, indem eine Applikation geschrieben wird, die die Daten dann automatisch abfängt bzw. herunterlädt. (vgl. [34]) Selbst so eine Applikation kann mittels einer entführten Benutzersitzung (Session)

hinzugefügt werden. Diese kann dann benutzt werden, um die Daten dieses Benutzerkontos zu extrahieren. (vgl. [8], Seite 9)

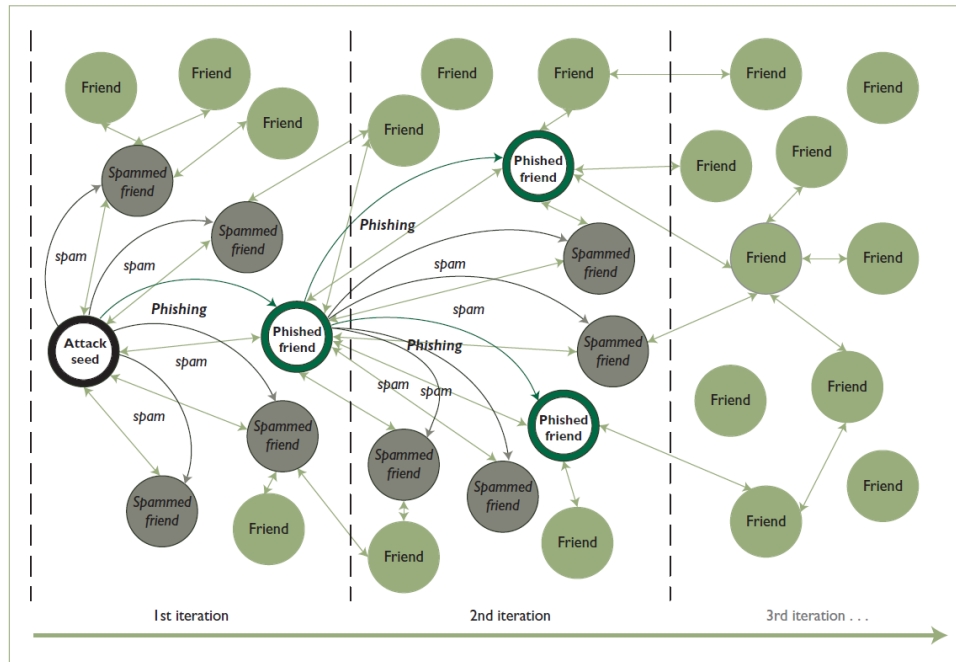


Abbildung 23: Friend-in-the-middle Attacke [34]

Abbildung 23 stellt einen Friend-in-the-middle Angriff grafisch dar. Die Abbildung gibt einen Überblick einer Spam Kampagne auf Basis des FiTM-Angriffes. Als erstes wird die Netzwerkverbindung überwacht und sobald eine aktive Social-Network-Session erkannt wird, wird der komplette http-Header inklusive der Session-Cookies geklont. Im nächsten Schritt wird dieser geklonte Header als Authentifizierungsschlüssel verwendet, um die Benutzersession zu übernehmen. Nun können Profilinhalte sowie Information über die Ziel-Freunde extrahiert werden und auch spezielle Drittanwendungen (Applikationen) hinzugefügt und anschließend wieder entfernt werden. Die extrahierten E-Mail Adressen und Profilinhalte können anschließend verwendet werden, um maßgeschneiderte Spam- und Phishing Mails zu generieren. (vgl. [8], Seite 10)

FBPWn Tool

Mit dem Tool „FBPWn“ kann man mit wenigen Einstellungen vollautomatisch Daten von Facebook-Usern abgreifen. Das Tool klonst die Identität von Freunden der Nutzer und schickt dann einen „Friend Request“. Nimmt das Opfer die Freundschaftsanfrage an so lädt die Software binnen Sekunden alle einsehbaren Daten des Profils herunter.

Die Software wurde von Technikern des ägyptischen Unternehmens „Raya IT Security Services Team“ programmiert. Der Hintergrund der Techniker ist nicht die Daten missbräuchlich zu verwenden, sondern sie wollen damit die Möglichkeiten und Gefahren der Social Engineering Techniken aufzeigen und darauf aufmerksam machen.

Das Tool kann unter folgendem Link heruntergeladen werden: <http://code.google.com/p/fbpwn/> (vgl. [35])

Maltego

Maltego ist das „Traum Tool“ für jeden Social Engineer und noch dazu ist es in einer Gratis-Version verfügbar. Will man die Einschränkungen der Gratis-Version entfernen (Anzahl der Transformationen, Speichern von Daten, usw.), bekommt man um ca. 650\$ eine vollständige Lizenz.

Christopher Hadnagy erzählt in seinem Buch eine Geschichte wie er mittels diesem Tool zahlreiche wertvolle Informationen herausgefunden hat. Er war beauftragt ein Sicherheitsaudit durchzuführen und wollte dabei den CEO unter die Lupe nehmen, dieser nutzte das Web nicht sehr ausführlich und trotzdem hat er binnen kürzester Zeit mittels Maltego folgende Informationen herausgefunden: (vgl. [6], Seite 348 und 349)

- Sein Liebessessen
- Sein Lieblingsrestaurant
- Namen und Alter seiner Kinder
- Dass er geschieden ist
- Die Namen seiner Eltern
- Den Namen seines Bruders
- Wo er aufgewachsen ist
- Seine Konfession
- Sein Lieblingsteam im Sport, usw.

Mittels dieser Informationen konnte er dann eine gezielte E-Mail verfassen mit einem PDF Anhang, wo natürlich eine Reverse Shell eingebaut war. Mittels eines Telefonats konnte er noch herausfinden, ob er das E-Mail wirklich bekommen und auch geöffnet hat. (vgl. [6], Seite 348 und 349)

Folgend werden einige Beispiele gezeigt, wie man mit Maltego zu nützliche Informationen kommt.

Abbildung 24 zeigt, wie man zu einen Namen E-Mail Adressen und Facebook Accounts herausfinden kann.

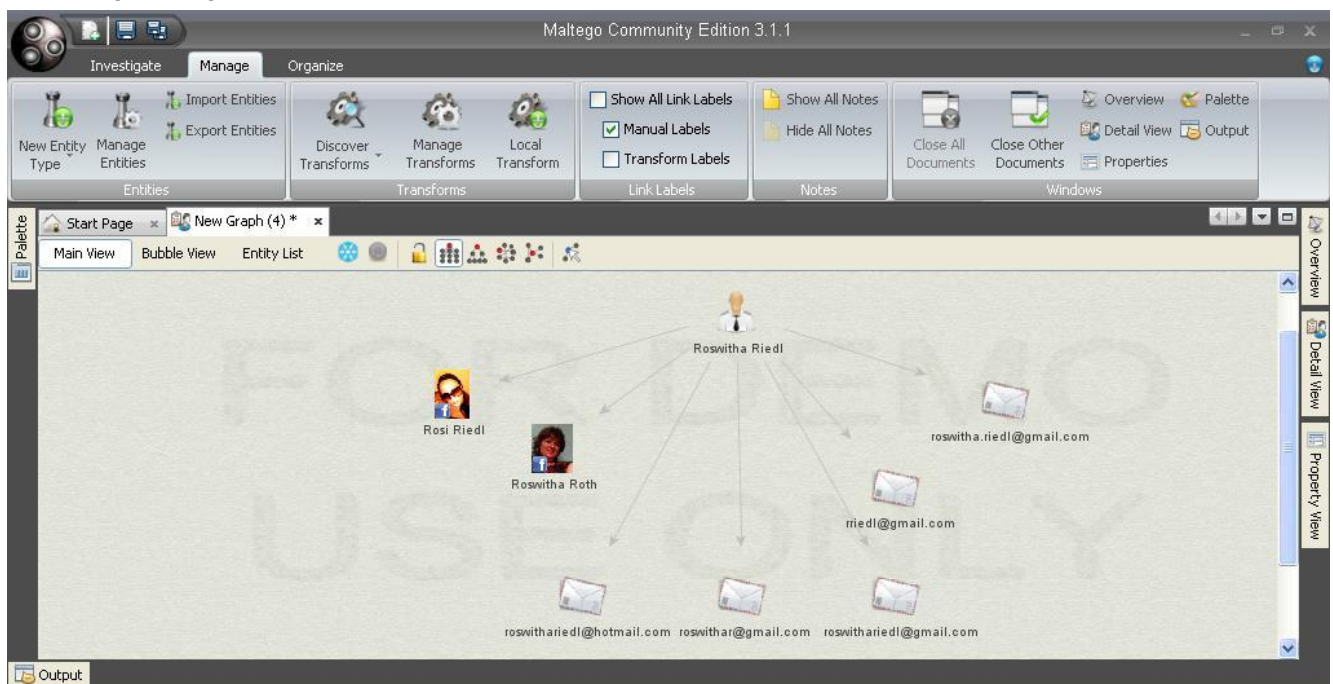


Abbildung 24: Maltego (Personensuche)

Abbildung 25 veranschaulicht, wie man zu einer Domäne E-Mail Adressen herausfinden kann und in weiterer Folge zu einer E-Mail Adresse weitere E-Mail Adressen und auch Accounts, wie zum Beispiel Flickr. Hierfür sind in Maltego nur wenige Schritte nötig. Man zieht sich eine Domäne heraus und gibt den Namen der Domäne ein, anschließend fügt man die „E-Mail Transformation“ hinzu und schon bekommt man die E-Mail Adressen. Genauso geht man für Name, Accounts usw. vor.

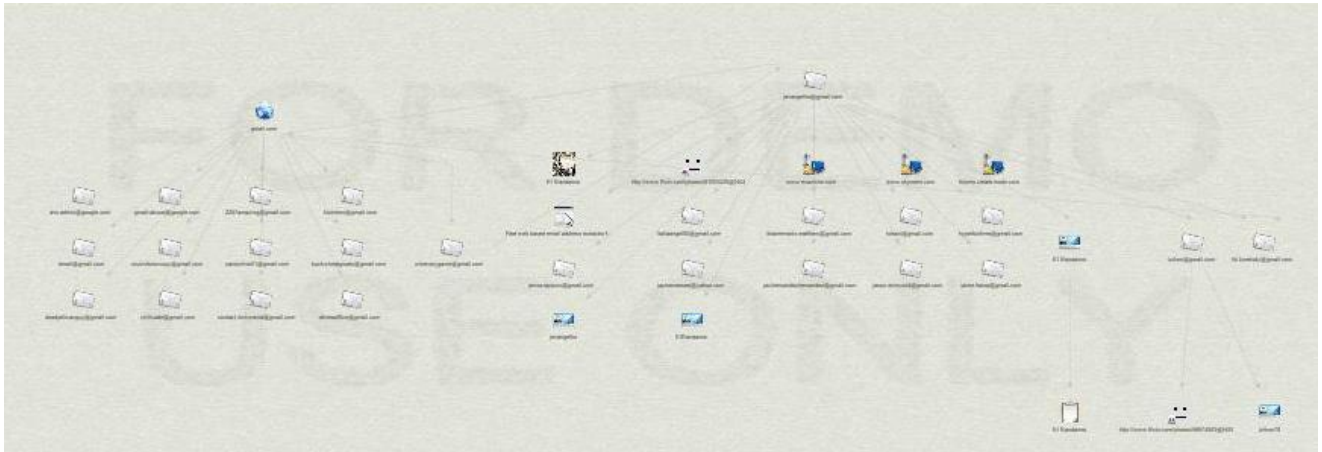


Abbildung 25: Maltego (E-Mail und Accounts)

In Abbildung 26 sieht man, dass zu der E-Mail Adresse ein Flickr Account gefunden wurde.



Abbildung 26: Maltego – gezielte Accountsuche

Social Engineer Toolkit (SET)

Das Social Engineer Toolkit ist ein Programm mit dem man PDF's und E-Mails automatisiert erstellen und verschicken kann, die heimtückischen Code enthalten. Dieses Tool wurde bereits bis 2011 1,5 Millionen Mal heruntergeladen und hat sich schnell zum Standard-Toolkit für Social Engineering Audits etabliert.

Heruntergeladen kann es unter www.social-engineer.org werden.

Standardmäßig ist dieses Tool (SET) bei BackTrack4 installiert, sonst kann es einfach nachinstalliert werden.

Spear Phishing mit SET

Was genau unter Phishing und Spear Phishing verstanden wird, wird in Kapitel 4.3 genau erklärt. Phishing zu erkennen und abzuschwächen, ist das Überleben in der heutigen Internetwelt unverzichtbar.

Mit SET kann der Auditor seine Kunden testen, indem er passend zugeschnittene E-Mails entwickelt und diese an seine Kunden verschickt. Nun kann er mitprotokollieren wie viele Angestellte auf diese Angriffe hereinfallen und kann diese Informationen für Schulungen verwenden um den Mitarbeitern solche Fallen vor Augen zu führen.

Mit dem SET kann man 3 verschiedene Spear Phishing Angriffe starten. Es kann ein Spear Phishing Angriff basierend auf E-Mails gestartet werden, es kann ein böswilliges PDF oder eine andere Datei erstellt werden oder es können Vorlagen für die spätere Nutzung erstellt werden.

Anschließend wird vom Tool ein automatisches Mail generiert welches die entsprechende Datei enthält oder es wird einfach das zuvor erstellte Mail verschickt.

Nachdem die E-Mails versendet wurden, richtet SET einen Listener ein und wartet darauf, dass die entsprechende Datei vom Ziel geöffnet wird. Wird die „manipulierte“ Datei geöffnet, so erhält der „Angreifer“ Zugriff auf den Computer des Opfers. Das Opfer merkt meist gar nichts, da es auf dem Bildschirm nicht zu erkennen ist, dass etwas Schlimmes passiert ist. (vgl. [6], Seite 354)

Web Attack Vector

Mit SET kann ein weiterer Angriff gestartet werden, es können nämlich Webseiten geklont und lokal gehostet werden. Nun braucht der Angreifer das Opfer nur noch überreden auf die von ihm genannte Webseite zu kommen und schon können verschiedene Teile eines Angriffs gestartet werden, wie zum Beispiel Informationssammlung, Abgreifen von Zugangsdaten, usw.

Für diese verschiedenen Arten gibt es in SET wieder verschiedene Optionen aus denen man wählen kann. (vgl. [6], Seite 354)

Andere Features von SET

SET wurde von Social Engineers für Auditor entwickelt, es basiert daher auf den im Auditing-Business üblichen Angriffen. Mit SET hat jeder Social Engineer ein leistungsfähiges Tool in der Hand, um bei Audits auf Schwächen aufmerksam machen zu können. Das Tool wird ständig weiterentwickelt und es erhält so ständig neue Features. (vgl. [6], Seite 356)

Cree.py

Cree.py ist eine Anwendung mit der die Ortsangaben der sozialen Netzwerke auf einer Karte dargestellt werden können. Derzeitige unterstützte soziale Netzwerke sind Twitter und Flickr. Eine weitere Funktion ist die Personensuche über Twitter und Flickr. Wie man in Abbildung 30 sehen kann wurde nach Christina Stürmer gesucht und auch fündig. Sofort bekommt man den dazugehörigen Twitter Account Name und ein Foto.

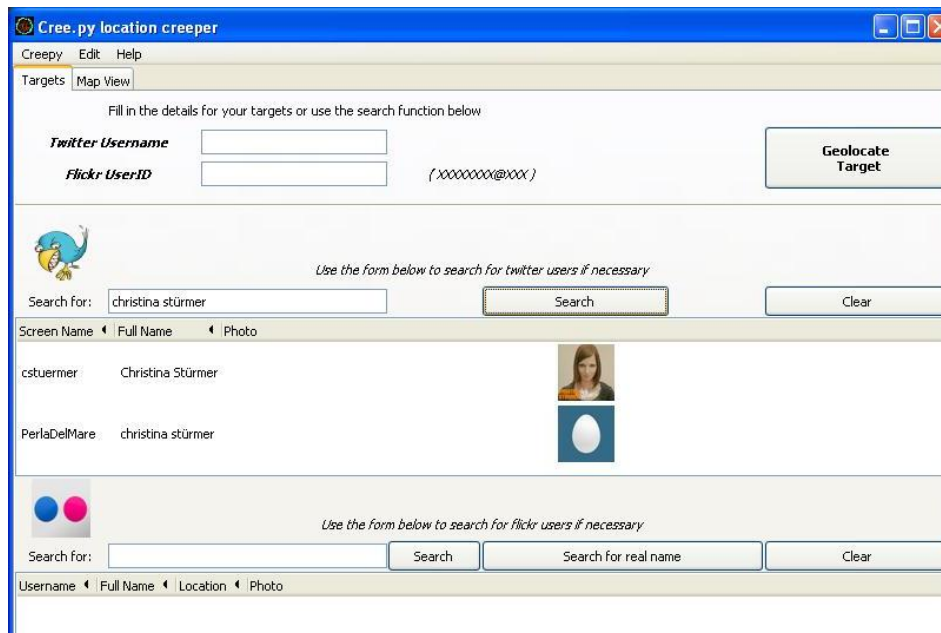


Abbildung 27: Cree.py Personensuche

Dieses Tool kann kostenlos unter <http://ilektrojohn.github.com/creepy/> heruntergeladen werden.

Facebook-Hacker-Tool

Die Sicherheits-Experten von BitDefender haben ein Tool gefunden, mit dem fast jeder ein Facebook-Konto knacken könnte. Dieses Tool (Facebook Hacker) ist einfach zu konfigurieren, denn man muss nur zwei Felder ausfüllen, eine E-Mail Adresse und ein Passwort an welche die gestohlenen Daten geschickt werden sollen.

Nach dem Klicken des build-Knopfes erstellt die Software eine Datei mit dem Namen „server.exe“ die danach per Mail an die Opfer verschickt wird. Fällt der Empfänger auf dieses Mail herein, so wird die Datei ausgeführt und das Tool klaut Facebook-Daten und das dazugehörige Passwort. Weiters kann das Tool gespeicherte Daten vom Browser und Instant Messenger abgreifen.

Außerdem kann dieses Tool auch gespeicherte Einwahl- und VPN-Daten wie Nutzernamen, Passwort und Domain sammeln. Damit dieses Tool möglichst unerkannt bleibt, versucht es alle Sicherheits-Tools auf dem infizierten Rechner zu erkennen und diese lahm zu legen.

Mittlerweile wird dieses Tool aber schon von BitDefender als Schadcode erkannt und die Nutzer werden dementsprechend gewarnt. (vgl. [36])



Abbildung 28: Facebook-Hacker Tool [36]

twitalyzer

Twitalyzer wurde von Eric T. Peterson, Web-Analyse-Guru entwickelt und wird von ihnen als “Serious Analytics for Social Media Experts” – Tool bezeichnet. Wie der Name schon sagt, konzentriert sich dieses Tool darauf Twitter-Statistiken auszuwerten.

Es werden sinnvolle Kennzahlen erhoben und diese danach in strukturierte und grafisch aufbereiteten Reports dargestellt. (vgl. [37])

Unter anderem werden diese Kennzahlen erhoben: (vgl. [37])

- Clout: Wie hoch ist die Wahrscheinlichkeit, dass der eigene Nutzernamen in einer Twitter-Suche auftaucht?
- Engagement: Wie oft verweisen andere auf die eigene Tweets?
- Impact: Was lösen die eigenen Tweets im Twitter-Universum aus. Reagiert jemand oder verhallt alles ungehört?
- Velocity: Die relative Postingfrequenz. Bleibt man am Ball oder macht man gerade schlapp beim Twittern?

Abbildung 29 zeigt wie sich Twitalyzer präsentiert:

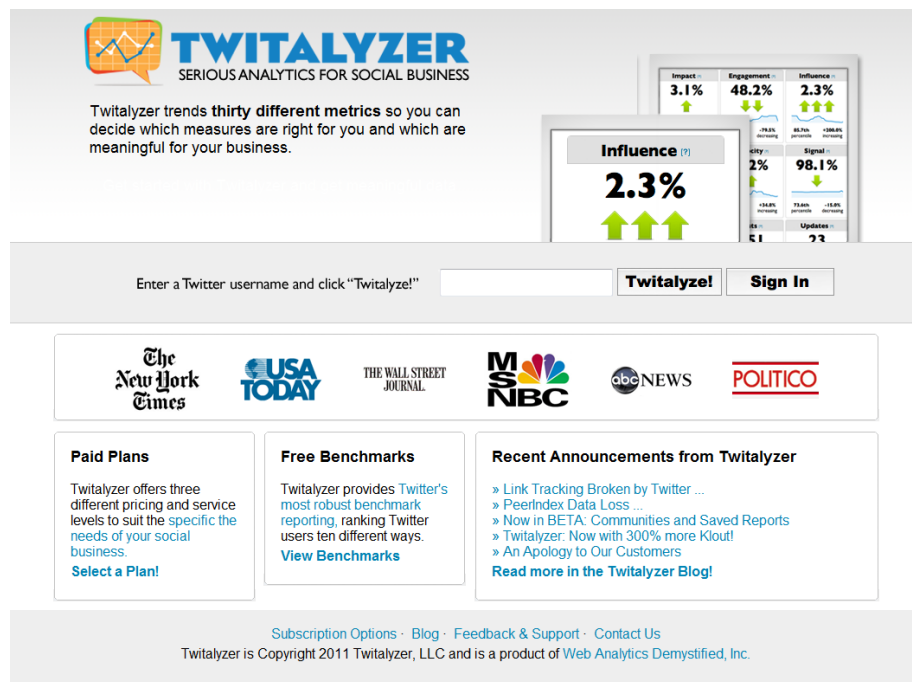


Abbildung 29: twitalyzer - Startseite

Diese Spezialisierung von Twitalyzer zahlte sich wirklich aus, denn diese Kennzahlen bekommt man nur über dieses Tool. (vgl. [37])

Abbildung 30 zeigt die Analyse des Christina Stürmer Twitter Accounts.

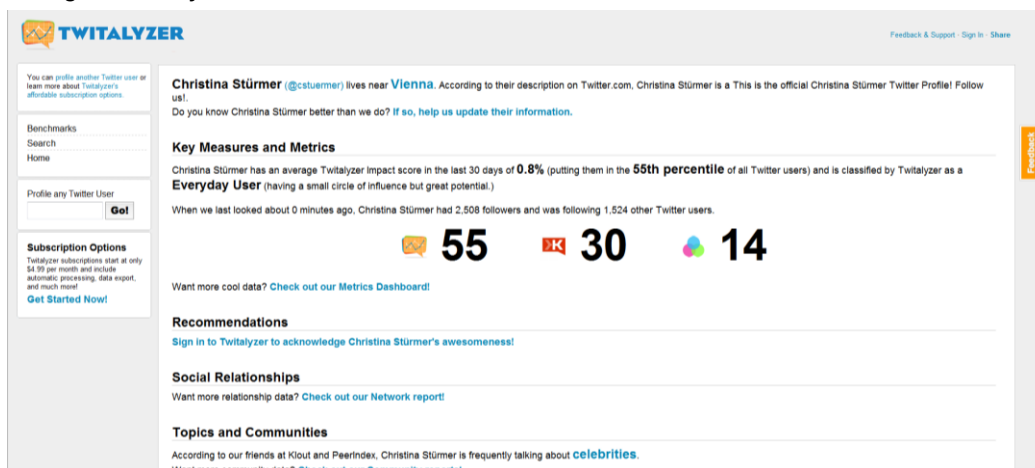


Abbildung 30: twitalyzer – Christina Stürmer Analyseergebniss

TwitterAnalyzer

TwitterAnalyzer ist eines der umfassendsten Twitter Analyse Tools die es zurzeit gibt. Mittels diesen Analyzer können die Tweets, Chats, Popularity, Reach, Subjects, Hash Tags, Links, Apps, Followers, Follower Map, Activity, Friends, Mentions, usw. analysiert werden. (vgl. [38])

Leider stand dieses Tool gerade nicht zur Verfügung als ich es ausprobieren wollte.



Abbildung 31: TwitterAnalyzer [38]

TweetPsych

Mit dem kostenlosen „TweetPsych“ Online Tool (<http://tweetpsych.com/>), können die Twitter User analysiert werden. Dieses Tool analysiert die letzten 1000 Tweets und analysiert anhand zwei verschiedener Algorithmen das Verhalten beziehungsweise die Themen des angegebenen Users.

Anhand der Daten und den Vergleichswerten zu den anderen Twitter Usern, erstellt diese Applikation ein Diagramm mit der Auswertung ob man Themen wie Zeit, Zukunft oder Erotik im Vergleich besonders oft oder selten ansieht oder twittert. (vgl. [39])

Folgende Abbildungen wurden selbst erstellt um zu zeigen wie dieses Tool funktioniert. Als Testperson wurde „Justin Bieber“ gewählt, da diese Person in der Öffentlichkeit steht und somit die Daten nicht vertraulich sind.



Abbildung 32: TweetPsych - Startseite

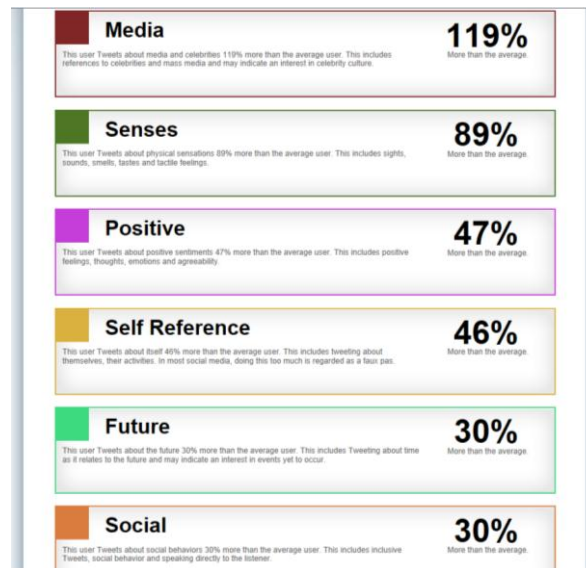


Abbildung 33: TweetPsych – Ergebnis 1 (Beispiel)

Facebook Search

Mittels „facebook search“ kann man Posts, Fotos, Personen, Seiten, Gruppen und Events suchen. Diese Suche basiert auch auf den Privatsphären Einstellungen von Facebook. Abbildung 34 zeigt die Startseite von „facebook search“.



Abbildung 34: facebook search

Abbildung 35 zeigt das Suchergebnis wenn über „facebook search“ nach Christina Stürmer gesucht wird. Es wird das Facebook Profil Foto und der Link zum Profil angezeigt. Mit einem Klick darauf kommt man direkt zum Profil.



Abbildung 35: facebook search – Christina Stürmer

pipl.com

Mittels “pipl” können Personen gesucht werden, die in sozialen Netzwerken aktiv sind. Abbildung 36 zeigt, dass für die gesuchte Person das LinkedIn Profil, FacebookProfil und ein Newsgroup Eintrag gefunden wurde. Mit einem Klick auf das gewünschte Ergebnis wird man sofort zum Profil auf Facebook oder LinkedIn geleitet.

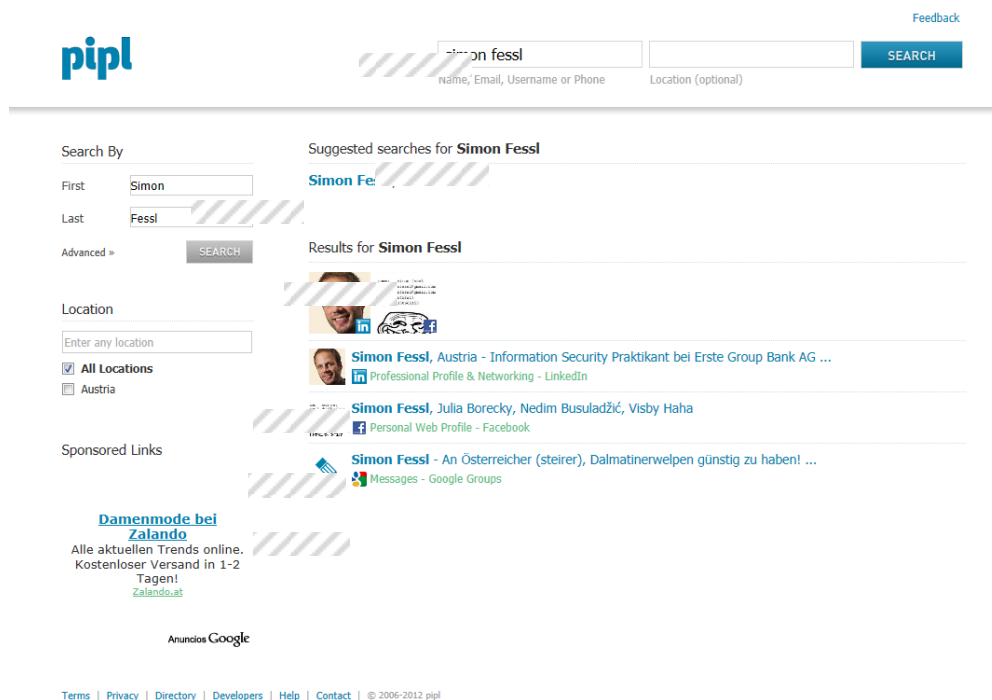


Abbildung 36: pipl - Personensuche

Facebook – Applikationen

Applikationen die direkt in Facebook installiert werden, liegen genauso im Trend wie Facebook an sich. Dabei handelt es sich meistens um Spiele die danach gemeinsam mit den Freunden gespielt werden können. Eines der berühmtesten Spiele derzeit ist „FarmVille“, wird von der amerikanischen Internet-Firma „Zynga“ hergestellt.

Wie einige Datenschützer berichten, erlaubt man, mit den Laden des Spieles in das Facebook Profil, den Zugriff auf die eigenen Profilinformationen, Fotos und Informationen über Freunde. Weiters werden auch hier Cookies eingesetzt um ein Profil von den Usern zu erstellen und somit kann gezielte Werbung eingesetzt werden. Eine weite Gefahr stellt, das Angeben von Kreditkartendaten oder Paypal-daten, denn mittels „echten Geld“ kommt man schneller zu Maschinen oder Häuser. Allerdings ist es schon vorgekommen, dass „Zynga“ gleich dreimal Geld vom Papal-Konto abgebucht hat, ohne Zustimmung des Users.

Welche Daten weitergeben werden hängt vom Betreiber der sozialen Netzwerke ab, bei Facebook werden standardmäßig alle öffentlich zugänglichen Informationen übertragen. Weiters ist es bei Facebook auch so, dass man unter anderem zulassen muss, dass E-Mail Adresse, Geburtsdatum, Freundesliste und Wohnort weitergeleitet werden. (vgl. [40], [41])

„FarmVille“ ist mit Sicherheit nicht die einzige Applikation die so arbeitet, denn man kann vermuten, dass alle kostenlosen Spiele oder Applikationen dieses Geschäftsmodell verfolgen. Aufgrund der Vielfalt der Applikationen wurde ein Beispiel (FarmVille) herausgenommen um zu zeigen, wie diese Applikationen arbeiten. Allerdings wird hier auch keine generelle Aussage getroffen, dass dies alle Applikationen tun.

4. Angriffsszenarien

In diesem Kapitel werden die Angriffsszenarien vorgestellt, die mittels Social Engineering sehr erfolgreich sein können. Weiters sind diese Angriffsszenarien meiner Meinung nach diese, die auch über soziale Netzwerke durchgeführt werden können bzw. für die, die Information aus sozialen Netzwerken sehr hilfreich sein können.

4.1. Identitätsdiebstahl

Identitätsdiebstahl ist eine große Bedrohung, denn herausgefundene Daten können weitergegeben werden und somit haben es böswillige Hacker leichter. Das Tool „FBPwn“, welches in Kapitel beschrieben ist, benutzt diese Methode, denn es klonst das Profil von Facebook-Kontakten und somit steigt die Erfolgsrate bei den Freundschaftsanfragen um vieles. (vgl. [35])

Wie man anhand der Statistik (Abbildung 37) sieht, ist der Identitätsdiebstahl von sozialen Netzwerken sehr erfolgreich. Immerhin sind soziale Netzwerke schon auf Platz 3 hinter Webmailkonten und Handelsplattformen.

Am häufigsten von Identitäts- und Passwortdiebstahl betroffene Plattformen in Deutschland 2010

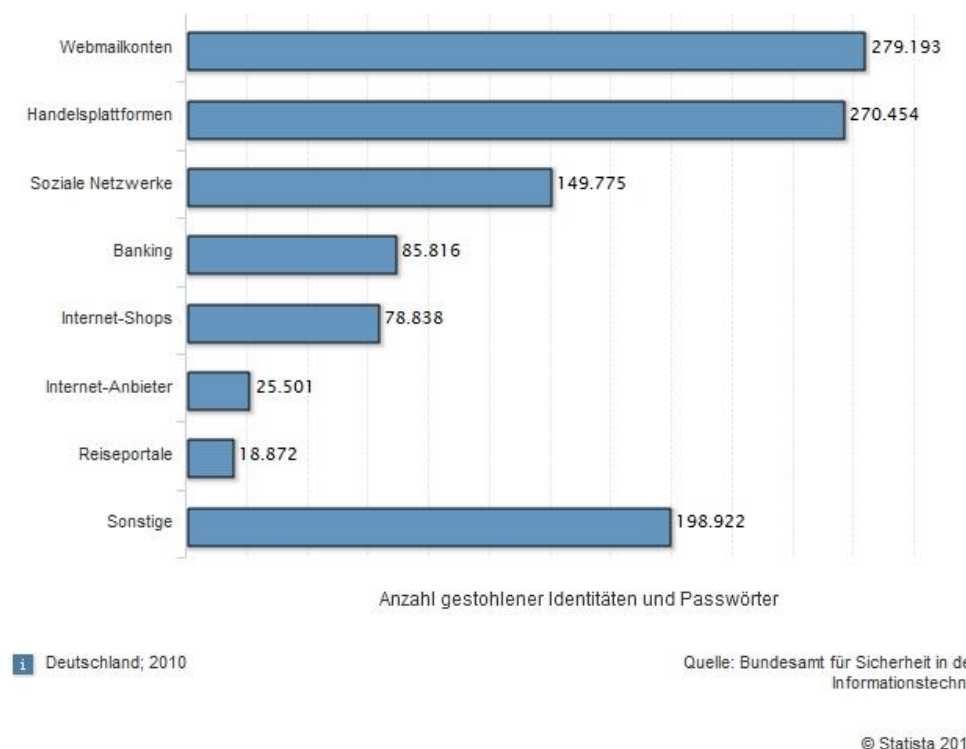


Abbildung 37: Anzahl der gestohlenen Identitäten und Passwörter in 2010 [2] basierend auf [42]

In den meisten Fällen wird versucht, bestehende Nutzerkonten zu hacken, um diese gestohlene Identität für Betrügereien zu nutzen. Im Namen diesen gestohlenen Accounts, können viele Sachen gemacht werden, da „Online-Freunden“ sehr stark vertraut wird, ist diese Form des Betruges sehr erfolgreich. Meist werden Nachrichten verschickt in denen eine Notsituation vorgetäuscht wird und aufgrund dessen um finanzielle Hilfe

gebeten wird. Die zusätzlichen persönlichen Informationen, die die „Hacker“ durch das Nutzerprofil haben, können sehr hilfreich sein, um die „Freunde“ zu täuschen.

Eine weitere Form des Identitätsdiebstahls ist „unechte“ Profile zu erstellen und dadurch Personen zu schaden. Denn Diebe können dadurch zum Beispiel ausspionieren, wann jemand auf Urlaub ist und die Wohnung leer steht (vgl. [43])

Zum Identitätsdiebstahl zählen auch die Nutzung fremder Adressdaten (Spaßbestellungen), Kreditkartenmissbrauch, Nutzung fremder E-Mail-Accounts und die Nutzung fremder Transaktionsidentitäten. (vgl. [44], Seite 27 und 28)

4.2. Cyber Mobbing bzw. Stalking

Cyber Mobbing bzw. Stalking verbreitet sich immer mehr, da die Hemmschwelle des persönlichen Gegenübertretens durch das Internet fällt. Hier ist es viel leichter beleidigende Dinge zu schreiben, als sie einer Person persönlich ins Gesicht zu sagen. Im folgenden Kapitel werden die verschiedenen Formen und Nutzungsarten vorgestellt. All diese Arten können auch über soziale Netzwerke betrieben werden.

4.2.1. Was ist Cyber Mobbing?

Cyber Mobbing wird auch Cyber-Stalking oder Cyber-Bulling genannt und man versteht darunter das absichtliche Beleidigen, Bedrohen, Bloßstellen oder Belästigen von Personen im Internet. Diese Belästigung erfolgt in der Regel über einen längeren Zeitraum hinweg. Im Internet werden vor allem Fotos- und Videoplattformen und Soziale Netzwerke für die Angriffe benutzt. (vgl. [45], Seite 6)

„In sozialen Netzwerken ist Cyber Mobbing besonders schmerzvoll, weil hier die NutzerInnen mit allen Bekannten und FreundInnen in ständigen Kontakt stehen und sich einmal veröffentlichte Gerüchte oder Beschimpfungen sehr schnell verbreiten.“ ([45], Seite 6)

Die TäterInnen werden oft auch als „Cyber-Bullys“ bezeichnet.

Cyber Mobbing findet häufig unter Jugendlichen statt, in seltenen Fällen werden auch Erwachsene gemobbt. Doch gerade unter Kinder und Jugendlichen kennen Opfer und Täter einander meist auch in der „realen“ Welt. (vgl. [45], Seite 6)

„Cyber- Mobbing geht in der Regel von Personen aus dem eigenen Umfeld aus – der Schule, dem Wohnviertel, dem Dorf oder der ethnischen Community. Fälle, in die gänzlich Fremde involviert sind, sind wenig verbreitet.“ ([45], Seite 6)

4.2.1.1. Unterschied - Cyber Mobbing und Cyber Stalking

Cyber Stalking ist eine Form von Stalking, bei dieser Form kommen das Internet und andere Kommunikationstechnologien zum Einsatz.

Das Internet wird auch für andere Belästigungsformen wie z.B. Cyber Mobbing oder Bullying genutzt, diese Formen erfüllen aber nicht den Tatbestand der beharrlichen Verfolgung. Trotzdem können diese Belästigungen zu einem Leidensdruck führen. (vgl. [46])

Von Stalkern spricht man, wenn folgende Vorgehensweisen einer Täterin/eines Täters das Opfer unzumutbar beeinträchtigen und das Verhalten über längere Zeit hindurch fortgesetzt wird:

„Die Stalkerin/der Stalker:

- *Sucht die räumliche Nähe des Opfers*
- *Stellt mithilfe von Telekommunikation oder durch sonstige Kommunikationsmittel oder durch Dritte den Kontakt zum Opfer her*
- *Bestellt unter Verwendung der persönlichen Daten des Opfers Waren oder Dienstleistungen in dessen Namen*
- *Bewegt unter Verwendung der persönlichen Daten des Opfers Dritte dazu, mit dem Opfer Kontakt aufzunehmen“ [46]*

4.2.2. Was ist neu an Cyber Mobbing?

Mobbing an sich gibt es schon immer, aber die Nutzung von Internet und Handy, um andere zu beleidigen, hat jedoch neue Konsequenzen:

■ **Cyber-Mobbing kann rund um die Uhr stattfinden**

Durch die neuen Medien, wie Soziale Netzwerke und Co., endet Cyber Mobbing nicht in der Schule oder der Arbeit, sondern geht rund um die Uhr weiter, da die Täter (Cyber – Bullys) über das Internet oder Handy, das Opfer rund um die Uhr angreifen können. Das heißt nicht einmal die eigenen vier Wände können einem vor den Angriffen schützen. (vgl. [47], Seite 4)

■ **Cyber – Mobbing erreicht ein großes Publikum**

„Soziale Netzwerke, E-Mail und Handy ermöglichen die schnelle Verbreitung von Inhalten an eine breite Öffentlichkeit. Mit nur einem einzigen Klick kann z. B. ein peinliches Foto an eine große Anzahl an Empfänger/innen geschickt werden. Sind solche Bilder einmal im Web veröffentlicht, können sie praktisch kaum mehr entfernt werden. Das Internet hat ein langes Gedächtnis: Auch wenn Inhalte von einer Website gelöscht werden, sind sie möglicherweise schon vielfach kopiert, weiterverschickt oder in Internet-Archiven abgespeichert.“ ([45], Seite 8)

■ **„Cyber-Bullys“ können anonym agieren**

Der „Cyber-Täter“ kann anonym agieren und so dem Opfer Angst machen, da das Opfer verunsichert ist und nicht weiß, wer es belästigt. Dies verleiht dem Täter oft eine zähe Ausdauer.(vgl. [47], Seite 4)
„Was die InternetnutzerInnen jedoch oft vergessen. Jede Aktion im Web (z.B. Chatten, eine E-Mail schreiben, eine Website besuchen) hinterlässt Spuren und über die sogenannte „IP-Adresse“ kann der benutzte Computer eindeutig identifiziert werden.“ ([45], Seite 8)

■ **Keine klare Abgrenzung von Rollen**

Die Rollen der Täter und der Opfer sind nicht immer eindeutig zu trennen, denn aus einer Attacke kann eine Gegenattacke stattfinden und so kann der Täter auf einmal zum Opfer werden. Weiter ist es so, dass Persönlichkeitsmerkmale, die oft auf klassische Mobbingopfer zutreffen, nicht relevant sind,

denn auch gut integrierte Menschen können auf einmal zum Cyber-Mobbing Opfer werden. (vgl. [45], Seite 8)

■ **Cyber – Mobbing kann auch unbeabsichtigt sein**

Da die Reaktionen der Opfer für den Täter nicht sichtbar sind, kann es passieren, dass jemand ohne böse Absicht verletzt wird, da dem Täter das Ausmaß verletzender Worte oder Bilder nicht klar ist. Oft wird einfach nicht darüber nachgedacht, was z.B. ein übler Scherz oder Witz für einen anderen bedeutet. (vgl. [47], Seite 8)

4.2.3. Formen von Cyber-Mobbing

Folgende Beispiele zeigen, wie man das Internet und Handy für Cyber-Mobbing Attacken missbrauchen kann.

■ **Beschimpfungen und Beleidigungen**

Über die Kommentarfunktion bei Fotos oder Videos oder über die Profil-Pinnwand in sozialen Netzwerken können gemeine Nachrichten hinterlassen werden, die für alle sichtbar sind. Weiters können boshafte Kommentare über Instant Messenger an die Empfänger geschickt werden. Via SMS haben es Täter leicht, denn hier kann man die Beschimpfungen mit unterdrückter Nummer senden. (vgl. [45], Seite 10)

■ **Drohungen und Erpressungen**

Mittels Handy können die Opfer mit unterdrückter Nummer angerufen werden und anschließend mit verstellter Stimme erpresst werden. Mit gestohlenen Passwörtern können die Profile und auch das Passwort geändert werden. (vgl. [45], Seite 10)

■ **Sexuelle Belästigungen und unangenehme Anmachen**

Diese Form tritt häufig bei Mädchen auf, die sehr „anregende“ bzw. „freizügige“ Bilder von sich im Internet veröffentlichen. Burschen versuchen dann meistens sich mit Pseudonymen an die Mädchen heranzumachen. Aber auch von Fremden können Mädchen sexuell belästigt werden. (vgl. [45], Seite 10)

■ **Veröffentlichung gefälschter, intimer oder peinlicher Fotos**

Peinliche Fotos oder Videos können mit Bildbearbeitungsprogrammen leicht verändert bzw. verunstaltet werden und anschließend veröffentlicht werden. Durch die Sozialen Medien (Soziale Netzwerke, Instant Messenger, usw.) werden Fotos sehr schnell und leicht weitergeschickt. Denn mit dem Handy werden schnell Fotos gemacht und anschließend gleich an alle Freunde weitergeschickt. (vgl. [45], Seite 11)

■ **Verbreitung von persönlichen Informationen oder Gerüchten**

„Für die Verbreitung von Gerüchten werden vor allem die Nachrichtenfunktionen in sozialen Netzwerken, Instant Messenger oder E-Mail verwendet. Um die Gerüchte besonders effektiv zu verbreiten, werden zuerst Personen informiert, die als besondere „Tratschen“ bekannt sind.“
([45], Seite 11)

■ **Ausschluss von Freundeslisten**

Für viele Personen ist die Anzahl der Freunde sehr wichtig, es wird als sozialer Status gehandhabt. Wird allerdings eine Person gemobbt, ziehen viele „Freunde“ ihre Verlinkung zurück und es sinkt das soziale Ansehen. (vgl. [45], Seite 11)

4.2.4. Wie werden die neuen Medien zum Mobben genutzt?

Folgende Tabelle 2 veranschaulicht, wie die neue Medien sinnvoll genutzt werden können, aber auch wie sie missbräuchlich verwendet werden können.

Technologie	Positive Nutzungsmöglichkeiten	Möglicher Missbrauch
Handys	- Kommunikation durch Text und Bild - Bilder und Filme aufnehmen und verschicken - Musik hören - spielen - ins Internet gehen - E-Mails schreiben - sehr nützlich im Notfall und um Kindern mehr Unabhängigkeit zu bieten	- wiederholt anonyme Anrufe tätigen und gemeine Nachrichten verschicken (einschließlich Drohungen, Einschüchterungen, Beleidigungen) - demütigende Bilder oder Videos aufnehmen, herumschicken oder im Internet veröffentlichen (z.B. Happy Slapping)
Instant Messenger	- mit Freunden chatten - schnelle und effektive Möglichkeit, in Kontakt zu bleiben	- gemeine Nachrichten, Bilder oder Videos verschicken - einen anderen Account benutzen, um fiese Nachrichten an die Kontaktliste zu verschicken
Chatrooms	eine gute Möglichkeit für Bekanntschaften	- gemeine und drohende anonyme Nachrichten verschicken - Freundschaften unter falschen Vorwand schließen
E-Mail	elektronische Briefe, Bilder, Dateien schnell und günstig in der ganzen Welt verschicken	- gemeine oder bedrohliche Nachrichten verschicken - unpassende Inhalte verschicken - auf einen anderen Account zugreifen, z.B. um persönliche E-Mails weiterzuleiten oder zu löschen
Webcams	- Bilder oder Videobotschaften von sich aufnehmen - andere über den Bildschirm sehen - Videokonferenzen	- unangenehme Inhalte aufnehmen und verschicken - junge Leute zu unangemessenem Handeln überreden oder zwingen - private Aufnahmen nach Trennungen online stellen
Soziale Netzwerke	- mit Freunden in Kontakt treten und innerhalb von Online-Communities neu Freunde finden und treffen - jungen Leuten die Möglichkeit geben, im Internet kreativ zu sein - persönliche Profile und Homepages können erstellt werden	- gemeine Kommentare zu Bildern oder auf die Pinnwand schreiben - fiese Bilder oder Videos veröffentlichen - auf einen anderen Account zugreifen und damit Unsinn anstellen - absichtlich gegründete Hassgruppen, die sich gegen eine Person richten „Fake-Profile“ erstellen und vorgeben, eine bestimmte Person zu sein
Video Portale	interessante, unterhaltende und künstlerische Videos abrufen oder eigene Hochladen	- beschämende, demütigende Videos über eine Person veröffentlichen - private Aufnahmen nach Trennungen online stellen

Tabelle 2: Neue Technologien im Überblick (vgl. [47], Seite 6-7)

4.2.5. Relevante Gesetzespassagen für Cyber-Mobbing

Dieses Kapitel zeigt, die relevanten Paragraphen der einzelnen Gesetze, die bei Cyber-Mobbing zu trage kommen können. Werden diese verletzt, so kann der Täter verklagt gezogen werden.

Nötigung (§ 105 StGB)

„§ 105. (1) Wer einen anderen mit Gewalt oder durch gefährliche Drohung zu einer Handlung, Duldung oder Unterlassung nötigt, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

(2) Die Tat ist nicht rechtswidrig, wenn die Anwendung der Gewalt oder Drohung als Mittel zu dem angestrebten Zweck nicht den guten Sitten widerstreitet.“ [29]

Es ist verboten, jemand anderen mit Gewalt oder durch Drohung zu einer Handlung zu nötigen.

z.B.: Person A droht Person B, Aktfotos zu veröffentlichen, wenn nicht noch weitere Fotos geschickt werden. (vgl. [45], Seite 29)

Beharrliche Verfolgung (§ 107a StGB), „Anti-Stalking-Gesetz“

„§ 107a. (1) Wer eine Person widerrechtlich beharrlich verfolgt (Abs. 2), ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

(2) Beharrlich verfolgt eine Person, wer in einer Weise, die geeignet ist, sie in ihrer Lebensführung unzumutbar zu beeinträchtigen, eine längere Zeit hindurch fortgesetzt

1. ihre räumliche Nähe aufsucht,
2. im Wege einer Telekommunikation oder unter Verwendung eines sonstigen Kommunikationsmittels oder über Dritte Kontakt zu ihr herstellt,
3. unter Verwendung ihrer personenbezogenen Daten Waren oder Dienstleistungen für sie bestellt oder
4. unter Verwendung ihrer personenbezogenen Daten Dritte veranlasst, mit ihr Kontakt aufzunehmen.

(3) (Anm.: aufgehoben durch BGBl. I Nr. 93/2007)“ [29]

Es ist verboten, eine Person über einen längeren Zeitraum hinweg beharrlich zu Verfolgen.

z.B.: durch vermehrtes Anrufen oder SMS schicken

Beispiel: Person A schickt Person B jeden Tag 50 SMS, obwohl Person B das nicht will oder Person A bestellt immer im Namen von Person B Waren im Internet. (vgl. [45], Seite 29)

Üble Nachrede (§ 111 StGB)

„§ 111. (1) Wer einen anderen in einer für einen Dritten wahrnehmbaren Weise einer verächtlichen Eigenschaft oder Gesinnung zeiht oder eines unehrenhaften Verhaltens oder eines gegen die guten Sitten verstoßenden Verhaltens beschuldigt, das geeignet ist, ihn in der öffentlichen Meinung verächtlich zu machen oder herabzusetzen, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Wer die Tat in einem Druckwerk, im Rundfunk oder sonst auf eine Weise begeht, wodurch die üble Nachrede einer breiten Öffentlichkeit zugänglich wird, ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(3) Der Täter ist nicht zu bestrafen, wenn die Behauptung als wahr erwiesen wird. Im Fall des Abs. 1 ist der Täter auch dann nicht zu bestrafen, wenn Umstände erwiesen werden, aus denen sich für den Täter hinreichende Gründe ergeben haben, die Behauptung für wahr zu halten.“ [29]

Es ist verboten, „in Gegenwart einer dritten Person jemand den Vorwurf zu einer verächtlichen Gesinnung oder Eigenschaft zu machen oder ihn einer ehrenhaften Verhaltens zu beschuldigen.

Beispiel: Person A beschuldigt Person B in einem öffentlichen Forum des Betruges, da sie angeblich bei Prüfungen geschummelt habe.“ [45], Seite 29)

Beleidigung (§ 115 StGB)

„§ 115. (1) Wer öffentlich oder vor mehreren Leuten einen anderen beschimpft, verspottet, am Körper mißhandelt oder mit einer körperlichen Mißhandlung bedroht, ist, wenn er deswegen nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, mit Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen zu bestrafen.

(2) Eine Handlung wird vor mehreren Leuten begangen, wenn sie in Gegenwart von mehr als zwei vom Täter und vom Angegriffenen verschiedenen Personen begangen wird und diese sie wahrnehmen können.

(3) Wer sich nur durch Entrüstung über das Verhalten eines anderen dazu hinreißen läßt, ihn in einer den Umständen nach entschuldbaren Weise zu beschimpfen, zu mißhandeln oder mit Mißhandlungen zu bedrohen, ist entschuldigt, wenn seine Entrüstung, insbesondere auch im Hinblick auf die seit ihrem Anlaß verstrichene Zeit, allgemein begreiflich ist.“ [29]

Es ist verboten eine Person in der Öffentlichkeit eine Person zu beschimpfen oder zu beleidigen.

z.B.: Person A postet ein öffentliches Kommentar auf dem Online Profil von Person B, in dem sie als „hässlich“ bezeichnet wird. (vgl. [45], Seite 29)

Datenbeschädigung (§ 126a StGB)

„§ 126a. (1) Wer einen anderen dadurch schädigt, daß er automationsunterstützt verarbeitete, übermittelte oder überlassene Daten, über die er nicht oder nicht allein verfügen darf, verändert, löscht oder sonst unbrauchbar macht oder unterdrückt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Wer durch die Tat an den Daten einen 3 000 Euro übersteigenden Schaden herbeiführt, ist mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bis zu 360 Tagessätzen, wer einen 50 000 Euro übersteigenden Schaden herbeiführt oder die Tat als Mitglied einer kriminellen Vereinigung begeht, mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.“ [29]

Es ist verboten, Daten anderer Personen zu verändern, zu löschen oder sonst unbrauchbar zu machen.

z.B.: Person A löscht absichtlich die Daten von Person B.

Kreditbeschädigung (§ 152 StGB)

„§ 152. (1) Wer unrichtige Tatsachen behauptet und dadurch den Kredit, den Erwerb oder das berufliche Fortkommen eines anderen schädigt oder gefährdet, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen. Die Freiheits- und die Geldstrafe können auch nebeneinander verhängt werden.

(2) Der Täter ist nur auf Verlangen des Verletzten zu verfolgen.“ [29]

Es ist verboten, unrichtige Tatsachen zu behaupten, wenn dadurch das Fortkommen der Person gefährdet ist.
Beispiel: Person A behauptet unrichtige Tatsachen über eine Person in einem öffentlichen Forum, damit diese Person von der Schule verwiesen wird. (vgl. [45], Seite 29)

Pornografische Darstellungen Minderjähriger (§ 207a StGB)

„§ 207a. (1) Wer eine pornographische Darstellung einer minderjährigen Person (Abs. 4)

1. herstellt oder

2. einem anderen anbietet, verschafft, überlässt, vorführt oder sonst zugänglich macht, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

(2) Mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren ist zu bestrafen, wer eine pornographische Darstellung einer minderjährigen Person (Abs. 4) zum Zweck der Verbreitung herstellt, einführt, befördert oder ausführt oder eine Tat nach Abs. 1 gewerbsmäßig begeht. Mit Freiheitsstrafe von einem bis zu zehn Jahren ist zu bestrafen, wer die Tat als Mitglied einer kriminellen Vereinigung oder so begeht, dass sie einen besonders schweren Nachteil der minderjährigen Person zur Folge hat; ebenso ist zu bestrafen, wer eine pornographische Darstellung einer minderjährigen Person (Abs. 4) unter Anwendung schwerer Gewalt herstellt oder bei der Herstellung das Leben der dargestellten minderjährigen Person vorsätzlich oder grob fahrlässig gefährdet.

(3) Wer sich eine pornographische Darstellung einer mündigen minderjährigen Person (Abs. 4 Z 3 und 4) verschafft oder eine solche besitzt, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen. Mit Freiheitsstrafe bis zu zwei Jahren ist zu bestrafen, wer sich eine pornographische Darstellung einer unmündigen Person (Abs. 4) verschafft oder eine solche besitzt.

(3a) Nach Abs. 3 wird auch bestraft, wer im Internet wissentlich auf eine pornographische Darstellung Minderjähriger zugreift.

(4) Pornographische Darstellungen Minderjähriger sind

1. wirklichkeitsnahe Abbildungen einer geschlechtlichen Handlung an einer unmündigen Person oder einer unmündigen Person an sich selbst, an einer anderen Person oder mit einem Tier,

2. wirklichkeitsnahe Abbildungen eines Geschehens mit einer unmündigen Person, dessen Betrachtung nach den Umständen den Eindruck vermittelt, dass es sich dabei um eine geschlechtliche Handlung an der unmündigen Person oder der unmündigen Person an sich selbst, an einer anderen Person oder mit einem Tier handelt,

3. wirklichkeitsnahe Abbildungen

a) einer geschlechtlichen Handlung im Sinne der Z 1 oder eines Geschehens im Sinne der Z 2, jedoch mit mündigen Minderjährigen, oder

b) der Genitalien oder der Schamgegend Minderjähriger, soweit es sich um reißerisch verzerrte, auf sich selbst reduzierte und von anderen Lebensäußerungen losgelöste Abbildungen handelt, die der sexuellen Erregung des Betrachters dienen;

4. bildliche Darstellungen, deren Betrachtung - zufolge Veränderung einer Abbildung oder ohne Verwendung einer solchen - nach den Umständen den Eindruck vermittelt, es handle sich um eine Abbildung nach den Z 1 bis 3.

(5) Nach Abs. 1 Z 1 und Abs. 3 ist nicht zu bestrafen, wer

1. eine pornographische Darstellung einer mündigen minderjährigen Person mit deren Einwilligung und zu deren eigenem Gebrauch herstellt oder besitzt oder

2. eine pornographische Darstellung einer mündigen minderjährigen Person nach Abs. 4 Z 4 zu seinem eigenen Gebrauch herstellt oder besitzt, sofern mit der Tat keine Gefahr der Verbreitung der Darstellung verbunden ist.“ [29]

Es ist die Herstellung, Veröffentlichung oder Verbreitung von Bildern mit sexuellem Fokus von unter 18-jährigen verboten.

Beispiel: Person A (13 Jahre) veröffentlicht von sich selbst sehr intime Fotos in ihrem Online-Profil. (vgl. [45], Seite 30)

Verleumdung (§ 297 StGB)

„§ 297. (1) Wer einen anderen dadurch der Gefahr einer behördlichen Verfolgung aussetzt, daß er ihn einer von Amts wegen zu verfolgenden mit Strafe bedrohten Handlung oder der Verletzung einer Amts- oder Standespflicht falsch verdächtigt, ist, wenn er weiß (§ 5 Abs. 3), daß die Verdächtigung falsch ist, mit Freiheitsstrafe bis zu einem Jahr, wenn die fälschlich angelastete Handlung aber mit einer ein Jahr übersteigenden Freiheitsstrafe bedroht ist, mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.

(2) Nach Abs. 1 ist nicht zu bestrafen, wer freiwillig die Gefahr einer behördlichen Verfolgung beseitigt, bevor eine Behörde etwas zur Verfolgung des Verdächtigten unternommen hat.“ [29]

Es ist verboten, jemand anderen einer strafbaren Handlung zu verdächtigen, obwohl klar ist dass der Vorwurf nicht zutrifft und aufgrund der Verdächtigung Gefahr einer behördlichen Verfolgung besteht.

Beispiel: Person A beschuldigt Person B etwas gestohlen zu haben. (vgl. [45], Seite 30)

Briefschutz (§ 77 UrhG)

„§ 77. (1) Briefe, Tagebücher und ähnliche vertrauliche Aufzeichnungen dürfen weder öffentlich vorgelesen noch auf eine andere Art, wodurch sie der Öffentlichkeit zugänglich gemacht werden, verbreitet werden, wenn dadurch berechnigte Interessen des Verfassers oder, falls er gestorben ist, ohne die Veröffentlichung gestattet oder angeordnet zu haben, eines nahen Angehörigen verletzt würden.

(2) Nahe Angehörige im Sinn des Abs. 1 sind die Verwandten in auf- und absteigender Linie sowie der überlebende Ehegatte oder Lebensgefährte. Die mit dem Verfasser im ersten Grade Verwandten und der überlebende Ehegatte oder Lebensgefährte genießen diesen Schutz Zeit ihres Lebens, andere Angehörige nur, wenn seit dem Ablauf des Todesjahres des Verfassers zehn Jahre noch nicht verstrichen sind.

(3) Briefe dürfen auch dann nicht auf die im Absatz 1 bezeichnete Art verbreitet werden, wenn hiedurch berechnigte Interessen dessen, an den der Brief gerichtet ist, oder, falls er gestorben ist, ohne die Veröffentlichung gestattet oder angeordnet zu haben, eines nahen Angehörigen verletzt würden. Absatz 2 gilt entsprechend.

(4) Die Absätze 1 bis 3 gelten ohne Rücksicht darauf, ob die im Absatz 1 bezeichneten Schriften den urheberrechtlichen Schutz dieses Gesetzes genießen oder nicht. Die Anwendung urheberrechtlicher Bestimmungen auf solche Schriften bleibt unberührt.

(5) Die Absätze 1 bis 3 gelten nicht für Schriften, die, wenngleich nicht ausschließlich, zum amtlichen Gebrauch verfaßt worden sind.

(6) Die Vorschriften des § 41 gelten entsprechend.“ [29]

Die öffentliche Verbreitung von vertraulichen Aufzeichnungen, ist verboten.

Beispiel: Person A veröffentlicht von Person B eine private E-Mail im Internet. (vgl. [45], Seite 30)

Bildnisschutz (§ 78 UrhG)

„§ 78. (1) *Bildnisse von Personen dürfen weder öffentlich ausgestellt noch auf eine andere Art, wodurch sie der Öffentlichkeit zugänglich gemacht werden, verbreitet werden, wenn dadurch berechnigte Interessen des Abgebildeten oder, falls er gestorben ist, ohne die Veröffentlichung gestattet oder angeordnet zu haben, eines nahen Angehörigen verletzt würden.*

(2) *Die Vorschriften der §§ 41 und 77, Absatz 2 und 4, gelten entsprechend.“ [29]*

Es ist verboten, Fotos zu veröffentlichen die jemanden bloßstellen.

Beispiel: Person A veröffentlicht „Sauf-Fotos“ von Person B. (vgl. [45], Seite 30)

Mediengesetz

„§ 6. (1) *Wird in einem Medium der objektive Tatbestand der üblen Nachrede, der Beschimpfung, der Verspottung oder der Verleumdung hergestellt, so hat der Betroffene gegen den Medieninhaber Anspruch auf eine Entschädigung für die erlittene Kränkung. Die Höhe des Entschädigungsbetrages ist nach Maßgabe des Umfangs und der Auswirkungen der Veröffentlichung, insbesondere auch der Art und des Ausmaßes der Verbreitung des Mediums, zu bestimmen; auf die Wahrung der wirtschaftlichen Existenz des Medieninhabers ist Bedacht zu nehmen. Der Entschädigungsbetrag darf 20 000 Euro, bei einer Verleumdung oder bei besonders schwerwiegenden Auswirkungen einer üblen Nachrede 50 000 Euro nicht übersteigen.*

(2) *Der Anspruch nach Abs. 1 besteht nicht, wenn*

1. *es sich um einen wahrheitsgetreuen Bericht über eine Verhandlung in einer öffentlichen Sitzung des Nationalrates, des Bundesrates, der Bundesversammlung, eines Landtages oder eines Ausschusses eines dieser allgemeinen Vertretungskörper handelt,*

2. *im Falle einer üblen Nachrede*

a) *die Veröffentlichung wahr ist oder*

b) *ein überwiegendes Interesse der Öffentlichkeit an der Veröffentlichung bestanden hat und auch bei Aufwendung der gebotenen journalistischen Sorgfalt hinreichende Gründe vorgelegen sind, die Behauptung für wahr zu halten,*

3. *es sich um eine unmittelbare Ausstrahlung im Rundfunk (Live-Sendung) handelt, ohne daß ein Mitarbeiter oder Beauftragter des Rundfunks die gebotene journalistische Sorgfalt außer acht gelassen hat,*

3a. *es sich um die Abrufbarkeit auf einer Website handelt, ohne dass der Medieninhaber oder einer seiner Mitarbeiter oder Beauftragten die gebotene Sorgfalt außer Acht gelassen hat, oder*

4. *es sich um eine wahrheitsgetreue Wiedergabe der Äußerung eines Dritten handelt und ein überwiegendes Interesse der Öffentlichkeit an der Kenntnis der zitierten Äußerung bestanden hat.*

(3) *Bezieht sich die Veröffentlichung auf den höchstpersönlichen Lebensbereich, so ist der Anspruch nach Abs. 1 nur aus dem Grunde des Abs. 2 Z 1, des Abs. 2 Z 2 lit. a, des Abs. 2 Z 3 oder des Abs. 2 Z 3a ausgeschlossen, im Falle des Abs. 2 Z 2 lit. a aber nur, wenn die veröffentlichten Tatsachen in unmittelbarem Zusammenhang mit dem öffentlichen Leben stehen.“ [29]*

„§ 7. (1) *Wird in einem Medium der höchstpersönliche Lebensbereich eines Menschen in einer Weise erörtert oder dargestellt, die geeignet ist, ihn in der Öffentlichkeit bloßzustellen, so hat der Betroffene gegen den*

Medieninhaber Anspruch auf eine Entschädigung für die erlittene Kränkung. Der Entschädigungsbetrag darf 20 000 Euro nicht übersteigen; im übrigen ist § 6 Abs. 1 zweiter Satz anzuwenden.

(2) Der Anspruch nach Abs. 1 besteht nicht, wenn

1. es sich um einen wahrheitsgetreuen Bericht über eine Verhandlung in einer öffentlichen Sitzung des Nationalrates, des Bundesrates, der Bundesversammlung, eines Landtages oder eines Ausschusses eines dieser allgemeinen Vertretungskörper handelt,
2. die Veröffentlichung wahr ist und in unmittelbarem Zusammenhang mit dem öffentlichen Leben steht,
3. nach den Umständen angenommen werden konnte, daß der Betroffene mit der Veröffentlichung einverstanden war,
4. es sich um eine unmittelbare Ausstrahlung im Rundfunk (Live-Sendung) handelt, ohne daß ein Mitarbeiter oder Beauftragter des Rundfunks die gebotene journalistische Sorgfalt außer acht gelassen hat, oder
5. es sich um die Abrufbarkeit auf einer Website handelt, ohne dass der Medieninhaber oder einer seiner Mitarbeiter oder Beauftragten die gebotene Sorgfalt außer Acht gelassen hat.“ [29]

„Auch das Mediengesetz sieht Schadenersatz für Opfer von Übler Nachrede, Beschimpfung, Verspottung und Verleumdung (§ 6) sowie für die Verletzung des höchstpersönlichen Lebensbereiches (§7) vor. Das Mediengesetz gilt auch für öffentliche Websites.“ ([45], Seite 30)

4.2.6. Statistiken über Cyber - Mobbing

Abbildung 38 zeigt, dass 22% der Befragten Jugendlichen zwischen 14 und 20 Jahren in Deutschland schon Drohungen, Beleidigungen oder andere unangenehme Nachrichten bekommen haben. Weiters waren bereits 15% Beleidigungen oder Gerüchten ausgesetzt und 11% waren schon von Identitätsdiebstahl betroffen und weitere 4% litten unter unberechtigter Datenweitergabe.

All dies kann über soziale Netzwerke sehr schnell und einfach passieren.

Erfahrungen von Jugendlichen mit Mobbing im Internet oder per Handy in Deutschland im Jahr 2011

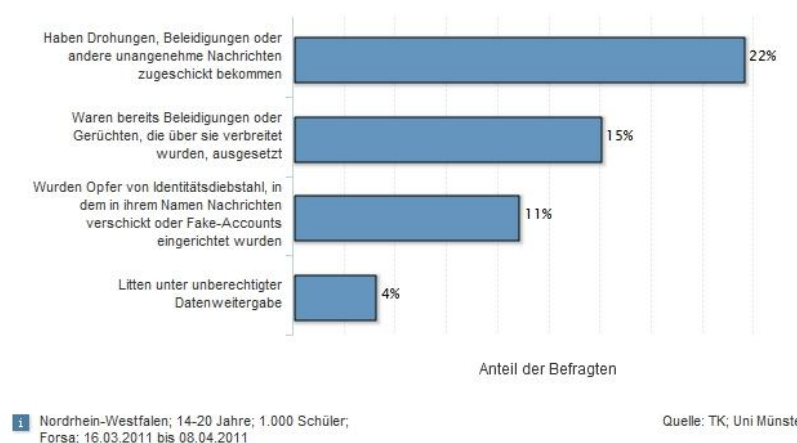


Abbildung 38: Cyber Mobbing Erfahrungen in Deutschland [2] basierend auf ([48], Seite 8)

Abbildung 39 zeigt, dass 18% der Befragten Jugendlichen schon einmal über Handy beleidigt oder bedroht wurden. Weitere 13% erlebten schon einmal, dass jemand über sie Beleidigungen oder Gerüchte verbreiten hat und 8% erlebten schon, dass jemand in ihrem Namen ein Benutzerkonto eingerichtet oder Nachrichten versendet hat. 3% erlebten, dass private E-Mail, Fotos, usw. gegen ihren Willen weitergeleitet wurden.

Verbreitung von Cybermobbing unter Jugendlichen in Deutschland in 2011

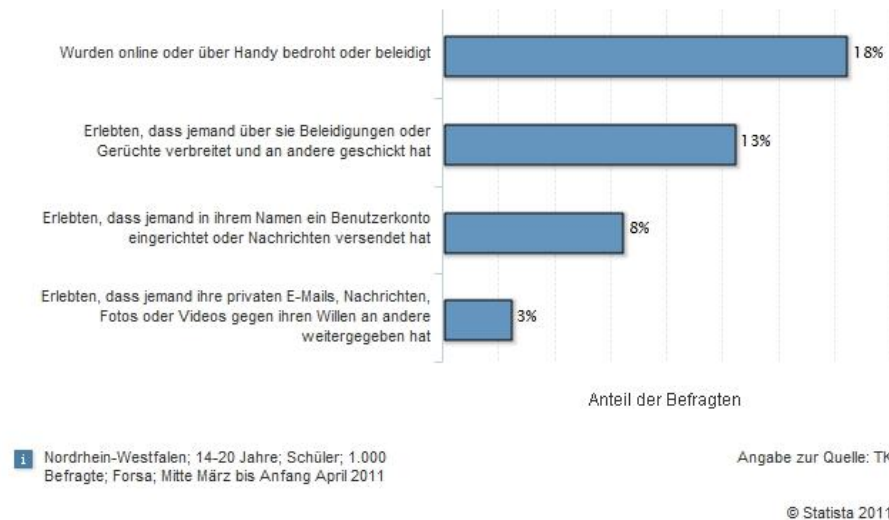


Abbildung 39: Verbreitung von Cybermobbing unter Jugendlichen [2] basierend auf [49]

Folgende Statistik (Abbildung 40) zeigt, dass 60% der Betroffenen von Cyber - Mobbing ihre Täter kennen, also die Täter in ihrem Bekanntenkreis sind.

Kenntnis der Täter von Cybermobbing aus Sicht der Opfer in Deutschland im Jahr 2011

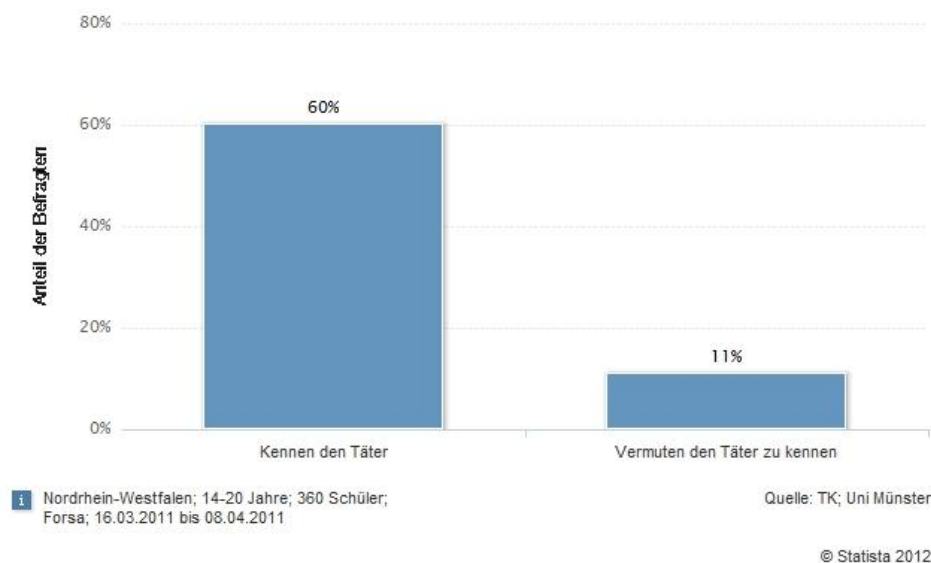
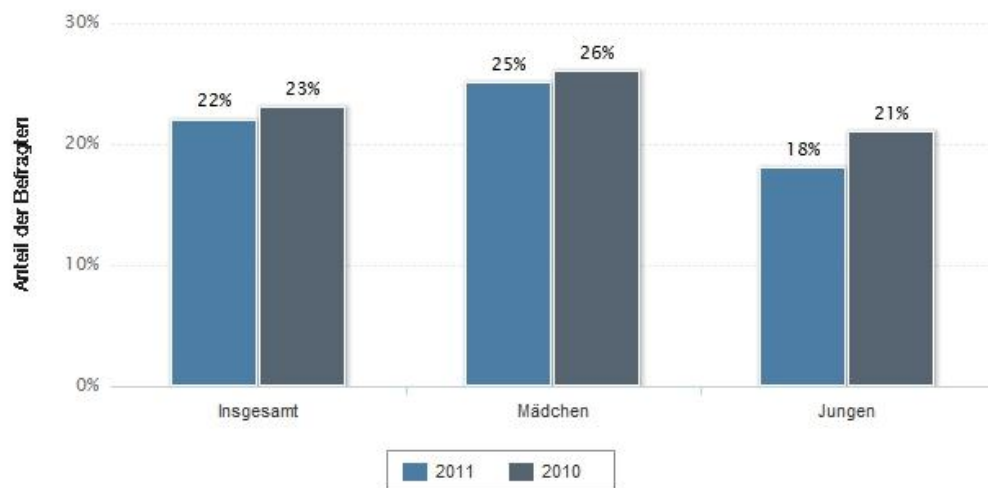


Abbildung 40: Cyber Mobbing Täter [2] basierend auf ([48], Seite 6)

Auch diese Statistik (Abbildung 41) zeigt, dass immerhin schon 22% der Befragten Jugendlichen zumindest in ihrem Bekanntenkreis mit Mobbing zu tun hatten. Außerdem zeigt die Statistik, dass Mädchen von Mobbing mehr betroffen sind als Buben.

Anteil der Jugendlichen, in deren Bekanntenkreis schon mal jemand im Internet fertig gemacht wurde



i Deutschland; 12-19 Jahre; 1.188 Internet-Nutzer;
ENIGMA GfK; 16.05.2011 bis 26.06.2011

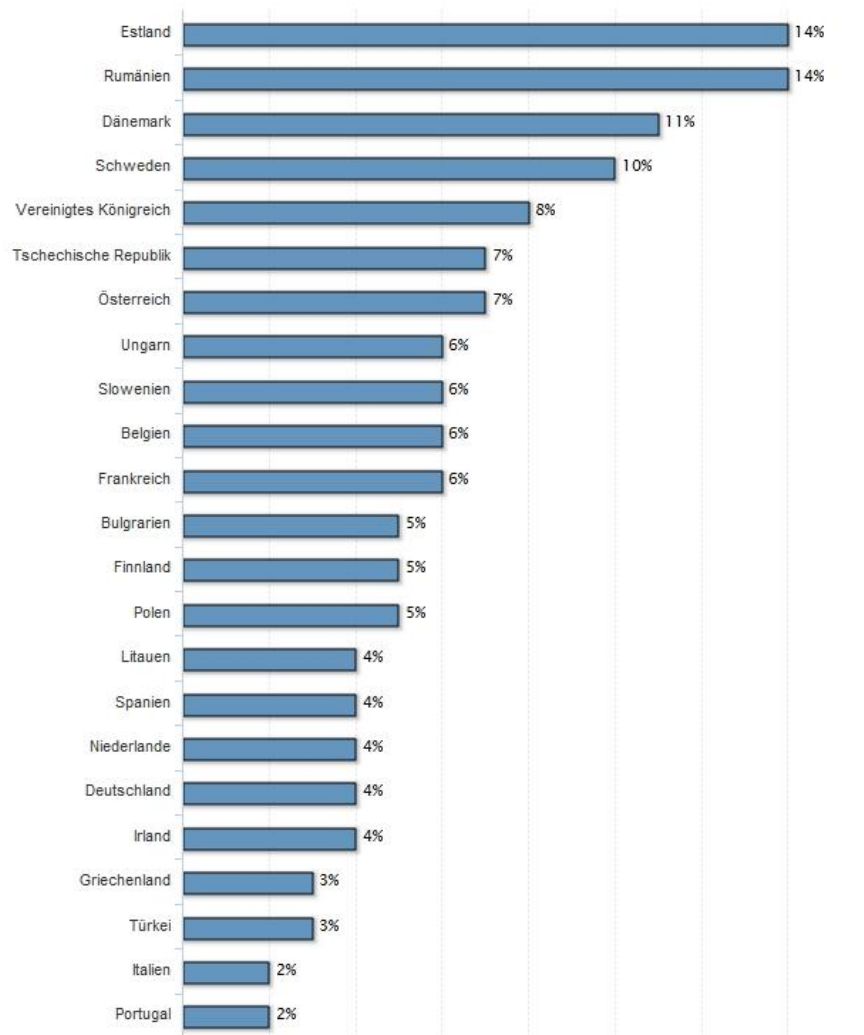
Quelle: mpfs

© Statista 2011

Abbildung 41: Jugendlichen, i. d. Bekanntenkreis schon gemobbt wurde [2] basierend auf ([15], Seite 40)

Anhand der nächsten Statistik (Abbildung 42) ist sehr schön zu sehen, dass auch in Österreich das Thema Cyber Mobbing vorhanden ist. Immerhin wurden 7% der Befragten Jugendlichen im Alter von 9 bis 16 Jahren schon im Internet gemobbt.

Anteil der Kinder und Jugendlichen im Alter von 9 bis 16 Jahren in europäischen Ländern, der in den letzten 12 Monaten im Internet gemobbt wurde



Anteil der Kinder und Jugendlichen

1 Europa; 9 bis 16 Jahre; 23.420 Kinder und Jugendliche, die das Internet nutzen, aus 25 Ländern, davon 1.000 aus Deutschland; The London School of Economics and Political Science;

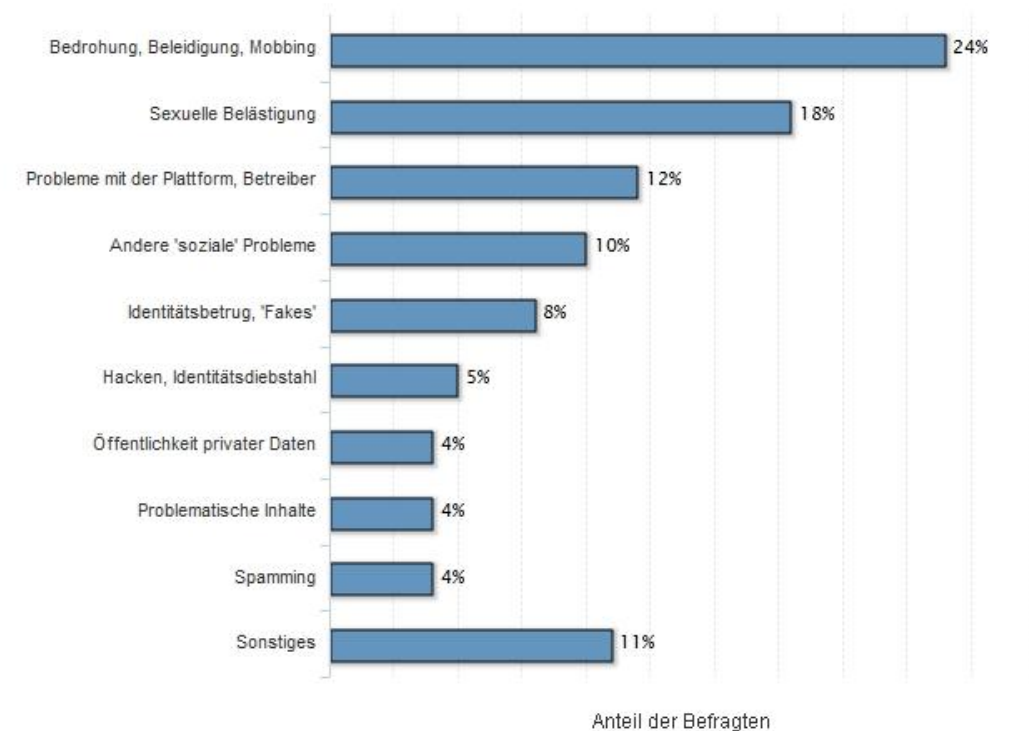
Quelle: EU Kids Online

© Statista 2011

Abbildung 42: Länderstatistik über Cyber Mobbing [2] basierend auf [50]

Abbildung 43 zeigt, dass Mobbing an erster Stelle der schlechten Erfahrungen im Internet steht. Laut dieser Statistik wurden 24% der Befragten schon einmal bedroht, beleidigt oder gemobbt. Der Anteil des Identitätsdiebstahls ist auch sehr hoch mit 5%.

Welche schlechten Erfahrungen hast Du in sozialen Netzwerken gemacht?



i Deutschland; 12 bis 19 Jahre; 1.816 Jugendliche, die schlechte Erfahrungen in sozialen Netzwerken gemacht haben; Winter 2008/2009

Quelle: MeMo

Abbildung 43: Schlechte Erfahrungen in sozialen Netzwerken [2] basierend auf [51]

4.3. Phishing

Phishing setzt sich aus den Wörtern „Passwort“ und „fishing“ zusammen und man versteht darunter eine besondere Form des Online-Betrugs. (vgl. [52]) Phishing wird im Allgemeinen für das Erschleichen von Passwörtern verwendet. (vgl. [4])

Phishing-Betrüger fälschen immer öfter E-Mails und Internetseiten, um an vertrauliche Informationen wie Passwörter, Zugangsdaten oder Kreditkartennummern zu kommen. (vgl. [53]) Die Betrüger verschicken hier sehr echt aussehende E-Mails, in denen sie die Benutzer auffordern, auf einen Link zu klicken und sich unter irgendeinem Vorwand in den Account einzuloggen, z.B. um dort die Benutzerdaten zu aktualisieren. Der Link verweist auf eine gefälschte Website, mittels der die Betrüger die Nutzerdaten abfangen und so können sie Bankkonten leerräumen. (vgl. [52])

Diese Phishing–Mails funktionieren immer wieder, da die Internetadressen, der echten Adresse sehr ähnlich sind bzw. ist es auch schon vorgekommen, dass die Betrüger die Adressleiste des Browsers mittels JavaScript gefälscht haben. (vgl. [53])

Solche Phishing–Angriffe kann man in zwei Teile einteilen. Zuerst bekommt man eine E-Mail, die ein Vertrauensverhältnis ausnutzt und meistens auf eine bösartige Internetseite lockt oder Schadprogramme im Anhang hat. Beim zweiten Teil des Angriffes passiert dann der eigentliche Betrug, nämlich hier wird man dazu verleitet vertrauliche Daten preiszugeben, indem der Benutzer glaubt, er sei auf seiner vertrauten Website. Diese Daten können dann von den Betrüger missbräuchlich verwendet werden, indem sie zum Beispiel das Konto leerräumen. (vgl. [53])

Spear-Phishing und Social–Phishing sind zwei neue Formen des Phishings, sie haben sich unter anderem wegen der sozialen Netzwerke entwickelt.

4.3.1. Spear Phishing

Beim Spear Phishing lebt der Phisher von der Vertrautheit mit den Daten des Opfers. Er kennt meistens den Namen und die E-Mail Adresse und spricht die Opfer meistens auch persönlich an. (vgl. [54]) Dieser Phishing Ansatz verschafft sich das Vertrauen des Opfers über Informationen aus den sozialen Netzwerken. Der E-Mailverkehr kommt dann anscheinend von einem Kollegen, einen virtuellen Freund oder vom Arbeitgeber. (vgl. [55]) Meist verweisen die E-Mails auf einen gemeinsamen Freund oder auf den letzten Online Einkauf im Internet. Da die E-Mail meist von einem Bekannten, Freund oder Arbeitskollegen kommt, geht man unachtsamer damit um. (vgl. [54])

Das Vorgehensmodell der „Spear-Phisher“ ist immer sehr ähnlich. Sie bauen zuerst Vertrauen auf und nutzen dadurch Insider Informationen, die sie sich vorher aus sozialen Netzwerken, Blogs, Website usw. beschaffen. In der nächsten Phase schicken sie dem Opfer E-Mails mit der Bitte, ihnen kurzfristig persönliche Daten zu schicken. Als letztes werden die Opfer dann meistens gebeten einen Link in einer E-Mail zu folgen und diesen anzuklicken, mit dem sie dann auf einer sehr realistisch erscheinenden Website landen. Auf dieser Website werden dann bestimmte persönliche Daten wie Bankverbindung, Identifikationsnummer, Zugangscode usw. abgefragt. Hier endet die „Spear-Phishing-Attacke“, dann genauso wie eine „normale“ Phishing Attacke. Es gibt noch weitere Spear-Phishing Ansätze, wie das Hacken von Adressbüchern usw. Die Kreativität der Spear-Phisher entwickelt sich immer weiter. (vgl. [55])

Das Ziel von Spear Phishing ist oft nicht nur das Stehlen von persönlichen Daten, sondern sich oft auch Zugang zu speziellen Organisationen zu verschaffen. (vgl. [56])

4.3.2. Social Phishing

Social Phishing ist ein Kunstwort und setzt sich aus den Worten Phishing und Social Engineering zusammen. (vgl. [57]) Beim Social Phishing handelt es sich um eine neue Art des Phishings, die den Angreifern viel höhere Erfolgsquoten bringen. Denn vermeintliche E-Mails von Bekannten oder Freunden, auch Facebook Freunden, wird viel eher vertraut, als wenn es sich um einen unbekannten Absender handelt.

Laut einer Studie von Wissenschaftlern an der Indiana University (USA) steigt die Erfolgsquote von 16% auf 72%.

Die Wissenschaftler verschickten Phishing Mails mit einem gefälschten Absender an eine Gruppe von Studenten (Testgruppe) und an eine weitere Gruppe (Kontrollgruppe). Der Inhalt der E-Mail lautete „Check this out!“ und der Link dahinter führte auf eine gefälschte Website außerhalb der Universität und verlangte das Universitätslogin und Passwort, mittels Kerberos konnten die Wissenschaftler testen ob das Passwort richtig ist oder nicht. Für die Kontrollgruppe verwendeten die Wissenschaftler die persönlichen E-Mail Adressen die den Studenten bekannt waren. Bei der Testgruppe verwendeten die Wissenschaftler gefälschte Absender, die den Studenten persönlich bekannt waren (z.B. Freunde, Bekannte), diese Namen der angeblichen Absender recherchierten die Wissenschaftler in den sozialen Netzwerken (z.B. MySpace, Facebook, usw.), in den die Studenten aktiv waren.

Das Ergebnis war erstaunlich, denn durch diesen Trick wurde die Erfolgsquote von 16% in der Kontrollgruppe auf 72% in der Testgruppe gesteigert. Dieser Trick ist natürlich auch jedem professionellen Phisher leicht zugänglich! (vgl. [57])

Social Phishing nutzt die spezifischen Informationen und ist somit effektiver als das herkömmliche Phishing. Zum Beispiel könnte die Meldung von einem „Freund“ erscheinen.

Mit der automatisierten Datenextraktion aus sozialen Netzwerken über FiTM (Friend in the Middle) Angriffen wird eine große Menge an verwertbaren Daten dem Angreifer zur Verfügung gestellt.

Zum Beispiel: Wenn herausgefunden wird, dass das Opfer vorwiegend auf Französisch kommuniziert, wird man keine Mail mit englischem Text schicken, sondern auf Französisch. Man kann auch Fotos des Opfers verwenden um einen Link mitzuschicken, der angeblich zu mehr Bildern führt. (vgl. [34])

4.3.3. Phishing über Soziale Netzwerke - Statistik

Soziale Netzwerke und Online-Spielewebseiten entwickeln sich immer mehr zu beliebten Angriffsflächen für Phishing-Attacken, um an Passwörter und persönliche Daten der User zu kommen. (vgl. [58]) Beim Phishing werden nicht immer nur Bankdaten gefischt, sondern es können auch die Zugangsdaten zu sozialen Netzwerken abgefischt werden.

*„Das hinterhältige an dieser Methode: die eigenen Freunde und Kollegen werden als vermeintliche Absender von Phishing-Nachrichten missbraucht. Insgesamt macht die Zahl der Phishing-Attacken über soziale Netzwerke mittlerweile **84,5 Prozent aller Phishing-Angriffe** aus. Im Vorjahreszeitraum waren es lediglich 8,3 Prozent.“ [58]*

Figure 34. Impressions for each type of phishing site each month in 2010

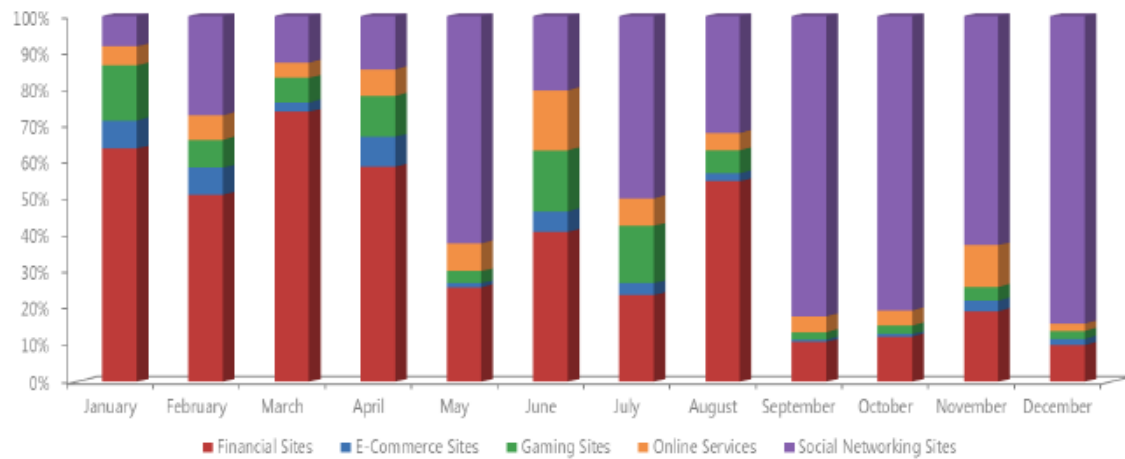


Figure 35. Active phishing sites tracked each month in 2010, by type of target

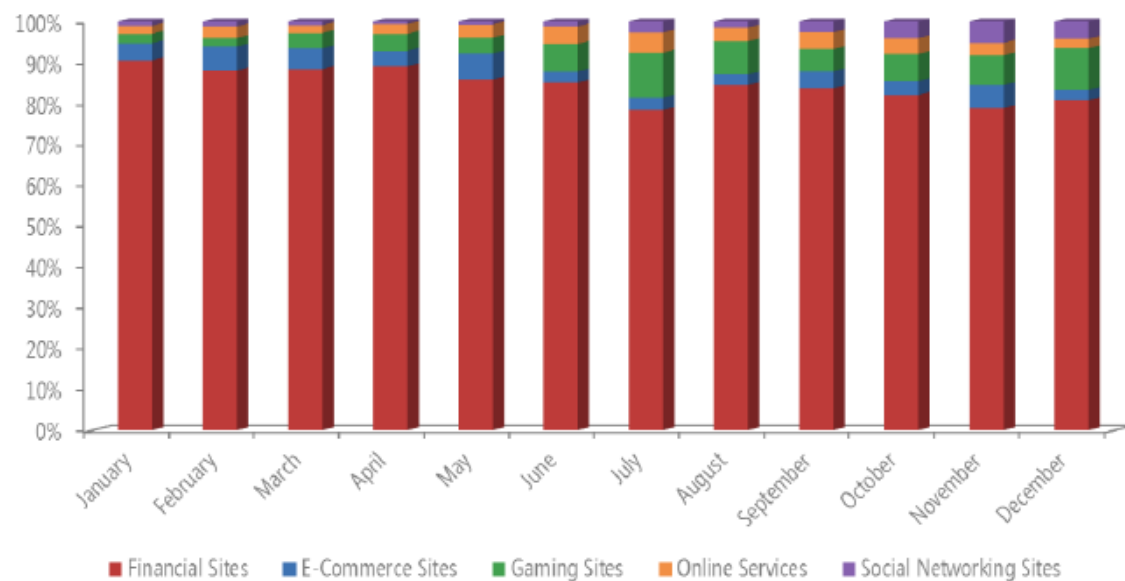


Abbildung 44: Entwicklung von Phishing über Soziale Netzwerke in 2010 ([59], Seite 58)

"Phishers have traditionally targeted financial sites more than other types of sites, but 2010 showed evidence of a shift to social networks. Phishing impressions that targeted social networks increased from a low of 8.3 percent of all impressions in January to a high of 84.5 percent of impressions in December. In particular, the final four months of the year show signs of a strong and sustained phishing campaign or campaigns against social networks." ([59], Seite 58 f)

Weitere Statistiken über Phishing

Abbildung 45 zeigt, dass Paypal noch immer am häufigsten von Phishern angegriffen wird. Aber die Statistik zeigt auch, dass Facebook schon an vierter Stelle der am häufigsten betroffenen Websites liegt. Diese zeigt, dass die sozialen Netzwerke für Angreifer immer interessanter werden.

Verteilung der Phishing Angriffe nach betroffenen Websites im ersten Halbjahr 2011

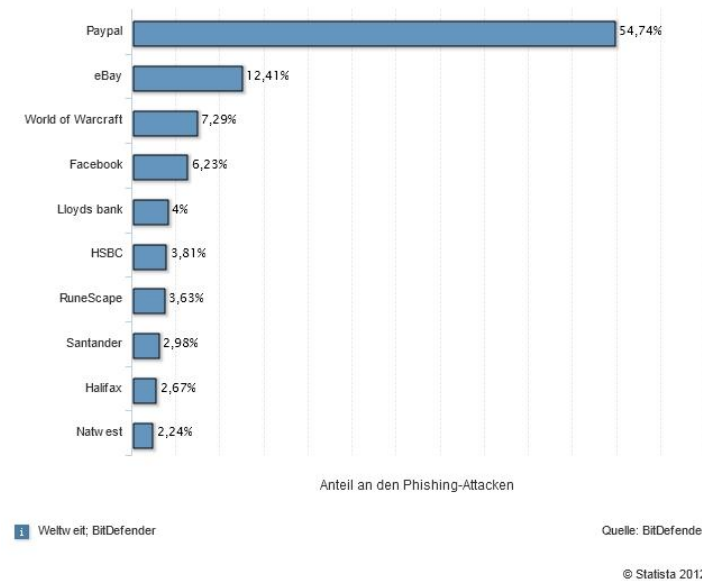


Abbildung 45: Phishing Angriffe nach Websites im 1.Halbjahr 2011 [2] basierend auf [60]

Auch diese Statistik (Abbildung 46) zeigt, dass Facebook immer häufiger im Angriffsfeld der Angreifer steht.

Am häufigsten von Phishern angegriffene Organisationen im Jahr 2010

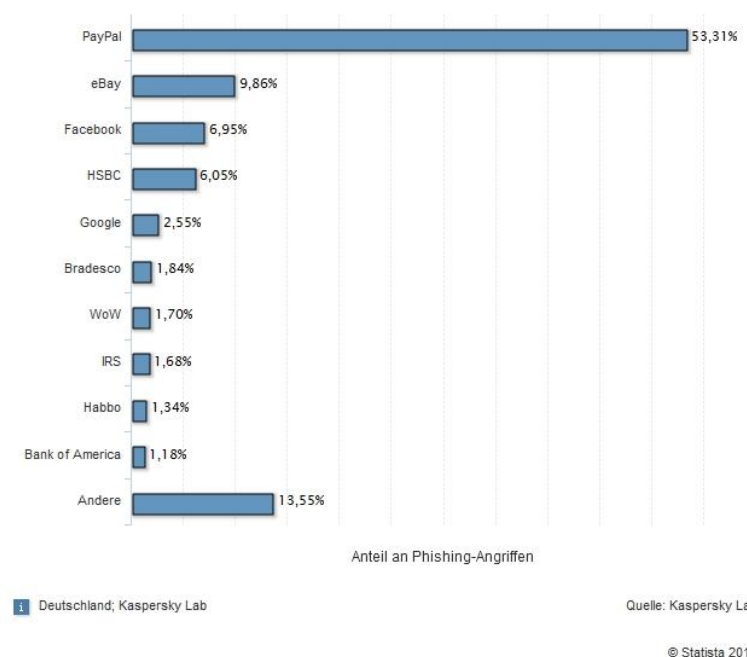


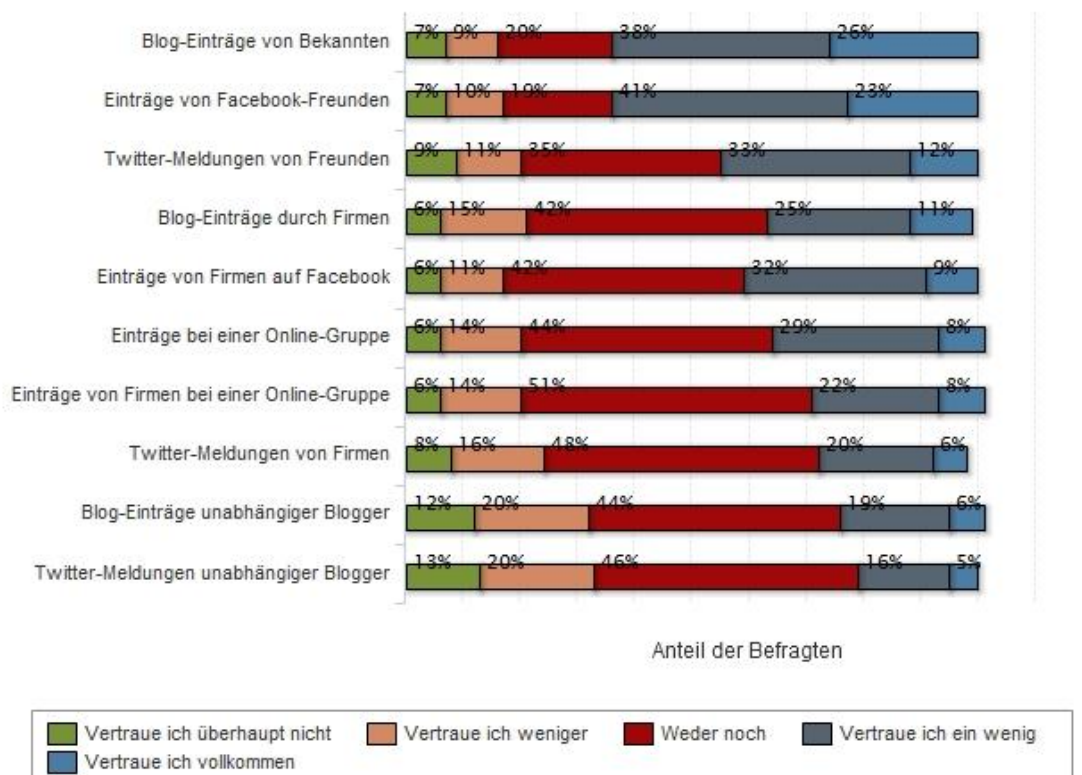
Abbildung 46: Angegriffene Organisationen durch Phishing in 2010 [2] basierend auf [61]

4.4. Verbreitung von Schadsoftware über sozialen Netzwerken

Schadsoftware lässt sich auf viele verschiedene Arten verbreiten, doch mit wachsender Beliebtheit der sozialen Netzwerke, wächst auch die Verbreitung der Schadsoftware über soziale Netzwerke. Denn wie einige Statistiken zeigen, werden Bekannten und Freunden in sozialen Netzwerken sehr stark vertraut und genau dieses Vertrauen wird von den Angreifern ausgenutzt, um ihre Schadsoftware zu verbreiten.

Diese Statistik (Abbildung 47) belegt, dass 26% der Befragten Blog Einträgen von Bekannten vollkommen vertrauen und immerhin 23% der Befragten vertrauen vollkommen Einträgen von Facebook-Freunden. Durch diese Statistik lässt sich sehr leicht erklären, warum Phishing Angriffe bzw. Schadsoftwareverteilung in sozialen Netzwerken sehr einfach und erfolgreich funktioniert. Dadurch dass der Vertrauenswert sehr hoch ist, werden auf Links die von Freunden oder Bekannten kommen oder empfohlen werden sehr schnell und ohne Skepsis geklickt. Aus diesem Grund haben sich Angreifer mittlerweile darauf spezialisiert Angriffe über soziale Netzwerke durchzuführen.

Vertrauenseinschätzung zu Informationsquellen im Bereich Social Media von Internetnutzern 2010



USA; Invoke Solutions; 29.07.2010

Quelle: eMarketer

© Statista 2011

Abbildung 47: Vertrauenseinschätzung zu Informationsquellen in sozialen Netzwerken [2] basierend auf [62]

Beispiel einer Schadsoftware, welche speziell über Facebook verbreitet wurde:

Der Koobface-Wurm tauchte 2008 das erste Mal auf und entwickelte sich über die Jahre weiter und er wurde auch „schlauer“. Koobface ist vor allem in Facebook aktiv. Dieser Wurm verschickt Chat-Nachrichten mit einem Link, dieser verspricht dem User ein Foto, doch beim Anklicken des Linkes öffnet sich ein Hinweis, dass das Foto an einen anderen Ort verschoben wurde und mit dem Link „View Photo“ wird der User nun weitergeleitet. Mit dem Klick auf „View Photo“ wird der automatische Download gestartet und anschließend installiert sich der Wurm auf der Festplatte. Jeder dieser Links ist nur einmal aktiv, deswegen ist dieser Wurm für die Antivirenhersteller sehr schwer zu verfolgen. Hat sich der Wurm einmal auf den Computer eingenistet, so sucht er nach Login-Daten von FTP-Konten oder anderen Internetseiten. Weiters verschickt er selbstständig Nachrichten an Freunde über Facebook, um sich weiter zu verbreiten. (vgl. [63])

Dieser Wurm war und ist so erfolgreich, weil er auf dem Vertrauen der Facebook User gegenüber den Freunden aufsetzt. Die Links zu interessanten Fotos oder Internetseiten kommen immer per Chat, Nachricht oder Mitteilung auf der Pinnwand. Somit glauben die Facebook User dies wird von einem Freund empfohlen und damit gibt es quasi keine Skepsis. Dieses Verhalten nutzen Online-Kriminelle aus und entwickeln Würmer, die im Namen der Freunde ihre Schadsoftware verteilen. Meist werden über Sicherheitslücken oder Phishing Attacken fremde Facebook-Zugänge „ergaunert“ und dann die gefährlichen Botschaften an die Freundesliste des „gehackten“ Facebook Accounts geschickt.

Die Absichten der Angreifer sind eigentlich immer die gleichen, sie wollen wertvolle oder sensible Daten ausspionieren. Dabei handelt es sich meist um Zugangsdaten für Online-Banking, denn die meisten Angreifer haben es auf Geld abgesehen. (vgl. [64])

Damit die User es nicht so einfach haben, existieren von diesem Wurm natürlich verschiedene Formen. So gibt es auch Formen, die nicht auf Fotos verlinken, sondern die mit Einladungen locken oder witzige Videos versprechen. Das Prinzip ist das Gleiche. Es wird ein Link verschickt, danach erhält man die Aufforderung seine Flash-Installation zu aktualisieren und statt dieser Aktualisierung wird der Koobface-Wurm heruntergeladen und installiert. Eine weitere Form ist, dass die Nutzer mit bedrohlichen Warnungen eines Virenbefalls konfrontiert werden und ihnen eine Sofort-Lösung angeboten wird. Diese ist natürlich nur gegen Geld zu beziehen. Auf diese Weise wurden ebenfalls Einnahmen lukriert. (vgl. [65])

Beispiel einer Schadsoftware die speziell über Twitter verbreitet wurde

Twitter wird häufig genutzt um Schadsoftware für Smartphones zu verbreiten. Ein Beispiel für so ein Schadprogramm ist der Schädling „Android.Opfake“, diese wurde mithilfe von Twitter unter die User gemischt. Es wurde ein Link in ein Tweet eingebaut und wenn man darauf klickte öffnete sich eine Downloadseite, klickte man auf diesen Link so wurde dieses Schadprogramm installiert. Es handelte sich dabei um ein spezielles Schadprogramm für Android Smartphones, diesen wurde dann auch geraten nur von der offiziellen Seite Programme herunterzuladen. (vgl. [66])

5. Verwundbarkeit in sozialen Netzwerken

Dieses Kapitel beschäftigt sich mit der Verwundbarkeit von Personen, die persönliche Daten bzw. Informationen in sozialen Netzwerken veröffentlichen. Auch wenn man meint, man gibt es nur für „Freunde“ frei, so ist man nicht davor geschützt, dass diese Informationen nicht auch an Personen gelangen, die diese vielleicht nicht erhalten sollen. Wie sehr viele Fälle zeigen, ist es immer wieder schon vorgekommen, dass Informationen an Personen herangetragen wurden, die für sie nicht bestimmt waren bzw. gibt es schon sehr viele Tools und Angriffsszenarien, die es Hackern ermöglicht, trotzdem an die gewünschten Informationen heranzukommen.

Deswegen werden in diesem Kapitel noch einmal die Angriffsszenarien und Gefahren der sozialen Netzwerke kurz beschrieben und dazu entsprechende Beispiele angeführt.

Tabelle 3 gibt einen Überblick, welche Informationen für die Angriffsszenarien bzw. Gefahren relevant bzw. kritisch sind, wenn diese öffentlich gemacht werden. Die Spalte mit den Informationen entspricht den Eingabefeldern in Facebook. In dieser Tabelle wird noch keine Gewichtung der einzelnen Informationen vorgenommen. Wie die Gewichtung bzw. die „x“ in Tabelle 3 zustande gekommen sind, wird in Kapitel 5.1 näher beschrieben.

Grundsätzlich beruht der Überblick auf einer Umfrage unter 8 Sicherheitsleuten in einem großen Unternehmen. Diese Umfrage diente allerdings nur als Datenbasis und wurde anhand einer umfangreichen Recherche ergänzt bzw. wurde teilweise das Ergebnis, wenn notwendig auch korrigiert auch wenn die Umfrage ein anderes Ergebnis lieferte. Die detaillierte Auswertung der Umfrage befindet sich im Kapitel 8 Anhang (Auswertung der Befragung).

Überblick über die Kritikalität, der zur Verfügung gestellten Informationen, in sozialen Netzwerken

Informationen (Eingabefelder)	Identitätsdiebstahl	Cyber-Mobbing	Phishing	Spear-Phishing	Social Phishing	Verbreitung von Schadsoftware	Verkauf der Daten - Werbung	Bewerbung	Kündigung
Name	X	X		X	X		X	X	
Nutzername		X							
Geschlecht	X	X			X			X	
Adresse	X	X					X	X	
Geburtstag	X	X		X	X		X	X	
Sprache		X		X	X		X	X	
E-Mail Adresse	X	X	X	X	X	X	X	X	
Telefonnummern		X					X		
andere Nutzernamen (anderer Netzwerke)		X							
Gefällt mir									
Netzwerke					X				
Verknüpfte Konten		X							
Profilbild		X						X	
Beziehungsstatus		X							
Familienmitglieder									
Interessiert an (Sexuelle Vorlieben)							X		
Arbeitgeber	X			X			X	X	X
Hochschule, Schule und Kurse				X			X		
Religion		X					X		X
Politische Einstellung		X		X			X	X	
Personen, die mich inspirieren							X		
Interessen und Aktivitäten (Hobbys, usw.)		X		X			X	X	
Musik, Bücher, Filme, Fernsehen, Spiele				X			X		
Lieblingssport-arten, -mannschaften, Lieblingssportler				X			X		
Fotos (Urlaubsfotos, Partybilder, usw.)		X			X			X	X
Aktueller Aufenthaltsort (GPS)		X					X		
Statusmeldungen (Neuigkeiten)						X		X	X
Anwendungen und Spiele						X	X		
Gruppen					X				
Pinnwandkommentare		X				X		X	X

Tabelle 3: Angriffsszenarien und Gefahren

Identitätsdiebstahl

Umso mehr Daten „Angreifer“ bzw. „Betrüger“ von einer Person wissen, umso besser, denn somit können sie das Opfer bzw. deren Bekannte oder „Freunde“ besser täuschen. Deswegen ist es gerade beim Identitätsdiebstahl sehr gefährlich, wenn die Betrüger auf sehr viele vertrauliche Daten Zugriff haben.

Beim Identitätsdiebstahl gibt es verschiedene Formen, da ein Angreifer könnte ein neues Facebook-Konto im fremden Namen eröffnen könnte, und somit Gerüchte verbreiten, welche nicht der Wahrheit entsprechen. Oder aber der Angreifer kann das Konto des sozialen Netzwerkes hacken und Gerüchte verbreiten, bzw. vielleicht auch Fotos veröffentlichen, die entstellt sind und so weiter. All dies sind Formen des Identitätsdiebstahl und können zu weiteren „Gefahren“ führen, wie beispielsweise zu einer Kündigung.

Beispiele:

Unbekannte haben im Namen des Rostocker Finanzsenators ein Profil bei Facebook eröffnet und unter dieser Identität Fotos, Links und Kommentare veröffentlicht. Diese Veröffentlichungen standen zum Teil im Zusammenhang mit seiner Arbeit für den Rostocker Oberbürgermeister. Außerdem wurde ein Artikel veröffentlicht, welcher zu einer Imageschädigung führte. Der Betroffene hat sich daraufhin später offiziell von diesem Profil distanziert, und auch vor Reaktionen auf Anfragen von diesem Profil gewarnt. (vgl. [67])

Ein Angreifer hat Mitarbeiter von einer Firma über soziale Netzwerke identifiziert, anschließend einen Account gehackt und somit übernommen. Mittels dieses Accounts hat der Angreifer herausgefunden, dass ein Firmenpicknick geplant ist. Weiters konnte der Angreifer die Kommunikation zwischen fünf guten Freunden beobachten. Nach dem Picknick versendete der Angreifer eine Nachricht mit der Angabe, dass sich im Anhang Fotos vom Picknick befinden. Doch statt den Fotos befand sich im Anhang ein Keylogger, welcher nach dem Klick automatisch installiert wurde. Durch diesen Keylogger kamen die Angreifer an die Firmen-login-Daten des Mitarbeiters. Schlussendlich haben die Angreifer zwei Wochen im Firmennetz verbracht, Informationen gesammelt und zwei Server unter ihre Kontrolle gebracht, ohne dass es bemerkt wurde. Erst als ein Freund den Betroffenen auf die Nachricht mit den nicht angezeigten Fotos angesprochen hat, wurde der Einbruch bemerkt. (vgl. [7])

Weitere Beispiele siehe: [68], [69], [70]

Cyber-Mobbing:

Cyber-Mobbing ist eine Form des „Beleidigens“. Hier können Fotos sehr hilfreich sein, denn diese kann man mit beleidigenden Kommentaren kommentieren oder es können auch bloßstellende Fotos des Opfers durch den „Täter“ veröffentlicht werden. Es kann auch passieren, dass persönliche Informationen - wie ein privates Ereignis, dass einem gerade sehr beschäftigt - dadurch das man es in einem Sozialen Netzwerk kundtut, missbraucht wird, um jemanden zu verletzen. Auch hier gab es schon sehr schlimme Fälle.

Cyber-Mobbing nimmt auch deshalb zu, weil die Hemmschwelle des „Jemanden-etwas-ins-Gesicht-sagen“, einfach nicht mehr vorhanden ist, denn im Internet über jemanden etwas zu schreiben, ist wesentlich einfacher, als es demjenigen „ins Gesicht“ zu sagen.

„Hänseleien, Beschimpfungen, Hasstiraden - das Internet macht es leicht, andere niederzumachen. Plattformen wie SchülerVZ, Facebook oder MySpace sind dafür besonders geeignet.“ [71]

Beispiele:

2011 ereignete sich ein tragischer Fall in Folge von Cyber-Mobbing. Ein 13-Jähriger beging Selbstmord, weil er im Internet als homosexuell bezeichnet wurde. Im Mai wurde der Junge in Facebook als homosexuell bezeichnet. Auf seiner Pinnwand befand sich ein Link, dieser führte auf eine Homepage auf der er als „schwul“ bezeichnet wurde. Aus Angst vor seinen Mitschülern, wählte er noch am selben Tag den Freitod. (vgl. [72])

Auch in England gab es schon einen Fall von Selbstmord als Folge von Cyber-Mobbing-Attacken. Eine 15-Jährige britische Schülerin wurde online derart gemobbt, dass sie keinen anderen Ausweg mehr sah als den Selbstmord. (vgl. [71])

Weitere Beispiele siehe: [73], [74], [75], [76]

Phishing, Spear Phishing und Social Phishing

Gerade für Phishing sind soziale Netzwerke sehr interessant geworden, denn die "Phisher" nutzen auch nur die wenig sichtbaren Informationen, um gezielt Phishing Mails zu verschicken. Denn ein Mail mit persönlicher Anrede oder mit einem Hinweis auf ein eigenes Hobby wird viel erfolgreicher sein, als ein Massenmail. Weitere sehr erfolgreiche Phishing Angriffe sind, wenn die Mails von einem „Freund“ kommen, so werden seit neuesten Phishing Mails von den „eigenen Online Freunden“ verschickt, indem die Angreifer einfach die Mail Adressen klauen.

Spear Phishing:

„(engl. *Spear(p)fischen*) Variante des Phishing Angriffs, bei der gezielt einzelne Personen oder eine Gruppe E-Mails mit entsprechender Spyware (z.B. Keylogger) erhält.“ ([4], *Sicherheitsprobleme im Internet*)

Social Phishing

Social Phishing ist ein Kunstwort und setzt sich aus den Worten Phishing und Social Engineering zusammen. (vgl. [4])

Verbreitung von Schadsoftware

Auch für die Verbreitung von Schadsoftware sind Informationen wie Name, Party- und Urlaubsfotos und die E-Mail Adresse von großer Bedeutung, denn über soziale Netzwerke können wunderbar Links verteilt werden, die zu „angeblichen“ Fotos oder Videos führen, die dann aber leider nicht geöffnet werden können, und sich stattdessen ein Wurm oder Trojaner installiert und so alle möglichen Daten vom Computer sammeln kann.

Beispiel:

Der Wurm „Ramnit“ treibt auf Facebook sein Unwesen, dieser Wurm hat die Absicht Login-Daten der Nutzer zu sammeln. Diesen Wurm gab es schon 2010 und 2011, damals hatte er es auf Online-Banking, Konzernnetzwerke und Finanzinstitute abgesehen, jetzt versucht er sein Unwesen auf Facebook zu treiben. (vgl. [77]) Auch er verbreitet sich mit Links, die von „Freunden“ stammen, denn die Angreifer nutzen die gehackten Login-Daten, um den Wurm über die Freundesliste weiter zu verbreiten. Außerdem können Cyberkriminelle davon profitieren, dass viele Nutzer dasselbe Passwort in verschiedenen Internetdiensten, wie Facebook, Gmail, Outlook usw., benutzen. So können Sie auch zu Zugangsdaten von Unternehmensnetzwerken usw. kommen. (vgl. [78])

Weitere Beispiele siehe [79], [80], [81]

Verkauf der Daten (Tracking)

Eine feste Einnahmequelle von Facebook ist, das Erlauben von Tracking-Cookies gegen Bezahlung. Das heißt Facebook erlaubt anderen Unternehmen, ihre Tracking-Cookies auf Facebook zu platzieren, damit die Unternehmen entsprechende Nutzerprofile erstellen können. Damit können sie danach gezielt Werbung schalten oder per E-Mail versenden. (vgl. [82])

„ . . . eine Beschreibung des Grundproblems: Wenn ich eine Spiegel-Seite aufrufe oder die Fan-Seite von Hannover 96 oder irgendeine andere Seite mit Facebook-Elementen, bekommt Facebook die Information, dass ich, Jürgen Schmidt, diese konkrete Seite gelesen habe. Da Facebook-Buttons quasi omnipräsent sind, kann Facebook eine komplette Liste aller Websites erstellen, die ich besuche und diese mit meiner Person verknüpfen – einer Person, deren Namen, Adresse, Vorlieben und Freunde es kennt.“ [82]

Neueste Meldungen zeigen außerdem, dass Facebook die Geschäftsbedingungen über eine „Aktualisierung der Erklärung der Rechte und Pflichten“ geändert hat. Diese Änderungen machen es Facebook einfacher Daten an Dritte zu verkaufen. Welche Daten genau verkauft werden wird nicht veröffentlicht, allerdings ist anzunehmen, dass gerade persönliche Daten wie Name, Adresse, E-mail Adresse, Telefonnummer und natürlich Vorlieben verkauft werden, denn auf diesen Daten können Marketingfirmen aufsetzen, um gezielt Werbung produzieren und zu verschicken.

Hier ein Auszug aus der aktuellen Erklärung von Rechten und Pflichten:

„Teilen deiner Inhalte und Informationen

Dir gehören alle Inhalte und Informationen, die du auf Facebook postest. Zudem kannst du mithilfe deiner Privatsphäre- und Anwendungseinstellungen kontrollieren, wie diese ausgetauscht werden. Ferner:

- *Für Inhalte wie Fotos und Videos, die unter die Rechte an geistigem Eigentum (sog. „IP-Inhalte“) fallen, erteilst du uns durch deine Privatsphäre- und Anwendungseinstellungen die folgende Erlaubnis: **Du erteilst uns eine nicht-exklusive, übertragbare, unterlizenzierbare, gebührenfreie, weltweite Lizenz zur Nutzung jeglicher IP-Inhalte, die du auf oder im Zusammenhang mit Facebook postest („IP-Lizenz“).** Diese IP-Lizenz endet, wenn du deine IP-Inhalte oder dein Konto löschst, außer deine Inhalte wurden mit anderen Nutzern geteilt und diese haben die Inhalte nicht gelöscht.*
- *Wenn du IP-Inhalte löschst, werden sie auf eine Weise entfernt, die dem Leeren des Papierkorbs auf einem Computer gleichkommt. Allerdings sollte dir bewusst sein, dass entfernte Inhalte für eine angemessene Zeitspanne in Sicherheitskopien fortbestehen (die für andere jedoch nicht zugänglich sind).*
- *Wenn du oder andere Nutzer, die deine Inhalte und Informationen sehen können, eine Anwendung verwendet, werden deine Inhalte und Informationen an die Anwendung übermittelt. Wir verlangen von Anwendungen, dass sie deine Privatsphäre respektieren. Deine Übereinkunft mit der Anwendung bestimmt, wie diese die Inhalte und Informationen nutzen, speichern und übertragen kann. (Weitere Informationen zur Plattform findest du in unseren Datenverwendungsrichtlinien und auf der Plattformseite.)*
- *Wenn du die Einstellung „öffentlich“ bei der Veröffentlichung von Inhalten oder Informationen verwendest, können alle Personen, einschließlich solcher, die Facebook nicht verwenden, auf diese Informationen zugreifen, sie verwenden und sie mit dir (d. h. deinem Namen und Profilbild) assoziieren.“ [83]*

Bewerbung

Ein Risiko, dass erst mit diesen „neuen Medien“ entstanden ist, ist auch, dass man einen Job nicht bekommt aufgrund von „privaten“ Angelegenheiten, die den Arbeitgeber eigentlich gar nichts angehen. Doch ist es schon vorgekommen, dass Arbeitgeber aufgrund von Fotos einer Person schlussendlich doch nicht aufgenommen haben.

Laut einer Studie suchen Arbeitgeber im Internet nach persönlichen Informationen wie Hobbys, Interessen, Meinungsäußerungen oder auch private Vorlieben. Bei der Hälfte der Bewerber entscheiden diese Informationen, ob sie zu einem Bewerbungsgespräch eingeladen werden oder nicht. Bei 20 Prozent sind diese

Informationen sogar für die Endausscheidung relevant und 25 Prozent der Unternehmer meinen sogar, dass diese Informationen schon dazu geführt haben, dass die Bewerber dann aufgrund dieser Informationen nicht eingeladen oder abgelehnt wurden. Aufpassen sollte man speziell bei Partyfotos, diese werden von 46 Prozent der Unternehmen als negativ bewertet. Wobei zum Beispiel Informationen über Hobbys und Soziales Engagement wiederum positiv von den Unternehmen (56 Prozent) bewertet werden. Als besonders kritisch sehen es Unternehmen, wenn sich die Bewerber über die gegenwärtige oder vergangene Jobsituation abfällig äußern. (vgl. [84])

Nicht nur für einen zukünftigen Job kann es gefährlich sein, was man in sozialen Netzwerken postet bzw. hochladet, denn - wie die Arbeiterkammer berichtet - ist es auch schon vorgekommen, dass eine Arbeitnehmerin gekündigt wurde, da sie auf Facebook über ihren Vorgesetzten geschimpft hat. Dieser hat dies mitbekommen und sie entlassen. Also auch für solche Äußerung soziale Netzwerke nicht der richtige Ort. Auch wenn man seine „Privatsphären-Einstellungen“ beachtet, kann es immer sein, dass die Wortmeldungen „leichte Füße“ bekommen. Diese können auch von „Freunden“ weitergesagt oder weitergeleitet werden und schon sind diese Meldungen auf einmal „sichtbar“. (vgl. [85])

Kündigung

Bei der Bewerbung werden neue Mitarbeiter oft erst gar nicht eingestellt, aber viel schlimmer ist es noch, wenn man sich an seinem Arbeitsplatz sicher fühlt und dann plötzlich gekündigt wird, weil man negatives über den Arbeitsplatz in sozialen Netzwerken kundgetan hat. Es sind schon einige Fälle bekannt geworden und man muss sich daran gewöhnen, dass soziale Netzwerke schon lang nicht mehr Privat sind und auch Vorgesetzte gerne beobachten, was ihre Mitarbeiter so tun.

Beispiele:

Bei einer Mitarbeiterin des Schweizer Unternehmens „Nationale Suisse“ kam es zu einer Kündigung aufgrund ihrer Facebook-Aktivitäten. Die Mitarbeiterin meldete sich an diesem Tag krank, weil sie starke Migräne hatte und dadurch nicht am Bildschirm arbeiten könne. Am selben Tag bemerkten Mitarbeiter, dass sie in Facebook aktiv ist. Dies wurde den Vorgesetzten gemeldet und diese entschieden sich für eine Kündigung mit der Begründung „Wer im Internet aktiv sein kann, kann auch arbeiten.“ Die Mitarbeiterin fühlte sich benachteiligt und argumentierte, dass sie nur vom Handy aus in Facebook online war, doch dies interessierte die Firma wenig und die Kündigung wurde nicht zurückgezogen. (vgl. [86])

Ein weiterer Fall wurde vor einiger Zeit in England bekannt. Hier äußerte sich ein Apple-Store-Mitarbeiter negativ über Apple in Facebook. Auch bei diesem Fall erfuhr der Vorgesetzte von dem „Posting“ nur erfahren, weil es ihm durch einen weiteren Mitarbeiter weitergeleitet wurde. Doch dies hinderte den Vorgesetzten nicht, den Mitarbeiter wegen eines negativen Kommentars über Apple zu entlassen. Er ging sogar vor Gericht, bei welchem ihm zwar Recht zur freien Meinungsäußerung zugesprochen wurde, doch gleichzeitig wurde auch Apple Recht gegeben, da diese im Arbeitsvertrag geregelt haben, dass deren Mitarbeiter die Anstellung bei Apple im Internet nicht erwähnen dürfen und sich auch nicht negativ über die Marke äußern dürfen. Somit wurde der Kündigung vor Gericht Recht gegeben. (vgl. [87])

Weitere Beispiele siehe: [88], [89]

5.1. Verwundbarkeitsdarstellung

Dieses Kapitel beschäftigt sich mit der Berechnung der eigenen Verwundbarkeit in sozialen Netzwerken.

Tabelle 4 wurde entworfen um die Verwundbarkeit darzustellen, anhand der eingetragenen Informationen. Mittels Tabelle 4 und Tabelle 6 kann jeder seine eigene Verwundbarkeit berechnen indem man sich überlegt, welche Daten man in Facebook gespeichert hat und die dementsprechenden Zahlen der Tabelle 4 addiert. Hat man diese Summe so geht man zu Tabelle 6 und überlegt sich zu welcher Zielgruppe man gehört und multipliziert die zuvor ausgerechnete Summe mit der Zahl der zutreffenden Zielgruppe. Enthält die zutreffende Zielgruppe keine Zahl so nimmt man nur die Summe und schaut bei den „Verwundbarkeitsschlüsseln“ (Tabelle 8 bis Tabelle 16) nach, wie Verwundbar man, für die jeweiligen Angriffsszenarien bzw. Gefahren, ist.

Verwundbarkeitsdarstellung:

Informationen (Eingabefelder)	Identitätsdiebstahl	Cyber-Mobbing	Phishing	Spear-Phishing	Social Phishing	Verbreitung von Schadsoftware	Verkauf der Daten - Werbung	Bewerbung	Kündigung
Name	100	16		16	16		16	2	
Nutzername		16							
Geschlecht	2	2			2			2	
Adresse	16	2					16	2	
Geburtstag	100	2		16	16		16	2	
Sprache		2		2	2		2	2	
E-Mail Adresse	16	100	100	100	100	16	16	2	
Telefonnummern		100					16		
andere Nutzernamen (anderer Netzwerke)		16							
Netzwerke									
Verknüpfte Konten		16			16				
Profilbild		2						16	
Beziehungsstatus		2							
Familienmitglieder									
Interessiert an (Sexuelle Vorlieben)							2		
Arbeitgeber	100			2	2		16	16	16
Hochschule, Schule und Kurse				2			2		
Religion		2					2		2
Politische Einstellung		2		2			16	2	
Personen, die mich inspirieren							2		
Interessen und Aktivitäten (Hobbys, usw.)		2		2			16	2	
Musik, Bücher, Filme, Fernsehen, Spiele				2			16		
Lieblingssport-arten, -mannschaften, -sportler				2			16		
Fotos (Urlaubsfotos, Partybilder, usw.)		16			16			100	16
Aktueller Aufenthaltsort (GPS)		16					2		
Statusmeldungen (Neuigkeiten)						100		16	100
Anwendungen und Spiele						100	2		
Gruppen				16					
Pinnwandkommentare		100				100		16	100

Tabelle 4: Verwundbarkeitsmatrix

2	Diese Informationen können hilfreich sein, sind zum Teil aber aus anderen Informationen abzuleiten.
16	Diese Informationen sind hilfreich für den Angriff, sind aber keine Schlüsselkriterien
100	Schlüsselkriterium, ohne diese Informationen wird der Angriff erheblich erschwert

Tabelle 5: Beschreibung der Kritikalitätsstufen

Nachfolgend werden die Werte der Tabelle 4 beschrieben und erklärt wie diese zustande gekommen sind bzw. welche Bedeutung sie haben. Grundsätzlich beruhen alle Zahlen auf einer Umfrage, die in einem großen Unternehmen unter 8 Sicherheitsleuten gemacht wurde, dieses Ergebnis wird als Basis herangezogen. Mittels anderer Quellen und Studien wird das Ergebnis bestärkt oder auch korrigiert.

Laut der Umfrage sind zum Teil mehr Informationen notwendig, als sich in der Recherche herausstellte. Aufgrund der Recherche wird das Ergebnis zum Teil angepasst.

Identitätsdiebstahl

■ **Name, Geburtsdatum und Arbeitgeber:**

Diese drei Informationen sind für den Identitätsdiebstahl entscheidend, sind diese Informationen vorhanden, so kann der Identitätsdiebstahl erfolgreich durchgeführt werden. Mittels dieser Informationen kann der Angreifer Warenbetrug und ähnliches durchführen. Anhand folgender Beispiele bzw. Quellen wurde diese Erkenntnis getroffen bzw. wurde die Kritikalität bestimmt: [90], [91]

■ **Geschlecht:**

Diese Information erhält eine geringere Gewichtung, da man sehr oft anhand des Namens das Geschlecht eruieren kann.

■ **Adresse und E-Mail Adresse:**

Da die gestohlenen Identitäten sehr oft für Warenbetrug verwendet werden, kann eine gültige Adresse für die Angreifer sehr hilfreich sein, daher wird der Adresse eine entsprechende Kritikalität zugeteilt. Die Angreifer können somit die richtige Adresse des Opfers als Rechnungsadresse benutzen und als Lieferadresse eine andere angeben.

Da sehr oft in der heutigen Zeit Rechnungen per E-Mail verschickt werden, ist diese Information natürlich für den Angreifer auch sehr nützlich.

■ **alle anderen Informationen:**

Alle anderen Informationen sind für dieses Angriffsszenario weniger relevant bzw. können keiner Kritikalität zugeordnet werden, da es keine Datenbestände gibt.

Generell gilt bei Identitätsdiebstahl, umso mehr Informationen man über das Opfer hat, umso besser kann der Angreifer diese Identität für seine eigenen Zwecke verwenden. (vgl. [92]) Diese Meinung kommt auch bei der Umfrage zum Vorschein, da sehr viele Informationen als kritisch angesehen werden.

Identitätsdiebstahl ist noch immer sehr häufig finanziell motiviert oder dient der Diskreditierung einer Person. (vgl. [92])

Cyber-Mobbing

■ **E-Mail Adresse, Telefonnummern und Pinnwandkommentare:**

Mittels der E-Mail Adresse, der Handynummer oder über Pinnwandkommentare kann das Opfer sehr gezielt gemobbt werden. Da Mobbing eine Form der Beleidigung und der Bloßstellung ist, können diese Informationen sehr hilfreich für den Täter sein, da gerade über Pinnwandkommentare sehr schnell und einfach Gerüchte bzw. Bloßstellungen „in die Welt“ gesetzt werden können. Diese drei Informationen bekommen die höchste Kritikalität zugewiesen, denn mittels dieser Informationen können die Opfer quasi 24-Stunden „terrorisiert“ werden.

■ Name, Nutzername, andere Nutzernamen, Fotos, aktueller Aufenthaltsort:

Diese Informationen werden von den Befragten, als kritisch bezeichnet, da man hiermit den Angriff verstärken kann. Mittels den anderen Nutzernamen kann man seinen Cyber-Mobbing Angriff auf verschiedene soziale Netzwerke ausbreiten und somit die „Beleidigungen“ viel weiter verbreiten. Fotos können auch dazu benutzt, werden um das Opfer dementsprechend zu beleidigen oder bloßzustellen. Informationen des aktuellen Aufenthaltsortes kann der Täter dazu benutzen, das Opfer auf gewissen Orten „abzupassen“ bzw. Buch darüber zu führen, wo sich das Opfer aufhält.

■ Geschlecht, Adresse, Geburtstag, Sprache, Profilbild, Beziehungsstatus, Religion, politische Einstellung und Interessen und Aktivitäten:

Diese Informationen lassen sich zum Teil von anderen ableiten, wie zum Beispiel vom Namen das Geschlecht oder von der Adresse eventuell die Sprache abgeleitet werden kann. Alle weiteren Informationen können für den Mobbing-Angriff benutzt werden und auch hier gilt wieder, umso mehr Informationen der Täter hat, umso mehr kann er das Opfer angreifen. Da für diese Informationen keine Daten vorliegen und die befragten Personen diese Informationen mit „trifft teilweise zu“ bewertet haben, werden diese Kästchen mit der niedrigsten Stufe bewertet.

■ alle anderen Informationen

werden frei gelassen, da es kein fundiertes Datenmaterial gibt und die befragten Personen diese mit „trifft nicht zu“ bewertet haben.

Aktuelle Studien wie 2. Oö. Jugend-Medien-Studie (2011) [93] , EU Kids Online II - Report (2010) [94] , BITKOM Studie Jugend 2.0 [95], sowie die Statistiken in Kapitel 4.2.6 enthalten nur generelle Informationen über Cyber-Mobbing, wie zum Beispiel „Wie viele Jugendliche schon einmal über das Internet gemobbt wurden“, aus diesen Informationen kann keine Einschätzung der Kritikalität abgegeben werden. Daher wurde das Datenmaterial der Umfrage herangezogen. Weiters handelt es sich bei den Tätern meistens um „noch“ Freunde, Kollegen oder andere Bekannte – somit spielt es meistens keine Rolle, welche Informationen wichtiger sind oder nicht, denn diese Personen kennen ihre Opfer ohnehin sehr gut und wissen wo sie ansetzen müssen.

Phishing, Spear Phishing, Social Phishing

■ E-Mail Adresse:

Die E-Mail Adresse ist für alle drei Arten von Phishing der Schlüsselfaktor, hat man diese Information kann man gezielt Phishing E-Mails verschicken. Aufgrund der zahlreichen Recherchen ([96], [97], [98], sowie der Statistiken in Kapitel 4.3) über Phishingmails und lesen einiger Phishingmails wurde diese Kritikalität festgelegt.

■ Name:

Sowohl beim Spear- als auch beim Social Phishing werden die Opfer meist mit Name angesprochen, damit die E-Mails vertrauenswürdiger erscheinen. Daher wird bei diesen beiden Angriffsszenarien die dementsprechende Kritikalität vergeben.

■ Geburtstag und Gruppen

werden der gleichen Kritikalität zugeordnet, da sie für Social-Phishing und Spear-Phishing sehr hilfreich sein können. Beim Social-Phishing baut der Angreifer ein Vertrauen zum Opfer auf, um dieses Vertrauen für die Bekanntgabe von Bankdaten, Kreditkartendaten, Login-Daten, usw. zu missbrauchen. Auch hier gilt wieder, umso mehr Informationen der Angreifer über das Opfer hat, umso gezielter kann er die Mails verfassen.

Beim Spear-Phishing werden gezielte E-Mails an die Personen oder Gruppen geschickt, da die Angreifer ihre Opfer kennen, werden diese E-Mails gezielt auf sie zugeschnitten, damit die Opfer dadurch „unvorsichtiger“ werden. (vgl. [99])

■ **Fotos und verknüpfte Konten:**

Beim Social-Phishing können auch Fotos hilfreich sein, da in weiterer Folge die Daten für den Identitätsdiebstahl benutzt werden können.

Verknüpfte Konten: Ein Social-Phishing Angriff kann soweit führen, dass mittels der gefischten Daten von Person A danach auch Person B auch angegriffen wird, da sie online mit Person A verlinkt ist, und somit können die weiteren Mails oder „persönlichen Nachrichten“ über Person A vom Angreifer verschickt werden. Somit sind die verlinkten Konten (also „Freunde“) für den Angreifer sehr interessant und werden daher mit der dementsprechenden Kritikalität beurteilt.

■ **Geschlecht und Sprache:**

Diese Informationen können anhand des Namen bzw. der Adresse abgeleitet werden, denn wenn das Opfer zum Beispiel in England lebt, kann man daraus ableiten, dass diese Person Englisch spricht. Daher bekommen diese Informationen die niedrige Kritikalitätsstufe.

■ **Arbeitgeber:**

Da sehr oft auch Login-Daten von Firmen interessant für Angreifer interessant sind, ist es sehr hilfreich zu wissen, wo die angegriffene Person arbeitet.

■ **Hochschule, Schule und Kurse, politische Einstellung, Interessen und Aktivitäten, Musik, Bücher, Filme usw., und Lieblingssport-arten, -mannschaften, -sportler**

Diese Informationen sind laut Befragung hilfreich für den Angriff, daher erhalten sie die niedrigste Kritikalitätsstufe.

■ **alle anderen Informationen:**

Alle anderen Informationen sind für dieses Angriffsszenario weniger relevant bzw. können keiner Kritikalität zugeordnet werden, da es keine Datenbestände gibt.

Die Kritikalitätseinstufungen beruhen auf der durchgeführten Umfrage, der getätigten Recherche in Kapitel 4.3 und folgenden Quellen [92], [99], [100], [101], [102]

Verbreitung von Schadsoftware

■ **E-Mail Adresse:**

Da noch immer sehr viele Schadprogramme per E-Mail verschickt werden, ist diese Information für den Angreifer sehr hilfreich, denn Mithilfe einer gültigen E-Mail Adresse, kann er seine Schadsoftware gezielt verteilen. Schlüsselkriterium ist es allerdings keines mehr, da wie mehrere Artikel bzw. Reports berichten, die Zahl der Schadprogramme über soziale Netzwerke enorm ansteigt.

■ **Anwendungen und Spiele, Pinnwandkommentare, Statusmeldungen oder Facebook-Chat:**

Diese Funktionen der sozialen Netzwerke werden derzeit am häufigsten benutzt, um Schadsoftware zu verbreiten, wie Beispiele ([63], [64], [65], [103], [104], [105]) zeigen, daher werden sie als Schlüsselkriterien definiert, wobei diese nicht alle erfüllt sein müssen, um den Angriff erfolgreich durchzuführen, hier reicht schon eine der vier Funktionen.

Verkauf der Daten (Werbung)

■ **Name, Adresse, Geburtstag:**

Mittels Name und Adresse kann auch Werbung per Post gezielt verschickt werden bzw. können die User in Werbemails persönlich angesprochen werden. Mithilfe des Geburtstages (Altersbeschränkung) können gewisse Werbungen deaktiviert bzw. aktiviert werden.

■ **Sprache:**

Beruhend auf dieser Information kann gezielte Werbung in der entsprechenden Sprache geschaltet werden.

■ **E-Mail Adresse, Telefonnummern:**

Wenn diese Informationen bekannt sind, können auch per E-Mail oder Telefon Werbeangebote gesendet werden.

■ **Interessiert an (sexuelle Vorlieben), Arbeitgeber, Hochschule, Schule und Kurse, Religion, politische Einstellung, Personen, die mich inspirieren, Interessen und Aktivitäten (Hobbys, usw.), Musik, Bücher, Filme, Fernsehen, Spiele, Lieblingssport-arten, -mannschaften, -sportler, aktueller Aufenthaltsort (GPS), Anwendungen und Spiele:**

All diese Information können verwendet werden, um den Usern gezielte Werbung zu schicken.

Prinzipiell werden beim „Verkauf der Daten (Werbung)“ keine Schlüsselkriterien festgelegt, da es dazu kein Datenmaterial gibt, die Abstufung der Kritikalität beruht auf der Umfrage – mit dieser Abstufung wird dargestellt, welche Daten mehr oder weniger kritisch sind, wenn sie veröffentlicht werden. Generell ist es so, dass die Daten an sich nicht verkauft werden, sondern es den Firmen erlaubt wird, ihre „Tracking-Cookies“ einzusetzen bzw. verwenden dies die Firmen selbst auf ihren Websites auch. Es ist ganz leicht festzustellen, ob „Tracking-Cookies“ im Einsatz sind, indem man beobachtet, ob gezielte Werbung geschaltet wird, zum Beispiel sucht man vermehrt nach Pferdeartikeln, so werden gezielt Werbungen von Pferdesportartikeln bzw. Kaufhäusern geschaltet. Diese „Tracking-Cookies“ werden auch in Facebook verwendet, um das Nutzerverhalten der User zu dokumentieren. Aus diesem Grund können hier keine Schlüsselkriterien genannt werden, denn diese „Cookies“ sammeln alles was die User im Internet machen.

Folgende Quellen wurden verwendet: [106], [107], [82]

Bewerbung und Kündigung

■ **Name, Geschlecht, Adresse, Geburtstag, Sprache, E-Mail Adresse:**

Diese Informationen erhält der Arbeitgeber normalerweise sowieso, denn wenn man sich bei einem Arbeitgeber bewirbt, so muss man seine Daten bekanntgeben. Aus diesem Grund werden diese Informationen zwar aufgenommen, aber nur mit der geringsten Stufe bewertet.

■ **Profilbild, Arbeitgeber, politische Einstellung, Interessen und Aktivitäten (Hobbys, usw.):**

Gerade bei Neueinstellungen, sind die Arbeitgeber an privaten bzw. persönlichen Informationen interessiert, für diese Informationen eignen sich die sozialen Netzwerke hervorragend. Das Datenmaterial stammt aus der Umfrage und dem Artikel [84]

■ **Fotos (Urlaubsfotos, Partybilder, usw.):**

Laut einigen Artikeln und einer Studie ([84], [85]) kommen gerade bei Bewerbungen Partybilder nicht sehr gut an und es gibt auch zahlreiche Beispiele, dass aus diesem Grund Bewerber nicht aufgenommen wurden. Aus diesem Grund wird diese Information zu einem Schlüsselkriterium bei der Bewerbung.

■ Statusmeldungen (Neuigkeiten), Pinnwandkommentare:

Bei einer Kündigung sind Statusmeldungen und Pinnwandkommentare sehr gefährlich, denn es gibt schon zahlreiche Fälle ([86], [87] und weitere in Kapitel 5 genannte), dass aufgrund von „dummen“ Kommentaren in sozialen Netzwerken, Personen fristlos entlassen wurden, daher werden diese Informationen als Schlüsselkriterien festgelegt.

Die Gewichtungen kommen aufgrund der Umfrage und der bereits genannten Quellen zustande.

5.1.1. Zielgruppen

Tabelle 6 zeigt, welche Zielgruppen für welche Angriffsszenarien gefährdet sind.

		Kinder (9 – 16 Jahre)	Schüler (14 – 20 Jahre)	Jugendliche (16 – 18 Jahre)	Konsumenten mit Kreditkarte oder Online Banking	Facebook – User und andere soziale Netzwerk - User	Paypal-User	Ebay-User	Führungskräfte
Angriffsszenarien und Gefahren	Identitätsdiebstahl				5				
	Cyber-Mobbing	1	2	5					
	Phishing					2	5	2	
	Spear-Phishing					2	5	2	2
	Social-Phishing					2	5	2	
	Verbreitung von Schadsoftware					5			
	Verkauf der Daten (Werbung)					5			
	Bewerbung					5			
	Kündigung					5			

Tabelle 6: gefährdete Zielgruppen

1	Diese Zielgruppe ist selten betroffen.
2	Diese Zielgruppe ist häufig betroffen.
5	Diese Zielgruppe ist am stärksten betroffen.
leer gelassen	Für diese Zielgruppe gibt es kein Datenmaterial. Das bedeutet aber nicht, dass diese Zielgruppen davon gar nicht betroffen sind.

Tabelle 7: Beschreibung der Gewichtung der Gefährdung der Zielgruppen

Bei den Zielgruppen handelt es sich um Gruppen die zum Teil in Literatur bzw. Artikel und Studien genannt werden, da es auf diesem Gebiet sehr wenig gibt, wurden die immer wieder genannten hier als die „gefährdetet Zielgruppen“ angenommen. Von einer Vollständigkeit der Tabelle kann keine Rede sein, da keine umfangreichen Umfragen bzw. Studien durchgeführt wurden.

■ Identitätsdiebstahl

Für Zielgruppen von Identitätsdiebstahl gibt es keine fundierten Daten, da es eigentlich jeden betreffen kann, aber anhand folgender Artikel kann man sagen, dass Konsumenten bzw. Personen mit Kreditkarte und/oder Online-Banking stärker betroffen sind als andere Personen.

Quellen: [91], [90],

■ Cyber-Mobbing

Von Cyber-Mobbing sind am stärksten Jugendlichen (16-18 Jahre) betroffen, wie in mehreren Studien hervorgeht, Cyber-Mobbing beginnt schon bei Kindern (9 – 16 Jahre) und umso älter diese werden, umso stärker sind sie von Cyber-Mobbing betroffen. Aufgrund folgender Studien und Statistiken werden die Zielgruppen Kinder (9-16 Jahre), Schüler (14 – 20 Jahre) und Jugendliche (16 – 18 Jahre) als am gefährdetsten betrachtet, zu den anderen Zielgruppen gibt es kein Datenmaterial:

2. Oö. Jugend-Medien-Studie (2011) [93] ,

EU Kids Online II - Report (2010) [94] ,

BITKOM Studie Jugend 2.0 [95],

sowie aus den Statistiken von Kapitel 4.2.6

■ Phishing, Spear Phishing und Social Phishing

Aufgrund einiger Reports von Sicherheitsfirmen ([59], [108], [109]) sowie einiger Statistiken (Kapitel 4.3.3) werden Facebook-, Paypal- und Ebay-User als die am meisten gefährdetsten Zielgruppen betrachtet. Da keine getrennten Daten für Phishing, Social – und Spear-Phishing vorliegen, werden die Gewichtungen gleich gehalten. Außer für Spear-Phishing gibt es eine zusätzliche Zielgruppe nämlich Führungskräfte, diese welche vom BSI ([92]) genannt werden.

■ Verbreitung von Schadsoftware

Mittlerweile gibt es schon zahlreiche Schadprogramme, die über soziale Netzwerke verbreitet werden, daher wird hier die Zielgruppe „Facebook-User und andere soziale Netzwerke-User“ als die am häufigsten betroffene definiert.

Folgende Artikel veranlassten mich zu dieser Entscheidung: [103], [104], [110]

■ Verkauf der Daten (Werbung)

Da die “Tracking-Cookies” in so gut wie allen sozialen Netzwerken bzw. auch Konsumenten-Websites (wie zum Beispiel Amazon, Thalia, usw.) eingesetzt werden sind alle User der sozialen Netzwerke davon betroffen. Spezielles Datenmaterial dazu gibt es keines.

■ Bewerbung und Kündigung

Für Bewerbung und Kündigung wird die Zielgruppe der Facebook-User bzw. User der sozialen Netzwerke genannt, denn nur wenn man in diesen Netzwerken präsent ist, kann man mit solchen Vorfällen konfrontiert werden. Aufgrund der bereits mehrmals genannten Beispiele ([84], [85], [86], [87] und in Kapitel 5 genannte) wurden diese Schlüsse gezogen.

5.1.2. Verwundbarkeitsschlüsseln:

Die Verwundbarkeitsschlüsseln wurden so berechnet, dass wenn die Schlüsselkriterien nicht vorhanden sind, dann befindet man sich in einer niedrigen bzw. mittleren Verwundbarkeitsklasse. Umso mehr Schlüsselkriterien vorhanden sind, umso höher wird die Verwundbarkeitsklasse bzw. muss man dann auch in der „gefährdeten“ Zielgruppe sein.

Für jedes Angriffsszenario bzw. für jede Gefahr gibt es einen eigenen Verwundbarkeitsschlüssel, da sich diese voneinander so stark unterscheiden, dass man die Verwundbarkeit nicht verallgemeinern kann.

Allgemein gehört gesagt, dass die Informationen an sich nicht schlecht sind, sondern es kommt immer darauf an wie und was der User hineinschreibt, denn zum Beispiel sind nicht alle Statusmeldungen gefährlich. Gefährlich werden sie dann, wenn der User Kommentare abgibt die man so besser nicht sagen bzw. schreiben würde.

Identitätsdiebstahl	
901 und höher	sehr hoch
501 – 900	hoch
35 – 500	mittel
0 – 34	niedrig

Tabelle 8: Verwundbarkeitsschlüssel Identitätsdiebstahl

Cyber-Mobbing	
501 und höher	sehr hoch
301 – 500	hoch
101 – 300	mittel
0 – 100	niedrig

Tabelle 9: Verwundbarkeitsschlüssel Cyber - Mobbing

Fehlt beim Phishing das Schlüsselkriterium, wird die Verwundbarkeit automatisch niedrig.

Phishing	
201 und höher	sehr hoch
101 – 200	hoch
1 - 100	mittel
0	niedrig

Tabelle 10: Verwundbarkeitsschlüssel Phishing

Fehlt beim Spear - Phishing das Schlüsselkriterium wird, die Verwundbarkeit automatisch niedrig.

Spear - Phishing	
401 und höher	sehr hoch
163 – 400	hoch
101 – 162	mittel
0 - 100	niedrig

Tabelle 11: Verwundbarkeitsschlüssel Spear Phishing

Fehlt beim Social - Phishing das Schlüsselkriterium, wird die Verwundbarkeit automatisch niedrig.

Social - Phishing	
201 und höher	sehr hoch
141 – 200	hoch
71 – 140	mittel
0 - 70	niedrig

Tabelle 12: Verwundbarkeitsschlüssel Social Phishing

Verbreitung von Schadsoftware	
300 und höher	sehr hoch
200 – 299	hoch
100 – 199	mittel
0 - 99	niedrig

Tabelle 13: Verwundbarkeitsschlüssel Schadsoftware

Verkauf der Daten – Werbung	
173 und höher	sehr hoch
0 - 172	hoch

Tabelle 14: Verwundbarkeitsschlüssel Werbung

Fehlt bei der Bewerbung das Schlüsselkriterium, wird die Verwundbarkeit automatisch um eine Stufe niedriger.

Bewerbung	
500 und höher	sehr hoch
101 – 499	hoch
0 - 100	mittel

Tabelle 15: Verwundbarkeitsschlüssel Bewerbung

Kündigung	
201 und höher	sehr hoch
35 – 200	hoch
0 - 34	mittel

Tabelle 16: Verwundbarkeitsschlüssel Kündigung

5.2. Beispiele für eine Verwundbarkeitsberechnung

Beispiel 1: Person, die sehr viele Daten in Facebook eingetragen hat

Eine 17-jährige Person (Student/in) hat folgende Daten online in Facebook eingetragen. Weiters besitzt diese Person Online-Banking und ist in anderen sozialen Netzwerken auch registriert. Die Daten sind zwar nur für Freunde sichtbar, aber ein Hacker schafft es „Freund“ zu werden und kann somit alle Daten sehen. Folgende Verwundbarkeit ergibt sich für diese Person für die angeführten Angriffsszenarien und Gefahren.

Alle Informationen, die nicht eingetragen sind wurden herausgenommen, zu sehen sind nur die eingetragenen.

Informationen (Eingabefelder)	Identitätsdiebstahl	Cyber-Mobbing	Phishing	Spear-Phishing	Social Phishing	Verbreitung von Schadsoftware	Verkauf der Daten - Werbung	Bewerbung	Kündigung
Name	100	16		16	16		16	2	
Nutzername		16							
Geschlecht	2	2			2			2	
Geburtstag	100	2		16	16		16	2	
Sprache		2		2	2		2	2	
E-Mail Adresse	16	100	100	100	100	16	16	2	
andere Nutzernamen (anderer Netzwerke)		16							
Verknüpfte Konten		16			16				
Profilbild		2						16	
Beziehungsstatus		2							
Interessiert an (Sexuelle Vorlieben)							2		
Hochschule, Schule und Kurse				2			2		
Interessen und Aktivitäten (Hobbys, usw.)		2		2			16	2	
Musik, Bücher, Filme, Fernsehen, Spiele				2			16		
Lieblingssport-arten, -mannschaften, -sportler				2			16		
Fotos (Urlaubsfotos, Partybilder, usw.)		16			16			100	16
Statusmeldungen (Neuigkeiten)						100		16	100
Anwendungen und Spiele						100	2		
Pinnwandkommentare		100				100		16	100
Summe	218	292	100	142	152	316	104	160	216
Zielgruppenfaktor	5	5	2	2	2	5	5	5	?
Verwundbarkeit	sehr hoch	sehr hoch	sehr hoch	hoch	sehr hoch	sehr hoch	sehr hoch	sehr hoch	

Tabelle 17: Beispiel einer Verwundbarkeitsberechnung (viele Daten)

Für diese Person kommt für alle Angriffsszenarien bzw. Gefahren eine hohe oder sehr hohe Verwundbarkeit heraus. Aufgrund ihres Alters und Berufes (Student/in) wird in der Spalte Kündigung keine Verwundbarkeit errechnet. Geht diese Person diese Risiken ein, so kann sie diese Informationen weiterhin in Facebook speichern. Sollte sie doch weniger verwundbar sein wollen, so müsste sie Maßnahmen setzen.

Beispiel 2: Person, die wenige Daten in Facebook eingetragen hat

Eine Person mittleren Alters (Mitarbeiter/in in einem großen Unternehmen) hat folgende Daten online in Facebook eingetragen. Weiters besitzt diese Person Online Banking, Kreditkarte, Ebay-Konto und ein Paypal-Konto. Die Daten sind zwar nur für „Freunde“ sichtbar, aber ein Hacker schafft es „Freund“ zu werden und kann somit alle Daten sehen. Folgende Verwundbarkeit ergibt sich für diese Person für die angeführten Angriffsszenarien und Gefahren.

Alle Informationen, die nicht eingetragen sind, wurden herausgenommen, zu sehen sind nur die eingetragenen.

Informationen (Eingabefelder)	Identitätsdiebstahl	Cyber-Mobbing	Phishing	Spear-Phishing	Social Phishing	Verbreitung von Schadsoftware	Verkauf der Daten - Werbung	Bewerbung	Kündigung
Name	100	16		16	16		16	2	
Nutzername		16							
Sprache		2		2	2		2	2	
Verknüpfte Konten		16			16				
Profilbild		2						16	
Beziehungsstatus		2							
Arbeitgeber	100			2	2		16	16	16
Interessen und Aktivitäten (Hobbys, usw.)		2		2			16	2	
Statusmeldungen (Neuigkeiten)						100		16	100
Gruppen				16					
Pinnwandkommentare		100				100		16	100
Summe	200	156	0	38	36	200	50	70	216
Zielgruppenfaktor	5		5	5	5	5	5	5	5
Verwundbarkeit	sehr hoch	niedrig	niedrig	niedrig	niedrig	sehr hoch	sehr hoch	mittel	sehr hoch

Tabelle 18: Beispiel einer Verwundbarkeitsberechnung (wenige Daten)

Wie man bei diesem Beispiel sieht wurde die Verwundbarkeit bei einigen Angriffsszenarien niedrig, aber trotzdem diese Person sehr viel weniger Informationen in Facebook gespeichert hat, bleiben einige Gefahren bzw. Angriffsszenarien bestehen.

6. Maßnahmen und Empfehlungen

Dieses Kapitel soll Lösungsvorschläge liefern, damit man soziale Netzwerke sicherer machen kann bzw. soll es die Nutzer aufmerksam machen, wie man sich besser schützen kann. Weiters tragen diese Maßnahmen und Empfehlungen dazu bei, dass man Risiken wie Identitätsdiebstahl, Phishing, Cyber-Mobbing usw. verringern kann.

6.1. Die wichtigsten Regeln für die Benutzung von sozialen Netzwerken

Mittlerweile gibt es schon einige Internetseiten, die sich mit der Sicherheit des Internets bzw. von sozialen Netzwerken beschäftigen, doch leider stellt sich immer wieder heraus, dass die Nutzer diese Seiten nicht kennen oder sie einfach nicht beachten. Außerdem finden schon lang bekannte Angriffsszenarien, wie Phishing und Co. leider noch immer sehr viele Opfer. Aus diesem Grund wird in dieser Diplomarbeit darauf eingegangen, was man beachten sollte, um sozialen Netzwerke sicher nutzen zu können.

Persönliche Daten geheim halten

Mit der Entstehung von sozialen Netzwerken wird auf das Geheimhalten persönlicher Daten leider sehr oft vergessen. Man sollte aber beachten, dass das Internet nicht vergisst und auch „geschützte“ Daten nicht immer geschützt sind und somit in falsche Hände geraten können.

Beim Veröffentlichen von privaten Daten sollte immer kritisch überlegt werden, welche der persönlichen Daten öffentlich gemacht werden wollen. Außerdem sollte bedacht werden, dass zum Beispiel Arbeitgeber über Bewerber recherchieren und auch Versicherungen und Vermieter an Hintergrundinformationen interessiert sein könnten. (vgl. [111])

Auswahl der Kontakthanfragen

Man sollte nicht „blauäugig“ jede Kontakthanfrage annehmen, denn auch Kriminelle senden Kontakthanfragen und können dann auf Daten zugreifen, die sie besser nicht wissen sollten. Zum Beispiel könnte man ausspioniert werden, wann die Wohnung leer steht und wann nicht. Daher immer kritisch prüfen, ob man diese Person in die Freundesliste aufnehmen will, sollte man sie aus dem „realen“ Leben nicht kennen. (vgl. [111] und [112], Seite 22)

Fotos veröffentlichen

Es sollte darauf geachtet werden welche Fotos in sozialen Netzwerken online gestellt werden, auch wenn sie nur für Freunde sichtbar sind, können sie durch verschicken an Personen gelangen, für die sie nicht bestimmt sind. Man sollte auf keinen Fall Fotos veröffentlichen, die einem später einmal peinlich sein oder zu einem Nachteil verwendet werden könnten. (vgl. [112], Seite 22)

Links in Kommentaren und auf der Pinnwand

Wie schon öfter in dieser Diplomarbeit erwähnt, werden soziale Netzwerke immer häufiger zur Verbreitung von Schadsoftware und für Phishing benutzt. Daher sollte man auch hier darauf achten, auf welche Links man klickt und nicht wahllos allen Links vertrauen, auch wenn sie scheinbar von Freunden empfohlen werden. Eine sehr beliebte Art sind die so genannten Kurz-URLs, bei denen der Nutzer die eigentliche Zieladresse nicht erkennt.

Mittels dieser Links wird man meistens auf gefälschte Seiten geschickt, die danach Benutzername und Passwort verlangen und diese Informationen werden sofort an die Betrüger weitergeleitet. (vgl. [111])

Sicherheitsregeln für Twitter (vgl. [113])

- In Tweet-Nachrichten sollte man nie persönliche Daten wie Name, Adresse, Telefonnummer oder E-Mail Adresse bekannt geben.
- Zugangsdaten sollten immer geheim gehalten werden, auch vor den besten Freunden.
- Man sollte nie zu viele persönliche Daten in Online Accounts speichern. Weniger ist mehr!
- Auch hier sollte man keine „merkwürdigen“ Links anklicken, auch wenn sie von Freunden stammen.
- Beim Verfassen von „Tweets“ sollte man immer daran denken, dass andere Personen wie Klassenkollegen, Arbeitskollegen, Arbeitgeber, Lehrer, Eltern usw. mitlesen könnten. Man sollte über Twitter nur das schreiben, was man auch im „echten Leben“ öffentlich sagen würde.

Allgemeine Regeln für soziale Netzwerke:

Damit nicht Kommentare oder Informationen in soziale Netzwerke gelangen, die später bereut werden, sollte man folgendes beachten: (vgl. [114])

- Man sollte unbedingt darauf achten, was man in sozialen Netzwerken postet, denn die Anbieter speichern diese Einträge sehr lange und aus diesem Grund gehören plötzliche Gefühlsausbrüche nicht auf Pinnwände oder ähnliches in sozialen Netzwerken.
- Ansonsten gelten eigentlich die Verhaltensregeln aus dem „normalen“ Leben, denn Beschimpfungen, Mobbing oder ähnliches sind auch in sozialen Netzwerken unerwünscht.
- Wie schon mehrmals erwähnt, sollte man speziell in sozialen Netzwerken sparsam mit persönlichen Daten umgehen, denn im Zusammenhang können diese unerwünschte Informationen verraten. Zum Beispiel: Die aktuelle Wohnadresse und die Angabe des nächsten Urlaubszeitraums wirkt wie eine Einladung für Diebe.

6.2. Technische Maßnahmen

In diesem Unterkapitel werden technische Maßnahmen vorgeschlagen, welche die User von sozialen Netzwerken vor den Angriffsszenarien schützen sollen. Hier handelt es sich zum Teil um Maßnahmen die sofort umgesetzt werden können, wie zum Beispiel den Virenschanner installieren, aber es werden auch Maßnahmen vorgeschlagen, welche erst in wissenschaftlicher Erarbeitung sind.

Virenschanner in Facebook installieren

Von Symantec gibt es bereits ein gratis Tool „Norton Safeweb for Facebook“ welches vor gefährlichen Links auf der Pinnwand warnt. Dieses Tool kann kostenlos unter <http://apps.facebook.com/nortonsafeweb/> genutzt werden und zeigt dem Nutzer an, ob eventuell die Links auf seiner Pinnwand Schadcode enthalten. (vgl. [115])

Auch „BitDefender safego“ ist ein kostenloses Tool, welches die Links und die Privatsphäreneinstellungen prüft und Warnungen abgibt. Hat man dieses Tool installiert, so schützt es den Account rund um die Uhr, auch wenn man nicht online ist. Erkennt dieses Tool einen Schadcode oder einen Link, so postet es automatisch zu diesem Kommentar zum Beispiel auf der Pinnwand, dass dieser Link Schadcode enthält. Somit sind auch die Freunde des Nutzers sofort informiert. Weiters kann man danach diesen Kommentar mit dem „x“ löschen. Bei den Privatsphären-Einstellungen warnt das Tool vor Schwachstellen. (vgl. [116])

Blocking Tool installieren

Es gibt verschiedene Möglichkeiten, um sich vor dem Tracking zu schützen bzw. dieses unter Kontrolle zu halten. Eine sehr effiziente Möglichkeit ist es ein sogenanntes „Blocking Tool“ zu installieren, dabei handelt es sich um Browser Plugins, die eine Liste von URLs haben, die Tracking durchführen möchten. Bei Aktivierung eines solchen Blockers kommuniziert der Rechner dann mit diesen URLs nicht mehr, was unter anderem auch die Funktionalität einschränken kann. Einzelne URLs können von dieser „Sperre“ ausgenommen werden, da sonst Funktionalitäten, wie das Einladen anderer zu sozialer Netzwerke oder zu Spielen in sozialen Netzwerken, nicht mehr funktionieren. (vgl. [82])

Beispiele für solche Tools sind Ghostery und Adblock Plus (ADP).

FaceCloak

FaceCloak ist eine Software welche sicherstellt, dass private Informationen auch wirklich privat bleiben. Diese Software soll ein Plug-in für Firefox werden und die Verwendung soll sehr einfach sein. Sie erlaubt es den Nutzern, Informationen zu kennzeichnen (mit einem doppelten „@“), die verschlüsselt werden sollen und nur Freunden zugänglich gemacht werden, die den entsprechenden Schlüssel haben. Das heißt die Software arbeitet mit einem geheimen Zugangsschlüssel und mit einem weiteren Schlüssel für die Freunde. Die Informationen die verschlüsselt werden, werden als zusätzliche Sicherheitsmaßnahme auf von Facebook getrennten Servers gespeichert.

Momentan konzentrieren sich Hengartner und seine Kollegen ausschließlich auf Facebook, da es das populärste ist, später kann es aber auch mit anderen sozialen Netzwerken funktionieren. (vgl. [117])

Die detaillierte Funktionsweise wird im Paper von Hengartner und seine Kollegen beschrieben.

Proxy-basierter Echtzeit-Schutz-Mechanismus für Social Networking Sites

Proxy-basierter Echtzeit-Schutz-Mechanismus für Social Networking Sites ist ein Konzeptvorschlag um ein Echtzeit Security Scanning Modul in Soziale Netzwerke einbauen zu können. Abbildung 48: Infrastruktur - Proxy-basierter Echtzeit-Schutz-Mechanismus für Social Networking Sites Abbildung 48 zeigt die Infrastruktur, diese nutzt einen Proxy um die Sicherheits-Scanning Dienstleistungen erbringen zu können.

Das Scanning Ergebnis wird in einer „schwarzen“ Liste gespeichert, falls die Seite bedrohlich ist. Diese Liste wird benutzt um den User das nächste Mal zu warnen, wenn er auf solche Website surfen will. (vgl. [118])

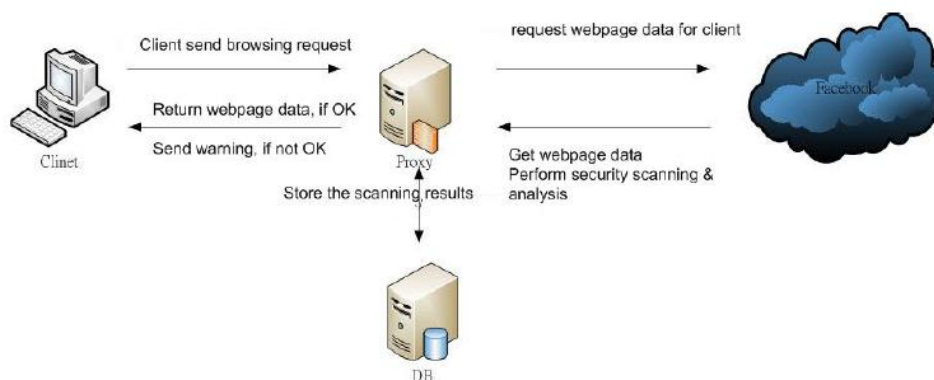


Abbildung 48: Infrastruktur - Proxy-basierter Echtzeit-Schutz-Mechanismus für Social Networking Sites [118]

Abbildung 49 stellt das gesamte Verfahren dar, es besteht aus fünf Schritten: (vgl. [118])

1. Benutzer nutzt seinen eigenen Browser um die gewünschte Seite anzufurten.
2. Statt direkt die Seite anzufurten, leitet der Browser die Anfrage an den Proxy um.
3. Proxy sendet die URL zum Online-Homepage-Analyse-Service, dieses Service ladet die Website herunter um den Scan durchzufuhren.
4. Das Ergebnis wird in die Datenbank aufgenommen, sollte es sich um eine bedrohliche Website handeln so wird sie in die „Blacklist“ aufgenommen und es wird eine Warnung an den User gesendet. Anderenfalls wird der User auf die Website umgeleitet.
5. Jeder User der danach diese Website besuchen will, bekommt automatisch eine Warnmeldung anhand der „Blacklist“.

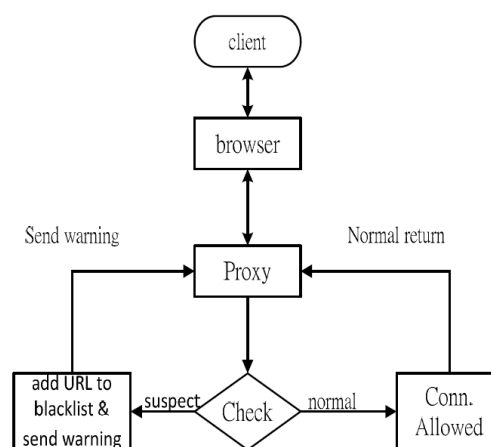


Abbildung 49: Skizze des gesamten Verfahrens [118]

6.3. Vorschläge an Facebook (Maßnahmen seitens Facebook)

Im folgenden Unterkapitel werden Vorschläge gemacht, wie man Facebook sicherer bzw. für die Benutzer einfacher machen könnte.

Profilarten

Ein Vorschlag wäre, Profilarten einzuführen. Man könnte vier bis fünf verschiedene Profilarten entwerfen und diese können von den Usern ausgewählt werden, somit würden auch die User die sich momentan mit den Privatsphäreneinstellungen gar nicht auseinandersetzt haben, die Chance haben sich mit einem Standardprofil besser zu schützen. Für die „fortgeschrittenen“ User könnte ein Userprofil „Benutzerdefiniert“ vergeben werden, hier hätten dann auch diese User die Möglichkeit, die Einstellungen zu treffen so wie sie es wollen.

Automatisiertes Löschen von Kommentaren

Ein weiterer Vorschlag wäre die Einführung einer automatisierten Löschung von Kommentaren. Zurzeit haben Facebook-User die Möglichkeit, Kommentare einzeln zu löschen, da dies ein sehr großer administrativer Aufwand (da sich mit zunehmender Zeit sehr viele Kommentare ansammeln können) ist, alle oder sehr viele Kommentare zu löschen, wäre der Vorschlag, eine Funktion einzuführen, um Kommentare auch gesammelt löschen zu können.

Standardeinstellungen überarbeiten

Ein weiterer Sicherheitsfaktor wäre, wenn standardmäßig alle Einstellungen von „öffentlich“ auf „nur Ich“ geändert werden würden. Somit hätten die User Zeit sich mit den Profileinstellungen auseinanderzusetzen, und aus Sicherheitssicht ist es immer besser, wenn zuerst einmal die „Facebook-Freunde“ gar nichts sehen dürfen, als „alle Facebook-User“ dürfen alles sehen.

6.4. Empfehlungen

Hier werden nochmals die wichtigsten Einstellungen für das sichere Nutzen sozialer Netzwerke zusammengefasst.

Freundeslisten benutzen

Mithilfe der Freundeslisten lassen sich „Facebook-Freunde“ in Gruppen einteilen und diesen Listen kann jeder Nutzer eigene Berechtigungen vergeben. Es gibt drei Arten solcher Listen: „Benutzerdefinierte Listen“, „Intelligente Listen“ und „Standard-Listen“. (vgl. [119], Seite 4)

„Benutzerdefinierte Listen“ sind Listen, die jeder User selbst erstellen und benennen kann, dieser Liste können anschließend „Freunde“ aus der Gesamtliste hinzugefügt werden. Diese Liste ist nur innerhalb des eigenen Benutzerkontos sichtbar und somit für andere Facebook-User nicht zu sehen. (vgl. [119], Seite 5)

„Intelligente Listen“ sind Listen, die von Facebook automatisch erstellt werden. Diese Listen werden auf Grundlage der eingegebenen Daten (Ausbildung und Beruf, Familie, Wohnort, Hochschule) erstellt. Die Kontakte, die eine bestimmte Kennzeichnung, wie zum Beispiel Familienmitglied, besitzen, werden automatisch in diese Listen aufgenommen. (vgl. [119], Seite 7)

„Standard-Listen“ sind Listen, die ebenfalls von Facebook automatisch erstellt werden, sie werden aber im Gegensatz zu den intelligenten Listen nicht aufgrund der Angaben im Profil erstellt, sondern alle Facebook-User verfügen über dieselben „Standard-Listen“. Es gibt drei „Standard-Listen“, „Enge Freunde“, „Bekannte“, und „Eingeschränkt“. (vgl. [119], Seite 10)

„Die Standard-Liste „Eingeschränkt“ bietet sich dazu an, „Freunde“ einzuordnen, die die eigenen Statusmeldungen nicht oder nur eingeschränkt erhalten sollen. Personen, die man hier einfügt, bekommen eigene Meldungen lediglich dann auf ihrer Pinnwand angezeigt, wenn sie „öffentlich“ verfasst, d.h. für alle Facebook-„Freunde“ freigegeben werden. Wählt der Nutzer also z .B. beim Verfassen neuer Statusmeldungen die Einstellung „Freunde“ bleiben die entsprechenden Beiträge vor den Mitgliedern der Liste „Eingeschränkt“ immer verborgen, obwohl sie zu den eigenen Facebook- „Freunden“ zählen.“ ([119], Seite 10)

Diese Listen sollten unbedingt dazu verwendet werden, die Freunde zu gruppieren, denn nicht alle Facebook-Freunde sollten alle Inhalte lesen dürfen. Detaillierte Beschreibungen zu diesem Thema findet man unter: <http://www.klicksafe.de/materialien/> - Modul Freundeslisten

Standardeinstellungen ändern

Standardmäßig werden die meisten der möglichen anzugebenden Profildaten „öffentlich“ freigegeben, das heißt jeder, der das Facebook-Profil besucht, kann auch die eingegebenen Daten sehen. Prinzipiell sollten die

Profilaten nie öffentlich gemacht werden, da hierdurch die Gefahr unerwünschte Kontakte, Werbung oder des Datenmissbrauches stark erhöht wird. Da aber auch nicht alle Facebook-Freunde auch „reelle“ Freunde sind, sollte auch hier kritisch hinterfragt werden, ob man wirklich allen Freunden den Einblick in seine Kontaktdaten bzw. persönlichen Informationen gibt. (vgl. [120], Seite 5)

Folgende Einstellungsoptionen stehen im Facebook-Profil zur Verfügung: (vgl. [120], Seite 6 und 7)

■ Einstellung „öffentlich“:

Jeder andere Facebook-Nutzer kann die Profilangaben sehen, wenn dieser das Profil besucht.

■ Einstellung „Freunde“:

Alle Personen, die in der persönlichen „Freundesliste“ sind, können die Profilangaben sehen, wenn das Facebook-Profil besucht wird.

■ Einstellung „Freunde ohne Bekannte“:

Alle „Facebook-Freunde“ können die Profilangaben sehen, außer die „Freunde“, die in die Liste „Eingeschränkt“ hinzugefügt wurden.

■ Einstellung „nur ich“:

Angaben, die mit dieser Einstellung versehen wurden, können nur vom Nutzer selbst gesehen werden.

■ Einstellung „Benutzerdefiniert“:

■ Einstellung „Freunde von Freunde“

Bei dieser Einstellung können auch alle „Facebook-Freunde“ der „Freunde“ die Profilangaben sehen.

■ Einstellung „Bestimmte Personen oder Listen“

Hier kann man selbst festlegen, welche Personen bzw. Freundeslisten die Angaben sehen dürfen.

Aufgrund der Vielfalt der Einstellungsmöglichkeiten sollte man sich mit dem Thema Einstellungen im Facebook-Profil und auch Privatsphäreneinstellungen sehr genau auseinandersetzen. Gute Materialien und Leitfäden dazu findet man unter: <http://www.klicksafe.de/materialien/>

Empfehlungen zusammengefasst:

- Die Einstellung „Freunde von Freunde“ sollte man meiden, da hier sehr schwer kontrolliert werden kann, welche Personen auf das eigene Profil Zugriff haben.
- Bei Freundschaftsanfragen, bei denen man die Personen aus dem „realen Leben“ nicht kennt, sollte man immer zuerst recherchieren und dann die Freundschaftsanfrage annehmen oder ablehnen. Freundschaftsanfragen sollte man nie „einfach nur so“ annehmen, denn auch Kriminelle senden Freundschaftsanfragen.
- Man sollte sich über „bekannte“ Angriffe über soziale Netzwerke im Internet informieren und aufmerksam bei Kommentaren und persönlichen Nachrichten sein.
- Privatsphäreneinstellungen und Profileinstellungen sollten eher zu „streng“ als zu „offen“ eingestellt werden.
- Freundeslisten sollte man von Beginn an erstellen, denn im Nachhinein bedeutet es einen extremen administrativen Aufwand.
- Felder wie politische Einstellung, Religion, E-Mail Adresse, Telefonnummern usw. sollten erst gar nicht ausgefüllt werden, denn dadurch verringert man die Angriffsmöglichkeiten.

- Die Pinnwand ist wie ein „öffentliches“ Tagebuch, daher sollte man damit auch sehr vorsichtig umgehen und nur Kommentare auf die Pinnwand schreiben, die man auch fremden Personen sagen würde. Auch wenn man die Pinnwand nur für Freunde freigeschalten hat, haben schon einige Beispiele (siehe Beispiele in Kapitel 5) bewiesen, dass sie trotzdem an Personen gelangt sind, für die diese Informationen nicht bestimmt waren.
- Neuerungen bezüglich Privatsphäreneinstellungen usw. sollten immer sorgfältig mitverfolgt werden, damit dementsprechend darauf reagiert und die Einstellungen angepasst werden können.

7. Schlussfolgerungen und Ausblick

Wir befinden uns im Zeitalter der virtuellen Gemeinschaften. Es gibt immer mehr Internetplattformen, auf denen sich Menschen aus aller Welt treffen und über Hobbys, gemeinsame Interessen und vieles mehr kommunizieren. Online-Communities oder auch Social Networks (Soziale Netzwerke) faszinieren längst nicht nur Erwachsene, denn die meisten Nutzer dieser Communities sind zwischen 13 und 29 Jahre. (vgl. [121] und [16])

Online-Communities oder auch Social Networks genannt, gehören zum Web 2.0. Dieser Begriff ist zum Schlagwort für eine neue, individuelle Mediennutzung geworden. In unserem Zeitalter kann jeder selbst Inhalte im Internet veröffentlichen, wie zum Beispiel Videos auf YouTube veröffentlichen, Social Network-Profilen erstellen oder einfach einen Eintrag im Online-Lexikon (Wiki) verfassen. All das sind Anwendungen, welche dank technischer Vereinfachung, heute sehr einfach sind und Menschen begeistern. (vgl. [121])

Mittlerweile gibt es Facebook seit 8 Jahren und die Begeisterung ist ungebremsbar, denn zurzeit hat Facebook circa 800 Millionen User weltweit. (vgl. [122])

Man muss allerdings bedenken, dass wir nun die erste Generation dieser Nutzer sind und speziell die Jugendlichen nutzen diese sozialen Netzwerke sehr intensiv. Mit zunehmendem Alter werden wir erst sehen, wie sich das Nutzerverhalten ändert bzw. den negativen und positiven Ereignissen anpasst.

Weiters muss auch erwähnt werden, dass es Social Engineering immer schon gegeben hat und mit den sozialen Netzwerken, es den Angreifern um einiges leichter gemacht wird, da diese Daten nun alle online verfügbar sind und nur Wege gefunden werden müssen um an die Daten heranzukommen.

Zusammenfassend kann man sagen, dass soziale Netzwerke eine geniale Erfindung sind und man die Nutzer auch davon nicht abbringen kann, diese zu nutzen. Dennoch muss man versuchen, das Sicherheitsbewusstsein zu stärken und vor allem die Nutzer auf Gefahren in diesen Netzwerken aufmerksam zu machen. Generell gilt, man sollte die sozialen Netzwerke mit „Hirn“ bedienen und keine momentanen Gefühlsausbrüche veröffentlichen. Weiteres sollte man sich im Vorhinein überlegen, was man veröffentlichen will, denn „Privat“ war das Internet nie und wird es auch nie sein.

Hier wird noch einmal kurz erläutert was in dieser Arbeit gemacht wurde. Zu Beginn wurden die Begrifflichkeiten erklärt und versucht auch zum Teil mit Statistiken zu hinterlegen. Danach wurde die Literaturrecherche begonnen um herauszufinden, wie man Daten überhaupt sammeln kann und welche Angriffsszenarien für Social Engineering in sozialen Netzwerken überhaupt in Frage kommen. Die Angriffsszenarien wurden anhand der momentanen Situation ausgewählt und diese wurden auch mit Statistiken unterstrichen.

Ein weiterer wichtiger Punkt in der Recherche waren die Tools für die automatisierte Informationsgewinnung. Hierbei handelte es sich um eine reine Literaturrecherche.

Der nächste Teil umfasst schon die Ergebnisse dieser Arbeit. Hierbei handelt es sich um die Verwundbarkeitsdarstellung die anhand der Literaturrecherche aufgebaut wurde. Herausgekommen ist eine „Selbstberechnung“ der eigenen Verwundbarkeit. Mit diesen Tabellen kann sich jeder die eigene Verwundbarkeit ausrechnen und danach entsprechende Maßnahmen setzen. Wo wir auch schon beim nächsten Ergebnis der Arbeit wären, nämlich der Maßnahmen und Empfehlungen. In diesem Kapitel wurden Maßnahmen und Empfehlungen abgegeben um die sozialen Netzwerke so sicher wie möglich zu machen bzw.

um die User darauf aufmerksam zu machen, dass sie mit ihren Informationen und Daten behutsam umgehen sollen und nicht jeden „Gefühlsausbruch“ in diesen Netzwerken veröffentlichen sollen.

Das Hauptergebnis nämlich die Verwundbarkeitsdarstellung war ein erster Versuch, den Usern grafisch und mit Zahlen zu zeigen, wie Verwundbar ihre Online - Profile sind. Es wäre schön wenn sich diese Darstellung viele User „zu Herzen“ nehmen würden und anfangen kritischer mit ihren Informationen umzugehen.

Da momentan keine exakten Daten zu all den Untersuchten Werten bestehen, konnte teilweise keine gesicherte Aussage getroffen werden, gerade bei den Zielgruppen und bei der Verwundbarkeitsdarstellung. Weiters ist diese Arbeit in keinsten Weise vollständig, sowohl bei der Datensammlung, bei den automatisierten Tools als auch bei den Angriffsszenarien gibt es keine Vollständigkeit, da sich diese fast täglich ändern können.

Um die Verwundbarkeitsdarstellung professioneller auszuführen zu können wäre der nächste Schritt eine umfassende Studie dazu aufzusetzen und, sehr viele User in den unterschiedlichsten Ziel- und Altersgruppen, zu befragen. Weiters sollten die Werte die zu Phishing usw. schon vorhanden sind auch auf andere Punkte wie Zielgruppen, wie wurden sie verschickt – per Mail oder über Posts in sozialen Netzwerken – ausgewertet werden können.

Ein weiterer Interessanter Punkt wäre sicher, zu erforschen, wie die sozialen Netzwerke speziell mit Smartphones genutzt werden bzw. welche Gefahren dies mit sich bringt. Auch hier sollten die Nutzer aufmerksam gemacht werden, dass die Synchronisation zwischen Handy und sozialen Netzwerk gewisse Gefahren und Risiken verbirgt. Weiters könnte man Apps wie „What’s app“ oder ähnliches untersuchen und schauen wie diese Apps arbeiten und wie sich Social Engineering mit diesen Apps betreiben lässt bzw. vielleicht gibt es schon Apps, die Social Engineering unterstützten. Eine weitere interessante Fragestellung wäre, welche Social Engineering Angriffsszenarien es über Apps schon gibt?

8. Anhang (Auswertung der Befragung)

Es wurde in einem großen Unternehmen in der Sicherheitsabteilung eine Umfrage durchgeführt. Es wurde den Mitarbeitern ein E-Mail geschickt, mit der Bitte die Tabelle anhand folgender Kriterien auszufüllen.

Legende:

Gewichtung	Beschreibung
A	trifft zu
B	trifft teilweise zu
frei lassen	trifft nicht zu

Die Frage zur Tabelle lautete:

Welche Informationen sind für die angegebenen Angriffsszenarien und Gefahren kritisch?

Acht Sicherheitsleute haben diese Tabelle ausgefüllt, anhand dieser Rückmeldungen wurde eine Auswertung durchgeführt. Generell werden die „A“ mehr bewertet als die „B“ und es wurde sich immer für die „Mehrheit“ entschieden, wobei zum Beispiel bei zwei A und zwei B das A genommen wird. Sind mehr Kästchen frei gelassen worden, als ausgefüllt, so wurde sich für „frei lassen“ entschieden.

Weiters wird sich zum Beispiel bei 4x „frei gelassen“ und 3x „B“ für „frei lassen“ entschieden.

Die „A“ werden in der Verwundbarkeitsdarstellung zu „16“, und die „B“ zu „2“ und die Schlüsselkriterien werden anhand der Befragung und der Recherche ausgewählt.

	Angriffsszenarien und Gefahren									
	Identitätsdiebstahl (Person 1)	Identitätsdiebstahl (Person 2)	Identitätsdiebstahl (Person 3)	Identitätsdiebstahl (Person 4)	Identitätsdiebstahl (Person 5)	Identitätsdiebstahl (Person 6)	Identitätsdiebstahl (Person 7)	Identitätsdiebstahl (Person 8)	Auswertung	
Name	A	A	A	A	A	A	A	A	A	
Nutzername	A	A	A	A	A	A	B		A	
Geschlecht		A	A	A	A	B	B	B	A	
Adresse	A	A	A	A	A	A	A	B	A	
Geburtsdag	A	A	A	A	A	A	A	A	A	
Sprache		A	B		A	B	B	B	B	
E-Mail Adresse	A	A	A	A	A	B	B	B	A	
Telefonnummern	A	A	A		A	A	B		A	
andere Nutzernamen (anderer Netzwerke)	B	B	A	A	A	B	B		B	
Gefällt mir	B		A							
Netzwerke	A		A		A		B			
Verknüpfte Konten	A	A	A		A		B		A	
Profilbild	A	A	A		A	A	A		A	
Beziehungsstatus	A	A	A	A	B	A			A	
Familienmitglieder	A	A	A	B	B	A			A	
Interessiert an (Sexuelle Vorlieben)	A		A		B	B	B			
Arbeitgeber	A	A	A	A	A	A	A	A	A	
Hochschule, Schule und Kurse	B	A	A		A	B	B	B	B	
Religion	A	A	B		A	B	B		B	
Politische Einstellung	A		B		B		B			
Personen, die mich inspirieren	B		B		B					
Interessen und Aktivitäten (Hobbys, usw.)	B	A	A	A	B	B	B		B	
Musik, Bücher, Filme, Fernsehen, Spiele	B	B	A		B	B			B	
Lieblingssport-arten, -mannschaften, Lieblingssportler	B	B	A		B	B			B	
Fotos (Urlaubsfotos, Partybilder, usw.)	B	A	A	A	B	B	A		A	
Aktueller Aufenthaltsort (GPS)	A	A	A	A	A		B		A	
Statusmeldungen (Neuigkeiten)	B	B	B		B	B	B		B	
Anwendungen und Spiele		B	B		B					
Gruppen		A	B	A	B		B		B	
Pinnwandkommentare	A		B		A					

Tabelle 19: Auswertung Identitätsdiebstahl

	Angriffsszenarien und Gefahren									
	Cyber-Mobbing (Person 1)	Cyber-Mobbing (Person 2)	Cyber-Mobbing (Person 3)	Cyber-Mobbing (Person 4)	Cyber-Mobbing (Person 5)	Cyber-Mobbing (Person 6)	Cyber-Mobbing (Person 7)	Cyber-Mobbing (Person 8)	Auswertung	
Name	A	A	B	A	A		B	B	A	
Nutzername	A	A		A	B		A	A	A	
Geschlecht	A	A		B	B	B	B	B	B	
Adresse	A	B		B			B	B	B	
Geburtsdag	A	B		B	B		B	B	B	
Sprache		A		B	B	B	B	B	B	
E-Mail Adresse	A	A	B	A		B	A	A	A	
Telefonnummern	A	B		A		B	A	A	A	
andere Nutzernamen (anderer Netzwerke)	A	A		B			A	A	A	
Gefällt mir			B	B						
Netzwerke	A		B		B					
Verknüpfte Konten	B	A	B	A						
Profilbild	A	B	B	B	B	B	B	B	B	
Beziehungsstatus	B	B	B	A	B	B			B	
Familienmitglieder	B	B	B	A						
Interessiert an (Sexuelle Vorlieben)	A		B	A	B	B				
Arbeitgeber	A	A		B						
Hochschule, Schule und Kurse		B								
Religion	A	A	B	B		B	B		B	
Politische Einstellung	B	B	B	A		B	B		B	
Personen, die mich inspirieren		B	B	B	B					
Interessen und Aktivitäten (Hobbys, usw.)	B	B	B	B			B		B	
Musik, Bücher, Filme, Fernsehen, Spiele			B	B						
Lieblingssport-arten, -mannschaften, Lieblingssportler			B	B	B		B			
Fotos (Urlaubsfotos, Partybilder, usw.)	A		A	A	B	B	A	A	A	
Aktueller Aufenthaltsort (GPS)	A	B	A	B			A	A	A	
Statusmeldungen (Neuigkeiten)			B							
Anwendungen und Spiele			B							
Gruppen			B							
Pinnwandkommentare	A	B	B	B	A		A	A	A	

Tabelle 20: Auswertung Cyber-Mobbing

	Angriffsszenarien und Gefahren										
	Phishing (Person 1)	Phishing (Person 2)	Phishing (Person 3)	Phishing (Person 4)	Phishing (Person 5)	Phishing (Person 6)	Phishing (Person 7)	Phishing (Person 8)		Auswertung	
Name	A		B	A	A	B					
Nutzername	A			A		B					
Geschlecht					B						
Adresse	B			B	B						
Geburtsdag	A			B	B						
Sprache			B		B						
E-Mail Adresse	A	A	A	A	A	A	A	A		A	
Telefonnummern	A			B	B	B					
andere Nutzernamen (anderer Netzwerke)	A			B							
Gefällt mir											
Netzwerke			B		B						
Verknüpfte Konten	A	A		B							
Profilbild	A				B						
Beziehungsstatus	B			B	B	B					
Familienmitglieder	B										
Interessiert an (Sexuelle Vorlieben)	A			B	B	B					
Arbeitgeber	B	A			B						
Hochschule, Schule und Kurse				B	B						
Religion				B	B	B					
Politische Einstellung				B	B		B				
Personen, die mich inspirieren				B							
Interessen und Aktivitäten (Hobbys, usw.)				B		A	B	B			
Musik, Bücher, Filme, Fernsehen, Spiele				B		A					
Lieblingssport-arten, -mannschaften, Lieblingssportler				B	B	A					
Fotos (Urlaubsfotos, Partybilder, usw.)	B				B						
Aktueller Aufenthaltsort (GPS)	A										
Statusmeldungen (Neuigkeiten)											
Anwendungen und Spiele				B							
Gruppen						A					
Pinnwandkommentare	B				B						

Tabelle 21: Auswertung Phishing

	Angriffsszenarien und Gefahren										
	Spear-Phishing (Person 1)	Spear-Phishing (Person 2)	Spear-Phishing (Person 3)	Spear-Phishing (Person 4)	Spear-Phishing (Person 5)	Spear-Phishing (Person 6)	Spear-Phishing (Person 7)	Spear-Phishing (Person 8)		Auswertung	
Name	A	A	A		A		B	B		A	
Nutzername	A	A									
Geschlecht		B	B	A	B						
Adresse	A	B	B		B		B	B		B	
Geburtsdag	A	B		B	B			B		B	
Sprache		B	B	B	B			B		B	
E-Mail Adresse	A	A	A	B	A	A	A	A		A	
Telefonnummern	B	B	B		B						
andere Nutzernamen (anderer Netzwerke)	B	B		B							
Gefällt mir				A							
Netzwerke	B	B	B	A	B						
Verknüpfte Konten	A	A									
Profilbild	A				B						
Beziehungsstatus	B		B	B	B						
Familienmitglieder	B		B								
Interessiert an (Sexuelle Vorlieben)	A		B	A	B						
Arbeitgeber	B	B	B	A	B		B	B		B	
Hochschule, Schule und Kurse	B	B	B	B	B					B	
Religion				A	B						
Politische Einstellung		B	B	A	B					B	
Personen, die mich inspirieren		B	B	A							
Interessen und Aktivitäten (Hobbys, usw.)		A	A	A		A				A	
Musik, Bücher, Filme, Fernsehen, Spiele		B	A	A		A				A	
Lieblingssport-arten, -mannschaften, Lieblingssportler		A	A	A	B	A				A	
Fotos (Urlaubsfotos, Partybilder, usw.)	B	A		B	B						
Aktueller Aufenthaltsort (GPS)	A	B		A							
Statusmeldungen (Neuigkeiten)		B									
Anwendungen und Spiele				A							
Gruppen			B	A		A	A	A		A	
Pinnwandkommentare				B	B						

Tabelle 22: Auswertung Spear-Phishing

	Angriffsszenarien und Gefahren										
	Social-Phishing (Person 1)	Social-Phishing (Person 2)	Social-Phishing (Person 3)	Social-Phishing (Person 4)	Social-Phishing (Person 5)	Social-Phishing (Person 6)	Social-Phishing (Person 7)	Social-Phishing (Person 8)		Auswertung	
Name	A	A			A	B	B	B		A	
Nutzername	A			B		B					
Geschlecht		A		B	B	B		B		B	
Adresse	A	A			B			B			
Geburtsdag	A	B		A	B	B	A	A		A	
Sprache		A	B	B	B	B	B	B		B	
E-Mail Adresse	A	A	B	B	A	A	A	A		A	
Telefonnummern	A	A			B	B					
andere Nutzernamen (anderer Netzwerke)	A	B		A		B					
Gefällt mir	B			A		B					
Netzwerke	B	B	B	B	B						
Verknüpfte Konten	A	B		A			A	A		A	
Profilbild	A	B			B	B					
Beziehungsstatus	B			A	B	A					
Familienmitglieder	B	A				B					
Interessiert an (Sexuelle Vorlieben)	A			A	B	B					
Arbeitgeber	A	A		B	B	B		B		B	
Hochschule, Schule und Kurse	B	B	B	A	B	B				B	
Religion		B		A	B	A					
Politische Einstellung	B			A	B	A					
Personen, die mich inspirieren	B			B		B					
Interessen und Aktivitäten (Hobbys, usw.)	B			B		A					
Musik, Bücher, Filme, Fernsehen, Spiele				B		A					
Lieblingssport-arten, -mannschaften, Lieblingssportler				B	B	A					
Fotos (Urlaubsfotos, Partybilder, usw.)	B			B	B		B	B		B	
Aktueller Aufenthaltsort (GPS)	B			B							
Statusmeldungen (Neuigkeiten)	A										
Anwendungen und Spiele				B							
Gruppen						A					
Pinnwandkommentare	B				B	A					

Tabelle 23: Auswertung Social-Phishing

	Angriffsszenarien und Gefahren										
	Verbreitung von Schadsoftware (Person 1)	Verbreitung von Schadsoftware (Person 2)	Verbreitung von Schadsoftware (Person 3)	Verbreitung von Schadsoftware (Person 4)	Verbreitung von Schadsoftware (Person 5)	Verbreitung von Schadsoftware (Person 6)	Verbreitung von Schadsoftware (Person 7)	Verbreitung von Schadsoftware (Person 8)		Auswertung	
Name							B				
Nutzername	A				B						
Geschlecht											
Adresse											
Geburtstag											
Sprache											
E-Mail Adresse	A	A		A	A	A	B	B		A	
Telefonnummern	B										
andere Nutzernamen (anderer Netzwerke)	A										
Gefällt mir											
Netzwerke	A	A				A					
Verknüpfte Konten		A		B							
Profilbild											
Beziehungsstatus											
Familienmitglieder		A									
Interessiert an (Sexuelle Vorlieben)				B							
Arbeitgeber	A	A									
Hochschule, Schule und Kurse		A									
Religion				B							
Politische Einstellung											
Personen, die mich inspirieren				B							
Interessen und Aktivitäten (Hobbys, usw.)		A		B							
Musik, Bücher, Filme, Fernsehen, Spiele				B							
Lieblingssport-arten, -mannschaften, Lieblingssportler				B							
Fotos (Urlaubsfotos, Partybilder, usw.)											
Aktueller Aufenthaltsort (GPS)											
Statusmeldungen (Neuigkeiten)							A	A			
Anwendungen und Spiele		A		A		A	A	A		A	
Gruppen		B	B				B				
Pinnwandkommentare		B					A	A			

Tabelle 24: Auswertung Verbreitung von Schadsoftware

	Angriffsszenarien und Gefahren										
	Verkauf der Daten - Werbung (Person 1)	Verkauf der Daten - Werbung (Person 2)	Verkauf der Daten - Werbung (Person 3)	Verkauf der Daten - Werbung (Person 4)	Verkauf der Daten - Werbung (Person 5)	Verkauf der Daten - Werbung (Person 6)	Verkauf der Daten - Werbung (Person 7)	Verkauf der Daten - Werbung (Person 8)		Auswertung	
Name	A	A	A	A	A		B	B		A	
Nutzername	B			A							
Geschlecht		A		A	A						
Adresse	A	A	B	A	B		A	A		A	
Geburtsdag	A	A		A	B		A	A		A	
Sprache		A		B	B	B	B	B		B	
E-Mail Adresse	A	A	A	A	A	B	A	A		A	
Telefonnummern	A	A	B	A	B					A	
andere Nutzernamen (anderer Netzwerke)	A			B							
Gefällt mir		A		B							
Netzwerke			B	B	B						
Verknüpfte Konten						B					
Profilbild							B				
Beziehungsstatus		A		B	B						
Familienmitglieder		A			B						
Interessiert an (Sexuelle Vorlieben)			B	B	B	B	B	B		B	
Arbeitgeber		A	B	A		A	A	A		A	
Hochschule, Schule und Kurse		A	B	A	B		B	B		B	
Religion			B	A	B	A	B	B		B	
Politische Einstellung		A	B	A	B	A	A	A		A	
Personen, die mich inspirieren		B	B	B		A	B	B		B	
Interessen und Aktivitäten (Hobbys, usw.)	A	A	A	B	A	A	A	A		A	
Musik, Bücher, Filme, Fernsehen, Spiele	A	A	A	A	A	A	A	A		A	
Lieblingssport-arten, -mannschaften, Lieblingssportler	A	A	A	A	B	A	A	A		A	
Fotos (Urlaubsfotos, Partybilder, usw.)						B					
Aktueller Aufenthaltsort (GPS)	A	A	B	B			B	B		B	
Statusmeldungen (Neuigkeiten)			B				B				
Anwendungen und Spiele	B	A	B	B		A	B	B		B	
Gruppen	B		B				B	B			
Pinnwandkommentare			B								

Tabelle 25: Auswertung Verkauf der Daten (Werbung)

	Angriffsszenarien und Gefahren										
	Bewerbung (Person 1)	Bewerbung (Person 2)	Bewerbung (Person 3)	Bewerbung (Person 4)	Bewerbung (Person 5)	Bewerbung (Person 6)	Bewerbung (Person 7)	Bewerbung (Person 8)		Auswertung	
Name	A	A	A				B	B		B	
Nutzername	B	A									
Geschlecht	A	A	A		B		B	B		B	
Adresse	A	A	A		B		B	B		B	
Geburtstag	A	A	A		B		B	B		B	
Sprache		A	B		B		B	B		B	
E-Mail Adresse	A	A	B		B		B			B	
Telefonnummern	A	A	B				B				
andere Nutzernamen (anderer Netzwerke)		B			B						
Gefällt mir				A		A					
Netzwerke		B	B		B						
Verknüpfte Konten		A				B					
Profilbild	A	A	B		B	A	A	A		A	
Beziehungsstatus		B			B	B					
Familienmitglieder		B	B		B						
Interessiert an (Sexuelle Vorlieben)				A	B	A					
Arbeitgeber	A	A	B	A	B		A	A		A	
Hochschule, Schule und Kurse	A	A	B		B		A	A		A	
Religion					B	A	A				
Politische Einstellung	A	B		B	B	A	B	B		B	
Personen, die mich inspirieren					B	B					
Interessen und Aktivitäten (Hobbys, usw.)	B	B	B	B	B	A	B	B		B	
Musik, Bücher, Filme, Fernsehen, Spiele		B			B						
Lieblingssport-arten, -mannschaften, Lieblingssportler		B			B						
Fotos (Urlaubsfotos, Partybilder, usw.)	A	A	A	A	B	A	A	A		A	
Aktueller Aufenthaltsort (GPS)						A					
Statusmeldungen (Neuigkeiten)		B		B	B	A	A	A		A	
Anwendungen und Spiele		B	B								
Gruppen			B	B		A					
Pinnwandkommentare	A	B	B		B	A	A	A		A	

Tabelle 26: Auswertung Bewerbung

	Angriffsszenarien und Gefahren										
	Kündigung (Person 1)	Kündigung (Person 2)	Kündigung (Person 3)	Kündigung (Person 4)	Kündigung (Person 5)	Kündigung (Person 6)	Kündigung (Person 7)	Kündigung (Person 8)		Auswertung	
Name	A	A	A				B				
Nutzername		A									
Geschlecht		A									
Adresse	A	A									
Geburtstag	A	A									
Sprache		A			B						
E-Mail Adresse		A			B		B				
Telefonnummern		B									
andere Nutzernamen (anderer Netzwerke)		B			B						
Gefällt mir		B		A							
Netzwerke					B						
Verknüpfte Konten		B				B					
Profilbild		A			B	A					
Beziehungsstatus		B			B	B					
Familienmitglieder		B			B						
Interessiert an (Sexuelle Vorlieben)				A	B	A					
Arbeitgeber	A	A		A	B		A	A		A	
Hochschule, Schule und Kurse					B						
Religion		B			B	A	B	B		B	
Politische Einstellung	A			B	B	A					
Personen, die mich inspirieren					B	B					
Interessen und Aktivitäten (Hobbys, usw.)				B	B	A					
Musik, Bücher, Filme, Fernsehen, Spiele					B						
Lieblingssport-arten, -mannschaften, Lieblingssportler					B						
Fotos (Urlaubsfotos, Partybilder, usw.)	A			A	B	A	A	A		A	
Aktueller Aufenthaltsort (GPS)						A					
Statusmeldungen (Neuigkeiten)				B	B	A	A	A		A	
Anwendungen und Spiele											
Gruppen				B		A					
Pinnwandkommentare	A	A			B	A	A	A		A	

Tabelle 27: Auswertung Kündigung

Literaturverzeichnis

- [1] „SaferInternet.at,“ [Online]. Available: <http://www.saferinternet.at/themen/soziale-netzwerke/>. [Zugriff am 11 02 2012].
- [2] G. Statista, „Statista.de,“ [Online]. Available: <http://www.statista.de/>. [Zugriff am 30 03 2012].
- [3] Integral, AIM - Austrian Internet Monitor, Austian Internet Monitor, April 2011.
- [4] P. Schaumann, „Sicherheitskultur.at,“ [Online]. Available: <http://sicherheitskultur.at>. [Zugriff am 11 02 2012].
- [5] K. D. Mitnik und W. L. Simon, Die Kunst der Täuschung, Heidelberg: mitp, 2003.
- [6] C. Hadnagy, Die Kunst des Human Hacking Social Engineering - Deutsche Ausgabe, mitp, 2011.
- [7] DerStandard, „derStandard.at - Social Engineering,“ [Online]. Available: <http://derstandard.at/1292462027991/WebStandard-Interview-Social-Engineering-oder-Wie-man-Menschen-knackt>. [Zugriff am 05 04 2012].
- [8] Markus Huber und Peter Kieseberg, „Phishing in sozialen Netzwerken,“ *Hakin9*, 05 2011.
- [9] M. Huber, Kommunikation im Web 2.0, Freiburg: UVK Verlagsgesellschaft, 2012.
- [10] A. Schwindt, Das Facebook-Buch, Köln: O'Reilly Verlag GmbH&Co KG , 2012.
- [11] BITKOM, „Soziale Netzwerke; Zweite, erweiterte Studie,“ 2011. [Online]. Available: http://www.bitkom.org/de/publikationen/38338_70897.aspx. [Zugriff am 06 04 2012].
- [12] Iasonas Polakis, Georgios Kontaxis, Spiros Antonatos, Eleni Gessiou, Thanasis Petsas, Evangelos P. Markatos, „Using social networks to harvest email addresses,“ in *In Proceedings of the 9th annual ACM workshop on Privacy in the electronic society (WPES '10)*, ACM, New York, NY, USA, 2010.
- [13] Crowd Science, *Attitudes towards social media among users.*, Social Media Insights, S.8, Dezember 2009.
- [14] J. Steinschaden, Phänomen Facebook, Wien: Carl Ueberreuter, 2012.
- [15] S. Medienpädagogischer Forschungsverbund, „mpfs.de - JIM 2011,“ 11 2011. [Online]. Available: <http://www.mpfs.de/index.php?id=11>. [Zugriff am 30 03 2012].
- [16] „SocialMediaRadar,“ [Online]. Available: <http://socialmediaradar.at/facebook.php>. [Zugriff am 11 02 2012].
- [17] G. SPIEGELnet, „Spiegel Online,“ [Online]. Available: <http://www.spiegel.de/thema/twitter/>. [Zugriff am 22 03 2012].
- [18] BSI, „BSI - Glossar und Begriffsdefinitionen,“ [Online]. Available: https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html. [Zugriff am 06 04 2012].
- [19] BSI, „BSI - Gefährdungen: Begriffserleuterungen, Einführung,“ [Online]. Available: https://www.bsi.bund.de/DE/Themen/InternetSicherheit/Gefaehrdungen/gefaehrungen_node.html. [Zugriff am 25 03 2012].
- [20] D. Emm, „Viruslist.com - alles über Internet-Sicherheit,“ Kaspersky Lab, 01 04 2010. [Online]. Available: <http://www.viruslist.com/de/analysis?pubid=200883688>. [Zugriff am 25 03 2012].
- [21] G. DATACOM Buchverlag. [Online]. Available: <http://www.itwissen.info/definition/lexikon/Angriff-attack.html>. [Zugriff am 11 02 2012].
- [22] ISACA, „ISACA® Glossary of Terms,“ ISACA, 2012.
- [23] ON Österreichisches Normungsinstitut, „ÖNORM ISO/IEC 27002 - Informationstechnologie - Sicherheitstechnik - Leitfaden für das Management der Informationssicherheit,“ Wien, 2005.

- [24] „Facebook - Hilfebereich,“ [Online]. Available: <http://www.facebook.com/help/?page=260315770650470&ref=hcnv>. [Zugriff am 13 02 2012].
- [25] BITKOM, Forsa, *Soziale Netzwerke in Deutschland*, BITKOM, April 2011.
- [26] . I. L. Facebook, „Facebook - Hilfe - Fotos markieren,“ [Online]. Available: <http://www.facebook.com/help/photos/tag-photos>. [Zugriff am 07 04 2012].
- [27] Pixable, *Anzahl Fotos der Facebook-User*, pixable.com, Februar 2011.
- [28] o.V., „heise.de - Facebook erkennt Gesichter,“ [Online]. Available: <http://www.heise.de/newsticker/meldung/Facebook-erkennt-Gesichter-1256586.html>. [Zugriff am 07 04 2012].
- [29] Bundeskanzleramt, „Rechtsinformationssystem,“ [Online]. Available: <http://www.ris.bka.gv.at/default.aspx>. [Zugriff am 22 03 2012].
- [30] Marketagent.com, Netural Communication, *CAWI-Befragung (Computer Assisted Web Interview)*, Marketagent.com, Mai 2009.
- [31] Tomorrow Focus Media, *Social Media Effects 2010*, Tomorrow Focus Media, November 2010.
- [32] TNS Infratest, *Wie sicher surft Deutschland*, Seite 7, Deutsche Telekom, November 2010.
- [33] SINUS-Institut Heidelberg, *DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet*, Seite 53, Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI), Februar 2012.
- [34] M. Huber, M. Mulazzani, E. Weippl, G. Kitzler und S. Goluch, „Friend-in-the-Middle Attacks: Exploiting Social Networking Sites for Spam,“ in *Internet Computing, IEEE*, May-June 2011.
- [35] G. presstext Nachrichtenagentur, „presstext,“ [Online]. Available: <http://www.presstext.com/news/20110922026>. [Zugriff am 30 03 2012].
- [36] Jürgen Donauer, „BITblokes,“ [Online]. Available: <http://www.bitblokes.de/2010/08/facebook-hacker-tool-klick-hack-und-drin/>. [Zugriff am 17 05 2012].
- [37] BandikutMedia, „Web-Analytics.org - Twitalyzer,“ [Online]. Available: <http://www.web-analytics.org/index.php/web-analyse-anbieter/details/twitalyzer/>. [Zugriff am 17 05 2012].
- [38] Aha Cafe LLC, „Top Five Twitter Analytical Tools,“ [Online]. Available: http://inventorspot.com/articles/top_five_twitter_analytical_tools_29218. [Zugriff am 17 05 2012].
- [39] CHIP Xonio Online GmbH, „chip.de - TweetPsych,“ [Online]. Available: http://www.chip.de/webapps/TweetPsych_46975198.html. [Zugriff am 17 05 2012].
- [40] Axel Springer AG, „WeltOnline - Datenschützer nehmen FarmVille in die Mangel,“ [Online]. Available: <http://www.welt.de/wirtschaft/webwelt/article6218107/Datenschuetzer-nehmen-Farmville-in-die-Mangel.html>. [Zugriff am 18 05 2012].
- [41] stern.de GmbH, „Stern.de - Kritik an FarmVille,“ [Online]. Available: <http://www.stern.de/digital/online/kritik-an-farmville-und-co-reiche-ernte-fuer-datensammler-1601571.html>. [Zugriff am 18 05 2012].
- [42] BSI, *Cyber-Sicherheit in Deutschland*, Seite 11, Juni 2011.
- [43] BSI, „BSI für Bürger - Sicherheitsrisiken Soziale Netzwerke,“ [Online]. Available: https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/KommunikationUeberInternet/SozialeNetzwerke/Sicherheitsrisiken/sicherheitsrisiken_node.html. [Zugriff am 05 04 2012].
- [44] BSI, „Identitätsdiebstahl und Identitätsmissbrauch im Internet - Studie,“ [Online]. Available: [http://www.trickbetrueger.info/Studie_Identitaetsdiebstahl_090610\(2\).pdf](http://www.trickbetrueger.info/Studie_Identitaetsdiebstahl_090610(2).pdf). [Zugriff am 07 04 2012].
- [45] B. Amann-Hechenberger, B. Buchegger und S. Schwarz, „Aktiv gegen Cyber-Mobbing - Vorbeugen – Erkennen – Handeln,“ ÖIAT, 2011.
- [46] Ö. Bundeskanzleramt. [Online]. Available: <https://www.help.gv.at/Portal.Node/hlpd/public/content/172/Seite.1720700.html>. [Zugriff am 08 03 2012].
- [47] S. Rack und M. Fileccia, „Was tun bei Cyber-Mobbing?,“ 2011.

- [48] Forsa, *Cybermobbing - Gewalt unter Jugendlichen*, Nordrhein-Westfalen: TK; Uni Münster, Juni 2011.
- [49] Forsa, *Meinungspuls Cybermobbing 2011*, Nordrhein-Westfalen: tk.de, Juni 2011.
- [50] P. S. The London School of Economics and , *Risks and safety on the internet: The perspective of European children*, Seite 69, EU Kids Online, Oktober 2010.
- [51] Medienkonvergenz Monitoring (MeMo), *Soziale Online-Netzwerke-Report 2010*, Seite 44, Januar 2011.
- [52] ÖIAT. [Online]. Available: <http://www.saferinternet.at/themen/datenschutz/#c727>. [Zugriff am 08 03 2012].
- [53] BSI. [Online]. Available: https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Phishing/phishing_node.html. [Zugriff am 08 03 2012].
- [54] Symantec Corporation, „Norton - Spear Phishing,“ [Online]. Available: <http://ch.norton.com/spear-phishing-scam-not-sport/article>. [Zugriff am 01 05 2012].
- [55] G. DATACOM Buchverlag. [Online]. Available: <http://www.itwissen.info/definition/lexikon/Spear-Phishing-spear-phishing.html>. [Zugriff am 08 03 2012].
- [56] M. Nohlberg, *Securing Information Assets*, Stockholm: Department of Computer and Systems Sciences, 2008.
- [57] P. Schaumann, „sicherheitskultur.at - Studie Social Phishing,“ 29 08 2007. [Online]. Available: http://mijozi.de/docs/informatik/ds_rechtliches_zensur/ds_hacking_malware/phishing/j/2007_08_29_sicherheitskultur_at.pdf. [Zugriff am 25 05 2012].
- [58] M. Deutschland, 12 05 2011. [Online]. Available: <http://www.microsoft.com/germany/newsroom/pressemitteilung.msp?id=533369>. [Zugriff am 08 03 2012].
- [59] M. Corporation, 2011. [Online]. Available: <http://www.microsoft.com/security/sir/archive/default.aspx>. [Zugriff am 08 03 2012].
- [60] BitDefender, *H1 2011 E-Threats Landscape Report*, Seite 21, Juni 2011.
- [61] Kaspersky Lab, *Am häufigsten von Phishing betroffene Organisationen*, viruslist.com, März 2011.
- [62] Invoke Solutions, eMarketer, August 2010.
- [63] „HR-Online,“ [Online]. Available: http://www.hr-online.de/website/rubriken/ratgeber/index.jsp?rubrik=55393&key=standard_document_43727433&seite=2. [Zugriff am 13 02 2012].
- [64] A. Lerg, „T-Online,“ Deutsche Telekom AG, [Online]. Available: http://computer.t-online.de/viren-alarm-bei-facebook-wurm-koobface-ist-wieder-da/id_43978264/index. [Zugriff am 04 04 2012].
- [65] „DiePresse.com,“ "Die Presse" Digital GmbH & Co KG , [Online]. Available: http://diepresse.com/home/techscience/internet/sicherheit/724589/Koobface_Kriminelle-hinter-FacebookWurm-enttarnt. [Zugriff am 04 04 2012].
- [66] IDG Magazine Media GmbH, „pcwelt.de - Android Malware über Twitter verbreitet,“ [Online]. Available: <http://www.pcwelt.de/news/Mobile-Schaedlinge-Android-Malware-ueber-Twitter-verbreitet-5053099.html>. [Zugriff am 05 05 2012].
- [67] . s. A. anwalt.de, „Anwalt.de - Einfach zum Anwalt,“ [Online]. Available: http://www.anwalt.de/rechtstipps/identitaetsdiebstahl-ueber-fake-profile-bei-facebook-und-wie-man-dagegen-vorgehen-kann_020415.html. [Zugriff am 05 04 2012].
- [68] heise online, „heise.de - Mobbing für Fortgeschrittene mit Facebook Gruppen,“ [Online]. Available: <http://www.heise.de/newsticker/meldung/Mobbing-fuer-Fortgeschrittene-mit-Facebook-Gruppen-1264593.html>. [Zugriff am 14 04 2012].
- [69] o.V., „paperblog.com - Neuer Fall von Identitätsdiebstahl auf Facebook,“ [Online]. Available: <http://de.paperblog.com/neuer-fall-von-identitaetsdiebstahl-auf-facebook-in-schweden-94706/>. [Zugriff am 14 04 2012].
- [70] NORDSEE-ZEITUNG GmbH , „nordsee-zeitung.de - Der diebische Doppelgänger,“ [Online]. Available:

- http://www.nordsee-zeitung.de/region/bremerhaven_artikel,-Der-diebische-Doppelgaenger-_arid,732353.html. [Zugriff am 14 04 2012].
- [71] „ORF.at - News,“ [Online]. Available: <http://sbgv1.orf.at/stories/392735>. [Zugriff am 05 04 2012].
- [72] „ORF.at - News (Cyber-Mobbing),“ [Online]. Available: <http://ktnv1.orf.at/stories/495006>. [Zugriff am 05 04 2012].
- [73] Yahoo! Deutschland GmbH, „nachrichten.yahoo.com - Schuldspruch tödlicher Cybermobbing Fall in den USA,“ [Online]. Available: <http://de.nachrichten.yahoo.com/schuldspruch-t%C3%B6dlichem-cybermobbing-fall-den-usa-051713975.html>. [Zugriff am 14 04 2012].
- [74] SPIEGEL ONLINE GmbH, „spiegel.de - Erneut Selbstmord wegen Cyber-Mobbing,“ [Online]. Available: <http://www.spiegel.de/netzwelt/web/0,1518,650340,00.html>. [Zugriff am 14 04 2012].
- [75] Hutter Consult GmbH, „Facebook: Erste Verurteilung für Cyber-Mobbing auf Facebook in der Schweiz,“ [Online]. Available: <http://www.thomashutter.com/index.php/2011/05/facebook-erste-verurteilung-fur-cyber-mobbing-auf-facebook-in-der-schweiz/>. [Zugriff am 14 04 2012].
- [76] Frankfurter Allgemeine Zeitung GmbH, „Bring dich doch um, alle wären froh, wenn du tot wärst,“ [Online]. Available: <http://www.faz.net/aktuell/feuilleton/medien/cybermobbing-bring-dich-doch-um-alle-waeren-froh-wenn-du-tot-waerst-11497475.html>. [Zugriff am 14 04 2012].
- [77] . A. Fonpit, „AndroidPIT,“ [Online]. Available: <http://www.androidpit.de/de/android/blog/401277/Schadsoftware-Ramnit-treibt-auf-Facebook-ihr-Unwesen>. [Zugriff am 06 04 2012].
- [78] G. netzwelt, „netzwelt.de - Guter Rat auf einen Klick,“ [Online]. Available: <http://www.netzwelt.de/news/90164-facebook-wurm-klaut-login-informationen.html>. [Zugriff am 06 04 2012].
- [79] Das Security-Ressort von c't, „heise.de - Facebook-Würmer breiten sich ungehindert aus,“ [Online]. Available: <http://www.heise.de/security/meldung/Facebook-Wuermer-breiten-sich-ungehindert-aus-1021650.html>. [Zugriff am 15 04 2012].
- [80] CHIP Xonio Online GmbH, „chiponline.de - Schau dir mal das Foto an,“ [Online]. Available: http://www.chip.de/news/Achtung-ICQ-Virus-Schau-Dir-mal-das-Foto-an_42534697.html. [Zugriff am 15 04 2012].
- [81] Andreas Proschofsky, „derstandard.at - Entwarnung Twitter stoppt Wurm Choas,“ [Online]. Available: <http://derstandard.at/1285042334426/Entwarnung-Twitter-stoppt-Wurm-Chaos>. [Zugriff am 04 05 2012].
- [82] P. Schaumann, „sicherheitskultur.at - Spuren im Internet,“ [Online]. Available: http://sicherheitskultur.at/spuren_im_internet.htm. [Zugriff am 27 04 2012].
- [83] . I. L. Facebook, „Facebook.com - Aktualisierung der Erklärung der Rechte und Pflichten,“ [Online]. Available: http://www.facebook.com/notes/facebook-site-governance/aktualisierung-der-erkl%C3%A4rung-der-rechte-und-pflichten/10151419988630301?comment_id=35999752. [Zugriff am 07 04 2012].
- [84] S. A. Axel, „Welt Online,“ [Online]. Available: <http://www.welt.de/News/article4370702/Private-Internet-Daten-als-Problem-bei-der-Bewerbung.html>. [Zugriff am 05 04 2012].
- [85] K. f. A. u. A. Wien, „Arbeiterkammer,“ [Online]. Available: <http://www.arbeiterkammer.at/online/vorsicht-mit-web-20-in-der-arbeitswelt-59595.html>. [Zugriff am 05 04 2012].
- [86] o.V., „diePresse.com - Kündigung nach Facebookbesuch im Krankenstand,“ [Online]. Available: <http://diepresse.com/home/techscience/internet/474144/Kuendigung-nach-FacebookBesuch-im-Krankenstand->. [Zugriff am 12 04 2012].
- [87] o.V., „Giga.de - Gericht bestätigt Apples Kündigung wegen Facebook Postings,“ [Online]. Available: <http://www.giga.de/unternehmen/apple/news/gericht-bestatigt-apples-kundigung-wegen-facebook-post/>. [Zugriff am 12 04 2012].
- [88] WAZ NewMedia GmbH & Co. KG, „derwesten.de - Facebook-Eintrag sorgt für fristlose Kündigung,“

- [Online]. Available: <http://www.derwesten.de/staedte/duesseldorf/facebook-eintrag-sorgt-fuer-fristlose-kuendigung-id4999698.html>. [Zugriff am 15 04 2012].
- [89] OAK – Online Akademie GmbH & Co. KG, „bildungsexperten.net - Auf Facebook über den Job lästern – ein Kündigungsgrund?“, [Online]. Available: <http://www.bildungsexperten.net/job-karriere/auf-facebook-uber-den-job-lastern-ein-kundigungsgrund/>. [Zugriff am 15 04 2012].
- [90] Zeitverlag Gerd Bucerius GmbH & Co. KG, „Zeit Online - Meine Identität gehört mir!“, [Online]. Available: <http://www.zeit.de/digital/datenschutz/2010-01/identitaetsdiebstahl-selbsterfahrung/seite-4>. [Zugriff am 03 05 2012].
- [91] Tina Groll, Diplom-Journalistin, „Tina Groll - Hilfe bei Identitätsdiebstahl“, [Online]. Available: <http://tina-groll.de/Identitaetsdiebstahl/Fragen-Antworten/1,000000275959,8,1>. [Zugriff am 03 05 2012].
- [92] BSI, „Register aktueller Cyber-Gefährdungen und -Angriffsformen“, [Online]. Available: <https://www.bsi.bund.de/ContentBSI/Themen/Cyber-Sicherheit/Analysen/Grundlagen/BSIa001.html?notFirst=true&docId=2537462>. [Zugriff am 03 05 2012].
- [93] Education Group, „Medienverhalten der Jugendlichen“, [Online]. Available: <http://www.edugroup.at/detail/2-ooe-jugend-medien-studie-2011.html>. [Zugriff am 04 05 2012].
- [94] Sonia Livingstone, Leslie Haddon, Anke Görzig, and Kjartan Ólafsson, with members of the EU Kids Online network, „eukidsonline.net“, [Online]. Available: [http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20\(2009-11\)/EUKidsOnlineIIReports/D4FullFindings.pdf](http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/D4FullFindings.pdf). [Zugriff am 04 05 2012].
- [95] BITKOM, „Jugend 2.0 - Eine repräsentative Untersuchung zum Internetverhalten von 10- bis 18-Jährigen“, [Online]. Available: http://www.bitkom.org/files/documents/BITKOM_Studie_Jugend_2.0.pdf. [Zugriff am 04 05 2012].
- [96] BSI, „Beispiele für Phishing Angriffe“, [Online]. Available: https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Phishing/BeispielePhishingAngriffe/beispielephishingangriffe_node.html. [Zugriff am 03 05 2012].
- [97] Gesellschaft für Software & Content Marketing & Se, „internetfallen.de“, [Online]. Available: <http://www.internetfallen.de/Hacker-Cracker/Fakes/Phishings/phishings.html>. [Zugriff am 03 05 2012].
- [98] MasterCard, „Phishing“, [Online]. Available: <http://www.mastercard.com/ch/personal/de/cardholderservices/phishing.html>. [Zugriff am 03 05 2012].
- [99] EURO Kartensysteme GmbH, „Spear-Phishing“, [Online]. Available: https://www.kartensicherheit.de/de/pub/oeffentlich/sicher_bezahlen/schutz_vor_phishing_internet/spear_phishing.php. [Zugriff am 03 05 2012].
- [100] Alexander Schultz, „Mediendelikte - Phishing for financial agents“, [Online]. Available: <http://www.mediendelikte.de/aufsatz00001.htm>. [Zugriff am 03 05 2012].
- [101] WEKA MEDIA GmbH & Co. KG, „Datenschutzpraxis - Cyberstalking, Social Phishing und Web 2.0“, [Online]. Available: <http://www.datenschutz-praxis.de/fachwissen/fachartikel/cyber-stalking-social-phishing-und-web-2.0>. [Zugriff am 03 05 2012].
- [102] Info-Point-Security GmbH, „InfopointSecurity - Kaspersky warnt: Spam wird gefährlicher“, [Online]. Available: <https://www.info-point-security.com/security-themen/malware-viren-spam-phishing/item/7135-kaspersky-warnt-spam-wird-gef%C3%A4hrlicher.html>. [Zugriff am 03 05 2012].
- [103] BSI, „Vorsicht vor Schadsoftware in Sozialen Netzwerken“, [Online]. Available: https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2010/Wurm_Facebook_160610.html. [Zugriff am 04 05 2012].
- [104] k.u.r.s. mediasystems gmbh, „computerhilfen.de - Gefährlicher SCR Virus verbreitet sich über Facebook“, [Online]. Available: <http://www.computerhilfen.de/info/gefahrlicher-scr-virus-verbreitet-sich-uber-facebook.html>. [Zugriff am 04 05 2012].
- [105] IDG Magazine Media GmbH, „pcwelt.de - Soziale Netzwerke zunehmend von Malware betroffen“,

- [Online]. Available: <http://www.pcwelt.de/news/Studie-Soziale-Netzwerke-zunehmend-von-Malware-betroffen-1533171.html>. [Zugriff am 04 05 2012].
- [106] 11media communications gmbh, „Privat im Internet - Tracking Cookies sind gefährlich und unnötig,“ [Online]. Available: <http://www.privat-im-internet.de/lxquick-News/Tracking-Cookies-sind-gefahrlich-und-unnotig.html>. [Zugriff am 04 05 2012].
- [107] Wochenzeitung DIE ZEIT, „ZeitOnline - Die tägliche Verfolgungsjagd,“ [Online]. Available: <http://www.zeit.de/digital/datenschutz/2012-04/cookies-tracking-gegenwehr>. [Zugriff am 04 05 2012].
- [108] KasperskyLab, „Viruslist - Juni 2011,“ [Online]. Available: <http://www.viruslist.com/de/analysis?pubid=200883745>. [Zugriff am 04 05 2012].
- [109] KasperskyLab, „Kaspersky Lab Security Bulletin 2011/2012. Spam im Jahr 2011,“ [Online]. Available: <http://www.viruslist.com/de/analysis?pubid=200883770>. [Zugriff am 04 05 2012].
- [110] pcwelt.de, „PCwelt.de - Soziale Netzwerke zunehmend von Malware betroffen,“ [Online]. Available: <http://www.pcwelt.de/news/Studie-Soziale-Netzwerke-zunehmend-von-Malware-betroffen-1533171.html>. [Zugriff am 03 05 2012].
- [111] BSI, „BSI für Bürger - Schutzmaßnahmen,“ [Online]. Available: [https://www.bsi-fuer-buerger.de/ContentBSIFB/SicherheitImNetz/KommunikationUeberInternet/SozialeNetzwerke/Schutzmasnahmen/schutzmassnahmen.html](https://www.bsi-fuer-buerger.de/ContentBSIFB/SicherheitImNetz/KommunikationUeberInternet/SozialeNetzwerke/Schutzmassnahmen/schutzmassnahmen.html). [Zugriff am 28 04 2012].
- [112] saferinternet.at, „Das Mitmach-Internet sicher und verantwortungsvoll nutzen,“ [Online]. Available: http://www.saferinternet.at/uploads/tx_simaterials/Web_2.0_Das_Mitmach-Internet_sicher_und_verantwortungsvoll_nutzen.pdf. [Zugriff am 28 04 2012].
- [113] saferinternet.at, „SaferInternet - 10 Safety Tipps für Twitter,“ [Online]. Available: http://www.saferinternet.at/news/news-detail/article/10-safety-tipps-fuer-twitter-155/?tx_ttnews%5BbackPid%5D=183&cHash=9336a0b47584f69d0c723747bf56566e. [Zugriff am 28 04 2012].
- [114] Kaspersky Lab, „Security-Guide: Social Media für Kinder und Eltern,“ [Online]. Available: http://newsroom.kaspersky.eu/de/texte/detail/article/security-guide-social-media-fuer-kinder-und-eltern/?no_cache=1&cHash=2cc3b7bb135a9bc3037e18ce8139bcba. [Zugriff am 01 05 2012].
- [115] PCWelt.de, „Facebook Sicherheit,“ [Online]. Available: <http://www.pcwelt.de/news/Facebook-Sicherheit-Norton-Safeweb-for-Facebook-warnt-vor-gefaehrlichen-Links-368679.html>. [Zugriff am 28 04 2012].
- [116] Newsgrape OG, „newsgrape.com,“ [Online]. Available: <http://www.newsgrape.com/a/bitdefender-safego-der-virenschutz-fuer-facebook/>. [Zugriff am 28 04 2012].
- [117] Wanying Luo; Qi Xie; Hengartner, U., „FaceCloak: An Architecture for User Privacy on Social Networking Sites,“ in *Computational Science and Engineering, 2009. CSE '09. International Conference on*, vol.3, no., pp.26-33, 29-31, <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5283227&isnumber=5282955>, Aug. 2009, doi: 10.1109/CSE.2009.387.
- [118] D.-R. Tsai, A. Chang, S.-C. Chung und Y. S. L., „A proxy-based real-time protection mechanism for social networking sites,“ in *Security Technology (ICCST), 2010 IEEE International Carnahan Conference on*, vol., no., pp.30-34, URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5678686&isnumber=5678668>, 5-8 Oct. 2010, doi: 10.1109/CCST.2010.5678686.
- [119] klicksafe Redaktion, „Modul Freundeslisten,“ [Online]. Available: <http://www.klicksafe.de/materialien/>. [Zugriff am 06 05 2012].
- [120] klicksafe Redaktion, „klicksafe.de - Modul Profileinstellungen und Inhalte, die du teilst,“ [Online]. Available: <http://www.klicksafe.de/materialien/>. [Zugriff am 06 05 2012].
- [121] klicksafe Redaktion, „www.klicksafe.de - Soziale Netzwerke,“ [Online]. Available: <http://www.klicksafe.de/themen/kommunizieren/soziale-netzwerke/was-sind-soziale-netzwerke/>. [Zugriff

am 06 05 2012].

- [122] WebMediaBrands, Inc., „Allfacebook.de - Happy Birthday Facebook,“ [Online]. Available: <http://allfacebook.de/news/happy-birthday-facebook-facebook-ist-jetzt-8-jahre-alt>. [Zugriff am 06 05 2012].