HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Herr
Daniel Meerwald

Analyse und Anatomie von Cyber-Angriffen

Mittweida, 2017

Fakultät Angewandte Computer- und
Bio-wissen-schaften

BACHELORARBEIT

Analyse und Anatomie von Cyber-Angriffen

Autor:
Herr

Daniel Meerwald

Studiengang:
IT-Sicherheit

Seminargruppe:
IF13WI-B

Erstprüfer:
Herr Prof. Dr. rer. nat. Dirk Labudde

Zweitprüfer:
Herr Prof. Dr. rer. nat. Christian Hummert

Einreichung:
Mittweida, 25.08.2017

Verteidigung/Bewertung:
Mittweida, 2017

Faculty Applied Computer Sciences &
Biosciences

BACHELOR THESIS

Analysis and anatomy of Cyber-Attacks

author:
Mr.

Daniel Meerwald

course of studies:
IT-Security

seminar group:
IF13WI-B

first examiner:
Herr Prof. Dr. rer. nat. Dirk Labudde

second examiner:
Herr Prof. Dr. rer. nat. Christian Hummert

submission:
Mittweida, 25.08.2017

defence/ evaluation:
Mittweida, 2017

Bibliografische Beschreibung:

Meerwald, Daniel:
Analyse und Anatomie von Cyber-Angriffen. - 2017. - V, 94 S.
Mittweida, Hochschule Mittweida, Fakultät Angewandte Computer- und Bio-wissen-schaften, Bachelorarbeit, 2017

Referat:

In der vorliegenden Arbeit wird das Thema Cybercrime umfangreich behandelt. Dabei wird unter anderem auf den klassischen Cyberangriff und auf das Thema Social Engineering eingegangen. Die Problematik der Cybercrime, wird für jeden leicht verständlich erklärt. Dabei wird eine neue und allgemeine Anatomie von Cyberangriffen erarbeitet und es werden aktuelle Beispiele diskutiert. Ziel der Arbeit ist es, ein Sicherheitsbewusstsein zu schaffen mit dem jeder sich sicherer in der digitalen Welt bewegen kann.

Inhalt

Abbildungsverzeichnis

Abkürzungsverzeichnis

AES	Advanced Encryption Standard
APT	Advanced Persistent Threat
BfV	Bundesamt für Verfassungsschutz
BK	Bundeskriminalamt (Österreich)
BKA	Bundeskriminalamt (Deutschland)
BSI	Bundesamt für Sicherheit in der Informationstechnik
CCC	Chaos Computer Club
DIVSI	Deutsches Institut für Vertrauen und Sicherheit im Internet
DIW	Deutschen Instituts für Wirtschaftsforschung
DNS	Domain Name System
HPI	Hasso Plattner Institut
IDS	Intrusion Detection System
IoD	Institute of Directors
IoT	Internet of Things
IPS	Intrusion Prevention System
IP	Internetprotokoll
IT	Informationstechnik
IVBB	Informationsverbund Berlin-Bonn
LAN	Local Area Network
LKA	Landeskriminalamt
MADICS	Maryland Adolescent Development In Context Study
NSA	National Security Agency
PC	Personal Computer
PKS	Polizeiliche Kriminalstatistik
SSL	Secure Sockets Layer

TAN	Transaktionsnummer
TZ	Teilzyklus
URL	Uniform Resource Locator
UZ	Unterzyklus
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

1 Übersicht

1.1 Vorwort

Der Moderne Cyber-Angriff besteht aus mehr als nur ein paar Zeilen Code. Eine Studie des Deutschen Instituts für Vertrauen und Sicherheit im Internet, kurz DIVSI, stellte bereits 2013 fest, dass sich das Vertrauen der Deutschen in die Sicherheit im Internet stark verschlechtert hat.[1]

Allgemein bekannt ist, dass die Anzahl der Internetnutzer und der Onlinedienste seit Beginn des digitalen Zeitalters stark gestiegen ist, damit allerdings auch die Anzahl der Kriminellen, die das Internet ausnutzen, um sich zu bereichern.

Die Grafik rechts zeigt, dass die Anzahl der Schadprogramme für Windows jährlich steigt. 2013 zu 2014 verdoppelte sich ihre Anzahl beinahe. Mit der erhöhten Anzahl von Schadwarevarianten vermehren sich auch ihre Verbreitungsmöglichkeiten. Im Internet finden sich heute demnach viel mehr Gefahren als zu Beginn des Internetzeitalters. Mit dem Anstieg der Gefahrenquellen im Internet senkt sich das Sicherheitsgefühl der Nutzer. Um dieser Entwicklung entgegenzuwirken, muss Internetkriminalität für die Täter unattraktiv gemacht werden.

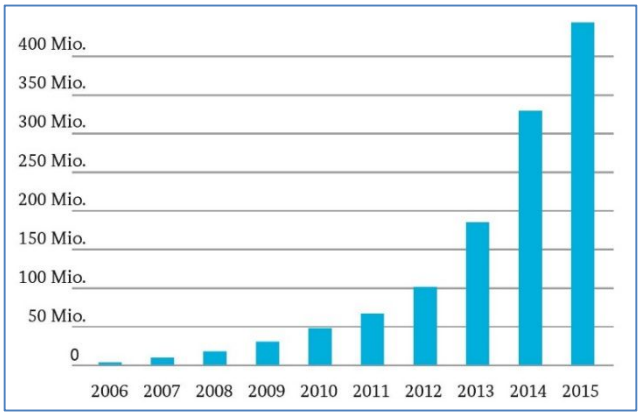


Abbildung 1: Anzahl bekannter Windows-Schadprogrammvarianten
Quelle: Quelle: BKA Bundeslagebild 2015 (Abschnitt 2.4 – Seite 17)

Niemand, der digitale Medien nutzt, kann absolut sicher sein, denn absolute Sicherheit gibt es in der IT-Welt nicht. Doch damit der Nutzer sich selbst so gut wie möglich schützen kann, muss er bestmöglich über die Methoden und Möglichkeiten der Angreifer Bescheid wissen. Um eine angemessene Sicherheit zu erreichen, muss er dem Angreifer sowohl online als auch offline so wenig Angriffsfläche wie möglich bieten. Deshalb behandelt diese Arbeit die Internetkriminalität, auch Cybercrime genannt, umfassend und allgemein verständlich.

In dieser Arbeit werden viele Fachwörter verwendet. Sofern diese für das Verständnis des Inhalts an der betreffenden Stelle essentiell sind, werden diese an Ort und Stelle erklärt.

[1] DIVSI, PRISM und die Folgen: Sicherheitsgefühl im Internet verschlechtert

Viele Begriffe sind bereits in die Umgangssprache übernommen worden und normalerweise mit einer gewissen Vorstellung konnotiert. Diese Wörter werden oft nur knapp, wenn überhaupt, erklärt. Für ein besseres Verständnis und um trotzdem den Lesefluss nicht zu stören, befindet sich deshalb am Ende dieser Arbeit ein Glossar-Kapitel, in dem all diese Begriffe noch einmal kurz erklärt werden. Des Weiteren befindet sich am Ende der Arbeit ein Index-Kapitel, in dem alle wichtigen Wörter mit den jeweiligen Seiten aufgezählt sind, auf denen diese erklärt oder in Zusammenhang gesetzt werden.

Auf die gleichzeitige Verwendung weiblicher und männlicher Sprachformen wird zugunsten der Lesbarkeit verzichtet. Die Personenbezeichnungen gelten dennoch für beide Geschlechter.

1.2 Motivation, Ziele und Kernfragen

Die Informationstechnik und damit auch die IT-Sicherheit gehört zum täglichen Leben. Die meisten Menschen sind auf die Nutzung dieser Technologien und des Internets angewiesen. Trotzdem interessieren sich die meisten Menschen nicht dafür, wie sie sicher mit dem Internet und den dazugehörigen Geräten umgehen können. Es scheint als sei es ihnen zu kompliziert oder der Sinn der Sicherheit nicht bewusst. Nutzer schrecken aus verschiedensten Gründen vor der Auseinandersetzung mit dem Thema der IT-Sicherheit zurück. Diese Einstellung ist grundlegend unangebracht und nicht zweckmäßig in einer sich rapide entwickelnden Gesellschaft wie der heutigen, die hauptsächlich auf Informationstechnik gründet.

Die Grundmotivation der Arbeit ist es, aus Verteidigungsgründen, einen leicht verständlichen Überblick über das Thema der IT-Sicherheit zu geben. Der „Schwarzmarkt“ mit Software zum Hacken, Hackerdiensten und geklauten Daten[2] explodiert geradezu. Es ist für Angreifer zurzeit besonders einfach, kriminelle Taten zu begehen, da sie oft auf ungeschulte und naive Opfer treffen.

Bei dieser Lage und einer rasant voranschreitenden technischen Entwicklung, besonders in der Komplexität von Informationssystemen[3], ist es nachvollziehbar, wenn der Mensch mittlerweile als größte Sicherheitslücke des IT-Systems gilt. In der IT-Welt wird für das ausnutzen dieser menschlichen Lücke oft das Wort „Social Engineering“ verwendet. Deshalb wird in dieser Arbeit verstärkt auf das Thema eingegangen.

Im Bericht des Bundesamt für Sicherheit in der Informationstechnik, kurz BSI, von 2014 wird eine klare Aussage über Social Engineering getroffen:

---

[2] BKA, Bundeslagebild 2015 (Abschnitt 2.4 – Seite 11)

[3] Piyush Michael: Quora - Does Moore's law apply to GPUs? Or only CPUs?

„Social Engineering ist elementarer Bestandteil gezielter Angriffe.“[4]

An anderer Stelle heißt es:

„[…] die klassischen Abwehrmaßnahmen verlieren weiter an Wirksamkeit. […] IT-Sicherheit muss als Gesamtkonzept verstanden und umgesetzt werden, wozu auch die Einbeziehung des Nutzers gehört.“[5]

Daher wird sich in den folgenden Kapiteln zum einen mit den klassischen Methoden des Cyber-Angriffs befasst, zum anderen mit dem modernen Cyber-Angriff, der oft eine Mischform aus Methoden des Social Engineering und der klassischen Angriffsmethoden ist. Es soll auf einer breiten Basis grundlegend informiert werden. Die Informationen über Cyber-Angriffe des 21. Jahrhunderts und somit auch über Social Engineering, sollen in einer neuen, bis jetzt nicht vorhandenen Form, zusammentragen und neu interpretiert werden. Dabei werden die Begriffe „Cyber-Angriff“ sowie „Social Engineering“ der heutigen Zeit angemessen definiert und analysiert.

In dieser Arbeit soll zum Teil die Angst vor dem abstrakten „Ungeheuer“ der Informatik genommen werden. Denn es gibt Möglichkeiten, wie sich jeder, auch ohne IT-Kenntnisse, sicherer als zuvor im Internet bewegen und eine Vorstellung vom Sicherheitskonzept der Informationstechnik erlangen kann.

Die **Ziele der Arbeit** sind folgende:

- Verständliche Informationen zur Lage der IT-Sicherheit bieten.
- Den modernen Cyber-Angriff darstellen.
- Über Social Engineering aufklären.
- Möglichkeiten zum Schutz aufzeigen, die jeder ohne großen Aufwand nutzen kann.
- Die Schaffung eines Sicherheitsbewusstseins, welches vor Cyber-Angriffen schützen kann und aufzeigen, wie dieses erreicht werden kann.

Die **Kernfragen,** mit der sich diese Arbeit in diesem Zuge beschäftigen wird, sind folgende:

- Was beinhaltet der moderne Cyber-Angriff und wie ist er aufgebaut?
- Was bedeutet Social Engineering heute?
- Wie kann man sich effektiv vor Cyber-Angriffen schützen?

Für eine effektive Verteidigung der eigenen Sicherheit gilt dasselbe Kredo, wie im Studium der IT-Sicherheit:
Wir können nur sinnvolle Gegenmaßnahmen zur Verteidigung erstellen, wenn wir genau

---

[4] BSI, Die Lage der IT-Sicherheit in Deutschland 2014 (Abschnitt 2.2.5 - Seite 19)

[5] BSI, Die Lage der IT-Sicherheit in Deutschland 2016 (Abschnitt 1.2.1 – Seite 19)

wissen, wie wir angegriffen werden, wie der Hacker (beziehungsweise der Social Engineer) denkt und was für Methoden er benutzt.
Daher wird diese Arbeit auch das Vorgehen des Angreifers beleuchten.

Da bekannt ist, dass häufig nur die ersten paar Seiten einer Arbeit gelesen werden, wird bereits an dieser Stelle einen Appell an das Bildungssystem und alle Eltern gerichtet. Denn sie haben es versäumt einen der mittlerweile wichtigsten Aspekte des modernen Lebens, sowie den richtigen und sicheren Umgang mit ihm, den Kindern bereits im Schulalter beizubringen. Wenn einem Kind der Zugang zu diesen Medien erlaubt wird, muss ihm im gleichen Zuge auch ein sicherer Umgang mit diesen Medien angelernt werden. Dies gilt auch für Erwachsene. Computer in jeder Form sowie das Internet sind aus der heutigen Zivilisation und Kultur nicht mehr weg zu denken, nicht ohne Grund bezeichnet man gemeinhin das aktuelle Zeitalter als „Informationszeitalter“ und nicht ohne Grund gibt es den Begriff „Internetkultur“.

1.3 Zielgruppe

Psychologieinteressierte:

Unter anderem werden grundlegende Prinzipien der Psychologie in Bezug auf Social Engineering besprochen. Diese Prinzipien werden für jeden Psychologieinteressierten interessante Denkanstöße bieten.

Unternehmer:

Als Unternehmer ist das eigene Unternehmen potentielles Ziel von Cyber-Angriffen. 2003 gab es eine Studie, in der Mitarbeiter zu Cyber-Angriffen im Unternehmen befragt wurden. 32 % gaben an, dass es nicht einmal Firmenrichtlinien dazu gäbe wie Kundendaten geschützt werden sollten.[6] Es bleibt zu hoffen, dass sich diese Zahl heute verbessert hat.

Penetrationstester und Audit interessierte:

Hacker und Penetrationstester die Gruppen sind, die Social Engineering besonders sicherheitsbezogen einsetzen. Da sie im Folgenden oft als Beispiele verwendet werden, verschafft diese Arbeit auch einen guten Überblick über die Arbeit eines Penetrationstesters beziehungsweise gibt einen Überblick über den Ablauf eines Audits.

Internetnutzer:

Als normaler Internetnutzer ist man Hauptziel von vielen ungerichteten Cyber-Angriffen. Der Verband der Internetwirtschaft e. V. (ECO) berichtet beispielsweise, dass im Jahr 2015 auf

[6] Joseph Ansanelli, Consumer Data Security Survey Highlights

38 % der vom Anti-Botnet-Beratungszentrum gescannten Rechnern Botnetz-Schadsoftware gefunden wurde.[7] Jeder Internetnutzer sollte über ein gewisses Maß an Sicherheitsbewusstsein verfügen. Was das genau ist und wie man es erreichen kann, wird im Verlauf dieser Arbeit besprochen.

1.4 Überblick

Im ersten Hauptteil der Arbeit wird sich intensiv mit dem Thema „Cybercrime“ auseinandergesetzt. Dabei wird zunächst definiert was Cybercrime ist und was Hacker sind. Danach folgt eine statistische Betrachtung zur Cybercrime. Anschließend wird die Anatomie eines typischen Audits, einem simulierten Cyber-Angriff zur Überprüfung der Sicherheit, sowie eines Cyber-Angriffs genauer beleuchtet. Zum Schluss des ersten Hauptteils der Arbeit werden typische Angriffe erläutert sowie erste Hinweise zum Schutz vor diesen gegeben.

Im zweiten Hauptteil der Arbeit wird näher auf das Thema Social Engineering eingegangen. Zunächst wird der Begriff definiert und der Zusammenhang mit dem Cyber-Angriff herausgestellt. Danach folgen die Prinzipien des Social Engineering sowie eine Liste typischer Angriffe. Zum Schluss wird Social Engineering noch einmal kritisch und moralisch betrachtet.

Im dritten Hauptteil wird das Sicherheitsbewusstsein behandelt und erläutert, warum es notwendig ist. In diesem Kapitel werden auch einfache und praktische Möglichkeiten zum Schutz vor Cyber-Angriffen geboten.

Im vierten Hauptteil der Arbeit werden Beispiele moderner Cyber-Angriffe analysiert und mit den vorangegangenen Teilen der Arbeit in Verbindung gebracht. Dabei werden Spekulationen und Schlussfolgerungen erstellt sowie anatomische Abläufe und die gemachten Fehler aufgezeigt. Anschließend werden Möglichkeiten genannt wie man die Angriffe hätte verhindern können.

Im fünften und letzten Hauptteil der Arbeit wird ein Fazit gezogen.

[7] ECO, über Anti-Botnetz-Beratungszentrum

2 Cybercrime

Cyber-Angriffe sind für die meisten Menschen etwas nicht direkt Greifbares, obwohl jeder bereits mehrfach Opfer von Cybercrime geworden ist. Deshalb wird in diesem Kapitel zunächst definiert, was Cybercrime ist und etwas Statistik herangezogen, damit das volle Ausmaß dieses Bereiches verstanden werden kann.
Anschließend wird der Cyber-Angriff genauer betrachtet und jeder Bereich einzeln beleuchtet. Dafür wird der Zyklus, nach dem professionelle Hacker ihre Taten begehen erläutert.

2.1 Definition

Das Bundeskriminalamt (BKA) definiert Cybercrime, zu Deutsch „Internetkriminalität", folgendermaßen:

„Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik begangen werden."[8]

Kurzgesagt ist Cybercrime im allgemeinen also jegliche Kriminalität, die mit Informationstechnologien begangen wird, wobei es große Unterschiede in deren Ausprägung und Professionalität gibt.

„Cybercrime im engeren Sinne" umfasst laut BKA nur *„[…] die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten […]"*[9]

Cybercrime ist laut BKA einer der wenigen Deliktbereiche mit einer *„kontinuierlich steigende Kriminalitätsentwicklung"*[10]. Dies lässt sich durch den seit den 1970ern anhaltenden technologischen Aufschwung im Bereich der Personal Computer (PCs) erklären.[11] Ironischerweise verdanken wir die Entwicklung persönlicher Computer, die jeder bei sich zu Hause stehen haben kann und die für den Normalverbraucher preiswert genug sind, um sie zu

[8] BKA, Definition Internetkriminalität/ Cybercrime

[9] BKA, Definition Internetkriminalität/ Cybercrime

[10] BKA, Definition Internetkriminalität/ Cybercrime

[11] Timeline of Computer History

erwerben, zumindest teilweise Hackern. Außer ihnen und einigen Technikbegeisterten erkannten nur wenige, dass Computer ein schier endloses Potential haben.[12]

2.1.1 Hacker

Hacker sind in erster Linie Personen, deren tiefes Verständnis für Computer und Programmierung über das des Durchschnitts weit hinausgehen und die somit die Beschränkungen der Programme, durch welche Computer funktionieren, überschreiten, verändern und neu definieren können. Als dies in der Frühzeit der Computer den ersten „Hackern“ bewusst wurde, stellten sie eine Hackerethik auf, die den Umgang mit den Computern regeln und Grenzen aufzeigen sollte.[13]

2.1.1.1 Hackerethik

Der Chaos Computer Club schreibt zur Hackerethik Folgendes:
„*Die ethischen Grundsätze des Hackens – Motivation und Grenzen:*

- *Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.*
- *Alle Informationen müssen frei sein.*
- *Mißtraue Autoritäten – fördere Dezentralisierung.*
- *Beurteile einen Hacker nach dem, was er tut, und nicht nach üblichen Kriterien wie Aussehen, Alter, Herkunft, Spezies, Geschlecht oder gesellschaftliche Stellung.*
- *Man kann mit einem Computer Kunst und Schönheit schaffen.*
- *Computer können dein Leben zum Besseren verändern.*
- *Mülle nicht in den Daten anderer Leute.*
- *Öffentliche Daten nützen, private Daten schützen.*

Die Hackerethik ist nur bedingt einheitlich definiert. Es gibt eine ursprüngliche Version aus dem Buch "Hackers" von Steven Levy (ISBN 0-440-13405-6). Unstrittig ist insofern, dass die ursprüngliche Version aus dem MIT-Eisenbahnerclub (Tech Model Railroad Club) kommt und demnach aus einer Zeit stammt, in der sich verhältnismäßig viele Leute wenige Computer teilen mussten und entsprechende Überlegungen zum Umgang miteinander und der Materie sinnvoll waren.“[14]

---

[12] Steven Levy, Hackers: Heroes of the Computer Revolution (Kapitel 2 Die Hackerethik - Seite 27 ff.)

[13] Steven Levy, Hackers: Heroes of the Computer Revolution (Kapitel 2 Die Hackerethik - Seite 27 ff.)

[14] Chaos Computer Club: Hackerethik

Die letzten beiden Einträge wurden vom Chaos Computer Club hinzugefügt, um die Hackerethik besser an die heutigen Umstände anzupassen.[15]

Der Tech Model Railroad Club ist eigentlich ein Modelleisenbahn-Club, welcher sich mit der Automatisierung beschäftigte. Er gilt als eine der Geburtsstätten der Hacker-Kultur.[16] Die Grundsätze der Hackerethik sollen die Nutzer und Hacker vor „Schandtaten" bewahren. Nach der eigentlichen Hackerkultur und Hackerethik stellen Hacker keine bösartigen „Nerds" dar, sondern eine Randgruppe motivierter Programmierer, mit enormen Wissen über Computer und Programmiersprachen.

2.1.1.2 Hackerfarben

Je nachdem, ob Hacker dieser Ethik folgen und infolge dessen eher als „gut" oder „böse", im Sinne von „gut" oder „schlecht" für die Gesellschaft, angesehen werden können, werden den Hackern heute 3 „Hut-Farben" zugewiesen. Der Black-Hat, Grey-Hat und White-Hat. Darüber hinaus werden in diesem Unterkapitel die Auditoren und Scriptkiddies erklärt und von den Hackern abgegrenzt.

Black-Hat:
Black-Hats sind bösartige Hacker, die der Hackerethik nicht entsprechen oder zumindest teilweise und regelmäßig mit ihr brechen. Black-Hats zeichnen sich dadurch aus, dass sie, wenn sie eine Lücke in der Software entdecken, diese zu ihrer eigenen Bereicherung nutzen.[17] Black-Hats werden am häufigsten als „Hacker" bezeichnet und entsprechen dem, was der normale Benutzer sich unter einem Hacker vorstellt. Dies ist dem Umstand geschuldet, dass Hacker in den Medien fast nur negativ auffallen und dort nur der Begriff „Hacker" benutzt wird, ohne nähere Definition oder Abgrenzung. Black-Hats sind die Sorte Hacker, die hauptsächlich professionelle Cyber-Angriffe verüben und vor denen man sich am meisten schützen muss.

Grey-Hat:
Grey-Hats sind nicht genau einzuordnen. Sie halten sich oft an die Hackerethik, brechen aber aus eigenen Interessen oder nach Belieben mit ihr. Sie können aus diversen Motiven agieren und sind, in ihrer Handlungsweise, manchmal eher als „gut" und manchmal eher als „schlecht" anzusehen.[18]

---

[15] Chaos Computer Club: Hackerethik

[16] Steven Levy, Hackers: Heroes of the Computer Revolution (Kapitel 1 The Tech Model Railroad Club - Seite 3 ff.)

[17] Chris Hoffman, How-To Geek: Hacker Hat Colors Explained: Black Hats, White Hats, and Gray Hats

[18] Chris Hoffman, How-To Geek: Hacker Hat Colors Explained: Black Hats, White Hats, and Gray Hats

White-Hat:
White-Hats halten sich streng an die Hackerethik und andere moralische Grundsätze. Der White-Hat deckt seine gefundenen Softwarelücken auf und meldet sie zunächst den zuständigen Softwareherstellern, damit diese sie schließen können.[19] White-Hats nutzen ihre Fähigkeiten demnach ausschließlich für das „Gute“ und versuchen durch ihr Handeln möglichst niemandem zu schaden und wenn möglich, Schaden zu verhindern.

Auditor:
Neben den Typischen Hackern gibt es noch eine weitere Gruppe, die oft mit ihnen in Verbindung gebracht oder mit ihnen verwechselt wird. Die Auditoren oder auch Penetrationstester genannt. Sie sind Sicherheitsexperten, die angeheuert werden, um Unternehmen, sowohl technisch als auch menschlich, auf ihre Sicherheit zu prüfen. Ihre Aufgabe ist es, von allen Seiten einen Angriff auf ein Unternehmen zu simulieren und die gefundenen Sicherheitslücken aufzudecken. Ziel ist es, die Sicherheitslücken zu schließen sowie anschließend das Personal zu schulen.[20] White-Hats können auch Auditoren sein, Auditoren sind aber nicht zwingend White-Hats. Ein Auditor besitzt oft sowohl Skills eines Hackers als auch eines Social Engineers. Häufig sind die Kenntnisse im eigentlichen „Hacken“ jedoch nicht so tiefgehend wie bei Black-, Grey-, und White-Hats.

Scriptkiddie:
„Scriptkiddies“ sind Hacker, die im eigentlichen Sinne keine sind. Sie sind Programmierer, deren Wissen über die Materie eher durchschnittlich, wenn nicht unterdurchschnittlich ist und denen viel Grundlagenwissen fehlt. Sie verüben häufig einzelne Attacken, oft rein zum Vergnügen und bedienen sich dabei hauptsächlich vorgefertigten Skripten, sowie Angriffen die automatisiert sind oder nur geringe eigene Anpassung benötigen. Sie sind im Allgemeinen nicht in der Lage einen Angriff selbst zu programmieren oder Sicherheitslücken zu entdecken. Scriptkiddies sind eine Erscheinung die der Vereinfachung von Angriffen in Frameworks geschuldet ist, welche sehr leicht zu bedienen sind.[21]

2.1.2 Cyber-Angriff

Laut Duden ist ein Cyber-Angriff ein „*von außen (durch einen einzelnen Hacker, durch eine Institution o. Ä.) zum Zweck der Sabotage oder der Informationsgewinnung geführter Angriff*

[19] Chris Hoffman, How-To Geek: Hacker Hat Colors Explained: Black Hats, White Hats, and Gray Hats

[20] Christopher Hadnagy, Die Kunst des Human Hacking (Kapitel 9.6.1 – Seite 432, Kapitel 9.6.3 – Seite 434 f., Kapitel 4.3.2 – Seite 132 f.)

[21] Heise online: The Kids are out to play

auf ein Computernetzwerk".[22] Diese Definition ist recht knapp und umfassend gehalten. Daher fallen alle im den Unterkapiteln 2.4.1 und 2.4.2 geführten Methoden bereits für sich unter diese Definition, was zur Folge hat, dass ein Cyber-Angriff aus mehreren Cyber-Angriffen bestehen kann.

2.2 Statistische Betrachtung

2014 verwendeten etwa 80 % aller Nutzer ein Windows Betriebssystem, heute sind es etwa 72 %.[23] Cyberkriminelle konzentrieren sich vorwiegend auf dass am meisten verwendete Betriebssystem, um möglichst viel Erfolg zu haben. Im Jahr 2014 kamen täglich etwa 300.000 neue Schadprogrammvarianten, zu den bestehenden, hinzu. [24]

Alleine in Deutschland ereignen sich monatlich mindestens eine Millionen Infektionen durch Schadprogramme auf dem PC, bei Mobilen Endgeräten wird sogar von 3 Millionen ausgegangen.[25] Einer 2015 erstellten Studie des Deutschen Instituts für Wirtschaftsforschung (DIW) zufolge werden jährlich rund 14,7 Millionen Cyberverbrechen begangen, mit einem Gesamtschaden von etwa 3,4 Milliarden Euro.[26]

Im Bereich „Computerbezogene Kriminalität" wird von einem extrem großen Dunkelfeld von mindestens 91 %[27] ausgegangen.[28] Dies bedeutet, dass 91 % aller Straftaten den Behörden komplett verborgen bleiben. Diese Verbrechen gehen somit in keine Kriminalstatistik ein. Warum nur 9 % aller Internetverbrechen angezeigt werden, wird in Unterkapitel 2.2.1 näher besprochen.

Die Polizeiliche Kriminalstatistik gibt aufgrund diverser Einschränkungen keine verlässlichen Auskünfte über die absoluten Zahlen und die genaue Aufteilung von Cyberverbrechen. Allerdings lässt sich anhand von Abbildung 2 erahnen welche Tendenz Cybercrime aufweist. Es ist deutlich zu erkennen, dass etwa 44 % der aufgelisteten Verbrechen auf den Bereich des „Computerbetrug" entfallen. Dies ist insofern relevant, da sich ein Nutzer vor

[22] Duden: Cyberangriff

[23] Statista, Marktanteile der führenden Betriebssysteme in Deutschland von Januar 2009 bis Mai 2017

[24] BKA, Bundeslagebild Cybercrime 2014 (Abschnitt 2.3 – Seite 9)

[25] BKA, Bundeslagebild Cybercrime 2014 (Abschnitt 2.3 – Seite 9)

[26] DIW, Tatort Internet: Kriminalität verursacht Bürgern Schäden in Milliardenhöhe

[27] LKA, Niedersachsen, Abschlussbericht Dunkelfeldstudie 2013 (Tabelle 32 – Seite 60)

[28] BKA, Bundeslagebild Cybercrime 2014 (Abschnitt 2.2 – Seite 5)

Betrug effektiver schützen kann, als vor Angriffen, die er nicht wahrnehmen oder nicht begreifen kann. Das bedeutet, dass jeder Benutzer effektiv daran arbeiten kann, seine private Sicherheit zu verbessern. In Kapitel 4 wird diese Thematik näher erläutert.

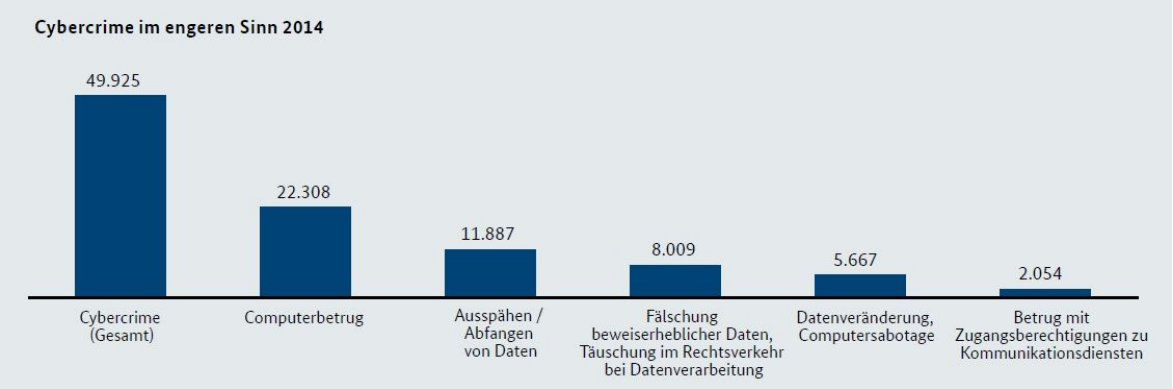


Abbildung 2: Cybercrime im engeren Sinn 2014 - Auszug aus der Polizeilichen Kriminalstatistik

Quelle: BKA Bundeslagebild 2014 (Abschnitt 2.1 – Seite 4) vergleiche
Definition Cybercrime Unterkapitel 2.1.2

Um zu verdeutlichen, wie verbreitet Schadware ist und wie häufig sich ein durchschnittlicher Internetnutzer infiziert, folgt eine Hochrechnung aus den Angaben des BKA. Geräte des „Internet of Things“ sind in dieser Statistik nicht berücksichtigt[29]:

79,1% aller erwachsenen Personen nutzen das Internet, das entspricht etwa 55,6 Millionen Personen über 14 Jahren. Monatlich ereignen sich mindestens eine Million Infektionen an PCs und mindestens 3 Millionen Infektionen an mobilen Endgeräten. Bei durchschnittlich 2,8 Geräten, die ein Nutzer besitzt, ergeben sich insgesamt 155,68 Millionen Geräte. Jeder Nutzer ist an durchschnittlich 5,9 Tagen in der Woche online und im Schnitt dabei täglich 166 Minuten. Das bedeutet, dass ein Monat für einen durchschnittlichen Nutzer in der Rechnung 23,6 Tage besitzt und ein Tag nur 166 Minuten beträgt, denn ein Nutzer kann sich hauptsächlich während der Onlinezeit infizieren. Um diese Schätzung nicht unnötig kompliziert zu machen und weil nicht erwähnt wird, wie sich die 2,8 Geräte auf mobile und stationäre Endgeräte verteilen, werden die Infektionen zusammengezählt und somit die Infektionschance für ein beliebiges Gerät eines Benutzers ausgerechnet. Darüber hinaus existieren keine Angaben zu Mehrfachinfektionen, weshalb diese in der folgenden Rechnung ignoriert werden. Es wird also davon ausgegangen, dass etwa vier Millionen Geräte pro Monat infiziert werden, ungeachtet der möglichen Mehrfachinfektionen.

Für die Infektionschance pro Tag bedeutet dies folgendes $\frac{\frac{4.000.000}{23,6}}{155.680.000} = \frac{125}{114814}$. Weiter wird mit der Gegenwahrscheinlichkeit gerechnet, also der Chance, dass ein Nutzer sich nicht infiziert, um die eigentliche Chance pro Benutzer pro Tag zu erhalten. Das sieht dann wie folgt aus: $1 - \left(1 - \frac{125}{114814}\right)^{2,8} = 3{,}0454 \ldots * 10^{-3}$. Dies entspricht einer Infektionschance von etwa 0,3% pro Tag pro Nutzer.

[29] BKA, Bundeslagebild Cybercrime 2014 (Abschnitt 3 – Seite 12 f.)

Da ein Tag 166 Minuten online entspricht und die Statistik auf eben diese Zahlen zurückgeht, bedeutet dies für Nutzer, die weniger als 166 Minuten am Tag online sind, eine geringere Chance, dass ein Gerät infiziert wird. Für Nutzer, die mehr online sind, ist die Chance entsprechend höher. Da keine exakten Zahlen vorliegen, kann davon ausgegangen werden, dass die eigentliche Infektionschance im Jahr 2014, pro 166 Minuten Onlinezeit über 0,3 % lag, je nach persönlichem Sicherheitsbewusstsein der Nutzer.
Heute im Jahr 2017 ist die Infektionschance vermutlich noch höher, da Cybercrime, wie bereits zu Beginn des Unterkapitels 2.1 erwähnt, eines der stetig wachsenden Kriminalitätsfelder ist. Was Sicherheitsbewusstsein bedeutet und wie die Chance sich zu infizieren möglichst gering gehalten werden kann, wird in Kapitel 4 näher erläutert.

Um die Zahlen noch etwas mehr in Relation zu setzen, folgt nun eine Hochrechnung, gesehen auf ein Jahr. Bei einer häufigen Wiederholung mit gleicher Wahrscheinlichkeit können schnell verblüffende Zahlen entstehen. Ähnlich dem Geburtstagsparadoxon, welches beweist, dass sich nur 23 Personen in einem Raum aufhalten müssen, damit die Wahrscheinlichkeit rund 50 % beträgt, dass 2 Personen in besagtem Raum, am selben Tag Geburtstag haben. Für diesen Anwendungsfall, der eine kumulierte binomiale Wahrscheinlichkeit ist, sieht das folgendermaßen aus: $\sum_{i=1}^{365}(365Ci) * 0{,}003^{i} * (1-0{,}003)^{n-i} = 0{,}66601\ldots$
Ein durchschnittlicher Internetnutzer infiziert sich also mit einer Wahrscheinlichkeit von 66,6% mindestens einmal im Jahr mit einem Virus oder Ähnlichem, an mindestens einem seiner Geräte. Dabei wird von einer Infektionschance von 0,3% am Tag ausgegangen, solange der Nutzer nur 166 Minuten pro Tag online ist.
Sofern die betreffenden Geräte regelmäßig überprüft werden, kann jeder sich nun selbst die Frage stellen, wie oft er bereits eine Infektion mit Schadware erlitten hat. Dabei ist zu beachten, dass die Rechnung eine Schätzung, mit Zahlen aus dem Jahr 2014, für den durchschnittlichen Internetnutzer, über 14 Jahre, ist.

Im Unterkapitel 1.4 wurde bereits erwähnt, dass 38 %, aller vom Anti-Botnet-Beratungszentrum gescannten PCs, Botnetz-Software gefunden wurde. Dabei wurde jedoch nicht erwähnt, ob einige Rechner mehrfach infiziert wurden, was allerdings zu vermuten ist. Botnetz-Software gewährt dem Hacker fast Vollzugriff auf den infizierten PC, um damit zum Beispiel Angriffe zu tätigen, Spam und Phishing Mails zu versenden oder ihn als Proxy zu nutzen. Diese Software kommt oft einem Vollzugriff auf den PC gleich und ist neben Krypto-Trojanern, die die Daten auf der Festplatte verschlüsseln, eine der unangenehmsten Schadsoftwares. Das Anti-Botnet-Beratungszentrum weist unter anderem darauf hin, dass die häufigste Ursache für die Infektionen veraltete Betriebssysteme der Betroffenen sind.[30]
Die Aktualität von Software ist für die IT-Sicherheit eine besondere Herausforderung, da oft

[30] ECO, über Anti-Botnetz-Beratungszentrum

jeder Nutzer selbst entscheiden kann, ob er Updates installiert und welche Betriebssystemversion er nutzt. In diesem Zusammenhang steht die IT-Sicherheit noch anderen Problemen gegenüber.

Das mooresche Gesetz, auch „Moore's law" genannt, besagt, dass sich die Komplexität von Schaltkreisen innerhalb eines bestimmten Zeitraumes verdoppelt.[31] Mit anderen Worten: Rechenleistung wächst exponentiell. Tatsächlich scheint es sogar so, dass durch die Entwicklung neuer Technologien, die nächste Technologie sogar noch schneller entwickelt wird.
Es wird heute so schnell neue Hardware entwickelt, dass die Softwareentwicklung nicht nachkommt. Durch diesen Umstand und weil neue Software, gerade für Unternehmen, sehr kostspielig ist, bleibt alte Software oft noch Jahre nach ihrem letzten Update in Verwendung und Kriminellen bleiben dadurch viele Angriffsvektoren offen.

Hinzu kommt, dass viele Nutzer veraltete Mobilgeräte verwenden, die keine sicherheitsrelevanten Updates mehr erhalten. Dies liegt vor allem daran, dass die Hersteller neue Smartphones nur noch etwa 2 Jahre lang mit Updates versorgen. Danach ist die Hardware, laut Hersteller, bereits so überholt, dass es sich für den Hersteller nicht mehr lohnt, das Gerät weiter zu unterstützen. Damit bleiben viele Lücken in den Systemen für immer offen. Hinzu kommt, dass mobile Geräte keine eingebauten Antivirensysteme besitzen und viele Nutzer auch keine nachinstallieren. Geübte Nutzer können, zumindest unter Googles Android Betriebssystem, sogenannte Custom-ROMs auf ihrem Smartphone installieren. Diese Versionen von Android werden von kleineren Gruppen von Entwicklern privat entwickelt und kostenlos zur Verfügung gestellt. Dadurch können auch alte Geräte weiterhin mit Updates versorgt werden. Nachteil dieses Vorgehens ist, der Verlust der Garantie des Smartphones sowie die Anfälligkeit der Software für Fehler, sogenannte Bugs.

Viel schlimmer als die Lage der mobilen Endgeräte ist die Lage im rapide wachsenden Markt des „Internet of Things" kurz IoT. Zum IoT gehören alle Geräte, die in irgendeiner Weise mit dem Internet verbunden sind, vom Drucker, über den Kühlschrank, bis hin zur W-LAN-Steckdose. Bis 2020 werden mehr als eine Billionen Endgeräte im IoT erwartet. Des Weiteren bleibt dem Nutzer eines Infizierten Gerätes des IoT momentan oft keine Möglichkeit, die Infektion zu überprüfen, geschweige denn diese zu beseitigen oder Sicherheitsupdates einzuspielen.[32] Geräte des IoT haben durch ihre große Zahl eine nicht zu unterschätzende Rechenleistung und können ebenso wie Botrechner für Cyber-Angriffe aller Art genutzt werden.

[31] Houghton Mifflin, Dictionary.com: Moore's Law

[32] BKA, Bundeslagebild 2015 (Abschnitt 3.2 – Seite 18)

Der Markt für IoT und der mobile Markt wachsen enorm schnell und bieten den Angreifern somit immer neue Angriffsflächen, die momentan nur minimal oder gar nicht verteidigt werden. Gegen die meisten Bedrohungen sieht auch das BKA die Sensibilisierung der Nutzer als effektive Gegenmaßnahme an.[33]

Eine Studie aus England gibt weitere Einblicke. In der Studie wurden anonym Mitglieder des „Institute of Directors“, kurz IoD, zu ihrem Unternehmen befragt. Das IoD ist eine englische Organisation, bestehend aus Unternehmern und Direktoren aus dem ganzen Land. Unter anderem gaben 12,5 % der Befragten an, im Jahr 2012 Opfer eines Computerverbrechens geworden zu sein.[34]

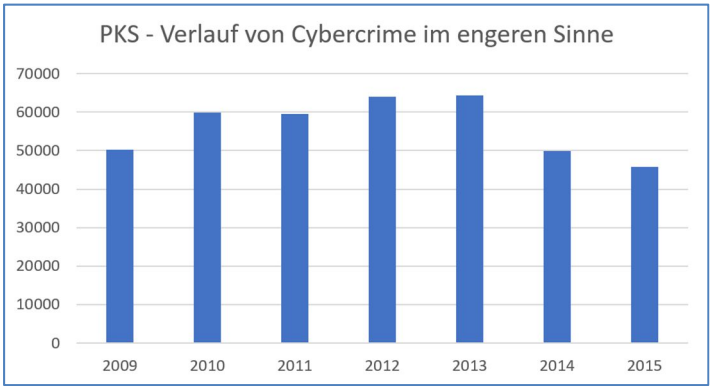


Abbildung 3: PKS - Verlauf von Cybercrime im engeren Sinne von 2009-2015

Quelle: Eigene Darstellung in Anlehnung an BKA, Bundeslagebild 2013 (Abschnitt 2.1 – Seite 5), BKA, Bundeslagebild 2014 (Abschnitt 2.1 – Seite 4), BKA, Bundeslagebild 2015 (Abschnitt 2.1 – Seite 6)

Betrachtet wird abschließend der Verlauf der absoluten Zahlen zu Cybercrime im engeren Sinne von 2009-2015, die bei der Polizei zur Anzeige gebracht wurden[35]. Zu erkennen ist ein Rückgang der in der Polizeilichen Kriminalstatistik verzeichneten Cyberverbrechen. Diese Entwicklung ist insofern verwunderlich, da die Anzahl an Schadwarevarianten weiter zunimmt und der Bereich, der Cybercrime laut BKA *„[…] wie in kaum einem anderen Deliktsbereich […]“*[36] kontinuierlich wächst. Daher ist zumindest in Betracht zu ziehen, dass sich das Dunkelfeld weiter vergrößert hat, was den anscheinend positiven Verlauf der Statistik erklären könnte.

2.2.1 Anzeigequote

Eine geringe Anzeigequote bei Cyberverbrechen kann für die Behörden ein großes Problem sein. Ihnen liegen keine Daten zum eigentlichen Ausmaß des Kriminalitätsfeldes vor,

[33] BKA, Bundeslagebild 2014 (Abschnitt 2.2 – Seite 5, Abschnitt 2.3 – Seite 7 und 10)

[34] IoD, Cyber Security: Underpinning the digital economy (The Institute of Directors Cyber Survey 2016 – key findings – Seiten 7-9)

[35] BKA, Bundeslagebild 2013 (Abschnitt 2.1 – Seite 5), BKA, Bundeslagebild 2014 (Abschnitt 2.1 – Seite 4), BKA, Bundeslagebild 2015 (Abschnitt 2.1 – Seite 6)

[36] BKA, Definition Internetkriminalität/ Cybercrime

was eine effektive Ressourcenverteilung zur Verbrechensbekämpfung im Internet erschwert. In diesem Unterkapitel wird diese Problematik näher beleuchtet und es werden Erklärungsmöglichkeiten geboten.

2.2.1.1 Sicht der Nutzer

Aus der Tabelle des LKA Niedersachsen geht hervor, dass nur etwa 9 % aller Cyberverbrechen zur Anzeige gebracht werden. Um genau zu sein, teilt sich diese Tabelle auf 3 Kriminalitätsfelder auf. Im Folgenden werden nun die jeweiligen Kriminalitätsfelder, wie vom LKA Niedersachsen bezeichnet, genannt und danach die jeweilige geschätzte Anzeigerate. [37]

- „Datenverlust durch Viren etc." - 5 %
- „Vertrauliche Daten aufgrund von E-Mail und Phishing" - 10 % (bezeichnet den Verlust dieser Daten aufgrund von Phishing zum Beispiel per E-Mail)
- „Betrug im Internet" - 24 %
- „Computerbezogene Kriminalität" insgesamt - 9 %

Aufgrund einer deutlich größeren Masse an Viren und Ähnlichem, wird hier wahrscheinlich eine größere Anzahl an Delikten vermutet, weshalb der gesamte Anteil der zur Anzeige gebrachten Kriminalfälle laut der Studie des LKA Niedersachsen 9 % beträgt. Genau genommen sind viele Arten des Phishings auch eine Art Betrug im Internet. Dadurch ist die Kategorien leider nicht klar definiert. Aus der Statistik kann geschlossen werden, dass möglicherweise ein Zusammenhang zwischen dem Aufwand der Anzeige und dem entstandenen Schaden besteht.
Das Hauptziel von Viren ist es nicht zwingend, Datenverlust zu erzeugen, weshalb diese Kategorie ohnehin nur ein verhältnismäßig kleines Feld abdeckt. Der Schaden, den Viren verursachen, drückt sich meist in einem zeitlichen Aufwand aus und Betroffene wissen oft bereits, dass eine Polizeiliche Anzeige mit hoher Wahrscheinlichkeit kein Ergebnis erzielen würde, da die Urheber solcher Schadware normalerweise nicht gezielt ermittelt werden können. Einen Rückgang der Aufklärungsquoten über die letzten Jahre, verzeichnen sowohl das BKA Deutschland[38] als auch das Bundeskriminalamt-Österreich(BK).[39] Verlorene Daten können von der Polizei, auch bei erfolgreicher Täterermittlung, nicht wiederhergestellt werden. Deshalb ist der örtliche Computerspezialist meist die erste und einzige Anlaufstelle der Opfer.
Alle der hier aufgeführten Verbrechen sind im Kern ungerichtete Angriffe gegen zufällige Opfer. Doch „Betrug im Internet", welches vom LKA Niedersachsen mit 24 % Anzeigequote

---

[37] LKA, Niedersachsen, Abschlussbericht Dunkelfeldstudie 2013 (Tabelle 32 – Seite 60)

[38] Bundeskriminalamt (BKA) - Michael Kraus (Kriminaloberrat), Vortrag Bekämpfung der Cybercrime aus Sicht des BKA (Folien 3 und 4)

[39] BKA - Michael Kraus, Kriminaloberrat, Vortrag Bekämpfung der Cybercrime aus Sicht des BKA (Seite 4), BK Österreich, Cybercrime Österreich Jahresbericht 2015 (Abschnitt: Zahlen und Fakten – Seite 12)

betitelt wurde, ist potenziell gefährlicher. Es ist oft ernüchternd, enttäuschend und peinlich für die Opfer. Diese fühlen sich durch den Betrug persönlich angegriffen und haben somit möglicherweise eine höhere Motivation das Verbrechen zur Anzeige zu bringen. Hinzu kommt, dass der Schaden der durch Betrug im Internet entsteht, meist ein direkter finanzieller Schaden ist und somit den Opfern viel realer erscheint, weshalb mehr Verbrechen in dieser Kategorie zur Anzeige gekommen sein könnten, als in den anderen.

2.2.1.2 Sicht der Unternehmen

Die Statistik des LKA Niedersachsen ist allgemein und deckt hauptsächlich Privatpersonen ab. Aber was ist mit Unternehmen? Hauptziel von professionellen Hackern sind Unternehmen, da bei ihnen die Gewinnspanne für die Kriminellen deutlich höher ist. Die im Unterkapitel 2.2 erwähnte Studie des IoD macht deutlich, wie groß das Dunkelfeld bei Unternehmen sein könnte. In der Studie wurden fast 1000 Unternehmer befragt und eines der Kernergebnisse der Studie besagt, dass nur 28 % der Cyber-Attacken der Polizei gemeldet wurden. Darüber hinaus sagten 49 % der Unternehmer aus, dass der größte entstandene Schaden aus der Unterbrechung des täglichen Geschäftes kommt.[40] Zunächst einmal ist festzustellen, dass nicht einmal ein Drittel aller Cyber-Angriffe gegen Unternehmen zur Anzeige kommen. Doch wie könnte sich diese geringe Quote erklären lassen?

1. Unternehmen haben einen Ruf zu verlieren. Bekanntwerden von Sicherheitslücken in Unternehmen senkt das Vertrauen der Kunden in das Unternehmen.
2. Eine Ermittlung im Unternehmen behindert den laufenden Betrieb, zusätzlich zum ohnehin schon entstandenen Schaden, durch den Stillstand des Betriebs, während und nach dem Cyber-Angriff.
3. Den Unternehmen ist bekannt, dass die Aufklärungsquote von professionellen Cyberverbrechen bei wenigen Prozent liegt.
4. Viele Angriffe bleiben zunächst komplett unentdeckt.

Für die meisten Unternehmen dürfte der Schaden im Vordergrund stehen. Sofern Ermittlungsaufwand eine finanzielle Einbuße aufgrund der Behinderung des Betriebs bedeutet und das Unternehmen einen nicht abschätzbaren Imageschaden erleidet, müssen diese Punkte für einen Unternehmer im Verhältnis zu den Erfolgschancen der Ermittlung stehen. Solange eine Ermittlung also weiteren Schaden verursacht, wird das Verbrechen nicht angezeigt. Solange die Aufklärungsrate professioneller Cyberdelikte also so gering bleibt, wie sie im Moment ist, darf nicht darauf gehofft werden, das Dunkelfeld verringern zu können. Im nächsten Abschnitt werden dazu die Zahlen der vergangenen Jahre aus der Polizeilichen Kriminalstatistik betrachten.

[40] IoD, Cyber Security: Underpinning the digital economy (The Institute of Directors Cyber Survey 2016 – key findings – Seiten 7-9)

2.2.2 Aufklärungsquoten

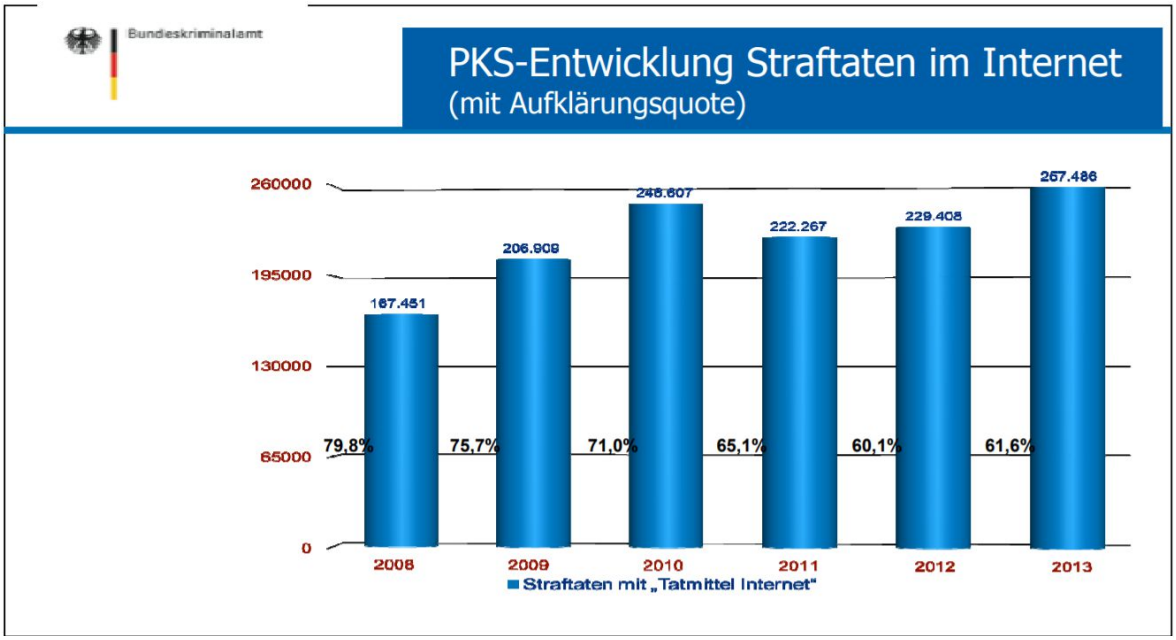


Abbildung 4: PKS - Entwicklung Straftaten im Internet mit Aufklärungsquote

Quelle: Bundeskriminalamt (BKA) - Michael Kraus, Kriminaloberrat, Vortrag Bekämpfung der Cybercrime aus Sicht des BKA (Folie 3)

Der hier zu sehende Auszug aus der Polizeilichen Kriminalstatistik zeigt den Verlauf der Straftaten mit dem Tatmittel Internet und der dazugehörigen Aufklärungsquote. Das Tatmittel Internet umfasst alle Straftaten die mit dem Computer oder dem Internet begangen wurden. Bei diesen Straftaten kann oft nicht von professionellen Angriffen gesprochen werden und ihre Aufklärungsquote ist entsprechend hoch. Das Tatmittel Internet erfasst neben Trojaner, Viren und Phishing, die anscheinend selten zur Anzeige kommen, hauptsächlich Betrugsfälle (74,5 %).[41] Betrugsfälle können von der Polizei gut verfolgt werden, da normalerweise eine direkte Interaktion der Täter und Opfer stattgefunden hat. Die Täter lernen stetig dazu, während die Strafverfolger dem Bereich der Cybercrime erst in den letzten Jahren mehr Aufmerksamkeit zukommen lassen haben. Dies könnte auch den Verlauf der Zahlen bis 2013 erklären. Die Anzahl der Taten ist über die Jahre Insgesamt gestiegen und die Aufklärungsquote gesunken. Eine Entwicklung die, bei steigender Komplexität der Schadware[42] sowie der Fallanzahl, nachvollziehbar ist. Mit Dunkelfeld beträgt die totale Aufklärungsquote etwa 5,5 %. Hierbei darf aber nicht vergessen werden, dass die Polizei nur Fälle bearbeiten und lösen kann, die ihr gemeldet werden. Allerdings lässt sich daraus schließen, dass sofern mehr Verbrechen zur Anzeige gebracht werden, die Beamten sehr wahrscheinlich schnell an ihre Leistungsgrenzen stoßen, da vermutlich nicht genügend Kapazitäten zur Verfügung stehen würden. Dieses Bild bestätigt sich, bei einem Blick auf die Cybercrimetabelle des BK-Österreich.

[41] BKA, Bundeslagebild 2015 (Abschnitt 2.1– Seite 17)

[42] BKA, Bundeslagebild 2013 (Abschnitt 2.2– Seite 10)

Cybercrime	Angezeigte Fälle	Geklärte Fälle	Aufklärungsquote
Jahr 2006	3 257	2 312	71,0 %
Jahr 2007	2 854	1 940	68,0 %
Jahr 2008	3 291	2 458	74,7 %
Jahr 2009	9 711	8 794	90,6 %
Jahr 2010	4 223	2 336	55,3 %
Jahr 2011	4 937	2 370	48,0 %
Jahr 2012	10 308	2 807	27,2 %
Jahr 2013	10 051	4 544	45,2 %
Jahr 2014	8 966	3 660	40,8 %
Jahr 2015	10 010	4 157	41,5 %
Veränderung	11,6 %	13,6 %	0,7 %-Punkte

Abbildung 5: Entwicklung der Anzahl der angezeigten und geklärten Fälle sowie der Aufklärungsquote von 2006 bis 2015

Quelle: BK Österreich, Cybercrime Österreich Jahresbericht 2015 (Abschnitt: Zahlen und Fakten – Seite 12)

Aus der Tabelle ist zu entnehmen, dass die Tendenz der Aufklärungsquoten über die Jahre fallend, sowie die Fallanzahl steigend ist. Ein Bild, das sich mit dem des BKA aus Deutschland deckt. Vom Jahr 2011 auf 2012 sind allerdings besonders viele Verbrechen zur Anzeige gekommen, die geklärten Fälle allerdings fast gleich geblieben. Dadurch sank die Aufklärungsquote stark ab. Dieser Umstand ist wahrscheinlich auf einen Personalmangel zurück zu führen. Mit einer Verdoppelung der zu bearbeitenden Fälle wurde vermutlich nicht gerechnet, obwohl im Jahr 2009 ein ähnlicher Sprung stattfand. Vermutlich wurden nach den Statistiken von 2010 und 2011 Kürzungen vorgenommen, die im Jahr 2012 für den extrem negativen verlauf der Bilanz verantwortlich sind. Das BK-Österreich macht leider zu diesen Umständen selbst keine Angaben. Kürzungen und jährliche Neuverteilungen des Etat, sind in vielen Ländern, wie der Bundesrepublik Deutschland, ganz normal. Die Verteilung des Etat geht dabei auf die Statistiken des jeweiligen Vorjahres oder der jeweiligen Vorjahre zurück.[43] Eine Erhöhung des Etat und damit auch der Beamten, zur Bearbeitung von beispielsweise Cybercrime, ist somit nur nach einer negativen Bilanz der Vorjahre zu rechtfertigen. Damit geht allerdings mindestens ein Jahr, in dem die Bilanz besonders schlecht ausfällt, einher, was das Vertrauen der Bürger senken könnte. Dieses kann in einem Rückgang der Anzeigequote resultieren, welcher in einem vermeintlichen Überschuss an Beamten und Etat resultieren würde. Daraus ergibt sich wiederum, bei einem erneuten Anstieg der Anzeigequote, eine weitere Unterbesetzung und so weiter. Eine solche Spirale ist unter anderem der Grund, warum, wie zu Beginn des Kapitels erwähnt, das Dunkelfeld für die Behörden ein großes Problem darstellen kann.

[43] Dr. Eggert Winter, Gabler Wirtschaftslexikon - Bundeshaushalt

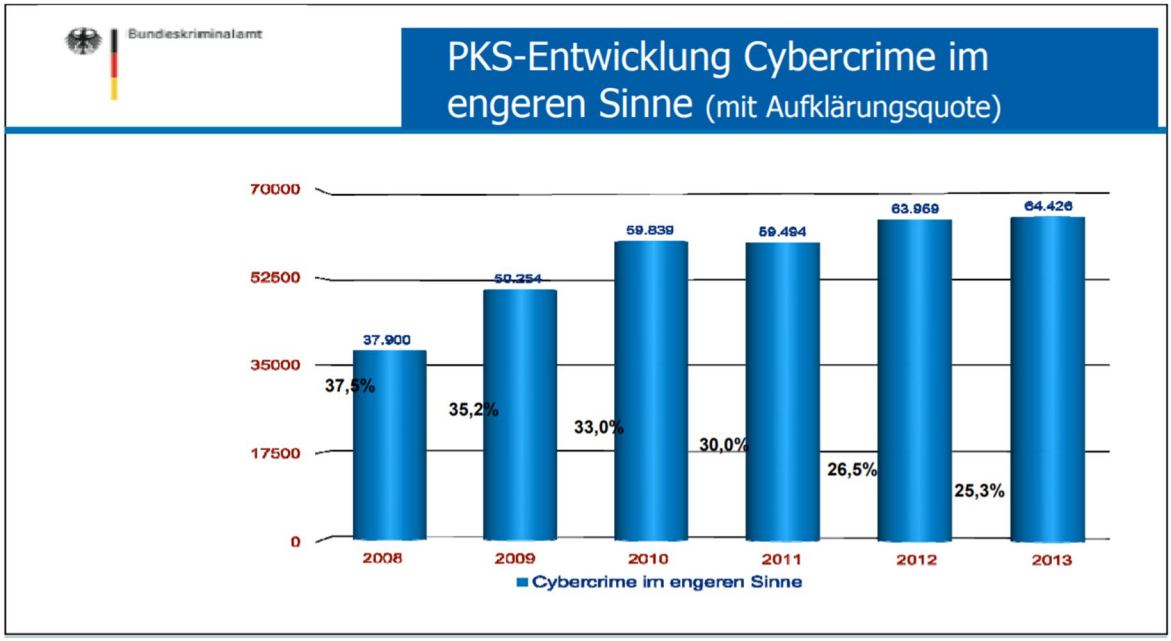


Abbildung 6: PKS - Entwicklung Cybercrime im Engeren Sinne mit Aufklärungsquote

Quelle: Bundeskriminalamt (BKA) - Michael Kraus, Kriminaloberrat, Vortrag Bekämpfung der Cybercrime aus Sicht des BKA (Folie 4)

Der hier zu sehende Auszug aus der Polizeilichen Kriminalstatistik zeigt den Verlauf der Cyberverbrechen im Engeren Sinne. Diese Verbrechen richten sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten.[44] Vorwiegend gehen in diese Statistik also deutlich professionellere Verbrechen ein als in die Statistik des „Tatmittel Internet“. Im Verlauf der Jahre hat auch hier die Verbrechensanzahl zugenommen und die Aufklärungsquote ist gesungen. Cybercrime im engeren Sinne ist aufgrund der Professionalität der Täter, für die Beamten vermutlich deutlich schwerer zu verfolgen. Die totale Aufklärungsquote beträgt hier im Jahr 2013 nur 2,3 %. Für die Behörden könnte in diesem Bereich die eben genannte Teufelsspirale entstehen.

Um abseits dieser Tatsachen mehr Erfolg bei der Suche nach digitalen Tätern zu haben, müssten Systeme besser überwacht und viele Kommunikationskanäle eines Rechnersystems transparent gemacht werden. Nutzer würden sich aber mit Sicherheit gegen diese Möglichkeit wehren, da sie dadurch das Gefühl bekommen würden, überwacht zu werden, was auch exakt der Fall wäre. Es bleibt am Nutzer, zu entscheiden, wie viel Überwachung er für angemessen hält und seine Interessen gegenüber dem Staat durchzusetzen. Da der Nutzer selbst nie nachvollziehen kann, was genau überwacht wird und wo genau seine Daten analysiert werden, lösen solche Überwachungsansätze Misstrauen gegenüber der Polizei und dem Staat aus.
Der Nutzer sollte sein System eher selbst besser überwachen können. Der beste Ansatz, um gegen Cybercrime vorzugehen, ist demnach nicht der bloße Einsatz von mehr Ressour-

[44] Vgl. Definition Cybercrime in Abschnitt 2.1

cen, sondern das Verhindern der Verbrechen selbst, durch Prävention, die aus Sensibilisierung entsteht. Der erfolgversprechendste Ansatzpunkt für die Bekämpfung von Cybercrime ist der Internetnutzer. Durch seine Sensibilisierung gegenüber den Gefahren, die digitale Technologien beinhalten, kann Cybercrime für die Täter unattraktiver gemacht werden.

2.3 Anatomie von Cyber-Angriffen

Da Ziel, Angreifer und äußere Umstände bei Cyber-Angriffen stark variieren, besteht ein Cyber-Angriff aus vielen verschiedenen Phasen. Je nachdem, ob es sich um einen klassischen Hack, ein Audit, Social-Engineering-Angriff, Scripting-Angriff oder eine Kombination aus diesen handelt, sind bestimmte Phasen unterschiedlich gewichtet oder fallen ganz weg. Daher gibt es keine generelle Anatomie des Cyber-Angriffs. Im Folgenden werden alle Phasen, die diese Angriffe aufweisen können, kategorisiert, benannt und in eine zeitliche Abfolge gebracht. Dabei entscheidet ein Angreifer immer individuell, welche Phasen er, je nach Aufwand und Nutzen, für angemessen hält. Um einen Überblick über alle möglichen Verhaltensweisen eines potentiellen Angreifers zu erlangen, werden nun drei Modelle besprochen, die die Anatomie der Angriffe näher beleuchten.

2.3.1 Phasen des Pentesting

Um einen Überblick über die Möglichkeiten der Verteidigung bei Cyber-Angriffen zu bekommen, werden zunächst die 5 Phasen, die das Bundesamt für Sicherheit in der Informationstechnik(BSI) für Penetrationstests erarbeitet hat, betrachtet und erläutert. Da sich das gesamte Unterkapitel 2.3.1 nur auf die Originalquelle des BSI bezieht, wird diese hier nur einmal angegeben. [45] Die Phasen bieten dabei ein Grundgerüst, an das sich professionelle Penetrationstester halten sollten, um seriös, erfolgreich und sicher einen Penetrationstest durchzuführen. Gleichzeitig soll hiermit über den grundsätzlichen Ablauf eines Penetrationstests informiert werden. Mittelständische und große Unternehmen sollten ihre Systeme regelmäßig professionell überprüfen lassen, um in dem sich ständig verändernden Informationszeitalter auf dem aktuellen Stand der Sicherheit zu bleiben.

Die 5 Phasen des Pentesting nach BSI:

1. Vorbereitung
2. Informationsbeschaffung und -auswertung
3. Bewertung der Informationen und Risikoanalyse
4. Aktive Eindringversuche
5. Abschlussanalyse

[45] BSI, Studie – Durchführungskonzept für Penetrationstests 2003 (Abschnitt 6.2 – Seite 45 f.)

Da ein Penetrationstest eine Art simulierter Cyber-Angriff auf Wunsch ist können, einige Parallelen zu bösartigen Cyber-Angriffen festgestellt werden. In seiner Studie von 2003 führt das BSI die einzelnen Phasen noch etwas genauer aus. Um sich eine Übersicht über die allgemeine Anatomie eines Cyber-Angriffs zu verschaffen, eignen sich diese Phasen jedoch nur bedingt. Sie können allerdings aufzeigen, an welchen Stellen die Verteidiger eines Systems limitiert sind. Im Rückschluss muss also besonders auf die Dinge geachtet werden, die Penetrationstests nicht abdecken, um effektiv dort zu schützen wo das System am verwundbarsten ist.

2.3.1.1 Vorbereitung

Vorbereitung ist die wichtigste Phase eines jeden Angriffs, egal, ob in der Cyber- oder klassischen Kriminalität. Penetrationstester müssen hier mit ihrem Auftraggeber genau abstimmen, was, wie, wo getestet werden soll und was auf keinen Fall getan werden darf. Ein Penetrationstest soll normalerweise den Workflow des zu testenden Unternehmens nicht stören oder gar zu Ausfällen von kritischer Infrastruktur führen, denn dies würde dem Unternehmen wirtschaftlich schaden.
Die Penetrationstester haben sich des Weiteren, solange das Unternehmen dies nicht selbst mit den Testern vereinbaren kann, an die gesetzliche Bestimmungen des jeweiligen Landes zu halten. Ein Datendiebstahl, soll zum Beispiel oft durchgeführt werden, um die Sicherheitsmaßnahmen zu testen. In diesem Fall sollte ein Kontrakt aufgesetzt werden, in dem sich die Tester verpflichten, alle gestohlenen Daten wieder auszuhändigen und das Unternehmen sich verpflichtet, diesen Akt nicht gesetzlich zu verfolgen. Ein Cyberkrimineller hält sich logischerweise nicht an solche Gesetze und Kontrakte. Ein Penetrationstest gibt also nur eine Vorstellung davon, welche negativen Konsequenzen sich im Ernstfall ergeben können. Sollte ein Penetrationstester erfolgreich in ein Unternehmen eindringen können, steht dieses einem professionellen Hacker, sehr wahrscheinlich, relativ schutzlos gegenüber. Die Aufgabe des Auditors ist es dann, die gefundenen Lücken aufzuzeigen und das Personal zu schulen.

2.3.1.2 Informationsbeschaffung und -auswertung

In dieser Phase gehen Penetrationstester und andere Angreifer gleich vor. Sie sammeln Informationen und katalogisieren diese in Programmen wie Dradis[46] oder BasKet[47]. Diese sind Tools, mit denen große Datenmengen beziehungsweise Informationen verwaltet und katalogisiert, sowie Querverbindungen zwischen ihnen hergestellt werden. Je mehr Informationen gesammelt und ausgewertet werden können, desto gezielter kann der Angriff erfolgen. Die Angreifer scannen die Netzwerke und Systeme und versuchen dabei unentdeckt

[46] www.dradisframework.com

[47] www.basket.kde.org

zu bleiben. Auch andere Informationen werden in dieser Phase gesammelt. Social Networks, wie Facebook bieten hier ein Paradies für bösartige Hacker, da ihre Opfer bereitwillig große Mengen Informationen über sich online stellen. Einem Angreifer sollten möglichst wenig Möglichkeiten gegeben werden, sich darauf vorzubereiten, was ihn erwartet. Auf keinen Fall sollte der ungeschützte Zugriff auf interne Dokumente von außen möglich sein. Auch wenn diese nicht über Websites oder ähnliches verlinkt sind, bedeutet dies nicht, dass sie nicht zu finden sind und gegen das jeweilige Unternehmen verwendet werden können. Privatpersonen sollten darauf achten, möglichst wenig Informationen über sich online zu stellen. Jede Information, die herausgeben wird, kann benutzt werden, um die jeweilige Person zu manipulieren, ihre Passwörter zu knacken oder Vertrauen aufzubauen. Viele Passwörter werden in kurzer Zeit gehackt, weil Menschen die Namen ihrer Haustiere oder Kinder online stellen und eben diese in beliebiger Kombination als Passwörter verwenden.

2.3.1.3 Bewertung der Informationen und Risikoanalyse

In dieser Phase beschreibt das BSI wie der Penetrationstester Risiken für seinen Auftraggeber abwägen soll, um diesem nicht wirtschaftlich zu schaden. Dabei werden möglicherweise kritische Systeme von den Tests ausgeschlossen. Ein Hacker würde natürlich keine Ziele auslassen, was gerade den Unternehmern, die möglicherweise bereits Penetrationstest haben machen lassen oder sich überlegen einen durchzuführen, immer bewusst sein sollte.

2.3.1.4 Aktive Eindringversuche

In dieser Phase wird aktiv versucht in das System einzudringen. Dabei gibt es viele verschiedene Methoden. Diese können in zwei Kategorien aufgeteilt werden Die lauten und die leisen Eindringversuche. Diese unterscheiden sich danach, ob sie im Netzwerkverkehr einfach zu identifizieren sind, beispielsweise durch das verursachen vieler gleicher oder ähnlicher Anfragen. Je nach Art und Intensität des Vorgehens dieser Eindringversuche können diese vom Admin oder anderen Sicherheitsmaßnahmen bemerkt werden. Sogenannte Intrusion Detection Systems, kurz IDS, sind genau zu diesem Zweck entwickelt worden. Als Privatperson sind diese nicht zweckmäßig. Dennoch können Privatpersonen einige Maßnahmen ergreifen, um sich sicherer im Netz zu bewegen. Diese Maßnahmen werden in Unterkapitel 4.3 genauer beschrieben.

2.3.1.5 Abschlussanalyse

In der Abschlussanalyse-Phase trägt der Penetrationstester seine gesammelten Informationen und Ergebnisse, die er im Verlauf des Tests dokumentiert hat, zusammen und wertet diese nochmals aus. Für den Auftraggeber wird der Verlauf des Tests dadurch transparent und nachvollziehbar. Die Informationen, die in dieser Phase verdichtet werden, geben dem Auftraggeber Aufschluss über seine Schwächen und Verbesserungspotentiale. Der Penetrationstester wird den Auftraggeber in dieser Phase über alle Vorgänge informieren und gegebenenfalls Schulungen und Weiterbildungen ausarbeiten um künftig die aufgedeckten

Fehler zu vermeiden und alle ermittelten Lücken zu schließen.
Bei Hackern entfällt diese Phase häufig. Im schlimmsten Fall analysiert dieser seinen Hack, um eventuell weitere Angriffe zu planen und durchzuführen. Für den Fall, dass ein Unternehmen gehackt worden ist, sollten schnellstmöglich alle entwendeten Informationen zusammengetragen und mit Experten analysiert werden. Dadurch kann sich optimal auf den nächsten möglichen Hackversuch vorbereitet werden.

2.3.2 Advanced Persistent Threats – APTs

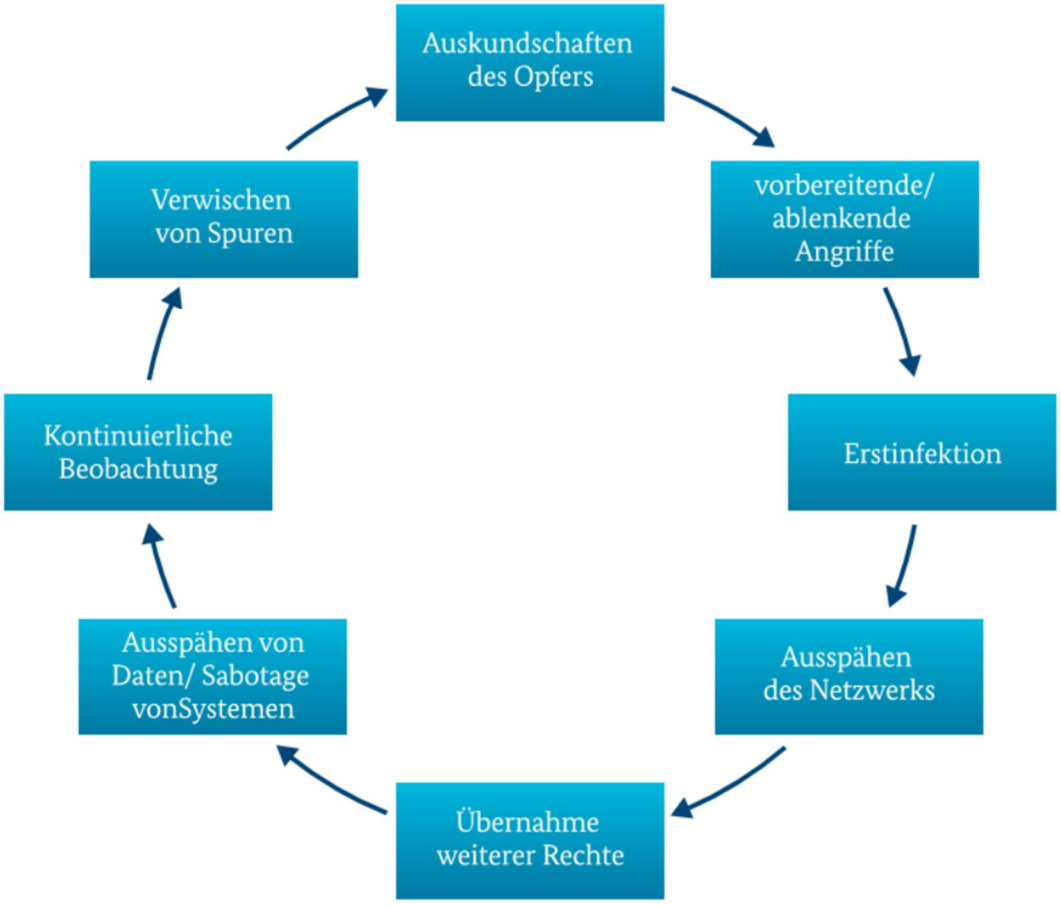


Abbildung 7: Vorgehen von Advanced Persistent Threats
Quelle: BSI, Die Lage der IT-Sicherheit in Deutschland (Abschnitt 2.2.3 – Seiten 26 f.)

Advanced Persistent Threats, zu Deutsch „fortgeschrittene, andauernde Bedrohungen“ zeichnen sich dadurch aus, dass den Angreifern ein großes Maß an Zeit, Geld, Informationen und Entwicklerkapazität zur Verfügung steht. Dabei gehen die Angreifer wie in Abbildung 7 gezeigt vor. Die APTs werden dabei nicht durch ihre oft hoch-komplexe Software klassifiziert, sondern vielmehr durch ihre Angriffsvektoren und die Tatsache, dass sie sich

über das Netzwerk ausbreiten und dauerhaft Zugang zum infizierten Netzwerk verschaffen.[48]

Unter die APTs fallen demnach die meisten modernen und professionellen Cyber-Angriffe. Das Vorgehen dieser Angriffe beziehungsweise ihre Anatomie ist einfach gehalten, aber sehr effektiv. Der Schlüssel zu den APTs ist die Erstinfektion, mit deren Hilfe Zugriff auf das interne Netzwerk, das LAN, erlangt wird. Die Erstinfektion erfordert dabei fast immer ein gewisses Maß an Social Engineering und eine Person, die dafür empfänglich ist. Der Aufbau der vom BSI entwickelten APT-Anatomie lässt nur den groben Überblick auf den Ablauf des Angriffs zu. APTs sind demnach eigentlich nur eine Klassifizierung für professionelle Angriffe und ihre Definition ist entsprechend grob gehalten.

[48] BSI, Die Lager der IT-Sicherheit in Deutschland 2015 (Abschnitt 2.2.3 – Seite 26 f.)

2.3.3 Cybercrimekreislauf

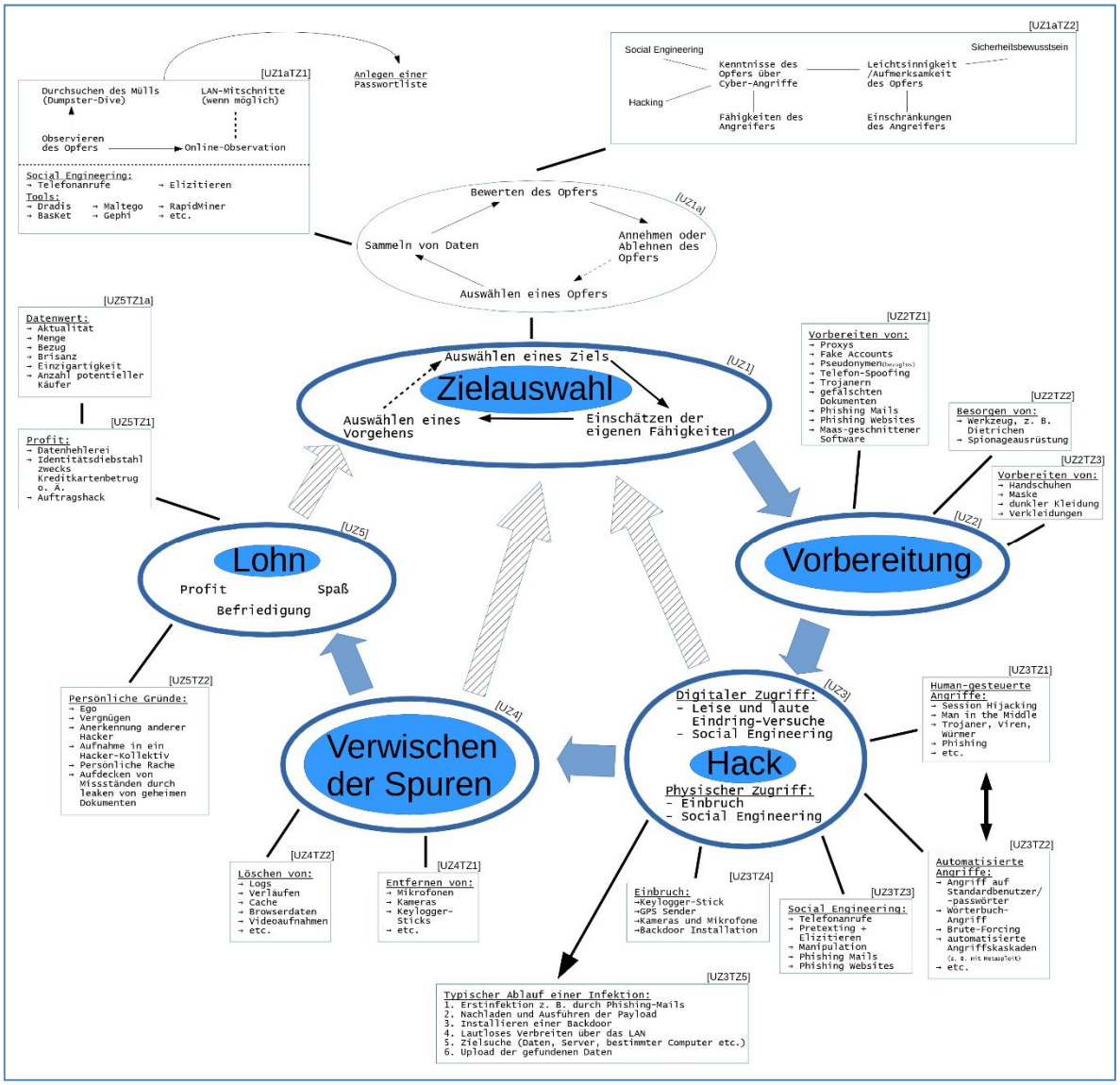


Abbildung 8: Cybercrimekreislauf

Quelle: Eigene Darstellung

Die hier zu sehende Abbildung 8 gibt einen Überblick über den Ablauf von professionellen Cyber-Angriffen. Unterzyklen sind durch UZ gekennzeichnet und Teilzyklen durch TZ. Schraffierte Pfeile zeigen Wiederholungsmöglichkeiten der Schritte an. Begriffe die nicht im Kreislauf oder dem dazugehörigen Text erklärt werden, finden sich im Glossar oder einem späteren Kapitel. Der Cybercrimekreislauf entstammt eigenen Überlegungen. Er ist ein Modell auf der Grundlage des IT-Sicherheitsstudiums und dem Buch „The Art of Human Hacking“ von Christopher Hadnagy. Er soll aufzeigen, welche Handlungen und Überlegungen für ein professionelles Cyberverbrechen notwendig sind. Dabei sollen möglichst alle Cyberverbrechen in ihrer Vorgehensweise in ihm wiederzufinden sein.

Der Zyklus wird im Folgenden näher erläutert. Dabei werden zentrale Methoden und Vorgehensweisen näher beschrieben oder Beispiele gegeben. Der Cyber-Angriff ist einem normaleren Angriff sehr ähnlich und besteht aus 5 Grundphasen die sich in den 5 Unterzyklen wiederspiegeln:

1. Zielauswahl
2. Vorbereitung
3. Eigentliche kriminelle Handlung
4. Beseitigen der Spuren
5. Entlohnung des Täters

Generell beschreiten Penetrationstester und bösartige Hacker oft den gleichen Weg. Der genaue Unterschied zwischen einem Penetrationstester und einem bösartigen Hacker wurde in Unterkapitel 2.1.1.2 bereits beschrieben.

2.3.3.1 Zielauswahl

Abbildung 9: UZ1 - Zielauswahlzyklus

Quelle: Eigene Darstellung

Zunächst muss ein Angreifer sein Ziel festlegen. Dabei ist das Ziel nicht die Zielperson oder das Zielunternehmen, sondern das allgemeine Ziel seines Arbeitsaufwandes. Ein Ziel kann auch schlicht Profit oder Schaden an einer Person, beziehungsweise einem Unternehmen sein. Laut BKA gewinnt auch der Bereich „Cybercrime-as-a-Service“ immer mehr an Bedeutung.[49] Hacker, die ihre Dienste zum Verkauf anbieten, bekommen ihr Ziel dementsprechend von ihrem Auftraggeber. Der eigentliche Cyber-Angriff besteht nicht selten aus mehreren Zielen, die nacheinander abgearbeitet werden. Oft wird die Zielauswahl entweder von der Hack-Phase oder von der Verwischen-der-Spuren-Phase angesteuert. Dabei fallen die Zielauswahl-Phase und die Vorbereitungs-Phase meist bedeutend kleiner aus als beim ersten Mal, sofern der Angreifer diese nicht ohnehin schon vorausgeplant hat. Ein Beispiel:

> Das eigentliche Ziel könnte der Aufbau eines Botnetzes sein. Dazu müssen zunächst einige Unterziele abgearbeitet werden. Der Angreifer geht nun rückwärts vor und überlegt wie er die Botnetzsoftware auf die PCs der Opfer bekommt. Er überlegt

[49] BKA, Bundeslagebild 2015 (Abschnitt 2.4 – Seite 11)

sich, dass Phishing-Mails eine Möglichkeit wären, die Schadware zu verteilen. Er weiß allerdings auch, dass die meisten Menschen diese ignorieren würden. Seine Lösungsidee ist einfach: Er will die Mails über Accounts von Privatpersonen an deren Kontakte verschicken. Ziel der ersten Runde ist also das Stehlen von möglichst vielen Zugangsdaten für private E-Mail-Accounts, Ziel der zweiten Runde ist mit diesen Mails möglichst viele Rechner aus den Kontaktlisten der Opfer, der ersten Runde, zu infizieren. Ziel der dritten Runde ist es dann, mit der eingeschleusten Schadware besagtes Botnetz aufzubauen.

Die Zielauswahl selbst ist also bereits der erste Zyklus, in dem ebenfalls das Vorgehen festgelegt wird. Im genannten Beispiel, hat der Angreifer sein Ziel festgelegt, seine Fähigkeiten eingeschätzt und sein Vorgehen festgelegt, welches daraus bestand, zwei Unterziele zu bilden. Er hat diese definiert und musste anschließend wieder seine Fähigkeiten abschätzen und ein Vorgehen auswählen, um besagte E-Mailzugänge zu erhalten. Dabei bilden sich häufig noch weitere Unterziele. Somit kann es sein, dass ein Hackversuch nicht ausreicht und das Opfer von einer anderen Seite aus angegriffen werden muss. In diesem Fall wird der Angreifer von der Hack-Phase wieder in die Zielauswahl-Phase springen. Hat er bereits viel „Lärm“ gemacht, wird er sich zunächst um die Spurenbeseitigung kümmern und danach zurück in die Zielauswahl-Phase springen.

Opferwahl

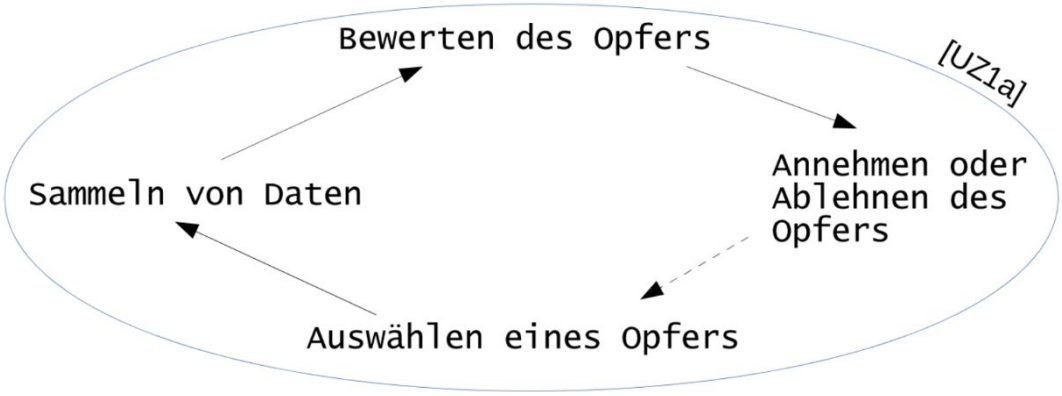


Abbildung 10: UZ1a - Opferauswahlzyklus
Quelle: Eigene Darstellung

Der abgebildete Unterzyklus beinhaltet die Wahl des ersten Opfers oder der ersten Opfergruppe, für den ersten Schritt des Vorgehens. Dabei kann das Opfer sowohl eine natürliche Person als auch ein Unternehmen, eine Regierung oder ein Server, beziehungsweise ein PC oder Mobilgerät sein. Ein erfolgreicher Hack braucht einen Startpunkt, welcher über das Opfer definiert wird. Die Auswahl eines Opfers resultiert also direkt aus dem, im UZ1 gewählten, Vorgehen und Ziel. Nach der Auswahl eines Opfers werden intensiv Daten zu diesem gesammelt. Dies wird in UZ1aTZ1 beschrieben. Mit den gewonnenen Daten können Abschätzungen zur Bewertung des Opfers erfolgen. Die Bewertung des Opfers wird in UZ1aTZ2 genauer beschrieben. Nachdem das Opfer bewertet wurde, wird es abgelehnt oder angenommen. Der Zyklus startet nun erneut oder der Angreifer begibt sich in die Vorbereitungsphase UZ2.

Datensammlung

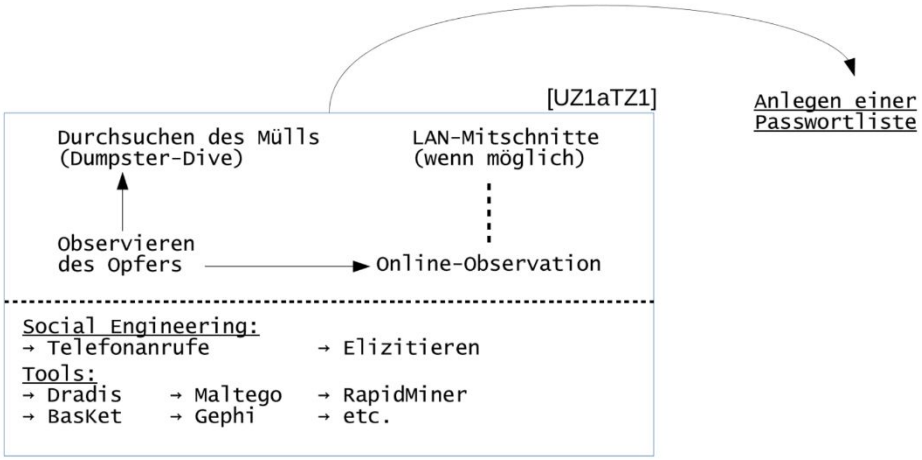


Abbildung 11: UZ1aTZ1 - Datensammlung

Quelle: Eigene Darstellung

Die Datensammlung ist der wichtigste Bestandteil bei der Bewertung des Opfers und dient gleichzeitig als Vorbereitung auf den Angriff. Sie ist der umfangreichste Teilschritt des gesamten Angriffs, egal ob rein digital, mit Social Engineering oder als klassischer Diebstahl. Hat der Angreifer nicht alle Informationen vorliegen, passiert es leicht, dass er vermeidbare Fehler macht. Der Angreifer agiert während der Datensammelphase wie ein Social Engineer. Ermittlungen beginnen oft mit einer Observation des wahrscheinlichsten Täters. Ein Verbrecher geht bei seinem Ziel sehr ähnlich vor.

Observation kann einerseits bedeuten, das Ziel physisch zu verfolgen, um seine Gewohnheiten, Hobbys, Arbeitszeiten und häufig zurückgelegte Wege heraus zu finden. Dabei entsteht langsam ein Bild des Opfers, wie es sich vermutlich verhalten oder wem es vertrauen würde. Im besten Fall kann der Angreifer sein Opfer bei Eingabe seiner PIN am Bankautomaten oder Ähnlichem beobachten. Dabei versucht der Angreifer, keine Spuren zu hinterlassen und so wenig Aufmerksamkeit wie möglich auf sich zu ziehen.

Observation kann aber auch bedeuten, das Opfer online zu beobachten. Ein Server zum Beispiel lässt sich schwer physisch verfolgen, er würde beispielsweise mit Portscannern bearbeitet werden, um Schwachstellen zu identifizieren. Aber auch Personen hinterlassen im Netz alle möglichen Daten über sich, die Angreifer gegen sie verwenden können. Die meisten Personen haben ein sehr aktives Onlineleben und verteilen bereitwillig große Mengen an persönlichen Informationen über sich im Internet. Durch den Einsatz von Datamining-Tools wie Maltego[50], RapidMiner[51] oder Gephi[52] können geübte Personen verdeckte Zusammenhänge über das Internet ausfindig machen und zu ihrem Vorteil nutzen.

[50] www.paterva.com

[51] www.rapidminer.com

[52] www.gephi.org

Für den Social Engineer ist der sogenannte Dumpster-Dive meist eine der lukrativsten Möglichkeiten, um an Informationen zu gelangen. Dabei durchsucht der Angreifer den Müll des jeweiligen Opfers oder dessen Umfeldes. Aus dem Müll von Firmen, aber auch aus dem von Privatpersonen können wichtige Informationen geborgen werden. Jedes Detail ist wichtig und kann von einem cleveren Social Engineer für sein Vorgehen ausgenutzt werden. Ein Internes Dokument könnte beispielsweise das Corporate Design der Firma beinhalten und dem Angreifer so die Möglichkeit geben, eine täuschend echte Fälschung anfertigen zu können. Ein Kontoauszug aus dem Müll einer Privatperson verrät die Bank und Kontonummer und kann so für einen betrügerischen Anruf genutzt werden. Daher ist es besonders für Unternehmen wichtig, Dokumente zu schreddern und nicht einfach nur in den Papiermüll zu werfen. Sollte der Angreifer tatsächlich Zugriff auf das LAN des Opfers bekommen haben, kann er Mitschnitte vom Netzwerkverkehr machen oder einen sogenannten „Man in the Middle“ Angriff durchführen. Dieser wird in Unterkapitel 2.4.1 noch näher beschrieben. Dadurch ist es ein Leichtes für ihn an die Passwörter und Konten des Opfers zu gelangen.

Die letzte Methode, mit der der Angreifer gezielt an bestimmte Informationen gelangen kann, ist das Opfer selbst zu fragen. Dabei kommt eine klassische Methode des Social Engineering zum Einsatz, das Elizitieren. Elizitieren ist eine Methode, gezielt Informationen zu erhalten und wird in Unterkapitel 3.3 näher besprochen. Durch scheinbar zufällige Begegnungen kann der Social Engineer sein Opfer oder dessen Umfeld in Gespräche verwickeln und ihnen Informationen entlocken. Hierzu benötigt er einen Vorwand, zum Teil auch Pretext genannt, den er zum Beispiel, aus den bis dort gesammelten Informationen erstellt. Pretexting wird ebenfalls in Unterkapitel 3.3 näher besprochen.
Auch das Telefon ist ein oft unterschätztes Werkzeug eines Social Engineers. Wer kennt schon alle Mitarbeiter seiner Bank? Wenn also ein Fremder am Telefon behauptet, er sei Mitarbeiter der Bank der Zielperson und mache eine Umfrage zur Kundenzufriedenheit oder es gebe ein Problem mit deren Konto, würde die Zielperson dies vermutlich nicht hinterfragen. Dabei würde der Angreifer zum Beispiel die Kontonummer aus seinem Dumpster-Dive verwenden und dann „zum Abgleich“ beispielsweise das Geburtsdatum oder das Internet-, beziehungsweise Telefonpasswort abfragen. Zwei absolut gängige Praktiken bei Kundenkommunikation. Auf diese Weise kann der Angreifer an Informationen gelangen, an die er sonst nur schwer kommen würde.

Nach beendeter Datensammlung trägt der Angreifer seine Daten zusammen und organisiert sie wiederum in Tools wie Dradis oder BasKet. Er versucht Zusammenhänge zu erkennen, Pretexte zu entwerfen und trägt alle Wörter, die im Zusammenhang mit dem Ziel stehen, in ein Wörterbuch ein. Aus diesem Wörterbuch entsteht die Passwortliste, die elementarer Bestandteil des Wörterbuchangriffs ist. Dabei werden alle Wörter im Wörterbuch mit einem Algorithmus neu zusammengemischt oder variiert und ergeben so mögliche Passwörter. Diese Methode funktioniert tatsächlich sehr gut, da viele Menschen sehr einfallslos mit ihren Passwörtern sind und Wörter aus ihrem direkten Umfeld benutzen. Diese

Daten kann ein Social Engineer mit relativ geringem Aufwand herausfinden und für sich nutzen.

Nach der Phase des Datensammelns folgt die Opferbewertung anhand der gesammelten Informationen.

Opferbewertung

[UZ1aTZ2]

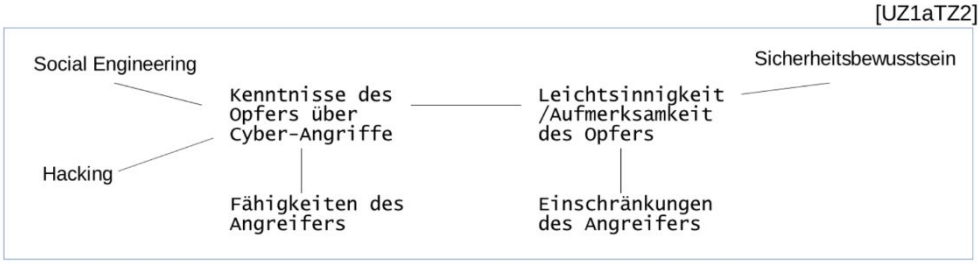


Abbildung 12: UZ1aTZ2 - Opferbewertung

Quelle: Eigene Darstellung

Durch die in UZ1aTZ1 gesammelten Daten hat sich der Angreifer ein Bild über sein Opfer gemacht. Er kennt nun seine Gewohnheiten, Hobbys, Wege durch die Stadt und so weiter. Darüber hinaus hat er sich ein Bild von der Verfassung der Person oder Firma gemacht. Im Fall eines Servers oder Netzwerkes, hat er das Netzwerk gescannt und mögliche Schwachstellen identifiziert.
Er stellt sich nun Fragen wie: Ist das Opfer leichtsinnig oder naiv und wenn ja, wie sehr? Hat es bereits Erfahrungen mit Computersicherheit, Social Engineering oder sich darüber belesen? Wie sicherheitsbewusst ist es und unter welchen Umständen lässt es dieses Bewusstsein außer Acht?
Ein Opfer, das zum Beispiel über Social Engineering und Methoden des Elizitierens Bescheid weiß, könnte schneller misstrauisch werden oder den Angreifer bei weiteren Handlungen enttarnen. Am besten ist es für den Angreifer, wenn das Opfer sich sicher fühlt und deshalb bei Fragen oder ungewöhnlichen Ereignissen nicht sofort vermutet, Ziel eines Angriffs zu sein. Der Angreifer trägt also seine Fähigkeiten zusammen und gleicht diese mit dem Wissen über Angriffe aller Art und dem Sicherheitsbewusstsein des Opfers ab. Er identifiziert mögliche Leichtsinnigkeiten des Opfers und gleicht diese mit seinen eigenen Handlungseinschränkungen ab, ob zum Beispiel durch einen weit entfernten Wohnort des Opfers, eine physische Interaktion mit ihm nicht oder nur begrenzt möglich ist und Ähnliches.

Die Erfolgschancen des Angreifers sind also maximal, wenn das Opfer so wenig Kenntnisse wie möglich über Angriffe im Bereich des Social Engineering und Hacking besitzt, es leichtsinnig handelt, sich sicher fühlt und der Hacker nicht in seinen Vorgehensmöglichkeiten eingeschränkt ist. Nach Abwägen der Erfolgschancen wird das Opfer nun angenommen oder abgelehnt. Bei Ablehnung wird wieder in UZ1 ein Opfer gewählt und der Zyklus beginnt erneut.

2.3.3.2 *Vorbereitung*

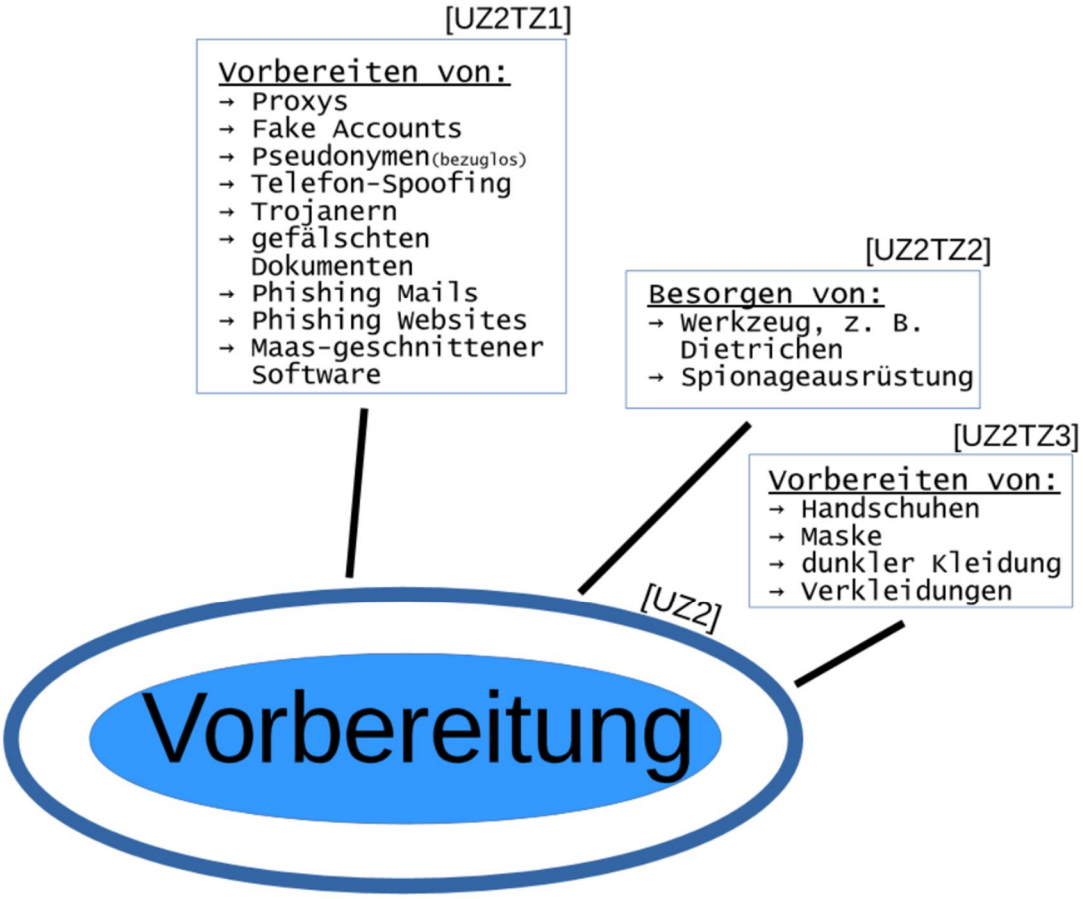


Abbildung 13: UZ2 - Vorbereitungsphase

Quelle: Eigene Darstellung

In der Vorbereitungsphase kennt der Angreifer bereits sein Opfer und hat sein Vorgehen festgelegt. Er bereitet sich zugleich auf seinen Angriff, als auch auf seine Absicherung vor. Er fälscht Dokumente, bereitet Viren und scheinbar sichere Dokumente vor, die bei seinem Hack zum Einsatz kommen sollen. Er legt Phishing Seiten an oder kreiert stark personalisierte Phishing Mails, um sein Opfer in die Falle zu locken. Darüber hinaus erschafft er falsche Identitäten, bereitet seine Proxy-Server vor, legt sich seine Pretexte zurecht und programmiert gegebenenfalls spezielle Software, die er für seinen Hack braucht. Die digitale Vorbereitung ist elementarer Bestandteil seiner digitalen Absicherung und soll unter anderem dafür sorgen, dass er nach Entdecken des Hacks nicht zurückzuverfolgen ist. Darüber hinaus sollen solche Maßnahmen die Konsistenz seiner Geschichten wahren. Wenn der Angreifer anruft, sollte seine Nummer unter Umständen keine Handynummer sein oder aus einem Dorf stammen in dem kein Sitz der Firma ist für dessen Mitarbeiter er sich ausgibt. Solche kleinen Ungereimtheiten erregen die Aufmerksamkeit des Opfers und lassen den Angreifer möglicherweise auffliegen.

Je nach Anwendungsfall muss der Angreifer Ausrüstung besorgen. Spionageausrüstung und Werkzeuge wie Dietriche sind frei verkäuflich, aber für physische Angreifer hoch effektiv. Aufzeichnungsgeräte aller Art, wie Diktiergeräte, kleine Mikrophone und versteckte Kameras, die man am Körper tragen kann, werden von Social Engineers benutzt, um jedes

Gespräch im Nachhinein noch einmal analysieren zu können und so das nächste Gespräch besser gestalten und lenken zu können.
Durch das Tragen von Handschuhen, dunkler Kleidung und dergleichen fällt der Angreifer weniger auf, wenn er Kameras installiert oder weitere Mülltonnen durchsucht. All diese Sachen werden in der Vorbereitungsphase zusammengetragen. Darüber hinaus muss er sich Gedanken machen, ob er selbst in Erscheinung tritt und dafür Verkleidungen oder Ähnliches braucht. Beispielsweise ein T-Shirt mit dem Namen einer Müllentsorgungsfirma.

2.3.3.3 Hack

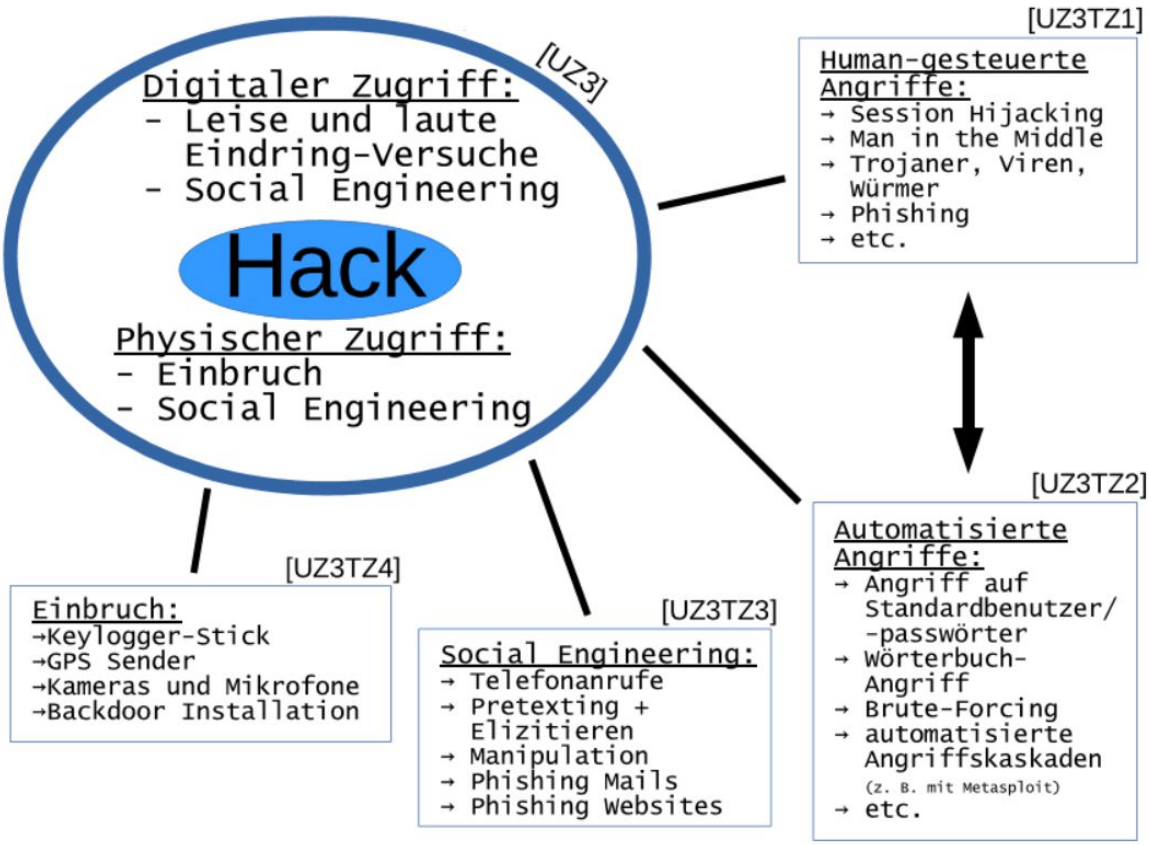


Abbildung 14: UZ3 - Hack
Quelle: Eigene Darstellung

UZ3 beschreibt den eigentlichen Hack. Diese Phase kann sich über Tage, Wochen oder Monate erstrecken und fordert vom Angreifer neben seinem Knowhow auch eine Menge Kreativität.
Die lauten und leisen Eindringversuche beziehen sich auf das Eindringen in Computernetze und Computer. Lautes Eindringen meint dabei auffälliges Agieren im Netzwerk, zum Beispiel viel Traffic im Netz zu verursachen, der leicht von einem Admin oder einem IDS (Intrusion Detection System) erkannt werden kann.
Leises Eindringen meint zum Beispiel das manuelle Scannen von ganz bestimmten Ports und das suchen nach ganz bestimmten Diensten, um gezielt Exploits anwenden zu können. Diese Aktionen werden von den meisten IDSs nicht automatisch als Bedrohung eingestuft und sind in der Masse von Daten, die normalerweise über ein Netz gehen, für einen Administrator, der den Datenverkehr überwacht, kaum zu erkennen.

Neben den lauten und leisen Angriffsmöglichkeiten kann zwischen humangesteuerten Angriffen und automatisierten Angriffen unterschieden werden.
Automatisierte Angriffe erfordern vom Angreifer wenig Grundlagenwissen und Einblicke in die Materie. Sie können also eher von allen Sorten Angreifern verwendet werden. Darüber hinaus muss der Angreifer sie höchstens vorbereiten, wie zum Beispiel beim Wörterbuchangriff, für den er Daten gesammelt hat. Danach startet er den Angriff und wartet ab. Dabei muss er bis zum Ergebnis selbst nicht mehr interagieren. Durch diesen Umstand sind diese Angriffe am wahrscheinlichsten und werden bei so gut wie jedem Hack zuerst gestartet. Danach kann der Angreifer sich parallel um die von ihm selbst gesteuerten Angriffe kümmern.
Für ein optimales Ergebnis wird der Hacker geschickt zwischen vielen Methoden wechseln, um mit möglichst geringem Zeitaufwand einzudringen und dabei, so unentdeckt wie möglich zu bleiben. Eine Privatperson wird in der Regel weder ein IDS benutzen, noch den Datenverkehr in seinem LAN persönlich überwachen. Besonders nicht zu jeder Zeit. Hier könnte der Hacker mit seinen Angriffen also laut werden, sofern er das Onlineerlebnis des Opfers dabei nicht allzu stark stört. Sollte er beispielsweise das Netz durch seine Aktivitäten überlasten, beziehungsweise blockieren so würde er dessen Aufmerksamkeit auf sich ziehen.

[UZ3TZ5]

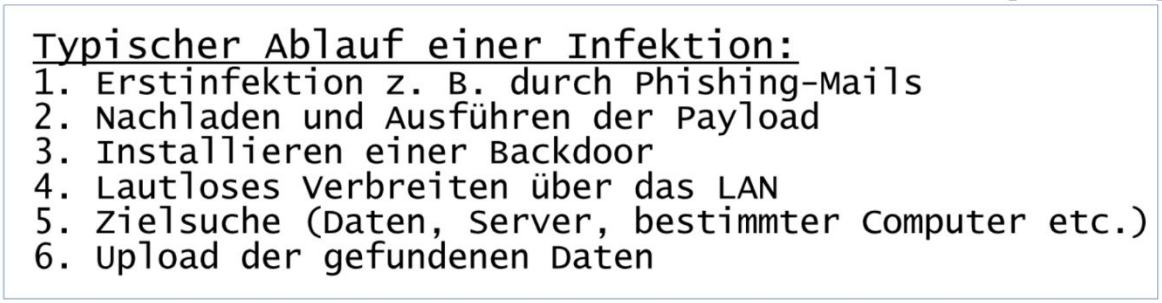


Abbildung 15: UZ3TZ5 - Typischer Infektionsablauf

Quelle: Eigene Darstellung

Hier zu sehen ist der typische Ablauf einer Infektion. Wichtig für einen Angreifer ist, einen Zugang zum Netz zu bekommen, in dem sich sein Ziel aufhält. Schadware kann sich in einem LAN deutlich einfacher verbreiten, als wenn sie von außen eindringen muss. Durch die Erstinfektion erreicht der Angreifer Zugriff auf das LAN. Er kann so sein Ziel suchen und seine Schadware verbreiten. Dabei wird er sich auf den infizierten Geräten einen dauerhaften Zugang einrichten, die sogenannte Backdoor. Nachdem der Angreifer sein Ziel gefunden hat, wird er mit dem Upload oder zerstören der jeweiligen Daten beginnen, danach seine Spuren verwischen und sich aus dem Netz zurückziehen.

Die dritte Angriffsmöglichkeit für den Angreifer ist es, einige Hürden zu umgehen, indem er bei dem Opfer zu Hause oder am Arbeitsplatz einbricht, beziehungsweise sich über Methoden des Social Engineering Zutritt zu seinem Büro oder Ähnlichem verschafft. Dabei könnte er einen kleinen unauffälligen Stick zwischen den USB-Port und die Tastatur hängen, der alle Eingaben mitschreibt, wodurch auch alle Passwörter mitgeschrieben werden, die das

Opfer eingibt. Bei Zugriff auf den Rechner könnte er ebenfalls seine Schadsoftware und eine Backdoor installieren sowie einen Keylogger, der ebenfalls die Eingaben mitschreibt. Vorteil bei der digitalen Variante ist, dass die Daten direkt über das Internet an den Hacker gesendet werden können und die Backdoor sich, nach getaner Arbeit, spurenfrei entfernen lässt, ohne dass nochmals physisch Zugriff auf das System gegeben sein muss. Der USB-Stick funktioniert in den meisten Fällen nicht über Funk, sondern speichert die Eingaben mit Zeitstempel in einer Textdatei auf dem Gerät.[53] Der Hacker muss also noch einmal wiederkommen um das Gerät zu entfernen. Dies erhöht das Risiko für den Angreifer, allerdings kann er sich durch physischen Zugriff viel Arbeit sparen und diverse digitale Hürden umgehen.

Ein Angreifer besitzt je nach Wissen und Erfahrung ein gewisses Angriffsrepertoire, welches die Gesamtheit der ihm zur Verfügung stehenden IT-Angriffe, beziehungsweise Hacks beschreibt. Eine Liste der gängigen IT-Angriffe steht in Unterkapitel 2.4. Solche Angriffe erfordern oft ein großes Maß an Wissen seitens des Angreifers und werden deshalb eher selten von Gelegenheitstätern benutzt. Heute geht die Tendenz allerdings in die Richtung der Schadwarebaukästen. Mit diesen Baukästen können auch unerfahrene Gelegenheitstäter oder sogenannte Scriptkiddies sich relativ einfach Schadware zusammenstellen und diese benutzen.
Hinzu kommen Angriffe auf Standardpasswörter und -logins. Diese Methode kann im Prinzip jeder Angreifer anwenden. Sie werden in Kapitel 2.4.2 näher beschrieben. Wegen solcher Angriffsmethoden ist es besonders wichtig, immer die Standardpasswörter an jedem Gerät auszutauschen.
Es ist aber ebenfalls wichtig, wie ein Passwort gestaltet ist. Passwörter mit Bezug auf das direkte Umfeld des Nutzers, sind besonders schwach gegenüber Angreifern, werden von den meisten Nutzern allerdings bevorzugt verwendet. Bei dem Wörterbuchangriff erstellt der Angreifer ein Wörterbuch mit möglichen Passwörtern. Ist die Datenmenge erst einmal groß genug, findet dieser Angriff so gut wie jedes Passwort. Am besten kann sich ein Nutzer davor schützen, indem er möglichst lange, unpersönliche und kryptische Passwörter verwendet.

Die folgenden Beispiele verdeutlichen den Sachverhalt:

> Ein Passwort, das nur aus Groß- sowie Kleinbuchstaben und Ziffern besteht, mit einer Länge von 7 Zeichen, wird mit einem durchschnittlichen Desktop PC in etwa einer Minute mit der Brute-Force-Methode geknackt. Auch mit Sonderzeichen ist ein Passwort mit 7 Stellen meistens in unter 24 Stunden mit der Brute-Force-Methode geknackt. [54] Gestoppt werden kann Brute-Force nur seitens der Onlinedienstbetrei-

[53] Christopher Hadnagy, Die Kunst des Human Hacking (Kapitel 7 – Seite 325 ff.)

[54] www.howsecureismypassword.net

ber durch das Implementieren einer begrenzten Anzahl an Versuchen während eines bestimmten Zeitraums. Es sollte sich dennoch nicht darauf verlassen werden, dass die Dienstbetreiber dies konsequent tun. Durch das Erhöhen der Rechenleistung und das Zuschalten mehrerer Rechensysteme kann der Zeitaufwand für Brute-Force stark gesenkt werden.

Da immer noch viele Menschen keinen Wert auf komplizierte oder lange Passwörter legen und die Rechenleistung der Computer immer weiter anwächst, bleibt Brute-Forceing trotz seiner Ineffizienz eine der effektivsten Methoden, um an Passwörter zu gelangen. Um diesen Punkt nochmals zu verdeutlichen, befinden sich rechts in Abbildung 16 die Liste der am häufigsten verwendeten Passwörter Deutschlands, die die Forscher des Hasso-Plattner-Instituts für Softwaresystemtechnik (HPI) aus etwa 30 Millionen geleakten Nutzerkonten ermittelt haben:[55]

1. hallo
2. passwort
3. hallo123
4. schalke04
5. passwort1
6. qwertz
7. arschloch
8. schatz
9. hallo1
10. ficken

Abbildung 16: Liste der beliebtesten deutschen Passwörter

Quelle: Eigene Darstellung in Anlehnung an die Ergebnisse des Hasso-Plattner-Instituts

Eine weitere hier aufgeführter und oft genutzte Methode, ein Computersystem anzugreifen, sind die automatisierten Angriffskaskaden. Diese finden sich zu Hauf im Internet oder dem Metasploit Framework, wie es zum Beispiel auf der BackTrack[56] oder KALI[57] Distribution zu finden ist. Der Angreifer muss nur ein paar Parameter in die Kommandozeile eingeben oder bekommt sogar eine grafische Benutzeroberfläche. Dann werden ganze Reihen von Angriffen gefahren und gehofft, dass das Zielsystem auf einen der Angriffe anspringt. Diese Methodik zählt definitiv zu den lauten Eindringversuchen und funktioniert meistens nicht bei gehärteten Systemen oder Systemen, die auf den neusten Stand geupdated wurden. Schwachstellen werden von den Angreifern spätestens nach Bekanntwerden ausgenutzt, Herstellern schließen diese im selben Zuge normalerweise in Sicherheitsupdates. Es ist deshalb besonders wichtig, sein System möglichst auf dem neusten Stand zu halten um sich vor Angriffen zu schützen.

Wie zu Beginn der Arbeit erwähnt, ist Social Engineering elementarer Bestandteil gezielter Angriffe. Social Engineering kann Türen öffnen, die sonst nur sehr schwer oder gar nicht zu öffnen sind. Mit einem gekonnt eingespielten Vorwand(Pretext) entlockt(elizitiert) der Angreifer seinem Ziel Informationen, am Telefon oder von Angesicht zu Angesicht. Eine zeitlich gut abgestimmte Phishing-Mail oder Website mit für das Opfer verführerischem Inhalt ist eine der besten Methoden für den Angreifer, um seine Schadware zu platzieren. Durch psychologische Tricks und das Einfließen lassen von Vorlieben oder Interessen des

[55] HIP, Hasso Plattner Institut - Pressemitteilung: Die Top Ten deutscher Passwörter

[56] www.backtrack-linux.org

[57] www.kali.org

Opfers kann ein Link in einer Mail unwiderstehlich werden. Dafür muss der Angreifer sein Ziel kennen und genug Wissen über dessen Verhalten und das Verhalten von Menschen allgemein besitzen, weshalb die Datensammlungsphase so wichtig für den Angreifer ist.

Physischer Zugriff kann auch über die Methoden des Social Engineering erfolgen. Dabei kann der Angreifer, die unter „Einbruch“ aufgeführten Hilfsmittel nutzen. Dafür muss der Angreifer allerdings zuerst einen Einbruch begehen. Viele Schlösser lassen sich mit etwas Übung und einem Dietrichset oder einem Schlagschlüssel in wenigen Minuten öffnen und der Eindringling hinterlässt dabei quasi keine Spuren. Danach kann er Kameras, Mikrophone, GPS-Sender, Keylogger und Backdoors auf den Systemen des Opfers und in dessen Wohnung installieren.[58] Bei physischem Zugriff auf ein System nützt das Passwort am PC im Allgemeinen nichts. Das Anmeldepasswort soll flüchtige Zugriffe verhindern, bietet aber keinen wirklichen Schutz vor jemandem, der weiß, wie er vorgehen soll. Einbruch ist deshalb eine andere Kategorie, da es ganz andere Fähigkeiten erfordert, als das Vorgehen über Social Engineering. Dennoch kann es denselben Effekt haben. Auch wird der Kontakt mit Menschen dadurch weitestgehend vermieden, womit es für den Angreifer einen ganz anderen Risikofaktor beinhaltet als klassisches Social Engineering. Die Methodiken des physischen Zugriffs auf ein Objekt oder eine Zielperson finden sich vorwiegend bei professionellen Angriffen und weniger bei Privatpersonen. Auditoren, sofern nicht anders in ihrem Auftrag erlaubt, sind von dieser Methode vollkommen ausgenommen, da sie an die lokalen Gesetze gebunden sind.

2.3.3.4 Verwischen der Spuren

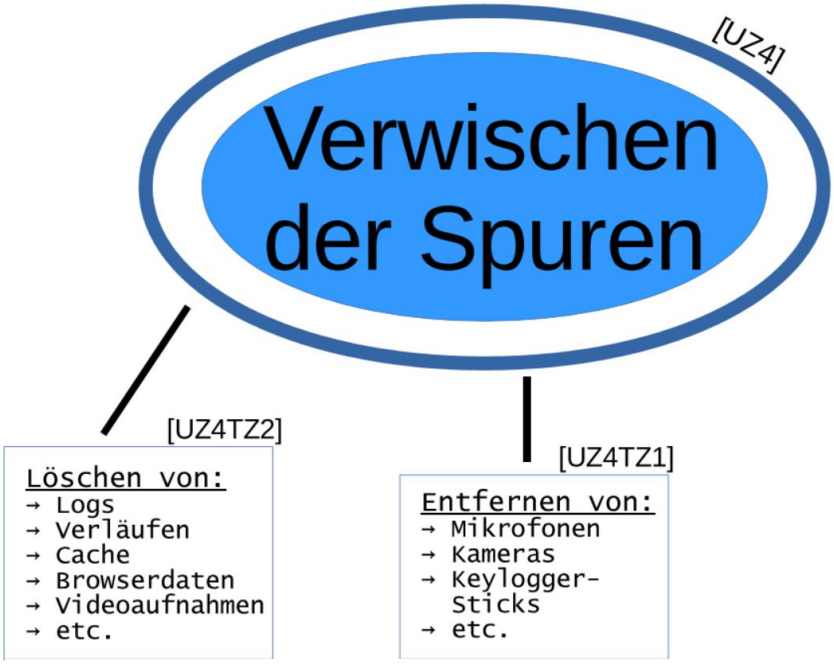


Abbildung 17: UZ4 - Verwischen der Spuren

Quelle: Eigene Darstellung

Nach dem Hack muss der Angreifer seine Spuren entfernen. Alle Geräte in den Originalzustand versetzen, Hardware einsammeln, Schadware von den PCs der Opfer wieder entfernen und so weiter. Das Verwischen der Spuren ist für den erfolgreichen Angreifer ein elementarer Schritt, da er normalerweise Wert darauf legt, unerkannt zu blei-

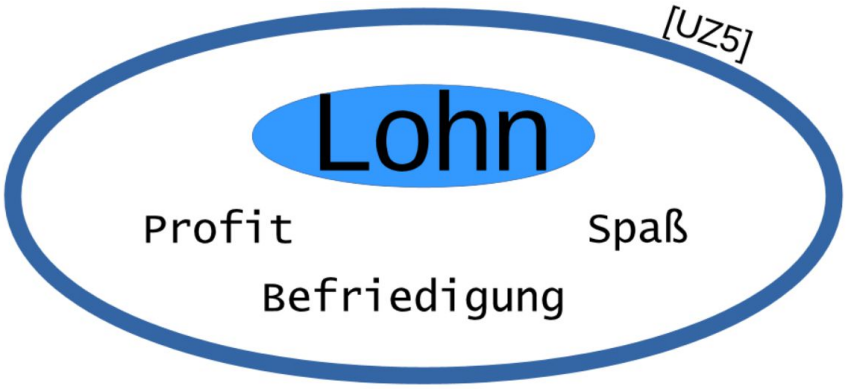
[58] Christopher Hadnagy, Die Kunst des Human Hacking (Kapitel 7.1 – Seite 326 ff.)

ben. Seine Chancen, unerkannt zu bleiben sind dann maximal, wenn nicht einmal der Hack entdeckt wird und falls er entdeckt wird, keine Hardware oder Software gefunden wird, die auf ihn zurückzuführen ist. Der Auditor muss nicht fürchten, später entdeckt zu werden, er sollte sogar alle Aufzeichnungen zusammentragen, da er sein Handeln belegen muss und sein Job beinhaltet, die Sicherheitslücken aufzudecken. Für den Auditor heißt dieser Schritt deshalb eigentlich „Zusammentragen von Spuren“.

Wie in UZ2 und UZ3 bereits erwähnt, kommt bei einem Social-Engineering-Audit oder einem professionellen Hack oft Spionagehardware zum Einsatz. Diese muss vor Ort zurückgelassen, aber hinterher wieder eingesammelt werden. Der Angreifer hat sich normalerweise eine Liste seiner verteilten Hard- und Software angefertigt um nichts zu vergessen. GPS-Ortungsgeräte und unauffällige Kameras sind besonders teuer und werden im Normalfall wieder vom Angreifer eingesammelt. Sollte ein Angreifer aufgeflogen sein und dies selbst noch nicht wissen, ist eine effektive Methode, um ihn zu schnappen sicherlich beim Aufräumen seiner Hardware.

Aber nicht nur Hardware muss eingesammelt werden, auch Softwareaufzeichnungen aller Art müssen vom Angreifer beseitigt werden. Ist der Einbruch des Angreifers geglückt, hat er womöglich auch Zugriff auf Logs oder Cache des Servers und kann diesen leeren, um unerkannt zu bleiben. Für den Ernstfall, dass die Polizei auf ihn aufmerksam wird, wird er alle Dateien, die er weiterhin benötigt, verschlüsseln und alles Unnötige löschen. Dazu gehören alle Aufzeichnungen, die er mit seiner Hardware gemacht hat sowie Spuren auf seinen eigenen Geräten.

2.3.3.5 Lohn



Es gibt viele verschiedene Gründe, warum ein Hack begangen wird. Der Lohn ist oft gleichbedeutend mit den Motiven des Angreifers.

Abbildung 18: UZ5 - Der Lohn
Quelle: Eigene Darstellung

Persönliche Gründe

[UZ5TZ2]

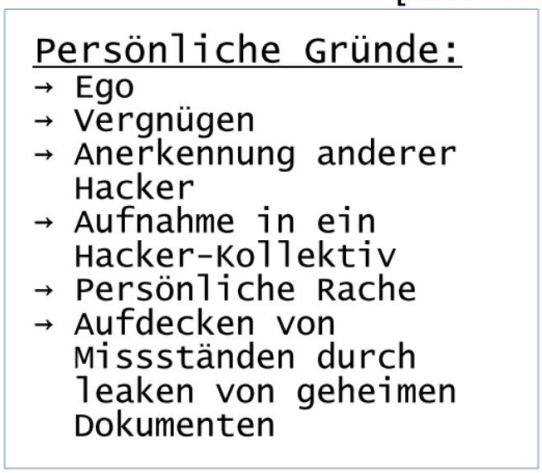


Abbildung 19: UZ5TZ2 - Persönliche Gründe
Quelle: Eigene Darstellung

Ein Hack kann durch persönliche Gründe motiviert sein. Viele kleinere Hacker und Hackergruppen agieren rein aus Spaß oder um ihrer Egos willen. Dabei spielt die Anerkennung anderer Hacker auch eine große Rolle und kann zu Aufnahme in Hackerkollektiven führen oder der Hack kann als „Test“ für die Aufnahme gelten. Viele geleakte Daten, wie sie bei WikiLeaks[59] veröffentlicht werden, stammen ursprünglich aus Hacks. Persönliche Gründe von Hackern sind oft undurchsichtig und verflochten. Sie können von harmlosen Scherzen wie dem Weiterleiten einer amerikanischen Regierungswebsite auf Schwulenpornos bis hin zu lebenszerstörender, persönlicher Rache führen.

Profit als Lohn

[UZ5TZ1]

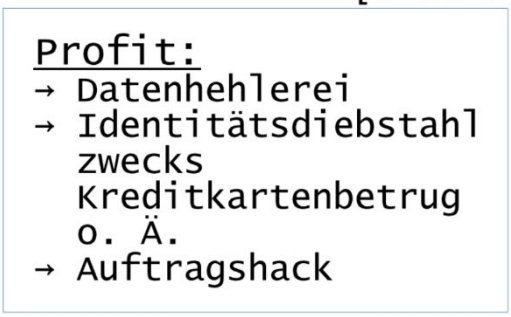


Abbildung 20: UZ5TZ1 - Profit als Lohn
Quelle: Eigene Darstellung

Beim Hacken gibt es drei grundsätzliche Möglichkeiten, Profit zu machen. Datenhehlerei spielt besonders bei Hacks von Unternehmen eine Rolle. Je nach den gestohlenen Daten sind diese der Konkurrenz möglicherweise viel wert. Wie der Wert sich genau zusammensetzt, wird in UZ5TZ1a näher beschrieben. Der Hacker muss sich bei der Datenhehlerei selbst um den Absatz seiner erbeuteten Daten kümmern. Eine klassische Methode, als Dieb Profit zu machen, ist der Identitätsdiebstahl. Ein Taschendieb klaut möglicherweise die EC-Karte und geht damit einkaufen. Ähnlich könnte ein Hacker auch vorgehen. Hat er zum Beispiel Zugriff auf das LAN des Opfers, weil er den Haupt-PC bereits infiziert hat, kann er von dort das Handy des Opfers infizieren. Mit einem Keylogger auf dem PC des Opfers kann er das Passwort für das Konto des Opfers erhalten und über das gehackte Handy kann er die TAN abfangen. So kann ein Hacker Geld direkt vom Konto seines Opfers transferieren und es in eine digitale Währung wie Bitcoins umwandeln, die nichtmehr zurückzuverfolgen ist. Eine Möglichkeit für einen Hack bezahlt zu werden, besteht darin einen Auftrag zu erhalten. In diesem Fall kann es zum einen sein, dass der Hacker ein Auditor ist

[59] www.wikileaks.org

und auf legalem Wege von dem Unternehmen bezahlt wird, die er gehackt hat. Zum anderen werden auch Aufträge für Hacker im Darknet und ähnlichen Netzen vergeben. Der Hacker wird hier vermutlich, im Austausch für die Daten ebenfalls in einer digitalen Währung bezahlt.

Datenwert

[UZ5TZ1a]

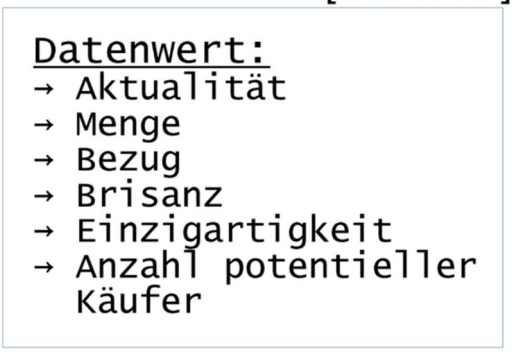


Abbildung 21: UZ5TZ1a - Datenwert
Quelle: Eigene Darstellung

Der Wert von Daten ist nur schwer zu schätzen, da es sich eigentlich um Informationen handelt und diese ihren Wert durch andere Informationen erhalten. Informationen sind nach den hier gelisteten Faktoren unterschiedlich viel Wert. Der Hacker muss darüber hinaus selbst in Aktion treten, um diese Informationen anzubieten und zu verkaufen. Er muss ebenso den Besitz, der Daten und deren Integrität beweisen. Datenhehlerei ist für den Hacker demnach mit relativ viel Aufwand und Risiko verbunden. Daher ist es wahrscheinlicher, dass ein Hacker, vor dem Hack, bereits weiß an wen er seine Daten verkaufen möchte.

2.3.3.6 Wiederholungen des Kreislaufs

Von vorne zu beginnen kann viele Gründe haben. Für den Auditor und manche Auftragshacker ist dies einfach ihre Arbeit. Denkbar wäre auch, dass die Daten korrumpiert worden oder schlicht nicht zufriedenstellend sind. In einigen Fällen führt ein Hack zum nächsten oder gibt Anreiz für einen weiteren oder wie im Beispiel von Unterkapitel 2.3.3.1 könnte der erste Durchlauf nur ein Teilschritt sein.

Im hier dargestellten Zyklus sind viele mögliche Teilschritte enthalten. Nicht bei jedem Angriff sind diese alle notwendig, beziehungsweise sinnvoll.

Zusammenfassend kann man sagen, dass der größte Teil der Arbeit oft auf die Phase der Datensammlung entfällt. Zusammen mit dem eigentlichen Hack erfordert die Datensammlung ein gesteigertes Maß an Social Engineering. Da der Mensch oft die größte Angriffsfläche bietet wird sich das Kapitel 3 mit dem Thema „Social Engineering“ befassen.

2.4 Häufige Arten klassischer Cyber-Angriffs-Vektoren

In diesem Kapitel wird erklärt, welche Angriffsarten am häufigsten vorkommen und wie sie funktionieren. Falls Gegenmaßnahmen existieren, werden auch diese angesprochen. Auf die Erklärung der genauen Funktionsweise und des Ablaufs der Methoden beziehungsweise Schadware wird verzichtet, da es hier um das Wissen über die Methoden selbst sowie ihre Gegenmaßnahmen gehen soll. Angriffe wie diese werden oft kombiniert um das Ziel zu erreichen, wie im Beispiel mit der Handy-TAN aus Unterkapitel 2.3.3.5. Es ist äußerst unwahrscheinlich, dass ein Angreifer alleine mit einer dieser Methoden an sein Ziel kommt.

2.4.1 Aktive Angriffe

Aktive Angriffe sind Angriffe, bei denen der Angreifer aktiv am Geschehen teilnehmen muss, um den Angriff auszuführen und sein Ziel zu erreichen.

Der **Zero-Day-Exploit** bezeichnet das Ausnutzen einer Schwachstelle am Tag des Bekanntwerdens oder davor.[60] Dadurch bleibt den Softwareherstellern keine Zeit, diese Lücke vor Eingehen der ersten Angriffe zu beheben, ihnen bleiben also 0 Tage.

Beim **Drive-by-Exploit** wird Schadcode auf einer Website eingebettet und über Lücken im Browser vom Nutzer unbemerkt Schadware auf dessen Rechner installiert.[61] Gegenmaßnahmen:

- Aktuellste Browserversion verwenden.
- Script- sowie Adblocker verwenden und Flashplayer deaktivieren, da die meisten solcher Angriffe über Flash und Javascript kommen.

Die **Watering-Hole-Attack** ist eine spezielle Form des Drive-by-Exploit. Es ist eine Praxis, bei der der Angreifer eine häufig vom Opfer frequentierte Webpage infiziert und dabei einen Drive-by-Exploit nutzt um die Zielgruppe zu infizieren. Watering-Hole-Attacks werden vor allem für die Infektion von Unternehmen oder Regierungen benutzt.[62] Watering-Hole-Attack bedeutet wörtlich übersetzt „Wasserloch-Angriff“ und soll auf das Wasserloch anspielen, an dem sich die selben Tiere wiederholt treffen um zu trinken. Dabei müssen auch die Tiere am Ende der Nahrungskette ihr Revier verlassen und ein Wasserloch aufsuchen an dem sie sich sicher fühlen. Der Angreifer informiert sich bei diesem Angriff gründlich über seine

[60] BSI, Glossar der Cyber-Sicherheit (Begriff: Zero-Day-Exploit)

[61] BSI, Lage der IT-Sicherheit in Deutschland 2016 (Abschnitt 1.2.8 – Seite 29)

[62] BSI, Lage der IT-Sicherheit in Deutschland 2016 (Abschnitt 1.2.8 – Seite 30)

Zielgruppe und nutzt deren Gewohnheiten aus um den Drive-by-Exploit wirksam zu platzieren.
Gegenmaßnahmen:

- Siehe Drive-by-Exploit.

Bei einem **Man-in-the-Middle Angriff** schaltet sich ein Angreifer zwischen zwei Kommunikationspartner und spiegelt diesen gegenseitig jeweils die Identität des anderen vor. Dadurch kann er allen Datenverkehr, den die beiden miteinander austauschen, sowohl mitlesen als auch manipulieren.[63] Durch diese Angriffstechnik kann der Angreifer die Verschlüsslung der beiden Kommunikationspartner umgehen, da beide Partner mit ihm die Verschlüsslungen eingegangen sind und er so den gesamten Verkehr entschlüsseln kann.
Gegenmaßnahmen:

- Extended-Validation-SSL-Zertifikate die die Identität des Kommunikationspartners eindeutig bestätigen.

Bei der **Denial-of-Service Attack**, kurz DoS-Angriff, ist das Ziel der Angreifer die Funktionsfähigkeit des Zielobjekts zu verhindern. Dies geschieht oft durch das Überfüllen des betreffenden Servers mit Anfragen. Dadurch sind Internetdienste für die Dauer des Angriffs nicht erreichbar. Das Ziel ist es durch die Nichtverfügbarkeit der Dienste wirtschaftlichen Schaden anzurichten.[64] Eine **Distributed Denial-of-Service Attack**, kurz DDoS-Angriff, wird nicht nur von einem Rechner, sondern von mehreren gleichzeitig ausgeführt, die beispielsweise vorher mit Botnetzsoftware infiziert wurden.[65]
Gegenmaßnahmen:

- DoS: Die IP-Adresse blockieren, von der die Anfragen kommen. Häufig wird dies vom Provider oder dem Router bereits erledigt.
- DDoS: Keine allgemein wirksamen. DDoS Angriffe können, zum Beispiel durch IDS, erkannt werden und die betreffenden Systeme können heruntergefahren werden um den Schaden durch beispielsweise verlorene Daten zu minimieren.

2.4.2 Passive Angriffe

Im Gegensatz zu den aktiven Angriffen muss der Angreifer bei passiven Angriffen den Angriff nur initiieren. Danach läuft dieser automatisch ab.

---

[63] Heise Online, Glossar - Man-in-the-Middle-Angriff (MITM)

[64] BSI, Glossar der Cyber-Sicherheit (Begriff: DOS / DDoS-Angriffe)

[65] BSI, Glossar der Cyber-Sicherheit (Begriff: DOS / DDoS-Angriffe)

Brute-Force bedeutet „rohe Gewalt“. Der Angreifer versucht dabei durch ausprobieren von möglichst vielen Passwörtern in möglichst kurzer Zeit, das richtige Passwort zu erraten.[66]
Gegenmaßnahmen:

- Lange und kryptische Passwörter mit möglichst vielen verschiedenen Zeichentypen (Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen). Das Erstellen eines sicheren Passwortes wird in Unterkapitel 4.3 näher erläutert.
- Bei Brute-Force-Angriffen über das Internet können die jeweiligen Anbieter der Dienste und Websites nur wenige Versuche das Passwort einzugeben, pro Zeiteinheit, zulassen.

Ein **Virus** ist ein Stück Software, das andere Dateien infiziert, indem es sich in deren Code einschreibt und dadurch mit den infizierten Programmen startet. Danach lädt er beliebige Schadware aus dem Internet nach und verbreitet sich dadurch weiter, indem es andere Dateien infiziert und mit ihnen den Vorgang wiederholt.[67] Wie ein biologischer Virus ist der Computervirus alleine nicht funktionsfähig und braucht andere Dateien, die er infizieren kann, um sich zu verbreiten.
Gegenmaßnahmen:

- Sicheres Onlineverhalten durch Sicherheitsbewusstsein: Keinen Download von unbekannten oder nicht vertrauenswürdigen Quellen durchführen, Deaktivieren von Scripten, Blockieren von automatischen Makros und ähnlichen Funktionen. In Kapitel 4 wird noch näher auf das Sichere Onlineverhalten eingegangen.
- Nach der Infektion können Viren mit Anti-Viren-Software entfernt werden.

Ein **Trojaner** ist eine Form der Schadware, die sich als harmloses Programm ausgibt oder sich in einem harmlosen Programm versteckt und beim ausführen des Programms mit gestartet wird, wodurch der Schadcode zur Ausführung kommt.[68]
Gegenmaßnahmen:

- Siehe Virus

Ein **Wurm** ist eine Form der Schadware, die sich im Gegensatz zum Virus selbstständig verbreiten kann und keine Dateien infiziert, sondern selbst die Schadwaredatei ist. Er verbreitet sich eigenständig über Computernetze und kann seinen Schadcode zu jeder Zeit

[66] BSI, Glossar der Cyber-Sicherheit (Begriff: Brute-Force-Angriff)

[67] Gabler Wirtschaftslexikon, Stichwort: Virus

[68] Gabler Wirtschaftslexikon, Stichwort: Trojaner

ausführen.[69]
Gegenmaßnahmen:

- Siehe Virus

Sniffing ist eine Methode, bei der der Angreifer den Netzverkehr mit Hilfe eines Netzwerk-Sniffers mitschneidet, um diesen später zu analysieren und Informationen aus ihm zu gewinnen. Der Angreifer muss sich für diese Art des Angriffs im selben Netzwerk wie das Ziel befinden.[70]
Gegenmaßnahmen:

- Verschlüsselung des Datenverkehrs, zum Beispiel durch VPNs

Beim **Wörterbuchangriff** verwendet der Angreifer eine Liste mit möglichen Passwörtern und probiert diese automatisiert der Reihe nach durch.[71] Dabei kann die Liste der Passwörter sowohl reguläre Wörter aus dem Duden enthalten als auch Slang-Ausdrücke oder Wörter aus dem persönlichen Umfeld des Opfers. Dabei kann der Angreifer die Passwörter auch kombinieren oder abändern um seine Liste zu erweitern.
Gegenmaßnahmen:

- Sicheres, Kryptisches Passwort verwenden wie es im Unterkapitel 4.3 erklärt wird.

Der **Angriff auf Standardpasswörter** sowie Standard-Logins beschreibt einen Angriff bei dem alle gängigen Standardbenutzer und Standardpasswörter und ihre Kombinationen durchprobiert werden. Hersteller verwenden beim Ausliefern ihrer Geräte häufig einfache Benutzernamen und Passwörterkombinationen wie zum Beispiel „Admin“, „admin“. Die Hersteller weisen oft darauf hin, dass diese Passwörter nach dem ersten Gebrauch zu ändern sind. Häufig wird dies allerdings vergessen oder ignoriert.
Gegenmaßnahmen:

- Standardpasswörter austauschen.

---

[69] Gabler Wirtschaftslexikon, Stichwort: Wurm

[70] Gabler Wirtschaftslexikon, Stichwort: Sniffer

[71] ITWissen.info, Wörterbuchangriff

3 Social Engineering

In diesem Kapitel wird der Begriff des Social Engineering diskutiert und umfangreich beleuchtet, da er oft nur einseitig und unzulänglich behandelt wird. Die gängigen Definitionen des Social Engineering erfassen nicht das ganze Thema, weshalb der Begriff oft missverstanden wird. In diesem Kapitel wird der Bezug zur IT-Sicherheit hergestellt und der Begriff umfangreich definiert sowie kritisch diskutiert und eingeordnet.

3.1 Definition

Der Begriff Social Engineering wurde erstmals 1945 im Buch „*The Open Society and Its Enemies“* von dem politischen Philosophen Karl Popper verwendet. Darin benutzt er den Begriff in einem stark politischen Zusammenhang. Popper definiert den Social Engineer als eine Person, die die Möglichkeiten des Social Engineering nicht zu seinem Vorteil nutzt, sondern der Gesellschaft dienlich. Dabei soll er mit ingenieurswissenschaftlichen Methoden das soziale Umfeld verändern. Daher der Begriff Social Engineering, wörtlich übersetzt „Sozial-Technik“.[72]

In den 1970er Jahren wurde der Begriff durch die Adaption auf ältere Werke populär. So wurde das „Behaviorist Manifesto“, das bereits 1913 von John B. Watson, einem US-amerikanischem Psychologen[73], verfasst wurde, mit dem Begriff des Social Engineering in Verbindung gebracht und in diversen Publikationen neu diskutiert, wie zum Beispiel von Alan E. Kazdin in seinem Buch *„History of behavior modification: Experimental foundations of contemporary research“.*[74] Watson untersuchte als einer der ersten Psychologen Verhaltensmanipulation frei von sozialem Stand oder Rasse. Ihm wird unter anderem folgendes Zitat zugeschrieben:

„Give me a baby and I can make any kind of man“ - zu Deutsch: *„Gib mir ein Baby und Ich kann jede Art von Mensch aus ihm machen“*

Der Begriff wurde dadurch in den 1970ern zum ersten Mal populärwissenschaftlich mit der gezielten Beeinflussung oder Manipulation von Menschen und insbesondere Kindern in Verbindung gebracht.

---

[72] Karl Popper, The Open Society and its Enemies (Kapitel 4 – Seite 25 f.)

[73] John B. Watson, Behaviorist Manifesto

[74] Alan E. Kazdin, *History of behavior modification: Experimental foundations of contemporary research*

Mit der Sicherheit wurde der Begriff nachträglich das erste Mal mit Ereignissen der 1970er bis 1990er assoziiert. Damals kam mit dem neu gebauten Telefonnetz das „Phreaking“ auf, eine Praxis, bei der mit Methoden des Social Engineering kostenlose Telefonanrufe oder ganze Telefonanschlüsse erschlichen wurden.[75]

Heute wird der Begriff stark mit der IT-Sicherheit in Verbindung gebracht. Durch immer besser abgesicherte Rechnernetze und komplexere Verschlüsselungsmethoden, wurde es mit der Zeit schwieriger, den Key einer verschlüsselten Leitung zu errechnen oder zu hacken. Mit dem Einführen von aus heutiger Sicht nicht trivial hackbaren Verschlüsselungsstandards wie zum Beispiel AES bekam der Mensch als Lücke im System immer mehr Aufmerksamkeit.

In Deutschland gewann der Begriff bei dem BKA und dem BSI erst 2005 an Bedeutung mit der ersten Erwähnung von Social Engineering im „Lagebericht der IT-Sicherheit in Deutschland 2005“.[76] Später wurde der Begriff in der Bevölkerung populärer durch Werke wie den international erfolgreichen, deutschen Film „Who am I – Kein System ist sicher“.[77]

Seitdem wurde der Begriff oft in Verbindung mit Sicherheit und insbesondere mit der IT-Sicherheit definiert, aber fast immer negativ konnotiert.

Norton definiert:
„Beim Social Engineering missbrauchen Cyberkriminelle zwischenmenschliche Interaktionen, um den Nutzer zur Preisgabe sensibler Informationen zu bewegen. Da Social Engineering auf der menschlichen Natur und gefühlsmäßigen Reaktionen basiert, gibt es zahlreiche Möglichkeiten, mit denen Angreifer Sie hereinlegen können – online und offline.“[78]

Anders gesagt geht es also um das Ausnutzen von menschlichem Vertrauen, um sich selbst einen Vorteil zu verschaffen. Erfolg hat der Social Engineer im Allgemeinen, wenn er dabei nicht als solcher entdeckt wird, oder erst erkannt wird, wenn es für sein Opfer zu spät ist. Jedoch weckt diese Definition von Norton den Eindruck, Social Engineering sei zwingend eine bösartige Handlung von Cyberkriminellen.

Tatsächlich umgibt uns Social Engineering in jedem Aspekt unseres Lebens und wird auf die eine oder andere Art und Weise von jedem angewendet. Diese Verflochtenheit zwischen Handlungen, die wir als gut oder schlecht ansehen, macht es noch schwieriger, eine bösartige Manipulation zu erkennen.

---

[75] Boris Gröndahl, Hacker Seite 38 f.

[76] BSI, Lage der IT-Sicherheit in Deutschland 2005 (Abschnitt 4.2.1 – Seite 18)

[77] Baran bo Odar, Who am I – Kein System ist sicher (Film)

[78] Norton_Team, Was ist Social Engineering? (Arten von Social Engineering-Angriffen)

Definieren wir Social Engineering also lieber wertungsfrei als: **„Das gezielte Beeinflussen menschlichen Handelns, damit etwas getan wird, was ohne diesen Einfluss nicht getan worden wäre."**

Tatsächlich ist Social Engineering darüber hinaus ein Gesamtkonzept, welches sich nur schwer in eine prägnante Definition pressen lässt und gleichzeitig die volle Tragweite des Begriffes abdeckt. Zum Konzept des Social Engineering gehören unter anderem folgende Eigenschaften:

- Das deduktive sowie persönliche Erkennen von Zusammenhängen in verschiedenen Ebenen menschlicher Interaktion.
- Das vollkommene Verkörpern anderer Personen oder zumindest die Fähigkeit sich in diese hineinzuversetzen.
- Das richtige Erkennen und Deuten von Emotionen.
- Starke Selbstreflektion.
- Erweiterte psychologische Kenntnisse.
- Eine starke Vorstellungskraft.

Nicht jeder Social Engineer muss all diese Felder beherrschen, noch kann jeder alles erlernen. Beim Social Engineering verbindet der Social Engineer viele verschiedene Bereiche der Wissenschaft miteinander, um ein gewünschtes Ziel zu erreichen. Dabei muss dieses nicht negativ motiviert sein, sondern kann auch einen uneigennützigen Hintergrund haben. Im nächsten Kapitel werden einige Arten von Social Engineers diskutiert, um die Sicht auf diese neue Begriffsauffassung des „Social Engineering" mit bekannten Bildern zu verknüpfen.

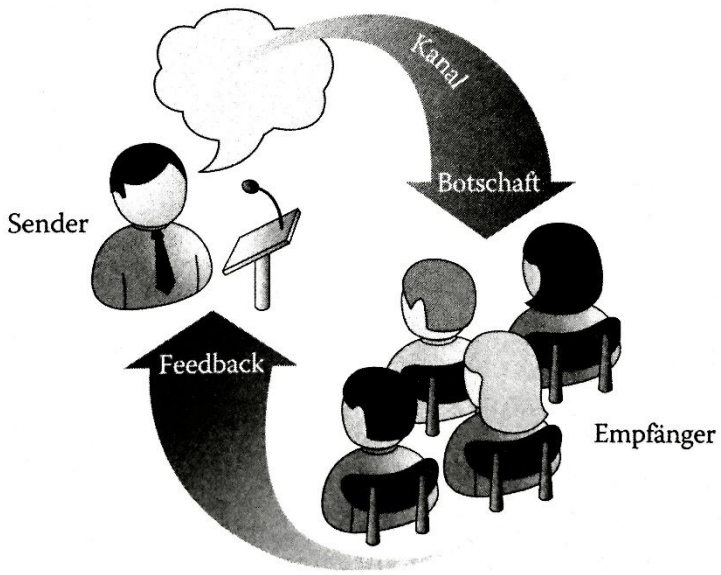


Abbildung 22: Kommunikationsmodell nach D. C. Balmund
Quelle: Christopher Hadnagy, Die Kunst des Human Hacking (Kapitel 2.3.1 – Seite 74)

Abbildung 21 zeigt das Kommunikationsmodell nach D. C. Balmund, wie es in der deutschen Fassung von Christopher Hadnagys Buch „Die Kunst des Human Hacking" enthalten ist. Ein Social Engineer versucht Kommunikation zu Manipulieren oder zu verbiegen, um an sein Ziel zu gelangen. Dadurch bleiben ihm zwei Angriffsmöglichkeiten. Die Manipulation des Kanals oder der Botschaft selbst, um beim Empfänger das gewünschte Feedback zu erzeugen. Hierzu folgen zwei Beispiele:

Ein Produkt das verkauft wird, enthält nur einen geringen Anteil an einem bestimmten Wirkstoff. Durch geschickte Formulierungen in der Produktbeschreibung und das Verwenden gleicher Mengenangaben wird dem Verbraucher suggeriert, das Produkt enthalte deutlich mehr des gewünschten Wirkstoffs. Im Kleingedruckten auf der Rückseite wird eine ungewöhnliche aber zulässige Schreibweise der Wirkstoffmenge benutzt wodurch der Verbraucher zusätzlich verwirrt wird. Er geht nun davon aus, dass das Produkt ein Schnäppchen sei und kauft es. Hier wurde eine Manipulation an der Botschaft durchgeführt und der Verkäufer konnte so Gewinn erschleichen.

Eine Phishing-Seite ist offensichtlich. Beim Versuch, die Seite zu schließen, wird oft ein Pop-up des Browsers eingeblendet, welches fragt, ob die Seite wirklich geschlossen werden soll. Der Social Engineer hat nun eine Bilddatei, die genauso aussieht, wie das Pop-up, an derselben Position auf der Seite platziert, wodurch das Opfer wie selbstverständlich auf den „Schließen“-Button drücken will. Es klickt auf das Bild und der PC wird infiziert. In diesem Beispiel wurde der Kanal selbst manipuliert, da dem Opfer ein anderer Kanal als der erwartete vorgespielt wurde und es auf diesen Trick hereingefallen ist.

Klassische Kommunikationskanäle sind etwa die Sinne des Menschen. Modernere Kanäle sind zum Beispiel ein Chat oder jegliche Art der Interaktion mit Menschen oder Maschinen. Die Botschaft selbst ist gleichbedeutend mit dem Inhalt beziehungsweise der Aussage einer Kommunikation.

Bei all seinen Ausprägungen nimmt Social Engineering für den Betrachter immer neue Formen an. Es benötigt weder das Vorspiegeln einer falschen Identität, das Verstellen der eigenen Persönlichkeit, noch das Anwenden von Tricks oder Lügen, um eine Handlung als Social Engineering beschreiben zu können. Viel mehr beschreibt Social Engineering das Gesamtkonzept der Beeinflussung, in Verbindung mit dem Social Engineer als Person, der gelernt hat, dieses Konzept und damit auch die wahrgenommene Realität seiner Kommunikationspartner zu verbiegen.

3.2 Social Engineers in der Gesellschaft

Um das Thema etwas greifbarer zu machen, folgt in diesem Abschnitt eine Vorstellung von verschiedenen Weisen, wie Social Engineering in unserer Gesellschaft täglich angewendet wird.

Ärzte, Psychologen, Rechtsanwälte und Pädagogen wenden in ihren Berufen die gleichen und andere Methoden der Beeinflussung an, um ihre Patienten, Mandanten oder Schützlinge positiv zu beeinflussen. Darüber hinaus müssen besonders Pädagogen und

Psychiater die Kinder beziehungsweise ihre Patienten oft stark beeinflussen oder ihnen geschickt Informationen entlocken, um ihnen zu helfen. Gleichzeitig dürfen sie das positive Gefühl der Kinder beziehungsweise Patienten, zu ihnen nicht zerstören. Diese Kategorie von Social Engineers nutzt ihre Fähigkeiten also im Allgemeinen, um anderen Menschen zu helfen.

Kinder sind eines der besten Beispiele für Social Engineers. Sobald Kinder merken, auf welche Arten sie Erwachsene beeinflussen können, um an ihre Ziele zu kommen, wenden sie dieses Verhalten ganz bewusst, verstärkt an, um zu bekommen was sie wollen. Oft wird dies von den Eltern zunächst nicht ernst genommen, unterbewusst können sie ihrem Kind in dem Moment in dem es sie ansieht, nichts mehr abschlagen, obwohl sie wissen, dass sie grade Manipuliert werden sollen. Gerade dann, wenn vorher ein positives Gefühl des Vertrauens, auch Rapport genannt, erzeugt wird indem es vorher noch Sätze sagt wie: „Papa, ich hab dich ganz doll lieb!“

Hacker und Penetrationstester sind die Gruppe, um die sich diese Arbeit dreht. Jeder kennt Phishing beziehungsweise Spam-Mails bei denen mit Penisvergrößerungen, Abnehmpillen oder Ähnlichem gelockt wird. Diese E-Mails existieren seit der Erfindung der E-Mail und sind trotzdem auch heute noch bei einigen Menschen effektiv. Anderenfalls würden die Verteiler sich nicht die Mühe machen, ständig neue zu entwerfen. Obwohl jeder Mensch diese offensichtlichen Spam-Mails eigentlich als solche identifiziert, klicken immer wieder Leute auf sie und möchten sich diese Produkte kaufen. Dies funktioniert nur, weil die Ersteller der Nachrichten geschickt auf die versteckten Wünsche vieler Menschen eingehen und eine zauberhafte Lösung für all ihre Probleme anbieten. Das dahinterstehende Prinzip ist das scheinbare Stillen eines Verlangens, welches Vertrauen (Rapport) aufbaut. Dieses Vertrauen wird von den Angreifern anschließend ausgenutzt, indem sie das gezahlte Geld einbehalten, aber kein Produkt liefern, überteuerte Preise für komplett wirkungslose Produkte verlangen oder über Lücken im Browser einen Drive-By-Exploit ausführen, um den PC der betreffenden Person zu kompromittieren.
Penetrationstester nutzen, sofern die Situation es erfordern, alle ihnen bekannten Methoden des Social Engineering, um den Audit erfolgreich auszuführen. Dabei benutzen sie diese, um sie hinterher offen zu legen und die Mitarbeiter bei gelungenem Audit mit ihren Pannen zu konfrontieren und sie zu Schulen. Dadurch können sie das Sicherheitsbewusstsein stärken, sowie die Auswirkungen eines echten Social-Engineering-Angriffs mindern. Penetrationstester sind eine weitere Gruppe, die ihre Fähigkeiten benutzen, um Menschen zu helfen, auch wenn es zunächst nicht so scheinen mag.

In der **Werbebranche** wird vermutlich am meisten massentaugliches Social Engineering verwendet. Werbung nutzt ein sehr breites Spektrum dieses Konzepts zu ihrem Vorteil, indem sie Produkte meist nicht sachlich bewirbt, sondern eine Bindung zwischen Zuschauer und Produkt herstellt. Dabei ist nicht wichtig, ob das Gesehene realistisch ist, sondern nur, dass es ein positives Gefühl hinterlässt. Dieses Gefühl verknüpft der Zuschauer mit dem Produkt und wird dieses Produkt eher einem ihm unbekannten, nicht beworbenem Produkt

vorziehen. Dabei werden in der Werbung geschickt Emotionen in Bild- und Ton-Form verwendet und das einfache Instrument der Wiederholung, um die Erinnerung zu stärken und das Gefühl mit dem Produkt zu verbinden. Robert B. Zajonc hat bereits 1965 eindrucksvoll in einem Experiment nachgewiesen, wie einflussreich alleine das Instrument der Wiederholung ist. Er streute Schriftzeichen und Phantasiewörter in Schülerzeitungen ein und ließ die Studenten diese Wörter später nach ihrer Güte bewerten. Das Experiment hatte zur Folge, dass die Studenten, die eine hohe Frequenz der Zeichen oder Wörter in ihrer Zeitung hatten, alle diese Wörter später positiver bewerteten als andere, die sie nicht gelesen hatten. Dabei kannten sie weder ihre Bedeutung noch wussten sie, dass sie diese schon einmal gelesen hatten.[79]

Verkäufer in Kaufhäusern verwenden ebenso Techniken, die zum Bereich des Social Engineering gezählt werden können. Hadnagy schreibt in seinem Buch, dass Verkaufspersonal dem Kunden erst persönliche Daten entlockt, um danach dessen Bedürfnisse herauszufinden und ihre Waren zu verkaufen[80] oder in besonders geschickten Fällen, diese Bedürfnisse überhaupt erst zu wecken. Malt ein Verkäufer zum Beispiel ein gut vorstellbares Bild aus, das auf den Kunden zugeschnitten wurde, stellt dieser sich vor, in dieser Situation zu sein, so als hätte er den Gegenstand bereits. Dadurch kann tatsächlich spontan ein Wunsch geweckt werden, den der Kunde vorher nicht verspürt hat. Verkäufer nutzen also das Entlocken von Informationen (Elizitieren), beeinflussen die Kunden und nutzen psychologische Prinzipien um diesen zu einem Kauf zu bewegen, den sie ohne die Verkäufer vermutlich nicht getätigt hätten.

Bei Verkäufern oder Vertretern fühlt der potentielle Kunde sich oft schlecht, besonders wenn er angesprochen wird, weil er genau weiß, dass ihm etwas „angedreht“ werden soll. Er weiß instinktiv, dass sehr wahrscheinlich ein Manipulationsversuch folgt und möchte diesen vermeiden, da er normalerweise nicht manipuliert werden will. Bei Werbung oder Kindern wissen die meisten Menschen ebenfalls, dass sie manipuliert werden sollen. Trotzdem fühlen sie sich nicht schlecht, sondern wimmeln in einen Moment den Vertreter an der Tür ab, um sich im nächsten Moment vor ihren Fernseher zu setzen und genüsslich Stunden an Werbung zu konsumieren, ohne sich dabei schlecht zu fühlen. Ein so betrachtet paradoxes Verhalten. Passive Werbung erschafft somit die Illusion, selbst entscheiden zu können und wird deshalb nicht als so unangenehm und aufdringlich empfunden wie der Vertreter an der eigenen Haustür.
Jeder Mensch der Handlungen mit Vorsatz begeht und dabei andere teilweise im Unklaren lässt, benutzt Social Engineering und sehr wahrscheinlich die im folgenden Kapitel genannten Prinzipien.

---

[79] Robert B. Zajonc, The attitudinal effects of mere exposure (Seiten 76 und 78)

[80] Christopher Hadnagy, The Art of Human Hacking (Kapitel 1.2.2 – Seite 41)

3.3 Prinzipien

In diesem Kapitel sollen die am häufigsten angewendeten Prinzipien des Social Engineering besprochen werden. Beherrscht ein Social Engineer eines dieser Prinzipien vollkommen wird dies als „Skill“, also Fähigkeit, eines Social Engineers bezeichnet. Dort wo diese Prinzipien angewendet werden, aber nicht ausdrücklich erwünscht sind, ist es oft zum Nachteil des Manipulierten. Das beste Beispiel hierfür ist Werbung, denn sie hilft nicht, eine objektive Kaufentscheidung zu treffen, eher im Gegenteil. Kennen Personen diese Prinzipien und haben ihre Funktionsweise verinnerlicht, können sie wieder die eigentliche Information filtern und freier über ihr Handeln entscheiden. Die hier aufgeführten Prinzipien sind nicht alle in diesem Zusammenhang definiert oder direkt erwähnt worden. Viele entstammen eigenen Überlegungen nach der eingehenden Beschäftigung mit dem Thema des Social Engineering.

Rapport ist ein Begriff, der eigentlich militärisch geprägt ist und eine Art Berichterstattung auf Wunsch oder Befehl hin darstellt.[81] Er wird aber auch in der Psychologie benutzt und bezeichnet hier eine Bindung zwischen dem Therapeuten und dem Patienten. Sigmund Freud bezeichnete den Rapport als „*leistungsfähige Übertragung*“,[82] die sich zwischen dem Patienten und dem Therapeuten bilden muss, quasi eine Art Vertrauensverhältnis. Menschen, die ein Rapportverhältnis zueinander haben, sind eher dazu geneigt, auf Ratschläge oder Forderungen zu hören und hinterfragen sich gegenseitig weniger. Die Skepsis bleibt also meistens aus. Darüber hinaus beschreibt Christopher Hadnagy in einem ganzen Kapitel, dass der Schlüssel zum Rapport meist die Empathie ist.[83] Empathie ist eine Art Vorstufe des Rapportes und bedeutet eine „*intellektuelle Identifikation […] mit den Gefühlen, Gedanken, und Standpunkten*“ einer Person.[84] Diese Empathie kann auf viele Arten hergestellt werden, zum Beispiel durch bloßes Zuhören einer Person, die sich dadurch verstanden fühlt oder durch kleinere psychologische Tricks.

Commitment ist eine Art Verpflichtung beziehungsweise ein Gefühl der Verpflichtung, das eng mit dem Prinzip der **Konsistenz** zusammenhängt. Das Prinzip des Commitment nutzt dabei den Drang des Menschen zu konsistentem Verhalten. Hadnagy schreibt über das Commitment und die Konsistenz Folgendes:

---

[81] Duden Suchbegriff „Rapport“ (Definition 1)

[82] Sigmund Freud, Kleine Schriften I (Kapitel 17 - Zur Einleitung der Behandlung, Weitere Ratschläge zur Technik der Psychoanalyse I)

[83] Christopher Hadnagy, Die Kunst des Human Hacking (Kapitel 5.5.6 – Seite 212)

[84] The Random House Dictionary Suchbegriff „empathy“ (Definition 1)

„*Der Schlüssel, um die Prinzipien Commitment und Konsistenz zur Manipulation einzusetzen, besteht im ersten Commitment. Das heißt, nachdem man ein Commitment eingegangen ist oder eine Stellung bzw. Position bezogen hat, ist man eher geneigt, Anfragen bereitwillig zu erfüllen, die mit dem vorigen Bekenntnis konsistent sind. Viele Profis […] werden versuchen, andere in eine Anfangsposition zu bringen, die mit einem Verhalten konsistent ist, das sie später abfragen oder einfordern werden.*“[85]

Das **Elizitieren** ist ein Prinzip der starken Beeinflussung, ohne das beim Gegenüber Misstrauen entsteht. Hadnagy schreibt über das Elizitieren: „*Mit Elizitieren ist gemeint, etwas hervorzubringen oder aufzudecken, jemandem etwas zu entlocken oder per Logik zu einer Schlussfolgerung zu gelangen (der Wahrheit beispielsweise). Alternativ wird Elizitieren definiert als ein Reiz oder Stimulus, der eine bestimmte Gruppe oder Verhalten auf oder abruft […]. […] In den Schulungsunterlagen definiert die National Security Agency der USA Elizitieren als >>subtile Extraktion von Informationen während einer offenbar normalen und harmlosen Unterhaltung<<.“*[86] Auf die Frage, warum Elizitieren so gut funktioniert, nennt Hadnagy folgende Gründe:

„

- *Die meisten Menschen wollen gern höflich sein, vor allem zu Fremden.*
- *Profis wollen gut informiert und intelligent erscheinen.*
- *Wenn man gelobt wird, redet man oft mehr und plaudert auch mehr aus.*
- *Die meisten würden nicht um des Lügens willen lügen.*
- *Die meisten Menschen reagieren freundlich auf andere, die sich scheinbar um sie kümmern.*

„[87]

Damit sind gleichzeitig die Grundmechanismen des Elizitierens genannt. Elizitieren ist ein Prinzip, welches normalerweise von Angesicht zu Angesicht stattfindet. Mit genügend Rapport kann es aber auch problemlos per Telefon oder Chat angewandt werden.

Pretexting ist eine Technik, in der eine vom Anwender fingierte Situation dazu benutzt wird, an sensible Informationen zu gelangen oder das Ziel zu einer Handlung zu bewegen. Trivial ausgedrückt ist ein Pretext ein Vorwand, doch bezeichnet der Begriff mehr als nur den Vorwand oder eine bloße Lüge. Bei Pretexting kommt es nicht selten vor, dass der Angreifer eine komplette Identität erschafft, um seiner herbeigeführten Situation den nötigen Realismus zu verleihen. Dabei muss der Social Engineer diese Person „leben“ und sich in allen

[85] Christopher Hadnagy, Die Kunst des Human Hacking (Kapitel 6.2.6 – Seite 260)

[86] Christopher Hadnagy, Die Kunst des Human Hacking (Kapitel 3.1 – Seite 82)

[87] Christopher Hadnagy, Die Kunst des Human Hacking (Kapitel 3.1 – Seite 83)

Situationen mit der Rolle konsistent zeigen. Pretexting erfordert vor allem eine sehr gründliche Recherche sowie Fantasie, um die Vorbereitung zu perfektionieren.[88]

Preloading, wörtlich übersetzt „vorab befüllen“, bezeichnet eine Methode, die noch nicht oft beschrieben wurde, aber zum Beispiel in Werbung oder Trailern von Filmen seit jeher benutzt wird. Dabei wird das Ziel mit den gewünschten Emotionen und Verlangen „befüllt“, indem ihm dies, trivial ausgedrückt, einfach gesagt wird. Dabei wird in Werbung genau gesagt, wie die Zuschauer sich fühlen sollen. Mit Worten wie „Der Beste Film des Sommers“ oder ähnlichen Phrasen, die diesem suggerieren, dass dies der beste, witzigste oder tollste Film ist, den man sehen könnte. Ein Social Engineer würde allerdings eher subtil Informationsbrocken fallen lassen, die sein Ziel bei bestimmten Fragen zu bereits vorher angedeuteten Assoziationen führen. Im Idealfall denkt das Ziel dabei, die Idee sei von ihm und springt deshalb darauf an und tut so eigentlich etwas, das der Engineer wollte. Dabei muss das Ziel aber auch zu einem gewissen Grad empfänglich für das Verlangte sein, etwas völlig Abwegiges kann durch diese Technik nicht erzeugt werden. Sie wird viel mehr dazu eingesetzt, eine Handlung oder ein Gespräch unterschwellig in eine gewünschte Richtung zu leiten.[89]

Baiting zu Deutsch „ködern“, ist ein Prinzip, bei der die Neugierde und Chancenlust der Menschen ausgenutzt wird. Dabei kann diese Methodik ebenso gerichtet wie auch ungerichtet eingesetzt werden. Wird beispielsweise ein USB-Stick mit Schadware liegengelassen ist es sehr wahrscheinlich, dass irgendjemand diesen an seinen PC anschließt, weil seine Neugierde, zu erfahren, was sich auf dem Stick befindet, groß ist und er dadurch kompromittiert wird.[90]

Es gibt eine Vielzahl an **psychologischen Tricks** die Social Engineers anwenden können, um an ihr Ziel zu gelangen. Die am häufigsten verwendeten werden hier vorgestellt.

> **Knappheit** ist den Meisten als sehr wirksames Mittel aus der Werbung bekannt. Es löst bei den Betroffenen das Gefühl aus, sie könnten einer von wenigen sein, dem dieses Angebot zu Teil wird. Dadurch werden oft Impulshandlungen getroffen, die bei näherer Betrachtung, nur auf diesem einen Faktor basieren.
>
> **Bedürfnisbefriedigung** ist ein Prinzip, bei dem scheinbar einfache Lösungen für Probleme geboten werden, die das Ziel sonst mehr Anstrengung kosten würden. Dadurch ist das Ziel bereits beeinflusst und gewillt, zum Beispiel eine Kaufhandlung zu tätigen oder seinem Gesprächspartner zu vertrauen.

---

[88] Christopher Hadnagy, Die Kunst des Human Hacking (Kapitel 4.1 – Seite 111 f.)

[89] Christopher Hadnagy, Die Kunst des Human Hacking (Kapitel 3.2.1 – Seite 89 f.)

[90] Norton_Team, Was ist Social Engineering? (Baiting (Ködern))

Wiedererkennung beziehungsweise **Wiederholung** ist eine besonders aus der Werbung bekannte Technik. Wie bereits im vorangegangenen Unterkapitel 3.2 erwähnt wurde, ist diese Technik allein durch die Verschiebung des Wiederholten ins Positive, die sie nach sich zieht, extrem wirkungsvoll.[91] Durch Wiederholung sind Menschen eher gewillt, eine Sache zu glauben und ihr zu vertrauen.

Spiegelung ist ein Prinzip, bei dem sich der Social Engineer ähnlich verhält wie sein Gegenüber. Tut er dies subtil und abgewandelt genug, hat dies zur Folge, dass eine Art Vertrauensbasis aufgrund der scheinbaren Ähnlichkeit zwischen Ausführendem und seinem Ziel entsteht. Bei einer exakten Spiegelung kommt es oft zum gegenteiligen Effekt, da diese in den meisten Fällen sofort auffällt. Spiegelung ist neben Empathie eine der Methoden, mit der direkt und schnell Rapport aufgebaut werden kann. Spiegelung wird meistens von Angesicht zu Angesicht benutzt, lässt sich aber auch am Telefon oder per Chat ausüben. Durch beispielsweise Übernahme leicht abgeänderter Formen von Redensarten oder Zustimmung. Dabei muss das Ziel nur glauben, der Social Engineer habe die gleichen Intentionen wie es selbst.

Suggestion ist in vielen Situationen ein mächtiges Werkzeug. Dabei unterstellt der Social Engineer seinem Ziel einen Gedanken, den dieses oft ohne zu Fragen annimmt. Suggeriert man zum Beispiel einem Sicherheitsmann durch Tragen von Klemmbrett und Mütze sowie Shirt mit dem Aufdruck der im Unternehmen tätigen Entsorgungsfirma, man gehöre zu dieser Firma, wird der Sicherheitsmann in vielen Fällen diese Suggestion nicht hinterfragen und sich so verhalten, wie er es normalerweise mit Mitarbeitern dieser Firma macht. Beispielsweise den Zugang zum Innenhof ermöglichen.

Reziprozität bedeutet Gegenseitigkeit oder Wechselwirkung. Dabei beschreibt es den Drang, der Menschen dazu bewegt, Andere gut zu behandeln, wenn diese zuvor von dieser Person auch gut behandelt wurden.[92] Durch Reziprozität kann das Ziel dazu bewegt werden, **Commitment**, also eine Art Verpflichtungsgefühl gegenüber dem Angreifer aufzubauen und würde ihm eher Gefallen tun oder seine eigenen Prinzipien für einen Moment ignorieren.

Das Ausnutzen von **Emotionen** ist einer der einfachsten Tricks, die ein Social Engineer anwenden kann. Je gefühlsbetonter ein Mensch ist, desto einfacher fällt es, dem Angreifer, seine Emotionen für seine Zwecke zu missbrauchen. Emotionen sind für die meisten menschlichen Handlungen der Motor. Sie können daher von Social Engineers gezielt dazu verwendet werden, bestimmte unüberlegte Handlungen her-

[91] Vergleiche Punkt 3.2, Unterpunkt „Werbebranche“

[92] Christopher Hadnagy, Die Kunst des Human Hacking (Kapitel 6.2.1 – Seite 240)

vorzurufen. Dabei kann absolut jede Emotion ausgenutzt werden, doch die besonders starken Emotionen scheinen am besten für kriminelle Zwecke missbraucht werden zu können. Die von bösartigen Social Engineers am häufigsten verwendeten Emotionen werden im Folgenden aufgeführt.

Angst ist eine der Emotionen, die bei den meisten Menschen funktioniert. Dabei muss der Social Engineer bei seinem Ziel nur genug persönlichen Bezug herstellen, sodass es Angst erfährt. Danach bietet der Angreifer seinem Ziel eine Lösung an, die dieses dankbar annimmt. Angst erzeugt in Menschen den Drang, aus der bedrohlichen Situation schnellstmöglich entkommen zu müssen. Dadurch sind die meisten Menschen, die Angst verspüren, gewillt den schnellstmöglichen Ausweg zu nehmen.

Glück wird gerne verwendet, indem dem Ziel ein Gewinn vorgespielt wird, um es auf Internetseiten mit Schadcode zu locken. Es kann aber genauso gut als Schmeichelei in einem Gespräch benutzt werden. Löst der Social Engineer diese Emotion aus, fühlt sich das Ziel als etwas Besonderes und ist gewillter, ihm Informationen zu geben, sowie nach seinen Wünschen oder Suggestionen zu handeln.

Mitgefühl wird oft ausgenutzt, da Menschen das Bedürfnis haben, anderen zu Helfen. Sobald die Menschen Mitgefühl zeigen, machen sie sich selbst verwundbar und werden oft unachtsam. Menschen stellen sich normalerweise nicht vor, dass jemand so skrupellos sein kann, dieses Mitgefühl auszunutzen, um sich zu bereichern.

Dieser Abschnitt sollte nicht ungezielte Paranoia wecken oder den Eindruck, dass hinter jeder Kommunikation Manipulation steckt. Tatsächlich ist es so, dass die meiste Kommunikation von Elementen des Social Engineering durchzogen ist. Man kann eine Person aber erst einen bösartigen Social Engineer nennen, wenn sie sich der Prinzipien bewusst ist und diese Fähigkeiten gezielt zum eigenen Vorteil einsetzt. Die meisten Menschen verhalten sich nach einem oder mehreren dieser Prinzipien, weil sie gemerkt haben, dass sie dadurch bei anderen besser ankommen oder leichter ans Ziel gelangen. Warum dies funktioniert, ist ihnen dabei oft nicht bewusst und selbst der Methode, die sie verwenden, sind sich die meisten nicht bewusst. Daher sollte ein vernünftiger Mensch dies zwar als eine Art der Manipulation sehen, doch mit dem Wissen darum kann er relativ, objektive und fundierte Entscheidungen treffen, trotz des Verhaltens des Gegenübers und ohne Angst vor bösartiger Manipulation. Social-Engineering-Prinzipien sind eigentlich grundsätzliche Mechanismen der Kommunikation, deren Wirkung bei genauerer Betrachtung den meisten Menschen bewusst ist, die diese aber nicht weiter beachten. Der Social Engineer hat diese analysiert und verwendet sie wie einen Baukasten, gezielt ihrer Wirkung und seines Ziels wegen.

3.4 Beispiele für Angriffsvektoren und Schadwarearten

Oft werden einige der Methoden, die im Unterkapitel 3.3 erwähnt wurden, bereits als Angriffe genannt. Dies ist allerdings nicht korrekt, da es fundamentale Prinzipien sind, aus denen sich mit etwas Fantasie beliebig viele Angriffe gestalten lassen. Angriffsarten beziehungsweise Schadware sind ein Konzept, welches oft mit der Zeit verändert wird und sich den unterliegenden Prinzipien und Methoden bedient. Die Grenzen scheinen nur zu verschwimmen, weil ein Cyber-Angriff aus mehreren kleineren Angriffsmethoden bestehen kann, so wie die Angriffsmethoden aus mehreren Prinzipien bestehen können. Laut der Definition von Cyber-Angriffen in Unterkapitel 2.1.2 kann auch eine der hier und im Unterkapitel 2.4 aufgeführten Methoden bereits für sich ein Cyber-Angriff sein.
In diesem Kapitel werden Beispiele für Angriffsvektoren und Schadwarearten, die aus den Prinzipien des Social Engineering entstanden sind, gegeben. All diese Angriffe können am effektivsten mit dem geschärften Menschenverstand verhindert werden, dem Sicherheitsbewusstsein. Sicherheitsbewusstsein wird Thema des Kapitel 4 sein.

Phishing, wörtlich „fischen“, ist eine Methode, bei der der Angreifer Spam-E-Mails mit Inhalten verschickt, die das Opfer locken oder ihm Angst machen und es dadurch zu unbedachten Handlungen verleiten oder Websites erstellt, die dasselbe Ziel haben. Wie zum Beispiel einen Artikel zu kaufen, der wirkungslos ist oder nie geliefert wird oder ein Programm herunterzuladen und zu installieren, welches in Wirklichkeit ein Trojaner ist. **Spear Phishing** ist eine gerichtete Version des Phishings, bei dem der Angreifer Methoden des Phishing für ein Opfer personalisiert, wodurch er eine deutlich höhere Erfolgsquote erzielt. Beim Phishing werden die Emotionen des Opfers ausgenutzt sowie Baiting betrieben.
Gegenmaßnahmen:

- E-Mail-Filter aller Art.
- Ad- und Scriptblocker.

Bei der **„Quid pro quo“-Attacke** bietet der Angreifer dem Opfer seine Hilfe oder einen anderen geringen Gegenwert, wie zum Beispiel eine Tafel Schokolade, an.[93] Danach verlangt der Angreifer etwas von seinem Opfer. Eine Studie zeigte, dass die Hälfte aller Teilnehmer den Forschern ihr Passwort verraten hat, nur weil sie vorher eine vergleichsweise wertlose Tafel Schokolade bekommen haben.[94] Wörtlich übersetzt bedeutet „quid pro quo“ „dies für das“. Bei diesem Angriff wird die Reziprozität ausgenutzt.

Tailgating, zu Deutsch oft auch „Huckepackangriff“, ist eine Technik, bei der der Angreifer einem Mitarbeiter mit Zutrittsberechtigung folgt und so Zutritt zu gesicherten Bereichen bekommt. Ein häufig verwendetes Szenario sieht zum Beispiel vor, dass der Angreifer sich

[93] Tripwire, 5 Social Engineering Attacks to Watch Out For (Abschnitt: QUID PRO QUO)

[94] Heise Technology Review, Passwort gegen Schokolade

als Paketbote ausgibt und einem Mitarbeiter folgt oder diesen sogar bittet, ihm die Tür aufzuhalten. Bei dieser Angriffsart wird die Kraft der Suggestion ausgenutzt. Sieht jemand so überzeugt davon aus, Zutritt zu einem bestimmten Bereich zu haben, hinterfragen die meisten Menschen dies nicht mehr weiter.[95] Der Angreifer geht sozusagen in der Masse unter.
Gegenmaßnahmen:

- Allgemeingültige Kontrollen und Zugangsbeschränkungen durch Schlüsselkarten oder ähnliches, die jede Person einzeln durchlaufen muss.
- Mehrfaktorautorisierung.

Ransomware ist eine Art Erpressersoftware, also eine Software, die den Menschen Angst machen soll und sie damit zu einer Zahlung an den Angreifer zu bewegen, um sich wieder freizukaufen. Sie geht dabei so vor, dass sie den PC sperrt und ihn dadurch für den Benutzer unbrauchbar macht. Die neueren Varianten der Ransomware verschlüsseln zusätzlich die Daten der Benutzer und wollen diese so zur Zahlung zwingen. Eine der bekanntesten Ransomwares ist der BKA-Trojaner. Eine Ransomeware, die dem Nutzer vorspielt, man habe illegale Inhalte auf seinem Computer gefunden und er müsse Geld als Strafe bezahlen, um seinen Computer wieder freischalten zu lassen. Diese Ransomware kombinierte sogar gleich mehrere Elemente, die sie für Menschen sehr überzeugend machte. Einerseits die Angst, vor weiterer Strafe sowie des dauerhaften Defektes des PCs, andererseits nutzte sie aber auch die Angst vor einer Autorität indem sie behauptete, vom BKA zu kommen und mit den entsprechenden Logos ausgestattet war. Darüber hinaus war diese Ransomeware sehr raffiniert, da die meisten Menschen in irgendeiner Form illegale Inhalte auf dem PC haben, und sei es nur ein einziger raubkopierter Film.
Gegenmaßnahmen:

- Aktuellste Betriebssystemversion mit allen verfügbaren Updates nutzen.
- Anti-Viren-Software nutzen.
- Sicherheitskopien aller wichtigen Arbeitsdaten auf einem externen Server oder einer Festplatte, die nur beim Sichern an den PC angeschlossen wird.
- Bei Bemerken der Ransomware den Rechner sofort ausschalten und die Software entfernen lassen. Alle bis dahin unverschlüsselten Daten können gerettet werden. Für die übrigen Daten erstellen Sicherheitsexperten häufig nach einer gewissen Zeit eine Software zum Entschlüsseln.

[95] Christopher Hadnagy, Die Kunst des Human Hacking (Kapitel 6.4.5 – Seite 312)

3.5 Vergleich von Auditor und Black-Hat

Wie in Unterkapitel 2.3.1 bereits angesprochen, können Auditoren nicht alle Sicherheitslücken überprüfen, über die bösartige Hacker möglicherweise in ein Unternehmen eindringen könnten.

Ein Auditor ist an moralische und gesetzliche Vorgaben gebunden. Der Kontrakt, den er mit seinem Auftraggeber abschließt, kann ihn nur innerhalb des Unternehmens von gesetzlichen Vorgaben entbinden. Christopher Hadnagy hat eine kleine Zusammenstellung von Aktionen, die ein Auditor auf jeden Fall nicht tun sollte, gemacht:

„

- *Der Angriff auf Familie und Freunde der Zielperson.*
- *Beweise für kriminelle Machenschaften oder Untreue unterschieben, um die Zielperson zu diskreditieren.*
- *Abhängig von den Gesetzen des Landes kann es illegal sein, sich als Strafverfolger oder Polizist auszugeben.*
- *In das Haus oder die Wohnung der Zielperson einzubrechen.*
- *Mit Beweisen einer echten Affäre oder peinlicher Umstände die Zielperson durch Erpressung gefügig machen.*

„[96]

Ein Auditor muss seine moralischen Grenzen selbst setzen. Da sein Auftrag, die Verbesserung der Situation bewirken soll, sollte er sich diese Grenzen vorher gut definieren. Der Nachteil ist offensichtlich: Ein Auditor kann niemals alle Lücken testen, da er in seinem Handeln eingeschränkt ist. Dadurch bleibt ein Angriff durch einen oder mehrere Black-Hats immer gefährlicher. Dabei ist aber nicht davon auszugehen, dass jeder Black-Hat Social Engineering gut genug beherrscht, um durch einen Auditor ausgebildete Mitarbeiter auszutricksen. Ebenso ist es unwahrscheinlicher, dass ein einzelner Black-Hat sich in Person zeigt, um Social Engineering Angriffe durchzuführen. Er wird seine Angriffe vermutlich auf Telefon und E-Mail beschränken.
Dies soll aber keineswegs bedeuten, dass die Aufmerksamkeit auf Personen sinken darf, die das Unternehmensgelände betreten.

Ein Auditor kann das direkte Verhalten der Angestellten vor Ort sehr gründlich überprüfen. Da die meisten Angriffe Social Engineering nutzen um eine Erstinfektion auszuführen, ist es vermutlich die beste Verteidigungsmöglichkeit, die sich Unternehmen bietet, regelmäßige Audits durchzuführen und so die Wachsamkeit der Mitarbeiter zu schulen.

---

[96] Christopher Hadnagy, Die Kunst des Human Hacking (Kapitel 9.6.3 – Seite 434)

3.6 Moralische Sicht

Die in Unterkapitel 3.2 und in diesem Abschnitt genannten Berufe sind nur Beispiele für Social Engineering in der Gesellschaft. Mit dem Wissen aus dieser Arbeit kann jeder selbst entscheiden, was Social Engineering bedeutet und wird viele weitere Berufsfelder entdecken, in denen es zum „Guten“ oder zum „Schlechten“ angewendet wird. Da es am anschaulichsten und am verständlichsten ist, die verschiedenen Arten von Social Engineering einzuordnen und zu verstehen, werden diese an kleineren Beispielen diskutiert.

Social Engineering ist ein zweischneidiges Schwert und das Wissen darum, lässt die Welt anders erscheinen. Bei allen Geschäften, die abgeschlossen werden, hat es Einfluss und jeder Mensch wird ständig mit mehr Social Engineering konfrontiert als ihm bewusst ist. Sobald etwas verkauft werden soll spielt Social Engineering generell eine große Rolle.

Werbung und Konsum ist in der heutigen Welt allgegenwärtig und mittlerweile so gut wie unvermeidlich. Daher verdient dieser Bereich eine genauere Betrachtung, endgültig über das Thema entscheiden, muss jeder Mensch allerdings für sich selbst. Werbung versucht mit allen Mitteln, jemandem zum Kauf zu bewegen. Kaufhäuser spielen Musik, die die Kunden dazu bringt, mehr Zeit im Laden zu verbringen. Selbst der Aufbau der Gänge, Regale und der Standort einzelner Produkte sind so angelegt, dass der Kunde dazu gedrängt wird, mehr zu kaufen. Die Verpackung erscheint groß und der Inhalt ist gering. Dies sind alles Methoden, die das primitiv veranlagte Gehirn der Menschen auszutricksen. Nicht einmal die Laufrichtung ist in Supermärkten Zufall. In Amerika werden in Kaufhäusern sogar anregende Düfte versprühen, um die Verkaufszahlen zu steigern.[97] An dieser Stelle könnte man sich die Frage stellen wie man sich dabei fühlt, auf diese Weise manipuliert zu werden, um eine klarere Sicht auf Social Engineering zu erlangen.

Unter der ständigen Flut von Social Engineering treffen Menschen irrationale Entscheidungen und unser Gehirn ist so veranlagt, dass es diese nachträglich zu rechtfertigen versucht. Der freie Wille wird durch den Einsatz von Social Engineering ein Stück weit verbogen.

[97] Professor Ittner, Hochschule Mittweida – Modul: Datamining

Es gibt 3 verschiedene Arten wie Social Engineering vorkommt:

- Natürlich und unabsichtlich.
- Gewollt und gezielt.
- Ungewollt und gezielt.

Natürlich und unabsichtlich bedeutet zum Beispiel die Art Social Engineering, die Kinder benutzen oder ein Mensch, der einem anderen ehrlich helfen möchte und ihn zu überzeugen versucht. Natürliches Social Engineering kommt überall vor und jeder muss für sich selbst entscheiden, wie viel davon für ihn anzuwenden in Ordnung ist oder wie viel er davon von anderen ertragen will und kann. Dabei ist die Interaktion zwischen Menschen kompliziert, da niemand mit Sicherheit sagen kann, ob eine Aktion vom gegenüber beabsichtig war und wenn ja, welche Absicht dahintersteckt. Die einzige und einzig richtige Möglichkeit, mit dieser Art des Social Engineering verantwortungsbewusst umzugehen, ist dass Menschen mehr und ehrlicher miteinander reden. Dadurch werden Fehlschlüsse sowie Konflikte vermieden, hinterhältiges Verhalten ausgebremst, Unsicherheit reduziert und das Gefühl, manipuliert worden zu sein auf ein Minimum gesenkt.

Gewollt und gezielt meint die Art von Social Engineering, die Ärzte, Pädagogen und Therapeuten verwenden. Gewolltes und gezieltes Social Engineering ist für unsere heutige Gesellschaft zwingend notwendig. Menschen, die Hilfe brauchen müssen diese von Therapeuten oder Ärzten bekommen. Dabei reicht es nicht aus, dass diese den Personen einfach sagen, was sie verbessern sollen. Diese Einsicht erreichen die meisten bereits ohne eine Therapie. Wichtig ist, dass diesen Menschen mitgeteilt werden kann, auf welche Weise sie sich selbst zum Positiven ändern können. Sich selbst sozusagen zu manipulieren, um wieder mit sich zufrieden sein zu können. Pädagogen und andere Ärzte hingegen haben eine Art Schutzauftrag. Pädagogen und ähnliche Berufe müssen Kindern Werte vermitteln und ihnen zur Seite stehen, gleichzeitig müssen sie aber Schranken aufweisen und den Kindern diese Werte, die sie noch nicht verstehen können, beibringen. Ohne eine gewisse Art des Social Engineering wären diese Dinge nicht möglich.

Ungewollt und gezielt meint die Art Social Engineering, die angewendet wird, um sich selbst zu bereichern. Black-Hats und Trickbetrüger sind hier eine besonders bösartige Gruppe. Diese Art des Social Engineering ist generell moralisch verwerflich, davon abgesehen, dass Diebstahl illegal ist. Aber nicht nur Betrüger verwenden Social Engineering zu ihrem persönlichen Vorteil und richten so Schaden an. Jeder kennt Menschen, die zumindest so wirken, als wenn sie bestimmte Dinge nur tun, um sich einen Vorteil gegenüber anderen zu verschaffen. Diesen Menschen sollte ihr Handeln und die negativen Folgen, die daraus entstehen, aufgezeigt werden und sie müssen sich freiwillig dazu entscheiden, dieses Verhalten zu unterlassen.

Wo Werbung und aggressives Verkaufsverhalten einzuordnen sind, muss jeder selbst entscheiden.

Um eine negative Ausprägung von Social Engineering für sich einordnen zu können, sollte sich jeder folgende Fragen stellen:

- Hat dieses Verhalten nur einer bestimmten Person geholfen oder vielen beziehungsweise allen?
- War es, nachdem ich die Manipulation erkannt habe, für mich unangenehm?
- Hat mir oder anderen dieses Verhalten lang- oder kurzfristig geschadet?

Natürlich ist die Frage, ob der jeweilige Social Engineer bösartig ist oder nicht beziehungsweise er eine Grauzone darstellt, in erster Linie eine persönliche Frage und benötigt zum Beantworten mehr als nur drei Fragen. Jeder Mensch hat neben seinen ethnischen noch persönliche Moralvorstellungen, die diese Fragen sowie die Einordnung von Richtig und Falsch beeinflussen. Diese Fragen sind Beispiele und stellen eine Art Orientierungshilfe dar, wie ein Verhalten einzuordnen ist.

3.7 Potential von Social Engineering

Social Engineering hat für Kriminelle ein besonders großes Potential. Doch in diesem Abschnitt soll es darum gehen, welches positive Potential das Social Engineering für die Gesellschaft haben kann.

Da Social Engineering allgegenwärtig ist, ist es wichtig, dass jeder über dessen Grundzüge Bescheid weiß und so bewusster und freier Entscheidungen treffen kann. Nur durch Aufklärung kann dieses Bewusstsein für Social Engineering entstehen, dementsprechend ist diese Aufklärung auch die wirkungsvollste Verteidigungsstrategie.

In der **Erziehung** könnte das Wissen des Social Engineering Verbesserungen bewirken, denn es gehört auch dazu, abschätzen zu können, wie sich ein anderer Mensch fühlt, wenn er diese Manipulation erfährt. Durch gezieltes Social Engineering könnten Eltern mit ihrem Kind besser umgehen und eher subtile positive Einflüsse unternehmen, anstatt mit Bestrafungen und negativer Konditionierung zu arbeiten. Eine Studie der Universität Pittsburgh hat gezeigt, dass Bestrafung und harte Erziehung die Kinder in ihrer Persönlichkeitsentwicklung beeinflusst und diese deutlich schlechter in der Schule abschnitten und eher einen Hang zur Kriminalität hatten.[98] Negative Konditionierung kann also noch viele Jahre ungeahnte Auswirkungen haben und Arbeits- sowie Motivationseinstellungen langfristig negativ schädigen oder schlimmere Folgen nach sich ziehen.

[98] Jacquelynne Eccles: Maryland Adolescent Development In Context Study (MADICS) - Newsletter Spring 2007

In der **Schule** sollte Social Engineering daher in einer gewissen Form unterrichtet werden und hätte dort darüber hinaus noch das Potential, das Bewusstsein der Kinder für ihr Verhalten und dessen Folgen deutlich zu steigern. Mobbing und mittlerweile auch „Pranking“ sind Erscheinungen, die von Individuen ausgeführt werden, die Macht ausüben wollen, sich aber der langfristigen Folgen ihres Handelns nicht bewusst sind. Selbst wenn der Unterricht über das Thema des Social Engineering nicht alle Täter zum Umdenken verleiten kann, so birgt es immer noch das Potential, den Opfern Verteidigungsmöglichkeiten in die Hand zu geben und ihr Verständnis für die Täter zu steigern, sodass sie die Fehler nicht bei sich selbst suchen und ihre Psyche davon weniger beeinträchtigt wird.

Wie im Unterkapitel 3.2 besprochen, brauchen Menschen in verschiedensten Berufen Social Engineering, um anderen Menschen helfen zu können. In anderen Berufsfeldern oder Branchen wird es wiederum nur wegen seines Potenzials der Manipulation genutzt. Die Entscheidung darüber, wie es Zukünftig verwendet werden soll, kann nur von aufgeklärten Menschen getroffen werden und erfordert die Schaffung eines moralischen sowie sicherheitstechnischen Bewusstseins, auf Basis von und mit Social Engineering.

Das letztlich größte Potential von Social Engineering, für jede einzelne Person, bleibt mit Sicherheit der Selbstschutz in Bezug auf die freie Entscheidungskraft. Da dem Social Engineering in unserem Informationszeitalter nicht mehr entgangen werden kann, ist es für den freien Willen und den freien Menschen unbedingt notwendig, Kenntnisse über diese Thematik zu erlangen.

Menschliches Verhalten und damit auch menschliches Fehlverhalten zu analysieren ist ein wichtiger Bestandteil einer modernen und verantwortungsvollen Gesellschaft. Social Engineering ist davon nur ein Teil, aber es ist der Teil, der sich mit der Manipulation dieses Verhaltens beschäftigt. Daher ist es besonders Wichtig für gegenseitiges Verständnis und eigenmotiviertes Handeln, welches über passive Beeinflussbarkeit hinausgehen soll.

4 Sicherheitsbewusstsein

In diesem Kapitel geht es um das Sicherheitsbewusstsein, welches benötigt wird, um sich effektiv vor Cyber-Angriffen aller Art zu schützen. In den vorangegangenen Kapiteln wurden hauptsächlich breite Grundinformationen gegeben, die notwendig sind, um auf ihnen das Sicherheitsbewusstsein aufzubauen. Dabei wird zunächst geklärt, was das Sicherheitsbewusstsein ist und wie es erreicht werden kann. Danach werden Methoden gezeigt, die jeder anwenden kann, um sich zu schützen. Das Sicherheitsbewusstsein ist kein definierter Begriff, es wird eher selbstbeschreibend verwendet. Dieses Kapitel beruht auf Überlegungen, die nach der Lektüre des Buchs „Die Kunst des Human Hacking“ von Christopher Hadnagy und aus dem IT-Sicherheitsstudium an der Hochschule Mittweida entstanden sind.

4.1 Bedeutung

Sicherheitsbewusstsein bedeutet, sich der Angriffsvektoren, Datenwerte und digitalen sowie menschlichen Schwächen bewusst zu sein und diese verinnerlicht zu haben. Durch dieses Bewusstsein kann ein größeres Pensum an Sicherheit gewährleistet werden. Durch das Verinnerlichen dieser Dinge erinnert das Unterbewusstsein zu jeder Zeit an die Gefahr, sobald eine Querverbindung mit einer Handlung geschlossen wird. Es ist ein einfacher Mechanismus unseres Gehirns, der auch dafür sorgt, dass bei einer roten Ampel gebremst wird oder daran erinnert, dass Feuer heiß ist und man sich daran verbrennen kann. Die Folge ist, dass die meisten Menschen mit Feuer vorsichtig und bewusst umgehen und an einer roten Ampel stoppen. Genau so muss das Sicherheitsbewusstsein für die Abwehr von Cyber-Angriffen geschaffen werden. Das Sicherheitsbewusstsein ist sozusagen eine Erweiterung für den gesunden Menschenverstand, der warnt und das richtige Verhalten impliziert.

Hadnagy redet von einer „Kultur des Sicherheitsbewusstseins“. Dieser Aspekt ist besonders für Unternehmen wichtig, da die Haltung, sich selbst und seine Daten zu schützen, eine andere ist, als die Daten anderer Personen zu schützen. Eine Kultur des Sicherheitsbewusstseins meint also ein global gesehen sicheres Denken, das über den Selbstschutz hinausgeht und auch die Daten des Arbeitgebers oder Dritter schützen kann.[99]

Im nächsten Abschnitt wird gezeigt, wie ein Sicherheitsbewusstsein erreicht werden kann.

[99] Christopher Hadnagy, Die Kunst des Human Hacking (Kapitel 9.2 – Seite 424)

4.2 Aufbau

Wie im Unterkapitel 4.1 bereits erwähnt wurde, bedeutet Sicherheitsbewusstsein sich der Angriffsvektoren, Datenwerte und digitalen sowie menschlichen Schwächen bewusst zu sein und diese verinnerlicht zu haben.

Ein **Angriffsvektor** bezeichnet einen Angriffsweg. Die Angriffsvektoren wurden in den vorangegangenen Kapiteln 2 und 3 besprochen und ihre Methodiken erläutert. Eine Auflistung häufiger Angriffsvektoren beziehungsweise Prinzipien des Social Engineering befindet sich im Unterkapitel 3.3. Die Angriffsvektoren für klassische Cybercrime in befinden sich im Unterkapitel 2.4. Diese Kapitel sollten verinnerlicht werden.

Ein Bewusstsein für den **Datenwert** kann durch einige Beispiele präzisiert werden. In Kapitel 5 werden Beispiele folgen, in denen unter anderem gezeigt, wird wie wertvoll scheinbar unwichtige Daten sein können. Um Datenwerte richtig einschätzen zu können, sollte sich Gedanken darüber gemacht werden welche, Daten ein Angreifer benötigt, um zum Beispiel die genannten Angriffsvektoren auszuführen. Daher wurde in den vorangegangenen Kapiteln gezeigt, wie ein Angreifer seinen Angriff planen kann und welche Möglichkeiten ihm dabei zur Verfügung stehen.

Digitale Schwächen sind jene Schwächen, an der die Technik limitiert ist oder nicht voll ausgenutzt wird oder werden kann. Beispielsweise reicht es nicht, ein 7 oder 8-stelliges Passwort für wichtige Informationen zu nutzen. Einerseits könnte man sagen, das schnelle Knacken des Passwortes mittels Brute-Force sei eine Stärke des Computers, es ist aber eher eine Stärke seiner Rechenleistung. Es ist demnach eine Schwäche des Systems, weil es nicht ausreicht, ein kurzes Passwort zu verwenden. Ein anderes Beispiel ist das Verwenden der beliebtesten Software ohne die aktuellsten Updates. Bösartige Hacker suchen vorwiegend in der beliebtesten Software nach Schwachstellen, um eine möglichst große Erfolgsrate bei Infektionsversuchen zu erreichen. Des Weiteren sollte jede Software immer aktuell gehalten werden und grade Sicherheitsrelevante Patches sollten so schnell wie möglich eingespielt werden. Dieser Zusammenhang sollte beispielsweise bekannt sein und der Umgang mit dieser Software entsprechend angepasst werden. Weitere Hinweise zum Passwort und dem Abdichten digitaler Schwächen werden in folgenden Unterkapitel 4.3 gegeben.

Menschliche Schwächen wurden in Kapitel 3 eingehend besprochen. Wichtig ist hierbei, sich selbst zu kennen und besonders die eigenen Schwächen und Neigungen herauszufinden. Neigt ein Mensch eher dazu, Fremden zu misstrauen und baut nur schwer Rapport auf, ist aber naiv, wenn es um Produktwerbung oder seine Hobbys geht, sollte er sich zunächst besonders darauf konzentrieren. Das bedeutet nicht, den Rest zu vernachlässigen. Da aber nicht alles auf einmal erlernt und angewendet werden kann, ist es besonders wichtig, zuerst die größten Sicherheitslöcher zu stopfen. Der Angriff eines Social Engineers beruht auf Informationen und die Wahrscheinlichkeit, dass er diese Neigungen herausfindet

und bei einem solchen Menschen gezielt über Spam und Hobbys angreifen würde, ist sehr groß.

Laut dem IoD haben 49 % der befragten Führungskräfte Training gegen Cyber-Angriffe mit ihren Angestellten durchgeführt.[100] Leider besteht dieses Training meist aus Schulungsvideos und unreflektiertem vorlegen von Fakten. Für die Angestellten ist es dadurch meist eine Last. Dazu kommt, dass diese Firmen häufig nur wenige Stunden jährlich dazu aufwenden, um ihre Angestellten zu schulen.[101] Dadurch verinnerlichen die Angestellten das Gesagte kaum bis gar nicht und nehmen eher gelangweilt und abgelenkt an diesem Pflichtprogramm teil. Dieser Ansatz ist nicht zielführend. Sicherheitstraining muss anschaulich, multimedial und interessant sein. Hadnagy setzt bei seinen Trainings unter anderem auf Überraschung und Angst, damit die Personen sich so gut wie möglich erinnern. Ihm ist bewusst, dass Angst ein gewisses Risiko zur Paranoia beinhaltet, er nimmt dieses jedoch in Kauf, um einen möglichst großen Lerneffekt zu erzielen. In seinem Vorgehen lässt er beispielsweise einen Mitarbeiter ein Passwort in den Rechner eintippen, welches er für sicher hält und lässt dann einen Passwortcracker live mitlaufen, sodass jeder sehen kann, wie der Computer arbeitet. Meist ist das Passwort nach wenigen Minuten geknackt und die Überraschung und Angst um die eigene Sicherheit macht sich breit. Danach lauschen alle Mitarbeiter gespannt und verinnerlichen das Gesagte, um sich aufgrund ihrer Angst besser schützen zu können.[102]

An sich sollte Sicherheitsbewusstsein, genau wie Cyber-Angriffe und Grundzüge des Social Engineering als Pflichtfach bereits in der Schule unterrichtet werden. Unser Zeitalter wird das „Informationszeitalter“ oder „Digitales Zeitalter“ genannt, doch trotzdem gehört Internetsicherheit nicht zum allgemeinen Lehrplan. Kinder bekommen ihre ersten Smartphones bereits in der Grundschule und gehen mit dem Internet wie selbstverständlich um. Die Gefahren werden ihnen aber nicht aufgezeigt. Dieses Verhalten kann eigentlich nur als nachsowie fahrlässig bezeichnet werden und liegt vermutlich vorwiegend am trägen Schulsystem, das Jahrzehnte lang nahezu dieselben Lehrpläne verwendet. So gesehen ist es eigentlich nicht verwunderlich, dass sich Cybercrime für die Täter so sehr lohnt. Sie können anonym und global agieren und treffen dabei häufig auf ungeschulte Opfer. Dadurch haben sie ein leichtes Spiel und stecken deshalb mehr Zeit in die Entwicklung neuer Angriffsmethoden. Würden mehr Menschen eine Grundausbildung in Internetsicherheit erhalten, ließe sich dieser Kriminalitätsbereich sicherlich ausbremsen. In einer britischen Studie fand man bereits 2011 heraus, dass sich 53 % der Befragten verärgert und 40 % sich einsam fühlen

[100] IoD, Cyber Security: Underpinning the digital economy (The Institute of Directors Cyber Survey 2016 – key findings – Seiten 7)

[101] Christopher Hadnagy, Die Kunst des Human Hacking (Kapitel 9.1 – Seite 424)

[102] Christopher Hadnagy, Die Kunst des Human Hacking (Kapitel 9.1 – Seite 424 f.)

würden, wenn ihnen der Zugang zum Internet untersagt würde.[103] Diese Zahlen dürften seitdem deutlich gestiegen sein. Angesichts dieser Tatsachen ist es an der Zeit, Internetsicherheit, mit den Teilbereichen Cybercrime, Social Engineering und der Bedeutung des Sicherheitsbewusstseins, unabhängig vom Bundesland in die allgemeinen Lehrpläne aufzunehmen.

4.3 Methoden zum Schutz vor Hacking

Zu allererst darf sich niemand der Illusion der absoluten Sicherheit hingeben. Auch wenn ein Virenschutzhersteller verspricht, alle Viren zu finden oder jemand keine sozialen Kontakte pflegt und kein Facebook nutzt, absolute Sicherheit gibt es nicht, niemals und ausnahmslos. Die hier genannten Methoden sind Beispiele für den passiven Schutz. Sie anzuwenden ist Teil des Sicherheitsbewusstseins und für jeden ausnahmslos möglich, selbst ohne tiefere Kenntnisse und ohne das gezielte Antrainieren eines Sicherheitsbewusstseins.

Zuerst soll geklärt werden, wie der Computer mit einfachen Maßnahmen sicherer gemacht werden kann.

- Das Benutzen eines aktuellen Betriebssystems, welches noch mit sicherheitsrelevanten Updates versorgt wird, ist essentiell für den Schutz gegen Hacking.
- Es sollte ein aktuelles Antivirensystem vorhanden sein, welches mindestens zwei Mal am Tag ein Sicherheitsupdate durchführt, um die neusten Virendefinitionen zu erhalten.
- Es sollte immer die aktuellste Version des Browsers verwendet werden. Alle Updates sollten so zeitnah wie möglich eingespielt werden. Bekannte Sicherheitslücken werden oft gepatcht, es kann also vermieden werden durch alte Lücken gehackt zu werden. Für Firmen ist dies besonders schwer umzusetzen, da es manchmal Richtlinien für Programmversionen und Kompatibilitätsprobleme mit den neusten Softwareversionen gibt. Bei besonders kleinen Unternehmen muss der Admin Software oft per Hand einspielen, was Zeit kostet. Das Einspielen von Updates ist allerdings besonders wichtig, weshalb verstärkt darauf geachtet werden sollte.
- Wenn möglich, sollte nicht die beliebteste Software verwendet werden. Zum Beispiel verwenden die meisten Nutzer den Adobe PDF-Reader, nur um PDFs zu lesen. Das lesen von PDFs ist mit jedem No-Name PDF-Reader genauso gut möglich, vermutlich aber deutlich sicherer, da bei diesen Produkten nicht gezielt nach Lücken gesucht wird, dementsprechend ist die Hackingsoftware der Angreifer wahrscheinlich nicht auf diese unbekannte Software ausgelegt. Dadurch ließen sich manipulierte PDFs nicht nur nicht öffnen, sondern der Exploit dahinter würde ins Leere laufen.

[103] Intersperience, Intersperience research highlights people’s emotional dependency on technology

Dabei sollte darauf geachtet werden, dass trotzdem eine aktuell unterstützte Software verwendet wird, damit mögliche Sicherheitslücken trotzdem noch geschlossen werden können.

- Es sollte ein Adblocker im Browser verwendet werden, der unerwünschte Werbung filtert und vor ungewollten Weiterleitungen auf andere Websites schützt. Viele Werbeflächenanbieter achten nicht darauf, wer ihre Werbeflächen im Internet kauft. Zwielichtige Werbung, die Drive-by-Exploits nutzt, auf gefährliche Seiten weiterleitet oder diese als Popup öffnet, findet sich überall im Internet. [104] Der Adblocker verhindert, dass die Werbung geladen wird und stoppt damit penetrante Werbekaskaden. Darüber hinaus verbessert ein Adblocker das Onlineerlebnis ungemein, da der Internet-Traffic reduziert wird und sich dadurch das Laden der Websites beschleunigt.
- Der Flashplayer sollte standardmäßig deaktiviert werden und nur für Websites freigegeben werde, die seriös genug erscheinen und diesen für funktionskritische Inhalte benötigen.
- Es sollte ein Scriptblocker verwendet werden. Die meisten Exploits im Browser gelangen durch den Flashplayer und Javascript auf die Computer der Anwender. Ein Scriptblocker kann diese Infektionswege effektiv einschränken. Scriptblocker sind anfangs etwas umständlich. Sie verlangen vom Nutzer, selbstständig auf jeder Seite, auf der Javascript für wichtigen Funktionsumfang verwendet wird, dieses Funktion freizugeben beziehungsweise zu „erlauben“. Doch nach ein paar Tagen bis Wochen sind alle Seiten, die normalerweise besucht werden, korrekt eingestellt. Die Einstellungen können später exportiert werden und auf andere Computer übertragen werden. Doch der Aufwand lohnt sich. Er verhindert erfolgreich die meisten Drive-by-Exploits, da alle Internetseiten, die unbekannt sind, kein Javascript ausführen dürfen. Darüber hinaus blockt der Scriptblocker ebenfalls alle Werbung, die über Javascript eingeblendet wird. Ein Scriptblocker ist vermutlich, neben einer Firewall, das effektivste Werkzeug, um eine Infektion durch den Browser zu verhindern.
- Es sollte eine gute Firewall installiert sein, die mindestens unautorisierten Traffic blockiert. Dabei greift diese auf ein festes Regelwerk zurück und erlaubt oder blockiert so den Zugriff von bestimmten Kommunikationspartnern im Netz untereinander, sowie nach außen.
- Es sollten lange und kryptische Passwörter verwendet werden. Ein sicheres Passwort sollte aus mindestens 10 Zeichen bestehen und sowohl Groß- als auch Kleinbuchstaben und Sonderzeichen beinhalten. Dabei sollte darauf geachtet werden, dass das Passwort keine Wörter benutzt, die in irgendeiner Form in einem normalen Wörterbuch vorkommen. Genauso darf es keine Namen oder Anspielungen enthalten. Das Passwort sollte darüber hinaus frei von jeglichen persönlichen Informationen sein. Für maximale Sicherheit sollten mehrere Passwörter verwendet werden. Alle wichtigen Accounts sollten durch verschiedene Passwörter gesichert sein. Die

[104] BSI, Schädliche Werbebanner in großem Umfang zur Verbreitung von Schadprogrammen mittels Drive-by-Exploits genutzt

beste Sicherheit wird mit einem Passwortsafe erreicht, in dem jedes Passwort zufällig generiert wird. Dadurch weiß der Nutzer nicht, wie sein Passwort lautet und läuft auch nicht Gefahr, dieses aus Versehen zu verraten. Zusätzlich kann so auf jedem Account ein anderes Passwort benutzt werden. Für den Zugriff auf den Safe wird ein Masterpasswort benötigt. Der offensichtliche Nachteil ist, sollte der Angreifer sich des Safes bemächtigt haben und Masterpasswort gehackt werden, so liegen alle Passwörter offen. Dieses Problem kann durch das Verwenden von Schlüsseldateien und Passwort in Kombination verhindert werden. Dabei kann eine Schlüsseldatei eine Beliebige Datei sein, beispielsweise ein Foto oder ein Dokument. Dieses wird mit dem Masterpasswort angegeben um den Passwortsafe zu öffnen. Das Masterpasswort eines solchen Safes sollte aus etwa 21 Zeichen mit Groß- und Kleinbuchstaben sowie Sonderzeichen bestehen. Passwörter sollten niemals in der Nähe des Computers aufgeschrieben werden (beispielsweise unter der Tastatur oder Ähnlichem). Eine relativ gute Sicherheit kann auch durch extrem lange Passwörter erreicht werden in denen nur Zahlen und Buchstaben vorkommen. Dabei können normale oder leicht veränderte Wörter im Passwort vorkommen, diese dürfen allerdings keinen Bezug zueinander haben. (Beispiel: 5liegenArmeisenkorrektur8acht)

- Öffentliche Netze sollten gemieden werden oder es sollte zumindest kein wichtiger Datenverkehr über sie laufen, wie zum Beispiel Onlinebanking oder Ähnliches. Angreifer haben über das LAN ein deutlich leichteres Spiel und können einfacher Angriffe ausführen. Die Auswirkungen eines Hacks über ein solches Netz würden vermutlich erst Wochen später in Erscheinung treten, wenn der Angreifer seine Strategie festgelegt hat und mit einem Klick das Bankkonto und alle Konten, die er finden konnte, leerräumt. Sollten öffentliche Netzwerke dennoch genutzt werden müssen, empfiehlt es sich eine VPN einzurichten, die den ausgehenden Traffic verschlüsselt und so für Angreifer im selben LAN unbrauchbar macht.
- Der Domain-Name von Links, insbesondere aus unbekannten E-Mails oder ein Link, der von einer Website zu einer unbekannten Website führt, sollten überprüft werden. Eine bösartige Phishing-Website kann, sofern die echte Website nicht gehackt wurde oder der PC bereits mit einer Schadware infiziert ist, welche die Seite umleitet, nicht den originalen Domain-Namen besitzen. Dabei ist der Teil direkt vor dem „.de“, „.com“ oder Ähnlichem wichtig. Zum Beispiel ist www.amazon.de eine bekannte Originaldomain. www.amazom.de ist mit nahezu absoluter Sicherheit eine Phishing-Website, die gemieden werden sollte. Kleine Rechtschreibfehler oder doppelte Buchstaben sind hier das Mittel, mit dem die Kriminellen arbeiten. Phishing-Websites besitzen genau dasselbe Aussehen wie die Originalseite und werden den Nutzer nach getaner Arbeit sogar wieder auf die Originalseite umleiten. Daher ist oft der einzige Weg, diese zu erkennen, den Domain-Namen in der URL zu überprüfen.

Es folgen nun die Möglichkeiten, sich vor Social Engineering besser zu schützen.

- Es sollten so wenig persönliche Informationen wie möglich online gestellt werden. Alle Informationen, die frei zugänglich sind, können von bösartigen Social Engineers gegen den Nutzer verwendet werden.
- Die Privatsphäre-Einstellungen der Social-Media-Kanäle sollte ernstgenommen und benutzt werden. Es sollte besonders darauf geachtet werden, dass „nicht-Freunde“ nicht alle Daten einsehen können.
- Passwörter sollten aus Prinzip niemals verraten werden, weder am Telefon, noch per E-Mail oder persönlich. Eine seriöse Firma würde nie nach Passwörtern fragen. Firmen haben dafür andere Methoden. Sollte ein Passwort tatsächlich einmal geteilt werden müssen, sollte sich gemeinsam auf ein Neues Passwort geeinigt werden und das alte Passwort geheim bleiben.
- Es sollte sich regelmäßig mit dem Thema Social Engineering auseinandergesetzt werden. Die regelmäßige Beschäftigung mit dem Thema schafft automatisch eine Art Sicherheitsbewusstsein. Dadurch können Angriffe leichter erkannt werden.
- Für wiederholte Handlungen und Serviceleistungen sollten Handlungsabläufe definiert werden. Damit ist gemeint, zu bestimmten wiederkehrenden Situationen ein Skript definiert zu haben, welches überprüft und abgehandelt wird. Zum Beispiel sollten bei einem dem Mitarbeiter unbekannten Gesprächspartner zuerst einmal alle dem Mitarbeiter bekannten Informationen vom Gesprächspartner abgefragt werden. Er sollte den Anrufer zum Beispiel nach seiner eigenen Mitarbeiternummer fragen, nach dem Projekt oder Paket, über welches er Daten haben möchte und wenn nötig nach dem Vorgesetzten des Anrufers, oder der Person, die ihn autorisiert hat.[105] Sind solche einfachen Handlungsabläufe in Form von Skripten bereits vordefiniert und jedem Mitarbeiter vorliegend, kann das Manipulationsniveau auf ein Minimum gesenkt werden. Der Angreifer benötigt somit deutlich mehr Informationen, an die er möglicherweise nicht kommen kann, oder die zumindest überprüfbar sind.

Die hier genannten Programme und Methoden sowie Anleitungen zum Einrichten der Programme sind zahlreich im Internet über Suchmaschinen wie Google zu finden. All diese Programme sind kostenlos verfügbar und somit von jedem nutzbar.

Leicht zu erkennen ist, dass die Liste der hier genannten „Patenttricks“ sich vor Social Engineering zu schützen unverhältnismäßig kleiner ist als die, sich vor klassischen Hacks zu schützen. Wohingegen viele Dinge zum Verhindern der klassischen Methoden nur aus Bequemlichkeit nicht getan werden, ist Social Engineering nur mit aufmerksamem und klarem Menschenverstand zu erkennen. Dabei muss das Sicherheitsbewusstsein geschärft und der Menschenverstand damit erweitert werden. Daher ist die einzig wirkungsvolle Möglich-

[105] Christopher Hadnagy, Die Kunst des Human Hacking (Kapitel 9.3 – Seite 431)

keit sich vor Social Engineering Angriffen zu schützen, die Methoden der Angreifer zu kennen und das Sicherheitsbewusstsein auf- sowie auszubauen. Man muss lernen wie ein Angreifer zu denken, um sich effektiv vor dessen Angriffsmöglichkeiten schützen zu können.

5 Analyse ausgewählter Beispiele

In diesem Kapitel werden Beispiele moderner Cyber-Angriffe analysiert, um einen Bezug zwischen der vorangegangenen Theorie und der Praxis zu bilden.
Dabei werden als erstes die jeweiligen Angriffe in ihrem Ablauf beschrieben. Danach werden Hintergrund und Folgen des Hacks beschrieben. Im Anschluss wird der jeweilige Cyber-Angriff mit Hilfe des Cybercrimekreislaufs auf seine Anatomie hin analysiert und Spekulationen zum wahrscheinlichsten Ablauf gegeben. Zum Schluss folgt eine Analyse über den Ablauf der Attacke sowie die verwendeten Mittel und Methoden.

5.1 "The Fappening"-Hack

Ablauf:
2014 hatte ein Hacker die Passwörter diverser Stars in Apples iCloud mittels einer Passwortliste und Brute-Force geknackt. Folge war ein Vollzugriff auf die betreffenden iClouds. Der Hacker konnte so diverse Nacktbilder der Stars entwenden und stellte diese später in das Internet. [106]

Hintergrund:
Nach Eingabe mehrerer falscher Passwörter sollte ein sicheres System die Eingabe weiterer Passwörter normalerweise unterbinden und den Nutzer informieren. Bei seiner „Find my iPhone“ Funktion vergaß Apple dies allerdings, wodurch der Hacker freie Hand hatte. Normalerweise wäre die Brute-Force-Methode sehr ineffizient gewesen, da der Angreifer die Passwörter direkt auf dem Server von Apple ausprobieren musste und die Antwortzeit des Servers so einen großen Einfluss auf die Methode gehabt hat. Der Angreifer konnte mit dem verwendeten Tool „iBrute“ rund eine Millionen Passwörter am Tag durchprobieren[107]. Die verwendete Passwortliste enthält rund 14,3 Millionen Passwörter. Hinzu kommt allerdings, dass die Passwörter der Stars extrem schwach waren. Abbildung 22 zeigt einen Auszug aus der verwendeten Passwortliste, der

```
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
```

Quelle: Eigene Darstellung in Anlehnung an die rockyou.txt Passwortliste

Abbildung 23: Auszug aus der rockyou.txt Passwortliste

[106] Fabian A. Scherschel, Heise Security: The Fappening: Promi-Nacktfotos über Find My iPhone aus der Cloud gesaugt

[107] Fabian A. Scherschel, Heise Security: The Fappening: Promi-Nacktfotos über Find My iPhone aus der Cloud gesaugt

rockyou.txt[108] [109], mit der der Angreifer über 100 Accounts hacken konnte. [110] Die Passwörter sind nach Häufigkeit geordnet.

Folgen:
Die Bilder der Stars verbreiteten sich rasant über das Netz und waren somit nicht mehr restlos zu entfernen.

Nach dem Vorfall haben einige Trittbrettfahrer versucht, Profit aus dem Hack zu schlagen, indem sie angaben, der Hacker zu sein und anboten, weitere Nacktbilder gegen Geld zu veröffentlichen.[111]

Der Angreifer wurde bis heute nicht gefasst.

Anatomie:
Es ist zu vermuten, dass der Angreifer durch einen Zufall auf die Lücke in der „Find my iPhone"-Funktion von Apple aufmerksam wurde.
Nachdem er diese bemerkt hatte, begann er mit der Zielauswahl-Phase. Dabei war das Ziel von vorne herein definiert: Die Lücke ausnutzen, um iCloud-Daten abzugreifen, denn das gefundene Passwort kann darüber hinaus nicht weiter verwendet werden, außer für das Ausfindig machen des aktuellen Standortes des iPhones.
In der Opferauswahl entschied sich der Angreifer für Prominente. Es ist nicht auszuschließen, dass er gezielt nach Nacktbildern der Stars suchte. Vermutlich war ihm bekannt, dass die meisten iPhone Nutzer die Backupfunktion, die Apple seinen Nutzern geradezu aufdrängt, sorglos genutzt haben, ohne den eigentlichen Funktionsumfang vollständig zu kennen. Diese Theorie wird zum Beispiel durch eine Aussage einer der Betroffenen gestützt. Jennifer Lawrence sagte in einem Interview zu dem Vorfall: *„Meine iCloud sagt mir dauernd, ich soll meine Daten sichern. Ich weiß aber gar nicht, wie. Ich lasse das Gerät das einfach machen."*[112] Eine naive Einstellung einer Person ohne Sicherheitsbewusstsein und ohne jegliches Wertgefühl für ihre Daten. Anscheinend ist dies aber kein Einzelfall. Die meisten Nutzer gehen mit ihrer Technik sorglos um. So, als wenn sie nicht wüssten, was ihre Geräte tun, noch wie sie funktionieren.
Durch die Lücke war dem Täter bereits der Zugang bekannt. Für ihn war die Datensammelphase besonders wichtig, da er so viele E-Mail-Adressen wie möglich von seinen potentiel-

---

[108] Ron Bowes, Skull Security (Subsite: Passwords – Datei: rockyou.txt.bz2)

[109] Semper Video, Youtube (Video: Nacktbilder in der Cloud) (Originalquelle zur Passwortliste in Verbindung mit dem Vorfall vom Netz genommen)

[110] Frankfurter Allgemeine, Hacker veröffentlicht Nacktbilder Wie sicher sind meine Fotos in der Cloud?

[111] Ole Reißmann, Spiegel online: Apple geht Hinweis auf iCloud-Hackerangriff nach

[112] Frankfurter Allgemeine, Hacker veröffentlicht Nacktbilder Wie sicher sind meine Fotos in der Cloud?

len Opfern herausfinden musste und diese weiterhin zu den jeweiligen iCloud-Konten passen mussten. Es ist unbekannt, wie er dies bewerkstelligte.
Die Bewertung der Opfer ist ihm vermutlich sehr leicht gefallen, da er sich seiner Methode und damit aller Fähigkeiten, die er brauchte, bereits bewusst war. Er konnte auch davon ausgehen, dass kein Nutzer den Angriff bemerken würde, da er nicht direkt mit den Geräten der Opfer interagierte.
In seiner Vorbereitungsphase schrieb der Angreifer das „iBrute“-Skript zum Ausführen des Angriffs. Er lud sich eine passende Passwortliste mit Passwörtern aus dem englischsprachigen Raum herunter und verband diese mit seinem Skript. Es ist zu vermuten, dass er auch einen Proxy vorbereitete, sowie sein Script an einer Art Test-Account ausprobierte, den er wahrscheinlich selbst erstellt hatte.
Beim eigentlichen Hack musste der Angreifer nur noch sein Skript mit der Liste der herausgefundenen E-Mails der Stars verknüpfen und starten. Das Skript lief vermutlich Tag und Nacht über mehrere Monate oder länger, um derart viele Ergebnisse zu erzielen.
Um das Verwischen der Spuren musste der Angreifer sich wenig Gedanken machen. Er ließ offenbar genug Zeit verstreichen, damit alle Log-Daten der Server gelöscht waren, bevor er seine Beute veröffentlichte. Dies ist aus der Aussage von Opfern abzuleiten, die angaben, einige Fotos bereits vor etwa einem Jahr gelöscht zu haben.[113]
Der Lohn und Grund seines Angriffs sind alle Daten, die er erbeutete. Dabei hat er nur die Nacktbilder unter den Funden veröffentlicht. Da er Vollzugriff auf alle in den kompromittierten iClouds gespeicherten Daten hatte, ist unbekannt, was noch entwendet wurde. Es ist allerdings sehr wahrscheinlich, dass der Hacker mehr heruntergeladen hat als nur gezielt die Nacktbilder seiner Opfer. Wahrscheinlicher ist sogar, dass er ein volles Backup aller Clouds machte und die Daten später sichtete.

Analyse:
Der Angreifer muss weit über 100 Accounts geknackt haben, da er von über 100 Stars Nacktbilder veröffentlichen konnte. Es ist davon auszugehen, dass nicht jeder Star Nacktbilder in die iCloud lädt.
Des Weiteren muss er dies, aufgrund der Eingabelimitierung von etwa einer Million Passwörter pro Tag, über einen sehr langen Zeitraum, vollkommen unentdeckt, getan haben.
Aus der Leichtigkeit, mit der der Angreifer an die iCloud der Betroffenen gekommen ist, kann man erkennen, wie simpel ihre Passwörter gestaltet gewesen sein mussten. Die Betroffenen hätten sich demnach besser schützen können und wären nicht durch einen simplen Wörterbuchangriff kompromittiert worden, wenn sie sichere Passwörter verwendet hätten. Die meisten der Passwörter in der Liste bestehen nur aus Kleinbuchstaben und wenigen Zahlen. Bei diesem Niveau hätte der Angreifer wahrscheinlich auch einen gewissen Erfolg gehabt, wenn er keine Passwortliste benutzt hätte.

[113] Frankfurter Allgemeine, Hacker veröffentlicht Nacktbilder Wie sicher sind meine Fotos in der Cloud?

Durch die Lücke war dem Täter bereits der Zugang bekannt. Für ihn war die Datensammelphase besonders wichtig, da er so viele E-Mail-Adressen wie möglich von seinen potentiellen Opfern herausfinden musste und diese weiterhin zu den jeweiligen iCloud-Konten passen mussten. Es ist unbekannt, wie er dies bewerkstelligte.

Apple trifft die Schuld der Nachlässigkeit, denn der Fehler in der „Find my iPhone“-Funktion scheint seit Veröffentlichung des Dienstes vorhanden gewesen zu sein.
Hauptschuld an dem Erfolg des Angriffs trifft die Stars, die ohne Sicherheitsbewusstsein gehandelt haben. Es ist äußerst unklug, Nacktbilder in eine Cloud zu laden. Die meisten haben vermutlich die Standardeinstellung der Apple iCloud verwendet, die alle Fotos automatisch hochlädt, ohne sich Gedanken über die Einstellungen zu machen. Viel schlimmer sind aber die absolut unsicheren Passwörter. Gerade als Star muss man sich absolut dem eigenen Datenwert bewusst sein und sollte davon ausgehen, dass private Accounts regelmäßigen Angriffen unterzogen werden. Das Interesse von „Fans“, gerade an die persönlichen Daten von Stars zu gelangen, ist extrem groß, was den Datenwert extrem steigert. Dieser Sachverhalt hätte den Stars bewusst sein müssen.

5.2 Wannacry-Krypto-Trojaner

Ablauf:
Der Wannacry-Krypto-Trojaner befiel im Mai 2017 in sehr kurzer Zeit viele tausend Rechner weltweit. Dabei nutzt die Wannacry-Schadware eine Lücke in Windows aus, die seit Windows XP vorhanden ist und sich durch alle folgenden Betriebssysteme zieht. Die Lücke existiert demnach seit 2011.[114] Wannacry sperrt den PC der Opfer und will diese so zu einer Zahlung an die Angreifer zwingen. Daher gehört Wannacry zur Gruppe der Ransomware, zu Deutsch „Lösegeld-Software“. Die Wannacry-Ransomware besitzt außerdem die Fähigkeit, über das LAN andere PCs zu befallen, wodurch sie sich extrem schnell verbreitet hat.[115]

Hintergrund:
Der Wannacry-Trojaner verschlüsselt die Daten des Benutzers im Hintergrund, deshalb wird diese Art der Ransomware oft auch Krypto-Trojaner genannt. Wannacry nutzt allerdings, anders als viele andere Ransomware-Varianten, eine Lücke im Windows Betriebssystem aus, wodurch er sich erhöhte Rechte sichern kann und sich wie ein Wurm über das LAN ohne Nutzerinteraktion verbreiten kann. Des Weiteren installiert Wannacry eine Backdoor und gliedert den Rechner so in ein Botnetz ein. Wannacry ist streng genommen also eine Chimäre, da es die Eigenschaften eines Wurms, eines Trojaners, einer Botnetz-Soft-

[114] Microsoft, Microsoft: Windows XP Is Here!

[115] Volker Briegleb, Heise online: WannaCry: Was wir bisher über die Ransomware-Attacke wissen

ware sowie eines Exploits beinhaltet. Durch die Möglichkeit, sich über das LAN zu verbreiten, ist Wannacry besonders gefährlich. Windows lieferte gegen die Lücke, die die Wannacry-Ransomware nutzt, ein Sicherheitsupdate, welches an alle unterstützten Betriebssysteme vor auftauchen der ersten Wannacry-Software ausgeliefert wurde. Obwohl Windows XP und Windows Server 2003 zu diesem Zeitpunkt nicht mehr unterstützt wurden lieferte Microsoft für Windows XP und Windows Server 2003 ebenfalls ein Sicherheitsupdate nach. [116]
Die Wannacry-Software konnte erstellt werden, da eine Hackergruppe zahlreiche Exploits der NSA-nahen Equation Group veröffentlicht hatten. Die ausgenutzte Lücke ist dort unter dem Namen EternalBlue bekannt gewesen und wurde von der NSA offenbar bereits mehrere Jahre lang ausgenutzt, statt sie an Microsoft zu melden.[117]

Folgen:
Die Folgen der Krypto-Chimäre waren verehrend. Nach wenigen Tagen hatte Wannacry bereits zehntausende Rechner infiziert. Darunter viele Krankenhäuser, deren Betrieb dadurch stark eingeschränkt wurde. Besonders in England war dies ein großes Problem.[118]

Betroffen waren unter anderem auch die Deutsche Bahn sowie die Telefónica in Spanien.[119]

Da zurzeit immer noch 2 % aller Rechner mit Windows XP laufen[120] und diverse Nutzer das von Microsoft rechtzeitig bereitgestellte Update nicht eingespielt hatten, konnte sich die Software mühelos durch alle Netze verbreiten.

Wenige Tage nach der Infektion hat ein Sicherheitsexperte eine „Kill-Switch“, also eine Art „Not-Aus“ Schalter, in der Software gefunden. Die Software versuchte, bevor sie sich über das Netzwerk verbreitete, auf eine bestimmte Internetadresse zuzugreifen. War diese Domain erreichbar, so verbreitete Wannacry sich nicht über das LAN weiter. Die Domain war ursprünglich nicht registriert, deshalb registrierte der Sicherheitsexperte die Domain auf eigenen Namen und stoppte so vorläufig die Ausbreitung. Wenig später tauchte eine Variante der Wannacry-Schadware auf, die keinen Kill-Switch mehr besaß.[121]

---

[116] Volker Briegleb, Heise online: WannaCry: Was wir bisher über die Ransomware-Attacke wissen

[117] Martin Holland, Axel Kannenberg, Heise online: WannaCry: Angriff mit Ransomware legt weltweit Zehntausende Rechner lahm

[118] Martin Holland, Axel Kannenberg, Heise online: WannaCry: Angriff mit Ransomware legt weltweit Zehntausende Rechner lahm

[119] Volker Briegleb, Heise online: WannaCry: Was wir bisher über die Ransomware-Attacke wissen

[120] Statista, Marktanteile der führenden Betriebssysteme in Deutschland von Januar 2009 bis Mai 2017

[121] Michael Link, Heise online: Ransomware WannaCry: Sicherheitsexperte findet "Kill-Switch" – durch Zufall

Kurz nach Bekanntwerden der Wannacry-Schadware, rieten Sicherheitsexperten in den Medien bereits ausdrücklich davon ab, auf die Lösegeldforderungen einzugehen.[122]

Nach etwa einer Woche waren bereits über 200.000 Rechner betroffen, die Erpresser haben etwa zu dieser Zeit, durch eine Backdoor, eine Nachricht an die Nutzer geschickt, in der sie angaben, bereits viele Rechner zahlender Opfer entschlüsselt zu haben und die Opfer nochmals dazu aufforderten, das Lösegeld zu zahlen.[123]

Bereits am 18.Mai haben Forscher ein Tool namens Wannakiwi zur Entschlüsselung der Daten online gestellt.[124]

Die Verantwortlichen für die Wannacry-Software wurden bis heute nicht gefasst.

Anatomie:
Anlass für die Schadware hat das Bekanntwerden der EternalBlue-Lücke in Windows gegeben. Somit war den Angreifern der Angriffsvektor bewusst und sie entschieden sich in der Zielauswahl-Phase, Profit als Ziel anzustreben.
Das Vorgehen, für welches sie sich entschieden, war eine Ransomware zu kreieren, die die Opfer möglichst schnell zu einer Zahlung zwingt. Denn durch das Bekanntwerden der Lücke war klar, dass sie nur wenig Zeit hatten, um möglichst viele Rechner ohne das von Microsoft kommende Update zu infizieren.
Die Opferauswahl war durch die Lücke ebenfalls zum Teil vordefiniert, da die Lücke nur in Windows Betriebssystemen ab Windows XP vorkam, waren alle Nutzer dieser Betriebssysteme potentielle Opfer.
Die Phase der Datensammlung konnte somit weitgehend entfallen, da der Angriff ungerichtet war. Es ist allerdings zu vermuten, dass die Angreifer sich bereits mit dem Erstellen von Ransomware auskannten oder sich zumindest andere erfolgreiche Ransomware ansahen, um die Wannacry-Software zu erstellen. Somit hatten die Angreifer sehr wahrscheinlich bereits einige Erfahrung mit Schadware und Phishing und wussten bereits, dass ein gewisser Anteil an Nutzern auf die E-Mails hereinfallen würde. Eine Bewertung der Opfer entfiel demnach. Den Rest erledigte die EternalBlue-Lücke, womit nur ein einziger Nutzer pro Netzwerk auf die Phishing-Mail hereinfallen musste.
In der Vorbereitungsphase haben die Täter die Software geschrieben und getestet. Dabei müssen sie auch entschieden haben, über welche Angriffsvektoren des Social Engineering sie in ihrer Software, den Druck auf die Opfer erhöhen wollen, um sie möglichst schnell zu einer Zahlung zu zwingen. Die Täter hatten entweder bereits eine Verteilungsmöglichkeit für Phishing, sowie eine umfangreiche Liste mit E-Mails potentieller Opfer oder kauften

[122] Bernd Kling, ZDNet: WannaCry: Experten raten von Lösegeldzahlung ab

[123] Judith Horchert, Spiegel online: "WannaCry"-Erpresser betteln um Lösegeld

[124] Matt Suiche, comae technologies: WannaCry—Decrypting files with WanaKiwi + Demos

diese über das Darknet oder Ähnliches ein. In dieser Phase haben die Angreifer auch Phishing-Mails vorbereitet, über die die Schadware verteilt werden sollte, sowie den genauen Weg ausgearbeitet, über den die Software später die Rechner der Opfer infizieren würde.
Die Phase des eigentlichen Hacks fiel für die Angreifer sehr klein aus. Sie mussten lediglich ihre Schadware in die jeweiligen Phishing-Mails laden und diese massenhaft versenden. Danach warteten sie die ersten Reaktionen ab. Die Phase des Verwischens der Spuren entfiel bei diesem Angriff, da dieser extrem unpersönlich und ungerichtet war. Durch das Verwenden von Bitcoin als Zahlungsmethode sind die Täter nicht zurück zu verfolgen, womit sie bereits in der Vorbereitungsphase einen Teil ihrer Spuren verwischt haben.
Nach wenigen Tagen hatte ein Sicherheitsexperte bereits den Kill-Switch in der Software entdeckt und die Domain registriert. Daraufhin sind die Täter zurück in die Zielauswahlphase gesprungen und mussten ihr Vorgehen anpassen. Das Ziel blieb gleich und das Vorgehen war klar, der Kill-Switch musste entfernt werden, damit die Software weiterhin Erfolg haben würde.
Es wurde in einer zweiten Vorbereitungs-Phase eine neue Schadware auf Basis der alten erstellt, ohne besagten Kill-Switch.
Diese wurde in einer zweiten Hack-Phase erneut in Umlauf gebracht. Es ist ebenfalls nicht auszuschließen, dass die Täter ihre bereits laufende Schadware updaten konnten, da sie eine Backdoor auf den Rechnern der Opfer installiert hatten und die Rechner durch ein Bot-Netzwerk für sie erreichbar waren.[125] [126] Weshalb die Täter einen Kill-Switch einbauten, ist unklar. Denkbar ist, dass es ein flüchtiger Fehler war und der Kill-Switch vor dem Release der Software hätte entfernt werden sollen. Denkbar ist ebenfalls, dass die Täter die Möglichkeit in Betracht zogen, dass ihre Software extremen internationalen Erfolg haben würde und sie deshalb eine Notbremse einbauten, bevor extrem kritische Infrastruktur betroffen wäre, wie zum Beispiel Flughäfen oder Ähnliches, was zum Tod tausender Menschen hätte führen können.
Die Software bekam in den Medien große Aufmerksamkeit und es wurde massenhaft von Sicherheitsexperten abgeraten, auf die Zahlungsforderungen einzugehen.[127] Dies muss sich stark im Profit der Täter abgezeichnet haben, weshalb sie sich entschieden, nochmals in die Zielauswahl-Phase zu gehen und ihr Vorgehen anzupassen. Dabei entschieden sie sich, ihre Backdoor über das Wannacry-Botnetz anzusteuern, um den Opfern eine weitere Zahlungsaufforderung zu schicken. Ein offenbar verzweifelter Versuch nochmals den Profit zu steigern. Bis Mitte Mai erbeuteten die Erpresser nämlich grade einmal 70.000 $.[128]

---

[125] BSI, Informationen zum Cyberangriff auf den Bundestag – hier: Abschlussbericht BSI (geleaktes Dokument)

[126] MalwareInt: Botnet Tracker - WCRYPT

[127] Bernd Kling, ZDNet: WannaCry: Experten raten von Lösegeldzahlung ab

[128] ZEIT ONLINE, dpa, Reuters, AFP, sre: Ransomware erbeutet weniger als 70.000 Dollar Lösegeld

Der Lohn und die Motive der Täter waren finanziell. Solange die Schadware noch Rechner befällt oder einige infiziert sind, ist nicht auszuschließen, das immer wieder Opfer zahlen werden. Zum jetzigen Zeitpunkt, dem 27.07.2017, sind immer noch über 220.000 Rechner mit der Botnetzsoftware des Wannacrypt-Bot-Netzwerks infiziert und waren innerhalb der letzten 24 Stunden online. Die insgesamt von MalwareInt gezählte Anzahl der Rechner, die sich mit dem Botnetz verbunden haben, beträgt zu diesem Zeitpunkt fast 560.000.[129]

Analyse:
Die Wannacry-Ransomware war bis zum heutigen Datum vermutlich die erfolgreichste ihrer Art. Keine Ransomware hatte sich bisher in ähnlich rasanter Zeit verbreitet und so viele kritische Infrastrukturen auf einmal getroffen.
Wannacry verbreitete sich dabei über zwei Angriffsvektoren, wie bei Ransomware und Trojanern üblich per Mail und zusätzlich per Exploit, über das LAN. [130] Dieses Vorgehen hatte zur Folge, dass nicht wie üblich, einzelne Rechner von der Ransomeware betroffen waren, sondern immer gleich ganze Netzwerke, weshalb der geschäftliche Betrieb an vielen Stellen gestört war.
Schuld trifft zum einen die NSA. Zwar ist es nachvollziehbar, dass Geheimdienste, im Zuge der Vorbereitung auf einen digitalen Krieg Sicherheitslücken horten. Es muss ihnen aber auch bewusst sein, dass eine solch kritische Lücke, sollte sie von Kriminellen ausgenutzt werden können, immer zum kurzfristigen Stillstand wichtiger Infrastruktur wie Krankenhäusern oder öffentlichen Verkehrsmitteln führen kann. Die NSA nutzte die Lücke offenbar schon seit vielen Jahren.[131] Die Lücke selbst ist dabei zum jetzigen Zeitpunkt 16 Jahre alt. Je älter eine solche Lücke ist, desto höher ist auch die Wahrscheinlichkeit, dass diese auch von anderen gefunden und ausgenutzt wird. Daher sollten sich Geheimdienste überlegen, ob gewisse Lücken, sofern sie alt genug sind, nicht lieber an die Softwarehersteller gemeldet werden sollten. Dadurch kann der Ausfall solcher Infrastruktur zumindest teilweise vermieden werden. Es ist nicht auszuschließen, dass durch solch effektive Schadware wie Wannacry, Menschenleben gefährdet werden. Die Geheimdienste der ganzen Welt trifft demnach eine moralische Schuld. Diese Lücke wurde darüber hinaus nicht einfach gefunden, sondern der Equation Group von einer Hackergruppe gestohlen. Daher trifft die NSA eine doppelte Schuld, da sie sich selbst, beziehungsweise ihre zugehörigen Gruppen, nicht genug absichern konnte, um die Lücke geheim zu halten.

---

[129] MalwareInt: Botnet Tracker - WCRYPT

[130] Volker Briegleb, Heise online: WannaCry: Was wir bisher über die Ransomware-Attacke wissen

[131] Martin Holland, Axel Kannenberg, Heise online: WannaCry: Angriff mit Ransomware legt weltweit Zehntausende Rechner lahm

Zum anderen trifft die betroffenen Nutzer eine genau so große Schuld. Microsoft hat rechtzeitig, vor Erscheinen der Wannacry Schadware, für alle unterstützten Betriebssysteme einen Sicherheitspatch veröffentlicht. Jeder, der regelmäßig Sicherheitsupdates einspielt, war demnach vor dem Angriff sicher.
Darüber hinaus verwenden immer noch verhältnismäßig viele Nutzer Windows XP und Windows Server 2003. Windows stellte den Support für das Betriebssystem Windows XP und damit alle sicherheitsrelevanten Updates bereits im April 2014 ein.[132] Für Windows Server endete der Support bereits im Juli 2015.[133] Damit hat Microsoft die Betriebssysteme bereits 2 und 3 Jahre länger unterstützt, als eigentlich angedacht, um den Nutzern die Zeit zum Umstieg zu geben. Jetzt, im Jahr 2017 sind bereits 4 neuere Versionen des Betriebssystems Windows auf dem Markt. Es ist also fahrlässig von den Nutzern, ein derart altes Betriebssystem zu verwenden. Spätestens nachdem der Support für ein System eingestellt wird, sollte dieses gewechselt worden sein. Die Hersteller der Betriebssysteme kündigen diese Schritte immer rechtzeitig an.

Abbildung 24: Screenshot der Wannacry Ransomeware

Quelle: Heise online, WannaCry: Angriff mit Ransomware legt weltweit Zehntausende Rechner lahm (Artikel von Martin Holland und Axel Kannenberg)

Die Software selbst nutzte darüber hinaus auch Methoden des Social Engineering. In Abbildung 23 ist ein Ausschnitt der Ransomeware zu sehen. Dabei kann man erkennen, das zwei Timer laufen. Der obere erhöht nach drei Tagen das Lösegeld und der untere droht damit, nach sieben Tagen alle verschlüsselten Daten zu löschen.

---

[132] Microsoft, Ende des Supports für Windows XP

[133] Microsoft, Am 14. Juli 2015 wurde der erweiterte Support für Windows Server 2003 eingestellt.

Im Gegensatz zu anderer Ransomeware, wie dem BKA-Trojaner, versucht die Wannacry-Ransomware sich gar nicht erst zu verstecken und zum Beispiel als eine Behörde auszugeben. Statt mit der Angst vor einer Obrigkeit oder Gefängnis zu arbeiten, gibt sich die Schadware gleich als solche zu erkennen. Sie nutzt gezielt die Angst des Nutzers, seine Daten zu verlieren. Durch die Timer wird zusätzlicher Druck aufgebaut, was vermutlich viele Nutzer zu einer Zahlung bewegt hat.

Die Täter hatten allem Anschein nach nicht vor, die Rechner zu entschlüsseln, da der Identifikationscode für die Bezahlung bei allen Infektionen gleich ist. Daher können die Entwickler der Software gar nicht wissen welche Opfer gezahlt haben. Es ist aber unklar, ob die Täter wirklich nie vorhatten, die Rechner zahlender Opfer zu entschlüsseln oder aus Zeitdruck keinen eindeutigen Schlüssel einbauten. Denkbar ist ebenfalls, dass sie auf Grund des Drucks einen Programmierfehler machten. [134]

Die Nachricht an die Opfer ist sehr untypisch, und lässt darauf schließen, dass die Täter deutlich weniger Geld eingenommen haben, als erwartet. Die Angabe, dass viele Rechner bereits entschlüsselt worden wären, war gelogen, da die Software nicht nur gewisse Verzeichnisse verschlüsselt, sondern darüber hinaus andere Daten einfach löscht, wodurch diese nur mit einem Wiederherstellungstool hätten wiederhergestellt werden können.[135]

Die Nachricht der Täter an die Opfer, das schnelle Finden des Kill-Switches der ersten Version sowie das schnelle Erstellen eines Entschlüsselungstools haben vermutlich alle mit der großen, öffentlichen Aufmerksamkeit zu tun, die der Ransomeware-Wurm erhalten hat.

Darüber hinaus haben die Täter zwei Fehler gemacht. In erster Linie den Kill-Switch überhaupt einzubauen, beziehungsweise die Domain vollständig unregistriert zu lassen. Zum anderen nicht einmal den Anschein zu erwecken, dass sie die PCs der Opfer wieder entschlüsseln würden, indem der Identifikationscode gleich war und Daten dauerhaft von der Festplatte gelöscht wurden. Den Sicherheitsexperten ist diese Tatsache durch den immer gleichen Code, der in der Software gut sichtbar war, sehr schnell aufgefallen. Für eine so hoch entwickelte Schadware sind dies Anfängerfehler, sehr wahrscheinlich sind sie aber dem Zeitdruck geschuldet, dem die Angreifer unterlagen.

---

[134] David Glance, The Conversation: WannaCry hackers had no intention of giving users their files back even if they paid

[135] Judith Horchert, Spiegel online: "WannaCry"-Erpresser betteln um Lösegeld

5.3 Parlakom-Hack

Ablauf:

Als Parlakom-Hack wird der Angriff auf das Netz des Deutschen Bundestags genannt, der Anfang Mai 2015 bekannt wurde. Aus einem geleakten Bericht des BSI geht hervor, dass der Verfassungsschutz Anfang Mai 2015 Anomalien im Parlakom-Netzwerk bemerkte und daraufhin den Deutschen Bundestag informierte. Das BSI hatte in etwa dem selben Zeitraum ebenfalls diese Anomalien im Netzwerk entdeckt. Alles deutete darauf hin, dass das zentrale Netzwerk des Bundestags kompromittiert worden war.[136]

Daraufhin wurden Gegenmaßnahmen eingeleitet. Zusätzlich zum Verfassungsschutz und den Mitarbeitern des BSI wurden Spezialisten der Karlsruher IT-Sicherheitsfirma BFK edv-consulting herangezogen.[137]

Die Spezialisten stellten fest, dass die Kompromittierung anscheinend von einem einzigen Rechner ausging. Dieser befand sich im Subnetz der Linksfraktion des Bundestages und der Angriff entspreche, laut BSI, dem klassischen APT-Muster, wie es in Unterkapitel 2.3.2 bereits erklärt wurde. Im Grunde bedeutet dies nur, dass die Täter anscheinend wussten, was Sie taten. Sie wollten bestimmte Daten abgreifen und hatten einen Plan, dies umzusetzen.[138]

Die Hacker suchten scheinbar gezielt nach Archivdateien für Outlook und nach aktuellen Office Dateien.[139]

Der Hack startete angeblich am 30. April 2015. Wobei eher der 13. April oder davor als Starttermin der Infektion angesehen werden kann. Denn bereits zu diesem Termin war dem Bundesamt für Verfassungsschutz (BfV) die Adresse des Controlservers der Schadware aufgefallen und der Zugang zu diesem Server wurde im Netz des IVBB, dem Informationsverbund Berlin-Bonn, einem Kommunikationverbund für oberste Bundesbehören, gesperrt. Der Bundestag wurde allerdings über diese Sperrung nicht informiert und nicht gewarnt. Das BSI und das BfV hatten Zugriff auf das vom Bundestag verwendete IDS und konnten die Daten auswerten.[140] Der Bundestag selbst konnte die Adresse aber aufgrund dieser Informationsbarrieren zwischen den Institutionen erst am 21. Mai sperren. So wurden die Behörden erst im Mai auf die Aktivitäten im Parlakom-Netzwerk aufmerksam.

Über den einzelnen infizierten Rechner luden die Hacker diverse andere Schadsoftware nach und verbreiteten sich über das Netzwerk des Bundestags. Auf verschiedenen

---

[136] BSI, Informationen zum Cyberangriff auf den Bundestag – hier: Abschlussbericht BSI (geleaktes Dokument)

[137] Bundestag, Kurzprotokoll der 7. Sitzung der IuK-Kommission (geleaktes Dokument)

[138] BSI, Informationen zum Cyberangriff auf den Bundestag – hier: Abschlussbericht BSI (geleaktes Dokument)

[139] Bundestag, Kurzprotokoll der 7. Sitzung der IuK-Kommission (geleaktes Dokument)

[140] Bundestag, Kurzprotokoll der 6. Sitzung der IuK-Kommission (geleaktes Dokument)

Rechnern des Netzes richteten die Hacker mehrere Backdoors, sowie Keylogger, Programme zum Erstellen von Screenshots und Scripte zum Sammeln von Daten ein. Sie bereiteten demnach den eigentlichen Angriff immer noch vor.
Ende April bis Anfang Mai war es dann so weit und die Hacker durchsuchten intensiv das Netzwerk des Bundestags und erbeuteten dabei rund 16 GB an Daten. Darunter hauptsächlich E-Mail-Archive. Nach Entdecken des Angriffs wurden diverse Sicherheitsmaßnamen der drei beteiligten Sicherheitsexperten eingeleitet. Ende Mai erklärte das BSI die Nutzung der Computersysteme im Bundestag wieder für sicher.[141] [142]

Hintergrund:
Die Angreifer drangen durch einen einzelnen Rechner der Linksfraktion in das Parlakom-Netzwerk ein. Es ist demnach zu vermuten, dass ein einzelner Abgeordneter durch eine Phishing-Mail die Kompromittierung seines Rechners auslöste. Die Struktur des Parlakom-Netzwerks war sehr zentral und auf den einfachen Datenaustausch der Abgeordneten untereinander abgestimmt. Dadurch war es für die Angreifer besonders einfach, sich über das Netz zu verbreiten, da sie nicht durch starke Firewalls oder Inselnetzwerke an der Ausbreitung gehindert waren. Somit gelang es den Angreifern mit einfachen Tools (zum Beispiel „mimikatz“[143]) diverse Passwörter zu extrahieren.[144] Letztendlich konnten die Angreifer dadurch 5 der 6 Accounts der Domänenadministratoren kompromittieren und 16 GB Daten entwenden.[145]

Folgen:
In den Medien wurde der Vorfall stark diskutiert und nicht ganz sachlich behandelt. Darin sprach man von einer hohen Komplexität, einer maßgeschneiderten Attacke, sowie großem Hintergrundwissen der Täter[146] und dass sie nach Adressbucheinträgen und Terminkalendereinträgen gesucht hätten.[147] Tatsächlich ist in den geleakten Dokumenten, auf die sich

[141] BSI, Informationen zum Cyberangriff auf den Bundestag – hier: Abschlussbericht BSI (geleaktes Dokument)

[142] Bundestag, Kurzprotokoll der 7. Sitzung der IuK-Kommission (geleaktes Dokument)

[143] https://github.com/gentilkiwi/mimikatz

[144] Bundestag, Kurzprotokoll der 7. Sitzung der IuK-Kommission (geleaktes Dokument)

[145] Bundestag, Kurzprotokoll der 8. Sitzung der IuK-Kommission (geleaktes Dokument)

[146] Maik Baumgärtner, Sven Röbel und Jörg Schindler, Spiegel online: Ermittler vermuten Geheimdienst hinter Cyberangriff

[147] Maik Baumgärtner, Sven Röbel und Wolf Wiedmann-Schmidt, Spiegel online: Hacker kopierten Abgeordneten-E-Mails

die Berichte stützen, davon keine Rede.[148] Die Täter suchten lediglich nach Outlook-Archivdaten und neuen Office-Dokumenten.

In Folge des Angriffs empfahlen Sicherheitsexperten ein dezentrales Netzwerk im Bundestag einzuführen, damit bei einer möglichen weiteren Infektion nur ein Inselnetz betroffen ist und die Angreifer sich nicht einfach über das Netzwerk ausbreiten können.[149]

Das BSI reagierte mit einem Drei-Phasen-Plan auf den Hack. [150]

1. Analyse
2. Abgesicherter Übergangsbetrieb
3. Konzeption sicherer Neustart

In der ersten Phase wurden die auffälligen Systeme forensisch untersucht, um die Methoden und Ziele der Hacker abzuleiten. Dabei halfen die Medien den Hackern angeblich durch ihre schnelle Berichterstattung indirekt und warnten sie so vor. Es wäre den Behörden vielleicht sogar möglich gewesen, die Angreifer zu identifizieren, wenn ihnen nicht aufgefallen wäre, dass sie entdeckt worden waren, so das BSI.
Ziel der zweiten Phase war es, den Datenabfluss zu unterbinden. Aus diesem Grund wurde der Internetverkehr des Bundestags über das Regierungsnetz IVBB geleitet, um Angriffe live zu erkennen und zu unterbinden. Hinzu kommt, dass in dieser Phase die gehackten Accounts deaktiviert und die kompromittierten Rechner neu aufgesetzt wurden.
In der dritten Phase wurden die gewonnenen Erkenntnisse benutzt, um das Parlakom-Netzwerk zu verbessern. Zentraler Punkt ist hierbei, dass die Infektion eines einzelnen Rechners nicht zur Infektion des ganzen Netzwerks führen darf.[151]

Wer für den Angriff auf den Bundestag verantwortlich ist, steht nicht fest, die Täter wurden nicht gefasst.

Anatomie:
Aus welchen Gründen genau die Täter auf das Netzwerk des Bundestags zugreifen wollten und ob sie überhaupt gezielt nach bestimmten Informationen zu einem bestimmten Thema gesucht haben, ist unklar. Denkbar ist, aufgrund der Daten die sie erbeuteten, das ihre Motive finanziell oder wirtschaftlich geprägt waren. Die erbeuteten Informationen könnten demnach für Erpressungen einzelner Abgeordneter eingesetzt werden.

---

[148] Anna Biselli, Netzpolitik.org: Wir veröffentlichen Dokumente zum Bundestagshack: Wie man die Abgeordneten im Unklaren ließ

[149] Bundestag, Kurzprotokoll der 8. Sitzung der IuK-Kommission (geleaktes Dokument)

[150] BSI, Informationen zum Cyberangriff auf den Bundestag – hier: Abschlussbericht BSI (geleaktes Dokument)

[151] BSI, Informationen zum Cyberangriff auf den Bundestag – hier: Abschlussbericht BSI (geleaktes Dokument)

Es kann ebenso sein, dass die Täter erst nachdem sie erfolgreich eingedrungen waren anfingen, sich Gedanken darüber zu machen, welche Daten sie stehlen wollen. Daher ist erst einmal davon auszugehen, dass ihr Ziel in erster Linie das Eindringen in das Netzwerk des Bundestags war. Es ist zu vermuten, dass die Angreifer ebenfalls von außen versucht haben, in das Netzwerk des Bundestags einzudringen, daran scheiterten und deshalb das Vorgehen über Phishing-Mails wählten.
Die Opferauswahl war durch das Ziel ebenfalls definiert. Als Opfer kamen alle Abgeordneten des Bundestags in Frage.
Die Fähigkeiten der Hacker waren vermutlich recht umfangreich und sie konnten davon ausgehen, dass die Abgeordneten keinen gezielten Angriff auf den Bundestag durch eine ihrer Mails erwarteten, beziehungsweise, dass ihr Angriff unter den üblichen Spam-Mails nicht groß auffiel.
In der Vorbereitungs-Phase bereiteten die Angreifer ihre Phishing-Mails vor, sammelten alle E-Mails der Abgeordneten, die sie über die Seite des Bundestags vermutlich recht einfach in Erfahrung bringen konnten und schrieben ihre Schadware.
In der Hack-Phase verschickten die Angreifer ihre Mails vermutlich an einen Großteil der Abgeordneten des Bundestags und warteten auf die Rückmeldung ihrer Software. Nachdem die Erstinfektion erfolgreich war, luden sie weitere Programme nach, um das Netz weiter zu infizieren. Sie scannten es und kehrten zurück in eine weitere Zielauswahl-Phase.

In der zweiten Zielauswahl-Phase durchsuchten sie vermutlich den infizierten PC. Dabei könnte ihnen aufgefallen sein, dass Outlook sowie Office auf dem PC installiert sind und sie könnten demnach das Ziel gefasst haben, möglichst viele und aktuelle Informationen aus dem Netz zu entwenden. Dabei ist zu vermuten, dass sie sich auf Outlook-Archivdateien sowie neue Office-Dokumente beschränkten, weil sie das E-Mail-Netzwerk des Bundestages nicht kompromittieren konnten.[152]
Infolge dessen haben sie sich in einer weiteren Vorbereitungs-Phase darauf vorbereitet, das restliche Netzwerk zu infiltrieren.
In einer weiteren Hack-Phase haben sie dann manuell das Netzwerk durchsucht und den Upload der Daten vorbereitet. Ihr erster Upload-Versuch am 08.05.2015 schlug fehl, sie wurden allerdings nicht direkt entdeckt, weshalb sie mit ihrem Plan fortfuhren und so insgesamt 16 GB Daten erbeuteten.[153]
Der Lohn der Täter waren am Ende 16 GB Daten und der größte bis jetzt bekannte, gelungene Angriff auf das Parlakom-Netzwerk des Bundestags.

Analyse:
Der Bundestag und alle Ermittlungsbehörden haben sich verständlicherweise sehr bedeckt gehalten und keine offiziellen Dokumente veröffentlicht. Alle konkreten Angaben stammen

[152] Bundestag, Kurzprotokoll der 7. Sitzung der IuK-Kommission (geleaktes Dokument)

[153] Bundestag, Kurzprotokoll der 6. Sitzung der IuK-Kommission (geleaktes Dokument)

aus geleakten Dokumenten des Bundestages und des BSI.
Festzuhalten ist, dass der Angriff allem Anscheins nach nicht so professionell zugeschnitten war, wie es zunächst durch die Medien den Anschein hatte. Die Täter hatten offenbar kein großes Hintergrundwissen über das Netz, noch suchten sie gezielt Dokumente. Sie haben lediglich nach Archivdateien von Outlook gesucht und nach neueren Office-Dokumenten. Dabei könnten sie durch den Rechner, auf dem die Erstinfektion stattfand, erst auf die Idee gekommen sein, diesen Daten zu suchen. Denn auf dem infizierten Rechner waren die betreffenden Programme mit Sicherheit vorhanden. Daher kann auch nicht davon ausgegangen werden, dass die Angreifer in irgendeiner Weise tieferes Hintergrundwissen hatten. Das E-Mail-Netzwerk des Bundestages wurde dabei nicht kompromittiert.[154]
Die Angreifer suchten demnach relativ simpel und ungezielt nach Informationen. Daher ist auch nicht davon auszugehen, dass zwingend ein Geheimdienst hinter der Attacke steckte. Die Struktur des Angriffs war eher simpel und der Erfolg hauptsächlich dem intern schlecht abgesicherten Netzwerk des Bundestags geschuldet. Zu einem derartigen Ergebnis kommt das BSI im Bundeslagebericht 2015 ebenfalls.
Darin heißt es des Weiteren, dass eine genaue Analyse der Erstinfektion durch die kurze Speicherfristen von 7 Tagen nicht möglich war.[155] Dadurch konnte der Zeitpunkt der Erstinfektion und seine genaue Quelle nicht identifiziert werden.
Im Parlakom-Netzwerk wurden Domainserver verwendet, die über Windows liefen und bekannterweise bei internem Zugriff mit wenig Aufwand gehackt und die Passwörter ausgelesen werden konnten. Der Bundestag war schlichtweg nicht darauf vorbereitet, von innen angegriffen zu werden.
Daher ist der Erfolg der Hacker der Erstinfektion zuzuschreiben, die offenbar durch eine einfache Phishing-Mail stattfand. Der E-Mail-Server des Bundestags konnte diese offenbar nicht filtern und die Abgeordneten des Bundestags haben offenbar kein ausgeprägtes Sicherheitsbewusstsein. Was die E-Mail genau beinhaltete, ist nicht bekannt. Es ist aber offensichtlich, dass den Hackern der Zugang zum Bundestag durch Social Engineering in Verbindung mit ungeschulten Abgeordneten gelang, deren Rechner Zugriff auf das gesamte interne Netz hatten.

Dem Bundestag ist des Weiteren vorzuwerfen, die ersten Anzeichen nicht ernstgenommen zu haben. Dabei wurde am 08.05.2015 bei einer Routineüberwachung bereits Folgendes festgestellt: *„Konkret sei ein Server der Bundestagsverwaltung in einem Festplattenbereich mit einer ungewöhnlichen Menge an Daten überlastet worden. In einer darauf folgenden Analyse der Kommunikationsbeziehungen sei festgestellt worden, dass zu diesem Server nicht vorgesehene Verbindungen von einem Abgeordnetenbüro bestanden haben.“*[156] Das Aufnehmen einer Verbindung eines Abgeortnetenbüro-Rechners zu einem Datenserver,

[154] Bundestag, Kurzprotokoll der 7. Sitzung der IuK-Kommission (geleaktes Dokument)

[155] BSI, Die Lager der IT-Sicherheit in Deutschland 2015 (Abschnitt 2.2.3 – Seite 26)

[156] Bundestag, Kurzprotokoll der 6. Sitzung der IuK-Kommission (geleaktes Dokument)

der obendrein mit einer ungewöhnlich großen Menge an Daten überlastet worden war, war bereits ein alamierender Hinweis. Dieser hätte ernstgenommen werden müssen. Es war vermutlich der erste Versuch der Täter, Daten zu entwenden.
Im gleichen Bericht heißt es weiter, dass das Bundestagsnetz häufig von Trojanern und Viren befallen wäre und der Vorfall deshalb *„[…] im Rahmen des Alltäglichen […]“* gehandhabt wurde.[157] Dies lässt weiter vermuten, das die Bundestagsabgeordneten keinerlei Sicherheitsbewusstsein besitzen und ihnen auch keines vermittelt wird. Ein Netz wie der Bundestag kann es sich nicht leisten, derart ungeschulte „Mitarbeiter“ an Computern arbeiten zu lassen, die sich in einem so einfach gestricktem Netzwerk frei bewegen dürfen.
Aus sicherheitstechnischer Sicht ist dieses Handeln und die Handhabung der inneren Sicherheit des Parlakom-Netzwerks höchst fragwürdig, unzureichend und fahrlässig. In diesem Sinne ist es nur eine Frage der Zeit, bis der nächste große Hack stattfindet, falls dieser überhaupt entdeckt werden würde.

Der Bundestag verfügte weiterhin über ein IDS, auf welches sie selbst aber keinen Zugriff hatten, sondern nur das BSI und das BfV. Im Kurzprotokoll der 7. Sitzung heißt es dazu: *„Der Bundestag setze seit einigen Jahren ein rudimentäres IDS ein. Rudimentär deshalb, weil die Informationen über verdächtige Server den Bundestag nur verspätet oder nie erreichten. So sei dem BSI seit dem 13. April 2015 die Adresse bekannt gewesen, an die die Daten aus dem Bundestag abgeflossen seien. Diese Adresse habe der Bundestag am 21. Mai sperren können, da diese Information erst zu diesem Zeitpunkt dem Bundestag mitgeteilt worden sei.“*[158] Es hat also über einen Monat gedauert bis die ersten Anzeichen, die von einem einfachen IDS entdeckt worden waren, bis zum Bundestag vorgedrungen waren. Hier zeigt sich, wie schlecht die interne Kommunikation der Behörden funktioniert. Ein Fehler, der dem Bundestag teuer zu stehen kam.
Der Datenverkehr des Bundestags wurde als Sicherheitsmaßname sogar über das Netz des IVBB gesendet, da dieser über eine Filterliste mit bekannten Servern verfügt, welche geblockt werden.[159] Es ist zu bemängeln, das es kein automatischer Datenabgleich der sicherheitsrelevanten Informationen zwischen dem Netz des IVBBs, BSIs und des Bundestags existiert. Des Weiteren ist zu bemängeln, dass der Bundestag nicht über den selben simplen Sicherheitsmechanismus wie das IVBB-Netz verfügt. Die Installation eines solchen „Mechanismus“, wie er vom Bundestag genannt wird, ist sowohl simpel als auch effektiv und die Daten ließen sich in kurzer Zeit mehrmals täglich abgleichen.

Der Bundestag sollte demnach neben dem Ausbau des Netzes auf den aktuellen Stand der Sicherheit auf die Ausbildung ihrer Abgeordneten setzen und regelmäßige

---

[157] Bundestag, Kurzprotokoll der 6. Sitzung der IuK-Kommission (geleaktes Dokument)

[158] Bundestag, Kurzprotokoll der 7. Sitzung der IuK-Kommission (geleaktes Dokument)

[159] Bundestag, Kurzprotokoll der 6. Sitzung der IuK-Kommission (geleaktes Dokument)

Sicherheitstrainings und -seminare durchführen. Diese Seminare und Trainings sollten für die Abgeordneten, vor der Erstnutzung des Netzwerks Pflicht sein. Die größte Lücke ist in diesem System ganz offensichtlich der Mensch. Der Parlakom-Hack ist ein weiteres gutes Beispiel dafür, weshalb es so wichtig ist, dass jeder, der mit dem PC arbeitet, in Social Engineering geschult ist und mit dem verwendeten Medium sicher, bewusst und verantwortungsvoll umgehen kann.

6 Zusammenfassung und Fazit

Cybercrime ist ein Problem des Informationszeitalter, es ist eines der sich am schnellsten entwickelnden und ausbreitenden Kriminalitätsfelder. Das Problem der Cybercrime wird so lange existieren, wie es Computer und digitale Medien gibt. Daher ist es für jeden Nutzer dieser Technologien wichtig, Angriffsflächen zu minimieren und den sicherheitsbewussten Umgang mit diesen Medien zu erlernen. Diese Arbeit stellt eine Informationssammlung dar, die den Nutzern ermöglicht, das Wesen der Cybercrime zu verstehen und zeigt auf, warum es nötig ist, dass jeder bei sich selbst anfangen muss, wenn es um das Thema Sicherheit geht.

Im Kapitel „Cybercrime“ wurde grundlegend die Problematik der Cybercrime erklärt, wie Angreifer vorgehen und wie die Angriffe ablaufen.
Im Kapitel „Social Engineering“ wurde der Ernst der Lage bezüglich Social Engineering in Verbindung mit modernen Cyber-Angriffen dargestellt und das Thema genau betrachtet.
Im Kapitel „Sicherheitsbewusstsein“ wurde dargestellt, warum Sicherheit bewusst wahrgenommen und angewendet, beziehungsweise erlernt werden muss und wie dies gelingen kann.
Das Kapitel „Analyse ausgewählter Beispiele“ diente dazu, den Bezug zu aktuell passierten Ereignissen herzustellen.

All diese Kapitel insgesamt ergeben das Bild, wie Cybercrime wahrgenommen werden muss, um die wachsende Kriminalitätsrate in diesem Bereich auszubremsen. Den Kriminellen darf es nicht so leicht gemacht werden, dass immer mehr ihr „Glück“ in diesem Bereich versuchen und damit die Internetkultur und das Onlineerlebnis zu einer gefährlichen Aufgabe machen. Technologie ist dazu geschaffen, den Menschen zu unterstützen und schwere Aufgaben zu erleichtern, sollte aber nie gedankenlos verwendet werden.
Damit diese Technologie nicht immer den faden Beigeschmack von Gefahr und Paranoia beinhaltet, müssen sich die Nutzer ebenso anpassen, wie die Kriminellen es getan haben. Der Mensch hinter dem Computer ist das System mit den meisten Fehlern. Er lässt sich am einfachsten täuschen und muss daher am meisten an seiner Selbstwahrnehmung und der Bewertung seiner Umwelt arbeiten. Die Umwelt, in der sich ein Nutzer der digitalen Medien und damit des Internets im 21. Jahrhundert bewegt, ist feindlicher geworden. Es ist demnach essentiell, sich mit dem Thema auseinanderzusetzen und dazuzulernen. Ignoranz, Naivität und Stumpfsinn haben in der Welt des Internets keinen Platz mehr, sofern man sich in einem gewissen Maß sicher und frei in der digitalen Welt bewegen möchte. Anwender müssen eine Eigenverantwortung für ihr Handeln übernehmen, denn die Verantwortung für diese Entwicklung tragen nicht alleine die Täter. Sie trifft auch diejenigen, die leichtsinnig genug sind, diesen Tätern alle Tore zu öffnen und sie damit förmlich einladen, weitere Taten zu begehen.

Das Fazit dieser Arbeit ist demnach, dass Cybercrime für Täter unattraktiv gemacht werden muss, damit das Internet und die digitalen Medien wieder sicherer werden kann. Dazu ist es zwingend erforderlich, dass sich die Nutzer mit der Thematik beschäftigen und sich nicht darauf verlassen, dass Programme sicher sind oder die Sicherheit für sie übernehmen. Diese Programme zu überwinden ist das Hauptbetätigungsfeld der Cyberkriminellen und ihre effektivste Schwachstelle ist heute der Nutzer. Solange das Internet von den meisten Nutzern als reines Konsummedium betrachtet wird, für das nichts getan oder erlernt werden muss, wird sich das Problem der Cybercrime nicht lösen. Wie gezeigt wurde, gibt es auch recht einfache Methoden, die allgemeine Sicherheit zu verbessern, die jeder mit wenig Anstrengung nutzen kann. Diese Möglichkeiten zu nutzen, ist das Minimum an eigenem Aufwand, dass von einem Nutzer des Internets erwartet werden darf.

Nur mit der Hilfe aller Nutzer des globalen Netzwerks kann es gelingen, dieses Netzwerk zu einem sicheren Ort zu machen, von dem man lernen kann und das einen positiven Effekt auf die Gesellschaft hat.

Glossar

Das Glossar beinhaltet kurze Erklärungen zu Fachbegriffen, die nicht in der Arbeit erklärt wurden. Es dient der Arbeit rein als Verständnishilfe. Das Glossar soll keine Fachlich umfassenden Informationen liefern, sondern dem IT-Laien das Wort oder den Satzzusammenhang in dem es verwendet wird, verständlich machen.
Leider sind viele einfache Begriffe der IT in keinem offiziellen Lexikon, über ihre reine Wortbedeutung hinausgehendend, definiert. Es müsste demnach auf diverse Drittquellen zurückgegriffen werden, deren Vertrauenswürdigkeit nicht einzuschätzen ist. Daher werden zu den im Glossar erklärten Begriffen keine Quellenangaben gemacht. Die folgenden Definitionen und Erläuterungen der Begriffe entstammen demnach eigenem Wissen, welches wiederum aus dem Studium der IT-Sicherheit an der Hochschule Mittweida stammt.

Administrator:
Ein Administrator ist ein Benutzer eines IT-Systems mit höchsten Rechten. Er kann Rechte an andere Benutzer vergeben oder diese entziehen. Er hat Vollzugriff auf das zugehörige IT-System.

Adware:
Adware ist Software die zusätzlich zu ihrer eigentlichen Funktion, Ads, zu Deutsch Werbung, anzeigt.

AES:
AES ist ein Verschlüsselungsstandard, der von Joan Daemen und Vincent Rijmen entwickelt wurde. AES auch Rijndael-Algorithmus genannt.

Audit:
Ein Audit im eigentlichen Sinne ist ein Verhör oder eine Vernehmung. In der IT meint ein Audit eine Überprüfung der Sicherheitsmaßnahmen in einem Unternehmen. Dabei kann es mit oder ohne Social Engineering ausgeführt werden. Ein Audit mit Social Engineering wird auch Social Engineering Audit genannt, eines ohne wird oft nur als Penetrationstest bezeichnet.

Auditor:
Auditoren werden auch Penetrationstester genannt. Sie sind Sicherheitsexperten, die ein Audit durchführen.

Backdoor:
Eine Backdoor, zu Deutsch „Hintertür“, bezeichnet einen, vom Nutzer eines Systems oft nicht gewollten, meist von Angreifern hinterlassenen, Zugang zu einem System.

BackTrack:
BackTrack ist eine Linux-Distribution, also ein Betriebssystem auf der Basis von Linux. BackTrack ist auf Penetrationstests spezialisiert und mit diversen Tools zum Eindringen in Computer ausgestattet. BackTrack wird aktuell nicht mehr von den Entwicklern weiterentwickelt.

Bitcoin:
Bitcoin ist eine nicht zurückverfolgbare, digitale Währung. Die Transaktionen der Währung sind Kryptographisch abgesichert, weshalb diese Art von Währungen auch Kryptowährungen heißen.

Bugs:
Bugs sind Fehler in Software die ungewolltes Programmverhalten zur Folge haben.

Chimäre:
Eine Chimäre ist eine Kreuzung zwischen verschiedenen Computer-Schadware-Arten. Beispielsweise wie der Wannacry-Krypto-Trojaner, der neben den Eigenschaften eines Trojaners auch die Eigenschaften eines Wurms besitzt.

Cybercrime-as-a-Service:
Cybercrime-as-a-Service, bedeutet, dass Cybercrime als Dienst~~,~~ gegen Geld~~,~~ angeboten wird.

Darknet:
Das Darknet ist ein Bereich des Internets der über Peer-to-Peer Verbindungen funktioniert. Das bedeutet, dass Verbindungen gezielt und über mehrere andere Verbindungsteilnehmer aufgenommen werden müssen. Dabei funktionieren die Verbindungen verschlüsselt und IP-Adressen werden verschleiert. Als Ergebnis surfen die Nutzer des Darknets sehr anonym und haben Zugriff auf Websites die dem restlichen Netz verborgen bleiben.

Datamining:
Datamining bedeutet, mit Methoden der Mathematik, Informationen aus großen Datenmengen zu extrahieren, die aus dem Zusammenhang und der Abhängigkeit der Daten entstehen und nicht trivial zu entdecken sind.

Domain:
Eine Domain ist ein Teilbereich eines Domain Name Systems, kurz DNS. Als Domain werden oft die Endungen der ausgeschriebenen Internetadressen im Freien Internet bezeichnet. Bekannte Top-Level-Domains sind zum Beispiel: .de .com .org .net .gov

Domäne:
Eine Domäne ist ein abgegrenzter Teilbereich eines Netzwerks. Unter Domäne versteht man häufig, im Gegensatz zur Domain, ein Abgegrenztes Netzwerk, welches meist in einem LAN existiert und das von einem oder mehreren Lokalen Servern Verwaltet wird.

Dumbster-Dive:
Als Dumbster-Dive wird der Vorgang des „Abtauchens“ in eine Mülltonne, zwecks der Informationsgewinnung beschrieben.

Extended-Validation-SSL-Zertifikate:
Sind streng geprüfte Zertifikate zur Verifizierung eines Kommunikationspartners. Sie dienen der Absicherung der Integrität einer Verbindung.

Flash:
Flash oder auch Flashplayer oder Adobe Flash ist eine Schnittstelle über die Animationen in Websites eingebunden werden können.

Framework:
Framework bedeutet wörtlich übersetzt Rahmenstruktur und bezeichnet in der IT „Gerüste“ für verschiedenste Anwendungsfälle.

Gehärtete Systeme:
Ein gehärtetes System beschreibt in der IT ein System, welches nur mit den nötigsten und vertrauenswürdigsten Programmen und Diensten Ausgestattet ist. Dabei werden alle überflüssigen Dienste deaktiviert, blockiert oder zugriffsbeschränkt.

Gerichteter Angriff:
Ein gerichteter Angriff bezeichnet einen Angriff, der sich gegen ein definiertes Ziel richtet. Meist eine einzelne Person oder Personengruppe oder ein einzelner Rechner oder Rechnernetzwerk.

IDS (Intrusion Detektion System):
Ein IDS ist ein automatisiertes System, welches nach festgelegten Regeln, Angriffe selbstständig identifizieren und melden kann.

IPS (Intrusion Prevention System):
Ein IPS kann zusätzlich zum IDS die identifizierten Angriffe nach einem festen Regelwerk verhindern.

Javascript:
Javascript ist eine Scriptsprache auf der Basis der Programmiersprache JAVA, welche den Funktionsumfang von Websites erweitert. Mit ihr können beispielsweise dynamische Inhalte und Animationen angezeigt werden.

KALI-Linux:
KALI-Linux ist, wie BackTrack, eine Linux-Distribution, also ein Betriebssystem auf der Basis von Linux. KALI-Linux ist ebenfalls auf Penetrationstests spezialisiert und mit diversen Tools zum Eindringen in Computer ausgestattet. KALI-Linux wird aktuell noch weiterentwickelt.

Keylogger:
Ein Keylogger ist eine Software, die unbemerkt vom Benutzer, alle Eingaben der Tastatur mitschneidet.

Kontrakt:
Ein Kontrakt ist eine schriftliche, rechtsgültig bindende Vereinbarung.

LAN:
LAN bedeutet zu Deutsch „Lokales Netz“ und bezeichnet ein meist privates Netzwerk von Computern die untereinander verbunden sind. Ein LAN wird typischerweise von jedem Privatbenutzer Zuhause benutzt und durch den Router verwaltet.

Mehrfaktorautorisierung:
Mehrfaktorautorisierung bezeichnet eine Autorisierung eines Benutzers über mehrere Faktoren, beispielsweise Passwort und Bestätigungs-SMS.

Metasploit Framework:
Das Metasploit Framework ist eine Sammlung von Tools zum Überprüfen der Sicherheit von Computernetzwerken.

Nerd:
Nerd ist eine gängige Bezeichnung für Personen mit einer starken Affinität zu einem bestimmten Themengebiet, die durch die ständige Auseinandersetzung mit diesem Gebiet, besonders großes Wissen anhäufen, aber gleichzeitig oft soziale Defizite entwickeln.

Netzwerksniffer:
Ein Netzwerksniffer, auch Sniffer genannt, ist ein Tool mit dem der gesamte zu Verfügung stehende Netzwerkverkehr mitgeschnitten werden kann.

Payload:
Die Payload bezeichnet eigentlich allgemein eine Nutzlast. In der IT-Sicherheit bezeichnet es in Bezug auf Schadware, den Teil einer Schadware, der mit der eigentlichen Funktion bestückt ist.

Phishing-Website:
Eine Website zum Ausführen von Phishing-Angriffen.

Polizeiliche Kriminalstatistik:
Ist die Statistik aller bei der Polizei angezeigten Straftaten der Vergangenen Jahre.

Portscanner:
Ein Portscanner durchsucht die Ports eines Computers nach laufenden Diensten und versucht diese zu identifizieren.

Pranking:
Eine oft gemeine oder erniedrigende Form von streichen, die häufig an Schulen vorkommt. Es ist oder ähnelt oft Mobbing.

Proxy oder Proxy-Server:
Ein Proxy oder Proxyserver bezeichnet eine Kommunikationsschnittstelle eines Netzwerks, über welche die Daten an einen anderen Kommunikationspartner übertragen werden. In der IT-Sicherheit wird der Begriff oft in Verbindung mit Computern gebraucht, die dazu genutzt werden Informationen zu einem anderen Computer zu übertragen ohne, dass die beiden Endpunkte der Kommunikation direkt miteinander kommunizieren müssen. Dadurch kann zum Beispiel die IP-Adresse eines Computers verschleiert werden.

Schlagschlüssel:
Ein Schlagschlüssel bezeichnet einen Schlüssel, der meist regelmäßig geformt ist und zum Öffnen von Schlössern benutzt werden kann. Dabei wird der „Universalschlüssel“ in das Schloss eingeführt, unter einen gewissen Druck gesetzt und es wird mit einer Art Hammer auf ihn geschlagen. Bei mehrfacher Anwendung verkanten sich so die Stifte des Schlosses nach und nach und das Schloss öffnet sich.

Script:
Ein Script bezeichnet im allgemeinen eine Vorlage oder ein Handlungsschema. Es kann beispielsweise einen Handlungsablauf grob beschreiben. In der IT beschreibt ein Script eine automatisch ablaufende Abfolge von Befehlen zwecks der Automatisierung bestimmter Aktionen.

Social Engineer:
Als Social Engineer wird jeder Anwender von gezieltem Social Engineering bezeichnet.

Ungerichteter Angriff:
Ein Ungerichteter Angriff zielt nicht auf ein Bestimmtes Ziel. Er wird ähnlich einer Falle ausgelegt oder wahllos bei diversen Opfern ausprobiert, bis er funktioniert.

Virtual Private Network:
Ein Virtual Private Network oder auch VPN ist ein geschlossenes Kommunikationsnetzwerk. Dadurch kann LAN über das Internet realisiert werden oder der gesamte Datenverkehr verschlüsselt über einen anderen Rechner laufen. Dadurch ist jeder Datenverkehr in das Internet vom LAN aus nur noch verschlüsselt zu sehen.

Workflow:
Workflow bedeutet Arbeitsfluss.

Index

Literatur

Alan E. Kazdin,. *History of behavior modification: Experimental foundations of.* Baltimore: University Park Press, 1978.

Allan Liska, Timothy Gallo. *Ransomware: Defending Against Digital Extortion.* United States of America: O'Reilly Verlag, 2016.

Anna Biselli. „Netzpolitik.org: Wir veröffentlichen Dokumente zum Bundestagshack: Wie man die Abgeordneten im Unklaren ließ.“ 07. 03 2016. https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestagshack-wie-man-die-abgeordneten-im-unklaren-liess/ (Zugriff am 26. 07 2017).

Armin Medosch. „Heise online: The Kids are out to play.“ 14. 06 2001. https://www.heise.de/tp/features/The-Kids-are-out-to-play-3449304.html (Zugriff am 28. 07 2017).

Who am I - Kein System ist Sicher. Regie: Baran bo Odar. Interpret: Baran bo Odar, Jantje Friese. 2014 (Film).

BasKet. kein Datum. www.basket.kde.org (Zugriff am 21. 08 2017).

Bernd Kling. *ZDNet: WannaCry: Experten raten von Lösegeldzahlung ab.* 15. 05 2017. http://www.zdnet.de/88296517/wannacry-experten-raten-von-loesegeldzahlung-ab/ (Zugriff am 25. 07 2017).

Boris Gröndahl. *Hacker.* Rotbuch : Europäische Verlagsanstalt, 2000.

Bundesamt für Sicherheit in der Informationstechnik (BSI). „Die Lage der IT-Sicherheit in Deutschland 2005.“ 07 2005. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/lagebericht2005_pdf.pdf?__blob=publicationFile&v=1 (Zugriff am 21. 06 2017).

—. „Die Lage der IT-Sicherheit in Deutschland 2014.“ 11 2014. https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html (Zugriff am 30. 06 2017).

—. *Die Lage der IT-Sicherheit in Deutschland 2016.* 10 2016. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?__blob=publicationFile&v=5 (Zugriff am 23. 06 2017).

—. „Einführung von Intrusion-Detection-Systemen.“ 31. 10 2002. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/IDS/Leitfadenv10_pdf.pdf?__blob=publicationFile&v=2 (Zugriff am 23. 07 2017).

—. „Glossar der Cyber-Sicherheit.“ kein Datum. https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/cyberglossar_node.html (Zugriff am 23. 07 2017).

—. „Schädliche Werbebanner in großem Umfang zur Verbreitung von Schadprogrammen mittels Drive-by-Exploits genutzt.“ 18. 01 2013. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/Schaedliche_Werbebanner_18012013.html (Zugriff am 23. 07 2017).

—. „Studie - Durchführungskonzept für Penetrationstests.“ 11 2003. https://www.internet-sicherheit.de/fileadmin/docs/downloads/andere_studien_dokumente/BSI/2003-11_penetrationstest.pdf (Zugriff am 17. 04 2016).

Bundeskriminalamt (BK) Österreich. „Cybercrime Österreich Jahresbericht 2015.“ 2015. http://www.bmi.gv.at/cms/BK/publikationen/files/30102016_Cybercrime_2015.pdf (Zugriff am 06. 07 2017).

Bundeskriminalamt (BKA) - Michael Kraus, Kriminaloberrat. „Vortrag Bekämpfung der Cybercrime aus Sicht des BKA.“ 09. 10 2014. https://www.bafin.de/SharedDocs/Downloads/DE/Veranstaltung/dl_141009_it_sicherheit_vortrag_kraus_cybercrime.pdf?__blob=publicationFile&v=1 (Zugriff am 2017. 07 05).

Bundeskriminalamt (BKA). „Bundeslagebild Cybercrime 2014.“ 2014. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2014.html (Zugriff am 15. 06 2017).

—. „Internetkriminalität / Cybercrime.“ 28. 05 2016. https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html (Zugriff am 27. 04 2017).

Chaos Computer Club (CCC). „Chaos Computer Club: Hackerethik.“ kein Datum. https://www.ccc.de/de/hackerethik (Zugriff am 28. 07 2017).

—. „Chaos Computer Club: Home.“ kein Datum. https://www.ccc.de/de/ (Zugriff am 27. 07 2017).

Chris Hoffman. *How-To Geek: Hacker Hat Colors Explained: Black Hats, White Hats, and Gray Hats.* 20. 04 2013. https://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/ (Zugriff am 14. 07 2017).

Christopher Hadnagy. *Die Kunst des Human Hacking.* 2. Auflage. Rheinbreibach: mitp Verlag, 2011.

D. C. Balmund. „Kommunikationsmodell." In *Die Kunst des Human Hacking*, von Christopher Hadnagy, 74. Rheinbreitbach: mitp Verlag, 2011.

David Bisson. *Tripwire: 5 Social Engineering Attacks to Watch Out For.* 23. 03 2015. https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/ (Zugriff am 13. 07 2017).

David Glance. *The Conversation: WannaCry hackers had no intention of giving users their files back even if they paid.* 15. 05 2017. http://theconversation.com/wannacry-hackers-had-no-intention-of-giving-users-their-files-back-even-if-they-paid-77751 (Zugriff am 25. 07 2017).

Deutschen Instituts für Wirtschaftsforschung (DIW). „Tatort Internet: Kriminalität verursacht Bürgern Schäden in Milliardenhöhe." *DIW Wochenbericht Nr. 12.2015.* 23. 03 2015. https://www.diw.de/documents/publikationen/73/diw_01.c.498298.de/15-12-6.pdf (Zugriff am 25. 06 2017).

Deutsches Institur für Vertrauen und Sicherheit im Internet (DIVSI). *PRISM und die Folgen: Sicherheitsgefühl im Internet verschlechtert.* 03. 07 2013. https://www.divsi.de/prism-und-die-folgen-sicherheitsgefuehl-im-internet-verschlechtert/ (Zugriff am 25. 06 2017).

Dr. Eggert Winter . *Gabler Wirtschafstlexikon.* kein Datum. http://wirtschaftslexikon.gabler.de/Definition/bundeshaushalt.html (Zugriff am 14. 08 2017).

Dr. Häger. „Netzpolitik.org: Wir veröffentlichen Dokumente zum Bundestagshack: Wie man die Abgeordneten im Unklaren ließ." *Abschnitt: Informationen zum Cyberangriff auf den Bundestag – hier: Abschlussbericht BSI.* 03. 11 2015. https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestagshack-wie-man-die-abgeordneten-im-unklaren-liess/#abschlussbericht_bsi_20151103 (Zugriff am 26. 07 2017).

Dradis. kein Datum. www.dradisframework.com (Zugriff am 21. 08 2017).

ECO - Der Verband der deutschen Internetwirtschaft e. V. „botfrei.de Jahresstatistik 2015: Zahl der Zombierechner weiter bedrohlich." 15. 02 2016.

https://www.eco.de/2016/pressemeldungen/botfrei-de-jahresstatistik-2015-zahl-der-zombierechner-weiter-bedrohlich.html (Zugriff am 10. 06 2017).

Fabian A. Scherschel. *Heise Security: The Fappening: Promi-Nacktfotos über Find My iPhone aus der Cloud gesaugt.* 01. 09 2014. https://www.heise.de/security/meldung/The-Fappening-Promi-Nacktfotos-ueber-Find-My-iPhone-aus-der-Cloud-gesaugt-2305588.html (Zugriff am 24. 07 2017).

Gephi. kein Datum. www.gephi.com (Zugriff am 21. 08 2017).

Hasso Plattner Institut - Digital Engineering Universität Podsdam (HIP). „Pressemitteilung: Die Top Ten deutscher Passwörter." 21. 12 2016. https://hpi.de/pressemitteilungen/2016/die-top-ten-deutscher-passwoerter.html (Zugriff am 09. 07 2017).

Heise online. *Glossar - Man-in-the-Middle-Angriff (MITM).* kein Datum. https://www.heise.de/glossar/entry/Man-in-the-Middle-Angriff-399039.html (Zugriff am 13. 07 2017).

Houghton Mifflin. *Dictionary.com: Moore's Law.* kein Datum. http://www.dictionary.com/browse/density (Zugriff am 14. 08 2017).

Institute of Directors (IoD) - James Sproule, Chief Economist and Director of Policy. „Institute of Directors." 03. 03 2016. https://www.iod.com/Portals/0/Badges/PDF's/News%20and%20Campaigns/Infrastructure/Cyber%20security%20underpinning%20the%20digital%20economy.pdf?ver=2016-04-14-101230-913 (Zugriff am 05. 07 2017).

Intersperience. *Intersperience: PRESS RELEASE: Majority of Brits feel 'upset' without Internet connection.* 22. 07 2011. http://www.intersperience.com/news_more.asp?news_id=39 (Zugriff am 16. 07 2017).

ITWissen.info, Technologiewissen Online. kein Datum. http://www.itwissen.info/Woerterbuchangriff-dictionary-attack.html (Zugriff am 21. 08 2017).

Jacquelynne Eccles. „Maryland Adolescent Development In Context Study (MADICS): Newsletter Spring 2007." 2007. http://www.rcgd.isr.umich.edu/pgc/newsletters/spring2007.pdf (Zugriff am 2017. 08 2017).

Joseph Ansanelli. „Consumer Data Security Survey Highlights." Harris Interactive Service Bureau and Vontu Inc. 24. 06 2013.

http://financialservices.house.gov/media/pdf/062403ja.pdf (Zugriff am 20. 06 2017).

Judith Horchert. *Spiegel online: "WannaCry"-Erpresser betteln um Lösegeld.* 19. 05 2017. http://www.spiegel.de/netzwelt/web/wannacry-erpresser-werben-um-loesegeldzahlung-bei-opfern-a-1148398.html (Zugriff am 25. 07 2017).

Karl Popper. *The Open Society and its Enemies.* Routledge, 2012 (Erstpublikation 1945).

Konrad Duden. *Duden.* Mannheim: Bibliographisches Institut Mannheim, 2017.

Landeskriminalamt Niedersachsen (LKA). „Dunkelfeldstudie - Befragung zu Sicherheit und Kriminalität in Niedersachsen.“ 08 2013. http://www.lka.niedersachsen.de/download/72346/Abschlussbericht_Dunkelfeldstudie.pdf (Zugriff am 27. 06 2017).

Levy, Steven. *Hackers: Heroes of the Computer Revolution.* Penguin Verlag, 1984.

Maik Baumgärtner, Sven Röbel und Jörg Schindler. „Spiegel onlne: Ermittler vermuten Geheimdienst hinter Cyberangriff.“ 20. 05 2015. http://www.spiegel.de/netzwelt/netzpolitik/bundestag-ermittler-vermuten-geheimdienst-hinter-cyberangriff-a-1034790.html (Zugriff am 26. 07 2017).

Maik Baumgärtner, Sven Röbel und Wolf Wiedmann-Schmidt. „Spiegel online: Hacker kopierten Abgeordneten-E-Mails.“ 18. 06 2015. http://www.spiegel.de/politik/deutschland/cyberangriff-auf-bundestag-abgeordneten-e-mails-erbeutet-a-1039388.html (Zugriff am 26. 07 2017).

Maltego. kein Datum. www.paterva.com (Zugriff am 21. 08 2017).

MalwareInt . „MalwareInt: Botnet Tracker - WCRYPT.“ 2017. https://intel.malwaretech.com/botnet/wcrypt/?t=24h&bid=all (Zugriff am 27. 07 2017).

Martin Holland, Axel Kannenberg. *Heise online: WannaCry: Angriff mit Ransomware legt weltweit Zehntausende Rechner lahm.* 12. 05 2017. https://www.heise.de/newsticker/meldung/WannaCry-Angriff-mit-Ransomware-legt-weltweit-Zehntausende-Rechner-lahm-3713235.html (Zugriff am 25. 07 2017).

Matt Suiche. *comae technologies: WannaCry—Decrypting files with WanaKiwi + Demos.* 18. 05 2017. https://blog.comae.io/wannacry-decrypting-files-with-wanakiwi-demo-86bafb81112d?gi=3643e886cc81 (Zugriff am 25. 07 2017).

Michael Link. *Heise online: Ransomware WannaCry: Sicherheitsexperte findet "Kill-Switch" – durch Zufall.* 13. 05 2017.

https://www.heise.de/newsticker/meldung/Ransomware-WannaCry-Sicherheitsexperte-findet-Kill-Switch-durch-Zufall-3713420.html (Zugriff am 25. 07 2017).

Microsoft. *Microsoft: Am 14. Juli 2015 wurde der erweiterte Support für Windows Server 2003 eingestellt.* 2015. https://www.microsoft.com/de-de/cloud-platform/windows-server-2003 (Zugriff am 25. 07 2017).

—. *Microsoft: Ende des Supports für Windows XP.* 2014. https://www.microsoft.com/de-de/windowsforbusiness/end-of-xp-support (Zugriff am 25. 07 2017).

—. „Microsoft: Windows XP Is Here!“ 25. 10 2001. https://news.microsoft.com/2001/10/25/windows-xp-is-here/ (Zugriff am 27. 07 2017).

„Netzpolitik.org: Wir veröffentlichen Dokumente zum Bundestagshack: Wie man die Abgeordneten im Unklaren ließ.“ *Abschnitt: Kurzprotokoll der 8. Sitzung der IuK-Kommission.* 02. 07 2015. https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestagshack-wie-man-die-abgeordneten-im-unklaren-liess/#protokoll_iuk_6_20150512 (Zugriff am 26. 07 2017).

„Netzpolitik.org: Wir veröffentlichen Dokumente zum Bundestagshack: Wie man die Abgeordneten im Unklaren ließ.“ *Abschnitt: Kurzprotokoll der 7. Sitzung der IuK-Kommission.* 11. 06 2015. https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestagshack-wie-man-die-abgeordneten-im-unklaren-liess/#protokoll_iuk_7_20150611 (Zugriff am 26. 07 2017).

Norton by Symantec - Norton_Team. „Was ist Social Engineering?“ 15. 12 2015. https://de.norton.com/norton-blog/2015/12/was_ist_social_engin.html (Zugriff am 10. 07 2017).

Ole Reißmann. *Spiegel online: Apple geht Hinweis auf iCloud-Hackerangriff nach.* 02. 09 2014. http://www.spiegel.de/netzwelt/web/icloud-apple-geht-hinweis-auf-angriff-nach-a-989343.html (Zugriff am 21. 08 2017).

Piyush Michael. *Quora: Does Moore's law apply to GPUs? Or only CPUs?* 13. 07 2016. https://www.quora.com/Does-Moores-law-apply-to-GPUs-Or-only-CPUs (Zugriff am 11. 08 2017).

Prof. (FH) Mag. Dr. Helmut Siller, MSc. *Gabler WIrtschaftslexikon Stichwort: Trojaner.* kein Datum. http://wirtschaftslexikon.gabler.de/Definition/trojaner.html (Zugriff am 13. 07 2017).

—. *Gabler Wirtschaftslexikon Stichwort: Virus.* kein Datum. http://wirtschaftslexikon.gabler.de/Definition/virus.html (Zugriff am 13. 07 2017).

—. *Gabler WIrtschaftslexikon: Sniffer.* kein Datum. http://wirtschaftslexikon.gabler.de/Definition/sniffer.html (Zugriff am 23. 07 2017).

—. *Gabler WIrtschaftslexikon: Wurm.* kein Datum. http://wirtschaftslexikon.gabler.de/Definition/wurm.html (Zugriff am 13. 07 2017).

Quelle: fsi. *Frankfurter Allgemeine (FAZ): Hacker veröffentlicht Nacktbilder Wie sicher sind meine Fotos in der Cloud?* 01. 09 2014. http://www.faz.net/aktuell/gesellschaft/hacker-veroeffentlicht-nacktbilder-wie-sicher-sind-meine-fotos-in-der-cloud-13129733.html (Zugriff am 24. 07 2017).

Random House (Ursprünglich: Jess M Stein). *The Random House Dictionary.* Ballantine Books, 2001.

Rapidminer. kein Datum. www.rapidminer.com (Zugriff am 21. 08 2017).

Robert B. Zajonc. „The attitudinal effects of mere exposure.“ 09 1965. http://www.psc.isr.umich.edu/dis/infoserv/isrpub/pdf/Theattitudinaleffects_2360_.PDF (Zugriff am 11. 07 2017).

Ron Bowes. *Skull Security: Passwords.* kein Datum. http://downloads.skullsecurity.org/passwords/rockyou.txt.bz2 (Zugriff am 24. 07 2017).

Sascha Mattke. *Heise Technology Review: Passwort gegen Schokolade.* 28. 06 2016. https://www.heise.de/tr/artikel/Passwort-gegen-Schokolade-3245447.html (Zugriff am 13. 07 2017).

Semper Video. *Youtube: Nacktbilder in der Cloud.* 02. 09 2014. https://www.youtube.com/watch?v=uwBRbbr6W5w&t=336s (Zugriff am 24. 07 2017).

Sigmund Freud. *Kleine Schriften I.* 1913.

Statista. „Marktanteile der führenden Betriebssysteme in Deutschland von Januar 2009 bis Mai 2017.“ 05 2017. https://de.statista.com/statistik/daten/studie/158102/umfrage/marktanteile-von-betriebssystemen-in-deutschland-seit-2009/ (Zugriff am 26. 06 2017).

Timeline of Computer History. kein Datum. http://www.computerhistory.org/timeline/ (Zugriff am 14. 08 2017).

Volker Briegleb. *Heise online: WannaCry: Was wir bisher über die Ransomware-Attacke wissen.* 13. 05 2017. https://www.heise.de/newsticker/meldung/WannaCry-Was-

wir-bisher-ueber-die-Ransomware-Attacke-wissen-3713502.html (Zugriff am 25. 07 2017).

ZEIT ONLINE, dpa, Reuters, AFP, sre. *Zeit Online: Ransomware erbeutet weniger als 70.000 Dollar Lösegeld.* 15. 05 2017. http://www.zeit.de/digital/internet/2017-05/wannacry-ransomware-cyberattacke-bitcoin-windows-microsoft-europol (Zugriff am 10. 08 2017).

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Mittweida, den 25.08.2017

Daniel Meerwald