F A C H H O C H S C H U L E W E D E L

S E M I N A R A R B E I T

in der Fachrichtung
Wirtschaftsingenieurwesen

mit dem Schwerpunkt
IT-Management

Sommersemester 2018

Thema:

Kryptoparty: Ricochet-Instant Messenger

Eingereicht von:	Deniz Ural 103337 (Matrikelnr.) Ebereschenweg 40 22850 Norderstedt Tel.: 040 / 5240442 E-Mail: deniz_ural@web.de
Erarbeitet im:	02. Fachsemester
Abgabetermin:	07.07.2018
Referent (FH Wedel):	Prof. Dr. Michael Anders Fachhochschule Wedel Feldstraße 143 22880 Wedel Tel.: (04103) 8048-24 E-Mail: an@fh-wedel.de

Eidesstattliche Erklärung

Ich erkläre hiermit an Eides statt, dass ich die vorliegende Arbeit selbstständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungskommission vorgelegt und auch nicht veröffentlicht.

Ort, Datum Unterschrift (Vor-und Nachname)

Inhaltsverzeichnis

1 Einleitung

Das Internet wird heutzutage in nahezu allen Lebensbereichen der Menschen ausgiebig genutzt. Es ermöglicht uns ständig erreichbar zu sein, Erlebnisse mit Freunden auf sozialen Netzwerken zu teilen und bietet uns eine unendliche Informationsvielfalt. Für viele ist das Internet und sein weitreichendes Angebot daher nicht mehr aus dem Alltag wegzudenken. Dabei drängt sich die Nutzung des Internets durch die Digitalisierung in Form der Industrie 4.0 auch in der Wirtschaft gleichermaßen in den Vordergrund. Digitale Vernetzung in der Produktion, bei Dienstleistungen und in der staatlichen Infrastruktur werden in der Zukunft höchste Relevanz aufweisen. Vor allem Global Player setzen vermehrt auf eine intelligente High-Tech-Vernetzung. Seit Herbst 2016 produziert Adidas beispielweise individuell auf den Kundenwunsch zugeschnittene Sportschuhe in einer sogenannten Speedfactory, welche hauptsächlich von Robotern betrieben wird und vollautomatisch funktioniert. Hiermit sollen wochenlange Wartezeiten zukünftig auf Tage oder wenige Stunden reduziert und vor allem Kosten gespart werden.[1] Neben der Wirtschaft revolutioniert die Digitalisierung allerdings auch andere Bereiche wie das Gesundheitswesen, indem beispielweise elektronische Patientendaten, Behandlungsmethoden und Therapien schneller untereinander kommuniziert werden können.[2]

Diese Beispiele zeigen die Vorteile und den Mehrwert der Digitalisierung und somit der Nutzung des Internets auf. Gleichzeitig bedarf es der Auseinandersetzung mit Aspekten der Sicherheit im Allgemeinen und der Datensicherheit im Besonderen. Viele Kritiker kreieren Szenarien des gläsernen Bürgers in Verbindung mit einer negativ empfundenen Überwachung von Seiten des Staates. Oftmals werden hierbei die Theorien „George Orwells“ zur Veranschaulichung und als Zukunftsszenario beschrieben. Über diese allgemeinen, gesellschaftlichen, kritischen Aspekte hinaus spielt der Schutz persönlicher Daten eine immer größer werdende Rolle. Gerade jüngste Skandale, wie zum Beispiel die durch Edward Snowden offengelegten Überwachungsmechanismen der NSA und die Zusammenarbeit von Facebook mit dem Analyseunternehmen Data Analytics im US-Wahlkampf zwischen Donald Trump und Hillary Clinton[3] haben bei vielen Menschen das

[1] (Weitzenbürger, 2016)
[2] (Unbekannt, PWC, 2018)
[3] (Voss, 2018)

Bewusstsein für Datensicherheit geweckt. Dieses Bewusstsein sehen viele Unternehmen mittlerweile sowohl als Chance als auch Herausforderung. So hat Apple bereits den Schutz der Daten als wesentlichen Marktvorteil erkannt und nutzt mittlerweile offensiv dessen Vermarktungspotenzial, indem Kunden zukünftig die über sie gespeicherten Daten einsehen können.[4] Auch Facebook kann sich der Relevanz des Schutzes persönlicher Daten nicht mehr entziehen. Der Gründer und CEO Mark Zuckerberg musste erst kürzlich sowohl vor dem US-Kongress als auch dem Europäischen Parlament zum Umgang persönlicher Daten innerhalb seines Konzerns Stellung beziehen. Demnach waren jahrelang persönliche Daten von mehr als drei Millionen Facebook-Nutzern öffentlich zugänglich, welche zuvor durch die App „myPersonality“ der Universität Cambridge gesammelt wurden.[5] Viele Beobachter und Experten, aber auch Politiker zeigten sich enttäuscht und skeptisch bezüglich der Aus- und Zusagen Zuckerbergs. Die schiere Anzahl der jüngsten Datenskandale ist ein Beleg angebrachter Skepsis. Daher sehen sich viele Internetnutzer aufgrund des Vertrauensverlusts gegenüber den großen Technologiekonzernen zum Selbstschutz verpflichtet. Zur Wahrung der Privatsphäre und insbesondere des Schutzes persönlicher Daten gewinnen technologische Lösungen, die Datensicherheit bzw. Anonymität im Internet versprechen, zunehmend an Bedeutung.

Viele Nutzer erkennen insbesondere in der persönlichen Kommunikation die Schutzbedürftigkeit ihrer Daten. Gängige Kommunikationsprogramme wie WhatsApp oder Telegram bieten bereits heute eine End-to-End Verschlüsselung.[6] Doch gerade WhatsApp, dass zum Facebook Konzern gehört, hat in Person von Mark Zuckerberg die Verknüpfung von WhatsApp- und Facebook-Daten zugegeben. Dabei wird vielfach auf die Existenz von sogenannten Schattenprofilen verwiesen. Hierbei handelt es sich um Profile für Menschen, die zwar nicht aktiv Facebook nutzen, jedoch automatisch durch das Unternehmen aufgrund von Datengenerierung über andere Plattformen oder der Profile von Freunden und Familien angelegte Profile (Schattenprofile) in diesen Netzwerken existieren. Es ist demnach äußerst fragwürdig, warum ein solches Interesse bei den verantwortlichen Unternehmen besteht und ferner, ob Konzerne wie Facebook überhaupt vertraulich mit unseren sensiblen Daten umgehen. Insbesondere wenn diese ohne unser Wissen

[4] (Warnecke, 2018)
[5] (Berger, 2018)
[6] (Whatsapp.com, kein Datum)

zusammengetragen wurden. Demnach suchen datenschutzorientierte Internetnutzer vermehrt nach Alternativen, um die gängigen Kommunikationsprogramme zu umgehen.

Ein Hilfsmittel hierbei bietet das Tor-Netzwerk, welches ein Netzwerk zur Anonymisierung von Verbindungsdaten darstellt und die IP-Adresse des Nutzers über mehrere Umwege verschleiert. Diese Technologie wird unter anderem durch den Instant Messenger Ricochet genutzt, welcher zum Erhalt der Privatsphäre einen metadatenfreien Chat ermöglicht und Nutzer somit anonym im Internet surfen können. Diese Seminararbeit befasst sich somit mit den technischen Grundzügen sowie ihrer Bedeutung für datensichere Kommunikation mit dem Ricochet Instant Messenger.

2 Ricochet Instant Messenger

Der Ricochet Instant Messenger (ehemals: Torsion) ist ein frei lizensiertes, plattformübergreifendes Kommunikationsprogramm, dessen Hauptmerkmal in der metadatenfreien Konzeption liegt.[7] Dabei handelt es sich um eine Weiterentwicklung des TorChat, welcher ebenfalls die Technik der Tor-Hidden-Services nutzt und sich noch im Alpha-Stadium befindet.[8] Die Konfiguration der Hidden-Services erfolgt dabei automatisch und es ist keine weitere Installation des Tor-Browsers notwendig. Ricochet kann zudem nach der Installation ohne weitere Konfigurationen verwendet werden und besitzt in Verbindung mit dem Betriebssystem Tails eine portable Lösung, welche an nahe jedem Computer dieser Welt ausgeführt werden kann.

Die Metadatenfreiheit dient den Entwicklern als Abgrenzungsmerkmal zu gängigen Kommunikationsprogrammen wie WhatsApp und Telegram und ermöglicht ihrer Intention nach den Erhalt und Schutz der Privatsphäre durch Anonymität. Beruhend auf der Tor-Technik verzichtet Ricochet auf den Austausch von Metadaten mit Servern und der Verbindung zu diesen. Durch die lokale Ausführung und Anwendung auf dem Computer des Nutzers ermöglicht die Software eine Kommunikation und Datenverbindung innerhalb des Netzwerkes, bei denen die Teilnehmer direkt miteinander verknüpft sind und Daten nicht über einen Zwischenserver geleitet werden. Der Informationsaustausch erfolgt demnach direkt von Computer zu Computer. Daher spricht man auch von einem dezentralen Netzwerk, dem sogenannten Peer-to-Peer-Netzwerk.[9] Die Identifizierung der Anwender innerhalb der Software erfolgt über einen automatisch generierten Nutzernamen. Für einen Transfer von Dateien kann als Ergänzung das Tool OnionShare genutzt werden, da Ricochet bislang lediglich einen anonymen Chat zur Verfügung stellt.

[7] (Unbekannt, Wikipedia, 2018)
[8] (Unbekannt, Privacy Handbuch, 2018)
[9] (Unbekannt, XOVI Handbuch, 2018)

2.1 Aspekte zum Schutz der Privatsphäre

Der Begriff der Anonymität, der der Intention des Ricochet IM zugrunde liegt, beruht auf der Tatsache, dass im Rahmen der Kommunikation die Identität des Nutzers nicht offegelegt wird – weder Dritten gegenüber noch dem Absender und Empfänger von versendeten Nachrichten.[10] Wie bereits zuvor erwähnt findet die Identifizierung der Nutzer innerhalb der Softwareumgebung gesprächsspezifisch über einen automatisch generierten Nicknamen statt. Parallel hierzu muss eine Nachverfolgbarkeit und der Zugang zu den Kommunikationsinhalten verhindert werden. Diesem Aspekt entspricht die Software durch eine kryptische Verschlüsselung, die ein nachträgliches Auslesen und somit auch Ändern der Kommunikation ähnlich der Blockchain-Technologie verhindert. Sämtliche Kommunikationsinhalte werden daher nach Beendigung des Programmes unwiederbringlich gelöscht.[11] Des Weiteren verzichtet die Software wie einleitend erwähnt auf die Erhebung und Verarbeitung von Metadaten. Bei Metadaten handelt es sich um die strukturierte Allokation von Informationen zur Beschreibung von bereits existierenden Daten. Hierbei handelt es sich zumeist um die durch Softwareprogramme generierten statistischen Informationen, wie zum Beispiel das Datum und die Zeit der Erstellung bzw. Modifikation von Daten und ihres Erstellers, welche oftmals im Hintergrund von Anwendungen ausgeführt werden. Im Prinzip handelt es sich bei Metadaten daher um Daten über andere Daten.[12] Die Intention der Ricochet Software schließt daher bereits im Ansatz die Erhebung und Verarbeitung von Metadaten aus. Die ebenfalls zuvor erwähnte Peer-to-Peer Kommunikation gewährleistet darüber hinaus, dass keinerlei Datenverkehr das zugrundeliegende Netzwerk verlässt.

2.2 Relevante Sicherheitsaspekte bei der Nutzung von Ricochet IM

Wie für sämtliche Softwareanwendungen beginnt auch bei der Nutzung von Ricochet die Sicherheit bereits beim Anwender. Bereits infiltrierte Systeme setzen hierbei sämtliche Sicherheitslösungen der Software außer Gefecht. Daher gilt es bereits den Zugang zu diesen Systemen, insbesondere unter dem Aspekt des fehlenden, passwortgeschützten Logins in der Anwendung von Ricochet zu schützen. Des Weiteren sollte man sich nicht

[10] (Michael G. Reed, 1998)
[11] (Rakan Alkhulaiwi, 2016)
[12] (Tanner, 2010)

ausschließlich auf den Schutz durch die Software verlassen, sondern ebenfalls der eigenen Verantwortung im Umgang mit Viren- und Malwareschutz nachkommen. Hierzu gehört auch die Tatsache, dass die Nutzung von Ricochet lediglich die Kommunikation schützt. Doch Datensicherheit betrifft auch die Überwachung des Surfverhaltens durch Cookies, dem Anlegen von Such- und Bewegungsprofilen bis hin zur Ausspähung des Privatlebens. Schutz hierbei bietet lediglich die konsequente, system- und anwendungsübergreifende Nutzung von Softwarelösungen wie Ricochet sowie den richtigen Umgang mit ihnen. Alles in Allem bietet der Messenger jedoch einen guten Schutz innerhalb der Softwareumgebung und erfüllt somit die an ihn gestellten Forderungen.

2.3 Geschichte

Im Juni 2014 wurde der Ricochet Instant Messenger, welcher ehemals unter dem Namen Torsion Instant Messenger bekannt war, umbenannt. Knapp einen Monat später veröffentlichte Kim Zetter einen Artikel im Wired Magazine, in dem sie von der zukünftigen Zusammenarbeit der Invisible.im-Gruppe sowie John Brooks berichtete. Der damalige Artikel enthielt außerdem Aussagen über die Zukunftspläne der neu geschlossenen Partnerschaft. Und zwar sollten zukünftig auch Dateitransfers möglich sein, sowie eine Neugestaltung des Protokolls vorgenommen werden. Diese Neugestaltung wurden dann im April 2015 umgesetzt. Der Transfer von Dateien ist bis dato weiterhin nicht möglich.

Im Februar 2016 haben die Ricochet-Entwickler ein Sicherheits-Audit ins Leben gerufen. Dieses Audit wurde von dem Open Technology Fund, einem von der US-Regierung ins Leben gerufene Programm zur Unterstützung von Technologien der Internetfreiheit und von der NCC-Gruppe durchgeführt. Bei der NCC-Gruppe handelt es sich um ein britisches Cyberunternehmen. Das Audit verlief relativ positiv, identifizierte jedoch mehrere Verbesserungsbereiche und eine Schwachstelle, welche die Anonymität von Nutzern gefährden könnte. Gemäß John Brooks sind diese Sicherheitslücken im letzten Update am 07. November 2016 behoben wurden. Bei der aktuellen Version handelt es sich um die Version 1.1.4. Seitdem gab es keine Softwareänderungen mehr.[13]

[13] (Unbekannt, Wikipedia, 2018)

2.4 Installationsbeschreibung und Einrichtung

Der Download und die Installation von Ricochet ist sehr simpel. Es folgt nun eine schrittweise Anleitung zur Installation des Messengers.

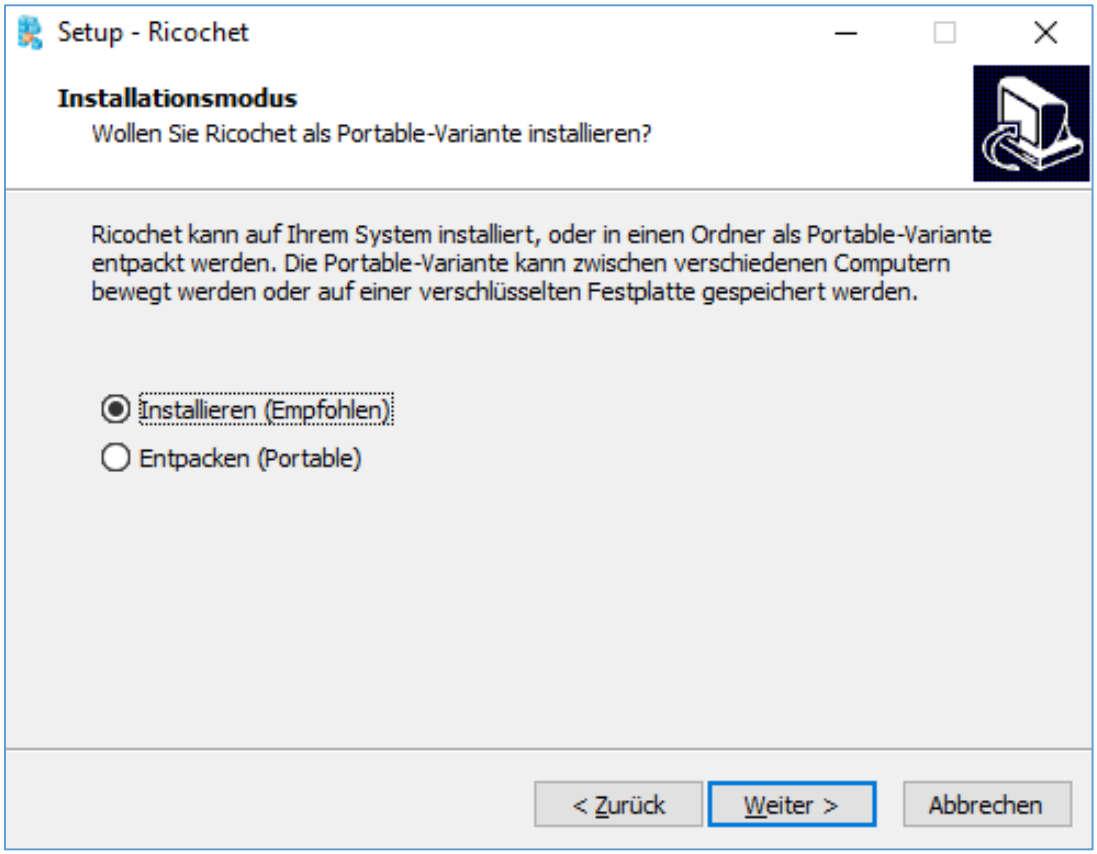
1. **Download des Ricochet Instant Messengers**
   Das Programm ist auf der Projektseite (https://ricochet.im/) jeweils für Windows, MacOS oder Linux verfügbar und muss heruntergeladen werden. Aus Sicherheitsgründen sollte hierfür keine alternative Website genutzt werden.

2. **Starten der Installation**
   Beim Öffnen der heruntergeladenen Datei erscheint folgendes Fenster. Hier sollte selbstverständlich der Installationsanweisung gefolgt werden indem man „Weiter“ drückt.

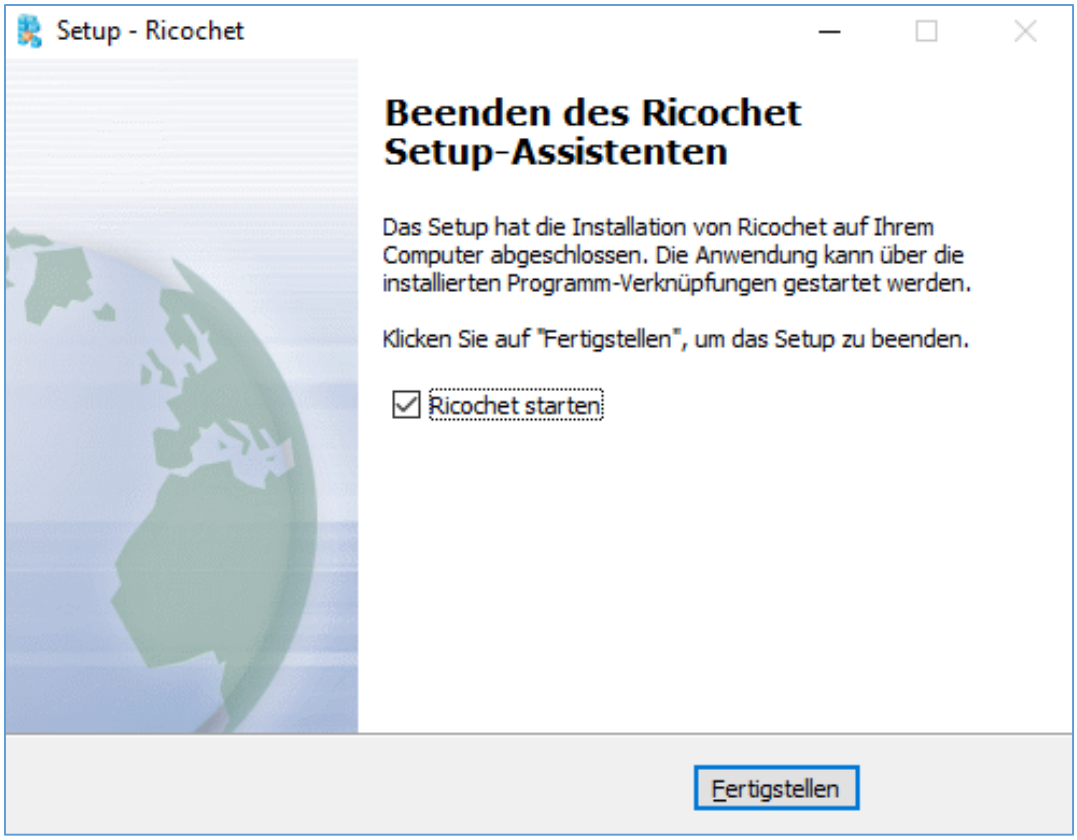
Anschließend kann man den gewünschten Installationsmodus auswählen. Hierbei bietet das Programm uns zwei unterschiedliche Varianten an:

a) **Installieren:** Installation der Software auf herkömmlichen Computern. Diese Variante ist die bequemere für den alltäglichen Gebrauch.
b) **Entpacken(Portable):** In Verbindung mit dem Betriebssystem Tails, kann Ricochet auf einem USB-Stick oder einer DVD installiert werden. Hierdurch wird ein Zugriff auf nahezu jedem USB-fähigen Computer ermöglicht. Dieser USB-Stick sollte selbstverständlich geheim gehalten, sowie zusätzlich passwortgeschützt werden, da Ricochet keine eigene passwortgeschützte Login-Funktion besitzt und Offline-Nachrichten durch manuellen physischen Zugang abgefangen werden könnten.

In diesem Installationsbeispiel wird die empfohlene Installation dargestellt. Durch Klicken auf „Weiter“ kann anschließend die Installation starten.

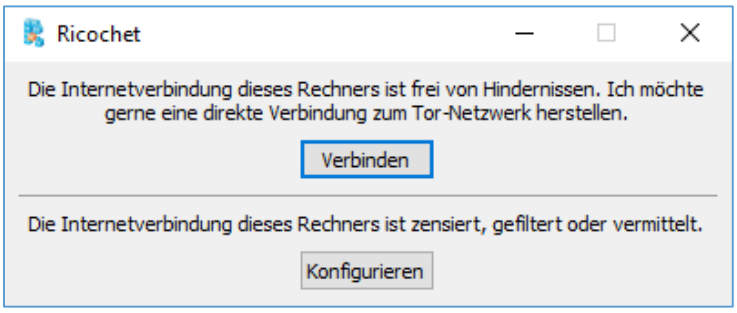


Nachdem die Installation abgeschlossen ist, muss anschließend noch auf „Fertigstellen“ gedrückt werden. Die Software bietet hier die Möglichkeit per Hakensetzung das Programm direkt zu starten.

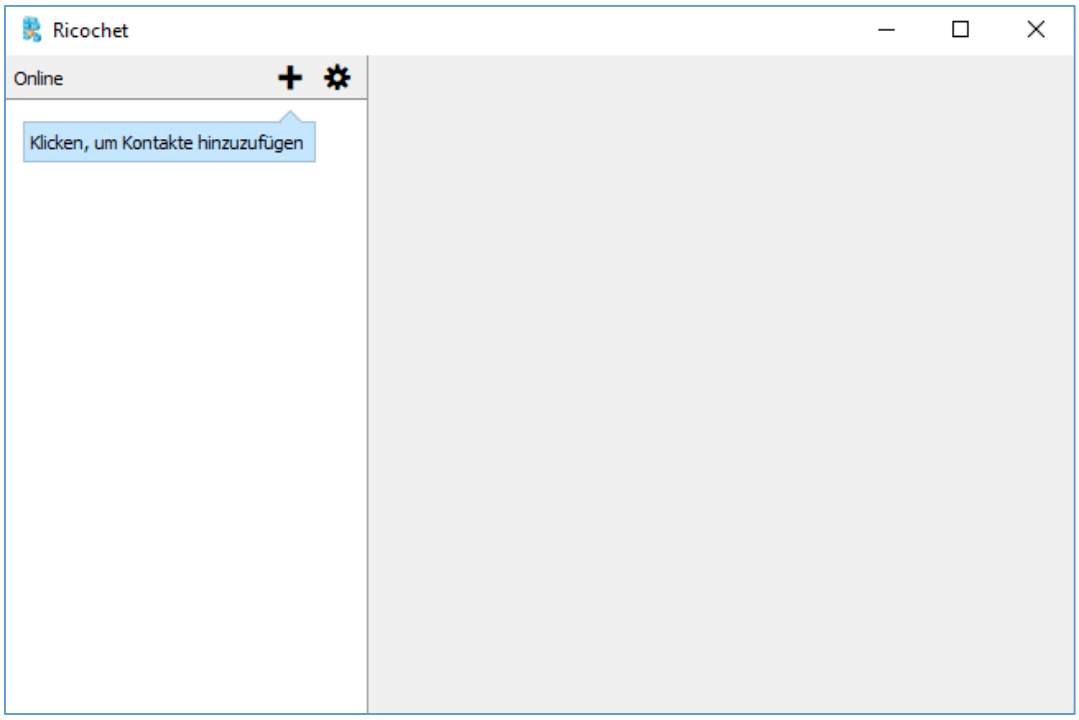


3. Starten des Ricochet Messengers

Beim ersten Start des Ricochet Messenger öffnet sich ein Fenster, in dem bei Bedarf einige Änderungen in den Einstellungen vorgenommen werden können. Wir entscheiden uns für die direkte Variante und stellen eine Verbindung zum Tor-Netzwerk her. Für diese Nutzung ist es nicht notwendig, dass der Tor-Browser auf dem jeweiligen Computer installiert ist, da ein Tor-Daemon im Hintergrund gestartet wird.

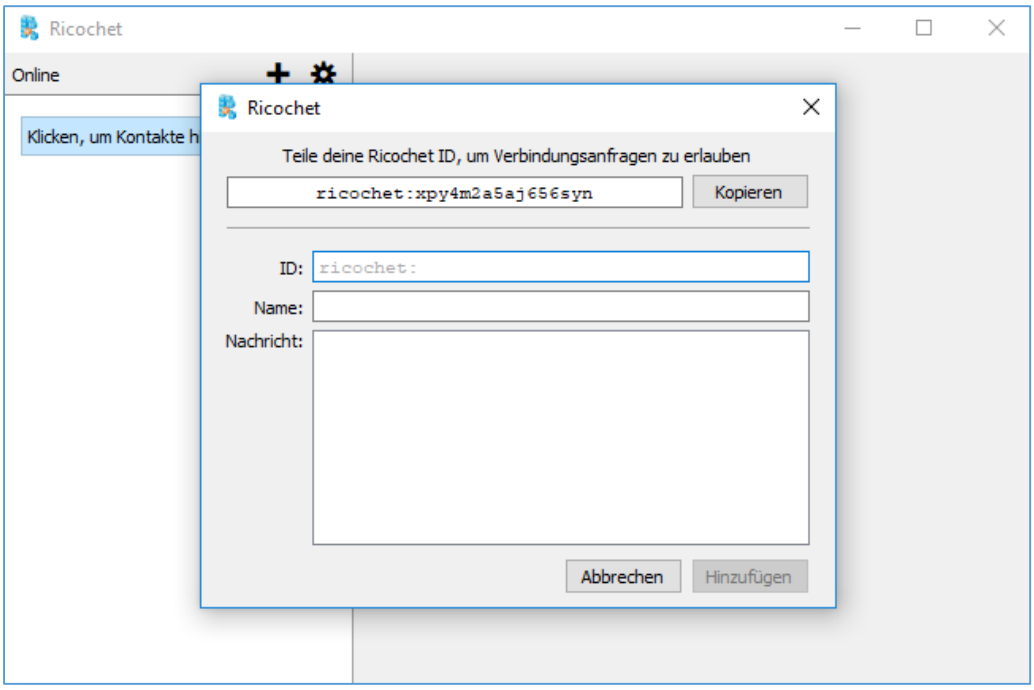


Nachdem eine Verbindung mit dem Tor-Netzwerk hergestellt wurde, öffnet sich Ricochet automatisch und kann nun genutzt werden.

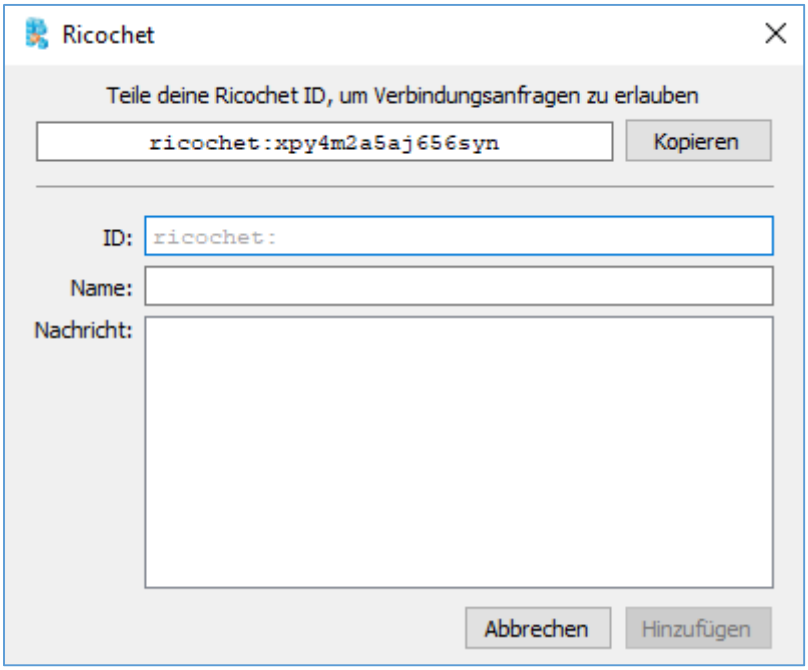


4. Hinzufügen von Kontakten

Zum Hinzufügen von Kontakten muss zunächst auf das in der oben gezeigten Grafik vorhandene Pluszeichen geklickt werden. Anschließend erscheint folgendes Fenster:



In der oberen Zeile befindet sich die eigene Ricochet-ID: (ricochet:xpy4m2a5aj656syn) Sie ist wie alle anderen nach dem gleichen Schema aufgebaut, beginnend mit einem „ricochet:“ am Anfang und einer zufälligen Kette aus Buchstaben und Zahlen.



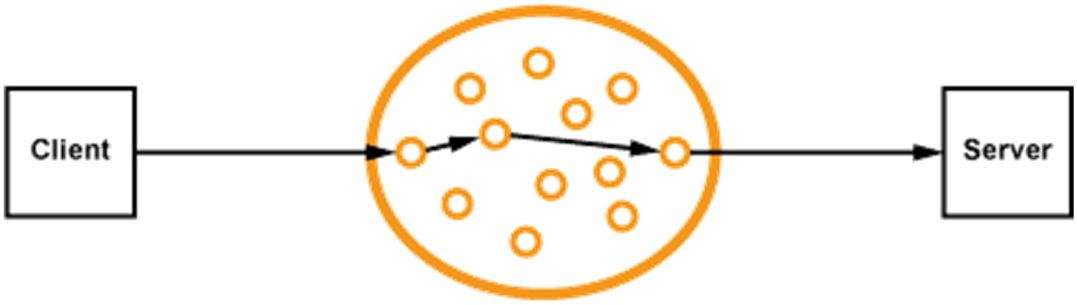
Möchte man nun einen Kontakt hinzufügen, muss zuvor irgendwie ein anonymer Austausch der eigenen bzw. der ID der Kontaktperson stattfinden. Die wohl sicherste Variante bietet hierbei wohl ein persönliches Treffen. Anschließend können sich die Parteien wie bei bereits bekannten Chatprogrammen gegenseitig hinzufügen. Für die Kontaktperson kann dabei ein Name ausgewählt, sowie eine Nachricht ähnlich einer Freundschaftsanfrage bei sozialen Netzwerken hinterlassen werden. Sobald der Kontakt hinzugefügt wurde, kann man anfangen zu chatten. Hierbei haben die Hersteller auf jegliche Extras verzichtet. Es ist lediglich möglich Textnachrichten zu verfassen und es können weder Dateien versendet, noch Emojis genutzt werden.

3 Das Tor-Netzwerk (The Onion Routing)

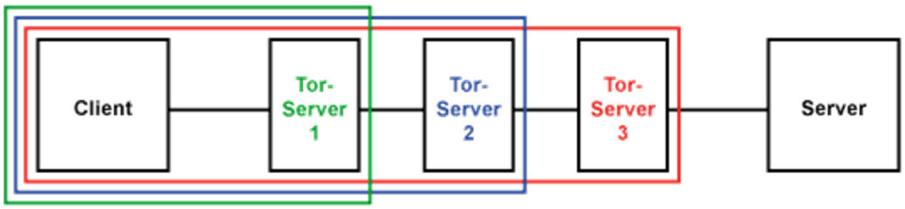
Tor oder auch The Onion Router, bezeichnet ein Netzwerk, welches für die Anonymisierung von Verbindungs- und Transferdaten verwendet wird und durch Verschleierung der ursprünglichen IP-Adresse eine anonyme Internetnutzung seiner Anwender ermöglichen soll.[14] Im folgenden Kapitel gehe ich näher auf die Funktionsweise, sowie die von Tor angebotenen Hidden-Services ein.

3.1 Funktionsweise

Prinzipiell handelt es sich bei dem Tor-Netzwerk um eine Sammlung von verschiedenen Servern, welche weltweit verstreut sind und zusammen das Tor-Netzwerk bilden. Dieses Netzwerk anonymisiert die eingehende IP-Adresse, da diese während eines Datenaustausches über drei verschiedene Knotenpunkte innerhalb des Tor-Netzwerkes verschleiert wird. Es ist somit nicht möglich als Empfänger der Daten den Absender anhand seiner IP-Adresse zu identifizieren. Die Software basiert dabei grundsätzlich auf der Annahme, dass ausspionierende Unternehmen und Regierungen nicht in der Lage dazu sind, das gesamte Internet zu überwachen. Je mehr Server aus unterschiedlichen Regionen sich somit im Tor-Netzwerk befinden, desto mehr Sicherheit bietet das Tor-Netzwerk. Selbstverständlich muss passend hierzu eine ausreichende Menge an Daten verschickt werden, da große Datenmengen verwirren und eine Rückverfolgung erschweren. Die verwendete Route während der Nutzung von Tor wird dabei zufällig gebildet und soll eine Zuordnung ein- und ausgehender Daten verhindern.

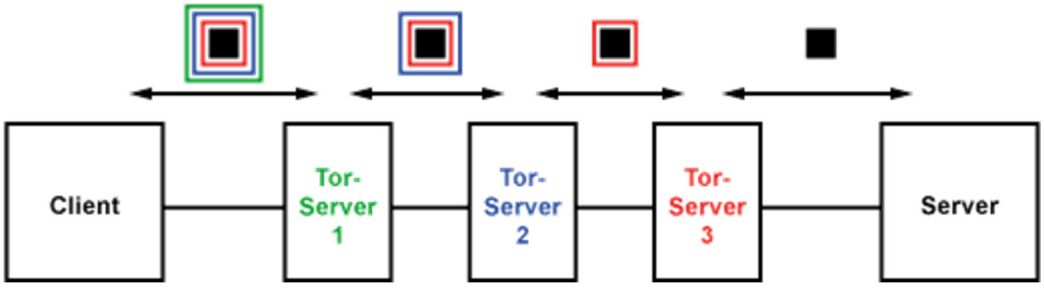


[14] (Golem.de, 2018)



Verschlüsselung nach dem Zwiebel-Prinzip

Der Tor-Client vereinbart nacheinander mit den 3 Tor-Servern jeweils eine eigene verschlüsselte Verbindung für jedes Datenpaket bzw. jede Zwischenstation innerhalb des Tor-Netzwerkes. Die Daten werden dabei in umgekehrter Reihenfolge, beginnend mit der Exit-Note (3. Tor-Server), über den 2. Tor-Server zum Entry-Guard (1. Tor-Server) verschlüsselt. Die oben gezeigte Abbildung soll dies nochmal verdeutlichen.



Anhand dieses Prinzips entschlüsselt jeder Tor-Server sein empfangenes Datenpaket und reicht es an den nächsten Server weiter. Hierbei ist jedem Tor-Server jeweils nur der nächstfolgende Tor-Server bzw. Identität bekannt. Jeder weitere Server lässt sich jedoch nicht mehr weiter nachverfolgen. Am Ende der Route entfernt der 3. Tor-Server seine Verschlüsselung und reicht die gesendeten Daten an den Ziel-Server weiter. Aufgrund dieser komplizierten Verschachtelung und Verschleierung ist die Internetverbindung über das Tor-Netzwerk deutlich langsamer als herkömmliche Browseraktivitäten. Je nach erzeugter Verbindung sind Dienste wie Streaming oder Gaming nicht möglich. Diese zufällige Route wird ferner sogar alle zehn Minuten erneuert um die Anonymisierung zusätzlich zu steigern.[15]

[15] (Unbekannt, Elektronik Kompendium, 2018)

3.2 Tor-Hidden-Serivces

Das Tor-Netzwerk bietet darüber hinaus die Nutzung der sogenannten Hidden-Services an. Hierbei handelt es sich um die Erstellung einer sogenannten Special-Use-Top-Level-Domain, welche ausschließlich innerhalb des Tor-Netzwerkes sichtbar ist[16] und sich nicht über herkömmliche Browser wie zum Beispiel Google Chrome oder Firefox erreichen lässt. Die Besonderheit der Hidden-Services beruht dabei auf den nicht zu ermittelnden Standorten bzw. Betreibern dieser Dienste, aufgrund der Anonymisierung durch die Tor-Technologie. Grundsätzlich erfolgt der Kontakt mit einem anderen Nutzer innerhalb des Tor-Netzwerkes über einen sogenannten „Meeting-Point“. Hierdurch wird ermöglicht, dass jeder Anwender innerhalb des Netzwerkes nur jeweils seinen nächsten Nachbarn kennt und die versendeten Daten selbst nicht mitlesen kann.[17]

Selbstverständlich machen sich auch Kriminelle diese Eigenschaften zu Nutze und missbrauchen die Tor-Dienste für illegale Aktivitäten. Mit ausreichender Suchbereitschaft ist es möglich, diverse Waffen, Drogen, Auftragsmörder oder gefälschte Dokumente problemlos über die temporär zur Verfügung gestellten Onion-Links zu finden und per Kryptowährung anonym zu bezahlen. Hierbei sollte nicht außer Acht gelassen werden, dass die einzelnen Adressen innerhalb des Tor-Netzwerkes kein Vertrauens- oder Reputationsmodell besitzen und die Betreiber somit nur schwer verifizierbar sind. Es besteht daher die Gefahr sogenannter „Honeypots“. Hierbei handelt es sich um Fake-Seiten, welche darauf abzielen, Information seiner Besucher bis hin zu Login-Daten zu erschnüffeln.[18] Gemäß Juha Nurmi, einem Betreiber der Hidden-Service-Suchmaschine Ahmia.fi, sind zum Teil hunderte Fake-Onion-Seiten in Betrieb, welche bereits bekannten bzw. originalen Adressen zum Verwechseln ähnlich sehen. Neben Ahmia.fi ist auch DuckDuckGo, die wohl bekannteste Suchmaschine innerhalb des Tor-Browsers davon betroffen gewesen.[19]

[16] (WikipediaOnion, kein Datum)
[17] (Schmidt, 2016)
[18] (Richard, 2018)
[19] (Unbekannt, PrivacyHandbuch, Unbekannt)

4 Betriebssystem Tails

Tails ist ein auf Debian bzw. Linux basiertes, frei verfügbares Live-Betriebssystem, welches über einen Computer mittels einer DVD oder einem USB-Stick gestartet werden kann und darauf abzielt, die Privatsphäre und Anonymität seiner Anwender zu bewahren. Es kann unabhängig von dem auf dem Computer installierten Betriebssystem genutzt werden und ermöglicht seinen Nutzern somit, nahezu jeden Computer dieser Welt anonym nutzen zu können, ohne dabei Spuren zu hinterlassen.[20] Das Betriebssystem beinhaltet verschiedene hinsichtlich der Sicherheit konfigurierte, mitgelieferte Programme, wie den Tor-Browser, einen Instant-Messaging-Client, ein-Email-Programm, ein Office-Paket, sowie einen Bild- und Audioeditor.[21] Des Weiteren lassen sich in Tails verschiedene Sprachen auswählen und die Benutzeroberfläche optisch an bereits bekannte Betriebssysteme, wie zum Beispiel Windows anpassen. Hiermit wird direkt eine gewohnte Arbeitsumgebung geschaffen.

4.1 Systemvoraussetzungen

Tails läuft prinzipiell auf jedem vergleichsweise aktuellen Computer, welcher nicht älter als zehn Jahre ist und folgende Voraussetzungen erfüllt:

- USB-Port oder internes/externes DVD-Laufwerk
- 2 GB Arbeitsspeicher
- Auf x86-64-Architektur basierter Prozessor[22]

Für die Installation wird benötigt:

- 2 Speichermedien (USB/DVD) mit mindestens 8GB Speicher
- 2 Stunden Wartezeit (Installation)
- 2 Computer (Installation / Befolgung weiterer Schritte)[23]

Es sei außerdem erwähnt, dass es derzeit nicht möglich ist, Tails direkt von Windows aus zu installieren. Hierzu muss zusätzlich ein zweiter USB-Stick mit einer vorübergehenden Tails-Version eingerichtet werden.

[20] (Tails, The amnesic incognito live system, 2018)
[21] (Darknetguide, 2018)
[22] (Tails, Tails Systemvoraussetzungen, 2018)
[23] (Darknetguide, 2018)

4.2 Sicherheitswarnungen

Neben den nützlichen Eigenschaften des Betriebssystems gibt es auch einige vom Hersteller erwähnte Sicherheitswarnungen, welche im Folgenden näher erläutert werden.

Demnach schützt Tails nicht vor kompromittierter Hardware, wie beispielweise einem Key-Logger und sollte daher nur vorsichtig an fremden Computern verwendet werden. Es schützt ebenfalls nicht vor BIOS-, Firmware- oder Man-in-the-middle-Angriffen und macht in gewissen Situationen auch sichtbar, dass Tor bzw. Tails genutzt wird (z.B. durch einen Systemadministrator). Theoretisch ist es ebenfalls möglich, Daten über ein Tor-Ausgangsrelais abzufangen, insbesondere da die Dokumente nicht standardmäßig verschlüsselt werden und auch Metadaten nicht automatisch gelöscht werden. Das Betriebssystem befindet sich außerdem dauerhaft in Bearbeitung und wird stets weiterentwickelt. Hierbei verweist der Hersteller sogar darauf, dass Programmfehler und Sicherheitslücken existieren können.[24]

[24] (Tails, kein Datum)

5 Zusammenfassung und Ausblick

Zusammenfassend lässt sich sagen, dass der Ricochet Instant Messenger sich aufgrund seiner Eigenschaften durchaus als gute Alternative für die anonyme Kommunikation eignet. Zwar ist die Nutzung des Messengers weniger praktikabel als z.B. ein Smartphone, jedoch wird dieses Maß an Anonymität im Internet von keinem anderen Messenger gewährleistet. Für die Zukunft wäre daher wohl eine mobile sowie passwortgeschützte Version von Ricochet sehr interessant für seine bisherigen Nutzer, vor allem um die Nutzung besser in das alltägliche Leben integrieren zu können.

Wie bereits zuvor erwähnt sollte trotzdem darauf verzichten werden, der Ricochet-Software bzw. anderen Softwares uneingeschränkt zu vertrauen. Vielmehr sollte man sich ganzheitlich über Schutzmaßnahmen im Internet informieren und diese so weit wie möglich umsetzen. Insbesondere Regierungsbehörden und Geheimdienste versuchen seit Jahren die Anonymität der Tor-Nutzer aufzuheben. Zwar waren bisherige Angriffe nicht erfolgreich, können jedoch in der Zukunft nicht ausgeschlossen werden. Hierbei sei nochmals erwähnt, dass auch während der Entwicklung von Ricochet bzw. während des im Jahre 2016 durchgeführten Sicherheitsaudits ebenfalls Regierungsbehörden und Unternehmen vertreten waren. Hierbei stellt sich natürlich die Frage, warum eine Behörde bei der Entwicklung eines medadatenfreien Chats mitwirkt, obwohl dieser vor allem innerhalb eines neuen Whistleblowing-Skandals gegen sie verwendet werden könnte. Die Vermutung liegt daher nahe, dass diese Regierungsbehörden an eventuellen Sicherheitslücken und Informationsvorsprüngen interessiert waren und daher an der Entwicklung teilgenommen haben.

Gemäß John Brooks soll Ricochet das Vertrauen in sichere Kommunikation stärken. Sobald man sich jedoch bereits auf dem Schirm der Geheimdienste befindet, ist man den ermittelnden Behörden praktisch schutzlos ausgeliefert, da diese über unvorstellbare Ressourcen verfügen. Ein 100-prozentiger Datenschutz kann daher nur durch das Zusammenspiel der Nutzer durch konsequentes Verhalten und einer vertrauensvollen Regierung gesichert werden.

Literaturverzeichnis

Onlinemedien:

Allgöwer, D. M. (10. Juni 2018). *IT-Zoom*. Von IT-Zoom: https://www.it-zoom.de/it-director/e/predictive-analytics-im-us-wahlkampf-12711/ abgerufen

Berger, D. (15. Mai 2018). *Heise*. Von Heise: https://www.heise.de/newsticker/meldung/Facebook-Neues-Datenleck-betrifft-3-Millionen-Nutzer-4049832.html abgerufen

Darknetguide. (7. Juni 2018). *Darknetguide*. Von Darknetguide: http://darknetguide.de/tails-usb.html abgerufen

Golem.de. (31. Mai 2018). *Golem.de*. Abgerufen am 31. Mai 2018 von https://www.golem.de/specials/tor-netzwerk/

Holland, M. (19. Januar 2017). *HeiseOnline*. Von HeiseOnline: https://www.heise.de/newsticker/meldung/NSA-Ausschuss-Facebook-Microsoft-Google-und-Apple-verweigern-Aussage-3602858.hmtl abgerufen

Michael G. Reed, P. S. (4. Mai 1998). *Michigan Technical University*. Von Michigan Technical University: http://www.csl.mtu.edu/cs6461/www/Reading/08/Reed-jsac98.pdf abgerufen

Rakan Alkhulaiwi, A. S. (12-14. Dezember 2016). *IEEE Xplore Digital Libary*. Von IEEE Xplore Digital Libary: https://ieeexplore.ieee.org/document/7906977/ abgerufen

Rotter, D. (8. September 2014). *sein.de*. Von sein.de: https://www.sein.de/die-kriegs-luegen-das-einfache-schema-der-manipulation/ abgerufen

Savkovic, B. (10. Juni 2018). *Mathworks*. Von Mathworks: https://de.mathworks.com/discovery/predictive-analytics.html abgerufen

Statista. (11. Juni 2018). *Statista*. Von Statista: https://de.statista.com/statistik/daten/studie/252278/umfrage/prognose-zur-zahl-der-taeglich-versendeter-e-mails-weltweit/ abgerufen

Tails. (kein Datum). Von Tails: https://tails.boum.org/doc/about/warning/index.de.html abgerufen

Tails. (7. Juni 2018). *Tails Systemvoraussetzungen*. Von Tails Systemvoraussetzungen: https://tails.boum.org/doc/about/requirements/index.de.html abgerufen

Tails. (7. Juni 2018). *The amnesic incognito live system*. Von The amnesic incognito live system: https://tails.boum.org/about/index.de.html abgerufen

Tanner, A. L. (2010). *Metadata: Why the Fuss? A White Paper on Metadata.* Bloomberg Law Reports.

Unbekannt. (14. Juni 2018). *Elektronik Kompendium*. Von Elektronik Kompendium: https://www.elektronik-kompendium.de/sites/net/1809171.htm abgerufen

Unbekannt. (13. Juni 2018). *Privacy Handbuch*. Von Privacy Handbuch: https://www.privacy-handbuch.de/handbuch_24u.htm abgerufen

Unbekannt. (14. Juni 2018). *PWC*. Von PWC: https://www.pwc.de/de/gesundheitswesen-und-pharma/digitalisierung-im-gesundheitswesen.html abgerufen

Unbekannt. (8. Juni 2018). *Wikipedia*. Von Wikipedia: https://en.wikipedia.org/wiki/Ricochet_(software) abgerufen

Unbekannt. (12. Mai 2018). *Wikipedia*. Von Wikipedia: https://en.wikipedia.org/wiki/Ricochet_(software) abgerufen

Unbekannt. (8. Juni 2018). *XOVI Handbuch*. Von XOVI Handbuch: https://www.xovi.de/wiki/Peer-to-Peer abgerufen

Voss, O. (19. März 2018). *Tagesspiegel*. Von Tagesspiegel: https://www.tagesspiegel.de/wirtschaft/cambridge-analytica-facebook-daten-illegal-fuer-trump-wahlkampf-genutzt/21088976.html abgerufen

Warnecke, A. (5. Mai 2018). *Frankfurter Rundschau*. Von Frankfurter Rundschau: http://www.fr.de/leben/computer_internet/news/datenschutz-verordnung-apple-macht-gespeicherte-daten-einsehbar-a-1511183 abgerufen

Weitzenbürger, G. (4. Oktober 2016). *Süddeutsche*. Von Süddeutsche: http://www.sueddeutsche.de/bayern/adidas-schuh-revolution-1.3189991 abgerufen

Whatsapp.com. (kein Datum). Von Whatsapp.com: https://faq.whatsapp.com/de/android/28030015/?category=5245250 abgerufen

Wietlisbach, O. (30. 11 2017). *Watson*. Von Watson: https://www.watson.ch/digital/native/865689393-was-google-facebook-instagram-und-snapchat-von-dir-wissen-die-laaaaange-liste abgerufen