Anonymität im Netz - Ein Ding der Unmöglichkeit?

Dimitri Graf und Timo Furrer
BMI4A
Jutta Lücking
Interdisziplinäre Projektarbeit
GIBZ Zug

April 2014

Inhaltsverzeichnis

Zusammenfassung

In Laufe dieser Arbeit wollten wir herausfinden, ob es möglich ist, sich im Netz Anonymität zu schaffen und welche Mittel dazu benötigt werden. Welches Know-How braucht es dazu? Lohnt sich der Aufwand? Wo lauern überhaupt die Gefahren?

Um diese Fragen zu beantworten, setzten wir uns mit drei Anwendungen auseinander, die heute Teil des täglichen Lebens sind: E-Mail-Verkehr, Surfen im Internet, Einsatz der Cloud. Parallel zu der theoretischen Abhandlung haben wir zudem Experimente mit Technologien durchgeführt, die diese Anwendung sicherer bzw. anonymer machen. Die Experimente wurden in Form von Handbüchern dokumentiert und sollen Interessierten die Möglichkeit bieten, diese Techniken selbst auszuprobieren.

Die Auseinandersetzung mit den Anwendungen und die Experimente haben gezeigt, dass es grundsätzlich möglich ist, sich Privatsphäre im Netz zu verschaffen. Es zeigte sich aber auch, dass es immer eine Frage des persönlichen Ehrgeizes und der Prioritäten ist. Letztendlich liegt es am Benutzer, sich für seine Privatsphäre einzusetzen.

1 Formelle Hinweise

1.1 Quellen

Im Zuge dieser Arbeit haben wir vorwiegend auf Quellen aus dem World Wide Web zurückgegriffen. Gerade Online-Enzyklopädien geniessen noch immer nicht den selben seriösen Ruf wie gedruckte Fachliteratur und das teils auch zu Recht. Sie werden aber auch oft unterschätzt. Wikipedia zum Beispiel hat inzwischen einen hohen Qualitätsgrad erreicht und ist, was seine Grösse und Abdeckung angeht, kaum zu übertreffen. Auch was unsere restlichen Quellen betrifft - Internetseiten, PDFs, News-Artikel - haben wir unser Wissen fast ausschliesslich online bezogen. Einerseits ist dies unsere Art zu arbeiten. Andererseits sahen wir uns aber auch gezwungen, so und nicht anders vorzugehen. Denn in der IT-Welt ist das, was heute noch aktuell ist, morgen schon wieder von vorgestern. Fachbücher zu den von uns behandelten Themen sind daher meist nicht mehr auf dem aktuellen Stand oder gar nicht erst vorhanden. Wir führen diese Erklärung an dieser Stelle auf, um den Leser auf diese Umstände aufmerksam zu machen und ein gewisses Mass an Verständnis zu erzeugen. Nicht zuletzt wollen wir auch erreichen, dass das Internet als Quelle des Wissens grössere Akzeptanz findet.

1.2 Aufbau

Dieses Dokument stellt den Kern unserer Arbeit dar. Es beinhaltet die theoretische Abhandlung zur Fragestellung *Anonymität im Netz - Ein Ding der Unmöglichkeit?* und ist in verschiedene Themengebiete unterteilt. Als Teil der Projektarbeit haben wir ausserdem mehrere Experimente durchgeführt, die direkten Bezug zu in diesem Dokument behandelten Themen haben. Diese Experimente sind stark praxisbezogen und wurden von uns in Form von Handbüchern dokumentiert. Die Handbücher sollen dem Anwender ermöglichen, die von uns beschriebenen Techniken zur Wahrung der Anonymität selbst anzuwenden, denn oft ist der Weg dahin, selbst für einen Laien, gar nicht so steinig wie vielleicht angenommen. Jedes Handbuch ist eine für sich abgeschlossene Einheit und kann unabhängig von den anderen Dokumenten verwendet werden. Die Handbücher befinden sich im Anhang zu diesem Dokument und können alternativ einzeln heruntergeladen werden. Mehr dazu im nächsten Abschnitt.

1.3 Veröffentlichung

Um diese Arbeit zu verwirklichen, haben wir viel an Wissen aus den Weiten des Internets holen können. All die Inhalte, von denen wir Gebrauch gemacht haben, sind das Ergebnis der Arbeit eines Dritten. Um das von uns erarbeitete Wissen zu teilen und der Gemeinschaft etwas zurückzugeben, werden das Hauptdokument und die Handbücher im Netz veröffentlicht und ohne Entgelt zum Download angeboten. Die Arbeiten können unter folgender Adresse heruntergeladen werden: `http://timofurrer.github.io/idpa`

2 Einleitung

2.1 Was bisher geschah

Anfang Juni 2013 gelangten erste Dokumente an die Öffentlichkeit, die belegen, dass der amerikanische Auslandsgeheimdienst NSA (National Security Agency) im grossen Stil die Telefongespräche von US-Amerikanern überwacht hatte.[1] In den darauf folgenden Tagen, Wochen und Monaten wurden immer mehr Dokumente und Zeitungsartikel veröffentlicht, die die wahren Ausmasse der Überwachung digitaler Medien -Telefonnetz, Mobilfunk, Internet - seitens diverser Geheimdienste ans Licht brachten. Und der Strom an Publikationen reisst noch immer nicht ab. Kurz nach den ersten Veröffentlichungen outete sich ein junger Mann namens Edward Snowden als entscheidender Informant, der die vielen Dokumente in seinen Besitz gebracht und an Journalisten seines Vertrauens weitergegeben hatte. Es ist bis heute nicht offiziell klar, welche Menge an Informationen der ehemalige NSA-Mitarbeiter an sich bringen und an wen er Kopien weitergeben konnte.[2] Die betroffenen Geheimdienste, darunter die NSA und der britische GCHQ (Government Communications Headquarters), und die darüber stehenden Regierungen bemühen sich seit den ersten Veröffentlichungen um Schadensbegrenzung. Nun ist schon seit geraumer Zeit eine rege Diskussion auf globaler Ebene im Gange, die sich mit den Tätigkeiten von Geheimdiensten, der Privatsphäre der Bürger und der Sicherheit eines jeden Landes beschäftigt. Barack Obama soll bei einer Rede, bei der er die Tätigkeiten der NSA verteidigte, gesagt haben: *"Man kann nicht 100 Prozent Sicherheit und 100 Prozent Privatsphäre und null Unannehmlichkeiten haben."*[3] Wir stehen dieser Aussage kritisch gegenüber und wollten uns näher mit der Thematik *Anonymität im Netz* auseinandersetzen.

2.2 Motivation

Als angehende Informatiker haben wir die Enthüllungen und die damit einhergehenden Diskussionen mit grossem Interesse und wachsendem Unmut verfolgt. Durch unser technisches Verständnis konnten wir uns möglicherweise mehr darunter vorstellen als jemand, der Technik hauptsächlich anwendet, ohne sie zu hinterfragen oder deren innere Funktionsweise zu kennen. Wir sind der Meinung, dass ein jeder Bürger das Recht auf Privatsphäre hat. Um diese zu schützen, braucht es heutzutage gewisse Massnahmen, die man so bis anhin vielleicht nicht angewandt, geschweige denn gekannt hat. Ist Anonymität im Netz heutzutage überhaupt noch möglich? Welches technische Know-How muss man besitzen, um zu verstehen, an welchen Punkten eine ungewollte Überwachung stattfinden kann? Und wie gross ist der Aufwand, sich an eben diesen Stellen zu schützen?

[1] heise, Linkverzeichnis, Link 1
[2] Spiegel, Linkverzeichnis, Link 2
[3] Wikipedia, Linkverzeichnis, Link 3

2.3 Ziel

Unser Ziel ist es, im Rahmen dieser Arbeit Antworten auf die oben gestellten Fragen zu finden. Wir wählten dafür drei Anwendungen aus dem täglichen Leben, die online, also über das Internet, erfolgen: E-Mail-Verkehr, Surfen im Internet und Arbeiten mit der Cloud. Jede dieser Anwendungen wird genauer unter die Lupe genommen und in einen grösseren Zusammenhang gestellt. Der Schwerpunkt liegt dabei auf dem Einsatz von Techniken bzw. Technologien, die diese Anwendungen sicherer machen und die Privatsphäre im Netz schützen oder zumindest erhöhen. Zusätzlich wollen wir die Technologien in praxisnahen Experimenten selbst testen und parallel dazu Handbücher erstellen, die dem Anwender ermöglichen, selbst Gebrauch von ihnen zu machen. Letzten Endes soll diese Arbeit den Leser für die Thematik *Anonymität im Netz* sensibilisieren und ihm Mittel in die Hand geben, sich diese zu sichern.

3 Edward Snowden Leaks

Während den Veröffentlichungen Edward Snowden's mussten eine Menge namhafter Firmen zusehen, wie teils für sie sehr unangenehme Wahrheiten ans Licht gebracht wurden. Wahrheiten, die wohl selbst treue Kunden nachdenklich gestimmt haben: Soll ich denn wirklich noch meine E-Mails bei Google verwalten? Kann ich noch im Internet surfen, ohne ausspioniert zu werden? Diese Fragen werden zu Recht gestellt, denn es ist wichtig, selbst namhaften Firmen gegenüber kritisch zu sein. Ausserdem kam es in Folge der Veröffentlichung des brisanten Materials zu interessanten Ereignissen, die zugleich besorgniserregend sind. In den folgenden Abschnitten wird als Einstieg in das Thema dieser Arbeit detaillierter auf Teile des veröffentlichten Materials und bestimmte Ereignisse eingegangen.

3.1 Google, Yahoo, Microsoft & Co. - Kunden werden belauscht

Noch vor ein paar Monaten dachte wohl noch so mancher Kunde, der ein E-Mail-Konto bei Google, Yahoo oder Microsoft hatte, dass die E-Mails nur für ihn selbst einsehbar wären. Man hat ja schliesslich ein sicheres Passwort gewählt, das auch den Vorgaben des entsprechenden Providers entspricht. Nach all den Veröffentlichungen von Edward Snowden wurde aber klar, dass man selbst mit einem guten Passwort keineswegs sicher ist, denn der Provider hat die Kontrolle über die Server, auf denen die Mails gespeichert werden. Was, wenn dieser die Daten seiner Kunden weitergibt? Die Privatsphäre würde verletzt und man hätte praktisch keine Chance, dem zu entgehen, geschweige denn, überhaupt etwas davon zu merken. Doch selbst wenn der Provider dies nicht tut, besteht die Gefahr, dass Geheimdienste oder andere Organisationen beginnen, sich in oben genannte Dienste einzuklinken und private, kundenspezifische Daten abzuschöpfen. Dies war beispielsweise der Fall mit einem Ausspäh-Werkzeug der NSA mit dem Namen *Muscular*. Mit diesem Werkzeug war es der NSA möglich, sich in die Leitungen von Google einzuklinken und Daten mehrerer hundert Millionen Nutzerkonten abzugreifen. Doch nicht nur Google war davon betroffen. Auch Yahoo wurden auf

diesem Weg private Nutzerdaten entzogen. Laut den NSA-Papieren vom 9. Januar 2013 hat die NSA innerhalb eines Monats über 181 Millionen Datensätze von Google und Yahoo an Datenzentren des NSA-Hauptquartiers geschickt. Erwähnenswert ist dabei, dass sich die NSA für dieses Vorhaben mit dem britischen Geheimdienst GCHQ zusammengetan hat. Sich also nur auf amerikanische Geheimdienste zu fokusieren wäre ein Fehler. Natürlich wurde das Programm von NSA-Chef General Keith B. Alexander vehement abgestritten: *"Wir haben keinen Zugang zu Google-Servern, Yahoo-Servern und so weiter."*[4]

Doch nicht nur E-Mail-Konten waren betroffen. Laut einem Artikel des britischen Guardian hat die NSA in Zusammenarbeit mit dem GCHQ ein Programm namens *Dishfire* entwickelt, das *so ziemlich alles sammelt, was es findet.* Informationen werden wahllos aus Reiseplänen, Adressbüchern, Finanztransaktionen und weiteren Ressourcen zusammengetragen und ausgewertet. Das Dokument aus dem Jahr 2011, auf das sich der Artikel bezieht, macht deutlich, dass pro Tag zum Teil bis zu 200 Millionen SMS gesammelt wurden. Diese SMS waren verknüpft mit Informationen zu Sender und Empfänger, Geodaten, Datum und Zeit und angehängten Dateien.[5]

3.2 Der Fall LavaBit

LavaBit ist - oder besser gesagt war - ein US-amerikanisches Unternehmen, welches einen sicheren Webmail-Service zur Verfügung gestellt hatte. Mit *sicher* ist gemeint, dass der Dienst dem Kunden die Möglichkeit bot, seine E-Mails zu verschlüsseln. Als am 10. Juni 2013 die Identität des NSA-Whisteblowers Edward Snowden bekannt wurde, verlangte die US-amerikanische Regierung die Herausgabe von Informationen eines bestimmten Benutzerkontos von LavaBit. Zu den verlangten Informationen gehörten Adressen, Aufzeichnungen von Sitzungen, Telefonnummern, MAC-Adressen sowie Bank- und Kreditkartendaten. Zudem stellte die Regierung die Forderung, ein Überwachungsgerät installieren zu dürfen, welches diese Daten direkt an sie übermitteln sollte. LavaBit-Gründer Ladar Levison lehnte jedoch alle Forderungen ab. Er war nicht bereit, die Daten seines Kunden freizugeben. Kurz darauf wurde Levison aufgefordert, alle öffentlichen und privaten SSL-Schlüssel seines Dienstes der Regierung zu übergeben. Dies hätte mit ziemlicher Wahrscheinlichkeit eine komplette *De-Anonymisierung* aller seiner Kunden bedeutet. Nach weiterem Hin und Her leistete Levison schliesslich Folge und druckte die Schlüssel auf Papier mit der Schriftgrösse vier aus. Das FBI berichtete, dass die Daten auf Grund der sehr kleinen Schrifftgrösse mehrheitlich unleserlich waren und nicht gebraucht werden konnten. Sie verlangten darauf eine Abgabe der Schlüssel in digitaler Form. Um die Nutzer seines Webmail-Services nicht an die Strafverfolger ausliefern zu müssen, sah sich Levison gezwungen, seinen Dienst per 8. August 2013 zu schliessen. Trotz der Schwärzung des Namens vom Inhaber des ursprünglich betroffenen E-Mail-Kontos ist es fast ohne Zweifel, dass es sich um das private E-Mail-Konto von Edward Snowden gehandelt hatte. Levison selbst bekam während der Geschehnisse auf Grund seines Widerstands

[4] n-tv, Linkverzeichnis, Link 4
[5] heise, Linkverzeichnis, Link 5

Probleme mit der Justiz und musste sich unter anderem vor Gericht verantworten. [6] [7] [8] [9]

3.3 Weite Anlaufstellen

Die Abschnitte in diesem Kapitel haben nur einen sehr kleinen Teil der Enthüllungen und der damit zusammenhängenden Ereignisse abgedeckt. Da der Fokus dieser Arbeit ein anderer ist, wird an dieser Stelle auch nicht detaillierter darauf eingegangen. Es ist aber wärmstens empfohlen, bei Interesse das Internet nach weiteren Informationen zu durchforsten, denn alle Enthüllungen sind von grosser Wichtigkeit und hochinteressant dazu. Vor allem auf IT-Seiten wird man schnell fündig. Als Beispiel soll an dieser Stelle der bekannte Nachrichtenticker *heise online* genannt werden. Dieser hat die NSA-Affäre zu einem Topthema erklärt und ist seit den ersten Enthüllungen bis heute am Ball geblieben. Zum Einstieg bietet er eine Übersichtsseite zu den Enthüllungen an. Man findet diese unter: `http://www.heise.de/thema/NSA`. Es wurde darüber hinaus eine *Time-Line* eingerichtet, der man von den ersten Enthüllungen bis zu den brandaktuellen Neuigkeiten folgen kann: `http://www.heise.de/extras/timeline`

4 Von der Black Box „Internet“ und dem Wesen der Kommunikation

4.1 Vom Brief zur E-Mail

Wenn man sich in früheren Jahrhunderten etwas Wichtiges und sehr Privates mitzuteilen hatte, traf man sich persönlich von Angesicht zu Angesicht. Wenn es die Distanz nicht erlaubte, musste man unter Umständen einen vertrauenswürdigen Boten engagieren, der die Nachricht in Form eines Briefes mit Siegel an die gewünschte Person überbrachte. Das Siegel sollte dabei die Integrität der im Brief enthaltenen Informationen gewährleisten. Was den zweiten Fall betraf, so hatte man auch da nicht die volle Kontrolle. Man musste wohl oder übel auf den Boten vertrauen. Hinzu kommt, dass dem Boten ja auch unterwegs etwas hätte zustossen können oder der Bote gezielt abgefangen wurde. Es gab also schon immer Unsicherheiten, was die Übertragung von Nachrichten betrifft, sofern man es nicht komplett selbst in die Hand nahm.
Mit der Entwicklung des Postwesens, wie man es heute kennt, änderte sich vieles schlagartig. Briefe zu verschicken wurde bequem, einfach und bezahlbar. Jeder mit den nötigen Kleinutensilien konnte nun Briefe um die ganze Welt schicken - vorausgesetzt natürlich man konnte

[6] heise, Linkverzeichnis, Link 6
[7] Spiegel, Linkverzeichnis, Link 7
[8] heise, Linkverzeichnis, Link 8
[9] Wikipedia, Linkverzeichnis, Link 9

schreiben. Wie sah es mit privaten bzw. geheimen Briefen aus? Erfahrungen aus der Vergangenheit, wie zum Beispiel die Postkontrollen zu STASI-Zeiten, haben gezeigt, dass es je nach Regierungsform der einzelnen Länder unterschiedlich sicher war, Privates per Post mitzuteilen. In den 80er Jahren wurden von der Abteilung M der STASI, welche für die Postkontrolle zuständig war, täglich bis zu 90 000 Briefe gelesen und/oder kontrolliert[10]. Der Briefverkehr wird aber auch heute noch rege genutzt für aller Hand oberflächlicher Kommunikation und nicht selten auch für Privates. Wie kann man wissen, ob die Post nicht auch heute noch stellenweise kontrolliert wird?
In den 70er-Jahren kam schliesslich das Internet und mit dem Internet das grosse Zeitalter der E-Mail. Die E-Mail war zu Beginn die meistgenutzte und wichtigste Anwendung des Internets und schon 1971 brauchte der E-Mail-Verkehr mehr Datenvolumen als alle anderen Dienste zusammen[11] Nachrichten konnten nun noch günstiger - und vor allen Dingen schneller - übermittelt werden. Es gab zudem keine topographischen Einschränkungen, wenn die Infrastruktur einmal vorhanden war. Mailverkehr über das Internet hat viele Vorteile, das kann man nicht bestreiten. Er hat aber auch eine sehr grosse Schwachstelle. Das Internet ist heute in seiner Komplexität so enorm und vielschichtig, dass man als Laie kaum einschätzen kann, welchen Weg die verschickte E-Mail genau nimmt und welche Posten sie dabei passiert.

4.2 Der Webbrowser - Das Fenster zum Internet

Ein weiterer Meilenstein in der Geschichte des Internets ist der Webbrowser. Mit der Einführung des ersten grafikfähigen Webbrowsers Mosaic im Jahre 1993 erhielt das Internet einen weiteren Aufwärtsschub[12]. Mit ihm war erstmals ein komfortables Durchstöbern des World Wide Web möglich, ganz ähnlich, wie man das heute mit bekannten Browsern wie dem Internet Explorer, Mozilla Firefox oder Google Chrome kann. Obwohl das Internet und das IT-Wesen allgemein immer komplexer und grösser werden, wird die oberflächliche Benutzung der Dienste immer einfacher. Surft man im Internet, um nach irgendwelchen Angeboten oder Online-Artikeln zu suchen, sieht man auf seinem Bildschirm lediglich ein Fenster, in dem man die gewünschten Inhalte in strukturierter und visuell aufbereiteter Form dargestellt bekommt. Woher die Daten genau kommen und welchen Weg sie nehmen ist nicht ersichtlich. Es ist eine Schnittstelle in ein riesiges Netzwerk von enormer Komplexität, die den Laien wohl sehr schnell überfordern würde. Und trotzdem ist die Bedienung kinderleicht.

4.3 Die Cloud - Daten immer und überall

Mit der passenden Software können heutzutage Daten immer und überall abgerufen werden. Beispielsweise werden Dokumente, die man auf verschiedenen Geräten braucht, regelmässig miteinander abgeglichen, um kein Durcheinander mit der Versionierung zu bekommen. Sie

[10]Berliner Bär, Linkverzeichnis, Link 10
[11]Wikipedia: Internet, Linkverzeichnis, Link 11
[12]Wikipedia: NCSA Mosaic, Linkverzeichnis, Link 12

können sogar online bearbeitet werden, ohne beispielsweise ein Microsoft Office auf dem gerade genutzten PC installiert zu haben. Diese Möglichkeiten ergeben sich durch das immer stärker genutzte Konzept der *Cloud*. Grosse IT-Unternehmen und Dienstleister mit der passenden Infrastruktur bieten dem Kunden eine Vielzahl von Diensten an, die alle über die Grossrechner der Unternehmen gehandhabt werden. Der Kunde hat dabei meist keine Einsicht in die technischen Einzelheiten und Prozesse und muss sich nicht mehr um technische Probleme kümmern. Er muss sich auch nicht fragen, wie denn eigentlich die Informationen von A nach B kommen und wo sie gespeichert werden. Für diesen Sachverhalt, der auch auf den E-Mail-Verkehr und das Surfen im Internet zutrifft, gibt es einen Fachbegriff. Man spricht von der sogenannten *Black Box*.

4.4 Das Prinzip der Black Box

Der Begriff Black Box hat einen wissenschaftlichen Hintergrund. Die englischsprachige Seite von Wikipedia gibt folgende Kurzdefinition des Begriffes an:

> *"A black box is a device, object, or system whose inner workings are unknown; only the input, transfer, and output are known characteristics."* [13].

Auf Deutsch übersetzt heisst das so viel wie: *Eine Black Box ist ein Gerät, Objekt oder System, dessen innere Funktionsweise unbekannt ist. Nur die Eingabe, der Transfer und die Ausgabe sind bekannt.* Man gibt also etwas in die Black Box hinein und erwartet einen bestimmten Output. Was genau in der Black Box vorgeht, wie der Output entsteht, interessiert einen nicht. Es zählt nur das Ergebnis. Eine einfache Grafik soll das Prinzip verdeutlichen.

Abbildung 1: Black Box

Die drei Anwendungsfälle *Mailverkehr*,*Surfen im Internet* und *Nutzung der Cloud* machen ebenfalls von diesem Prinzip gebrauch. Möchte man einen Mailaccount einrichten, kann man dies gratis innerhalb weniger Minuten erledigen. Mails zu schreiben und anschliessend zu verschicken ist ebenfalls sehr komfortabel. Was das Surfen im Internet betrifft, so kann dies heute wohl jeder Zehnjährige. Das World Wide Web mit seinem riesen Fundus an Information ist zur Selbstverständlichkeit geworden. Lediglich der Gebrauch der Cloud ist für den Normalverbraucher noch nicht so selbstverständlich. Doch auch hier ist ein Trend zur vermehrten Verbreitung und Nutzung erkennbar. Im technischen Umfeld und in Unternehmen

[13] Wikipedia: Blackbox, Linkverzeichnis, Link 13

hat sich die Cloud aber schon längst durchgesetzt.

Es macht durchaus Sinn, dass man Dienste bewusst auslagert. Es kann schliesslich nicht jeder Mensch dieser Welt IT-Spezialist sein. Warum sollte man die technischen Fragen nicht denen überlassen, die sich in diesem Gebiet spezialisiert haben? Eine mögliche Antwort darauf gaben die letzten paar Monate, seit Edward Snowden die massenhafte und tiefgreifende Überwachung digitaler Medien durch die Geheimdienste aufgedeckt hat. Ähnlich wie früher beim Briefboten, legt man auch heute die Daten in die Hände von Dritten. Dies sind oft grosse, internationale Unternehmen, welche die Daten verarbeiten und aufbewahren. In die Einzelheiten des Verarbeitungsprozesses hat man dabei keinen Einblick. Es ist eine Black Box. Es war also bis heute alles eine Frage des Vertrauens und wird es vielleicht auch in Zukunft sein.

Die Enthüllungen Snowdens und die dadurch entstandenen Diskussionen zeigen aber eines ganz klar auf: Es braucht ein neues Bewusstsein, was das Internet, dessen Möglichkeiten, Gefahren und die Privatsphäre der Nutzer betrifft. Die Frage des Datenschutzes ist einmal mehr in aller Munde und das zu Recht. Der gläserne Mensch - ein Mensch ohne Privatsphäre und Geheimnisse - scheint in greifbarer Nähe. Und ist er einmal Realität, lässt er sich nur schwer wieder verbannen [14].

Die Redewendung „Vertrauen ist gut, Kontrolle ist besser!“, die dem russischen Politiker Lenin zugeordnet wird [15], passt in diesem Zusammenhang ironischerweise sehr gut. Der Nutzer sollte mehr Kontrolle darüber haben, was mit seinen Daten passiert oder zumindest genau darüber Bescheid wissen. Es gibt dazu unterschiedliche Ansätze und Möglichkeiten, diese Kontrolle zu erlangen. In den nächsten Kapiteln sollen ein paar davon gezeigt werden.

5 E-Mails und deren Tücken

Täglich werden heute bis zu 180 Milliarden E-Mails versendet. Eine gewaltige Menge, wenn man bedenkt, dass es ein wenig mehr als sieben Milliarden Menschen auf diesem Planeten gibt. Doch nur wenige E-Mail-Nutzer machen sich wohl Gedanken darüber, was denn eigentlich hinter einer E-Mail steckt. Wohin geht sie genau? Wer kann diese E-Mail theoretisch lesen? Wo wird diese Nachricht überall gespeichert? Und für wie lange? Gibt es Kopien? Backups? Auf anderen Servern? All diese Fragen sind sehr wichtig, wenn man vertrauliche Daten per Mail versendet. Doch auch wenn der Inhalt der Nachricht nicht von grosser Bedeutung ist, möchte man eine gewisse Privatsphäre wahren, oder? Was kann man also als „0815“ Nutzer tun, um seine eigenen E-Mails möglichst sicher zu versenden, zu speichern und zu empfangen?
Im nächsten Kapitel wird versucht auf diese Fragen eine Antwort zu finden. Zuerst einmal muss man aber verstehen, wie das genau funktioniert mit den „Mails“.

[14] Wikipedia: Gläserner Mensch, Linkverzeichnis, Link 14
[15] Wikipedia: Vetrauen ist gut, Kontrolle ist besser, Linkverzeichnis, Link 15

5.1 Funktionsweise des Mailverkehrs

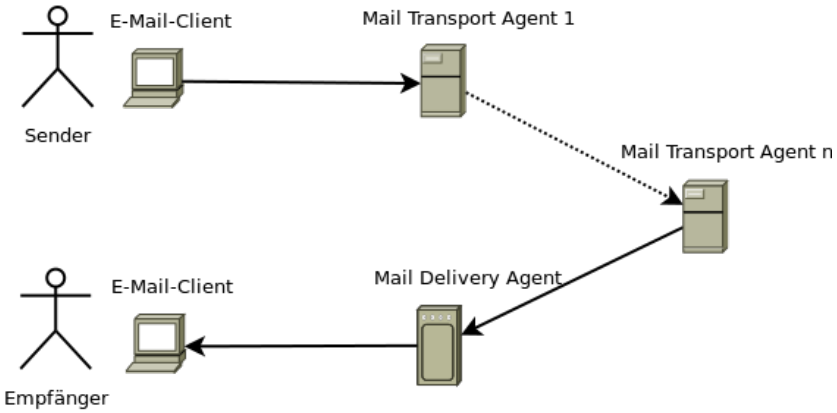

Abbildung 2: Funktionsweise des Mailverkehrs

Eine E-Mail passiert von der Erzeugung beim Sender bis zur Abgabe beim Empfänger mehrere Posten. Um die Funktionsweise des E-Mail-Verkehrs beschreiben zu können, müssen diese Posten zuerst erklärt werden:

- E-Mail-Client: Beim Client handelt es sich um das Mail-Programm, welches E-Mails senden und empfangen kann. Sowohl der Sender als auch der Empfänger sind auf ein solches angewiesen.
- Mail Transfer Agent (MTA): Der Mail Transfer Agent ist für den Transport der E-Mail verantwortlich. [16]
- Mail Delivery Agent (MDA): Der Mail Delivery Agent hat die Aufgabe, die E-Mail beim Empfänger abzuliefern, sobald diese vom Mail Transfer Agent übermittelt wurde. [17]

Bei MTA und MDA handelt es sich jeweils um Computer-Programme, welche typischerweise auf den Servern (Computern) des jeweiligen Providers laufen.

Ablauf des E-Mail-Verkehrs:

1. Der Sender verfasst mit Hilfe des Clients eine Mail für einen bestimmten Empfänger und drückt anschliessend auf *Senden*.
2. Der Client übermittelt die E-Mail bei aktiver Internetverbindung an den ersten MTA.

[16] Wikipedia: Mail Transport Agent, Linkverzeichnis, Link 16
[17] Wikipedia: Mail Delivery Agent, Linkverzeichnis, Link 17

3. Die Mail wird nun von MTA zu MTA geschickt, bis derjenige des Empfängers gefunden wird.

4. Der MTA des Empfängers übermittelt die Mail an den MDA, welcher die Mail aufbewahrt.

5. Der Client des Empfängers holt die Mail bei aktiver Internetverbindung beim MDA ab und stellt sie dem Empfänger zur Verfügung.

Je nach verwendetem Protokoll wird dem Empfänger eine Kopie der Mail zugestellt (IMAP), wobei das Original auf dem Server bleibt, oder er erhält das Original selbst (POP3).

IMAP (Internet Message Access Protocol) hat den Vorteil, dass man im Falle eines lokalen Datenverlusts das Original des Mails auf dem Server hat. Es eignet sich zudem sehr gut für die parallele Nutzung von mehreren Geräten (Computer, Tablet, Smartphone), da die E-Mails jeweils synchronisiert (abgeglichen) werden. [18]

POP3 (Post Office Protocol 3) bietet diese Möglichkeiten nicht. Es eignet sich aber für Nutzer, die gerne selbst bestimmen, wo ihre E-Mails aufbewahrt werden. Seit den Snowden-Enthüllungen scheint dieses Argument wichtiger denn je. [19]

5.2 Mein Provider und seine Server

Der erste Schritt, den man tun muss, um überhaupt eine E-Mail versenden zu können, ist es, sich einen passenden Provider auszusuchen. Ein Provider ist eine Firma, die ihren Kunden eine Mail-Adresse zur Verfügung stellt. Dies kann z.B. Google mit Gmail, Microsoft mit Hotmail oder eine Firma wie GMX sein. Der Provider muss diese E-Mail-Adresse konfigurieren, damit der Kunde sie gebrauchen kann. Zur Konfiguration gehört unter anderem die Adresse zum Mail Transfer Agent und die Adresse zum Mail Delivery Agent. Diese Programme bzw. die Server, auf denen sie laufen, sind nicht nur in Bezug auf die allgemeine Mailfunktionalität von Bedeutung. Nein, denn dort, auf diesen Servern, unter der Kontrolle des jeweiligen Providers, geht jede einzelne E-Mail, die versendet oder empfangen wird, durch. Das bedeutet, dass dort theoretisch ein Mitschnitt aller Nachrichten gemacht werden kann. Auch macht der Provider, natürlich nur zum Besten seiner Kunden, Backups (Sicherungen) von deren Postfächer. Das mag ja schön und gut sein und ist im Falle eines Datenverlusts äusserst praktsich, aber wer kann sonst noch auf dieses Postfach oder die Backup-Daten zugreifen? Die Systemadministratoren vom Provider? PR-Firmen? Datenanalysten? Geheimdienste? Wer weiss.

[18] Wikipedia: POP3, Linkverzeichnis, Link 18
[19] Wikipedia: IMAP, Linkverzeichnis, Link 19

5.3 E-Mails verschlüsseln

Doch es gibt ein paar Dinge, die man tun kann, um seine E-Mails besser vor ungewollten Blicken zu schützen. So gibt es mehrere Verfahren, um E-Mails zu verschlüsseln. Eines der beliebtesten und wohl meist verbreitetsten hierfür ist PGP (Pretty Good Privacy) oder deren Weiterentwicklung GPG (GNU Privacy Guard). Bei beiden handelt es sich um ein Public-Key-Verfahren mit asymmetrischer Verschlüsselung. Bei dieser Art von Verschlüsselung gibt es einen öffentlichen Schlüssel, mit dem jeder Sender Daten für den Empfänger verschlüsseln und signieren kann und es gibt einen privaten, geheimen Schlüssel, der vom Empfänger benutzt wird, um die Nachricht, die mit seinem öffentlichen Schlüssel verschlüsselt wurde, wieder zu entschlüsseln. Solange man seinen privaten Schlüssel geheim hält, ist es für einen "Angreifer" sehr schwierig sowie rechen- und zeitintensiv eine solche verschlüsselte Nachricht zu knacken. Es gibt eine Menge Erweiterungen für die gängigsten Mail-Clients, um diese Verschlüsselungsfunktion nachzurüsten. Im Internet findet man viele Anleitungen, die einem zeigen, wie man dazu vorgehen muss und welche Erweiterungen sich empfehlen.

5.4 Ich als Provider

Wenn man plant, seine Mails selbst zu verwalten und komplett auf einen Mail-Provider zu verzichten, muss man sich fragen, was einen Provider ausmacht und welche Aufgaben er hat. Ein Provider muss einen MDA und einen MTA zur Verfügung stellen, damit Mails versendet und empfangen werden können. Diese müssen am Internet angehängt sein und dauerhaft laufen, damit die E-Mails ihr Ziel auch erreichen.
Ausserdem muss er die E-Mail-Adresse des Kunden so konfigurieren, dass die Mails den richtigen Weg nehmen. Jeder Provider hat seine eigene Domain, wie zum Beispiel Google's *gmail.com* oder Swisscom's *bluewin.ch*. Die E-Mail-Adressen der Kunden enden deshalb immer auf jene Domains: *max@gmail.com*, *muster@bluewin.ch*. Als "Selbstversorger" braucht man nun ebenfalls eine solche Domain. Dabei muss es sich nicht zwingend um eine Top-Level-Domain handeln [20]. Auch eine kostenlose Domain mit der Endung *.ch.vu* würde genügen.
Dieser Domain braucht man dann nur noch einen DNS-Server [21] zuzuweisen, der den MDA kennt. Ein Problem gibt es da aber noch. Normale Haushaulte bekommen vom Internetprovider standardmässig keine statische IP-Adresse zugewiesen, was bedeutet, dass diese ständig ändern kann und so der DNS-Server nicht mehr weiss, wohin er jetzt den Datenverkehr weiterleiten muss. Um dieses Problem zu lösen gibt es zwei Möglichkeiten: Man kann beim Provider eine kostenpflichtige statische IP-Adresse erwerben oder man registriert sich bei einem dynamischen DNS-Anbieter. Dieser stellt eine Schnittstelle zur Verfügung, über die man die IP-Adresse seines Server bei jeder Änderung dem DNS-Server mitteilen kann. Somit kennt der DNS-Server stets die aktuelle IP-Adresse des Servers.

Hinweis: IP-Adressen und DNS-Server werden in Kapitel 6 - Surfen im Internet noch ge-

[20] Wikipedia: Top Level Domain, Linkverzeichnis, Link 20
[21] Wikipedia: Domain Name System, Linkverzeichnis, Link 21

nauer erklärt.

5.4.1 Vor- und Nachteile

Natürlich gibt es nicht nur Vorteile, wenn man sein eigener E-Mail-Provider ist. Eine kurze Auflistung einiger Vor- und Nachteile soll eine Übersicht bieten.

Vorteile:

- Volle Kontrolle
- Verschlüsselung
- Eigener Spam und Virenfilter

Nachteile:

- Hardware- und Unterhaltungs-Kosten
- Benötigte Zeit bzw. benötigtes Know-How
- Risiko von Datenverlust

5.5 Vertrauenswürdige Provider?

Seine Mails selbst zu verwalten ist ein schwieriges unterfangen und mit viel Aufwand verbunden. Für Laien ist dies definitiv keine empfehlenswerte Lösung. Die Frage, die sich deshalb stellt ist, ob es denn bereits vertrauenswürdige und sichere E-Mail Provider gibt, auf die man stattdessen zurückgreifen kann.
Leider ist es sehr schwierig oder gar unmöglich eine Antwort auf diese Frage zu finden, denn Tatsache ist, dass in der Theorie jeder Provider gehackt werden kann. Die Daten sind beim Provider somit nie hundert Prozent sicher.
Es bleibt einem nichts anderes übrig, als zu vertrauen. Vertrauen in den Provider, dass dieser bestrebt ist, jede mögliche Massnahme zu treffen, um die höchsten Sicherheitsstandards einzuhalten.
Ein Beispiel hierfür ist *NEOMAILBOX*[22]. Diese Firma stellt einen kostenpflichtigen Service zur Verfügung, der einen schnellen, sicheren und anonymen E-Mail-Dienst verspricht. Zudem soll der Service mit einem top Spam- und Virenfilter ausgestattet sein.

[22]Neomailbox, Linkverzeichnis, Link 22

5.6 Experiment

5.6.1 Zielsetzung

Das Ziel war es, einen Computer aufzusetzen, auf dem ein Mailserver läuft. Der Mailserver soll aus einem Mail Delivery Agent und aus einem Mail Transport Agent bestehen. Als Computer kam zu Testzwecken ein Raspberry Pi zum Einsatz. Dabei handelt es sich um einen Einplatinen-Computer.
Sobald man vor hat nur noch den eigenen Mailserver zu benutzen, sollte man einen richtigen Computer als Server in Betracht ziehen. Als Betriebssystem kam das auf GNU/Linux Debian basierende Betriebssystem Raspbian zum Einsatz. Alle genutzte Software ist frei Verfügbar und sogar Open Source.

5.6.2 Installation

Das Experiment *Installation eines Mailservers* war das anspruchsvollste der drei Experimenten. Es gibt recht viele Konfigurationsdateien zu bearbeiten, was ein hohes Fehlerrisiko mit sich bringt. So haben auch wir im ersten Versuch gescheitert. Zwar war es möglich E-Mail zu verschicken, doch das Empfangen war unmöglich. Nach einem kompletten Neustart des Experimentes ist es uns doch gelungen einen funktionierenden Mailserver in Betrieb zu nehmen. Selbst das Aufsetzen eines funktionierenden Spamfilters hat am Ende funktioniert.

Der Zugriff per POP3 und IMAP für das Empfangen der Mails ging mit dem Mail Client Thunderbird ohne Probleme. Auch mit dem Mail Client des iPhones war es möglich die Mails zu empfangen. Gleiches gilt auch für das Senden von E-Mails.

5.6.3 Fazit

Einen eigenen Mailserver aufzusetzen, ist nicht für jedermann gedacht. Man muss unbedingt bedenken, dass dies mit recht viel Arbeit verbunden sein kein, vor allem dann, wenn man sich noch nicht so gut mit der Thematik auskennt. Erfreulich war, dass das Senden und Empfangen von E-Mails am Ende ohne Probleme funktioniert hat. Auch das installierte Webinterface macht einen guten Eindruck. Für Interessierte ist es sicher lohnenswert dieses Projekt in Angriff zu nehmen. Hat man es einmal am laufen, ist man stolz drauf seinen eigenen Mailserver unter Kontrolle zu haben.

Das Handbuch, in dem der Installationsprozess detailliert beschrieben ist, befindet sich im Anhang oder kann einzeln heruntergeladen werden unter: `https://github.com/timofurrer/idpa/raw/master/pdfs/mailserver.pdf`

6 Surfen im Internet - Wie anonym ist anonym?

Wenn man im Internet surft, hat man vielleicht das Gefühl, alleine und anonym unterwegs zu sein. Diese Annahme ist aber falsch, denn *das Internet* ist sich sehr wohl darüber bewusst, wer wann wo unterwegs ist. Um zu verstehen, wie man sich mehr Anonymität verschaffen kann, müssen zuerst gewisse Bestandteile und Funktionsweisen des Internets bekannt sein.

6.1 IP-Adressen und Domänennamen

Das Internet besteht aus Millionen von Computern und anderen Geräten, die miteinander vernetzt sind. Auch der private Computer mit Internetzugang, den man für tägliche Arbeiten benutzt, ist ein Teil davon. Jedes dieser Geräte hat nach aussen hin einen eindeutigen Identifikator, die sogenannte IP-Adresse. Die IP-Adresse besteht aus mehreren aneinandergereihten Zahlenblöcken, die durch Punkte unterteilt sind. Sie ist dabei immer eindeutig und wird einem vom Provider (z.B. Swisscom) zugeteilt. Eine IP-Adresse könnte folgendermassen aussehen: *143.39.238.12*. Die IP-Adresse wird aber nicht nur Privatanwendern zugewiesen, damit diese sich im Internet bewegen können. Auch hinter *www.google.ch* steckt eine IP-Adresse und genau so verhält es sich mit allen anderen Internetdiensten (Webseiten, Datei-Servern, Download-Plattformen, etc.). Jeder Dienst lässt sich über seine IP-Adresse ansprechen, sofern diese bekannt ist. Da sich Menschen Namen aber deutlich leichter merken können als Abfolgen von Zahlen, hat man das *Domain Name System* (DNS) eingeführt. Das DNS ist ein Verzeichnisdienst, der den Namensraum des Internets verwaltet und ist weltweit auf tausende von Servern verteilt. Seine Aufgabe besteht darin, sogenannte Domänennamen wie *google.ch* in die zugehörigen IP-Adressen umzuwandeln[23].

[23] Wikipedia: Domain Name System, Linkverzeichnis, Link 21

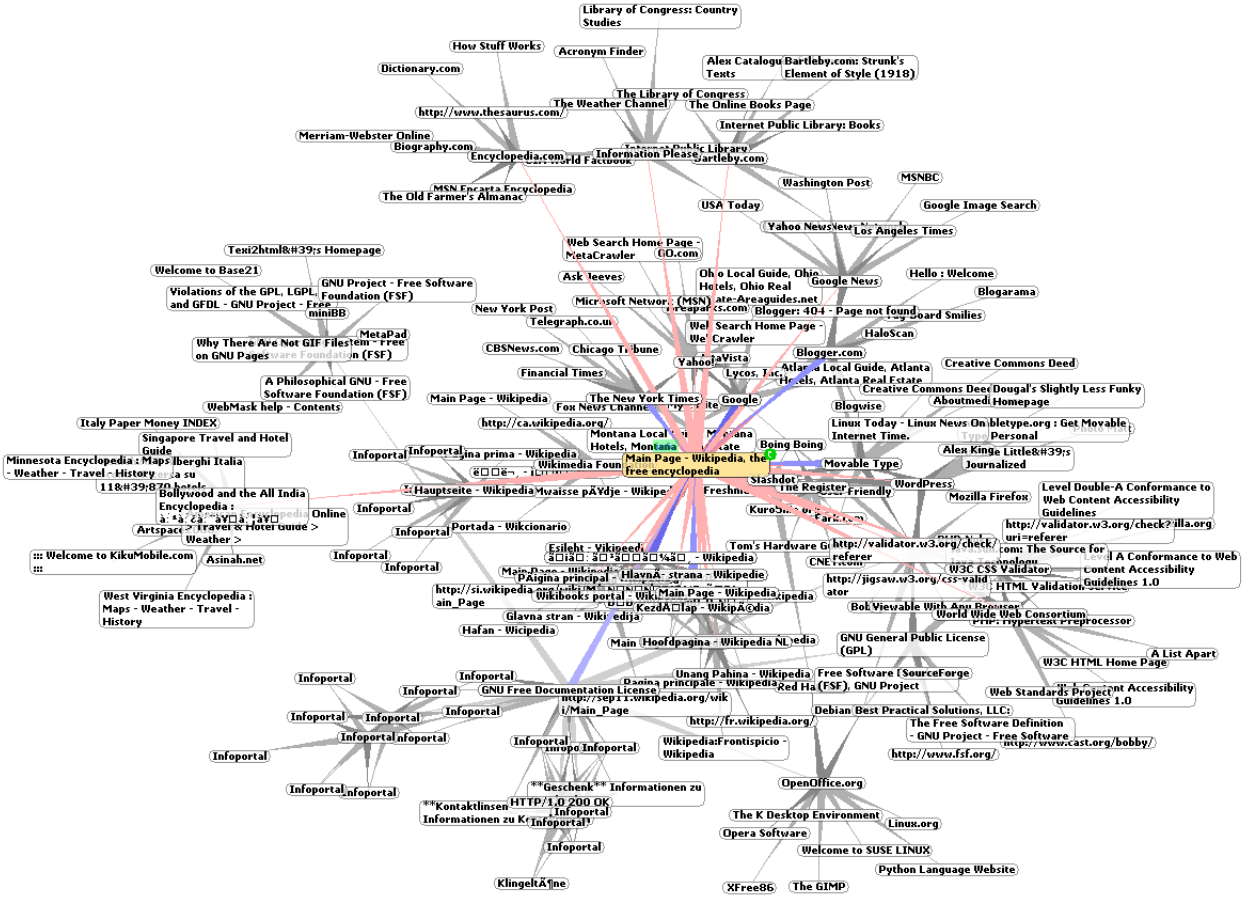

Abbildung 3: Darstellung der Vernetzung im Internet - Hier Webseiten um *en.wikipedia.org*

6.2 Server und Client

Aus den obigen Erklärungen lässt sich ableiten, dass sich hinter einem Internetdienst immer auch ein Computer bzw. Server befinden muss. Doch was ist ein Server eigentlich? Wikipedia gibt folgende Definition an:

> *"Ein Server ist ein Computerprogramm oder ein Computer für den Zugriff auf eine zentrale Ressource oder Dienst in einem Netzwerk."* [24]

Ein Server stellt also einen Dienst bereit, der vom sogenannten *Client* benutzt werden kann. Der Dienst ist beispielsweise eine Webseite, die vom Client - in diesem Zusammenhang dem Webbrowser - abgerufen und dargestellt wird. Wie im vorherigen Abschnitt schon erwähnt, gibt es eine Vielzahl von verschiedenen Diensten und demnach auch eine Vielzahl von verschiedenen Servern. Wenn es um Privatsphäre und Anonymität geht, stellen sich hier gleich

[24] https://de.wikipedia.org/wiki/Server

mehrere Fragen: Wem gehören diese Server? Ist der Besitzer eines Servers gleichzeitig auch der Administrator? Welche Informationen speichern die Server über seine Nutzer und geben sie diese weiter? Welche Informationen können von den Server überhaupt eingesehen werden? Lediglich die letzte Frage lässt sich klar beantworten. Diese verweist auch auf die Möglichkeiten, die man hat, die Privatsphäre im Internet zu erhöhen. Zu den Spuren, die man im Internet hinterlässt, gehören unter anderem die IP-Adresse und damit zusammenhängend Informationen zum Provider und dessen Niederlassung. Auch Informationen zum Browser inklusive dem verwendeten Betriebssystem können von den passierten Servern eingesehen werden. Es gibt darüber hinaus viele verschiedene Technologien und Techniken, die es Servern erlauben, detailliertere Nutzerinformationen abzuschöpfen. In diesem Kapitel liegt der Fokus aber auf den Verbindungsdaten - den IP-Adressen - und deren Anonymisierung. Und an dieser Stelle kommt Tor ins Spiel.

6.3 Verbindungsdaten anonymisieren mit Tor

Tor, ein Akronym für *The Onion Routing*, ist ein Netzwerk, welches geschaffen wurde, um Verbindungsdaten zu anonymisieren. Die Entwicklungen an Tor begannen 2002 an der Universität in Cambridge und dauern bis heute an. Um das Tor-Netzwerk zu verwenden, wird ein gleichnamiges Computerprogramm benötigt, welches frei nutzbar ist. Der Quellcode der Software ist veröffentlicht und für jedermann einsehbar. Global betrachtet nutzt wohl nur ein kleiner Teil der Leute Tor, da es erstens nicht sehr bekannt ist und zweitens die Nutzung mit einem gewissen Mehraufwand verbunden ist, der zusätzliches technisches Know-How verlangt. Im Rahmen der Enthüllungen von Edward Snowden hat Tor aber an Bedeutung gewonnen. Die kritischen Stimmen wurden jedoch ebenfalls lauter und das zu Recht.

6.4 Der zweifelhafte Ruf von Tor

Tor hat einen zweifelhaften Ruf, der einen potenziellen Nutzer möglicherweise zwiegespalten zurücklässt. Es heisst oft, dass im Tor-Netzwerk auf Grund der Anonymisierung verstärkt illegaler Handel getrieben wird. Dies betrifft den Handel mit Drogen, Waffen und auch Kinderpornographie.[25] [26] Möchte man als gewissenhafter Nutzer tatsächlich mit solchen Tätigkeiten in Verbindung gebracht werden? Was den zweifelhaften Ruf von Tor noch verstärkt, ist die Finanzierung des Projektes. So wird die Weiterentwicklung von Tor bis heute zu grossen Teilen von militärischen Organisationen der USA sowie der US-amerikanischen Regierung unterstützt. [27] [28] Dies grenzt beinahe schon an Ironie, sind es doch die amerikanischen Geheimdienste, die das Internet im grössten Masse aushorchen. Die Frage, die sich deshalb aufdrängt ist die Folgende: "Kann man überhaupt noch auf die anonyme Funktionsweise von Tor vertrauen oder muss man davon ausgehen, dass amerikanische Geheimdienste das

[25] Zeit, Linkverzeichnis, Link 23
[26] NZZ, Linkverzeichnis, Link 24
[27] Wikipedia: Tor Netzwerk, Linkverzeichnis, Link 25
[28] heise, Linkverzeichnis, Link 26

Netzwerk bewusst aufgebaut haben, um jeden abzuhören, der offenbar etwas zu verstecken hat?"
Kürzlich ist bekannt geworden, dass die Bemühungen der NSA, Nutzer vom Tor-Netzwerk gezielt zu de-anonymisieren, sehr ineffizient sind.[29] Handelt es sich dabei um eine bewusste Falschmeldung? Oder ist Tor vielleicht doch sicherer als es den Anschein macht? Diese Frage lässt sich leider nicht abschliessend beantworten. Trotzdem sollte nicht ausser Acht gelassen werden, dass die Tor-Software aus vielen Fachkreisen befürwortet wird. Es lohnt sich deshalb, die Funktionsweise von Tor zu analysieren, um mehr Substanz für ein Urteil zu gewinnen.

6.5 Wie funktioniert Tor?

Der Name *The Onion Routing* kommt nicht von ungefähr. Die verwendete Anonymisierungstechnik *Onion-Routing* lässt auf Grund ihrer Funktionsweise Vergleiche mit einer Zwiebel zu. Nachfolgend soll diese genauer erklärt werden. Dazu müssen zuerst ein paar Begriffe definiert sein:

- Client: Computerprogramm, das auf dem Rechner des Nutzers installiert und verwendet wird
- Tor-Server: Rechner im Tor-Netz, dessen Aufgabe es ist, Daten bzw. Anfragen zu empfangen und diese anschliessend an einen neuen Tor-Server weiterzuleiten
- Entry-Guard: Erster Tor-Server in der Kaskade, der die Daten bzw. die Anfrage direkt vom Nutzer bekommt und diesen somit noch kennt
- Exit-Node: Letzter Tor-Server in der Kaskade, der als Endpunkt auftritt und die Daten bzw. die Anfrage an das gewünschte Ziel weiterleitet

Im Folgenden werden die verschiedenen Stationen bzw. Phasen der Prozedur genauer beschrieben. Man bekommt vielleicht das Gefühl, dass der Ablauf aufwendig und zeitintensiv ist. Tatsächlich handelt es sich aber von Start bis Ende des Ablaufs lediglich um Millisekunden. Das Ganze hängt natürlich auch immer von der eigenen Verbindungsgeschwindigkeit, der konkreten Anwendung und der Performanz des Tor-Netzwerks ab.

1. Um Tor überhaupt nutzen zu können, muss als erstes der Client (Onion-Proxy) gestartet werden.
2. Dieser verbindet sich automatisch mit dem Tor-Netzwerk und lädt eine Liste aller verfügbaren Tor-Server herunter.
3. Ist die Liste komplett, entscheidet sich der Client für eine zufällige Route über die Tor-Server.

[29] heise, Linkverzeichnis, Link 27

4. Er baut nun eine verschlüsselte Verbindung mit dem ersten Tor-Server (Entry-Guard) der Route auf und sendet ihm die Daten.

5. Der Entry-Guard verschlüsselt die Daten erneut und sendet diese an einen weiteren Tor-Server.

6. Dieser tut genau das Gleiche noch einmal, worauf die Daten schliesslich zum letzten Server (Exit-Node) kommen.

7. Der Exit-Node entschlüsselt die Daten und leitet sie zum gewünschten Ziel weiter. Das ist die einzige Strecke im ganzen Ablauf, auf der die Daten nicht mehr verschlüsselt weitergeleitet werden.[30] [31]

Die versendeten Daten werden im Laufe der Kaskade in mehrere Verschlüsselungsschichten verpackt, damit die passierten Tor-Server nicht sehen können, worum es sich dabei handelt. Daher kommt auch der Name der Prozedur. Der finale Aufbau des Pakets gleicht einer Zwiebel mit mehreren Schichten, die schlussendlich wieder entpackt werden müssen. Diese Aufgabe übernimmt dann der Exit-Node. Generell gilt, dass die Daten immer drei Tor-Server passieren. Da die Tor-Server jeweils nur die Rechner links und rechts von sich kennen, weiss nur der erste Tor-Server über die Identität des Nutzers Bescheid. Der dritte und letzte Tor-Server kennt dann nur noch den Tor-Server, der ihm die Daten weitergeleitet hat, die Daten selbst und das finale Ziel.[32] Die zufällig gewählte Route wird vom Tor-Client ungefähr alle zehn Minuten gewechselt. So soll eine möglichst hohe Sicherheit gewährleistet werden.

Gefährlich wird es für den Nutzer dann, wenn jemand Eintritts- und Austrittsknoten kontrolliert. Die Anonymität wäre dann aufgehoben, da der *Lauscher* Ursprung, Ziel und Inhalt der Daten kennt.

[30] Tor Project, Linkverzeichnis, Link 28
[31] Wikipedia: Tor Netzwerk, Linkverzeichnis, Link 29
[32] Wikipedia: Onion Routing, Linkverzeichnis, Link 30

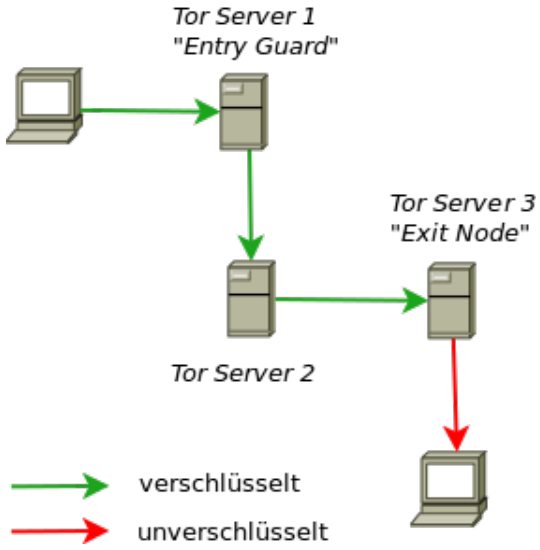

Abbildung 4: Tor

Beim Einsatz von Tor müssen zusätzlich gewisse Regeln beachtet werden, die es für eine erfolgreiche Anonymisierung einzuhalten gilt:

- Wann immer möglich, eine verschlüsselte Verbindung aufbauen (HTTPS)
- Soziale Netzwerke vermeiden, da sie die Identität preisgeben
- Web-Extensions, wie Java-Script und Flash-Cookies vermeiden (beides Technologien für spezielle Funktionalitäten und Multimediainhalte im Web)
- Keine persönlichen Angaben machen in Webformularen und dergleichen
- Tor nur dann benutzen, wenn es auch wirklich Sinn macht

Der letzte Punkt ist sehr wichtig, da die Anonymität durch Protokollierung gebrochen werden kann. Protokolliert ein Tor-Server genügend lang die passierenden Daten, kann nach durchschnittlich sechs Monaten die Identität aufgedeckt werden. Je öfter man den Dienst also braucht, desto mehr Informationen gibt man dem vermeintlichen Schnüffler. Die Zeit bis zum Aufdecken der Identität ist dabei stark von der Infrastruktur abhängig. Staatliche Behörden mit immensen Rechenzentren hätten folglich keine grossen Probleme, die Anonymität von passierenden Nutzern nach kurzer Zeit aufzuheben.[33]

6.6 Vor- und Nachteile

Tor hat ganz klare Vorteile aber auch bestimmte Nachteile, die nicht ausser Acht gelassen werden sollten. Nachfolgend werden die Vor- und Nachteile noch einmal kurz aufgelistet.

[33]heise, Linkverzeichnis, Link 31

Vorteile

- Relativ sicher
- Einfach einzurichten
- Open-Source

Nachteile

- Bei falscher Anwendung ineffektiv
- Zusammenhang mit amerikanischen Behörden (finanz. Unterstützung)
- Schlechter Ruf
- Noch relativ langsam

6.7 Experiment

6.7.1 Zielsetzung

Das Ziel war es, einen Computer in einen Access Point umzuwandeln und auf diesem Tor aufzusetzen. Der Access Point hat dabei die Aufgabe, jedes Gerät, das sich mit ihm verbindet, über das Tor-Netzwek ins Internet weiterzuleiten und so eine Anonymisierung der Verbindungsdaten zu ermöglichen. Als Computer kam ein Raspberry Pi zum Einsatz. Es handelt sich dabei um einen Einplatinen-Computer mit beschränkten Ressourcen, der sich vor allem wegen seiner geringen Grösse sehr gut für dieses Experiment eignete. Einzelheiten dazu sind im Handbuch beschrieben. Als Betriebssystem wurde eine für den Pi angepasste Version von Debian mit dem Namen *Raspbian* verwendet. Es handelt sich dabei um eine Linux-Distribution, die jedermann frei herunterladen und benutzen kann.

6.7.2 Installation

Die erste Hürde bei dem Experiment war die Wahl des WLAN-Adapters, welcher für die Access Point Funktionalität benötigt wird. Nicht jeder Adapter kann in den "Access Point Modus" versetzt werden, weshalb zuerst ein kompatibles Gerät angeschafft werden musste. Die restlichen Komponenten, die vor allem für den Betrieb des Raspberry Pis gebraucht werden, waren bereits vorhanden und schnell eingerichtet. Die Installation selbst funktionierte

ohne grosse Probleme. Man kann diese grob in zwei Schritte aufteilen. Der erste Schritt, das Einrichten des Raspberry Pis als Access Point, ist der aufwendigere der beiden und es gab diverse Konfigurationen, die vorgenommen werden mussten. Der zweite Schritt, das Installieren und Einrichten von Tor, war relativ einfach und schnell erledigt. Beim anschliessenden Testen des Tor Access Points wurde zudem noch die eine oder andere Einstellungsmöglichkeit entdeckt, die die Sicherheit von Tor zusätzlich erhöhen.

6.7.3 Fazit

Das Einrichten von Tor war gut bewältigbar und spannend dazu. Anhand von Hilfestellungen und Anleitungen im Internet liessen sich auch die oben beschriebenen Probleme gut lösen. Die benötigte Hardware - Raspberry Pi und Zubehör - kostet knapp unter 100 Franken. Wer Tor ausprobieren möchte, ohne die Software auf seinem Produktivsystem zu installieren, sollte auf diese Variante zurückgreifen.
Obwohl das Experiment erfolgreich war und Tor ein ernst zu nehmendes "Produkt" ist, kann dessen Einsatz an dieser Stelle nicht uneingeschränkt empfohlen werden. Dazu gibt es schlicht zu viele Ungereimtheiten. Ausprobieren und Kennenlernen lohnt sich aber allemal. Man kann viel dabei lernen und evtl. gibt es in Zukunft klarere Antworten auf die Fragen, die sich im Zusammenhang mit Tor stellen.

Das Handbuch, in dem der Installationsprozess detailliert beschrieben ist, befindet sich im Anhang oder kann einzeln heruntergeladen werden unter: `https://github.com/timofurrer/idpa/raw/master/pdfs/tor.pdf`

7 Cloud-Computing - Gewitterwolke oder Schattenspender?

Der Begriff Cloud bzw. Cloud-Computing wurden in den letzten paar Jahren immer populärer. Das Interesse an der mystischen Wolke und deren Konzept ist stetig gewachsen und ein Ende ist nicht in Sicht. Gerade in den letzten Monaten, während den Enthüllungen Edward Snowdens über die Machenschaften der Geheimdienste, bekam die Cloud aber auch einen bitteren Beigeschmack. Für Privatanwender und Unternehmen gleichermassen stellt sich die Frage, ob ihre Geheimnisse bei Anbietern wie Microsoft, Google oder Amazon sicher sind. Um diese Frage überhaupt beantworten zu können, muss man das Konzept von Cloud-Computing verstehen.

7.1 Was ist Cloud-Computing?

Cloud-Computing bezeichnet das Modell, IT-spezifische Dienste einem Kunden abstrahiert über ein Netzwerk zur Verfügung zu stellen und an dessen Bedarf anzupassen. Der Zugriff auf die Dienste soll dabei möglichst bequem und allgegenwärtig möglich sein. Die zur Verfügung gestellten Dienste können dabei von hardwareseitiger Natur sein (Rechenkapazitäten, Netzwerkkapazitäten, Rechenleistung) oder in Form von fertiger Software angeboten werden[34]. Die zuvor erwähnte Abstraktion ist dabei ein sehr wichtiger Punkt. Privatpersonen oder Unternehmen, die ein funktionierendes System oder eine funktionierende Software wünschen, ohne sich mit den technischen Aspekten auseinandersetzen zu müssen, kommen so voll auf ihre Kosten. Die Preise für die verschiedenen Dienste werden oft in Form von Abonnements angeboten und dabei zusätzlich an den Bedarf angepasst. Der Kunde erhält somit ein auf ihn zugeschnittenes Paket, das er nur noch einsetzen muss.

Das Konzept scheint aufzugehen und der Beweis dafür sind die unzähligen Firmen/Dienste, welche in den letzten Jahren, wie Pilze im Wald, aus dem Boden spriessen:

- SkyDrive (Online-Speicher, Microsoft)
- Office 365 (Online Office Suite, Microsoft)
- Google Drive (Online-Speicher, Google)
- Google Docs (Online Office Suite, Google)
- Dropbox (Online-Speicher, Dropbox Inc.)
- Evernote (Online-Notizverwaltung, Evernote Corporation)
- ownCloud (Online-Speicher, ownCloud Inc./Community)
- u.v.m.

7.2 Alltagsbeispiel – Microsoft Office 365

Eines der wohl am meisten verwendeten Programme in der Geschäftswelt und auch privat ist die Office Suite von Microsoft. Diese wird nun, dem Trend folgend, seit ungefähr zwei Jahren ebenfalls über die Cloud angeboten. Die Vorteile dabei scheinen, zumindest auf den ersten Blick, ein Kaufgrund zu sein:

- Stets neueste Version der Programme
- Auf bis zu 5 Geräten nutzbar

[34] csrc nist, Linkverzeichnis, Link 32

- Offline und online nutzbar, Installation nicht zwingend erforderlich
- 20 GB+ Online-Speicher, um Dokumente zu speichern und zu synchronisieren
- Monatlich oder jährlich bezahlbar
- 60+ „Skype-Minuten“ monatlich in alle Länder (Skype ist eine Telefonie-Software, welche über das Internet kommuniziert)[35]

Das Ziel ist es natürlich, Office hauptsächlich in Verbindung mit der Cloud zu nutzen. Nur dann kann man von überall seine Dokumente verwalten, ohne dass man die Programme auf den jeweiligen Computern installiert haben muss. Die Daten landen dann alle in der Cloud, womit eigentlich die Server von Microsoft gemeint sind. Microsoft bietet dafür einen eigenen Online-Speicher-Dienst namens *Sky-Drive* an. Ein Käufer von Office 365 erhält also kurz gesagt die volle Funktionalität, ohne sich viel mit technischen Fragen auseinandersetzen zu müssen. Das Angebot richtet sich dabei nicht nur an Privatpersonen, sondern auch an Firmen, wobei natürlich die Ausstattung und die Preise variieren.

Das obige Beispiel ist nur ein Angebot von vielen. Auf den ersten Blick scheint es auch nichts Schlechtes daran zu geben und natürlich schreiben die jeweiligen Anbieter die mit ihren Diensten verbundenen Risiken nicht auf ihre Flaggen. Schaut man aber genauer hin, tauchen Fragen auf, die gerade mit der zurzeit laufenden Debatte um Datenschutz und Anonymität im Netz vieles überschatten, was zuvor rosig wirkte.

7.3 Gewitterwolke statt Schattenspender?

Das grosse Wort, das bei Debatten über die Risiken von Cloud Computing im Raum steht und immer öfter auch ausgesprochen wird, lautet Datenschutz. Datenschutz kann je nach Betrachtungsweise verschiedene Dinge ansprechen:

- Schutz vor missbräuchlicher Datenverarbeitung
- Schutz des Rechts auf informationelle Selbstbestimmung
- Schutz des Persönlichkeitsrechts bei der Datenverarbeitung
- Schutz der Privatsphäre[36]

Einfach ausgedrückt ist das Ziel von Datenschutz der Schutz aller persönlichen Daten eines jeden Bürgers. Jeder Bürger soll selbst entscheiden können, welche seiner persönlichen Daten

[35] Microsoft Products, Linkverzeichnis, Link 33
[36] Wikipedia: Datenschutz, Linkverzeichnis, Link 34

wem zugänglich sind, zu welchem Zeitpunkt dies geschieht und in welcher Art. Die Frage lautet nun, ob Cloud-Dienste diesen Schutz gewährleisten können oder ob er allein in der Natur der Cloud-Dienste schon aufgehoben ist. Da die Anbieter und ihre Rechenzentren sich oftmals in einem anderen Land oder gar auf einem anderen Kontinent befinden als der Kunde, kann dieser kaum kontrollieren, was mit seinen Daten wirklich passiert. Die Anbieter müssen sich zudem meist an die Gesetze halten, die in dem Land gelten, in dem die Server stehen oder ihr Firmensitz sich befindet. Es kann also schnell einmal vorkommen, dass der Kunde und der Anbieter andere Vorstellungen davon haben, was Datenschutz in der Praxis bedeutet. Dem Kunden bleibt nichts anderes übrig, als entweder auf die Unternehmen zu vertrauen oder ganz auf die Dienste zu verzichten. Heute weiss man, dass es tatsächlich so ist, dass der Kunde nicht über alles in Kenntnis gesetzt wird, was mit seinen Daten passiert. Aus den von Snowden veröffentlichten Dokumenten geht hervor, dass beispielsweise die NSA immer wieder Daten direkt bei Unternehmen angefragt hatte. Gleichzeitig wurde den Unternehmen verboten, ihrerseits den Kunden über die Anfrage in Kenntnis zu setzen.[37]
Aber nicht nur Datenschutz ist im Zusammenhang mit Cloud-Computing wichtig. Die Informationssicherheit ist ebenfalls ein Punkt, der nicht vergessen werden sollte. Der Fokus liegt dabei mehr auf den Daten selbst als auf der Person dahinter. Folgende Fragen verlangen dabei nach einer Antwort:

Kann der Anbieter gewährleisten, dass

- Daten nicht von Dritten gelesen, gelöscht oder modifiziert werden?
- Daten nicht unabsichtlich verändert werden und getätigte Änderungen nachvollziehbar sind?
- Daten nicht verloren gehen oder nicht abrufbar sind auf Grund eines systembedingten Ausfalls?[38]

Es geht hier zwar mehr um technische Fragen als um politische, aber trotzdem muss es auf jede Frage eine Antwort geben, wenn man seine Daten in guten (oder eben nicht guten) Händen wissen will.

7.4 Was man tun kann - Nutzen und Aufwand

Hat man sich erst einmal ein Bild über die aktuelle Lage gemacht und ist sich der Chancen und Risiken von Cloud-Computing bewusst, bleibt die Frage, wie man denn nun fortfahren soll. Total auf die Dienste zu verzichten wäre eine Verschwendung von hilfreicher Technologie. Blindes Vertrauen hingegen wäre mit vielen Risiken verbunden. Es gibt zum Glück verschiedene Lösungsansätze, die nicht ganz so radikal sind. Man könnte zum Beispiel nur

[37] heise, Linkverzeichnis, Link 35
[38] Wikipedia: Informationssicherheit, Linkverzeichnis, Link 36

Unternehmen beauftragen, die ihre Server im selben Land haben, womit man mehr Kontrolle über das Geschehen hätte. Das klappt aber nur, wenn sich Polizei und die Geheimdienste besagten Landes an die jeweiligen Gesetze halten müssen und dies nachweislich auch tun. Schlägt man diesen Weg ein, bleiben aber immer noch gewisse Zweifel bestehen, die man vielleicht nie wird aus dem Weg räumen können. Möchte man ganz sichergehen, bleibt einem nichts anderes übrig, als eine eigene Cloud einzurichten. Auf Firmenebene braucht man dafür die entsprechende Hardware, geschultes Personal und Software, die die gewünschte Funktionalität zur Verfügung stellt. Die unmittelbaren Kosten können somit stark in die Höhe schnellen. Auf Dauer aber könnte sich die Investition allemal lohnen. Bei der privaten Nutzung verhält es sich ähnlich. Die Hardware kann aber in diesem Einsatzgebiet deutlich weniger leistungsfähig sein. Zudem könnte man zusammen mit Freunden oder Verwandten eine gemeinsame Cloud einrichten, um Kosten und Aufwand zu teilen. Ein gewisses technisches Know-How ist aber auch hier gefragt.

7.5 ownCloud - eigene Cloud leicht gemacht

ownCloud ist ein Programm, das einen ortsunabhängigen Speicherbereich zur Verfügung stellt, der über eine grafische Benutzeroberfläche verwaltet werden kann. Man kann Dateien verwalten, Kontakte & Kalender synchronisieren und je nach Bedarf noch vieles mehr[39]. Das Tolle an ownCloud ist - abgesehen von den bereits genannten Funktionen - dass es jeder kostenlos herunterladen und benutzen kann. Auch einer eigenen Cloud für ein Unternehmen stünde somit nichts im Wege. Es unterstützt alle gängigen Betriebssysteme und bietet ausserdem einen separaten Client, der auf den jeweiligen Rechnern oder gar dem Smartphone installiert werden kann, um noch bequemer mit der Cloud zu kommunizieren.
Besonders erwähnenswert im Zusammenhang mit dem Thema Datenschutz sind folgende Punkte:

- Mögliche Verschlüsselung der Daten auf dem Server
- Verschlüsselte Übertragung (SSL/TLS)
- Open-Source-Software

ownCloud ist wie Tor ein Open-Source-Programm. Das bedeutet, dass man neben dem ausführbaren Programm auch den Programmcode beziehen kann. Beides darf man nach Belieben kopieren, weitergeben oder modifizieren. Gewisse Einschränkungen oder Regeln, an die man sich zu halten hat, hängen dabei von der jeweils verwendeten Lizenz ab, unter der das Programm veröffentlicht wurde.[40] Die Eigenschaften von Open-Source-Software können je nach Anwendungsgebiet Fluch oder Segen sein. Einerseits kann dadurch jeder nachprüfen, was der Programmcode macht. Andererseits könnte aber genau diese Offenheit dazu genutzt werden,

[39] owncloud, Linkverzeichnis, Link 37
[40] Open Source, Linkverzeichnis, Link 38

um mutmasslichen Schadcode einzuschleusen. Es hängt dann von der Community, einem selbst oder dem Zufall ab, ob solche Hintertüren entdeckt und geschlossen werden. Würde man wirklich auf Nummer sicher gehen wollen, bliebe einem nichts anderes übrig, als den ganzen Code zu kontrollieren, was je nach Grösse des Programms unglaublich viel Zeit und somit auch Geld in Anspruch nehmen würde. Die Wahrscheinlichkeit von eingeschleustem Schadcode ist aber eher gering und sicherlich nicht grösser als bei proprietärer (geschlossener) Software.

Im Endeffekt hat ownCloud das Ziel, wartbar, kontrollierbar und frei zu sein. Die versprochenen Funktionalitäten decken dabei viele Bedürfnisse des "0815-Anwenders" ab und sprechen somit für das Programm als Alternative zu den Grossen im Geschäft.

7.6 Wie funktioniert ownCloud

ownCloud muss, wie die meisten Programme, auf einem Computer installiert werden. Der Einsatz der Cloud ist hierbei massgeblich für die Entscheidung, welche Hardware zum Einsatz kommt. Braucht man die Cloud nur für sich selbst, kann ein alter PC dienen, der anderweitig nicht mehr gebraucht wird. Soll aber eine Cloud für ein kleines Unternehmen, die Familie oder einen Verein aufgesetzt werden, macht es sicherlich mehr Sinn, aktuelle und performante Hardware zu verwenden. Natürlich braucht es neben der Cloud-Software selbst ein Betriebssystem, um die Anwendung überhaupt laufen zu lassen. Hierbei hat man ebenfalls die Wahl. ownCloud läuft unter Linux, OS X und Microsoft Windows. ownCloud braucht ausserdem noch andere Software-Komponenten, mit denen sie *zusammenarbeitet*. Doch auch diese sollten in den meisten Fällen frei einsetzbar sein.
Die Benutzung der Cloud bzw. der diversen Dienste ist ziemlich einfach. Jeder Benutzer kann mittels Webbrowser über ein sogenanntes *Webinterface* auf die Cloud zugreifen. Er kann beispielsweise Dokumente hoch- und herunterladen, Kontakte verwalten, Musik abspielen und vieles mehr. Inzwischen gibt es sogar Programme für Android- und iOS-basierte Smartphones und Tabletcomputer, mit denen man einfach auf die in der Cloud verwalteten Daten zugreifen kann. Die Verbindung zur Cloud wird dabei über das Netzwerk hergestellt. Je nach Einsatz und Einrichtung der Software, kann ownCloud nur im heimischen Netz, also den eigenen vier Wänden, oder aber auch von ausserhalb des Heimnetzwerkes angesprochen werden. Für den zweiten Fall braucht es aber zusätzliche Dienste, für die man in den meisten Fällen bezahlen muss.

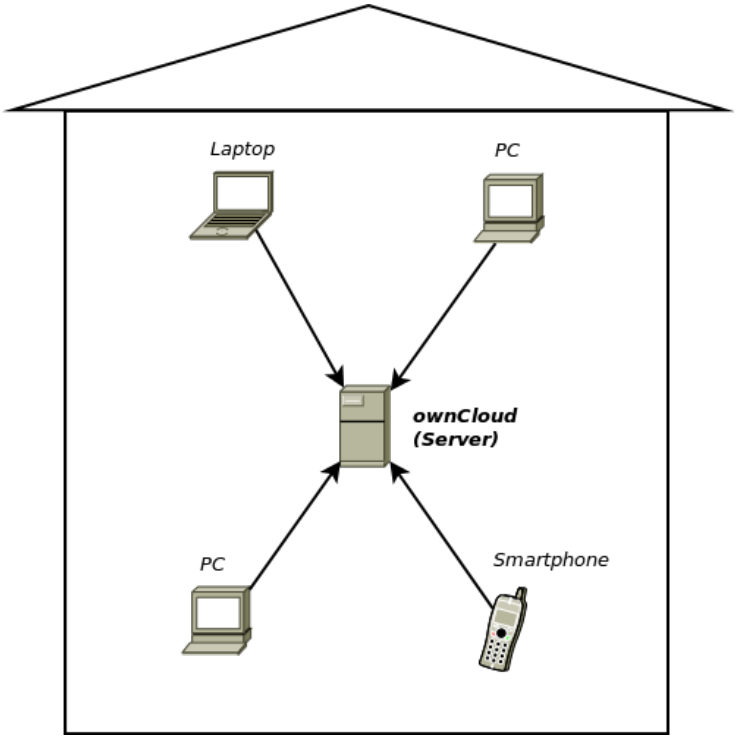

Abbildung 5: ownCloud im Heimnetzwerk

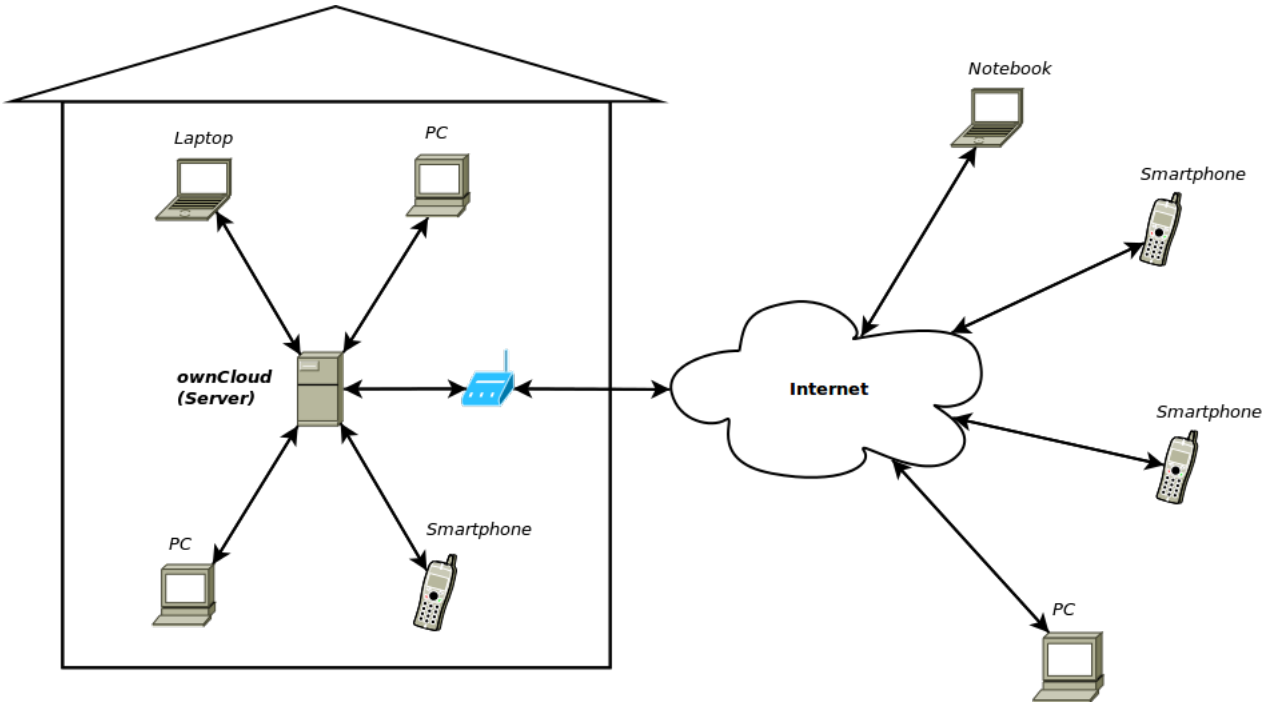

Abbildung 6: ownCloud im Heimnetzwerk & im Internet

7.7 Vor- und Nachteile

Grundsätzlich ist man bei ownCloud genau richtig, möchte man Herr seiner Daten sein. Was dadurch aber nicht vermieden werden kann ist eine gewisse Einarbeitungszeit bzw. ein gewisses technisches Know-How. Zusätzlich darf man auch nicht vergessen, dass die Cloud gewartet werden muss. Privatsphäre und Sicherheit haben ihren Preis und jede Privatperson bzw. jedes Unternehmen muss selbst entscheiden, wo die Prioritäten gesetzt werden. Die Cloud ist letztendlich nur so sicher, wie der Anwender sie gestaltet und selbst dann gibt es noch gewisse technologisch bedingte Einschränkungen. Nachfolgend werden noch einmal einige Vor- und Nachteile stichwortartig aufgelistet, bevor das Experiment und dessen Ergebnisse beschrieben werden.

Vorteile

- Anwender ist der Souverän
- Einsatz von Verschlüsselung bei Speicher und Übertragung
- Kostenlos
- Support durch Community
- Open-Source-Software

Nachteile

- Setzt gewisses technisches Know-How voraus
- Wartung
- Kauf eigener Hardware
- Verbindungsgeschwindigkeit und Komfort u.U. nicht so hoch wie bei grossen Anbietern

7.8 Experiment

7.8.1 Zielsetzung

Das Ziel war es, eine Cloud für das heimische Netzwerk einzurichten. Das bedeutet, dass man von zu Hause aus auf die Cloud und die angebotenen Dienste zugreifen kann. Ausserhalb des heimischen Netzes ist dies dann nicht mehr möglich. ownCloud kann aber mit ein bisschen Mehraufwand so konfiguriert werden, dass auch dies möglich ist. Will man die eigene Cloud

professionell nutzen, sollte dieser Mehraufwand definitiv betrieben werden. Als Computer kam zu Testzwecken ein Raspberry Pi zum Einsatz. Das ist ein Einplatinen-Computer mit eher beschränkten Ressourcen, der nicht für grössere Projekte geeignet ist. Als Betriebssystem wurde eine für den Pi angepasste Version von Debian mit dem Namen *Raspbian* verwendet. Es handelt sich dabei um eine Linux-Distribution, die jedermann frei herunterladen und benutzen kann.

7.8.2 Installation

Die Installation selbst ging erstaunlich einfach vonstatten. Es gibt in den weiten des Internets viele Anleitungen und Tipps, die einem die Arbeit deutlich erleichtern. Mit ein bisschen Fleiss und Geduld hat man das nötige Know-How so sehr schnell zusammen. Zuerst mussten die Hardware- und die Softwarekomponenten ausgewählt werden. In beiden Bereichen hat man einen gewissen Spielraum. Dann ging es auch schon los mit dem Aufsetzen des Betriebssystems. Einmal korrekt eingerichtet, konnten die Software-Komponenten installiert werden, die neben der Cloud-Software für eine korrekte Ausführung benötigt werden. ownCloud selbst benötigte dann den kleinsten Aufwand. Innerhalb kürzester Zeit war das Programm installiert und eingerichtet.

Standardmässig kann man sich mittels Webbrowser mit der Cloud verbinden. Die Bedienung ging dabei kinderleicht vonstatten. Es konnten mit wenigen Klicks alle Einstellungen vorgenommen und zusätzlich Funktionalitäten installiert werden.

7.8.3 Fazit

Eine eigene Cloud zu erstellen mit ownCloud ging einfacher als erwartet. Hat man das benötigte Know-How einmal gesammelt, sollte der Einrichtungs-Prozess auch für einen Laien kein grosses Problem sein. Möchte man noch keine produktive Umgebung einrichten, sondern ownCloud zu Testzwecken ausprobieren, reicht ein alter Computer vollkommen aus. Auch die Anschaffung eines Raspberry Pis ist an dieser Stelle empfohlen. Zusammen mit dem nötigen Zubehör liegt der Preis immer noch unter 100 Franken.
ownCloud hat einen sehr guten Eindruck hinterlassen. Die Bedienung ist leicht und ganz ähnlich, wie man es sich von anderen Programmen gewohnt ist. Das Programm bietet dabei eine Vielzahl von Zusatzdiensten, die man bei Bedarf nachinstallieren kann. Damit übersteigt der potenzielle Funktionsumfang von ownCloud sogar den der Grossen im Geschäft. Auch die Client-Programme für Computer, Smartphone und Tablets sind sehr praktisch. Möchte man Herr seiner Daten sein, ist ownCloud definitiv einen Versucht wert.

Das Handbuch, in dem der Installationsprozess detailliert beschrieben ist, befindet sich im Anhang oder kann einzeln heruntergeladen werden unter: `https://github.com/timofurrer/idpa/raw/master/pdfs/owncloud.pdf`

8 Rückblick

8.1 Sicherer Mailverkehr

Den Mailverkehr sicher zu gestalten sollte eigentlich eine Selbstverständlichkeit sein. Schliesslich geht es um private Nachrichten, die mehr oder weniger heikle Informationen beinhalten. Wie der Versuch gezeigt hat, ist es für einen Laien sehr schwierig oder gar unmöglich, einen eigenen Mail-Server einzurichten und zu betreiben. Das dafür nötige Know-How kann zwar mit viel Aufwand erarbeitet werden, jedoch lohnt sich dies in der Praxis oft nicht.
Die bessere bzw. einfachere Alternative ist, einen sicheren und vertrauenswürdigen Mailprovider ausfindig zu machen. Ein Provider in der Schweiz ist hierbei sicher keine schlechte Wahl. Ein grosser Kritikpunkt bleibt aber bestehen: Die volle Kontrolle über den Mail-Server hat nur der Provider selbst!
Eine dritte Möglichkeit wäre, eine Person oder eine Gruppe von Leuten mit gleichem Interesse zu finden. In der Gruppe ist es einfacher die finanziellen Mittel und das technische Know-How anzuschaffen, das es braucht, um einen sicheren Mail-Server zu betreiben.

8.2 Anonym Surfen

Das Risiko der Privatsphärenverletzung ist im World Wide Web beinahe omnipräsent. Die Karten liegen vollkommen offen - jeder Webseitenaufruf kann auf einen bestimmten Benutzer zurückgeführt werden. Das in dem Experiment verwendete Tor-Netzwerk ist eine gute Möglichkeit, die Privatsphäre im Netz zu erhöhen. Tor ist aber nur effektiv, wenn es korrekt eingerichtet, angewendet und mit weiteren Techniken und Programmen kombiniert wird. Wenn man sich bei der Einrichtung von Tor nicht hundert Prozent sicher ist, sollte man deshalb lieber auf Alternativen zurückgreifen..
Es gibt beispielsweise Erweiterungen für den Browser, die das Surf-Erlebnis sicherer gestalten. Eine kurze Recherche im Internet wird viele Möglichkeiten aufzeigen, wie genau man sich im Web anonymer fortbewegen kann.

8.3 Private Daten in der Cloud

Heutzutage werden Daten immer häufiger online gespeichert, also auf irgendwelchen Servern von grossen Providern abgelegt. Private, personenbezogene Daten könnten also potenziell eingesehen werden. Das Experiment, eine eigene Cloud einzurichten, hat gezeigt, dass es möglich ist, seine Daten selbst zu verwalten, ohne von grossen Dienstleistern abhängig zu sein. Es ist für einen Laien mit ein wenig Recherche gut umsetzbar und bringt einen grossen Ertrag für verhältnismässig wenig Aufwand. Das verwendete Programm ownCloud hat einen grossen Funktionalitätsumfang und kommt somit sehr nahe an grosse, kommerzielle Anbieter.
Ist einem der Aufwand trotzdem zu gross, gäbe es auch hier die Möglichkeit, einen vertrauens-

würdigen Anbieter zu wählen, der einem die gwünschte Funktionalität zur Verfügung stellt. Die Souveränität über die Daten wäre dann aber nicht mehr gegeben.

8.4 Fazit

Die Experimente haben gezeigt, dass es definitiv möglich ist, sich im Internet mehr Privatsphäre zu schaffen. Es ist letzendlich eine Frage des Aufwands und der persönlichen Prioritäten. Jemand mit technischen Vorkenntnissen und genügend Ehrgeiz hat die Möglichkeit mit eigenen Mitteln seine Privatsphäre zu schützen. Hat man aber nicht das technische Know-How oder den Ehrgeiz, sich dieses anzueignen, muss man sich auf Dienstleister verlassen. Aber auch da braucht es ein gewisses Mass an Eigeninitiative, um einen vertrauenswürdigen Provider ausfindig zu machen. Sofern es denn einen gibt. Die Frage *Anonymität - Ein Ding der Unmöglichkeit?* kann schlussendlich nicht mit *Ja* oder *Nein* beantwortet werden. Vielmehr geht es darum, sich bewusst im Netz fortzubewegen und die Möglichkeiten wahrzunehmen, die sich zum Schutz der Privatsphäre bieten.

9 Glossar - Fachbegriffe

Begriff	Bedeutung
WWW	Word Wide Web Bezeichnung für das Internet
PDF	Portable Document Format Plattform unabhängiges Dateiformat für Dokumente
NSA	National Security Agency Der Auslandsgeheimdienst der Vereinigten Staaten
GCHQ	Government Communications Headquarters Britische Regierungsbehörde, zuständig für Kryptographie, Datenübertragung und Fernmeldeaufklärung
Cloud	Internet Datenspeicher
MAC Adresse	Eindeutige Identifikationsnummer einer Netzwerkkarte
SSL	Secure Sockets Layer Verschlüsselungsverfahren
IT	Information Technology
Stasi	Ministerium für Staatssicherheit Ehemaliger Inlands- und Auslandsgeheimdienst der DDR
PC	Personal Computer
Firefox	Webbrowser von Mozilla
Google Chrome	Webbrowser von Google
Internet Explorer	Webbrowser von Microsoft
MTA	Mail Transport Agent
MDA	Mail Delivery Agent
POP3	Post Office Protocol Version 3
IMAP	Internet Message Access Protocol
GMX	E-Mail Provider
Backup	Datensicherung
PGP	Pretty Good Privacy
GPG	GNU Privacy Guard
IP	Internet Protocol
IP Adresse	Eindeutige Identifikationsnummer eines Internetanschlusses
DNS	Domain Name System Dient der Auflösung von Internet Domains
TOR	The Onion Routing Netzwerk zur Anonymisierung von Verbindungsdaten
HTTP	Hypertext Transfer Protocol Protokol zur Übertragung von Daten über ein Netzwerk
Linux	Unix Betriebssystem
Raspberry Pi	kreditkartengrosser Einplatinencomputer

10 Linkverzeichnis

Nr.	Link	Letzter Zugriff
1	http://www.heise.de/newsticker/meldung/Bericht-NSA-sammelt-Telefondaten-von-Millionen-US-Buergern-1883586.html	31.03.2014
2	http://www.spiegel.de/netzwelt/netzpolitik/nsa-raetselt-ueber-ausmass-der-snowden-enthuellungen-a-939145.html	31.03.2014
3	https://de.wikipedia.org/wiki/%C3%9Cberwachungs-_und_Spionageaff%C3%A4re_2013#Politik	31.03.2014
4	http://www.n-tv.de/politik/Google-kritisiert-Ausspaehung-durch-NSA-Gmail-Docs-und-Maps-offenbar-betroffen-article11640736.html	31.03.2014
5	http://www.heise.de/newsticker/meldung/NSA-sammelt-offenbar-fast-200-Millionen-SMS-pro-Tag-2087918.html	31.03.2014
6	http://www.heise.de/security/meldung/Kritik-an-Lavabits-Konzept-fuer-sichere-E-Mail-2041924.html	31.03.2014
7	http://www.spiegel.de/netzwelt/netzpolitik/dark-mail-alliance-lavabit-und-silent-circle-planen-e-mail-standard-a-931026.html	31.03.2014
8	http://www.heise.de/newsticker/meldung/NSA-Affaere-E-Mail-Anbieter-Lavabit-lieferte-sich-Katz-und-Maus-Spiel-mit-US-Justiz-1972173.html	31.03.2014
9	http://en.wikipedia.org/wiki/Lavabit	31.03.2014
10	http://www.briefmarkenverein-berliner-baer.de/vereinszeitung/241-1-stasi.htm	31.03.2014
11	https://de.wikipedia.org/wiki/Internet#Geschichte	31.03.2014
12	https://de.wikipedia.org/wiki/NCSA_Mosaic	31.03.2014
13	https://en.wikipedia.org/wiki/Black_box_%28disambiguation%29	31.03.2014
14	https://de.wikipedia.org/wiki/Gl%C3%A4serner_Mensch_%28Datenschutz%29	31.03.2014
15	https://de.wikipedia.org/wiki/Vertrauen_ist_gut,_Kontrolle_ist_besser!	31.03.2014
16	http://de.wikipedia.org/wiki/Mail_Transport_Agent	31.03.2014
17	http://de.wikipedia.org/wiki/Mail_Delivery_Agent	31.03.2014
18	http://de.wikipedia.org/wiki/POP3	31.03.2014
19	http://de.wikipedia.org/wiki/IMAP	31.03.2014
20	http://de.wikipedia.org/wiki/Top-Level-Domain	31.03.2014
21	http://de.wikipedia.org/wiki/Domain_Name_System	31.03.2014
22	http://www.neomailbox.com/	31.03.2014
23	http://www.zeit.de/digital/internet/2013-10/darknet-tor-netzwerk-vice	31.03.2014

24	http://www.nzz.ch/aktuell/digital/freedom-hosting-eric-eoin-marques-tor-1.18127905	31.03.2014
25	https://de.wikipedia.org/wiki/Tor_%28Netzwerk%29#Geschichte	31.03.2014
26	http://www.heise.de/security/meldung/Neue-Diskussion-ueber-Finanzierung-des-Tor-Projektes-1955851.html	31.03.2014
27	http://www.heise.de/security/meldung/Neues-von-der-NSA-Tor-stinkt-1972983.html	31.03.2014
28	https://www.torproject.org/about/overview.html.en#thesolution	31.03.2014
29	https://de.wikipedia.org/wiki/Tor_%28Netzwerk%29#Anonymes_Surfen	31.03.2014
30	https://de.wikipedia.org/wiki/Onion-Routing#Verschl.C3.BCsselungsschema	31.03.2014
31	http://www.heise.de/security/meldung/Tor-Benutzer-leicht-zu-enttarnen-1949449.html	31.03.2014
32	http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf	31.03.2014
33	https://office.microsoft.com/de-ch/products/microsoft-office-365-home-premium-kaufen-FX102853961.aspx	31.03.2014
34	https://de.wikipedia.org/wiki/Datenschutz	31.03.2014
35	http://heise.de/newsticker/meldung/PRISM-Skandal-Internet-Konzerne-fordern-von-US-Regierung-mehr-Transparenz-1919620.html	31.03.2014
36	https://de.wikipedia.org/wiki/Informationssicherheit	31.03.2014
37	http://owncloud.org/about/	31.03.2014
38	http://opensource.org/osd	31.03.2014

Abbildungsverzeichnis