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

SEMINARARBEIT

in der Fachrichtung
Wirtschaftsingenieurwesen mit
Schwerpunkt Informationsmanagement

Thema:

Anonymität im Netz, Mix Netzwerke, Onion Routing, der Tor-Browser, das Deep Web und das Darknet

Eingereicht von:	Marco Wessel (Wing101328)
	E-Mail: marco.wessel@online.de
Erarbeitet im:	7. Semester
Abgegeben am:	04. Juni 2018
Betreuer:	Prof. Dr. Michael Anders Fachhochschule Wedel Feldstraße 143 22880 Wedel Tel. (04103) 8048-24 E-Mail: an@fh-wedel.de

Inhaltsverzeichnis

I. Abbildungsverzeichnis

1 Einleitung

Heutzutage ist das Internet nicht mehr wegzudenken, doch wie bei allem gibt es auch hierbei eine schlechte Seite. Während wir im Alltagsleben in der realen Welt sehr viel Wert auf Anonymität legen, ist die Anonymität bei den meisten von uns im Netz nebensächlich. Viele wissen gar nicht, dass wir mit der alltäglichen Anonymität ein Grundrecht ausüben, und zwar das Recht auf informationelle Selbstbestimmung. Wäre dies nicht der Fall, müsste jedermann jederzeit sichtlich seinen Namen für andere an seinem Körper tragen. Da uns die Anonymität jedoch so wichtig ist tun wir dies nicht. Doch warum ist es uns im Netz „egal", dass andere unsere personenbezogenen Daten sehen und analysieren können? Ein gutes Beispiel hierfür, um dies zu verdeutlichen, ist der Nachrichtenaustausch im Netz und im Alltagsleben. Während wir damals vermehrt Briefe bei der Post abgegeben haben, die keiner automatisch registriert hat, schreiben wir heutzutage lieber E-Mails, wobei man den Mailverkehr lückenlos nachvollziehen kann. Der alte Menschheitstraum, Gedanken von anderen zu lesen, wird durch das Internet daher durchaus real. Man müsste sich nur mal vorstellen, all diese Daten in der Offline-Welt aufzuzeichnen. Wann und welche Geschäfte man gerne besucht, welche Vorlieben man hat und wie lange man sich dort aufhält. Dies wäre eine groteske Vorstellung, doch durch das Internet machbar.

Um sich genau vor so etwas zu schützen und sein Recht auf informationelle Selbstbestimmung wahrzunehmen, muss man selber dagegen etwas tun. Man sollte sich nicht darauf verlassen, dass die Unmengen an Daten, die im Internet permanent erzeugt werden, einen anonym machen, sondern sich aktiv dagegen wehren. Der Gesetzgeber hat dies auch bereits erkannt und im Teledienste-Datenschutzgesetz ein Recht geschaffen, sich anonym durch das Netz zu bewegen. Es darf nämlich kein Provider aufzeichnen, wann, wer und was man im Netz getan hat, außer es dient zu Abrechnungszwecken. Das Konzept klingt gut, doch leider halten sich nur wenige an diese Regeln (Bäumler and Mutius, 2013).

Daher muss man sich an technischen Vorkehrungen bedienen, wie unter anderem den Tor-Browser, um sein Recht auf informationelle Selbstbestimmung zu wahren.

2 Anonymität

2.1 Unterschied Pseudonym und Anonymität

An erster Stelle möchte ich gerne die Begriffe „Pseudonym“ und „Anonymität“ näher erläutern, da diese beiden Begriffe häufig als Synonym verwendet werden. Dies ist jedoch falsch, da sie unterschiedliche Bedeutungen haben. Laut § 3 Abs. 6 BDSG ist Anonymität *„das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.“*.

Ein Beispiel dafür sind Wahlen. Aufgrund dessen, dass sie geheim sind, sind sie somit auch anonym. Man kann letztendlich noch nachvollziehen, wer gewählt hat und wer nicht, jedoch lässt sich der Wahlzettel keiner bestimmten Person zuordnen. Das bedeutet, dass eine Identifizierung einer natürlichen Person nicht möglich ist(Datenschutzbeauftragter Info, 2018).

Eine Pseudonymisierung dagegen ist nach § 3 Abs. 6a BDSG *„das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren“*.

Ein Beispiel hierfür wäre eine E-Mail-Adresse wie itmaster9000@anbieter.com oder Nicknames in Foren. Hierbei hat man noch die Möglichkeit, die Daten so zusammen zuführen, dass man diese dem Originalnamen wieder zuordnen kann. Es ist quasi ein Deckname oder Künstlername.

Das heißt, nur weil jemand ein Pseudonym trägt, ist er nicht gleich automatisch anonym.

2.2 Vor- und Nachteile der Anonymität

Die Anonymität im Netz ist ein sehr umstrittenes Thema mit vielen Vor- und Nachteilen, die man auf beiden Seiten nachvollziehen kann. Einige Aspekte, die für die Anonymität im Netz sprechen, sind unter anderem:

- Whistleblowing (Aufdeckung von Menschenrechtsverletzungen, Korruption, etc.)
- politische Meinungsäußerung, ohne Verfolgung befürchten zu müssen
- objektive Einschätzung von Äußerungen, da das Gegenüber keinerlei soziale Hintergründe kennt, mit dem Nachteil fehlender Glaubwürdigkeit aufgrund unbekannter Identität
- Recherchen nach Themen, welche man lieber für sich behalten möchte
- Recht auf informationelle Selbstbestimmung

Wie bei allem gibt es auch hierbei Menschen, die die Anonymität im Netz missbrauchen. Daher sprechen folgende Aspekte dagegen:

- durch Anonymität sind Urheber einer Handlung nicht bestimmbar
- Austausch von illegalen Inhalten (beispielsweise Kinderpornographie oder verfassungsfeindliche Schriften)
- Herstellung von Kontakten für illegale Geschäfte
- Beeinträchtigung von Computerinfrastrukturen, wie DoS-Attacken (Denial of Service englisch für „Dienstverweigerung“) auf Webseiten (Computerbetrug, 2011)

Man sollte versuchen, beide Seiten abzuwägen und für sich selbst entscheiden, ob man seine persönlichen Daten für jedermann im Internet darlegen möchte oder nicht.

3 Internet

Das Internet ist im Prinzip eine Vielzahl von kleineren und größeren Computern, die über ein inhaltliches Protokoll, das sogenannte TCP/IP (Transmission Control Protocol /Internet Protocol) Daten austauschen (Brombach, 1999, pp. 20–24).

Zu Beginn des Internets gab es das Arpanet (Advanced Research Projects Agency Network). Dies war ein Netzwerk von Computern, das in den sechziger Jahren dazu diente, die militärische Kommunikation für den Fall eines atomaren Krieges zu sichern. Aufgrund dessen, das viele Universitäten und Forschungseinrichtungen sich dabei einbrachten, entwickelte sich das Netz im Laufe der Jahre zu einem globalen Rechnerverbund, dem Internet. Das World Wide Web (WWW) ist nicht

gleichzusetzen mit dem Internet. Es ist ein Dienst im Internet und ermöglicht uns, Seiten mit Texten, Grafiken oder Videos aufzurufen und auszutauschen (Gruenderszene, 2010).

3.1 Welche Informationen gebe ich beim Surfen preis?

Wer unbekümmert im Internet surft weiß meist gar nicht, was der Gegenüber all für Informationen von einem erhält. Dieses kann man mit vielen unterschiedlichen Websites testen, unter anderem mit www.wieistmeineip.de oder www.anonym-surfen.com. Um zu verdeutlichen, welche Informationen preisgegeben werden, habe ich diesen Test einmal durchgeführt.

Abbildung 1: *Informationen ohne Proxy*

Wie man in *Abbildung 1* erkennen kann, sieht mein Gegenüber welche IP-Adresse, welches Betriebssystem, welchen Browser ich besitze, in welchem Land ich mich zur Zeit befinde – letzteres erfährt er durch die IP-Adresse und auf anderen Websites noch viele weitere Informationen. Einige Internetseiten, die solche Prüfungen anbieten, können den eigenen Standort sogar bis auf 30 Km bestimmen.

Doch gerade die IP-Adresse eines Rechners ist wie ein Fingerabdruck. Das Kürzel IP steht für Internet Protocol und identifiziert jedes Gerät innerhalb eines Datennetzwerkes. Jeder Computer, der über das Internet kommuniziert, benötigt eine IP-Adresse, um Daten auszutauschen (T-Online, 2012).

Eine IP-Adresse ist nach dem alten Standard von IPv4 immer gleich aufgebaut. Ein Beispiel hierfür ist die IP-Adresse 192.36.27.6. Vier Zahlen zwischen 0 und 255, getrennt durch einen Punkt. Jedoch lässt sich mit diesem System nur eine begrenzte Anzahl von Kombinationen darstellen, welche auch bereits fast aufgebraucht sind. Daher findet man immer häufiger die neue Version IPv6. Mit diesem Format stehen nun $3{,}4 \times 10^{38}$ (340 000 000 000 000 000 000 000 000 000 000 000) IP-Adressen zur

Verfügung. Statt einer Adresslänge von 32-Bit ist heutzutage eine Länge von 128-Bit möglich. Die Schreibweise für IPv6 ist hexadezimal und besteht aus acht Blöcken, die durch einen Doppelpunkt getrennt werden. So wird aus der IPv4 192.36.27.6 das neue Format IPv6 2A03:F85:8::6 (Hessling, 2017).

Abbildung 2: *Informationen mit Proxy*

Um seinen „Fingerabdruck“ zu verschleiern und all seine persönlichen Daten an weitere preiszugeben, nutzt man Proxy Server – wie ein Proxy funktioniert wird in Abschnitt 4.2.1 behandelt. Nur so viel. Ein Proxy dient als Vermittler und gibt die Anfrage mit einer anderen IP-Adresse weiter. Ich habe daher denselben Test am gleichen Rechner zur selben Zeit durchgeführt, während ein Proxy-Server dazwischengeschaltet war. Wie nun in *Abbildung 2* gut zu erkennen ist, unterscheiden sich die Informationen zur *Abbildung 1* komplett. Das liegt daran, dass nun nicht mehr die eigene IP-Adresse lokalisiert wird, sondern die des Proxy-Servers. Daher ist nun anonymes Surfen, ohne Informationen über sich preiszugeben, möglich.

3.2 Deep Web und Darknet

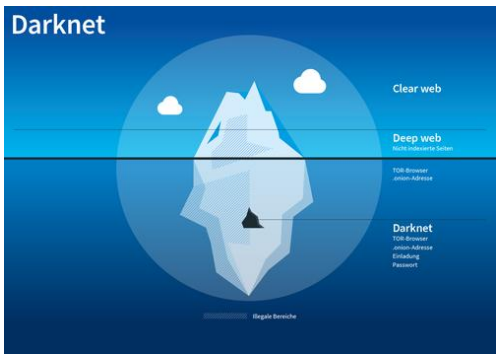

Abbildung 3: *Darknet*

Auch diese Begriffe werden häufig als Synonym verwendet, doch auch diese beiden Begriffe haben unterschiedliche Bedeutungen. Allgemein kann man sagen, dass man unter dem Deep Web alle Webseiten versteht, die nicht von den freizugänglichen Suchmaschinen, wie beispielsweise Yahoo, Bing oder Google, gefunden werden können. Ein Beispiel hierfür sind Intranets von Firmen (How to inter, 2010).

Das Darknet hingegen ist ein anonymisiertes und verschlüsseltes P2P-Netzwerk (Peer-to-Peer-Netzwerk), bei dem man eine spezielle Software benötigt, um Zugang zu bekommen. Das englische Wort *Peer* steht für einen Gleichrangigen bzw. Ebenbürtigen. Peer-to-Peer bezeichnet daher ein Treffen unter Gleichen. Es gibt keine Hierarchie - sprich keiner kontrolliert oder gibt Anweisungen. Es ist daher ein Netzwerk, das gleichrangig miteinander verbindet ohne Instanzen und Kontrollen. Jeder Teilnehmer kann Anbieter und Konsument sein. Bereiche, bei dem das P2P-Netzwerk zum Einsatz kommen, sind zahlreiche Filesharing-Services oder Blockchains. Dabei werden die Daten direkt von Peer zu Peer kopiert und stehen nicht auf einem zentralen Server zur Verfügung (Mahlmann and Schindelhauer, 2007, p. ff. 1)

4 Tor-Browser

Tor ist ein Programm, welches man auf seinem Computer ausführen kann, um anonym im Internet zu surfen und Zugang zum Darknet zu bekommen. Die Abkürzung „Tor“ steht für „The Onion Router“ und leitet sich von der Technologie des Schichten-Prinzips ab. Mit diesem Prinzip versprechen die Entwickler des Tor-Netzwerkes dem Benutzer Anonymität im Internet und unterbinden somit auch „trafficanalysis“. Ursprünglich wurde Tor, im Jahre 2000 an der University of Cambridge, für die U.S. Navy entwickelt im Hinblick auf den Schutz der Regierungskommunikation. Zwei Jahre später wurde die erste Alpha Version veröffentlicht. Im Jahr 2006 wurde dann eine non-profit Organisation gegründet mit dem Namen „The Tor Inc.“, welche für die Wartungsarbeiten im Tor-Netzwerk zuständig sind (Mey, 2017).

4.1 Wer nutzt Tor?

Heutzutage wird Tor von (fast) jedem verwendet, nur nutzt jede Benutzergruppe Tor aus unterschiedlichen Gründen. Normale Leute, wie Sie und ich nutzen Tor, um die eigene Privatsphäre zu schützen und nicht jedem Zugang zu unseren Daten zu geben. Wir schützen uns somit vor unseriösen Unternehmen, die vorhaben, unsere Daten weiter zu verkaufen oder für Forschungen zu benutzen, obwohl wir nicht zugestimmt haben. Auch in Ländern, in denen es Zensuren gibt, kann man diese damit umgehen. Somit hat man die Möglichkeit, auch sensible Themen, wie beispielsweise Krankheiten, anonym zu recherchieren oder sich Videoinhalte anzuschauen, die das Land verbietet.

Auch Journalisten bedienen sich an dem Programm, um ihre Privatsphäre zu schützen und sich und ihre Quellen in Sicherheit zu wissen. Außerdem nutzen Journalisten, welche sich in sogenannten „Internet Black Holes“ befinden, Tor, um staatliche Propaganda und gegensätzliche Standpunkte zu recherchieren, Geschichten mit nicht staatlich kontrollierten Medien einzureichen und die persönlichen Konsequenzen intellektueller Neugier zu vermeiden.

Tor wird außerdem durch viele Aktivisten und Whistleblower genutzt. Gerade diese Gruppe von Menschen befindet sich ständig in der Angst der Überwachung. Allerdings haben sie mit Tor die Möglichkeit, anonym für die Allgemeinheit wichtige Informationen aus einem geheimen bzw. geschützten Zusammenhang an die Öffentlichkeit zu bringen. Menschenrechtsaktivisten können so ihre Regierungs- und Unternehmenszensuren umgehen und Whistleblowern gibt es die Möglichkeit Gerechtigkeit ohne persönliche Auswirkungen zu erlangen.

Ursprünglich wurde die Software extra für das Militär entwickelt mit dem vorrangigen Ziel, die Regierungskommunikation zu schützen. Heutzutage wird Tor allerdings für eine große Bandbreite genutzt, unter anderem für Soldaten, die ihren Standort verschleiern oder Operationen schützen müssen, um keinen physischen Schaden zu erleiden (The Tor Project, no date).

4.2 Funktionsweise

Bevor ich die Funktionsweise von Tor – das sogenannte „Onion Routing“ – erörtere, möchte ich vorerst einige Begriffe erläutern.

4.2.1 Proxy-Server

Zunächst einmal möchte ich erklären, was ein Proxy ist und warum dieser so wichtig für das anonyme Surfen ist. Dafür muss man wissen, was passiert, wenn man eine Website aufruft. Dabei schickt der Computer eine Anfrage mit der eigenen IP-Adresse an den Webserver, der die gewünschte Website verwaltet. Der Webserver speichert die IP-Adresse des eigenen PCs und übermittelt die geforderten Daten. Mit diesen übermittelten Daten wird dann die Website aufgebaut.

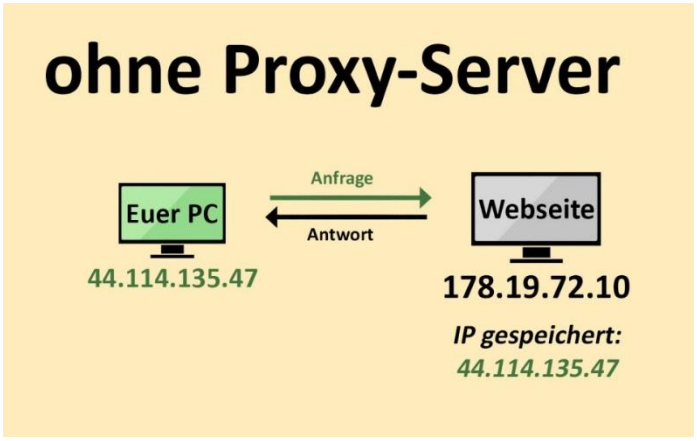

Abbildung 4: *Verbindungsaufbau ohne Proxy Server*

Somit kann der Server anhand der IP-Adresse eindeutig identifizieren, wer die gewünschten Daten angefragt hat.

Der Proxy fungiert, wie in *Abbildung 5* gut zu sehen, als Vermittler. Dieser Proxy-Server hat eine andere IP als die vom eigenen PC. Die Anfrage wird daher nicht direkt über die eigene IP-Adresse gestellt, sondern geht erst an den Proxy-Server. Dieser leitet die Anfrage dann mit seiner eigenen IP an den Webserver weiter und speichert nur die IP vom Proxy. Das bedeutet, dass der Webserver auch nicht die Antwort direkt an den eigenen PC übermittelt, sondern erst wieder über den Proxy-Server (GIGA, 2017).

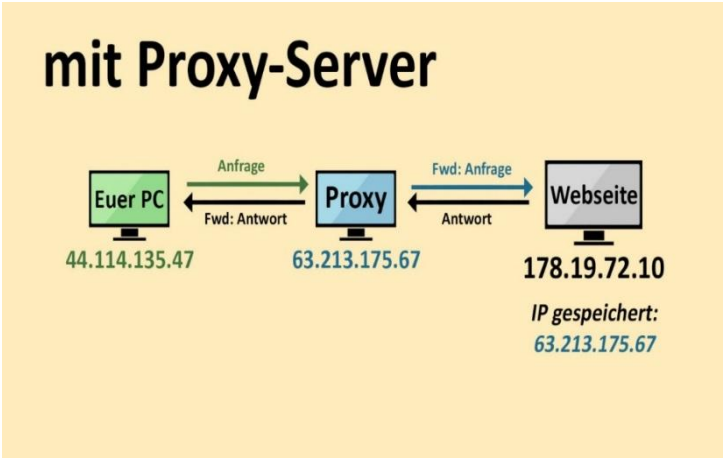

Abbildung 5:*Verbindungsaufbau mit Proxy Server*

Es kann unter Umständen sein, dass die Proxys die eigene IP-Adresse speichern. Daher gilt, je mehr Proxys man zwischen sich und dem Webserver zwischenschaltet, desto schwerer ist eine Rückverfolgung. Der große Nachteil daran ist allerdings, dass

die Internetgeschwindigkeit immer langsamer wird, je mehr Proxys man dazwischenschaltet. Ein Proxy ist daher sehr wichtig, damit man keine direkte Verbindung zu seinem eigenen PC herleiten kann.

4.2.2 Mix-Netzwerke

Das eigentliche Konzept des Mix-Netzwerkes basiert auf einem Verschlüsselungsverfahren von Chaum, welches jede Nachricht einzeln durch eine Kombination von Verschlüsselungsverfahren sichert. Das Ziel eines Mix-Netzwerks ist es, die Kommunikation der Teilnehmer innerhalb des Netzwerkes geheim zu halten. Dies wird dadurch sichergestellt, dass zwischen dem Client und dem Server mindestens zwei Mix-Server dazwischengeschaltet sind, wie in *Abbildung 6* zu sehen. Je mehr Mixe man hat desto höher ist zwar die Sicherheit, allerdings erhöht sich ebenfalls die Latenz.

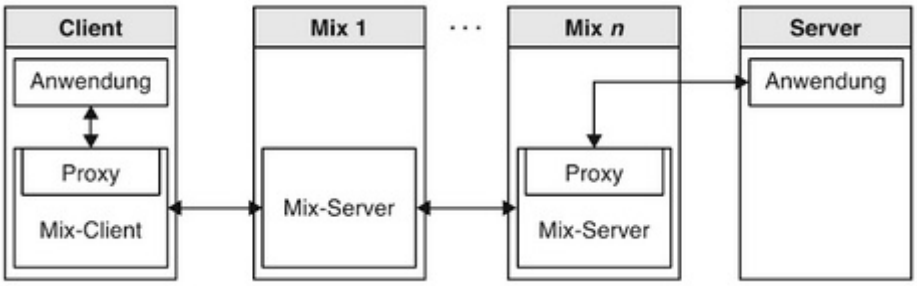

Abbildung 6:*Schematische Architektur eines Mix-basierten Anonymitätsdienstes*

Die Mix-Server kennen nur ihren direkten Vorgänger und Nachfolger, sie kennen niemals die komplette Route. Dies schafft, unter der Prämisse, dass die Mix-Server unabhängig von einander sind, Senderanonymität und Beziehungsanonymität. Der Mix-Server dient daher, wie der Proxy-Server, als Nachrichtenübermittler. Nur das bei einem Mix-Netzwerk der Nachrichtenaustausch verschlüsselt ist.

So wird beispielsweise bei drei Mix-Servern die Nachricht zuerst mit dem öffentlichen Schlüssel des letzten Mix-Servers verschlüsselt und danach wird der resultierende Chiffretext ein weiteres Mal verschlüsselt, allerdings mit dem öffentlichen Schlüssel des vorletzten Mix-Servers. Auch dieser resultierende

Chiffretext wird erneut verschlüsselt durch den ersten Mix. Die Nachricht ist somit über drei Instanzen verschlüsselt. Als nächstes wird die Nachricht der Reihe nach entschlüsselt wobei jeder Mix-Server seinen privaten Schlüssel dafür nutzt und die entschlüsselte Nachricht danach weiter an den nächsten Mix-Server leitet. Der letzte Mix-Server erhält schließlich den Klartext und übermittelt die Nachricht an den Empfänger (Herrmann, 2016, pp. 230–240).

Die Funktion eines Mix-Servers ist es daher, eingehende Nachrichten gleicher Art zu filtern, Nachrichten gleicher Länge von unterschiedlichen Absendern in einem Schub zu puffern, diese dann umzucodieren und anschließend umzusortieren, sodass man die Reihenfolge der eingehenden Nachrichten nicht nachvollziehen kann. Anschließend wird der Schub an den nächsten Mix weitergeleitet (TU Dresden, 2012).

Mehrere Mix-Server, die hintereinander geschaltet sind, nennt man Mix-Kaskade. Dabei unterscheidet man zwischen einer festgelegten Mixkaskade und einer freien Mixkaskade, wie dies beim Tor-Netzwerk der Fall ist.

4.2.3 Onion Routing

Das Wort *Onion* kommt aus dem Englischen und steht für Zwiebel. Dieser Begriff leitet sich vom verwendeten Verschlüsselungsschema ab, indem ein virtueller Kanal erstellt wird, der durch mehrere andere Knoten verläuft. Diese Knoten entfernen jeweils eine „Hülle“ des mehrfach verschlüsselten Pakets von der sogenannten *Onion*.

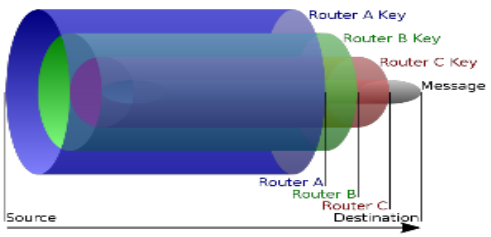

Abbildung 7: *Verschlüsselungsprinzip*

Tor nutzt dieses Verschlüsselungsverfahren und wählt dabei immer eine Route die über drei Nodes (auf Deutsch Knoten) verläuft. Der erste Node ist der sogenannte Entry-Node, der zweite Node ist der Middle-Node und der letzte Node ist der Exit-Node. Für die Anzahl von genau drei Nodes entschied man sich aufgrund dessen, da dies das optimale Verhältnis zwischen hoher Sicherheit und geringer Latenz ist. Um

nun eine anonyme Verbindung zum Server aufzubauen verbindet sich als erstes der Tor-Client, in dieser Veranschaulichung *Alice*, mit dem Tor-Netzwerk *Dave* und lädt dabei eine Liste mit allen nutzbaren und vorhandenen Tor-Servern runter. Wie in *Abbildung 8* zu sehen, weiß der Tor-Client nun, welche Tor-Server vorhanden sind und welche er nutzen kann.

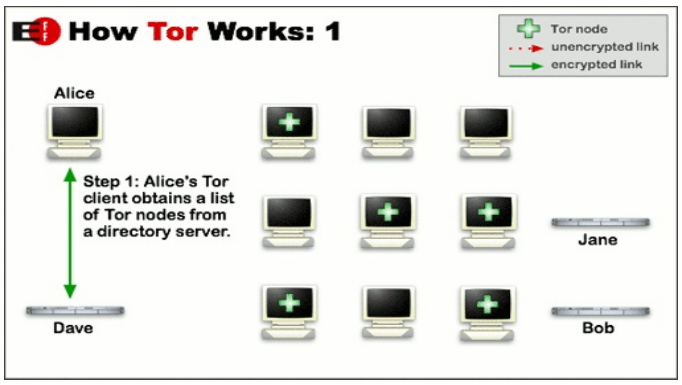

***Abbildung 8**: How Tor Works 1*

Wenn nun *Alice* wie in *Abbildung 9* die Website von *Bob* erreichen möchte, wählt der Tor-Client, wie bereits erwähnt, eine Route von genau drei Servern, die jeweils nur ihre direkten Vor- und Nachfolger und nie die gesamte Route kennen.

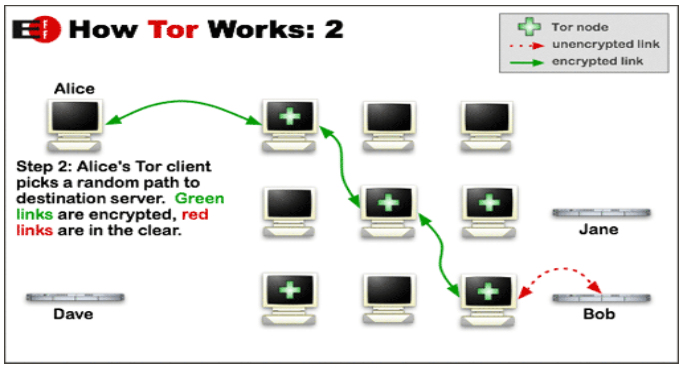

***Abbildung 9:** How Tor Works 2*

Für jeden Node wird ein eigener Satz von Verschlüsselungsschlüsseln erstellt. Dies geschieht nachdem Alice die Verbindung zum Verzeichnis aufgebaut hat und die öffentlichen Schlüssel der Nodes erhalten hat. Alice erstellt für den ersten Node einen Diffie-Hellmann-Wert. Diesen Wert verschlüsselt sie dann mit Hilfe des öffentlichen Schlüssels vom ersten Mix und verschickt den chiffrierten Wert auch an diesen. Nach dem der erste Mix den chiffrieren Wert erhalten hat entschlüsselt er diesen mit dem privaten Schlüssel und berechnet seinen eigenen Diffie-Hellmann-

Wert. Mittels des Diffie-Hellmann-Verfahrens kann der erste Node somit einen symmetrischen Schlüssel generieren und erstellt anschließend für diesen Schlüssel einen Hash-Wert. Dieser Hash-Wert und der vom ersten Node berechnete Diffie-Hellmann-Wert werden vom ersten Mix zurück an Alice versendet, damit sie ebenfalls mit Hilfe des Diffie-Hellmann-Verfahrens den symmetrischen Schlüssel erzeugen kann. Um zu prüfen, ob beide denselben Schlüssel erstellt haben, generiert Alice ebenfalls für den symmetrischen Schlüssel einen Hash-Wert und vergleicht diesen mit dem zugeschickten Hash-Wert vom ersten Node. Wenn die Hash-Werte identisch sind, kann Alice ihre Nachricht mit dem symmetrischen Schlüssel verschlüsseln. Dieser Vorgang findet für alle drei Nodes statt, um für jede Verbindung ein symmetrisches Schlüsselpaar zu besitzen (Petrlic and Sorge, 2017, pp. 54–60).

Alle 10 Minuten oder sobald die Website gewechselt wird, wird eine neue zufällige Route gewählt. Dies dient dazu, die Sicherheit noch weiter zu erhöhen um es potenziellen Angreifern zu erschweren, die Nachrichten zu verfolgen (The Tor Project, no date-a). (*Abbildung 10*)

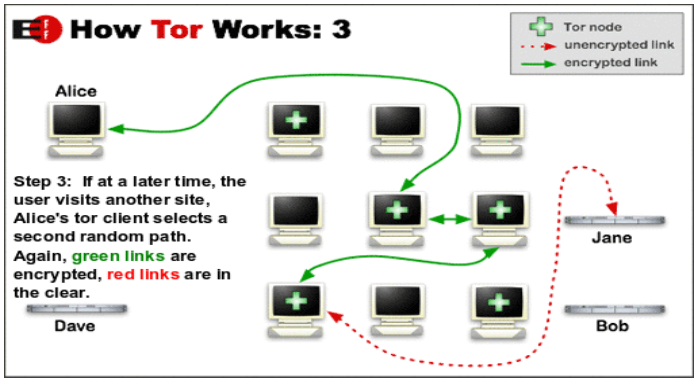

Abbildung 10: *How Tor Works 3*

4.3 Vor- und Nachteile von Tor

Die Vorteile von Tor liegen auf der Hand. Tor bietet die Möglichkeit, anonym im Netz zu surfen ohne private Daten weiterzugeben. Es ist einfach zu installieren und denkbar leicht zu bedienen. Die Nachteile sind allerdings auch nicht außer Acht zu lassen. Ein wirklich schnelles Surfen ist mit Tor nicht möglich und an große Downloads ist gar nicht erst zu denken. Dies liegt allerdings an den zahlreichen Sprüngen, durch die die Daten weitergeleitet werden, wie in *Abbildung 11* zu erkennen.

Abbildung 11: *Tor Kanäle*

5 Anleitung

In diesem Abschnitt möchte ich zeigen, wie einfach es ist, den Tor-Browser zu installieren und möchte erste Einblicke zur Nutzung geben.

5.1 Installation

Den Tor-Browser kann man am besten herunterladen bei :

https://www.torproject.org/projects/torbrowser.html.en

Dort gibt es – wie in *Abbildung 12*– Versionen für Windows, macOS, Linux und Versionen für das Smartphone. Einfach das benötigte Betriebssystem und die gewünschte Sprache auswählen und den Download starten.

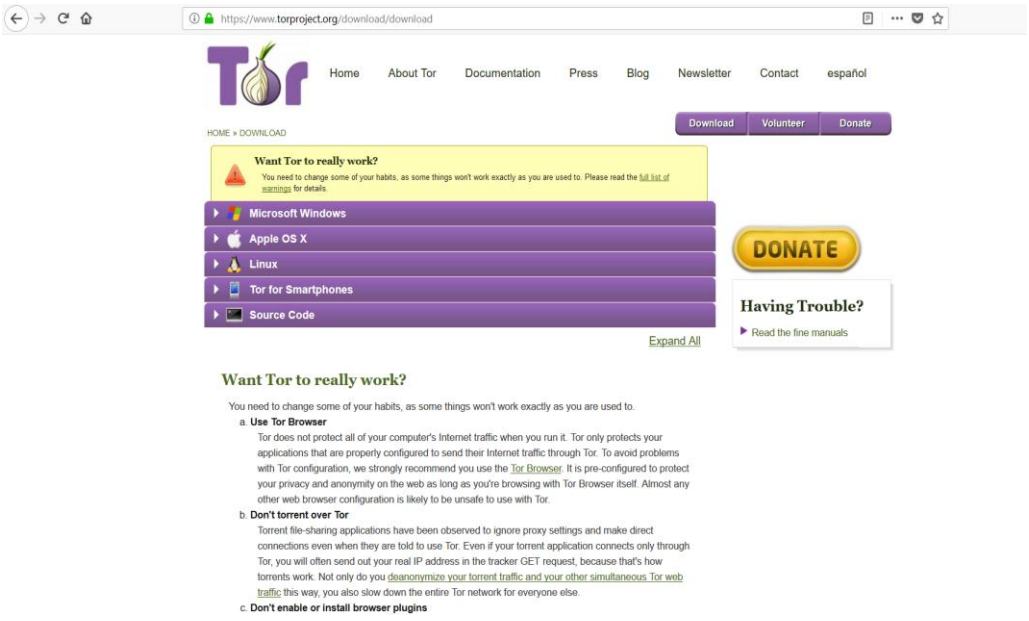

Abbildung 12: *Tor Download*

Bei Windows muss man nach dem Download die Datei ausführen. Dabei startet ein Installationsprogramm, mit dem man die Möglichkeit hat, das Programm in der gewünschten Sprache zu installieren und ein Verzeichnis anzugeben, wohin der Tor-Browser installiert werden soll. Die Installation ist relativ schnell durchgeführt. Am Ende der Installation hat man die Möglichkeit einen Short-Cut auf dem Desktop zu hinterlegen. (siehe *Abbildung 13*)

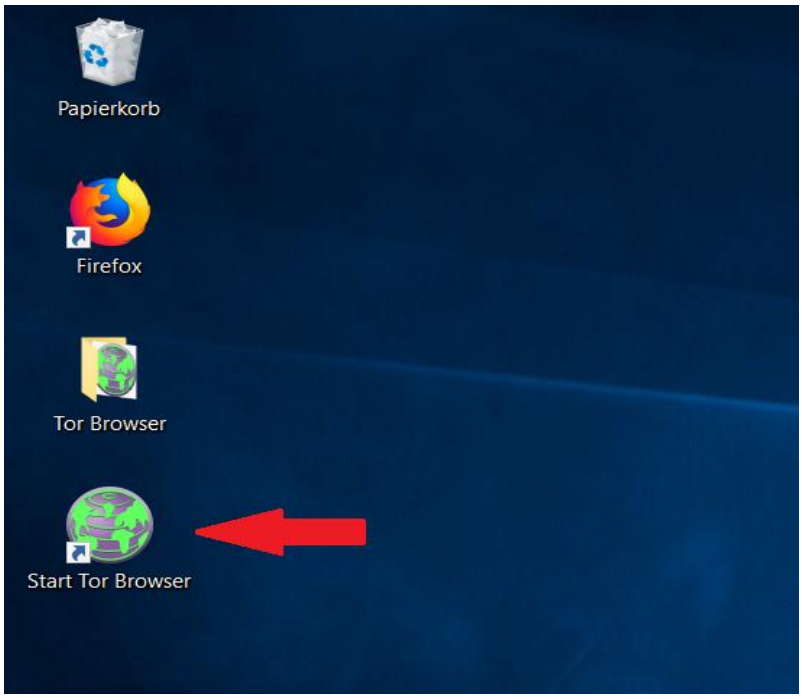

Abbildung 13: Tor-Browser

Beim ersten Starten des Tor-Browsers wird gefragt, ob man eine spezielle Konfiguration benötigt, da der Internetanschluss eingeschränkt ist. Bei den meisten Internetanschlüssen ist dies nicht der Fall und man klickt auf „Verbinden“,

Abbildung 14: Verbindung zu Tor

Danach braucht der Tor-Browser etwas Zeit, sich mit dem Tor-Netzwerk zu verbinden. Falls sich dieser Vorgang außergewöhnlich lange hinzieht, empfiehlt es sich, das Programm zu schließen und neu zu starten.

Sobald der Verbindungsvorgang vollständig durchgeführt wurde, erscheint – wie in *Abbildung 15* zu sehen – der Tor-Browser und das anonyme Surfen kann beginnen.

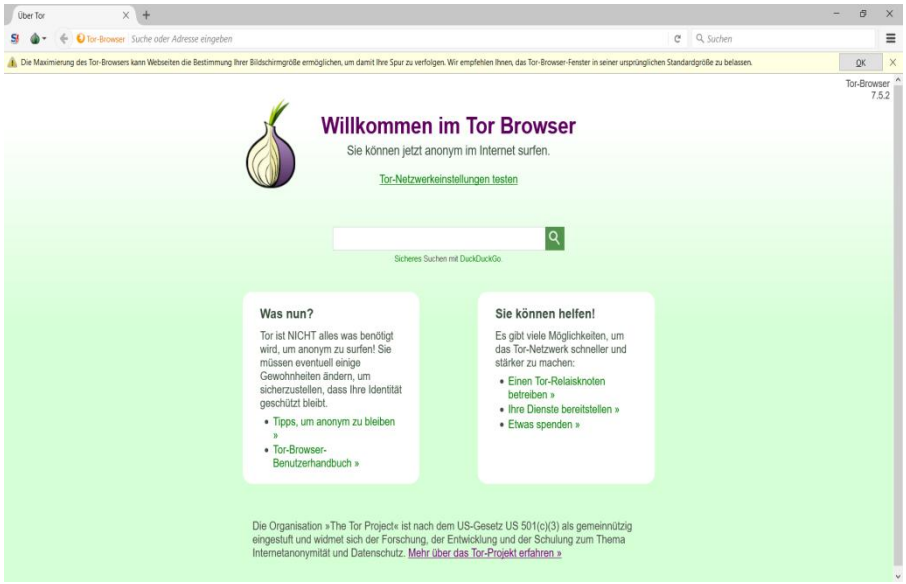

Abbildung 15:*Willkommen bei Tor*

5.2 Bedienung

Der Tor-Browser funktioniert im eigentlichen Sinne wie ein normaler Browser. Um wirklich vollständig anonym im Internet zu surfen, stellt die Website Tor-Projekt Sicherheitshinweise zur Verfügung, die man im besten Falle auch einhalten sollte. Dies findet man unter folgendem Link:

https://www.torproject.org/download/download-easy.html.en#warning

Ansonsten werden, wie im Inkognitomodus auch, keine Verläufe und Cookies gespeichert.

Man findet mit dem Tor-Browser ganz normale Internetseiten, die man mit anderen Browsern auch findet. Mit Hilfe von Tor kann man allerdings auch auf die .onion-Links zugreifen. Ein Beispiel für ein .onion-Link ist dieser

http://3g2upl4pq6kufc4m.onion/. Solch eine Adresse kann man nicht ohne Weiteres finden, daher haben einige Portale eine Auflistung von .onion-Links erstellt. Viele dieser Links sind allerdings nicht mehr aktiv oder momentan offline. Diese Portale findet man auch mit einem normalen Browser. Beispiele hierfür sind unter anderem:

https://thehiddenwiki.org/

http://the-hidden-wiki.com/

https://securityzap.com/massive-deep-web-links-2015-updated-june-2015/

Eine Auflistung verschiedener Foren habe ich hierunter gefunden:

https://www.deepwebsiteslinks.com/deep-web-forums-links/

Man hat ebenfalls die Möglichkeit Suchmaschinen mit dem Tor-Browser zu nutzen. Die gängigste ist DuckDuckGo (http://3g2upl4pq6kufc4m.onion/). Diese liefert einem Suchergebnisse, ohne dabei den Nutzer zu analysieren – dieser bleibt völlig anonym– allerdings sucht sie nur das Clearweb ab. Im Übrigen funktioniert die Suchmaschine Google mit dem Tor-Browser nicht, sobald man eine Suche startet.

Um nach den Inhalten im Darknet zu suchen, nutzt man Suchmaschinen wie Torch (http://xmh57jrzrnw6insl.onion/). Diese funktioniert wie eine normale Suchmaschine, findet jedoch nicht besonders viel und sieht auch nicht sehr ansprechend aus.

Ansonsten muss man einfach die Links durchklicken und die eigenen Interessengebiete im Darknet durchforsten.

6 Strafbar?!

Ein häufig verbreitetes Gerücht über das Darknet ist, dass man sich durch dessen Nutzung strafbar macht. Aber ist dies wirklich eine Straftat? Fakt ist, dass man illegale Waren und Dienstleistungen dort erwerben kann. Man kann außerdem Seiten finden, die man im „normalen“ Internet nicht finden kann. Aber nur allein mit dem Surfen im Darknet macht man sich nicht strafbar. Solange man keine illegalen Inhalte, wie Kinderpornographie oder illegale Waren und Dienstleistungen kauft, ist man auf der sicheren Seite. Es kommt einfach darauf an was man dort macht. Das eigentliche Surfen per se ist nicht illegal.

7 Fazit

Zusammenfassend kann man sagen, dass Tor ein gutes Open Source Projekt ist, was einfach zu installieren und zu bedienen ist. Jedoch sollte man darauf achten, nur auf https-Seiten zuzugreifen, um für mehr Sicherheit zu sorgen. Außerdem soll Gerüchten zufolge monatelang über die Hälfte der Exit-Nodes dem Geheimdienst gehören, um kriminelle Machenschaften früher zu erkennen und aufzudecken. Wenn man jedoch nichts zu verbergen hat, braucht man sich diesbezüglich keine Sorgen machen. Nur im Hinblick auf die Surfgeschwindigkeit gibt es meines Erachtens Verbesserungspotenzial.

Ansonsten ist Tor jedoch eine gute Alternative, um sich anonym im Internet frei und relativ unbeobachtet zu bewegen. Wir sollten auch darauf achten, mehr von unserem Recht auf informationelle Selbstbestimmung Gebrauch zu machen und nicht ungefragt jedem unsere persönlichen Daten weitergeben, um ständig analysiert zu werden.

8 Literaturverzeichnis

Bäumler, H. and Mutius, A. (2013) Anonymität im Internet: Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts. Springer-Verlag.

Brombach, S. (1999) Web-Academy - Entwicklung eines nutzerorientierten, integrierten Programms im Internet für das Dienstleistungsunternehmen Hochschule: Dargestellt am Beispiel des geplanten Studiengangs 'Master of Business Administration (MBA) in Entrepreneurial Studies' an der Fachhochschule Gelsenkirchen. diplom.de.

Computerbetrug (2011) DDoS-Attacken: Wenn Angreifer die Webseite lahmlegen, computerbetrug.de - Infos über Gefahren des Internet. Available at: http://www.computerbetrug.de/sicherheit-im-internet/ddos-attacken [Accessed 26 March 2018].

Datenschutzbeauftragter Info (2018) Pseudonymisierung – was ist das eigentlich?, Datenschutzbeauftragter. Available at: https://www.datenschutzbeauftragter-info.de/pseudonymisierung-was-ist-das-eigentlich/ [Accessed 26 March 2018].

GIGA (2017) Was ist ein Proxy-Server? Und warum ist er so wichtig? Einfach erklärt, GIGA. Available at: https://www.giga.de/extra/server/specials/was-ist-ein-proxy-server-und-warum-ist-er-so-wichtig-einfach-erklaert/ [Accessed 26 March 2018].

Gruenderszene (2010) World Wide Web Definition, Gründerszene Magazin. Available at: https://www.gruenderszene.de/lexikon/begriffe/world-wide-web [Accessed 26 March 2018].

Herrmann, D. (2016) Beobachtungsmöglichkeiten im Domain Name System: Angriffe auf die Privatsphäre und Techniken zum Selbstdatenschutz. Springer-Verlag.

Hessling, L. (2017) Technische Details zu IPv6. Available at: https://www.teltarif.de/internet/ipv6/details.html [Accessed 26 March 2018].

How to inter (2010) Deep Web - How to Internet. Available at: http://howtointer.net/Chapters/Chapter16/Deep-Web.html [Accessed 26 March 2018].

Mey, S. (2017) Darknet: Waffen, Drogen, Whistleblower. C.H.Beck.

Petrlic, R. and Sorge, C. (2017) Datenschutz: Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie. Springer-Verlag.

The Tor Project [no date-a] Tor Project: Overview. Available at: https://www.torproject.org/about/overview.html.en [Accessed 26 March 2018].

The Tor Project [no date-b] Who uses Tor? Available at: https://www.torproject.org/about/torusers.html.en [Accessed 26 March 2018].

T-Online (2012) Was ist eine IP-Adresse? Available at: http://www.t-online.de/digital/hardware/wlan-dsl/id_47922534/was-ist-eine-ip-adresse-.html [Accessed 26 March 2018].

TU Dresden (2012) Technische Universität Dresden, Das MIX-Netz. Available at: https://tu-dresden.de/ing/informatik/sya/ps/ressourcen/dateien/studium/materialien/mat_kp_datensicherheit/v09_doku.pdf?lang=de [Accessed 17 May 2018].