Anonymität im Internet

Seminararbeit

vorgelegt von Johannes Nolte

Matrikelnummer: xxxxxx

E-Mail: xxxxxx

Modul: Sicherheit, Privatsphäre und Vertrauen im Netz

Abgabedatum: 15.01.2019 (WS 2018/19)

Dozent: xxxxxx

TH Köln - Fakultät 10

Abstract

Nutzer surfen im Internet in der Regel nicht anonym. Neben Logins sorgen Cookies, Fingerprinting sowie Netzwerküberwachung dafür, dass Nutzer von verschieden Stellen überwacht werden bzw. werden können. Wenn es nur darum geht, eine IP zu verbergen, kann ein Proxyserver eingesetzt werden. Wirkliche Anonymität bietet dieser jedoch nicht. Mehr Schutz bietet VPN, wo Internetverkehr verschlüsselt zu einem VPN-Server übermittelt wird. Noch weiter geht das Tor-Netzwerk, wo Datenpakete mehrfach verschlüsselt über verschiedene Knoten weitergeleitet werden, sodass ihr Ursprung verschleiert wird. Dies ermöglicht es verschiedensten Personen mit unterschiedlichen Hintergründen anonym zu surfen. Werkzeuge zur Anonymisierung müssen jedoch für jeden Anwendungsfall individuell ausgewählt werden, da sie sich in ihrer Funktion unterscheiden und unterschiedlichen Zielen gerecht werden. Alle Tools haben Vor- und Nachteile, die je nach Anwendungsfall abgewogen werden müssen.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Wenn Verbrecher in der echten Welt während ihrer Tat nicht erkannt werden möchten, tragen sie häufig eine Sturmhaube. In Medien wird dieses Vorgehen gerne auch auf digitale Ganoven übertragen. Dass das in Agentur-Bildmaterial nicht unübliche Tragen einer Sturmhaube vorm Laptop nicht zur Anonymität im Internet beiträgt, dürfte dabei wohl auch technischen weniger versierten Personen klar sein. In dieser Seminararbeit werden gängige Techniken zum Erreichen von Anonymität im Internet vorgestellt und erläutert. Dabei muss die Motivation zur anonymen Nutzung des Internets keinesfalls kriminell sein.

Die Anonymität im Internet gibt es nicht. Vielmehr gibt es verschiedene Szenarien mit verschiedenen Anforderungen an Anonymität gegenüber verschiedenen Parteien. Mal soll nur ein Webdienst nicht wissen, mit wem er es zu tun hat, in anderen Fällen soll ein Netzwerkprovider nichts über den Inhalt der gesendeten Daten wissen, mal soll der Staat keine Möglichkeit haben, Inhalte zu zensieren. Allgemein ist mit Anonymität im Internet gemeint, dass keine Verbindung zwischen einem Internet-Nutzer und dessen Identität hergestellt werden kann. Diese Verbindung kann jedoch potenziell an vielen Stellen eines Datenaustauschs übers Internet hergestellt werden, sodass anonymes Surfen, je nachdem gegenüber wem die Anonymität gewahrt werden sollen, komplex sein kann.

Um besser verstehen zu können, wie Anonymität im Internet funktionieren kann, wird im folgenden Kapitel nun zunächst dargestellt, warum Nutzer im Internet in der Regel nicht anonym sind.

2 Nutzererkennung im Internet

Die banalste Form, seine Identität im Internet preiszugeben, ist dies aktiv selbst durch das Eingeben von Daten zu tun. Technische Anonymisierung, wie sie in den folgenden Kapiteln vorgestellt ist, kann nutzlos werden, wenn der Nutzer nach Durchführung dieser Maßnahmen bspw. in einem Formular eine E-Mail-Adresse mit seinem Klarnamen darin übermittelt oder er einen Nutzernamen verwendet, der schon einmal ohne Nutzung von Anonymisierungstools verwendet wurde. Doch auch wer immer nur fiktive Namen etc. verwendet, ist im Internet noch nicht anonym unterwegs. Verschiedene Techniken ermöglichen es, Nutzer zu erkennen oder zumindest wiederzuerkennen.

2.1 Cookies

Die klassischste Form zur Wiedererkennung von Nutzern sind die so genannten Cookies. Dabei handelt es sich um Textdateien, die von aufgerufenen Webseiten auf dem Computer eines Nutzers abgelegt werden können (MOZILLA O.J.). Diese Dateien können beispielsweise eine für jeden Nutzer individuelle Zeichenkette enthalten, sodass ein Webserver einen Nutzer wiedererkennen kann. Eine Identifizierung der Identität eines Nutzers ist mit Cookies allein jedoch nicht möglich, diese können

nur für eine Wiedererkennung eines Browsers sorgen. Ist mit einem Cookie aber bspw. ein persönlicher Login verknüpft, kann die Identität des Nutzers oder zumindest ein Pseudonym, unter dem er auftritt, mit Hilfe dieses Cookie identifiziert werden.

Die Wiedererkennung eines Nutzers mit Cookies kann im direkten Interesse des Nutzers sein, weil dieser dann bspw. eine Webseite in der zu einem früheren Zeitpunkt ausgewählten Sprache ausgeliefert bekommt oder sich nicht bei jedem Besuch neu einloggen muss. Oft erfolgt eine Wiedererkennung von Nutzern jedoch auch ohne deren Wissen und damit ggf. sogar gegen deren Willen. Ein gängiger Fall sind Cookies von Werbenetzwerken und Analysetools, die in einer Webseite integriert sind.

Aus der Perspektive von datenschutzorientierten Nutzern gesehen ist es ein großer Vorteil, dass Cookies auf den Endgeräten der Nutzer gespeichert werden, da diese so die Kontrolle über die Cookies haben. Nutzer können in den Einstellungen ihres Browsers bisher gesetzte Cookies gezielt löschen oder bspw. durch Nutzung des Privat-/Inkognito-Modus dafür sorgen, dass Cookies gar nicht erst länger als während einer Session gespeichert werden. Auch der Einsatz von Werbeblockern kann dafür sorgen, dass Cookies gar nicht erst abgelegt werden können. Daher wurden andere Techniken entwickelt, um Nutzer im Web wiedererkennen zu können.

2.2 Fingerprinting

Beim Fingerprinting werden Nutzer bzw. ihre Browser nicht durch das Ablegen von Cookies erkannt, sondern durch verschiedene technische Eigenschaften ihrer Nutzungsumgebung, die ein Webserver auslesen kann. Diese Eigenschaften werden zu einem sinnbildlichen Fingerabdruck zusammengefasst und können in vielen Fällen einen Nutzer eindeutig identifizieren (im Sinne von Wiedererkennung/Individueller Fingerabdruck wie ein Cookie, nicht der realen Identität einer Person). Geeignete Eigenschaften sind beispielsweise installierte Schriftarten oder die Bildschirmauflösung (zusammen mit vielen anderen). Weitere Eigenschaften und deren konkreten Werte beim eigenen Endgerät sind im Online-Tool *Panopticlick*[1] der Electronic Frontier Foundation einsehbar. Besonders gut wiedererkennen lassen sich Nutzer durch das so genannte Canvas-Fingerprinting. Dabei wird versteck ein HTML Canvas-Element erzeugt und aus dem Ergebnis ein Hash berechnet (MOWERY & SHACHAM 2012). Da Canvas-Elemente je nach eingesetzter Grafikkarte sowie aufgrund anderer Eigenschaften auf verschiedenen Endgeräten oft minimal unterschiedlich aussehen, eignet sich der Hash daraus sehr gut um einen (weiteren) Faktor zur Wiedererkennung von Nutzern durch Fingerprinting zu erhalten.

[1] https://panopticlick.eff.org

Fingerprinting lässt sich schwieriger unterdrücken als Cookies, da einige der genutzten Eigenschaften zwangsläufig übermittelt werden müssen. Es kann jedoch deutlich erschwert und damit oft auch verhindert werden, indem browserseitig (bspw. durch Addons, die den Browser um diese Funktion erweitern) so wenig Daten wie möglich an Webserver übermittelt werden und Canvas-Elemente sowie bekannte Fingerprinting-Skripte geblockt werden.

2.3 Provider

Während Cookies und Fingerprinting von Webservern, die ein Nutzer besucht, ausgelöst werden, kann die Anonymität eines Nutzers selbstverständlich auch an anderer Stelle aufgelöst werden. Sofern Datenpakete nicht Ende-zu-Ende verschlüsselt sind oder die Verschlüsslung gebrochen wird, können andere Personen im lokalen Netzwerk, Internetzugangsprovider und Betreiber von Internetknoten den versendeten Datenverkehr mitlesen. Auch staatliche Stelle könnten sich einklinken und mitlauschen.

Der Anonymität im Internet grundsätzlich im Wege steht, dass IP-Pakete eine Quell- und eine Ziel-IP-Adresse enthalten müssen, um sie zustellen zu können. Zumindest in Deutschland stellen Provider ihren Kunden einen Internetanschluss nicht anonym zur Verfügung und so kann (wenn die entsprechende Rechtsgrundlage gegeben ist) ein Bezug zwischen IP-Adressen und Anschlussinhaber hergestellt werden, indem beim Provider die Kundendaten hinter einer IP-Adresse angefragt werden. Aus diesem Grund kann es zum Erreichen von Anonymität im Internet sinnvoll sein die eigene IP-Adresse zu verbergen, was im folgenden Kapitel näher erläutert wird.

3 Konzepte und Strukturen für Anonymität im Internet

3.1 Proxy-Server

Wenn in den Einstellungen eines Betriebssystems oder bspw. Browsers ein Proxy-Server eingetragen wird, wird ausgehender Datenverkehr nicht an die eigentliche Zieladresse gesendet, sondern zunächst an den Proxy-Server. Dieser kann die Pakete dann weiterleiten, sodass für den Empfänger der Proxy-Server und nicht der eigentliche Sender die Quelle der Pakete ist. Der Proxy-Server muss die Datenpakete dabei nicht zwingend nur durchleiten, auch das Filtern von Paketen ist möglich. Denkbare Anwendungsszenarien sind beispielsweise Jugendschutzfilter oder das Sperren bestimmter Dienste wie Telnet (Datenverkehr auf Port 23). Auch kann ein Proxy-Server Inhalte vorhalten und diese bei passenden Anfragen direkt ausspielen, anstatt die Anfrage an den Zielserver weiterzugeben und dessen Antwort zurückzusenden. Mit einem solchen Caching können etwa schnellere Ladezeiten von Webseiten erreicht werden (INDIANA UNIVERSITY 2018).

Datenpakete werden beim Senden an den Proxy-Server nicht gesondert verschlüsselt. Handelt es sich also um Daten, die mit Protokollen ohne Verschlüsselung übertragen werden (bspw. HTTP) kann ein Angreifer im Netz diese, genauso wie als würde kein Proxy eingesetzt werden, mitlesen. Auch eine Person mit Zugriff auf den Proxy-Server hat Zugriff auf die ein- und ausgehenden Daten. Kommt bspw. HTTPS zum Einsatz sind zumindest die IP Header noch lesbar. Zur Anonymität im Internet trägt ein Proxy-Server somit nur bei der Verschleierung einer Quell-Adresse gegenüber dem Zielserver bei. Techniken zur Identifizierung von Nutzern können weiterhin angewandt werden und bei einer Überwachung des Internetverkehrs durch den Staat/Provider hilft ein Proxy-Server wenig. Gängige Anwendungen für Proxys sind daher Fälle, in denen es weniger um Anonymisierung geht, sondern bspw. um die Umgehung von Geoblocking indem dem Zielserver eine ausländische IP-Adresse vorgegeben wird.

3.2 VPN

Beim Einsatz eines Virtual Private Networks (VPN) wird ein Transporttunnel zwischen zwei Kommunikationspartnern etabliert. Datenpakete werden nicht sofort an den eigentlichen Empfänger gesendet, sondern verschlüsselt („durch den VPN-Tunnel“) an das VPN-Gateway eines anderen Netzes geschickt. Dort werden sie entschlüsselt und an ihr eigentliches Ziel weitergeleitet. Für dieses Vorgehen sind verschiedene Protokolle geeignet, ein gängiges ist IPSec. Dabei wird das eigentliche IP-Paket mit ESP (Encapsulating Security Payload) verschlüsselt und erhält einen zweiten, äußeren IP-Header (PETRLIC & SORGE 2017 S. 25).

Eine gängige Anwendung für VPN ist die Anbindung von Mitarbeitern im Homeoffice an ihre Firma oder von Studenten an eine Hochschule. Durch die Nutzung von VPN können diese arbeiten wie als befänden sie sich im Netzwerk ihrer Organisation und beispielsweise auf ein Intranet oder andere Dienste, die nur im Netzwerk der Organisation zur Verfügung stehen, zugreifen.

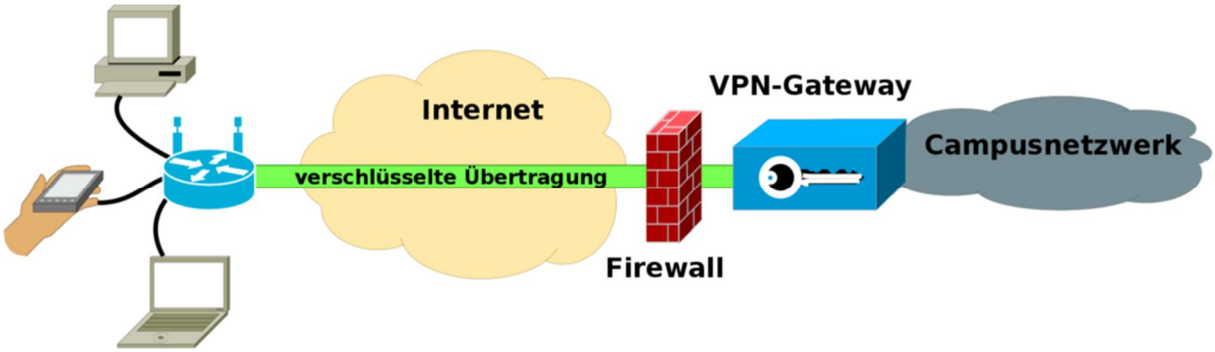

Abbildung 1 Funktionsweise eines VPN-Netzwerks (*REGIONALES RECHENZENTRUM ERLANGEN 2017*)

Da die ausgehenden Datenpakete bei Nutzung eines VPN Dienstes vor dem Versenden verschlüsselt und „verpackt“ (also um den äußeren Header erweitert) werden, kann ein Angreifer im Netzwerk

nicht nur deren Inhalt, sondern auch den tatsächlichen IP-Header eines Pakets nicht mitlesen. Dies ist ein entscheidender Unterschied zur Verschlüsslung mit bspw. TLS wo zwar der Inhalt eines Paketes verschlüsselt wird, nicht aber der Header. Bei einer VPN Verbindung sieht ein Angreifer lediglich, dass Daten zwischen den beiden VPN-Partnern ausgetauscht werden, woraus deutlich weniger Schlüsse gezogen werden können als wenn alle Header eines Nutzers analysiert werden können. VPN Protokolle bieten daher, sofern sie nicht gebrochen oder in ihrer Umsetzung manipuliert werden, einen Schutz vor Überwachung von Internetverkehr. Auch Internetzensur kann damit umgangen werden, vorausgesetzt die VPN-Pakete werden nicht auch unterdrückt und das VPN Gateway befindet sich außerhalb des zensierten Netzwerks. Da die Datenpakete beim VPN Gateway entschlüsselt werden, sollte dieses von einer vertrauenswürdigen Instanz angeboten werden, die sich durch ein Zertifikat ausweist.

Wenn sich Anfragen eines VPN-Nutzers nicht auf interne Dienste im Netz des VPN-Anbieters beziehen, sondern „normaler“ Internettraffic sind, wird dieser vom VPN Anbieter in der Regel nur ins Internet durchgeleitet. Da der Quellserver nun der VPN Anbieter ist, kann so die IP-Adresse des eigentlichen Nutzers gegenüber dem Zielserver und gegenüber einer Netzwerküberwachung zwischen VPN-Anbieter und Zielserver versteckt werden. Der Überwachende weiß, dass eine Anfrage von einem Nutzer des VPN Dienstes stammt, aber nicht von welchem. Aufgrund von Inhalten der übermittelten Daten (Header oder unverschlüsselte Payload) und Tracking-Technologien kann der User vom Webserver-Anbieter jedoch möglicherweise dennoch identifiziert oder wiedererkannt werden.

3.3 Onion Routing

Das Tor-Projekt (Tor für „**T**he **O**nion **R**outer“ oder „…**R**outing“) will die Anonymität seiner Nutzer durch das Prinzip des so genannten Onion-Routings erzielen. Dabei wird ein Datenpaket nicht direkt vom Sender zum Empfänger geleitet, sondern passiert auf dem Weg dorthin mehrere Tor-Server (Knoten bzw. engl. Nodes), sinnbildlich mehrere Schichten einer Zwiebel (TOR PROJECT 2018). Somit kennt kein Knoten beide Kommunikationspartner, sondern nur maximal einen. Zudem enthält der Header eines Datenpakets nicht wie üblich Absender und Empfänger (zumindest nicht beide tatsächlichen Kommunikationspartner gleichzeitig). Damit die Knoten den Inhalt der gesendeten Pakete nicht mitlesen können, werden diese verschlüsselt übertragen. Diese Verschlüsselung bezieht sich jedoch nur auf das Tor-Netzwerk. Beim Verlassen dieses durch einen so genannten Exit-Node ist das Datenpaket nur noch „normal“, etwa durch TLS, oder eben gar nicht wie bei klassischen HTTP-Aufrufen oder IMAP-Mailabfragen verschlüsselt. Dies macht Exit-Nodes sehr attraktiv für die

Überwachung etwa durch staatliche Stellen. Am einfachsten ist die Überwachung, indem der Exit-Node schlichtweg von den Überwachenden betrieben wird. Auch wenn insgesamt viele Nodes von einer Stelle bzw. einer Gruppe, betrieben werden, ist die Anonymität der Tor-Nutzer gefährdet (EIKENBERG 2016). Grundsätzlich lässt sich festhalten: Je mehr individuelle Nutzer das Tor-Netzwerk hat, desto schwieriger ist die Anonymität dieser zu brechen.

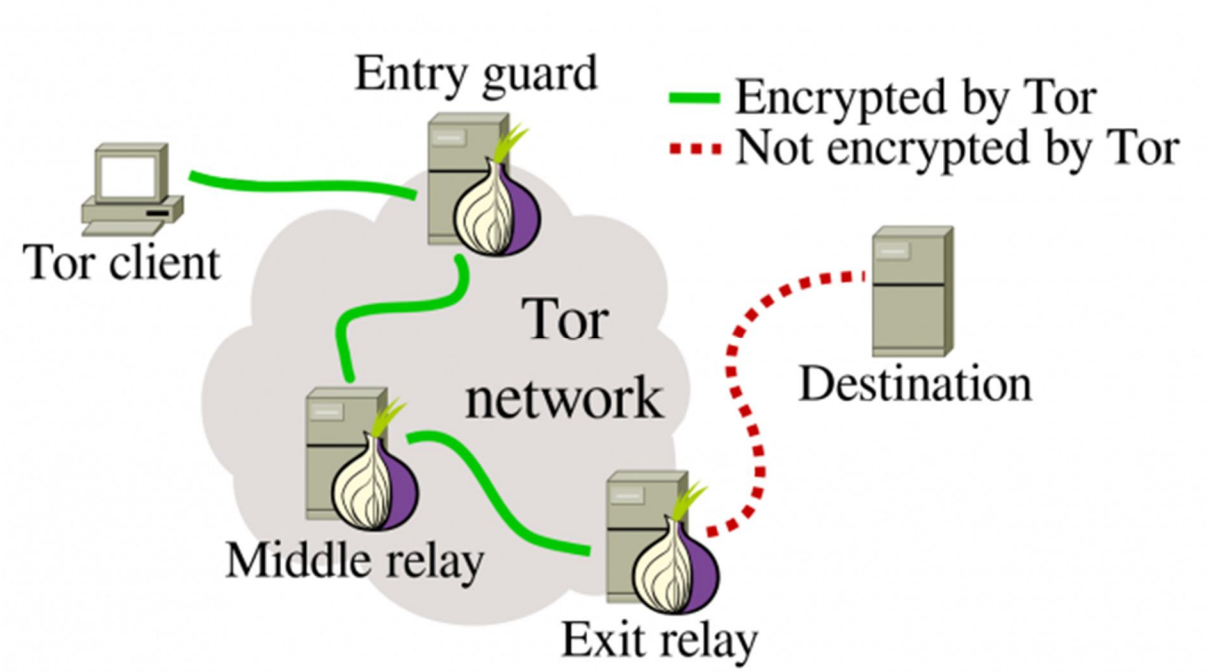

Abbildung 2 Aufbau des Tor-Netzwerks (*WHITWAM 2014*)

Zum Enttarnen von Nutzern braucht es jedoch nicht zwingend eine Kompromittierung der Tor-Infrastruktur. Beispielsweise können die ab dem Exit-Node eventuell unverschlüsselt übertragenen Daten einer Kommunikation aufgrund Ihres Inhalts Rückschlüsse auf die Identitäten der Absender geben. Dies können zum Beispiel Angaben in Formular-Feldern sein oder allein die URLs aufgerufene Webseiten oder Mailserver. Ebenfalls können Nutzer vom Kommunikationspartner oder etwa durch staatliche Lauschangriffe an Internetknoten durch die in Kapitel 2 vorgestellten Methoden auch beim Nutzen des Tor-Netzwerks de-anonymisiert oder zumindest wiedererkannt werden. Der Tor-Browser versucht dieses Risiko zu verringern. Beim Tor-Browser handelt es sich um einen angepassten Mozilla Firefox Web-Browser, der eine einfache Nutzung des Tor-Netzwerks erlaubt. Näheres dazu in Kapitel Tor-Browser5.2.

Innerhalb des Tor-Netzwerks können so genannte Hidden Services angeboten werden. Wenn ein Nutzer einen solchen Hidden Service aufruft, verlassen die Datenpakete das Tor-Netzwerk nicht, was die Anonymität der Nutzer gegenüber einen Hidden Service Betreiber im Gegensatz zu einem

Betreiber eines klassischen Webservers außerhalb des Tor-Netzwerks deutlich erhöht. Zudem erfolgt die gesamte Kommunikation im Tor-Netzwerk verschlüsselt, sodass es im Rahmen staatliche Onlineüberwachung schwer ist, überhaupt von der Kommunikation des Nutzers mit dem Hidden-Service zu erfahren. Der Aufruf eines Tor Hidden Service erfolgt im Tor-Browser über eine *.onion*-Adresse. Diese ist für die Hidden Serivce Anbieter nicht beliebig wählbar, sondern besteht aus den ersten 16 Zeichen des SHA1-Hashes (Base32-kodiert) des öffentlichen Schlüssels. Dies verhindert, dass ein Angreifer bspw. eine CA kompromittiert und so den eigentlich verschlüsselte Datenaustausch zwischen Nutzer und dessen Zielwebseite belauscht, da er ein Zertifikat für die Zielseite besitzt, dem der Nutzer vertraut (SCHMIDT 2016). Facebook hat sehr viel Rechenzeit aufgewandt um ein Schlüsselpaar zu generieren, das die für Menschen relativ leicht merkbare Onion-Adresse *facebookcorewwwi.onion* hat (SCHMIDT 2018). Darüber können bspw. Menschen in Ländern, in denen die Nutzung von Facebook überwacht wird, die Plattform unerkannt nutzen. Viele Hidden Services dienen kriminellen Geschäften, aber auch legale Angebote sind vorhanden. Weiteres dazu in Kapitel 6.

Das Tor-Netzwerk eignet sich nicht gut dafür, es dauerhaft zum Surfen im Internet zu verwenden. Zum einen benötigt das Onion-Routing Zeit und der Aufbau von Webseiten erfolgt so deutlich langsamer als ohne Onion-Routing. Zum anderen ist wie zuvor beschrieben davon auszugehen, dass Exit Nodes, durch die die gesendeten Pakete das Tor Netzwerk verlassen, von einer unbekannten Stelle überwacht wird, sodass dieser gegenüber der gesamte HTTP-Verkehr und die Header verschlüsselter Pakte zugänglich gemacht werden.

3.4 Weitere Konzepte

In den vorherigen Unterkapitel ging es darum, einen Quell-Internetanschluss oder ein Quell-Gerät eines Datenverkehrs zu verschleiern. Die Motivation für diese Verschleierung ist, dass wie in Kapitel 2.3 beschrieben ein Bezug zwischen Quell-IP und Anschlussinhaber hergestellt werden kann. Bezogen auf Endgeräte kann die regelmäßige Verwendung eines Gerätes Spuren im Internet hinterlassen und somit zur De-Anonymisierung führen. Es ist daher naheliegend gar nicht erst das eigene Gerät und den eigenen Internetanschluss zu verwenden, wenn man anonym im Internet surfen möchte. Möglich ist dies beispielsweise in Bibliotheken oder Internetcafés. Auch das Nutzen von offenen WLANs etwa in Cafés oder im öffentlichen Raum ist möglich, ebenso wie der Einsatz von Sim-Karten, die vor Juli 2017 anonym gekauft wurden oder die beim Kauf (aus welchen Gründen auch immer) bereits aktiviert sind. Dabei entsteht jedoch kein Schutz vor Wiedererkennung von Nutzern durch Tracking und, ebenso wie beim Nutzen eines fremden Rechners und Anschlusses bspw. in einem Internetcafé oder Hotel, kein Schutz vor Identifizierung von Nutzern durch eine inhaltliche

Auswertung des Datenverkehrs (Zieladresse, Formulareingaben etc.). Die vorgestellten Beispiele zeigen jedoch, dass neben Softwaretools wie VPN und Tor simplere „Real World"-Methoden zur Erreichung von Anonymität im Internet möglich sein können. In ihrer Praxistauglichkeit und Funktionsweise haben diese jedoch genauso Vor- und Nachteile wie die Softwaretools.

4 Einsatzmöglichkeiten und Motivation anonymer Internetnutzung

Die Einsatzmöglichkeiten bzw. Gründe, warum Menschen anonym im Internet surfen bzw. dies müssen oder sollten sind vielfältig. Für alle Internetnutzer kann Tracking auf Webseiten ein Grund sein, bspw. den Tor-Browser zu nutzen. Das Tracken von Nutzern im Web ist heute sehr umfangreich. Insbesondere große Webfirmen und Werbenetzwerke wie Google und Facebook haben umfangreiche Möglichkeiten, Aktivitäten von Nutzern nicht nur auf ihren eigenen Seiten zu verfolgen, sondern auch als eingebundene Drittanbieter auf sehr vielen anderen Webseiten. Die gesammelten Daten könnten verkauft werden oder durch Staaten oder Hacker, die diese beim Datensammler erbeuten, missbraucht werden. Dies könnte ebenso durch andere Nutzer oder Betreiber von öffentlichen WLANs bspw. in Cafés und Flughäfen passieren. Vorsichtige Nutzer setzen in öffentlichen Netzwerken daher einen VPN-Dienst ein. Im heimischen Umfeld könnten beispielsweise sehr persönliche Suchanfragen Grund sein, diese bspw. über den Tor-Browser mit einer anderen IP als gewöhnlich abzusetzen. In größeren Unternehmen mit statischer IP können Anonymisierungstools eingesetzt werden, um Webseiten von Konkurrenzanbietern unerkannt zu evaluieren.

In nicht-demokratischen Staaten sind die in dieser Arbeit vorgestellten Tools, insbesondere VPN und Tor, zudem von existenzieller Bedeutung für regierungskritische (oder auch nur neutrale) Journalisten und Aktivisten. Diese können damit Internetzensur umgeben und müssen ohne Anonymisierungstools davon ausgehen, dass der Staat ihren Internetverkehr mitliest und sie ggf. für ihr Handeln bestraft. Auch ganz normale Bürger in solchen Ländern können sich dank der Tools frei informieren. Aber auch in westlichen Demokratien kommt die Möglichkeit, anonym zu surfen, Journalisten und deren Quellen sowie Whistleblowern entgegen. Beispielsweise betreibt der heise Verlag einen anonymen „sicheren Briefkasten" als Tor Hidden-Service (s. Abbildung 4).

Ebenfalls Nutzer von Anonymisierungstools sind Kriminelle, die damit ihre Straftaten ohne erkannt zu werden, ausüben können. Das kann zum Beispiel Drogenhandel, Hacking oder Austausch von Kinderpornographie sein. Die Existenz von Anonymisierungstools erschwert Ermittlungsbehörden

dabei die Täter zu erfassen, sodass Polizei und Geheimdienste etwa auf aufwendigere Social-Engineering Methoden zurückgreifen müssen.

In einigen Ländern ist aufgrund der zuvor beschrieben Anwendungsfälle der Einsatz von einigen Anonymisierungstools verboten und wird (soweit dies möglich ist) technisch behindert oder unterdrückt. In Deutschland ist der Einsatz aller in dieser Arbeit vorgestellten Tools laut dem Portal anwalt.org an sich legal. Strafbar können aber natürlich Handlungen mit diesen Tools sein, bspw. Drogenhandel über einen Tor Hidden-Service oder Urheberrechtsverletzungen.

5 Implementierungsvarianten

In diesem Kapitel werden Programme und Dienstanbieter zur Nutzung von VPN, Proxys und dem Tor-Netzwerk vorgestellt.

5.1 VPN und Proxy Programme

Zur Nutzung eines VPN-Dienstes muss ein VPN-Client auf dem Endgerät installiert werden. Ein verbreiteter Client für verschiedene Betriebssystem ist bspw. Cisco AnyConnect, es gibt jedoch sehr viele VPN-Clients. Wenn es sich nicht um ein Hochschul- oder Firmen-VPN handelt, stammen die Clients in der Regel vom Anbieter des VPN-Services selbst. Bekannte Anbieter sind bspw. Cyberghost VPN, HideMyAss und HotspotShield. Auch viele Hersteller von Antiviren-Programmen bieten VPN-Dienste an, etwa Avira, F-Secure und Sophos. Entscheidend bei der Auswahl eines VPN-Anbieters ist das Vertrauen in diesen, da bei Nutzung des VPNs der Internet-Traffic (bei verschlüsselten Protokollen zumindest die Metadaten) vom VPN-Anbieter potenziell mitverfolgt werden kann. Land des Firmensitzes, AGB, Datenschutzbestimmungen und Geschäftsmodell des Anbieters sollten daher in die Auswahlentscheidung einfließen. Datenschutzaktivisten raten stark davon ab, kostenlose VPN-Dienste zu nutzen (FANTA ET AL. 2018). Weniger relevant für die Anonymität der Nutzer aber trotzdem entscheidend können auch Features der VPN-Anbieter sein. Bei einigen Anbieter lassen sich bspw. verschiedene Ausgangsserver in verschiedenen Ländern auswählen, sodass Geoblocking umgangen werden kann. Alternativ zur Nutzung eines VPN-Anbieters kann auch ein VPN-Dienst auf einem eigenen Server eingerichtet werden. Eine verbreitete Open Source Software dafür ist OpenVPN. Auch einige Heimrouter (z.B. Modelle von AVM) bieten eine VPN-Server-Funktion.

Proxys lassen sich im Gegensatz zu VPN bei vielen Betriebssystemen direkt in die Einstellungen dieser eintragen. Auch viele Programme wie Internet-Browser bieten in ihren Einstellungen die Möglichkeit, ausgehenden Datenverkehr an einen Proxy zu senden. Anbieter und Adressen von Proxy-Servern lassen sich im Internet recherchieren, auch hier gilt jedoch, dass man dem Anbieter vertrauen sollte. Im Zweifelsfall tauscht man die Offenlegung eigener Daten gegenüber einem Internet-Diensteanbieter gegen die Offenlegung gegenüber einem Proxy-Anbieter ein. Gegebenenfalls

verschleiert der Proxy sogar nicht einmal die eigene IP-Adresse sicher, da diese sich über JavaScript auslesen lässt, wenn der Proxy-Server solche Befehle nicht filtert. Sinnvollere Implementierungen von Proxys sind daher bspw. Firmen-interne Lösungen für Caching oder Webfilter und nicht kostenlose Web-Proxys unbekannter Anbieter.

5.2 Tor-Browser

Die gängige Variante das in Kapitel 3.3 vorgestellte Tor-Netz und die darin enthaltenen Hidden Services zu nutzen, ist der Tor-Browser. Dabei handelt es sich um eine modifizierte Version des Mozilla Firefox, welche unter torproject.org zum Download zur Verfügung steht. Der Browser bietet dem Nutzer eine unkomplizierte Nutzung des Tor-Netzwerks, da er sich automatisch damit verbindet und die Bedienung nicht schwerer als die eines normalen Webbrowsers ist. Darüber hinaus enthält der Tor-Browser Erweiterungen, die die Anonymität des Nutzers erhöhen. Dazu gehört beispielsweise die standardmäßig aktivierten Addons „NoScript“ und „HTTPS Everywhere“. Zudem sind im Tor-Browser diverse Einstellungen im Gegensatz zum Standard-Firefox so gesetzt, dass die Privatsphäre des Nutzers geschützt wird. Insbesondere soll die Identifizierung von Personen bzw. das Wiedererkennen dieser vermieden werden. Außerdem gibt der Tor-Browser Tipps zur Verhaltensweise, bspw. dass die Größe des Browserfensters nicht verändert werden soll damit sich die eigene Installation des Tor-Browsers möglichst wenig von anderen unterscheidet. Auch sind, je nach gewählter Sicherheitsstufe verschiedene Funktionen, etwa für Canvas-Grafiken und Schriftarten, deaktiviert.

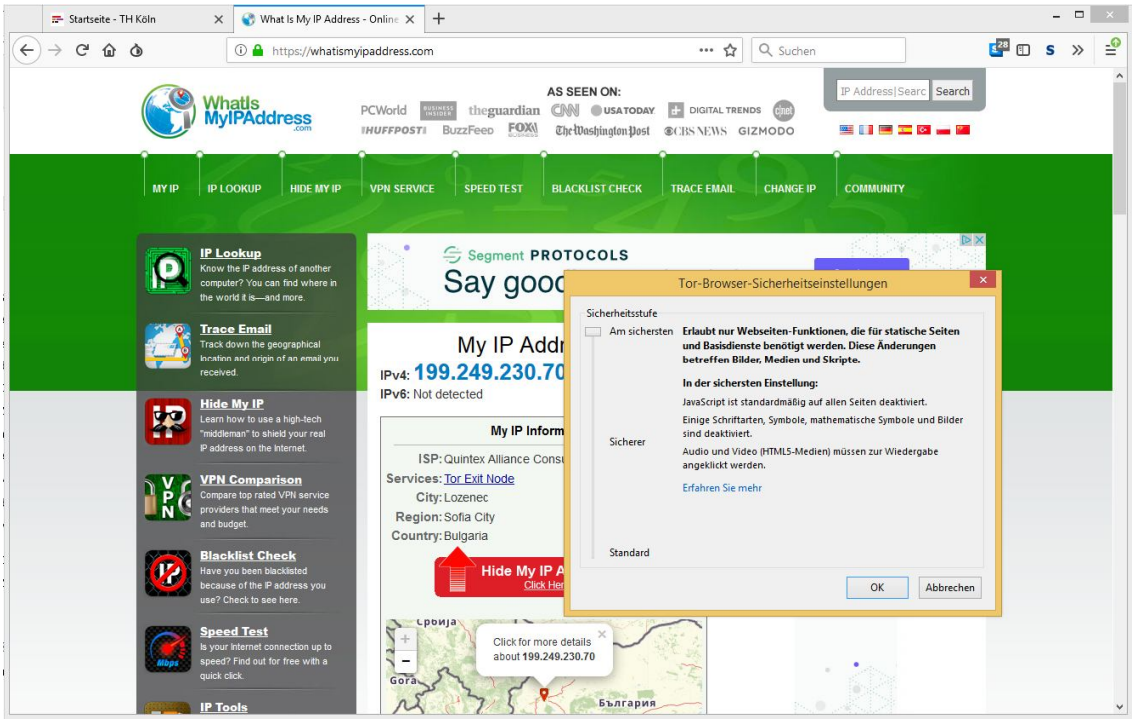

Abbildung 3 Screenshot: Nutzung des Tor-Browsers

Grundsätzlich ist anzumerken, dass die durch den Tor-Browser entstandene Anonymität hinfällig werden kann, wenn der Computer, auf dem der Browser läuft, mit einem Trojaner infiziert ist. Wie alle anderen Sicherheit-Softwarekomponenten bietet der Tor-Browser nur Schutz vor dem Angriff, zu dessen Verteidigung er entwickelt wurde.

6 Deep- und Darknet

Besonders seit in der Presse berichtet wurde, dass der Amokläufer von München vom 22.07.2016 seine Waffe über ein Darknet-Forum erwarb, ist der Begriff „Darknet“ in der breiten Bevölkerung in Deutschland bekannt. Eine einheitliche Definition gibt es dabei genauso wenig wie *das eine* Darknet (GRUBER & SICKERT 2016). Grundsätzlich lässt sich das Darknet vom oft als Clearnet bezeichneten Teil des Internets abgrenzen, der öffentlich für alle Internetnutzer erreichbar ist, also „ganz normale“ Webseiten. Ebenfalls abzugrenzen ist das Darknet vom Deepnet. Beim Deepnet handelt es sich um versteckte Seiten im Internet, die bspw. erst nach einem Login zugänglich sind und nicht von Suchmaschinen indexiert sind. Das können beispielsweise wissenschaftliche Paper, Teile von Sozialen Netzwerken oder passwortgeschützte Foren sein.

Oft mit dem Darknet gleichgesetzt werden Hidden Services im Tor-Netzwerk. Der Unterschied zum Deep- und Clearweb ist, dass diese nicht über einen normalen Browser abrufbar sind und der Nutzer oft die .onion-Adresse eines Service kennen muss. Zwar gibt es auch Suchmaschinen für Hidden Services, dort sind aber nicht alle Hidden Services indexiert und der Nutzungskomfort ist nicht mit dem von Google vergleichbar. Einige Darknet-Definitionen gehen noch weiter und bezeichnen nur passwortgeschützte Hidden Services als Darknet, quasi das „Deepnet im Tor-Netzwerk“. Andere, technischere Definitionen beschränken sich dagegen nicht auf Tor, sondern bezeichnen allgemein Peer-to-peer Netzwerke als Darknet, in denen sich die Clients nicht automatisch verbinden, sondern Nutzer sich gezielt ohne das Wissen anderer direkt verbinden (SCHMIDT 2018).

Laut metrics.torproject.org gibt es derzeit rund 100.000 .onion-Adressen. Hinter diesen verbergen sich die verschiedensten Angebote. Die Sicherheitsfirma Hyperion Gray hat eine „Darknet Karte“ erstellt[2], die rund 6600 Darknet-Seiten als Screenshots enthält und aus der lediglich die Seiten entfernt wurden, deren Darstellung bereits illegal wäre. Die Karte enthält neben offensichtlich illegalen Angeboten wie Drogenhandel, Verkauf erbeuteter Login-Daten und dubiosem Glücksspiel auch viele teils skurrile, aber (zumindest auf den ersten Blick) nicht illegale Inhalte wie Blogs und Pornographie. Ein nicht unerheblicher Teil besteht auch aus Fehlerseiten und nicht befüllten CMS-

[2] https://www.hyperiongray.com/dark-web-map/

Default-Templates. Verschiedener Quellen nach sind etwa die Hälfte der Darknet-Seiten kommerziell (VON WESTERNHAGEN 2018). Geschäfte werden dabei oft über Mittelsmänner als Vertrauensinstanzen abgewickelt, da sich Käufer und Verkäufer aufgrund der herrschenden Anonymität nicht vertrauen könne. Neben anonymen Betreibern von Darknet-Seiten gibt es auch nicht anonyme, bekannte Betreiber von Hidden Services, etwa die bereits erwähnten, Facebook und heise.

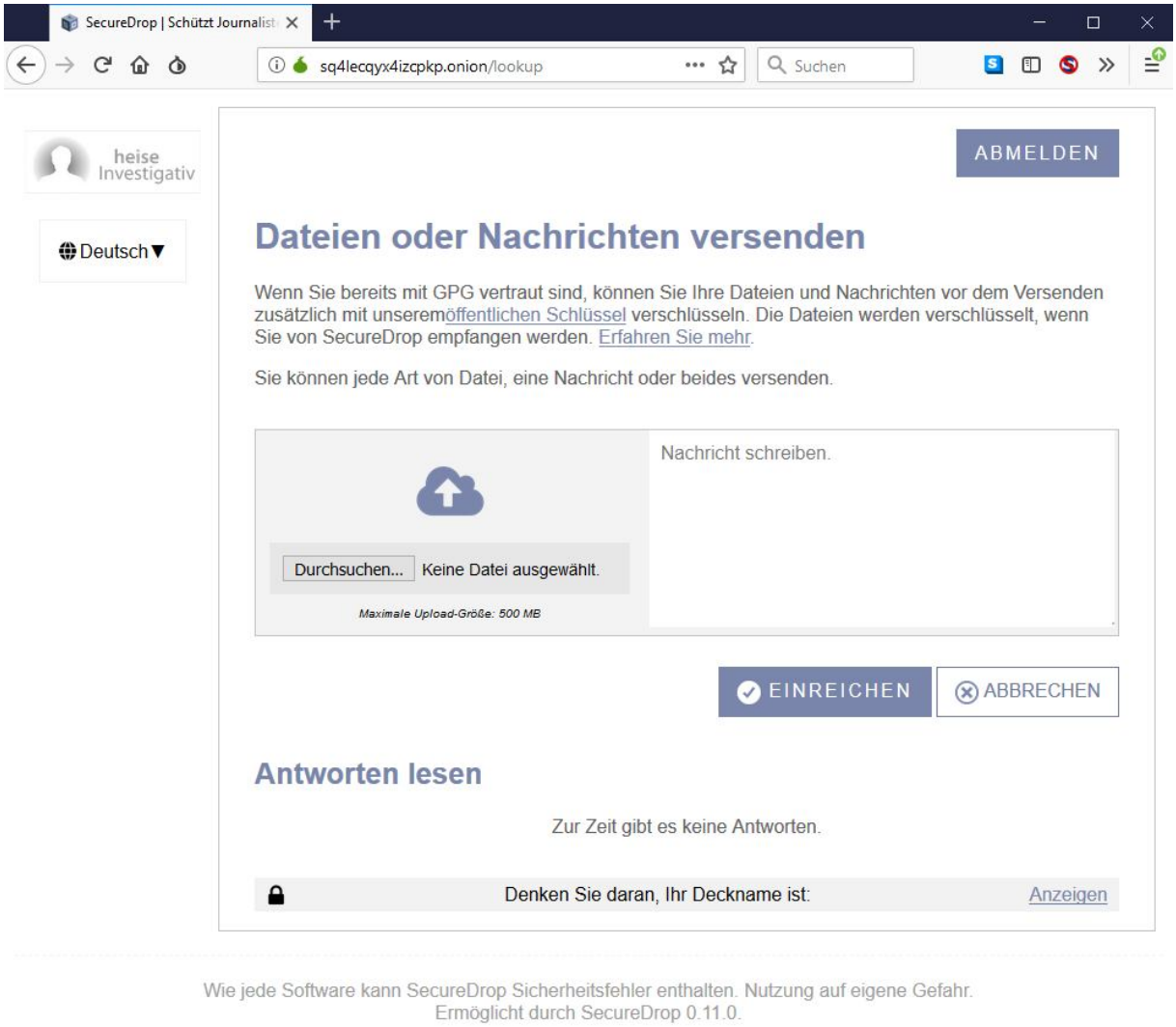

Abbildung 4 Aufruf des anonymen Briefkastens des heise Verlags im Darknet (Tor Hidden Serivce)

7 Fazit

Wer „anonym im Internet surfen“ will, sollte sich zunächst überlegen, was damit eigentlich gemeint sein soll. Gegenüber wem soll Anonymität gewahrt werden? Alle Vorgestellten Tools/Techniken haben Vor- und Nachteile. Die höchste Anonymisierung bringt dabei das Tor Netzwerk mit sich, auch dieses hat jedoch Schwächen. Je nachdem was ein Nutzer vorhat und wie groß das Interesse anderer ist, dieses Vorgehen zu beobachten oder die Person dahinter zu identifizieren, desto genauer sollte der Nutzer sich über die eingesetzten Techniken informieren. Anonymität im Internet zu erreichen ist aufgrund der vielen Datenspuren, die beim Surfen hinterlassen werden und den verschiedenen Stationen eines Datenpaketes leichter gesagt als erreicht.

8 Literaturverzeichnis

Eikenberg, Robert (2016) *Tor einfach nutzen*, verfügbar unter https://www.heise.de/security/artikel/Tor-einfach-nutzen-3284536.html (abgerufen am 17.11.18)

Fanta, Alexander, Dachwitz, Ingo, Rudl, Thomas (2018) *Kleines Einmaleins der digitalen Selbstverteidigung*, verfügbar unter https://netzpolitik.org/2018/kleines-einmaleins-der-digitalen-selbstverteidigung/#VPN (abgerufen am 11.01.19)

Gruber, Angela, Sickert, Teresa (2016) *Waffe des Münchner Amokläufers: Was ist eigentlich das Darknet?*, verfügbar unter www.spiegel.de/netzwelt/web/waffe-des-muenchen-amoklaeufers-was-ist-eigentlich-das-darknet-a-1104549.html (abgerufen am 12.01.19)

Indiana University (2018) *About proxy servers*, verfügbar unter https://kb.iu.edu/d/ahoo (abgerufen am 09.12.18)

Mowery, Keaton, Shacham, Hovav (2012) *Pixel Perfect: Fingerprinting Canvas in HTML5*, verfügbar unter: http://cseweb.ucsd.edu/~hovav/dist/canvas.pdf (abgerufen am 10.11.18)

Mozilla (o.J.) *Cookies – Informationen, die Websites auf Ihrem Computer ablegen*, verfügbar unter https://support.mozilla.org/de/kb/cookies-informationen-websites-auf-ihrem-computer (abgerufen am 29.12.18)

Petrlic, Ronald, Sorge, Christoph (2017) *Datenschutz Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie*, Wiesbaden: Springer Vieweg.

Regionales Rechenzentrum Erlangen (2017) *VPN*, verfügbar unter: https://www.rrze.fau.de/internet-e-mail/internet-zugang/vpn/ (nur Grafik; abgerufen am 09.12.18)

Schmidt, Jürgen (2016): *Tor und die versteckten Dienste*, verfügbar unter: https://www.heise.de/security/artikel/Tor-und-die-versteckten-Dienste-3280904.html (abgerufen am 06.12.18)

Schmidt, Jürgen (2018) *Vom Darknet lernen*, c't magazin für Computertechnik, 17/2018, S. 70-73

Tor Project (2018) *Tor: Overview*, verfügbar unter: https://www.torproject.org/about/overview.html.en (abgerufen am 10.11.18)

Von Westernhagen, Olivia (2018) *Die Grenzen der Anonymität*, c't magazin für Computertechnik, 17/2018, S. 80-84

Whitwam, Ryan (2014): *PORTAL is a travel router that offers instant anonymity after one-time setup*, verfügbar unter: https://www.extremetech.com/internet/188095-portal-is-a-travel-router-that-offers-instant-anonymity-after-one-time-setup (nur Grafik; abgerufen am 06.12.18)