Anonym

Darknet. Ein Leitfaden im Umgang mit dem dunklen Fleck im Deep Web

Diplomarbeit

GRIN

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de/ abrufbar.

Impressum:

Copyright © 2018 GRIN Verlag
ISBN: 9783668790391

Dieses Buch bei GRIN:

https://www.grin.com/document/439305

Anonym

Darknet. Ein Leitfaden im Umgang mit dem dunklen Fleck im Deep Web

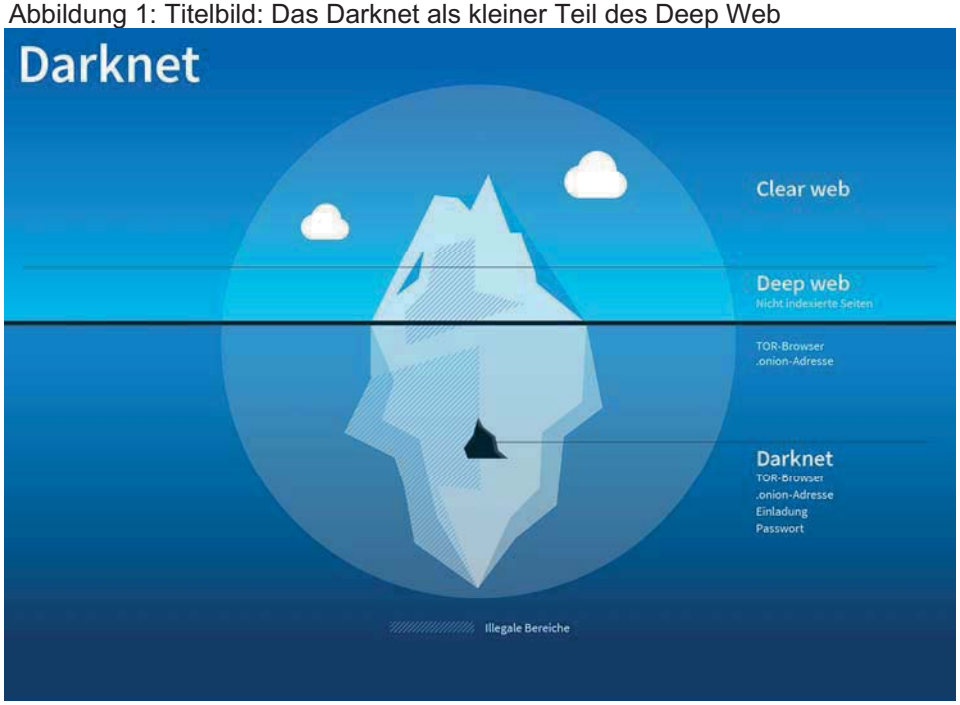
GRIN Verlag

DARKNET

–

EIN LEITFADEN IM UMGANG MIT DEM DUNKLEN FLECK IM DEEP WEB

Abbildung 1: Titelbild: Das Darknet als kleiner Teil des Deep Web



Anmerkung: (Eckermann, 2017).

Zertifikatsarbeit im
CAS Digital Risk Management

Zürcher Fachhochschule
HWZ Hochschule für Wirtschaft Zürich

Zürich, 29. Juni 2018

Management Summary

Vom Darknet wird in den Medien viel berichtet. Dass sich im Darknet unter anderem illegale Geschäfte abspielen, scheint der Allgemeinheit unterdessen bekannt zu sein. Dass die dahinterliegende Ursprungsidee von mehr Anonymität bei der Nutzung des Internets keine illegale war und dass das Darknet nur ein kleiner Teil des sogenannten «Deep Web» ist, wissen jedoch die wenigsten.

Das Deep Web beinhaltet die Daten im Internet, die nicht mehr über normale Web Suchmaschinen auffindbar sind. Dies ist zum Beispiel der Fall, sobald eine Website ein Login benötigt, was dazu führt, dass inzwischen 90 bis 99 Prozent der Daten im Internet zum Deep Web zählen.

Das Darknet ist ein Teil des Deep Web, der nicht nur über Web Suchmaschinen unauffindbar ist, sondern ganz bewusst unsichtbar sein will. Um auf die Bereiche im Darknet zugreifen zu können, wird spezielle Software benötigt, wie z.B. der Tor Browser. Dabei verläuft der Datenverkehr verschlüsselt und über unzählige, zufällig ausgewählte Rechner. Dadurch lassen sich Informationen über die Kommunikation nur schwer überwachen und rückverfolgen. Staatliche Zensuren, wie sie zum Beispiel in autoritär regierten Ländern mit inexistenter Meinungs- und Informationsfreiheit vorherrschen, können so umgangen werden. Politisch verfolgte Personen können sich dank solchen anonymen, nicht rückverfolgbaren Kommunikationswegen untereinander austauschen, sich organisieren und allenfalls Gegenbewegungen zu Diktaturen oder Repressionen entstehen lassen. Es gibt Stimmen, die der Ansicht sind, dass das Darknet zum Funktionieren einer modernen Demokratie beiträgt.

Das Darknet kann als Spiegel der Gesellschaft verstanden werden. Im vermeintlich anonymen und geschützten Umfeld wird angeboten und preisgegeben, was sowieso bereits schon tief im Inneren einer Person schlummert. Dementsprechend werden über die Seiten im Darknet auch sogenannte «Hidden Services», also Dienste, die der Öffentlichkeit verborgen bleiben sollen, angeboten. Spitzenreiter und somit die am meisten übers Darknet gehandelten Waren sind Drogen.

Der allgemeine Internetnutzer findet in einer Schritt-für-Schritt Anleitung verschiedene Tipps und Tricks, die zeigen, wie der Einstieg ins Darknet gelingt und wie man dabei möglichst sicher und möglichst anonym unterwegs ist.

Das Darknet ist kein rechtsfreier Raum und ist in den Fokus der Ermittlungs- und Strafverfolgungsbehörden geraten. Neuste Meldungen zeigen beispielhaft, dass im Darknet ermittelt wird und dies immer wieder mit Erfolg.

In Diskussionen um die Gefahren des Darknet kann man sich überlegen, ob es nicht sinnvoll wäre, das Darknet einfach gänzlich zu verbieten. Jedoch ändert ein Verbot nichts an den Personen, die sich darauf bewegen und deren Einstellung. Es verlagert nur das Geschehen an einen anderen Ort. Ob das Darknet verboten werden soll, muss sich jeder Einzelne selber überlegen. Hierzu liefern offene Fragen einen Denkanstoss und bilden gleichzeitig den Abschluss der vorliegenden Zertifikatsarbeit.

Inhaltsverzeichnis

Abbildungsverzeichnis

Begriffsverzeichnis und -erklärung

Begriff	Erklärung
Bitcoin	Digitale Währung und Name des weltweit verwendbaren dezentralen Buchungssystems
Blacklisting	Schwarze Liste, Sperrliste mit Personen oder Dingen, die gegenüber den nicht aufgeführten in irgendeiner Form benachteiligt werden sollen
Browser	Computerprogramm zum Darstellen von Webseiten im World Wide Web
Clear Net	Synonym für «Surface Web». In der vorliegenden Zertifikatsarbeit wird wenn immer möglich der Begriff «Surface Web» verwendet.
Clear Web	Synonym für «Surface Web». In der vorliegenden Zertifikatsarbeit wird wenn immer möglich der Begriff «Surface Web» verwendet.
Client	Endgerät, das Dienste von einem Server abruft
Crawler	Synonym für «Spider», Computerprogramm, das automatisch das World Wide Web durchsucht und Websiten analysiert.
Deep Web	Teil des Internets, der für normale Web Suchmaschinen nicht auffindbar ist. Dies trifft vor allem auf Websites zu, die mit einem Passwort geschützt sind oder sich in einem verschlüsselten Netzwerk befinden (darkwebnews.com, o. J.-b).
Darknet	Teil des Deep Web, der bewusst versteckt ist und dessen IP-Adressen anonymisiert sind. Für den Zugriff wird spezielle Software (Browser Tor, I2P, Freenet) benötigt (darkwebnews.com, o. J.-b).
Dark Net	Alternative Schreibweise von «Darknet». In der vorliegenden Zertifikatsarbeit wird wenn immer möglich die Schreibweise «Darknet» verwendet.
Dark Web	Synonym für «Darknet». In der vorliegenden Zertifikatsarbeit wird wenn immer möglich der Begriff «Darknet» verwendet.
Escrow	Escrow bedeutet so viel wie Treuhand oder Hinterlegung. Einige Marktplätze im Darknet bieten diesen Dienst an. Dabei wird der durch den Käufer bezahlte Betrag so lange für den Verkäufer gesperrt bis der Käufer bestätigt hat, dass er die Ware einwandfrei erhalten hat.
Fake	Schwindel, Betrug, Fälschung
Hacker	Person, die versucht, sich Zugang zu Computersystemen zu verschaffen. Kann positiver wie auch krimineller Natur sein.
IP-Adresse	Adresse in Computernetzen, die – wie das Internet – auf dem Internetprotokoll (IP) basiert.
Internet	Weltweiter Verbund von Rechnernetzwerken

Link	Kurzform für Hyperlink, Querverweis der einen Sprung zu einem anderen elektronischen Dokument oder an eine andere Stelle innerhalb eines Dokuments ermöglicht
Log File	Enthält das automatisch geführte Protokoll aller oder bestimmter Aktionen von Prozessen auf einem Computersystem
.onion	Special-Use-Top-Level-Domain zur Nutzung von hidden services (versteckte Dienste) im Anonymisierungsdienst The Onion Routing (Tor)
Server	Computer, der Computerfunktionalitäten wie Dienstprogramme, Daten oder andere Ressourcen bereitstellt, damit andere Computer oder Programme („Clients“) darauf zugreifen können, meist über ein Netzwerk.
Spider	Synonym für «Crawler», Computerprogramm, das automatisch das World Wide Web durchsucht und Websiten analysiert.
Surface Web	Teil des Internets, der an der Oberfläche liegt, öffentlich zugänglich ist und/oder über Web Suchmaschinen aufgerufen werden kann.
Tor	The Onion Routing, Netzwerk zur Anonymisierung von Verbindungsdaten
TOR	Alternative Schreibweise von «Tor». In der vorliegenden Zertifikatsarbeit wird wenn immer möglich die Schreibweise «Tor» verwendet, da diese der offiziellen Schreibweise von «The Tor Project» entspricht (The Tor Project, 2018b).
VPN	Virtual Private Network, virtuelles privates (in sich geschlossenes) Netzwerk, welche eine Punkt-zu-Punkt-Verbindung zur sicheren Datenübertragung ermöglicht
Webbrowser	Computerprogramm zum Darstellen von Webseiten im World Wide Web
WWW	World Wide Web

1. Einleitung

1.1. Ausgangslage

Das Darknet: «Was ist es?», «Wie komme ich da rein?» und «Gibt es dort wirklich nur illegale Ware?». Solche oder ähnliche Fragen wird sich der allgemeine Internetnutzer stellen, wenn er das Wort «Darknet» hört. Es scheint als ob bei der breiten Allgemeinheit wenig bis kein Wissen über das Darknet vorhanden ist. Der Name suggeriert jedoch, dass es sich dabei um etwas Dunkles, Verbotenes, Illegales handeln wird. Dass die Ursprungsidee – nämlich mehr Anonymität bei der Nutzung des Internets – keine illegale war und dass das Darknet nur ein kleiner Teil des sogenannten «Deep Web» ist, weiss nur, wer sich intensiver mit der Thematik befasst.

1.2. Problemstellung, Kontroverse

In den meisten deutschsprachigen Populärmedien werden die Begriffe Darknet und Deep Web synonym verwendet. In Wirklichkeit sind Darknet und Deep Web aber keineswegs identisch. Denn das Darknet ist nur ein kleiner Teil des Deep Web und es eilt ihm ein schlechter Ruf voraus: so soll das Darknet ein Marktplatz für Schurken, Banditen, Dealer, Mörder, Vergewaltiger und andere Personen illegaler Machenschaften sein. Dies zeigt sich in Alltagsgesprächen immer wieder von Neuem. Dass die ursprüngliche Idee und die damit verbundene Anonymisierungstechnik namens «Onion Routing» bzw. «**T**he **O**nion **R**outing» oder kurz «Tor» eine durchaus legale und gutartige gewesen ist, scheint sich dem Wissen der Allgemeinheit jedoch zu entziehen.

Anonymität für den Benutzer ist der Hauptnutzen der Tor Technik. Und Anonymität ist vor allem für zwei Gruppen, die gegensätzlicher nicht sein könnten, interessant:

GUT	**BÖSE**
Menschen, die zur Kommunikation Schutz benötigen	Menschen, die die Anonymität nutzen, um den negativen Konsequenzen, die aus ihrem Handeln folgen können (z.B. Strafverfolgung, Gewalt), zu entgehen
Teilen sensible Daten und Informationen	Üben Aktivitäten aus, die im sichtbaren Internet sehr schnell zu einer Anzeige sowie Geld- und Haftstrafen führen würden. Im Darknet finden sich Foren, Webshops und Handelsplattformen für Dienstleistungen und Waren, die sonst entweder illegal oder strengen gesetzlichen Regelungen unterworfen sind.

Müssen zum Teil um ihr eigenes Leben oder das ihrer Informanten fürchten	Müssen mit strafrechtlichen Konsequenzen und Gewalt rechnen
Politisch Unterdrückte oder Dissidenten, Oppositionelle aus diktaturgeführten Ländern, Journalisten, Whistleblower	Dealer, Mörder, Pädophile, Käufer und Konsumenten illegaler Waren und Dienstleistungen

Für den allgemeinen Internetnutzer ist es relativ einfach möglich, sich mittels Internetrecherche ausreichend (Halb-)Wissen anzueignen, um so ins Deep Web zu gelangen. Einmal im Deep Web ist der Schritt ins Darknet ein kleiner – und dabei dürften die Gefahren sowie die rechtlichen Aspekte im Umgang mit dem Darknet kaum oder nicht bekannt sein.

Diverse Berichterstattung zu Fahndungserfolgen im Darknet lassen Stimmen nach einem Verbot des Darknet laut werden. Doch es gibt auch andere Meinungen, die finden, das Darknet als Ganzes helfe dabei, Kontrolle und Zensur zu entgehen. Demnach wäre ein Verbot der zugrundeliegenden Technologien ein Angriff auf die moderne Demokratie («INTERVIEW ZU VORTEILEN VON DARKNET», 2017).

1.3. Zielsetzungen der Arbeit und erwartete Ergebnisse

Die Zertifikatsarbeit befasst sich mit der ursprünglichen Idee der Anonymisierungstechnik Tor und zeigt die Abgrenzung der zwei Begriffe «Deep Web» und «Darknet» sowie deren Einordnung im Internet auf. Die verschiedenen Einsatzzwecke (legaler sowie krimineller Natur) sollen erläutert werden. Es ist dem Verfasser wichtig, darstellen zu können, dass der Grundgedanke grundsätzlich positiven Ursprungs ist.

Als Ergebnis wird ein Leitfaden im Umgang mit dem Darknet angestrebt, der dem allgemeinen Internetnutzer die Vorteile der Tor Technik aufzeigt und wie er diese für legale Einsatzzwecke nutzt. In einer Schritt-für-Schritt Anleitung erfährt der allgemeine Internetnutzer, was für den Einstieg ins Deep Web und Darknet benötigt wird. Er erhält einen groben Überblick über die Funktionsweise und die Navigation und lernt zudem, welche Gefahren und rechtlichen Aspekte es zu berücksichtigen gilt. In einem Selbstversuch wird eine Bestellung übers Darknet getätigt. Die dabei gewonnen Erkenntnisse werden ebenfalls in den Leitfaden miteinfliessen.

2. Inhaltlicher Teil

2.1. Erklärung der Begrifflichkeiten und deren gegenseitige Abgrenzung

Was sich hinter den Begrifflichkeiten «Deep Web» und «Darknet» verbirgt und wie sie sich voneinander abgrenzen, wird nachfolgend erläutert:

2.1.1. Das Deep Web

Das Internet als Gesamtes besteht aus unzähligen Netzwerken (Shuler, 2002). Der öffentlich zugängliche Teil des Internets ist das Internet, wie wir es kennen. Synonyme hierfür sind «Free Web», «Freenet», «Visible Net», «Surface Web», «Clear Web» und «Clear Net». Es lässt sich am Namen erkennen, dass es sich hier um öffentliche Daten im Internet handelt, die über Web Suchmaschinen gefunden werden können.

Sobald Daten im Internet nicht mehr über normale Web Suchmaschinen auffindbar sind, spricht man vom Deep Web oder Invisible Net. Dies ist zum Beispiel der Fall, sobald eine Website ein Login benötigt, sie über einen unüblichen Port betrieben wird oder nur einer kleinen Gruppe bekannt ist (Ruef, 2016).
Je nachdem welcher Quelle man Glauben schenkt, sind zwischen 90 und 99 Prozent der Daten im Internet nicht über Web Suchmaschinen auffindbar und somit nicht indexiert (20 Minuten, 2017; darkwebnews.com, o. J.-a, o. J.-b). Um diese Websites aufzurufen, muss dem User die genaue Domain oder IP-Adresse bekannt sein. Eine Suchanfrage bei einer Web Suchmaschine wird keine Ergebnisse mit nicht-indexierten Websites aus dem Deep Web anzeigen.

Der oben angeführten Definition nach beinhaltet das Deep Web alle Websites, die durch Benutzerlogins geschützt sind sowie alle internen Websites und internen Daten innerhalb von geschützten Netzwerken von Unternehmen, Organisationen und auch privaten Personen. Die Mehrheit der im Deep Web existierenden Daten haben demnach keinen illegalen Hintergrund.

Vergleicht man das Internet mit einem Eisberg, der im Meer treibt, so ist bildet der unter der Wasseroberfläche liegende, nicht sichtbare Teil das Deep Web. Um zu diesem Teil des Eisbergs zu gelangen, muss gezielt getaucht werden.

Abbildung 2: Veranschaulichung des Free Web, Deep Web und Dark Web an der Metapher eines Eisbergs

Anmerkung: (Ruef, 2016).

2.1.2. Das Darknet

Das Darknet ist Teil des Deep Web und zeigt sich als Summe derjenigen Netzwerke, die nicht nur über Web Suchmaschinen unauffindbar sind, sondern ganz bewusst unsichtbar sein wollen. Hierüber werden sogenannte «Hidden Services», also Dienste, die der Öffentlichkeit verborgen bleiben sollen, angeboten.

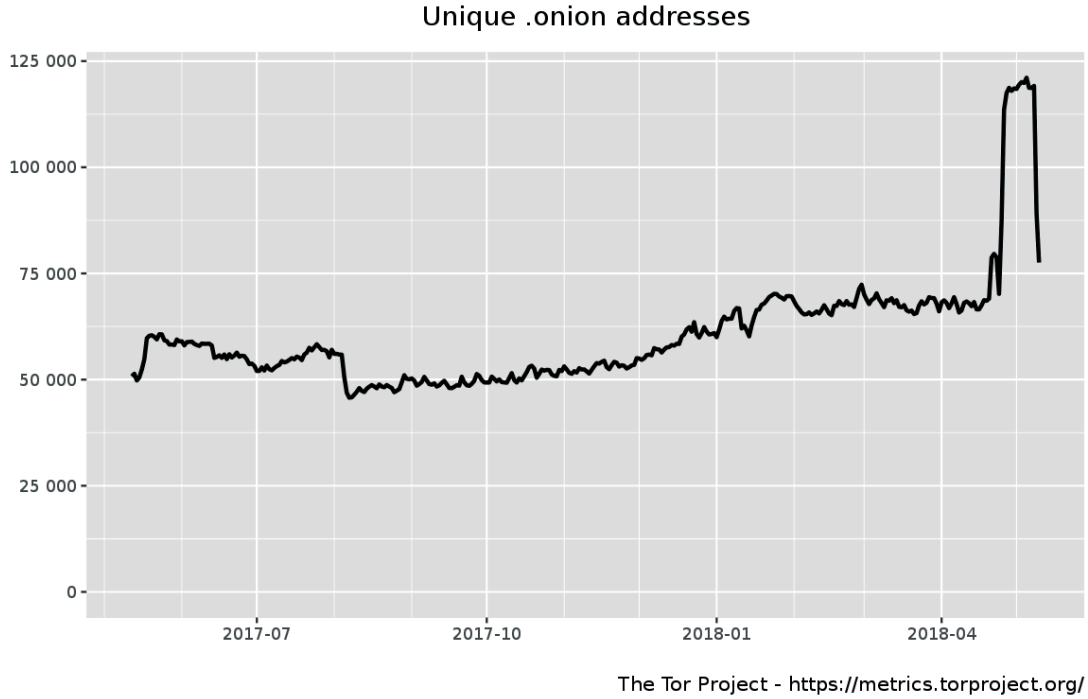
Der Begriff «Dark Web», der in Abbildung 2 verwendet wird, ist mit dem Begriff «Darknet» gleichgestellt. In der vorliegenden Zertifikatsarbeit wird, wenn immer möglich, der Begriff «Darknet» verwendet.

Im Darknet gibt es wie beim Free Web und Deep Web entsprechende Websites. Per Januar 2018 gab es im Darknet 6'608 Dark Websites (Hyperion Gray, 2018) – eine ziemlich überschaubare Anzahl im Vergleich zu den 1'876'077'522 (=1.876 Milliarden) aktiver Websites (Stand: 12. Mai 2018) im gesamten Internet (Internet Live Stats, 2018; Netcraft, 2018). Einen Überblick über die verschiedenen Dark Websites bietet die «Dark Web Map» – eine Art digitale Landkarte mit Screenshots aller Dark Websites (Hyperion Gray, 2018).

Nebst Dark Websites gibt es im Darknet auch Chat- oder Filesharing-Dienste, die als Hidden Service betrieben werden. Die 6’608 Screenshots in der Landkarte von Hyperion Gray stellen

also nur einen Ausschnitt des tatsächlichen Darknet dar. Weil es aber kein komplettes, öffentlich zugängliches und durchsuchbares Verzeichnis der derzeit mehr als 75’000 Hidden Services (gemäss Abbildung 3) gibt, ist dieser Ausschnitt eine nützliche Annäherung (spiegel.de, 2018).

Abbildung 3: Anzahl eindeutige .onion Adressen und Entwicklung von Mai 2017 bis Mai 2018



Anmerkung: (The Tor Project, 2018a).

Bei den speziellen Friend-2-Friend-Netzen (F2F) werden Daten nur noch dezentral unter Freunden ausgetauscht. Man sich also zuerst einen Bekannten- und Freundeskreis aufbauen bis man dort Daten austauschen kann (Ruef, 2016).
Bei den privaten Foren handelt es sich um exklusive Clubs, zu denen man nur auf Einladung Zutritt erhält. Solange man niemanden kennt, der für einen bürgt, wird der Zugriff verunmöglicht (Ruef, 2016).
Und schlussendlich gibt es noch die temporären Chat-Server. Diese werden kurzfristig und für ganz spezifische Transaktionen aufgebaut, um danach wieder abgeschaltet zu werden. Die Kommunikation wird vollständig verschlüsselt und auf das Anlegen von Logs wird verzichtet (Ruef, 2016).

Um auf die Bereiche im Darknet zugreifen zu können, wird spezielle Software benötigt, wie z.B. der Tor Browser (Reilly, 2017). Übertragen auf die in Abbildung 2 gezeigte Metapher mit dem Eisberg bedeutet dies, dass das Darknet den untersten Teil des Eisbergs darstellt. Um dorthin zu tauchen, wird spezielles Tauch-Equipment benötigt.

Es zeigt sich, dass je tiefer man sich im Darknet bewegt, desto grösser der Aufwand wird. Der Komfort und die Bedienerfreundlichkeit werden zu Gunsten einer höheren Sicherheit und Anonymität aufgegeben. Für normale Aktivitäten sind diese Bereiche deshalb nicht attraktiv, jedoch umso mehr für Akteure illegaler Machenschaften (Ruef, 2016).

2.2. Ursprungsidee des Deep Web und der Tor Technik

Der Datenverkehr verläuft beim Zugriff ins Darknet verschlüsselt und über unzählige, zufällig ausgewählte Rechner. Dadurch lassen sich Informationen über die Kommunikation nur schwer überwachen und rückverfolgen. Gerade bei der Kommunikation mit sensiblen Informationen als Inhalt ist keine Überwachung und Rückverfolgbarkeit durchaus gewünscht. Auch das Umgehen von staatlichen Zensuren, wie sie zum Beispiel in autoritär regierten Ländern mit inexistenter Meinungs- und Informationsfreiheit vorherrschen, kann ein Motivationsgrund sein, weshalb verschlüsselte, anonymisierte Kommunikationsmöglichkeiten genutzt werden. So wurde zum Beispiel im Rahmen des arabischen Frühlings in Ägypten eine Zunahme der Kommunikation via Tor Technik festgestellt (Zahorsky, 2011). Aktivisten des arabischen Frühlings konnten über das Tor Netzwerk auf die dort üblicherweise gesperrten Social Media Kanäle zugreifen und ihre Informationen über die Revolution verbreiten. Auch Whistleblower (der wohl bekannteste unter ihnen ist der ehemalige CIA Mitarbeiter Edward Snowden) nutzen das Deep Web, um brisante Informationen an die Öffentlichkeit zu bringen. Aber auch politisch verfolgte Personen nutzen die Möglichkeiten von anonymen Kommunikationswegen. Die Anonymisierung hilft Journalisten dabei, Ihre Quellen zu schützen. Anonyme, nicht rückverfolgbare Kommunikation spielt also eine wichtige Rolle bei der Vermeidung von negativen Konsequenzen durch staatliche Zensur, Repressalien und Verfolgung.
Marc Ruef, Mitinhaber der auf Informationssicherheit spezialisierten Firma scip AG und Dozent an der HWZ Zürich antwortet in einem Interview mit 20 Minuten wie folgt: «Die Idee des Darknet ist, sich anonym und unkontrolliert austauschen zu können.». Und weiters fügt er an: «...auch in Ländern mit umfangreicher staatlicher Kontrolle und harter Zensur spielt das Darknet eine wichtige Rolle. Ein technologisch ungehemmter Datenaustausch ist ein wichtiger Bestandteil einer modernen Demokratie.» (20 Minuten, 2017).

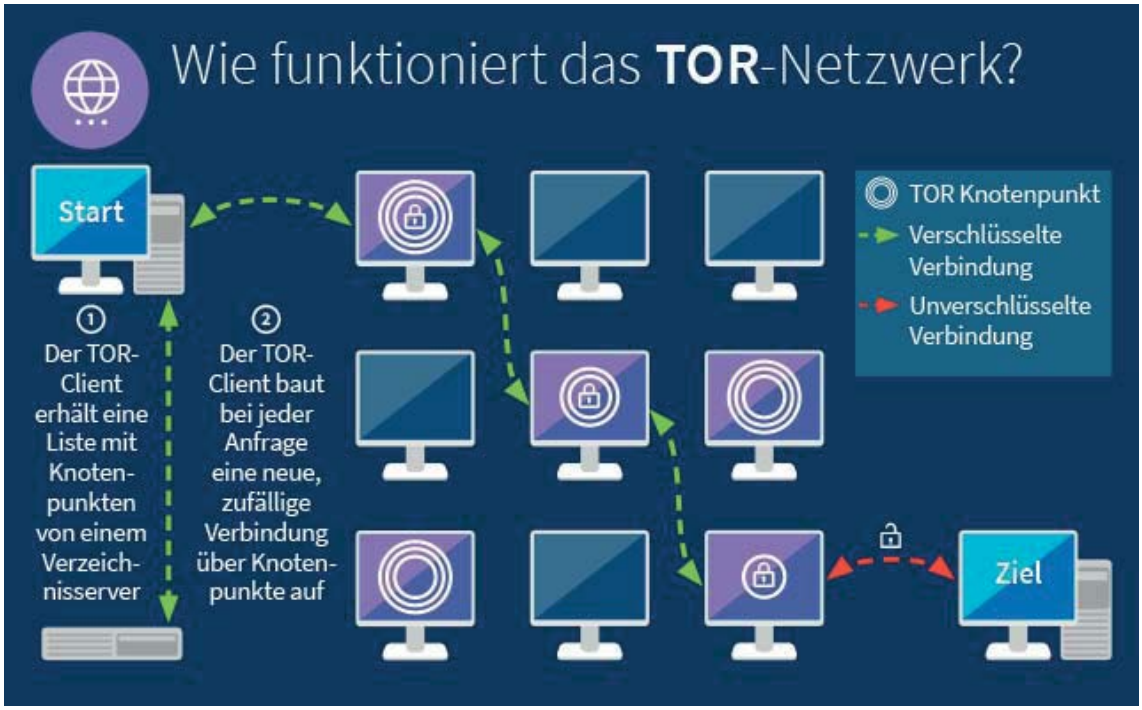
2.3. Erklärung der Tor Technik

Die im Darknet benutzte Anonymisierungs- und Verschlüsselungstechnologie kann als eine Art digitale Tarnkappe bezeichnet werden. Vorherrschend ist Tor. Tor stand ursprünglich für «**T**he **O**nion **R**outing». Die Grundidee des Aufbaus gleicht der einer Zwiebel: Bei der Zwiebel ist der Kern unter mehreren Schalen versteckt. Genauso verhält es sich bei Tor: der Kern, bestehend aus Identität und Aktivität der jeweiligen Internetnutzer verbirgt sich unter mehreren Anonymisierungsschichten (Mey u. a., 2017).

Die Anonymisierungstechnik nennt sich Onion Routing. Hierbei werden die Webinhalte über ständig wechselnde, zufällige Routen – über sogenannte «Knoten» – geleitet. Diese Verbindung ist verschlüsselt und der einzig ungesicherte Schritt ist der letzte: derjenige vom Tor

Exit Knoten zur Zieldestination (Bärlocher, 2017). Dadurch bleibt die wahre Identität dessen, der die Daten angefordert hat, für den Webserver auf der anderen Seite anonym.

Abbildung 4: Schematische Darstellung des Verbindungswegs von Client zu Client über das Tor Netzwerk

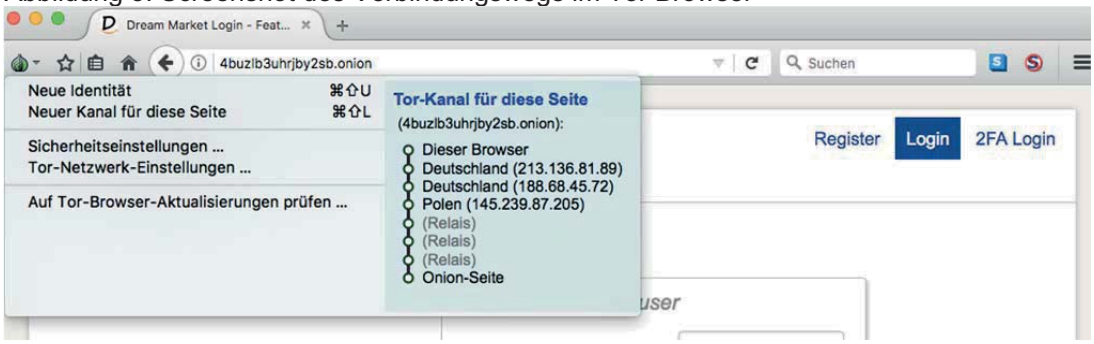


Anmerkung: (Eckermann, 2017).

Die Tor Knoten kennen nur den jeweils letzten Schritt, also von welchem Knoten der Pfad kommt, nicht aber dessen Anfang und dessen Zieldestination. Kein Knoten kennt je den gesamten Pfad. Jeder Sprung von Knoten zu Knoten ist mit einer eigens für diese Verbindung ausgehandelten Verschlüsselung versehen, was die Nachverfolgung des Pfades extrem schwierig bis unmöglich macht (Bärlocher, 2017).

Der Verbindungsweg über die verschiedenen zufällig ausgewählten Knoten kann im Tor Browser jederzeit abgerufen werden:

Abbildung 5: Screenshot des Verbindungswegs im Tor Browser



Anmerkung: Eigener Screenshot aus Tor Browser.

2.4. Top-Level-Domain .onion

Im Tor Netzwerk gibt es die bekannten Top-Level-Domain (.ch, .com, .de., .org und so weiter) nicht. Dafür gibt es eine einzige Top-Level-Domain: .onion.
Die URLs für die verschiedenen Dark Websites der Hidden Services bestehen aus einer kryptisch anmutenden Abfolge von Zahlen und Buchstaben. Der Marktplatz Dream Market zum Beispiel ist über verschiedene URLs zu erreichen [für Publikation entfernt] oder andere Onion-Adressen zu erreichen. Es kommt oft vor, dass die Onion-Adressen im Darknet häufig wechseln oder sogenannte «Mirror Links» als alternative Links verwendet werden. Dies ist eine Vorsichtsmassnahme der Marktplatzbetreiber, um es den Ermittlern etwas schwieriger zu machen.

2.5. Suchmaschinen im Deep Web und Darknet

Ja, es gibt sie: die Suchmaschinen fürs Deep Web. Jedoch lassen sich das Deep Web und damit auch das Darknet bewusst nur schwer durchsuchen, weshalb Suchmaschinen häufig weniger effektiv sind als vom Public Web gewohnt. Empfehlenswert ist, für jede Suche mehrere verschiedene Suchmaschinen zu benutzen, da nicht jede Suchmaschine die gleichen Resultate zeigt. Mögliche Suchmaschinen im Deep Web sind zum Beispiel Torch, TorSearch. Die von früher bekannte Suchmaschine namens Grams – die bislang nützlichste Suchmaschine im Deep Web – ist seit Ende 2017 offline (Beuth, 2017).

3. Systematische Betrachtung

3.1. Sinnvolle Anwendungsgebiete und deren Begründungen

In der Schweiz lebende Personen mögen sich fragen, wofür Anonymität im Internet denn nützlich oder sogar notwendig sein mag. Schliesslich hat man in der Schweiz – abgesehen von möglichen Stalkerangriffen – wenig zu befürchten. Die Schweiz gilt nicht als terroristisch gefährdetes Land. Hier kann man seine eigene Meinung frei verbreiten ohne dafür um sein eigenes Leben fürchten zu müssen. Und vom eigenen Staat geht ebenfalls keine Gefahr aus (Bärlocher, 2017). Dieses freie Leben gilt für Schweizer als Selbstverständlichkeit. Und dies zeigt sich auch bei einem Blick auf den Schweizer Eintrag bei Open Observatory of Network Interference (OONI) – einem globalen Netzwerk, welches sich zum Auftrag gemacht hat, Zensur, Überwachung und Verbindungsmanipulation im Internet aufzuspüren und sichtbar zu machen: Die Schweiz hat keine vom Staat zensierten Websites und der Zugang zu allen freien Informationen im Internet steht der Schweizer Bevölkerung offen (Open Observatory of Network Interference (OONI), 2018a).
In der Türkei zum Beispiel sieht die Situation etwas anders aus. Der Türkei Eintrag auf OONI zeigt eine lange Liste von zensierten Websites (Open Observatory of Network Interference (OONI), 2018b):

- Pornosites
- Sites über sexuelle Aufklärung
- Dating-Sites für Homosexuelle
- Filesharing Sites
- Streaming Sites
- Glücksspielportale
- Sites über die Aufklärung über Drogen, insbesondere Cannabis
- Websites mit politisch divergierender Meinung, wie zum Beispiel Hizb ut-Tahrir, eine islamistische und neofundamentalistische Organisation

Zudem ist bekannt, dass die Türkei situativ soziale Netzwerke, Google und verschiedene Newsportale komplett sperrt (Frankfurter Allgemeine, 2016). Hier spiegelt sich die in der Türkei vorherrschende staatliche Zensur wieder. Das Regime rund um Recep Tayyip Erdogan versucht so, Marschproteste, Kundgebungen und Aufstände bereits im Keim zu ersticken. Denn wenn sich die Oppositionellen und Andersdenkenden nicht organisieren können und keiner weiss, dass es einen Marschprotest gibt, dann geht auch keiner hin. Wenn in keiner Zeitung und auf keinem Newsportal zu lesen ist, dass das Regime Unschuldige attackiert, dann regt sich auch keiner darüber auf (Bärlocher, 2017).
Genau hier kann der anonyme Zugang ins Internet und damit die Umgehung von Zensur den Menschen in Krisengebieten helfen, sich frei zu informieren und mitzuteilen. In Ländern mit

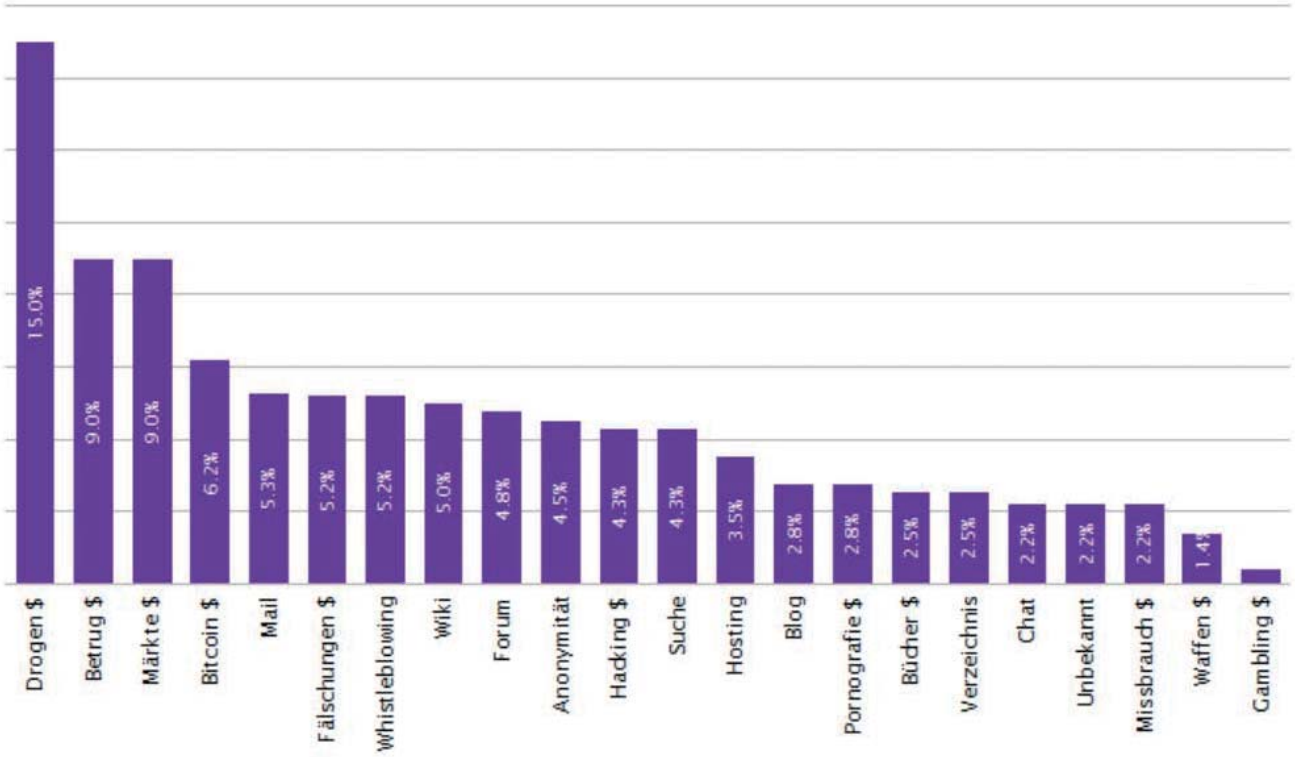
Unterdrückung und politischer Aufruhr kann zum Beispiel Tor helfen, dass sich Dissidenten und Oppositionelle organisieren und ihre Meinung frei äussern können. So hätte die Revolution rund um den arabischen Frühling nie stattgefunden, wenn es das Darknet nicht gegeben hätte, wo sich die Menschen anonym und vor dem Regime sicher organisiert haben (Bärlocher, 2017).

3.2. Illegale Anwendungsgebiete

Trotz der aufgezeigten Vorteile und der Tatsache, dass das Darknet und die damit einhergehende Anonymisierung ein für die Demokratie wichtiger Pfeiler darstellt, liegt es auf der Hand, dass sich unter dem Deckmantel der Anonymität auch viel Illegales abspielt.

Im Darknet tummeln sich die verschiedensten Angebote und Händler. Die nachfolgende Abbildung zeigt eine von Marc Ruef der Firma scip AG erstellten Auswertung zur Kategorisierung der verschiedenen Angebote im Darknet gehandelten Waren und Dienstleistungen. Spitzenreiter und somit die am meisten übers Darknet gehandelten Waren sind Drogen.

Abbildung 6: Kategorisierung der übers Darknet gehandelten Waren und Dienstleistungen



Anmerkung: (Ruef, 2016).

Die einzelnen Marktplätze funktionieren dabei ähnlich wie zum Beispiel Amazon: Es gibt verschiedene Angebote (Listings) mit Fotos, Beschreibungen, Hinweisen zur Qualität, Versandart, Lieferzeit, usw. Escrow – die Hinterlegung des bezahlten Kaufpreises bis zur erfolgreichen Lieferung des gekauften Artikels – gehört bei vielen Marktplätzen zum Standard. Anbieter können von Käufern mit Sternen und Kommentaren bewertet werden. Anbieter, die sich als Scammer (Betrüger) entpuppen, können von den Betreibern der Marktplätze gesperrt werden.

4. Leitfaden für den allgemeinen Internetnutzer im Umgang mit dem Darknet und der dahintersteckenden Tor Technik

4.1. Zwei Personas zur Beschreibung des allgemeinen Internetnutzers

Dieser Leitfaden richtet sich ganz bewusst an den allgemeinen Internetnutzer, sprich an Personen mit durchschnittlicher Anwendernutzung, ohne fachtechnische Kenntnisse (keine Informatiker, keine Digital Risk Managers oder anderes Fachpublikum). Es kann sinngemäss auch vom «Otto Normalverbraucher» gesprochen werden. Zur besseren Veranschaulichung, auf wen die Beschreibung des allgemeinen Internetnutzers zutrifft und ein Interesse am vorliegenden Leitfaden haben könnte, wurden die folgenden zwei Personas erstellt:

Abbildung 7: Zwei Personas zur Beschreibung des allgemeinen Internetnutzers

Judith Müller			**Stefan Graf**	
	**Merkmale, Motivation, Hintergrund:** Ist politisch interessiert, sieht sich als Gegnerin von Zensur und Einschränkung der Meinungs- und Informationsfreiheit, Neugier welche Möglichkeiten den unterdrückten und politisch verfolgten Personen zur Verfügung stehen			**Merkmale, Motivation, Hintergrund:** Ist kreativ, hat Auge für das Extravagante und nicht Alltägliche, ist weltoffen, hat eine liberale Denkhaltung, raucht gerne ab und zu einen Joint, ist für die Legalisierung von Cannabis, ist neugierig, was es im Darknet alles gibt, möchte wissen ob auf diesem Weg Cannabis erworben kann
Alter: 26 **Arbeit:** Praktikum bei einem grossen Schweizer Medienunternehmen **Ausbildung:** Abgeschlossenes Studium in Kommunikations- und Medienwissenschaft **Beziehungsstatus:** single **Wohnsituation:** WG mit zwei Freunden in der Stadt Zürich			**Alter:** 33 **Arbeit:** Webdesigner bei einer kleinen Web Agentur **Ausbildung:** Abgeschlossene Berufsausbildung als Grafiker **Beziehungsstatus:** in einer Beziehung, ledig **Wohnsituation:** lebt mit seiner Freundin in der Stadt Basel	

Anmerkung: Eigene Darstellung. Bildquellen: («Pixabay», 2017; Sakelli, 2018).

4.2. Schritt-für-Schritt Anleitung: «Wie komme ich rein und worauf muss ich achten?»

Im Internet existieren unzählige Anleitungen, die beschreiben, was benötigt wird, damit der Zugang ins Darknet gelingt. Eine einfache Suche mit einer normalen Web Suchmaschine wie Google oder Bing reicht aus, um entsprechende Schritt-für-Schritt Anleitungen zu finden. Es ist demnach äusserst einfach, aufs Darknet zuzugreifen. Um dabei möglichst sicher und möglichst anonym unterwegs zu sein, hilft die nachfolgende Schritt-für-Schritt Anleitung, die Tipps und Tricks verschiedener Quellen aufgreift. Diese sind als Ratschlag zu verstehen, sollten demnach befolgt werden – müssen jedoch nicht und haben keinen Anspruch auf Richtigkeit und Vollständigkeit. Zudem gilt es zu beachten, dass aufgrund der Geschwindigkeit von technischen Entwicklungen, einzelne oder mehrere Ratschläge nicht mehr aktuell sein können.

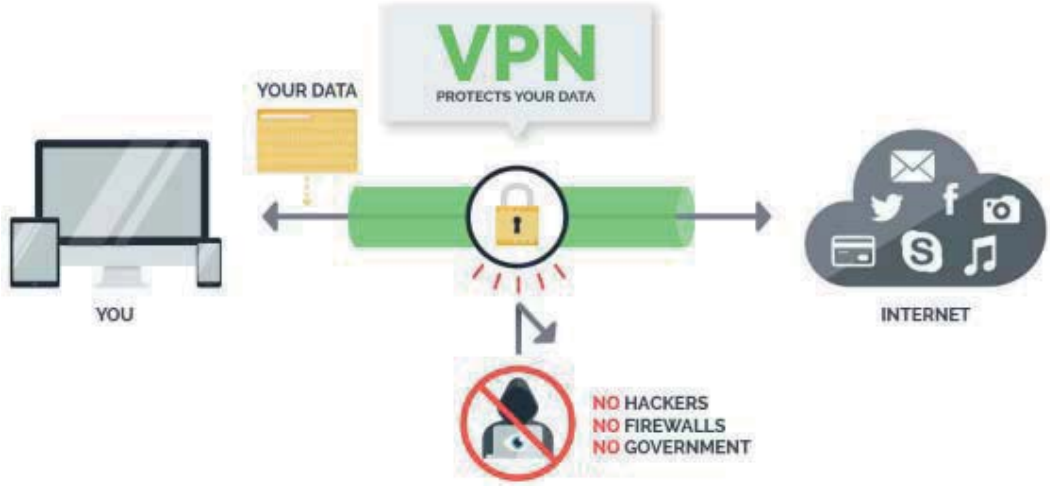
4.2.1. Schritt 1: Bewusstsein für Anonymität schaffen

Das wichtigste im Umgang mit dem Darknet und generell mit dem Internet ist, dass man sich bewusst ist, dass der Datenverkehr ohne geeigneten Massnahmen immer und überall mitgelesen werden kann.

4.2.2. Schritt 2: VPN herunterladen und installieren

Zuallererst sollte ein VPN Client (Virtual Private Network) installiert werden, der beim Surfen am besten immer verwendet wird, egal ob man über den Tor Browser surft und sich im Darknet bewegt oder nicht. Ein VPN Client sorgt dafür, dass die Verbindung ins Internet verschlüsselt und dadurch eine abhör- und manipulationssichere Kommunikation ermöglicht (Wikipedia.org, 2018) und dies kann bei sämtlichen Schritten im Internet von Vorteil sein.

Abbildung 8: Schematische Darstellung eines VPN



Anmerkung: (darkwebnews.com & Tarquin, 2018).

Bei der Wahl des VPN Clients ist darauf zu achten, dass dieser keine log files anlegt, eine schnelle Performance bietet, Kryptowährungen wie Bitcoin akzeptiert, mit dem Tor Browser kompatibel ist und über eine kill switch für DNS leaks verfügt (d.h. eine Art Notausschalter, der die Internetverbindung sofort unterbricht, sobald der VPN Tunnel nicht funktioniert wie er sollte, bis die sichere VPN-Verbindung wieder steht (R., 2017)). Bietet der VPN Client zudem die Möglichkeit für die Nutzung einer Fake IP-Adresse, zum Beispiel die eines anderen Landes, wird dadurch der Schutz weiter erhöht, da – für den Fall dass der Tor Browser kompromittiert sein sollte – die Spur nicht zu seiner effektiven IP-Adresse zurückverfolgt werden kann (darkwebnews.com & Tarquin, 2018). Die Website https://topvpnsoftware.org zeigt beispielsweise die fünf besten VPN Clients inklusive Bewertungen und weiteren hilfreichen Informationen für die Wahl des passenden VPN Clients (https://topvpnsoftware.org, 2018).

Abbildung 9: Screenshot der Website https://topvpnsoftware.org

Anmerkung: (https://topvpnsoftware.org, 2018).

4.2.3. Schritt 3: Tor Browser herunterladen und installieren

Wie an vorgängiger Stelle ausgeführt, wird für den Zugang ins Darknet spezielle Software benötigt. Gängige Webbrowser wie Internet Explorer, Google Chrome, Mozilla Firefox, Apple Safari, usw. sind nicht in der Lage, sich mit den Websites im Darknet zu verbinden. Es wird ein entsprechender Browser benötigt: entweder der weiterverbreitete Tor Browser, auf den sich die vorliegende Zertifikatsarbeit konzentriert, oder die weniger bekannten Browser I2P und Freenet (Reilly, 2017).

Es wird empfohlen, vor dem Download alle sich mit dem Internet verbindenden Dienste zu stoppen und erst den unter Schritt 2 heruntergeladenen und installierten VPN Client zu starten

und sich mit einem anderen Land zu verbinden. Ist die Verbindung über VPN hergestellt, kann der Tor Browser über die offizielle Website https://www.torproject.org mit dem gängigen Webbrowser, der bis jetzt normalerweise benutzt wurde, heruntergeladen werden. Der Tor Browser sollte unbedingt über die offizielle Website https://www.torproject.org heruntergeladen werden, da Download Files anderer Websites kompromittiert sein könnten.

Die Installation des Tor Browsers unterscheidet sich nicht von der Installation anderer gängigen Programme und gestaltet sich einfach. Ab diesem Zeitpunkt sind alle notwendigen Programme, die man für den anonymen Zugang ins Deep Web und Darknet benötigt, installiert und ab sofort können die Onion Websites besucht werden.

4.2.4. Schritt 4: Onion Websites finden und besuchen

Für den allgemeinen Internetnutzer vermag es anfangs ungewohnt und komisch wirken, dass fürs Surfen im Deep Web und Darknet die gewohnten WWW-Adressen nicht funktionieren bzw. keine solchen existieren und auch nicht über die gängigen Web Suchmaschinen wie Google oder Bing gefunden werden können. Die verschiedenen Websites im Deep Web und Darknet werden über sogenannte «Onion-Adressen» angesteuert. Um Onion-Adressen zu finden, können die unter Ziffer 2.5 erwähnten Suchmaschinen fürs Deep Web und Darknet genutzt werden. Oder man besucht eine der zahlreichen im Internet öffentlichen und ohne Tor Browser zugänglichen Websites, die Onion-Adressen zu verschiedenen Websites im Deep Web und Darknet auflisten. Eine solche Liste mit 4'715 Links verschiedener Kategorien kann zum Beispiel bei Darkwebnews.com gefunden werden.

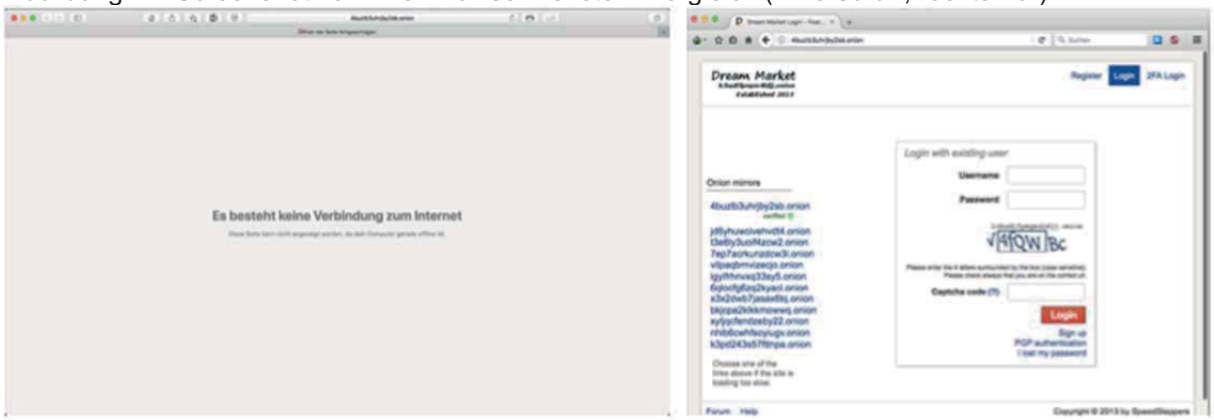
Abbildung 10: Screenshot der Website https://darkwebnews.com/deep-web-links

Name	URL	Description	Goods/Services	Need Registration	Need Invite	Status	Category	Screenshot
#1 Dream Market	http://4buzlb3uhrjby2sb.onion	Dream Market is Marketplace for Drugs, Digital Goods and Other Services.	Drugs, Digital Goods	Yes	No	Online	Marketplace Drugs	
#2 Silk Road 3	http://silkroad7rn2puhj.onion/	Silk Road 3 is the DarkNet's most resilient Marketplace. Products are sorted in categories. They sell Cannabis, Stimulants, Ecstasy, Opioids, Benzos, Dissociatives, Psychedelic, Prescription, and Other products.	Drugs, Weapons	Yes	No	Online	Marketplace Drugs	
#3 Valhalla	http://valhallaxmn3fydu.onion/	Valhalla is marketplace for Drugs sorted in categories. There are a lot of Cannabis, Stimulants, Empathogens, Psychedelics, Opiates, Pharmacy, Dissociatives and Depressants.	Drugs	Yes	No	Online	Marketplace Drugs	
#4 Point / Tochka Free Market	http://tochka3evlj3sxdv.onion	Tochka is dark market shipping to all countries. Drugs and other categories are sorted in categories.	Drugs, Digital Goods	Yes	No	Online	Marketplace Drugs	
#5 WallStreet Market	http://wallstytjzjhkrvmj.onion	WallStreet Market is one of the newest markets on the darknet and it particularly specializes in digital goods.	Drugs, Digital Goods	Yes	No	Online	Marketplace Drugs	
$$$	http://2jv5rmgnmze5l6l4.onion/	Only old users have access to join this website for cash	-	Yes	Yes	Online	Uncategorized	
$$$	http://2jv5r7k66ralyk3g.onion/	Only old users have access to join this website for cash	-	Yes	Yes	Online	Uncategorized	
$$$	http://2jv5rmgnmze5l6l4.onion	$$$ is invite only website, only old users have access to join or invite you.	-	Yes	Yes	Online	Uncategorized	

Anmerkung: (darkwebnews.com, o. J.-a).

Klickt man zum Beispiel auf den ersten Link (#1 Dream Market, http://4buzlb3uhrjby2sb.onion) in der Liste, so öffnet man die Website von Dream Market, einem Marktplatz für Drogen, Digitale Waren und anderen Services. Die Website öffnet sich – wie an früherer Stelle dargestellt – nur, wenn der Link über den Tor Browser geöffnet wird. Wird der Link über einen gängigen Webbrowser geöffnet, kann keine Website angezeigt werden, wie in der nachfolgenden Abbildung 11 zu sehen ist.

Abbildung 11: Screenshot von zwei Browser Fenstern Vergleich (links Safari, rechts Tor)



Anmerkung: Eigene Darstellung.

Wichtig: Es gibt auch normale Websites im Free Web, über welche die Onion-Adressen angesteuert und die Seiten im gängigen Webbrowser dargestellt werden können. Dies vermag einfach klingen – denn schliesslich entfällt die Installation des Tor Browsers – und scheint dementsprechend verlockend. Davon ist jedoch in jeglicher Hinsicht abzuraten, da hierüber die eigene IP-Adresse sichtbar, die Anonymität nicht sichergestellt und man dadurch angreifbar und rückverfolgbar ist.

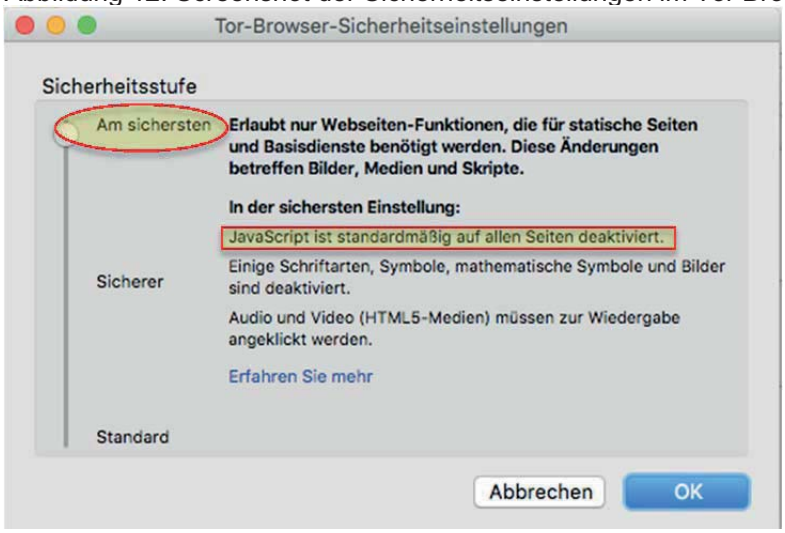
4.2.5. Schritt 5: Grösse des Tor Browser Fensters nicht verändern

Es vermag für den allgemeinen Internetnutzer komisch klingen, aber die Grösse, mit der sich das Fenster des Tor Browsers öffnet, sollte nicht verändert werden. Der Grund liegt darin, dass bereits kleinste Veränderungen der Fenstergrösse eine individuelle Einstellung auf dem einzelnen Rechner bedeuten. Diese individuelle Einstellung kann von den Strafverfolgungsbehörden entdeckt und zurückverfolgt werden. Wird die Fenstergrösse nicht verändert, bewegt man sich mit den gleichen standardmässigen Einstellungen wie der Grossteil der anderen Benutzer des Tor Browsers, sticht so nicht aus der Masse hervor und kann nicht zurückverfolgt werden.

4.2.6. Schritt 6: JavaScript im Tor Browser deaktivieren

Dass JavaScript als nicht sehr sicher gilt, ist unlängst bekannt (Tung, 2016). Deshalb wird empfohlen, das unsichere JavaScript im Tor Browser in den Sicherheitseinstellungen zu deaktivieren.

Abbildung 12: Screenshot der Sicherheitseinstellungen im Tor Browser



Anmerkung: Eigene Darstellung.

4.2.7. Schritt 7: Webcam trennen oder abdecken

Hacker und Regierungen verfügen über die technischen Mittel, um sich Zugriff auf fremde Rechner zu verschaffen und Webcams unbemerkt zu aktivieren. Es wird deshalb empfohlen, die Webcam vom Rechner entweder zu trennen oder – falls diese fest im Rechner verbaut ist – in geeigneter Art und Weise abzudecken, zum Beispiel mit einem schwarzen, blickdichten Klebeband, einem Webcam Cover (Link: https://soomz.io/de/) oder anderen Hilfsmitteln.

Abbildung 13: Webcam Covers

Anmerkung: (soomz.io, o. J.).

4.2.8. Schritt 8: Mikrofon trennen oder abdecken

Für das Mikrofon gilt das gleiche wie für die Webcam: auch das Mikrofon kann von extern durch Dritte unbemerkt aktiviert werden. Dementsprechend sollte das Mikrofon vom Rechner getrennt oder – falls dieses fest im Rechner verbaut ist – in geeigneter Art und Weise abgedeckt werden, zum Beispiel mit einem schwarzen, dicken Klebeband.

4.2.9. Schritt 9: Keine persönlichen Daten verwenden

Ist man zu leichtsinnig im Umgang mit seinen persönlichen Daten, nützen der beste VPN Client und die aktuellste Version des Tor Browsers nichts. Deshalb sollten persönliche Daten wie der eigene richtige Name, die Wohnortadresse, Telefonnummern, Fotos, die übliche E-Mailadresse und das Standardpasswort (welches man im schlechtesten Fall für unzählige Dienste verwendet) auf keinen Fall im Darknet benutzt werden. Es wird empfohlen, jedes Mal neue, noch nie im Darknet verwendete Daten zu verwenden. Für die E-Mailadresse wird der Einsatz von anonymen E-Mailservices empfohlen, die je nach Anbieter über Open PGP Datenverschlüsselung verfügen, keine Logfiles anlegen, Spam Schutz bereitstellen oder über andere Services zur Wahrung der Privatsphäre und Anonymität verfügen. Solche Anbieter

können beispielsweise auf der Website https://darkwebnews.com/anonymous-email gefunden werden (darkwebnews.com, o. J.-c).

4.2.10. Schritt 10: Ware kaufen und bezahlen im Darknet

Sollte die Intention bestehen, im Darknet Ware zu kaufen, gibt es auch hierfür wichtige Tipps, die es fürs sichere Bezahlen zu beachten gilt. Im Darknet wird mit Kryptowährungen bezahlt und die bekannteste und am weitesten verbreite heisst Bitcoin. Wie Bitcoins erworben werden können, wird in dieser Zertifikatsarbeit bewusst nicht behandelt, sondern es wird auf entsprechende Unterlagen zum Thema verwiesen.

Eine wichtige goldene Regel, um unter dem Radar der Polizei zu bleiben und um kein Geld durch die Schliessung des eigenen Wechselkontos für Kryptowährungen zu verlieren ist die folgende: Es wird empfohlen, Kryptowährungen niemals direkt vom eigenen Wechselkonto zu einem Marktplatz oder anderswo im Darknet (gilt auch für die umgekehrte Richtung) zu transferieren. Denn durch eine direkte Transferierung kann genau nachverfolgt werden, woher die Kryptowährung kam, beziehungsweise wohin sie geflossen ist. Dies kann dazu führen, dass das eigene Wechselkonto geschlossen wird, das Guthaben verloren geht und weitere Massnahmen (Blacklisting, Strafverfolgung, etc.) ergriffen werden. Um dies zu vermeiden, sollten Kryptowährungen immer vom eigenen Wechselkonto auf ein sogenanntes «Wallet» und von dort aus ins Darknet transferiert werden. Das gleiche gilt auch für die umgekehrte Richtung.

5. Schlussfolgerung / Empfehlungen

5.1. Gefahren, rechtliche Aspekte, Empfehlungen an den allgemeinen Internetnutzer

Im Darknet lauern Gefahren. So tummeln sich hier Personen unterschiedlichster Art mit einem oft kriminellen Motiv, weshalb das Darknet in den Fokus der Ermittlungs- und Strafverfolgungsbehörden geraten ist. Und den Behörden ist es auch bereits schon gelungen, trotz Verschlüsselungs- und Anonymisierungstechnologien, Darknet User zu identifizieren (Richard, 2017). Denn auch der Tor Browser hat Schwachstellen, die nach Bekanntwerden von Hackern, Kriminellen, Behörden und anderen ausgenutzt werden konnten (Richard, 2018b). Diesen Gefahren muss man sich im Umgang mit dem Darknet bewusst sein.

Das Darknet ist kein rechtsfreier Raum. So etwas wie einen rechtsfreien Raum gibt es nicht. Viele der Verbrechen, die mithilfe des Darknet begangen werden, lassen sich durch bestehende Gesetze adressieren. Drogen werden angebaut, verkauft, verschickt, importiert und konsumiert. Dafür braucht es keine neuen Gesetze. Das gilt auch für Verbrechen im Bereich Cybercrime (z. B. Verkauf von gestohlenen Daten). Entsprechende Gesetze sind vorhanden, um diese ahnden zu können (20 Minuten, 2017). Und dass dies geschieht, zeigen folgende Meldungen beispielhaft:
«FBI Employed CMU To Unmask Dark Web Suspects» (Richard, 2017)
«FBI Hacked Tor and Took Down A Child Sexual Exploitation Site» (Richard, 2018a)
«Schweiz ermittelt gegen Dealer im Darknet» (20 Minuten, 2018)

Es gilt jedoch zu bedenken: wenn die Polizei in der Lage ist, Kinderschänder im Darknet mit technologischen Mitteln aufzuspüren, dann können z.B. auch autoritäre Regime dieselbe Methode verwenden, um Freiheitskämpfer zu verfolgen (Bärlocher, 2017)

5.2. Fazit, Schlusswort

In Diskussionen um die Gefahren des Darknet kann man sich überlegen, ob es nicht sinnvoll wäre, das Darknet einfach gänzlich zu verbieten. Den Zugang zu blockieren und jeden Versuch, sich trotzdem irgendwie Zugang zu verschaffen, unter Strafe zu stellen. Es darf jedoch nicht vergessen werden, dass eine moderne Demokratie darauf baut, dass sich scheidende Meinungen und Weltansichten in Punkto Moral und Ethik auf einer Ebene begegnen können, ohne sich verfolgt fühlen zu müssen (Bärlocher, 2017). Das Darknet kann als Spiegel der Gesellschaft verstanden werden. Im vermeintlich anonymen und geschützten Umfeld wird angeboten und preisgegeben, was sowieso bereits schon tief im Inneren einer Person schlummert. Ob dies nun kriminelle Absichten oder pädophile Gelüste sind. Ein Verbot des Darknet ändert nichts an dieser Person und deren Einstellung. Es verlagert nur das Geschehen an einen anderen Ort.

Ob das Darknet verboten werden soll, muss sich jeder Einzelne selber überlegen. Dazu liefern die folgenden Fragen einen Denkanstoss:

«Wie viel Freiheit wollen wir für die Sicherheit aufgeben, die dann oft nur Illusion ist?» (Bärlocher, 2017).

«Sind 14 verhaftete Pädophile es wert, dass hunderttausende Freiheitskämpfer in Angst, verfolgt zu werden, leben müssen?» (Bärlocher, 2017).

«Wen schützen wir wie? Und während wir die einen schützen, wen bringen wir in Gefahr?» (Bärlocher, 2017).

Quellenverzeichnis

20 Minuten. (2017). Das Darknet zu verbieten hätte verheerende Folgen. Abgerufen 21. April 2018, von http://www.20min.ch/digital/news/story/-Das-Darknet-zu-verbieten--haette-verheerende-Folgen--16335092

20 Minuten. (2018). Schweiz ermittelt gegen Dealer im Darknet. Abgerufen 16. Juni 2018, von http://www.20min.ch/schweiz/news/story/Schweiz-arbeitet-an-Schlag-gegen-Dealer-im-Darknet-16128478

Bärlocher, D. (2017). Das Darknet: Ein wichtiges Instrument für die Freiheit - digitec. Abgerufen 21. April 2018, von https://www.digitec.ch/de/page/das-darknet-ein-wichtiges-instrument-fuer-die-freiheit-5377

Beuth, P. (2017). Darknet-Suchmaschine Grams wird abgeschaltet. *Zeit Online*. Abgerufen von https://www.zeit.de/digital/internet/2017-12/tor-netzwerk-grams-darknet-suchmaschine-abgeschaltet-bitcoin

Coinbase. (2018). Coinbase.

CyberGhost. (2018). CyberGhost. Abgerufen 28. April 2018, von https://www.cyberghostvpn.com/de_DE/

darkwebnews.com. (o. J.-a). Deep Web Links Grand List (7839 Hidden Links). Abgerufen 21. April 2018, von https://darkwebnews.com/deep-web-links/

darkwebnews.com. (o. J.-b). Deep Web What is it and how to access it (Ultimate Guide 2018). Abgerufen 21. April 2018, von https://darkwebnews.com/deep-web/

darkwebnews.com. (o. J.-c). Worried about privacy? Create Anonymous Email in 2018 (Free-Paid). Abgerufen 21. April 2018, von https://darkwebnews.com/anonymous-email/

darkwebnews.com, & Tarquin. (2018). How To Access Notorious Dark Web Anonymously (10 Step Guide). Abgerufen 21. April 2018, von https://darkwebnews.com/help-advice/access-dark-web/

Dream Market. (2018). Abgerufen 28. April 2018, von http://7ep7acrkunzdcw3l.onion/

Eckermann, I. M. (2017). Was ist eigentlich das Darknet? Abgerufen 25. Juni 2018, von https://www.gdata.de/ratgeber/was-ist-eigentlich-das-darknet

Frankfurter Allgemeine. (2016, November 4). Soziale Netzwerke in der Türkei blockiert. *Frankfurter Allgemeine*. Abgerufen von http://www.faz.net/aktuell/politik/ausland/europa/tuerkei-sperrt-whatsapp-twitter-und-facebook-nach-festnahmen-14512369.html

Grenzpaket. (2018). Abgerufen 23. Juni 2018, von https://www.grenzpaket.ch/de/

https://topvpnsoftware.org. (2018). Find The Top VPN Software For Your Needs. Abgerufen 21. April 2018, von https://topvpnsoftware.org

Hyperion Gray. (2018). Dark Web Map. Abgerufen 12. Mai 2018, von https://www.hyperiongray.com/dark-web-map/

Internet Live Stats. (2018). Total number of Websites. Abgerufen 12. Mai 2018, von http://www.internetlivestats.com/total-number-of-websites/

INTERVIEW ZU VORTEILEN VON DARKNET. (2017). Abgerufen 21. April 2018, von https://www.scip.ch/?news.20170809

Mey, S., Hostettler, O., Beutelspacher, A., Moßbrucker, D., Schulze, M., Brenneis, F., & Tzanetakis, M. (2017). *APuZ AUS POLITIK UND ZEITGESCHICHTE: Darknet*. Bundeszentrale für politische Bildung, Bonn.

Netcraft. (2018). April 2018 Web Server Survey. Abgerufen 12. Mai 2018, von https://news.netcraft.com/archives/2018/04/26/april-2018-web-server-survey.html

Open Observatory of Network Interference (OONI). (2018a). Switzerland. Abgerufen 21. Mai 2018, von https://explorer.ooni.torproject.org/country/CH

Open Observatory of Network Interference (OONI). (2018b). Turkey. Abgerufen 21. Mai 2018, von https://explorer.ooni.torproject.org/country/TR

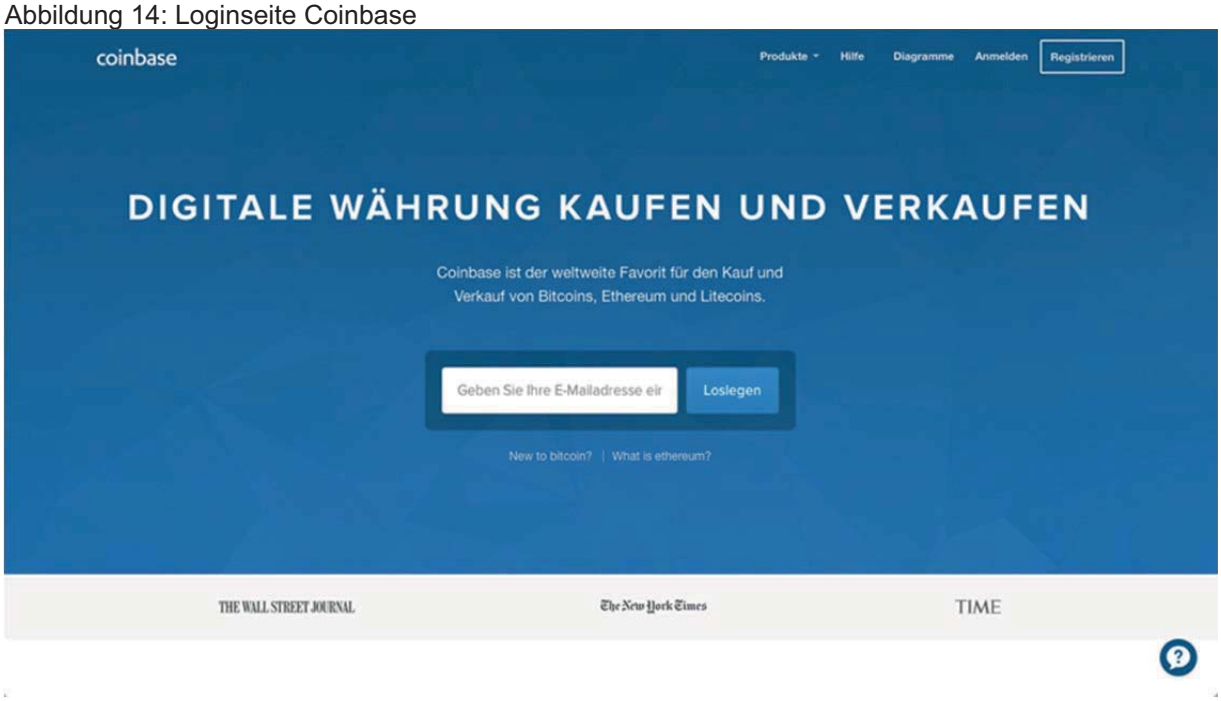
Pixabay. (2017). Abgerufen 12. Mai 2018, von https://pixabay.com/en/vsta-co-women-vans-relaxation-2142005/
R., C. (2017). VPN Kill Switch, What Is And Why You Should Use It. Abgerufen 20. Juni 2018, von https://anonymster.com/vpn-kill-switch-guide/
Reilly, C. (2017). Dark Web 101: Your guide to the badlands of the internet. Abgerufen 12. Mai 2018, von https://www.cnet.com/news/darknet-dark-web-101-your-guide-to-the-badlands-of-the-internet-tor-bitcoin/
Richard. (2017). FBI Employed CMU To Unmask Dark Web Suspects. Abgerufen 16. Juni 2018, von https://darkwebnews.com/dark-web/fbi-employed-cmu-to-unmask-dark-web-suspects/
Richard. (2018a). FBI Hacked Tor and Took Down A Child Sexual Exploitation Site. Abgerufen 16. Juni 2018, von https://darkwebnews.com/anonymity-tools/tor/fbi-hacked-tor-and-taken-down-a-child-pornography-site/
Richard. (2018b). Update Now – Critical TorMoil Vulnerability Found in Tor Browser. Abgerufen 16. Juni 2018, von https://darkwebnews.com/anonymity-tools/tor/tor-turmoil-vulnerability/
Ruef, M. (2016). Darknet - Einsicht in den virtuellen Schwarzmarkt. Abgerufen 21. April 2018, von https://www.scip.ch/?labs.20160114
Sakelli, J. (2018). Pexels. Abgerufen 12. Mai 2018, von https://www.pexels.com/photo/man-smoking-cigarette-stick-1011529/
Shuler, R. (2002). How Does the Internet Work? Abgerufen 12. Mai 2018, von https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm
soomz.io. (o. J.). Webcam Cover - Webcam Abdeckung | soomz.io. Abgerufen 21. April 2018, von https://soomz.io/de/detail/webcam_covers_a54
spiegel.de. (2018). Das Darknet in einer Landkarte. Abgerufen 12. Mai 2018, von http://www.spiegel.de/netzwelt/web/darknet-als-landkarte-pornos-exkremente-whistleblower-a-1198474.html
The Tor Project. (o. J.). The Tor Project. Abgerufen 21. April 2018, von https://www.torproject.org/
The Tor Project. (2018a). Onion Services – Tor Metrics. Abgerufen 12. Mai 2018, von https://metrics.torproject.org/hidserv-dir-onions-seen.html
The Tor Project. (2018b). Tor: Onion Service Protocol.
Tung, L. (2016). Why is Java so insecure? Buggy open source components take the blame. Abgerufen von https://www.zdnet.com/article/why-is-java-so-insecure-buggy-open-source-components-take-the-blame/
Wikipedia.org. (2018). Virtual Private Network. Abgerufen 21. April 2018, von https://de.wikipedia.org/wiki/Virtual_Private_Network
Zahorsky, I. (2011). Tor, Anonymity, and the Arab Spring: An Interview with Jacob Appelbaum. Abgerufen 12. Mai 2018, von http://www.monitor.upeace.org/innerpg.cfm?id_article=816

Anhang A: Eine Bestellung im Darknet tätigen im Rahmen eines Selbstversuches

Der Leser beziehungsweise die Leserin der vorliegenden Zertifikatsarbeit mag sich fragen, ob die in den verschiedenen Marktplätzen angebotenen Waren und Dienstleistungen auch wirklich echt sind und bei Bestellung geliefert/ausgeführt werden. Der Autor hat sich entschieden, im Rahmen eines Selbstversuches eine Bestellung im Darknet zu tätigen und seine Erkenntnisse in diese vorliegende Zertifikatsarbeit einfliessen zu lassen. Da der Selbstversuch nach Rücksprache mit der Studiengangsleitung keinen Einfluss auf die Bewertung der vorliegenden Zertifikatsarbeit hat, finden sich die daraus resultierenden Erkenntnisse im Anhang wieder. Die nachfolgenden Screenshots sind vom Autor selbst erstellt und enthalten teilweise persönliche Daten. Aus Selbstschutz und auch im Bewusstsein, dass dieser Selbstversuch die Grenze zur Illegalität überschreitet, sind einzelne Stellen mit einem schwarzen Balken mit der Inschrift «zensiert» überdeckt.

Coinbase ist ein Marktplatz, um Kryptowährungen wie Bitcoin, Bitcoin Cash, Ethereum und Litecoin zu kaufen und zu verkaufen. Zudem bietet es den Service eines Wallets, um die gekauften Kryptowährungen sicher aufzubewahren und Zahlungen zu tätigen und zu erhalten.

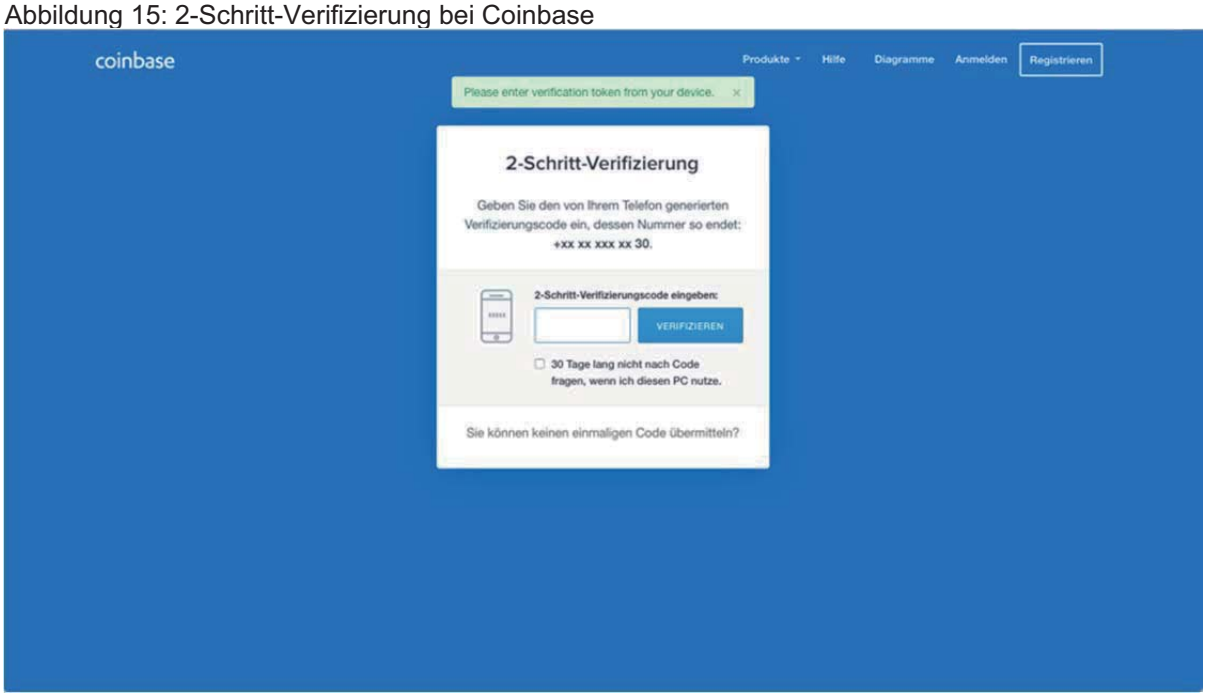
Abbildung 14: Loginseite Coinbase



Anmerkung: (Coinbase, 2018).

Das Login bei Coinbase funktioniert mittels E-Mailadresse und Passwort sowie einer 2-Schritt-Verfizierung mittels zugesendetem Einmalcode via SMS.

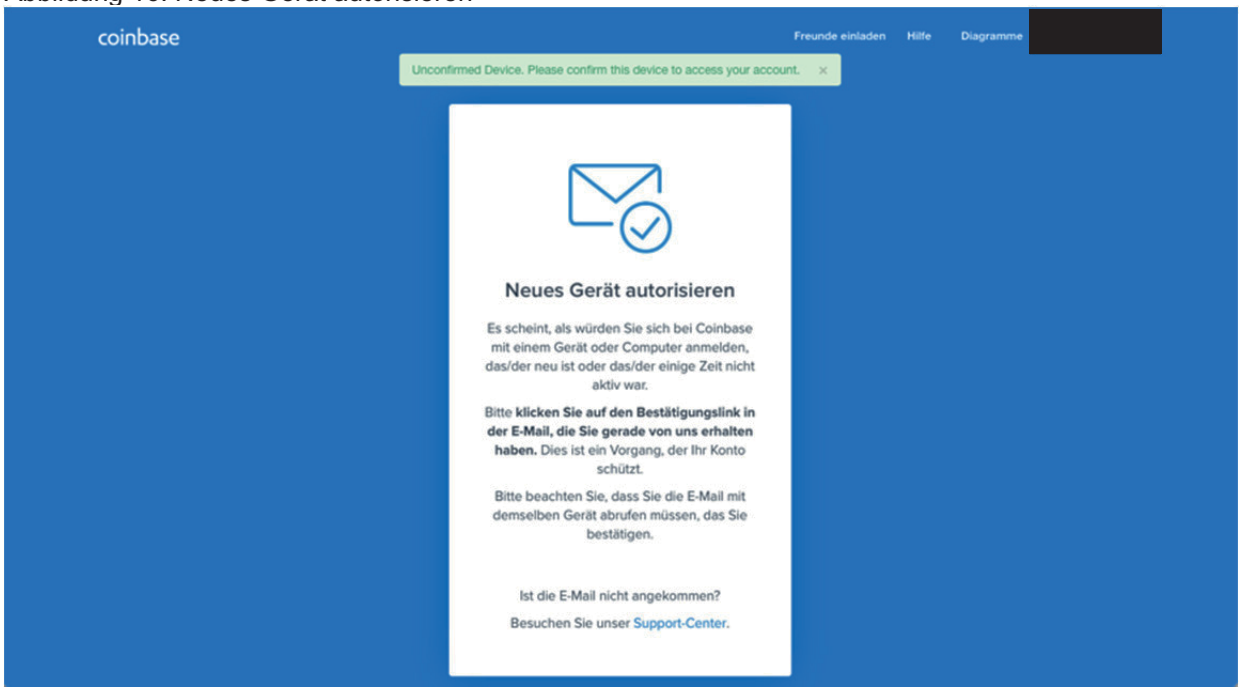
Abbildung 15: 2-Schritt-Verifizierung bei Coinbase



Anmerkung: (Coinbase, 2018).

Als weitere Sicherheitsmassnahme verlangt Coinbase, dass jedes neue Gerät autorisiert wird. Hierzu wird eine E-Mail mit einem Link an den User gesendet. Das neue Gerät wird durch einen Klick auf diesen Link autorisiert.

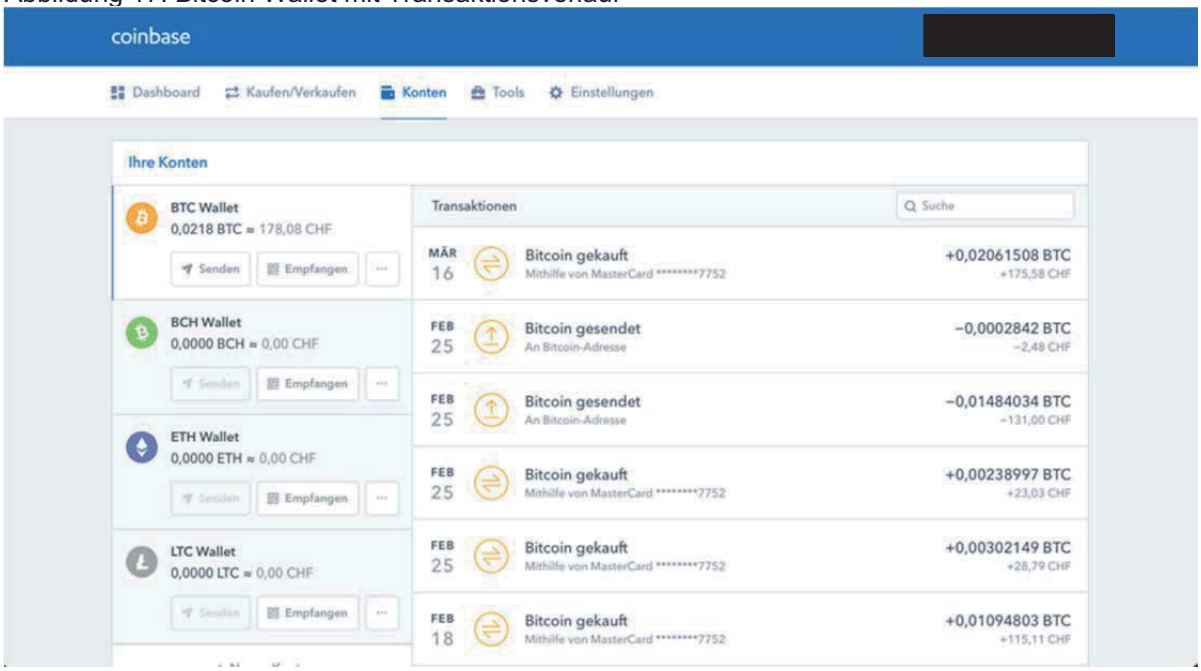
Abbildung 16: Neues Gerät autorisieren



Anmerkung: (Coinbase, 2018).

Nach dem Login bei Coinbase ist das Wallet mit dem Transaktionsverlauf sichtbar. Es zeigt den aktuellen Guthabenstand sowie die vergangenen Transaktionen (Bitcoins gekauft, Bitcoins verkauft, Bitcoins gesendet, Bitcoins erhalten).

Abbildung 17: Bitcoin Wallet mit Transaktionsverlauf



Anmerkung: (Coinbase, 2018).

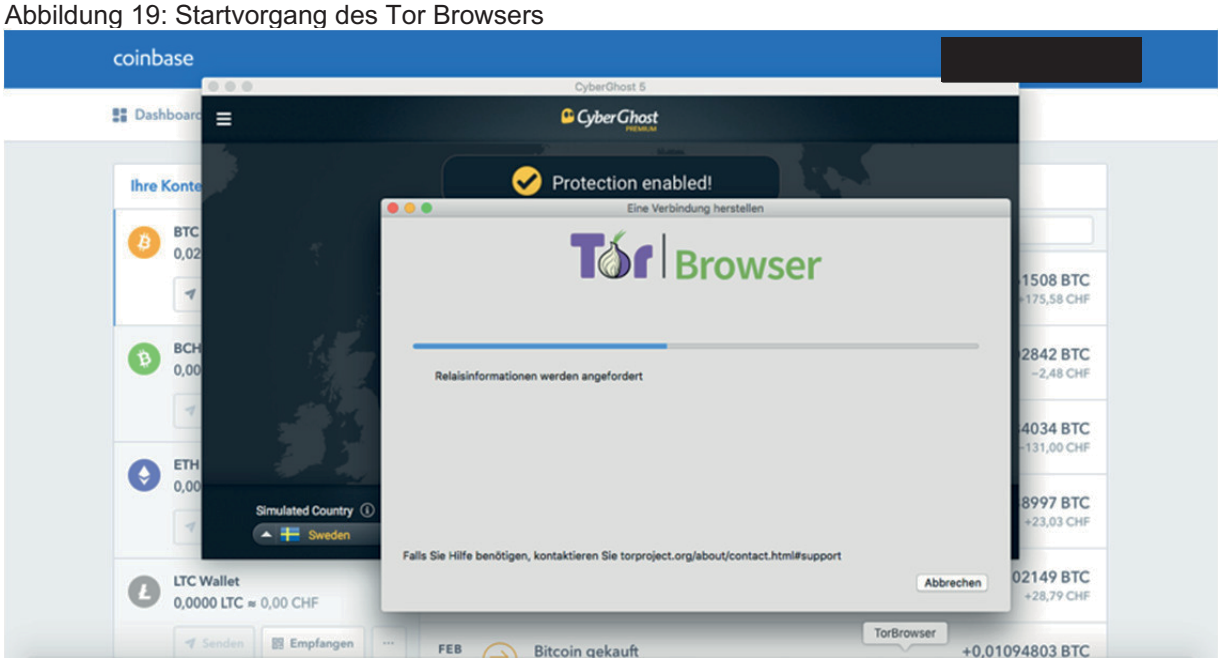
Nachdem das Bitcoin Wallet über genügend Guthaben verfügt, kann nun der Schritt ins Darknet gemacht werden. Hierzu ist erst der VPN Client zu öffnen und zu aktivieren.

Abbildung 18: VPN Client CyberGhost aktiviert

Anmerkung: (CyberGhost, 2018).

Da die VPN-Verbindung steht, kann nun der Tor Browser gestartet werden.

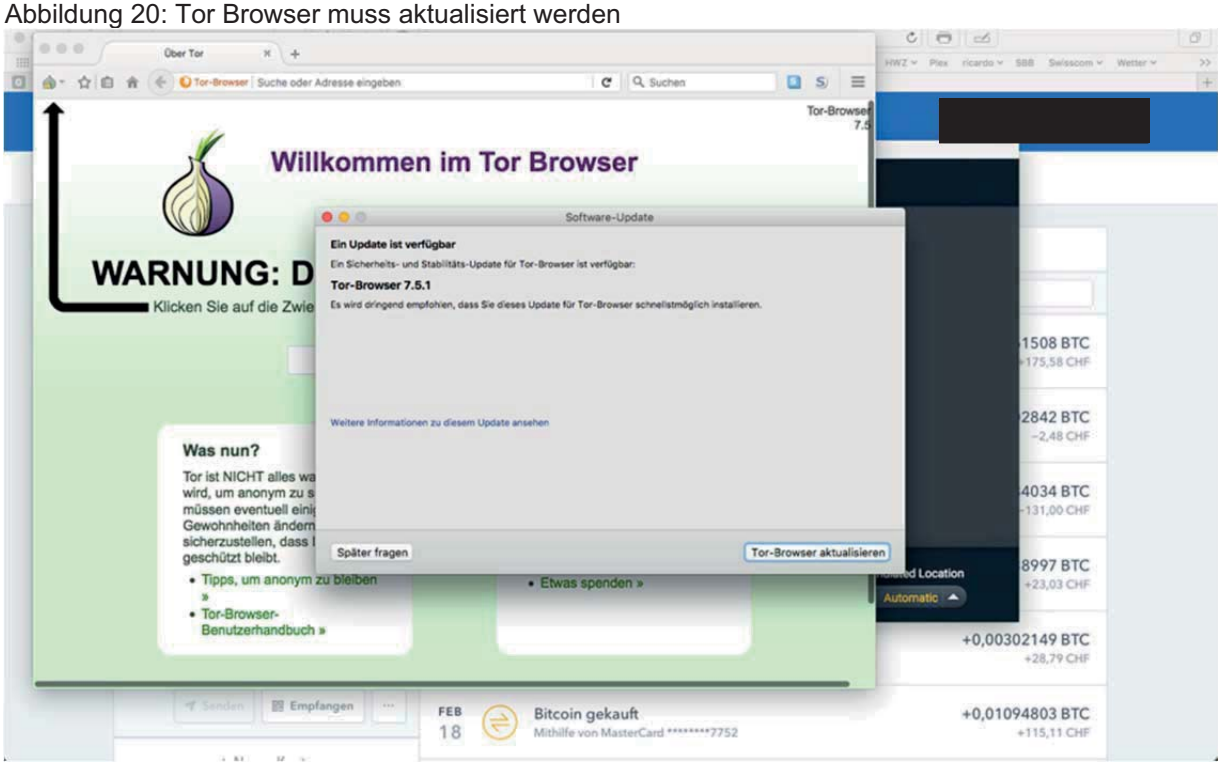
Abbildung 19: Startvorgang des Tor Browsers



Anmerkung: (The Tor Project, o. J.).

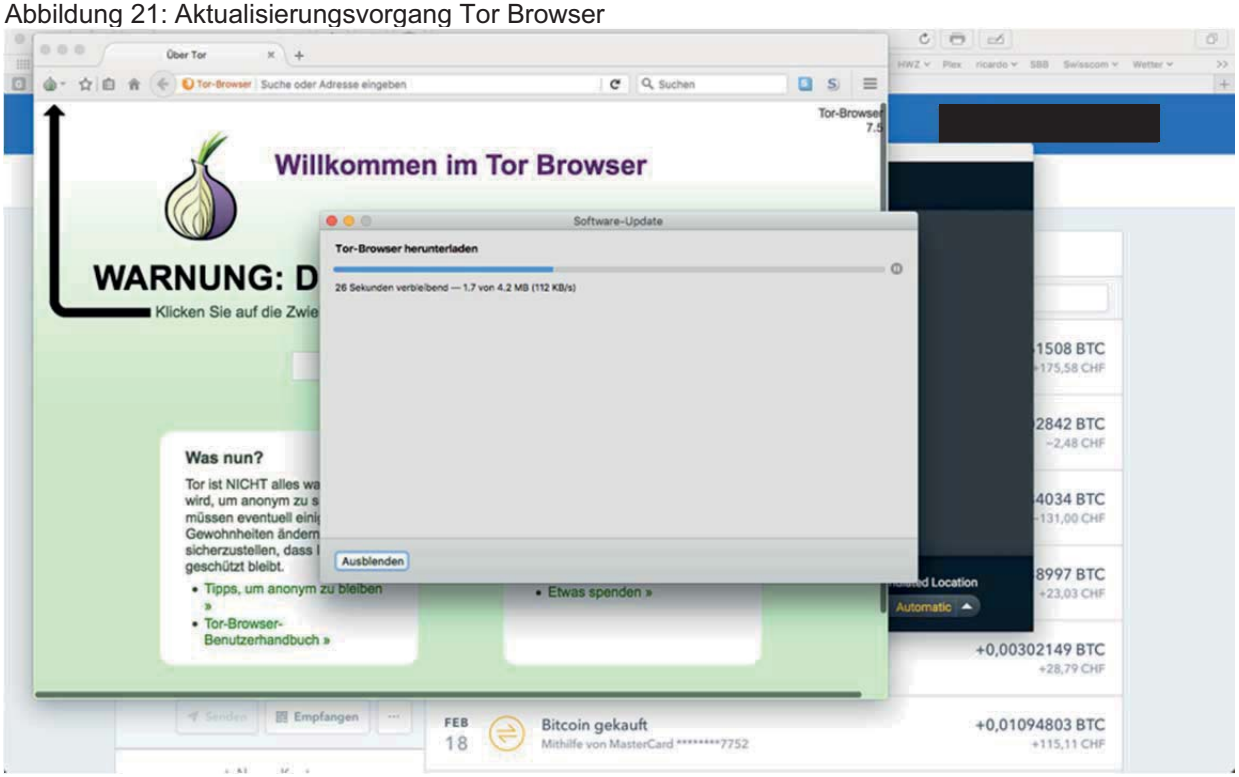
Während des Startvorgangs des Tor-Browser wird geprüft, ob Updates verfügbar sind. Im vorliegenden Fall sind Updates verfügbar und der Tor Browser muss aktualisiert werden.

Abbildung 20: Tor Browser muss aktualisiert werden



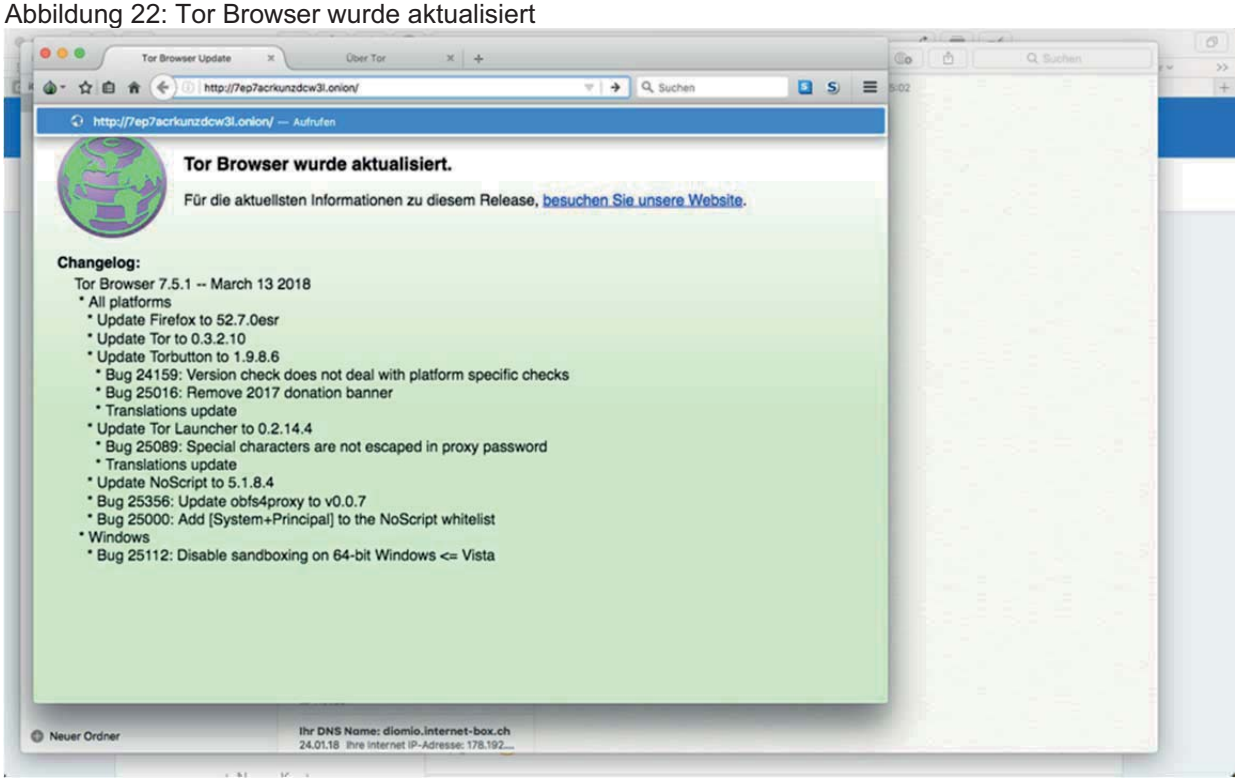
Anmerkung: (The Tor Project, o. J.).

Abbildung 21: Aktualisierungsvorgang Tor Browser



Anmerkung: (The Tor Project, o. J.).

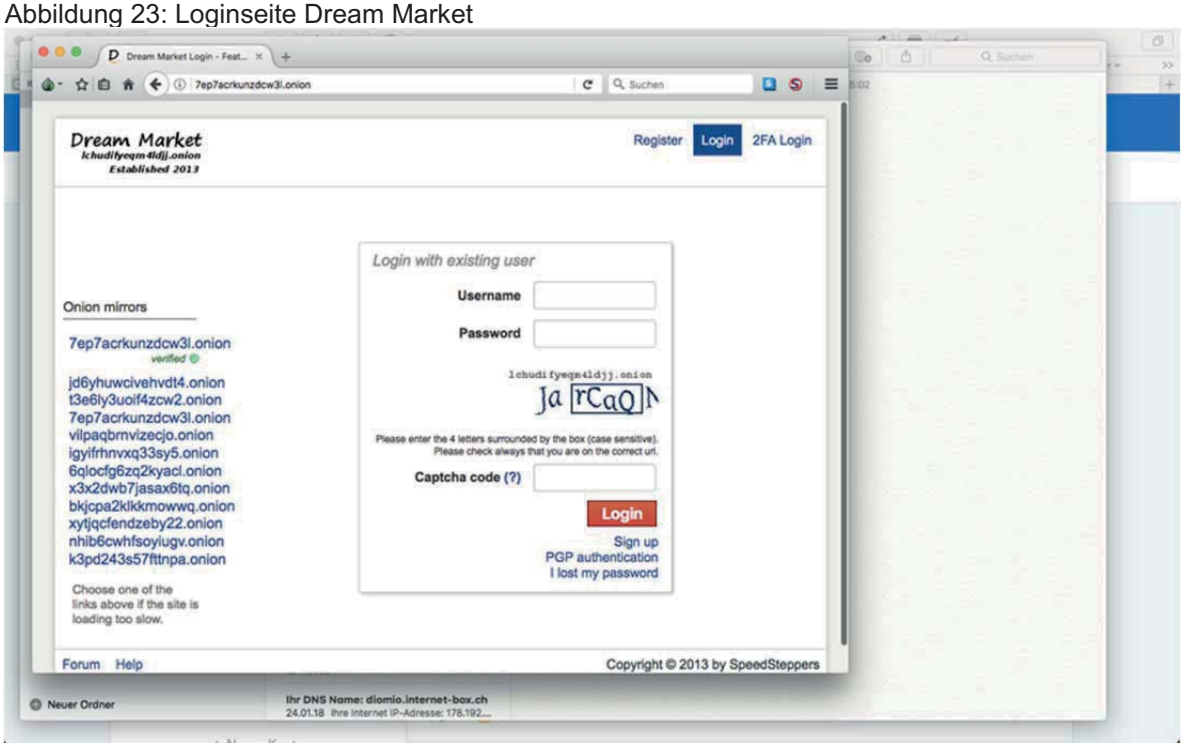
Abbildung 22: Tor Browser wurde aktualisiert



Anmerkung: (The Tor Project, o. J.).

Nachdem der Tor Browser aktualisiert wurde, kann nun der Marktplatz Dream Market besucht werden. Dieser ist über die Onion-Adressen [Links für Veröffentlichung entfernt] oder andere alternative Mirror-Links zu erreichen.

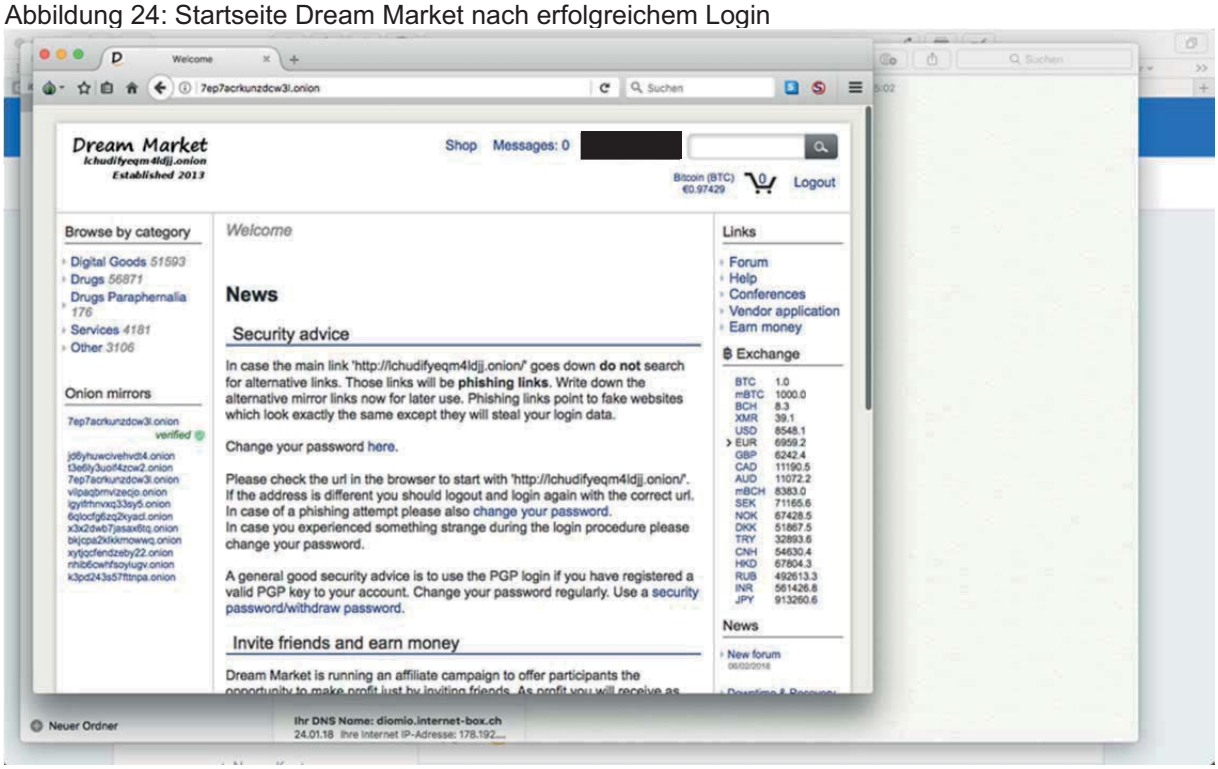
Abbildung 23: Loginseite Dream Market



Anmerkung: («Dream Market», 2018).

Das Login funktioniert beim Dream Market mittels Benutzername, Passwort sowie einem Captcha code. Nach erfolgreichem Login ist das aktuelle Guthaben, die Anzahl ungelesener Nachrichten, Neuigkeiten sowie eine Menüstruktur und ein Suchfenster, die das Durchsuchen des Marktplatzes ermöglichen, sichtbar.

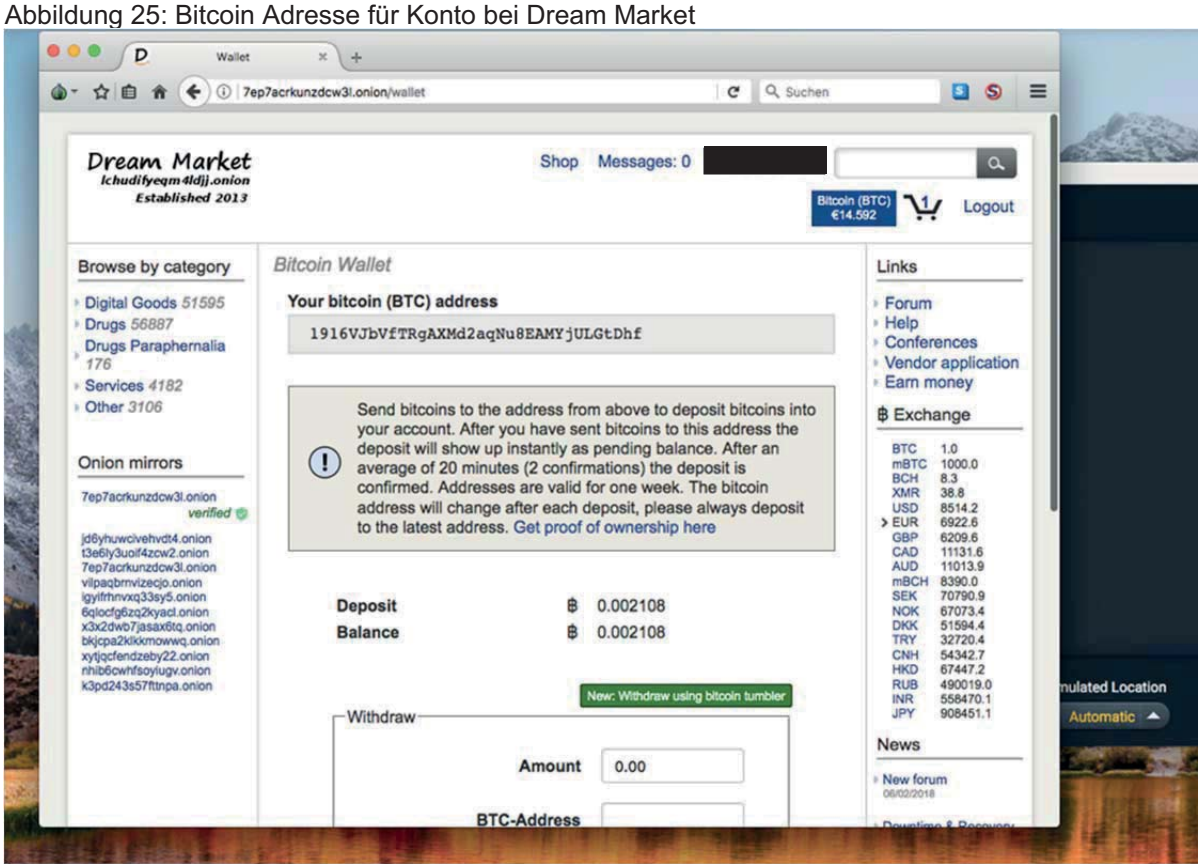
Abbildung 24: Startseite Dream Market nach erfolgreichem Login



Anmerkung: («Dream Market», 2018).

Der Marktplatz bietet jedem Benutzer ein eigenes Bitcoin Wallet an. Dieses Bitcoin Wallet ist über eine eigene Bitcoin Adresse ansteuerbar. Diese Bitcoin Adresse wird benötigt, um Bitcoins von seinem Wallet (z.B. bei Coinbase) auf dasjenige bei Dream Market zu transferieren. Aus Sicherheitsgründen ändert sich diese Bitcoin Adresse regelmässig; spätestens aber nach jeder erfolgreichen Überweisung. Demnach muss vor jeder neuen Überweisung die aktuellste Bitcoin Adresse abgerufen werden.

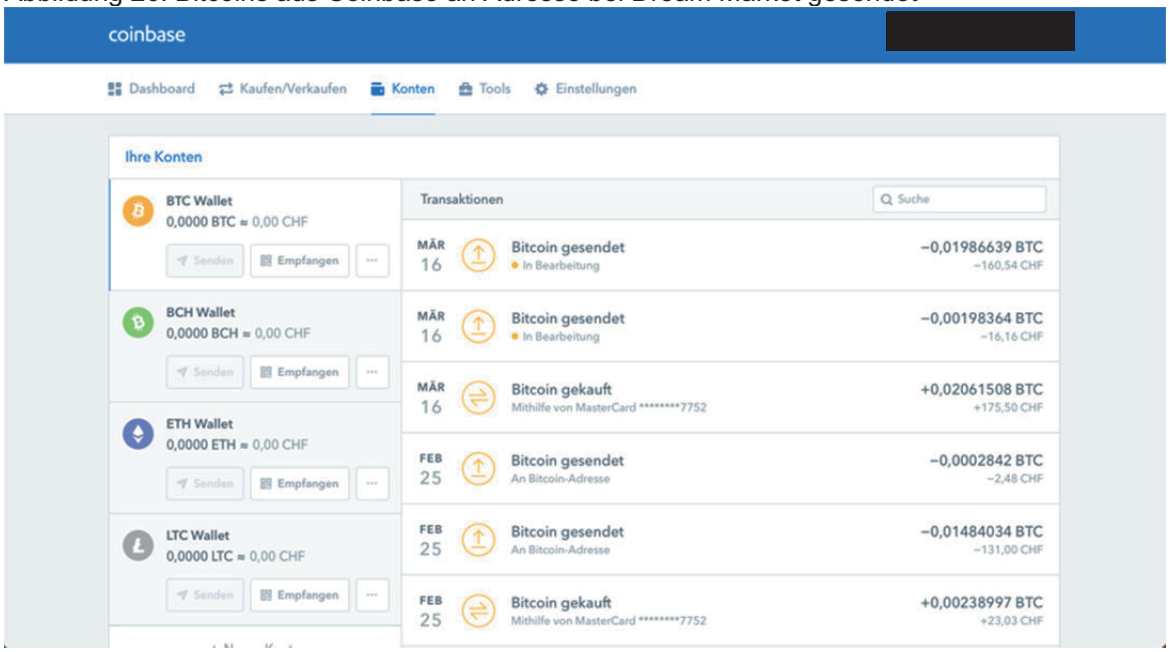
Abbildung 25: Bitcoin Adresse für Konto bei Dream Market



Anmerkung: («Dream Market», 2018).

Die Bitcoin Adresse wird einfach aus dem Tor Browserfenster kopiert und bei der Coinbase Überweisung eingefügt.

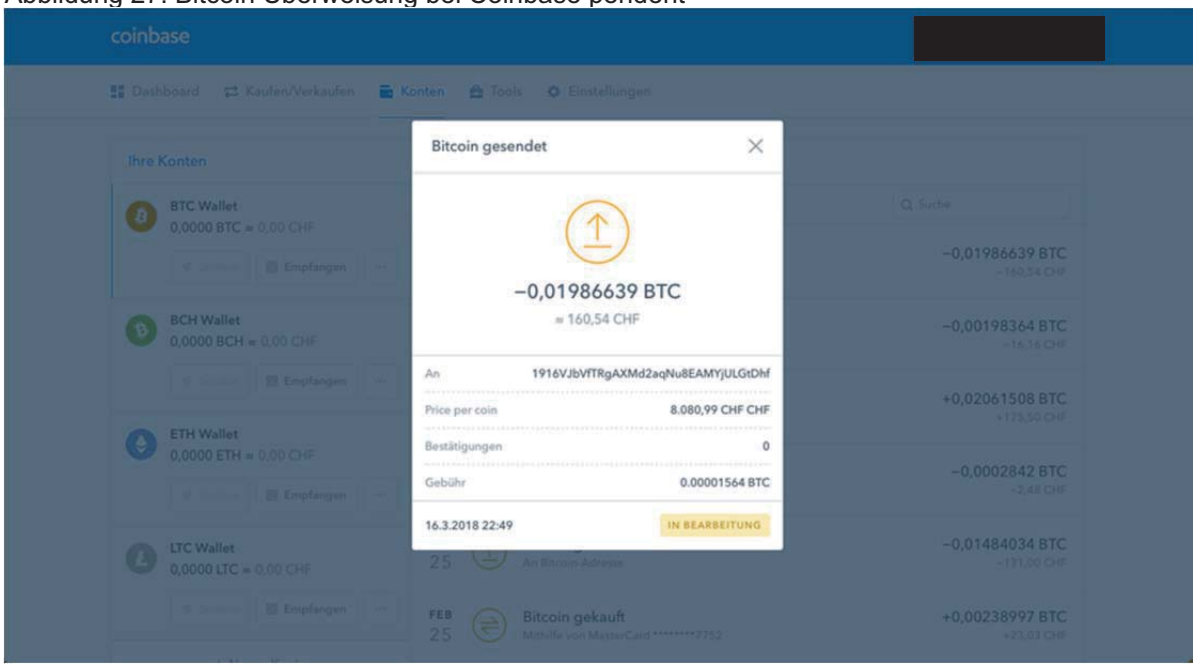
Abbildung 26: Bitcoins aus Coinbase an Adresse bei Dream Market gesendet



Anmerkung: (Coinbase, 2018).

Die Bitcoin Überweisung dauert einen Moment, abhängig des Zahlungsverkehrsaufkommens auf dem weltweiten Bitcoin Markt. Der Status der Bitcoin Überweisung kann bei Coinbase jederzeit abgerufen werden.

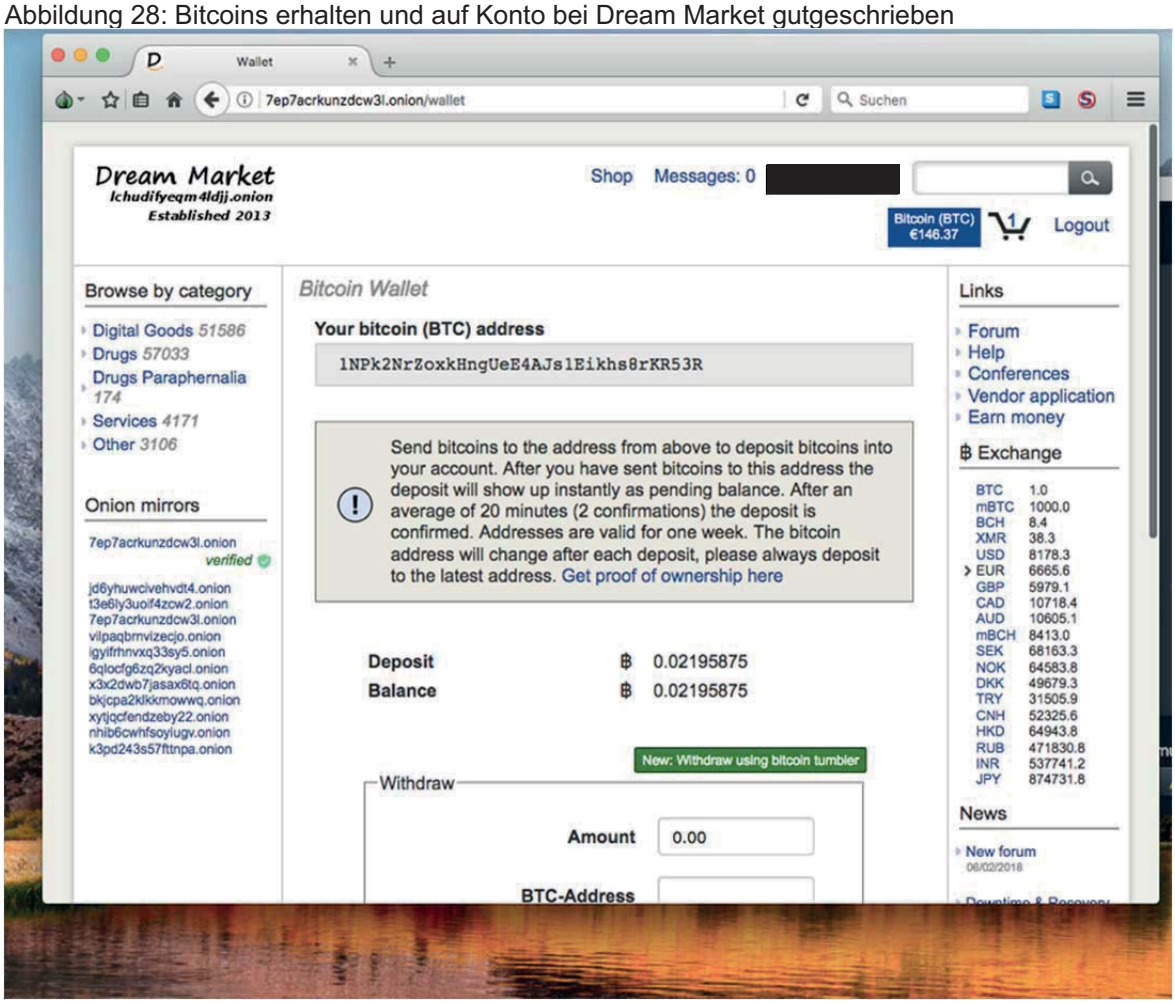
Abbildung 27: Bitcoin Überweisung bei Coinbase pendent



Anmerkung: (Coinbase, 2018).

Ist die Überweisung abgeschlossen, wurden die Bitcoins dem Wallet auf Dream Market gutgeschrieben. Dies lässt sich am neuen höheren Bitcoin Guthaben erkennen.

Abbildung 28: Bitcoins erhalten und auf Konto bei Dream Market gutgeschrieben



Anmerkung: («Dream Market», 2018).

Nun sind alle Voraussetzungen erfüllt, um auf Dream Market einzukaufen. An dieser Stelle wird verzichtet, das breite Angebot der auf Dream Market angebotenen Waren und Dienstleistungen vorzustellen.

Stattdessen folgt ein wichtiger Tipp: Damit eine Bestellung ankommt, wird eine korrekte Postadresse benötigt. Die Angabe des Namens und der Wohnortadresse ist jedoch in keiner Weise empfehlenswert. Um im Darknet Waren ohne persönliche Angaben bestellen zu können, sind beispielsweise Grenzpaketdienste eine gute Möglichkeit. Hiervon gibt es verschiedene Anbieter und einer davon ist zum Beispiel die Grenzpaket GmbH, die über die URL www.grenzpaket.ch zu erreichen ist.

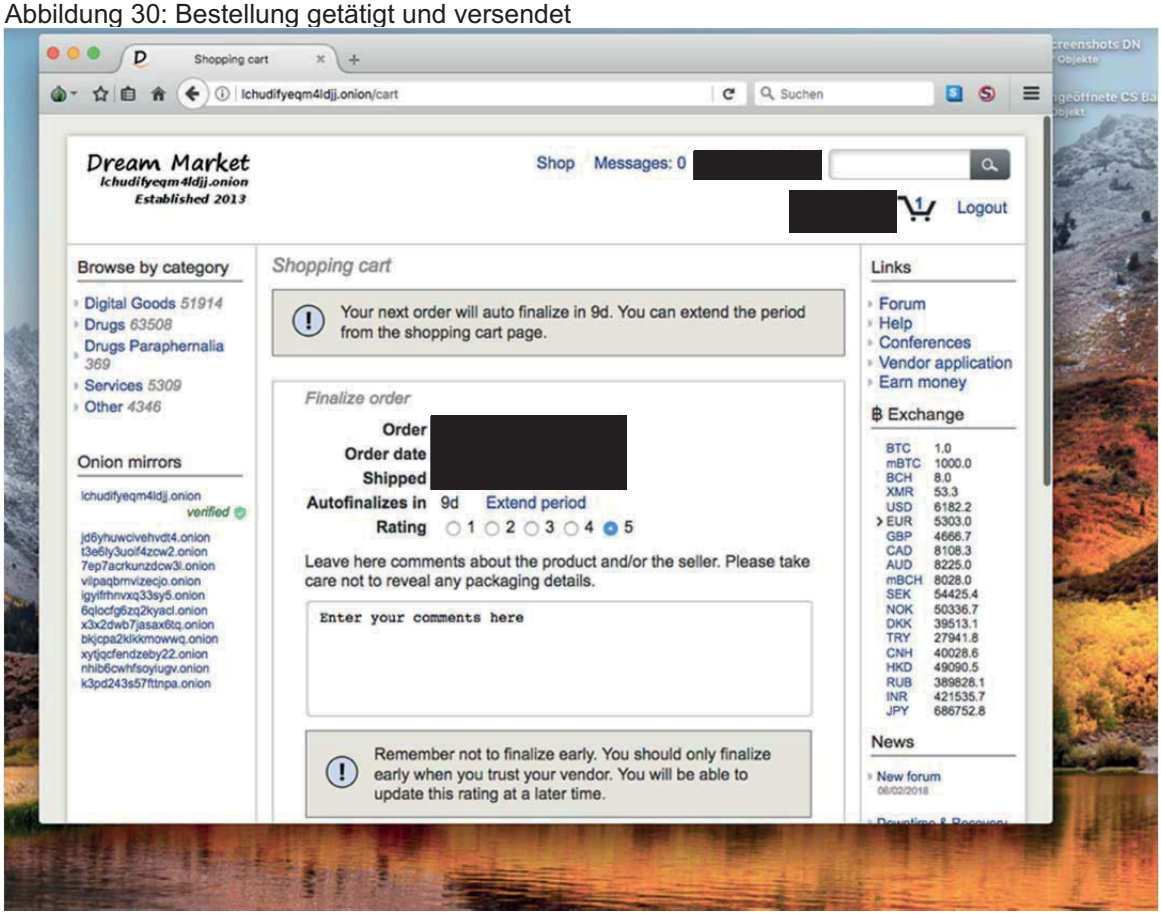
Abbildung 29: Website www.grenzpaket.ch

Anmerkung: («Grenzpaket», 2018).

Ein Kunde von Grenzpaket erhält eine Art Postfach mit einer ID Nummer. Diese ID Nummer sowie die Adresse des Postfachs ist bei der Bestellung im Darknet anzugeben. Sobald eine Sendung bei Grenzpaket eingetroffen ist, erhält der Kunde eine Benachrichtigung wahlweise per SMS und/oder E-Mail.

Die Bestellung im Darknet ist getätigt und im Dream Market Benutzerkonto mit Status ersichtlich.

Abbildung 30: Bestellung getätigt und versendet



Anmerkung: («Dream Market», 2018).

An dieser Stelle wird auch angezeigt, in wie vielen Tagen die automatische Finalisierung des Escrow stattfindet. Dies bedeutet, dass das System die Bestellung automatisch auf Erledigt setzt und dadurch den bezahlten Betrag für den Verkäufer freigibt – und dies ohne Zutun des Käufers. Der Käufer hat jedoch vor Ablauf der Anzahl Tage die Möglichkeit, die Frist zur automatischen Finalisierung zu verlängern. Dies falls die bestellte Ware noch nicht angekommen ist. Ebenfalls an dieser Stelle hat der Käufer die Möglichkeit, einen sogenannten «Disput» zu eröffnen. In diesem Schlichtungsverfahren können Käufer und Verkäufer ihre Situation darlegen und der Marktplatz findet eine für beide Parteien gerechte Lösung.
Das Rating, welches der Käufer anhand von Punkten (5 = beste Note, 1 = schlechteste Note) abgeben kann, fliesst in eine Gesamtbewertung des Verkäufers ein. Ausserdem hat der Käufer die Möglichkeit, zu seiner Bewertung einen Kommentartext einzugeben.

Rund eineinhalb Wochen nach erfolgter Bestellung ist die bestellte Ware auch tatsächlich eingetroffen. Dieser Selbstversuch zeigt auf, dass es tatsächlich möglich ist, im Darknet illegale Waren und Dienstleistungen zu bestellen und diese auch geliefert werden können.

Abschliessend ist jedoch davon auszugehen, dass einige der im Darknet angebotenen Waren und Dienstleistungen nicht echt sind, nicht geliefert werden, von Betrügern genutzt werden um Geld zu ergaunern oder aber auch fiktiv sind und von Ermittlern als Falle genutzt werden.