Fraunhofer SIT

TECHNISCHE UNIVERSITÄT DARMSTADT

FRAUNHOFER - INSTITUT FÜR SICHERE INFORMATIONSTECHNOLOGIE SIT

WHITE PAPER

Was ist das Darknet?

PANDA: Parallelstrukturen, Aktivitätsformen und Nutzerverhalten im Darknet

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Impressum

Autoren
Florian Platzer
Robert Landwirth
Sandra Wittmer
York Yannikos

Kontakt
Florian Platzer
Fraunhofer-Institut
für Sichere Informationstechnologie SIT
Rheinstraße 75
64295 Darmstadt

Bildquellen
Seite 1: System, https://pixabay.com/de/illustrations/system-netz-netzwerk-verbindung-3699542/

Motivation

Während das Darknet bei den meisten Menschen bedrohliche Assoziationen hervorruft, ist es für andere ein Ort, dem in Zeiten der Snowden-Enthüllungen rund um die umfangreichen Überwachungs- und Spionagetätigkeiten der NSA die Hoffnung auf ein besseres Internet zugrunde liegt. Zu größerer Bekanntheit gelangte es hierzulande, nachdem im Juli 2016 die Hintergründe des Amoklaufs vor dem Olympia-Einkaufszentrum in München ans Licht gekommen waren. Ein 18-jähriger Schüler hatte dort mit einer Waffe, die er über das deutschsprachige Darknet-Forum "Deutschland im DeepWeb" erworben hatte, neun Menschen erschossen und vier weitere verletzt. Seitdem ist das dunkle Netz in den Fokus der medialen Berichterstattung gerückt und dominiert die netzpolitischen Debatten. Jenseits der überwiegend negativen Berichterstattung hat die Verwendung von Darknet-Technologien jedoch zahlreiche 'helle Seiten', wie beispielsweise die Umgehung von (Internet-)Zensur in totalitären Regimen oder das Bereitstellen von sicheren Kommunikationsplattformen für WhistleblowerInnen. Immer mehr Menschen wollen wissen, was es mit dem „Mythos Darknet" auf sich hat und welche technische Infrastruktur dahinter steht. Da der Begriff bislang uneinheitlich verwendet wird, wollen wir unser Verständnis davon, was das Darknet umfasst, im Rahmen dieses Whitepapers vorstellen. Dafür ist es sinnvoll, sich zunächst mit der Begriffsgeschichte auseinanderzusetzen und das Darknet von anderen Teilbereichen des Internets abzugrenzen.

Begriffsgeschichte

Der Begriff „Darknet" ist schon lange im Umlauf. Die Art, wie wir ihn heute verwenden, als Synonym für Netzwerke wie Tor oder allgemeiner, für Anonymitätsnetzwerke, hat sich erst um 2011 etabliert. Zum ersten Mal trat das „Darknet" in die öffentliche Debatte in Folge eines wissenschaftlichen Artikels von vier Microsoft-Mitarbeitern aus dem Jahr 2002. Biddle und seine Co-Autoren definieren ein Darknet als jedes Netzwerk, in dem lizenzrechtlich geschützte Objekte (bspw. Filme, Musik, Software usf.) unautorisiert verbreitet werden [1]. So bezeichnen die Autoren u.a. die P2P-Netzwerke Napster und Gnutella als Darknets und argumentieren, dass durch die Existenz hinreichend großer Darknets der Einsatz jeglicher Kopierschutzmechanismen für digitale Medien schlussendlich folgenlos bleiben würde.

Zwischen 2002 und 2005 wandelt sich diese ursprüngliche Bedeutung von Darknets. In Zeitungsartikeln werden sie nicht mehr als Filesharingnetzwerke im Allgemeinen thematisiert, sondern als private Filesharingnetzwerke, die wie Waste oder WinNY einladungsbasiert operieren und so ihre NutzerInnen schützen. Dabei spitzt sich die Diskussion um Darknets entlang einer Konfliktlinie zwischen FilesharerInnen und RechteinhaberInnen zu: Filesharingnetze werden immer populärer und die sie ermöglichenden Technologien werden dabei immer ‚anonymer'. Zwei Ereignisse symbolisieren diesen Konflikt: 2005 fällt das amerikanische Gericht ein Urteil gegen die Filesharing-Plattform Grokster. Nach diesem Urteil sind Firmen, die das Austauschen lizenzrechtlich geschützter Software ermöglichen, rechtlich für den Austausch dieser Software mitverantwortlich [2]. Ebenfalls 2005 veröffentlicht J.D. Lasica das Buch „Darknet: Hollywood's war against the digital generation" [3], welches die Definition von Biddle et al. als Ausgangspunkt der Argumentation nimmt und der Zuspitzung dieser Konfliktlinie zwischen

FilesharerInnen und RechteinhaberInnen Ausdruck verleiht.

Die eben skizzierte Diskussionslinie wird durch eine weitere Entwicklung reflektiert, der von Freenet. Im Jahr 2000 veröffentlicht Ian Clarke sein design paper „Freenet: A Distributed Anonymous Information Storage and Retrieval System" [4] zu großer wissenschaftlicher Resonanz. Freenet ist eine peer-to-peer Netzwerksoftware, die Anonymität herstellt, indem sie den Besitz und die Indexierung von Daten depersonalisiert. Eine algorithmische Entwicklung Oskar Sandbergs [5] ermöglichte es, Freenet effizient durchsuchen zu können, obwohl NutzerInnen über die Software nur mit spezifisch autorisierten Personen verbunden sind (wie in bisherigen einladungsbasierten Filesharingnetzwerken). Diese neue Form der Suche wird in Freenet 0.7 implementiert, welches nun neben seiner normalen Operationsweise im „Opennet"-Modus (mit einer Verbindung zu allen anderen NutzerInnen), nun einen sogenannten „Darknet"-Modus anbietet, in dem der eigene Computer nur mit dem von FreundInnen verbunden wird [6].

Entlang dieser Entwicklungen werden Darknets in der Medienberichterstattung zu Werkzeugen von FilesharerInnen gegen RechteinhaberInnen und gesetzlichen Autoritäten. Und entlang dieser Entwicklungen werden Darknets als die Anonymität immer stärker schützend wahrgenommen: Zuerst durch die reine Anzahl der NutzerInnen in Filesharingnetzkwerken, dann dadurch, dass Netzwerke einladungsbasiert operieren, und schließlich durch bestimmte Techniken technischer Anonymisierung. Die so entstandene Bedeutung von Darknets als private und anonyme Filesharingnetze bleibt bis 2011 erhalten.

Ab 2011 gibt es einen Wandel in der Begriffsbedeutung von Darknets. Langsam wird das Darknet zum Synonym für Netzwerke wie Tor [7]. In der Medienberichterstattung wird diese Verbindung 2011 durch Ereignisse wie beispielsweise Anonymous' „Operation Darknet" [8] hergestellt, bei der die hacktivist group Anonymous persönliche Daten von NutzerInnen der Kindesmissbrauchsseite „Lolita City", die im Tor-Netzwerk gehostet wurde, veröffentlicht hat. Eine weiterreichende und wirkungsreichere Entwicklung, die das Tor-Netzwerk ins Zentrum der Öffentlichkeit rückt, ist dabei der Start und das Ende von Silk Road. Silk Road war der erste Marktplatz, der sowohl die Anonymität der Netzverbindung durch Tor als auch die Anonymität der Zahlung durch Bitcoin [9] realisiert hat. Silk Road folgt eine Vielzahl weiterer Marktplätze und eine weitreichende öffentliche Beschäftigung mit ihnen. Neben einer Vielzahl von Meldungen aus der Presseberichterstattung findet man beispielsweise bei Google Scholar heute ungefähr 2000 Artikel zum Begriff „Cryptomarket". Dabei sind die Veröffentlichungen seit 2013 rapide angestiegen, mit 14 Veröffentlichungen im Jahr 2013, aber 709 Veröffentlichungen allein im Jahr 2019.

Durch diese medienrelevanten Ereignisse [10] hat sich der Begriff Darknet von seiner ursprünglichen Bedeutung als (anonyme) Filesharingnetze gelöst und wurde zur Bezeichnung für Netzwerke wie Tor, deren Hauptziel die Wahrung der Anonymität der TeilnehmerInnen ist. Dabei schwingt in Beschreibungen von Darknets der Subtext als Orte, an dem sich Drogenmarktplätze und Austauschplattformen für Kinderpornografie befinden, oft mit. Insgesamt lässt sich feststellen, dass der Begriff Darknet keinesfalls über die Zeit hinweg einheitlich verwendet wird, sondern sich stets mit unterschiedlichen Ideen verknüpft fand. Unsere hierauf folgende Definition knüpft an die derzeitige Verwendung von Darknets als Anonymitätsnetzwerke an.

Begriffsdifferenzierung

Der Begriff Darknet wird im Kontext einiger weiterer Begriffe, wie Deep Web, Dark Web, Clearnet oder Surface Web und manchmal auch in Verwechslung mit diesen verwendet. Bevor wir zu unserer Definition von Darknet kommen, möchten wir hier differenzierend auf diese Begriffe eingehen.

Der Begriff des **Internets** kann alle folgenden Begriffe und ihre Phänomene unter sich versammeln. Das Internet ist ein Netzwerk bestehend aus vielen kleineren und größeren Computernetzwerken. Es bietet eine weltweite Infrastruktur, um u.a. Webinhalte, E-Mail-Dienste, Dateiübertragungen und Chatnachrichten zur Verfügung stellen zu können. Die Kommunikation zwischen den einzelnen Endgeräten erfolgt auf Basis von standardisierten Netzwerkprotokollen.

Das **World Wide Web** oder auch einfach nur Web genannt, ist nur ein Teil des Internets. Es beinhaltet Hypertext-Dokumente und andere Web-Ressourcen, auf die man über einen Internetbrowser, wie zum Beispiel Firefox, Internet Explorer oder Chrome, zugreifen kann. Die im World Wide Web benutzten Protokolle sind HTTP und HTTPS. Andere Teile des Internets, die nicht zum World Wide Web gehören, sind Dienste, die zum Beispiel Dateien übertragen (FTP), E-Mails verschicken und empfangen (SMTP/IMAP/POP3), für die Namensauflösung (DNS) verwendet werden, oder um Netzwerkverbindungen mit entfernten Internetgeräten (SSH) herstellen zu können.

Das **Surface Web** ist eine Teilmenge des World Wide Webs und beinhaltet alle Webinhalte des Internets, die von Web-Suchmaschinen wie z.B. Google, Bing oder Yahoo gefunden und indexiert werden können. Dies ist nur ein prozentual kleiner Teil der Inhalte, die im gesamten World Wide Web vorhanden sind.

Das **Deep Web** hingegen, auch bekannt als das Invisible Web oder Hidden Web, ist ein großer Teil des World Wide Webs. Sein Inhalt ist der Teil des Internets, der nicht von Web-Suchmaschinen aus unterschiedlichen technischen Gründen indexiert wird. Dazu gehören beispielsweise Datenbanken, private (Firmen-)Netzwerke oder Plattformen mit einer Login-Seite, wie es bei sozialen Medien oft der Fall ist.

Dabei existiert keine harte Grenze zwischen Surface Web und Deep Web, und sogar einzelne Websites können in Anteilen dem Deep und Surface Web zugerechnet werden. Dies passiert beispielsweise durch das Anbieten sowohl statischer als auch dynamischer Inhalte auf einer Seite. So werden die Inhalte dynamischer Seiten, beispielsweise eines Onlineshops, erst nach Nutzereingabe gewisser Such- oder Filterkriterien zur Verfügung gestellt und würden so von gewöhnlichen Websuchmaschinen nicht gefunden und indexiert werden. Ebenfalls existieren Webinhalte, die aus technischer Sicht zum Surface Web gehören, da sie von Suchmaschinen indexierbar sind, die aber aufgrund ihrer schlechten Auffindbarkeit nicht tatsächlich indexiert werden. Die Unterscheidung von Deep und Surface beschränkt sich also auf das Web und organisiert Inhalte nach ihrer Auffindbarkeit und Indexierbarkeit durch Suchmaschinen. Die Grenze zwischen dem, was indexierbar oder nicht indexierbar ist, verschiebt sich ständig, vor allem durch Änderung an der Funktionsweise der Suchmaschinen.

Auch das **Darknet** ist ein Teil des Internets und besteht ebenfalls aus mehreren voneinander getrennten Netzwerken. Diese Netzwerke können nur durch zusätzliche Software erreicht werden, benutzen aber jeweils die Infrastruktur des Internets. Das Darknet beinhaltet dabei Teile des Deep Webs, kann Teile des World Wide Webs oder auch Inhalte außerhalb des World Wide Webs beinhalten. Diese Inhalte wären dann beispiels-

weise E-Mail-Dienste, die nur durch die zusätzliche Software genutzt werden können.

Das **Dark Web** steht in derselben Relation zum Darknet, wie das World Wide Web zum Internet steht. Demnach beinhaltet das Dark Web Ressourcen, die über einen Internetbrowser mithilfe der zusätzlichen Software angezeigt werden können und demzufolge HTTP oder HTTPS benutzen.

Schließlich ist das **Clearnet** der gesamte Teil des Internets, der nicht zum Darknet gehört. Das Clearnet summiert sich zusammen mit dem Darknet zum gesamten Internet.

Darknet-Definition

Nachdem wir die Anteile des Internets und die einzelnen Begriffe, die sie bezeichnen, in Relation zu einander gebracht haben, können wir nun das Darknet im Gros des Internets einordnen. Wie wir beschrieben haben, besteht das Darknet aus mehreren voneinander getrennten Netzwerken. Jedes dieser Netzwerke stellt ein eigenes Darknet. Demzufolge gibt es nicht nur ein Darknet, sondern mehrere, auf Basis unterschiedlicher Technologien realisierte Darknets.

Definition: Wir verstehen Darknets als Netzwerke, die als dezentral betriebene Infrastrukturen technisch anonymisierte Kommunikation und das Anbieten von Diensten ermöglichen. Beispiele sind Netzwerke wie Tor, I2P oder Freenet. Darknets sind Anonymisierungstechnologien, die auf dem Internet aufbauen (sog. Overlay-Netzwerke) und die Kommunikation durch das Internet, aber unter anderen Bedingungen, realisieren. Somit benötigen NutzerInnen von Darknets auch jeweils eine zusätzliche Software.

Darknets reagieren auf technische Aspekte ‚regulärer' Internetkommunikation insofern, als dass im Internet die Identifikatoren von Sender- und EmpfängerInnen (ihre IP-Adressen) im Klartext bei jedem Teil der Nachrichtenübermittlung mit verschickt werden (Diese stehen im Header jedes Datenpakets, einer Art Briefkopf, der die notwendigen Informationen für die technische Übermittlung des Pakets bereitstellt). Die so realisierte Kommunikation ermöglicht eine Reihe von Anonymitätsproblemen: So können beispielsweise die Internetanschlüsse kommunizierender Parteien identifiziert und überwacht werden, oder es kann versucht werden, DienstleisterInnen am Bereitstellen von Diensten zu hindern. Darknets versuchen solche Anonymitätsprobleme zu verhindern. So versucht Tor beispielsweise seine NutzerInnen zu schützen, indem ihre IP-Adressen verschleiert werden, und Freenet legt Daten in einer Weise ab, dass keine klare Zuweisung des Datenbesitzes zu bestimmten NutzerInnen des Netzwerks möglich ist. Weiterhin verhindern Darknets, dass Verbindungen abgehört, manipuliert oder blockiert werden können.

Damit sind Darknets für uns in erster Linie Technologien. Als Technologien können sie verschiedene Aufgaben erfüllen und im Rahmen verschiedener Praxen Anwendung finden. Sie bestehen aus unterschiedlichen TeilnehmerInnen mit unterschiedlichen Motivationen und Interessen. Und als Technologien haben sie auch nur solange Popularität, Sichtbarkeit und Effekte, wie sie benutzt und beobachtet werden, und wie über sie berichtet wird. Folglich können sich einzelne Darknets auch komplett auflösen, sofern nicht mehr genügend TeilnehmerInnen für das jeweilige Netzwerk existieren. Die Popularität von Darknets kann über die Zeit stark schwanken.

Referenzen

[[1] Biddle, Peter, Paul England, Marcus Peinado, and Bryan Willman. "The darknet and the future of content protection." In ACM Workshop on digital rights management, pp. 155-176. Springer, Berlin, Heidelberg, 2002.

[2] Eine zusammenfassende Darstellung des Falls findet sich bspw. unter: https://www.oyez.org/cases/2004/04-480 (gesehen 20-02-14)

[3] Lasica, Joseph Daniel. Darknet. Wiley, 2005.

[4] Clarke, Ian, Oskar Sandberg, Brandon Wiley, and Theodore W. Hong. "Freenet: A distributed anonymous information storage and retrieval system." In Designing privacy enhancing technologies, pp. 46-66. Springer, Berlin, Heidelberg, 2001.

[5] Sandberg, Oskar. "Searching in a small world." PhD diss., Chalmers tekniska högskola, 2005.

[6] Interessant hierbei ist, dass Tor durch die für Tor verantwortlichen Personen, im Gegenzug zu Freenet, überhaupt nicht als Darknet bezeichnet wird.

[7] Diesbezüglich siehe die Beschreibungen unter: https://freenetproject.org/pages/about.html (gesehen 20-02-14)

[8] Berichterstattung durch die BBC diesbezüglich: https://www.bbc.com/news/technology-15428203 (gesehen 20-02-14)

[9] Bitcoin geht auf eine 2008 unter dem Namen Satoshi Nakamoto veröffentlichte Konzeptionalisierung zurück und stellte die bis dato letzte fehlende Komponente für anonymen Handel im Internet: Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system. Manubot, 2019.

[10] Die bisher nachgezeichnete Entwicklung spiegelt sich auch im Google Trends Graph zum Suchbegriff "Darknet": Eine erste Spitze findet sich 2005 zur Zeit als das Grokster Urteil gefällt wurde, eine zweite Spitze 2013 einhergehend mit der Schließung von Silk Road, eine dritte 2016 könnte eventuell mit dem Amoklauf in München in Verbindung gebracht werden. Der Google Trends Graph kann unter https://trends.google.com/trends/explore?date=all&q=darknet (gesehen 20-02-14) eingesehen werden.

Über PANDA

Das interdisziplinäre Projekt Parallelstrukturen, Aktivitätsformen und Nutzerverhalten im Darknet (PANDA) ist ein auf fünf Jahre angelegtes, BMBF-gefördertes Verbundprojekt in der zivilen Sicherheitsforschung. Das von der TU Darmstadt und dem Fraunhofer-Institut für Sichere Informationstechnologie gemeinsam durchgeführte Projekt verbindet Informatik, Philosophie, Soziologie, Psychologie und Jura in einer interdisziplinären Arbeitsgruppe. PANDA leistet einen Beitrag zum interdisziplinären Verständnis der im Darknet entstandenen Infrastrukturen, Sozial- und Gesellschaftsformen, Machtstrukturen und Interaktionsformen und -prozesse. Wir erforschen das Darknet technikwissenschaftlich, sozialwissenschaftlich und philosophisch. Unser Ziel ist ein geschärftes Bild des Darknets, um politisch und wirtschaftlich motivierte illegale Aktivitäten besser zu verstehen, gerade auch, wenn diese im Clearnet, dem bekannten und leicht zugänglichen Bereich des Internets, beginnen, bevor sie im Darknet fortgeführt und konkretisiert werden. Hieraus werden rechtliche Rahmenbedingungen gewonnen und technische Instrumente abgeleitet, um Chancen und Risiken durch das Darknet besser einschätzen und beispielsweise auf besonders gesellschaftsgefährdende Strukturen und Aktivitäten im Darknet spezifisch, nötigenfalls auch präventiv einwirken zu können.

Mit PANDA werden wir im Rahmen der zivilen Sicherheitsforschung dazu beitragen, die Bekämpfung von Kriminalität im Darknet zu verbessern, ohne einseitig seine legitimen Verwendungsweisen oder gar anonyme Kommunikation insgesamt zu beeinträchtigen. Wir wollen der Spannung zwischen beiden Zielen so weit wie möglich ausweichen, indem wir unsere Forschung auf solche Ansätze konzentrieren, die den Gebrauch des Darknets für kriminelle Aktivitäten erschweren, ohne dessen Funktion bei der Umgehung von Zensurmechanismen oder der Gewährleistung anonymer und privater Kommunikation zu beschädigen.

Internet: https://www.panda-projekt.de