Tor zur Freiheit

Anonym surfen und Zensur umgehen mit Tor

Bild: Andreas Martini

In den Medien wird meist nur thematisiert, wie Kriminelle das Darknet nutzen. Doch das Tor-Netz ist in Staaten ohne Presse- und Meinungsfreiheit oft auch der einzige unzensierte Zugang zum Internet. Hierzu leistet Deutschland einen wichtigen Beitrag. Wir erklären, wie Sie von Tor profitieren, wo im Tor-Netz die Grenze der Anonymität verläuft und wie Sie Tor-Nutzer aus aller Welt schützen und unterstützen können.

Von Mirko Dölle

Das Darknet hat in Deutschland einen miserablen Ruf: ein unbeherrschbarer Sumpf für Waffen- und Drogenhändler, Pädophile, Querdenker, Rechts- und Linksextreme, den man dringend trocken legen müsste, mit Staatstrojanern und am besten durch Überwachung des gesamten Internetverkehrs. Es sind vor allem diese Facetten, die in deutschen Medien thematisiert werden. Dabei ist das Darknet für Millionen Menschen der einzige Weg, Zensur zu umgehen, an unabhängige Informationen zu kommen, Missstände aufzuzeigen oder sich anderweitig gegen das herrschende Regime zur Wehr zu setzen, ohne dafür im Knast zu landen oder spurlos zu verschwinden. Freiheiten, die wir hierzulande wie selbstverständlich genießen, die wir aber auch verteidigen müssen, um sie nicht zu verlieren.

Wer vom Darknet spricht, meint damit meist das Tor-Netz (The Onion Router), auch wenn es Alternativen wie das Invisible Internet Project (I2P) und RetroShare gibt. Diese spielen zahlenmäßig aber keine Rolle und nutzen zum Teil sogar Tor, um ihr eigenes Darknet aufzuspannen. Allen Darknets gemein ist, dass man dafür spezielle Software benötigt, für Tor zum Beispiel den Tor Browser (ab Seite 20) oder den Messenger Briar (ab Seite 24) der die Nachrichten nicht nur über Tor, sondern etwa bei Demonstrationen auch ohne Internet über ein lokales Peer-to-Peer-Netz versenden kann.

Unsichtbar

Dass sich Inhalte aus dem Darknet nicht bei Google finden lassen, heißt aber nicht, dass es dafür keine Suchmaschinen gäbe: Die Standard-Suchmaschine des Tor Browser etwa ist DuckDuckGo, eine gute Alternative dazu Ahmia. Beide gibt es sowohl als sogenannte Clearnet-Seiten, erreichbar über die altbekannten Internetadressen duckduckgo.com respektive ahmia.fi, als auch als sogenannte Onion Services (früher „Hidden Services“ genannt) mit der Endung .onion. Auf den Abdruck der Onion-Adressen verzichten wir an dieser Stelle bewusst, denn sie sind über 60 Zeichen lang und bestehen aus Zahlen und Buchstaben – das wird niemand abtippen. Das ist auch nicht erforderlich, denn Sie finden die Onion-Adressen von Ahmia auf der Clearnet-Seite der Suchmaschine, wenn Sie sie über den Tor Browser besuchen, und DuckDuckGo ist im Tor Browser hinterlegt.

Sie können auch versuchen, die Google-Suche im Tor Browser zu öffnen. Das funktioniert aber nur selten, weil Google Anfragen über das Tor-Netz meist als „ungewöhnlichen Datenverkehr“ einstuft und darum bittet, später wiederzukommen. Dabei hätte Google es leicht, den Datenverkehr aus dem Tor-Netz zu erkennen und freizugeben, denn die IP-Adressen der weltweit rund 1500 Tor Exit Nodes sind öffentlich gelistet: Sie sind es, die letztlich die Google-Suche oder jede andere Seite aus dem allseits bekannten Internet abrufen und auf verschlungenen, verschlüsselten Pfaden durch das insgesamt gut 7000 Knoten große weltweite Tor-Netz an den Tor Browser ausliefern. Die weltweit meisten Exit Nodes mit einer schnellen Internetanbindung von 100 Mbit/s oder mehr stehen übrigens in Deutschland. Wer also in China die Seiten der New York Times aufrufen möchte und deshalb das Tor-Netz bemüht, wird mit hoher Wahrscheinlichkeit in Deutschland, den USA oder in den Niederlanden herauskommen. Diese und weitere Zahlen, etwa wie sich die Tor-Nutzung in der Ukraine und in Russland seit Beginn der Kämpfe verändert hat, finden Sie ab Seite 28.

Zwiebel-Prinzip

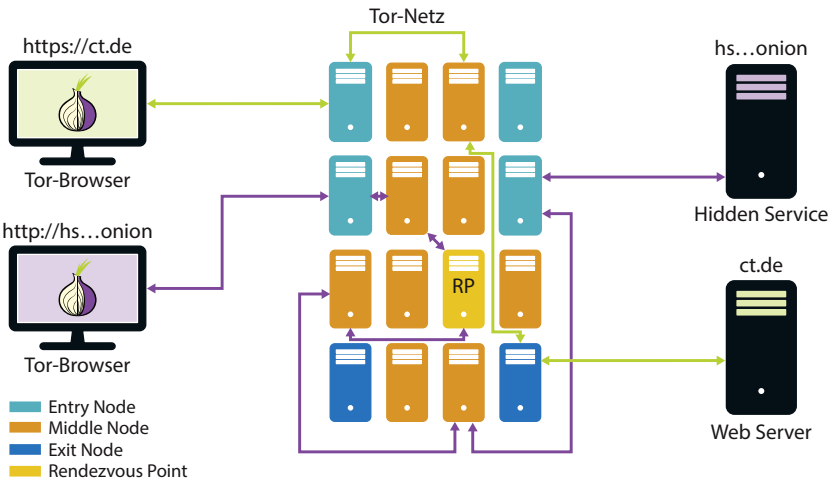
Neben dem Exit Node gibt es bei jeder Verbindung noch einen Entry Node, auch Guard (Beschützer) genannt, sowie einen Middle Node. Auch deren IP-Adressen sind öffentlich, denn nur so kann sich der Tor Browser nach dem Start einen Knoten jeder Sorte selbst heraussuchen. Um die Anonymität der Nutzer zu gewährleisten, ändert der Tor Browser spätestens nach zehn Minuten Middle Node und Exit Node.

Einen weiteren Schutz vor Identifizierung bietet die mindestens dreifache Verschlüsselung des Datenverkehrs. Daher verwendet das Tor-Projekt die Zwiebel als Symbol. Schon die Verbindung zum Entry Node verschlüsselt der Tor Browser. Die Datenpakete zum Middle Node sind noch einmal verschlüsselt, sodass auch der Entry Node den Inhalt nicht mitlesen kann, und eine dritte Verschlüsselungsschicht schützt den Datenaustausch mit dem Exit Node. Dieser ruft dann, im Idealfall per HTTPS noch ein weiteres Mal verschlüsselt, die Inhalte der gewünschten Website ab.

Facebook betreibt neben der Website im Clearnet auch einen Tor Onion Service – manchmal auch als Darknet-Seite bezeichnet. Auch dessen Onion-Adresse drucken wir an dieser Stelle nicht ab: Es genügt, wenn Sie einmalig im Tor Browser die Adresse facebook aufrufen; Sie bekommen dann auf der rechten Seite der Adressleiste den Hinweis eingeblendet, dass es diese Seite auch als Onion-Domain gibt. Klicken Sie auf den Hinweis, landen Sie automatisch auf der korrekten Onion-Adresse. Auch Twitter und viele andere Dienste haben inzwischen Onion-Domains, die Sie über die Adressleiste direkt ansteuern können, wenn Sie die Clearnet-Seite im Tor Browser öffnen. Das ist angesichts der ellenlangen neuen Onion-Domain-Namen auch äußerst hilfreich, um nicht versehentlich auf der Seite von Betrügern zu landen, die eine sehr ähnliche Onion-Domain einsetzen.

Wege durchs Tor-Netz

Verbindungen ins allseits bekannte Internet, auch Clearnet genannt, verschleiert der Tor-Browser mithilfe dreier Knoten und einer dreifachen Verschlüsselung. Bei Hidden Services, den Onion-Domains im Darknet, sind es sogar sechs Knoten und eine sechsfache Verschlüsselung.



Surft man einen versteckten Onion Service an, so kommen anstelle der Exit Nodes zwei weitere Tor-Knoten ins Spiel – nämlich ein zweiter Middle Node auf Nutzerseite, der als Rendezvous-Punkt dient, und ein zweiter Middle Node auf der Seite des Onion Service. So wird der Verkehr insgesamt gleich sechsmal verschlüsselt und über sechs Umwege kreuz und quer durchs Netz geschickt, um sowohl die Anonymität der Tor-Nutzer als auch die der Onion Services zu garantieren. Deshalb kostet es den Behörden auch so viel Mühe, gegen illegale Drogenmärkte im Darknet vorzugehen: Dank Tor ist ihr Standort nur schwer auszumachen.

Kurz und geknackt

Bei den langen und komplizierten Onion-Domains haben Kriminelle allerdings leichtes Spiel: So haben Betrüger jahrelang ähnliche Designs und ähnlich klingende Onion-Adressen der einstmals wichtigsten Darknet-Suchmaschine Grams benutzt, um Leute ihrer Bitcoins zu berauben. Onion-Domain-Namen waren damals lediglich 16 Zeichen lang, eine der bekanntesten, weil gut zu merken ist Facebooks Darknet-Adresse facebookcorewwwi.onion. Da das Tor-Netz dezentral organisiert ist, gibt es keine Domain Registry, wo man sich einen bestimmten Namen aussuchen kann. Stattdessen benutzt Tor als Namen den in lesbare, weil Base32-kodierte Zeichen konvertierten Hash-Wert des öffentlichen Schlüssels, den ein Onion-Service zur verschlüsselten Kontaktaufnahme verwendet. Um eine einprägsame sogenannte Vanity-Domain zu finden, muss man am Fließband neue geheime Schlüssel erzeugen und dann jeweils schauen, welcher Onion-Domain-Name dabei herauskommt.

Was Facebook vor Jahren etliche Monate und erhebliche Rechenleistung gekostet haben dürfte, schaffen heutige Rechner und leistungsfähige Grafikkarten in einem Bruchteil der Zeit. Deshalb wurden mit der neuesten Version 3 des Tor-Protokolls längere Schlüssel und längere Namen mit nunmehr 56 Zeichen eingeführt. Auch dafür gibt es Vanity-Adress-Generatoren wie „mkp224o“ (siehe ct.de/y3ab), sodass Facebooks Onion-Adresse weiterhin mit „facebook“ beginnt.

Grenzen der Anonymität

Die Anonymisierung durch das Tor-Netz ist nicht grenzenlos und daher nicht für alle Fälle gewährleistet. Darknet-Nutzer sind ständig der Gefahr ausgesetzt, identifiziert zu werden. Das Risiko lässt sich durch richtiges Verhalten minimieren, jedoch nie völlig ausschließen. Die Gefahr besteht schon beim Download des Tor Browser: Gelingt es Behörden oder Angreifern, Ihnen hier ein trojanisches Pferd unterzuschieben, erlangen sie schlimmstenfalls die Kontrolle über den kompletten Rechner. Der Artikel auf Seite 20 beschreibt, wie Sie den Tor Browser herunterladen und installieren sollten und erklärt auch die grundlegenden Sicherheitseinstellungen

In die Kategorie der unvermeidlichen Risiken fallen Bugs und Sicherheitslücken im Tor Browser, der ein modifizierter Firefox ESR ist. Dies wurde etwa 2013 ausgenutzt, um die Malware „Magneto“ auf Rechnern einzuschleusen und anschließend das Surfverhalten zu überwachen. Zusätzliche Angriffsfläche bieten Sicherheitslücken in Systembibliotheken wie der für JPEGs, die der Tor Browser gemeinsam mit vielen Programmen auf Ihrem Rechner verwendet. Stets den neuesten Tor Browser zu benutzen und vorher sämtliche verfügbaren Updates einzuspielen, ist deshalb nicht nur selbstverständlich, sondern im Zweifel lebenswichtig.

Die mit dem Tor Browser zusammen ausgelieferten Plug-ins HTTPS Everywhere und NoScript tragen zusätzlich maßgeblich zur Anonymität und Sicherheit im Darknet bei: Ruft man eine herkömmliche Internetseite aus dem Clearnet im Tor Browser auf, so werden die Daten im Darknet zwar dreifach verschlüsselt. Am Ende ist es jedoch der Exit Node, der die gewünschte Internetseite abruft – etwa eine Login-Seite. Passiert das unverschlüsselt per HTTP, passieren auch Ihre Zugangsdaten unverschlüsselt den Exit Node und können dort abgegriffen werden. HTTPS Everywhere sorgt dafür, dass stets die verschlüsselt übertragene HTTPS-Version einer Website geöffnet wird, sofern verfügbar.

NoScript ist dafür zuständig, JavaScript auf Websites im Zaum zu halten. Mit JavaScript kann man nicht nur nervige Popup-Fenster aufploppen lassen, es wird auch für das sogenannte Fingerprinting von Rechner und Browser missbraucht. Dabei werden zum Beispiel gezielt Lastspitzen durch verschiedene Rechenoperationen erzeugt und gemessen, wodurch sich Rückschlüsse auf die verwendete Hardware ergeben. Auch die Größe des Browser-Fensters lässt sich mittels JavaScript auslesen und so ein weiteres individuelles Merkmal ermitteln, weshalb sich die Größe des Tor Browser inzwischen nur noch in großen Schritten verändern lässt.

Im Netz mit doppeltem Boden

Kann ein Angreifer über den Tor Browser Schadcode einschleusen, so ist die Anonymität akut gefährdet: Außerhalb des Tor Browser verwenden sämtliche Programme weiterhin den normalen Internetzu-

gang ohne jegliche Tarnung. Diese Angriffsmethode nutzte das amerikanische FBI 2015 zur Deanonymisierung der Nutzer der Kinderporno-Seite Playpen: Nachdem der Webserver von Playpen beschlagnahmt war, installierte man Schadcode, der mittels Zero-Day-Exploits im Tor Browser einen Ping an das FBI auslöste. So kamen die Ermittler an die echte IP-Adresse aller Besucher.

Um diesen Angriffsweg zu blockieren, gibt es das Live-Linux Tails (siehe ct.de/y3ab): Es verwendet Tor grundsätzlich für alle Internetverbindungen, ist also nicht auf den Tor Browser beschränkt. Damit können Sie auch mittels Thunderbird Ihre E-Mails per Tor verschlüsselt abrufen, ohne dass dies zurückverfolgt werden könnte. Besonders interessant ist Tails für Dissidenten und Journalisten, aber auch für Geschäftsleute: Steht eine Reise in ein Land bevor, das etwa die Daten von Notebooks im Rahmen der Einreise kopiert, so nimmt man ein Gerät ohne oder mit gelöschter Festplatte und Tails auf USB-Stick mit. Die benötigten Dateien besorgt man sich dann erst am Zielort über das Tor-Netz vom heimischen NAS oder aus der firmeneigenen Cloud. Tails enthält unter anderem LibreOffice und etliche andere Programme, lässt sich also nicht nur zum Surfen verwenden.

Etliche Darknet-Händler gehen sogar so weit, ein bestimmtes Notebook ausschließlich mit Tails zu benutzen. So verhindern sie, dass selbst nach einem erfolgreichen Angriff auf Tails kompromittierende Daten von der Festplatte des Rechners ausgelesen werden können. Dass ein solcher Angriff kein theoretisches Szenario ist, wurde im August 2020 bekannt: Facebook hatte 2017 zur Ergreifung eines Sexualstraftäters die Entwicklung einer Zero-Day-Lücke in Tails beauftragt und dafür nach eigenen Angaben eine sechsstellige Summe bezahlt. Mithilfe eines präparierten Videos konnte das FBI die Sicherheitslücke im Videoplayer von Tails ausnutzen und so letztlich die echte IP-Adresse des Täters ermitteln.

Voll verschleiert

Behörden mancher Länder sowie manche Streamingdienste und auch Content Delivery Networks nutzen aus, dass die IP-Adressen der Tor-Knoten öffentlich abrufbar sind. Damit lässt es sich leicht feststellen und blockieren, wenn jemand etwa einen Film über einen Tor Exit Node abrufen möchte – das Geo-Blocking wird quasi um das Darknet erweitert. Wir haben aber auch Hinweise von Lesern erhalten, dass verschiedene Inhalte aus ihrer Netflix-Mediathek verschwanden, nachdem sie an ihrem Internetanschluss einen Tor-Knoten in Betrieb nahmen – also lediglich das Tor-Netz unterstützten, ohne es für Netflix zu verwenden. Wir baten den Pressesprecher von Netflix um eine offizielle Stellungnahme, erhielten bis Redaktionsschluss aber keine Antwort.

Manche Länder wie China nutzen die IP-Adressen der Entry Nodes und zusätzlich Techniken wie Deep Packet Inspection (DPI), um Tor zu blockieren. Damit der Tor Browser trotzdem Kontakt ins Tor-Netz findet, wurden die sogenannten austauschbaren Übertragungsarten (Pluggable Transports) entwickelt. Besonders erwähnenswert ist dabei Snowflake: Snowflake ist fest im Tor Browser eingebaut und lässt sich mit wenigen Mausklicks einschalten. Über das Snowflake-Add-on für Chrome und Firefox ist es aber auch besonders einfach, das Tor-Netz mit dem eigenen Internetanschluss als Snowflake-Proxy zu unterstützen. Näheres zu Snowflake finden Sie im Kasten „Tor trotz(t) Zensur“. Nachteile wie Beschränkungen bei Netflix muss man dabei nicht fürchten.

Fazit

Solange man (noch) in einer freiheitlichen Demokratie wie Deutschland lebt, ist es leicht, das Darknet als kriminelles Ghetto des Internet abzutun. Tatsächlich dient es Millionen Menschen in weniger freien Ländern als Weg, Zensur zu umgehen und sich unabhängig zu informieren – ohne unmittelbar ihre Freiheit und ihr Leben riskieren zu müssen.

Dabei spielt Deutschland als größter Standort für schnelle Tor Exit Nodes eine wichtige Rolle und dank Snowflake kann jeder Internet-Nutzer hierzulande das Tor-Netz mit wenigen Mausklicks effektiv unterstützen. Dass Kriminelle das Darknet missbrauchen, muss eine freiheitliche Demokratie aushalten. Nicht zuletzt, um das Tor-Netz selbst einsetzen zu können, falls ein faschistisches Regime an die Macht kommen sollte. Aber sie kann das auch aushalten, denn Strafverfolgung und Justiz funktionieren auch im Darknet, wie die Verhaftungen und Verurteilungen von Darknet-Marktbetreibern der letzten Jahre beweisen. *(mid@ct.de)* c't

Tails: ct.de/y3ab

Tor trotz(t) Zensur

Snowflake dient zur Verschleierung des Datenverkehrs im Tor Browser und nutzt dazu das Web-Echtzeitprotokoll WebRTC. Da WebRTC auch von etlichen modernen Web-Anwendungen genutzt wird, etwa für Videotelefonie, wird es selten blockiert und die Tor-Nutzer gehen in der Masse anderer Internetnutzer unter.

Snowflake lebt davon, dass möglichst viele Freiwillige Ihren Internetanschluss als Snowflake-Proxy zur Verfügung stellen und dass sich die IP-Adressen regelmäßig ändern, etwa durch die tägliche Zwangstrennung bei DSL-Anschlüssen. So wird es für einen Zensor schwierig bis unmöglich, sämtliche jemals für Snowflake verwendeten IP-Adressen zu sperren, ohne den Zugang zum Internet gänzlich zu blockieren.

Um über Snowflake zu surfen, drücken Sie beim Start des Tor Browser mehrfach die Escape-Taste, damit keine direkte Verbindung zum Tor-Netz aufgebaut wird. Anschließend aktivieren Sie in den Netzwerk-Einstellungen des Tor Browser unter „Tor/Brücken“ lediglich „Eine Brücke verwenden“ und wählen rechts daneben „snowflake“ aus. Sie müssen dann nur noch die Einstellungen schließen und auf „Verbinden“ klicken.

Wenn Sie Ihren eigenen Rechner als Snowflake-Proxy zur Verfügung stellen wollen, können Sie in Chrome oder Firefox das gleichnamige Add-on installieren. Alternativ genügt es aber auch, die Adresse https://snowflake.torproject.org/embed.html aufzurufen und den Schalter auf „Aktiv“ zu stellen. Zudem gibt es ein Docker-Image für den Dauerbetrieb eines Stand-alone-Proxy.

Probleme handelt man sich als Proxy-Betreiber nach derzeitigem Kenntnisstand nicht ein: Die Proxies schleusen lediglich verschlüsselte Datenpakete ins Tor-Netz und haben keine Kenntnis über deren Inhalt. Die Pakete nehmen anschließend ihren Weg durch das anonymisierende Tor-Netz. *(rei@ct.de)*