Technology Review
26.06.09
Infotech | Sicherheit

Retter für die freie Meinungsäußerung

Von David Talbot

Roger Dingledine, Mitgründer des Rechnernetzwerks Tor, das den Weg von Daten durchs Internet verschleiert
Bild: Chris Crisman

„Sokwanele“ bedeutet in einer der Bantu-Sprachen des südlichen Afrika „genug ist genug“. Es ist auch der Name eines **investigativen Online-Dienstes[1]** für Demokratie in Simbabwe, der im vergangenen Jahr Berichte über Gräueltaten des Regimes von Robert Mugabe veröffentlichte. Nach der Parlamentswahl posteten die Betreiber Berichte über die Einschüchterung von Wählern und Manipulationen von Wahlurnen. Wer bei Sokwanele das „Terror Album“ anklickt, findet schreckliche Bilder: von einer 70-jährigen Frau, die zusammengeschlagen und auf ihre Feuerstelle geworfen worden war (laut Sokwanele starb sie später), von niedergebrannten Häusern oder von Menschen mit tiefen Schnittwunden, die ihnen Mugabes Schergen beigebracht hatten. Auf regelmäßig aktualisierten Karten sind politisch motivierte Gewalttaten und andere Vorfälle eingezeichnet. Außerdem wartet die Seite mit Nachrichten über neue Todesfälle auf: „Leiche von Joshua Bakacheza gefunden“ lautet eine der traurigen Schlagzeilen bei Sokwanele.

Dass diese Schilderungen so einfach zugänglich sind, lässt vergessen, wieviel Mut dazu gehört, sie zu veröffentlichen. Denn den anonymen Fotografen und Bloggern, die die Sokwanele-Seite beliefern, droht bei Enttarnung Gefängnis oder Schlimmeres. Sie müssen immer auf der Hut sein, mit wem sie sprechen oder wenn sie eine Klinik betreten, um heimlich Aufnahmen von Gewaltopfern zu machen. Und sie müssen verhindern, dass sie über die IP-Adresse ihres Computers identifiziert werden können. Zum Beispiel mit Tor.

Tor[2] ist ein Open-Source-System, das den Zugang zum Internet anonymisiert, indem es die von einem Rechner abgehenden Daten verschlüsselt und über eine Kette von zwischengeschalteten Rechnern, so genannten Proxies, leitet, um die Spur des Absenders zu verwischen. Auf diese Weise lässt sich der Ort eines Computers verschleiern und die Filtersoftware eines autoritären Regimes, die den Zugang zu bestimmten Websites blockiert, umgehen. Datenschnüffler können als Absender nur die Proxies ausmachen. Ohne Systeme wie Tor hätten die Menschen in Ländern wie Simbabwe oder aktuell Iran keine Möglichkeit, frei ihre Meinung zu äußern oder Inhalte ins Netz zu stellen.

Anders als die meisten Anonymisierungstechnologien nutzt Tor mehrfache Proxies und Verschlüsselungsschritte, um möglichst hohe Sicherheit zu erreichen. Das bedeutet auch, dass sich nicht einmal herausfinden lässt, ob Blogger wie die von Sokwanele überhaupt Tor nutzen. „Wer Tor braucht, um anonym zu bleiben, wird auf keinen Fall sagen, dass er Tor benutzt“, sagt **Ethan Zuckerman[3]**, Mitgründer von **Global Voices[4]**, einer Online-Plattform und Hilfsorganisation für Blogger in aller Welt. Die Betreiber von Sokwanele seien äußerst ausgefuchst und würden verschiedene Verschlüsselungsverfahren nutzen, um ihre Identität zu schützen.

Für viele Internetnutzer geht es dabei nicht einfach nur um den Schutz der Privatsphäre, sondern um die schiere Notwendigkeit, den Häschern autoritärer Regime zu entgehen. Bereits 2006 stellte die **OpenNet Initiative[5]** – ein Forschungsprojekt der Universitäten Harvard, Toronto, Oxford und Cambridge zur Untersuchung von Internetzensur und Überwachung – fest, dass in 25 von 46 geprüften Ländern Inhalte gefiltert werden. Das sind weit mehr als die üblichen Verdächtigen China, Iran oder Saudi-Arabien. In einer neuen, laufenden Studie hat sich die Zahl der filternden Länder bereits auf 36 erhöht. Geblockt werden politische Inhalte, religiöse Seiten, Pornographie und auch, wie in einigen islamischen Ländern, Online-Glücksspiele. „Es gibt definitiv einen Trend hin zur Ausweitung von Internetfiltern“, betont **Ronald Deibert [6]**, Politikwissenschaftler an der Universität Toronto und einer der Gründer von OpenNet. „Ausmaß, Reichweite und Wirksamkeit der Filter nehmen weltweit zu.“

Tor kann hier zweifach helfen: Dieselben Proxies, die Internetnutzer schützen, entwickeln sich zugleich immer mehr zu Portalen für blockierte Websites. Als Tor vor fünf Jahren offiziell startete, bestand das Netzwerk aus 30 Proxies auf zwei Kontinenten. Inzwischen sind es 1500 Proxies auf fünf Kontinenten, die von Hunderttausenden aktiv genutzt werden. Aber die Tor-Entwickler wollen die Reichweite des Systems noch ausdehnen. Auch in den USA: Dort blockieren Bibliotheken und Unternehmen zunehmend Webinhalte, und Internetprovider zeichnen die Surfgewohnheiten von Usern auf, um sie der Werbewirtschaft zu verkaufen. „Das Internet wird allmählich zerstückelt, gefiltert und überwacht“, so Deibert, es finde eine Art digitale Erosion statt. „Deshalb müssen die Bürger etwas dagegen unternehmen, und da kommt Tor gerade richtig. Es schützt das Internet als Forum freier Information.“

Neutrale Knoten

Tor ist das Produkt einer kleinen Nonprofit-Organisation, die acht bezahlte Entwickler und ein paar Dutzend freiwillige Sicherheitsberater in aller Welt hat. Das System baut darauf auf, dass der Datenverkehr im Netz aus zweiteiligen Paketen besteht. Der erste Teil transportiert Inhalte, also Daten, die zu Bildern oder Webseiten gehören. Der andere besteht aus Metadaten: Dazu gehören die IP-Adressen des sendenden und des empfangenden Rechners. Diese Daten nutzt Tor beim Aufbau eines Netzes aus verschlüsselten Verbindungen über vermittelnde Rechner, die die Daten weiterleiten und

zusammen Proxies bilden. Betrieben werden sie von Universitäten, Unternehmen, Sicherheitsexperten und Bürgerrechtsgruppen in aller Welt.

Entstanden ist Tor wie das Internet selbst, nämlich aus einem militärischen Forschungsprojekt. Am US Naval Research Laboratory in Washington wurde Mitte der neunziger Jahre der erste Prototyp entwickelt. Man suchte einen Weg, um die Anonymität von Agenten zu schützen, wenn sie etwa von einem Hotel aus Webseiten mit der Domainendung „.mil“ – die dem US-Militär vorbehalten ist – aufriefen. Denn selbst wenn die Daten verschlüsselt waren, konnte jemand mit Zugriff auf die Computer des Hotels leicht aus den aufgerufenen Webadressen schließen, dass der User etwas mit dem US-Militär zu tun haben könnte. Das ist nur eine Möglichkeit unter vielen: Tatsächlich können IP-Adressen mit verschiedenen Methoden realen Orten zugeordnet werden. Im Irak etwa wäre eine Liste von IP-Adressen in Baghdad, die Emails von .gov- oder .mil-Konten bekommen, wohl bares Geld wert.

Das ursprüngliche Projekt der US-Marine kam zwar nie aus dem Prototypenstadium heraus, weckte aber das Interesse des Kryptographen **Roger Dingledine[7]**. Ihn beschäftigte, wie sich die Privatsphäre im Internet entwickeln würde, wenn Provider und Seitenbetreiber das Surfverhalten und die Suchbegriffe ihrer Nutzer in immer größeren Datenbanken festhielten. Auf einer Konferenz im Jahre 2000, auf der er seine Master-Arbeit am MIT über verteilte anonyme Datenspeicherung vorgestellt hatte, traf Dingledine den Mathematiker Paul Syverson, der am US Naval Research Lab arbeitete. Ihnen wurde klar, dass sich die Anonymität von Agenten und die von Internetnutzern eigentlich mit demselben Ansatz schützen lassen könnten. Zusammen stellten sie bei der Forschungsagentur des Pentagon, der DARPA, einen Förderantrag, um das Projekt wiederaufzunehmen.

Ergebnis war die erste öffentliche Version von Tor, die 2003 veröffentlicht wurde. Nutzen konnte sie jeder, der sich die Mühe machte, sie auf seinem Rechner zum Laufen zu bringen. Allerdings lief sie nur auf Open-Source-Betriebssystemen wie Linux, so dass schon ein gewisses Knowhow nötig war. Die **Electronic Frontier Foundation[8]**, eine Organisation für digitale Bürgerrechte, finanzierte dann eine Windows-Version, und schon bald wuchs die Nutzerbasis. „Meine ursprüngliche Intention war, den Leuten in Nordamerika und Europa etwas an die Hand zu geben, um ihre Informationen vor Konzernen und anderen großen Organisationen zu schützen, denn die behalten Nutzerdaten eher selten für sich“, sagt der inzwischen 32-jährige Dingledine, der das Tor-Projekt leitet. Inzwischen würden es aber auch Polizeibehörden einsetzen, um diskret Online-Nachforschungen in Betrugsfällen anstellen zu können und die Betrüger nicht durch die IP-Adressen von Polizeicomputern zu warnen, fügt Dingledine hinzu. Unternehmen wiederum würden Tor nutzen, um anonym die Online-Angebote der Konkurrenz zu studieren.

Es waren diese vielfältigen Anwendungsmöglichkeiten, die maßgeblich zum Erfolg von Tor beitrugen. „Sicherheit resultiert nicht nur aus der Menge der Nutzer, sondern auch aus ihrer Vielfalt“, sagt Dingledine. Es sei von Anfang darum gegangen, alle potenziellen Nutzergruppen, die ein Interesse an einem System wie Tor haben, in ein und dasselbe Netzwerk zu integrieren. Um es weiter zu verbreiten, wurde die Installation vereinfacht. 2006 wurde schließlich der „Torbutton“ veröffentlicht, ein Plug-in für den Firefox-Browser, mit dem sich die Nutzung von Tor ganz simpel ein- und ausschalten lässt, während man im Netz unterwegs ist. Ohne Tor surft es sich zwar schneller, aber dafür fehlt der Schutz.

Globale Verbreitung

Eines der repressivsten Länder hinsichtlich der Nutzung des Internet ist Syrien. So wurde kürzlich der Syrer Tariq Biasi zu drei Jahren Haft verurteilt, weil er „das Nationalgefühl geschmäht“ habe – er hatte sich im Netz kritisch über den Geheimdienst geäußert. Syrien verfolgt nicht nur Kritiker, sondern blockiert auch zahlreiche Websites – darunter Facebook, YouTube und Skype. Ich habe kürzlich mit dem syrischen Blogger **Anas Qtiesh[9]** gechattet, der dabei mit seinem Rechner in einem Internetcafé in Damaskus saß. Zwar publiziert er keine für syrische Behörden bedenklichen Inhalte, da er sich allgemein mit arabischer Politik beschäftigt. Aber auch Qtiesh hat den Torbutton installiert, weil er einfach mehr sehen und lesen will, als ihm die Regierung erlaubt. Und mit einem Klick ist das Internet in Damaskus dasselbe wie in Nordamerika oder Europa. „Tor bringt das Internet zurück“, schrieb mir Qtiesh.

Tor hatte sich schnell in Ländern wie Syrien herumgesprochen, aber erst der Torbutton verhalf dem System zum Durchbruch. Einen großen Anteil daran haben aber auch Verfechter wie Ethan Zuckerman vom Global-Voices-Netzwerk und etliche Bürgerrechtler in Asien und Afrika, die die Verwendung von Tor aktiv unterstützt haben. Der Einsatz hat sich gelohnt, wie **Wendy Seltzer[10]**, Juristin und Gründerin des Internetrechtsprojekts **Chilling Effects[11]**, im vergangenen Jahr in China feststellen konnte. Auf einer Blogger-Konferenz in Guangzhou hätten viele Blogger Tor genutzt, sagt sie. Die chinesische Regierung betreibt die weltweit rigidesten Internetsperren und hat in den letzten zehn Jahren Hunderte Nutzer und Blogger verhaften lassen. „In einem Internetcafé, in das ich gegangen bin, war die Tor-Software auf sämtlichen Rechnern bereits installiert“, sagt Seltzer.

Während Tor in China ein Mittel von vielen ist, hat es in Mauretanien die staatliche Zensur im Alleingang ausgehebelt. Verantwortlich dafür war der Bürgerrechtsaktivist **Nasser Weddady[12]**, Sohn eines mauretanischen Diplomaten, der in Boston lebt. Seit langem setzt er sich gegen die in seinem Heimatland immer noch praktizierte Sklaverei ein. Weitgehend unbeachtet von der Weltöffentlichkeit werden bis heute schwarze Moslems in Haushalten der arabischstämmigen Bevölkerung als Sklaven gehalten. Als die mauretanische Regierung 2005 einen Netzfilter installierte, übersetzte Weddady kurzerhand eine Tor-Gebrauchsanleitung ins Arabische und sorgte dafür, dass sie in den Internetcafés in Mauretanien verteilt und die Software installiert wurde. Die Folge: Die Regierung hob die Netzsperren wieder auf. Weddady glaubt zwar nicht, dass die Filterverantwortlichen wussten, dass plötzlich überall Tor genutzt wurde. Aber sie hätten wohl irgendwann gemerkt, dass ihre Netzsperren nichts bewirkten.

Auf solchen Erfolgen sollte man sich aber nicht ausruhen. Weddady erwartet, dass die Regierung schon bald mit einem

neuen Filtersystem nachlegen wird. „Der Nahe Osten ist eine wahre Wüste für Bürgerrechte“, sagt er, „die Internetfilter dort sind mit die ausgeklügeltsten der Welt.“ Er kenne viele in der Region, die Tor nutzen. Die Daten, die sie über das System auf ihren Rechnern empfangen, können von den Filtern keiner zu blockierenden Website zugeordnet werden, da als Absenderadresse die eines vermittelnden Rechners im Netzwerk erscheint. „Der Ansatz von Tor ist nicht: ‚Vertraut uns und übergebt uns eure Daten’. Tor ist so konstruiert, dass niemand Daten verraten kann, weil niemand sie tatsächlich hat“, betont Wendy Seltzer, die ehrenamtlich im Beirat des Tor-Projekts sitzt. Sie hält Tor für die derzeit beste Lösung.

Ein Herr von Brückenköpfen

Unangreifbar ist aber auch Tor nicht. Da es ein Open-Source-Projekt ist, ist sein Quellcode für jeden zugänglich. Sogar die Adressen der Zwischenrechner werden offengelegt. Im Prinzip könnten also Staaten mit Netzsperren diese Adressen ihren Filtern hinzufügen. Gemacht wurde das jedoch bislang nicht. Saudi-Arabien, Iran und den Vereinigten Arabischen Emiraten gelang es im vergangenen Jahr allerdings, Tor für ein paar Monate auf andere Weise zu blockieren. Ein praktischer Nachteil von Tor ist, dass es den Internetzugang bis zu zehnmal langsamer machen kann, wie eine Studie des **Berkman Center for Internet & Society[13]** an der Harvard University ermittelte. Dieses Problem dürfte noch größer werden, weil die Zahl der Tor-Nutzer schneller steigt als die der vermittelnden Rechner.

Das größte Problem ist aber, dass Hilfsmittel wie Tor nur von einem kleinen Teil aller Internetnutzer in der Welt eingesetzt werden. Ein Geschäftsreisender in China etwa, der genug Know-how und Bandbreite hat – oder jemanden bezahlen kann, um ein Anonymisierungssystem einzurichten –, wird die Netzsperren dort umgehen können. Insgesamt nutzen aber nur einige Millionen User Tor oder ähnliche Software, wie eine Abschätzung des Berkman Center ergab (die Datenbasis stammt dabei aus dem Jahr 2007). Allein in China sind 300 Millionen Menschen online. Und inzwischen beginnen sogar Staaten wie die Türkei mit Netzblockaden – dort will man Kritik am Staatsgründer Kemal Atatürk herausfiltern.

Um die Blockade von vermittelnden Rechnern zu verhindern, arbeitet das Torprojekt an so genannten Brückenknoten. Das ist eine Liste von IP-Adressen, die sich ständig ändert und die den Tor-Nutzern als Zugangspunkte zum eigentlichen Proxy-Netzwerk dienen. Eine solche IP-Adresse kann man per Email anfordern. Das könnte natürlich auch ein iranischer Zensor machen, aber die Tor-Entwickler wollen diese Möglichkeit ausschließen, indem immer mehr Internetnutzer ihre Rechner als Brückenknoten zur Verfügung stellen. „Der entscheidende nächste Schritt, den die Leute von Tor noch nicht implementiert haben, wäre, dass jeder Tor-Nutzer automatische zu einem Tor-Knoten wird, sobald er das System auf seinem Rechner aktiviert“, meint Jonathan Zittrain vom Berkman Center. „Dann skaliert das ganze System total hoch.“

Das würde aber bedeuten, dass dann die Datenmengen, die durch den Rechner eines Tor-Nutzers fließen, enorm zunehmen. Wenn jeder Nutzer automatisch zum Knoten wird, untergräbt das zudem den ursprünglichen Zweck von Tor. Denn der Rechner in einem Internetcafé, über den man Tor nutzt, würde plötzlich aufgrund seines Datenverkehrs auffallen. Andrew Lewman, Geschäftsführer des Tor-Projekts, sieht die Gefahr, dass dann „ein Wettrüsten mit Providern und Netzwerk-Administratoren einsetzt“. Denn die müssten einen Rechner, auf dem Tor läuft, allein wegen des anschwellenden Datenverkehrs blockieren. „Das ist schließlich ihr Job.“ Man wolle zwar sichere Wege finden, um mehr Hilfe einzubinden, aber im Moment gehe es um Zwischenschritte, etwa um den Datenfluss zwischen existierenden Tor-Knoten zu verbessern.

Nicht nur zensurwütigen Staatsbeamten bereitet Tor Kopfschmerzen. Kritik kommt auch von ganz anderer Seite, weil Tor etwa die Verbreitung von Kinderpornographie schütze. Roger Dingledine kontert, Tor helfe ja gerade Fahndern dabei, verdeckt im Netz zu ermitteln. Außerdem sei es für Kriminelle einfacher, drahtlose Netzwerke von Nachbarn oder in Cafés oder gehackte Rechner zu nutzen, um ihre Identität zu verschleiern.

Anonymisierungssysteme, die nur einen zentralen Proxy nutzen, bergen noch ein anderes Risiko. Wie Hal Roberts vom Berkman Center vor einigen Monaten herausfand, verkaufen die in China populären Dienste DynaWeb Freegate, GPass und FirePhoenix offenbar Listen, die festhalten, welche Seiten ihre Nutzer aufgerufen haben. Zwar gibt es keinen Beleg dafür, dass dabei persönliche Nutzerdaten preisgegeben wurden. Aber der Vorgang zeigt die Krux vieler Anonymisierungsdienste: Wer sie nutzt, weil er dem Staat misstraut, muss dennoch dem Betreiber des Systems trauen. „Ich zweifle nicht die Ernsthaftigkeit der Betreiber an, aber ich frage mich, ob sie die Daten schützen“, sagt Roberts. „Das Problem ist: Sie haben die Daten.“ Bei Tor immerhin ist das anders, weil nirgendwo Daten über die gesamte Route durchs Proxy-Netzwerk aufgezeichnet werden. Vertrauen muss der Nutzer hier nur den Algorithmen, die die Verbindung zwischen Absender und Adressat verschleiern.

Dingledine geht davon aus, dass jeder weitere Privacy- oder Zensurvorfall die Anwendung von Tor und ähnlichen Systemen fördert. 2006 zum Beispiel **veröffentlichte AOL[14]** die Suchbegriffe von einer halben Million AOL-Kunden für Forschungszwecke. Die Listen mit den Suchbegriffen waren zwar mit Zufallsnummern und nicht mit echten Identitäten versehen, aber Blogger und Journalisten konnten in einigen Fällen anhand der Begriffe schnell Zuordnungen zu realen Personen herstellen. Solche Verletzungen der digitalen Privatsphäre, aber auch neue Blockaden von Nachrichtenseiten oder Diensten wie YouTube irgendwo auf der Welt würden die Menschen automatisch nach Lösungen suchen lassen, so Dingledine. „Unser Ansatz ist: Sollen die Schurken selbst die Überzeugungsarbeit leisten. Lasst die AOLs und die chinesischen Firewalls Mist bauen.“ Dann werden sich immer mehr Menschen sagen: Genug ist genug.

Mehr über Tor: ***deutsche Informationsseite[15]*** *des Projekts.*

(**bsc[16]**/Technology Review)

URL dieses Artikels:
http://www.heise.de/tr/artikel/141122

Links in diesem Artikel:
[1] http://www.sokwanele.com/

[2] http://www.torproject.org/
[3] http://globalvoicesonline.org/author/ezuckerman/
[4] http://de.globalvoicesonline.org/
[5] http://opennet.net/
[6] http://deibert.citizenlab.org/
[7] http://www.freehaven.net/~arma/cv.html
[8] http://www.eff.org
[9] http://globalvoicesonline.org/author/anas-qtiesh/
[10] http://wendy.seltzer.org/
[11] http://www.chillingeffects.org/
[12] http://advocacy.globalvoicesonline.org/author/nasserweddady/
[13] http://cyber.law.harvard.edu/
[14] http://www.heise.de/newsticker/AOL-veroeffentlichte-Suchanfragen-von-ueber-500-000-Mitgliedern--/meldung/76474
[15] http://www.torproject.org/index.html.de
[16] mailto:bsc@tr.heise.de