„Jeder hat das Recht auf Meinungsfreiheit und freie Meinungsäußerung; dieses Recht schließt die Freiheit ein, Meinungen ungehindert anzuhängen sowie über Medien jeder Art und ohne Rücksicht auf Grenzen Informationen und Gedankengut zu suchen, zu empfangen und zu verbreiten.“ – Allgemeine Erklärung der Menschenrechte, Artikel 19, Vereinte Nationen, 10. Dezember 1948

Überblick

Mit Tor existiert seit 10 Jahren ein wirksames und von hunderttausenden Menschen verwendetes Werkzeug, um Zensurmaßnahmen im Internet zu umgehen. Bislang mangelt es dabei an technischer Infrastruktur. Mit unserem Verein ergreifen wir als Datensicherheitsexperten und Informatiker die nötigen Maßnahmen, um das Tor-Netzwerk für alle Nutzer schneller und sicherer zu machen. Wir suchen nach Partnern, die uns dabei finanziell unterstützen.

Internetzensur

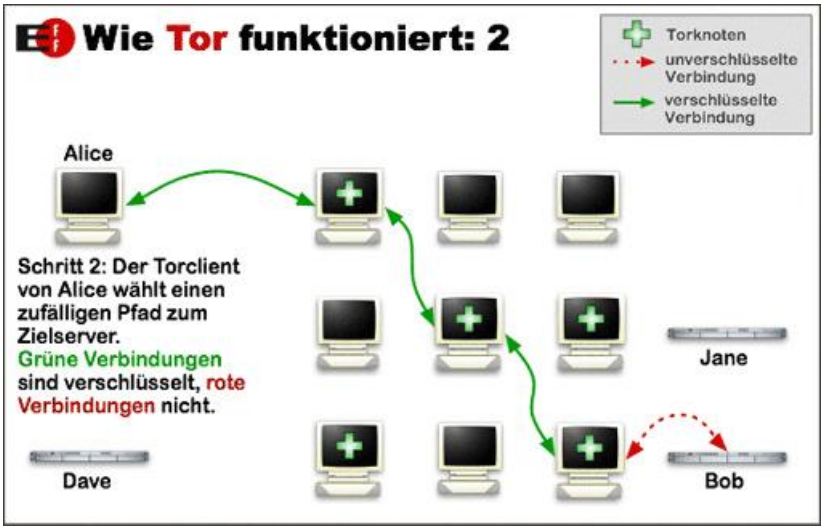
Durch die rasant zunehmende Verbreitung des Internets steigt auch die Anzahl der Länder, die das Nutzungverhalten ihrer Bevölkerung im Netz überwachen und zensieren. In einem Report von November 2010 spricht Google von mehr als 40 Regierungen, die den Netzzugang „in breitem Stil“ beschränken.

There is a growing consensus that governments must do more than appeal for the protection of human rights and encourage development of tools that allow users to bypass government firewalls. Censorship on the Internet poses a significant economic threat to companies seeking a level playing field as the established markets overseas. [1]

Reporter ohne Grenzen sprechen in ihrem Report „Enemies of the Internet“ von etwa 60 Ländern mit aktiver Internetzensur im Jahr 2009, einer Verdopplung gegenüber 2008.[2]

Tor

Tor ermöglicht es jedem Internetnutzer, sich einer Internetüberwachung und -zensur zu entziehen. Dabei leitet es den Datenverkehr verschlüsselt über Zwischenstationen, so genannte „Knoten". Es nutzt dabei ausschließlich Bandbreite, die von Freiwilligen zur Verfügung gestellt wird, die ihren Internetzugang so mit Tornutzern teilen. Momentan werden etwa 2000 solcher Knoten von Einzelpersonen und kleineren Organisationen betrieben. Tor stellt mit geschätzten 100.000 Nutzern täglich die erfolgreichste und vielversprechendste Lösung zur Zensurumgehung überhaupt dar.



Zu den Nutzern von Tor gehören neben NGOs, Journalisten und Menschenrechtsaktivisten auch Firmen und Regierungsmitglieder. Die Website des Projekts listet zahlreiche Beispiele.[3]

Dabei setzt Tor seit inzwischen 10 Jahren Forschungsergebnisse aus dem Bereich Datenschutz und Datensicherheit in die Praxis um. Die Entwicklergruppe Torproject Inc. bezog im Jahr 2009 rund 1,25 Millionen US-Dollar aus staatlichen und privaten Fördermitteln. Zu den Förderern gehören Internews, die National Science Foundation, das Naval Research Laboratory (US Navy), Human Rights Watch und Google. Derzeit arbeiten 15 Vollzeitmitarbeiter und etwa ein Dutzend Ehrenamtliche an der Weiterentwicklung.[4] Torproject Inc. kooperiert mit zahlreichen Universitäten. Jährlich erscheinen mehr als 20 wissenschaftliche Arbeiten, die sich mit Tor beschäftigen.[5] Die Forschungsergebnisse fließen in die bestehende Software ein, die so beständig weiterentwickelt wird. Unter einer Open Source-Lizenz steht Tor kostenlos für Windows, Mac, Linux, Android und iPhone zur Verfügung.

Bridges

Damit die Zwischenstationen von der Software gefunden und genutzt werden können, kann man diese in einer Liste öffentlich abrufen. Die Torstatus-Seiten erlauben einen Überblick über alle aktiven Knoten.[6] Im September 2009 begann China als eines der ersten Länder, die öffentlich bekannten Torknoten zu sperren. Das neu eingeführte Konzept der „Bridges“ arbeitet dem entgegen: Bridges sind nichtöffentliche Torknoten, deren IP-Adressen in kontrollierter Form an Aktivisten und Menschenrechtsorganisationen weitergegeben werden können, und die diesen als Einstiegspunkt in das Tornetzwerk dienen. Momentan existieren etwa 500 Bridges, Nutzer können einzelne Adressen per Email, Webinterface und Internet Relay Chat anfordern. Auch Bridges werden ausschließlich von Freiwilligen, zumeist auf Heimanschlüssen, betrieben. Da viele Heimanschlüsse eine wechselnde IP haben und nicht in jedem Fall rund um die Uhr stabil betrieben werden, gibt es Versorgungsschwierigkeiten. Bei der Zusammenarbeit mit NGOs ergab sich so das Problem, dass verlässliche Partner zur Bereitstellung von Bridges fehlten, obwohl die Kosten für eine solche Bridge mit weniger als einem Euro pro Adresse und Monat sehr überschaubar sind - es gab bisher nur niemanden, der diese professionell anbietet. Bridges können von vielen Personen gleichzeitig genutzt werden und müssen nur getauscht werden, wenn die jeweilige Regierung sie ermittelt und sperrt.

Torservers.net – Projekt und Vereinsgründung

Die Softwareentwickler hinter Torproject Inc. betreiben keine eigene technische Infrastruktur und sind somit auf Mithilfe angewiesen. Die Nutzerzahlen steigen, gleichzeitig stagniert der Anteil derer, die ihrerseits Bandbreite zur Verfügung stellen. Die Bandbreite üblicher Heimanschlüsse ist nicht ausreichend, für schnellere Knoten ist eine Rechenzentrumsanbindung und technisches Knowhow nötig. Torservers.net ging im Juni 2010 online und betreibt mit Hilfe von privaten Spenden seitdem Torknoten in mehreren Rechenzentren in verschiedenen Ländern, darunter einer der schnellsten Torknoten weltweit. Der Betrieb wird von ehrenamtlichen Experten aus dem Bereich der Informatik sichergestellt, die in engem Kontakt zu den Entwicklern von Tor stehen und selbst auch in diesem Bereich arbeiten und forschen.

Für die Koordination der Aktivitäten ist die Gründung eines gemeinnützigen Vereins noch in diesem Jahr geplant. Die Aufgaben des Vereins sollen dabei unter anderem umfassen:

- Betrieb von Torknoten und Bridges

- Vorträge, Workshops und Schulungen im Bereich Datenschutz und Datensicherheit, Zensur und Anonymität
- Regelmäßige Treffen von interessierten Nutzern und Entwicklern
- Kooperation mit Menschenrechtsorganisationen und Journalisten
- Erstellung von Informationsmaterial für Nutzer, Förderer und Betreiber

Das Tor-Netzwerk ist auf stabile und schnelle Knoten angewiesen. Dank ehrenamtlicher Mitarbeiter fallen nur die reinen Betriebskosten an - momentan sind das 150 Euro monatlich, die wir bislang über private Spenden zu decken versuchen. Da wir die dezentrale Architektur des Tor-Netzwerks und damit die Anonymität aller Nutzer stärken möchten, wollen wir weitere Server und Bridges in verschiedenen Rechenzentren betreiben. Voraussichtlich im ersten Quartal 2011 wird einer der schnellsten Knoten des Tornetzes abgeschaltet. Er wurde bisher auch von einer Privatperson finanziert und betrieben. Durch die Abschaltung entsteht eine Versorgungslücke, die wir rechtzeitig schließen wollen.

Bislang erforderte die Unterstützung technische Kenntnisse. Wir ermöglichen auch technischen Laien, zur Stärkung einer der wichtigsten Zensurumgehungsmaßnahmen beizutragen.

Die Vermittlung von Schutztechniken an Menschenrechtler und Journalisten ist uns dabei besonders wichtig. Ein weiteres Ziel ist die politische Aufklärung über Anonymität als Grundstein für die Entfaltung einer freien Gesellschaft. Deshalb nehmen wir regelmäßig an Konferenzen und Kongressen teil. Wir stehen in engem Kontakt mit anderen Organisationen, um beispielsweise gemeinsam Stellungnahmen bei EU-Konsultationen einzureichen. Künftig möchten wir außerdem Kontakte zu Organisationen aufbauen, die Bridge-Adressen direkt an Aktivisten weiterleiten können. Die Reise- und Teilnahmekosten werden bislang von den ehrenamtlichen Mitarbeitern selbst getragen.

Transparenz

Eine größtmögliche Transparenz ist uns wichtig, und zwar sowohl in Bezug auf Einnahmen und Ausgaben, als auch was unsere Arbeit direkt betrifft. Wir streben deshalb eine Veröffentlichung aller anfallenden Posten an. Unsere technische Dokumentation zum Betrieb von Tor-Knoten und unser Informationsmaterial werden unter einer freien Lizenz veröffentlicht und können so von jedem Interessierten nachvollzogen und frei genutzt werden.

Finanzierungsplan

1800 Euro jährlich beträgt die Miete eines 300Mbit/s-Servers in den USA. Damit transportieren wir bis zu 37,5 Megabyte pro Sekunde für Nutzer des Tor-Netzwerks – und das in beide Richtungen. In einem ersten Schritt gilt es, diese Kosten anstatt über unregelmäßige Privatspenden über feste Partner zu sichern. Daneben fallen etwa 200 Euro für Verwaltung, Druck von Broschüren etc. im Jahr an, die bisher von den Mitgliedern getragen werden.

Mittelfristig planen wir, weitere Server innerhalb Europas anzumieten, und unseren Mitarbeitern zumindest Teile ihrer Unkosten zu erstatten (ab Förderbeträgen um 3000 Euro jährlich). Langfristig wäre es sehr von Vorteil, über eigene Hardware zu verfügen, und den Serverstandort ganz von den USA nach Europa verlegen zu können (ab ca. 10.000 Euro jährlich).

Wie profitieren Organisationen von einer Förderung?

Im Gegenzug können wir Partnerorganisationen nicht nur auf unseren Seiten bewerben, sondern auch die Torknoten selbst können frei wählbare Namen der Organisationen tragen. Je höher die Förderung, desto schneller ist der jeweilige Knoten, und desto häufiger taucht der Name in den aktuellen Verbindungen der Nutzer und in der Liste der Torknoten auf. Momentan tragen unsere Server neutrale Namen (TORSERVERSNETX). Bezeichnungen wie AMNESTYINT oder REPORTEROHNEGRENZEN wären denkbar.

Ruft man die Adresse eines Torknotens direkt im Browser auf, erscheinen Inhalte, die wiederum die Partnerorganisation(en) bewerben können.

Missbrauch

Technologie als Werkzeug kann missbraucht werden. Tor ist da leider keine Ausnahme. Auch wenn viel dafür getan wird, um Missbrauch vorzubeugen, gibt es vereinzelt Fälle, in denen die angebotene Anonymität zu Fehlverhalten im Internet führt.

Die Erfahrung der letzten 10 Jahre hat gezeigt, dass solche Fälle bei Tor selten sind. Für Kriminelle ist es ein Leichtes, eine vergleichbare Infrastruktur selbst zu schaffen; Botnetze sind ein bekanntes Beispiel dafür. In der Tradition von Professor Andreas Pfitzmann, bis 2010 Lehrstuhlinhaber und Dekan der Fakultät Informatik in Dresden, vertreten wir die Auffassung, dass durch ein Verbot von Verschlüsselung oder Anonymisierung nur „unbescholtenen Bürgern“ geschadet wird. Kriminelle werden sich durch Verbote nicht vom Einsatz solcher Technologien abhalten lassen. Professor Pfitzmann hat bei zahlreichen politischen Entscheidungen als Gutachter gezeigt, dass das Recht auf informationelle Selbstbestimmung auch ein Recht auf Anonymität umfasst.[7]

Der Betrieb von Torknoten ist legal. Ohne Anonymisierung kann auch Zensur nicht wirksam umgangen werden. Nach unserer Auffassung ist diese die beste technische Möglichkeit, Menschenrechtsverletzungen im Ausland zu begegnen und Journalisten in unsicheren Netzen zu unterstützen.

Nutzt man Tor, stammt die ausgehende Verbindung augenscheinlich vom letzten Glied in der Stellvertreter-Kette, also dem letzten Torknoten. Es ist ein Fall dokumentiert, in dem der Betrieb eines Tor-Anonymisierungsdienstes zu einer Hausdurchsuchung geführt hat. Die Ermittlungen gegen die Betreiber wurden eingestellt, nachdem geklärt werden konnte, dass der Betreiber nicht der Verursacher war. Viele staatlichen Behörden sind mittlerweile dazu übergegangen bei eindeutig gekennzeichneten Tor-Knoten die Ermittlungen einzustellen bzw. gar nicht erst einzuleiten, da der Betreiber keine Möglichkeit hat, die Verbindung zum Ursprung zurück zu verfolgen.

Momentan laufen mehrere Forschungsarbeiten, die sich mit der Problematik beschäftigen, um in Zukunft Missbrauch noch besser zu verhindern bzw. stark einzuschränken.[8,9,10]

Kontakt

Moritz Bartl, 28, beschäftigt sich seit 1996 mit Datenschutz und Datensicherheit und ist für verschiedene Internetprojekte ehrenamtlich tätig. Mit 18 Jahren gründete er seine erste Firma zur Kundenbetreuung und dem Vertrieb eigener Software. Momentan studiert und arbeitet er an der TU Dresden, Fachrichtung Informatik, und ist Initiator und Gründer von torservers.net.

Moritz Bartl, Görlitzer Str. 2, 01099 Dresden, Tel. 0176/96 373 484, moritz@torservers.net

Quellen

[1] Google: Internet Censorship Amounts to Undeclared Trade War – http://arstechnica.com/tech-policy/news/2010/11/google-net-censorship-amounts-to-undeclared-trade-war.ars
[2] Reporters Without Borders: Enemies of the Internet (März 2010) – http://en.rsf.org/IMG/pdf/Internet_enemies.pdf
[3] Tor Project: Users – https://www.torproject.org/about/torusers.html.en
[4] Tor Project: Sponsors – https://www.torproject.org/about/sponsors.html.en
[5] Freehaven: Selected Papers in Anonymity – http://freehaven.net/anonbib/date.html
[6] Tor Network Status – z.B. http://torstatus.all.de/
[7] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Sicherheit im Internet durch Anonymität – https://www.datenschutzzentrum.de/download/anonheft.pdf
[8] Y. Chen, R. Sion, B. Carbunar - XPay: Practical anonymous payments for Tor routing and other networked services (Nov 2009) – http://www.cs.sunysb.edu/~sion/research/sion2009wpes-xpay.pdf
[9] T. Ngan, R. Dingledine, D. Wallach - Building Incentives into Tor (Jan 2010) – http://freehaven.net/anonbib/papers/incentives-fc10.pdf
[10] R. Henry, K. Henry, I. Goldberg - Making a Nymbler Nymble using VERBS (Jul 2010) – http://www.cacr.math.uwaterloo.ca/techreports/2010/cacr2010-05.pdf