WO STEHEN WIR?

„Snowden Effekt“

Seit der „Prism“-Affäre ist Anonymität ein gefragtes Gut

Noch nie waren so viele Menschen anonym im Netz unterwegs wie heute. Die Nutzer des „The Onion Router“ („Tor“)-Netzwerks haben sich in einem Jahr stark vermehrt, die Infrastruktur, die dahinter steht, wächst ebenfalls. Nach den Angaben von Sam Grüneisen, dem Präsidenten der „Frënn vun der Ënn“, gibt es weltweit 6.000 „Tor“-Server. 4.000 Einstiegsserver befinden sich in Ländern, wo umfassende Zensur herrscht und es deshalb schwierig ist, das Internet frei zu nutzen. Die Beliebtheit des Netzwerkes gründet sich teilweise auf dessen Ruf bei den Geheimdiensten.

Die NSA bezeichnete „Tor“ als „den König der hoch-sicheren Internet Anonymität mit niedriger Latenz“ - Wenn das nicht mal ein Gütesiegel ist? Doch die „Prism“-Leaks waren nicht der einzige Antrieb für diese Entwicklung. Bereits während der Proteste im Iran und in Ägypten kam das Netzwerk zum Einsatz, wurde das Internet immer stärker zensiert und teils auch die Verbindung dazu gekappt. Der Bedarf für ein Untergrundnetzwerk stieg während des Arabischen Frühlings drastisch. Ähnlich sieht es in der Türkei aus, denn kaum versucht Erdogan mal wieder, Dienste zu blockieren, steigen schlagartig die Nutzerzahlen bei Tor an. Zuletzt war dies im März diesen Jahres der Fall. Die Zahl der Server steigt aktuell stetig, auch, wenn sie mal abstürzen.

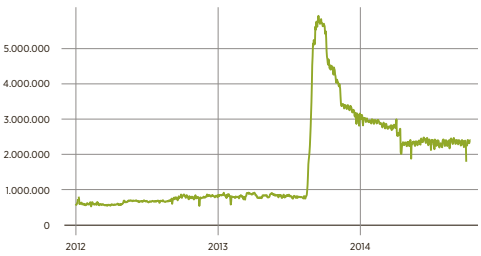
Das Netzwerk sorgt aber gleichzeitig auch für immer mehr Bandbreite: Lag man vor 2013 noch unter 4.000 Mbit die Sekunde, sind es mittlerweile über 12.000 Mbit die Sekunde. Auch die Anzahl der so genannten „Bridges“ steigt immer weiter. Dabei handelt es sich um Zugangspunkte zum Tor-Netzwerk, die dem Netzwerk selbst nicht bekannt sind und nur eine Brücke zu den offiziellen Einstiegsknoten bilden. Diese werden nötig, falls ein Staat versucht, die Einstiegsknoten unzugänglich zu machen. Der Kampf um ein anonymes und freies Internet ist somit einer wahrer Wettstreit: Totalitäre Regimes und Staaten, die ihre Bevölkerung unterdrücken, versuchen, den Betreibern der freien Software das Leben schwer zu machen. Dabei macht bereits die schiere Masse an Nutzern bereits die Überwachung schwer. Mehr als sechs Millionen nutzen es mittlerweile.

Das Netzwerk zu knacken ist mittlerweile ein begehrtes Ziel. Dieses Jahr gab die Regierung Russlands bekannt, dass jeder, der es schaffen würde, herauszufinden, wie man Nutzerinformationen aus dem Netzwerk abschöpfen könnte, 110.000 US-Dollar erhalten könnte. Apropos Finanzierung: 1,8 Millionen US-Dollar betrug das Budget im Jahr 2013. Überraschend ist, wer das Projekt unterstützt. Im Jahr 2011 wurde 60% des Budgets durch die Regierung der Vereinigten Staaten von Amerika getragen. Sponsoren hat das Projekt allerdings auch. Aktuell sind dies ein anonymer amerikanischer Internetdienstanbieter, Googles „Summer of Code“ sowie mehr als 4.300 Einzelpersonen, die Geld spendeten. Ebenfalls mit dabei sind das „US Department of State Bureau of Democracy, Human Rights, and Labor“ (bis 2015) und die „National Science Foundation“ zusammen mit der „Georgia Tech and Princeton University“ (bis 2016).

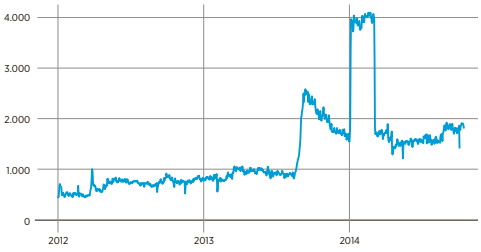
Eigentlich kein Wunder, dass die USA so stark in das Netz investieren, stellen sie doch die meisten „Tor“-Nutzer: Durchschnittlich 350.202 Nutzer gehen damit jeden Tag online. Das sind 15,09% aller Nutzer. Darauf folgen Deutschland (207.841 Nutzer), Russland (146.568), Frankreich (140.245), Brasilien (120.164) und Spanien (92.169). SVEN WOHL

SPRUNGHAFTES INTERESSE

ANZAHL „TOR“-NUTZER WELTWEIT



ANZAHL „TOR“-NUTZER LUXEMBURG



OBEN Snowdens Enthüllungen im Juni 2013 ließen die Nutzerzahlen weltweit steigen
UNTEN Auch in Luxemburg gab es den „Snowden-Effekt“

Quelle: Torproject.org

KLOERTEXT - VERSCHLÜSSELUNG

JAN GUTH
Chaos Computer Club Lëtzebuerg

Jeder hat etwas zu verbergen

Daten sind kostbares gut: Sowohl Geheimdienste als auch Unternehmen zeigen an ihnen großes Interesse. Seit den Snowden-Leaks ist bekannt, dass Geheimdienste auch Durchschnittsbürger ausspionieren. Damit ist der Bedarf an effizienter und einfacher Verschlüsselung gestiegen. Jan Guth vom Chaos Computer Club Lëtzebuerg (C3L) erklärt uns, wieso und wie man verschlüsseln sollte:

„Früher war es mal so, dass man nicht unbedingt verschlüsseln musste. Doch heute ist die Frage relativ schnell geklärt: Daten sollten möglichst immer verschlüsselt werden. Geheimdienste und internationale Firmen versuchen mit so ziemlich allen Mitteln an diese zu kommen. Auch wer kein Terrorist ist, sondern ‚nur‘ ein stinknormaler Durchschnittsbürger sollte Interesse daran haben, zu verschlüsseln. Das ist auch eine Sache des Respekts zeigen, schließlich haben die vorigen Generationen für unsere Freiheit hart gekämpft! Wir haben also die Pflicht, es den Geheimdiensten und Firmen so schwer wie möglich zu machen, an unsere Daten zu kommen. Dabei ist es egal, aus welchen Gründen die Firmen und Dienste uns bespitzeln: Ob das nun Interessen oder politische Einstellungen oder sonst etwas sind, ist irrelevant. Deshalb müssen wir in die Köpfe der Menschen hineinkriegen, dass sie verschlüsseln sollen.

Dabei zündet das Argument ‚Ich habe nichts zu verstecken‘ einfach nicht. Jeder hat etwas zu verbergen – Das kann man ganz einfach testen, indem man sich an einen öffentlichen Ort stellt und die Menschen auffordert, alle ihre Informationen preis zu geben. Die wenigsten werden fähig sein, ihre Lieblingsstellung beim Sex oder sämtliche Ansichten zu jedem Thema einfach so heraus zu posaunen. Verschlüsslung ist das gleiche, wie an einem öffentlichen Ort den Mund zu halten. Es gibt eben Informationen, die man nur mit dem engsten Vertrauten teilen möchte und die sonst niemanden etwas angehen. Das gilt auch für Staatsbeamte: Alle Daten sind gleich und sollen gleich behandelt werden. Die Beamten arbeiten nun einmal auch mit Daten, die jeden im Land betreffen, auch wenn Daten mal mehr, mal weniger kritisch sind. Zudem müssten Politik und Beamte in dieser Hinsicht als Vorbild dienen. So gäbe es auch ein größeres Bewusstsein in der Bevölkerung für dieses Thema.

Doch wie verschlüsseln? Relativ einfach hat man es auf Seiten wie www.prism-break.org: Hier wird ganz einfach erklärt, wie man verschlüsseln kann. Das ist ein erster wichtiger Schritt, auch für uns Hacker: Wir müssen versuchen, diese Programme so nutzerfreundlich zu machen, wie nur möglich! Diese Website stellt dafür einen guten Anfang dar, wobei es immer mehr Programme gibt, die auch bewertet werden. Für Luxemburg gibt es www.Cypherpunk.lu, wo ähnlich verfahren wird.“

„Verschlüsslung ist das gleiche, wie an einem öffentlichen Ort den Mund zu halten“

Wie James Bond
„Tails“ ist ein verschlüsselndes Betriebssystem, das auf den USB-Stick passt. Es hinterlässt keine Spuren, muss nicht installiert werden und ist gratis auf https://tails.boum.org/ zu kriegen.

Beim Häuten der Zwiebel

Wie das „Deep Web“ für Sicherheit sorgt

LUXEMBURG
SVEN WOHL

Die Zwiebel ist quasi das Maskottchen für Nutzer des anonymen Netzes „The Onion Router“ („Tor“). Das hat seine Gründe: Mit ihren zahlreichen Schichten erinnert die Zwiebel an das Netzwerk an sich. Denn es sind diese Schichten, die Internetnutzer im „Deep Web“ (auch „Darknet“) vor Abhöraktionen schützen. Doch wie genau funktioniert eigentlich ein System wie das von „Tor“?

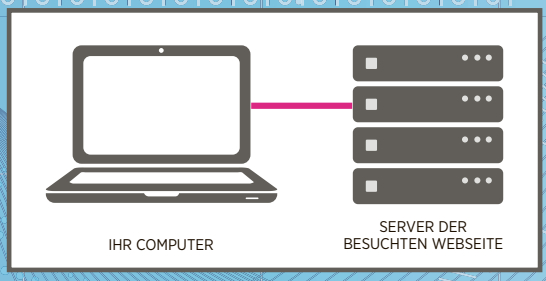
Gut umgeleitet

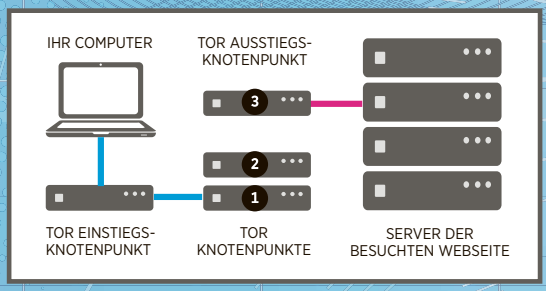
Gehen wir einmal vom Normalfall aus: Ein Internetnutzer sitzt an seinem Computer und tippt die Adresse einer Internetseite in seinen Browser ein. Alles, was nun passiert, ist von außen her einsehbar: Sowohl Hacker, als auch der Internetdienstleister und die Webseite wissen, wer der Nutzer ist und wo er herkommt. Sie wissen auch, welche Daten er überträgt. Kurz: Der Internetnutzer ist für all jene, die lauschen wollen, so etwas wie ein offenes Buch.

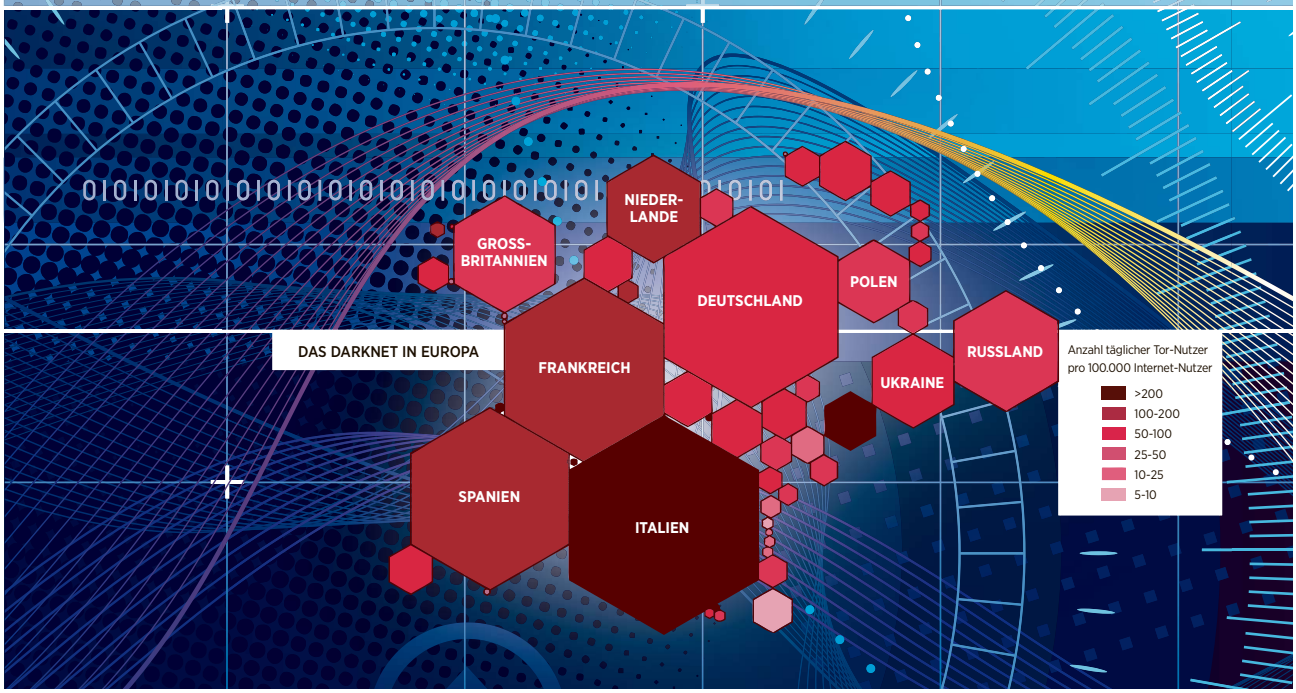
Anders sieht es bei einem Netzwerk wie Tor aus: Wer dieses nutzt, steuert nicht mehr direkt die Webseite mit seinem Rechner an, sondern nimmt gleich mehrere Zwischenstationen. Ein Einstiegs-Knotenpunkt des Tor-Netzwerks wird kontaktiert und dieser vermittelt einen, über verschlüsselte Wege an andere Tor-Knotenpunkte weiter. Die Kommunikation innerhalb des Netzwerks ist verschlüsselt und für die einzelnen Knotenpunkte ist nicht nachvollziehbar, von wo die Information eigentlich ursprünglich herkommt. Der Ausstiegs-Knotenpunkt stellt am Ende die Verbindung zur gewünschten Seite im Netz her. Diese weiß, im Falle einer unverschlüsselten Seite, welcher Knotenpunkt mit ihm kommuniziert, aber nicht, wo die Kommunikation ihren Ursprung hat. Einen Nachteil hat dies allerdings: Die Geschwindigkeit wird durch die vielen Zwischenstationen sehr gedrosselt.

Fehlerquelle Mensch

Der Nutzer bleibt also anonym, sofern er keine persönlichen Daten preisgibt. Wer bei der Zielseite etwa mit seiner Kreditkarte etwas einkauft, der gibt in dem Moment zumindest einen Teil seiner Anonymität wieder auf. Der Mensch ist also in dieser Kette der Anonymität wie so oft das schwächste Glied. Wer „Tor“ nutzen möchte, hat gleich zwei Möglichkeiten: Entweder man holt sich auf www.torproject.org die Vidalia-Software und konfiguriert alles selbst, oder man holt sich das „Tor-Browser-Bundle“ – Die Software ist in beiden Fällen frei. Diese kleine, praktische Lösung enthält einen separaten Browser, der auf Firefox basiert, jedoch einige Sicherheitslücken schließt und die Kommunikation zum Internet durch das Tor-Netzwerk leitet.







Anonym unterwegs
Die App „Onion Browser" erlaubt es, auf dem iPhone und iPad anonym zu surfen. Android-Nutzer greifen auf „Orbot" zurück.

Abgedunkelt

Verschlüsselung wird immer mehr zu einem Muss für Bürger

LUXEMBURG Ihr Name erinnert an einen lokalen Gartenverein, doch technischer geht's eigentlich kaum: Die „Frënn vun der Ënn" setzen sich hier im Lande für das Anonymisierungsnetzwerk „Tor" ein. Damit stehen sie zunehmend im Rampenlicht, da das Thema immer mehr an Bedeutung gewinnt. Doch müssen sich Otto-Normalbürger eigentlich dafür interessieren? „Es gab Zeiten, da hätte ich das noch verneint. Doch in Zeiten erwiesener globaler Massenüberwachung sollte jeder sich Gedanken um seine Privatsphäre machen. Schützen kann man diese sehr gut, in dem man in Darknets, ein Paralellinternet, welches komplett verschlüsselt und anonym ist, unterwegs ist. Früher war dies nur ein Geheimtipp, doch heute wohl eher ein Muss für den Bürger", erklärt Sam Grüneisen, Präsident der „Frënn vun der Ënn", im Interview mit dem „Journal".

Wachstumspotenzial

Ein Muss also, doch bedeutet dies, dass die Kapazitäten gleich durch eine Flutwelle von neuen Nutzern überstrapaziert werden? Sam Grüneisen beruhigt: „Die aktuellen Infrastrukturen reichen momentan vollkommen und werden es auch noch wenn 1.000 oder mehr User dazu kommen." Doch was, wenn es wesentlich mehr sind? „Wenn nun plötzlich 20.000 oder mehr neue Nutzer dazu kommen - Was wir jedoch sehr begrüßen würden! - ist ein Infrastrukturausbau alternativlos. Das versuchen wir als Verein zu erreichen. Wir würden gerne heute schon mehr Server zur Verfügung stellen. Doch als gemeinnütziger Verein sind wir auf Spenden angewiesen. Je mehr Spenden, desto mehr Server können wir ins Netzwerk speisen. Dies erhöht die Stabilität, Anonymität sowie die Geschwindigkeit des Tor-Netzwerkes."

Massen-Anonymität

Mehr „Tor"-Nutzer tragen zudem zur Sicherheit bei, meint Sam Grüneisen. Dabei gehe man regelrecht in der Masse unter! Doch was sagt der Spezialist zu den immer wieder auftauchenden Nachrichten, dass das Netzwerk gar nicht so sicher sei, wie das immer behauptet wird. „Diese Meldungen werden leider zu oft gehyped, da sie auf Altbekanntem basieren. Zum Beispiel kann jeder einen ‚Tor'-Server betreiben. Das umfasst, sie, mich, ihren Nachbarn, ihren Chef. Aber auch Geheimdienste", erläutert Sam Grüneisen. „Wenn nun tausende Server von Geheimdiensten betrieben werden, dann ist das, offensichtlich, schlecht", erzählt er weiter und ergänzt, dass selbst die Betreiber die verschlüsselten Datenströme nicht auswerten können. „Nur bei dem Ausgangsserver könnte man Klartext mitlesen. Doch hier peitschen ja Gottseidank Vereine wie der Chaos Computer Club Lëtzebuerg Entwicklungen voran, dass jeder Kontakt mit einer Webseite verschlüsselt passiert", fügt Sam Grüneisen hinzu. Doch macht man sich mit dem Nutzen von „Tor" nicht automatisch verdächtig? „Kurz und knapp: Ja", meint er darauf. Für die Geheimdienste seien „Tor"-Nutzer automatisch Terroristen. „Das macht mich damit zum stolzen Gründer einer terroristischen Vereinigung", erklärt Sam Grüneisen.

SVEN WOHL

➲ **Mehr Informationen auf www.enn.lu**

Abgenutzter Terminus

Alexandre Dulaunoy von CIRCL im Kurzinterview

LUXEMBURG „Müsste man „Tor" nicht verbieten, weil es illegal ist?" Alexandre Dulaunoy vom Computer Incident Response Centre Luxembourg (CIRCL) muss schmunzeln, währendem er diese an ihn und seine Kollegen oft gestellte Frage im „Journal"-Gespräch wiederholt. Müsse man dann, rein theoretisch betrachtet, nicht auch alle Modems der Welt verbieten, die dem User Zugang zum WWW gewähren, lautet seine kurze, aber sehr plausible Gegenfrage? Dulaunoy ist um Aufklärung bemüht. Viele Menschen benutzen nämlich fälschlicherweise den Terminus „Darknet", um ein illegales Netzwerk zu bezeichnen, „Tor" ist für sie der ultimative Schlüssel zur Webhölle. Nicht jede Seite im Darknet sei nun aber illegal, unterstreicht der CIRCL-Mitarbeiter und fügt hinzu, dass der Begriff „Darknet" seines Erachtens schon ziemlich abgenutzt sei.

Angesichts der aufflammenden Debatten um das „Darknet" vergessen heute viele User, dass das klassische World Wide Web schon seit langem ein Hort zahlreicher Internetseiten ist, die über früh oder lang riskieren wegen ihres illegalen Inhaltes die Aufmerksamkeit der Ermittlern auf sich zu ziehen. Beim „Darknet" handele es sich um ein schwieriges Thema, reflektiert Dulaunoy.

CIRCL werde regelmäßig von Privatpersonen oder Firmen auf Darknet-Seite aufmerksam gemacht, die illegale Dienste anbieten würden, erklärt Alexandre Dulaunoy. „Seiten, die etwa Kreditkarten zum Verkauf bieten".

PAV

Fotos: Shutterstock, Editpress

„Nicht jede Seite im Darknet ist illegal"

ALEXANDRE DULAUNOY, Mitglied des CIRCL