Jürgen Schmidt

Eigen-Tor

Gefahren der Tor-Nutzung im Alltag

In der aktuellen Diskussion hört man häufig den Rat, für mehr Privatsphäre und Sicherheit solle man den Anonymisierungsdienst Tor nutzen. Tatsächlich ist dies jedoch ein sehr gefährlicher Tipp. Für normale Anwender erhöht er de facto das Risiko, tatsächlich überwacht und ausspioniert zu werden.

Vorweg sei gesagt, dass Tor gute Dienste leisten kann, wenn man genau weiß, worauf man sich einlässt und sich dann auch dementsprechend verhält. Für den Internet-Alltag von Lieschen Müller Tor hingegen ungefähr so sinnvoll, wie eine Abkürzung zum Supermarkt über einen Schleichweg durch ein hochgiftiges Sumpfgebiet.

Die Missverständnisse beginnen schon mit der Aussage, dass Tor die übertragenen Daten verschlüssele. Das stimmt zwar für den Verkehr zum und durch das Tor-Netzwerk. Aber was man unverschlüsselt in Tor hineinschickt, kommt auf der anderen Seite auch unverschlüsselt wieder heraus und wird dann auch im Klartext weiter durch das Internet verschickt.

Im Endeffekt vergrößert Tor damit sogar die Gefahr, dass Dritte Ihre Daten mitlesen. Um Sie zu belauschen, muss sich ein Überwacher erstmal Zugang zu Ihrem Internet-Verkehr verschaffen – etwa mit einem entsprechenden Durchsuchungsbefehl bei Ihrem Provider. Doch das bedeutet Aufwand und es gibt Regeln, die einzuhalten sind.

Wenn Sie jedoch Tor benutzen, kommt Ihr Internet-Verkehr automatisch bei einem Tor-Exit-Knoten vorbei – ganz ohne weiteres Zutun und quasi als Freiwild. Und dessen Betreiber kann alles mitlesen, was Sie nicht explizit verschlüsseln. So hat etwa der Schwede Dan Egerstad in kurzer Zeit über tausend E-Mail-Passwörter aus dem Netzwerkverkehr seiner Tor-Exit-Nodes gefischt – unter anderem von diversen Botschaften und Behörden.

Das Tor-Netz wird von Freiwilligen betrieben. Da es keinerlei Kontrollen gibt, muss man schon angesichts der reizvollen Man-in-the-Middle-Position davon ausgehen, dass ein beträchtlicher Teil der Tor-Exit-Nodes nicht etwa von Menschenrechtsaktivisten, sondern von Geheimdiensten betrieben wird. Beim normalen Surfen besteht also ein gewisses Risiko, dass Ihr unverschlüsselter Datenverkehr belauscht wird; wenn Sie Tor nutzen, ist das so gut wie sicher.

Man muss also alles, was über Tor geht, aktiv verschlüsseln und selber durch entsprechende Vorkehrungen dafür sorgen, dass da nicht etwa aus Versehen etwas Unverschlüsseltes durchrutscht. Und dann schicken Sie Ihre verschlüsselten Daten bei den besten Codeknackern der Welt vorbei und sagen: „Ätsch!“

Das kann funktionieren. Zumindest dann, wenn Sie sich richtig gut auskennen, alle notwendigen Sicherheitsvorkehrungen einhalten, etwa weil Sie wissen, dass Ihr Leben davon abhängt. Immerhin kann man heutzutage durchaus Daten so verschlüsseln, dass sich auch Geheimdienste wie die NSA daran die Zähne ausbeißen.

Wenn Sie allerdings nur am Abend nach einem anstrengenden Arbeitstag bei einem Bier ein bisschen Surfen wollen, sieht die Sache anders aus. Dann kann es vielleicht schon mal passieren, dass Sie genervt eine Fehlermeldung wegklicken. Die hätte Sie darauf aufmerksam machen sollen, dass mit dem Zertifikat der Seite, die Sie gerade aufrufen wollen, etwas nicht in Ordnung war. Und dann haben die NSA-Jungs, denen Sie eine Nase gedreht haben, Sie am Wickel.

Wenn Sie Pech haben, gibt es vorher noch nicht einmal eine Fehlermeldung. Denn man muss wohl davon ausgehen, dass die NSA zumindest eine Zwischenzertifizierungsstelle betreibt, mit der sie als Man-in-the-Middle Zertifikate ausstellen kann, die jeder Browser klaglos akzeptiert. Wer Microsoft, Apple, Google & Co. zur Mitarbeit bewegen kann, wird sich von Zertifikatsherausgebern nicht abweisen lassen. Einfache SSL-Verschlüsselung von https-Seiten bietet dann keinen ausreichenden Schutz mehr. Stattdessen muss man eigentlich die Fingerabdrücke der Web-Seiten-Zertifikate prüfen – und zwar jedes Mal.

Aktive Angriffe

Die Verbindungen über das Tor-Netzwerk werden auch keineswegs nur passiv belauscht. Geheimdienste und Strafverfolger betrachten die Tor-Nutzer quasi als Freiwild und greifen die nach Belieben an. Vor wenigen Wochen hat jemand ganz gezielt über das Tor-Netz Sicherheitslücken in einer Firefox-Version ausgenutzt, die nahezu ausschließlich im Anonymisierungspaket Tor Browser Bundle zum Einsatz kam. Auf diesem Weg wurde ein kleines Spionageprogramm auf die Rechner der Tor-Nutzer geschleust. Es sieht alles so aus, als sei das Teil einer FBI-Aktion zum Sprengen eines Kinder-Porno-Ringes gewesen.

Insgesamt steigt die Wahrscheinlichkeit, dass Ihre Privatsphäre als Kollateralschaden geopfert wird, durch die Nutzung von Tor deutlich an. Sieht man sich die Ratschläge der Tor-Entwickler zur sicheren Nutzung ihres Dienstes an, wird klar, wohin die Reise geht. Unter anderem legen sie den Wechsel von Windows zu einer speziellen Linux-Live-Distribution auf DVD ans Herz, empfehlen das Abschalten von JavaScript und ein zufälliges Setzen der Mac-Adresse bei jedem Systemstart. Die Nutzung von Flash und anderen Erweiterungen ist ohnehin tabu. Also nix mit „noch 'n bisschen rumsurfen, spielen und Spaß haben“ – ohne Helm, Gasmaske und kugelsichere Weste hat man im Tor-Netz nichts zu suchen.

Mittlerweile gibt es auch noch berechtigte Zweifel, ob Tor das Versprechen der Anonymität überhaupt noch halten kann. Server-Betreiber und auch herkömmliche Strafverfolger beißen sich daran zwar die Zähne aus. Aber wenn die NSA tatsächlich beträchtliche Teile des Internet-Verkehrs systematisch auswerten kann, bietet ihr das einen Hebel, diese Anonymität zu knacken. Ganz grob vereinfacht könnte sie das Opfer auf eine Web-Seite locken, die weitere Ressourcen wie Bilder nachlädt. Größe und zeitliche Abfolge der zugehörigen Pakete bilden dann ein Muster, das man „auf der anderen Seite“ des Tor-Netzes erkennen und damit einer konkreten Adresse zuordnen könnte.

Nimmt man noch hinzu, dass die Daten nur im Schneckentempo und mit fühlbarer Verzögerung durchs Tor-Netz tröpfeln, wiegt der Nutzen für Otto Normal und dessen Bedürfnis nach Privatsphäre die damit verbundenen Einschränkungen und Risiken kaum mehr auf. Auf der anderen Seite steht und fällt das Konzept damit, dass genug normale Internet-Anwender Tor benutzen und damit denen, die wirklich auf Anonymität angewiesen sind, sozusagen Deckung bieten. Im Idealfall sind das Dissidenten und Menschenrechtsaktivisten, die von ihrer Regierung verfolgt werden und auf diesen Schutz wirklich angewiesen sind. (ju) c't

Tor als Anonymisierungsdienst

Für den Server sieht es so aus, als spräche er mit der Tor-Exit-Node. Deren Betreiber kann den kompletten Verkehr mitlesen.