Von Zwiebeln und Schnüfflern

Risiken und Nutzen von Anonymisierungsdiensten

Schon seit einiger Zeit ist die Verwendung von Diensten wie JAP oder gar TOR unter Leuten, die sich überwachungsarm im Internet bewegen möchten, verbreitet, und wir werden bei unseren Veranstaltungen nicht selten gefragt, was davon zu halten sei. Im Zuge der Debatte um die Vorratsdatenspeicherung (vgl. Get Connected in der RHZ 3/2007) wird das Interesse wohl weiter wachsen.

Bei beiden handelt es sich um Anonymisierungsdienste, deren Ziel es ist, Kommunikation im Internet weniger leicht (oder gar nicht) nachvollziehbar zu machen. An sich ist das eine feine Sache, doch wer solche Dienste einsetzt, sollte wissen, was er/sie tut, denn falsch eingesetzt können sie mehr schaden als nutzen. Deshalb wollen wir in einem Zweiteiler einen kleinen Einblick in die Welt der anonymisierenden Proxies, der verschlüsselten Protokolle und der Angriffe darauf geben. Dass es dabei dann und wann ein wenig technisch zugeht, ist nicht zu vermeiden. Wer allerdings einen Rechner am Netz betreibt (und dafür reicht schon die normale „Einwahl“), sollte von all den Dingen jedenfalls mal gehört haben.

Worum geht es?

Anonynmisierungsdienste haben grundsätzlich die Funktion, gegenüber einem entfernten Rechner zu verschleiern, woher eine Anfrage kam. Das kann z.B. bei Google interessant sein, weil dort durchaus gespeichert wird, von welchem Rechner (identifiziert durch seine IP-Adresse oder kurz IP) welche Suchanfrage kam. Fragt nun die Polizei, wer wohl alles nach „Gentrifizierung“ gesucht hat[1] , kann durch die IP spätestens in Zeiten der Vorratsdatenspeicherung tatsächlich rückverfolgt werden, wer das so war.

Um das zu verhindern, tritt im einfachsten Fall ein so genannter Proxy („Stellvertreter“) zwischen euch und, im Beispiel, Google. Ein Proxy ist nichts anderes als ein weiterer Rechner, dessen Aufgabe ist, eure Anfragen an den Rest des Netzes weiterzugeben. Euer Rechner sagt diesem Proxy also beispielsweise, welche Webseite ihr haben wollt, und der Proxy fragt an eurer Stelle den Zielrechner. Für Google, und das ist der erste Knackpunkt, sieht es dann so aus, als wolle *der Proxy* Näheres über die Gentrifizierung wissen. Über so einen Proxy lassen aber idealerweise viele Menschen ihre Anfragen laufen, so dass jedenfalls Google nicht mehr weiß, wer sich nun für Städtebau interessiert und wer es bei der Bundesliga bewenden lässt[2] .

So etwas ist nett, wenn es nur gegen Google geht, reicht aber nicht aus, um einem ganzen Staat zu entkommen. Der kann sich einfach auf eure Leitung ins Netz setzen und zusehen, was ihr mit dem Proxy zu reden habt -- dafür reicht eine gerichtliche Anordnung, und die ist hierzulande nicht schwer zu bekommen. Eine recht offensichtliche Abhilfe ist, den Verkehr zwischen euch und dem Proxy zu verschlüsseln, so dass es jedenfalls prohibitiv teuer wäre, die Sachen mitzuschneiden. So in etwa funktionierten die ersten Versionen von JAP, und für den Anfang ist das auch gar nicht schlecht.

Für einen Staat allerdings ist es keine große Kunst, sich vor und hinter den Proxy zu klemmen und nachzusehen, was der Proxy tut, nachdem von irgendwem ein Wunsch hereinkam -- jedenfalls im großen Mittel wird er damit weit kommen. Noch erschweren geltende Gesetze so etwas, aber da etliche Betreiber solcher Proxies längst gelobt haben, mit den sie beherbergenden Staaten zusammenzuarbeiten, ist das vorläufig nicht wichtig. Der Staat kann sich das ganze Abhören sparen und einfach die Betreiber fragen, die genau sagen können, was da durch ihre Rechner gegangen ist.

Onion-Routing

Es ist also jedenfalls riskant, den in der Regel kommerziellen BetreiberInnen von Proxies zu trauen, denn die

sind für ihr Geschäft auf die Kooperation mit den zuständigen Staaten angewiesen -- bei weitem nicht nur chinesische DissidentInnen, die von Yahoo ans Messer geliefert wurden, werden davon beredt Zeugnis geben können, wenn sie den Knast verlassen haben.

Um nun auch ohne Vertrauen zu individuellen BetreiberInnen anonym kommunizieren zu können, haben Hacker das so genannte Onion Routing (OR) ersonnen und ein Programm namens TOR („The Onion Router“) geschrieben, das diese Idee umsetzt. Beim OR verpackt euer Rechner ein Datenpaket mit einer Reihe Schalen, deren jede die nächstinnere komplett umhüllt. Eine Zwiebel (daher der Name) ist ein ganz gutes Modell dafür. Im Unterschied zu einer Zwiebel braucht man aber für jede Schale ein anderes Messer, ohne das an den Inhalt nicht heranzukommen ist. Diese Messer sind nun quer durchs Netz verteilt, über einen ganzen Satz von Proxies.

Auf dem Weg zum Zielserver entfernt der erste Proxy nur die äußerste Schale und weiß zwar, woher das Paket kam, nicht aber, wohin das Paket am Schluss soll und auch nicht, was drin ist. Er weiß nur, an welchen Proxy es als nächstes soll. Dieser nächste Proxy entfernt die nächste Schale, kennt aber nicht mehr euch als ursprünglicheN SenderIn, sondern nur seinen unmittelbaren Vorgänger und den Proxy, der die nächste Schale entfernen kann. So geht das eine Weile, am Schluss jedoch muss dann doch die letzte Schale ab und das Paket an seine Zieladresse, also vielleicht den Webserver von Indymedia oder euren jabber-Server. Das besorgt der letzte Proxy in der Kette, ein so genannter Exit Node (bei TOR spricht man statt von Proxies lieber von Nodes, also Knoten, gemeint ist aber das Gleiche).

Dieser kennt nun den Inhalt eures Pakets, weiß aber nicht mehr, woher es kam, sondern nur, an welchen Proxy eine eventuelle Antwort des Zielrechners gehen soll. Wenn diese Antwort kommt, wird sie in ähnlicher Weise zurückgeschickt, und zwar so, dass nur ihr den Inhalt der Nachricht lesen könnt und kein Proxy in der Kette mehr weiß als seinen unmittelbaren Vorgänger und Nachfolger.

Rechtsfreie Räume

In der Tat macht das der Staatsgewalt das Leben ziemlich schwer, und so dürfte es nicht verwundern, dass sie etwas dagegen unternimmt. Es ist natürlich nichts an all dem illegal, aber das muss in einem Rechtsstaat nicht stören: Willkürliche Hausdurchsuchungen gehen immer und taugen wunderbar als extralegale Strafaktion.

Seit etwa zwei Jahren bekommen die BetreiberInnen von Exit Nodes ziemlich absehbar zu meist unmöglichen Zeiten verbeamteten Besuch, der jedenfalls mal alles auf den Kopf stellt und, je nach Laune, auch mal die gesamte Hardware mitgehen lässt. Vorwand ist typischerweise, dass über den der/dem Heimgesuchten zuzuordnenden Exit Node Urheberrechtsverletzungen begangen oder Kinderpornografie besorgt wurde.

Die Durchsuchungen sind durchweg sinnlos, da die Exit Nodes nicht bei den BetreiberInnen zuhause stehen. Weiter ist sogar den Staatsanwaltschaften klar, dass der Internetverkehr des Exit Nodes in aller Regel überhaupt nichts mit dem Internetverkehr des/der BetreiberIn zu tun hat und dass, selbst wenn das nicht so wäre, garantiert keine Spuren der inkriminierten Taten auf deren Rechnern zuhause nachzuweisen sein werden. In der Tat wurde am Rande solcher Hausdurchsuchungen schon mehrfach eingestanden, man wisse schon, dass es nichts zu finden gebe, aber „rechtsfreie Räume“ seien ja nicht tolerierbar. Der Erfolg, namentlich die Einstellung des Betriebs des Exit Nodes, bleibt dann auch nur selten aus.

Der Staat verfolgt hier ein Kalkül, das erfahrene Castor-AktivistInenn kennen dürften. So wie diese versuchen, die uneinnehmbaren Festungen der Kraftwerke an der Achillesferse der Transporte anzugehen, versucht der Staat hier, das an sich recht sichere TOR-Netzwerk durch Verknappung der Ausgänge zu packen. Müssen die BenutzerInnen typischerweise zwei Stunden auf eine Antwort aus dem „echten“ Netz warten, werden sie entnervt wieder überwachbar und mithin aus Sicht der Obrigkeit „sicher“ kommunizieren. Unterdessen können kommerzielle Unternehmungen das Angebot entsprechender Dienste unter geregelter Staatsaufsicht fortführen. Womit fraglos Freiheit und gedeihliche Wirtschaftsentwicklung gerettet sind.

TOR verwenden?

Dass der Staat mit harten Bandagen gegen TOR vorgeht, hat gute Gründe -- es macht ihm das Belauschen seiner BürgerInnen in der Tat fast unmöglich, wenn diese wissen, was sie tun. Die gilt übrigens unabhängig von der eingangs erwähnten Vorratsdatenspeiche-

rung, die nur eher mittelbar mit TOR zu tun hat; die in diesem Rahmen erfassten Daten haben größtenteils mit dem eigentlichen Internetverkehr nicht viel zu tun.

Anonymisierungsdienste sind im politischen Bereich wertvoll, wenn etwa die Staatsgewalt die komplette Internet-Verbindung abhört (das erfreut sich massiv steigender Popularität in diesen Kreisen), oder wenn sie durch Beschlagnahme oder Ausforschung Daten von Rechnern, mit denen mensch kommuniziert hat (also z.B. Webserver), in die Hände bekommt. Und auch sonst mag der Rückschluss von Aliasen (etwa in Instant Messaging- oder Filesharing-Programmen) auf reale Personen durch Anonymisierung schwieriger werden. In weiterer Ferne könnte sogar das Anbieten von Inhalten (also das Betreiben von Webseiten) anonym möglich werden.

Andererseits ist TOR kein Allheilmittel, auch TOR kommt nicht gegen die Weisheit an, dass es auf absehbare Zeit nichts geben wird, das mit einem Klick für Sicherheit gegen Überwachung sorgt. Dieser Wahrheit musste sich jüngst auch die Gegenseite stellen, als haufenweise Zugänge zu Mailaccounts von Botschaften und anderen Regierungsstellen auf einer Webseite veröffentlicht wurden[3] . Auch diese hatten TOR verwendet, aber dabei offenbar nicht bedacht, dass dem Exit Node der Datenverkehr ohne Zwiebelhäute offensteht. Ist er ohne TOR unverschlüsselt, läuft er auch am Exit Node unverschlüsselt vorbei. Auch ohne den Absender des Pakets zu kennen, kann man in unverschlüsselte Datenpakete reingucken, und das lässt, z.B., wenn sich jemand gerade auf einem Webmail-Account einloggt, durchaus interessante Schlüsse zu, und im (nicht unwahrscheinlichen) Extremfall bekommt man dann eben die Passwörter frei Haus geliefert. TOR kontrolliert nicht, wer Exit Nodes betreibt -- solche Möglichkeiten stehen also auch dem Inlandsgeheimdienst oder dem Staatsschutz offen.

Also: TOR kann für Anonymität sorgen, nicht aber für Verschlüsselung der Daten selbst -- natürlich nicht, denn diese muss zwischen euch und dem *Ziel* eurer Kommunikation ausgehandelt werden. Dieses Ziel ist aber nicht Teil des TOR-Netzes[4] , und so ist TOR da machtlos. Für unverschlüsselte Kommunikation ist TOR sogar eine zusätzliche Gefährdung, denn der durch TOR gehende Verkehr wird die Ohren der Lauscher bis auf weiteres quasi magisch anziehen.

Ohne Verschlüsselung seid ihr *vielleicht* -- so nämlich nicht aus den Daten selbst hervorgeht, wer ihr seid, siehe Google-Cookies oder Mailadressen -- anonym, aber die Daten, die ihr übertragt, werden mit deutlich höherer Wahrscheinlichkeit beachtet. Im Effekt habt ihr eine Nachricht des Typs „Schaut alle auf meine geheimen Daten“ geschickt. Das könnt ihr machen, wenn ihr mit euren Daten wie mit geheimen Daten umgeht, sie also verschlüsselt. Ansonsten ist die Wahrscheinlichkeit hoch, dass ihr euch in den Fuß schießt.

Im nächsten Heft wird es dann darum gehen, was ihr guten Gewissens über TOR verschicken könnt und was nicht ins TOR-Netz -- und eigentlich auch nicht ins normale Internet -- gehört. Außerdem werden wir an zwei Beispielen (Debian/Ubuntu und dem Privacy Dongle für Windows) kurz diskutieren, wie ihr TOR verwenden könnt.

Datenschutzgruppe der Roten Hilfe Heidelberg

datenschutzgruppe@rotehilfe.de

PGP Fingerprint: a3d8 4454 2e04 6860 0a38 a35e d1ea ecce f2bd 132a

http://www.datenschmutz.de

[1] Staatsgewaltiges Interesse daran ist bekanntlich nicht fiktional.

[2] Es sei denn, Google hätte andere Möglichkeiten, das herauszufinden; Google und etliche andere verwenden dazu nämlich auch Cookies. Etwas mehr dazu im nächsten Heft.

[3] http://www.heise.de/security/news/meldung/95262.

[4] Tatsächlich ist auch vorgesehen, allerlei Dienste, ggf. sogar anonym, im TOR-Netz anzubieten. Das ist allerdings noch so experimentell, dass es für diese Betrachtung keine Rolle spielt.