# Von Zwiebeln und Schnüfflern

Teil Zwei des Artikels zu Anonymisierungsdiensten

Nachdem ja nun alle, die die Autoritäten nicht gerne mitlesen lassen, ihre Mails mit PGP verschlüsseln (ahem), könnte der zweite Schritt kommen: Tor, das am Web ähnlich nützlich sein kann wie PGP -- nicht zuletzt, damit es das BKA demnächst nicht mehr so einfach hat mit dem Rückverfolgen, wer alles seine Seiten liest.

Im ersten Teil dieses Artikels (RHZ 4/2007) haben wir beschrieben, wie Tor dafür sorgt, dass euer Netzwerkverkehr schwerer überwachbar wird -- es schickt Pakete so durch etliche Rechner (so genannte Proxies oder Nodes), dass, sofern nicht alle BetreiberInnen zusammenarbeiten, insgesamt nicht mehr realistisch nachzuvollziehen ist, woher ein gegebenes Paket kam.

Warum man das haben möchte, wurde seit dem Erscheinen des ersten Teils schön im Rahmen des mg-Prozesses illustriert: Das BKA hatte eine einschlägige Seite ins Netz gestellt und gespeichert, von welchen Rechnern aus diese Seiten gelesen wurden (das übrigens tun so gut wie alle Betreiber von Webseiten). Das BKA versuchte dann, 400 von diesen Rechnern realen Personen zuzuordnen, was ihm -- noch war die Vorratsdatenspeicherung keine düstere Realität -- nur in 120 Fällen gelang[1] .

Hätten die Betreffenden Tor benutzt, hätte das BKA nur die Adresse des „Exit Node“ (vgl. erster Teil) gesehen und eine Rückverfolgung wäre praktisch unmöglich gewesen.

Doch hatten wir warnend hinzugefügt, dass die Benutzung von Tor ihre eigenen Risiken birgt, da durch Tor laufender Verkehr naturgemäß besondere Aufmerksamkeit auf sich zieht und der Inhalt der Datenpakete am Exit Node so vorliegt, wie er auch normalerweise durchs Netz gehen würde. Wenn, und niemand hindert ihn daran, der Verfassungsschutz so einen Exit Node betreibt, würde er eure Daten quasi auf dem Präsentierteller bekommen.

## Protokolle

Um das zu verhindern, müsst ihr für die Verschlüsselung eurer Daten sorgen, *bevor* ihr sie an einen Anonymisierer schickt. Tatsächlich solltet ihr euch um so eine Verschlüsselung kümmern, egal, ob ihr nachher anonymisieren wollt oder nicht, schon, weil es verglichen mit dem Telefonnetz immer noch recht einfach ist, es vor allem aber eventuell direkt abhörender Staats- oder Lohngewalt das Leben bereits richtig arg erschwert[2] .

Rechner übermitteln inzwischen jede Menge „Typen“ von Information, etwa Mails, Internet-Seiten, Dateien, Instant Messages (IM), Radio usf. Je nach Art der Daten und Charakter des Dienstes verwenden sie dafür verschiedene „Protokolle“, also Vorschriften, welche Fragen ein Rechner stellen und welche Antworten er darauf erwarten darf. Ein Verfassungsschützer, der versucht, Staatsfeinde auszuforschen, hat nun, je nach Protokoll, verschiedene Möglichkeiten. Erschöpfend lässt sich das im Rahmen eines Artikels nicht darstellen. Dennoch lohnt es sich, eine grobe Idee zu haben, was Lauscher so alles wünschen können.

Ein schlichter Mitschnitt der Daten dürfte wohl fast immer erstes Ziel sein. Bei unverschlüsselten Protokollen geht das mit sehr moderatem Aufwand immer, entweder direkt bei euch an der Leitung oder, wenn Tor o.ä. im Spiel ist, eben am Exit Node (wobei dort die Zuordnung zu euch schwierig ist, wenn nicht Personenkennzeichen wie Mailadressen oder Cookies in den Nutzdaten selbst mitschwimmen). Zu diesen besonders einladenden Protokollen gehören ftp und telnet; insbesondere ersteres wird leider immer noch häufig zur Pflege von WWW-Seiten verwendet und lässt sich prinzipbedingt kaum sichern. Ähnliches gilt häufig für „modernere“ Protokolle zur Verwaltung vor allem von Webseiten wie etwa DAV -- das sich aber immerhin leicht sichern lässt.

Leider sind sämtliche Protokolle, die mit Mail zu tun

haben -- also POP, IMAP und SMTP -- von vorneherein erstmal unsicher. Wenn ihr allerdings eure Mails (etwa mit PGP) verschlüsselt, bekommen LauscherInnen nur das mit, was in den Kopfzeilen steht, also AbsenderIn, EmpfängerIn, Betreff, Datum und noch einiges mehr in der Art. Was ihr am Web macht, ist grundsätzlich auch offen, Seiten mit URLs, die mit http:// anfangen, gehen unverschlüsselt übers Netz. Ähnliches gilt für übliche Internettelefonie[3] .

Grundsätzlich: Praktisch alles, was ihr mit dem üblichen Kram im Netz macht, kann geradezu obszön einfach abgehört werden.

## Passwortklau

Es kommt aber noch lustiger: Sofern die Dienste, die ihr benutzt, passwortgeschützt sind, kann es sein, dass auch diese Passwörter offen übers Netz gehen. Damit können die LauscherInnen eure Daten gleich abonnieren und häufig (etwa bei Verwendung von ftp zur Pflege von Webseiten oder IMAP zum Lesen von Mails) auch noch ändern -- nützlich etwa bei Mangel an Beweisen. Unter welchen Umständen das so ist, ist nicht ganz einfach zu sagen: Bei ftp sind die Passwörter praktisch immer lesbar, bei http in der Regel, bei POP heute meistens nicht mehr.

Weil speziell der Passwortklau auch für Menschen sehr ärgerlich ist, die staatliche Überwachung nicht kümmert (die sich aber z.B. um ihr Bankkonto sorgen), wurden einige Methoden ersonnen, Passwörter nicht im Klartext übers Netz schicken zu müssen. Auch dann könnte ein Exit Node -- je nach Protokoll und Einstellung der Programme -- unter Umständen den Rückfall auf Klartextpasswörter erzwingen. Noch subtiler ist das bei http (also im Web), wenn zwar das Einloggen über eine verschlüsselte Leitung abgewickelt wird (https an Anfang der URL), dann aber wieder unverschlüsselt kommuniziert wird. Als Ergebnis des Einloggens wird nämlich auf dem Browser des/der NutzerIn häufig ein Cookie hinterlegt, also letztlich ein paar Bytes, die bei jedem Abruf der betreffenden Seiten übertragen werden. Diese Cookies kann einE AngreiferIn nun abfangen und selbst verwenden. Nicht selten gelten sie lange Zeit und können verwendet werden, um auf der betreffenden Webseite das zu tun, was der/die NutzerIn auch kann.

## Abhilfe

Wenn euch jetzt der Kopf schwirrt: Ja, unverschlüsselte Protokolle sind eine Pest und bergen viele Risiken. Liest mensch einfach nur öffentliche Webseiten, mag das mehr oder minder egal sein, denn was auf diesen steht, kann auch der Kontaktbereichsbeamte lesen. Bei fast allem anderen müssen verschlüsselte Protokolle her, auch und gerade bei Verwendung von Tor oder ähnlichem.

Zu den in diesem Sinne „guten“ Protokollen gehören ssh (für den Zugang zu Maschinen), sftp (zum Dateitransfer), https (im Web), die SSL- oder TLS-verschlüsselten[4] . Varianten von POP3, IMAP oder SMTP (für Mail), SSL-gesichertes Jabber/XMP (für Instant Messaging (IM); werft ICQ, MSN und Co einfach weg, im absoluten Notfall gibts Gateways von Jabber zu diesen proprietären Diensten) oder WebDAV über https (zur Pflege von Webseiten).

Leider gibt es kein allgemeines Rezept, wie man für die Benutzung dieser „sicheren“ Protokolle sorgt. Teilweise sind andere Programme nötig (etwa bei Verwendung von Jabber), teilweise müssen die Server kooperieren (im Web etwa werden die meisten Server schlicht nicht antworten, wenn ihr in der URL http:// durch https:// ersetzt), in anderen Fällen reichen ein paar Einstellungen.

Als Beispiel sei der Mailclient Thunderbird erwähnt: Dort könnt ihr unter Bearbeiten/Konten/Server-Einstellungen (o.ä., je nach gewählter Sprache) in „Sicherheit und Authentifizierung“ die Optionen TLS oder SSL auswählen und „Sichere Authentifizierung verwenden“ ankreuzen sowie ähnliches unter Postausgangsserver/Bearbeiten tun -- immer vorausgesetzt, die Maschinen, über die ihr Mails austauscht, unterstützen das. Tun sie es nicht, geht Versenden oder Empfangen von Mail nicht mehr (dabei dürfte das Versenden gegenwärtig noch kritischer sein als das Empfangen).

## Man in the Middle

Leider reicht auch das noch nicht, um das Abgreifen von Information am Exit Node sicher zu verhindern. Zwar ist es extrem schwierig, *in* eine durch SSL gesicherte Kommunikation reinzuhorchen. Es ist aber für den Exit Node möglich, sich eurem Rechner gegenüber als euer Zielrechner auszugeben. Dann würde

euer Rechner mit dem Exit Node einen Schlüssel ausmachen. Der Exit Node könnte dann eine weitere Verbindung zum echten Zielrechner öffnen und die Datenpakete nach Inspektion in beide Richtungen weiterreichen. Angriffe dieser Art heißen im Jargon „man in the middle"-Angriffe.

Auch gegen sowas ist ein Kraut gewachsen, das LeserInnen unseres PGP-Artikels schon kennen könnten, nämlich die digitale Signatur, die im Zusammenhang mit der Verschlüsselung von Datenströmen meist als „Zertifikat" bezeichnet wird. Im Mailbereich braucht es leider meist recht tiefe Kenntnisse, um die Prüfung solcher Zertifikate zu veranlassen, und wie beim Web of Trust von PGP stellt sich die Frage, wie eigentlich die Echtheit des Zertifikats selbst geprüft werden kann.

Im Web könnte das alles einfacher sein, denn Browser prüfen bei jeder https-Verbindung ganz selbstverständlich die Zertifikate, die der Zielrechner ihnen vorlegt. Leider gibt es dabei aber auch (mindestens) zwei Probleme, die sich regelmäßig in beunruhigenden Warnungen des Browsers äußern:

(a) warnt der Browser, wenn das Zertifikat nicht für den Namen der Webseite ausgestellt ist, also etwa ein Zertifikat für www.foo.org für server.evil-business.com ausgestellt ist. Das ist gerade auf Servern, die „irgendwo mitlaufen", nur schwer zu vermeiden, denn letztlich liegt es daran, dass auch Server IP-Adressen haben und es (in etwa) für jede IP-Adresse nur ein Zertifikat geben kann. IP-Adressen werden aber knapp gehalten, und deshalb teilen sich politische Seiten oft die IP-Adressen -- nur eine davon kann dann das Zertifikat wirklich auf ihren Namen ausgestellt haben.

(b) warnt der Browser, wenn das Zertifikat von keiner „vertrauenswürdigen" Organisation unterschrieben ist. Bei politischen Seiten hat fast nie eine solche Organisation unterschrieben, denn die, die die Browser anerkennen, verlangen relativ viel Geld für so eine Unterschrift. Wenn ihr „freien" Alternativen wie CA-CERT vertrauen wollt (und das würde solche Warnungen seltener machen, so etwa auch auf unserer Seite www.datenschmutz.de), seht euch mal auf http://wiki.cacert.org/wiki/ImportRootCert um.

Diese beiden Effekte bewirken, dass ihr bei https-Verbindungen zu politischen Seiten fast immer Warnungen seht, die eigentlich auf Man-in-the-middle-Angriffe hindeuten würden, aber in Wirklichkeit nur ökonomisches Rauschen sind. Das ist blöd, weil so „echte" Angriffe kaum zu erkennen sind.

## Ein Fazit zu Tor

Wir hoffen, euch überzeugt zu haben, dass Tor oder auch JAP keine „Silver Bullets" sind. Sie lösen recht weitgehend ein Teilproblem sicherer Kommunikation im Netz -- die Anonymität --, verschlimmern die Situation aber, wenn das andere Teilproblem -- die Vertraulichkeit der Inhalte -- nicht vorher gelöst ist. Es bleibt, dass es einiger Expertise bedarf, um in diesem Sinne „sicher" zu kommunizieren.

Andererseits sind für etliche Anwendungen die beschriebenen Angriffe vielleicht gar nicht relevant. Wenn es euch nur darum geht, google-Suchanfragen so zu stellen oder Webseiten unter Regierungskontrolle so zu lesen, dass eure Zugriffe im Nachhinein mit großer Sicherheit auch vom Staat nicht auf euch zurückzuverfolgen sind, ist Tor eine gute Wahl -- solange ihr wisst, was die Grenzen sind. In den beiden Kästen geben wir ein paar Hinweise, wie man Rechnern so viel Funktionaltät ohne große Klimmzüge gibt.

Wer keine Lust hat, sich um all den Wahnsinn zu kümmern, muss deshalb nicht aufs Netz verzichten -- viele Zentren bieten beispielsweise Internetzugang an, der häufig von Leuten gebastelt wurde, die all die Schrecklichkeiten verstehen. Wenn ihr die Möglichkeit habt, ist es fast sicher eine gute Idee, einschlägige Kommunikation von dort aus durchzuführen. Selbst Internet-Cafes haben in der Hinsicht klare Vorteile, und verglichen mit dem Geld und der Zeit, die ihr in eigene Rechner und Anschlüsse steckt, kann das durchaus attraktiv sein.

Datenschutzgruppe der Roten Hilfe Heidelberg

datenschutzgruppe@rotehilfe.de

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

http://www.datenschmutz.de

### In der Praxis

Die Installation und Kofiguration von Tor und der begleitenden Software ist -- wie

eigentlich immer, wenn es um Sicherheit und Privatheit geht -- nicht ganz einfach. Am einfachsten ist noch anonymes „Surfen“. Dazu braucht es neben Tor noch ein Programm, das die Schwatzhaftigkeit von Web-Browsern kontrolliert und zusätzlich verhindert, dass der Browser allerlei Anfragen an Tor vorbei an so genannte DNS-Server schickt, um herauszukriegen, welche Nummer der Rechner www.steinewerfende-autonome.de wohl hat. Auch unabhängig von Tor empfehlenswert ist dabei Privoxy. Dieses Programm bietet zusätzlich umfangreiche Möglichkeiten, lästige Werbung auszublenden usf.

Eine fertig vorinstallierte Kombo von Tor und Privoxy für Windows bietet der kostenlose xbBrowser, der vom FoeBUD unter dem Namen PrivacyDongle auch komplett mit USB-Stick für 20 Euro (inkl. lohnende Spende) verkauft wird.

Incognito ist ein integriertes System (d.h., man kriegt auch noch gleich ein kompaktes Linux mit), das von CD oder USB-Stick gestartet werden kann und das als Startpunkt für allerlei Aktivitäten in Richtung sicheren Umgang mit Rechnern dienen kann.

### In der Praxis II

Wenn ihr Tor fest in euer System installieren wollt, ist etwas mehr Arbeit nötig. Um euch eine Vorstellung zu geben, beschreiben wir hier das Vorgehen unter Debian oder verwandten Distributionen (z.B. Ubuntu).

Zunächst solltet ihr die Pakete tor und privoxy installieren. Wenn euer System das tor-Paket noch nicht kennt, solltet ihr es mit den Backports bekannt machen, im Paketmanager Synaptic etwa durch Auswahl von Einstellungen->Paketquellen, dann „Hinzufügen“, „Benutzerdefiniert“. Die „APT-Zeile“ ist „deb http://www.backports.org/debian etch-backports main“ (wenn ihr die Signaturen eurer Pakete überprüfen lasst -- und ihr solltet das tun --: die Kennung des Archiv-Schlüssels ist 16BA136C).

Nach der Installation ist Tor schon als Client konfiguriert und bedarf keiner weiterer Aufmerksamkeit. Privoxy hingegen muß angepaßt werden: öffnet als root oder Administrator die Datei /etc/privoxy/config und sucht eine Zeile, in der „chain Privoxy and Tor“ steht. Unter dieser ist eine Zeile, die mit „forward-socks4a“ anfängt -- löscht das # an deren Anfang, um sie zu aktivieren. Um Überraschungen vorzubeugen, wollt ihr so auch die drei Forward-Zeilen darunter aktivieren.

Dann sucht ihr die Zeilen die „logfile logfile“, „jarfile jarfile“ und „debug 1“ enthalten und deaktiviert sie, indem ihr als erstes Zeichen ein „#“ hineinschreibt. Dann den Rechner (oder einfach nur tor und privoxy) neu starten). Mehr Erklärungen, warum ihr das alles tun wollt, findet ihr unter http://tor.eff.org/docs/tor-doc-unix.html.

Als letztes muß die Firefox-Erweiterung Torbutton installiert werden. Diese bekommt ihr von https://addons.mozilla.org/de/firefox/addon/2275; leider ist sie nicht signiert. Nach dem installieren muß Firefox bzw. Iceweasel neu gestartet werden, danach habt ihr rechts unten in der Statusleiste einen Knopf „Tor Disabled“. Wenn ihr darauf klickt, wird Tor aktiviert, und die Beschriftung ändert sich in „Tor Enabled“. Nochmaliges Klicken deaktiviert Tor wieder. Wenn der Browser mit Tor Seiten nicht findet, ohne aber schon, wartet einfach eine runde Viertelstunde, bis Tor genug Informationen aus dem Netz gesammelt hat.

Wenn ihr weitere Dienste (also etwa IRC oder jabber) durch Tor ziehen wollt, hilft häufig das Paket socat -- aber wie gesagt, wenn ihr solche Dinge probieren wollt, solltet ihr wissen, was ihr tut. Mehr dazu findet ihr in der Tor-Dokumentation in /usr/share/doc/tor.

[1] http://www.heise.de/tp/r4/artikel/26/26483/1.html

[2] Von 2004 auf 2005 nahm die Zahl der überwachten Mailboxen um 342%, die der überwachten Internetanschlüsse um 110% zu.

[3] Das proprietäre Skype ist demgegenüber durchaus verschlüsselt, aber der Hersteller wartet nach eigenen Angaben bereits seit Jahren auf die ersten Abhörgesuche aus der BRD; dass die bisher ausgeblieben sind, dürfte damit zusammenhängen, dass die Verschlüsselung von Skype prima als Argument für Bundestrojaner-verwandte Angriffe herhalten soll.

[4] SSL („Secure Sockets Layer“) und TLS (Transport Layer Security) sind Verfahren zur Verschlüsselung von weitgehend beliebigen Datenströmen im Internet -- diese beiden Namen werden euch immer wieder begegnen, wenn ihr eure Verbindungen sichert]