Humanistische Union

Wie funktioniert der Anonymisierungsdienst Tor?

Welche Möglichkeiten des anonymen Verkehrs im Internet gibt es? Wie funktioniert das Onion-Routing und der Tor-Dienst?

Um gegenüber einer Webseite oder einer Suchmaschine seine Identität (IP-Adresse) zu verbergen, reicht im einfachsten Fall ein so genannter Proxy-Server ("Stellvertreter") aus. Ein Proxy-Server ist nichts anderes als ein in die Kommunikationskette zwischen Ihnen und dem Internet zwischengeschalteter Rechner. Seine Aufgabe ist es, Ihre Anfragen an den Rest des Internets weiterzugeben bzw. den Informationsrücklauf für Ihren Rechner entgegenzunehmen.

Die einfache Zwischenschaltung eines Proxy-Dienstes reicht aus, um seine Nutzerdaten vor einem Suchdienst wie Google oder einem anderen Webanbieter geheim zu halten. Sie reicht aber nicht aus, um sich vor einer staatlichen Überwachung seines Internetverkehrs abzusichern. Ermittlungsbehörden und Geheimdienste könnten einfach Ihren Internetzugang bei Ihrem Zugangsprovider überwachen (z.B. Telefon-, DSL- oder Breitbandanschluss) und über eine Protokollierung Ihres Datenverkehrs ausforschen, welche Anfragen Sie an den Proxy-Server senden. Dafür reicht eine gerichtliche Anordnung nach § 100a der Strafprozessordnung, und die ist hierzulande unschwer zu bekommen. Auch die Verschlüsselung der Kommunikationsinhalte hilft gegen die Ausforschung der Verbindungsdaten nur begrenzt: Die im Kopf der IP-Datenpakete verschickten Angaben über Sender und Empfänger einer Nachricht lassen sich nicht verschlüsseln. Schließlich könnte auch ein einzelner Proxy-Server leicht überwacht werden.

Vor diesem Hintergrund entstanden in den letzten Jahren zahlreiche Anonymisierungssysteme, die nicht mehr mit *einem* Proxy sondern einer ganzen Reihe von hintereinander geschalteten Proxy-Server arbeiten. Mit solchen Übertragungsketten kann die Anonymität der Kommunikation gewährleistet werden, solange mindestens eine der Zwischenstationen nicht kompromittiert wurde.

Der von der Humanistischen Union ausgewählte Dienst Tor ("The Onion Router"), weist neben einer großen Verbreitung gegenüber anderen Diensten einen weiteren Vorteil auf: Der über Tor erreichbare Grad an Anonymität basiert nicht auf dem Vertrauen in die Betreiber der einzelnen Tor-Server. Es gibt zahlreiche kommerzielle Anbieter von Proxy-Diensten, die einen anonymen Zugang zum Internet versprechen. Deren Anonymisierungsdienste setzen jedoch die Integrität des Betreibers voraus. Die Nutzerin/der Nutzer muss am Ende darauf vertrauen, dass der Betreiber keine (verdeckte) Kontrolle des Datenverkehrs vornimmt bzw. Dritten (kommerziellen oder staatlichen Kunden) einen Zugriff auf die durchgeleiteten Daten gewährt. Als Anbieter von Internetzugangsdiensten sind solche Betreiber jedoch zur Kooperation mit staatlichen Stellen verpflichtet: Wenn Ermittlungsbehörden Ihnen einen richterlichen Beschluss zur Abfrage von Verbindungsdaten (§ 100g StPO) vorlegen, müssen sie alle gespeicherten und künftigen Verbindungsdaten des entsprechenden Kunden vorlegen. Tor dagegen setzt auf ein großes Netzwerk vieler verschiedener Betreiber, deren Server international verteilt sind. Diese lassen sich - praktisch gesehen - nicht alle gleichzeitig überwachen. Die Gewährleistung der Anonymität im Tor-System steigt deshalb mit der Verfügbarkeit möglichst vieler Tor-Server an.

Der Tor-Dienst bietet - im Gegensatz zu einem einfachen Proxy-Server - daneben auch die Möglichkeit, andere Kommunikationsprotokolle (z.B. Chat, E-Mail) über das TOR-Netzwerk weiterzuleiten. Damit eröffnet er auch die Möglichkeit, durch Internetprovider oder Zensurbehörden gesperrte Kommunikationsdienste nutzen zu können.

Wie funktioniert's?

Beim Tor-Service wird der Datenaustausch zwischen Ihrem Computer (im Beispiel: "Alice") und dem Zielrechner (bspw. einer Webseite auf dem Rechner "Bob") über drei Tor-Rechner (sogenannte Nodes) umgeleitet. Das Tor-Programm auf Ihrem Rechner fragt dafür zunächst eine Liste der aktuell verfügbaren Tor-Server im Netz ab. Aus dieser Liste wählt es drei Rechner (1, 2, 3) als Zwischenstationen der nächsten Übertragung aus. Die Auswahl erfolgt nach dem Zufallsprinzip. Die Zusammensetzung der Übertragungskette (welche Rechner für die Stationen 1, 2 und 3 verwendet werden) ändert das Tor-Programm auf ihrem Rechner "Alice" nach jeweils etwa 10 Minuten, um die Integrität der Kette zu sichern.

Beim Aufbau der Verbindung zu einer Webseite ("Bob") handelt der Tor-Client auf Ihrem Rechner zunächst eine verschlüsselte Verbindung mit dem ersten der drei Zwischenstationen aus (1). Von dort wird die Verbindung zum zweiten Tor-Server (2) weiter geleitet usw.

Quelle: http://www.torproject.org/overview.html.de

Image not found or type unknown
Quelle: http://www.torproject.org/overview.html.de

Für den Informationsaustausch werden die Daten zwischen dem Absender und dem letzten Tor-Server verschlüsselt übertragen. Die übertragene Information (Inhaltsdaten) und die Verbindungsdaten (Absender/Empfänger) werden dabei dreimal hintereinander verschlüsselt: je eine Verschlüsselung ist für einen Abschnitt der Übertragung von Alice -> 1, von 1 -> 2 und 2 -> 3 zuständig. Die übertragene Information liegt deshalb wie unter den Schalen einer Zwiebel unter drei verschiedenen Verschlüsselungsschichten - daher der Name dieses Routingprinzips "Onion Routing". Diese mehrfache Verschlüsselung hat zur Folge, dass jeder Tor-Server bei der Datenübertragung deshalb nur seinen Vorgänger (von dem er die Daten empfängt) und seinen Nachfolger (wo er die Daten hinsenden soll) "sieht". Der letzte Tor-Server der Übertragungskette, der sogenannte Exit-Node (3), sendet die Daten dann unverschlüsselt zum Empfänger der Nachricht ("Bob"). Mit dem Datenpaket wird zugleich eine Kennung für die Rückübertragung versandt, die wieder nach dem gleichen Prinzip funktioniert: Der Webserver ("Bob") kann seine Rückantwort nur den letzten Punkt der Tor-Kette (3) senden, da er die anderen Stationen der Übertragungskette nicht kennt.

Zum Schluss noch eine Warnung:

Wie aus dieser - zugegebenermaßen sehr vereinfachten - Darstellung des Onion-Routing-Prinzips hervorgeht, verschlüsselt Tor die Informationen nur für einen Teil des Übertragungsweges. Die Übertragung zwischen dem letzten Glied des Tor-Netzwerkes (dem Exit-Node) und dem Zielrechner findet unverschlüsselt statt. Diese Verschlüsselung dient aber nur der Sicherstellung der Anonymität des Übertragungsweges. Tor ist kein Verschlüsselungsprogramm, dass die Inhalte der von Ihnen übertragenen

Informationen (etwa Eingaben in ein Webformular) verschlüsselt! Insofern ist Tor kein Allheilmittel, das Ihre Privatsphäre im Internet umfassend sichern kann. Neben der Nutzung eines Anonymisierungsdienstes sollten Sie sich deshalb immer auch darüber Gedanken machen, wie Sie die Inhalte Ihrer Kommunikation schützen wollen.

Weiterführende Informationen:

Übersicht zur Funktionsweise auf den Seiten des Tor-Projektes: http://www.torproject.org/overview.html.de

Marc Störing: Im Visier der Strafverfolger - Staatlicher Zugriff auf Anonymisierungsserver In: c't 24/2006, S. 208-210.

Wikipedia-Eintrag "Tor(Netzwerk)": http://de.wikipedia.org/wiki/Tor_%28Netzwerk%29
