

Humanistische Union

In fünf Minuten zu einem besseren Schutz Ihrer Privatsphäre im Internet

Anleitung zur Installation, Einrichtung und Nutzung des Tor-Dienstes auf einem Rechner mit Windows-Betriebssystem in nur drei Schritten

Einige Vorbemerkungen, bevor Sie auf Tor vertrauen:

- Die Nutzung eines Anonymisierungsdienstes ist - wenn auch ein wichtiger - so doch nur ein Schritt zur Sicherstellung ihrer Privatsphäre in der virtuellen Realität. Wer einen Anonymisierungsdienst benutzt, aber seine Passwörter über unverschlüsselte Verbindungen sendet, den kann auch Tor nicht vor einem Ausspähen seiner privaten Daten schützen. Tor ist kein Verschlüsselungsprogramm, d.h. an den sog. Exit-Nodes können alle übertragenen Informationen - wie bei jeder anderen unverschlüsselten Internetverbindung auch - von anderen mitgelesen werden. Die Nutzung eines Anonymisierungsdienstes ist kein Ersatz für die Verschlüsselung sensibler Daten!
- Wenn Ihnen die Sicherheit Ihrer persönlichen Privatsphäre im Internet am Herzen liegt, dann versuchen Sie bitte, die Funktionsweise von Tor zu verstehen und informieren Sie sich über bekannte Missbrauchsversuche und Lücken des Programms. Auf den Webseiten der Tor-Betreuer finden Sie dazu hilfreiche Informationen über potentielle Attacken, denen Sie als Tor-Nutzer ausgesetzt sein könnten und Warnungen über andere Missbrauchsversuche von Tor: <http://www.torproject.org/>.
- Tor arbeitet grundsätzlich mit allen üblichen Webbrowsern wie dem Internet Explorer, Mozilla Firefox, Opera oder Konqueror zusammen. Wir empfehlen jedoch die Nutzung des Mozilla Firefox, den Sie sich unter <http://www.mozilla-europe.org/de/products/firefox/> laden können. Dieser Browser ist eine Open-Source-Software, d.h. der Quellcode des Programms unterliegt einer öffentlichen Kontrolle der Programmierer (womit zugleich sichergestellt ist, dass keine versteckten Hintertüren für den Zugang Dritter eingebaut sind). Daneben eignet sich Firefox besonders für die Arbeit mit Tor, da er über eine praktische Erweiterung (Plugin) verfügt, mit dem der Start und die Nutzung des Anonymisierungsdienstes Tor bequem aus dem Browser heraus möglich ist.

So richten Sie den Tor-Dienst auf Ihrem Windows-Rechner ein:

1. Tor-Vidalia aus dem Netz laden und installieren

Für die Nutzung von Tor steht ein fertiges Programmpaket zur Verfügung, welches folgende Komponenten enthält:

Tor: ein Dienstprogramm für den Verbindungsaufbau zum Tor-Anonymisierungsnetzwerk

Vidalia: eine grafische Bedienoberfläche für den TOR-Dienst

Privoxy: ein lokaler Proxy-Filter, der als Schnittstelle für die Weiterleitung von Internetverbindungen dient

Zur Installation des Programms gehen Sie zu folgender Internetadresse und laden sich das für Ihr Betriebssystem passende Programmpaket: <http://www.torproject.org/download.html.de>

Download der TOR-Software

Image not found or type unknown

Nach dem Laden der Installationsdatei (im Bild: die Version für Windows) muss die Installationsroutine gestartet werden. Dazu starten Sie die soeben geladene Datei. Sie werden vom Installationsprogramm nach der gewünschten Sprache gefragt. Dann folgt eine Abfrage, welche Programmbestandteile Sie installieren wollen. Hier sollten Sie (sofern Sie Firefox als Browser benutzen) alle Optionen aktiviert lassen. Schließlich legen Sie noch den Speicherort fest, an dem das Programm installiert werden soll (der voreingestellte Wert unterhalb von C:Programme... kann beibehalten werden).

Wenn die Installation erfolgreich verlief und Sie den sofortigen Start der Dienste bejaht haben, öffnet sich automatisch die grafische Benutzeroberfläche von Vidalia. Sie zeigt einerseits an, ob der TOR-Client einsatzbereit ist. Außerdem lässt sich über den Schalter "Einstellungen" die individuelle Nutzung des Anonymisierungsdienstes anpassen:

TOR-Verwaltung mit Vidalia

Image not found or type unknown

Hinweis: Sie können die obige Anzeige von Vidalia übrigens abschalten, indem Sie die Option "Dieses Fenster beim Start anzeigen" deaktivieren und anschließend den Button "Verstecken" drücken.

Der Tor-Dienst ist ab jetzt auf Ihrem Rechner verfügbar. Vidalia zeigt Ihnen mit einem grünen Symbol im Tray-Menü von Windows an, wenn der Tor-Dienst einsatzbereit ist:

TOR-Statusanzeige

Image not found or type unknown

2. Ihren Browser für die Nutzung von Tor einrichten

Wenn Sie den Browser Firefox auf Ihrem Rechner bereits vor Tor installiert haben, können Sie jetzt schon den anonymen Internetzugang nutzen. Mit dem Tor-Vidalia-Paket wurde auch die Erweiterung Torbutton installiert, die ein bequemes Ein- und Ausschalten des Tor-Dienstes erlaubt. (Sollten Sie die Erweiterung später einmal aktualisieren müssen, finden Sie die Torbutton-Erweiterung auf dieser Webseite: <https://addons.mozilla.org/firefox/2275/>).

Mit installiertem Torbutton zeigt der Browser Firefox in seiner Fußleiste an, ob Ihre Verbindung zum Internet über das Tor-Netzwerk erfolgt oder nicht:

Schalter der TOR-Button-Erweiterung

Image not found or type unknown

Wenn Sie den Webzugriff über den Internetdienst aktivieren wollen, klicken Sie einfach auf den Schriftzug

"Tor Disabled" - damit wird die Umleitung aller Webanfragen über den laufenden Tor-Dienst auf Ihrem Rechner aktiviert. (Umgekehrt funktioniert auch die Abschaltung des Tor-Dienstes in Firefox.) Sofern Firefox den Tor-Dienst für seine Webverbindungen nutzt, wird dies entsprechend angezeigt:

Tor-Vidalia funktioniert aber auch mit allen anderen gebräuchlichen Webbrowsern. Sie müssen Ihrem Browser dann nur mitteilen, dass er für die Kommunikation mit dem Internet künftig ihren lokalen Tor-Proxy nutzen soll. Dies können Sie manuell über die Proxy-Einstellungen Ihres Browsers festlegen, indem Sie in Ihrem Browser (je nach verwandtem Modell) bitte folgende Menüs aufrufen:

- Opera: Extras -> Einstellungen -> Erweitert -> Netzwerk -> Proxy-Server
- Internet Explorer: Extras -> Internet Optionen -> Verbindungen -> Lan-Einstellungen
- Firefox unter Mac OS X: Firefox -> Einstellungen -> Allgemein -> Verbindungseinstellung
- Mozilla/Firefox unter Windows: Extras -> Optionen -> Allgemein -> Verbindungseinstellungen

In das erscheinende Eingabefeld für die Nutzung eines Proxy-Servers tragen Sie bitte folgende Daten ein (dies sind Standardwerte für einen lokal installierten Tor-Clients):

Proxy-Einstellungen für TOR

Image not found or type unknown

Damit haben Sie Ihrem Browser mitgeteilt, dass er Internetverbindungen grundsätzlich über das TOR-Netzwerk aufbauen soll. Wenn Sie dies wieder rückgängig machen wollen, wählen Sie an der gleichen Stelle die Nutzung eines Proxys ab ("direkte Verbindung zum Internet" aktivieren).

3. Der obligatorische Test

Um sicher zu gehen, dass der Tor-Service auf Ihrem Rechner zuverlässig funktioniert bzw. ob andere Sicherheitslücken des Internetbrowsers die Anonymität gefährden, empfiehlt sich ein Besuch dieser

Webseite mit aktiviertem Tor-Dienst: <https://torcheck.xenobite.eu/>

Nach dem Aufruf der Seite wird einem bereits mitgeteilt, ob der Aufruf der Webseite über das Tor-Netzwerk erfolgte oder nicht: Je nachdem erscheint eine entsprechende Meldung, ob man als Tor-Nutzer identifiziert wurde (grüne Schrift) oder nicht (rote Schrift). Mit dem Start-Button kann ein erweiterter Test des Browsers gestartet werden, um die Zulässigkeit von Cookies, die Nutzung von Javascript etc. zu prüfen.

Prüfung der TOR-Anonymisierung

Image not found or type unknown

Das war's auch schon. Viel Spaß beim anonymen Internetbesuch wünscht die Humanistische Union!

<https://www.humanistische-union.de/thema/in-fuenf-minuten-zu-einem-besseren-schutz-ihrer-privatsphaere-im-internet/>

Abgerufen am: 30.06.2022