Tor Browser

Computeria 31.03.2016
Fritz Glarner

Was bedeutet Tor?

Die Buchstaben Tor sind ein Akronym für **T**he **O**nion **R**outer, den "Zwiebel-Router".
Die Struktur von Tor nutzt verschiede Schichten der Verschlüsselung zum Schutz der Daten.
Das Prinzip von Tor ist weitgehend sicher. Die Software Tor-Browser kostet nichts und kommt fertig konfiguriert mit dem Internet-Browser Firefox in einer portablen, also sofort startfähigen Version:

Wofür nutzt man Tor?

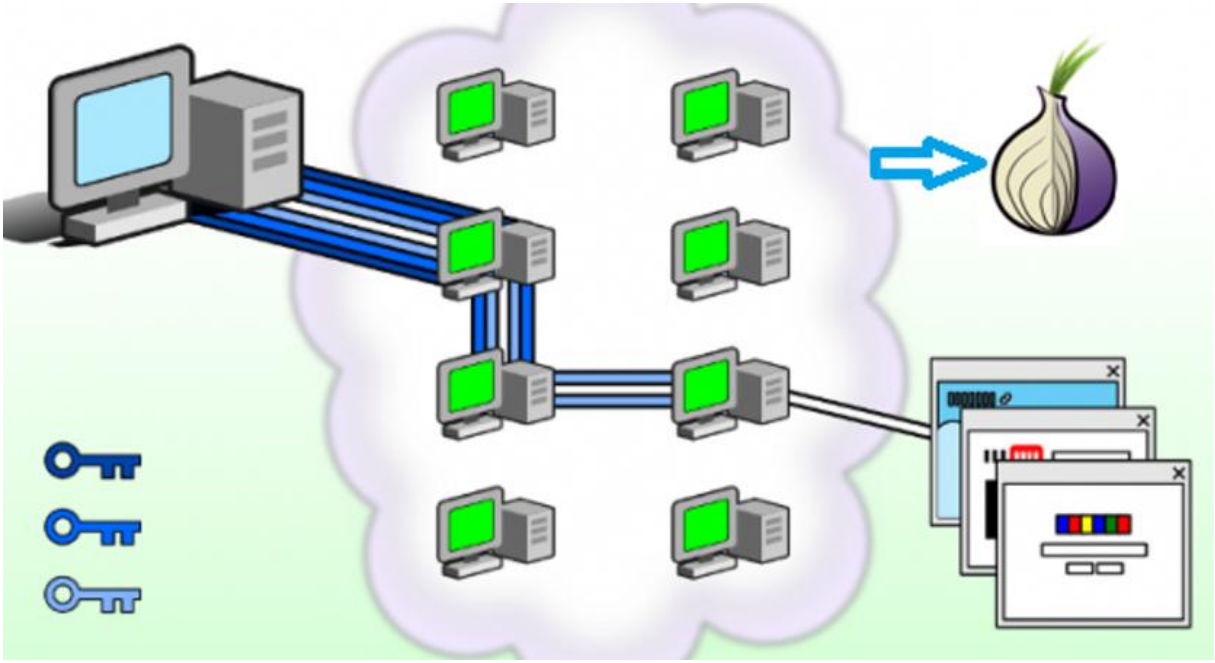
Tor schafft Anonymität im Internet. Der Dienst sorgt dafür, dass eine Aktion im Internet nicht mit der Person in Verbindung gebracht werden kann, die sie ausführt.

Diese Anonymität kann für die unterschiedlichsten Zwecke genutzt werden: z.B. für Personenschutz, aber auch für zwielichtige illegale Kommunikation und Geschäfte.

Dank der Anonymisierung können über den Tor-Browser auch für bestimmte Domänen gesperrte Server erreicht werden.

Wie funktioniert Tor?

Wenn man eine Internetseite aufruft, versucht der Rechner oder das Smartphone die Seite auf dem direktesten Weg zu erreichen. Das ist schlicht eine Frage der Effizienz und Geschwindigkeit.
Wie die namensgebende Zwiebel besteht das Tor-Netz aus mehreren Schichten:



Daten wandern unter verschlüsselten Tarnkappen durch das Netz. Am Ende des Weges erscheinen sie wieder in Klaransicht.

Verschiedene Router führen nach dem Zufallsprinzip durch das innere Tor-Netzwerk. Dazu braucht ein Verbindungsaufbau über das Tor-Netzwerk allerdings mehr Zeit als bei direktem Zugang.
Der Weg beginnt immer mit einem Eingangsknoten (Entry Node), mit dem sich der Tor-Client verbindet. Diese Verbindung zwischen Client-Computer und Entry Node ist verschlüsselt. Da der Entry Node die IP-Adresse des Clients kennt, wird nun der

Verkehr zum nächsten Tor-Knoten weitergeleitet. Dieser hat nur auf die IP-Adresse seines Vorgängers Zugriff. Somit ist die Quell-IP-Adresse des Clients nicht mehr bekannt, wenn der Ausgangsknoten (Exit Node) schließlich das Datenpaket über das Internet anfragt.
Am Ausgangknotenpunkt wird die Information wieder entschlüsselt und kommt beim Empfänger in Klaransicht an. Ab diesem Moment sind die Daten nicht mehr geschützt – es sei denn, dass die Daten dem Eingangsknoten bereits verschlüsselt übergeben werden (https).

Ist Tor sicher?

Bei richtiger Nutzung garantiert Tor Anonymität, aber keinen Schutz der Privatsphäre. Werden die Daten nach dem Verlassen des letzten Knotenpunkts abgefangen, kann man sie lesen. Eine weitere Schwachstelle von Tor sind Plug-ins. Flash beispielsweise verletzt die Anonymität von Tor, da es die Konfiguration der Datenverbindung ignoriert und seine eigenen Cookies speichert.