WAS IST DER TOR-BROWSER UND WAS KANN MAN DAMIT TUN?

Veröffentlicht am 23. Mai 2019 von Janina

Ob Internet Explorer, Mozilla Firefox, Google Chrome oder Opera – hinter diesen vier Begriffen steht eine Gemeinsamkeit: Es handelt sich um Internetbrowser und sie sind nicht allein. Um im Internet zu surfen, gibt es viele verschiedene Möglichkeiten. Zahlreiche Programme öffnen Dir die Tür zum Web. Hinter dem Namen Tor (Akronym für: The Onion Routing) verbirgt sich eine solche Software, mit der Du das Internet nutzen kannst. Was der Tor-Browser ist und was er kann, erfährst Du in unserem Überblick.

Ob Internet Explorer, Mozilla Firefox, Google Chrome oder Opera – hinter diesen vier Begriffen steht eine Gemeinsamkeit: Es handelt sich um Internetbrowser und sie sind nicht allein. Um im Internet zu surfen, gibt es viele verschiedene Möglichkeiten. Zahlreiche Programme öffnen Dir die Tür zum Web. Hinter dem Namen Tor (Akronym für: **The Onion Routing**) verbirgt sich eine solche Software, mit der Du das Internet nutzen kannst. Was der Tor-Browser ist und was er kann, erfährst Du in unserem Überblick.

WAS IST DER TOR-BROWSER?

Der Tor-Browser ist eine Software der amerikanischen Organisation **The Tor Project Inc.**
und wurde entwickelt, um die Kommunikation im Internet sicherer zu machen. Das Programm sollte beispielsweise zur Geheimhaltung von Kommunikation bei Spezialoperationen dienen.

Der Client
ermöglicht es, über das Tor-Netzwerk

anonym im Internet zu surfen.
Betritt man mit diesem Browser das World Wide Web, wird die IP-Adresse verschlüsselt, sodass man nahezu keine Spuren beim Surfen hinterlässt. Lediglich die Verbindung vom letzten Server (**Tor-Knoten**) ins Internet ist unverschlüsselt. Jeder Server kennt ausschließlich die IP-Adresse des vorigen Servers. Routen über die Tor-Knoten werden alle 10 Minuten zufällig geändert.

Das Tor-Browser-Paket kannst Du über gängige Download-Plattformen herunterladen. Es beinhaltet den Browser und nützliche Erweiterungen.
Mittlerweile funktioniert er auf allen Plattformen und ist auch als mobile App erhältlich. In den vergangenen Jahren erwies sich Tor als äußerst **nützlich für politisch verfolgte Menschen** oder User in Ländern, die von starker Zensur betroffen sind. Im Jahre 2011 erhielt das Projekt sogar einen Preis für **gesellschaftlichen Nutzen** und galt als äußerst wichtig für die Oppositionsbewegung in Ägypten und im Iran.

Anonym bist Du nur, bis Du Dich mit echten Daten auf Webseiten anmeldest – beispielsweise bei Facebook. Dennoch gibt es seit 2014 die Möglichkeit, sich über eine bestimmte Internetadresse über den Tor-Browser bei Facebook einzuloggen. Dadurch wird der Zugang zum sozialen Netzwerk auch für diejenigen ermöglicht, in deren Ländern **Facebook blockiert** wird.

Mit dem Tor-Browser kann man sowohl das „normale" Internet (Clear Web) besuchen als auch in das **Darknet** eintauchen, das ein Teil des sogenannten Deep Web ist.

DAS TOR-NETZWERK

Damit Du Dich anonym im Internet bewegen kannst, musst Du das **Tor-Netzwerk betreten**.
Dies funktioniert mittels **Onion-Routings**.

Nutzt Du das Netzwerk, wird jede Aktivität im Web auf verschiedenen Routen über mehrere Server geleitet. Dieses Prinzip ist so vielschichtig wie der Aufbau einer Zwiebel. Deine Identität wird durch die stets unterschiedliche Umleitung verschleiert.

Jeder Webinhalt wird über 3 Knoten geleitet. Der Verlauf der **Route ist zufällig**. Alle Verbindungen sind verschlüsselt, außer die vom dritten Knoten zum Ziel der Anfrage.

Die Tor-Server werden von unterschiedlichen Menschen, Organisationen und Behörden zur Verfügung gestellt. Im Prinzip kann jeder seinen Teil zum Netzwerk beitragen und seinen Server zu einem Tor-Server machen. Daher können auch **staatliche Behörden Tor-Punkte** besitzen und Deine Identität zurückverfolgen.

WIE FUNKTIONIERT DAS ANONYME SURFEN?

Um Dich **anonym im Internet** aufhalten zu können, reicht es nicht aus, Deine IP-Adresse durch das Tor-Netzwerk zu verschleiern. Das Tor-Browser-Paket enthält daher Erweiterungen, die Dich und Deine Privatsphäre weiter absichern. Mit **NoScript** werden automatisch alle Skripte deaktiviert, die ausgeführt werden, sobald Du eine Website betrittst. Werbung wird nicht geschaltet und es findet **kein Tracking** statt. Der Seitenbetreiber kann also nicht nachvollziehen, dass Du Dich auf seiner Seite bewegt hast.

Tipp: **NoScript** gibt es übrigens auch als Add-On für Standard Internetbrowser.

Eine weitere Erweiterung des Tor-Browsers sorgt dafür, dass ein Drittanbieter (Werbepartner) Deine Daten nicht auslesen kann. **HTTPS Everywhere** verschlüsselt alle Verbindungen mit einem HTTPS-Protokoll. Jede Website, die in der HTTPS Everywhere Atlas-Datenbank gelistet ist, wird dadurch mit einer sicheren Verbindung ausgeführt. Was eine HTTPS und SSL Verschlüsselung ist, erfährst Du in unserem Blogbeitrag „HTTPS und SSL Verschlüsselung – Was ist das und warum ist das für Webseiten unverzichtbar?“.

Mittels Geoblocking können Seitenbetreiber im Internet ihre Inhalte für regionale Usergruppen sperren. Der Tor-Browser umgeht dies durch die Anonymisierung der Nutzer. Dadurch kannst Du beispielsweise Videoinhalte auf **Netflix** und **YouTube** ansehen, die für Dein Land (noch) nicht freigegeben sind. Besonders wichtig ist diese Funktion jedoch für all diejenigen, die wegen starker Zensur in ihrem Land nur begrenzt auf das Internet zugreifen können.

DIE VORTEILE VON TOR

Ein großer Vorteil des Tor-Netzwerks und des Tor-Browsers sehen die Nutzer eindeutig in der Anonymisierung. Du kannst dort vergleichsweise sicher surfen, ohne verfolgt zu werden. Das ist jedenfalls dann der Fall, wenn Du den Browser richtig konfigurierst und verantwortungsvoll surfst. Mit dem Tor-Browser kannst Du nämlich auch das **Darknet betreten.** Weitere Informationen über das Darknet erfährst Du weiter unten.

DAS GESAMTE INTERNET ENTDECKEN

Ein weiterer Vorteil des Tor-Browsers ist, dass Du damit auf das sogenannte **Deep Web zugreifen** kannst. Dort erreichst Du all die Seiten, die von normalen Suchmaschinen (z.B.: Google) nicht gefunden werden können oder sollen. Hierzu gehören **Fachdatenbanken**, private Webseiten oder Seiten, die aus technischen Gründen nicht indexiert werden (können).

DIE NACHTEILE VON TOR

AM RANDE DER LEGALITÄT

Dadurch, dass Du mit dem Tor-Browser auf das **Darknet zugreifen** kannst, läufst Du schnell Gefahr, dich auf unsicheren oder sogar illegalen Pfaden zu bewegen. In Deutschland ist sowohl das Darknet

als auch der **Tor-Browser legal.** Das „dunkle Internet" wird jedoch häufig für illegale Aktivitäten genutzt. Der unerfahrene User kann hier möglicherweise nicht nachvollziehen, wann er die Grenzen der Legalität überschreitet.

Außerdem kann es passieren, dass die unverschlüsselte Verbindung Deiner Aktivität im Internet auf einen Server einer staatlichen Behörde führt. Dies kann bedeuten, dass beispielsweise der BND beginnt, Dich zu überwachen, auch wenn Du keine illegalen Absichten hast. Da die Routen über die Server stets zufällig sind, ist es vergleichsweise unwahrscheinlich, dass Dir das passiert. Möglich ist es aber!

SURFVERHALTEN ÄNDERN

Wenn Du das gesamte Internet (Clear und Deep Web) durchforsten willst, benötigst Du im Tor-Browser eine spezielle Suchmaschine. Google und Co. funktionieren zwar, liefern Dir aber nur Ergebnisse im Clear Web. Um auch die nicht indexierten Seiten zu finden, kannst Du **DuckDuckGo** verwenden. Die Suchmaschine ermöglicht anonymes Suchen auch im Clear Web und zeigt Dir über den Tor-Browser Ergebnisse im Deep Web an. Weitere Informationen über die Suchmaschine erhältst Du in unserem Blogbeitrag „DuckDuckGo erweitert seine Version auf Deutsch."

Das Surfen mit dem Tor-Browser gestaltet sich etwas umständlich und langsamer als Du es gewohnt bist. Verabschiede Dich von gut sortierten Suchergebnissen und einer kurzen Ladezeit von Webseiten. Dadurch, dass Deine Anfrage über drei Server geleitet wird, baut sich Dein Ziel vergleichsweise langsam auf. Zum Streamen von hochauflösenden Filmen ist Tor daher nur bedingt zu gebrauchen. Auch kann es sein, dass Du gewisse **Angebote nicht nutzen** kannst. Deine IP-Adresse ändert sich stetig, sodass Dein Account in Foren oder Portalen von den Bots der Seiten möglicherweise als „ungewöhnliche Aktivität" erfasst und gesperrt wird.

Angreifer können das Deep Web für die Verbreitung von Viren nutzen. Beim Surfen mit dem Tor-Browser solltest Du daher also besonders vorsichtig sein.

DAS DARKNET

Das Darknet (oder auch **Invisible Web**) ist ein versteckter Teil des Internets, in dem man nur über das Tor-Netzwerk surfen kann. Dadurch entzieht sich das Geschehen dort meist den Augen der „normalen" Internet-Nutzer.

Dank dem anonymen Surfen wird das Darknet unter anderem auch für **illegale Geschäfte** genutzt. Von Drogen- und Waffenhandel über Raubkopien und Identitätsdiebstahl gibt es einen großen Marktplatz für Kriminelle. Das ist aber noch nicht alles!

Das Darknet ist auch ein **wichtiger Ort für die Kommunikation** von politisch verfolgten Menschen, Unterdrückten, Journalisten oder Whistleblowern. Auch für Menschen, die unter Zensur in ihrem Land leiden, ist das Darknet eine gute Möglichkeit, Informationen zu erhalten und sich auszutauschen.

WOZU DIENT DER TOR-BROWSER – FAZIT

Der Tor-Browser bietet Dir eine gute Möglichkeit, Dich anonym im Internet zu bewegen. Der Zugriff auf das Tor-Netzwerk ist durch die Software vergleichsweise einfach und Du kannst nach Ausführen des Programms prinzipiell direkt mit dem Surfen beginnen.

Wenn Du nicht nur auf das Clear Web zugreifen möchtest, solltest Du vorsichtig vorgehen und Dich mit den Einstellungen des Browsers intensiv vertraut machen. Außerdem solltest Du Dir im Klaren sein, dass es im Darknet viele illegale Angebote gibt, auf die Du zugreifen könntest. Zwar ist die Nutzung von Tor und dem Darknet nicht verboten, doch letztlich gilt auch hier: „Unwissen schützt vor Strafe nicht". Du solltest das Programm daher **mit Bedacht einsetzen**.

Hast Du Fragen zum Tor-Browser oder

wie Seiten in Suchmaschinen indexiert und gefunden werden? Schreibe uns gerne einen Kommentar oder eine E-Mail.