

## **Tor - Übersicht**

Tor ist ein Netzwerk virtueller Tunnel, das es Menschen und Gruppen ermöglicht, den Schutz ihrer Privatsphäre und ihre Sicherheit im Internet zu verbessern. Es ermöglicht ausserdem Softwareentwicklern, neue Kommunikationswerkzeuge zu entwickeln, die die Privatsphäre bereits eingebaut haben. Tor stellt die Grundlage für eine Reihe von Anwendungen zur Verfügung, die es Organisationen und Individuen erlaubt, Informationen über öffentliche Netze auszutauschen, ohne ihre Privatsphäre zu gefährden.

Individuen können mittels Tor, andere Webseiten daran hindern, ihren Weg beim Surfen aufzuzeichnen. Weiterhin können sie es dazu verwenden, um sich zu anderen Seiten oder Instant-Messaging-Services zu verbinden, die von ihrem ISP gesperrt wurden. Die versteckten Services von Tor bieten die Möglichkeit, Webseiten und andere Dienste zu veröffentlichen, ohne den Standort der Seite preiszugeben. Menschen nutzen Tor auch, um sensitive Informationen zu kommunizieren: Chaträume und Webforen für Vergewaltigungsopfer und Überlebende von Misshandlungen oder auch Menschen mit Erkrankungen.

Journalisten nutzen Tor, um sicherer mit ihren Informanten bzw. Dissidenten zu kommunizieren. Nichtstaatliche Organisationen (NGOs) nutzen Tor, damit sich ihre Mitgliedern mit den Seiten verbinden zu können, ohne preiszugeben, dass sie für die Organisationen arbeiten.

Gruppen wie Indymedia empfehlen ihren Mitgliedern Tor für ihre Sicherheit und die Absicherung ihrer Privatsphäre. Gruppen wie die Electronic Frontier Foundation (EFF) unterstützen die Entwicklung von Tor, um bürgerliche Freiheitsrechte online aufrecht zu erhalten. Firmen untersuchen Tor daraufhin, ob mit ihm sichere Wettbewerbsanalysen möglich sind. Weiterhin überlegen sie, Tor zu verwenden, um neue und experimentelle Projekte zu testen, ohne ihren Namen mit diesen zu verbinden. Tor wird auch genutzt, um traditionelle VPNs zu ersetzen. Denn diese enthüllen sowohl Zeit wie auch Grössen der Kommunikation. So wird klar, an welchen Standorten ein Arbeiter zuletzt gearbeitet hat, welche Standorte besuchen häufig Angebote von Jobbörsen und welche Forschungseinheiten kommunizieren mit Patentanwälten.

Ein Zweig der US-Marine verwendet die Software, um Informationen aus offenen Quellen zu gewinnen (Open Source Intelligence). Eines ihrer Teams verwendete Tor, als es neulich im Nahen Osten eingesetzt war.

Die Vielfalt der Tor-Nutzer, ist ein Teil von dem, was Tor so sicher macht. Tor versteckt dich in der Menge der anderen Benutzer des Netzwerks. Damit ist deine Anonymität um so stärker geschützt, je grösser und differenzierter die Benutzerbasis von Tor ist.

## Warum wir Tor brauchen

Die Nutzung von Tor schützt gegen eine übliche Form der Internetüberwachung, die als Analyse des Netzverkehrs bekannt ist. Die Analyse kann dazu verwendet werden, Informationen abzuleiten, wer mit wem über ein öffentliches Netzwerk kommuniziert. Wenn jemand Quelle und Ziel deines Internetverkehrs kennt, kann er dein Verhalten und deine Vorlieben nachvollziehen. Das kann sich auf deinen Geldbeutel auswirken, indem z.B. eine E-Commerce-Seite ihre Preise vom Herkunftsland und deiner Firma abhängig macht. Es kann sogar deinen Arbeitsplatz und körperliche Unversehrtheit bedrohen, wenn öffentlich wird, wer du bist und wo du wohnst. Wenn du dich beispielsweise im Ausland auf Dienstreise befindest und dich mit dem Computer deines Arbeitgebers verbindest, kannst du ungewollt deine Nationalität und Arbeitgeber jedem gegenüber offenbaren, der das Netzwerk beobachtet, auch wenn die Verbindung verschlüsselt ist.

Wie funktioniert nun die Analyse des Netzverkehrs? Die Datenpakete haben zwei Teile: die Nutzlast, die die eigentlichen Daten trägt und der Kopf, wo verschiedene Informationen zum Routing zu finden sind. Auch wenn du die Nutzlast verschlüsselst, enthüllt diese Art der Analyse noch, was du tust und eventuell auch, was du sagst. Dies geschieht deshalb, da sie sich auf die Kopfdaten fokussiert, die die Quelle, Ziel, Grösse etc. enthalten.

Ein grundlegendes Problem für jemanden, der am Schutz seiner Privatsphäre interessiert ist, ist das der Empfänger an den Kopfdaten sehen kann, dass du die Daten versandt hast. So können es auch autorisierte Vermittler, wie ISPs, und manchmal auch unauthorisierte tun. Eine sehr einfache Form der Verkehrsanalyse ist es, irgendwo zwischen dem Sender und Empfänger zu sitzen und die Kopfdaten zu verfolgen.

Natürlich existieren auch mächtigere Formen der Verkehrsanalyse. Einige Angreifer spionieren in verschiedenen Teilen des Internets und nutzen fortgeschrittene statistische Methoden, um die Kommunikationsmuster von verschiedenen Organisationen und Menschen zu verfolgen. Verschlüsselung hilft nicht gegen diese Angreifer. Denn es verbirgt nur den Inhalt der Kommunikation und nicht die Kopfdaten.

Die Lösung: ein verteiltes, anonymes Netzwerk

Tor hilft dabei, das Risiko sowohl der einfachen als auch der ausgefeilten Verkehrsanalyse zu verringern, indem es deine Transaktion über verschiedene Stellen des Internet verteilt. Damit gibt es keinen einzelnen Punkt, an dem du mit der Kommunikation in Verbindung gebracht werden könntest. Die Idee lässt sich damit vergleichen, eine verwinkelte, schwer zu verfolgende Route zu benutzen, um einen Verfolger abzuschütteln - und ausserdem regelmässig Fussabdrücke zu verwischen. Anstatt einen direkten Weg vom Ausgangspunkt zum Ziel zu nehmen, verwenden Datenpakete im Tor-Netzwerk einen zufälligen Pfad über mehrere Server. Diese verwischen ihre Spuren und an keiner Stelle kann ein Beobachter sagen, woher ein Datenpaket kam und wohin es unterwegs ist.

Tor-Verbindung Schritt eins

Um einen privaten Netzwerkpfad mit Tor zu erzeugen, baut die Software des Benutzers oder Clients inkrementell eine Menge an verschlüsselten Verbindungen zu den Servern im Netzwerk auf. Dieser Kreis wird um jeweils einen Schritt erweitert und jeder Server entlang des Wegs weiss nur, von welchem Server er Daten bekam und zu welchem er sie weitergibt. Kein einzelner Server kennt jemals den gesamten Pfad, den ein Datenpaket genommen hat. Der Client handelt für jeden Schritt entlang des Pfads einen eigenen Satz von Verschlüsselungsschlüsseln aus und stellt damit sicher, dass kein Server die Verbindungen nachvollziehen kann, während sie bei ihm vorbeikommen.

Torverbindung Schritt zwei

Sobald ein Kanal eröffnet ist, können unterschiedliche Datenarten über ihn ausgetauscht und unterschiedliche Arten von Anwendungen können mit einem Tornetzwerk verwendet werden. Da jeder Server nur einen Schritt kennt, kann weder ein Lauscher noch ein kompromittierter Server Verkehrsanalyse verwenden, um die Quelle einer Kommunikation mit ihrem Ziel zu verbinden. Tor funktioniert nur über TCP-Streams und kann mit jeder Anwendung verwendet werden, die SOCKS unterstützt.

Aus Effizienzgründen verwendet die Tor-Software den selben Kanal für alle Verbindungen, die innerhalb von etwa zehn Minuten aufgebaut werden. Spätere Anforderungen erhalten einen neuen Kanal, damit niemand deine früheren Handlungen mit den neuen in Verbindung bringen kann.

Torverbindung Schritt drei

Versteckte Dienste

Tor ermöglicht es Benutzern, ihren Aufenthaltsort zu verbergen, während sie verschiedene Dienste wie z.B. Veröffentlichungen im Web oder Instant-Messaging verwenden. Durch die Verwendung von Tor "Rendezvouspunkten" können andere Tor-Benutzer auf versteckte Dienste zugreifen, ohne dabei die Netzwerkidentität des Anderen zu kennen. Die Funktionalität dieser versteckten Dienste kann es Torbenutzern ermöglichen, eine Webseite einzurichten, auf der Menschen ohne Angst vor Zensur Material veröffentlichen können. Niemand wäre in der Lage festzustellen, wer die Webseite anbietet und niemand, der die Webseite anbietet wüsste, wer auf ihr was veröffentlicht. Auf den anderen Seiten kannst du mehr darüber erfahren, wie man einen versteckten Dienst konfiguriert und wie das Protokoll funktioniert.

Anonym bleiben

Tor kann nicht alle Anonymitätsprobleme lösen. Es konzentriert sich darauf, den Transport von Daten zu schützen. Du musst protokollspezifische Software verwenden, wenn du nicht möchtest, dass die von dir besuchten Seiten, Informationen über deine Identität erhalten. Beispielsweise kannst du einen Webproxy wie Privoxy verwenden, um Cookies und die Herausgabe von Informationen über den Browsertyp zu blockieren.

Sei clever, wenn du deine Anonymität schützen möchtest. Gib weder deinen Namen noch andere Informationen über dich in Formularen an. Sei dir der Tatsache bewusst, dass Tor, wie jedes Anonymisierungsnetzwerk, das schnell genug für das Webbrowsing ist, nicht gegen Ende-zu-Ende-Timing-Angriffe schützt: wenn der Angreifer den von deinem Computer

ausgehenden Verkehr und auch den am gewählten Ziel ankommenden Verkehr beobachten kann, kann er statistische Analysen verwenden um zu erkennen, dass beide Teil desselben Endes sind.

## **Die Zukunft von Tor**

Es ist eine andauernde Herausforderung, ein dauerhaftes Anonymisierungsnetzwerk im Internet anzubieten. Wir wollen Software, die den Bedürfnissen der Benutzer entspricht. Wir wollen auch das Netzwerk auf eine Art in Betrieb halten, die so viele Benutzer wie möglich verträgt. Sicherheit und Benutzerfreundlichkeit dürfen keine Gegensätze sein: Während Tors Benutzerfreundlichkeit steigt, wird es mehr Benutzer anziehen, die die Zahl der möglichen Quellen und Ziele für jede Kommunikation erhöhen und damit die Sicherheit für jeden verbessern. Wir machen Fortschritte, aber wir benötigen deine Hilfe. Bitte überlege, ob du einen Server installieren oder ob du freiwillig als Entwickler einen Beitrag leisten möchtest.

Andauernde Trends in Gesetzgebung, Politik und Technologie bedrohen Anonymität wie niemals zuvor und sie untergraben unsere Möglichkeiten, frei online zu sprechen und zu lesen. Diese Trends untergraben auch die nationale Sicherheit und kritische Infrastruktur, indem sie die Kommunikation zwischen Individuen, Organisationen, Firmen und Regierungen angreifbarer für Spionage machen. Jeder neue Torbenutzer und -server liefert zusätzliche Verschiedenheit und erhöht damit Tors Fähigkeit, die Kontrolle über deine Sicherheit und Privatsphäre wieder in deine Hände zu legen.