Maßnahmen: Tor-Netzwerk

Table of Contents

1. Übersicht

In der Präsentation werden folgende Themen behandelt:

- Allgemeines/Einführung
- Technische Erklärung
  - Grafiken
- Vor und Nachteile
- Für wen ist das Tor-Netzwerk gedacht?
- Hosting → Werde teil von Tor
- Beispiele für Tor-Unternehmen
- Gefahren von Tor
- Live-Demo
- Wie hoste ich etwas auf dem Tor-Netzwerk?

2. Allgemeine Einführung

Das Synonym TOR steht hierbei für "The Onion Router". Das Projekt TOR wurde von dem U.S Naval Research Laboratory ins Leben gerufen, um eine sichere Firmeninterne Kommunikationsmöglichkeit gewährleisten zu können.

Folgende Entwickler haben die führende Rolle bei der Entwicklung des Tor-Netzwerkes übernommen:

- Roger Dingledine
- Nick Matheweson
- Paul Syverson

Paul Syverson und Nick Matheweson spielten bei der Forschung eine große Rolle. Die Hauptsächliche Entwicklung übernahmen aber dafür alle drei erwähnten Programmierer.

Die erwähnte Organisation hinter TOR ist heutzutage keine Forschungsgruppe mehr, sondern eine gemeinnützige Organisation, welche sich auf Schutz von Privatsphäre und auf das Recht der Anonymität im Internet spezialisiert hat.

Um das Tor-Netzwerk für die Allgemeinheit benutzbarer zu machen, wurde der Tor-Browser entwickelt, welcher primär den Datenverkehr durch das Tor-Netzwerk regelt, leitet und steuert. Dieser Browser basiert auf dem herkömmlichen und sehr weit verbreiteten Firefox Browser mit zusätzlichen Privatsphäre & Sicherheitsfunktionen.

Da das Tor-Projekt zur Gänze ein Open-Source Projekt darstellt war demnach nicht nur das Team hinter dem U.S Naval Research Laboratory für die Entwicklung des Projektes zuständig, sondern auch zahlreiche weitere über den Globus verteilte Entwickler, welche zum Projekt Tor "contributet" haben.

Kombiniert man nun TOR mit Tails-OS laufend auf CUBES OS stehen einem alle Türen zur Sicherheit "geschlossen :)". Durch diese Kombination ist man vor Malware, Spionage, Tracking, etc.. voll und ganz geschützt.

3. Wie funktioniert Tor?

3.1. Standard Way-To-Go:

- Jeder Rechner im Netzwerk, auch der Client, ist durch eine eindeutige IP-Adresse identifizierbar. Dies ist der erste Schritt in der Kommunikation und sollte sicherheitsbewusst gehandhabt werden.
- Die Eingabe einer Webadresse startet den Prozess, die dazugehörige IP-Adresse zu ermitteln.
- Der Domain Name System (DNS)-Server(großes Wörterbuch zu IP’s und Domain-Namen) übersetzt die Webadresse in eine IP-Adresse. Dieser schickt die IP-Adresse zurück an den Client, also dem Nutzer.
- Die Verbindung zum Webserver wird hergestellt. Hierbei könnten unsichere Protokolle oder fehlende Verschlüsselung potenzielle Angriffspunkte darstellen.
- Der Webserver sendet die angeforderten Daten in Form eines Responses zurück. Unverschlüsselte Übertragungen könnten dazu führen, dass sensible Informationen abgefangen werden können.

(Frage an das Publikum) Wer sieht hierbei ein Problem?

Das Problem ist die fehlende Anonymität, da der kontaktierte Youtube-Webserver, die Public-IP-Adresse vom Client kennt. Somit kann der Client jederzeit zurückverfolgt werden und es ist einfach nachvollziehbar, welcher Internetprovider hinter der Public-IP steckt. Dadurch kann man, zwar durch Umwege, aber jedoch relativ einfach die Adresse des Endnutzers herausfinden und diesem bei bedarf auf unzählige Arten und Weisen schaden.

3.2. Wie funktioniert TOR?:

Das Ziel des Tor-Netzwerks besteht darin, die Anonymität der Benutzer zu wahren, sodass niemand wissen soll, wer zu einer bestimmten IP-Adresse gehört. Dies wird durch die Einbeziehung verschiedener Knotenpunkte in das Netzwerk erreicht, wobei jeder Knotenpunkt eine spezifische Funktion hat.

- Knotenpunkte im Tor-Netzwerk:
  - Eintrittspunkt (Entry Node):
    - Funktion: Der Eintrittspunkt ist der erste Knotenpunkt, den der Datenverkehr betritt. Verschlüsselung: Die Verbindung zum Eintrittspunkt erfolgt verschlüsselt, um die IP-Adresse des Benutzers zu schützen.
  - Weiterleitungspunkt (Middle-Relay):
    - Funktion: Der Weiterleitungspunkt leitet den verschlüsselten Datenverkehr vom Eintrittspunkt zum Austrittspunkt weiter. Verschlüsselung: Die Kommunikation bleibt weiterhin verschlüsselt, um die Anonymität zu bewahren.
  - Austrittspunkt (Exit Node):
    - Funktion: Der Austrittspunkt ist der letzte Knotenpunkt, an dem die Daten entschlüsselt und zum ursprünglichen Ziel geschickt werden. Verschlüsselung: Die Datenverbindung wird am Austrittspunkt entschlüsselt.

3.3. Der TOR-BROWSER:

Der Tor-Browser stellt eine effektive Möglichkeit dar, das Tor-Netzwerk zu nutzen und die Privatsphäre der Benutzer zu schützen. Es ist essenziell, den Browser von der offiziellen Webseite des Tor-Projekts https://www.torproject.org/ herunterzuladen, um sicherzustellen, dass keine Veränderungen am Code vorgenommen wurden, die die Sicherheit beeinträchtigen könnten.

Um eine höhere Anonymität zu gewährleisten, sollten Benutzer bestimmte Gewohnheiten ablegen, die potenziell ihre Identität preisgeben könnten. Dies beinhaltet das Vermeiden von personalisierten Logins und das Zurücklassen von persönlichen Informationen.

Die Einstellung der Standardsprache des Tor-Browsers auf Englisch trägt zur Anonymität bei, da viele Webseiten die Browsersprache kennen und eine gebräuchliche Sprache auf den Benutzer hinweisen könnte. Um noch weiter in der Masse zu verschwinden, empfiehlt es sich, gängige Verhaltensweisen zu vermeiden und beispielsweise Youtube-Videos mit doppelter Geschwindigkeit anzusehen.

Die Nutzung des Tor-Browsers sollte nicht auf eine bestimmte Personengruppe beschränkt werden, um individuelle Nutzermuster zu verschleiern. Es ist wichtig zu beachten, dass der Tor-Browser

effektiv verhindert, dass Webseiten die tatsächliche IP-Adresse des Benutzers sehen. Stattdessen wird die IP-Adresse des Exit-Nodes angezeigt, was zur Anonymität beiträgt.

Um eine umfassende Privatsphäre und Sicherheit zu gewährleisten, ist es entscheidend, nicht nur den Tor-Browser zu verwenden, sondern auch die generellen Online-Gewohnheiten zu überdenken und bewusster zu gestalten. Indem diese Praktiken berücksichtigt werden, können Benutzer die Vorteile des Tor-Netzwerks optimal nutzen und ihre digitale Identität schützen.

4. Vor & Nachteile

- Vorteile des Tor-Netzwerks:
  - Anonymität: Das Tor-Netzwerk bietet eine hohe Anonymität, da die Daten durch mehrere Knotenpunkte geleitet werden, wodurch es schwierig wird, die wahre Identität eines Benutzers zu ermitteln.
  - Zensurumgehung: Tor ermöglicht es Benutzern, Zensur zu umgehen, da der Datenverkehr durch verschiedene Länder geleitet wird, wodurch geografische Beschränkungen umgangen werden können.
  - Privatsphäre: Durch die Verschlüsselung des Datenverkehrs wird die Privatsphäre der Benutzer geschützt, da Dritte Schwierigkeiten haben, den Inhalt der Kommunikation zu überwachen.
  - Dezentralisiertes Netzwerk: Tor ist dezentralisiert und wird von einer Vielzahl von Freiwilligen betrieben, was es schwieriger macht, das Netzwerk zu kontrollieren oder zu zensieren.
- Nachteile des Tor-Netzwerks:
  - Langsamere Geschwindigkeiten: Aufgrund der Umleitung des Datenverkehrs durch mehrere Server kann die Geschwindigkeit im Tor-Netzwerk im Vergleich zu direkten Verbindungen langsamer sein.
  - Nicht für alle Anwendungen geeignet: Aufgrund der langsamen Geschwindigkeiten und der Art der Anonymisierung ist Tor nicht für alle Arten von Internetaktivitäten geeignet, insbesondere für datenintensive Anwendungen.
  - Vertrauen in Exit-Nodes: Benutzer müssen darauf vertrauen, dass die Betreiber der Exit-Nodes die Daten nicht abfangen oder manipulieren, da die Entschlüsselung des Datenverkehrs am Exit-Node erfolgt.
  - Missbrauch durch Kriminelle: Aufgrund der Anonymität im Tor-Netzwerk kann es auch von kriminellen Akteuren genutzt werden, um illegale Aktivitäten zu verschleiern.
  - Eingeschränkter Schutz vor Endpunktangriffen: Das Tor-Netzwerk bietet keinen vollständigen Schutz vor Endpunktangriffen. Wenn das Endgerät eines Benutzers unsicher ist, kann die Anonymität des Tor-Netzwerks beeinträchtigt werden.

Zusammenfassend bietet das Tor-Netzwerk einen effektiven Schutz der Privatsphäre und Anonymität, aber es ist wichtig, die spezifischen Anforderungen und Einschränkungen zu beachten, um es angemessen zu nutzen.

5. Für wen ist Tor gedacht?

Für folgende Personengruppen ist das Tor-Netzwerk und somit auch der Tor-Browser gedacht

- Journalisten und Aktivisten: Personen, die in Ländern mit eingeschränkter Meinungsfreiheit leben oder arbeiten, nutzen Tor, um ihre Online-Aktivitäten zu schützen und Zensur zu umgehen.
- Whistleblower: Menschen, die sensible Informationen veröffentlichen möchten, können Tor verwenden, um ihre Identität zu schützen und Repressalien zu vermeiden.
- Nutzer in Ländern mit Überwachung: In Ländern, in denen die Internetaktivitäten stark überwacht werden, bietet Tor eine Möglichkeit, sich vor staatlicher Überwachung zu schützen.
- Bürgerrechtler: Personen, die sich für Bürgerrechte und Datenschutz engagieren, nutzen Tor, um ihre Online-Aktivitäten vor unerwünschter Überwachung zu schützen.
- Menschen in autoritären Regimen: Individuen, die in Ländern mit autoritären Regimen leben, verwenden Tor, um ihre digitale Freiheit zu bewahren und Zensur zu umgehen.
- Privatnutzer mit Datenschutzbedenken: Personen, die ihre Privatsphäre im Internet schützen möchten, verwenden Tor, um ihre IP-Adresse zu verbergen und ihre Online-Aktivitäten zu verschleiern.
- Forscher und Sicherheitsexperten: Personen, die Sicherheitsforschung betreiben oder Schwachstellen im Netzwerk identifizieren möchten, nutzen Tor, um anonyme und sichere Tests durchzuführen.

Es ist wichtig zu beachten, dass Tor nicht nur für Personen in kritischen Situationen relevant ist, sondern auch für jeden, der seine Online-Privatsphäre schützen möchte. Die Vielseitigkeit von Tor macht es zu einem Werkzeug für verschiedene Benutzergruppen, die ein Interesse an der Wahrung ihrer Anonymität haben.

6. Werde Teil vom Tor-Netzwerk

- Exit-Node:
  - Sicherheitsrisiken: Als unsicher und potenziell illegal geltend, da der Exit-Node den unverschlüsselten Datenverkehr entschlüsselt und somit den Datenverkehr des Benutzers sichtbar macht. Hosting-Verantwortlichkeiten: Personen, die als Exit-Node fungieren, müssen sich bewusst sein, dass sie für den Datenverkehr verantwortlich sind, der ihren Node passiert. Dies könnte rechtliche Konsequenzen haben, wenn illegale Aktivitäten darüber durchgeführt werden. Middle-Node:
  - "Hosting-Starter Pack": Ein sichererer Knotenpunkt, der den verschlüsselten Datenverkehr durch das Tor-Netzwerk weiterleitet. Geeignet für Einsteiger im Hosting-Bereich.
- Entry-Node:
  - Upgrades nach Hosting-Länge: Eintrittspunkt mit der Möglichkeit zum Upgrade erst nach einer bestimmten Hosting-Dauer. Dies dient als Schutzmechanismus und erfordert ein gewisses Maß an Erfahrung. Geräte für das Hosting:
  - Empfohlene Spezifikationen: Ein Hosting-Setup mit einer Empfehlung von 40 MB/s

Übertragungsgeschwindigkeit und 512 MB bis 1 GB RAM. Vielfältige Optionen: Von alten Android-Smartphones über Raspberry Pi Pico bis hin zu Cloud-Providern wie Linode, OC und DigitalOcean. Config:

  - Konfigurationsempfehlungen gemäß den Richtlinien des Tor-Projekts: Link zur Konfigurationsanleitung. Sorgfältige Einhaltung dieser Richtlinien ist entscheidend, um einen sicheren und effizienten Node-Betrieb zu gewährleisten. Phasen:

- **Tag 3-8):** Set-Up Brennweitenmessung:
  - Initiierung des Hosting-Prozesses, während Messungen und Anpassungen vorgenommen werden, um die Leistung des Nodes zu optimieren.
- **Tag 8-64):** Upgrade auf Entry-Node:
  - Nach einer erfolgreichen Hosting-Phase kann der Middle-Node aufgerüstet werden, um die Funktionen eines Entry-Nodes zu übernehmen.
- **Tag 68+):** TOR-"Veteran":
  - Erreichen des Status eines TOR-"Veterans" markiert einen fortgeschrittenen Status im Tor-Netzwerk, kommt jedoch ohne funktionalen Nutzen aus. Die beschriebenen Phasen zeigen, wie ein individueller Knotenpunkt im Tor-Netzwerk aufgebaut werden kann, von einfachen Hosting-Praktiken bis zum erfahrenen Status als TOR-"Veteran".
- Exit-Node:
  - Sicherheitsrisiken: Als unsicher und potenziell illegal geltend, da der Exit-Node den unverschlüsselten Datenverkehr entschlüsselt und somit den Datenverkehr des Benutzers sichtbar macht. Hosting-Verantwortlichkeiten: Personen, die als Exit-Node fungieren, müssen sich bewusst sein, dass sie für den Datenverkehr verantwortlich sind, der ihren Node passiert. Dies könnte rechtliche Konsequenzen haben, wenn illegale Aktivitäten darüber durchgeführt werden. Middle-Node:
  - "Hosting-Starter Pack": Ein sichererer Knotenpunkt, der den verschlüsselten Datenverkehr durch das Tor-Netzwerk weiterleitet. Geeignet für Einsteiger im Hosting-Bereich.
- Entry-Node:
  - Upgrades nach Hosting-Länge: Eintrittspunkt mit der Möglichkeit zum Upgrade erst nach einer bestimmten Hosting-Dauer. Dies dient als Schutzmechanismus und erfordert ein gewisses Maß an Erfahrung. Geräte für das Hosting:
  - Empfohlene Spezifikationen: Ein Hosting-Setup mit einer Empfehlung von 40 MB/s Übertragungsgeschwindigkeit und 512 MB bis 1 GB RAM. Vielfältige Optionen: Von alten Android-Smartphones über Raspberry Pi Pico bis hin zu Cloud-Providern wie Linode, OC und DigitalOcean. Config:
  - Konfigurationsempfehlungen gemäß den Richtlinien des Tor-Projekts: Link zur Konfigurationsanleitung. Sorgfältige Einhaltung dieser Richtlinien ist entscheidend, um einen sicheren und effizienten Node-Betrieb zu gewährleisten. Phasen:
- **Tag 3-8):** Set-Up Brennweitenmessung:
  - Initiierung des Hosting-Prozesses, während Messungen und Anpassungen vorgenommen werden, um die Leistung des Nodes zu optimieren.
- **Tag 8-64):** Upgrade auf Entry-Node:

    - Nach einer erfolgreichen Hosting-Phase kann der Middle-Node aufgerüstet werden, um die Funktionen eines Entry-Nodes zu übernehmen.

- **Tag 68+):** TOR-"Veteran":
    - Erreichen des Status eines TOR-"Veterans" markiert einen fortgeschrittenen Status im Tor-Netzwerk, kommt jedoch ohne funktionalen Nutzen aus. Die beschriebenen Phasen zeigen, wie ein individueller Knotenpunkt im Tor-Netzwerk aufgebaut werden kann, von einfachen Hosting-Praktiken bis zum erfahrenen Status als TOR-"Veteran".

7. Darknet-Shops

7.1. Silk-Road

Silk Road, 2011 von Ross Ulbricht gegründet, war ein Darknet-Marktplatz. Nutzer konnten dort Verkaufsanzeigen erstellen und illegale Produkte wie Drogen kaufen. Die Plattform ermöglichte anonyme Transaktionen über Kryptowährungen.

Im Jahr 2013 wurde die Silk Road-Domain beschlagnahmt, und Ross Ulbricht wurde vom FBI festgenommen. Diese Maßnahmen markierten das Ende des illegalen Darknet-Marktplatzes und demonstrierten die Bemühungen der Strafverfolgungsbehörden gegen illegale Online-Aktivitäten.

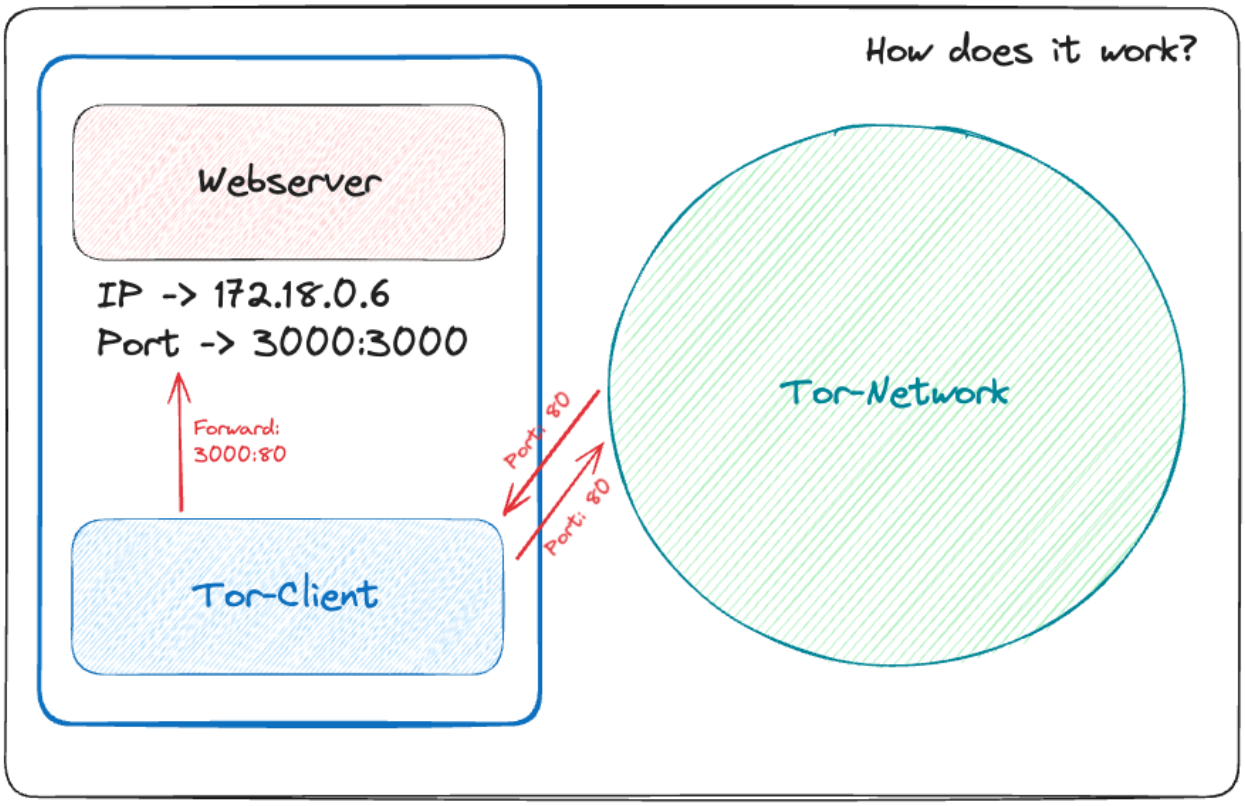
7.2. Alphabay

AlphaBay, gegründet 2014 von Alexandre Cazes, war ein großer Darknet-Marktplatz für illegale Waren wie Drogen und Hacking-Tools. Die Plattform ermöglichte anonyme Transaktionen mit Kryptowährungen und bot Sicherheitsfunktionen wie das ESCROW-Bezahlsystem.

Im Juli 2017 wurde AlphaBay von internationalen Strafverfolgungsbehörden geschlossen. Alexandre Cazes, der Gründer, wurde in Thailand festgenommen und beging Selbstmord in seiner Gefängniszelle. Die Schließung markierte einen Sieg im Kampf gegen illegale Darknet-Aktivitäten, ähnlich wie bei Silk Road, und löste Diskussionen über die Regulierung von Online-Marktplätzen aus.

8. How to Sell Drugs Online (fast) → Docker-Demo

- Link: https://github.com/Stevan06v/nextjs-hidden-service/



8.1. QUELLEN

- Erfahrung durch Nutzung & eigene Projektumsetzungen
- https://www.youtube.com/watch?v=fsfoqdqyykI
- https://www.youtube.com/watch?v=KlgjEGd-Gmk&t=123s
- https://de.wikipedia.org/wiki/Tor_(Netzwerk)
- https://community.torproject.org/relay/relays-requirements/
- https://github.com/Stevan06v/nextjs-hidden-service
- https://www.youtube.com/watch?v=QSxUG7kBjPQ
- https://de.wikipedia.org/wiki/Silk_Road
- https://de.wikipedia.org/wiki/AlphaBay

1,883 Wörter