Christoph Döpmann, Matthias Marx, Hannes Federrath, Florian Tschorsch

Tor Relays an Universitäten

Erfahrungen und Abwägungen

Während Universitäten mit ihrer Infrastruktur und Kompetenz ideale Bedingungen für den Betrieb von Tor-Knoten bieten, ist ihr Anteil am Tor-Netz erstaunlich gering. Wir berichten über unsere Erfahrungen beim Betrieb von zwei Exit-Knoten an Universitäten und geben Empfehlungen für deren Betrieb.

Christoph Döpmann

ist wissenschaftlicher Mitarbeiter am Fachgebiet für Distributed Security Infrastructures der Technischen Universität Berlin

E-Mail: christoph.doepmann@tu-berlin.de

Matthias Marx

ist wissenschaftlicher Mitarbeiter am Arbeitsbereich Sicherheit in Verteilten Systemen an der Universität Hamburg.

E-Mail: marx@informatik.uni-hamburg.de

Prof. Dr. Hannes Federrath

ist Leiter des Arbeitsbereichs Sicherheit in Verteilten Systemen an der Universität Hamburg und Präsident der Gesellschaft für Informatik e.V.

E-Mail: federrath@informatik.uni-hamburg.de

Prof. Dr. Florian Tschorsch

ist Professor für das Fachgebiet Distributed Security Infrastructures an der Technischen Universität Berlin und dem Einstein Center Digital Future (ECDF)[1]

E-Mail: florian.tschorsch@tu-berlin.de

1 Einleitung

Mit mehr als zwei Millionen Nutzerinnen und Nutzern pro Tag [1] stellt das Tor-Netz [2] das derzeit populärste Anonymisierungsnetz dar. Die Infrastruktur, insbesondere die zahlreichen Relay-Server, werden von Freiwilligen betrieben und laufen häufig auf deren privaten oder angemieteten Servern. Relays stellen damit das Rückgrat des Tor-Netzes dar und sind maßgeblich für die Sicherheit und Performanz verantwortlich.

In diesem Beitrag berichten wir von unseren Erfahrungen mit dem Betrieb von Tor-Exit-Knoten an Universitäten. Während der Forschung im Bereich der Anonymisierung im Allgemeinen und am Tor-Netz im Speziellen sind wir auf eine Vielzahl an Bedenken gestoßen, die beim Betrieb eines Tor-Knotens aufkommen. Mit den Argumenten und Gegenargumenten werden wir uns in diesem Beitrag auseinandersetzen, wollen damit die Diskussion anregen und zugleich motivieren, eigene Erfahrungen beim Betrieb eines Tor-Knotens zu sammeln.

Universitäten stellen hervorragende Umgebungen für den Betrieb von Tor-Knoten dar. Sie besitzen für gewöhnlich eine gute Netzanbindung, die notwendige technische Expertise ist vorhanden und zudem sind sie geschützte Umgebungen für freie Forschung und ermöglichen somit selbstverständlich die Forschung an und mit Anonymisierungsnetzen. Obwohl die Sicherheitsforschung auch und gerade in Deutschland einen hohen Stellenwert hat, werden derzeit nur an zwei Universitäten Tor-Exit-Knoten betrieben.

Im Folgenden erklären wir kurz, wie das Tor-Netz funktioniert. Anschließend argumentieren wir für einen Betrieb von Tor-Knoten an Universitäten und quantifizieren den Anteil am Tor-Netz, den Universitäten global und insbesondere in Deutschland über die vergangenen zehn Jahre zu dessen Betrieb beigetragen haben. Außerdem berichten wir auf technischer und organisatorischer Ebene über unsere Erfahrungen beim Aufbau und Betrieb von Tor-Exit-Knoten, wie wir sie an zwei deutschen Universitäten gemacht haben. Wir nutzen diese Erkenntnisse schließlich, um typische Bedenken zu diskutieren und entwickeln daraus eine Checkliste, um Universitäten dabei zu helfen, Tor-Knoten zu betreiben. Unsere Arbeit zeigt, dass zwar Herausforderungen bestehen, aber auch, dass diese vollständig handhabbar sind.

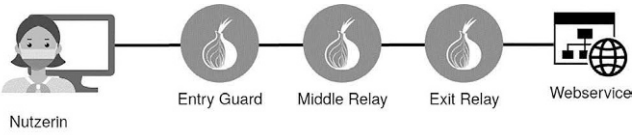
1 Foto: ECDF/PR/Noak

In der Vergangenheit haben andere Studien Erfahrungen aus dem Betrieb von Anonymisierungsdiensten präsentiert [3, 4, 5], doch diese Beiträge liegen schon viele Jahre zurück, sodass eine Einschätzung aus heutiger Sicht geboten scheint.

2 Tor Relays

Im Kern besteht das Tor-Netz [2] aus einer Menge sogenannter Tor-Knoten (auch Relays oder Weiterleitungsknoten genannt). Ihre Funktion besteht darin, gemäß dem Onion-Routing-Protokoll [6] Daten weiterzuleiten und damit durch das Netz zu transportieren. Typischerweise werden drei Tor-Knoten von einem Tor Client, der im Vertrauensbereich der jeweiligen Nutzerinnen und Nutzer betrieben wird, zu einem sogenannten Circuit (Kanal) zusammengeschlossen. Jeder Knoten verwaltet viele Circuits von unterschiedlichen Tor Clients gleichzeitig.

Abbildung 1 | Drei Relays werden zu einem Circuit kombiniert. Jedes Relay kennt nur seinen direkten Vorgänger und Nachfolger.



Je nachdem, an welcher Position im Circuit sich ein Relay befindet, kommen ihm unterschiedliche Rollen zu, die in Abbildung 1 dargestellt sind. Zwei dieser Rollen kommt dabei eine besondere Bedeutung zu: Das erste Relay ist das einzige, das eine direkte Verbindung vom Tor Client entgegennimmt und wird daher auch Entry Guard (Eingangsknoten) genannt. Insbesondere die besonders vertrauenswürdige Funktion eines Guard wird dabei nur an Relays vergeben, die dafür einige Bedingungen, im Hinblick auf eine hohe Verfügbarkeit und Bandbreite, erfüllen müssen. Betreiberinnen und Betreiber solcher Knoten können zwar die IP-Adressen von Clients beobachten, nicht jedoch, mit welchen Zielservern sich diese verbinden. Auf der anderen Seite stellen Exit Relays (Ausgangsknoten) das Ende eines Circuits dar und sind von besonderer Bedeutung, da sie letztendlich den anonymen Zugang ins Internet realisieren. Insbesondere stellen Exit Relays im Auftrag der Tor Clients TCP-Verbindungen zu Zielservern im Internet her. Betreiberinnen und Betreiber solcher Knoten können also beobachten, wohin sich Tor Clients verbinden, kennen jedoch die IP-Adressen der dahinter stehenden Nutzerinnen und Nutzer nicht. Aufgrund ihrer Funktion sind Exit Relays gegenüber externen Servern im Internet sichtbar und können in deren Log-Dateien auftauchen. Im Falle einer missbräuchlichen Nutzung von Tor, beispielsweise um eine Internetseite anzugreifen, scheint dann das Exit Relay der Angreifer zu sein. Da dies für Betreiberinnen und Betreiber von Exit Relays mit Komplikationen verbunden sein könnte, übernehmen Relays diese Funktion standardmäßig nicht. Stattdessen muss die Exit-Funktionalität explizit aktiviert werden. In der Vergangenheit führte dies dazu, dass die von Exit Relays zur Verfügung gestellte Bandbreite eine knappe Ressource war [7]. Betreiberinnen und Betreiber von Exit Relays können zudem den Zugriff auf bestimmte IP-Adressen und Ports einschränken. Diese Regeln werden als Exit Policy bezeichnet. Exit Relays spielen noch aus einem anderen Grund eine besondere Rolle: Sie sehen den Datenverkehr der Clients im Klartext. Um Integrität und Vertraulichkeit zu garantieren, muss die Kommunikation zusätzlich durch geeignete Verschlüsselungs- und Authentifizierungsmechanismen wie TLS gesichert sein.

Über den anonymen Internetzugriff hinaus bietet Tor die Möglichkeit, mittels sogenannter Onion Services Daten vollständig anonym Tor-intern zur Verfügung zu stellen. Somit können auch Diensteanbieter (und nicht nur die Tor Clients) anonym bleiben. Dabei verlassen die Daten an keiner Stelle das Tor-Netz.

3 Tor an Universitäten

Das Tor-Netz besteht derzeit (Stand Januar 2021 [1]) aus insgesamt ca. 6.800 Relays (davon knapp 1.400 Exits), die von Freiwilligen betrieben werden. Rund um Tor existiert ein Ökosystem, das unter anderem die Tor-Nutzerinnen und -Nutzer und die Forschungsgemeinschaft umfasst. Obwohl umfassend an und mit Tor geforscht wird, stellen Universitäten nur einen Bruchteil der Relays und Bandbreite. In diesem Abschnitt quantifizieren wir diesen Sachverhalt. Aufgrund seiner Bedeutung für das Tor-Netz konzentrieren wir uns zunächst auf Deutschland. Weiterhin diskutieren wir, warum die Situation in Deutschland ein re-

Abbildung 2 | Anzahl der Relays im Deutschen Forschungsnetz (AS 680) und in Deutschland über die letzten zehn Jahre.

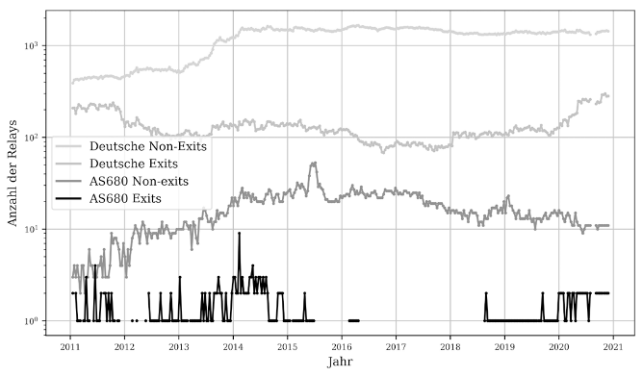
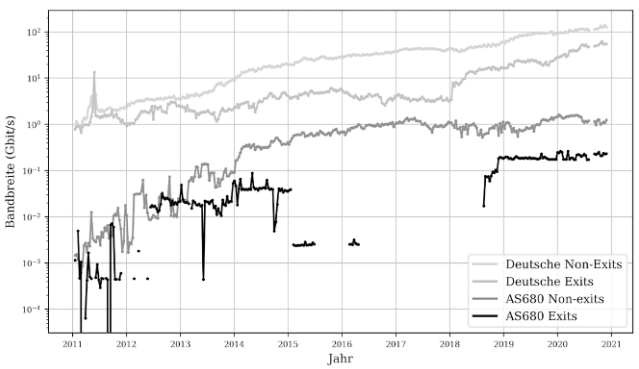


Abbildung 3 | Bandbreite (Gbit/s) der Relays im Deutschen Forschungsnetz (AS 680) und in Deutschland über die letzten zehn Jahre



präsentatives Beispiel für das gesamte Tor-Netz darstellt. 3.1 Situation in Deutschland

Wir konzentrieren uns aus mehreren Gründen auf das Beispiel Deutschland: Erstens werden in Deutschland mit Abstand die meisten Tor-Knoten betrieben [1]. Zweitens haben Datenschutz und Forschungsfreiheit als Grundrechte in Deutschland einen hohen Stellenwert. Man würde daher erwarten, dass eine große Anzahl von Exit Relays auch an deutschen Universitäten betrieben wird. Drittens ist der Internetzugang deutscher Universitäten homogener als in anderen Ländern, da die überwiegende Mehrheit der Universitäten mit dem Deutsches Forschungsnetz (DFN, AS 680) denselben öffentlichen gemeinnützigen Internet-Provider nutzt. Aus diesem Grund kann zuverlässig ermittelt werden, ob Relays zu einer Hochschule gehören oder nicht.

Um die Situation von Relays an deutschen Universitäten beurteilen zu können, konzentrieren wir uns zunächst auf Exit Relays und untersuchen die folgenden Größen:

(1) Die gesamte Exit-Bandbreite des Tor-Netzes,
(2) die Exit-Bandbreite von Relays in Deutschland und
(3) die Exit-Bandbreite von Relays im DFN (AS 680).

Wir betrachten nicht nur die heutige Situation sondern auch die historische Entwicklung. Wir haben hierzu historische Daten zu Relays verarbeitet und nutzen die MaxMind-Datenbank[2] für IP-Geolokalisierung und AS-Informationen.

Deutsche Knoten stellen etwa 30% der Exit-Bandbreite von Tor. Deutsche Universitäten machen nur 0,2% der weltweiten Exit-Bandbreite aus. Innerhalb des DFN werden 13 Relays betrieben, darunter zwei Exit Relays. Im Vergleich dazu gibt es Vereine und Einzelpersonen, die zwischen 1% und 20% der Exit-Bandbreite beitragen [8].

Ein Blick auf die historischen Daten zeigt, dass dies in der Vergangenheit ähnlich war. Abbildungen 2 und 3 zeigen die Anzahl sowie die Bandbreite der Relays für Exits und Non-Exits in Deutschland in den vergangenen zehn Jahren. Seit 2014 ist die Anzahl der Non-Exits in Deutschland mit rund 1.400 relativ konstant. Die Anzahl der Exit Relays in Deutschland schwankte stärker und erreichte 2011 (244) und 2020 (261) ihre Höhepunkte. 2016 sank die Zahl auf 71 Relays. Die bereitgestellte Bandbreite weist einen konstanten Aufwärtstrend auf.

Der Anteil der Relays an deutschen Universitäten war sowohl hinsichtlich der Bandbreite als auch in Bezug auf die Anzahl der Knoten immer klein. An den Universitäten wurden höchstens 73 Non-Exits betrieben (2015). Seitdem ist die Zahl auf 13 Relays gefallen. Bei Exits sind die Zahlen noch deutlicher. In den letzten zehn Jahren gab es an deutschen Universitäten maximal fünf Exits, meist ein, zwei oder über lange Zeiträume auch gar keine. Seit August 2018 gibt es mindestens ein Exit Relay (betrieben an der TU Berlin). Seit Januar 2019 gibt es mit Unterbrechungen ein zweites Exit Relay (betrieben an der Universität Hamburg). Wir stellen fest, dass die Universitäten in Deutschland nur wenig zum Tor-Netz beitragen.

Wir glauben, dass Universitäten ein geeigneter Ort sind, um Tor Relays zu betreiben. Dies liegt nicht nur daran, dass Tor Gegenstand von Forschung und Lehre ist. Universitäten können auch als Orte der akademischen Freiheit (Freiheit der Forschung, Lehre und des Studiums) dazu beitragen, dass Überwachung verhindert wird und Meinungen frei geäußert werden können. Universitäten sind auch aus technischen Gründen gut geeignet. Sie verfügen häufig über einen eigenen IP-Adressbereich, der zur Vermeidung von Konflikten bei Missbrauchsbeschwerden hilfreich ist. Darüber hinaus verfügen sie normalerweise über eine gute und zuverlässige Anbindung ans Internet. Daher wäre es wünschenswert, dass in Zukunft mehr (Exit) Relays an Universitäten betrieben werden.

3.2 Globale Situation

Während unser Hauptaugenmerk auf Deutschland liegt widmen wir uns in diesem Abschnitt der globalen Situation. Wir zeigen, dass die nationale Situation repräsentativ für das gesamte Tor-Netz scheint. Da nicht jedes Land über ein ausgewiesenes Forschungsnetz für Universitäten verfügt, was die automatisierte Einordnung erschwert, konnte die Messung für das globale Netz nicht direkt reproduziert werden. Wir nutzen stattdessen einen Dienstleister[3], der IP-Adressen bestimmten Nutzergruppen zuordnet (z. B. „Unternehmen“, „Hosting“ oder „Bildung“). Wir können keine bestimmte Genauigkeit garantieren. Die Ergebnisse erscheinen jedoch plausibel. Zudem haben wir manuell überprüft, dass unsere Ergebnisse keine falsch positiven Zuordnungen enthalten.

Wir haben alle Tor Relays anhand einer aktuellen Momentaufnahme des Tor-Netzes (am 8. Dezember 2020) klassifiziert und festgestellt, dass Bildungseinrichtungen weltweit etwa 0,5% der Exit-Bandbreite beitragen (10 von 1.381 Exit Relays). Dieser Eindruck stimmt weitestgehend mit der Situation in Deutschland überein und zeigt, dass die Universitäten mehr zum Tor-Netz beitragen sollten.

4 Erfahrungen mit Exit-Knoten

Im Folgenden fassen wir unsere Erfahrungen beim Betrieb von Exit Relays an unseren Universitäten zusammen. Nach heutigem Stand handelt es sich hierbei um die beiden einzigen Exits an deutschen Universitäten.

4.1 Fallstudie: Technische Universität Berlin

Seit August 2018 betreibt unsere Forschungsgruppe „Distributed Security Infrastructures“ an der TU Berlin einen Exit-Knoten für das Tor-Netz.[4] Diese Entscheidung trafen wir, um das Tor-Netz zu stärken, aber auch um unsere Forschung zu unterstützen, beispielsweise um ein besseres Verständnis der Dynamik des Datenverkehrs im Tor-Netz zu erlangen. Darüber hinaus bieten wir Lehrveranstaltungen zum Thema anonyme Internetkommunikation an und das Exit Relay erlaubt es uns, praktische Erfahrungen in die Lehre einfließen zu lassen. Nachdem wir zuvor an anderen Universitäten schon Relays betrieben hatten, war dies unser erstes Exit Relay. Die technische Umsetzung an der TU Berlin gestaltet sich wie folgt: Die Universität betreibt vor Ort ein Rechenzentrum, welches sowohl ein Housing von physischen Servern als auch die Bereitstellung virtueller Maschinen anbietet. Wir entschieden uns für eine virtuelle Maschine mit zwei CPU-Kernen, 2 GB RAM und einer Internetanbindung von 1 Gbit/s. Die Internetverbindung des Rechenzentrums wird über das DFN

2 https://dev.maxmind.com/geoip/geoip2/geolite2/

3 https://ipinfo.io/

4 Relay-Fingerabdruck E91905CFEB230B1BEA6B0309816F9EE9C1A1A83A

realisiert. Wir sind uns etwaiger Nachteile der Benutzung virtueller Maschinen bewusst, beispielsweise der Beeinträchtigung anderer virtueller Maschinen. Im Allgemeinen wird empfohlen, Tor-Knoten auf physischen Maschinen zu betreiben, um sie von der restlichen Infrastruktur zu trennen. Aufgrund finanzieller Rahmenbedingungen ergab sich diese Option für unsere Forschungsgruppe jedoch zunächst nicht. Dank einer Hardware-Spende, die vom Artikel10 e.V. vermittelt wurde, werden wir jedoch in naher Zukunft dazu in der Lage sein, einen eigenen physischen Server zu nutzen. Das Housing stimmen wir gerade mit dem Rechenzentrum ab.

Bei der Konfiguration der Tor-Software legten wir großen Wert darauf, gültige und funktionierende Kontaktinformationen zu hinterlegen. Beispielsweise wird auf Port 80 eine Informationsseite angezeigt, die Tor und unsere Forschung erläutert, zusammen mit den Kontaktdetails. Damit beabsichtigen wir, Dritte, welche von unserem Relay stammenden Datenverkehr beobachten, offen und direkt zu informieren. Weiterhin wird auf diesem Weg für die Tor-Community ersichtlich, dass unser Knoten auch für Forschungszwecke genutzt wird. Als Exit-Policy verwenden wir einen der empfohlenen Regelsätze, der einen Kompromiss zwischen Nutzbarkeit und Missbrauchsrisiko darstellt [9]. Zudem entschieden wir uns dazu, zunächst mit einer stark beschränkten Bandbreite zu beginnen, um Erfahrungen zu sammeln. Später erhöhten wir die Bandbreite auf 160 Mbit/s. Unseren Beobachtungen zufolge nutzen wir damit die verfügbaren Systemressourcen (insbesondere CPU und RAM) vollständig aus. Die konstante Inanspruchnahme hoher Datenraten stellte für die TU Berlin kein Problem dar, im Gegensatz zu den anderen Universitäten, an denen wir in der Vergangenheit Relays betrieben hatten.

Wir ziehen von der Einrichtung und dem Betrieb des Knotens ein sehr positives Fazit. Wir wurden nur mit sehr wenigen Vorfällen konfrontiert, die unsere Aufmerksamkeit erforderten. Einmal nahmen das DFN und die Betreiber des Rechenzentrums der TU Berlin Kontakt zu uns auf – angesichts eines möglicherweise missbräuchlichen Verhaltens unseres Exit Relays, der Schadsoftware zu verteilen schien. Wir erklärten die Situation und der Betrieb konnte normal weitergehen. Als eine ähnliche Meldung erneut aufkam, baten wir im Sinne einer dauerhaften Lösung darum, derartige Warnungen zu unserem Server an uns zu delegieren. Dies erwies sich als möglich, da das DFN solche Warnungen als Dienstleistung gegenüber seinen Kunden (in diesem Fall die TU Berlin) auffasst und die Bearbeitung solcher Fälle nicht streng einfordert. Ein weiteres Mal hatten wir direkten Kontakt mit einer australischen Firma, die von unserem Server ausgehende Brute-Force-Angriffe beobachtete. Auch hier war die Situation schnell geklärt. Weitere Vorfälle wurden uns nicht bekannt. Die angegebene Kontakt-E-Mail-Adresse empfängt große Mengen an Spam, doch da wir ein separates E-Mail-Konto verwenden, stellt dies kein Problem dar. Der Wartungsaufwand ist nahezu vernachlässigbar. Letztlich besteht er hauptsächlich darin, regelmäßig Software-Updates durchzuführen, was auch automatisiert werden könnte.

4.2 Fallstudie: Universität Hamburg

Unser Arbeitsbereich „Sicherheit in verteilten Systemen“ an der Universität Hamburg betreibt seit Januar 2019 ein Tor Relay.[5] Nachdem uns im September 2019 ein eigener kleiner IP-Adressbereich zugeteilt wurde, wird dieses als Exit Relay betrieben. Mit seinem eigenen IP-Adressbereich ist der Arbeitsbereich auch für die Bearbeitung von Missbrauchsmeldungen (Abuse-Meldungen) verantwortlich. Damit mehrere Beschäftigte die Meldungen bearbeiten können, wurde ein Mailverteiler aufgesetzt. Außerdem wurde eine einfache Antwort als Template vorbereitet.

Während der Vorbereitung des Betriebs wurden die Empfehlungen des Tor-Projekts für den Betrieb von (Exit) Relays berücksichtigt [12,13]. Die Richtlinien zur Nutzung der Universitätsinfrastruktur waren aus anderen Projekten bekannt.

Tor läuft auf einem dedizierten Server, der über das DFN mit dem Internet verbunden ist. Die Software Ansible[6] wird zur Verwaltung des Relays verwendet.

Ungefähr einmal pro Tag erhält die Arbeitsgruppe automatisierte Warnungen vom DFN-CERT, da Malware auf dem Server ausgeführt zu werden scheint. Tatsächlich nutzt Malware das Exit Relay lediglich, um über Tor eine Verbindung zu Command and Control Servern herzustellen. Da diese Warnungen keine Antwort erfordern und die Ursache bekannt ist, ergreifen wir keine weiteren Maßnahmen.

Um die Anzahl der Missbrauchsmeldungen gering zu halten, ist die Exit Policy normalerweise auf die Ports 80 und 443 beschränkt. Während verschiedener Experimente wurden jedoch vorübergehend auch andere Ports zugelassen. Experimente sind auch der Grund für verschiedene Ausfallzeiten. Es fällt auf, dass die Freigabe von Port 22 (SSH) zu einer signifikanten Zunahme von Missbrauchsmeldungen geführt hat.

Die meisten der erhaltenen Abuse-Meldungen wurden automatisch generiert (z. B. von Fail2Ban) und beziehen sich auf Brute-Force-Angriffe. Einige Meldungen enthielten keine gültige Antwortadresse. In einigen wurde darum gebeten, künftigen Missbrauch zu verhindern. Die betroffenen IP-Adressen wurden dann über die Exit Policy ausgeschlossen.

In einem Fall im Jahr 2020 wandte sich die Polizei mit einem Ermittlungsersuchen an uns. Die Polizei wurde darüber informiert, dass unter der angefragten IP-Adresse ein Exit Relay betrieben werde und eine Zuordnung von IP-Adressen zu einzelnen Nutzerinnen und Nutzer technisch nicht möglich sei. Außerdem wurden laufende, das Tor Relay betreffende Forschungsvorhaben kurz erläutert.

5 Diskussion

Bei dem Betrieb eines Tor-Knoten sollten einige Punkte beachtet und abgewogen werden. Im Folgenden diskutieren wir, basierend auf unseren Erfahrungen, typische Bedenken und Argumente.

5.1 Mögliche Bedenken

Tor-Knoten können erhebliche Mengen an Daten weiterleiten. Betreiberinnen und Betreiber können die genaue Menge jedoch gut steuern. Dazu bietet die Tor-Software Konfigurationsoptionen an, mit denen sich obere Schranken für die durchschnittliche sowie die Burst-Datenrate festlegen lassen. Damit erhalten Relay-Betreiberinnen und -Betreiber die Möglichkeit, die zur Verfügung gestellte Bandbreite genau zu steuern.

5 Relay-Fingerabdruck 83C50784528AD3823CB7E7DF4B34B92A42CC7639

6 https://www.ansible.com

Eine Herausforderung besteht an Universitäten unter Umständen darin, die ordnungsgemäße Erreichbarkeit des Dienstes zu gewährleisten. Insbesondere müssen etwaige Firewalls entsprechend konfiguriert werden. In solchen unternehmensartigen Umgebungen können strenge Firewall-Regeln und mangelnde Bereitschaft, diese anzupassen, dem Betrieb eines Tor-Knotens entgegenstehen. Diesbezüglich gibt die Tor-Software den Betreiberinnen und Betreibern jedoch einige Flexibilität: Die TCP Ports, unter denen das Relay erreichbar sein soll, können frei gewählt werden und lassen sich damit an die Netzwerkumgebung anpassen.

Um den Tor-Datenverkehr von anderem Datenverkehr klar trennen zu können, ist es empfehlenswert, den Tor-Knoten auf einem separaten Server mit separater IP-Adresse zu betreiben. Dies beugt ggf. rechtlichen Streitigkeiten im Fall von Beschwerden über eine missbräuchliche Nutzung vor. Ein separates IP-Subnetz kann auch von Vorteil sein, da manche Anbieter von E-Mail- und anderen Diensten IP-Adressen von Tor-Knoten sperren [10].

Der Konfigurationsaufwand zur Bereitstellung eines Tor-Knotens kann insgesamt als niedrig eingeschätzt werden, auch aufgrund der vom Tor-Projekt bereitgestellten Beispiel-Ressourcen.

Eine wichtige Entscheidung beim Einrichten eines Tor-Knotens besteht darin, ob dieser auch als Exit-Knoten agieren soll. In dieser Betriebsart wird die IP-Adresse von Exit-Knoten von öffentlichen Internetdiensten, auf die darüber zugegriffen wird, als Quelladresse wahrgenommen. Eine etwaige missbräuchliche Nutzung würde zunächst der Relay-Betreiberin bzw. dem –Betreiber zugeschrieben werden. Die praktische Erfahrung hat gezeigt, dass Anonymität auch illegale Aktivitäten anzieht. Betreiberinnen und Betreiber von Exit-Knoten sollten daher darauf vorbereitet sein, mögliche Beschwerden zu dem vom Exit-Knoten weitergeleiteten Datenverkehr zu bearbeiten. Die beiden Fälle der von uns betriebenen Exit Relays haben jedoch gezeigt, dass die Häufigkeit solcher Beschwerden nach heutigem Stand recht gering ist. Dabei spielt die Wahl einer geeigneten Exit Policy eine wichtige Rolle, insbesondere der Ausschluss von SSH-Verbindungen.

Wir gehen davon aus, dass verschiedene Faktoren dazu beigetragen haben, das Risiko für Betreiberinnen und Betreiber von Exit-Knoten deutlich zu senken. So wird beispielsweise die Funktionsweise von Tor inzwischen deutlich besser von offiziellen Behörden wahrgenommen. Zudem haben schärfere Datenschutzgesetze wie die DSGVO dazu geführt, dass beispielsweise WHOIS-Daten mehr geschützt werden und nicht mehr anlasslos öffentlich einsehbar sind. Dadurch werden vollständig automatisierte Beschwerden gegen die Betreiberinnen und Betreiber von Tor-Knoten erschwert.

5.2 Gewonnene Erkenntnisse

Wir nutzen unsere Erfahrungen vom Aufbau und Betrieb von Exit-Knoten an Universitäten, um eine Checkliste zu erstellen, die dabei helfen soll, dieses Vorhaben auch an anderen Universitäten umzusetzen. Die Liste basiert dabei auf mehreren öffentlichen Quellen [11, 12, 13], doch wir nutzen unsere Erfahrungen, um deren Punkte geeignet zu filtern, zusammenzufassen und zu ergänzen. Die Liste geht davon aus, dass die Betreiberinnen und Betreiber bereits ausreichende (technische) Kenntnis des Tor-Netzes besitzen, um Tor-Knoten aufzusetzen und zu konfigurieren. Damit ist die Checkliste als eine Sammlung von Aktivitäten zu verstehen, die im Vorfeld bewusst erwogen werden sollten.

- **Offen kommunizieren**: Kontaktieren Sie Verantwortliche an der Universität und erläutern Sie das Vorhaben. Stellen Sie auch an anderer Stelle funktionierende Kontaktdaten zur Verfügung (WHOIS etc.), um etwaige Fragen und Beschwerden zu beantworten.
- **Freiheiten nutzen**: Gerade in Deutschland ist die Freiheit der Forschung ein hohes Gut, auf das Sie sich berufen können. Mit dem Betrieb eines Tor Relays kann Ihre Universität zudem Ihren Einsatz für eine freie Gesellschaft unterstreichen.
- **Zusammenarbeiten**: Suchen Sie sich Unterstützer an der Universität, aber auch in der Tor Community. Letztere ermöglicht Ihnen z. B. durch Mailing-Listen oder Meetups, auf dem aktuellen Stand über Tor zu bleiben.
- **Wartung organisieren**: Der Wartungsaufwand eines Tor Relays ist gering. Zeigen Sie jedoch, dass Sie auf Unwägbarkeiten vorbereitet sind, indem Sie bereits im Voraus Zuständigkeiten und ggf. Abläufe festlegen, wie beispielsweise Beschwerden bearbeitet werden.
- **Tor vermitteln**: Greifen Sie Tor in der Lehre auf. Nicht nur profitieren Studierende und Mitarbeitende von einem tieferen technischen Verständnis von Tor. Der Betrieb eines Tor Relays, beispielsweise im Rahmen eines Seminars, kann auch eine besondere, praktische Perspektive auf Privatsphäre im Internet vermitteln.

Insgesamt zielen die genannten Punkte darauf ab, den Betrieb eines Exit-Knotens zu ermöglichen, denn davon kann das Tor-Netz am meisten profitieren. Es besteht jedoch immer die Option, zunächst mit einem Non-Exit zu beginnen und die Exit-Funktionalität später zu aktivieren, wenn die Betreiberinnen und Betreiber genügend Vertrauen in den Aufbau gewonnen haben. Unsere Erfahrung ist, dass Verantwortlichkeiten vorab geklärt werden müssen und dass es wichtig ist, mit allen beteiligten Personen in Kontakt zu treten und sich mit typischen technischen und nichttechnischen Argumenten gegen den Betrieb von (Exit)-Knoten auseinanderzusetzen. Zudem eröffnet der Betrieb eines Tor-Knotens neue Möglichkeiten in der Forschung und Lehre. Mögliche Themengebiete umfassen dabei Anonymisierungstechniken im Allgemeinen oder Verbesserungen für Tor im Speziellen, Zensur im Internet sowie juristische und ethische Erwägungen beim Betrieb von Anonymisierungsnetzen.

6 Fazit

Unsere Ergebnisse zeigen, dass ein stärkeres Engagement von Universitäten bei der Unterstützung des Tor-Netzes, durch den Betrieb von Tor-Knoten, nicht nur sinnvoll und vielleicht sogar notwendig, sondern auch möglich ist. Am Beispiel von Deutschland haben wir aufgezeigt, dass das Tor-Netz mit zusätzlichem Engagement von Bildungseinrichtungen erheblich gestärkt werden könnte. Basierend auf unseren Erfahrungen beim Betrieb von Exit Relays an Universitäten ermuntern wir dazu, eigene Erfahrungen im Betrieb von Tor-Knoten zu sammeln und die Forschung in diesem Bereich zu stärken.

Literatur

[1] The Tor Project, „Tor Metrics," 2020. [Online]. Available: https://metrics.torproject.org/. [Zugriff am 24 November 2020].

[2] R. Dingledine, N. Mathewson und P. F. Syverson, „Tor: The Second-Generation Onion Router," in *USENIX Security*, 2004.

[3] S. Köpsell, H. Federrath und M. Hansen, „Erfahrungen mit dem Betrieb eines Anonymisierungsdienstes," *Datenschutz und Datensicherheit*, Bd. 27, Nr. 3, pp. 139-142, 2003.

[4] S. Köpsell, „Entwicklung und Betrieb eines Anonymisierungsdienstes für das WWW," Technische Universität Dresden, 2010.

[5] J. Victors, „IamAn operator of eight Tor relays including two exits, AMA!," Reddit, 10 März 2014. [Online]. Available: https://www.reddit.com/r/IAmA/comments/20243q/iaman_operator_of_eight_tor_relays_including_two/. [Zugriff am 24 November 2020].

[6] D. M. Goldschlag, M. G. Reed und P. F. Syverson, „Hiding Routing Information," in *IHW*, 1996.

[7] R. Jansen, T. Vaidya und M. Sherr, „Point Break: A Study of Bandwidth Denial-of-Service Attacks against Tor," in *USENIX Security*, 2019.

[8] nusenu, „OrNetStats," 2020. [Online]. Available: https://nusenu.github.io/OrNetStats/. [Zugriff am 24 November 2020].

[9] The Tor Community, „Reduced Exit Policy," 2018. [Online]. Available: https://trac.torproject.org/projects/tor/wiki/doc/ReducedExitPolicy. [Zugriff am 08 12 2020].

[10] R. Singh, R. Nithyanand, S. Afroz, P. Pearce, M. C. Tschantz, P. Gill und V. Paxson, „Characterizing the nature and dynamics of Tor exit blocking," in *USENIX Security*, 2017.

[11] Electronic Frontier Foundation, „Tor on campus," 2004. [Online]. Available: https://web.archive.org/web/20200825150621/https://www.eff.org/tor-challenge/tor-on-campus.html. [Zugriff am 25 August 2020].

[12] nusenu, „The New Guide to Running a Tor Relay," The Tor Project, 8 Februar 2018. [Online]. Available: https://blog.torproject.org/new-guide-running-Tor Relay. [Zugriff am 24 November 2020].

[13] The Tor Project, „Community Resources: Tor Relay Universities," [Online]. Available: https://community.torproject.org/relay/community-resources/Tor Relay-universities/. [Zugriff am 24 November 2020].