Vom Darknet lernen

Spannende Techniken und Lösungsansätze aus dem Darknet

Vom Darknet lernen ..... **Seite 70**
Der Tor-Browser ..... **Seite 74**
Treuhänder-Modelle ..... **Seite 76**
Grenzen der Anonymität ..... **Seite 80**

Auch jenseits von illegalem Schwarzmarkt und Anonymität hat das Darknet viel zu bieten. Wer sich nicht von Sensationsgeschichten blenden lässt, findet spannende Lösungen für Probleme, die uns auch im Alltag beschäftigen.

Von Jürgen Schmidt

Das Darknet – fast jeder denkt dabei sofort an illegale Waffen, Drogen und Kinderporno-Tauschringe. Ja, all das gibt es im Darknet. Doch darum soll es in den folgenden Artikeln nicht gehen. Denn das Darknet hat viel mehr zu bieten als Illegales. Es ist ein einzigartiges Biotop mit interessanten Formen der Interaktion und spannenden Lösungen für Probleme, die uns auch im ganz normalen Leben umtreiben. Wer genau hinschaut, findet im Darknet Ansätze, die sich auch auf den Alltag und die helle Seite des Internet anwenden lassen.

Zum Beispiel Marktplätze: Wer schon mal versucht hat, im Internet ein gebrauchtes iPhone zu verkaufen, kennt das Problem. Teile der ganz normalen Internet-Märkte sind derart von Kleinkriminellen dominiert, dass man seine Waren oder sein Geld auch gleich wegwerfen kann – und sich dann wenigstens den Ärger spart. Im Darknet ist die Ausgangssituation noch krasser: Man muss dort davon ausgehen, dass das Gegenüber ein gewissenloser Betrüger ist, der jede sich bietende Gelegenheit nutzen wird, einen skrupellos über den Tisch zu ziehen. Und Sie werden keinerlei Möglichkeit haben, ihn dafür zu Rechenschaft zu ziehen. Wie soll man da noch Geschäfte machen?

Doch genau das funktioniert auf manchen Schwarzmarkt-Plattformen erstaunlich gut. Der Käufer bekommt die ihm zugesicherte Ware und der Verkäufer sein Geld; Betrugsfälle sind selten. Das hat rein gar nichts mit der bekanntermaßen ohnehin nicht vorhandenen Ehre unter Dieben zu tun. Sondern es beruht auf einem raffinierten Treuhändermodell. Bei dem übrigens die Treuhänder in aller Regel ebenfalls Gauner sind. Wie das alles funktioniert, erklärt der Artikel „Handel unter Gaunern“ auf Seite 76 ausführlicher.

Doch auch wer sich weniger für sozioökonomische Studien interessiert als für solide Technik, kommt auf seine Kosten. Denn vor allem im Bereich Security und Privacy kann das Darknet mit interessanter Technik und pragmatischen Lösungen glänzen, die keineswegs auf illegale Aktivitäten beschränkt sind.

Das Tor zum Darknet

So pflegen die Tor-Entwickler einen Browser, der sich vorzüglich als unabhängiger Zweit-Browser eignet. Damit muss man seinen Alltags-Browser nicht mit unkomfortablen Einschränkungen vernageln, sondern kann für all die Fälle, in denen man gern „auf Nummer sicher“ gehen will, auf den Tor-Browser zurückgreifen. Der setzt nämlich die Sicherheit ganz kompromisslos an die erste Stelle: kein Flash, nur explizit erlaubtes JavaScript und wo immer möglich erzwungene Verschlüsselung (siehe S. 74).

Apropos Tor: Dieses Netz im Netz bildet die technische Grundlage für große Teile des Darknet. Das liegt daran, dass Tor sehr weitreichende Garantien für Anonymität und Abhörsicherheit bietet, die bei Kriminellen hoch im Kurs stehen. Doch man muss nicht kriminell sein, um sich im Internet mehr Privatsphäre zu wünschen.

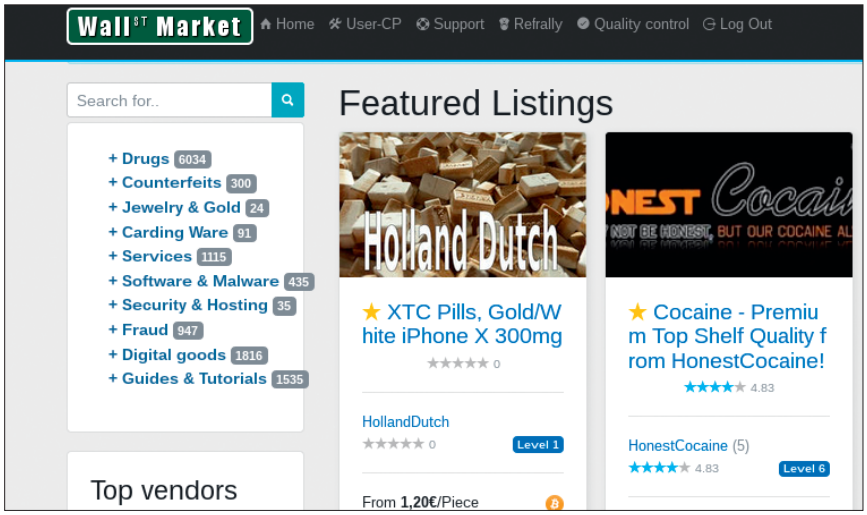
Die versprochene Anonymität erzeugt das Tor-Netz, indem das „Tor Onion Routing“ die Daten über mehrere Zwischenstationen schickt, die auf einer strikten „Need to know“-Basis operieren. Im normalen Internet trägt jedes Datenpaket die IP-Adresse des Absenders und des Empfängers; jede Station auf dem Weg kann diese Information einfach mitlesen. Bei Tor sieht jeder Netzwerkknoten immer nur den jeweiligen vorigen und nächsten Hop – aber keiner kennt sowohl Absender als auch Empfänger.

Erst wenn die Daten das Tor-Netz verlassen, um etwa an einen herkömmlichen Internet-Server geschickt zu werden, sieht der dafür zuständige Tor-Exit-Knoten die wirkliche Zieladresse. Er weiß aber nicht mehr, wer der ursprüngliche Absender war. Den kennt nur der sogenannte Tor Entry Guard – der aber weder Empfänger noch Inhalt der Daten sehen kann.

Diese Anonymität hat allerdings durchaus Grenzen. Sie liegen jedoch nicht bei den bekannten technischen Limitierungen, wie unsere Recherchen zur Praxis der Strafverfolgung im Darknet zeigen. Auch Tor ist kein universeller Garant für Anonymität – im Zweifelsfall steht das Sonderkommando schneller vor der Haustür, als man es sich träumen lässt. Der Artikel auf Seite 80 erklärt, warum das so ist.

Abhörfreier Raum

Anders sieht es mit der Abhörsicherheit aus. Die von Tor eingesetzte Verschlüsse-



Auf vielen Darknet-Marktplätzen geht es vor allem um Drogen – viel spannender ist jedoch die Technik dahinter.

lung funktioniert tatsächlich auf einem so hohen Niveau, dass Polizei und auch Geheimdienste davor schlicht kapitulieren und andere Wege suchen, an die gewünschten Daten zu kommen. Das geschieht dann etwa über Spionage-Trojaner, die sie auf den Endgeräten der Verdächtigten installieren.

Dabei geht die Abhörsicherheit von Tor noch einen Schritt weiter, als man das von der Transport-Verschlüsselung TLS im herkömmlichen Internet kennt. Die legt nämlich immer noch offen, wer wann welche Dienste nutzt. Wenn Sie etwa regelmäßig Heise über die mittlerweile standardmäßig verschlüsselte HTTPS-Verbindung lesen, sehen Ihr Provider oder die Admins Ihres Arbeitgebers immer noch, dass und wann Sie mit dem Heise-Server sprechen. Und die mit entsprechenden Verfügungen ausgestattete Staatsgewalt hat ebenfalls Zugriff auf diese Daten.

Das ist einer der Gründe, warum heise Investigativ einen eigenen Briefkasten im Darknet eingerichtet hat. Nicht nur wir als Empfänger sehen dabei nicht, woher das eingehende brisante Material stammt. Auch eventuelle Lauscher im Netz sehen bestenfalls, dass da jemand Tor benutzt. Selbst wenn jemand den kompletten Datenverkehr einer Zielperson mitlesen und analysieren kann, wird er keinen Hinweis auf eine Verbindung zwischen dem Tippgeber und dem Heise-Investigativ-Briefkasten finden. Das ist gelebter Informanten-Schutz.

Die offen einsehbare Information, wer wann welche Webseiten abruft, mag in Deutschland derzeit noch kein großes Problem sein. Doch als im arabischen Frühling repressive Regimes in Bedrängnis gerieten und die Machthaber mit voller Staatsgewalt zurückschlugen, sah das völlig unvermittelt ganz anders aus. Die vornehmlich jugendlichen Demonstranten organisierten ihren Protest nämlich hauptsächlich über Facebook. Und plötzlich war die intensive Facebook-Nutzung zur falschen Zeit ein verräterisches Indiz, das im Zweifelsfall sogar Lebensgefahr bedeutete.

Als direkte Konsequenz aus diesen Vorkommnissen bietet Facebook deshalb mittlerweile einen Zugang über einen sogenannten Hidden Service im Darknet (https://facebookcorewwwi.onion/) an. Der nutzt exakt die gleiche Technik wie die illegalen Marktplätze und ist einer der meistgenutzten Darknet-Dienste. Allerdings spielt Anonymität dabei keine Rolle. Denn spätestens nach der Anmeldung weiß Facebook sehr genau, wer da am anderen Ende ist. Es geht einzig darum, dass kein Dritter sehen kann, dass jemand Facebook benutzt.

Facebook ermöglicht Nutzern mit dem Hidden Service also einen abhörsicheren Zugang, auch wenn deren Leben vielleicht davon abhängt, dass sie niemand dabei beobachtet. In der Praxis bedeutet das natürlich, dass schon die Nutzung von Tor verdächtig macht und oft sogar technisch unterbunden wird. Auch da gibt es eine Reihe von Tricks, das zu umgehen, die an dieser Stelle jedoch zu weit führen würden.

Technisch realisiert Tor die Abhörsicherheit durch eine mehrstufige Verschlüsselung, bei der jeder Tor-Knoten nur für ihn – und alle potenziellen Lauscher – unlesbaren Cipher-Text transportiert. Im Wesentlichen sieht er nur nutzlose Nullen und Einsen, die er an einen anderen Tor-Knoten weiterleiten soll. Die mehrstufige Verschlüsselung legt sich dabei wie Schalen um die zu schützenden Inhalte – was die Zwiebel des Tor-Logos symbolisieren soll.

Versteckte Dienste

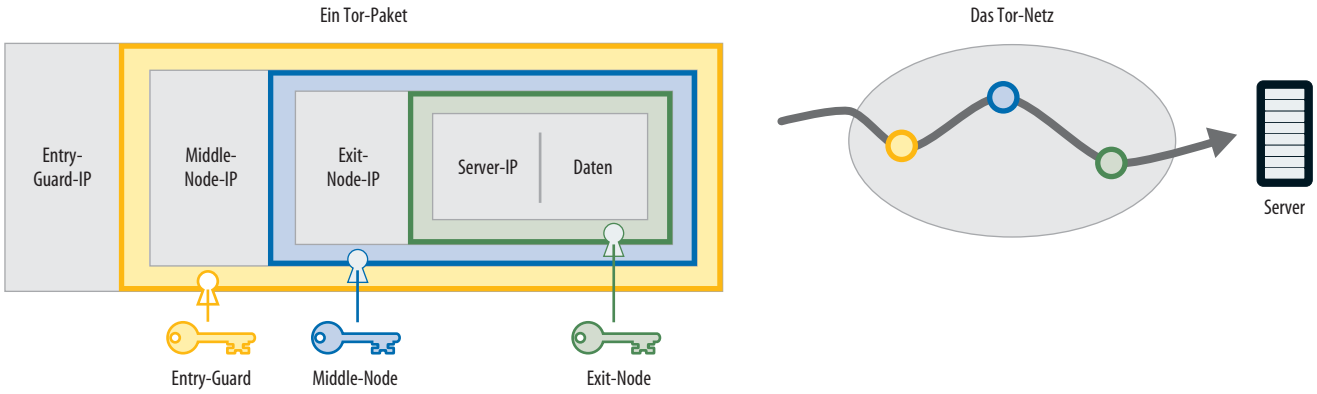
Tor Hidden Services machen einen Großteil des Darknet aus. Jeder kann einen solchen versteckten Dienst aufsetzen und betreiben (ein c't-Artikel in Ausgabe 22/2017 beschreibt das genauer). Anwender müssen nur den exakten Namen kennen, um ihn aufzurufen. Damit können Sie den Dienst dann wie gewohnt im Tor-Browser öffnen und benutzen. Doch hinter den Kulissen funktioniert einiges anders als im World Wide Web.

Das beginnt bei den Namen, die bei Hidden Services immer in .onion enden. Das ist eine künstliche Top-Level-Domain, die übers normale Domain Namen System (DNS) nicht aufgelöst werden kann. Stattdessen muss man einen Tor Directory Server konsultieren, der dann einen Introduction Point für die Tor-Verbindung zum Hidden Service im Tor-Netz liefert. Das alles klingt komplizierter als es ist. In der Praxis übernimmt der Tor-Browser das im Hintergrund; der Anwender muss dort nur wie gewohnt die URL eintippen und los gehts.

Wichtig ist dabei, dass der Tor-Nutzer und der Hidden Service – anders als im In-

Anonymität und Abhörsicherheit

Der Tor-Client baut sich seine eigene Route durch das Tor-Netz, bestehend aus Entry Guard, Middle Node und Exit Node.
Jedes Daten-Paket ist mehrfach verschlüsselt, und zwar so, dass die Empfänger der Reihe nach die IP-Adresse der nächsten Station entschlüsseln können. Erst der letzte in der Reihe, der Exit-Node, sieht die Adresse des Ziel-Servers und die für ihn bestimmten Daten. Er kennt aber den Absender nicht.



ternet – keinen direkten Kontakt haben. Das bedeutet, dass man vom einen Ende der Leitung aus nicht feststellen kann, wo der andere wirklich ist. Wegen des Tor-Routings über mehrere Zwischenstationen und eines zwischengeschalteten Rendezvous-Points im Tor-Netz kann man den physischen Server, auf dem ein Hidden Service läuft, nicht über das Netz aufspüren.

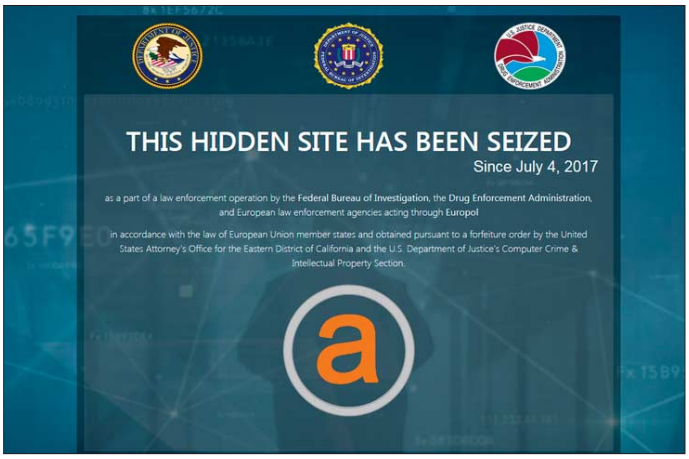
Das führt dazu, dass unter anderem illegale Schwarzmarkt-Plattformen sehr gern als Hidden Service operieren, um der Strafverfolgung zu entgehen. Wie dann jedoch Waffen- und Drogenumschlagplätze wie der berüchtigte Hansa Market dennoch hoppsgenommen wurden, erklärt der bereits erwähnte Artikel zu den Grenzen der Anonymität auf Seite 80.

Vertrauen ist Namenssache

Zurück zu den Namen, die eine wichtige Funktion im Tor-Netz innehaben. Der Teil vor dem .onion ist meistens unmerkbares Kauderwelsch. Das kommt daher, dass die Namen aus Hash-Werten über einen öffentlichen Krypto-Schlüssel gebildet werden. Auf diesem Weg löst Tor nämlich das Grundproblem der Verschlüsselung gänzlich anders als das normale Web.

Für die Heise-HTTPS-Seiten bestätigt eine angeblich vertrauenswürdige Zertifizierungsstelle (CA), dass ein Schlüssel tatsächlich Heise gehört. Doch Diginotar und andere CAs wurden gehackt; Symantecs CA wurde mehrfach dabei erwischt, dass sie unberechtigt Zertifikate ausgestellt hat. Und wer sich auf diesem Weg ein Heise-Zertifikat mit der Unterschrift einer CA erschleicht, kann sich in die Verbindung zwischen dem Heise-Server und dem Browser einklinken und alles mitlesen. Das mit dem Vertrauen im Web – das funktioniert also bestenfalls so lala.

Beim Tor-Netz gibt es hingegen nur einen Schlüssel, der zu „sq4lecqyx4iz cpkp“ passt. Und das ist der, den wir auf dem Server des Heise-Investigativ-Briefkastens auf http://sq4lecqyx4izcpkp.onion/ deponiert haben. So lange Sie den richtigen Namen (etwa aus dem Impressum der c’t) verwenden und wir unseren Original-Schlüssel sicher verwahren, kann niemand so tun, als ob er der richtige Heise-Investigativ-Server wäre und sich etwa in eine verschlüsselte Verbindung zum Heise-Briefkasten einklinken. Keine Zertifizierungsstelle der Welt kann einen passenden Schlüssel für diesen Server ausstellen.



Das Darknet ist kein rechtsfreier Raum: Die Polizei hat die zentralen Marktplätze Alpha-Bay und Hansa geschlossen und die Betreiber verhaftet.

Der Nachteil ist, dass die Namen in aller Regel sehr kryptisch und schwer zu merken sind. Facebook hat enorm viel Rechenzeit verbraten, um Millionen und Aber-Millionen von Schlüsseln zu erzeugen, bis sie die halbwegs sinnvolle Zeichenkette facebookcorewwwi hatten (die ich trotzdem jedes Mal nachschauen muss).

Damit die potenziellen Nutzer einen Dienst finden, benötigen sie also dessen Namen, der – anders als im Web – in aller Regel nicht aus dem Namen des Dienstes ableitbar ist. Dreh- und Angelpunkt des Darknet sind deshalb Verzeichnisse der verfügbaren Hidden Services und deren Onion-URLs. Das erinnert ein wenig an die digitale Steinzeit, als Sites wie Yahoo versuchten, das Internet zu katalogisieren – und fühlt sich in der Praxis auch oft so an. Das historisch wichtigste Verzeichnis ist das Hidden Wiki; Fresh Onions klappert das Darknet selbst nach neuen Diensten ab und liefert aktuellere Listen. Etwas gezielter kann man über die Darknet-Suchmaschinen „Not Evil“ und „Torch“ navigieren (siehe ct.de/yrdc).

Doch der erste eigene Kontakt mit dem Darknet führt ohnehin fast zwangsläufig zu Frust und Enttäuschung. Viele Links sind bereits kaputt; die verfügbaren Inhalte sind oft trivial oder ganz offensichtliche Betrugsversuche. Ersparen Sie sich das und lesen Sie lieber die nächsten Artikel zum Tor-Browser, den Treuhändermodellen oder den Grenzen der Anonymität. *(ju@ct.de)* c't

Einstieg ins Darknet: **ct.de/yrdc**

Was ist das Darknet?

Für die meisten ist Darknet ein eher flapsiger Begriff für die „dunklen Seiten des Internet“ – also vor allem für illegale Inhalte und Angebote. Manche machen das Dunkle auch daran fest, dass die Inhalte anders als das „Clearnet“ nicht einmal von den quasi allwissenden Suchmaschinen wie Google durchleuchtet und erfasst werden. Das firmiert dann auch unter Deep Web.

Diese Definition bezieht aber alle Communities mit ein, auf die man erst nach einer Registrierung Zugriff erhält. Also beispielsweise sogenannte Carder-Foren, in denen Kreditkarten-Betrüger und solche, die’s werden wollen, Tipps und Erfahrungen austauschen. Aber natürlich auch kommerzielle Inhalte, auf die man nur gegen Bezahlung zugreifen kann oder die private Nachbarschafts-Community, zu der man nur auf Einladung Zugang erhält.

Eher technisch orientierte Menschen nutzen Darknet als Oberbegriff für Overlay-Netze, die das Internet lediglich als Transport-Medium nutzen und darauf eine eigene, auf Anonymität der Teilnehmer abzielende Infrastruktur aufbauen. Das prominenteste Netz dieser Art ist The Onion Router, kurz Tor; I2P, Freenet, GNUnet und RetroShare sind weitere Vertreter. Ursprünglich bezeichneten Internet-Techniker die Teile des Internet als Darknet, die nicht geroutet werden. Diese Definition ist jedoch heute nicht mehr gebräuchlich.