Zeitschrift: Schweizer Monat : die Autorenzeitschrift für Politik, Wirtschaft und Kultur

Band: 96 (2016)

Heft: 1040

Artikel: Darknet : Freiheit im Untergrund

Autor: Grob, Ronnie

DOI: https://doi.org/10.5169/seals-736379

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Siehe Rechtliche Hinweise.

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. Voir Informations légales.

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. See Legal notice.

Download PDF: 20.10.2024

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Darknet – Freiheit im Untergrund

In seiner Grenzenlosigkeit wirkt das Darknet auf Libertäre wie eine Traumwelt. Die dort florierende Schattenwirtschaft konkurriert allerdings mit der Realwirtschaft. Und die muss, anders als kriminelle Unternehmer, Steuern zahlen.

von Ronnie Grob

Am Boulevard steht ein hell erleuchtetes Kaufhaus. Seine Besitzer zahlen Steuern und müssen sich an die Gesetze halten. Wenn es seine Kunden befriedigt, kann es Gewinn erwirtschaften, wenn es sie schädigt, kann es verklagt und verurteilt werden. Dasselbe gilt für Kaufhäuser im Internet wie Amazon, Siroop oder Galaxus. Der Kunde hat aber natürlich auch andere Möglichkeiten, zu den Gütern zu kommen, nach denen er sucht. Er kann etwa jene dunklen Seitengassen aufsuchen, in denen zwielichtige Strassenhändler vor Schuppen mit schlecht sortierten, illegalen Waren stehen. Irgendwann, wenn er dann mal wieder hingeht, weil er Waren nachkaufen will oder eine Reklamation hat, sind sie einfach verschwunden. So etwa ist das Einkaufen im Darknet.

Ronnie Grob
ist Redaktor dieser Zeitschrift. Er lebt in Zürich.

Deep Web

Aber wie funktioniert es im Detail? Zunächst: neben den frei zugänglichen Teilen des World Wide Web gibt es viele von Suchmaschinen nicht indexierte Teile, die unter dem Begriff «Deep Web» zusammengefasst werden. Die breite Masse benutzt sie täglich: passwortgeschützte E-Mail- oder Bankkonten zum Beispiel, Intranets oder Datenbanken. Das Darknet dagegen, ein kleiner Teil des «Deep Web», ist mit konventionellen Browsern wie Firefox oder dem Internet Explorer nicht auffindbar: es ist zugänglich mit einem Peer-to-Peer-System (P2P) oder mit dem Verschlüsselung garantierenden Browser TOR («The Onion Browser»). Trotz über 1,5 Millionen täglichen Nutzern weltweit, davon 10 000 bis 15 000 aus der Schweiz, ist der kostenlos installierbare TOR-Browser bisher ein zumeist von Spezialisten benutztes Nischenprodukt geblieben. Nachvollziehbar, denn noch ist es zeitraubend und umständlich, seine Privatsphäre im Netz zu bewahren.

Bemerkenswert am TOR-Browser, dem Zugang zum Darknet, ist, dass er von der US-Regierung entwickelt und finanziert wurde. 2011 bezahlte sie 60 Prozent des Budgets[1], und auch heute noch weist das inzwischen unabhängige Open-Source-Projekt TOR das dem US-State Department angegliederte Bureau of Democracy, Human Rights, and Labor als einen seiner Sponsoren aus. Das Interesse der US-Regierung ist zunächst der Schutz von Demokratieaktivisten in unfreien Staaten. Aber auch die Verschleierung von Aktivitäten eigener Agenten. Diese, so die Legende, wären als alleinige Nutzer des verschlüsselten Browsers doch etwas auffällig geworden. Heute stellen Russland und Deutschland zusammengenommen gleich viele Nutzer wie die USA. In diesen drei Ländern wird der TOR-Browser am häufigsten benutzt.[2]

Drogen

Eine Studie der Carnegie Mellon University von 2015[3] errechnete ein tägliches Handelsvolumen von 300 000 bis 500 000 US-Dollar im Darknet. Den grössten Teil des Warenangebots machen Drogen aus, und das ist kein Zufall. Es ist bequemer und sicherer, im Darknet einzukaufen, als einen Dealer persönlich zu treffen. Wie beim Drogenkauf im Hinterhof fürchtet der Einkäufer dreierlei: Selbst ertappt zu werden von der Polizei. Das Verschwinden des Händlers mit dem ihm anvertrauten Geld, also die Unterlassung einer Gegenleistung. Und die Verhaftung des Händlers, also die polizeiliche Erlangung von Informationen über den Käufer. Nicht zu fürchten dagegen hat der Käufer physische Gewalt des Verkäufers, da die Transaktion nur online abläuft. Wird sie über einen etablierten Darknet-Händler abgeschlossen, ist sogar das finanzielle Risiko überschaubar.

Einige der Drogenanbieter geben sich alle Mühe, nicht wie undurchschaubare Dealer, sondern wie vertrauenswürdige Produzenten aufzutreten. Die Bewertungen des Händlers «Hashishmaster» auf dem Branchenblog Deepdotweb.com etwa loben nicht nur die gute Kommunikation des Marihuanapakete aus Kanada schickenden Produzenten, sondern explizit auch seine herausragende Ware. Man habe es hier nicht mit einem «Dealer» zu tun, sondern mit einem echten, erfahrenen «Farmer». Seine Kun-

[1] TorProject Annual Report 2012, https://www.torproject.org/about/financials.html.en
[2] Quelle: https://metrics.torproject.org/userstats-relay-table.html
[3] Kyle Soska und Nicolas Christin: Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. Web: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska-updated.pdf

den, die angeben, aus Japan, Frankreich oder Grossbritannien zu stammen, schreiben übereinstimmend, sie hätten einwandfreie Ware erhalten, und das bereits drei bis sechs Tage nach der Bestellung: «Er ist einfach der Beste. Und es ist so schwierig, im Darknet einen echten, leidenschaftlichen Bauern zu finden, der nicht nur auf Geld aus ist», so eine Kundenbewertung.

Darknet-Marktplätze gibt es viele. Silk Road, gegründet 2011, war bis zur Schliessung im Oktober 2013 der grösste von ihnen. An Gründer Ross Ulbricht, der zu einer lebenslangen Haft ohne die Möglichkeit auf Bewährung verurteilt wurde, hat die US-Justiz ein Exempel statuiert. Der Wegfall des damals fast monopolistisch agierenden Branchenleaders war aber nicht das Ende solcher Marktplätze, im Gegenteil, er schuf viele neue. Sie heissen «AlphaBay», «Hansa Market», «Nucleus Market» oder «Valhalla» und funktionieren ähnlich wie Ebay oder Amazon als Verkaufsplattform für Subunternehmer. Die meisten dieser Subunternehmer sind vergleichsweise kleine Fische – über die Hälfte der Transaktionen wird von nur einem Prozent der Verkäufer abgewickelt.

Anders als bei Ebay kann der Kunde allerdings nie sicher sein, dass es diese Plattformen morgen noch gibt. Es kommt immer wieder vor, dass grosse Marktplätze plötzlich verschwinden, aufgrund eines Eingreifens der Polizei oder weil die Betreiber die Guthaben bei sogenannten «Exit Scams» haben mitgehen lassen: 2015 verschwand «Evolution» mit einem Bitcoin-Guthaben im Wert von 11 Millionen Euro, 2013 der «Sheep Marketplace» mit 36 Millionen Euro Kundenguthaben.[4] Das kostenlose P2P-Netzwerk «Open Bazaar» ist schon einen Schritt weiter und ermöglicht den Handel von Gütern via Bitcoin in einem dezentral organisierten Markt. Exit Scams sind so nicht mehr möglich, und die Behörden sind vor das Problem gestellt, dass weder Websites noch Server bestehen, die man schliessen könnte.

Die Fälschung von Ausweisen, wie man sie im Darknet findet, ist gemäss Art. 252 StGB untersagt. Verboten ist nicht nur das Fälschen und Verfälschen, sondern auch der Gebrauch eines unechten oder der Missbrauch eines echten Ausweises.
Bild: Musterkarten eines Darknet-Anbieters, Screenshot & Collage: Schweizer Monat.

Recht auf Privatsphäre

Darknet-Marktplätze sind erfolgreich, weil sie das anonyme Einkaufen ermöglichen. Mittels des TOR-Browsers sind die IP-Adressen der am Handel Beteiligten nicht rückvollziehbar und die gesendeten Datenpakete verschlüsselt. Mit dem Einsatz einer der aktuell rund 700 Kryptowährungen wie Bitcoin, Ethereum, Ripple oder Monero bleibt von der Zahlungsanweisung meist nur eine Nummer. Diese Sicherheitsmassnahmen sind schon einzeln schwierig zu entschlüsseln, gemeinsam angewendet bieten sie aber eine fast perfekte Privatsphäre, auch vor den Behörden. Wäre also ein Verbot der Verschlüsselung wünschenswert? Nein. Einerseits ist weder Technik noch Handel mit Verboten leicht beizukommen, andererseits ist das Recht auf Privatsphäre – vor allem vor dem Staatsapparat – eines der wichtigsten Grundrechte des freien Bürgers. Auch Whistleblower und Journalisten, die versteckt gehaltene Skandale aufdecken, zählen auf diese Verschlüsselungssysteme. Nur so können sie sich und ihre Quellen schützen. In Ländern, in denen keine Meinungsfreiheit, aber Gesinnungskontrolle herrscht, sind die Bürger ebenfalls darauf angewiesen, sich auf diesem Wege dem Zugriff des Staats oder der Religionspolizei zu entziehen und miteinander kommunizieren zu können.

«Es haben alle Bürger ein Recht auf Privatsphäre. Ein Staat, der die Verschlüsselung generell verbietet, kann keine Demokratie mehr sein», sagt Marc Ruef. Er ist einer der Inhaber der 2002 in Zürich gegründeten Scip AG, die Sicherheitsüberprüfungen macht und Firmen und Behörden in Sicherheitsfragen berät. An der Gesetzgebung müsse die Politik grundsätzlich keine Änderungen vornehmen: «Das Darknet ist nur ein Werkzeug, um das Verbrechen zu orchestrieren. Tatsächlich findet es aber in der realen Welt statt.» Das zeigt auch die Einschätzung der Nato, die den Cyberspace neu als operativen Bereich betrachtet, so wie Luft, Wasser und Land.[5]

Ermittlungen

Was Ermittlungen im Darknet angeht, gibt sich die Polizei wortkarg. Die Kommunikationsverantwortliche des Fedpol, Cathy Maret, sagt nicht mehr als: «Es ist ein Ort, an dem sich die Kriminellen bewegen. Ermittlungen sind möglich.» Der Kanton Zürich hat auf Beschluss des Regierungsrats ein «Kompetenzzentrum Cybercrime» ins Leben gerufen. 2015 beschäftigte es sechs polizeiliche Ermittler, davon zwei von der Stadtpolizei, zwei Staatsanwälte sowie zwei Sekretariatsmitarbeitende.[6] Um brauchbare Informationen aus dem Darknet zu beziehen und Zugang zu bestimmten Märkten zu erhalten, muss man sich über Wochen, eher über Monate und Jahre hinweg Kontakte und Vertrauen aufbauen. Eine von konkreten Ermittlungen getriebene Polizeistelle hat diese Zeit jedoch in der Regel nicht. Und ohne gezielte Hinweise ist es schwierig bis unmöglich, ein Netz, an dem nur wenige Nutzer beteiligt sind, aufzuspüren. Viele Kriminelle, so Marc Ruef, scheitern aber so oder so irgendwann an sich selbst, meist an einer

«Man habe es hier nicht mit einem ‹Dealer› zu tun, sondern mit einem echten, erfahrenen ‹Farmer›. Seine Kunden, die angeben, aus Japan, Frankreich oder Grossbritannien zu stammen, schreiben übereinstimmend, sie hätten einwandfreie Ware erhalten, und das bereits drei bis sechs Tage nach der Bestellung.»

Ronnie Grob

Nachlässigkeit oder bei der guten alten Steuererklärung: «Wer plötzlich eine Million Franken auf dem Konto oder einen Sportwagen in der Garage stehen hat, wird verdächtig. Das Waschen von Geld kostet Zeit und eben auch Geld – je mehr, desto schneller man es gewaschen haben will.» Eine gängige Praxis ist es, mit Kryptowährungen in Online-Casinos zu spielen. Gegenüber den Steuerbehörden wird versucht, den dort ausbezahlten Betrag als glücklichen Gewinn zu verkaufen.

Besondere Sorgen macht den Schweizer Ermittlern das Aufkommen von Crime-as-a-Service-Dienstleistungen, also der Einkauf von kriminellen Aktivitäten: «Cyberverbrechen sind längst nicht mehr Spezialisten vorbehalten. Jeder, der das nötige Geld hat, kann mitmischen. Und alles deutet darauf hin, dass sich diese Entwicklung in den kommenden Jahren verstärkt.»[7] So ist es ein Leichtes, eine DDoS-Attacke einzukaufen, also die Überflutung einer unliebsamen Webseite mit Anfragen, so dass der reguläre Betrieb nicht aufrechterhalten werden kann. Kurze Angriffe sind schon für 50 Franken zu haben, Dauerangriffe über mehrere Tage kosten mehrere Tausend Franken. Eingekauft werden können auch Kreditkartendaten, gefälschte Ausweise, verbotene Pornografie oder Waffen. Mit grosser Wahrscheinlichkeit abschreiben kann man allerdings überwiesenes Geld, das zu einem Auftragsmord an einer prominenten Person führen soll. Vieles im Darknet ist schlicht Betrug.

Libertärer Traum

Welche Gefahren stellt das Darknet für unbescholtene Unternehmer dar? Marc Ruef sagt es so: «Wenn die Servicequalität der Realwirtschaft abnimmt oder die Preise zu hoch sind, fangen die Leute an, Waren aus der Schattenwirtschaft zu beziehen. Die Professionalisierung des Darknets nimmt ständig zu, das kann man beobachten.» Wie das Silicon Valley ist das Darknet von Männern dominiert, vieles erinnert exakt an die Entwicklung des WWW in den 1990er Jahren. Technisch hinkt es dem WWW, von der Verschlüsselung abgesehen, über ein Jahrzehnt hinterher. Die Suchmaschinen finden ihr Ziel so ungenau wie seinerzeit Altavista. In den Foren herrscht die freie Rede mit all ihren mitunter unangenehmen Ausprägungen.

Auf einen ersten Blick scheint das Darknet wie die Erfüllung eines libertären Traums: Endlich gibt es einen Raum, in dem freier Handel betrieben werden kann, ohne dass dieser von lästigen Vorschriften, Gesetzen, Abgaben und Regulierungen beeinträchtigt wird. Tatsächlich aber sind Handelsgeschäfte ohne Rechtssicherheit anarchisch – und so der Willkür unterworfen. Ohne Gesetze, die herangezogen, und ohne Gerichte, die im Streitfall angerufen werden können und ein Urteil fällen, bleibt jeglicher Handel ein ungleich höheres Risiko. Während der legale Händler, das Kaufhaus am Boulevard, dazu gezwungen wird, Steuern zu bezahlen und Gesetze zu befolgen, beschränkt sich der regulatorische Aufwand des illegalen Händlers in der Seitengasse darauf, sich den Strafverfolgern zu entziehen.

Es bleibt festzustellen, dass beispielsweise die Repression von Drogen nicht zielführend war. Sie hat nicht zu weniger Süchtigen geführt – und an Drogen heranzukommen ist heute simpler denn je. Die Politik kann sich dem Handel im Darknet nur entgegenstellen, indem sie die staatlichen Eingriffe in den freien Markt prüft: Jene Verbote und Massnahmen, die sich als obsolet erweisen, sind aufzuheben, um so das bisher illegale zu einem neu legalen und freien Handelsprodukt zu machen. Schliesslich entstehen Schattenmärkte nur dort, wo der Staat mit Verboten, Gesetzen oder Rationierungen auf eine Weise eingreift, die von Teilen des Marktes nicht akzeptiert werden. ‹

[4] «The Internet Organized Crime Threat Assessment 2015» von Europol. Web: europol.europa.eu
[5] Pressekonferenz der Nato vom 14. Juni 2016. Web: http://www.nato.int/cps/en/natohq/opinions_132349.htm
[6] Protokoll des Regierungsrates des Kantons Zürich, Sitzung vom 26. August 2015.
[7] Jahresbericht KOBIK 2014, Seite 41.

Verschlüsselung Made in Switzerland

Schweizer Firmen, die für Privatsphäre bei der Kommunikation sorgen.

Wie ein Messer, das Gemüse schneiden oder jemanden töten kann, ist die Verschlüsselung von Daten ein Schutz für die Privatsphäre oder für kriminelle Aktivitäten. Die Schweizer Wirtschaft, traditionell stark bei den Themen Sicherheit und Privatsphäre, hat einige Firmen hervorgebracht, die sich der verschlüsselten Kommunikation annehmen und damit auch international Erfolg haben. (RG)

E-Mails

Eine Schweizer Firma, die per Crowdfunding im Internet 550 000 US-Dollar von über 10 000 Unterstützern einsammelt? Die Genfer **Proton Technologies AG,** Anbieterin eines verschlüsselten E-Mail-Dienstes, hat es vorgemacht und mit dem gespendeten Geld Server gekauft, mehr Nachrichten pro Monat kostenlos angeboten und eine App gebaut. Während Protonmail Cloud-Services bereitstellt, offerieren andere Verschlüsselungslösungen zur lokalen Installation, erweitert um Cloud-Lösungen für verschlüsselte E-Mails, so wie zum Beispiel **SEPPmail** aus Neuenhof (AG). Mit **IncaMail** bietet auch die Schweizerische Post den vertraulichen Versand über eine E-Mail-Verschlüsselung an. Hinter dem Kürzel **p≡p** steht **pretty Easy privacy,** ein Open-Source-Projekt der pep Foundation in Winterthur. Es ermöglicht die Verschlüsselung und Anonymisierung von bereits bestehenden E-Mail-Konten.

Messaging

Nach der Ankündigung des Mobilchats WhatsApp, die anvertrauten Telefonnummern an seinen Besitzer Facebook weiterzureichen, boomten bei der **Threema GmbH** in Pfäffikon (SZ) die Downloads. Die Firma verkauft eine verschlüsselte Messaging-App, die bereits millionenfach heruntergeladen wurde – mehr als 85 Prozent der Nutzer sind aus dem deutschsprachigen Raum. Einen alternativen Messenger mit Ende-zu-Ende-Verschlüsselung betreibt die **Wire Swiss GmbH** in Zug; «Wire» kann auf Smartphones, Tablets und Apple-Laptops eingesetzt werden.

Telefonie

Die **Blackphone SA** aus Genf und die **Silent Circle SA** aus Le Grand-Saconnex (GE) haben das Blackphone 2 auf den Markt gebracht, ein Smartphone, das die Verschlüsselung von Gesprächen, E-Mails, SMS und Internetseiten verspricht und seit Oktober 2015 für rund 1000 Franken verkauft wird. Die **TelePhoenix AG** aus Emmetten (NW) bietet mit OpusTel eine App für verschlüsselte Telefongespräche an. Die **Veeting AG** in Zürich bietet mit TLS oder DTLS-SRTP verschlüsselte Kommunikation per Audio und Video an. Auf Cloud-Services wird verzichtet, die Server stehen alle in der Schweiz.

Datensicherung

Die **DSwiss AG** in Zürich schützt ihren Online-Datenspeicher «Secure Safe» mit Verschlüsselungsmethoden, einer Benutzerauthentifizierung und einer dreifach redundanten Datensicherung. Eines der Schweizer Datenzentren befindet sich in einem ehemaligen Militärbunker in den Bergen. Ebenso tut es die **MOUNT10 AG** in Baar (ZG), die zwei 256-bit-AES-verschlüsselte Datencenter in den Schweizer Alpen betreibt, die sie «Swiss Fort Knox» nennt. In Zug betreibt die **Digitale Gesellschaft** aus Basel zwei Tor-Exit-Server, denn damit der TOR-Browser funktioniert, braucht es Server, die auch von Schweizer Anbietern gehosted werden.

Währungen

Mit rund einer Milliarde US-Dollar Marktkapitalisierung ist Ethereum derzeit nach Bitcoin die Nummer 2 auf der Weltrangliste der derzeit über 700 existierenden Kryptowährungen. Gemäss Handelsregister bezweckt die dahinter stehende, nicht auf Profit ausgerichtete **Stiftung Ethereum** in Baar (ZG) insbesondere die «Förderung von neuen offenen dezentralisierten Softwarearchitekturen». 1 Ether war im September 2016 für 11 Franken zu haben.