Bild: Albert Hulm

# Razzia in der Silk Road

## Wie das Amazon des Darknet aufflog

**Von 2011 bis 2013 war die Silk Road ein florierender Umschlagplatz für Drogen und Waffen im Darknet. Auf die Spur kamen die Ermittler dem Betreiber durch einen Trick.**

**Von Klaus Schmeh**

Eine Szene wie aus einem Hollywood-Film: In einer Bibliothek in San Francisco inszenierten zwei als Liebespaar getarnte Polizisten des FBI einen Streit, mit dem sie den an seinem Laptop sitzenden Bibliotheksbesucher Ross Ulbricht kurz ablenkten. Ein dritter Polizist war zur Stelle und nahm Ulbrichts Rechner an sich, bevor dieser ihn sperren konnte. Während Ulbricht verhaftet wurde, kopierten IT-Spezialisten die auf dem Laptop gespeicherten Daten auf eine USB-Festplatte.

Mit der Verhaftung Ulbrichts endete nach zweieinhalb Jahren die Geschichte von Silk Road, jener illegalen Online-Plattform, die dem Drogenhandel im Internet eine erste große Blüte beschert hatte. Ulbricht, Jahrgang 1984, war Gründer und Kopf des Darknet-Marktplatzes. 2010 hatte der Computerexperte aus Texas mit der Umsetzung begonnen, im Januar 2011 ging Silk Road online. Unter dem Pseudonym Dread Pirate Roberts (nach einer Figur aus dem Fantasyfilm „Die Braut des Prinzen“) leitete Ulbricht eine schnell wachsende Handelsplattform, auf der es neben Drogen, Raubkopien, gefälschten Ausweise und Waffen auch einige legale Waren zu kaufen gab. Da Ulbricht den Betrieb von Silk Road schon bald nicht mehr alleine bewältigen konnte, heuerte er Mitarbeiter an, die Ad-

ministrationszugänge erhielten, aber meist anonym blieben.

Silk Road war zwar nicht die erste Plattform ihrer Art, doch bis dahin die mit Abstand erfolgreichste. Laut der Klageschrift soll die Plattform innerhalb von zweieinhalb Jahren einen Umsatz von 1,2 Milliarden US-Dollar generiert haben. Dies lag nicht zuletzt an der professionellen Aufmachung der Webseite, die an eBay oder Amazon erinnerte. Die Anonymität des Darknet schützte die Betreiber. Bezahlt wurde mit Bitcoin, was der damals noch neuen Blockchain-Währung erheblichen Auftrieb verschaffte. Das Postgeheimnis sorgte dafür, dass die meisten Lieferungen unentdeckt blieben.

Vor allem in den USA boomte die Silk Road. Das illegale Portal war den Behörden schnell ein Dorn im Auge. Gleich mehrere staatliche Organisationen machten sich auf die Jagd nach Dread Pirate Roberts – zunächst ohne Erfolg. Erst im Herbst 2013 konnten die Ermittler schließlich besagten Ross Ulbricht als Silk-Road-Betreiber identifizieren. Im Oktober 2013 wurde dieser wie eingangs beschrieben vom FBI verhaftet.

## Verräterischer Laptop

Ein gutes Jahr später musste sich Ulbricht in New York City vor Gericht verantworten. Die Staatsanwaltschaft konnte mit Daten vom konfiszierten Laptop und dem Silk-Road-Server sowie mit beschlagnahmten Unterlagen leicht nachweisen, dass Ulbricht hinter Silk Road steckte.

Dieser bestritt den Vorwurf nicht, behauptete jedoch, er habe das Portal lediglich in der Gründungsphase und eine kurze Zeit vor seiner Verhaftung betrieben. Dazwischen hätte dies eine andere Person übernommen, die damit die Hauptschuld treffe. Als die Schlinge sich zuzog, so Ulbricht, hätte der Unbekannte die Verantwortung wieder an ihn zurückgegeben, worauf er sich naiverweise eingelassen hätte.

Mit dieser Verteidigungsstrategie kam Ulbricht jedoch nicht durch. Chatprotokolle, Kostenaufstellungen, ein digital geführtes Tagebuch und handschriftliche Aufzeichnungen belegten eindeutig, dass er bei der Arbeit an Silk Road keine größere Pause eingelegt hatte. Außerdem ließ sein beträchtliches Bitcoin-Vermögen keinen Zweifel daran, dass ein Großteil der Silk-Road-Provisionen bei ihm gelandet war.

Am 4. Februar 2015 sprach die Jury Ulbricht schuldig. Für die Festlegung der Strafe war Richterin Katherine Forrest zuständig. Die Staatsanwaltschaft forderte einen Freiheitsentzug von „weit über der Mindeststrafe von 20 Jahren“. Forrest entschied sich für ein besonders harte Form:

Bild: United States Sentencing Commission

**Ross Ulbricht gründete 2011 die Handelsplattform Silk Road im Darknet. Zweieinhalb Jahre später wurde er spektakulär vom FBI verhaftet.**

zweimal lebenslänglich zuzüglich 40 Jahre. Die beiden lebenslänglichen Strafen gegen ihn wurden als „Life without Parole“ (LWOP) ausgesprochen. Dies bedeutet, dass Ulbricht nicht vorzeitig auf Bewährung (parole) freigelassen werden kann. Nur eine Begnadigung durch den US-Präsidenten ist laut Gesetz möglich.

## Nach dem Urteil

Ungeachtet des Urteils florierte der illegale Handel im Darknet weiter. Bereits knapp einen Monat nach Ulbrichts Verhaftung ging Silk Road 2.0 an den Start. Offensichtlich steckten einige Administratoren der ursprünglichen Seite dahinter. Die Benutzeroberfläche blieb nahezu unverändert. Das Angebot war schon bald größer und die Umsätze höher als die der ursprünglichen Silk-Road-Seite.

Silk Road 2.0 existierte fast genau ein Jahr, bevor es einem internationalen Team von Ermittlern im Rahmen der Operation Onymous gelang, das Portal zu schließen. Einige der Hintermänner waren schon deutlich früher ausfindig gemacht und verhaftet worden.

Im Vergleich zu Ulbricht kamen die Betreiber von Silk Road 2.0 äußerst glimpflich davon. Am härtesten traf es noch den US-Computerexperten Brian Farrell, obwohl dieser nur eine Assistentenrolle eingenommen hatte. Ein US-Gericht verurteilte ihn zu acht Jahren Gefängnis. Thomas White, einer der Haupttäter, hatte das Glück, dass er in Großbritannien vor Gericht stand, wo die entsprechenden

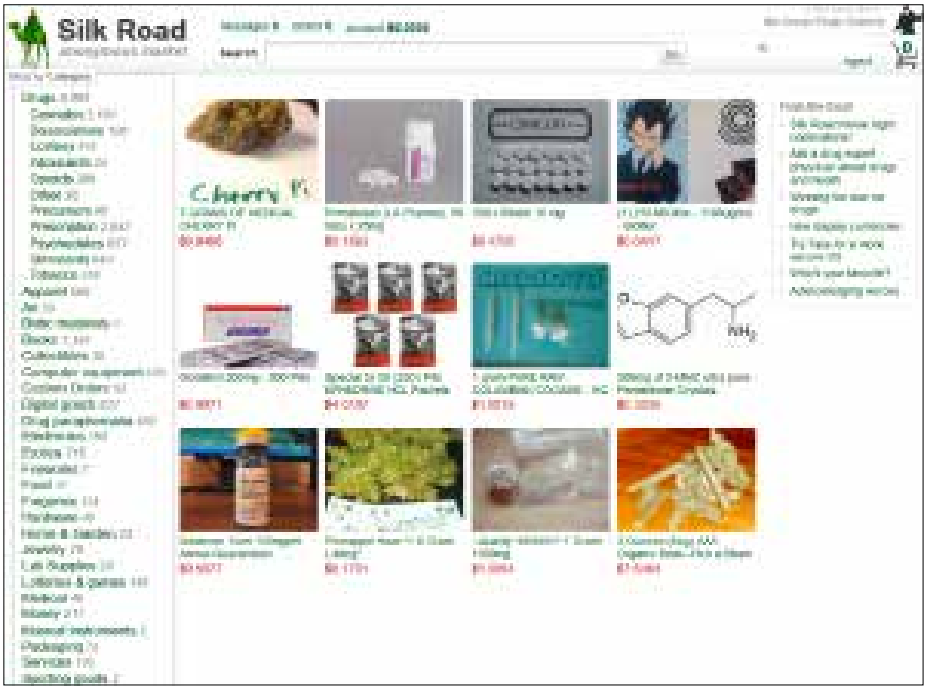


Bild: Silk-Road-Webseite

**Auf Silk Road wurden vor allem illegale Drogen gehandelt. Die professionell gestaltete Benutzeroberfläche, die der von Amazon oder eBay ähnelte, trug zum großen Erfolg der Seite bei.**

Bild: Bitcointalk.org

**In einem Onlineforum wies Ross Ulbricht unter dem Pseudonym „altoid“ auf Silk Road hin (oben). In einem anderen Beitrag fanden Ermittler eine E-Mail-Adresse von altoid, die dessen Klarnamen enthielt (unten).**

Gesetze deutlich weniger streng sind. Er erhielt fünf Jahre und vier Monate.

Ohne nennenswerte Gefängnisstrafe kam Blake Benthall davon, ein weiterer Hauptbeschuldigter im Zusammenhang mit Silk Road 2.0. Er hatte es zwar, wie Ulbricht, mit der US-Justiz zu tun, doch anders als dieser kooperierte Benthall vollständig mit den Behörden, woraufhin diese ihn lediglich wegen Steuerbetrug anklagten. Dabei hatte Benthall in Silk Road 2.0 eine ähnliche Rolle gespielt wie zuvor Ulbricht in der ursprünglichen Version des Portals.

## Kampf gegen Hydra

Mit dem Ende der Version 2.0 war die ursprüngliche „Silk Road“-Plattform zwar endgültig Geschichte, doch illegale Handelsportale gab es nach wie vor. Dazu gehörten Silk Road Reloaded oder Silk Road 3.0, die mit der ursprünglichen Seite jedoch nur den Namen gemeinsam hatten. Weitere Plattformen dieser Art wie Agora, AlphaBay, Evolution, Project Black Flag, Wall Street Market oder Hansa kamen und gingen. Einige davon wurden von der Polizei ausgehoben, andere stellten den Betrieb ein, nachdem sich die Betreiber mit den Bitcoins der Kunden aus dem Staub gemacht hatten (Exit Scam).

Auch Deutsche mischten im illegalen Online-Geschäft mit. So zählte Sascha Flamm aus Bayern zu den umsatzstärksten Händlern auf Silk Road, bevor ihn die Polizei im Sommer 2014 (drei Monate vor der Verhaftung Ulbrichts) festnahm. Ein Gericht verurteilte ihn zu siebeneinhalb Jahren Gefängnis.Das konnte den illegalen Handel hierzulande jedoch nicht stoppen. Als internationale Ermittler im Mai 2019 das Portal Wall Street Market hochnahmen, verhafteten sie drei Verdächtige aus Bad Vilbel, dem Landkreis Esslingen und Kleve.

## Beweisaufnahme

Doch wie kamen die Ermittler Ross Ulbricht überhaupt auf die Spur? Silk Road lief im Darknet, jenem Teil des Internets, das mit kryptografischen Techniken gegen staatliche Mitleser geschützt ist und außerdem ein hohes Maß an Anonymität bietet. Auch die zahlreichen Nachfolger von Ulbrichts illegaler Plattform nutzen dieses schwer kontrollierbare Netzwerk, das mit Hilfe von mehreren tausend speziell konfigurierten Routern betrieben wird. Das übliche Zahlungsmittel im Darknet sind Kryptowährungen. Silk Road akzeptierte ausschließlich die damals noch neue Zahlungsmethode Bitcoin. Auf heutigen Darknet-Märkten kann man meist auch mit anderen Blockchainwährungen bezahlen.

Als zusätzliche Sicherheitsmaßnahme administrierte Ross Ulbricht Silk Road nie von zu Hause aus, sondern nutzte beispielsweise den Internet-Zugang einer Bibliothek. Er verwendete außerdem eine Lösung zur Full Disk Encryption (FDE), um die Daten auf seinem Laptop zu schützen. FDE sorgt dafür, dass im Normalzustand alle Daten auf der Festplatte verschlüsselt sind und nur die gerade gebrauchten Informationen entschlüsselt werden. Wenn der Nutzer beispielsweise den Bildschirm sperrt, verschlüsselt die FDE-Lösung automatisch sämtliche Nutzdaten. Wer einen gesperrten FDE-gesicherten Rechner klaut, kann daher die darauf gespeicherten Informationen nicht lesen.

## Don't talk about Fight Club

Ulbrichts Sicherheitskonzept für Silk Road war durchaus durchdacht und nicht leicht zu knacken. Dennoch kamen ihm die Ermittler auf die Schliche. Einen entscheidenden Fehler machte Ulbricht bereits in der Anfangsphase, als er am 27. Januar 2011 unter dem Pseudonym „altoid“ in einem Diskussionsforum auf Silk Road hinwies („Has anyone seen Silk Road yet?“), um Werbung in eigener Sache zu machen. Die Plattform war zu diesem Zeitpunkt erst seit wenigen Tagen online und so gut wie unbekannt. Dieser frühe Hinweis fiel später dem Ermittler Gary L. Alford auf. Er vermutete – zu Recht –, dass hinter dem Beitrag der Betreiber von Silk Road selbst oder jemand aus dem unmittelbaren Umfeld steckte. Ulbricht hatte die erste Regel aus dem Film „Fight Club“ gebrochen und über seine illegale Plattform gesprochen. Nach kurzer Suche fand Alford im selben Forum ein weiteres Posting von altoid zu einem anderen Thema. Dieses enthielt eine E-Mail-Adresse: rossulbricht at gmail dot com.

Kurz darauf entdeckte der Zoll bei einer Routinekontrolle an der kanadischen Grenze ein an Ulbricht adressiertes Paket mit gefälschten Reisepässen, die alle dessen Foto trugen. Dies passte zu einem Beitrag von Dread Pirate Roberts im Silk-Road-Forum, in dem er von falschen Pässen berichtete, mit denen er zusätzliche Server anmieten wollte. In der Zwischenzeit war es dem FBI gelungen, die IP-Adresse des Silk-Road-Servers herauszubekommen – ein Konfigurationsfehler hatte dies möglich gemacht. Die Spur führte nach Island, wo die Behörden den Rechner ausfindig machten und die darauf gespeicherten Daten dem FBI zur Verfügung stellten. Ein Teil des Codes glich einem Programmiertipp, den Ulbricht unter seinem Klarnamen in einem Onlineforum erhalten hatte.

Das FBI hatte nun endlich einen Verdächtigen, gegen den sich schnell weitere belastende Indizien fanden. Schließlich erging ein Haftbefehl. Die Ermittler mussten jedoch noch eine letzte Hürde überwinden, die transparente Festplatten-Verschlüsselung (FDE), die Ulbricht mutmaßlich nutzte. Es war klar: Gelang es Ulbricht, seinen Laptop vor der Verhaftung zu sperren, waren sämtliche darauf gespeicherten

Daten unlesbar. Die Polizisten ließen sich daher den Trick mit dem vermeintlichen Liebespaar einfallen, das Ulbricht ablenkte – mit Erfolg.

## Abwehrtechnik

Doch die Betreiber der nachfolgenden illegalen Plattformen lernten schnell aus dem Silk-Road-Fall und verfeinerten ihre Tarnung. Einige anarchistisch angehauchten IT-Spezialisten reagierten auf die Umstände, unter denen Ulbricht festgenommen wurde, und entwickelten Tools, die der Polizei den Zugriff auf einen Laptop bei laufendem Betrieb erschweren sollen. Ein anonymer Programmierer, der sich Hephaest0s nannte, veröffentlichte beispielsweise eine kostenlose Software namens USBKill. Diese führt eine Liste von USB-Geräten, die auf dem jeweiligen Rechner als vertrauenswürdig gelten. Steckt jemand ein nicht gelistetes Gerät ein (beispielsweise einen USB-Stick, der die Festplatte spiegeln soll), dann sperrt das Programm das Betriebssystem und verschlüsselt gleichzeitig alle Daten.

Für eine ähnliche Zielgruppe stellte der Software-Entwickler Michael Altfield Anfang des Jahres eine Lösung namens BusKill vor. Diese sieht vor, dass der Nutzer eines Laptops ein USB-Kabel in den Rechner steckt, dessen anderes Ende er an seinem Gürtel befestigt. Zieht jemand den Laptop weg und wird dabei der USB-Stecker herausgezogen, dann startet auf dem Rechner ein Programm, das beispielsweise den Bildschirm sperrt und die Festplatten-Verschlüsselung in Gang setzt.

Etwas bequemer und schon länger erhältlich sind kontaktlose RFID-Tokens, die den Computer sperren, sobald sich der Nutzer von diesem entfernt. Solche Tokens sollen in erster Linie sicherstellen, dass ein PC-Anwender seinen Bildschirm sperrt, wenn er den Arbeitsplatz verlässt – sie lassen sich aber auch nutzen, um der Polizei die Beschlagnahme eines Rechners zu erschweren.

Ebenso wurden Krypto-Währungen weiterentwickelt. Für anonyme Geldgeschäfte mit Bitcoin existieren sogenannte Bitcoin-Mixer, die mittels zufälliger Auszahlungen aus einem geteilten Pool die Herkunft einer Zahlung verschleiern. Darüber hinaus sind in den letzten Jahren mehrere BitCoin-Alternativen entstanden, die mehr Anonymität bieten als das Original. Sie werden als Privacy Coins bezeichnet. Bekannte Vertreter heißen Monero, Dash und Zcash. Diese Systeme verwenden verschiedene Techniken, um eine Geldübertragung zu verschleiern. Zum Einsatz kommen beispielsweise Dummy-Signaturen, die von relevanten Signaturen ablenken, nur einmal verwendete Adressen, Zero-Knowledge-Protokolle und ähnliche Methoden. Es ist sicherlich kein Zufall, dass gerade Privacy Coins als Zahlungsmittel auf den heutigen Darknet-Plattformen besonders oft anzutreffen sind – und deshalb in der Kritik stehen.

## Hoffnung auf Begnadigung

Beim Kampf gegen die Drahtzieher im Darknet sind die Ermittler also mal mehr, mal weniger erfolgreich. Wenn die Falle einmal zuschnappt und Richter ein Exempel statuieren wollen, besteht wenig Hoffnung für die Ertappten.

Nach dem Urteil reichten die Anwälte von Ross Ulbricht einen 145-seitigen Antrag ein, in dem sie auf zahlreiche vermeintliche Fehler im Verfahren hinwiesen, um das Urteil anzufechten. Insbesondere verwiesen sie darauf, dass sich zwei der Ermittler illegal mit Bitcoins bereichert hatten und zu mehrjährigen Haftstrafen verurteilt wurden. Im Prozess durfte dies gegenüber der Jury jedoch nicht erwähnt werden.

Laut den Verteidigern erschien es möglich, dass die beiden Beamten falsche Beweise auf Ulbrichts Laptop platziert hatten, um von ihren Taten abzulenken. Dieser Antrag sowie ein weiterer, der die Verfassungsmäßigkeit der Überwachung von Ulbrichts Internetverkehr und der Höhe des Strafmaßes in Zweifel zog, wurden jedoch abgewiesen. Das Urteil gegen Ulbricht wurde damit rechtskräftig.

Ulbrichts letzte Hoffnung ist die Öffentlichkeit und eine Begnadigung durch den US-Präsidenten. Derzeit wächst in den USA die Kritik an der Schwemme von „Life without parole"-Urteilen, die auf Gesetzesverschärfungen aus den Achtzigerjahren beruhen. Im Rahmen des „War on Drugs" versuchte die Regierung damals, Drogenhändler durch besonders strenge Gesetze abzuschrecken. Mittlerweile fragen sich jedoch viele, ob man im Kampf gegen Drogen tatsächlich Tausende von Personen Jahrzehnte lang wegschließen muss, die nie Gewalt angewendet haben und bei denen die Rückfallgefahr äußerst gering ist.

Einige Prominente sprechen sich inzwischen für eine Begnadigung Ulbrichts aus. Dazu zählen der Linguist Noam Chomsky und der Schauspieler Keanu Reeves. Es erscheint daher möglich, dass eine US-Regierung die Gesetze irgendwann entschärft und bestehende Haftstrafen reduziert.

Ulbricht und seine Mitstreiter hoffen, dass sie Donald Trump oder einen zukünftigen US-Präsidenten milde stimmen können. Ulbrichts Mutter Lyn informiert auf der Webseite Freeross.org über den Fall und die Widersprüche in den Ermittlungsakten. Um ihrer Forderung Nachdruck zu verleihen, startete sie 2018 eine Online-Petition zur Freilassung ihres Sohnes, die inzwischen 250.000 Unterschriften gesammelt hat. *(hag@ct.de)* c't

Bild: Michael Altfield

**Nach der Verhaftung von Ulbricht nutzen Betreiber anderer illegaler Plattformen besondere Vorsichtsmaßnahmen wie die USB-Sicherung BusKill: Greifen Behörden zu und trennen den Träger von seinem Laptop, werden die Daten sofort verschlüsselt oder zerstört.**