IWW INSTITUT
INFORMATIONSDIENSTE

STRAFRECHT

Ermittlungen im Darknet: Schwarzmarkt 2.0 und die Instrumente der Strafverfolgungsbehörden

von RAin Diana Nadeborn, Berlin

| Ein sehr kleiner Teil des Internets erfährt durch spektakuläre Prozesse wie das Verfahren gegen den Darknet-Waffenhändler Philipp K. vor dem Landgericht München I große Aufmerksamkeit. Welche Technologie steckt hinter dem modernen Schwarzmarkthandel? Und welche Instrumente stehen den Strafverfolgungsbehörden zur Verfügung? DR gibt die Antworten. |

Schwarzmarkt 2.0

Jeder IWW-Leser nutzt das Surface Web, den durch Suchmaschinen indexierten Teil des Internets. Eine fünfhundertfach größere Datenmenge findet der geneigte Nutzer aber im Deep Web, dem nicht durch Google, Bing & Co. indexierten Teil. Dazu gehören alle Webseiten, die nur einem eingeschränkten Nutzerkreis zugänglich sind, seien es kostenpflichtige Angebote oder Dienste unter Verwendung von Privatsphäre-Einstellungen. Ein kleiner Teil des Deep Web ist das Darknet, das nur durch den Tor Browser erreicht werden kann. Der Tor Browser, dessen Nutzung kostenlos und legal ist, ermöglicht durch mehrere hintereinander geschaltete verschlüsselte Verbindungen, die durch Server (nodes) verbunden sind, die Verschleierung der IP-Adresse des Nutzers. Somit können die Ermittler weder die von Seitenbetreibern gespeicherten IP-Adressen noch die im Rahmen der Vorratsdatenspeicherung nach §§ 113a, b TKG gespeicherten Verkehrsdaten zu einer Identifikation des Standorts des tatverdächtigen Internetnutzers heranziehen (Safferling/Rückert, Das Strafrecht und die Underground Economy, Konrad-Adenauer-Stiftung, Februar 2018, 6, www.kas.de/wf/de/33.51506).

Über den Tor Browser sind zum einen allgemein zugängliche Angebote wie iww.de erreichbar. Zum anderen sind die sogenannten Hidden Services erreichbar, die an der Endung .onion erkennbar sind. Hier ist auch die IP-Adresse des Anbieters verschleiert. Die Technologie der Hidden Services verwendeten auch Betreiber von Marktplätzen wie Silk Road, Alpha Bay und Hansa Market, auf denen Drogen, Waffen und Kreditkartendaten gehandelt wurden.

Hauptziel der Ermittlungen: die Administratoren

Der Betreiber eines solchen Marktplatzes fungiert als Mittler zwischen Käufer und Verkäufer und nimmt bei jedem Vertragsschluss eine Provision ein. Auf ihn konzentrieren sich typischerweise zunächst die Ermittlungen, berichtete Kriminalhauptkommissar Jürgen Gause, Leiter der Internetermittlungen im Bundeskriminalamt, auf dem Erlanger Cybercrime Tag 2018. Niederländischen Kollegen sei es bei den Ermittlungen gegen Hansa Market gelungen, den Server zu lokalisieren, auf dem der Hidden Service gehostet wurde. Da die beiden Betreiber auf demselben Server auch einen Privatchat abgelegt hätten, hätten deutsche Ermittler Rückschlüsse auf deren Identität zie-

hen und diese im Juli 2017 verhaften können. Dabei seien 1.400 Bitcoins im Wert von über 10 Mio. Euro sichergestellt worden. Die staatliche Veräußerung einer so großen Menge Bitcoins sei problematisch, da sie den Kurs der volatilen Währung beeinflussen könne.

Große Koalition will neuen Straftatbestand

Da auf Darknet-Marktplätzen vorrangig mit Drogen gehandelt werde, werden die Betreiber bisher wegen Verschaffung oder Gewährung einer Gelegenheit zum unbefugten Erwerb bzw. zur unbefugten Abgabe von Betäubungsmitteln gemäß § 29 Abs. 1 Nr. 10 BtMG belangt. Die Parteien der neuen Regierungskoalition haben beschlossen, einen neuen Straftatbestand wegen „Betreiben eines Darknet-Handelsplatzes für kriminelle Waren und Dienstleistungen" einzuführen (Koalitionsvertrag zwischen CDU, CSU und SPD vom 7.2.18, 128, www.cdu.de/system/tdf/media/dokumente/koalitionsvertrag_2018.pdf). Es ist also zu erwarten, dass die strafrechtliche Verantwortung für Darknet-Handel neu gefasst wird.

„Das würde allerdings zu einer enormen und damit bedenklichen Ausweitung der Vorfeldkriminalisierung führen", meint Professor Dr. Christoph Safferling, Inhaber des Lehrstuhls für Strafrecht und Strafprozessrecht an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Anderer Auffassung sind die Ermittler. Kriminalhauptkommissar Gause betonte auf dem Erlanger Cybercrime Tag 2018 vielmehr, die Formulierung des angedachten Straftatbestands gehe auf eine Initiative des BKA zurück. Es sei praktischer, nicht auf einen Spezialtatbestand zurückgreifen zu müssen. Die Strafbarkeit der Betreiber wegen Beihilfe zu den Straftaten der Nutzer der Darknet-Marktplätze bilde den Unrechtsgehalt nicht ausreichend ab, pflichtete ihm Staatsanwalt Cai Rüffer, Dezernent für Darknet-Verfahren in der Zentralstelle für Internetkriminalität, bei.

Kontaktpunkte in der Realwelt und verdeckte Ermittlungen

Da die Verkäufer Drogen und Waffen übergeben und Kryptowährungen zurücktauschen müssen, stehen den Ermittlern über diese Kontaktpunkte der digitalen mit der realen Welt eine Reihe von Zugriffsmöglichkeiten zur Verfügung. Paketdienste und Banken können Ausgangspunkte für strafrechtliche Ermittlungen sein.

Seit 2015 führten verdeckte Ermittlungen im Darknet zu Ermittlungserfolgen und mündeten aufgrund der hohen Straferwartungen im Bereich der Betäubungsmittel-Delikte und des Waffenhandels fast ausnahmslos in Untersuchungshaft und Verurteilungen zu mehrjährigen Freiheitsstrafen (Oberstaatsanwalt Andreas May, BKA Herbsttagung 2017, Beitrag am 16.11.17, www.bka.de/DE/AktuelleInformationen/Publikationen/BKA-Herbsttagungen/2017/ProgrammUndRedebeitraege/programmUndRedebeitraege_node.html). Als einfachste Maßnahme können Ermittler als sogenannte nicht öffentlich ermittelnde Polizeibeamte (noeP) auf „Online-Streife" gehen. Rechtsgrundlage ist die Ermittlungsgeneralklausel gemäß §§ 161, 163 StPO. Als verdeckte Ermittlungsmaßnahme kommt vor allem das Einschleusen von

Polizeibeamten als Käufer, Verkäufer oder sogar Moderatoren/Administratoren auf Darknet-Handelsplätzen in Betracht. Rechtsgrundlage hierfür ist § 110a StPO.

Die auf dem Server gespeicherten Daten der Nutzer stellen zusätzliche Beweismittel dar. Aufgrund der Anonymität im Darknet, die einen Betrug gegenüber den Kunden erleichtert, sind Kundenbewertungen besonders wichtig, um eine Vertrauensbasis zu den Verkäufern zu schaffen. I. d. R. sei die Abgabe einer Bewertung erst nach Abschluss eines Geschäfts möglich, erklärte Staatsanwalt Rüffer auf dem Erlanger Cybercrime Tag 2018. Werbe der Verkäufer außerdem mit der durchschnittlichen Verkaufsmenge, könne der Staatsanwalt Anzahl und Umfang der Verkäufe hochrechnen und auf dieser Basis einen Haftbefehl beantragen.

Zugriff auf verschlüsselte Kommunikation

Darknet-Foren dienen dem Meinungsaustausch und der Kontaktanbahnung. Sollen illegale Geschäfte abgewickelt werden, wechseln die Interessenten zu Messenger-Diensten wie WhatsApp, Threema & Co., die inzwischen alle standardmäßig Ende-zu-Ende verschlüsselt sind. Gelingt es den Ermittlern, die Endgeräte eines bereits identifizierten Beschuldigten mit einem Staatstrojaner zu infiltrieren, können sie die Kommunikation vor bzw. nach der Verschlüsselung ausleiten (sogenannte Quellen-Telekommunikation gemäß § 100a Abs. 2 StPO). Hierfür müssen Schwachstellen auf dem Zielsystem vorhanden sein. Schwachstellen zu erhalten, statt sie dem Hersteller zu melden, ist damit eine Voraussetzung für den Einsatz des Staatstrojaners.

Eine technische Alternative wäre die Verpflichtung der Messenger-Diensteanbieter, eine Schnittstelle zu implementieren, damit Ermittler auf die Inhalte der Kommunikation zugreifen können. Diese Hintertür stünde aber ebenfalls nicht nur Strafverfolgungsbehörden, sondern auch Cyberkriminellen offen. Eine Tür, die in Deutschland – bisher – nicht aufgestoßen wurde.

ZUR AUTORIN | Die Autorin Diana Nadeborn ist Strafverteidigerin in Berlin und betreibt den Blog www.it-strafrecht.org.