Vom deutschen Zoll sichergestelltes „Crystal Meth“: Synthetische Drogen werden auch über das „Darknet“ gehandelt.

Die finstere Seite des Internets

Raubkopien, illegale Drogen, Kinderpornografie: Im „Darknet“ ist das Verbotene nur einen Mausklick entfernt. Anonym vernetzen sich Kriminelle ebenso wie Pädophile und Freiheitskämpfer.

Das „Darknet“ ist mit Suchmaschinen wie „Google“ nicht auffindbar. Ihre Suchalgorithmen scheitern an den zugangsbeschränkten Foren, Datenbanken und Katalogen. Im Gegensatz zum „normalen“ Internet gibt es im „Deepweb“ und in den „Hidden Services“, wie das Darknet auch genannt wird, keine zentralen Server zum Datenabruf. Es wird aus privaten PCs gebildet, die untereinander verschlüsselt Daten bereitstellen, abrufen und weiterleiten.

„Tor“ ins Dunkel. Ermöglicht wird der anonyme Austausch unterschiedlichster Inhalte vor allem durch das Netzwerk „Tor“ („The Onion Router“). Um diese digitale Tür benutzbar zu machen, muss ein Software-Paket („Tor Browser Bundle“) installiert werden, das sich in den Browser einklinkt. Es verschleiert die IP-Adresse des Users, indem eine lange Verbindungskette kreiert wird und das Betreiben verborgener Server ermöglicht. Rund 5.000 Server, sogenannte „Knoten“, hängen in diesem Netz. Jeder Server kennt nur den Knoten davor und danach. Passiert ein Datenpaket drei Server, ist die IP-Adresse des Absenders nicht mehr ermittelbar, da die Daten nach jedem Knoten neu verschlüsselt werden. Hinzu kommt, dass alle zehn Minuten die Verbindung neu aufgebaut wird.

Nach der Installation von „Tor“ können gewöhnliche Seiten nach wie vor angesteuert werden, daneben gelangt der User mithilfe des digitalen Portals auch zu illegalen Inhalten. So finden sich im „finsteren“ Teil des Netzes etwa illegale Film-Downloads, raubkopierte Musikdateien sowie Anbieter von verbotenen Drogen. Kontakte zu Auftragskillern sind ebenso in Umlauf wie verbotenes pornografisches Material. Auch die Rubriken „Geldwäsche“, „gefälschte Dokumente“ und „Waffenhandel“ sind im Untergrundnetz anzutreffen. Bezahlt wird mit der digitalen Währung „Bitcoins“, wofür abermals eine eigene Transaktions-Software installiert werden muss.

Dissidenten und Datenschützer. Neben Dealern und Pädophilen sind im virtuellen Rückzugsraum auch überzeugte Datenschützer und verfolgte Dissidenten anzutreffen. Etwa syrische Aktivisten finden den Weg in die digitale „Terra incognita“, um sich zu vernetzen ohne von Kräften des Regimes ertappt zu werden. Auch Journalisten nützt das Netzwerk immer wieder, um Kontakt mit „Quellen“ aufzunehmen – ein Vorgehen, das dem Leitgedanken der Darknet-Entwickler entspricht. Ab Mitte der 1990er-Jahre suchten For-

FOTO: DEUTSCHE BUNDESZOLLVERWALTUNG

scher am *U.S. Naval Research Lab* nach Möglichkeiten, die Online-Kommunikation der US-Marine gegen Spionage abzusichern. Seit 2006 wird „Tor“ von einem gemeinnützigen Verein betreut, zu dem unter anderem der Netz-Aktivist Jacob Appelbaum zählt, der sich zuletzt für Edward Snowden und zuvor für den Gründer der Plattform „Wikileaks“, Julian Assange, eingesetzt hat.

Viren und Komplizen. Wie in einem legalen (Online-)Geschäft besteht im Darknet die Möglichkeit, sich das Angebot anzusehen. Der Download von Raubkopien oder das Anfordern von Drogen wird ebenso geahndet, wie die „Komplizenschaft“. Ab der Installation von „Tor“ bzw. der „Tor“-Browser-Einstellung „Relaisverkehr“ ist nicht mehr kontrollierbar, welche kriminellen Geschäfte über den eigene Computer transferiert werden. Der Einzelne wird damit zum Mittäter. Eine weitere Gefahr im Darknet stellen Viren, Trojaner und andere Schadsoftware dar.

Coup auf der „Seidenstraße“. So verschlungen die Wege des Deepweb auch sind, immer wieder gelingt es den Ermittlern, Dealer aufzugreifen. Der bisher spektakulärste Coup ereignete sich im Jänner 2011: Auf der „Silk-Road“ (eine Anspielung auf die frühere Handelsroute, die von Asien nach Europa verlief) wurden Drogen, Hackerdienste, gefälschte Ausweise und Waffen gehandelt. Es wird geschätzt, dass an die 20 Prozent der US-amerikanischen Drogenhändler die „Einkaufsstraße“ für ihre Geschäfte nutzten. Laut Angaben des FBI soll hier innerhalb von drei Jahren 1,2 Milliarden Dollar Umsatz gemacht worden sein. Mithilfe von Undercover-Agenten konnten mehrere „Big Player“ gefasst werden. 2013 folgte ein weiterer Schlag: Das FBI erhielt Zugang zu 1,2 Millionen Finanztransaktionsdaten – wie, ist bis heute unklar. Kurz darauf folgten weltweit Verhaftungen, das Netzwerk wurde stillgelegt. Es dauerte nicht lange und Nachfolgerplattformen nahmen den Betrieb auf.

Auch der österreichischen Polizei gelangen bereits mehrere Zugriffe auf „Hidden Services“. So konnten im Frühjahr zwei Niederösterreich aufgegriffen werden, die Drogenpakete auf einem niederösterreichischen Postamt aufgeben wollten. *Hellin Sapinski*