Im Untergrund

◢ Würde man das **Internet** auf DIN-A4-Seiten ausdrucken, bräuchte man mehr als 135 Milliarden Blatt Papier. Doch dieser sichtbare Teil des WWW macht nur ein Drittel aller Inhalte aus. Das ___**DARKNET**___ ist noch erheblich größer. Auf den nicht-indexierten Seiten verticken ___**KRIMINELLE**___ aus aller Welt Drogen, Waffen und gefälschte Papiere. ›

◢ Mitten in der Sciencefiction-Abteilung einer Stadtbücherei von San Francisco schnappten die Fahnder zu. Die Verhaftung des Chefs des größten kriminellen Marktplatzes im Internet war ähnlich skurril wie sein rasanter Aufstieg. Dread Pirate Roberts, mit bürgerlichem Namen Ross Ulbricht, hatte seine Website Silk Road innerhalb von drei Jahren zu einer einzigartigen Plattform ausgebaut. Gehandelt wurden dort vor allem Drogen aller Art. Aber auch Waffen, Schadsoftware, gestohlene Bank- und Kreditkartendaten, Falschgeld, Kinderpornos und Auftragsmorde. Über 1,5 Millionen Transaktionen im Gesamtwert von mehr als 1,2 Milliarden US-Dollar wurden zwischen tausenden Verkäufer- und über 100 000 Käuferkennungen ausgeführt. Bis 2013, zum Zeitpunkt seiner Verhaftung, hatte der damals 29-jährige Ulbricht mit seinem Startup 80 Millionen Dollar an Provisionsgebühren eingenommen. Die Quittung: Im Mai 2015 wurde er zu einer lebenslänglichen Haftstrafe verurteilt.

Die Behörden machten zwar Silk Road vorläufig ein Ende, doch es dauerte nicht lange, bis die Idee mit neuem Management wieder auflebte. Es entstanden ähnliche Marktplätze, die auch die Vorteile des Darknets für sich nutzen. Inzwischen gibt es dutzende Plattformen, neue Kanäle kommen und gehen. Das Darknet oder Deep Web ist um ein Vielfaches größer als das frei zugängige Web. Es besteht aus nicht-indexierten Webseiten, die von Suchmaschinen wie Google nicht gefunden werden können. Das Darknet nutzt Verschlüsselung und Peer-to-Peer-Kanäle, um die IP-Adressen der Nutzer zu verbergen und so deren Anonymität zu schützen. Das „dunkle Netz“ arbeitet also dezentral. Jeder Computer speichert verschlüsselt nur einen Teil der nötigen Informationen. Die Datenpakete werden über drei zufällig ausgewählte Rechner verschickt. Mit jeder Zwischenstation erhält ein Paket so eine andere Absenderadresse und es ist am Ende nicht mehr nachvollziehbar, von welchem Rechner aus die Daten losgeschickt wurden. Allerdings ist das Surfen im Darknet dadurch deutlich langsamer als im regulären Internet. Die Anonymität wird auch dadurch geschützt, dass es tausende von Chatrooms und Foren gibt, an denen man sich nur auf Einladung beteiligen kann. Das gilt besonders für die Schwerkriminalität. Wer die genaue alphanumerische Adresse nicht kennt, bleibt außen vor. Trotz konzertierter Aktionen der Strafverfolgungsbehörden ist die Anzahl der gelisteten Produkte in den Märkten jedes Jahr mit zweistelligen Prozentraten gewachsen. Der Drogenhandel im Darknet erzielt täglich einen Umsatz von 300 000 bis 500 000 Dollar. Nach Schätzungen des Bundeskriminalamts kaufen bis zu einer Million Menschen allein in Deutschland dort Drogen, Waffen, gefälschte Personalausweise und Pässe.

TOR-Browser-Bundle: der Eingang in die vernetzte Unterwelt

Der populärste Zugang zum Darknet ist das Netzwerk TOR (The Onion Router). Die Software kann jedermann auf www.torproject.org herunterladen. Wie der Sicherheitsexperte und langjährige Interpolberater Marc Goodman in seinem Buch „Future Crimes“ schreibt, routet der Anonymisierungsdienst TOR Anfragen über 5000 Server weltweit. Sie werden von Privatleuten und Unis betrieben. Der 2004 gegründete Dienst wurde vom US Naval Research Laboratory finanziert. Anfänger können sich zunächst auf Wikis und Übersichtsseiten orientieren. Dort finden sie eine Sammlung von Adressen für das dunkle Web. Seit 2014 gibt es sogar eine erste Suchmaschine: Grams sucht auf acht Marktplätzen des Darknets – und das sogar mit bezahlter Werbung wie Google AdWords. Kommunizieren kann man unter anderem mit Tormails. Sie können nur im Darknet versendet und empfangen werden und sind PGP-verschlüsselt. „TOR wird von Kriminellen genutzt, zum Beispiel für Erpressungen und die Vorbereitung von Straftaten. Es gibt aber durchaus lautere Zwecke, denen TOR dient: Möchten sich zum Beispiel Regimekritiker in Diktaturen austauschen, so ist dies nach unserem Verständnis

absolut legitim. Das Gleiche gilt für Patienten oder Personen in einer Lebenskrise, die ohne Preisgabe ihrer Identität mit Gleichgesinnten in Kontakt treten wollen“, sagt Sebastian Schreiber, Geschäftsführer des IT-Sicherheitsunternehmens Syss. Da er Penetrationstests für Kunden durchführt, beschäftigt er sich intensiv mit dem Darknet. Schätzungen des kriminellen Anteils von TOR schwanken zwischen 50 und 85 Prozent. Zwei Millionen Nutzer greifen täglich darauf zu. Dazu zählen Al-Qaida, aber auch das US-Militär, Menschenrechtler und politisch Verfolgte. Absolute Anonymität vor Überwachern kann TOR jedoch nicht gewährleisten. Angeblich war die NSA sogar an der Entwicklung des Netzwerks beteiligt und konnte dadurch eine Schwachstelle einbauen, die sie später ausgenutzt hat. Auf alle Fälle erschwert TOR es den Geheimdiensten, die Nutzer auszuspionieren. Je mehr Menschen es einsetzen, desto höher wird der Überwachungsaufwand für die Behörden. Auch aus diesem Grund propagiert der US-Netzaktivist und Überwachungskritiker Jacob Appelbaum, ein wichtiges Mitglied des TOR-Projektteams, seit dem NSA-Skandal die Nutzung des virtuellen Identitätsschutzes. Ein anderer Zugang ins Deep Web ist Freenet: Dafür gibt jeder Nutzer Speicherplatz auf seinem Rechner frei und macht ihn so zum Teil des Darknets. Eine weitere Alternative zu TOR ist I2P (The Invisible Internet Project).

Betrug und Erpressung im Darknet: Es kann jeden treffen

Anonymität ist auch beim Bezahlen der gekauften Waren oberstes Gebot. Käufer und Verkäufer setzen meist auf die Internetwährung Bitcoin. Sie besteht aus Dateien, die man anonym austauscht. Die Bitcoins landen so in einem digitalen Portemonnaie. Sie können nicht beliebig vermehrt werden und lassen sich legal in reales Geld umtauschen. Wohin sie im Darknet überwiesen werden, kann man nicht zurückverfolgen, denn die Vertragspartner tragen Decknamen. „Früher nutzten die Täter Western Union, jetzt Bitcoins. Dadurch sind die Aufklärungsraten der Polizei stark gesunken“, sagt Schreiber. Die wirtschaftliche Bedeutung des dunklen Netzes lässt sich nur grob einschätzen, da es naturgemäß keine Statistiken gibt. Viele Milliarden schwer ist der Markt an kriminellen Gütern aber auf alle Fälle. Da Cyberkriminalität in den vergangenen Jahren einen starken Aufschwung genommen hat, erfreuen sich auch die dunklen Ecken des Internets steigender Beliebtheit. Für IT-Angriffe muss man heute kein Hacker mehr sein, denn Sicherheitslücken und die passende Schadsoftware dafür samt versiertem Experten lassen sich problemlos auf den Schattenmärkten einkaufen. „Durch das Darknet hat sich ein spezialisiertes Betrugs- und Erpressungssystem entwickelt. Auch Mittelständler und Freiberufler sind ins Visier geraten. Wer zum Beispiel gezielt Steuerberater durch Datendiebstahl erpressen will, findet im Darknet darauf spezialisierte Cyberkriminelle“, erklärt Götz Schartner, professioneller Hacker im Auftrag von Unternehmen, Banken und Regierungen und Autor des Buchs „Vorsicht, Freund liest mit!“. Angriffe auf kleine Unternehmen haben zudem den Vorteil, dass sie technisch leichter zu bewerkstelligen sind, als einen Konzern zu hacken. Im Trend liegt insbesondere Ransomware – Schadprogramme, mit denen ein Eindringling den Zugriff auf Daten oder auf das gesamte Computersystem verhindert. Dabei werden die Daten auf einem fremden Computer verschlüsselt, um für die Entschlüsselung oder Freigabe ein Lösegeld zu fordern. Darüber hinaus werden auch Geschäftsgeheimnisse gehandelt. Schreiber berichtet: „Wir haben schon Passwortlisten eines Kunden im Darknet gefunden.“ Buchstäblich auf den Punkt bringt den Geschäftszweck der Name eines Marktplatzes für gestohlene Kreditkartendaten, nämlich die International Association for the Advancement of Criminal Activity (IAACA). Unternehmen sind gut beraten, ihre Arbeitnehmer über die Risiken des Darknets aufzuklären und sie zu sensibilisieren. Schließlich nutzen viele Mitarbeiter auch zu Hause den Firmen-Laptop, mit dem sie sich privat im Darknet tummeln können. „Wenn dabei zu oft Server genutzt werden, die überwacht werden, drohen Razzien. Man muss bedenken, dass der Polizei auch Fahndungsfehler passieren. Eine Razzia hat für ein Unternehmen fatale Folgen. Es kommt dann zum Stillstand“, sagt Schartner. Er rät daher zum Sperren von TOR und zu einer Überwachung durch die Unternehmens-IT.

Autor: Ulrich Hottelet

Illustration: Wenceslas Hollar Digital Collection

Keine Straffreiheit.
Polizei patrouilliert im Darknet

Händler und Käufer illegaler Güter fühlen sich im Darknet sicher vor Strafverfolgung. Dass sie sich dabei irren, zeigte Mitte November 2015 das gemeinsame Vorgehen des Bundeskriminalamtes und einiger Landespolizeibehörden gegen Falschgeldverbreiter. In mehreren Bundesländern wurden zahlreiche Wohnungen durchsucht. Die Betroffenen standen im Verdacht, Falschgeld im Darknet bestellt und mit digitaler Währung bezahlt zu haben. Der Versand der Noten erfolgte auf dem Postweg. Bei den bestellten Falsifikaten handelte es sich um Fälschungen von 20- und 50-Euro-Noten, die in Italien hergestellt wurden. Die mittels Offset-Druckverfahren produzierten Falschnoten waren von guter Qualität und im üblichen Bargeldverkehr nur schwer als „Blüten“ zu erkennen.