DR.
ALLWISSEND

Wie funktioniert eigentlich das Darknet?

DAS DUNKLE NETZ ist leichter zu erreichen, als die meisten glauben: Man braucht nur einen speziellen Browser, den man mit einer einfachen Websuche finden kann, oder ein spezielles Betriebssystem. Wenn das World Wide Web eine globale Megacity ist, dann ist das Dark Web ein Bahnhofs- oder Hafenviertel bei Nacht: Man bewegt sich dort unerkannt, illegale Geschäfte werden gemacht, Arglose abgezockt, Geheimnisse ausgetauscht und erstaunlich offene Gespräche zwischen Wildfremden geführt. Das Dark Web ist nur ein winziger Teil des Internets, aber vielen gilt er als der, in dem die alten Netz-Ideale aus den Neunzigerjahren noch gültig sind: totale Anonymität, absolute Meinungsfreiheit, Abwesenheit von Überwachung und staatlicher Gängelung. Ein Ort der Anarchie.

Genau genommen gibt es mehrere Dark Webs, aber das größte und bekannteste basiert auf Tor, einem Anonymisierungsdienst, der einst von Wissenschaftlern des US-Militärs entwickelt wurde, um die Kommunikation von Spionen zu verschleiern. Tor stand ursprünglich für The Onion Router, einen Verweis auf die Zwiebelschalentechnik, die dem Dienst zugrunde liegt: Wer über dieses Netz im Netz online geht, schickt alle Datenpäckchen in diverse Schichten Verschlüsselung verpackt in ein Labyrinth aus Servern, betrieben von Freiwilligen rund um den Globus. Die Päckchen werden dort nach einem absichtlich chaotischen Prinzip hin und her geworfen, bis sich ihre Herkunft nicht mehr herausfinden lässt. Wer im WWW eine Website aufruft, der hinterlässt eine Datenspur, die sich auf seinen Internetanschluss zurückführen lässt. Ruft er dieselbe Website aber über Tor auf, tut er das nicht.

Das eigentliche Dark Web versteckt sich innerhalb des Labyrinths: Man kann ganze Websites im Tor-Netzwerk verbergen, etwa Onlineshops, die nicht Bücher und Katzenfutter verkaufen, sondern Ecstasy, Heroin und LSD. Diese Websites werden „hidden services“ genannt, versteckte Dienste, und man kann sie ausschließlich über Tor erreichen. Ihre Adressen sind kryptische Buchstabenkombinationen, und sie enden auf .onion statt auf .html. Sowohl die Nutzer als auch die Betreiber bleiben, wenn sie keine Fehler machen, anonym. Bezahlt wird mit der digitalen Kryptowährung Bitcoin, die es schwierig macht, Transaktionen konkreten Personen zuzuschreiben.

Die Anonymität dient auch ehrenhaften Zwecken: Dissidenten in Iran oder China nutzen Tor, um zu kommunizieren und sich zu informieren, Whistleblower nehmen dort Kontakt mit Journalisten auf, paranoide Freidenker philosophieren über den „Ausstieg aus der Matrix“. Sogar Facebook betreibt eine eigene Tor-Seite für Nutzer aus Staaten mit rigider Internetzensur. Doch man kann im Dark Web auch Drogen kaufen, Waffen, Handbücher für den Bombenbau, Falschgeld, gestohlene Kreditkarten – und Gewalt- und Kinderpornografie. Oder man wird bei dem Versuch von Betrügern ausgenommen, schließlich sind hier Kriminelle am Werk.

Gelegentlich schlagen die Behörden trotz Verschlüsselung und Verschleierung zu. Im November 2014 etwa schloss eine internationale Koalition, an der unter anderen das FBI und Europol beteiligt waren, auf einen Schlag 410 „hidden services“, beschlagnahmte Bargeld, Bitcoin, Drogen, Gold und Silber. Bis heute ist unklar, wie das gelang. Klar ist: Hundertprozentige Sicherheit vor Strafverfolgung kann auch das Dark Web nicht bieten. *Christian Stöcker*

OLIVER SCHWARZWALD / SPIEGEL WISSEN