idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

FernUniversität in Hagen

Carina Grewe

10/31/2024

http://idw-online.de/en/news842189

Research results
Information technology
transregional, national

Das Darknet – ein Ort voller Kriminalität?

Viele Kriminelle tummeln sich im Darknet, doch für Journalist:innen oder Verfolgte ist dies oft der einzige sichere Ort. FernUni-Infromatiker Pascal Tippe forscht zum Thema Tor Onion Services und wie Strafbehörden im Darknet ermitteln.

Wir kennen alle Berichte, in denen von kriminellen Machenschaften wie Drogen- und Menschenhandel oder Kinderpornografie im Darknet gesprochen wird. Es ist ein Ort zwischen Freiheit und Kriminalität. Einerseits ein Handelsplatz für Straftaten und illegale Güter aller Art. Kriminelle nutzen die verschlüsselte Kommunikation und können weitestgehend anonym handeln. Auf der anderen Seite bietet gerade diese Anonymität einen sicheren Ort für Journalist:innen, Whistleblower, Verfolgte oder politische Oppositionelle. So können sie die Zensur in ihren Ländern umgehen, mit anderen Personen kommunizieren und auf Missstände hinweisen. Wikileaks nutzt das Darknet, die BBC und auch der NDR in Deutschland betreiben im Tor-Netzwerk „anonyme Briefkästen“, über die Whistleblower Daten sicher übermitteln können. Andere Medien wie die Deutsche Welle betreiben ihre Webseite auch im Darknet, um der Zensur in einigen Ländern zu entgehen. Doch was ist eigentlich das Darknet?

Das Darknet ist nicht getrennt von dem Internet „dem Clear Web“, in dem wir shoppen oder mit unseren Freunden schreiben. Vielmehr ist es ein kleines Teilstück des Deep Webs. Das Deep Web bildet mit Abstand (90 % des gesamten Internets) den größten Bereich, dort befinden sich Firmendatenbanken oder Online-Speicher. Diese Inhalte sind jedoch geschützt. Daher ist auch das Darknet nicht auf die herkömmliche Weise zu finden. Nur mit Hilfe von einem Anonymisierungsnetzwerk wie Tor (ursprünglich „The Onion Routing“). Der Name beschreibt, dass es wie eine Zwiebel (englisch: Onion) aufgebaut ist. Die Identität der Nutzenden wird durch viele verschlüsselte Weiterleitungen verschleiert. Das Darknet bietet Anonymität und Schutz – und das nutzen auch Kriminelle aus. Doch die Verwendung von Tor schließt eine Zurückverfolgung nicht ganz aus.

Auswertung von US-Gerichtsdokumenten

Pascal Tippe aus dem Lehrgebiet Parallelität und VLSI der FernUniverstität forscht gemeinsam mit Adrian Tippe (Hochschule für Technik und Wirtschaft Berlin) zum Thema Tor Onion Services. „In der Literatur wird immer wieder zum Thema geforscht, aber sie betrachtet beispielsweise nicht die Nutzenden. Auch gibt es noch keine Guidelines, um das Darknet ethisch zu nutzen. Zudem wollten wir erfahren, welche Fehler Nutzende machen, die dazu führen, dass Strafbehörden ihre Identität herausfinden können“, sagt Pascal Tippe.

Als Grundlage für ihre Forschung haben sie Gerichtsverfahren in den USA untersucht, in denen Strafbehörden im Darknet ermittelten. Diese Dokumente sind in den USA öffentlich verfügbar und decken einen Zeitraum von 2011 bis 2022 ab. Insgesamt konnten 136 Fälle aus 38 von 94 US-Bezirksgerichten ausgewertet werden, was einen Großteil der relevanten Pressemeldungen mit Schlagwörtern wie "Darknet", "Tor network" und "hidden service" abdeckt. In Deutschland gibt es zu große Hürden, um eine vergleichbare Akteneinsicht zu erlangen.

Die beiden Forschenden haben bei der Auswertung verschiedene Kategorien gebildet, um zu erfahren, wie Strafbehörden die Identität der Täter:innen ermitteln konnten. Gab es zum Beispiel eine physische Komponente wie eine Hausdurchsuchung zusätzlich zur Online-Ermittlung? Oder wurden sie observiert? „Leider können wir dadurch nur die Fehler von Kriminellen untersuchen und nicht die der ethischen Tor-User, aber diese möchten und dürfen auch nicht erkenntlich gemacht werden."

Juristisch nicht klar geregelt

Bei der Aufklärung von Verbrechen im Zusammenhang mit Tor ist beiden Forschenden aufgefallen, dass diese oft problematisch ist. „Es gibt in jedem Land andere Gesetze, welche Beweise rechtmäßig zugelassen sind und welche Methoden Strafbehörden anwenden dürfen." Die Verfahren sind dabei nicht immer transparent. „Es gab einen Fall, in dem das FBI eine Schadsoftware bei einem Angeklagten einschleusen konnte. Den Code dafür wollten sie nicht herausgeben und begründeten dies damit, dass der Code im Laufe der Ermittlungen verloren ging." Ein weiteres Problem ist die technische Verifikation von digitalen Beweisen vor Gericht. Angeklagte haben oft Schwierigkeiten, die Zuverlässigkeit und Authentizität der gegen sie vorgelegten Beweise anzufechten. Die schiere Menge an Daten, die Strafverfolgungsbehörden während Ermittlungen sammeln können, erschwert es zusätzlich, alle Beweise genau zu prüfen.

Den Wissenschaftlern geht es nicht darum, dass Straftäter:innen geschützt werden, sondern darum, dass es in der Justiz in allen Ländern noch keine einheitliche Linie gibt, wie mit diesen Beweisen rechtmäßig umgangen wird. „Es kann je nach Richterin oder Richter unterschiedlich sein, ob solche Beweise zu einer Verurteilung führen. Angeklagte können diese Beweise schwer anfechten", so Tippe. Besonders komplex wird es bei internationalen Ermittlungen. Ist es dann rechtens, wenn Straftäter:innen ausgeliefert werden? Dürfen ausländische Behörden die Identität von beispielweise deutschen Staatsbürger:innen deanonymisieren und gelten diese Beweise in Deutschland? „Das sind alles Fragen, die noch nicht klar geregelt sind."

Guideline für ethische Nutzung von Tor

Gemeinsam mit Adrian Tippe hat er Guidelines für ethische Tor-Nutzende erstellt, damit diese sicher einen Tor Onion Service betreiben und nutzen können. Dort haben sie zusammengefasst, was bei einer ethischen Nutzung zu beachten ist und wie sie Fehler vermeiden, die dazu führen können, dass andere ihre Identität herausfinden. Typische Fehler sind sowohl bei ethischen Tor-Nutzenden als auch bei Straftäterinnen und Straftätern, dass sie dasselbe Pseudonym auch in sozialen Netzwerken wie Facebook verwendeten oder sie ihre private E-Mail-Adresse für eine E-Mail-Verschlüsselung hinterlegten. „Bisher gibt es noch keine Guidelines für ethisch Nutzende. Wir wollen uns an die Organisation Tor wenden. Vielleicht können die Beschäftigten dort die Guidelines nutzen und weitergeben." Tor ist mittlerweile ein organisiertes Non-Profit-Unternehmen in den USA. Es gibt Mitarbeitende, die Journalist:innen oder Whistleblower trainieren und ihnen aufzeigen, wie sie Tor sicher nutzen können. Zukünftig vielleicht auch mit dem Leitfaden von Pascal und Adrian Tippe.

Die Kriminalität bahnt sich auch anders ihren Weg

„Es gibt viele Möglichkeiten kriminellen Machenschaften nachzugehen, auch wenn das Darknet nicht mehr existieren würde", sagt Tippe. Tor ist ein wichtiger Ort für all diejenigen, die ihre Meinung nicht frei äußern dürfen. Für Menschen, die in Ländern leben, in denen es keine Presse- und Meinungsfreiheit gibt. So können sie weiterhin das Internet ungefiltert nutzen. Tor gibt die Möglichkeit, der Zensur zu entgehen und kein einzelner Staat kann hier den Fluss der Information regulieren. „Es braucht einen Schutzraum, in dem Menschen auf Missstände hinweisen können, auch in demokratischen Staaten", erklärt Tippe.

Strafbehörden immer erfolgreicher

Immer öfter gelingt es Strafbehörden die Tor-Anonymisierung auszuhebeln – ein erfolgreicher Schritt in der Bekämpfung von Kriminalität. In Recherchen des ARD-Politikmagazin Panorama und STRG_F fanden Journalistinnen und Journalisten heraus, dass Strafverfolgungsbehörden in Deutschland Server im Tor-Netzwerk teils monatelang überwachen, um Straftaten zu verfolgen. Umgekehrt bedeutet dies aber auch, dass die Zeiten für Journalistinnen und Journalisten oder politisch Verfolgten noch unsicherer werden könnten. Das Tor-Projekt steht vor der Aufgabe den Anonymitätsschutz zu verbessern, damit es auch für diese Menschen die Möglichkeit gibt, sich ohne Angst auszudrücken und auf Missstände in unserer Welt hinzuweisen.

Über Tor
Tor ist weltweit das größte Netzwerk, für Personen, die sich anonym im Netz bewegen möchten. Die Anonymität ergibt sich für Tor-Nutzende daraus, dass sie ihre Verbindung über viele verschiedene Server leiten – die Tor-Knotenpunkte. Dabei kennt jeder Server nur den Absender und Empfänger eines Datenpakets und der ursprüngliche Absender bleibt anonym. Momentan gibt es laut Recherchen der ARD 8.000 Knotenpunkte in 50 Ländern. Rund zwei Millionen Menschen nutzen täglich Tor.

contact for scientific information:
Pascal Tippe, pascal.tippe@fernuni-hagen.de

Original publication:
https://doi.org/10.56553/popets-2024-0117