VDI nachrichten
TECHNIK WIRTSCHAFT GESELLSCHAFT

http://www.vdi-nachrichten.com/Fokus/Fahndungserfolge-im-finsteren-Netz

Fahndungserfolge im finsteren Netz

05/10/17

Die Detektive im Cyber-Untergrund, ob beim Bundeskriminalamt oder die Kollegen des FBI in den USA, lassen sich bei ihrer Tätigkeit im Darknet ungern in die Karten schauen. Doch es gibt Ausnahmen.

Foto: Foto [M]: panthermedia.net/Leo Lintang/VDIn

Denken Sicherheitsexperten ans Darknet, können sie Albträume bekommen. Hier herrscht Anonymität, die klassischen Methoden polizeilicher Ermittlungsarbeit greifen nicht. IP-Nummern oder Domain-Name-Registrierungen, durch die sich gewöhnlich Betreiber illegaler Websites feststellen lassen, existieren im Tor-Netz nicht – einem Netzwerk, das auf der Anonymisierungssoftware Tor basiert (s. Kasten).

Technik hinter dem Darknet

Auch Geldströme liefern keinen Ansatzpunkt, denn im Darknet wird anonym mit Bitcoins bezahlt. Ob Bundeskriminalamt (BKA) oder das Federal Bureau of Investigation (FBI) der USA: Die Fahnder sind vor neue Herausforderungen gestellt. Sie waren den Cyberkriminellen lange nicht gewachsen. Das geändert sich jetzt, in letzter Zeit gab es immer mehr Verhaftungen.

Ermittlungen gestalten sich extrem aufwendig. Oftmals über Scheinkäufe, wie im Falle des Waffenhändlers, der die Waffe für den Amokläufer im Münchener Olympia-Einkaufszentrum 2016 beschafft haben soll. Bei der persönlichen Übergabe schlugen die Polizisten zu; allerdings sind persönliche Übergaben bei Käufen im Darknet recht ungewöhnlich. Die Ware erreiche den Empfänger in der Regel per Post, oftmals in Einzelteile zerlegt, aufwendig verpackt und über Umwege versandt, erzählt Bundeswehroberstleutnant Volker Kozok, der viele Ermittlungen begleitet hat.

Die Methoden der deutschen Fahnder unterscheiden sich von denen in den USA. Einblick in deren Ermittlungsarbeit bekommt man normalerweise nicht, Behörden halten sich bedeckt, die Mitarbeiter sind zum Schweigen verurteilt. Am Rande einer Presseveranstaltung im kalifornischen San Jose am Donnerstag letzter Woche aber ergab sich eine der seltenen Gelegenheiten für ein Gespräch mit US-Ermittlern.

Dabei werden die Unterschiede deutlich: US-Ermittlungsbehörden arbeiteten mit Undercover-Agenten, erklärte Michael Levin, ehemaliger stellvertretender Direktor beim Department of Homeland Security. Dazu seien deutsche Behörden so nicht in der Lage, das sei rein rechtlich nicht möglich, erläuterte er.

Durch den Einsatz verdeckter Ermittler habe sich herausgestellt, dass der Personenkreis im Darknet tendenziell überschaubar sei, es träten oft wiederholt die gleichen Akteure auf. Ronald Layton vom US-amerikanischen Secret Service ergänzte: „Wir monitoren ihre Aktivitäten und wissen, wer mit wem zusammenarbeitet. Wir versuchen herauszufinden, welche Technik sie nutzen, wie sie programmieren oder welche Kenntnisse sie haben.“

Die US-Ermittler analysierten die Sprache, das verwendete Vokabular, die Ausdrucksformen. Cyberkriminelle seien oft nicht sehr kreativ bei ihren Operationen. Wenn etwas Neues auftaucht, sehe das oft aus wie das, was wir schon mal gesehen haben, erklärt Layton, es stecke häufig ein bestimmtes Muster dahinter. Nach einer Weile sei man mit den Verhaltensmustern der Kriminellen vertraut. „Es ist ein kleines Universum und wir kennen es“, sagt Layton. Und Levin deutet an: In diesem Universum befinden sich auch zahlreiche Agenten der US-Behörden.

Oberstleutnant Kozok kennt ein spektakuläres Beispiel: Ross Ulbricht betrieb seit 2011 einen der größten Darknet-Marktplätze namens Silk Road. Bereits nach einem Jahr habe er damit 12,2 Mio. $

Umsatz erzielt, berichtet Kozok. Ulbricht habe Werbung in Untergrundforen gemacht und dort mit Kunden über deren Zufriedenheit diskutiert.

Das FBI sei auf ihn aufmerksam geworden und habe ihn seit 2011 beobachtet. Die Ermittler kannten jedoch zunächst nur das Pseudonym, unter dem er agierte. Schließlich machte er einen Fehler: Aus Versehen habe er einmal seine E-Mail-Adresse in ein Forum gepostet: rossulbricht@gmail.com. Für die Ermittler ein entscheidendes Puzzlestück.

Im Jahr 2013 waren bei Silk Road bereits über 1 Mio. Nutzer registriert. Ulbricht brauchte Mitarbeiter und postete entsprechende Jobangebote, in denen er die verwendete Technik offenlegte. Nun kannten die Ermittler technische Details der Plattform. Laut einem Bericht des Onlinemagazins Ars Technica konnten sie dadurch die Server ausfindig machen.

Schließlich nahm die Geschichte eine dramatische Wendung: Silk Road wurde gehackt und die Hacker versuchten, Ulbricht zu erpressen. Der versuchte, sich seines Problems durch einen Auftragsmord zu entledigen. Doch die Ermittler waren ihm bereits dicht auf der Spur: Der vermeintliche Killer war ein FBI-Agent. Die Fahnder planten Ulbrichts Verhaftung, doch vorher mussten noch entscheidende Belege gesichert werden: „Man braucht Beweise, dass der Verdächtigte auch wirklich der Betreiber der Plattform ist, beispielsweise weil er die Administrationsrechte dafür besitzt“, erklärt Kozok dazu. Es gelang den Ermittlern, einen Agenten als Mitarbeiter von Ulbricht einzuschleusen. Die Kommunikation zwischen Ulbricht und dessen Mitstreiter lief über einen geheimen, verschlüsselten Online-Chat. Ulbricht wurde beobachtet. Als er eines Tages Kontakt zu seinem Mitarbeiter aufnahm, schlugen die Ermittler zu.

Ulbricht saß in einer öffentlichen Bibliothek in San Francisco und chattete über das WLAN mit seinem Mitarbeiter, sie loggten sich in die Darknet-Plattform ein. In diesem Moment wurde Ulbricht durch plötzlichen Krach abgelenkt, dadurch konnte ein FBI-Agent blitzschnell den Laptop beiseiteschieben, um zu verhindern, dass Ulbricht Programme beendete oder Daten löschte. Er wurde verhaftet, der laufende Laptop offenbarte die nötigen Beweise.

Häufig müssten bei den Ermittlungen „Beweise rückwärts, also im Nachhinein, erhoben werden“, erläutert Kozok. Dabei würden auf sichergestellten Servern weitere Nutzer der illegalen Angebote identifiziert und angeklagt.

Deutsche Experten stehen nach eigenen Angaben in regelmäßigem Kontakt mit US-Ermittlungsbehörden. Einmal pro Jahr fährt Kozok gemeinsam mit anderen Cybersicherheitsexperten in die USA, um sich mit den dortigen Sicherheitsbehörden auszutauschen. Daher weiß er: „Das FBI hat auch eigene Angebote im Tor-Netzwerk. Damit konnten schon Fälle im Bereich der Kinderpornografie aufgeklärt werden.“