Bild: Frank Leonhardt/dpa

Spur des Geldes

Wie das größte deutsche Darknet-Forum aufflog

Seit Anfang November läuft der Prozess gegen den Betreiber des Darknet-Forums, über das der Attentäter von München seinen Waffenhändler fand. Die nun vorgelegten Details vervollständigen das Bild, das sich c't über Jahre vom deutschen Darknet erarbeitet hat.

Es war ein Zugriff wie aus einem Hollywood-Streifen: Am Abend des 8. Juni 2017 durchbrach um 21:08 Uhr ein Rammbock der Spezialeinheit GSG-9 die Tür zu einer Wohnung in Karlsruhe. Schwer bewaffnete Beamte stürmten in den Raum und überwältigten binnen Sekunden den gerade am Computer beschäftigten Bewohner.

Damit war das größte deutschsprachige Darknet-Forum „Deutschland im Deep Web“ (DiDW), in dem der Holocaust geleugnet, Verschwörungstheorien verbreitet und Drogen und Waffen verkauft wurden, Geschichte. c't hatte undercover und über Informanten Kontakt zu Luckyspax, wie sich der Betreiber nannte, dem Sicherheitsexperten Blab, der nun verzweifelt gesucht wird, sowie zu mehreren Händlern und Benutzern. So konnten wir die Tiefen des deutschen Darknets ausloten.

Seit Anfang November muss sich nun Luckyspax, im realen Leben der 31-jährige Informatik-Student Alexander U., vor Gericht verantworten. Ihm wird nicht nur Beihilfe zu Drogen- und Waffenhandel vorgeworfen, sondern auch fahrlässige Tötung: Der Attentäter, der im Sommer 2016 am Münchner Olympia-Einkaufszentrum neun Menschen tötete, hatte den Verkäufer der Tatwaffe über das Darknet-Forum des nun Angeklagten kennengelernt. Der Waffenhändler Philipp K. wurde bereits Anfang des Jahres zu sieben Jahren Gefängnis verurteilt. Jetzt geht es darum, die Mitverantwortung des Forumsbetreibers zu untersuchen.

„Deutschland im Deep Web“ war in erster Linie ein Diskussionsforum auf Basis von phpBB. Es war keine an eBay angelehnte Handelsplattform; es gab keinen Warenkorb, in den man illegale Waren legen und anschließend mit Bitcoins beim Plattformbetreiber bezahlen konnte. Die größte Überraschung der Ermittler war angeblich, dass es keine sonst übliche Arbeitsteilung gab. U. soll laut Staatsanwaltschaft allein gehandelt haben. Das deckt sich jedoch nicht mit den Recherchen von c't: U. arbeitete zumindest beim Treuhand-Service für Zahlungen an Händler des Forums mit drei weiteren Personen zusammen.

Für Lucky, wie Luckyspax in der Szene genannt wurde, standen technisches Interesse und Informationsfreiheit im Vordergrund. So bezeichnete er in Gesprächen die Drogenangebote in seinem Forum ebenfalls als eine Form der freien Meinungsäußerung, die er nicht zensieren wolle. Nur bei einer Sache war er unnachgiebig: Kinderpornografie war in jeglicher Form verboten, Links auf solche Untergrundseiten wurden sofort gelöscht.

Frei- und Treuhandel

Während illegale Handelsplattformen wie AlphaBay, Dream Market, Hansa Market, und Valhalla vierstellige Anmeldegebühren oder Kautionen und Provisionen zwischen 8 und 30 Prozent von Händlern kassier(t)en, war der Handel im DiDW-Forum kostenlos und sogar ohne vorherige Anmeldung möglich: In der Freihandelszone durften selbst Gäste Angebote erstellen. In der sogenannten Spielwiese war sogar offensichtlicher Betrug erlaubt.

Neben der Freihandelszone und der Spielwiese gab es im Marktplatz die Rubriken „Biete“ und „Biete verifiziert“. Um von Lucky aus der Freihandelszone in den Biete-Bereich verschoben zu werden, mussten die Angebote einige Kriterien erfüllen – etwa nicht nachbearbeitete Bilder der Ware nebst einem Schild mit Benutzernamen und Datum des Fotos sowie dem Namen des Forums. Auf diese Weise sollte sichergestellt werden, dass ein Händler tatsächlich über die angebotene Ware verfügt und es sich auch nicht um die Bilder eines anderen Händlers oder von einer anderen Plattform handelt. Lucky hatte die Angebote des Biete-Bereichs also eigens geprüft.

Die Hürde für den verifizierten Bereich war nochmals höher. Hier war vor allem die Teilnahme am foreninternen Treuhandsystem Pflicht: Um Betrügereien zu erschweren, hatte Lucky eigens für den Handel zwischen Forumsteilnehmern ein Multisignatur-Treuhandverfahren mit Bitcoin für phpBB implementiert.

Einer der Treuhänder war Luckyspax selbst, zusätzlich ernannte er die Benutzer

BioBauerBernd, HalbMenschHalbSofa und Zombieholocaust zu Treuhändern. Um die Forenbenutzer mit der Handhabung des Multisignatur-Treuhandverfahrens zu schulen, unterhielt BioBauerBernd sogar ein sogenanntes Trainingslager, wo Benutzer risikolos üben konnten.

Es dürfte also kaum zu leugnen sein, dass Alexander U. die illegalen Handelsaktivitäten in seinem Forum aktiv unterstützte. Doch er ging noch weiter: So implementierte er ein API und eine OAuth-Schnittstelle (Open Authorization), mit dem externe Anbieter das Foren-Treuhandsystem nutzen können sollten. Auf diese Weise hätten im Forum registrierte Händler einen eigenen Shop betreiben und trotzdem auf die Dienste der Treuhänder im DiDW-Forum zurückgreifen können. Soweit wir wissen, konnte Lucky die Entwicklung nicht abschließen.

Doch im Fall des Münchner Attentäters wurden nach allen uns vorliegenden Informationen der Verkauf von Tatwaffe und Munition außerhalb des Forums abgewickelt – in bar. Maurächer und Rico, so die Pseudonyme des Attentäters und des Waffenhändlers, lernten sich lediglich im DiDW-Forum kennen. Dort hatte Maurächer in einem Thread gefragt, wer ihm eine Waffe beschaffen könne. Es gab also kein offenes Angebot eines Händlers, schon gar nicht eins, das Lucky unbestreitbar geprüft und verschoben hätte. Der Prozess wird zeigen, wie die Staatsanwaltschaft den Vorwurf des Totschlags untermauern kann.

Fatale Spenden

Auch wenn U. den Handel offenkundig förderte, eine Gewinnerzielungsabsicht hatte er nicht: Lucky verlangte von niemandem Geld oder sonstige Gegenleistungen, auch nicht von Händlern aus den besonders vertrauenswürdigen Biete-Bereichen. Es gab keine Zahlungs- oder Spendenforderungen. Davon konnten wir uns im Rahmen unserer Recherchen aus erster Hand überzeugen: Selbst als wir uns als Händler registriert und Lucky unser getürktes Angebot in den Biete-Bereich verschoben hatte, sprach uns Lucky niemals auf Geld an.

Luckys einzige Einnahmequelle, die ihm später auch das Genick brechen sollte, war ein Spenden-Wallet für den Betrieb des Servers. Die einzigen Anreize für Benutzer waren, dass ein Spendensymbol unterhalb des Namens eingeblendet wurde und man einen Benutzertitel auswählen konnte, wenn man mindestens 10 Euro gespendet hatte. Dennoch kam einiges zusammen, angeblich sollen es bis zu 10.000 Euro im Monat gewesen sein, die vor allem Drogenhändler freiwillig an Lucky zahlten. Drogenproben soll er nach übereinstimmenden Berichten mehrerer Händler stets abgelehnt haben.

Das war auch nötig, denn die Behörden versuchten bereits vor dem Attentat in München, den Betreiber des Forums ausfindig zu machen. Nachdem auch über die Presse bekannt wurde, über welches Darknet-Forum der Münchner Attentäter die Tatwaffe organisiert hatte, nahm der Ermittlungsdruck zu. Lucky und viele andere Forenmitglieder gingen davon aus, dass das Forum längst von Ermittlern unterwandert war, die „Uwe“ genannt wurden.

Lucky erhöhte seine Schutzmaßnahmen, so verwendete er nur noch handverlesene ausländische Tor-Entry-Nodes für den Zugang zum Darknet – vorwiegend aus dem Osten, denn westliche Länder könnten ja mit den deutschen Ermittlungsbehörden kooperieren. Was er nicht kaschieren konnte, war die tägliche Zwangstrennung – denn er betrieb das größte deutsche Darknet-Forum zu Hause auf einem unscheinbaren Rechner neben der Waschmaschine. Insider vermuteten lange, dass die Behörden U. durch die Korrelation zwischen der täglichen Zwangstrennung seines DSL-Anschlusses und dem gleichzeitigen Verschwindens des Forums auf die Spur kamen.

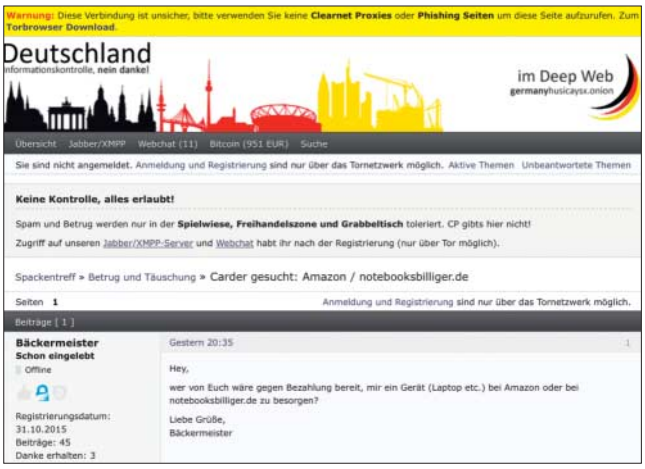
Die Prozessakten enthüllten jedoch, dass es die Spur der Spendengelder war, die die Ermittler zu seiner Tür führte: U. hatte mindestens einmal Spenden über seinen privaten Bitcoin.de-Account in Euro umgetauscht – wo seine vollständige Adresse hinterlegt war. Doch sie mussten ihn im richtigen Moment schnappen, während U. auf dem Server eingeloggt und sein Notebook unversperrt war.

Der Reinfall

Deshalb stellten sie ihm eine Falle: Unter dem Pseudonym Gazza kontaktierten sie Luckyspax und behaupteten, dass sein Server für eine SQL-Injection anfällig sei – näheres würde man Lucky im Chat mitteilen. Bereits um 20:24 loggten sich die Ermittler auf dem zum Forum gehörigen Chat ein und warteten. Alexander U. biss an, loggte sich um 20:50 Uhr auf dem Darknet-Server sowie im Chat ein und suchte nach der vermeintlichen Lücke. Um 21:08 Uhr brach die GSG-9 die Tür auf und überwältigte ihn am Laptop sitzend. Der Coup war gelungen, alle Systeme standen den Ermittlern offen. Danach begann die Beweissicherung, während der die Ermittler Unterhaltungen, die Lucky bereits begonnen hatte, fortführten.

Gegen 4:30 Uhr war dann plötzlich Schluss mit Deutschland im Deep Web: Wie im Prozess bekannt wurde, zog ein Beamter versehentlich einen Stromstecker, an dem der Server des Darknet-Forums hing. So konnten die Ermittler nur rund 2 von insgesamt 75 GByte Daten sichern, darunter angeblich die Inhalte des Forums. Weil die Dateisysteme verschlüsselt sind, kommen die Ermittler nicht mehr an die Daten heran: Alexander U. hat verständlicherweise kein Interesse, ihnen das Passwort zu verraten.

Der Ausgang des Prozesses wird nicht zuletzt von den Betreibern der Nachfolge-Foren aufmerksam beobachtet, etwa denen des DiDW Zwei, wo etliche altbekannte Händler weiter Drogen verkaufen. Kinderpornos sind genau wie im DiDW Tabu, außerdem nun Waffen. Man hat also etwas gelernt. *(mid@ct.de)* c't



Warum ein Notebook kaufen, wenn man es per Kreditkartenbetrug viel billiger haben kann? Mit einer ähnlichen Anfrage fand der Münchner Attentäter im DiDW-Forum seinen Waffenhändler.