IWW INSTITUT
INFORMATIONSDIENSTE

VERDECKTE ERMITTLER IM NETZ

Ermittlungserfolge gegen die digitale Schattenwirtschaft

von RAin Diana Nadeborn, FAin für Strafrecht, Berlin, IT-Strafrecht Blog: www.iww.de/s2188

In einem sog. Underground-Economy-Forum tauschen sich Nutzer u. a. über die Begehung von Straftaten aus und bieten die dafür erforderlichen Waren und Dienstleistungen an, welche die Betreiber in verschiedene Kategorien aufteilen. DR stellt die aktuelle Rechtslage dazu dar, wie Polizisten im Darknet mit Tatverdächtigen kommunizieren und gibt einen Ausblick auf den Gesetzesentwurf des Innenministeriums zu 163g StPO-E.

Meilensteine in den Ermittlungen

Das Landeskriminalamt Rheinland-Pfalz hat im Jahr 2019 beachtliche Ermittlungserfolge erzielt. Am 3.7.19 wurde der Administrator des ehemals größten deutschsprachigen Underground-Economy-Forums „Fraudsters" festgenommen. In diesem Forum, wo vorwiegend mit Betäubungsmitteln, Daten und gefälschten Urkunden gehandelt wurde, waren im Juli 2019 mehr als 30.000 Nutzer registriert. Durchsuchungen und Festnahmen des Landeskriminalamts Rheinland-Pfalz richteten sich am 26.9.19 außerdem gegen ein als „Cyberbunker" bekanntes Rechenzentrum. Dort wurden Underground-Economy-Foren gehostet. „Fraudsters" und „Wall Street Market" gehörten zu deren bekanntesten Kunden. Die Betreiber des Wall Street Market, bei dem weit über eine Mio. Nutzer registriert waren, hatte das Bundeskriminalamt bereits am 23.4.19 festgenommen.

Generelle Funktionsweise der Foren

Die Nutzer melden sich in den Foren unter Pseudonymen an. Wenn ein Nutzer als gewerblicher Händler auftreten möchte, muss er beim Foren-Betreiber eine Art entgeltliche Lizenz als „Vendor" bzw. „Multivendor" erwerben. Mit dieser Lizenz können die Händler z. B. Inserate schalten. Zu dem professionellen Aufbau eines Marktplatzes gehören ein Beschwerdemanagement und ein Treuhandsystem, bei dem der Käufer den Kaufpreis zunächst an den Marktplatz zahlt, der ihn wiederum erst nach erfolgreichem Abschluss des Geschäfts an den Verkäufer auszahlt.

Kommunikation zwischen Händlern und Kunden

Nicht alle Kommunikation zwischen Händlern und Kunden erfolgt heimlich. Die Nutzer können öffentlich einsehbare Beiträge einstellen, z. B. ein Inserat für den Verkauf von illegal erlangten Kontodaten. Andere Nutzer können darauf öffentlich einsehbar antworten. Für die Kommunikation zu den Modalitäten des Geschäfts wählen die Nutzer jedoch verschlüsselte Chats, die (ohne Kenntnis der privaten Schlüssel) von Ermittlungsbehörden nicht eingesehen werden können. I. d. R. sind bei den verwendeten Chatprogrammen außerdem sehr kurze Löschfristen voreingestellt.

Nach der Geschäftsabwicklung können die Kunden wiederum öffentlich einsehbare Bewertungen schreiben, denen im Rahmen der Schätzung des Um-

fangs der Straftaten durch die Ermittlungsbehörden besondere Bedeutung zukommt. Die Bewertungen sollen – losgelöst von der tatsächlichen Identität der Händler – eine Grundlage für das Vertrauen in die geschäftliche Verlässlichkeit schaffen.

Heimliche Ermittlungen unter falschem Namen

Um verdeckt in Underground-Economy-Foren ermitteln zu können, erstellt die Polizei eigene Benutzerkonten unter falschen Namen. In dieser Form wird entweder nach digitalen Spuren von Cybercrime gesucht oder aber aktiv versucht, in Kontakt mit Cyberkriminellen zu kommen.

Für die virtuellen verdeckten Ermittler gibt es keine speziellen Ermächtigungsgrundlagen in der StPO. Zunächst gilt in der realen wie in der virtuellen Welt: Es besteht kein schutzwürdiges Vertrauen in die Identität des Kommunikationspartners (BVerfG 27.2.08, 1 BvR 370/07, Rn. 310 f.). Jeder Nutzer eines Underground-Economy-Forums geht davon aus, dass sein Gegenüber nicht seinen tatsächlichen, sondern einen Phantasienamen verwendet. Die Nutzer haben weder ein Interesse noch die Möglichkeit, die Identität des anderen zu prüfen. Nur ein Polizist sollte es wohl möglichst nicht sein. Es besteht jedoch selbstverständlich auch kein schutzwürdiges Vertrauen dahin gehend, jedenfalls nicht mit einem Ermittlungsbeamten zu kommunizieren.

Anders als bei der Erhebung von Kommunikationsdaten beim Provider, die gem. § 100a StPO hohen Hürden unterliegt, bestehen für die Teilnahme als Chatpartner in einem Forum nur geringe Voraussetzungen. Tarnidentitäten können von Strafverfolgungsorganen grundsätzlich auf Grundlage der Ermittlungsgeneralklausel gem. §§ 161, 163 StPO eingesetzt werden (Wissenschaftliche Dienste des Deutschen Bundestags, Nutzung von Tarnidentitäten in sozialen Netzwerken durch die Polizei und die Strafverfolgungsorgane, Stand: 30.8.18).

Geht der Ermittlungsauftrag jedoch über wenige, konkret bestimmte Ermittlungshandlungen hinaus und wird es erforderlich, eine unbestimmte Vielzahl von Personen über die wahre Identität des verdeckt operierenden Polizeibeamten zu täuschen, und ist außerdem wegen der Art und des Umfangs des Auftrags von vornherein abzusehen, dass die Identität des Beamten in künftigen Strafverfahren auf Dauer geheim gehalten werden muss, dann handelt es sich um den Einsatz eines verdeckten Ermittlers gem. § 110a StPO (BGH 7.3.95, 1 StR 685/94). Auch die Teilnahme an einem Chat, für den der Ermittler eine Zugangssicherung überwinden musste, z. B. durch die Freischaltung durch den Inhaber eines Accounts oder durch die Aufnahme als „Freund", nachdem seine Vertrauenswürdigkeit durch die Abwicklung von Probegeschäften und Aussagen von Leumundszeugen überprüft wurde, richtet sich nach § 110a StPO (Köhler in: Meyer-Goßner/Schmitt, StPO, 62. Aufl. 2019, § 100a Rn. 7, § 110a Rn. 4; Rosengarten/Römer, NJW 12, 1764, 1767).

Woher kommen die Zugangsdaten?

Viele Nutzer von Underground-Economy-Foren sind jedoch misstrauisch gegenüber neuen Nutzern, die noch keine nachvollziehbare Historie in dem Forum haben. Schließlich könnte es sich um Strafverfolger handeln, die zu Ermittlungszwecken eigene Benutzerkonten unter falschen Namen erstellt haben. Aus Ermittlersicht Erfolg versprechender ist daher die Übernahme

bereits bestehender Accounts. Die Zugangsdaten können sie auf klassischem Wege im Rahmen einer Vernehmung erfahren oder sie finden bei einer Durchsuchung notierte Zugangsdaten oder erfahren sie durch abgehörte Telefongespräche. Für die freiwillige Preisgabe von Zugangsdaten zu einem Benutzerkonto, die dazu beiträgt, dass Straftaten wie Drogen- oder Datenhandel in Underground-Economy-Foren aufgeklärt werden können, steht immerhin eine Strafmilderung gem. § 46b StGB im Raum. Dennoch möchte nicht jeder Beschuldigte von dieser Möglichkeit Gebrauch machen, Straftaten anderer aufzuklären. Grundsätzlich kann auch kein Beschuldigter zu einer Aussage gezwungen werden (§ 136 StPO). Erst als rechtskräftig Verurteilter kann er in Verfahren gegen andere Beschuldigte als Zeuge zu einer Aussage gezwungen werden (§§ 163 Abs. 4, 51, 70 StPO). Mit dem IT-Sicherheitsgesetz 2.0 soll eine Rechtsgrundlage zur zwangsweise Herausgabe der Zugangsdaten zu Benutzerkonten geschaffen werden. Der Gesetzesentwurf sieht u. a. die Einfügung des § 163g StPO-E vor:

§ 163g StPO-E

„Der Verdächtige ist verpflichtet, die zur Nutzung der virtuellen Identität erforderlichen Zugangsdaten herauszugeben. § 95 Absatz 2 gilt entsprechend mit der Maßgabe, dass die Zugangsdaten auch herauszugeben sind, wenn sie geeignet sind, eine Verfolgung wegen einer Straftat oder einer Ordnungswidrigkeit herbeizuführen. Jedoch dürfen die durch Nutzung der Zugangsdaten gewonnenen Erkenntnisse in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Verdächtigen oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen des Verdächtigen nur mit Zustimmung des Verdächtigen verwendet werden." (Quelle)

§ 163g StPO-E sieht zwar zum Schutz der Selbstbelastungsfreiheit des Beschuldigten ein Verwendungsverbot in Anlehnung an § 97 Abs. 1 InsO vor. Offen ist jedoch die Streitfrage, ob die herauszugebenden Benutzerdaten nur dann nicht für Ermittlungen gegen den Verdächtigen verwendet werden dürften, wenn sie nicht hypothetisch auf andere Weise hätten erlangt werden können. Der Umfang eines „hypothetischen Ersatzeingriffs" zur Erlangung von Zugangsdaten ist nur schwer fassbar. Insofern scheint es problematisch, das ohnehin in seiner Reichweite umstrittene insolvenzrechtliche Verwendungsverbot als Vorbild für gesetzgeberische Tätigkeiten für IT-Ermittlungsmaßnahmen heranzuziehen (Nadeborn/Irscheid, Erzwingung von Zugangsdaten im Strafverfahren, StraFo 19, 274, 277). Eine Klarstellung des Gesetzgebers, ob das sog. Fernwirkungsverbot des § 97 Abs. 1 S. 3 InsO ebenso umfassend für § 163g StPO-E gelten soll, wäre daher wünschenswert (Oehmichen/Weißenberger, Digitaloffensive im Strafrecht! Verbesserte Bekämpfung von Cyberkriminalität durch das IT-Sicherheitsgesetz 2.0?, KriPoZ 19, 174, 179).

FAZIT | Es gelingen Ermittlern immer wieder weitreichende Ermittlungserfolge gegen Betreiber von Underground-Economy-Foren und dort registrierte Händler. Die „freiwillige" Übernahme von digitalen Identitäten erscheint praktisch umsetzbar. Die anschließende Nutzung der Tarnidentität zur Kommunikation mit potenziellen Straftätern ist rechtlich geklärt. Ein Reformbedarf hinsichtlich der Erzwingung von Zugangsdaten ist insofern nicht ersichtlich. Gegen die Neuregelung sprechen vielmehr die erheblichen Zweifel hinsichtlich des Schutzes der Selbstbelastungsfreiheit und der sie flankierenden Reichweite von Beweisverwertungsverboten.