Verbrechen in neuer Dimension

Internet-Kriminalität

Im Internet ist eine Parallelwelt entstanden: Fernab von Google und Facebook lassen sich Daten, Drogen, Waffen und alles, was das Licht der Öffentlichkeit scheut, handeln. Verbrechen ist plötzlich skalierbar. Wie funktionieren diese digitalen Märkte des Bösen? Eine Expedition in die Welt des Darknet.

Matthias S. ist Drogendealer und wüsste nicht, warum er deshalb besonders vorsichtig sein sollte. Der junge Mann sitzt auf einer Rattancouch, lehnt sich zur Seite, schlägt die Beine übereinander und nimmt einen tiefen Zug Marlboro Gold. „Angst? Wovor sollte ich Angst haben?“, fragt er und pustet den Rauch hörbar aus. „Die Gefahr, dass ich von einem Auto überfahren werde, ist größer, als dass ich erwischt werde.“ Die Gesichtsmuskeln des jungen Manns bewegen sich kaum. Er ist sich der Unmöglichkeit, ihn ob seiner dubiosen Geschäfte zu verfolgen, sehr sicher. Und das liegt daran, dass Matthias S. seinen Handel nicht an dunklen Bahnhofsecken und nicht in zwielichtigen Stadtparks betreibt, wo er von der Polizei enttarnt werden könnte. Matthias S. zieht seine Sicherheit aus dem Marktplatz, auf dem er handelt: Er verkauft sein Kokain im „Darknet“.

Das ist der Teil des Internets, den Suchmaschinen wie Google nicht finden. Der Teil, in dem nahezu niemand Spuren hinterlässt und in den man nicht über Internet Explorer, Firefox oder Chrome eintritt, sondern über eine Software namens Tor, die keine Daten sammelt und Identitäten verschleiert. Es ist ein Jahrmarkt der unbegrenzten Möglichkeiten, auf dem sich Dissiden-

ILLUSTRATION: TIM MCDONAGH

ten treffen, die sich der Kontrolle durch Geheimdienste entziehen möchten, aber auch Kriminelle – mal als Einzeltäter, mal als internationale Banden mit mafiösen Strukturen.

Dass die digitale Revolution nicht nur ungeahnte Möglichkeiten des Miteinanders schafft, sondern auch neue Möglichkeiten des Gegeneinanders eröffnet, ist schon länger klar: geknackte Online-Konten, heimlich auf Rechner geschmuggelte Trojaner, gefälschte Identitäten. Jetzt aber wächst eine neue Gefahr heran: neue Wege, mit all diesen Daten und allerlei schummrigen Zeugs anonym zu handeln. Von überall, zu jeder Zeit, mit jedem. Kriminalität ist somit plötzlich skalierbar: Früher gab es Grenzen, wie viele Menschen ein Verbrecher pro Tag ausrauben konnte, er musste physisch vor Ort sein. Heute ist das anders.

Im Darknet wird gehandelt, was hohe Profite abwirft: Drogen, Sex, Kreditkarten, Blüten, Waffen, Pässe. Auch die Software, mit der der Hacker-Angriff auf den Deutschen Bundestag durchgeführt wurde, könnte aus dem Darknet stammen.

„Die kriminellen Banden sind straff organisiert, sie arbeiten wie reguläre Firmen, indem sie im Darknet Aufträge an Profis vergeben“, sagt Peter Kestner, Ex-Hacker und Spezialist für Cyber Security bei der Wirtschaftsprüfungsgesellschaft Deloitte. „Dadurch bleiben die Strippenzieher im Hintergrund und werden von der Polizei meist nicht erwischt.“ Der dunkle Teil des Internets bietet, wonach sich Kriminelle seit Jahrhunderten sehnen: die perfekte Tarnkappe. „Das Verbrechen auf Bestellung erobert den digitalen Untergrund“, warnt das European Cybercrime Center, eine Spezialeinheit von Europol in Brüssel. „Für nahezu jede Art von Cyberkriminalität gibt es inzwischen im Darknet eine Vielzahl von kommerziellen Angeboten.“ Schäden laut Europol: mehr als 300 Milliarden US-Dollar pro Jahr.

Wie funktioniert dieser Untergrundmarkt? Und wer tummelt sich dort? Um Antworten darauf zu finden, steigen wir selbst ins Darknet, vergleichbar einem Höhlenforscher, der hinter einer Felsspalte eine bislang unerschlossene Schattenwelt entdeckt.

Abtauchen in einen rechtsfreien Raum

Der Felsspalt in die virtuelle Welt ist der Browser Tor, der eigentlich nichts Böses tut und auch von Demokratiebewegungen in diktatorisch regierten Ländern als vertraulicher Kommunikationskanal eingesetzt wird.

App exklusiv

Auf Streife

Mehr Eindrücke von unserem Ausflug ins Darknet bekommen Sie in unserer App-Ausgabe.

300
Milliarden US-Dollar pro Jahr beträgt laut Europol der Schaden durch Kriminalität im Darknet

80
Millionen Dollar verdienten die Betreiber der Drogenplattform Silk Road an Provisionen

„Die Banden sind organisiert wie eine professionelle Firma, die im Darknet Aufträge an Profis vergibt“

Netzsicherheit-Spezialist bei Deloitte, Peter Kestner

Knapp drei Millionen Internet-Nutzer aktivieren täglich diese Software, die ursprünglich für das US-Verteidigungsministerium entwickelt wurde und alle Daten so verschlüsselt, dass nicht mehr feststellbar ist, welcher Computer gerade welche Inhalte abruft.

Das Herunterladen des kostenlosen Tor-Browsers ist simpel. Ein Fenster auf dem Laptop geht auf: „Herzlichen Glückwunsch! Sie können jetzt anonym im Internet surfen“, empfängt uns die grün eingefärbte Homepage mit dem markanten Zwiebel-Logo der Organisation „The Tor Project“, eine in den USA gegründete gemeinnützige Stiftung, die den Schutz der Privatsphäre auf ihre Fahnen geschrieben hat.

Schon beim Einsatz des Tor-Browsers ist höchste Vorsicht geboten. Kurz in der Mittagspause vom Firmen-PC ins Darknet wechseln? Lieber nicht. Die Darknet-Bewohner lauern darauf, einen PC mit Schadprogrammen zu infizieren. Vor solchen Angriffen gefeit ist nur, wer einen Laptop ohne Verbindung ins Firmennetz benutzt.

Wir wagen den zweiten Schritt und stehen vor der nächsten Hürde: Die Suche im Schattenreich des Internets ist längst nicht so schnell und unkompliziert wie die Suche im World Wide Web. Die Internet-Adressen der Marktplätze bestehen aus kryptischen Zahlen- und Buchstabenkolonnen.

Dieses Versteckspiel ist offenbar auch der Unterwelt zu kompliziert. Einige Portale – wie die TorLinks und das Hidden Wiki – bieten deshalb Orientierungshilfen an. Wir geben die Adresse von TorLinks ein und es passiert – erst einmal nichts. Adressen im Darknet werden nicht direkt angesteuert, sondern über andere Netzwerk-Nutzer umgeleitet. So wird jede Identität verschleiert. Deshalb dauert es länger, bis sich die Seiten aufbauen, in unserem Fall knapp 30 Sekunden. Dann öffnet sich die erste Tür in die digitale Unterwelt.

Schon die Startseite verrät: Wir betreten einen rechtsfreien Raum. Hier gibt es all das zu kaufen, wofür man in der realen Welt sofort ins Gefängnis kommt. Eine Liste mit „Links“ zu rund 250 Marktplätzen erscheint – fein säuberlich in verschiedene Kategorien wie „Financial Services“, „Hacking“ oder „Drugs“ unterteilt: Ganz unverblümt bietet die Seite „Hqer“ in der Rubrik „Financial Services“ gefälschte 50-Euro-Noten zum Kauf an. Ein Bündel mit 25 Scheinen (Wert: 1250 Euro) kostet nur 500 Euro. Die Noten sind angeblich so perfekt gefälscht, dass sie sogar den Echtheitstest mit dem im Handel oft eingesetzten Prüfstift bestehen.

Wer die Bündel kauft, muss kaum Angst haben: Weil im Darknet in der Regel mit Bitcoins bezahlt wird, bleiben neben den Nutzerdaten auch die Zahlungsströme verborgen. Die digitale Währung Bitcoin können die Nutzer untereinander über virtuelle Konten austauschen, ohne dass eine Bank oder andere Abwicklungsstelle dazwischengeschaltet werden muss.

Geldfälscher erleben dank Internet einen zweiten Frühling. In Deutschland brachten sie laut Bundeskriminalamt (BKA) im vergangenen Jahr 76 000 Euro-

ILLUSTRATION: TIM MCDONAGH

Blüten mit einem Nennwert von 5,3 Millionen Euro in Umlauf – 60 Prozent mehr als 2013. Ein Grund für den Anstieg, so das BKA: Das Falschgeld werde zunehmend durch organisierte Banden auf illegalen Handelsplattformen im Darknet verbreitet.

Vier Links weiter wirbt „Rent-A-Hacker“ um Aufträge. „Hacken ist mein Geschäft, seit ich 16 Jahre alt bin“, schreibt er. „Ich hatte noch nie einen anderen Job und habe in den vergangenen 20 Jahren richtig viel Geld damit gemacht.“ Er sei Computerexperte. „Kleinere Jobs“ wie E-Mail-Hacking kosten 200 Euro pro Stunde, größere Jobs wie das „Ausspionieren von Unternehmen“ oder das „Ruinieren von Leuten“ übernimmt er ab 500 Euro pro Stunde. „Für Geld tue ich alles. Ich kann Geschäfte zerstören, aber auch das Leben einer Person.“

40000
Marktplätze bieten mindestens im Darknet ihre Ware an

60
Prozent mehr Falschgeld geriet 2014 in Deutschland in Umlauf. Grund laut BKA: das Darknet

Das Muster der Hacker ist immer gleich. Erster Kriminalakt: Über das illegale Eindringen in fremde Rechner werden Daten gesammelt. Zweiter Akt: Diese Daten werden über die Marktplätze im Darknet verkauft. Beides passiert in der Regel innerhalb weniger Tage.

Zu den Bestsellern dort gehören Kreditkartendaten (inklusive persönlicher Identifikationsnummer) und gestohlene Zugangsdaten für Online-Shops wie Ebay (siehe Seite 26).

Das Angebot auf den weit mehr als 40 000 Marktplätzen im Darknet ist so vielfältig, dass eine bislang unbekannte Gruppe dort unter der Marke „Grams“ ein Pendant zu Google im Darknet aufbaut. Das Grams-Logo enthält sogar das gleiche blau-gelb-rot-grüne Regenbogen-Muster wie das legale Vorbild. Selbst die Suchergebnisse präsentiert Grams wie Google. Wer das Wort „Cannabis“ eingibt, bekommt 1572 Treffer, in Klammern dahinter die genaue Zeitangabe, wie lange Grams danach gesucht hat. An der Spitze der Trefferliste blendet Grams sogar Werbeanzeigen ein. „Komme zum ‚The Real Deal Market‘ heute – Kaufe und Verkaufe, was immer Du willst.“ Derzeit durchsucht Grams elf Schwarzmärkte – darunter die drei großen Handelsplätze AlphaBay, Agora und Nucleus Market, die in die Fußstapfen des ehemaligen Marktführers Silk Road treten wollen.

„Ich kann Geschäfte zerstören, aber auch das Leben einer Person“
Darknet-Händler „Rent-A-Hacker“

Silk Road war bis Oktober 2013 der größte Drogenumschlagplatz im Darknet – und der erste öffentlich dokumentierte Beweis, welche Dimension die Kriminalität dort angenommen hat. Seit dem Start im Januar 2011 hatte Silk Road 4000 Anbieter und 150 000 Kunden weltweit angelockt, die Waren und Dienstleistungen im Wert von 1,2 Milliarden US-Dollar austauschten. Allein die Provisionszahlungen für die Betreiber summierten sich auf mehr als 80 Millionen Dollar.

So virtuell der kriminelle Handel, so real die Folgen: Silk-Road-Gründer Ross Ulbricht wurde zu einer lebenslangen Gefängnisstrafe verurteilt. Die Geschäfte im Schmuddel-Web stört das nicht (siehe Seite 24). Aktuelle Untersuchungen in Großbritannien kommen zu dem Ergebnis, dass sich bereits jeder fünfte Drogensüchtige seinen Stoff im Darknet bestellt.

Die noch dubiosere Subkultur des Darknet

Wir wollen tiefer ins Darknet – und stoßen auf eine neue Barriere: geschlossene Foren und Marktplätze, deren „Adressen“ nur noch kleinsten Kreisen bekannt sind und die ständig wechseln. Wer hier verdächtige Fragen stellt und nicht die Szenesprache beherrscht, wird ausgesperrt. Wir brauchen Experten als Reisebegleiter, handeln uns von Profi-Hackern aber genauso Absagen ein wie vom BKA – und landen schließlich bei Privatdetektiven, die im Auftrag von Unternehmen das Darknet durchleuchten.

Einer davon ist Bert Weingarten, Chef der Pan Amp AG in Hamburg. Das Unternehmen entwickelt Filter- und Analysewerkzeuge, die Alarm schlagen sollen, sobald gestohlene Daten auf einem der Schwarzmärkte im Darknet auftauchen. Welche Unternehmen Pan Amp anheuern, will Weingarten nicht verraten. Aber warum sie ihn buchen, ist klar: Manchmal liefern erst die Inserate im Darknet Hinweise, dass ein Unternehmen Opfer eines Cyberangriffs geworden ist.

In den tieferen Schichten des Darknet verstecken die Profis ihre Angebote und organisieren ihr „Großkundengeschäft“ – wie Weingarten es nennt. Mitmachen darf nur, wer sich das Vertrauen einer Community erworben hat oder Bürgen vorweisen kann. „Verkäufer analysieren die Nachfrage auf Authentizität und Bedarf, um gegebenenfalls selbst in Kontakt zu treten, um bessere Konditionen und sichere Übergabemöglichkeiten für die illegalen Produkte zu unterbreiten“, sagt Weingarten. „Weicht ein Käufer von der Norm ab, wird der Kontakt abgebrochen.“

Hier dominieren vor allem Banden das Geschäft. Ein russischer Schwarzmarkt im Darknet bot jüngst die Software, die Ende 2014 beim Hacking-Angriff auf Sony eingesetzt wurde, für 30 000 US-Dollar an. Am teuersten gehandelt werden Sicherheitslücken in IT-Systemen. Hacker fanden allein im vergangenen Jahr 700 Programmierfehler in den Produkten von Softwareriesen wie Microsoft und Adobe. Statt wie früher die bisher unbekannten Lücken selbst für Angriffe auszunutzen, bieten Hacker sie im Darknet zum Verkauf an. Die Käufer, darunter auch Geheimdienste, zahlen dafür bis zu 400 000 US-Dollar. Das Kalkül: Programmierer brauchen Monate, um den Fehler zu korrigieren und den Kunden ein Update aufzuspielen. So lange können Hacker die Lücke nutzen.

Mit dem „Bitcoin Fog“ betreibt die organisierte Kriminalität sogar eine eigene Geldwaschanlage. „Wer hier Bitcoins einzahlt, bekommt gewaschene Bitcoins ab-

➔

züglich einer Provision zurück“, erklärt Pan Amp-Chef Weingarten.

Je einfacher die Bezahlung wird, desto skrupelloser weiten die Händler des Bösen ihre Angebotspalette aus. Bei unserer Expedition ins Darknet gewinnen wir den Eindruck, dass an jeder Ecke mit Waffen gehandelt wird. Da wäre etwa ein Online-Shop namens „Executive Outcomes“. Hier entdecken wir halbautomatische Gewehre wie das Ruger Mini-14 für etwa 1100 Euro. Der Shop bewirbt neben einem sicheren Zahlungsverfahren eine Geld-zurück-Garantie und eine 100-prozentige Erfolgsrate. Die Shopbetreiber behaupten, den Hauptsitz in Texas zu haben und die Waren über mehrere Zweigstellen weltweit, eine davon in Rostock, zu versenden. Ob die Firma tatsächlich ein professionelles Handelsunternehmen ist, bleibt unklar. In einigen Forenbeiträgen wird behauptet, dass es sich bei dem Händler um einen „Scam“ – einen Vorschussbetrüger – handelt. Die Gefahr, im Darknet auf Täuscher hereinzufallen, ist groß. Die amerikanische Nichtregierungsorganisation Rand mutmaßt über den digitalen Schwarzmarkt, dass 30 Prozent aller Darknet-Verkäufer Betrüger sind.

Mit Pan Amp an unserer Seite tauchen wir noch tiefer ins Darknet ein. In dieser dritten Stufe verstecken sich die Syndikate der organisierten Kriminalität. Wir stoßen auf Banden, die mit dem vernetzten Auto das ganz große Geschäft wittern. Eine nennt sich „Erfurt Connection“ und ist angeblich auf Mercedes-Fahrzeuge spezialisiert. „Unsere dynamische Crew“, wirbt die Bande, „hat viel Erfahrung beim Programmieren von Microchips, die in den neuesten Modellen von Mercedes eingesetzt werden.“ In Ganovenkreisen hat sich die „Erfurt Connection“ offenbar schon einen guten Ruf beim Zurückdrehen von Kilometerzählern erworben. Gebrauchtwagenhändler nutzen seit Jahren im Darknet angebotene Programme, die den Kilometerstand älterer Fahrzeuge manipulieren. Jetzt will die „Erfurt Connection“ ein neues Standbein aufbauen: das Kopieren von elektronischen Autoschlüsseln. Zielgruppe sind professionelle Autoschieber, die Aushilfskräfte in den Park-Service von Veranstaltungen oder Hotels einschleusen und so kurzzeitig in den Besitz von Autoschlüsseln kommen. Die könnten dann schnell kopiert werden. Preis pro Autoschlüssel: 980 Euro, ab zehn Fahrzeugen gibt es Mengenrabatt – dann kostet eine Kopie 760 Euro.

700
Programmierfehler, die Angriffe erlaubten, fanden Hacker im vergangenen Jahr in Software von großen Anbietern

Die Bande traut sich sogar, ein Video mit einer Bauanleitung ins Darknet zu stellen. Ein Mitglied demonstriert, wie sich der Chip aus dem Schlüsselgehäuse herauslösen lässt, die dort hinterlegten Daten ausgelesen und auf einen neuen Chip übertragen werden können. Daimler bestätigt solche Angriffsversuche. „Mit der im Video gezeigten Methode könnte mit speziellen Kenntnissen sowie spezieller Hard- und Software ein entwendeter Fahrzeugschlüssel kopiert werden“, heißt es in einer Stellungnahme des Konzerns. Die Methode funktioniere aber nur bei Fahrzeugen bis Baujahr 2009, und sie ist auch besonders umständlich. Anzeichen, dass das Programm rege genutzt wird, gibt es nicht.

Eine Gelddruckmaschine haben die Tüftler mit der Software also wohl kaum erfunden. Wie überhaupt neben haufenweise krimineller Energie auch viel Schmuh im Darknet zu finden ist.

Sicherheitsexperte Manfred Göth sieht allerdings keinen Grund für Entwarnung. „Die Erfurt Connection benutzt ein älteres Verfahren“, sagt der Geschäftsführer des Kriminaltechnischen Prüflabors Göth GmbH in Mayen. Andere Banden sind offensichtlich kreativer. „In Beirut sitzt ein Systementwickler, der schon die aktuelle Version der Sicherheitssysteme in den neuen Mercedes-Modellen geknackt hat.“

Es wäre also wie bei so vielen Ideen für ein kriminelles Geschäftsmodell im Darknet, die anfangs klein wirkten: Die Möglichkeit, es irgendwann zu Geld zu machen, ist keine Frage des Ob – sondern des Wann. ■

Jahrmarkt unendlicher Möglichkeiten *Bildschirmdarstellung eines Waffenhandels im Darknet*

ICON: ROBERT CRUM

melanie.bergermann@wiwo.de,
juergen.berke@wiwo.de

DROGEN

Insider: So läuft der Darknet-Handel

Matthias S., noch keine 30 Jahre alt, wirkt wie ein Versicherungsvertreter. Oder vielleicht ein Banker. In jedem Fall aber wie einer, der jeden Tag einem Bürojob nachgeht. Er trägt ein kariertes Hemd, eine schwarze feine Hose. Darüber eine graue Cordjacke, am Handgelenk eine dicke Uhr. Die Hände sind von körperlicher Arbeit bislang sichtlich verschont geblieben. Die dichten Haare sind makellos gelegt.*

Kein Bekannter, der sich vorstellen kann, dass Matthias seinen Lebensunterhalt damit verdient, in den Untiefen des Darknet Drogen zu verkaufen.

Nichts hatte darauf hingewiesen, dass er in die Kriminalität abdriften könnte. S. wuchs in geordneten Verhältnissen auf, hat einen guten Schulabschluss und später stets Arbeit, sagt er. Sein Vorstrafenregister sei sauber.

Damit ist S. so etwas wie der Prototyp eines Drogenhändlers, der sich im Darknet herumtreibt. „Wir haben es mit einer ganz neuen Generation an Tätern zu tun“, sagt Frank Lange, der als Oberstaatsanwalt in Verden die Abteilung für Internet-Kriminalität leitet. Sie seien nicht selten gebildet, technisch außerordentlich begabt und führten ein bürgerliches Leben. „Die meisten Täter kämen wahrscheinlich nie auf die Idee, sich an den Hauptbahnhof zu stellen und Drogen zu verkaufen“, sagt er. Erst die Anonymität des Internets und der vermeintlich 100-prozentige Schutz vor Entdeckung verleite sie.

Bei S. hatte alles mit der Faszination für die Internet-Währung Bitcoin angefangen. Der Bitcoin ist eine Währung, die nur auf virtuellen Konten im Internet existiert. Die Nutzer können Bitcoins direkt austauschen, ohne dass eine Bank dazwischengeschaltet ist. Geldtransfers können so relativ anonym abgewickelt werden. Im Darknet werden die meisten Produkte so bezahlt.

Matthias S.: ***„Bitcoins sind die Basis von allem. Ohne Bitcoins gäbe es keinen Schwarzmarkt im Internet. Wenn du völlig anonym an dein Geld kommst, kannst du alles handeln. Da wollte ich mitverdienen. Und dann dachte ich: Drogen. Da kommst du am ehesten ran. Über einen Verwandten, der einen Händler kannte, habe ich dann das erste Kokain bekommen.“***

Auf den Marktplätzen im Darknet gibt es alles an Drogen, was auch im Drogenhandel in der echten Welt zu haben ist – Marihuana, Kokain, Speed. Aber auch Anabolika stehen hoch im Kurs. S. hat sich für Kokain entschieden.

„Irgendwelche Pillen für vier Euro zu verkaufen, lohnt sich nicht. Für gutes Kokain zahlen die Leute bis zu 100 Euro. Ist schon irgendwie krank, für ein Gramm so viel zu zahlen. Aber dafür muss die Qualität stimmen. Die Käufer im Netz sind Profis. Denen kannst du keinen Schrott andrehen. Ich hab erst mal selbst ohne Ende konsumiert, bevor ich mit dem Verkauf angefangen habe. Ich muss ja wissen ob mein Stoff gut ist.“

Schlechten Stoff zu verkaufen oder bei der Menge zu schummeln können sich die Internet-Händler nicht leisten: Die Handelsplattformen im Darknet funktionieren ähnlich wie Ebay. Die Käufer bewerten ihre Händler nach dem abgeschlossenen Geschäft. Ohne Bewertungen etwas zu verkaufen ist fast unmöglich. Neulinge verschenken deshalb meist zunächst Proben, um an die ersten positiven Bewertungen zu kommen.

„Die Konkurrenz ist groß. Das werden immer mehr. Wenn gerade viele Drogen im Umlauf sind, fahren Händler Aktionen, um den Handel anzukurbeln. Das läuft genauso wie im Supermarkt. Die verkaufen ein Produkt als Sonderangebot, obwohl es keines ist. Im Darknet behaupten die Händler, dass gerade ein ganz besonders guter Stoff gekommen ist, sie aber nicht viel auf Lager haben. Schon schießen die Bestellungen hoch.“

Wegen der generell guten Qualität der Netz-Ware können viel gelobte Händler im Darknet 30 Prozent mehr für Kokain verlangen als auf der Straße. Phasenweise liegt der Preis noch drüber, wenn das Angebot gerade knapp ist. S. sagt, dass er an jedem verkauften Gramm Kokain 35 Euro verdient. Pro Monat verkauft er im Schnitt ein Kilo Koks. Das macht einen jährlichen Reingewinn von 420 000 Euro.

„Ich genieße die Möglichkeiten, die mir das Geld eröffnet. Ich kann zum Beispiel viel reisen. Aber ich war nicht weniger glücklich, als ich kein Geld hatte. Deswegen allein würde ich es nicht machen. Das gibt mir auch irgendwie einen Kick.“

S. muss permanent vorsichtig sein. Die Polizei ermittelt mit spezialisierten Abteilungen im Darknet. Bevor er mit dem Handel beginnen konnte, hat sich S. monatelang damit beschäftigt, wie die Profis ihre Geschäfte aufgezogen haben, etwa der kolumbianische Drogenkönig Pablo Escobar, der mit Drogenschmuggel zu einem der reichsten Menschen der Welt geworden war.

„Du darfst nie in ein Geschäft einsteigen, wenn das noch Neuland ist. Du musst erst mal schauen, wie die anderen es machen und vor allem welche Fehler die machen. Ich will ja

* Name von der Redaktion geändert

nicht in den Knast. Meine Logistik muss perfekt sein.“

So ruft S. Bestellungen etwa niemals von zu Hause ab. Er geht in ein Café mit frei zugänglicher Internet-Verbindung. Nachdem er das Laptop aufgeklappt hat, muss alles ganz schnell gehen. Falls die Polizei ihn doch mal lokalisiert, will er weg sein, bevor die Beamten da sind. Das würde etwa 15 Minuten dauern, rechnet er vor. Deshalb gibt er sich maximal zwölf Minuten Zeit, um die Bestellungen in seinem Postfach durchzusehen. Dann fährt er los und fischt die Kokaintüten aus mehreren öffentlichen Seen.

„Ich habe mal gelesen, dass ein Drogenhändler die Beutel mit verwesten Hunden eingerieben hat, weil die Drogenspürhunde den Geruch nicht ertragen und dann nicht anschlagen. Ich will keine Hunde töten, aber das Problem mit den Spürhunden musste ich lösen. 100 Prozent sicher ist dann nur noch, die Ware unter Wasser zu lagern.“

Die Drogen innerhalb Deutschlands sicher zu versenden scheint lediglich reine Formsache zu sein. Im Darknet gibt es zahlreiche Hinweise dazu. Jac27a empfiehlt etwa, die Versandware im Folienbeutel zu vakuumieren und dann zusammen mit anderen Waren zu verschicken, damit nicht allein das Gewicht oder das Aussehen den Inhalt verraten. Als Beigabe empfiehlt Jac eine Tüte Suppe Marke „Heisse Tasse“ mit Sweet Chili Geschmack.

„Ich weiß nicht, ob eines meiner Pakete schon mal bei der Polizei gelandet ist. Und wenn, dann trifft es den Käufer, nicht mich. Ich gebe die Post immer woanders ab und nur dort, wo es keine Videoüberwachung gibt. Oft lasse ich das auch von anderen machen. Ich habe keine Angst, dass sie mich kriegen. Die Gefahr, dass ich von einem Auto überfahren werde, ist größer.“

30
Prozent mehr als im Straßenhandel können Dealer im Darknet für Drogen verlangen

1
Kilo Koks verkauft Matthias S. pro Monat über das Netz

Die Täter fühlen sich im Darknet unverwundbar. Dabei bekommt die Polizei immer wieder Händler zu fassen. Nachdem das FBI den Betreiber der Handelsplattform Silk Road geschnappt hatte, wurden auch in Deutschland mutmaßliche Drogenhändler verhaftet, die auf Silk Road gehandelt haben sollen.

Der Staatsanwaltschaft in Verden gelang es 2013, mit „Kron0s“ eine der Szene-Größen im Marihuana-Handel zu schnappen. Er sitzt nun eine sechsjährige Haftstrafe ab. Die Identität der Nutzer wird im Darknet mittels einer Software verschleiert. Die meisten Täter, die geschnappt wurden, haben sich selbst verraten. Oft haben sie zuvor irgendwo Informationen preisgegeben, die Rückschlüsse auf ihre wahre Identität zuließen. Wird S. erwischt, ist ihm der Knast sicher, obwohl er keinerlei Vorstrafen hat. Das ist typisch für die Internet-Täter. Sie handeln anders als klassische Kriminelle gleich mit großen Mengen. Bewährungsstrafen kommen deshalb kaum mehr infrage. „Reichweite und technische Möglichkeiten des Netzes eröffnen Cyberkriminellen ganz andere Handlungsoptionen“, sagt Carsten Meywirth, Leiter der Gruppe zur Bekämpfung von Cybercrime beim Bundeskriminalamt. Sie werden häufig gleich schwerstkriminell. Bei konventionellen Kriminellen ist das meist anders. „Hier sehen wir Karrieren. Sie fangen mit einfachen Taten an und steigern sich dann.“

S. ist noch unschlüssig, wie seine Karriere weiter verlaufen soll.

„Neulich traf ich jemanden, der beruflich mit Waffen zu tun hat. Wenn wir im Gespräch darauf gekommen wären, würde ich vielleicht heute mit Waffen handeln. Wenn du mich in zehn Jahren noch mal besuchst, bin ich da vielleicht eingestiegen. Vielleicht hole ich aber auch mein Abitur nach und werde Beamter. Stell dir mal vor, ich würde Lehrer werden oder sowas Ähnliches. Das wäre doch echt krass.“ ■

melanie.bergermann@wiwo.de

Heißes Tütchen
Suppenverpackungen wie diese werden gerne zum Drogenschmuggel genutzt

ICON: JÓNAS UNNARSSON

KREDITKARTEN

Grenzenloses Angebot an gestohlenen Bezahldaten

Auf rotem Untergrund saust ein ICE über den Bildschirm, gefolgt von einem Schriftzug: „Bahntickets zu teuer? Damit ist jetzt Schluss. Nur 25 % des Gesamtpreises zahlen und Tickets am Automaten abholen“. Schnäppchen dieser Art werden regelmäßig im Netz beworben. Die Anbieter kaufen die Tickets bei der Deutschen Bahn zum regulären Preis, bezahlen sie dann aber mit gestohlenen Kreditkartendaten. Im Schnitt 2000 Mal im Monat wurde die Bahn 2014 so um insgesamt fünf Millionen Euro betrogen.

2000
Mal pro Monat versuchen Kriminelle mit gestohlenen Kreditkartendaten bei der Bahn Tickets zu kaufen

Das scheinbar grenzenlose Angebot an Bezahldaten im Darknet macht diese spezielle Form des Tickethandels möglich. Daten einer deutschen Karte inklusive der Sicherheitsnummer, die für Einkäufe in vielen Internet-Shops benötigt wird, gibt es so schon für 10 bis 15 Euro. Amerikanische Kreditkartendaten werden ab drei Euro pro Stück gehandelt. „Mr. Lim“ bietet ergänzend Geräte an, mit denen Kreditkartendaten auf Rohlinge kopiert werden können. Die Preise für die Daten orientieren sich an Kreditlimit, Laufzeit und der gerade im Darknet umlaufenden Menge. Wenn nach großen Hackerangriffen etwa der Markt mit Daten geflutet wird, drückt das laut einer Analyse der amerikanischen Organisation Rand den Preis – manchmal auf bis zu 70 Cent. Angebot und Nachfrage gelten eben auch in dubiosen Parallelwelten.

Mit den so erworbenen Kartendaten gehen die Käufer vor allem auf Einkaufstour im Internet. „Die Verlockung ist riesengroß, weil es so einfach ist“, sagt Jürgen Lewandrowski, Oberstaatsanwalt für Internet-Kriminalität in Osnabrück. Er gehört zu den wenigen Darknet-Experten im Lande.

Die gehandelten Daten stammen zum Beispiel aus Hackerattacken von professionellen Banden. Auf der Käuferseite tummeln sich einerseits kriminelle Gruppen, die die Daten in einer konzertierten Aktion zum Einsatz bringen. Lewandrowski hat es aber auch oft mit Einzeltätern zu tun. „Viele sind zwischen 15 und 20 Jahre alt und nutzen die Karten, um Markenkleidung zu kaufen, die sie sich sonst nicht leisten können.“

Genauso gängig wie Kreditkartendaten sind im Darknet Zugangsdaten für Internet-Shops. Mit einem „Checker“, den es für 30 Euro gibt, lässt sich auch gleich prüfen, ob die im dunklen Netz feilgebotenen Konten des Online-Modehauses Zalando noch existieren oder wie viele Bewertungen ein Kunde bei Ebay hat.

Wie hoch die Schäden sind, wollen weder Zalando noch Ebay sagen. Die Banken schweigen ebenfalls. Heiko Wolf, Vorstand der von mehreren Instituten gegründeten Initiative gegen Internet-Kriminalität „German Competence Centre against Cyber Crime“, sagt, dass die Verluste überschaubar seien. Über Schäden zu sprechen würde die Kunden unnötig verunsichern.

Seiner Ansicht nach stellt Internet-Kriminalität eine Bedrohung dar, in Teilen würden die Gefahren aber von der Sicherheitsindustrie aufgebauscht.

Die russische IT-Sicherheitsfirma Kaspersky verkündete kürzlich, Kriminelle hätten mittels eines Hackerangriffs 100 Finanzdienstleister um insgesamt 900 Millionen Euro erleichtert. „Nach unseren Informationen waren aber nur wenige, vornehmlich osteuropäische Institute betroffen, und deren Schaden lag jeweils bei maximal zehn Millionen Euro“, sagt Wolf.

Hierzulande sei seines Wissens kein Institut betroffen gewesen. „Deutsche Banken geben derzeit mehr Geld für den Schutz vor Datenmissbrauch aus als für die Schäden.“ ■

Günstiger gehts's kaum
Marktplätze im Darknet bieten gestohlene Zahldaten in Masse

melanie.bergermann@wiwo.de,
jürgen berke

ICON: DIEGO NAIVE