HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Frau
Antonia Justine Franke

Anlagebetrug im digitalen Zeitalter – Aktuelle Herausforderungen im Umgang mit dem Straftatphänomen Cybertrading

Mittweida, 2022

Fakultät Computer- und Biowissenschaften

BACHELORARBEIT

Anlagebetrug im digitalen Zeitalter – Aktuelle Herausforderungen im Umgang mit dem Straftatphänomen Cybertrading

Autor:
Frau Antonia Justine Franke

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO19w4

Erstprüfer:
Herr Prof. Ronny Bodach

Zweitprüfer:
Herr B.Sc. Michael Hofmann

Einreichung:
Leipzig, 14.08.2022

Verteidigung/Bewertung:
Mittweida, 2022

Faculty Applied Computer Sciences and Biosciences

BACHELORTHESIS

Investment fraud in the digital age – Current challenges in dealing with the criminal phenomenon cybertrading

author:
Ms. Antonia Justine Franke

course of studies:
Allgemeine und Digitale Forensik

seminar group:
FO19w4

first examiner:
Mr. Prof. Ronny Bodach

second examiner:
Mr. B.Sc. Michael Hofmann

submission:
Leipzig, 14.08.2022

defence/ evaluation:
Mittweida, 2022

Bibliografische Beschreibung:

Franke, Antonia Justine:
Anlagebetrug im digitalen Zeitalter – Aktuelle Herausforderungen im Umgang mit dem Straftatphänomen Cybertrading. - 2022. - XI, 52, LXII S.
Mittweida, Hochschule Mittweida, Fakultät Computer- und Biowissenschaften, Bachelorarbeit, 2022

Referat:

Die Bachelorarbeit umfasst eine Auseinandersetzung mit dem aktuellen Straftatphänomen Cybertrading. In Zusammenarbeit mit Beteiligten des Strafverfolgungsprozesses und entsprechender Literatur wird das Phänomen aus den Gesichtspunkten der Wirtschaft, des Bankwesens, des Rechts, der Psychologie und der Polizei näher beleuchtet. Mithilfe dieser Erkenntnisse werden die Problemfelder im Umgang mit der Betrugsstraftat aufgedeckt.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Zeichen	Bedeutung
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BKF	Bankkauffrau
bspw.	beispielsweise
bzw.	beziehungsweise
CaaS	(Cyber-)Crime-as-a-Service
CPI	Client Portal Interface
CRM	Customer-Relationship-Management
d.h.	das heißt
DNS	Domain Name System
E	Ermittler
evtl.	eventuell
FIU	Financial Intelligence Unit
FQDN	Fully Qualified Domain Name
GES	Geschädigter
ggf.	gegebenenfalls
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
i.F.v.	in Form von
i.H.v.	in Höhe von
ISP	Internet Service Provider
ITE	IT-Experte
JU	Juristin

KPS	Kriminalpsychologe
MaRisk	Mindestanforderungen an das Risikomanagement
o.ä.	oder ähnliches
u.a.	unter anderem
u.v.m.	und vieles mehr
VPN	Virtual Private Network
WpHG	Wertpapierhandelsgesetz
www	World Wide Web

1 Einleitung

„Die Erfindung des Geldes galt als Kulturleistung, seine Vernichtung in Form von Aktien und Spekulationen mag Kultur beenden.“[1]

Als Raymond Walden 2010 diesen Aphorismus mit der Welt teilte, konnte er nicht wissen, dass er selbst zwölf Jahre später aktueller denn je ist. Von Naturalien über die ersten Münzen bis hin zu Geldscheinen, Kartenzahlung und Onlinebanking: Das Geld ist aus dem Alltag nicht mehr wegzudenken. Und dort wo Geld ist, muss es auch Abnehmer geben. Der Markt wird seit jeher von Angebot und Nachfrage reguliert. Dort, wo gehandelt wird und wo das Angebot groß ist, herrscht auch großer Wettbewerb.

Seit vielen Jahren lässt sich ein Trend beobachten: Der Markt der Angebote dringt immer weiter in die digitale Welt vor. Denn nicht nur bares Geld ist viel Wert, auch sein digitaler Zwilling erfreut sich größter Beliebtheit. Obwohl es sich dabei bloß um digitale Zahlen und Zeichen handelt, können sie ebenso für Geschäfte genutzt werden wie Bargeld. Entsprechend groß ist der Andrang auf Börsen und das Interesse der Bevölkerung für Kapitalanlagemöglichkeiten und Kursentwicklungen.

Befeuert wurde dieses Phänomen nach der Jahrtausendwende. Das in den 2000ern unter dem Pseudonym Satoshi Nakamoto veröffentliche Whitepaper über Bitcoin leitete die Revolution des Währungssystems ein.[2] Kryptowährungen als Pendant zu Fiat-Währungen sollen neue Möglichkeiten auf dem Markt schaffen. Ob als spekulative Anlage oder als zugelassenes Zahlungsmittel, Kryptowährungen wie Bitcoin, Litecoin oder Ethereum und die dahinter stehende Technologie der Blockchain erfreuen sich zunehmend großer Bedeutung.[3] [4]

Doch das digitale Geld hat auch seine Nachteile. Aufgrund der Komplexität und Anonymität der digitalen Welt, der technischen Möglichkeiten und der Unwissenheit der Menschen, stellt der Umgang mit Kryptowährungen ein großes Potenzial für Kriminelle und eine ebenso große Herausforderung für die Strafverfolgungsbehörden dar.[5] Hierarchisch strukturierte, teils weit verzweigte Betrügernetzwerke werden aufgebaut und falsche Handelsplattformen für die nichtsahnende Bevölkerung zugänglich gemacht. Der Aufwand, der betrieben wird, um den Leuten ihr Geld betrügerisch zu entwenden, ist enorm.

---

[1] R. Walden: Sequenzen von Skepsis (39). (2010) Abgerufen am 27.05.2022 von https://raymond-walden.blogspot.com/2010/07/sequenzen-von-skepsis-39.html.
[2] Vgl. P. Rosenberger: Bitcoin und Blockchain - Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik. (Berlin: Springer Vieweg, 2018) S.1.
[3] Vgl. ebd. S.3.
[4] Vgl. E. Sixt: Bitcoins und andere dezentrale Transaktionssysteme - Blockchains als Basis der Kryptoökonomie. (Wiesbaden: Springer Gabler, 2017) S.112,189.
[5] Vgl. P. Rosenberger: Bitcoin und Blockchain - Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik. (Berlin: Springer Vieweg, 2018) S.35ff.

Die aktuellen Fallzahlen der Polizeilichen Kriminalstatistik legen nahe, dass sich Tatorte zunehmend in Richtung Internet verschieben. Im Zeitraum von 2017 bis 2021 sanken die Betrugsfälle um rund 120.000, während Fälle des Computerbetruges um rund 30.000 anstiegen.[6] [7]

So bekannt und umfassend der Begriff Betrug ist, umso weniger bekannt sind gewisse Erscheinungsformen. Beim Anlagebetrug mit Kryptowährungen, dem sogenannten Cybertrading, spielen heute weitaus mehr Faktoren eine Rolle, als vor der Zeit der Digitalisierung.

Das Ziel der Arbeit soll sein, das Straftatphänomen Cybertrading von verschiedenen Gesichtspunkten aus zu betrachten und herauszufinden, welche Probleme im Umgang damit auftreten. Dazu werden Erkenntnisse von Beteiligten solcher Strafverfahren einbezogen, um eine erste wissenschaftlich fundierte Basis für künftige Verfahren zu schaffen und den Erkenntnishorizont für die Allgemeinheit zu erweitern.

Die Arbeit ist untergliedert in die großen Teilbereiche Grundlagen, Methodik, Durchführung inklusive Ergebnisse und Gegenüberstellung.

Im Folgenden werden die deskriptiven Faktoren der Wirtschaftsstraftat näher erläutert. Das Kapitel Wirtschaft umfasst die Themen Handel, Geld, Kryptowährungen, Blockchain und Geldwäsche. Im Kapitel Technik werden die Wallet, Handelsplattformen und deren Ursprung, das Client-Server-Modell, Crime as a Service (CaaS) und Remotesoftware angesprochen. Nachfolgend dazu wird das Betrügernetzwerk und dessen Rollen- und Aufgabenverteilung betrachtet. Abschließend wird der Ablauf der Straftat skizziert und erläutert, welche Ermittlungen zur Klärung dieses Sachverhalts durchgeführt werden.

Der praktische Teil dieser Arbeit umfasst Interviews mit fünf verschiedenen Personen und ein Literaturstudium. Die persönlichen Erfahrungen im Umgang mit Cybertrading und Erkenntnisse der Literatur leisten einen großen Beitrag zu dieser Arbeit. Die Antworten werden zu guter Letzt gegenübergestellt und verglichen, um Gemeinsamkeiten und Unterschiede aus den verschiedenen Fachbereichen hervorzuheben.

---

[6] Bundeskriminalamt: Polizeiliche Kriminalstatistik (PKS): PKS 2017 - Standard Übersicht Falltabellen: Tabelle 01. (2022) Abgerufen am 27.05.2022 von https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2017/Standardtabellen/standardtabellenFaelle.html?nn=96600.

[7] Bundeskriminalamt: PKS 2021 Bund - Falltabellen: T01 Grundtabelle - Fälle (V.1.0). (2022) Abgerufen am 27.05.2022 von https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2021/PKSTabellen/BundFalltabellen/bundfalltabellen.html?nn=194190.

2 Grundlagen Cybertrading

Zum Straftatphänomen Cybertrading gibt es aufgrund der Aktualität sehr wenig bis keine frei zugängliche kriminologisch-wissenschaftliche Lektüre. Sämtliche Informationen und Erkenntnisse werden in Zusammenarbeit mit der Polizeidirektion Leipzig gemacht.

Dabei werden die Faktoren näher beleuchtet, die einen großen Einfluss auf das Straftatphänomen ausüben und welche sich auch durch öffentlich zugängliche Lektüre näher beschreiben lassen. Nur dadurch lässt sich das Straftatphänomen abstrahiert betrachten und besser verstehen.

2.1 Deskriptive Faktoren

Das Phänomen Cybertrading wird durch drei wesentliche Faktoren definiert: Wirtschaft, Technik und Soziales.

2.1.1 Wirtschaft

Der wirtschaftliche Einfluss wird hauptsächlich geprägt durch die Geldtransfers. Dabei spielt es keine Rolle, ob es sich um den Transfer von Fiat-Währungen, also staatlich regulierten Währungen[8], handelt oder den Tausch in Kryptowährung und anschließenden Transfer.

2.1.1.1 Die Historie des Handelns

Am Anfang dieser Entwicklungskette steht klassischer Weise das Prinzip des Handelns. Bereits die ersten Menschen müssen verstanden haben, dass alles einen Wert hat. Entsprechend erfordert eine Leistung auch eine Gegenleistung. Von Tauschgeschäften, über Naturalgeld in Form von Muscheln und Steinen, bis hin zu den ersten Münzen, Scheinen und Onlinebanking: Das Handeln begleitet den Menschen seit vielen Jahrtausenden.

Der Handel selbst findet dabei zumeist in der Öffentlichkeit statt. Marktplätze waren seit jeher Dreh- und Angelpunkt der Dörfer und Städte. Denn dort, wo sich viele Menschen treffen, gibt es auch viele Gelegenheiten ein Geschäft abzuschließen. Händler aus nah und fern bieten ihre Waren an und werben für ihre Produkte. Der Wettbewerb ist groß, wenn unterschiedliche Händler zur gleichen Zeit die gleichen Produkte anbieten. Um Kunden zu gewinnen, müssen sich die Händler untereinander im Preis unterbieten. Interessenten steht es frei, bei welchem Händler sie ein Geschäft abschließen möchten. Hat ein Händler jedoch eine Art Monopolstellung auf dem Markt, da seine Waren einzigartig

[8] Vgl. R. Alt & S. Huch: Fintech-Lexikon: Begriffe für die digitalisierte Finanzwelt. (Wiesbaden: Springer Gabler, 2022) S.67.

sind, so hat der Interessent keine freie Wahl. Der Händler legt einen Preis fest und kann von niemandem unterboten werden. Es herrscht das Angebot-Nachfrage-Prinzip. Je mehr von einem Produkt angeboten wird, umso günstiger sind deren Preise. Gleichzeitig ist ein Produkt teurer, wenn es auf dem Markt weniger vertreten ist.[9]

2.1.1.2 Das Angebot-Nachfrage-Prinzip

Heute ist das Angebot-Nachfrage-Prinzip nach wie vor im Alltag zu finden. Jedoch hat sich das Angebot zunehmend in der digitalen Welt ausgebreitet. Wo damals persönliche Geschäfte abgewickelt wurden, steht es den Interessenten heute frei, aus jedem Teil der Welt einen Handel online abzuschließen.[10]

Auch das Angebot selbst hat sich erweitert. Unternehmen, die expandieren möchten und dies finanziell nicht aus eigener Kraft schaffen, gehen an die Börse. „Mit Aktien verkauft ein Unternehmen Anteilsrechte und beteiligt Menschen am Unternehmen, die dann zu Miteigentümern, sogenannten Aktionären, werden.“[11] Dabei handelt es sich um eine Win-Win-Situation: Der Aktionär erhält einen Anteil an den jährlichen Gewinnen des Unternehmens und das Unternehmen selbst erhält seine gewünschte Finanzspritze. Auch hier gilt wieder das Angebot-Nachfrage-Prinzip. „Bei guter Wirtschaftslage steigt […] auch der Preis der Aktie, denn sind weitere potentielle Anleger davon überzeugt, dass das Unternehmen auch in Zukunft erfolgreich sein wird, wollen auch sie Aktien des Unternehmens erwerben. Damit steigen Nachfrage und Kurs der Aktie an der Börse.“[12]

Ein wunderbares Beispiel lässt sich anhand der Energiekonzerne zur Hochzeit der Coronapandemie 2019 bis 2021 eruieren. „Geschlossene Firmen und Homeoffice sorg[t]en für eingeschränkten Personen- und Güterverkehr. Hinzu [kam] der gesunkene Strom- und Ölverbrauch durch Produktionsrückgänge, sowie der eingestellte Reiseverkehr, insbesondere Flugreisen.“[13] Im Zeitraum dieser drei Jahre ist der Kurs von konventionellen Energiekonzernen gesunken, während parallel dazu das Bewusstsein für Nachhaltigkeit und Klimafreundlichkeit wuchs.

Die beispielhaft in Abbildung 1 dargestellten Kursverläufe der E.ON-Aktie (blauer Graph) und der Shell-Aktie (roter Graph) unterstreichen diese Aussage für den angegebenen Zeitraum.[14] Die horizontale Achse stellt dabei den Verlauf über die letzten drei Jahre dar, während die vertikale Achse den Preis der Aktie in Prozent darstellt. Demnach startet jede Aktie bei einem festgelegten Preis und dem Prozentsatz von hundert. Je nach Erfolg an der Börse, steigt oder fällt die Aktie über oder unter den Ausgangspreis von hundert Prozent.

---

[9] Vgl. K. Schroer: Angebot und Nachfrage. (2022) Abgerufen am 14.06.2022 von https://www.bwl-lexikon.de/wiki/angebot-und-nachfrage/.
[10] Vgl. Deutsche Börse: So funktioniert die Börse. (2022) Abgerufen am 14.06.2022 von https://www.boerse-frankfurt.de/einstieg/so-funktioniert-die-boerse.
[11] Deutsche Börse: Aktien - An Unternehmen teilhaben. (2022) Abgerufen am 14.06.2022 von https://www.boerse-frankfurt.de/einstieg/aktien-an-unternehmen-teilhaben.
[12] Ebd.
[13] A.-K. Hentsch: Kurzfristig positiv: Corona-Effekte auf die Umwelt. (2022) Abgerufen am 13.06.2022 von https://www.nationalgeographic.de/umwelt/2020/03/kurzfristig-positiv-corona-effekte-auf-die-umwelt.
[14] Vgl. ARD-aktuell: E.ON Kurs. (2022) Abgerufen am 13.06.2022 von https://www.tagesschau.de/wirtschaft/boersenkurse/eon-ag-aktie-enag99/.

Als 2022 annähernd Normalität in Deutschland einkehrte und wieder fossile Brennstoffe gekauft wurden, wuchs der Kurs des konventionellen Energiekonzerns über den Kurs des nachhaltigen Energieerzeugers hinaus. Auch wenn es in Abbildung 1 so wirkt, als würden sich die beiden Kurse nun ein Kopf-an-Kopf-Rennen liefern, so täuscht der Graph. Stand 13.06.2022 kostet die Shell-Aktie 26,53 Euro (siehe Anhang 1.1), während die E.ON-Aktie nur 9,39 Euro (siehe Anhang 1.2) kostet.

Abbildung 1 – Kursvergleich der Aktien für E.ON und Shell PLC EO-07[15]

Ganz offensichtlich üben die Politik einzelner Staaten oder deren Zusammenschlüsse großen Einfluss auf den (Miss-)Erfolg einzelner Aktien aus. Beim Handel mit Kryptowährungen soll das nicht passieren.

2.1.1.3 Kryptowährungen

Kryptowährungen funktionieren dezentral, d.h. es ist möglich, überall auf der Welt ohne Zwischeninstanz Geld von A nach B zu transferieren.[16] Aktuell handelt es sich bei den digitalen Währungen zumeist noch um spekulative Anlagen.[17] Ihren Ursprung haben sie in den 2000er Jahren, als ein Whitepaper zum Bitcoin unter dem Pseudonym Satoshi Nakamoto veröffentlicht wurde. Darin wird beschrieben, wie ein Gegenstück zum Fiat-Geld, also eine digitale Währung geschaffen werden kann, welche zwischen zwei Parteien direkt und geschützt durch kryptographische Verfahren ausgetauscht wird.[18] Ein System, welches den Finanzsektor revolutioniert. Die dabei genutzte Technik nennt sich Blockchain.

---

[15] ARD-aktuell: E.ON Kurs. (2022) Abgerufen am 13.06.2022 von https://www.tagesschau.de/wirtschaft/boersenkurse/eon-ag-aktie-enag99/.
[16] Vgl. P. Rosenberger: Bitcoin und Blockchain - Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik. (Berlin: Springer Vieweg, 2018) S.1f.
[17] Vgl. ebd. S.3.
[18] Vgl. S. Nakamoto: Bitcoin Whitepaper – Bitcoin: A-Peer-to-Peer Electronic Cash System. (2008) Abgerufen am 07.06.2022 von https://www.bitcoin.com/satoshi-archive/whitepaper/.

2.1.1.4 Die Technik hinter der Kryptowährung

Bei der Blockchain handelt es sich um eine endlose Kette an Blöcken, wie Abbildung 2 zeigt. Jeder dieser Blöcke setzt sich aus „mehrere[n] tausend Transaktionen [zusammen] und [wird] mit einer Prüfsumme versehen […]. Neue Blöcke werden in einem rechenintensiven Prozess erschaffen, der sich Mining nennt, und anschließend über das Netzwerk an die Teilnehmer verbreitet. Die Transaktionen eines Blocks werden paarweise miteinander verschlüsselt und nur der letzte Hashwert, der Root-Hash, als Prüfsumme im Header des Blocks vermerkt. […]. [So] ist die Reihenfolge der Blöcke festgelegt [und] das nachträgliche Modifizieren vorangegangener Blöcke bzw. Transaktionen praktisch ausgeschlossen.“[19] Als Genesis-Block wird der erste Block dieser Kette bezeichnet, welcher damals von Nakamoto selbst gemint wurde.

Jede Transaktion, die auf der Blockchain basiert, wird also vermerkt. Dabei wird davon ausgegangen, dass es sich beim Bitcoin um eine anonyme Form des Bezahlens handelt. Tatsächlich ist es zwar möglich, den Verlauf jedes Bitcoins bzw. jeder Blockchain öffentlich einzusehen, doch aufgrund der hinterlegten alphanumerischen Adresse des Senders und Empfängers ist es nicht möglich, direkt auf eine reale Person zu schließen.[20] Voraussetzung dafür ist, dass die Person ihre Kennung nicht öffentlich preisgibt. „Bitcoin ist daher streng genommen pseudonym, nicht anonym.“[21]

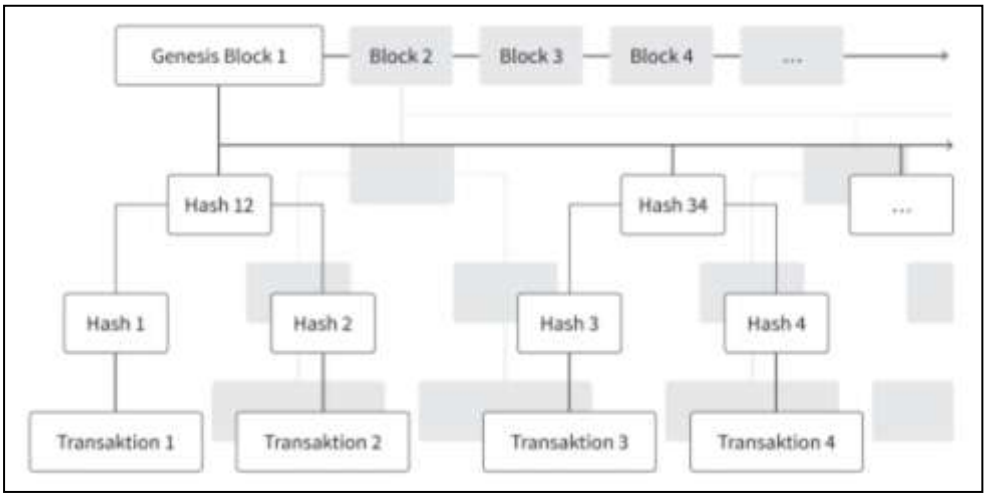


Abbildung 2 – Das Prinzip der Blockchain (vereinfacht)[22]

Unter dem rechenintensiven Prozess wird das Lösen eines mathematischen Rätsels verstanden. Da sich viele Miner gleichzeitig an dem Rätsel versuchen, ist der Wettbewerb ziemlich hoch. Bei der Lösungsfindung gilt das Mehrheitsprinzip. Erst wenn eine definierte Anzahl an Minern eine Lösung bestätigt, wird der Block der Kette angehängt. Derjenige, der die Lösung des Rätsels gefunden und somit den Block berechnet hat, bekommt als

[19] P. Rosenberger: Bitcoin und Blockchain - Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik. (Berlin: Springer Vieweg, 2018) S.66.
[20] Ebd. S.56
[21] Ebd. S. 56.
[22] Ebd. S.18.

Belohnung einen gewissen Wert in Bitcoin als Entschädigung für die aufgebrachte Rechenleistung.[23]

2.1.1.5 Der Bitcoin

Beim Bitcoin handelt es sich um eine endliche Währung. Nakamoto implementierte ein Protokoll, welches eine Obergrenze von 21 Millionen Bitcoins festlegt.[24] Entsprechend groß ist mittlerweile der Ansturm auf die virtuelle Währung. Damit die Münzen über mehrere Jahre hinweg geschürft werden können, wird ein Block circa alle zehn Minuten berechnet. Wird diese Zeit unterboten, passt das Protokoll automatisch den Schwierigkeitsgrad des Rätsels an.[25] Das Protokoll dient demnach als eine Art Sicherheitsmechanismus, welches den Prozess des Schürfens vor der wachsenden Zahl an Minern und deren zunehmend effizienten Techniken schützt und so das Schürfen bis in das Jahr 2140 gewährleistet.[26]

So populär der Bitcoin mittlerweile auch ist, so hat er laut Kritikern sein Ziel verfehlt. „Die Kryptowährung ist 2009 angetreten, um Finanztransaktionen weltweit zu revolutionieren, […] [dies] führte letztlich aber dazu, dass das hohe Wertsteigerungspotenzial […] mehr Anleger als Nutzer anzog und der Kurs seit 2010 stark schwankt.“[27]

2.1.1.6 Missbrauch von Kryptowährungen

Die Kursschwankungen machen sich viele Anleger zunutze. Darunter auch die Betrüger beim Cybertrading. Unwissende Anleger investieren ihr Geld bei inkriminierten Plattformen oder überweisen es an ein vom Betrüger angegebenes Bankkonto. Je nach Zahlungsart stellt sich das Zurückholen des Geldes im Betrugsfall als mehr oder weniger schwierig heraus. Hinzu kommt, dass digitale Zahlungsströme, besonders in Bezug zu Kryptowährungen, kompliziert und komplex sind.

Die Betrüger machen es den Ermittlern nicht leicht. Geldwäsche ist ein wichtiges Thema bei Cybertrading. „Unter Geldwäsche versteht man in der Regel den Vorgang, bei dem für rechtswidrig erlangte Vermögenswerte der Anschein erweckt werden soll, dass es sich um legale Vermögenswerte handele. […] Sie erfasst den Umtausch, das Weiterleiten, das Verschleiern, den Erwerb, den Besitz und die Verwendung derart unmittelbar, aber auch mittelbar durch die Vortat vorbelasteten Vermögens […].“[28] Diese Tat ist nach §261 StGB[29] strafbar und wird von den Strafverfolgungsbehörden geahndet.

---

[23] Vgl. P. Rosenberger: Bitcoin und Blockchain - Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik. (Berlin: Springer Vieweg, 2018) S.19f.
[24] Vgl. ebd. S.67.
[25] Ebd. S.67f.
[26] Vgl. ebd.
[27] Ebd. S.142.
[28] P. Derleder, K.-O. Knops und H. G. Bamberger: Deutsches und europäisches Bank- und Kapitalmarktrecht. Bd. 2. (Berlin, Heidelberg: Springer, 2017) S. 1783.
[29] Vgl. Bundesministerium der Justiz. Strafgesetzbuch (StGB) - §261 Geldwäsche. (2021) Abgerufen am 24.06.2022. von https://www.gesetze-im-internet.de/stgb/__261.html.

2.1.2 Technik

Wie bereits erwähnt, findet der Handel zunehmend online statt. Unabhängig von der Investition mit Fiat-Währungen oder Kryptowährungen wird ein internetfähiges Gerät benötigt, bspw. ein PC, Laptop oder Smartphone.

2.1.2.1 Die Wallet

Um mit Kryptowährungen zu handeln, bedarf es den Einsatz einer digitalen Geldbörse, einer Wallet. „Als Wallets werden sowohl Bitcoin-Clients als auch die Dateien bezeichnet, in denen die Adressen und privaten Schlüssel des Bitcoin-Anwenders gespeichert sind. Der aufsummierte Wert der Adressen steht dem Nutzer als verwendbares bitcoin-Guthaben zur Verfügung. Der Nutzer hat immer die alleinige Kontrolle über seine diversen privaten Schlüssel. […].“[30] Jede Wallet hat dabei eine ID, welche die eindeutige Zuordnung zwischen Kunde und Geldbörse herstellt.[31]

Des Weiteren gibt es mehrere Möglichkeiten im Umgang mit der Wallet. Einerseits können Anleger selbst entsprechende Software herunterladen und ihre Wallet eigenständig anlegen und verwalten, andererseits können sie die Verwaltung in die Verantwortung eines Handelsdienstleisters geben.[32]

Im ersten Fall wird von einer Cold Wallet gesprochen. Die Wallet ist dabei nicht mit dem Internet verbunden, weshalb die Münzen vor Onlineangriffen geschützt sind. Im zweiten Fall handelt es sich um eine Hot Wallet. Die Hot Wallet liegt direkt beim Onlinedienstleister und unterliegt deshalb dem Risiko für Cyberattacken. Die dritte Möglichkeit funktioniert rein analog. Als Paper Wallet werden die für kryptografische Verfahren nötigen öffentlichen und privaten Schlüssel i.F.v. QR-Codes auf Papier gedruckt. Auch wenn Cyberkriminelle auf die Papierwallet nicht zugreifen können, so haben (Taschen-)Diebe an der Stelle leichteres Spiel, sofern die QR-Codes nicht voneinander getrennt aufbewahrt werden.[33]

2.1.2.2 Der Handel mit Kryptowährungen

Für den Kauf von Kryptowährungen benötigt der Anleger eine Handelsplattform, das kann ein Broker sein oder eine Börse. Der Broker ist eine Art Schnittstelle zwischen Anbieter und Käufer. Stellvertretend für den Käufer führt er dessen Aufträge an der Börse durch und berechnet dafür eine Provision.[34] Alternativ dazu kann der Kunde persönlich mit den

---

[30] E. Sixt: Bitcoins und andere dezentrale Transaktionssysteme - Blockchains als Basis der Kryptoökonomie. (Wiesbaden: Springer Gabler, 2017) S.16.
[31] Vgl. P. Rosenberger: Bitcoin und Blockchain - Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik. (Berlin: Springer Vieweg, 2018) S. 22
[32] Vgl. E. Sixt: Bitcoins und andere dezentrale Transaktionssysteme - Blockchains als Basis der Kryptoökonomie. (Wiesbaden: Springer Gabler, 2017) S.34ff.
[33] Vgl. F. Krause: Wie und wo kann ich Kryptowährungen kaufen? (2022) Abgerufen am 14.06.2022 von https://blockchainwelt.de/kryptowaehrung-kaufen/.
[34] Vgl. R. Alt & S. Huch: Fintech-Lexikon: Begriffe für die digitalisierte Finanzwelt. (Wiesbaden: Springer Gabler, 2022) S.24.

Anbietern auf der Börse in Kontakt treten. Dies ist zwar günstiger, birgt aber auch die Gefahr des Totalverlustes aufgrund teils fehlender staatlicher Regulierung und Aufsicht.[35]

Alternativ zu den Plattformen gibt es in einigen Großstädten auf Bitcoin ausgelegte Geldautomaten. Über sie kann Fiat-Geld direkt eingezahlt, in Bitcoin gewechselt und einer Wallet per QR-Code gutgeschrieben werden.[36]

Kauft ein Kunde Kryptowährungen, so zahlt er einen Betrag X in seiner Landeswährung ein. Anschließend wird der eingezahlte Betrag zum tagesaktuellen Kurs in die entsprechende Kryptowährung getauscht. Die erworbenen digitalen Münzen werden der Wallet des Käufers gutgeschrieben.[37]

Bei der Wahl der Handelsplattform sollten sich Kunden vorher belesen. Neben bekannten Plattformen wie eToro[38] oder Coinbase[39] gibt es auch weniger bekannte Plattformen, die evtl. von betrügerischen Gruppen betrieben werden. Auch optisch ähnliche Webseiten mit ähnlichem Namen sollten mit Vorsicht genutzt werden.

2.1.2.3 Die Anbieter

Ausgehend von den Betreibern ist die Anschaffung der Technik für den Betrieb von Webseiten o.ä. ein kostspieliges Unterfangen. Kleinere Unternehmen oder Privatleute, darunter auch Betrüger, greifen deshalb auf die Hosting-Services zurück. Der Markt bietet auch hier verschiedene Lösungen für unterschiedliche Anforderungen. Grundlegend gilt: „Jede Webanwendung ist auf einen Server angewiesen, der Daten im Netz bereitstellt und bei Bedarf an Clientprogramme ausliefert.“[40]

2.1.2.4 Die Server

Server können sowohl hardwarebasiert, als auch softwarebasiert laufen. Der Unterschied liegt in der Ressourcennutzung. Während bei hardwarebasierten Servern das gesamte physische Gerät einem Kunden zur Verfügung steht, laufen mehrere softwarebasierte Server virtuell auf einem physischen Gerät. Die Ressourcen sind somit für jeden virtuellen Server festgelegt.[41] Eine Sonderform des virtuellen Servers ist der Cloud-Server. Um die Redundanz zu erhöhen, verteilt er die „Nutzerdaten […] über mehrere physische Festplatten“[42], sogenannte Cluster. Die Ressourcen der Cluster lassen sich aus Sicht der Kunden

---

[35] Vgl. F. Krause: Wie und wo kann ich Kryptowährungen kaufen? (2022) Abgerufen am 14.06.2022 von https://blockchainwelt.de/kryptowaehrung-kaufen/.
[36] Vgl. ebd.
[37] Vgl. Kryptonauten: Teil 4: Wie kaufe ich Kryptowährungen? (2022) Abgerufen am 16.06.2022 von https://www.blockchaincenter.net/kryptowaehrungen-kaufen/.
[38] eToro: Die Power des Social Investing. (2022) Abgerufen am 14.. 06. 2022 von https://www.etoro.com/de/
[39] Coinbase: Jetzt durchstarten mit Ihrem Krypto-Portfolio. (2022) Abgerufen am 14.06.2022 von https://www.coinbase.com/de/.
[40] J. Behrens: Webhosting: Server im Vergleich. (2020) Abgerufen am 28.06.2022 von https://www.ionos.de/digitalguide/server/knowhow/so-behalten-sie-den-ueberblick-beim-server-vergleich/.
[41] Vgl. ebd.
[42] Ebd.

leichter skalieren, wodurch schnell auf Veränderungen seitens der Serveranforderungen reagiert werden kann.[43]

Server können unterschiedliche Aufgaben erfüllen, Tabelle 1 zeigt die bekanntesten kurz auf. Beim Cybertrading genutzte Server sind vor allem Web-, Datenbank-, Proxy- und Mailserver.

Tabelle 1 – Serverarten und deren Aufgaben[44]

Servertyp	Aufgabe
Webserver	Speicherung, Aufbereitung und Bereitstellung von Webseiten für Clients
File-Server	Dateien zentral speichern, um sie für Clients im gesamten Netzwerk bereitstellen zu können
Mailserver	Empfangen, Weiterleiten, Senden, Abrufen von E-Mails
Datenbankserver	Clients ermöglichen auf Datenbanksysteme zuzugreifen
Gameserver	Verwaltung der Daten eines Onlinespiels; zeitgleiche Interaktion mit Spielinhalten
Proxy-Server	Filtern von Kommunikation; Kontrolle der Bandbreite; Caching; Anonymisierung des Clients
DNS-Server	Namensauflösung von Hostnamen in IP-Adressen

Je nach Anforderung, können sich die Betrüger entsprechende Server anmieten, um darüber ihre Plattform zu betreiben.

2.1.2.5 Die Handelsplattform

Eine Handelsplattform ist schlussendlich nicht mehr als eine Webseite mit Interaktion. Jede Webseite hat einen Namen, auch Domain bzw. Domäne genannt. „Bei einer Domain handelt es sich um einen weltweit einmaligen, eindeutigen Namen für einen logisch abgegrenzten Teilbereich des Internets […]. [Sie gibt an,] wo eine Ressource innerhalb des

[43] Vgl. J. Behrens: Webhosting: Server im Vergleich. (2020) Abgerufen am 28.06.2022 von https://www.ionos.de/digitalguide/server/knowhow/so-behalten-sie-den-ueberblick-beim-server-vergleich/.
[44] Vgl. ebd.

hierarchisch strukturierten Domain Name Systems (DNS) zu finden ist.“[45] Der vollständige Domainname, der Fully Qualified Domain Name (FQDN), besteht aus dem Rechnernamen (Host) und dem Namen der Domain. Letzterer ist wiederum hierarchisch unterteilt in das Root-Label und die Level-Domains.[46]

Als kurzes Beispiel dient die URL *https://www.beispiel.de*.

Die Abstufung der Level erfolgt von rechts nach links. Demnach ist die Top-Level-Domain *de* und steht für die Zuordnung der Adresse in Deutschland. Die Second-Level-Domain ist der Name der Webseite, hier *beispiel*. Die Third-Level-Domain beschreibt die Subdomain, hier *www* (World Wide Web). Vorangestellt steht das genutzte Protokoll, in diesem Fall *https* (Hypertext Transfer Protocol Secure). Der vollständige Domainname setzt sich aus der Top-Level-Domain und der Second-Level-Domain zusammen, somit *beispiel.de*. Diese in Kombination mit der Third-Level-Domain ergibt den vollständigen Hostnamen *www.beispiel.de*.[47]

2.1.2.6 Die Webseite

Wie die Suche nach einer Webseite funktioniert, zeigt das Client-Server-Modell aus Abbildung 3. Möchte ein Nutzer, bspw. Client 3, die Webseite der Polizei Sachsen besuchen, gibt er den Klarnamen ein. Im Hintergrund laufen je nach Dienst verschiedene Protokolle zur Kommunikation zwischen Client und Server. Der Webbrowser sucht nach dem DNS-Server, der die umgewandelte IP-Adresse besitzt. Hat der Client diese gefunden, sendet er einen HTTP-Request, in der Abbildung orange dargestellt, um vom Server eine Kopie der gewünschten Webseite zu erhalten. Akzeptiert der Server die Anfrage, antwortet er, indem er den entsprechenden Webserver kontaktiert, welcher die Webseite in einzelnen Datenpaketen weiterleitet, in der Abbildung lila dargestellt. Der Browser fügt diese Pakete dann zusammen und der Nutzer sieht die Webseite als Ganzes.[48]

Damit eine Webseite überhaupt erreicht werden kann, bedarf es einen Internet Service Provider (ISP) oder auch einfach nur Provider genannt. „Ein ISP (Internet Service Provider; Internetdienstanbieter) ist ein Unternehmen, das Personen, Organisationen und Firmen mit dem Internet und den dazugehörige[n] Services verbindet. […] [Dazu] verfügt [er] über die Ausrüstung und den Zugriff auf die Telekommunikationsleitungen in einem bestimmten Areal […].“[49] Bekannte Vertreter sind Telekom, Vodafone oder 1&1.

---

[45] J. Behrens: Was ist eine Domain? (2021) Abgerufen am 28.06.2022 von https://www.ionos.de/digitalguide/domains/domaintipps/was-ist-eine-domain/.
[46] Vgl. J. Behrens: Was ist eine Domain? (2021) Abgerufen am 28.06.2022 von https://www.ionos.de/digitalguide/domains/domaintipps/was-ist-eine-domain/.
[47] SISTRIX: Was ist der Unterschied zwischen URL, Domain, Subdomain & Hostnamen? (2021) Abgerufen am 28.06.2022 von https://www.sistrix.de/frag-sistrix/seo-grundlagen/was-ist-der-unterschied-zwischen-einer-url-domain-subdomain-hostnamen-usw.
[48] Vgl. Shidigital: Wie das Internet funktioniert. (2021) Abgerufen am 27.06.2022 von https://developer.mozilla.org/de/docs/Learn/Getting_started_with_the_web/How_the_Web_works#credit.
[49] TechTarget: ISP (Internet Service Provider). (2016) Abgerufen am 28.06.2022 von https://www.computerweekly.com/de/definition/ISP-Internet-Service-Provider.

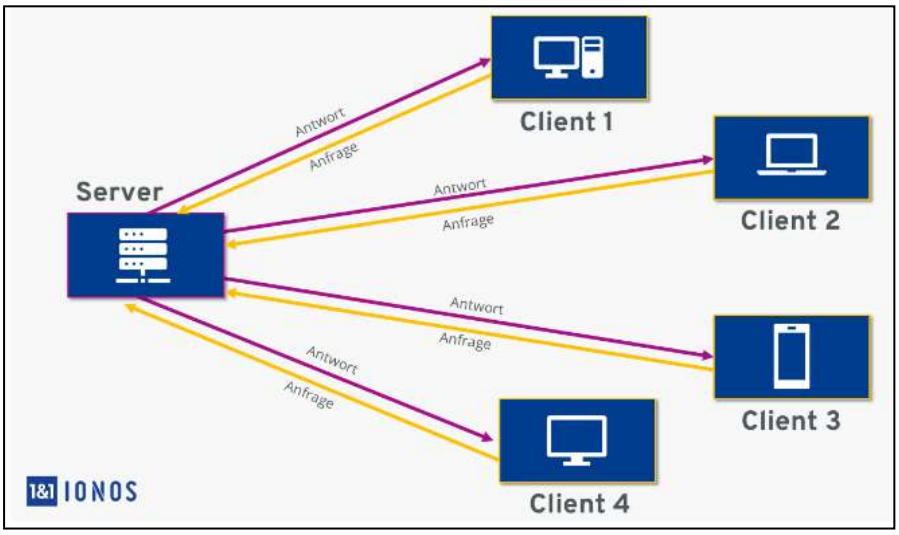


Abbildung 3 – Das Client-Server-Modell[50]

2.1.2.7 Kriminelle nutzen technische Möglichkeiten

Dass sich Kriminelle den Vorteilen der Kryptowährungen bewusst sind, ist unumstritten. Geldwäsche, Steuerhinterziehungen oder schnell viel Geld ins Ausland überweisen, ohne bei Kontrollinstanzen auffällig zu werden: Die Pseudonymität der Blockchain macht es möglich.[51] Mit Fiat-Geld ginge das nicht so einfach.

Doch auch Fiat-Geld kann für rechtlich umstrittene Ausgaben genutzt werden. Nicht selten bedienen sich Betrüger dem sogenannten (Cyber-)Crime-as-a-Service (CaaS). Gegen einen gewissen Preis bieten Spezialisten ihre Dienste im Internet an. „Der Markt wird auch als ‚Underground Economy' bezeichnet. Dabei handelt es sich um ein international vernetztes, organisiertes, kriminelles Konstrukt, über das illegal finanzielle Ziele bedient werden."[52]

Abbildung 4 zeigt, welche Dienstleistungen nach dem Neun-Säulen-Modell käuflich erworben werden können. Darunter zählen „Hacking-Angriffe, Bereitstellung und Verbreitung von Schadsoftware, Beschaffung und Verkauf sensibler Daten, […], Vermittlung von Finanz- oder Warenagenten, die die Herkunft der durch Straftaten erlangten Finanzmittel oder Waren gegen Bezahlung verschleiern, Bereitstellung von Kommunikationsplattformen zum Austausch von kriminellem Know-how, Anonymisierungs- und Hostingdienste zum Verschleiern der eigenen Identität und die Bereitstellung sogenannter Dropzones zum Ablegen illegal erlangter Informationen und Waren."[53]

---

[50] J. Behrens: Was ist ein Server? (2020) Abgerufen am 28.06.2022 von https://www.ionos.de/digitalguide/server/knowhow/was-ist-ein-server-ein-begriff-zwei-definitionen/.
[51] Vgl. P. Rosenberger: Bitcoin und Blockchain - Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik. (Berlin: Springer Vieweg, 2018) S. 35f.
[52] A. Brockhaus: Cybercime as a Service (CaaS) - So funktioniert die professionalisierte Cyberkriminalität. (2021) Abgerufen am 16.06.2022 von https://www.is-its.org/it-security-blog/cybercrime-as-a-service-caas-so-funktioniert-die-professionalisierte-cyberkriminalitaet.
[53] H.-J. Lange, T. Model und M Wendekamm: Zukunft der Polizei - Trends und Strategien. (Wiesbaden: Springer VS, 2019) S. 54.

Das BKA bezeichnet Dienstleistungen, die im Rahmen des CaaS angeboten werden, als „Teiltatbeiträge“.[54] Es ermöglicht „auch weniger cyber-affine[n] Straftäter[n] […], aus technischer Sicht komplexere Straftaten und Angriffsmodelle zu realisieren.“ [55]

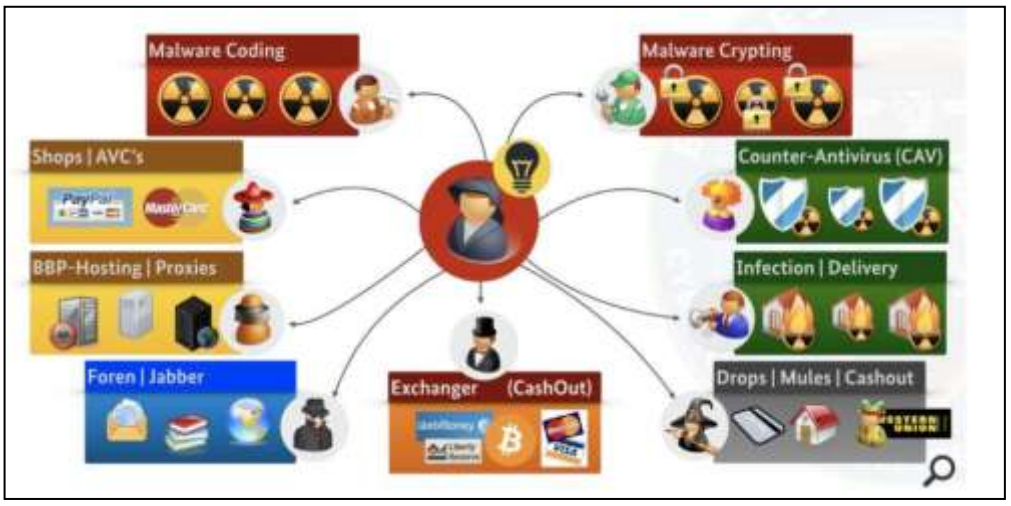


Abbildung 4 - Neun Säulen Modell: Cybercrime-as-a-Service[56]

Doch eine Webseite oder ein Programm können noch so gut gestaltet sein. Wenn der Anleger nicht die nötigen Kenntnisse hat, sie zu bedienen, nützt die Investition der Täter in den teuren Service nichts. Für solche Fälle wird Fernsteuerungssoftware missbraucht.

2.1.2.8 Fernsteuerungssoftware

Fernsteuerungssoftware, auch Remotesoftware oder Remote-Desktop genannt, verknüpft zwei Endgeräte über den Globus hinweg miteinander. Dabei handelt es sich nicht um eine Bildschirmübertragung im klassischen Sinne. Von außerhalb kann von einem Gerät auf ein anderes zugegriffen werden.[57] Während bei einer Telefonberatung der Kunde nach Anleitung des Kundenberaters agiert, kann der Kundensupport mittels Remote-Desktop die nötigen Handgriffe selbst vornehmen. Das spart nicht nur Zeit, sondern gibt dem Kunden ein Gefühl von intensiver fachkundiger Betreuung.

Dass solche Software auch von Betrügern genutzt wird, bietet sich regelrecht an. Die Kunden geben mangels besseren Wissens ihre Software-ID und Passwort an den Kundenberater weiter und gewähren ihm im besten Falle sogar Einblick in weitere sensible Daten, wie Logins, Bankdaten und persönliche Informationen. Sind die Betrüger einmal im

[54] Bundeskriminalamt: Abteilung "Cybercrime" (CC). (2022) Abgerufen am 13.05.2022 von https://www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/Cybercrime/cybercrime_node.html.
[55] Ebd.
[56] Ebd.
[57] Vgl. AnyDesk: Was ist ein Remote-Desktop und wofür wird er verwendet? (2021) Abgerufen am 16.06.2022 von https://blog.anydesk.com/de/was-ist-ein-remote-desktop-und-wofuer-wird-er-verwendet/.

Besitz dieser sensiblen Kundendaten, so können sie diese für ihre Zwecke missbrauchen. Zu den gängigsten Remote-Desktop-Programmen zählen TeamViewer[58] und AnyDesk[59].

2.1.3 Soziales

Wie in den vorangegangenen Abschnitten bereits geschlussfolgert werden kann, wird Cybertrading nicht durch einen Alleintäter betrieben. Die Zeit, Ressourcen und das nötige Know-how müssen von mehreren Teilnehmern gebündelt und zum Zwecke des Betruges eingesetzt werden. Dabei stellt sich natürlich die Frage, wer inwieweit bei dem Straftatphänomen Cybertrading beteiligt ist, geschweige denn über die Tat Bescheid weiß.

Für das bessere Verständnis muss also das Täternetzwerk auseinander genommen werden. Als abstrahiertes Beispiel dient Abbildung 5. Dargestellt wird eine Form der Hierarchie, wobei die Punkte P für Personengruppen einer jeweiligen Ebene stehen.

Es wird angemerkt, dass der Aufbau eines Netzwerks in unterschiedlichen Fällen niemals identisch ist. Das hier gezeigte Beispiel dient ausschließlich dem Zweck der Veranschaulichung für ein Beispiel von vielen Möglichen.[60]

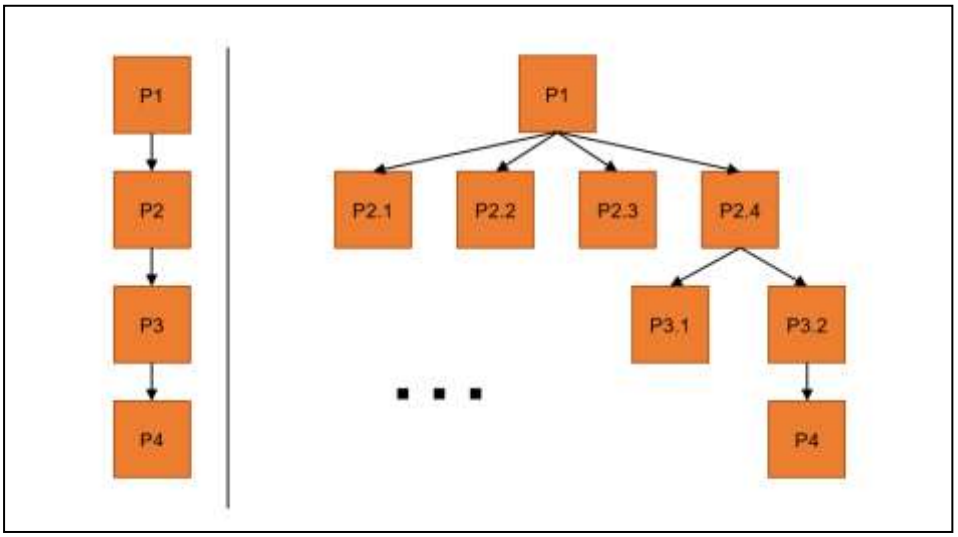


Abbildung 5 – Netzwerk der Beteiligten (vereinfacht)

P1: Am Anfang eines Netzwerks steht der Kopf einer Gruppe. Er ist zumeist derjenige mit der Idee. Seine Aufgabe ist es, Dritte für seine Idee zu begeistern und zur Beteiligung zu animieren. Beim Cybertrading ist dies das Interesse am schnellen und zahlreichen Geld.

[58] TeamViewer Germany: Digitale Transformation "Made in Germany". Abgerufen am 16. 06. 2022 von https://www.teamviewer.com/de/.
[59] AnyDesk: Access.Now. (2022) Abgerufen am 16. 06. 2022 von https://anydesk.com/de.
[60] Vgl. T. May und B. Bhardwa: Organized Crime Groups Involved in Fraud. Crime Prevention and Security Management. (London: Palgrave Macmillan, 2018) S. 57-68

P2: Basierend auf der durch P1 beworbenen Personen, besteht P2 aus einer Gruppe Eingeweihter. Ihnen wird, basierend auf ihrem Metier aus dem sie kommen, jeweils ein Teilbereich zugewiesen. Ihre Aufgabe besteht darin, wiederum Personen zu finden, die entsprechend des Fachbereiches besondere Fähigkeiten und Fertigkeiten aufweisen. So könnte P2.1 ein Bankkaufmann sein, der Kontakt zu wohlhabenden Geldgebern hat oder P2.2 ein Wirtschaftsinformatiker, der eng mit P2.3, einem Programmierer und P2.4, einem Angestellten für Unternehmenskommunikation zusammenarbeitet.

P3: In der dritten Gruppen finden sich die Eingeweihten zweiten Grades. Sie erhalten ihre Informationen von dem jeweiligen Vertrauten der Gruppe P2. Inwieweit die höher gestellten Rollen die Informationen an niedere Rollen weitergeben ist fraglich. Es wird angenommen, dass der Kreis der Eingeweihten verhältnismäßig klein ist, im Vergleich zu den Beteiligten. Demnach liegt es nahe, dass auch hier die Aufgaben weiterverteilt werden. Der Angestellte für Unternehmenskommunikation P2.4 hat bspw. Kontakt zur Geschäftsleitung einer Marketingfirma P3.1 und einem Jungunternehmer P3.2, der mehrere Callcenter in unterschiedlichen Ländern betreibt. Die Aufgabe von P3.1 könnte es sein, eine Werbekampagne für die Cybertradingplattform aufzustellen, Videos zu drehen und online Anzeigen zu schalten, um so viele Menschen wie möglich zu erreichen. P3.2 hingegen nutzt seine Callcenter als Vermittlungsportal, um über telefonischem Weg Kunden zu gewinnen.

P4: Da sich das Netzwerk ewig erweitern lassen könnte, kommen in der untersten Ebene der Hierarchie, hier Ebene 4, alle Personen zusammen, die schlussendlich Auswirkungen auf das Erscheinungsbild der Cybertradingplattform gegenüber dem Kunden haben. Ausgehend vom Zweig des Marketings betrifft dies die Schauspieler, Cutter, Tontechniker etc. Sie erhalten den Auftrag, eine Werbekampagne zu drehen und führen diesen aus. Dass sie dabei am Aufbau einer illegalen Betrügerplattform beteiligt sind, wissen sie höchst wahrscheinlich nicht. Parallel dazu nutzt der Jungunternehmer P3.2 seine Callcenter und dessen Angestellte für die Kundenakquise. Ihr Aufgabe ist simpel: Den Kunden ein Produkt verkaufen. Auch sie wissen vermutlich nicht, dass es das Produkt, wofür sie werben, nicht gibt. Gleichermaßen fallen auch die Retriever, die Geldrückholer in die Gruppe P4. Bei ihnen kann es sich erneut um unwissende Callcenter-Agents handeln oder um einzelne Personen, die in die illegalen Prozesse eingeweiht sind.

Es ist davon auszugehen, dass je niedriger die Ebene, umso weniger wissen die Beteiligten über das tatsächliche Vorgehen Bescheid. In jedem Fall gibt es pro Ebene einen Kontaktmann, eine Person, die als Informant für die jeweils höher gestellte Ebene fungiert. So ist die Informationsweiterleitung von der untersten bis zur obersten Ebene des Netzwerks gewährleistet.

Im Grunde erfüllt auch jede Personengruppe die Aufgabe des Recruiting. Abgeleitet aus dem Englischen, steht es für die „Suche nach bzw. Vermittlung von qualifizierten Arbeitskräften“.[61] Dabei kann jeder Knoten des Netzwerks wiederum ein eigenes Netzwerk und somit eine eigene Hierarchie bilden. Erst durch die Aufteilung der Aufgaben entwickelt

[61] Bibliographisches Institut: Recruiting. (2022). Abgerufen am 21.06.2022 von https://www.duden.de/rechtschreibung/Recruiting.

sich ein weit verzweigtes Netzwerk, dessen Verständnis sich teilweise erst bei vollständiger Betrachtung ergibt.

Doch nicht nur Arbeitskräfte werden vermittelt. Mittels Lead Recruiting werden potenzielle Kunden bzw. Opfer gesucht.[62] Der Begriff Lead hat hierbei nichts mit einer führenden Position zu tun, sondern mit den Kunden. Eine Lead Liste entspricht demnach einer Kundenliste[63], welche Personalien, E-Mails, Telefonnummern, Accountdaten u.v.m. enthalten. Diese Listen können von den Betrügerplattformen selbst erstellt und/oder von anderen Unternehmen (ab-)gekauft werden und vice versa. Die Rolle, die der Verkäufer dabei einnimmt, nennt sich Lead Dealer.

Jeder Zweig des Netzwerks hat also seine eigene Aufgabe. Der Erfolg der betrügerischen Masche hängt dabei in nicht unwesentlichem Maße vom Erfolg der einzelnen Zweige ab. Die Zweige sind interdependent voneinander. Angenommen der Programmierer P2.3 und sein Team aus Gruppe P3 stecken ihre gesamte Arbeitskraft in das Schreiben einer neuen Finanzsoftware und die Implementation einer schönen App. Doch die Marketingkampagne von P3.1 scheitert. Damit würde sich die Verbreitung der Software bzw. App erheblich verzögern. Das Risiko, weniger Geld zu machen, würde täglich steigen, während gleichermaßen auch das Entdeckungsrisiko wächst.

Der Aufbau eines Betrügernetzwerks ist demnach sehr komplex und möchte aus Sicht der Betrüger gut durchdacht sein. Ein solches Netzwerk allein zu organisieren, dürfte überaus schwer sein, wenn nicht sogar unmöglich. Erst durch Mithilfe anderer und durch Aufgabenteilung, nimmt die Last für jeden einzelnen etwas mehr ab. Dabei sollten sich die Beteiligten, sofern sie voneinander wissen, vertrauen können oder gar nicht erst über zu viele Informationen verfügen.

2.2 Ablauf der Straftat

Cybertrading ist ein Straftatphänomen des Betruges, welches sich der Wirtschaftskriminalität zuordnen lässt. Die deskriptiven Faktoren wurden bereits erläutert, weshalb nun zum eigentlichen Ablauf der Straftat übergegangen werden kann.

Es wird darauf hingewiesen, dass die Straftaten niemals identisch sind. Der hier beschriebene Ablauf ist rein exemplarisch und kann in anderen Fällen mehr oder weniger stark abweichen.

Ein Interessent möchte Geld anlegen. Durch Onlinewerbung stößt er dabei auf einen Link, der ihn zu einer Handelsplattform weiterleitet. Das Versprechen klingt gut: 250,00 Euro für Kryptowährungen investieren und in einem Monat verzehnfacht sich der Betrag. Daraufhin zahlt der Interessent 250,00 Euro ein und hinterlegt seine Kontaktdaten. Nur wenige Stunden später erhält er einen Anruf, sein persönlicher Kundenberater meldet sich. Er

[62] Vgl. AT Internet: Glossar - Lead. (2022). Abgerufen am 24.06.2022 von https://www.atinternet.com/de/glossar/lead/.
[63] Vgl. N. Shover, G. S. Coffey und C. R. Sanders: Qualitative Sociology: Dialing for Dollars: Opportunities, Justifications, and Telemarketing Fraud. Bd. 27 No. 1. (Tennessee: Springer, 2004) S.64.

bestätigt die Registrierung des Interessenten. Da der Interessent in Kryptowährungen investiert hat, benötigt er eine Wallet für die digitalen Münzen. Der Interessent hat leider keine Ahnung, wie er sich so eine Wallet anlegt und bittet den Kundenberater um Hilfe. Dieser zeigt sich hilfsbereit und bietet dem Interessenten an, per Remotesoftware auf seinen PC zuzugreifen und mit ihm gemeinsam ein Kundenkonto anzulegen.

Der Interessent lädt sich also die Software herunter und gibt seine ID an den Kundenberater weiter. Als die Zugriffsanfrage auf seinem Bildschirm erscheint, bestätigt er diese. Der Kundenberater greift von außerhalb auf den Browser des Interessenten zu und sucht nach der Handelsplattform. Dort legt er gemeinsam mit dem Interessenten ein Konto auf dessen Namen an und trägt ein Passwort ein. Um das Handelskonto zu verifizieren, muss der Interessent einen obligatorischen Cent auf sein neues Konto überweisen. Dazu gibt er dem Kundenberater seine Bankdaten weiter, damit dieser den Prozess für ihn durchläuft. Der Interessent bestätigt die Transaktion und nach kurzer Zeit erscheint der Cent auf dem neuen Handelskonto. Er bedankt sich für die Hilfe und beendet das Telefonat.

Innerhalb der kommenden Tage und Wochen ruft der Kundenberater regelmäßig beim Interessenten an. Da die Kurse einen Aufschwung erleben, animiert er den Interessenten zu weiteren Einzahlungen, um höhere Gewinne zu erzielen. Nach einem Monat hat der Interessent insgesamt 5.000,00 Euro in Kryptowährungen investiert. Für die weitere Zeit behält er den Kurs auf der Handelsplattform im Auge und steht mit seinem Kundenberater in regelmäßigem, teilweise unfreiwillig-aufdringlichem Kontakt.

Drei Monate nach der Ersteinzahlung hat sich eine beachtliche Summe auf dem Handelskonto angesammelt. Von den über 20.000,00 Euro möchte sich der Interessent einen Teil auszahlen lassen. Dazu fordert er vom Handelskonto den gewünschten Betrag von 10.000,00 Euro an. Es dauert nicht lange, da meldet sich sein Kundenberater. Das Geld könne nicht sofort ausgezahlt werden, es müssen erst die Steuern und eine Provision gezahlt werden. Also überweist der Interessent die geforderten Beträge an den Berater. Dieser verspricht sich am folgenden Tag zu melden, nachdem er mit seinem Chef gesprochen hat.

Daraufhin hört der Interessent nie wieder etwas von seinem Berater. Weder persönlich noch über das Servicetelefon ist jemand erreichbar. Der Interessent fühlt sich betrogen und erstattet Anzeige bei der Polizei.

Mittlerweile sind fast zwei Jahre vergangen, seit der Interessent sein Geld verloren hat. Die Polizei konnte bisher keine Tatverdächtigen ausmachen, da das Betrügernetzwerk im Ausland zu sitzen scheint.

Der Interessent erhält einen Anruf. Es ist ein Mitarbeiter einer Firma, die sich auf Schadensbegleichung betrogener Kryptoinvestoren spezialisiert. Offenbar haben sie die Wallet des Interessenten mit den digitalen Münzen im Wert von über 20.000€ sichergestellt. Da das Handelskonto wegen Betrugsmeldung jedoch eingefroren wurde, kann der Betrag nur mithilfe einer Ablösesumme i.H.v. 4.000,00 Euro freigegeben werden.

Der Interessent ist skeptisch, hatte er doch erst eine große Summe Geld verloren. Sein Erspartes ist weg, große Risiken kann er nicht eingehen. Doch will er sein damals investiertes Geld samt Gewinn gern wiederhaben. Also gibt er an, nur die Hälfte zahlen zu

können. Der Berater konnte diese Entscheidung nicht ohne Rücksprache mit seinem Chef treffen, weshalb er den Interessenten zurückrufen wollte.

Diesmal kommt am nächsten Tag tatsächlich ein Rückruf. Die Firma könne dem Interessenten die andere Hälfte vorgestrecken. Die Schulden könne er nach Auszahlung seines Guthabens auf dem Handelskonto begleichen. Er überweist den ersten Teil der Ablösesumme auf ein eigens dafür angelegtes Konto und wartet auf den Eingang des zweiten von der Firma. Mehrere Tage vergehen, in denen das Geld nicht auf dem Konto des Interessenten einging und er regelmäßig die Servicehotline anruft, welche ihn nur auf den nächsten Tag vertröstet. Schlussendlich kommt das Geld, jedoch viel mehr als vereinbart. Auf seine Rückfrage hin, erklärt ihm der Berater, dass es sich um zusätzliche Gelder handle, über die sich der Interessent keine Gedanken machen müsse. Er solle lediglich das Geld von dem Handelskonto an die Firma weiterleiten, damit sein Handelsguthaben freigegeben werden kann.

Nachdem der Interessent das Geld weitergeleitet hatte, wurde sein Handelskonto trotzdem nicht freigegeben. Stattdessen sollte er weiter Geldsummen an die Firma überweisen, die ihm zuvor überwiesen wurden. Schlussendlich überwiegt die Skepsis und der Interessent entscheidet sich, kein Geld mehr weiterzuleiten, solange sein Konto noch eingefroren ist. Daraufhin wirft ihm die Firma vor, sich nicht an die Abmachung zu halten und forderte ihr Geld zurück. In Folge dessen erstattet der Interessent erneut Anzeige wegen Betruges bei der Polizei.

2.3 Ermittlungen

Entschließt sich ein Geschädigter zur Polizei zu gehen, so dient seine Zeugenaussage als Grundbaustein und damit als Initiationshandlung für die Ermittlungen.

Besonderes Augenmerk gilt dabei natürlich der Plattform. Wird eine (Handels-)Plattform als betrügerisch eingestuft und sind Vermögensschäden in Bezug zu dieser Plattform entstanden, so erfolgen die Ermittlungen aufgrund des Tatorts vorranging im digitalen Raum.

Das Ziel der Ermittlungen besteht darin, ausgehend von den Informationen des Geschädigten die Kommunikations-, Verbindungs- und Transaktionswege zu verfolgen, um schlussendlich die Täter zu finden.

2.3.1 Verfolgung der Kontaktmöglichkeiten

Da die Täter mit den Geschädigten in irgendeiner Form in Kontakt gestanden haben müssen, werden, sofern vorhanden, Telefonnummern und E-Mail-Verkehr für die Rückverfolgung näher untersucht.

Wie ein E-Mail-Header beispielhaft aussieht, zeigen Abbildung 6 und Abbildung 7. Davon ausgehend, dass die empfangene E-Mail als Originalnachricht dargestellt werden muss,

um den Header anzuzeigen, stellen die rot hervorgehobenen Worte Platzhalter für tatsächlich verfügbare Daten der Täter dar. Die E-Mail-Adressen und IP-Adressen können im weiteren Vorgehen nach §100j StPO[64] und Telefonnummern nach §§173, 174 TKG[65] [66] abgefragt werden. Die Personalien können anschließend über polizeiinterne Systeme überprüft oder mittels OSINT recherchiert werden.

```
Delivered-To: *Email-Adr. Empfänger*
Received: by 2002:a17:906:2506:b0:730:82d3:1c5e with SMTP id i6csp115712ejb;
        Sun, 31 Jul 2022 09:40:00 -0700 (PDT)
X-Received: by *IPv6 Absender*                          with SMTP id f11-
20020a056870210b00b00101cb628cccmr6401707oae.26.1659285600701;
        Sun, 31 Jul 2022 09:40:00 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1659285600; cv=none;
        d=google.com; s=arc-20160816;
        b=kn3X7KWq04mrVsod2c7jqwsItaG2kaZGsI3/y8Howyl/xva+/po6TCPa1HtJ1VL7qB
         GJHBNgd5Zy9QdO+JgL7yUf+E1pmaev+LWsRlKL/GA4x66LAai3aMuoZX3Pgby5089X2z
         Gur2NiBbLSEz82kE6EExMVL2RPikQ6x7ujZGNPJRLbFZWoLqY4FPEOq9YtzlzZvh3SaO
         z5WBugobrhALWPwJIYRIIka+dj5XkLvVCot/V1W6OhQMa11oE1thtT+R2VY3tPepwa0t
         Hr3jf9gJ4hqWdFmzy0Tbr5sI1t8uE1+7J9fAvZH3WagRFHZwknfilIOU8UtGbyaSQ1Gv
         CwKg==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-
20160816;
        h=to:subject:message-id:date:from:mime-version:dkim-signature;
        bh=SJX4vjdgX2JaxpXdriZHGBFIvDpB6xLkwF3exgWysoQ=;
        b=ZuPO1Kmb4ort7wQwCq7oA2n+YcynmM9EDdjI0gS7Is26EsLUY2ZlF3cAKgrgG38wrn
         ZVi6fVAX0LlHSq2cCgztjqgyFuzjZv223xQE5Lms3iQ++TmHaUhnDs5loqkmm3v8BWO/
         XeN4isQJwq6ZFhTGGzrPP7O1i6qviAM9pHWopfILoBW5nVOUTyc8b403HjlKzNP7ths/
         Dk/TtvCn3lC19XobNM5x8t9eQvMZ3XFE0ynKe/3hx7pvCIICJCcBgKWGG0dRDkqZ/Cmd
         vr/eyPOb2LYC+MnTQ+kXELi3gb0R2qHuAq/E9yEM7gJT1hNkQSSFMc7nnrj5L4SdPHIb
         1ivA==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20210112 header.b=K2J00h8A;
       spf=pass (google.com: domain of *Email-Adr. Absender*  designates *IPv4 Absender*  as
permitted sender) smtp.mailfrom= *Email-Adr. Absender*
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
Return-Path:*Email-Adr. Absender*
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [ *IPv4 Absender* ])
        by mx.google.com with SMTPS id v203-
20020aca61d4000000b0033b2b051459sor1250514oib.171.2022.07.31.09.40.00
        for *Email-Adr. Empfänger*
        (Google Transport Security);
        Sun, 31 Jul 2022 09:40:00 -0700 (PDT)
Received-SPF: pass (google.com: domain of *Email-Adr. Absender*  designates *IPv4 Absender*
as permitted sender) client-ip= *IPv4 Absender* ;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20210112 header.b=K2J00h8A;
       spf=pass (google.com: domain of *Email-Adr. Absender*  designates *IPv4 Absender*  as
```

Abbildung 6 – E-Mail-Header 1/2

[64] Vgl. Bundesministerium der Justiz: Strafprozeßordnung (StPO) - §100j Bestandsdatenauskunft. (2022) Abgerufen am 29.06.2022. von https://www.gesetze-im-internet.de/stpo/__100j.html.

[65] Vgl. Bundesministerium der Justiz: Telekommunikationsgesetz (TKG) - § 173 Automatisiertes Auskunftsverfahren. (2021) Abgerufen am 29.06.2022 von https://www.gesetze-im-internet.de/tkg_2021/__173.html.

[66] Vgl. Bundesministerium der Justiz: Telekommunikationsgesetz (TKG) - § 174 Manuelles Auskunftsverfahren. (2021) Abgerufen am 29.06.2022 von https://www.gesetze-im-internet.de/tkg_2021/__174.html.

```
permitted sender) smtp.mailfrom= *Email-Adr. Absender*
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20210112;
        h=to:subject:message-id:date:from:mime-version:from:to:cc;
        bh=SJX4vjdgX2JaxpXdriZHGBFIvDpB6xLkwF3exgWysoQ=;
        b=K2J00h8Ajpgk5RtwDJYs3TeDwoGiL8m13AMSgsFzHT1FJzXeM/G/E7qCKNWFYyOIF7
         E6LyjVXs2HJ4L0GswpL19nkQni7p4R/ciyf7AQLRWV2aEpPXD4cGOtZdB7oEVoQOD+u9
         E7FfevxXXB3VydVQ9us9zDpguL/RPHsuLMfsmxtqEaNPMNKhz6qrBt2YKEEncDkaUdQT
         2gVNeA59UNOVfHrf6oHyMWzckNXm0U4QhMHkB9EcDYuENw7sWi+LYv7RmRBCSsg4ZrdA
         4j/z12YylvSXMGK7oQ0JmHCFId/pl+V7NteMlmZQRpUPKpR+mIZ1gS/x6Q9AcVpjMtIa
         pVOA==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=1e100.net; s=20210112;
        h=to:subject:message-id:date:from:mime-version:x-gm-message-state
         :from:to:cc;
        bh=SJX4vjdgX2JaxpXdriZHGBFIvDpB6xLkwF3exgWysoQ=;
        b=1nnGOHIZiE3LzTCJSlLeAFCYR0+eA+gB9mnWPIessqFphYpO/r9aJOmIxbfumEycTo
         fN6S+MCUBF98U1igIFND8aW8aYXHDTD158x3Em+u4YbbOte5BHAX4TTCDBlO5TG1lnXA
         ku3i+yTQ4pfTjTriP0QLi8AwYlFwKOTuqWVLgE9rAAHeh0vR9we2fc0SydimQmEetlMr
         IlliOCFqNTEzgZbL9ZsP55VWW0iz2qVnen4nbEGnz38TyMUPD6wtQWBTHLtseFndrsWk
         0vZCQNqzmWC+aMcRZFv0i27v6QrXvwZSrOIfJ6X0WAj4y4bP66YkOZchBNb0d+jARvgt
         6dFA==
X-Gm-Message-State: ACgBeo1/G3q0W9zGl2gZxTWGzllRGMtZNN2dmdXm4n1gY4uJI9SGS6nB
SFwOY5HpGBZJFrs4almzWH07gMHbvvBr25BJxXBiceID
X-Google-Smtp-Source:
AA6agR6ZfuZgJeM3GWP/4tAhRyVKQ/S+6meMyeZmvX9A5halzrgEH7ElW3uRM57rG9+is/yA/MnQR4iEv9Ta5
EbE+zk=
X-Received: by  *IPv6 Absender*                    with SMTP id x21-
20020a544015000000b003402eb762e9mr446836oie.65.1659285599973; Sun, 31 Jul 2022
09:39:59 -0700 (PDT)
MIME-Version: 1.0
From: "A. Franke" *Email-Adr. Absender*
Date: Sun, 31 Jul 2022 18:39:43 +0200
Message-ID: <CANZ=jXBPd-MMx+ig3hAKJ0ZJ93rf=9bmYShMYCFGo_Ue7e28GA@mail.gmail.com>
Subject: Test
To: *Email-Adr. Empfänger*
Content-Type: multipart/alternative; boundary="000000000000c4733805e51c8871"

--000000000000c4733805e51c8871
Content-Type: text/plain; charset="UTF-8"

Das ist ein Test.

--000000000000c4733805e51c8871
Content-Type: text/html; charset="UTF-8"

<div dir="ltr">Das ist ein Test.</div>

--000000000000c4733805e51c8871--
```

Abbildung 7 – E-Mail-Header 2/2

Wie viele Täter mit dem Geschädigten in Kontakt stehen, ist von Fall zu Fall unterschiedlich. Es ist von größter Wichtigkeit, die Täter und Drahtzieher der Netzwerke ausfindig zu machen und sie zu fassen. Das Auffinden der investierten Gelder der Anleger nimmt dabei eine untergeordnete Rolle ein.

2.3.2 Verfolgung der Geldströme

Werden Gelder bei den Ermittlungen gefunden, die den Tätern eindeutig zuzuordnen sind, können diese im Rahmen einer gerichtlich angeordneten Vermögensabschöpfung nach §73 StGB[67] eingezogen werden.

Um den Geldfluss zu verfolgen, werden Transaktionsübersichten erstellt und die Zielkonten der Überweisungen untersucht. Deutsche IBANs werden zur Überprüfung an die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) übermittelt, um die Existenz eines Kontos zu bestätigen/widerlegen und ggf. den Kontoinhaber zu ermitteln. Ausländische IBANs können nur mittels juristischer Rechtshilfe an das entsprechende Land oder mithilfe der FIU (Financial Intelligence Unit) abgefragt werden. Bei der FIU handelt es sich um eine Zollbehörde, deren Aufgabe in der Untersuchung auffälliger Transaktionen im Zusammenhang mit Geldwäsche innerhalb und außerhalb Deutschlands besteht.[68]

Für die Geldtransfers werden viele Konten bei unterschiedlichen Banken angelegt. Aufgrund der gesetzlichen Vorgaben, ist „[die] Bank […] verpflichtet, die Identität des Antragstellers [anhand von entsprechenden Ausweisdokumenten] zu überprüfen.“[69] Bei den Finanzermittlungen können somit in jedem Fall die Inhaber der bekannten Transferkonten ausfindig gemacht werden. Doch auch hier greift erneut die Problematik der Informationsweiterleitung. Es kann nicht ausgeschlossen werden, dass die Kontoinhaber nicht wissen, dass die unter ihrem Namen angelegten Konten für den Transfer betrügerisch erlangter Gelder missbraucht werden.

Die Transferkonten fallen besonders dadurch auf, dass sie zum einen vergleichsweise neu sind und zum anderen die Geldeingänge beinahe eins zu eins innerhalb kurzer Zeit wieder ausgehen. Abgesehen von Kontoführungsgebühren und den Transaktionen, verzeichnet das Konto meist keine weiteren Bewegungen.

Ergänzend dazu werden bei Transaktionen mit Kryptowährungen die genutzten Wallets betrachtet. Die entsprechenden IDs können vorerst über blockchair.com[70] betrachtet werden, um einen Überblick über die Transaktionshistorie zu erhalten. Für den gerichtsfesten Nachweis werden die IDs dem LKA übermittelt. Dort wird der Dienstleister festgestellt, welcher anschließend über die Inhaber der IDs beauskunftet werden kann.

2.3.3 Überprüfung anderer technischer Daten

Gleichermaßen werden User-IDs bei den Dienstleistern der Fernsteuerungssoftware abgefragt, um die Logdaten inklusive IP-Adressen, Zeitstempel, Verbindungspartner und

---

[67] Vgl. Bundesministerium der Justiz: Strafgesetzbuch (StGB) - §73 Entziehung von Taterträgen bei Tätern und Teilnehmern. (2021) Abgerufen am 27.06.2022 von https://www.gesetze-im-internet.de/stgb/__73.html.
[68] Vgl. Generalzolldirektion: Financial Intelligence Unit. Abgerufen am 01.07.2022 von https://www.zoll.de/DE/Der-Zoll/Aufgaben-des-Zolls/Schutz-fuer-Buerger-Wirtschaft-und-Umwelt/FIU-Aufgaben/fiu-aufgaben_node.html.
[69] BaFin: Basiskonto. (2017) Abgerufen am 24.06.2022.von https://www.bafin.de/DE/Verbraucher/Bank/Produkte/Basiskonto/basiskonto_node.html.
[70] Blockchair: Blockchain explorer, analytics und web services. (2022) Abgerufen am 01.07.2022 von https://blockchair.com.

Richtung der Verbindung zu erhalten. Die IP-Adressen können anschließend mithilfe einer Bestandsdatenabfrage überprüft werden.

Obwohl manche Täter ihre Präsenz zu verschleiern versuchen, indem sie VPNs (Virtual Private Networks) nutzen oder ausländische Telefonnummern anmieten, können die Ermittler hin und wieder Teilerfolge verzeichnen. Je schneller die Ermittlungen aufgenommen werden können und je unvorsichtiger die Täter sind, umso größer ist die Wahrscheinlichkeit, die frischen Spuren erfolgsversprechend verfolgen zu können.

So können beispielsweise Callcenter im Süd-Osten Europas mithilfe der ausländischen Behörden ausfindig gemacht werden. Im weiteren Vorgehen stehen zumeist die Verdichtung der Informationen rund um die Verdächtigen, sowie Durchsuchungen in den betroffenen Objekten an. Wie in Kapitel 2.1.3 Soziales aufgezeigt, zielen die Ermittlungen dabei vorrangig auf die höher gestellten Personen des Netzwerks ab. Sofern vorhanden, werden Computer, Server und andere beweiserhebliche Gegenstände nach §94 StPO[71] bzw. dem ausländischen gesetzlichen Äquivalent dazu beschlagnahmt oder sichergestellt.

In jedem Fall werden technische Geräte und/oder Daten nach der Beschlagnahme auf tatrelevante Inhalte untersucht. Besonders die Daten der Server der IT-Dienstleister oder Hoster haben großes Beweispotenzial in den Cybertrading-Fällen. Welche Daten der Dienstleister für die Auswertungen zur Verfügung stellt, ist von Anbieter zu Anbieter verschieden.

In vielen Fällen stehen die Server außerhalb des Herrschaftsgebiets der deutschen Strafverfolgungsbehörden, weshalb zumeist um Mithilfe der ausländischen Behörden und Dienstleister gebeten wird.

2.3.4 Datensicherung

Wenn ein Server gesichert wird, gibt es, abhängig von der zur Verfügung stehenden Technik und der Arbeitsweise des Hosts, vier Möglichkeiten. Abbildung 8 veranschaulicht diese.

[71] Vgl. Bundesministerium der Justiz: Strafprozeßordnung (StPO) - § 94 Sicherstellung und Beschlagnahme von Gegenständen zu Beweiszwecken. (2021) Abgerufen am 01.07.2022 von https://www.gesetze-im-internet.de/stpo/__94.html.

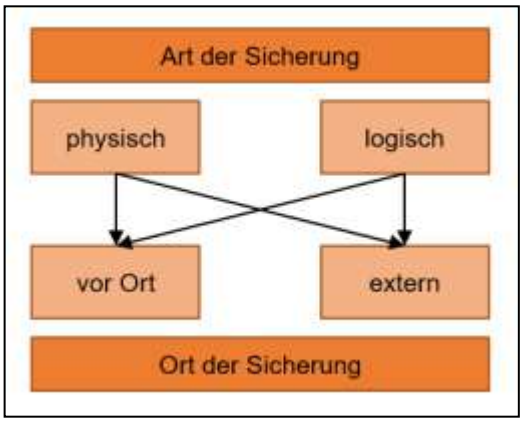


Abbildung 8 – Möglichkeiten der Datensicherung

Im Vergleich zur physischen Sicherung, bietet eine logische Sicherung nur Bruchteile von zu untersuchenden Daten. Der IT-Dienstleister übersendet den Ermittlern eine logische Kopie, welche nur die nötigsten Verzeichnisse des Servers enthält und somit keinen vollumfänglichen Einblick auf die Maschine liefert.

Als oberstes Gebot bei der Sicherung von digitalen Daten gilt, „[d]ie Unveränderthеit des Dateninhalts eines Datenträgers [zu wahren] […], wenn dieser ein Beweisstück eines juristischen Prozesses ist.“[72] Um bei einer physischen Sicherung zu gewährleisten, dass an den Originaldaten nichts verändert wird, werden Writeblocker als Schnittstelle zwischen dem zu untersuchenden und dem extrahierenden Gerät eingesetzt. Mithilfe von bspw. im BSI-Leitfaden benannten forensischen Werkzeugen wie dcfldd, LinEn oder EnCase und dem Writeblocker können so die Daten i.F.v. dumps auf ein anderes Speichermedium kopiert werden.[73]

Da der Leitfaden des BSI von 2011 heute teilweise überholt ist, werden zunehmend neue Techniken für eine digitale Sicherung genutzt. Für Linux-Systeme kommen u.a. dd, ddrescue und guymager zum Einsatz, während für Windows-Systeme eher FTK Imager, EnCase und X-Ways-Forensics genutzt werden.

Für die Auswertung der unterschiedlichen Datenträger wird vorrangig X-Ways Forensics[74] genutzt. Die Software bietet viele Möglichkeiten im Umgang mit digitalen Daten und deren Aufbereitung für die rechtssichere Beweiserhebung. Dazu wird das vorher gesicherte Image i.F.v. einem .E01-Image oder dd-Image eingebunden.

Zu Beginn der Analyse verschafft sich der Auswerter einen Überblick über die Datenträger anhand des Verzeichnisbaums am linken Fensterrand der Anwendung und dem Aufrufen der Eigenschaften. (siehe Abbildung 9) Ausgehend davon kann er erkennen, welches Betriebssystem auf dem Datenträger bzw. Server zur Zeit der Nutzung lief. Da sich die Betriebssysteme in ihrem Aufbau grundlegend unterscheiden, liegen die fallrelevanten Daten auch in unterschiedlichen Verzeichnissen.

---

[72] BSI: Leitfaden IT-Forensik, Vers. 1.0.1. (2011) S. 236.
[73] Vgl. ebd. S. 236f.
[74] X-Ways AG.: X-Ways Forensics: Integrierte Software für Computerforensik. Abgerufen am 04.07.2022 von http://www.x-ways.net/forensics/index-d.html.

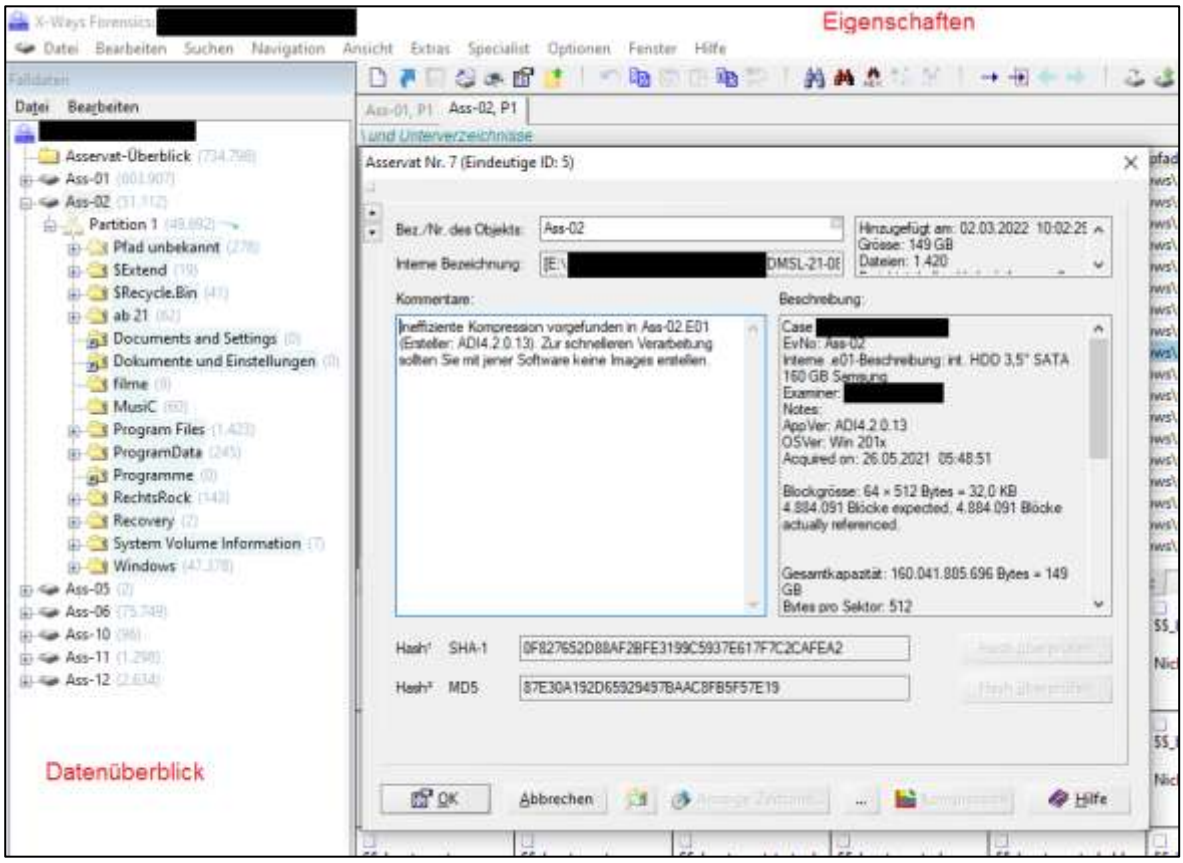


Abbildung 9 – Ausschnitt X-Ways-Forensics

In einem Linux-System sind die Verzeichnisse *etc*, *home*, *var* und falls vorhanden *opt* von großer Bedeutung. Für Auswertungen von Windows-Systemen werden, getrennt nach Nutzer, die jeweiligen Standardverzeichnisse untersucht, z.B. *appdata, Downloads, Dokumente* und *Desktop*. Ergänzend dazu werden globale Verzeichnisse wie *Programme*, *Programme x86* oder Systemdateien, darunter *SAM, SYSTEMS, SOFTWARE, SECURITY* und diverse Logfiles untersucht.

2.3.5 Serverauswertung

Der Einfachheit halber wird sich für eine beispielhafte Serverauswertung folgend nur auf eine physische Sicherung unter Linux bezogen, da so die größte Aussagekraft gegeben ist. Wo die folgend genannten Dateien jeweils liegen, kann sich von Distribution zu Distribution unterscheiden. Deshalb wird nachfolgend nur vom Web-, Datenbank-, Proxy-, Nutzer- und Mailverzeichnis gesprochen.

Die Server bieten die Grundlage zum Bereitstellen der Betrügerplattformen bzw. Webseiten. Zu Beginn der Auswertung steht die Kontrolle, ob und inwieweit ein Server aktiv genutzt wurde. Dazu gehören Daten, die auf eine Webseite hinweisen, diverse *config*-Dateien, das Datenbankverzeichnis und das Mailverzeichnis. Allgemein erfolgen die Auswertungen nach folgendem Schema:

Um Hinweise auf die Nutzer eines Systems zu erhalten, wird die *shadow*-Datei und das *home*-Verzeichnis betrachtet. Je nach zu untersuchender Linux-Distribution können Daten

zu Logins bspw. in den Systemdateien *secure*, *authlog* oder **tmp*[75] aufgefunden werden. In diesen könnten IP-Adressen und Zeitstempel eingetragen sein, die für weitere Abfragen zur Verfügung stehen.

Auch über die *history* der jeweils genutzten Shell, also den Befehls-Historien, können Informationen über den oder die Täter gesammelt werden. Agieren mehrere User, haben sie Skripte genutzt, welche Aktionen führt der User auf dem Server aus, worauf soll zugegriffen werden, wo wollten sie sich einloggen? All das kann der Auswerter den Zeilen im Idealfall entnehmen.

Um wichtige Informationen über die Systemzugriffe von außen zu erhalten, sucht der Auswerter nach Logfiles, hier *positive file* und *negative file* genannt.

Im *positive file* werden alle erfolgreichen Zugriffe auf den Server und die IP des Zugreifenden vermerkt. Dort lassen sich ggf. Hinweise zu weiteren Zugriffen von externen Servern finden und so das Netzwerk der tatrelevanten Geräte erweitern.

Ebenso interessant ist das *negative file*. Es speichert alle fehlgeschlagenen Zugriffsversuche auf ein Nutzerkonto des Servers und die IPs der Zugreifenden. Jedes System hat Standardnutzer, bei Linux wäre es bspw. root. Es ist üblich, dass auf diese Standardnutzerkonten regelmäßig und zumeist erfolglos von außerhalb zugegriffen wird. Findet jedoch ein Zugriff auf ein Nicht-Standardnutzerkonto eines Servers statt, bspw. ein Konto namens Lisa Müller, so kann davon ausgegangen werden, dass der Zugreifende von diesem Konto weiß.

Wenn die Täter agieren, dann zumeist mit verschleierten IPs über bspw. VPN. Unterlaufen ihnen jedoch kleine Fehler aufgrund von großer Eile, kann es vorkommen, dass sie vergessen den VPN zu aktivieren. Ohne VPN kann der Auswerter die Klar-IP der Täter erhalten und abfragen.

Unter Umständen können aus diversen *config*-Dateien Passwörter eingesehen werden. Deren Nutzen liegt viel weniger im Versuchen des Einloggens, als im Vergleich zweier beschlagnahmter Server. Ähnliche Passwörter können auf eine (un-)bekannte Tätergruppe hindeuten.

Das Gleiche gilt für die Webadresse einer Plattform. Die Webseiten besitzen entsprechende Adressen, welche unter Linux im Webverzeichnis des Servers abgelegt werden. Für den Fall die Webseite wurde bereits aus dem Netz genommen, kann der Auswerter diese mithilfe der entsprechenden Dateien zu Beweiszwecken virtualisieren.

Aus den Daten der Webseite können ggf. Rückschlüsse auf weitere Brands[76] gezogen werden. So heißt eine untersuchte Webseite bspw. Stockfunds.com, doch im Quelltext der Seite angegebene Daten verweisen auf Moneyfunds.com. Diese beiden Brandnamen lassen sich demnach eindeutig korrelieren und als Indizien werten. Angenommen es liegen beide WordPress-Datenbanken vor, dies wäre der Idealfall, so kann ein Abgleich der

[75] Das Zeichen * steht in dem Fall für u, b oder w und wird abhängig von der Linux-Distribution eingesetzt.
[76] Als Brand wird der Name einer Plattform der Betrüger bezeichnet.

genutzten CPIs und CRMs erfolgen. Sollten beide Brands auf denselben Server verweisen, wäre dies der direkte Nachweis für eine Zusammengehörigkeit der Brands, deren Webseiten als Landing-Pages[77] genutzt werden. Abbildung 10 veranschaulicht dies.

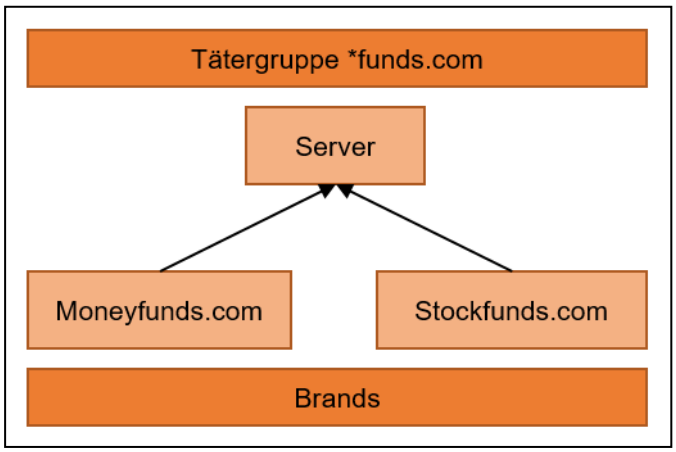


Abbildung 10 – Beispielhafte Verbindung zweier Brands

In diesem Zusammenhang herausfordernd für den Auswerter ist die Tatsache, dass hunderte solcher Landing-Pages aufgesetzt werden und deren BackOffice[78] namentlich nicht zwingend zum vorliegenden Brand passen muss. Die schiere Menge an Brands und zugehörigen Daten erschwert die Zuordnung.

[77] Eine Landing-Page ist die erste Webseite, die ein User besucht, wenn er auf der Suche nach der Investitionsplattform ist.
[78] Das BackOffice einer Webseite enthält die für eine Webseite hinterlegten technischen Daten.

3 Methodik

Für die praktische Bearbeitung des Themas Cybertrading werden Erkenntnisse aktueller Fälle zusammengetragen. Dies beinhaltet sowohl die Aufarbeitung von Fallakten als auch das Führen von Interviews mit Beteiligten des strafrechtlichen Prozesses und Literaturstudien.

Anlass dazu bietet die Gegebenheit, dass aufgrund der Aktualität und doch zeitgleichen Unbekanntheit des Themas Cybertrading keine umfängliche Lektüre zu finden ist. „Die Medien berichten beinahe täglich aus der Welt der Wirtschaftsdelikte. Im Fokus stehen insbesondere überzeugende, charismatische Persönlichkeiten, die das Vertrauen ihrer Anleger, Aktionäre und Stakeholder aufs Gröbste missbraucht haben […].“[79] Über die digitale Variante dessen, das Cybertrading, alternativ auch Boiler Room Fraud genannt, werden lediglich wenige Artikel geschrieben. Warnhinweise und Aufklärung zum Thema digitaler Anlagebetrug? – Nicht oft genug. Nur wer intensiv danach sucht, wird fündig.[80] [81] [82] Umso wichtiger ist es, dass dieses Straftatphänomen endlich ausgiebig beleuchtet wird und zusätzliche (Experten-)Interviews die Unwissenheit beseitigen. Dort, wo aus Kapazitätsgründen keine Interviews geführt werden können, wird auf Lektüre zurückgegriffen.

Ausgehend von Fallakten werden erste Informationen zu den Sachverhalten zusammengetragen. Durch die Bearbeitung der Fälle werden diese mittels weiterer polizeilicher Maßnahmen wie Auskunftsersuchen und Abfragen erweitert. Die erweiterten Erkenntnisse bilden die Grundlage für die ausgearbeiteten Fragebögen und Interviews.

Bei den Interviews liegt der Fokus auf der Qualität. In der Kürze der Zeit war es der Autorin nicht möglich, eine breite Masse an Beteiligten zu befragen. Umso mehr wurde darauf geachtet, Personen aus verschiedenen Bereichen zu dem Thema zu interviewen, um den Umfang der Einschätzungen und Erfahrungen entsprechend groß zu halten. Für diese Arbeit wurden fünf Interviews und ein fachbereichsspezifisches Literaturstudium durchgeführt.

Die Gesprächspartner werden basierend auf den deskriptiven Faktoren aus Kapitel 2.1 gewählt. Basierend auf internen Kontakten der Polizei Sachsen wurden passende Kandidaten für die Interviews ausgewählt und angeschrieben. Im Anschreiben (siehe Anhang 2) wird auf die Relevanz des Themas Cybertrading aufmerksam gemacht. Um die Kandidaten zu motivieren, wird betont, dass die Zusammenarbeit von großer Bedeutung für die

[79] S. Stirnimann: Der Mensch als Risikofaktor bei Wirtschaftskriminalität - Handlungsfähig bei Non-Compliance und Cyberkriminalität. (Wiesbaden: Springer Gabler, 2021) S. VII.
[80] Vgl. C. Deker et al: Ermittler zerschlagen Betrügerring. (2019) Abgerufen am 21.06.2022 von https://www.tagesschau.de/investigativ/ndr/trading-portale-101.htm.
[81] Vgl. M. Zierer und H. Tanriverdi: Abzocke mit Bitcoins. (2022) Abgerufen am 21.06.2022 von https://www.tagesschau.de/investigativ/br-recherche/bitcoin-betrug-101.html.
[82] Vgl. C. Uhl und N. Resch: Prozess um Cybertrading-Portale startet. (2022) Abgerufen am 21.06.2022 von https://www.tagesschau.de/investigativ/trading-portale-betrug-prozess-101.htm.

schriftliche Ausarbeitung ist. Dabei wird vollste Anonymität zugesichert (siehe Anhang 3) und die ausschließliche Verarbeitung der Daten zu wissenschaftlichen Zwecken.

Bei der Zusage des Kandidaten entscheidet dieser über Ort und Zeit des Interviews. Dazu zählt auch seine freie Wahl, zwischen einem persönlichen oder telefonischen Gespräch. Er soll bei einer angenehmen Atmosphäre frei sprechen können, ohne sich durch äußere Faktoren verunsichern oder beeinflussen zu lassen.

Die Interviews werden von der Autorin selbst durchgeführt. Zu Beginn wird den Respondenten der Interviewleitfaden vorgestellt. (siehe Anhang 4) Er beinhaltet eine Erklärung zum Umfang des Interviews, den Grund für dessen Durchführung und betont erneut die Anonymität des Gesprächspartners. Anschließend wird um Bestätigung der Aufzeichnung per Tonband gebeten.

Die Interviews erfolgen teilstrukturiert. Vorab formulierte Fragen bilden einen roten Faden für das Gespräch. Die Fragen werden jedoch nicht vorab bekannt gegeben. Für den Einstieg des Gesprächs bietet es sich an, dass sich der Respondent vorstellt und über seine Tätigkeit erzählt. Im Anschluss werden die Fragen besprochen. Basierend auf den Antworten der Respondenten können anschließende Fragen und Anmerkungen vom Leitfaden abweichen. Dabei wird darauf geachtet, dass sich die Antworten nicht zu weit vom Themenbereich entfernen, um den Zeitrahmen nicht zu überstrapazieren. Abgerundet wird das Interview, indem die Respondenten abschließende Anmerkungen, Anregungen oder Kritiken äußern können.

Da sich eine einzelne Person unmöglich alles Wissen selbstständig zum Themengebiet Cybertrading aneignen kann, bedarf es der Mithilfe der spezialisierten Beteiligten im strafrechtlichen Prozess. Das Ziel der Interviews besteht darin, von den Erkenntnissen der Respondenten aus unterschiedlichen Fachbereichen zu partizipieren und Antworten auf die Leitfrage, welche Herausforderungen im Umgang mit Cybertrading auftreten, zu finden.

Die Tonbandaufzeichnungen werden von der Autorin persönlich transkribiert. Dabei werden irrelevante Füllwörter wie „ähm“ entfernt und Pausen weggekürzt. Spezifische Angaben wie Institutionsnamen oder Personalien werden soweit möglich generalisiert. Für das optimale Leseverständnis werden einige Sätze umgestellt und Einschübe entsprechend vermerkt. Aufgrund der zugesicherten Anonymität gegenüber den Gesprächspartnern, werden alle Personen mit einem entsprechenden Code abgekürzt. Die genaueren Bezeichnungen folgen im nächsten Kapitel. Die Autorin und zugleich Fragenstellende wird jeweils mit A abgekürzt. Die Transkripte sind unter Anhang 6 zu finden.

Ausgehend von den Transkripten, werden die Antworten der Respondenten anschließend qualitativ analysiert und in einen Sinnzusammenhang gebracht. Eine Gegenüberstellung aller Antworten und Erkenntnisse erfolgt in Kapitel 5, um Gemeinsamkeiten und Unterschiede in Abhängigkeit vom Fachgebiet zu eruieren.

Es finden Gespräche mit folgenden Personen aus folgenden Gründen statt:

Für das Verständnis des sozialen Faktors wird ein Gespräch mit einem Geschädigten geführt. Ziel ist das Verständnis über die Betrugsmasche und die dabei beteiligten Perso-

nen des Netzwerks zu gewinnen. Außerdem ist es wichtig zu betrachten, welche Folgen der Betrug für den Geschädigten hat.

Als Vertreterin der Wirtschaft wird eine Bankkaufrau interviewt. Da es sich bei Cybertrading um einen Anlagebetrug und damit teilweise einhergehende Geldwäsche handelt, sind die Erkenntnisse und Herausforderungen seitens der Banken von großer Bedeutung. Welche Erfahrungen konnten durch diese Betrugsfälle gemacht werden, wo liegen Schwierigkeiten im Umgang mit so einem Fall und welchen Handlungsbedarf sehen die Banken bei sich selbst und bei der Strafverfolgung.

Um den Faktor Technik und Ermittlung zu untersuchen, werden ein Ermittler und ein IT-Experte der Polizei Leipzig befragt. In Zusammenarbeit werden Cybertrading-Fälle von Beginn an aufgearbeitet, anfallende digitale Daten analysiert und betrügerische Aktivitäten im In- und Ausland untersucht. Wichtige Fragen an der Stelle befassen sich mit dem Aufwand und den Möglichkeiten der Polizei, Cybertrading-Fälle strafrechtlich zu verfolgen.

Ergänzend dazu führt eine Unterhaltung mit einer Juristin zur rechtlichen Einordnung des Themas. Dabei soll geklärt werden, worauf die Justiz bei der Strafverfolgung besonders großen Wert legt, wo Probleme in der Kette der Zuständigkeit bzw. bei den Handlungsmöglichkeiten auftreten und wo Verbesserungen durchgesetzt werden sollten.

Da sich für den Einblick in die Tätertypologie kein Gesprächspartner im vorgegebenen Zeitraum gefunden hat, wird der Aspekt der Psychologie mithilfe von Lektüre näher betrachtet. Kernfragen befassen sich mit den Merkmalen eines Täters, sowie der Erfolgsstrategie der Betrugsmaschen.

4 Durchführung und Ergebnisse

Basierend auf den eigens geschaffenen Erkenntnissen bei der Bearbeitung von Cybertrading-Fällen, werden kurze, fachbereichsspezifische Fragebögen (siehe Anhang 5) angefertigt und mit den jeweiligen Interviewpartnern besprochen. Die Transkripte der Interviews befinden sich im Anhang 6.

Eine kurze Zusammenfassung der Parameter befindet sich in Tabelle 2.

Tabelle 2 – Parameter der Interviews[83]

Code für Respondent	Datum des Interviews	Beginn des Interviews	Art des Gesprächs	Dauer des Interviews in Minuten	Dauer der Aufnahme in Minuten
Geschädigter (GES)	17.07.2022	16.20Uhr	persönlich	35	23:44 + 9:34
Kriminalpsychologe (KPS)	--	--	--	--	--
Bankkauffrau (BKF)	02.08.2022	16Uhr	Telefonisch	45	40:11
Ermittler (E)	11.07.2022	13.40Uhr	persönlich	30	27:12
IT-Experte (ITE)	27.07.2022	13.30Uhr	persönlich	65	59:06
Juristin (JU)	12.07.2022	9.50Uhr	persönlich	30	27:39

[83] Adaptiert nach A. Schuchter: Perspektiven verurteilter Wirtschaftsstraftäter - Gründe ihrer Handlungen und Prävention in Unternehmen. (Wiesbaden: Springer Gabler, 2012) S. 215.

4.1 Geschädigter (GES)[84]

Das Gespräch mit dem Geschädigten fand am 17.07.2022 statt und erfolgte persönlich. Durch einen mehr oder weniger (un-)glücklichen Zufall handelt es sich dabei um eine Bekanntschaft, die bereits außerhalb der wissenschaftlichen Arbeit bestand. Entsprechend ist das Gespräch als sehr offen und ehrlich einzuschätzen. Die Fragen zielten vorrangig auf seinen Alltag und seine Erfahrung mit den Tätern ab.

Der GES ist Rentner und füllt seinen Tag mit üblichen Haushaltsarbeiten. Nebenher macht er Musik und verbringt seine Zeit gern im Garten. Die Entscheidung, Geld anlegen zu wollen, kam ihm, als er bei Facebook auf eine Annonce stieß. Er investierte eine Startgebühr von 256,00 Euro und gab seine Daten an. Zunächst war es die reine Neugier, die ihn zu der Investition verleitete. Doch wie er selbst sagt, haben ihn die Täter ständig in neue Gespräche verwickelt, wobei sie schlussendlich an seinen wunden Punkt gerieten und ihn manipulierten. Er selbst brauchte das Geld nicht, doch für seine Tochter, die sich irgendwann selbstständig machen wollte, legte er schlussendlich 4.000,00 Euro an und verlor es an die Betrüger.

Der GES erzählt, dass er kurze Zeit nach der Investition einen Anruf von einer österreichischen Nummer erhielt. Eine Frau mit ausländischem Akzent versuchte ihn auf die Plattform zu navigieren. Laut Aussage des GES hatte die Frau jedoch keine Ahnung und verwies ihn an einen Kollegen, einen Herrn Schmidt. Dieser wiederum wusste, wovon er sprach und beriet den GES bei seinen Investitionen, half ihm beim Zurechtfinden auf der Webseite bzw. der dazugehörigen Tradingapp. Herrn Schmidt schätzt der GES als sehr kompetent und vorbereitet ein, gleichzeitig jedoch als sehr manipulativ. Herr Schmidt setzte ihn dem psychischen Druck aus, sein Geld zu verlieren, würde er die günstigen Gelegenheiten nicht nutzen und nicht mehr investieren.

Als dem GES suggeriert wurde, er hätte 10.000,00 Euro auf dem Handelskonto, wollte er sich die Hälfte auszahlen lassen und mit dem Rest weiter handeln. Die Funktionstaste der Webseite funktionierte jedoch nicht. Auf seine Frage hin, wieso das nicht funktioniert, gab es nie eine anständige Antwort.

Die Täter versuchten natürlich dem GES noch mehr Geld zu entlocken. Dieser wollte aber nicht mehr zahlen und gab an, nicht mehr zu besitzen. Der Kundenberater verwies jedoch auf den Kontostand des GES. Er wusste, wie viel der GES besitzt und dass er sehr wohl mehr investieren könnte. Der GES gibt an, dass dies der ausschlaggebende Punkt gewesen ist, an dem er der Plattform und den Tätern sein Vertrauen entzog. Er wollte das Verhältnis beenden und forderte sein Geld zurück.

In den vergangenen Wochen und Monaten kontaktierten ihn die Täter mehrfach und forderten ihn auf, die Schulden zu begleichen. Diese umfassen jedoch nicht nur die Einzahlung des GES sondern auch die Gewinne, die er damit erzielt hatte, also in Summe 20.000,00 Euro. Weil er darauf nicht einging, meldete sich ein Geldrückholer bei ihm. Das Angebot: vier Mal 5.000,00 Euro einzahlen und die damals investierten 4.000,00 Euro

[84] Vgl. Anhang 6.1: Transkript – Interview – GES.

zurück erhalten. Weder nach den Gesetzen der Mathematik, noch für den GES ergibt das einen Sinn. Der GES wird bis heute kontaktiert und zu Zahlungen aufgefordert. Darauf reagiert er, indem er die Kontakte blockiert oder schlichtweg ignoriert.

Auf die Frage hin, ob der GES von dieser Masche bereits vor dem Betrug Kenntnis hatte, verneint er. Er hatte sich schon vorher für Aufklärungs- und Präventionssendungen im Fernsehen interessiert, doch Cybertrading wurde dabei nie angesprochen. Erst durch seine eigenen Recherchen, stieß er auf weitere Fälle, teilweise auch zur Plattform selbst. Zu dem Zeitpunkt hatte er jedoch bereits investiert.

Das Verhalten der Täter durchläuft nach Aussage des GES einen Wandel. Abhängig von der Bereitschaft zu investieren, wechselt es von freundlich zu frech und grantig.

Als besonders auffällig, war die Person des Kundebetreuers, Herrn Schmidt. Abgesehen davon, dass er nie etwas über sich preisgegeben hat, ist der GES davon überzeugt, dass sich zwei Personen als Herr Schmidt ausgegeben haben. Der erste Herr Schmidt gab dem GES eine Telefonnummer, die er angeben sollte, wenn sich eine fremde Person bei ihm meldet. Von dieser Nummer wusste der zweite Herr Schmidt jedoch nichts. Auch der Geldrückholer erweckte Zweifel beim GES, da der Täter zwar dessen Kontaktdaten besaß, jedoch keinerlei Wissen über die Plattform geschweige denn die Investitionen des GES.

Bis heute hat der GES sein Geld nicht zurück erhalten. Vor finanzielle Schwierigkeiten hat ihn der Verlust jedoch nicht gestellt. Er gibt an, dass es durchaus weh tut, so hintergangen zu werden. Mit dem Geld, was er hat und noch verdient, kommt er gut zurecht. Auch gesellschaftlich wurde er nicht verurteilt. Er hat nur seinem engsten Kreis davon erzählt, obwohl es ihm unangenehm war.

Die Erfahrung, die der GES mehr oder weniger freiwillig gemacht hat, schreckt ihn vor künftigen Anlagen im Internet ab. Obwohl er skeptisch war hat er diese moderne Form der Anlagemöglichkeit ausprobiert und nun seinen Lehre daraus gezogen. Für die Zukunft will er sein Geld ausschließlich der Bank anvertrauen.

Anderen Interessenten rät der GES ausdrücklich von den Onlineplattformen ab. So lukrativ die Angebote auch klingen, so groß ist auch das Risiko, auf Betrüger hereinzufallen. Solange sich ein Anleger über die Seriosität und den Erfolg des Angebots nicht sicher sein kann, sollte er besser auf die Banken und die Börse zurückgreifen.

4.2 Kriminalpsychologie (KPS)

Interviewanfragen an das LKA Sachsen wurden mit Verweis auf mangelnde wissenschaftliche Erkenntnisse zum Phänomenbereich Cybertrading abgelehnt. Auch Anfragen bei Autoren wissenschaftlicher Lektüre blieben erfolglos. Eine Rückmeldung des BKA erfolgte außerhalb des festgelegten Bearbeitungszeitraums, weshalb an der Stelle abgesagt werden musste. Aus diesem Grund wird der Aspekt der Tätertypologie ausschließlich durch Lektüre erläutert, deren Ergebnis einen Teil der Fragen aus Anhang 5.2: Interviewfragen – KPS abdeckt.

Es sei angemerkt, dass die Lektüre sich auf Betrüger der analogen Welt bezieht und keinen direkten Bezug zum Straftatphänomen Cybertrading besitzt. Es kann jedoch davon ausgegangen werden, dass sich die ein oder andere kriminalpsychologische Einschätzung gleichermaßen auf Betrüger des digitalen Raumes übertragen lässt.

4.2.1 Betrug und Kriminalitätstheorien

Zu einem Betrug gehören grob formuliert mindestens zwei Parteien, ein Betrüger und ein Betrogener. Die Gründe, weshalb sich Menschen dafür entscheiden zu betrügen, könnten vielfältiger nicht sein. Entsprechend gibt es viele Kriminalitätstheorien, die mit wachsenden Erkenntnissen und Erfahrungen weiter überarbeitet wurden.

Die erste dieser Theorien ist die Rational-Choice-Theorie[85]. Sie besagt, dass eine kriminelle Handlung eine rationale Entscheidung bedarf, bei der der Täter die Kosten und den Nutzen abwägt. Zu dieser Theorie zählt das Routine-Aktivitätsmodell von Cohen und Felson von 1979.[86] Es umfasst die drei Komponenten *Tatmotivation*, *Schutz des Ziels* und das *Tatobjekt*. „Je höher die Tatmotivation, günstiger die Gelegenheit und geringer der wahrgenommene Schutz, desto wahrscheinlicher wird eine betrügerische Handlung.“[87]

Das wohl bekannteste Modell stammt aus der Mitte des 20. Jahrhunderts und wurde vom Kriminologen Cressey entwickelt.[88] Mithilfe des Fraud-Triangles versuchte er die Beweggründe für Betrugsstraftaten zu erklären. Die drei Eckpunkte dieses Modells sind der innere und äußere *Druck* auf den Täter, die *Gelegenheit* zur Tatbegehung und die *Rationalisierung* der Tat. Die Fraud Scale von Albrecht und Kollegen greift diese Komponenten ebenfalls auf, ersetzt die Rationalisierung jedoch mit *Integrität*.[89] Erst ein halbes Jahrhundert später entwickelten Wolfe und Hermanson das Triangle-Modell weiter zu einem Fraud-Diamond, indem sie die Komponente *Fähigkeit* des Täters ergänzten.[90]

Während das Fraud-Triangle bzw. der Fraud-Diamond sich mit den Beweggründen für die Tatbegehung beschäftigen, liegt der Fokus des Triangle of Fraud Action auf den Handlungen, die ein Betrüger begeht.[91] Dazu zählen die *Tat* selbst, *Verschleierungsmaßnahmen* und die *Umwidmung* der Beute in nützliches Gut für den Betrüger.

Es wird, wie auch bei anderen Straftaten, unterschieden zwischen Gelegenheitstätern und Gewohnheitstätern.[92] Um das betrügerische Handeln zu erklären, entwickelte Hoffmann 2015 die Pyramide des Betruges, welche in Abbildung 11 dargestellt wird.

[85] Vgl. M. Allwinn, et al: Betrügerisches Verhalten aus kriminalpsychologischer Sicht. (2018) S. 33.
[86] Vgl. ebd.
[87] Ebd.
[88] Vgl. ebd.
[89] Vgl. ebd. S.34f.
[90] Vgl. ebd. S. 35.
[91] Vgl. ebd. S. 34.
[92] Vgl. ebd. S. 40.

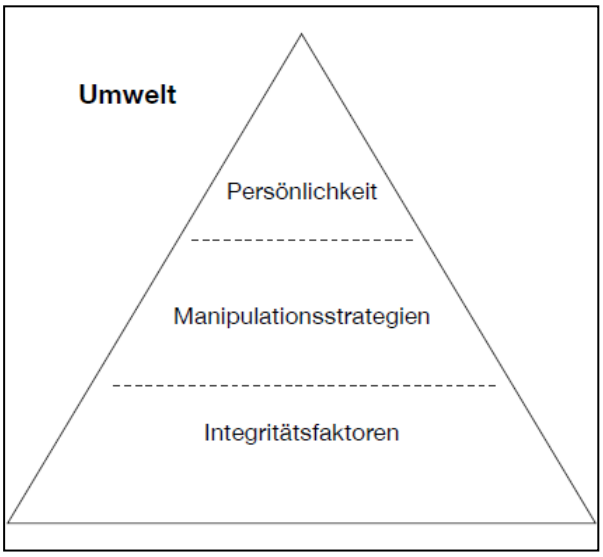


Abbildung 11 – Pyramide des Betruges nach Hoffmann[93]

Die Pyramide wird gestützt von der *Ebene der Integrität*. Dazu zählen sämtliche Rationalisierungstechniken, tatbegünstigende Normen und Werte des Täters sowie die Bereitschaft zur Begehung einer Betrugsstraftat.

Die zweite Ebene umfasst die *Manipulationsstrategien*. Hier befinden sich die Fähigkeiten eines Täters, welche zum Taterfolg beitragen.

Die dritte Ebene beinhaltet alle *Persönlichkeitsmerkmale und –eigenschaften* des Täters. Es wird angenommen, dass der größte Erfolg einer Tat auf der höchsten Ebene der Pyramide zu erreichen ist. Gleichzeitig erfolgt mit jeder höheren Ebene der Pyramide ein Übergang von Gelegenheitstat zu professioneller Tat.

Beeinflusst wird dieses Modell durch *Umweltfaktoren* wie Kontroll- und Sicherheitsmechanismen und Strafverfolgung.

4.2.2 Der Charakter des Betrügers

Bei jedem Menschen bilden sich Charakterzüge im Laufe der Entwicklung aus. Gewisse Merkmale werden angeboren, andere durch das Zusammenleben mit Anderen erlernt.[94] Obwohl es keine allgemeingültige Betrügerpersönlichkeit gibt[95], so fallen doch drei Charakterstile regelmäßig auf.

Der erste ist der *narzisstische Betrüger*[96]. Narzissten stehen gern im Mittelpunkt. Ihr Leben dreht sich um Erfolg und Ruhm. Doch so groß ihre Selbstverliebtheit auch ist, so verletzlich ist ihr Selbstwertgefühl. Trifft eine entgegengesetzte Meinung die des Narzissten,

[93] Vgl. M. Allwinn, et al: Betrügerisches Verhalten aus kriminalpsychologischer Sicht. (2018) S. 41.
[94] Vgl. J. Hoffmann: Psychologie von Betrügern. (2011) S.15.
[95] Vgl. M. Allwinn, et al: Betrügerisches Verhalten aus kriminalpsychologischer Sicht. (2018) S. 35.
[96] Vgl. J. Hoffmann: Psychologie von Betrügern. (2011) S.15.

reagiert dieser häufig gereizt, aggressiv oder abwertend“[97]. Sie wollen bewundert werden, nicht kritisiert. Dass sie dabei große Geldsummen für Statussymbole ausgeben, ist nur ein Schritt zum Erfolg.

Der zweite Charakter ist der *psychopathische Betrüger*.[98] Psychopaten werden Merkmale wie Angstlosigkeit und mangelnde Loyalität ihren Mitmenschen gegenüber zugeschrieben. Sie werden als risikobereit und impulsiv eingeschätzt. „Sie sind wahre Egoisten.“[99] Ihre Fähigkeiten Gefühle nachzuahmen und Menschen entsprechend erfolgreich zu täuschen, zeichnen sie besonders aus. Jedoch schrecken sie auch nicht vor der Erniedrigung anderer zurück. Sie wollen zeigen, wer die Kontrolle hat und diese auch zu ihren Gunsten ausnutzen.[100]

Der dritte Charakter ist der *dramatische Betrüger*.[101] Ähnlich wie der Narzisst liebt der Dramatiker die Aufmerksamkeit anderer. Er fällt durch seine ausdrucksstarken Emotionen und sein theatralisches Verhalten auf. Stimmungsschwankungen sind für diesen Personentyp charakteristisch. Um die Aufmerksamkeit auf sich zu lenken, erfinden sie Geschichten, übertreiben und prahlen von sich und ihren Taten.

Alle drei Persönlichkeitsstile basieren auf machiavellistischen Zügen, da die Täter grundlegend ihre Manipulationsfähigkeiten zu ihren Gunsten nutzen. Betrüger sind „emotional kalte[s], selbstgerechte[s] und egoistische[s] Individu[en].“[102]

4.2.3 Tatbegünstigende Faktoren und Eigenschaften

Nach Allwinn et al. gibt es drei Kernfaktoren, die einen Betrüger in seinem Tun bestärken. Der erste ist eine geringe *Integrität*. Sie beschreibt die „individuelle Einstellung eines Menschen in Bezug auf deviantes Verhalten, Normen und Werte.“[103] Je geringer die Integrität eines Menschen, umso eher begeht er deviante, also von der Norm abweichende Handlungen. Der zweite Faktor befasst sich mit den *Rationalisierungstechniken* eines Betrügers. Dabei handelt es sich um „kognitive Prozesse, die darauf abzielen, sich von der eigenen Verantwortung für eine Tat zu distanzieren“[104] bzw. diese zu entschuldigen. Dabei unterscheidet Allwinn fünf Techniken:

a) Leugnen der Verantwortung: Der Täter sieht sich nicht in der Schuld. Sein Handeln sei nicht kontrollierbar gewesen, als würde er von außen gesteuert. Teilweise stellt er sich dabei selbst als „Opfer widriger gesellschaftlicher Verhältnisse“[105] dar.

---

[97] J. Hoffmann: Psychologie von Betrügern. (2011) S.15.
[98] Vgl. ebd. S. 15f.
[99] Ebd.
[100] Vgl. ebd.
[101] Vgl. M. Allwinn, et al: Betrügerisches Verhalten aus kriminalpsychologischer Sicht. (2018) S. 39.
[102] Ebd. S. 40.
[103] Ebd. S. 36.
[104] Ebd.
[105] Ebd.

b) Leugnen der Fremdschädigung[106]: Der Täter verharmlost den entstandenen Schaden. Er gibt bspw. vor, sich das Geld nur ausgeliehen zu haben oder das fehlende Geld würde das Opfer nicht verarmen lassen.

c) Leugnung der Opferrolle[107]: Der Täter ist sich sicher, sein Opfer habe die Tat verdient. Er sieht sich dabei selbst als Rächer oder Held.

d) Verdammung der Verdammenden[108]: Der Täter erachtet das Verhalten und Handeln derer, die ihn „verurteilen“ als schwerwiegender als seine eigene Tat. Dadurch richtet er den Fokus von sich auf andere.

e) Berufung auf höhere Instanzen[109]: Der Täter verteidigt sein Handeln mit der Begründung, dass er im Namen von Dritten oder deren Anweisung gehandelt habe. Er selbst trage keine Schuld.

Der dritte Kernfaktor befasst sich mit der *Manipulationsfähigkeit* des Täters. Dabei wird ihnen die Fähigkeit zugeschrieben, sich gut mit Menschen auszukennen.[110] Indem sie ihre Opfer analysieren, finden sie deren Schwachstellen, welche sie später als Angriffspunkte nutzen. Sie entschlüsseln gesellschaftliche Codes und sind geübte Nachahmer, wodurch sie sich in bestimmte Rollen versetzen und diese adäquat abbilden können. Typische Prinzipien dabei sind:

a) die Reziprozität[111]: Der Täter erweist dem Opfer einen Gefallen und dieses will sich dafür revanchieren.

b) die soziale Bewährtheit[112]: Wenn viele Menschen etwas tun, dann muss es richtig sein.

Betrüger verspüren wenig bis keine soziale Angst.[113] Sie sind sich ihrer Tricks bewusst und vertrauen auf ihre Fähigkeiten. Das Lügen fällt ihnen nicht schwer. Diese Fähigkeiten gehen einher mit einem gewissen Grad an Intelligenz. Betrüger müssen sich merken können, welche Rollen sie spielen und bei wem sie sich wie verhalten haben.

4.2.4 Die Betrugsopfer

Nachforschungen zu den Betrugsopfern zeigen, dass besonders die Menschen für Betrugsmaschen anfällig sind, die nach dem schnellen Geld suchen.[114] Damit einher gehen typische Eigenschaften wie Naivität, Gier und ein geringes Maß an Selbstkontrolle. Im

[106] M. Allwinn, et al: Betrügerisches Verhalten aus kriminalpsychologischer Sicht. (2018) S. 36.
[107] Vgl. Ebd.
[108] Vgl. Ebd.
[109] Vgl. Ebd.
[110] Vgl. J. Hoffmann: Psychologie von Betrügern. (2011) S.14.
[111] Vgl. M. Allwinn, et al: Betrügerisches Verhalten aus kriminalpsychologischer Sicht. (2018) S.37.
[112] Vgl. ebd.
[113] Vgl. J. Hoffmann: Psychologie von Betrügern. (2011) S. 14.
[114] Vgl. M. T. Whitty: Mass-Marketing Fraud: A Growing Concern. In: IEEE Security & Privacy. Bd. 13 Nr. 4 (2015) S.85.

Durchschnitt handelt es sich bei den Opfern um ältere, ärmere, weniger gebildete und alleinstehende Personen.

Durch Selbstüberschätzung und falsche Hoffnungen bestärkt, liegt der Grund für den Erfolg der Betrugsmaschen in den Fehlentscheidungen der Opfer.[115] Die Betrüger schaffen mit ihren Angeboten bewusst Szenarien und Situationen, die Fehlentscheidungen der Opfer begünstigen und verstärken.

4.2.5 Taktiken der Betrüger

Die Betrüger bedienen sich dabei einer geringen Anzahl klassischer Taktiken. Die erste ist die *„Fuß-in-der-Tür"-Technik*[116]. Der Betrüger macht dem Opfer Angebote zu kleinen Preisen und steigert diese kontinuierlich. Da es sich hierbei um ein stetiges Wachstum handelt, fällt die Differenz von Beginn und Ende der Zahlungen erst im Vergleich auf.

Die zweite Taktik nennt sich *„Mit-der-Tür-ins-Haus-fallen"*[117]. Der Betrüger setzt den Preis des Angebots sehr hoch und senkt ihn anschließend kontinuierlich, bis das Opfer darauf eingeht.

Eine weitere Taktik zielt auf das *Angebot-Nachfrage-Prinzip*[118] ab. Der Betrüger setzt sein Opfer unter Druck, indem er ihm ein lukratives Angebot macht, welches jedoch nur zeitlich begrenzt verfügbar ist.

Die vierte Taktik besteht im *Aufbau einer Vertrauensbasis* zwischen Betrüger und Opfer[119]. Denn wenn das Opfer dem Täter vertraut, ist es vermutlich eher bereit, auf ihm empfohlene Angebote einzugehen.

4.2.6 Prävention von Betrugsstraftaten

Um Betrug verhindern zu können, müssen grundsätzlich die Drahtzieher gefasst werden. Diese befinden sich zumeist jedoch im Ausland und sind so für die inländischen Strafverfolgungsbehörden kaum bis gar nicht greifbar.[120] Ihre Spuren zu verfolgen und sie zur Rechenschaft zu ziehen erfordert viel Zeit. Die Strafverfolgung muss digitale Daten auswerten, um Indizien und Beweise zu finden und die Taktik der Täter zu verstehen.

Banken wurde die Möglichkeit eingeräumt, verdächtige Transaktionen und Geldströme betrügerischen Ursprungs zu melden. Ob das die Täter in ihrem Tun ausbremst, ist jedoch fraglich. Sie sind stets sehr adaptiv und die Wahrscheinlichkeit, dass sie neue Schlupflöcher finden, ist entsprechend groß.

---

[115] Vgl. M. T. Whitty: Mass-Marketing Fraud: A Growing Concern. In: IEEE Security & Privacy. Bd. 13 Nr. 4 (2015) S.85.
[116] Ebd.
[117] Ebd.
[118] Vgl. ebd.
[119] Vgl. ebd. S.86.
[120] Vgl. ebd.

Anstatt die Leichtgläubigkeit der Betrogenen zu verurteilen, sollten Systementwickler die Schwachstellen ihrer Systeme ausfindig machen und Sicherheitsmechanismen optimieren oder nachrüsten.[121]

Um Betrüger länderübergreifend verfolgen zu können, muss die internationale Zusammenarbeit gestärkt werden.

Von technischer Seite her könnten Programme und Software entwickelt werden, welche die Strafverfolgungsbehörden bei der Aufklärung von gefälschten Profilen und betrügerischen Handlungen unterstützt.[122] Gleichermaßen müssen die Bürger auf verlässliche Kontaktmöglichkeiten bei ihrer Hausbank oder Behörden aufmerksam gemacht werden, um den Kontakt zu Betrügern zu unterbinden.

Im Unternehmensbereich ist es ratsam, neue Mitarbeiter zunächst mit Skepsis zu beobachten. Betrüger sind klug und finden Mittel und Wege, um sich rar zu machen. Dabei verkaufen sie sich auch gern besser, als sie eigentlich sind. Wenn das Bauchgefühl nicht stimmt, besser einmal mehr zu der Person recherchieren, die vorgegebenen Fakten überprüfen und eine weitere Meinung einholen. „Betrüger sind – bildlich gesprochen – oft besser mit Abstand zu erkennen als aus der Nähe.“[123]

„Die Betrugsbekämpfung kann letztlich nur erfolgreich sein, wenn sowohl in der Technik als auch in die Menschen und ihre Aus- und Weiterbildung investiert wird.“[124]

4.3 Bankkauffrau (BKF)[125]

Das Gespräch mit einer Bankkauffrau fand am 02.08.2022 statt und erfolgte telefonisch. Die Fragen zielten vorrangig auf den Umgang mit Betrugsmeldungen, den daraus resultierenden (Präventions-)Maßnahmen und Erfolgschancen ab.

Die BKF befasst sich seit 2014 mit der Geldwäsche, hat jedoch zum Straftatphänomen Cybertrading keine direkten Bezugspunkte, geschweige Kenntnis von Fällen in der Bank. Hingegen häufiger tritt es auf, dass Kunden der Bank ihr eigenes Geld und/oder das von Freunden oder Verwandten einsammeln, um es an einer Kryptobörse zu investieren. Dass sie sich dabei nach § 261 StGB strafbar machen, ist ihnen nicht bewusst. Um einen Betrug handelt es sich nach § 263 StGB in diesem Fall jedoch nicht, da der subjektive Tatbestand nicht gegeben ist.[126]

---

[121] Vgl. M. T. Whitty: Mass-Marketing Fraud: A Growing Concern. In: IEEE Security & Privacy. Bd. 13 Nr. 4 (2015) S. 87.
[122] Vgl. ebd.
[123] J. Hoffmann: Psychologie von Betrügern. (2011) S.17.
[124] Vgl. M. Allwinn, et al: Betrügerisches Verhalten aus kriminalpsychologischer Sicht. (2018) S.44.
[125] Vgl. Anhang 6.2: Transkript – Interview – BKF.
[126] Vgl. S. Einbock, et al: Betrug - § 263 StGB - Vortäuschung falscher Tatsachen - Schema. (2022) Abgerufen am 04. 08. 2022 von https://www.juraforum.de/lexikon/betrug#:~:text=Der%20objektive%20Tatbestand%20des%20Betruges,eine%20T%C3%A4uschung%20%C3%BCber%20Tatsachen%20vorliegen.

Das Geschäftsmodell der Bank der Gesprächspartnerin befasst sich vorrangig mit den Kunden aus der Region. Bundeslandübergreifende Beziehungen zu Kunden gibt es selten und gehören eher weniger zum Standard der Bank. Dabei verweist die BKF auf die Ungeeignetheit dieses Modells für die Betrüger, da diese auch länderübergreifend Kunden akquirieren und betreuen.

Die Bank besitzt ein Geldwäschefrüherkennungssystem, welches anhand von Filterkriterien auffällige Konten findet und Bankmitarbeiter darüber informiert. Der Algorithmus des Systems durchläuft täglich den Kundenstamm der Bank. Die finale Entscheidung, ob ein Konto, welches vom Algorithmus als verdächtig eingestuft wurde, wirklich verdächtig ist oder nicht, trifft jedoch ein Mitarbeiter. Schätzt der Mitarbeiter das Konto ebenfalls als verdächtig ein, so erstattet er eine Verdachtsmeldung und ggf. Strafanzeige.

Abseits von den Geldwäscheverdachtsmeldungen, befassen sich die Mitarbeiter ebenfalls mit Anfragen aus den einzelnen Filialen bezüglich der Legitimation von Kunden oder Auffälligkeiten u.a. im Zusammenhang mit der Kontoführung. Nebenher werden Fragen der Kunden aus dem Tagesgeschäft beantwortet und systematisch gesteuerte Aktivitäten wie sanktionierte Transaktionen beobachtet.

Auf die Frage hin, ob die Bankkunden aktiv vor Betrugsmaschen gewarnt werden, verneint die BKF. Entweder muss ein Kunde auf seinen Kundenberater zugehen und seinen Sachverhalt schildern bzw. Anzeige erstatten oder der Bankmitarbeiter spricht den Kunden an, sobald er Auffälligkeiten in der Kontoführung feststellt. Zu solchen Auffälligkeiten zählen nach Aussage der BKF Bargeldabhebungen oder Transaktionen in großen Mengen, sowohl einzeln als auch regelmäßig, sofern diese nicht plausibel erklärbar sind. Ansonsten finden die Kunden sämtliche Informationen zu Betrugsfällen und Neuigkeiten auf der Homepage der Bank, auf welche sie auch durch den Kundenberater verwiesen werden.

Wenn ein Kunde einen Betrug bei seiner Bank anzeigt, ist es die Aufgabe des Mitarbeiters, zu überprüfen, ob die Anzeige legitim ist und eine Validierung von offizieller Stelle, also der Polizei vorliegt. Es kann auch vorkommen, dass der Kunde sich zuerst an seine Bank wendet, um Anzeige zu erstatten, diese den Sachverhalt aufnehmen und im Anschluss an die Polizei verweisen. Ist eine Betrugsmeldung valide, veranlasst die Abteilung Zahlungsverkehr die weiteren nötigen Schritte, darunter Kontosperren, Telefonate und ggf. Kontaktaufnahmen zu anderen beteiligten Kreditinstituten.

Die BKF bestätigt, dass es regelmäßig neue Betrugsmeldungen gibt. Dabei geht sie auch auf das technische und psychologische Geschick der Betrüger ein. Sie geben sich bspw. als seriöse Bankmitarbeiter aus und verwickeln Kunden in Gespräche, um an deren Daten zu gelangen. Auch CEO-Fraud-Versuche gab es in der Vergangenheit, wobei Täter über den internen Bankweg Geldzahlungen zu veranlassen versuchten.

Um die Mitarbeiter entsprechend zu informieren, werden intern regelmäßig Infomails verschickt. Die BKF hebt jedoch hervor, dass ein Phänomen erst bekannt sein muss und genügend Fälle mit einer gewissen Gesamtschadenssumme bekannt sein müssen, um zum Handeln anzuregen. Einzelfälle mit geringem Schaden gehen dabei unter.

Unabhängig von der Masche, mit der ein Kunde betrogen wurde, stehen die Chancen, überwiesene Gelder zurück zu erhalten, nach Einschätzung der BKF insgesamt sehr schlecht. Werden die Gelder innerhalb Deutschlands transferiert, kann ggf. mit dem entsprechenden Kreditinstitut Kontakt aufgenommen und rechtliche Schritte eingeleitet werden. Befindet sich das Geld jedoch im (EU-)Ausland, so wird es meist innerhalb kürzester Zeit ausgezahlt und ist somit nicht verfolgbar.

Ein anderes Problem befasst sich mit dem Szenario einer Sicherstellung. Angenommen im Laufe der Ermittlungen wird ein Bruchteil einer Schadenssumme sichergestellt, jedoch gibt es mehrere Geschädigte. Wem der Geschädigten wie viel Geld zusteht, darf die Bank nicht entscheiden. Stattdessen hinterlegt sie den Betrag beim Amtsgericht und überlässt die weitere Entscheidung der Justiz.

Im Bereich Handeln mit und Kaufen von Kryptowährungen kennt sich die BKF nicht genug aus, um explizite Aussagen treffen zu können. Sie sieht darin jedoch eine Gefahr für Anleger, die sich nicht ausreichend über die Konditionen, Chancen und Risiken informieren. Sie vergleicht es mit dem Wertpapierhandel, welcher jedoch im Gegensatz zu dem Markt der Kryptowährungen reguliert ist und nur durch geschulte Bankmitarbeiter beworben und aufgeklärt wird.

Die Anleger sollten sich nicht von den überwältigenden Renditeversprechen blenden lassen und stattdessen erst zu der Plattform recherchieren. Die BKF empfiehlt ungeübten Anlegern ausschließlich Investitionen bei bekannten und regulierten Anbietern, deren Firmensitz in Deutschland oder innerhalb der EU ist und deren Kundenrezensionen plausibel sind. Eine Nachfrage zu der Plattform bei der Hausbank kann dabei ebenfalls nützlich sein.

Bei der Bekämpfung der Betrugsdelikte sieht die BKF keine weiteren Möglichkeiten. Der Schutz der Kunden ist eines der obersten Gebote der Bank und interne Mechanismen oder Informationen werden bereits regelmäßig optimiert und aktualisiert. Trotzdem nehmen die Banken stets eine reaktive Rolle bei der Strafverfolgung von Betrugstätern ein.

4.4 Ermittler (E)[127]

Das Gespräch mit einem Ermittler fand am 11.07.2022 statt und erfolgte persönlich. Die Fragen zielten vorrangig auf die Aufgaben eines Polizeibeamten im Bereich Cybertrading ab und den Erfolg der Maßnahmen.

Der E befasst sich seit Ende 2019 mit dem Straftatphänomen Cybertrading und hatte zuvor selbst noch nie davon gehört. Erst durch die Vielzahl an Fällen im darauffolgenden Jahr kam die Erkenntnis, dass es sich nicht um Einzelfälle handelt. Dass dieses Phänomen nicht nur aus Daten abfangen und Bitcoins handeln besteht, sondern mehr dahinter steckt.

[127] Vgl. Anhang 6.3: Transkript – Interview – E.

Im Laufe der Zeit, in der der E die GES zu sich geladen hat, durfte er bereits eine Vielzahl an unterschiedlichen Menschentypen kennenlernen. Die einen sind peinlich berührt, da sie sich den Tätern emotional geöffnet haben und dieses Vertrauen missbraucht wurde. Die anderen sind wütend, dass solche Maschen erfolgreich sind. Häufig erstatten die GES Anzeige, ohne wirklich zu verstehen, was da eigentlich mit ihnen und ihrem Geld passiert ist. Die Aufgabe des E besteht dann darin, über den Vorfall aufzuklären und vor weiteren Straftaten zu warnen.

Eine Auffälligkeit der vergangenen Jahre besteht darin, dass die Daten der GES in großem Stil gesammelt werden. Jedes Telefonat, jeder Schriftverkehr, alles wird von den Betrügern verwertet, um so viele Informationen über die Kunden wie möglich zu sammeln. Jeder Broker, der mit dem GES in Kontakt steht, erhält Einblick in diese Datensammlung. So kann er sich auf die Person einstellen, ihre Schwachstellen ausnutzen und optimal manipulieren.

Die Position der Täter schätzt der E dabei als sehr geeignet ein. Die GES stoßen bei Recherchen zu Geldanlagemöglichkeiten oder durch Werbeanzeigen auf die Betrügerplattform. Indem sie ihre Kontaktdaten hinterlegen, bekunden sie aktiv ihr Interesse und erwarten eine Rückmeldung der Täter. Für diese ist wiederrum klar, da hat jemand Geld, was er anlegen möchte. Sie melden sich bei den GES und verkaufen ihnen ein Modell, mit welchem sie in kurzer Zeit sehr viel Geld machen können. Gleichermaßen bekunden sie aber auch den Erfolg von Investitionen im höherstelligen Bereich und setzen die GES einem psychischen Druck aus.

Die Täter spielen den GES in jedweder Hinsicht Interesse vor, am Ende wollen sie jedoch nur das Geld. Geschichten über die Familie oder den Erfolg dienen nur als Druckmittel, um zu höheren Investitionen zu drängen. Sobald die GES die Gelder überweisen, fließt es praktisch direkt in die Taschen der Betrüger. In der Finanzsoftware werden den GES jedoch aufsteigende Kurse gezeigt, die zu weiteren Einzahlungen anregen.

Der E unterstreicht, dass kein GES sein Geld ausgezahlt bekommt. Die Täter reden sich heraus, berufen sich auf Klauseln im Vertrag, die zur Zahlung von Zinsen oder Steuern auffordern. Dabei handelt es sich wieder um Lockmittel. Von dem Geld sieht der GES nichts wieder.

Bei den Ermittlungen selbst setzt der E auf eine eigene Matrix. Zu Beginn steht das intensive Aktenstudium, um einen Überblick zum Sachverhalt zu bekommen. Der E benötigt alle zur Verfügung stehenden Informationen, die der Aufklärung des Sachverhaltes dienen. In den meisten Fällen ist eine Ladung des GES dabei unabdingbar. Gegebenenfalls gibt es in den polizeilichen Auskunftssystemen bereits Erkenntnisse zu der Plattform, bei der der GES investiert hat. Die Tatsache, ob eine Plattform noch online ist oder bereits offline, entscheidet darüber, ob eine Serverbeschlagnahme beantragt wird oder nicht. Bei der Verfolgung der Kommunikationswege betrachtet der E die E-Mail-Header, um an die IP-Adresse des Absenders zu gelangen. Bei Fernzugriffen mittels Remotesoftware wird der Rechner des GES nach vorhandenen Logdateien gesucht. Ebenso verfolgt der E die Transaktionen ins In- oder Ausland auf die Täterkonten. Diese können über die BaFin oder die FIU beauskunftet werden, um Informationen zum Inhaber zu erhalten.

Ähnlich funktioniert das mit Investitionen in Kryptowährungen. Der E verfolgt die Kryptoströme bei den Exchangern von einem Konto auf das nächste. Seine Auswertungen dazu kann er sowohl händisch machen oder auch das LKA um Hilfe bitten.

Auf Nachfrage hin, ob es einen Unterschied bei den Ermittlungen zwischen dem Versuch der Betrugsstraftat oder der abgeschlossenen Tat gibt, verneint er. Die Entscheidung, was schlussendlich für strafrechtliche Maßnahmen ergriffen werden, trifft in jedem Fall die Staatsanwaltschaft.

Laut Einschätzung des E dauern die Ermittlungen mehrere Jahre. Die Chancen dabei eine reelle Person zur Rechenschaft ziehen zu können, stehen dabei sehr schlecht. Das liegt zum einen daran, dass die Täter im Ausland und damit außerhalb des Herrschaftsgebietes der deutschen Justiz sitzen. Andererseits handelt es sich bei den Pseudonymen der Täter um einen logischen Trugschluss. Die Ermittlungen werden gegen einen Täter geführt, der sich irgendeinen Namen hat ausdenken können. Der E geht davon aus, dass innerhalb einer Gruppierung immer die gleichen Pseudonyme verwendet werden. Doch nur den Namen des Täters zu kennen, bedeutet nicht, den Fall gelöst zu haben. Das betonte der E mehrfach. Die große Schwierigkeit besteht schlussendlich darin, die Täter zu lokalisieren und ihnen gerichtsfest nachweisen zu können, dass sie die Betrugsstraftaten begangen haben.

Bereits die Sammlung von Informationen stellt den Sachbearbeiter vor große Herausforderungen. Ermittlungsersuchen im Inland lassen sich laut seiner Aussage schneller und einfacher umsetzen, als im Ausland. Abhängig von den Rechtshilfeabkommen, die zwischen Deutschland und anderen Ländern geschlossen werden, benötigt auch die Unterstützung in der Strafverfolgung unterschiedlich viele Ressourcen. Neben bürokratischem Aufwand gehört ein großer diplomatischer Aufwand zu den Ermittlungen. Über die inländischen Instanzen der Staatsanwaltschaft, Gerichte und Botschafter werden die Ersuchen zum ausländischen Ermittler geleitet. Dessen Antwort benötigt denselben Weg zurück zum E.

Dies zu vereinfachen, würde die Sachbearbeiter der deutschen Polizei ungemein unterstützen. Ein direkter Austausch der Polizeidienststellen über die Landesgrenzen hinweg würde nicht nur Aufwand, sondern auch viel Zeit sparen.

4.5 IT-Experte (ITE)[128]

Das Gespräch mit einem IT-Experten fand am 27.07.2022 statt und erfolgte persönlich. Die Fragen zielten vorrangig auf die Ermittlungen eines Auswerters im Bereich Cybertrading ab und den Erfolg der Maßnahmen.

Der ITE erhält seinen Arbeitsauftrag von den Sachbearbeitern der jeweiligen Fachkommissariate. Ein GES erstattet Anzeige, diese gelangt zur Polizei und dort zum entsprechenden Sachbearbeiter. Dieser erhält die Daten vom GES selbst oder fordert sie auf

[128] Vgl. Anhang 6.4: Transkript – Interview – ITE.

anderem Wege an, um sie anschließend an den ITE zu übergeben. Grundlegend ist es dessen Aufgabe, Datensätze zu untersuchen und im Falle des Cybertrading Server oder andere Datenspeicher auszuwerten.

Seit 2019, also seit Bekanntwerden des Straftatphänomens Cybertrading beschäftigt sich der ITE mit den dazugehörigen digital-forensischen Auswertungen. Er ist sich jedoch sicher, dass das Phänomen älter ist, als offiziell bekannt. Als Grund für den zeitlichen Verzug, hebt der ITE die Stadt-Land-Diskrepanz hervor. In den Städten vergeht weniger Zeit für die Einordnung der Anzeigen als auf dem Land.

Das Ziel der Auswertungen wird im Arbeitsauftrag des ITE festgehalten. Welche und wie viele Daten er dazu erhält, hängt wiederum vom Serverdienstleister ab. Der litauische Provider Hostinger[129] stellt für die Auswertungen ausschließlich die Webseite als logische Datenkopie und die genutzten Datenbanken i.F.v. Datenbankdumps zur Verfügung. Bei dem ebenfalls in Litauen ansässigen Provider Cherry Servers[130] erhält der ITE stattdessen das vollständige dd-Image[131] des Servers. Somit steht ihm der gesamte Server inklusive der wichtigen *config*-Dateien zur Verfügung. Mithilfe derer kann er zusätzlich zur Rekonstruktion der Webseite Informationen zu den Nutzern, Logfiles, Zugriffsdaten und Webseitenaufrufe einsehen. Diese Daten können Aufschluss über das Handeln der Täter, deren Zugehörigkeit zu einer Gruppe und ggf. einen Aufenthaltsort geben.

Sofern im Datenpaket des Providers enthalten, kann der ITE ebenfalls den Verlauf der Kommandozeileneingaben der Täter nachvollziehen. In einigen Fällen sei es so möglich gewesen, Hinweise auf externe Zugriffe weiterer Server zu erlangen und so die Ermittlungen ausweiten zu können.

Die mitgelieferten Webseiten selbst haben laut ITE keine besonders große Bedeutung. Prinzipiell werden die Landing-Pages als „Wegwerfware“ produziert, deren Schutz aus Sicht der Täter aufgrund ihrer geringen Beweiskraft unwichtig ist. Sie fungieren allein zur Vermarktung der Brand und sind in großer Stückzahl auf Standardservern angelegt. Die technisch relevanten Daten des BackOffice oder die Zieladressen der URLs befinden sich dort jedoch nicht. Sie liegen meist extern und können ohne Hinweise in den Datenbanken nicht ausfindig gemacht werden. Die URLs dieser BackOffices werden von den Tätern mithilfe der Nameserver angepasst und zusätzlich durch Anonymisierungsdienste wie Cloudflare verschleiert, um den Zugriff durch Strafverfolgungsbehörden zu verhindern.

Das Vorgehen des ITE zur Auswertung erscheint simpel. Er rekonstruiert die Webseite in einer virtuellen Maschine, um sie genauer untersuchen zu können. Dabei betrachtet er nicht nur die Aufmachung der Seite selbst, sondern bezieht auch die hinterlegten Datenbanken in die Auswertung mit ein.

---

[129] Vgl. Hostinger: Eins. Zwei. Online. (2022) Abgerufen am 31. 07. 2022 von https://www.hostinger.de/uber-uns.
[130] Vgl. Cherry Servers: Let's Democratize Cloud Together. (2022) Abgerufen am 31. 07. 2022 von https://www.cherryservers.com/company#about.
[131] Bei einem dd-Image handelt es sich um ein forensisches Abbild eines Datenspeichers.

Selbst bei unklaren Gegebenheiten und Neuheiten müssen die Auswerter akribisch nach Hinweisen auf genutzte Programme und Dateien suchen. Wenn ein Täter etwas verstecken will, dann wird er auch Wege dazu finden. Ein bekanntes Beispiel nennt der ITE aus dem Bereich der Kinderpornografie, wo einzelne Clips in größeren Filmen versteckt werden können. Im Bereich Cybertrading ist dies jedoch bisher nicht der Fall, da die ausschlaggebenden Daten extern geschützt und die kurzlebigen Landing-Pages für die Verfolgung zumeist ungeeignet sind.

In der Vergangenheit durfte sich der ITE bereits mit einer unbekannten App befassen. Dazu speiste er diese in eine virtuelle Maschine ein und startete sie. Das daraus entstandene Logfile bot ihm Infos über das Programm und dessen Nutzer. Wie die App ursprünglich aussah, war daraus jedoch nicht ersichtlich. Der Name der App war der einzige Hinweis auf dessen Funktion als Bezahlsoftware. In solchen Fällen kann der ITE nur mit den in den Datenbanken hinterlegten Informationen arbeiten und diese sinngebend interpretieren. Sie gaben Aufschluss über sämtliche Nutzer der App, deren E-Mail-Adressen und Registrierungsdaten.

Das Thema Verschlüsselung ist im Bereich Cybertrading bisher ebenfalls nicht allzu präsent. Der ITE gibt an, dass es durchaus möglich ist, dass Nutzer ihre Daten auf den Servern verschlüsseln könnten. Diese seien bei den Auswertungen ohne Passwort nicht einsehbar. Gleichermaßen betont er, dass die Hostprovider eine Hintertür zu den Servern besitzen, da sie diese auch im vermieteten Zustand pflegen müssen. Inwiefern sie also die Verschlüsselung der Nutzer umgehen oder diese gar zurücksetzen können, ist nicht klar.

Grundsätzlich gilt, wenn der Verschlüsselungsmechanismus und die Länge des Passwortes unklar sind, erweist es sich für den ITE als äußerst schwierig, das Passwort herauszufinden. Gleichermaßen ist es auch für den Täter wesentlich aufwändiger.

Wenn dem ITE tatsächlich verschlüsselte Datenträger vorlagen, dann nur, weil Geräte wie MacBooks mithilfe von FileVault dies von sich aus machten oder weil terroristische Vereinigungen ihre Daten schützen wollten. So wurden in der Vergangenheit vollverschlüsselte Laptops sichergestellt, welche nur mithilfe eines bestimmten Sticks, der die *keyfiles* enthielt, entschlüsselt werden konnten.

Der ITE stellt klar, dass es viele Ansätze zur Umgehung von Verschlüsselung gibt und diese sich in jedem Sachverhalt unterscheiden können. Für die Auswertung beschlagnahmter Geräte nennt er drei gängige Möglichkeiten. Sofern möglich wird der Datenspeicher des Gerätes ausgebaut. Ansonsten muss über die Eingabe des Nutzerpasswortes oder durch Fremdstarten Zugriff auf den Speicher gewährt werden. Sind die Daten nach der Extraktion dennoch verschlüsselt, sind sie nicht verwertbar.

Auf Nachfrage, ob es eine Art Muster bei den Auswertungen gab, verweist der ITE auf eine Reihe aktueller Fälle. Ihm ist aufgefallen, dass bei verschiedenen Brands auf verschiedenen Servern beinahe identische Passwörter genutzt wurden. Diese unterscheiden sich ausschließlich im ersten Zeichen, welches entsprechend dem ersten Buchstaben im Brandnamen gewählt wurde. Daraus lässt sich ein modus operandi ableiten, der auf eine Tätergruppierung oder einen CaaS hinweisen könnte.

Wie lange eine digitale Auswertung dauert ist laut ITE von Sachverhalt zu Sachverhalt verschieden. Er gibt ein Minimum von einem Tag und eine Zeitspanne von drei bis sechs Monaten im Durchschnitt an. Ausschlaggebend für die Dauer der Auswertungen sei der Umfang an zur Verfügung gestellten Daten und der Art der Auswertung.

Der ITE bevorzugt die Variante, bei der er die Webseite virtualisiert und sich als Admin beim weit verbreiteten Content-Management-System WordPress[132] einloggt. So kann er die Strukturen intern betrachten. Die Alternative bestünde in der händischen Auswertung, indem SQL-Abfragen entsprechend der vorliegenden Plug-Ins gestartet werden, welche der ITE jedoch wegen des großen Aufwandes eher ablehnt.

In einem besonders komplexen Fall lag dem ITE der Endserver einer Server-Kette von 17 Servern vor. Bei der Grobauswertung konnte er die Enddatenbanken und Excel Tabellen der zehn einzelnen Nutzer einsehen. Der Superuser hatte bereits das weitere Vorgehen geplant und vermerkt, welche Server unter welchem Brandnamen angemietet werden sollten. In diesem Sachverhalt betonte der ITE, wie sehr sich der Komplexitätsgrad der Auswertungen verändern kann. Dieser Sachverhalt wurde mittlerweile an das LKA übergeben und wird immer noch bearbeitet.

Um die Wichtigkeit des schnellen Handelns zu unterstreichen, berichtet der ITE von einem seltenen Fall. Innerhalb eines Tages zeigte eine GES einen Kreditkartenbetrug an. Da sie sich direkt an das Fachkommissariat wendete und diese sämtliche Handlungen des Täters innerhalb Deutschlands lokalisieren konnten, wurde der Täter zeitnah gefasst und verurteilt.

Heute sind solche schnellen Ermittlungen selten. Als größte Herausforderungen bezeichnet der ITE den zeitlichen Verzug bis zum Erhalt der ersten Daten. Bis GES merken, dass sie geschädigt sind, vergehen Wochen. Bis die Anzeige im entsprechenden Fachkommissariat eingeht, kann es ebenfalls dauern. In dieser Zeit erwirtschaften die Täter weiterhin Geld und planen bereits ihr weiteres Vorgehen. Sobald eine Brand auffliegt, wird sie vernachlässigt und die Täter fokussieren sich auf die neuen Brands. Um überhaupt an die technischen Daten zu gelangen, müssen Beschlüsse beantragt werden, welche ebenfalls Zeit in Anspruch nehmen.

Im Hinblick auf die Serverbetreiber sieht der ITE gleich zwei Herausforderungen. Einerseits müssen die Betreiber aufgrund des Datenschutzgesetzes in Deutschland sämtliche Daten eines Kunden nach Beendigung des Vertragsverhältnisses löschen. Andererseits beenden sie ein Vertragsverhältnis von sich aus, wenn sie bspw. durch Zahlungsdienstleister wie PayPal auf den Missbrauch von Konten aufmerksam gemacht werden und löschen daraufhin ebenfalls alle Daten des Kunden. Somit sind sämtliche fallrelevante Daten für die Auswertungen unwiederbringlich verloren.

Bezugnehmend auf die digital-forensischen Untersuchungen sieht der ITE die sich stetig entwickelnde Technik als große Schwierigkeit. Kein Bereich entwickelt sich so stark wie

[132] Bei WordPress handelt es sich um ein Content-Management-System, welches zum Erstellen von Webseiten genutzt wird. Die meisten Webseiten basieren darauf.

Cybercrime. Heutzutage müssen digitale Ermittler entweder Allrounder sein und sich stetig an neue Gegebenheiten und Veränderungen der digitalen Möglichkeiten anpassen oder sie sind Experte auf einem kleinen Fachgebiet, wozu sie sich kontinuierlich weiterbilden müssen. Eine perfekte Fusion kann es laut Einschätzung des ITE nicht geben.

Der ITE bezweifelt, dass das Phänomen an Aktualität verlieren wird. Dort, wo die Polizei eine Tätergruppe zerschlägt, wird stets eine neue nachrücken. Cybertrading ist für die Täter eine ideale Möglichkeit schnell viel Geld zu verdienen. Um zukünftigen Straftaten entgegen zu wirken, müsste die Gesellschaft mehr auf Cybercrime aufmerksam gemacht werden. Denn solange es jemanden gibt, der naiv genug ist und auf die Maschen der Betrüger eingeht, solange wird dieses Phänomen nach Einschätzung des ITE bestehen bleiben.

Handlungsbedarf sieht er vor allem bei den Behörden und deren Gesetzgebung. Obwohl es Rechtshilfeersuchen gibt, die die Länder zu gegenseitiger Unterstützung bei der Aufklärung von Straftaten auffordern, ist das System nach Einschätzung des ITE zu langsam. Er betont die Notwendigkeit von internationalen Gesetzen und/oder Verträgen, die die Länder zu schnellerer Zusammenarbeit anregen.

Auch die Optimierung der Regelungen innerhalb Deutschlands erachtet der ITE als unumgänglich. Er sieht das Potenzial in der Koordinierung bzw. Angleichung der Polizeigesetze. Der Bund könnte, basierend auf einer Fusion aller aktuellen Landespolizeigesetze, ein Regelwerk entwickeln, welches einen einheitlichen Standard zur Vereinfachung der Prozesse für alle 16 Bundesländer festlegt. So könnten bereits innerstaatliche Hürden überwunden werden.

Im kleineren Umfang sind Präventionsmaßnahmen bereits umgesetzt worden. Dass Unternehmen ihre Mitarbeiter aktiv schulen und den Kenntnisstand regelmäßig überprüfen, findet der ITE sehr gut. Seiner Meinung nach müssten viel mehr Unternehmen ihre Mitarbeiter im Bereich der digitalen Möglichkeiten und Gefahren weiterbilden. Die Kosten zur Aufklärung sind im Vergleich zu einem potenziellen Schaden vermutlich weitaus geringer.

Für die breite Gesellschaft empfiehlt der ITE mehr Präsenz der Polizei. Um die Menschen für aktuelle Fälle und neue Maschen sensibilisieren zu können, muss sowohl digital als auch analog Präventionsarbeit geleistet werden. Durch Einbeziehen der lokalen Printmedien könnten sie die Bürger in regelmäßiger Aktualität über die Geschehnisse in den Stadt- und Landkreisen informieren. Infotafeln, Aushänge an zentralen Stellen und Annoncen in der lokalen Zeitschrift könnten die Aufmerksamkeit der Bürger auf aktuelle Geschehnisse lenken und Falschinformationen entgegenwirken.

Ergänzend dazu bieten sich auch Werbung im Radio oder Infosendungen im Fernsehen an. Außerdem müsste es eine bundesweit verfügbare Internetseite geben, auf der sich jeder Bürger unabhängig von seinem Aufenthaltsort über die Geschehnisse in Deutschland informieren kann.

4.6 Juristin (JU)[133]

Das Gespräch mit einer Juristin fand am 12.07.2022 statt und erfolgte persönlich. Die Fragen zielten vorrangig auf die Aufgaben eines Anwalts im Bereich Cybertrading ab und die Durchsetzungsmöglichkeiten der Maßnahmen.

Die JU befasst sich seit 2019 mit dem Straftatphänomen Cybertrading/Fraud. Den Anlass lieferte ein Kollege des LKA. Er machte die JU darauf aufmerksam, dass in Sachsen viele Fälle im Bereich der Wirtschaftsstraftaten zu gleichen Plattformen angezeigt wurden. Daraufhin fiel die Entscheidung, dass diese und künftige Verfahren koordiniert und von den Cybercrime-Kommissariaten der Polizeidienststellen bearbeitet werden.

Die grundlegende Aufgabe der Staatsanwaltschaft besteht darin, die Ermittlungen zu einer Strafsache zu führen. Dabei arbeitet sie eng mit der Polizei zusammen. Die GES können sowohl persönlich oder vertreten durch einen Anwalt bei der Polizei oder Staatsanwaltschaft Anzeige erstatten. Bei Letzterem folgt ein entsprechender Ermittlungsauftrag an die Polizei. Diese ist für die weiteren Ermittlungen zuständig. Für die Beantragung weiterer Ermittlungsschritte oder beim Abschluss eines Verfahrens unterstützen Staatsanwaltschaft oder Gericht die Polizei.

Auf Nachfrage, ob es eine Priorität in der Verfolgung von Tätern, Geldströmen oder Verbindungen gibt, verneint die JU. Alle Aspekte werden gleichrangig betrachtet und verfolgt. Ausgehend davon, welche Anhaltspunkte es während der Ermittlungen gibt, richten sich anschließende Maßnahmen danach aus.

Wie groß die Tatbeteiligung einer Person beim Cybertrading ist, muss laut Aussage der JU immer im Einzelfall betrachtet werden. Wie viel weiß ein Beteiligter über die Tat, welche Rolle spielte er bei der Umsetzung oder ist er unschuldig? Als besonders schwierig stellt sich dabei das Dual Use Problem heraus, wobei bspw. eine Software aufgrund ihrer freien Verfügbarkeit auf dem Markt legal und illegal genutzt werden kann. Die juristischen Fragen zu Teilnahme, Mittäterschaft und Beihilfe einer Person müssen wiederum gerichtsfest belegt werden. Die JU hebt jedoch hervor, dass das aktuelle Problem bei der Bearbeitung der Cybertrading-Fälle in der Aufklärung der betrügerischen Strukturen und anschließenden Lokalisierung der Tatverdächtigen besteht.

Die juristisch anregbaren Ermittlungsmöglichkeiten schätzt die JU als geringfügig ein. Dies ist der Tatsache geschuldet, dass die Täter zumeist im Ausland sitzen und der Handlungsspielraum im Inland entsprechend eingeschränkt ist. Abgesehen von der Kontaktaufnahme mit den GES, der Auswertung technischer Geräte und den Ermittlungen zu IP-Adressen müssen länderübergreifende Maßnahmen via Rechtshilfeübereinkommen durchgeführt werden. Dies erfordert wiederum die Zusammenarbeit mit ausländischen Behörden.

Stoßen die Ermittler bei der Verfolgung der Zahlungswege auf Konten, deren Gelder den betrügerischen Aktivitäten eindeutig zugeordnet werden können, dann liegt es im Ermes-

[133] Vgl. Anhang 6.5: Transkript – Interview – JU

sen der Staatsanwaltschaft, diese Gelder mittels eines Arrestbeschlusses einzuziehen. Bei Kryptowährungen ist dies laut Aussage der JU nicht ganz so einfach. Da es sich bei ihnen nicht um Geldforderungen gegenüber einer Bank handelt sondern digitale Gegenstände, müssen sie beschlagnahmt werden.

Als größte Schwierigkeit bei den Ermittlungen sieht die JU den zeitlichen und finanziellen Aufwand. Bis die GES Strafanzeige erstatten, vergeht viel Zeit. Bereits ein Vierteljahr Abstand zwischen Täter und Strafverfolgung können zu viel sein. Das Transferieren der Gelder ins Ausland erweitert den Abstand zusätzlich auf globaler Ebene.

Hinzu kommt, dass nicht alle Institutionen mit den Behörden zusammenarbeiten. Bei manchen muss sogar befürchtet werden, dass sie die Ermittlungen gefährden könnten. Punkt zwei betrifft die Komplikationen über die Landesgrenzen hinweg. Rechtshilfeersuchen müssen in der Landessprache verfasst sein, in welches sie gesendet werden. Die Übersetzungen kosten den Staat Geld und bis eine Antwort eingeht, können Monate vergehen. In der Zwischenzeit können die Gelder weiterfließen und der Abstand zu den Tätern vergrößert sich weiter.

Um dem entgegenzuwirken, braucht es aus Sicht der JU mehr Polizeibeamte im Bereich Cybercrime. Die Ermittlungen zu Cybertrading-Verfahren stuft sie als sehr aufwändig und umfangreich ein, da dieses Phänomen aufgrund mangelnder Bekanntheit des Täters nicht mit Delikten im Straßenverkehr oder Diebstahl vergleichbar ist.

Auch der bürokratisch-diplomatische Aufwand stellt eine Hürde für den zügigen Verlauf der Ermittlungen dar. Aufgrund der Globalisierung und Digitalisierung sämtlicher Unternehmen, darunter auch Banken, würden vereinfachte Rechtswege die Ermittlungen vermutlich ausschlaggebend unterstützen.

Der JU ist bewusst, dass Polizei und Staatsanwaltschaft zu schwerfällig sind, um auf neue Maschen zu reagieren. Gleichermaßen unterstreicht sie auch die Notwendigkeit in der Politik und im Bankwesen, die nötigen Entscheidungen zu treffen. Wenn es um viele, international verteilte GES geht, die eine enorme Summe an Schaden haben, dann sollte es das Ziel aller sein, diese Straftaten aufzuklären und die Täter zu finden.

5 Gegenüberstellung

Die Gespräche mit den Beteiligten der Betrugsstraftat Cybertrading und Lektüre zum Fachbereich Kriminalpsychologie waren sehr aufschlussreich. Obwohl alle Erkenntnisse von unterschiedlichen Perspektiven zusammengetragen wurden, zeichnen sich einige Gemeinsamkeiten ab.

Es gibt zehn grundlegende Herausforderungen im Umgang mit Cybertrading:

(1) Es gibt sehr viele Fälle mit Geschädigten jeder Gesellschaftsklasse, Alter und Geschlecht.
(2) Das Phänomen Cybertrading erstreckt sich über den Globus.
(3) Anleger kennen sich nicht genug in dem Bereich aus, auf dem sie betrogen wurden.
(4) Ein Phänomen muss erst als solches erkannt werden, indem genügend Fälle mit ähnlichem Sachverhalt angezeigt werden.
(5) Der Zeit- und Ressourcenaufwand sind enorm. Zugleich fehlen sie an entscheidenden Stellen.
(6) Es entstehen enorm große Schadenssummen.
(7) Die Ermittlungen ziehen sich in die Länge, werden behindert oder sind erfolglos.
(8) Kriminelle wissen sich, ihre Technik und Daten zu schützen.
(9) Es gibt zahlreiche Täter und Gruppierungen, welche die Fähigkeiten und Fertigkeiten haben, ihre Opfer zu manipulieren.
(10) Die Rechtslage ist für Anlagebetrug im digitalen Raum bzw. für schnelles Reagieren über Länder hinweg nicht ausgelegt.

Je nach Fachbereich der Befragten liegen die Fokusse entsprechend unterschiedlich. Während der Geschädigte mit Vertrauensproblemen zu kämpfen hat, sehen der Ermittler und der IT-Experte die Probleme eher bei der Langwierigkeit und Komplexität der Ermittlungen und Auswertungen. Diese Bedenken gelten gleichermaßen für die Juristin, wobei sie zusätzlich die Schwierigkeit in der Koordination der Ermittlungen und Verfolgung der unterschiedlichen Ermittlungsziele Täter, Geld und Netzwerk sieht. Der Fokus der Bankkauffrau liegt vorrangig bei den Geldströmen. Aus ihrer Sicht sind die Phänomenerkennung und die Transfers über Landesgrenzen hinweg die größten Herausforderungen.

In einem Punkt sind sich demnach alle Befragten einig: Es gibt zu viele Fälle, zu viele Geschädigte und zu große Schadenssummen, die von fähigen Tätern weltweit verursacht werden.

Um Cybertrading entgegen zu wirken, gibt es folgende Vorschläge und Wünsche:

(1) Die Bürger müssen besser auf aktuelle Phänomene aufmerksam gemacht werden.
(2) Über Anlagemöglichkeiten im digitalen Raum muss, wie bei einer Bank, besser aufgeklärt werden.

(3) Es müssen ausreichend Ressourcen für die Bekämpfung von Cybertrading und anderen speziellen Phänomenen i.F.v. Zeit und Personal zur Verfügung stehen.
(4) Die Zusammenarbeit der Behörden muss im In- und Ausland unkomplizierter und schneller von statten gehen.
(5) Die rechtlichen Grundlagen müssen den Gegebenheiten des digitalen Zeitalters entsprechend angepasst und optimiert werden.

Erstaunlicherweise überschneiden sich die Vorstellungen der Befragten zur Verbesserung der Maßnahmen im Umgang mit Cybertrading. Der Grundgedanke aller Befragten besteht eindeutig in der Präventionsarbeit. Nicht nur firmenintern, sondern auch allgemein soll die Bevölkerung auf die aktuellen Phänomene aufmerksam gemacht werden und auch die Möglichkeit haben, sich digital und analog bei entsprechenden Stellen informieren zu können. Der IT-Experte liefert dazu einen besonders guten Gedanken, indem er die örtlichen Printmedien einbeziehen möchte. Ergänzend dazu könnten regelmäßige Schulungen zur Sensibilisierung der Bürger beitragen. Auch auf technischer Ebene ist eine Einführung von Sicherheitsmechanismen und spezieller Software inklusive regelmäßiger Überprüfung und Optimierung hilfreich.

Auch bei den Wünschen zur Verbesserung gibt es einen Konsens: Im Falle des Falls darf nicht so viel Zeit vergehen, bis tatsächliche eingegriffen wird bzw. werden kann.

6 Fazit

Beim Cybertrading handelt es sich um ein noch recht junges Straftatphänomen im Bereich des digitalen Anlagebetruges. In dieser Arbeit wurden erste Erkenntnisse über die Herausforderungen im Umgang mit dem Phänomen zusammengetragen mit dem Ziel, einen ersten wissenschaftlich fundierten Einblick in das Zusammenspiel der straftatbeeinflussenden Faktoren zu geben und auf die Betrugsstraftat aufmerksam zu machen.

Für das grundlegende Verständnis über die deskriptiven Faktoren wurden die drei großen Bereiche Wirtschaft, Technik und Soziales beleuchtet. Zum Bereich der Wirtschaft zählen der Handel mit Geld in seiner analogen und digitalen Form, die Blockchain, auf der Kryptowährungen basieren, sowie die Missbrauchsmöglichkeiten des digitalen Geldes für Kriminelle. Wichtige Technikaspekte umfassen den Prozess des Handelns mit digitalen Währungen und den dahinterstehenden Anbietern für Plattformen, Server und Dienstleistungen, sowie käufliche Teiltatbeiträge und Fernsteuerungssoftware. Abgerundet wird dies mit einem beispielhaften Einblick in die soziale Hierarchie und der damit einhergehenden Rollen- und Aufgabenverteilung. Der theoretische Teil dieser Arbeit schließt ab, mit dem exemplarischen Ablauf einer Cybertrading-Tat und den darauffolgenden Ermittlungsansätzen für die Polizei.

Für die Erkenntnisgewinnung wurden ein Sachbearbeiter der Polizei, ein IT-Experte, eine Juristin, eine Bankkauffrau und ein Geschädigter befragt und ein Literaturstudium zur Täterpsychologie geführt. Dabei wurden Antworten auf die Kernfrage gesucht, welche Herausforderungen im Umgang mit dem Straftatphänomen Cybertrading bestehen.

Trotz einzelner Abweichungen in den Fachbereichen bilden die Aussagen der Befragten einen gewissen Konsens im Bezug zu Cybertrading. Allen Beteiligten ist bewusst, dass es sich beim Cybertrading um ein global verbreitetes Phänomen handelt, dessen krimineller Erfolg sich in der großen Anzahl von Strafanzeigen, Geschädigten und Schadenssummen widerspiegelt. Besonders im Bereich der Polizei ist klar, dass die Täter über ausreichend technisches und psychologisches Wissen verfügen, um sich einerseits die Unwissenheit der Opfer zunutze zu machen und andererseits im digitalen Raum verstecken bzw. anonymisieren zu können.

Gleichermaßen kosten die Ermittlungen aus Sicht der Polizei und der Staatsanwaltschaft, aufgrund der Globalisierung und Bürokratie, viele Ressourcen, darunter besonders Zeit und Personal. Der Verlust an Zeit beginnt bei der erschwerten Phänomenerkennung und zieht sich hinweg über die Erfolgschancen der Ermittlungen, welche unweigerlich von der internationalen Zusammenarbeit und dem bürokratisch-diplomatischen Aufwand beeinflusst werden.

Aus diesen Erkenntnissen lassen sich nicht nur die Forderung nach mehr Aufklärung und Prävention schlussfolgern, sondern zugleich die Notwendigkeit von mehr Ressourcen für die Ermittlungen und ein besseres Rechtssystem, welches die internationale Zusammenarbeit von Behörden bekräftigt. Es ist davon auszugehen, dass ein unkompliziertes Sys-

tem zu schnelleren Ermittlungsverfahren führt und somit die Erfolgschancen der zeitnahen Täterverfolgung erheblich unterstützt.

Ein erster Einblick für das Zusammenspiel der verschiedenen Faktoren und Einschätzungen von Beteiligten wurde in dieser Arbeit gegeben. Als besonders positiv hervorzuheben ist die Bereitschaft der Befragten, an der Aufarbeitung des Phänomens Cybertrading mitzuwirken. Auch das BKA erklärte sich bereit, diese Arbeit mit den Erkenntnissen der letzten Jahre zu unterstützen. Jedoch erfolgt die Rückmeldung außerhalb des gesteckten Zeitrahmens, weshalb von Seiten der Autorin abgesagt werden musste.

Für weitere Forschungen zu diesem Themenbereich besteht die Notwendigkeit, den Zeitrahmen größer zu fassen, um den Kreis der Befragten zu erweitern und auch andere Sektoren einzubeziehen. Interessant wären natürlich die Expertise des BKA, Erfahrungen unterschiedlicher Banken, darunter auch Onlinebanken und die Befragung der Dienstleister des technischen Bereiches.

Abschließend lässt sich sagen, dass aufgrund der Neuheit dieses Straftatphänomens nicht davon auszugehen ist, dass Cybertrading weniger attraktiv für Betrüger wird. Der Handel mit Geld und Kryptowährungen und die Gier nach Reichtum werden künftige Täter und Gruppen anlocken. Dort wo eine Bande gefasst wird, wird die nächste nachrücken. Ohne entsprechende Maßnahmen wird sich daran aber auch nichts ändern.

Literaturverzeichnis

Allwinn, M., et al. *Betrügerisches Verhalten aus kriminalpsychologischer Sicht*. 2018. 04. 08. 2022. <https://www.researchgate.net/publication/325497320_Betrugerisches_Verhalten_aus_kriminalpsychologischer_Sicht>.

Alt, R. und S. Huch. *Fintech-Lexikon: Begriffe für die digitalisierte Finanzwelt*. Wiesbaden: Springer Gabler, 2022. <https://doi.org/10.1007/978-3-658-32961-7>.

AnyDesk. *Access.Now.* 2022. 16. 06. 2022. <https://anydesk.com/de>.

—. *Was ist ein Remote-Desktop und wofür wird er verwendet?* 2022. 16. 06. 2022. <https://blog.anydesk.com/de/was-ist-ein-remote-desktop-und-wofuer-wird-er-verwendet/>.

ARD-aktuell. *E.ON Kurs*. 2022. 13. 06. 2022. <https://www.tagesschau.de/wirtschaft/boersenkurse/eon-ag-aktie-enag99/>.

—. *Shell PLC EO-07 Kurs*. 2022. 13. 06. 2022. <https://www.tagesschau.de/wirtschaft/boersenkurse/gb00bp6mxd84-132007880/>.

AT Internet. *Glossar - Lead*. 2022. 24. 06. 2022. <https://www.atinternet.com/de/glossar/lead/>.

BaFin. *Basiskonto*. 2017. 24. 06. 2022. <https://www.bafin.de/DE/Verbraucher/Bank/Produkte/Basiskonto/basiskonto_node.html>.

Behrens, J. *Was ist ein Server?* 2020. 28. 06. 2022. <https://www.ionos.de/digitalguide/server/knowhow/was-ist-ein-server-ein-begriff-zwei-definitionen/>.

—. *Was ist eine Domain?* 2021. 28. 06. 2022. <https://www.ionos.de/digitalguide/domains/domaintipps/was-ist-eine-domain/>.

—. *Webhosting: Server im Vergleich*. 2020. 28. 06. 2022. <https://www.ionos.de/digitalguide/server/knowhow/so-behalten-sie-den-ueberblick-beim-server-vergleich/>.

Bibliographisches Institut. *Recruiting*. 2022. 21. 06. 2022. <https://www.duden.de/rechtschreibung/Recruiting>.

Blockchair. *Blockchain explorer, analytics und web services*. 2022. 01. 07. 2022. <https://blockchair.com>.

Brockhaus, A. *Cybercime as a Service (CaaS) - So funktioniert die professionalisierte Cyberkriminalität*. 2021. 16. 06. 2022. <https://www.is-its.org/it-security-

blog/cybercrime-as-a-service-caas-so-funktioniert-die-professionalisierte-cyberkriminalitaet>.

BSI. *Leitfaden "IT-Forensik"*. Vers. 1.0.1. 2011. 04. 07. 2022. <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=1>.

Bundeskriminalamt. *Abteilung "Cybercrime" (CC)*. 2022. 13. 05. 2022. <https://www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/Cybercrime/cybercrime_node.html>.

—. *PKS 2021 Bund - Falltabellen: T01 Grundtabelle - Fälle (V.1.0)*. 2022. 27. 05. 2022. <https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2021/PKSTabellen/BundFalltabellen/bundfalltabellen.html?nn=194190>.

—. *Polizeiliche Kriminalstatistik (PKS): PKS 2017 - Standard Übersicht Falltabellen: Tabelle 01*. 2022. 27. 05. 2022. <https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2017/Standardtabellen/standardtabellenFaelle.html?nn=96600>.

Bundesministerium der Justiz. *Strafgesetzbuch (StGB) - § 261 Geldwäsche*. 2021. 24. 06. 2022. <https://www.gesetze-im-internet.de/stgb/__261.html>.

—. *Strafgesetzbuch (StGB) - § 73 Entziehung von Taterträgen bei Tätern und Teilnehmern*. 2021. 27. 06. 2022. <https://www.gesetze-im-internet.de/stgb/__73.html>.

—. *Strafprozeßordnung (StPO) - § 100j Bestandsdatenauskunft*. 2022. 29. 06. 2022. <https://www.gesetze-im-internet.de/stpo/__100j.html>.

—. *Strafprozeßordnung (StPO) - § 94 Sicherstellung und Beschlagnahme von Gegenständen zu Beweiszwecken*. 2021. 01. 07. 2022. <https://www.gesetze-im-internet.de/stpo/__94.html>.

—. *Telekommunikationsgesetz (TKG) - § 173 Automatisiertes Auskunftsverfahren*. 2021. 29. 06. 2022. <https://www.gesetze-im-internet.de/tkg_2021/__173.html>.

—. *Telekommunikationsgesetz (TKG) - § 174 Manuelles Auskunftsverfahren*. 2021. 29. 06. 2022. <https://www.gesetze-im-internet.de/tkg_2021/__174.html>.

Cherry Servers. *Let's Democratize Cloud Together*. 2022. 31. 07. 2022. <https://www.cherryservers.com/company#about>.

Coinbase. *Jetzt durchstarten mit Ihrem Krypto-Portfolio*. 2022. 14. 06. 2022. <https://www.coinbase.com/de/>.

Deker, C., et al. *Ermittler zerschlagen Betrügerring*. 2019. 21. 06. 2022. <https://www.tagesschau.de/investigativ/ndr/trading-portale-101.html>.

Derleder, P., Knops, K.-O. und Bamberger, H. G. *Deutsches und europäisches Bank- und Kapitalmarktrecht*. Bd. 2. Berlin, Heidelberg: Springer, 2017. <https://doi.org/10.1007/978-3-662-52805-1>.

Deutsche Börse. *Aktien - An Unternehmen teilhaben*. 2022. 14. 06. 2022. <https://www.boerse-frankfurt.de/einstieg/aktien-an-unternehmen-teilhaben>.

—. *So funktioniert die Börse*. 2022. 14. 06. 2022. <https://www.boerse-frankfurt.de/einstieg/so-funktioniert-die-boerse>.

Einbock, S., et al. *Betrug - § 263 StGB - Vortäuschung falscher Tatsachen - Schema*. 2022. 04. 08. 2022. <https://www.juraforum.de/lexikon/betrug#:~:text=Der%20objektive%20Tatbestand%20des%20Betruges,eine%20T%C3%A4uschung%20%C3%BCber%20Tatsachen%20vorliegen.>.

eToro. *Die Power des Social Investing*. 2022. 14. 06. 2022. <https://www.etoro.com/de/>.

Generalzolldirektion. *Financial Intelligence Unit*. kein Datum. 01. 07. 2022. <https://www.zoll.de/DE/Der-Zoll/Aufgaben-des-Zolls/Schutz-fuer-Buerger-Wirtschaft-und-Umwelt/FIU-Aufgaben/fiu-aufgaben_node.html>.

Hentsch, A.-K. *Kurzfristig positiv: Corona-Effekte auf die Umwelt*. 2020. 13. 06. 2022. <https://www.nationalgeographic.de/umwelt/2020/03/kurzfristig-positiv-corona-effekte-auf-die-umwelt>.

Hoffmann, J. *Psychologie von Betrügern*. 2011. 04. 08. 2022. <https://www.researchgate.net/publication/317504047_Psychologie_von_Betrugern>.

Hostinger. *Eins. Zwei. Online*. 2022. 31. 07. 2022. <https://www.hostinger.de/uber-uns>.

Krause, F. *Wie und wo kann ich Kryptowährungen kaufen?* 2022. 14. 06. 2022. <https://blockchainwelt.de/kryptowaehrung-kaufen/>.

Kryptonauten. *Teil 4: Wie kaufe ich Kryptowährungen?* 2022. 16. 06. 2022. <https://www.blockchaincenter.net/kryptowaehrungen-kaufen/>.

Lange, H.-J., Model, T. und Wendekamm, M. *Zukunft der Polizei - Trends und Strategien*. Wiesbaden: Springer VS, 2019. <https://doi.org/10.1007/978-3-658-22591-9>.

May, T. und Bhardwa B. *Organized Crime Groups Involved in Fraud. Crime Prevention and Security Management*. London: Palgrave Macmillan, 2018. <https://doi.org/10.1007/978-3-319-69401-6_4>.

Nakamoto, S. „Bitcoin Whitepaper.“ 2008. 07. 06. 2022. <https://www.bitcoin.com/satoshi-archive/whitepaper/>.

Rosenberger, P. *Bitcoin und Blockchain - Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik*. Berlin: Springer Vieweg, 2018. <https://doi.org/10.1007/978-3-662-56088-4>.

Schroer, K. *Angebot und Nachfrage*. 2022. 14. 06. 2022. <https://www.bwl-lexikon.de/wiki/angebot-und-nachfrage/>.

Schuchter, A. *Perspektiven verurteilter Wirtschaftsstraftäter - Gründe ihrer Handlungen und Prävention in Unternehmen*. Wiesbaden: Springer Gabler, 2012. <https://doi.org/10.1007/978-3-8349-3606-6>.

Shidigital. *Wie das Internet funktioniert*. 2021. 27. 06. 2022. <https://developer.mozilla.org/de/docs/Learn/Getting_started_with_the_web/How_the_Web_works#credit>.

Shover, N., Coffey, G. S. und Sanders, C. R. *Dialing for Dollars: Opportunities, Justifications, and Telemarketing Fraud. In: Qualitative Sociology*. Bd. 27 Nr. 1. Tennessee: Springer, 2004.

SISTRIX. *Was ist der Unterschied zwischen URL, Domain, Subdomain & Hostnamen?* 2021. 28. 06. 2022. <https://www.sistrix.de/frag-sistrix/seo-grundlagen/was-ist-der-unterschied-zwischen-einer-url-domain-subdomain-hostnamen-usw>.

Sixt, E. *Bitcoins und andere dezentrale Transaktionssysteme - Blockchains als Basis der Kryptoökonomie*. Wiesbaden: Springer Gabler, 2017. <https://doi.org/10.1007/978-3-658-02844-2>.

Stirnimann, S. *Der Mensch als Risikofaktor bei Wirtschaftskriminalität - Handlungsfähig bei Non-Compliance und Cyberkriminalität*. Wiesbaden: Springer Gabler, 2021. <https://doi.org/10.1007/978-3-658-34631-7>.

TeamViewer Germany. *Digitale Transformation "Made in Germany"*. kein Datum. 16. 06. 2022. <https://www.teamviewer.com/de/>.

TechTarget. *ISP (Internet Service Provider)*. 2016. 28. 06. 2022. <https://www.computerweekly.com/de/definition/ISP-Internet-Service-Provider>.

Uhl, C. und Resch, N. *Prozess um Cybertrading-Portale startet*. 2022. 21.. 06. 2022. <https://www.tagesschau.de/investigativ/trading-portale-betrug-prozess-101.html>.

Walden, R. *Sequenzen von Skepsis (39)*. 2010. 27. 05. 2022. <https://raymond-walden.blogspot.com/2010/07/sequenzen-von-skepsis-39.html>.

Whitty, M. T. *Mass-Marketing Fraud: A Growing Concern. In: IEEE Security & Privacy*. Bd. 13 Nr. 4. 2015.

X-Ways AG. *X-Ways Forensics: Integrierte Software für Computerforensik*. kein Datum. 04. 07. 2022. <http://www.x-ways.net/forensics/index-d.html>.

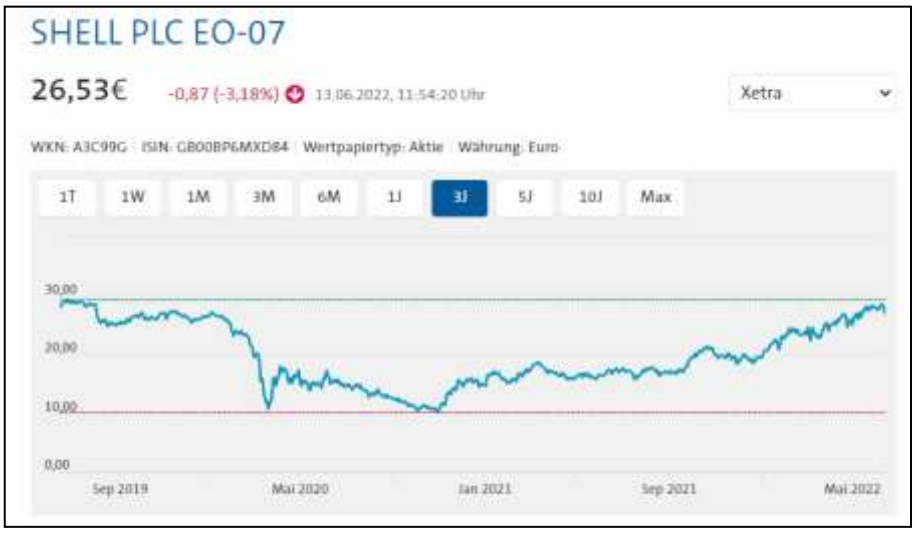
Zierer, M. und Tanriverdi, H. *Abzocke mit Bitcoins*. 2022. 21. 06. 2022. <https://www.tagesschau.de/investigativ/br-recherche/bitcoin-betrug-101.html>.

Anhangverzeichnis

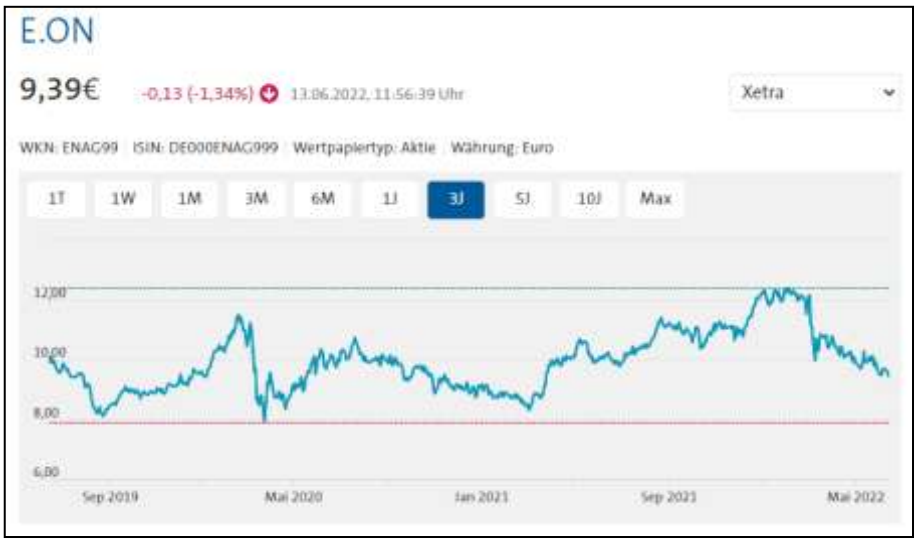
Anhang

Anhang 1: Kursverläufe an der Börse

Anhang 1.1: Kursverlauf der Shell PLC EO-07 Aktie der letzten drei Jahre[134]



Anhang 1.2: Kursverlauf der E.ON Aktie der letzten drei Jahre[135]



[134] ARD-aktuell: Shell PLC EO-07 Kurs. (2022) Abgerufen am 13.06.2022 von https://www.tagesschau.de/wirtschaft/boersenkurse/gb00bp6mxd84-132007880/.
[135] ARD-aktuell: E.ON Kurs. (2022) Abgerufen am 13.06.2022 von https://www.tagesschau.de/wirtschaft/boersenkurse/eon-ag-aktie-enag99/.

Anhang 2: Anfrage für ein Interview[136]

Persönlich/Vertraulich

Datum

Anfrage – Interview – Bachelorarbeit

Sehr geehrte Frau *(Name der Adressatin)* bzw. Sehr geehrter Herr *(Name des Adressaten)*,

im Rahmen meines Studiums an der Hochschule Mittweida im Fachbereich Forensik schreibe ich eine Bachelorarbeit zum Thema „Herausforderungen im Umgang mit dem Straftatphänomen Cybertrading".

Beim Cybertrading, auch Boiler Room Fraud genannt, handelt es sich um eine Wirtschaftsstraftat, bei der Anleger auf betrügerischen Plattformen in Aktien oder Kryptowährungen investieren und ihr Geld nie ausgezahlt bekommen.

Obwohl es weitreichende Lektüre zu den Fachbereichen Finanzen, Technik und Betrugsstraftaten gibt, verlaufen Suchanfragen zum spezifischen Thema Cybertrading trotz demonstrativer Aktualität ins Leere. Daraufhin habe ich es mir zur Aufgabe gemacht, in meiner Abschlussarbeit einen ersten wissenschaftlich fundierten Einblick in das Zusammenspiel der Faktoren Wirtschaft, Technik, Soziales und Ermittlung zu geben und so auf diese Betrugsstraftat aufmerksam zu machen.

Hiermit möchte ich bei Ihnen höflichst um ein Gespräch mit einer Dauer von ungefähr 30 Minuten anfragen. Wenn Sie dem zustimmen, wird das Gesprochene vertraulich behandelt und ausschließlich für den wissenschaftlichen Zweck verwendet. Um Anonymität zu gewährleisten, wird Ihr Name nirgendwo erwähnt.

Das Gespräch kann telefonisch durchgeführt werden oder an einem für Sie vertrauten Ort. Das Interview beinhaltet folgende Kernfrage: Welche Herausforderungen sehen Sie im Umgang mit dem Straftatphänomen Cybertrading?

Ich möchte Sie höflichst bitten, mir Ihre Bereitschaft zur Teilnahme persönlich mitzuteilen unter

Telefon (privat): [redacted]
E-Mail:

Sollten Sie Fragen oder Anmerkungen haben, zögern Sie bitte nicht, mich vorab zu kontaktieren.

---

[136] Adaptiert nach A. Schuchter: Perspektiven verurteilter Wirtschaftsstraftäter - Gründe ihrer Handlungen und Prävention in Unternehmen. (Wiesbaden: Springer Gabler, 2012) S. 216

Ich würde mich freuen, wenn Sie mich bei meinem Vorhaben mit Ihrer Erfahrung unterstützen.

Mit besten Grüßen

Antonia J. Franke

Anhang 3: Zusicherung der Anonymität[137]

Persönlich/Vertraulich

Datum

Zusicherung der Anonymität

Sehr geehrte Frau *(Name der Adressatin)* bzw. Sehr geehrter Herr *(Name des Adressaten)*,

hiermit bestätige ich, Antonia Justine Franke, geboren am [redacted], Ihnen gegenüber die vollständige Anonymität bezüglich des Interviews, welches am *(Datum)* in *(Ort)* stattgefunden hat.

Sämtliche Aussagen werden höchst vertraulich behandelt und ausschließlich für die Verarbeitung zu wissenschaftlichen Zwecken genutzt. Hiermit sichere ich Ihnen zu, Ihren Namen an keiner Stelle der schriftlichen Ausarbeitung zu nennen und auch anderweitig keine Angaben zu machen, die auf Ihre Person hinweisen.

Ich möchte damit bewirken, dass Sie frei heraus erzählen können und so die Ausarbeitung mit Ihren authentischen Erfahrungen bereichern.

Ich danke Ihnen herzlichst für Ihre Kooperation.

Mit freundlichen Grüßen

Antonia J. Franke

[137] Adaptiert nach A. Schuchter: Perspektiven verurteilter Wirtschaftsstraftäter - Gründe ihrer Handlungen und Prävention in Unternehmen. (Wiesbaden: Springer Gabler, 2012) S. 220.

Anhang 4: Interviewleitfaden[138]

Bevor wir anfangen, möchte ich mich recht herzlich für Ihre Teilnahme bedanken.

Das Interview besteht aus *(Anzahl)* Fragen und dauert, je nach Ausführung Ihrer Antworten circa 30 Minuten.

Wie im Anschreiben angesprochen, gibt es in der wissenschaftlichen Fachliteratur keine disziplinübergreifende Untersuchung zur Wirtschaftsstraftat Cybertrading. Beim Cybertrading oder Boiler Room Fraud handelt es sich um eine Form des Anlagebetrugs mit zum Teil Kryptowährungen. Dank der Digitalisierung und Globalisierung sind Betrugsstraftaten im Bereich Anlage- und Kapitalmöglichkeiten um einiges komplexer als vorher. Um einen ersten Eindruck zu gewinnen, werden die Faktoren Wirtschaft, Technik und Soziales untersucht. Es ist davon auszugehen, dass Ihre Erfahrung einen wesentlichen Beitrag zum Verständnis über diese Straftat leisten kann.

Alles was hier gesagt wird, bleibt unter uns. Wie versprochen, werden Ihre Aussagen vertraulich behandelt und anonymisiert ausgewertet.

Das heißt:

1. Ihr Name wird in keinster Weise erwähnt,

2. es werden ausschließlich Ihre Aussagen verwertet und

3. spezifische Angaben im geschriebenen Text werden entweder entfernt oder soweit möglich generalisiert („Bank X“ wird zu „Institution“, Namen werden entfernt)

Ich bin mir im Klaren, dass es sich hierbei um ein ernstzunehmendes Thema handelt. Aus diesem Grund werden Ihre Aussagen diskret und anonym behandelt. Ich möchte damit bezwecken, dass Sie frei heraus erzählen können und so einen authentischen Einblick geben können.

Der Anlass:

Das Ziel besteht darin, die Aufmerksamkeit auf moderne Betrugsstraftaten zu lenken und so einerseits die Herausforderungen im Umgang mit diesen Straftaten hervorzuheben und andererseits einen Mehrwert für die Ermittlungen zu schaffen.

Sind Sie damit einverstanden, dass das Gespräch ab jetzt aufgezeichnet wird, um es anschließend transkribieren und auswerten zu können?

---

[138] Adaptiert nach A. Schuchter: Perspektiven verurteilter Wirtschaftsstraftäter - Gründe ihrer Handlungen und Prävention in Unternehmen. (Wiesbaden: Springer Gabler, 2012) S. 218.

Wenn Sie damit einverstanden sind, dann wird die Aufnahme im Anschluss von mir persönlich transkribiert, ausgewertet und interpretiert.

Haben Sie noch Fragen?

Anhang 5: Interviewfragen

Anhang 5.1: Interviewfragen – GES

1. Erzählen Sie mir von sich. Wie gestalten Sie Ihren Lebensalltag?
2. Wie sind Sie auf die Idee gekommen, Ihr Geld anzulegen?
3. Schildern Sie mir bitte kurz, wie der Betrug von Statten ging.
4. Haben Sie sich zu der Plattform im Vorhinein belesen? Warum (nicht)?
5. Wie war das Verhalten des/der Täter/s Ihnen gegenüber? Hat etwas Zweifel erregt oder die Seriosität unterstrichen? Was hat er über sich preisgegeben?
6. Haben Sie immer noch Kontakt zu dem/den Täter/n? Warum (nicht)?
7. Haben Sie in Krypotwährungen investiert? Wenn ja, wissen Sie, was es damit auf sich hat?
8. Haben Sie Gelder zurück erhalten?
9. Vor welche Herausforderungen hat Sie das finanziell/gesellschaftlich gestellt?
10. Haben Sie bereits vorher schon einmal von dem Begriff Cybertrading bzw. Boiler Room Fraud gehört oder gelesen?
11. Wie ist Ihre Einstellung gegenüber der Geldanlage, nachdem Sie betrogen wurden? Würden Sie wieder investieren? Wenn ja, wo und warum?
12. Was würden Sie rückblickend anders machen, wenn Sie es könnten?
13. Wenn Sie Ihren anderen Anlegern einen Ratschlag geben könnten, welcher wäre es?
14. (Schluss) Gibt es etwas was Sie dem Gespräch noch beifügen wollen?

Anhang 5.2: Interviewfragen – KPS

1. Erzählen Sie mir von sich. Welche Funktion nehmen Sie bei Ermittlungen ein und welche Aufgaben erfüllen Sie dort?
2. Haben Sie bereits vorher schon einmal von dem Begriff Cybertrading bzw. Boiler Room Fraud gehört oder gelesen?
3. Was treibt Menschen dazu, andere zu ihrem Vorteil zu beeinflussen? Gibt es Merkmale, die immer wieder auftreten?
4. Wie kann es sein, dass Leute immer wieder in die Falle von Betrügern tappen?
5. Inwieweit kann man Betrüger aus der digitalen Welt mit denen der analogen Welt vergleichen?
6. Wie viele/Welche Personen des hierarchischen Netzwerks lassen sich wirklich als Täter einordnen? (Tätermerkmale)
7. Wie gehen Sie mit Betrügern um? Welchen Eindruck erwecken sie?
8. Welche Maßnahmen müssten ergriffen werden, um Betrüger besser strafrechtlich verfolgen zu können?

Anhang 5.3: Interviewfragen – BKF

1. Erzählen Sie mir von sich. Welche Funktion nehmen Sie bei Ihrer Bank ein und welche Aufgaben erfüllen Sie dort?
2. Haben Sie bereits vorher schon einmal von dem Begriff Cybertrading bzw. Boiler Room Fraud gehört oder gelesen?
3. Inwieweit warnen Sie Ihre Kunden vor (neuen) Betrugsmaschen? Sind diese Maßnahmen erfolgreich?
4. Wie gehen Sie bei der Betrugsmeldung eines Kunden vor?
5. Wie stehen die Chancen, das Geld der geschädigten Kunden zurückzuholen? Wodurch wird das beeinflusst?
6. Welche Faktoren bedarf es, damit ein Kundenkonto den Verdacht zur Geldwäsche erregt?
7. Wie stehen Sie zu Kryptowährungen? Sehen Sie darin Potenzial oder eine Gefahr?
8. Wo sehen Sie Schwierigkeiten bei der Bearbeitung von Betrugsfällen? Was können Sie oder Dritte dagegen tun?
9. Welchen Tipp können Sie Anlegern geben, wenn es um das Investieren von und Handeln mit Geldwerten geht?
10. (Schluss) Gibt es etwas was Sie dem Gespräch noch beifügen wollen?

Anhang 5.4: Interviewfragen – E

1. Erzählen Sie mir von sich. Welche Funktion nehmen Sie bei den Ermittlungen ein und welche Aufgaben erfüllen Sie dort?
2. Wie lange befassen Sie sich bereits mit Cybertrading?
3. Wie sieht ein klassischer Fall aus?
4. Wie gehen Sie mit den Geschädigten um? Welchen Eindruck erwecken sie?
5. Gibt es eine Art Struktur oder Muster seitens der Betrüger, welches Ihnen bei den zahlreichen Ermittlungen aufgefallen ist?
6. Wie lange dauert es im Schnitt, einen Sachverhalt zu klären?
7. Wie gut stehen die Chancen, die Täter zu fassen?
8. Woran scheitern manche Ermittlungen?
9. Wie könnten die Ermittlungen intern und extern besser unterstützt werden?
10. (Schluss) Gibt es etwas was Sie dem Gespräch noch beifügen wollen?

Anhang 5.5: Interviewfragen – ITE

1. Erzählen Sie mir von sich. Welche Funktion nehmen Sie bei den Ermittlungen ein und welche Aufgaben erfüllen Sie dort?
2. Wie lange befassen Sie sich bereits mit Cybertrading?
3. Wonach suchen Sie bei der Auswertung von digitalen Daten?
4. Wie lange dauert eine Auswertung im Durchschnitt?
5. Können Sie bei den Auswertungen eine Veränderung der Schwierigkeit/Komplexität wahrnehmen?
6. Gibt es eine Art Struktur oder Muster seitens der Betrüger, welches Ihnen bei den zahlreichen Ermittlungen aufgefallen ist?
7. Welche Probleme können bei den Ermittlungen auftreten und wie werden diese gelöst?
8. Wie könnten die Ermittlungen intern und extern besser unterstützt werden?
9. (Schluss) Gibt es etwas was Sie dem Gespräch noch beifügen wollen?

Anhang 5.6: Interviewfragen – JU

1. Erzählen Sie mir von sich. Welche Funktion nehmen Sie bei der Strafverfolgung ein und welche Aufgaben erfüllen Sie dort?
2. Wie lange befassen Sie sich bereits mit Cybertrading?
3. Wo liegen die Prioritäten aus Sicht der Justiz? (Geld, Täter, Netzwerk, Dienstleister)
4. Welche Personen des hierarchischen Netzwerks lassen sich strafrechtlich verfolgen? (Täter/Mittäter/Teilnehmer/Beihilfe)
5. Wie bewerten Sie den inländischen und ausländischen Aufwand bei der Durchsetzung von Maßnahmen? (Durchsuchungen, Beschlagnahmen, Kryptos, Fiat, Zusammenarbeit)
6. Woran scheitern manche Maßnahmen zur Strafverfolgung?
7. Wo sehen Sie Schwierigkeiten bei der Bearbeitung von Betrugsfällen? Was können Sie oder Dritte dagegen tun?
8. (Schluss) Gibt es etwas was Sie dem Gespräch noch beifügen wollen?

Anhang 6: Transkripte der Interviews

Anhang 6.1: Transkript – Interview – GES

A: Hallo nochmal, vielen Dank für die Möglichkeit. Bevor wir anfangen, für das Protokoll, ist es ok, wenn ich du sage?

GES: Ja.

A: Durch einen „unglücklichen“ Zufall sind wir zueinander gekommen und kennen uns schon. Bitte erzähl‘ mir von dir. Wie gestaltest du deinen Lebensalltag, was machst du so?

GES: Ich bin in Rente und gestalte meinen Alltag ganz normal. Ich bin alleine und muss alles alleine machen. Einkaufen, Waschen, etc., was man so alles machen muss. Ich mache nebenbei ein bisschen Musik. Ansonsten im Sommer [bin ich] im Garten, im Winter wird es ein bisschen langweilig. Ganz normaler Alltag, wie jeder Rentner das so veranstaltet.

A: Dann natürlich die große Preisfrage, wie bist du überhaupt auf die Idee gekommen Geld anzulegen? Was war der ausschlaggebende Punkt?

GES: Das war aus einer dummen Laune heraus. Ich bin auf diese Annonce bei Facebook aufmerksam geworden und dachte mir, das probierst du einfach mal. Die 256,00 Euro einzuzahlen, das tut mir nicht weh. Ich hatte auch gelesen, dass das funktionieren sollte. Ich habe [eingezahlt], bin angerufen worden und auf diese komische Seite geleitet worden, deren App. Ich hatte am Anfang gesagt, dass ich eigentlich nur mal schauen will, wie das bei denen funktioniert.

A: Also aus reiner Neugier?

GES: Genau, denn wenn ich die 256,00 Euro verloren hätte, das hätte mir das nicht wehgetan. Ich habe denen das auch gesagt, aber derjenige, der mich angerufen hatte, hat mich ausgefragt bis zum geht nicht mehr. Bis wir dann im Gespräch auf meine Tochter gekommen sind. Der [Broker] hat gefragt, was sie macht. Sie ist Friseurmeisterin und will sich irgendwann mal selbstständig machen. Da hat er mich gegriffen. Er hat gesagt, ich könne meine Tochter unterstützten. Ich sollte Geld anlegen, damit verdiene ich einen Haufen [Geld] und kann [meine Tochter] unterstützen, wenn sie sich selbstständig macht. Da sagte ich ok, können wir probieren.

Ich habe das erste Mal 1.000,00 Euro überwiesen und habe geguckt wie das alles funktioniert auf ihrer App. Ich dachte, das sieht professionell aus, das haben sie richtig gut gemacht. Da kam mir gar nicht in den Sinn, dass das alles fake ist. Jedenfalls hat er gesagt,

wir setzen auf den fallenden Ölpreis. Ich sagte ok, aber der wird irgendwann wieder steigen. Dann drehen wir das wieder um, [meinte er]. Ich sagte ok, machen wir. Dann rief er wieder an. Können sie nicht noch mehr Geld überweisen, es läuft gerade so gut. Sie sehen doch, wie das steigt. Ja das sehe ich. Ok ich überweise nochmal 1.000,00 Euro.

Dann habe ich gesehen, dass ich ein Plus von 10.000,00 Euro hatte und wollte 5.000,00 Euro auszahlen lassen. Ich habe auf den Auszahlungs-Knopf gedrückt, der ging natürlich nicht. Ich habe gefragt, warum das nicht geht. Er hat nur gesagt, es geht nicht. Da war ich schon stutzig. Dann rief er wieder an und sagte, [der Kurs] fällt langsam, wir müssen mehr Geld einzahlen. Ich fragte, wieso mehr Geld einzahlen? Ja das muss so, sonst verliere ich alles. Gut, da habe ich mich nochmal breitschlagen lassen und habe 2.000,00 Euro überwiesen. Am nächsten Tag rief er wieder an. [Der Kurs] geht nach unten, um den Verlust auszugleichen müsse ich noch mehr investieren. Ich sagte, ich habe kein Geld mehr, soll ich mich nackig machen oder was? Da meinte er, ich verliere alles. Ich sagte, ich habe nicht mehr Geld, sie können nicht mehr kriegen. [Daraufhin meinte er], er habe gesehen, dass ich genug Geld auf dem Konto habe. Da bin ich stutzig geworden. Ich fragte, wieso können sie sehen, dass ich so viel Geld auf dem Konto habe. Ja, das haben wir gesehen. Das haben die gesehen, als ich eine Überweisung gemacht habe. Die haben gesehen, was ich auf dem Konto habe. Da bin ich stutzig geworden. Das ist eine Frechheit, dass sie in mein Konto reingucken, was ich an Geld habe! Das geht euch einen Scheißdreck an! Ich bezahle nicht mehr. Da fing er an zu plappern, den ganzen Verlust müsse ich dann tragen. Ich sagte, mein Verlust ist das, was ich ihnen überwiesen habe, den anderen Verlust können sie selber tragen. Für mich ist hier Ende. Ich vertraue euch nicht. [Er antwortete,] sie haben mir doch auch vertraut. Ich sagte ja, ihr wollt nur mein Geld.

Das war für mich eigentlich abgeschlossen, aber die haben natürlich immer wieder versucht mich per E-Mail, per Anruf zu locken. [Sie] wollten immer wieder Geld haben und haben mich [auf die] 20.000,00 Euro Verlust [hingewiesen]. Die haben mir selber Gelder eingetragen, wie Kredits, was [gar nicht] von mir war und auch nie verlangt hatte. Jedenfalls waren dann 20.000,00 Euro im Minus, die meinten, dass ich das bezahlen müsste. Natürlich bezahle ich das, wenn ihr das ins Minus laufen lasst?! Ich sagte tschüss, macht es gut.

[Ich] habe die angeschrieben, dass ich mein Geld zurück haben will. Da hat sich dann ein anderer [Mann] gemeldet. Um die 4.000,00 Euro wieder zurück zu kriegen, sollte ich viermal 5.000,00 Euro überweisen. Ich sagte wie bitte, wie soll denn das funktionieren? Der sagte das ist so, anders geht es nicht, um an mein Geld zu kommen. Ich sagte, ich glaube ihnen kein Wort. Da hat sich das für mich völlig erledigt.

A: Es war immer wieder so: du zahlst ein, das war denen aber nicht genug und 24 Stunden später wollten die wieder mehr haben. Das ging dann die ganze Zeit so weiter?

GES: Ja

A: Das ist dann schon relativ penetrant.

GES: Ja. Ich habe mich auch ein bisschen kundig gemacht im Internet über sowas. Da sind Leute abgezockt worden, Wahnsinn. Die haben Hof und Haus verloren.

A: Hast du damals auch was gefunden zu der Plattform, wo du investiert hast? Hast du dich insgesamt zu der Plattform mal belesen oder war es damals schon zu spät?

GES: Da war es schon zu spät, das hätte ich eher machen sollen. Ich habe mich kundig gemacht. Auf manchen Plattformen wurden sie positiv dargestellt, fake wahrscheinlich. Andere Plattformen haben natürlich gemerkt, was das für Verbrecher sind und dass sie nur die Leute abzocken wollen.

A: Wieso hast du dich damals nicht dafür entschieden, das vorher mal zu recherchieren?

GES: Keine Ahnung. Das hätte ich eher machen sollen. Aber ich habe daran dummerweise geglaubt.

A: Wie schätzt du das Verhalten des Täters oder der Täter, ich weiß nicht, mit wie vielen du am Ende Kontakt hattest, dir gegenüber ein?

GES: Am Anfang sind sie sehr nett, solange du mitspielst. Wenn du nicht mehr mitspielst, werden sie grantig, frech und reden dir Sachen ein, die gar nicht relevant sind. Zum Beispiel das Geld zu bezahlen, was da an Verlust war. Auch per E-Mail habe ich ab und zu ein bisschen frech hin geschrieben, weil ich gemerkt habe, dass sie nur betrügen wollen. [Gemeldet haben sie sich] ab und zu per E-Mail, [haben] telefonisch ständig angerufen, bis heute, monatelang.

A: Und sind die da immer noch nett, wenn du ans Telefon gehst oder wenn sie eine Mail schreiben?

GES: Am Anfang sind sie noch nett, aber wenn du nicht mitspielst, dann sind sie nicht mehr nett.

A: Wann war bei dir der Zeitpunkt erreicht, wo du Zweifel hattest an der Seriosität der Täter bzw. der Plattform?

GES: Wo der [Broker] sagte, ich habe doch genügend Geld auf dem Konto. Da hat es bei mir Klick gemacht. Ich finde das unverschämt, dass sie Einsicht auf mein Konto genommen haben, da bin ich hellhörig geworden. Von dem Zeitpunkt an war Ende bei mir.

A: Hattest du die Täter auch auf deinen Rechner zugreifen lassen?

GES: Ja, die konnten teilweise zugreifen.

A: War dir bewusst, dass, wenn du eine Überweisung tätigst, die das sehen?

GES. Nein, es war mir nicht bewusst, dass die das einsehen können.

A: Die sehen ja theoretisch alles, das ist [eine Art] Bildschirmübertragung. Ich weiß nicht, ob man das als Zweifel nennen kann, wenn das eigentlich ein blöder Zufall war, [ausgehend davon, dass] du unachtsam warst oder?

GES: Möglich.

A: Hat denn der Täter oder die Täter etwas über sich preisgegeben?

GES: Nein, die haben meistens nur mich ausgefragt. Von sich haben sie gar nichts erzählt.- Die wollten immer nur von mir irgendwelche Sachen wissen und haben mich in Gespräche verwickelt.

A: Hast du noch Kontakt zu den Tätern?

GES: Nein, den lehne ich konsequent ab.

A: Aber sie probieren es immer noch?

GES: Ja, [auch letztens]. Ich bin [meist] gar nicht rangegangen an die Nummern und habe sie alle blockiert.

A: Hast du damals in Kryptowährungen investiert oder ausschließlich in die Ölwerte?

GES: Nein, nur in diese fallenden Ölwerte. Da hatte mal einer angerufen, der wollte mir Kryptowährungen andrehen. Der hat sich für [den Herrn Schmidt] ausgegeben, mit dem ich das am Anfang gemacht hatte. Das war ein Ausländer, der sagte ich bin der Herr Schmidt. Ich sagte nein, sind sie nicht. Geben sie mir die Nummer. Herr Schmidt hatte mir die Nummer [gegeben], die ich nur angeben musste, wenn mal jemand Fremdes anruft. Die hat [der neue Anrufer] nicht gesagt. Da habe ich gesagt, nein, mit ihnen rede ich nicht. Der wollte mir Kryptowährungen andrehen.

A: Weißt du denn was Kryptos sind?

GES: Ja, aber für mich ist das eigentlich eine Fake-Währung.

A: Hast du bisher [Geld] zurück erhalten oder ist immer noch alles weg?

GES: Nein, alles weg.

A: Vor welche Herausforderungen hat dich diese Abzocke am Ende gestellt, finanziell und gesellschaftlich betrachtet?

GES: Es ging bei mir nur um 4.000,00 Euro, die kann ich verschmerzen. Klar ist das nicht schön und tut irgendwo weh. Man ist menschlich hinter das Licht geführt worden.

A: Es hat dich demnach nicht finanziell in den Ruin getrieben.

GES: Nein, Gott sei Dank nicht.

A: Wenn du mehr eingezahlt hättest, wäre es wahrscheinlich krasser geworden. Hattest du gesellschaftlich Probleme? Wenn du jemandem davon erzählt hast, dass dich jemand über‘s Ohr gehauen hat, hat man dich da gewissermaßen wie verurteilt, weil du auf sowas reingefallen bist?

GES: Nein, kann ich nicht sagen. Es wissen vielleicht zwei oder drei Personen davon, weil es mir unangenehm ist, das weiterzuerzählen. Verurteilt hat mich da keiner.

A: Wie würdest du das einschätzen, wenn dir fremde Leute gegenübertreten und dir Ähnliches anbieten? Da schrillt vielleicht bei dir eine Alarmglocke. Wäre das eine Herausforderung, weil du dann skeptisch bist?

GES: Ja klar, normalerweise bin ich immer skeptisch. Ich habe in meinem Leben auch schon andere Sachen erlebt, bloß diesmal haben sie mich mit meiner Tochter gepackt. Ich bin auf das Geld, was ich da eventuell gewonnen hätte, gar nicht angewiesen. Die Burschen haben mich an einem wunden Punkt getroffen, [sodass] ich den Mist mitgemacht habe.

A: Du weißt ja, das Phänomen heißt Cybertrading. Wurde dir damals gesagt, dass die Betrugsmasche so heißt?

GES: Nein.

A: Hast du es erstmal von mir und meinem Kollegen gehört?

GES: Ich habe es im Internet gelesen.

A: Das ist auch gut. Hattest du vorher schon irgendwas darüber gehört oder gelesen, wenn du sagst du hast recherchiert?

GES: Manchmal im Fernsehen. Über diese Sache, wie das hier abgelaufen ist, habe ich nichts gehört. Die haben gewisse andere Betrugsmaschen am Start. Es ist ja nicht nur [Cybertrading]. Es gibt so viele Betrugsmaschen.

A: Falsche Handwerker, falsche Polizisten, Enkeltrick…

GES: Genau, das ist mir geläufig. Das mit dem, was ich gemacht habe, da wusste ich null Bescheid.

A: Ansonsten guckst du im Fernsehen aktiv nach solchen Sendungen? Sowas wie Aktenzeichen XY ungelöst?

GES: Ja.

A: Dann bist du ja quasi auf dem Laufenden, was gerade so Masche ist.

GES: Das interessiert mich immer.

A: Auch vorher schon?

GES: Teilweise schon, aber jetzt natürlich wesentlich mehr.

A: Dadurch kann man sich vielleicht ein bisschen wappnen, vor dem was vielleicht noch kommt.

GES: Man kann aus Fehlern nur lernen.

A: Richtig. Wie ist deine Einstellung gegenüber der Geldanlage, nachdem du betrogen wurdest? Würdest du wieder Geld anlegen und wenn ja wo?

GES: Nein, auf keinen Fall. Lieber stecke ich es in das Bankfach.

A: Also hat dir diese Erfahrung das total vergrault?

GES: Total. Es ist eine Frechheit, was die machen.

A: Du würdest lieber mit deinem Geldcouvert zum Schalter gehen und sagen, ich möchte mein Geld anlegen, geben sie mir ein Konto?

GES: Ja, das habe ich eigentlich jahrelang so gemacht. Ich muss dazu sagen, ich hatte zu dem Zeitpunkt aufgehört zu rauchen und ich merke, dass ich da nicht ganz richtig im Kopf war. Sonst wäre mir das vielleicht gar nicht passiert.

A: Auf der anderen Seite ist es eine Möglichkeit gewesen. Du hast die [Anzeige] online gesehen und vielleicht gedacht, warum nicht probieren? Probieren geht über Studieren.

GES: Genauso ist es. Ich wollte ja nur probieren, bis er mich gepackt hat mit meiner Tochter. Deswegen haben die mich ausgefragt über Familie und was ich so alles mache. Die wollten von mir Sachen wissen, da hat man sich gefragt.

A: Rückblickend, was würdest du anders machen? Angenommen du siehst heute nochmal die Anzeige.

GES: Natürlich würde ich da nichts mehr machen, das ist vollkommen klar. Ich habe das nur aus Dummheit und Langeweile vielleicht gemacht. Denn nötig habe ich es ja gar nicht, noch mehr Geld zu machen. Ich komme mit meinem Geld was ich habe und was ich verdiene gut zurecht. Was will ich mit hunderttausenden von Euros?

A: Wenn es die überhaupt gibt, in den paar Tagen. Es ist ja ein sehr lukratives Angebot was die machen, eigentlich zu schön um wahr zu sein. Gar nicht erst anlegen wäre deine Antwort?

GES: Auf keinen Fall.

A: Wenn du jetzt anderen Anlegern einen Tipp geben könntest, die vielleicht noch nicht über‘s Ohr gehauen wurden, die aber Interesse haben ihr Geld anzulegen oder zu mehren, welcher wäre es?

GES: Denen würde ich total abraten.

A: Wovon genau?

GES: Irgendwo reinzufallen, um Geld anzulegen, obwohl man gar nicht weiß, ob das funktioniert. Früher haben es die Banken macht und heutzutage macht es jeder Hanswurst.

A: Also von der Anlage nicht direkt abraten, sondern von Plattformen die unbekannt sind?

GES: Genau. Das [die Banken] sowas überhaupt aus der Hand gegeben haben. Früher haben es die Banken gemacht. Klar, gab es auch Private, die das gemacht haben. Das war aber auch meistens Betrug.

A: Wir sind bei der letzten Frage. Gibt es etwas, was du diesem Gespräch noch beifügen möchtest? Anmerkungen, Kritik, etwas was dir unter den Nägeln brennt.

GES: Nein. War sehr nett.

A: Dann danke ich dir nochmal recht herzlich, dass du mir so einen Einblick gegeben hast und würde an der Stelle die Aufnahme beenden.

Ergänzung:

A: Du hast gerade gesagt, du hast mit mehreren [Personen] Kontakt gehabt?

GES: Der erste Kontakt war mit einer Frau. Das war eine Telefonnummer aus Österreich. Sie hatte einen ausländischen Akzent. Das war die Frau, die mich sozusagen auf die Plattform führen wollte mit dem Laptop, aber die hatte davon keine Ahnung. Da hat sie das weitergegeben, an den Herrn Schmidt.

A: Der hat dich dann besser betreut?

GES: Ja.

A: Wie war er drauf, klang er Deutsch?

GES: Ja, der klang Hochdeutsch. Am Anfang alles sehr nett. [Hat mich] ausgefragt, bis ich nicht mehr wollte. Dann ist er frech geworden und laut.

A: Wie hat er dich da betreut, in deinem Anlegerdasein?

GES: Er hat mir erklärt, wie das auf der Plattform abläuft und wo wir investieren können. Er hat gesagt, er [setzt] auf den fallenden Ölpreis. Ich sagte ok, wenn sie denken. Ich habe denen ja vertraut, dass da jemand [ist, der] Ahnung hat mit dem Trading [hat]. Der wollte ja auch etwas daran verdienen, also wird er nicht viel falsch machen wollen.

A: Ich habe ja das Bild [von der Plattform] gesehen, wie das aussah, mit dem riesigen Graph. Hättest du dich ohne Hilfe zurechtgefunden? Ich fand das ja schon ziemlich kompliziert.

GES: Nein, ich hätte mich da überhaupt nicht zurechtgefunden.

A: Das war auch alles nur Englisch oder konntest du das umschalten? Ich meine, nicht jeder ist des Englischen mächtig. Das ist ja dann für die nochmal ein bisschen schwerer.

GES: Das weiß ich jetzt nicht. [Ich kann es] auch nicht. Ich habe denen einfach vertraut.

A: Dann hat er gesagt dort klicken da klicken?

GES: Er hat gesagt wir [setzen] auf fallende Ölpreise. Und er hat erklärt wieso, weshalb.

A: Klang [er] professionell?

GES: [Er] klang sehr professionell, rhetorisch haben die was drauf gehabt! Die haben dir den Kopf gewaschen, das ist schon Wahnsinn. Deswegen fallen auch viele Leute darauf rein.

A: Aber das man auch darauf reinfällt und einem Wildfremden alles offenlegt ist doch eigentlich auch ein bisschen wild.

GES. Ja, das ist crazy.

A: Ansonsten würdest du nie jemanden auf der Straße treffen, der dich fragt, ob du Kinder hast, wenn ja wo die leben und wie alt die sind. Da würdest du [doch sicherlich] fragen, ob er eine Meise hat, dass sagst du ihm doch nicht?

GES: Genau, wie gesagt, zu dem Zeitpunkt war ich nicht ganz sauber im Kopf. Anders kann ich mir das nicht erklären. Ich habe daran am Anfang geglaubt.

A: Hattest du das Gefühl, wenn du mit denen telefoniert hast, dass da im Hintergrund Gemurmel ist? Teilweise wie Callcenter?

GES: Teilweise schon. Zurückrufen konnte man die Nummern aber nicht.

A: Was kam da?

GES: Man konnte die zwar anrufen, aber da ging niemand ran. Nur die konnten mich anrufen. Die haben auch sofort gemerkt, wenn ich geguckt habe, ob [der Kurs] gestiegen oder gefallen ist.

A: Die haben getrackt, wann du dich eingeloggt hast?

GES: Das haben die sofort gecheckt. Teilweise haben die dann angerufen. Zum Beispiel wo ich die 5.000,00 Euro haben wollte, [die haben] sofort angerufen.

A: Das grenzt ja schon an Überwachung. Hast du jetzt die Software immer noch auf deinem Laptop?

GES: Nein, die haben die gelöscht.

A: Auch mit Fernzugriff?

GES: Das war ja eine App, die haben die gelöscht. Die war dann weg und [ich] hatte dann keinen Zugriff mehr. Ich hatte da einen gewissen Code, den ich eingeben musste, der ging dann nicht mehr.

A: Wie auch immer das funktioniert. Davon habe ich noch nie gehört. Ich weiß, wenn ich bei meinem Telefon eine App installiere, dann muss ich die auch selber wieder deinstallieren, das also aktiv auslösen. Die war einfach von heute auf morgen weg?

GES: Ja. Wenn ich da wieder draufgehen wollte und mich anmelden wollte, ging das nicht mehr.

A: Gab es da auch eine Webseite?

GES: Ja.

A: Da kommst du aber nicht mehr rein?

GES: Nein.

Anhang 6.2: Transkript – Interview – BKF

A: Hallo und herzlich willkommen nochmal. Vielen Dank, dass Sie mir die Möglichkeit geben, einen Einblick in die Welt der Wirtschaft zu erhalten. Ich habe zehn Fragen vorbereitet und würde gleich anfangen. Bitte erzählen Sie mir von sich. Welche Funktion nehmen Sie bei Ihrer Bank ein und welche Aufgaben erfüllen Sie dort?

BKF: Ich bin Geldwäschebeauftragte in meinem Kreditinstitut und zusätzlich Abteilungsleiterin des Bereiches Compliance. Dazu gehören die Bereiche Compliance WpHG[139], Compliance MaRisk[140], Geldwäsche, strafbare Handlungen, Information, Sicherheit und Datenschutz.

A: Wie sieht ein üblicher Alltag bei Ihnen aus, wie kann ich mir das vorstellen?

BKF: Das ist schwer zu beschreiben, vor allem in meiner Funktion als Abteilungsleiterin und Führungskraft. Der [Alltag] weicht natürlich erheblich von dem der „normalen“ Mitarbeiter ab. Aber ich kann Ihnen gern ein Bild geben zu einem Mitarbeiter Geldwäsche.

A: Das wäre auch in Ordnung.

BKF: Wir haben ein Geldwäschefrüherkennungssystem, was wir mit Indizien gefüttert haben, die wir natürlich selber gestaltet haben. Die Indizien durchlaufen über Nacht unseren Kundenstamm und am nächsten Tag erkennen wir anhand der Auffälligkeiten, welche Geschäftsbeziehung so einem Indiz entspricht. Also wo man mal schauen müsste, ob da in irgendeiner Form Geldwäscheaktivitäten oder betrügerische Aktivitäten laufen.

Neben [der Bearbeitung dieser Fälle], und das macht den ganz erheblich Teil der Arbeit aus, gibt es natürlich zahlreiche Anfragen von Kollegen aus dem Haus, aus den Filialbereichen zur Legitimation der Kunden oder Auffälligkeiten auch im Zusammenhang mit der Kontoführung. Dass bspw. große Bargeldabhebungen oder Einzahlungen erfolgen. Fragen aus dem Tagesgeschäft [beantworten], wenn der Kunde direkt am Schalter steht. In dem Zuge kommen natürlich auch systemisch gesteuerte Aktivitäten [dazu], jetzt bspw. durch die Russland-Sanktionen, dass wir den Zahlungsverkehr beobachten müssen, damit keine sanktionierten Zahlungen [stattfinden].

A: Das klingt auf jeden Fall nach einem sehr guten Einstieg. Können Sie ungefähr schätzen, wie lange Sie sich schon mit dem Thema Geldwäsche beschäftigen?

BKF: Da muss ich nicht schätzen, das weiß ich ganz genau. Seit 2014.

---

[139] Wertpapierhandelsgesetz
[140] Mindestanforderungen an das Risikomanagement

A: Das ist ja dann schon eine ganze Weile.

BKF: Ich habe allerdings Kollegen, die machen das schon deutlich länger.

A: [Geldgeschäfte Geldwäsche] gibt es ja auch schon eine ganz Weile. In Ihrer Karriere, wann war das erste Mal, wo Sie mit dem Thema Cybertrading in Berührung gekommen sind?

BKF: Da sind wir jetzt an dem Punkt, ich nehme Bezug auf unser gestriges Telefonat, wo wir nochmal sortieren müssen. Also diesen Sachverhalt, den Sie schildern, dass Kunden animiert werden Geld zu sammeln, um das auf ein weiteres Konto zu transferieren, was es evtl. gar nicht in der Form gibt, da kann ich mich nicht wirklich an einen Fall erinnern. Das ist eine spezielle Ausprägung. Wir kennen hier Fälle mit Kryptowährungen, aber nicht in dieser betrügerischen Ausprägung. Die Fälle die uns auffallen, sind solche, dass Kunden für Bekannte Gelder einsammeln, um diese an einer Kryptobörse anzulegen oder es selber für sich tun. Dass aber ein betrügerischer Hintergrund besteht, solche Fälle sind mir noch nicht bekannt geworden.

A: Sicherlich ist es dann im Nachgang so, dass die Personen, die die Gelder von ihren Verwandten und Bekannten einsammeln, dann trotzdem der Geldwäsche schuldig gemacht werden, kann ich mir das so vorstellen?

BKF: Richtig. Das ist so, weil es nicht zulässig ist, dass ich Gelder einer anderen Person [oder Fremden überlasse.] Freunde sind auch völlig fremde Menschen. [Selbst, wenn sie] der Meinung sind, sie haben eine Quelle für eine Investition entdeckt. Das ist der geldwäscherechtliche Aspekt, den wir da berücksichtigen. Geldwäsche, aber kein Betrug. Wir sind noch längst nicht in der Betrugssphäre.

A: Bleiben wir beim Betrug. Ich habe auf Ihrer Webseite gesehen, dass die Bank auch auf aktuelle Betrugsstraftaten aufmerksam macht oder was es aktuell für Vorfälle gegeben hat. Inwieweit werden die Kunden gewarnt, abseits vom Internet, wenn sie sich nicht aktiv belesen?

BKF: An sich [werden sie] nicht [gewarnt]. Wenn wir z.B. aufgrund der Kontobewegungen Auffälligkeiten feststellen, dass ältere Herrschaften Gelder in Größenordnungen irgendwo hin überweisen, was keinen erkennbaren Sinn [ergibt], dann [gehen wir] im Einzelfall auf die Kunden zu. Auch dieser typische Enkeltrick, [davon] haben Sie wahrscheinlich auch schon mal gehört, der hin und wieder durch die Medien geht. Wenn wir die siebzig, achtzig Jahre alte Omi, die zigtausend Euro plötzlich Bar abheben will und auf Nachfrage zur Mittelverwendung, was ja unsere Aufgabe ist, irgendwas daher stammelt, wo man stutzig wird, dann versuchen wir die Sache zu verhindern. Auch unter Einbeziehung der Polizei. Aber das sind Einzelfälle. Die systematische Warnung vor Betrugsdelikten, das sind die Hinweise auf der Homepage. Es ist bei uns nicht die Aufgabe der Kundenberater, einfach so Kunden über Betrugskonstellationen zu informieren.

A: Das würde dann wahrscheinlich eher erfolgen, wenn der Kunde sich aktiv im Kundecenter meldet und seinen Sachverhalt schildert.

BKF: Richtig. Erstens das. [Zweitens, wenn er] allgemein fragt, ob so etwas bekannt ist. Es endet immer darin, dass er auf die [Beispiele der] Homepage verwiesen wird. Oder er muss über einen konkreten Fall sprechen, der ihn selber betrifft. Man redet ja nicht mit Kunden über pauschale Themen. Es muss einen Anlass geben, [z.B.] der Kunde sagt, [was er gemacht hat, dass ihm das komisch vorkommt und ob man die Zahlung noch stoppen kann]. Wie gesagt, dieses bewusste Geldeinsammeln im Zusammenhang mit Kryptowährungen vor betrügerischem Hintergrund, das ist mir nicht bewusst.

A: Cybertrading ist ja eigentlich ziemlich umgreifend. Es ist ja nicht nur Technik und Internet, sondern auch Geld. Geldwäsche gehört da unabdingbar dazu.

BKF: Das gab es in der Vergangenheit, mit solchen Schneeballsystemen. Das hat man auch immer wieder in der Presse gelesen. Dass Firmen Gewinnversprechen abgeben und Kunden entweder ratierlich oder auf einmal größere Geldbeträge hin überweisen, weil ihnen das Blaue vom Himmel versprochen wurde. Wobei ich auch da sagen muss, es ist mir aus den letzten Jahren kein Fall bekannt, der unser Haus betraf.

A: Das klingt doch gut.

BKF: Ja, gut für uns, für Sie vielleicht weniger.

A: Alles gut. Mir ist bewusst, dass solche Fälle wahrscheinlich eher bei Banken auftauchen, die eher weniger erreichbar sind. Eher sowas wie Onlinebanken.

BKF: Das ist ein richtiger Gedanke. In einer Bank besteht immer dieses Regionalprinzip. Wir haben eine sehr große Kundennähe. Das ist unser Geschäftsmodell. Geschäfte mit Kunden zu machen, Verträge mit Kunden abzuschließen, die wir kennen. Natürlich ist das auch manchmal mehr Wunschdenken. Man kann nicht alle Kunden kennen. Aber es ist eben doch eine ganz andere Zusammenarbeit, als mit Kunden, die nur online agieren oder wo die Kreditinstitute nur online agieren. Wo z.B. der Kunde aus Schleswig-Holstein kommt und wir in Sachsen die Bank haben, das gibt es sicher auch, aber das ist definitiv nicht unser Geschäftsmodell. Zu uns kommen die Kunden aus der Umgebung und die Kundenberater kennen ihre Kunden. Ich schließe nicht aus, dass auch wir schwarze Schafe unter unseren Kunden haben. Aber wir sind nicht das prädestinierte Geschäftsmodell für Betrüger.

A: Das ist wahrscheinlich einfach zu riskant für die [Täter]. Angenommen wir haben eine Person, die wurde betrogen und möchte eine Betrugsmeldung aufgeben. Die [Person] wendet sich entweder an das Kontaktformular auf Ihrer Webseite oder an den Kundeservice direkt. Wie funktioniert das, was passiert mit der Betrugsmeldung?

BKF. Das hängt vom Inhalt [der Meldung] ab. Bei uns gibt es eine interne Abteilung, die heißt Zahlungsverkehr. Das ist nicht mein Bereich. Dort wird die Meldung aufgenommen. Es kann sein, dass Kontosperren erforderlich sind oder Rückrufe veranlasst werden.

Man muss auch immer aufpassen. Wenn ein Kunde sagt, er ist betrogen worden, dann kann das zum einen der Fall sein, zum anderen aber kann es auch sein, dass er bereut eine Zahlung getätigt zu haben. Wir sind keine Ermittler. Wir müssen dann abwägen, [ist der Kunde betrogen worden] oder hat er bloß den Kauf bereut und will das Geld zurück? Das sind immer Sachen, wo man differenzieren muss.

Bei uns die Abteilung, die den Zahlungsverkehr überwacht, die trifft die weiteren Entscheidungen. Spielt noch ein anderes Kreditinstitut eine Rolle, kann das Geld noch zurückgeholt werden bzw. wenn wir als Haus eine Aufgabe bekommen, veranlassen wir die erst, wenn der Kunde auch eine polizeiliche Anzeige erstattet hat, um die Glaubhaftigkeit auch zu belegen.

Es gibt auch Fälle wo der eine sagt, er hat dem anderen 150,00 Euro überwiesen für einen Umzug, aber leider hat er ihm nie beim Umzug geholfen. Da weiß man dann nicht, ob der eine oder der andere die Wahrheit sagt. Das muss alles validiert sein. Ein Indiz dafür ist, wenn auch eine polizeiliche Anzeige erstattet wurde bzw. wenn es um Zahlungen geht, die vielleicht noch zurückgeholt werden können. Da gibt es natürlich auch Vereinbarungen zwischen den Kreditinstituten. Wenn die Gelder noch nicht gutgeschrieben wurden, dass es auch dann möglich ist, Gelder wieder zurück zu holen.

A: Da würde tatsächlich die nächste Frage darauf kommen. Aber ich will nochmal nachhaken. Wenn jetzt ein ganz neuer Fall, ein ganz neuer Sachverhalt kommt von einem Geschädigten und angenommen das ist validiert von der Polizei, wird dann entsprechend auch die Webseite aktualisiert oder die Kundenberater entsprechend gebrieft?

BKF: Das hängt vom Fall ab. Man muss schon sagen, dass die Fälle, die jeden Tag geschehen, häufig ähnliche Fälle sind. Es gibt hin und wieder neue Auffälligkeiten, insbesondere wenn Sachverhalte bekannt werden über neue Manipulationen. Wenn Betrüger Kunden anrufen und sagen, hier ist ein Mitarbeiter der Bank, gib mal deine PIN und TAN ein, das ist erforderlich, um die AGBs zu aktualisieren. Die [Täter] erzählen den Leuten wirklich völlig authentisch und in schöner deutscher Sprache, was sie machen sollen. [Sie] beeinflussen die Kunden am Telefon, eben unter der Vorgabe [sie seien] Bankmitarbeiter. Dann könnte es sein, dass die Masche bekannt wird.

Wir bekommen hin und wieder aktualisierte Meldungen, auch intern. Auch wir müssen das ja wissen. Da gibt es von der Organisationsabteilung eine Information: neue Masche – Kunden werden angerufen um die AGBs zu bestätigen oder Kunden werden angerufen, weil bei der Bank ein System ausgefallen ist. Da gibt es tausenderlei Varianten. Wenn da etwas Neues bekannt wird, dann kann es sein, dass diese Veröffentlichungskriterien angepasst werden.

Der erste Schritt ist ja immer Theorie. Es müssen erst Fälle bekannt werden, die unser Haus betreffen. Finanzinformatik heißt die große Firma, über die unsere ganze Technik läuft, auch die weisen uns auf Muster hin. Das bedeutet aber letztlich immer noch nicht, dass unsere Kunden tatsächlich betroffen sind. Erst wenn das eine gewisse Bedeutung hat, fließt das auf die Homepage ein und nicht jeder „kleine“ bekanntgewordene Fall. Ich glaube, die Nuancen auch zwischen den Fällen sind massiv.

A: Also muss das Phänomen erst als solches erkannt werden, bevor andere Schritte ergriffen werden können?

BKF. Auf jeden Fall. Und sie müssen auch eine gewisse Bedeutung haben. Wenn bekannt geworden ist, dass [eine Person] 100,00 Euro verloren hat, da wird sich hier nichts bewegen.

A: In Summe [wäre das] wahrscheinlich etwas anderes, wenn 50.000 Leute 100,00 Euro verlieren.

BKF. Richtig. Wenn das ein massenhaftes Phänomen ist. Es gab mal eine Zeit [in der] die CEO-Fraud-Methode [besonders häufig auftrat]. Wo Betrüger sich als unser Vorstand ausgeben, bei mir als Mitarbeiterin anrufen, [weil ich] über Konten verfügen kann und sagen Frau x, ich bin gerade in einer Konferenz, ich kann nicht mit Ihnen reden. Veranlassen sie mal, ich übertreibe bewusst, dreißig Millionen [Euro] auf das und das Konto. Das ist wichtig für den und den Abschluss. Es klingt erstmal etwas absurd, aber das muss reihenweise vorgekommen sein. Da bekommen [die Mitarbeiter] eine Mail, die sehr authentisch aussieht, wo sie dann losflitzen und denken, sie tun ihrem Chef etwas Gutes.

A: Wider besseren Wissens. Da sieht man mal wie manipulativ [die Täter sein können].

BKF: Richtig, auch Bankmitarbeiter sind gefährdet. Wir haben auch [Fälle] bei Kunden unseres Hauses. Ich weiß ganz genau, ein größerer Kunde war auch betroffen und hat viele hunderttausend Euro verloren dadurch. Das Geld ist dann weg.

A: Ich würde das tatsächlich aufgreifen [wollen]. Wenn jetzt ein Kunde Opfer von Betrug geworden ist, egal welche Masche, und er hat den Betrug angezeigt. Sie recherchieren wahrscheinlich intern, was wo hin gegangen ist. Wie stehen denn die Chancen, dass man das Geld wiederkriegt?

BKF: Gefühlt würde ich sagen sehr schlecht. Die besten Chancen stehen noch dann, wenn es auf dem Konto des Empfängerinstituts, was dann hoffentlich ein Deutsches ist, noch liegt. Ansonsten werden die Gelder in der Regel sofort ab verfügt. In dem Moment, wo das Geld vom Konto weg ist, haben [die Geschädigten] keine Chance mehr.

Das sind Formalitäten, die dann ablaufen. Wir erstatten Geldwäscheverdachtsmeldungen [und Strafanzeigen]. Natürlich hängt das vom Einzelfall ab. Aber dass die Kunden das Geld wiederbekommen, das ist eher noch im kleinteiligen Bereich möglich.

Ein Kunde hat bspw. nur ein iPhone, verkauft aber zehn über eBay. Er kassiert zehn Kaufpreise und verfügt die in der Regel gleich ab, weil er natürlich genau weiß, irgendwann schlagen die Sicherungssysteme der Kreditinstitute zu. Jetzt könnte es ja sein, dass tatsächlich noch 500,00 Euro auf dem Konto sind. [Es] ist natürlich schwierig, das Geld zu verteilen, wenn zehn Geschädigte da sind. Im Zweifel kann es auch dazu kommen, dass wir das [Geld] beim Amtsgericht hinterlegen, wenn wir nicht wissen, wem von den ganzen Geschädigten es zustehen soll.

Die richtigen Betrugsfälle, da muss man ehrlich sagen, gehen häufig über die Landesgrenzen hinaus. Da ist das Geld dann weg.

A: Da kommt man nicht mehr ran?

BKF: Nein. Vor allem nicht, wenn es Bar verfügt wurde. Vielleicht, wenn es bei einer Bank im EU-Raum noch liegt, wobei mir da kein Fall gerade präsent ist. Dann könnte es noch möglich sein, durch die SEPA [ran zu kommen. Die] EU ist ja ein relativ geschützter Raum. Es gibt viele Zahlungen, die dann in Länder gehen, die nicht mehr EU sind. In der Regel verfügen die Ganoven das Geld in Bar ab und dann ist es weg.

A: Man sieht dann quasi, [das Geld] war [auf dem Konto] drauf und ist sofort raus. Dann war’s das.

BKF. Richtig. Man sieht vielleicht noch ein Bild, ein Foto, von dem, der es abgehoben hat. Aber das ist dann irgendein Schattenmann, einer, den sie vorgeschoben haben. Man muss natürlich auch immer sagen, dass das alles von den Konstellationen abhängt. Es gibt ja auch die Konstellation, wo die Kunden ihre Bankdaten preisgeben, wo dann die Ganoven hinten rum auf dem Konto der Geschädigten [agieren]

Wir hatten Fälle, da haben die [Täter] sämtliche [Lastschriften storniert]. Wenn man Lastschriften eingerichtet hat für Strom, Gas, Daueraufträge, [und diese] storniert, [dann] staut sich wieder ein Guthaben auf dem Konto auf. Sämtliche Wertpapiere, die auf dem Konto waren, alles verkauft, um den Betrag, der auf dem Konto ist, weg zu verfügen. Das überweisen die dann, ich nenne lieber keine Länder, woanders hin und dann ist es weg.

A: Das ist ja dann Kreditkartenmissbrauch?

BKF: Nein. Die [Geschädigten] merken [den Betrug] gar nicht. Sie gehen über eine Verlinkung scheinbar auf die Homepage der Bank, loggen sich dort ein und in Wirklichkeit sind sie längst bei dem Ganoven zu Hause und der guckt mit auf das Konto.

A: Also Phishing. Da sind die Täter auch immer gewieft.

BKF: Das bedeutet eben, dass [der] Kunde einen Fehler gemacht hat, auch wenn [er sich] nicht daran erinnern kann.

A: Man sieht das ja teilweise nicht, die Phishingseiten sind so gut gemacht.

BKF: Richtig. Man denkt, man ist in der Bankwelt. Es ist dasselbe wie der Bankmitarbeiter am Telefon, der mich veranlasst, eine PIN oder TAN rauszugeben.

A: Ich würde mal weitermachen und zwar würde ich nochmal zur Geldwäsche zurückkommen wollen. Welche Faktoren bedarf es, damit ein Kundenkonto den Verdacht der Geldwäsche erregt?

BKF: Eine Vortat zur Geldwäsche, da können Sie sich § 261 StGB in Ruhe zu Gemüte führen. Das ist eine Vielzahl von Handlungen. Betrugsdelikte, Diebstahlsdelikte, Steuerhinterziehung, also ganz viele vermögensrelevante Delikte. Auch wenn ein Kunde unseres Hauses sich am unerlaubten Glücksspiel [beteiligt und] daraus einen sogenannten Tatertrag erzielt, ist das eine Vortat zur Geldwäsche und wir müssen eine Verdachtsmeldung erstatten.

Unsere [Kriterien] in unserem Geldwäschefrüherkennungssystem sind so gestaltet, dass wir sowas erkennen. Oder bleiben wir beim Betrug, es kommen Anzeigen von mehreren Kunden, die Gelder überwiesen haben und auf ihr [bei eBay erworbenes] Handy warten. Das reicht natürlich dann auch [für einen Verdacht]. Das ist außerhalb des Systems, das sind Hinweise von Kunden, die zu einer Verdachtsmeldung führen.

[In] unserem Früherkennungssystem sind [Kriterien] hinterlegt. Die Fälle, die jeden Tag angezeigt werden und das sind viele, die werden einzeln analysiert, angeschaut und abgewogen. Geht das mit rechten Dingen zu oder gibt es dafür eine Begründung, dass plötzlich eine Bareinzahlung von 300.000,00 Euro erfolgte oder größere Transaktionen ins Ausland oder hat das ein G'schmäckle. Wenn es ein G'schmäckle hat, wird Geldwäscheverdachtsmeldung erstattet.

A: Das klingt jetzt so, als würden tatsächlich aktiv Menschen dahinter sitzen und kein Algorithmus, habe ich das richtig verstanden?

BKF: Der Algorithmus arbeitet in dem Moment, wo die [Kriterien] unseren Kundenstamm abgleichen. Wir haben feste Kriterien hinterlegt. Wenn ein [Kriterium] bspw. heißt, zeige mir Kunden an mit Staatsangehörigkeit Nicht-Deutsch, bei denen 100.000,00 Euro aufs Konto gehen, dann macht das das System alleine. Trotzdem sitzt am nächsten Tag ein Mensch davor, der sich das anschaut. Das kann ja ein [Geschäftsmann] sein, der ausländische Kunden hat oder es kann eine Notiz in unserem System existieren, wo drin steht, der Kunde hat gestern sein Haus oder ein teures Auto verkauft. Es muss dann dafür eine Erklärung ran. Entweder kann man die schon aus der Technik sehen, also aus den Kundenbeziehungen, die hier geführt werden und den Notizen dazu oder der Kundenberater kann vielleicht eine Aussage treffen. [Hinter dem System] steht ein Mensch, der sagt, es gibt eine Verdachtsmeldung oder es gibt keine. Es ist plausibel oder es ist nicht plausibel.

A: Das wusste ich tatsächlich so noch nicht. Ich bin davon ausgegangen, dass es hauptsächlich alles der Algorithmus macht. Wieder was gelernt.

BKF: Der Algorithmus bietet die Fälle an, aber nicht die Entscheidung.

A: Dann darf nicht alles die Technik machen, man sich noch ein bisschen auf den menschlichen Kopf verlassen können. Ich würde kurz nochmal einen Sprung wagen und Sie fragen, wie Sie zu den Kryptowährungen stehen und ob Sie darin eher ein Potenzial oder eine Gefahr sehen für den Anleger?

BKF: Wir als Bank unterstützten das ja nicht. Es ist bei uns kein angebotenes Produkt. Für welche, die sich fachlich, technisch damit auskennen, warum nicht? Das ist eine persönliche Meinung. Ich selber kenne mich zu wenig in dem Bereich aus.

Ich glaube, die Gefahr besteht darin, dass Kunden sich nicht wirklich damit auskennen, wie das Produkt läuft, wie hoch die Wertschwankungen da sein können und sich einfach von den Renditeerwartungen hinreißen lassen. Sie denken, sie geben jemandem 100,00 Euro und er macht daraus 1.000,00 Euro, das hört sich erstmal schön an. Dass das ganz schnell nur 50,00 Euro sein können, ob das [dem Kunden] immer so bewusst ist?

Das Schwierige ist, glaube ich, man muss immer Chancen und Risiken kennen. Das ist im weiteren Sinne vergleichbar mit dem Wertpapiergeschäft. Wobei das Wertpapiergeschäft durch reguliert ist. Eine seriöse Bank in Deutschland klärt die Kunden auf. Natürlich beschweren sich die Kunden, dass im Augenblick die Kurse trotzdem alle runter gesaust sind, aber ein aufgeklärter Kunde weiß, dass durch politische Themen, durch Finanzkrisen so etwas passieren kann.

Bei Kryptowährungen bin ich mir nicht ganz sicher. Ich würde sagen, da hält sich die Aufklärung in sehr engen Grenzen. Ich muss Ihnen sagen, das kann ich nicht in aller Gänze beurteilen. Möglicherweise gibt es auch seriöse Anbieter. Aber das Bild, was wir hier gelegentlich sehen, [ist, dass bspw.] der Müller das Geld von seinen Freunden auf dem Campingplatz einsammelt. Da kann ich mir nicht direkt vorstellen, dass der Müller aufklärt, dass die Kurse auch in den Keller gehen können und zwar gewaltig. Da sehe ich eher die Gefahr. Wenn das professionelle Berater machen oder [Personen], Profis, die dann Wissen für sich haben und die Kunden vollumfassend aufklären [wäre es eine andere Sache]. Aber ich befürchte, dass das nicht der Fall ist, [deshalb] sehe ich das skeptisch. [Die Anlage in Kryptowährungen] ist aber nicht verboten.

A: Wie Sie es richtig gesagt haben, Kryptowährungen werden „noch nicht richtig“ reguliert oder nicht ausreichend reguliert. Ich habe ja schon Einblicke von Geschädigten gehabt, die sagten, das waren kleine Plattformen [von denen sie betrogen wurden]. Aus der Werbung, im Fernsehen kennt man eToro o.ä., die sind relativ groß, die sind bekannt. Da ist auch ein größeres Vertrauen in eine große Plattform als in kleine, von denen man noch nie gehört hat. Ich habe die Geschädigten gefragt, warum sie nicht aktiv recherchiert haben. Da kam die Aussage, dass ihnen das erst danach eingefallen ist.

BKF: In dem Moment, wo man liest 10% Rendite oder 50% Rendite, da schaltet bei dem ein oder anderen Menschen der Kopf aus bzw. der Menschenverstand.

A: Es klingt einfach zu gut, um wahr zu sein. Da müsste man eigentlich drauf kommen. Nächste Frage: Wo sehen Sie Schwierigkeiten bei der Bearbeitung von Betrugsfällen? Was können Sie oder Dritte dagegen tun?

BKF: Man sagt immer so schön, die Betrüger sind uns immer einen Schritt voraus. Wir rennen immer nur hinterher aufgrund uns bekannt gewordener Szenarien. Jemand, der wirklich kriminelles Blut hat, ein Betrüger sozusagen, Banden, wer dieses Potenzial hat, dem sind wir nicht gewachsen.

Wir versuchen aus den Sachen, die uns bekannt geworden sind, natürlich Maßnahmen abzuleiten, sodass die Kunden geschützt werden. Letztlich ist das immer nur ein Reagieren in ganz vielen Fällen. Dann kommt die nächste Masche, es fällt wieder jemand darauf rein und dann reagieren wir. Ich wüsste nicht wirklich [was man gegen] Betrug [noch machen kann], weil das so individuell ist. Geldwäscheszenarien kann man konstruieren, aber betrügerische Handlungen, da fällt mir gar nichts ein, was man noch machen kann.

Die, die betrügen wollen, haben sowohl das technische Potenzial, als auch das geistige und die Ideen. Wir haben viele Menschen, die darauf reinfallen. Wir können immer nur reagieren und unsere Kunden schulen und sensibilisieren. Aber es bleibt dabei, es wird immer ein Schritt hinterher sein.

A: Ich wollte gerade sagen, Sie können reagieren und aus dieser Erfahrung können Sie gewisse Präventionsmaßnahmen einleiten, indem Sie die Kunden auf der Webseite informieren. Aber das entstand ja auch bloß aus einer Reaktion heraus. Künftige [Personen] könnten dadurch nicht mehr geschädigt werden.

BKF: Nichts zu tun ist keine Option. Selbst eine Schulung oder eine Information auf der Homepage [kann vorbeugen]. Wir haben ja technische Sicherungsmittel, da noch an Stellschrauben zu drehen, das gehört natürlich dazu. Neue Maschen müssen erstmal bekannt werden.

A: Das ist dann Aufgabe der Polizei wahrscheinlich, darüber zu informieren.

BKF: Wenn es uns bekannt wird, versuchen wir auch zu reagieren. Dann ist meist schon ein Schaden entstanden.

A: Bevor es bei Ihnen bekannt wird, muss ja erstmal eine Anzeige erstattet werden…

BKF: Nein, nicht davor. Wenn einem Kunde 100.000,00 Euro vom Konto fehlen, das merkt er hoffentlich schnell. Er würde [vermutlich] als erstes bei uns anrufen und den Sachverhalt schildern. Erst dann [verweisen wir ihn an die] Polizei. Wir erfahren das schon recht schnell. Dann werden nach und nach die Hintergründe und Zusammenhänge [aufgedeckt]. Was ist überhaupt passiert, hat der Kunde Daten preisgegeben, war es ein Phishing-Fall, hat er selber agiert, hat der Bankmitarbeiter angerufen? Wir erfahren schon zeitig davon. Eben wenn es der Kunde bemerkt.

A: Ja, wenn. Gehen wir zur nächsten Frage, zur vorletzten Frage. Welchen Tipp können Sie Anlegern geben, wenn es um das Investieren von und Handeln mit Geldwerten geht? Wenn ein Kunde die Möglichkeit oder die Wahl hat, online zu investieren oder zur Bank zu gehen.

BKF: Wir reden jetzt wieder über Kryptowerte?

A: Nicht zwingend. Cybertrading funktioniert ja auch ohne Krypto. Angenommen es hat ein Kunde 100.000,00 Euro und möchte die anlegen, um das Geld zu vermehren. Dann kann er ja entweder zur Börse gehen oder mit Aktien handeln oder mit Wertpapieren.

BKF: Wertpapiere wären mir in den Kopf gekommen. Es gibt auch diesen Weltzins, wo Kunden Gelder hin zahlen können und bestmögliche Renditen angeboten werden. Ich sage immer, das funktioniert wie Trivago. Eine Plattform, die von allen möglichen Kreditinstituten die Konditionen hinterlegt. Dann wird den Kunden das aktuell günstigste Angebot unterbreitet.

Mir fällt nichts anderes ein, als dass ich mich umfassend über den Anbieter informiere und Kundenmeinungen lese, schaue, ob das ein reguliertes Unternehmen ist. Ob es auch in Deutschland sitzt oder der EU zumindest. Es gibt Länder, die sollten da nicht vorkommen. Ich wüsste kein anderes Mittel.

Ich als Privatperson, würde so loslaufen. Ich würde aber, glaube ich, bei meiner eigenen Bank fragen, ob das eine gute Idee ist. Klar, es wird für Kunden immer eine Rolle spielen, wo sie das Meiste für ihr Geld kriegen können. Wenn es halt nicht die Bank ist, sondern der Weltzins bspw., dann ist das so. Dann liegt es in der Verantwortung des Kunden, die Einlagensicherung anzuschauen und was passiert, wenn der Schuss für ihn nach hinten losgeht. Das muss ihm bewusst sein. Auch, ob er sein ganzes liquides Vermögen da rein steckt.

Es gibt auch Kunden, die sagen, 500,00 Euro im Monat kann ich verzocken, egal was damit passiert. Es muss eine bewusste Entscheidung sein. Ich kann da nicht global was sagen. Ich weiß nicht, was sie da hören wollen.

A: Die Frage ist tatsächlich sehr gut beantwortet. Das war dann auch fast die letzte Frage. Der Schluss ist ganz einfach: ob Sie noch etwas haben, was Sie loswerden möchten, was Sie beifügen möchten?

BKF: Dass es nicht mehr so viele Geldwäsche-Sachverhalte gibt und wir weniger Arbeit haben. Das ist schon sehr massiv, die Auffälligkeiten die es da gibt. Da sind wir jetzt bei Wünsch-Dir-Was. Den Wunsch können Sie mir nicht erfüllen, das weiß ich schon. Und was noch?

A: Das war die letzte Frage.

BKF: Ach so. Ich hoffe, Sie konnten aus meinen Antworten etwas für sich herausnehmen. Es ist natürlich immer alles eine weiche Geschichte. Ich glaube, Sie haben jetzt die große Herausforderung das zu sortieren, inwieweit es Ihnen helfen kann.

A: Ich bin mir eigentlich ziemlich sicher, dass mir das Gespräch heute sehr gut helfen wird. Es muss ja irgendjemand mal den Anfang machen. Irgendjemand muss sich damit beschäftigen, ein bisschen überall mal rein zu greifen und zu gucken. Wer weiß, vielleicht gibt es in drei Jahren jemanden, der sagt, er führt das fort. Ich werde schon etwas [aus unserem Gespräch] zaubern. Ich würde noch kurz Ihre Zustimmung holen, dass ich die Aufnahme jetzt beende?

BKF: Ja, ist in Ordnung.

Anhang 6.3: Transkript – Interview – E

A: Hallo nochmal. Herzlichen Dank für Ihre Teilnahme.

E: Sehr gerne.

A: Ich frage gleich vorab, ist es in Ordnung, dass ich du sage, da wir uns nun schon eine gewisse Zeit kennen?

E: Ja, ich bitte darum.

A: Gut. Erzähl' mir bitte von dir selbst. Welche Funktion nimmst du bei den Ermittlungen ein und welche Aufgaben erfüllst du dabei?

E: Ich bin Ermittler in dem Bereich, das heißt, ich arbeite im Auftrag der Staatsanwaltschaft und fange ganz am Anfang an, diese Sachverhalte zu bearbeiten. Es geht los bei den Zeugenvernehmungen. Die Geschädigten werden vernommen, es werden von ihnen die Daten erhoben, die Daten werden ausgewertet von mir und ich führe dann die notwendigen Erstmaßnahmen durch. Ich ermittle bei den Banken nach den Konten, ich ermittle den IT- Dienstleister nach möglichen IP-Adressen oder Accounts, die von Interesse sind. Die ganzen Ermittlungen oder Ergebnisse führe ich zusammen und bereite sie in einem aussagekräftigen Ermittlungsbericht für die Staatsanwaltschaft auf oder vor, um z.B. Beschlüsse beantragen zu können und weitere Maßnahmen zu bekommen wie Durchsuchungsbeschlüsse oder Sicherstellungs-/Beschlagnahmebeschlüsse bei IT-Dienstleistern. Dann werden diese auch durch mich ausgewertet, um den Beschuldigten zu ermitteln bzw. die Tätergruppierung.

A: Das klingt doch nach einem sehr guten Einstieg. Das klingt vor allem auch nach ziemlich vielen Aufgaben, die du da erfüllst. Wie lange beschäftigst du dich jetzt schon mit dem Fall Cybertrading oder mit dem Straftatphänomen?

E: Also mit dem Phänomen an sich würde ich sagen seit Ende 2019, Anfang 2020. Die ersten Fälle sind mir November, Dezember 2019 untergekommen, da wusste ich tatsächlich noch gar nicht, was das ist. Da habe ich auch gedacht, dass sind Betrüger die einfach [eine Aktion] starten, Daten abfragen oder Bitcoins von den Leuten haben wollen. Da habe ich noch gar nicht erkannt, dass das wirklich ein Phänomen darstellt. Das kam erst Anfang 2020, wo die Verfahren immer mehr wurden, wo man gemerkt hat, da ist doch ein bisschen mehr dran als irgendeine Phishing-Mail. Da wurde es dann erst deutlich für mich, dass es ein Phänomen ist.

A: Also ist es auch noch gar nicht so alt. Das sind ja jetzt maximal zwei Jahre.

E: Genau.

A: Wenn du dir jetzt einen Fall vorstellst, ganz beispielhaft, wie läuft das ab? Du hast vorhin erzählt, was deine Aufgaben sind. In einer ungefähren Reihenfolge: Was ist passiert, was macht ihr, wie sieht so ein Fall aus, den ihr bearbeitet?

E: Meinst du das jetzt aus der Sicht, wie das Cybertrading tatsächlich abläuft oder wie das aus Sicht des Geschädigten abläuft, was passiert oder was ich mache?

A: Aus deiner Sicht. Du kriegst die Akte auf den Tisch und was ist dann?

E: Wie ich da vorgehe?

A: Genau, wie sieht der Fall aus, wie sehen deine Arbeitsschritte aus?

E: Als erstes habe ich mehr oder weniger eine Matrix im Kopf, was ich erwarte an Informationen, was ich benötige an Informationen, um meine Ermittlungen zu führen und danach bereite ich die Akte auf. Ich mache ein Aktenstudium, lese die Anzeige, lese die Erstvernehmung, werte die ersten Daten aus, die die Geschädigten geliefert haben. Danach entscheide ich: das reicht mir, die Ermittlungen zu führen oder ich sehe das reicht bei weitem noch nicht. Dann muss ich den Geschädigten nachvernehmen bzw. muss noch weitere Daten anfordern.

In 95% der Fälle ist es so, dass man nochmal mit den Geschädigten Kontakt aufnehmen muss und nochmal Daten nachfordern, um die notwendigen Ermittlungen führen zu können. Das geht eigentlich so los, dass ich schaue, hab ich schon Informationen zu der Plattform, zu der URL, wo der Geschädigte investiert hat oder habe ich noch keine Informationen darüber? Ist diese Plattform bzw. die Domain noch online oder ist sie bereits offline? Das entscheidet darüber, welche weiteren Maßnahmen da zu machen sind, ob der Server zu beschlagnahmen ist oder zumindest anzuregen ist zur Beschlagnahme.

Da spielt natürlich auch der Schaden eine gewisse Rolle. Wenn keiner investiert hat, sondern es war bloß ein Versuch, also [der Geschädigte] hat bloß die Anfrage gekriegt, hat nichts investiert, dann ist es fraglich, ob man wirklich die Beschlagnahme letztendlich kriegt, bestätigt vom Richter.

Ansonsten schaue ich zum einen die technische Schiene an. Ist diese Plattform noch online, welche Kommunikation hat mit dem Geschädigten stattgefunden? Sprich, hat es Zugriffe auf den Rechner mit einer Remotesoftware gegeben, habe ich die Logdaten von der Remotesoftware? Dann schaue ich mir noch die E-Mail-Header an, wenn der Betrüger Kontakt hatte. Dann schaue ich mir die Transaktionen an. Hat der Geschädigte auf richtige IBAN-Konten überwiesen im In- oder im Ausland? Muss ich da noch irgendwelche Maßnahmen machen?

Im Inland ist es ja relativ einfach. Da kann man über die BaFin eine Abfrage machen, ob ich da Daten von dem Konto bekomme. Im Ausland muss man die FIU oder über die poli-

zeilichen Informationssysteme schauen, ob es irgendwelche Informationen gibt oder man da Informationen bekommt.

Dann gibt es das Ganze noch mit der Investition direkt in die Kryptowährung. Das heißt, der Geschädigte hat ein eigenes Konto bei einem Exchanger und hat die Transaktionen selber ausgeführt bzw. unter Anleitung von den Tätern. Dann schaue ich mir die Transaktionsdaten an und versuche nachzuvollziehen, auf welches Konto oder welche Wallet sind die Bitcoins hingewandert. Das mache ich entweder, wenn es einfach nachzuvollziehen ist, händisch über einen frei verfügbaren Blockchain-Dienstleister oder ich lasse eine Auswertung machen über das LKA.

A: Weil du gerade gesagt hast „Ermittlungen beim Versuch bzw. beim Vollstrecken der Tat“: Gibt es da einen Unterschied zwischen Ermittlungen die bei einem Versuch, also wenn der Geschädigte nicht investiert hat? Er ist ja dann nicht geschädigt, er erstattet Anzeige, er ist dann der Anzeigenerstatter. Wenn er merkt, [der Täter] hat [den Betrug] versucht, [der Geschädigte hat] aber nicht investiert, [er ist] quasi dran vorbei gekommen oder er hat eben investiert, unterscheidet sich das in den Ermittlungen?

E: Also prinzipiell sind das die gleichen Ermittlungen. Einen wirklichen Unterschied gibt es da nicht. Ich muss es genauso der Staatsanwaltschaft vorlegen und ich darf selbst nicht entscheiden, ob überhaupt ein Versuch vorliegt. Ich erkenne, dass es ein Versuch ist. Aber die weiteren Ermittlungsmaßnahmen muss dann letztendlich trotzdem die Staatsanwaltschaft entscheiden. Ob sie das Verfahren einstellen wegen z.B. einer Geringfügigkeit. Das darf ich selber nicht machen.

A: Angenommen der Geschädigte will das alles nicht am Telefon erzählen oder es ist so komplex, dass man sagt, der muss unbedingt hier herkommen. Wie gehst du mit den Geschädigten um, welchen Eindruck erwecken die Personen, wenn sie hier sitzen und dir das alles schildern?

E: Es gibt mehrere Ebenen. Es gibt die einen, die sind völlig pikiert, dass denen das überhaupt passiert ist. Es ist ihnen peinlich darüber zu reden, weil sie ganz viel Geld investiert haben. Sie haben eigentlich gedacht, sie haben es unter Kontrolle, mehr oder weniger. Tatsächlich bemerken sie dann, dass sie von vorn bis hinten nur betrogen worden sind. Dass alles, was ihnen erzählt worden ist, erlogen ist.

Ganz oft ist es so, dass die Broker auch Einblick in das Familienleben erhalten haben, dass die Täter Infos über Wünsche usw. abgefragt haben und dass sie damit arbeiten. Die [Täter] wissen viel über die Familie und ob [die Geschädigten] Kinder haben. Es ist [den Geschädigten] dann äußerst unangenehm, dass sie auf sowas reingefallen sind.

Dann gibt es die, die dagegen wettern, dass [so ein Betrug] überhaupt möglich ist. Die meisten haben es einfach gar nicht verstanden, was da tatsächlich passiert ist. Denen muss man das komplett erklären, weil sie nach wie vor, selbst wenn sie bei der Polizei auf dem Revier die Anzeige gemacht haben, das nicht verstanden haben. Man muss sie wirk-

lich darauf hinweisen, dass es nicht nur diese eine Masche gibt, sondern dass es immer wieder zu Anschlussstraftaten kommen kann und wie sie sich dagegen schützen müssen oder wehren müssen. Dass man neben diesen ganzen Informationen abfischen im Rahmen der Vernehmung auch ganz viel Präventionsarbeit für Straftaten [leistet], die vielleicht dort passieren könnten, [das ist meine Aufgabe].

A: Also als Schutzmaßnahme schon. So nach dem Motto „es könnte sein, dass…"

E: … weitere Anrufe kommen, genau. Dass jemand sagt, wir haben ganz viel Geld sichergestellt. Sowas passiert immer wieder und da muss man die Leute wirklich darauf hinweisen, sonst machen sie das. Weil sie das nicht glauben, dass das auch wieder ein Betrug ist.

A: Gibt es eine Art Struktur oder ein Muster seitens der Betrüger oder der Tatverdächtigen, welches dir bei den Ermittlungen aufgefallen ist? Du sagst, die [Täter] haben viel Einblick ins Familienleben, das heißt ja, irgendwie müssen sie an die Informationen kommen.

E: Ja genau, die Täter haben eigentlich eine ganz gute Position. Die meisten Geschädigten basieren nicht auf einer Kaltakquise. Sie haben sich aktiv auf eine Werbung im Internet hin gemeldet und haben ihre Personalien und ihre Kontaktadressen hinterlassen. [Sie haben] Interesse in Bitcoin zu investieren bzw. dass sie darüber gelesen haben und deswegen Interesse haben mehr darüber zu erfahren.

Das heißt, die Täter wissen, die Leute erwarten einen Anruf und wollen auch investieren, die muss ich nur noch [überreden], das tatsächlich zu machen. Die [Geschädigten] haben ein gewisses Interesse, sie haben Geld, was sie irgendwo investieren wollen. [Die Täter] haben diese gute Position, dass sie auf [die Geschädigten] zugehen können und schon ein bisschen Vorlauf haben. Ich glaub das ist ein ganz wichtiger Aspekt, weil die [Täter] den [Geschädigten] natürlich sagen können, wir haben das und das Modell und wir können mit 250,00 Euro anfangen. [Das ist] der Klassiker und das machen die [Geschädigten] auch meistens.

Dann wird den [Geschädigten] gezeigt wie sie 250,00 Euro innerhalb von, ich spinne jetzt mal, ein, zwei, drei Tagen entwickelt haben und dass das super gelaufen ist. [Doch sie sagen auch, dass] man das wirkliche Geld nur damit macht, wenn man ganz viel investiert. Also wenn man hoch reingeht mit 10.000,00 Euro oder 15.000,00 Euro. Je mehr, desto besser [ist] die Gewinnmarge. Dann werden die Leute ganz stark bombardiert mit Anrufen, dass es jetzt wahnsinnige Wertsteigerung gab und sie jetzt unbedingt einsteigen müssen. Es wird ein psychologischer Druck aufgebaut, Geld zu investieren.

Viele Leute, die fallen einfach darauf rein und die gehen davon aus, [der Broker] ist wirklich jemand, der investiert, der auch sein Know-How da rein bringt, der Interesse hat, dass die [Geschädigten] einen Gewinn machen. Den Geschädigten wird sehr oft gesagt, dass die Broker da auch einen bestimmten Prozentsatz von dem Umsatz bekommen. Deswe-

gen denken [die Geschädigten], die [Täter] haben auch ein Interesse dran, dass [sie] viel Umsatz machen. Dass das Geld in dem Moment, wo sie die Überweisung machen, eigentlich schon weg ist, das wissen sie nicht und davon gehen sie auch nicht aus. Dann wird ihnen das in diesem fiktiven Trading-Programm oder Trading-Verlauf dargestellt, wie der Kurs sich entwickelt. Der ist natürlich immer positiv am Anfang, denn die Broker wollen die Geschädigten dazu bringen, nochmal zu investieren.

Sobald, und das passiert ganz oft, [die Geschädigten] eine Auszahlung wollen, [heißt es], dass nur ein kleiner Betrag ausgezahlt werden kann. [So nach dem Motto], wir können einen kleinen [Betrag] ausbezahlen aber mehr geht erstmal nicht, sie müssten dann nochmal investieren. Und wenn die Geschädigten viel ausgezahlt haben wollen oder das Konto auflösen wollen, dann ist entweder innerhalb kürzester Zeit ein Kursverlust eingetreten oder es müssen fiktive Steuern und Zollgebühren bezahlt werden. Wenn das bezahlt ist, dann wird ausgezahlt. Aber es ist auch bloß eine Masche um noch mehr Geld von den Geschädigten zu bekommen. Die wissen ja dann angeblich, dass sie aus ihren 10.000,00 Euro 40.000,00 Euro gemacht haben und sind natürlich bereit, dafür ein paar Prozente an Zinsen oder Steuern zu bezahlen. Das ist halt nochmal on-top für die Täter sozusagen.

A: Die [Täter] machen bestimmt auch gut Geld damit. Also ist es von vornherein ein abgekartetes Spiel und das ziehen sie einfach mit hunderten, tausenden Menschen ab und alle springen drauf an. Dann zieht sich das wie ein roter Faden durch jede Plattform, durch jede Tätergruppierung.

E: Genau. Was die Täter wirklich machen, das haben wir in den Ermittlungsverfahren mitbekommen, sie führen eine Datenbank, wo sie sämtliche Informationen von den Telefongesprächen erfassen. Sie schreiben sich alles auf: wer die [Geschädigten] sind, wo sie arbeiten, wie viele Kinder, was sie für Wünsche, was sie für Träume haben, was sie mit dem Geld machen wollen. Das wird natürlich jedem Broker, der sich weiter mit dem [Geschädigten] beschäftigt, zur Verfügung gestellt. Das heißt, [die Täter] können sich sofort darauf einstellen, was das für ein Mensch [der Geschädigte] ist, wie er tickt. Braucht er Druck, braucht er gutes Zusprechen um ihn mürbe zu machen, mehr zu investieren.

Die [Täter] haben ein psychologisches Screening und betreiben die [Datenbank] von den Geschädigten. Je nach dem werden die [Geschädigten], wenn sie „angebissen“ haben, wenn sie ein paar hundert, ein paar tausend Euro investiert haben, zu den nächsten Brokern weitergegeben. Die sind nicht mehr die einfachen Broker, sondern speziell geschulten Leute, die den [Geschädigten] richtig bearbeiten um das Maximale rauszuholen.

A: Angenommen man hat jetzt die Ermittlungen schon ziemlich weit getrieben und man hat hier und da einen Lichtblick. Wie lange dauert das im Schnitt, so einen Sachverhalt zu klären? Es gibt bestimmt Ermittlungen, die dauern eine ganze Weile, andere gehen schneller.

E: Das ist eine gute Frage. Ich denke, um das wirklich zu klären, vergehen mehrere Jahre. Wenn man wirklich die Beschuldigten, die vielleicht im Ausland sitzen, zur Anklage bringen [will]. Wenn es schnell geht eins, zwei Jahre, ansonsten länger.

A: Wie gut stehen denn dann die Chancen, dass man den Täter auch tatsächlich zu fassen kriegt? Vielleicht in Prozent angeben oder basierend auf deinen Ermittlungen, die du bisher geführt hast.

E: Das ist echt schwer. Also wirklich effektiv habe ich bis jetzt null.

A: Keine gute Quote.

E: Nein, keine gute Quote. Ich weiß ganz viel, wer für bestimmte Sachen in Frage kommt, aber oft sind es Decknamen. Die [Täter] werden als bekannt geführt. Zum Beispiel ein Broker, der gibt sich als eine Mary aus und dann wird das als bekanntes Verfahren gegen die Mary xy geführt. [Obwohl] wir eigentlich wissen, dass ist nicht die Mary xy, sondern da steht eine Gruppierung dahinter und ein anderer Broker, der ganz anders heißt.

Deswegen heißt es noch lange nicht, dass man das Verfahren geklärt hat, bloß weil man einen Täter bekannt gemacht hat. [Das] ist nicht ganz so einfach zu beantworten. Ich kann die Verfahren bekannt machen, [bspw. ermittle] ich eine IP-Adresse, weil die zu dem Mann oder der Frau oder der Firma in Albanien, Georgien, Serbien oder in Deutschland [gehört]. Das heißt aber noch lange nicht, dass ich den verantwortlich dafür machen kann, das ist immer das Problem. Denn das komplett nachweisen zu können und [die Person] strafrechtlich zur Verantwortung ziehen zu können als den Betrüger oder den der dem Betrüger Hilfe geleistet hat, [das ist sehr schwer].

A: Also kann man als Schwierigkeit bei den Ermittlungen auch einfach sagen, dass diese Pseudonyme, die genutzt werden, am Ende sämtliche Klarpersonalien völlig verschleiern. Die geben bestimmt auch nicht genug preis, dass man da auf eine echte Personalie schließen könnte.

E: Das ist richtig. Sie geben logischerweise nicht ihre Klarpersonalien an. Wenn sie mit den Geschädigten reden, ist alles nur fiktiv ausgedacht. [Sie] nehmen immer wieder die gleichen Decknamen, dass denke ich schon. Zumindest in den Gruppierungen haben sie gleiche Namen. Bei Ermittlungen, wenn man die tief genug führt, findet man auch die Hinweise, wer wirklich hinter welchem Decknamen steht. Also welche reelle Person da dahinter steht. Die Frage ist aber, ob man die zur Verantwortung ziehen kann, weil man die erst lokalisieren muss. Dann muss man die entsprechenden Beschlüsse bekommen und man muss sehen, ob es im Inland oder im Ausland ist. Je nach dem entstehen neue Schwierigkeiten in den Ermittlungsverfahren, die man erstmal zur Seite schaffen muss.

A: Es liegen auf dem Weg der Ermittlungen so viele Steine im Weg, dass ihr die erstmal alle beiseiteschaffen müsst. Und wenn ihr dann einen beiseite geschafft habt, kommt der nächste Stein zum Vorschein.

E: Genau, so in der Art ist das.

A: Na gut, das erklärt dann auch, warum das dann so lange dauert.

E: Richtig, weil die meisten Täter/Tätergruppierungen sind nicht in Deutschland, sondern sitzen im Ausland. [Dabei ist] erstmal egal ob in Portugal, Spanien oder in Albanien, Nord Mazedonien oder Israel. Je nach dem in welchem Land das ist, gibt es unterschiedliche Rechtshilfeabkommen bzw. kann man unterschiedlich mit denen kommunizieren. Demnach ist es auch im einen oder anderen Land einfacher oder schwieriger Ermittlungserkenntnisse zu bekommen.

Innerhalb von Deutschland ist es kein Problem wenn es [darum geht], Informationen von Behörden zu bekommen. Innerhalb der EU mag das auch noch gehen. Wenn man jetzt ein Land hat, was auch sehr kooperativ ist, dann kriegt man vielleicht auch relativ schnell Informationen von Behörden.

Wenn es außerhalb von der EU ist, muss man dann teilweise diplomatische Wege einhalten. Da geht ein Ersuchen die Tippel-Tappel-Tour von der Polizei zum Staatsanwalt, zum Gericht, vom Gericht wieder zum Staatsanwalt, zum Bundesministerium für Justiz oder sächsischen Bundesministerium für Justiz, dann zu einem Botschafter, vom Botschafter über den Botschaftsweg zum ausländischen Botschafter und dann geht das wieder die Tippel-Tappel-Tour bis zum eigentlichen Ermittler im Ausland, der dann das Ersuchen beantwortet. Dann geht das die Tippel-Tappel-Tour wieder zurück. Deswegen dauern manche Ersuchen Monate.

A: Wenn du jetzt einschätzen müsstest, wie man die Ermittlungen intern und extern unterstützen könnte, was hättest du für Wünsche oder Anregungen?

E: Wünsche hätte ich viele. Das Genialste wäre, dass, wenn man bestimmte Informationen hat, diese einfach abfragen kann wie in Deutschland. Dass ich sozusagen eine Ansprechstelle habe im Ausland, denen meine Informationen schicke und dass ich innerhalb von kürzester Zeit die Erkenntnisse bekomme. Also z.B. habe ich eine Call-Center-IP-Adresse, das ist meinetwegen in Albanien. Ich schicke die IP-Adresse mit einem Ersuchen nach Albanien und bekomme innerhalb von zehn Tagen das Callcenter lokalisiert, habe einen physikalischen Anschluss. Dann kann ich meine Ermittlungen darauf fokussieren, schreibe ich den [Behörden] zurück und die machen ein Parallelverfahren. [Die ausländischen Behörden] durchsuchen dort und ich bekomme die Ergebnisse von der Durchsuchung. Sie haben dann die Leute, denen sie die Tat nachweisen können. Das wäre absolut super, aber so funktioniert [das] leider nicht, weil diese diplomatischen Wege einzuhalten sind. Es gibt Landesgrenzen und es gibt Grenzen im Bürgerrecht und die müssen eingehalten werden.

A: Dann hat es nicht einmal was mit dem bürokratischen Aufwand zu tun, sondern nochmal eine Stufe weiter. Es ist bürokratisch aufwändig ohnehin, aber dann nochmal diplomatisch aufwändig.

E: Genau, diese Rechtshilfewege sind einzuhalten. Jede Gerichtsbarkeit ist für jedes Land verantwortlich. In manchen Ländern kann [die Polizei] eine IP-Adresse bei dem Provider anfragen und bekommt die Daten. In anderen Ländern ist es so, da braucht man einen richterlichen Beschluss, [damit] man die IP-Daten bekommt [oder] die Bestandsdaten. Deswegen muss man diesen Rechtshilfeweg einhalten. Wir kennen ja logischerweise nicht die Voraussetzungen, wie man was bekommt im Ausland. Deswegen muss es die Tippel-Tappel-Tour gehen.

A: Dann hätte ich noch eine letzte Frage an dich. Gibt es etwas, was du diesem Gespräch unbedingt beifügen möchtest? Irgendwas, was dir auf der Seele brennt, was du gerne abgearbeitet haben möchtest? Anregungen, Kritik, Anmerkungen nehme ich auch gern entgegen.

E: Nein, tatsächlich wüsste ich jetzt nichts.

A: Dann danke ich dir nochmal recht herzlich, dass du dir die Zeit genommen hast für dieses kleine aber feine Interview.

E: Gerne.

Anhang 6.4: Transkript – Interview – ITE

A: Hallo nochmal. Schön, dass wir uns hier zusammengefunden haben. Ist es in Ordnung, wenn ich du sage?

ITE: Ja.

A: Gut. Erzähl‘ mir bitte von dir. Welche Funktion nimmst du bei den Ermittlungen ein, was sind so die alltäglichen Aufgaben, die du erfüllst?

ITE: Im Endeffekt mache ich die Auswertungen zu beschlagnahmten Servern oder Datensätzen allgemein. Der Sachbearbeiter [führt] Ermittlungen und [stößt] dabei auf Server bzw. auf Daten, die er vielleicht als interessant empfindet. Er bekommt die auf welchem Weg auch immer zur Polizei. Dann bekomme ich [diese Daten] und werte sie aus nach Maßgabe des jeweiligen Sachbearbeiters.

A: Also der Sachbearbeiter kommt auf dich zu, du bekommst einen Auftrag und den erfüllst du?

ITE: Genau, so ist das laut Konzeption vorgesehen.

A: Wie lange befasst du dich bereits mit dem Straftatphänomen Cybertrading?

ITE: Seitdem das wahrscheinlich hier das erste Mal aufgetaucht ist.

A: Das wäre dann, aus verschiedenen Quellen, 2019 ungefähr.

ITE: Ja, vermutlich. Das [Phänomen] gab es wahrscheinlich schon vorher. Das Problem bei der Polizei ist immer, dass sie ein Phänomen als solches erkennen [muss]. Es gab vielleicht schon vorher mal eine einzelne Anzeige. Das nächste Problem: Es kommen hier die Anzeigen für Leipzig rein. Wenn das auf einem Dorf war, dann geht der Geschädigte zu seiner Dorfpolizei oder macht eine Onlineanzeige. Wenn [die Beamten] das nicht richtig einsortieren, dann läuft das erstmal unter normalem Betrug. Es kann auch sein, dass es erst eine Weile nicht als Phänomen erkannt wurde. Das ist ein typisches Polizeiproblem.

A: Stadt-Land-Diskrepanz, nicht?

ITE: Genau.

A: Wenn du jetzt einen Auftrag bekommst, Server auszuwerten, Festplatten auszuwerten oder dergleichen, nach welchen Daten hältst du da Ausschau?

ITE: Das kommt darauf an, was es für ein Grundsachverhalt ist. Beim Cybertrading [liegt] der Unterschied [darin], welche Daten ich bekomme. Im Vergleich gerade beim Kollegen:

[Bei] Hostinger[141] gibt es nur die Webseite als logische Datenkopie und die Datenbanken als Datenbankdump. Mehr bekomme [ich] von denen nicht. Alles was Logfiles angeht, Zugriffe, das wird nicht mitgeliefert. Das heißt ich kann das auch nicht auswerten. Ich kann nicht gucken, wie oft oder wann sich der Nutzer auf dem Server eingeloggt hat. Das sind Daten, die runterfallen.

Das nächste Problem gerade bei den Cybertrading-Webseiten: Du hast diese Landing-Page. Meistens ist die nur dafür da, um diese Brand[142] zu [vermarkten]. Das ganze BackOffice, alles was Nutzer oder die Charts [angeht], das liegt irgendwo extern. Das [erhalte] ich in dem Moment natürlich nicht. A liegt es extern und B [gibt es eine] URL, aber wo die hinführt, weiß ich nicht, da es nicht in der Datenbank vermerkt ist, jedenfalls in dem Fall. Normalerweise hast du bei dem WordPress[143] diese CRMs[144] und CPIs[145] als Option hinterlegt. Da könnte man sagen, das liegt auf der URL oder auf der Subdomain. Das hat man bspw. bei Hostinger, bei diesen schlechteren Datendumps nicht mehr. Es fehlen eben Informationen, die einen ein bisschen weitere bringen „könnten“. Was war noch die Teilfrage?

A: Nach was für Daten du Ausschau hältst. Du hast gesagt Logs und Zugriffe bekommst du bei Hostinger nicht, wären aber gut, so klingt das.

ITE: Genau. Bei Cherry-Servers oder bei den Servern, die das BKA beschlagnahmt hat, da bekommen wir den Server als dd-Image. Sprich, das ist der komplette Server. Da hast du die Passwörter in vielen config-Dateien, entweder im Klartext oder zumindest gehasht. Du hast die Nutzernamen, diverse Logfiles, Zugriffe, Webseitenaufrufe, Datenbankaufrufe. Das sind alles Daten, die bei einer Komplettsicherung auswertbar sind und wo man auch reingucken kann.

Allgemein was Cybertrading angeht, gucke ich mir die Webseite an, virtualisieren die bei mir, [überprüfe, ob sie funktioniert und] wie sie grob aussieht. Dann gucke ich mir die kleinen hinterlegten Datenbanken für diese WordPress-Installationen an. Da kann man auch immer wieder das gleiche Schema bei diesen Standard-Passwort-Nutzern sehen. Es kommt darauf an, was ich sonst noch so sehe auf dem Server, was natürlich nur funktioniert, wenn ich den ganzen Server habe.

Im Cybertrading ist es mir noch nicht aufgefallen, aber aus anderen [Fällen, da gibt es] z.B. Spam-Mail-Versand. Das ist wie gesagt beim Cybertrading nicht dabei gewesen bisher, aber [sowas] war auch schon auf diversen Servern drauf. Nicht im Bereich Cybertrading, aber Cybercrime. Also Spam-Mails, klassischer Versand. Aber wie gesagt,

---

[141] Bei Hostinger handelt es sich um einen Serverdienstleister.
[142] Als Brand wird der Name einer Plattform der Betrüger bezeichnet.
[143] Bei WordPress handelt es sich um ein Content-Management-System, welches zum Erstellen von Webseiten genutzt wird. Die meisten Betrüger-Webseiten basieren darauf.
[144] Customer-Relationship-Management Systeme
[145] Client Portal Interface

das kann man halt nur machen, wenn man den Server komplett hat. Weil ich dann sehe kann, welche Programme installiert sind und was damit gemacht wurde.

Die bash-History ist auch ein schöner Anlaufpunkt [um zu sehen] was hat denn der Nutzer, der sich auf dem Server eingeloggt hat, da eigentlich alles getrieben. Das ist die History von den Benutzereingaben auf der Kommandozeile. Da kann man schön sehen, was er installiert hat, ob er sich bspw. extern versucht hat einzuloggen. Es gab bei einem Kollegen auch so einen Fall. Da hat man in der bash-History gesehen, dass er sich als Root, Root ist nun mal der Hauptnutzer unter Linux, auf einem anderen Server angemeldet hat, [der eine] andere IP [hatte]. Darüber hatte man einen neuen Server, eine neue Brand und konnte sich da weiter hangeln. Die Möglichkeit, so etwas zu finden, hat man aber nur, wenn man einen ganzen Server hat.

A: Also kann es dann auch sein, wenn du jetzt eine Ermittlung startest oder eine Auswertung startest, dass du von einem Server auf den nächsten, auf den nächsten… also dass es sich in einer Kette abbildet?

ITE: Genau.

A: Das dauert dann wahrscheinlich auch ziemlich lange, bis man dann irgendwann alles hat. Bekommt man dann überhaupt noch die anderen Server im Nachgang oder ist das dann eher erfolglos?

ITE: Das kommt ein bisschen darauf an. Es gibt diese Standardserver für diese Landing-Pages, das ist, sage ich mal, „Wegwerfware“. Da werden hunderte relativ schnell aufgesetzt, das funktioniert mit „einem Mausklick“. Es gibt aber diverse Server, das muss man ein bisschen mehr machen. Die liegen, deshalb werden die ja versteckt, nicht mit auf dem gleichen Server, sondern extern. Wenn man den immer wieder neu aufsetzen müsste, da ist wirklich Arbeitsaufwand dahinter. Deshalb wird versucht die Daten mehr oder weniger, in meinen Augen, technisch geheim zu halten, dass man da nicht zu schnell rankommt.

Dann ist das nächste Ding: die arbeiten mit URLs. Du kannst den Server irgendwo verstecken. [Dazu] brauchst den Server nicht umziehen, sondern du änderst [Nameserver mäßig] immer nur die URL, die auf den Server verweist. Wenn du das noch hinter Cloudflare oder einen anderen Anonymisierungsdienst [stellst], ist es schwierig, bis zum letzten Server zu kommen, wo dann wirklich die Daten liegen.

A: Hattest du schon mal so einen Endserver?

ITE: Ja, hatten wir. Das macht gerade das LKA. Das waren diese 17 Stück oder so. Da hatte man auch wirklich die Enddatenbanken. Der, der am meisten Spaß gemacht hat beim Auswerten, war der Windows-Server. Da hast du zehn Nutzer, Callcenter-Agenten, drauf gehabt. Jeder hatte seine eigene Excel Tabelle und der Superuser hatte schon [die Server] vorbereitet für Februar, März, die sie anmieten wollen und wie sie heißen usw. Da

ging es um hunderte Server. Die [Täter] bereiten das alles schon vor und dann geht es nur noch Zack, Zack, Zack. Auswertetechnisch ist das eine riesen Blase.

A: Das klingt auch so, als ob die Täter ihre Masche durchführen, aber haben schon die nächste in der Hinterhand. Sobald die aktuelle [Masche] scheitert oder kurz vorher lösen sie das aus, sodass dann der Rest aktiv ist.

ITE: Ja, auf jeden Fall.

A: Das ist ja theoretisch auch ein hinterher Gerenne oder?

ITE: Ja.

A: Wie lange würdest du schätzen, dauert eine Auswertung im Durchschnitt, wenn wir jetzt von einem Server ausgehen und nicht der Kette?

ITE: Da kommt es darauf an, welche Daten angeliefert wurden. Bei diesem [Fall mit] Hostinger: ein Tag für die zwei Server, mehr nicht. Da gebe ich mir schon ein bisschen mehr Mühe, indem ich die Webseiten und die Datenbanken noch virtualisiere, sodass ich optisch, wenn es gewollt ist, ein Bild machen kann. Theoretisch könnte man das auch manuell machen und einfach die Datenbank als solche im Text nach den Optionen durchgucken, die relevant sein könnten. Das kann man machen, aber es ist unschön.

Die benutzen alle WordPress, das ist ein Content-Management-System. Wenn ich mich einlogge, weil ich ja Zugriff auf die Datenbank habe, kann ich es auch manipulieren. Das heißt, ich kann mein eigenes Passwort reinsetzen und ich kann mich als Admin in dieses WordPress-Backend einloggen. Dann klicke ich auf Settings [und es] wird mir alles schön in einer Maske angezeigt.

WordPress ist das grobe Schema und man kann selber einzelne Plug-Ins nachladen. Jedes Plug-In hat auch wieder eigene Optionen in der Datenbank. Entweder kennt man alle Plug-Ins irgendwann, die benutzt wurden oder man muss für jedes Plug-In diese SQL-Abfrage für die Datenbank anpassen, weil die Felder oder die Optionsnamen sich ändern je Plug-In. Da ist es in meinen Augen schneller und einfacher, wenn man die Webseite und die Datenbank komplett virtualisiert und sich in dem Backend vom Admin anguckt.

A: Wenn du jetzt eine Zeitspanne angeben müsstest? Ein Tag ist relativ kurz, was ist das längste, woran du gesessen hast?

ITE: Von dem Windows-Server, wo die ganzen Datenbanken und Excel Tabellen waren, habe ich nur eine Grobauswertung gemacht. Der ist ja zum LKA gegangen. Das ist richtig übel, was da alles drauf ist. Da wird, glaube ich, immer noch ausgewertet. Also bis zu sechs Monaten, je nachdem was da vielleicht für Datensätze hinterlegt sind, kann das schon dauern.

Die Frage ist, wie definiere ich, dass die Auswertung beendet ist? Ich [stoße bei der Auswertung eines Servers auf] eine Excel Tabelle für den März 2022. Da steht drin, die [Täter] wollen [bestimmte] Server anmieten mit [bestimmten] Brandnamen. Sprich, ich weiß schon, wie die neuen Cybertrading-Webseiten heißen werden. Das heißt, ich [muss überlegen, ob] ich den Server beschlagnahme. Gehört das [dann] mit zu der Auswertung? Ich sage [die Auswertung dauert] wahrscheinlich drei bis sechs Monate für diesen einen Datensatz.

A: Ist zumindest kürzer als die Ermittlungen in Summe. Der Kollege sprach von zwei bis drei Jahren, wenn man gut ist.

ITE: Das Hinterherlaufen ist meistens das Problem. Erstmal wieder zur Staatsanwaltschaft einen Beschluss beantragen. Jetzt sind wir beim Thema grenzübergreifend. Dann muss [man den Beschluss] vielleicht ins Ausland schicken. Das ist es, was am längsten dauert.

A: Sind dir bei den Auswertungen über die verschiedenen Jahre Veränderungen in Bezug auf die Schwierigkeit oder die Komplexität der Server aufgefallen? Verschlüsselung, Verschleierung, sowas in der Art?

ITE: Allgemein erstmal nicht. Klar, es gibt immer diverse neue Techniken bzw. [Fälle, die] man noch nicht hatte. Auf diesem Windows-Server war auch eine windows.net-App, sowas hatte ich vorher auch noch nie. Das ist auswertetechnisch ein wenig schwierig.

Der erste Ansatz bei mir ist immer stupide rauskopieren und in einer virtuellen Maschine starten, Mal gucken, was passiert. Das hat schon relativ gut funktioniert, also das Programm versucht zu starten. Man [erhält] ein kleines Logfile und sieht, [die Maschine] will sich zu einer Datenbank verbinden. Erster Hinweis: Ich brauche eine Datenbank, sonst funktioniert das Programm nicht. Im Logfile konnte man schon den Nutzer ablesen, es war ein bekannter Nutzer oder Brand-Nutzer. Aber primär, wie die App aussieht, weiß ich erstmal nicht. Ich kann sie ja vorerst nicht starten. Rein vom Namen her geht es um Bezahlungsströme. Sprich, es kann sein, dass das eine App ist, um Gelder zu verschieben. Das wäre meine erste Intention.

Jetzt bin ich dran, die wahrscheinlich zugehörige Datenbank anzugucken. Die heißt [idealerweise] genauso wie das Programm. Ich kann in dem Fall erstmal nur in die Datenbank gucken und [logisch untersuchen], was ich habe. Ich habe mehrere Tabellen. Dann gucke ich mir an, was da gespeichert ist. Da hast du die Tabellennamen bzw. die Spaltennamen. Rein vom technischen Verständnis her, wie man eine Datenbank aufbaut oder aufbauen sollte, bedeutet das Folgendes: Es gibt eine relativ lange Liste von Nutzern. [Damit habe] ich auf jeden Fall E-Mail-Adressen, Namen und Registrationsdaten. Aber was die App per se erstmal macht, kann ich, aufgrund der Daten, die ich in der Datenbank vorfinde, nur „raten“.

A: Das war jetzt eine Neuheit, aber was hat das mit der Schwierigkeit zu tun?

ITE: Die Schwierigkeit besteht eigentlich meist darin, [dass] es nichts gibt, was sich so schnell verändert wie Cybercrime oder allgemein Technik. Man kann halt nicht alles wissen heutzutage. Entweder man ist ein Allrounder und kann sich überall reinfitzen oder man ist ein Experte auf einem relativ kleinen Gebiet. Zu sagen, egal was mir vorgelegt wird, ich kann damit umgehen und zwar richtig gut, ohne mich nochmal einlesen zu müssen, der lügt. Das funktioniert nicht.

Wenn [ein Täter] etwas verstecken will, habe ich [als Auswerter] vielleicht Glück, [indem] ich irgendwo einen Hinweis finde, z.B. [einen Hinweis auf das Programm] Veracrypt. Dann kann ich anfangen zu suchen. Bei Veracrypt verschlüsselt [der Täter] entweder die ganze Festplatte oder einen USB-Stick. [Er] kann auch Dateien, also Dateicontainer mit Veracrypt aufmachen bzw. erstellen. Da kann [er festlegen], wie groß die sind. [Er] muss bloß grob wissen, wie viele Daten [er] da drin speichern will.] [Angenommen er] hat einen Haufen Videos oder runtergeladene Filme. Die sind heutzutage, wenn sie [eine] gute Qualität haben, acht bis neun Gigabyte groß. Wenn [er] clever [ist, packt er in die] Filmliste eine andere Datei und [nennt] sie .mkv. [Theoretisch] muss nur [er] wissen, dass das Ding verschlüsselt ist bzw. dass es sich um eine versteckte Truecrypt oder Veracrypt Container-Datei handelt.

Ich [als Auswerter] gucke mir die Filme nicht alle an. Man klickt vielleicht mal ein, zwei an und [stellt fest], das sind Filme, es ist auch das drin, was [drin sein sollte]. Das würde mich aber beim Cybercrime nicht interessieren. Das heißt, ich würde die gar nicht mal anfassen, obwohl die auf dem Rechner oder Server rumliegen.

Wenn ich einen KiPo-Fall habe, dann ist es wieder etwas anderes. Da gab es auch Fälle, dass einzelne KiPo-Ausschnitte in anderen [Dateien] versteckt waren. [Die Auswertung] funktioniert da automatisiert. Ich lasse alle Filme durchlaufen und mache zehn Bilder pro Film. Dann gucke ich mir die Bilder an und [entscheide]. Klar kann es [vorkommen], dass der Film zwei Stunden geht. Wenn [ein Täter] viel Mühe hat oder viel Energie dafür aufwenden möchte, schneidet er nach einer Stunde ein fünf Minuten KiPo-Video rein. Das zu finden mit zehn Bildern pro Sekunde oder Film, das ist dann Zufall. Aber ehrlich gesagt, gerade was KiPo angeht, machen sich die [Täter] die Mühe nicht. Warum sollten sie es verstecken. Deren Denke ist meistens so, das ist auf meinem Rechner…

A: … es findet eh keiner.

ITE: Es findet eh keiner. Oder anders herum, um das überhaupt finden zu können, muss [die Polizei] Zugriff auf meinen Rechner haben. Wenn ich aber nicht auffalle, wie soll [die Polizei] an meinen Rechner kommen.

Bei den „Konsumenten“ ist das natürlich genauso. [Die müssen wissen, in welchem Film sind die] fünf Minuten KiPo, meistens sind die KiPo-Schnipsel viel kürzer. Das heißt, sie machen den Film an, müssen eine Stunde reinspringen, damit sie sich das angucken können. Wollen sie sich etwas anderes angucken, müssen sie einen anderen Film [su-

chen]. Da müssen sie auch wieder [vorspulen]. [Wenn] man sagen kann, [dass die KiPo-Ausschnitte] immer nach genau einer Stunde [eingefügt werden], dann muss man nicht [lange suchen]. Aber das machen die [Täter] alles nicht. Die laden sich das [Material] runter, [teilweise] auf externe Festplatten. Und nicht mal die sind meist verschlüsselt. Die [besitzen] das einfach und Punkt aus Ende. Das ist jetzt ein Abzweig gewesen.

A: Alles gut, es ist noch im Rahmen. Ich verstehe den Ansatz. Abgewandelt auf Cybertrading könnte man das so sehen: Da hat jemand eine Datenbank, benennt die anders und wer was verstecken will, der wird Wege finden oder es zumindest versuchen. Entweder es glückt oder es glückt nicht.

ITE: Gerade beim Cybertrading, was diese Landing-Pages angeht, das ist Wegwerfware. Die [Täter] machen sich nicht die Mühe, da irgendwas zu verstecken. Es ist mehr Aufwand das zu verstecken. Es gibt keine Daten auf diesen Wegwerf-Landing-Pages, die relevant sein könnten. Außer die Admin-E-Mails, aber die sind meistens Protonmail oder Wegwerfadressen.

A: Die relevanten Dinge liegen ja dann auf dem Server. Da müssten sie schon davon ausgehen, mit den Machenschaften, die sie betreiben, dass es früher oder später jemanden gibt, der auf den Dunst kommt und nachforscht.

ITE: Ja, bisher waren die Server, die das LKA auswertet, alle unverschlüsselt. Eigentlich wäre es kein Problem, die Nutzerdaten vom Server zu verschlüsseln, sodass, wenn der Nutzer nicht angemeldet ist und ich aus dem Nutzer die Daten kopiere, die [Daten] verschlüsselt sind. Man sieht die [Daten zwar], aber sie sind eben verschlüsselt. Das würde alles gehen. Die machen sich eben in dem Fall komischerweise nicht die Mühe.

A: Das wäre jetzt ein guter Tipp für Möchtegern-Kriminelle.

ITE: Es gab Fälle, da war der Laptop vollverschlüsselt. Da steckte ein USB-Stick dran und da waren wahrscheinlich keyfiles [drauf]. Sobald du den [Stick] wieder abziehst, ist der Laptop wieder vollverschlüsselt. Man kann die Daten zwar ziehen, aber man bekommt nur „Datengulasch“. Ohne das Passwort kommst du nicht ran. Je nach dem was es für eine Verschlüsselung ist und wie lang das Passwort ist, ist es eigentlich unmöglich sowas zu knacken. Wenn du nicht irgendwelche anderen Wege hast.

Da sind wir wieder beim Thema Cybercrime und Webseitenbetreiber bzw. Hostprovider. Es ist ja deren Hardware, deren Server. Die [Betreiber] müssen die Server auch warten können. Das heißt, sie haben eigentlich hinten rum einen Login. Wenn die Polizei hinkommt und den Server [inklusive unverschlüsselter Daten haben will, können die Betreiber durch ihr eigenes Backend] das Passwort [der Täter] zurücksetzen?

Es kommt immer darauf an, [welche] Technik [genutzt wird]. Es gibt virtuelle Server, richtige Root-Server usw. Da [gibt es] wieder das Problem, [dass] es so viele verschiedene

Ansatzpunkte gibt, wo man vielleicht doch Daten herkriegen könnte. Das ist von Sachverhalt zu Sachverhalt verschieden.

Vielleicht noch eine Anmerkung: Wenn die Daten bisher verschlüsselt gewesen waren, dann nur, weil das Gerät an sich, also das Handy oder MacBook, das von Hause aus schon gemacht hat, ohne dass der Nutzer da viel groß zutun musste. Bei den neueren Macs gibt es mehrere Möglichkeiten, FileVault etc. Das macht der Nutzer einmal. Er wird evtl. bei der Installation, beim ersten Start gefragt, [ob er seine] Daten verschlüsseln [möchte]. Wenn er ja anklickt, muss der Nutzer nicht viel machen. Das läuft, wenn überhaupt, eh alles im Hintergrund ab. [Der Nutzer] gibt nur noch sein Passwort ein und seine Datensätze werden dann on-the-fly verschlüsselt.

Das MacBook kommt ein- oder ausgeschaltet bei uns an. Wenn es etwas älter ist, kann man evtl. die SSDs ausbauen. Ansonsten muss man den Mac mit einem Nutzerpasswort starten. Oder man startet den Mac fremd, mit einem Linux, um Zugriff auf den verbauten Datenspeicher [zu erhalten]. Dann kann man die Daten theoretisch auch sichern. Problemtisch in dem Falle: Wenn das [System] von Hause aus verschlüsselt ist, kann ich den Datensatz angucken und sehe nichts.

Wenn [Geräte] verschlüsselt [waren], ging es entweder um terroristische Vereinigungen, die Wert darauf legen, ihre Daten zu verschlüsseln und/oder zufällige Nutzer, [deren] Gerät [das] von sich aus gemacht hat. So richtig aktiv [schützen sich die Täter nicht]. Denen ist das zu viel Aufwand, bisher.

A: Ist doch gut wenn es dabei bleibt, das macht es euch einfacher. Gibt es eine Art Struktur oder Muster seitens der Betrüger, welches dir bei den Ermittlungen aufgefallen ist?

ITE: Das ist uns beiden aufgefallen, wenn du dich erinnern kannst. Im Zuge der Ermittlungen bzw. dass ich mehrere Server ausgewertet habe, ist mir aufgefallen, dass [in den Datenbanken] immer das gleiche Passwort ist, immer die gleichen Nutzer [hinterlegt] sind. Das habe ich irgendwann laut gedacht bzw. laut in die Runde gesagt. Uns ist ja dann [das Passwort] aufgefallen. Der Startbuchstabe wird je nach Brand gewählt. Sprich, bei Tradingsolutions war es das „t“, bei StockLux war es das „s“. Man kann sogar sagen, es ist ein modus operandi. [Die Täter] benutzen immer dasselbe Passwort und wenn sie es leicht ändern, ändern sie in dem Fall nur [den Startbuchstaben entsprechend des] Brandnamen. Da das Passwort so „speziell“ ist, kann man schon [vermuten], dass [es sich] immer [um] dieselbe Gruppe oder immer denselben Crime as a Service Dienstleister handelt, der die Datenbanken aufsetzt bzw. zur Verfügung stellt.

A: Irgendeiner muss es ja machen. Du hattest jetzt schon von Verschlüsselung gesprochen und dass es die nicht wirklich gibt, glücklicherweise. Welche anderen Probleme sind dir bei den Ermittlungen aufgefallen und wie kann man diese lösen, wenn überhaupt?

ITE: Geht es um die Ermittlung oder meinst du die Auswertung?

A: Die Frage hat so ziemlich jeder gestellt bekommen, weil es um die Herausforderungen geht. Das ist ja die Kernfrage meiner Bachelorarbeit.

ITE: Im Endeffekt ist immer der zeitliche Verzug bei vielen [Fällen] gegeben. Bis sich die Geschädigten melden bei der Polizei, müssen sie erstmal mitkriegen, dass sie Geschädigte sind. Es gibt auch welche, die [gehen immer noch davon aus, dass das funktioniert. Die Webseite ist nur nicht mehr erreichbar].

Die [Täter] machen vielleicht eins, zwei Wochen Kohle mit ihrem Brandnamen x. Dann melden sich vielleicht nach zwei, drei Wochen die ersten Nutzer, die [ihr] Geld zurück haben [wollen]. Sie werden dann vertröstet. Die Callcenter-Mitarbeiter oder die Leute, die miteinander konferieren, die sind psychologisch echt gut drauf. Sie sind wahrscheinlich auch geschult. Bis sich einer von den Geschädigten entschließt, eine Anzeige zu machen, gehen wahrscheinlich vier, fünf, sechs Wochen ins Land. Da sind wir bei anderthalb Monaten.

Aus dem Windows-Server wissen wir, die [Täter] haben ihre Listen schon Monate vorgearbeitet. Im Endeffekt ist denen nach sechs Wochen der Server bzw. der Brand, mit dem sie Geld gemacht haben, scheißegal. Der wird einfach abgeschaltet. Dann kommt [der Eintrag] in die Excel Tabelle und es interessiert sie nicht mehr. Sie machen einfach weiter.

Jetzt sind wir beim Thema: Es kommt die Onlineanzeige bzw. die Anzeige vom Geschädigten. Das wird aufgenommen, in den Postumlauf gegeben und zur zuständigen Stelle geschickt. Dort liest es sich wieder jemand durch. [Die Person entscheidet, ob die Anzeige dort richtig ist oder nicht.] Bis dann das erste Mal ermittelt wird, gehen zwei, drei Monate ins Land.

[Im Anschluss] guckt man, ob die Server noch online sind. Wenn ja, beantragt man Beschlüsse. Die gehen rüber zur Staatsanwaltschaft, [wobei] vorher eine Akte gebaut werden muss. Dann geht [der Beschluss an die nächste Instanz. Es folgt] die Tippel-Tappel-Tour.

Wie im Fernsehen funktioniert [es nicht. Von wegen] ich will den Server haben, klicke in der Polizeidienststelle auf [die IP des] Servers und am nächsten habe ich die Daten. Dieser zeitliche Verzug, bis man anfängt zu ermitteln und vielleicht durch die Ermittlung neue Daten bekommt, ist viel zu lang. Das wird sich auch nicht ändern können. Der erste große zeitliche Verzug [findet bei den Geschädigten selbst statt]. Wenn die [Täter] schneller arbeiten, als die [Geschädigten das] mitkriegen, dann ist es vorbei.

Da gab es einen Fall. Eine Kollegin aus dem Revier hat eine Spam-Mail bekommen und ist drauf reingefallen. Sie hatte [kurz zuvor] ihre Bankverbindung geändert. [Daraufhin gab es] Probleme mit PayPal, ihr Konto zu ändern. Das heißt, sie hat die ganze Zeit schon per E-Mail mit PayPal konferiert. Während sie mit PayPal [in Kontakt stand], Zufälle gibt es leider, fliegt bei ihr eine PayPal Phishing-Mail ein und sie gibt da ihre Daten an. Sie hatte alles schön reingeklimpert und aufgefallen ist es, als [sie ihre] Onlinebanking-Daten und

Kreditkartendaten [angeben sollte. Da hatte sie gemerkt], das ist nicht richtig, das ist nicht PayPal. Ihre Kreditkartendaten wurden gleich am ersten Tag noch missbraucht, das ist wirklich schnell gewesen. [Die Karte] ist für eine Deutsche Bahn Karte oder einen Gutschein benutzt worden. Die Spam-Mail kam auch von einem Deutschen Provider.

[Die Geschädigte] ist gleich hochgekommen in die 33. Da haben wir uns das angeguckt. Ich habe mir den Server, dessen Inhalt angesehen, der online war. Es lag nicht nur eine PayPal-Phishing-Seite darauf, sondern auch eine Amazon-Webseite. Am ersten Tag habe ich die aufgerufen, da kam die normale Phishing-Seite von PayPal. Einen Tag später [habe ich die gleiche Seite] aufgerufen, da habe ich den Inhalt des Web-Servers gesehen. Wahrscheinlich [hatte der Täter] einen Fehler gemacht. Da waren [noch weitere Phishing-Webseiten] drauf und, was ich auch mitbekommen habe, es kamen aktiv neue Ordner hinzu. Das heißt, es wurde gerade auf dem Server gearbeitet.

Wenn der Chef merkt, da geht was, dann ist er Feuer und Flamme. Dann haben wir angefangen. [Es] ist auch ein schöner Sachverhalt geworden. Der [Täter] ist zu viereinhalb Jahren verurteilt worden. Wir waren [damals] auch in einem anderen Bundesland durchsuchen, das hat Spaß gemacht.

Wenn es nicht die Kollegin gewesen wäre, wenn sie nicht gleich am ersten Tag da gewesen wäre, [wenn nicht] aktiv auf dem Server gearbeitet worden wäre und der Server nicht auch noch Deutsch wäre, [wäre es] zwei, drei Wochen später im Revier gelandet. Ob dann noch etwas ermittelt worden wäre, will ich mal dahin stellen. Selbst wenn es im Nachgang beim [zuständigen Fachkommissariat] gelandet wäre… Wenn das Kind in den Brunnen gefallen ist und ertrunken ist, brauchst du es auch nicht mehr heben.

A: Der Drops ist gelutscht.

ITE: In dem Falle wäre der Drops gelutscht gewesen. Bei [dem Täter] war es so. Diese Server hat er mit gefakten Daten angemeldet und sie waren auch nicht lange online. [Der Provider will natürlich für seine Dienste bezahlt werden.] Der [Täter] hat ja PayPal-Konten gephisht….

Bei dir ist jetzt in PayPal eine Abbuchung drauf. Heutzutage mit der App bekommst du sofort eine Nachricht, das war damals nicht so. Du musstest auch nicht dein Handy hinterlegen, sondern hast dich regelmäßig auf der Webseite eingeloggt oder auf deinen Kontoauszügen [nachgesehen]. Wenn du nicht zeitnah mitbekommst, dass dein Konto missbraucht wird, hast du das gleiche Problem des Zeitverzuges.

[In dem Fall] war es so, [dass der Täter] mit geknackten PayPal-Konten den Server bezahlt hat. Manchmal sind die Server nach drei Tagen wieder weggewesen, weil der [Kontoinhaber eine Nachricht über die Transaktion bekommt, die er nicht getätigt hat. Er meldet den Betrug bei PayPal] und die buchen das Geld wieder zurück. Der Serverbetreiber [will natürlich sein Geld und fragt nach]. PayPal [antwortet mit dem Hinweis auf] betrügerische [Aktivität. Daraufhin] macht [der Betreiber] den Server dicht.

Wenn der Serverbetreiber den Server dicht macht, dann löscht er ihn meistens auch oder wirft die virtuelle Maschine weg. Im Nachgang könnte man sagen, natürlich [muss er davon ausgehen], dass irgendwann die Polizei vielleicht klingeln kommt oder [nach Daten fragt]. Wenn er jede virtuelle Maschine aufheben müsste, wo Betrügereien [dahinter stecken], dann [kostet ihn das] zu viel Speicherplatz, so viel hat er nicht.

Dann haben wir das nächste Problem: Datenschutz in Deutschland. Wenn ich mir als Nutzer einen Webserver anmiete und kündige zum Tag x, dann ist der Provider verpflichtet, meine persönlichen Daten von dem Webserver [zu entfernen]. Er muss ihn löschen und wegwerfen. Er darf ihn nicht zur Sicherheit drei Monate behalten. Es sind ja Daten von einem Dritten. Theoretisch könnte es ja sein, dass dort Daten von einem dritten Geschädigten drauf sind. Das heißt, er darf die auch nicht behalten. Das ist ein bisschen gesponnen. Rein rechtlich gibt es keinen Grund, es sei denn die Polizei hat schon nachgefragt, die Daten von einem betrügerischen Webserver, zu behalten.

A: Das war jetzt auf jeden Fall erstmal ein Wummer. Wie könnte man denn die Ermittlungen intern oder extern besser unterstützen? Du hast ja jetzt eigentlich ziemlich viele Ansatzpunkte genannt, wo man etwas reininterpretieren kann.

ITE: Die Gesellschaft müsste sich, gerade was Internetkriminalität angeht, einig werden, dass es mit nationalen Gesetzen eben nicht geht. Und dann Strukturen schaffen, [um schneller agieren zu können]. Das ist wohl schon besser geworden, weil es Staatsanwälte gibt, die nur das machen, die nur dazu da sind, um Anfragen schnell ans Ausland zu steuern.

Das war früher definitiv nicht so. Das mussten die Staatsanwälte vor Ort selber machen und die haben meistens die Hände gehoben [mit der Begründung, das] haben sie noch nie gemacht, [sie] wissen gar nicht wie das geht. Dann müssen sie das [Schriftstück] erstmal auf Deutsch schreiben, [welches wiederum] in die jeweilige Sprache übersetzt werden [muss] usw.

[Wir bräuchten] Gesetze, die global gelten. Das ist vielleicht ein bisschen utopisch. Gerade was die EU angeht, man kann ja da diverse Länder mit rein nehmen, [dass man] gesetzlich den Rahmen schafft, es gibt für uns global als Gemeinschaft geltende Gesetze. Die werden eins zu eins ins nationale Recht übernommen. Das kann man alles mit Verträgen [besiegeln]. Und wir haben uns alle daran zu halten.

Wir müssen im Land eine Stelle oder eine Behörde schaffen, die nur für sowas da ist. Wenn von einem anderen Mitgliedsstaat Anfragen kommen, um die auf einem kurzen Dienstweg, schnell zu bearbeiten. [Diese Stelle] macht dann nur noch diesen einen Bereich bzw. ist dafür zuständig. Dann muss sie nicht immer neu überlegen [was zu tun ist], wenn eine Anfrage von Staat x kommt.

Ansonsten das größte Problem, und das wird man aber auch mit solchen Strukturen nicht wirklich lösen können, [besteht in der Proaktivität der Polizei, solchen Geschehnissen

entgegenzutreten. Man muss erst] dem Geld hinterher laufen, aber irgendwann bekommt man [die Täter]. Das dauert eine Weile. Es wird [meist] groß in den Medien gezeigt, aber wieviel Manpower und vor allem wieviel Arbeitszeit, Stunden, Tage, Monate, Jahre hinten dran hängen, sieht man dann meist nicht mehr.

Es ist schön, dass man [hin und wieder] einen Erfolg hat. Wenn man die [Passwortgruppe und das ist in meinen Augen eine der größten Gruppen,] mal komplett wegnehmen würde, dann entsteht ein Vakuum. Irgendjemand [wird diesen] Raum ausfüllen [wollen]. Hydra mäßig: Ich schlage einen Kopf ab und es wachsen zwei nach. Man kann mit Cybercrime gerade extrem viel Geld verdienen. Nur weil eine Gruppe weg ist, wird die andere [nicht auch aufhören, aus Angst vor der Polizei]. Nein, die sagen sich, das Geld was bei denen geflossen ist, könnte jetzt zusätzlich zu uns fließen. Das wird es immer geben. Sobald die „Nachfrage“ da ist, wird es beliefert. Dabei ist es egal von wem.

A: Das klingt jetzt natürlich nicht so optimistisch [bezüglich der] Gegenmaßnahmen, um dem entgegenzusteuern.

ITE: Die Polizei hat ja eigentlich auch den Auftrag …

A: Prävention?

ITE: [Präventionsarbeit] zu [leisten], genau. Man könnte in meinen Augen viel mehr machen. Gerade die [Klassiker], Enkeltrick. Das [geht auf und ab und] steht regelmäßig in der Zeitung. [über] das Phänomen Cybercrime habe ich noch nicht in der Zeitung gelesen, obwohl es so ein großes Ding ist, [obwohl] da so viel Geld rum geht. Das könnte man forcieren.

Da ist aber wieder das Thema: Deutschland - Landespolizei bzw. Polizei ist Ländersache. Jeder macht sein eigenes Ding. Es kann ja jeder seine eigene Landespolizei haben, aber die Gesetzgebung und die Polizeigesetzgebung sollte der Bund in die Hand nehmen. Dann sind die nämlich von Land zu Land nicht mehr unterschiedlich. Man muss sich vielleicht überlegen, [was man bei einer Durchsuchung in einem anderen Bundesland beachten muss] oder nach welcher Rechtsgrundlage [man agieren muss].

Der Bund [sollte] die Gesetze [machen], der macht die für alle Bundesländer gleich. Es gibt in dem Fall keine Unterschiede, wir haben alle den gleichen Level, womit wir arbeiten können. Wenn man [die Polizeigesetze] vorher vergleichen würde, [könnte man die Passagen der verschiedenen Bundesländer übernehmen, die nützlich sind]. Wenn wir das auf Bundesebene machen, dann können die ganzen Justizminister und Polizeipräsidenten miteinander reden. Das wäre schön.

Man kann [bei] Prävention, gerade was Cyber angeht, relativ viel machen. Es gibt zum Beispiel Firmen, die verschicken intern selbst Spam/Phishing-Mails, um zu gucken, wer fällt darauf rein. [Die machen das nicht], um dem einzelnen Mitarbeiter eine reinzuwürgen. Man sagt, so [ist der Stand. Damit die] Firma sieht, [ob] die Schulung was gebracht [hat].

Wenn 90% nicht darauf reinfallen, ist ja schon mal vielen geholfen. Im Vergleich, wenn man sagen würde, 90% sind drauf reingefallen, dann würde ich wahrscheinlich als Firma sagen, ich mache lieber das Internet aus. Prävention würde viel gehen, aber manchmal hat man das Gefühl, es ist nicht gewollt, es kostet zu viel.

A: Es gibt so viele Sendungen im Fernsehen, wo ich sage, das muss man sich nicht geben. Da ist es doch eigentlich besser, wenn es etwas Informatorisches gibt. [Der] Geschädigte, mit dem ich gesprochen habe, hat mir z.B. gesagt, dass er sich von vornherein schon für solche Sendungen interessiert hat, z.B. Aktenzeichen xy ungelöst. Gut, bis das natürlich ins Fernsehen kommt, vergeht auch ein bisschen Zeit oder bis da insgesamt mal eine Doku darüber gedreht wird. Oder Mordfälle, sowas wie Sky [Crime] oder true crime. Das drehen sich so viele Leute rein. Aber dass man da vielleicht nicht einfach einen Mehrwert daraus ziehen kann für die Gesellschaft, finde ich schade. Dann die, die es interessiert, die kriegen nichts von dem mit, was aktuell ist. Also eher auf Aktualität anspielen, nicht immer wieder Enkeltrick zeigen. Klar ist das auch wichtig, aber dass man halt auch guckt, was ist neu.

ITE: Genau. Man könnte, wenn man wöllte, viel mit Gesetzen machen. Zum Beispiel die LVZ. Ich hab regionale Printmedien. Die sollen das auch bezahlt bekommen, aber ich verpflichte die. Ich mache als PD Prävention: einen Flyer oder layoute eine Seite. [Nach dem Motto] Achtung, wir haben gerade folgende Phänomene auf dem Schirm die entweder neu sind oder wieder verstärkt auftreten. Das hat ja damals ganz gut funktioniert, das machen [die Täter] mal wieder. Man muss ja keine schicken Bilder machen, sondern es geht um Text, Informationen, kurz und knapp. Da kann man relativ viel auf einer Zeitungsseite machen in meinen Augen. Entweder ich gehe an die LVZ ran und sage, ihr druckt das jeden Monat. Das kann ja auch ganz hinten [in der Zeitung] sein. [Wen es interessiert], die Polizei informiert. Dann hast du einen Bereich, das kann [sich] monatlich oder auch wöchentlich ändern. [Sowas, wie] „Aktuell wieder vermehrt Kellereinbrüche, bitte darauf achten“, mehr muss ja nicht sein.

Auf der anderen Seite kann man einzelne Phänomene wie Cybertrading kurz vorstellen und woran man sowas erkennen kann. Der Klassiker sind ja die 250,00 Euro. Nein, sobald [die Bürger] 250,00 Euro irgendwo [einzahlen sollen], nein, machen Sie es nicht! Natürlich ein bisschen schöner.

[Natürlich] kostet [es] etwas, eine Seite zu drucken oder noch eine Seite hinten anzuheften. Aber als Gesellschaft würde ich diese Printmedien dazu verpflichten, das zu machen. Die bekommen jeden Monaten oder jede Woche, aller zwei Wochen von der örtlich zuständigen Polizei eine E-Mail mit der PDF oder mit dem Pagelayout und dann haben die das zu drucken. Vielleicht [strahlt man] mal [bundesweit] eine Infosendung oder eine Werbung [aus, gibt das Vorgehen] durch. In jeder ihrer lokalen Zeitung und/oder im Internet unter der Webseite können sich [die Bürger] über gerade aktuelle Phänomene in ihrem Bereich und/oder global informieren. Es wäre wirklich einfach.

Klar ist es ein bisschen Arbeit, das immer aktuell zu halten. Dafür hat man ja eigentlich die Social Media Teams vor Ort. Die würde ich dafür einspannen, meine Meinung. Die bekommen dann jeden Monat, regelmäßig von den einzelnen Bereichen, Reviere etc. [die Informationen]. Wenn das Revier sagt, sie haben gerade wieder viele Wohnungseinbrüche bzw. Kellereinbrüche: Info [rausgeben]: Im Bereich x kommt es gerade vermehrt zu Einbrüchen, bitte mal ein bisschen darauf achten. Mehr braucht man ja nicht. [Bis es] irgendwann in der Gesellschaft angekommen ist.

Wenn ich wissen will, was gerade bei mir los ist, dann gucke ich entweder auf die letzte Seite der LVZ oder ein anderes Printmedium, das mir gefällt und/oder ich gehe ins Internet auf diese eine Seite und weiß [Bescheid].

A: Das ist der Punkt, die Leute müssen aktiv mitmachen. Die Polizei informiert, die Banken informieren, du findest auch Schlagzeilen in den Nachrichten. Aber das Interesse fehlt. [Ein Thema] kocht mal kurz hoch, wie beim Cyberbunker. Das ist mal das Thema schlechthin und danach geht [das Interesse] wieder runter. Aber die Idee mit den Printmedien find ich ganz gut. Ich denke, immer noch viele Leute lesen Zeitung oder dass man einfach mal im Radio eine Art Annonce [aufgibt]. Dass man sagt, so [ist der Stand, seid bitte wachsam]. Die Idee gefällt mir tatsächlich ziemlich gut. Da müssen wir mal mit der Präventionsabteilung bei euch sprechen, was die so machen.

ITE: Meistens ist es so, egal wo es ein Printmedium gibt, bei uns im Dorf oder der Stadt, da gibt es zumeist einen Aufsteller. Ich meine die LVZ hat das auch. Da kannst du die aktuelle Ausgabe lesen. Die [Zeitschrift wird] aufgeklappt und ins Schaufenster [gelegt]. Wenn man sich damals im Dorf informieren wollte, ist man ja entweder zum …

A: Rathaus, Bürgeramt?

ITE: Rathaus, Bürgeramt, genau sowas, [gegangen]. Bei uns ist es alles dasselbe. Entweder waren da Aushänge oder eben auf dem Marktplatz.

A: Litfaßsäulen, die gibt es doch schon gar nicht mehr!

ITE: Litfaßsäulen. Ja doch, in Leipzig gibt es noch welche, aber genau sowas: Neuralgische Punkte. Meistens ist es der Stadtkern mit einem Marktplatz, [wo ein] Aufsteller [steht] und da sowas drauf steht.

Wenn ich [heute] etwas wissen will, dann fange ich an zu googeln, der Klassiker. Aber es gibt diese typische zentrale [Stelle], das ist vielleicht ein bisschen oldschool gedacht. Ich habe einen Punkt, wo ich mich immer hin wenden kann, wenn ich etwas wissen will. Das gibt es heutzutage nicht mehr. Auf der einen Seite, ist es cool, dass das Internet so groß ist und ich tausende Quellen habe, wenn ich mich informieren will. [Auf der anderen Seite] haben wir das Problem, dass die meisten mit den tausend Quellen einfach überfordert sind, nicht wissen, welche Informationen sie aus welcher Quelle ziehen sollen oder ziehen können.

Der Staat oder das Land hat in meinen Augen die Verpflichtung, seinen Bürgern ein bisschen was zu bieten. In dem Falle Informationen, die abgesegnet sind, die valide sind, [zu bieten].

Wenn ich sage, jetzt bin ich wieder bei den Einbrüchen, es gibt gerade [in dem Stadtteil] viele Einbrüche, dann ist das eine Information. Die hat mir die Stadt oder die Polizei in dem Schaukasten zur Verfügung gestellt, die muss ich nicht hinterfragen. Einbruch ist jetzt vielleicht ein sehr einfaches Beispiel, aber es ist eine Information, auf die kann ich zählen.

Wenn ich ins Internet gehe und sage, die Erde ist flach, dann bekomme ich Videos oder pseudowissenschaftlichen Abhandlungen. Wenn ich leichtgläubig bin, dann falle ich auf so etwas rein. Es gab mal einen Artikel, den fand ich eigentlich sehr witzig, da ging es um die typische Nigeria-Connection - der Prinz.

A: Ja, der sagt mir was.

ITE: Die Frage, die der Schreiberling gestellt hat, war, wieso es diese Masche immer noch gibt, warum es immer noch Leute gibt, die darauf reinfallen. Es sollte doch langsam bekannt sein. Das Ende des Artikels [klärt auf], es funktioniert immer noch, denn „frage tausend Dumme und du findest einen richtig Dummen“ und die fallen auf sowas rein. Deshalb läuft das immer noch. Wie heißt es immer so schön, jeden Tag steht ein Dummer auf. Es ist nicht so, dass die Masche so schlecht ist oder so dumm ist, dass die eigentlich gar nicht funktionieren kann, sondern die funktioniert halt auch nur bei Dummen.

A: [Da greift das] Zitat: Die Menschheit will betrogen werden, drum sei sie betrogen. Das trifft eigentlich den Nagel auf den Kopf. Man findet immer irgendjemanden, der darauf reinfällt.

Ok ich glaube wir haben den Rahmen zeitlich doch ziemlich gut gesprengt. Gibt es trotzdem noch irgendwas, was du dem Gespräch beifügen möchtest. Etwas, wo du sagst, das muss unbedingt mit rein?

ITE: Über die Frage hätte ich wahrscheinlich vorher mal drüber nachdenken müssen. So auf die Schnelle nichts.

A: Du hast auch ziemlich viel erzählt, ich denke da ist auf jeden Fall eine ganze Menge dabei, was zur „Aufklärung“ beitragen wird, ohne Frage. Ich nehme das jetzt als nein?

ITE: Nein, ja, so auf die Schnelle nein.

A: Gut, dann danke ich dir nochmal recht herzlich und würde die Aufnahme beenden.

Anhang 6.5: Transkript – Interview – JU

A: Hallo Frau Staatsanwältin, herzlichen Dank für die Gelegenheit. Dann wollen wir gleich anfangen. Erzählen Sie mir bitte von sich. Welche Funktionen nehmen Sie bei den Ermittlungen bzw. bei der Strafverfolgung ein und welche Aufgaben erfüllen Sie in diesem Bereich?

JU: Ich bin Abteilungsleiterin und leite die Abteilung die sich [unter anderem] mit Cybercrime beschäftigt. In dieser Abteilung bekommen wir insbesondere Ermittlungsverfahren, die sich dem Betrugsphänomen Cybertrading/Fraud widmen. Wir haben in der Abteilung circa sechs Staatsanwälte, die diese Verfahren bearbeiten.

A: Was machen Sie so, wie sieht ein typischer Alltag bei Ihnen aus?

JU: Die Anzeigen [kommen] zum Teil direkt über Anwälte oder über die Betrugsgeschädigten zur Staatsanwaltschaft oder werden bei der Polizei erstattet. Die Polizei ermittelt in den angezeigten Verfahren und legt [diese] nach Abschluss oder im Rahmen der Ermittlungen der Staatsanwaltschaft vor. Soweit die Anzeigen direkt bei der Staatsanwaltschaft erfolgen, werden die Anzeigen hier erfasst und werden dann der Polizei vorgelegt, mit entsprechendem Ermittlungsauftrag.

A: Also sind Sie praktisch die obere Instanz, die dann gewissermaßen die Fäden zieht und leitet?

JU: Wir sind nicht die obere Instanz, sondern wir arbeiten mit der Polizei zusammen. Die Ermittlungen zu diesem Kriminalitätsphänomen, wie auch alle anderen Ermittlungen, werden durch die Polizei geführt. Wenn die Ermittlungen abgeschlossen sind oder Ermittlungsschritte notwendig sind, z.B. Beschlüsse, die durch den Ermittlungsrichter verfasst werden müssen, also wo eine Beteiligung der Staatsanwaltschaft oder des Gerichts erforderlich ist, da beteiligen wir uns an den Ermittlungen. Die Staatsanwaltschaft ist gesetzlich vorgesehen die „Herrin des Ermittlungsverfahrens“. Das heißt die Staatsanwaltschaft führt die Ermittlungen, natürlich immer in Zusammenarbeit mit der Polizei, weil sie die Erkenntnisse aus den Verfahren hat.

A: Wie lange befassen Sie sich bereit mit dem Straftatphänomen Cybertrading, wenn Sie jetzt schätzen müssten?

JU: Seit 2019 circa.

A: Also seit das so richtig aufgekocht ist, seit die ersten Fälle aufgetaucht sind.

JU: Ja. Ich erinnere mich daran, 2019 ist ein Kollege vom LKA auf mich zugekommen, weil diese Straftaten hauptsächlich in den Wirtschaftsabteilungen bearbeitet wurden. Es ist aufgefallen, dass gerade in Sachsen viele Geschädigte bei verschiedenen Polizei-

dienststellen die Taten angezeigt haben und es sich oft um dieselbe Plattform gehandelt hat. Da kam 2019 bereits der Vorschlag, dass diese Verfahren koordiniert werden müssen. Die zweite Frage war, inwieweit man diese Verfahren in den Wirtschaftsabteilungen führen sollte und durch Wirtschaftsdezernate der Polizei oder inwieweit bei den Staatsanwaltschaften die Ermittlungen in den damals speziell eingerichteten Cyberdezernaten zu führen sind und bei der Polizei eben auch durch die IUK-Kommissariate.

Diese Absprachen, die damals in die Wege geleitet wurden, auf diesem Weg befinden wir uns heute noch. Es wird bei uns auch versucht zu koordinieren, dass die Ermittlungen nicht doppelt geführt werden und es wurde auch die Übereinkunft getroffen, dass dieses Phänomen nicht in der Wirtschaftsabteilung bearbeitet wird, obwohl es sich um organisierte Wirtschaftskriminalität handelt, mit Mitteln des Internets. Sondern dass dieses Phänomen durch die Sonderdezernate Cybercrime und die Cybercrime-Kommissariate hauptsächlich bearbeitet wird.

A: Sie haben gesagt die Staatsanwaltschaft ist die „Herrin des Verfahrens“. Wo liegen denn dann die Prioritäten aus Sicht der Justiz, wenn es um die Strafverfolgung geht. Geld wiederkriegen und die Geschädigten damit besänftigen oder Täter fassen, Tätergruppierungen auseinander reißen?

JU: Es gibt keine Priorität. Es geht natürlich immer vornehmlich darum, die Tat aufzuklären und den Täter zu ermitteln und vor Gericht zu stellen. Natürlich [geht es] auch genauso darum, den Betrugsschaden wieder auszugleichen, den durch den Betrug begangenen oder erreichten Vermögensverlust wieder zu nivellieren und das Vermögen dem Geschädigten zurückzugeben. Das sind gleichrangige Ziele der Strafverfolgung und die verfolgen wir auch gleichrangig.

Es hängt davon ab, wo man eher einen Ansatzpunkt hat. Gerade bei dem Betrugsphänomen Cybertrading/Fraud hat man Schwierigkeiten, aufgrund der Verschleierungsmöglichkeiten, die Täter zu ermitteln. Da ist es zumindest eine Chance, wenn die Anzeigen rechtzeitig erstattet werden, möglicherweise zu verhindern, dass Gelder weitergeleitet werden, so dass da etwas abgeschöpft werden kann.

A: Weil Sie gerade die Verschleierung angesprochen haben: Es sind bei dieser Straftat viele Leute beteiligt oder zumindest geht man davon aus, dass es keine Einzelperson ist oder eine kleine Gruppe, sondern dass das genügend Menschen sind die sich da strukturieren. Das geht ja vom Anrufer im Callcenter über einen Finanzdienstleister, die im Hintergrund mit beteiligt sind oder wo die Server stehen. Wie kann man aus Sicht der Justiz bewerten, dass jemand wirklich rechtlich belangt werden kann, weil er daran beteiligt ist? Oder ist das eher schwierig zu beurteilen, weil man das eigentlich gar nicht richtig greifen kann teilweise?

JU: Man muss immer ganz genau prüfen, was derjenige gemacht hat, welche Rolle er bei der Tat gespielt hat. Dann kommt es immer auf den Einzelfall an. Wenn jemand eine

Tradingsoftware entwickelt, die für legale Zwecke verwendet werden kann, diese Software verkauft und ein Betrugstäter diese Software verwendet um Betrugsstraftaten zu begehen, inwieweit man den [Entwickler] belangen kann. Dual Use nennt man das, ein Produkt [zu schaffen], was man sowohl für kriminelle Zwecke als auch für legale Zwecke verwenden kann. Das kann man möglicherweise dann, wenn [der Programmierer] wusste, dass seine Software für kriminelle Zwecke benutzt wird und [er] vielleicht trotzdem noch Wartungsarbeiten für diese Plattform übernommen hat.

Man muss immer genau prüfen, was wusste derjenige und was [hat] er noch gemacht. Wir sehen Anzeigen gegen Banken, gegen Bankmitarbeiter, dass sie der Geldwäsche schuldig sind, weil sie Konten eröffnen und auf diesen Konten Gelder weiterleiten. In der Regel ist ein Bankgeschäft ein neutrales Geschäft und ein Bankmitarbeiter und eine Bank, auch wenn über diese Bank, weil es eine Onlinebank ist, inkriminierte Gelder transferiert werden, heißt es noch lange nicht, dass der Bankmitarbeiter und die Bank Mittäter beim Cybertrading/Fraud sind.

Man muss immer ganz genau untersuchen, welchen Tatanteil hat derjenige und was kann ich nachweisen, was hat er gewusst bei der Tat. Wusste die Person, dass es sich um einen Betrug handelt? Nächstes Beispiel ist der Callcenter-Agent. Der sitzt im Callcenter, ruft die Leute an und sagt denen, [er hat] super Anlagemöglichkeiten. Weiß der Callcenter-Agent, dass die Gelder nicht tatsächlich angelegt werden oder geht er davon aus, dass das echte Geldanlagen sind?

Wir gehen in der Vielzahl der Fälle davon aus, dass die Callcenter-Agenten wissen, dass sie betrügen. Aber auch das kann man nicht einfach sagen, sondern das muss man nachweisen. Die nächste Frage ist, es gibt einen Betreiber des Callcenters, der dieses Haus angemietet hat und das zur Verfügung stellt und da das Personal rekrutiert. Weiß er, was die da machen. Das ist sehr schwierig, das im Einzelfall nachzuweisen und muss es in jedem Einzelfall nachgewiesen werden.

A: Kann es dann sein, wenn man zu viele Zweifel hat, dass dann die Person, angenommen die wäre dann [vor Gericht], freigesprochen werden könnten? Dass es dann daran scheitert?

JU: Das kann immer das Ergebnis von Ermittlungen sein, aber das ist gerade noch gar nicht unser Problem. Aufgrund dieser vielen Verschleierungsmöglichkeiten müssen wir erstmal die Strukturen aufklären und die Personen, die beteiligt sind, ermitteln. Erst dann kommt der nächste Schritt, dass die natürlich angehört werden, dass wir rauskriegen müssen, inwieweit sie tatsächlich vorwerfbar an der Tat beteiligt waren, ob sie Täter waren, ob sie Teilnehmer waren, ob sie Beihilfe geleistet haben oder eben von dem Ganzen nichts wussten und unschuldig sind.

A: Bei den Ermittlungen kommt raus, dass teilweise viele dieser „Unternehmen“ im Ausland sitzen und nicht zwingend in Deutschland. Wie schätzen Sie aus Ihrer Perspektive

den Aufwand ein, den man aus juristischer Sicht im Inland betreiben kann oder muss, um die Straftaten zu verfolgen bzw. die dann im Ausland betrieben werden?

JU: Im Inland gibt es sehr wenige Ermittlungsmöglichkeiten. Hier kann man lediglich die Betrugsopfer befragen und deren technische Geräte auswerten um an IP-Adressen der Täter zu gelangen und die Kommunikation, die die Opfer mit den Tätern geführt haben. Weiterhin kann man Kontoauswertungen im Inland machen.

Wie Sie schon gesagt haben, die Täter agieren aus dem Ausland, das heißt weitere Ermittlungen zu den Callcentern, zu den angemieteten Servern zum Betrieb der Plattform müssen dann im Ausland stattfinden, sodass wir davon ausgehen, dass ein Großteil der Ermittlungen zu diesem Kriminalitätsphänomen über Rechtshilfe im Ausland erfolgen muss.

Dieses Kriminalitätsphänomen ist nicht auf Landesgrenzen beschränkt, das heißt es trifft deutsche Betrugsopfer, genauso wie spanische, französische, Schweizer, österreichische. Und alle Länder machen die gleichen Ermittlungen im Ausland. [Es] sind auch oft ähnliche Länder, aus denen die Täter agieren und da ist es wichtig, dass man diese Ermittlungen bündelt und gemeinsam diese Ermittlungen im Ausland führt. Sonst kann es dazu kommen, dass Deutschland anfängt eine Durchsuchung im Ausland zu machen und damit eine spanische Ermittlung konterkariert, weil sie zwei Wochen später vielleicht noch mit anderen Ergebnissen [dort] hingehen wollten. Dadurch würden die Täter gewarnt werden. Es ist also sehr komplex und bedarf vieler Absprachen.

A: Angenommen man hat eine Tätergruppierung im Ausland lokalisiert, was für Maßnahmen können Sie anregen bezüglich Durchsuchungen, Beschlagnahmen? Gibt es da eine Reihenfolge oder ist das auch wieder fallabhängig?

JU: Genau, das ist fallabhängig. In der Regel versuchen wir im Ausland die dort befindlichen Server zu beschlagnahmen, um sie hier auswerten zu können. Wenn wir Täter identifiziert haben oder Lokalitäten, wo die Täter handeln, dann gibt es die Möglichkeit dort zu durchsuchen. Wenn es einen dringenden Tatverdacht gibt, dann gibt es auch die Möglichkeit Haftbefehle zu beantragen und mit einem entsprechenden Haftbefehl dort hinzufahren und die Täter vor Ort festzunehmen und nach Deutschland ausliefern zu lassen, um sie hier vor Gericht zu stellen.

A: Also aktive Zusammenarbeit dann mit den Behörden?

JU: Es ist keine Zusammenarbeit mit den Behörden. Es sind Durchsuchungsbeschlüsse, Beschlagnahmebeschlüsse und Haftbefehle, die werden durch deutsche Gerichte, also durch den Ermittlungsrichter hier vor Ort ausgestellt und im Wege der Rechtshilfe vollzogen.

A: Also die Anregung kommt von hier und dann wird auf Anregen [der Beschluss umgesetzt]?

JU: Es ist keine Anregung. Die Beschlüsse werden hier ausgestellt. Es gibt Rechtshilfeübereinkommen zwischen allen möglichen Ländern. Dort hat man sich geeinigt, dass Gerichtsbeschlüsse aus Deutschland auch in einem anderen Land, ich sage mal in Albanien, vollzogen werden. Da gibt es dann vereinbarte Wege, wie man das macht. Diese Wege werden gegangen und dann arbeitet man z.B. mit den albanischen Behörden zusammen und kann die in Deutschland erlassenen Beschlüsse auch in Albanien umsetzen.

A: Wie sieht es denn aus, mit Währungen, also mit Geld? Das ist ja nun teilweise auf Onlinebanken oder digital irgendwo sichtbar. Welche Maßnahmen kann man da ergreifen aus juristischer Sicht?

JU: Wenn wir auf Bankkonten Gelder sehen und wir können die als betrügerisch erlangte Gelder identifizieren, dann gibt es die Möglichkeit eines Arrestbeschlusses. Da gibt es auch die Möglichkeit, im Wege eines der europäischen Ermittlungsanordnungen und mit ähnlichem Instrument diesen Arrest im Ausland relativ schnell zu vollziehen. Hinsichtlich Kryptowährungen ist es natürlich nur möglich, diese zu sichern, wenn die bei Exchangern auf Accounts liegen. Es kommt darauf an, inwieweit diese Exchanger direkt mit uns zusammenarbeiten. Im Wege der Rechtshilfe würde man einen Arrest oder bei Kryptowährungen einen Beschlagnahmebeschluss [beantragen], die rechtliche Einordnung ist schwierig. Ist Kryptowährung eine Forderung oder ein Gegenstand?

Einen Arrest erlässt man bei Geldforderungen. Geld auf einem Konto ist lediglich eine Forderung gegenüber der Bank. Eine Kryptowährung, Bitcoin könnte man auch sagen, gegen wen soll das eine Forderung sein? Von daher ist das eher wie ein digitaler Gegenstand. Der Jurist muss sich immer irgendwie behelfen, weil die StPO natürlich relativ veraltet ist und die technischen Entwicklungen heute nicht alle in der StPO wiedergespiegelt werden. Gegenstände werden beschlagnahmt, daher gibt es Möglichkeiten, dass man sagt, man beschlagnahmt das Guthaben bei einem Kryptowährungsanbieter. Man muss versuchen, das im Wege der Rechtshilfe [zu prüfen und umzusetzen], [auch] wenn [der Anbieter im Ausland] sitzt oder manche, wie Binance, die gar keinen Sitz haben.

A: Das schließt tatsächlich sehr passend auf die nächste Frage. Woran scheitern manche Maßnahmen zur Strafverfolgung?

JU: Strafverfolgungsmaßnahmen scheitern gerade in diesem Zusammenhang, wenn es Exchanger gibt, die gar nicht mit der Polizei zusammen arbeiten. Da lohnt sich eine Anfrage nicht, weil möglichweise davon ausgegangen werden muss, dass sie die Accountinhaber informieren und damit das Ermittlungsverfahren gefährden.

Die Maßnahmen scheitern auch an diesem hohen zeitlichen und finanziellen Aufwand. Immer, wenn man im Rahmen der Rechtshilfe tätig ist, müssen die Rechtshilfemaßnahmen in der Sprache des Landes, wo man hin will, geführt werden. Das heißt ich muss das erst übersetzen lassen und muss gewisse Formalien einhalten. [Man] muss das teilweise über das Bundesjustizministerium in ein Land übersenden und das dauert alles sehr lan-

ge. Bis das [Ermittlungsersuchen] dort ist, ist das Geld oft schon weiter. Wenn ich die Erkenntnisse bekomme, bekomme ich die wieder in der Landessprache, lasse die wieder übersetzen und sehe dann, das Geld ist auf das nächste Konto gegangen, im nächsten Land. Dann laufe ich wieder hinterher. Wir können nicht so schnell agieren, wie die Betrugstäter, die ja keine Grenzen haben. Dadurch sind wir sehr oft zweiter Sieger.

A: Sie laufen praktisch den Tätern hinterher und können nur [reagieren].

JU: Genau, also das Problem ist, dass erst wenn die Tat passiert ist, [Anzeige erstattet wird]. Gerade bei diesem Phänomen ist es so, dass die Leute davon ausgehen, sie legen längerfristig Geld an. Es ist nicht so wie beim Fake-Shop, dass das Geld gezahlt wird und drei Tage später ist die Ware immer noch nicht da. Die Leute haben bemerkt, hier [wurden sie] betrogen und gehen zur Polizei. Hier ist es so, dass die Leute ihr Geld anlegen und von den Callcenter-Agenten gesagt wird, jetzt ist es gerade gut und sie müssen noch mehr anlegen. Dann legen die Leute noch mehr an und werden hingehalten. Oft merken sie erst ein Vierteljahr, ein halbes Jahr später, dass sie gar nicht reich sind, sondern Opfer eines Betruges. In dem Moment fangen wir an, dem Geld hinterherzugehen. Die [Täter] haben [allerdings] ein Vierteljahr Vorsprung und das über Landesgrenzen hinweg. Da ist das Geld nicht mehr sicherbar.

A: Also ist es wirklich der große Faktor Zeit und Geld, der ganz große Schwierigkeiten macht.

JU: Ja.

A: Wenn Sie wünschen könnten, was würden Sie am besten ändern lassen wollen oder könnten Sie vielleicht sogar selber ändern, damit man besser dem Ganzen hinterherkommt bei der Bearbeitung solcher Fälle?

JU: Wir brauchen mehr Polizeibeamte für dieses Kriminalitätsphänomen, weil es wirklich ein erheblicher Schaden ist und das sehr umfangreiche, aufwändige Ermittlungen sind, die geführt werden müssen. Die sind nicht vergleichbar mit einem Diebstahl oder Straßenverkehrsdelikt. Das wird aufgenommen, da hat man eine bekannte Person, die wird vernommen und dann wird das abgeschlossen. Hier dagegen muss sich jemand sehr lange mit sehr vielen, theoretisch deutschlandweit, europaweit Geschädigten auseinandersetzen. Das heißt sehr viel ermitteln, sehr viel auswerten und dazu braucht man sehr viel Personal. Das steht derzeit noch nicht zur Verfügung, das ist das eine.

Das zweite [sind die] Landesgrenzen, die uns am Ermitteln hindern. [Das ist] durch das Internet und durch die Bankenöffnung [nicht mehr zeitgemäß]. Dass sich ein Grieche [online aus Griechenland] ein Konto [in Deutschland] aufmachen kann, aber ich nach Griechenland mit der Rechtshilfe sehr aufwändig ermitteln muss. Diese Ermittlungsgrenzen machen uns das Leben auch sehr schwer. Die müssen letztendlich möglichst fallen.

A: Ich habe ja nun Ihren Schreibtisch gesehen, der ist brechend voll mit Akten. Haben Sie das Gefühl, dass das für Sie auch sehr viel Arbeit ist? Könnten Sie sich vorstellen, dass da jemand mehr mit unter die Arme packen kann aus juristischer Sicht?

JU: Wir machen ja nicht nur Cybertrading/Fraud. Wenn wir nur Cybertrading/Fraud machen würden, dann wären wir gut aufgestellt. So haben wir auch eine Vielzahl anderer Verfahren. Das ist aber derzeit in Ordnung, weil letztendlich können wir nur die Ermittlungsverfahren betreuen, die die Polizei bearbeitet. Solange die Polizei so aufgestellt ist, wie sie ist, liegt das glaube ich nicht an der Staatsanwaltschaft. Natürlich ist auch hier vorgesehen, dass es eine Aufstockung gibt, bzw. eine Entlastung an Verfahren, die wir derzeit bearbeiten, um uns auf die großen Verfahren konzentrieren zu können. Bloß das muss erst dann erfolgen, wenn wir auf der Polizeiebene die Ermittlungsunterstützung haben, die wir brauchen. Die Arbeit wird letztendlich bei der Polizei gemacht. Wenn der Sachverhalt aufgeklärt, der Täter ermittelt ist, dann ist es der kleinere Punkt, die Anklage zu schreiben und das Verfahren vor Gericht zu bringen.

A: Das klingt doch alles sehr aufschlussreich. Damit wären wir tatsächlich bei der letzten Frage. Gibt es etwas, was Sie diesem Gespräch beifügen wollen, irgendwas was Ihnen auf der Seele brennt? Anmerkungen, Kritik, nehme ich auch gern entgegen.

JU: Ich glaube es ist einfach sehr schade, dass so ein Phänomen, wo Leute seit 2019 schon Betrugsopfer werden, dass wir in den Ermittlungen so lange brauchen, um uns diesem Phänomen anzunähern. Es kommen ja immer neue Phänomene. Die Justiz und die Polizei als Behördenapparat [sind] relativ schwerfällig, [um] auf solche neuen Straftaten zu reagieren. Das bedeutet, dass es sehr viele Opfer gibt, die sehr viel Geld verloren haben, wo wir nicht hinterher kommen. Das liegt jetzt nicht nur an der Justiz und an der Polizei, das liegt auch an unserem Bankensystem. Das sind auch, denke ich, politische Entscheidungen, die nicht getroffen werden, die vielleicht getroffen werden müssten, was z.B. die Regulierung von Kryptowährungen angeht.

Es ist schade für alle Opfer. Prävention ist vielleicht ein wichtiger Punkt, aber gerade sind wir, denke ich, auf einem guten Weg. Man hört überall in den Medien, dass vor Betrügern im Internet jeglicher Art gewarnt wird. Natürlich wird es immer neue Möglichkeiten geben, vor denen die Leute nicht gewarnt wurden und sie werden dann über diesen Weg Betrugsopfer. Das ist nicht nur Cybertrading/Fraud. Man kann sich nur wünschen, dass wir da weniger schwerfällig sind und unsere eingefahrenen Wege bei Änderungen des modus operandi der Täter, dass wir da schneller darauf eingehen können.

A: Das klingt auf jedem Fall nach einem Ziel, das man verfolgen möchte. Dann ist das das letzte gewesen. Ich danke nochmal herzlich für die Teilnahme und würde die Aufnahme beenden an der Stelle.

Eidesstattliche Erklärung

Hiermit versichere ich an Eides statt, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe.

Sämtliche Stellen der Arbeit, die im Wortlaut oder dem Sinn nach Publikationen oder Vorträgen anderer Autoren entnommen sind, habe ich als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt oder anderweitig veröffentlicht.

Leipzig, 12.08.2022	Antonia Justine Franke	[redacted]
(Ort, Datum)	(vollständiger Name)	(Unterschrift)

Nutzungs- und Verwertungsrechte

Ich übertrage zusätzliche Nutzungs- und Verwertungsrechte für die vorliegende Arbeit und allen damit in Zusammenhang stehenden Daten auf Grundlage der Creative Common Lizenz „CC0“ an alle genannten Betreuer dieser Arbeit.

Leipzig, 12.08.2022 

(Ort, Datum) (Unterschrift)