Das Ausmaß der #BrokerScams in Europa

Die Bedrohung der Europäischen Kleininvestoren durch Online Investment Scams und international agierende Cybercrime Organisationen

Elfriede Sixt[1]

Zusammenfassung

Der monatliche Schaden, der durch Betrug auf Online Trading-Webseiten (in der Folge auch als #BrokerScams oder #InvestmentScams bezeichnet) momentan in Europa an europäischen Kleinanlegern entsteht, beträgt laut Schätzungen bis zu 1 Mrd[2]. Euro pro Monat (!). Wobei es sich nur um eine grobe Schätzung handelt, da es bis dato - 10 Jahre nach Beginn dieser Art von Kriminalität - keinerlei einheitliche Erfassung der Strafanzeigen für diese Art der Verbrechen in den einzelnen europäischen Ländern gibt.

Diese fehlende einheitliche Erfassung verhindert in der Folge jegliche zentrale, effiziente und effektive Strafverfolgung dieser Art von Kriminalfällen innerhalb der einzelnen europäischen Länder, ganz zu schweigen von einer europaweit-koordinierten Strafverfolgung dieser Kriminalfälle.

Damit sind die Europäischen Kleinanleger den global tätigen mafiös organisierten Cyberkriminellen, die hinter den Tausenden im Internet verfügbaren #BrokerScams stehen, hilflos ausgeliefert.

Betrügerische internationale Verbrecherorganisationen, denen durch die lange Untätigkeit der Strafverfolgungsbehörden massive Finanzmittel (12 Mrd. USD * 10 Jahre) zur Verfügung stehen, bauen globale Organisationsstrukturen auf, unter bewusster Nutzung der Unfähigkeit der europäischen Strafverfolgungsbehörden grenzüberschreitend zu arbeiten. Diese kriminellen Organisationsstrukturen umfassen Medienhäuser (vgl. Crypto Daily (gehört Uwe Lenhoff), CryptoVest (gehört Ilan Tzorya), legale und illegale Finanzdienstleistungsunternehmen, eine boomende Call Center-Industrie und Tradingtechnologie-Anbieter, sowie Dienstleister wie Rechtsanwälte und Steuerberater, die die unzähligen involvierten Mantelgesellschaften administrieren. Mittels sogenannter White Label-Lösungen können derartige neue #BrokerScams mit neuen Domains, einem Angebot an verschiedensten Zahlungsdienstleister und der entsprechenden Boiler Room Betreuung binnen 24 Stunden ins Web gestellt werden.

Das Leid und das Verbrechen, das in Europa täglich und offensichtlich von den Medien und der Öffentlichkeit unbeachtet vor sich geht, ist gigantisch.

Die Skrupellosigkeit der Betreiber dieser Systeme ist unbeschreiblich und die gegebene Hybris der Verbrecher basiert auf der Tatsache, dass sie inzwischen jahrelang unbehelligt ihren verbrecherischen Tätigkeiten vor allem in Westeuropa nachgehen konnten.

Das Ausmaß des Verbrechens kann sich jedoch noch erhöhen, da wir beobachten, dass die kriminellen Organisationen vermehrt dazu übergehen für diese Art von Verbrechen Kryptowährungen zu nutzen und damit den Grad der Schwierigkeit für die Strafverfolgungsbehörden noch erhöhen.

---

[1] Wirtschaftsprüferin und Steuerberaterin in Wien, Co-Founder der EFRI-Initiative.

[2] Diese Schätzung basiert auf einer durchschnittlichen Einzahlung eines Kleininvestors von € 1.700,- und einer durchschnittlichen Kundenanzahl von 9.500 pro Brokersystem. Momentan gibt es bis zu 550 betrügerische Webseiten (eine Webseite gilt als #BrokerScam). Die Zahlen basieren auf den beschlagnahmten Kundenlisten der BrokerScams xTraderfx (25.000 Kunden; Durchschnittseinzahlung von € 1.700) und safemarkets (4.100 Kunden; Durchschnittseinzahlung von € 1.400,-), goldenmarkets und getfinancial (für mehr Details bitte kontaktieren Sie uns).

Appell: Die europäischen Länder müssen umgehend erhöhte Anstrengungen in die aktive, effiziente und effektive (damit zumindest europaweit koordinierte) Strafverfolgung dieser Art von Verbrechen legen, jede Digitalisierungsbemühung der europäischen Länder führt sich ansonsten ad absurdum.

Grenzlose Cyberkriminalität

Die zunehmende Digitalisierung der Gesellschaft im Allgemeinen und die damit verbundene Virtualisierung des Geldes im Besonderen bringen eine neue, massive Bedrohung mit sich - die Cyberkriminalität. Die Kombination modernster Technologien mit neuen Marketingmethoden und ein massives Gefälle in der Technologieaffinität der Internetnutzer schaffen eine noch nie dagewesene Ökosphäre für Kriminelle. Traditionelle Verbrechen wie Bankraub oder Autodiebstahl erweisen sich als deutlich weniger lukrativ als cyberkriminelle Aktivitäten.

Cybercrime kennt keine Ländergrenzen. Mittels ausgefeilter Webkampagnen auf den sozialen Medien lassen sich Milliarden von Menschen auf einfachste Art erreichen.

Die Schadenssummen erreichen bei den diversen Onlinebetrugssystemen immense Beträge. Laut der UK *National Crime Agency* machte der Anteil von Cybercrime 2018 bereits mehr als 50% aller gemeldeten Straftaten in UK aus[3]. Laut der UK Financial Conduct Authority (FCA)[4] verursachten alleine die *Investment Scams* in UK im Jahr 2018 GBP 197 Millionen Schaden. Nach den Ergebnissen einer Umfrage der *British Crime Survey* aus dem Jahr 2012 haben 2% der Teilnehmer angegeben, Opfer von traditionellen Straftaten wie Einbruch oder Diebstahl gewesen zu sein. Hingegen gaben bereits 2012 mehr als doppelt so viele Teilnehmer an, dass sie bereits einmal Opfer von Cyberkriminalität waren.

Auch die 2019 von mehreren europäischen Universitäten durchgeführte Studie *Measuring the Changing Cost of Cybercrime*[5] belegt oben dargestellte Fakten:

Die Studie schätzt, dass 2019 bereits 6% der europäischen Bevölkerung Opfer von Cyberkriminalität geworden sind.

Statistisch gesehen ist es heute für Menschen in Europa wahrscheinlicher, Opfer von Cyberkriminalität als von traditioneller Kriminalität zu werden[6].

Wobei festgehalten werden muss, dass die Datenbasis für die Auswertung der Zahlen im Bereich der Cyberkriminalität derzeit noch immer dünn ist. Cyberkriminalität ist für die Statistik wie auch für die Behörden noch immer ein relativ neues Phänomen.

Erkenntnisse der EFRI-Initiative

Die *European Fund Recovery Initiative* mit Sitz in Wien begann im Jänner 2019, Online-Kampagnen zur Wiedergewinnung von Anlegergelder aus verschiedenen **#CyberScams** im Bereich des Online-Tradings (d.h. Investment Scams bzw. **#BrokerScams**) durchzuführen.

Seit Jänner 2019 haben sich über 1.108 Geschädigte auf der Webseite www.efri.io mit einem Gesamtschaden von mehr als 20 Mio Euro registriert. Zu 99% handelt es sich bei den Geschädigten um europäische Kleinanleger im Alter zwischen 50 und 85 Jahren.

---

[3] Office for National Statistics, Crime in England and Wales: year ending March 2019, Link https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2019

[4] FCA warns public of investment scams as over £197 million reported losses in 2018, Link https://www.fca.org.uk/news/press-releases/fca-warns-public-investment-scams-over-197-million-reported-losses-2018

[5] https://www.paccsresearch.org.uk/wp-content/uploads/2019/06/WEIS_2019_paper_25.pdf

[6] European CyberSecurity Month, Link: https://cybersecuritymonth.eu/

Nach Durchsicht der von den Geschädigten übermittelten Sachverhaltsdarstellungen, Schilderungen und Dokumenten wird offensichtlich, dass die bloße Registrierung bei einem #BrokerScam im Regelfall ausreicht, um einen für den Kleinanleger fatalen Kreislauf in Gang zu setzen:

Social-Media-Kanäle dienen als hauptsächlicher Werbekanal

Die Kleinanleger werden durch vertrauenserweckende und ansprechende Werbemaßnahmen auf den sozialen Medien - vor allem Facebook und YouTube- angeworben mit dem Versprechen rascher Gewinne.

Boiler Rooms/Call Center als kritischer Erfolgsfaktor

Nach Registrierung auf den Online Trading-Plattformen erfolgt umgehend eine Kontaktaufnahme durch Call Center Mitarbeiter der Betrugssysteme.

Call Center im Bereich der **#BrokerScams** werden als Boiler Rooms bezeichnet. Deren Mitarbeiter erhalten massive Erfolgsprovisionen von jeder erfolgreichen Einzahlung der Kleininvestoren, sie animieren in der Folge systematisch unter Einsatz professioneller psychologischer Methoden die Kleinanleger zum Transfer immer größerer Beträge.

In Bulgarien, Serbien, Bosnien-Herzegowina sind in den letzten Jahren regelrechte Call Center-Industrien entstanden, die über Mitarbeiter mit verschiedensten Sprachkenntnissen verfügen. Diese Call Center arbeiten mit modernsten Technologien, Datenbanken und Customer-Relationship-Management (CRM)-Systemen.

Psychologen trainieren die Call Center-Agenten, professionelle Schreiber entwickeln die Gesprächsleitfäden und Experten erstellen ausgeklügelte Kundenprofile. Kundendaten werden über verschiedenste Quellen besorgt, Kunden werden segmentiert und entsprechend "bedarfsgerecht" bearbeitet.

Ausgefeilte Technologie als Basis des Betrugs

In den Dashboards der jeweiligen **#BrokerScams** wird den Kleinanlegern mittels falscher modernster Charttechnologie Professionalität vorgegaukelt und vermittelt, dass ihre getätigten Investitionen hohe Gewinne erzielen und die Gelder zu ihrer Verfügung stehen.

In dieser Zeit des Glücksgefühls bauen die Boiler Room-Agenten ein trügerisches Vertrauensverhältnis mit dem vertrauensvollen Kleinanleger auf. Dieses Vertrauensverhältnis wird schlussendlich genutzt, um den Kleinanleger um ihr gesamtes Vermögen zu bringen und sie sowohl finanziell als auch psychisch ausgebeutet zu hinterlassen.

Legale und illegale europäische Zahlungsdienstleister als weiterer kritischer Erfolgsfaktor

Die Einzahlungen der Kleinanleger in die **#BrokerScams** erfolgen

- über Banküberweisungen (offline Cash-Transfers)
- mittels Kreditkartenzahlungen (online Cash Transfers) oder
- zunehmend über Kryptowährungen und Krypto-Zahlungsverkehrsdienstleister.

Für Banküberweisungen ist die Involvierung von europäischen Finanzdienstleistungsinstituten unabdingbar, denn die europäische Kleininvestoren vertrauen auf die Rechtssicherheit des europäischen Finanzmarkts und dieses Vertrauen resultiert darin das hohe Beträge ohne Bedenken überwiesen werden.

Für die Entgegennahme der Investorengelder mittels Banküberweisung kommen zwei Alternativen zur Anwendung

- die Betreiber der #BrokerScams eröffnen Konten bei lizenzierten Fintech-Unternehmen für den Empfang und Weiterleitung der Kundengelder. Beispiele dafür sind Altair Entertainment Ltd, Curacao (WireCard). Von diesen Konten werden die

Gelder in der Folge direkt an Offshore Konten der wirtschaftlichen Eigentümer der Betrugssysteme überwiesen.

- Oder sie bedienen sich der Dienstleistung von Vermittlern illegaler Zahlungsdiensteanbietern: dabei werden systematisch Mantelgesellschaften in Westeuropa gegründet, die über Konten bei renommierten europäischen Banken verfügen. Diese Konten werden zur Entgegennahme von Investorengeldern genutzt, die Gelder werden in der Folge nach Abzug einer Provisionszahlung für die Zahlungsdiensteanbieter an die Offshore Konten der wirtschaftlichen Eigentümer der Betrugssysteme überwiesen. Meist bedienen diese Mantelgesellschaften mehrere Betrugssysteme.

Mantelgesellschaften (aus aller Welt) mit **deutschen** Bankverbindungen werden als "premium Accounts" gehandelt und mit einer hohen Provision versehen.

Totalverlust als Resultat

Sobald die Kleininvestoren ihre Investition samt ausgewiesenen Gewinnen ausgezahlt bekommen haben wollen, verschlechtert sich das Kundenverhältnis unmittelbar. Innerhalb kurzer Zeit wird aus den simulierten Gewinnen ein Totalverlust des Investments. Der Hinweis auf eine unkorrekte Vorgangsweise durch den Kunden wird mit Drohungen, Schließung des Kontos und Nichtmehrerreichbarkeit des Kundenbetreuers beantwortet.

Die Registrierung bei den Betrugssystemen resultiert in 99% aller Fälle in einem Totalverlust der Ersparnisse dieser Kleinanleger. Im schlimmsten Fall sogar mit einer zusätzlichen finanziellen Belastung, da viele Opfer durch falsche Versprechungen und Zusicherungen auch noch zu einer Kreditaufnahme animiert werden.

Wenn offensichtlich ist, dass von dem einzelnen Kleinanleger "nichts" mehr zu holen ist, werden die Kundendaten an andere Betreiber von Online-Trading-Plattformen bzw. an sogenannte *Funds Recovery Organisationen* verkauft. Damit beginnt erneut eine monatelange Belästigung der Geschädigten per email und per Telefon. Unzählige Spam-Emails und Anrufer aus den verschiedensten Ländern der Welt belästigen die Geschädigten noch monatelang.

Diese Recovery Organisationen werden oftmals von denselben Betrügern betrieben wie die Trading-Plattformen, es wird dabei bewusst versucht die Not und Verzweiflung der Betrogenen nochmals auszunutzen. Es wird versprochen gegen die Anzahlung von weiterem Geld, das beim Betrugssystem verlorenen Gelder zurückzuholen. Auch dieses Geld ist in der Folge verloren.

Der Leidensweg geht weiter

Das Drama der betrogenen Kleinanleger ist damit jedoch noch nicht zu Ende, denn nach der für sie bestürzenden und verstörenden Erkenntnis, dass sie möglicherweise 2*mal betrogen wurden, beginnt eine neue Leidensgeschichte für sie: der Gang zu den involvierten Finanzinstituten, Aufsichtsbehörden und Strafverfolgungsbehörden mit der Bitte um Hilfestellung.

Abweisung der Finanzinstitute

Die zahllosen Charge Back-Anträge verzweifelter Investoren bei Kreditkartenunternehmen und Bankinstituten zur Rückholung des Geldes aus solchen Transaktionen werden bestimmt und entschieden zurückgewiesen, meist mit dem Hinweis auf eine Eigenverantwortung bei Investitionen in Online-Gambling Systemen.

Anfragen nach Informationen über die involvierten Zahlungsdienste-Anbieter unter Hinweis auf den erfolgten Betrug werden unter Hinweis auf die Verschwiegenheitsverpflichtung zu 99,9% abgewiesen.

Abweisung der Finanzmarktaufsichtsbehörden

Seit Jahren erhalten die Finanzmarktaufsichtsbehörden in Europa Beschwerden von geschädigten Kleinanlegern. Auf diese Beschwerden von Kleinanlegern wird entweder überhaupt nicht oder mit nichtssagenden und abweisenden Massenemails reagiert.

Ahnungslosigkeit der Strafverfolgungsbehörden

Auch die Meldung des Betrugs bei den Strafverfolgungsbehörden ist frustrierend für die Geschädigten: Das mangelnde Verständnis über das Wesen dieser Cyberkriminalität führt in 99% der eingebrachten Strafanzeigen dazu, dass die gemeldeten Fälle von den regionalen Polizeibehörden in den europäischen Ländern

- entweder überhaupt nicht entgegengenommen werden,
- unmittelbar eingestellt werden - beispielsweise wegen Auslandsbezug (!)
- und als "bewusstes Gambling" abgetan werden.

90% der Geschädigten erzählten, das bereits bei Aufnahme der Strafanzeige der Bearbeiter der Strafverfolgungsbehörde darauf hinweist, dass so gut wie keine Chance besteht, dass die Betrüger gefasst werden und das Geld zurückgeholt werden kann.

Problemlösungsansätze!

Wir haben folgende Lösungsansätze identifiziert, die unmittelbar von den europäischen Regierungen zu ergreifen sind, um dieser Art von Verbrechen Einhalt zu gebieten:

- Die europäischen Länder müssen unmittelbar beginnen erhöhte Anstrengungen in die aktive, effiziente und effektive (damit zumindest europaweit koordinierte) Strafverfolgung dieser Art von Verbrechen legen.
- Es muss von den sozialen Kanälen wie Facebook und YouTube eine Beendigung der betrügerischen Werbung der #BrokerScams verlangt werden - europaweit. Notfalls gerichtlich.
- EU-Länder, die entweder den #BrokerScams erlauben auf ihrem Gebiet tätig zu werden (v.a. Bulgarien, Estland) ebenso wie jenen Ländern deren Finanzmarktaufsichtsbehörden "erleichterten" Zugang zu "Pseudo"lizenzen ermöglichen (Zypern, Malta, usw, Estland und Litauen) ist Einhalt zu gebieten.
- Den EU-Beitrittskandidaten Serbien, Montenegro (momentan Sitz unzähliger Call Center der #BrokerScams) ist der sofortige Stopp der Beitrittsgespräche anzudrohen bei Nichtschließung der hunderten Call Center.
- europäischen legalen und illegalen Zahlungsdienstleistern (fiat und crypto) ist unverständlich klarzumachen, das jegliche Mittäterschaft bei solchen kriminellen Machenschaften als Beitragstäterschaft zu einer kriminellen Vereinigung klassifiziert wird und mit massiven Strafen bedroht ist sowie unmittelbarer Entzug der Lizenz droht.
- unverzüglich ist eine europäische zentrale Strafverfolgungseinheit einzurichten, spezialisiert auf diese Verbrechen wobei eine internationale Zusammenarbeit anzustreben ist.
- eine Medienkampagne auf europäischer Ebene ist zu starten, um die Kleinanleger auf diese Art von Verbrechen aufmerksam zu machen.