Immer öfter fallen Menschen auf die Masche der Betrüger herein, mit wenig Aufwand viel Geld zu gewinnen.

Trügerische Gewinnversprechen

Der Onlinehandel mit Finanzinstrumenten wird bei Anlegern immer beliebter. Diesen Trend machen sich Betrüger zunutze. Sie versprechen hohe Gewinne mit betrügerischen Cybertrading-Plattformen.

Der regelmäßige Austausch von Erkenntnissen und Erfahrungen zwischen Experten des Bundeskriminalamts und des Landeskriminalamts Niederösterreich, mit deutschen und kosovarischen Behörden führte zu einem Ermittlungserfolg. Ermittlungen der Zentralstelle Cybercrime in Bayern und der Kriminalpolizeiinspektion Neu-Ulm führten Ende März 2021 zu einem Schlag gegen ein betrügerisches Cybertrading-Netzwerk, das vorwiegend vom Kosovo aus operierte. In den vergangenen Jahren sind dem Netzwerk Anleger aus ganz Europa in die Fänge geraten – sie wurden um Millionenbeträge betrogen.

Festnahmen. In der Republik Kosovo wurden 18 Tatverdächtige festgenommen und 17 Objekte durchsucht. Die Männer im Alter zwischen 22 und 45 Jahren sollen an betrügerischen Online-Anlage-Plattformen mitgewirkt haben. Für drei der Personen hatte die Generalstaatsanwaltschaft Bamberg bereits im Vorfeld in Kooperation mit der Kriminalpolizeiinspektion Neu-Ulm wegen des Verdachts des gewerbs- und bandenmäßigen Betrugs Haftbefehle erwirkt.

Die Festgenommenen stammen aus der Republik Kosovo, aus Albanien und aus Deutschland. Es handelt sich bei den Tätern zum Teil um Call-Center-Mitarbeiter, die bei deutschsprachigen Geschädigten besonders erfolgreich waren und als vermeintliche Top-Broker für Schäden in Millionenhöhe verantwortlich sein sollen.

Die Ermittler forschten auch die führenden Köpfe aus. Bei Hausdurchsuchungen an den Arbeitsplätzen der Call-Center-Mitarbeiter wurden mitunter detaillierte Anweisungen und Leitfäden für den Kontakt zu den Opfern gefunden. Ferner wurden im Zuge der Durchsuchungen sieben Fahrzeuge sowie 160.000 Euro Bargeld sichergestellt. Bei weiteren Ermittlungen wurden mehrere Konten mit einem Guthaben von 700.000 Euro beschlagnahmt. 240 kosovarische Polizeibeamte waren am Schlag gegen das Betrugsnetzwerk beteiligt.

Zeitgleich kam es in Berlin zur Umsetzung zweier Durchsuchungsbeschlüsse an der Privat- und Geschäftsanschrift eines weiteren mutmaßlichen Mitglieds der internationalen Tätergruppe.

Plattformen. Die Täter, gegen die sich die Maßnahmen in der Republik Kosovo sowie in Berlin richteten, sollen seit 2017 unter anderem die Plattformen *FXCMarkets, FXOptexGroup, Swissinv24, CFXPoint, IForex24, CodexFX, HBCMarket, CapitalGFX, Investment Department, Tradingmarkets24* und *Brokermasters* betrieben haben, teilten die Generalstaatsanwaltschaft Bamberg und das Polizeipräsidium Schwaben Süd/West in einer Presseaussendung mit.

FOTO: GROOVERIDER2/STOCK.ADOBE.COM

Die Software-Lösungen hinter den Cybertrading-Plattformen bieten die Möglichkeiten zur Manipulation von Kursverläufen oder die Simulation von Gewinnen oder Verlusten.

Internationale Betrugsmasche. Der Ablauf des betrügerischen Cybertradings gestaltet sich in den Grundzügen immer gleich. Die Täter spiegeln den potenziellen Kunden vor, digitale Plattformen für den Handel mit unterschiedlichen Finanzinstrumenten zur Verfügung zu stellen. Es werden keine Optionen platziert, eingezahltes Geld wird nicht investiert, es gibt keine Gewinnausschüttung und auch keine Rückzahlung.

„Die für den Kunden sichtbare Handelsplattform ist ebenso wie das angebliche Kundenkonto reine Täuschung. Häufig kommt es nach einzelnen missglückten vermeintlichen Trades zu einem Totalverlust des eingesetzten Kapitals“, erläutert ein Ermittler des Büros für Finanzermittlungen und Vermögenssicherheit im Bundeskriminalamt in Wien. „Wir sprechen dabei von einem Deliktsphänomen, das der internationalen organisierten Cyber-Kriminalität zuzurechnen ist. Zahlreiche Fälle werden gar nicht erst angezeigt, da vielen Anlegern das hohe Verlustrisiko der gewählten Investmentart von vornherein bekannt ist. Der Erfolg des ‚Action-Days‘ in der Republik Kosovo hat gezeigt, wie wichtig die grenzüberschreitende polizeiliche Zusammenarbeit ist, um diesen weltweit operierenden Betrugsnetzwerken auf die Schliche zu kommen.“

Werbung mit Prominenten. Veranlagungen und Depots bei Online-Brokern sind nichts Außergewöhnliches mehr. Die Broker verrechnen den Kunden Gebühren für das Depot, die Kontoführung und für jeden Handel. Neben einer Lizenz oder einer Konzession für den Wertpapierhandel besitzen Online-Broker vereinzelt Bankkonzessionen und unterliegen damit der Einlagensicherung.

Falsche Werbung für Anlageprodukte mit Promis wie Lena Meyer-Landrut: Die Sängerin hat damit nichts zu tun.

Das Angebot der Online-Broker wurde im letzten Jahrzehnt zunehmend durch hochspekulative Produkte erweitert. Die Täter erstellen professionell wirkende Trading-Webseiten und geben vor, Broker-Häuser zu sein. Es werden außergewöhnlich hohe Gewinnausschüttungen versprochen. Die Opfer stoßen auf diese Angebote über diverse Webseiten, auf denen eine hohe Rendite für das eingesetzte Kapital angeboten wird. Insbesondere in sozialen Medien und in Online-Ausgaben bekannter Zeitungen wird für Veranlagungen in verschiedene Finanzprodukte geworben. Die Werbung und Seriosität der Plattform wird durch Veröffentlichungen positiver Berichte in Nachrichtenportalen oder sozialen Medien untermauert. Mit der Werbung angesprochene Interessenten finden bei Überprüfungen in Suchmaschinen vorerst nur positive Nachrichten und Bewertungen. Schließlich registrieren sie sich mit ihren Kontaktdaten auf der beworbenen Webseite.

„Mit falscher Berichterstattung wird ihnen suggeriert, dass auch prominente Persönlichkeiten derartige Trading-Plattformen nützen würden und damit ihr Vermögen erworben hätten“, erklärt

Fotos: leungchopan/Stock.adobe.com, Screenshot

Online-Werbungen sind mit Webseiten von betrügerischen Online-Plattformen oder Broker-Häusern verlinkt. Wer sich registriert, wird von Callcenter-Agents angerufen.

Ministerialrat Mag. Dr. Gerald Rak, MA MSc. Er leitet das Büro für Finanzermittlungen und Vermögenssicherung (Büro 7.2) im Bundeskriminalamt.

Hintermänner und Täter. Früher wurde hauptsächlich mit Insider-Tipps für lukrative Aktien geworben. Heutzutage werben unseriöse Broker-Häuser mit Wetten auf ein Währungspaar (Forex bzw. FX), Differenzkontrakte (Contracts for Difference – CFDs) und binäre Optionen auf Aktien, Rohstoffe, Indizes, Währungen und Kryptowährungen. „Zahlreiche Online-Werbungen sind mit Webseiten von betrügerischen Online-Plattformen oder Broker-Häusern verlinkt. Auf derartigen Seiten geben Interessenten bei der Registrierung ihre Kontaktdaten an und werden in der Folge von Callcenter-Agents angerufen und von ihnen betreut. Bei Interesse erhalten sie nach der Registrierung auf der Webseite ein mit einem Passwort geschütztes Anlagekonto für die vermeintlichen zukünftigen Finanzgeschäfte. Die für die Überweisungen der Opfer bekannt gegebenen Bankkonten lauten zumeist auf im Ausland existierende und eigens für diesen Zweck gegründete Gesellschaften, die einen von der Plattform abweichenden Namen haben“, erklärt Rak. „Die von den Opfern eröffneten und über die Täter-Webseite oder per Handy-App online einsehbaren Veranlagungskonten weisen – solange keine Auszahlung verlangt wird – regelmäßig Gewinne aus. Genau das verleitet die Geschädigten zu weiteren Überweisungen auf verschiedene ausländische Bankkonten, die ihnen von den Tätern bekannt gegeben werden. Die Gelder landen in einem Geldwäschenetzwerk mit Weiterüberweisungen auf andere Konten und Wallets für Kryptowährungen. Die Opfer verlieren dabei häufig ihr eingesetztes Kapital.“

Die unmittelbaren Täter in den Callcentern werden hauptsächlich aus der Bevölkerung im ehemaligen Jugoslawien und aus dem osteuropäischen Raum angeworben. Die Callcenter-Agents verwenden in der Regel gut klingende englische oder deutsche Namen, um ihre wahre Identität zu verschleiern und ein seriöses Image der Plattform vorzutäuschen. Die Hintermänner und Drahtzieher errichten oberhalb der Callcenter-Ebene häufig unternehmensähnliche Strukturen.

Manipulation von Kursverläufen. Diese Plattformen, genauer gesagt die Software-Lösungen dahinter, bieten unter anderem die Möglichkeiten zur Manipulation von Kursverläufen oder die Simulation von Gewinnen oder Verlusten. „Die findigen Betrüger betreiben neben den Webseiten speziell dafür eingerichtete Callcenter, in denen bis zu 100 Callcenter-Agents arbeiten. Damit die Ermittlungsbehörden die Täter nicht so einfach ausforschen oder die Standorte der Callcenter lokalisieren können, bedienen sich die Kriminellen zahlreicher technischer Verschleierungsmaßnahmen. Die Callcenter werden überwiegend in Niedriglohnländern eingerichtet, in denen potenzielle Angestellte mit Sprachkenntnissen rekrutiert werden können“, schildert ein Kriminalbeamter des Landeskriminalamtes Niederösterreich, der sich seit 2017 mit dieser Betrugsform auseinandersetzt. „Die Täter setzten zudem immer häufiger auf Kryptowährungen, um die Geldflüsse zusätzlich zu verschleiern, was die Ermittlungsarbeit der Strafverfolgungsbehörden erschwert.“ Webdesigner gestalten für die Täter Webauftritte, die sehr professionell und fast immer mehrsprachig ausgestaltet sind. Die Anonymität, die das Internet zweifellos bietet, ermöglicht es den tatsächlichen Betreibern der Webseiten, unerkannt zu bleiben.“

Opfer aus Österreich. Ein 35-Jähriger aus dem Bezirk Melk wurde, nachdem er im November 2020 auf einer Webseite seine Kontaktdaten angegeben hatte, von Unbekannten telefonisch kontaktiert. Diese gaben sich offenbar unter dem Namen „Lorenz, Bergmann und Fischer“ als Broker eines britischen Unternehmens aus und bewegten den 35-Jährigen zu Investitionen in diverse Finanzgeschäfte. Zum einen überwies das Opfer Geld für die Investitionen mittels Banküberweisungen auf ein irisches Konto, zum anderen wurden Beträge auf Bitcoin-Wallets übertragen. Als er sich im Februar 2021 einen Teil der vermeintlichen Finanzgeschäfte auszahlen lassen wollte, jedoch kein Geld erhielt, schöpfte der Niederösterreicher Verdacht. Er erstattete Anzeige beim LKA Niederösterreich. Der Schaden bewegt sich im hohen sechsstelligen Eurobereich.

Strukturierte Ermittlungen. Die kriminalpolizeilichen Ermittler gehen davon aus, dass durch das zögerliche Anzeigeverhalten der Opfer von einer hohen Dunkelziffer auszugehen ist. Die

FOTO: SCREENSHOT

Schäden dürften aufgrund der bisherigen Erfahrungen aus Ermittlungsverfahren mehrere hundert Millionen Euro pro Jahr in Mittel- und Westeuropa betragen. In Österreich kann nach Angaben der Kriminalisten von Schäden in der Höhe von mehreren Millionen Euro jährlich ausgegangen werden – Tendenz steigend.

Datenbank. Zur Verhinderung von „Doppelgleisigkeiten" bei den Ermittlungen und um die Tragweite des Phänomens in Österreich erfassen zu können, wurde vom BK eigens dafür eine Datenbank (CTF) eingerichtet. Diese Faktotum-Datenbank soll die ermittelnden Landeskriminalämter in die Position versetzten, unmittelbar nach der Erfassung einer Anzeige feststellen zu können, ob zu der angezeigten Trading-Plattform (Brand) schon Ermittlungen von anderen Polizeidienststellen in Österreich geführt werden. So können verschiedene Ermittlungen zusammengeführt und auf einen gemeinsamen Nenner gebracht werden.

„Die Aktzusammenführung in einem frühen Ermittlungsstadium, idealerweise noch vor der ersten Berichterstattung an die Staatsanwaltschaft, hat den Effekt, dass Akte, die inhaltlich zusammengehören, von Beginn an von der gleichen Staatsanwaltschaft bearbeitet werden. Dies führt zu einer Verfahrensbeschleunigung. Durch die Zusammenführung mehrerer Ermittlungen können wir auch einen raschen Überblick über den Schaden, der durch einen Brand verursacht wird, gewinnen", erläutert Rak. Die Datenbank ermöglicht den Nutzungsberechtigten in den Landeskriminalämtern im Bedarfsfall eigene Analysen des Datenmaterials anzustellen.

Vom Bundeskriminalamt (Abteilung 4) wird in regelmäßigen Abständen eine Gesamtanalyse der Daten durchgeführt. Den Landeskriminalämtern werden neue Entwicklungen mitgeteilt. Bei diesem Betrugsphänomen hat sich gezeigt, dass durch einen Brand meistens mehrere Länder betroffen und auch mehrere Ermittlungsverfahren anhängig sind.

Die Abteilung 7 im Bundeskriminalamt hat in diesen Fällen die Aufgabe, den internationalen Informationsaustausch sicherzustellen und die Ermittler bei der Organisation von zielführenden Meetings, beispielsweise via Europol, sowie bei der Planung und Koordinierung von operativen Maßnahmen im Ausland zu unterstützen.

Die Täter setzten zunehmend auf Kryptowährungen, um Geldflüsse zu verschleiern.

Prävention. Das Bundeskriminalamt (Büro 1.6 – Kriminalprävention) informiert die Bevölkerung laufend mit Präventionskampagnen über die Gefahren von verlockenden Angeboten oder betrügerischen Investment-Seiten. Menschen sollen sensibilisiert werden, auf bestimmte Warnsignale zu reagieren, um den Betrügern nicht auf den Leim zu gehen.

Präventionstipps findet man auf der Webseite des Bundeskriminalamtes *(www.bundeskriminalamt.at)* unter der Registerkarte „Prävention und Opferhilfe". Es findet regelmäßig ein Informationsaustausch zwischen der Kriminalpolizei und der Finanzmarktaufsicht (FMA) statt, die auf dem Gebiet der Prävention ebenfalls sehr aktiv ist. Die FMA veröffentlicht zum Schutz der Anleger Warnmeldungen über Unternehmen, die in Österreich unerlaubt am Finanzmarkt tätig geworden sind *(www.fma.gv.at/category/news/investorenwarnung)*. Die *International Organization of Securities Commissions (IOSCO)*, bei der auch die FMA Mitglied ist, betreibt ein Portal mit Links zu den offiziellen Warnmitteilungen ihrer Mitgliedsländer. Waren es 2018 noch 1.038 Warnmitteilungen, die veröffentlicht wurden, hat sich 2020 die Anzahl mit 2.471 Warnmitteilungen mehr als verdoppelt. Die größte Sammlung zu weltweiten offiziellen Warnmitteilungen der verschiedenen Finanzmarktaufsichtsbehörden findet man unter *www.gmlitigationassistance.com/de/weltweite-warnungen-b.shtml*.

Anleger sollten sich die Webseite ihres Brokers genau ansehen und überprüfen, ob dieser eine in Österreich gültige Konzession für sein Angebot hat. Diese Information findet man im Impressum. Wichtig ist auch zu recherchieren, ob eine Gesellschaft am angegebenen Sitz existiert. Betrügerische Webseiten erkennt man häufig an der erst kürzlich durchgeführten Registrierung der Domain. Herausfinden lässt sich das über den Zeitstempel der Registrierung, der bei einer WHOIS-Anfrage angezeigt wird.

Neben der FMA bieten auch die Präventionsplattformen *www.watchlist-internet.at* oder *www. ombudsstelle.at* Informationen, Checklisten und häufig gestellte Fragen und Antworten rund um die Thematik des Cybertrading-Frauds an. *Gernot Burkert*

Fotos: WrightStudio/Stock.adobe.com