

Kampf gegen Online-Anlagebetrug

Von Krypto-Scams bis Pig-Butchering und falsche Finfluencer: Online-Anlagebetrug geschieht in Österreich immer häufiger. Die Finanzmarktaufsicht, das Bundeskriminalamt und das Europäische Verbraucherzentrum haben eine gemeinsame Aufklärungskampagne gestartet.

Dem Anlagebetrug fallen nicht nur unvorsichtige Personen zum Opfer. Die aktuellen Täuschungsmodelle sind professionell gestaltet, technisch gut umgesetzt und psychologisch durchdacht. Sie reichen von gefälschten Handelsplattformen bis zum Aufbau persönlicher Beziehungen, in denen Vertrauen schrittweise als Druckmittel genutzt wird. Der Schaden entsteht selten in einem einzigen Moment, meist geht ein Prozess voran – vom ersten Kontakt über mehrere Zahlungsstufen bis zum Zeitpunkt, an dem Auszahlungen nicht mehr möglich sind.

Die Fallzahlen und die Schadenssummen zeigen einen deutlichen Trend: Für 2021 bis 2024 wurden über 10.000 Fälle mit einem Schaden von 300 Millionen Euro angezeigt. Vor allem die Schadenssummen haben zugenommen: von 50 Millionen Euro 2021 über 60 Millionen im Folgejahr, 75 Millionen 2023 und 110 Millionen Euro 2024. Angesichts dieser Entwicklung haben die Finanzmarktaufsicht (FMA), das Bundeskriminalamt (BK) und das Europäische Verbraucherzentrum (EVZ) eine gemeinsame Aufklärungskampagne gestartet.

Gemeinsame Antwort. Weil Anlagebetrug häufig international organisiert ist, ist es notwendig, Zuständigkeiten festzulegen. Das BK bündelt kriminalpolizeiliches Know-how, koordiniert komplexe Verfahren und setzt auf strukturierte Prävention, um Warnzeichen früh zu erkennen. Die FMA ergänzt den Ansatz, indem sie unerlaubte Finanzdienstleistungen sichtbar macht, Warnhinweise veröffentlicht und eine Orientierung für Konsumentinnen und Konsumenten bietet.

Eine weitere Rolle übernimmt das Europäische Verbraucherzentrum (EVZ), das grenzüberschreitende Beratungsfälle bündelt, Entwicklungen früh erkennt und Betroffene bei den nächsten Schritten unterstützt. Da Tätergruppen oft in mehreren Ländern agieren, ist eine internationale Zusammenarbeit wichtig: Vernetzung und Informationsaustausch mit Partnerbehörden sowie



Krypto-Betrug: Dashboards, Kursgrafiken und Gewinnanzeigen vermitteln den Eindruck eines echten Tradingkontos

mit Europol und Interpol sollen Strukturen, Zahlungswege und Infrastruktur zusammenführen.

Fake-Trading und Krypto-Investments. Ein verbreitetes Muster beginnt mit Online-Werbung oder scheinbar redaktionell aufgemachten Inhalten. Der Einstieg ist niederschwellig und beginnt mit der Registrierung und einem „Probeinvestment“. Anschließend erfolgt der Kontakt durch eine angebliche Beraterin bzw. Berater. Entscheidend ist die Inszenierung auf der Plattform: Dashboards, Kursgrafiken und Gewinnanzeigen vermitteln den Eindruck eines echten Handelskontos.

Tatsächlich werden Werte simuliert oder manipuliert. Kleine Erfolge zu Beginn dienen der Vertrauensbildung und teilweise werden geringe Auszahlungen zugelassen, um Seriosität vorzutäuschen. Später werden für Auszahlungen plötzlich „Gebühren“, „Steuern“, „Sicherheitsleistungen“ oder „Verifizierungen“ verlangt. In vielen Fällen spielen Fernwartungstools eine zentrale Rolle. So erhalten die Täter unter dem Vorwand, technische Unterstützung leisten zu wollen, Zugriff auf die Geräte ihrer Opfer und können

Transaktionen tätigen. Am Ende steht der vollständige Kontaktabbruch, während das Geld bereits über Zahlungsdienstleister, verschiedene Konten oder Krypto-Transfers weitergeleitet wurde.

Pig-Butchering. Eine weitere, für Betroffene belastende Variante setzt weniger auf den schnellen „Investment-Impuls“, sondern auf Beziehung und Bindung. Die Täter knüpfen über soziale Netzwerke, Messenger oder Dating-Plattformen Kontakte und investieren Zeit in den Aufbau von Vertrauen und Nähe. Der spätere Geldbezug wirkt dann nicht wie ein Verkaufsgespräch, sondern wie ein Schritt innerhalb einer scheinbar persönlichen Beziehung. Die „Anlage“ wird als exklusiv beschrieben. Auch hier können gefälschte Plattformen zum Einsatz kommen, psychologisch ist der Hebel ein anderer: Scham, Loyalität und Hoffnung führen dazu, Warnzeichen erst (zu) spät zu erkennen oder zu verdrängen.

Recovery-Scam. Nach einem ersten Betrug folgt nicht selten ein zweiter. Betroffene werden von angeblichen

Rechtsanwaltskanzleien, Behörden oder Finanzdienstleistern kontaktiert, die behaupten, dass das verlorene Geld rückholbar sei. Voraussetzung sei lediglich, eine Vorauszahlung. Dass die Ansprechpersonen Details kennen, ist kein Beweis für Seriosität, sondern oftmals die Folge von Datenweitergabe innerhalb krimineller Netzwerke.

Pump-and-dump-Manipulationen

werden häufig an der Börse festgestellt. Dabei kaufen Täter zunächst sehr günstige Aktien, treiben den Kurs durch Verbreitung falscher oder irreführender Informationen künstlich nach oben und verleiten andere zum Kauf. Potenzielle Anlegerinnen und Anleger erreichen die Täter über Social-Media-Kanäle, Cold Calling, Spam-Mails oder Empfehlungen in Börsenbriefen. Sobald der Kurs stark gestiegen ist, verkaufen die Manipulanten ihre Aktien mit Gewinn, während Kleinanlegerinnen und -anleger oft auf ihren wertlosen Aktien sitzen bleiben.

Unseriöse Finfluencer. In sozialen Netzwerken können sich Informationen schnell verbreiten und eine breite Mas-



Pig-Butchering: Täter ködern Opfer über soziale Netze oder Dating-Plattformen, um ihnen Geld abzuluchsen

se erreicht bzw. beeinflusst werden. Finfluencer sind Personen, die Finanzinhalte mit ihrer Community teilen, ohne dass dahinter zwingend eine Ausbildung oder eine regulierte Finanzdienstleistung steht. Dabei gibt es mehrere Risiken: Inhalte sind oft stark vereinfacht dargestellt oder auf Aufmerksamkeit getrimmt, sprechen Emotionen an und können zu vorschnellen Entscheidungen verleiten.

Häufig ist nicht klar, ob hinter den Empfehlungen ein Eigeninteresse steht, wie etwa bezahlte Kooperationen oder Provisionen über Links. Manche der beworbenen Finanzprodukte und Stra-

tegien wie CFDs, Kryptos oder Copytrading sind hochriskant und können zu einem Totalverlust führen.

Auffällig ist die Arbeitsteilung der Täter: Callcenter-Strukturen mit Rollen wie „Agents“, „Manager“ und Backoffice für IT, Zahlungsabwicklung und Dokumentenfälschung sowie das Zukaufen von Spezialleistungen (Crime as a Service) wie etwa Programmierer für Plattformmanipulationen oder Werbenetzwerke für aggressive Kampagnen. Dieses Vorgehen macht Betrug skalierbar und erklärt, warum einzelne Muster parallel in vielen Varianten auftauchen.

Ist ein Deliktsfeld so stark prozessgetrieben, muss auf Information und Prävention gesetzt werden. So ist es wichtig, Lizenzen zu prüfen, Warnhinweise ernst zu nehmen, Fernwartung nicht zuzulassen, bei Auszahlungsblockaden besonders skeptisch zu sein und bei „Recovery“-Angeboten von einem hohen Risiko auszugehen. Ebenso wichtig ist die frühe Sicherung von Belegen. Kommunikationsverläufe, Zahlungsdaten, Wallet-Adressen und Transaktionsdetails helfen den Ermittlungen erheblich. *Romana Tofan*