Milliardenschaden. Wiener Forscher haben ausgerechnet, dass Kryptobetrüger seit 2017 30 Milliarden Dollar erbeutet haben. Die Dunkelziffer dürfte noch viel höher sein

Wenn die Kryptofalle zuschnappt

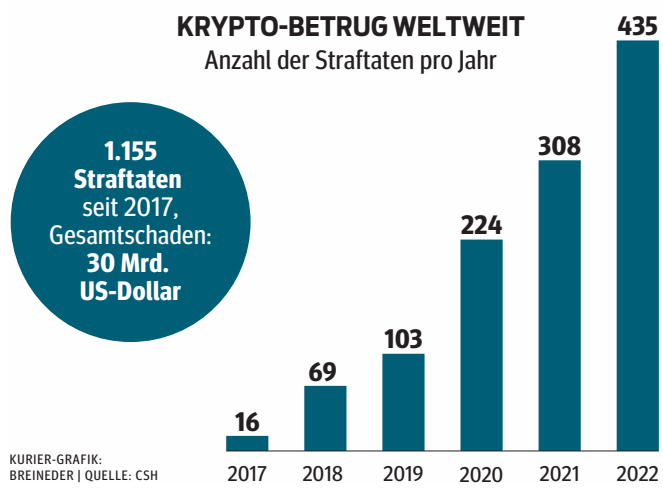
VON **MARKUS STROHMAYER**

Mundpropaganda war es, die einen Kärntner dazu brachte, 10.000 Euro in die ehemalige Kryptoplattform EXW zu investieren. Geld, das der Mann nie wieder sehen wird. Die einstigen Betreiber stehen derzeit nämlich in einem Mega-Betrugsprozess in Klagenfurt vor Gericht. Sie sollen 40.000 Investoren hinters Licht geführt haben. Und trotzdem meint der Investor, der um Tausende Euro erleichtert wurde: „Ich hatte Glück. Ich kenne andere, die ihre Altersvorsorge in dieses System gesteckt haben und nun wohl durch die Finger schauen."

Dass der Mann sich glücklich schätzt, überrascht nicht, geht es in dem Prozess doch um Schäden von 100 Millionen Euro. Und selbst dabei dürfte es sich nur um einen Tropfen auf den heißen Stein handeln. Wie eine Wiener Studie des Complexity Science Hub (CSH) jetzt nämlich zeigt, gingen seit 2017 weltweit mindestens 30 Milliarden US-Dollar durch Krypto-Betrügereien verloren.

„Es ist wichtig, zu betonen, dass wir von einer Mindestsumme sprechen", erklärt Bernhard Haslhofer, der am CSH die Forschungsgruppe „Cryptofinance" leitet. Die Wissenschaftler haben erstmals alle global dokumentierten Straftaten im Kryptobereich zusammengetragen. Ausgewertet wurden 1.155 davon.

Dass die Dunkelziffer höher ist, glaubt man auch bei der Finanzmarktaufsicht (FMA), wo der Schaden im Zusammenhang mit Kryptobetrug in Österreich von Jänner bis September mit durchschnittlich 42.000 Euro pro Fall beziffert wird. Dabei handle es sich jedoch nur um die angezeigten Fälle. Viele Menschen würden aus Scham gar nie bei der Polizei vorstellig werden, heißt es seitens des Bundeskriminalamts. Auch dürften viele Betrogene zunächst nicht bemerken, dass sie Opfer Krimineller wurden.



Mensch stößt an Grenzen

Die Studie zeigt zudem die vielen Facetten des Kryptobetrugs. „Einerseits haben wir seriöse Anbieter, die das Investment ihrer Anleger durch technische Schwächen gefährden", kritisiert Haslhofer. Das sei etwa bei Hackerangriffen der Fall. Andererseits gebe es Anbieter, die wissentlich manipulierte Kryptowährungen handeln, um Menschen abzuzocken. „Da ist eine Hintertür eingebaut, durch die Täter Gelder abziehen." Mithilfe von künstlicher Intelligenz wie ChatGPT könne mittlerweile fast jeder Kryptowährungen erstellen.

Letztlich sei es aber nicht so wichtig, ob Menschen mit Absicht um ihr Erspartes gebracht werden oder ein Systemversagen vorliegt, findet Studien-Co-Autorin Masarah-Cynthia Paquet-Clouston von der Universität Montreal. „Entscheidend ist, dass das Geld unwiederbringlich verloren ist und wir bei diesen komplex verschachtelten Finanzprodukten mit menschlichen Kapazitäten derzeit kaum Möglichkeiten haben, den Weg des Geldes zu verfolgen", ergänzt Haslhofer.

Aktuell zeigt das der Fall der US-Kryptohandelsplattform FTX. Deren Gründer Sam Bankman-Fried muss derzeit in New York vor Gericht erklären, wohin bis zu neun Milliarden Dollar verschwunden sind. Am CSH ist die aktuelle Studie deshalb der Startschuss für ein Projekt, das verschleierte Krypto-Zahlungsströme nachverfolgbar machen soll. In den kommenden zwei Jahren möchte das Wiener Forscherteam forensische Methoden entwickeln, um Kriminellen künftig das Handwerk zu legen.

Wie man sich vor Krypto-Betrug schützen kann

Kriminelle nutzen zunehmend Kanäle wie Dating-Apps oder Messaging-Dienste, um ihren Opfern Geld zu entlocken

VON **PATRICK DAX**

Wenn die Bekanntschaft auf der Dating-Plattform Tinder plötzlich beginnt, von guten Anlagemöglichkeiten zu erzählen, sollte man hellhörig werden. Auch wenn man von vermeintlichen Anlageexperten oder selbst ernannten „Finanz-Gurus" auf Chat-Apps wie Telegram kontaktiert wird oder eine Einladung in eine entsprechende Gruppe erhält, sollten die Alarmglocken schrillen.

Zuletzt seien Betrüger zunehmend dazu übergegangen, die Anbahnungen von dubiosen Geschäften auf privatere Kanäle zu verlagern, sagt Thorsten Behrens von der Watchlist Internet, einer unabhängigen Informationsplattform zu Internet-Betrug.

Sie versuchen, ein Vertrauensverhältnis zu ihren Opfern aufzubauen, und leiten sie dann zu betrügerischen Anlageplattformen weiter. Dort werden Anlegern, die anfangs meist nur kleine Summen eingezahlt haben, hohe Gewinne vorgegaukelt. So sollen sie dazu gebracht werden, den Einsatz zu erhöhen. Probleme treten spätestens dann auf, wenn sie versuchen, sich Gewinne oder ihr Guthaben auszahlen zu lassen.

Die Betrugsopfer werden dann nicht nur davon abgehalten, sondern auch dazu überredet, noch mehr zu investieren. Bis schließlich das Geld weg ist. Oft werden für die betrügerischen Plattformen auch individuelle Internet-Adressen für die jeweiligen Opfer erstellt. Das mache es schwieriger, vor ihnen zu warnen, sagt Behrens.

Betreiber überprüfen

„Was zu gut ist, um wahr zu sein, ist auch nicht wahr", heißt es aus der Finanzmarktaufsicht (FMA). Hat man eine vermeintlich lukrative Anlageplattform vor sich, sollte man auf jeden Fall nachsehen, wer sie betreibt. Ist das nicht eruierbar, sollte man die Finger davon lassen, rät Behrens. Sind die Daten vorhanden, sollte man überprüfen, ob die Betreiber auch über entsprechende Berechtigungen verfügen bzw. ob sie von der FMA beaufsichtigt wird. „Ist das nicht der Fall, Hände weg", sagt ein FMA-Sprecher.

Neben einer Unternehmensdatenbank, über die das überprüft werden kann, hat die FMA auch eine mehr als 900 Einträge umfassende Liste mit Investorenwarnungen online. Viele davon sind Krypto-Unternehmen. Auch auf der Watchlist Internet werden fast 700 Internet-Adressen im Zusammenhang mit Finanzbetrug gelistet.

Seit die Kurse von Kryptowährungen stark gesunken sind, haben auch andere Anlagethemen bei Betrugsversuchen Konjunktur, erzählt Behrens. Derzeit werde etwa verstärkt für Investitionen geworben, bei denen Künstliche Intelligenz (KI) für hohe Gewinne sorgen soll.

Was tun im Schadensfall? Den Kontakt abbrechen und sofort Anzeige erstatten. Die Plattformen sollten auch bei der FMA und der Watchlist Internet gemeldet werden. Man sollte sich auf keinen Fall auf Vorschläge einlassen, bei denen man aufgefordert wird, noch einmal etwas zu bezahlen, um Geld zurückzubekommen, sagt Behrens.

Hüten sollten sich geschädigte Anleger auch vor Folgebetrug. Dabei werden die Opfer von den Betrügern nach einiger Zeit erneut kontaktiert. Diesmal geben sich die Kriminellen als Behörden aus und stellen in Aussicht, bei der Rückholung des Geldes zu helfen. Häufig wird dabei neuerlich Geld verlangt und auch eine Ausweiskopie angefordert. Beides sollte man ignorieren.