Die Masche der Bitcoin-Betrüger

Der Boom der Kryptowährungen wird immer öfter für betrügerische Angebote genutzt. Der Betrug folgt meist bekannten Mustern. Daher sollte man auf bestimmte Anzeichen achten.

Roman Taudes

Geschätzte 2,6 Milliarden Dollar Schaden hat der Betrug mit Bitcoin und Co im Vorjahr weltweit angerichtet.
Foto: EPA / Erdem Sahin

Als Reaktion auf die Finanzkrise im Jahr 2008 geschaffen, ist Bitcoin, ebenso wie andere Kryptowährungen, im Mainstream angekommen. Die anhaltende Kursrallye des Bitcoin, gepaart mit der zunehmenden medialen Berichterstattung, führt dazu, dass immer mehr Kleinanleger in den Kryptomarkt drängen und partizipieren möchten. Dieser Trend blieb auch Betrügern nicht verborgen und wird von diesen schamlos ausgenutzt. Laut der polizeilichen Kriminalstatistik wurden im Jahr 2020 in Österreich über 35.000 Anzeigen im Zusammenhang mit Cybercrime erhoben. Der weltweit entstandene Schaden durch „Crypto Scams" betrug 2020 rund 2,6 Milliarden Dollar, Tendenz steigend. Diese Betrugsfälle folgen meist einer Dramaturgie in drei Akten.

Prolog: Die Anbahnung

Werbebanner auf bekannten Websites, E-Mails mit Interviews von bekannten Persönlichkeiten über ein bewährtes Bitcoinsystem oder Direktnachrichten von attraktiven Menschen auf Datingplattformen: Betrüger nutzen das gesamte Spektrum des Internets auf der Suche nach ihren Opfern. Allen Maschen gemein ist das Versprechen von hohen Gewinnen, ohne Risiko und bereits ab geringen Einzahlungen. Klickt man auf den zur Verfügung gestellten Link, gelangt man auf eine mehr oder weniger aufwendig gestaltete Fake-Investment-Website, die einen zur Registrierung einlädt. Nach erfolgter Anmeldung dauert es nicht lange, bis man von seinem persönlichen „Investment-Manager" kontaktiert und zum ersten Kryptoinvestment überredet wird.

Akt 1: Vorgetäuschte Gewinne

Akzeptiert werden von den Betrügern in der Regel nur Kryptowährungen. Sofern das Opfer noch über kein Konto bei einer Kryptowährungsbörse verfügt, ist der „Investment-Manager" hierbei gern „behilflich". Mittels Fernwartungssoftware (z. B. Anydesk) wird es durch den Prozess „Know Your Customer" (KYC) geführt und ein persönliches Konto angelegt.

Das Opfer soll nun auf das Konto bei der Kryptowährungsbörse Gelder einzahlen, die sofort in Bitcoin gewechselt und an die vom „Investment-Manager" bekanntgegebene Walletadresse transferiert werden. Die auf diese Weise „einbezahlten" Beträge scheinen als Guthaben auf der Fake-Investment-Website auf und werden dem Kontoinhaber als gefälschte Handelsbewegungen sowie erste Gewinne präsentiert. Unter Verweis auf die vermeintlichen Gewinne und verschiedenste weitere Anreize (Bonusprogramme, weniger Gebühren etc.) wird der Geschädigte vom „Investment-Manager" laufend zu höheren Einzahlungen motiviert.

Akt 2: Auszahlungsbetrug

Sobald die Auszahlung der Gewinne gefordert wird und der „Investment-Manager" erkennt, dass keine weiteren Einzahlungen erfolgen, beginnt der Auszahlungsbetrug. Dem Opfer wird vorgetäuscht, dass die Auszahlung des Gewinns selbstverständlich möglich ist. Bevor die Auszahlung allerdings erfolgen kann, müssten von den erwirtschafteten Gewinnen jedoch „Steuern" gezahlt werden. Die Einbehaltung der Steuern vom auszuschüttenden Gewinn ist freilich nicht möglich, sodass der Geschädigte gezwungen ist, neuerliche Einzahlungen vorzunehmen.

Wurden die „Steuern" beglichen, werden weitere Zahlungen abverlangt. Angeblich vereinbarte Provisionen, „Blockchain-Gebühren", Kautionszahlungen an Geldwäschebehörden etc. – die Kreativität der Betrüger ist grenzenlos. Früher oder später erkennt das Opfer, dass es einem Betrug aufgesessen ist, konfrontiert die Betrüger und stellt die Zahlungen ein.

Akt 3: Wiederbeschaffungsbetrug

Aus (falscher) Scham wenden sich viele Opfer nicht an die Polizei oder einen spezialisierten Rechtsanwalt. Stattdessen suchen sie im Internet nach Hilfe und werden schnell fündig. Die Suchanfrage bei Google liefert eine Vielzahl von Anbietern sogenannter „Recovery-Services", die versprechen, Opfern von Bitcoin-Betrügern zu helfen und die transferierten Bitcoins zurückzuholen. Um das Vertrauen des mittlerweile sensibilisierten Geschädigten zu gewinnen, wird neben der verpflichtenden Vorableistung auch ein Erfolgshonorar vereinbart. Die Vorableistung ist natürlich wieder per Bitcoin zu leisten. Nach erfolgter Bezahlung bricht der Kontakt zum „Recovery-Service" ab.

Selbst diejenigen, die nicht im Internet nach Wiederbeschaffungsmöglichkeiten suchen, sind vor dieser Masche nicht gefeit. Betrüger treten auch aktiv mit dem Opfer in Kontakt und bieten ihre „Wiederbeschaffungsdienste" an. Zur Plausibilisierung der Kontaktaufnahme wird erklärt, dass dessen Daten aus einem bereits gelösten Betrugsfall stammen. Da der Anbieter entsprechende Details (Homepage, Name des Trading-Managers etc.) kennt, schöpfen viele Geschädigte nochmals Hoffnung, für die Betrüger wiederum eine Gelegenheit, dies schamlos auszunutzen.

Wie kann man sich schützen?

Wer in Kryptowährungen investieren möchte, sollte sich – wie bei jeder Geldanlage – entsprechend Zeit nehmen und das jeweilige Angebot kritisch hinterfragen. Grundsätzlich gilt: If it's too good to be true ... Werden hohe Gewinne ohne Risiko versprochen oder gar garantiert, ist besondere Vorsicht geboten.

In vielen Fällen ist der Betrug bereits anhand der Angaben auf der Website erkennbar. Zu prüfen ist zuerst das Impressum. Ist keines vorhanden, handelt es sich sehr wahrscheinlich um einen Betrug. Findet sich ein Impressum, empfiehlt sich eine Internetrecherche nach der genannten Gesellschaft. Übertrieben positive Rezensionen täuschen jedoch meist, diese werden häufig von den Betrügern selbst geschrieben. Der Fokus der Recherche sollte auf Betrugswarnungen, insbesondere von Aufsichtsbehörden wie der Finanzmarktaufsicht, liegen.

Woran erkennt man den Betrug?

Steht man bereits mit Mitarbeitern des Investmentanbieters in Kontakt, kann die Art der Kommunikation Hinweise auf Betrugsversuche geben. Seriöse Anbieter kommunizieren nicht über Whatsapp, Telegram oder Signal. Die Verwendung von verschiedenen ausländischen Telefonnummern durch den Anbieter sowie der Umstand, dass diese nicht zurückgerufen werden können, sind ebenfalls deutliche Zeichen für einen Betrugsversuch.

Jedes seriöse Investment ist mit bürokratischem Aufwand in Form von Verträgen, Allgemeinen Geschäftsbedingungen etc. verbunden. Wird kein Vertrag vorgelegt, ist dringend von einem Investment abzuraten. Wird ein Vertrag übermittelt, sollte dieser – auch wenn versichert wird, dass es sich um reine Formalitäten handelt – zumindest sinnerfassend gelesen, besser noch durch einen Experten geprüft werden. Finden sich viele Rechtschreibfehler oder klingt der Text nach Übersetzungsprogramm, sind Zweifel angebracht.

Und niemals sollten Fremden Zugangsdaten zu Bank- oder Kryptowährungskonten überlassen oder der Zugang zum Computer per Fernwartungssoftware gewährt werden.

ROMAN TAUDES ist selbstständiger Rechtsanwalt, spezialisiert auf Anlegerschutz und Kryptowährungen.