expertenReport

Quelle: ronniechua / fotolia.com

Betrugsmasche „Finanzagenten“ immer raffinierter

Die Methoden der Internetbetrüger werden immer ausgefeilter. Neuerdings locken sie mit scheinbaren Arbeitsverträgen als Trader für Kryptowährungen. Welche Schutzmaßnahmen Kontoinhaber und Kreditinstitute ergreifen sollten.

Dr. Stephan Schulz, BKL Fischer Kühne + Partner
Die Kanzlei BKL warnt vor einer besonders trickreichen Masche: Betrüger tarnen sich als Unternehmen im Börsenhandel und schließen mit Finanzagenten scheinbar echte Arbeitsverträge. Man gaukelt den „Angestellten“ vor, sie wären für Transaktionen mit Bitcoins und Co. zuständig. Nach einer gewissen Einarbeitungszeit sollen sie Trader werden. Kandidaten träumen davon, schnell am Handel mit Kryptowährungen teilzunehmen und hohe Verdienstmöglichkeiten zu haben. Damit nicht genug: Betrüger täuschen vermehrt einen Videoanruf zur Identitätsprüfung für den Arbeitsvertrag vor. Dabei wird heimlich per „Video-Ident-Verfahren“ ein Konto für den Bewerber eingerichtet. Über das Konto können die Täter dann sogar ohne Wissen des Finanzagenten Gelder schleusen.

Wer Zahlungen mit fraglicher Herkunft über das eigene Konto abwickelt, macht sich womöglich gleich mehrfach strafbar. Es drohen Strafverfahren wegen Geldwäsche, Betrug oder Hehlerei. Gerade bei gut dotierten Arbeitsverträgen ist Vorsicht geboten. Je enger die Geschäftsbeziehung zwischen Internetbetrügern und Finanzagenten ist, desto eher werden Richter ein fahrlässiges Handeln anzweifeln. Finanzagenten sehen sich dann dem Vorwurf ausgesetzt, dass die Herkunft des Geldes offensichtlich rechtswidrig war und sie sich persönlich bereichern wollten.

Für geschädigte Kontoinhaber sind unberechtigte Abbuchungen ein Schock. Doch sie können oft schnell aufatmen: Wenn es sich um eine unautorisierte Verfügungen handelt, haben sie gegenüber dem Kreditinstitut einen Anspruch auf Wiedergutschrift. Gleichwohl kosten solche Fälle viel Zeit und Nerven. Zusätzliche Schutzmaßnahmen können dazu beitragen, Internetbetrügereien zu unterbinden oder zumindest deutlich zu erschweren. Kontoinhaber sollten ihre Überweisungslimits regelmäßig prüfen und möglichst niedrig ansetzen. Dazu zählen auch die Obergrenzen von bevollmächtigten Personen, wie Ehepartnern. Von zentraler Bedeutung ist auch die sichere Verwahrungen aller Zugangsdaten sowie die Beachtung aller aktuellen Sicherheitshinweise.

Besonders fatal sind die Auswirkungen für Kreditinstitute. Sie müssen bei Phishing-Attacken geschädigten Kontoinhabern das Geld gutschreiben und den Betrag von dem Finanzagenten auf eigenes Risiko wieder einklagen. Schnell stehen Anwalts- und Gerichtskosten in fünfstelliger Höhe im Raum. Obendrein tragen sie ein hohes Insolvenzrisiko, da unter den Finanzagenten viele finanzschwache Personen

sind. Für Kreditinstitute ist es daher besonders wichtig, bereits im Vorfeld wirksame Schutzmaßnahmen zu treffen.

Gerade bei auffälligen Kontoverfügungen sollten Banken vorsichtig sein und die persönlichen Sicherheitsmerkmale nochmal systematisch überprüfen. Gleiches gilt für untypische Kundenanfragen über elektronische oder telefonische Kommunikationsmittel. Sobald eine Kundenbeschwerde über eine unrechtmäßige Verfügung eingeht, sollten Banken umgehend aktiv werden. Sie sollten zügig klären, wohin das Geld transferiert wurde und das empfangende Institut informieren. Nur so gibt es eine Chance, den Geldtransfer eventuell noch zu stoppen. Denn die Zahlungen werden in der Regel schnell weiter transferiert. Gleichzeitig sollten Kreditinstitute unter Beachtung der geldwäscherechtlichen Vorgaben eine Verdachtsanzeige prüfen. Zudem ist in Abstimmung mit dem geschädigten Kontoinhaber eine Strafanzeige ratsam. So können die Betroffenen ihre Rechte wahren und mithelfen, Finanzagenten schneller zu enttarnen.

Autor: Dr. Stephan Schulz, BKL Fischer Kühne + Partner

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4917129/betrugsmasche-finanzagenten-immer-raffinierter/