Das Ende der **Pseudonymität**

Quelle: IDnow GmbH

Von Rupert Spiegelberg

Dass Kryptoanbieter bald Anforderungen in Sachen Kundenidentifizierung erfüllen müssen, gilt als ausgemacht, so Rupert Spiegelberg. Nicht immer ist klar, wann die Vorschriften des Geldwäschegesetzes greifen. Doch gerade deshalb beobachtet Spiegelberg ein wachsendes Interesse der Anbieter an KYC-Lösungen. Die Videoidentifikation ist vielen dabei zu aufwendig. Doch auch beim Verfahren mit der Ausweiskopie werden die Sicherheitsanforderungen wohl bald steigen. In der Schweiz scheint das schon in Kürze anzustehen **Red.**

Als im Dezember 2017 alle Kryptowährungen zusammen erstmals eine Marktkapitalisierung von über 500 Milliarden US-Dollar erzielten, herrschte noch Goldgräberstimmung am Kryptomarkt. Aber nach starken Kurseinbrüchen und vermehrten Berichten über Betrugsfälle unter Anbietern sowie Anlegern hat sich Ernüchterung breit gemacht. Der Druck auf ICOs und Kryptowährungen wächst – vor allem seitens der Regulatoren.

Besonders kritisch wird die Anonymität von Anlegern im regulatorischen Vakuum der Kryptowährungen beäugt. So hat der BaFin-Chef Felix Hufeld unlängst in einem Interview die „Pseudonymität, also die Intransparenz der Teilnehmer, eindeutig [als] das größte Problem," bezeichnet, „das den Einsatz von Kryptotoken zu Geldwäschezwecken oder zur Finanzierung von terroristischen Aktivitäten oder anderen Straftaten in besonderem Maße anfällig macht."

In Anbetracht der allgemeinen Unklarheit darüber, wie die digitalen Währungen regulatorisch gehandhabt werden sollen, werden die internationalen Stimmen nach einer baldigen und eindeutigen Regulierung immer lauter.

BaFin bringt Licht in die regulatorische Grauzone

Wenige Tage nach der schweizerischen FINMA hat sich nun auch die BaFin explizit zu sogenannten Initial Coin Offerings geäußert. In ihrem Hinweisschreiben vom 20. Februar zur „Einordnung von Token beziehungsweise Kryptowährungen als Finanzinstrumente" hat die BaFin auf bestehende Gesetze verwiesen und die Notwendigkeit zur Einhaltung der Geldwäsche- und Finanzgesetzgebung aufgezeigt. Damit sind die Handelsplattformen in Deutschland angehalten, ihre Kunden Geldwäschegesetz-konform zu legitimieren.

Zum Autor

Rupert Spiegelberg, CEO, IDnow GmbH, München

Bei den ICOs gilt es zu prüfen, ob es sich bei den Token um

- ein Finanzinstrument im Sinne des WpHG beziehungsweise der Richtlinie über Märkte für Finanzinstrumente (MiFID II),
- um ein Wertpapier im Sinne des Wertpapierprospektgesetzes (WpPG)
- oder um Vermögensanlagen nach dem Vermögensanlagengesetz (VermAnlG) handelt.

Wenn das Initial Coin Offering die Token als Finanzinstrumente nutzt und somit in den Bereich der Geldwäsche- oder Terrorismusbekämpfung fällt, dann sieht die BaFin ähnlich wie die schweizerische FINMA die Notwendigkeit zur Identifizierung der entsprechenden Person nach den Vorgaben des geltenden Geldwäschegesetzes vor.

Bedarf an Kundenidentifikation im Kryptomarkt

Nach dem Vorstoß der Finanzaufsichtsbehörden in Deutschland und der Schweiz verfolgt die Branche nun mit Spannung den dortigen Kryptomarkt ebenso wie die regulatorischen Entwicklungen in den anderen europäischen Märkten. Derzeit arbeiten die nationalen Regulatoren quasi weltweit mit Hochdruck an entsprechenden Entwürfen. Wie diese genau aussehen und inwieweit sie den gültigen Geldwäsche-

Gesetzen entsprechen werden, bleibt abzuwarten.

Sicher ist, dass für Kryptoanbieter Vorschriften zur Kundenidentifizierung gelten werden und dass die Sicherheitsanforderungen je nach nationaler Regulatorik unterschiedlich streng ausfallen. Dass auch ungeachtet der Regulatorik im Kryptobereich schon heute akuter Handlungsbedarf in puncto Kundenidentifizierung besteht, zeigt der Blick in die Praxis.

Die Kryptoplattformen handeln

Systembedingt sind Kryptowährungen besonders anfällig für Betrugsfälle. Zwar sind die Transaktionen der jeweiligen Blockchain, auf der die Währung basiert, rein theoretisch von allen einsehbar, doch bleiben die einzelnen Netzteilnehmer komplett anonym, solange sie nicht identifiziert werden. Für mehr Transparenz setzen daher vermehrt Kryptoanbieter auf „Know Your Customer" (KYC).

Wann immer ICOs und Kryptoplattformen einem Geldwäschegesetz unterliegen, sind sie wie alle sonstigen Finanzinstitute dazu verpflichtet, ihre Kunden nach den geltenden Vorschriften zu legitimieren. Die Gretchenfrage aktuell: Wann genau ist das der Fall?

Da das im Einzelfall zu prüfen ist und bei Versäumnis der Vorschriftseinhaltung zu hohen Strafen führen kann, lassen schon seit längerem viele Kryptoanbieter ihre Kunden legitimieren, auch wenn sie bis dato noch nicht dazu verpflichtet waren.

So verzeichnet IDnow bereits seit über einem Jahr einen verstärkten Zuwachs an Kryptoplattformen und ICOs, die auf die in vielen europäischen Ländern Geldwäschegesetz-konforme Videoidentifizierung setzen. Allein im Dezember letzten Jahres wurden achtmal mehr Videoidentifizierungen für eine Kontoeröffnung im Kryptobereich durchgeführt als noch 10 Monate zuvor.

Das liegt nicht nur daran, dass das Verfahren Geldwäschegesetz-konform ist und somit dem Sicherheitsbedürfnis von Kryptoanbietern entgegenkommt. Außerdem lassen sich in einem komplett digitalen Prozess deutlich mehr Neukundenregistrierungen in kürzerer Zeit bewältigen als in einem analogen Verfahren.

Sofern unreguliert, ist der Handel mit virtuellen Währungen äußerst lukrativ für Betrüger. Das lässt sich bereits an den Betrugsfällen beim Anmeldeprozess ablesen. So ist Erfahrung die Identitätsbetrugsrate bei Kontoeröffnungen im Kryptobereich viermal so hoch wie bei traditionellen Finanzgeschäften. Bei der Online-Legitimation haben wir es vor allem mit drei Betrugsszenarien zu tun:

- Teil- und Vollfälschungen,
- Ähnlichkeitsbetrug und
- Social Engineering.

Betrugsszenario Social Engineering

Fälschungen, bei denen echte Ausweise manipuliert oder Ausweisdokumente komplett neu erstellt werden, sind alt bekannt und werden in überschaubarer Anzahl praktiziert. Beim Ähnlichkeitsbetrug verwendet ein Betrüger den Ausweis einer ähnlich aussehenden Person für die Identifizierung. Auch hiervon gibt es wenige Fälle, da das Bild auf einem gestohlenen Ausweis dem Aussehen eines Betrügers zumindest ähnlich sein muss.

Das Betrugsszenario, das im Kryptobereich mit Abstand am weitesten verbreitet ist, ist das sogenannte Social Engineering. Hierbei wird eine echte Person unter Vorspiegelung falscher Tatsachen dazu gebracht, zum Beispiel ein Kryptokonto in ihrem Namen zu eröffnen. Die Zugangsdaten gehen dann direkt an den Betrüger. Die Aussichten, mit einem (teil-) gefälschten Ausweisdokument oder mit Social Engineering einen Prüfprozess zu bestehen, sind allerdings so gut wie Null, da einerseits durch die Software-basierte Überprüfung und andererseits dank einer speziellen Fragestrategie des Prüfpersonals solche Fälle de facto immer enttarnt werden.

FINMA kündigt höhere Sicherheitsanforderungen an

Daher haben sich im Sinne der Betrugsprävention und in Erwartung der Regulatorik in Europa derzeit zwei digitale Identifizierungsverfahren bei Kryptoanbietern durchgesetzt: die Identifizierung per Videochat und via elektronischer Ausweiskopie. Denn schon allein die digitale DNA von Kryptowährungen verlangt noch mehr als der konventionelle Bankensektor nach einem vollständig digitalisierten Identifizierungsprozess, der das Betrugsrisiko signifikant senkt. Das Videoverfahren kommt dann zum Einsatz, wenn das Geldwäschegesetz greift. Das Fotoverfahren ist ideal für jene Anbieter, die ihre Kunden sicher, schnell und trotzdem günstig identifizieren wollen.

Auch jenseits des durch das Geldwäschegesetz regulierten Bereichs besteht bei Kryptoanbietern ein Bedürfnis nach mehr Sicherheit und somit der Bedarf an einem Identifizierungsverfahren, das weniger Ressourcen bindet als der GwG-konforme Videoidentprozess. Daher wurde speziell für solche ICOs und Kryptoanbieter die IDnow Crypto-Ident-Lösung entwickelt, die mittels elektronischer Ausweiskopie funktioniert.

Wie die schweizerische FINMA unlängst erklärt hat, wird sie auch beim Identifizierungsverfahren via Ausweisfotokopie die Sicherheitsanforderungen anheben – wahrscheinlich nicht zuletzt mit Blick auf jene ICOs und Kryptoplattformen, die nicht zur Videoidentifizierung verpflichtet sind. Ob via Foto oder Videochat – beide Verfahren setzen an der Achillesferse von Kryptowährungen an und sorgen für mehr Transparenz.