Blockchain-Spur zum Dieb

Kryptobörsen sind Handelsplätze von Kryptowährungen und „beaufsichtigen“ Crypto-Assets von Millionen von Kunden in Milliardenhöhe. Ein attraktives Ziel für Hacker.

Hacker haben es auf Kryptobörsen abgesehen, die ein Milliarden-Vermögen von Kunden verwalten. Von der Kryptobörse *Binance* erbeuteten Cyber-Kriminelle etwa 7.000 Bitcoins. *Binance* ist eine der größten Börsen weltweit mit über 12 Millionen registrierten Kunden. Mit einem täglichen Handelsvolumen von ca. 1,8 Milliarden US-Dollar ist diese Firma die Nummer 1 weltweit. *Binance* verdient an jeder Transaktion ihrer Plattform. Der Jahresgewinn 2018 war höher als jener der Deutschen Bank.

Werden gestohlene Bitcoins bewegt, sind ihre Spuren in der Blockchain jederzeit ersichtlich.

Hot Wallet vs. Cold Wallet. Eine Bitcoin-Wallet ist eine „virtuelle Geldbörse“, die den öffentlichen und den privaten Schlüssel zu den Bitcoins in der Blockchain speichert. Die Blockchain ist eine Art digitales Kassabuch, in dem Einträge unveränderbar gespeichert werden. In unserem digitalen Zeitalter gilt alles online (hot) Zugängliche als permanent gefährdet. Alles offline (cold) Gelagerte hat bessere Sicherheitschancen. *Binance* versichert, über technische und organisatorische Sicherungsmaßnahmen zu verfügen, um milliardenschwere Crypto-Assets (Vermögen in Kryptowährungen) ihrer Kunden zu schützen. Eine dieser Maßnahmen lautet, immer einen gewissen Anteil der Kunden-Assets in Cold Wallets zu sichern. Bei hohen Handelsvolumina wird zwischen Hot und Cold Wallets aus Sicherheitsgründen transferiert.

Dieses Szenario hatten Hacker ausgenutzt. Sie haben laut *Binance* verschiedenste Techniken für den Diebstahl eingesetzt. Dazu zählen Phishingverfahren und eingeschleuste Softwareviren, um Wallet-Adressen zu kontrollieren und Transaktionen tätigen zu können. Durch eine Versicherung von *Binance – SAFU (Secure Asset Fund for Users)* sind finanzielle Schäden für Betroffene in vollem Umfang abgedeckt. Jeder, der seine Kryptowährungen auf einer Kryptobörse oder einem Drittanbieter lagert, vertraut somit deren Technik und Expertise.

Marktauswirkung. Der Bitcoindiebstahl bei *Binance* hat den Bitcoinpreis um 3 Prozent gesenkt. Tage später war dieser Rückgang wieder gut gemacht. Solche Hacks oder Diebstähle sind nicht selten. 2019 hat es die neuseeländische Kryptobörse *Cryptopia* erwischt. Sie ist mittlerweile in der Insolvenz. Einige Hunderttausend Kunden haben ihre Crypto-Assets ohne Versicherung verloren. Der größte Diebstahl war jedoch 2014 der *Mt.-Gox*-Diebstahl mit einem Verlust von über 850.000 Bitcoins. *Mt. Gox* war einer der weltweit größten Handelsplätze für Bitcoins. Damals war die Börse für über 70 Prozent des weltweiten Handelsvolumens verantwortlich und führte zu einem Kursrückgang um ca. 80 Prozent.

Hacker haben es auf Kryptobörsen abgesehen, die ein Milliarden-Vermögen ihrer Kunden verwalten.

Blockchainspur. Kunstdiebe wissen, dass zum Beispiel ein gestohlenes Gemälde nicht öffentlich angeboten werden kann. Bei Kryptowährungen sind alle jemals getätigten Transaktionen in der Blockchain gespeichert und jederzeit einsehbar. Damit ist gewährleistet, dass der Weg der Bitcoins über alle „Konten“ nachvollziehbar ist. Spezielle Softwaresysteme können die jeweiligen Wallet-Adressen der gestohlenen Bitcoins kennzeichnen. Somit könnte verhindert werden, dass Diebesgut auf Kryptobörsen weiterverkauft wird und zugleich die registrierte Person ausfindig gemacht und eine mögliche Spur zu den Tätern gefunden wird.

Die Frage lautet: Wer hat Zugang (technisch und finanziell) zu diesen Softwaresystemen und wer setzt diese tatsächlich ein und ab welchem Zeitpunkt sind diese Informationen von welcher offiziellen Stelle verfügbar? Durch dieses offene „Kassenbuch“ mit allen enthaltenen Transaktionen ist der Bitcoin für kriminelle Machenschaften ungeeignet.

Fotos: Igor Stevanovic/Stock.adobe.com

Sobald die gestohlenen Bitcoins bewegt werden, sind die Spuren für alle sichtbar und an der Schnittstelle zwischen Bitcoin und Euro auffindbar. Anonymität bleibt gewahrt, solange die Bitcoins nicht bewegt werden. Jede Transaktion gibt einen weiteren digitalen Hinweis auf den oder die Täter. Wer im Darknet z. B. Cannabis für 50 Euro in Bitcoins verkauft, stellt für den Käufer eine Bitcoin-Wallet-Adresse zum Zahlungsempfang zur Verfügung. Der Käufer überweist und sollte die Ware geliefert bekommen. Diese Transaktion ist auf ewig in der Blockchain gespeichert.

Der Diebstahl von Bitcoins würde sich nur lohnen, wenn die Crypto-Assets so schnell wie möglich wieder zu echtem Geld gemacht würden. Es ist sehr schwierig, die jeweiligen Assets wieder in Fiatgeld (z. B. Euro) zu tauschen. Auf den großen Plattformen mit *KYC (Know your Customer)* ist es nicht möglich. Auch *Coinfinity*, der älteste Bitcoin-Broker Österreichs, würde direkte Überweisungen, die den Ausgang von solchen Wallets haben, nicht akzeptieren bzw. den jeweiligen Auftraggeber bei den Behörden melden.

Bitcoins und einige andere Kryptowährungen haben weltweite Bekanntheit und sind immer mehr in Verwendung. Behörden in den Nationalstaaten sollten sich vernetzen, um Transaktionsinformationen schneller weitergeben zu können. Damit könnten Firmen oder Softwaresysteme einheitlich und schnell upgedatet werden. Dies lässt den Handlungsspielraum der Kryptodiebe stark einschränken und trägt zu größerer Sicherheit bei.

Open Source. Einmal in Besitz der Information der Wallet, kann jeder diese nachverfolgen. Wenn man unter *https://www.walletexplorer.com/* die Wallet-Adresse im Suchfeld eingibt, sieht man alle bisherigen Ein- und Ausgänge. Unter dem Link *www.blockchain.com/btc/tx/e8b406091959700dbffcff30a60b190133721e5c39e89bb5fe23c5a554ab05ea* kann man alle Diebstahltransaktionen einsehen.

Matthias Reder

Der Autor Mag. (FH) Matthias Reder ist Leiter Compliance und AML bei Coinfinity GmbH und Ansprechpartner für Großkunden sowie Banken und Behörden (www.coinfinity.co)