Kriminelle lieben Kryptowährungen

Kritiker machen für den Erfolg der Kryptowährungen vor allem einen Faktor aus: Die Web-Währungen seien wie geschaffen für Kriminelle. So warnte der Vizepräsident des Bundesverbands Digitale Wirtschaft e.V. (BVDW) Christoph von Dellinghausen schon 2011: „Bitcoins sind gefährlich und haben das Potenzial, der gesamten Gesellschaft durch illegale Geschäfte nachhaltig zu schaden.“ Tatsächlich eroberte die Kryptowährung dubiose Internet-Marktplätze wie den Silk Road Anonymous Marketplace, auf dem zum Beispiel Drogen gehandelt wurden, im Sturm. Auch Cyberkriminelle fordern Lösegeld für gekaperte Computer durch Erpresser-Trojaner gerne in Bitcoin. Steuerhinterzieher, Geldwäscher und Schmuggler setzen ebenfalls immer wieder auf die Cyberwährung.

Verbrecher stehen auf Cybergeld

Das Kryptowährungen Kriminelle magisch anziehen, ist nicht von der Hand zu weisen. Drei aktuelle Beispiele: In Las Vegas wurde der Betreiber eines illegalen Bitcoin-Handelsplatzes verhaftet, nachdem er von einem verdeckten Ermittler bei einer angebahnten Geldwäsche ertappt wurde. Auf Island stahlen Unbekannte 600 Computer im Wert von 1,5 Millionen um Kryptowährungen zu schürfen. Und Apple-Mitgründer Steve Wozniak wurden sieben Bitcoin entwendet, als er sie verkaufen wollte. Er fiel auf einen Betrüger herein, der eine gestohlene Kreditkarte verwendete.

Die Blockchain weiß alles

Anonymität ist dabei vermeintlich eines der wichtigsten Tools im Werkzeugkasten der Verbrecher. Insbesondere bei der Geldwäsche liegt der Fokus der Kriminellen darauf, die eigene

Identität von finanziellen Transaktionen zu trennen. Erschwerend für die Geldwäscher ist allerdings die Tatsache, dass Bitcoins selbst alles andere als anonym sind. Denn im Gegensatz zu Bargeld lassen sich alle Transkationen in der Blockchain haarklein nachvollziehen. Darüber hinaus liefert jede Transaktion Ermittlern Informationen, die sie zu den IP-Adressen der Computer führen, die Zahlungen senden und empfangen. Das Problem aber: Den Ermittlern fehlen bislang oft noch die erforderlichen Monitoring-Tools für die Überwachung potenzieller Straftäter. Nichtsdestotrotz nimm die Zahl der Fälle, in denen Kriminelle durch Bitcoin-Tracing identifiziert wurden, laut Europol deutlich zu.

Mehr Anonymität durch neue Währungen

Die „Nachteile“ von Bitcoin registriert zunehmend auch der Untergrund – und schwenkt auf andere Kryptowährungen um. Laut Europol handelt es sich dabei vornehmlich um Monero, Ethereum, Dash und Zcash. Aus gutem Grund. Monero, entwickelt 2014, bietet zum Beispiel deutlich bessere Anonymität als Bitcoin. Die dahinterstehende Technologie macht es unmöglich, Transaktionen einem bestimmten Benutzer oder einer IP-Adresse zuzuordnen. Es verschlüsselt die Adresse des Empfängers in der Blockchain und generiert gefälschte Adressen, um den Absender sowie den Betrag zu verschleiern. Im Darknet wird Monero aus diesen Gründen bereits auf mehreren Märkten akzeptiert und kam auch schon bei Ransomware-Angriffen zum Einsatz. „Zcash, Dash und anderen aufstrebende Bitcoin-Varianten wie Verge und Nav Coin machen digitale Transaktionen nahezu unauffindbar. Im Moment sehe ich nicht, was die Polizei tun kann, um das zu verhindern.“ so Albert Mavashev, CTO bei Nastel Technologies, einem Monitoring-Unternehmen, das Software für Business Transaction Management (BTM) und Anwendung entwickelt.

Strafverfolgung durch Monitoring

Unabhängig vom Grad der technischen Anonymität von Cyberwährungen selbst, gibt es für Ermittler eine Chance: Irgendwann müssen auch Kriminelle Ihre Krypto-Münzen gegen Bares eintauschen. Eine weitreichende Beobachtung solcher Transaktionen kann daher zur Demaskierung unvorsichtiger Akteure führen. „Es gibt zwei Ansätze zur Erkennung verdächtiger Aktivitäten: Deanonymisierung und Anomalieerkennung“, erklärt Juan Llanos, Financial and Regulatory Technology Lead beim Blockchain-Inkubator ConsenSys. „Einige dieser Techniken sind bereits weit verbreitet in traditionellen Finanzdienstleistungen, insbesondere solche, die sich auf Volumen, Frequenz und Geschwindigkeit konzentrieren.“

Ermittler schlagen zurück

Einer der innovativsten Ansätze zur Überwachung von Cyber-Währungstransaktionen setzt dabei selbst auf die Blockchain. „Die Blockchain eignet sich naturgemäß ideal für die dezentrale Überwachung von Finanztransaktionen“, erklärt Floyd D’Costa, Unternehmensberater und Mitbegründer von Blockchain Worx. „Blockchain-basierte Plattformen bieten Regulierungsbehörden, Wirtschaftsprüfern und anderen Interessengruppen effektive und leistungsstarke Instrumente für die Überwachung von verdächtigen Transaktionen im gesamten System“.

Fazit

Kryptowährungen wie Monero und Zcash stehen bei Kriminellen definitiv hoch im Kurs. Allerdings rüsten die Fahnder auf, es scheint sich ein Katz und Maus-Spiel um die besseren Technologien zu entwickeln.