Blockchain-Ermittlungen

Rund 200 Vertreterinnen und Vertreter von Strafverfolgungsbehörden aus Österreich, Deutschland und der Schweiz nahmen in Wien an einer Konferenz über Kryptowährung teil.

Kryptowährungen wie Bitcoins werden immer öfter zur Bezahlung krimineller Machenschaften verwendet oder von Erpressern als Lösegeld zur Freigabe mittels Ransomware verschlüsselter Daten gefordert. Über das Darknet werden vermehrt kriminelle „Dienstleistungen" in Form von „Crime as a Service" angeboten, etwa das Zurverfügungstellen von Software, Technik und Wissen, um kriminelle Handlungen zu begehen.

Blockchain-Konferenz: Erhard Friessnik, C4, Michael Fischer, stellvertretender BK-Direktor, Klaus Mits, Abteilungsleiter im BK, Alexander Haslinger, BK-Ermittler.

Das Cybercrime-Competence-Center (C4) im Bundeskriminalamt ist nationale und internationale Ansprechstelle für die elektronische Sicherung und Auswertung von Beweismitteln. Die Spezialisten des C4 führen selbst Ermittlungen und koordinieren die Bekämpfung von Cybercrime. Seit 2017 gibt es im C4 Spezialisten für Blockchain-Ermittlungen. Die Blockchain-Technologie ist die Grundlage von Kryptowährungen.

Fachkonferenz. Das C4 lud vom 22. bis 24. Jänner 2020 rund 200 Polizistinnen und Polizisten sowie Vertreterinnen und Vertreter von Strafverfolgungsbehörden zur Konferenz „Blockchain und virtuelle Währungen. Gezielt ermitteln und sicherstellen". In dieser Tagung konnten die Teilnehmerinnen und Teilnehmer den Umgang mit Kryptowährungen und „Smart Contracts" lernen; das sind Computerprotokolle, die Verträge abbilden, überprüfen oder die Verhandlung und Abwicklung eines (Kauf-)Vertrages technisch unterstützen.

Coin-O-mat. Dazu entwickelten die IT-Spezialisten des C4 einen „BK-Token", der mit einem selbst geschriebenen „Smart Contract" in die „Ethereum-Blockchain" hochgeladen wurde und öffentlich einsehbar war. Er stellt keinen finanziellen Gegenwert dar und wird nicht gewerblich gehandelt. Dazu wurde ein Automat namens „Coin-O-Mat" entwickelt, der mit dem „Smart Contract" interagieren kann. Wenn der Benutzer des Automaten die Übung mit dem BK-Token richtig abschließt, wirft der Automat eine Challenge-Coin aus. In Expertenworkshops wurden die Transaktionen mit den BK-Token auf forensische Spuren untersucht.

Trainings mit dem BK-Token werden künftig auch in weiteren Schulungen national und international abgehalten. Die Konferenz wurde von der EU über die *Fonds für die innere Sicherheit (ISF)* kofinanziert.

Kryptowährungen und Blockchains. Kryptowährungen sind digitale Zahlungsmittel, die auf verschlüsselten Datensätzen basieren. Mit dieser Form von Zahlungsmitteln ist ein digitaler Zahlungsverkehr ohne Bank möglich. Der Besitz des Codes stellt dabei das Eigentum dar. Zahlungstransaktionen mit Kryptowährungen werden in Blöcken gespeichert. Das Buchungssystem nennt man Blockchain. Die bekannteste Kryptowährung ist der Bitcoin.

Obwohl Kryptowährungen im letzten Jahr Kursverluste hinnehmen mussten, ist eine Zunahme der Zahl an Bezahlvorgängen zu beobachten. Insbesondere im Cybercrime-Bereich haben sich „Cryptos" durchgesetzt, besonders bei den ansteigenden Fallzahlen in Zusammenhang mit Massenerpresser-E-Mails. Auch wenn Bitcoins unter den Kryptowährungen immer noch an erster Stelle stehen, wird mittlerweile auch mit anderen Kryptowährungen bezahlt. Kryptowährungen, die nicht Bitcoins sind, werden als Altcoins bezeichnet.

Behördenwallets. Das C4 ist seit 2018 rechtlich und technisch in der Lage, Kryptowährungen sicherzustellen. Dazu werden „Behördenwallets" erstellt und zur Aufbewahrung von virtuellen Währungseinheiten verwendet. Derzeit stehen im BK 1.000 Behördenwallets für Amtshandlungen zur Verfügung. Bisher wurden bei 80 Hausdurchsuchungen Kryptowährungen im Wert von fünf Millionen Euro sichergestellt. Werden die sichergestellten Kryptowährungen vom Gericht für verfallen erklärt, führt das C4 die Verwertung durch und überweist die Geldsummen an die jeweiligen Gerichte.

Cybercrime-Zahlen im Vergleich. Die Zahl der Cybercrime-Anzeigen stieg von 16.804 Anzeigen im Jahr 2017 auf 19.627 2018. Bei Cybercrime-Delikten im engeren Sinn ist die Anzahl der gemeldeten Fälle von 3.546 (2017) auf 3.070 (2018) gesunken, dies bedeutet ein Minus von 13,4 Prozent. Die Aufklärungsquote bei den Delikten von Cybercrime im engeren Sinn stieg von 28,2 Prozent (2017) auf 32,1 Prozent (2018). Die Zahl der Anzeigen von Cybercrime-Delikten im weiteren Sinn stieg im Vergleich zu 2017 um 23,9 Prozent auf 16.557.

Zu Cybercrime im weiteren Sinn zählen Straftaten, bei denen die Informations- und Kommunikationstechniken zur Planung, Vorbereitung und Ausführung herkömmlicher Straftaten, wie Betrugsdelikte oder Erpressung unter Nutzung von Informationstechnologien sowie Urkundenfälschung verwendet werden. *M. R.-E.*

FOTO: ARMIN HALM