Cyber-Erpressung: Bitcoin-Forderungen werden oft an die finanziellen Möglichkeiten der Opfer – meist Firmen – angepasst.

Verfolgung digitaler Geldflüsse

Die Zahl der Cybercrime-Anzeigen steigt an. Täter nützen zur Verschleierung der Geldflüsse digitale Währungen. Spezialisten des Bundeskriminalamts sind den Tätern in der virtuellen Welt auf der Spur.

Im April 2019 wurde in Wien ein Bitcoin-Automat gehackt, der Täter war flüchtig. Im Laufe der Fahndung wurde ein georgischer Staatsbürger als mutmaßlicher Täter identifiziert und wenige Zeit später festgenommen. Der Verdächtige machte keine Angaben zur Tat, hatte aber zahlreiche Belege von Bitcoin-Käufen bei sich. Die Polizisten nahmen Kontakt zum Automatenbetreiber auf, der den Angriff auf den Automaten bestätigte und die Ermittler auf weitere Unregelmäßigkeiten hinwies, die einige Tage vor der Tat aufgetreten waren. Da der mutmaßliche Täter weiterhin nicht kooperativ war, standen die Ermittler des Landeskriminalamts (LKA) Wien vor einem Rätsel, da die Blockchain als nicht hackbar gilt. Um die Spuren am Automaten und in der Blockchain zu sichern und auszuwerten, wendete sich das LKA Wien an das *Cybercrime-Competence-Center (C4)* im Bundeskriminalamt. Die Ermittlungen übernahm Kontrollinspektor Alexander Haslinger, seit 2017 provisorischer Leiter des Bereichs „Blockchain-Ermittlungen“ im *C4*.

Ergebnisse der Ermittlungen. Der Bitcoin-Automat wurde sichergestellt und ins *C4* gebracht. Bei der Auswertung konnte festgestellt werden, dass es zu zahlreichen irregulären Auszahlungen nicht nur an diesem, sondern auch an weiteren Automaten gekommen war. Der Verdächtige wurde mit den Logdateien konfrontiert, die ihn schwer belasteten. Er gestand, innerhalb von drei Tagen über 50.000 Euro von Bitcoin-Automaten behoben zu haben. Er war in seinem Heimatland als IT-Administrator tätig, verdiente damit aber zu wenig, weswegen er sich zu den Taten hinreißen ließ.

Blockchain. Bitcoins sind nichts anderes als Daten aus einer Datenbank, die als Vermögenswert angesehen werden. Durch Spekulationen steigt oder sinkt der Kurs, vergleichbar mit Aktien. Bitcoins können von einer Bitcoin-Adresse an eine andere versendet werden. In der Blockchain werden die Transaktionen gespeichert. Die Blockchain wird als eine Art dezentrales Kassabuch angesehen, das es ermöglicht, digitale Einträge fälschungssicher und unveränderbar zu speichern.

Softwarefehler. „Es hat sich gezeigt, dass die Analyse und Verfolgung von Geldströmen oft einen Hinweis auf die Täter bringt und die Unverfälschbarkeit der Daten in der Blockchain aus polizeilicher Sicht auch ihre Vorteile hat, da die Spuren dort zumindest nie verschwinden“, erklärt Kontrollinspektor Haslinger. „Im Falle des Automaten-Hackers ist es für uns zunächst unklar gewesen, wie er es geschafft hat, sich unrechtmäßig Geld auszahlen zu lassen. Nachdem die Transaktionen nicht fälschbar sind, hat nur der Automat selbst der Schwachpunkt sein können“, erläutert Haslinger. Der Täter dürfte laut den Ermittlern den Automaten über den Touchscreen manipuliert

Foto: Parilov/Stock.adobe.com

Bitcoin-Automat: Durch Manipulation des Automaten veranlasste ein Mann Bitcoinüberweisungen auf sein Konto.

Bei der Blockchain-Konferenz im Jänner 2020 in Wien wurde der Coin-O-mat des Bundeskriminalamts präsentiert.

haben. Er entdeckte eine Schwachstelle in der Software des Automaten, die mittlerweile ausgebessert wurde, und nutzte sie zu seinem Vorteil. So konnte er dem Automaten weismachen, dass Bitcoins zu ihm transferiert wurden, ohne dass jemals eine Transaktion stattgefunden hatte. Der Softwarefehler ermöglichte die Ausgabe des Bargeldes. In Österreich gibt es etwa 400 solcher Automaten, die in Cafés, Trafiken oder Postfilialen aufgestellt sind.

Bitcoin und Ransomware. Unter Ransomware, auch Verschlüsselungstrojaner genannt, wird die Verschlüsselung von Daten bezeichnet, für deren Freigabe die Täter ein „Lösgeld“ in Form von Bitcoins fordern. Ransomware-Attacken wurden anfangs von wenigen Tätergruppen begangen, auf die sich die Cybercrime-Ermittler des BK konzentrieren konnten. Durch die vielen gleichartigen Fälle konnten Ermittlungsansätze gewonnen werden und auf die anderen Fälle angewendet werden. Lösegeldforderungen wurden pauschal gestellt. Dieses Bild hat sich verändert. Es agieren viele kleine Tätergruppen, und die Bitcoin-Forderungen werden oft an die finanziellen Möglichkeiten der Opfer, oft sind es Firmen – angepasst. Um ihren Forderungen Nachdruck zu verleihen, veröffentlichen die Kriminellen oft die Daten der Unternehmen im Internet.

Zur Bekämpfung von Ransomware wurde im Bundeskriminalamt Mitte 2016 die „Soko Clavis“ errichtet, die bis Mai 2019 bestand. Diese hatte die Aufgabe, alle in Österreich angezeigten Fälle von Ransomware zentral zu bearbeiten. Entscheidend war, eine Kategorisierung der verschiedenen Tätergruppen vorzunehmen, um gegen sie ermitteln zu können. Dadurch gelang es, mehrere Beschuldigte und Verdächtige zu großen Ransomware-Familien auszuforschen. Ransomware-Fälle werden nach wie vor zentral vom *C4* bearbeitet.

BK-Token. Der Umgang mit Kryptowährungen und der Blockchain erfordern Wissen und Praxiserfahrung in der Verwendung von beispielsweise Bitcoins voraus, um die Spuren der Blockchain verstehen zu können. Da nicht alle Polizisten Erfahrungen mit fiktiven Währungen und „Smart Contracts“ haben, hat das *C4* ein besonderes Übungsszenario entworfen und im Jänner 2020 präsentiert. Bei „Smart Contracts“ handelt es sich um Computerprotokolle, die Verträge abbilden, überprüfen oder die Verhandlung und Abwicklung eines (Kauf-) Vertrages technisch unterstützen.

Polizisten des *C4* haben für die Übungen eine eigene Kryptowährung erfunden, den „BK-Token“. Dieser Token wurde mit Hilfe eines selbst geschriebenen „Smart Contracts“ für die Bedürfnisse der Polizei adaptiert, sodass verschiedene Übungsabläufe in vier verschiedenen Schwierigkeitsstufen simuliert werden können. In der ersten Stufe werden Polizisten dazu animiert, sich mit dem Grundlegendsten auseinanderzusetzen – der Transaktion von Kryptowährungen. Um aus der fiktiven Welt der Bitcoins herauszutreten und etwas Reales und Greifbares zu schaffen, wurde von den Spezialisten des *C4* ein „Coin-O-Mat“ konstruiert.

Alexander Haslinger, Kryptowährung- und Blockchain-Experte des BK.

Coin-O-Mat. Der Automat verfügt über eine Anbindung zur Blockchain, wodurch er mit den „Smart Contracts“ kommunizieren kann. Wenn die Polizisten die Übung mit dem „BK-Token“ richtig ausführen, sich zunächst ein eigenes Wallet erstellen, sich mit den Transaktionsgebühren beschäftigen und abschließend den „BK-Token“ zum Automaten überweisen, dann wirft dieser eine geprägte Münze aus. Seit der Präsentation des Automaten wurden bereits rund 300 Polizisten in den Grundlagen der Kryptowährungen und Blockchain geschult. Diese Praxiserfahrungen sollen dazu dienen, eine höhere Aufklärungsquote bei Cybercrime-Delikten zu erzielen.

Behördenwallets. Wallets sind eine „digitale Brieftasche“, in der die Bitcoins oder andere Kryptowährungen gespeichert sind. Das *C4* hat einen Erlass für die Sicherstellung von Kryptowährungen erstellt, wodurch jeder Polizist die Möglichkeit hat, Bitcoins sicherzustellen und an die Wallets der Polizei beziehungsweise Justiz zu übermitteln. Um dies zu gewährleisten, hat das *C4* Tausende Behördenwallets mitsamt eines Sicherheitskonzeptes erstellt. Dieses stellt sicher, dass die Wallets bis zur Verwertung nicht mit dem Internet verbunden sind. Aufgrund des Erfolgs dieser Vorgehensweise und Methodik wurde sie von mehreren Ländern der EU übernommen und von Europol als empfehlenswerte Strategie befunden. *Romana Tofan*

Fotos: Armin Halm (2), Parilov/Stock.adobe.com