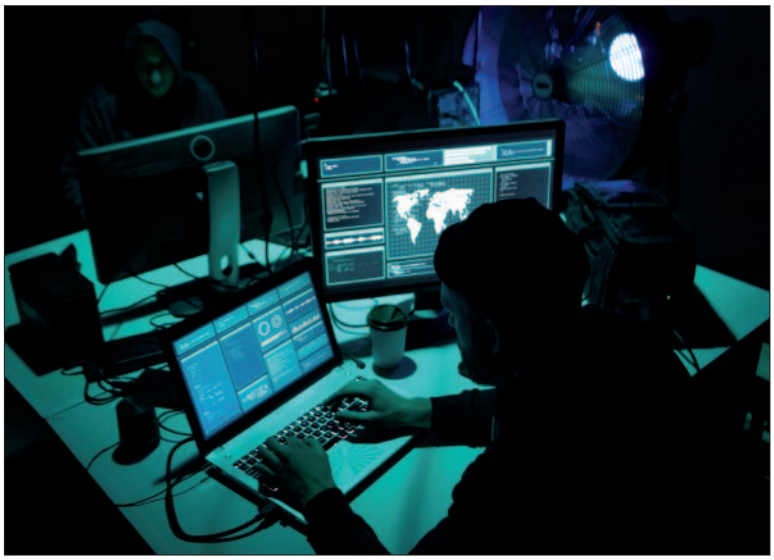
Sicherstellung virtuellen Geldes

Bei der 6. „Virtual-Currency"-Konferenz von Europol vom 12. bis 14. Juni 2019 in Den Haag wurde nach Möglichkeiten gesucht, gegen Kriminelle vorzugehen, die illegal Kryptowährungen einsetzen.

Auf Einladung des europäischen Polizeiamts Europol diskutierten Mitarbeiter von Sicherheitsbehörden und Vertreter privater Firmen, mit welchen Tools und Strategien man kriminelle Transaktionen verfolgen und Straftäter beim Umwechseln von Kryptowährungen in reales Geld enttarnen kann. Auch die großen digitalen „Wechselstuben" arbeiten eng mit den Behörden zusammen, da sie nicht riskieren wollen, wegen Geldwäscheverdachts oder der Beitragstäterschaft zu anderen Straftaten in Verdacht zu geraten.



Kryptowährungen werden immer öfter als Zahlungsmittel für kriminelle Geschäfte im Darknet verwendet.

Leitfaden für Sicherstellungen. Immer mehr Kriminelle verwenden anstelle von Bargeld, Gold oder anderen Wertgegenständen Kryptowährungen, vor allem wenn sie in Computerkriminalität, Betrug, Erpressung oder Drogenhandel involviert sind. Behörden sind bei Hausdurchsuchungen oft damit konfrontiert, Behältnisse, digitale Geräte oder schriftliche Aufzeichnungen sicherzustellen, die Kryptowährungen beinhalten oder sich auf diese beziehen.

Bei der Europol-Konferenz waren Vertreter vieler Polizeibehörden anwesend, die ihre Vorgehensweise präsentierten, um die vielen unterschiedlichen Objekte aufzuspüren. Die belgische Polizei entwickelte einen Leitfaden, in dem Hunderte technische Begriffe, Produktnamen und Fotos von Objekten angeführt sind, die Sicherheitskräften helfen.

Über die Verwertung von sichergestelltem virtuellem Geld entscheidet das Gericht auf Antrag der Staatsanwaltschaft. Das stellt große Herausforderungen an die jeweiligen Stellen dar, da eine Auswahl des richtigen Wechselanbieters getroffen werden und bei einem Freispruch des Beschuldigten das beschlagnahmte Vermögen an ihn zurückerstattet werden muss. Das kann im Falle von unvorhersehbaren Kursschwankungen bei Krypto-Assets eine wirtschaftlich schwierige Angelegenheit sein.

Informationen über Täter. Die wichtigste Informationsquelle zur Enttarnung von Personen und Organisationen, die Kryptowährungen missbrauchen, stellen Anzeigen bei den Sicherheitsbehörden dar. Wichtig sind auch Hinweise aus der Bevölkerung oder, wenn es beispielsweise auffällt, dass jemand aus unerklärlichen Gründen sehr vermögend geworden ist, aus dem Umfeld dieser Personen.

Hinweise können auch anonym über die Hinweisgeberplattformen der Wirtschafts- und Korruptionsstaatsanwaltschaft *(https://www.bkms-system.net/wksta)* oder der Finanzmarktaufsicht – *FMA (https://www.fma.gv.at/whistleblowing)* elektronisch eingebracht werden. Etwa 30 bis 40 Prozent der Whistleblower-Anzeigen betreffen Kryptowährungen, hieß es dazu etwa Ende Jänner 2018 von *FMA*-Vorstand Helmut Ettl.[1]

Betrüger. Während nach Schätzungen der Nationalbank über 90 Prozent der Österreicher noch nie mit Kryptowährungen in Kontakt gekommen sind, müssen sich die Sicherheitsbehörden regelmäßig mit ihrer missbräuchlichen Verwendung auseinandersetzen. Dabei geht es um Anlagebetrug, bei dem Kryptowährungen vorgeblich gekauft oder verkauft werden, oder mit ihnen zusammenhängende Finanzinstrumente.

Bekanntheit erlangten die Fälle rund um die österreichischen Anlegerplattformen *Optioment* und *Cointed* sowie um den angeblichen „Verlustausgleichsverein" *Rocket-Chain (RCI-ID)*[2]. Nachdem Anlegern hohe Zinszahlungen für Investments in Kryptowährungen versprochen worden sind bzw. später das Abfedern von Verlusten, stehen nun Delikte wie gewerbsmäßig schwerer Betrug, das Betreiben von Ketten- oder Pyramidenspielen, Untreue, die Bildung einer kriminellen Vereinigung und mögliche Verstöße gegen die Prospektpflicht im Raum[3].

Dubioses Geschäftsmodell. Ein Kunde von *Optioment* erläuterte, wie das Geschäftsmodell aussah: Er kaufte nach Empfehlung im Freundeskreis einen Bitcoin bei dieser Firma mit dem Versprechen, dass dieser innerhalb der nächsten zwei Jahre für den Kauf weiterer Bitcoins eingesetzt würde. Laufend wurde ihm im Wege von Kontonachrichten mitgeteilt, dass sein Investment stark steigende Renditen abwerfe. Am Ende der Laufzeit wies sein Konto den 47-fachen Wert aus – aus 900 Euro waren 42.000 Euro in Bitcoin geworden. Als er in der folgenden Krise der Kryptowährung die Bitcoins aus seinem Portfolio verkaufen wollte, war der für ihn zuständige Mitarbeiter der Firma lange Zeit nicht erreichbar, und erzählte ihm letztlich, dass er selbst Opfer eines Betrugs geworden sei und gar keine Bitcoins vorhanden seien. Die zuständigen Manager hätten sich ins Ausland abgesetzt, und alles Geld sei verschwunden.

Betrügereien durch Geldanlageangebote wie Pyramidenspiele mit Kryptowährungen nehmen zu.

Erpresser. Immer öfter werden Firmen mit Schadsoftware konfrontiert, die ihre Computersysteme und manchmal auch Mobiltelefone sperrt oder verschlüsselt. Diese „Ransomware“ wird meist über infizierte USB-Sticks, über Attachments oder Links von E-Mails in Umlauf gebracht. Die Erpresser verlangen für die Übersendung des Codes zur Entschlüsselung der Systeme eine Zahlung auf eine Krypto-Geldbörse. Die Service-Webseite *nomoreransom.org* von Europol bietet eine gute Information über diese bedrohlichen Technologien und hilft Betroffenen bei der Problemlösung.

„Ransom-Mails“. Hochkonjunktur haben derzeit „Ransom-Mails“, in denen Menschen das Passwort zu einer ihrer Benutzer-IDs im Klartext zugesandt wird – mit dem Hinweis, man habe sie gehackt und so ihr Passwort in Erfahrung gebracht. Manchmal wird behauptet, dass man die Betroffenen überdies nackt an ihrem Computer gefilmt oder sie bei der Konsumation von fragwürdigen Videos aufgezeichnet habe.

Zu Beginn dieses Jahres wurde bekannt, dass Hacker fast 800 Millionen Passwörter und E-Mail-Adressen von Online-Diensten wie *Yahoo, LinkedIn, eBay* oder *YouPorn* gestohlen hatten, und danach Millionen Betroffenen Mails sandten, in denen sie diese aufforderten, Zahlungen an sie mittels einer Kryptowährung vorzunehmen.

Angesichts der Überraschung, mit dem eigenen entschlüsselten Passwort konfrontiert zu werden, zahlen viele Menschen auf die geforderte Weise Geld an die Erpresser, die dieses Kryptogeld dann über verschiedene Mechanismen wieder in echtes Geld umwandeln und meist unbehelligt bleiben.

Foto: Maxim_Kazmin/Stock.Adobe.com

„Ransom-Mails“: Nutzer werden mit der Veröffentlichung von intimen Daten oder Videos über sie bedroht.

Darknet. Illegale Einnahmen werden auch im Darknet umgesetzt, um andere illegale Dienste zu bezahlen. Beispielsweise können E-Mail-Adressen gekauft werden – wie im illegalen Handelsplatz „Berlusconi-Market“, wo 380.000 österreichische Adressen für jeweils 10 Euro verkauft werden. Bezahlt werden kann in den Kryptowährungen *Litecoin*, *Monero* und *Bitcoin*. Auf solchen Handelsplätzen finden die Erpresser auch andere Straftäter, die in ihrem Auftrag Spam-Mails versenden, Schadsoftware schreiben oder Computersysteme hacken.

Cornelius Granig

Über den Autor:

Dr. Cornelius Granig ist ein österreichischer Unternehmensberater und Cybersecurity-Experte. Er leitete in den letzten Jahren die IT- und Sicherheits-Abteilungen im Vorstand großer Banken und Versicherungen und war im Management der internationalen Technologiekonzerne IBM und Siemens tätig. Im April 2019 veröffentlichte er im Kremayr & Scheriau-Verlag das Buch „Darknet: Die Welt im Schatten der Computerkriminalität“.

Anmerkungen:

[1]Vgl. Kurier: Bitcoin ist typische Blase, 23. Januar 2018.

[2]Vgl. Vilgut, Roman. In: Kleine Zeitung, 20. Februar 2018.

[3]Vgl. Hahn, Alexander, Pfluger, Bettina: Justiz ermittelt im Fall Optioment gegen elf Personen. Razzien auch bei insolventer Bitcoin-Automatenfirma Cointed. In: Der Standard, 2. Februar 2019.

[4]Vgl. Sempf, Julia: Erpresser machen Kasse – und das ganz ohne Malware. In: Hornet Security, 18. Januar 2019.

Foto: Pira555/Stock.adobe.com