Erpressern und Netzdealern auf der Spur

Das Geldsystem Bitcoin nützt die Möglichkeiten des Internets auf neue Art – und zieht damit auch illegale Akteure an. Das Projekt Bitcrime lotet Strategien gegen den Missbrauch aus.

Alois Pumhösel

Foto: AFP / Rick Bowmer

Geld, das nur aus Daten am Computer besteht: Per Bitcoins kann man im Netz bezahlen, ohne die Dienste von Finanzunternehmen in Anspruch nehmen zu müssen. Weil es weitgehend anonyme Transfers erlaubt, zieht das Zahlungssystem aber Kriminelle an.

Innsbruck – Plötzlich kann man nicht mehr auf die eigenen Daten zugreifen. Das private Fotoarchiv oder andere „Eigene Dateien" lassen sich nicht mehr öffnen. Stattdessen erscheint eine Aufforderung, einen Geldbetrag an einen Erpresser zu übermitteln. Dann würde man ein Passwort erhalten, das die verschlüsselten Dateien wieder zugänglich macht. Ransomware – nach dem englischen Wort für Lösegeld – lautet diese Art von Schadsoftware, die wie andere Trojaner oder Viren etwa als E-Mail-Anhang auf den Computer gelangen. Das Lösegeld soll meist auf eine bestimmte Art bezahlt werden: in Bitcoins.

Das Zahlungssystem, das weitgehend anonyme Geldtransfers über ein dezentrales, sogenanntes Peer-to-Peer-Netzwerk erlaubt und, anders als konventionelle Währungen, von keiner zentralen staatlichen Instanz geregelt wird, hat seit seiner Etablierung im Jahr 2009 stark an Popularität gewonnen. „Bitcoins eröffnen die Chance auf mehr wirtschaftliche Interaktion im Netz", erläutert Rainer Böhme, seit 2015 Professor am Institut für Informatik der Universität Innsbruck, die dahinterstehende Vision. „Zahlungen im Netz abzuwickeln ist teuer, Gebühren, die an die Dienstleister gehen, wirken wie Zusatzsteuern, die den Gewinn schmälern. Günstige Zahlungen im Internet forcieren Gründungen und Innovation." Im Vergleich zu bisherigen Zahlungssystemen, „die noch nicht im Internetzeitalter angekommen sind", böten Bitcoins einen völlig neuen Ansatz.

Im deutsch-österreichischen Forschungsprojekt Bitcrime, das Böhme leitet, beschäftigt er sich allerdings mit einer Realität, die in vielen Fällen weitab von dieser Vision liegt: „Kryptografische Währungen wie Bitcoins werden nicht nur für legale Zahlungsvorgänge, sondern im hohen Ausmaß für kriminelle Machenschaften wie Ransomware, Geldwäsche oder Handel mit illegalen Waren verwendet." Gemeinsam mit Ökonomen und Juristen erarbeiten die Informatiker rechtliche, regulatorische und technische Grundlagen, die eine Unterbindung der kriminellen Aktivitäten ermöglichen sollen, ohne das Zahlungssystem zu verbieten – eine Maßnahme, die in manchen Ländern erwogen oder bereits durchgeführt wurde.

Ransomware gibt es mittlerweile in zigtausenden Varianten. Eines der erfolgreichsten der bekannten Programme ist Cryptowall, vor dem die US-Sicherheitsbehörde FBI im Juni 2015 warnte. Bis dahin hatte der digitale Schädling Verluste von insgesamt 18 Millionen Euro bei seinen Opfern verursacht. Abgesehen davon begünstigen die nur schwer nachvollziehbaren Transaktionsflüsse der Bitcoins das Vorhaben, kriminell erwirtschaftetes Geld wieder in einen legalen Währungskreislauf zurückfließen zu lassen.

Geldwäsche, Waffen, Drogen

Wo es keine Banken oder staatlichen Instanzen gibt, greifen auch keine Maßnahmen zur Geldwäsche-Prävention. Und auch der Handel mit Waffen, Drogen, Schadsoftware und anderen illegalen Gütern über das sogenannte Darknet, das über Anonymisierungssoftware wie Tor zugänglich wird, erfolgt vielfach mittels Bitcoins. Ein tatsächliches Volumen der kriminellen Geschäfte sei aber kaum zu schätzen, sagt Böhme. Zu unübersichtlich ist das Geflecht an legalen und illegalen Transaktionen und Umbuchungen.

Im Projekt Bitcrime, das sowohl vom österreichischen Verkehrsministerium als auch vom deutschen Forschungsministerium finanziert wird, sind auch die Aufgabenstellungen klar aufgeteilt. In Deutschland kümmert sich die Westfälische Wilhelms-Universität Münster, Böhmes frühere Hochschule, mit Konsortialpartnern um die Verbesserung polizeilicher Ermittlungsmethoden und die Erarbeitung von Regulierungsansätzen, die Kriminalität verhindern und nichtkriminelle Nutzer schützen sollen. Dabei wurde unter anderem eine eigene Testumgebung, in der das Währungssystem simuliert wird, etabliert.

In Österreich untersucht dagegen das AIT, das Austrian Institute of Technology, mit Partnern die Transaktionsmuster und analysiert entsprechende Daten aus Social Media und den Untergrund-Marktplätzen. Die Forscher gehen davon aus, dass Transfers auf bestimmte Merkmale hin analysiert und somit in der Vielzahl an Geldbewegungen identifiziert werden können.

Transfers melden

Die politischen Prozesse könne man nicht vorwegnehmen, sagt Böhme, aber man könne im Projekt Optionen aufzeigen und Konsequenzen durchdenken. Dass man bei den einfachen Nutzern ansetzt, sei letzten Endes wohl nicht zielführend.

„Ein logischer Ansatzpunkt wäre, Instanzen, die beispielsweise gewerbsmäßig Zahlungen annehmen, in die Pflicht zu nehmen. Diese sogenannten Intermediäre könnten bestimmte Daten zu den Transaktionen an Kontrollorgane weitermelden", sagt der Informatiker. „Allerdings müsste auch definiert werden, welche Informationen sie im Sinne des Datenschutzes nicht melden dürfen."