BITCRIME – Sicherheitsforschung schützt Bitcoin-Nutzer vor Kriminalität (31.01.2017)

Virtuelle Währungen wie Bitcoin ermöglichen Zahlungen über das Internet. Das Besondere daran ist, dass keine Bank oder andere zentrale Stelle eingeschaltet wird. Nutzer können selbst Konten erzeugen und Bitcoins direkt untereinander handeln.

Anders als bei Eröffnung eines Bankkontos, müssen sich die Nutzer virtueller Währungen nicht identifizieren. Das lockt auch Kriminelle an: So werden Bitcoins teilweise auch zum illegalen Waffenhandel oder zur Geldwäsche genutzt. Auch Kriminelle, die Erpressungstrojaner verbreiten, nutzen häufig Bitcoin zur Abwicklung von Lösegeldzahlungen. Dabei wird den Opfern der Zugriff auf einzelne Dateien oder die ganze Festplatte des eigenen Computers gesperrt und die Freischaltung nur gegen die Überweisung eines bestimmten Betrags an Bitcoins in Aussicht gestellt.

Bekannte Methoden der Strafverfolgung stoßen bei virtuellen Währungen an ihre Grenzen. Anders als bei Girokonten fehlt den Behörden in den dezentralen Systemen ein Ansprechpartner, der Auskünfte über verdächtige Nutzer erteilen könnte. Gehen Kriminelle bei der Nutzung virtueller Währungen geschickt vor, können sie sich dem Zugriff der Strafverfolger entziehen. Ehrliche Nutzer virtueller Währungen sind demnach einem erhöhten Risiko ausgesetzt, mit Kriminalität in Berührung zu kommen, und davor unzureichend geschützt. So besteht für Nutzer etwa die Gefahr, erpresst zu werden oder aus Straftaten herrührende Bitcoins zu erhalten und sich in der Folge mit Ermittlungen der Strafverfolgungsbehörden konfrontiert zu sehen.

Deshalb müssen neue, auf virtuelle Währungen zugeschnittene Maßnahmen zur Verfolgung und Verhinderung von Kriminalität entwickelt werden. Das haben sich die Forschungspartner des vom deutschen Bundesministerium für Bildung und Forschung und vom österreichischen Bundesministerium für Verkehr, Innovation und Technologie geförderten deutsch-österreichischen Projekts BITCRIME im Programm „Forschung für die zivile Sicherheit“ zum Ziel gesetzt.

Dazu haben sie vor allem zwei Wege verfolgt:

1. Täter ermitteln durch die Nachverfolgung von Bitcoins

Ansatzpunkt ist eine besondere Eigenschaft von virtuellen Währungen wie Bitcoin: Hierbei werden sämtliche Überweisungen in einer öffentlichen Datenbank, der sogenannten Blockchain, gespeichert. Die Daten aus der Blockchain können Ermittler auswerten und so den Weg jedes Bitcoins nachvollziehen. Dies ist normalerweise mit einem hohen zeitlichen und personellen Aufwand verbunden. Doch eine im Projekt BITCRIME erarbeitete Software zur Unterstützung der Strafverfolgung ermöglicht umfassende Überprüfungen. So lassen sich zum Beispiel erpresste Bitcoins schneller verfolgen: Tauschen die Täter diese später gegen Geld ein, können die Ermittlungen bei den Anbietern der Wechselbörsen (in der Regel Online-Handelsplattformen) fortgesetzt werden.

Mit der neuen Software lässt sich aber nicht jede Straftat aufklären. Denn häufig gelingt es nicht, alle an den Überweisungen Beteiligten zu identifizieren. Zum Schutz der ehrlichen Nutzer von virtuellen Währungen ist deshalb auch ein Konzept zur Verhinderung des Umtauschs von illegal erworbenen Bitcoins entwickelt worden.

2. Empfehlung zur Verhinderung von Straftaten mit Bitcoins

Im Projekt BITCRIME wurden entsprechende Maßnahmen ausgearbeitet. Ziel ist es, Tätern die Vorteile ihrer Straftaten zu entziehen. Das setzt voraus, dass Täter illegal erlangte Bitcoins nicht gegen Geld eintauschen oder anderweitig einsetzen können. Die Forscherinnen und Forscher schlagen deshalb vor, den Annahmestellen (z.B. Wechselbörsen) zu verbieten, Bitcoins aus illegalen Quellen entgegenzunehmen. Auch diese Maßnahme setzt bei der Blockchain an: Der Weg aller Bitcoins lässt sich verfolgen. Erfasst man Bitcoins, die aus Straftaten stammen, wie z.B. erpresste Bitcoins, kann deren Handel gezielt eingeschränkt werden. Die Regulierung wirkt wie eine digitale Farbpatrone: Illegal erlangte Bitcoins werden markiert und in der Folge nicht mehr von den Wechselbörsen entgegengenommen – ebenso wie gestohlenes Geld durch Farbpatronen unbrauchbar gemacht wird. Das macht Bitcoin für Kriminelle weniger attraktiv, verhindert so Straftaten und schützt zugleich legale Nutzer, die auch weiterhin selbst Konten erzeugen können, ohne sich bei einer Bank identifizieren zu müssen.

Weitere Informationen unter: https://www.bitcrime.de/deutschland/index.html

Ansprechpartnerin:
Projektkoordinatorin Dr. Paulina Pesch
Westfälische Wilhelms-Universität Münster
Forschungsgruppe IT-Sicherheit
Leonardo-Campus 3
48149 Münster
Tel.: +49 251 83-38234
Fax: +49 251 83-38259
E-Mail: paulina.pesch@uni-muenster.de