Neue Österreichische Analyseplattform geht virtuellen Währungen auf die Spur

Ob im Kampf gegen Cyberkriminelle im jüngst gestarteten EU-Projekt Titanium oder zur Entwicklung neuer Blockchain-Dienste für die Wirtschaft und hier besonders für die boomenden Fintechs: das AIT Austrian Institute of Technology, europaweit führend bei der Analyse von Cyberwährungen, bietet mit der in jahrelanger Forschungsarbeit entwickelten GraphSense Plattform das perfekte Tool zur forensischen Analyse virtueller Währungstransaktionen.

Wien, 29. Mai 2017 – Die jüngste Cyberattacke mit dem Verschlüsselungstrojaner WannaCry ist nur einer der stark zunehmenden Erpressungsversuche über das Internet, bei der meist ein Lösegeld über die schwer verfolgbare Kryptowährung Bitcoin verlangt wird. Doch wie kann man solche Täter am effektivsten ausforschen? Dabei helfen den Strafverfolgungsbehörden insbesondere die Zahlungsflüsse und sonstige Aktivitäten auf den Schwarzmärkten und Foren im Darknet.

Das AIT Austrian Institute of Technology hat mit der **Analyseplattform GraphSense** in mehreren Forschungsprojekten die passende Technologie entwickelt, um mit Hilfe von hochperformanten Big Data-Technologien und speziellen Algorithmen **relevante Information aus der Blockchain extrem schnell extrahieren** zu können. Wichtige Grundlagen für die Entwicklung des Tools wurden im bilateralen KIRAS Projekt BITCRIME,das vom Bundesministerium für Verkehr, Innovation und Technologie gefördert wurde, geschaffen. Hier ging es darum, neue Methoden zur Bekämpfung der organisierten Finanzkriminalität zu entwickeln.

GraphSense bietet aber ebenso für die Wirtschaft wichtige Einblicke in die Blockchain. „Aktuell steigt das Interesse an unserer Analyseplattform besonders bei Fintechs“, erklärt **Ross King**, Data Science Experte am AIT und Leiter der Forschungsgruppe Digital Insight Lab. „Dies ist unter anderem darauf zurückzuführen, dass bestehende Compliance-Richtlinien auch zunehmend für virtuelle Währungen gelten und FinTechs ebenso wie traditionelle Finanzdienstleister zur Einhaltung dieser Richtlinien verpflichtet werden.“

Internationale Forschungsinitiative gegen die kriminelle Nutzung des Darkweb und virtueller Währungen

Zugleich startete im Mai das **EU-Projekt Titanium** (Tools for the Investigation of Transactions in Underground Markets). Für das vom AIT geleitet Forschungsvorhaben haben sich 15 Konsortialpartner, Sicherheitsbehörden, Ministerien, Universitäten und Unternehmen aus sieben EU-Staaten sowie INTERPOL, vereint. “Kriminelle und terroristische Aktivitäten, die mit virtuellen Währungen und den Schwarzmärkten des Darknets arbeiten, tauchen immer schneller auf unterscheiden sich hinsichtlich ihres technischen Reifegrads, der Widerstandsfähigkeit und der Ziele oft beträchtlich“, erklärt Projektkoordinator Ross King. In den nächsten drei Jahren werden deshalb mit einem Projektvolumen von fünf Millionen Euro technische Lösungen entwickelt, die bei der **Eindämmung von Cyberverbrechen und Terrorismus** helfen. In Titanium werden aber nicht nur **forensische Werkzeuge** entwickelt, sondern auch Fragen zur Privatsphäre und anderen fundamentalen Bürgerrechten bei kriminaltechnischen Untersuchungen behandelt. Im Fokus stehen virtuelle Währungen, Onlineforen, Peer-to-Peer Netzwerke im Darknet und von Ermittlungsbehörden sichergestellte Gerätschaften.

Neues mächtiges Analysewerkzeug für Fintechs

Die **AIT Analyseplattform bietet aber auch wertvolle Dienste für die Wirtschaft**. Die ForscherInnen rund um **Ross King** und **Bernhard Haslhofer**, Projektleiter von GraphSense, beschäftigen sich in Forschungsprojekten auf internationaler Ebene schon länger intensiv mit der Struktur und der Dynamik virtueller Währungssysteme. Unzählige **Fintechs**, aber auch **Energieversorger**, **Banken** und viele andere Branchen wollen virtuelle Währungen und die schnelle, kostengünstige und sichere Blockchain-Technologie (siehe Anhang: Was ist eine Blockchain?) für sich nutzen. Denn sie ermöglichen direkte, weltweite Transaktionen, ohne dass etwa eine Bank oder ein Vermittler zur Authentifizierung notwendig ist. Deshalb fallen auch nur relativ geringe Transaktionskosten an, wenn beispielsweise auch nur ein Euro in die USA überwiesen wird.

Die vielen neuen Möglichkeiten, die sich durch diese dezentrale und zugleich transparente und sichere Zahlungsform und Transaktionstechnologie ergeben, hat in den letzten Jahren

besonders die Finanztechnologie-Industrie beflügelt. Fintechs bieten schon in allen Bereichen Lösungen an – ob für mobile Bezahllösungen, Social Trading oder Anlageberatung – und bereiten der alten Banken- und Finanzindustrie Konkurrenz, die deswegen ebenfalls kräftig in die neuen Technologien investiert. Besonders das Finanzwesen wird derzeit vom digitalen Wandel voll erfasst.

Doch wie kann man die mit virtuellen Währungen verbundene, rapide anwachsende Datenmenge effizient verarbeiten und mittels effektiver Analyseverfahren die richtigen Schlüsse ziehen? Die am AIT entwickelte „Big Data" Analyseplattform **GraphSense kann hunderte Gigabyte in wenigen Minuten verarbeiten** und ist durch die darunterliegende verteilte und somit skalierbare Rechner-Infrastruktur auch für die Zukunft gerüstet. „Wir verstehen virtuelle Währungen, können sie genau analysieren und auch künftige Entwicklungen abschätzen", erklärt Ross King. Die bekannteste Währung Bitcoin wurde vom AIT für blitzschnelle Analysen schon komplett auf den eigenen Serverstrukturen erfasst.

Dienste rund um die Blockchain

Viele Unternehmen setzen bereits auf virtuelle Währungen. Wer sich in diesen neuen, sehr zukunftsträchtigen Markt begeben will, für den ist es wichtig, die neuen Zahlungswege auch von Grund auf zu verstehen. So ist etwa Bitcoin prinzipiell eine hochtransparente Währung, bei der Transaktionen öffentlich einsehbar sind und sich Zahlungsflüsse genau nachvollziehen lassen. Auch wenn die einzelnen Transaktionen anonym sind, kann mittels Netzwerkanalyseverfahren genau nachvollzogen werden, welche Adressen miteinander in Beziehung stehen und welche Summen zwischen Akteuren geflossen sind. Mittlerweile gibt es eine Vielzahl von Kryptowährungen und Blockchaindiensten, die sehr unterschiedlich aufgebaut sind. Neben öffentlichen Blockchains wie Bitcoin gibt es auch private Blockchains, die etwa nur für Unternehmenskunden offenstehen und unterschiedliche Berechtigungsbereiche umfassen.

GraphSense soll Benutzer dabei unterstützen, die Struktur und Abläufe in verteilten, Blockchain-basierten Services und Diensten zu erfassen und diese besser zu verstehen. Neben dem derzeitigen Hauptanwendungsgebiet „Virtuelle Währungsanalyse" wird derzeit der Einsatz des Tools auch für andere Anwendungsbereiche, wie zum Beispiel dem Energie-Sektor, evaluiert.

Data Science Lösungen made in Austria

Die Forschungsaktivitäten des AIT rund um das Themengebiet „Virtuelle Währungen" und „Blockchain Technologie" konzentrieren sich in der **Forschungsgruppe Digital Insight Lab** im **Center for Digital Safety & Security**. Ein **interdisziplinäres Team aus Data Scientists** konzentriert sich darauf, neue Erkenntnisse aus großen Datenbeständen durch die

Anwendung quantitativer Methoden und Techniken auf skalierbare Datenverarbeitungs- und Analyse-Infrastrukturen zu gewinnen. Von der ersten Problemformulierung über die Datensammlung, den Analysen, Visualisierungen und der Veröffentlichung bis hin zur sicheren Langzeitspeicherung und Reproduzierbarkeit wird der gesamte Datenlebenszyklus abgedeckt. **Helmut Leopold**, Head of Center for Digital Safety & Security: In den Bereichen Cyber Security und Data Science haben wir und heute erfolgreich als international anerkannter Akteur positioniert, wie nicht zuletzt die neue große EU-Initiative Titanium erfolgreich zeigt."

Berichterstattung in der internationalen Presse

- Dark Reading (news portal for information security community) "International Consortium Launches to Prevent Criminal Use of Dark Web and Virtual Currencies" http://www.darkreading.com/threat-intelligence/international-consortium-launches-to-prevent-criminal-use-of-dark-web-and-virtual-currencies/d/d-id/1328917
- The Scotsman (main Scottish daily newspaper) "Blockchain consortium seeks to tackle cyber crime" http://www.scotsman.com/business/companies/tech/blockchain-consortium-seeks-to-tackle-cyber-crime-1-4453230
- Law Enforcement Cyber Center "Blockchain consortium seeks to tackle cyber crime" http://www.iacpcybercenter.org/news/blockchain-consortium-seeks-tackle-cyber-crime/
- AIT Presseaussendung „Internationale Forschung gegen die kriminelle Nutzung des Darkweb und virtueller Währungen" https://www.ait.ac.at/news-events/single-view/detail/4861/

Kurz erklärt

Was ist eine Blockchain?

Die Blockchain-Technologie, ursprünglich für die Internet-Währung Bitcoin entwickelt, könnte laut Experten das nächste große Ding sein, dass viele Bereiche des Wirtschaftslebens und der Gesellschaft revolutionieren wird. Zumindest scheint dies im Bereich digitaler Finanztransaktionen bereits zuzutreffen. Bei der Blockchain-Technologie handelt es sich eigentlich nur um eine verteilte, selbstverwaltete Datenbank zur Speicherungen von Transaktionen jeglicher Art – etwa auch Verträge oder Wertpapiere - die in Blöcken zusammengefasst werden. Es können also Werte ohne Intermediär (Vermittler) ausgetauscht werden. Die Technologie ist ein neutrales System der Informationsverarbeitung, ein Peer-to-Peer-Netz, das niemanden bzw. allen gehört und bietet eine automatisierte, fälschungssichere und für alle teilnehmenden Akteure einsichtige

Notarfunktion. Damit bietet sie der digitalen Ökonomie eine zuverlässige Basis für eine vertrauensvolle Zusammenarbeit und stellt Informationen revisionssicher zur Verfügung. Mit der Blockchain können neben Währungen auch viele automatisierte Dienste, sogenannte Smart Contracts, gestaltet werden, die dank der hinterlegten, unveränderbaren Dokumente und der direkten Abwicklung für die Finanzindustrie, Logistikbranche und vielen weiteren Sektoren, etwa auch für Behörden im E-Government, ein riesen Potenzial bieten. Hier werden meist private Blockchains eingesetzt, die nur für einen gewissen Kundenkreis offenstehen.

Fest verkettet

Die Blockchain besteht aus einer unveränderbaren, zusammenhängenden Kette von Blöcken mit einer bestimmten Anzahl von Transaktionen, die durch sogenannte Miner in einem Proof-of-Work-Verfahren erstellt werden. Für diese rechenintensive Arbeit (zur Erstellung eines neuen, unveränderbaren Blocks muss eine richtige kryptografische Hash-Funktion ermittelt werden, wofür nach dem Zufallsprinzip einige Milliarden möglicher Zahlenkombinationen mittels einer speziellen Software ausprobiert werden), werden die Miner selbst mit Bitcoins belohnt. Jeder neue Block ist an den vorherigen Block angebunden und enthält die Prüfsumme des vorherigen Blocks und zusätzlich die Prüfsumme der gesamten Kette. Somit ist jeder Transaktionsblock sicher verifiziert, signiert und versiegelt. Bei Bitcoin wird beispielsweise alle 10 Minuten ein neuer Block erstellt.

Kontakt:

Dr. Ross King
Head of Digital Insight Lab
AIT Austrian Institute of Technology
Center for Digital Safety & Security
T +43(0) 50550-4271 | M +43(0) 664 825 1045
ross.king@ait.ac.at | http://www.ait.ac.at

Mag. (FH) Michael W. Mürling
Marketing and Communications
AIT Austrian Institute of Technology
Center for Digital Safety & Security
T +43 (0)50550-4126 | M +43 (0)664 2351747
michael.muerling@ait.ac.at | www.ait.ac.at