Elitenetzwerk Bayern

Einblicke in die Forschungsarbeit

MASTERARBEIT

„Forensische Aufklärung von IT Sicherheitsvorfällen mithilfe der Blockchain Technologie“

BENEDIKT PUTZ

Elitestudiengang „Honors“-Wirtschaftswissenschaften

Universität Regensburg, Dezember 2018

Forensische Aufklärung von IT Sicherheitsvorfällen

Benedikt Putz hat innerhalb des Elitestudiengangs „Honors“-Wirtschaftswissenschaften den M.Sc. Wirtschaftsinformatik an der Universität Regensburg absolviert. Im Rahmen seiner Masterarbeit beschäftigte er sich damit, wie Blockchain Systeme für den Unternehmenseinsatz beitragen können, IT Sicherheitsvorfälle in Unternehmen aufzuklären und die Täter vor Gericht haftbar zu machen.

Blockchain Technologie im Unternehmenseinsatz

Viele kennen den Begriff Blockchain nur im Zusammenhang mit Bitcoin, der virtuellen Kryptowährung, die Anfang 2018 durch enorme Wertzuwächse öffentliches Aufsehen erregte. Dahinter versteckt sich aber eine Technologie, die in Unternehmen auch für ganz andere Zwecke eingesetzt werden kann. Blockchain Systeme, oder allgemeiner Distributed Ledgers, verstehen sich als verteilte Transaktionsdatenbanken, die eine gemeinsame Datenbasis für Interaktionen zwischen unabhängigen Teilnehmer ermöglichen. Dabei sind die Teilnehmer gleichberechtigt und es gibt keine zentrale Instanz, die den Informationsfluss oder die Daten kontrolliert. Der erste Teil der Arbeit von Benedikt Putz beschäftigt sich wissenschaftlichen Aufarbeitung der Grundlagen und sicherheitsrelevanten Aspekte der Blockchain Technologie.

In den Jahren 2017 und 2018 wurden erstmals Blockchain Frameworks entwickelt, die frei im Internet verfügbar sind. Diese Frameworks ermöglichen Softwareentwicklern, neue Anwendungen auf Basis der Blockchain zu entwickeln. Der zweite Teil der Arbeit entwickelte erstmals einen strukturierten Ansatz, diese Blockchain Frameworks zu vergleichen und auf ihre Tauglichkeit für den Unternehmenseinsatz zu überprüfen. Die Ergebnisse zeigten, dass die vorhandenen Frameworks noch nicht ausgereift sind und oft noch wichtige (teils sicherheitsrelevante) Features fehlen (Stand: Juli 2018). Nichtsdestotrotz bieten sie eine gute Basis, um die Anwendbarkeit der Technologie zu überprüfen und Prototypen zu erstellen.

Forensische Aufklärung von Sicherheitsvorfällen

Die Aufklärung von Sicherheitsvorfällen in IT Systemen erfolgt in der Regel über Log-Einträge (Logs), die von vielen Anwendungen kontinuierlich generiert werden. Da diese Logs als Dateien auf einer Festplatte repräsentiert werden sind sie prinzipiell veränderbar. Dies erschwert die Beweisführung in der forensischen Aufklärung, da hierbei sichergestellt werden muss, dass der Beweis nicht mutwillig abgeändert wurde.

Der dritte Teil der Arbeit beschäftigte sich damit, wie mit Hilfe der Blockchain die Unveränderbarkeit der Logs sichergestellt werden kann. Im vorgeschlagenen Konzept geschieht dies durch Speicherung eines Fingerabdrucks des Log-Eintrags (Hash-Wert) in der verteilten Blockchain-Datenbank. Da die Knoten des Blockchain Netzwerks von unabhängigen Organisationen oder Organisationseinheiten verwaltet werden, ist so die Unveränderbarkeit der Fingerabdrücke gewährleistet. Bei der forensischen Aufklärung können diese Fingerabdrücke dann mit den Original-Dateien verglichen werden, um deren Unberührtheit nachzuweisen.

Zur Implementierung eines Prototyps wurden nun die Ergebnisse des Framework-Vergleichs aus dem vorhergehenden Abschnitt genutzt. Der Prototyp diente vor allem zur Evaluation der Performanz und Sicherheit des Systems. Im Rahmen des vom BMBF geförderten DINGfest Forschungsprojekts wurde die Anwendung an die bestehende Sicherheitsinfrastruktur angebunden, um die Praxistauglichkeit zu gewährleisten.

Benedikt Putz setzt aktuell seine Arbeit an diesem Thema im Rahmen seines Promotionsvorhabens am Lehrstuhl für Wirtschaftsinformatik I fort.

Mehr zum Elitestudiengang „Honors“-Wirtschaftswissenschaften:

https://www.honors.de