Management von Informationssicherheitsaudits mithilfe von Verteilten Systemen und Blockchains

Lukas König, FH St. Pölten

Michael Feldmann, FH St. Pölten

Martin Pirker, FH St. Pölten

Peter Kieseberg, FH St. Pölten

Abstract. Informationssicherheit wird aufgrund der steigenden Bedrohungen im digitalen Raum immer wichtiger. Besonders bei Lieferketten ist es unverzichtbar darauf zu achten, dass alle teilnehmenden Unternehmen ein adäquates Schutzniveau erreicht haben, da Schwachstellen in einer Organisation die gesamte Lieferkette gefährden können.
Wir stellen ein Konzept für Blockchain-basierte, verteilte Informationssicherheitsaudits vor, bei dem Firmen sich gegenseitig ihr Schutzniveau beweisen können, und Vertrauen in die Sicherheit der Lieferkette gesteigert wird.

Keywords: Blockchain, Verteilte Systeme, Informationssicherheit, Distributed Audit, Lieferkette

Beitrag im Rahmen des 16. Forschungsforums der österreichischen Fachhochschulen von 19.-20. April 2023 an der FH St. Pölten.

1 EINLEITUNG

Das Absichern von Lieferketten wird für moderne Unternehmen immer mehr zu einem zentralen Aspekt ihrer gesamtheitlichen Risikobetrachtung. Sicherheit und Resilienz [1] der zugrundeliegenden IKT-Systeme spielen hierbei eine immer größer werdende Rolle, wie auch von der EU erkannt wurde, und mit dem Cyber Resilience Act [2] genau diese Thematik auf legislativer Ebene aufgegriffen wird. Informationssicherheitsüberprüfungen, besonders im Rahmen von weltweit etablierten Normen wie der ISO 27001 [3], erfüllen den Zweck einer unabhängigen und objektiven Betrachtung des Sicherheitsniveaus eines Unternehmens.

Wenn nun alle Organisationen einer Lieferkette eine solche Zertifizierung erlangt haben, kann davon ausgegangen werden, dass demnach die Mühen jeder einzelnen Organisation gesamtheitlich betrachtet ein Vielfaches an Mehrwert für alle Beteiligten erbringen. Eine Überprüfung dieser Art legt jedoch sensible Informationen über bspw. die Sicherheitslücken einer Organisation offen, wodurch ein Teilen dieser Ergebnisse nicht im eigenen Schutzinteresse liegt.

Der Austausch von Informationen über Sicherheitsvorfälle, sowie technische und organisatorische Maßnahmen, die an externe Dritte übermittelt werden, erfordert ein hohes Maß an Vertrauen. Solche Informationen können offensichtliche Schwachstellen einer Organisation aufzeigen und stellen daher eine Bedrohung für die allgemeine Informationssicherheit dar.

In diesem Vortrag wird das Konzept eines neuartigen Systems beschrieben, mit dem Vertrauen in die Sicherheit der IKT-Systeme einer Organisation auf einer B2B-Ebene geschaffen werden kann, ohne dass sensible und sicherheitskritische Informationen veröffentlicht werden müssen. Die zentrale Frage lautet darum wie folgt:

> *Wie können Blockchains und verteilte Systeme dazu genutzt werden, um Vertrauen und Transparenz zu Informationssicherheits-Audits diverser Organisationen über ganze Lieferketten zu gewährleisten?*

Um diese Frage zu beantworten untersuchen wir die Möglichkeit der Nutzung von Blockchains und verteilten Systemen, um Informationen über Informationssicherheitsaudits sicher und transparent zwischen Organisationen auszutauschen, um so Vertrauen und Sicherheit von Lieferketten zu stärken. Ahmad et al. [4] beschreiben, dass Blockchains eine ideale Technologie für so ein Vorhaben sind, unter Anderem wegen der herausragenden Fähigkeit zur Dokumentation und Registerführung.

2 METHODEN

Zu Beginn werden wichtige Kerninformationen und Begriffe diskutiert, die eine Grundlage zum Verständnis der Thematik bilden. Anschließend wird ein Konzept vorgestellt und beschrieben, mit dem die Problematik der Forschungsfrage gelöst werden kann.

3 GRUNDLAGEN

3.1 Blockchain Technologie und Verteilte Systeme

Panwar und Bhatnagar [9] beschreiben eine Vielzahl an Blockchains und verteilten Systemen in ihrer Arbeit. Dabei inkludiert sind Systeme wie DAG (gerichtete azyklische Graphen), und die Agent-zentrierte Holochain. Zentraler Aspekt dieser Arbeit liegt jedoch auf der Speichertechnologie Blockchain selbst, welche sich durch verbesserte Sicherheitseigenschaften, herausragende Fähigkeiten zur lückenlosen Datenaufzeichnung, und Unveränderlichkeit auszeichnet.

Da für ein System wie das hier geplante die Interoperabilität zwischen einzelnen Strängen von Blockchains fundamental ist werden zwei Frameworks näher betrachtet, die diese Anforderungen erfüllen. Dabei handelt es sich um einerseits das Agent-zentrierte System Holochain[1], und andererseits das modulare Blockchain-Framework Substrate[2]

Bei Holochain ist das zentrale Element ein globales Regel-Set im Netzwerk, welches als DNA bezeichnet wird. Mit dieser DNA werden die individuell betriebenen verketteten Daten der einzelnen Teilnehmer im Netzwerk validiert.

Das Blockchain-Framework Substrate basiert auf der Polkadot-Blockchain und ermöglicht ebenfalls das Betreiben von lokalen Blockchains, welche dann über eine globale Polkadot-Blockchain miteinander interoperabel sind. Diese Möglichkeit der Nutzung von mehreren „Schichten“ von Blockchains ermöglicht beispielsweise das Betreiben einer firmeninternen Blockchain, bei der gezielte Informationen dann in eine globale Blockchain übermittelt werden können, bei der mehrere Firmen teilnehmen, wie bei einer Lieferkette.

3.2 Informationssicherheitsaudits

Informationssicherheitsaudits sind ein wichtiger Bestandteil zur Ermittlung des Sicherheitsniveaus einer Organisation [10]. Besonders in Hinblick auf zertifizierte Informationssicherheitsmanagementsysteme (ISMS) sind unabhängige Überprüfung unerlässlich. Audits helfen Organisationen dabei die Einhaltung ihrer Sicherheitsziele zu garantieren.

3.3 Verteilte Audits und Risikomanagement

Böhme [5] beschreibt in seiner Arbeit die Zusammenhänge von sicheren Lieferketten und dem Sicherheitsniveau einer einzelnen Organisation. Schwachstellen an einer einzigen Stelle können langfristig die gesamte Lieferkette gefährden. Demnach ist es nicht nur wichtig, dass eine einzelne Organisation regelmäßig Sicherheitsüberprüfungen durchführt, sondern alle teilnehmenden Organisationen einer Lieferkette.

Obwohl das Absichern von Lieferketten immer wichtiger wird gibt es weiterhin einen Mangel an wissenschaftlichen Arbeiten zu diesem Thema. Bisherige Publikationen zu verteilten Audits befassen sich beispielsweise mit Metriken für Reifegrade des Sicherheitsniveaus [6], Aufzeichnungen von Netzwerk-Monitoring [7], oder aber auch dezentrales Risikomanagement [8]. Ein tatsächliches dezentrales System zur Absicherung

[1] https://www.holochain.org/
[2] https://substrate.io/

und Kommunikation von Informationssicherheitsaudits ist jedoch noch nicht beschrieben.

4 ANSATZ

Ein grundlegender Ansatz für ein verteiltes Audit-System umfasst externe und interne Informationssicherheitsaudits, d.h. Prüfungen, die von jedem Unternehmen selbst durchgeführt werden, sowie Prüfungen von externen, unabhängigen Prüfern. Sicherheitsaudits können eine Menge sensibler Informationen über ein Unternehmen ans Licht bringen. Unabhängig davon, ob das Ergebnis eines Audits positiv oder negativ ausfällt, werden durch ein Audit implizit wichtige Informationen über Unternehmensstrategien und Geschäftsabläufe offengelegt.

Aus diesem Grund sollte ein Genehmigungsmodell eine Trennung zwischen Organisation gewährleisten. Dadurch kann garantiert werden, dass sensible Informationen nur von dazu berechtigten Stellen eingesehen werden können. Also firmenintern, extern, und eine Sonderstellung für unabhängige Prüfstellen. Es handelt sich also um ein System, bei dem Vertrauen zwischen Firmen durch Vertrauen in die Technologie sichergestellt wird.

5 KONZEPT

Das Grundkonzept des verteilten Audit-Systems besteht darin, dass jede teilnehmende Organisation eine lokale/interne Version einer Blockchain betreibt, auf der die Ergebnisse von Informationssicherheitsüberprüfungen gespeichert werden (siehe Abbildung 1). Diese lokalen und organisationsinternen Überprüfungen können sowohl als internes Audit, wie auch als externes Audit durch eine unabhängige Prüfstelle durchgeführt werden. Jede Organisation kann auf der internen Blockchain beliebig viele Überprüfungen durchführen, und die Ergebnisse dadurch manipulationssicher und miteinander verknüpft aufbewahren.

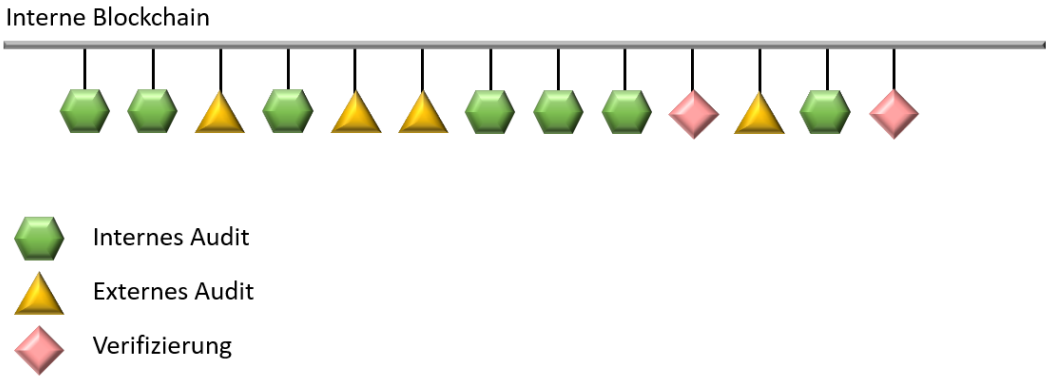

Abbildung 1: Darstellung einer organisationsinternen Blockchain zur Aufzeichnung von Audits

Um, beispielsweise als Teil einer Lieferkette, anderen Organisationen das Sicherheitsniveau der eigenen Organisation beweisen zu können wird eine globale Blockchain verwendet (siehe Abbildung 2). Diese wird von einer unabhängigen Stelle betrieben und mit Datenblöcken und Informationen befüllt. Einträge für die globale Blockchain ergeben sich aus Validierungsüberprüfungen der unabhängigen Stelle einer jeder teilnehmenden Organisation. Hierbei wird die Organisation und ihre bisherigen lokalen Blockchain-Einträge überprüft, und dann mittels dafür eingerichteter Funktionen

ein Validierungsblock an die lokale und globale Blockchain angehängt, um sie miteinander zu „verknüpfen“.

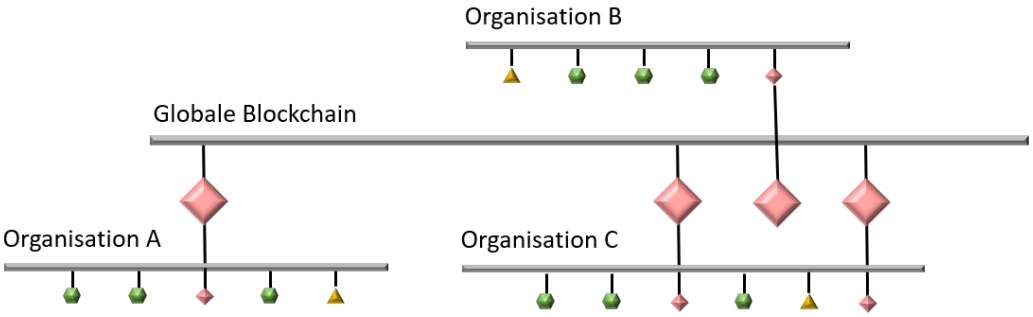

Abbildung 2: Darstellung einer globalen Blockchain zur Validierung von Audits über Organisationen hinweg

6 CONCLUSIO

In dieser Arbeit wird das Konzept eines Blockchain-basierten, verteilten Informationssicherheitsaudits beschrieben. Ein System dieser Art hilft dabei, Vertrauen und Sicherheit über mehrere Organisationen hinweg zu steigern, beispielsweise in Lieferketten. Ein konzeptioneller Prototyp wurde im Zuge dieser Arbeit erstellt, der sich in erster Linie auf die Sicherheitsmaßnahmen und -anforderungen aus der internationalen Norm ISO 27001 orientiert.

Zukünftige Arbeiten werden den Fokus haben, ein praktikables Blockchain-Framework zu identifizieren, oder zu erstellen, damit das hier beschriebene Konzept zum Einsatz kommen kann.

7 REFERENZEN

[1] Boyens, Jon, et al. "Supply chain risk management practices for federal information systems and organizations." NIST Special publication 800.161 (2015): 32.

[2] Europäisches Parlament, Rat der Europäischen Union. „Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)". Amt für Veröffentlichungen der Europäischen Union, Luxemburg.

[3] ISO/IEC (2013). Information technology – Security techniques – Information security management systems – Requirements. Standard, International Organization for Standardization, Geneva, CH.

[4] Ahmad, A., Saad, M., Bassiouni, M., and Mohaisen, A. (2018). Towards blockchain-driven, secure and transparent audit logs. In Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, pages 443–448

[5] Böhme, R. (2012). Security audits revisited. In International conference on financial cryptography and data security, pages 129–147. Springer.

[6] Brotby, W. K. and Hinson, G. (2013). Pragmatic security metrics: applying metametrics to information security. CRC Press

[7] Mounji, A., Le Charlier, B., Zampunieris, D., and Habra, N. (1995). Distributed audit trail analysis. In Proceedings of the Symposium on Network and Distributed System Security, pages 102–112

[8] Ino, E. and Watanabe, K. (2021). The impact of covid-19 on the global supply chain: A discussion on decentralization of the supply chain and ensuring interoperability. Journal of Disaster Research, 16(1):56–60.

[9] Panwar, A. and Bhatnagar, V. (2020). Distributed ledger technology (dlt): the beginning of a technological revolution for blockchain. In 2nd International Conference on Data, Engineering and Applications (IDEA), pages 1–5. IEEE.

[10] Vroom, C. and Solms, R. v. (2003). Information security: Auditing the behaviour of the employee. In IFIP International Information Security Conference, pages 401–404. Springer.