Verarbeitung strafrechtlich relevanter Daten in öffentlichen Cloud-Umgebungen – Ist das möglich?

Martin Morgenstern

Hochschule Stralsund, Zur Schwedenschanze 15 18435 Stralsund

Zusammenfassung

Forensiker übersetzen zur Aufklärung von Straftaten regelmäßig rechtliche Fragestellungen in wissenschaftliche Fragen. Dazu ist es notwendig, Spuren – zunehmend auch digitale Spuren – zu sichern, die einen Tathergang stützen oder widerlegen können. Damit Spuren gerichtlich verwertbar sind, müssen sowohl die Integrität als auch die Authentizität der Spuren nachgewiesen werden. Unter Integrität ist zu verstehen, dass die Spur weder durch die Sicherung noch danach verändert wurde. Die Authentizität einer Spur besagt, dass diese auch tatsächlich die ihr zugesprochene Beweiskraft hat. (Dewald & Freiling, 2015)

In dieser Arbeit wird der Bereich der Digitalen Forensik betrachtet, der oft auch als Computer-Forensik bezeichnet wird. Hierbei könnte die Nutzung von öffentlichen Cloud-Diensten ein ortsunabhängiges und zeitsparendes kollaboratives Arbeiten ermöglichen, sodass keine Datenträger vorgehalten oder versendet werden müssten. Es soll untersucht werden, unter welchen Voraussetzungen digitale Beweismittel gerichtsverwertbar direkt in eine öffentliche Cloud-Umgebung gespeichert werden und verarbeitet werden können, ohne die Integrität und Authentizität zu verlieren.

1. Ausgangssituation

Die Akquise von digitalen Beweismitteln in Strafverfahren hat in den letzten Jahren erheblich an Bedeutung zugenommen. Gleichzeitig sind auch die Datenmengen gestiegen. Seit Jahren ist in der Fachwelt die Notwendigkeit bekannt, Cloud- bzw. Big-Data-Lösungen für IT-Forensik zu nutzen, um die permanent steigende Datenmenge und Fallzahlen effizient bearbeiten zu können. (Tabona & Blyth, 2016) (Hack, 2021) (Jordaan, 2021)

Durch die Nutzung öffentlicher Cloud-Anbieter – wie etwa Amazon AWS und Microsoft Azure – zur Sicherung und Analyse digitaler Beweismittel könnten Ressourcen skalierbar und flexibel genutzt werden. Bisher müssen Forensik-Dienstleister eine große Anzahl an Datenträgern für forensische Sicherungen vorhalten, da diese im Ernstfall sofort verfügbar sein müssen. Eine langfristige Planung, Vorhaltung und Bereitstellung von Datenträgern würde bei der Nutzung öffentlicher Cloud-Anbieter entfallen, da notwendige Ressourcen in wenigen Sekunden hochskaliert werden könnten. Die Nutzung öffentlicher Cloud-Anbieter für die Sicherung und Analyse digitaler Beweismittel scheint in der Fachwelt bisher jedoch aufgrund rechtlich nicht geklärter Fragestellungen oder aufgrund sonstiger Vorbehalte quasi ausgeschlossen zu sein.

Eine denkbare Lösung ist nach Ansicht des Autors die Entwicklung einer Cloud-in-Cloud-Software inklusive entsprechender Upload-Clients, wie in Abbildung 1 dargestellt. In der zu entwickelnden Lösung müssten alle noch zu erhebenden Anforderungen zur Erhaltung der gerichtlichen Verwertbarkeit digitaler Spuren umgesetzt werden.

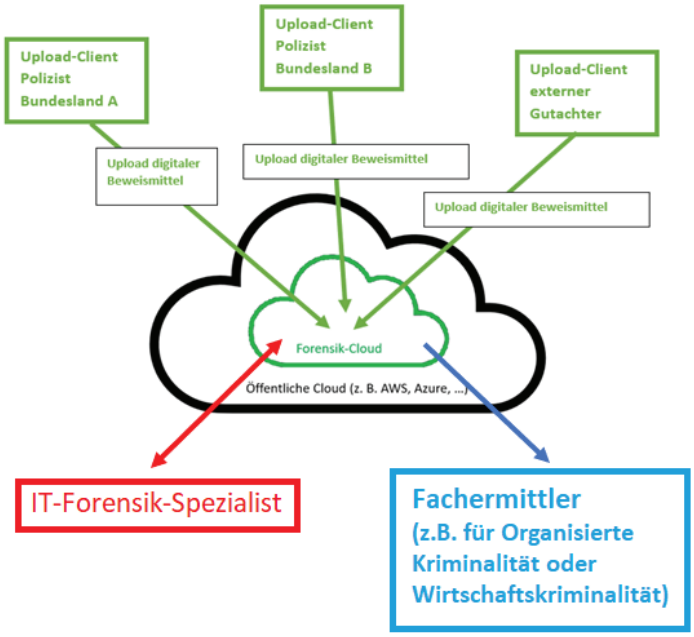

Abbildung 1 Darstellung Forensik-Cloud

2. Relevanz

Für eine effiziente Analyse digitaler Beweismittel ist es notwendig, dass kurzfristig auf geänderte Anforderungen reagiert werden kann. Dies ist schon aus vergaberechtlichen Gründen derzeit eine große Herausforderung für die Polizei. Durch die Nutzung einer öffentlichen Cloud-Infrastruktur kann der momentan vorhandene Bedarf kurzfristiger Anpassungsmöglichkeiten von Auswerteumgebungen in kurzer Zeit realisiert werden.

Der Bedarf an IT-Forensik ist auch außerhalb der Strafverfolgungsbehörden permanent steigend. Beispielsweise hat die kassenärztliche Bundesvereinigung im Januar 2023 Dienstleistungen im Bereich Incident-Response und IT-Forensik im geschätzten Umfang von 500 TEUR für einen Zeitraum von 48 Monaten ausgeschrieben. (Kassenärztliche Bundesvereinigung K. d. ö. R., 2022)

IT-Forensik hat sich in den letzten Jahren zu einem wichtigen Geschäftsfeld privater Unternehmen entwickelt. Aufgrund der zunehmenden Zahl an IT-Forensik-Experten, ist absehbar, dass die Zahl von privaten Forensik-Dienstleistern in den nächsten Jahren zunehmen wird. Gerade für kleine Forensik-Firmen ist die Beschaffung von leistungsfähiger Hard- und Software jedoch eine große Hürde. Durch die Bereitstellung von Cloud-Lösungen für die IT-Forensik, die nicht nur Analyse-Tools, sondern die nahezu die komplett benötige Infrastruktur, beginnend bei der forensischen Sicherung von Daten, umfasst, kann die Einstiegshürde in die Selbstständigkeit für IT-Forensiker deutlich gesenkt werden.

In der IT-Forensik gibt es viele Spezialgebiete, deren Anzahl permanent steigend ist. Neben der Quantität an Daten nimmt jährlich auch die Anzahl möglicher Datenquellen zu (Morgenstern et al., 2022). Dies hat dazu geführt, dass gerade kleinere Forensik-Dienstleister sich häufig auf einen Bereich der Computerforensik spezialisiert haben. Hierbei kann es sich um Spezialisten für die Auswertung bestimmter Datenarten, z.B. Multimedia-Forensik (Böhme et al., 2009), aber auch um Spezialisten für bestimmte Datenquellen handeln wie etwa KFZ-Forensik (Hansen, 2021). Die zu entwickelnde Forensik-Cloud soll eine anbieterunabhängige Möglichkeit zur Zusammenarbeit verschiedenster IT-Forensik-Spezialisten ermöglichen.

3. Methodik

Zur Schaffung eines ersten Überblicks der Thematik wurde ein Scoping-Review durchgeführt. Basierend auf den Erkenntnissen des Scoping-Reviews werden Experten-Interviews nach Helfferich vorbereitet. (Helfferich, 2014)

Als Experten werden Personen mit langjähriger Erfahrung im Bereich Computerforensik oder Cybercrime-Ermittlungen interviewt. Weitere Auswahlkriterien für die Experten sind:

- Prozesserfahrung der Experten
- Verschiedene Rollen der Experten (z. B. externe Gutachter und polizeiliche Ermittler)
- Verfügbarkeit der Experten im geplanten Befragungszeitraum

Insgesamt sollen vier oder fünf Experten befragt werden. Die Interviews werden im April und Mai 2023 durchgeführt und mit einer qualitativen Inhaltsanalyse nach Mayring ausgewertet (Mayring, 2016). Die Ergebnisse der Interviews sowie der sonstigen Recherchen werden genutzt, um Anforderungen an eine Forensik-Cloud zu definieren. Die definierten Anforderungen werden in verschiedene Kategorien – etwa rechtliche und funktionale Anforderungen – unterteilt. Im nächsten Schritt soll eine Prioritätenliste der Anforderungen erstellt werden. Dabei werden die Anforderungen in unverzichtbare und optionale Anforderungen eingeteilt; erstere werden bei der Priorisierung höher bewertet.

Als Ergebnis des Projekts soll ein Demonstrator entwickelt werden, der sowohl die Server- als auch die Clientsoftware enthält. Die Entwicklung soll agil und im ständigen Austausch mit der Fachwelt erfolgen. Mögliche Organisationsformen sind Scrum oder Kanban.

4. Zwischenergebnisse und Ausblick

Es wurde dargelegt, dass aufgrund permanent steigender Quantität und Komplexität von Daten deren Akquise und Auswertung mit traditionellen Methoden bereits heute kaum noch umsetzbar sind. Es gibt bereits Lösungsansätze und Produkte mit denen Daten in Cloud-Umgebungen bzw. einer klassischen Client-Server-Architektur gesichert und analysiert werden können. Die bisherigen Lösungen sind jedoch herstellerabhängig.

Ein primäres Ziel des Forschungsprojekts ist es, eine gerichtsfeste Sicherung digitaler Beweismittel direkt in Cloud-Umgebungen für jedermann zu ermöglichen, unabhängig

ob es sich dabei um Polizisten oder Privatpersonen handelt, die Opfer eines Cyberangriffs geworden sind. Dies ist mit bisherigen Lösungen nach Ansicht des Autors nicht möglich, da sowohl technisches Spezialwissen als auch häufig die Konfiguration einer Client-Software notwendig sind.

Im geplanten Forschungsvorhaben liegt der Fokus bei der Speicherung und gemeinsamen Analyse strafrechtlich relevanter Daten in öffentlichen Cloud-Umgebungen. In einem möglichen Folgeprojekt kann untersucht werden, wie ein rechtssicherer Zugriff von Justiz und Anwälten auf relevante Verfahrensdaten umgesetzt werden kann.

5. Literaturverzeichnis

Böhme, R., Freiling, F., Gloe, T., & Kirchner, M. (2009). *Multimedia-Forensik als Teildisziplin der digitalen Forensik* [Aufsatz]. https://subs.emis.de/LNI/Proceedings/Proceedings154/gi-proc-154-115.pdf

Dewald, A., & Freiling, F. C. (Hrsg.). (2015). *Forensische Informatik* (2. Auflage). BoD - Books on Demand.

Hack, U. (2021, September 8). What's the real story behind the explosive growth of data? *Redgate*. https://www.red-gate.com/blog/database-development/whats-the-real-story-behind-the-explosive-growth-of-data

Hansen, S. (2021, Dezember 23). *Car-Forensiker: Wie werden eigentlich Daten aus den Autos analysiert?* [Heise online]. c't Magazin. https://www.heise.de/news/Car-Forensiker-Wie-werden-eigentlich-Daten-aus-den-Autos-analysiert-6292428.html

Helfferich, C. (2014). Leitfaden- und Experteninterviews. In N. Baur & J. Blasius (Hrsg.), *Handbuch Methoden der empirischen Sozialforschung* (S. 559–574). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-531-18939-0_39

Jordaan, J. (2021). *2021 SANS Digital Forensics Survey: Digital Forensic Essentials and Why Foundations Matter*. https://www.sans.org/white-papers/40420/

Kassenärztliche Bundesvereinigung K. d. ö. R. (2022, Dezember 16). *Öffentliche Ausschreibung Berlin 2022 Rahmenvertrag digitale Forensik und Incident-Response 2022-12-16*. Öffentliche Ausschreibungen Deutschland. https://ausschreibungen-deutschland.de/1002019_Rahmenvertrag_digitale_Forensik_und_Incident-Response_2022_Berlin

Mayring, P. (2016). *Einführung in die qualitative Sozialforschung: Eine Anleitung zu qualitativem Denken* (6., überarbeitete Auflage). Beltz.

Morgenstern, M., Fähndrich, J., & Honekamp, W. (2022). *Ontology in the Digital Forensics Domain: A Scoping Review*. Gesellschaft für Informatik, Bonn. https://doi.org/10.18420/inf2022_05

Tabona, O., & Blyth, A. (2016). A forensic cloud environment to address the big data challenge in digital forensics. *2016 SAI Computing Conference (SAI)*, 579–584. https://doi.org/10.1109/SAI.2016.7556039