Forensische Artefakte im Umfeld von SAP

Studiengang: MAS Digital Forensics & Cyber Investigation

SAP-Systeme sind geschäftskritisch. Manipulationen oder Angriffe können erhebliche finanzielle Schäden verursachen. Diese Arbeit untersucht, welche forensischen Artefakte im SAP-Umfeld relevant sind, wie sie gesichert werden können und wie Unternehmen ihre Forensic Readiness im SAP-Kontext verbessern können.

Ausgangslage

SAP-Systeme übernehmen in Unternehmen zentrale Aufgaben und kritische Geschäftsprozesse. Manipulationen durch externe Angriffe oder interne Betrugsfälle können erheblichen finanziellen Schaden verursachen und Ermittlungen durch Behörden oder Revision nach sich ziehen. Aufgrund der hohen Komplexität von SAP und der Vielzahl an Komponenten, stellt die forensische Untersuchung solcher Vorfälle eine besondere Herausforderung dar.

Ziel

Ziel dieser Arbeit war es, relevante forensische Artefakte im Umfeld von SAP zu identifizieren und Möglichkeiten für deren Sicherung aufzuzeigen. Darüber hinaus sollten Handlungsempfehlungen abgeleitet werden, wie Unternehmen ihre Systeme gezielt so konfigurieren können, dass forensische Analysen effizienter und zuverlässiger durchgeführt werden können.

Vorgehen

Die Arbeit folgt einem explorativen Forschungsansatz und kombiniert Literaturrecherche, Expertenaustausch und praktische Systemanalysen. Untersucht wurden die in einem Unternehmen eingesetzten SAP S/4HANA On-Premise-Systeme. Dabei wurden sowohl klassische Logs auf Betriebssystemebene als auch SAP-spezifische Artefakte und Werkzeuge analysiert. Ergänzend wurde der aktuelle Forschungsstand mit praxisnahen Experimenten abgeglichen, um sowohl die theoretische Relevanz als auch die praktische Anwendbarkeit der Artefakte zu überprüfen.

Ergebnisse

Die Ergebnisse zeigen, dass eine Vielzahl forensisch relevanter Artefakte existiert, darunter Logdateien, Änderungsprotokolle, Benutzer- und Systemaktivitäten sowie Konfigurationseinstellungen. Ihre Sicherung erfordert jedoch einen hybriden Ansatz, der sowohl klassische forensische Methoden auf Dateisystemebene als auch den Einsatz von SAP-internen Tools und Reports umfasst. Zudem konnte aufgezeigt werden, dass bestimmte Artefakte nur mit SAP-spezifischen Mechanismen zugänglich sind, was eine saubere Dokumentation und Validierung der Vorgehensweise unverzichtbar macht.

Die Arbeit verdeutlicht, dass das Themenfeld aufgrund der Komplexität von SAP-Systemen sehr gross ist und nicht vollständig abgedeckt werden kann. Sie schafft jedoch eine fundierte Grundlage, auf der zukünftige Analysen und Konzepte aufbauen können. Entweder durch die Entwicklung standardisierter Verfahren, die Vertiefung spezifischer Artefakte oder durch die Integration ausgewählter Artefakte in zentrale Monitoring-Systeme wie Splunk. Damit eröffnet die Arbeit nicht nur eine theoretische Perspektive, sondern liefert auch konkrete Anknüpfungspunkte für die Praxis.

Remo Sieber