Titel: Die DSGVO und das Problem der Löschung von Daten in Datenbanken.

Einleitung: In der Umsetzung der DSGVO als nationale Implementierung der General Data Protection Regulation (GDPR) dominieren in der derzeitigen Debatte die Themen der Datenanonymisierung, sowie des korrekten Einholens von Zustimmung (Consent). Weitere wesentliche Aspekte der DSGVO betreffen allerdings die Themen der Richtigstellung von Informationen, der Möglichkeit des Zurückziehens der Zustimmung, sowie der Löschung von Daten. Letzteres, obwohl ein fundamentales Recht, wird derzeit in Diskussionen nur sehr rudimentär und als nicht so bedeutend betrachtet, obwohl die Implikationen auf technischer Ebene große Bedeutung haben. Dies liegt vor allem darin begründet, dass die Forderung nach Löschung nicht weiter technisch spezifiziert wurde, es derzeit also nicht klar ist, was die Forderung konkret beinhaltet. Geht man nach einer strengen Rechtsauslegung vor, so ist allerdings das reine logische Löschen, d.h. das reine Entfernen aus Suchanfragen, zu wenig [1]. Dies betrifft vor allem komplexe Systeme wie Datenbanken, die speziell auf Transaktionssicherheit und Wiederherstellbarkeit von Daten, bspw. im Rahmen „irrtümlicher“ Löschung oder von Crashes der zugrundeliegenden Infrastruktur, ausgelegt sind, gleichzeitig aber wesentlicher Bestandteil der meisten datengetriebenen Anwendungen und Systeme sind.. Hier ist die Umsetzung der Forderung eines nichtrückgängig machbaren Löschens speziell problematisch in Hinblick auf forensischer Verfahren zur Wiederherstellung eben dieser Daten.

Methode: Anhand der internen Strukturen von MySQL erläutern wir schrittweise wie bereits gelöschte Daten wieder hergestellt werden könne, wobei wir stufenweise vorgehend immer komplexere und mächtigere Löschwerkzeuge und Strategien betrachten. Die betrachteten Analysetechnologien benötigen dabei unterschiedliche technologische Fertigkeiten des Angreifers, basieren jedoch auf bereits publizierten und in der akademischen Forschung rezipierten forensischen Methoden. MySQL ist dabei ein perfektes Illustrationsbeispiel, da die zugrundeliegenden Technologien sehr ähnlich zu anderen etablierten Datenbankmanagementsystemen (DBMS) sind, die Quelloffenheit gleichzeitig aber eine tiefgehende und überprüfbare Analyse ermöglicht. Viele der aufgegriffenen Probleme gelten dabei in leicht abgewandelter Form auch für viele Dateisysteme.

Ergebnisse: In diesem Paper analysieren wir die Schwierigkeit des Löschens von Daten aus Datenbanken und andere komplexen, indexbasierten Speichersystemen basierend auf Methoden der Datenbankforensik. Dazu wird auch auf die extrem schwierige Frage des Cut-Offs zwischen der Forderung maximalen Datenschutzes und gleichzeitiger Nutzbarkeit allgegenwärtiger Technologien und Systeme eingegangen, wobei wir existierende

Lösungsansätze evaluiert und verglichen haben und entsprechende forensische Gegenmaßnahmen, bzw. andere Probleme wie unrealistische Annahmen aufzeigen werden.

Diskussion/Conclusio: In dieser Arbeit kumulieren wir Erkenntnisse der Datenbankforensik der letzten Jahre und geben einen Überblick über die Konsequenzen in Hinblick auf die Nutzung von Datenbanken zur Verwaltung sensibler personenbezogener Daten und des Löschens ebendieser. Dabei werden wir das Problem auf mehreren Ebenen betrachten, je nach forensischer Expertise des Angreifers, sowie der Wirksamkeit der eingesetzten Löschmechanismen. Diese Darstellung ist unserer Meinung nach wichtig für die weitere Diskussion, was Löschen im Rahmen der DSGVO/GDPR tatsächlich bedeuten darf und kann und wo die roten Linien in Hinblick auf die Forderung der Unmöglichkeit der Wiederherstellung zu ziehen sind.

Quellen:

[1] Villaronga, E.F., et al., 2018. Humans forget, machines remember: Artificial intelligence and the right to be forgotten. Computer Law & Security Review, 34(2), pp.304-313. [2]