B. Mitschang et al. (Hrsg.): Datenbanksysteme für Business, Technologie und Web (BTW 2017),
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2017 597

Fraud Detection 2.0 – Real Time SIP Analytics mithilfe von Complex Event Processing

Markus Schneider[1]

Abstract

Das Ziel des zweijährigen Forschungsprojektes war es, eine Weiterentwicklung der auf dem Markt bereits existierenden Fraudlösungen mithilfe eine CEP-Lösung zu schaffen. Die herkömmlichen Lösungen zeigen Schwächen, weil sie die im Nachgang eines Gespräches aufgezeichneten Abrechnungsdaten (CDR-Call Detail Records) analysieren. Die hier beschriebene Entwicklung analysiert die beim Verbindungsaufbau einer VoIP-Sprachverbindung notwendigen SIP-Signalisierunginformationen (Invites). Somit können Anomalien bereits vor Gesprächsbeginn erkannt werden. Eine nachgelagerte Verarbeitung und Analyse der CDR's birgt immer die Gefahr, dass ein Schaden erst „ex post" erkannt und vermieden werden kann. Insofern redet man hier auch allgemein von einer Schadensminimierung. Eine „ex ante" Missbrauchserkennung mithilfe einer Echtzeitdatenbankanalyse versetzt ein Unternehmen in die Lage, eine Anomalie bereits zu erkennen und demzufolge zu handeln, bevor ein finanzieller Schaden entstehen kann. Die hierbei angewandte Methodik untersucht neben dem Verhalten des Endnutzers hinsichtlich Anomalien während des Verbindungsaufbaus (z.B. Kuba -– diese Destination hat der Endkunde in der Vergangenheit noch nie angewählt), auch eine missbräuchliche Nutzung während eines Gesprächs (Überschreitung von individuellen Thresholds). Anhand der in diesem Projekt eingesetzten Apama Streaming Analytics Platform der Software AG können sehr große Datenmengen in Echtzeit verarbeitet und analysiert werden. Die sogenannten Pattern für die Erkennung der Anomalien wurden von wissenschaftlichen Mitarbeiten der Hochschule Darmstadt in Verbindung mit den Erfahrungen der toplink bezüglich Fraud entwickelt. Die erzielten Ergebnisse wurden in einer Wirkumgebung der toplink GmbH erfolgreich getestet. Diese effiziente Missbrauchserkennung und Vermeidung sorgt nun dafür, dass Telekommunikations-unternehmen dem Thema Fraud zukünftig noch wirksamer entgegnen und somit den finanziellen Schaden für sich und ihre Kunden nochmals deutlich minimieren können.

[1] toplink GmbH, Robert-Bosch-Straße 20, 64293 Darmstadt, markus.schneider@toplink.de