In-Memory-Analytics und Compliance: Innovation trifft Regulatorik

In Zeiten von Big Data spielt die schnelle Auswertung von Daten eine immer wichtigere Rolle. Mit In-Memory-Technologien lassen sich in vielen Bereichen Analysen schneller und gezielter durchführen – auch für die Compliance-Themenbereiche wie Betrug und Geldwäsche. Um Schäden fernzuhalten, müssen Unternehmen Massendaten schnell und zielgerichtet auswerten können. Das ist Grund genug, um existierende Paradigmen in der Sicherheitsarchitektur zu überdenken.

Die Unternehmensverantwortlichen für Informationssicherheit, Risiken und Compliance haben naturgemäß unterschiedliche Sichtweisen auf Gefahren, die auf den Umfang ihrer Aufgabenbereiche und mithin ihrer unterschiedlichen persönlichen Haftung zurückzuführen ist. Allen gemein ist jedoch die Datensicht: Im Falle von externem Betrug und strafbaren Handlungen geht es immer auch um Kunden-, Transaktions-, Produkt- und Authentifizierungsdaten. Um innerhalb von Unternehmen parallele Logiken in der Prävention zu verhindern, braucht es eine konsistente Risikoanalyse, synchronisierte Präventions- und Kontrollmaßnahmen und – mit am wichtigsten – die Möglichkeit, Handlungsmuster von Betrügern schnell zu erkennen und zu bewerten.

Massendaten in Echtzeit abgleichen

Das Erkennen von Handlungsmustern gleicht der Suche nach der Nadel im Heuhaufen. Neben der expliziten regelbasierten Prüfung von bekannten Handlungsweisen können neue Verhaltensmuster gut durch den Abgleich mit erwarteten Mustern erkannt werden. Sind alle Geschäftstätigkeiten berücksichtigt, lassen sich Kunden auf Basis ihrer Verhaltensweise in verschiedene Gruppen einteilen. Durch die Prüfung einzelner geschäftlicher Transaktionen gegen das Muster einer Vergleichsgruppe werden zwar gute Ergebnisse erzielt, diese sind aber teilweise fehlerbehaftet. Um das Risiko eines nicht identifizierten Betrugsversuchs so gering wie möglich zu halten wird ein gewisser Satz an sogenannten „False Positives“ akzeptiert. Dieser liegt meist bei Werten bis zu zwei Prozent, bezogen auf das gesamte Transaktionsvolumen. Den entscheidenden Mehrwert eines modernen Präventionsmodells liefern die Perspektivenumkehr vom Sender auf den Empfänger einer geschäftlichen Transaktion und die verknüpfte Bewertung von Online-Zugangs- und Transaktionsdaten. Dazu ist eine parallele Verarbeitung granularer Informationen erforderlich.

Sopra Steria Consulting hat 2013 auf Basis einer In-Memory-Datenbank einen „Proof of Concept“ durchgeführt, bei dem ein konventionelles Anti-Financial-Crime-Regelwerk bestehend aus 150 einzelnen Regeln implementiert wurde. Diese Lösung bewältigte in vier Minuten die Auswertung der Monatsverarbeitung von zehn Millionen Kunden sowie einer Milliarde Transaktionen. Eine konventionelle Lösung basierend auf relationaler Datenbanktechnologie benötigt dazu bis zu fünfzig Stunden. Allein der Transfer auf eine In-Memory-Technologie brachte eine Zeitersparnis um den Faktor 1200. Derartige Beschleunigung eröffnet die Möglichkeit, von der bekannten Tages- und Wochenendverarbeitung abzuweichen und zeitnahe oder sogar Echtzeitverarbeitung in Angriff zu nehmen: Um eine komplette Tagesendverarbeitung durchzuführen, wurden etwa elf Sekunden benötigt, für das Transaktionsvolumen einer Viertelstunde nur noch 0,4 Sekunden.

Umfassende Regelwerke erforderlich

Die steigenden Compliance-Anforderungen und die damit einhergehenden Gegenmaßnahmen zeigen zunehmend Wirkung: So weichen einfache Betrugsmuster komplexeren Methoden, bei denen viele Akteure zusammenwirken. Komplexe Betrugsmethoden verlangen ausgereifte Detektions- und Präventionsmuster. Die verbesserte Feststellung krimineller Handlungen und ihre Abgrenzung gegenüber legitimen Verhalten sind nur möglich, wenn sich der Kontext hinreichend beurteilen lässt. Um beispielsweise im Bereich Betrugsmanagement komplexe Prozesse transparent zu machen, müssen Unternehmen – je nach Branche – Massendaten aus den unterschiedlichsten Quellen wie zum Beispiel Personenanzahl, Flugbuchungen und Hotelzimmerreservierungen kombinieren.

Eine solche Auswertung lässt sich nur mit umfassenden Regelwerken durchführen, unter anderem mit der Fähigkeit zur Analyse von Beziehungsnetzwerken. Tendenziell verlängern sie die Laufzeiten und produzieren mehr Auffälligkeiten. Dadurch steigt die Anzahl der echten Treffer und die Quote der Fehlalarme wird schlechter. Um dies zu verhindern, sind strengere Regeln mit komplexerer Bedingungsstruktur beziehungsweise Kontra-Indikatoren erforderlich. Sie kennzeichnen legitimes Verhalten und erhöhen die Produktivität der Investigation. Die Laufzeiten steigen eventuell prohibitiv an und die zeitliche Distanz zwischen betrügerischer Aktion und Entdeckung wird größer. Das schränkt die Handlungsmöglichkeiten zur Schadensminderung ein.

Dreistufige Einführung von In-Memory

Die beauftragten Unternehmensverantwortlichen für Informationssicherheit, Risiken und Compliance sind nicht immer in der Lage, die Möglichkeiten von In-Memory-Datenbanken zu erkennen. Denn die fehlende Ex-ante-Transparenz über den erzielbaren Nutzen stellt eine große Hürde dar. Durch eine dreistufige Einführung lässt sich diese leichter überwinden, wenn auf jeder Stufe Transparenz über die erschlossenen Vorteile und die Investition herrscht:

1. Stufe: Technologie-Transformation

Die existierende konventionelle Technologie-Infrastruktur wird durch die neue Infrastruktur ersetzt und die bestehende Prüflogik eins zu eins abgebildet. Dadurch müssen bestehende Prozesse nicht oder nur wenig verändert werden. Investments und Friktionen bleiben gering, die Akzeptanz der Anwender ist hoch.

2. Stufe: Fortgeschrittene Prüflogik

Die konventionelle Regelbasis wird erweitert sowie geschärft und Kontra-Indikatoren werden eingeführt. Dazu ist kein spezielles Know-how notwendig. Die Zahl der verifizierten Treffer wird erhöht und die „False Positives“ reduziert. Die Qualitätsoptimierung sorgt für Effizienzgewinne und spart Kosten.

3. Stufe: Paradigmenwechsel

Ergänzend oder ersetzend werden neue Analyse- und Prüfmethoden eingesetzt. Die Kundensegmentierung erfolgt auf Basis des Transaktionsverhaltens, die Entdeckung wird um Mechanismen der selbstständigen Musteridentifikation ergänzt. Mit Methoden der Predictive Analytics lassen sich Verdachtsmomente sammeln und prognostizieren. Riskante Transaktionen können vor ihrer Ausführung in einen zusätzlichen Prüfungs- und Autorisierungsprozess übergeleitet werden. Der Schadenseintritt wird verhindert. Dazu ist

neues methodisches Know-how notwendig, das während der ersten beiden Stufen aufgebaut werden kann.

Mit dieser Vorgehensweise lassen sich Nutzenpotenziale der In-Memory-Technologien schrittweise erschließen und Investitionen sowie Prozessänderungen „schlank“ halten. Durch die Performanz der In-Memory-Technologien können Entdeckung, Investigation, Case-Management und Reporting verschiedener Sachgebiete in einer Anwendung integriert werden.

Fazit

Die neuen digitalen Zugangskanäle sowie die Endgeräte eröffnen sowohl Kunden als auch Betrügern neue Handlungsmöglichkeiten. Zugunsten der Bedienbarkeit verzichten viele Unternehmen darauf, einzelne Geräte ihrer Kunden zu autorisieren. Mit Hilfe von Informationen wie „User Agent“ und Geotargeting lassen sich im Zusammenhang mit Kunden- und Produktraten betrügerische Merkmale erkennen. In Kombination mit einem „Security-Information-Event-Management-System“ (SIEM), das Log-Informationen auf Basis verhaltensbasierter Muster prüft, steigt die Erkennungsrate deutlich an. Durch den Aufbau eines umfangreichen Datenpools und einer flexiblen Verarbeitung lassen sich aktuelle und zukünftige Anforderungen erfüllen.

Der Autor:

Martin Stolberg, Director Banking bei Sopra Steria Consulting