

Geldwäscheprävention und Datenschutz – ein Widerspruch?

„Geldwäschebeauftragter deckt mittels Monitoringsystem Geno-SONAR Korruptionsskandal auf“ oder „Geno-SONAR lieferte Geldwäschebeauftragtem entscheidenden Hinweis zur Festnahme eines Terrorverdächtigen“. So oder so ähnlich könnten die Schlagzeilen lauten. Tun sie aber nicht. Warum eigentlich?

Dass sie dies nicht tun, liegt u.a. daran, dass Monitoringssysteme als Arbeitsmittel von Beauftragten in der öffentlichen Wahrnehmung kaum eine Rolle spielen. Zudem ist die Steuerung bzw. Parametrisierung des Systems – aus verständlichen Gründen – ein gut gehütetes Geheimnis. Schließlich sollte krimineller Energie nicht noch eine Gebrauchsanweisung für eine erfolgreiche Umsetzung gegeben werden.

Dass Monitoringssysteme bei der Bekämpfung von Geldwäsche und Terrorismusfinanzierung allerdings eine zentrale Rolle spielen, ist in der Finanzbranche und bei den Ermittlungsbehörden bereits seit langem bekannt. Anders als mit intelligenten technischen Hilfsmitteln lässt sich die Flut an zu überwachenden Transaktionen nicht beherrschen.

Doch in Zeiten von Facebook, Google und Co., in denen Datenschutzdiskussionen an der Tagesordnung sind, kommt es auch zu kritischen Fragen: Ist das eigentlich erlaubt? Darf eine Bank ihre Kunden einfach so durchleuchten und überwachen?

Ihre rechtliche Legitimation erfahren Monitoringssysteme aus dem Kreditwesengesetz. In § 25h Abs. 2 heißt es: „... Kreditinstitute haben Datenverarbeitungssysteme zu betreiben und zu aktualisieren, mittels derer sie in der Lage sind, Geschäftsbeziehungen und einzelne Transaktionen im Zahlungsverkehr zu erkennen ... die im Verhältnis zu vergleichbaren Fällen besonders komplex oder groß sind, ungewöhnlich ablaufen oder ohne offensichtlichen wirtschaftlichen oder rechtmäßigen Zweck erfolgen ... Die Kreditinstitute dürfen personenbezogene Daten verarbeiten, soweit dies zur Erfüllung dieser Pflicht erforderlich ist ...“ Das Monitoring stellt somit eine der wichtigsten Sicherungs-

maßnahmen bei der Bekämpfung von Geldwäsche, Terrorismusfinanzierung und sonstiger strafbarer Handlungen dar.

Das A und O von Geno-SONAR sind die hinterlegten Indizien. Diese sollen eine Art Netz spannen, in dem sich nur Transaktionen mit ernsthaften Auffälligkeitskriterien verfangen. Geno-SONAR verfügt systemseitig bereits über vorinstallierte Indizien, die anhand der im Sektor erarbeiteten Typologien kreiert wurden.

In der GenoTec betreuen wir mehrere Mandanten gleichzeitig. Aus unseren Erfahrungen und Erkenntnissen heraus entwickeln wir diese vorinstallierte Steuerung permanent weiter. Wir tun dies aber nicht nur, um das Netz um Geldwäscher und Betrüger immer enger zu spannen. Wir tun dies auch, um alle unbescholtenen Bürger NICHT in das weiterführende Netz von Verdachtsmeldungen und möglichen Strafverfolgungsmaßnahmen zu verstricken.

Meldung auffälliger Transaktionen

Ab wann gilt eine Transaktion als auffällig? Als Kriterien kommen neben offensichtlichen Punkten wie der Betragshöhe auch zahlreiche weitere Daten der Transaktion in Frage. So erfolgt u.a. eine unterschiedliche Gewichtung je nach Kundengruppe oder beteiligtem Land. Neben den reinen Transaktionsdaten liegt ein besonderes Augenmerk auch auf den individuellen Eigenschaften des jeweiligen Instituts. Hier gilt es, die Verschiedenheit der Produkte, aber auch der Kunden, bei der Bewertung von Auffälligkeiten angemessen zu berücksichtigen. Sie sind in ein Verhältnis zu setzen, damit unterschieden werden kann, wo lediglich Abweichungen

von einer gemeinsamen Norm auffallen und wo Auffälligkeiten weiter bearbeitet werden müssen.

Dies ist jedoch ein „laufender Prozess“. Die Monitoringssysteme bedürfen einer laufenden Überprüfung. Diese Herausforderung können gerade wir als Mehrmandantendienstleister in besonderem Umfang meistern, da wir eine Vielzahl von IT-Auswertungen eigener deutschlandweiter Quellen nutzen. Unser speziell hierfür eingerichtetes und auf Basis von statistischen Daten operierendes Fachgremium tagt regelmäßig, um einen möglichen Anpassungsbedarf zu besprechen und umzusetzen.

Bei der großen Anzahl an relevanten Faktoren und dem laufenden Anpassungsbedarf ist natürlich auch die betriebswirtschaftliche Sicht relevant. Darüber hinaus spielt das Risiko der persönlichen Haftbarkeit von Geldwäschebeauftragten, Bankmitarbeitern und Bankvorstand aufgrund vorschnell oder unsauber abgearbeiteter Auffälligkeiten eine wichtige Rolle. Eine angemessene Administration von Monitoringsystemen stellt somit hohe Anforderungen an die Institute und ihre Mitarbeiter, bringt aber auch – richtig durchgeführt – einen erheblichen Zusatznutzen.

Was passiert, wenn das Monitoringsystem anschlägt?

Je nach Schwere der Auffälligkeit werden die sogenannten Treffer in unterschiedlichen Prioritätsstufen von den Mitarbeitern bearbeitet. Erste Priorität – vor Abgabe einer möglichen Verdachtsmeldung – hat immer eine Verifizierung der Auffälligkeit unter Einbeziehung des Kundenberaters der Bank.

Aufgrund der möglichen Konsequenzen ist uns die Qualifikation der hierbei eingesetzten Mitarbeiter sehr wichtig. Nur so können wir kurzfristig auf die ständig wechselnden Kriminalitätsmuster reagieren und Geno-SONAR entsprechend feinjustieren. Gleichzeitig können wir dadurch auch den Aufwand für die Kundenberater in der Bank reduzieren.

Im Detail heißt das, dass es uns infolge unserer Analysen und Vorgehensweisen gelungen ist, in der Regel bei weniger als 5 % der systemseitigen Treffer eine Anfrage an Ihre Kundenberater zu versenden.

Warum ist das so wichtig und was hat dies mit Datenschutz zu tun?

Die Erfahrungen zeigen, dass die Behörden verstärkt Druck auf Institute ausüben, häufigere und zeitnahe Verdachtsmeldungen zu generieren, und dies durch Androhung oder

Durchführung von Ordnungswidrigkeitsverfahren (inklusive Bußgelder) auch untermauern. Die Angst vor Konsequenzen und Ordnungswidrigkeitsverfahren steigt, zumal diese nun – auch im Falle eines Vergleiches – an einem sogenannten „Schwarzen Brett“ veröffentlicht werden. Das ist keine gute Werbung und schadet der Reputation.

Die Behörden wollen damit die Bedeutung der Betrugs- und Geldwäscheprävention unterstreichen. Aber: Mindestens genauso wichtig ist es, unbescholtene Kunden zu schützen.

Dieser Aspekt erfährt durch die Datenschutz-Grundverordnung noch eine weitere Facette. Grundsätzlich ist die Weitergabe von Kundendaten im Rahmen eines Verdachtsmeldeverfahrens auch ohne Zustimmung der Kunden durch den Gesetzesrahmen geschützt. Aber auch hier sollte bei allen Bemühungen, die Vorgaben des Gesetzes im Rahmen der eigenen Aufgaben als Bank, Vorstand, Mitarbeiter oder Geldwäschebeauftragter umzusetzen, der Grundsatz gelten, nicht mehr Daten als zwingend erforderlich in einen Kreislauf zu geben, der nicht (mehr) den eigenen Überwachungssphären der Datenkontrolle unterliegt.

Der Kunde steht immer noch im Mittelpunkt

Ein intelligentes Treffertuning zahlt dagegen auf die gezielte Identifizierung qualifizierter Treffer ein. Die beschriebene Vorgehensweise trägt aktiv und fortlaufend dazu bei, die „echten Auffälligkeiten“ als meldenswert zu identifizieren und damit

- ▶ zum Schutz der Daten Ihrer Kunden beizutragen,
- ▶ den Arbeitsaufwand in Ihrem Haus nach Möglichkeit und trotz steigender regulatorischer Komplexitäten zu reduzieren oder zumindest konstant zu halten,
- ▶ die Reputation Ihres Hauses bei verschärftem strafrechtlichem Vorgehen zu schützen. ■

AUTOREN UND ANSPRECHPARTNER

Andreas Brenner
Beauftragter Zentrale Stelle,
E-Mail: andreas.brenner@
geno-tec.de

Dominik Tiburtius
Leiter Überwachung & Kontrolle,
E-Mail: dominik.tiburtius@
geno-tec.de