FINANZDIENSTLEISTUNGEN | E-Book

Banken setzen auf Intelligenz:

Wie KI und ML Banken dabei helfen, Cyber-kriminellen und Compliance-Bestimmungen einen Schritt voraus zu sein

ABBYY

Inhaltsverzeichnis

Wo das Geld ist

Als der berühmte amerikanische Bankräuber Willie Sutton gefragt wurde, warum er Banken ausgeraubt hat, antwortete er: „Weil dort das Geld ist."

Noch heute sind Banken der Ort, wo „das Geld ist". Aber die kriminellen Techniken haben sich verändert und sind weit entfernt von den bewaffneten Raubüberfällen, für die Sutton bekannt war. Die Finanzkriminalität ist nun digital. Cyberkriminelle erfinden schneller neue Methoden für Betrug und Geldwäsche, als Banken Gegenmaßnahmen ergreifen können.

Im Bankwesen sind die jährlichen Kosten für Cyberangriffe unter allen Branchen am höchsten – mehr als 18,3 Millionen US-Dollar pro Jahr und Unternehmen.

IM APRIL 2020 STARTETE EINE GRUPPE CYBERKRIMINELLER, DIE ALS „FLORENTINE BANKER GROUP" BEKANNT IST, ANGRIFFE GEGEN FÜHRENDE FINANZUNTERNEHMEN IN ISRAEL UND GROSSBRITANNIEN UND STAHL MIT NUR

VIER GETRENNTEN TRANSAKTIONEN

1,3 MILLIONEN US-DOLLAR.

Quelle

Die Know Your Customer- (Legitimationsprüfung von Neukunden, KYC) und Anti Money Laundering-Vorschriften (Bekämpfung von Geldwäsche, AML) gehen auf das US-amerikanische Bankgeheimnisgesetz von 1970 zurück (Bank Secrecy Act). Nach den Terroranschlägen vom 11. September 2001 wurden diese Vorschriften nochmals verstärkt. Im Verlauf der nachfolgenden Untersuchung stellte der US-Kongress schnell fest, dass die Operation durch Cyberkriminalität und Geldwäsche finanziert worden war.

Zum ersten Mal wurde Cyberkriminalität offiziell als Terrorismus kodifiziert. Bei der Formulierung von Maßnahmen zur Terrorismusbekämpfung, einschließlich der Bekämpfung der Terrorismusfinanzierung (CFT), wurde ein besonderes Augenmerk auf Cyberkriminalität gelegt.

Die Einhaltung dieser Vorschriften kann Betrug und Diebstahl wirksam verhindern. Die Banken müssen jedoch wachsam bleiben und zusätzliche Schritte unternehmen, um mit den sich schnell entwickelnden Methoden der Cyberkriminalität Schritt zu halten. Bei Verstößen gegen die KYC- und AML-Vorschriften drohen hohe Geldstrafen sowie Markt- und Reputationsrisiken. Umso wichtiger sind angemessene Schutzmaßnahmen. Im Dezember 2019 beliefen sich die weltweiten Strafen für Verstöße gegen KYC/AML-Vorschriften auf 36 Milliarden US-Dollar.

Um raffinierte Verbrechen zu verhindern, braucht es raffinierte Maßnahmen.

Glücklicherweise erhalten Banken dank der heutigen, auf künstlicher Intelligenz basierenden Technologien die benötigte Transparenz über ihre Prozesse und Inhalte, um die KYC/AML/CFT-Vorschriften einzuhalten und sich flexibel an sich ändernde Bedingungen anzupassen.

Die Weiterentwicklung der Finanzkriminalität

Aufgrund des verschärften Wettbewerbs und der sich wandelnden Kundenerwartungen verlassen sich Finanzinstitute zunehmend auf Automatisierung, mobile Technologie und kontaktlose Interaktionen, insbesondere seit Ausbruch der COVID-19-Pandemie. Diese Maßnahmen bieten zwar erhebliche Vorteile in Bezug auf Produktivität und Kundenzufriedenheit, können jedoch auch neue Schwachstellen schaffen, die Cyberkriminelle ausnutzen können – was sie auch tun.

COVID-19 wirkt sich auch auf die Fähigkeit aus, Verpflichtungen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (AML/CFT) umzusetzen – von der Überwachung, Regulierung und Richtlinienüberarbeitung bis hin zur Meldung verdächtiger Transaktionen und zur internationalen Zusammenarbeit.

Die Zunahme von Remote-Transaktionen bietet Kriminellen einen fruchtbaren Boden: Sie richten sich an Bevölkerungsgruppen, die mit Online-Plattformen möglicherweise weniger vertraut sind, und nutzen Anreizmaßnahmen aus.

Fundraising für falsche Wohltätigkeitsorganisationen, Investitionsbetrug, vermehrtes Phishing und Ransomware-Angriffe erhöhen die physischen Bargeldtransaktionen. Wenn sich der Markt stabilisiert, könnten große Geldbewegungen zur Rückzahlung von Finanzmitteln dazu führen, dass illegale Gelder verdeckt gewaschen werden. Durch COVID-19 kam es zudem zu einer Unterbrechung bei der Umsetzung neuer AML/CFT-Richtlinien und -Gesetzgebungsinitiativen.

Die heutigen Finanzverbrecher haben herausgefunden, wie sie die eigenen Systeme und Prozesse eines Instituts als Mechanismen zum Waschen und Stehlen von Geld nutzen können. Zum Beispiel:

1. **Virtualisierung:** System- und Anwendungsschwachstellen können ausgenutzt werden, um unbefugten Zugriff auf Kontodaten zu ermöglichen.
2. **Prozessautomatisierung** Kriminelle können Lücken in automatisierten Prozessen aufdecken, die bei automatisierten Überprüfungen möglicherweise übersehen werden.
3. **Kundenidentifikation:** Die Kundenidentifikation kann gestohlen werden, um Identitätsdiebstahl zu begehen.
4. **Kunden-Onboarding:** Cyberkriminelle können mithilfe gefälschter Kundenidentitäten synthetische Konten erstellen.

DIE JÄHRLICH WELTWEIT GEWASCHENE GELDMENGE WIRD AUF

800 MILLIARDEN BIS 2 BILLIONEN US-DOLLAR GESCHÄTZT,

UNGEFÄHR

2 BIS 5% DES GLOBALEN BIP.

Quelle

UNTER EINBEZIEHUNG DER DURCH BETRUG ENTSTEHENDEN FOLGEKOSTEN VERLIEREN FINANZINSTITUTE **FÜR JEDEN** DOLLAR, DER DURCH BETRUG VERLOREN GEHT, 3 WEITERE DOLLAR.

Quelle

Was können Finanzinstitute gegen diese ständigen Angriffe unternehmen? Manuelle Überwachung kann hilfreich sein, ist jedoch von Natur aus durch folgende Faktoren begrenzt:

- Die Unfähigkeit menschlicher Mitarbeiter, rund um die Uhr mit dem Umfang und der Geschwindigkeit der Transaktionen Schritt zu halten, kombiniert mit unzureichenden Kontrollen über die Transaktionsüberwachung und -berichterstattung
- Das erhöhte Risiko menschlicher Fehler
- Die Schwierigkeit, menschliche Mitarbeiter ständig über die neuesten kriminellen Techniken zu informieren
- Das Risiko, dass menschliche Mitarbeiter selbst Finanzverbrechen begehen

Aus Sicht der Compliance: Erfüllung der KYC- und AML/CFT-Anforderungen

Um sich an die KYC- und AML-Vorschriften anzupassen, müssen Finanzinstitute nachweisen, dass sie über Verfahren verfügen, um kriminelle Aktivitäten aufzudecken und Maßnahmen zu ergreifen, einschließlich der Überprüfung der Identität von Kunden und der Echtheit von Transaktionen.

Viele Banken verfügen über Verifizierungsprozesse und Aufzeichnungssysteme für ihre strukturierten Daten. Die große Menge an Kundendaten, die aus Dokumenten stammen, stellt jedoch eine Schwachstelle dar. Ihnen fehlt die Verknüpfung zwischen ihren Datenarchitekturen und den Dokumenten, aus denen ein großer Teil des Kunden- und Transaktionsverhaltens – und Erkenntnisse über dieses Verhalten – stammen.

Ein Fall, in dem diese dokumentbasierten Daten zu Compliance-Problemen führen können, ist die Regelung zur Verfolgbarkeit der Aufbewahrungskette. Der Begriff Aufbewahrungskette (Chain of Custody) bezieht sich auf die Verfolgung des Lebenszyklus von Daten – vom Zeitpunkt ihres Eintritts in das Unternehmen bis zum Tag ihrer Vernichtung oder Lagerung. Ein konformes Chain-of-Custody-Protokoll kann Fragen beantworten, z.B. woher die Daten in der Organisation stammen, wohin sie weitergeleitet wurden, wer mit ihnen befasst war und welche Änderungen gegebenenfalls daran vorgenommen wurden.

Dokumente sind wesentliche Geschäftsunterlagen und müssen während der gesamten Aufbewahrungskette ihre Integrität bewahren. Wenn Änderungen vorgenommen werden, müssen diese notiert werden. Bei Dokumenten kann die Verfolgung der Aufbewahrungskette aus drei Gründen problematisch sein, die alle gleich wichtig sind:

- Unvollständiges Verständnis der Dokumente selbst
- Unvollständiges Verständnis der Prozesse, die die Dokumente durchlaufen
- Unzureichende Transparenz darüber, wer mit den Dokumenten interagiert hat

Beispiel: Kunden-Onboarding

Wenn ein Kunde im Rahmen des Onboarding-Prozesses einen Führerschein einreicht, sollte in einem Chain-of-Custody-Protokoll angegeben werden, wann und wie das Dokument gescannt wurde, wie die Daten extrahiert und überprüft wurden, was mit dem gescannten Bild nach dem Onboarding passiert ist und wie die extrahierten Daten bis zum Dokument zurückverfolgt werden können.

Lücken in dieser Kette können nicht nur zu KYC-Verstößen führen, sondern auch zu Sicherheitslücken, die von Cyberkriminellen ausgenutzt werden können. Das Kunden-Onboarding, bei dem die Bank erstmals die Identität des Kunden anhand von Dokumenten feststellt, ist der entscheidende erste Schritt, um die Einhaltung der KYC-Richtlinien zu gewährleisten.

ALLEIN 2017 GABEN BANKEN UNGEFÄHR

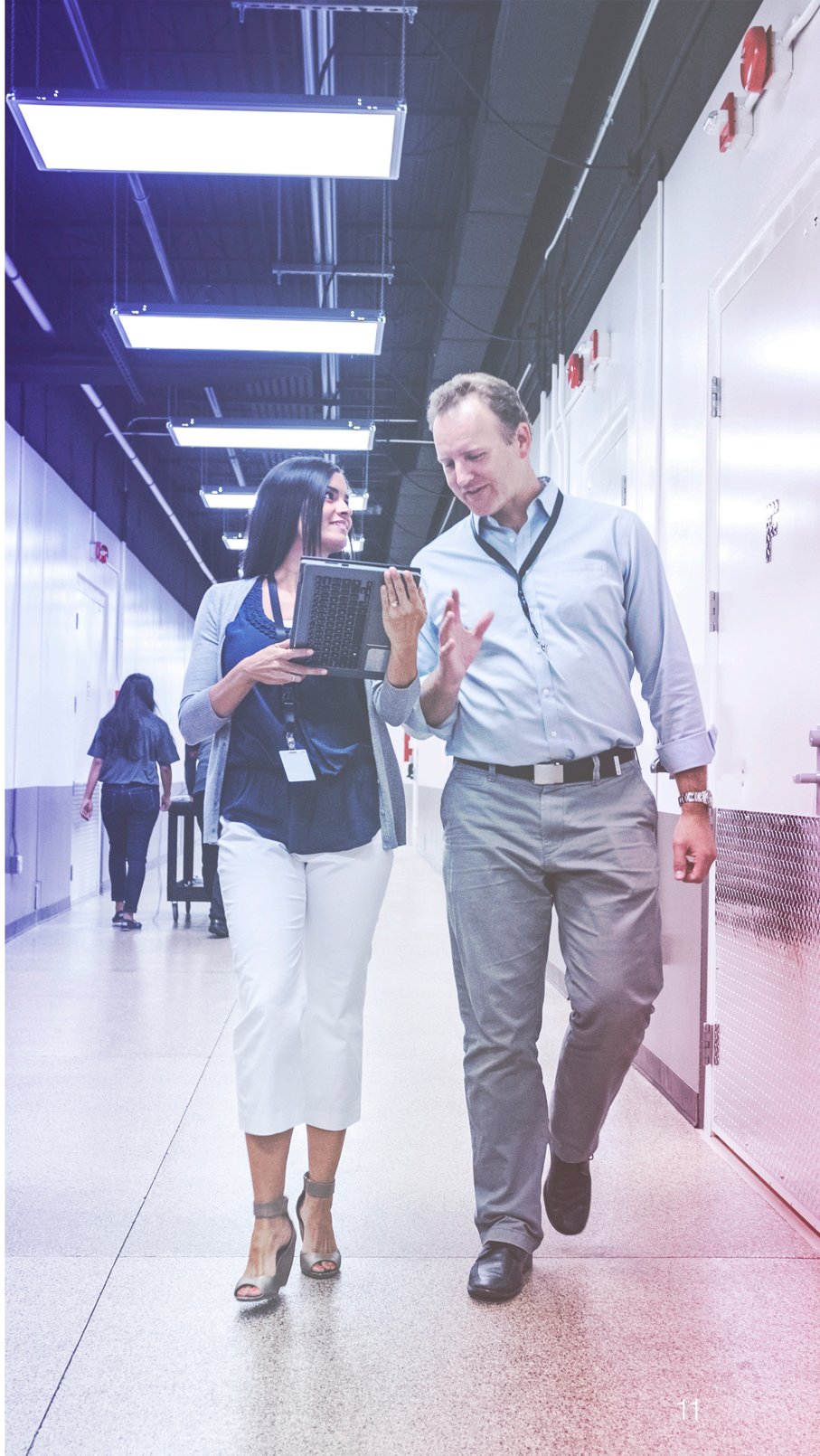
8,2 MILLIARDEN US-DOLLAR

FÜR DIE BEKÄMPFUNG VON GELDWÄSCHE (AML) AUS.

Quelle

Mit Digital Intelligence einen Schritt voraus sein

Um die doppelte Herausforderung der Einhaltung der KYC/AML/CFT-Vorschriften und der Verhinderung krimineller Aktivitäten zu bewältigen, die von den Compliance-Anforderungen möglicherweise nicht abgedeckt werden, benötigen Finanzinstitute einen Schlachtplan, der sich an mehrere Fronten richtet: Personen, Prozesse und Dokumente. Erstens müssen sie über die Möglichkeit verfügen, Dokumente zu überprüfen, um versuchten Betrug aufzudecken. Zweitens benötigen sie Transparenz über ihre Prozesse. Diese muss eine kontinuierliche Überwachung auf Unregelmäßigkeiten ermöglichen, die auf betrügerisches Verhalten hinweisen könnten. Drittens benötigen sie Einblicke in die Weise, wie Menschen mit den Prozessen und Dokumenten interagieren, die auf verdächtiges Verhalten hinweisen könnte. Dieser Ansatz wird Banken mit der benötigten Digital Intelligence ausstatten, um sich sowohl vor Betrug als auch vor Verstößen gegen Vorschriften zu schützen.



Digital Intelligence ist ein neuer Ansatz zur Verwendung der neuesten Technologien für künstliche Intelligenz (KI) und maschinelles Lernen (ML), um Schlüsselfunktionen bereitzustellen, die Banken Vertrauen in die Aufbewahrungskette von Dokumenten geben:

- Validierung von Kunden-Onboarding-Dokumenten (strukturiert und unstrukturiert) und von deren Inhalt zum Zeitpunkt der Eingabe
- Intelligente Extraktion von Inhalten aus Dokumenten, die validiert und/oder als verdächtig gekennzeichnet werden können
- Prozesserkennung, die Muster verdächtigen Verhaltens zwischen Personen und Dokumenten sowie Lücken in Prozessen aufdeckt, die zu angreifbaren Schwachstellen führen können

In Bezug auf die Betrugsprävention bietet Digital Intelligence Finanzinstituten die Tools, die sie benötigen, um Compliance-Anforderungen zu erfüllen und Kriminellen einen Schritt voraus zu sein. Gleichzeitig werden die Fallstricke manueller Ansätze vermieden, die mit der Herausforderung nicht Schritt halten oder nicht entsprechend skaliert werden können.

Dokumentenintegrität

Obwohl die Finanzbranche die digitale Transformation immer mehr umsetzt, stammen viele Kundendaten von Banken aus Dokumenten: Identifikationsformulare, Unternehmensnachweise, Kreditanträge, Steuererklärungen usw. Wenn Finanzinstitute Betrug verhindern und ihren Compliance-Verpflichtungen nachkommen möchten, müssen sie jedes Kundendokument zuverlässig auf Unregelmäßigkeiten prüfen können, die auf kriminelle Absichten hinweisen könnten. Sie müssen auch eine direkte Verknüpfung zwischen ihren Aufzeichnungssystemen für die KYC/AML-Einhaltung und ihren Kundeninteraktionen herstellen, vom Onboarding über ganze Customer Journeys.

Die Dokumentenintegrität spielt eine wichtige Rolle bei der Überwachung und Dokumentation der Aufbewahrungskette, die für die KYC/AML-Einhaltung von entscheidender Bedeutung ist (siehe „Aus Sicht der Compliance“).

Durch die Validierung von Dokumenten und deren Inhalten während des Onboarding-Prozesses können Banken Kundendaten vom Zeitpunkt ihres Eintritts in das Unternehmen (Kunden-Onboarding) über ihren gesamten Lebenszyklus bis hin zum Offboarding verfolgen. Sollte ein Compliance-Beauftragter eine Dokumentation der Aufbewahrungskette anfordern, kann das Finanzinstitut auf jeden Kontaktpunkt eingehen.

Prozessintegrität

Sobald Kundendaten in ein Finanzinstitut eingehen, sei es über Dokumente oder aus digitalen Quellen, werden sie zur Basis für eine beliebige Anzahl von Prozessen, einschließlich Kunden-Onboarding, Compliance-Prüfungen, Kreditgenehmigungen und vielem mehr. Die meisten Banken haben eine gute Vorstellung davon, wie diese Prozesse ablaufen sollen. Doch die Lücken zwischen Theorie und Praxis können größer sein als sie denken – und Möglichkeiten für Betrug oder Datendiebstahl bieten.

Bei der Prozesserkennung werden Daten aus digitalen und physischen Quellen verwendet, um Banken einen Einblick in die tatsächliche Ausführung ihrer Prozesse von Anfang bis Ende zu geben. Durch das Sammeln und Analysieren der von Informationssystemen generierten Zeitstempeldaten verwendet Process Intelligence erweiterte Algorithmen, um einen „digitalen Zwilling“ von Geschäftsabläufen und -prozessen zu erstellen. Diese visuellen Modelle bieten detaillierte Einblicke in die tägliche Ausführung von Prozessen – vom „Standard“- oder „Ideal“-Pfad bis hin zu allen anderen Variationen.

Um Betrug und Geldwäsche zu verhindern, kann die Prozessüberwachung Unregelmäßigkeiten in der Handhabung von Daten aufdecken, die von Cyberkriminellen ausgenutzt werden könnten. Sie kann Prozesse rund um die Uhr auf potenzielle Sicherheitslücken überwachen und Prozessverantwortliche automatisch warnen, wenn sofortige Interventionen erforderlich sind.

Wie oben erläutert, ist die Verfolgung der Aufbewahrungskette mit ihren Dokumenten und Daten ein wesentlicher Bestandteil der KYC/AML-Einhaltung. Durch die automatische Zuordnung der Prozessausführung können Banken den Lebenszyklus von Kunden- und Transaktionsdaten auf ihrem Weg durch Prozesse und zwischen diesen mit ihren wesentlichen Dokumenten verfolgen und bei Bedarf eine genaue Dokumentation der Aufbewahrungskette bereitstellen.

Kontinuierliches Lernen

Compliance und Betrugsprävention sind in ständigem Wandel, da laufend neue Vorschriften entstehen und Kriminelle neue Betrugsmaschen finden.

Digital Intelligence-Lösungen sind sehr anpassungsfähig, wenn sich die Bedingungen sowie Compliance-Vorschriften und -Richtlinien ändern. Mithilfe der ML-Technologie können diese Lösungen aus jeder Iteration lernen und sich entsprechend anpassen.

Ausblick

Banken und andere Finanzinstitute setzen die digitale Transformation immer mehr um. Die Nebenwirkungen dieses Fortschritts können jedoch manchmal zu ungünstigen Ergebnissen führen. Die heutigen Cyberkriminellen haben herausgefunden, wie sie die eigene digitale Infrastruktur eines Unternehmens nutzen können, um Betrug und Datendiebstahl zu begehen. Um ihnen einen Schritt voraus zu sein, müssen alle verfügbaren Tools eingesetzt werden.

KI-gesteuerte Lösungen können Hunderte von Prozessen und Tausende von Dokumenten schnell und genau automatisch überprüfen und überwachen, um Anzeichen möglicher krimineller Aktivitäten zu erkennen. KI wird Compliance- und Betrugspräventionsexperten nicht ersetzen. Im Gegenteil: Durch KI werden Mitarbeiter von routinemäßigen Überwachungsaufgaben befreit, sodass sie sich auf komplexere Probleme konzentrieren können. Die Kombination aus menschlichem Fachwissen und einer digitalen Belegschaft, die Finanzinstituten hilft, schnell zu skalieren und sich anzupassen, schafft einen einzigartigen Vorteil im Kampf gegen Finanzkriminalität. Banken können die KYC/AML-Vorschriften einhalten und gleichzeitig ihre eigene Abwehr gegen Cyberkriminalität stärken – heute, morgen und in den nächsten Jahren.

ABBYY

Weitere Informationen finden Sie unter
www.abbyy.com/de/solutions/financial-services

Kontaktieren Sie unsere Niederlassungen auf der ganzen Welt: www.abbyy.com/de/contacts

© ABBYY 2021 ABBYY ist ein eingetragenes Warenzeichen von ABBYY Software Ltd. Alle anderen hierin erwähnten Produktnamen und Markenzeichen sind Eigentum ihrer jeweiligen Inhaber. #12505