kyriba

E-BOOK

Ein Leitfaden zur Erkennung von Zahlungsbetrug

Bereitstellung KI-basierter Tools zum Schutz Ihrer Transaktionen

Einführung

Moderne Betrugsversuche sind innovativ und entwickeln sich ständig weiter. Um diese Bedrohungen in den Griff zu bekommen, benötigen Unternehmen topaktuelle Erkennungs- und Präventionslösungen.

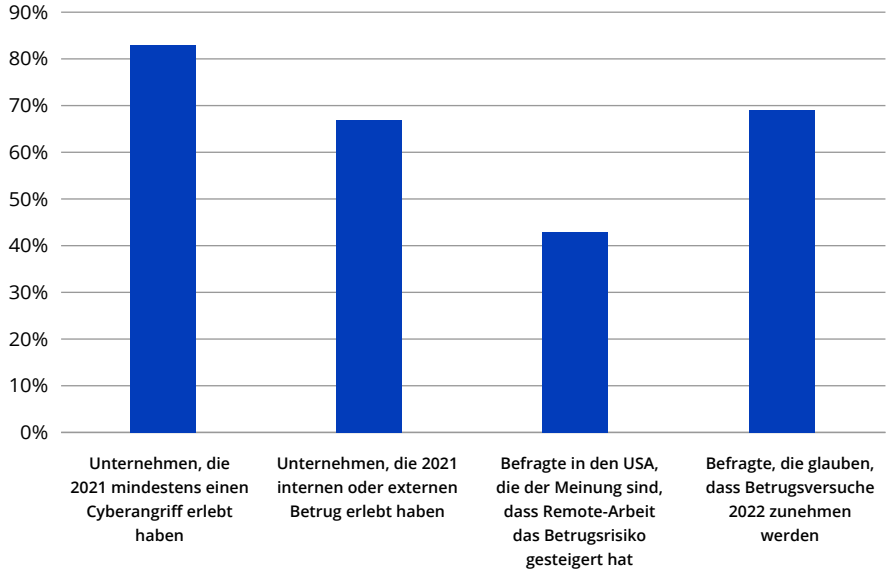
In diesem E-Book stellen wir Ihnen die häufigsten Betrugsrisiken in der aktuellen Unternehmenswelt vor und untersuchen die führenden KI-basierten Tools, mit denen CFOs und CIOs Angriffe aufhalten können, noch bevor sie passieren. Wir bei Kyriba kennen die Gefahren, die Cyberkriminelle für das Geld Ihres Unternehmens darstellen. Im Folgenden sehen wir uns an, auf welche Weise wir unsere Kunden schützen, und teilen unser Wissen mit Ihnen. Tools wie künstliche Intelligenz (KI), Machine Learning (ML) und Application Programming Interfaces (APIs) sind echte Gamechanger im Kampf gegen Betrug. Wir nutzen diese Technologien bereits – und das sollten Sie auch.

kyriba

Betrug im Wandel

Betrugsrisiken haben mit der Coronapandemie exponentiell zugenommen, im Homeoffice konnten die strengen Sicherheitsprotokolle vom Unternehmen nur sehr schwer umgesetzt werden. Laut einer KPMG-Studie 2022, bei der über 600 Führungskräfte befragt wurden, **hat die Umstellung auf Remote-Arbeit das Betrugsrisiko gesteigert** und die meisten Unternehmen haben im letzten Jahr Betrugsfälle erlebt.

BETRUGSAUSBLICK



Quelle: KPMG Fraud Outlook 2022

kyriba

Die Verluste, die sich aus Betrugsfällen ergeben, sind signifikant. Die Befragten verzeichneten 2021 einen durchschnittlichen Gewinnverlust von einem Prozent aufgrund von Betrug und fehlender Compliance. Und je größer das Unternehmen ist, desto mehr Kriminelle werden es angreifen.

BETRUGSVERLUSTE

Prozentsatz der Unternehmen, die aufgrund von Betrug Gewinnverluste zwischen 0,5 und 1 % erlitten haben

Prozentsatz großer Unternehmen, die 2021 Verluste durch Betrug erlitten haben

Prozentsatz der Unternehmen, die über ein Programm zur Betrugsprävention verfügen

Quelle: KPMG Fraud Outlook 2022

Es braucht Investitionen und Aufmerksamkeit

Die Pandemie wird in absehbarer Zeit nicht enden, sondern es Unternehmen weiterhin erschweren, mittels eines effektiven Betriebs- und der richtigen Personalplanung der immer größeren Betrugsgefahr zu begegnen. Daher überrascht es, dass mehr als die Hälfte der Befragten nicht vorhaben, ihre Budgets für Investitionen in Betrugsbekämpfungsmaßnahmen anzupassen. Da jedoch derzeit weniger als die Hälfte der Unternehmen über Programme zur Prävention, Erkennung und Abwehr von Betrugsversuchen verfügt, ist es offensichtlich, dass größere Investitionen in den Betrugsschutz absolut erforderlich sind. CFOs, Treasurer und CIOs benötigen ganz klar ein umfassenderes Abwehrsystem in Form einer neuen, führenden, automatisierten KI-basierten Art der Betrugserkennung.

kyriba

Allgegenwärtige und immer neue Betrugsrisiken

Betrug per Business Email Compromise (BEC) stellt auch weiterhin ein riesiges Problem für Treasury- und Finanzabteilungen dar. BEC-Angriffe beginnen in der Regel damit, dass ein Mitarbeiter eine dringende E-Mail erhält, die scheinbar von einem Mitglied der oberen Führungsebene stammt und in der eine Geldüberweisung angefordert wird. In Wahrheit imitiert der Angreifer jedoch eine legitime E-Mail-Adresse. Hierzu verschaffen sich Kriminelle in der Regel per Phishing Zugang zum E-Mail-System des Unternehmens. Eine Abwandlung dieser Betrugsart umfasst E-Mail-Rechnungen, die scheinbar von einem häufig genutzten Lieferanten stammen und in denen die Zahlungsanweisungen aktualisiert werden. Laut der Cyber Division des FBI haben die Verluste durch BEC-Angriffe zwischen 2019 und 2020 um 5 % zugenommen – mit über 1,7 Milliarden US-Dollar Verlust in 2019 und über 1,8 Milliarden US-Dollar Verlust in 2020.

Scheck- und Überweisungsbetrug bereitet Treasury- und Finanzabteilungen auch weiterhin Kopfzerbrechen, da diese Zahlungsmethoden am anfälligsten für Betrugsversuche sind. AFP fand in einer Studie heraus, dass 66 % bzw. 39 % der Finanzexperten 2020 Betrugsaktivitäten unter Verwendung dieser beiden Zahlungsarten gemeldet hatten. Scheckbetrug nimmt jedoch seit einigen Jahren konstant ab, da immer weniger Unternehmen Schecks für B2B-Zahlungen einsetzen.

HÄUFIGE SCHWACHSTELLEN IN UNTERNEHMEN

Technik

- Fehlende Verschlüsselung von Plattformen
- Fragmentierte Systeme und Verbindungspunkte (mehrere ERPs mit unterschiedlichen Workflows darin)

Prozesse

- Fehlende Standardisierung
- Keine systematischen Workflows zur Verwaltung sämtlicher Aspekte von Zahlungsaktivitäten
- Mangelnde Transparenz des Audit Trails

Mitarbeiter

- Nicht eingehaltene Compliance
- Unzureichende Schulung
- Falsche Beurteilung von Situationen
- Interne Absprachen

Deepfake-Stimmbetrug ist eine verhältnismäßig neue Angriffsmethode, die sich jedoch als äußerst effektiv erwiesen hat. Bei dieser Betrugsmasche setzen Kriminelle in Telefonaten Deepfake-Stimmtechnologie ein. Diese Software kann die Stimme einer Person allein anhand eines kleinen Audioclips imitieren. Deepfake-Angriffe haben im letzten Jahr internationale Aufmerksamkeit erregt, als bekannt wurde, dass Betrüger mit dieser Methode 35 Millionen US-Dollar von einer Bank gestohlen hatten.

Ransomware-Angriffe sind zwar technisch gesehen kein Betrug, doch sie stellen dennoch eine allgegenwärtige Gefahr für die Systeme und Bankkonten von Unternehmen dar. Bei einer Ransomware-Attacke wird das interne System eines Unternehmens infiziert (in der Regel über Phishing) und vom Angreifer übernommen. Benutzer werden aufgefordert, ein Lösegeld zu zahlen, wenn sie nicht dauerhaft aus ihren Systemen ausgeschlossen werden wollen. Ransomware as a Service (RaaS) ist die neueste Entwicklung in diesem Bereich. Hierbei verkaufen oder vermieten Entwickler ihre Ransomware-Exploits an Kunden, die sie dann ganz einfach auf ihre unglücklichen Opfer loslassen können.

Tools zum Schutz vor Betrug

Um moderne Bedrohungen wirksam zu bekämpfen, sollten Betrugspräventionslösungen folgende Funktionen bieten:

- Automatisierte Zahlungsprozesse zur Standardisierung von Kontrollen
- Echtzeitscreening sämtlicher Zahlungsdaten zur Erkennung verdächtiger Transaktionen
- Benutzerdefinierte Zahlungsscreening-Regeln
- Lösungsworkflow zur Untersuchung verdächtiger Zahlungen
- Option, um zu verhindern, dass Benutzer, die gegen eine Zahlungsregel verstoßen haben, gewarnt werden
- Überwachung des Status und der Priorität von Alarmen in einem KPI-Dashboard

Moderne Lösungen zur Erkennung von Zahlungsbetrug, wie z. B. das Payment Fraud Detection-Modul von Kyriba, bieten diese Funktionen und mehr.

kyriba

Screening, Alarme und Benachrichtigungen in Echtzeit

Mit der Zunahme von Same-Day- und Echtzeit-Zahlungssystemen sind auch Echtzeitreaktionen auf Betrugsversuche immer wichtiger geworden. Moderne Software für Betrugserkennung nutzt künstliche Intelligenz (KI) und Machine Learning (ML), um Zahlungen anhand von Verlaufsdaten zu screenen und Anomalien zu erkennen. Durch die Bereitstellung vollständiger Daten ermöglichen solche Lösungen eine datenbasierte Entscheidungsfindung.

So bestimmt beispielsweise die Lösung „Payment Fraud Detection“ von Kyriba die Refelmäßigkeit jeder Zahlung – egal, ob automatisiert oder manuell – und kennzeichnet solche mit geringer Refelmäßigkeit. Die Lösung stellt Einblicke in die Variablen bereit, mit denen die ZahlungsrRefelmäßigkeit festgelegt wird. So können Benutzer einsehen, warum etwas als Anomalie eingestuft wurde. Und der vielleicht größte Vorteil für Benutzer besteht darin, dass Prozesse in keiner Weise verlangsamt werden – trotz der gesteigerten Transparenz der Zahlungsdaten.

Zahlungen können aus verschiedenen Gründen als Anomalie gekennzeichnet werden:

- hohe Anzahl von Zahlungen desselben Dritten
- Zahlungen mit ungewöhnlich hohen Beträgen
- Zahlungen an Länder, die laut Unternehmensrichtlinie unzulässig sind
- verdächtige Änderungen an Zahlungen, die aus einem ERP importiert werden
- Zahlungen an ein Bankkonto, das von mehreren third parties verwendet wird
- doppelte Zahlungen

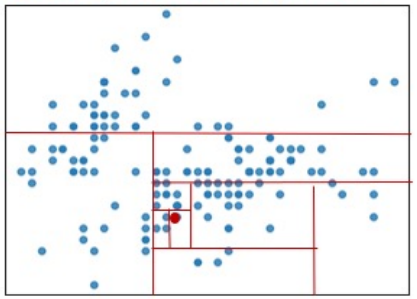
Nachdem die Datenwissenschaftler von Kyriba mehrere Machine-Learning-Modelle getestet hatten, wählten sie zwei Lösungen aus, um Unregelmäßigkeiten in Zahlungen zu erkennen.

Isolation Forest

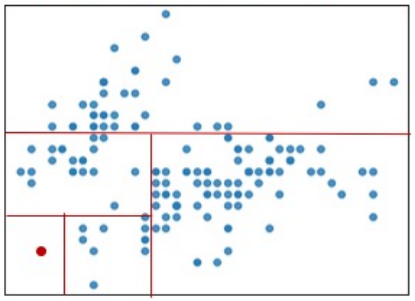
Ein Isolation-Forest-Modell ist ein unüberwachter Algorithmus, der nach dem Prinzip der Isolation von Anomalien arbeitet – anomale Instanzen in einem Datensatz sind tendenziell leichter vom Rest der Stichprobe zu trennen.

Im folgenden Beispiel sehen wir, dass die Isolation von Anomalien im Vergleich zu den Normalpunkten weniger zufällige Partitionen erfordert:

Normalpunkt: 8 zufällige Partitionen



Anomalie: 4 zufällige Partitionen



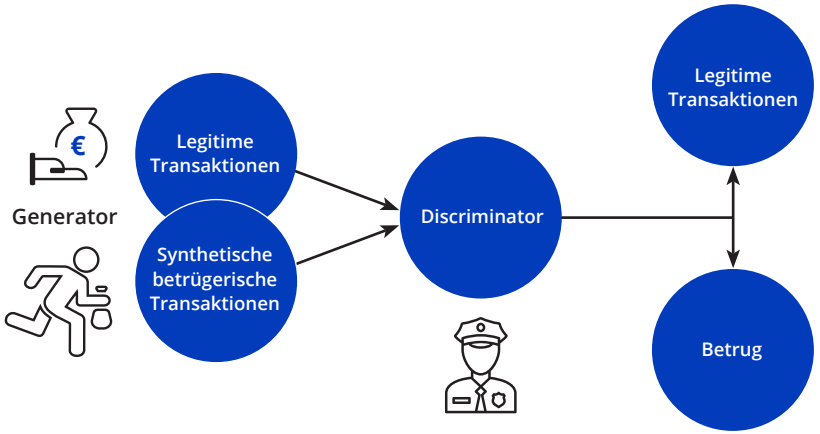
Generative Adversarial Network

Ein Problem, auf das viele Machine-Learning-Modelle bei der Betrugserkennung stoßen, sind die fehlenden Daten in diesem Bereich. Die meisten Unternehmen haben bisher keinen signifikanten Zahlungsbetrug erlebt, weshalb es ihnen an umfangreichen Stichproben fehlt. Andere waren vielleicht Opfer von Zahlungsbetrug, aber können oder wollen keine Details nennen. Das Trainieren von KI-Modellen gestaltet sich also schwierig, da Algorithmen nur aus guten Zahlungen und – im besten Fall – aus einer Handvoll schlechter lernen können.

Generative Adversarial Networks (GANs) können dieses Problem lösen. Ein GAN ist ein Deep-Learning-Modell, das zwei separate neuronale Netze gegeneinander antreten lässt. Ein Netzwerk (der Generator) vermischt echte Daten mit synthetischen und versucht so das gegnerische Netzwerk (den Discriminator) auszutricksen.

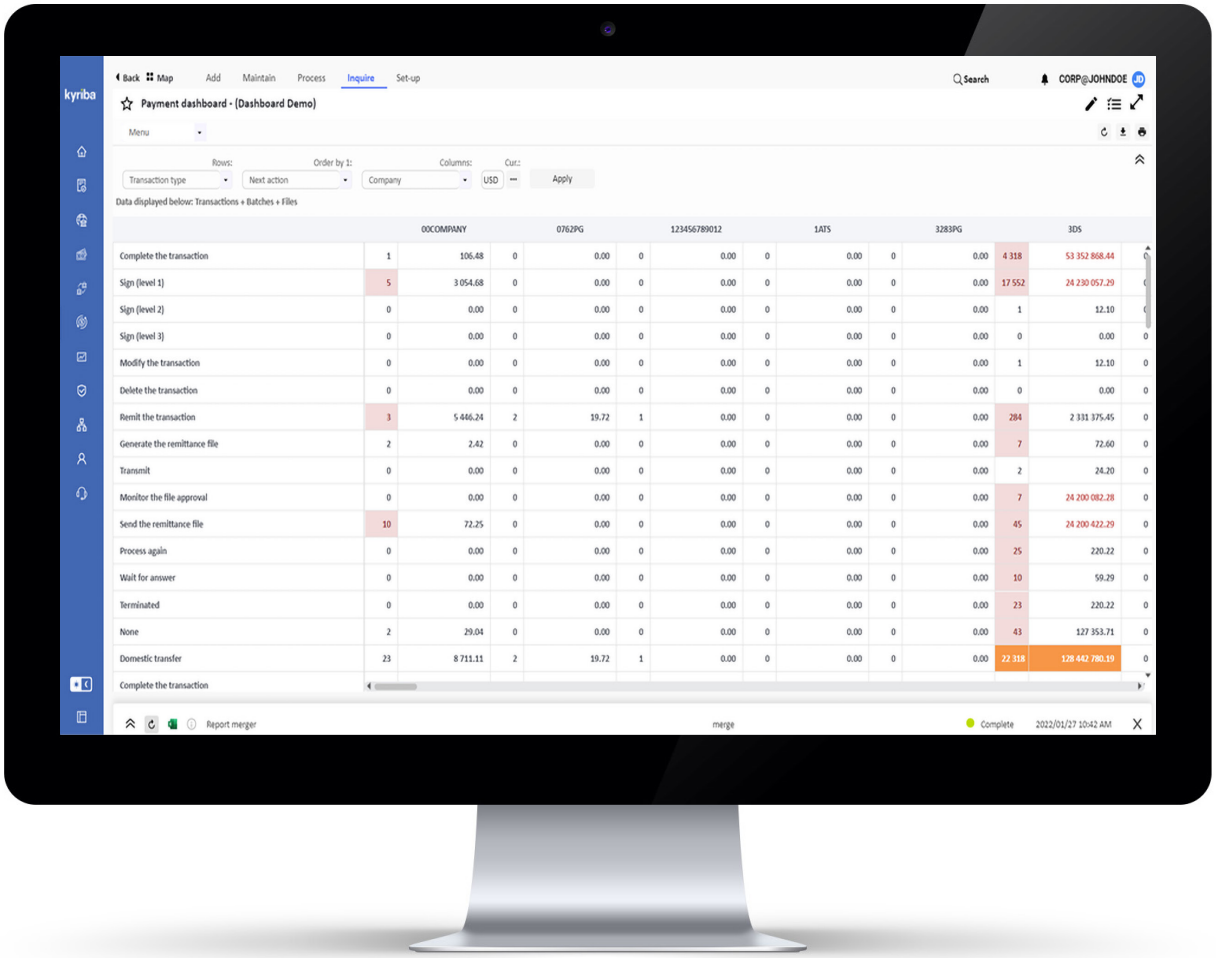
Kyriba erstellt ein „Betrüger"-Netzwerk (den Generator), das synthetische betrügerische Transaktionen in Zahlungen versteckt, die gemäß Kundenverlauf legitim sind. Dann geht ein „Polizei"-Netzwerk (der Discriminator) die Daten durch und trennt die unzulässigen Transaktionen von den richtigen. Indem das Betrugserkennungsmodell mithilfe dieser konkurrierenden Netzwerke trainiert wird, kann Kyriba betrügerische Transaktionen in Echtzeitdaten besser erkennen.

GAN-Modell (Generative Adversarial Network)



Dashboards

Dashboards können so eingerichtet werden, dass sämtliche verdächtigen Zahlungen angezeigt und in der Lösung priorisiert werden – anhand von Faktoren wie Erkennungsregeln, Risiko, Anzahl von Vorfällen und einer Scorecard zur Betrugserkennung. Dashboards bieten autorisierten Benutzern ganzheitliche Einblicke in sämtliche Zahlungsscreenings und können ausstehende Aktionen effizient handhaben.



Workflows zur Betrugsprävention

Moderne Module zur Verhinderung von Zahlungsbetrug unterstützen auch vollständig automatisierte End-to-End-Workflows zur Handhabung ausstehender verdächtiger Zahlungen. Darüber hinaus können Benutzer festlegen, wie die einzelnen erkannten Zahlungen gemanagt werden sollen, und dabei die Aufgabentrennung zwischen Veranlasser, Genehmiger und Prüfer einer erkannten Zahlung durchsetzen. Prüfer können nach Zahlungsregel und spezifischem Szenario bestimmt werden (z. B. prüft der Treasury-Manager Zahlungen unter einer Million US-Dollar, während Zahlungen über einer Million an den Treasurer gehen). Außerdem können auch Mitarbeiter abseits der Treasury-Abteilung mit der Prüfung bestimmter erkannter Zahlungen beauftragt werden.

Berichterstellung und Audit Trails

Führende Technologielösungen können gewährleisten, dass erkannte Zahlungen dauerhaft im System verfolgt werden – für tägliche, monatliche oder jährliche Berichte. Der Verlauf wird nie gelöscht und sämtliche Details verdächtiger Transaktionen, darunter auch der Audit Trail erkannter und gehandhabter Aktionen, werden für immer zwecks interner und externer Berichte aufbewahrt.

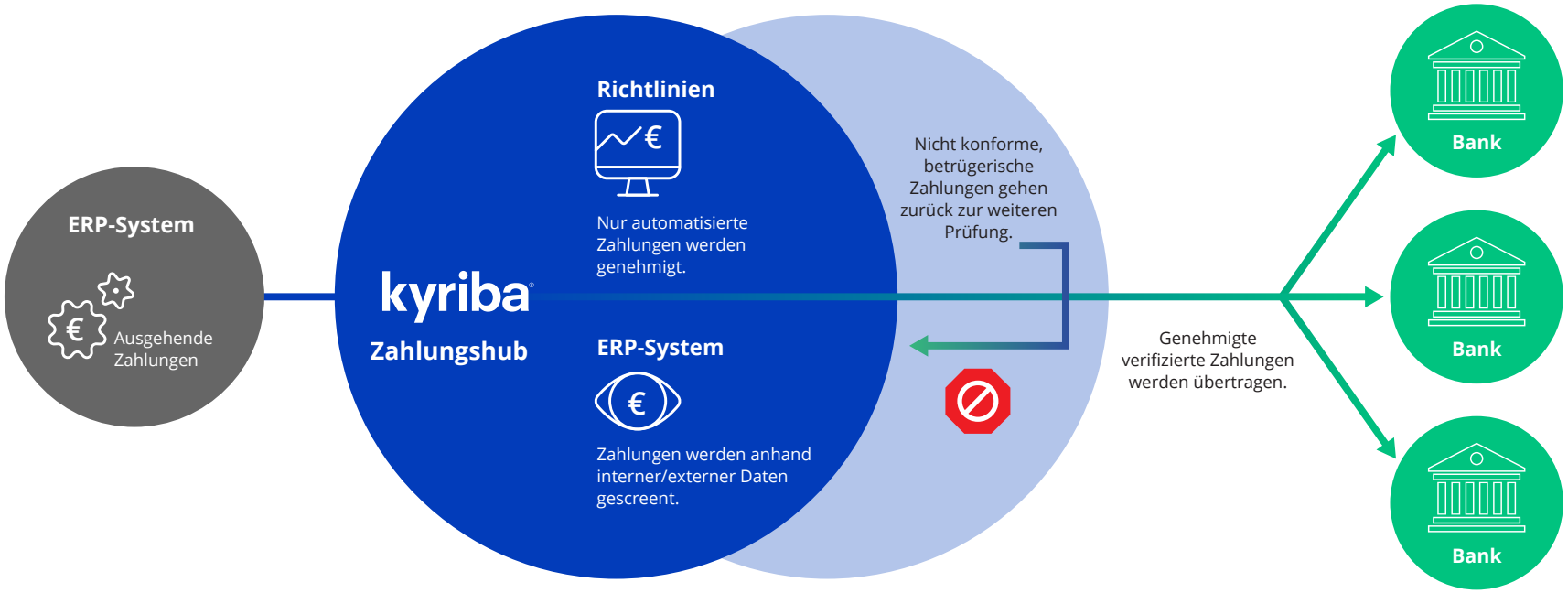
kyriba

Zahlungshubs

Mit einem Zahlungshub können Unternehmen über einen zentralen Ort auf all ihre Betrugsschutz-Funktionen zugreifen. Zahlungshubs konsolidieren Zahlungsströme aus ERPs, Finanz- und Rechtsabteilungen, Treasury, Kapitalmarkt und dezentralen Teams und verwandeln so disaggregierte Prozesse in eine zentrale Datenquelle für sämtliche ausgehenden Zahlungen. Ein Zahlungshub transformiert außerdem Zahlungsdaten in bankenspezifische Dateiformate und stellt mithilfe verschiedener Protokolle, darunter Host-zu-Host, SWIFT und regionale Netzwerke, direkte Verbindungen zu globalen Banken her.

Durch Integration von Zahlungen aus ERPs oder anderen Systemen kann die gesamte Zahlungsumgebung eines Unternehmens in einem einheitlichen, risikobasierten Framework zur Betrugsprävention untergebracht werden. Mit API-basierten Verbindungen und Integrationen in einen Workflow zur Genehmigung und Betrugsprävention werden die Kontrollen verbessert und lassen sich ganz leicht verwalten.

Betrugsschutz per Zahlungshub



Matrix mit Lösungen zur Betrugsabwehr

Treasury- und Finanzmitarbeitern stehen viele Tools zur Betrugsprävention zur Verfügung. Die folgende Liste bietet eine Übersicht einiger wichtiger Funktionen, mit denen moderne Tools Betrugsrisiken mindern.

Tabelle mit Lösungen zur Betrugsabwehr

Lösung	Wichtige Schutzmaßnahmen	Funktionen
Szenarien der Betrugserkennung	Vordefinierte Erkennungsregeln	Kennzeichnet ungewöhnliche Zahlungen zur weiteren Prüfung Regeln können einfach angepasst oder neu erstellt werden
Echtzeitscreening	KI-/ML-Dashboard	Screent Zahlungen anhand von Zahlungsverlaufsdaten Zeigt sämtliche verdächtigen Zahlungen an und priorisiert ihre Lösung
Workflow zur Betrugsprävention	Vollständig automatisierter Workflow	Ermöglicht Benutzern die Handhabung ausstehender verdächtiger Zahlungen Bietet Benutzern die Möglichkeit festzulegen, wie Zahlungen gemanagt werden sollen Setzt die Trennung von Aufgaben rund um erkannte Zahlungen durch Weist Prüfer nach Zahlungsregeln und spezifischem Szenario zu Ermöglicht es, Mitarbeiter außerhalb der Treasury-Abteilung zur Zahlungsprüfung zuzuweisen Bietet eine Option, um Alarme vor Veranlassern/Genehmigern einer Zahlung zu verstecken Ermöglicht szenariobasierte Stopps von Zahlungen, bis diese auf gelöst wurden Bietet eine Umgehungsoption für Zahlungen mit niedrigen Werten Richtet abgestufte Genehmigungen ein
Berichterstellung und Audit Trails	Umfassendes KPI-Reporting	Erkannte Zahlungen werden dauerhaft im System verfolgt Der Verlauf wird nie gelöscht

APIs: Die Zukunft der Betrugserkennung

Echtzeitzahlungen, die sich immer stärker verbreiten, erfordern den Einsatz von APIs. Mithilfe dieser Technologie können zwei oder mehr Softwareanwendungen über interne oder externe Server hinweg kommunizieren. Durch offene Verbindungsprotokolle, mit denen Drittanbieter ihre Technologielösungen entwickeln können, ermöglichen APIs Echtzeitzahlungen in der Unternehmenswelt. Die alte Methode per Dateiübertragung ist einfach zu langsam, um Daten in Echtzeit zu übertragen.

Und da Zahlungen, die einmal per Echtzeittransaktion überwiesen wurden, nicht mehr aufgehalten werden können, muss Betrug bereits im Genehmigungsprozess erkannt und verhindert werden. Durch die Implementierung von APIs in Ihre Zahlungsplattform können Benutzer Bankkonto-Validierungen und Zahlungsrichtlinien-Screenings vollständig automatisieren und automatisch Ausnahmen erkennen.

APIs können Zahlungen sofort mit Drittanbieterdaten abgleichen. So kann beispielsweise sichergestellt werden, dass Zahlungsempfänger nicht auf Sanktionslisten stehen oder dass das Bankkonto auch wirklich dem Empfänger gehört, an den Ihr Unternehmen Geld senden will. Indem Sie APIs in Ihre Zahlungsplattform implementieren, kann Ihr Unternehmen nicht nur in Echtzeit auf Drittanbieterdaten zugreifen, sondern sie auch in Echtzeit abgleichen und Ausnahmen handhaben. Ungewöhnliche Zahlungen werden zur weiteren Prüfung unter Quarantäne gestellt, während normale Zahlungen wie gehabt verarbeitet werden.

kyriba

Erkenntnisse und Fazit

- CFOs und Treasurer brauchen heutzutage umfassende Zahlungskontrollen, um moderne Betrugsrisiken in den Griff zu bekommen – und dazu zählen neben künstlicher Intelligenz und Machine Learning auch APIs.
- In Unternehmen gibt es drei Bereiche, durch die sie anfällig für Betrug sind: technische Systeme, Prozesse und menschliches Versagen.
- Moderne Bedrohungen umfassen BEC-Angriffe, Scheck- und Überweisungsbetrug, Deepfake-Stimmfälschung und Ransomware.
- Auf der anderen Seite stehen Technologien zur Betrugsbekämpfung, wie z. B. Erkennungsregeln, Echtzeitscreening, -alarme und -benachrichtigungen, Workflows zur Betrugsprävention, Berichterstellung und Audit Trails sowie Zahlungshubs.
- Während sich Bedrohungen immer weiterentwickeln, müssen Treasury- und Finanzteams ihr Bewusstsein für diese Bedrohungen schärfen.

kyriba

kyriba

AUSGEWÄHLTE MARKEN, DIE AUF KYRIBA VERTRAUEN

INFORMATIONEN ZUR KYRIBA CORP.

Kyriba ermöglicht CFOs, Treasurern und ihren IT-Kollegen die Transformierung bezüglich der Optimierung von Finanztechnologielösungen, der Minimierung von Risiken bei der ERP-Cloud-Migration sowie der Aktivierung der Liquidität als dynamisches Echtzeitinstrument für das Wachstum und die Wertschöpfung. Mit über 2.500 Kunden weltweit, einschließlich 25 % der Fortune-500- und Eurostoxx-50-Unternehmen, beinhaltet die bahnbrechende „Connectivity as a Service“-Plattform von Kyriba interne Treasury-, Risiko-, Zahlungs- und Working-Capital-Anwendungen, die wichtige externe Quellen wie Banken, ERP-Systeme, Handelsplattformen und Marktdatenanbieter integrieren. Als Teil der Connectivity-Plattform verwaltet Kyriba jährlich mehr als 1,3 Millionen Banktransaktionen sowie 200 Millionen Zahlungen in 140 Länder. Kyriba ist eine sichere, skalierbare SaaS-Plattform, die künstliche Intelligenz nutzt, Zahlungsworkflows automatisiert, mehreren tausend multinationalen Corporations und Banken die Maximierung der Wachstumschancen ermöglicht, Schutz vor Verlust durch Betrug und finanziellen Risiken bietet und die Betriebskosten reduziert. Kyriba hat seinen Hauptsitz in San Diego und unterhält Niederlassungen in Dubai, Frankfurt, London, Minsk, Paris, Schanghai, Singapur, Tokio, Warschau sowie an anderen wichtigen Standorten. Weitere Informationen finden Sie unter **www.kyriba.com**.