LexisNexis®
RISK SOLUTIONS

White Paper

Betrug verstehen und bekämpfen

Die Einführung einer neuen Generation autorisierter Push-Zahlungen

Inhalt

2 Überblick

3 Betrugsmaschen und APP-Betrug verstehen

5 APP-Betrug: Ein zunehmendes Problem

6 APP-Betrug erkennen

7 Sicherheitsebenen zur Erkennung von APP-Betrug

10 Lösungen von LexisNexis® Risk Solutions

Überblick

Betrüger verfolgen hauptsächlich ein Ziel: Mit möglichst geringem Aufwand möglichst viel Geld zu entwenden.

Betrugsmaschen entwickeln sich laufend weiter, um stets die leichtesten Ziele ins Visier zu nehmen. Die Weiterentwicklung der verfügbaren Lösungen zur Überwachung von digitalen Identitäten und Transaktionen macht es Betrügern zusehends schwer, Konten durch Brute-Force-Angriffe zu übernehmen und falsche Identitäten zu verwenden. Unregelmäßigkeiten können effektiv in Echtzeit isoliert werden, um eine Beeinträchtigung der Konten- oder Identitätssicherheit zu verhindern.

Aus diesem Grund haben Betrüger sich einen neuen Ansatzpunkt gesucht. Da ihre Hauptkontrahenten, die Banken, nun ihre Schutzmaßnahmen verstärken, richten sie ihre Aufmerksamkeit nun auf das nächste naheliegende Ziel: die Kunden selbst. Entsprechend rasch hat die Zahl und Komplexität der Betrugsmaschen zugenommen, was sich schnell zur Plage für Finanzdienstleister und E-Commerce-Händler entwickelt.

So verleiten beispielsweise perfekt ausgeklügelte Social-Engineering-Versuche unter dem Vorwand, Konten oder Vermögenswerte zu schützen, ahnungslose Kunden dazu, persönliche Daten preiszugeben oder eine autorisierte Zahlung an den vom Betrüger angegebenen Empfänger zu senden. Anders als bei herkömmlichen Betrugsversuchen, bei denen ein Gerät des Betrügers oder gestohlene Daten zum Einsatz kommen würden, sind die üblichen Erkennungsmethoden, die sich auf Unregelmäßigkeiten in puncto Geräte, Standort oder Identitätsdaten beziehen, unwirksam, wenn der Kunde unwissentlich Beihilfe leistet.

Wie können Organisationen eine moderne Betrugsabwehr aufbauen, die Brute-Force-Betrugsversuche und Identitätsdiebstahl von komplexem Betrug mit autorisierten Push-Zahlungen (Authorized Push Payment, APP) unterscheidet?

In diesem White Paper befassen wir uns mit APP-Betrug und den Best Practices zur Auswahl einer Betrugsabwehrlösung.

Betrugsmaschen entwickeln sich laufend weiter, um stets die leichtesten Ziele ins Visier zu nehmen.

Inhalt

2 Überblick

3 Betrugsmaschen und APP-Betrug verstehen

5 APP-Betrug: Ein zunehmendes Problem

6 APP-Betrug erkennen

7 1A;@=J@=ALK=:=F=F zur Erkennung von APP-Betrug

10 Lösungen von LexisNexis® Risk Solutions

Betrugsmaschen und APP-Betrug verstehen

Es gibt diverse Arten von Betrugsmaschen, doch alle das gleiche Ziel: Kunden dazu zu bringen, Geld oder Informationen herauszugeben, welche seinem Glauben nach einem rechtmäßigen Empfänger zugeführt werden oder einem legitimen Zweck dienen sollen. Die Absicht könnte beispielsweise sein, Güter, Dienstleistungen oder einen neuen Partner zu bezahlen oder ein angeblich gefährdetes Konto bzw. einen kompromittierten Dienst zu schützen.

Beim Kontoübernahmebetrug (Account Takeover, ATO) verschafft sich der Betrüger mit sensiblen Kunden-, Bank- oder Zahlungsdaten unbefugt Zugang zum Konto seines Opfers, das dann für betrügerische Käufe oder Zahlungen verwendet wird. Der Begriff „Social Engineering“ bezeichnet die Praxis von Betrügern, Opfer zur Preisgabe der Informationen zu verleiten, die sie benötigen, um sich für ATO- und andere Betrugsversuche Zugang zu Konten zu verschaffen.

Ein häufig zu beobachtendes Szenario ist, dass sich ein Betrüger mit den Anmeldedaten eines Kunden für das Online-/Mobile-Banking registriert. Dazu fängt der Betrüger die Einmalkennung (One-Time Passcode, OTP) ab, die zur Authentifizierung der Online-Banking-Registrierung versendet wird. Der Täuschungsversuch besteht darin, dass der Betrüger durch Social Engineering entweder beim Mobilfunkanbieter des Kunden eine neue SIM-Karte bestellt und Nachrichten auf sein Gerät umleitet oder das Opfer selbst dazu bringt, den OTP preiszugeben. Anschließend verwendet der Betrüger diese Informationen, um sein Gerät für das Konto des Kunden zu registrieren und Betrug zu begehen.

Wie bei anderen Betrugsmaschen auch besteht das Ziel von APP-Betrug darin, den Kunden zu einer Zahlung an den Betrüger zu bewegen – entweder über die Website eines Dritten oder direkt auf das gewünschte Bankkonto. APP-Betrug unterscheidet sich von anderen Betrugsmaschen darin, dass die Taktiken komplexer sind und sich ausgefeilter, gezielter Social-Engineering-Techniken bedienen, oft über einen langen Zeitraum.

Zudem beinhaltet APP-Betrug in der Regel eine direkte Interaktion zwischen Kunde und Betrüger. Der Betrug kann neben dem anfänglichen finanziellen Schaden auch künftige Schäden nach sich ziehen, wenn der unbefugte Zugriff auf ein Konto länger besteht. Da die finanziellen Schäden sich aus einer vom Opfer veranlassten Zahlung ergeben, sind sie nur schwer rückgängig zu machen.

Beim Kontoübernahmebetrug (Account Takeover, ATO) verschafft sich der Betrüger mit sensiblen Kunden-, Bank- oder Zahlungsdaten unbefugt Zugang zum Konto seines Opfers, das dann für betrügerische Käufe oder Zahlungen verwendet wird.

Inhalt

2 Überblick

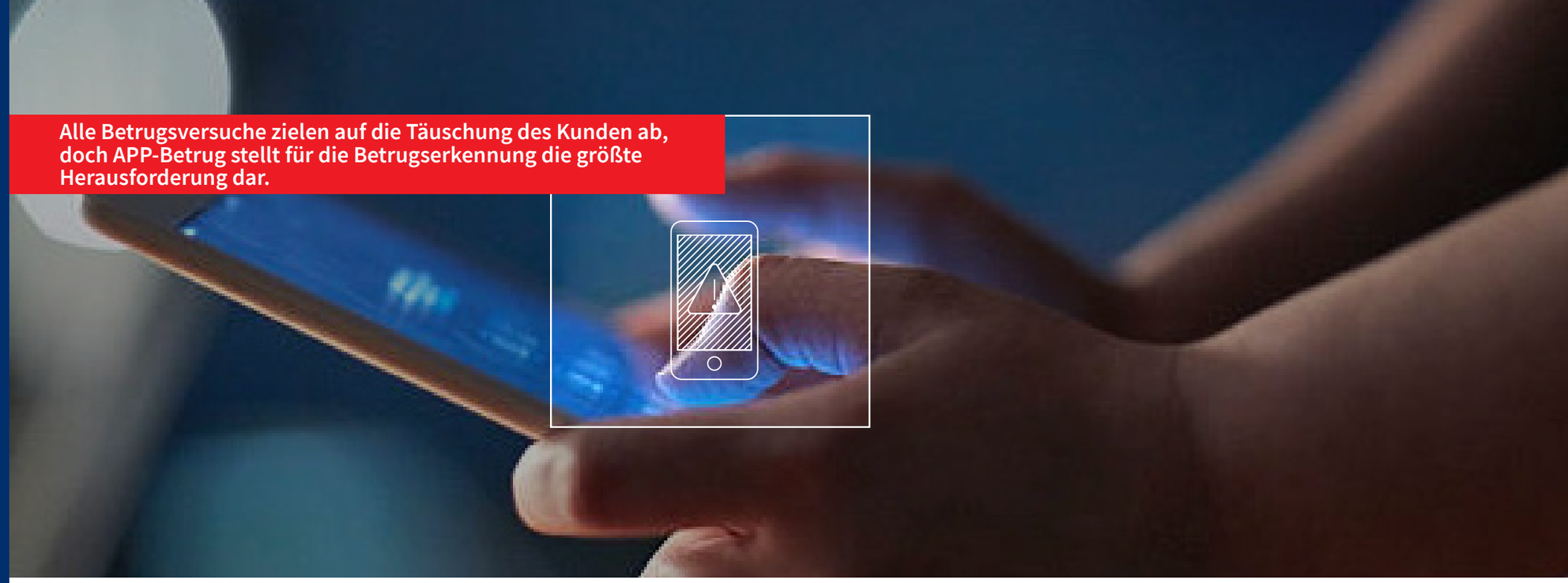
3 Betrugsmaschen und APP-Betrug verstehen

5 APP-Betrug: Ein zunehmendes Problem

6 APP-Betrug erkennen

7 **Sicherheitsebenen** zur Erkennung von APP-Betrug

10 Lösungen von LexisNexis® Risk Solutions



Alle Betrugsversuche zielen auf die Täuschung des Kunden ab, doch APP-Betrug stellt für die Betrugserkennung die größte Herausforderung dar.

Es gibt viele unterschiedliche Formen von APP-Betrug, darunter Romance Scams, Identitätsbetrug (d. h. der Betrüger gibt sich als Banksachbearbeiter, Staatsbediensteter, Mitarbeiter des Telekommunikationsanbieters usw. aus und fordert vertrauliche Daten oder eine Zahlung an) und Betrugsversuche mit kompromittierten Konten. Andere Betrugsmaschen verbinden Elemente von ATO-Betrug, Social Engineering und APP-Betrug.

So gibt es etwa prominente Beispiele für so genanntes „Smishing“ (Phishing per SMS), bei dem der Kunde unter dem Vorwand einer verpassten Lieferung oder attraktiven Anlagemöglichkeit zur Preisgabe sensibler Daten verleitet wird. Während der Kunde den Eindruck hat, einen Liefertermin verschoben oder sich für ein Anlagekonto registriert zu haben, nutzt der Betrüger diese Gelegenheit tatsächlich dazu, vertrauliche Daten über das Bankkonto seines Opfers zu beschaffen.

Anschließend nutzt der Betrüger die Tatsache aus, dass der Kunde auf den einleitenden Betrugsversuch hereingefallen ist, um ihn zu der Annahme zu verleiten, er müsse sein Bankkonto gegen weitere Betrugsversuche absichern. Dies beinhaltet in der Regel, den Kunden dazu zu bewegen, sein Guthaben über eine autorisierte Push-Zahlung (APP) auf ein „sicheres“ Konto zu verschieben.

Alle Betrugsversuche zielen auf die Täuschung des Kunden ab, doch APP-Betrug stellt für die Betrugserkennung die größte Herausforderung dar. Der Grund: Der Betrüger agiert wie ein Puppenspieler im Hintergrund und steht nicht im Fokus des Geschehens. Er ist daher weit schwieriger aufzuspüren, da er durch die scheinbare „Normalität“ der Transaktion des Kunden geschützt ist. Selbst starke Kundenauthentifizierung (SKA) ist wirkungslos gegen APP-Betrug, da es der – vom Betrüger manipulierte – Kunde ist, der die Überprüfung im Rahmen einer laufenden Card-not-present-Transaktion (CNP) validiert.

Inhalt

2 Überblick

3 Betrugsmaschen und APP-Betrug verstehen

5 APP-Betrug: Ein zunehmendes Problem

6 APP-Betrug erkennen

7 Sicherheitsebenen zur Erkennung von APP-Betrug

10 Lösungen von LexisNexis® Risk Solutions

APP-Betrug: Ein zunehmendes Problem

Einer aktuellen Meldung von UK Finance zufolge nimmt die Zahl der APP-Betrugsversuche derzeit zu.[1] Sie machen inzwischen rund 38 % aller betrugsbedingten Schäden aus und liegen damit auf dem zweiten Platz hinter Kartenbetrug. 2020 verursachte dieser Betrugstyp in Großbritannien Schäden in Höhe von 479 Millionen Pfund. Das ist mehr als doppelt so viel, wie durch unbefugtes Telebanking verloren ging – eine Betrugskategorie, die Kontoübernahmen und Identitätsbetrug beinhaltet. Das Problem ist bereits groß und wird noch größer. Entsprechend steht APP-Betrug zunehmend im Fokus der Finanzinstitute.

Zudem hat sich mit dem CRM Code (Contingent Reimbursement Model) die Haftung für die durch Betrug entstandenen Schäden vom Kunden auf die Finanzinstitute verlagert. Obwohl dies anscheinend nicht zu einer merklichen Zunahme der APP-Betrugsversuche geführt hat, hat es die Aufmerksamkeit erneut auf deren Opfer gelenkt.

Der CRM Code räumt nicht nur ein Stück weit mit der Stigmatisierung von Kunden und deren Scham auf, denen der „Fehler“ einer APP unterlaufen ist, sondern verbessert auch die Chancen auf Rückerstattung. Das ist besonders für Kunden, für die digitales Banking noch Neuland ist, sowie für andere vulnerable Kundenkategorien relevant, die dieser sich entwickelnden Betrugsmasche eher zum Opfer fallen können.

1. ukfinance.org.uk/policy-and-guidance/reports

Inhalt

2 Überblick

3 Betrugsmaschen und APP-Betrug verstehen

5 APP-Betrug: Ein zunehmendes Problem

6 APP-Betrug erkennen

7 Sicherheitsebenen zur Erkennung von APP-Betrug

10 Lösungen von LexisNexis® Risk Solutions

APP-Betrug erkennen

Das Aufspüren und Unterbinden von APP-Betrug ist besonders schwierig, weil es der Kunde ist, der die Bank oder den Zahlungsdienstleister zur Überweisung des Geldes von seinem Konto veranlasst – nicht der Betrüger. Die folgenden Aspekte veranschaulichen, warum APP-Betrug so schwer aufzuspüren ist.

Die Zahlung wird vom legitimen Kontoinhaber im Rahmen einer vollständig authentifizierten Online-Banking-Sitzung getätigt. Alternativ absolviert der Kunde eine SKA-Prüfung im Rahmen einer vom Betrüger eingeleiteten CNP-Transaktion.

Schon wenige Informationen können verheerende Wirkung haben: Betrüger können persönliche Daten ihrer Opfer über die sozialen Medien, Datenraub und sonstige Phishing-Attacken beziehen, um ihren Schwindel plausibler wirken zu lassen.

Das Opfer hält die Zahlung für legitim, was bedeutet, dass Aufklärungs- und Sensibilisierungsversuche bisweilen ins Leere laufen.

Betrüger nutzen die Sorgen, Bedenken oder den wahrgenommenen Handlungsdruck ihres Opfers aus, was das Unterbrechen einer Zahlungstransaktion sehr schwierig machen kann.

Echtzeit-Überweisungen führen dazu, dass Geld unmittelbar das Konto eines Opfers verlässt und sehr schwer nachzuverfolgen oder zurückzufordern ist, besonders, wenn der Betrag aufgeteilt und über eine Reihe von Zwischenkonten weitergereicht wurde.

Inhalt

2 Überblick

3 Betrugsmaschen und APP-Betrug verstehen

5 APP-Betrug: Ein zunehmendes Problem

6 APP-Betrug erkennen

7 Sicherheitsebenen zur Erkennung von APP-Betrug

10 Lösungen von LexisNexis® Risk Solutions

Zur Bekämpfung von APP-Betrug sollten Finanzinstitute eine Betrugsabwehrlösung der nächsten Generation in Erwägung zu ziehen.

Sicherheitsebenen zur Erkennung von APP-Betrug

Die Entwicklung einer effektiven Lösung zur Identifikation potenzieller Betrugsversuche hängt von der Fähigkeit ab, die Kontoinhaber ganzheitlich betrachten zu können.

Dies schließt die Untersuchung ihres Verhaltens sowie ihrer Interaktion in Online-Banking-Sitzungen ein, deren Ergebnisse mit Erkenntnissen zu ungewöhnlichen oder einmaligen Ereignissen und Informationen zu Zahlungsempfängern verknüpft werden.

Zur Bekämpfung von APP-Betrug sollten Finanzinstitute eine Betrugsabwehrlösung der nächsten Generation in Erwägung zu ziehen. Diese sollte fünf wichtige Funktionen beinhalten:

1.

Informationsaustausch

Der Informationsaustausch bezeichnet die Fähigkeit, Daten und Erkenntnisse mit anderen auszutauschen, um in Form eines besseren Verständnisses der eigenen Kunden zu profitieren. Dies kann Folgendes beinhalten:

- Abfrage eines globalen Informationsnetzwerks: Wurde dieses Gerät, diese Persona oder dieses Verhaltensmuster bereits im Kontext eines anderen Betrugsversuchs beobachtet?
- Datenaustausch: Wurde der Empfänger bei anderen Finanzorganisationen mit Betrugsaktivitäten oder betrügerischen Zwischenkonten in Verbindung gebracht?
- Informationsgewinnung über mehrere Kanäle: Durch die Sammlung von Informationen aus mehreren Quellen können in der Filiale und im Callcenter fundiertere risikobezogene Entscheidungen getroffen werden.

1. ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2021

Inhalt

2 Überblick

3 Betrugsmaschen und APP-Betrug verstehen

5 APP-Betrug: Ein zunehmendes Problem

6 APP-Betrug erkennen

7 Sicherheitsebenen zur Erkennung von APP-Betrug

10 Lösungen von LexisNexis® Risk Solutions

2.

Verhaltensanalyse

Indem sie ein klares Bild davon zeichnet, wie und aus welchen Gründen Kunden mit Geräten und Software interagieren, ermöglicht die Verhaltensanalyse genaue Vorhersagen darüber, wie Kunden sich künftig wahrscheinlich verhalten dürften. Die Verhaltensanalyse kann folgende Erkenntnisse liefern:

- Informationen zu neuen Geräten: Identifiziert neue Software für den Fernzugriff auf das Konto, die bislang nicht genutzt wurde, was ein Anzeichen für eine Kontrollübernahme durch Betrüger sein kann.
- Risikoreiche Kontoverwaltungsmuster: Einrichtung neuer Empfänger, rasch gefolgt von Überweisungsversuchen.
- Zahlungsanomalien: Im Vergleich zum Durchschnitt des Kunden höhere Zahlungen als sonst. Überweist der Kunde sein gesamtes Guthaben oder einen großen Teil davon?
- Ungereimtheiten bezüglich des Empfängers: Möglichkeit zur Überwachung, wohin eine Überweisung geht, mit Informationen über den Empfänger sowie den Zahlenden. Kennzeichnung von risikoreichem Verhalten im Zusammenhang mit dem Empfängerkonto, beispielsweise mehrere Zahlungen mit hohem Volumen, Verbindungen zu Money Mules oder Überweisungen an andere risikoreiche Bankleitzahlen oder Konten.

3.

Transaktionsüberwachung entlang der Customer Journey und des Zahlungsprozesses

Transaktionsüberwachung bezeichnet die Überwachung von Kundentransaktionen einschließlich der Beurteilung historischer/aktueller Kundeninformationen und -interaktionen, um ein Gesamtbild der Kundenaktivität zu gewinnen. Effektive Lösungen gegen APP-Betrug sollten Flags für folgende Punkte bieten:

- Ungewöhnliches Verhalten bei der Anmeldung: Kunde meldet sich häufiger an als üblich, Anmeldung erfolgt zu einem ungewöhnlichen Zeitpunkt, über einen neuen Kanal (z. B. Desktop-PC) oder einen Browser, der zuvor nicht verwendet wurde.
- Risikoreiche Kontoverwaltungsmuster: Einrichtung neuer Empfänger, rasch gefolgt von Überweisungsversuchen.
- Zahlungsanomalien: Im Vergleich zum Durchschnitt des Kunden höhere Zahlungen als sonst. Überweist der Kunde sein gesamtes Guthaben oder einen großen Teil davon?
- Ungereimtheiten bezüglich des Empfängers: Möglichkeit zur Überwachung, wohin eine Überweisung geht, mit Informationen über den Empfänger sowie den Zahlenden. Kennzeichnung von risikoreichem Verhalten im Zusammenhang mit dem Empfängerkonto, beispielsweise mehrere Zahlungen mit hohem Volumen, Verbindungen zu Money Mules oder Überweisungen an andere risikoreiche Bankleitzahlen oder Konten.

Inhalt

2 Überblick

3 Betrugsmaschen und APP-Betrug verstehen

5 APP-Betrug: Ein zunehmendes Problem

6 APP-Betrug erkennen

7 Sicherheitsebenen zur Erkennung von APP-Betrug

10 Lösungen von LexisNexis® Risk Solutions

4.

Opfer-Profiling

Mithilfe digitaler Analyse kann das Profiling potenzieller Opfer ermitteln, ob ein Kunde ein attraktives Ziel für Betrüger ist. Unter anderem werden folgende Punkte berücksichtigt:

- War der Kunde bereits Opfer eines Betrugs?
- Wurde der Kunde bei anderen Organisationen mit betrügerischen Aktivitäten in Verbindung gebracht?
- Entspricht dieser Kunde dem Profil anderer Betrugsopfer?

5.

Gewinnung zusätzlicher/externer Daten zur Verbesserung risikobezogener Entscheidungsfindung

Daten liefern zusätzliche Erkenntnisse und tragen so zu einer Rundumansicht des Kunden bei, die fundiertere Entscheidungen ermöglicht. Quellen für Mehrwert schaffende Daten sind unter anderem:

- Sprachbiometrie: Wird verwendet, um in der Stimme des Kunden Anzeichen für Anspannung oder Zwang zu erkennen.
- Modellierung der Money-Mule-Tendenz: Verarbeitung zusätzlicher Risikosignale/-kennzahlen, um zu ermitteln, mit welcher Wahrscheinlichkeit es sich beim Empfängerkonto um das eines Money Mule handelt.
- Telefonnutzungsinformationen: In Zusammenarbeit mi Mobilfunknetzbetreibern werden zusätzliche Daten zur Herkunft, Häufigkeit und zum Ursprungsort betrügerischer Nachrichten und Anrufe gesammelt
- Identitätsprüfungen: Nutzung zusätzlicher Informationen von Identitätsprüfungsdienstleistern, um zusätzlichen Kontext zum Zahlungsempfänger zu erhalten.

Inhalt

2 Überblick

3 Betrugsmaschen und APP-Betrug verstehen

5 APP-Betrug: Ein zunehmendes Problem

6 APP-Betrug erkennen

7 Sicherheitsebenen zur Erkennung von APP-Betrug

10 Lösungen von LexisNexis® Risk Solutions

Lösungen von LexisNexis® Risk Solutions

LexisNexis Risk Solutions unterstützt Sie mit folgenden Produkten und Dienstleistungen beim Aufbau einer strategischen Betrugsabwehr.

Das LexisNexis® Digital Identity Network®

Das Digital Identity Network ist ein globaler Speicher tokenisierter Daten, die per Crowdsourcing von allen Organisationen zusammengetragen wurden, die unsere digitale Identitätslösung **LexisNexis ThreatMetrix** nutzen. Das Netzwerk verarbeitet mehr als 55 Milliarden Transaktionen pro Jahr aus einer Vielzahl von Branchen in den meisten Weltregionen.

Organisationen, die ThreatMetrix nutzen, profitieren von einer gemeinsamen Informationsquelle, die Daten zu Geräten, Standorten, Verhaltensmustern und bekannten Bedrohungen auf globaler, regionaler, Branchen- und Unternehmensebene enthält. Mit ThreatMetrix können Finanzinstitute besser nachvollziehen, ob ein Gerät, eine Persona oder ein Empfänger innerhalb des Netzwerks mit vertrauenswürdigem, risikoreichem oder ungewöhnlichem Verhalten assoziiert wurde.

Verhaltensanalyse und maschinelles Lernen mit ThreatMetrix

Die intelligente Analyse von ThreatMetrix verbindet Informationen aus dem Digital Identity Network mit Verhaltensanalyse (intelligente Regeln) und maschinellem Lernen (intelligentes Lernen).

Die intelligenten Regeln von ThreatMetrix helfen Banken dabei, Widersprüche zwischen dem aktuellen und früheren Kundenverhalten zu identifizieren, um auf Kundenebene einen Richtwert der durchschnittlichen Zahlungsbeträge zu erhalten. ThreatMatrix setzt Banken darüber in Kenntnis, wenn eine Transaktion von diesem Richtwert abweicht, und bietet flexible Möglichkeiten zur Anpassung von Variablen und zur Aufnahme bzw. dem Ausschluss einzelner Datenpunkte.

Das intelligente Lernverhalten von ThreatMetrix kann dafür verwendet werden, ungewöhnliches oder risikoreiches Verhalten besser zu modellieren. Intelligentes Lernen ist ein Clear-Box-Ansatz, der eine Bewertung generiert und zeigt, warum das Modell eine bestimmte Entscheidung getroffen hat. In Verbindung mit den eigenen Bewertungskennzahlen einer Organisation stellt intelligentes Lernen eine optimale Kombination aus KI und einem traditionelleren regelbasierten Ansatz dar.

Inhalt

2 Überblick

3 Betrugsmaschen und APP-Betrug verstehen

5 APP-Betrug: Ein zunehmendes Problem

6 APP-Betrug erkennen

7 Sicherheitsebenen zur Erkennung von APP-Betrug

10 Lösungen von LexisNexis® Risk Solutions

Verhaltensbiometrische Daten

Verhaltensbiometrie bietet zusätzlichen Kontext in Bezug auf Risiken. Dabei wird analysiert, wie ein Nutzer seine Geräte online verwendet und welche digitale Identität dadurch geschaffen wird.

LexisNexis Risk Solutions kann während der gesamten Journey im Online Banking Daten zur Verwendung von Tastatur und Maus, Touchscreen-Sensordaten sowie Bewegungsdaten eines Geräts sammeln. Diese Daten werden dann mittels moderner Methoden des maschinellen Lernens analysiert, um Szenarien zu ermitteln, die auf Social Engineering hindeuten können. Es werden automatisch Risikoscores generiert und mit Kunden geteilt, die sie für ihre betrugsbezogenen Entscheidungen und Regeln nutzen können.

Neben den Scores und Begründungscodes stehen die meisten im Zuge des Profiling gesammelten Daten im ThreatMetrix-Portal zur Verfügung. Betrugsanalysten können diese Rohdaten abrufen und nutzen und erhalten somit wichtige Erkenntnisse über Kundentransaktionen.

Consortium

Mit Consortium können ähnlich ausgerichtete Organisationen Informationen und Feedback zu Betrugsfällen mit zusätzlichen Vertrauens- und Kontextinformationen in Echtzeit austauschen. Banken im Consortium können auf umfassende kontextbezogene Daten zugreifen, zum Beispiel zu bestätigtem First-Party-Fraud und Konten von Money Mules. Darüber hinaus können Mitglieder dank komplexer Analysen und der Implementierung von Regeln ein Verständnis davon erlangen, mit welchen anderen Mitgliedern im Consortium sie am stärksten korrelieren, um so Risikoentscheidungen besser abzuwägen.

Ein Konsortium aus britischen Banken baut derzeit ein gemeinsames Repository von Risikoindikatoren (z. B. betrügerische Geräte, IP-Adressen, Konten von Money Mules) zur Nutzung durch die Mitglieder auf.

Zwei-Parteien-Zahlungsmodell

Das Zwei-Parteien-Zahlungsmodell von LexisNexis Risk Solutions ermöglicht Organisationen, sich in Bezug auf den von der Zahlung Begünstigten denselben Grad an Kontext und Informationen zunutze zu machen wie der Zahler.

Mit dem Zwei-Parteien-Zahlungsmodell werden nun standardmäßig zusätzlich sowohl Daten zum Kontoinhaber, der die Zahlung vornimmt, als auch zum Zahlungsempfänger – dem Begünstigten – über die ThreatMetrix-API abgerufen. Beide Parteien werden somit auf globaler Ebene standardmäßige Instanzen mit sämtlichen verhaltens- und kontextbezogenen Informationen und Betrugsindikatoren, die zu beiden Instanzen zur Verfügung stehen. Die in einer Organisation vorliegenden Angaben zum Begünstigten der Zahlung stimmen mit den Kontodaten bei der anderen Organisation überein, wo der Begünstigte angesiedelt ist. Dies erleichtert die Analyse zur Netzwerk- und Transaktionsüberwachung.

Integration Hub

Der Integration Hub ermöglicht Organisationen den Zugriff auf relevante Drittquellen und individuelle Dienstleistungen, um zusätzliche Informationen zu Opfern, Begünstigten oder bekannten Konten von Money Mules zu erhalten. Eine REST-basierte API stellt die Verbindung zu Cloud- und Unternehmensdatenquellen und -diensten sowie zu zusätzlichen Services im Rahmen von LexisNexis Risk Solutions her, zum Beispiel zu LexisNexis® IDU® (Identitätsprüfung). Als Brücke zwischen verschiedenen Systemen bietet der Integration Hub während der Erstbereitstellung oder später bei Erreichung der Systemreife Zugang zu umfangreicheren Datenquellen.

Weitere Informationen erhalten Sie online unter risk.lexisnexis.com/global/de oder unter der Telefonnummer +49 (0) 721 205 96 2925.

LexisNexis®
RISK SOLUTIONS

LexisNexis Risk Solutions

LexisNexis® Risk Solutions setzt auf die Macht der Daten und stützt sich auf moderne Analytik, um Unternehmen und staatlichen Behörden zu Erkenntnissen zu verhelfen, mit denen sie Risiken reduzieren und bessere Entscheidungen im Sinne aller treffen können. Wir bieten Daten- und Technologie-Lösungen für verschiedenste Branchen wie beispielsweise die Versicherungsbranche, die Finanzdienstleistungsindustrie und das Gesundheitswesen sowie staatliche Stellen. Unsere Zentrale befindet sich in Atlanta, Georgia; zudem verfügen wir über Büros in verschiedenen Ländern der Welt. LexisNexis® Risk Solutions ist Teil des globalen Informationsanbieters RELX (LSE: REL/NYSE: RELX). Weitere Informationen finden sich unter www.risk.lexisnexis.com und www.relx.com.

NXR15048-01-0921-EN-DE