Best Practice Toolkit zur Betrugsprävention.

Praktische Schritte zur nachhaltigen und optimalen Betrugsbekämpfung.

NUANCE

Inhaltsverzeichnis

Traditioneller Identitätsnachweis ist tot

Persönliche Identifikationsnummern (PINs), Passwörter und komplexe Sicherheitsfragen - die Antworten, an die sich viele Kunden nicht erinnern können - haben endlich ausgedient. Die hohe Zahl von Datenschutzverletzungen bei personenbezogenen Daten und Benutzerdaten hat dazu geführt, dass laut einem Gartner-Analysten[1] durchschnittlich 15%-30% der Kunden den eigenen Identitätsnachweis nicht bestehen, während bis zu 60% der Kriminellen ihn erfolgreich ablegen.

Es ist schwer vorstellbar, dass eine Ausfallquote von 15%-30% in anderen Geschäftsbereichen akzeptabel wäre - geschweige denn einen mit so negativen Auswirkungen und so weitreichenden Folgen für die Kundenbindung. Man geht daher davon aus, dass innerhalb von fünf Jahren antwortbasierte Authentifizierung verschwunden sein wird, um sensible Konten oder Daten vor Betrug zu schützen.

Ein Grund dafür ist die zunehmende Zahl von Unternehmen, die sich für Lösungen wie die Nuance Security Suite entscheiden. PINs, Passwörter und Sicherheitsfragen werden durch Sprachbiometrie und andere Merkmale, die Betrüger schwieriger umgehen können, ersetzt. Im Jahr 2017 wurden weltweit 90 Milliarden wissensbasierte Zugangsdaten verwaltet, dem gegenüber standen 300 Millionen Sprachprints zur Authentifizierung, die mit Sprachbiometrie-Lösungen von Nuance genutzt wurden. Die Anzahl der aktiv verwendeten Sprachabdrucke wächst exponentiell, bereits im Jahr 2017 verdoppelte sich die Anzahl und für das Jahr 2018 wurde ein ähnlicher Trend erwartet.

Wenn auch Ihr Unternehmen wie auch andere führende Unternehmen aktuell seinen Ansatz zur Kundenauthentifizierung und Betrugsprävention im Kundenservice überdenkt, können Sie von diesem Best Practice Toolkit von Nuance profitieren. Sie erhalten Einblick in umfassende Erfahrungen in der Erstellung und Pflege optimaler Lösungen zur Betrugsprävention, einschließlich Antworten auf Fragen wie:

– Wie stellt sich Ihre Organisation gegen Betrug?
– Wie können Sie die Betrugsanfälligkeit Ihres Unternehmens bewerten?
– Welches sind die Vorteile von Offline- und Echtzeit-Betrugserkennung?
– Wie sehen die Zyklen der Betrugsangriffe aus?
– Wie können Sie den Wert von Warnungen und Managementinformationen steigern, das Blacklist-Management und die Datenanalyse optimieren sowie Warnmeldungen priorisieren und umfangreiche Metadaten erfassen?
– Wie kann Ihre Betrugsprävention, an die sich ständig ändernden Betrugsvorgehen, angepasst werden?

Finden Sie heraus, wie Ihre Organisation mit Betrug umgeht

Das offensichtliche Ziel einer Betrugspräventionslösung liegt darin, die Verluste durch Betrug für das Unternehmen zu minimieren. Doch in Wirklichkeit kann die Toleranz für Betrugsvorfälle sehr weit auseinanderliegen.

Die 3 wichtigsten Vorteile der Sprachbiometrie:

Kostenreduzierung

Betrugsminimierung

Markendifferenzierung

1 Avivah Litan, Gartner Analyst, Absolute Identity Proofing is Dead, November 2015

So könnte beispielsweise ein neu gegründetes Kreditkartenunternehmen das Ziel haben, Transaktionsvolumen und Umsätze zu steigern, um am Markt Fuß zu fassen.

Daher soll es dessen Kunden sehr einfach gemacht werden per Kreditkarte zu zahlen, ohne Hindernisse für einen reibungslosen bargeldlosen Ablauf.

Das könnte bedeuten, dass neben einem grundlegenden Authentifizierungsverfahren wie einer PIN auch Transaktionen durch die Unterschrift des Kunden verifiziert werden können - auch wenn diese selten überprüft wird und praktisch keinen Schutz vor Betrug bietet. Das Unternehmen wird somit entschieden haben, auf Kosten der Sicherheit erhebliche Betrugsverluste abzuschreiben, nur um den Kunden eine einfache Bezahlung zu ermöglichen und den eigenen Umsatz zu steigern.

Im Gegensatz dazu steht die Einstellung eines Finanzinstituts, das neben traditionellen und langfristigen Finanzprodukten wie z. B. Renten, Hypotheken, Versicherungen nun auch Kreditkarten anbietet - oder dessen Agilität durch alte Systeme und eine konservative Kultur und Denkweise eingeschränkt ist. Da dieses Unternehmen jetzt neben einmaligen und hochwertigen Transaktionen auch volumen- und wertmäßig niedrigere Transaktionen aus Kreditkartenkäufen abwickeln muss, wird die Risikotoleranz - einschließlich Betrug – weitaus geringer sein.

Infolgedessen kann die Betrugsprävention mit den dazugehörigen Mechanismen, Prozessen und Kontrollen bei der Authentifizierung und Verifizierung sehr viel komplexer sein, als bei innovativeren Kreditkartenunternehmen - auch für so etwas Einfaches wie die Ausgabe einer neuen PIN. Hier spielt ebenso die Unternehmenskultur eine wichtige Rolle, und kann Veränderungen verhindern, auch wenn dies negative und potenziell schädliche Auswirkungen auf das Kundenerlebnis haben wird.

Auch wenn beide im Beispiel genannte Unternehmen ansonsten identische Kreditkartenprodukte anbieten, wird sich ihre eklatant unterschiedliche Risikobereitschaft nicht nur auf die Betrugssicherheit, sondern auch auf die Authentifizierungs- und Verifizierungsprozesse, die Kommunikation und den Umgang mit ihren Kunden auswirken.

Best Practice von Nuance

Diese Beispiele veranschaulichen die unterschiedliche Herangehensweise an die Themen Sicherheit und Kundenzufriedenheit. Auf der einen Seite werden strenge Sicherheitskontrollen implementiert und erzeugen schwerfällige und unfreundliche Kundeninteraktionen, die sich negativ auf die Marke auswirken können. Andererseits wird das Kundenerlebnis so einfach wie möglich gestaltet und kann zu unvollständigem Betrugsschutz und somit zu hohen betrugsbedingten Verlusten führen.

Damit Ihr Unternehmen die beste Lösung finden kann, muss vorab immer eine Risikobewertung durchgeführt werden. Hierbei wird die Risikobereitschaft Ihrer Organisation ermittelt und die Einschätzung zwischen Komfort und Sicherheit herausgearbeitet. Es wird empfohlen den Punkt zwischen diesen beiden Extremen anzustreben, der das optimale Gleichgewicht zwischen der Minimierung von Betrugsverlusten und dem besten Kundenservice sicherstellt. Nuance unterstützt außerdem:

– mit der Authentifizierung und Verifizierung durch Sprachbiometrie, Identitätsbetrug zu verhindern, und so die Sicherheit nach innen zu verbessern.
– Maßnahmen zur Betrugsbekämpfung einzusetzen, die es Ihnen ermöglichen, bekannte und hartnäckige Betrüger zu identifizieren und den Schutz gegen sie zu verstärken.

Bewertung Ihrer Betrugsanfälligkeit

Bevor Sie beginnen, Ihre Anfälligkeit für Betrug zu verringern, müssen Sie sich ein klares Bild von den Betrugsvorfällen machen, einschließlich der Höhe des Betrugs und der Art der Angriffe, die Sie derzeit erleben.

Auf diese Weise können Sie das Ausmaß Ihres Betrugsproblems verstehen; sind die Betrugskosten angesichts der Art Ihres Unternehmens akzeptabel; wie und wo kann ein Lösungsanbieter wie Nuance Ihnen am besten helfen, die Betrugsangriffe und Verluste zu reduzieren; und welche Auswirkungen hat Ihre Risikobereitschaft, im Gleichgewicht zwischen Sicherheit und Qualität der Kundenerfahrung.

Als Praxisbeispiel betrachten wir uns die unterschiedlichen Betrugsvorfälle und Schutzmaßnahmen in einem Versorgungsunternehmen, einer Bank und einem Kreditkartenunternehmen.

- Wenn ein Versorgungsunternehmen für Kabel- oder Satellitenfernsehen einen neuen Kunden gewinnt, ist seine Haftung in der Regel auf den Wert der beim Kunden installierten Set-Top-Box (und Satellitenschüssel) beschränkt. Deren Kosten sind niedrig und werden über den Vertrag des Kunden erstattet. Mögliche Betrugsverluste sind wahrscheinlich auf Prozessmissbrauch zurückzuführen, wie z.B. die Verwendung einer privaten Set-Top-Box in Geschäftsräumen oder der Versuch, die Verschlüsselung der Box zu knacken, um Kanäle zu empfangen, die nicht abonniert sind.
- Für eine Bank wird jedoch nicht nur die finanzielle Haftung viel größer sein, sondern auch die Art der Betrugsangriffe, denen sie ausgesetzt ist. Es handelt sich hierbei hauptsächlich um Transaktionen, für die die Bank im Betrugsfall allesamt zur Rückerstattung verpflichtet ist, z.B. im Fall, dass der Betrüger nach einem Kontoübernahmeangriff ein Darlehen unter dem Namen des Kunden aufnimmt, oder dessen Kontokorrentkredit nutzt usw.
- Ein Kreditkartenunternehmen kann Unsummen Geld verlieren, wenn es einem betrügerischen Kunden ein beträchtliches Kreditlimit anbietet, das dieser benutzt und nie zurückzahlt.

Basierend auf diesen unterschiedlichen Verlustprofilen könnte ein Versorgungsunternehmen daher deutlich weniger Betrugsprüfungen und Kaufhürden einführen, als eine Bank oder ein Kreditkartenunternehmen.

Best Practice von Nuance

Viele Unternehmen haben ein ungenaues Verständnis ihrer Betrugslandschaft und finden es daher sehr schwierig, betrugsbezogene Entscheidungen auf der Grundlage solider Finanzinformationen zu treffen. Während einige Finanzinstitute beispielsweise jährliche Betrugsverluste in Höhe von vielen Millionen Pfund oder Euro verzeichnen, schätzen andere diese Verluste auf Zehntausende - was bedeutet, dass sie entweder keinen nennenswerten Betrug erlitten haben oder aber aufgetretene Betrugsfälle nicht wahrnahmen.

Selbst Unternehmen, die ihre Betrugslandschaft relativ gut verstehen, stellen fest, dass sie nach der Implementierung einer Lösung wie dem FraudMiner™ von Nuance das volle Ausmaß der Verluste deutlich unterschätzt haben.

Wägen Sie die Vorteile der Offline- und Echtzeit-Betrugserkennung ab

Eine Organisation konnte bereits 6 Wochen nache Einführung der Nuance Security Suite Verluste in Höhe von £ 4,5 Mill. verhindern.

Nachdem Sie Ihre Risikobereitschaft und die Art der Betrugsvorfälle für Ihr Unternehmen verstanden haben, können Sie die Vorteile besser einschätzen, die Sie von einer Offline- und/oder Echtzeit-Betrugserkennung erwarten können.

Offline-Betrugserkennung
Viele Unternehmen berichten, dass sie nach der Einführung einer Offline-Betrugserkennung sehr schnell die Betrugsverluste reduzieren konnten – so hat z.B. eine Organisation in den ersten sechs Wochen nach Einführung der Nuance Security Suite in ihrem Contact Center 4,5 Millionen Pfund Verluste verhindert.

Nehmen wir das Beispiel eines Kreditkartenunternehmens - ein Betrüger, der versucht ein Konto zu übernehmen, fragt nach einer Ersatzkarte, die an eine andere Adresse als die des echten Kontoinhabers geschickt werden soll. Die Ausstellung einer neuen Karte umfasst die Herstellung, den Druck und die Auslieferung der Karte - ein Prozess, der in der Regel mehrere Tage dauern kann. Innerhalb dieser Zeit kann der Angriff erkannt und die neue Karte gelöscht werden, bevor sie versendet wird. Diese Offline-Betrugserkennung kann daher sehr effektiv solche Angriffe stoppen.

Betrugserkennung in Echtzeit
Im Vergleich dazu steht das Beispiel einer Bank, bei der ein Bankkunde Geld von einem Konto auf ein anderes mit einer schnelleren Zahlungsmethode überweisen kann. Ein Betrüger ruft nun im Contact Center der Bank an, um sich Geld von diesem Konto zu überweisen. Ohne Echtzeit-Betrugserkennung kann das betreffende Geld vor dem Ende des Anrufs bereits verloren gehen.

Nuance-Kunden berichten, dass in diesen Situationen das überwiesene Geld in etwa 50% der Fälle wieder eingezogen werden kann (z.B., wenn es an eine andere Bank innerhalb derselben Gruppe überwiesen wurde). Mit der Echtzeit-Betrugserkennung können die anderen 50% der Betrugsfälle, jene die nicht derart zurückgefordert werden können (z.B., weil das Geld in ein anderes Land überwiesen wurde), gestoppt werden.

– Ein wesentlicher Unterschied zwischen Offline- und Echtzeit-Betrugserkennung besteht darin, dass bei der unmittelbaren Prüfung noch während der Anrufdauer die Betrugsbewertung durchgeführt und der Kunde geschützt wird. Im Gegensatz zur Offline-Erkennung, bei der ein Anruf erst nach Abschluss untersucht werden kann, und ein Kunde eventuell fälschlicherweise als Betrüger gekennzeichnet, und somit frustriert oder verärgert wird.
– Bei der Offline-Betrugserkennung wird die gesamte Dauer eines Anrufs überprüft, während bei der Echtzeiterkennung dies bereits während des Identifikations- und Verifizierungsprozesses der Fall sein kann. Es gibt jedoch Situationen, in denen es vorteilhaft sein kann, Betrugswarnungen so spät wie möglich während eines Anrufes auszusprechen, - zum Beispiel dann, wenn der Agent kurz davorsteht, eine Zahlung zu bestätigen - um die maximale Audiomenge, die für die Betrugsbewertung notwendig ist, zu erfassen.

Die Art und Weise, wie Contact Center-Agenten mit Echtzeit-Alarmen umgehen, erfordert ebenfalls eine sorgfältige Voraussicht. Das Besondere an Echtzeit-Alarmen ist, dass es statistisch gesehen immer mehr Fehlalarme als echte Alarme geben wird, da weitaus mehr echte Kunden sich einwählen als Betrüger. Das bedeutet, dass nicht jeder Alarm automatisch als betrügerischer Anruf gewertet werden sollte.

Die Agenten müssen verstehen, wie sie auf solche Warnungen reagieren sollen - z.B. indem sie mehr Sicherheitsfragen stellen oder den Anruf an ein anderes Team weiterleiten. Dieses Verhalten kann je nach Risikoprofil der Organisation oder je nach Anrufabsicht variieren.

– Wenn z.B. jemand anruft, um eine Ersatzbankkarte zu beantragen, und diese Anfrage als eine kritische Transaktion kategorisiert ist, kann die Prüfung auch offline stattfinden. Dafür wird dem Anrufer mitgeteilt, dass die neue Karte innerhalb der nächsten fünf Werktage zugestellt wird, und im Anschluss der Anruf offline nach Betrugsverdachtsfällen untersucht.
– Wenn jedoch jemand versucht, einen großen Geldbetrag auf einen neuen Zahlungsempfänger zu übertragen, und dies als potenzieller Betrug klassifiziert wurde, wäre eine ganz andere Reaktion erforderlich. Der Agent teilt dann dem Anrufer mit, dass die Zahlung innerhalb von zwei Stunden vorbehaltlich der üblichen Betrugsprüfungen erfolgt, und nach Ende des Anrufes wird diese Anfrage zur Offline-Prüfung weitergeleitet.

Best Practice von Nuance

Welche Lösung oder Lösungskombination ist nun die richtige für Sie?

– Wenn Sie die Art der für Sie relevanten Betrugsfälle kennen, können Sie festlegen, ob Ihrem Unternehmen die Authentifizierung mit Sprachbiometrie helfen kann und in welchem Umfang. Sie wissen dann auch, ob Sie eine Echtzeit-Betrugserkennung benötigen oder eine Offline-Prüfung ausreichend wäre.
– Wenn die Analyse Ihrer Betrugslandschaft beispielsweise ergibt, dass Sie 40% des Betrugs mit einer Offline-Lösung stoppen können, ist dies in der Regel die einfachste Lösung, die den geringsten Integrations- und Entwicklungsaufwand erfordert und innerhalb von nur drei Monaten einsatzbereit sein kann. Sie könnten sich auch entscheiden, eine Offline-Lösung zu implementieren, um eine sofortige Betrugsreduzierung zu erreichen, parallel aber damit beginnen, Echtzeit-Erkennung und -Authentifizierung zu prüfen, um die restlichen 60% des Betrugs zu bekämpfen und somit einen strategischen Bereitstellungsplan zu entwickeln.
– Die Echtzeit-Betrugserkennung benötigt andere Verwaltungsmuster und Reaktionen auf Betrugsmeldungen als Offline. Dies ist abhängig von der Art der Transaktion als auch von Ihrem Risikoprofil.

Bei der Eastern Bank gaben

94%

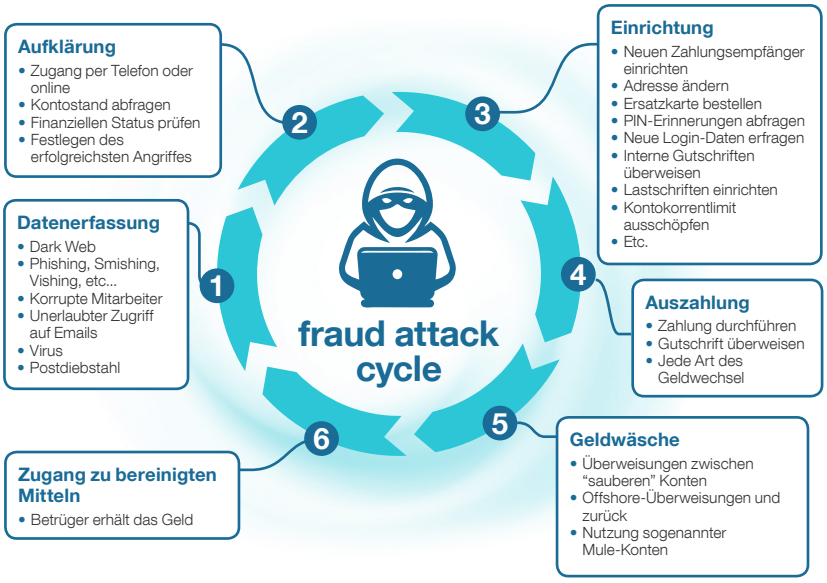
der Agenten an, dass sie durch die Sprachbiometrie leichter qualitativ hochwertige

60%

Dienstleistungen erbringen können, und dass sich ihre Arbeitszufriedenheit dadurch verbessert hat.

Erkennen Sie die Zyklen der Betrugsangriffe

Einer der Gründe für die erfolgreiche und schnelle Betrugserkennung der Nuance Security Suite liegt in der Tatsache begründet, dass Betrüger nicht nur einen einzigen Angriff auf ein Unternehmen durchführen, sondern mehrmals, wobei jeder ihrer Angriffe mehrere Schritte umfasst. Daher können Sie Ihre Betrugsverluste weiter reduzieren, in dem Sie die Zyklen der Betrugsangriffe verstehen: Datenerfassung, Aufklärung, Einrichtung, Auszahlung, Geldwäsche und Zugang zu bereinigten Mitteln.



– Die meisten Unternehmen sind sich bewusst, dass im Hinblick auf die Datenerfassung einige ihrer Daten gehackt und im Dark Web verfügbar gemacht wurden; einige ihrer Kunden werden von außen veranlasst, ihre Daten preiszugeben; betrügerische Mitarbeiter verkaufen Kundendaten; etc.
– Sobald ein Betrüger solche Daten erworben hat, beginnt er in der Regel mit der Aufklärung, d.h. er greift auf das Konto einer Person zu, um Details wie den Kontostand aufzudecken und möglicherweise den Kontoverlauf zu betrachten und den Angriff auf intelligente Weise zu planen.
– Die meisten Unternehmen konzentrieren sich typischerweise auf leicht messbare Ereignisse in der Auszahlungsphase (d.h. den Zeitpunkt, an dem sie Geld verlieren) und vernachlässigen die Auswirkungen von vorgelagerten Aktivitäten wie Aufklärungs- und Aufbauschritte.

Best Practice von Nuance

Während Betrug durch den FraudMiner von der Aufklärungs-, über die Einrichtungs- bis hin zur Auszahlungsphase erkannt wird, kann die Offline-Erkennung nur während der Aufklärung und Einrichtung genutzt werden, reduziert dabei aber die Notwendigkeit für eine Echtzeit-Prüfung zum Auszahlungszeitpunkt. Banken, die sich beispielsweise tendenziell stark auf die Auszahlung konzentrieren, stellen durch FraudMiner fest, dass sie deutlich mehr Aufklärungs- und Einrichtungsanrufe erhalten, als erwartet. Mit dieser Erkenntnis können sie viel früher im Betrugsangriffszyklus reagieren.

– Nach den Erfahrungen einer Großbank befinden sich rund 25% der von FraudMiner generierten Betrugswarnungen in der Pre-Cashing-Out-Phase, d.h. sie können früh erkennen, wenn ein Konto kompromittiert wurde, und mit entsprechend vorbeugenden Maßnahmen (bevor Geld verloren geht) die Betrüger aufhalten.

FraudMiner kann Betrug bereits ab Stufe 2, 3 und 4 erkennen.

Wird Betrug bereits in frühen Stadien wie 2 oder 3 erkannt, kann verhindert werden, dass er bis zur letzten Stufe 4 kommt. Stufe 4 ist der Zeitpunkt, an dem die Echtzeit-Erkennung wichtig wird. Offline-Prüfung, während der Stufen 2 und 3, minimiert den Einsatz von Echtzeit-Prüfung in Stufe 4.

Somit kann Betrug bereits Offline sehr effizient gestoppt werden, bevor er jemals die Auszahlungsphase erreicht hat.

Schritte 5 und 6 finden höchstens dann Einsatz, wenn der Betrug über verschiedene Finanzinstitute stattfindet. Nutzen Banken **AudioShare**, kann die wahre Identität des Betrügers mit **FraudMiner** ermittelt werden.

Immer mehr Betrüger werden durch sprachbiometrische Daten als Beweismittel erfolgreich verfolgt.

– Dies kann einen zusätzlichen Imagevorteil bringen. Die Bank kann ihre Kunden darauf hinweisen, dass ihre Konten und Daten gefährdet sind, und empfehlen den Status aller Konten auch bei anderen Unternehmen zu überprüfen und zu sichern. Somit erscheint sie den Kunden gegenüber als äußerst gewissenhaft.

Auch nach der Auszahlungsphase können Unternehmen, die wahre Identität bekannter Betrüger ermitteln. Mit dem AudioShare Service von Nuance in Kombination mit dem FraudMiner, können Kriminelle, die sich im Prozess der Geldwäsche befinden oder versuchen, auf gereinigte Gelder zuzugreifen, ermittelt, festgenommen und der Strafverfolgung zugeführt werden.

Steigern Sie den Wert von Warnungen und Managementinformationen

Durch die Identifizierung der Stimme eines einzelnen Betrügers auf dem Telefonkanal konnte eine Bank 1.390 Konten identifizieren, die online gefährdet waren. Dies unterstreicht die essenzielle Bedeutung der kontinuierlichen Analyse der durch FraudMiner generierten Warnmeldungen und Managementinformationen (MI).

Durch die Identifizierung der Stimme eines einzelnen Betrügers auf dem Telefonkanal konnte eine Bank 1.390 Konten identifizieren, die online gefährdet waren.

Während ursprünglich der Schwerpunkt der Datenerfassung auf einem besseren Verständnis der Betrugslandschaft lag, wird nach der Implementierung von Offline- und/oder Echtzeit-Betrugserkennung auf MI umgestellt, um sich mit den spezifischen Bedrohungen zu befassen, denen das Unternehmen ausgesetzt ist.

Optimierung des Blacklist-Managements
Um ihre MI umsetzen zu können, führen die meisten Unternehmen eine Vielzahl von Listen, einschließlich:

– Blacklists (auch bekannt als Fraudster Watchlists) - die sich immer auf bekannte Betrüger beziehen. Blacklist-Einträge werden hinzugefügt, sobald sie als “bestätigter Betrug” definiert sind, d.h. die Bank kann diese Person zu einem Anruf zurückverfolgen, bei dem bereits ein Betrugsverlust bestätigt ist.
– Watchlists - ein Begriff, der auch für Blacklists verwendet wird. Hier finden sich Einträge, die auch aus nicht betrügerischen Gründen verwendet werden können, wie z.B. zur Hervorhebung gefährdeter Personen, Kunden, die Probleme mit ihren Konten hatten, oder von Kunden, die wiederholt wegen Betrugs durch die Erstellung von Blacklist-Matches verdächtig sind.
– Whitelists - beziehen sich auf Kunden, die, obwohl sie Betrugsmeldungen auslösen, als vertrauenswürdig bekannt sind.

Da ein sehr hoher Prozentsatz der Betrugsverluste durch eine sehr geringe Anzahl von Betrügern verursacht wird, ist das Blacklist-Management das “Kronjuwel” der Betrugserkennung und ist damit sehr wertvoll.

– Sobald eine Organisation begonnen hat eine Liste bekannter Betrüger zusammenzustellen, wird diese möglichst regelmäßig abgeglichen, indem sie mehr und mehr Daten über jeden Betrüger sammelt.
– Jedes Mal, wenn der Betrüger anruft, wird sein Sprachsignal klarer erkennbar. Dadurch erhält das Unternehmen nicht nur eine bessere Übereinstimmung und einen sicheren echten Alarm, sondern reduziert auch die Wahrscheinlichkeit von Fehlalarmen bei Personen mit ähnlichen Stimmen.

Der Schlüssel zu erfolgreichem Blacklist-Management liegt in der sich verbessernden Abgrenzung von Stimmen der Betrüger von den Stimmen der Nicht-Betrüger, der steigenden Erkennung von Stimmen aller Betrüger und dem Abgleich jeder einzelnen Stimme auf der Blacklist.

– Ganz gleich ob Sie 100 oder 1.000 Einträge in Ihrer Blacklist haben, es wird immer eine bestimmte Anzahl von Fehlalarmen erzeugt, so dass wenn Ihre Blacklist das 10-fache dieser Größe beträgt, Sie wahrscheinlich 10-mal so viele Fehlalarme erhalten. Wenn möglich, sollten Sie also versuchen, die Größe Ihrer Blacklist gering zu halten, um die Anzahl der Fehlalarme zu reduzieren.
– Wenn Sie wirklich von 1.000 Betrügern angegriffen werden, dann sollten alle diese Personen auf Ihrer schwarzen Liste stehen. Aber wenn Ihre MI zeigt, dass von denen 200 im letzten Jahr nicht mehr aktiv waren, sollten Sie diese aus der Liste deaktivieren (aber nicht löschen), da sie sonst nur Fehlalarme auslösen.
– Sie sollten jedoch auch bedenken, dass inaktive Betrüger wieder aktiv werden können. Daher sollten Sie regelmäßig deaktivierte Einträge mit Ihrer Datenbasis abgleichen, um sicherzustellen, dass reaktivierte wieder auf Ihre schwarze Liste gesetzt werden.

Die Analyse der Blacklist-Performance, die Bestimmung, welche Einträge aktiviert bzw. deaktiviert werden, und die Sicherstellung, dass Ihre Blacklist-Inhalte so relevant und leistungsstark wie möglich sind, sind für den Betrieb Ihrer Betrugserkennungslösung von entscheidender Bedeutung. Für die Zufriedenheit Ihrer Kunden ist es auch wichtig, wie Sie mit jenen Kunden umgehen, die fälschlicherweise auf die Blacklist gesetzt wurden, obwohl sie keine kriminellen Verbindung haben.

– Stellen Sie sich folgendes vor: Eine kleine Gruppe Ihrer Kunden hat einen besonders ausgeprägten ethnischen oder regionalen Akzent und Ihre Betrugsbekämpfungslösung hat bereits einen Betrüger (oder eine Betrugsbande) mit dem gleichen Akzent identifiziert. Dann können aufgrund dieser biometrischen Merkmale und der Klassifizierungen im Hintergrund andere völlig unschuldige Mitglieder der Gruppe selbst regelmäßige Betrugsmeldungen auslösen.
– Um dies zu beheben, fügen Sie die Stimmen der echten Kunden ebenfalls zu einer Whitelist hinzu, so dass, wenn diese Stimmen mit der Blacklist und der Whitelist übereinstimmen, kein Alarm ausgelöst wird.

Analyse Ihrer Daten und Priorisierung von Warnmeldungen
Das Team, das für die Bearbeitung und Pflege der Blacklist und die Verwaltung Ihrer Betrugsbekämpfungslösung betraut ist, muss auch für die Datenanalyse und Benachrichtigung verantwortlich sein. Ihr Team muss entsprechend strukturiert werden, damit eine Gruppe Ihre Blacklist verwaltet, eine andere mit Ihrer MI arbeitet und von ihr lernt und eine dritte Gruppe Warnmeldungen priorisiert.

Die MI-Analyse umfasst die Auswertung von Warnmeldungen, Betrugs- und Sprachabdrücken, Grenzwerten und die Extrapolation über Metadaten auf andere Kanäle. Es werden zunächst all jene Warnmeldungen priorisiert, die einem Betrug am nächsten kommen, danach erfolgt die Einstufung nach Punktzahl, Identität der Anrufleitung (CLI), Branche usw.

– Unternehmen, die FraudMiner nutzen, berichten, dass die Daten, die sie von der Lösung erhalten, betrugsrelevanter sind als ihre anderen Warnmechanismen, und sie dadurch mehr Betrüger identifizieren können. Somit sollten Personen, die mit anderen Alarmsystemen arbeiten, fortan auch FraudMiner nutzen, um Alarme produktiver zu untersuchen.
– Unternehmen werden auch feststellen, dass aufgrund von FraudMiner die Anzahl der aufgedeckten Warnungen und Betrüger im Laufe der Zeit abnehmen kann. Da das Unternehmen kein einfaches Ziel mehr ist, verlaufen Betrugsversuche weniger erfolgreich und Betrüger wenden sich dann ab. Die Anzahl der Personen, die zur Untersuchung dieser Warnmeldungen erforderlich sind, kann sich daher im Laufe der Zeit ändern.

– Wie effektiv das Team arbeitet, wird durch die MI-Bewertungen, die Betrachtung der Betrugsvorfallraten und die Analyse des Betrügerverhaltens ersichtlich. Das bedeutet, dass im Idealfall das gesamte Team harmonisch zusammenarbeitet – bei der Verwaltung der Blacklist und der Bearbeitung der Benachrichtigungen basierend auf den Managementinformationen.

Erfassung umfangreicher Metadaten
Die Erfassung so vieler Metadaten wie möglich während der Entwicklung und dem Aufbau der Lösung zum Schutz vor Betrug, befähigt das Team eine sehr detaillierte Aussage über die Betrugslandschaft treffen zu können.

Umfangreiche Metadaten können auch verwendet werden, um Filter auf Anrufe anzuwenden wie z.B. Rückverfolgung oder Clustering, Einblicke in das Verhalten von Betrügern zu gewinnen, Prozessschwächen zu identifizieren und den Abruf von Originalanrufen zu vereinfachen. Folgend sind nur einige Beispiele genannt:

– Viele Unternehmen verwenden verschiedene Telefonnummern, über die Kunden mit ihnen Kontakt aufnehmen können. So kann beispielsweise eine Bank unterschiedliche Telefonnummern anbieten für Kunden, die bzgl. Hypotheken, Kreditkarten, Business Banking usw. anrufen. Diese Informationen machen es möglich Kontaktwege zu identifizieren, die anfälliger für Betrugsangriffe sind und somit eine Prozessanfälligkeit aufweisen, die von Betrügern ausgenutzt wird.
– Eine Bank richtete eine dedizierte Telefonnummer ein, über die Betrugsverdacht gemeldet werden kann. Hierüber stellten sie fest, dass Betrüger ihr Betrugsteam angriffen - die Anzahl der Sicherheitsprüfungen, die das Team durchführte, war geringer als die der anderen Teams. Betrüger konnten hierüber anrufen und vorgeben sie hätten eine Sprachnachricht erhalten, die sie darüber informierte, dass angeblich eine betrügerische Zahlung auf der Kreditkarte verzeichnet worden sei, aber tatsächlich keine echte Zahlung vorlag. Trotzdem keine Aufzeichnung von der vermeintlichen Sprachnachricht vorlag, der Betrüger aber die Sicherheitskontrolle bestanden hatte, ging das Betrugsteam davon aus, dass der Agent es versäumt hatte eine Notiz des Anrufs zu erstellen. Sie klassifizierten daher das Konto als betrugsgefährdet und ermöglichten es dem Betrüger so, ein neues Konto zu eröffnen.
– Eine andere Bank entdeckte einen Prozessschaden, der durch ihr Inkasso-Team entstand. Das Team konzentrierte sich auf den Einzug verspäteter Zahlungen, und beachtete dabei nicht die Geldquelle. Betrüger nutzten nun eine Karte der Bank, um das Kreditlimit vollends auszuschöpfen, zahlten den Betrag aber nie zurück. Daraufhin rief das Inkasso-Team bei ihnen an. Die Regel, dass Kunden das Defizit einer Kreditkarte nicht mit einer anderen ausgleichen können, wurde nicht befolgt. Betrüger waren daher in der Lage, ihre Schulden mit einer weiteren betrügerisch erhaltenen Karte zu begleichen, und verlängerten so die Einsatzdauer beider Karten.

Passen Sie Ihren Schutz an die sich ständig ändernden Betrugsvorgehen an

Die Nuance Security Suite bietet kanalübergreifende Sicherheit und Betrugsprävention über digitale, telefonische und Selbstbedienungskanäle hinweg; mit Lösungen zur sprachbiometrischen Authentifizierung und zur Betrugsbekämpfung, die die Betrugsanfälligkeit von Unternehmen verringern und Betrüger stoppen.

Es gibt jedoch keine Möglichkeit, Betrüger wirksam in allen Situationen zu erkennen. Daher erfordert erfolgreiche Betrugsprävention, wie z.B. in der Authentifizierung, einen mehrschichtigen Ansatz. Mit Hilfe von KI können Betrugsmuster und Betrüger besser erkannt werden.

Da Verbraucher und Unternehmen zunehmend Biometrie für Authentifizierungszwecke einsetzen, werden Betrüger unweigerlich versuchen, die jeweilige Biometrie zu umgehen. Nuance entwickelt daher eine Reihe von Technologien, um diese Angriffe abzuschwächen und zu verhindern.

- Um Betrüger zu identifizieren, die Spoofing-Mechanismen einsetzen, um Aufzeichnungen, Sprachbiometrie, Bilder oder Videos zur Gesichtserkennung, etc. zu manipulieren, entwickelt Nuance technisch ausgereifte Anti-Spoofing-Algorithmen in Bereichen wie Kanalwiedergabe, Footprint-Wiedergabe, synthetische Sprach-, Bild- und Videoerkennung sowie ANI-Spoofing-Erkennung.
- Um die Leistung der Sprachbiometrie und der textbasierten Kommunikation zu verbessern, fügt Nuance ConversationPrint™ eine Verhaltensbiometrie hinzu, die auf dem Wortschatz, der Grammatik und der Satzstruktur eines Anrufers basiert, einschließlich Skripte. Dies kann verwendet werden, um Einzelpersonen oder Betrugsbanden anhand ihrer Sprachmuster und Gewohnheiten zu identifizieren, um eine weitere Authentifizierungsschicht bereitzustellen, die andere Biometrien ergänzt, um neue Betrüger zu erkennen und falsche Betrugsmeldungen zu reduzieren.
- Mit der Nuance Channel ID kann zusätzlich zum Sprachabdruck der Telefontyp eines Anrufers erkannt werden. Mit der GeoID werden das Land und die Stadt identifiziert, in denen das Gerät jeweils im Telefonnetz verzeichnet ist. Nuance Device Print prüft ob das aktuelle Gerät dem entspricht, das in der Vergangenheit vom rechtmäßigen Kontoinhaber verwendet wurde. Alle über diese Tools gesammelten Daten, ergänzen die Metadaten bestimmter Personen, komplettieren die Authentifizierung und helfen bei der Risikobewertung.
- Die Verhaltensbiometrie verfolgt die Interaktion eines Kunden oder einer Person mit seinem Gerät, bewertet und analysiert die Daten, um sie hierüber zusätzlich zu identifizieren.
- All diese Informationen können in eine KI-Engine eingegeben werden, um die Ergebnisse ganzheitlich zu überprüfen, verschiedene Datenpunkte zu gewichten und zu bewerten, die Verhaltensbiometrie und die Kontextfaktoren zu verstehen und einen einheitlichen Authentifizierungswert und Betrugswert pro Interaktion zu erzeugen.

Zusammenfassend lässt sich sagen, dass Verhaltensabdrucke von legitimen Kunden erstellt und als Berechtigungsnachweis oder Ersatz für PINs oder Passwörter verwendet können; aber auch von Betrügern. Sie helfen somit bekannte Betrugsversuche und -profile zu erkennen und zu verhindern, dass Betrüger die Kanäle der Kundenbetreuung manipulieren.

Um mehr darüber zu erfahren, was Nuance-Lösungen zur Betrugsprävention für Ihr Unternehmen leisten können, wenden Sie sich bitte an Sylvia Lohr.

Über Nuance Communications, Inc.
Nuance Communications erfindet das Verhältnis zwischen Mensch und Technik neu. Durch seine Stimm- und Sprachangebote schafft das Unternehmen eine menschlichere Konversation über Systeme, Geräte, Elektronik, Anwendungen und Dienstleistungen hinweg. Jeden Tag nutzen Millionen von Menschen und Tausende von Unternehmen intelligente Systeme von Nuance, die zuhören, verstehen, lernen und sich an ihr Leben und ihre Arbeit anpassen können. Für weitere Informationen besuchen Sie bitte nuance.com.

NUANCE

NUAN-CS-3632-01-WP-GER, 15 Mai 2019