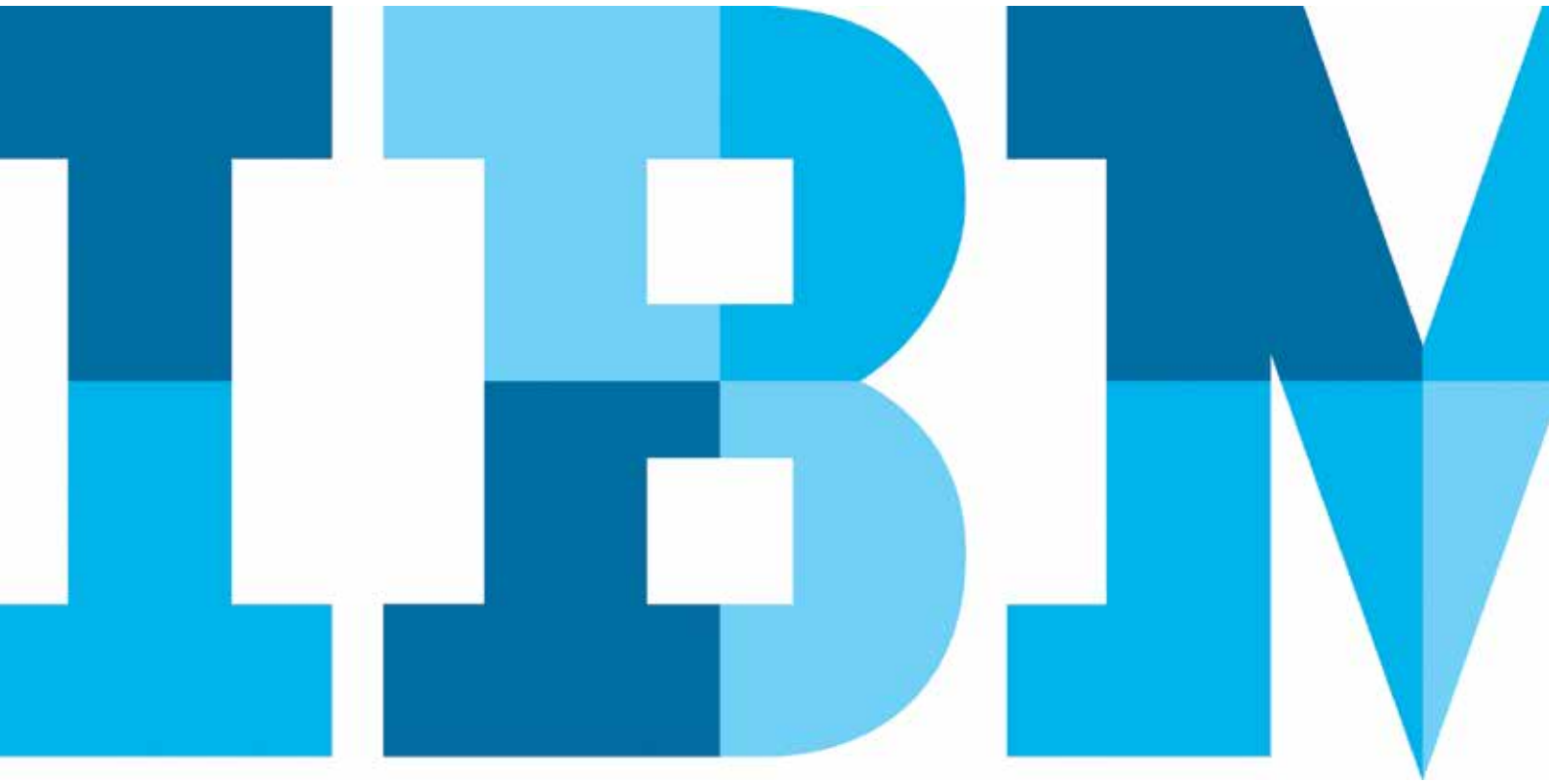
Sicherheit

White Paper

Versicherungswirtschaft

Ein nahtloses digitales Erlebnis für Versicherungskunden

Mit IBM Trusteer können Versicherungsunternehmen Risiken im Zusammenhang mit digitalen Identitäten transparent bewerten



IBM

Inhalt

Einführung

Früher kamen Versicherungsunternehmen mit Kunden hauptsächlich über ihre Versicherungsexperten (auch als Versicherungsvertreter bekannt) in Kontakt. Versicherungsexperten spielen in der Zusammenarbeit mit dem Kunden zwar nach wie vor eine wichtige Rolle, aber Versicherungen nutzen inzwischen – wie viele andere Branchen auch – zunehmend kostengünstige digitale Kanäle, um externe Benutzer besser ansprechen zu können und neue Märkte zu erschließen.

In den letzten Jahren haben Versicherungen digitale Anwendungen eingeführt, mit denen die Verbraucher über ihr Mobiltelefon oder ihr Desktopsystem Angaben in einer Versicherungspolice überprüfen, Leistungen überprüfen, Kosten vergleichen, Rechnungen bezahlen, Schadensfälle melden und sogar Versicherungsschutz beantragen können. Diese Transformationsmaßnahmen verringern die Kosten für den Kundenservice und schaffen gleichzeitig neue Möglichkeiten, um engeren Kontakt mit dem Kunden aufzubauen und die Markentreue zu stärken.

Im Zuge der digitalen Transformation bemühen sich die Versicherungen um eine Ausweitung des Vertriebs mit neuen Versicherungsprodukten speziell für den digitalen Kanal – diese werden mithilfe von APIs (Application Programming Interfaces) entweder direkt auf ihren Websites oder über Partner bereitgestellt.

Die Versicherungen haben zudem in die Optimierung von Prozessen und Serviceleistungen mit Drittanbietern investiert, die Dienstleistungen zur Schadensregulierung erbringen (z. B. Ärzte, Unternehmen für Haushaltsreparaturen, Unternehmen für die Reparatur von Windschutzscheiben an Fahrzeugen). Dadurch können Versicherungen ihren Kunden Dienstleistungen zur Schadensregulierung anbieten und mehr Anbieter für eine Zusammenarbeit mit dem Unternehmen gewinnen.

Für Verbraucher, Anbieter und Versicherungsexperten kann die Schaffung eines nahtlosen digitalen Erlebnisses aber eine echte Herausforderung darstellen.

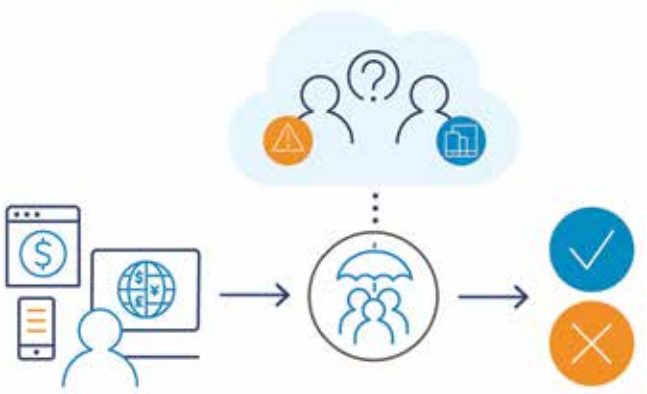
Verbraucher, Anbieter und Versicherungsexperten erwarten heutzutage Komfort – sowohl in Bezug auf eine einfache Nutzung digitaler Services als auch auf die Möglichkeit, jederzeit und von überall aus Serviceleistungen zu erhalten. Wenn hierfür mehrere Schritte erforderlich sind (entweder zu viele Schritte für die Authentifizierung oder zu viele Formulare, die über einen Versicherungsexperten oder digital eingereicht werden müssen), kann dies von den Benutzern als lästig empfunden werden. Solch komplexe Prozesse können das digitale Erlebnis des Benutzers beeinträchtigen und letztendlich zu einer hohen Abbruchrate führen. Verbraucher, Anbieter und Versicherungsexperten wenden sich dann entweder teureren Kanälen zu (z. B. dem Call-Center) oder an eine andere Versicherung.

Im digitalen Zeitalter von heute haben die Verbraucher die Möglichkeit, auf Knopfdruck Preise und Angebote miteinander zu vergleichen und sogar zu bestimmen, wie und wann sie mit der Versicherung Geschäfte abwickeln möchten. Der Ruf eines schlechten Kundenservices oder eines geringen Sicherheitsniveaus kann in dieser hart umkämpften Branche erhebliche Auswirkungen haben. Ein kompromittierter digitaler Account eines Anbieters oder Versicherungsexperten kann für die Versicherung ein hohes Risiko darstellen, da ein Schadenskonto verwendet werden kann, um zahlreiche Schadensfälle einzureichen oder kostengünstige Policen zu generieren.

Die Frage ist also: Wie können Sie Vertrauen über digitale Kanäle aufbauen, um neue und bestehende Kunden sowie Anbieter und Versicherungsexperten nahtlos anzusprechen, und gleichzeitig böswillige Benutzer fernhalten?

Die Antwort liegt darin, wie Sie das Risiko digitaler Identitäten bewerten.

Um echte Benutzer in digitalen Kanälen transparent identifizieren und potenzielle böswillige Akteure genauer erkennen zu können, sind Versicherungen auf eine aussagekräftige Bewertung der Risiken bei digitalen Identitäten angewiesen. Sie können so den digitalen Fußabdruck jedes Benutzers anhand verschiedener sensorischer Eingaben von Systemen untersuchen.



Wie können Sie nahtlos auf Kunden eingehen und böswillige Benutzer fernhalten?

Der geschäftliche Nutzen aussagekräftiger Risikobewertungen

Im Folgenden sind vier potenzielle Vorteile einer aussagekräftigen Risikobewertung zu Beginn jeder digitalen Interaktion aufgeführt (unabhängig davon, ob es sich um einen neuen Kunden handelt, der eine Police beantragt, einen bestehenden Kunden, der den digitalen Kanal anstelle eines herkömmlichen Kanals nutzt, oder einen Anbieter, der sich anmeldet, um neue Versicherungsansprüche einzureichen).

Ein vollkommen nahtloses Benutzererlebnis

Erstens kann eine aussagekräftige Risikobewertung digitaler Identitäten dazu beitragen, dass Sie bestehenden Benutzern bei jeder Anmeldung bei ihrem Account ein nahtloses Erlebnis bieten können. Durch eine kontinuierliche, risikobasierte Authentifizierung anstelle mehrerer Authentifizierungsprotokolle bei jeder Anmeldung erhalten Sie Einblicke, die es Ihnen ermöglichen, nur Benutzer mit einem hohen Risiko für böswillige Absichten anzusprechen. Darüber hinaus können Sie mithilfe einer kontinuierlichen Authentifizierung Benutzer immer dann bewerten, wenn diese einen äußerst sensiblen Vorgang durchführen. Dadurch müssen Vertrauenswürdigkeit und Risiken nur bei Bedarf überprüft werden. Versicherungen, die ein schlechtes digitales Erlebnis mit zusätzlichen Verzögerungen bei der Authentifizierung bieten, müssen letztendlich möglicherweise in Kauf nehmen, dass die Benutzer keine digitalen Services mehr in Anspruch nehmen, zu Wettbewerbern abwandern oder kostenintensivere Kanäle nutzen.

Ein nahtloses Erlebnis kann Versicherungen auch helfen, die Kundenbindung zu stärken. Bestehende Kunden nutzen digitale Kanäle häufig nach einem belastenden Ereignis, z. B. einem Autounfall, einer Krankheit oder dem Tod eines geliebten Menschen. Einige dieser Kunden melden sich möglicherweise nicht regelmäßig bei ihren Benutzerkonten an und müssen daher eher komplexe Authentifizierungen in Kauf nehmen oder vergessene Kennwörter erneut anfordern. Durch eine Vereinfachung des Prozesses können Versicherungen unter Beweis stellen, dass sie Kunden bei der Bewältigung schwieriger Situationen unterstützen, und diese Momente wiederum als Chance zur Stärkung der Markenbindung nutzen. Für einen Anbieter oder Versicherungsexperten kann jede Minute, die er mit der Authentifizierung verbringt, entgangene Umsätze bedeuten, weil er sich nicht um zusätzliche Ansprüche kümmern konnte. Die Verringerung von Problemen bei der Authentifizierung ohne Einbußen bei der Sicherheit kann dazu beitragen, die Kundenbindung und die bevorzugte Geschäftsbeziehung mit der Versicherung zu bewahren.

Kunden gewinnen und an das Unternehmen binden

Zweitens kann es den Versicherungen dabei helfen, Kunden zu gewinnen und an das Unternehmen zu binden. Übermäßig hohe Anforderungen bei der Authentifizierung sind ein erhebliches Hindernis für Verbraucher, die in der Lage sein möchten, jederzeit und überall einen neuen Versicherungsschutz zu erwerben. Wenn es für die Verbraucher zu schwierig ist, ihre Identität nachzuweisen, wenden sie sich anderen Versicherungen zu, die das gewünschte reibungslose Erlebnis bieten.

Kundendaten schützen

Drittens kann es Initiativen zu Risiken und Richtlinien zum Schutz von Kundendaten voranbringen. Cyberkriminelle haben viele Möglichkeiten entwickelt, um Authentifizierungsprozesse zu umgehen, einschließlich der Zwei-Faktor-Authentifizierung, und sich als Benutzer auszugeben. Über einen kompromittierten Account eines Versicherungsexperten oder Anbieters werden böswilligen Benutzern möglicherweise umfangreiche Kundendaten offengelegt. Aussagekräftige Risikobewertungen digitaler Identitäten mit passiver Authentifizierung können dabei helfen, versteckte Muster aufzudecken, die darauf hindeuten, dass

der Benutzer, der sich gerade anmeldet, kein rechtmäßiger Kunde, Anbieter oder Versicherungsexperte ist, sondern ein böswilliger Akteur, der sich die Zugangsdaten des Benutzers verschafft hat.

Betriebliche Auswirkungen verringern

Und schließlich können aussagekräftige Risikobewertungen digitaler Identitäten dazu beitragen, die betrieblichen Auswirkungen böswilliger Aktionen zu verringern. Wenn böswillige Akteure bereits zu Beginn einer digitalen Interaktion gestoppt werden, können Versicherungen die Kosten für manuelle Untersuchungen und Bearbeitungen verringern und vermeiden, Ablehnungsschreiben versenden oder hohe Kosten für die Datenschutzverletzung in Kauf nehmen zu müssen. Herkömmliche Tools mit veralteten Technologien erfordern oft zu viele laufende Bedienereingriffe. Mit Strategien auf der Basis adaptiver Intelligenz lassen sich mehr Funktionen für die Automatisierung nutzen und die Abhängigkeit von Bedienereingriffen verringern. Außerdem können sie dazu beitragen, die Genauigkeit in größerem Umfang zu erhöhen und gleichzeitig Risiken durch Betrugsfälle und die Betriebskosten zu verringern.

Überlegungen zur Bewertung digitaler Identitäten

Eine der Herausforderungen bei der effektiven Bewertung digitaler Identitäten besteht darin, dass Versicherungen im digitalen Umfeld viele sich weiterentwickelnde Sicherheitsbedrohungen bekämpfen müssen.

Verschiedene böswillige Akteure begehen verschiedene Arten von Straftaten in verschiedenen Phasen der Benutzerinteraktion – vom Kauf einer Versicherung über das Einreichen von Ansprüchen bis hin zum Kundenservice. Sie verfolgen u. a. folgende Strategien:

- Erstellen von gefälschten oder synthetischen Identitäten (Identitäten, die gestohlene Daten enthalten oder echte Identitäten um falsche Daten ergänzen) für Betrugsfälle mit Dritt- und Erstanbietern
- Verwenden echter, aber gestohlener Identitäten – ein immer größeres Problem angesichts des Umfangs von Benutzerinformationen wie Name, Adresse, Geburtsdatum, zweiter Vorname und Sozialversicherungsnummer, die durch Datenschutzverletzungen kompromittiert wurden
- Auftreten als bestehender Kunde, Anbieter oder Versicherungsexperte, um Ansprüche zu stellen, Zahlungen zu erhalten, Darlehen anhand einer Versicherungspolice aufzulösen oder aufzunehmen oder einfach Kundendaten zu stehlen
- Wiederholtes Abschließen einer Versicherung bei verschiedenen Versicherungen, nur um einen Anspruch einzureichen und eine Zahlung zu erhalten

Je mehr Daten Sie daher in Ihre Risikobewertungen einfließen lassen können, desto genauer werden die Warnhinweise. Eine größere Genauigkeit kann dazu beitragen, dass die zur Bekämpfung von Betrugsfällen zuständigen Mitarbeiter weniger falsch positive Warnhinweise erhalten und dass die Betriebskosten sinken.

Daher sollten Versicherungen bei der Beurteilung der Rechtmäßigkeit jedes einzelnen Nutzers eine Vielzahl von Daten berücksichtigen. Dazu gehören:

- Geräteauthentifizierung und Spoofing-Nachweise zur Verbesserung der Zuverlässigkeit von Geräte-Fingerabdrücken. Geräte-Fingerabdrücke und die Zuordnung der Geräte zu Benutzern können die Authentifizierung transparenter gestalten. Da der Fingerabdruck von Geräten jedoch von böswilligen Benutzern gefälscht wird, sollte seine Verwendung überprüft werden, um die Zuverlässigkeit zu gewährleisten.
- Verbindungs- und Netzwerkmerkmale, um festzustellen, woher und wann sich die Benutzer verbinden und welche Arten von Verbindungen (Web, mobil, Virtual Private Network (VPN) usw.) und Verschlüsselung sie verwenden.
- Verhaltensbezogene und biometrische Erkenntnisse zur Ermittlung von Verhaltensmustern der Benutzer, z. B. Muster bei Mausbewegungen und Eingabefrequenz, und zur Identifizierung von Unregelmäßigkeiten.
- Analyse des Benutzerprozesses, um zu erfahren, wie ein Benutzer in der Anwendung navigiert, und Unregelmäßigkeiten in seinem Verhalten zu ermitteln.
- Informationen von Mobilfunkbetreibern, um zusätzliche Erkenntnisse über potenzielle Risiken durch den Benutzer zu erhalten. Beispielsweise wird ein Benutzer mit einem modernen, zwei Tage alten Mobiltelefon als ein höheres Risiko angesehen als ein Benutzer mit einem drei Jahre alten Account. Ein Mobiltelefon, das bei einem Netzbetreiber registriert ist, von dem bekannt ist, dass er von Betrügern aufgrund schlechter Sicherheitsvorkehrungen ausgenutzt wird, gilt als ein höheres Risiko als ein Mobiltelefon, das bei einem etablierten Netzbetreiber registriert ist.
- Böswillige Muster, sowohl auf individueller Ebene als auch unternehmensübergreifend, um Versuche zu erkennen, Authentifizierungsmaßnahmen zu manipulieren oder zu umgehen, und um zu erkennen, wann bekannte Angriffstools wie Remote Access Trojaner (RATs) oder Malware verwendet werden. Diese Erkenntnisse können helfen, Social-Engineering-Angriffe zu identifizieren, die bei digitalen Interaktionen nur einen sehr kleinen Fußabdruck haben können.

- Gesammelte Daten zu böswilligen Benutzern aus einem weltweiten Netzwerk, um bekannte böswillige Akteure zu erkennen, die andere Unternehmen angreifen.

Ohne dieses breite Spektrum an Daten ist es möglicherweise viel schwieriger zu bestätigen, dass ein Benutzer tatsächlich vertrauenswürdig ist.

Vertrauen in allen digitalen Kanälen aufbauen

Die Chancen sind groß: Wenn Sie rechtmäßige Aktivitäten genauer bestätigen und potenziell böswillige Aktivitäten identifizieren können, sind Sie eher in der Lage, Benutzern das von ihnen erwartete nahtlose Erlebnis zu bieten.

IBM® Trusteer hilft Versicherungen dabei, von Anfang an eine vertrauensvolle digitale Beziehung zu Benutzern aufzubauen. Es kombiniert umfassende Informationen über das Verhalten von Benutzern, Sitzungen und Geräten mit kognitiven Echtzeitanalysen, um die Rechtmäßigkeit jeder digitalen Aktivität transparent zu bestimmen und eine kontinuierliche, risikobasierte Authentifizierung zu fördern.

IBM Trusteer kann Versicherungsunternehmen dabei helfen, Vertrauen über digitale Kanäle aufzubauen, indem es umfassende proprietäre Erkenntnisse mit globalen Informationsquellen korreliert.

Um dies zu erreichen, verwendet die Trusteer-Lösung einen Ansatz nach dem Motto „Vertrauen ist gut, Kontrolle ist besser“ und arbeitet im Hintergrund, um Hinweise auf digitale Aktivitäten aufzudecken, die auf böswillige Benutzer hindeuten.

Benutzerinformationen im Hintergrund überprüfen

IBM Trusteer integriert dank eines globalen weltweiten Netzwerks eine Vielzahl von Daten in die Risikobewertung, um Benutzerinformationen zu überprüfen. Zu diesen Daten gehören:

- Informationen von Mobilfunkbetreibern, um festzustellen, ob die angegebene Telefonnummer darauf hinweist, dass der Benutzer nicht vertrauenswürdig ist.
- Geräteinformationen, um festzustellen, ob das verwendete Gerät nicht vertrauenswürdig ist – durch Malware beeinträchtigt, von böswilligen Benutzern gefälscht oder in der Vergangenheit von einem böswilligen Benutzer bei einem anderen böswilligen Versuch verwendet wurde.
- Netzwerk- und Sitzungsinformationen, um eine fehlende Übereinstimmung in den Standortinformationen zu erkennen oder auf spezielle Methoden zu verweisen, die von Cyberkriminellen verwendet werden, z. B. Ort der Ausbeutung oder spezielle Tools und Browsing-Muster.
- Verhaltensbezogene biometrische Daten, die passiv das Verhalten des Nutzers während des gesamten Prozesses identifizieren, um echte Benutzer nahtlos von böswilligen unterscheiden zu können. Bei neuen Kunden können mit verhaltensbezogenen biometrischen Daten böswillige BOT-Angriffe oder bekannte Nutzungsmuster böswilliger Akteure erkannt werden, die auf einen Diebstahl von Identitäten abzielen. Bei bestehenden Kunden kann mit verhaltensbezogenen biometrischen Daten das Nutzungsverhalten des Kunden erlernt werden. So können Benutzer kontinuierlich und transparent überprüft werden, wenn sie auf die Website zugreifen, um Angaben zu Versicherungspolicen zu überprüfen, Ansprüche zu verwalten oder Änderungen am Account anzufordern.
- Proprietäre Informationen, die in der globalen Nachweisdatenbank von IBM Trusteer verwaltet werden. Zu diesen Informationen gehören Erkenntnisse über bereits identifizierte Nachweise und bekannte Nachweise über böswillige Akteure wie E-Mail-Adressen, Telefonnummern, Geräteelemente, Verbrecherorganisationen und Konten für Drogenschäfte – alles basierend auf Sicherheitsinformationen aus Hunderten von Unternehmen weltweit.

Muster erkennen, die auf böswillige Absichten hindeuten

Böswillige Benutzer zeigen häufig ein anderes Verhalten als rechtmäßige Benutzer. Solche Verhaltensweisen sind oft eher hintergründig, z. B. die Vorgehensweise beim Eingeben von Informationen in einen Antrag oder die Geschwindigkeit beim Ausfüllen eines Formulars. Infolgedessen identifiziert und integriert IBM Trusteer auch böswillige Muster in die Risikobewertung, indem eine Vielzahl von Datenelementen zu Geräte-, Sitzungs- und Nutzungsmustern mit Funktionen für maschinelles Lernen analysiert werden. Einige der analysierten Datenelemente sind folgende:

- Erkenntnisse über die Vorgehensweise des Benutzers, z. B. wie lange er sich auf einer Seite aufhält, wie das Formular ausgefüllt wird, wie schnell er tippt und wie sich der Gesamtablauf darstellt – ob dies zum Verhalten des wahren Benutzers passt oder aufgrund der Eingaben den Anschein erweckt, dass etwas nicht stimmt.
- Identifizieren von Verknüpfungen. Wurden die Daten zur Beantragung einer neuen Versicherungspolice oder zur Eröffnung eines neuen Accounts in einem anderen Antrag oder zuvor bei einem anderen Unternehmen verwendet?
- Einblicke in Aktivitäten neuer Kunden. Gibt es Aktivitäten im Zusammenhang mit böswilligen Mustern, die nach der Account-Einrichtung auftreten und darauf hindeuten, dass der Account von böswilligen Benutzern eingerichtet wurde?

Unternehmensübergreifende intelligente Funktionen nutzen

Böswillige Akteure verwenden oft dieselbe Vorgehensweise oder dieselben gestohlenen oder synthetischen Identitätselemente in verschiedenen Unternehmen. IBM Trusteer-Lösungen analysieren daher auch böswillige Muster bei anderen Anbietern weltweit, die bei der Sicherheit auf IBM Trusteer-Lösungen setzen. Mit diesen globalen unternehmensübergreifenden Informationen kann IBM Trusteer Unternehmen dabei helfen zu erkennen, ob:

- die Identität, die einen Antrag auf Versicherungsschutz stellt, bereits versucht hat, ein oder mehrere Konten mit einer Geschwindigkeit und Rate zu eröffnen, die bekannten böswilligen Mustern bei anderen Anbietern ähneln, die bei der Sicherheit auf IBM Trusteer-Lösungen setzen.
- das Gerät oder dieselben Identitätselemente die Eröffnung mehrerer Konten im Namen verschiedener Benutzer anfordert.
- dieselbe Telefonnummer, E-Mail-Adresse oder Adresse in mehreren Anträgen für verschiedene Personen verwendet wird.

Dauerhafte Agilität dank adaptiver Intelligenz

Welche Strategien wenden böswillige Akteure in Zukunft an? Um Versicherungen in einem sich ständig verändernden Umfeld den größtmöglichen Vorteil zu verschaffen, setzt IBM Trusteer sowohl fortschrittliche Technologien als auch außergewöhnliche Sicherheitsexperten ein, um die täglichen Veränderungen bei Sicherheitsbedrohungen nachzuverfolgen.

Die Trusteer-Sicherheitsinfrastruktur integriert ständig neue Informationen mit Hilfe von:

- Funktionen für maschinelles Lernen, einschließlich verschiedener Ebenen kognitiver Betrugserkennung und -analyse, um das Risiko böswilliger Versuche bei digitalen Aktivitäten zu verstehen, zu erkennen und vorherzusagen.
- Globale Echtzeitinformationen über Sicherheitsbedrohungen und globale Erkenntnisse aus der Cloud.
- Neu aufkommende Muster, die von IBM X-Force, einem der erfahrensten Teams in der kommerziellen Sicherheitsforschung der Welt, verfolgt werden.

Diese kontinuierliche Erweiterung der Daten bietet eine neue Dimension von Einblicken und macht die Plattform wirklich vielseitig. Es kann Versicherungen dabei helfen, das Risiko böswilliger Versuche schnell zu verstehen, zu erkennen und vorherzusagen, sich vor neuen Strategien von Cyberkriminellen zu schützen, die Genauigkeit von Bewertungen zu erhöhen und die Betriebskosten zu senken – und dabei werden gleichzeitig die Grundlagen für ein nahtloses Kundenerlebnis geschaffen.

Festlegung eigener Richtlinien mit der erweiterten Intelligenz in IBM Trusteer

Versicherungen müssen sich oft mit einer Vielzahl von globalen und lokalen Geschäftsanforderungen auseinandersetzen, abhängig von den festgestellten Nutzungsmustern und der Risikosensitivität jedes Unternehmens.

Daher sind viele Unternehmen daran interessiert, die Modelle zu kontrollieren, die sie bei der Bewertung potenzieller Risiken verwenden. Der IBM Trusteer Policy Manager liefert Unternehmen Einblicke in Modelle, die Fähigkeit zur Anpassung von Modellen und die Flexibilität, um die Wirksamkeit neuer Gegenmaßnahmen schnell zu überprüfen und anzuwenden. Sie können damit neue Account-Richtlinien festlegen, die internen und externen Anforderungen und Vorschriften gerecht werden.

Der Policy Manager nutzt maschinelles Lernen, um Wissen über aktuelle und neue Sicherheitsbedrohungen und Trends aufzubauen, denen Unternehmen gegenüberstehen. Er bietet die Möglichkeit, neue Richtlinien anzupassen, Regeln zu simulieren und Risikomodelle automatisch oder basierend auf bestimmten Informationen und Erkenntnissen anzupassen – ohne dass hierfür Vorkenntnisse oder besonderes Fachwissen benötigt werden.

Fazit

Die digitale Transformation schafft neue Möglichkeiten für Versicherungen, um sowohl die Zusammenarbeit mit bestehenden Kunden, Anbietern und Versicherungsexperten zu verbessern als auch neue Kunden und Anbieter durch innovative Produkte und Services zu gewinnen. Im digitalen Zeitalter erwarten Verbraucher, Anbieter und Versicherungsexperten die Möglichkeit, Informationen, Ansprüche und Versicherungsschutz bei Bedarf zu erhalten oder zu ändern.

Der geschäftliche Erfolg von Versicherungen kann in den kommenden Jahren daher ebenso davon abhängen, wie einfach es für die Benutzer ist, ihre digitalen Kanäle zu nutzen, wie die digitalen Produkte und Services, die sie anbieten. Noch wichtiger aber ist, dass Lösungen wie Trusteer Versicherungsunternehmen, die ihr Angebot erweitern und vielfältiger gestalten möchten, dynamische Funktionen bieten, mit denen sie direkt das nächste Projekt angehen können.

Die Komplexität von Anwendungen oder Prozessen, z. B. Probleme durch mehrere Authentifizierungen, kann Benutzer frustrieren. Dies wirkt sich dann nachteilig auf die Zufriedenheit der Benutzer aus und führt möglicherweise dazu, dass sie sich anstelle dieses digitalen Kanals für einen kostenintensiveren Kanal oder das Angebot eines Wettbewerbers entscheiden. Umgekehrt kann ein nahtloses digitales Erlebnis Versicherungen dabei helfen, die Markentreue und den Ruf des Unternehmens auf dem Markt für seinen Kundenservice aufzubauen oder zu verbessern.

Durch den Aufbau einer vertrauenswürdigen digitalen Geschäftsbeziehung zu den Benutzern können Versicherungen rechtmäßigen Verbrauchern die Möglichkeit bieten, neue Versicherungspolicen zu beantragen sowie rechtmäßigen Anbietern und Versicherungsexperten, sich ohne hohe Anforderungen bei der Authentifizierung bei ihren Konten anzumelden. Benutzer, die mit einem hohen Sicherheitsrisiko eingestuft wurden, müssen dagegen zusätzliche Anforderungen bei der Authentifizierung erfüllen.

Wie nehmen Sie echte Kunden in Ihrem digitalen Kanal auf? Wie bewahren Sie dieses Vertrauen in die digitale Geschäftsbeziehung? Wie halten Sie böswillige Akteure fern?

Die IBM Trusteer-Lösung wurde entwickelt, um Versicherungen dabei zu helfen, diese vertrauenswürdige digitale Geschäftsbeziehung schnell und transparent aufzubauen. Sie überprüft Benutzerinformationen passiv, deckt Muster auf, die auf böswillige Absichten hindeuten, und basiert auf Informationen aus einem globalen Netzwerk von Finanzdienstleistungsunternehmen. Mit dieser Lösung kann auch Ihr Unternehmen feststellen, ob es sich bei einem Benutzer um einen rechtmäßigen Kunden und keinen getarnten böswilligen Akteur handelt.

Weitere Informationen

Wenn Sie mehr über die Trusteer-Lösungen zur Risikobewertung im Zusammenhang mit digitalen Identitäten erfahren möchten, wenden Sie sich bitte an den zuständigen IBM Vertriebsbeauftragten oder IBM Business Partner, oder besuchen Sie uns unter: **ibm.com/security/trusteer**

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Please Recycle

WGW03353-DEDE-00