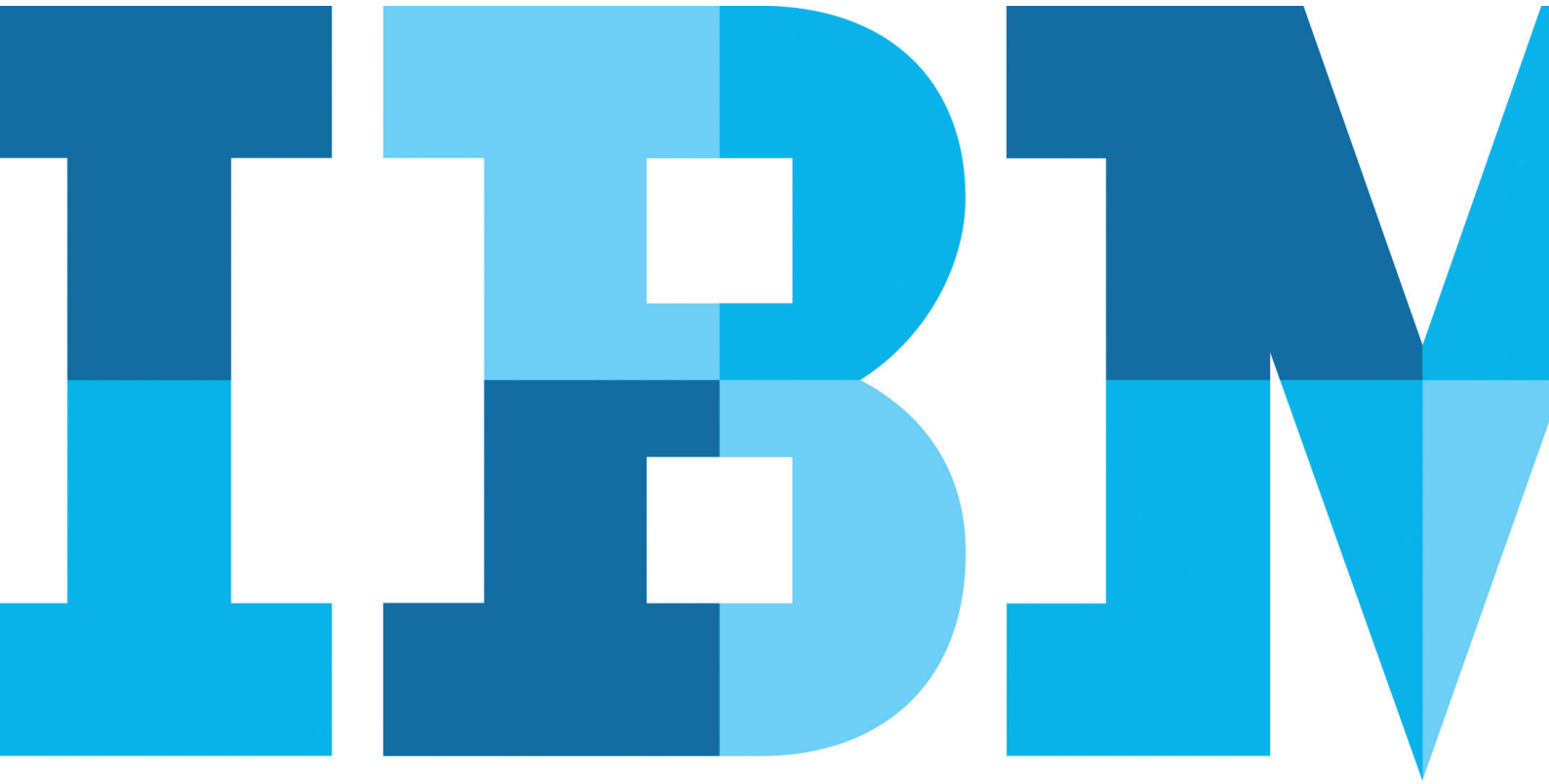
Budowanie przyjaznych kanałów cyfrowych dla klientów w branży ubezpieczeniowej

IBM Trusteer pomaga firmom ubezpieczeniowym w niezauważalny dla użytkowników sposób oceniać ryzyko związane z ich tożsamością cyfrową



IBM

Spis treści

Wprowadzenie

Dawno minęły czasy, gdy głównym kanałem kontaktu ubezpieczycieli z klientami byli przedstawiciele (agenci) ubezpieczeniowi. Chociaż ci ostatni nadal grają ważną rolę na ścieżce zakupowej klienta, branża ubezpieczeń – jak wiele innych branż – w kontaktach z użytkownikami zewnętrznymi i przy wkraczaniu na nowe rynki w coraz większym stopniu polega na niskokosztowych kanałach cyfrowych.

W ostatnich latach firmy ubezpieczeniowe wdrażają aplikacje umożliwiające ich klientom sprawdzanie danych zawartych polis, przeglądania świadczeń, porównywania cen, płacenia rachunków, zgłaszania szkód, a nawet składania wniosków o ubezpieczenie za pomocą telefonów komórkowych i komputerów osobistych. Wysiłek włożony w przeobrażenie branży pozwolił znacznie zmniejszyć koszty obsługi klienta, stwarzając jednocześnie nowe możliwości zbliżenia się do klientów i wzmocnienia ich lojalności względem marki.

W miarę dalszych postępów transformacji cyfrowej, firmy ubezpieczeniowe zaczynają skupiać się na zwiększaniu sprzedaży przez wprowadzanie nowych produktów ubezpieczeniowych, zaprojektowanych specjalnie dla kanałów cyfrowych i oferowanych klientowi albo bezpośrednio przez ich własne witryny internetowe, albo za pośrednictwem partnerów korzystających z udostępnionych przez nie interfejsów API.

Ubezpieczyciele inwestują też obecnie w optymalizację i usprawnianie procesów i usług realizowanych przy udziale firm zewnętrznych i osób trzecich, którym powierzają likwidację szkód (np. lekarzy, firm remontowych, warsztatów specjalizujących się w wymianie szyb samochodowych itp.). Współpraca ta wspiera firmy ubezpieczeniowe w świadczeniu na rzecz ich klientów tego typu usług i ułatwia im nawiązywanie współpracy z kolejnymi usługodawcami współdziałającymi z nimi w tym zakresie.

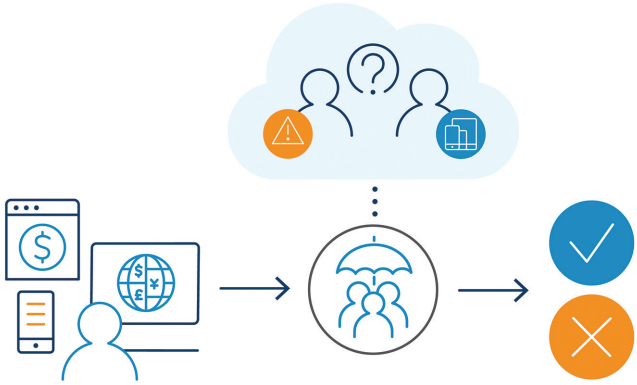
Stworzenie spójnego, łatwego w użytkowaniu kanału elektronicznego dla klientów końcowych, dostawców i pośredników ubezpieczeniowych może jednak być nie lada wyzwaniem.

Współcześni konsumenci, dostawcy usług i agenci ubezpieczeniowi oczekują wygody, oznaczającej dla nich zarówno łatwość korzystania z usług cyfrowych, jak i możliwość uzyskania oczekiwanej obsługi w każdej chwili i z dowolnego miejsca na świecie. Wygodą na pewno nie będzie dla użytkownika wymóg przebrnięcia przez jakąkolwiek kilkuetapową procedurę – czy to przez nadmiernie złożony proces uwierzytelniania, czy wymóg wypełnienia zanadto rozbudowanych formularzy, bez względu na to, czy są one dostępne w formie elektronicznej, czy przekazywane za pośrednictwem agenta ubezpieczeniowego. Złożoność takiego procesu może negatywnie wpłynąć na postrzeganą przez użytkownika jakość kanału cyfrowego, a w rezultacie – spowodować wzrost wskaźnika porzuceń koszyka i zwiększyć liczbę klientów końcowych, dostawców usług i pośredników ubezpieczeń nadal korzystających z bardziej kosztownych w utrzymaniu kanałów kontaktu (np. infolinii telefonicznej) lub decydujących się na skorzystanie z usług ubezpieczeniowych konkurencji.

W obecnej erze cyfrowej klienci za paroma dotknięciami wyświetlacza mogą z łatwością porównywać ceny i oferty, a nawet decydować, kiedy i jak chcą zawierać transakcje z firmami ubezpieczeniowymi.
Biorąc pod uwagę zaciętą konkurencję, powstanie obiegowej opinii o słabej obsłudze klienta lub niskim poziomie bezpieczeństwa może znacząco podkopać pozycję każdego ubezpieczyciela. Co więcej, włamanie na konto współpracującego z firmą ubezpieczeniową dostawcy usług lub pośrednika stwarza dla niej poważne ryzyko, że przejęty w złej wierze dostęp zostanie wykorzystany do zalania jej roszczeniami lub do generowania korzystnych dla oszusta niskokosztowych polis.

Należy więc postawić pytanie: Jak w prawidłowy sposób rozpoznawać prawdziwych, zaufanych użytkowników w kanałach cyfrowych, aby dzięki temu szybko i bezproblemowo obsługiwać zarówno nowych, jak i istniejących klientów, dostawców usług i pośredników ubezpieczeniowych, a jednocześnie skutecznie uniemożliwiać dostęp szkodliwym użytkownikom?

Kluczem do rozwiązania tego problemu jest wybór optymalnego sposobu oceny ryzyka wiążącego się z tożsamościami cyfrowymi.



Jak sprawnie obsługiwać klientów, skutecznie uniemożliwiając dostęp szkodliwym użytkownikom?

Dobre narzędzie, które oferuje taką funkcję, pomaga firmom ubezpieczeniowym identyfikować prawdziwych użytkowników kanałów cyfrowych i skuteczniej wykrywać tych potencjalnie szkodliwych, badając cyfrowe ślady pozostawiane przez każdego z nich przy interakcjach z różnymi systemami.

Wartość trafnej oceny ryzyka

Poniższa lista przedstawia cztery potencjalne korzyści wynikające z dostępu do trafnych ocen ryzyka na samym początku każdej interakcji drogą elektroniczną (np. przy składaniu przez nowego klienta wniosku ubezpieczeniowego, korzystaniu przez istniejącego klienta z kanału cyfrowego zamiast tradycyjnego, lub przy logowaniu się dostawcy usług w celu przesłania nowych zgłoszeń szkód).

Sprawniejsza i bardziej przyjazna obsługa użytkownika

Po pierwsze, trafna ocena ryzyka związanego z tożsamościami cyfrowymi może pomóc zapewnić istniejącym użytkownikom płynniejszą i szybszą obsługę podczas każdego logowania się przez nich na ich konta. Zastąpienie obciążania użytkowników szeregiem kroków weryfikujących przy każdym logowaniu ciągłym, bazującym na ryzyku uwierzytelnianiem dostarcza właścicielowi usługi informacji, dzięki którym może on zawęzić stosowanie dodatkowych kroków sprawdzających tylko do tych użytkowników, którzy będą zdradzać symptomy ewidentnie złych zamiarów. Co więcej, stosowanie uwierzytelniania ciągłego oferuje możliwość oceny użytkowników za każdym razem, gdy mają wykonać czynność wymagającą szczególnego poziomu bezpieczeństwa. Tym sposobem weryfikacja zaufania i ryzyka jest dokonywana wyłącznie wtedy, gdy to potrzebne. Firmy ubezpieczeniowe o mało przyjaznych dla użytkownika kanałach elektronicznych, zmuszające swoich klientów i kontrahentów do częstego tracenia czasu i nerwów na czynności uwierzytelniające, powinni być gotowi na to, że w pewnym momencie użytkownicy ich usług porzucą interakcję cyfrową na rzecz bardziej kosztownych w utrzymaniu form komunikacji lub odejdą do konkurenta.

Płynniejsza i szybsza obsługa może natomiast pomóc firmom ubezpieczeniowym podnieść wskaźniki lojalności klientów. Należy pamiętać, że właściciele polis często nawiązują kontakt z ubezpieczycielem w stresujących okolicznościach trudnych zdarzeń życiowych – wypadków drogowych, chorób lub śmierci bliskiej osoby. Niektórzy z nich być może nie logują się na swoich kontach zbyt często, co zwiększa prawdopodobieństwo, że w przypadku wysokiej złożoności procesu uwierzytelniania skorzystanie z kanału elektronicznego sprawi im trudność – choćby z powodu zapomnianego hasła. Upraszczając proces obsługi, ubezpieczyciele mają okazję udowodnić, jak bardzo zależy im na ułatwieniu ich klientom poradzenia sobie z formalnościami w najtrudniejszych dla nich momentach – i w ten sposób dobrze wykorzystać cenną okazję do zaskarbienia sobie ich lojalności. Z kolei dla dostawców usług likwidacyjnych i pośredników ubezpieczeniowych każda minuta poświęcona na uwierzytelnienie się w systemie oznacza stracone potencjalne przychody z dodatkowych zgłoszeń, którymi mogli się zająć w tym czasie. Zmniejszenie uciążliwości związanych z procesem uwierzytelniania bez rezygnowania z odpowiedniego poziomu bezpieczeństwa to doskonała recepta na utrzymanie lojalności klientów i przewagi nad konkurencją.

Pomoc w pozyskaniu i utrzymaniu klientów

Po drugie, dzięki takiemu atutowi łatwiej jest pozyskać i utrzymać klientów. Nadmiernie uciążliwy proces uwierzytelniania stanowi poważną przeszkodę dla klientów końcowych, oczekujących swobody kupowania nowej ochrony ubezpieczeniowej w dowolnym momencie i z dowolnego

miejsca. Jeżeli na drodze do upragnionego produktu napotkają zbyt wiele barier, przy każdej z których będą musieli udowadniać, że są osobami, za które się podają, mogą wreszcie stracić cierpliwość i poszukać innych firm ubezpieczeniowych, oferujących im zadowalającą ich obsługę bez utrudnień.

Pomoc w ochronie danych klientów

Po trzecie, posiadanie takiego narzędzia może okazać się cennym wsparciem dla wewnętrznych inicjatyw w dziedzinie ryzyka i polityki firmy w zakresie ochrony danych klientów. Cyberprzestępcy znają wiele sposobów obchodzenia procesów uwierzytelniania i podszywania się pod innych użytkowników, z uwierzytelnianiem dwuetapowym włącznie. Wystarczy, że uda im się uzyskać dostęp do konta jednego pośrednika ubezpieczeniowego lub dostawcy usług likwidacyjnych, a mogą wyprowadzić z firmy dane setek klientów. Skuteczna i trafna ocena ryzyka związanego z tożsamościami cyfrowymi przy użyciu pasywnych metod uwierzytelniania może pomóc w odkryciu ukrytych wzorców i symptomów wskazujących, że logujący się użytkownik nie jest dostawcą lub pośrednikiem, za którego chce uchodzić, lecz szkodliwym użytkownikiem, któremu udało się pozyskać dane uwierzytelniające konta.

Pomoc w ograniczeniu wpływu na działalność firmy

Na koniec należy koniecznie wspomnieć, że możliwość trafnego oceniania ryzyka związanego z tożsamością cyfrową użytkowników pozwala zmniejszyć wpływ, jaki przeprowadzane w złej wierze ataki mogą mieć na działalność firmy. Zatrzymując agresora na samym początku interakcji, firmy ubezpieczeniowe mogą obniżyć potencjalny koszt ręcznie prowadzonego dochodzenia i przetwarzania danych, a także uniknąć potrzeby wysyłania pisemnych wyjaśnień powodów odmowy dostępu – nie wspominając już o niekiedy druzgoczących stratach powodowanych wyciekami danych. Starsze, używane niegdyś i już przestarzałe technologie często wymagają zbyt wiele stałego udziału i uwagi zarządzających nimi pracowników. Strategie bazujące na elastycznie pozyskiwanych, właściwych informacjach, w większym stopniu zautomatyzowane i odciążające personel, mogą przyczynić się do zwiększenia precyzji mimo znacznie większej ilości przetwarzanych danych, zmniejszając ryzyko oszustwa i obniżając koszty operacyjne.

Aspekty oceny tożsamości cyfrowych

Jedną z trudności stojących na drodze skutecznej oceny tożsamości cyfrowych jest różnorodność i stałe ewoluowanie zagrożeń, z którymi muszą borykać się firmy ubezpieczeniowe oferujące obsługę elektroniczną.

Różne rodzaje szkodliwych użytkowników dopuszczają się różnych rodzajów przestępstw, i to na różnych etapach cyklu interakcji użytkownika z systemem ubezpieczyciela – począwszy od zakupu polisy, przez zgłaszanie szkód po obsługę klienta. Ich taktyka może obejmować:

- tworzenie fałszywych lub syntetycznych tożsamości (łączących dane skradzione lub fałszywe z tożsamościami istniejących osób), wykorzystywanych następnie w oszustwach dokonywanych pod rzeczywistym nazwiskiem sprawcy;
- wykorzystywanie prawdziwych, skradzionych tożsamości – co stanowi rosnący problem, zważywszy na ilość i zakres danych użytkowników, które zdążyły dotąd wyciec z różnych firm: imion i nazwisk, adresów, dat urodzenia, nazwisk panieńskich matki, numerów PESEL;
- podszywanie się pod istniejących klientów końcowych, dostawców usług lub pośredników ubezpieczeniowych w celu zgłaszania szkód, wyłudzania płatności i kredytów z naruszeniem warunków kredytowych, oraz po prostu wykradanie danych klientów;
- wielokrotne nabywaniepolis od różnych ubezpieczycieli wyłącznie w celu zgłoszenia szkody i uzyskania odszkodowania.

Nietrudno zgadnąć, że im więcej danych uda się włączyć w ocenę ryzyka, tym trafniejsze będą uzyskiwane alerty. Większa trafność może pomóc zmniejszyć liczbę fałszywych alarmów, którymi musi zająć się komórka do walki z oszustwami, a przez to – obniżyć koszty operacyjne.

Podczas oceny wiarygodności każdego użytkownika firmom ubezpieczeniowym opłaca się więc uwzględnić jak największy zakres danych. Obejmują one:

- prawdziwość urządzenia i dowody pozwalające odkryć i udokumentować spoofing – jako dane ułatwiające zwiększenie niezawodności identyfikacji urządzenia (jego tzw. fingerprint). Fingerprint każdego z urządzeń i wiązanie urządzeń z określonymi użytkownikami pomaga w uwierzytelnianiu użytkownika w sposób dla niego przezroczysty. Należy przy tym pamiętać, że fingerprint każdego urządzenia może stać się celem spoofingu, jego prawdziwość wymaga więc dodatkowej weryfikacji;
- czas i miejsce, z którego łączą się użytkownicy, rodzajów wykonywanych połączeń (witryna internetowa, łączność mobilna, VPN itp.) oraz stosowanego szyfrowania pomocne są atrybuty sesji i sieci;
- wyniki analizy behawioralnej i biometrii behawioralnej oraz wiedzy o nawigacji użytkownika, na podstawie których są tworzone wzorce jego działań – np. nietypowych ruchów myszą czy charakterystycznych sekwencji naciskanych klawiszy – które są używane następnie do wykrywania anomalii;
- analizę nawigacji, pozwalającą poznać sposób poruszania się przez niego po aplikacji i identyfikować w jego zachowaniu ewentualne anomalia;
- dodatkowe wskazówki na temat potencjalnego ryzyka wiążącego się z danym użytkownikiem pochodzące od operatora jego sieci komórkowej. Na przykład, użytkownika posługującego się zakupionym dwa dni wcześniej telefonem na kartę pre-paid uznaje się za źródło większego ryzyka, niż użytkownika telefonu od trzech lat opłacanego w abonamencie. Podobnie, telefonowi zarejestrowanemu u operatora popularnego wśród oszustów ze względu na mało rygorystyczne środki bezpieczeństwa będzie przypisywany wyższy poziom ryzyka niż telefonowi działającemu w sieci operatora o dobrej reputacji.

- Wiedza o wzorcach działań szkodliwych – zarówno doświadczonych przez pojedynczą firmę, jak i przez całą branżę – pomaga w wykrywaniu prób manipulowania zabezpieczeniami lub obchodzenia ich, a także w identyfikowaniu obecności używanych do ataku narzędzi, np. trojanów RAT lub złośliwego oprogramowania. Pozwala ona rozpoznawać ataki, których istotnym elementem jest socjotechnika, nierzadko pozostawiające bardzo niewiele śladów cyfrowych.
- W wykrywaniu szkodliwych działań ukierunkowanych na nowe organizacje pomagają dane historyczne, pochodzące z ogólnoświatowej sieci dokumentującej aktywność użytkowników szkodliwych i kierujących się złą wolą.

Bez tak szerokiego zakresu danych potwierdzenie, czy konkretnemu użytkownikowi naprawdę można ufać, może być o wiele trudniejsze.

Rozpoznawanie zaufanych użytkowników w kanałach cyfrowych

Zyskać można wiele: Zdobycie zdolności trafnego upewniania się co do legalności działań użytkowników i identyfikowania aktywności potencjalnie szkodliwej ułatwia zapewnienie użytkownikom oczekiwanej przez nich wygody i sprawnego, bezproblemowego korzystania z usług.

Platforma IBM® Trusteer® wychodzi naprzeciw tej potrzebie, oferując firmom ubezpieczeniowym możliwość potwierdzania wiarygodności użytkowników już od pierwszych momentów interakcji.

Rozwiązanie IBM Trusteer może pomóc firmom ubezpieczeniowym w rozpoznawaniu zaufanych użytkowników w kanałach cyfrowych dzięki korelowaniu informacji pochodzących z ich obszernych zasobów wewnętrznych z wiedzą czerpaną ze źródeł globalnych.

Łączy ona dostęp do kompleksowych i szczegółowych danych na temat ich zachowań, sesji i urządzeń z działającymi w czasie rzeczywistym kognitywnymi funkcjami analitycznymi, pomagając w ustalaniu w sposób niezauważalny dla użytkownika zasadności i legalności każdej jego czynności w środowisku elektronicznym i zapewniając ciągłe jego uwierzytelnianie w oparciu o stale aktualizowaną ocenę poziomu ryzyka.

Rozwiązanie Trusteer stosuje podejście, które można opisać jako „ufaj, ale sprawdzaj”, zakulisowo poszukując w działaniach korzystającego z kanałów cyfrowych użytkownika symptomów wskazujących na ich zamierzoną szkodliwość.

Zakulisowa ocena informacji o użytkowniku

Dzięki dostępowi do globalnej sieci gromadzącej dane z całego świata, platforma IBM Trusteer ocenia związane z użytkownikiem ryzyko i jego wiarygodność na podstawie szerokiego wachlarza danych. Dane te obejmują:

- informacje pochodzące od operatora sieci komórkowej, służące ocenie wiarygodności użytkownika na podstawie podanego przez niego numeru telefonu.
- Informacje o urządzeniu, pozwalające stwierdzić, czy używane do logowania się urządzenie nie jest podejrzane, czy to w wyniku spoofingu, czy zainfekowania złośliwym oprogramowaniem, czy nawet użycia w przeszłości w celu wyrządzenia innej szkody;
- informacje o sieci i sesji, pozwalające ujawnić niespójności w danych o lokalizacji użytkownika lub zasygnalizować stosowanie unikalnych metod, narzędzi i sposobów przeglądania stron i zasobów internetowych charakterystycznych dla zorganizowanej przestępczości elektronicznej;
- biometrię behawioralną, pasywnie identyfikującą zachowanie użytkowników w trakcie korzystania przez nich z aplikacji i usług cyfrowych, służącą automatycznemu odróżnianiu prawdziwych użytkowników od tych szkodliwych. W przypadku nowych klientów, biometria behawioralna pozwala wykryć ataki złośliwych botów i rozpoznać znane systemowi wzorce działania charakteryzujące szkodliwych użytkowników usiłujących dokonać kradzieży tożsamości. W przypadku klientów istniejących, funkcje takie są w stanie „uczyć się” typowych dla nich wzorców zachowań przy korzystaniu z usług, i następnie wykorzystywać tę wiedzę do ciągłego i niewidocznego dla użytkowników weryfikowania ich tożsamości za każdym razem, gdy odwiedzają witryny i aplikacje ubezpieczyciela w celu sprawdzenia szczegółów polisy, zarządzania zgłoszeniami szkód lub wprowadzania zmian na swoich kontach.

- Wewnętrzne bazy danych szkodliwych użytkowników platformy IBM Trusteer. Informacje te obejmują dokumentację dowodową wcześniejszych działań elektronicznych szkodliwych użytkowników – w tym adresy e-mail, numery telefonów, identyfikatory urządzeń, dane zorganizowanych siatek przestępczych i kont–słupów — opracowane w całości na podstawie danych analitycznych setek firm i instytucji z całego świata.

Odkrywanie wzorców identyfikujących szkodliwe zamiary

Szkodliwi użytkownicy często wykazują pewne charakterystyczne dla nich zachowania, odróżniające ich od użytkowników działających legalnie. Zachowania te bywają bardzo trudne do wychwycenia – np. sposób wprowadzania danych w aplikacjach lub tempo wypełniania formularzy na stronach internetowych. Pozwalają jednak rozwiązaniom z rodziny IBM Trusteer wykrywać wzorce zachowań szkodliwych i włączać je w zasób wiedzy używanej przez inteligentne, uczące się algorytmy oceny ryzyka przy analizie licznych informacji charakteryzujących urządzenia, sesje i prawidłowości sposobu działania użytkowników. Uwzględniane w takiej analizie elementy danych to m.in.:

- informacje o historii działań użytkownika, np. czas spędzony na konkretnych stronach, sposób wypełniania określonych formularzy, tempo pisania na klawiaturze oraz specyfika nawigacji po kanale cyfrowym – analizowana w zestawieniu z zachowaniem prawdziwych, legalnych użytkowników w poszukiwaniu różnic, które mogłyby rodzić jakiekolwiek podejrzenia;
- powiązania tożsamości: czy dane wprowadzone we wniosku o nowe ubezpieczenie lub przy rejestracji nowego konta zostały już wcześniej użyte w innym wniosku lub w innej firmie ubezpieczeniowej?
- analiza działań posiadaczy nowych kont: czy daje się wykryć jakakolwiek aktywność sugerująca znane wzorce zachowań szkodliwych bezpośrednio po założeniu konta? Taka działalność mogłaby sugerować, że dane konto utworzono w celu jego wykorzystania w oszustwie lub ataku.

Zalety dostępu do wiedzy zgromadzonej przez wiele firm

Atakując różne firmy i instytucje, szkodliwi użytkownicy często stosują taką samą taktykę lub te same elementy tożsamości skradzionych lub syntetycznych. Rozwiązania IBM Trusteer wykorzystują tę prawidłowość, uwzględniając w analizie wzorce zachowań szkodliwych zaobserwowane przez różnych dostawców usług ubezpieczeniowych na całym świecie, korzystających z ochrony oferowanej przez narzędzia platformy IBM Trusteer. Dostęp do tak szerokiej wiedzy, pochodzącej z tylu źródeł globalnych pozwala rozwiązaniom IBM Trusteer skuteczniej wspierać firmy w wykrywaniu, czy:

- użytkownik wnioskujący o ubezpieczenie nie próbował wcześniej otworzyć u innych ubezpieczycieli chronionych rozwiązaniami IBM Trusteer jednego lub większej liczby kont w tempie i z częstotliwością typowymi dla użytkowników szkodliwych;
- dane urządzenie (lub elementy tożsamości jego użytkownika) nie jest używane do otwarcia wielu różnych kont w imieniu różnych użytkowników;
- ten sam numer telefonu, adres e-mail lub adres korespondencyjny nie pojawia się w różnych wnioskach złożonych przez różne osoby.

Elastyczność dzięki dostępowi do właściwych informacji

Jakiej taktyki szkodliwi użytkownicy będą używać w przyszłości? Aby zaoferować firmom ubezpieczeniowym jak najwięcej korzyści w dziedzinie, w której jedyną stałą rzeczą jest ciągła zmiana, IBM Trusteer sięga zarówno po zaawansowane technologie, jak i po światowej klasy specjalistów z dziedziny bezpieczeństwa, stawiając przed nimi zadanie codziennego monitorowania zmieniających się zagrożeń.

Infrastruktura bezpieczeństwa platformy Trusteer bezustannie rozszerza się o nową wiedzę i nowe informacje, których źródłem są:

- funkcje uczenia maszynowego, w tym warstwy sztucznej inteligencji odpowiedzialne za wykrywanie i analizę oszustw; ich zadaniem jest umożliwienie zrozumienia, wykrywania i przewidywania pojawiającego się ryzyka szkodliwych działań użytkowników usług elektronicznych;
- globalne, dostępne dzięki chmurze w czasie rzeczywistym informacje o zagrożeniach oraz wiedza dostarczana przez firmy z całego świata;
- śledzenie pojawiających się dopiero wzorców zachowań przez IBM X-Force®, jeden z najbardziej rozpoznawalnych na świecie zespołów analityków bezpieczeństwa w biznesie.

Zapewniona w ten sposób ciągłość dopływu aktualnych danych podnosi wartość dostarczanych przez rozwiązanie informacji na całkiem nowy poziom, czyniąc z niego narzędzie prawdziwie uniwersalne. Pomaga to w szybkiej orientacji w istniejącym ryzyku pojawienia się prób nadużyć i ataków, ich wykrywaniu i przewidywaniu, a także wspiera ochronę przed cyberprzestępczością mimo ciągłego ewoluowania stosowanych przez nią taktyk, zwiększa trafność oceny ryzyka i obniża koszty operacyjne – a przy tym pozwala zapewnić działającym w dobrej wierze użytkownikom niczym niezakłócone, szybkie i sprawne korzystanie z oferowanych usług.

Budowanie własnych zbiorów zasad przy użyciu zaawansowanych mechanizmów pozyskiwania informacji platformy IBM Trusteer

Firmy ubezpieczeniowe muszą nierzadko spełniać szeroki wachlarz wymogów biznesowych, zarówno globalnych, jak i lokalnych, dostosowując się przy tym do faktycznie obserwowanych sposobów korzystania przez klientów i kontrahentów z oferowanych przez nie kanałówi do poziomu ich własnej wrażliwości na ryzyko.

W rezultacie wiele firm i instytucji poszukuje rozwiązań, które umożliwią im kontrolę nad stosowanymi przez nie modelami oceny potencjalnego ryzyka. Oferuje im to właśnie narzędzie do zarządzania politykami platformy IBM Trusteer, dając im wgląd w takie modele, zdolność do ich przystosowywania do własnych potrzeb oraz gwarantując elastyczność pozwalającą na szybką ocenę skuteczności istniejących i stosowania nowych środków zaradczych, a dzięki temu – tworzenia nowych zasad zarządzania kontami, umożliwiających im skuteczne spełnianie wewnętrznych i zewnętrznych wymogów i przepisów.

Dzięki mechanizmom uczenia maszynowego, narzędzie to łączy wiedzę o znanych zagrożeniach i trendach i tych dopiero co zauważonych, którym dana organizacje musi stawić czoła, i wyposaża ją w narzędzia pozwalające jej dostosować nowe zasady, wypróbować je w symulacjach i odpowiednio przystosować modele ryzyka – i to zarówno w sposób automatyczny, jak i na podstawie konkretnych informacji i wiedzy; wszystko to bez konieczności posiadania przez firmę specjalistycznej wiedzy ani zaawansowanych umiejętności.

Wnioski

Transformacja cyfrowa otwiera przed firmami ubezpieczeniowymi możliwość wzmocnienia więzi z istniejącymi klientami, dostawcami usług i pośrednikami ubezpieczeniowymi, a także umożliwia przyciąganie nowych klientów i kontrahentów innowacyjnymi produktami i usługami. W erze cyfrowej zarówno konsumenci, jak i partnerzy biznesowi – dostawcy i pośrednicy – oczekują jednak istniejącej w dowolnym momencie możliwości pozyskiwania i zmieniania dotyczących ich informacji, zgłoszeń i polis.

Oznacza to, że sukces biznesowy firm ubezpieczeniowych w nadchodzących latach będzie w znacznej mierze zależeć od tego, na ile łatwo będzie wchodzącym z nimi w interakcję osobom i podmiotom korzystać z ich oferty produktów i usług. Jeszcze ważniejsza staje się zdolność ubezpieczycieli do wykorzystywania pozyskanych wcześniej dynamicznych zdolności i procesów w nowych elementach oferty – a umożliwiają to właśnie takie rozwiązania, jak IBM Trusteer.

Nadmierna złożoność aplikacji i procesów, np. zmuszanie klientów i partnerów do wielokrotnego uwierzytelniania się w systemach ubezpieczyciela, będzie niechybnie powodować ich frustrację, obniżając wskaźniki ich zadowolenia i skutkując porzuceniem przez nich kanałów elektronicznych na rzecz bardziej pracochłonnych i kosztownych w utrzymaniu lub wręcz ucieczką do konkurencji. Zapewnienie użytkownikowi sprawnej i szybkiej obsługi przy kontakcie drogą elektroniczną pozwoli natomiast zbudować – lub poprawić – poziom lojalności klientów i reputację usług firmy na rynku.

Zyskując zdolność trafnego weryfikowania wiarygodności użytkowników w kanałach elektronicznych, firmy ubezpieczeniowe ułatwiają swoim klientom końcowym wnioskowanie o nowe polisy, a zaufanym dostawcom usług i pośrednikom ubezpieczeniowym – logowanie się na swoje konta bez konieczności przechodzenia nużących procedur uwierzytelniających, które zostają zarezerwowane dla użytkowników słusznie identyfikowanych jako powiązanych z wysokim ryzykiem.

Jak rozpoznać i powitać prawdziwych użytkowników kanału cyfrowego? Jak utrzymać zaufanie do zidentyfikowanej tożsamości cyfrowej? Jak uniemożliwić dostęp szkodliwym użytkownikom?

Rozwiązanie IBM Trusteer jest zaprojektowane tak, aby pomóc firmom ubezpieczeniowym w szybkim i niezauważalnym dla użytkowników rozpoznawaniu zaufanych tożsamości cyfrowych. Pasywnie sprawdza one dostępne informacje na ich temat, rozpoznaje wzorce sygnalizujące nieczyste intencje potencjalnych agresorów i korzysta z wiedzy zgromadzonej w globalnej sieci instytucji finansowych specjalnie w celu umożliwienia innym firmom z branży odróżnienia prawdziwych klientów od podszywających się pod nich szkodliwych użytkowników.

Więcej informacji

Więcej informacji na temat oferowanych przez platformę IBM Trusteer rozwiązań służących do oceny ryzyka związanego z tożsamością cyfrową można uzyskać od przedstawiciela lub Partnera Handlowego® IBM, a także znaleźć pod adresem: **ibm.com**/security/trusteer

© Copyright IBM Corporation 2020

IBM Security
Route 100
Somers, NY 10589

Wyprodukowano w Stanach Zjednoczonych
Marzec 2020

IBM, logo IBM, ibm.com, Trusteer oraz X-Force są znakami towarowymi należącymi do International Business Machines Corp., zarejestrowanymi w wielu krajach na całym świecie. Pozostałe nazwy produktów i usług mogą być znakami towarowymi IBM lub innych podmiotów. Aktualna lista znaków towarowych IBM jest dostępna w dokumencie pt. „Copyright and trademark information" (Informacje o prawach autorskich i znakach towarowych), dostępnym pod adresem **ibm.com**/legal/copytrade.shtml

Niniejszy dokument jest aktualny na dzień jego publikacji. IBM zastrzega sobie prawo do wprowadzania w nim zmian w dowolnym momencie. Niektóre oferty mogą być niedostępne w niektórych krajach, w których działa IBM.

Przywoływane wskaźniki, wyniki i przykłady klientów służą wyłącznie do celów poglądowych. Wyniki uzyskiwane w rzeczywistości mogą odbiegać od opisanych, zależnie od konfiguracji systemów i warunków operacyjnych.

INFORMACJE ZAWARTE W TYM DOKUMENCIE SĄ PRZEDSTAWIONE W STANIE WIDOCZNYM, BEZ JAKICHKOLWIEK GWARANCJI JAWNYCH BĄDŹ DOMNIEMANYCH, W TYM BEZ JAKICHKOLWIEK GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU I BEZ GWARANCJI NIENARUSZANIA PRAW OSÓB TRZECICH. Na produkty IBM udziela się gwarancji zgodnych z warunkami i postanowieniami umów dotyczących dostarczanych produktów.

Odpowiedzialność za zapewnienie zgodności z obowiązującymi przepisami prawnymi ponosi klient. Spółka IBM nie oferuje porad prawnych ani nie gwarantuje zgodności jej usług i produktów z obowiązującymi klienta przepisami prawa.

Oświadczenie dotyczące dobrych praktyk w dziedzinie bezpieczeństwa: Bezpieczeństwo systemów informatycznych polega na ochronie systemów i informacji przez zapobieganie, wykrywanie oraz reagowanie na niepożądany dostęp do nich z wewnątrz lub z zewnątrz firmy. Może on skutkować modyfikacją danych, ich zniszczeniem lub przywłaszczeniem; może też prowadzić do uszkodzenia lub niewłaściwego użycia systemu, włącznie z użyciem go do ataku na inne systemy. Żaden system lub produkt IT nie powinien być uważany za całkowicie bezpieczny i żaden produkt, usługa lub środek bezpieczeństwa nie jest w stanie całkowicie ochronić przed nadużyciami ani niepożądanym dostępem. Systemy, produkty i usługi IBM są zawsze projektowane jako część kompleksowego podejścia do zagadnienia ochrony i do osiągnięcia swojej maksymalnej skuteczności wymagają na ogół dodatkowych procedur, systemów, produktów i usług. IBM NIE GWARANTUJE, ŻE JAKIEKOLWIEK SYSTEMY, PRODUKTY LUB USŁUGI BĘDĄ ODPORNE (ALBO ZAPEWNIĄ SYSTEMOM PRZEDSIĘBIORSTWA ODPORNOŚĆ) NA SZKODLIWE LUB NIEZGODNE Z PRAWEM DZIAŁANIA JAKICHKOLWIEK OSÓB LUB PODMIOTÓW.

Proszę Segreguj

WGW03353-PLPL-00