OPEN BANKING

Twój bank jak Facebook? Zalogujesz się do sklepu albo zamówisz pizzę!

Czasy banków, w których klienci w kolejkach czekali na obsługę, odchodzą w przeszłość. Współcześni klienci oczekują nie tylko nieustającego dostępu do swoich pieniędzy, ale też do szerokiej gamy produktów bankowych. Kredyt wzięty w środku nocy przez telefon nie jest niczym niespotykanym. Ubezpieczenie podróżne, lokaty – wszystko to chcemy robić nie wychodząc z domu, nieograniczeni czasem działania banku czy dostępnością konsultantów na infolinii.

Adam **Wojtkowski**

General Manager CEE, Red Hat

Chcąc móc spełniać rosnące i wciąż zmieniające się potrzeby klientów, banki muszą zmieniać się wewnętrznie i unowocześniać swoją infrastrukturę IT. Jak pokazują badania IDC przeprowadzone na zlecenie Red Hat, jednym z najchętniej stosowanych przez instytucje bankowe rozwiązań mających zapewnić rozwój instytucji bankowych i spełnianie rosnących oczekiwań klientów jest open API.

Co to jest to open API i skąd się wzięło?

Wiele osób może kojarzyć skrót PSD2. To oznaczenie dyrektywy unijnej nakładającej na banki i instytucje finansowe nowe obowiązki. W jej kontekście w Polsce najwięcej mówiono o nowych sposobach logowania do kont bankowych (tak zwane podwójne uwierzytelnienie) oraz konieczności potwierdzania kodem PIN niektórych transakcji zbliżeniowych. Jednak dyrektywa UE to znacznie więcej regulacji i zmian. PSD2 wprowadziła powszechnie pojęcie otwartej bankowości i to właśnie z nią nierozerwalnie związane jest pojęcie open API. Czym ono jest w praktyce? Dzięki temu rozwiązaniu zewnętrzni dostawcy, oczywiście za naszą zgodą, mogą mieć dostęp do niektórych informacji, np. o stanie naszego konta czy inicjować płatności. Przykładowo, na telefonie mamy zainstalowaną aplikację ulubionego sklepu. Jeśli robimy przez nią zakupy i będziemy chcieli zapłacić za nie za jej pośrednictwem, to dzięki open API aplikacja będzie mogła się połączyć z bankiem i obciążyć nasze konto opłatą za zakupy. Mówimy tutaj o pieniądzach oraz dostępie do informacji o naszym koncie, dlatego kluczowym aspektem, wobec którego obiekcje miały także same banki, jest kwestia bezpieczeństwa. Popularnym API jest Facebook, dzięki któremu można logować się w dziesiątkach tysięcy miejsc w sieci. A gdyby tak wykorzystać do tego swój login z banku? Dla instytucji finansowych open API to szansa na potężny rozwój i unowocześnienie. Banki dostrzegły, że mogą stać się nowoczesnymi platformami, które dzięki API będą realizować na rzecz usługodawców różne zadania i operacje zlecone im przez klientów. Pokazują to badania IDC, przeprowadzone na zlecenie Red Hat.

Najważniejsze wyzwanie – uwolnić się od zamkniętych, przestarzałych platform

Analitycy z IDC[1] wprost nazywają przestarzałe systemy bankowe „ociężałymi statkami”, które nie są w stanie szybko reagować na prądy morskie, pogodę i zmieniające się warunki. Open API to natomiast wygodny, szybki i bardzo łatwo sterowalny nowoczesny jacht, w którym można swobodnie kierować ustawieniem każdego żagla, silnika i tym samym ekspresowo dopasowywać się do zmieniających się warunków zewnętrznych. Nietrudno sobie wyobrazić, co wybiorą klienci instytucji finansowych. Wybiorą te, które będą szybko reagowały na ich potrzeby, styl życia dając im poczucie, że ich bank zawsze dotrzymuje im kroku.

Co ważne, również banki dostrzegły potencjał i ogromne możliwości open API. Inwestując w rozwój tej technologii dziś, jednocześnie budują swoją pozycję w przyszłości. To swoistego rodzaju przekształcanie napotykanych wyzwań w szanse na sprostanie rosnącym oczekiwań klientów, ale także ograniczanie kosztów.

Z badań IDC, przeprowadzonych na zlecenie firmy Red Hat, wynika, że działy IT instytucji finansowych najczęściej borykają się z wyzwaniami w postaci:

– rosnących oczekiwań klientów, którzy chcą mieć dostęp do usług bankowych w trybie 24/7 z każdego miejsca na świecie

– regulacji i przepisów (także te związane ze środowiskiem i jego ochroną), które potrafią pochłonąć nawet 30-50 proc. budżetu działu IT

– wykorzystywania starej, drogiej w utrzymaniu i trudno integrowalnej infrastruktury IT, która znacząco wydłuża czas reagowania na potrzeby rynku

Jednocześnie z wywiadów przeprowadzonych przez IDC[2] wynika, że aż 83 proc. banków postrzega open API jako drogę do modernizacji infrastruktury IT, zwiększenia satysfakcji klientów i dopasowania się do wymogów prawa. Również 83 proc. respondentów wskazało open API jako szansę na wdrożenie zupełnie nowych modeli biznesowych.

Ważne kwestie bezpieczeństwa

Przedstawiciele sektora bankowego na samym początku uchwalania dyrektywy PSD2 mieli obawy związane z bezpieczeństwem zarówno danych, jak i samych pieniędzy swoich klientów. Słusznie zadawano pytania o bezpieczeństwo otwartych API i o to, jak dalece można je zabezpieczyć przed dostępem osób nieuprawnionych, ale także odseparować od najbardziej wrażliwych danych i systemów. IDC, powołując się na dane IDC Financial, podkreśla, że wyróżnić należy trzy główne rodzaje open API – prywatne, przeznaczone dla partnerów oraz publiczne. Część prywatna jest mocno zintegrowana z wewnętrznymi systemami bankowymi i wykorzystana jest wyłącznie wewnątrz organizacji. Nikt postronny nie ma do niej dostępu. Część partnerska tworzona jest wspólnie z partnerem, gdzie dokładnie projektuje się zakres dostępu i odpowiednio go zabezpiecza. Część publiczna jest zwyczajowo najbardziej ograniczona i prezentuje niewielkie ilości danych, do tego mocno zabezpieczonych.

Przyszłość rysuje się ciekawie

Open API wniosło na rynek ogromne możliwości. Praktyczna dowolność w kształtowaniu nowych rozwiązań, produktów i funkcjonalności niesie ze sobą konieczność wyjątkowego dbania o bezpieczeństwo. Banki będą zmuszone do wprowadzenia zasad i procedur pozwalających w sposób niezakłócony monitorować open API. Według badania IDC3, nowe modele zarządzania bezpieczeństwem będą wymagały nie tylko zmiany w szkoleniach zespołów IT, ale także umiejętne łączenie DevOps, metodyk zwinnych i zarządzania procedurami czy procesami.

Banki nie uciekną, a nawet nie chcą uciekać przed strategią biznesową opartą o cyfrową transformację. Korzyści z niej płynące są dużo większe niż potencjalne zagrożenia, a open API jest odpowiedzią na rosnące i wciąż zmieniające się potrzeby rynku i klientów.

1. Badanie IDC dla Red HAT „Beyond Banking Through Open APIs” https://www.redhat.com/cms/managed-files/ve-idc-financial-services-api-strategy-analyst-paper-f12428-201806-en.pdf

2. Badanie IDC dla Red HAT „Beyond Banking Through Open APIs” https://www.redhat.com/cms/managed-files/ve-idc-financial-services-api-strategy-analyst-paper-f12428-201806-en.pdf

3. Badanie IDC dla Red HAT „Beyond Banking Through Open APIs” https://www.redhat.com/cms/managed-files/ve-idc-financial-services-api-strategy-analyst-paper-f12428-201806-en.pdf

CO DAJE DZIŚ „ZWYKŁEMU KOWALSKIEMU” OPEN BANKING?

Dzięki obowiązującej od dwóch lat dyrektywie unijnej PSD2, konsumenci otrzymali m.in. łatwy dostęp do podglądu swoich kont z różnych banków i możliwości zarządzania swoimi finansami. Obecnie mogą oni w jednym miejscu widzieć stan środków czy historię transakcji na wszystkich kontach we wszystkich bankach i łatwo zlecać usługi pomiędzy różnymi kontami itp.

A dzięki ewentualnym zgodom udzielonym innym podmiotom finansowym na dostęp do danych konta – konsumenci otrzymali znacznie szersze możliwości dokonywania tanich lub nawet bezpłatnych transakcji bezgotówkowych przy użyciu np. urządzeń zbliżeniowych opartych o technologię NFC, takich jak karty czy implanty płatnicze.

Co to jest open banking?

Otwarta bankowość to po prostu system (na który składają się regulacje prawne i technologia), który umożliwia uprawnionym podmiotom trzecim (innym bankom, fintechom, serwisom płatniczym – określanym jako TPP, czyli Third Party Providers), oczywiście zawsze za zgodą klienta, dostęp do określonych funkcjonalności infrastruktury bankowej (konta bankowego klienta) za pomocą dedykowanych API (interfejsów programistycznych rządzących wzajemnym komunikowaniem się aplikacji). Dzięki temu konsument może otrzymać w jedynym miejscu (np. aplikacji na smartfonie) pełen obraz swoich wszystkich kont: osobistych, firmowych, oszczędnościowych, kart kredytowych i przedpłaconych. To bardzo wygodne, żeby np. szybko zorientować się w kolejce przed kasą w sklepie, której karty użyć za zakupy.

– Dostęp zgodny z dyrektywą PSD2 może opierać się na jednym z dwóch elementów. Po pierwsze może polegać on na pozyskaniu informacji o rachunku (TPP jako dostawca uzyskuje od banku prowadzącego rachunek np. dane o transakcjach użytkownika), czyli usługa AIS. Drugim elementem może być polecenie bankowi wykonania określonej operacji z konta klienta (TPP jako dostawca „zleca” bankowi wykonanie polecenia przelewu o określonych parametrach), czyli usługa PIS. TPP (ang. Third Party Provider) – jest to dosłownie „dostawca będący stroną trzecią”, czyli podmiot trzeci świadczący nowe usługi płatnicze wynikające z dyrektywy PSD2 (AIS lub PIS). Duża część TPP to podmioty z sektora fintech, choć oczywiście usługi te mogą być też świadczone np. przez bank, który występuje wówczas jako TPP – mówi Artur Bilski, ekspert w dziedzinie bankowości elektronicznej, Chief Legal Officer (CLO) w polsko-brytyjskiej firmie sektora fintech, tj. Walletmor Ltd.

Bezpieczeństwo

Pozytywne zmiany wynikające z dyrektywy PSD2, które bezpośrednio wpływają na bezpieczeństwo transakcji bezgotówkowych „zwykłego Kowalskiego” nakładają m.in. na instytucje finansowe obowiązek tzw. silnego uwierzytelniania. W praktyce oznacza to, że wykonując dowolną operację w bankowości elektronicznej czy aplikacji mobilnej, system poprosi nas o dodatkowe potwierdzenie np. w postaci wpisania kodu z otrzymanego SMS-a, czy dodania identyfikatora biometrycznego (odcisk palca albo face ID). Agregacja kont klientów może być też pomocna w weryfikacji zdolności kredytowej. Dostęp do informacji z różnych kont z różnych banków usprawni wnioskowanie o debet, pożyczkę bądź kartę kredytową.

Nie tylko konsumenci się cieszą

Open banking pozytywnie wpłynął już na polski rynek usług płatniczych. Personalizacja ofert banków, bezpieczeństwo danych i szybkość reakcji na problemy klientów znacznie poprawiły relację klienta z instytucją finansową. Dzięki PSD2 banki mają techniczną możliwość i jednocześnie okazję do częstszych kontaktów ze swoim klientem oraz podniesienia sprzedaży dodatkowych produktów. Finalnie klient otrzymuje ofertę dopasowaną do swoich indywidualnych potrzeb, a bank cieszy się, bo klient nie będzie szukać potrzebnych usług gdzieś indziej. Z kolei zaletami dla sprzedawców mogą być niższe koszty (brak opłaty interchange oraz innych opłat mających zastosowanie do transakcji kartowych) oraz relatywnie trudniejsze, w porównaniu do transakcji kartowych, cofnięcie już zleconej transakcji. Co równie istotne, dzięki założeniom dyrektywy PSD2, zwiększać się może zyskowność sprzedawców z każdej transakcji z uwagi na potencjalne wyeliminowanie pośredników (np. operatorów kart kredytowych). Przykładem może być polskie rozwiązanie BLIK, dzięki któremu sprzedający otrzymują 100 procent kwoty wpłacanych przez kupujących. W całym obrocie handlowym zostaje więcej pieniędzy, nabywcy kupują taniej, sprzedawcy tańszych towarów realizują większy obrót.

PSD II – matka chrzestna open banking

Jak każda branża tak i świat finansów ulega wielu czynnikom zewnętrznym mającym wpływ na formę usług oferowanych przez działające w niej podmioty. W dobie błyskawicznie rozwijających się technologii i zmieniających się potrzeb zakupowych ewoluują też wymagania prawne, które nierzadko redefiniują całe ekosystemy. Przykładem może być opublikowana w 2015 roku, kluczowa dla branży finansowej dyrektywa PSD II (ang. Payment Service Directive 2).

Marek **Trąbiński**

ekspert rozwiązań płatniczych POS i eCommerce, eService

Jej głównym celem było określenie zasad świadczenia wcześniej nieuregulowanych prawnie usług płatniczych oraz zwiększenie bezpieczeństwa podmiotów uczestniczących w obiegu pieniądza elektronicznego. Wpłynęła ona znacząco na działalność m.in. instytucji płatniczych – standaryzując formę niektórych świadczonych przez nie usług oraz banków – przełamując ich monopol na dostęp do kont bankowych. Banki zostały zmuszone do otwarcia świata danych i systemów bankowych na dostęp zewnętrznych instytucji płatniczych, a te drugie musiały spełnić określone wymogi regulacyjne, by korzystać z nadanych im uprawnień i móc tworzyć nowe rozwiązania, uzyskując licencje od lokalnych organów nadzorczych – wszystko z korzyścią dla użytkowników końcowych.

Open banking, czyli alternatywa do obecnych Przelewów Online

Jeszcze do niedawna najczęściej wybieraną metodą płatności elektronicznych były tzw. przelewy online, polegające na przekierowaniu płatnika do jego bankowości elektronicznej i zainicjowaniu przelewu z podstawionymi danymi odbiorcy. By taka usługa mogła być świadczona przez bramkę płatniczą, instytucja ją dostarczająca musiała podpisać odrębną umowę z każdym z banków i dla każdego wykonać integrację techniczną. Stawiało to banki w pozycji lidera negocjacyjnego i pozwalało dyktować warunki. By zrównoważyć tę dysproporcję, w dyrektywie PSD II zdefiniowano dwie nowe usługi: AIS (ang. Account Information Service), rozwiązanie wykorzystywane do scoringu kredytowego oraz agregowania danych z wielu kont bankowych, oraz PIS (Payment Initation Service), znajdującą zastosowanie w płatnościach elektronicznych, a służącą instytucjom płatniczym do inicjowania w imieniu płatnika przelewu – z jego konta, na konto odbiorcy. Banki zostały też zobowiązane do przygotowania otwartych interfejsów, poprzez które licencjonowane podmioty trzecie mogą korzystać z usług AIS czy PIS, bez konieczności podpisywania umów. W efekcie PIS zastąpi z czasem obecną architekturę przelewów online. Dostarczy przy tym korzyści firmom sprzedającym swoje produkty i usługi w Internecie – m.in. zwiększając konwersję koszyków zakupowych, a płacącym, pozwoli szybciej i łatwiej sfinalizować transakcję. Dla operatorów płatności elektronicznych, takich jak eService oznacza to możliwość samodzielnego wykonania prac technicznych integrujących bramkę płatniczą z każdym z banków oddzielnie lub skorzystania z usług integratorów open bankingu – takich jak np. litewski startup KEVIN. Sformalizowanie open bankingu w postaci dyrektywy PSD II dało tym samym szansę na powstanie i rozwój zupełnie nowej gałęzi sektora finansowego.

Większe bezpieczeństwo płacącego

Kolejnym ważnym aspektem, który wprowadziła dyrektywa, jest obowiązek zastosowania podczas obsługi transakcji mechanizmów Silnego Uwierzytelnienia Klienta (ang. Stron Customer Authentication). Wiążą się one m.in. z koniecznością weryfikacji, co najmniej dwóch elementów, należących do trzech typowych kategorii zasobów właściwych wyłącznie dla konkretnego posiadacza karty: czegoś, co ZNA (PIN karty, hasło lub odpowiedź na pytanie zabezpieczające), czegoś, co POSIADA (karta lub inny nośnik danych karty) lub czegoś, co JEST cechą charakterystyczną (odcisk palca, skan twarzy, sygnatura głosu itp.). Decyzję czy i w jakim zakresie dla danej transakcji, jest stosowany mechanizm SCA zawsze podejmuje bank, w którym klient posiada konto, jednak zawsze wynika to z jasnych i konkretnych zasad wskazanych w PSD II. Skutkuje to np. tym, że w trakcie płatności kartą w internecie, klient może zostać poproszony o wpisanie dodatkowego kodu z SMS-a wysłanego na jego numer telefonu lub potwierdzenie transakcji w bankowości mobilnej.

Zmiany wynikające z SCA można również zauważyć podczas płatności kartą na terminalu w sklepie tradycyjnym. Przyzwyczajeni do tego, że przy płatnościach zbliżeniowych o wartości poniżej 100 zł nie trzeba ich autoryzować za pomocą kodu PIN, zgodnie z regułami SCA, w określonych przypadkach możemy zostać poproszeni o jego wpisanie, nawet jeżeli transakcja jest poniżej wspomnianego wcześniej limitu.

Tak niewielkie niedogodności są jednak bardzo niewygórowaną ceną za zdecydowany wzrost poziomu bezpieczeństwa płatności bezgotówkowych i skuteczną eliminację nieautoryzowanych transakcji.

Bankowość otwarta, czyli odpowiedź na zmiany zachowań konsumentów

Open banking to nowy trend, regulacja i praktyka bankowa, która zapewnia zewnętrznym dostawcom usług finansowych otwarty dostęp do bankowości konsumenckiej, transakcji i innych danych finansowych z banków i innych instytucji finansowych za pośrednictwem interfejsów programowania aplikacji (API).

Piotr **Siuda**
Head of Financial Services
Strategic Business Unit
w Capgemini

Otwarta bankowość wymaga od banków współdzielenia danych klientów, takich jak konta, transakcje, produkty bankowe czy inne informacje finansowe z dostawcami zewnętrznymi. Otwarte interfejsy (open API) z kolei są coraz częściej udostępniane podmiotom trzecim w celu zaoferowania konsumentom nowoczesnych usług, banki coraz częściej współpracują z FinTechami, specjalistycznymi firmami technologicznymi.

Nowe możliwości

Taka otwartość rodzi zarówno zagrożenia, związane z zapewnieniem bezpieczeństwa danych czy utratą części dotychczasowych źródeł dochodów, jak i nowe możliwości dla banków.

Do tych ostatnich należy udostępnianie klientom zaawansowanych usług, na przykład zarządzania finansami osobistymi w czasie rzeczywistym na wszystkich posiadanych przez klienta rachunkach, we wszystkich bankach. Warto dodać, że to właśnie zadowolenie klienta odgrywa obecnie kluczową rolę na rynku bankowości detalicznej. To, z czym zmagają się obecnie banki i w ogólnym ujęciu branża finansowa, to bardzo dynamiczny wzrost oczekiwań klientów. Wyzwanie to wzrasta w miarę rozwoju organizacji FinTech, które bardzo szybko wpływają na branżę – banki muszą dziś doskoczyć do tego wysokiego poziomu. Z tegorocznego badania Capgemini – World Retail Banking Report 2022 – wynika, że znaczna większość klientów (aż 75 proc. z próby 8 tys. badanych) wskazuje, że bardzo docenia i czerpie przyjemność z doświadczeń i interakcji, w jakie wchodzi z organizacjami typu FinTech. W związku z tym, że klienci mogą dziś zmienić dostawcę usług bankowych za jednym kliknięciem myszki, banki powinny w większym stopniu wykorzystywać dane i sztuczną inteligencję (AI), aby dostosowywać doświadczenia klientów, tworzyć silniejsze więzi i maksymalizować wartość klienta. Aby dotrzymać kroku konkurentom, tradycyjne instytucje będą musiały przemyśleć swoje modele biznesowe i skupić się na zwiększaniu zaangażowania klientów.

Zaufanie

Mocną stroną banków jest integralność i niezawodność usług oraz zaufanie. To, na czym dziś muszą skupić się te instytucje to zdolność angażowania użytkownika, dawanie mu dodatkowych wartości. Przyzwyczajeni do szybkich i prostych usług online, konsumenci oczekują, że ich bank zaproponuje im proaktywne podejście oraz spersonalizowaną i wieloaspektową obsługę. Kilka lat temu pojawiły się organizacje FinTech, które obserwowały działania bankowe, przemyślały je i zaproponowały lepsze doświadczenia. Dziś banki powinny zrobić to samo, prowadząc do połączonego, omnichannelowego doświadczenia z myślą o użytkowniku. Nie chodzi jednak o to, by te instytucje budowały wszystko od zera – metodą na „pójście z duchem czasu" i odpowiedzenie na oczekiwania klientów jest współpraca z organizacjami technologicznymi, która pozwoli wejść na zdigitalizowaną ścieżkę.

Mówiąc jednak o trendach, należy wspomnieć o tym, że mimo iż open banking nie osiągnął jeszcze dojrzałości, sektor usług finansowych już teraz wkracza w nową fazę innowacji, określaną jako „Open X". Będzie ona wymagała głębszej współpracy i specjalizacji, dlatego banki oraz inne podmioty ekosystemu finansowego już muszą zacząć planować zmianę i odpowiednio rozwijać swoje modele biznesowe.

Coraz skuteczniej

Open X ma być bardziej skuteczną, ustrukturyzowaną formą współpracy, wspieraną przez standaryzację interfejsu API i wspólną analizę danych klientów. Era Open X stworzy zintegrowany rynek z wyspecjalizowanymi rolami dla każdego uczestnika, który umożliwi bezproblemową wymianę danych i usług, poprawę jakości obsługi klienta i szybsze wprowadzanie innowacji produktowych. Czeka nas ewolucja rynku finansowego w skali, jakiej wcześniej nie zakładaliśmy. Open banking jest tylko jednym z elementów tego szerokiego krajobrazu. Oznacza to, że banki, które już teraz miewają problem z otworzeniem się na strony trzecie, będą musiały bardzo głęboko wejść w kooperację z FinTechami, a FinTechy będą musiały wykorzystać zasięg banków, żeby szerzej zaistnieć na rynku. Strony nadal mają trudności z wzajemnym zrozumieniem, wykazują też obawy związane z bezpieczeństwem danych. Zarówno banki, jak i FinTechy mają dużo pracy do wykonania, aby były w pełni gotowe na przyszłość. Zintegrowane organizacje, czyli takie, które wykonują wszystkie funkcje samodzielnie, bez współpracy lub wykorzystywania innych firm w ekosystemie (jak wiele banków dziś), prawdopodobnie będą miały trudności z dopasowaniem czasu wprowadzania produktów na rynek do wyspecjalizowanego otoczenia. Będzie im również trudno sprostać wyjątkowym wymaganiom klientów – dlatego już dziś muszą rekrutować odpowiednie talenty, wykorzystywać dane i technologię oraz współpracować z FinTechami, aby zapewnić wewnętrzne możliwości konkurencyjnego dostarczania odpowiednich usług w obecnym scenariuszu otwartej bankowości.

> ”
>
> Open X ma być bardziej skuteczną, ustrukturyzowaną formą współpracy, wspieraną przez standaryzację interfejsu API i wspólną analizę danych klientów. Era Open X stworzy zintegrowany rynek z wyspecjalizowanymi rolami dla każdego uczestnika.

Wzmożona czujność

Wszystkie najnowsze rozwiązania technologiczne wymagają od banków wzmożonej czujności i specjalistycznych systemów, zapobiegających nadużyciom i wyłudzeniom. Banki muszą zatem nie tylko jak najszybciej wdrażać nowe procedury uwierzytelniania i autoryzacji, takie jak biometria i biometria behawioralna, lecz też proaktywnie inwestować w strategie zarządzania ochroną danych i cyber-ryzykiem – co może decydować o ich przewadze konkurencyjnej w przyszłości.

To, co stanowi dzisiaj zagrożenie dla banków, może okazać się ich szansą na rozwój i finalne zwiększenie zysków. Banki powinny koncentrować swoje działania na strategicznym wykorzystaniu danych w celu poprawy obsługi klienta oraz na wykorzystaniu nowych źródeł przychodów. Współpraca z partnerami technologicznymi może otworzyć ogromne możliwości dla instytucji finansowych.

Prościej i szybciej

Otwarta bankowość to unijny standard umożliwiający klientom dostęp do salda czy historii rachunków w jednym miejscu, nawet jeśli dane pochodzą z różnych banków. Jego coraz powszechniejsze wykorzystywanie wspiera także rozwój sektora ecommerce, ponieważ dzięki rozwiązaniom open banking, proces kredytowy staje się prostszy i szybszy. Z nowych technologii od lat konsekwentnie korzysta Inbank. W Polsce ocena wniosku i wydanie decyzji kredytowej, dzięki automatyzacji całego procesu, zajmuje w nim niespełna osiem sekund.
Wydruki historii kredytowej, wyszukiwanie, pobieranie danych i udostępnianie ich online to już przeszłość. Dzięki rozwiązaniom z zakresu open banking, banki mogą mieć dostęp do wszystkich niezbędnych informacji w sposób automatyczny. Oczywiście za zgodą klienta, który oszczędza czas. Zalety otwartej bankowości to m.in. uproszczenie procesu kredytowego oraz zarządzanie przez klienta środkami własnymi z różnych banków w jednym miejscu.

Finanse firmowe lub osobiste w jednym miejscu
„Otwarta bankowość to szybki i bardziej kompleksowy wgląd w sytuację finansową firmy lub klienta indywidualnego, bez konieczności logowania się do wielu kont. Z punktu widzenia banku, takie usprawnienia i automatyzacje procedur sprawiają, że manualna ocena wiarygodności klienta ubiegającego się o kredyt niebawem będzie należała u nas do rzadkości" – tłumaczy Tomasz Rzeski, Country Sales Manager Oddziału Inbank w Polsce.

Młodzi Polacy najczęściej korzystają z banków i e-sklepów

Ponad 80 proc. Polaków w wieku 18-34 lat sięga w internecie po płatności online i bankowość mobilną. Z usług finansowych korzystają najczęściej za pośrednictwem banków, e-sklepów i platform sprzedażowych. Takie postawy sugerują, że jednym z większych beneficjentów rozwoju otwartej bankowości, który gwarantuje unijna dyrektywa PSD2, może być branża e-commerce. Tak wynika z raportu spółki Easy Check i Krajowego Rejestru Długów.
Spośród usług finansowych, z których korzystamy za pośrednictwem internetu, Polacy najczęściej wybierają płatności online (79 proc.) oraz bankowość mobilną (74 proc.). Pierwszego rozwiązania najchętniej używają ludzie młodzi w wieku 18-34 lata (ponad 83 proc.). Podobnie wygląda to w przypadku bankowości online. W tym przypadku odsetek młodych Polaków, którzy z niej korzystają wynosi około 80 proc. Ta statystyka maleje wraz ze wzrostem wieku ankietowanych.
Zapytani o to, w jakich instytucjach korzystają z zaznaczonych wcześniej usług finansowych, młodzi ankietowani najczęściej wskazują na banki (72 proc.) i serwisy typu marketplace np. Allegro i OLX (69 proc.). Wysoko na liście znalazły się również sklepy internetowe, które wybrało ponad 63 proc. badanych. Co ciekawe, najmłodsi w wieku 18-24 lata są grupą, w której banki znalazły się dopiero na trzecim miejscu (67 proc.). Częściej korzystają w sieci ze sklepów online (75 proc.) i serwisów sprzedażowych (73 proc.).

Zmiany zachowań konsumentów a open banking – jak dobrze wykorzystać dostępne dane?

Transformacja cyfrowa dzieje się na naszych oczach. Zgodnie z prognozami zawartymi w raporcie PwC w 2026 roku wartość brutto polskiego rynku handlu e-commerce ukształtuje się na poziomie 162 mld zł. To wzrost o średnio 12 proc. rocznie.

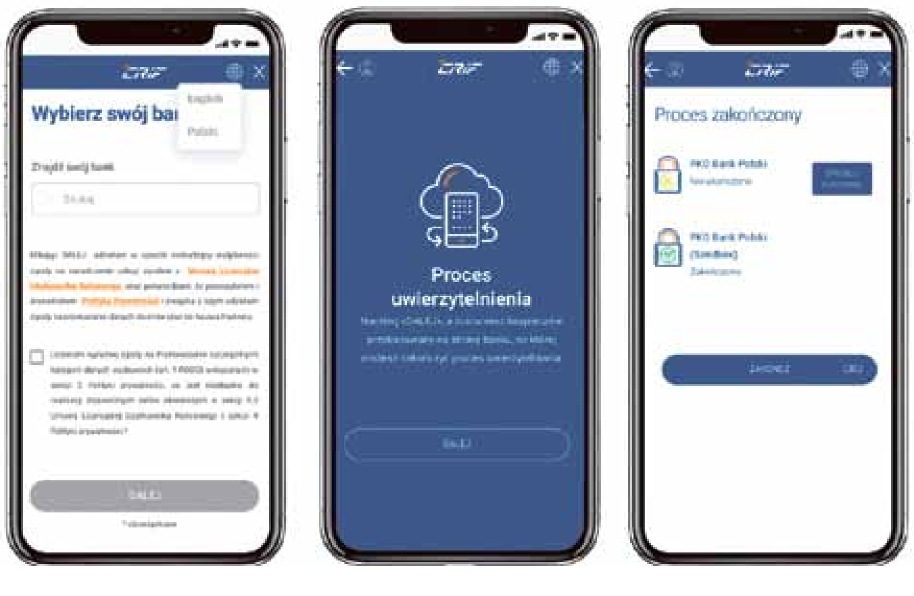
Źródeł przyrostu możemy upatrywać w pandemii, która w nagły sposób przyspieszyła wejście wielu organizacji w świat online. To ogromne wyzwanie, ale także szansa na dotarcie i pozyskanie nowych klientów, którzy przyzwyczaili się już do zamawiania produktów czy usług, nie opuszczając swojego domu.

Nowa grupa konsumentów – szansa czy wyzwanie?
Oprócz klientów, którzy tak jak organizacje, musieli przystosować się do nowej rzeczywistości, istnieje spora grupa tych, którzy w świecie online się urodzili. Mowa tu o pokoleniu Z zdecydowanie różniącym się od tych poprzednich. Różnice te są coraz bardziej widoczne także w sferze zachowań zakupowych i sposobie zarządzania ich finansami.
To zazwyczaj osoby w wieku 18-25 lat, które studiują, ale bardzo często również pracują, dzięki czemu osiągają stosunkowo spore dochody. Technologie mają we krwi – na co dzień korzystają z mediów społecznościowych. Zamiast brać mieszkanie na kredyt – wolą je wynajmować. Nie kupują samochodów – biorą je w leasing lub korzystają z elektrycznych hulajnóg. Nie boją się pożyczać – często korzystają z możliwości, jakie daje odroczona płatność czy raty. Są mniej ostrożni od poprzednich pokoleń – bardziej ufają swoim decyzją, które przy małej wiedzy finansowej mogą wpędzić ich w spirale zadłużenia. Kwotowo nie są najbardziej zadłużoną grupą Polaków, natomiast dynamika ich wzrostu zadłużenia jest największa w porównaniu do innych.

Open banking – innowacyjne podejście do zarządzania finansami
Naprzeciw Pokoleniu Z i innym konsumentom, a także firmom, wychodzi otwarta bankowość. Nazwać nią możemy ogół usług i technologii w obszarze finansów oparty na otwartych interfejsach programistycznych (Open API), które umożliwiają stronom trzecim (ang. Third Party Providers) wytworzenie aplikacji czy serwisów wykorzystujących dane klientów udostępnianie przez instytucje finansowe za wyraźną zgodą konsumentów. Dostęp do transakcji konsumentów to nieograniczone źródło wiedzy o nich. Jednak same surowe dane nie pomogą nam w znalezieniu ciekawych spostrzeżeń. Aby je wydobyć, musimy te transakcje odpowiednio zagregować i przeanalizować.

Kategoryzacja transakcji podstawą personalizacji ofert
Narzędziem, które nam w tym pomoże, są silniki kategoryzacji. To mechanizmy oparte o algorytmy uczenia maszynowego, które opisują w sposób biznesowy każdą transakcję, np. subskrypcję platformy streamingowej, zakupy w Lidlu czy spłatę zadłużeń. Im z większą precyzją możemy opisać te transakcje, tym lepiej będziemy mogli poznać nawyki zakupowe naszego konsumenta i zaoferować mu najbardziej dopasowane produkty, zwiększając tym prawdopodobieństwo, że skorzysta on z naszej oferty.
Takie możliwość daje rozwiązanie N.E.O.S. dostarczane przez CRIF Sp. z o.o. Silnik kategoryzacji oparty o algorytmy sztucznej inteligencji pozwala na opisanie każdej transakcji na prawie 200 sposobów. Dzięki takiemu dostępowi do danych za pomocą otwartej bankowości możemy „szyć" oferty na miarę potrzeb każdego klienta. Co więcej, możemy oferować klientom zniżki na produkt lub usługę, z której korzystają, albo której właśnie w tym momencie potrzebują. Wszystko to w jednym cyfrowym doświadczeniu użytkownika – od zaproponowania produktu lub usługi, po jego wybór i możliwość szybkiej i łatwej płatności, np. przez płatność odroczoną, w środowisku cyfrowym – naturalnym dla Pokolenia Z.
Dowiedz się, jak na naszym rozwiązaniu może skorzystać Twoja firma – umów się na crif.pl/neos-um proc.C3 proc.B3w-si proc.C4 proc.99-na-demo/ już dziś!

Otwarta bankowość a pokolenie Z
Młodzi ludzie mają często po kilka rachunków w różnych bankach, kredyty konsumenckie i zobowiązania, o których czasem zapominają. Rozwiązaniem tego problemu jest wykorzystanie otwartej bankowości w formie aplikacji typu manager finansów, które dają możliwość zintegrowania w jednym widoku wszystkich swoich kont, co pozwala odzyskać kontrolę nad swoimi finansami i nauczyć się nimi zarządzać.
Aby sprawdzić, czy nasze przypuszczenia dotyczące przedstawicieli Pokolenia Z są prawdziwe, CRIF Sp. z o.o. we współpracy z Banking Magazine oraz Uniwersytetem Ekonomicznym we Wrocławiu przygotowuje badanie świadomości finansowej młodych Polaków pod kierownictwem dr hab. Barbara Mróz-Gorgoń, prof. UEW, które pozwoli uzyskać szczegółowy obraz podejścia Pokolenia Z do zarządzania swoimi finansami, a także zbadania ich wiedzy na ten temat. Raport z badania będzie dostępny na początku czerwca.



MATERIAŁ PARTNERA

WDRAŻANIE NOWOCZESNYCH ROZWIĄZAŃ CYBEROCHRONNYCH W SEKTORZE FINANSOWYM

Cyfrowa transformacja wpływa na sposób, w jaki pracujemy, żyjemy i korzystamy z usług – także finansowych. Bankowość zorientowana na klienta i zapewniająca bezproblemowe korzystanie z oferowanych przez bank usług bazuje na zaufaniu.

Wojciech **Ciesielski**

menedżer ds. sektora
finansowego, Fortinet

Instytucje finansowe przechowują nie tylko oszczędności klientów, ale także informacje umożliwiające ich identyfikację. W związku z tym bezpieczeństwo tych zasobów odgrywa kluczową rolę w utrzymaniu zaufania. Aby skutecznie chronić dane, sektor finansowy powinien inwestować w nowoczesne rozwiązania ochronne, bazujące na sztucznej inteligencji i uczeniu maszynowym.

Nadążyć za zmianami

Firmy oraz instytucje działające w sektorze finansowym są narażone na ataki głównie ze względu na fakt, że gromadzone przez nie dane finansowe i osobowe osiągają wysoką wartość na czarnym rynku. Dodatkowo wyciek danych osobowych może skutkować kradzieżą tożsamości klientów. Zwiększona liczba ataków na ten sektor ma związek m.in. ze zwiększeniem zakresu pracy zdalnej. Osoby wykonujące obowiązki z domu łączą się z firmową siecią za pośrednictwem często nieodpowiednio chronionych urządzeń.

O ile zarządzanie tradycyjnym ryzykiem, związanym z przetwarzaniem wrażliwych danych, jest już prawdopodobnie częścią strategii IT każdego przedsiębiorstwa świadczącego usługi finansowe, o tyle zarządzanie nagłym wzrostem ilości pracowników zdalnych już nie. Przeciwdziałanie zagrożeniom związanym z nowym modelem pracy w sektorze usług finansowych było dużym wyzwaniem, ale na powodzenie tej operacji może skutecznie wpłynąć wykorzystanie odpowiednich, innowacyjnych technologii ochronnych przez zespoły ds. bezpieczeństwa.

Sektor finansowy musi też patrzeć w przyszłość, jeśli chodzi o dostępność specjalistów ds. cyberbezpieczeństwa i zaplanować działania zmierzające do złagodzenia konsekwencji ich powszechnego niedoboru. Już teraz, wg raportu Fortinet 2022 Cybersecurity Skills Gap, w 8 na 10 badanych firmach miało miejsce przynajmniej jedno naruszenie, które można przypisać brakowi kwalifikacji lub wiedzy w zakresie cyfrowej ochrony.

Sztuczna inteligencja – teraźniejszość i przyszłość cyberochrony

W tej sytuacji osoby odpowiedzialne za bezpieczeństwo IT w bankach i innych podmiotach sektora finansowego coraz częściej kierują swoją uwagę w stronę rozwiązań bazujących na sztucznej inteligencji oraz uczeniu maszynowym, a także umożliwiających automatyzację procesów ochronnych. Pozwala to na znaczną oszczędność czasu pracy personelu, co jest ważne w przypadku przeciążonych pracą zespołów IT, ale też na wyeliminowanie ludzkich błędów w łańcuchu zabezpieczeń. Jedno z największych wyzwań przy wykorzystaniu sztucznej inteligencji i uczenia maszynowego leży w jakości pozyskiwanych informacji o zagrożeniach. Mechanizmy uczenia maszynowego zasilane są dużymi ilościami danych pozyskiwanych m.in. z urządzeń IoT oraz aplikacji przewidujących zdarzenia w sieci. Natomiast często, zanim administratorzy sieci odkryją zagrożenie, na skuteczne zareagowanie jest już zbyt późno. Problem ten można rozwiązać poprzez automatyczne przekazywanie informacji pomiędzy rozwiązaniami wykrywającymi zagrożenia i blokującymi je. Automatyzacja pozwoli też zespołom IT poświęcać więcej czasu na analizę zdarzeń w celu planowania lepiej zorganizowanych działań prewencyjnych.

Bazujące na sztucznej inteligencji systemy cyberbezpieczeństwa będą stale dostosowywać się do zmieniających się źródeł, celów, metod i skali ataków.

EDR i XDR – nowa kategoria rozwiązań ochronnych

Przykładami systemów, które bazują na sztucznej inteligencji oraz służą do automatyzacji procesów zabezpieczających, są narzędzia z kategorii XDR (*eXtended Detection and Response*), w których połączone ze sobą i rozwinięte zostały koncepcje EDR (*Endpoint Detection and Response*) oraz NDR (*Network Detection and Response*). Służą one do ochrony odpowiednio urządzeń końcowych (komputerów, telefonów, tabletów) oraz sieci.

XDR zapewnia inteligentny i zautomatyzowany sposób łączenia w jednym systemie funkcji zwykle dostarczanych przez odizolowane rozwiązania. Ponadto, ułatwia zarządzanie złożonymi środowiskami zabezpieczeń IT, na które składają się rozwiązania od wielu dostawców. Narzędzie to koncentruje się na badaniu informacji o zdarzeniach pochodzących z różnych produktów i nie wymaga indywidualnego zaangażowania zespołów odpowiedzialnych za ochronę środowiska IT. Sprawia to, że zajmujący się tym eksperci mają więcej czasu, aby dokładniej skupić się na sprawach strategicznych w kontekście całego przedsiębiorstwa. Pomaga też firmie skutecznie konkurować na rynku, a jednocześnie, dzięki konsolidacji funkcji obecnych dotychczas w różnych narzędziach, rozwiązuje problemy związane ze wzrostem liczby dostawców produktów ochronnych.

Jak działa XDR? Przykłady zastosowań

Poniżej znajduje się kilka przykładów podejrzanego zachowania, które uruchamia proces śledztwa prowadzony przez narzędzie bazujące na sztucznej inteligencji – FortiXDR. W wielu przypadkach są to rodzaje zachowania, które mogły nie zostać wykryte wśród innych informacji o potencjalnych zagrożeniach.

– **Nieudane próby logowania** – Użytkownicy często zapominają lub błędnie wpisują dane uwierzytelniające, co sprawia, że powtarzające się nieudane próby logowania są powszechnym zjawiskiem. Jednak powtarzające się próby logowania mogą być również jedną z faz cyberataku i wymagają dalszej analizy. Użycie narzędzia XDR pozwala wykryć anomalie, takie jak niemożliwe do odbycia podróże (biorąc pod uwagę niespójności związane z lokalizacjami, w których przebywa logująca się osoba). Jeśli istnieje dowód, że doszło do cyberataku, uruchamiana jest wcześniej zdefiniowana reakcja – od prostego powiadomienia o incydencie, aż po wygaśnięcie danych uwierzytelniających użytkownika.

– **Potencjalny atak phishingowy** – Poczta elektroniczna wciąż pozostaje głównym wektorem ataków, a jedno nieopatrzne kliknięcie w złośliwy link w phishingowej wiadomości może mieć poważny wpływ na losy przedsiębiorstwa. Narzędzie ochronne jest w stanie zastosować mechanizmy rozszerzonej analityki wobec każdej wiadomości e-mail, aby zidentyfikowa te, które zawierają adresy URL prowadzące do złośliwego kodu. Gdyby doszło do naruszenia bezpieczeństwa, to predefiniowane działania obejmują kwarantannę urządzeń, na których zostały zainstalowane złośliwe pliki, aktualizację informacji o zagrożeniach znajdujących się w złośliwych plikach, witrynach internetowych itd.

– **Wykrywanie nieautoryzowanych urządzeń** – Inną popularną metodą ataku, wykorzystywaną przez cyberprzestępców, jest infiltracja urządzeń IoT. XDR zapewnia głęboki wgląd w sprzęt z tej kategorii i umożliwia zidentyfikowanie prawdziwych źródeł aktywności.

Podsumowanie

Koncepcja XDR zyskuje na popularności. Większość obecnych na rynku rozwiązań zapewnia jednak tylko rozszerzone procedury wykrywania zagrożeń. Chociaż są to oczywiście kluczowe elementy, mogą okazać się niewystarczające. Na szczęście odpowiednio skonfigurowany system, bazujący na sztucznej inteligencji, może wykrywać i niwelować incydenty szybciej i dokładniej. Jesteśmy na takim etapie cyfrowej transformacji, że nadszedł już odpowiedni czas, aby przestać podchodzić reaktywnie do incydentów bezpieczeństwa, a wprowadzać proaktywne zmiany w postawach i strategiach ochronnych. Odpowiedniej klasy rozwiązanie XDR pomaga osiągnąć ten cel.

Polacy a open banking

Zbigniew **Hordecki**

prezes zarządu, Easy Check

Od trzech lat funkcjonujemy w rzeczywistości zdefiniowanej przez dyrektywę PSD2, która otworzyła drogę do wprowadzenia szeregu nowych usług i przyczyniła się do rozwoju otwartej bankowości. Pomimo tego, że cały czas oswajamy się z możliwościami, jakie nam to gwarantuje, już teraz, na podstawie wyników badań zleconych przez Easy Check, wiemy dużo na temat tego, jaki stosunek do open bankingu mają Polacy.

Jak wynika ze wspomnianych badań, ponad połowa z nas jest skłonna udostępnić historię transakcji rachunku bankowego innym podmiotom w zamian za określone korzyści. Wśród tych najczęściej wskazujemy na korzystniejszą cenę produktu, ofertę specjalną lub przyspieszenie procesu zakupowego (np. poprzez szybszą weryfikację tożsamości). Usługodawca, który będzie umiał odpowiedzieć na te potrzeby, zyska dostęp do wartościowych informacji.

To istotne z punktu widzenia kierunku rozwoju usług. Na podstawie udostępnionych i odpowiednio uporządkowanych danych sprzedający są bowiem w stanie dokonać rzetelnej oceny sytuacji klienta oraz ocenić jego preferencje zakupowe, które pozwolą dopasować ofertę oraz produkt do jego możliwości (np. ubezpieczenie lub finansowanie). Informacje z rachunku bankowego pozwolą im także lepiej ocenić ryzyko i zadbać o swoje bezpieczeństwo finansowe.