WYZWANIA INFORMATYKI BANKOWEJ

Redakcja
Andrzej Kawiński
Andrzej Sieradz

2016

PUBLIKACJA EUROPEJSKIEGO KONGRESU FINANSOWEGO

Wyzwania informatyki bankowej 2016

© Copyright by
Instytut Badań nad Gospodarką Rynkową
-- Gdańska Akademia Bankowa
80-227 Gdańsk, ul. Do Studzienki 63
tel. 58 524 49 01
fax. 58 524 49 09
www.gab.com.pl
www.efcongress.com
e-mail: poczta@gab.com.pl

Redaktorzy: Andrzej Kawiński, Andrzej Sieradz

Opracowanie redakcyjne: Wojciech Gryciuk

Projekt graficzny: TOFU

Skład: Łukasz Sitko

ISBN 978-83-88835-27-8

Spis treści

Wstęp 7

Mariusz Zarzycki
Digital banking 11

Bartłomiej Nocoń, Bartosz Zborowski
Budowanie pozytywnego doświadczenia klienta w bankowości 23

Andrzej Sieradz, Grzegorz Kuliszewski
Bank w chmurach 37

Piotr Puczyński
CRM czyli w poszukiwaniu Świętego Graala 51

Magda Dziewguć, Marta Guzek, Michał Olczak
FinTech – wróg czy przyjaciel 71

Maciej Łuczak
Blockchain 83

Sebastian Ptak
Przyszłość systemów płatniczych 105

Piotr Pinchinat-Miernik, Paweł Mucha, Artur Wojtczuk, Krzysztof Pycia
Bankowa rewolucja na rynku płatności zobowiązań 123

Andrzej Kawiński
Jak obniżyć koszty obrotu gotówki? 135

Andrzej Gibas, Karol Mazurek
Centralny system bankowy na nowej platformie 149

Aleksander P. Czarnowski
Cybersecurity – moda, mit czy rzeczywistość? 163

Adam Marciniak
Bankowy CERT – nowa broń w walce z cyberprzestępczością 181

Maciej Gawroński, Sławomir Szepietowski, Adam Łukaszewski
PSD 2 – nowa wersja dyrektywy w sprawie usług płatniczych 197

Artykuły prezentują osobiste opinie i poglądy autorów
i nie powinny być odbierane,
jako oficjalne stanowisko pracodawców.

Wstęp

Oddajemy w Państwa ręce już trzecie opracowanie dotyczące wpływu technologii informatycznych na sektor finansowy. Wiele zagadnień z poprzednich edycji, takich jak np. cyberbezpieczeństwo, jest nadal na tyle aktualnych, że postanowiliśmy powtórzyć je w bieżącym wydaniu, chociaż w rozszerzonej wersji. Książka zawiera jednak także sporo nowych tematów, które, naszym zdaniem, będą mieć coraz większe znaczenie w najbliższych latach.

Dynamiczne zmiany zachodzące w modelu biznesowym powodują, że współpraca biznesu z działami IT i bezpieczeństwa jest obecnie głównym motorem rozwoju sektora finansowego. Cieszy zatem inicjowanie współpracy banków w ramach Związku Banków Polskich w zakresie bezpieczeństwa i wymiany informacji, co do zagrożeń cybersecurity.

Nowe tendencje w opracowywaniu produktów i usług finansowych, czasami oferowanych niekoniecznie przez „tradycyjne" organizacje finansowe, są konsekwencją dynamicznie rozwijających się usług opartych na nowych technologiach IT, zwłaszcza tych mobilnych. W tym roku zwracamy uwagę na coraz bardziej dynamicznie rozwijający się rynek FinTech, a także na wysyp nowych rozwiązań informatycznych.

Wystarczył niespełna rok a coraz powszechniej mówi się nie tylko o konieczności zastosowania całkowitej zmiany podejścia do klienta i przeniesienia usług finansowych do przestrzeni określanej jako „digital", ale też i o tym, że jest to nieuniknione. W tegorocznej edycji opracowania kontynuujemy dyskusję na ten temat.

Podobnie, jak w poprzednich edycjach, zależało nam na przeanalizowaniu starych i nowych wyzwań przede wszystkim z punktu widzenia przyszłości usług finansowych, a nie pojedynczego uczestnika rynku. Właśnie dlatego na liście omówionych zagadnień znalazły się takie tematy, jak bankowość mobilna, bezpieczeństwo transakcji płatniczych, blockchain technology, współpraca spoza-bankowymi uczestnikami rynku płatniczego czy wymiana

technologiczna związana z wielokanałowością dystrybucji produktów i usług finansowych (omnichannel).

Zupełnie nowym zagadnieniem jest zbliżająca się rekomendacja PSD2. Mimo tego, że ostateczne wymagania technologiczne w chwili publikacji opracowania nie są jeszcze znane uznaliśmy, że regulacja ta ma fundamentalny wpływ na przyszły model biznesowy banków w Polsce i Europie.

Funkcjonowanie instytucji finansowych nie jest obecnie możliwe bez informatyki. Aktualne trendy rynkowe i technologie umożliwiają z jednej strony zmniejszenie kosztów IT, a z drugiej przyspieszenie cyklu rozwoju produktów, co w efekcie prowadzi do tworzenia bardziej nowoczesnych usług dla klientów. Nie wszyscy uczestnicy tego rynku są jednak pewni, czy już warto przenosić rozwiązania IT do chmury obliczeniowej. Warto o tym rozmawiać, szczególnie w kontekście nowych obciążeń, w tym podatku bankowego i dodatkowych wpłat na BFG.

Naczelną intencją publikacji było przedstawienie skomplikowanych zagadnień rynku sektora finansowego w taki sposób, by były zrozumiałe dla szerokiego grona odbiorców, a szczególnie tych, którzy są użytkownikami tego typu rozwiązań lub decydentami. Zależało nam też, aby poruszone w publikacji zagadnienia stosunkowo szeroko omawiały wyzwania, które stoją przed informatyką bankową i mamy nadzieję, że nam się to udało.

Chcemy bardzo serdecznie podziękować wszystkim autorom za włożony trud i zaangażowanie w przygotowanie tegorocznej publikacji. Mamy nadzieję, że lektura zamieszczonych artykułów będzie dla Państwa inspiracją do własnych przemyśleń i decyzji.

Wyrazy podziękowania chcielibyśmy przekazać prof. Leszkowi Pawłowiczowi za wsparcie duchowe i cenne uwagi w czasie przygotowywania publikacji, a całemu zespołowi GAB za organizację całego przedsięwzięcia.

Andrzej Kawiński
Andrzej Sieradz

Mariusz Zarzycki

Dyrektor, Dział Doradztwa Informatycznego EY

Posiada ponad dwudziestoletnie doświadczenie zawodowe w zakresie zarządzania obszarem IT w największych polskich firmach, przede wszystkim w bankowości. Specjalizuje się w zarządzaniu IT, projektach wdrożenia i integracji systemów informatycznych, restrukturyzacji, a także zarządzaniu operacjami, zakupami i logistyką. Jest absolwentem studiów ekonomicznych na Uniwersytecie Łódzkim oraz bankowości i finansów na Uniwersytecie w Sztokholmie.

W latach 1993–1998 pracował w Powszechnym Banku Gospodarczym. Następnie przez 10 lat był związany z BRE Bankiem, gdzie pełnił funkcję dyrektorskie w departamentach Informatyki Bankowości Detalicznej (mBanku) oraz Rozwoju Technologii Informatycznych. W tym czasie był również dyrektorem Banku ds. Informatyki. W latach 2008–2010 był wiceprezesem Zarządu PKO BP, gdzie odpowiadał za obszar informatyki i usług. Równocześnie był członkiem Rady Nadzorczej Inteligo Financial Services. W latach 2011–2016 pełnił funkcję członka Zarządu Poczty Polskiej oraz przewodniczącego Rady Nadzorczej Postdata.

Mariusz Zarzycki, Ernst & Young

Digital banking

Ten stosunkowo nowy i coraz częściej używany termin nie doczekał się do dziś jednoznacznej definicji – nie ma nawet swojego hasła w Wikipedii (stan na początek kwietnia 2016 r.).

Pojawiają się opinie, że digital banking to kolejny modny, „sezonowy" termin, który za chwilę zniknie i zostanie zastąpiony nowym. Być może tak się stanie, jednak z pewnością nie zniknie zjawisko, które przy pomocy tego terminu się określa – przemożnego wpływu nowych technologii na rynek usług finansowych, banki i ich usługi, procesy wewnętrzne, pracowników i wreszcie klientów bankowości. Technologie otwierają zupełnie nowe możliwości, ale i wywołują poważne zagrożenia. Obserwujemy także rosnące tempo pojawiania się i upowszechniania nowych technologii. Dzieje się to w wyniku angażowania w ich rozwój coraz większych zasobów finansowych, wykorzystania zainstalowanej już infrastruktury, sprawniejszych metod wdrażania i coraz łatwiejszego przyswajania wywoływanych przez technologię zmian.

Funkcjonowanie banków w coraz bardziej i coraz szybciej „digitalizowanym" i złożonym świecie wymaga od nich całościowego, systematycznego podejścia do *digital banking* oraz zapewnienia zdolności do sprawnej reakcji na zmiany technologiczne, których często nie da się przewidzieć.

W ramach dyskusji prowadzonej w publikacjach i na forach dyskusyjnych kształtuje się szerokie rozumienie terminu *digital banking*. Dobrze odzwierciedla je ujęcie zaproponowane przez Johna Ginovsky'ego, edytora magazynu Banking Exchange[1]. Według niego *digital banking jest „zastosowaniem w banku nowych i rozwijających się technologii wraz z wprowadzeniem*

1 http://www.bankingexchange.com/blogs-3/making-sense-of-it-all/item/5187-what-really-is-digital-banking

związanych z tym zmian w relacjach z otoczeniem zewnętrznym oraz wewnątrz organizacji, w celu zapewnienia klientom skutecznie i efektywnie lepszej jakości usług i customer experience"[2].

Poniżej staram się zaledwie dotknąć różnych aspektów *digital banking*, ilustrując je zagranicznymi przykładami, aby następnie zaproponować jak bank może skutecznie nim zarządzać.

Szansa 1 – lepsze *customer experience*

Takie ujęcie jasno lokuje klientów w centrum uwagi. Ich zachowania i oczekiwania wobec banków ewoluują pod wpływem korzystania z nowych technologii i opartych na nich usług. Korzystając na co dzień z wygodnych, intuicyjnych i bezpłatnych serwisów internetowych oraz aplikacji mobilnych oczekują tego samego od usług bankowych. Ich oczekiwania zmieniają się też wraz ze zmianą pokoleniową, wchodzeniem w dorosłe życie pokolenia wyrosłego w dobie dojrzałego internetu (tak zwane pokolenie Y i ostatnio nawet Z) oraz mediów społecznościowych. Technologia pozwala dzisiaj na zbudowanie bliższych relacji z klientami i dostarczenie im niedostępnego dotychczas *customer experience.*

Bankom wprawdzie trudno jest czasem sprostać wymaganiom kształtowanym przez serwisy firm internetowych, ale mimo to znajdują się w lepszej, w stosunku do innych branż, pozycji. Mają bowiem ogromne ilości danych o klientach, które są niedostępne dla innych. Możliwości technologii analitycznych, algorytmy, wydajność maszyn i pojemność infrastruktury pozwalają na niedostępne do niedawna przetwarzanie ogromnych ilości danych, jakie banki zebrały na temat klientów i ich zachowań (głównie transakcji). Dane te, wraz z wykorzystaniem zewnętrznych źródeł i big data, pozwalają na doskonalenie algorytmów zarządzania ryzykiem i podejmowanie przez bank lepszych i natychmiastowych wręcz decyzji.

To również szansa na lepsze rozumienie sytuacji i potrzeb klientów oraz pomoc w zarządzaniu ich finansami, na oferowanie spersonalizowanych produktów, porad i ostrzeżeń w momencie, kiedy są dla klientów rzeczywiście potrzebne i wartościowe. Często oferty te rozszerzane są z sukcesem o różnorodne produkty i usługi niefinansowe. Przykładem sukcesu takiego podejścia

2 *Customer experience* rozumiany jako doznania, doświadczenia, zadowolenie klienta nie ma chyba dobrego i krótkiego polskiego odpowiednika.

jest turecki Garanti Bank i jego serwis iGaranti, który dla kilkuset tysięcy aktywnych klientów łączy mobilne serwisy bankowe z poradami dotyczącymi zakupów i z mediami społecznościowymi.

Banki (np. HSBC) zaczynają też wykorzystywać tak unikalną wiedzę do rozszerzania współpracy i doradztwa dla klientów korporacyjnych[3]. Mogą pomóc lepiej zrozumieć firmom obsługującym tych samych klientów ich zachowania i preferencje.

Bankowość mobilna jest obecnie najdynamiczniej rozwijającym się obszarem *digital banking*. Jest znakomitym przykładem jak szybko przełomowe innowacje – smartfon i platforma do tworzenia i dystrybucji aplikacji – mogą się błyskawicznie upowszechnić i zmodyfikować zachowania osób i firm. Serwisy mobilne po latach raczkowania i pozostawania w cieniu znalazły się nagle w centrum uwagi klientów banków. W ciągu zaledwie kilku lat bankowość mobilna stała się na tyle popularna, że nie jest zapewne odosobnionym przypadkiem – weźmy przykład banku Halifax, w którym ilość transakcji mobilnych jest już ponad dwukrotnie wyższa niż transakcji wykonywanych na PC.

Prawdziwą szansą, ale i wyzwaniem, jest naprawdę osobisty charakter smartfonów, które klienci stale mają przy sobie i wykorzystują niezależnie od tego, gdzie się znajdują. Otwiera to możliwość znacznie częstszej interakcji z klientami, składania precyzyjnie dobranych propozycji lub porad, np. w kontekście znajomości ich aktualnej lokalizacji. Wymaga jednak wyczucia granic prywatności i poczucia wolności wyboru, których przekroczenie, nawet z najbardziej korzystną propozycją, może wywołać nieoczekiwane negatywne reakcje. Znanym przykładem zbyt daleko posuniętych działań spoza branży bankowej jest bezpłatna dystrybucja przez Apple albumu „Song of Innocence" zespołu U2 w 2014 r., która spotkała się z oburzeniem wielu „obdarowanych" użytkowników iTunes. Wyzwaniem dla „banku w smartfonie" jest też odpowiedni dobór i sformatowanie usług dostępnych w „tradycyjnym" kanale internetowym, tak aby nie generować zbyt wielu transakcji, dostosować je do innej wydajności, wymiarów i ergonomii urządzeń mobilnych.

Omnichannel stara się sprostać kolejnemu oczekiwaniu klientów, jakim jest zharmonizowanie usług dostępnych w różnych kanałach dystrybucji, uwzględniając specyfikę i ograniczenia obsługi w oddziale, kanale mobilnym, „internetowym", strefach samoobsługowych czy *contact center*. Celem jest zapewnienie spójności informacji, *customer experience*, a jednocześnie skłanianie klientów do

3 EY-and-BBA-The-way-we-bank-now-A-world-of-change

samodzielnego wykonywania możliwie wielu transakcji (najlepiej „predefiniowanych" przez bank na podstawie analizy dostępnych informacji), uwalniając czas pracowników do zadań sprzedażowych i doradczych. Utrudnia to rozproszone z reguły zarządzanie kanałami dystrybucji i obsługujące je rozwiązania informatyczne, pochodzące od różnych dostawców.

Media społecznościowe, z reguły najczęściej używane przez klientów serwisy internetowe, pozwalają na budowanie wizerunku banku, utrzymywanie z nimi dialogu, uzyskiwanie informacji zwrotnej szybko i tanio w formie, która może być automatycznie analizowana. Włączane w serwisy internetowe i mobilne banków, są też coraz częściej wykorzystywane do wygodnego dla klientów wzajemnego rozliczania drobnych kwot. Wymagają jednak stałej uwagi i moderowania wątków oraz błyskawicznej reakcji w sytuacjach kryzysowych.

Przykładem innowacji łączącej w sobie wiele opisanych powyżej aspektów *digital banking* jest oferowane przez australijski Commonwealth Bank sklepom, stacjom benzynowym, restauracjom czy punktom usługowym rozwiązanie Albert[4]. Jest to tablet, który służy jako mobilny terminal płatniczy z zestawem aplikacji. Pozwala merchantom m.in. wystawiać i wysyłać faktury, zarządzać zapasami, analizować profil i zachowania klientów oraz być z nimi w kontakcie przez media społecznościowe lub mail. Aplikacje (obecnie 15) można pobrać z platformy Appbank, która, co ciekawe i ważne, została także udostępniona zewnętrznym twórcom aplikacji.

Szansa 2 – sprawniejsze usługi i tańsze procesy

Najlepiej zaprojektowane systemy i bogate funkcjonalnie aplikacje bankowości internetowej czy mobilnej nie usatysfakcjonują klientów, jeżeli bank nie zareaguje na ich działania natychmiast i to niezależnie od pory dnia (tryb 24/7). Wzrastające oczekiwania w tym zakresie kształtują sklepy internetowe, serwisy rezerwacyjne i finansowe, których modele biznesowe opierają się na działaniu w trybie rzeczywistym.

Digital banking wymaga zautomatyzowanych, pozbawionych papieru i podpisów procesów operacyjnych i decyzyjnych, ale także w coraz większym stopniu administracyjnych. Ich budowie sprzyjają sprawniejsze i tańsze technologie, *digital managing* i *e-podpisy*, rozwiązania klasy *document managment*, zaawansowane systemy decyzyjne oraz zmiany w regulacjach i zakresie

4 https://www.commbank.com.au/business/merchant-services/eftpos-options/in-store/albert.html

informacji dostępnej elektronicznie (e-rejestry). Wyzwaniem dla coraz szerszego wdrażanie procesów płynnych (seamless), realizowanych w od początku do końca w trybie rzeczywistym jest skala niezbędnych zmian i powiązanie różnorodnych procesów. Obecna presja na rentowność banków sprzyja podejmowaniu takich trudnych przedsięwzięć w poszukiwaniu redukcji kosztów.

Szczególnie duże oszczędności przynosi restrukturyzacja sieci oddziałów, które są z reguły najbardziej kosztownym obszarem banku. Firma Celent[5] ocenia, że w wyniku redukcji i przedefiniowania roli oddziałów integracja z kanałami cyfrowymi może zredukować koszty operacyjne banku o ponad 5%.

Najpoważniejsze zagrożenia

Nowe technologie i związane z nimi zmiany niosą także poważne zagrożenia, ale dotyczy to raczej tych banków, które nie będą potrafiły odpowiednio się zaadaptować, niż całej bankowej branży.

Ryzyko technologiczne jest obecnie postrzegane jako jedno z czterech najważniejszych zagrożeń[6]. Poczucie zagrożenia narasta, a ryzyko technologiczne przesuwa się w rankingu w ostatnich latach do góry – w miarę jak banki natrafiają na coraz większe trudności w dotrzymaniu tempa zmian i obserwują jak narasta konkurencja ze strony niebankowych (FinTech) graczy. Poczucie zagrożenia wzmacniają też obserwacje jak silnie zostały przez technologię zrewidowane modele biznesowe w innych branżach (np. medialnej).

Łatwość porównywania ofert i przenoszenia rachunków powoduje, że klienci stają się coraz mniej lojalni. Internet nie promuje trwałości relacji, innowacje kuszą klientów a niektóre rządy dla zapewnienia transparentności konkurencji tworzą infrastrukturę ułatwiającą wybór najlepszej oferty bankowej oraz przeniesienie rachunków. W Wielkiej Brytanii serwis midata[7], zajmujący się różnymi usługami, w tym bankowymi, ułatwia klientom dokonanie wyboru. Z kolei serwis Current Switch Service zapewnia w ciągu siedmiu dni przeniesienie rachunku wraz ze wszystkimi zleceniami stałymi. W ciągu roku wspomniany serwis przenosi ponad milion rachunków i liczba ta rośnie.

---

5 http://bankingblog.celent.com/tag/branch-transformation/

6 BankingBanana Skins 2015 The CSFI and PWC survey of bank risk

7 http://www.gocompare.com/money/midata/

Przestarzałe już systemy podstawowe, złożona architektura systemów (często dodatkowo skomplikowana w wyniku fuzji banków), dług technologiczny oraz uzależnienie od dostawców rozwiązań IT powodują, że wiele banków ma poważny problem aby dostosowywać systemy IT w niezbędnym czasie. Nic więc dziwnego, że takie banki jak Santander, Deutsche Bank, HSBC czy UBS wskazują uproszczenie architektury IT jako priorytet w swoich strategiach.

Znacznie rosną zagrożenia w obszarze cyberbezpieczeństwa. Za atakami stoją coraz częściej potężne środki finansowe i techniczne, dostarczane przez struktury państwowe lub organizacje przestępcze operujące z terenów, na których są praktycznie bezkarne. Nowe technologie niosą nowe ryzyka, dla których nie upowszechniły się jeszcze środki zaradcze. Szczególnym problemem wydają się obecnie urządzenia mobilne, m.in. dlatego, że system tworzenia i dystrybucji aplikacji mobilnych utrudnia kontrolowanie ich zabezpieczeń. Jak wskazują badania, bezpieczeństwo ma dla klientów priorytetowe znacznie przy ocenie relacji z bankiem[8]. Ryzyko reputacyjne banku i relacje z klientami są więc rzeczywistą stawką w walce z hakerami.

Narastającym problemem jest coraz silniejsza konkurencja ze strony firm niebankowych (FinTech), począwszy od innowacyjnych startupów aż po potężne firmy technologiczne. Najpoważniejszy wpływ na banki ma obecnie konkurencja w obszarze płatności. Nie tylko poprzez zmniejszanie wolumenów usług i przychodów prowizyjnych, ale również odcinanie banków od cennych informacji na temat transakcji klientów. Konkurowanie z „natywnie technologicznymi" firmami, poprzez wyścig innowacji, sprawność i elastyczność procesów czy lepsze rozumienie potrzeb klientów okazuje się trudne. Banki przyjmują więc coraz częściej formułę współpracy z takimi firmami czy to przez wspólne prace nad innowacjami (np. Barclays Accelerator), obsługę klientów (CitiGroup z LendingClub) czy też po prostu nabywając takie podmioty. Przykładam intensywnego stosowania tej ostatniej strategii jest bank BBVA, który zainwestował m.in. w firmy fintec: Madiva, Spring Studio, Sum up, Radius, Taulia. Równocześnie nabył udziały w bankach „internetowych" Atom i Simple oraz utworzył specjalizowane w FinTech fundusze inwestycyjne.

8 EY-global-commercial-banking-survey-2014

Internet of Things – kolejna fala rewolucji technologicznej

Bardzo intensywnie omawianym obecnie tematem jest Internet of Things (IoT). Możliwości zastosowania tych technologii w bankowości wydają się jeszcze dość ograniczone, np. wykorzystanie inteligentnych zegarków lub innych *wearable devices* do płatności bezstykowych lub komunikacji z klientami. Jednak branża bankowa powinna uważnie śledzić IoT z co najmniej kilku powodów.

Analitycy spodziewają się, że ta kolejna fala rewolucji technologicznej przyniesie znacznie szybsze i rozleglejsze zmiany niż poprzednie, zmieniając zachowania zakupowe klientów i kompletnie redefiniując niektóre branże. Ocenia się, że liczba urządzeń podłączonych do Internetu w roku 2020 osiągnie 50 mld[9], a wydatki na IoT osiągną, według firmy IDC, 1,3 bln dolarów w 2019 r.

Największe firmy technologiczne (Microsoft, IBM, Google) i dotychczas nietechnologiczne (General Electric) oraz wielu mniejszych graczy już starają się zająć wiodącą pozycję na rynku rozwiązań IoT, przyjmując zbliżone strategie. Oferują w modelu płatności za rzeczywiste użycie rozwiązania cloudowe z wyspecjalizowanymi aplikacjami (głównie analitycznymi), narzędzia i wsparcie dla twórców aplikacji oraz platformę cyfrową dla dystrybucji aplikacji. Będzie to prawdopodobnie miało (podobnie jak to jest w rozwiązaniach mobilnych) ogromny wpływ na tempo i koszt tworzenia, testowania i upowszechniania innowacyjnych rozwiązań. Dostawcom serwisów cloudowych pozwala również na pozyskiwanie wielkich ilości danych, które potrafią przetworzyć w cenne i zbywalne informacje.

Należy się więc spodziewać, że rewolucja IoT będzie miała wpływ na banki i prędzej lub później wytworzy kolejną przełomową innowację.

Zmiany te będą też wywoływać szersze zaakceptowanie sprawniejszego i tańszego modelu budowania usług informatycznych w oparciu o cloud computing (również dla systemów krytycznych) i ekosystem zewnętrznych dostawców aplikacji. Wymaga to nie tylko pewnej zmiany przyzwyczajeń i sposobu myślenia o IT, ale dysponowania innymi wewnętrznych kompetencjami w zakresie zarządzania architekturą, współpracy i kontrolowania dostawców usług IT.

9 http://www.ey.media.pl/pr/301760/raport-ey-do-2020-roku-liczba-urzadzen-na-swiecie-podlaczonych-do-internetu-przekroczy-50-miliardow

Wyzwanie dla zarządzających

Powyższy opis, w którym świadomie pominąłem wiele zagadnień, w tym taki intrygujący temat jakim jest blockchain, zaledwie zarysowuje różnorodność i złożoność zagadnień opisywanych terminem *digital banking*. Pojawia się pytanie jak skutecznie zarządzać tym zagadnieniem, aby unikać zagrożeń i wykorzystywać możliwości oferowane przez technologie.

Należy przede wszystkim zaadresować dwa problemy:

- rozproszone i nieskoordynowane zarządzanie poszczególnymi aspektami digital banking,
- zdolność do sprawnego wprowadzenia nowych technologii i wynikających z tego zmian.

Digital banking wymaga skoordynowanego zarządzania *cross-functional,* obejmującego wszystkie aspekty uporządkowanego podejścia od strategii do konkretnych działań operacyjnych oraz budowania zdolności banku do adaptacji do zmian technologicznych.

Zarządy banków rozumieją znaczenie technologii i odzwierciedlają to w strategiach biznesowych. Niektóre opracowują „strategie dziedzinowe" dla *digital banking*, odzwierciedlające ich cele i ambicje oraz wysokopoziomowe plany. Koncentrują się obecnie na innowacjach, upraszczaniu procesów i zarządzaniu ryzykiem, przebudowie architektury IT oraz kooperacji z FinTech.

Wyniki przyprowadzonej przez firmę doradczą EY analizy wskazują, że wiele czołowych banków nadal nie ma na poziomie zarządów osób czy komitetów dedykowanych innowacjom i technologiom, ale takie kompetencje i stanowiska coraz częściej się pojawiają, np. często poprzez rozszerzenie funkcji COO.

Digital banking jest istotne i ma wpływ na wiele jednostek i aspektów działania banku. Wymaga więc zaangażowania na poziomie zarządu do skoordynowanego rozwinięcia tych strategii w plany konkretnych działań operacyjnych oraz monitorowanie ich realizacji.

Działania w zakresie *digital banking*, podejmowane w jednostkach IT, marketingu, operacji, poszczególnych liniach biznesowych czy wyspecjalizowanych komórkach „digital" powinny być koordynowane. Sposób koordynacji powinien być dostosowany do specyfiki banku, jego struktur organizacyjnych,

relacji w grupie kapitałowej. Konieczna jest jednak stała platforma wymiany informacji, ustalania priorytetów i planów działań oraz ich monitorowania. Może to przyjąć formę powtarzanego cyklicznie „programu digital banking".

Trzeba jednak uniknąć ryzyka sparaliżowania działań przez zbyt rozbudowane i wieloszczeblowe struktury decyzyjne oraz tworzenie zbyt wielu powiazań miedzy inicjatywami realizacyjnymi.

Wypracowane decyzje i priorytety muszą być odzwierciedlane w budżetach i decyzjach innych ciał (np. komitetu inwestycyjnego).

Digital banking wymaga skoordynowanego programu rozwoju, zdolności do sprawnego wdrażania oraz przygotowania na nieoczekiwane zmiany. Można go wyobrazić sobie jako cykliczną realizację dwóch strumieni prac:

- działań wynikających z przeprowadzanego oceny dojrzałości banku w zakresie stosowania nowoczesnych technologii,
- działań dla usunięcia zidentyfikowanych barier zmiany.

Strumień pierwszy może składać się z następujących kroków:

1. Diagnoza – odniesienie do najlepszych praktyk i strategii banku m.in. w zakresie:
   - kompetencji do śledzenia i analizowania trendów technologicznych i *digital banking*, rozumienia rynku,
   - dostosowania inicjatyw rozwojowych do głównych trendów *digital banking* i strategii banku,
   - kanałów dystrybucji (internet, mobile, etc.) dla różnych linii biznesowych (ocena funkcjonalności, technologii, ekonomiki),
   - harmonizacji usług w różnych kanałach dystrybucji (omnichannel),
   - stosowania mediów społecznościowych do dialogu z klientami oraz przygotowania do zapobiegania kryzysom wizerunkowym oraz reagowania w przypadku ich wystąpienia,
   - stopnia automatyzacji transakcji i procesów inicjowanych w kanałach elektronicznych,
   - wykorzystania technologii dla obniżenia kosztów operacyjnych (np. oddziałów),
   - stosowania narzędzi analitycznych do budowania zrozumienia klienta oraz zdolności praktycznego wykorzystywania tej wiedzy (np. dostosowywania oferty, precyzyjnych porad i alertów).

Diagnoza powinna być przeprowadzona m.in. w perspektywie: organizacji, systemu zarządzania, kompetencji, priorytetów, funkcjonalności, oferty, rozpoznawalności rynkowej, technologii, bezpieczeństwa oraz architektury rozwiązań.

2. Zdefiniowanie i priorytetyzacja działań dla zaadresowania stwierdzonych zagrożeń i problemów oraz realizacji ambicji strategicznych banku.
3. Określenie i opracowanie planów realizacyjnych oraz właściwej dla nich formuły realizacyjnej. Ustalenie celów i mierników ich realizacji oraz mechanizmów nadzoru.

Strumień drugi ma zapewnić bankowi niezbędną zdolność do adaptacji – ustalić i zrealizować zestaw działań pozwalających na sprawną reakcję na nieoczekiwane zmiany oraz skuteczniejsze realizowanie zmian przewidzianych. Składać się on może z następujących kroków:

1. Przeanalizowanie nie tylko aktualnego stanu rozwiązań w zakresie *digital banking*, ale także przyczyn takiego stanu, przebiegu wdrożeń rozwiązań i największych problemów w celu określenia ich przyczyn.
2. Przeprowadzenie dla obszarów *digital banking* diagnozy możliwości reakcji na zmianę w zakresie:
   - kompetencji i mechanizmów ich rozwoju,
   - procesów decyzyjnych (w tym relacji w grupie kapitałowej),
   - prowadzenia projektów,
   - stosowanych technologii,
   - współpracy biznesu z IT,
   - dostawców technologii i rozwiązań (stopnia uzależnienia, pozycji rynkowej, strategii produktowych, reaktywności),
   - sourcingu usług IT,
   - metod wytwórczych i architektury systemów,
   - rozwiązań i procesów w obszarze cyberbezpieczeństwa.
3. Zdefiniowanie i spriorytetyzowanie kwestii utrudniających reakcję na zmiany (barier zmiany).
4. Określenie i opracowanie planów usunięcia barier zmiany oraz właściwej dla nich formuły realizacyjnej. Ustalenie celów i mierników ich realizacji oraz mechanizmów nadzoru.

Jak wspomniano, działania powyższe powinny być realizowane w sposób cykliczny, a diagnoza i plany aktualizowane w zależności od skali problemu i dynamiki zmian w obszarze digital co najmniej raz w roku.

Podsumowanie

Digital banking pomimo oparcia na uniwersalnych „transgranicznych" technologiach jest zjawiskiem specyficznym dla danego rynku. Wynika to z lokalnych preferencji klientów, dojrzałości użytkowników i infrastruktury, ale także z obciążenia banków „bagażem przeszłych dokonań" *(legacy)*. Dlatego strategie i plany operacyjne dotyczące *digital banking*, o ile są tworzone na poziomie grupy kapitałowej, powinny być dostosowywane do lokalnej specyfiki rynku w danym kraju.

Ta lokalna specyfika *digital banking* wymaga również lokalnych kompetencji. Dotyczą mediów społecznościowych, śledzenia trendów na rynku, dostosowywania się w niezbędnym zakresie usług, procesów i rozwiązań technicznych. Przede wszystkim wymaga jednak skoordynowanego zarządzania kompleksem zagadnień, które zawiera w sobie *digital banking* i przygotowaniem banku do zmian (planowanych i nieznanych) poprzez identyfikację i usuwanie najpoważniejszych barier, jak brak niezbędnych kompetencji, zbyt złożona architektura systemów lub *vendor lock*.

Bartłomiej Nocoń

Dyrektor Zarządzający Departamentem Bankowości Elektronicznej w Pionie Bankowości Detalicznej Banku Pekao S.A.

Absolwent Akademii Ekonomicznej w Krakowie (obecnie Uniwersytet Ekonomiczny) na kierunku międzynarodowe stosunki gospodarcze i polityczne, specjalność handel zagraniczny oraz stypendysta The Swedish School of Economics and Business Administration w Helsinkach. Z obszarem bankowości elektronicznej i mobilnej oraz zarządzaniem finansami on-line związany od początku swojej kariery zawodowej. Na obecnym stanowisku od grudnia 2007 r., odpowiedzialny za realizację strategii wielokanałowej obsługi oraz rozwój bankowości elektronicznej i mobilnej Pekao24/PekaoBiznes24 dla klientów indywidualnych oraz mikro i małych przedsiębiorstw. Członek Rady Nadzorczej Contact Center – Centrum Bankowości Bezpośredniej Sp. z o.o.

Posiada bogate doświadczenie w zarządzaniu projektami w sektorze usług finansowych. Wielokrotny prelegent na krajowych i zagranicznych konferencjach poświęconych zagadnieniom z obszaru zarządzania i sprzedaży w kanałach elektronicznych oraz aspektom związanym z nowoczesnymi technologiami IT i bezpieczeństwem w sektorze finansowym.

Bartosz Zborowski

Dyrektor Biura Projektów Strategicznych w Pionie Bankowości Detalicznej Banku Pekao S.A.

Absolwent Akademii Ekonomicznej w Krakowie na kierunku finanse i bankowość oraz studiów podyplomowych „Zarządzanie Projektami Internetowymi" w Szkole Przedsiębiorczości i Zarządzania AE w Krakowie.

Przez 16 lat kariery zawodowej uczestniczył w licznych projektach z obszaru bankowości detalicznej i działalności brokerskiej. Na obecnym stanowisku od 2007 r., zaangażowany m.in w połączenie banków: BPH i Banku Pekao S.A., organizację aktywności Banku na EURO 2012, wdrożenie operacyjnego CRM, wdrożenie akceptacji kart w największej sieci detalicznej w Polsce, a także rozwój Banku w obszarze szeroko pojętych płatności. Odpowiedzialny za powstanie innowacyjnego systemu płatności mobilnych PeoPay.

Bartłomiej Nocoń, Bartosz Zborowski, Bank Pekao S.A.

Budowanie pozytywnego doświadczenia klienta w bankowości

Upowszechnienie nowoczesnych technologii, wzrost znaczenia roli estetyki w projektowaniu rozwiązań i rosnące oczekiwania klientów związane ze spersonalizowaną obsługą i ofertą znacząco wpłynęły na wzrost roli *customer experience* w otaczającej nas rzeczywistości. Niemniej ważną rolę odegrały także media społecznościowe, które uprościły komunikację i spowodowały, że wymiana doświadczeń i opinii, zarówno tych pozytywnych, jak i, przede wszystkim, negatywnych, jest wygodna i łatwiejsza niż kiedykolwiek. We współczesnym społeczeństwie to w szczególności przedstawiciele generacji Y (urodzeni w połowie i pod koniec lat 80.) oraz Z (urodzeni po roku 1990), którzy dorastali razem z technologiami cyfrowymi i z nich intensywnie korzystają, są motorem zmian i podkreślają rolę oraz znaczenie pozytywnego doświadczenia klienta w codziennych interakcjach, zarówno w swojej codziennej pracy jak i będąc w roli klientów korzystających z usług.

Czym jest *customer experience*?

Istnieje wiele definicji *customer experience* (CX, z ang. doświadczenie klienta), w najprostszym jednak ujęciu, jest to suma wszystkich doświadczeń klienta, które wiążą się z daną firmą. W szerszym rozumieniu są to natomiast wszystkie interakcje pomiędzy klientem a organizacją, będące połączeniem percepcji klienta dotyczącej fizycznych aktywności organizacji, stymulowanych zmysłów klienta i wywołanych u niego emocji. Interakcje te są intuicyjnie

oceniane przez klienta względem jego oczekiwań, po pierwsze, poprzez cały czas trwania kontaktu z firmą, a po drugie, we wszystkich punktach styku klient-firma.[1]

Kim są współcześni klienci banków i czego oczekują?

Zrozumienie potrzeb klientów banków i w konsekwencji zbudowanie najlepszego doświadczenia klienta wymaga przede wszystkim odpowiedzi na pytanie: kim są dzisiaj klienci banków? Banki oferują bowiem swoje produkty i usługi wielu różnorodnym grupom klientów począwszy od klientów indywidualnych i zamożnych, aż po firmy i korporacje. Najbardziej istotny i wyraźny, z punktu widzenia *customer experience*, jest jednak podział na klientów tzw. nowoczesnych i tradycyjnych. Klient nowoczesny to najczęściej przedstawiciel generacji Y lub Z (ale nie tylko!), który korzysta na co dzień z nowych technologii i oczekuje nowoczesnej i najwyższej jakości bankowości elektronicznej (internetowej, mobilnej), możliwości korzystania z dowolnego, preferowanego przez niego, kanału dostępu, a także dostępności banku natychmiast – „tu i teraz". Są to także osoby, które są bardziej skłonne do zmiany banku w przypadku, gdy ten nie spełni ich oczekiwań. Klienci tradycyjni natomiast cenią sobie głównie rozbudowaną sieć bankomatów i oddziałów, obsługę osobistą, a w szczególności wsparcie pracowników (w oddziałach, *contact center*) oraz poczucie bezpieczeństwa, które daje im bank. Oczekiwania i potrzeby każdej z grup klientów są zatem inne i inne też są sposoby banków na ich spełnienie. Niezależnie jednak od grupy, współcześni klienci stawiają przed bankami także pewne wspólne oczekiwania, tj.:

- spersonalizowanej obsługi i oferty,
- stałej i nieprzerwanej dostępności do preferowanego kanału kontaktu z bankiem,
- produktów użytecznych, prostych i intuicyjnych, a także o najwyższej jakości.

Potrzeby klientów i ich umiejętne spełnienie przez bank składa się na sumę doświadczeń klienta banku, które, w konsekwencji, pozwala zdobyć

1 Customer Experience od początku, czyli co to za zwierzę?, http://goodcustomerexperience.pl/customer-experience-od-poczatku/

i podtrzymać jego zaufanie, a nawet skłonić go do bycia „ambasadorem marki". Potwierdzają to także badania – w raporcie EY[2] klienci (aż 41%) wskazali „doświadczenie z dostawcami usług finansowych" jako najważniejszy z powodów, dla którego otworzyli rachunek lub skorzystali z usługi.

Customer experience w kontekście kanałów interakcji z bankiem

Rozpatrując oczekiwania klientów warto podkreślić, że doświadczenie klienta w kontakcie z bankiem będzie inne podczas wizyty w oddziale, inne podczas korzystania z bankowości internetowej czy mobilnej, a także inne podczas kontaktu poprzez *social media* czy *contact center* – bo za każdym razem inny jest np. poziom intymności. Dlatego też banki dążą do zapewnienia pozytywnego, ale też odpowiednio dostosowanego *customer experience* poprzez realizację oczekiwań klienta w każdym kanale, z którego klient korzysta.

Dążenie banków do zaoferowania jak najlepszego doświadczenia klienta jest szczególnie widoczne w bankowości elektronicznej. Jeszcze dekadę temu wystarczało wdrożenie bankowości internetowej, aby być konkurencyjnym. Dzisiaj, kiedy większość serwisów bankowych oferuje podobne funkcje, dla podtrzymania zaangażowania klientów i ich zmieniających się oczekiwań banki skupiają się na dostarczaniu jak najlepszego doświadczenia dla klienta. Przemyślane cyfrowe doświadczenie pozwala im budować przewagę na niezwykle konkurencyjnym rynku usług finansowych. Banki od lat stawiają więc konsekwentnie na wdrażanie innowacji, które są uważane za jeden z najważniejszych czynników mogących zapewnić przewagę konkurencyjną i w praktyce pozwalają zbudować nowoczesne doświadczenie klienta. Współczesna bankowość elektroniczna to usługi dostosowane do urządzenia, z którego klient korzysta, funkcjonalne i podane w wygodny, atrakcyjny wizualnie sposób.

Bankowość mobilna i płatności mobilne są natomiast doskonałym przykładem obrazującym, jak banki wychodzą naprzeciw potrzebom klientów. Mimo, że jeszcze niedawno mobilna bankowość były postrzegana przez klientów jako ciekawostka, banki odważnie inwestowały w ten obszar antycypując, że wraz z upowszechnieniem smartfonów to właśnie dostęp do banku „tu i teraz"

2 EY, W centrum uwagi – doświadczenie klienta w kontakcie z marką. Światowe Badanie Klientów Banków Detalicznych 2014, http://www.ey.com/Publication/vwLUAssets/Global_Consumer_Banking_Survey_2014/$FILE/EY-Global-Consumer-Banking-Survey-2014-PL-final.pdf

będzie oczekiwanym przez klientów kierunkiem rozwoju. Dzisiaj mamy już niemal 6 mln aktywnych użytkowników bankowości mobilnej[3], a wiele banków opiera swoje plany rozwoju w oparciu o strategię „mobile first" (projektowanie rozwiązań w pierwszej kolejności dla urządzeń mobilnych).

Większość operacji bankowych, które były zarezerwowane dla oddziałów, jak chociażby wykonywanie przelewów, są obecnie realizowane samodzielnie przez klienta w bankowości elektronicznej, co oznacza, że zmieniła się tradycyjna rola oddziału banku. Stał się on bowiem miejscem, gdzie najbardziej liczy się osobiste doradztwo i swoboda w rozmowie między klientem a doradcą, np. na temat bardziej skomplikowanych form inwestowania (aż 54% klientów w przypadku doradztwa preferuje kontakt poprzez oddział[4]). Spotkanie „twarzą w twarz" to nadal najlepszy i najefektywniejszy sposób na budowanie relacji z klientem, a tym samym wzrost jego zaufania i lojalności. Banki zauważają tę potrzebę i obok nowoczesnych serwisów internetowych czy mobilnych budują także nowoczesne placówki nastawione na budowanie pozytywnego *customer experience* poprzez wartość dodaną, umożliwiając załatwienie spraw niezwiązanych bezpośrednio z czynnościami bankowymi lub po prostu pozwalają miło spędzić czas. Niektóre banki stawiają także na tzw. „zdigitalizowane" oddziały, które wyglądają jak nowoczesne salony ze sprzętem elektronicznym. Wyposażone są w tablety, wielkoformatowe ekrany, a pracownicy nie siedzą przy stanowiskach, lecz podchodzą do klientów i doradzają im w wyborze produktów.

Obok oddziału banku klienci często szukają osobistego kontaktu poprzez *contact center*. To jeden z najczęściej wykorzystywanych kanałów w obsłudze klienta (aż 81% spośród nich sięga po kontakt przez telefon w celu uzyskania wsparcia[5]) i budowaniu relacji. Banki zatem sukcesywnie rozwijają usługi *contact center* i obecnie, oprócz standardowej rozmowy telefonicznej czy kontaktu poprzez e-mail, oferują także możliwość skontaktowania się bezpośrednio z pracownikiem poprzez chat czy wideo-rozmowę. Pojawiają się także inicjatywy tzw. wirtualnych oddziałów, które mają ambicję dostarczenia

3 PRNews, *Raport PRNews.pl: Rynek bankowości mobilnej – IV kw. 2015*, http://prnews.pl/raporty/raport-prnewspl-rynek-bankowosci-mobilnej-iv-kw-2015-6552323.html

4 EY, W centrum uwagi – doświadczenie klienta w kontakcie z marką. Światowe Badanie Klientów Banków Detalicznych 2014, http://www.ey.com/Publication/vwLUAssets/Global_Consumer_Banking_Survey_2014/$FILE/EY-Global-Consumer-Banking-Survey-2014-PL-final.pdf

5 PWC, Customer care evolution, http://www.pwc.com/us/en/industry/entertainment-media/publications/consumer-intelligence-series/assets/pwc-cis-customer-care.pdf

klientowi spersonalizowanej, zbliżonej do oddziałowej obsługi, która umożliwi zdalną realizację zarówno operacji dostępnych w bankowości internetowej, jak i profesjonalnego doradztwa. W przypadku *contact center*, analogicznie jak dla oddziałów banku, ważne jest posiadanie wykwalifikowanej kadry pracowników, którzy, doskonale znając ofertę banku, dostarczą najwyższą jakość w rozwiązaniu problemu klienta, przekazaniu informacji czy sprzedaży produktu.

We współczesnym banku jednym z najistotniejszych kanałów kontaktu z klientami są również media społecznościowe. Podobnie, jak w *contact center* czy w oddziale, klient może tą drogą poinformować bank o swoim doświadczeniu czy problemie. Kluczową różnicą jest natomiast fakt, że ta opinia jest publicznie dostępna i każdy odwiedzający portal społecznościowy może się z nią zapoznać. To szczególnie istotne jeżeli weźmiemy pod uwagę, że *social media* są coraz częściej wybierane przez klientów jako miejsce gdzie mogą napisać skargę – 45% klientów dzieli się negatywną opinią w mediach społecznościowych (z negatywnymi opiniami zapoznaje się z kolei 63% klientów)[6]. Często czynią to zanim podejmą kroki związane z kontaktem poprzez oddział czy *contact center*. Od szybkości reakcji banku i umiejętnego wsparcia klienta w mediach społecznościowych zależy więc coraz bardziej budowanie i podtrzymanie jego lojalności – jeżeli bank nie spełnia potrzeb klienta, ten wybierze firmę, która to zrobi, a jednocześnie świadkami tego będą inni obserwujący profil. Obecnie media społecznościowe są więc, obok bycia narzędziem marketingowym, często wykorzystywane jako narzędzie do rozwiązywania problemów klientów. Inną, szczególnie ważną z punktu widzenia *customer experience*, rolą mediów społecznościowych jest wykorzystanie ich do zaangażowania wszystkich członków społeczności banku w tworzenie nowych produktów i usług. Dzięki temu oferta banków może staje się bardziej dopasowana do potrzeb klientów, a same produkty i usługi są dla nich bardziej zrozumiałe.

Jak budować najlepsze doświadczenia klienta?

Zapewnienie pozytywnego *customer experience* powinno stanowić fundament projektowania rozwiązań dla klientów. Dlatego też nad dążeniem zbudowania jak najlepszego doświadczenia klienta powinno czuwać wiele jednostek,

6 zendesk, The good, the bad, and the ugly: the impact of customer service, https://www.zendesk.com/resources/the-impact-of-customer-service/

które z jednej strony zadbają o spójność produktu czy usługi z wizerunkiem i strategią rozwoju banku, a z drugiej szukają rozwiązań, które spełniają oczekiwania klientów. Zapewnienie pozytywnego doświadczenia klienta wymaga także od banku holistycznego podejścia do działania. Nie jest ono bowiem efektem pracy pojedynczego specjalisty czy działu, lecz powinno być postrzegane w kontekście sprawnego działania całego banku – wszystkich działów, komórek i pojedynczych pracowników, a widoczne w szczególności w każdej usłudze i produkcie. Zróżnicowane podejście dostosowane do specyfiki kanału obsługi jest wskazane, jednak pamiętać należy także o zachowaniu nadrzędnej „spójności przekazu", zapewniającej klientowi poczucie obsługi wciąż w tym samym banku niezależnie od metody kontaktu.

Na przykładzie Banku Pekao S.A., do podstawowych działań w zakresie projektowania rozwiązań dostarczających najlepszego *customer experience* należą:

1. pogłębiona analiza rynków polskich i zagranicznych, nie tylko sektora bankowego,
2. przygotowanie rozwiązań użytecznych, łatwo identyfikowalnych z marką, które z jednej strony wyróżniają się i dla klienta, i na tle konkurencji, a z drugiej oferują zaspokojenie konkretnych potrzeb (wartość dodana),
3. przemyślana i logiczna architektura informacji, tak aby klient nie czuł się zagubiony przy korzystaniu z rozwiązania, rozumiał układ poszczególnych elementów,
4. projektowanie rozwiązań i produktów w drodze ewolucji, nie rewolucji,
5. budowanie serwisów zbliżonych możliwościami i oferujących podobne doświadczenie (brak konieczności uczenia się „na nowo") – efekt ewolucji z multi do omnikanałowości,
6. skrupulatność testów, zarówno tych wewnętrznych, jak i z udziałem klientów oraz zbadanie produktu lub usługi pod kątem jej użyteczności,
7. niezaniedbywanie kwestii bezpieczeństwa kosztem złudnej „wygody" rozwiązania (klienci nadal wskazują bezpieczeństwo jako jedną z podstawowych przeszkód w korzystaniu z bankowości elektronicznej).

Aż 66% klientów jest skłonnych wydać więcej w firmie, która dostarcza obsługę wysokiej jakości[7]. Szczególnie istotne jest więc, aby w każdym punkcie kontaktu z klientem obsługa miała pełen wgląd do jego sytuacji (np. w zakresie złożonych reklamacji, aktualnego zadłużenia czy złożonych wniosków). Ważną rolę w budowaniu pozytywnego doświadczenia klienta pełni więc także analiza danych, która pozwala bankom zbudować właściwą „drogę klienta" (tzw. *customer journey*) i spersonalizowane doświadczenie. Pozwala także na wykreowanie potrzeby i dostarczenie rozwiązania odpowiadającego na nią bądź jej uświadomienie (z takiego podejścia narodziły się chociażby płatności mobilne).

Wiele banków w dobie cyfrowej rewolucji coraz częściej korzysta z ujednoliconych narzędzi CRM i Call Center Service Desk, aby zapewnić milionom klientów lepszy standard usług. Jednocześnie warto zauważyć, że analiza danych często wymaga nowych technologii i procesów, aby pobierać, przechowywać i zarządzać dużą ich ilością. Tradycyjne podejście do zarządzania danymi stosowane przez banki nie spełnia obecnie tych wymagań.

Na odbiór usług banku przez klientów przemożny wpływ ma również prostota procesów. Często obserwujemy jak czasem drobne uproszczenia procesów mogą wpłynąć na znaczny wzrost popularności danej usługi czy produktu. W przypadku polskiego rynku bankowego przykładów jest wiele, zaczynając od wdrożenia kartowych płatności zbliżeniowych, uproszczeń w aktywacji kanałów elektronicznych, przejścia z wielostronicowych wniosków kredytowych do ofert typu „one click", odejścia od mobilnych płatności kodem czy opartych na sim-centric do płatności zbliżeniowych HCE.

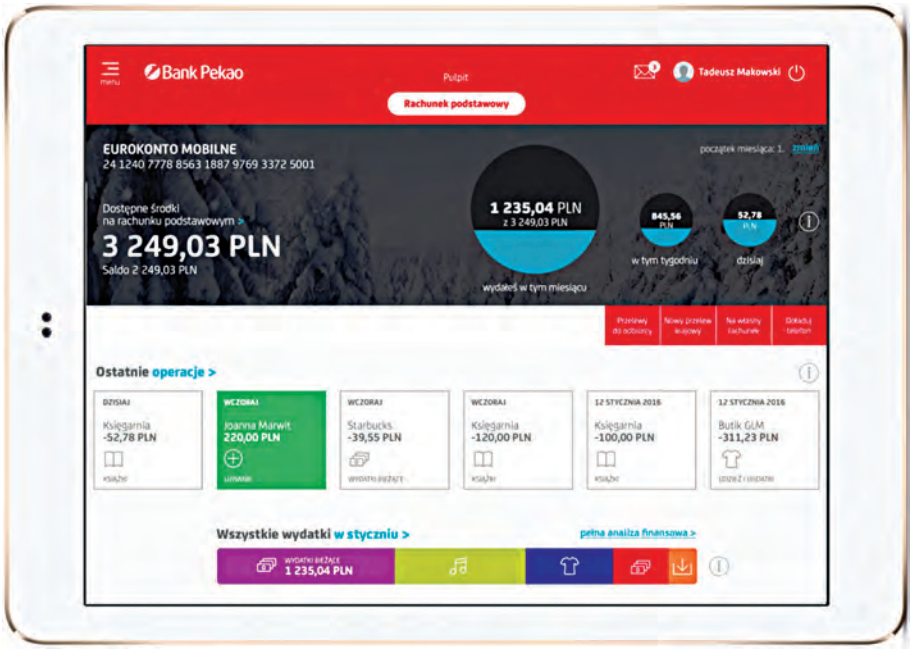
Przykłady pozytywnego *customer experience*

Sporo jest pozytywnych przykładów na rynku, natomiast jednym z ciekawszych banków, który z powodzeniem stosuje pozytywne *customer experience* jest brytyjski Metro Bank, który „tworzy fanów, a nie klientów". Bank źródeł sukcesu upatruje w dojrzewaniu cyfrowego klienta oraz w odejściu od modelu skoncentrowanego na transakcjach do modelu skoncentrowanego na kliencie. Wykorzystuje technologie mobilne i media społecznościowe, aby jego klienci–fani mogli kontaktować się z bankiem w najdogodniejszy dla nich sposób.

7 echo, 2012 Global Customer Service Barometer. Findings in the United States, http://about.americanexpress.com/news/docs/2012x/axp_2012gcsb_us.pdf

Z perspektywy doświadczeń Banku Pekao S.A., przykładem nowoczesnego podejścia do customer experience może być najnowsza aplikacja „Pekao24 na tablety". W banku już 15% logowań miesięcznie do serwisu internetowego Pekao24 odbywa się z urządzeń mobilnych, w tym głównie z tabletów. To istotny sygnał, że klienci oczekują wygodnego i funkcjonalnego dostępu do bankowości na tablecie. Odpowiedzią na tą potrzebę jest najnowsza aplikacja „Pekao24 na tablety". Jednocześnie aplikacja adresuje podstawowe oczekiwania, tj. użyteczność, intuicyjność i prostotę obsługi, których wymaga budowanie pozytywnego *customer experience*. Klient od razu po zalogowaniu widzi na pulpicie najważniejsze dla niego informacje (dostępne środki, ostatnie operacje, wydatki w danym okresie czasu) i ma dostęp do najczęstszych operacji (przelewy, doładowania). Układ informacji jest przejrzysty i czytelny, a aplikacja dostarcza klientowi wartość dodaną w postaci podsumowań wydatków i kategoryzacji operacji.

Pulpit aplikacji „Pekao24 na tablety" jako przykład budowania pozytywnego customer experience w bankowości elektronicznej



Kolejnym przykładem produktu, gdzie *customer experience* odgrywa kluczową rolę jest aplikacja płatności mobilnych Pekao – PeoPay. Jednym z głównych celów systemu PeoPay jest umożliwienie wykorzystania telefonu do szybkich i wygodnych płatności w taki sposób, by proces płacenia maksymalnie odzwierciedlał wygodę użytkowania karty zbliżeniowej w przypadku sklepów stacjonarnych, a w przypadku sklepów internetowych ograniczał się do wykonania tylko dwóch czynności: zeskanowania kodu QR i wpisania PINu. W celu dokonania płatności nie jest wymagane uprzednie logowanie do aplikacji, co znacznie przyśpiesza proces rozpoczęcia płatności. Mamy więc z jednej strony zaspokojenie konkretnej potrzeby klienta, z drugiej maksymalnie uproszczony proces nastawiony na wygodę w korzystaniu z aplikacji

Aplikacja PeoPay na Android

Pierwsze na świecie płatności zbliżeniowe HCE na Windows 10 Mobile – PeoPay

Dobrych praktyk i przykładów budowania pozytywnego doświadczenia klienta warto także szukać w działaniach firm spoza sektora usług finansowych np. w sprzedaży detalicznej. Firmy z tej branży są silnie skoncentrowane na tworzeniu bezproblemowego doświadczenia dla swoich klientów. W szczególności firmy te stworzyły silne oferty dla klienta za pośrednictwem kanałów mobilnych[8]. Jako pozytywne przykłady rozwiązań z zakresu omnikanałowości i *customer experience* po stronie detalistów wskazuje się także: sprawdzanie stanu zamówienia online, dostawa następnego dnia, odbiór i zwroty w sklepach czy rozpoczęcie procesu zakupu w jednym kanale (np. mobile) i dokończenie w innym (np. sklep stacjonarny). Jednym z przykładów firmy spoza branży bankowej, która dba o pozytywne *customer experience* jest Apple i jego sklepy Apple Store. Pracownicy sklepów są odpowiednio przeszkoleni do „słuchania sygnałów, które ujawniają na czym klientom zależy w życiu" i wskazywania sposobów, w jakich produkty Apple dostarczą

8 KPMG, Customer Experience Barometer, https://www.kpmg.com/dutchcaribbean/en/Documents/Publications/customer-experience-barometer-v1-fs.pdf

dodatkową wartość w życiu klienta. W obsłudze bardzo ważną rolę odgrywa także zadawanie właściwych pytań. Zdaniem jednego z przedstawicieli firmy najważniejszym elementem doświadczenia firmy Apple jest to, że koncentruje się na budowaniu relacji i sprawianiu aby życie ludzi było lepsze.[9]

Jakie trendy mogą wpłynąć na doświadczenie klienta w banku?

Interesującymi trendami w obszarze customer experience są obecnie tzw. bankowość emocjonalna (*emotional banking*) oraz niewidzialny bank (*invisible banking*). U podstaw koncepcji emotional banking leży analiza i wykorzystanie zależności pomiędzy finansami a emocjami i założenie, że ludzie nie «potrzebują» produktów bankowych (np. nie mają „potrzeby" posiadania rachunku osobistego), lecz mają potrzeby, np. bezpieczeństwa, które te produkty spełniają. W praktyce zrozumienie i reakcja na emocje klienta związane z pieniędzmi powinny poprzedzić budowanie i dostarczanie usług i produktów, wdrażanie i rozwój obsługi klienta a nawet budowę podstawowych systemów banku.[10] *Invisible banking* to z kolei bankowość, która „dzieje się w tle". W tej koncepcji zarządzanie finansami przez klienta odbywa się w drodze wyjątku, dopóki nie zdarzy się coś nowego lub nieprzewidywalnego. Bank po otrzymaniu wpływu wynagrodzenia klienta płaci jego rachunki czy też wykonuje regularne przelewy. Koncepcja zakłada, że nie ma potrzeby wykonywania żmudnych operacji bankowych, wystarczy jedynie pilnować wydatków.[11]

W budowaniu pozytywnego doświadczenia klienta dużą rolę pełnią także szeroko pojęte nowe technologie i związane z nimi trendy, jak np.:

1. RWD (Responsive Web Design)[12] – daje bankom większą elastyczność w projektowaniu serwisów i lepszy „time-to-market", bowiem zmiana jest od razu widoczna we wszystkich kanałach bankowości elektronicznej

9 Forbes, How The Apple Store Creates Irresistible Customer Experiences, http://www.forbes.com/sites/carminegallo/2015/04/10/how-the-apple-store-creates-irresistible-customer-experiences/

10 The Financial Brand, Banking Needs To Put Emotion Into Customer Experience, http://thefinancialbrand.com/51909/emotion-customer-experience-banking/

11 Duena Blomstrom, *Invisible Banking – Which superpower would Tom choose?*, http://duenablomstrom.com/2015/09/16/invisible-banking-which-superpower-would-tom-choose/

12 Responsive Web Design – (RWD) to technika projektowania strony www, tak aby jej wygląd i układ dostosowywał się automatycznie do rozmiaru okna urządzenia, na którym jest wyświetlany np. przeglądarki, smartfonów czy tabletów, https://pl.wikipedia.org/wiki/Responsive_Web_Design

– internetowej, na tablety czy mobilnej. Korzyść płynąca z RWD to także większa użyteczność – klient zna serwis internetowy, a więc bez problemu odnajduje się w jego mniejszej wersji, która w wydaniu mobilnym eksponuje najważniejsze funkcje (standard w *user experience*).

2. Synergia między analizą danych i kanałami mobilnymi, co w praktyce oznacza spersonalizowaną komunikację dostosowaną do cech demograficznych klienta, jego preferencji, jak również do kontekstu właściwego miejsca, czasu czy potrzeb.
3. „Dojrzały mobile" – w 2016 r. rynek mobile w dalszym ciągu będzie rósł (wg eMarketer już 2 mld ludzi na świecie będzie posiadało smartfony[13]), firmy muszą więc przejść z tworzenia stron „mobile-friendly" w kierunku tworzenia mobilnych doświadczeń użytkownika, np. umożliwiając klientowi pokonanie całej drogi zakupowej bezpośrednio na urządzeniu[14].
4. Technologie ubieralne (*wearables*, np. *smart watch*) – najbardziej mobilni i świadomi klienci oczekują od instytucji finansowych większego zaangażowania w tym kanale. Accenture szacuje, że wskaźnik tzw. „adoption rate" (osób zamierzających kupić dane urządzenie) dla wearables osiągnie poziom 28%[15] w 2016 r. Wearables to doskonałe źródło danych o zachowaniach klientów dzięki różnego rodzaju funkcjonalnościom tych urządzeń, które analizują parametry użytkownika (np. dane biometryczne czy lokalizacja), co w praktyce otwiera drogę dla takich rozwiązań, jak np. informowanie klienta na wyświetlaczu smart-zegarka o spersonalizowanej ofercie czy o saldzie rachunków, gdy ten przechodzi obok oddziału banku.

Podsumowanie

We współczesnym świecie klienci mają większy wybór, są bardziej skomunikowani niż kiedykolwiek, są coraz lepiej poinformowani, ale także sceptyczni

13 eMarketer, *2 Billion Consumers Worldwide to Get Smart(phones) by 2016*, http://www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694

14 iperceptions, *Top 5 Customer Experience Trends For 2016*, https://www.iperceptions.com/blog/customer-experience-trends-2016

15 Accenture, *Accenture Interactive – Point of View Series. The Internet of Things: The Future of Consumer Adoption*, https://www.accenture.com/t20150624T211456__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Technology_9/Accenture-Internet-Things.pdf

i wymagający. Oczekują również lepszych, bardziej spersonalizowanych doświadczeń w każdym kanale interakcji z bankiem. Budowanie jak najlepszego doświadczenia klienta poprzez dostosowanie się i zwracanie szczególnej uwagi na użyteczność produktów, wygodę korzystania oraz ich dostępność „tu i teraz" staje się dla banków odpowiedzią na oczekiwania klientów, zbudowania i podtrzymania ich lojalności, a także, przede wszystkim, sposobem na wyróżnienie się na rynku. Umieszczenie klienta w centrum uwagi odgrywa znaczącą rolę w budowaniu rozwiązań bankowych zarówno w obszarze bankowości elektronicznej, jak i standardowej obsługi. Jednocześnie banki mają obecnie lepsze niż kiedykolwiek możliwości zbudowania jak najlepszego doświadczenia klienta w głównej mierze dzięki nowoczesnym technologiom, które otwierają niedostępne do tej pory możliwości w zakresie dostarczenia produktów użytecznych, spersonalizowanych i dostosowanych do potrzeb klientów.

W nadchodzących latach, w celu utrzymania ważnej pozycji na ewoluującym rynku, banki muszą skupić się na podejściu klientocentrycznym i kontynuować dostarczanie jak najlepszego doświadczenia klienta.

Dr Andrzej Sieradz

Doktor nauk ekonomicznych Uniwersytetu Gdańskiego.

Ukończył Politechnikę Warszawską w 1983. Uzyskał również tytuł MBA Business International School w Warszawie oraz ukończył studia podyplomowe z zakresu finansów i bankowości w Szkole Głównej Handlowej. Zanim związał się z Bankiem BGŻ w 2010, w latach 2006–2010 był dyrektorem operacyjnym i członkiem zarządu ING Towarzystwo Ubezpieczeń na Życie S.A. oraz członkiem zarządu ING Usługi Finansowe S.A., gdzie odpowiadał za dział informatyki, obsługę klienta oraz zarządzanie projektami. W latach 2002–2006 związany z ING Bank Śląski S.A. W latach 1997–2002 pracował w Coca-Cola HBC w Polsce i w centrali w Wiedniu. Obecnie pracuje w Microsoft Polska, gdzie zajmuje architekturą korporacyjną.

Grzegorz Kuliszewski

Dyrektor Sektora Finansowego w IBM Polska.

Doświadczony menedżer, specjalizujący się w bankowości, informatyce i finansach. Były wiceprezes Banku BISE i Banku DnB NORD odpowiedzialny za informatykę, zaplecze banku, administrację i bezpieczeństwo oraz księgowość. Posiada wieloletnie doświadczenie w konsultingu („wielka czwórka"), zarówno w rozwoju biznesu, jak i we wdrożeniach. Przeobrażał organizacje w ramach fuzji i przejęć, wykorzystując zdolności w obszarze zarządzania zmianami. Prezentuje rozległe doświadczenie w zarządzaniu projektami i portfelami projektów. Zarządzał wdrożeniami kluczowych systemów informatycznych dla banków i instytucji finansowych.

Andrzej Sieradz, Microsoft Polska,
Grzegorz Kuliszewski, IBM Polska

Bank w chmurach

Według szacunków firmy Forrester Research, globalny rynek usług „chmury publicznej" ma osiągnąć wielkość 191 mld dolarów w 2020 r. Zaczął on gwałtownie rosnąć od 2013 r. od sumy 58 mld dolarów. Firma Forrester twierdzi, a za nią wszyscy analitycy biznesowi, że aplikacje chmurowe mają największy wpływ na ten wzrost i w 2020 r. będą warte ok. 133 mld dolarów. Przychody platform w „chmurze" mają szansę przynieść szacunkowo 44 mld dolarów przychodów. Gartner, inna firma zajmująca się badaniem rynku i technologii IT, określa chmurę jako jeden z 10 największych strategicznych trendów technologicznych na rok 2016, który będzie miał decydujący wpływ na organizacje komercyjne w ciągu najbliższych lat. Usługi chmurowe „Cloud" to nowy styl zarządzania IT – elastycznie skalowalnej informatyki samoobsługowej, gdzie aplikacje wewnętrzne i zewnętrzne będą budowane w ten nowy sposób.

Rys. 1. Udział rozwiązań chmurowych w transformacji biznesowej 2014

Źródło: *KPMG Cloud Survey Report, 2014, s. 4*

Według badania KPMG Cloud Survey Report[1] (rys. 1) z 2014 r. menedżerowie wykorzystują usługi chmurowe głównie ze względu na efektywność kosztową (49%). Wyniki badania pokazują także, że zwiększa się liczba organizacji wykorzystujących technologię usług chmurowych do wprowadzenia zmian na dużą skalę zarówno w obrębie jednostki biznesowej, jak i w całym przedsiębiorstwie. Transformacyjne zastosowania chmury pozwalają na wyższą elastyczność we wprowadzanych modernizacjach i dostarczenie pracownikom rozwiązań mobilnych (42%), poprawę interakcji z klientami, dostawcami i partnerami biznesowymi (37%) oraz lepsze wykorzystanie danych do decyzji biznesowych (35%).

Rys. 2. Obszary biznesowe o największym wzroście efektywności biznesowej jako rezultat zastosowania rozwiazań chmurowych

Źródło: *KPMG Cloud Survey Report, 2014, s. 12*

Według opinii liderów biznesowych (rys. 2) największe efekty biznesowe związane z rozwiązaniami chmurowymi pojawiają się w obszarach wyników biznesowych (73%), automatyzacji procesów usługowych (72%) oraz redukcji kosztów operacyjnych (70%).

1 KPMG Global Technology Innovation Survey, 2014

Rys. 3. Największe wyzwania przy adaptacji rozwiązań chmurowych

Utrata danych i ryzyko danych prywatnych

Ryzyko utraty wartości intelektualnej

Wpływ na organizację IT

48% Wpływ na pomiar ROI

48% Wysokie koszty wdrożenia

46% Aspekty prawne i compliance

46% Integracja z istniejącą Architekturą

46% Braki w oszacowaniu wszystkich kosztów

Źródło: *KPMG Cloud Survey Report, 2014 s.12*

Liderzy biznesowi widzą też zagrożenia związane z rozwiązaniami chmurowymi. Największe z nich mogą dotyczyć utraty: danych biznesowych (53%), własności intelektualnej, know-how (50%) oraz wpływu na wewnętrzny zespół IT (49%).

Chmura – zaawansowany outsourcing?

Technologicznie nie ma co do tego wątpliwości, że chmura może być realizowana jako:

- IaaS (Infrastructure As A Service), czyli outsourcing z przeniesieniem własności sprzętu,
- PaaS (Platform as a Service), wówczas gdy pod czyjąś opiekę oddamy również system operacyjny,
- SaaS (Software as a Service), gdy korzystamy również z użyczonego oprogramowania.

Wszystkie te usługi są dostępne od dawna, również dla banków, i reprezentują modele biznesowe, w których technologia przestała być traktowana jako źródło przewagi technologicznej stając się obszarem szybkich oszczędności, krótkiego time-to-market i metodą na uwolnienie wartości zatrzymanych w środkach trwałych.

Co takiego nadzwyczajnego jest w zastosowaniu chmury w banku?

Uważamy, że to kolejna rewolucja w bankowości. Poprzednia nastąpiła, gdy z banków zniknęły skarbce, a ich rola i znaczenie zostały przejęte przez systemy IT. Informatyzacja doprowadziła do przekształcenia banków z przedsiębiorstw lokalnych w globalnych graczy na rynkach finansowych. Informatyka umożliwiła bankom inną skalę działalności, często bardzo oderwaną od klienta detalicznego, od którego obsługi zaczynały.

Teraz przychodzi następna rewolucja – centrum świata bankowego stał się klient, a dokładnie wiedza na jego temat. Niestety, banki poprzez liczne ograniczenia prawne oraz poprzez koncentrację na efektywności operacyjnej „przegapiły"[2], w znacznym stopniu, rewolucję internetowo-mobilną. Jak to ocenia Scott C. Cambell[3]: „Wiemy, że oczekiwania klientów banków wzrastają, ale czego dokładnie chcą klienci? Tego jeszcze nie wiemy albo tylko wydaje nam się, że wiemy. Oczekiwania te nie są tworzone przez nas czy naszych konkurentów bankowych. Są one często zupełnie poza naszą branżą, w strefie wpływów klientów Apple czy Amazona czy też mediów społecznościowych. Tak naprawdę to właśnie oni są naszą konkurencją." Dziś wiedzę i informację o potrzebach klienta mają sieci detaliczne, które pozbawione wielu ograniczeń bankowości, analizują, profilują, ofertują i przez to wiążą klienta ze sobą.

Chmura rośnie… także w bankach

Chmura jest jednym z głównych trendów technologicznych, które pojawiły się w ciągu ostatnich kilku lat. Opiera się na podstawowej idei traktowania wszelkich rozwiązań oferowanych szerokiemu gronu odbiorców jako usługi. Tak budowane usługi są już dostępne. Firma Uber oferuje usługi transportowe nie posiadając ani jednej taksówki. Ta koncepcja wdziera się w świat bankowy. Ludzie potrzebują usług bankowych, ale już niekoniecznie samych banków. Dla banków, ze względu na rosnącą konkurencję, chmura jest metodą na ograniczenie kosztów i próbą szybkiej odpowiedzi na dynamicznie zmieniający się

2 Raport Big Data, Forum Technologii Bankowych przy Związku Banków Polskich – 2015, www.zbp.pl

3 Scott C. Campbell, Wiceprezes, American National Insurance Company, Stany Zjednoczone, Wnioski z globalnego badania IBM C-suite Study 2015 w sektorze finansowym, 2015, IBM Institute for Business Value

rynek. Według badania firmy IDC z 2015 r. 25% europejskich instytucji finansowych wykorzystuje rozwiązania chmurowe. Zgodnie z eWeek zaakceptowanie nowego podejścia SaaS (*Software as a Service*), spowodowało pięciokrotne zwiększenie wykorzystywania rozwiązań chmurowych z 13% w 2011 do 74% w 2014 r.[4]. Według IBM, 58% przedsiębiorstw w 2014 r. wydało więcej niż 10% swoich rocznych budżetów IT na rozwiązania chmurowe.

Mimo że niektóre korporacje już zdecydowały o przeniesieniu krytycznej infrastruktury informatycznej, rdzenia aplikacji biznesowych i danych wrażliwych w chmurę, ich największym wyzwaniem pozostaje bezpieczeństwo, tym razem wymagające ochrony aktywów umieszczonych w chmurze. Badanie przeprowadzone wśród menedżerów z branży bankowej w ponad 20 krajach przez Security Alliance Cloud (CSA) sugeruje, że dla 68% jego uczestników głównym powodem przechodzenia do chmury jest elastyczność i wydajność nowej infrastruktury.

Kilka banków europejskich zaczęło już wykorzystywać nowe rozwiązania i przenosić swoje dane finansowe do chmury. Część z nich nadal wykorzystuje „chmurę prywatną" czekając na rozwiązania regulacyjne. Inne przenoszą do chmury publicznej dane „niekrytyczne" i „niewrażliwe". Są również organizacje, jak De Nederlandsche Bank (DNB), krajowy organ regulacyjny systemu bankowego w Holandii, wykorzystujące chmurę do usług bankowych takich jak aplikacje mobilne, platforma bankowości detalicznej czy rozwiązania do zarządzania ryzykiem kredytowym.

Atrakcyjność chmury dla banków

Utrzymanie elementów infrastruktury IT, serwerów czy centrów danych jest kosztowne. Wybierając rozwiązania chmurowe banki nie będą musiały inwestować środków w serwery, oprogramowanie i zasoby ludzkie. Jak podkreśla James O'Neill, Senior Analityk z firmy konsultingowej Celent, jest to szczególnie interesujące dla mniejszych banków, które mają okazję sprawdzić, czy outsourcing operacji centrów danych jest realną opcją. Dla nich łatwiej jest aktualizować swoją infrastrukturę IT poprzez chmurę korzystając z modelu „pay per use".

Przetwarzanie w chmurze może zaoferować instytucjom finansowym szereg korzyści, a w tym: redukcję kosztów operacyjnych, szybkość i ela-

4 https://cashmanagement.bnpparibas.com/print/33631

styczność dostosowania wielkości infrastruktury do potrzeb czy też łatwość tworzenia nowego oprogramowania w oparciu o dostarczone jako usługa zestawy oprogramowania.

Atrakcyjność zmniejszenia kosztów jest bardzo duża. Warto przypomnieć, że koszty utrzymania rozwiązań IT stanowią przeciętnie 14,3% całkowitych kosztów operacyjnych banku. Jest to najwyższy wskaźnik wśród wszystkich branż gospodarki. Mierząc w inny sposób, koszty bankowe IT to średnio ok. 7,3% przychodów banków. Jest to ok. dwa razy więcej niż średnia dla wszystkich pozostałych branż przemysłowych.

Czy banki mogą uzyskać podobne oszczędności bez chmury?

Teoretycznie tak, jest to jednak bardzo trudne w praktyce. W klasycznym outsourcingu za dostawcą przemawiały:

- efekt skali,
- specjalizacja,
- narzędzia i rozwiązania automatyzujące,
- możliwość lepszego wykorzystania zasobów krytycznych,
- większa elastyczność księgowa wynikająca z niestosowania międzynarodowych standardów księgowości.

Przeciwnicy outsourcingu wskazywali na:

- zagrożenie utratą kontroli nad IT,
- wzrost skomplikowania zarządzania zmianą,
- VAT od zasobów ludzkich.

Rozwiązania chmurowe, szczególnie te opierające się na chmurze publicznej dodatkowo pozwalają na wykorzystanie zmiennej mocy obliczeniowej. Nie dość, że odbiorca płaci jedynie za moc wykorzystaną, to dodatkowo dostawca może dzielić zapas mocy pomiędzy wielu odbiorców. Pozwala to na znacznie lepsze wykorzystanie mocy obliczeniowej a co za tym idzie energii potrzebnej na zasilenie i chłodzenie urządzeń. Olbrzymie serwery obsługujące wirtualne środowiska wraz ze wspartym automatyką dynamicznym przydziałem zasobów jeszcze bardziej wzmocniły efekt skali.

Wszelakie wymogi regulacyjne stawiane przed centrami danych, chociażby rozwiązania *disaster recovery* czy plany ciągłości działania, przygotowane dla jednego odbiorcy pasują do każdego następnego.

Zaawansowana wirtualizacja wraz z automatyzacją pozwalają tworzyć gotowe instancje serwerowe w ciągu sekund. Zaawansowane środowiska deweloperskie są dostarczane w modelu SaaS z opłatą powiązaną z komercyjnym wykorzystaniem stworzonego oprogramowania. Środowiska te mają wbudowane setki API pozwalające na łatwość integracji z otaczającym światem. Wszystko to ma wpływ na „time to market" dla nowych produktów i usług bankowych.

Chmurowe wyzwania

Co nas powstrzymuje przez upowszechnieniem bankowości w chmurze?

Na pewno regulacje, których istnienie w znaczącym stopniu wynika z:

- obaw o bezpieczeństwo powierzonych bankom środków i przetwarzanych przez banki danych,
- obaw o jednoznaczność co do odpowiedzialności za popełnione błędy,
- oczekiwania wskazania miejsca przetwarzania danych – coraz śmieszniej wyglądające w naszym zwirtualizowanym świecie,
- konieczności budowania innych, nowych umiejętności zarówno przez bank, jak i organy nadzorcze,
- niechęci do outsourcingu – bo przecież bank w chmurze to jego forma,
- przekonania banków, że nikt nie zrobi tego lepiej niż my sami.

Wchodząc w rozwiązania chmurowe w Polsce, w szczególności dla procesów krytycznych, banki muszą zwrócić uwagę na następujące obszary[5]:

1. **Odpowiedzialność**. Korzystanie przez banki z usług informatycznych w modelu przetwarzania chmurowego należy weryfikować pod kątem wymogów ustawowych dotyczących outsourcingu w działalności bankowej. Polski nadzór bankowy regulując outsourcing na ogół nie zezwala na to, aby dostawca usługi krytycznej mógł ograniczyć swoją odpowiedzialność za szkody wyrządzone nienależytym jej wykonaniem.
2. **Bezpieczeństwo informacji.** Regulatorzy europejscy, w tym polski, oczekują , aby instytucja finansowa znała i kontrolowała swoje ryzyko operacyjne, w tym, w szczególności, aby zapewniała bezpieczeństwo informacji prawnie chronionej. Warunkiem zapewnienia bezpieczeństwa i świado-

5 Cloud computing w sektorze finansowym. Regulacje i standardy, www.zbp.pl, 2011

mego zarządzania ryzykiem jest znajomość ryzyka. Ustawodawca i regulator oczekują od organizacji, że nawet w przypadku przekazania na zewnątrz danej czynności, organizacja będzie w dalszym ciągu faktycznie monitorować ryzyko z tym związane, nie poprzestając na sferze zobowiązań prawnych czyli zapewnień.

3. **Ciągłość działania.** Jest to jeden z aspektów bezpieczeństwa informacji – bezpieczeństwa w aspekcie dostępności informacji.
4. **Monitorowanie ryzyka.** Wiedza o tym, jakie jest rzeczywiste ryzyko związane z korzystaniem z usług podmiotu zewnętrznego.
5. **Ochrona danych osobowych.** Przetwarzanie danych w chmurze będzie legalne, o ile odbiorca chmury dopełni wszystkich obowiązków z zakresu ochrony danych osobowych. Praktycznie oznacza to, że dostawca chmury musi zapewnić odbiorcy chmury (który odpowiada za dane osobowe przetwarzane w chmurze), że przetwarzanie danych osobowych w chmurze nastąpi zgodnie z regulacjami.
6. **Dopuszczalne miejsce przetwarzania poza Polską (jeśli mamy do czynienia z takim przypadkiem).** Dodatkowo, jeśli lokalizacja chmury miałaby wykraczać poza Europejski Obszar Gospodarczy, konieczne jest zapewnienie podstawy prawnej (najczęściej zgody GIODO) na eksport danych do dostawcy chmury.

Nadzory innych krajów Unii Europejskiej potrafią mieć bardziej otwarte podejście do zagadnienia wykorzystania chmury w bankowości. O regulacjach obowiązujących w Holandii pisaliśmy powyżej, teraz omówimy podejście brytyjskiego regulatora sektora finansowego, który reprezentuje[6] dość pragmatyczne podejście do tematu wykorzystania chmury przez banki:

1. Nie ma zastrzeżeń, co do metody – w dokumencie z listopada 2015 r. można znaleźć następujące stwierdzenie:

   Punkt 1.6: „Nie widzimy żadnego powodu, dla którego podstawowe usługi chmurowe (łącznie z usługami w chmurze publicznej) nie mogą być wprowadzone w życie, z odpowiednim uwzględnieniem cech i sposobu, który jest zgodny z obowiązującymi przepisami.
2. „Cloud computing" jest usługą outsourcingową i w jego przypadku mają zastosowanie wszystkie przepisy outsourcingu.

6 „Proposed guidance for firms outsourcing to the 'cloud' and other third-party IT services"p. 2

3. Wydaje się, że jest to kluczowy punkt, ważny dla banków i potencjalnych dostawców tych usług:
   Punkt 6.5: „W przypadku, gdy prawna osoba trzecia świadczy usługi w imieniu firmy regulowanej – w tym dostawcy chmury/usług chmurowych należy pamiętać, że jest to uważane za outsourcing, firmy muszą podlegać odpowiednim obowiązkom regulacyjnym i sprawdzić jak są one zgodne z nimi". Przede wszystkim oznacza to, że klient nie może uchylać się od obowiązku wymagań audytowych twierdząc, że dostawca zlecenia ma do czynienia z nimi. Bank lub instytucja finansowa musi wykonywać z należytą starannością i w sposób ciągły badania firmy outsourcingowej w zgodności z regulacjami.
4. Możliwe jest zablokowanie przez dostawców usług dostępu do niektórych pomieszczeń. Głównym celem audytu powinny być elementy istotne dla sprawowania skutecznego nadzoru niekoniecznie wymaga to dostępu do wszystkich pomieszczeń roboczych. Usługodawcy mogą, z uzasadnionych względów bezpieczeństwa, ograniczyć dostęp do niektórych miejsc, takich jak centra danych.
5. Tak więc przedmiotem dyskusji jest definicja „uzasadnione względy bezpieczeństwa". Problem istnieje w przypadku usługodawców, którzy mają wielu klientów, oczekiwanie zatem nie leży w sprzeczności z wymogiem, ale ryzykiem, by nie odsłonić różnic konfiguracji pomiędzy klientami.

Zmiana otoczenia rynkowego

Korzystając z regulacji Narodowego Banku Holandii (DNB – organ regulacyjny systemu bankowego Holandii), bank ROBECO N.V. przeniósł całą swoją bankowość detaliczną na platformę w chmurze w celu zmniejszenia złożoności swojej infrastruktury i kosztów operacyjnych, przy jednoczesnym zmniejszeniu czasu dostarczania nowych rozwiązań.

Bankinter – szósty co do wielkości bank w Hiszpanii wykorzystując usługi chmurowe skrócił symulację ryzyka kredytowego z 23 godz. do 20 min. Używając rozwiązań chmurowych może skalować ogromne ilości technologii i infrastruktury na żądanie, a płacić tylko za to, co wykorzystuje. Taka zdolność obliczeniowa dostępna na żądanie jest niezwykle ważna w bankowości.

Bank Suncorp z Australii, który zawsze kładł nacisk na innowacje, rozpoczął pracę w prywatnej chmurze i wirtualnym centrum danych w czasie krótszym niż trzy miesiące, z planem przeniesienia do chmury 2 tys. aplikacji.

Zitouna Bank w Tunezji wybrał usługi chmurowe dla swojego bankowego systemu centralnego TEMENOS. Celem projektu ma być wspieranie strategii banku i umożliwienie otwierania nowych placówek oraz rozwijania bankowości mobilnej i usług internetowych.

Ogromne znaczenie dla rozwoju rozwiązań chmurowych powinna mieć regulacja PSD2. Poprzez wymuszenie na bankach możliwości dostępu do rachunków bankowych przez szeroko dostępne API, dość hermetyczny świat banków automatycznie otworzy się na integrację z otoczeniem. Świat FinTech-ów od początku istnieje i działa w chmurze i w naturalny sposób oczekuje się, że banki będą przetwarzać swoje dane w chmurze, co zostanie wsparte również przez regulatorów.

Podsumowanie

Rozwiązania chmurowe są dzisiaj dylematem strategicznym dla banków. Dyskusja dotycząca skali i zakresu adopcji tych rozwiązań powinna być poprzedzona wnikliwą analizą, przeprowadzaną przez cały zespół zarządzający bankiem. Tak, jak w przypadku outsourcingu, pewne decyzje co do wyboru rozwiązań i partnerów biznesowych (dostawców) powinny być podejmowane z rozwagą i przekonaniem. W wielu przypadkach jest to podróż w jednym kierunku: dostawcę można oczywiście zmienić, ale powrót do poprzednich rozwiązań IT jakie obserwujemy w sektorze bankowym dzisiaj, może być trudna. Poniżej zostały przedstawione trzy elementy zaczerpnięte z raportu [2], które pomagają firmom dokonać udanej transformacji do rozwiązań chmurowych i o których należy pamiętać, zaczynając takie przedsięwzięcie.

Transformacja organizacji do rozwiązań chmurowych to proces ciągły, który ma początek

Aby zrealizować zakończone sukcesem wdrożenie rozwiązań w chmurze, realizując przy tym długoterminowe korzyści biznesowe poszczególne etapy przeniesienia nie powinny być postrzegane jako kolejny projekt wdrożenia technologii, ale raczej jako podróż prowadząca do realizacji strategii.

Transformacja do rozwiązań chmurowych – wymaga przywództwa

Organizacje, w których brakuje jasno określonej hierarchii decyzyjnej mogą być narażone na wewnętrzne konflikty związane z wywoływanymi zmiana-

mi, co może utrudnić transformację. Organizacje powinny dążyć do zarządzania projektami transformacji centralnie, z zespołem wyższego szczebla, który nadzoruje proces transformacji i prowadzi do strategicznych decyzji.

Działanie nastawione na mierzalny sukces
Organizacje powinny zakreślić realistyczny plan i opracować wymierne metody pomiaru efektów dla swoich projektów transformacyjnych, tak aby transformacja chmurowa była związana z kluczowych celami biznesowymi.

Wnioski

Czy bankowość w chmurze to po prostu nowa metoda na oszczędności kosztów?

Sądzimy, że nie – dla nas rozwiązania chmurowe są tylko etapem prowadzącym w stronę innego świata. Jest to również kolejny krok w świat innych modeli biznesowych dla banków. Czy warto czekać ? Wydaje się, że nie. Może się okazać, ze opóźnienia z wykorzystaniem rozwiązań chmurowych w porównaniu do świata będzie bardzo trudno nadgonić. Dziś lubimy powtarzać, że mamy bardzo nowoczesną bankowość z unikalnymi rozwiązaniami. Ale jak długo tak będzie?

Dwa kolejne trendy technologiczne – Internet rzeczy (IoT – Internet of Things) oraz Blockchain – dokonają w przyszłości jeszcze większej rewolucji. Moc obliczeniowa, której banki poszukują w chmurze, jest dostępna w telefonach komórkowych klientów – w ilości spokojnie wystarczającej do przetworzenia transakcji niejednego banku. A przecież w każdym domu, biurze, samochodzie są setki, o ile nie tysiące, małych niewykorzystanych procesorów. Żyjemy w świecie nadmiaru mocy obliczeniowej. Procesory już teraz zaczynają tworzyć świat internetu rzeczy. Jeśli połączymy to z technologią blockchain możemy uzyskać rozwiązanie zarówno wydajne jak i bezpieczne.

Bibliografia:

Global Spending on Cloud Computing: An Evolutionary Road Map for Financial Services, Tower Group, May 2010

KPMG Global Technology Innovation Survey – 2014

Proposed guidance for firms outsourcing to the ‘cloud’ and other third-party IT services – UK FCA – November 2015

Sudhir Sriram, Cloud Computing in Banking, CapGemini,2010

https://cashmanagement.bnpparibas.com/print/3363, published 08.09.2015

Christian Nentwich, The Cloud and Banks: A summary of the FCA’s Guidance, January 2016

Some Banks Are Heading To The Cloud -- More Are Planning To. Forbes-26.06.2014

Guidance consultation 15/6, Proposed guidance for firms outsourcing to the ‘cloud’ and other third party IT services, Financial Counduct Authority

David Mote, How banks are now making their way into the cloud, Safe Swiss Cloud

Timothy Prickett Morga, Why Clouds are a risky proposition for big banks and brokers. 22.09.2015, The Next Platform

Piotr Puczyński

Wiceprezes Banku Gospodarstwa Krajowego.

W trakcie swojej trwającej ponad 25 lat kariery zawodowej zajmował się przede wszystkim wprowadzaniem nowych rozwiązań, zmian i innowacji w dużych instytucjach sektora finansowego. Działania te podejmował pracując zarówno jako menedżer odpowiedzialny za IT i finanse w firmie wprowadzającej zmianę, jak i jako osoba świadcząca usługi w zarządzaniu zmianą w formie zewnętrznych konsultacji. Do BGK przyszedł z Poczty Polskiej SA, gdzie pełnił funkcję Dyrektora odpowiedzialnego za Strategię IT, Architekturę IT oraz za zarządzanie portfelem projektów. W latach 2009-2013, jako niezależny konsultant oraz Szef działu Sprzedaży Usług Microsoft Polska współpracował m.in. z Bankiem DNB w projekcie restrukturyzacji operacji finansowych na Litwie, z Bankiem BOŚ, Bankiem ING Bank Śląski i BRE Bankiem. Wcześniej w latach 2004-2009 pełnił funkcję CIO w Grupie PZU, gdzie przeprowadził projekt centralizacji IT zarówno w warstwie organizacyjnej, jak i w części aplikacji. W latach 1989-2004 pracował w sektorze bankowym (Bank Millenium, Bank BWE, Bank NORD L/B) pełniąc funkcje CIO i CFO. W tym okresie uczestniczył w szeregu projektach związanych z wprowadzaniem do polskiej bankowości nowoczesnych technologii.

Ukończył Wydział Matematyki, Informatyki i Mechaniki na Uniwersytecie Warszawskim na kierunku zastosowań matematyki, a także program AMP na prestiżowej uczelni IESE.

Piotr Puczyński, BGK

CRM czyli w poszukiwaniu Świętego Graala

Praca w dużej amerykańskiej korporacji miała być dla mnie nowym wyzwaniem. Po pierwsze po raz pierwszy przechodziłem na drugą stronę „barykady", czyli miałem pracować „u dostawcy". Po drugie, nigdy wcześniej w mojej karierze nie miałem do czynienia z tak rozległą, globalną organizacją. Rozpoczynałem zdając sobie sprawę, że wiele spraw będzie dla mnie nowych i zaskakujących. Tak naprawdę to było głównym powodem podjęcia się nowego zadania, które z punktu widzenia mojego życiorysu było zadaniem „dziwnym".

Tak więc pojawiając się w nowym miejscu wydawało się, że jestem przygotowany na kwestie związane z koniecznością stosowania globalnych procedur, z pracą z zespołem, który zna klienta tylko „od zewnątrz", z wyzwaniami braku czasu i zasobów. Jednak naprawdę dużym i zaskakującym problemem stał się system X, określany przez wszystkich jako „nasz CRM".

Wstępna analiza pokazała, że problem nie powinien zupełnie istnieć. Każdy sprzedawca raz w tygodniu, na podstawie własnej oceny, wypełnia dane w systemie, mające określić zaawansowanie w procesie sprzedażowym. Dla mnie, człowieka o myśleniu projektowym, było to naturalne. Każdy uczestnik projektu, odpowiedzialny za konkretny wątek, musi wypełnić przynajmniej raz w tygodniu raport/narzędzie, które pokaże zaawansowanie prac. Bez tego zarządzanie projektem to jak poruszanie się po lesie w gęstej mgle. Jednak im więcej rozmawiałem na ten temat, tym mniej rozumiałem. Osoby, o wykształceniu w większości technicznym, mówiły coś o niejasności systemu i niewygodzie z korzystania. System podobno się zawieszał (sam tego nigdy nie doświadczyłem). Ogólny przekaz – „nie da się". Z drugiej strony presja na korzystanie z systemu rosła, gdyż służył on m.in. do prognozowania sprzedaży. Sprawę na bieżąco udało się unormować w formie polecenia, wykonywanego posłusznie, acz

bardzo niechętnie. Dla mnie jednak pytanie, dlaczego system X stanowił taki problem, większy nawet niż rzeczywista realizacja planu, pozostawało otwarte. Poniższe rozważania to podsumowanie podjętej przeze mnie próby odpowiedzi.

Przykładowe „case study"

Najczęściej historia CRM zaczyna się od podstawowego i strategicznego pytania – „Co możemy zrobić, aby zwiększyć sprzedaż?". Standardowo, jako jeden z wniosków z dyskusji pojawia się stwierdzenie – „Potrzebujemy CRM". Nieważne, w jakim sektorze gospodarki i jak duże jest to przedsiębiorstwo. Nieważne, czy działamy globalnie, czy też nasz rynek jest ograniczony do kraju, czy też nawet jednego miasta.

Kolejny krok to przygotowanie analizy opłacalności projektu wdrożenia CRM. Każda firma wymaga takiej analizy przy podejmowaniu decyzji inwestycyjnej. Analizy te są bardziej lub mniej zaawansowane, konieczne jest jednak najczęściej stworzenie tzw. „business case". I tutaj zaczyna się problem, bo mimo, że zaczęliśmy od przychodów („Jak zwiększyć sprzedaż?"), to określenie, ile konkretnie możemy oczekiwać zwiększenia sprzedaży po zakończeniu projektu i jaki będzie nasz zwrot z inwestycji, okazuje się być skomplikowane.

W jednej z firm, dla których pracowałem, miałem przyjemność prowadzić mały warsztat na temat – „Co dla nas oznacza inwestycja w CRM?". Bardzo szybko udało nam się opisać funkcjonalności jakich potrzebujemy, choć lista była długa. Oszacowaliśmy również niezbędne nakłady. Drobny spór pojawił się, gdy poruszyliśmy temat wdrożenia i ile czasu nam na nie potrzeba, ale i to udało nam się uzgodnić. Wszystko szło sprawnie, aż do momentu określania, jak zwiększy się sprzedaż firmy po wdrożeniu nowego rozwiązania. Skąd pojawią się strumienie przychodów? W jakiej wysokości? Tutaj utknęliśmy na dobre. Nie udało nam się wyjść ponad bardzo ogólne sformułowania, których przełożenie na konkretne liczby wymagane przez model finansowy było absolutnie niemożliwe. A model finansowy nie przyjmuje w części opisującej przychody sformułowań „będziemy więcej wiedzieli o kliencie" czy „stworzymy produkty lepiej dopasowane do klienta".

To jest moment, do którego dociera wiele firm w procesie „wdrożenia" CRM. Ale ponieważ mamy ogromna potrzebę posiadania CRM – stosowne wyliczenia powstają, a decydenci (najczęściej jest to Zarząd Firmy) ten mało

realistyczny plan akceptują. Nikt przecież nie będzie kwestionował, że potrzebujemy CRM. Poza tym „Wszyscy przecież już to mają". Po cichu jednak każdy zadaje sobie pytanie – ale co to jest ten CRM?

Dalsze kroki idą nam już jak z płatka. Powołujemy nowego Szefa Projektu, który dostaje bardzo precyzyjne zadanie – ma wdrożyć CRM. Do wykonania zadania dostaje przypadkowo wybrany zespół – przecież wszyscy inni są zajęci zwiększaniem przychodów i mogą co najwyżej pracować w Komitecie Sterującym.

Pieniądze płyną szerokim strumieniem i cały zespół jest niezmiernie zajęty. Nikt tak precyzyjnie nie potrafi powiedzieć, co jest określone jako nasz cel. Jaka jest miara sukcesu. Wiemy natomiast, że wszystko powinno być zrobione na wczoraj. I wszystko, każdy nawet najdrobniejszy pomysł realizujemy z najwyższym priorytetem.

Wreszcie nadchodzi TEN DZIEŃ. System zostaje uruchomiony. Najczęściej bez fanfar, gdyż oczywiście jest już „za późno".

I, niestety, okazuje się po kilku miesiącach, że z systemu nikt nie korzysta…

CRM wg Gartnera

Być może ktoś zarzuci mi nadmierny pesymizm lub wręcz złośliwość w ocenie projektów CRM. Można powiedzieć, że w trakcie mojej pracy zawodowej miałem wyjątkowego pecha i napotykałem w większości nieudane projekty. Być może trudno moje doświadczenia uogólniać…

A jednak powyżej zarysowany scenariusz, tak bliski moim doświadczeniom, znalazłem w raporcie firmy Gartner „CRM Implementation and Economics" przygotowanym przez Scott'a Nelsona już wiele lat temu (2001). Niestety, od tego czasu w mojej opinii niewiele się zmieniło w podejściu do projektów CRM.

Jednym z problemów jest brak jasnych kryteriów sukcesu czy też dokładnej definicji, co dla nas dzisiaj znaczy CRM. A to akurat uległo ogromnej zmianie i rozwojowi od wspomnianego wcześniej roku 2001. Niestety, sprawa znacznie się skomplikowała. O ile na przełomie wieków można było mówić o prostym podziale na CRM operacyjny i analityczny, to dziś jest to podział o wiele niewystarczający. Systemy klasy CRM, bo o takich należy dzisiaj mówić, są tak różnorodne, że Gartner zaprzestał tworzenia na ten temat swojego podstawowego raportu „Magic Quadrant", uznając, że na tak wysokim

poziomie ogólności klasyfikowanie dostawców może być dla odbiorców raczej mylące, a nie pomocne.

Obecnie Gartner dzieli aplikacje CRM na 100 podkategorii. W raporcie „Use Gartner's CRM aplication functionality starfish to evaluate your functionality requirements" znajdujemy informację, że w 2012 r. tylko 20% projektów klasy CRM miały charakter ogólno-korporacyjny. Większość to małe wyspecjalizowane rozwiązania ograniczające się nawet do wspierania pracowników w obrębie departamentu. Pokazuje to, że w jakiś sposób korporacje nauczyły się radzić sobie z różnorodnością i poprawnym definiowaniem potrzeb.

Jednak w tymże samym raporcie wskazane jest, że ponad 70% budżetu wydawane jest na cztery kategorie rozwiązań CRM:

- kampanie marketingowe,
- wsparcie procesu sprzedaży (Sales Force Automation – SFA),
- platformy e-commerce,
- obsługę zgłoszeń w „call center".

Jak CRM wspiera „proces sprzedażowy"

Jest wśród tych kategorii jeden specyficzny obszar, który nawet po wdrożeniu cieszy się powszechnie złą sławą wśród sprzedawców. To rozwiązania wspierające tzw. „proces sprzedażowy". Niemal w każdej korporacji konieczność uzupełniania CRM staje się niemal rytualnym problemem na każdym zebraniu sprzedażowym. Tworzone są nawet specjalne okna czasowe, w których sprzedawcy powinni zasiąść w biurze i wprowadzić dane pod czujnym okiem swojego kierownika. Podejście raczej jak do niesfornych uczniów niż do dojrzałych i odpowiedzialnych dorosłych ludzi.

Producenci oprogramowania starają się zyskać przychylność swoich przyszłych użytkowników dodając do podstawowej szereg dodatkowych funkcjonalności. Nie tylko integracja z kalendarzem i listą kontaktów, ale też mobilny dostęp ze smartfonu/tableta, integracja z mapą pozwalająca na wskazywanie drogi i czasu dojazdu do klienta, bieżący dostęp do danych o zrealizowanej kwocie i analizy typu „what if" – to tylko niektóre z nich. Ciekawe, czy zostaną one potraktowane przez „sprzedawców" jako gadżety, czy też pozwolą im bardziej oswoić się z narzędziem typu SFA. Obawiam się, że raczej to pierwsze.

Obserwując zespół sprzedażowy w jednej z dużych korporacji sprzedającej produkty technologiczne nie mogłem się nadziwić, jaka jest niechęć do systemu SFA. Na pewno nie była to bariera technologia, gdyż niemal wszystkie osoby wywodziły się z obszaru IT. Większość narzekań była zupełnie nieuzasadniona. Co więc było powodem tak wielkiej niechęci?

Pierwsza teza, jaka została postawiona to niechęć dzielenia się wiedzą o kliencie z kimkolwiek. Zwłaszcza z pracodawcą. Klient jest mój i wiedza o nim to moje aktywo. To coś co świadczy o mojej wartości na rynku. Zmieniając pracodawcę przechodzę do nowego ja i mój notes. Jest to opinia dość powszechna, jednak, gdy porozmawiamy zwłaszcza z doświadczonymi osobami zajmującymi się sprzedażą, musimy ją bardzo gruntownie zweryfikować. Bo czyż w dzisiejszych czasach tak trudno jest zdobyć numer telefonu do WAŻNEGO CZŁONKA ZARZĄDU? Przykłady pokazują, że przy odrobinie wysiłku można zadzwonić nawet do Papieża. Problem polega jednak nie na posiadaniu numeru telefonu, a na RELACJI. W uproszczeniu mówiąc – na tym, że osoba po drugiej stronie odbierze mój telefon i poświęci mi tyle czasu, ile potrzeba. Ważne, żeby mnie z uwagą wysłuchała. A do tego potrzeba znacznie więcej niż wiedzy o numerze telefonu, czy nawet o tym gdzie ostatnio Pani Prezes spędzała wakacje.

Rozmawiając z zespołem sprzedażowym zadałem pytanie, czy gdyby ktoś zabrał z biurka ich zeszyt z telefonami i informacjami o klientach, to czy byłby go w stanie wykorzystać. Po chwili zastanowienia stwierdzili, że w bardzo małym stopniu. Bo wartość ich relacji zapisana jest nie w tym zeszycie, a u klienta w postaci zaufania, jakim ich darzy.

Tak więc chęć utrzymania informacji o kliencie w poufności własnego zeszytu nie jest podstawą niechęci do SFA.

Nie jest to też konieczność spędzenia czasu na wpisywaniu informacji do systemu. Systemy zintegrowane z kalendarzem, systemem do prowadzenia notatek (np. OneNote), listą kontaktów, itp. znacznie ten czas skracają. Samo wprowadzanie danych nie jest tak bardzo obciążające, problemem wydaje się to co chcemy do systemu wpisać. Ale o tym za chwilę…

Pewnym problemem w akceptacji systemów SFA jest poddanie się kontroli. Wpisujemy dane, które stanowią podstawę do oceny naszej, sprzedawców, aktywności. Zapewne jest to temat wart dyskusji – na ile zespoły sprzedażowe powinny mieć „wolną rękę", a na ile powinny podlegać korporacyjnym procedurom. Jednak kwestia ta nie jest powiązana bezpośrednio z wdrażaniem

systemów SFA. Często systemy „kontroli" bazują na arkuszach kalkulacyjnych. Tak więc wprowadzenie nowego systemu może usprawnić sposób w jaki „kontrola" jest prowadzona.

Wygodniej jest też spędzić trochę czasu w samotności wpisując dane do narzędzia, niż na bieżąco opowiadać postępy prac podczas rozmowy z szefem w cztery oczy.

Jest to więc realna obawa. Nie jest ona jednak specyficzna dla systemu SFA. Każdy, nawet początkujący pracownik sprzedaży, zdaje sobie sprawę z istnienia systemu raportowania i konieczności informowania kierownika sprzedaży o swoich aktywnościach. Dlatego sprawnie funkcjonujący system SFA powinien być postrzegany jako ułatwienie komunikacji z Szefem. Nasze spotkania mogą być krótsze i bardziej treściwe, niż w przypadku braku jakiegokolwiek narzędzia. Dlatego sądzę, że po 2–3 miesiącach po wdrożeniu powinny zniknąć obawy o nadmierną kontrolę, a wszelkie dodatkowe funkcjonalności powinny wpłynąć na pozytywny odbiór nowego rozwiązania.

Inna kwestią jest, że na podstawie danych wprowadzanych do systemów, które mają „wspierać sprzedaż" powstają prognozy sprzedaży. Prognozy te są oczywiście „złem koniecznym". Konieczność wynika z wymagań rynków finansowych, a presja na precyzję tych prognoz na pewno będzie się utrzymywała na wysokim poziomie. Ta rola systemów SFA często staje się funkcją podstawową (albo nawet jedyną). Wprowadzamy do systemu dane dlatego, że na tej podstawie nasi szefowie i szefowie naszych szefów przygotowują prognozy sprzedażowe. Nie ma to więc wiele wspólnego z ideą CRM, czy też węziej – pomysłem na system SFA. Wydaje się, że należałoby opracować narzędzia w jeszcze jednej kategorii systemów „sprzedażowych" – prognozowanie sprzedaży. Współcześnie coraz częściej do wszelkiego rodzaju prognoz z coraz większym sukcesem wykorzystywane są narzędzia klasy Big Data oraz wszelkiego rodzaju metody BI. Firma DHL stosuje te metody do prognozowania ilości paczek, jakich spodziewa się w najbliższym czasie obsługiwać. Stosowanie takich narzędzi i zaawansowanych metod statystycznych wydaje się być bardziej poprawną metodą niż poleganie na danych wpisywanych przez sprzedawców pod presją budżetu.

Jak skutecznie wdrożyć CRM

Widać więc, że wykorzystywanie narzędzi SFA do prognozowania efektów sprzedaży i budowanie na tej podstawie systemów kontrolnych może być

realną przeszkodą przy wdrażaniu systemów. Jest to jeden z powodów braku akceptacji dla tych narzędzi. Czy jednak jest to diagnoza kompletna?

Wspomniany już wcześniej Gartner w raporcie autorstwa Eda Thompsona, opublikowanym w lutym 2013 („The eight building blocks of CRM"), prezentuje podstawowy schemat wdrażania CRM.

We wprowadzeniu autor pisze: "Każda inicjatywa CRM wymaga sprawdzonego sposobu, który zapewni, że podejdziemy do projektu w sposób zrównoważony, spójny i ze strategiczną wizją. Zastosowanie takiej metody pomoże inicjatorom i liderom projektu osiągnąć maksimum korzyści z prowadzonej przez nich inicjatywy CRM".

Zaproponowany schemat opiera się na ośmiu filarach:

- wizja CRM, czyli co rozumiemy pod pojęciem CRM,
- strategia CRM, czyli jak nasze działania wpisują się w ogólna strategię,
- doświadczenie klientów, czyli jaką wartość dodaną przynosi im nasz projekt,
- współpraca całej organizacji, wspierająca wprowadzane zmiany,
- procesy CRM, czyli spisane sposoby działania,
- informacja w CRM, czyli jak zbierać dane,
- technologia,
- miary sukcesu, czyli ustalone sposoby mierzenia i wartości parametrów wskazujących, czy osiągamy cele.

Jak widać procesy są równie ważne jak strategia, czy technologia. W zasadzie nie powinno to dziwić. O procesach we współczesnych korporacjach mówimy niemal we wszystkich aspektach ich funkcjonowania. W niektórych powstają specjalne komórki organizacyjne mające na celu budowanie czegoś, co określane jest jako „świadomość procesowa".

Takie podejście ma bardzo dużo zalet. Przede wszystkim, zwłaszcza dużym korporacjom, zapewnia jednolitość działania. To pozwala na zorganizowanie zarządzania korporacją w skali globalnej. Każdy dobrze opisany proces posiada jasno określone i mierzalne wskaźniki efektywności. Mierzenie i porównywanie tych wskaźników, przynajmniej w teorii, powinno wskazywać, jak skutecznie działają poszczególne jednostki regionalne.

Procesy to też wpisanie w nasze działania zasady przyczynowo – skutkowej. Całość działań podzielona jest na etapy tak, że zakończenie jednego z nich stanowi jednocześnie początek kolejnego. Określamy produkty każdego z etapów. Zakładamy, że początek kolejnego kroku jest uzależniony od

zakończenia poprzedniego, gdyż korzysta on z produktów swojego poprzednika. W ten sposób proces porządkuje nam rzeczywistość. Daje nam też możliwość przewidywania, kiedy dana praca się skończy, gdyż monitorujemy stan prac na zasadzie stanu, gdzie jesteśmy w porównaniu do czasu przewidzianego w naszych miarach efektywnościowych.

Na końcu wszelkie podejście procesowe jest szczególnie „odpowiednie" dla wszelkiego rodzaju systemów IT. Logika procesu, kolejność działań ustalona i niezmienna, odpowiednio określone produkty poszczególnych etapów bardzo odpowiadają „żelaznej" logice systemów. Na tym bazują m.in. wszelkie systemy typu „workflow".

Podstawowa zasada jest jedna – nie zaczynaj kolejnego etapu, jeżeli nie skończyłeś poprzedniego.

Zwracam uwagę, że powyższe fundamenty dla wdrożenia CRM są jednolite dla wszystkich kategorii CRM. Również dla będącego w naszym obszarze zainteresowania systemu klasy SFA. Nie jest to dziwne, gdyż powszechnie mówimy o procesie sprzedażowym. Proces ten jest szczególnie dokładnie opisany w dużych korporacjach, a jego przestrzeganie stanowi jedno z podstawowych przykazań biznesu. W niektórych firmach wiara w skuteczność procesu jest tak silna, że w przypadku, gdy zaczynają się kłopoty związane z brakiem realizacji zakładanego poziomu sprzedaży – procesy ulegają większemu uszczegółowieniu i są egzekwowane bardzo restrykcyjnie.

Podejście procesowe stanowi także podstawę wielu metod określania prognozy sprzedażowej. To, na jakim etapie są prace nad konkretnym kontraktem, stanowi podstawę do określania, kiedy potencjalnie można spodziewać się podpisania kontraktu. Ponieważ, jak już wcześniej wspominałem, systemy SFA niezwykle często stosowane są do wspierania procesu przygotowywania prognozy sprzedażowej, są one w naturalny sposób skonstruowane i wdrażane z myślą o „procesie sprzedażowym". Proces ten stanowi wręcz osnowę wokół której poszczególne funkcjonalności powstają. Jednocześnie wdrażając tej klasy rozwiązanie mamy nadzieję, że, automatyzując opisany wcześniej proces, dostarczamy wartość, która spowoduje akceptację systemu przez zespół sprzedażowy. A dzięki tej akceptacji unikniemy wspomnianej na początku klasycznej sytuacji związanej z wdrożeniami systemu – czyli stanu, w którym nikt z niego nie korzysta.

Powstaje tutaj pytanie, czy takie podejście rzeczywiście daje nam dużą szansę na sukces wdrożenia. Sukces w tym przypadku opisany powinien być

jako powszechna akceptacja nowego systemu ze wskazaniem, że spełnia on wszystkie wymagania stawiane mu w ramach strategii, wartości dla klientów i efektów biznesowych.

Problemy z akceptacją zmiany

Z moich doświadczeń wynika, że w najlepszym wypadku udaje się uzyskać neutralny stosunek do takiego „procesowo" wdrożonego rozwiązania.

Starając się zrozumieć ten fenomen, spędziłem sporo czasu dyskutując ze sprzedawcami, gdzie leży problem. Nie udało mi się co prawda uzyskać precyzyjnej odpowiedzi, ale najczęściej powtarzające się zdanie to „… bo nasza praca nie tak wygląda, a sprzedaż nie tak działa".

Jeżeli więc proces sprzedażowy został wiernie odzwierciedlony w systemie, to skąd taka odpowiedź? Doszedłem do wniosku, że skoro brak nam „konkretnych" zarzutów, to mamy do czynienia z problemem w warstwie psychologicznej. Nie jest to nic zaskakującego w projektach. Większość problemów przy wdrażaniu nowych narzędzi wiąże się z brakiem akceptacji zmiany. Wstępne odrzucenie „nowego" to często spotykana i w miarę „naturalna" reakcja. Problemy w projektach w ogromnej większości nie mają charakteru technicznego, a są związane z psychologią.

Jednak w omawianym tutaj przypadku systemów SFA niechęć utrzymuje się nawet po latach korzystania z systemów. Nie zmienia się, gdy sprzedawca zmienia pracę i trafia w nowe środowisko z nowym systemem. Dlatego myślę, że niechęć do „nowego" nie ma tutaj zastosowania.

Podążyłbym jednak tropem psychologii jako źródła „odrzucenia" systemów SFA.

Problemy ze współpracą

Metody bazujące na teoriach psychologicznych stosowane są w teorii i praktyce zarządzania od dawna. Wydaje się jednak, że w ostatnich latach stały się one niezmiernie popularne. W szczególności zwrócono uwagę na kwestie związane ze współpracą w zespołach. Dlaczego dla niektórych współpraca jest naturalna z jednymi, a z innymi wręcz przeciwnie? Co to znaczy „brak chemii" między dwoma pracownikami? Jak budować zespoły?

Badając te kwestie zwrócono uwagę na teorie związane z typologiami osobowości. Za ojca współczesnych teorii typologii osobowości uważa się Karola Gustawa Junga. Zauważył on, że pomimo identycznego zbioru archetypów, które napędzają nas od wewnątrz (instynkty), różnimy się w naszych preferencjach, skłonnościach do tego, co wybieramy i w jaki sposób funkcjonujemy. Na tej bazie powstały tzw. funkcje psychiczne kategoryzujące ludzkie osobowości. Należy pamiętać, że wkraczamy tutaj na terytorium mocno nieokreślone. Poczynając od definicji samego słowa „osobowość". Jedna z popularnych definicji to „osobowość to niepowtarzalny i względnie stabilny wzorzec zachowań, myślenia i emocji prezentowanych przez daną osobę" (*D.M. Buss, N.Cantor „Personality psychology: Recent trends and Emerging Directions", Nowy Jork, Springer 1989).*

Mimo pewnych niedokładności warto zwrócić uwagę, jak udało się zbudować kilka typologicznych podejść do kwestii osobowości.

Wiele z nich to systemy czterech typów powstające jako iloczyn dwóch wymiarów. Najbardziej klasyczne podejście, wywodzące się od wspomnianego wcześniej Karola Junga ustanawia te dwa wymiary w następujący sposób. Jeden z nich mieści się pomiędzy „myśleniem" i „uczuciem". Drugi to przestrzeń pomiędzy „intuicją" i „zmysłami". Z czasem stwierdzono, że klasyczny podział jest zbyt restrykcyjny i utworzono systemy uwzględniające obszary pośrednie. Powstał też system oparty na koncepcji osobowości Junga, rozszerzający podstawowe parametry o jeszcze dwa wymiary i wprowadzający następujące osie: *ekstrawersja – introwersja, myślenie – uczucia, intuicja – doznanie i obserwowanie – ocenianie.* Dodając do tego praktyczne narzędzie typologii utworzono niezmiernie popularną w biznesie typologię MBTI. Zetknęli się z nimi pracownicy większości globalnych korporacji na całym świecie. Wyniki badań za pomocą tego narzędzia są uważane za wiarygodne i znaczące przy podejmowaniu decyzji personalnych. Dotyczy to zarówno określania wymagań w procesach rekrutacyjnych, jak i postępowania w sytuacjach konfliktowych. Sam wielokrotnie doświadczałem, jak osoby często skonfliktowane, po przejściu badania MBTI i skonfrontowaniu wzajemnych wyników, wypracowywały metodę współpracy, która usunęła większość barier.

Metodę możemy stosować również ustalając optymalny skład zespołu, czy też określając wymagania na określone stanowisko.

Ponieważ jestem „użytkownikiem" a nie badaczem powyższych teorii, w tym miejscu zatrzymam rozważania na temat kolejnych wersji typologii,

zostawiając je specjalistom. Wracając do głównego nurtu rozważań skoncentruję się na podstawowej wersji typologii opierającej się na modelu dwuwymiarowym. Jest on nadal często stosowany. Dla ułatwienia opisu dwuwymiarowej typologii stosujemy skonstruowany na tych wymiarach układ współrzędnych, gdzie oś X reprezentuje skalę „zmysły/empiria" – „intuicja", a oś Y to „myślenie/logika" – „emocje". W tym modelu powstają cztery obszary, określane kolorami: czerwony – łączący „logikę" i „intuicję"; żółty – łączący „intuicję" i „emocje"; zielony – łączący „empirię" i „emocje", oraz niebieski – łączący „empirię" i „logikę".

W tym miejscu warto poczynić kilka zastrzeżeń.

Po pierwsze, żadne z powyższych określeń nie jest określeniem zalet i wad. Nie należy traktować, że logika to coś lepszego niż emocje albo „empiria" jest lepsza od „intuicji". Są to przybliżone opisy cech, które sprawiają, że ludzie są różni. Nie ma jednak tutaj miejsca na ocenę i wartościowanie. Raczej mówimy o odpowiednich sposobach zachowań i dopasowaniu do roli.

Po drugie, jak już wcześniej wspomniałem, wszelkie typologie mają charakter przybliżony. Nie jest to dokładne określenie osobowości. Odnosi się to zarówno do przyporządkowania konkretnej osoby do właściwego typu, jak i do wszelkich opisów związanych z typami. Wiadomo, że jest to próba opisania czegoś tak skomplikowanego jak ludzka osobowość, co jest skazane na szereg uproszczeń i uogólnień.

Po trzecie wreszcie, dopasowanie typów do konkretnych ról też ma charakter uśredniony. Jeżeli powiemy, że typ niebieski to klasyczny typ księgowego, nie oznacza to, że ktoś określany jako czerwony nie może z powodzeniem wykonywać tego zawodu. Staram się wnioskować na bazie obserwacji statystycznych, uznając jednak, że istnieją specyficzne sytuacje wymagające zupełnie innych niż podstawowe cechy.

Wracając do rozważań dotyczących obszaru sprzedaży i narzędzi wspierających typu SFA, popatrzmy na ten obszar z perspektywy typów osobowościowych.

Oczywiście specjaliści będą się wielokrotnie zastrzegać, że nie ma idealnego profilu, że zależy to od wielu czynników. Zależy od branży, produktów, modelu biznesowego, etc. Jest to, moim zdaniem, bardzo asekuracyjne podejście. Pamiętając wszelkie zastrzeżenia poczynione powyżej, aby teorie typologii miały jakiś sens praktyczny, musimy podjąć się pewnych kategoryzacji.

Zresztą jeżeli jesteśmy w stanie (przy pewnych założeniach) skategoryzować osobowości w 4., albo nawet w 8. kategorii, to przypisanie pewnej grupie zawodowej szczególnie predysponowanej kategorii nie wydaje mi się zbyt wielkim uogólnieniem.

Dodatkowym argumentem wydaje się być istnienie wielu osób, które pracowały z sukcesem w sprzedaży zupełnie niezależnie od branży, grupy klientów czy modelu biznesowego. Spotkałem znakomitego sprzedawcę, który z równym sukcesem sprzedawał w trakcie swojej kariery groszek w puszkach, kredyty w banku i spawarki we własnej firmie. Sam twierdził, że sprzedaż to sprzedaż i albo to potrafisz, albo nie.

Powyższe argumenty bardzo zachęcają mnie do przynajmniej przybliżonego określenia idealnego typu osobowości dla ogólnie rozumianej grupy sprzedawców.

Osobowość sprzedawcy

Zacznijmy od kategorii „niebieskiej" czyli łączącej w sobie „logikę" z „empirią". Ogólny opis tej osobowości mówi, że mamy do czynienia z osobą, która zwraca uwagę na szczegóły, fakty, analizy i dane. Bardzo dokładnie analizuje. Precyzja i dokładność to są określenia dobrze opisujące jej styl pracy. Co ważne, jest to osoba myśląca linearnie. W tym myśleniu linearnym działanie sekwencyjne jest dla niej naturalne. Widać więc, że proces to jego żywioł. Osoby „niebieskie" zawsze wszystko precyzyjnie analizują, poddają obiektywnej refleksji i pozostają bardzo realistyczne.

Wydaje mi się, że jest to osobowość niemal dokładnie przeciwna do klasycznego sprzedawcy. Sprzedawca to chodzący optymizm. Analizy go nudzą. Najczęściej powie, że nie ma co gadać, tylko trzeba iść do klientów.

Ciekawe jest obserwować, jak dobry inżynier decyduje się podjąć wyzwanie związane ze sprzedażą. Szczególnie w firmach technologicznych jest to bardzo kuszące dla specjalistów. W końcu jako wykonawcy kontraktów mają kontakty z klientami, a możliwości większych zarobków, przynajmniej teoretycznie (to znaczy z uwzględnieniem premii sprzedażowej) są bardzo kuszące. Taka osoba przede wszystkim spojrzy na dostępne „narzędzia", zaczynając od procesów i procedur, a na wszelkiego rodzaju sesjach analitycznych typu „account planning" kończąc. W kolejnym kroku zadba, żeby wszystko zostało wdrożone. Procedury dokładnie wdrożone, plany dla wszystkich

klientów przygotowane, mechanizmy kontrolne ustawione. Jak wszystko będzie gotowe, to wówczas spodziewa się, że ten cały mechanizm zadziała. Maszyna zbudowana zgodnie z planami powinna dobrze funkcjonować. Wówczas pojawia się zdziwienie – nie działa. Bo sprzedaż to nie tylko mechanizmy i procedury. To również, albo przede wszystkim część związana z relacjami, emocjami i… szczęściem.

Dlatego poszukując idealnego opisu osobowości sprzedawcy mocno przyjrzałbym się kategorii „żółtej" łączącej „emocje" z „intuicją". Jest to kategoria pozostająca w opozycji do kategorii „niebieskiej".

Osoby o takiej osobowości cieszą się z przebywania między ludźmi. Ich optymizm i zapał udziela się otoczeniu. Spontanicznie podejmuje działanie. Lubi eksperymentować i szuka cały czas nowych rozwiązań. Jest to osoba myśląca całościowo i wielowątkowo. Lubi wykonywać wiele czynności jednocześnie. Mająca pozytywne nastawienie wobec innych. Uwielbiająca towarzystwo i autentycznie każdym się interesująca. Każda osoba to wyzwanie poznawcze. Zawsze pełna energii i nawet ciężko pracując, potrafiąca cieszyć się życiem.

W jednej z charakterystyk „żółtych" można dostrzec ich „mimowolny" wpływ na otoczenie, związany z powszechną akceptacją, która jest dla nich bardzo ważna. Ten „przypadkowy" wpływ sprawia, że… wydarzenia często układają się po ich myśli. Czy nie jest to właśnie to coś nazywane przez nich samych szczęściem? Wygląda, że poprzez otwarte podejście do innych dają szansę pozytywnemu przebiegowi wydarzeń.

IT kontra sprzedawcy

Pracując jako kierownik projektów z ogromnym składnikiem technologicznym (tzw. projekty IT) oraz zarządzając dużymi organizacjami IT wspierającymi główny biznes (banki i ubezpieczenia), wielokrotnie przychodziło mi rozstrzygać spory pomiędzy biznesem i IT. Z założenia spory, które nie powinny powstawać, często mnożyły się i powodowały wręcz zastój w projektach, bo konflikty potrafiły trwać miesiącami. Często próbowałem zanalizować powstające spory i dojść do ich sedna. Co leży u jego podstaw?

Na początku zauważyłem, że relatywnie łatwo realizuje się projekty w księgowości. Na zupełnie drugim biegunie były produkty w obszarze sprzedaży. Dlatego zacząłem spędzać więcej czasu na dyskusjach z działami

sprzedaży. Zwłaszcza, że słyszałem stałe narzekania, że „Oni" (czyli „sprzedaż") nie wiedzą czego chcą i, mówiąc wprost, mogliby zacząć myśleć. Znałem tych ludzi i uważałem ich za mądrych, więc zaciekawiło mnie, skąd ta opinia o myśleniu.

Po pewnym czasie doszedłem do wniosku, że sposób myślenia zespołów sprzedażowych przypomina mi patchwork. Zaczynamy budować w różnych miejscach, nieraz bardzo odległych. Czasem wydaje się, że od końca, a czasem, że od środka. Człowiek myślący „linearnie", procesem, szybko ma poczucie chaosu. Gubi logikę. Bardzo to różniło się od „uporządkowanego" świata księgowych. Co ciekawe jednak – jeżeli wyczekało się do końca, to te „wyspy" łączyły się w jedną całość. Powstawał, może i nieco łatany, ale jednak piękny „patchwork". Sprzedawcy po prostu myśleli inaczej. Wróciłem z myślą, że jeżeli ktoś nie myśli tak jak MY, nie oznacza to, że nie myśli.

Jakiś czas później, gdy podzieliłem się powyższym przykładem z jednym z psychologów, z którym miałem przyjemność pracować, usłyszałem, że ten „patchwork" to po prostu „mind mapa"!!!!

Nie ma tutaj procesu. Trudno złapać początek i koniec. Jest centrum, w którym znajduje się IDEA, POMYSŁ. Realizacja pomysłu czy też wprowadzanie idei w życie polega na rozwijaniu różnych wątków jednocześnie. Często porzucamy jeszcze niedokończony, aby rozpocząć trzy inne. Przeskakujemy z tematu na temat, ale ostatecznie powstaje sieć, która jest odzwierciedleniem realizacji POMYSŁU. Dla wielu „mind mapa" jest o wiele bardziej naturalnym wyrażeniem myśli, niż proces oparty na przyczynie i skutku.

Odrywając się od wątpliwej idei „naturalności", niewątpliwie posiadająca więcej stopni swobody „mind mapa" bliska jest sposobowi pracy „żółtych". Jak powiedziała mi jedna z osób zdecydowanie klasyfikowana jako „żółta" – tam, gdzie inni widzą chaos, ja widzę ideę.

Jedna z charakterystyk „żółtych" mówi, że nie potrafią wytrwać do końca zadania, bo lubią zmiany. Podejmują wiele (niekiedy nawet zbyt wiele) zadań naraz. Klasyczna struktura „mind mapy" pokazuje właśnie te przeskoki pomiędzy wątkami. Pozwalają one osobom „żółtym" utrzymać uwagę na głównej IDEI. Nie ma tutaj żmudnego procesu podzielonego na etapy, gdzie muszę skończyć jeden etap w 100%, aby zacząć kolejny. Można w każdej chwili, wtedy, kiedy nam to odpowiada, przerzucić się z jednego wątku na kolejny.

Wyzwanie stanowi tutaj doprowadzenie ostatecznie podstawowej idei do końca. Zwróćmy uwagę, że brak „domykania" kontraktów stanowi jeden

z podstawowych zarzutów w kierunku sprzedawców. Bez względu na metodę, to co liczy się w sprzedaży to ostateczny rezultat – mamy kontrakt czy nie mamy?

Patrząc z punktu widzenia „ostatniej mili" szczególnie sprawni są pracownicy o osobowości „czerwonej". Mocno nastawieni na rezultat. Jednak są to osoby niejednokrotnie bardzo niecierpliwe. Mocno nastawione na siebie i nie potrafiące słuchać innych (w tym klientów). Dlatego na pewno „domieszka" czerwonej osobowości jest przydatna w końcowej fazie sprzedaży. Jednak bez emocjonalnego i relacyjnego fundamentu nigdy do tego końcowego etapu nie dojdziemy.

Podobnie możemy podejść do kwestii „mind mapy". Nie jest ona oczywiście gwarantem podpisania kontraktu. Na pewno nie rozwiązuje problemu „ostatniej mili". Doprowadza ona jednak nas do tego punktu w sposób zgodny z naturą „sprzedawcy". Sądzę, że gdy jesteśmy odpowiednio blisko celu włączają się motywatory zupełnie innej natury – szansa na bonus. U dobrych sprzedawców działa to znacznie lepiej niż „domieszka" natury „czerwonej".

Pożądana osobowość

Ostatecznie skonfrontujmy powyższe z naszym podstawowym zagadnieniem – brak akceptacji rozwiązań typu SFA. Dlaczego coś co powinno pomagać – nie pomaga?

Po pierwsze, wydaje się, że pokazałem powyżej wystarczającą ilość argumentów, aby w pewien sposób utożsamić osobowość „żółtą" z ogólnie rozumianym obszarem sprzedażowym. Przy wszelkich ostrożnych założeniach i zastrzeżeniach z dużą dozą prawdopodobieństwa można przyjąć, że średnio w obszarach sprzedażowych mamy do czynienia z osobowościami „żółtymi".

Po drugie – większość systemów SFA bazuje na tzw. „procesie sprzedażowym". Samo to wyrażenie powoduje dreszcz u większości sprzedawców. „A co mam zrobić, jak klient chce kupić już na drugim etapie procesu, kiedy, ja mam standardowo przewidziane jeszcze pięć?". Systemy te, budowane przez osoby o charakterystyce „niebieskiej", przykładającej uwagę do detali, wydają się tym osobom idealne.

I tutaj pojawia się ogromny dysonans i niezrozumienie. Mamy idealny system, który kompletnie nie nadaje się do użytku. Zderza nam się idealny proces z chaosem mind mapy. Albo też próbujemy wpisać nasze wielowątkowe

myślenie w prosty schemat jednego wątku i wielu jego etapów. Szans na zrozumienie brak, zwłaszcza, jeżeli proces staje się nadrzędny. Nie możesz zacząć etapu trzeciego, jeżeli nie skończyłeś pierwszego i drugiego w 100%. A często proces w postaci narzędzia staje się nadrzędny czyli obowiązkowy. Dzieje się tak głównie dlatego, że narzędzie służy do realizacji jeszcze jednego ważnego celu – prognozowania wyniku sprzedaży. A z tego zrezygnować nam nie wolno, gdyż są to wymagania inwestorów.

Wówczas technicznie prosta obsługa systemu staje się merytorycznie niezmiernie trudna. Osoba, dla której narzędzie miało stanowić wsparcie, stara się swój wielowymiarowy świat przekształcić w jeden wymiar procesu. Jednocześnie nie chce gubić informacji o zaawansowaniu działań sprzedażowych, gdyż jest to główne kryterium oceny jej pracy przez przełożonych. I dlatego coś, co autorom systemów i niektórym przełożonym wydaje się być zadaniem na 15 minut tygodniowo, zajmuje znacznie więcej czasu i powoduje ogromną frustrację pracowników sprzedaży.

SFA a prognozy sprzedażowe

Czy jest jakieś wyjście z sytuacji? Myślę, że przede wszystkim konieczne jest zupełnie inne podejście do prognoz sprzedażowych. Stosowanie do tych celów systemów SFA buduje nie tylko frustrację w zespołach sprzedażowych, ale ostatecznie daje nam obraz bardzo zniekształcony. Tak, jak musi ulec zniekształceniu każdy obraz, który z wielu wymiarów przenosimy do jednego. Sugerowałbym aby do wyznaczania prognoz sprzedażowych zastosować nieco bardziej zaawansowane narzędzia, które pomogą nam zbudować modele prognozowania w oparciu o dane związane z zachowaniami sprzedawców (narzędzie oparte o metody behawioralne). Niniejsze opracowanie nie stawia sobie za cel przedstawienia tego konceptu w szczegółach. Chciałbym zwrócić uwagę, że obecnie do wszelkiego rodzaju prognoz stosuje się już znacznie bardziej wyrafinowane technologie, opierające się o narzędzia typu „BIG DATA", zaawansowane rozwiązania BI, wszelkiego rodzaju analityczne systemy pozwalające wskazywać trendy i korelacje. Budowanie prognoz na podstawie mocno nieobiektywnej opinii sprzedawców swoją archaicznością przypomina prognozowanie pogody na podstawie opinii starego górala. Czasem się udaje, bo góral może mieć duże doświadczenie i wiedzieć, co znaczy „łupanie w kościach", ale opieranie na tym prognoz globalnych wydaje

się nieco ryzykowne. Współcześnie dobrze zorganizowane firmy potrafią, na podstawie analizy dużej ilości danych, ze sporą dokładnością prognozować, tak wydawałoby się nieprzewidywalne zdarzenia, jak ilość klientów, którzy pojawią się konkretnego dnia w sklepie czy też ilość paczek do przewiezienia w konkretnym dniu przez firmę logistyczną.

Dane o codziennej aktywności sprzedawców, częstotliwości kontaktów z klientem, proporcji czasu spędzanego nad konkretnym kontraktem, ilości telefonów i maili, dają podstawę do zbadania odpowiednich korelacji, zarówno dla całych zespołów, jak i dla konkretnych sprzedawców. Korzystając z dostępnych narzędzi, jesteśmy w stanie zbudować model, który oceni prawdopodobieństwo zajścia konkretnego zdarzenia sprzedażowego (podpisania kontraktu) w określonym czasie. Piękno tego podejścia polega na tym, że jest to model samodoskonalący się. Wstępna parametryzacja pojawi nam się na podstawie analizy danych historycznych, a bieżące informacje będą pozwalały na dokładniejszą kalibrację i większą precyzję prognoz. Jestem przekonany, że otrzymana w ten sposób prognoza będzie znacznie dokładniejsza niż poddane wielokrotnym transformacjom dane z systemów klasy SFA.

Po drugie, chcąc wspierać siły sprzedażowe w ich pracy powinniśmy odejść od koncepcji „procesu sprzedażowego". Odrzucenie procesu jako uniwersalnego modelu może wydawać się trudne, ale tylko tak możemy zbliżyć się do rzeczywistości sprzedażowej. Stosując takie podejście oderwiemy się od nadrzędności narzędzia i przygotujemy rozwiązanie, które, będąc zgodne z osobowością sprzedawców, pozwoli im lepiej panować nad wielowątkowymi działaniami. Odchodzimy od wyobrażenia sprzedaży jako taśmy produkcyjnej. Nadal musimy wykonać szereg czynności – opisać potrzeby klienta (albo właściwie wykreować potrzeby u klienta), przygotować ofertę, wynegocjować kontrakt i wiele, wiele innych… Jednak sama kolejność tych działań i ich ustawienie na osi czasu nie musi być stałe. Zarówno nasze możliwości, jak i działania po stronie klienta podlegają wielu wpływom przychodzącym z otoczenia. Zmiana oferty produktowej u nas, zmiana w Zarządzie u klienta, nieoczekiwane pieniądze w budżecie (lub ich brak)… Wszystko to wpływa na ogólne poczucie chaosu. Ale w takim właśnie środowisku „rasowi" sprzedawcy czują się najlepiej.

Jeżeli więc mielibyśmy rozważać powstanie narzędzia wspierającego pracę sprzedawcy, to sądzę, że rozwiązanie takie powinno bazować na koncepcji „mind mapy". W swoim założeniu miałoby ono na celu przede wszystkim

ułatwiać kontrolę wielu wątków, przypominać o tych, które powoli stają się zapomniane, wskazywać na działania, których brak blokuje postęp w akcji sprzedażowej. Narzędzie takie mogłoby stosować pewne prognozy i przybliżenia, dzięki którym sprzedawca mógłby otrzymywać "podpowiedzi działań". Pojawiałyby się one w oparciu o mechanizmy behawioralne i mogłyby być bardzo spersonalizowane, gdyż ogólny model bardzo szybko dostosuje się do zachowań konkretnej osoby. Wykorzystanie takich mechanizmów z jednej strony zapewni korporacjom jednolite podejście do akcji sprzedażowej, z drugiej zaś da konkretnym sprzedawcom poczucie indywidualnego podejścia i komfort pracy w środowisku odpowiadającym jego osobowości.

Warto tu podkreślić, że użyte sformułowanie „jednolite podejście" nie odnosi się do precyzyjnie opisanego procesu, gdzie kolejne kroki przyjmują formę „check listy". Odchodzimy tutaj od czysto mechanicznego modelu. Proponujemy model oparty na prawdopodobieństwach i statystyce, który znacznie lepiej opisuje współczesny świat. Wiele lat temu przekonali się o tym fizycy – teraz czas na świat biznesu.

Nie lekceważyć technologii

Zmiany zachodzące wokół nas w ostatniej dekadzie spowodowały, że przestaliśmy być po prostu użytkownikami technologii. Technologia to już nie „zło konieczne". Technologia stała się częścią nas. Gdy zapomnimy rano telefonu komórkowego (zwanego tak już tylko przez sentyment, bo urządzenie to ma z telefonem bardzo niewiele wspólnego), to czujemy jakby część nas została w domu. Musimy jak najszybciej odzyskać tą utraconą „część ciała", aby odzyskać wewnętrzny spokój.

Te indywidualne zachowania w świecie prywatnym przenosimy do świata biznesu. Chcemy się tutaj czuć tak samo wygodnie i „u siebie". Oczekujemy, że środowisko w którym spędzamy wiele godzin, będzie zgodne z naszym ja, z naszą osobowością.

Tutaj pojawia się dla twórców nowych narzędzi szczególne wyzwanie. To już nie jest po prostu własna tapeta na pulpicie (w niektórych firmach nawet to nadal jest zabronione). To już nie jest nawet BYOD, pozwalające działać w swoim „domowym" środowisku własnego tabletu czy też smartfona. To oczekiwanie, że będę mógł realizować cele biznesowe w sposób, który dla mnie jest najbardziej odpowiedni. I jeżeli korzystam z narzędzi to oczekuję,

że one w sposób realny wspierają mnie w moich działaniach. A działań tych i sekwencji ich występowania jest tyle, ile mamy różnych typów osobowości. Jak dać ten komfort?

Myślę, że jest to możliwe dzięki wielu nowym trendom technologicznym. Dostaliśmy do ręki nowe bardzo silne technologiczne narzędzia. Naszą szansę upatruję nie w odtwarzaniu za ich pomocą starych procesów. Musimy spojrzeć na świat w sposób nowy, znacznie bardziej ludzki.

Bibliografia:

Scott D. Nelson „CRM Implementation and Economics" Gartner G00105520 Październik 2001

Ed Thompson "Use Gartner's CRM Application Functionality Starfish to Evaluate Your CRM Requirements" Gartner G00247825 Czerwiec 2013

Ed Thompson "The Eight Building Blocks of CRM" Gartner G00247824 Luty 2013

Michal Čakrt „Kto jest kim. Typy osobowości dla managerów." Onepress 28 września 2006

D.M.Buss, N.Cantor „Personality psychology: Recent trends and Emerging Directions" Springer 1989

Magda Dziewguć
Pomysłodawczyni i założycielka fundacji FSCD oraz Head of Google for Work CEE.
Wcześniej pracowała w zarządzie Exatela i kilku Radach Nadzorczych, zarządzała m.in. rynkiem biznesowym sieci komputerowych Polkomtela. Ekspert zarządzania segmentem B2B i budowania strategii rozwoju dla firm. Obecnie pracuje zarówno z bankami, wspierając ich proces transformacji cyfrowych, jak i ze startupami, pomagając im w budowie modeli biznesowych umożliwiających współpracę z dużymi instytucjami finansowymi.

Marta Guzek
Finance Industry Head w Google Polska. Wcześniej zajmowała się kompleksowo wdrażaniem innowacji technologicznych i nowych koncepcji biznesowych w bankach i firmach ubezpieczeniowych, pracując m. in. dla Mastercard, Orange i Exatela.

Michał Olczak
Założyciel i współtwórca Obserwatorium.biz – organizacji oferującej usługi doradcze z zakresu Digital Consulting & FinTech dla firm. Obecnie prowadzi również NextApps – startup, który oferuje aplikacje mobilne. Ma za sobą wieloletnie doświadczenie w prowadzeniu projektów innowacyjnych dla banku BZ WBK.

Magda Dziewguć, Google,
Marta Guzek, Google,
Michał Olczak, Obserwatorium.biz

FinTech – wróg czy przyjaciel

Rewolucja cyfrowa w świecie finansów trwa na dobre. Przez ostatnie dwa lata widzimy bardzo wyraźne zainteresowanie inwestorów nowymi modelami biznesowymi budowanymi w tej branży. Niewątpliwie trwa wielka redefinicja sposobu korzystania z usług finansowych a jej głównym katalizatorem jest smartfon. Rok 2015 można uznać za przełomowy w zakresie wykorzystania urządzeń mobilnych, ponieważ po raz pierwszy w skali globalnej liczba zapytań do wyszukiwarki Google z telefonów i tabletów przekroczyła liczbę zapytań z komputerów stacjonarnych (w Polsce wyszukiwania mobilne dla kategorii finanse kształtowały się na poziomie 25% z kilkudziesięcioprocentową dynamiką wzrostu rok do roku)[1]. Jednocześnie do grona użytkowników usług finansowych zaczynają dołączać osoby z generacji "Z" (urodzeni po roku 1995), tzw. *digital natives*, które nie znają świata bez internetu i telefonów mobilnych. To oni są najszybszymi adopterami nowych technologii, błyskawicznie przemieszczając się w obszar kolejnych innowacji (czego przykładem może być migracja z Facebooka na Instagram czy Twitter[2]).

Dwa kluczowe rynki, na których najszybciej pojawiają się i zostają przez konsumentów przyjęte usługi finansowe z nowego rodzaju interfejsem to Stany Zjednoczone i Wielka Brytania. Za dynamiczną migracją do cyfrowego świata FinTech podążają inwestorzy. Tylko w czwartym kwartale 2014 r. zainwestowano w tym segmencie ponad 3 mld dolarów w 214 projektów

1 Dane wewnętrzne Google

2 http://www.businessinsider.com/facebook-is-losing-its-grip-on-the-teen-demographic-as-visual-social-networks-gain-popularity-2015-6

inwestycyjnych[3]. Rok 2015 przyniósł dalszy wzrost inwestycji w startupy z sektora finansów, osiągając według raportu Citi GPS kwotę 19 mld dolarów, co oznacza dziesięciokrotny wzrost w ciągu ostatnich 5 lat[4].

W Wielkiej Brytanii wdrażana jest zintegrowana strategia mająca na celu przeprowadzenie tradycyjnego „City", będącego istotnym elementem gospodarki, do momentu uzyskania przez Londyn statusu nieformalnej globalnej stolicy FinTech'u. Strategia jest wspólna i jednoczy w swoich działaniach wysiłki rządowe, regulacyjne, tradycyjnych uczestników rynku oraz startupy. Nie ma jeszcze na dzień dzisiejszy rynku referencyjnego na tyle zaawansowanego, że można byłoby go uznać za modelowy przykład efektu końcowego ewolucji sektora. Nawet na bardziej zaawansowanych rynkach nadal mamy do czynienia z wieloma wyzwaniami. Główne bariery szybkich zmian tkwią w szeroko rozumianej zgodności z porządkiem administracyjno-prawnym obecnego systemu bankowego. Najważniejsze grupy przeszkód to:

- brak właściwych regulacji i konserwatywne nastawienie regulatorów do wdrażanych nowinek,
- przestarzała architektura IT utrudniająca szybkie wdrożenia nowych projektów pro-konsumenckich,
- brak właściwych kompetencji u pracowników (data science, mobile, video, customer experience design),
- brak struktury celów wspierających współpracę biznesu i technologii,
- brak świadomości kluczowych decydentów oraz ograniczona zdolność do wprowadzenia zmian w organizacjach, którymi zarządzają.

3 2016 SVB Financial Group, *2015 FinTech Report: Investment Trends in FinTech.*

4 March 2016, Citi GPS, *Digital Disruption. How FinTech is Forcing Banking to a Tipping Point.*

Awareness of start-ups by executives at banks

Entrants	I'm aware of the company and what they do.	I'm aware of them but don't know what they do.	I've never heard of them.
nutmeg	23%	35%	43%
Betterment	8%	19%	73%
Square	15%	27%	57%
venmo	6%	15%	78%
azimo	6%	26%	67%
TransferWise	15%	35%	51%
LendingClub	18%	36%	45%
Rate%Setter	17%	26%	56%
PayPal	92%	8%	0%

* 110 senior execs ranging from director to C-suite were asked about the startups they were aware of.

Źródło: *Bye Bye Banks? © July 2015 Financial Brand*

Ze względu na ograniczoną zdolność dużych organizacji finansowych do prowadzenia samodzielnie projektów FinTech'owych, jedyną skuteczną drogą wydaje się bliska współpraca z ekosystemem startupów i think tanków pracujących na krawędzi zmiany. Dlatego pozostaną one głównym inwestorem i odbiorcą kreatywnej twórczości finansowych innowatorów i od ich zdolności dystrybucyjnych zależy tempo adopcji nowych rozwiązań na rynku. Nie jest to prosta relacja, dlatego do barier musimy dopisać:

- ograniczoną zdolność banków do współpracy ze środowiskiem startupów,
- brak narzędzi i kompetencji do systemowej analizy i testowania pomysłów na swoich bazach klientów.

Rozpoczynając analizę polskiego sektora finansowego z perspektywy zaangażowania we współpracę z rozwijającą się w środowisku startupów kategorią

FinTech, bardzo trudno zdefiniować punkt wyjścia. Opracowania analizujące poziom zaawansowania rozwoju cyfrowego w Polsce wskazują bowiem sektor finansowy jako lidera na czele wszelkich branż. Zgodnie z raportem zrealizowanym przez Ośrodek Analityczny Polityka Insight *„Czas na przyspieszenie"*[5] Ubezpieczenia i Finanse to najbardziej cyfrowy spośród wszystkich sektorów polskiej gospodarki. Polska jest dużym i bardzo atrakcyjnym rynkiem dla usług finansowych ze względu na dobre parametry gospodarcze, co pozytywnie wpływa na jego konkurencyjność. Stała obecność międzynarodowych graczy połączona z dużą dynamiką rynku zaowocowała szybszym niż na Zachodzie tempem wprowadzania nowych metod płatności i innowacyjnych produktów finansowych. Do roku 2011 ogromny wpływ na ten przyspieszony rozwój miała proaktywna i liberalna polityka Komisji Nadzoru Finansowego. Nowinki bankowe wynikające z rozwoju technologicznego były przyjmowane z otwartością i akceptacją Regulatora, stąd dynamiczny rozwój np. kart zbliżeniowych i płatności mobilnych na rynku polskim. Należy podkreślić, że jest to jedyna branża, w której Polska zalicza się do pierwszej dziesiątki w rankingu zaawansowania rozwojowego krajów Unii Europejskiej.

Polscy innowatorzy, podobnie jak międzynarodowi, wybrali do stworzenia swoich startupów najbardziej dochodowy obszar, jakim jest bankowość detaliczna (globalnie w projektach adresujących klientów indywidualnych oraz SME inwestorzy ulokowali ok. 70% kapitału[6]) i są to:

- pożyczki (w tym społecznościowe),
- przelewy i transfer pieniędzy,
- płatności,
- wymiana walut,
- porównywarki produktów finansowych (optymalizujące decyzje zakupowe),
- inwestycje kapitałowe oraz informacje inwestycyjne,
- infrastruktura bankowa.

Nie wszystkie te kategorie rozwijają się w równolegle we wszystkich krajach. Otwartość lokalnego regulatora finansowego, dostępność kapitału, penetracja internetu i smartfonów – wszystkie te czynniki mają wpływ na to, które kategorie FinTech'owe rozwijają się szybciej.

5 Styczeń 2016, Piotr Arak, Andrzej Bobiński PI Research

6 March 2016, Citi GPS, *Digital Disruption. How FinTech is Forcing Banking to a Tipping Point.*

W Polsce widzimy kilka kategorii wyróżniających się:

- płatności – jesteśmy wskazywani jako kraj bardzo szybkiego rozwoju nowych metod w tym zakresie, warto wymienić choćby niektóre z polskich projektów: iZettle, eCard, Dotpay, PayU, Blik, SkyCash,
- przelewy i transfer środków: Azimo, Valuto.pl,
- waluty: Cinkciarz.pl, internetowykantor.pl,
- bankowe aplikacje mobile: INGMobile, mBank, IKO, BZ WBK24 mobile, Alior mobile, Bank Millennium, Pekao24, PeoPay, Getin Mobile, Eurobank mobile.

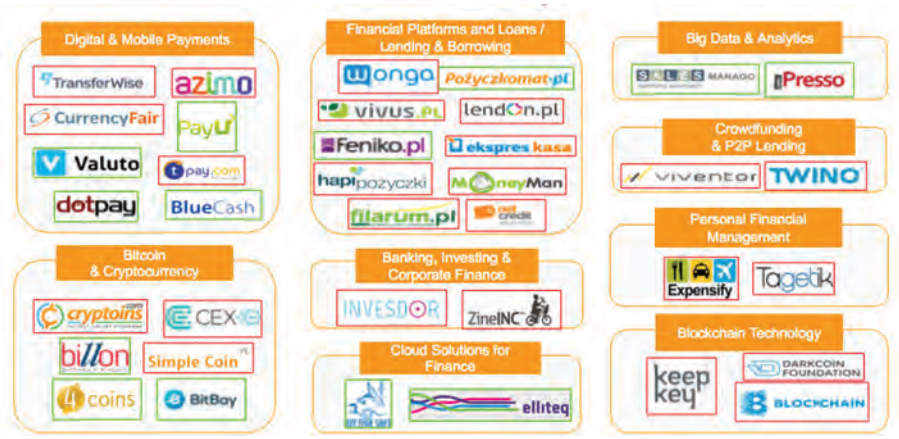
Wstępna analiza skłania nas zatem do pozytywnych wniosków. Jeśli jednak przyjrzymy się tej sytuacji zmieniając perspektywę analizy, wnioski będą już mniej optymistyczne. Czechy, Rumunia, Litwa, Łotwa i Estonia – wszystkie te kraje mogą się już pochwalić szeregiem udanych wdrożeń w zakresie modyfikacji technologicznej koncepcji działania banku, które bazują na modelu chmurowym. W Polsce pierwsze takie wdrożenie dopiero trwa. Warto tutaj zaznaczyć, że rozwiązania chmurowe stanowią podstawę funkcjonowania startupów, nie tylko wpływając na ich efektywność kosztową i pozwalając na szybkie i elastyczne skalowanie biznesu wokół najnowszych technologii, ale także kształtując specyficzną kulturę pracy.

Ekosystem finansowy – w jakich obszarach i dlaczego pojawiają się nowi gracze

Jednym ze źrodeł inspiracji do tworzenia nowych biznesów w ekosystemie cyfrowym jest analiza zapytań do wyszukiwarki, pozwalająca zauważyć trendy, ich lokalizacje oraz nasilenie. Analizując przestrzeń do rozwoju dla poszczególnych kategorii, poprzez zapytania do wyszukiwarki Google, można zaobserwować stabilny ogólny trend rosnący, zarówno jeśli chodzi o finanse ogólnie (Europa – 15%, świat – 17%, Polska – 13% wzrostu w latach 2015 vs 2014), jak i w poszczególnych podkategoriach, np. bardzo szybko rosnącym obszarze wymian walut (30% wzrostu) czy pożyczek (18%)[7]. Polski ekosystem FinTech'owy rozwija się nie tylko w efekcie powstawania lokalnych startupów, ale również dzięki zagranicznym graczom. Skalowanie globalne jest wręcz zapisane w DNA każdego nowego podmiotu (nie tylko z sektora FinTech), który zakłada osiągnięcie znaczących

7 Dane wewnętrzne Google

udziałów rynkowych w ramach gospodarki cyfrowej. Szczególnie rynki Europy Środkowo-Wschodniej, za wyjątkiem Polski, nie pozostawiają wielkiego pola do działania sprawiając, że startupy z krajów Bałtyckich czy Bałkanów od samego powstania nastawione są na ekspansję zagraniczną, w tym do Polski (przykłady firm prezentuje poniższy rysunek, przy czym spółki polskie oznaczone są zielonymi ramkami, a zagraniczne – czerwonymi).



Co charakterystyczne i powtarzające się nie tylko w sferze startupów FinTech'owych to uzyskanie przewagi konkurencyjnej na bazie jednego produktu czy usługi i koncentracja na zbudowaniu wartości wokół potrzeb i doświadczeniach klienta. Postawienie człowieka w centrum procesu jest podstawą innowacyjnych kultur korporacyjnych największych firm obecnych w cyfrowym wyścigu technologicznym, jak np. Apple, Google, Uber, Airbnb czy Facebook. Technologia i zastosowany model biznesowy stanowią wyłącznie dopełnienie czynnika nadrzędnego w budowaniu firm nowej generacji, jakim jest koncentracja na potrzebie klienta, co np. potwierdza swoimi wynikami badanie EY "FinTech adoption index". Badanie przeprowadzone na 10 tys. aktywnych cyfrowo użytkownikach usług finansowych w Australii, Kanadzie, Hongkongu, Singapurze i USA miało na celu zrozumienie przez nich stopnia adopcji rozwiązań i produktów FinTech'owych oraz poznania przewidywań dotyczących przyszłości. Respondenci EY zdecydowanie wskazali jako wiodący powód zmiany dostawcy usług finansowych łatwość założenia rachunku (43,4%), a nie cenę (tylko 15,4%), co wyraźnie wskazuje, że powody,

dla których spółki FinTech zostały utworzone są głównymi czynnikami, dla których klienci postanowili z nich korzystać[8].

Oprócz wspomnianych już najpopularniejszych obszarów działania startupów FinTechowych, jak pożyczki społecznościowe, wymiana walut, płatności czy porównywarki, w przyszłości możemy się spodziewać dalszego przejmowania rynku usług finansowych przez startupy w efekcie wdrożenia Dyrektywy PSD2, która ułatwi podmiotom pozabankowym dostęp do rachunków bankowych oraz płatności. Wejście w świat otwartego API będzie stanowiło dla banków zagrożenie nie tylko w kontekście konkurencji pozabankowej i FinTech'owej, ale również obecnych rywali. Jednocześnie dla tych graczy, którzy potraktują wdrożenie Dyrektywy nie tylko z perspektywy compliance, ale także okazji biznesowej, umożliwi zaoferowanie targetowanym klientom swoich konkurentów wysoko marżowych oraz innowacyjnych produktów.

Innowacyjne rozwiązania są już częściowo obecne w innych obszarach usług finansowych, jednak wraz z rozwojem ekosystemu cyfrowego i technologii ich rozwój powinien znacząco przyspieszyć, np. w takich obszarach jak:

- świat produktów inwestycyjnych (zwłaszcza w oparciu o agregację i sztuczną inteligencję, która pozwoli na szerszy dostęp do pomocy wysokiej jakości, ułatwiając klientowi proces podejmowania decyzji, np. doradztwo z użyciem rozszerzonej rzeczywistości czy robotów),
- produkty finansowe dla dużych firm i korporacji, które wraz z rozwojem również dołączą do ekosystemu cyfrowego – obecnie poszukują one rozwiązań wspierających automatyzację i integrację cyfrową oraz zapewniających bezpieczeństwo świadczonych usług,
- rozwiązania oparte o technologię blockchain i distributed ledger – tu jako przykład projektów, które toczą się z udziałem startupów oraz banków można wyróżnić projekt Enigma[9] lub Ripple[10] we współpracy z Santander; te rozwiązania mają szansę wykorzystać sukces BitCoinów do budowania nowych biznesów opartych o rozproszoną własność i technologię blockchain, ponadto dzięki oderwaniu od modelu centralnego pozwolą na łatwiejszy start nowych biznesów.

8 http://www.ey.com/GL/en/Industries/Financial-Services/ey-fintech-adoption-index

9 http://enigma.media.mit.edu/

10 http://santanderinnoventures.com/founder-interview-chris-larsen-ceo-ripple-continued/

Perspektywa nowego gracza – do czego (jeśli w ogóle) startup finansowy potrzebuje tradycyjnego modelu bankowości i dlaczego banki potrzebują startupów

Banki stają się partnerami startupów, inwestując w rozwój spółek FinTech'owych, wymieńmy choćby CitiGroup Ventures, J.P. Morgan, Goldman Sachs czy Barclay's. Dodatkowe źródło wsparcia dla rozwoju nowych firm stanowią inkubatory czy akceleratory mające swe źródło np. w konsultingu, jak FinTech Innovation Lab – program mentoringowy Accenture realizowany w Nowym Jorku, Londynie i Hongkongu, mający na celu połączenie startupów z bankami, czy Fundusz Santander InnoVentures, mający swoje korzenie w banku i zlokalizowany w Londynie.

Doskonały przykład budowania relacji pomiędzy bankami (oraz innymi przedstawicielami tradycyjnego biznesu) a ekosystemem startupowym mamy też w Polsce – swoje stałe grono uczestników mają już spotkania organizowane przez firme D-Raft[11], zwłaszcza Demo Days, na których startupy mają okazje zaprezentować swoje rozwiązania oraz porozmawiać z potencjalnymi partnerami czy inwestorami.

W związku ze wzrostem znaczenia innowacji i technologii dla klientów usług finansowych, nowym graczom jest coraz łatwiej wejść na rynek i zdobyć zainteresowanie inwestorów – w tym tradycyjnych banków – czego przykładem może być Atom Bank, stworzony z myślą o ludziach w wieku 18–34 lat, w całości oparty o kanał bankowości mobilnej, który jeszcze przed uruchomieniem zyskał wsparcie BBVA. Równie ciekawym przypadkiem współpracy z tradycyjnym graczem może być tez Loot, który bazując na licencji bankowej stworzył w ciągu 100 dni markę dedykowaną studentom, koncentrując się wyłącznie na potrzebach i doświadczeniu młodych ludzi związanych z usługami bankowymi.

Schodząc do poziomu współpracy produktowej startupy finansowe mogą się integrować z istniejącymi usługami bankowymi w celu budowy nowych rozwiązań. Przykładowo, w przypadku pożyczek społecznościowych, banki mogą współpracować ze startupami przekazując im klientów o nieakceptowalnym dla nich poziomie ryzyka co miało już miejsce w przypadku współpracy ING i Seedrs, Santander i Funding Circle czy RBS i Funding Circle. W Polsce rynek pożyczek społecznościowych rozwija się od 2008 r. zapoczątkowany przez platformy Kokos.pl czy Finansowo.pl. Klienci jednego

11 http://d-raft.com/

z większych serwisów, na którym możliwe jest zawieranie tego rodzaju transakcji pożyczyli już ponad 100 mln zł, przy czym dla porównania rynek pożyczek bankowych wg prognoz wynosi ok. 73 mld zł a rynek pozabankowych firm pożyczkowych – ok. 5,1 mld zł (wg danych Związku Firm Pożyczkowych[12]). Z uwagi na wysoki koszt pozyskania pieniądza oraz poziom ryzyka klientów (dochodzący do 8% wartości udzielanych pożyczek) rynek ten rozwija się znacząco wolniej niż jego możliwości, co widać po porównaniu go z brytyjskim czy amerykańskim, gdzie jest większa otwartość na rynek pożyczek społecznościowych, a, co za tym idzie, łatwiejsza konkurencja z bankami i tradycyjnymi firmami z sektora pożyczkowego.

Innym scenariuszem jest udział banku jako kanału dostępu dla pożyczkodawców, tak jak w przypadku kooperacji Fidor Bank i Smava.

Innowacje w banku – kogo naśladować i od kogo się uczyć: challenger bank czy startup

Dynamiczny rozwój technologii wpływa na zmieniające się oczekiwania klientów, co w połączeniu z rosnącym zainteresowaniem pokoleń wchodzących na rynek pracy i zainteresowanych tworzeniem własnych firm powoduje, że usługi finansowe będą ewoluować w kierunku ich prostoty i wygody. Wiele dzisiejszych rozwiązań powstało w wyniku niezadowolenia z istniejących produktów lub procesów finansowych bądź w odpowiedzi na braki w ekosystemie bankowym, jak np. Azimo, Internetowykantor.pl czy Finansowo.pl.

W ramach reakcji banki przyjmują jedną z czterech strategii:

- negacji zagrożenia ze strony startupów,
- przejmowania lub inwestycji w startupy[13],
- ochrony własnych zasobów przez blokowanie dostępu do kont użytkowników oraz przez wypracowanie rozwiązań biznesowych lub prawnych, które chronią istniejące status quo,
- pójścia ścieżką rozwoju i utrzymania klientów poprzez zaoferowanie innowacyjnych rozwiązań i produktów (challenger bank) często w kooperacji ze startupami lub firmami technologicznymi.

12 Związek Firm Pożyczkowych, kwartalnik *ProMeritum*, 04/2016.

13 http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf

Która z tych strategii okaże się najkorzystniejsza z punktu widzenia banku, nie jest w tym momencie oczywiste, jednak kolejne badania i rosnące znaczenie innowacji wskazuje, że strategia oparta o otwartość na współpracę i innowację w kooperacji z firmami z sektora FinTech może okazać się kluczowa dla utrzymania relacji z klientem. Ciekawym przykładem w budowaniu innowacyjnych i masowych usług finansowych dla klientów może być kooperacja Alior Banku oraz mBanku z firmą PayU we wdrożeniu usługi zakupów z kredytem ratalnym w serwisie Allegro.

Doskonałymi przykładami banków, który podjęły wyzwanie w wyścigu technologicznymi ze startupami, są:

- mBank z nową odsłoną Personal Finance Management, wyszukiwarką, integracją z CRM, platformą Foreign Exchange oraz usługami dla firm,
- Idea Bank z platformą chmurową, mobilnymi wpłatomatami oraz Idea Hubami.

Inną drogą jest stworzenie nowego banku od podstaw w oparciu o najnowsze rozwiązania technologiczne jak bankowość mobilna i budowanie relacji z klientem poprzez systemy lojalnościowe lub oferowanie konkurencyjnych cenowo usług finansowych. Za dobry przykład może posłużyć Atom Bank (Wielka Brytania) czy Number26 (Niemcy) w Europie oraz Orange Finanse, a także Alior Sync (obecnie T-Mobile Usługi Bankowe) w Polsce.

Z uwagi na wykładniczy przyrost innowacji technologicznych trudno przewidzieć, która z niżej wymienionych będzie miała największy wpływ na transformację bankowości. Warto jednak wskazać kilka wyraźnych trendów, które mogą odegrać kluczową rolę w sektorze FinTech:

- prostota usług z wykorzystaniem aplikacji mobilnych,
- tożsamość cyfrowa oraz usługi zaufane,
- otwarte API (rola Dyrektywa PSD2),
- biometria w ułatwieniu dostępu do rachunku,
- big data i analiza predyktywna/personalizacja,
- cyberbezpieczeństwo usług finansowych,
- internet rzeczy (wartości),
- wirtualna rzeczywistość,
- roboty doradzające klientom,
- blockchain do budowy nowego ekosystemu FinTech (zdecentralizowanego).

Z uwagi na różnice w podejściu do kwestii technologicznych, regulacyjnych i tworzenia biznesu optymalny model współpracy między bankami a firmami z sektora FinTech powinien opierać się na kooperacji i wspólnym budowaniu ram współpracy. Zdecydowanie warto podkreślić pozytywny model wspólnego udziału banków oraz firm z sektora FinTech w programach akceleracyjnych, których celem jest wsparcie innowacyjności i budowanie kolejnych startupów, które zredefiniują usługi finansowe i będą miały duży wpływ na transformację cyfrową banków.

Maciej Łuczak

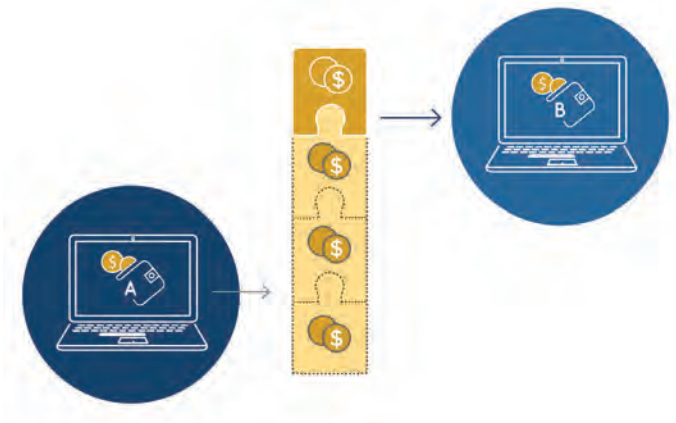
Członek zarządu Billon, firmy, która dostarcza rozwiązanie blockchain pieniądza elektronicznego dla banków-wydawców, agentów rozliczeniowych, sprzedawców oraz konsumentów.

W firmie Billon odpowiada za współpracę z klientami. Rozpoczął karierę pracując dla amerykańskich banków inwestycyjnych, Goldman Sachs w Nowym Jorku oraz Citibank w Londynie, gdzie zajmował się sektorem TMT (Telecom, Media, Technology). Następnie doradzał bankom oraz instytucjom finansowym w Europie i na Bliskim Wschodzie, będąc konsultantem McKinsey. Następnie przez dwa lata odpowiadał za strategię amerykańskiej grupy medialnej Viacom (do której należy m.in. MTV, Comedy Central, Nickodeleon, Viva). Od 2010 r. związany z rynkiem usług płatniczych, najpierw w ramach MasterCard, gdzie prowadził projekty dla europejskich banków wydawców oraz agentów rozliczeniowych, następnie współzałożył Payleven, pierwszego europejskiego dostawcę mobilnych terminali płatniczych, który szybko zdobył znaczący udział na rynkach płatności mobilnych Brazylii, Wielkiej Brytanii czy Niemczech.

Jest absolwentem SGH, uniwersytetu w St. Gallen (Szwajcaria), studiował także w MGIMO (Rosja) oraz na UBA (Argentyna). Zna cztery języki. Chciałby, aby jego SAAB stał się zalążkiem kolekcji young-timerów.

Maciej Łuczak, Billon

Blockchain



Blockchain może zmienić bankowość detaliczną, tak jak e-mail zmienił komunikację między ludźmi. E-mail zmienił (lub wyeliminował) więcej niż tylko wysyłanie listów pocztą tradycyjną – przekształcił odległe od siebie rynki i zachowania – rynek reklamy, wystawiania faktur, kontaktu między rodzinami, sposób pracy w firmach oraz dochodzenia do porozumień biznesowych czy składania ofert. Ograniczył również potrzebę niektórych podróży służbowych, stał się podstawą do rejestracji w usługach cyfrowych na stronach internetowych, pozwala odnajdywać znajomych na Facebooku czy Linkedinie. Poczta elektroniczna doprowadziła do ogromnych zmian, ponadto dzięki niej wiele osób nauczyło się korzystać z komputerów. Podobnie jak w przypadku gry Saper w MS Windows, która przez zabawę uczyła używania myszki oraz prawego i lewego przycisku myszki.

Dziś już wiemy, że blockchain zmieni to, jak będziemy realizować transakcje. Blockchain pozwala jednoznacznie określić, zrealizować, przeprowadzić, rozliczyć i zapisać dowolną transakcję. Prawie wszystkie światowe banki korporacyjne podejmują pierwsze próby w usługach korporacyjnych – np. ewidencjonowanie szybko zmieniających się udziałów w akcjach giełdowych firm[1]. Już dziś widać tę zmianę w bankowości detalicznej, bankowości transakcyjnej – blockchain umożliwia pozyskiwanie nowych klientów dla banków i generuje z nich przychody bez ponoszenia kosztów obsługi i kosztów operacyjnych związanych z nimi, czyli pozwala skoncentrować się na akwizycji i sprzedaży (również x-sell) usług. Pierwsze wdrożenia nastąpiły właśnie w Polsce, ponieważ nasz kraj należy do światowych liderów zarówno w obszarze bankowości detalicznej, jak i myśli technologicznej.

Warto przyjrzeć się głębiej technologii, która w raporcie Światowego Forum Ekonomicznego z czerwca 2015 r. została opisana jako zdecentralizowany system, który „spowoduje wycięcie pośredników w praktycznie każdym procesie usług finansowych”[2].

Bank to usługa technologiczna do zarządzania pieniędzmi

Obecnie bank to nie jest już tylko instytucja zarządzająca ryzykiem finansowym. To przede wszystkim instytucja technologiczna zarządzająca produktem, który nazywa się ryzyko finansowe. Bez zaawansowanych rozwiązań technologicznych żaden bank nie jest w stanie istnieć. Dlatego tak wiele uwagi i budżetów bankowych jest poświęcanych na rozwiązania technologiczne i wdrożenia nowoczesnych platform. Jednak, mimo że banki starają się być konserwatywne i chciałyby wdrażać wszelkie nowości technologiczne w ostatniej kolejności, to nie mogą sobie na to pozwolić. Konkurencja i konsumenci już teraz korzystają z tych technologii. Stanie z boku i czekanie nie jest opcją, która pozwoli bankom na przetrwanie.

Potrzeba postępu technologicznego ma trzy główne powody.

Po pierwsze, jest wynikiem zmian zachowań klientów, którzy np. przestali odwiedzać placówki bankowe na rzecz samoobsługi przez Internet[3].

---

1 NBER Report: Blockchain Could Shift Balance of Corporate Power, New York University (NYU), professor David Yermack, grudzień 2015

2 World Economic Forum, The Future of Financial Services, June 2015

3 Badanie OMNIBUS TNS OBOP, listopad 2015

Po drugie, presja otoczenia radykalnie wzrasta. Firmy, takie jak Facebook czy dostawcy poczty e-mail, chcą mieć każdego użytkownika Internetu jako swojego klienta, więc eliminują wszelkie przeszkody stojące przed nim. Klientem firm internetowych, np. Facebooka, może bowiem zostać każdy. W modelu firm internetowych nikt nie wymaga od nas skomplikowanych czynności, by z tych usług skorzystać. Nikt podczas pierwszej wizyty na wp.pl nie podpisuje umowy, a firma wp.pl nie prosi o dane z dowodu osobistego. I choć różnice wynikają m.in. z regulacji prawnych, to klienci nie interesują się tym – chcą korzystać z pieniędzy (a nie banku) tak samo wygodnie, jak z innych usług cyfrowych. Można byłoby zignorować to porównanie, gdyby nie fakt, że Facebook i Google – obecnie dwie najpotężniejsze firmy konsumencie w Internecie – aktywnie wkraczają w obszar płatności i usług bankowych. Google, posiadający relację z 99% polskich internautów[4], rozwija usługę Google Wallet, a Facebook, obsługujący ok. 13 mln polskich użytkowników (więcej niż wszystkich klientów bankowych z internetowym dostępem do ROR'a) uzyskał licencję bankową na całą Europę[5].

Po trzecie, co najważniejsze – obecne produkty bankowe na bazie dotychczasowej technologii nie są w stanie tak szeroko dotrzeć do klientów jak inne usługi cyfrowe. Dopiero zmiana technologiczna pozwoli bankom dotrzeć do dwóch grup klientów:

- do nowych (nieubankowionych),
- do już istniejących w sytuacjach, gdzie istniejąca usługa bankowa jest niedostosowana do ich potrzeb. Dla zobrazowania – dziś nie da się zrobić pełnego przelewu bankowego wyłącznie na podstawie informacji pozostawionych na Facebookowej ścianie znajomego o treści: „Janku, tu masz 50 PLN". Bez robienia czegokolwiek więcej.

Technologie płatnicze nie nadążają za zmianami. Banki nie są w stanie samodzielnie obsłużyć płatności w sklepach i Internecie, zmuszone są korzystać przy tym z usług firm pośredniczących, np. systemów płatniczych izb rozliczeniowych. Przelewy międzynarodowe wciąż kojarzą się z długim czasem oczekiwania i wysokimi prowizjami. Nawet w kraju przelew z konta w jednym banku na konto w innym wiąże się z długim czasem oczekiwania.

4 Badania Gemius, styczeń 2016 r.

5 Is Facebook Angling to Take on Banking?, Kevin Tynan, czerwiec 2015, http://www.americanbanker.com/bankthink/three-ways-facebook-may-break-into-banking-1074647-1.html

Nie można jednak pominąć faktu, że wiele krajów jest całkowicie wyłączona z systemu finansowego. W związku z tym można zadać sobie pytanie, dlaczego w czasach, kiedy wymiana informacji przebiega natychmiastowo, usługi finansowe wciąż są oporne i przestarzałe?

Internet w sposobie działania opiera się na założeniach polegających na otwartej nauce (open science), czyli dzieleniu się informacjami, byciu otwartym na nowe informacje i przekazywaniem ich za darmo.

W 1995 r. ekonomista James Orlin Grabe przewidywał, że kryptografia będzie reprezentować przyszłość pieniądza, bankowości i finansów. Podobnie wypowiadał się w 1999 r. noblista Milton Friedman: *„Jedyna rzecz, której brakuje, ale niedługo zostanie wynaleziona, to niezawodna e-gotówka"*. Cyfrowy pieniądz, zdaniem Friedmana, miałby być podobny do fizycznej gotówki i pozwolić na przekazanie jej dowolnej osobie na świecie bez żadnych pośredników i bez konieczności znania tożsamości drugiej osoby. *„Taka rzecz powstanie w Internecie i uprości korzystanie z niego"* – dodał.

Kto komu ufa?

Dlaczego nie da się przekazać 50 zł na Facebooku za pomocą jednego zdania? Bo kto komu ma zaufać i jak tę wolę („Janku, tu masz") zamienić w realizację bardzo skomplikowanej transakcji finansowej („masz 50 zł"). W technologii blockchain jest to możliwe dzięki integralnemu połączeniu zaufania do danych z samymi danymi. Blockchain pozwala natychmiast rozpoznać wolę („przekazuję Jankowi") i wartość („50 zł") tej transakcji, umożliwi pobranie od autora 50 zł i natychmiastowe przekazanie Jankowi bez udziału pośredników, czyli zaufanej trzeciej strony. Jeśli Jan (lub jego bank, albo jego dostawca e-maila) korzysta z blockchaina, to Jan otrzyma 50 zł. Ani autor, ani Jan nie będą musieli nic zrobić, aby ta transakcja doszła do skutku. Nie będą musieli logować się do bankowości online, podawać wzajemnie numerów telefonów, kont bankowych albo adresów do przekazów pocztowych. Dzięki wyeliminowaniu zaufanej trzeciej strony możliwe jest radykalne uproszczenie. Jan po prostu otrzyma 50 zł od autora. Jan będzie miał 50 zł więcej, a autor 50 zł mniej.

Jednak na chwilę pozostawmy ten trudny przykład i przeanalizujmy prostszy, z codziennego życia.

Większość naszej („konsumenta") relacji z bankiem opiera się nie na zaufaniu banku do nas, ale odwrotnie: na naszym zaufaniu do banku. Podając

numer naszego konta bankowego do pracodawcy ufamy, że bank pracodawcy wyśle pieniądze do naszego banku. To zaufanie bierze się z tradycji (bank, jako instytucja zaufania), reguł prawnych (prawo bankowe) i doświadczenia (pieniądze zazwyczaj docierają). Dopiero, gdy chcemy pożyczyć pieniądze od banku, to wtedy bank musi zaufać nam. A tak naprawdę dopiero wtedy bank musi potwierdzić, kim jesteśmy i ocenić naszą zdolność kredytową, czyli możliwość spłaty pożyczki. To rozróżnienie przebiegu schematów zaufania jest jednym z fundamentów uzasadnienia biznesowego i technologicznego dla potrzeby wykorzystania platformy blockchain.

W technologii blockchain zaufanie nie jest oparte o kolejne potwierdzenie przez tzw. niezależnego arbitra faktów (z ang. *3rd party authorisation*), ale o zaufanie wynikające bezpośrednio z przedstawianych informacji. W blockchain wola: „chcę pożyczkę na 1000 zł" jest tożsama z przekazaniem bankowi prawdziwej i gwarantowanej przeze mnie informacji: kim jestem (z wielokrotnym potwierdzeniem mojej tożsamości przez wielu różnych partnerów) oraz ile pieniędzy chcę (1000 zł). Dzisiejsze pożyczki czy w ogóle interakcje z bankiem to pasmo bezustannych potwierdzeń, że ja to ja (np. logując się do banku trzeba coraz częściej podać zapamiętane hasło i przepisać hasło z SMS), a zlecając transakcję trzeba wielokrotnie ją potwierdzać (zapamiętane hasło i znów przepisywanie hasła z SMS lub e-maila). Dziś w relacji z bankiem, instytucją zaufania, nikt nikomu nie ufa i każdy non-stop weryfikuje drugą stronę („czy na pewno jest to strona mojego banku, a może ktoś się pod nią podszył?"[6]).

Z czego się bierze dziś zaufanie i ile ono kosztuje?

Dlaczego ufamy bankowi – czyli de facto technologii bankowej?
Bank to nic innego jak książka z ciągłym zapisywaniem kto, komu i ile jest winien oraz kto ile ma pieniędzy. Dziś ta książka (księga główna banku) jest przechowywana cyfrowo na serwerach bankowych.

Dostęp do tych serwerów opiera się o kombinację: login + hasło. Czyli każdy, kto ją zna (lub ją złamie) może przeczytać i zmienić zawarte w niej informacje. Znakomita większość przestępstw elektronicznych opiera się właśnie na zmianie takich zapisów w wyniku wykradzenia haseł i loginów z centralnego serwera w banku.

---

6 Ataki wyłudzające dane klientów to codzienność: http://www.bankier.pl/wiadomosc/Atak-phishingowy-na-klientow-mBanku-7242596.html, marzec 2015

Maksymalne możliwe zabezpieczenie tychże serwerów jest priorytetem operacyjnym banku. Niestety, wiąże się to z ogromnymi kosztami oraz komplikuje procesy wewnętrzne[7]. Komplikuje także procesy zewnętrzne i usługi dla klientów, przez co bank nie może być obecny tam, gdzie tak naprawdę są oni obecni, np. nie ma możliwości wysłania pieniędzy wiadomością na Facebooku. Tym samym bank nie może zarabiać na obsłudze klientów, skoro nie potrafi i nie może ich obsługiwać.

Ten zamknięty układ tworzy tzw. błędne koło technologiczne[8]: bank wydaje ogromne pieniądze na ochronę pieniędzy klientów tworząc bezpieczne systemy, ale są one tak bardzo bezpieczne, że aż nieużywalne, więc bank nie jest w stanie na nich zarabiać (bo nikt ich nie chce używać), z racji czego musi pobierać od klientów wysokie opłaty za inne usługi (np. drogie kredyty), aby utrzymywać własne drogie systemy bezpieczeństwa.

Obecna centralna infrastruktura bankowa (czyli przetwarzanie wszelkich danych w drogich i nieoptymalnych serwerach) jest całkowicie nieefektywna – regularnie ogranicza dostęp do usług, prawie całkowicie eliminuje komfort używania i nie pozwala na wprowadzanie usług tam, gdzie klienci współcześnie spędzają czas, choćby w serwisach internetowych.

Dodatkowo to niefunkcjonalne zaufanie jest bardzo drogie. W opinii branżowych ekspertów koszt utrzymywania (bez używania) jednego rachunku ROR (nie licząc generowanych transakcji) to ok. 50 euro rocznie. Dostawcy technologii bankowych, tzw. ksiąg głównych banków, rozpoczynają cenniki od ok. 40–50 euro za jednego klienta (konsumenta).

Jeśli dodamy do tego koszty obsługi klientów, którzy aktywnie korzystają z ROR, całkowite koszty obsługi ROR'a są dużo wyższe. A duża część działań klientów wcale nie przynosi przychodów, np. każde logowanie się klienta do rachunku, otrzymanie i wysłanie przez niego przelewu, przeniesienie środków pomiędzy rachunkami, przygotowanie zestawienia miesięcznego, wyszukiwanie historycznej transakcji, przygotowanie zlecenia stałego, etc.

---

7 Banki przed skokiem w technologie i w koszty, Jacek Ramatowski, NBP, http://www.obserwatorfinansowy.pl/tematyka/bankowosc/banki-przed-skokiem-w-technologie-i-w-koszty/

8 Handbook of Safeguarding Global Financial Stability: Political, Social, Cultural, and Economic Theories and Models, Gerard Capio, Williams College, Elsevier, 2012

Dlaczego rozwiązaniem problemów bankowości detalicznej jest blockchain?

Blockchain to kolejny etap rozwoju przetwarzania danych (baz danych). To sposób na zamianę kilku słów z Facebookowej ściany na w pełni zautomatyzowany proces bezpiecznego przekazania pieniędzy od nadawcy do odbiorcy bez udziału pośredników (i generowanych przez nich kosztów), ale z pełną bankową gwarancją realizacji takiej transakcji.

Dotychczasowe systemy (bazy danych) nie pozwolą na zrealizowanie tego typu transakcji, ponieważ są:

- przetrzymywane centralnie – czyli wszelkie informacje znajdują się zawsze w centralnej bazie, co znaczy, że nigdy nie znajdują się poza nią, a tym samym centralna baza danych nie potrafi w sposób automatyczny (i autonomiczny) korzystać z obcych zasobów,
- administrator bazy danych zna login i hasło każdego użytkownika bazy danych – czyli bankowa baza danych wymaga, aby użytkownik zalogował się do banku (a nie Facebooka) w celu realizacji zlecenia; prawdziwe zagrożenie centralnego rejestru haseł i loginów leży w ryzyku ataku hackerskiego – wystarczy zaatakować jeden słaby punkt całej bazy, aby otrzymać dostęp do wszystkich haseł i loginów zebranych w bazie[9],
- awaria centralnej bazy danych blokuje wszystkim użytkownikom dostęp do korzystania z bazy – czyli gdy serwer centralnej bazy danych nie działa, żaden użytkownik nie ma dostępu; problem ogólnie podsumował już w 2010 r. pan Michał Mazur, dyrektor w firmie Sygnity: „Złożoność i stopień komplikacji technicznej współczesnych systemów bankowości elektronicznej powoduje, iż dosyć często wyjaśnienie przyczyn w sposób prosty jest niemożliwe dla ludzi niebędących fachowcami. Z tego powodu banki najczęściej bardzo ogólnie mówią o przyczynach awarii".

Rozwiązaniem powyższych problemów oraz wynikających z nich konsekwencji są platformy blockchain – wielowymiarowe rozwiązania przede wszystkim łączące bazy danych oraz sposoby zabezpieczenia dostępu do nich. W przeciwieństwie do obecnie stosowanych platform technologicznych mają inną strukturę (architekturę), inne rozwiązania bezpieczeństwa oraz wykorzystują inny typ zasobów (chmurę zamiast serwerów).

9 MoneyGram Fined $100 Million for Wire Fraud, Brian Krebs, http://krebsonsecurity.com/2012/11/moneygram-fined-100-million-for-wire-fraud/

Po pierwsze, w blockchainie dane nie są przetrzymywane centralnie, ale mogą być w pełni rozproszone. Tym samym nie znajdują się one w jednym miejscu, a w wielu. Ten schemat jest zbieżny z chmurą obliczeniową, np. Microsoft Azure.

Po drugie, nie ma kogoś takiego jak administrator, bo ewentualny zarządzający danymi nie zna haseł ani loginów innych użytkowników. Nie zna haseł, ponieważ nie są one przetrzymywane w centralnym rejestrze i zna je tylko właściciel hasła. Dzięki temu nie ma obawy, że te dane (hasła) zostaną skradzione i wykorzystane do przestępstwa. Hasła i loginy, podobnie jak sama baza danych są rozproszone i mogą być np. przetrzymywane w chmurze. Brak centralnie przetrzymywanych haseł ma kluczowe znaczenie z punktu widzenia kosztów bankowych – brak potrzeby ochrony wrażliwych danych (haseł) eliminuje konieczność budowania, utrzymywania i zarządzania drogimi systemami ochrony teleinformatycznej. Eliminuje też coś bardziej prozaicznego, a znacznie częstszego – błędy ludzkie i wyłudzanie danych[10].

Po trzecie, ponieważ nie ma centralnego punktu (z ang. *central point of failure*), nie występuje ryzyko „odcięcia" innych użytkowników od dostępu do bazy danych w wyniku awarii „centrali". To ryzyko nie występuje z racji tego, że taka centrala nie istnieje. Dzięki temu można dostarczać 100% dostępne systemy zbudowane na blockchainie, ponieważ interakcje pomiędzy uczestnikami mogą zachodzić bez udziału centralnego punktu czyli bez centralnej autoryzacji (z ang. *3rd party authorisation*).

We wrześniu 2015 r. Światowe Forum Ekonomiczne opublikowało raport „Deep Shift – Technology Tipping Points and Societal Impact". Raport zakłada, że do 2025 r. 10% światowego PKB ma być powiązane z technologią blockchain. W efekcie należy spodziewać się:

- zwiększenia integracji finansowej na rynkach rozwijających się i wschodzących w wyniku korzystania z usług finansowych opartych o blockchain,
- eksplozji aktywów zbywalnych w momencie, kiedy wszystkie rodzaje wartości wymiennych będą mogły być przechowywane na blockchainie,
- lepszych rejestrów własności na rynkach wschodzących oraz możliwości przekształcenia wszystkiego w zbywalne aktywa,
- kontraktów i usług prawnych coraz bardziej przywiązanych do kodu związanego z blockchainem, które miałyby być użyte, jako nierozerwalne escrow albo programowo zaprojektowane inteligentne umowy,

10 Phishing danych

- zwiększenia przejrzystości w momencie, kiedy blockchain będzie globalną księgą przechowującą wszystkie transakcje.

Zdaniem ekonomistów Forum technologia blockchain znosi konieczność korzystania z trzeciej strony w zapewnieniu bezpieczeństwa w finansach, kontraktach i głosowaniach.

Komisarz US Securities and Exchange Commission, Kara Stein, uważa, że można sobie wyobrazić świat, w którym pożyczki papierów wartościowych, transakcje repo i finansowanie depozytu są do prześledzenia poprzez transparentny łańcuch bloków, co może zrewolucjonizować podejście środowiska regulacyjnego do monitorowania ryzyka systemowego w tych dziedzinach.

Dlaczego dla wielu światowych banków brak centralnej bazy danych, brak ryzyka utraty haseł i brak centralnej autoryzacji jest tak wielką nadzieją na kolejny etap rozwoju bankowości

Najprościej przytoczyć przykłady działań dużych instytucji, w szczególności banków korporacyjnych.

- Konsorcjum ok. 40 banków korporacyjnych, nazwane R3CEV, eksperymentuje łącząc kilka pozornie rozdzielnych obszarów. Łączy blockchain (czyli firmy zajmujące się tą technologią), bankowość korporacyjną (np. obszar obligacji, akredytyw, wielkokwotowych transgranicznych przelewów zabezpieczonych depozytami i rachunkami escrow) z wydzielonymi zespołami odpowiedzialnymi za badanie innowacji w bankach (z ang. *fintech labs*).
- Citibank zorganizował poszukiwania rozwiązania blockchain dla płatności peer-to-peer, wybierając polską firmę Billon jako najlepsze globalne rozwiązanie[11].
- Goldman Sachs (również uczestnik R3CEV) w raporcie z grudnia 2015[12] powiedział: „technologia blockchain zmienia wszystko, co wiemy o bankowości". Bank dodał również, że przeznaczy kilka miliardów dolarów na rozwój biznesowych zastosowań tej technologii.

---

11 Citi Announces Top Innovations from Citi Mobile Challenge in Jerusalem, London, Nairobi and Warsaw, http://www.citigroup.com/citi/news/2015/150528a.html

12 What if I Told You … the Blockchain Could Disrupt … Everything, Goldman Sachs, grudzień 2015, http://www.goldmansachs.com/our-thinking/pages/macroeconomic-insights-folder/what-if-i-told-you/report.pdf

- JP Morgan, Daniel Pinto, szef bankowości korporacyjnej i inwestycyjnej, w corocznym liście do pracowników przekazał, że bank powołał zespoły R&D i w efekcie wdrożeń technologii blockchain. Dodał, że coroczny budżet 9 mld dolarów przeznaczany na wewnętrzne rozwiązania technologiczne jest wystarczającym powodem dla znaczących inwestycji.
- Barclays w maju 2015 r.[13] powiedział, że technologia blockchain jest lepsza do zawierania transakcji niż obecnie stosowane przez bank rozwiązania. W pierwszej fazie bank skupił się na rozwiązaniu problemu bancassurance, w szczególności na ubezpieczeniach samochodów, aby wystawca polisy mógł śledzić cykl życia samochodu i odnotowywać ewentualne wypłaty odszkodowań w blockchainie, który krążyłby wraz z samochodem po rynku wtórnym.
- UBS powołał zespół Crypto 2.0, który ma zajmować się problemem „smart kontraktów", czyli zastosowanie blockchain do wydania obligacji, wyliczenia stopy procentowej, wypłaty kuponu oraz procesu wykupu obligacji po upływie terminu (z ang. *bond maturity process*).

Dzięki blockchain, banki mogą dostarczyć kilka lub kilkanaście najważniejszych cech współczesnych usług bankowych

- Bezpieczeństwo – fakt, że blockchain jest rozproszoną bazą danych powoduje, że atak hackerski jest praktycznie niemożliwy, przez co redukuje wymagania wobec utrzymania serwerów i poprawia bezpieczeństwo banków.
- Przejrzystość – dane odbiorcy i nadawcy płatności w sposób zakodowany są zapisane w każdym blockchainie i dane te są możliwe do wglądu. W efekcie, blockchain zawiera informacje o kanałach przepływu pieniędzy w systemie finansowym oraz o rynkach, na których jest używany.
- Prywatność – dane osobowe nie muszą być wymieniane pomiędzy uczestnikami transakcji ograniczając liczbę danych, jakie muszą być przetwarzane i jakie mogą zostać przechwycone np. w transakcji transgranicznej. Przypisanie danych osobowych do danych użytkownika może następować np. jedynie w banku. Dodatkowo pozwala to na oszczędność czasu i pieniędzy przy realizacji każdej transakcji.
- Ryzyko – ponieważ nie ma jednego podmiotu sprawującego kontrolę, nie istnieje ryzyko utraty kontroli oraz że ekosystem może działać bez przerw.

13 Blockchain: understanding the potential, https://www.barclayscorporate.com/content/dam/corppublic/corporate/Documents/insight/blockchain_understanding_the_potential.pdf

To pozwala bankom na wyeliminowanie ryzyk operacyjnych związanych z m.in. zmianami i awariami obecnych, centralnych, systemów.

- Szybkość – ponieważ dzięki blockchain transakcje mogą odbywać się bez pośredników i centrum autoryzacyjnego, czas realizacji transakcji został skrócony wyłącznie do czasu potrzebnego dwóm stronom transakcji na skomunikowanie się. Pozwala to bankom na oferowanie usług z natychmiastowym (a nie pozornym) czasem rozliczenia. Przygotowanie, zrealizowanie, autoryzacja i rozliczenie transakcji w blockchain jest jednym zdarzeniem mającym miejsce w czasie rzeczywistym bez rozbijania tych czynności na pojedyncze zdarzenia w różnych systemach bankowych.
- Wydajność – systemy rozproszone umożliwiają wielokrotnie wyższą wydajność niż rozwiązania centralne. Dostęp do informacji potrzebnej w transakcji blockchain nie wymaga interakcji z centralną bazą danych (ponieważ jej nie ma). Dzięki temu banki nie muszą rozbudowywać własnej infrastruktury (i planować jej na maksymalne obciążenie), ale mogą dynamicznie wykorzystywać zewnętrzną moc obliczeniową (z ang. *throughput i scaling*).
- Transparentność – dzięki blockchain ryzyko nieautoryzowanego udziału pośredników jest eliminowane (np. zachowania korupcyjne). Pozwala to na wdrożenie w pełni automatycznych (bezobsługowych) procedur, m.in. identyfikacji klienta, przeciwdziałania praniu brudnych pieniędzy, finansowania terroryzmu (z ang. *KYC, AML*), białych i czarnych list użytkowników. Całkowicie eliminuje to wysokie koszty, przeznaczane dziś na te procedury, które nie zwiększają źródeł przychodów bankowych.
- Efektywność kosztowa – dzięki współdzieleniu infrastruktury technologicznej (rozproszona baza danych w chmurze) następuje radykalne obniżenie kosztów. To pozwala na wyeliminowanie przeszkód (z ang. *friction*) takich jak ręczne działania w przestarzałej infrastrukturze bankowej. Dzięki temu banki będą w stanie konkurować z podmiotami o innej strukturze technologicznej i kosztowej, takimi jak np. spółki technologiczne (z ang. *fintech*). To pozwoli bankom na obniżenie kosztów, dziennej płynności oraz (w mniejszym wymiarze) potrzeb kapitałowych.
- Dostosowanie – rozproszona baza danych pozwala bankom na oferowanie swoich usług (finansowych) w nowo powstających obszarach rynkowych, gdzie tradycyjne rozwiązania są nieadekwatne. Usługi rozliczeń pomiędzy urządzeniami w Internecie Rzeczy (z ang. *Internet of Things*)

jest możliwe jedynie w modelach *machine-to-machine*, bez zaangażowania końcowego użytkownika (np. automatyczna opłata autostradowa).

Kryptowaluty dały początek technologii blockchain i distributed ledger technology

W pierwszej fazie rozwoju blockchaina użytkownikami byli cyfrowi alterglobaliści, którzy stworzyli rozwiązania technologicznie bezpieczne, ale bez udziału banków. Wieloletnia próba rozwiązania antybankowego bitcoina potwierdziła, że blockchain jest technologicznie rozwiązaniem doskonałym. Pokazała również, że do powszechnego użycia wymaga on zaufania, które mają jedynie banki. W efekcie bitcoin, podobnie jak inne krypto-waluty (dogecoin, etc.) ma ogromną zmienność wartości (od 1–1215 do obecnych ok. 400 dolarów), a w efekcie nie jest rozwiązaniem bazowym z punktu widzenia prowadzenia biznesu. Wiele z cech blockchaina zostało wdrożonych w kryptowalutach. Różnice pomiędzy rozwiązaniem technologicznym blockchain a zastosowaniem biznesowym bitcoin (i innymi) wynika z założeń i wymagań cyfrowych alterglobalistów. Wśród tych specyficznych wymagań kryptowalut, dwa odgrywają kluczową rolę:

- brak wydawcy pieniądza (banku centralnego, komercyjnego), co wymusza konieczność „tworzenia pieniądza" w wyniku operacji matematycznych (kopanie, z ang. *minning*). Jedynie stworzenie pierwszego blockchaina w infrastrukturze bankowej (tzw. *genesis block*) eliminuje ten problem.
- Konieczność ciągłego uzgadniania transakcji w wyniku braku zaufanego wydawcy pieniądza (banku). To wymusza potrzebę tzw. konsensusu (z ang. *consensus voting*), który powoduje dwa duże problemy kryptowalut. Po pierwsze, nieefektywne wykorzystywanie zasobów. Problemem jest wymóg, że wszystkie elementy rozproszonej bazy muszą uzgadniać czy dana transakcja jest uczciwa, czy nie. Po drugie – duże opóźnienia. Ponieważ daną transakcję musi uzgadniać wielu uczestników, wydłuża to czas trwania transakcji, tym samym tracąc natychmiastowość. Jedynie w oparciu o zaufanie do bankowego genesis block (z ang. *indisputable ownership*), można wyeliminować problem opóźnień (uzgadniania) transakcji.

Wszystko to stało się możliwe, dzięki zupełnie różnemu od bankowego modelu prywatności. W systemie bankowym informacje o transakcjach są

ukryte przed społeczeństwem, natomiast w przypadku bitcoina i innych kryptowalut wszystkie informacje o transakcjach zapisane są w publicznej rozproszonej bazie, jednak nikt nie ma dostępu do informacji o tożsamości poszczególnych użytkowników.

Bitcoin cechuje się wciąż słabą infrastrukturą, dużą zmiennością, brakiem regulacji, trudnością w wycenie, a giełdy bitcoina mogą być podatne na ataki, ale mimo to po siedmiu latach zdobył ogromną popularność, liczba jego użytkowników stale rośnie, a inwestorzy ochoczo wspierają startupy bitcoinowe.

Oczy największych instytucji zarówno finansowych, jak i technologicznych skierowane są nie w stronę samego bitcoina, a technologii, na której się opiera *distributed ledger technology*, bo okazała się niezwykle stabilna i odporna na różnorodne ataki. Otwarty system typu peer-to-peer wymagał stworzenia niezawodnej bazy danych, która jednocześnie byłaby publicznie dostępna i to ona wzbudza największe emocje.

Blockchain jest technologią, która stoi u podstaw bitcoina i obecnie powszechne jest przekonanie, że to właśnie ten pierwszy jest dużo ważniejszym wynalazkiem od tego drugiego. Uważają tak m.in. eksperci The Bank of England, którzy już w 2014 r. udostępnili dwa raporty „Innowacje w technologiach płatniczych i pojawienie się walut cyfrowych" i „Ekonomia walut cyfrowych", w których zauważyli, że technologia Blockchain pozwoli nie tylko na spore oszczędności, ale także może być receptą na problemy w postaci ryzyka kredytowego, ryzyka braku płynności finansowej i ryzyka operacyjnego.

Informacja o wszystkich transakcjach od momentu powstania jest zapisywana w blockchainie. Jakakolwiek próba ingerencji w historyczne informacje zostałaby natychmiast zauważona, ponieważ każdy kolejny blok posiada sumę kontrolną bloku poprzedniego.

Każda transakcja w sieci wiąże się z prześledzeniem historii pochodzenia danej monety aż do momentu jej emisji, w związku z czym podwójne wydanie środków nie jest możliwe. W momencie emisji algorytm generuje nowy blockchain z wykorzystaniem klucza publicznego oraz dwóch funkcji skrótu SHA256 i RIPEMD-160. Klucz publiczny natomiast wywodzi się z klucza prywatnego poprzez multiplikację krzywych eliptycznych. Klucz prywatny pozwala na przeniesienie środków pomiędzy użytkownikami.

Kryptografia klucza prywatnego stanowi podstawę działania całego Internetu. Gdyby nie krzywe eliptyczne i wykorzystanie dużych liczb pierwszych, Internet, jaki znamy, nie mógłby istnieć, ponieważ wszystkie zabezpieczenia opierają się właśnie na tego typu kryptografii.

Blockchain, jako nowy rodzaj bazy danych, daje szereg zupełnie nowych możliwości. Może pozwolić na stworzenie niezawodnych systemów giełdowych, systemów bankowych, systemów wyborczych, a także na tworzenie inteligentnych kontraktów, zaawansowanej ekonomii w grach komputerowych i rozwój Internetu rzeczy.

We wrześniu 2015 r. The Wall Street Journal cytował słowa prezesa IBM Research, Arvinda Krishna, który powiedział: „Przez ostatni rok badacze rozwijali własną wersję cyfrowego rejestru. System może zapisywać transakcje na przykład pomiędzy bankami albo firmami działającymi międzynarodowo".

Z kolei Open Ledger Projekt ma pozwolić firmom na stworzenie własnych rozwiązań opartych na rozproszonych rejestrach bez konieczności tworzenia swoich Blockchainów, takich jak bitcoin albo Ethereum.

Technologię łańcucha bloków wykorzystuje już Nasdaq, który pod koniec 2015 r. udostępnił swój produkt Nasdaq Linq. Linq jest częścią Nasdaq Private Market. Platforma pozwala na handel akcjami a dokumentacja jest zarządzana cyfrowo poprzez wykorzystanie platformy opartej na blockchainie.

Nad możliwościami wykorzystania łańcucha bloków pracują także Visa, MasterCard, PayPal, Londyńska Giełda Papierów Wartościowych czy Australian Securities Exchange (największa australijska giełda papierów wartościowych).

Chris Skinner, uznany wizjoner świata FinTech, opublikował w American Banker artykuł[14], w którym rozważa czy blockchain ma szansę zastąpić SWIFT (Stowarzyszenie na rzecz Światowej Międzybankowej Telekomunikacji Finansowej). Artykuł ten wywołał duże poruszenie w branży bankowej, ponieważ dla wielu bankierów jest to rzecz niewyobrażalna. SWIFT jest podstawą przemysłu bankowego na całym świecie, jest to sieć stworzona w latach 70. Poprzedniego wieku, która pośredniczy w transakcjach pomiędzy bankami, domami maklerskimi, giełdami i innymi instytucjami finansowymi. Każdego dnia w sieci realizowanych jest ok. 14 mln operacji. We wrześniu 2010 r. z sieci korzystało ponad 9 000 instytucji finansowych z 209 krajów.

Zdaniem wielu to właśnie technologia rozproszonej księgi głównej może wyprzeć 40-letnią sieć. Blockchain, za którą stoi więcej mocy obliczeniowej niż za dowolnym projektem otwartoźródłowym w historii, może fundamentalnie przekształcić system bankowy. SWIFT jest jedynie systemem wymiany infor-

14 Will the Blockchain Replace Swift?, Chris Skinner, marzec 2016, http://www.americanbanker.com/bankthink/will-the-blockchain-replace-swift-1079740-1.html

macji i nie przechowuje żadnych aktywów, a zaangażowanie SWIFT w inicjatywę blockchain może sugerować, że po prostu zaadoptuje nową technologię. „Jestem przekonany, że już za kilka lat każdy z nas będzie na co dzień korzystać z technologii blockchain i większość osób nawet nie będzie sobie zdawała z tego sprawy" napisał Daniel Haczyk, właściciel serwisu bitcoinet.pl.

W listopadzie 2015 r. Microsoft ogłosił „Blockchain, jako usługę" wprowadzając pierwsze usługi finansowe oparte o blockchain i bitcoin do Microsoft Azure – platformy obliczeniowej w chmurze. Usługa Microsoftu udostępnia mechanizmy pozwalające na przetwarzanie danych i ich przechowywanie. Są to narzędzia dla deweloperów, które pozwalają m.in. na szybki rozwój inteligentnych kontraktów opartych o zintegrowane środowisko deweloperskie oraz o prywatne i półprywatne środowiska łańcucha blockchain. Zapewni to elastyczność i rozciągliwość, na której zależy wielu uczestnikom, a przede wszystkim sprawia, że korzystanie z technologii blockchain stało się dużo tańsze, łatwiejsze i przyjemniejsze.

Model 1: Tradycyjna bankowość – wszystko wpisywane w jednym miejscu

Model 2: Kryptowaluty – wszyscy wszystko muszą uzgodnić

Model 3: Bankowy Blockchain – zaufanie do banków, transakcje bez pośredników

Blochchain w usługach płatniczych

Blockchain często jest błędnie utożsamiany z bitcoinem. Poniżej porównanie dwóch typów rozwiązań opartych o technologię blochchain: rozwiązania kryptowalut (np. bitcoin) oraz distributed ledger technology (np. billon, czyli pierwszego komercyjnego wdrożenia technologii blockchain w banku[15])

Kryptowaluty vs. Distributed ledger technology – obszary techniczne

Obszary techniczne	**Distributed ledger technology (np. billon)**	**Kryptowaluty (np. bitcoin)**
Technologia blockchain	tak	tak
Czy używanie wymaga jakiejkolwiek wiedzy technicznej?	nie	tak
Możliwość podwójnego wydawania tych samych środków (z ang. *double spend*)	nie	nie
Własność środków należy wyłącznie do jednej osoby	tak	tak
Baza danych przetrzymywana centralnie	nie	nie
Czas trwania transakcji	natychmiast	do 10 min. (czas konieczny do potwierdzenia transakcji)
Czy jest techniczny koszt realizacji transakcji?	nie	tak (koszt *3rd party authorisation*[16])
Możliwość zarządzania środkami z różnych urządzeń	tak	tak
Możliwość indywidualnego dostosowania poziomu zabezpieczeń	tak	nie
Czy łatwo zintegrować np. w sklepie internetowym?	tak	tak

15 Jest to pierwsze zastosowanie technologii blockchain zgodnie z przepisami pieniądza elektronicznego opisanego w dyrektywie Unii Europejskiej 2009/110/WE z 2009 r. oraz przepisach lokalnych poszczególnych państw członkowskich

16 Każda transakcja w bitcoin wymaga autoryzacji (3rd party authorisation wykonywane przez nody – serwery pośredniczące). Obecnie jest możliwa bezpłatna autoryzacja, ale czas oczekiwania na autoryzację wynosi ok. 60 minut. Od 2040 r. (gdy zostanie wykopany ostatni bitcoin) wszystkie autoryzacje, czyli transakcje, będą płatne. Wynika to z konieczności pokrycia kosztów i zysku nodów autoryzacyjnych.

Kryptowaluty vs. Distributed ledger technology – obszary formalno-prawne

Obszary formalno-prawny	Distributed ledger technology (np. Billon)	Kryptowaluty (np. bitcoin)
Źródło podstawy pochodzenia środków	ustawa (bank wydawca)	algorytm (maszyna kontrolowana przez nieznanych użytkowników (z ang. *bitcoin minors*)
Czy jest to nowa waluta?	nie	tak
Zgodność z regulacjami prawnymi (prawo bankowe, AML, KYC)	tak	nie
Czy jest stabilny finansowo?	tak (1 złoty to zawsze 1 złoty)	nie (dziś 1 bitcoin to $400, w 2015 – $1200)
Środki cyfrowe są legalnym środkiem płatniczym	tak	nie
Czy istnieje podmiot mający uprawnienie do weryfikowania użytkowników (cel – ochrona przed nielegalnymi praktykami)?	tak	nie
Zgodność z istniejącym systemem bankowym	tak	nie
Czy istnieje obawa użycia do nielegalnych praktyk np. prania brudnych pieniędzy?	nie	tak

Blockchain w rozwiązaniach bankowych musi łączyć w sobie kilka obszarów. Musi spełniać europejskie ramy prawne, w szczególności przepisów o pieniądzu elektronicznym, przeciwdziałaniu praniu brudnych pieniędzy i finansowania terroryzmu (AML), identyfikacji klienta (KYC) oraz innych szczegółowych przepisów prawnych. Musi być wygodnym rozwiązaniem dla konsumentów (użytkowników), tak aby korzyści kolejnej technologii były łatwo zrozumiałe. Musi być narzędziem do masowego pozyskiwania klientów dla banków. W innym wypadku byłoby to powielanie zasady „najpierw zabranie kompletu danych klienta, potem zostanie klientem bankowym", a nie naśladowałoby rozwiązań usługodawców internetowych – „najpierw zostań klientem, a dopiero potem, gdy to konieczne, podaj swoje dane".

Technologia blockchain pozwala każdemu bankowi na emisję (wydawanie) pieniądza elektronicznego, który posiada praktycznie wszystkie cechy

gotówki. Nie jest on produktem fizycznym, takim jak papierowe pieniądze, a produktem elektronicznym – pieniądzem elektronicznym (cyfrowym). Banki mogą prowadzić masowe akcje akwizycji klientów, podobnie jak firmy internetowe, gry internetowe lub każdy inny biznes konsumencki. Tym sposobem dotychczas nieubankowieni klienci (np. młodzież) mogą rozpocząć korzystanie z usług bankowych. Podobnie bank wydawca może przejąć klientów, którzy posiadają już relację bankową z innym bankiem, ale dzięki technologii blockchain klient ten chętniej skorzysta z usług banku wydawcy (np. w celu wygodnego odebrania lub wysłania pieniędzy przez Facebooka).

Koszty, nie tyle wdrożeniowe, a wiążące się z utrzymaniem nowego zestawu usług finansowych dla klientów są istotne dla banków. Wdrażanie technologii blockchain w banku może mieć charakter modułowy:

Stand-alone blockchain – czyli rozwiązanie, gdzie całkowite koszty technologiczne są po stronie użytkownika (konsumenta lub sprzedawcy). Jest to rozwiązanie podobne do tych znanych z kryptowalut, gdzie tzw. wallet jest zainstalowany u użytkownika, a jedynie informacja o nowym użytkowniku jest wysyłana do banku wydawcy.

Thin cloud blockchain client – czyli rozwiązanie, gdzie koszty utrzymania i obsługi klienta są dzielone pomiędzy samego użytkownika a bank wydawcę. Jest to rozwiązanie podobne do obecnych rozwiązań bankowości mobilnej, z tą różnicą, że ok. 50% kosztów utrzymania ponosi sam użytkownik (np. poprzez zainstalowanie blockchainowej aplikacji bankowej na własnym urządzeniu).

Bank-side blockchain – czyli rozwiązanie, gdzie bank ponosi koszty utrzymania klienta, a klient korzysta z technologii blockchain poprzez stronę internetową, bez konieczności instalacji blockchainowej aplikacji na swoim urządzeniu. Doświadczenia klienta (z ang. *customer journey, customer experience*) jest podobne jak w bankowości online. Natomiast koszty świadczenia usługi bankowej są praktycznie wyeliminowane.

Każde z tych rozwiązań pozwala wykorzystać blockchain do zaoferowania lekkiego konta bankowego każdemu nowemu klientowi, ponieważ proces jego akwizycji jest oparty o schematy usług internetowych, a nie usług finansowych. Dzięki takiemu podejściu bank może wyeliminować praktycznie wszystkie bariery konwersji z jakimi stykają się potencjalni klienci tradycyjnych usług bankowych. Dodatkowo, koszt obsługi nowo pozyskanych klientów jest o ok. 80-90% niższy niż w przypadku tradycyjnych usług rachunku bankowego. W kontekście prawnego obowiązku udostępniania darmowego

rachunku bankowego[17], regulacji PSDII – optymalizacja kosztów świadczenia usług bankowych ma coraz większe znaczenie.

Blockchain to radykalne obniżenie kosztów dla banków, bez kosztów braku skali[18]

W rozwiązaniach *thin cloud blockchain client* oraz *bank-side blockchain*, bank nie musi przygotowywać żadnej własnej infrastruktury, może korzystać np. z platformy chmury obliczeniowej Microsoft Azure. Dzięki połączeniu technologii blockchain z chmurą obliczeniową Azure, bank eliminuje dotychczas największy koszt uruchomienia nowej usługi dla klientów – przygotowania i utrzymania kolejnej infrastruktury technologicznej. Połączenie trzech obszarów: blockchain, chmury obliczeniowej oraz wiedzy bankowej pozwala na stworzenie produktów i usług bankowych, które pozwolą bankowi na skuteczne i efektywne kosztowo konkurowanie o klientów. Dotychczasowe wyliczenia pozwalają na wycenę całkowitych kosztów obsługi klienta na poziomie 1 zł miesięcznie. Dzięki wykorzystaniu chmury obliczeniowej Azure są to realne koszty, nawet w przypadku małej bazy klientów banku korzystających z blockchain. Tak radykalne obniżenie kosztów obsługi klientów, pozwoli bankowi na przeniesienie budżetów na rzecz akwizycji i marketingu konsumenckiego.

17 Każdy bank będzie musiał oferować darmowe konto, Wojciech Boczoń, bankier.pl, http://www.bankier.pl/wiadomosc/Kazdy-bank-bedzie-musial-oferowac-darmowe-konto-7273106.html

18 Szczytowych obciążeń, z ang. *peak scaling costs*

Sebastian Ptak
jest Członkiem Zarządu Blue Media S. A., odpowiada między innymi za obszar bezpieczeństwa oraz rozwój biznesu, szczególnie za rozwój i nadzór nad Systemem Płatności BlueCash (system międzybankowych przelewów natychmiastowych).
Absolwent Wydziału Prawa Uniwersytetu Gdańskiego, stypendysta Ministerstwa Edukacji Narodowej. Jest Członkiem Prezydium Forum Technologii Bankowych przy Związku Banków Polskich. W roku 2009 uhonorowany przez Związek Banków Polskich tytułem Ambasadora Gospodarki Elektronicznej, zaś w roku 2010 – Odznaką Honorową ZBP.

Sebastian Ptak, Członek Zarządu Blue Media SA

Przyszłość systemów płatniczych

Historia płatności to historia stopniowego pozbywania się w procesie płacenia fizycznej reprezentacji wartości nabywanego bądź zbywanego dobra lub usługi. Droga ta wiodła od wymiany barterowej przez reprezentację wartości w kruszcu, gotówkę, kartę płatniczą aż do technologii pozwalających płacić bez fizycznego nośnika.

Jednocześnie pierwszy raz w historii polskich płatności ich rozwój jest w tak dalekim stopniu zintegrowany z europejskimi i światowymi trendami. Wpływa na to zarówno globalny obrót gospodarczy (w szczególności handel internetowy), jak i powstające na poziomie Komisji Europejskiej regulacje (w szczególności przyjęta niedawno dyrektywa PSD2, do implementacji której członkowie Unii Europejskiej, a zatem również Polska, są zobligowani do końca 2017 r.).

Prócz dostępnych technologii i próbujących nadążyć za nimi regulacji o tym, jak będziemy płacić w przyszłości zdecyduje rynek, czyli jego uczestnicy. W szczególności zaś – płatnicy oraz akceptanci. To oni zdecydują, które z technologii dopuszczonych do wykorzystania na rynku płatniczym rozpowszechnią się, a które zostaną odrzucone lub zepchnięte do niszy. Oczywiście będą to te technologie, które w możliwie pełnym stopniu zaspokoją potrzeby uczestników rynku.

Analizując rozwój płatności możemy wyróżnić trzy kluczowe grupy trendów determinujące kształtowanie się tego rynku:

- technologiczne,
- społeczno-rynkowe,
- regulacyjne.

Ich analiza będzie punktem wyjścia do odpowiedzi na pytanie, jak będą wyglądały płatności przyszłości. Niektóre przedstawione w tym artykule rozwiązania mogą sprawiać wrażenie, jakby pochodziły z literatury *science fiction*. Nic bardziej mylnego! Te technologie są dostępne już teraz. Trzeba jednak pamiętać, że na system płatności prócz technologii – czyli nośników – składają się również źródła pieniądza oraz podmioty pośredniczące w procesie płatności. One też będą ewoluowały. Już ewoluują.

Trendy technologiczne

Zanim przejdziemy do przeglądu wschodzących technologii płatniczych, warto przyjrzeć się temu, jakie metody płatności są obecnie najbardziej popularne i dlaczego?

Gotówka

Są miejsca jak Szwecja, gdzie na poważnie myśli się o odejściu od emisji pieniądza, ale póki co, pogłoski o śmierci gotówki są grubo przesadzone.

Jak popularna jest ciągle gotówka pokazują m.in. wyniki badań TNS Polska[1]. Aż 53% Polaków za zakupy spożywcze płaci wyłącznie gotówką (wyłącznie karty płatniczej w tym celu używa jedynie 3% z nas, a 43% używa raz karty, raz gotówki). Podobnie płacimy kupując ubrania – 52% wskazań na wyłączność gotówki i 4% na wyłączność karty. Niewiele częściej sięgamy po kartę płacąc za większe zakupy – wyłącznie z karty korzysta wówczas 8% Polaków, zaś wyłącznie z gotówki – 48%.

A jak opłacamy domowe rachunki? Według tych samych badań najwięcej, bo w przypadku czterech na dziesięć gospodarstw domowych robi się to na poczcie. (Warto wspomnieć, że Poczta Polska dopiero w 2016 r. rozstrzygnęła przetarg na dostarczenie do placówek terminali POS do obsługi kart płatniczych. Do tej pory płatność kartą możliwa była w niewielu wybranych placówkach i obciążona relatywnie wysokimi prowizjami. Możemy zatem przyjąć, że gros pocztowych opłat to opłaty w gotówce.). Do tego 17% gospodarstw zadeklarowało opłacanie rachunków gotówką w banku lub agencji bankowej, dalsze 6% – gotówką, w kasie wystawcy rachunku, 5% – gotówką w punkcie finansowym, 4% – gotówką w sklepie, 2% – gotówką u inkasenta.

1 NS Polska, wrzesień 2015, badania przeprowadzone techniką wywiadów bezpośrednich wspomaganych komputerowo na reprezentatywnej grupie dorosłych Polaków; http://www.tnsglobal.pl/wp-content/blogs.dir/9/files/2015/09/K.65_Jak_placa_Polacy_O08a-15.pdf

Ciekawe światło na popularność gotówki rzucają również badania przeprowadzone przez ICAN Research na zlecenie Blue Media[2]. Pokazują bowiem, że gotówka cieszy się dużą popularnością nawet w… e-commerce. Na korzystanie z płatności „za pobraniem", realizowanej u kuriera lub na poczcie, wskazało 51% ankietowanych klientów e-sklepów. Metodę tę wyprzedziło jedynie samodzielne realizowanie przelewu z własnego konta bankowego, z 60% wskazań. Dodatkowo 9% ankietowanych wskazało, że płaci gotówką w punkcie odbioru towaru. Biorąc pod uwagę, że mówimy tu o zakupach robionych w internecie, popularność gotówki daje wiele do myślenia.

Skąd takie przywiązanie do gotówki? Strategiczny dokument Koalicji na rzecz obrotu bezgotówkowego i mikropłatności[3] zwraca uwagę głównie na kwestie psychologiczne – w szczególności brak zaufania do banków jako miejsca przechowywania pieniędzy, przekonanie o wysokich kosztach. Przekonanie to przez lata utrwalał wysoki poziom opłat organizacji kartowych, jakie te nakładały na obsługę transakcji. Mimo, iż w ostatnich latach uległy one zdecydowanemu obniżeniu, przeświadczenie o wysokich kosztach ciągle pokutuje, chociażby w drobnym handlu.

Istotnym czynnikiem wpływającym na popularność rozwiązań bezgotówkowych są nawyki starszego pokolenia. Te jednak ulegają zmianie, ze względu na konsumencką „zmianę pokoleniową" – do głosu dochodzą otwarci na technologię i ceniący wygodę przedstawiciele pokolenia Y (więcej o tej grupie: czytaj poniżej).

Pay by link – polska specjalność

Bardzo istotnym rozwiązaniem dla obecnego i przyszłego modelu płatności w Polsce są tzw. Pay by linki. Działają one w oparciu o rachunki bankowe jako źródło pieniądza. Osoba dokonująca płatności (np. za zakupy w sklepie internetowym) po wybraniu produktów klika w ikonę płatności swojego banku i jest automatycznie przekierowywana do swojej bankowości internetowej, gdzie czeka na nią wypełniony już formularz z informacjami o płatności – wysokością, numerem bankowym, adresatem. Metoda ta wymaga identyfikacji

2 ICAN Research na zlecenie Blue Media, wrzesień 2015, badania przeprowadzone techniką wywiadu telefonicznego na reprezentatywnej grupie dorosłych Polaków; http://www.slideshare.net/BlueMedia_Sopot/191015-co-decyduje-o-wyborze-sklepu-badanie

3 Program Rozwoju Obrotu Bezgotówkowego w Polsce na lata 2016–2020, grudzień 2013; http://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/obrot_bezgotowkowy/dokumenty_dla_czlonkow/Cz_I_Dokument_strategiczny.pdf

i autoryzacji klienta na stronie banku (przez podanie loginu i hasła do internetowego konta bankowego) oraz autoryzacji płatności (za pomocą narzędzia autoryzacyjnego danego banku, np. numeru ze zdrapki lub hasła SMS).

Pay by linki powstały z autentycznej potrzeby, jaka pojawiła się wraz z pierwszymi sklepami internetowymi. U zarania polskiego e-commerce karty płatnicze były w naszym kraju mało rozpowszechnione i raczej postrzegane jako narzędzie do wypłacania gotówki z bankomatu niż płacenia w internecie. Podawanie numerów karty w sieci uważane było za ryzykowne.

Potrzebne było więc inne rozwiązanie, pozwalające zastąpić kartę płatniczą w oparciu o środki zgromadzone na rachunku bankowym.

Technologie mobilne i zbliżeniowe

Karta płatnicza, a w szczególności zbliżeniowa, czyli PayPass, swoją popularność zawdzięcza wygodzie. Były obawy co do bezpieczeństwa i zaufania klientów, ale najwyraźniej stosunek wygody do akceptowanego poziomu bezpieczeństwa oraz mechanizmy gwarancyjne okazały się wystarczające, by ta forma przyjęła się wśród klientów. Według szacunków z końca roku 2015, w obiegu jest ok. 27,6 mln kart zbliżeniowych, co stanowi blisko 80% kart płatniczych w Polsce.

Rozwinięciem idei kart płatniczych jest wykorzystanie technologii mobilnych. Skoro każdy ma w kieszeni telefon komórkowy, po co dodatkowo nosić kartę? Do niedawna przeszkodą w popularyzacji tej technologii było wykorzystanie karty SIM jako narzędzia autoryzacji transakcji. Klient musiał więc mieć podpisaną umowę z firmą telekomunikacyjną, uzyskać stosowną kartę SIM oraz telefon z funkcją zbliżeniową. Problem ten częściowo został rozwiązany dzięki technologii Host Card Emulation (HCE), przenoszącej proces autoryzacji do chmury obliczeniowej. W efekcie aby płacić telefonem zbliżeniowo nie trzeba być nawet w zasięgu sieci GSM. Cały czas trzeba jednak pobrać odpowiednią aplikację na telefon i ją aktywować – tę musi stworzyć i udostępnić nam nasz bank. Obecnie na polskim rynku płatności HCE oferuje pięć banków: Pekao, Getin, BZ WBK, PKO BP i Eurobank, a nad ich wdrożeniem pracują kolejne. Również te banki, które początkowo inwestowały w rozwiązania oparte o karty SIM – takie jak Raiffeisen czy mBank.

Oddzielną grupę stanowią rozwiązania wykorzystujące powszechną dostępność telefonów komórkowych, takie jak SkyCash czy mPay. Swoją niszę znalazły one tam, gdzie płatność musiała być dokonana „w terenie" i to w czasach, kiedy nikt jeszcze nie myślał o smartfonach ani o powszechnym

dostępie do mobilnego internetu. Do tej pory są popularnym rozwiązaniem do płacenia za bilet komunikacji miejskiej lub parkowanie. Jako źródło pieniądza wykorzystują karty płatnicze oraz wirtualne portmonetki (pozabankowe rachunki płatnicze, na które użytkownik musi przelać środki).

Schematy lokalne

Inicjatywę w tworzeniu rozwiązań i organizowaniu wygodnych rozwiązań płatniczych przejawiają również banki.

W tym miejscu warto wspomnieć o wspólnej inicjatywie tych polskich, która zmaterializowała się jako system Blik, który wystartował w lutym 2015 r. Uczestniczą w nim takie banki, jak Alior, Millenium, Bank Zachodni WBK, ING Bank Śląski, mBank, PKO Bank Polski oraz Orange Finanse, a narzędzia autoryzacyjnego dostarcza powołany w tym celu podmiot – Polski Standard Płatności. System pozwala płacić za zakupy w internecie, w naziemnych punktach sprzedaży (również zbliżeniowo) oraz wypłacać gotówkę z bankomatu. Planowane jest również uruchomienie możliwości przelewania pieniędzy na inne prywatne konto (p-2-p) z wykorzystaniem numeru telefonu. W Blik autoryzacja oparta jest o kod cyfrowy generowany przez Polski Standard Płatności. Na początku marca 2016 r. system miał ponad 1,4 mln użytkowników, którzy w ciągu roku od jego uruchomienia wykonali ponad 2 mln transakcji.

Swój lokalny system płatniczy pod nazwą PayM organizują też banki w Wielkiej Brytanii. PayM to inicjatywa dziewięciu banków, która wystartowała na początku 2014 r., a do której dołączyły szybko kolejne. Obecnie w zasięgu systemu jest 90% tzw. current accounts (rachunki bankowe używane w Wielkiej Brytanii do płatności). System służy głównie do płatności p-2-p, na konto osób prywatnych lub np. sprzedawców na targu. Rachunki użytkowników powiązane są z ich kontami bankowymi. Jest to więc rodzaj „przelewu na telefon". Z 18 mln użytkowników bankowości mobilnej w Wielkiej Brytanii aplikację PayM ściągnęło na telefon 3 mln użytkowników. Jednak w ciągu ostatnich kwartałów dynamika pobrań spada, a liczba faktycznie wykonywanych przelewów jest bardzo niska – przeciętny zarejestrowany użytkownik korzysta z aplikacji średnio raz do roku.

… i ponadnarodowe

Ciekawe propozycje w technologiach zbliżeniowych proponują światowi giganci technologiczni: Google, Samsung, Apple, a ostatnio również Huawei.

Firmy te nie są bankami, a płatności realizowane są w oparciu o rozwiązania kartowe. Ich innowacyjność polega na implementacji rozwiązań płatniczych na poziomie telefonu i systemu operacyjnego. Pomysły te są o tyle krokiem do przodu, że „narzędzie" dostajemy od razu z telefonem. Nie trzeba instalować ani uruchamiać aplikacji, a do autoryzacji wykorzystywane są czytniki linii papilarnych.

Na powyższych przykładach widać ważną prawidłowość – dążenie do wygody. Im szybsza forma płatności, im mniej angażuje klienta, im mniej kroków od niego wymaga – tym lepiej.

Jakie technologie czekają za rogiem? Co jeszcze jest możliwe z technologicznego punktu widzenia?

Internet of things i wearables

Płatności w oparciu o tzw. internet rzeczy (IoT) to płatności wykonywane przez maszyny lub urządzenia. Przewiduje się, że internet rzeczy może spopularyzować automatyczne płatności, takie jak za przejazd autostradą, opłatę za parking, a nawet za codzienne zakupy. Projekt samoczynnego zamawiania produktów spożywczych online i płacenie za takie zakupy za pomocą lodówki rozwija Samsung. Lodówka Family Hub będzie wyposażona w kartę sieciową WiFi, ekran, system operacyjny (Android) oraz aplikację, za pomocą której można wybierać produkty z list dostarczanych przez dostawców spożywczych – partnerów projektu. Do aplikacji jest również dostęp zdalny – ze smartfona lub tabletu.

Miniaturyzacja pozwala na komunikowanie się za pośrednictwem internetu nie tylko dużym urządzeniom, ale nawet elementom garderoby. Zegarek, pasek, biżuteria – jeśli coś może zostać podłączone do sieci, może tez posłużyć do wykonywania transakcji. Źródłem pieniądza w takich rozwiązaniach najczęściej jest karta płatnicza. Autoryzację coraz częściej zapewniają zaś rozwiązania biometryczne – czytniki linii papilarnych (takie jak w telefonie), ale też np. detektory pulsu umieszczone w pasku zegarka czy bransoletki.

Biometria

Dane biometryczne już dzisiaj wykorzystywane są jako jedna z metod w procesach autoryzacji bądź uwierzytelniania. W Polsce niektóre aplikacje mobilne banków umożliwiają logowanie przez odcisk palca. W Japonii od kilku

lat powszechnie funkcjonuje system skanowania układu krwionośnego palca (*finger vein*) w oddziałach banków i bankomatach. W Polsce także coraz więcej bankomatów wyposażonych jest w funkcje biometryczne, oparte o skanowanie układu krwionośnego palca. Na masową skalę biometrię zaczęła wykorzystywać w swoich maszynach m.in. firma Planet Cash (obecnie ok. 2 400 bankomatów w całej Polsce). Wprowadzenie czytników biometrycznych w bankomatach jeszcze w 2016 r. zapowiedział również największy polski bank – PKO BP. Biometrię w procesie uwierzytelniania zaczęły wykorzystywać niektóre banki (Bank BPH, Getin) także w swoich placówkach.

Z kolei w Wielkiej Brytanii klienci bankowości telefonicznej banku Barclays mogą weryfikować swoją tożsamość za pomocą głosu. W ten sposób klient jest identyfikowany i dostaje dostęp do swoich danych w bankowości elektronicznej, a zatem do świadczonych tą drogą usług.

Biometria może być także wykorzystana do autoryzowania płatności. Tzw. *selfie pay* polega na potwierdzeniu operacji poprzez rozpoznanie kształtu twarzy użytkownika. Autorem rozwiązania jest MasterCard, a wykorzystujący je program testowy został wdrożony w Stanach Zjednoczonych m.in. przez Tech Federal Credit Union.

Z kolei w marcu 2016 r. Google poinformował o publicznych testach swojego projektu płatniczego Hands Free. Umożliwia on wykonywanie płatności mobilnych bez potrzeby dotykania telefonu, a potwierdzenia transakcji dokonując głosowo. Wystarczy powiedzieć „Płacę z Google".

Rozważając szanse na popularyzację rozwiązań biometrycznych warto zwrócić uwagę na dwa czynniki. Pierwszy to powszechność telefonów z czytnikiem biometrycznym. Drugi to kwestie prywatności i akceptacji użytkowników dla przekazywania swoich danych biometrycznych. Najprawdopodobniej jednak bariery te zostaną przezwyciężone – wskazują na to aktualne trendy społeczno-rynkowe.

Trendy społeczno-rynkowe

Ten wątek to nic innego jak zmieniające się podejście i oczekiwania płatników. Ci nie stanowią jednorodnej grupy, dlatego konieczne jest podzielenie ich na kategorie: klientów indywidualnych oraz biznes, czyli małe i średnie oraz duże przedsiębiorstwa.

Klienci indywidualni

W kontekście rozwoju płatności, podobnie jak w kontekście rozwoju każdego innego obszaru konsumenckiego, najważniejszą obecnie grupę stanowią tzw. millenials (zwani również pokoleniem Y). Dlaczego ta grupa jest tak ważna?

Przede wszystkim ze względu na swoją liczebność – w Polsce ludzi urodzonych między rokiem 1980 a 2000 (bo tak definiowane jest pokolenie Y) jest 11 mln. Druga istotna kwestia to wysoka absorbcja nowych technologii – internet jest dla nich naturalnym środowiskiem, miejscem zaspakajania najróżniejszych potrzeb.

Co jeszcze charakteryzuje millenialsów? Poniżej kilka wybranych cech:

- cenią sobie wygodę – szybkość i łatwość użycia technologii, jej integrację z innymi usługami, z których korzystają,
- wykazują słabe przywiązanie do marki – pójdą tam, gdzie dostaną lepsze warunki lub lepszą usługę,
- mają inne spojrzenie na dostarczycieli usług – usługi finansowe wcale nie muszą być dla nich świadczone przez banki,
- deklarują specyficzne podejście do prywatności – nie cenią jej tak, jak starsze pokolenie, nie widzą tak wyraźnie zagrożeń związanych z jej utratą.

63% procent ankietowanych przez ICAN Research klientów sklepów internetowych wskazało, że przy wyborze metody płatności najważniejsza jest dla nich „wygoda". Kolejne 43% respondentów wskazało „łatwość". Bezpieczeństwo wymieniło 47% ankietowanych[4].

Mali przedsiębiorcy

Tu, podobnie jak w przypadku klientów indywidualnych, najważniejsza jest wygoda rozwiązania, przynajmniej w przypadku płatności nisko- i średniokwotowych. To właściciel często zajmuje się finansami i swoje przyzwyczajenia i oczekiwania przenosi na grunt firmy.

Innym czynnikiem wpływającym na sposób rozliczeń z udziałem firm, w szczególności małych i średnich, są limity wysokości transakcji, jakie firmy mogą realizować za pomocą gotówki. Te były stosunkowo wysokie

4 ICAN Research na zlecenie Blue Media, wrzesień 2015, badania przeprowadzone techniką wywiadu telefonicznego na reprezentatywnej grupie dorosłych Polaków; http://www.slideshare.net/BlueMedia_Sopot/191015-co-decyduje-o-wyborze-sklepu-badanie

i wymieniane jako jeden z hamulców rozwoju obrotu bezgotówkowego[5]. Na początku marca br. Ministerstwo Finansów złożyło projekty nowelizacji ustaw (o CIT, PIT oraz swobodzie działalności gospodarczej), które mają te limity obniżyć z 15 000 euro do 15 000 zł. Jest to posunięcie mogące radykalnie zwiększyć wartość obrotu bezgotówkowego. Będzie też bodźcem dla banków i firm technologicznych z nimi współpracujących do generowania nowych rozwiązań dedykowanych średnim i małym przedsiębiorcom.

Nie sposób w tym miejscu również nie wspomnieć o roli, jaką gotówka pełni w szarej strefie gospodarczej. Według różnych szacunków wielkość szarej strefy w Polsce sięga od 12 do aż 19%.

Duże firmy

Wraz ze wzrostem przedsiębiorstwa i wysokości kwot większą wagę w procesie transakcji płatniczych zyskuje bezpieczeństwo. Duże przedsiębiorstwa są tak istotnym klientem dla banków i szerzej, dla rynku płatniczego, że tworzone są dla nich specjalne rozwiązania dostosowane do wewnętrznych systemów i procedur poszczególnych firm. Czynnikiem coraz bardziej istotnym staje się czas, w jakim środki znajdą się na rachunku adresata płatności i będą do jego dyspozycji.

Warto zauważyć, że duże firmy nie tylko wysyłają i przyjmują duże kwoty. Tzw. Masowi Wystawcy Faktur – firmy telekomunikacyjne, dostarczyciele energii elektrycznej i innych mediów przyjmują regularnie setki tysięcy i miliony małej i średniej wysokości wpłat od swoich klientów. W ich przypadku tzw. spłacalność zobowiązań, czyli to czy i jak szybko rachunek zostanie opłacony (wystawcom oczywiście zależy na możliwie szybkiej zapłacie) w dużym stopniu zależy od wygody rozwiązania zaoferowanego klientowi. Im łatwiejszy sposób zapłaty, tym szybsza i pewniejsza spłacalność.

Według wspomnianych już badań[6] Polacy najchętniej płacą przez internet – taką formę deklaruje dwie trzecie badanych. Nie znaczy to, że płacimy natychmiast – tylko 15% Polaków opłaca rachunki, jak tylko otrzyma fakturę. 44% robi to raz w miesiącu, a 36% – kiedy zapada termin płatności. Aż 40%

---

5 Program Rozwoju Obrotu Bezgotówkowego w Polsce na lata 2016–2020, grudzień 2013; http://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/obrot_bezgotowkowy/dokumenty_dla_czlonkow/Cz_I_Dokument_strategiczny.pdf

6 ICAN Research na zlecenie Blue Media, wrzesień 2015, badania przeprowadzone techniką wywiadu telefonicznego na reprezentatywnej grupie dorosłych Polaków: http://www.slideshare.net/BlueMedia_Sopot/15-11-26jak-polacy-placa-za-prad-gaz-i-wode

respondentów przyznało, że zdarzyło się im zapomnieć o opłaceniu rachunku. Dlatego Masowi Wystawcy Faktur szukają możliwie łatwych sposobów płacenia (np. tzw. Pay by linkiem) z poziomu e-faktury lub elektronicznego Biura Obsługi Klienta. Co ważne, przez swoją masowość technologie wykorzystywane przez Masowych Wystawców Faktur mają szansę na szerszą popularyzację – ze względu na obeznanie i przyzwyczajenie klientów.

Na wygodę rozwiązań płatniczych, jakie oferowane są klientom równie baczną uwagę zwraca sektor e-commerce. Płatność jest elementem tzw. customer experience. Jak pokazują badania – aż 24% klientów sklepów internetowych zdarzyło się zrezygnować z zakupu, kiedy nie znaleźli odpowiadającej im formy płatności[7]. Wygoda płatności przekłada się w ten sposób na sprzedaż – płacenie jest najbardziej niewdzięcznym elementem procesu sprzedaży, dlatego powinien on być najmniej kłopotliwy i najmniej widoczny.

Trendy regulacyjne

Dwa najsilniejsze trendy regulacyjne w obszarze płatności i nowych technologii to troska o podniesienie bezpieczeństwa oraz budowa konkurencyjnego, innowacyjnego rynku usług płatniczych.

W obszarze bezpieczeństwa płatności bardzo aktywny jest polski regulator. Pełniąca *de facto* tę rolę Komisja Nadzoru Finansowego zgodnie z politycznym i społecznym oczekiwaniem przede wszystkim stoi na straży interesu obywateli.

W imię bezpieczeństwa klientów właśnie KNF wydała jeszcze w 2014 r. instrukcję zakazującą tzw. *screen scrappingu* – czyli metody automatycznego logowania się do konta bankowego klienta (oczywiście za jego zgodą) i pobierania z niego danych albo inicjowania płatności. W tym czasie nie było jeszcze pewne, jaki w tym obszarze ostateczny kształt przyjmie dyrektywa PSD2.

Pod koniec 2015 r. KNF zakazała również wprowadzania wszelkich usług opartych o dostęp do rachunku przez tzw. podmioty trzecie – przynajmniej do momentu implementacji unijnej dyrektywy PSD2, czyli do końca 2017 r. Wejście w życie zapisów unijnej dyrektywy radykalnie zmieni sytuację.

---

7 ICAN Research na zlecenie Blue Media, wrzesień 2015, badania przeprowadzone techniką wywiadu telefonicznego na reprezentatywnej grupie dorosłych Polaków; http://www.slideshare.net/BlueMedia_Sopot/191015-co-decyduje-o-wyborze-sklepu-badanie

Za pomocą PSD2 Komisja Europejska chce bowiem modelować rynek płatności elektronicznych w Europie, a przez to ułatwić rozwój e-gospodarki. Jej implementacja ma doprowadzić do obniżenia kosztów transakcyjnych i podniesienie bezpieczeństwa transakcji, w szczególności poprzez:

- podniesienie konkurencyjności przez dopuszczenie nowych podmiotów,
- stymulację rozwoju nowych technologii płatniczych online i mobile,
- standaryzację płatności, w szczególności w wymiarze międzynarodowym,
- zabezpieczenie interesu konsumentów, m.in. przez uregulowanie i objęcie nadzorem nowych usług płatniczych.

Co konkretnie wprowadza dyrektywa? Obok banków, instytucji płatniczych, operatorów pocztowych, pojawią się instytucje określane jako TPP (Third Party Provider), które będą mogły świadczyć dwa typy nowych usług: Account Information Service (AIS) oraz Payment Initiation Service (PIS).

AIS umożliwi m.in. zagregowanie informacji o stanie wielu rachunków bankowych, dając klientom łatwy wgląd online w stan ich finansów. Możliwość pobierania danych z rachunku bankowego otwiera także szerzej drzwi dla usług związanych z przenoszeniem rachunku między bankami.

PIS to de facto realizacja płatności z wykorzystaniem rachunku bankowego klienta w jego imieniu. TPP, po otrzymaniu danych do logowania w bankowości internetowej klienta, będzie inicjować płatność w określonej kwocie do określonego odbiorcy i raportować klientowi o jej realizacji. Pomijając kwestie biznesowe, najważniejsza różnica między takim rozwiązaniem a popularnym w Polsce rozwiązaniem Pay by link to kwestia komu przekazywane są dane do logowania i do autoryzacji transakcji. W przypadku usług dopuszczanych przez PSD2 dane podajemy podmiotowi trzeciemu, w przypadku polskiego rozwiązania Pay by link dane podajemy swojemu bankowi.

Jeśli wszystko potoczy się po myśli KE, powstanie otwarty, konkurencyjny, zdolny do generowania innowacyjnych rozwiązań rynek płatności, który ułatwi elektroniczna wymianę gospodarczą w obrębie krajów członkowskich. W tym kontekście ciekawym przypadkiem jest rynek brytyjski. Tutaj brytyjski regulator dążąc do budowy innowacyjnego i konkurencyjnego rynku poszedł jeszcze dalej i na początku 2016 r. zalecił bankom sprzedaż swoich udziałów w brytyjskiej izbie rozliczeniowej – VocaLink.

Pisząc o trendach regulacyjnych warto wspomnieć też o idei cashless głośnej ostatnio za sprawą zapowiedzi Ministerstw: Rozwoju i Cyfryzacji.

Cashless i *paperless Poland*, w obiegu administracyjnym i gospodarczym, ma być istotnym elementem cyfryzacji administracji i modernizacji gospodarki.

Bodźcem do tej zmiany na pewno będą takie regulacje, jak w prowadzona w marcu br. wspomniana wyżej obniżka minimalnej kwoty rozliczenia między firmami, jakie musi być realizowane przelewem.

Przyszłość płatności

Aby nakreślić prawdopodobny model płatności przyszłości warto odwołać się do trzech decydujących o nim kategorii. Są to :

1. nośnik informacji,
2. źródło pieniądza,
3. podmioty pośredniczące w procesie płatności.

Nośnik informacji

Ta kategoria najbardziej działa na wyobraźnię i skłania do futurystycznych rozważań. Współczesna technologia pozwala na bardzo wiele, a ta, która nadchodzi – w zasadzie na wszystko, łącznie z takimi rozwiązaniami jak wyrażenie chęci zapłaty i jej autoryzacja głosowa lub wizualna. Barierą mogą być koszty implementacji – chociaż te, jak w przypadku każdej technologii – maleją wraz z umasowieniem. Istotniejszą barierą będzie akceptowany poziom bezpieczeństwa/ryzyka oraz poszanowania prywatności związanych z danym sposobem płatności. O ile coraz młodsi klienci, którzy nie znają świata bez Internetu, z oboma zagadnieniami mają coraz mniejszy problem, o tyle regulatorzy mogą arbitralnie „zadbać" o ich prywatność i bezpieczeństwo.

Jeśli chodzi o płatności w obrocie administracyjnym i gospodarczym – tu też wygoda technologii płatniczych (w tym szybkość transakcji) będzie istotnym czynnikiem, chociaż jej waga spadnie na rzecz bezpieczeństwa oraz funkcjonalności wpływających na inne procesy biznesowe i rozliczeniowe (takich jak księgowanie czy polityka zwrotów w e-commerce).

Tak więc szanse na sukces będzie miała taka technologia, która okażą się najwygodniejsza dla klienta (najprostsza, najszybsza, wymagająca

najmniejszego możliwego zaangażowania), która jednocześnie spełni oczekiwania regulatorów co do poziomu bezpieczeństwa i poszanowania prywatności. Patrząc jednak na tendencje wśród konsumentów, akceptowany próg w obu tych kwestiach będzie się obniżał.

Źródło pieniądza

Dziś to bank jest podstawowym i dominującym źródłem pieniądza, za pomocą którego płacimy. Nawet karty płatnicze (poza mało znaczącymi wyjątkami) będące w istocie elektronicznym substytutem portfela z gotówką powiązane są z rachunkiem bankowym (lub udzielonym przez bank kredytem) i wykorzystują środki na nim zgromadzone.

Oczywiście istnieją też rachunki płatnicze (tzw. wirtualne portmonetki) prowadzone przez inne podmioty niż bank. Nie zyskały one jednak wielkiej popularności. Stało się tak z dwóch powodów. Po pierwsze, tylko rachunki bankowe mają swój zestandaryzowany numer, który może być odczytywany i przetwarzany. Po drugie, tylko rachunki bankowe zapewniają wysoki poziom bezpieczeństwa, m.in. dzięki gwarancjom Bankowego Funduszu Gwarancyjnego. Dopóki rachunki płatnicze nie zostaną objęte podobnymi rygorami jak rachunki bankowe, mało prawdopodobne, by się upowszechniły i stały miejscem przechowywania środków.

Niemniej jednak różnego rodzaju rozwiązania oparte o ideę „wirtualnej portmonetki" co jakiś czas pojawiają się na rynku.

Tu warto wrócić do dyrektywy PSD2, która ma dać dostęp podmiotom trzecim do rachunków bankowych. Najwyraźniej KE w rachunkach bankowych właśnie widzi źródło pieniądza. Dostęp do nich zwyczajnie podważy sens innych rozwiązań.

Pisząc o źródłach pieniądza nie sposób nie wspomnieć o rozwiązaniach alternatywnych, czyli kryptowalutach. Ich atrakcyjność w dużej mierze polega na anonimowości, wynikającej z ominięcia kontrolowanego systemu bankowego. Mogą być atrakcyjne również z innych względów. Eksperyment z własną narodową kryptowalutą podjęła Islandia, kiedy to światowy kryzys gospodarczy doprowadził jej bank centralny do upadku. Równolegle do Korony Islandzkiej rząd wprowadził wówczas kryptowalutę o nazwie Auroracoin, celem stabilizacji gospodarki.

Pomysł islandzki jest jednak wyjątkiem potwierdzającym regułę, a nie zwiastunem nowego trendu. Kryptowaluty, jeśli faktycznie będą się rozwijały, to mimo, a nie dzięki wysiłkom rządów i regulatorów. Możliwość śledzenia przepływu pieniądza jest istotnym sposobem walki z przestępczością, również w wymiarze ponadnarodowym. Wspierając kryptowaluty rządy i organizacje ponadnarodowe pozbyłyby się potężnego narzędzia kontroli, jakim jest możliwość śledzenie przepływu pieniędzy. Raz zdobywszy takie narzędzie, administracja z pewnością tak łatwo się go nie wyrzeknie.

Są też przypadki, kiedy rozwój alternatywnych systemów płatniczych stymulowany jest nie przez dążenie do anonimowości, a przez słabość systemu bankowego. Przykładem są państwa afrykańskie, które w obszarze płatności „przeskoczyły" swoje zapóźnienie, dołączając do technologicznej awangardy, a wręcz ją tworząc. Mobilny pieniądz funkcjonuje tam niemal równolegle do waluty oficjalnej. Najbardziej znanym przykładem jest tu M-Pesa, system stworzony przez rząd kenijski i Vodafone. Do zainicjowania transakcji wykorzystuje on technologie SMS, a jako autoryzacji używa numeru telefonu oraz PIN.

Powyższe przykłady są interesujące, niemniej jednak przy dobrze rozwiniętym, konkurencyjnym systemie bankowym, z dobrze rozwiniętą infrastrukturą teleinformatyczną, rachunek bankowy jawi się jednak jako najbardziej prawdopodobne źródło pieniądza. Bez względu na to jaki model biznesowy rynku płatniczego ostatecznie ukształtuje się po wejściu PSD2. Szczególnie, że dostęp do niego dostaną podmioty trzecie.

Podmioty pośredniczące w procesie płatności

To, kto będzie organizował systemy płatności oraz kto będzie pośredniczył w rynku płatniczym jest wypadkową działań regulatora oraz zachowań konsumenckich klientów.

Klienci chcą wygody i dopasowania usługi do swoich potrzeb. Regulatorzy – większej konkurencji, dopływu nowych technologii, stymulacji rozwoju wymiany gospodarczej. Przyszłością płatności będzie zatem multistandardowość.

Oznacza ona, że równolegle funkcjonowały będą różne rozwiązania technologiczne oferowane przez różne podmioty, czasem „rywalizujące", a czasem „uzupełniające się". Spełniać będą one różne oczekiwania, odpowiadać będą na różne potrzeby, w różnym stopniu zapewniać będą bezpieczeństwo i prywatność.

Tu warto wrócić to opisywanych wyżej polskich doświadczeń i powstania płatności typu Pay by link. Początkowo sklepy internetowe na własną rękę podpisywały umowy z bankami i integrowały się z ich systemami. Na dłuższą metę, przy gwałtownie rosnącej liczbie e-sklepów, takie rozwiązanie było nie do utrzymania, w szczególności dla banków. Pojawili się integratorzy – podmioty pośredniczące między bankami a akceptantami, dostarczający tym ostatnim gotowych, zintegrowanych z bankami rozwiązań płatniczych.

Dlatego można przewidywać, iż dalej istotna będzie rola podmiotów, które będą w stanie zintegrować wielość standardów i wystawić użytkownikowi uniwersalny, prosty w użyciu interfejs. Bo czy Jana Kowalskiego robiącego zakupy w serwisie internetowym albo opłacającego rachunek za prąd naprawdę musi interesować w jakim systemie realizowana jest ta płatność?

Wnioski dla Polski

Polski model organizacji rynku płatniczego, jaki mamy obecnie, pod wieloma względami może być wzorem dla innych państw. Technologicznie wyprzedamy inne rynki, nawet zachodnioeuropejskie. Wystarczy wspomnieć takie rozwiązania jak Pay by link, autoryzację biometryczną, przelewy na telefon, czy przelewy natychmiastowe.

Polski model rozwoju technologii płatniczych oparty jest z jednej strony na współpracy firm technologicznych z bankami, z drugiej zaś na konkurencji między dostawcami technologii. W efekcie wszystkie te rozwiązania, o których zachodni konsumenci dopiero się dowiadują, u nas wykorzystywane są od lat.

W najbliższym czasie ta sytuacja może ulec zmianie. Już dziś zagraniczni dostawcy oferują narzędzia płatnicze – tanie i wygodne – stworzone i działające „w duchu PSD2", w oparciu o rachunki bankowe jako źródło pieniądza. Nie pytają przy tym o zgodę banków, ani nie zwracają specjalnej uwag na rekomendacje naszego polskiego regulatora – KNF.

W takiej perspektywie rysują się dwa scenariusze dla polskiego rynku płatniczego. Pierwszy to ostre wejście na rynek nowych graczy – technologicznych gigantów dysponujących lubianą przez klientów marką, zasięgiem swoich urządzeń i systemów operacyjnych, a także nowych FinTech-owych firm, których tak bardzo obawiają się banki zachodnie.

W takim układzie banki zostaną zmarginalizowane do dostarczyciela pieniądza, stracą tym samym źródło dochodu jaki obecnie czerpią z obsługi płatności. Natomiast polscy pośrednicy będą musieli dostosować się do nowych warunków i ostrej konkurencji ze światowymi liderami. Konkurencja ta może być również bodźcem do rozwoju i oferowania swoich rozwiązań na szerokim rynku europejskim.

Drugi scenariusz to wyłonienie się modelu płatności w oparciu o współpracę banków i dostawców rozwiązań płatniczych – integratorów. Za tym rozwiązaniem przemawia tradycja współpracy i przyzwyczajenie konsumentów, a także dobre zaplecze technologiczne. Narzędzia płatnicze, zaoferowane rynkowi przez tę naturalną koalicję, muszą być jednak równie wygodne jak te proponowane przez zagraniczną konkurencję, a ich używanie musi być konkurencyjne cenowo.

Piotr Pinchinat-Miernik
Dyrektor Biura Projektów Strategicznych Banku Pekao S.A.
Odpowiedzialny za wdrażanie nowoczesnych produktów bankowych, w tym rozwój biznesu w obszarze współpracy z polskimi i zagranicznymi klientami Banku Pekao SA.
Ukończył Politechnikę Warszawską z tytułem Magistra Inżyniera Informatyki oraz uzyskał tytuł EMBA University of Illinois at Urbana-Champaign.
Karierę w bankowości rozpoczął w Raiffeisen Bank Polska, gdzie zajmował się wdrażaniem nowoczesnych kanałów komunikacji dla Klientów indywidualnych oraz firm. Następnie dołączył do kadry kierowniczej Banku Pekao SA, gdzie powierzono mu zarządzanie bankowością elektroniczną dla firm z obszaru średnich i dużych korporacji.
Należy do Komitetu Bankowości Elektronicznej przy Związku Banków Polskich. Od 2014 r. przewodzi pracom Forum ds. e-Faktury i e-Opłat przy ZBP.

Paweł Mucha
Główny Specjalista w Biurze Produktów Bankowości Elektronicznej Banku Pekao SA, odpowiedzialny za rozwój i wdrażanie nowych produktów bankowych na platformie internetowej PekaoBiznes24.
Z wykształcenia specjalista automatyki przemysłowej i informatyki. Karierę w bankowości rozpoczął w Powszechnym Banku Kredytowym, gdzie zajmował się wdrażaniem rozwiązań informatycznych, następnie pracował w Banku BPH i obecnie w Pekao SA, w zespole zajmującym się wdrażaniem i rozwojem systemów bankowości elektronicznej dla firm z obszaru średnich i dużych korporacji. Od 2014 r. uczestnik prac Forum ds. e-Faktury i e-Opłat przy Związku Banków Polskich.

Artur Wojtczuk
Dyrektor Linii biznesowej płatności internetowe KIR S.A.
W Krajowej Izbie Rozliczeniowej S.A. odpowiada za rozwój usługi prezentacji i płatności rachunków Invoobill oraz usługi płatności internetowych Paybynet. Ukończył Informatykę na Politechnice Łódzkiej oraz Zarządzanie projektami na Uniwersytecie Warszawskim. Przed dołączeniem do KIR w 2007 r. przez 6 lat związany z branżą IT. W latach 2001-2004 pracował jako Konsultant ds. technicznych w spółce Ster-Projekt S.A., a następnie w latach 2004–2007 w Action S.A. jako Product Manager. Prywatnie pasjonat motoryzacji oraz szeroko rozumianych nowych technologii.

Krzysztof Pycia
Ekspert w Obszarze Usług Kartowych i Internetowych KIR S.A.
Od 2009 r. w Krajowej Izbie Rozliczeniowej S.A. Aktywnie uczestniczy w rozwoju nowych produktów płatniczych. Przed dołączeniem do KIR przez blisko 9 lat był konsultantem i menedżerem w dziale doradztwa strategicznego Deloitte. Wcześniej pracował w Banku Pekao SA oraz w Szkole Głównej Handlowej w Warszawie. Zaangażowany w prace sektora bankowego mające na celu rozwój obrotu bezgotówkowego.

Piotr Pinchinat-Miernik, Paweł Mucha, Bank Pekao S.A.
Artur Wojtczuk, Krzysztof Pycia, KIR S.A.

Bankowa rewolucja na rynku płatności zobowiązań

Czy mam uregulowane wszystkie rachunki, które były do zapłacenia w tym miesiącu? Do kiedy należy zapłacić za użytkowanie garażu? Czy nie zalegam z opłatami, o których nie pamiętam?

Te lub podobne pytania nurtują co miesiąc każdego z nas. Z odpowiedzią na nie radzimy sobie na różne sposoby. Niektórzy korzystają z Polecenia Zapłaty, inni prowadzą rejestr płatności w kalendarzu lub w komputerze, jeszcze inni cyklicznie logują się do kilku portali, aby w każdym z nich zweryfikować swoje zobowiązania…

Tymczasem właśnie teraz powstaje nowy międzybankowy system opłacania zobowiązań, który uczyni proces monitorowania i dokonywania płatności łatwym i przyjemnym. System pozwoli nam w jednym miejscu sprawdzić, jakie zobowiązania aktualnie czekają na uiszczenie i podjąć szybką decyzję, co i kiedy ma zostać opłacone.

Wstęp

Żyjemy w czasach powszechnego dostępu do lawinowo rosnącej liczby usług, z których w coraz większym stopniu korzystamy. Są to nie tylko usługi zapewniające podstawowe potrzeby bytowe: czynsz, woda, prąd, gaz, ale i szczególnie szybko rozwijające się usługi telekomunikacyjne i informatyczne: telewizja kablowa i satelitarna, Internet, dostęp do płatnych usług internetowych, przechowywania zasobów, coraz bardziej powszechne abonamenty na oprogramowanie oraz usługi ubezpieczeniowe i edukacyjne. Generuje to

dużą liczbę stałych płatności, do uiszczania których jesteśmy zobligowani, a które chcielibyśmy regulować łatwo i szybko, mając wgląd w szczegóły tych zobowiązań. Usługodawcy także poszukują wygodnego i pewnego sposobu dostarczenia do odbiorców informacji o zobowiązaniach, aby zapewnić sobie terminowy spływ i jednoznaczną identyfikację należności.

Postępująca cyfryzacja administracji publicznej rodzi potrzebę kontaktu z obywatelami za pośrednictwem kanałów elektronicznych, zarówno w celu przekazywania informacji o zobowiązaniach (podatki lokalne, opłaty za wywóz śmieci, opłaty jednorazowe), jak również dostarczania innych dokumentów i ważnych informacji.

W Polsce jest 14,5 mln[1] aktywnych użytkowników bankowości internetowej. Dostęp tak wielu osób do zabezpieczonego kanału elektronicznego warto wykorzystać z jednej strony do przekazywania informacji o zobowiązaniach, a z drugiej do i dokonywania na ich podstawie płatności online. Mechanizm ten może być użyty również do bezpiecznej dystrybucji dokumentów.

Krótka historia upraszczania procesu opłacania zobowiązań

Płacenie rachunków to mało przyjemny obowiązek, choć możliwe, że podświadomie młodzi ludzie chcą płacić swoje rachunki, bo to oznacza samodzielność.

O ile opłacenie pierwszego czynszu czy rachunku za energię elektryczną może dawać satysfakcję, to w praktyce każdy kolejny to już obowiązek.

I nie jest to tylko konieczność zapewnienia środków na pokrycie zobowiązań, ale także potrzeba zrealizowania płatności, najlepiej szybko i wygodnie.

Kiedyś – przede wszystkim gotówka

Historycznie płaciliśmy za rachunki głównie w kasie wystawcy rachunku lub na poczcie.

Tak czy inaczej – gotówką. A poza spacerem lub „wycieczką" w celu wniesienia opłat często konieczne było stanie w kolejce. I, niestety, zła pogoda nie przesuwała terminu płatności zobowiązań.

Dodatkowo, o ile wpłata w kasie nie generowała dodatkowych opłat, o tyle na poczcie stawki za dokonanie przekazu nie były niskie.

1 Źródło: ZBP, Raport NetB@nk za IV kw. 2015 r.

Jeszcze na początku lat 90. również płatności bankowych dokonywaliśmy zwykle podczas osobistej wizyty w placówce. Niektórzy klienci korzystali z usług takich jak opłacanie rachunków przez bank (faktury przychodziły na adres banku i pracownik tej instytucji opłacał je w imieniu klienta), ale usługa ta nigdy nie była wykorzystywana masowo i siłą rzeczy była droga w obsłudze.

Z perspektywy całego rynku płatność rachunków była mało wygodna i droga, tak dla konsumentów (opłaty pocztowe, koszty dojazdu oraz czas poświęcony na dokonanie płatności), jak i wystawców faktur (koszty utrzymania punktów przyjmowania wpłat, wysokie koszty rozliczania wpłat).

Kanały zdalne – rewolucja w płatnościach

Rozwój kanałów zdalnych, początkowo bankowości telefonicznej, a później internetowej dał możliwość prostego zlecania płatności bez konieczności wizyty w banku, na poczcie czy w kasie wystawcy.

Nawet każdorazowe podanie całego numeru rachunku i danych odbiorcy (np. w bankowości telefonicznej) było prostsze i szybsze niż „wyjście" z domu w celu uiszczenia należności.

Prawdziwy przełom przyniósł jednak rozwój bankowości internetowej, która umożliwiła składanie zleceń przelewów drogą elektroniczną. W połączeniu z możliwością definiowania odbiorców oraz składania zleceń stałych dokonywanie opłat stało się jeszcze prostsze. Dziś prostotę przelewów internetowych uzupełniają smartfony – w bankowości mobilnej akceptacja płatności jest jeszcze wygodniejsza i szybsza.

Jednocześnie upowszechnienie systemów płatności masowych w bankach sprawiło, że coraz więcej klientów posiada indywidualnie dedykowane numery rachunków. Wyeliminowało to konieczność każdorazowego wpisywania tytułu polecenia przelewu i zminimalizowało ryzyko błędu.

Warto podkreślić, że mamy w Polsce 14,5 mln aktywnych użytkowników bankowości internetowej (osób logujących się do systemu co najmniej raz w miesiącu). Osoby te cenią sobie wygodę zdalnego dostępu do banku i tym samym stanowią dużą bazę potencjalnych użytkowników kolejnych innowacyjnych rozwiązań.

Polecenie zapłaty

Polecenie zapłaty, pomimo wielu zalet, nie jest w Polsce popularne. Dziś to zaledwie średnio 0,6 transakcji na mieszkańca rocznie i statystyka ta jest stabilna na przestrzeni ostatnich lat. Dla porównania[2], średnia w Strefie Euro w 2014 r. wyniosła 52 transakcje polecenia zapłaty na mieszkańca, a w Niemczech – które są najbardziej aktywnym pod tym względem krajem – aż 105.

Choć nie ma dziś w Polsce perspektyw na taki rozwój polecenia zapłaty, to jest potencjał dla innych form bezgotówkowych płatności zobowiązań.

Szybkość płatności

Równie istotna, co wygoda, jest szybkość realizacji zlecenia przelewu – obecnie płatność jest przesyłana do odbiorcy zwykle tego samego dnia. Zaś każdy przelew z datą realizacji w przyszłości jest wykonywany (w miarę dostępności środków na rachunku) w ustalonym dniu i tego samego dnia pieniądze są dostępne na koncie odbiorcy.

W przypadku pilnych płatności można skorzystać z przelewów natychmiastowych, coraz częściej dostępnych w bankach. Klient ma wówczas pewność nie tylko zlecenia płatności, ale i jej natychmiastowej realizacji i dostępności środków u wierzyciela.

W poszukiwaniu prostoty płatności

Invoobill

Bankową inicjatywą, mającą na celu popularyzację automatyzacji płacenia rachunków, jest usługa Invoobill (początkowo pod nazwą Bilix). Jest to tzw. usługa EBPP (Electronic Bill Presentment and Payment) polegająca na prezentacji i płatności rachunków za usługi świadczone klientom w banku.

Płatność jest autoryzowana i realizowana „jednym kliknięciem" dzięki przygotowanym przez system, gotowym do zaakceptowania przelewom w bankowości internetowej (lub mobilnej). Klient nie musi sam wpisywać numeru rachunku bankowego i danych przelewu. Invoobill eliminuje papierowe rachunki i faktury z obrotu pomiędzy dostawcami a odbiorcami usług. Użytkownicy zyskują czas i wygodę przy opłacaniu rachunków i faktur, które otrzymują w postaci elektronicznej.

2 Źródło: Dane ECB

System ten pozwala klientom na wydanie dostawcy usług dyspozycji przekazywania faktur (lub tylko żądań płatności) do swojego banku. Klient sam decyduje kiedy (i czy) daną fakturę opłaci. Usługa jest dostępna dla ponad 90% klientów banków. Pomimo kilku lat istnienia na rynku nie stała się jeszcze powszechna wśród wystawców faktur. Jej wprowadzenie zbiegło się bowiem z masowym wdrażaniem nowoczesnych systemów eBOK.

Ze względu na duży potencjał usługa jest obecnie gruntownie przebudowywana. W wyniku prac ZBP z udziałem KIR i banków opracowano nowe zasady jej działania, opisane w dalszej części artykułu.

Kody QR

Kolejną możliwością jest oznaczanie faktur kodami kreskowymi i kodami QR, które są łatwo odczytywane przez aplikacje mobilne. Dzięki temu dane do przelewu można pobrać poprzez proste zeskanowanie faktury, bez konieczności ich przepisywania.

Od kilkunastu lat w polskim systemie bankowym istnieją rozwiązania kodowania informacji istotnych z punktu widzenia realizacji przelewu bankowego w formie kodu kreskowego. Kod QR może być jego naturalnym następcą odpowiadającym na potrzeby rozwijającego się rynku technologii mobilnych.

W celu upowszechnienia kodów QR powstała grupa robocza przy ZBP, która opracowała rekomendację w sprawie przyjęcia w Polsce standardu specyfikacji kodu dwuwymiarowego. Dzięki temu został ustalony standard zawartości kodu QR, z którego korzystają banki wdrażające tę usługę oraz kolejni wystawcy, którzy decydują się na umieszczanie kodu QR z danymi płatności na fakturach lub rachunkach.

Kody QR mogą być wykorzystywane do adresowania dowolnych przelewów, nie tylko płatności rachunków. Warto podkreślić, że zeskanowane dane odbiorcy przelewu mogą być także zapisane pod postacią zlecenia stałego lub jako zdefiniowany odbiorca w bankowości elektronicznej, co pozwala uniknąć ponownego wprowadzenia ich danych.

Kody QR są też wykorzystywane w systemie płatności mobilnych PeoPay oraz w pozabankowych aplikacjach mobilnych służących do opłacania faktur.

Niezależne platformy internetowe i mobilne

Faktury można opłacać z różnych niebankowych platform mobilnych oraz internetowych. Przykładem dedykowanej platformy mobilnej jest Sprytny Bill.

Usługa ta wymaga używania osobnego programu, co wydaje się mniej wygodne niż płacenie za pomocą posiadanej bankowości mobilnej. W praktyce sama usługa reklamuje się jako gadżet dający możliwość zarabiania na programach lojalnościowych banków. Dodatkową atrakcją może być ewentualny darmowy kredyt w przypadku korzystania z karty kredytowej, przy czym należy oszacować czy związane z tym korzyści nie zostaną skonsumowane przez koszty obsługi transakcji. Z kolei przykładami platform internetowych są BM.pl oraz rachunki.przelewy24.pl. Portale te w imieniu klienta ściągają z eBOK dane o płatnościach (klient musi podać dane logowania, a faktury można pobierać tylko od ograniczonej liczby podmiotów). Płatność może być regulowana automatycznie w ciężar karty płatniczej, a w przypadku płatności inicjowanej ręcznie także poprzez mechanizm paybylink. Zaletą jest automatyzacja pobierania danych o płatności, przy czym wiąże się ona z oddaniem (przekazaniem) pełnego dostępu do danych i części zleceń dostępnych w eBOK u danego wierzyciela, a nie tylko do faktur.

Płacenie rachunków przy okazji tradycyjnych zakupów

Przykładem jest usługa „Wygodne rachunki" oferowana przez Bank Pekao (dostępna m.in. w sieci sklepów Żabka pod nazwą „Zielone Okienko") oraz podobne usługi takie jak „VIA™ – Moje Rachunki" czy PayTel.

Szczegóły płatności są skanowane z rachunku. Usługi są płatne i konkurencyjne cenowo do opłat pocztowych, zaś w porównaniu do płatności kanałami zdalnymi – relatywnie drogie. Ich głównym atutem jest oszczędność czasu wynikająca z płacenia rachunków, gdy już stoimy przy kasie w sklepie.

Bezpośrednio w eBOK – karta lub paybylink

Płatności typu paybylink są dostępne bezpośrednio w wielu elektronicznych biurach obsługi klienta (eBOK). Jeśli klient korzysta z eBOKa, to jest przydatna usługa dodana. Wydaje się jednak, że w praktyce (gdy kwota płatności jest w oczekiwanej wysokości) klient właściwie nie ma potrzeby ani widzieć faktury ani mieć dostępu do pełnego eBOK. Co więcej, niektóre mechanizmy, takie jak wysyłka e-maila z linkiem do płatności, o ile są bezpieczne przy pojedynczych zakupach (klient właśnie nabył coś w sieci, dostaje jeden e-mail z potwierdzeniem zamówienia i linkiem do płatności), to w przypadku opłat cyklicznych niosą ze sobą ryzyko nadużyć (relatywnie łatwo przesłać fałszywy link prowadzący do innej płatności).

Najnowsze rozwiązanie, czyli wszystko w jednym miejscu – w banku

Inicjatywa banków, KIR i ZBP

Na bazie rozwiązania Invoobill banki, wspólnie z ZPB i KIR, postanowiły wypracować model usługi nowej generacji. Celem prac było stworzenie mechanizmu maksymalnie prostego dla klienta i jednocześnie łatwego w implementacji u wierzycieli.

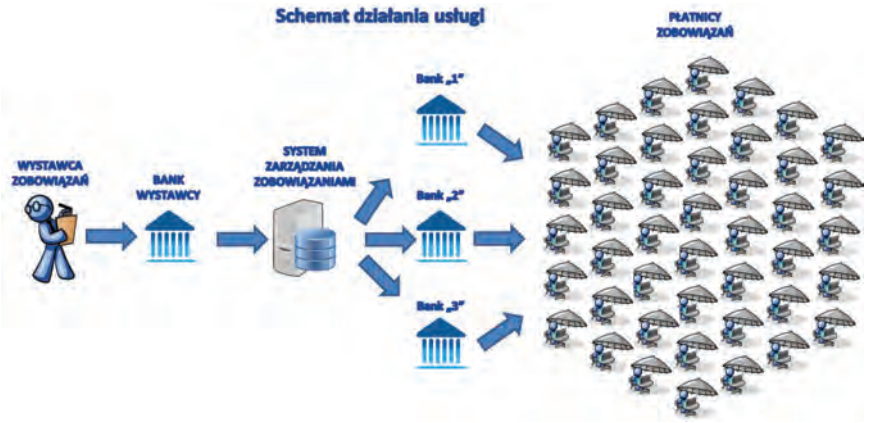
Zainteresowanie wierzycieli nowością jest bardzo duże. Można się zatem spodziewać, że liczba wystawców w nowym systemie już „na starcie" będzie większa niż liczba podmiotów dostępnych w dotychczasowych usługach prezentacji i płatności faktur.

Szybko i wygodnie

Klient będzie musiał tylko raz wyrazić zgodę na korzystanie z nowej usługi w swoim banku. Sposób wyrażania zgody leży w gestii banku (domyślnie w bankowości internetowej, przy czym w przyszłości można oczekiwać, że będzie to jedna ze zgód wyrażana już przy otwieraniu rachunku). Dzięki temu klient będzie widział w swojej bankowości elektronicznej faktury od wszystkich wystawców korzystających z nowej metody płatności zobowiązań.

Jednocześnie banki będą oferować wystawcom tę usługę jako część systemów płatności masowych, co uczyni wdrożenie bardzo prostym. Samo żądanie płatności będzie kolejną opcją dostępną obok dzisiejszego polecenia zapłaty. Jednocześnie wystawca faktur będzie mógł przekazywać komplet danych, które będą udostępniane tylko w przypadku zgody klienta na tę usługę.

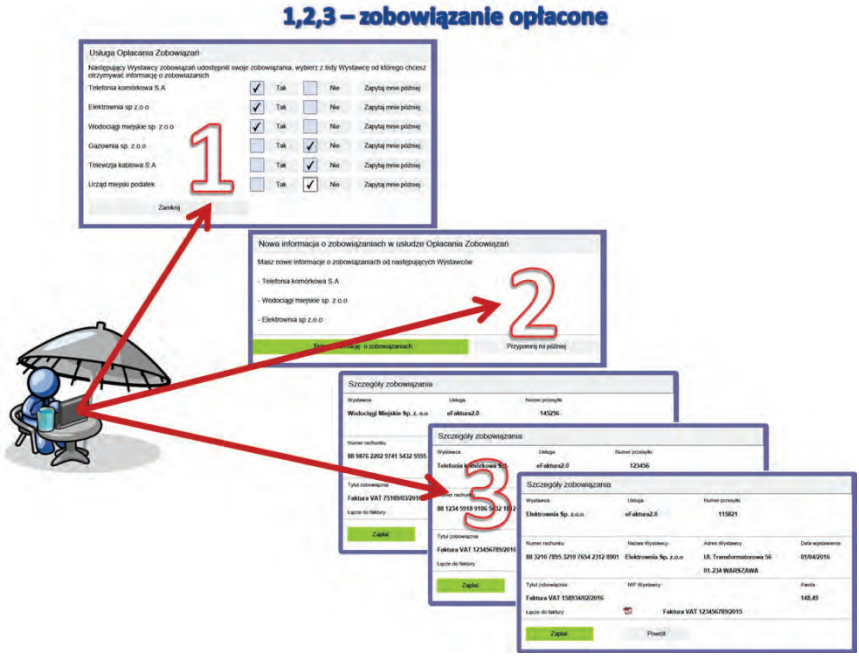
Faktury będą adresowane poprzez unikatowe identyfikatory. W przypadku konsumentów będzie to numer PESEL, dzięki czemu klient indywidualny będzie mógł zobaczyć w bankowości elektronicznej wszystkie rachunki i faktury, które ma do opłacenia.



Korzyści dla klienta indywidualnego

- Pełna obsługa płatności zobowiązań w bankowości elektronicznej (co najmniej w systemie internetowym, a – zależnie od banku – również w innych kanałach, także w mobilnym).
- Swoboda decyzji konsumenta o zapłaceniu zobowiązań i pewność poprawnie wprowadzonych danych przelewu.
- Możliwość dostępu do faktur w postaci elektronicznej.
- Możliwość uregulowania płatności z więcej niż jednego banku (o ile klient posiada wiele rachunków i w wielu bankach wyraził stosowną zgodę).
- Proste przystąpienie do usługi poprzez wyrażanie jednorazowej zgody.
- Automatyczne przyrastanie liczby wystawców dostępnych w systemie, bez konieczności osobnej zgody klienta na każdego wierzyciela.
- Szansa na upowszechnienie indywidualnych numerów rachunków u mniejszych wystawców faktur.

Podsumowując, nowa usługa jest prosta i wygodna dla klienta zarówno na etapie uruchamiania, jak i późniejszego dokonywania płatności zobowiązań. Zaś baza wystawców faktur, które można opłacać tą metodą rozrasta się bez interwencji klienta.



Korzyści dla wierzycieli

- Łatwa integracja z bankiem poprzez wykorzystanie systemów płatności masowych, powszechnych u dużych wystawców oraz coraz popularniejszych u mniejszych wystawców faktur lub innych zobowiązań (np. spółdzielni mieszkaniowych).
- Możliwość przesyłania zarówno żądań płatności, jak i faktur.
- Spodziewane duże wykorzystanie usługi przez klientów indywidualnych ze względu na łatwą aktywację, a tym samym potencjalnie duży strumień płatności spływających tym kanałem.
- Poprawa terminowości wpływu należnych opłat dzięki bezpośredniemu przekazywaniu żądań płatności (opcjonalnie wraz z fakturami) do banku klienta.
- Zwiększenie satysfakcji i lojalności klientów indywidualnych – odbiorców usług wierzyciela.
- Niższe koszty operacyjne rozliczania wpłat w przypadku małych wystawców, którzy dotąd nie korzystali z systemów płatności masowych.

Podsumowując, uruchomienie usługi jest proste zwłaszcza w przypadku wierzycieli posiadających systemy płatności masowych, a podmiotom, które dotychczas nie korzystały z takich systemów zapewni realny spadek kosztów rozliczania płatności. Wszystkim wystawcom usługa ułatwi zarządzanie należnościami i poprawi terminowość spływu opłat.

Korzyści dla banków

- Wzrost zadowolenia klientów – płatników.
- Wzrost zadowolenia klientów – wystawców faktur.
- Dodatkowe przychody generowane zarówno z usługi dla wystawców, jak i od płatników w związku z korzystaniem z usług dodatkowych, takich jak np. automatyczne opłacanie faktur do ustalonej kwoty raz w miesiącu.
- Większa wiedza o kliencie.
- Wsparcie sprzedaży systemów masowych mniejszym wystawcom faktur.

Podsumowując, unowocześniona usługa przekłada się na zadowolenie klientów banku, sprzyja kreowaniu nowych produktów i generuje wpływy.

Co dalej?

Nowa platforma KIR jest elastyczna i uniwersalna, co oznacza, że może obsłużyć dowolne unikatowe identyfikatory, a co za tym idzie – różne usługi. Na początku priorytetem będzie rozwój i promocja usługi płatności faktur dla konsumentów (B2C). Z czasem zakres obsługiwanych produktów będzie rozszerzany o płatności B2B, G2C, G2B.

Płatności B2B

Żądania płatności będą mogły być przekazywane nie tylko między wystawcami a konsumentami, ale także do firm posługujących numerem NIP jako identyfikatorem.

Oznacza to, że dostosowaniu będą musiały podlegać nie tylko kanały internetowe czy mobilne, ale także interfejsy bankowości korporacyjnej, tak aby nowe możliwości pojawiły się bezpośrednio w połączonych z bankami systemach księgowych firm.

To rozwiązanie jest szansą na uproszczenie elektronizacji faktur. Docelowo powinno pozwolić na przesyłanie między dowolnymi firmami nie tylko faktur za rozliczenia okresowe (np. za media), ale również za bieżące rozliczenia operacyjne.

Płatności G2C oraz G2B
W przyszłości usługa może usprawnić relacje obywateli i firm z administracją publiczną. Żądania zapłaty mogłyby dotyczyć np. podatków okresowych czy pojedynczych opłat.

Otwartość na różne standardy faktur
Nowa usługa może obsługiwać różne standardy faktur, w szczególności będzie uwzględniać standard efaktury, który ma zostać przyjęty jako obowiązujący w relacjach firm z administracją publiczną w ramach cyfryzacji administracji.

Usługa nowej generacji ma potencjał, by zrewolucjonizować polski rynek płatności zobowiązań. Im więcej wystawców i płatników z niej skorzysta, tym proces wzajemnych rozliczeń będzie dla nich łatwiejszy i bardziej efektywny.

Andrzej Kawiński

Country Manager Banknote Processing w firmie Giesecke & Devrient GmbH od 1 marca 2014 r., gdzie odpowiada za Polskę i kraje skandynawskie.

Absolwent Politechniki Warszawskiej i Automatyki Procesow Technologicznych. W 2005 r. ukończył studia Executive MBA w Gdańskiej Fundacji Kształcenia Menedżerów we współpracy z Rotterdam School of Management i Uniwersytetem Gdańskim.

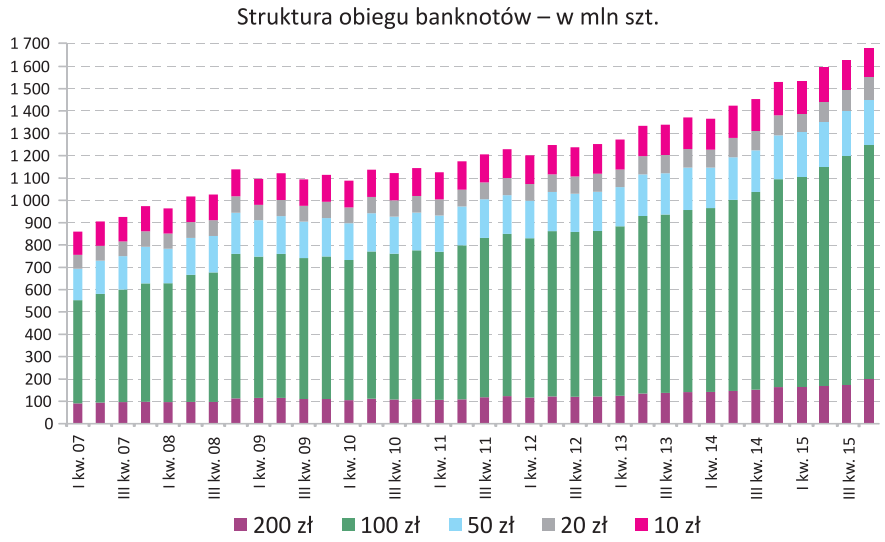
Zawodowo związany z branżą nowoczesnych technologii i systemów bankowych zapewniających automatyzację usług i bezpieczeństwo obrotu gotówki w sektorze bankowym oraz handlu. Promotor nowoczesnych rozwiązań w sektorze płatności bezgotówkowych i mobilnych. W przeszłości zarządzał firmami Wincor Nixdorf, Siemens Nixdorf, IMPAQ.

Założyciel Instytutu Analiz i Prognoz Rynkowych. W latach 2007-2013 piastował stanowisko Przewodniczącego Forum Technologii Bankowych w Związku Bankow Polskich. Przewodniczący Rady Programowej konferencji „IT w Instytucjach Finansowych", organizowanych przez Gdańską Akademię Bankową.

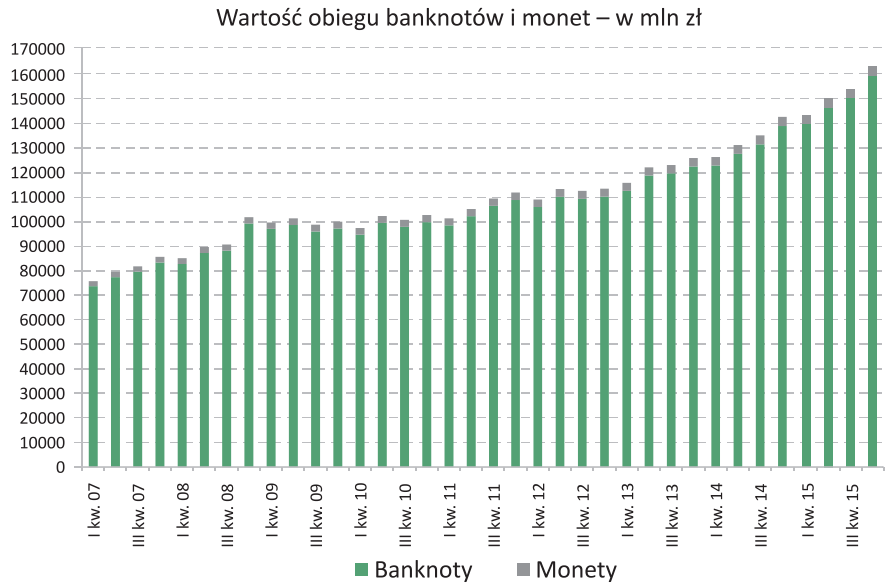
Andrzej Kawiński, Giesecke & Devrient GmbH

Jak obniżyć koszty obrotu gotówki?

Od czasu wynalezienia gotówki przez Fenicjan w VII w p.n.e. ta forma płatności w dalszym ciągu cieszy się dużo popularnością w obecnych czasach. Światowe statystyki pokazują że rokrocznie poziom gotówki znajdującej się w obrocie wzrasta. Również Narodowy Bank Polski w oficjalnie publikowanych statystykach podaje, że na koniec roku 2015 liczba sztuk banknotów znajdujących się w obiegu wzrosła o 11,67% w stosunku do liczby banknotów będących w obiegu na koniec roku 2014.



Wartościowo wzrost ten wynosi 14,39%.



Gotówka dla banku oznacza koszty związane z jej przeliczaniem, przechowywaniem oraz transportem. Wprowadzony w ostatnich miesiącach podatek bankowy liczony od aktywów, w którego skład wchodzi gotówka, dodatkowo podnosi koszty związane z obrotem gotówkowym. Instytucje finansowe ograniczając koszty od wielu lat promują inne formy płatności (przelewy, płatności kartowe, mobilne), które ze swoje natury charakteryzują się niskim kosztem albo generują dla banku dodatkowe przychody. Analizy pokazują, że w Polsce najbardziej popularną formą płatności pozostaje gotówka. Według badania TNS Polska, aż 53% Polaków za zakupy spożywcze płaci wyłącznie gotówką a tylko 3% wyłącznie kartą. Nawet w kanale internetowym, e-commerce, gdzie naturalnym wydaje się korzystanie z płatności elektronicznych, aż 51% badanych zadeklarowało płatność gotówką przy odbiorze towaru (Badania ICAN Research na zlecenie Blue Media).

W krajach skandynawskich, nazywanych często *cashless society*, gotówka w dalszym ciągu jest istotną alternatywą do płatności kartowych. W czasie konferencji zorganizowanej przez Ministerstwo Rozwoju w marcu 2016 r. – „Obrót bezgotówkowy – Polska vs. Szwecja 20:80", Eric Lenntorp ze szwedzkiego Riksbanku (Szwedzki Bank Centralny) podkreślił, że zbyt szybki rozwój transakcji bezgotówkowych w Szwecji jest problemem. Według Riksbank w Szwecji są miejsca, gdzie dostępność gotówki i możliwości jej zdeponowa-

nia jest ograniczona, co ogranicza prawa obywatelskie. W przeciwieństwie do innych krajów, szwedzkie placówki handlowe nie mają obowiązku stosowania obrotu gotówkowego. Bank Centralny Szwecji zastanawia się nad działaniami, które umożliwią każdemu obywatelowi wybór sposobu płatności.

Obecny niski poziom stóp procentowych powoduje zwiększenie poziomów gotówki przechowywanej w banku. Analitycy prognozują że w najbliższych latach stopy procentowe zostaną podniesione. Dlatego warto się już teraz zastanowić, w jaki sposób ograniczyć koszty obrotu gotówki.

Polski rynek obrotu gotówki, charakteryzujący się wysokim poziomem outsourcingu w zakresie liczenia wartości, w porównaniu do innych rynków europejskich, również centralnej i wschodniej Europy, jest regulacyjnie i technologicznie opóźniony. W niniejszym opracowaniu postaram się przedstawić doświadczenia i najlepsze praktyki stosowane przez inne kraje europejskie w optymalizacji procesów obrotu gotówki, szczególnie w zakresie ograniczenia kosztów transportu i tak zwanego recyclingu gotówki w sortowniach.

Historia gotówki

Twórcami pieniądza w znanej nam dzisiaj postaci byli prawdopodobnie Fenicjanie i miało to miejsce w VII w p.n.e. W tamtych czasach Fenicjanie prowadzili działalność handlową z wszystkim krajami ówczesnej cywilizacji. Wprowadzone przez nich paramonety umożliwiały zastąpienie skomplikowanego handlu barterowego na dużo prostszą formę pieniądza. Wynalazek pieniędzy usprawnił wykonywanie transakcji handlowych. Niezależnie od formy wykonywania płatności, łatwość regulowania zobowiązań jest aktualną wytyczną także w obecnych czasach. Najstarszą znalezioną monetą jest bryłka elektrum (w starożytności nazywano tak stop złota i srebra) posiadająca stempel złotnika z Efezu.

Prywatnie bite paramonety były pierwszym etapem wprowadzania monet wydawanych przez władze państwowe. Monety wynaleziono równolegle w VII w p.n.e. w państwach cywilizacji greckiej: w Lidii, położonej na zachodnich wybrzeżach Azji Mniejszej (obecnie Turcja), oraz w Argolidzie (obecnie Peloponez).

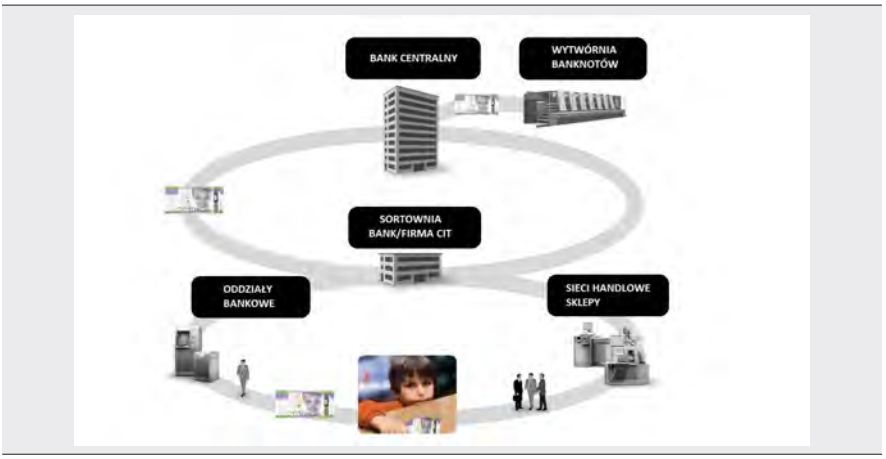
Wytwarzanie monet ze złota i srebra było bardzo kosztowne, a ilość dostępnych metali do produkcji monet nie zaspokajała potrzeb. Bezpieczeństwo przechowywania dużych ich ilości stawało się problemem, zaczęto więc za-

stawiać zasoby u złotników otrzymując jako potwierdzenie kwit depozytowy. Regulował on wzajemne zobowiązania pomiędzy złotnikiem a właścicielem monet. Z czasem kwit depozytowy stał się dokumentem, na podstawie którego złotnik wypłacał należność okazicielowi. Ludzie coraz częściej regulowali swoje zobowiązania za ich pomocą. Złotnicy, którzy stali się pierwszymi bankierami wystawiali je nie tylko potwierdzając zdeponowanie kruszców, ale również udzielając pożyczek. Odsetki od wystawionych w ten sposób kwitów depozytowych stały się dodatkowym dochodem bankierów. Wydawane kwity depozytowe zostały zatwierdzone przez Państwo i stały się przodkiem dzisiejszego pieniądza papierowego. Państwa zaczęły wydawać rozporządzenia regulujące obrót kwitami depozytowymi, jednocześnie ustanawiając bank będący emitentem kwitów. Regulacje te miały na celu likwidację chaosu powstałego przez emisję różnych banknotów indywidualnie przez każdy z banków. Z czasem banki emitujące pieniądze zostały upaństwowione, wiążąc je z centralną władzą monetarną.

Cykl obrotu gotówki w gospodarce

Typowy cykl obrotu gotówki można przedstawić za pomocą następującego schematu.

Cykl obrotu gotówki



Giesecke & Devrient

W Polsce Państwowa Wytwórnia Papierów Wartościowych (PWPW) na zlecenie Narodowego Banku Polskiego produkuje banknoty. Narodowy Bank Polski wprowadza pieniądze do obrotu zasilając banki. Większość instytucji finansowych w Polsce już od kilku lat zleca procesowanie gotówki wyspecjalizowanym firmom CIT (*Cash in Transit*). Firmy te na zlecenie banków odbierają gotówkę z Narodowego Banku Polskiego, a następnie w swoich sortowniach przygotowują zasiłki oddziałów bankowych i bankomatów. Społeczeństwo, pobierając gotówkę w oddziałach bankowych oraz bankomatach, uzyskuje środki do realizacji swoich potrzeb. Zapłata za towary powoduje przekazanie gotówki od obywateli do przedsiębiorcy będącego dostawcą towaru. Przedsiębiorcy deponują gotówkę w banku. Funkcję tę typowo świadczą firmy CIT, które na zlecenie banku odbierają gotówkę od przedsiębiorców, przeliczają wpłaty i księgują na odpowiednich kontach. Firmy CIT odbierają również gotówkę wpłaconą w oddziałach bankowych. Gotówka przeliczana w sortowniach jest dzielona na pieniądze o dobrej jakości, które mogą wrócić do ponownego obrotu w gospodarce, i destrukty, które muszą być przekazane do Narodowego Banku Polskiego. Każdego dnia banki podejmują decyzję, jaka część odebranej z rynku gotówki jest nadmiarowa i powinna być przekazana do depozytu NBP, zmniejszając w ten sposób obowiązkową rezerwę. Pozostałe środki wracają do ponownego obiegu w gospodarce (zasilenia oddziałów i bankomatów). Usługę transportu wykonują na zlecenie banków firmy CIT.

Gotówka deponowana w Narodowym Banku Polskim po przeliczeniu i sprawdzeniu jakościowym wraca ponownie do obiegu. Depozyty NBP przechowywane są przez Bank Centralny i usługa ta nie jest obecnie zlecana firmom zewnętrznym zajmującym się procesowaniem gotówki.

Recycling gotówki w sortowni

Powierzenie przez bank firmie CIT usługi liczenia gotówki uwarunkowany jest następującymi założeniami:

- właścicielem gotówki jest bank a nie firma CIT,
- firma CIT nie może mieszać gotówki jednego banku z gotówką innego,
- gotówka w sejfie jednego banku musi być fizycznie oddzielona od gotówki innego klienta.

Zwykle sortownie firm CIT obsługują kilka banków. Firmy CIT na zlecenie banków odbierają depozyty od ich klientów, które spływają równolegle do sortowni. Krótki czas przeliczenia powoduje konieczność uruchomienia kilku równoległych procesów liczenia i sortowania. Typowym rozwiązaniem w polskich sortowniach jest rozliczenie depozytu na małych stanowiskowych liczarkach a następnie układanie, dzielenie na nominały, paczkowanie i wiązkowanie banknotów na większych sorterach. Tak ustawiony proces powoduje konieczność kilkukrotnego przeliczenia każdego z banknotów na poszczególnych etapach, co przekłada się na liczbę personelu i czas pracy. Ideałem, standardowo wdrożonym na innych europejskich rynkach, jest aby banknot w sortowni tylko jeden raz był liczony w urządzeniu. Wymaganie układania banknotów zgodnie z orientacją (cztery położenia) w połączeniu z liczbą polskich nominałów (a jest ich pięć) wymaga wdrożenia dużych dwudziestokieszeniowych (4 x 5 = 20) urządzeń. Tylko takie sortery umożliwiają przeliczenie, posortowanie i ułożenie banknotów w jednym cyklu.

W zależności od potrzeb część przeliczonej w sortowni gotówki wraca na rynek w postaci zasiłków kasjerskich lub zasileń bankomatów. Reszta jest odprowadzana do Narodowego Banku Polskiego. Warto w tym miejscu podkreślić, że tylko gotówka danego banku może być użyta do zasileń bankomatów i oddziałów. Nie ma możliwości przekazania gotówki jednego banku do drugiego bezpośrednio w sortowni. Typową rynkową sytuacją jest, gdy jeden bank ma nadmiar gotówki (*cash positive*) a drugi niedomiar (*cash negative*). Nawet w sytuacji, gdy oba banki korzystają z usługi tego samego outsourcera (firmy CIT) jedyną możliwością jest fizyczne przewiezienie gotówki pierwszego banku do oddziału Narodowego Banku Polskiego a następnie w imieniu drugiego banku jej pobranie. Każde przekazanie gotówki związane jest z jej liczeniem. W powyższym przykładzie gotówka jest liczona trzykrotnie, pierwszy raz w firmie CIT przy jej przyjęciu, drugi raz w Narodowym Banku Polskim a trzeci ponownie w firmie CIT przy przygotowaniu zasileń.

Obecny sposób funkcjonowania rynku gotówki wynika z dwóch czynników:

- braku uregulowań w zakresie przechowywania depozytów Narodowego Banku Polskiego w sejfach banków,
- braku regulacji w zakresie maszynowego sprawdzania jakości obiegowej banknotów.

Europejskie standardy przechowywania depozytów Banku Centralnego

Historycznie podstawą wdrożenia modelu zewnętrznego przechowywania depozytów Banku Centralnego był kilka aspektów:

- ograniczenie kosztów transportów pomiędzy sortowniami a Bankiem Centralnym,
- zmniejszenie emisji banknotów – transporty, jak również czas potrzebny na przeliczenia powoduje konieczność dodatkowych emisji banknotów,
- bezpieczeństwo gotówki,
- ograniczenie liczby przeliczeń gotówki; każde przekazanie gotówki do innego podmiotu powoduje konieczność jej przeliczenia, liczba przeliczeń ma wpływ na jakość banknotów, a czas przeliczenia gotówki stanowi koszt obrotu gotówki w gospodarce.

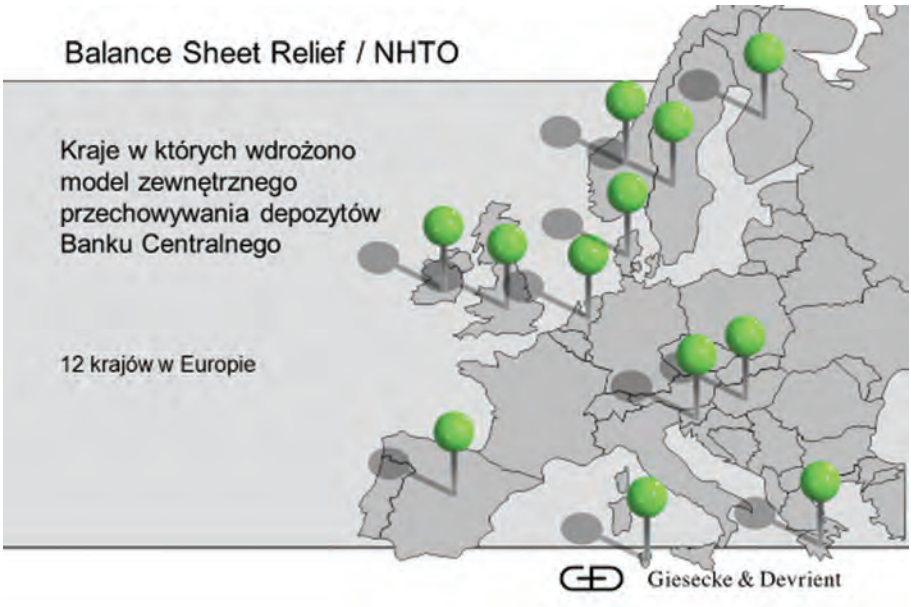
W Europie generalnie może wyróżnić dwa modele przechowywania depozytów poza skarbcami Banku Centralnego:

- model NHTO (Notes Held to Order) – Bank Centralny zezwala na przechowywanie gotówki której jest właścicielem w sejfie niebędącym własnością Banku Centralnego; gotówka ta znajduje się w bilansie Banku Centralnego,
- model depozytowy – Bank Centralny płaci odsetki za gotówkę Banku, która jest przechowywana w sejfie banku/CIT poza Bankiem Centralnym; gotówka nie znajduje się w bilansie Banku Centralnego.

Model depozytowy stosowany jest w krajach, gdzie Bank Centralny ma niedużą liczbę oddziałów a większość procesów liczenia gotówki została zlecona firmom CIT. Metoda ta jest substytutem oddziałów Banku Centralnego. Model depozytowy funkcjonuje od roku 2004 w Finlandii, gdzie Bank Centralny ze względu na duże odległości, pragnąc ograniczyć koszty transportu, wdrożył ten model.

W zależności od lokalnej polityki Banku Centralnego, występują różne warianty wskazanych wyżej modeli. Jednym ze wspólnych czynników jest regulacja zabraniająca zaliczenie banknotów znajdujących się w bankomatach czy oddziałach bankowych do depozytów Banku Centralnego. Również banknoty znajdujące się w transporcie nie mogą być do depozytów zaliczane.

Kraje, w których wdrożono jeden z modeli zewnętrznego przechowywania depozytów Banku Centralnego jest przedstawiony na poniższym rysunku.



Kolejne kraje, gdzie rozważane jest wdrożenie modelu depozytowego to: Polska, Litwa, Włochy i Portugalia.

Brak uregulowań w zakresie przechowywania depozytów Narodowego Banku Polskiego w sejfie banku lub w imieniu banku w firmie CIT może mieć wpływ na procesy w sortowniach. Sortownie firm CIT obsługując kilka banków muszą stosować zamiast jednego procesu kilka równoległych. Obecnie gotówka jednego banku fizycznie nie może być mieszana z gotówką drugiego banku. Cały proces liczenia i sortowania gotówki dla każdego z banków realizowany jest oddzielnie.

Krótkie czasy przeliczeń, wynoszące niekiedy kilka godzin, wymuszają na firmach CIT duży nakład pracy manualnej. Wolumeny gotówki wpływające do sortowi są podstawą do automatyzacji procesu i wdrożenia dużych szybkich sorterów, tak aby pieniądze liczone były tylko jeden raz. Konieczność separowania gotówki klientów utrudnia a czasami uniemożliwia taki rodzaj pracy.

Brak standardu przechowywania depozytów NBP generuje konieczność dodatkowych transportów gotówki. Koszty transportu gotówki pomiędzy sortownią a oddziałem NBP pokrywają banki. Każde przekazanie gotówki do innego podmiotu powoduje konieczność jej ponownego przeliczenia. W sytuacji deponowania gotówki przez Bank w Narodowym Banku Polskim,

gotówka (często liczona, paczkowana, wiązkowana kilka godzin wcześniej) jest ponownie liczona przez NBP. Proces ten wymaga zdjęcia banderoli z każdej paczki banknotów, przeliczenia gotówki na sorterze, założenia nowej banderoli oraz połączenia gotowych paczek w wiązki. Koszty ponownego przeliczenia są pokrywane przez Narodowy Bank Polski i są elementem kosztu obrotu gotówki w gospodarce.

Europejskie doświadczenia pokazują, że wdrożenie standardu przechowywania depozytów może mieć wpływ na zmniejszenie emisji gotówki. Konieczność dodatkowych transportów i czas potrzebny na ich przeliczanie, może wymagać dodatkowej ilości banknotów i monet. Koszty emisji są również elementem kosztu obrotu gotówki w gospodarce.

Regulacje w zakresie maszynowego sprawdzania jakości obiegowej banknotów

Jednym z zadań Narodowego Banku Polskiego jest nadzór nad jakością banknotów i monet znajdujących się w obiegu. NBP dla zapewnienia właściwej jakości banknotów wprowadzanych do obrotu i wzorując się przy tym na przepisach obowiązujących w Eurosystemie, zawartych w decyzji EBC z dnia 16 września 2010 r. w sprawie weryfikacji autentyczności i jakości obiegowej oraz powtórnego wprowadzania do obrotu banknotów euro opracował i ogłosił 4 stycznia 2015 r. rekomendowane rozwiązania w zakresie kwalifikacji jakościowej banknotów.

W rekomendacji zostały zawarte minimalne kryteria dla maszynowego oraz ręcznego sprawdzania jakości obiegowej banknotów. Rekomendacja opisuje również klasyfikacje i postępowanie z banknotami przeliczanymi lub sortowanymi zarówno w urządzeniach obsługiwanych przez klienta, jak również przez wykwalifikowany personel.

Wymieniona rekomendacja jest pierwszym tego typu dokumentem tak szczegółowo opisującym standard banknotów, które trafiają do obiegu, nie jest jednak obowiązującym przepisem. W strefie Euro, jak również w innych krajach takie regulacje obowiązują już od kilku lat. Polska jest obecnie jednym z ostatnich krajów w Europie, gdzie nie obowiązują przepisy maszynowego sprawdzania jakości obiegowej banknotów. Brak do tej pory w naszym kraju tak szczegółowych standardów powodował, że ocena stanu jakości banknotu była bardzo subiektywna i w różnych sortowniach różnie interpretowana.

Ustawienie sorterów i zdefiniowanie poziomu jakości banknotów obiegowych zależy od subiektywnej interpretacji kierownika sortowni a czasami kierownika zmiany.

Narodowy Bank Polski, realizując nadzór nad jakością banknotów znajdujących się w obiegu, przy braku wymienionych wyżej regulacji, zobowiązany jest do sprawdzania jakości w swoich sortowniach. Brak przepisów w zakresie maszynowego sprawdzania jakości banknotów jest jednym z elementów blokujących wprowadzenie standardu przechowywania depozytów NBP poza sejfem Banku Centralnego.

Sortowanie jakościowe w sortowni banku lub firmy CIT wymuszane jest selekcjonowaniem banknotów najlepszej jakości dla zasileń bankomatów. Banknoty o niskiej jakości powodują awarie urządzeń i konieczność wizyty serwisowej celem naprawy. Szczególnie wymagającym klientem w tym zakresie są podmioty oferujące wypłaty gotówki, gdzie ich przychód jest zależny od liczby transakcji. Każdy przestój urządzenia obniża poziom przychodów operatora.

Stosowane przez Narodowy Bank Polski sortery jednoznacznie maszynowo dzielą banknoty na obiegowe i destrukty. Obecnie w Polsce sortownie Narodowego Banku Polskiego są jedynym miejscem gdzie jednoznacznie odbywa się sortowanie jakościowe banknotów. Brak regulacji wymusza powrót banknotów do Banku Centralnego, bo tylko w ten sposób Narodowy Bank Polski jest w stanie kontrolować jakość banknotów znajdujących się w obrocie.

Oferowanie przez dostawców technologii urządzenia posiadają możliwość maszynowego rozdziału banknotów na obiegowe i destrukty. Brak regulacji powoduje że często urządzenia ustawiane są indywidualnie i nierzadko bywają sytuacje gdzie kierownik jednej zmiany oczekuje innego ustawienia parametrów niż kierownik zmiany kolejnej. Podział banknotów na obiegowe i destrukty jest dodatkową czynnością w sortowni, którą z reguły nie jest obciążany klient czyli bank. Zagrożenie utraty klienta (operatora bankomatów, banku) jest jednym z motywatorów wykonywania tych czynności. W Polsce, w odróżnieniu do innych europejskich krajów, banki nie ponoszą finansowych konsekwencji w wyniku wprowadzenia do obrotu zniszczonego banknotu.

Europejskim przykładem, gdzie uregulowano zagadnienie maszynowego sprawdzania jakości obiegowej banknotów są kraje skandynawskie. W Szwecji pracownicy Banku Centralnego przeprowadzają niezapowiedziane kontrole w sortowniach firm CIT. Pracownik Banku Centralnego, wyposażony w odpowiednią ilość zużytych banknotów i fałszywek, przeprowadza testy

urządzeń zainstalowanych w sortowniach. Wprowadzenie banknotu zużytego do obrotu obłożone jest wysoką karą. Firmy CIT zobowiązane są w procesie sortowania dzielić banknoty na obiegowe i destrukty. Destrukty odprowadzane są do Banku Centralnego. Bank Centralny regularnie organizuje spotkania z przedstawicielami firmy CIT, w czasie których omawiany jest poziom jakości banknotów przekazywanych do Banku Centralnego

Innym modelem, stosowanym we Francji, jest pełne wymuszenie zwrotu każdego banknotu do Banku Centralnego. Recycling gotówki w sortowni banku nie jest dozwolony. Bank Centralny w ten sposób całkowicie kontroluje jakość banknotów powracających do obiegu.

Brak w Polsce regulacji w zakresie maszynowego sprawdzania jakości obiegowej banknotów nie daje pewności, że banknoty powracające do obiegu posiadają wszystkie cechy i pełne właściwości banknotów dopuszczonych do obrotu. Istnieją, co prawda, przepisy określające nakaz wycofywania z obrotu banknotów zużytych, ale definicje poziomu zniszczenia banknotu zbyt ogólnie określają stopień zużycia, uniemożliwiając maszynowe sortowanie.

Recycling gotówki a wyzwanie informatyczne

Wdrożenie modelu przechowywania depozytów NBP poza siedzibą Banku Centralnego wymaga odpowiedniego rozwiązania teleinformatycznego. Właścicielem takiego rozwiązania jest Bank Centralny a jego użytkownikami uczestnicy rynku obrotu gotówki (firmy CIT i banki).

Głównymi cechami rozwiązania jest:

- kontrola magazynów gotówki i optymalizacja zapasów,
- zarządzanie i monitorowanie limitów gotówki,
- zarządzanie łańcuchem dostaw, w tym monitorowanie transportów,
- raportowanie stanów magazynów gotówki w każdym miejscu jej przechowywania,
- planowanie optymalnego poziomu gotówki według miejsc jej przechowywania, wartości, nominałów oraz jakości,
- planowanie emisji nowych banknotów i kontrola utylizacji banknotów zużytych,
- automatyczne zarządzanie przesunięciami gotówki celem optymalizacji jej poziomu i minimalizacji kosztów transportu,
- zarządzanie zamówieniami na gotówkę.

Przykładem takiego rozwiązania jest platforma Compass ICO firmy Giesecke & Devrient wdrożona przez Bank of Canada w roku 2013. Bank ten ze względu na znaczne odległości, ograniczając koszty transportu, wprowadził model zewnętrznego przechowywania depozytów. Wdrożony model umożliwia zarządzanie on-line magazynami gotówki i wspiera dokumentowanie oraz rozliczanie jej przesunięć. Istotnym elementem rozwiązania, który przyniósł konkretne korzyści jest moduł planowania i optymalizacji poziomu gotówki. Zarządzanie zewnętrznymi magazynami gotówki umożliwiło bankowi ograniczenie kosztów emisji nowych banknotów i zmniejszenie nakładu pracy związanego z liczeniem gotówki w sortowniach banku centralnego.

Podsumowanie

Niski poziom stóp procentowych, jak również wynegocjowane niskie stawki za odbieranie, przeliczanie i przechowywanie gotówki nie motywują instytucji finansowych do podjęcia działań celem zmniejszenia kosztów obrotu gotówki. Zagadnienie to nie jest na liście głównych priorytetów banków.

Sytuacja taka nie będzie jednak trwała wiecznie. Zgodnie z zapowiedziami Marka Belki, Prezesa Narodowego Banku Polskiego, stopy procentowe mogą w przyszłości oscylować w granicach 3% przez długie lata, a taka sytuacja zwiększa koszty gotówki w instytucjach finansowych.

Planowane przez Rząd Polski wprowadzenie minimalnej stawki godzinowej będzie miało wpływ na koszty bezpośrednie zatrudnienia konwojentów oraz liczarzy a finalnie przełoży się na wysokość stawek płaconych przez banki firmom CIT. Już obecnie znalezienie i utrzymanie pracowników przy tak niskich stawkach jest dużym wyzwaniem w sektorze.

Badania pokazują, że gotówka jest najbardziej ulubioną formą płatności w Polsce. Również klienci platform e-commerce preferują gotówkę jako formę płatności za zakupione towary. Nie wydaje się realnym radykalne obniżenie ilości gotówki w obiegu i zmiana preferencji płatniczych Polaków w najbliższych latach.

Polska jest jednym z ostatnich krajów w Europie, gdzie nie obowiązują regulacje w zakresie maszynowego sprawdzania jakości obiegowej banknotów. Prawidłowa jakość banknotów i monet jest jednym z zadań Narodowego Banku Polskiego. Brak regulacji wymusza przekazywanie gotówki do Banku Centralnego i generuje koszty transportów i przeliczania.

Zagraniczne doświadczenia pokazują, że wprowadzenie modelu zewnętrznego przechowywanie depozytów Banku Centralnego ogranicza koszty obrotu gotówkowego, w tym koszty transportu i koszty emisji. W Polsce taki model nie został wdrożony.

Obecnie, w okresie niskich stóp procentowych, banki nie widzą potrzeb ograniczania kosztów obrotu gotówkowego. Przeprowadzone w ostatnich latach przetargi na usługi transportów i przeliczeń gotówki, w wyniku wojny cenowej dostawców, dodatkowo obniżyły koszty tych usług dla instytucji finansowych. Prowadzone przez banki kampanie promocyjne płatności bezgotówkowych nie przynoszą efektu drastycznej zmiany przyzwyczajeń Polaków. Mleko się rozlało i zaczyna fermentować. Firmy CIT mają coraz większe problemy z prowadzeniem zyskownej działalności. Niskie płace w sektorze przekładają się na rotację pracowników i coraz trudniejsze ich znalezienie. Już teraz przedstawiciele sektora coraz głośniej akcentują konieczność podniesienia stawek. Podniesienie stóp procentowych przełoży się na konkretne dodatkowe koszty w bankach. Już dzisiaj należy zastanowić się nad przyszłymi scenariuszami.

Reasumując, warto już teraz podjąć działania, które dadzą możliwość optymalizacji a więc uproszczenia procesów związanych z transportem, przeliczaniem i przechowywaniem gotówki. Większy poziom automatyzacji procesów oraz zastąpienie pracy manualnej dużymi sorterami ogranicza koszty obrotu gotówkowego. Aby to osiągnąć potrzebne są wspólne działania kluczowych uczestników rynku – Narodowego Banku Polskiego, banków, firm CIT oraz dostawców technologii.

Bibliografia:

http://pl.wikipedia.org/wiki/Pieniądz

http://pieniadze.fakt.pl/pieniadze-w-historii-jak-ludzie-placili-w-dawnych-czasach,artykuly,459857,1.html

http://www.nbp.pl/home.aspx?f=/statystyka/pieniezna_i_bankowa/struktura-obiegu.html

http://wyborcza.pl/1,91446,19783059,konferencja-w-mr-w-2030-szwecja-panstwem-bezgotowkowym.html#ixzz44b9op55j

Andrzej Gibas

Dyrektor Sprzedaży do Sektora Finansowego w polskim oddziale Microsoft.

Z wykształcenia inżynier po Wydziale Elektrotechniki i Automatyki Politechniki Świętokrzyskiej w Kielcach. Ukończył studia podyplomowe w dziedzinie handlu zagranicznego w Szkole Głównej Handlowej w Warszawie oraz Client Executive Program w INSEAD w Fontainebleau, we Francji.

Od 20 lat związany z branżą informatyczną. Jego główny obszar działania to współpraca w zakresie rozwiązań informatycznych dla sektora finansowego. W latach 1999–2010 związany z IBM, gdzie pełnił m.in. funkcję Dyrektora Sektora Finansowego (2004–2009). Z kolei w latach 2010–2013 pracował na stanowisku Dyrektora ds. Sprzedaży w Oracle Polska.

W swojej działalności na rzecz sektora finansowego w Polsce pełnił m.in. funkcję Członka Prezydium Forum Technologii Bankowych przy Związku Bankow Polskich (w latach 2007–2010), był też członkiem mRady doradzającej Zarządowi pierwszego polskiego banku internetowego – mBanku (w latach 2002–2005), publikował artykuły nt. zastosowań rozwiązań informatycznych w sektorze finansowym, był uczestnikiem i organizatorem wielu branżowych konferencji.

Karol Mazurek

Managing Director, Accenture Polska.

Ukończył Wydział Fizyki Technicznej i Matematyki stosowanej na Politechnice Warszawskiej. Z firmą związany jest od 1998 roku i odpowiada za współpracę z klientami z sektora finansowego w ramach pionu Technology.

Posiada wieloletnie doświadczenie w kierowaniu dużymi i złożonymi projektami z obszarów integracji oraz architektury systemów, strategii IT oraz outsourcingu - przede wszystkim dotyczącymi wdrożeń, rozwoju i utrzymania głównych systemów dla klientów z sektora bankowego.

Andrzej Gibas, Microsoft,
Karol Mazurek, Accenture

Centralny system bankowy na nowej platformie

Na przełomie XX i XXI wieku dyrektorzy IT banków działających w Polsce otrzymywali nagrody za projekty „odmiejscowienia rachunku bankowego". Powyższe zdanie jest zupełnie niezrozumiałe dla współczesnych, najmłodszych klientów banków, realizujących przelewy bankowe za pomocą własnych telefonów komórkowych. To najlepiej pokazuje drogę w dziedzinie informatyzacji, jaką przeszedł polski sektor bankowy od początku transformacji do dzisiaj.

Już na pierwszym etapie do oddziałów banków wstawiono komputery, które automatyzowały procesy biznesowe i ułatwiały obsługę klienta. Był on jednak nadal „uwiązany" do swojego oddziału i „nie istniał" w bazie klientów pozostałych oddziałów tego samego banku. Mówiąc dzisiejszym językiem, takie „doświadczenie klienta" stało się szybko nie do zaakceptowania przez społeczeństwo, w którym transformacja systemu i gospodarka przyspieszały, a klienci banku stawali się coraz bardziej wymagający i „mobilni". Możliwość obsługi klientów w całej sieci oddziałów, a nie tylko w jednym – zwłaszcza w czasach braku dostępu do Internetu i telefonów komórkowych – dawało większe możliwości i poczucie autentycznej mobilności.

„Odmiejscowienie rachunku" to w istocie złożony projekt informatyczny, który warto było nagradzać. Wymagał przede wszystkim zapewnienia spójności i centralizacji baz danych klientów w oddziałach, czyli wprowadzenia ich unikalnych identyfikatorów, zarządzenia duplikatami rekordów i doprowadzenia do posiadania ich właściwych danych (bo wcześniej ten sam klient mógł istnieć w wielu oddziałach i mieć w nich na przykład inne dane meldunkowe), replikacji i integracji danych. Potrzebne było również zapewnienie

odpowiedniej infrastruktury teleinformatycznej, pozwalającej na dostęp do centralnej bazy oraz wprowadzenie systemów zabezpieczeń, które pozwalały na rozróżnienie uprawnień pomiędzy oddziałami. Oddzielnym wyzwaniem było zapewnienie rozliczeń między nimi, tak aby transakcje wykonane poza oddziałem właściwym klientowi były widoczne nie tylko na rachunku klienta ale też odzwierciedlone w księgach oddziału. Kolejny temat to dostęp do dokumentów, a przynajmniej wzoru podpisu – tu potrzebne było prezentowanie skanów poza oddziałem klienta.

Stan obecny i wyzwania współczesności

Kierownictwo banków bardzo szybko doszło do wniosku, że skuteczniejszym rozwiązaniem jest zbudowanie jednego, centralnego systemu bankowego, obsługującego wszystkich klientów w całej sieci oddziałów. Poza opisanym już „odmiejscowieniem rachunku" system taki charakteryzował się wieloma korzyściami:

- zapewniał spójność oferty produktowej i możliwość centralnego zarządzania ofertą,
- umożliwiał łatwiejszą implementację zmian w systemie bez potrzeby złożonych roll-outów oddziałowych,
- pozwalał na oszczędności na infrastrukturze – jeden centralny host, zamiast serwerów oddziałowych,
- zapewniał spójną, aktualną i dostępną on-line informację o kliencie i jego produktach, co dało możliwość budowy kanałów samoobsługowych.

Ten etap rozwoju organizacji i technologii znaczna część banków w Polsce ma już za sobą. Polska gospodarka, a więc i instytucje finansowe są dziś na trwałe połączona z gospodarką krajów Unii Europejskiej i dalej z globalnym obiegiem gospodarczym. Powoduje to, że również globalne trendy i wyzwania silnie oddziałują na banki operujące na polskim rynku. Główne z nich to:

- zagrożenia ze strony firm technologicznych, wchodzących na rynek bankowy, przejmujących część usług oferowanych przez banki, szczególnie w obszarze płatności,
- działalność parabankowych organizacji oferujących produkty bankowe, np. *crowdlending*,
- zmiany regulacyjne, zwłaszcza rynku płatności,

- duża zmienność rynków i wrażliwość na parametry makroekonomiczne,
- zmieniające się zachowania konsumentów na skutek upowszechnienia się technologii internetowych i mobilnych oraz zmniejszająca się lojalność klientów.

Na sytuację sektora finansowego w Polsce oddziaływują także czynniki wynikające z wewnętrznej sytuacji makroekonomicznej, gospodarczej i politycznej. Najważniejsze z nich związane są z:

- wprowadzeniem nowego podatku bankowego, uzależnionego od wysokości zgromadzonych aktywów,
- zwiększeniem opłat na Bankowy Fundusz Gwarancyjny, wynikającym z sytuacji w niektórych SKOKach i bankach spółdzielczych,
- niepewnością i oczekiwaniami branży bankowej, co do rozwiązania kryzysu kredytów hipotecznych udzielanych w walutach obcych,
- zmniejszeniem wpływów odsetkowych w dobie spadających stóp procentowych.

Wszystkie przedstawione powyżej wyzwania zmuszają zarządy banków do poszukiwania nowych pomysłów nakierowanych na:

- dalsze podnoszenie efektywności działania – rozwój biznesu przy nierosnącej lub wręcz obniżonej bazie kosztów,
- oferowanie lepszego doświadczenie klienta,
- budowanie prawdziwie omnikanałowej oferty produktów i usług, a, co za tym idzie, bardziej elastycznych modeli obsługi,
- pozycjonowanie banku jako elementu bądź też centrum ekosystemu dostawców zapewniających realizację codziennych potrzeb konsumenckich,
- dobrą wiedzę o kliencie i o jego zachowaniu, pozwalającą na dokonywanie właściwej segmentacji i oferowanie produktów w czasie rzeczywistym.

Jednym z działań, które banki realizują by wypełnić wymienione cele jest modernizacja lub wręcz wymiana centralnego systemu bankowego.

Nowa platforma – katalog wyzwań

W tym momencie pada pytanie, czy wymiana systemu centralnego jest właściwym działaniem. Zanim zostanie podjęta decyzja o uruchomieniu takiego

projektu, należy rozważyć szereg kwestii. Przede wszystkim, czy istnieje lepsze i alternatywne do posiadanego w naszej organizacji rozwiązanie? Większość obecnie oferowanych produktów to wynik ewolucji systemów, które zostały zaprojektowane w latach 80. lub 90. ubiegłego wieku. Nie powstała żadna nowa generacja systemów bankowych, albowiem budowa ich od podstaw to przedsięwzięcie wymagające ogromnych inwestycji. Proces wymiany systemu bankowego jest złożony, kosztowny i pełen ryzyka.

Złożony, ponieważ systemy centralne są zwykle obudowane dziesiątkami interfejsów z różnorodnymi systemami: kanałami samoobsługowymi, oddziałowymi systemami typu *front end*, systemami rozliczeniowymi, sprawozdawczymi, scoringowymi czy wreszcie hurtownią danych. Lista interfejsów jest długa, a struktury przesyłanych w nich danych często podlegały ewolucji i nie zawsze były dobrze udokumentowane. Podobnie nie zawsze jest w pełni dostępny i udokumentowany sam model danych systemu centralnego. Samo porządkowanie i czyszczenie danych może być zatem dużym wyzwaniem.

Kosztowny, bo parametryzacja i stabilizacja nowego systemu zwykle sama w sobie jest przedsięwzięciem złożonym i trudnym do przeprowadzenia. Do tego dochodzi wysiłek związany z migracją danych: wspomniane już porządkowanie i czyszczenie danych źródłowych, mapowanie ich na struktury systemu docelowego, budowa silnika konwersyjnego oraz mechanizmów uzgodnień danych. Nie można zapomnieć o wielokrotnych, żmudnych testach, szkoleniach, dostosowywaniu procesów i organizacji. Jest to zwykle wysiłek liczony w dziesiątkach tysięcy osobodni.

A ryzykowny ze względu na skalę i mnogość problemów, które mogą się pojawić w trakcie realizacji projektu. Ryzyko wynika również z wpływu na bieżącą realizację biznesu. Wdrażanie centralnego systemu bankowego wiąże się zazwyczaj z koniecznością zamrożenia lub istotnej redukcji rozwoju produktów i usług, co jest zwykle decyzją niezwykle trudną w dzisiejszym, szybko zmieniającym się otoczeniu biznesowym.

Jednocześnie w dużej części przypadków systemy główne nie są łatwe do modyfikacji. Często są zamknięte przez dostawców albo budowane w technologiach nie poddających się łatwo zwinnym metodykom budowy oprogramowania. Często także zdarza się, że dostępność specjalistów od takich zamkniętych technologii jest na rynku ograniczona, co podwyższa koszty ewentualnego projektu i generuje dodatkowe ryzyka.

Dominujące dzisiaj podejście do architektury polega najczęściej na tym, że w systemie centralnym zachowuje się funkcjonalność dotyczącą przetwarzania produktów bankowych, naliczania odsetek, opłat i prowizji, rejestrowania i rozliczania transakcji oraz generowania odpowiednich zapisów księgowych, które odkładane są albo w wewnętrznej księdze pomocniczej albo przekazywane do księgi głównej.

System taki obudowany jest nowoczesnymi systemami wsparcia, najczęściej nakierowanymi na sprzedaż i obsługę klienta w kanałach samoobsługowych oraz wymagających asysty pracownika banku. Dane z systemu centralnego przekazywane są do hurtowni danych w celach raportowych i sprawozdawczych oraz coraz częściej do repozytoriów danych niezbędnych do budowy modeli statystycznych oraz zastosowań analitycznych. Modele analityczne są wykorzystywane do definiowania kampanii sprzedażowych, ale również do oceny ryzyka czy też prewencji wyłudzeń. W tym modelu system centralny pozostawiony jest niejako w tle, co pozwala na minimalizację wprowadzanych w nim zmian. Dzięki temu ogranicza się ryzyka wynikające ze złożoności systemu oraz zdejmuje się system centralny ze ścieżki krytycznej projektów, co pozwala na skrócenie czasu niezbędnego na ich realizację.

Niestety takie podejście, zwłaszcza w kontekście wyzwań, przed którymi stoją dzisiaj banki w Polsce, wydaje się niewystarczające. Banki muszą wciąż poszukiwać usprawnienia swojej działalności przy jednoczesnej redukcji kosztów. A to oznacza, że powinny także poważnie rozważać dalszą modernizację swoich systemów centralnych. Jednak w rozmowie z CIO banków działających w Polsce temat wymiany systemu centralnego wciąż jest traktowany z dużą dozą wątpliwości. Dyrektorzy zarządzający informatyką zauważają, że często ich systemy są nowsze i nowocześniejsze niż systemy eksploatowane w centralach ich grup finansowych. Nie do przecenienia jest też skala ewentualnych problemów i ryzyka związana z migracją, które opisaliśmy powyżej.

Jednocześnie, w związku z wyzwaniami, przed jakimi stoją obecnie banki w Polsce, tak duży obszar, jakim jest system centralny, nie może zostać pozbawiony uwagi. Dlatego coraz częściej dyskutuje się o tym aby nie wymieniać całego systemu, ale skupić się na fundamencie technologicznym na jakim taki system jest postawiony. Ewentualna wymiana takiego fundamentu wydaje się nieco łatwiejsza, a spodziewane oszczędności uzasadniają realizacje projektu.

Nowa platforma – dlaczego warto

Jak wykazaliśmy powyżej, wydaje się, że w chwili obecnej nie istnieje „kolejny, fantastyczny system centralny", który oferowałby funkcjonalności i elastyczność uzasadniające inwestowanie w całkowitą wymianę. Jednocześnie w zestawieniu w tabeli nr 1 widać wyraźnie, że cały fundament technologiczny, na którym dzisiaj postawione są systemy centralne od co najmniej dekady nie był zmieniany (pomijając aktualizacje do najnowszych wersji danych komponentów technologicznych).

Tab. 1 **Wybrane banki w Polsce i ich systemy centralne wspierające bankowość detaliczną**

Nazwa Banku	Centralny System Bankowy	Platforma technologiczna (OS, DB, HW)
PKO Bank Polski	Accenture Alnova	IBM z/OS, IBM DB2, IBM z System
Bank Pekao SA	Alltel Systematics	IBM z/OS, IBM DB2, IBM z System
Santander BZ WBK	Fiserv ICBS	IBM i/OS, IBM DB2, IBM Power System
mBank	Accenture Altamira	IBM z/OS, IBM DB2, IBM z System
ING BSK	Fiserv ICBS	IBM i/OS, IBM DB2, IBM Power System
Getin Noble Bank	Asseco DEF 3000	IBM AIX, Oracle DB, IBM Power System
Bank Millennium	Fiserv ICBS	IBM i/OS, IBM DB2, IBM Power System
Alior Bank	Fidelity Profile	HP UX, Oracle DB, HP HW
BGŻ BNP Paribas	Misys Equation	HP UX, Oracle DB, HP Intel Servers
Raiffeisen Polbank	Temenos T24	IBM AIX, Jbase DB, IBM Power System

W ciągu ostatniej dekady nastąpił dynamiczny rozwój różnorodnych komponentów technologicznych. W efekcie na rynku istnieje możliwość większego wyboru takich, które będą w stanie sprostać najwyższym wymaganiom technicznym (wydajność, skalowalność, niezawodność) przy często bardziej atrakcyjnych warunkach cenowych. Stwierdzenie to dotyczy wszystkich warstw technologicznych. Przykładowo w warstwie sprzętowej dynamiczny rozwój platformy Intel spowodował zmniejszenie dystansu w stosunku do

procesorów budowanych w oparciu o inne technologie, a w obszarze technologii dyskowej obserwujemy dramatyczny spadek cen przy jednoczesnym dynamicznym rozwoju funkcjonalności.

Rozwój technologii hardware'owych, przy równoległym rozwoju technologii sofware'owych, skutkuje tym, że dzisiaj nawet najbardziej wymagające systemy informatyczne można uruchamiać na znacznie bogatszej palecie systemów operacyjnych, w tym na Windows Server czy Linuksie. Konkurencja w obszarze rozwoju baz danych przyczyniła się do tego, ze dawni gracze dominujący na rynku (IBM, Oracle) są dzisiaj detronizowani przez rynkowych challengerów – patrz rys. 1.

Rys. 1. Magiczny Kwadrant dla Operational Database Management Systems

Źródło: Gartner, październik 2015, https://www.gartner.com/doc/reprints?id=1-2PMFPEN&ct=151013&st=sb

Biorąc pod uwagę powyższe uwarunkowania proponujemy, aby w obszarze centralnego systemu bardzo poważnie rozważyć wymianę platformy technologicznej. Projekt taki może przynieść bankowi następujące korzyści:

- obniżenie poziomu inwestycji w infrastrukturę – tańsze komponenty technologiczne,
- obniżenie kosztów eksploatacji i utrzymania – także ze względu na niższe koszty pracy związane z utrzymaniem nowoczesnej platformy technologicznej,
- szybsze wdrożenie nowych procesów biznesowych i lepsze sprostanie wymogom regulacyjnym,
- wykorzystanie nowoczesnych funkcjonalności, niedostępnych na starszych platformach,
- obniżenie poziomu ryzyka ze względu na łatwiejszy dostęp do specjalistów znających współczesne technologie.

Przykłady wdrożeń

Wymienione powyżej korzyści dostrzeżono w wielu organizacjach na świecie o czym świadczą zrealizowane projekty.

Skandinavisk Data Center (SDC)
SDC powołano do życia w 1963 r. Jest ono własnością 150 instytucji finansowych działających na terenie Danii, Szwecji, Norwegii i Wysp Owczych. Zadaniem tej organizacji jest dostarczanie usług w obszarze przetwarzania informacji (w tym usług systemu centralnego) bankom działającym na terenie Skandynawii. Zapewnienie usług dla tak wielu instytucji pozwala uzyskać efekt ekonomii skali, dzięki czemu przewagą konkurencyjną SDC, poza wysokim poziomem jakości usług, jest synergia kosztowa. W rezultacie obsługiwane banki ponoszą niższe koszty w porównaniu do modelu, w którym każdy z nich prowadziłby samodzielnie swoje centrum przetwarzania danych i utrzymywał w nim własne systemy informatyczne.

Podczas dziesięcioleci eksploatacji systemów okazało się, że presja na obniżanie kosztów nie słabła. Presja ta stała u źródeł decyzji o migracji platformy technologicznej, na której eksploatowano systemy informatyczne SDC. W maju 2009 r. rozpoczęto proces migracji systemów z technologii mainframe IBM na platformę Microsoft SQL Server i Windows Server. Dzięki tej operacji

SDC uzyskało oszczędności na poziomie 20 mln dolarów rocznie. Migracja do nowych technologii pozwoliła SDC na oferowanie swoich usług przy znacznie niższym poziomie kosztów i umożliwiła redukcję kosztów operacyjnych o ok. 30 proc. To w konsekwencji dało szansę utrzymania istniejących i pozyskanie nowych klientów.

Projekt migracji podzielono na 3 etapy. Pierwsza faza polegała na przeniesieniu 71 najcięższych aplikacji transakcyjnych z mainframe (COBOL/JCL) do .NET i oparciu ich na platformie Windows Server. W kolejnym etapie przeniesiono pozostałe aplikacje transakcyjne, w tym wspierające bankowość internetową. W trzeciej fazie, poza migracją pozostałych aplikacji transakcyjnych przeniesiono przetwarzanie bazodanowe z bazy danych DB2 do platformy Microsoft SQL Server.

Erik Jakobsen, CEO SDC, powiedział:

„Naszym głównym wyzwaniem jest redukcja kosztów bez utraty jakości. Rosnąca konkurencja, w połączeniu z kryzysem finansowym, koncentruje uwagę sektora finansowego w całym zachodnim świecie na redukcji kosztów. To odnosi się również do banków powiązanych z SDC. (…) Ważne jest, że koszty mogą być redukowane bez narażania naszego bankowego systemu centralnego na utratę niezawodności i wydajności. System ten jest, jak sama nazwa wskazuje, rdzeniem codziennej pracy dla naszych klientów. Nasze doświadczenie pokazuje, że znaczna redukcja kosztów bez utraty jakości jest możliwa także w przypadku systemów wielkiej skali, z jakimi mamy do czynienia w SDC".

Bank SinoPac, Tajwan

Tajwański Bank SinoPac obsługuje trzy miliony klientów poprzez 129 oddziałów krajowych, przetwarzając ok. dwóch milionów transakcji dziennie. Poza Tajwanem prowadzi swoje operacje także w Hongkongu, Makao, Chinach i Wietnamie. Będąc liderem na swoich rynkach i oferując nowoczesne i innowacyjne produkty, a jednocześnie podążając za stale rosnącymi wymogami klientów, bank podjął decyzje o zastąpieniu przestarzałego systemu informatycznego nowym centralnym systemem bankowym TEMENOS T24 Universal Banking. Bank z sukcesem uruchomił produkcję na nowym systemie w sierpniu 2012 r. na platformie technologicznej Microsoft Windows Server i SQL Server.

T24 uruchomiony w takiej technologicznej architekturze jest platformą wspierającą kluczowe potrzeby biznesowe banku, zapewniającą wysoką dostępność, skalowalność i wydajność przy jednoczesnym niskim całkowitym

koszcie utrzymania. Wykorzystanie nowoczesnych technologii oznacza także elastyczność reagowania na pojawiające się potrzeby rynkowe. Uproszczenie architektury aplikacyjnej oraz optymalizacja procesów pozwoliły Bankowi na znaczący wzrost automatyzacji pracy oraz skrócenie procesów zamknięcia dnia o połowę. Wszystkie produkty bankowe, takie jak: depozyty, pożyczki, operacje w handlu międzynarodowym itd. są przetwarzane w ramach jednej, wspólnej platformy, dzięki czemu bank ma dostęp do jednolitego i spójnego widoku klienta we wszystkich oddziałach i kanałach. Takie spojrzenie ułatwia zarządzanie poziomem ryzyka i limitami kredytowymi dostępnymi dla klienta. Bardziej elastyczna architektura to także korzyści dla służb IT banku, które mogą brać na siebie większą odpowiedzialność za utrzymanie i rozwój systemu. A to oznacza szybsze reagowanie na potrzeby biznesu i lepszą kontrolę kosztów.

BlueShore Financial (marka North Shore Credit Union), North Vancouver, British Columbia, Kanada

Podobne cele do tych realizowanych przez bank na Tajwanie postawiła sobie kanadyjska instytucja finansowa BlueShore Financial. Również tutaj poszukiwano platformy technologicznej, która spełniając wszystkie wymogi w zakresie funkcjonalności, niezawodności i wydajności, oferowałaby jednocześnie najniższe całkowite koszty posiadania (TCO – *total cost of ownership*). Podobnie, jak w przypadku Bank SinoPac, w obszarze przetwarzania bazodanowego wybór padł na Microsoft SQL Server. W przeszłości BlueShore Financial zgromadził spore doświadczenie w zastosowaniu SQL Server w obszarach automatyzacji oddziałów, bankowości internetowej czy mobilnej. Technologia ta nie była jednak używana jako silnik bazodanowy w głównym systemie bankowym. To jednak uległo zmianie. Nie bez przyczyny na poprawę opłacalności takiej migracji wpływał fakt szerokiej dostępności kadry znającej technologie SQL Server oraz fakt, że koszt takiej kadry był niższy niż w przypadku innych technologii.

Podejście do projektu przejścia na nową platformę

Projekt zmiany platformy jest projektem złożonym, jednak istnieją sprawdzone metodyki i narzędzia wspierające ten proces. Bardzo ważne jest oczywiście wczesne rozpoznanie potencjalnych problemów oraz zaplanowanie procesu migracji, a w szczególności potwierdzenie czy będzie rozłożony w czasie, czy

też zostanie przeprowadzony jednorazowo, metodą „big-bang". W pierwszym przypadku konieczne jest zaplanowanie koegzystencji rozwiązań i uwzględnienie kosztów z nią związanych, w drugiej zaplanowanie i przeprowadzenie szczegółowych testów tak, aby zmniejszyć ryzyko.

W identyfikacji potencjalnych problemów i weryfikacji założeń może pomóc metoda prototypowania, pozwalająca na szybkie sprawdzenie zachowania komponentów systemu po przeniesieniu na nową platformę. W przypadku systemów bankowych szczególne istotne jest potwierdzenie na wczesnym etapie wydajności i skalowalności części transakcyjnej oraz zweryfikowanie złożoności przenoszenia przetwarzania wsadowego. Konieczne jest wczesne sprawdzenie wymaganej wydajności i skalowalności rozwiązania a także dostępności zamienników narzędzi wspomagających w środowisku mainframe (np. scheduler zadań wsadowych, monitor transakcyjny, etc.)

W procesie tym pomagają dostępne na rynku pakiety, które pozwalają emulować środowisko mainframe na procesorach Intel albo wręcz wykorzystać kod oprogramowania z mainframe›a (najczęściej napisany w COBOLu) i skompilować go do kodu binarnego możliwego do uruchomienia w systemie Unix lub Windows Server. Przykłady takich rozwiązań to produkty firmy Microfocus – emulator mainframe'a na systemy Unix lub Windows, a także kompilator COBOLa. Ciekawym rozwiązaniem jest produkt firmy Raincode, pozwalający na kompilowanie kodu COBOLa do obiektów środowiska .Net w systemie Windows Server. Firma ta posiada w ofercie również produkt umożliwiający emulowanie środowiska przetwarzania wsadowego – uruchamianie zadań JCL w systemie Windows. Zastosowanie tych narzędzi pozwala na uniknięcie konieczności translacji kodu na inny język programowania, co znacząco zmniejsza wysiłek niezbędny do przeprowadzenia przedsięwzięcia. Oprócz tego na rynku dostępnych jest sporo rozwiązań odtwarzających w środowisku Windows i Unix funkcjonalność narzędzi mainframe wykorzystywanych w przetwarzaniu danych - np. SORT lub ICETOOL.

Dzięki tym narzędziom możliwe jest istotne ograniczenie kosztów przedsięwzięcia. Zastosowanie sprawdzonej metodyki prowadzenia projektu pozwala na wczesną identyfikację najistotniejszych kwestii do rozstrzygnięcia oraz minimalizację ryzyka.

Co dalej?

Pojawia się pytanie, czy wymiana platformy technologicznej wyczerpuje możliwości, które współczesne IT oferuje bankom. Czy migracja do nowocześniejszych komponentów sprzętowych, systemowych i aplikacyjnych to już koniec drogi. Nam wydaje się, że jest krokiem pośrednim, dającym znaczące oszczędności i zwiększającym elastyczność, jak wskazano w przykładach powyżej. Krokiem pośrednim, bo umożliwiającym przeprowadzenie dalszej zmiany – przede wszystkim otwierającym możliwość przejścia na przetwarzanie oparte na chmurze obliczeniowej.

Obecnie w departamentach IT banków panuje dobre zrozumienie zalet przetwarzania w chmurze. Widoczna jest natomiast niepewność związana z bezpieczeństwem danych i dotycząca zgodności takiego modelu z wymogami regulacji. Wierzymy, że takie obawy zostaną rozwiane i banki będą miały możliwość korzystania z zalet chmury obliczeniowej w całym spektrum jest zastosowań – od środowisk rozwojowych i testowych przez przechowywanie danych aż po kompletne aplikacje działające w chmurze. Nic nie stoi na przeszkodzie aby w pierwszym kroku korzystać z chmury prywatnej. Takim wdrożeniem jest opisany wcześniej przykład SDC. Instytucja ta skupiła wokół siebie pewne środowisko banków, którym udostępniła usługi ze wspólnej platformy systemowej. Innymi słowy banki powiązane z SDC zbudowały wspólną infrastrukturę, z której dostarczane są usługi w modelu SaaS. Wydaje się, że również w Polsce taki alians miałby szansę zaistnieć - chociażby w środowisku banków spółdzielczych. Kolejny krok to użycie chmury publicznej. Na dzisiaj przeniesienie do niej systemu centralnego banku wydaje się perspektywa odległą. Nie ma przeszkód, aby różne systemy okalające system centralny i systemy wspierające już dzisiaj wynosić do chmury.

Podróż do chmury mogą także przyspieszyć kolejne regulacje pojawiające się na rynku. Przykładem tej, która będzie wpływać na rozwój architektury głównych systemów bankowych jest dyrektywa PSD2 i koncepcja otwartych API bankowych. Jeśli zostanie podchwycona przez rynek, pozwoli ona na budowę kompletnych ekosystemów w oparciu o usługi bankowe udostępniane na zewnątrz poprzez API.

Koncepcja ta będzie wymagała od banków dużej elastyczności rozwoju, a ta jest dużo łatwiejsza po przejściu na nowoczesne platformy technologiczne. Wizja otwartego API pozwoli na «oderwanie rachunku od banku». Będzie to kompletne odmiejscowienie rachunku, którego nikt nie wyobrażał sobie w latach 90., a które nawet dla dzisiejszych użytkowników bankowości na smartfonach będzie nowością.

Aleksander P. Czarnowski

Prezes AVET Information and Network Security sp. z o.o., spółki zajmującej się od 17 lat konsultingiem w zakresie bezpieczeństwa informacji w Polsce, Rumunii, Holandii i Wielkiej Brytanii oraz na Ukrainie i Słowacji.

Członek Komisji Technicznej 182, która w Polskim Komitecie Normalizacyjnym odpowiada za rodzinę standardów ISO 27000, a także rady programowej Zakładu Systemów Jakości i Zarządzania działającego w ramach Wojskowej Akademii Technicznej. Od 2013 r. ekspert w grupie eksperckiej odpowiedzialnej za kontraktowanie usług cloud computingu dla sektora SMB przy Komisji Europejskiej, gdzie odpowiada m.in. za zagadnienia związane z dostępnością i ciągłością działania. Wieloletni autor i wykładowca, doskonale znany czytelnikom magazynu i uczestnikom konferencji Virus Bulletin.

Aleksander P. Czarnowski, AVET

Cybersecurity – moda, mit czy rzeczywistość?

Pojęcie cybersecurity zagościło na dobre w świadomości zarządów i rad nadzorczych. Czym jednak jest cybersecurity i jaki ma wpływ, zwłaszcza na sektor finansowy? Jakie są trendy w tym obszarze i na ile przewidywania mają szansę się spełnić? Na te i inne pochodne zagadnienia staram się odpowiedzieć w dalszej części tekstu.

Jak przejawia się moda na cybersecurity?

To, że zapanowała moda na „cybersecurity" najlepiej widać na następującym przykładzie: niektóre organizacje do zgłaszania incydentów oraz komunikacji nt. bezpieczeństwa swoich usług nie używają już adresu security@nazwa-organizacji.com lub incidents@nazwa-organizacji.com, lecz korzystają z konta cybersecurity@. Tak jest na przykład w niektórych spółkach oferujących usługi w chmurze z grupy SAP.

Oczywiście zmiana adresu z security@ na cybersecurity@ nie świadczy o niczym innym poza tym, że… marketing zaczął postrzegać kwestie zapewnienia bezpieczeństwa jako istotny element komunikacji z otoczeniem. Jest to niewątpliwie bardzo dobry, pożądany trend – ważne jednak, aby przed działaniami marketingowymi podejmowano rzeczywistą pracę zmierzającą do zapewnienia bezpieczeństwa.

Dlaczego pojęcie „cybersecurity" może być szkodliwe?

Pojęcie cybersecurity lub cyberbezpieczeństwa zaczęło być powszechnie używane ok. dwóch lat temu. Dziś już poszukuje się specjalistów od cybersecurity

z co najmniej 2-, a jeszcze lepiej z 5-letnim doświadczeniem. Przypomina to bardzo sytuację z rynku cloud computing, gdzie w cenie są specjaliści z co najmniej 5-, a najlepiej 10-letnim stażem. W przypadku cloud computing problemem jest fakt, że takich ludzi praktycznie nie ma, ponieważ dekadę temu prawie nikt nie słyszał o chmurze. Nie przeszkadza to jednak działom HR tworzyć takie wymagania. Oczywiście odpowiedź rynku pracy jest przewidywalna: nagle pojawiło się wielu „specjalistów" z wieloletnim doświadczeniem, właśnie rozważających zmianę miejsca zatrudnienia. W wielu przypadkach ci ludzie nie mieli nawet wiele wspólnego z technologiami internetowymi. O ile jednak w przypadku usług cloud computing najgorsze co może się zdarzyć to strata finansowa inwestorów na skutek zatrudnienia niekompetentnych osób, o tyle powielenie tego schematu w obszarze bezpieczeństwa ma dalekosiężne, negatywne skutki. Z drugiej strony niedobrze jest, gdy w procesie rekrutacji odpadają eksperci od bezpieczeństwa, bo nie przykleili sobie łatki „cyber". Temat braku kompetentnych ludzi w organizacji i właściwej edukacji zostanie poruszony jeszcze dalej.

Pojęcie „cybersecurity" może więc sugerować, że wcześniej nikt nie zajmował się bezpieczeństwem infrastruktury sieciowej, bezpieczeństwem aplikacyjnym, ochroną fizyczną, ochroną danych osobowych, polityką bezpieczeństwa, compliance czy zarządzaniem ryzykiem… Można tak jeszcze długo wymieniać, ale od razu widać, że tak nie jest. Przecież – zwłaszcza w sektorze finansowym – od lat zatrudnione są kompetentne osoby odpowiedzialne za powyższe zagadnienia. Od lat stosowane jest stanowisko Chief Information Security Officer (CISO) w średnich i dużych organizacjach. Czym w takim razie powinien zajmować się ekspert od cyberbezpieczeństwa? Czy w dobie Internet of Things czy chmury powinien się zajmować takim zagadnieniem, jak np. bezpieczeństwo fizyczne? W teorii jest to zagadnienie nie bardzo „cyber". Praktyka okazuje się jednak inna. Załóżmy na chwilę, że „nasz" ekspert będzie dbał o cybersecurity w organizacji pełniącej funkcję Cloud Service Provider (CSP). Organizacja nie posiada jednak własnej infrastruktury IT, lecz sama korzysta z chmury. Skoro żadna infrastruktura IT nie jest własnością organizacji ani nie jest zlokalizowana po jej stronie, łatwo sobie również wyobrazić, że nie potrzeba biur – cała praca może być wykonywana zdalnie. Nie trzeba więc zajmować się nieciekawymi zajęciami, takimi jak wydawanie i odbieranie identyfikatorów z kartą dostępu, organizować ćwiczeń ewakuacji obiektów, zarządzać planami ochrony obiektu, itd. Świetnie, a więc

bezpieczeństwo fizyczne w wydaniu „cyber" nie jest istotne. Stop. Rzeczywistość jest jednak inna: otóż jak taki „ekspert" ma przeprowadzić inspekcję chociażby jednego z wielu centrów przetwarzania danych, w których znajdują się dane jego organizacji? Przecież nie ma wiedzy na temat bezpieczeństwa fizycznego, identyfikatorów, fizycznej kontroli dostępu, awaryjnego zasilania, bilansów energetycznych, itp. Więc jednak „ekspert" musi się znać i na tych zagadnieniach. Prowadzi to do bardzo niebezpiecznej sytuacji, w której „ekspert" musi znać się na wszystkim, w efekcie czego jest dyletantem w każdej dziedzinie. Jak widać z powyższych rozważań pojęcia „cybersecurity" i „ekspert od cybersecurity" są w dużej mierze wytworzone sztucznie i wcale nie musi się za nimi kryć nowa jakość. Ważne jest, aby adekwatnie i efektywnie zarządzać bezpieczeństwem informacji, a że jest to dzisiaj przede wszystkim informacja w formie elektronicznej, nikogo już przekonywać nie trzeba.

Trendy i prognozy w obszarze cybersecurity

Po lekturze dowolnej prognozy w obszarze cybersecurity lub IT security na lata 2014, 2015 czy 2016 można darować sobie – w większości przypadków – czytanie kolejnych. Od razu podam prognozy (które niestety się sprawdzą) na kolejne lata aż do 2020 r. minimum. Co roku będzie rosła cyberprzestępczość (to akurat termin, który ma więcej sensu niż ekspert ds. cybersecurity). W konsekwencji będzie rosła liczba incydentów, w tym prób ataków DDoS, oraz straty wynikające z tego tytułu przestępczej działalności. Rosła będzie także liczba próbek złośliwego oprogramowania – to jest trend praktycznie utrzymujący się nieprzerwanie od końca lat 80. ubiegłego wieku. Oznacza to, niestety, że większość analiz trendów ma charakter stricte marketingowy i nie dostarcza rzeczywistej wiedzy.

FBI i cyberprzestępcy

FBI posiada odrębną kategorię dla cyberprzestępców i także dla nich publikuje swoją listę „most wanted" dostępną pod adresem: https://www.fbi.gov/wanted/cyber. Warto zwrócić uwagę na jej aktualną zawartość – są tam np. wojskowi z Chińskiej Republiki Ludowej. Nagroda za informacje waha się od zera do kilku milionów dolarów. Wielu poszukiwanych jest powiązanych z ransomware i atakami DDoS.

Ransomware czyli różne oblicza szantażu

Ransomware to złośliwe oprogramowanie, którego celem jest wymuszenie opłaty od użytkownika zainfekowanego systemu. Zazwyczaj, aby zapewnić sobie wpływy z tego typu działalności, trojan szyfruje pliki lub dyski zainfekowanego systemu. W ten sposób użytkownik ma do wyboru: albo dokonać reinstalacji systemu i odzyskać dane z kopii zapasowych, albo zapłacić i uzyskać program umożliwiający odszyfrowanie zaszyfrowanych danych. W takim przypadku wykrycie i usunięcie trojana przez oprogramowanie antywirusowe powoduje tylko usunięcie infekcji a nie odzyskanie danych. Zazwyczaj do szyfrowania danych używany jest silny algorytm z losowo generowanym kluczem. Z tego powodu analiza kodu trojana nie zapewnia możliwości odszyfrowania danych czy opracowania uniwersalnej metody usuwania infekcji wraz z odszyfrowaniem zaszyfrowanych plików.

Oczywiście istnieje wiele wariantów ransomware. Ciekawym przypadkiem jest Locky, którego proces szyfrowania można zatrzymać. Locky wymienia klucze szyfrujące w pamięci ze swoim centrum dowodzenia (C&C). Zakłócenie procesu wymiany – np. poprzez zerwanie połączenia z siecią – powoduje, że proces szyfrowania zostanie zatrzymany. Locky jest interesujący z jeszcze jednego powodu: jest on łączony z autorami złośliwego oprogramowania z rodziny DRIDEX (poprzednikiem była rodzina CRIDEX), które stara się kraść informacje potrzebne do uwierzytelnienia z systemów bankowości elektronicznej.

Innym interesującym przypadkiem jest Petya. W przeciwieństwie do typowych przedstawicieli tego typu złośliwego oprogramowania, Petya nie szyfruje tylko plików, lecz całe dyski. Co więcej, nie zostawia systemu w stanie do dalszego użytku: po zaszyfrowaniu dysku systemowego i kolejnym restarcie lub uruchomieniu systemu Petya wyświetla fałszywy komunikat programu chkdsk o uszkodzonym wolumenie. Następnie wyświetla ekran z instrukcjami co należy zrobić, aby odzyskać dostęp do systemu. Petya instaluje się w tablicy partycji dysków ignorując sposób startu systemu operacyjnego w przypadku obecności UEFI. To może powodować zamazanie części informacji na dysku i uszkodzenie systemu niezależnie od procesu szyfrowania. Co więcej, pierwsza faza szyfrowania opiera się na prostej i odwracalnej operacji XOR. Autorzy zapewne zaimplementowali to w ten sposób, aby skrócić czas zaszyfrowania dysków i odcięcia użytkownika od jego systemu. Tym samym w teorii skrócili czas oczekiwania na wpłaty od szantażowanych użytkowników.

Technologia sandbox i jej omijanie

Od pewnego czasu modna jest technologia sandbox do wykrywania złośliwego oprogramowania. Istnieją nawet produkty oparte tylko o tę technologię. Jest to, niestety, kolejny smutny dowód na to, że bezpieczeństwem rządzi czasami moda a nie rozsądek. Po pierwsze, w samej technologii nie ma nic nowego. Firmy antywirusowe stosowały ją już od pierwszej połowy lat 90. ubiegłego wieku i robiły to wtedy z całkiem niezłymi rezultatami. Ówczesne złośliwe oprogramowanie było jednak pod wieloma względami bardzo prymitywne, podobnie jak i systemy operacyjne, które należało emulować aby uzyskać sandbox. Oczywiście jakość emulacji środowiska wykonania wpływa na jakość sandbox. Sandbox, czyli piaskownica, to bowiem nic innego jak stworzenie kontrolowanego środowiska wykonania – zazwyczaj częściowo lub całościowo emulowanego. Do tak przygotowanego środowiska wstrzykuje się kolejne podejrzane próbki, które mogą być złośliwym oprogramowaniem. Następnie na podstawie jego analizy behawioralnej – np. dostępu do plików, używanych funkcji API – automatycznie jest podejmowana decyzja, czy dany program jest złośliwy czy nie. W teorii jest to świetne rozwiązanie, w praktyce niestety okazuje się ono zawodne, bowiem autorom złośliwego oprogramowania jest niezwykle łatwo się przed tego typu rozwiązaniami bronić. Co więcej, część technik utrudniających analizę kodu złośliwego oprogramowania może być także użyte przeciwko technologii sandbox. Oto kilka przykładów mechanizmów ochronnych stosowanych przez złośliwe oprogramowanie:

- Wykrywanie obecności maszyny wirtualnej, technologii wirtualizacyjnej lub emulatora – każde oprogramowanie, takie jak VMWare, VirtualBox, QEMU czy bochs zostawia charakterystyczne ślady w systemie, który emuluje lub dla którego tworzy warstwę wirtualizacyjną (w przypadku hypervisorów). Najbardziej trywialnym jest sprawdzenie konfiguracji sprzętowej oraz wersji firmware'u. Innym przykładem może być szukanie charakterystycznych dla VMWare czy VirtualBox zainstalowanych rozszerzeń. Bardziej zaawansowane metody analizują stan pamięci i procesorów.
- Wykrywanie uruchomienia pod kontrolą automatycznej maszyny wirtualnej lub emulatora za pomocą wywołań funkcji systemowych i analizy struktur systemu operacyjnego. Jeżeli mamy do czynienia ze środowiskiem sztucznie wytworzonym, np. za pomocą emulatora, to emulowany

system nigdy nie dostarcza pełnego API rzeczywistego systemu operacyjnego wraz z jego wewnętrznymi strukturami. W efekcie wystarczy jedno lub kilka wywołań legalnych, udokumentowanych funkcji aby stwierdzić, że kod uruchomiony jest w sandboxie.

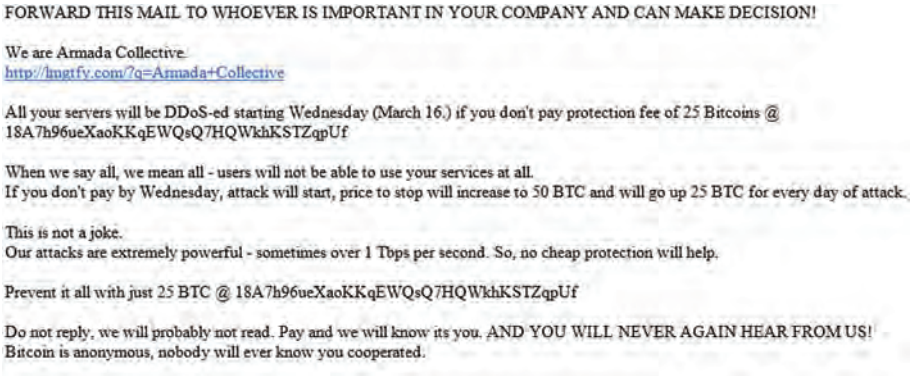
- Wykrywanie uruchomienia pod kontrolą automatycznej maszyny wirtualnej lub emulatora za pomocą środowiska sieciowego. Podobnie, jak w poprzednim przypadku, żaden emulator czy maszyna wirtualna nie może dostarczyć pełnego środowiska sieciowego. Jego brak sugeruje wykonanie kodu w kontrolowanym przez sandbox środowisku.
- Wykrywanie uruchomienia pod kontrolą automatycznej maszyny wirtualnej lub emulatora za pomocą zależności czasowych i zdarzeń. W prawdziwym systemie następują określone zdarzenia, takie jak naciśnięcia klawiszy, ruch myszką, otwieranie i zamykanie okien czy połączenia sieciowe. To wszystko może być użyte do detekcji sandboxa. Jeśli na przykład w systemie nie dochodzi do żadnych zdarzeń tego typu, można podejrzewać, że mamy do czynienia ze środowiskiem kontrolowanym a nie prawdziwym systemem nadającym się do infekcji.

Powyższa lista nie jest kompletna, ale pokazuje jak prosto jest omijać zabezpieczenia typu sandbox. Biorąc pod uwagę inwestycję finansową i czasową w takie zabezpieczenie jest to doskonały przykład asymetryczności środków poniesionych na atak oraz ochronę.

Inne formy szantażu

O ile ransomware wymaga pewnego przygotowania a więc i inwestycji finansowej, okazuje się, że inne formy szantażu z użyciem internetu nie wymagają nic ponad zdobycie bazy adresów e-mailowych. Jak w każdym szantażu opisany poniżej mechanizm funkcjonuje, gdyż oparty jest na strachu oraz na żądaniu relatywnie niewielkich kwot. Pomysł jest banalnie prosty: po co budować duże sieci DDoS i je utrzymywać lub kupować, skoro można wykorzystać „sławę" innych przestępców. W tym celu wystarczy wysłać tylko żądanie – podszywając się pod prawdziwego atakującego – o przelanie kilkudziesięciu np. bitcoinów w zamian za odstąpienie od ataku DDoS na adresata. Niektóre takie wiadomości nawet zawierają gwarancję, że po zapłaceniu szantażysta już więcej nie wróci z kolejnymi propozycjami nie do odrzucenia.

Rys. 1: Przykładowa wiadomość – w tym przypadku szantażysta podszył się pod znaną grupę Armada Collective



FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.
http://lmgtfy.com/?q=Armada+Collective

All your servers will be DDoS-ed starting Wednesday (March 16.) if you don't pay protection fee of 25 Bitcoins @ 18A7h96ueXaoKKqEWQsQ7HQWkhKSTZqpUf

When we say all, we mean all - users will not be able to use your services at all.
If you don't pay by Wednesday, attack will start, price to stop will increase to 50 BTC and will go up 25 BTC for every day of attack.

This is not a joke.
Our attacks are extremely powerful - sometimes over 1 Tbps per second. So, no cheap protection will help.

Prevent it all with just 25 BTC @ 18A7h96ueXaoKKqEWQsQ7HQWkhKSTZqpUf

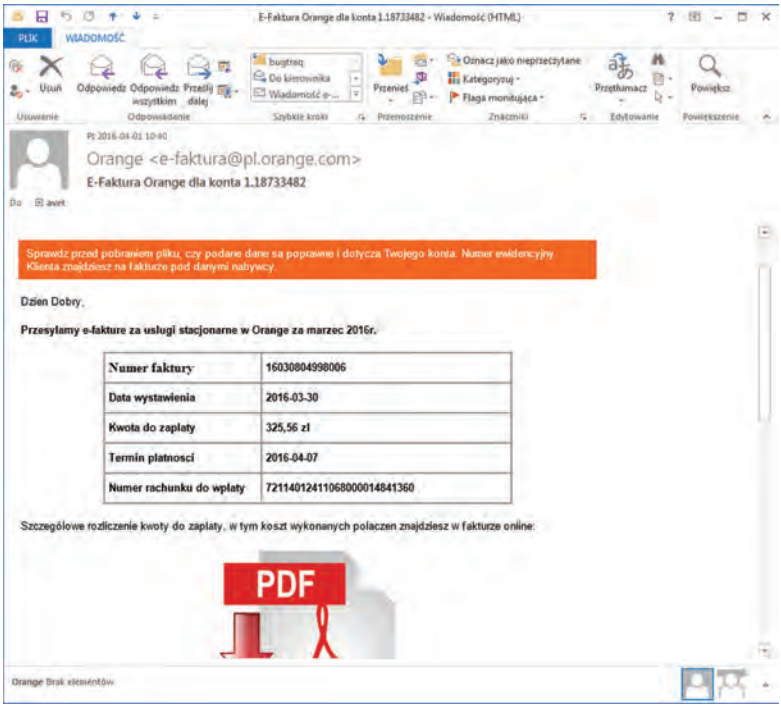
Do not reply, we will probably not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!
Bitcoin is anonymous, nobody will ever know you cooperated.

Wiadomości poczty elektronicznej jako nośnik złośliwego oprogramowania

Oczywiście zarówno wiadomości poczty elektronicznej, jak i komunikacja przesyłana za pomocą for dyskusyjnych lub formularzy kontaktowych jest doskonałym nośnikiem złośliwego oprogramowania. W przypadku kanałów komunikacyjnych akceptujących HTML dodatkowo mogą być wykorzystywane podatności typu Cross Site Scripting (XSS). Jeśli podatność taka zostanie znaleziona w aplikacji webowej – np. do obsługi forum – wtedy atak ma charakter stały, bowiem każdy użytkownik, który otworzy daną stronę będzie zaatakowany.

W przypadku poczty elektronicznej dobrze podszyć się pod nadawcę zaufanego lub takiego, który miałby powód przysłać nam jakąś korespondencję. Typowymi są urzędy skarbowe, kurierzy, dostawcy usług takich jak media czy w usługi telekomunikacyjne (patrz rys. 2 i 3)

Rys 2. Przykład fałszywej wiadomości.



Rys. 3: Fałszywy dokument pdf – proszę zwrócić uwagę na adres URL oraz rozszerzenie pliku pdf. Nadawcą nie może być Orange.

(Kliknij obrazek aby pobrac fakture)

Klasyczny phishing

Rejestrowanie domen podobnych do legalnych jest nadal popularne i, co ciekawe, nadal dobrze funkcjonuje jako metoda ataku. Jednym z najnowszych był atak na klientów ANZ Bank. Przestępcom udało się zarejestrować domenę personal-anz.com, bank tymczasem korzystał z adresu URL: www.anz.com/personal. Fałszywy adres został rozesłany masowo za pomocą poczty elektronicznej. Żadna wiadomość nie była adresowana personalnie do indywidualnego klienta. Aby zachęcić ich do logowania, użyto tradycyjnego już tricku: prośby o zweryfikowanie swojego konta. Powyższy przykład pokazuje, że nawet stare metody ataku są nadal aktualne i nie wymagają wielkiego wyrafinowania poza „inspiracją" podczas rejestrowania domen.

Metody eksfiltracji

Zainstalowanie złośliwego oprogramowania to dopiero połowa „sukcesu". Jeśli atakujący chce ukraść dane, a nie tylko zbudować sieć botów do np. ataku DDoS, musi opracować metody eksfiltracji. Problemem jest fakt, że mechanizmów eksportu danych na zewnątrz organizacji jest nieskończenie wiele. Im bardziej nietypowa (niekoniecznie bardziej zaawansowana) jest używana metoda eksfiltracji, tym trudniej ją wykryć. W przypadku ataków profilowanych metoda eksportu danych może być dopasowana do profilu organizacji. Np. wiele firm tworzących oprogramowanie korzysta z serwisów takich jak github.com czy travis-ci. Można więc użyć gotowego klienta git lub API github do eksportu danych na zewnętrzne serwery. Metoda taka jest o tyle ciekawa, że w przypadku detekcji naruszeń bezpieczeństwa, opartej o analizę anomalii, ruch sieciowy nadal będzie wyglądał na legalny i pasował do przyjętego profilu.

Innym potencjalnym problemem jest pozyskiwanie danych, które np. są przechowywane w formie zaszyfrowanej lub w bazie, ale w setkach tysięcy plików. W praktyce atakujący nie musi znać dokładnej lokalizacji bowiem wiele danych, w tym te kartowe mają określony format i łatwo je identyfikować w pamięci używając metod „brutalnej siły".

IoT

Internet of Things z pewnością jest jednym z ważniejszych akceleratorów cyberprzestępczości. Połączenie wszystkich urządzeń ze sobą nie tylko ułatwi życie, ale będzie stanowiło także istotne wyzwanie od strony bezpieczeństwa. Można oczywiście dyskutować, czy toster lub inne urządzenie kuchenne musi koniecznie mieć dostęp do internetu i korzystać z Twittera. Jest to jednak droga, z której nie ma już odwrotu i tylko kwestią czasu jest powszechne zaadaptowanie takich rozwiązań. Podobnie stało się z chmurą. Cloud computing zawojował szturmem świat, ponieważ pokazał jak w prosty sposób, zazwyczaj na skutek efektu skali oraz standaryzacji, można obniżyć koszty IT a jednocześnie skupiać się na głównych celach biznesowych. Niestety za IoT podąża niezwykle istotny problem ochrony prywatności. Każde z urządzeń IoT to potencjalne źródło wycieku informacji. Wystarczy jeden błąd w firmware popularnego urządzenia IoT, którego efektem będzie podatność i nagle okaże się, że kilka milionów tosterów lub lodówek utworzyło sieć botów gotowych do ataku DDoS. A kto się będzie zajmował usuwaniem podatności w tosterach lub innych urządzeniach IoT już nie wspieranych przez producenta lub nieistniejących już producentów? Oczywiście można na różne sposoby skracać czas życia danego produktu tak, aby potencjalne okno czasowe życia podatności po wygaśnięciu wsparcia było jak najmniejsze. Pytanie tylko czy chcemy co kwartał wymieniać toster.

CaaS czyli Container-as-a-Service

Przywykliśmy już do modelu pracy w chmurze typu: IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service) i najpopularniejszy SaaS (Software-as-a-Service). Od pewnego czasu jest też dostępny nowy rodzaj usługi – CaaS, czyli Container-as-a-Service, który wewnętrznie oparty o ideę kontenerów. Oryginalnie taka koncepcja została zrealizowana już wiele lat temu w kilku systemach uniksowych i nie tylko (w systemie Solaris zaimplementowany mechanizm nawet nazywał się Solaris Containers). Szerokie zastosowanie to jednak ostatnie kilka lat dzięki implementacji mechanizmów lxc i cgroups w jądrze systemu Linux. Inną przykładową implementacją podobnej koncepcji jest OpenVZ. Wszystkie te rozwiązania zaliczane są dzisiaj do jednej grupy VPS (z ang. *Virtual Private Servers*) lub częściej używanej VE

(z ang. *Virtual Environments*). Popularnym w tej chwili sposobem wykorzystania kontenerów jest Docker, który pierwotnie bazował właśnie na mechanizmie lxc w systemie Linux. Docker – podobnie, jak jego inny popularny konkurent Vagrant – to tak naprawdę kolejna warstwa abstrakcji, działająca ponad warstwą wirtualizacyjną. Rozwiązania te przyjęły się z kilku prostych powodów:

- Kontenery w implementacji takiej jak lxc są lżejsze od całych maszyn wirtualnych, jednak nie oferują tak doskonałej izolacji jak typowe maszyny wirtualne – ma to swoje konsekwencje z perspektywy bezpieczeństwa.
- Docker i Vagrant zapewnieją łatwiejsze zarządzanie i przygotowanie maszyn wirtualnych (lub kontenerów) do wielokrotnego użycia oraz dystrybucji.
- Kontenery są często tworzone do chwilowych zadań, np. testów, demonstracji czy określonej sesji. Są też popularnie wykorzystywane w procesach Continous Integration (CI). Ta chwilowość także ma swoje konsekwencje z perspektywy bezpieczeństwa.

Ze względu na ograniczone miejsce, omówię tylko dwie wskazane powyżej kwestie bezpieczeństwa:

- Niedoskonała izolacja – nie jest w tym nic złego pod warunkiem, że ma się świadomość takiego ograniczenia. Niektóre zastosowania nie wymagają pełnej izolacji. Kolejnym problemem może być kontrola dostępu. Vagrant np. domyślnie wykorzystuje SSH do dostępu do maszyny wirtualnej, jednak z poziomu użytkownika, który utworzył maszynę lub kontener każdy ma dostęp do klucza SSH.
- Tymczasowość kontenerów – zwłaszcza w przypadku użycia rozwiązania typu Vagrant – może być bardzo złudna. To że maszyna wirtualna jest zatrzymywana (np. poleceniem vagrant halt) lub niszczona (vagrant destroy[1]) wcale nie oznacza, że dane przetwarzane w niej faktycznie uległy nieodwracalnemu zniszczeniu. W praktyce są to po prostu pliki kasowane z poziomu hypervisora – nie jest to więc operacja gwarantująca bezpieczne usunięcie danych. Innym problemem tymczasowości są aktualizacje. Kontenery zazwyczaj nie są uwzględnione w procesie patch management.

1 W przypadku Vagrant także usunięcie potem boksa poleceniem vagrant box remove nie ma znaczenia

Podatności w SSL/TLS oraz algorytmach kryptograficznych

Ostatnie lata obfitowały w podatności w implementacjach protokołów SSL i TLS. Co więcej starsze wersje tych protokołów, choć od dawna uznawane za niebezpieczne nadal są stosowane w wielu rozwiązaniach. Podobnie sytuacja wygląda z funkcją skrótu SHA-1, która od 2005 r. nie jest uznawana za bezpieczną na skutek ataków z użyciem kryptoanalizy. SHA-1 nie jest wyjątkiem, jeśli chodzi o używanie niebezpiecznych funkcji skrót. Nadal popularne jest wykorzystywanie funkcji MD5, o której od wielu lat wiadomo, że nie jest bezpieczna. Kardynalnym przykładem wykorzystania jej słabości jest robak Flame.

Wracając do podatności w implementacji protokołów SSL/TLS należy pamiętać, że ponad połowa używanych dzisiaj rozwiązań współdzieli kod z biblioteką OpenSSL (albo wręcz wykorzystuje samą bibliotekę). Rosnąca liczba podatności w OpenSSL spowodowała powstanie projektu LibreSSL, który w założeniu miał być bezpieczną reimplementacją funkcjonalności OpenSSL. W praktyce jednak, twórcy LibreSSL także nie ustrzegli się od błędów prowadzących do podatności.

Omawiając podatności związane z protokołami SSL/TLS oraz ich implementacjami nie wolno zapomnieć o dwóch istotnych atakach:

- DROWN – pozwala atakującym na odczytanie zaszyfrowanej komunikacji. Według jego autorów 33% serwerów HTTPS jest podatnych na ten atak [1]. W uproszczeniu jest on możliwy, gdy włączona jest obsługa SSLv2.
- HeartBleed [2] – pozwala na odczytanie zaszyfrowanej komunikacji. Atak jest możliwy na skutek błędu w obsłudze rozszerzenia heartbeat w starszych wersjach OpenSSL.

Analizując powyższe problemy z bezpieczeństwem warto się zapoznać z podatnościami: CVE-2016-0703, CVE-2016-0704, CVE-2015-0293 i CVE-2014-0160.

Innym istotnym protokołem używanym powszechnie – zwłaszcza w wielu usługach IaaS i PaaS w chmurze – jest SSH. Tutaj sytuacja wygląda lepiej, ponieważ rynek serwerów SSH jest praktycznie zdominowany przez implementację OpenSSH, która domyślnie od dawna ma wyłączoną obsługę protokołu v1 uznawanego za niebezpieczny. Jednakże nawet wyłączenie określonej funkcjonalności domyślnie przez twórcę nie gwarantuje, że użytkownicy lub producenci nie włączą jej ponownie. Idealnie obrazuje to podatność xauth

(CVE-2016-3115) w OpenSSH w wersjach poniżej 7.2p2 z włączoną opcją X11Forwarding. Opcja ta w oryginalnej dystrybucji OpenSSH jest wyłączona, jednak wielu dostawców systemów linuksowych włączyło ją w domyślnej konfiguracji.

Rola edukacji

Edukacja jest jednym z kluczowych elementów zarządzania bezpieczeństwem. Idealnym materiałem dydaktycznym są prawdziwe przypadki. Dlatego poniżej przedstawiam jeden z incydentów, który miał miejsce na początku 2016 r. w Polsce.

Analiza przypadku 2be.pl

Przypadek ten pokazuje, jak wiele jeszcze jest pracy w ramach edukacji w zakresie bezpieczeństwa. Równocześnie stanowi doskonały – wręcz książkowy – przykład na to, jak nie należy zarządzać bezpieczeństwem oraz jak nie postępować w przypadku incydentu. Cała historia (która toczyła się jeszcze w trakcie pisania niniejszego tekstu) jest opisana w [3]. Oto w dużym skrócie dotychczasowy przebieg wydarzeń: w dniu 27 lutego 2016 r. w firmie hostingowej 2be.pl doszło (rzekomo) do włamania. Na skutek nieudolnej komunikacji pierwsze komunikaty sugerowały wręcz włamanie fizyczne do samego data center. Później okazało się jednak, że włamanie miało miejsce na serwery firmy hostingowej. Na skutek splotu różnych wydarzeń do serwerów firmy hostingowej w I kw. 2016 r. miało dostęp wielu osób z różnych organizacji. Poniżej przedstawione są tylko najważniejsze fakty wynikające z wypowiedzi pracowników oraz osób reprezentujących spółkę stojącą za marką 2be.pl:

- Niewystarczające zasoby ludzkie: z wypowiedzi wynika, że było dwóch administratorów. Trudno sobie wyobrazić w takim układzie pracę zmianową.
- Administratorzy uważali, że zabezpieczenie dostępu do serwerów za pomocą usługi SSH i uwierzytelnienia kluczem było wystarczającym mechanizmem kontrolnym. Tymczasem wszystkie dobre praktyki wymagają zabezpieczenia takiego klucza dodatkowo silnym hasłem, a o tym administratorzy nie wspominają w swojej wypowiedzi. Należy zauważyć, że zabezpieczenie dostępu to proces o wiele bardziej złożony niż tylko

instalacja i konfiguracja serwera SSH. O tym jednak nie ma słowa w opublikowanych materiałach.

- Brak polityki bezpieczeństwa i procedur zarządzania incydentem: z wypowiedzi jasno wynika, że coś takiego, jak polityka bezpieczeństwa, nie istniało w tej organizacji. Dziwi to w kontekście przetwarzania przez nich danych osobowych klientów.
- Żadna z wypowiedzi nie sugeruje, aby prace naprawcze – zlecane różnym podmiotom – były regulowane profesjonalnymi kontraktami na outsourcing. Oznacza to całkowity brak kontroli nad danymi klientów a w konsekwencji ich ochrony.

Bardzo niepokojący może być fakt, że NASK we wrześniu 2015 r., wybrał grupę Adweb (do której należy marka 2be.pl) do zarządzanie domenami .eu. Biorąc pod uwagę istotną rolę, jaką CERT NASKu ma odgrywać w opublikowanych przez Ministerstwo Cyfryzacji [4] „Założeniach strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej", nie świadczy to najlepiej o współpracy pomiędzy różnymi jednostkami organizacyjnymi NASK. Podobno następne warunki wyboru przez NASK firmy do zarządzania domenami mają być zaostrzone. Logika podpowiada, aby nowe warunki obejmowały przede wszystkim wymagania odnośnie standardów bezpieczeństwa. W przeciwnym razie CERT będzie obsługiwał incydenty a nie im zapobiegał.

Z przypadku 2be.pl płynie kilka ważnych wniosków:

- Dla przeciętnego człowieka hasło to nadal synonim bezpieczeństwa. Pokazuje to, jak bardzo rozwiązania typu *two-factor authetication* muszą się przebić, bo nawet, gdy są oferowane, użytkownicy nadal z nich nie korzystają.
- Organizacja może nie być bezpośrednio celem ataku, ale nie oznacza to, że nie zostanie wciągnięta w incydent. W przypadku 2be.pl w incydent zostały wciągnięte inne firmy: outsourcingowe, zajmujące się odzyskiwaniem danych czy hostingowe. Część z nich nie miała nigdy nic wspólnego z 2be.pl.
- Zarządzanie cyberbezpieczeństwem to nie tylko zabezpieczenia techniczne i organizacyjne, ale także przygotowanie się na wypadek incydentu a później efektywne nim zarządzanie i komunikowanie. Wymaga to dobrej koordynacji po stronie osób odpowiedzialnych za PR w danej organizacji.
- Na skutek całego ciągu zdarzeń pojawiły się głosy, że żadnego incydentu polegającego na nieautoryzowanym dostępie nie było. „Włamanie" zostało użyte tylko do uzasadnienia problemów technicznych.

Two-factor i multi factor authentication

W poprzednim punkcie wspomniałem o potrzebie silnego uwierzytelnienia z użyciem metody *two-factor authentication*. Zwana także czasami *multi factor authentication* lub *2 step authentication* wymaga do poprawnego uwierzytelnienia posiadania przynajmniej dwóch z trzech rzeczy:

- czegoś, co wie tylko użytkownik (np. identyfikator, nazwa użytkownika, hasło),
- czegoś, co ma użytkownik (np. urządzenie mobilne),
- czegoś, czym użytkownik jest (np. metody biometryczne oparte o głos, odciski placów itp.).

Standardy bezpieczeństwa

Nie tylko technologia, ale i standardy bezpieczeństwa starają się nadążyć za przestępcami i atakującymi. Obecnie globalnie jest stosowanych co najmniej kilkadziesiąt różnych standardów w zakresie (cyber)bezpieczeństwa. Samo ich pobieżne omówienie wystarczyłoby na osobną książkę. Dlatego ograniczyłem się tylko do jednego przykładu, który dobrze wiąże się z rynkiem finansowym oraz omówionymi wcześniej problemami. Oczywiście w sektorze finansowym w Polsce niezwykle istotnym standardem jest Rekomendacja D KNF oraz bazujące na niej wytyczne dla pozostałych podmiotów rynku finansowego.

PCI DSS

Standard ten jest doskonałym przykładem, jak bardzo standardy bezpieczeństwa nie nadążają za zmieniającą się dynamicznie rzeczywistością oraz wymaganiami względem realnego bezpieczeństwa. Najnowsza wersja 3.2 (w trakcie pisania tego tekstu aktualną była 3.1) ma się ukazać prawdopodobnie pod koniec kwietnia 2016 r. Zmiany pomiędzy wersją 3.0 a 3.1 objęły m.in. zaostrzenie wymagań odnośnie testów bezpieczeństwa (w tym testów penetracyjnych) oraz uwzględniły poruszone wcześniej problemy i ataki na implementacje protokołów SSL/TLS. Szybko jednak okazało się, że wyłączenie ze środowisk produkcyjnych rozwiązań, które wspierają (tylko) starsze, a w konsekwencji niebezpieczne wersje protokołów nie jest możliwe

w krótkim czasie. Dla niektórych procesorów płatności oznaczałoby to bowiem potrzebę np. wymiany praktycznie od razu istotnego procenta terminali POS[2]. Do tego należy uwzględnić także wiele pomocniczych systemów IT, które mogą nie wspierać zalecanych protokołów. Kolejnym problemem są konfiguracje systemów zgodnie z PA DSS – jeśli klient otrzyma system z taką konfiguracją, raczej próbuje jej nie zmieniać, aby zapewnić sobie zgodność z PCI DSS. Oznacza to, że potencjalnie niebezpieczne ustawienia systemu bądź aplikacji mogą być utrzymywane do momentu ponownej certyfikacji właściwej konfiguracji przez dostawcę.

Innym problemem może być separacja systemów i środowisk przetwarzające dane kartowe od tych nie zawierających takich informacji. W przeszłości PCI nie był jednoznaczny jeśli chodzi o stosowanie wirtualizacji, bo standard bazował na założeniu galwanicznej separacji systemów. Dzisiaj podobna sytuacja występuje w przypadku kolejnej warstwy abstrakcji wirtualizacji jaką są kontenery. Np. bardzo popularny Docker – tak jak wspomniano w podrozdziale CaaS – jest oparty o implementację lxc w przypadku systemów linuksowych. Ta implementacja nie musi być uznana za pełną separację.

Oto kilka istotnych zmian jakie zostaną wprowadzone w wersji 3.2 PCI DSS:

- położono większy nacisk na *two-factor authentication,*
- zasady maskowania PAN zostaną lepiej wyjaśnione,
- zaostrzenie wymagań wobec niektórych podmiotów podlegających pod PCI DSS poprzez dodatkowe procedury weryfikacji codziennych procesów, co ma pomóc w upewnieniu się, że organizacja spełnia wymogi PCI DSS podczas normalnego, codziennego funkcjonowania.

Najnowsza wersja standardu uwzględnia także docelowe daty migracji SSL i TLS, które były już opublikowane wcześniej w formie suplementów.

Podsumowanie

W powyższym artykule – ze względu na ograniczenia techniczne – nie poruszyłem jednej, lecz niezwykle ważnej dla bezpieczeństwa kwestii: zagadnień legislacyjnych. Niewątpliwie legislacja, podobnie jak standardy, nie nadąża za dynamicznie zmieniającymi się metodami ataku.

2 Warto w tym miejscu zauważyć, ze statystyki z ostatnich lat pokazują ciągły wzrost liczby ataków i infekcji terminali POS.

Niezależnie od tego jakich określeń będzie się używało w odniesieniu do zarządzania bezpieczeństwem, nikt już nie powinien mieć wątpliwości, że każda organizacja – bez względu na jej profil i rozmiar – musi to robić. Niewątpliwym problemem jest, po pierwsze, brak wykwalifikowanych ludzi w tym zakresie. Z drugiej strony rosnące wymagania regulatorów oraz łatwość kradzieży środków finansowych kanałami elektronicznymi zmusza, zwłaszcza sektor finansowy, do aktywnych działań zmierzających do ograniczenia ryzyka w tym obszarze. Należy jednak zadać sobie pytanie, czy budowanie kolejnej – siedemnastej już z rzędu – zapory sieciowej coś zmieni? Odpowiedź brzmi – nie. Żadne oprogramowanie ani rozwiązania sprzętowe nie rozwiążą sytuacji. Doskonale przekonały się o tym niektóre banki wdrażając rozwiązania klasy SIEM na fali wymogów rekomendacji D. Nawet najlepsze silniki korelacyjne bez ludzi, którzy będą reagować zarówno na zgłaszane zdarzenia, jak i na zmieniające się dynamicznie zagrożenia bardzo szybko stają się drogą, mało użyteczną zabawką.

Bibliografia:

https://drownattack.com/

http://heartbleed.com/

Włamanie na serwery i blackout grupy AdWeb http://hostingnews.pl/wlamanie-na-serwery-adweb/

https://mc.gov.pl/aktualnosci/zaproszenie-do-konsultacji-zalozen-strategii-cyberbezpieczenstwa-dla-rp

Adam Marciniak

Dyrektor Pionu Rozwoju i Utrzymania Aplikacji w PKO BP.

Swoją przygodę z IT rozpoczął od studiów na kierunku Inżynierii Komputerowej wydziału Cybernetyki Wojskowej Akademii Technicznej w Warszawie. W 2003 r. ukończył je z wyróżnieniem zdobywając tytuł magistra inżyniera oraz stopień podporucznika Wojska Polskiego. W 2007 r. zyskał dodatkowe kwalifikacje – specjalisty ds. projektów informatycznych kończąc studia w Instytucie Sterowania i Elektroniki Przemysłowej Politechniki Warszawskiej.

W 2004 r. rozpoczął pracę w Pekao SA jako programista i projektant systemów IT. W latach 2007-2011 był Dyrektorem Biura Rozwoju i Zarządzania Kanałami Elektronicznymi w Pekao SA. Równolegle w latach 2009-2011 zajmował stanowisko Dyrektora Departamentu Rozwoju Informatyki w Centralnym Domu Maklerskim Pekao SA.

Od lutego 2011 r. Adam Marciniak jest dyrektorem Pionu Rozwoju i Utrzymania Aplikacji w PKO Banku Polskim. Odpowiada m.in. za kompleksową realizację projektów IT oraz cały cykl życia aplikacji włączając utrzymanie systemów. Równolegle, od października 2011 do listopada 2014 roku pełnił funkcję wiceprezesa odpowiedzialnego za rozwój systemów IT w Inteligo Financial Services S.A w ramach Grupy Kapitałowej PKO. W tym czasie odpowiadał za skuteczne inkorporowanie usługi IT ze spółki Inteligo do PKO Banku Polskiego.

Wśród wielu zrealizowanych pod jego kierownictwem projektów na szczególną uwagę zasługują te związane z rozwojem bankowości transakcyjnej, automatyzacją i wirtualizacją procesów sprzedażowych, kompleksowymi rozwiązaniami z zakresu CRM i centralizacji funkcji BO oraz intensywnym rozwojem kanałów elektronicznych (iPKO, iPKO Biznes, iPKO Dealer, Inteligo, IKO, Blik). Na szczególną uwagę zasługują również przedsięwzięcia o charakterze migracyjnym – w ostatnim czasie kierował migracją klientów i systemów Inteligo, Nordea Bank Polska oraz SKOK Wesoła do systemów PKO.

Przewodniczący Grupy Zarządzania Cyberbezpieczeństwem Banków w Bankowym Centrum Cyberbezpieczeństwa.

Adam Marciniak, PKO BP

Bankowy CERT – nowa broń w walce z cyberprzestępczością

Napady z bronią w ręku przechodzą do historii i coraz częściej traktowane są jako ciekawostki. Zgoła inaczej wygląda świat w cyberprzestrzeni – dramatycznie rośnie znaczenie skutków działania profesjonalnych grup przestępczych, dla których usługi finansowe dostępne w Internecie stają się kolejnym i relatywnie mało ryzykownym źródłem zarabiania kosztem banków i ich klientów.

Postęp i dobra cywilizacji, które powodują, że dzięki bankowości elektronicznej i mobilnej żyje się łatwiej i przyjemniej (czy ktoś pamięta jeszcze kolejki w celu opłacania rachunków?) ma, niestety, swoją mroczną stronę. Rozwój informatyki, wzrost skali skomplikowania systemów IT, a jednocześnie zwiększanie się roli pieniądza elektronicznego w obiegu łącznie z transakcyjnością internetową i mobilną powoduje, że wiele organizacji przestępczych, ale także i pojedynczy przestępcy, upatruje w cyberprzestrzeni często zbyt łatwego źródła przychodu.

Co mówią liczby? Według opublikowanego w styczniu br. raportu PwC liczba wykrytych cyberataków na firmy w 2015 r. w Polsce wzrosła o 46 proc. w porównaniu do 2014 r. Zagrożenie atakami na systemy IT (zewnętrzne i wewnętrzne) jest, wg Ernst&Young, najważniejszym czynnikiem ryzyka w sektorze finansowym (wzrost w tym obszarze wskazało 74% respondentów w badaniu „Wrzuć wyższy bieg – ogranicz ryzyko i pokaż korzyści" z tego roku), przebijając „tradycyjne" zagrożenia, jak korupcja (50% respondentów wskazujących wzrost zagrożenia), nadużycia wewnętrzne typu nieuzasadnione narażenie na koszty (47%), ryzyko inwestycyjne (24%), ryzyko związane z połączeniami (25%) i praniem brudnych pieniędzy (46% wskazujących na wzrost zagrożeń). CERT.PL podał w raporcie jeszcze w 2014 r., że ponad

50 tys. komputerów w tym samym czasie posiadało trojana bankowego z ogółu 230 tys. komputerów zainfekowanych złośliwym oprogramowaniem. KNF zauważył w 2015 r., że na przestrzeni ostatnich 3,5 lat liczba użytkowników bankowości mobilnej wzrosła o 250 proc. do ok. 4,3 mln, przy czym udział procentowy właścicieli smartfonów, korzystających z bankowości mobilnej w 2013 r. wynosił 12 proc., a w 2015 – aż 43 proc.

Widać zatem, że wraz ze skalą wykorzystywania nowoczesnych technologii rosną zagrożenia i ryzyko związane z obszarem IT, stając się – wobec sytuacji, w której ryzyka te coraz częściej się materializują – istotnym obszarem w analizie i ocenie ryzyka banku.

Przegląd zagrożeń

Analizując zmiany zachodzące obszarze cyberprzestępczości można zauważyć kilka zjawisk.

Niektóre scenariusze wyłudzeń są złożone i przez to wrażliwe na ryzyko strat – patrząc z perspektywy przestępcy. Takim scenariuszem jest tzw. *phishing*, czyli operacje prowadzone przez cyberprzestępców celem wyłudzenia danych używanych do logowania się do systemów bankowości elektronicznej i wykonywania przelewów. W pierwszym kroku przestępcy prowadzą kampanie mailingowe lub SMS-owe, które, dzięki wykorzystaniu metod inżynierii społecznej, powodują, że klient podaje im wrażliwe dane logowania i autoryzacji transakcji czy kompletne dane kart płatniczych. Jakość tych kampanii i pomysłowość jest na coraz większym poziomie, adresy domenowe mocno przypominają właściwe i trzeba niekiedy poświęcić sporo uwagi, aby dostrzec różnice.

Po uzyskaniu nieuprawnionego dostępu do systemu oraz danych autoryzujących przestępca dokonuje przelewu na konto tzw. „słupa", które zostało specjalnie utworzone w tym celu korzystając z jednej z wypracowanych metod: przez osoby złakomione obietnicą szybkiego zarobku czy poprzez konta otwarte metodą z potwierdzeniem przelewem z innego banku. Coraz częściej słychać też o kontach osób oszukanych poprzez symulację uczestnictwa w procesie rekrutacji, w ramach którego nieświadoma osoba bądź zakłada konto wykorzystywane do przestępczych manipulacji, bądź podaje dane – zwykle jednak dość chronione – wystarczające do utworzenia konta kontrolowanego przez przestępców. W wyniku prowadzonych postępowań

i wewnętrznego nadzoru w poszczególnych bankach gromadzona jest wiedza o podejrzanych kontach i transakcjach, jednak zwykle ograniczona do konkretnej organizacji, podczas gdy cyberprzestępcy swobodnie mogą korzystać z kont w różnych bankach do prowadzenia swych operacji.

Zasadniczo problemem w takich atakach jest osoba klienta i jego urządzenia – komputery czy urządzenia mobilne. Zgodnie z wynikami analizy ankiet zebranych w bankach przez KNF, łącznie ok. 40% incydentów jest powiązanych właśnie z infrastrukturą klientów. Ci ostatni są bowiem podatni na manipulacje i emocje, które skłaniają do nieostrożnych zachowań, a do tego same urządzenia są podatne na skompromitowanie poprzez zainfekowanie oprogramowaniem dystrybuowanym przez Internet (e-mail z niebezpiecznym kodem, złośliwe strony internetowe, serwisy pirackiego software'u) i niejednokrotnie nie wystarczy rekomendowana przez banki „higiena": regularne łatanie oprogramowania, aktualne bazy oprogramowania antywirusowego i użycie firewalla. Ale nie można zapominać, że po drugiej stronie są ci, którzy to oprogramowanie dystrybuują oraz wykorzystują i to z nimi toczy się walka.

Kolejnym zjawiskiem jest pojawienie się zaawansowanych ataków ukierunkowanych (APT, z ang. *Advanced Persistent Threats*) – są to jedne z najbardziej niebezpiecznych ataków i to na firmy, a nie na ich klientów. Rynek cyberprzestępczości, jeśli możemy mówić o rynku, profesjonalizuje się. Organizacje przestępcze zaczynają działać podobnie do organizacji IT – kupują pakiet oprogramowania od wyspecjalizowanych dostawców, do tego stosowne wsparcie, zatrudniają administratorów oraz specjalistów od inżynierii społecznej, inwestują w infrastrukturę licząc na zwrot z inwestycji przy niewielkim ryzyku. Zwykle na celowniku przestępców jest kilka banków, pod które parametryzują oprogramowanie pod kątem ich systemów, co widać po analizie malware'u. Ataki APT wymagają czasu, pieniędzy i wiedzy niezbędnej do przeprowadzenia ataku, co łącznie prowadzi do przekonania, że są możliwe do wykonania wyłącznie przez zorganizowaną przestępczość. Klienci tych organizacji już nie muszą takiej wiedzy posiadać – przykładem użytkownicy trojanów ZeuS czy SpyEye, którzy wykorzystują je do „zarabiania" pieniędzy nie mając większej wiedzy o sposobie budowy tego narzędzia.

Emanacją ataku APT były również w ostatnich trzech latach narzędzia i metody znane pod nazwą Carbanak – spektakularny atak z uwagi na skalę skutecznego dokonania nadużyć (ponad 100 banków w 30 krajach!). Atak ten łączył użycie złośliwego oprogramowania z wypracowanymi praktykami,

które łącznie pozwoliły wyprowadzić, jak się szacuje, 1 mld dolarów. Scenariusz ataku zakładał użycie złośliwego oprogramowania Carbanak dystrybuowanego przez e-mail. Od momentu infekcji stanowiska pracowników były monitorowane, włączając w to rejestrowanie wciśniętych klawiszy, zrzuty ekranu, nawet wideo. Atakujący udawał pracownika w celu wyprowadzenia pieniędzy; nie było zatem ważne, jakie oprogramowanie było wykorzystywane. Dokonywano również manipulacji saldami kont, więc właściciel konta nie widział żadnej różnicy. Atakującym udało się wręcz przeprogramować bankomaty tak, aby wydawały środki w określonym czasie, nawet bez fizycznej aktywności użytkownika. Mimo podobieństwa scenariusza ataku w każdym z banków, gdzie atak trwał od dwóch do czterech miesięcy, można przypuszczać, że w sytuacji tak rozproszonych geograficznie ataków poszczególne banki nie miały wiedzy o tym, co spotkało ich zagraniczną konkurencję. Kaspersky Lab doniósł niedawno, że robak ten zyskał w 2015 r. nową odsłonę – Carbanak 2.0; pojawiły się też inne zagrożenia o podobnym charakterze: Metel oraz GCMan, gdzie grupy przestępcze realizują podobny scenariusz, atakując organizacje finansowe poprzez ukradkowy rekonesans, wykorzystując dedykowane oprogramowanie, typowe narzędzia zdalnej administracji oraz nowe techniki mające na celu kradzież pieniędzy. Dzisiaj każdy z banków na własną rękę walczy z tym zagrożeniem, blokując w miarę możliwości podejrzany ruch oraz informując o prowadzonych kampaniach przestępczych swych klientów i pracowników, bo w zasadzie niewiele więcej może samodzielnie zrobić.

Walka z przestępcami nieustanie trwa. Zorientowali się oni, że banki coraz sprawniej wychwytują transakcje mające znamiona anomalii – co dla transakcji przez konta-słupy miało do tej pory miejsce (długi okres uśpienia i kilka transakcji na dużą kwotę), w związku z czym wkładają więcej sił i energii w upodobnienie działania do charakterystyki ruchu klientów, np. poprzez zwiększenie liczby i zmniejszenie wartości przelewów lub chowanie ich wśród innych przelewów o podobnej charakterystyce. W takiej sytuacji wiedza o tym, że dany rachunek, mimo iż nie budzi podejrzeń w danym banku, w innym został uznany za podejrzany, ma istotne znaczenie dla minimalizacji strat.

Powyższe obserwacje umożliwiają postawienie tezy, że gdyby organizacje bankowe mogły i współpracowały bliżej ze sobą, w skali krajowej i międzynarodowej, istnieje prawdopodobieństwo, iż przeciwdziałanie przestępczym operacjom byłoby skuteczniejsze.

Gdzie banki mogą spodziewać się ataków? W zasadzie na każdy element operacji, gdzie istnieje możliwość pozyskania jakiejś wartości, czy to pieniężnej, czy też w postaci wiedzy, mającej znaczenie dla atakującego. Atakom mogą podlegać bankomaty (ataki fizyczne i zdalne), systemy dostępne przez Internet i telefon, Call Center, systemy sieciowe, systemy zarządzania informacją (tajemnice przedsiębiorstwa, są też zagrożenia wynikające z aktywności wewnętrznej: od sabotażu technicznego, przez wykonywanie nieuprawnionych operacji, po wpływanie na parametry finansowe na rynkach kapitałowych). Jak widać zagrożeń jest wiele i wiedza o potencjalnych scenariuszach mogłaby wydatnie pomóc w ich przeciwdziałaniu.

Innym przykładem zagrożeń, które mogą spotkać banki, są ataki na systemy mające na celu ich zablokowanie lub ograniczenie dostępności – ataki DDoS (z ang. *Distributed Denial of Service*), gdzie cel realizowany jest bądź przez ataki na infrastrukturę (wysycenie pojemności urządzeń sieciowych), bądź przez ataki na funkcjonalność aplikacji. Pierwszy scenariusz może spotkać nie tylko banki, bo w takich atakach ucierpiało wiele znanych firm branży internetowej – portale, sklepy. Ostatnio skala tych ataków nieco się zmniejszyła, m.in. dzięki współpracy z telekomami, przez które taki złośliwy ruch przechodzi i które mają techniczne możliwości jego ograniczania, nie mniej jednak nadal to zjawisko nie może być marginalizowane. Inną kategorią ataku odmowy usługi jest DDoS aplikacyjny – atak, w którym poprzez wykorzystanie interfejsu aplikacji blokowana jest np. funkcjonalność logowania. W tym przypadku konieczne jest odpowiednie przygotowanie aplikacji i infrastruktury pośredniczącej, aby wychwytywać takie sytuacje i zapobiegać stosownymi mechanizmami. Powody ataków, których skutkiem jest zaszkodzenie atakowanemu podmiotowi mogą być różne – chuligaństwo, chęć wykazania się, jak choćby przy atakach na sieć Sony Playstation Network, która stała się „ulubionym" celem ataku tego typu (chociaż nie omijają też i konkurencyjnej sieci) – jak twierdzą jej przedstawiciele ataki odbywaja się każdego dnia, sieć skutecznie zaatakowano w grudniu 2014 r., następnie prawdopodobnie DDoS spowodował niedostępność w styczniu 2016 r. Nie można również zapominać o powodach politycznych, jak choćby ataki cybernetyczne na Estonię w 2007 r., w wyniku których zostały zablokowane serwery i strony Zgromadzenia Państwowego, agend rządowych, banków i mediów. W efekcie banki zanotowały straty finansowe, cyberataki odczuły mocno instytucje państwa, dla obrony zostały na kilka dni zamknięte niektóre połączenia zagraniczne,

skutkując izolacją kraju od reszty świata, a to z kolei uniemożliwiło Estończykom np. dostęp do ich kont bankowych w trakcie zagranicznych podróży.

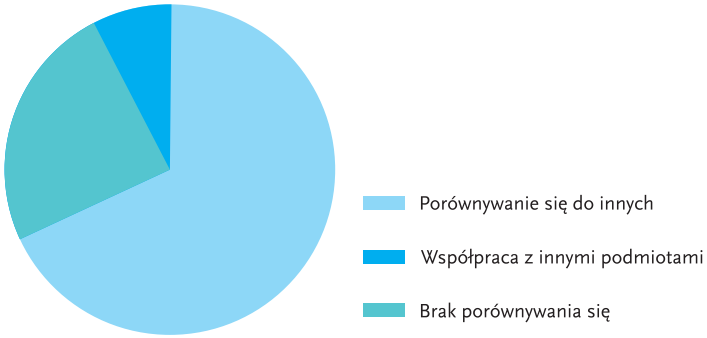
Miara dojrzałości

Istnieje szereg metod oceny skali dojrzałości organizacji w zakresie bezpieczeństwa informatycznego. Wg A.T. Kearney takie badanie może być przeprowadzone w obszarach związanych ze strategią (czy organizacja posiada ją w związku z zarządzaniem bezpieczeństwem informatycznym i stosowną politykę), organizacją (czy istnieją operacyjne metody zarządzania bezpieczeństwem wewnątrz firmy bądź instytucji i u partnerów), procesami (zarządzanie tożsamością i dostępem, aktualizacjami, realizacja procesu planuj-wykonaj-sprawdzaj-działaj), technologią (infrastruktura sieciowa, serwery i aplikacje, stacje robocze i telefony, bezpieczeństwo fizyczne) oraz kulturą (znaczenie bezpieczeństwa dla zarządu, edukacja pracowników, budowa świadomości i poprawnych zachowań). Na tej bazie można zdefiniować zasady, których świadome stosowanie zapewnia efektywne zarządzanie bezpieczeństwem informacji. Wśród nich znajduje się automatyzacja procesów i funkcji, zaangażowanie pracowników w aktywne zwalczanie naruszeń bezpieczeństwa, ochrona aktywów stosownie do ich wartości i związanego z tym ryzyka, transformacja działu bezpieczeństwa w jednostkę zapewniającą wartość biznesową, zapewnienie poparcia wyższego szczebla zarządzania oraz mapy rozwoju obszaru bezpieczeństwa z zabezpieczoną perspektywą zbalansowanego finansowania, regularne testy bezpieczeństwa oraz – i tutaj ważna jest kwestia w kontekście niniejszego artykułu – wyjście poza porównywanie się do innych podmiotów z branży i rozpoczęcie współpracy.

Porównywanie się jest pomocne w budowie własnych standardów bezpieczeństwa, poszukiwaniu nowych rozwiązań, jednakże proste kopiowanie strategii bezpieczeństwa bez uwzględnienia indywidualnych cech biznesowych danego podmiotu nie pozwoli na osiągnięcie optymalnego rezultatu. Prawdziwą wartością jest nawiązanie współpracy, która dzięki wspólnym wysiłkom może przynieść lepszy skutek dla zespołów bezpieczeństwa informacji pod względem poprawy efektywności, redukcji kosztów oraz strat. Z badania A.T. Kearney przytoczonych w opracowaniu „The Golden Rules of Operational Excellence in Information Security Management" wynika, że wiele organizacji dzieli się wiedzą i stosowanymi praktykami z innymi podmiotami, szczególnie wśród

odpowiedników branżowych i odpowiadających wielkością. Powodem jest to, że dzielenie się najlepszymi praktykami może pomóc w zwiększaniu efektywności we wczesnym wykrywaniu zagrożeń i zmniejszaniu poziomu ryzyka, ograniczając konieczność samodzielnej walki z nimi. Najbardziej doświadczone organizacje często współpracują poprzez branżowe stowarzyszenia.

Czy współpracujesz lub porównujesz swą działalność w zakresie bezpieczeństwa informacji z innymi podmiotami?



Źródło: *A.T. Kearney*

Organizacje branżowe

Organizacje finansowe w wielu krajach w Europie i na świecie doszły do przekonania, iż współpraca w zakresie cyberbezpieczeństwa niesie istotne korzyści i stworzyły różne formy podmiotów zajmujących się walką z cyberprzestępczością i innymi zagrożeniami internetowymi. Z ciekawszych przykładów, jakie można przedstawić, jest FinansCERT z Norwegii.

FinansCERT Norwegia został formalnie powołany 23 kwietnia 2013 r. przy branżowej instytucji zrzeszającej organizacje finansowe w wyniku podjęcia przez sektor finansowy wspólnego wysiłku w zwalczaniu ataków i zagrożeń cyberprzestępczością. W momencie powstawania pozytywnie odniósł się do tej inicjatywy norweski nadzór finansowy, podobny był również oddźwięk medialny. Powstanie FinansCERT poprzedziła trwająca formalnie od 2007 r. współpraca banków w zakresie wymiany informacji o atakach na internetowe usługi bankowe. Współpraca doprowadziła do szybszego wykrywania nadużyć oraz sprawniejszej walki z phishingiem. W wyniku tych doświadczeń oraz konsul-

tacji branżowych narodziła się koncepcja organizacji, która wzmocni sektor finansowy w przeciwdziałaniu przestępstwom internetowym.

Organizacja ta pełni rolę CERTu (z ang. *Computer Emergency Responce Team*) dla norweskiego sektora finansowego – bankowego i ubezpieczeniowego – i jest to na dzień dzisiejszy jedyny CERT branży finansowej, niezależny od wewnętrznch CERTów banków. FinansCERT ma kilka zadań:

- aktywne śledzenie zagrożeń zewnętrznych,
- funkcja pogotowia ratunkowego – wsparcie w zwalczaniu ataku i ograniczaniu strat,
- koordynacja współpracy z instytucjami publicznymi i służbami porządkowymi (Policja, Europol/EC3).

FinansCERT współpracuje z innymi podmiotami o podobnym charakterze (narodowy CERT, CERTy innych branż), również zagranicznymi, a także z operatorami internetowymi i telekomunikacyjnymi (m.in. w zakresie blokowania domen), ma dostęp do informacji wywiadowczych.

Organizacja ma duże znacznie dla sektora, m.in. z powodu faktu, iż ograniczona liczba banków ma sprawnie działające CERTy, ale także dlatego, że ma własne laboratorium do analizy malware'u. W ocenie ekspertów E&Y sukces tej organizacji wynika m.in. z kultury otwartości i braku mentalnych przeszkód w zakresie wymiany informacji.

Budżet FinansCERT w momencie powstania wynosił 4,2 mln koron (czyli ok. 2 mln zł), a pełne koszty działalności oszacowano na 11 mln koron z uwzględnieniem kosztów współpracy z wyspecjalizowanymi podmiotami trzecimi zapewniającymi wiedzę operacyjną. Koszty FinansCERT Norwegii są pokrywane przez instytucje finansowe, na rzecz których organizacja ta działa, przy czym według założeń część to opłata stała w wysokości ok. 40% budżetu, pozostałe koszty są dzielone w proporcji wynikającej z liczby klientów bankowości elektronicznej mierzonej liczbą podpisanych umów. Spółka zatrudnia 4 osoby, pozostałą obsadę stanowią oddelegowani pracownicy innych banków, co stanowi efektywny operacyjny link między FinansCERT i podmiotami branży.

Organizacji branżowych zajmujących się zagrożeniami bezpieczeństwa informacji jest wiele, oto przykłady:

Przykłady organizacji	sektor	kraj	własność	dzielenie się wiedzą	współpraca w czasie rzeczywistym	doradztwo i przeciw-działanie	audyty, badania bezpieczeństwa	ostrzeżenia i rzeczy-wiste działania	inne istotne aktyw-ności
National Cyber-Forensics& Training Alliance (NCFTA)	różne	USA/glo-balna	prywatna	X	X	X	X	X	
Financial Services Information Sharing and Analysis Center (FS-ISAC)	finan-sowy	USA/glo-balna	prywatna	X		X	X		
Soltra	różne	USA/glo-balna	prywatna	X	X	X	X		
European Financial Institutes –Informa-tion Sharing and Analysis Centre (FI-ISAC)	finan-sowy	UE	prywatno -publiczna	X		X			współpraca z Europol EC3
Cyber Security Coordination Group (CSCG)	różne	UE	prywatno -publiczna	X		X			standardy cyberbez-pieczeństwa
EuropeanCyberCri-meCentre (EC3)	różne	UE	prywatno -publiczna	X				X	szkolenia i budowa potencjału
EuropeanOrgani-zation for Security (EOS)	różne	Europa	prywatna	X		X			
Deutsche CyberSi-cherheits-Organisa-tion(DCSO)	różne	Niemcy	prywatna	X		X	X	X	publiczne forum cyberbezpieczeństwa
Cyber Security Sharing and Analyt-ics (CSSA)	różne	Niemcy	prywatna	X		X			
Cyber-security Information Sharing Partnership (CiSP)	różne	Wielka Brytania	prywatno -publiczna	X	X	X	X	X	
CBEST	finan-sowy	Wielka Brytania	prywatno -publiczna			X	X		
Cyber Essentials	różne	Wielka Brytania	prywatno -publiczna			X	X		certyfikacja firm małych i średnich
Financial Crime Alerts Service (FCAS) – w stadium powstawania	finan-sowy	Wielka Brytania	prywatno -publiczna	X	?	?	?	?	

Źródło: *A.T. Kearney*

Ciekawym przykładem z ojczyzny Internetu jest NCFTA – National Cyber-Forensics & Training Alliance (Narodowe Stowarzyszenie Informatyki Śledczej i Szkoleń). Jest to powstała w 2002 r. organizacja non-profit z siedzibą w Pittsburghu, koncentrująca się na identyfikacji, łagodzeniu oraz neutralizowaniu zagrożeń cyberprzestępczością. Stowarzyszenie koordynuje wymianę informacji o zagrożeniach w czasie rzeczywistym, współpracując blisko z ekspertami branżowymi oraz instytucjami akademickimi, identyfikuje zagrożenia w celu podjęcia środków zapobiegawczych w celu złagodzenia lub uniknięcia skutków potencjalnych ataków. W zakresie aktywności NCFTA są strumienie działań na rzecz branży finansowej i handlu elektronicznego, ale nie tylko – obecnie działa na rzecz ponad 100 organizacji z różnych branż z całego świata, w tym telekomunikacji, przemysłu wytwórczego, farmaceutycznego, energetyki. NCFTA dysponuje własnym laboratorium analizy malware współpracującym z bankami, dysponuje również specjalistami i potencjałem do analizy przeprowadzonych ataków, aby badać scenariusze ich przeprowadzenia wraz z możliwymi wariantami i przekazywać zdobytą wiedzę swoim członkom.

Na szczeblu europejskim działa kilka organizacji wspierających zwalczanie zagrożeń cyberprzestępczością. European Cybercrime Centre (EC3) skupia się na przestępstwach w Internecie – centralizuje informacje o cyberprzestępstwach i wspiera operacje członków Unii Europejskiej w zakresie ich zwalczania, specjalizując się w informatyce śledczej. European Financial Institutes –Information Sharing and Analysis Centre (FI-ISAC) ma rolę informacyjną dla bezpieczeństwa sektora finansowego, wpierając wymianę informacji o zagrożeniach w kanałach elektronicznych, systemach centralnych, kartowych, stanowiąc źródło informacji o potencjalnych ryzykach i nowych scenariuszach ataków. Z kolei Cyber Security Coordination Group (CSCG) jest organizacją wspierającą standaryzację w zakresie bezpieczeństwa informatycznego, stanowiąc źródło rekomendacji dla Komisji Europejskiej w tworzeniu ustawodawstwa, współpracując z innymi podobnymi agendami w innych krajach.

W poszczególnych państwach funkcjonują instytucje wspierające operacyjnie walkę z zagrożeniami i atakami. Przykład niemieckiego DCSO jest interesujący o tyle, że wspólną inicjatywę podjęły firmy Allianz, BASF, Bayer i Volkswagen, a wiec z branż tak odległych, jak finanse, farmacja, motoryzacja i chemia. Uznano jednak, że wiele scenariuszy ataków i zagrożeń jest wspólnych, a wobec tego współpraca może przynieść wszystkim ewidentne korzyści. DCSO zajmuje się koncentracją wiedzy specjalistycznej, wymianą informacji, świadczy usługi wczesnego ostrzegania oraz audyty.

Bogaty dorobek w organizowaniu się przeciw cyberprzestępczości ma Wielka Brytania – funkcjonuje tam kilka organizacji o różnym charakterze, od pełniących funkcję wczesnego ostrzegania i doradztwa (Cyber-security Information Sharing Partnership – CiSP), testowania i weryfikacji zabezpieczeń instytucji finansowych kontrolowanymi atakami opracowanymi na podstawie analizy rzeczywistych ataków (CBEST) oraz opracowywania standardów, wytycznych i certyfikacji dla sektora przedsiębiorstw (Cyber Essentials). Obecnie rozwijana jest organizacja Financial Crime Alerts Service (FCAS), która zajmować się będzie wymianą informacji wywiadowczych w czasie rzeczywistym, tak aby wesprzeć banki w walce z przestępstwami. FCAS wywodzi się z wprost z organizacji JMLIT (z ang. *Joint Money Laundering Intelligence Taskforce*), powstałej w lutym 2015 r. w wyniku działań podmiotów sektora finansowego (w tym Lloyds, Santander, HSBC, Nationwide, RBS, Barclays), zrzeszenia banków BBA oraz instytucji publicznych, takich jak Home Office (odpowiedzialne za sprawy wewnętrzne, w tym walkę z przestępczością), czy londyńska Policja. JMLIT z założenia ma służyć wymianie informacji o praniu brudnych pieniędzy oraz innych przestępstwach o charakterze ekonomicznym. Sektor bankowy w Wielkiej Brytanii ma motywację, aby skutecznie walczyć z przestępczością internetową – jak podaje BBA roczne straty sektora z tego tytułu to 24 mld funtów.

Bankowe Centrum Cyberbezpieczeństwa

W Polsce o konsolidacji sektora bankowego w zakresie wspólnej walki z cyberprzestępczością mówiło się od kilku lat. Milowym kamieniem było przyjęcie przez VI Europejski Kongres Finansowy, odbywający się w dniach 13–15 czerwca 2016 r., Rekomendacji w zakresie Cyberbezpieczeństwa Sektora Finansowego, która dotyczyła m.in. powołania organizacji/jednostki międzybankowej koordynującej działania w zakresie wymiany informacji o wektorach ataków na poszczególnych uczestników sektora, we współpracy z regulatorem, nawiązania współpracy przez banki i inne instytucje monitorujące bezpieczeństwo oraz podjęcia działań prewencyjnych i edukacyjnych (pełna treść rekomendacji dostępna jest pod linkiem http://www.efcongress.com/pl/cyberbezpieczestwo-sektora-finansowego). Rekomendacja ta istotnie przyczyniła się do przyśpieszenia prac i zmaterializowania idei Bankowego Centrum Cyberbezpieczeństwa.

Z inicjatywy Rady Bankowości Elektronicznej działającej przy ZBP we wrześniu 2015 r. wydana została Rekomendacja Związku Banków Polskich dotycząca bezpieczeństwa oraz zapobiegania niedostępności bankowości elektronicznej, w której rekomenduje się m.in. żeby banki zrzeszone w ZBP nawiązały współpracę w ramach sektora bankowego w szczególności w zakresie:

a) przeciwdziałania atakom na systemy bankowości elektronicznej oraz klientów bankowości elektronicznej,
b) reagowania na zaistniałe ataki.

Jako pierwszy krok do realizacji tego celu (na podstawie w/w rekomendacji) rozpoczęto prace nad powołaniem międzybankowej struktury organizacyjnej, do zadań której należy zaliczyć przede wszystkim:

- stworzenie infrastruktury umożliwiającej w sytuacji kryzysowej uruchomienie i funkcjonowanie sztabu kryzysowego,
- przygotowanie procedur zarządzania sytuacją kryzysową, a w szczególności technicznych i proceduralnych rekomendacji, działań w sytuacji kryzysowej, uwzględniających różnorodne scenariusze ataków,
- przygotowanie systemu komunikacji w trybie 24/7/365,
- opracowanie działań i rekomendacji do realizacji w trybie normalnego działania,
- zbudowanie aktualnej bazy wymiany informacji o zagrożeniach, kontach „słupów" czy innych danych wskazujących na podejrzanych klientów w sektorze,
- zobligowanie wszystkich uczestników do bieżącego przekazywanie informacji o zagrożeniach, wykrytych atakach i przestępczych kontach/klientach/transakcjach w celu prewencyjnego wykorzystania przez pozostałych uczestników,
- wypracowanie kanałów komunikacji i procedur współpracy z jednostkami zewnętrznymi, w tym z instytucjami odpowiedzialnymi za bezpieczeństwo publiczne, organizacjami typu CERT oraz producentami oprogramowania i systemów zabezpieczeń,
- wypracowanie propozycji zmian w przepisach prawa powszechnie obowiązującego w celu umożliwienia implementacji wypracowanych działań.

Prace prowadzone w październiku i listopadzie 2015 r. doprowadziły do utworzenia Bankowego Centrum Cyberbezpieczeństwa (BCC) – struktury, która do czasu powstania odrębnej instytucja działa przy ZBP.

Wpisuje się ona w europejskie i krajowe trendy porządkujące sferę walki z zagrożeniami cyberprzestępczością, w tym wdrażaną dyrektywę UE Network and Information Security (NIS) w zakresie centralizacji współpracy w zwalczaniu przestępstw internetowych, a także powstającej strategii Cyberbezpieczeństwa Państwa, w której założeniach istotną rolę w zwalczaniu ataków internetowych pełnić mają CERTy branżowe.

BCC posiada strukturę hierarchiczną składającą się z:

- Komitetu Sterującego,
- Grupy Zarządzania Cyberbezpieczeństwem Banków,
- Grupy Operacyjnej.

Opracowano szereg procedur regulujących działanie BCC, wybrano tymczasową platformę komunikacyjną (wymiany informacji o zdarzeniach z zakresu cyberbezpieczeństwa), wypracowano mechanizm dyżurów banków w ramach których śledzona i analizowana jest sytuacja w sektorze bankowym.

W razie konieczności BCC przekształca się w Sztab Kryzysowy posiadający możliwości zarządzania sytuacja kryzysową dotyczącą cyberbezpieczeństwa w sektorze bankowym.

Należy zaznaczyć, że BCC na stałe współpracuje z przedstawicielami Policji oraz Krajowej Izby Rozliczeniowej. Inicjatywa spotkała się z bardzo przychylnym przyjęciem Komisji Nadzoru Finansowego. W ramach prac BCC nawiązywane są kontakty z operatorami telekomunikacyjnymi, giełdami bitcoin, operatorami szybkich płatności oraz innymi instytucjami, które w sposób pośredni wpływają na bezpieczeństwo sektora.

W chwili obecnej działalność BCC koncentruje się na następujących obszarach:

1. Prowadzenie stałego monitoringu sytuacji sektora w zakresie cyberbezpieczeństwa i w razie potrzeby podejmowanie stosownych działań (w tym powołanie Sztabu Kryzysowego w razie potrzeby).
2. Opracowanie i wdrożenie technicznych rozwiązań wykorzystywanych na potrzeby bieżącego funkcjonowania struktury oraz na wypadek zarządzania sytuacją kryzysową.
3. Opracowanie, rekomendowanie i monitorowanie wdrożenia oraz nadzór nad aktualnością procedur niezbędnych do realizacji w przypadku wystąpienia sytuacji kryzysowej i na czas „pokoju".
4. Zarządzanie komunikacją.

- Opracowanie ogólnobankowej, spójnej polityki informacyjnej w stosunku do mediów i klientów, opartej na założeniu, że w przypadku zagrożenia cyberbezpieczeństwa lub awarii informatycznych systemów związanych bezpośrednio lub pośrednio z bankowością elektroniczną (skutkujących istotnym ograniczeniem obsługi klientów), banki o tych zdarzeniach będą niezwłocznie informowały.
- Wypracowanie systemu i procedur komunikacji między uczestnikami.
- Wypracowanie kanałów komunikacji i procedur współpracy m.in. z Policją, ABW, firmami typu CERT, producentami oprogramowania oraz systemów zabezpieczeń (np. IBM, Microsoft, Symantec, itp.).
- Wyposażenie uczestników w możliwości techniczne pozwalające na zaimplementowanie powyższej komunikacji.

5. Definiowanie, uzgodnienie terminów realizacji oraz monitorowanie wdrożenia działań prewencyjnych na poziomie sektora i banków o realizacji w warunkach bieżącego (nie kryzysowego) funkcjonowania sektora bankowego.
6. Przygotowanie i monitorowanie realizacji programu podnoszenia świadomości, aktywności w tym temacie (ze względu na tymczasowość dokumentu zestaw przytoczonych poniżej działań ma charakter przykładowy i stanowi zbiór otwarty).
7. Podejmowanie wspólnych przedsięwzięć na arenie międzybankowej.

Równolegle do operacyjnej działalności trwają prace nad dalszym rozwojem Bankowego Centrum Cyberbezpieczeństwa. Przedstawiciele branży dostrzegają korzyści z wymiany informacji i wyciąganiu wniosków dla całego sektora (choćby łączenie incydentów w sprawy), toczące się prace obejmują m.in. zdefiniowanie zakresu innych usług, które stanowiłyby wartość dla sektora, uwzględniając potrzeby zarówno dużych podmiotów z rozwiniętymi strukturami zarządzania bezpieczeństwem informacji, jak też mniejszych, które potencjalnie mogłyby istotnie zyskać dzięki współpracy branżowej.

Analizowane są m.in. możliwości sprawnej współpracy BCC z podmiotami innymi niż instytucje finansowe – tak, jak czynią to podobne organizacje w innych krajach – pozostając w zgodzie z lokalnym prawodawstwem, szczególnie w zakresie ustawy Prawo Bankowe i ograniczeniach w zakresie udostępniania informacji mogącej stanowić tajemnicę bankową. Planowany jest również rozwój współpracy z giełdami wirtualnej waluty i innymi podmiotami, które mogą w sposób aktywny ograniczać skalę przestępstw realizowanych przez Internet.

Maciej Gawroński

Partner zarządzający w polskim biurze kancelarii Bird & Bird.

Ma ponad 20-letnie doświadczenie w doradztwie z zakresu prawa nowych technologii, IT, jak również outsourcingu oraz bankowości i finansów. Doradzał przy kilkuset projektach wdrożeń informatycznych, w tym przy największym wdrożeniu w sektorze finansowym w Polsce. Od 2009 r. zajmuje się zagadnieniami cloud computingu i jest jednym z najbardziej poważanych ekspertów w tym obszarze w Polsce. Ekspert Komisji Europejskiej ds. Kontraktów Cloud Computingowych i konsultant Grupy Roboczej Artykułu 29. Ekspert prawny Krajowej Izby Gospodarczej. Redaktor i współautor Raportu Związku Banków Polskich „Cloud Computing w sektorze finansowym – regulacje i standardy" (2011), współautor raportu Związku Banków Polskich „Cloud computing 2013". Autor publikacji „Aspekty prawne cloud computingu w odniesieniu do sektora bankowego (regulacje EU)" (2014). Współautor analizy wykonalności wdrożenia cloud computingu w administracji publicznej w Polsce (2014). Współautor książki „Wyzwania Informatyki Bankowej" (2014, 2015). Jest także wykładowcą studiów podyplomowych Szkoły Głównej Handlowej „Zastosowanie technologii cloud computingu w modelowaniu biznesowym".

Sławomir Szepietowski

Partner kierujący praktyką bankowości i finansów w polskim biurze Bird & Bird. Ma ponad 18-letnie doświadczenie w doradztwie dla sektora bankowego i finansowego, które zdobył pracując w instytucjach bankowych oraz międzynarodowych kancelariach prawniczych. Specjalizuje się w obsłudze prawnej instytucji finansowych, w tym banków, spółek publicznych i funduszy inwestycyjnych, w zakresie pełnej oferty biznesowej, corporate governance, jak i wymogów regulacyjnych. Pracuje przy transakcjach na rynku finansowym, w tym dotyczących finansowania kredytem, emisji papierów dłużnych, instrumentów pochodnych oraz rynku private equity. Posiada szerokie doświadczenie w obsłudze międzynarodowych instytucji finansowych w procesie wchodzenia na polski rynek (działalność transgraniczna, tworzenie oddziałów przedsiębiorstw zagranicznych, otwieranie nowych linii biznesowych). Jest doświadczonym koordynatorem prac zespołów prawników obsługujących określone linie biznesowe i projekty. Nagrodzony przez Związek Banków Polskich za wkład w rozwijanie praktyki bankowej w Polsce. Ekspert prawny Krajowej Izby Gospodarczej.

Adam Łukaszewski

Junior Associate w zespole prawa bankowości i finansów w polskim biurze Bird & Bird.

Zajmuje się kwestiami regulacyjnymi z zakresu rynków i usług finansowych, w tym wprowadzaniem nowych produktów na rynek oraz rozpoczynaniem działalności przez podmioty zagraniczne. W zakres jego specjalizacji wchodzą również transakcje finansowania oraz zagadnienia prawa cywilnego i bankowego, w szczególności kwestie regulacji publicznoprawnych. Ma doświadczenie w sporządzaniu i negocjowaniu dokumentacji finansowych, zwłaszcza dokumentacji zabezpieczeń. Przygotowuje liczne opinie i analizy prawne. Uczestniczył w procesie nadzoru spełniania warunków wypłat kredytów oraz w postępowaniach rejestrowych. Pracuje dla klientów z sektora bankowego oraz branży IT.

Maciej Gawroński, Sławomir Szepietowski,
Adam Łukaszewski, Bird & Bird

PSD 2 – nowa wersja dyrektywy w sprawie usług płatniczych

Rynek płatności elektronicznych i mobilnych to jeden z bardziej dynamicznie rozwijających się obszarów usług płatniczych. W ślad za tym powstają nowe i coraz mocniej rozbudowane produkty w ramach e-commerce wymagające lepszych i wydajniejszych narzędzi informatycznych. W związku z tak intensywnym rozwojem w obecnym systemie prawnym pojawiły się luki, których uregulowanie jest niezbędne, aby zapewnić jednolite standardy i minimalny poziom bezpieczeństwa. W sukurs ma przyjść dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego[1] („**Dyrektywa PSD 2**"), która istotnie zmieni europejski rynek e-commerce i krajobraz usług płatniczych. Jej implementacja pociągnie za sobą nie tylko nowelizację ustawy z 19 sierpnia 2011 r. o usługach płatniczych[2] („**Ustawa o usługach płatniczych**"), ale i spore zmiany w modelu funkcjonowania dostawców usług płatniczych, które dotkną wielu obszarów ich codziennej działalności, m.in. regulaminów, wzorów umów, procedur, infrastruktury informatycznej czy relacji z organami nadzoru. Dyrektywa PSD 2 wpłynie także na sektor bankowy, ustanawiając nowe zasady współpracy banków z innymi podmiotami świadczącymi usługi płatnicze, np. przyznając tym ostatnim więcej swobody w samodzielnym, niezależnym od banków, oferowaniu tego typu usług. Proces dostosowania się do nowych przepisów może wymagać sporych nakładów i zasadniczo jedynie poprzez odpowiednie działania wyprzedzające można będzie zminimalizować ryzyko wystąpienia zakłóceń. Innymi słowy, należy spodziewać się zmienionego kształtu polskiego i europejskiego rynku usług płatniczych. Niniejszy artykuł ma na celu przedstawienie najważniejszych skutków prawnych Dyrektywy PSD 2.

1 Dz. Urz. UE L 337 z 23 grudnia 2015 r.

2 Dz. U. z 2011 r. Nr 199, poz. 1175, ze zm.

PSD 2 w pigułce

Poszerzenie zakresu stosowania PSD 2	Nowe regulowane usługi płatnicze – usługa inicjowania płatności oraz usługa dostępu do informacji o rachunku	
	Redukcja katalogu wyłączeń odnośnie m.in. mikropłatności za treści cyfrowe, pośrednictwa agenta handlowego i ograniczonej sieci	
Usługa inicjowania płatności	Zostanie objęta ustawą o usługa płatniczych – wymóg uzyskania licencji KNF oraz spełnienia określonych wymogów regulacyjnych	
	Umożliwia natychmiastową płatność za towar lub usługę	Bank będzie musiał zapewnić dostęp do swojej infrastruktury
Usługa dostępu do informacji o rachunku	Zostanie objęta ustawą o usługach płatniczych – jedynie wymóg rejestracji i ograniczony zakres stosowania wymogów regulacyjnych	
	Analiza i przetwarzanie danych z wielu rachunków	Bank będzie musiał zapewnić dostęp do swojej infrastruktury
Pozostałe skutki prawne	Wzmocnienie pozycji organów nadzorczych	Zakaz pobierania dodatkowych opłat (*surcharge*)
	Nowe regulacje dot. nieautoryzowanych transakcji	Nowe środki bezpieczeństwa w zakresie ochrony danych

Rozszerzenie zakresu stosowania Dyrektywy PSD 2

Komisja Europejska wskazała na potrzebę uregulowania nowych obszarów usług płatniczych oraz doprecyzowania obecnie obowiązujących regulacji. W związku z powyższym, w porównaniu do pierwotnej wersji dyrektywy oznaczonej numerem 1 wprowadzono następujące zmiany:

- uregulowano nowe usługi płatnicze, w tym dostęp do informacji o rachunku oraz inicjowanie płatności (więcej na ten temat w dalszej części artykułu),
- objęto Dyrektywą PSD 2 transakcje z krajami trzecimi, gdy tylko jeden z dostawców usług płatniczych znajduje się na terenie UE,
- w sposób pośredni poszerzono zastosowanie Dyrektywy PSD 2 poprzez m.in.:

- Sprecyzowanie katalogu wyłączonych spod Dyrektywy PSD 2 transakcji płatniczych przeprowadzanych za pośrednictwem dostawcy sieci lub usług łączności elektronicznej – przykładowo, będzie to zakup treści cyfrowych takich jak filmy, pliki muzyczne czy gry mobilne za pośrednictwem operatora telekomunikacyjnego, o ile nie przekroczy się określonych limitów (tj. 50 euro dla pojedynczej transakcji lub 300 euro w przypadku wszystkich transakcji w danym miesiącu).
- Obecnie obowiązujące przepisy wywołują wątpliwości interpretacyjne (nie ma chociażby wspomnianych wyżej jasno określonych limitów), więc prawodawca europejski postanowił je doprecyzować, oraz wprowadzić zmianę zasad funkcjonowania tzw. ograniczonej sieci opierającej się na tym, że wydawane w jej ramach instrumenty płatnicze można wykorzystywać jedynie w ograniczony sposób (tj. w szczególności, gdy obejmuje ona limitowany asortyment towarów lub usług) – przykładowo będą to karty sklepowe w ramach programów lojalnościowych, karty transportu publicznego czy karty wydawane na stacjach benzynowych.
- W związku z tym, że obecne przepisy nie są jednoznaczne, zdarzało się, że płatności w ramach tzw. ograniczonych sieci osiągały spore wolumeny i dotyczyły tysięcy różnych produktów oraz usług. Dyrektywa PSD 2 zakłada, że podmiot prowadzący tzw. ograniczoną sieć będzie musiał wystosować do właściwego organu powiadomienie, gdy całkowita wartość transakcji płatniczych wykonanych podczas ostatnich 12 miesięcy w ramach tzw. ograniczonej sieci przekracza 1 mln euro. Na podstawie tego powiadomienia, w przypadku gdy dany rodzaj działalności nie kwalifikuje się jako działalność w ramach tzw. ograniczonej sieci, właściwy organ może nawet wydać decyzję o zakazie prowadzenia tej działalności.

Obecnie działające instytucje płatnicze w kontekście przepisów przejściowych – ponowne przyznawanie zezwoleń

Dyrektywa PSD 2 w stosunku do obecnie działających podmiotów reguluje kwestię ponownego przyznawania zezwoleń na działalność regulowaną w zakresie usług płatniczych w następujący sposób:

- Obowiązkowo państwa członkowskie wymagają, aby obecnie działające instytucje płatnicze przekazały właściwym organom wszystkie stosowne informacje w celu umożliwienia przeprowadzenia oceny tego, czy insty-

tucje te spełniają określone wymogi regulacyjne zawarte w Dyrektywie PSD 2, a jeżeli nie spełniają, to jakie środki trzeba podjąć w celu zapewnienia zgodności, lub czy odpowiednim środkiem jest cofnięcie zezwolenia.

- W związku z powyższym obowiązkiem przekazywania informacji, jeżeli właściwe organy państwa członkowskiego wejdą w posiadanie dokumentacji potwierdzającej spełnienie wymogów regulacyjnych ustanowionych w Dyrektywie PSD 2, to mogą one automatycznie udzielić zezwolenia (ewentualnie wpisać do stosownych publicznych rejestrów, jeżeli zezwolenie nie jest wymagane) instytucjom płatniczym, które do dnia 13 stycznia 2018 r. (tj. końcowej daty implementacji Dyrektywy PSD 2 do krajowego porządku prawnego) podjęły zgodnie z prawem działalność w zakresie usług płatniczych.
- Jeżeli państwa członkowskie zrezygnują z możliwości automatycznego przedłużania zezwolenia, to właściwe organy tych państw, na podstawie przekazanych danych od instytucji płatniczych, będą musiały w sposób pozytywny albo negatywny rozstrzygnąć w drodze decyzji kwestię wydania zezwolenia albo wpisu do właściwego rejestru w kontekście spełnienia przez obecnie działające instytucje płatnicze wymogów przewidzianych przez Dyrektywę PSD 2.
- Szczególna regulacja przewidziana jest dla osób prawnych, które przed dniem 12 stycznia 2016 r. prowadziły na terytorium tych państw usługę inicjowania płatności i usługę dostępu do informacji o rachunku – w stosunku do nich państwa członkowskie nie mogą zakazać kontynuowania tej samej działalności w okresie przed implementacją przepisów Dyrektywy PSD 2, jeżeli tylko odbywa się to zgodnie z aktualnie mającymi zastosowanie przepisami regulacyjnymi.

Usługa inicjowania płatności (PIS)

Usługa tego typu jest już dawno stosowana w praktyce świadczenia usług płatniczych[3], lecz dopiero Dyrektywa PSD 2 przewiduje, że państwa członkowskie będą musiały ją uregulować i zapewnić stosowne ramy prawne. Można wyróżnić cztery podmioty, które pośrednio lub bezpośrednio są zaangażowane w operacje odbywające się w ramach struktury tej usługi:

3 Wśród podmiotów świadczących tego typu usługi można wymienić SOFORT GmbH działającą głównie w Niemczech, IDeal operującą na rynku holenderskim czy Trustly z główną siedzibą mieszczącą się w Szwecji.

- Płatnik (posiadacz rachunku bankowego), a więc potencjalny nabywca oferowanych w sieci produktów i usług – jako dysponentowi środków zgromadzonych na rachunku zależy mu na błyskawicznej realizacji płatności w celu szybszego dostarczenia zakupionego towaru lub natychmiastowego dostępu do zakupionej usługi.
- Dostawca usługi bądź produktu (w szczególności sklep internetowy), który w ramach handlu elektronicznego jest zainteresowany spełnieniem oczekiwań klientów w zakresie natychmiastowych płatności, ale także szybkim uzyskaniem informacji czy nabywca posiada wystarczające środki do zakupu danego produktu czy usługi.
- Tzw. podmiot trzeci (z ang. *third party payment service provider*), a konkretnie dostawca świadczący usługę inicjowania płatności pełniący niejako funkcję pośrednika – na polskim rynku taką usługę oferuje chociażby Sofort, który nawet wszedł w medialny spór z Komisją Nadzoru Finansowego („**KNF**") odnośnie jej bezpieczeństwa.
- Instytucja finansowa prowadząca rachunek płatnika, którą najczęściej będzie bank.

Podmiot oferujący usługę inicjowania płatności z rachunku bankowego dostarcza interfejs programowy czy też bazę informatyczną umożliwiającą natychmiastowy przepływ stosownych danych odnośnie płatności między stroną internetową sprzedawcy a platformą bankowości internetowej. Zgodnie z Dyrektywą PSD 2 usługa inicjowania płatności stanie się usługą płatniczą i jako taka będzie wymagała zezwolenia Komisji Nadzoru Finansowego. Obecnie usługa ta nie jest regulowana i np. wspomniany już Sofort nie jest wpisany do rejestru usług płatniczych prowadzonego przez KNF. Zgodnie z Dyrektywą PSD 2 wśród warunków uzyskania zezwolenia na świadczenie usługi inicjowania płatności można wymienić m.in. dysponowanie kapitałem założycielskim w minimalnej wysokości 50 tys. euro czy konieczność posiadania ubezpieczenia odpowiedzialności z tytułu prowadzenia działalności zawodowej albo porównywalnej gwarancji. Działalność ograniczająca się wyłącznie do świadczenia usługi inicjowania płatności lub usługi dostępu do informacji o rachunku jest traktowana preferencyjnie w zakresie wymogów natury regulacyjnej (na przykład odnośnie posiadania funduszy własnych).

Natomiast w przypadku, gdy dostawca świadczący usługę inicjowania płatności zamierza świadczyć inne usługi płatnicze, w związku z którymi wejdzie w posiadanie środków pieniężnych użytkownika, będzie musiał spełnić

dodatkowe wymogi w celu uzyskania zezwolenia na ich świadczenie. Ponadto dostawca usługi powinien przestrzegać stosownych przepisów w zakresie ochrony danych i bezpieczeństwa transakcji, szczególnie że korzystanie z tej usługi często polega na bezpośrednim podaniu przez klienta indywidualnych danych uwierzytelniających, w tym loginu i hasła do konta bankowego.

Obecnie skorzystanie z tego typu „poszerzonej" usługi w Polsce tworzy ryzyko prawne chociażby w zakresie naruszenia postanowień umowy o prowadzenie rachunku bankowego bądź integralnie z nią związanego regulaminu danej instytucji finansowej. Co więcej, KNF wydała nawet ostrzeżenie przed dopuszczeniem pośredników do rachunku bankowego w płatnościach internetowych[4]. W zupełnie przeciwnym kierunku podąża Dyrektywa PSD 2, która wyraźnie wskazuje, że państwa członkowskie będą musiały zapewnić, by konsument miał prawo do korzystania z usługi inicjowania płatności. Z kolei banki prowadzące rachunek nie będą mogły stawiać nieprzewidzianych prawem wymogów, a podmioty świadczące usługę inicjowania płatności będą zasadniczo zobowiązane jedynie do uzyskania zezwolenia od kompetentnego organu publicznego. Co więcej, świadczenia usług inicjowania płatności nie będzie można uzależniać od istnienia stosunku umownego pomiędzy dostawcami świadczącymi tego typu usługę a bankami prowadzącymi rachunek do tego celu. Wyraźnie więc widać, że Dyrektywa PSD 2 ma na celu większe otwarcie rynku usług płatniczych na tzw. podmioty trzecie, a państwa członkowskie będą musiały stworzyć ku temu odpowiednie ramy prawne. W Polsce istnieją już analogiczne usługi, takie jak choćby Express Elixir oferowany przez Krajową Izbę Rozliczeniową czy przelew ekspresowy w systemie BlueCash, które powinny spodziewać się teraz większej konkurencji na rynku. Same standardy techniczne w zakresie komunikacji między systemami dostawców usług płatniczych prowadzących rachunek bankowy a podmiotami trzecimi (tj. w szczególności dostawcami świadczącymi usługę inicjowania płatności i usługę dostępu do informacji o rachunku) zostaną opracowane przez Europejski Urząd Nadzoru Bankowego („**EUNB**").

Usługa dostępu do informacji o rachunku (AIS)

Usługa dostępu do informacji o rachunku, podobnie jak usługa inicjowania płatności, jest kolejną usługą płatniczą świadczoną na zasadzie dostępu do rachunku przez podmioty trzecie.

4 http://www.knf.gov.pl/Images/KNF_podawanie_danych_dostepu_do_rachunku_18_11_2013_tcm75-36300.pdf

Zagraniczne podmioty profesjonalnie trudnią się taką działalnością już od kilkunastu lat, a ich wartość rynkowa sięga nawet kilkuset milionów dolarów[5]. W Polsce tego typu usługę (jeszcze oficjalnie nieuregulowaną) oferuje chociażby Kontomierz.pl. Usługa ta zapewnia użytkownikowi możliwość uzyskania zagregowanej informacji na temat wszystkich rachunków posiadanych przez tego użytkownika w różnych instytucjach finansowych. W jej ramach możliwa jest również analiza oraz przetwarzanie danych płynących z posiadanych rachunków w celu optymalizacji polityki użytkownika w kontekście chociażby planowania wydatków czy zarządzania swoimi finansami. Osoby fizyczne lub prawne, świadczące wyłącznie usługę dostępu do informacji o rachunku, są zwolnione z konieczności uzyskania zezwolenia i spełnienia wiążących się z tą procedurą wymogów regulacyjnych. Niemniej będą musiały złożyć wniosek o zarejestrowanie oraz będą traktowane jako instytucje płatnicze, do których należy stosować odpowiednie przepisy Dyrektywy PSD 2 (w szczególności w zakresie obowiązków informacyjnych względem użytkowników tego typu usług). Podobnie jak w przypadku usługi inicjowania płatności państwa członkowskie muszą zapewnić, by użytkownik usług płatniczych miał prawo do korzystania z usług umożliwiających dostęp do informacji o rachunku. Dostawca usług płatniczych prowadzący rachunek (tj. zasadniczo bank) nie będzie mógł odmówić dostępu do danego rachunku płatniczego, chyba że będzie to uzasadnione obiektywnymi i należycie udokumentowanymi względami (np. nieuprawnione lub nielegalne zainicjowanie usługi). Z drugiej strony nie można używać, uzyskiwać ani przechowywać żadnych danych do celów innych niż do wykonania usługi dostępu do informacji o rachunku świadczonej na podstawie wyraźnej zgody użytkownika (tj. posiadacza poszczególnych rachunków).

Wzmocnienie pozycji organów nadzoru

Dyrektywa PSD 2 rozszerza zakres współpracy i wymiany informacji pomiędzy odpowiednimi organami nadzoru państw członkowskich. W znaczący sposób akcentuje również silną rolę nadzorczo-regulacyjną EUNB będącego częścią Europejskiego Systemu Nadzoru Finansowego. Wśród najważniejszych zadań EUNB na mocy Dyrektywy PSD 2 można wymienić:

5 Przykładowo Yodlee INC. została przejęta w 2015 roku przez Envestnet Inc. w ramach transakcji opiewającej na ok. 610 mln dolarów

- opracowywanie regulacyjnych standardów technicznych dotyczących uwierzytelniania i komunikacji między określonymi podmiotami świadczącymi usługi płatnicze,
- określanie ram współpracy i wymiany informacji w zakresie działalności transgranicznej między właściwymi organami państwa członkowskiego pochodzenia a właściwymi organami przyjmującego państwa członkowskiego,
- prowadzenie bezpłatnego, elektronicznego i centralnego rejestru, w którym publikowany będzie wykaz nazw podmiotów świadczących usługi płatnicze,
- pełnienie roli koordynatora w zakresie zarządzania informacją na temat incydentów związanych z bezpieczeństwem w zakresie usług płatniczych.

Oczywiście bezpośrednim organem nadzorczym w Polsce będzie KNF, ale Dyrektywa PSD 2 wzmacnia przepisy w przedmiocie działalności i współpracy organów nadzoru państw członkowskich. Dyrektywa PSD 2 nakłada również kolejne obowiązki notyfikacyjne na przedsiębiorców. Przykładowo operatorzy telekomunikacyjni muszą przesyłać powiadomienia odnośnie tego, że przeprowadzane za ich pośrednictwem transakcje zakupu treści cyfrowych nie przekraczają określonych limitów.

Pobieranie dodatkowych opłat

W prawie unijnym wyraźnie widać tendencję do wydawania aktów prawnych, których celem jest wprowadzenie określonego limitu ograniczającego możliwość pobierania dodatkowych opłat z tytułu korzystania z określonych sposobów płatności czy instrumentów płatniczych. Przykładowo rozporządzenie 2015/751 Parlamentu Europejskiego i Rady z 29 kwietnia 2015 r. w sprawie opłat interchange w odniesieniu do transakcji płatniczych realizowanych w oparciu o kartę[6] („**Rozporządzenie MiF**") wprowadza przepisy dotyczące m.in. maksymalnych stawek opłat interchange pobieranych z tytułu transakcji realizowanych w oparciu o kartę płatniczą. W tym zakresie, aby zapobiec zjawisku pobierania dodatkowych opłat, Dyrektywa PSD 2 nakłada na państwa członkowskie obowiązek, aby te zapewniły, by odbiorca środków pieniężnych nie żądał opłat za korzystanie z instrumentów płatniczych (w szczególności kart debetowych i kredytowych), do których stosuje się re-

6 Dz. Urz. UE L 123 z 19 maja 2015 r.

gulacje odnośnie opłat interchange na mocy rozporządzenia MiF. Komisja Europejska podaje, że zakaz pobierania dodatkowym opłat w przypadku kart płatniczych pozwoli konsumentom zaoszczędzić ok. 730 mln euro, choć brak jest precyzyjnych i szczegółowych wyliczeń w tym zakresie.

Zasady odpowiedzialności

Co do zasady w przypadku nieautoryzowanej transakcji płatniczej dostawca usług płatniczych musi dokonać na rzecz płatnika (najczęściej posiadacza rachunku) zwrotu kwoty nieautoryzowanej transakcji płatniczej, z wyjątkiem sytuacji gdy dostawca usług płatniczych płatnika ma uzasadnione podstawy, by podejrzewać oszustwo. W przypadku usługi inicjowania również podmiot prowadzący rachunek zwraca kwotę nieautoryzowanej transakcji, przy czym przysługuje mu roszczenie zwrotne jeżeli to dostawca świadczący usługę inicjowania płatności jest odpowiedzialny za nieautoryzowaną transakcję płatniczą. W zakresie sporu o zaistnienie nieautoryzowanej transakcji płatniczej obowiązuje odwrócenie ciężaru dowodowego, gdyż to do dostawcy usług płatniczych należy udowodnienie, że transakcja przebiegła prawidłowo i nie ma podstaw do zwrotu kwoty nieautoryzowanej transakcji płatniczej na rzecz płatnika. Z kolei odpowiedzialność płatnika (czyli kupującego lub posiadacza rachunku) za nieautoryzowane transakcje płatnicze ma charakter wyjątkowy i jest ograniczona do maksymalnej wysokości 50 euro, czyli o 100 euro mniej w porównaniu do poprzedniej wersji dyrektywy i ustawy o usługach płatniczych. Jednakże, aby w ogóle mówić o odpowiedzialności płatnika, transakcja płatnicza musi być skutkiem posłużenia się utraconym lub skradzionym instrumentem płatniczym lub przywłaszczenia instrumentu płatniczego. Przy czym wspomniane już kwotowe ograniczenie odpowiedzialności płatnika nie ma zastosowania, gdy można mu przypisać nieuczciwe zamiary lub określone przypadki celowego lub rażącego zaniedbania. Natomiast pewne okoliczności, takie jak zaniechania ze strony dostawcy usług płatniczych czy brak obiektywnej możliwości stwierdzenia utraty, kradzieży lub przywłaszczenia instrumentu płatniczego przed płatnością całkowicie wyłączają odpowiedzialność płatnika za nieautoryzowane transakcje płatnicze. Odrębne (bardziej niekorzystne dla dostawcy usług płatniczych) zasady odpowiedzialności mają zastosowanie, gdy dostawca usług płatniczych nie wymaga silnego uwierzytelniania klienta (o którym niżej).

Nowe środki bezpieczeństwa

Dyrektywa PSD 2 wprowadza pojęcie silnego uwierzytelnianie klienta, które oznacza uwierzytelnianie w oparciu o zastosowanie co najmniej dwóch elementów należących do trzech poniższych kategorii (coś wiem, coś mam, czymś jestem):

- wiedza (coś, o czym wie tylko użytkownik np. hasło czy numer PIN),
- posiadanie (coś, co posiada wyłącznie użytkownik np. spersonalizowane tokeny),
- cechy klienta (coś, co jest charakterystyczne dla samego użytkownika np. układ linii papilarnych, a zatem kwestia biometrycznej identyfikacji użytkownika).

Silne uwierzytelnianie ma na celu odpowiednią ochronę poufności danych uwierzytelniających. W praktyce wiele instytucji finansowych stosuje już ten rodzaj uwierzytelniania, a Komisja Nadzoru Finansowego w wydanej w listopadzie 2015 r. rekomendacji dotyczącej bezpieczeństwa transakcji płatniczych wykonywanych w internecie („**Rekomendacja KNF**") jednoznacznie wskazała na potrzebę stosowania przez dostawców usług płatniczych procedury silnego uwierzytelniania klienta. Niemniej Dyrektywa PSD 2 wyraźnie przewiduje, że państwa członkowskie w pewnych sytuacjach (np. możliwość dostępu do rachunku on-line czy uruchomienie elektronicznej transakcji płatniczej) będą musiały wprowadzić na poziomie prawa powszechnie obowiązującego nakaz stosowania silnego uwierzytelniania klienta. Standardy techniczne odnośnie silnego uwierzytelniania klienta zostaną opracowane przez EUNB, a samo wdrożenie konieczności korzystania z tego środka bezpieczeństwa jest odroczone i będzie obowiązywało później niż większość przepisów Dyrektywy PSD 2. Zatem mimo czasowego braku obowiązku stosowania tego rodzaju uwierzytelniania i tak znajdą zastosowanie bardziej rygorystyczne zasady odpowiedzialności dostawcy usług płatniczych, które aktualizują się w razie braku stosowania silnego uwierzytelniania klienta.

Transpozycja

Implementacja Dyrektywy PSD 2 przez państwa członkowskie, co do zasady, musi nastąpić najpóźniej 13 stycznia 2018 r, z wyjątkiem nowych środków bezpieczeństwa (m.in. silnego uwierzytelniania klienta oraz standardów komu-

nikacji między poszczególnymi podmiotami świadczącymi usługi płatnicze), których wdrożenie powinno nastąpić w ciągu 18 miesięcy od daty wejścia w życie regulacyjnych standardów technicznych opracowanych przez EUNB.

Powyższa sytuacja sprawi, że mimo wejścia w życie norm prawnych dotyczących usługi dostępu do informacji o rachunku czy usługi inicjowania płatności i objęcia ich nadzorem, przez jakiś czas brak będzie pełnych ram prawnych dla relacji pomiędzy dostawcami tych usług, a dostawcami usług płatniczych prowadzących rachunek, szczególnie w zakresie technicznych standardów komunikacji. W związku z okresem przejściowym Komisja Europejska wskazała na potrzebę zastosowania środków tymczasowych i przykładowo, w zakresie internetowych płatności, będą to końcowe wytyczne w sprawie bezpieczeństwa płatności internetowych z dnia 19 grudnia 2014 r. wydane przez EUNB[7]. Również Rekomendacja KNF wskazuje na potrzebę stosowania wspomnianych wytycznych, która to, podobnie jak Dyrektywa PSD 2, podkreśla konieczność zapewnienia stosownych standardów bezpieczeństwa w zakresie płatności internetowych. Jednakże w zakresie wytycznych co do używania spersonalizowanych danych uwierzytelniających (między innymi login, hasło czy kod sms) Rekomendacja KNF stoi w sprzeczności w stosunku do Dyrektywy PSD 2, gdyż wyraźnie przestrzega przed udostępnianiem tychże danych jakimkolwiek podmiotom trzecim. Z kolei jednym z ważniejszych postulatów Dyrektywy PSD 2 jest zakaz przyjmowania przez państwa członkowskie środków, których celem byłoby nie tylko blokowanie, ale i utrudnianie świadczenia usługi inicjowania płatności, której istotą jest wprowadzenie indywidualnych danych uwierzytelniających do systemu informatycznego podmiotu oferującego taką usługę.

Podsumowanie

Dyrektywa PSD 2 stanowi fundament dla istnienia europejskiego rynku płatności wyznaczając podstawowe reguły prawne i zasady jego funkcjonowania. Jednak skutki jej implementacji wywołały podzielone zdania wśród przedstawicieli podmiotów świadczących usług płatnicze. Niektóre banki już teraz dostrzegają w tym ryzyko utraty części rynku. Rozwiązania wprowadzane przez Dyrektywę PSD 2 nie tylko zwiększają dostępność rynku dla podmiotów

7 https://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments

działających w obszarze e-commerce, ale również mogą pośrednio prowadzić do marginalizacji roli banków na rynku płatności, których rola w niektórych sytuacjach zostanie sprowadzona jedynie do prowadzenia „marketingowo niewidzialnego" rachunku bankowego, gdyż to dostawca usługi płatności będzie tym podmiotem, którego logo będzie najbardziej widoczne. Również Związek Banków Polskich w kontekście udostępnia osobom trzecim identyfikatora oraz hasła dostępu do konta bankowego podziela zastrzeżenia opisane w ramach Rekomendacji KNF. Z kolei przedstawiciele dostawców płatności online wskazują na szansę wzmocnienia swojej pozycji względem dominujących dotychczas firm amerykańskich, a także na zwiększenie obrotów, nie tylko w obrębie całego sektora e-commerce. Niemniej podnosi się także to, że beneficjentami rozwiązań zawartych w Dyrektywie PSD 2 będą również banki[8]. Wydaje się jednak, że pełne skutki w zakresie zmiany układu sił na rynku usług płatniczych trudno przewidzieć, choć Dyrektywa PSD 2 z pewnością zwiększy bezpieczeństwo użytkowników usług płatniczych, a także wprowadzi nowe wyzwania dla dostawców tych usług.

Nowe regulacje dają też dodatkową przestrzeń dla ekspansji usług firm z sektora FinTech. Nie tylko przy realizacji usługi dostępu do informacji o rachunku czy inicjowania płatności, w tym w zakresie sprostania wymogom bezpieczeństwa tych operacji po obu stronach (tj. banku i inicjatora), ale także w obszarze dostarczania rozwiązań związanych z silnym uwierzytelnianiem klienta. Obecne już na rynku (także w Polsce) rozwiązania, oparte na identyfikacji osoby na podstawie cech biometrycznych, np. głosu lub tętna, mogą istotnie zyskać na powszechności w sektorze usług finansowych. Nowe regulacje idą ramię w ramię z nowymi technologiami.

8 W tym kontekście należy przytoczyć wypowiedź Georga Schardta, wiceprezesa Zarządu SOFORT AG, który powiedział, że „*Największymi beneficjentami tych rozwiązań będą jednakże banki, ponieważ PSD 2 ma za zadanie regulować usługi pośredników, umożliwiających konsumentom dokonywanie płatności w Internecie za pomocą swoich e-kont bankowych. Pozwoli to bankom na realny come back w Internecie, po obniżeniu ich pozycji na rzecz PayPal i podobnych rozwiązań. Pieniądze będą transferowane z rachunku klienta bezpośrednio na konto sklepu. Dzięki temu zachowana zostanie płynność oraz ruch środków w środowisku bankowym, pod jednoczesną kontrolą nadzoru finansowego. Jest to ogromny krok naprzód, który zapewni europejskim pośrednikom równe szanse w konkurowaniu z amerykańskimi gigantami e-commerce*".

W dobie cyfrowej rewolucji, zmieniającej wszystkie aspekty znanej nam dotychczas rzeczywistości, wyzwania, przed którymi stają przedsiębiorstwa, dyktowane są przede wszystkim przez nowe technologie. Bankowość jest jednym z obszarów, gdzie cyfrowa rewolucja jest widoczna najbardziej. Znaczenia takich pojęć jak digital banking, big data, mobile banking, czy user experience już dawno wyszły poza swój pierwotny zakres – nie odnoszą się tylko do działań informatycznych, są raczej centralnym punktem strategii budowanej przez banki. Tymczasem już teraz pojawiają się kolejne megatrendy, takie jak Internet rzeczy czy sztuczna inteligencja, których wpływ na biznes, zgodnie z analizami PwC, będzie jeszcze silniejszy.

Trudno dzisiaj wyobrazić sobie bank detaliczny, który nie posiada zaawansowanych aplikacji internetowych, umożliwiających klientom dokonywania wszelkiego rodzaju transakcji za pomocą kilku kliknięć w smartphone. Tak samo trudno wyobrazić sobie bank, który nie ma przemyślanej strategii wykorzystania danych, jednego z najważniejszych zasobów instytucji finansowych.

Książka „Wyzwania informatyki bankowej 2016" w jasny i precyzyjny sposób opisuje najważniejsze zagadnienia związane z bankowością w czasach cyfrowej rewolucji, która będzie dominującym czynnikiem zmian przez wiele kolejnych lat.

Anna Sieńko, partner w PwC

ISBN 978-83-88835-27-8