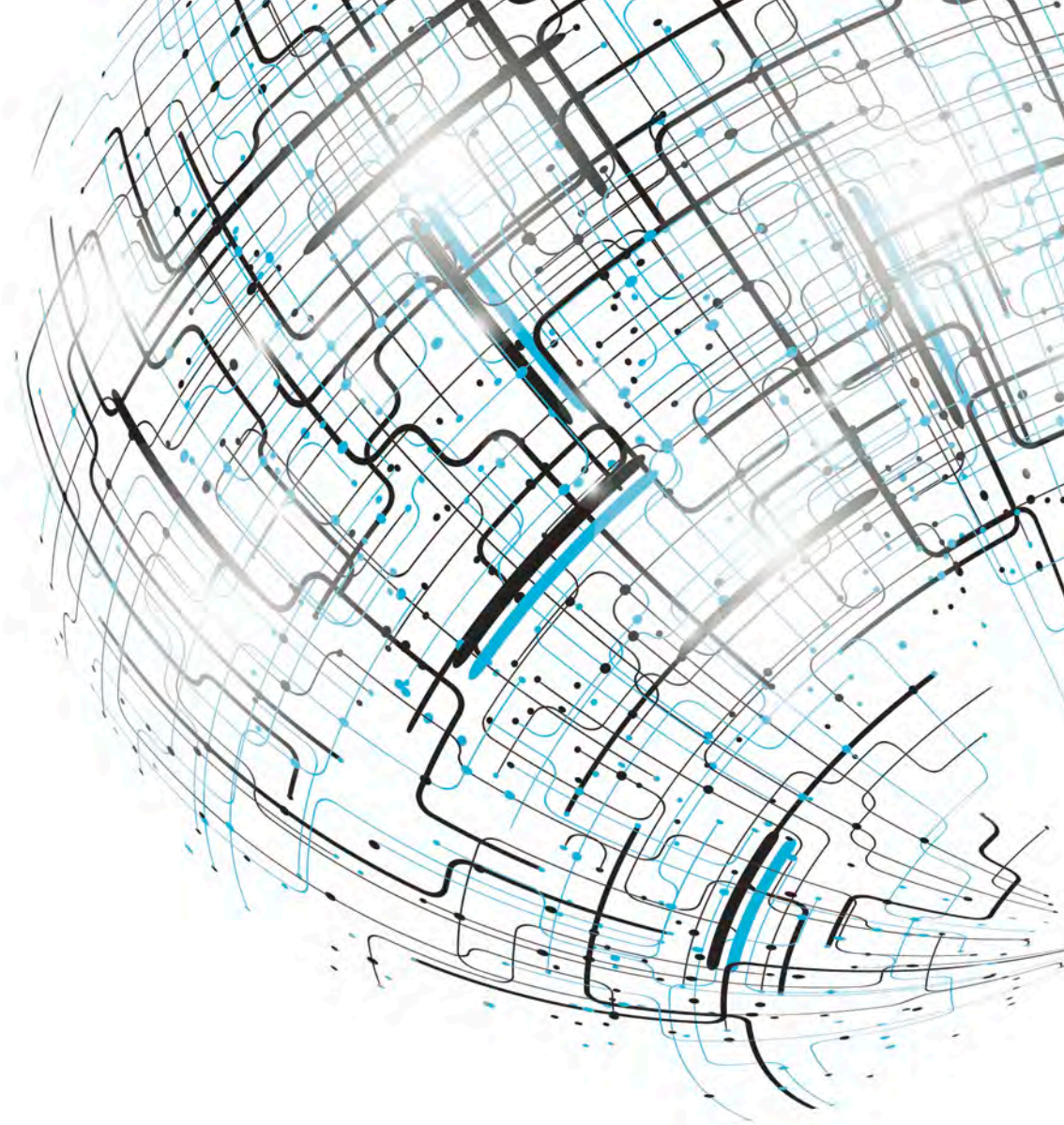


WYZWANIA INFORMATYKI BANKOWEJ

2017

REDAKCJA
ANDRZEJ KAWIŃSKI
ANDRZEJ SIERADZ

PUBLIKACJA
EUROPEJSKIEGO
KONGRESU
FINANSOWEGO

Wyzwania informatyki bankowej 2017

© Copyright by
Centrum Myśli Strategicznych
ul. Powstańców Warszawy 19
81-718 Sopot

Redaktorzy: Andrzej Kawiński, Andrzej Sieradz

Opracowanie redakcyjne: Wojciech Gryciuk

Korekta angielska: Lydon Pearsall

Projekt graficzny: Sopocka Grupa Marketingowa

Skład: Łukasz Sitko

ISBN 978-83-945091-1-8

Spis treści

Wstęp 7

Bartłomiej Nocoń, Jakub Garbus
Nowe pokolenia klientów w bankowości – wyzwania dla sektora 11

Artur Derwiszynski
PSD II – rewolucja, która w sektorze finansowym nie zdarza się często 23

Karol Mazurek
Czy API Management to szansa dla banków? Jak ją wykorzystać? 37

Mariusz Cholewa, Andrzej Zduńczyk
Wykorzystanie danych alternatywnych w lepszym zarządzaniu ryzykiem. 49

Adam Marciniak
Digitalizacja w wielkim banku 59

Michał Furmankiewicz
Co może zyskać firma migrując swoje usługi do chmury publicznej? 71

Joanna Molik, Andrzej Sieradz
Digital banking – four dimensions of digital transformation 89

Karolina Marzantowicz
Architektura Banku Przyszłości – Banking as a Platform 105

Jacek Figuła
Blockchain i rozproszona księga główna – bankowe tsunami czy szansa dla sektora bankowego 115

Piotr Puczyński, Andrzej Sieradz
What does a red rose from Kenya have to do with the blockchain? 125

Robert Trętowski
Bankowe okno na świat – „jedno okienko" dla obywatela 141

Piotr Malec, Artur Wach
Zarządzanie cyberbezpieczeństwem w globalnym banku 165

Marcin Spychała
Medytacje o bezpieczeństwie pierwszym 179

Aleksander P. Czarnowski
Ochrona danych osobowych a bezpieczeństwo rozwiązań bankowych 191

Maciej Gawroński
Odpowiedzialność za cyberbezpieczeństwo w banku
w czasach reformy ochrony danych 203

Andrzej Kawiński
Zarządzanie gotówką w krajach europejskich..... 213

Sebastian Ptak
Czy bankowcy śnią o elektronicznych płatnościach? 225

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

Wstęp

Oddajemy w Państwa ręce kolejne, coroczne opracowanie będące już od czterech lat próbą zachęcenia Drogich Czytelników do ważnych i coraz bardziej naglących przemyśleń na temat zmian technologicznych ważnych dla sektora finansowego, zarówno bankowego, jak i ubezpieczeniowego. Coroczne spotkanie organizowane przez Gdańską Akademię Bankową w Lesznie pod Warszawą, w ośrodku szkoleniowym BGŻ BNP Paribas, odbyło się 23 i 24 marca 2017 r. Jak co roku wysoka frekwencja przedstawicieli sektora finansowego potwierdziła potrzebę dyskusji na temat nowych modeli biznesowych oraz rozwiązań IT, jakie im towarzyszą. Podobnie, jak w latach ubiegłych, dyskusje dotyczyły całego spektrum nowych wyzwań, jakie stoją przed sektorem bankowym w Polsce. Oprócz „starych" regulacji, takich jak PSD II, są też „nowe", jak RODO i MiFiDII, a także te związane z bezpieczeństwem teleinformatycznym, wzrastającą konkurencją ze strony fintechów, dalszą koncentracją sektora w Polsce, zmianami właścicielskimi czy też „dojrzewającymi" technologiami, jak blockchain. I to im wszystkim towarzyszą coraz to większe wyzwania technologiczne.

Również w tym roku dyskusje, jak można było usłyszeć w Lesznie, są bardzo istotne dla sektora i warte wypracowania rekomendacji sektorowych. Jako przykład można tu podać PSD II, rozwiązania chmurowe, technologię blockchain czy też nowe regulacje dotyczące ochrony danych osobowych.

Dyskusja o zagadnieniach prezentowanych w publikacji w latach ubiegłych przekonała nas do kontynuacji inicjatywy wydawania, jak również rozszerzenia listy tematów, jakie wydają się być interesujące dla całego sektora finansowego. Większość artykułów w tegorocznej edycji odnosi się do cyfryzacji sektora bankowego, próbując dać odpowiedź na pytanie na czym ona polega i co jest jej istotą.

Analizując wyzwania, jakie stoją przed nowoczesnym sektorem finansowym, jak i nowe zjawiska na rynku finansowym, zmieniającym dynamicznie dotychczasowy model biznesowy sektora finansowego, doszliśmy do wniosku,

że wiele z nich już staje się naszą rzeczywistością. Dokonujące się zmiany są fundamentalne dla przyszłości sektora finansowego. Współpraca i wzajemne zrozumienie zagadnień pomiędzy departamentami biznesu, informatyki i bezpieczeństwa, jak i przedstawicielami instytucji regulatora (KNF) nabiera obecnie szczególnego znaczenia dla sektora finansowego. Cieszą zatem inicjowane we współpracy ze Związkiem Banków Polskich dyskusje na temat bezpieczeństwa i wymiany informacji co do zagrożeń w zakresie cyberbezpieczeństwa czy też dyskusja na temat polskiego kształtu dyrektywy PSD II.

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, w szczególności technologiach mobilnych. W tym roku zwracamy uwagę na dynamicznie rozwijający się rynek fintechów i powstających nowych rozwiązań.

Podobnie, jak w poprzednich edycjach opracowania, chcieliśmy raczej odnieść się do szeregu wyzwań i potencjalnych problemów, z jakimi większość instytucji finansowych w Polsce będzie musiała się zmierzyć w nadchodzących latach.

W tym roku na liście najważniejszych zagadnień znalazły się: bankowość mobilna połączona z usługami niefinansowymi, bezpieczeństwo transakcji płatniczych, technologia blockchain, BOT, współpraca z pozabankowymi uczestnikami rynku płatniczego, w tym usługi e-administracji czy też technologie związane z wielokanałowością dystrybucji produktów i usług finansowych.

Najważniejszym wyzwaniem w najbliższych miesiącach będzie bez wątpienia wdrożenie rekomendacji PSD II, co ma nastąpić w styczniu 2018 r. Ostateczne wymagania technologiczne w chwili publikacji opracowania będą już ostatecznie znane. Ta regulacja ma fundamentalny wpływ na przyszły model biznesowy banków w Polsce i Europie, na co wskazują wszelkie dyskusje jakie odbyły się w ciągu ostatniego roku.

Naczelną intencją publikacji było przedstawienie skomplikowanych zagadnień rynku sektora finansowego związanego z bankowością i ubezpieczeniami w sposób prosty i zrozumiały, adresując je do szerokiego grona odbiorców, szczególnie tych, którzy są użytkownikami tego typu rozwiązań lub decydentami.

Zależało nam 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 zarówno wybór zagadnień, jak i lektura opublikowanych artykułów będzie dla Państwa interesującą i pobudzającą do własnych przemyśleń i decyzji.

Tradycyjnie podziękowania chcielibyśmy przekazać prof. Leszkowi Pawłowiczowi za nieustającą inspirację i wsparcie duchowe oraz cenne uwagi w czasie przygotowywania publikacji, a całemu zespołowi GAB serdeczne podziękowanie za organizację całego projektu.

Andrzej Kawiński
Andrzej Sieradz

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. Pełni funkcję Wiceprzewodniczącego Rady Bankowości Elektronicznej przy Związku Banków Polskich.
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.

Jakub Garbus
Ekspert w Departamencie Bankowości Elektronicznej w Pionie Bankowości Detalicznej Banku Pekao S.A.

Absolwent Uniwersytetu Łódzkiego na kierunku administracja, specjalność finanse publiczne. W Banku Pekao S.A. związany z obszarem bankowości mobilnej Pekao24 dla klientów indywidualnych. Pasjonat nowych technologii i ich zastosowania w bankowości.

Bartłomiej Nocoń, Jakub Garbus, Bank Pekao S.A.

Nowe pokolenia klientów w bankowości – wyzwania dla sektora

W ostatnich kilkunastu latach upowszechnienie dostępu do internetu, popularyzacja smartfonów i tabletów oraz rozkwit interakcji międzyludzkich poprzez media społecznościowe zdefiniowały nowe generacje klientów – Y (Millenialsi), Z (iGen) oraz C (Connected). To pokolenia, które nie znają lub nie pamiętają czasów przed „digitalizacją", a częste zmiany, szczególnie w obszarze technologii to dla nich codzienność. Dzięki stałemu dostępowi do internetu i urządzeń mobilnych świat stał się dla nich globalną wioską. Najmłodsze generacje klientów w samych tylko Stanach Zjednoczonych i Europie stanowią już ok. 1/4 populacji[1], a najstarsi z nich mają dopiero 36 lat.

Jacy są nowi klienci?

Millenialsi to pokolenie wyżu demograficznego, urodzeni w latach 1981–1996. Podczas gdy starsze pokolenia na swój status materialny musiały dopiero zapracować (np. w Polsce w wyniku zmian ustrojowych), tę generację od razu wyposażono w dobra. W większości przypadków o ten stan rzeczy zadbali ich rodzice, zapewniając im wykształcenie i dobrobyt czy finansując wakacje i rozrywki. Według szacunków liczba Millenialsów w Polsce to ok. 9 mln osób[2].

1 *What millennials and Generation Z expect from their banks and service providers*, http://global.wellsfargobank.com/wfinsights-articles-millenials

2 *Niepotrzebne im auto czy mieszkanie. To nowe wyzwanie dla banków*, http://tvn24bis.pl/pieniadze,79/ekf-pokolenie-millenialsow-ogromnym-wyzwaniem-dla-sektora-bankowego,652542.html

Wychowywani i dorastający między schyłkiem popularności walkmana a narodzinami Google'a, w dobie rozkwitu technologii, internetu i Facebooka, nie pamiętają czasów bez komputera i najszybciej oswajają technologie/nowinki cyfrowe, a Wi-Fi, smartfon i media społecznościowe stanowią nieodłączny element ich życia. Przykładowo, przeciętnie w ciągu dnia Millenialsi są bardziej skłonni do interakcji ze swoim smartfonem (39%) niż kimkolwiek/czymkolwiek innym, nawet ze swoim partnerem czy partnerką (27%)[3]. Millenialsi żyją z nastawieniem „gdziekolwiek i kiedykolwiek" w dostępie do treści i to oczekiwanie przenoszą na wszystkie sfery swoich interakcji. Doceniają nowoczesne i innowacyjne marki, z którymi chętnie się utożsamiają (np. Apple, Google).

Wśród Millenialsów znajdziemy osoby młode, przedsiębiorcze, ale też skoncentrowane na sobie, często niesamodzielne. Cechuje ich duża mobilność. Szacuje się, że do 2025 r. będą stanowić aż 72% pracowników na świecie[4]. W perspektywie globalnej istotny wpływ wywarł na nich kryzys finansowy, bowiem wielu z nich rozpoczynało wówczas karierę zawodową (lata 2007–2008), przez co mieli możliwość doświadczenia jego negatywnego wpływu na przyjaciół, rodzinę czy ich samych.

Pokolenie Z, zwane także iGen, to osoby urodzone w latach 1997–2003, a więc najstarsi przedstawiciele tej generacji mają dopiero 20 lat! Szacuje się, że do 2020 roku generacja Z będzie stanowiła aż 1/3 populacji USA[5], a ich zachowania czy preferencje zakupowe wpłyną na oferty firm bardziej niż Millenialsów.

To, co istotnie odróżnia generację Z od Millenialsów czy starszych pokoleń, to fakt, że to pierwsza prawdziwie cyfrowa generacja – pokolenie multimediów, technologii i „ulotnych treści". Urodzeni w czasach popularności mediów społecznościowych, urządzeń mobilnych i Wi-Fi swobodnie poruszają się między *offline* a *online*. Dla tego pokolenia serwis e-commerce firmy Amazon jest symbolem sprzedaży detalicznej, Facebook synonimem kontaktu ze znajomymi, a wszelkich porad szukają na YouTube. Wolą wysłać wiadomość

3 *Bank of America Trends in Consumer Mobility Report*, http://newsroom.bankofamerica.com/press-kits/bank-america-trends-consumer-mobility-report

4 Raport EY: *Banki muszą dopasować się do potrzeb nowego pokolenia pracowników i klientów – generacji Y*, http://www.ey.media.pl/pr/319393/raport-ey-banki-musza-dopasowac-sie-do-potrzeb-nowego-pokolenia-pracownikow-i-klientow-generacji-y

5 *Preparing for Gen Z: 3 Lessons Learned from Overlooking Millennials*, https://thefinancialbrand.com/60483/generation-z-millennial-strategy/

przez WhatsApp lub inny komunikator niż zadać pytanie podczas tradycyjnej rozmowy, są bowiem przyzwyczajeni, że w ten sposób szybciej otrzymają odpowiedź. To „przyzwyczajenie" przejawia się także w tym, że nie widzą nic przeciwko, aby już trzynastolatkowie posiadali smartfony[6].

Korzystanie „non-stop" z szybkich i wygodnych aplikacji mobilnych, takich jak Uber czy Spotify stanowi część ich stylu życia, a zdolność do skupienia uwagi to 10-sekundowy *snap* (wiadomość lub video w aplikacji Snapchat, która jest wyświetlana maksymalnie przez 1–10 sekund). Ikonki, emotki/emoji, memy, grafiki i video zastępują tekst. Do tego pokolenia w istotny sposób przemawia komunikacja wizualna.

Przedstawiciele pokolenia Z szybko podejmują decyzje, ale nie zawsze zważają na ich konsekwencje, równocześnie prezentując wrażliwość na tzw. „ściemę" w przekazie marketingowym. Wykazują mniejszą dbałość o swoją prywatność, gdy korzystają z technologii dla nich natywnych, jak chociażby płatności mobilnych czy mediów społecznościowych.

Obserwacja przedstawicieli tego pokolenia najpełniej pokazuje, w jakim kierunku będą zmierzały w przyszłości trendy w obszarze zachowań konsumenckich, technologii, prywatności, bezpieczeństwa czy pracy.

Współcześnie, wśród nowych pokoleń klientów, często wyodrębnia się tzw. generację C. Jej nazwa pochodzi od słów *connect*, *communicate*, *change*, wskazujących na istotne cechy ją charakteryzujące. Znajdziemy w niej głównie przedstawicieli Millenialsów i generacji Z, należą do niej jednak także osoby ze „starszych" pokoleń, które dobrze znają i intensywnie korzystają z nowych technologii. To zatem pierwsza generacja, dla której brak jednoznacznie wyznaczonych ram czasowych, gdyż to zachowania, a właściwie upowszechnienie korzystania z internetu wyznaczają przynależność do niej a nie data ich urodzenia.

Cechą charakterystyczną generacji C jest wychowanie/„bycie w stanie" ciągłego podłączenia do internetu (*connect*). *Homo Digitalis* jest na bieżąco z tym, co się dzieje *online*, chętnie dzieli się w mediach społecznościowych (Facebook, YouTube, Snapchat) pomysłami i opiniami, a jego życie w realu i stała obecność w świecie wirtualnym przenikają się.

6 iGEN TECH DISRUPTION, 2016 National Study on Technology and the Generation after Millennials, http://genhq.wpengine.com/wp-content/uploads/2016/01/iGen-Gen-Z-Tech-Disruption-Research-White-Paper-c-2016-Center-for-Generational-Kinetics.pdf

Zachowania konsumenckie nowego pokolenia klientów

Niezależnie od tego, do jakiego pokolenia należą – generacji Y, Z czy C – nowi klienci przejawiają pewne wspólne zachowania charakterystyczne dla nowego typu konsumenta i jego interakcji z firmami.

1. Poczucie własnej wartości
Klient nowej generacji doskonale zna swoją wartość. Jest dobrze poinformowany, bo dzięki zasobom internetu ma nieograniczony dostęp do wiedzy. W praktyce oznacza to, że nowy konsument jest wymagający, stawia warunki i ma wysokie oczekiwania. Lubi być doceniany i mieć poczucie, że jest dla marki ważny.

2. Wygoda i dostępność „tu i teraz"
Nowi konsumenci przyzwyczajeni są także do prostych, estetycznych i wygodnych usług online, w konsekwencji poszukują tych cech także w innych instytucjach, np. w banku czy w urzędzie. Oczekują spersonalizowanej oferty i kontaktu/interakcji przez preferowany przez siebie kanał dostępu - stronę internetową, aplikację mobilną, ale też fizyczne punkty (tzw. ROPO – *Research Online Purchase Offline*, czyli sprawdzenie oferty w internecie i zakup w sklepie stacjonarnym). Wymagają natychmiastowej dostępności usługi czy serwisu, podobnie jak przy korzystaniu z internetu, i akceptują tylko krótkie, wizualne przekazy (jak np. Snapchat). Ma być szybko, wygodnie, natychmiast i „na klik".

3. *Slow*
Szczególnie interesująca jest zmiana w postrzeganiu czasu – z jednej strony spodziewają się natychmiastowej reakcji, dostępności (strony, produktu, usługi), z drugiej coraz bardziej cenią swój czas prywatny, spędzony z rodziną i rzeczywistymi przyjaciółmi, a nie tymi z sieci oraz aktywności *offline*, np. gry planszowe czy terenowe. Czas spędzony w „realu", zwracanie uwagi na to, co niweluje pośpiech, nadaje życiu wolniejszy, spokojniejszy rytm (*slow life*, *slow food* – czyli produkty wyciszające a nie np. energetyki) i pozwala zaoszczędzić czas, aby mieć go więcej „dla siebie".

4. Ufają znajomym
Nowi konsumenci są bardziej sceptyczni niż wcześniejsze generacje wobec wielkich korporacji czy instytucji finansowych, a zatem również w stosunku do reklam, którym nie ufają. Dlatego też nowe pokolenia chętniej wybierają

produkty rekomendowane przez innych konsumentów, do których mają zaufanie i którzy mówią wprost, czy coś jest „fajne", czy „niefajne" – rówieśników, youtuberów czy bloggerów. Marki coraz częściej angażują więc wpływowe osoby z mediów społecznościowych (influencerzy) do promowania produktów.

5. Niska lojalność

Brak większych oporów przed zmianą dostawców usług. Niska lojalność wobec „brandów" i częste przechodzenie między markami jest dla nich czymś typowym. Nowi konsumenci są *smart*, a więc testują lub szukają lepszych ofert, nie tylko ze względów finansowych. Na lojalność mogą liczyć tylko tzw. *lovebrands* (marki pożądania). Z drugiej strony chętnie płacą za to, co jest – ich zdaniem – warte swojej ceny.

6. Autentyzm

Młode pokolenia poszukują autentyczności w markach, z których korzystają. Od firm i przedsiębiorstw oczekują transparentności. Gdy produkt nie spełni ich oczekiwań na pewno poinformują o tym w internecie, a siła recenzji jest dla nich ważniejsza niż cena.

7. Świadomość społeczna

Bardzo ważne dla nowego konsumenta jest także zaangażowanie społeczne i konieczność dbania o środowisko naturalne. Zwraca uwagę na to, jak firma dba o otoczenie np. w procesie produkcji, jak przebiega ten proces, czy wykorzystuje tanią siłę roboczą, a może wspiera kraje Trzeciego Świata. Młodzi doceniają także firmy zaangażowane w działalność charytatywną. Aż 89% z nich chętniej kupi produkt od tej, która angażuje się społecznie lub w ochronę środowiska i aż 91% z nich bardziej im ufa[7].

8. Mam i chcę więcej, nie mam – współdzielę

Dostęp do dóbr jest ważny. Mimo posiadania wielu produktów chcą mieć więcej. Przy czym produkty te muszą wyrażać ich samych. Przywiązują wagę spersonalizowania rzeczy, których używają, bo to pozwala im wyróżnić się w towarzystwie. Często nie stać ich na to, czego potrzebują, dlatego dużą popularnością cieszą się wszelkie formy tzw. współdzielenia, pozwalające im korzystać z danego dobra bez konieczności zakupu (np. popularność rowerów miejskich czy podróżowanie via BlaBlaCar).

7 *2016 Millennial Banking Trends*, http://www.avoka.com/blog/2016-millennial-banking-trends/

Wyzwania dla sektora finansowego

Nowe pokolenia klientów stawiają także istotne wyzwania bankom.

1. Oczekują prostoty i wygody znanej z innych branż
Nowe pokolenia nie porównują już banków ze sobą, ale spodziewają się od nich takiej samej jakości usług i *customer experience*, jakie oferują ich ulubione firmy, niekoniecznie ze świata finansów (np. porównują jakość obsługi w banku z obsługą w ulubionym sklepie online). Założenie konta w banku ma być równie proste, jak założenie konta e-mail, powinno odbyć się *online* oraz zapewnić natychmiastowy dostęp.

2. Postrzegają instytucje finansowe jako „skomplikowane"
Czują się zagubieni w świecie finansów. Zazwyczaj brakuje im odpowiedniej wiedzy finansowej, a banki mówią do nich trudnym językiem używając skomplikowanej terminologii i dlatego mają problem ze zrozumieniem produktów bankowych. Nie czytają regulaminów czy umów, przez co wyrażają obawy przed np. ukrytymi w nich opłatami.

3. Wizyta w oddziale banku (raczej) nie wchodzi w grę
Bankowość i płatności mobilne to dla nowego pokolenia standard. Nie są zainteresowani wizytą w oddziale banku, skoro wszystko mogą zrobić w smartfonie. W konsekwencji do 2020 r. przewiduje się, że aż 8 z 10 młodych nigdy nie pojawi się w oddziale banku.[8] Mimo to, paradoksalnie, nadal oczekują kontaktu z ich pracownikami. To, co ich jednak zdecydowanie wyróżnia, to sposób komunikacji i technologia, z której korzystają. Zamiast wizyty w oddziale preferują zdalne kanały (czat, wideo, media społecznościowe), w których wygodnie komunikują się i – wtedy, kiedy tego potrzebują – mogą porozmawiać z doradcą, aby uzyskać pomoc lub poradę.

4. Ograniczone zaufanie do instytucji finansowych
Szczególnie istotnym wyzwaniem jest brak zaufania i lojalności. Nowe pokolenia klientów szukają instytucji, która pomoże im osiągnąć założone cele w najwygodniejszy i szybki sposób. Dla nowego konsumenta np. płatność za usługę to jedynie mały element większego procesu, jakim jest realizacja jego potrzeby – zakupu wymarzonego smartfona czy płatności za przejazd Uberem na imprezę. Nie interesuje

8 *Generation Z: The digital (r)evolution*, https://www.bbva.com/en/news/general/generation-z-digital-revolution/

ich, kto dostarcza produkt, dlatego też są niezwykle otwarci na usługi finansowe oferowane przez firmy inne niż banki, np. fintechy, które przyciągają ich prostymi i przejrzystymi zasadami dostępu do usług. W konsekwencji np. w USA aż 73% Millenialsów jest bardziej zainteresowanych usługami finansowymi oferowanymi przez Google czy Amazon niż usługami oferowanymi przez banki.[9]

Interesującym faktem jest to, że w zakresie posiadanych produktów bankowych młodzi klienci, paradoksalnie, wcale nie różnią się tak bardzo od poprzednich pokoleń. Tak samo chętnie korzystają z rachunków osobistych, kart kredytowych czy lokat.[10]

Warto w tym miejscu wspomnieć o tym, że istotne wyzwania dla banków niesie postęp technologiczny. Przedstawiciele nowych generacji, przyzwyczajeni do zmian w obszarze technologii, chętnie sięgają po takie nowinki jak Wirtualna Rzeczywistość (*VR*) czy Internet Rzeczy (*Internet of Things*). Możemy zatem przyjąć, że w nadchodzących latach należy spodziewać się zmiany obecnych zachowań klienckich. Szczególnie interesująca jest w tym kontekście Sztuczna Inteligencja (*AI*). Już dzisiaj coraz większą popularnością cieszą się chociażby *chatboty* na Facebook'u czy wirtualni asystenci, np. w aplikacji Google Allo, którzy w rozmowie do złudzenia przypominają człowieka. Należy oczekiwać, że w perspektywie kilku lat wirtualny asystent może stać się jedną z powszechnych form interakcji z bankiem (np. via chat wykonamy przelew) czy urządzeniami (np. Siri).

Jak odpowiedzieć na potrzeby nowego pokolenia klientów?

Banki mają za zadanie odpowiedzieć na kwestie związane z budową relacji z klientem, który nie jest lojalny wobec marki, spędza większość czasu ze smartfonem lub tabletem, jest „odporny" na reklamę oraz oczekuje prostych i wygodnych rozwiązań „tu i teraz".

Aby odpowiedzieć na te aspekty konieczne są:

1. Zbudowanie kompleksowej oferty opracowanej specjalnie dla nowych pokoleń klientów.
2. Odpowiednia komunikacja, zrozumiała dla młodszych generacji.
3. Edukacja finansowa – szczególnie ważna w przypadku klientów, którzy dopiero zaczynają korzystać z produktów i usług bankowych.

9 *The Millennial Disruption Index*, http://www.millennialdisruptionindex.com/

10 *Millennial Banking Customers: Two Myths, One Fact*, http://www.gallup.com/businessjournal/187364/millennial-banking-customers-two-myths-one-fact.aspx

Oferta dopasowana do nowego klienta musi być przede wszystkim prosta i zrozumiała. Klient, który szybko może porównać ze sobą oferty różnych banków, powinien od razu widzieć i rozumieć, dlaczego akurat produkt tego banku jest dla niego najlepszy. To także oznacza, że wie, za co ponosi opłaty. O ile młodszego klienta przyciągnie do banku brak opłat, o tyle klienci, którzy już pracują i mają własne rodziny chętniej sięgną po produkt droższy, jeżeli bank zaoferuje im realną wartość dodaną, np. rachunek osobisty z dobrym ubezpieczeniem. Oferta adresowana do nowego pokolenia musi być także angażująca. To ważne, bowiem aby zatrzymać i pozyskać lojalność nowego pokolenia klientów, należy ich także stale doceniać. Budowanie lojalności powinno polegać na oferowaniu rabatów, zniżek tam, gdzie chętnie robią zakupy czy nagradzać stałych klientów lepszymi warunkami cenowymi.

Banki muszą zapewnić także pozytywne i spersonalizowane doświadczenie podczas kontaktu – czy to w bankowości internetowej, mobilnej, czy w oddziale banku (w szczególności biorąc pod uwagę fakt, że te wizyty są coraz rzadsze). Nowe pokolenia klientów chętniej sięgają po produkty, które mogą spersonalizować, np. karty płatnicze z indywidualnie wybranym zdjęciem. W ciekawy sposób adresuje to oczekiwanie brytyjski Atom Bank, który jest pierwszym w Wielkiej Brytanii wyłącznie dla użytkowników mobilnych. Bank wyróżnia się tym, że pozwala klientom na spersonalizowanie marki poprzez możliwość nadania mu nazwy, stworzenia własnego logo czy wybrania koloru aplikacji. To podejście docenił hiszpański bank BBVA, słynący z inwestycji w innowacje. W 2015 r. stał się właścicielem 29,5% udziałów Atom Banku.[11]

Dla pokolenia, które stale pobiera nowe aplikacje i usuwa te nieprzydatne, szczególnie ważne jest, aby bankowość mobilna spełniała najwyższe standardy. Aplikacja powinna być atrakcyjna wizualnie i dostarczać potrzebne informacje przy minimalnej liczbie akcji. Przykładem takiej aplikacji bankowej jest PeoPay, który zamienia telefon w narzędzie do szybkich i wygodnych płatności – szybkich, ponieważ aplikacja prosi o zatwierdzenie płatności i nie wymaga wcześniejszego logowania oraz wygodnych, gdyż telefon mamy zawsze przy sobie.

W komunikacji z nowym pokoleniem klientów szczególnie istotne jest „mówienie" językiem dla nich zrozumiałym. Bankowa terminologia, ulotki

11 *App-only bank Atom is now worth £150 million — and it hasn't even launched yet*, http://www.businessinsider.com/bbva-invests-45-million-in-atom-bank-at-150-valuation-2015-11?IR=T

i tradycyjne spotkanie twarzą w twarz z doradcą nie są atrakcyjne dla nowych klientów i nie ułatwiają zrozumienia produktów bankowych. Wprost przeciwnie, prowadzą do tego, że klienci chętniej sięgają po szybkie i wygodne rozwiązania finansowe oferowane przez instytucje pozabankowe. To oznacza dla banków konieczność oparcia przekazu na szybkich, chwytliwych treściach w formie atrakcyjnej wizualnie i naturalnej dla nowego pokolenia – wideo, memy, etc. Szczególnie ważna jest także autentyczność przekazu. Treści kierowane do Millenialsów, generacji Z i C powinny być prawdziwe – merytoryczne a nie marketingowe, opierać się na doradztwie i być przydatne w osiąganiu celów.

Nowi konsumenci chcą przejąć kontrolę nad swoim życiem finansowym, ale często nie są do tego przygotowani i brakuje im odpowiedniej wiedzy. Banki muszą więc zadbać o nowe sposoby edukowania nowego pokolenia w zakresie swoich usług. Nowi klienci docenią materiały edukacyjne bogate np. w wizualizacje czy infografiki. Banki mogą także wspierać klienta oferując narzędzia do zarządzania budżetem domowym, które ułatwiają monitorowanie i analizę wydatków. Przykładem takiego rozwiązania jest aplikacja Pekao24 na tablety. Aplikacja przypisuje operacje do odpowiednich kategorii, a następnie prezentuje wydatki i wpływy w atrakcyjnej wizualnie formie (kolorowe koła z wydatkami), dzięki czemu klienci w prosty sposób mogą kontrolować swoje finanse.

Efektywna komunikacja musi odbywać się poprzez te kanały, z których korzystają klienci. Nowe pokolenia komunikują się dzisiaj przede wszystkim przez media społecznościowe, dlatego obecność banków w social mediach to konieczność. Banki muszą nie tylko słuchać klientów, ale też szybko reagować na pytania oraz stale podtrzymywać zaangażowanie. Dobrym przykładem, „jak robić media społecznościowe" jest chociażby brytyjski Barclays Bank, który ma już ponad 500 000 „lajków" na Facebooku. Gdy Barclays uruchamiał Your Bank, nową stronę internetową dla klientów do dzielenia się pomysłami, prowadził na żywo dyskusje ze swoimi klientami właśnie na Facebooku.

Ponieważ nowi konsumenci, a w szczególności pokolenia Millenialsów i Z, doceniają także zaangażowanie społeczne i działalność charytatywną, banki powinny dbać o tę stronę swojego wizerunku. Bank, który wspiera i chętnie angażuje się w akcje społeczne będzie postrzegany jako godny zaufania i autentyczny w swoim działaniu („robi, a nie tylko mówi").

Podsumowanie

Pozyskanie Millenialsów, klientów z generacji Z czy C powinno stanowić jeden z najważniejszych celów każdego banku. Szacuje się, że sami Millenialsi już dzisiaj stanowią 30% wszystkich klientów banków w Polsce.[12] Ci nowocześni konsumenci, będący tzw. *digital natives* (cyfrowymi tubylcami) stawiają przed bankami zupełnie nowe, często nieznane wcześniej, wyzwania, a w nadchodzących latach ich wpływ na kierunki rozwoju banków będzie jeszcze większy. Dla nowego konsumenta posiadanie lokaty czy skorzystanie z kredytu są bowiem tylko krokami do osiągnięcia właściwego celu, np. zakupu mieszkania. Dysonans między oczekiwania tych pokoleń a przedstawicielami „starszych generacji" wymusza więc na bankach konieczność zdefiniowania nowego podejścia. Banki stoją przed koniecznością zmiany strategii oraz zastosowania innowacyjnego podejścia w obszarze oferty produktowej i komunikacji. Te banki, które odpowiedzą na potrzeby nowych klientów i dopasują do ich stylu życia w konsekwencji pozyskają lojalność młodych klientów, staną się instytucją pierwszego wyboru przy podejmowaniu ważnych decyzji finansowych, a także będą chętnie polecane innym. Banki powinny zatem przyjąć rolę przewodnika, który prowadzi nowe pokolenia klientów przez świat finansów i wspiera je w osiąganiu zamierzonych celów w jak najszybszy i jak najwygodniejszy sposób.

12 *Niepotrzebne im auto czy mieszkanie. To nowe wyzwanie dla banków*, http://tvn24bis.pl/pieniadze,79/ekf-pokolenie-millenialsow-ogromnym-wyzwaniem-dla-sektora-bankowego,652542.html

Artur Derwiszynski
Head of Financial Services Industry, CEE w SAP i Członek Zarządu schematu SEPA w European Payments Council

Od lat łączy doświadczenie korporacyjne z tworzeniem startupów i inwestycjami w młode spółki. Ekspert w zakresie budowy strategii rozwoju oraz monetyzacji projektów w nowych obszarach gospodarki. Obecnie pomaga europejskim bankom w transformacji cyfrowej i przygotowaniu strategii biznesowej wokół open bankingu i PSD II. Jako mentor i ekspert współpracuje z centrami fintechowymi w Azji, Europie i USA.

Artur Derwiszynski

PSD II – rewolucja, która w sektorze finansowym nie zdarza się często

Unia Europejska za pośrednictwem swoich instytucji wydaje akty prawne regulujące wiele obszarów gospodarki – od sławetnego kształtu bananów (EC 2257/94) po taryfy roamingowe operatorów komórkowych (EU 531/2012). Rynek płatności również ma swoją regulację – dyrektywę w sprawie usług płatniczych (2007/64/WE).

Celem tej dyrektywy, zwanej potocznie PSD (*Payment Services Directive*) było stworzenie bardziej konkurencyjnego, zintegrowanego rynku płatniczego. Jednolity standard dla usług płatniczych objął teren Europejskiego Obszaru Gospodarczego (EOG, w skład którego wchodzą kraje Unii Europejskiej oraz Europejskiego Stowarzyszenia Wolnego Handlu z wyłączeniem Szwajcarii) i dotyczył wszystkich walut używanych na tym obszarze. Dyrektywa wprowadziła nową kategorię podmiotu na rynku finansowym, tj. instytucję płatniczą, która – nie będąc bankiem – może na równi z nim świadczyć usługi płatnicze.

Wiele osób mylnie utożsamia dyrektywę o usługach płatniczych z Jednolitym Systemem Płatności Euro (SEPA). Powołany przez banki European Payment Council (EPC) rozpoczął prace nad zharmonizowanym rynkiem płatniczym w 2002 r., a dyrektywa 2007/64/WE wprowadziła podstawy prawne do wdrożenia schematu SEPA i do dnia 31 października 2016 r. wszystkie kraje członkowskie Unii Europejskiej, niezależnie od obowiązującej w nich waluty, zaadoptowały nowe regulacje.

Jednak z punktu widzenia ewolucji samego rynku płatności kilka lat, jakie upłynęło od przyjęcia dyrektywy w sprawie usług płatniczych przyniosło ogromne

zmiany zarówno w rozwoju handlu elektronicznego, jak i w warstwie możliwości technologicznych. Dynamicznie rosnąca liczba transakcji w sklepach internetowych, zwiększenie dostępności smartfonów czy pojawienie się nowych usług skierowanych do konsumentów korzystających z płatności internetowych przyspieszyło prace Komisji Europejskiej nad nową regulacją. Ostatecznie poprawiona dyrektywa w sprawie usług płatniczych, czyli PSD II, weszła w życie 12 stycznia 2016 r. i państwa EOG mają czas na jej implementację do 13 stycznia 2018 r.

Zakres PSD II, czyli – zanim dotrzemy do clou programu – nowych szans biznesowych

Kluczowe obszary regulacji to:

- wprowadzenie nowych usługodawców i usług płatniczych,
- bezpieczeństwo konsumenta.

Nowi usługodawcy będą mogli świadczyć usługi w zakresie:

a) **Inicjowania płatności (*Payment Initiation Service Provider* – PISP).**
Operator takiej usługi działając w imieniu klienta będzie mógł zalogować się do systemu bankowości elektronicznej/internetowej w banku prowadzącym rachunek danego konsumenta i zlecić realizację płatności. Oczywiście klient będzie miał w każdej chwili prawo wycofania takiego upoważnienia a PISP nie będzie miał prawa do dokonania transakcji z wykorzystaniem swojego rachunku.

b) **Dostępu do informacji o rachunku (*Account Information Service Providers* – AISP).**
Operator tej usługi będzie mógł uzyskać dane, oczywiście po uzyskaniu zgody klienta, dotyczące historii transakcji oraz salda rachunku. Najprostszą usługą, którą będą mogły zaoferować AISP jest agregacja danych dotyczących sald i historii transakcji na różnych rachunkach w wielu bankach. Jednak usługę tę będzie można wykorzystać również do kalkulacji ryzyka kredytowego, personalizacji oferty handlowej, wsparcia decyzji zakupowych czy potwierdzenia tożsamości użytkownika.

Kluczowym dostawcą usługi w ramach PSD II będzie ASPSP – *Account Servicing Payment Service Provider*, czyli bank utrzymujący rachunek klienta.

Umożliwienie funkcjonowania AISP i PISP niesie za sobą znaczące konsekwencje dla sektora bankowego. Banki w ramach PSD II będą musiały

umożliwić dostęp dostawcy usługi inicjowania płatności i dostawcy informacji o rachunku do swoich systemów w celu zapewnienia realizacji nowych usług.

To pozwala nam spojrzeć szerzej na nową regulację, gdyż jeszcze w fazie przygotowań przyczyniła się ona do rozwoju pojęcia *open bankingu* jako nowego obszaru rozwoju bankowości. Jednym z krajów, który najszybciej dostrzegł potencjał w tym sektorze jest Wielka Brytania, gdzie na żądanie HM Treasury powołano we wrześniu 2015 r. *Open Banking Working Group* (OBWG)[1]. Ciało to przygotowało zestaw wytycznych dla *Open Banking Standard* (OBS) i już w grudniu 2016 r. banki działające w Wielkiej Brytanii były technologicznie przygotowane do realizacji OBS. W bieżącym roku zakończą się testy wymiany danych w ramach OBS oraz uruchomiona zostanie warstwa komercyjna projektu, co sprawi, że sektor bankowy w Wielkiej Brytanii będzie pierwszym w ramach krajów G20 posiadającym otwartą infrastrukturę technologiczną z wdrożonymi scenariuszami biznesowymi. Na kilkanaście miesięcy przed „wdrożeniem" PSD II.

Pozostałe kraje UE mają różne strategie uruchomienia projektów *open bankingu* czy adaptowania się do nowej regulacji. Dla przykładu „*Polish API*" – projekt realizowany w ramach Związku Banków Polskich – można zaliczyć do liderów zarówno pod względem zaawansowania prac, jak i przyjętych rozwiązań, podczas gdy w południowo-wschodniej części Unii uczestnicy rynku i regulatorzy praktycznie nie rozpoczęli prac nad *open bankingiem* czekając na formalne wdrożenie dyrektywy.

Z punktu widzenia Komisji Europejskiej, która od dawna podkreślała znaczenie zwiększenia bezpieczeństwa konsumentów w zakresie płatności, będzie to kluczowy obszar wprowadzony w ramach PSD II. Podstawowe instrumenty w tym zakresie to:

a) silne uwierzytelnienie klienta (SCA), jako odpowiedź na wzrost liczby wyłudzeń danych klientów, transakcji oszukańczych i wycieku danych z instytucji finansowych,
b) konieczność informowania właściwych organów nadzorczych przez dostawców usług płatniczych o incydentach – informacja ta będzie następnie przekazywana do europejskich instytucji nadzorujących (EBA i ECB), które będą weryfikować ryzyko danego incydentu w skali unijnej.

1 https://www.scribd.com/doc/298568600/Introducing-the-Open-Banking-Standard

Scenariusze użycia silnego uwierzytelnienia klienta a w szczególności odstępstwa od jego stosowania stanowią kolejne wyzwanie w określeniu ryzyka i kosztów wdrożenia dyrektywy. Wystarczy tylko nadmienić możliwość stosowania przez dostawców usług płatniczych analizy ryzyka transakcyjnego (TRA), która w czasie rzeczywistym powinna obejmować analizę dotychczasowych zachowań osoby dokonującej transakcji wraz z detekcją zachowań nietypowych z dokładnością do pojedynczej transakcji, analizę logów urządzenia lub oprogramowania używanego do transakcji oraz inne działania wpływające na zmniejszenie ryzyka wystąpienia transakcji oszukańczej. Artykuł 16 ostatecznej wersji roboczej kluczowego dla dyrektywy dokumentu przygotowanego przez *European Banking Authority* zwanego *Regulatory Technical Standard* (RTS) szczegółowo opisuje warunki.

Czy na PSD II da się zarobić?

Z punktu widzenia zmian dla sektora bankowego PSD II można rozpatrywać na trzech poziomach:

- regulacji,
- technologii,
- biznesu.

Z punktu widzenia regulacji, PSD II będzie dla banku kolejnym kosztem. Wzrost obciążeń regulacyjnych wpływa na pogorszenie wyników finansowych banków oraz zwiększenie kosztów w tym obszarze. Przykładowo w latach 2011–2015 liczba zatrudnionych w dziale *compliance&regulatory* tylko w banku JP Morgan zwiększyła się z 24 000 do 43 000[2].

W warstwie technologicznej PSD II również jest kosztem, w głównej mierze przystosowania systemów informatycznych. W wersji „minimalnej" bank będzie musiał zapewnić dostęp do swoich systemów nowym usługodawcom (PISP i AISP). Największą niewiadomą w tym przypadku jest ostateczny kształt rekomendacji technologicznych. W chwili pisania tego artykułu dalej nie mamy oficjalnej wersji RTS a jedynie ostateczną wersję roboczą.

Jak zwykle najciekawiej temat wygląda z perspektywy biznesu. Generalnie w świecie PSD II banki będziemy mogli podzielić na dwie kategorie – pasywne i aktywne. W pierwszym przypadku będą to instytucje, które spełnią wymogi regulacyjne nie widząc jednocześnie dla siebie przestrzeni biznesowej płynącej

2 https://www.jpmorganchase.com/corporate/investor-relations/document/2015-annualreport.pdf

z nowej regulacji. W długiej perspektywie można założyć, że zostaną one centrami kosztów regulacyjnych i operacyjnych, na bazie czego AISP, PISP a przede wszystkim konkurencyjne banki będą budować swój biznes. Od czasu uchwalenia dyrektywy część pasywnych banków zastanawiała się w jaki sposób obniżyć możliwy zasięg oddziaływania przepisów. Jednym z takich pomysłów było oferowanie dostępu do serwisów banku na dwóch płaszczyznach. Pierwsza zakłada bezpłatny dostęp w ramach PSD II – z założenia niezbyt „szybki" i o nie gwarantowanej „jakości" odpowiedzi na zapytanie z PISP/AISP. Do tego wersja „premium" – szybka i stabilna, ale dostępna za opłatą. Ten pomysł zostanie jednak prawdopodobnie skutecznie zablokowany, gdyż ostateczna wersja robocza RTS, przygotowana przez EBA, zawiera zapis, że standard usługi świadczonej przez bank w ramach PSD II wobec AISP/PISP musi posiadać taki sam poziom dostępności/jakości, jaki bank oferuje bezpośrednio swoim klientom.

Druga kategoria to banki aktywne, które będą oferować nowe usługi finansowe i niefinansowe. Ta grupa banków widzi w PSD II szansę na rozwój, unowocześnienie portfela produktów i poprawę relacji z klientem.

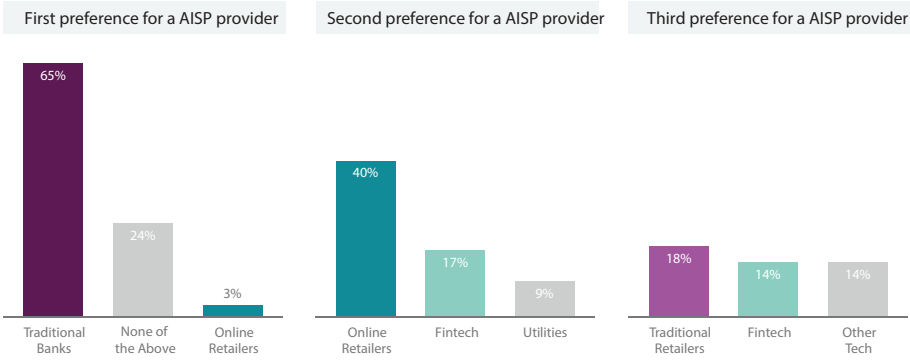
Niemniej, to co na początek czeka banki aktywne to dodatkowe inwestycje. Zazwyczaj ich skala jest proporcjonalna do wizji sukcesu, jaki dany bank chce odnieść w ramach walki o dominację w świecie post-PSD II. Mając na uwadze nową regulację, konfrontację z innymi graczami spoza sektora bankowego (fintechy, operatorzy GSM, sieci handlowe) rośnie więc ryzyko prowadzenia działalności. Obserwując rynek zarówno z pozycji Brukseli, jak i poszczególnych krajów można powiedzieć, że tylko nieliczne banki mają przygotowaną strategię (nie mówiąc o planie operacyjnym) pod PSD II.

Część banków próbuje zaadoptować strategię w ramach istniejącej infrastruktury i zasobów. W tym miejscu pozwolę sobie na subiektywny komentarz, niestety, niezbyt optymistyczny. Najpierw spojrzenie na środowisko konkurencyjne, które nie jest pewne. Nie ze względu na to, co planuje konkurencja, tylko kto w ogóle jest konkurentem? Banki jako stabilne, bezpieczne instytucje, porównują się zazwyczaj do innych banków, a w najlepszym razie śledzą działania fintechów. Jednak, jak historia pokazała już niejednokrotnie, najgroźniejszy konkurent nie zawsze pochodzi z tej samej branży. I nie chodzi tu o przykład Garmin vs. Google, w którym konkurent dla tradycyjnego biznesu przyszedł spoza rynku tradycyjnych dostawców map cyfrowych. Ten nowy konkurent udostępniając nową usługę, która zmusiła Garmin'a do natychmiastowego przemyślenia swojego modelu biznesowego, nie czuł się nawet konkurentem a jego celem nie była

walka z Garmin'em. Pomyślmy, jakie efekty dla sektora bankowego będą miały działania mniejszych i większych, a na pewno agresywnych graczy, którzy w ramach PSD II zyskają dostęp do infrastruktury bankowej. Wracając do niezbyt optymistycznego, subiektywnego komentarza… Większość banków myśli o realizacji nowatorskiej strategii PSD II w ramach istniejących zespołów, istniejących procedur. Niestety, dużym i stabilnym organizacjom właśnie z powodu tego, czym są, będzie zdecydowanie trudniej konkurować z nowymi, dynamicznymi uczestnikami rynku i mogą nie być w stanie zaadoptować się do nowych realiów. Nawet jeśli w ramach takiej organizacji udaje się stworzyć dedykowany zespół czy produkt, jest on często „zarażany" starym podejściem. Część z banków zdaje sobie z tego sprawę i wdraża strategię albo poprzez wydzielenie projektu PSD II poza obecne struktury organizacyjne albo poprzez przejęcie (z zachowaniem autonomii biznesowej) małego, dynamicznego gracza.

Elementem wspierającym banki w transformacji wymuszonej dyrektywą o dziwo wydają się być sami klienci. Według badań konsumentów[3], 65% spośród nich uważa, że oczekiwanym dostawcą usługi dostępu do informacji o rachunku powinien być bank. Jeszcze lepszy wynik banki notują w przypadku wyboru preferowanego dostawcy inicjacji płatności. W tym przypadku, aż 76% badanych uważa, że preferowanym PISP powinien być bank.

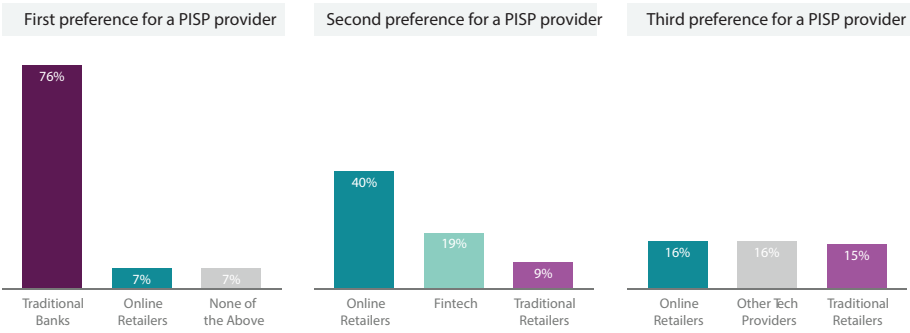
Rys. 1. Preferencje konsumentów dotyczące potencjalnego dostawcy usługi informacji na rachunku.



Źródło: Accenture

3 https://www.accenture.com/t00010101T000000__w__/gb-en/_acnmedia/PDF-29/Accenture-UK-Banking-PSD II-Consumer-Reactions.pdf#zoom=50

Rys. 2. Preferencje konsumentów dotyczące potencjalnego dostawcy usługi inicjowania płatności.



Źródło: Accenture

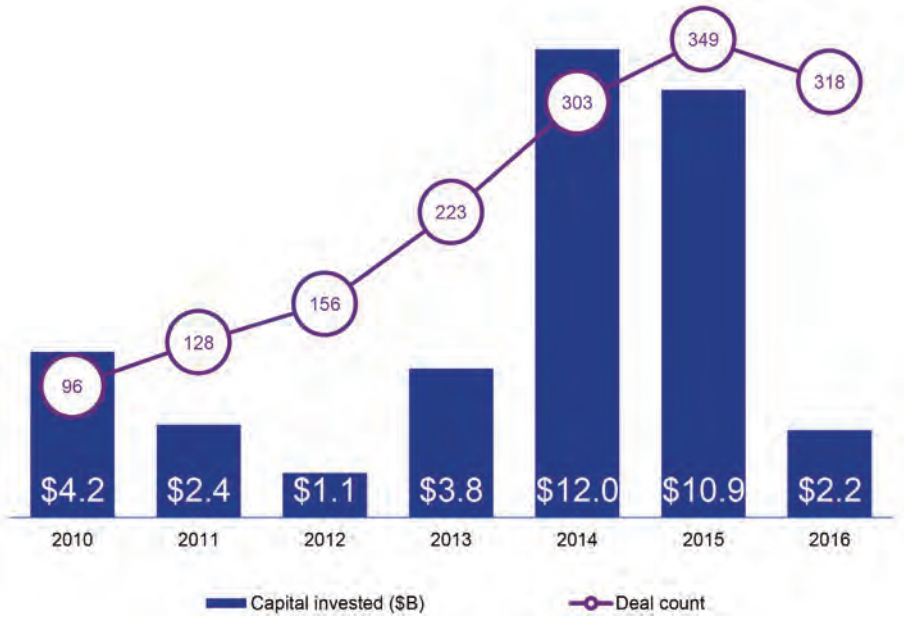
W tym miejscu warto dokładnie przyjrzeć się temu, co w ramach PSD II oferują firmy działające poza lokalnymi ustawami o bankowości.

Co na to rynek niebankowy?

Wszyscy mówią – szaleństwo. I z perspektywy inwestycji i z perspektywy modeli biznesowych. Poziom nakładów inwestycyjnych w fintechy w Europie w 2014 r. wyniósł aż 12 mld USD[4]. Popatrzmy jednak na to, co się wydarzyło w 2015 r., kiedy to liczba inwestycji wzrosła ponad 15% z 303 do 349, a ich wartość spadła o ponad 9% do 10,9 mld USD. Ochłodzenie? To dołóżmy dane z 2016 r., kiedy to wynik ten pomniejszył się o 80% do poziomu 2,2 mld USD!

4 https://www.accenture.com/t00010101T000000__w__/gb-en/_acnmedia/PDF-29/Accenture-UK--Banking-PSD II-Consumer-Reactions.pdf#zoom=50

Rys. 3. Inwestycje w fintechy w Europie w latach 2010–2016.



Źródło: KPMG

Te wyniki można zinterpretować w różnorodny sposób. Jednak wydaje się, że inwestorzy, po pierwszej fali dużych inwestycji, czekają teraz na weryfikację deklarowanych modeli biznesowych w realiach rynkowych. Oczywiście nie wszystkie przedstawione wyżej inwestycje były realizowane pod kątem PSD II. Jednak już teraz można powiedzieć, że niektóre proste usługi oparte np. tylko o zwiększenie dostępności informacji o zagregowanych saldach mogą mieć problem z monetyzacją. Po pierwsze dlatego, że konsumenci nie będą skłonni płacić za samą usługę prezentacji salda/historii. Po drugie dlatego, że wiele osób oczekiwało łatwej dostępności zagregowanego salda w trybie 24/365. Jednak ze względu na konieczność zapewnienia limitowanego dostępu do systemów centralnych w bankach zdecydowano się na ograniczenie możliwości zapytania banku o saldo do czterech razy w ciągu 24 godz. Chociaż istnieje spór czy zniesienie tego ograniczenia w przypadku, kiedy klient „aktywnie zażąda takiej informacji" dotyczy również przypadku zwykłego wciśnięcia przez klienta ikonki, np. „zaktualizuj saldo" w aplikacji dostawcy usługi informacji na rachunku.

Rynek kwitnie i liczba nowych podmiotów, które chcą pełnić rolę integratora czy inicjatora płatności gwałtownie rośnie. Do tego dochodzą firmy oferujące *Bank-as-a service* (BaaS) – formalnie banki będące bardziej dostawcą i operatorem technologii bankowej niż oferentem usług bankowych. Platformy BaaS będą wykorzystywane przez mniejszych i większych graczy z sektorów poza bankowych, w szczególności operatorów telekomunikacyjnych, sieci handlowych czy dostawców usług masowych. Firm, które mają już (często negatywne) doświadczenia z realizacji projektów płatniczych oraz bankowych i wykorzystanie skalowalnej, elastycznej platformy BaaS może być szansą na kolejną, tym razem dochodową próbę zaistnienia w sektorze zarezerwowanym dotychczas dla specjalizowanych dostawców usług płatniczych i banków. Mimo, że pierwsze projekty BaaS były oferowane przez nowe firmy technologiczne, które na potrzeby realizacji swojej strategii uzyskały licencję bankową, obecnie coraz więcej banków rozważa komercyjne uruchomienie oferty Bank-as-a-service doszukując się przewagi konkurencyjnej w lepszej znajomości kluczowych produktów związanych z zarządzaniem ryzykiem i utrzymaniem płynności.

Ciekawym przykładem jest rynek niemiecki, który z jednej strony uważany jest za najszybciej rosnącą scenę fintechową w Europie, z drugiej skupiający największą ilość dostawców Bank-as-a-service, z trzeciej pokazujący jak dobrze banki i fintechy mogą przejść z modelu konkurencji do współpracy. Schemat na rys. 4. pokazuje, jak wygląda mapa relacji między poszczególnymi graczami na rynku niemieckim.

Rys. 4. Współpraca między bankami i fintechami w Niemczech, marzec 2017[5]

Jako ciekawostkę warto wskazać, że jednym z liderów „integracji" jest mimo wszystko bank-startup Fidor Bank, który oferując wielomodułową strukturę usług w ramach Bank-as-a-service pozwala na korzystanie poprzez API z usług ponad 50 partnerów oferujących zarządzanie depozytami i pożyczkami, monitorowanie fraudów, wydawanie kart płatniczych, płatności mobilne czy rozbudowane środowiska testowe do opracowania i wdrażania nowych usług finansowych.

Jak w tym wszystkim ma się odnaleźć klient?

Jak zaznaczyłem wcześniej Komisja Europejska pracując nad PSD II informowała, że jej głównym celem jest zwiększenie konkurencyjności na rynku płatności przy wzroście bezpieczeństwa konsumentów. I, mimo wielu ryzyk związanych z prowadzeniem działalności przez uczestników rynku po wejściu w życie dyrektywy, wydaje się, że przynajmniej z punktu widzenia dostępności i ceny usług najbardziej zadowolony powinien być klient. Oczywiście nie wiemy dzisiaj jak sytuacja zmieni się w długiej perspektywie i kiedy

5 https://www.it-finanzmagazin.de/banken-und-fintechs-das-hecheln-nach-der-moehre-kostet-zeit-fokus-und-nimmt-den-grossen-hunger-20330/

dojdzie do konsolidacji rynku oraz weryfikacji strategii cenowych. Jednak już teraz wydaje się, że nowa regulacja przyspieszyła weryfikację strategii w wielu instytucjach finansowych i, zwłaszcza w zdefiniowanych wcześniej „aktywnych" bankach, widać przejście z koncentracji na produkcie bankowym do koncentracji na potrzebach klienta i zaoferowaniu odpowiedniego rozwiązania. Zmiana może wydawać się mało czytelna, jednak przybliża ona modele biznesowe banków do zaadoptowanych już wcześniej przez dużych graczy rynku detalicznej sprzedaży internetowej czy operatorów telefonii komórkowej. W obu przypadkach narzędzia do walki o klienta są bardziej zaawansowane niż w sektorze bankowym przy jednoczesnym spadku marży na oferowanym produkcie czy usłudze. Jednak nie tylko cena i nakłady marketingowe pozwalają wygrać najlepszym. Zaawansowana analityka predykcyjna, oddziaływanie w zależności od sentymentu klienta czy integracja i automatyzacja procesów to czynniki, które zwiększają szanse na zajęcie dominującej pozycji na wysoce konkurencyjnym rynku.

Jednak mówiąc o zmianie strategii biznesowej odeszliśmy od głównego tematu tego rozdziału – jak w nowym otoczeniu zachowa się klient? Czy będzie dostrzegał różnicę między bankiem a fintechem oferującym usługi bankowe innego podmiotu? Czy będzie rozumiał, który podmiot za co jest odpowiedzialny? Czy będzie miało dla niego znaczenie, gdzie są jego pieniądze czy wystarczy tylko świadomość, że ma dostęp do oczekiwanych zasobów finansowych?

Na część z tych pytań będą musieli odpowiedzieć regulatorzy, ponieważ można przypuszczać, że tak istotna zmiana na rynku dostawców usług płatniczych i bankowych przyciągnie organizacje przestępcze, które będą chciały wykorzystać moment jego rozchwiania.

Natomiast wraz ze wzrostem świadomości oraz dostępu do informacji wydaje się, że klienci funkcjonujący w świecie zmienionym przez PSD II powinni odczuć korzyści z korzystania z nowych narzędzi płatniczych i usług około bankowych. Jednym z wyznaczników sukcesu biznesu w czasach cyfrowej ekonomii jest pozycja aplikacji mobilnej na ekranie użytkownika. Niepotrzebna aplikacja nigdy nie zostanie zainstalowana, ta wykorzystywana rzadko i niemająca wartości w codziennym zastosowaniu ląduje zazwyczaj na odległych „ekranach" lub jest grupowana z innymi, mało potrzebnymi programami. Natomiast prawdziwym sukcesem aplikacji jest jej obecność na ekranie startowym telefonu, w zasięgu ruchu palca użytkownika. Jeśli wyobrazimy

sobie możliwości związane z zarządzaniem swoimi kontami w różnych bankach i kartami różnych wydawców w jednym miejscu, pozwalającym na korzystanie z programów lojalnościowych, upraszczającym nie tylko sam proces płatności, ale również zakupów w ulubionych sklepach, to łatwo dostrzec, że aplikacja bankowa (lub fintechowa) może w ramach nowej regulacji zyskać zupełnie nowy wymiar i znacząco zwiększyć cyfrowy *foot flow* klienta.

Podsumowanie

PSD II nadchodzi. Pamiętaj, że pośrednio lub bezpośrednio dotknie również Twój biznes. Tym mocniej im jest on bliższy usługom bankowym i płatniczym. Każda instytucja w tym sektorze będzie musiała podjąć decyzje w sprawie pozycji, jaką przyjmie wobec regulacji. Czy jest gotowa na transformację, uruchomienie nowych usług i współpracę lub walkę z firmami o znacznie większej zwinności i zdolności do akceptowania ryzyka? Czy może lepiej okopać się w warstwie regulacyjnej, skoncentrować na podstawowej działalności i marżę budować na obniżaniu kosztów?

Instytucje finansowe, aby odnaleźć się w nowej perspektywie będą musiały zweryfikować swoje modele biznesowe, ponieważ nawet w przypadku „pasywnego" podejścia do regulacji środowisko konkurencyjne ulegnie zmianie. Warto jednak zauważyć, że wiele z tych zmian już teraz wymuszają klienci, którzy oczekują od banków i operatorów płatności aktywnego poszukiwania nowych źródeł przychodów i większej koncentracji na użyteczności usług.

Karol Mazurek
Managing Director, Accenture Polska

Z firmą związany od 1988 r., gdzie 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.
Ukończył Wydział Fizyki Technicznej i Matematyki Stosowanej na Politechnice Warszawskiej.

Karol Mazurek, Accenture

Czy API Management to szansa dla banków? Jak ją wykorzystać?

Koncepcja API (*Application Programming Interface*) jest znana programistom od dawna, ale dopiero od niedawna przechodzi bardzo dużą zmianę w wyniku coraz większego otwarcia organizacji poprzez właśnie interfejsy programistyczne. 75% ruchu na Twitterze czy 65% transakcji Salesforce.com jest generowanych przez API. Są one wykorzystywane do budowania aplikacji na smartfony działających w sieciach społecznościowych, urządzeniach połączonych z siecią, a wszystko to może prowadzić do zwiększenia sprzedaży i dotarcia do szerszych grup klientów.

Czym jest API Management?

Udostępnianie API zewnętrznym programistom w sposób naturalny generuje szereg wyzwań i zagrożeń. Jak ochronić informacje przed niepowołanym dostępem? Jak dostarczyć API w sposób niezawodny z wysoką dostępnością? Jak zarządzić dostępem do API i monitorować ich wykorzystanie? Jak zarobić na udostępnianiu API?

Odpowiedzi na te pytania dostarcza API Management – procedury i narzędzia niezbędne zawsze, gdy udostępnia się usługi w postaci API. W zakresie zarządzania API znajdziemy m.in. następujące funkcjonalności:

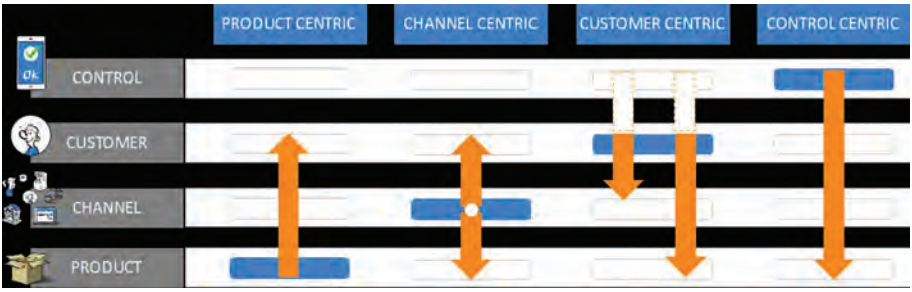
- **Zarządzanie bezpieczeństwem API** – zapewnienie obsługi uwierzytelnienia zewnętrznego, uwierzytelnianie programistów, wykorzystanie federacyjnych modeli i standardów tożsamości cyfrowej.
- **Zarządzanie cyklem życia API** – udostępnienie wsparcia dla procesu migracji API pomiędzy środowiskami, zarządzanie metadanymi, automatyzacja procesów akceptacji dla promocji na środowisko produkcyjne i wycofywania kodu w przypadku awarii.
- **Zarządzanie wsparciem dla API** – wsparcie utrzymywania SLA, monitorowanie zgłoszeń problemów itd.
- **Zapewnienie dostępu zewnętrznym programistom.**
- **Monetyzacja** – wycena dostępu, pomiar ich wykorzystania (ilość wywołań, pobrane dane itd.) w celu rozliczenia się ze stronami wykorzystującymi nasze API.

Klient przejmuje władzę

Od dłuższego już czasu modele biznesowe we wszystkich sektorach przedsiębiorczości zmieniają się tak, aby jak najbardziej odpowiedzieć na oczekiwania klienta, rozumieć go i dać mu narzędzia do definiowania sposobu interakcji z dostawcą usług lub produktów zgodnie z jego wolą. Dużo na ten temat można się dowiedzieć z materiału *„Open Banking: putting the customer in control"*[1], opublikowanego niedawno przez *European Banking Association*.

1 *„Open Banking: putting the customer in control" Euro Banking Association*, Version 0.99 26 January 2017, https://www.abe-eba.eu/Repository.aspx?ID=90679c33-e798-4700-a574-23565c223da9

Rys. 1. Przesunięcie modelu biznesu od zorientowanego na produkt do zorientowanego na klienta.



Źródło: „Open banking: putting the customer in control"

Dla banków ruch w stronę klienta zaczął się wraz z pojawieniem się bankowości internetowej i nabrał tempa, gdy pojawiła się bankowość mobilna. Perspektywa PSD II[2] bardzo się do tego przyczynia, promując ideę otwartej bankowości, która pozwala bankom na budowanie współpracy z graczami spoza sektora finansowego, innowatorami ze świata fintech czy firmami czysto technologicznymi. Umieszczenie klienta w centrum oznacza w gruncie rzeczy, że dajemy mu możliwość intuicyjnego załatwiania swoich spraw w coraz bardziej połączonym i coraz szybciej działającym ekosystemie. W szczególności oznacza to:

- Możliwość wykorzystania cyfrowej tożsamości potwierdzonej przez bank do zalogowania się do usług e-administracji lub usług komercyjnych.
- Przekazanie stronom trzecim wybranych atrybutów (np. wiek, adres) udostępnianych przez bank po potwierdzeniu tożsamości.
- Możliwość połączenia aplikacji firm trzecich bezpośrednio ze swoim rachunkiem bankowym, np. w celu zainicjowania płatności.
- Połączenie informacji o swoich zasobach i zobowiązaniach finansowych w celu lepszego zarządzania wydatkami i oszczędnościami.

Dla zapewnienia tej funkcjonalności kluczowe są dwa komponenty:

- Architektura zarządzania i udostępniania tożsamością cyfrową.
- Wdrożenie spójnej dla rynku specyfikacji API bankowego oraz wdrożenie narzędzi i procesów zarządzania API – nie tylko na poziomie technicznym.

2 *Revised Payment Services Directive*, https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en

Oprócz tych technologiczno-procesowych komponentów bardzo istotna jest również edukacja klienta – otwarcie platform bankowych to w istocie wygoda i odpowiedź na jego oczekiwania, ale też zwiększenie ryzyk związanych z cyberbezpieczeństwem.

Otwarte API bankowe – o czym trzeba pamiętać?

Przygotowując się do uruchomienia architektury opartej na API należy pamiętać o kilku kluczowych kwestiach, które wymagają przemyślenia już na wczesnych etapach przedsięwzięcia:

- **Nieprzewidywalne obciążenie systemów** – systemy banku muszą być przygotowane na skoki obciążenia generowanego przez strony trzecie. Gracze agregujący informacje z banków będą zapewne odpytywać je w podobnych momentach, np. po przetworzeniu sesji rozliczeniowych lub w godzinach spodziewanego niższego obciążenia, gdy ruch on-line jest niewielki.
- **Rosnące wolumeny transakcji** – do ekosystemu będą dołączali kolejni gracze, generując wzrost ilości zapytań do systemów bankowych.
- **Wymagana wysoka dostępność API** – dostęp poprzez API będzie tak samo ważny, jak obecnie dostęp przez własne systemy bankowości internetowej czy mobilnej.
- **Elastyczność architektury** – należy spodziewać się szybko zmieniających się modeli biznesowych i mieć narzędzia technologiczne i procesowe pozwalające na szybką odpowiedź na te zmiany. Dotyczy to zarówno architektury, jak i podejścia do rozwoju systemów.
- **Bezpieczeństwo, ale i wygoda** – API musi zapewniać wymagane poziomy bezpieczeństwa, ale jednocześnie intuicyjną integrację z systemami banku.

Jakie mogą być scenariusze użycia API?

Oczywiście przestrzeń możliwych zastosowań może być bardzo duża – poniżej wymienię kilka przykładów:

- Podłączenie aplikacji firmy trzeciej do systemu banku w celu dokonywania płatności za usługi. Klient autoryzuje dostęp do rachunku i potem usługa jest opłacana bez konieczności logowania się do serwisu transakcyjnego banku.

- Automatyczne płatności dokonywane przez zautoryzowane urządzenia (IoT), np. wypożyczenie samochodu czy zakupy dokonywane przez inteligentną lodówkę.
- Przekazanie firmie trzeciej danych wykorzystywanych finansowych dla dokonania analizy predykcyjnej przepływów finansowych.
- Przekazanie danych w celu uzyskania lepszych warunków pożyczki gotówkowej.

W jaki sposób podejść do wdrożenia architektury opartej na API?

Projekt wdrożenia architektury opartej na API możemy podzielić na kilka etapów:

1. **Strategia i priorytetyzacja** – jak w każdym projekcie, przed jego startem musimy zdefiniować cel, jaki chcemy osiągnąć. W tym przypadku oprócz standardowego uzasadnienia biznesowego (*business case'u*) trzeba zastanowić się nad:
   a. strategią monetyzacji API – czyli jak będziemy na API zarabiać,
   b. definicją przypadków użycia (*use cases*).

   Definicja architektury i wybór technologii – zdefiniowanie architektury referencyjnej, standardów i zasad rozwoju API, wybór narzędzi oraz wyspecyfikowanie wymagań dla infrastruktury
2. **Zdefiniowanie zasad zarządzania API** – powołanie ciała odpowiedzialnego za nadzór nad budową i rozwojem architektury, zasad i procesów zarządzania.
3. **Zdefiniowanie i wdrożenie procesów wytwórczych** – wybór metodyki, jej wdrożenie i narzędzi ją wspierających, budowa architektury rozwojowej.
4. **Uruchomienie produkcyjne, testowanie rynku** – stworzenie strategii marketingowej, grup fokusowych, hakathonów. Zbudowanie procesu zarządzania partnerami korzystającymi z API, obsługa prawna, zbudowanie procesów rozliczeniowych (biling za korzystanie z API).
5. **Wsparcie produkcji** – zarządzanie wydaniami, obsługa incydentów, optymalizacja usług.

Czy API Banking to przyszłość czy teraźniejszość?

Wciąż jeszcze wprawdzie czekamy na finalne wersje specyfikacji dla dyrektywy PSD II, wiele banków jednak zdecydowało się już na zbudowanie architektury opartej na API. Poniższe zestawienie przedstawia przykład istniejących wdrożeń architektury API w bankach.

Credit Agricole jest jednym z pierwszych tradycyjnych banków, które udostępniły swoje usługi poprzez publiczne API. W tej chwili z usług banku korzysta ponad osiem aplikacji stworzonych przez zewnętrzne firmy i graczy z sektora fintech.

API CA Store wystawia *Web Services REST*, które pozwalają na dostęp do:

- danych bankowych uwierzytelnionego klienta (rachunków, kart, operacji, itd.),
- oddziałów wg geolokalizacji oraz praktycznych informacji (adresu, godziny, numerów alarmowych, itp.),
- przelewów za pośrednictwem agencji lub rachunku bankowego.

Oprócz podstawowych funkcji API zawiera również kilka takich, które ułatwiają rozwój i utrzymanie stałego poziomu bezpieczeństwa między aplikacjami CA Store. W szczególności są to:

- znormalizowana metoda uwierzytelniania przez serwer aplikacji Store CA (protokół OAuth v1.0a),
- anonimowy mechanizm wychodzących danych (brak informacji o rzeczywistej tożsamości klienta lub numerów rachunków),
- dane testowe dla programistów.

Royal Bank of Scotland (RBS) rozpoczął współpracę z kilkoma startupami technologicznymi w celu rozszerzenia współpracy w obszarze rozliczeń międzynarodowych. RBS łączy swoje usługi z innowacjami dostarczanymi przez startupy.

BBVA uruchomił supermarket API finansowych w celu przyśpieszania innowacji – API jest wykorzystywane przez firmy trzecie do wzbogacania swoich usług o usługi finansowe.

W 2014 r. wdrożył strategię rozwoju cyfrowego, mającą na celu formalne stworzenie banku digitalowego.

W jej ramach nastąpiło otwarcie Open API i poszerzenie oferty o produkty i usługi na jego bazie. Celem było też wsparcie innowacji pochodzących od dostawców zewnętrznych (Fintechów).

Całość koordynuje dedykowany department Open API.

10 dostępnych kategorii: *Merchants categories*, *Basic Stats*, *Customer Zip Codes*, *Age Distribution*, *Gender Distribution*, *Payment Distribution*, *Category Distribution*, *Consumption Pattern*, *Cards Cube*, *Payments Cube*.

Fidor to przykład w całości i od początku cyfrowego banku, który wykorzystał otwartą bankowość do rozbudowy swoich usług. Klienci poprzez API Fidora mogą dodawać nowe waluty do obsługi, traktować jako walutę metale szlachetne, uruchamiać bezpośrednie (*peer-to-peer*) pożyczki, płatności, dołączać funkcje zarządzania finansami (PFM).

Dzięki Open API fintechy mogą oferować swoje usługi łącząc się z Fidor Bankiem, który posiada licencję bankową.

Rozwiązania przygotowywane przez partnerów na bazie Open API są włączane do oferty banku. Największe zainteresowanie API pojawia się w obszarze płatności, zarządzania aktywami oraz kredytów.

Bradesco udostępnił API do integracji z Facebookiem. Dzięki temu klienci mogą sprawdzać saldo rachunku i wykonywać transakcje na nim bezpośrednio ze swojego konta na Facebooku.

Citi udostępnia szereg API, wzbogacając funkcjonalność banku dzięki swoim partnerom technologicznym.

10 listopada 2016 r. bank ogłosił rozpoczęcie nowego globalnego *API Developer Hub* (developer.citi.com), aby szybko połączyć się z deweloperami i zezwalać im na budowanie innowacyjnych rozwiązań szybciej niż kiedykolwiek wcześniej.

Zdaniem banku „*Citi Global Hub* zmienia nasze podejście do otwartej innowacji, dostarczania najnowocześniejszych rozwiązań i tworzenia nowych strumieni wartości dla klientów, partnerów i deweloperów".

Uwolnienie Citi API oznacza ewolucję technologii Citi w otwartej architekturze, co ułatwi współpracę i partnerstwo z firmami fintech oraz markami konsumenckimi na całym świecie oraz da korzyści klientom. Dzięki globalnej *Hub API Developer Citi* przyznają deweloperom dostęp do API w ośmiu kategoriach użytkowania, w tym zarządzania rachunkiem, płatnościami P2P, transakcjami inwestycyjnymi, autoryzacją.

Santander podjął współpracę z Kabbage, aby zapewnić elastyczny dostęp do finansów przedsiębiorstw.

Jeśli firma ma siedzibę w Wielkiej Brytanii i działa jako spółka komandytowa lub spółka z ograniczoną odpowiedzialnością, Santander może pomóc zarządzać przepływami pieniężnymi za pomocą Santander Working Capital. Firma może otrzymać limit od 2 000 GBP do 100 000 GBP w ciągu kilku minut i fundusze w ciągu 24 godzin, jeśli weźmie pożyczkę.

26 maja 2016 r. Santander ogłosił, że jako pierwszy bank w Wielkiej Brytanii wprowadzi blockchain w celu ułatwienia płatności międzynarodowych. Trwa pilot dla personelu, z zamiarem aby rozwinąć technologię w późniejszym terminie.

- Gdy aplikacja zostanie pobrana, wystarczy wypełnić swoje dane profilu i zacząć dokonywać płatności. Łączy Apple Pay, gdzie użytkownicy mogą korzystać z potwierdzenia płatności bezpiecznie używając wybieranie identyfikatora. To pozwala użytkownikom przesyłanie między 10 GBP i 10000 GBP, a płatności mogą być transferowane z GBP na EUR i USD. Płatności w euro mogą być wysłane do 21 krajów, a płatności w dolarach amerykańskich do USA.
- Ripple dostarcza technologię stanowiącą podstawę aplikacji.
- Czołowe banki jak Santander, korzystają z rozwiązań blockchain do poprawy płatności transgranicznych, zmniejszając czas i koszt rozliczenia.

Otwarcie API i organizacja hackathlonów ma na celu zainteresowanie programistów oraz przedstawicieli fintechów współpracą z **Deutsche Bankiem**. Ponadto bank próbuje w ten sposób pozyskać najciekawsze pomysły i inspiracje do tworzenia dalszej strategii w obszarze cyfryzacji.

Uczestnicy hackathlonów są zachęcani do tworzenia innowacyjnych rozwiązań wykraczających poza tradycyjny biznes bankowy: zarządzania wspólnymi wydatkami, optymalizacją podatkową, zarządzaniem ubezpieczeniami, gamifikacją.

Open API:

- ***read_accounts*** – dostęp do odczytu podstawowych danych rachunków, takich jak bieżące saldo czy dane ogólne,
- ***read transactions*** – dostęp do odczytu transakcji dla wszystkich rachunków bieżących danego klienta. API zapewnia dostęp do 90 dni historii transakcji,
- ***read_user_info*** – dostęp do podstawowych danych bieżącego użytkownika, tzn. imienia, nazwiska i daty urodzenia,
- ***read_addressess*** – dostęp do odczytu danych adresowych dla danego klienta. Aktualnie obsługiwane są dwa typy: adres i adres rejestracyjny.

Strategia API – jaką rolę może pełnić bank w nowym ekosystemie?

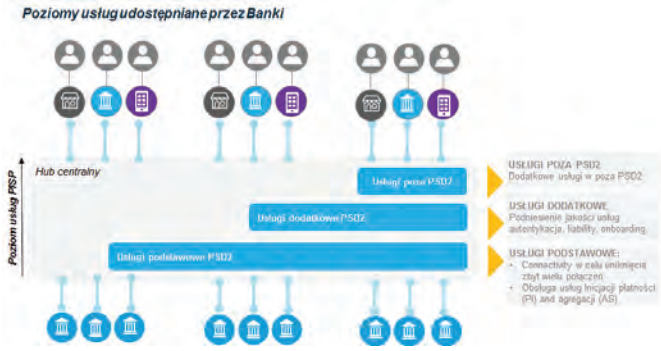
Każdy z banków musi odpowiedzieć sobie na pytanie, jak wykorzystać możliwości, które daje otwarta architektura API i jak zareagować na regulacje wynikające z dyrektywy PSD II. W tej chwili można wyróżnić kilka potencjalnych scenariuszy:

1. **Po prostu zachowanie zgodności** – wykonanie minimalnych zadań wynikających z PSD II, udostępnienie API wymaganych przez dyrektywę. Udostępnienie bez dodatkowych opłat tylko bazowej funkcjonalności, dotyczącej przekazywania informacji o rachunku i inicjowania płatności.
2. **Sprzedawanie dostępu** – dodanie informacji uzupełniających, atrybutów, które nie są wymagane przez dyrektywę i pobieranie opłaty za wykorzystanie takich informacji. Przykładem może być podawanie prostych danych analitycznych o kliencie, danych demograficznych czy informacji o produktach nie opisanych wprost przez PSD II (np. kredyty hipoteczne czy rachunki maklerskie).
3. **Sprzedawanie poszerzonej wiedzy i usług** – przejście z prostego udostępniania API do udostępniania wiedzy na temat klienta. Przykładem może być zaawansowana analityka, marketing, programy lojalnościowe, crowd-sourcing, rabaty/oferty.
4. **Budowanie ekosystemu** – budowa wielu API w celu stworzenia ekosystemu między bankiem, merchantem i klientem w celu zaoferowania finansowych i pozafinansowych produktów i usług. Wykorzystanie omnikanałowości, analityki, zintegrowanego IT i współdzielenie informacji w całym przedsiębiorstwie.

Każdy z tych scenariuszy różni się potencjalną wartością, którą można uzyskać oraz wysiłkiem, który jest wymagany do wdrożenia tego scenariusza. Po kolei:

1. **Po prostu zachowanie zgodności** – to scenariusz, którego uruchomienie będzie wymagało relatywnie małego wysiłku, ale też nie przyniesie dużej wartości.
2. **Sprzedawanie dostępu** – ten scenariusz wymaga wciąż niewielkiego wysiłku przy większym potencjale wartości niż scenariusz pierwszy.
3. **Sprzedawanie poszerzonej wiedzy i usług** – ten scenariusz z kolei wymaga większego wysiłku, ale może przynieść relatywnie większe zyski.
4. **Budowanie ekosystemu** – ta opcja wymaga zdecydowanie największego wysiłku i przygotowania, ale też może przynieść bankowi największą wartość.

Ilustracja poniżej przedstawia poziomy usług, które mogą być udostępniane przez banki w ramach otwartego API.



Podsumowanie

Architektury i ekosystemy oparte na API są już rzeczywistością w większości sektorów gospodarki. Pojawianie się nowych graczy, przenikanie się sektorów, szybkie zmiany rynku wymuszają wykorzystanie istniejących rozwiązań. Rozwój internetu rzeczy (IoT) jest kolejnym stymulatorem wykorzystania API.

Sektor finansowy i bankowość będą musiały przejść na otwarte architektury oparte na API – zarówno ze względów czysto rynkowych, jak i regulacyjnych – zmiana te będzie wymagana po wejściu w życie dyrektywy PSD II. Przed bankami stanie wybór strategii dostosowania się do wymagań PSD II i rynku – dostępne jest tutaj całe spektrum rozwiązań – od prostego wdrożenia API wymaganych prawem do budowania ekosystemu biznesowego w oparciu o API. W każdym przypadku konieczne jest jednak wdrożenie funkcji zarządzania API.

Dr Mariusz Cholewa
Prezes Zarządu BIK

Absolwent Wydziału Zarządzania Uniwersytetu Gdańskiego (1995 r.). W 2005 r. uzyskał tytuł doktora nauk ekonomicznych w zakresie ekonomii. Ukończył również podyplomowe studia Bankowości i Finansów, specjalność bankowość inwestycyjna, organizowane przez Uniwersytet Guildhall w Londynie, Akademię Bankową oraz Uniwersytet Gdański. W latach 1993-1998 współpracował z Gdańską Akademią Bankową, m.in. jako członek zarządu, a jednocześnie brał udział w badaniach dotyczących restrukturyzacji finansowej przedsiębiorstw i banków, prowadzonych przez Instytut Badań nad Gospodarką Rynkową. W latach 1995-2003 wykładał na Uniwersytecie Gdańskim na Wydziale Zarządzania. W okresie 2007-2010 był prezesem Zarządu Banku Rozwoju Cukrownictwa SA. Od 1998 r. związany z Bankiem Handlowym w Warszawie SA, gdzie zajmował szereg stanowisk managerskich, a do kwietnia 2013 r. był dyrektorem Departamentu Strategii. Zasiadał w radach nadzorczych wielu spółek, m.in. z branży bankowej, inwestycyjnej i ubezpieczeniowej. Od 2012 r. był członkiem Rady Nadzorczej Biura Informacji Kredytowej S.A. Od czerwca 2013 r. pełni funkcję prezesa Zarządu BIK S.A.

Andrzej Zduńczyk
Dyrektor Departamentu Produktów Bankowych Biura Informacji Kredytowej.

Absolwent Wydziału Finansów i Bankowości Uniwersytetu Łódzkiego. Swoją przygodę z bankowością rozpoczął w roku 1999 w banku PKO BP. Od czerwca 2003 r. związany z duńskim bankiem Nykredit Realkredit A/S, gdzie zajmował stanowiska eksperckie związane z obszarem oceny ryzyka kredytów hipotecznych. Pracę z Biurze Informacji Kredytowej S.A. rozpoczął w grudniu 2008 r. w obszarze produktów dedykowanych sektorowi bankowemu. Od października 2015 r. pełni funkcję Dyrektora Departamentu Produktów Bankowych BIK i jest odpowiedzialny m.in. za biznesowe utrzymanie i rozwój oferty produktowej BIK kierowanej do banków.

dr Mariusz Cholewa, Andrzej Zduńczyk
Biuro Informacji Kredytowej

Wykorzystanie danych alternatywnych w lepszym zarządzaniu ryzykiem

Według szacunków Banku Światowego aktualnie na świecie blisko 2 mld dorosłych osób nie posiada rachunku bankowego. W blisko 60% przypadków osoby te mają po prostu zbyt niski dochód by mogły bądź by opłacało się im korzystać z oferty banków. W pozostałych przypadkach kluczowe bariery to brak dostępności usług bankowych, brak zaufania do banków czy przyczyny natury religijnej.[1]

Na 2 mld nieubankowionych osób warto również spojrzeć w kontekście stosowanych przez banki metod oceny klientów ubiegających się o kredyt czy pożyczkę. Otóż w procesie oceny ryzyka stosują one powszechnie metody oceny punktowej (*scoring*), które porównują profil wnioskującego klienta z profilem klientów, którzy już otrzymali kredyt w oparciu o dane, jakie o nich posiadają. W przypadku osób nieposiadających relacji z bankowością lub posiadających zbyt krótką lub negatywną historię kredytową, naliczenie *scoringu* często nie jest możliwe lub nawet jeśli *scoring* zostanie naliczony to wynik – ocena punktowa – jest z reguły poniżej poziomu, od którego klient kwalifikuje się do finansowania. Zatem w praktyce osoby te nie mają szans na uzyskanie kredytu czy jakiejkolwiek innej formy finansowania w bankach. Mamy zatem do czynienia z tzw. „wykluczeniem finansowym", które skutkuje tym, że ludzie zmuszeni są pozyskiwać finansowanie poza sektorem bankowym, często na znacznie gorszych warunkach. Warto zauważyć, że w przypadku firm aż 200 mln głównie mikrofirm cierpi na brak możliwości pozyskania finansowania.[2]

1 http://www.worldbank.org/en/topic/financialinclusion/overview#1

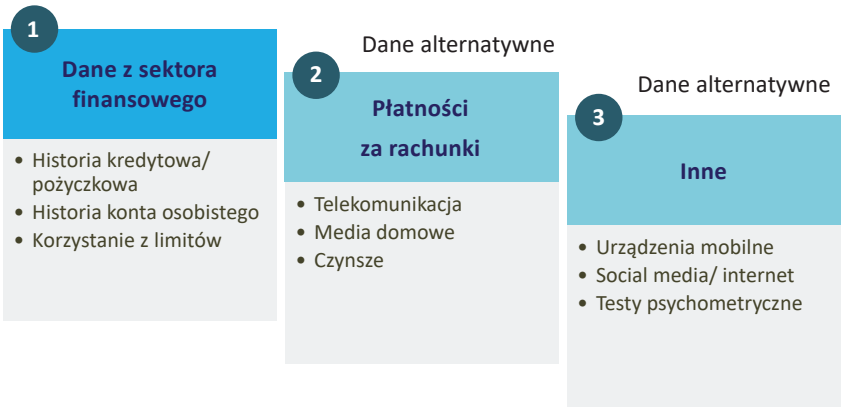
2 http://www.worldbank.org/en/topic/financialinclusion/overview#1

Dane alternatywne szansą dla „wykluczonych finansowo”

Wykluczenie finansowe blokuje istotnie możliwości poprawy statusu materialnego zarówno osób fizycznych, jak również ogranicza szanse rozwoju małych firm, które, jak powszechnie wiadomo, są zwykle jednym z istotnych motorów wzrostu gospodarki danego kraju. Co ciekawe, problem „wykluczenia finansowego”, wbrew pozorom, dotyczy nie tylko krajów trzeciego świata, ale również gospodarek wysoko rozwiniętych, takich jak np. Stany Zjednoczone, gdzie zgodnie z badaniami organizacji PERC (*Policy&Economic Research Council*) ok. 55 mln osób jest wykluczonych z finansowania bankowego z uwagi na brak lub zbyt krótką historię kredytową w bankach.

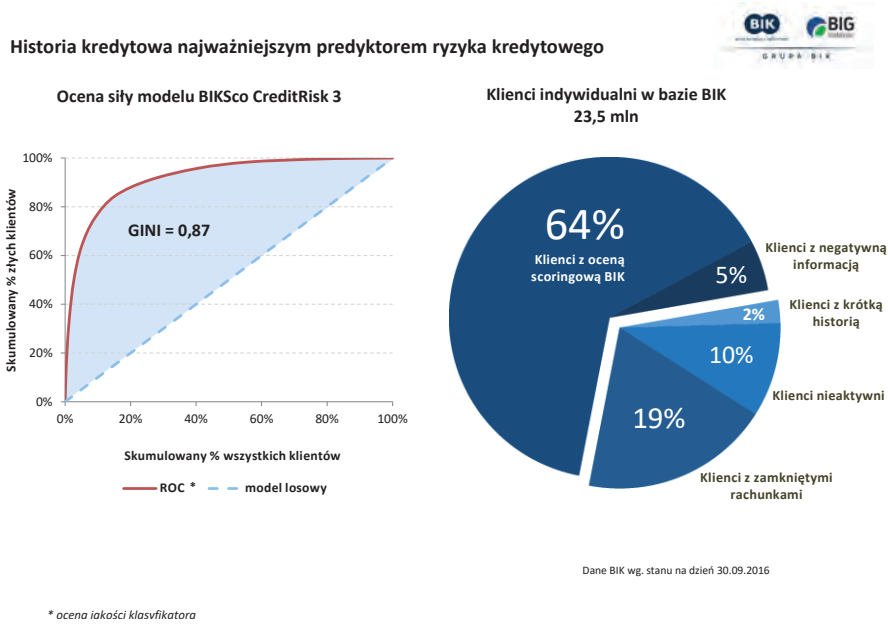
Jak pokazują badania i doświadczenia z ostatnich kilku lat, pomocne w ograniczaniu zjawiska „wykluczenia finansowego” może być wykorzystanie przez banki tzw. danych alternatywnych. Rozumie się przez nie wszelkie dane pochodzące spoza sektora finansowego, a dotyczące w szczególności terminowości regulowania rachunków w firmach telekomunikacyjnych czy użyteczności publicznej (np. prąd, gaz, wodociągi) oraz aktywności klienta w sieci, sposobu w jaki klient korzysta z telefonu komórkowego czy też danych pozyskanych w oparciu o testy psychometryczne.

Hierarchia ważności danych w ocenie ryzyka kredytowego



Zarówno doświadczenia światowe, jak i na gruncie polskim wskazują, że nadal największą wartość w kontekście oceny ryzyka kredytowego stanowią

„twarde" dane z sektora finansowego, takie jak: historia kredytowa czy pożyczkowa, wykorzystanie limitów a także dane dotyczące operacji i transakcji na koncie osobistym klienta. Przykładem z rodzimego podwórka może być model oceny ryzyka BIKSco CreditRisk3, zbudowany w oparciu o historię kredytową klienta w sektorze bankowym, którego siła dyskryminacyjna wyrażona wskaźnikiem GINI[3] na poziomie 0,87 stanowi poziom praktycznie nieosiągalny dla modeli ryzyka opartych o dane alternatywne.



Jednak mimo, iż dane alternatywne zajmują niższe miejsce w hierarchii ważności, to jednak okazują się nieocenione w ocenie ryzyka kredytowego klientów, którzy posiadają krótką lub nie posiadają w ogóle historii kredytowej. Analizy przeprowadzone przez wspomniany wcześniej PERC udowadniają, że włączenie w proces oceny ryzyka klientów „wykluczonych finansowo" danych o terminowości płatności rachunków w firmach użyteczności

3 Wskaźnik GINI – Pozwala ocenić zdolność modelu scoringowego do pozycjonowania kredytobiorców wg poziomu ryzyka. Pokazuje na ile zastosowanie do oceny ryzyka klienta modelu scoringowego będzie lepsze od stosowania losowego systemu podejmowania decyzji. Wskaźnik ten zawiera się w przedziale od 0 do 1. Im wyższy wskaźnik, tym większa korzyść ze stosowania modelu scoringowego. W praktyce zakłada się, że poprawnie działający aplikacyjny model scoringowy przyjmuje wartość wskaźnika GINI >0,35

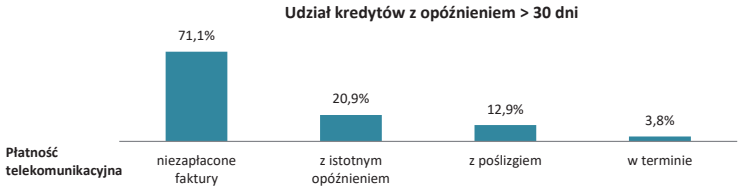
publicznej (dostawcy wody, ogrzewania, energii elektrycznej), u operatorów sieci kablowych czy w firmach telekomunikacyjnych przynosi wymierne rezultaty. W przypadku USA uwzględnienie tych danych w modelu scoringowym umożliwiło ocenę ryzyka dla blisko 22 mln osób, które były dotychczas wykluczone z finansowania bankowego z uwagi na brak, zbyt krótką lub złą historię kredytową. Dodatkowo połowa ankietowanych przez PERC stwierdziła, że przekazywanie pełnej historii płatności z wspomnianych wyżej firm do biura kredytowego i jej wykorzystanie w scoringu wpłynęłoby na większą skłonność do regulowania płatności na czas.

Również z badań firmy Experian wynika, że ok. 20% klientów uzyskałoby lepsze warunki finansowania, gdyby modele oceny ryzyka uwzględniały również terminowość opłat klienta realizowanych w firmach użyteczności publicznej (np. dotyczących zużycia woda, prądu, gazu itp.).

Jak wykorzystać doświadczenia dotyczące danych alternatywnych na ryku polskim?

W Biurze Informacji Kredytowej przeprowadzono analizę zależności pomiędzy terminowością regulowania zobowiązań telekomunikacyjnych, a problemami ze spłatą kredytów bankowych. W ramach przeprowadzonego badania przy zastosowaniu mechanizmów anonimizacji danych porównano informacje zgromadzone o kliencie w BIK (status płatności kredytowych) w danym miesiącu z informacjami zgromadzonymi na temat klienta w Burze Informacji Gospodarczych InfoMonitor (informacje gospodarcze dot. płatności telekomunikacyjnych). Zgodnie z wynikami przeprowadzonych badań, udział klientów indywidualnych posiadających problemy ze spłatą kredytów jest najwyższy dla osób, które nie płacą faktur za telefon (aż 71,1% klientów) i maleje wraz z liczbą dni opóźnienia w spłacie rachunku telefonicznego. Wśród osób opłacających rachunki w terminie tylko 3,8% ma problemy ze spłatą kredytów. Badania wykazały zatem silną zależność pomiędzy sposobem regulowania rachunków telefonicznych a regulowaniem zobowiązań kredytowych.

Silna zależność danych kredytowych oraz telekomunikacyjnych w ocenie ryzyka



Dane BIK wg. stanu na dzień 30.09.2016

Warto ponadto podkreślić, że np. w przypadku podmiotów gospodarczych, których dane znajdują się w BIG InfoMonitor blisko 2/3 tj. ok. 400 tys. posiada historię płatności tylko w sektorze pozabankowym, innymi słowy firmy te nie korzystają z finansowania bankowego, zatem nie ma informacji o historii spłat ich kredytów w BIK.

Czy zatem regularna spłata zobowiązań pozabankowych może być gwarantem prawidłowości obsługi zobowiązań kredytowych w przyszłości? Czy przerwa w regularnych płatnościach może być sygnałem o przyszłych problemach ze spłatą kredytów? Wyniki badań dla firm wykazały, że pojawienie się przerwy w płatnościach w ostatnim badanym miesiącu dwukrotnie zwiększało szansę na to, że w kolejnych sześciu status płatności kredytów ulegnie pogorszeniu (opóźnienie w spłacie przekroczy 30 dni). Podobne wyniki otrzymano dla klientów indywidualnych. Brak płatności za telefon jest zatem ostrzeżeniem o potencjalnych przyszłych problemach ze spłatą zobowiązań kredytowych. Wyniki analiz wykazały ścisłą zależność pomiędzy terminowością spłacania zobowiązań poza kredytowych, a wiarygodnością kredytową klientów.

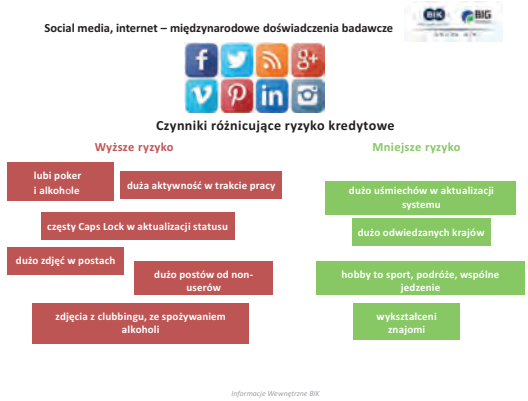
Modele scoringowe oparte o sposób korzystania z urządzeń mobilnych

Szacuje się, że ok. 75% „wykluczonych finansowo" posiada telefony komórkowe (w większości w formule *pre-paid*). Firmy, takie jak Cignifi, First Access czy EFL, dostarczające rozwiązania do oceny ryzyka, stworzyły modele *scoringowe*, które na bazie danych związanych ze sposobem korzystania z telefonu komórkowego prognozują skłonność klienta do spłaty kredytu. Okazuje się bowiem, że np. czym więcej inicjujemy połączeń (w przeciwieństwie do ich

odbierania) oraz czym dłużej trwają nasze pojedyncze rozmowy telefoniczne, tym jako klienci jesteśmy mniej ryzykowni kredytowo. Za to odbieranie dużej liczby połączeń w godzinach pracy lub posiadanie niewielkiej grupy osób, do których telefonujemy to czynniki identyfikujące podwyższone ryzyko kredytowe. Implementacja przez firmę Cignifi w Meksyku, Chile i Brazylii scoringu uwzględniającego zachowania związane z korzystaniem telefonu komórkowego zaowocowało ponad 25-procentowym wzrostem poziomu akceptacji wniosków kredytowych (karty kredytowe, krótkoterminowe pożyczki) przy jednoczesnym zachowaniu poziomu ryzyka na niezmienionym poziomie.

Social Media w ocenie punktowej

Lenddo, DemystData oraz Kreditech to firmy, które używają danych z szeroko rozumianych *social mediów* do swoich modeli scoringowych. Dane te wykorzystywane są zarówno do wsparcia identyfikacji klienta, jak również estymacji dochodu czy statusu zatrudnienia. Znaczna liczba danych i źródeł, z których one pochodzą sprawia, iż powszechną praktyką jest wzajemne ich porównywanie oraz sprawdzanie ich spójności np. z danymi zadeklarowanymi przez klienta na wniosku kredytowym. Czynniki różnicujące poziom ryzyka są często dość zaskakujące, np. włączony Caps Lock w trakcie aktualizacji statusu na portalu społecznościowym, podobnie jak duża liczba zdjęć w postach wskazuje na podwyższone ryzyko kredytowe klienta, podczas gdy np. zamiłowanie do podróży, objawiające się dużą liczbą odwiedzonych krajów wiąże się z wyższym prawdopodobieństwem terminowej obsługi kredytu przez klienta.



Testy psychometryczne a ryzyko kredytowe

Testy psychometryczne to nic innego, jak kwestionariusze czy quizy on-line mające na celu pomiar wiedzy, umiejętności, postawy oraz cech osobowości klienta, które mogą mieć przełożenie na poziom ryzyka kredytowego. Analizując odpowiedzi na szereg pytań, firmy takie jak np. VisualDNA czy EFL są w stanie określić prawdopodobieństwo spłaty kredytu oraz inne czynniki ryzyka. Dla przykładu, informacje takie jak relacje z innymi oraz zdolność wnioskodawcy do logicznego myślenia w trudnych sytuacjach sugeruje w jaki sposób wnioskodawca może reagować, jeśli jego sytuacja finansowa się pogorszy. Testy psychometryczne sprawdziły się na rynkach rozwijających, gdzie np. dzięki rozwiązaniu firmy VisualDNA osiągnięto 50-procentowy wzrost poziomu akceptacji dla klientów z krótką lub bez historii kredytowej przy jednoczesnym braku wpływu na poziomu szkodowości portfela.

Historia transakcji na koncie płatniczym

Do dalszego rozwoju metod i środków oceny ryzyka w oparciu o dane alternatywne może przyczynić się Dyrektywa PSD II, w myśl której uprawnione podmioty trzecie (tzw. *Account Information Service Providers*) otrzymają, za zgodą klienta, dostęp do danych transakcyjnych z jego rachunków płatniczych w bankach. Można się z całą pewnością spodziewać, że zarówno banki, jak i fintechy będą tutaj szukać szansy budowy zarówno modeli oceny ryzyka, jak i modeli szeroko rozumianej segmentacji klientów. Należy pamiętać, że historia transakcji na koncie osobistym zaliczana jest do tzw. „twardych" wartościowych danych behawioralnych, stąd można oczekiwać, że również modele oparte o te dane będą cechować się wysoką siłą predykcyjną. Czas pokaże, czy dane transakcyjne w połączeniu z innymi danymi alternatywnymi pozwolą na stworzenie metod i modeli oceny ryzyka, które będą równie predykcyjne, jak poczciwa historia kredytowa klienta.

Dotychczasowe doświadczenia z wykorzystaniem danych alternatywnych do oceny ryzyka kredytowego klienta pokazują wymierne korzyści w zakresie oceny tych nie posiadających wystarczającej historii kredytowej (brak historii lub za krótką historię). Przekłada się to na redukcję zjawiska wykluczenia finansowego dzięki zwiększeniu dostępności finansowania bankowego zarówno dla osób fizycznych, jak i podmiotów gospodarczych. Kluczowe może

okazać się umiejętne wykorzystanie danych o historii płatności rachunków w instytucjach użyteczności publicznej. Jak udowadniają analizy prezentowanie w niniejszym artykule, zachowania płatnicze klientów w tym obszarze mają bezpośrednie silne przełożenie na poziom ryzyka kredytowego. Testy psychometryczne, dane z telefonów komórkowych, dane dotyczące aktywności klientów w *social mediach* mogą stanowić cenne, aczkolwiek z punktu widzenia banków raczej uzupełniające źródło danych alternatywnych do wiarygodnej oceny ryzyka kredytowego klienta.

Adam Marciniak
Dyrektor Pionu Rozwoju i Utrzymania Aplikacji w PKO Banku Polskim

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 roku zyskał dodatkowe kwalifikacje – specjalisty ds. projektów informatycznych kończąc studia w Instytucie Sterowania i Elektroniki Przemysłowej Politechniki Warszawskiej.
W 2004 roku rozpoczął pracę w Pekao SA, jako programista i projektant systemów informatycznych. 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. jest dyrektorem Pionu Rozwoju i Utrzymania Aplikacji w PKO Banku Polskim. Odpowiada, m.in. za kompleksową realizację projektów IT, 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.
Obecnie jest również Członkiem rad nadzorczych PKO FINAT i PKO Banku Hipotecznego, a także Członkiem Prezydium Rady Bankowości Elektronicznej oraz wiceprzewodniczącym Forum ds. IT przy Związku Banków Polskich (ZBP).

Adam Marciniak, PKO Bank Polski

Digitalizacja w wielkim banku

Jak wygląda cyfryzacja bankowości z perspektywy największego polskiego Banku

Polska znajduje się u progu bezprecedensowej przemiany technologicznej, za którą stoi cyfryzacja codziennych aspektów naszego życia. Ta znacząca transformacja prowadzi do zmiany sposobu kontaktu obywateli z państwem, zrewolucjonizuje całe branże i zmieni to, jak ze sobą współdziałamy. To też obiecujący sposób na ożywienie gospodarki. Dlatego przejście Polski od „papierowej" do „cyfrowej" jest częścią przyjętego „Planu na Rzecz Odpowiedzialnego Rozwoju".

Bankom, które same muszą stawać się coraz bardziej cyfrowe, jest jak najbardziej po drodze z elektronicznym państwem. Są one nośnikami nowoczesnych technologii i rozwiązań finansowych ułatwiających codzienne życie milionom Polaków. Inicjują innowacyjne rozwiązania z myślą o tzw. cyfrowym obywatelu. Banki poczyniły już także duże postępy w cyfryzacji. Są to przede wszystkim obszary powszechnej dostępności bankowości elektronicznej, identyfikacji i uwierzytelniania użytkownika. Te doświadczenia i systemy zostały już wykorzystane w administracji publicznej. Przykładami współpracy banków i administracji jest możliwość składania wniosków o świadczenie z programu „Rodzina 500 plus" i Platforma Usług Elektronicznych ZUS dostępna poprzez serwisy bankowości internetowej czy integracja z Profilem Zaufanym.

Trend ten będzie dalej kontynuowany. Jednym z głównych kierunków opracowanej nowej strategii PKO Banku Polskiego jest właśnie digitalizacja.

Zakłada ona nie tylko wyjście naprzeciw potrzebom klientów, którzy chcą prostych, mobilnych, elastycznych i dopasowanych rozwiązań, ale także ewolucję procesów wewnętrznych Banku. Postrzegamy cyfryzację jako naturalną konsekwencją rozwoju technologicznego oraz zmieniających się preferencji konsumentów usług finansowych. Jest ona także sposobem na podnoszenia efektywności działania naszego banku na rynku, który podlega coraz bardziej restrykcyjnym i kosztownym regulacjom.

Liderzy digitalizacji

Trendy w zakresie cyfrowych doświadczeń klienta wyznaczają dziś globalni potentaci, jak Amazon, Google, Facebook czy też Apple, Samsung i wreszcie PayPal. Skala ich działalności kształtuje przyzwyczajenia i oczekiwania kolejnych generacji konsumentów. Na rynku finansowym z ich praktyk umiejętnie korzystają coraz liczniejsze startupy fintech. Wnoszą one na rynek finansowy potencjał rozwojowy i pomysłowość poprzez naturalne zrozumienie i wpisanie się w potrzeby cyfrowych konsumentów. Banki już teraz starają się wykorzystać te nowe możliwości wchodząc z nimi w kooperację, wskazując i stymulując ich rozwój w obszarach swoich zainteresowań czy wreszcie dokonując przejęć w tym segmencie.

PKO Bank Polski jest Partnerem Głównym programu akceleracyjnego MIT Enterprise Forum Poland skierowanego do startupów. Dzięki niemu młode polskie firmy z branży technologicznej mają możliwość skorzystania ze wsparcia międzynarodowego zespołu mentorów i doświadczonych ekspertów, współpracy z MIT Technology Review, a także networkingu w rozległym ekosystemie innowacji skupionym wokół Massachusetts Institute of Technology. Jednym z podstawowych celów tego projektu jest ułatwienie skutecznej komercjalizacji technologii cyfrowych. Jako Bank podjęliśmy także bezpośrednią współpracę z polskimi naukowcami. W ubiegłym roku rozpoczęte zostały z Politechniką Gdańską prace nad kompleksowym rozwiązaniem biometrycznym.

Korzyści dla banków

Digitalizacja jest źródłem wymiernych korzyści pozytywnie wpływając na efektywność biznesową i doświadczenia klientów. Nowoczesne rozwiązania

doskonalą obsługę klienta i dają mu do wyboru najłatwiejsze i najszybsze drogi do korzystania ze swojego konta i oferty banku. W efekcie zapewniają wzrost bazy klientów, szczególnie przyrost liczby młodych klientów, wychowanych już w świecie ery cyfrowej (tzw. *digital natives*). Do korzyści digitalizacji można również zaliczyć wyższe uproduktowienie, lepsze wskaźniki retencji, a także ograniczenie kosztów operacyjnych. W modelu wysokiego ucyfrowienia czynności o niższej wartości przychodowej i mniej skomplikowane realizowane są w kanałach zdalnych przez samych klientów, co pozwala efektywniej gospodarować czasem i zasobami pracowników tradycyjnej sieci oddziałów, a tym samym pozwala wzmocnić ich rolę doradczą.

Wyzwania digitalizacji

Wydaje się, że dzięki tej transformacji banki czeka świetlana przyszłość, jednak jest to jednostronny ogląd sytuacji. Cyfryzacja procesów bankowych to zarówno szansa, ale też i znaczne wyzwanie dla sektora bankowego. Rysuje się co najmniej klika kluczowych problemów.

Pierwsza kwestia to odpowiednie dostosowanie cyfrowych usług, ich użyteczności do potrzeb klientów banków a w konsekwencji ich pełne, zakładane wykorzystanie. Dla przykładu, obecne statystyki wskazują, że większość klientów kanału mobilnego ogranicza swoją aktywność jedynie do sprawdzenia wysokości swojego salda na rachunku i wykonania prostych transakcji.

Kolejnym problemem i jedną z głównych barier adaptacji, mogącą ograniczyć rozwój usług cyfrowych, są obawy klientów o bezpieczeństwo realizowanych w oparciu o nie transakcji. Ich konstrukcja musi być nierozerwalnie powiązana z, niejako osadzonym w nich, aspektem bezpieczeństwa danego produktu.

Pamiętając o bezpieczeństwie transakcji i ochronie użytkownika musimy balansować na cienkiej granicy pomiędzy użytecznością z jednej strony, a zapobieganiem obniżania standardów bezpieczeństwa z drugiej. Przenoszenie naszego życia w wymiar elektroniczny wymaga także wzmożonej odporności na cyberataki zarówno bankowych rozwiązań w internecie, jak i aplikacji mobilnych.

Za wirtualizacją procesów bankowych stoi również wydajność systemów, baz danych, ich dostępność, replikacja, synchronizacja czy dywersyfikacja oraz cały szereg aspektów technologicznych rozwiązań IT wymagających

właściwego ich skalowania do działalności banku i elastyczności dla przeniesienia wymaganego, zmiennego w czasie i praktycznie nieprzewidywalnego obciążenia. Towarzyszy temu również wymóg generowania nowej wartości dla organizacji w tempie dotychczas nieobserwowanym w świecie zdominowanym przez techniczne środki produkcji, jakim jest IT.

Cyfryzacja jest niewątpliwie narzędziem do poprawiania warunków bytowych klientów, niosąc całkowicie nową jakość. Jednak relacje między cyfryzacją procesów bankowych a tradycyjną formą powinny być bardzo dobrze zbalansowane, potrzeba szerszej strategii nie tylko rozwiązań technicznych. Jest to tym bardziej istotne, iż jesteśmy u progu zmian w strukturze społecznej. Brak takiej równowagi może prowadzić do wykluczenia osób starszych, nieposiadających odpowiednich kompetencji. Przykładowo, pewnej grupy klientów nie przyciągniemy do bankowości aplikacją mobilną, natomiast stopniowe wprowadzanie ich w świat bankowości cyfrowej może odbywać się poprzez bankowość internetową i dalszą edukację w tym kanale.

Wreszcie cyfryzacja to koszt a bezpieczna cyfryzacja to jeszcze większy koszt. Natomiast tak jak przy większości innowacji możliwości zarabiania są odłożone w czasie. W dobie szukania oszczędności, uzyskanie właściwego balansu pomiędzy tymi elementami będzie dużym wyzwaniem przy konstruowaniu obecnych budżetów, tak aby ewentualne nie przekreśliły one możliwości sięgnięcia po rysujące się szanse biznesowe.

Cyfrowa transformacja banku

Niewątpliwie firmy, które chcą wykorzystać cyfryzację muszą w pełni zrozumieć, gdzie jest ich źródło wartości w nowych technologiach. Dla jednych firm może to być marketing, dla innych sprzedaż, może być to także automatyzacja procesów lub wreszcie kombinacja tych wszystkich elementów.

Jednak warto podkreślić, iż w każdym przypadku niezbędne jest zbudowanie odpowiedniego zaplecza dla tej transformacji. Jej skuteczność wymaga bowiem zrównoważonego podejścia do cyfryzacji odczuwanej przez klientów, jak też cyfryzacji samego środowiska pracy organizacji. Należy mieć także świadomość, że cyfryzacja to inwestycja w proces zmian, realizowany na przestrzeni dłuższego czasu a nie doraźnie.

Do tej pory digitalizacja w PKO BP miała zasadniczo charakter projektowy lub programowy (tj. połączenia kliku projektów w jeden strumień), np.

wdrożenie IKO, rozwój CRM, Polski Standard Płatności, iPKOdealer czy iPKObiznes.

Dopiero w planie strategicznym na lata 2016–2020 rola digitalizacji znacząco wzrasta poprzez zdecydowanie większy wpływ na całą filozofię prowadzonej przez nasz bank działalności. Przyjęty model transformacji cyfrowej zakłada skupienie naszej aktywności rozwojowej wokół trzech obszarów wartości, tj. doświadczenia klienta (*customer experience*), wzrostu efektywności operacyjnej oraz rozwoju nowych źródeł przychodów.

Nadrzędnym celem ma być satysfakcja klienta i jego pozytywne doświadczenia w kontakcie z bankiem. Liczy się szybkość i wygoda. Służyć temu będzie m.in. zmniejszenie liczby dokumentów papierowych, rozbudowa bazy wiedzy o klientach i ułatwienie dostępu do tych zasobów, jak też czerpanie z niej wiedzy, a także jednolita obsługa w kanałach czy wreszcie wykorzystanie potencjału współpracy z zewnętrznymi firmami (w tym fintech) do zwiększenia wartości dodanej usług bankowych.

Ważnym komponentem tego modelu będzie również digitalizacja wewnętrzna, czyli zmiany w obszarze procesów *backoffice'owych* organizacji. Motywujące i elastyczne środowisko pracy, nowe rodzaje stanowisk, automatyzacja procesów, robotyzacja czy dostępność nowych narzędzi ułatwiających współpracę to tylko wybrane przykłady.

W praktyce operacyjnej digitalizacja w naszym banku przekłada się na doskonalenie takich domen jak: omnikanałowość, analityka, procesy E2E, organizacja (*backoffice*) oraz bezpieczeństwo (np. wspomniany już projekt biometryczny realizowany wspólnie z Politechniką Gdańską).

W naszym rozumieniu digitalizacja jest w dużej mierze odpowiedzią na oczekiwania klientów. Klienci chcą dziś korzystać z przyjaznej bankowości 24 godziny na dobę, z dostępem do sprofilowanej informacji i fachowego, spersonalizowanego, proaktywnego doradztwa w czasie rzeczywistym. Temu mają służyć zakładane inicjatywy rozwojowe naszego banku.

Bez wątpienia paliwem cyfryzacji są dane, tym bardziej że ich ilość rośnie lawinowo. Stanowią one bardzo cenny zasób w rękach banków, ale żeby ten skarb wykorzystać, by dane monetyzować potrzebne są rozwiązania pozwalające na spięcie w całość wszystkich elementów w organizacji.

Już dziś biznes wymaga szybkiego, niezawodnego dostępu do danych on-line, z kolei PSD II, poprzez wprowadzenie koncepcji otwartego API, jak nigdy dotąd podniesie jeszcze dodatkowo aspekt ich bezpieczeństwa oraz

ciągłości działania usług. Tym bardziej, że wdrożenie bankowego interfejsu nie tylko umożliwia dostęp do danych w banku, ale również pozwala otworzyć się bankom na nowych, zewnętrznych usługodawców.

Cyfrowe platformy biznesowe

Można się spodziewać, że najbliższych latach to nie tylko sposób przetwarzania i zastosowania danych na temat oczekiwań klientów, lecz także umiejętność bliskiej współpracy i wymiany wiedzy w oparciu o nie z innymi podmiotami na rynku będzie także kluczem do sukcesu biznesowego. Stąd konieczność zmiany dotychczasowego podejścia i budowania rdzenia do zarządzania cyfrowymi środkami banku otwartego na zmienne uwarunkowania zewnętrzne. W jej konsekwencji będziemy obserwować intensywny rozwój platform elektronicznych łączących dane i transakcje firm.

Tradycyjne instytucje finansowe replikują „stałe systemy". Widok biznesu firmy przez taki system zakłada bardzo jasny podział na wewnątrz i na zewnątrz, ludzi wewnątrz i dostawców dostarczających określone wejścia, zasoby. W efekcie oznacza to możliwości tworzenia produktów i usług poprzez zafiksowane procesy biznesowe i określone technologie. Wprowadzanie ich w stosunkowo krótkim okresie wymaga od organizacji dużych nakładów, a w przypadku ich modyfikacji dodatkowo naraża firmy na znaczne koszty i ryzyko. Te produkty i usługi są dostarczane do klientów głównie poprzez posiadane lub związane z tymi systemami kanały.

Nowe podejście wiąże się z tworzeniem cyfrowej platformy, która integruje się z szerokimi ekosystemami wartości dla klientów. Umożliwia ona budowanie nowoczesnych produktów na bazie już istniejących rozwiązań, tym samym stale zwiększając propozycje wartości całego ekosystemu. Taka platforma stwarza także możliwości rozwoju wielu modeli biznesowych czy typów przychodów, np. wynajem czy subskrypcja.

Te sieci biznesowe, określone ekosystemami, dzięki nowym technologiom cyfrowym będą mogły zaoferować znacznie lepsze produkty i usługi, niż te firmy, które działają w pojedynkę. Zagwarantują one efektywną współpracę cyfrowych organizacji zarówno z sektorem komercyjnym, jak i państwowym.

Co więcej, doskonale wpisują się one także w gwałtownie rosnące zapotrzebowanie na bezpieczeństwo produktów, procesów i usług w cyfrowej gospodarce. Dzięki nim możliwe będzie uwierzytelnianie w różnych serwisach

firm trzecich (serwisy e-commerce, systemy płatnicze, portale administracji publicznej) oraz rozwijanie szerokich możliwości silnej identyfikacji klientów w środowisku mobilnym kładącej nacisk na lokalizację i inne nie sprzętowe rozwiązania uwierzytelnienia biometrycznego.

Banki, pełniąc rolę instytucji zaufania publicznego, pozostają naturalnym, głównym graczem w tym ekosystemie uwierzytelniania tożsamości klientów cyfrowego świata. Otwarte API banków, wspierające w tym zakresie środowiska powstających, nowych cyfrowych możliwości, tj. serwisy społecznościowe, ekosystemy partnerskie firm trzecich i inne zasoby są źródłem generującym bezwzględnie nowe wartości dla cyfrowych klientów. Rodzi to także możliwość „sterowania" siłą uwierzytelnienia poprzez dobór lub wybór określonych elementów z różnych zasobów, także zewnętrznych, jak i zebranych danych biometrycznych klienta.

Platformo-centryczne firmy oraz rozwój tak tworzonego ekosystemu wartości dla klienta wymagają innego biznesowego myślenia i tworzą potencjalnie bardzo potężną dźwignię wzrostu dla organizacji już od samego momentu ich wdrożenia.

To właśnie platformy biznesu cyfrowego, wespół z konkretnymi produktami, będą decydować o przewadze konkurencyjnej firm. To one pozwolą na szybszą implementację w działalności biznesowej nowych produktów, usług czy innowacji, ich weryfikację i potencjalną modyfikację dla lepszego dopasowania do sposobu ich wykorzystywania przez klientów.

Digitalizacja IT

W tej wirtualizującej się rzeczywistości oprogramowanie, aplikacja i kod w coraz większym stopniu stają się nieodłącznym elementem całości tworząc rdzeń nowego cyfrowego biznesu.

Dlatego też tę specyfikę nowego podejścia do działalności cyfrowego banku, w coraz większym stopniu opartej o świat technologii, należy także przenosić na obszar IT.

IT rozumiane jako platforma elastyczna, pozwalająca na rozbudowę warstwy aplikacyjnej we współpracy zarówno z klientami, utrzymaniem, jak i dostawcami IT staje się kluczowym elementem przyszłego rozwoju firm.

Nie oznacza to, że takie rozwiązania jak systemy CRM, ERP czy bazy danych znikną. Nadal pozostaną podstawą funkcjonowania wielu procesów

wewnętrznych banków. Jednak nie one będą kluczowe dla transformacji cyfrowej.

Do tworzenia cyfrowych produktów niezbędne jest innego rodzaju oprogramowanie otwarte na zmiany, umożliwiające wspólne tworzenie nowatorskich modeli biznesowych oraz zapewniające elastyczność niezbędnej do odwzorowywania nowych procesów cyfrowych i tworzenia nowatorskich koncepcji.

Wymogiem obecnych czasów jest więc z jednej strony stabilność, bezpieczeństwo i ciągłość działania systemów w krytycznych obszarach dla organizacji, natomiast z drugiej zachowanie elastyczności, szybkich i wyskalowanych rozwiązań oraz łatwej adaptacji do zmiennego otoczenia i podejmowania ryzyka.

W tych warunkach, jakie przynosi ze sobą digitalizacja wewnętrzne IT musi sprostać wyzwaniom technologicznym i organizacyjnym, które zapewnią unifikację i przepływ procesów na wskroś całej organizacji.

Wydaje się, że podział dla tego celu zasobów informatycznych na dwie grupy, z których jedna jest bardziej stabilna, a druga elastyczna, jest jak najbardziej celowy. Tylko w ten sposób można pomyślnie przeprowadzić transformację na poziomie poszczególnych struktur i w warstwie technologicznej.

Dlatego m.in. dla organizacji samego IT, jak i jego funkcjonowania w kolejnych latach istotne będą koncepcje IT dwóch prędkości czy DevOps.

Zgodnie z koncepcją „bimodalnego IT", pierwsza grupa koncentruje się właśnie na tradycyjnych operacjach IT, rozwijając bieżące aplikacje korporacyjne zgodnie z klasycznym modelem IT, kładąc nacisk na bezpieczeństwo, skalowalność i efektywność. Natomiast druga zajmuje się aplikacjami i usługami nowej generacji, gdzie istotne jest szybkość dostarczania i elastyczność.

I tu z kolei ma pomóc DevOps. Ta metodyka tworzenia oprogramowania zakłada ścisłą współpracę pomiędzy obszarami odpowiedzialnymi za projektowanie, przekazanie i eksploatację usług. W założeniu ma pomóc organizacji szybko wytwarzać oprogramowanie, produkty i usługi, niejako w efekcie współzależności rozwoju i operacji.

Szczególnie istotna wydaje się ta metoda w przypadku organizacji, które wytwarzają bądź wdrażają wiele zmian w środowiskach produkcyjnych i chciałyby to robić w jak najkrótszym czasie i z zachowaniem wysokiej jakości. Pozwala ona zbudować odpowiednie środowisko zarządzania wdrożeniem nowej usługi lub zmian w usłudze. Dzięki niemu możliwe jest

minimalizowanie przestojów, problemów w czasie wdrażania oraz roll-back aplikacji. Zwiększa to zdolność do reprodukcji i naprawy błędów oraz minimalizuje średni czas przywrócenia (MTTR).

W rezultacie przekłada się to na zmniejszenie kosztów i czasu dostarczenia produktu, krótszy czas i koszt testowania przy jednoczesnym zwiększeniu jego zasięgu, jak i możliwości wykorzystania środowiska.

Oczywiście bimodalne IT czy DevOps nie będą jedną z możliwych opcji na przyszłość, lecz stanowić będą jeden z niezbędnych warunków dla efektywnego funkcjonowania cyfrowej organizacji.

Zastosowanie tych metodyk wymaga jednak właściwego przeniesienia mechanizmów ich dziania na specyfikę organizacyjną danego przedsiębiorstwa. Poza niewątpliwymi korzyściami niosą one również różnego rodzaju zagrożenia dla działania IT.

Źródłem niepowodzenia dla transformacji IT może być bezrefleksyjna próba przeniesienia mentalności klasycznego IT na świat nowej generacji usług i aplikacji. W tradycyjnym modelu zarządzania praca jest wykonywana dlatego, że ktoś o nią poprosił i napisał do tego procedurę. W nowym podejściu, informatyce drugiej prędkości, każda osoba zaangażowana w proces jest decyzyjna, pracownicy identyfikują się z własną firmą i jej produktami, nie czują się jedynie trybikiem w wielkiej anonimowej machinie, na której działanie nie mają żadnego wpływu. To wymaga zmiany kultury w całym przedsiębiorstwie.

Po wtóre, źródłem niepowodzeń mogą być także nieprzystosowani do nowych warunków tradycyjni dostawcy rozwiązań IT. Ten czynnik jest tym istotniejszy, im w większym stopniu dana organizacja jest od nich zależna oraz budżet IT jest wydawany poza kontrolą działu IT.

Cyfrowy biznes i bimodalna informatyka znacząco zmieniają także podejście do zarządzania ryzykiem. Cyfrowe ryzyko nie jest czymś, co można całkowicie wyeliminować. Akceptacja określonego ryzyka powinna być więc świadomą decyzją kierownictwa. Jest to kolejne wyzwanie dla cyfrowego przywódcy w organizacji.

Będzie on musiał także pogodzić napięcia występujące pomiędzy klasyczną i szybką częścią IT, w szczególności, aby rozwiązania innowacyjne (wdrażane na szybko) nie zepsuły klasycznego IT. Z drugiej strony powinien on także zadbać, aby dobre pomysły, sprawdzone w świecie innowacji, były stosowane w klasycznym świecie IT.

Bimodalna informatyka nie jest rywalizacją pomiędzy tymi dwoma modelami, to struktura pracująca zarówno klasycznie, jak i szybko w warunkach pewnej rynkowej nieprzewidywalności, która w cyfrowym świecie nabiera większego znaczenia. Oznacza to solidne wewnętrzne IT, zdolne do zwinnego działania, które znakomicie adresuje ten problem.

Warto również zwrócić uwagę, iż nowe trendy w sektorze bankowym i rosnąca konkurencja sprawiają, że dzisiejszym bankom jest coraz trudniej zachować pozycję lidera branży także pod względem innowacji. Umiejętne wykorzystanie możliwości płynących ze zmian rynku może w znaczący sposób przyspieszyć zarówno wyszukiwanie pomysłów, jak i wdrażanie projektów. Budowanie kompetencji, jak i rozwój w zakresie obszaru R&D w IT pomoże bankom efektywnie korzystać z potencjału technologii, dla których dopiero szuka się zastosowania, np. open API, biometrii, sztucznej inteligencji czy *blockchain*.

Współpraca z innymi wpisana w cyfrową organizację

Najbliższe lata mogą w znacznym stopniu zmienić sposób myślenia o biznesie bankowym. Wygrają ci gracze, którzy już dziś wpisują digitalizację i współpracę z innymi podmiotami na rynku w działalność firmy.

Sposobem na sukces będzie stworzenie łańcucha dostaw maksymalizującego wartość dla klientów i wykorzystywanie cyfrowych platform. Do tego potrzebne będą zewnętrzne firmy, specjalizujące się w różnych dziedzinach oraz zaawansowane technologie informatyczne.

Prowadzone przez liderów działających w swoich branżach elektroniczne platformy wymiany produktów i usług będą głównym motorem innowacji na rynku, integrując cyfrowe dane zarówno swoje, jak i partnerów zewnętrznych.

Konieczna będzie też umiejętność wykorzystywania gromadzonych danych nie tylko do podejmowania decyzji, ale przede wszystkim sprzedaży pożądanych produktów dostosowanych do konkretnych odbiorców.

Michał Furmankiewicz
Architekt Rozwiązań Chmurowych w firmie Microsoft

Ostatnio dziewięć lat spędził pracując jako programista, następnie konsultant w obszarze produktywności, by później pełnić rolę architekta, współpracując m.in. z takim klientami jak ING Bank, Millennium Bank, PKO BP, mBank czy Credit Agricole. W swojej karierze był również odpowiedzialny za jedne z największych projektów chmury prywatnej w Europie Środkowo-Wschodniej.
Pasjonuje się nowymi technologiami i ich wykorzystaniem w biznesie. Chmurę postrzega jako narzędzie, które może pomóc w transformacji firmy. W czasie wolnym chętnie dzieli się wiedzą z innymi, występując na konferencjach, spotkaniach grup czy poprzez wpisy na blogu. Ostatnio szuka rozwiązania problemu umierających pszczół korzystając z koncepcji rozwiązań IoT oraz uczenia maszynowego. Prywatnie pasjonuje się inwestycjami na rynkach finansowych, biega lub gra w koszykówkę a wieczorami chętnie czyta o zawiłościach ludzkiej natury.

Michał Furmankiewicz, Microsoft

Co może zyskać firma migrując swoje usługi do chmury publicznej?

Chmura obliczeniowa, mimo że na rynku istnieje od prawie 10 lat, dopiero w ostatnich dwóch staje się w Polsce tematem rozmów i debat jako nowy model dostarczania usług IT. Poza samym modelem to właśnie chmurę wymienia się jako jedno z tych narzędzi, które będzie najważniejszym elementem transformacji cyfrowej, a które dziś jest celem większości nawet najbardziej tradycyjnych gałęzi gospodarki. Chmurze równie często towarzyszą takie pojęcia jak Big Data, IoT, uczenie maszynowe czy usługi kognitywne, które, mimo że istnieją i działają niezależnie, dopiero w chmurze rozwijają pełnię możliwości. Żeby zrozumieć i wyobrazić sobie ten potencjał należy jednak najpierw wyjaśnić, jakie usługi chmura może zaoferować oraz na czym polegają różnice w ich dostarczaniu i konsumowaniu.

„Prawdziwa" definicja chmura obliczeniowej

Formalnych czy akademickich definicji chmury jest wiele. W 2011 r. swoją definicję opublikował amerykański *National Institute of Standards and Technology*[1], dwa lata później zrobił to uniwersytet techniczny MIT[2], nad terminem pochylił się również polski GUS[3]. Wszystkie definicje można natomiast sprowadzić do stwierdzenia, że jest to model oferowania usług IT w skali globalnej przez centra danych dostawców chmury, w modelu *pay-per-use* czyli opłat tylko za

1 *The NIST Definition of Cloud Computing*, http://bit.ly/gab-cloud-nist

2 *What is Cloud Computing?* http://bit.ly/gab-cloud-mit

3 Główny Urząd Statystyczny, Słownik pojęć, http://bit.ly/gab-cloud-gus

usługi powołane i tylko za czas, kiedy były aktywne. Czasami definicja nawiązuje również do różnych modeli oferowania usług i tu często pojawia się podział na usługi typu IaaS (*Infrastructure as a Service*), PaaS (*Platform as a Service*) czy SaaS (*Software as a Service*), aczkolwiek podział ten jest nieostry i pojawiają się kolejne modele takie, jak choćby *Function as a Service*[4].

Główne cechy chmur obliczeniowych

Niezależnie od przyjętej definicji, usługa chmury, oferowana przez trzech największych dostawców, ma pewne cechy szczególne:

1) **Oferowana jest ogromna skala usług, która z perspektywy pojedynczego przedsiębiorstwa, korzystającego z chmury, może być traktowana jako nieograniczona i globalnie dostępna.**

To bardzo ważny element, szczególnie dla dużych firm o zasięgu globalnym, które swoje usługi chcą dostarczać najbliżej klienta lub przenosić akurat tam, gdzie on się znajduje. To również możliwość wykorzystania potencjału tej skali w biznesie o silnym charakterze okresowym. W chmurze można bowiem wykupić bardzo dużo mocy na pewien określony kwant czasu i zrealizować proces cykliczny, np. raz w tygodniu. Takie przetwarzania to nie tylko domena naukowców czy firm badawczych, ale np. drużyn sportowych5 w Formule 1, firm samochodowych, np. Volvo6 czy Scania7, wydarzeń medialnych, które towarzyszą Olimpiadzie8 czy choćby przemysłu filmowego9. Żeby pokazać rozmiar tej skali, dość powiedzieć, że trzech największych dostawców usług chmurowych w 2017 r. będzie posiadało łącznie ponad 60 regionów przetwarzania danych, rozsianych po całym świecie. Sam tylko Microsoft oferuje 38 regionów, w których znajduje się ponad 100 centrów danych. Niesamowita jest też ilość serwerów, które wypełniają te centra danych. Choć dostawca nie publikuje takich danych oficjalnie, to przeszło pięć

4 *Serverless Architecture*, https://martinfowler.com/articles/serverless.html

5 *ANSYS CFD and Microsoft Azure perform best HPC scalability in the cloud*, https://azure.microsoft.com/en-us/blog/ansys-cfd-and-microsoft-azure-perform-the-best-hpc-scalability-in-the-cloud/

6 *Automakers choose Microsoft as connected car partner*, http://bit.ly/gab-azure-auto

7 *Scania Leads a New Era of Trucking Services with Data and the Cloud*, http://bit.ly/gab-azure-scania

8 *Olimpiada w Soczi*, http://bit.ly/gab-olimpics

9 *Kiedy warto używać chmur*, http://bit.ly/gab-azure-pixar

lat temu Microsoft przyznał, że wykorzystuje ponad milion fizycznych serwerów. Poza wielkością i skalą inwestycji imponująca jest też szybkość rozwoju infrastruktury. Dwaj najwięksi dostawcy chwalą się, że dziś dodają dziennie więcej serwerów, niż jeszcze kilka lat temu przez cały rok. Ta skala jest już na tyle duża, że największe firmy badawcze na świecie twierdzą, że nie ma już dziś kolejnej firmy, która jest w stanie dogonić pierwszą trójkę ani w zakresie oferowanej skali usług ani w zakresie oferty usług.

Rys. 1. Zdjęcie z lotu ptaka jednego z regionów Microsoft Azure gdzieś w USA. Prezentowana wielkość regionu w odniesieniu do amerykańskiej ciężarówki. Zdjęcie zrobione w 2015 r. Jedno z dwóch oficjalnie zaprezentowanych przez firmę.

2) **Oferowany jest szeroki portfel usług dostarczanych w różnych modelach.**

Krytycy chmury często mówią o niej jako o ofercie utrzymywania maszyn wirtualnych w innych Centrach Danych. Co ciekawe, żaden z dużych dostawców chmury historycznie nie rozpoczął od oferowania maszyn wirtualnych10, ale raczej od usług, które miały pomóc programistom szybciej i łatwiej wykonywać ich pracę, oferując gotowe usługi w postaci dostępnego API. Nawet dziś oferta maszyn wirtualnych stanowi tylko niewielką część całej oferty.

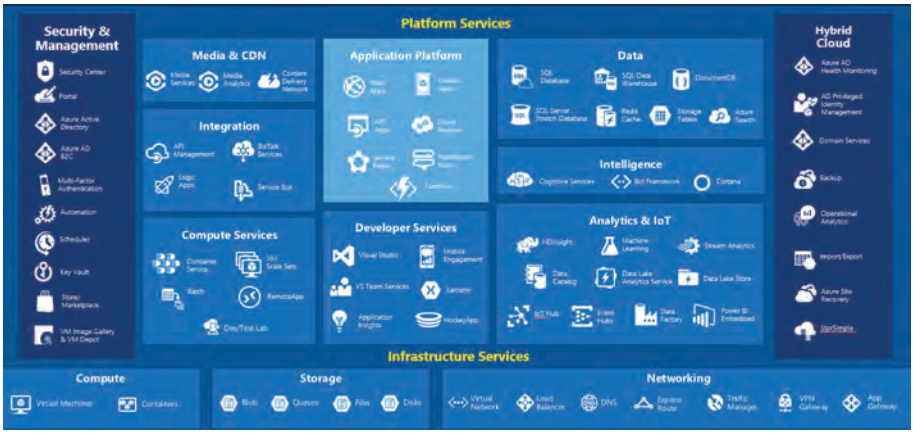
10 *Microsoft ogłasza usługę Windows Azure w trakcie konferencji w Los Angeles w 2008 r.*, https://www.cnet.com/news/microsoft-launches-windows-azure/

Gdyby tylko skupić się na grupach usług a nie pojedynczych pozycjach, których mamy już ponad 10011, trzeba powiedzieć o takich grupach jak:

- usługi infrastrukturalne (*Infrastructure Services*), oferujące m.in. usługi obliczeniowe, usługi przechowywania danych czy rozmaite usługi sieciowe,
- usługi dla programistów (*Application Platform*), gdzie można znaleźć serwery aplikacyjne, systemy wersjonowania i utrzymania kodu, systemy zarządzania API,
- usługi do analizy danych i prowadzenia eksperymentów (*Analytics & IoT*) z predefiniowanymi algorytmami predykcyjnymi,
- usługi do składowania relacyjnych i nierelacyjnych danych (*Data*), budowania hurtowni,
- usługi dla budowania sztucznej inteligencji (*Intelligence*).

Oczywiście platforma chmury innej platformie nie równa, jednak najwięksi dostawcy oferują bardzo zbliżone grupy usług.

Rys. 2. Grupy usług dostępne w Microsoft Azure.



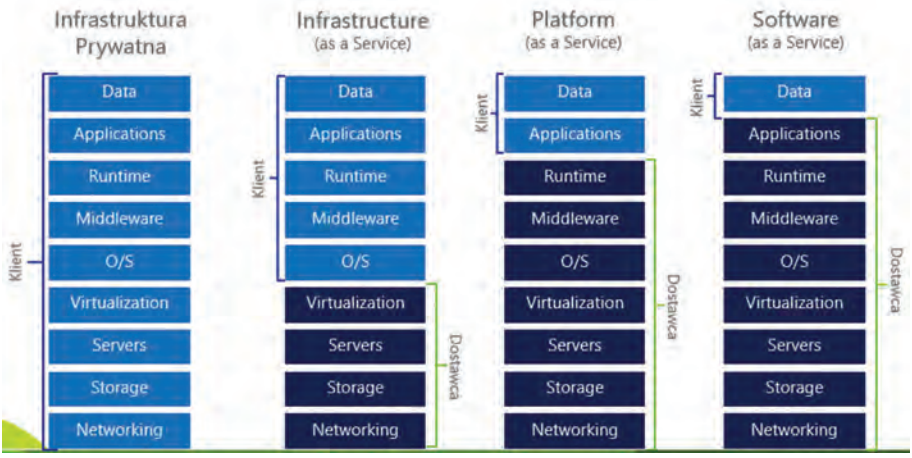
Co ciekawe, ilość tych usług bardzo dynamicznie rośnie a one same stają się coraz bardziej dojrzałe, oferując nowe możliwości. Dość powiedzieć, że w uprzednim roku Microsoft zapowiedział wdrożenie ponad 1 500 aktualizacji do swojej oferty usługowej. Tak jak skala infrastruktury jest czynnikiem wyróżniającym dostawców chmury, tak też zakres oferowanych usług i ich

11 *Katalog usług Microsoft Azure*, https://azure.microsoft.com/en-us/services/

możliwości jest niespotykany nigdzie indziej. Nie wspominając już o tempie wydań i aktualizacji, które zdarzają się prawie codziennie[12].

3) **Usługi oferowane są w różnych modelach, co zapewnia różny poziom swobody konfiguracji i wiąże się z różnym nakładem pracy utrzymaniowej.**

Rys. 3. Modele dostarczania usług



Klienci bowiem mogą wybrać pomiędzy usługami w modelu, który zapewnia największe możliwości konfiguracji i największą elastyczność, ale okupione jest to największą ilością pracy administracyjnej. Mogą też wybrać usługi bezobsługowe z perspektywy lokalnego administratora, w których jednak możliwości konfiguracji są mniejsze i nie są to usługi tak elastyczne. Wspomniany już wcześniej model IaaS, pozwala na wykorzystanie prostych usług takich jak maszyny wirtualne, sieci czy konta składowania danych. W tym modelu jest największy poziom swobody, gdyż operuje się na poziomie systemu operacyjnego, który możemy dowolnie skonfigurować i uruchomić na nim prawie dowolne usługi. Swobodzie towarzyszy jednak odpowiedzialność za typowe procesy operacyjne, takie jak kopie zapasowe, monitoring środowiska na poziomie konfiguracji czy wydajności, aktualizacje, migracje do wersji wyższych ect.

12 *Aktualizacje wydawane w ramach Microsoft Azure*, https://azure.microsoft.com/en-us/updates/

To, co zyskujemy w modelu IaaS, poza skalą i możliwością szybkiego powoływania usług, to fakt, że przenieśliśmy na dostawcę odpowiedzialność za utrzymanie SLA dla dostarczania usługi i nie musimy zajmować się takimi elementami, jak choćby budynek serwerowni i jego zabezpieczenia, redundantne zasilanie czy zasilanie na wypadek braku prądu, wymiana sprzętu i jego serwis, łączność dla dostawców sieci czy tak prozaicznym aspektem jak utylizacja zużytego sprzętu[13]. Dla firm o zasięgu globalnym już sam fakt przeniesienia tej odpowiedzialności na jednego dostawcę w wymiarze globalnym, z jednym punktem wsparcia, z jedną procedurą wykonywania operacji oraz przewidywalnym modelem płatności jest znaczną korzyścią. Dodając do tego fakt, że proces planowania pojemności i zarządzania pojemnością środowisk fizycznych został w tym procesie przeniesiony na stronę trzecią, możemy znacznie skrócić czas w projekcie, poświęcony tym zadaniom.

Model PaaS (Platform as a Service), który jest tak chętnie wykorzystywany przez programistów, oferuje nieco mniej swobody konfiguracyjnej, gdyż mamy jednie wpływ na zachowanie się usługi, tracąc dostęp do systemu operacyjnego, wirtualizacji czy konfiguracji samego serwera aplikacyjnego. Za to zyskujemy gotowe usługi wyższego poziomu, takie jak serwery aplikacyjne, bazy danych, czy usługi strumieniowania mediów do prowadzenia eksperymentów czy wreszcie do porównywania twarzy. Dla tych usług to dostawca dba o procesy operacyjne związane z migracją do wyższych wersji, bezpieczeństwem, skalą, aktualizacjami etc. Ich dużą zaletą jest też fakt, że dostępne są prawie od razu, zaraz po ich stworzeniu, dużo szybciej mogą zmienić swoją skalę i ilość obsługiwanych żądań oraz nie wymagają monitoringu na wielu warstwach. Model wdrożenia zmian czy samego rozwiązania jest często prostszy i zintegrowany z narzędziami do wdrażania kodu, takimi jak Git, GitHub czy Visual Studio Team System, co znakomicie ułatwia pracę. To właśnie programiści, dla których chmura jest bardzo wygodnym środowiskiem pracy zyskują usługi, które pozwalają im skupić się na najważniejszym, czyli tworzeniu rozwiązania.

Wreszcie model SaaS. Często wymieniany jest jako najwyższy model usługowy, gdyż dostawca oferuje kompletne, biznesowe rozwiązanie, gdzie dba o wszystkie jego aspekty platformy, a rola zamawiającego ogranicza się do konfiguracji usługi, załadowania danych i ew. integracji. Salesforce, Office365 czy Microsoft CRM oferowane są właśnie w takim modelu, ale zakres tych

13 *Historia migracji do chmury w wymiarze globalnym firmy Maersk*, https://channel9.msdn.com/Events/Ignite/2016/BRK2291

usług powiększa się stale. Dostawcy chmur oferują również sklepy z gotowymi aplikacjami firm trzecich, które można uruchomić na infrastrukturze chmury niemalże jednym kliknięciem, zyskując model zbliżony do SaaS. Liczba tych gotowych usług stale rośnie i pochodzą one zarówno ze świata komercyjnego, jak i OpenSource.

Pojawiają się również takie modele jak XaaS czy FaaS, określane często mianem architektury bez serwerów (*Serverless Architecture*). W uproszczeniu, mamy możliwość po prostu uruchomienia kodu w praktycznie dowolnym języku, nie dbając o środowisko systemu operacyjnego, środowisko uruchomieniowe, zarządzanie pamięcią, procesorem czy sposobem wykonania. Łatwość uruchamiania usług jest tu najwyższa z możliwych, oddając właściwie wszystkie prace administracyjne w ręce dostawcy. Możliwości takiego modelu są jeszcze dziś ograniczone, jednak stale się rozwijają i już dziś są podstawą Bot'ów[14] czy projektów przetwarzających duże ilości danych z czujników w rozwiązaniach klasy IoT.

4) **Koszty usług rozliczane są „za użycie" w rozumieniu czasu działania usługi i poziomu wydajności, jaką usługa oferuje czy ilość przetwarzanych danych.**

Jedna z najmniej docenianych cech, która oferuje niesamowitą wartość biznesową, jeśli używana jest umiejętnie. Po pierwsze, płacimy za usługę wtedy, kiedy z niej korzystamy, a więc wtedy, kiedy maszyna wirtualna działa, kiedy na koncie składowania danych znajdują się dane, kiedy usługa CDN transferuje dane, czy też kiedy realizujemy eksperyment w usłudze uczenia maszynowego. Z reguły rozliczamy się, chodź są wyjątki, za aktywne minuty usługi, GB transferowanych danych, ilość włączonych funkcji, monitorowanych usług czy wykonanych porównań obrazów. I teraz, jeśli zdamy sobie sprawę, że nie wszystkie usługi muszą działać w modelu 24x7, ale mogłyby np. w modelu 12x5 (jak np. środowiska developerskie czy testowe), to wtedy cena takich środowisk będzie o ponad 55% niższa. Jeśli do tego dodamy możliwość płynnej zmiany poziomu wydajności, to wtedy okazuje się, że nie musimy przez wszystkie dni tygodnia być gotowi na maksymalne obciążenie, które przecież nie tak często ma miejsce. Dostosowanie aplikacji posiadanych w portfelu firmy od wielu lat do takiego modelu działania nie zawsze jest

14 Definicja słowa Bot – http://bit.ly/gab-bot

proste, ale korzyści płynące z tego tytułu dla nowo powstających aplikacji mogą być niezwykle wymierne. Dla środowisk archiwalnych, rzadko używanych, stwarza to szansę na realne obniżenie kosztów rocznego utrzymania, tak jak np. w rozważanym projekcie Tezeusz15. Co więcej, do pewnego poziomu użycia wiele usług po prostu nie kosztuje nic16. Dodając do tego możliwość zautomatyzowania operacji włączania, wyłączania czy skalowania w górę i wszerz, otrzymujemy bardzo ciekawy model zarządzania kosztami, który nie jest osiągalny we własnym centrum danych. Raz wydany budżet na serwerownie czy osprzęt nie może być przecież „odzyskany", jeśli usługi nie pracują albo pracują z mniejszym obciążeniem. Chmury oferują tę elastyczność i projektując usługę działającą w chmurze należy stale mieć to na uwadze. Nowoczesne technologie tworzenia aplikacji, które powstały w chmurach, takie jak kontenery, funkcje czy środowiska wspierające mikrousługi, wspierają taki model działania.

Model rozliczeń to jedno, natomiast istotny jest jeszcze model płatności. Na rynku są różne modele nabywania chmury, zaczynając od najprostszych, takich jak użycie karty kredytowej i zakup przez stronę po dedykowane umowy, podpisywane na kilka lat, które gwarantują konkurencyjne ceny, dodatkowe usługi wsparcia, gwarancję utrzymania ceny przez okres trwania umowy czy specjalne gwarancje i możliwości dla wybranych sektorów.

Najwięksi gracze na świecie

Tych cech chmury zapewne można wymieniać więcej, natomiast te wymienione dotyczą trzech największych dostawców chmur, jakimi są Amazon, Microsoft i Google. Tak też widzą to największe firmy analityczne i badawcze, takie jak Gartner, Forrester czy IDC.

Na koniec należy dodać jeszcze jedną cechę, która dla mnie osobiście jest kluczowa. Otóż dostawcy chmur potrafią zaoferować w bardzo atrakcyjnym modelu kosztowym usługi, które niezwykle trudno zbudować we własnym centrum danych lub też ich dostosowanie może być kosztowne i długotrwałe. Mam na myśli takie usługi, jak wykrywanie i rozpoznawanie mowy, identyfikacja obrazów czy twarzy, przeszukiwanie ogromnych zbiorów danych, identyfikacja

15 *Projekt TEZEUSZ: przeniesienie systemów archiwalnych banku do chmury publicznej*, http://bit.ly/gab-zbp-tezeusz

16 *See what you can do with Azure for free*, https://azure.microsoft.com/en-us/free/pricing-offers/

sieci botnet czy domowi asystenci, tacy jak Cortana lub Echo. Często wymagana jest duża skala zasobów czy choćby zbiorów treningowych, by taki algorytm przygotować. Nie mniej interesujące są takie usługi, jak możliwość zbierania danych z czujników (IoT) czy dostępność gotowych algorytmów predykcyjnych, które są wstępnie wytrenowane, ale pozwalają na dalsze dostosowanie. Firma Ford nie zdecydowałaby się na budowę rozwiązania monitorującego wszystkie sprzedane przez siebie pojazdy w USA, gdyby nie miała dostępu do rozwiązania, które umożliwia zbieranie ponad 1 mln zdarzeń pomiarowych na sekundę[17]. W szybko zmieniającym i rozwijającym się świecie dostępność szerokiego wachlarza stale rozwijanych usług w takim modelu kosztowym może stanowić element strategii budowania przewagi konkurencyjnej nad innymi. Budowanie tej przewagi oznacza często inwestycję i nie sprowadza się do ograniczania kosztów utrzymania aktualnej infrastruktury.

O czym dziś marzy każdy zarządzający firmą i co to ma wspólnego z chmurą?

W dobie usług cyfrowych prawie każda firma usługowa w swojej strategii rozwoju obok czynników biznesowych wymienia trendy technologiczne, które staną się narzędziem i środkiem do realizacji strategii, ale też osiągania celów biznesowych. Jedno nie istnieje bez drugiego. W swojej książce „Bank 3.0" Brett King świetnie opisał, co technologia i cyfryzacja zmieniły w branży bankowej i jak to wpłynęło na czas realizacji projektów, wybór technologii czy choćby pracę typowego *call center.* W tym kontekście wypowiadał się również CIO roku 2014, Mirosław Forystek, mówiąc o banku, jak o firmie technologicznej[18].

Podsumowując dwie przytoczone publikacje oraz własne doświadczenia, można powiedzieć, że dziś zarządzający firmami oraz kierujący działami IT zwracają uwagę na takie procesy jak:

- Digitalizacja biznesu zarówno z perspektywy klienta, jak i pracownika, która dąży do optymalizacji czasu i kosztów realizacji.
- Wprowadzenie zupełnie nowej, wcześniej nieznanej usługi na rynek, wprowadzenie zupełnie nowego modelu analizy danych, który dostarcza wcześniej nieznanych informacji bądź predykcji[19].

17 *Ford develops new service delivery network for its vehicles powered by Microsoft Azure*, http://bit.ly/gab-iot-ford

18 Bank to firma technologiczna, http://www.klubcio.pl/artykuly/401029/Bank.to.firma.technologiczna.html

19 Grupa OLX rośnie na danych, http://news.microsoft.com/pl-pl/2017/01/31/grupa-olx-rosnie-na-danych/

- Skupienie się na efekcie biznesowym a nie technologicznej czy architektonicznej doskonałości.
- Skrócenie czasu od zatwierdzenia pomysłu do przekazania nowego produktu do klienta.
- Możliwość stałego badania zadowolenia klientów z oferowanych usług oraz usprawniania rozwiązań i procesów.
- Przewidywalne, niskie koszty uruchomienia projektu i krótki czas dostarczania odpowiedniej infrastruktury, która może reagować na zmieniające się wykorzystanie usług.
- Dostępność i wykorzystanie gotowych usług i rozwiązań w celu skrócenia czasu zbudowania rozwiązania.
- Dodanie elementów „sztucznej inteligencji", by transformować rozwiązania w kierunku personalnych doradców klienta, prowadzących go za rękę.

Na chwilę zostawmy więc rozważania o chmurze „na boku" a skupmy się na tych celach. To, co dziś motywuje przedsiębiorstwa przede wszystkim, to pragnienie dalszego rozwoju swoich usług i zmiana modeli biznesowych, którymi się posługują lub dodanie nowych[20]. Trend transformacji cyfrowej, w świecie *mainstreamowych* mediów pojawia się dopiero od niedawna. Niektórzy obserwatorzy twierdzą, że po rewolucji przemysłowej ta rewolucja może odcisnąć największe[21] piętno w wymiarze społecznym, jak i gospodarczym. Nieraz w kontekście rewolucji cyfrowej mówi się o potrzebie rozwiązania problemu bezrobocia, który powstanie masowo po tym, jak większość naszej pracy zastąpią maszyny czy roboty, czy wprowadzenia bezwarunkowego dochodu podstawowego. Zanim jednak zaobserwujemy zmiany społeczne, na pewno już teraz widzimy, jak zmienia się rola typowego działu IT w świecie biznesu i jak zmienia się model działania na linii biznes-IT. Już teraz każdy zarządzający IT nastawiony jest na szybkie i zwinne dostarczanie nowych usług do biznesu i klienta końcowego. Poza szybkością dostarczania nowych rozwiązań biznesowych rośnie również ilość dostarczanych rozwiązań, gdyż w wysoko konkurencyjnym świecie tylko część tych usług przetrwa i pozostanie na rynku. Biorąc statystyki ze świata startupów – tylko 1 na 10 odniesie sukces komercyjny a wśród tych tylko 1 na 1000 będzie w krótkim

20 *The Guardian, What is digital transformation*, https://www.theguardian.com/media-network/media-network-blog/2013/nov/21/digital-transformation

21 Rewolucja przemysłowa, https://pl.wikipedia.org/wiki/Rewolucja_przemys%C5%82owa

czasie dużą firmą. Stąd też tak istotne jest by nowe rozwiązania powstawały przy niskim koszcie wejścia w projekt i by, w razie niepowodzenia, można było je wyłączyć bez ponoszenia dalszych kosztów. Dla firm o zasięgu światowym równie ważne stało się to, by w jednym momencie zaoferować usługi klientowi w każdej części globu, blisko klienta. Digitalizacja biznesu oznacza również wykorzystanie modeli biznesowych i technologicznych, które dziś wprowadza np. Uber, Facebook czy AirBnB. Jeśli się temu bliżej przyjrzeć, widać niezwykłą synergię pomiędzy przedstawionymi motywacjami a możliwościami usług chmurowych. Czy w takim razie należy wszystkie aplikacje migrować do chmury i rozpocząć ten proces już?

Co jest istotne w procesie migracji do chmury i dlaczego migracja „wszystkiego" i „na już" nie ma sensu

Nawet jeśli wydaje się to oczywiste, to najważniejszym elementem, zanim zdecydujemy się wykorzystać chmurę lub migrować do niej rozwiązania, jest oczywiście cel biznesowy. Jeśli rozważamy modyfikację rozwiązania lub budowę nowego i zalety modelu chmurowego oraz motywacje, które podnosiłem wcześniej są dla nas atrakcyjne, to cel został postawiony. Jeśli jednak migrujemy rozwiązania to powody, poza wymienionymi, mogą być różne, w tym korzyść finansowa pod tytułem „będzie taniej". Te motywacje i faktyczne efekty finansowe są bardzo zróżnicowane, a wielkość firmy, ilość środowisk i rozproszenie geograficzne ma niebagatelne znaczenie. Przy badaniu efektu kosztowego przestrzegam przed bardzo prostymi uproszczeniami, z którymi nieraz się spotkałem. Wszystkie je można sprowadzić do stwierdzenia: koszt maszyny wirtualnej w naszym centrum danych jest niższy niż w chmurze. Po pierwsze, bardzo rzadko firmy potrafią precyzyjnie policzyć koszt maszyny wirtualnej o zadanych parametrach uwzględniając w tym koszty związane z serwerownią, dostarczeniem prądu, ochroną, gwarancją, licencjami, *backupem*, dostarczaniem sieci czy wreszcie utraconymi kwotami związanymi z niedotrzymaniem SLA. Jeśli nie mamy danych by wykonać porównanie zbliżonych ofert, trudno mówić o rzetelnym zestawieniu. Nie wspominając już o takich aspektach, jak koszty związane z migracją czy wydaniem nowych wersji, ale również z przestojami i oczekiwaniem na uruchomienie nowych usług ze względu na proces zakupowy, instalację, konfigurację itd. Moje doświadczenie

pokazuje również, że usługi utrzymywane wewnątrz organizacji są często przeskalowane a badanie utylizacji środowisk pokazuje niskie średnie użycie zasobów. Jak widać, porównywanie kosztów, choć często przytaczane, bardzo rzadko w istocie ma miejsce ze względu na trudności, które wymieniłem. Jeśli faktycznie zależy nam na rzetelnej dyskusji w tym aspekcie, proponuję posługiwać się miarami typu TCO (*Total Cost of Ownership*) dla całego, konkretnego rozwiązania. Lub też wykorzystać dostępne metody kalkulacji, oferowane przez firmy konsultingowe lub dostawców chmury, dzięki którym można zrobić analizę i wybrać aplikacje, które warto wynieść i te, które należy pozostawić we własnym centrum danych. Jeśli już cel migracji został określony i nie dotyczy tylko jednej aplikacji, ale dużego portfela rozwiązań firmy, wtedy warto nie popełnić błędów poprzedników, tylko przygotować się na metodyczne podejście, które w długim horyzoncie pozwoli na skorzystanie z wielu zalet chmur opisywanych wcześniej i przygotować swoją organizację do tej zmiany. Poniżej szereg aspektów, którym polecam się przyjrzeć w trakcie planowania procesu migracji.

Rys. 4. Co warto wziąć pod uwagę planując migrację do chmury

Migracja do chmury to nie tylko migracja danych czy maszyn, to także proces, który może być o wiele bardziej rozbudowany i złożony, adresujący wiele różnych aspektów. Stąd raczej nie zdarza się jednego dnia, tylko jest rozłożony w czasie, przynosząc firmie coraz więcej korzyści.

Zdecydowanie warto przeanalizować historię migracji np. firmy Walmart, która rozpoczęła się już w 2011 r. i nadal trwa[22].

Jak i dlaczego firmy polskie i światowe korzystają z chmury publicznej?

Jeśli przeanalizować koncepcję i wizję usług samej chmury publicznej i połączyć to z dziejącą się transformacją cyfrową oraz uwzględniając priorytety, którymi dziś kierują się zarządzający firmami, zobaczymy niezwykłą synergię. Jak wspomniałem wcześniej ani sama chmura nie doprowadzi do transformacji cyfrowej, ani sama migracja do chmury nie musi oznaczać bezpośrednio zwiększenia konkurencyjności firmy. Chmura to nie magiczny Święty Graal czy rozwiązanie wszystkich problemów firmy. Natomiast samo nastawienie zarządzających firmami do transformacji bez narzędzi do ich realizacji, które pozwalają wykonać to szybko, również nie jest efektywne. Pomiędzy tymi wszystkimi elementami musi być czynnik spajający, którym jest cel biznesowy wraz ze wskaźnikami, które pozwolą kontrolować jego osiągnięcie.

Transformacja cyfrowa za pomocą chmury

Jedną z najbardziej tradycyjnych branż, w której dokonuje się wielka zmiana w ostatnich latach jest bez wątpienia branża motoryzacyjna. Samojeżdżące i samoaktualizujące się samochody, o ile jeszcze jakiś czas temu mogły uchodzić za nowinki technologiczne, stają się powoli rzeczywistością. Producenci aut[23] w poszukiwaniu nowych strumieni przychodów sięgają po coraz ciekawsze modele ekonomiczne, oparte o takie modele konsumpcyjne, jak chociażby używanie opon w przeliczeniu na mile[24] czy wypożyczanie aut na godziny.

Jeden z największych producentów samochodów na świecie zdecydował się na wybór chmury, bo jego model biznesowy wymagał rozwiązań, których budowa byłaby absolutnie nieopłacalna. Zaoferował bowiem swoim klientom szeroką ofertę monitorowania pojazdu nie tylko pod kątem pozycji na mapie, ale również charakterystyki pracy kierowcy czy spalania, przewidywania

22 *Walmart*, https://www.microsoft.com/en-us/research/wp-content/uploads/2016/09/Microsoft-Azure-The-Ultimate-Flexible-EnterpriseLevel-Solution.pdf

23 http://www.techtimes.com/articles/179488/20160926/renault-and-nissan-team-up-with-microsoft-for-connected-cars-initiative-azure-cloud-to-power-advanced-navigation-system.htm

24 *Consumption Economics: The New Rules of Tech*, J.B. Wood, Todd Hewlin, Thomas Lah

nadchodzących awarii oraz optymalizacji trasy przejazdu w przyszłości. Internet Rzeczy, pozwalający zbierać niewyobrażalne dotychczas ilości danych, pozwolił poprzez ich analizę zaoferować usługi dodane, które opłacane w modelu subskrypcyjnym stały się nowym biznesem firmy. Co ciekawe, czasem bardziej marżowym niż biznes macierzysty, choć zapewne jeszcze nie większym.

Nasz lokalny, polski rynek również zaczął eksplorować możliwości chmury w bardzo różnych aspektach. Co ciekawe, pierwszą motywacją nie były koszty, choć oczywiście są ważnym elementem każdego przedsięwzięcia. Trudno powiedzieć, że duże polskie firmy rozpoczęły już proces migracji całych centrów danych, ale organizacje z praktycznie wszystkich branż, również tych najbardziej regulowanych, jak medyczna czy bankowa, umieszczają rozwiązania sprawdzając możliwości chmury, rozwijając kompetencje swoich zespołów, szukając nowych zastosowań i budując element swojej strategii transformacji.

Jeden z polskich banków, pracując nad zupełnie nowym wizerunkiem oraz nowym portalem online dla klienta, zdecydował się na wykorzystanie filmów spersonalizowanych, prezentowanych wybranym klientom. Filmy były przygotowywane co miesiąc, a trafiając do wybranej grupy klientów (ok. 30 tys.) prezentowały cztery różne scenariusze oferty. Dlaczego wybrano chmurę? Po pierwsze dlatego, że firma oferująca możliwość przygotowania takich filmów działała w środowisku chmury zarówno w Polsce, jak i poza nią. Po drugie, przygotowanie tysięcy filmów dla klienta końcowego i strumieniowanie ich na dowolne platformy nie wymagało ingerencji pracowników banku, będąc całkowicie po stronie dostawcy rozwiązania oraz dostawcy chmury. Wreszcie, ogromny ruch sieciowy, który został wygenerowany został całkowicie przerzucony na rozwiązanie chmurowe i bank nie musiał dla tej potrzeby czynić żadnej inwestycji. I ostatni element to czas – zespół miał ok. trzech dni na końcu każdego miesiąca by takie filmy na kolejną kampanię przygotować. Wreszcie, kiedy po sześciu miesiącach okres kampanii się skończył, rozwiązanie można było zatrzymać i nie ponosić kolejnych kosztów. Aż do rozpoczęcia kolejnej kampanii.

Inna instytucja finansowa, realizując projekt o skali ogólnopolskiej, natrafiła na dwa wyzwania. Czas potrzebny na zamówienie infrastruktury, instalację i konfigurację przekraczał realny czas na wdrożenie i uruchomienie projektu. Z drugiej strony, nieprzewidywalna skala projektu, dynamiczne zmiany terminów jego przekazania do obywateli oraz konieczność zabezpieczenia

rozwiązania przed potencjalnymi atakami i ogromnym ruchem. Oba te powody były wystarczające, by rozważyć chmurę i w niej umieścić rozwiązanie JPK czyli Jednolity Plik Kontrolny.

Nowoczesny bank średniej wielkości zdecydował się realizować projekt tak, jakby robił to startup. Ale startup w ramach banku. Dedykowany zespół do marketingu, sprzedaży, dedykowany zespół programistów. Co było dla nich najważniejsze? Wykorzystanie gotowych usług i architektury rozwiązań tak, by nie wymyślać przysłowiowego koła od początku, krótki czas dostarczenia infrastruktury pod projekt oraz minimalny zakres prac administracyjnych w jego ramach. Coraz bardziej kurczący się rynek specjalistów IT sprawia, że usługi o niskiej ilości pracy administracyjnej są silne pożądane. Biorąc to pod uwagę, z pełną premedytacją wybraliśmy usługi w modelu PaaS oraz FaaS. Dość powiedzieć, że na prawie dwadzieścia usług, jakie są używane, wykorzystujemy tylko dwie maszyny wirtualne dla potrzeb analizy ruchu sieciowego. Projekt właśnie ujrzał światło dzienne, a zespół buduje plan rozwoju na kolejne miesiące.

Tych przykładów jest więcej, choćby w branżach takich jak e-commerce, energetyka czy ubezpieczania, gdzie budowany jest zupełnie nowy zakres usług. A będą kolejne, jeszcze większe, jeszcze ciekawsze i publicznie opisywane oraz omawiane na konferencjach. Tak, by z tych doświadczeń korzystali inni. Kolejne, inspirujące doświadczenie startuje już za chwilę. Oto największy polski bank wybrał firmy z obszaru fintech[25], który bardzo często i chętnie korzysta z chmurowych modeli oferowania usług.

Kto pierwszy, ten lepszy, czyli o ściganiu się z czasem

W świecie cyfrowym wiele osób podnosi kwestię, że bankowość jako usługa przetrwa, natomiast banki, w swoim aktualnym kształcie, niekoniecznie. Bankowość to nieustanna praca by zaoferować klientowi dobre usługi, zainteresować go usługami dodanymi, pogłębić jego zaangażowanie, by chętniej do nas wracał, jednocześnie nie powiększając kosztu jego obsługi. Szczególnie tam, gdzie konsumenci są świadomi i korzystają z wielu usług, zaoferowanie klientowi wartości unikalnej jest niebanalne. Ta niebanalność bierze się również stąd, że jesteśmy stale podłączeni do sieci, która zalewa nas informacjami i ofertami. Ofertami, które są niechętnie przez nas analizowane i rozważane.

25 *LET'S FINTECH WITH PKO BANK POLSKI!* https://www.pkobp.pl/fintech/

Polska oferta bankowa na tle „starej" Europy czy USA jest naprawdę innowacyjna, rozbudowana i niesamowicie skupiona na mobilności.

W świecie transformacji cyfrowej nową, unikalną usługę realizujemy raz, nie da się jej łatwo powielić pomiędzy organizacjami. Jeśli więc priorytetem jest rozwój, zdobywanie klientów, oferowanie ciekawszych usług szybciej i lepiej niż inni, wtedy patrzenie tylko na pryzmat platformy chmurowej jako na metodę optymalizację kosztu jest błędne i, co pokazały przytoczone wcześniej przykłady, nieuzasadnione.

Andrzej Sieradz PhD
Digital Advisory Services – Microsoft Central & Eastern Europe

With 25 years of experience in the banking, finance and retail industries, Andrzej has managed and completed complex IT projects in Poland and abroad. He holds a PhD in Economics from the University of Gdańsk (2014), graduated from the Technical University in Warsaw, holds an MBA from the University of Illinois and has completed postgraduate studies in finance and banking at the Warsaw School of Economics.
In the years 2010 to 2015, he was Vice President of Bank BGŻ responsible for IT and operations. In the years from 2006 to 2010, he was a member of the Board of ING Life Insurance Company SA and ING Financial Services SA, where he was responsible for the IT, customer service and project management departments. From 2002 to 2006, he associated with ING Bank Śląski SA, first as Managing Director of IT and later as Managing Director of strategy and organization. From 1997 to 2002 he worked at Coca-Cola HBC in Poland and the headquarters in Vienna. Andrzej has many years of experience in business development and in transformation projects and has extensive experience of changing organizations within the framework of mergers and acquisitions which represents several years of experience of project management in his portfolio. He has managed implementations of key IT systems for banks and the insurance sector. Currently, he works at Microsoft Poland.

Joanna Molik
Digital Advisory Services – Microsoft Central & Eastern Europe

A digital architect with over 16 years of professional experience, Joanna has worked with Microsoft financial service clients on digital business transformation and specializes in the planning and delivery of complex transformation programs. Her programs concern customer experience, process digitization, digital workplaces and organizational change management, enabling value realization from strategic investment in technology solutions.
Prior to joining Microsoft in 2016, Joanna worked as a manager at Accenture Financial Services, delivering complex business and technology projects for top financial institutions, public administration and non-profit clients, both in Poland and globally.
She is a software engineering graduate from Poznan University of Technology.

Joanna Molik, Andrzej Sieradz

Digital banking – four dimensions of digital transformation

The outcome of the 2008 financial crisis brought three factors which drove the disruption in banking: customers expect products and services they understand, can access, and of which they can understand and compare the charges. The second major factor is the technological shift forward of people and the connectivity they can exercise. The worldwide population has become "mobile", not only for banking but for life. Customers need banking services, but they do not need "old banks".

The new reality following the 2008 financial crisis has moved financial markets toward greater inequality in three distinct ways. The first involves moving a big share of the total national wealth into the hands of the financial sector. The second involves concentrating on the importance of the financial sector to prevent the next crisis - that means regulatory measurements. The third way in which the financial sector increased inequality before 2008 is by convincing corporate executives and asset managers that company growth has to concentrate on almost immediate income paid to shareholders rather than a focus on the products and workforce they deliver. Today with the number of new post-crisis regulations, the entire sector is under pressure. The diagram below shows potential threats and opportunities linked to the digital transformation.

Figure 1. McKinsey analysis

Impact of digitalization – percentage of net profit for a retail bank

Source: McKinsey analysis

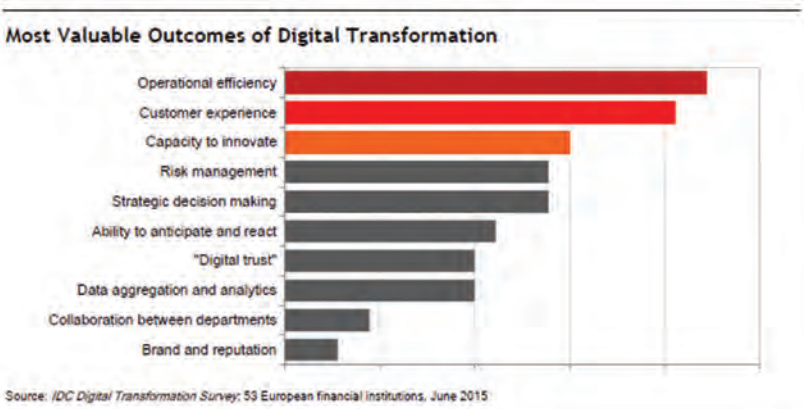
The digital transformation of banking should combine the benefits of two worlds: a new and rich customer experience on the outside, with new products and services and an effective operating model inside reacting closely to online services, both enabled by digitization and the underlying technologies, processes, and structures (see Figure 2).

On the inside, banks need immediate interactions and transactions performed seamlessly and quickly with a high degree of security. That should lead to a situation where customers are proactively informed about a rich spectrum of personalized products and services, including financial advice and new opportunities.

Figure 2. A.T. Kearney analysis

According to IDC's 2015 Digital Transformation Survey, the top expectation of leadership of the banks starts with operational efficiency (see Figure 3).

Figure 3. IDC Digital Transformation Survey 2015



The road to digital banking leads through the transformation of the current business model to enabling institutions to interact with consumers in new and exciting ways, empower professionals with new insights and tools, help businesses operate more efficiently and open new opportunities never thought possible. The strategy to enable digital transformation in the banking sector should address the following issues:

1. Customer experience.
2. Employee empowerment.
3. Operational excellence.
4. Transformation of products and services for wider ecosystems.

Digital transformation involves a continuous process of combining strategy with execution, beginning with the customer journey. Better understanding of customers empowers employees to support them more effectively, reduces the risk and cost of servicing them, simplifies and optimizes operations, and develops new products that customers want and need. The net result is a transformed business.

Management of adoption and change is a critical part of this process, because we need to continue to operate during the transformation. This often leads to the concept of a two-tier approach where we support our legacy environment as we transition to a new model.

Focus on customer experience

Digital transformation in that area should focus on rethinking customer engagement – bank customers are active in dozens of channels researching and talking about brands, products and services, which gives banks endless opportunities to join the conversations. With customer engagement, banks should look at more holistic ways to:

- Approach customer-centricity across the company.
- Reach out and personalize interactions with customers.
- Use data to understand what consumers want now.
- Partner marketing leaders with IT to select the most strategic tools and solutions.

Great customer experience and efficient operations are not mutually exclusive. Bots and intelligent assistants are natural solutions for the first wave of customer contact. Much like how interactive voice response (IVR) transformed inbound service calls, AI can intercept and handle common, straightforward issues through chat and messaging services so customers can quickly and independently resolve simple issues that would otherwise have required human intervention.

Conversation is now a service. Instead of looking through multiple apps or pages of websites, you could simply ask a question through a conversational interface you already use. Think of these services as bots. Bots are the new apps, and digital assistants are the new browsers. In this way, all interactions are infused with intelligence. A bot can be built once and connect across multiple communication services such as text messaging, email, LinkedIn, Facebook, Skype, Slack, kik, web chat, and Office 365.

Reach people where they are and engage them conversationally, contextually, and naturally. By gathering information through dialogue and understanding context via emotional cues, bots can easily escalate and route the most complex and sensitive conversations to humans for resolution. When bots and customer service reps work together to help customers answer their questions, they improve customer experience and loyalty, and because AI scales to meet demand virtually without limit, employees can spend more of their time on higher priority customer interactions, resulting in both cost savings and service quality benefits. What's more, according to the latest research, people actually prefer engaging with machines instead of people in certain scenarios.

Understand customers to personalize experience. Combining Big Data analytics and business intelligence can target each customer individually with the right products at the right time. Not only should banks and insurers be able to understand their clients, they should predict their behavior to create sales opportunities. Think of transforming customer experience as a start-up operation. Take a customer segment, remap the digitally transformed customer journey, build the new business around this and then transfer that success in stages to the rest of the enterprise. In the long term perspective, the traditional approach to customer segmentation will evolve to an almost individual personalized experience, resulting in having segments of one.

Provide a frictionless service. All customer touchpoints, business processes, and data sources must be integrated to provide a frictionless experience. Customers should never need to provide information more than once, and processes should be streamlined to minimize administration for customers and staff alike, making data integration and reuse a top priority. Other areas of focus

for banks and FinTechs alike is payments innovation. With the rising adoption of contactless cards and mobile wallets, seamless digital payments are the key to enabling access to banking services in a convenient and secure manner.

Build an omni-channel experience. Give customers the option of how to interact with the bank. Be present where your customers are - online, mobile, on the go, in social media and in retail (non-banking) locations. Data collected from all channels should be integrated in real time and therefore be ready to be presented through whichever channel the customer is using. Your products and customer experience should be optimized for the desired product/channel mix and the preferences of your customers, shifting the relationship from transactional to seamless customer experience across physical and digital touchpoints.

Workforce transformation

Digital workplaces use new technologies to drive employee engagement and business agility, but it's much more than just the consumerization of IT and much more is needed to ensure success. Major analysts share a common understanding of digital workplace imperatives and key capabilities (see Figure 4):

Figure 4. Microsoft analysis

Per Deloitte Digital University research on "Digital transformation in financial services", improving employee experience requires successful alignment of organization culture — "how work gets done"— with the business, operating, and customer models found in the enterprise. This implies the necessity of combining the customer and employee experience approach to prepare organizations for digital disruption. According to Deloitte, by 2020, 50% of the workforce will be "digital natives", connected 24/7 and working the way they want, any place, on any device.

For the banks, enabling a digital workforce means strengthening the focus on value-adding activities based on contacts with clients and requires reskilling the employees for the new era in customer service. Every activity of the bank employees, despite their organizational alignment, should be concentrated on clients.

Empower a mobile workforce. With the lower chance to make direct contact with clients, an enterprise-wide mobility strategy for employees is required— in the field, in the branch, or in the back-office operations. Make the most of the interaction with the customer and enable your employees with mobile devices and tools allowing for end-to-end processing of customer requests during one visit. These are two key measures of how digital your bank is and will support the reduction of paper and increase straight-through processing rates.

Encourage digital collaboration. Help employees digitize and share valuable knowledge within the organization, enable virtual meetings and agile teams with tools that bring employees together. Employees today are flooded with constantly growing volumes of information, impacting individual and team productivity, so you need enterprise-grade search tools, knowledge base hubs and portals. The need for agile teams and flexible workspace for collaboration – both physical and virtual – is constantly growing while the number of projects and initiatives executed concurrently is increasing as well, so we all need to establish new ways of working supporting new forms of collaboration.

Improve agility and time to market. Digital transformation should allow organizations to bring new offers at a lower marginal cost, not least by adopting cloud computing. This allows them to carry out development and launch products with little upfront investment — and at lightning speed.

Operational excellence

Access to large quantities of transaction data, underwriting and custom-scoring customers for credit-worthiness and understanding and managing operations through credit and economic cycles – these are unique assets, skills and capabilities that banks have built and leveraged over centuries. Today they have to maintain all those values and assets and concentrate (see Figure 5) on several areas in order to reach operational excellence. According to Microsoft, the most important are, among others: reducing cost, through enhanced automation achieving scalability, and integration - which should in the end shorten the time to market (faster roll out) - and at the same time mitigating risk. Data scientists will be in high demand to address all the data-driven needs.

Figure 5.

The operating model for banks needs to be reshaped, with a lean, high level of automation in the back-office based on the organization structures to allow for fast processing. Decision and governance processes will need to be streamlined, with a new more agile culture to support a customer experience in real time. Digital banking will change the way revenue is generated. The more customer-centricity becomes a major driver, deep customer insights have a potential to open up new sources of revenue, such as third-party advertising and customers paying for value-added services.

The biggest problem and challenge for banks is that most of their internal processes were designed and developed a long time ago. This has created a

major problem: when banks want to switch to a digital world, they have to redesign their processes. The new participants on the market (FinTech) don't have the legacy the banks do – and this is one of the main reasons why it's so difficult for a more traditional bank to simplify all of its operations. At this stage, particularly in Europe, banks are confronted with local regulations relating to privacy and data protection like MiFID II and PSD2. These create another barrier to transforming the digital processes – they might hit the boundaries of the legal framework.

Going paper free as part of operational excellence. Replacing paper-based activity and data processing with digital is faster, cheaper, and more secure, and helps enterprises integrate and use the data for better products and services. Digital transformation allows reusability of client data.

Paper culture prevails due to industry needs, technology maturity, legislation and employee habits. According to research, the top reason for the use of paper is the need for physical signatures (55%), followed by 48% using paper due to suppliers/customers continuing to send paper and 41% due to internal staff preference. Paper signatures are most commonplace in banks with 75% indicating this was a top driver for paper use. Consequently, cultural resistance to minimizing paper in banks usage is 28%. Workflow solutions which enable more effective information sharing, collaboration and efficiency are critical in supporting any digitization strategy. 80% of most digitally transformed banks have implemented digital documents and 69% are using e-signatures – this compares to just 44% and 25% of banks at the beginning of transformation.

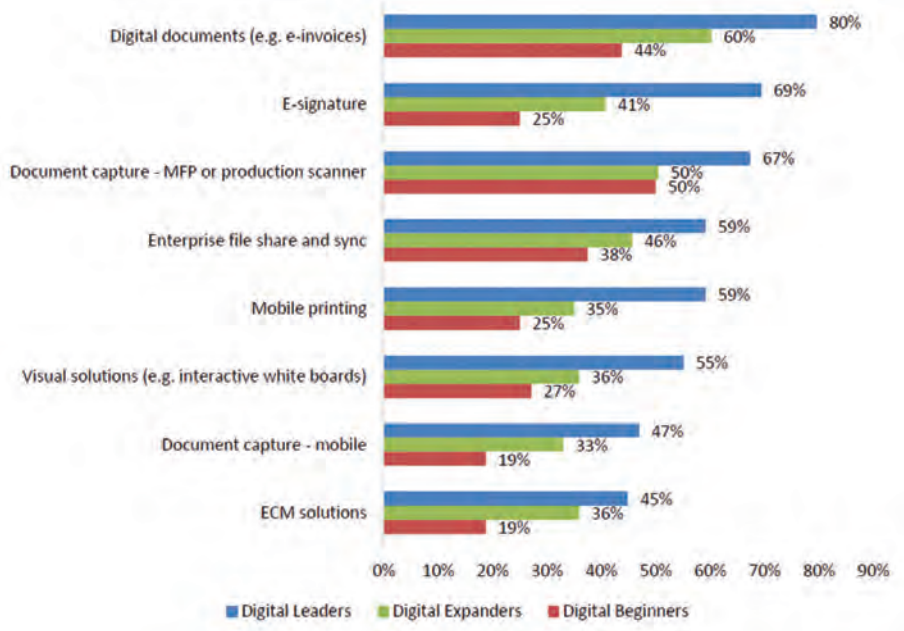
Lower Costs and Risks with Paper Free Processing

It is estimated that information workers spend up to 20% of their time filing and searching through paper documents. Our estimates indicate that a DMS can reduce time spent locating, retrieving and filing documents by nearly 75%. A shift from a paper-based to a digitized system reduces costs associated with lost and misplaced documents as well as printing and distribution costs. It also lowers error and rework rates. Cost analysis for those companies shows that implementation of a DMS typically delivers close to 6% in cost savings annually.

Digital Signature Cuts the Costs and Speed up the Processing

The financial services sector continues to be heavily reliant on manual signatures. Recent research indicates that 80% of businesses print documents to be signed, with the figure rising to 94% for the financial services sector. The use of a digital signature solution can dramatically reduce paper costs. Digital signature solutions can also drive higher conversion rates. For instance, the combination of digital signature and straight-through processing helped a leading UK-based bank achieve cost savings and a significant increase in overall sales volumes. The bank's personnel have become familiar with the system (see Figure 6).

Figure 6. Idatix survey



Reduce cost

However, once the bank wants to avoid the need for the customer to fill in the same data numerous times, everything can become much more difficult if the processes are organized into silos, which is the case in most banks.

Branch transformation
Branches are evolving into centers of sales and advisory hubs, with the aim of increasing the value to the bank of each customer visit through relationship building.

Data architecture
The ability to create, store, access and analyze data is at the heart of a digital transformation. Inside customer data are the leading aspects of a new way of offering banking products and services. Introducing a data architecture which is connected to and understood by all distribution participants is the foundation for operational excellence.

Automation and STP
A digital business model with automation and straight-through processing can enable staff to focus on value-adding activities, but they will need to be reskilled.

Provide a frictionless service
All customer touchpoints, business processes, and data sources must be integrated to provide a frictionless experience. Customers should never need to provide information more than once, and processes should be streamlined to minimize administration for customers and staff alike. Key to all this is reuse of the data, which is still a big challenge in the banking sector.

Time to market
Digital transformation should allow organizations to bring new offers at a lower marginal cost, not least by adopting new technologies (cloud computing, advanced analytics, IoT, blockchain). This allows them to carry out development and launch products with little upfront investment and at a much faster speed.

Transformation of products and services for wider ecosystems

New FinTech companies are targeting origination of sales and the customer-facing side of the bank. Even a partial loss of direct customer relationships will have a significant negative impact for banks. McKinsey expects consumer

finance, up to 40 percent of revenue and up to 60 percent of profits are at risk of loss by 2025. That is equivalent to about 50% lost compare to the current level. In payment services, 30 percent of revenue and 35 percent of profits are at risk. Considering the major five retail banking businesses – consumer finance, mortgages, SME lending, payments and wealth management – the situation is similar. How should banks respond to this threat?

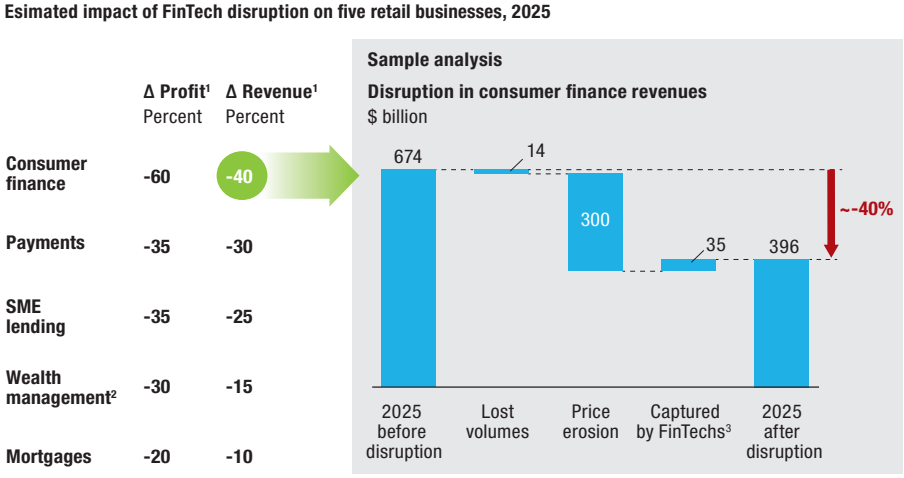
Banking as a Platform solution

It's clear from research that the BaaP (Banking as a Platform) concept in banks is possible but will require enormous changes to take place. The idea of creating a universal platform to combine banking services enriched by non-banking products is the future of the banking sector. BaaP thinking is starting to emerge in Europe and Asia, taking advantage of favorable regulatory frameworks and market opportunities. One of the European examples is Solaris Bank – offering BaaP opportunities to FinTech companies and enabling them to take their services to market. It is done via a licensed organization, a fully digital bank. There are already three platform services, Escrow and E-money, Rapid Credit and Digital Banking Engine offering nearly plug-and-play solutions to most regulatory and technical challenges across industries.

Prepare for digital business landscape

The next generation of disruptive technology – such as cognitive, new generation security and the Internet of Things – needs to be anticipated. Financial institutions can future-proof themselves by developing an enterprise-wide IT architecture underpinned by APIs in such a way that their strengths can be easily combined with other players in the digital ecosystem. This new landscape has to be open to the outside world. There are two options: isolate or cooperate. It seems like the second option is more appealing (see Figure 7).

Figure 7. McKinsey research



[1] Compared to 2025 projections without the impact of Fintech and digital attackers; profit numbers include the impact of savings on operating costs as a result of digital; revenues are after risk cost, profits are after tax; figures are rounded.

[2] Excluding deposits

[3] Includes currently unbanked segments

Source: McKinsey Panorama

Conclusion

Banks will become more digital. It's only a matter of time. As customers, competitors, and even regulatory agencies push in this direction, the promise of anytime, anywhere banking with transparency and convenience will ultimately bring together today's branch-based traditional players with the no-frills offers of direct banks and the innovative financial technology players, all coming from different directions, and it's hard to say who will arrive first.

For traditional banks carrying a heavy heritage, it will be crucial to overcome internal obstacles to achieve fast, robust decision making and processing, customer-centric channel management with revised governance mechanisms, and agile, high-performance IT landscapes - but the cultural barriers may be even more challenging; a new mindset is required in many regards - better and faster innovation, a fair and transparent product and service offerings, and new sources of revenue need to be tapped into.

- Banks need to become more open and look at new business models and ways of working. Collaboration and partnership with a wide group of non-banking parties is the way forward and APIs can facilitate this.
- Access to data and systems via an API is just the first step with the obvious next step for banks being the packaging together of access and services in the manner popularized by one of those looming non-bank payments competitors.
- It is important for banks to see the API framework, API strategy and own APIs as business issues, business decisions and business architectures rather than a technology problem to be solved in the IT department.

Bibliography:

1. American Banker, „Banks Use More Paper Despite E-Statements' Popularity", August 2012
2. Association for Information and Image Management; Edge Systems, „Document Management Return On Investment"
3. BPCE, „Groupe BPCE: results for the first quarter of 2013", May 2013
4. Capgemini and MIT Center of Digital Business, „The Digital Advantage: How Digital Leaders Outperform Their Peers in Every Industry", November 2012
5. Capgemini Consulting client
6. Capgemini, „Trends in Retail Banking Channels: Meeting Changing Client Preferences", 2012
7. Deilotte University Press, "Digital transformation in financial services. The need to rewire organizational DNA", 2016
8. Idatix, „Financial Services: Helping the Environment & Going Paperless, Properly", July 2012
9. IDC "Digital Transformation Survey", 2015
10. IDC through Laserfiche, „5 Easy Ways to Show ROI for Document Management Software", 2012
11. Mind the gaps: The 2015 Deloitte Millennial Survey," Deloitte Touche Tohmatsu, 2015
12. Trivaeo, „Automating Back Office", March 2013
13. YouTube, „La signature électronique en agence", April 2013

Karolina Marzantowicz
Distinguished Engineer, FSS&Blockchain, IBM Polska

Jest entuzjastką technologii i innowacji specjalizującą się w projektach transformacji cyfrowej, tworzeniem nowoczesnych koncepcji biznesowych i rozwiązań informatycznych. Doradza firmom, głównie z sektora finansowego w Europie Środkowo-Wschodniej. Pasjonują ją nowoczesne technologie takie jak: blockchain, sztuczna inteligencja i internet rzeczy. Jest autorką licznych publikacji w prasie naukowej, branżowej i ekonomicznej, współautorką dwóch książek oraz mówcą o wydarzeniach publicznych w Polsce i na świecie.
Posiada ponad 23-letnie doświadczenie zawodowe zdobyte w sektorze bankowym oraz IT, a od 16 lat jest związana z firmą IBM. Jest członkiem IBM Academy of Technology oraz Rady Naukowej CAS przy Politechnice Gdańskiej.
Prywatnie mama trojga wyjątkowych dzieci. Kocha góry o każdej porze roku. Najlepiej odpoczywa biegając (także maratony).

Karolina Marzantowicz, IBM

Architektura Banku Przyszłości – Banking as a Platform

Nie tylko technologia rozwija się w niesamowitym tempie, ale też sposób, w jaki działają firmy i branże oraz jak my sami funkcjonujemy na co dzień jako ludzie.

Od ubiegłego stulecia obserwujemy rozwój kolejnych er informatyzacji. Komputery mainframe'owe wspierały automatyzację procesów wewnętrznych przedsiębiorstw. Sektor bankowy mógł z sukcesem automatyzować procesy obsługi produktów i klientów w głównych systemach bankowych. Potem nastała era komputerów osobistych, które rozprzestrzeniły się poza serwerownie na nasze służbowe i domowe biurka. Architektura aplikacji rozwinęła się w kierunku klient-serwer. Rozwinęło się wsparcie dla obsługi informatycznej oddziałów bankowych. Wraz z doskonaleniem się technologii sieciowych i teleinformatycznych przywitaliśmy erę informatyki sieciowej i jej dziecka – Internetu, a następnie przetwarzania w chmurze (*cloud computing*). Aplikacje weszły w architekturę wielowarstwową. Banki rozszerzyły ilość kanałów współpracy z klientem o *Call Center* (centrum obsługi telefonicznej) oraz bankowość internetową. Internet pomógł w intensywnym rozwoju nowoczesnych rozwiązań do płatności elektronicznych.

Obecna era rozwoju technologii komputerowych to tzw. *smart computing*, czyli inteligentne przetwarzanie lub *ambient computing*, czyli przetwarzanie w globalnym, coraz mocniej połączonym świecie. To przetwarzanie, które już dawno wyszło poza serwerownie banków i dziać się może na setkach typów urządzeń mobilnych. Przyniosło ono bankowość mobilną oraz umobilnienie pracowników banków.

Technologie, takie jak cloud, sztuczna inteligencja (*artificial intelligence*), Internet Rzeczy (*Internet of Things*) i *blockchain* zmieniają nie tylko sposób, w jaki używamy technologii, ale też redefiniują obecne modele biznesowe. Dają możliwości budowania nowoczesnych sposobów na kreowanie nowych wartości w gospodarce, zmieniając bankowość. Usługi bezpośrednie (*Peer 2 Peer*) w obszarze płatności czy finansowania są dobrym przykładem na to, jak innowacyjne technologie redefiniują usługi finansowe.

Te technologie spowodowały m.in. rozbicie łańcucha wartości, jaki funkcjonował od lat. I stało się to nie tylko w sektorze finansowym, ale praktycznie w każdej dziedzinie gospodarki.

Platform Economy

Przez lata w bankowości mieliśmy do czynienia z rozwojem i innowacyjnością dookoła produktów oraz wspierającymi to modelami biznesowymi. Gospodarka cyfrowa w takim kształcie, jak obecnie to już nie gospodarka oparta o produkty. Weszliśmy w tzw. gospodarkę platformową (*platform economy*). Czym jest platforma? Platforma to pośrednik, który łączy uczestników rynku: sprzedających i kupujących. Przykładem może być giełda akcji publicznych (NYSE/Nasdaq, GPW) czy platformy handlu internetowego: eBay, Amazon, Allegro i OLX. Z kolei Apple App Store czy Google Play to przykłady platform dookoła systemów operacyjnych.

Możemy spojrzeć szerzej na zjawisko platformy jako modelu biznesowego: platforma staje się pośrednikiem, który nie tylko łączy dwie strony, ale przynosi ze sobą grupy użytkowników w celu ułatwienia wymiany gospodarczej i społecznej. Tu przykładem z rynku finansowego są sieci płatności: Visa, MasterCard czy PayPal. Inny przykład to media społecznościowe (Facebook, Twitter) oraz media cyfrowe (gazety, strony internetowe) łączące reklamodawców, konsumentów, producentów treści i jednocześnie wnoszące grupy swoich użytkowników jako zasób.

Modele platform cyfrowych fundamentalnie zmienią sposób w jaki przedsiębiorstwa będą mogły robić interesy i odnieść sukces w epoce cyfrowej. W przeciwieństwie do tradycyjnych modeli, platformy nie tylko tworzą i dostarczają produkty na rynek. Pozwalają one na tworzenie sieci uczestników, którzy w oparciu o produkty dostarczają wartości dodane konsumentom końcowym.

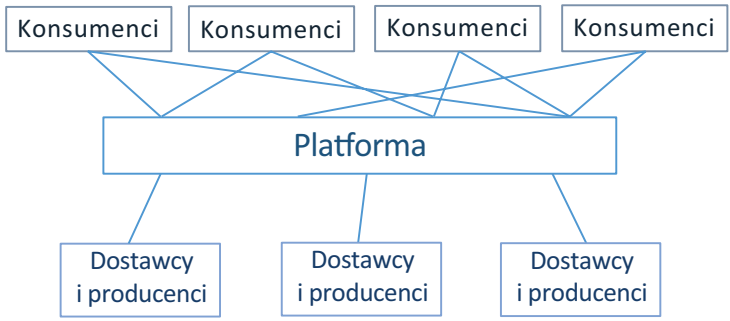
Platformy naruszyły, działające sprawnie od lat, tradycyjne modele biznesowe. Uber zrewolucjonizował myślenie o usługach transportowych, a Airbnb stało się konkurencją dla największych sieci hotelowych. Mamy do czynienia z nowym ładem gospodarczym, który zależy od Internetu, jego użytkowników, danych i możliwości ich przetwarzania. Ekosystem, jaki jest tworzony przez platformy jest źródłem wartości dla wszystkich jego uczestników i ustala warunki, na których można uczestniczyć. Platformy wzmacniają też trend konwergencji pomiędzy branżami i wzajemnego przenikania się. Sprawdzają się w handlu, rozrywce i turystyce.

Czy banki mogłyby funkcjonować jako platformy usług finansowych i nie tylko?

Co mogłyby wnieść i jak skorzystać?

Architektura platformy

Architektura platformy rozróżnia następujące dwie główne role: producentów i konsumentów.

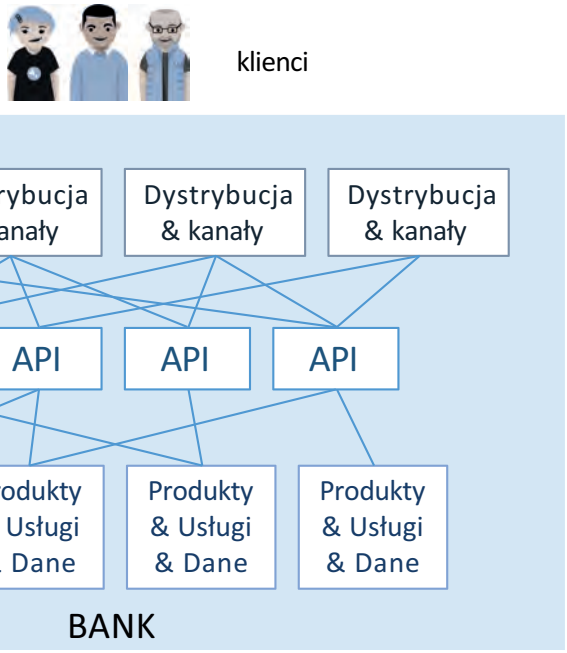


Z punktu widzenia architektury w dużym uproszczeniu rozróżniamy następujące komponenty:

- Produkcję i zarządzanie cyklem życia produktów oraz usług – częściowo w systemach centralnych banków oraz w dedykowanych rozwiązaniach do obsługi danych produktów (systemy kartowe, systemy płatnościowe).
- Integrację klientów banków opartą o API. Nie zmienia to faktu, że bank może potrzebować takich komponentów w architekturze, jak szyna usług do integracji wewnętrznej systemów (ESB/SOA) czy silnik procesów (BPM).

- Warstwę dystrybucji produktów i usług oraz kanały dostępu – tradycyjne i nowoczesne kanały kontaktów i obsługi klientów.

Rys. 2. Tradycyjny Bank Uniwersalny



Tradycyjna architektura banku zakłada, iż na potrzeby swojej działalności posiada on architekturę IT obejmującą wszystkie te trzy warstwy. Główne systemy bankowe odpowiadają za zarządzanie produktami i usługami finansowymi. Integracja ze światem zewnętrznym opiera się o API, które eksponuje wyodrębnione usługi biznesowe banku. Ekspozycja usług i produktów poprzez API daje możliwość stronom trzecim (programistom, startupom) rozszerzyć funkcjonalność systemów bankowych z korzyścią dla klientów końcowych.

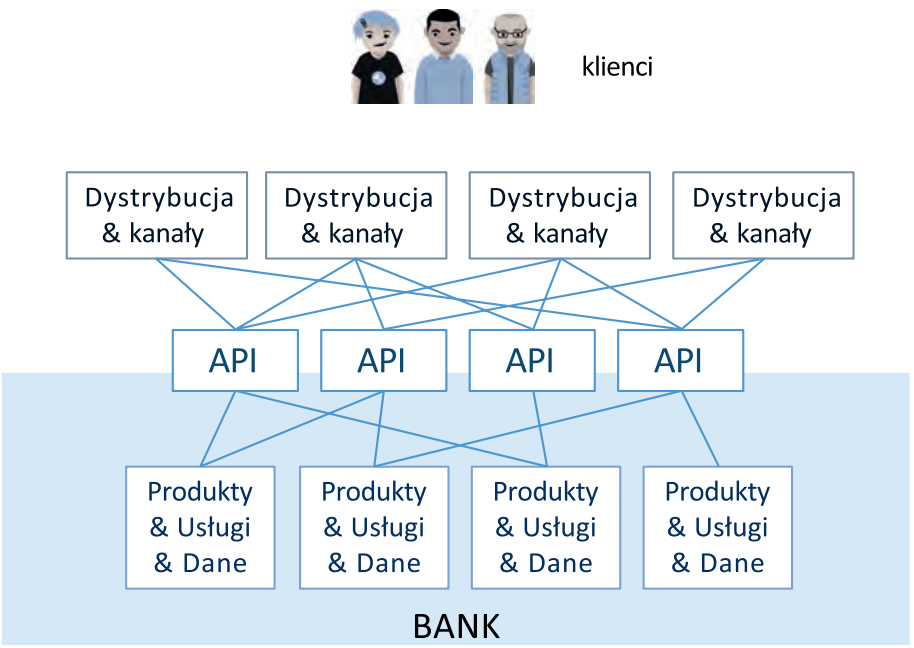
Implementacja europejskiej dyrektywy PSD II będzie dla banków okazją do przetestowania ekspozycji usług biznesowych w oparciu o API.

Zazwyczaj bank jest właścicielem kanałów kontaktu i obsługi klientów.

Ten tradycyjny model ulega w ostatnich latach zachwianiu. Rośnie ilość konkurencji spoza sektora bankowego. Banki ciągle w dużej mierze starają się budować strategie w oparciu o to, co posiadają. A w cyfrowej gospodarce dużo bardziej liczy się to, czym się dzielimy i z kim współpracujemy (*Sharing Economy*). Rozczłonkowanie łańcucha wartości ekosystemu bankowego powoduje, że banki nie tylko mogą, ale często powinny wybrać, w jakiej roli strategicznie widzą siebie na bazie paradygmatów cyfrowej transformacji.

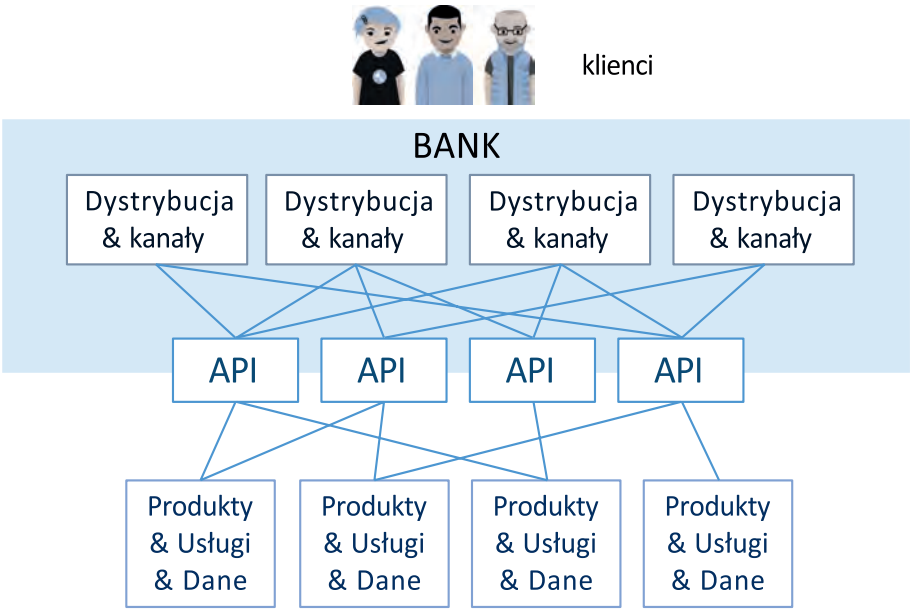
Słyszymy od czasu do czasu, iż banki znikną w przyszłości lub całkowicie przejdą do zaplecza tracąc bezpośredni kontakt z klientami. W takim modelu mówimy o architekturze, w której oczywiście bank nie znika, tylko istnieje nadal. Prowadzi obsługę produktów i pewnych procesów bankowych, ale pozbywa się całkowicie interakcji z klientami i ich obsługą.

Rys. 3. Bank jako producent



Bank może skupić się na warstwie kontaktu z klientami oraz dystrybucji produktów i usług, a zrezygnować całkowicie z utrzymywania produktów. W takim przypadku może współpracować z wieloma różnymi dostawcami produktów i usług finansowych.

Rys. 4. Bank jako dystrybutor

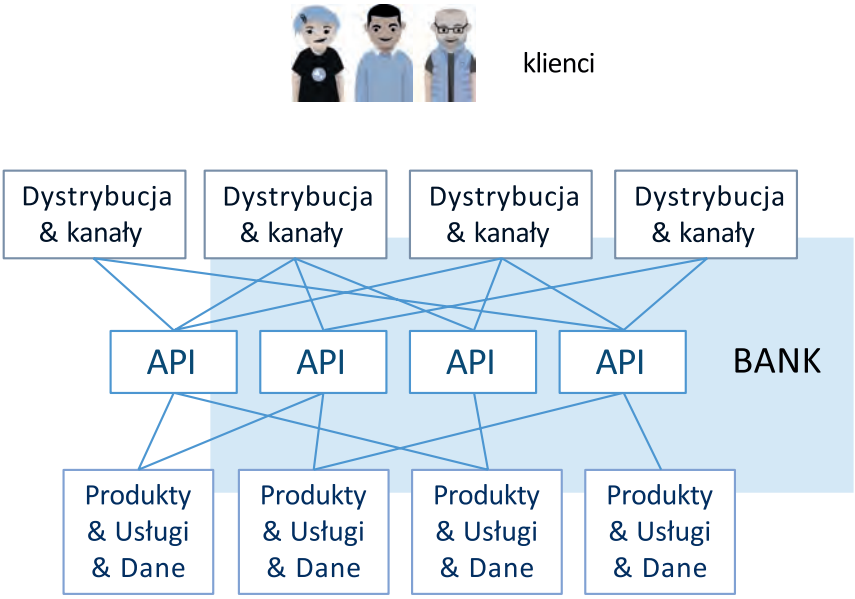


W takim modelu działa m.in. Moven Bank. Wiele startupów z obszaru fintech jest w stanie dostarczyć lepsze z punktu widzenia użytkownika końcowego rozwiązania do wielokanałowej obsługi, a oferowane produkty i usługi mogą pochodzić od wielu dostawców. W modelu tym łatwiej rozszerzyć ofertę o usługi niefinansowe, mając przede wszystkim na celu potrzeby klientów, a nie, jak często bywa, ograniczenia, na oferowanie czego pozwalają nasze systemy centralne. Brak konieczności inwestowania w zaplecze informatyczne pozwala na większą elastyczność biznesową i optymalizacje kosztów oraz inwestycji. Utrzymywanie relacji z klientem oraz dostarczanie mu wartości wydaje się być ważną część strategii cyfrowej.

Ostatni kierunek, w jakim może się rozwijać omawiana architektura to bank jako platforma usług finansowych. W podejściu tym bank może utrzymywać niektóre z komponentów odpowiedzialnych za produkty, te które z jego punktu widzenia są kluczowe. Ale przede wszystkim bank tworzy platformę, na której umieszcza swoje i innych dostawców usługi, tak aby konsumenci mogli budować rozwiązania o unikalnej i najwyższej wartości dla

wybranej grupy użytkowników. Bank tworzy ekosystem partnerów budując portfolio usług dla swoich i ich klientów. Może także wybrane kanały kontaktu z klientem utrzymywać i rozwijać sam, a także udostępniać je jako usługa dla innych.

Rys. 5. Bank jako platforma



Efekt sieciowy, jaki daje taka architektura nie ogranicza się do optymalizacji kosztów i maksymalizacji profitowości.

Nowoczesne technologie umożliwiają bezpośrednie interakcje zarówno z partnerami, jak i klientami banku. A wartość końcowa jest budowana wspólnie.

Technologie takie jak Internet, przetwarzanie w chmurze, integracja oparta o API, sztuczna inteligencja i zaawansowana analityka są kluczowe do budowania architektury banku, tak aby wspierała ona wyzwania gospodarki cyfrowej, nadążała za trendami transformacji i dawała korzyści zarówno bankowi jak i klientom.

Architektura Banku a efekty sieciowe

Efekty sieciowe wpływają na nas wszystkich codziennie, choćby za pośrednictwem portali społecznościowych. Te platformy tworzą trendy, jak interakcje powinny wyglądać w świecie cyfrowym. Klienci oczekują podobnego poziomu obsługi również od banku. Klienci chcą móc wypowiedzieć swoje zdanie. Chcą być słyszani. Chcą współtworzyć. I wiedzą, że technologia współczesna powinna im to umożliwiać.

Nawyki wyniesione z mediów społecznościowych, gier czy platform *peer 2 peer* (p2p) kreują wymagania w obszarze usług finansowych, płatności, finansowania. A banki mają przed sobą jedną z trzech ścieżek rozwoju ich architektury IT:

- bank jako producent, z zaplecza obsługujący produkty i usługi,
- bank jako dystrybutor pierwszego kontaktu, koncentrujący się na relacjach z klientami i docieraniu do nich w najbardziej optymalny sposób,
- bank jako platforma, czyli integrator, który tworzy i buduje ekosystem dookoła siebie, oferowanych produktów, partnerów i klientów.

Transformacja cyfrowa będzie wymagała od banków większej otwartości.

Warto proaktywnie budować architekturę banku tak, aby nie ograniczała możliwości biznesowych dając jednocześnie wysoki poziom bezpieczeństwa.

Jacek Figuła
Strateg i szef sprzedaży w Billon Group

Firma pracuje nad zrewolucjonizowaniem systemów płatności i rozpowszechnieniem działającej w Polsce gotówki elektronicznej opartej na technologii *blockchain*.
Wcześniej przez siedem lat w Cisco Systems budował i realizował strategię sprzedaży usług, w tym wsparcia i konsultingu inżynierskiego w Polsce i krajach Europy Środkowej. Zbudował kilkunastoosobowy zespół oparty na zaufaniu i wzajemnym wsparciu co zaowocowało bardzo ambitnym wzrostem sprzedaży. Przedtem w kilku innych korporacjach odpowiedzialny za sprzedaż rozwiązań IT w Polsce.

Jacek Figuła, Billon Group

Blockchain i rozproszona księga główna – bankowe tsunami czy szansa dla sektora bankowego

W ciągu ostatnich lat kilka pojęć z zakresu informatyki nabiera na znaczeniu w budowaniu nowoczesnych rozwiązań, również w sektorze bankowości. Po erze automatyzacji i wirtualizacji centrów danych oraz przetwarzania w chmurze zainteresowaniem coraz większej rzeszy architektów systemów bankowych zaczynają cieszyć się systemy samouczące się, analiza olbrzymich ilości danych czy systemy rozproszone, zwane z angielskiego *Distributed Ledger* bądź *Blockchain*.

W wielu dużych bankach funkcje systemu centralnego są od lat minimalizowane do tych podstawowych, głównie księgowych. Jest to spowodowane rosnącymi kosztami utrzymania takich rozwiązań, które też stanowią duże ograniczenia w procesie dynamicznego rozwoju banku będąc hamulcem we wdrażaniu innowacji. Sytuacja ta powoduje, że banki przygotowują nowe produkty i usługi poza systemem centralnym, w ten sposób stopniowo wymieniając systemy tradycyjne. Prawdziwą sztuką jest wtedy jednoczesne zarządzanie „starymi" i „nowymi" rozwiązaniami.

Interesującą alternatywę do utrzymywania czy rozwoju systemów centralnych zaprezentował kilka lat temu IBM, wykorzystując w tym celu narzędzia *middleware*. Przykładowo, aplikacja bankowości mobilnej łączy się z warstwą komunikacyjną i wykorzystuje system centralny tylko wtedy, gdy istnieje potrzeba wykonania transakcji – przelew lub uznanie. We wszystkich innych sytuacjach wykorzystuje inne systemy banku. Warstwa *middleware* umożliwia połączenie z systemami *back-office* nowych rozwiązań *front-office*, a tym

samym zapewnia możliwość oferowania zaawansowanych i nowoczesnych rozwiązań bankowych.

Innym rozwiązaniem problemów kosztowych i ograniczeń funkcjonalnych systemów centralnych jest, proponowana przez firmy takie jak Microsoft czy Amazon, migracja do przetwarzania w chmurze. Przełomem w Europie była decyzja Holenderskiego Banku Centralnego (DNB) w 2014 r., który zgodził się na wykorzystywanie przez banki platform współdzielonych. Coraz więcej instytucji finansowych decyduje się na ten krok w odniesieniu do swoich systemów wspomagających. Firma Temendos opublikowała nawet prognozę, że do 2020 r. większość projektów wymiany systemu centralnego banku będzie wykonywana w technologii „chmury", choć jednocześnie zaznacza, iż duże banki będą wykorzystywały do tego celu własne centra przetwarzania danych, zbudowane w sposób odzwierciedlający rozwiązania publiczne. To kompromis pomiędzy zaletami elastyczności i oszczędności kosztów, ale jednak w środowisku kontrolowanym przez bank.

Jednym z wyzwań migracji danych instytucji finansowych do przestrzeni publicznej jest ich wrażliwość i konsekwencje odczytania czy wręcz modyfikacji przez osoby niepowołane. Pomoc przychodzi ze strony kryptografii, która odpowiednio zaimplementowana pozwala doskonale ograniczyć możliwości czytania czy ingerowania w dane bez znajomości klucza prywatnego użytkownika. Wykorzystując dalej rozwiązania typu *blockchain* daje się dodatkowo wyeliminować możliwość anonimowej modyfikacji bez pozostawienia śladu czy zafałszowania historii.

Dziś już wiemy, że *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. Widać tę zmianę w bankowości detalicznej i nawet w bankowości transakcyjnej. Pierwsze wdrożenia nastąpiły właśnie w Polsce, dzięki czemu nasz kraj stał się jednym ze światowych liderów zarówno w obszarze nowoczesnej bankowości detalicznej, jak i myśli technologicznej. To również w naszym kraju ministerstwo cyfryzacji w swoim programie *Od Polski papierowej do cyfrowej* określiło *blockchain* jako jedną z technologii pozwalających na duży skok w rozwoju kraju.

Warto więc 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*", a prezes banku Barclays określił ją jako system operacyjny przyszłości.

Czym jest *blockchain*? Czy rzeczywiście jest to rewolucja?

Blockchain to kolejny etap rozwoju przetwarzania danych, a precyzyjniej – baz danych. To w pełni zautomatyzowany proces bezpiecznego przekazania wartości (tzn. pieniędzy) od nadawcy do odbiorcy bez udziału pośredników (i generowanych przez nich kosztów), ale z pełną gwarancją realizacji takiej transakcji. To spełnienie marzenia o *Internecie Wartości*, o którym przez lata opowiadały i nadal opowiadają firmy konsultingowe, często wskazując na kolejną rewolucję internetową. To również odpowiedź na ograniczenia centralnych systemów, które ze swojej natury są:

- Centralne – wszelkie informacje znajdują się zawsze w centralnej bazie danych, 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, co oznacza, że baza danych wymaga, aby użytkownik zalogował się do pośrednika, tzn. banku (a nie dostawcy wartości) 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 w niej zgromadzonych.
- Awaria centralnej bazy danych blokuje wszystkim użytkownikom dostęp do korzystania z bazy, co przekłada się na to, że gdy serwer centralnej bazy danych nie działa, żaden użytkownik nie ma do niej dostępu.

Rozwiązaniem powyższych problemów oraz wynikających z nich konsekwencji jest właśnie system oparty o technologię rozproszonej księgi głównej – *blockchain* – kombinacja architektury rozproszonej danych, szyfrowania i zabezpieczenia do nich dostępu. Wymieńmy jego kluczowe cechy:

1. 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.

2. 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.
3. 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 czemu można dostarczać w 100 procentach dostępne systemy zbudowane na *blockchainie*, ponieważ interakcje pomiędzy uczestnikami mogą zachodzić bez udziału centralnego punktu czyli bez centralnej autoryzacji (z ang. *3rd party authorisation*).

Tym samym *blockchain* niesie łatwość oferowanie nowoczesnych usług finansowych. Jakie są jego zalety?

- **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 są zapisane w sposób zakodowany w każdym *blockchainie*, ale 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.
- **Brak ryzyka** – ponieważ nie ma jednego podmiotu sprawującego kontrolę, nie istnieje ryzyko jej utraty oraz że ekosystem może działać bez przerw. To pozwala bankom na wyeliminowanie ryzyk operacyjnych związanych m.in. ze 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 obu stronom 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 planując ją na maksymalne obciążenie, ale mogą dynamicznie wykorzystywać zewnętrzną moc obliczeniową (z ang. *throughput* i *scaling*).
- T**ransparentność** – dzięki *blockchain* ryzyko nieautoryzowanego udziału pośredników jest eliminowane, a to istotnie ogranicza 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).

Jednak blockchain to nie tylko korzyści

Systemy rozproszonej księgi głównej nie są odporne na wszystkie możliwe cyberataki. Głównie dlatego, że, co do zasady działania takich rozwiązań, ktokolwiek kto potrafi zmodyfikować jedną kopię łańcucha i taką zmianę uwiarygodnić, wtedy owa zmiana będzie przez całą księgę traktowana jako wiarygodna. Dlatego tak istotnym jest upewnienie się, że taki scenariusz nie może mieć miejsca. Są jednak dwie klarowne przewagi systemu rozproszonego nad centralnym:

1. Koszt uwiarygodnienia zmiany, o której mowa powyżej jest znaczący, a potencjalny zysk z takiego oszustwa niewielki. Powoduje to nieopłacalność podobnego włamu do rozwiązania rozproszonego.
2. Uwiarygodnienie takiej transakcji nie może odbywać się bez wymazania jej historii, a co za tym idzie możliwości jej skorygowania.

Ważnym aspektem jest specyfika regulowanych systemów rozproszonych, a więc takich, gdzie nie istnieje pojęcie wydobywania kolejnych bloków ani konsensusu społecznego. To systemy, gdzie podaż wartości (pieniądza) jest nadzorowana przez bank centralny lub licencjonowane banki komercyjne. W takich systemach historia i długość bloków została ograniczona i, co za tym idzie, bezpieczeństwo systemu częściowo leży po stronie systemu centralnego – banku wydawcy (Instytucji Pieniądza Elektronicznego), który dba o integralność struktur emitowanego pieniądza. Transakcje jednak są zabezpieczane kryptograficznie i bez ingerencji banku czy jakiegokolwiek systemu centralnego, aż do momentu powrotu pieniądza elektronicznego do banku wydawcy.

Dodatkowo, systemy rozproszone charakteryzują się stosunkowo niewielkimi kwotami przechowywanymi i przesyłanymi. Dlatego jakikolwiek atak na poszczególną transakcję jest niewspółmiernie kosztowny w stosunku do potencjalnego zysku. Można tym samym powiedzieć, że szkoda wyrządzona przez taki atak jest pomijalna.

Ważnym aspektem jest tożsamość użytkownika systemu opartego o *blockchain*. Ze swojej natury jest to medium przesyłania wartości elektronicznie – przez Internet. Dlatego istotna jest pewność, kto z kim dokonuje transakcji. Problematyka KYC (czyli *Know Your Customer*) w formie elektronicznej nie jest jeszcze w pełni rozwiązana. Jak więc upewnić się z kim mamy do czynienia

po drugiej stronie? Jest wiele dostępnych innowacyjnych rozwiązań, ale, jak do tej pory, banki centralne czy urzędy nadzoru nie zdecydowały się zaakceptować ich do użycia w systemach bankowych czy pieniądza elektronicznego. Nadal stosowane jest wysyłanie umowy kurierem, aby klient podpisał umowę, a kurier sprawdził jego tożsamość, bądź klient zapraszany jest do oddziału banku w celu osobistego podpisania umowy.

Prawdziwy przełom w systemach informatycznych dla sektora finansowego

Prezes banku Barclays odważył się na określenie rozwiązań *blockchain* mianem systemu operacyjnego przyszłości. Trudno się nie zgodzić, gdyż systemy rozproszonej księgi głównej mają potencjał otwierać nowe możliwości i nowy sposób interakcji z klientem czy kontrahentem. Fakt posiadania narzędzia, które w czasie rzeczywistym, nieodwracalnie i niewielkim kosztem pozwala przekazać elektronicznie wartość, czyli np. rozliczyć transakcje, tworzy nowe modele cyfrowej relacji z klientem. Od jego pozyskania, aż do końcowego rozliczenia. Systemy takie można również stosować we wszelakiej dokumentacji, identyfikacji, hipotekach, itp.

Na pewno innowacyjność rozwiązania powoduje, że wiele podmiotów, które dzisiaj działają w sposób tradycyjny mogą się poczuć zagrożone. Poprzez interakcje typu *peer-to-peer* (osoba do osoby) wiele organizacji może być zmuszona przedefiniować wartość, którą dostarcza. W szczególności tzw. zaufana trzecia strona (dzisiaj nie tylko jedna) biorąca udział w każdej elektronicznej transakcji bądź Ci, którzy dziś przechowują wartość lub tylko pośredniczą w jej przekazywaniu.

Mówiąc o rozwiązaniach nowych najlepiej jest się z nimi zapoznać w praktyce. Polski rząd we wcześniej wspomnianym programie rozwoju *Od Polski papierowej do cyfrowej* wskazuje na *blockchain* jako obiecująca technologię przyszłości. Powstała grupa robocza przy Ministerstwie Cyfryzacji, która pozwala „eksperymentować" z systemami *blockchain*. Pomysłów jest wiele i należy tylko chwilę poczekać, aż pierwsze systemy pilotażowe oparte o rozproszoną księgę będą działały w Polsce w ramach tej inicjatywy.

Firma Billon już od kilku lat testuje rozwiązanie polskiego złotego w formie elektronicznej. Jest to wdrożenie z Plus Bankiem, które przez ostatnie dwa lata udowodniło, że system jest dojrzały i działa bez zarzutu. Od grudnia 2016 r. właśnie polska firma Billon jako pierwsza na świecie uruchomiła

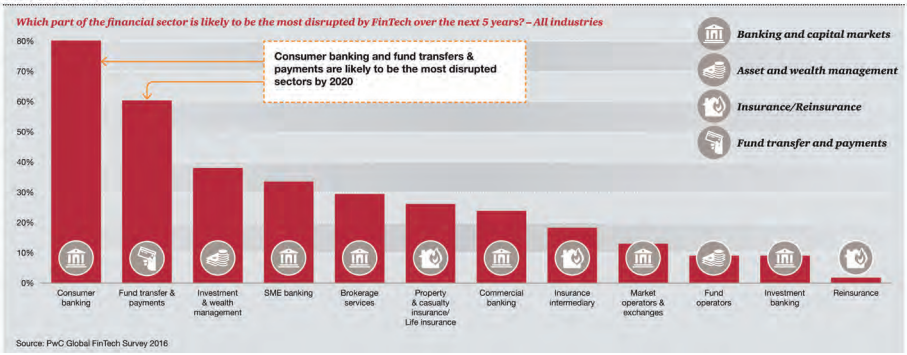
również w Wielkiej Brytanii funta brytyjskiego w wersji elektronicznej (e--Money). Działa on w ramach piaskownicy regulacyjnej brytyjskiego organu kontroli finansowej – FCA.

Podobnie jak polski rząd, Wielka Brytania również myśli o szerszym zastosowaniu systemów rozproszonych. Wspomina się o takich jak:

- zabezpieczanie systemów przed atakami cybernetycznymi,
- redukcja kosztów operacyjnych,
- walka z wykluczeniem finansowym, ubankowienie ludzi słabo bądź nieubankowionych,
- redukcja nieprawidłowości podatkowych, nielegalnych przepływów pieniędzy.

Firma Price Waterhouse Coopers opisuje te obszary na ilustracji poniżej.

Figure 3: Areas of disruption



Bardzo ciekawa ankieta z początku lutego 2017 r.[1], przeprowadzona przez Synechron & TABB Group, napawa wielkim optymizmem odnośnie możliwości, jakie systemy rozproszone będą oferować. Stąd odpowiedzi osób decyzyjnych w firmach zajmujących się usługami finansowymi i *High Tech*:

- 94% respondentów zdecydowanie wierzy w rozwój projektów opartych na *blockchainie*.
- 87% widzi dla nich miejsce w budżecie.
- 67,4% instytucji finansowych **już** zaangażowanych w *blockchain*.
- 16,7% **już** zidentyfikowało *use case*.

1 https://bitcoinmagazine.com/articles/survey-shows-overwhelming-support-blockchain-tech-financial-services-executive-boards/

Blockchain i systemy rozproszone coraz odważniej będą wchodzić w poszczególne aspekty bankowości ze względu na architekturę nowej generacji, która dostarcza wymierne korzyści w porównaniu do dotychczasowej – centralnej. Dodatkowo presja regulacyjna na obniżanie kosztów (np. interchange i PSD II) oraz do oferowania usług bankowych na zasadzie dostępnych dla wszystkich kont bez opłat (PSD II) zmusza sektor bankowy do innowacji. Dlatego najpewniej banki rozpoczną współpracę z fintechami, które takie systemy rozwijają lub same zaczną tworzyć swoje rozwiązania idące w kierunku systemów rozproszonych.

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.

Andrzej Sieradz
Wiceprezes Zarządu Banku BGŻ

Doktor nauk ekonomicznych Uniwersytetu Gdańskiego. Ukończył Politechnikę Warszawską w 1983 r. 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 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., najpierw jako dyrektor zarządzający. W latach 1997–2002 pracował w Coca-Cola HBC w Polsce i w centrali w Wiedniu.

Piotr Puczyński, Andrzej Sieradz

What does a red rose from Kenya have to do with the blockchain?

A ledger could be a book or a file or a record of transactions or public records of anything. The most common reference for ledgers people have is within the financial and accounting world – and accounting is not commonly known as being extremely exciting. For many years, accountancy as a profession was a synonym of a boring job for boring people. It was a closed world. Every company was making transactions, boosting sales, signing contracts, out of which, "magicians" called accountants were creating financial reports. Those reports were believed to present figures describing the financial condition of the company for that moment in time. To make sure that the results of the reports were comparable, there were common rules established by law. Additionally, to make sure that everything was done according to the rules and regulations, a role of "super-accountant" was established, and these called financial auditors. Before issuing financial reports, companies were hiring auditors so they could confirm that all was prepared according to the law. The system seemed to be working well until… October 2001. That was the first of a series of scandals – the bankruptcy of ENRON (that in turn lead to the bankruptcy of audit firm Arthur Andersen). The system failed in all the most important aspects – revenue recognition, mark to market accounting, special purpose entities and corporate governance (including auditing practices).

The system tried to defend itself. More complicated rules and regulations were provided. New legislation was established with one goal in mind – to improve the accuracy of financial reporting for public companies. There were also increased penalties for all sorts of fabrication and alteration of records (the Sarbanes – Oxley Act).

The first and immediate effect was that the world of accounting became even less clear for outsiders. It became difficult even for professionals – but has it helped to achieve the main goal – to regain trust of investors by public companies?

It didn't take long until the economy was struck again. This time globally and in the most regulated sector – finance. The global banking crisis of 2007–2008 came with full surprise – in the area of economy which was supposed to be the most transparent and trustworthy. It occurred despite complicated regulations – the same issues from 2001 emerged again. Behind all the complicated accounting rules, the actual financial condition of banks was obscured. The complexity of the financial reporting system was beaten by the complexity of all sorts of artificial products. The complexity of the system was so high that instead of assuring investors by its accuracy, it created a "foggy" atmosphere ideal for manipulation. None of the new regulations were able to stop it. What was more surprising – at the end of the day, almost no one was found guilty of causing the enormous crisis. Maybe a couple of dealers were the ones to blame.

The Crisis was brought under control mostly with the help of public money. Then the same cure was applied as after the ENRON scandal – more regulations. But this time that was not enough to ease anger of the public. The most valuable virtue of banks and public companies – trust, had disappeared. People got angry because highly paid managers didn't take the blame and most of the costs were taken by "ordinary" people.

In such an atmosphere, someone called Satoshi Nakamoto published his new concept of a ledger – a blockchain (mostly now call a Distributed Ledger). The principle of that work was to create a financial world where a trusted third party (e.g. a bank) is not needed. Furthermore, the currency issuers are not needed either; currency is issued by an algorithm. The same protocol makes sure that transactions are properly registered in a single, but decentralized, ledger. All of that is designed with security, integrity and transparency in mind.

Suddenly the whole idea of ledgers became trendy. Everybody started talking about accounting which in reality had no accounting at all. A ledger is just a register of transaction details. No chart of accounts is needed and accounting rules are simple and based on the principle of consensus between all participants – and those principles are guarded by algorithm, not by auditors.

This is the real revolution. So far, in the modern era, the implementation of choice for a ledger was a database, found in all modern accounting systems. Now we do not have a database with structure and strict rules; we have a register of transactions. After developing all our accounting principles over hundreds of years, we are back to the simple ledger. Like the old bookkeeper Rzecki in the novel "Lalka" by Prus, we are writing line by line in a book transactions as they occur. No possibility to change what is already written. No chance to change the order of transactions. No room for interpretation. Everything time-stamped.

So, it seems that we have discovered the way for real transparency of public companies. That is why we are back to the bookkeeping rather than accounting. No difficult rules but a simple register. We signed a contract today and we are registering it in the Ledger without any chance of erasing it.

If anybody remembers, in the early ,90s, multi-branch organizations ran their ledgers in decentralized, but also fragmented form. Each branch had its own full ledger, and could run its own balance sheet and P&L reports. Those reports were consolidated at the HQ level to form the financial statement of the company. As new technology was developed (especially in the area of telecommunications), organizations (among them all the banks) converted their ledgers so they could run them in one register for all entities. Still, it is possible to get, for example, P&L for each separate branch, but both the branch and corporate financial statement are run on one register of transactions.

A blockchain promises to go one step further. We can run our business and register its transactions in one global ledger. That might allow us to use all sorts of reporting, but also allows (with all the security restrictions) us to run similar reports on just our part of the register by investors and/or regulators.

Is this a way to regain trust? Do we find a solution in the simplicity of the concept?

Why has the blockchain concept got so much interest?

The blockchain – the technology behind cryptocurrency Bitcoin – has so far played a marginal role in the global economy. Why then is there so much fuss? Why are there so many conferences about it? Why are the big players in the financial industry running Proof of Concept projects and forming consortiums to investigate all the possibilities? Is it only because there is a threat that rebels are going to destroy the status quo in the financial world?

There are several reasons, but probably the most interesting is the fact that the blockchain is a technology that allegedly solves the issue of integrity in business and assures trust between the parties, mostly by algorithm and consensus of users. Technology to solve the ethical issues.

In today's world, we decided to solve the issue of integrity and trust using a so-called "trusted third party". Whether that is a bank, insurer, exchange, registry or government – we decided to trust the work they do. Unfortunately, we still have the issue of potential forgery or simple omissions.

Robert Sams, CEO of Clearmatics, describes a centralized transaction ledger's three weak points as "sin of commission" – forgery of a transaction; "sin of deletion" – reversal of a transaction; and "sin of omission" – censorship of a transaction.

The blockchain promises to address all those issues in the very transparent form of a combination of consensus and algorithms.

In its generic form as a bitcoin ledger, the blockchain allows for transactional interaction between unknown parties. Unknown meaning no direct trust exists, but if our transaction is going to be overseen by many participants, we agree our deal with comfort. Isn't it fascinating that, with the help of an algorithm, using very advanced theories from game theory to social studies, we can create a society in which its members can trust each other without even knowing each other? But that is not all.

By using a decentralized form of a ledger, we create a very reliable environment. It is not only the issue of not having any one point of failure, but we are having an architecture that is not possible to be switched-off. Registers of our assets will survive, whatever happens to a part of our network. Actually, all the participants are keeping a complete register. If they are entitled to ask, we will allow them to look into the content of our records. We can say that by distributing our register we are becoming fully transparent. Regulators can check every single one of our transactions and investors do not have to wait for periodic financial reports, as they are published presenting past performance of public company. They can get access to the live coverage of the financial life of the company.

By putting into the register time-stamped records of transactions and not allowing any single one of them to be reversed, all the observers are assured that they are getting the full picture of the financial status of the company. They can track back as deeply as they want.

So, our technology brings back not just trust into our society; it also delivers full transparency.

Are we ready for it? Are we ready to keep our records on the machine of our competitor?

Sounds very strange, but there is one more of the blockchain's important features that helps – security. All transactions are kept not in the databases in the form of files, but each position in the register is encrypted separately in a very secure form, so there is no way that we can disclose the entire file of data. The worst case is that details of one particular transaction can be revealed. That makes most of the efforts worthless, as the energy spent on the decryption of several records (and first of all finding them in the right blocks) is going to cost more than potential gain.

All of those virtues from the "old school" bookkeeping requirements remain. Transactions cannot be overwritten in any form. Corrections of transactions can move them forward only and all of these with the full record. We register only facts of the contracts that are having effect on our assets. The concept of distributed ledger can also be used for more than bookkeeping purposes. If this mechanism can store the full record of ownership for cryptocurrencies, it can also be used as a register of ownership or other right to any assets or IP. We can keep a record of real estate ownership, arts including music or any other intellectual rights. All of these with the security, integrity and transparency as mentioned above.

This is not just theory. The full concept described by Satoshi Nakamoto was implemented in the form of open-source code to support Bitcoin. That cryptocurrency has existed for many years now, and in practice proves that all the ideas are possible to implement in real business activity. Many bitcoin owners are making transactions daily without knowing their counterparties. Satoshi Nakamoto created an idea that works.

But do we understand how?

How that works (without the technology) – the magic pen

Let's imagine two people living in two different places in the world. They do not know each other. One day one of them decides to make a transaction. In order to do they both get the "magic pen".

This pen has two functionalities. The first one demonstrates the way this pen has been constructed, with all the complexity of the "magic". This magic consists of the cryptology, the way the writing is organized, how whatever is written by this pen is secure, irreplaceable and written forever, and how we will know who was using the magic pen and when. The user of the pen does not need to know about that. The importance is that the magic pen works.

The second side of this magic pen demonstrates the "ability" of the pen. In short, what anybody who has access to it can do with it.

- the magic pen never stop writing, it always has an ink, 24h/365 days,
- since it is used by many people, in practice it is used to write "sentences" – one by one,
- those "sentences" are recorded according to time,

- every "sentence" is linked with previous one,
- the logical link between "sentences" cannot be broken, replaced or change,
- in order to correct a "previous sentence" one would have to write a new one,
- the fact that "a sentence" has been written is known to everybody who is using the magic pen,
- this pen can be used to write the proof that two completely unknown people can make a transaction, can exchange assets.

This magic pen can drive us to envision a "global logical ledger"

(Blockchain-DLT) where all economic actors will interact and which will allow any parties to record and manage agreements amongst themselves in a secure, consistent, reliable, private and authoritative manner.

Distributed ledger technology (DLT) is a more general name for the blockchain technology. The blockchain was developed as part of cryptocurrency Bitcoin as a way for it to circumvent central banks. The technology uses complex cryptography and the wisdom of the crowd to verify transactions, rather than a traditional middleman. Records are shared across multiple servers and must be checked against each other, rather than a central ledger. It represents a major change in using technology since:

It's shared
A blockchain's value is directly linked to the number of organizations or companies that participate in it. There is huge value for even the fiercest of competitors to participate with each other in these shared database implementations.

It's secure
The blockchain uses cryptography to create transactions that are impervious to fraud and establishes a shared truth.

It's fixed
The database can only be appended – not modified – so it is an immutable record of every transaction that has occured.

It's distributed
There are many replicas of the blockchain database. In fact, the more replicas there are the more trustworthy it becomes.

Exporting a rose from Kenya

The Netherlands imports the majority of flowers to Europe. A major flower market in Amsterdam trades 95% of African roses. Those are coming from Ethiopia, Zimbabwe, Uganda or Zambia, with half of them from Kenya. The shipment of those flowers is very simple. Loaded in planes they travel to Amsterdam only to be traded, repackaged and travel again, this time in cooled trucks to the next step – wholesale warehouses. The final step takes them finally to the flower shop. The average price for a rose in the Eurozone is 4 Euro, while the African producer gets 8–12 Euro cent per rose. That simple example

shows how distribution works today and how it is completely dependent on middlemen. DLT and the Internet has a chance to change that dramatically and move the world to an Internet of Value. In the future, the economy might work differently with many fewer intermediaries. Let us then compare how a letter of credit will work in a scenario today and in the future with DLT.

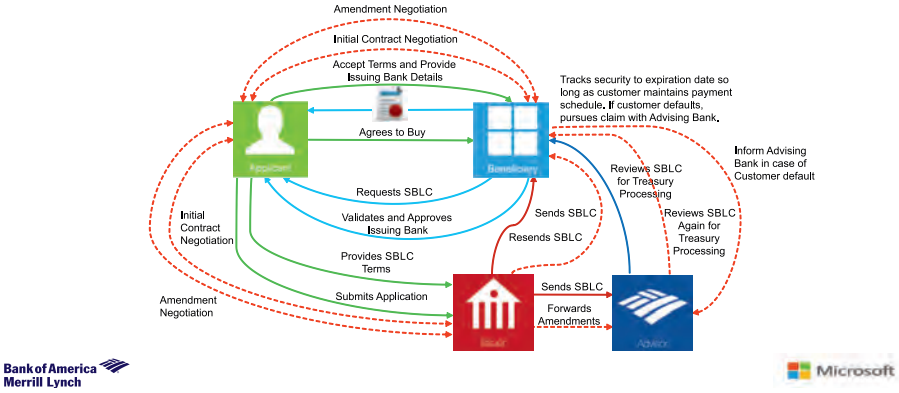
The present and the future: a standing letter of credit

Trade finance processes are typically time and labor intensive, involving multiple documents and checks to reduce the risk and provide assurance to sellers, buyers and their banks. A letter of credit (LC), or documentary credit, is essentially a guarantee provided by a bank that a seller will receive payment from a buyer once certain conditions are met; for example, once the seller can provide proof that they have shipped the buyer's goods. Blockchain technologies that are centered around the trade of financial assets are potentially the most interesting category for the transaction banking and payments domain, both for processes within and between organizations. One of the main benefits of blockchain technology comes from being able to speed up processes and reduce the transaction complexity and risk.

The standard process works like this:

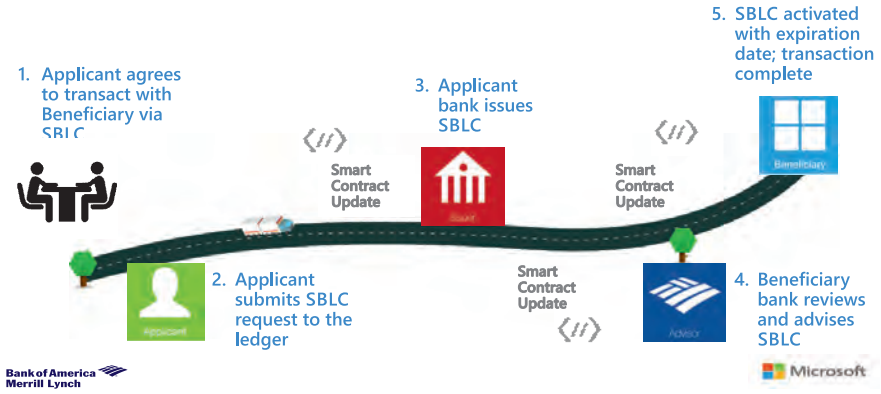
1. The Seller and Buyer make a deal (perhaps the Seller is an exporter and the Buyer wants him to ship 10,000 red roses on open credit).
2. The Buyer does not want to take the risk of the Seller failing to deliver on his promises, so she asks the Seller to obtain a letter of credit as part of their agreement.
3. The Seller asks his bank for a standby letter of credit. Because he has sufficient credit and collateral, the bank issues the letter.
4. The Seller's bank sends the letter to the Buyer's bank.
5. The Buyer reviews the letter of credit to make sure it is acceptable and decides that it is.
6. If the Seller fails to meet his obligations, the Buyer submits the documentation to the Seller's bank as required by the letter of credit (possibly using her bank or other banks as intermediaries).
7. The Seller's bank pays the Buyer (again, possibly indirectly), and the Seller will have to repay his bank.

Standby Letter of Credit (SBLC) - Current State Overview



Source: Microsoft/BOA Merrill Lynch

SBLC New Process Flow - Distributed Ledger



Source: Microsoft/BOA Merrill Lynch

The new process is much simpler and with additional functionality represented by "Smart contracts", even more safe. Smart contracts – software attached to the DLT transaction and acting based on certain events – may foresee the most transformative application at the moment. Smart contracts can

automate payments or the transfer of currency or assets if negotiated conditions are met. A firm could signal via blockchain that goods have been received or the shipment could have GPS functionality which would automatically log a location update that, in turn, triggered a payment.

The implications are fascinating. Firms are acting and exchanging based on contracts, from buyer-supplier relationships to employee relations.

Bank of America Merrill Lynch and Microsoft Treasury announced a collaboration using blockchain technology that aims to transform Trade Finance business processes. Commonwealth Bank of Australia (CBA), Wells Fargo and trading firm Brighann Cotton have completed the "first" global trade transaction between two banks using blockchain, smart contracts and the Internet of Things (IoT). The transaction involved a shipment of cotton from Texas to Qingdao, China, using a distributed ledger. The trade involved an open account transaction, mirroring a letter of credit, executed through a collaborative workflow on a private distributed ledger between the seller (Brighann Cotton in the US), the buyer (Brighann Cotton Marketing Australia), and their respective banks (Wells Fargo and CBA).

Five examples from last year from the blockchain world (PoC)

Fidor Bank

German online bank Fidor was one of the first to try new blockchain technology – but after efforts in 2014, when the Bank formed a consortium and ran several proofs of concept to integrate Ripple, things became a little quiet, but then in 2016, Fidor revealed its plans to replace its core banking system with the new design, built on blockchain technology. The Bank foresees an Ethereum based blockchain solution replacing low-level banking systems. In the prototype, accounts were built to store balances, overdrafts, AML checks etc. The new ledger holds all account information and ensure users have the necessary funds to execute transactions.

SWIFT

Global payment servicing organization SWIFT has set up a team of experts from its standards team – security experts, architects, developers and more – to work on two active proofs of concepts.

The first is a standing settlement instructions blockchain, but it is the

second that is supposed to form a unique solution – an attempt to implement the ISO 20022 standard on a blockchain. The PoC is designed to allow smart contracts written in Solidity, a high-level programming language created for Ethereum.

The first goal was to assess how many of the existing standards could be used on a blockchain and whether transaction data could be stored directly on the distributed ledger and how smart contracts might be implemented.

The second was to build a real use case on how the distributed ledger might help banks to serve their customers. They built the complete lifecycle of a short term, fixed rate corporate bond into the open-source Eris technology. The use of that particular platform was driven by the need to provide a permissioned blockchain solution that is able to support smart contracts with much faster consensus algorithm than Bitcoin's proof-of-work.

In April 2016, SWIFT published a report listing "critical factors" that need to be addressed prior to adoption of distributed ledger technology. Among them there is a need to improve governance when things go wrong, compliance with regulatory requirements, and scalability.

Standard Chartered

Standard Chartered, in cooperation with Development Bank of Singapore, has set up a project to tackle the trade finance process with the new technology. Both parties are working on improving bills of lading (BLs) – documents issued by carriers that specify what is contained in a specific shipment and then transfer the title to those goods to receiving party.

The real problem to be solved here is to improve the bank's ability to detect duplicate financing of the same set of invoices or BL. Unfortunately, today it is common that customers are able to obtain financing from multiple banks for the same invoices. A consortium of Standard Chartered and Development Bank of Singapore decided to use for their PoC a technology delivered by Ripple. Currently the consortium is looking for more banks to join.

Deutsche Borse

Deutsche Borse has unveiled a blockchain proof-of-concept focused on commercial bank cash transfers. The project is designed in cooperation with Eurex Clearing. Using the Hyperledger Fabric project's code, the firm is seeking patent approval for its transfer solution.

The main principle of the project is that all peer-to-peer payments based on tokenized commercial bank money are accompanied by movements of collateral between the respective EurexClearing members using the central counter party's functionality and rules.

Digital Trade Chain (DTC) by KBC

The initiative was derived from of an earlier proof-of-concept delivered by KBC Bank and first unveiled in July of last year.

Those backing the platform's development are looking to establish a secure place to manage open account trade transactions for both domestic and international commerce. DTC utilizes a permissioned DLT, with authorized parties allowed to submit transactions on the platform.

Open account trade transactions can involve products being shipped before the actual payment is due, meaning that trust among the transaction's parties is imperative. With DTC, those plugged into the system will be able to track the progression of those transactions, from initiation to settlement.

Banks involved – KBC, Deutsche Bank, HSBC, Natixis, Rabobank, Société Générale and UniCredit – have signed a memorandum of understanding that lays out the basic groundwork to launch DTC sometime in 2017 in markets like France, Germany and the UK.

What are the challenges with commercial implementation of blockchain technology?

Blockchains derive their value from the extent of participation in them. This is nothing new to scholars of network economics, where, in simple terms, the value of the network depends on the number of nodes participating in it. The more people who use Facebook, the more valuable the network becomes, and the harder it becomes for another network to compete in the absence of more participants (Google+ anyone?). If you would like to set up a private blockchain, it may be a lot easier to set up a traditional, private database with timestamps instead.

If the new technology is so ingenious, why is the world still in the early stage of PoC projects? Why does it seem that we are much closer to having driverless cars than many different purpose distributed ledgers – despite driverless cars seeming to be less important than the creation of a trustworthy platform for global business?

The answer is simple – there are still challenges to be solved.

The original implementation of a blockchain, being present for nearly ten years, might be considered as an already matured technology, but this initial version of the protocol is difficult for mass commercial implementation. The issue lays in the cost of delivering trust. To make sure that honesty is rewarded properly and dishonesty is not productive, the algorithm consumes electrical energy. A lot of it. Estimations differ but it is said that for a block of one million transactions, there is a need for power consumption worth almost 1 million USD. There is a certain mechanism in Bitcoin to compensate that cost, but it seems to be difficult to adopt this mechanism in other business models.

To overcome such a challenge there are projects to create different platforms with different consensus models. The most promising one is Ethereum, which is intensively testing how to replace the proof-of-work concept with proof-of-stake, but as a result of those inventions we are getting less mature versions of distributed ledger implementations. These are not tested yet even in the Bitcoin scale. One has to also remember that less energy expended means less trust delivered. It seems to be easier (and definitely cheaper) to cheat in the proof-of-stake environment than with proof-of-work, so there is a next question – how to keep the balance between cost and level of trust delivered by a platform?

To start thinking about using new protocols one needs more than just theoretical proofs of concept, but there is a need for the involvement of many players (companies and organizations) in most of the problem-solving solutions where the distributed ledger concept might be used. A typical example for the potential use of a distributed ledger would be for cross-border payments. If the banks desired to replace the current expensive and time consuming process with the new one, based on blockchain technology, it would require the involvement of many entities (banks) in many countries. One should also think about international organizations as SWIFT. Are we going to replace them or are we going to reform them? This way or another it seems that we have a large international project in front of us – and all of this on new and not fully matured technology, where so far one can see only theoretical proofs of concept. Sounds like a risk, doesn't it?

If we think a little more about our cross-border payments example, one might see that there is a need to establish international cooperation of several entities. But to make such cooperation possible there is a need for some legal

framework. Here we have another weak point. So far, legislation regarding new technologies has often been ill-suited and old-fashioned. How to legally treat transactions agreed between two parties based on social consensus? Do we have any possibility to act in case of failing to fulfill contract obligations by any of the counterparties? There are several such questions that are creating real concerns for everyone planning to get into the distributed ledger project.

Although the technology is not in practical use in the financial sector, already one might see that regulators have picked up on the subject. There is concern expressed in several papers published already that the new platform is not secure enough. Furthermore, some of the issues raised in those documents are attacking the blockchain principles. For example, in the document "Distributed ledger technology & cybersecurity. Improving information security in the financial sector", published by ENISA in January 2017, among other concerns, we can find the requirement to implement "the right to be forgotten". The authors of the report are saying: "The right to be forgotten where information needs to be removed from a ledger is challenging to implement". Just this little example shows how difficult it is going to be to fulfill all the requirements of different regulators.

All the things mentioned above are the real challenges. Thinking about all the positive aspects of new technology, and potential cost savings, one should also remember that there are still areas of uncertainty, but that should not stop us from actively searching for effective solutions.

Summary

Many financial institutions don't know where or how to start. In 2017 we will continue to see blockchain (DLT) experimentation and we will, for a variety of reasons, see the rise and fall of blockchain consortiums and mutual agreements. Nevertheless, the appetite for DLT and banks working together will accelerate and leverage blockchain. Banks will run proof of concepts or controlled pilot programs for internal and new possibilities outside the banking industry. The biggest challenge facing the industry today is standardization. There is sort of race to provide solutions with the acceptance of the ideas. DLT has captured vigorously the imagination of financial sector, but as Marco Iansiti and Karim R. Lakhami (2) notice:

"Blockchain is a foundational technology: It has the potential to create new foundations for our economic and social systems. But while the impact will be enormous, it will take decades for blockchain to seep into our economic and social infrastructure. The process of adoption will be gradual and steady, not sudden, as waves of technological and institutional change gain momentum."

Bibliography

1. CBA and Wells Fargo in "world-first" interbank blockchain trade transaction, 25 October, 2016 Written by Antony Peyton (http://www.bankingtech.com/621602/cba-and-wells-fargo-in-world-first-interbank-blockchain-trade-transaction/)
2. Insiti M. Lahami K.R.HBR , Jan-Feb 2017, The truth about blockchain.
3. http://www.coindesk.com/digital-trade-chain-banks-blockchain-2017/
4. The Future of financial infrastructure , WEF, August 2016
5. Distributed Ledger Technology & Cybersecurity, ENISA, December 2016
6. Tapscott D.,Tapscott A. The impact of the blockchain goes behind Financial Services , HBR, May 2016
7. Nakamoto S., Bitcoin: A Peer-to-Peer Electronic Cash System, atoshin@gmx.com., www.bitcoin.org
8. Yermack D., Corporate Governance and blockchain, http://www.nber.org/papers/w21802 , National Bureau of Economics Research, December 2015
9. Walport M., Distributed Ledger Technology: beyond block chain, UK Government Chief Scientific Adviser, December 2015

Robert Trętowski
Wiceprezes Zarządu KIR, odpowiedzialny za Obszar Rozwoju Systemów i Sektor Publiczny

W latach 2011–2016 pełnił funkcję Dyrektora Departamentu Inicjatyw Informatycznych i Testów w PKO Banku Polskim S.A., gdzie odpowiadał m.in. za analizę, monitorowanie i zarządzanie portfelem projektów informatycznych. Pełnił kluczową rolę w procesach przejęcia Nordea Bank Polska oraz SKOK Wesoła przez PKO BP S.A. Koordynował prace podczas migracji Inteligo do systemów PKO oraz wdrożenia nowej bankowości elektronicznej dla klientów indywidualnych iPKO oraz korporacyjnych iPKO Biznes. Nadzorował uruchomienie aplikacji IKO dla klientów PKO. Pracował przy powołaniu spółki Polski Standard Płatności i budowie standardu BLIK, zasiadając w Radzie Nadzorczej Spółki. Współpracował przy rozwoju oferty kartowej, alternatywnych metod płatności oraz wdrożeniach programu Rodzina 500+, integracji banków z ZUS oraz z Profilem Zaufanym ePUAP. Był także Członkiem Komitetu Architektury i Bezpieczeństwa PKO Banku Polskiego.
W okresie 2002–2011 w BRE Bank S.A. na stanowisku Dyrektora Biura Bankowości Elektronicznej odpowiadał m.in. za realizację iBRE Banking, Cards, Cash, Invoice.net, Connect, Trade Finance, strefę sprzedażową oraz migrację klientów z Dresdner Bank Polska do BRE Banku S.A. Zarządzał usługami IT świadczonymi dla korporacji oraz portfelem projektów IT.
Kieruje Zespołem Roboczym eID Rady Bankowości Elektronicznej Związku Banków Polskich.
Absolwent Wydziału Nauk Ekonomicznych Uniwersytetu Warszawskiego.

Robert Trętowski
Wiceprezes Zarządu KIR

Bankowe okno na świat – „jedno okienko" dla obywatela

Bankowość internetowa jest w Polsce rozpowszechniona podobnie jak Facebook. Według danych z początku 2015 r. mieliśmy w Polsce 13,5 mln aktywnych kont na Facebooku[1], natomiast według danych z końca 2015 r. było ich aż 20,1 mln[2]. Z kolei według danych Infosocialmedia za sierpień 2016 r. aktywnych użytkowników Facebooka było ok. 14 mln. Dla porównania w bankowości – klientów z dostępem internetowym do rachunków bankowych według Raportu NetB@nk ZBP[3] na koniec Q3 2016 było ponad 33 mln, z czego 15,3 mln aktywnych (wśród indywidualnych klientów). Do tej liczby należy dodać 2,43 mln MSP, z czego aktywnych użytkowników bankowości internetowej wśród MSP mamy 1,37 mln. Można zatem przyjąć, że w sumie aktywnych użytkowników bankowości elektronicznej jest nawet więcej niż aktywnych użytkowników Facebooka. Natomiast pod względem bezpieczeństwa i pewności tożsamości użytkowników tych serwisów są to kwestie nieporównywalne. W tym kontekście warto też podsumować liczbę wykorzystywanych podpisów elektronicznych, których nadal mamy poniżej 400 tysięcy na całym rynku.

1 http://socialpress.pl/2015/03/facebookowi-przybylo-w-polsce-ponad-1-mln-uzytkownikow/

2 http://antyweb.pl/gemius-kto-w-polsce-korzysta-z-facebooka-i-twittera/

3 https://zbp.pl/wydarzenia/archiwum/konferencje-prasowe/2017/styczen/raport-netb-nk-polacy-maja-juz-33-mln-rachunkow-bankowych-dostepnych-przez-internet

Branża finansowa i bankowa rozwija się szybko, ale już dziś można przewidywać, jak będzie wyglądać relatywnie bliska przyszłość instytucji finansowych. Eksperci zgadzają się, że zmiany pójdą w kierunku maksymalnego uproszczenia metod płatności, przyspieszenia rozliczeń, rozwiązań mobilnych i multikanałowych procesów cyfrowych. Szybkie tempo rozwoju i rozpowszechniania się w Polsce nowoczesnych usług w obszarze finansów i płatności świadczy o tym, że w Europie należymy do ich największych entuzjastów, a czasami nawet prekursorów. Dobrą ilustracją jest bankowość mobilna, której liczba aktywnych użytkowników na koniec 2016 roku wzrosła do blisko 7,7 mln osób – o dwa miliony przewyższając wartości z analogicznego okresu roku 2015[4]. Przechodzenie klientów banków ze sfery płatności on-line do sfery płatności mobilnych jest jednym z ważniejszych trendów kształtujących przyszłość bankowości. Według niektórych szacunków[5], do 2020 roku ponad połowa wszystkich transakcji bezgotówkowych w Europie będzie dokonywana za pomocą urządzeń przenośnych. Można się spodziewać, że zjawisko to będzie szczególnie widoczne w Polsce, zwłaszcza że już mamy dynamicznie rozwijający się system BLIK. Już teraz ponad 60 proc. konsumentów chciałoby móc płacić w sklepie przy pomocy smartfona, a dwie trzecie Polaków przewiduje, że do 2020 r. co najmniej raz w tygodniu wykona płatność mobilnie[6].

4 http://prnews.pl/raporty/raport-prnewspl-rynek-bankowosci-mobilnej-iv-kw-2016-6553798.html

5 https://www.visa.pl/o-nas/aktualnosci/polska-gotowa-na-platnosci-mobilne-1244053?returnUrl=/o-nas/aktualnosci/listing?tag=hce

6 https://www.visa.pl/o-nas/aktualnosci/polska-gotowa-na-platnosci-mobilne-1244053?returnUrl=/o-nas/aktualnosci/listing?tag=hce

Aspekt **'Paperless'** przewiduje, że w ciągu 5 lat połowa obywateli będzie załatwiała **80%** swoich spraw przez internet, a **'Cashless'**, że w tym czasie udział gotówki spadnie z obecnego poziomu **21,5%** do **~15%**.

Standardem staje się też przesyłanie pieniędzy na numer telefonu. Kluczową zaletą takich płatności jest wygoda wynikająca z faktu, że do zlecenia przelewu nie trzeba pamiętać ani wpisywać 26-cyfrowego numeru rachunku bankowego. Transakcje inicjowane przez BLIK rozliczane są w obsługiwanym przez KIR systemie przelewów natychmiastowych Express Elixir. Dzięki temu przelew trafia do odbiorcy w czasie liczonym w sekundach, także w dni standardowo wolne od pracy i w święta. Nie można przy tym również nie wspomnieć o ogromnej popularności kart zbliżeniowych – już dwie trzecie Polaków płaci tą metodą[7], a, jak wynika z danych NBP na koniec września ub.r., rodzimi konsumenci mieli w portfelach 28 mln takich kart[8], jednocześnie już ponad 90% terminali POS akceptuje płatności zbliżeniowe, a 77% płatności mobilne.

Wiele wskazuje na to, że w przyszłości nie będziemy musieli pamiętać również naszych numerów PIN. Ponad dwie trzecie (68 proc.) konsumentów w całej Europie pozytywnie odnosi się do biometrii[9] jako metody uwierzytelniania transakcji, a nawet metody płatności[10]. W deklaracjach konsumentów, co do zaufania przypisywanego poszczególnym metodom, przoduje weryfikacja linii papilarnych (81%) i skanowanie obrazu tęczówki oka (76%). Już teraz funkcjonuje w Polsce około tysiąca bankomatów, które identyfikują posiadaczy karty na podstawie wzorca naczyń krwionośnych palca[11].

Dzięki wykorzystaniu mechanizmów uwierzytelniania w bankowości internetowej, uzyskujemy efekt „jednego okienka" umożliwiającego łatwy i bezpieczny dostęp do usług komercyjnych i bankowych, dodatkowo poszerzony

7 https://www.visa.pl/o-nas/aktualnosci/gotowka-odchodzi-w-przeszlosc-1703662?returnUrl=/o-nas/aktualnosci/index; http://newsroom.mastercard.com/eu/pl/press-releases/mastercard-2016-przelomowym-rokiem-w-rozwoju-platnosci-cyfrowych-w-polsce/

8 http://www.nbp.pl/systemplatniczy/karty/q_03_2016.pdf, s. 10

9 http://prnews.pl/wiadomosci/europejscy-konsumenci-gotowi-do-korzystania-z-biometrii-przy-uwierzytelnianiu-platnosci-3562061.html

10 http://www.cashless.pl/felietony/2255-nie-tylko-bez-karty-ale-i-bez-smartfona-oraz-terminala-tak-bedziecie-placic-w-przyszlosci-oto-fingopay

11 http://www.cashless.pl/temat-dnia/1338-czy-to-bedzie-finger-vein-reaktywacja-chca-rejestrowac-dane-biometryczne-w-bankomatach

o aspekt zarządzania procesami dotyczącymi każdego klienta banku – zarówno osób fizycznych, jak i podmiotów prawnych. Umożliwienie klientowi banku funkcjonowania w relacji z administracją państwową i podmiotami komercyjnymi, np. dostawcami usług typu telekomunikacja czy prąd, w trybie online wiąże się z konkretnymi korzyściami, w tym z realną oszczędnością czasu. Przykładowo, w przypadku zakładania nowej firmy, kolejne etapy uruchamiania działalności gospodarczej, oprócz pokonania standardowej ścieżki postępowania administracyjnego i uruchomienia rachunku bankowego, obejmują wiele punktów wymagających bieżącego zarządzania (m.in. wynajem przestrzeni biurowej, procesowanie umów związanych z regularnymi opłatami eksploatacyjnymi, współpraca z dostawcami usług, etc.). Usprawnienie relacji biznesowych między podmiotami komercyjnymi, dzięki zapewnieniu weryfikacji tożsamości w oparciu o uwierzytelnianie użytkowników na poziomie banku, przyczynia się do urzeczywistniania idei cyfrowej gospodarki.

Kwestie bezpiecznych i niezawodnych narzędzi potwierdzania tożsamości blisko wiążą się z przyszłością e-administracji – szczególnie w kontekście procesów uzyskiwania zdalnego dostępu do zasobów w relacji państwo-obywatel. Rządowy program „Od papierowej do cyfrowej Polski" zakłada, że w stosunkowo krótkim czasie połowa Polaków będzie załatwiać 80 proc. swoich spraw przez Internet. Co więcej na koniec 2017 r. rząd planuje wdrożyć kolejne usługi publiczne dla obywateli i biznesu w cyfrowej, ergonomicznej i bezpiecznej formule. Tak ambitnie zarysowane plany wymagają zbudowania kompleksowych i wygodnych dla użytkownika rozwiązań w krótkim czasie, stąd optymalnym wyborem jest wykorzystanie już istniejących narzędzi. Naturalnym i już sprawdzonym partnerem administracji w tych przedsięwzięciach wydają się, jako instytucje zaufania publicznego, podmioty funkcjonujące w ramach sektora bankowego. Dobrym przykładem jest KIR, odpowiadający w ramach swojej podstawowej działalności za sprawne i niezawodne rozliczenia międzybankowe, ale również dysponujący narzędziami pozwalającymi wesprzeć lub uruchomić procesy związane z rozwojem polskiej e-administracji oraz odpowiednim doświadczeniem i kompetencjami, aby efektywnie tworzyć i wdrażać nowe rozwiązania na styku administracji i sektora bankowego.

Wśród usług KIR znajduje się m.in. kwalifikowany podpis elektroniczny, który uwierzytelnia użytkownika w sposób wiążący prawnie, identycznie jak w przypadku odręcznego podpisu. E-podpis, eliminując konieczność

osobistej wizyty w urzędzie, stanowi ważną składową sprawnego funkcjonowania e-administracji i wpisuje się w założenia rządowego programu „Od papierowej do cyfrowej Polski". Z kolei usługa Invoobill 2.0 (Qlik), udostępniana w bankowości elektronicznej, może być doskonałą platformą do kontaktu między obywatelami a państwem. Już w tej chwili system umożliwia sprawne regulowanie opłat za prąd, gaz czy telefon komórkowy prosto z e-konta bankowego, a w przyszłości może zapewnić także łatwy dostęp do usług publicznych.

Jednym z warunków koniecznych dla urzeczywistniania nowoczesnego modelu administracji jest usprawnianie procesu dokonywania opłat w urzędach przez obywateli. Według założeń programu „Od papierowej do cyfrowej Polski", docelowo w każdym urzędzie będzie można płacić bezgotówkowo. Już teraz KIR, wraz z bankami i PSP, umożliwia dokonywanie w urzędach opłat przy pomocy systemu BLIK oraz PeoPay, udostępniając specjalną aplikację w systemie płatności internetowych Paybynet. Dzięki usłudze WebPOS Paybynet szybciej i wygodniej zapłacimy np. za wydanie prawa jazdy lub rejestrację pojazdu, ponieważ opłata skarbowa może zostać wniesiona bezpośrednio w okienku urzędnika i nie wymaga wizyty w kasie. Co więcej, techniczne wdrożenie tego rozwiązania w urzędzie jest niemalże bezkosztowe, a jedynym wymogiem w zakresie sprzętu jest komputer z dostępem do Internetu, co w jednostkach administracji jest praktycznie krajowym standardem.

Określając zakres dostępnych rozwiązań i rzeczywistego wykorzystania nowoczesnych usług w e-gospodarce, warto także wspomnieć o znaczeniu upowszechniania płatności natychmiastowych na rzecz administracji (ZUS, organy podatkowe i celne). Przelewy realizowane w czasie liczonym w sekundach przyspieszają obrót pieniądza w gospodarce, przyczyniają się do równoważenia relacji między stronami w kontaktach biznesowych, uatrakcyjniają ofertę banków w obszarze płatności, ale są także przykładem wprowadzania do administracji innowacyjnych rozwiązań usprawniających jej funkcjonowanie.

W kontekście charakterystycznego dla Polski cyfrowego zaawansowania sektora bankowego, zarówno pod względem modelu funkcjonowania banków jak i przygotowania klientów do sprawnego adoptowania innowacyjnych rozwiązań, współpraca z bankami może pozytywnie wpłynąć na tempo i jakość cyfryzacji procesów gospodarczych. Posłużenie się ekspertyzą sektora bankowego może wszystkim zaangażowanym stronom przynieść konkretne

korzyści, dalece wykraczające poza oszczędność czasu i poprawę komfortu. Przykładowo:

- **klienci** – korzystają z optymalizacji i przyspieszenia procesów, uzyskują atrakcyjniejsze oferty dzięki niższym cenom,
- **administracja** – osiąga redukcję pracochłonności, poprawę bezpieczeństwa i efektywności, wdraża nowoczesne rozwiązania przynoszące korzyści wizerunkowe, zwiększa wygodę klientów pozycjonując urzędy jako miejsca przyjazne i wrażliwe na potrzeby lokalnych społeczności,
- **przedsiębiorcy** – poprawiają rentowność dzięki optymalizacji procesów biznesowych, uzyskują łatwiejszy i wygodniejszy dostęp do usług, redukują koszty związane z działalnością operacyjną,
- **banki** – udostępniając instrumenty bankowe w celu uwierzytelniania i potwierdzania tożsamości, umacniają pozycję zaufanego partnera klientów i administracji, wspierając cyfryzację procesów gospodarczych przyczyniają się do usprawniania procesów bankowych, budują własną konkurencyjność i silną pozycję rynkową.

Niebagatelną korzyścią ogólną jest w tej sytuacji także wzrost kapitału zaufania społecznego uzyskiwany dzięki znaczącym ułatwieniom, udostępnianym w całkowicie bezpiecznym środowisku, co z kolei przekłada się na optymalizację kosztów w skali makro, poprawę konkurencyjności polskich rozwiązań i procesów oraz wzrost przedsiębiorczości – czyli wymierne korzyści dla polskiej gospodarki i przedsiębiorczości.

Program „Od papierowej do cyfrowej Polski" a sektor bankowy

Rządowy program „Od papierowej do cyfrowej Polski" (Paperless, Cashless Poland) dotyka szeregu konkretnych obszarów – m.in. obejmuje: cyfrowe usługi publiczne, eID, cyberbezpieczeństwo. Aspekt „paperless" przewiduje, że w ciągu pięciu lat połowa obywateli będzie załatwiała 80% swoich spraw przez Internet, a „cashless", że w tym czasie udział gotówki spadnie z obecnego poziomu 21,5% do ~15%[12]

12 https://mc.gov.pl/files/prezentacja_programu_od_papierowej_do_cyfrowej_polski_-_wersja_skrocona.pdf

Zakładając zwiększenie obrotu bezgotówkowego jako narzędzia wskazano e-Fakturę, e-Paragon, e-Zdrowie, e-Daniny i e-Świadczenia. We wszystkich tych obszarach warto uwzględnić wykorzystanie – charakterystycznego dla Polski – wysokiego poziomu ubankowienia i możliwość zacieśnienia współpracy administracji z sektorem bankowym.

Pierwszym przykładem dowodzącym słuszności powyższego założenia jest sukces współpracy kanału bankowego z administracją publiczną przy okazji wdrażania programu Rodzina 500+, w ramach którego ok. 95% wniosków wypełnionych w trybie online zostało złożonych za pośrednictwem banków. Był to dla sektora bardzo wymagający projekt, zrealizowany w rekordowo krótkim czasie. Sprawność i niezawodność banków, zweryfikowana w praktyce, pozwala założyć, że w realizacji projektów w środowisku cyfrowym sektor bankowy jest właściwym partnerem dla administracji. Istotną korzyścią z takiej współpracy jest pełna gwarancja bezpieczeństwa procesów, dostarczana przez banki w ramach ich standardu funkcjonowania, także w zakresie potwierdzania tożsamości. Jednocześnie, w kontekście założeń programu „Od papierowej do cyfrowej Polski", można stwierdzić, że sukces projektu Rodzina 500+ wyznaczył kierunek budowy podwalin cyfryzacji procesów gospodarczych i publicznych, tj. uzyskanie optymalizacji w zakresie efektywności podejmowanych działań dzięki wdrożeniu federacyjnego modelu tożsamości. Jest to cenne doświadczenie uzyskane w realiach rynkowych i – także ze względu na to – może być traktowane jako przykład wart naśladowania przy wdrażaniu planowanych zmian. Zwłaszcza, że projekt Rodzina 500+ zrealizowany został w stosunkowo łatwym do replikowania modelu, wykorzystującym istniejący potencjał bazy klientów bankowości elektronicznej i wysokowydajne systemy komunikacji elektronicznej. Dzięki temu możliwe było wypracowanie standardu podłączenia do administracji wielu banków jednocześnie i rozłożenie ruchu internautów na ponad 20 portali, z których każdy jest zarządzany w wysokim reżimie usług komercyjnych.

Założenia strategiczne, przyjęte w ramach programu „Od papierowej do cyfrowej Polski", stworzyły nowe możliwości wykorzystania wysokiego poziomu digitalizacji sektora bankowego. W szerszym kontekście działania wpisujące się w założenia programu prowadzą do upraszczania prawa, przyczyniają się do stymulacji rozwoju gospodarczego i pobudzania innowacyjności. Jednym z zakładanych celów jest zapewnienie obywatelom i przedsiębiorcom szybkich i wygodnych e-usług publicznych oraz przygotowanie narzędzi

informatycznych, pozwalających na obniżenie kosztów funkcjonowania państwa. Przewidziane w ramach programu projekty – m.in. e-tożsamość (eID), zwiększenie obrotu bezgotówkowego, strumień „Cyberbezpieczeństwo" – wiążą się w wielu aspektach z działalnością sektora bankowego, a także z obecnym i perspektywicznym zakresem usług świadczonych przez KIR. Obszarem, na który warto zwrócić szczególną uwagę w kontekście możliwości współpracy administracji i sektora bankowego w Polsce jest e-tożsamość (eID). Projekt uwzględnia wdrożenie – od strony prawnej, organizacyjnej i technicznej – federacyjnego modelu weryfikacji tożsamości, w tym identyfikacji oraz uwierzytelniania.

Dlaczego rozporządzenie eIDAS jest ważne dla polskiej gospodarki, a w szczególności polskiej e-administracji?

Od 1 lipca 2016 r. obowiązują przepisy rozporządzenia eIDAS, tj. Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do e-transakcji na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE. Celem rozporządzenia eIDAS jest zwiększenie zaufania do transakcji elektronicznych poprzez zapewnienie wspólnej podstawy interakcji elektronicznej pomiędzy przedsiębiorstwami, obywatelami i organami publicznymi, co ma podnieść skuteczność publicznych i prywatnych usług internetowych, e-biznesu czy handlu elektronicznego w Unii Europejskiej oraz ułatwić korzystanie z usług internetowych o charakterze transgranicznym. Rozporządzenie eIDAS wprowadza narzędzia wspierające realizację tego celu: środek identyfikacji elektronicznej, pieczęć elektroniczną, znakowanie czasem, certyfikaty dla stron www czy też usługi rejestrowanego doręczenia elektronicznego. Stąd przy tworzeniu nowych publicznych systemów teleinformatycznych przeznaczonych do świadczenia usług elektronicznych lub dostosowaniu dotychczas istniejących, konieczne będzie uwzględnianie uznawania i obsługi środków identyfikacji elektronicznej osób fizycznych i prawnych, objętych tzw. notyfikowanymi systemami identyfikacji elektronicznej z innych państw członkowskich UE. Obsługa zagranicznych środków identyfikacji będzie realizowana z wykorzystaniem przygotowywanych, celem udostępnienia w Internecie, węzłów identyfikacji eIDAS.

Ministerstwo Cyfryzacji planuje budowę takiego węzła krajowego i węzła transgranicznego do usług publicznych, nie ma natomiast planów objęcia tym

projektem usług komercyjnych, które byłyby pożądaną ofertą komplementarną. Tworzy to możliwość uzupełnienia oferty usług identyfikacji i usług zaufania, dostarczanych na zasadach komercyjnych, przez podmioty z sektora bankowego. W tym aspekcie szczególnie atrakcyjne dla rynku może być wykorzystanie kompetencji KIR w zakresie świadczenia usług identyfikacji i zaufania do tworzenia i propagowania, wspólnie z sektorem bankowym, dobrych praktyk w zakresie uwierzytelnia klientów przy wykorzystaniu bankowych środków identyfikacji. Korzyści, wynikające ze zmiany regulacji i powstania nowych rozwiązań, może w tym scenariuszu odnieść zarówno administracja – dzięki temu, że więcej odpowiednio zabezpieczonych dokumentów będzie wpływać w postaci elektronicznej, jak i przedsiębiorcy. Każdy kontakt z urzędem czy z innym przedsiębiorcą w formie elektronicznej przekłada się na oszczędność czasu, a uzyskiwany komfort jest w tym przypadku dodatkowo opatrzony gwarancją bezpieczeństwa. Zatem, jeśli rozporządzenie eIDAS uznamy za legislacyjne rusztowanie dla procesów cyfryzacji, to KIR – realizując strategię cyfrowego przyspieszenia – może pełnić funkcję partnera dostarczającego konkretnych elementów konstrukcyjnych dla gospodarki cyfrowej i cyfrowej administracji.

Na bazie dotychczasowej roli konsolidacyjnej w kontekście usług świadczonych dla sektora bankowego – m.in. w zakresie rozliczeń transakcji międzybankowych – usytuowanie komercyjnego węzła tożsamości eID przy KIR pozwoli sektorowi bankowemu na przyjęcie roli komercyjnego dostawcy tożsamości dla biznesu i dla administracji publicznej. Będzie to podstawą umożliwiającą budowanie rozwiązań dostępu do krajowych i zagranicznych usług cyfrowych za pomocą dostarczanych w sektorze bankowym bezpiecznych i sprawdzonych metod uwierzytelniania. Wykorzystanie w tym projekcie KIR jako integratora pozwoli na redukcję kosztów budowy rozwiązana w sektorze bankowym oraz umożliwi m.in. tworzenie rozwiązań sektorowych odpowiadających na nowe wyzwania rynkowe – czy to działania globalnych graczy, czy też regulacje typu PSD II, AIS, PIS. Współpraca KIR z sektorem bankowym w celu wykreowania oferty w zakresie eIDAS stwarza możliwość zaoferowania przez sektor bankowy nowego obszaru usług cyfrowych, jak: uwierzytelnienie i identyfikacja (tożsamość cyfrowa) oraz usługi zaufania (podpis elektroniczny, znakowanie czasem), a także elektroniczna archiwizacja. KIR jest optymalnym partnerem technologicznym do realizacji tego typu inicjatywy, ponieważ może zaproponować bankom atrakcyjny model wdrożenia

i utrzymywania węzła identyfikacji, pod względem biznesowym i technologicznym. Środek identyfikacji elektronicznej oparty o dane bankowe polega na użyciu danych służących do logowania i autoryzacji przelewów w bankowości elektronicznej do bezpiecznego zidentyfikowania się przy korzystaniu z cyfrowych usług pozabankowych. Użytkownik dzięki temu uzyska dostęp np. do administracji publicznej, dostawcy mediów, sklepów internetowych itp. Można w skrócie opisać tą usługę jak „loguj się z bankiem".

Węzeł eID daje także możliwość redefinicji modelu świadczenia nowoczesnych usług podpisu elektronicznego, tj. zarządzania danymi do składania podpisów (kluczami prywatnymi) poprzez kwalifikowany podmiot świadczący usługi zaufania. W praktyce oznacza to możliwość zastąpienia karty kryptograficznej, jaką obecnie posługują się użytkownicy składający kwalifikowany podpis elektroniczny, przechowywaniem kluczy w modułach kryptograficznych, zarządzanych przez kwalifikowany podmiot. Przy czym należy zauważyć, że dla tego stosunkowo nowego narzędzia wciąż brak norm technicznych regulujących świadczenie usług (wydanie ich jest przewidziane na koniec 2017 roku). W konsekwencji brak również gotowych rozwiązań realizujących taką funkcjonalność. Warto jednak zauważyć, że podmioty funkcjonujące na polskim rynku z wyprzedzeniem opracowują rozwiązania prototypowe, przygotowując się na konkurowanie w realiach otwartego rynku, poszerzonego o nowych – także zagranicznych – graczy.

Sektor bankowy – ze względu na obecne mechanizmy zapewniania bezpieczeństwa, weryfikacji tożsamości oraz posiadane zaufanie klientów – jest naturalnym partnerem sektora publicznego, który może efektywnie, zarówno pod względem czasu, jak i nakładów finansowych zainwestować w tożsamość cyfrową zbudowaną na bazie własnych rozwiązań. O potencjale takiego rozwiązania świadczy powodzenie wykorzystania tożsamości bankowych na potrzeby składania wniosków w Programie Rodzina 500+. Kolejnymi etapami były: umożliwienie logowania z poziomu bankowości elektronicznej do portalu PUE-ZUS oraz zakładanie Profilu Zaufanego przy wykorzystaniu tożsamości bankowej.

Profil Zaufany

Profil Zaufany został wdrożony jako metoda potwierdzania tożsamości obywatela Polski w elektronicznych systemach administracji. Jest narzędziem będącym w tym przypadku alternatywą dla podpisu kwalifikowanego, łączącą

możliwości narzędzia identyfikacji i składania podpisu. Pozwala między innymi na wnoszenie do urzędów podań, wniosków, skarg, opłat i deklaracji drogą elektroniczną, bez osobistej wizyty w urzędzie. Dotychczas uzyskanie Profilu Zaufanego wymagało złożenia odpowiedniego wniosku poprzez ePUAP i osobistej wizyty z dowodem osobistym lub paszportem w punkcie potwierdzającym tożsamość. Alternatywnie, samodzielnego potwierdzenia profilu mogli dokonać posiadacze podpisu kwalifikowanego. Profil Zaufany jest ważny przez trzy lata, przy czym można go przedłużyć przez ePUAP.

Do systemów wykorzystujących Profil Zaufany jako metodę uwierzytelnienia należą m.in.:

- elektroniczna Platforma Usług Administracji Publicznej,
- Platforma Usług Administracyjnych,
- Centralna Ewidencja i Informacja o Działalności Gospodarczej,
- Europejska Karta Ubezpieczenia Zdrowotnego,
- Centralna Ewidencja Pojazdów i Kierowców,
- usługi Wojskowych Komend Uzupełnień.

Profil Zaufany wykorzystywany jest także przez serwisy administracji publicznej, m.in.:

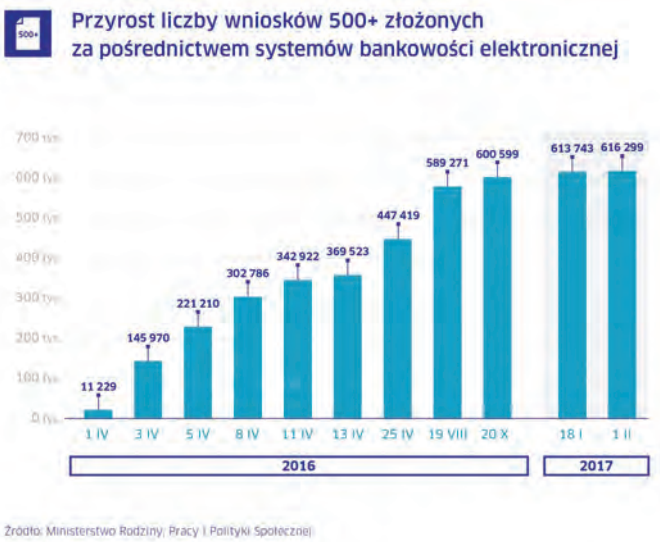
- ePUAP (Elektroniczna Platforma Usług Administracji Publicznej),
- PUE ZUS (Platforma Usług Elektronicznych ZUS),
- CEIDG (Centralna Ewidencja i Informacja o Działalności Gospodarczej),
- Serwis Ministerstwa Rodziny, Pracy i Polityki Społecznej – Emp@tia,
- Serwis o usługach państwowych obywatel.gov.pl,
- Serwis o prowadzeniu działalności gospodarczej dla przedsiębiorców biznes.gov.pl,
- Serwis o usługach elektronicznych urzędów pracy praca.gov.pl,
- Serwis Ministerstwa Sprawiedliwości – Krajowy Rejestr Karny,
- Serwis Krajowej Informacji Podatkowej,
- Regionalne platformy e-administracji, np. Wrota Mazowsza, SEKAP, Cyfrowa Małopolska.

Przykładowe usługi dostępne przez Internet obejmują:

- podpisywanie dokumentów przekazywanych przez Internet do urzędów,
- wniosek o dowód osobisty dla siebie lub dziecka, zgłoszenie utraty lub zniszczenia dokumentu,

- Karta Dużej Rodziny,
- EKUZ (Europejska Karta Ubezpieczenia Zdrowotnego),
- wydanie wtórnika prawa jazdy, zawiadomienie o zbyciu pojazdu,
- odpisy aktów z Urzędu Stanu Cywilnego: (m.in. akty urodzenia, małżeństwa),
- wybory: dopisanie do listy wyborców,
- zaświadczenie o niekaralności,
- rejestracja działalności gospodarczej,
- usługi ZUS: np. zwolnienie z powodu choroby dziecka lub innego domownika, zaświadczenie płatnika składek ZUS dla pracodawców zatrudniających do 21 pracowników.

Profil Zaufany ePUAP jest dzisiaj jedynym ogólnopolskim i darmowym mechanizmem uwierzytelniania w procesach dokumentowych administracji publicznej. W związku z faktem, że do tej pory założenie PZ wymagało wizyty w urzędzie w celu potwierdzenia tożsamości i kontrolowania ważności podpisu (wraz z okresowym przedłużaniem), korzystało z niego ~500 tys. obywateli, z czego wydaje się, że większość stanowili urzędnicy państwowi. Od niedawna PZ można założyć także online – dzięki nowej usłudze klienci banku mogą to zrobić za pośrednictwem bankowości elektronicznej w ciągu kilkunastu sekund.



Wdrożenie potwierdzania PZ online początkiem rewolucji w dostępie do usług państwowych

W procesie cyfryzacji administracji publicznej sektor bankowy jest naturalnym sprzymierzeńcem działań rządowych. Widać to choćby w wysokim potencjale nowej usługi – osób aktywnie korzystających z bankowości internetowej, których w całej Polsce jest już 15,3 mln. Skokowa popularyzacja elektronicznych usług państwowych, uzyskiwana poprzez likwidację głównej bariery z ich korzystania, jest urzeczywistnieniem idei cyfrowego państwa. Dynamiczny rozwój nowych państwowych usług online i konsekwencja w prowadzeniu tego procesu przez administrację publiczną stanowi również szansę rozwoju szybszych procesów w bankowości, obarczonych przy tym mniejszym kosztem i ryzykiem, np. elektroniczne przekazywanie danych z zasobów administracji, wymaganych m.in. przy procesach kredytowych, weryfikacji danych i oświadczeń klienta. Zrównoważone partnerstwo publiczno-prywatne, które w Europie staje się standardem, przyczynia się do wzmocnienia wizerunku banku jako instytucji zaufania publicznego, zarówno jako dostawcy tożsamości dla sektora publicznego i komercyjnego, jak również na rynku – w kontekście konkurencji ze strony podmiotów parabankowych. Z punktu widzenia banku edukacja klientów w wykorzystywaniu kanałów online do wypełniania wniosków może wpływać na zwiększenie sprzedaży produktów bankowych w kanałach zdalnych.

W obszarze e-Identyfikacji i płatności należy zidentyfikować również konkretne wyzwania, szczególnie dotyczące aspektów regulacji na poziomie europejskim i krajowym (eIDAS w zakresie identyfikacji i PSD II w zakresie płatności), standardów i technologii. Wdrażane narzędzia muszą zapewniać równowagę w odniesieniu ponoszonych kosztów i zapewnianego bezpieczeństwa – np. biometria naczyń krwionośnych, czy to palca (*fingervein* od Hitachi) czy dłoni (*palmvein* od Fujitsu) jest świetnym rozwiązaniem, ale jej wdrożenie może okazać się niemożliwe. Nie ma możliwości zapewnienia tych urządzeń ani w domach klientów, ani w każdej placówce bankowej. Podejmując temat przyjmowanego modelu i tempa adopcji poza dostępnością i kosztem, należy zwrócić uwagę na wygodę, przyzwyczajenia i preferencje oraz konieczny wysiłek edukacyjny.

Jak w kontekście kosztów wykorzystać szanse i zmitygować ryzyka związane z wdrożeniem PSD II?

PSD II to dyrektywa Parlamentu Europejskiego i Rady (UE) w sprawie usług płatniczych w ramach rynku wewnętrznego (2015/2366), zmieniająca wcześniejszą dyrektywę (PSD). Pierwsza dyrektywa PSD została przyjęta do prawa polskiego w ramach Ustawy o Usługach Płatniczych, obecnie trwa przygotowanie do wdrożenia PSD II do regulacji państw unijnych, w tym w Polsce (termin wdrożenia to styczeń 2018).

Implementacja PSD II może się wiązać ze znaczącymi kosztami dla sektora bankowego. O ile sama dyrektywa ma wejść do prawa polskiego poprzez nowelizację Ustawy o Usługach Płatniczych w wskazanym powyżej terminie, to już dwie rewolucyjne nowe usługi pozwalające na dostęp do rachunku stronom trzecim (*Third Party Provider*, TPP) oraz umożliwienie świadczenia usług inicjacji płatności (*Payment Initiation Service*, PIS) oraz usług dostępu do informacji o rachunku (*Account Information Service*, AIS) wejdą w życie dopiero w 18 miesięcy od przejęcia regulacyjnych standardów technicznych dotyczących m.in. tych usług (RTS, *Regulatory Technical Standards*). 23 lutego 2017 roku Europejski Urząd Nadzoru Bankowego (EBA, *European Banking Authority*) przedstawił finalny draft RTS w tym zakresie, zgodnie z nim najwcześniejszy możliwy termin wejścia w życie tych regulacji do listopad 2018 roku, termin ten może być jednak później, wszystko zależy od tempa akceptacji RTS.

W kontekście tak poważnej zmiany konieczne jest właściwe przygotowanie sektora bankowego pod względem zgodności z nowymi wymogami prawnymi. W wybranych obszarach efektywne wsparcie tego procesu może zapewnić KIR, jako podmiot dysponujący potencjałem umożliwiającym przyjęcie roli integratora dla sektora bankowego i TPP w ramach PSD II. Prywatna sieć międzybankowa, której operatorem jest KIR oraz wirtualizacja stosowana na poziomie infrastruktury IT w KIR może stanowić podstawę budowy sektorowej chmury obliczeniowej.

Chmura sektorowa KIR może być interesująca zwłaszcza dla sektora bankowego jako rozwiązanie minimalizujące koszty IT banków, co jest istotne ze względu na rosnącą presję ekonomiczną (m.in. obciążenia związane z bankowym funduszem gwarancyjnym, podatkiem bankowym, zwiększające się obowiązki sprawozdawcze i regulacyjne) przy potencjalnie wyższym, niż w przypadku chmur publicznych, poziomie bezpieczeństwa.

Wdrożenie dyrektywy PSD II spowoduje możliwość oferowania nowych usług nie tylko tych wymaganych przez nowe regulacje, ale także potencjalnie usług w szerszym zakresie. Pozwoliłoby to budować modele *win-win*, korzystne tak dla klientów, banków jak i stron trzecich. Skoro banki będą zmuszone do szerszego otwarcia się na współpracę z firmami trzecimi, to warto to zrobić może trochę szerzej, ale z korzyścią dla wszystkich stron.

Zgodnie z PSD II nowe przepisy pozwolą tzw. podmiotom trzecim realizować wspomniane usługi (dostępu do informacji i inicjacji płatności) bez umowy z bankami. Warto jednak podkreślić, że podmiotami trzecimi mogą i zapewne także będą nie tylko fintechy, ale także banki. Z kolei PSD II daje dostęp nie tyle do banków, ale do wszystkich podmiotów prowadzących rachunki płatnicze dla swoich klientów oraz udostępniających do nich dostęp poprzez Internet. Na moment wejścia w życie nowych przepisów bardzo możliwe, że największa grupa podmiotów trzecich to będą właśnie banki.

Usługi inicjacji płatności to w praktyce nowa odsłona popularnych na rynku *paybylinków*, zmniejszająca barierę wejścia dla nowych podmiotów. Z kolei usługi dostępu do informacji to w praktyce nowość. Podobne usługi istniały co prawda na rynku, ale korzystały z tzw. *screen scrappingu*, który nie spotkał się ani z przychylnością konsumentów, ani nadzoru bankowego w Polsce. Usługi te, dzięki możliwości odpytywania o transakcje na rachunku klienta bez jego udziału (po wcześniej wyrażonej zgodzie) pozwolą np. na zebranie informacji o transakcjach na rachunkach płatniczych klienta.

Usługi wymagane przepisami nie dadzą jednak pełnej informacji. Usługi informacyjne odnoszą się tylko do rachunków płatniczych, a to znaczy, ze salda depozytu czy wartość portfela inwestycyjnego nie będzie możliwa do poznania w inny sposób niż poprzez analizę transakcji na rachunku (a i tu będą mogły być udostępniane tylko dane, które nie są wrażliwe). Dla obu usług możliwe będzie także obciążanie klienta prowizjami. Co prawda dziś za dostęp do informacji przez Internet zazwyczaj nie płaci się, ale nie oznacza to, że tak będzie zawsze, a zapis dyrektywy mówi o braku dyskryminacji, który nie jest równoważny darmowości dla żadnych usług.

Należy pamiętać, że dostęp do istotnych usług, zwłaszcza finansowych, wymaga dbałości o bezpieczeństwo wdrażanych rozwiązań. Odpowiedzią sektora powinno być połączenie sił i świadome współdziałanie. Warto tu wykorzystać doświadczenie i kompetencje KIR, który może zaoferować bezpieczne rozwiązania w zakresie dostępu do rachunków bankowych (KIR oferuje

m.in. bramki płatnicze *Paybynet*, z których w różnym zakresie już dziś korzysta wielu konsolidatorów internetowych), a także zaangażować się w budowanie biznesowo-technologicznego ośrodka R&D oraz usług wspólnych i tworzenie sektorowych rozwiązań technologicznych – w obszarach eID, cyberbezpieczeństwa czy też usług wspierających popularyzacją bezpiecznych bankowych API, w tym w ramach tzw. Huba PSD II w ramach projektu Polish API, który jest realizowany w ramach Związku Banków Polskich.

W ramach ZBP toczą się intensywne prace, których efektem będzie powstanie standardu komunikacji, który będzie adresował specyfikę polskiego rynku, zapewniał bezpieczną komunikacją oraz wspierał konkurencyjność na rynku. Podsumowując wątek nowych usług wynikających z PSD II, warto podkreślić także, że te usługi pomogą cyfryzować gospodarkę i opierać kolejne innowacje o bezpieczne i już dziś powszechne cyfrowe usługi bankowe.

Cyfryzacja usług publicznych a sektor bankowy

Podobnie jak w przypadku **PSD2**, naturalną rolą **KIR** jest **rola węzła** lub **integratora** dla **sektora bankowego** i **administracji**.

Poziom zaawansowania sektora bankowego w Polsce, w połączeniu z gotowością społeczną do korzystania z rozwiązań udostępnianych w trybie online oraz nowymi regulacjami prawnymi, tworzą korzystne środowisko, w którym cyfryzacja usług publicznych może przebiegać szybciej i sprawniej. Można się spodziewać, że w dłuższej perspektywie ten proces przyczyni się do zwiększenia efektywności działania tak administracji, jak i banków (np. dostęp do wiarygodnej informacji o kliencie z US i ZUS) oraz ograniczy ryzyko operacyjne. Wsparcie rozwoju obrotu bezgotówkowego bezpośrednio wpłynie na upowszechnienie instrumentów płatniczych, a w efekcie także na skalę bankowego biznesu. W tym kontekście, podobnie jak w przypadku PSD II, naturalną rolą KIR wydaje się być rola węzła lub integratora dla sektora bankowego i administracji. Poza świadczeniem kompleksowych i niezawodnych usług rozliczeniowych, KIR ma także ambicję uczestniczenia w realizacji wyzwań stojących przed polskim sektorem bankowym, zwłaszcza w kontekście dynamicznie zmieniającego się otoczenia i zadań związanych z wdrażaniem procesów umożliwiających cyfryzację gospodarki i administracji. We współpracy z bankami i sektorem publicznym KIR wspiera wykorzystywanie innowacyjnych

technologii w celu kreowania rozwiązań rozszerzających ofertę sektora bankowego i zwiększających cyfrową świadomość i jakość życia Polaków.

Także w obszarze *Electronic Bill Presentment and Payment* (EBPP) KIR posiada ofertę (*Invoobill 2.0* – Qlik), która bezpośrednio odpowiada na potrzeby programu „Od papierowej do cyfrowej Polski", a jednocześnie ma duży komercyjny potencjał o wymiernym znaczeniu dla wszystkich uczestniczących podmiotów. Mechanizm tego rozwiązania zakłada, że bankowość internetowa i mobilna jest okienkiem na świat faktur. Dzięki usłudze Qlik klient otrzymywać będzie e-faktury w jednym miejscu – wprost do systemu bankowości elektronicznej i za usługi będzie płacić „jednym klikiem". W ten sposób już wkrótce będzie można udostępniać faktury za prąd, gaz, usługi telekomunikacyjne, ale być może także mandaty, podatki gruntowe i inne zobowiązania publiczne. Identyfikacja klienta bazować będzie na numerach PESEL i NIP, a po wyrażeniu zgody na korzystanie z usługi, system sprawdzi w bazie wszystkie faktury wystawione na dany numer PESEL i dostarczy je wprost do systemu bankowości internetowej klienta. Można się spodziewać, że z czasem usługa zyska nowe zastosowania, ponieważ dzięki jednoznacznej identyfikacji w oparciu o numer PESEL można np. dostarczać klientowi płatności za podatki czy nawet korespondencję od e-administracji. Upowszechnienie tego rozwiązania w relacjach z administracją otworzy perspektywę szerokiego zastosowania także w obszarze B2C. Wiąże się z tym potrzeba zaprojektowania rynku faktur elektronicznych, gdzie z racji swojej dotychczasowej pozycji, KIR może przyjąć rolę koordynatora i dostawcy ponadbankowej, a nawet pozasektorowej platformy do obiegu faktur elektronicznych.

Bankowe eID

W **e-commerce** brak zaufania do dostawcy, związany z wymogiem przekazania danych personalnych, może być powodem rezygnacji z zakupów.

Korzystanie z eID niesie ze sobą szereg wymiernych biznesowo zalet. Pozwala dostawcom usług na zwiększenie zyskowności dzięki redukcji kosztów oraz wzrostowi obrotów, przy jednoczesnej poprawie bezpieczeństwa. Weryfikacja klientów stanowi istotną pozycję kosztową dla firm wykorzystujących kanały cyfrowe do interakcji z klientami – eliminacja tych kosztów pozwala na zwiększenie skali biznesu. Z kolei dla klientów e-commerce

brak zaufania do dostawcy, związany z wymogiem przekazania danych personalnych, może być powodem rezygnacji z zakupów. Eliminacja ryzyka w tym aspekcie przyczyni się do wzrostu obrotów. Z kolei przykładowe korzyści w służbie zdrowia z punktu widzenia pacjenta obejmują ułatwienia w dostępie do placówek medycznych, uproszczenie systemu rejestracji, a w przyszłości być może także możliwość odbierania recept (zwłaszcza w przypadku powtarzalnych terapii w dobrze kontrolowanych chorobach przewlekłych i chronicznych). Z perspektywy systemu opieki zdrowotnej istotną zaletą będzie optymalizacja procesów i wzrost efektywności zarządzania, ułatwienie zrównoważenia podaży i popytu w kontekście dostępności i poziomu wykorzystania usług medycznych oraz lepsza kontrola wykorzystania budżetu przeznaczanego na realizację usług zdrowotnych. W administracji publicznej nastąpi ujednolicenie i zoptymalizowanie procesu weryfikacji petentów, skutkując przyspieszeniem obsługi i zmniejszeniem wydatków na przechowywanie i bezpieczeństwo danych. Dzięki tym zmianom wzrośnie liczba świadczonych usług zarówno publicznych, jak i komercyjnych. Uproszczenie procedury zakupowej oraz zwiększone poczucie bezpieczeństwa użytkowników przyczyni się do zwiększenia poziomu zaufania do partnerów, dynamizując ich przychody.

Istotnym aspektem wartym uwagi jest poprawa bezpieczeństwa. Partnerzy w wielu przypadkach narażeni są na błędy użytkowników lub próby oszustw i wyłudzeń. Możliwość pobierania zweryfikowanych danych z eID zmityguje ryzyko poniesienia szkód z tym związanych. Uproszczona i skuteczna weryfikacja znacznie zmniejszy to ryzyko. Wśród przykładowych obszarów wykorzystania można wskazać następujące kwestie:

- natychmiastowe potwierdzenie tożsamości i zawarcie umowy, podpisanie aneksu do umowy,
- wygodne logowanie jednym kontem do wielu serwisów i ochrona danych osobowych w sieci,
- zgłoszenie na studia, rejestracja jednym kontem we wszystkich systemach rekrutacyjnych,
- rejestracja na usługę medyczną,
- rejestracja do sklepu internetowego,
- zakup ubezpieczenia online.

Kluczem do cyfrowej administracji publicznej jest bankowa tożsamość pozwalająca na oszczędność czasu i poprawę doświadczeń klienta. W procesie przekazania tożsamości użytkownika KIR może pełnić funkcję pośrednika pomiędzy dostawcami usług a bankiem. Bankowe eID jest pierwszym krokiem we właściwym kierunku, ale można sobie wyobrazić, że przewidywana w rządowym programie e-Skrzynka, jednolity kanał komunikacji w relacji obywatel-administracja[13], będzie także uruchomiona w środowisku bankowym. KIR już dziś ma narzędzie w postaci systemu *Invoobill*, które może służyć jako jeden punkt zbiorczy dla komunikacji ze wszystkimi agendami publicznymi. System dziś wykorzystywany do opłacania regularnych zobowiązań, w przyszłości mógłby umożliwić także prezentację urzędowych dokumentów w bezpiecznym kanale bankowym.

Bankowy węzeł eID

Sprawne **uruchomienie Węzła Bankowego** możliwe jest dzięki wykorzystaniu istniejącej infrastruktury teleinformatycznej na linii **KIR – Banki.**

Bankowy węzeł ID, co do funkcji i mechanizmu działania, będzie w dużej mierze lustrzaną strukturą odpowiadającą węzłowi krajowemu, uruchomionemu na poziomie administracji w konsekwencji zmian wprowadzanych rozporządzeniem eIDAS. Jako najważniejszy punkt styku administracji i komercji, węzeł pozwoli na skonsolidowanie w jednym miejscu dostawców tożsamości z dostawcami usług i ustanowienie łączności z krajowym węzłem identyfikacji. Usługi identyfikacji otwierają zupełnie nowe możliwości w kontekście potencjału biznesowego. Należą do nich m.in. potwierdzanie tożsamości dla dostawcy usług przez bank, logowanie do portalu dostawcy usług za pomocą bankowej tożsamości, silna bankowa autoryzacja oraz dostarczanie atrybutów. Opracowanie założeń budowy węzła identyfikacji jest wynikiem współpracy między ZBP i KIR, co pozwala na wypracowanie optymalnego wsparcia projektu w kwestiach technicznych, legislacyjnych, zarządzania projektem i konsultacji merytorycznych w procesie integracji z Węzłem Krajowym.

13 http://www.mr.gov.pl/media/21329/Od_papierowej_do_cyfrowej_PL_prez_dluzsza_20062016.pdf

Wśród uzyskiwanych dzięki temu rozwiązaniu korzyści warto wymienić:

- wykorzystanie istniejącej infrastruktury teleinformatycznej (w relacji KIR – banki),
- zarządzenie technologiczne (m.in. uprawnieniami, certyfikatami) dostawców,
- łatwiejsze wprowadzanie zmian technologicznych,
- klarowny proces obsługi reklamacji.

Sprawne uruchomienie węzła bankowego możliwe jest dzięki wykorzystaniu istniejącej infrastruktury teleinformatycznej na linii KIR – banki, co pozwala przyspieszyć wdrożenie przy jednoczesnym obniżeniu kosztów. Należy przy tym podkreślić, że przyjęte zasady obejmują zapewnienie jednego punktu styku węzła krajowego z węzłem komercyjnym i uzyskanie dostępu do portali administracji w trybie pojedynczego logowania (*single sign*), ale banki nie będą przechowywać i wykorzystywać informacji do jakich portali administracji logują się obywatele.

Z dużą dozą prawdopodobieństwa można przyjąć, że użytkownikami końcowymi rozwiązania będą osoby fizyczne, za których zgodą dostawcy tożsamości (banki) udostępnią poprzez węzeł komercyjny eID, utrzymywany przez KIR, informacje dostawcom usług. Szacując potencjał rozwiązania przyjmuje się, że odpowiada on liczbie osób korzystających z usług bankowości elektronicznej – to zbiór klientów już posiadający odpowiednie kompetencje z uwagi na aktywne użytkowanie technologii cyfrowych. Banki mają narzędzia umożliwiające weryfikację tożsamości tych użytkowników i dysponują bazą ich atrybutów. Do węzła komercyjnego eID, jako dostawcy usług, będą mogli przystąpić gracze komercyjni, których obecność wzmocni propozycję wartości dla użytkowników końcowych rozwiązania i zachęci ich do korzystania z eID. Wśród dostawców usług szczególnie zainteresowane korzystaniem z usług mogą być podmioty z sektora finansowego, platformy eCommerce, media, służba zdrowia, administracja publiczna, media cyfrowe. Dla każdego segmentu można oszacować wskaźniki związane z penetracją – rozumianą jako procent użytkowników korzystających z usług eID oraz liczbą interakcji – rozumianą jako weryfikacja tożsamości lub udostępnienie atrybutów. Korzyści uzyskane poprzez wprowadzenie eID w większości są wymierne choć najlepiej zostaną zweryfikowane w realiach rynkowych.

Podsumowanie

Pod względem doświadczenia sektora bankowego w sprawnym i relatywnie szybkim przeprowadzaniu procesów związanych z digitalizacją Polska jest wyjątkowym krajem. Jesteśmy rynkiem zaawansowanym zarówno pod względem modelu funkcjonowania banków, jak i przygotowania klientów do sprawnego adoptowania innowacyjnych rozwiązań. Nasza bankowość od lat plasuje się na pozycji europejskiego lidera w zakresie usług internetowych i mobilnych. Banki w Polsce oferują bezpieczne i wysokowydajne rozwiązania, są technologicznymi innowatorami. Podlegają także ścisłej kontroli i nadzorowi instytucji państwowych, mają zaawansowane procedury i regularnie poddawane są audytom. Cieszą się wysokim poziomem zaufania i dysponują stabilnymi bazami klientów. Przygotowując się do dynamicznych zmian na rynku, już pracują nad udostępnianiem usług z zakresu eID i podpisem w chmurze.

Odbiciem zaawansowania oferty sektora bankowego jest także wysoki poziom świadomości klientów, którzy korzystają z usług bankowych – w tym z bankowości internetowej i mobilnej – wielokrotnie w ciągu miesiąca, pamiętając swoje hasła dostępu i wiedząc w jaki sposób postąpić w przypadku konieczności zablokowania dostępu do rachunku. Gotowość klientów do korzystania z innych usług w oparciu o bankowe narzędzia uwierzytelniania została udowodniona przy okazji programu Rodzina 500+. Poszerzenie możliwości uzyskiwanych dzięki bankowemu eID wydaje się naturalnym kierunkiem w procesie cyfryzacji administracji i gospodarki. Dzięki wykorzystaniu ekspertyzy sektora bankowego można uzyskać wymierne korzyści, optymalizując czas i koszt wdrożenia nowych rozwiązań, przy jednoczesnym zachowaniu wysokiego poziomu bezpieczeństwa. Poza oszczędnością czasu, optymalizacją procesów i poprawą komfortu funkcjonowania wszystkich stron – klientów banków, przedsiębiorców, administracji i samych banków – korzyścią ogólną jest wzrost kapitału zaufania społecznego, co z kolei przekłada się na oszczędności w skali makro, poprawę konkurencyjności oraz wzrost przedsiębiorczości – czyli wymierne korzyści dla polskiej gospodarki i przedsiębiorczości.

Narzędzia dostępu do rachunku bankowego, poprzez ich poufność, budują zaufanie klientów, które stanowi fundament działania sektora. Ze względu na niepodważalną wartość bezpieczeństwa, mechanizmy umożliwiające

dostęp do rachunku, są i powinny pozostać zlokalizowane na stronach bankowych. Naruszenie tej zasady może determinować trudne do przewidzenia skutki, nie tylko w odniesieniu do sfery usług finansowych. Udostępnienie wygodnego i bezpiecznego mechanizmu identyfikacji tożsamości poprzez Węzeł Bankowy, w połączeniu z funkcjonalnością Węzła Krajowego, pozwoli na przeprowadzenie sprawnej cyfryzacji w sposób optymalny pod względem kosztów, bezpieczeństwa i uzyskiwanych korzyści.

Biorąc pod uwagę szerszą perspektywę stajemy – jako państwo – przed wyzwaniem upowszechnienia rozwiązań cyfrowych w administracji i gospodarce na poziomie analogicznym do tego, który już się dokonał w sektorze bankowym. Program „Od papierowej do cyfrowej Polski" wyznacza kierunki rozwoju e-państwa i cyfryzacji polskiej gospodarki na najbliższe lata. W tym kontekście rozwiązania proponowane przez KIR odpowiadają na zapotrzebowanie zarówno administracji, jak i innych interesariuszy i mogą być z powodzeniem stosowane w szerszej skali. KIR wykorzystywać będzie swoje zasoby dla wsparcia cyfryzacji procesów gospodarki i administracji, zwiększania obrotu bezgotówkowego, a w konsekwencji dla budowy Polski Cyfrowej.

Podsumowując, warto zadać sobie proste pytanie: po co to robimy? Robimy to po to, aby administracja oraz rynek komercyjny dołączyły tam, gdzie obywatele już są, czyli do świata wirtualnego.

Artur Wach
Dyrektor ds. Ryzyka i Kontroli w Citibank Europe plc

Przed dołączeniem do Citibank Europe Plc w 2016 r., od 2011 r. pełnił funkcję Dyrektora Departamentu Bezpieczeństwa Systemów Informatycznych w Banku Handlowym SA w Warszawie. Posiada również bogate doświadczenie w pracy w firmach konsultingowych zdobyte przy realizacji projektów z zakresu wdrażania systemów IT oraz bezpieczeństwa dla firm z sektora finansowego, telekomunikacyjnego oraz publicznego. Absolwent Wydziału Elektroniki Politechniki Warszawskiej. Dysponuje wiedzą z zakresu systemów zarządzania bezpieczeństwem informacji (ISMS) oraz zarządzania ciągłością działania (BCP) oraz ma uprawnienia i certyfikaty audytora wiodącego ISMS (ISO27001) oraz CISA i CISSP.

Piotr Malec
Dyrektor Programu Transformacji Przeciwdziałania Praniu Pieniędzy i Finansowania Terroryzmu dla regionu EMEA w Citibank Europe Plc

Przed dołączeniem do zespołu Citibanku pracował m.in. ponad 10 lat w Deloitte (w Polsce i w Nowym Jorku), a także po stronie dostawców systemów. Ma ponad 20-letnie doświadczenie w kierowaniu projektami i programami oraz w zarządzaniu dużymi portfelami projektów i programów. Kierownik i Dyrektor Projektu w wielu wdrożeniach systemów bankowych (obejmujących analizę wymagań, wybór systemu, negocjacje kontraktowe, wdrożenie, przegląd powdrożeniowy). Ma doświadczenie m.in. z następującymi systemami: Alnova, Profile, IBIS, IBS-90, Globus, MIDAS, BankMaster, FlexCube, różne systemy bankowości internetowej.
Dysponuje wiedzą na temat polskiego oraz amerykańskiego sektora finansowego oraz ma unikatowe praktyczne doświadczenia w obszarze wykrywania nadużyć i zagadnień przeciwdziałania praniu pieniędzy (AML), tworzenia i korzystania z planów ciągłości działania w sytuacjach kryzysowych – powódź we Wrocławiu czy przywracanie funkcjonowania firmy Deloitte na obszarze Nowego Jorku po ataku terrorystycznym 11 września.
W latach 2005–2006 pełnił społecznie rolę Prezesa, a w latach 2006–2007 Wiceprezesa PMI Poland Chapter, a od maja 2016 r. Wiceprezesa ds. Członkostwa i Administracji. Od ponad 20 lat wykłada na studiach podyplomowych i Executive MBA.

Piotr Malec, Artur Wach
Citibank Europe

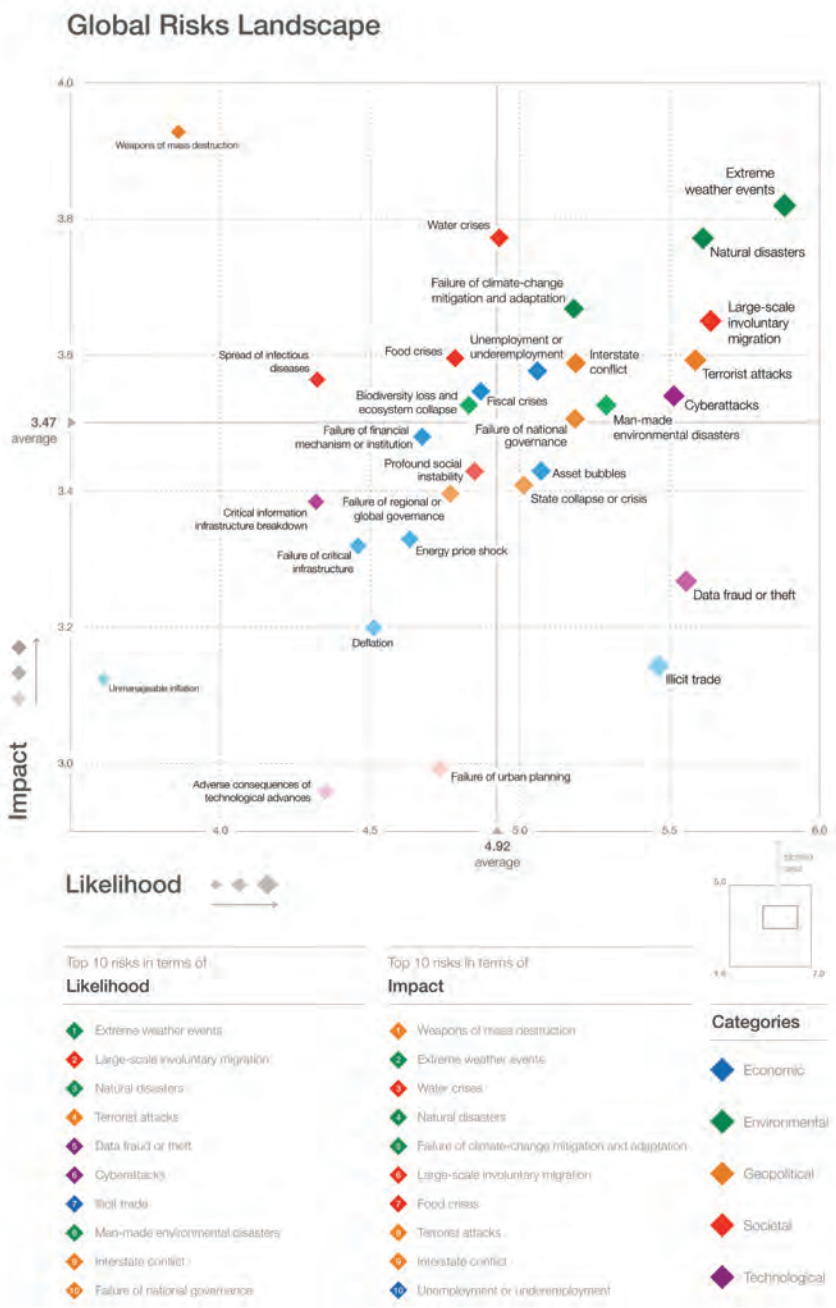
Zarządzanie cyberbezpieczeństwem w globalnym banku

Zagrożenie ze strony cyberprzestępców jest jednym z najwyżej plasowanych zagrożeń podczas oceny ryzyka. Światowe Forum Ekonomiczne (*World Economic Forum*) w swoim raporcie z 2017 r.[1] klasyfikuje ryzyko cyberataków na bardzo wysokim 6. miejscu pod względem prawdopodobieństwa wystąpienia, zaraz po kradzieży danych i atakach terrorystycznych. W połączeniu z rosnącym uzależnieniem gospodarek światowych od kanałów cyfrowych i digitalizacji stanowi to bardzo duże wyzwanie dla systemów finansowych, systemów rozliczeń światowych, a szczególnie dla uczestników/pośredników tych rozliczeń jakimi są banki.

Wyjątkowego znaczenia nabiera ryzyko cyberataków dla globalnych instytucji finansowych, takich jak Citibank, które stanowią kluczowe elementy w krwioobiegu światowych rozliczeń.

Citibank przypisuje należycie wysoką rangę cyberbezpieczeństwu. W poniższym rozdziale postaramy się pokazać, na przykładzie doświadczeń światowych instytucji finansowych, jakie konsekwencje może nieść za sobą brak przygotowania na cyberataki, jak problem cyberbezpieczeństwa jest rozumiany przez regulatorów oraz jakie dodatkowe zagrożenia czyhają na globalną instytucję finansową, taką jak Citibank.

1 *The Global Risk Report 2017 12th Edition, World Economic Forum*, http://www3.weforum.org/docs/GRR17_Report_web.pdf


Global Risks Landscape
Weapons of mass destruction
Extreme weather events
Water crises
Natural disasters
Failure of climate-change mitigation and adaptation
Large-scale involuntary migration
Spread of infectious diseases
Food crises
Unemployment or underemployment
Interstate conflict
Terrorist attacks
Biodiversity loss and ecosystem collapse
Fiscal crises
Cyberattacks
3.47 average
Failure of financial mechanism or institution
Failure of national governance
Man-made environmental disasters
Profound social instability
Asset bubbles
State collapse or crisis
Critical information infrastructure breakdown
Failure of regional or global governance
Energy price shock
Failure of critical infrastructure
Data fraud or theft
Deflation
Unmanageable inflation
Illicit trade
Failure of urban planning
Adverse consequences of technological advances
Impact
4.92 average
Likelihood
Top 10 risks in terms of Likelihood
1 Extreme weather events
2 Large-scale involuntary migration
3 Natural disasters
4 Terrorist attacks
5 Data fraud or theft
6 Cyberattacks
7 Illicit trade
8 Man-made environmental disasters
9 Interstate conflict
10 Failure of national governance
Top 10 risks in terms of Impact
1 Weapons of mass destruction
2 Extreme weather events
3 Water crises
4 Natural disasters
5 Failure of climate-change mitigation and adaptation
6 Large-scale involuntary migration
7 Food crises
8 Terrorist attacks
9 Interstate conflict
10 Unemployment or underemployment
Categories
Economic
Environmental
Geopolitical
Societal
Technological

Przykłady cyberataków na globalne instytucje finansowe w ostatnich latach

Banki, które pozostają przede wszystkim instytucjami zaufania publicznego i w których bezpieczeństwo powierzonych środków jest fundamentalną wartością, stają obecnie przed dylematem: jak dostarczyć skuteczny poziom zabezpieczeń przy zachowaniu prostoty i funkcjonalności serwisu, konkurując jednocześnie z pojawiającymi się na rynku firmami z branży fintech.

Przy 30 mln umów na świadczenie usług bankowych przez Internet klientom indywidualnym (ZBP, wrzesień 2015 r.) widać, że jako kraj jesteśmy świadkami cyfrowej rewolucji. Powszechny dostęp do informacji i nieograniczony przepływ danych przez WWW oferuje nie tylko nowe możliwości, lecz także nowe zagrożenia.

Słabość systemu i jego wrażliwość na cyberataki nie jest zaskoczeniem, gdy weźmiemy pod uwagę rozpowszechnienie Internetu i jego dynamiczny rozwój w ostatnich latach. W 1995 r. zaledwie 16 mln osób korzystało z Internetu, dziś jest to już ponad 3 mld, czyli niemal połowa mieszkańców globu. W samych Stanach Zjednoczonych w 2015 r. aż 88% mieszkańców korzystało z Sieci. Dla porównania, w Polsce w tym samym czasie z Internetu korzystało 70 proc. Polaków (wg Gemius).

Przy takim tempie rozwoju oraz nastawieniu na monetyzację kwestie bezpieczeństwa pozostały zaniedbane, czego przykładem były głośne ataki hakerów w 2014 r. na JP Morgan, w efekcie których wykradziono dane 76 mln osób prywatnych i 7 mln firm czy też włamanie z wykorzystaniem *malware* na konta Sony Pictures Entertainment, przez co utracono 100 terabajtów danych.

Dodatkowo obserwujemy też rosnące znaczenie *customer experience* w konkurencji o klientów na rynku bankowym. Doświadczenie osobiste stało się jednym z dominujących kryteriów decydujących o lojalności i utrzymaniu relacji z firmą czy konkretnym produktem. Współcześni klienci, przyzwyczajeni przez *social media* do nieustającego kontaktu i wysokiej responsywności marek, zaczynają przenosić te oczekiwania na sektor bankowy.

Przyczynia się do tego technologia, która dostarcza coraz to nowsze narzędzia do łączenia się z siecią i bankiem. Jest to kolejny poziom wymagający uszczelnienia pod kątem zabezpieczeń. Paradoksalnie, rozwój technologiczny może być naszym sprzymierzeńcem w tworzeniu bezpiecznej i zarazem komfortowej usługi bankowej przez wykorzystanie natywnych funkcjonalności produktu jako nowych form zabezpieczeń, np. identyfikacji biometrycznej,

płatności z wykorzystaniem odcisków palców, elektrokardiogramu czy rozpoznawania twarzy (*Selfie Pay* MasterCard'a).

Kradzież tożsamości staje się zjawiskiem coraz bardziej powszechnym i coraz więcej osób jest na nią narażonych, głównie w związku z nieostrożnym dzieleniem się informacjami osobistymi w Internecie przez indywidualne osoby. Z tej perspektywy jest to dziś realny problem o rosnącej skali. O kradzieży tożsamości mówimy w sytuacji, w której ktoś bezprawnie wejdzie w posiadanie naszych danych osobowych i wykorzysta je wbrew naszej woli, podszywając się pod nas. Niestety, kradzież tożsamości jest zazwyczaj dokonywana w celu osiągnięcia korzyści majątkowej. Dane mogą zostać pozyskane np. z wyrzucanych na śmietnik dokumentów czy nośników, ale coraz częściej przede wszystkim poprzez włamanie do komputera. Każdy z nas ma największy wpływ na bezpieczeństwo swoich danych, na co z kolei największy wpływ ma ciągła edukacja i świadomość zagrożeń czyhających w cyberświecie.

Poniżej kilka przykładów incydentów bezpieczeństwa dotyczących globalnych instytucji finansowych z ostatnich miesięcy.

Na początku 2016 Bank HSBC musiał publicznie przepraszać swoich klientów za niedostępność ich systemów bankowości internetowej w wyniku ataku *denial of service*, ale nie nastąpiła kradzież środków klientów.

Standard Bank of South Africa stracił 13 mln USD w wyniku ataku przeprowadzonego 15 maja 2016 r. przez zorganizowaną grupę ok. 100 osób, która w ciągu trzech godzin wyprowadziła środki klientów banku wykorzystując 1400 bankomatów w Japonii.

W lipcu 2016 r. dwa sfałszowane transfery SWIFT z First Bank of Nigeria na kwoty 15,1 mln i 6,5 mln dolarów zostały przesłane do odbiorcy w RHB Indochina Bank in Cambodia.

W tym samym czasie Morgan Stanley został ukarany kwotą jednego mln USD przez Amerykańską Komisję Papierów Wartościowych i Giełd (SEC – *Securities and Exchange Commission*) za dopuszczenie do przejęcia w nieuprawniony sposób i upublicznienia informacji o klientach.[2]

Były pracownik banku Galen Marsh, mając nieograniczony dostęp do informacji o rachunkach klientów banku z niezabezpieczonych wewnętrznych aplikacji, przez trzy lata ściągał i publikował na prywatnym serwerze informacje w celu ich sprzedaży grupom przestępczym.

2 *US SEC ADMINISTRATIVE PROCEEDING File No. 3-17280*
http://www.complinet.com/net_file_store/new_rulebooks/3/4/34-78021.pdf

W listopadzie 2016 r. brytyjski Tesco Bank musiał czasowo wstrzymać działalność po kradzieży środków z 20 000 rachunków klientów. Bank zarządzający w sumie 136 tys. rachunków nie był w stanie wyjaśnić, w jaki sposób pieniądze z nich zniknęły. Szacuje się, że skradziono ok. 2,5 mln GBP.

Najbardziej znanym skutecznym atakiem było wyprowadzenie z Banku Centralnego Bangladeszu 81 mln dolarów w lutym 2016 r. w wyniku nieuprawnionego transferu z użyciem sieci SWIFT z rachunku banku w Federal Reserve Bank of New York. Przestępcy włamali się do siedziby banku w Dhaka i wytransferowali środki do kasyna w Las Vegas.

W styczniu 2017 r. w wyniku cyberataku klienci bankowości prywatnej Lloyds Banking Grup zostali tymczasowo pozbawieni dostępu do swoich środków. Jak podaje bank, w wyniku ataku nie skradziono żadnych środków klientów.

W ostatnim czasie regulatorzy zwracają uwagę instytucjom finansowym, że nie tylko duże kwoty pozyskane w wyniku cyberataku, lecz także drobniejsze przestępstwa mają znaczenie. W opublikowanym w październiku 2015 r. raporcie FATF (*Financial Action Task Force*), międzynarodowego organu zajmującego się tworzeniem i promowaniem standardów chroniących globalny system finansowy przed praniem brudnych pieniędzy, finansowaniem terroryzmu czy działaniem na rzecz nierozprzestrzeniania broni masowego rażenia, a dotyczącym rosnącego ryzyka finansowania terroryzmu[3] zwracana jest uwaga, że organizacja ataków terrorystycznych wymaga coraz mniejszych nakładów. Przykładowo, według szacunków ONZ, całkowity koszt ataków bombowych w Londynie w 2005 r. wymagał ok. 14 tys. dolarów, ataki w Paryżu na redakcję Charlie Hebdo i sklepy z koszerną żywnością sfinansowano z wyłudzonych kredytów o łącznej wartości ok. 32 tys. dolarów. Jeżeli porównać to z kosztem ok. 0,5 mln dolarów potrzebnych do przeprowadzenia ataków z 11 września 2001 r., najnowsze ataki z wykorzystaniem skradzionych ciężarówek w Marsylii i Berlinie odbyły się bezkosztowo.

Odpowiedź regulatorów na rosnące ryzyko cyberatakami

Ubiegły rok był szczególnie bogaty w nowe regulacje o zasięgu lokalnym lub światowym w zakresie cyberbezpieczeństwa. W przypadku banku globalnego zgodność z wymogami różnych regulatorów ma szczególne znaczenie

3 *FATF (2015), Emerging Terrorist Financing Risks, FATF, Paris*, www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html

w związku z prowadzeniem działalności w wielu jurysdykcjach. Poniżej przedstawiono wybrane, nowe regulacje z największych centrów finansowych na świecie – USA, Wielkiej Brytanii oraz Unii Europejskiej.

We wrześniu 2015 r. *Office of Compliance Inspections and Examinations'* (OCIE's) ogłosił nowe wytyczne dotyczące przeglądów instytucji finansowych z ramienia SEC – *Cybersecurity Examination Initiative*. Reguły bezpieczeństwa zakładają konieczność posiadania pisemnych polityk i procedur zapewniających bezpieczeństwo informacji o klientach oraz ich danych, spisanych zasad na wypadek przewidywanych zagrożeń naruszenia integralności danych i informacji klientów, ochrony przed nieuprawnionym dostępem lub użyciem informacji lub danych klientów, które może skutkować znaczącą szkodą lub niedogodnością dla jakichkolwiek klientów.

W październiku 2016 r. *Financial Crimes Enforcement Network* (FinCEN) wydał nowe zalecenie[4] składania doniesień o każdym cyberataku w formie SAR (*Suspicious Activity Report*) dotychczas używanych tylko do raportowania Prania Pieniędzy i Finansowania Terroryzmu. W uzasadnieniu FinCEN powołuje się na wspominany już raport FATF, mówiący o wykorzystaniu środków z cyberprzestępczości do finansowania działalności grup przestępczych oraz przygotowywaniu aktów terrorystycznych.

W październiku 2016 r. ministrowie finansów Grupy G7 (Wielkiej Brytanii, Kanady, Francji, Niemiec, Włoch, Japonii i Stanów Zjednoczonych) wypracowali wytyczne chroniące globalny system finansowy przed ryzykiem cyberataków. Oprócz wypracowania na poziomie poszczególnych krajów mechanizmów zapobiegawczych kraje zobowiązały się do wzajemnego informowania o zagrożeniach i współpracy przy ściganiu sprawców.

We wrześniu 2016 r. *Commodity Futures Trading Commission* zaaprobował poprawki w regulacjach dotyczących obrotu papierami wartościowymi wprowadzające konieczność przeprowadzania cybertestów i weryfikacji zabezpieczeń systemów tradingowych.[5]

Także we wrześniu 2016 r. *New York State Department of Financial Services* (NYDFS) wprowadził bardzo szczegółową regulację[6] nakładającą obowiązek wdrożenia szczególnych zasad bezpieczeństwa chroniących przed

4 https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf

5 http://www.cftc.gov/PressRoom/PressReleases/pr7293-15

6 http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf

cyberatakami i zabezpieczających środki klientów dla wszystkich instytucji finansowych zarejestrowanych na terenie stanu Nowy Jork.

W lipcu 2016 r. Parlament Europejski przyjął dyrektywę NIS przygotowaną przez Komisję Europejską w sprawie bezpieczeństwa sieci i systemów informatycznych.[7]

Połączone siły Compliance i Technologii

Wspomniane już zalecenie *Financial Crimes Enforcement Network* (FinCEN) wyraźnie wskazuje, że należy spodziewać się coraz bliższej współpracy pomiędzy pracownikami odpowiedzialnymi za bezpieczeństwo i *Compliance*. Nie tylko z powodów już wspomnianych czyli konieczności zalegalizowania przez grupy przestępcze środków uzyskanych z cyberataków.

Współpraca pomiędzy obydwiema grupami ma zdecydowanie większe i szersze znaczenie. Ataki na systemy banku mają, oprócz wymiernych materialnych strat w przypadku powodzenia i wyprowadzenia środków z systemu bankowego, także olbrzymi aspekt reputacyjny. Banki jako instytucje zaufania publicznego, którym klienci powierzają swoje pieniądze, w wyniku ataku mogą stracić o wiele więcej niż tylko pieniądze – mogą stracić zaufanie.

Dlatego tak ważne jest skuteczne współdziałanie oficerów *compliance* z innymi podmiotami odpowiedzialnymi za bezpieczeństwo. Współpraca i częsta wymiana informacji mogą budować zarówno świadomość zagrożeń płynących ze świata zewnętrznego, jak i dobre praktyki. Dodatkowo pozwala uświadamiać pracownikom, że kradzież informacji czy danych klientów może wynikać nie tyle ze słabości zabezpieczeń systemów informatycznych, o ile ze skutecznego zastosowania socjotechnik przez zorganizowane grupy przestępcze.

Celem ataku nie są już tylko same systemy, lecz także informacja w nich zawarta, a informacja może być ujawniona w różnorodny sposób.

7 DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016L1148&from=PL

Podejście banków globalnych

W komunikacie prasowym ze stycznia br. JP Morgan przekazał swoim akcjonariuszom, że o ile całkowite wydatki na utrzymanie zgodności z regulacjami (*Compliance*) mają tendencje spadkowe, o tyle wydatki na zachowania cyberbezpieczeństwa będą w dalszym ciągu rosły. Wydaje się to być w obecnych czasach trendem światowym.

Globalne instytucje finansowe ze względu na skalę działalności oraz powszechną rozpoznawalność marki stają się celem cyberatakówprzez wiele przestępczych organizacji, jak również indywidualnych osób – hakerów, poszukujących możliwości zyskania rozgłosu. Można zaryzykować stwierdzenie, że organizacje o globalnym zasięgu działalności są ciągle celem różnego rodzaju ataków przeprowadzanych przez osoby i organizacje kierujące się różnymi motywami: od poszukiwania rozgłosu przez nadużycia finansowe, aż po szpiegostwo gospodarcze i konflikty polityczne na poziomie krajów.

Cyberprzestępczość to potężny biznes, który w ostatnich latach intensywnie się rozwija. Specjaliści ds. bezpieczeństwa informacji stając do nierównej walki muszą osiągnąć równowagę między innowacją a bezpieczeństwem. To prawdziwa wojna, w której kluczowym elementem decydującym o skuteczności jest dostęp do informacji i szybkość podejmowanych działań.

Potrzeby związane z bezpieczeństwem stale rosną ze względu na ogromne ilości danych oraz powszechność rozwiązań mobilnych. Aby chronić działalność instytucji finansowej przed zagrożeniami cybernetycznymi, kluczowe jest zapewnienie ciągłego monitorowania bezpieczeństwa sieci i systemów oraz występujących w nich zdarzeń bezpieczeństwa, wykrywanie ataków i prób ataków w czasie rzeczywistym oraz szybkie reagowanie w celu zneutralizowania incydentów bezpieczeństwa. Monitorowanie bezpieczeństwa własnych sieci i systemów pozwala jednak tylko na podejmowanie działań reaktywnych i umożliwia skuteczną obronę w przypadku ataku. Aby zwiększyć zdolność organizacji do zmierzenia się z obecnymi cyberzagrożeniami coraz więcej globalnych firm buduje specjalizowane jednostki bezpieczeństwa zajmujące się zbieraniem i analizą zdarzeń z własnych systemów i dba o budowę złożonej sieci kontaktów z innymi firmami i jednostkami sektora publicznego w celu pozyskiwania informacji o aktualnych cyberzagrożeniach. Dostęp do tych informacji umożliwia podejmowanie proaktywnych działań pozwalających organizacji na przygotowanie się na to, co jeszcze nie jest znane

we własnej sieci w myśl zasady, że „dobrze uczyć się na swoich błędach, ale jeszcze lepiej uczyć się na błędach cudzych".

Nie ulega wątpliwości, że cyberbezpieczeństwo powinno być traktowane jako wspólny interes wszystkich podmiotów, które są uczestnikami nowoczesnej gospodarki opartej na Internecie. Szczególną rolę odgrywają instytucje państwowe, firmy informatyczne oraz firmy z sektorów krytycznych dla gospodarki, takich jak firmy telekomunikacyjne, energetyczne czy instytucje finansowe. Zapewnienie bezpieczeństwa w świecie cyfrowym państwom, instytucjom i obywatelom będzie możliwe wyłącznie w wyniku współpracy i partnerstwa wielu podmiotów, zarówno z sektora prywatnego, jak i publicznego.

Jednym z przykładów realizacji tej koncepcji w Polsce jest powołane w lipcu 2016 r. Narodowe Centrum Cyberbezpieczeństwa, w którym eksperci gromadzą informacje o zagrożeniach od różnych podmiotów biorących udział w przedsięwzięciu. W oparciu o te informacje specjaliści prowadzą analizy i wydają rekomendacje. Są one tym lepsze i dokładniejsze, im lepsze i bardziej kompletne informacje dostarczane są przez współpracujące podmioty.

NC Cyberbezpieczeństwa będzie odgrywać również kluczową rolę w procesie dostosowywania Polski do wymogów unijnej dyrektywy NIS, dyrektywy ds. Bezpieczeństwa Sieci i Informacji, której celem jest budowa spójnego europejskiego systemu cyberbezpieczeństwa przez państwa członkowskie. Jednym z najważniejszych postanowień ubiegłorocznego szczytu NATO w Warszawie było również uznanie cyberprzestrzeni za kolejny obszar prowadzenia działań zbrojnych, tak samo istotny jak ląd, woda, kosmos i przestrzeń powietrzna. Powtórzone zostały deklaracje ze szczytu w Newport, że cyberataki mogą być tak samo szkodliwe jak konwencjonalne działania oraz że cyberobrona stanowi integralną część systemu obrony NATO.

Praca u podstaw – edukacja pracowników

Z perspektywy globalnego banku, gdzie ogromna większość wszystkich transakcji finansowych i niefinansowych klientów przeprowadzanych jest przez Internet, edukacja klientów w kwestii cyberbezpieczeństwa staje się niejako immanentnym elementem działalności. Banki prowadzą zarówno dla klientów sektora detalicznego, jaki i korporacyjnego specjalne akcje i projekty edukacyjne z zakresu bezpieczeństwa danych w sieci, ochrony tożsamości, etc. Dbałość o cyberbezpieczeństwo klientów i ich środków wiąże się ściśle

ze stałą edukacją i szkoleniami pracowników banków, którzy jako pierwsza linia kontaktu z klientem muszą być gotowi do bieżącego reagowania na zagrożenia. Zapewnienie stałego dostępu do najświeższych informacji, co wraz z odpowiednimi procedurami na okoliczność danych naruszeń (przykładowo nieautoryzowanego pobrania środków z rachunku bankowego) gwarantuje szybką i właściwą reakcję.

Każdy z naszych pracowników, a w szczególności osoby bezpośrednio kontaktujące się z klientami, powinny znać najlepsze praktyki bezpiecznego korzystania z bankowości elektronicznej i być w stanie odpowiedzieć na najczęściej zadawane pytania. Dlatego poza obowiązkowymi dla wszystkich szkoleniami z zakresu bezpieczeństwa informacji i ochrony danych osobowych pracownicy regularnie powinni otrzymywać bieżące wiadomości z zakresu cyberzagrożeń oraz porady, jak ich unikać.

Jednym z najsłabszych ogniw w każdym systemie zabezpieczeń jest człowiek. O edukacji klientów wspominaliśmy już, teraz chcielibyśmy przedstawić inne zagrożenie – pracowników, a dokładniej brak ich świadomości. Do niedawna błąd ludzki lub brak odpowiednich procedur i systemów kontrolnych był głównym elementem, na który liczyli cyberprzestepcy. Wprowadzenie dodatkowych regularnych kontroli zarówno ze strony kierowników, jak i niezależnych jednostek, jak audyt wewnętrzny wystarczało do zmniejszenia ryzyka lub ograniczenia skutków potencjalnego ataku. W chwili obecnej bardzo częstym elementem jest próba przeniknięcia do wewnątrz banku nie za pośrednictwem pracownika, a dedykowanego oprogramowania, otwierającego drzwi od środka. W tym celu wykorzystywane są różne metody oparte na socjotechnikach i braku uważności pracowników, niekoniecznie posiadających wrażliwe pozycje. Czasami wykorzystywani są także klienci, partnerzy lub dostawcy mający dostęp do systemów poprzez coraz liczniejsze interfejsy do systemów bankowych.

Jednym z najczęściej wymienianych sposobów przenikania przestępców przez zabezpieczenia globalnych instytucji finansowych jest wprowadzanie złośliwego oprogramowania *malware* do sieci wewnętrznych banku.

Jeden z najbardziej spektakularnych ataków w ciągu ostatnich lat na dużą międzynarodową instytucję finansową miał miejsce z małego oddziału dla zamożnych klientów w jednej z dzielnic Londynu. Pracownik po znalezieniu kluczy pozostawionych przez jednego z klientów z przypiętym nośnikiem USB chciał ustalić tożsamość roztargnionego właściciela kluczy na podstawie zawartości nośnika odczytując go na komputerze. W ten sposób wpuszczony

został do globalnej wewnętrznej sieci jeden z najbardziej złośliwych wirusów, którego usunięcie zajęło ekipom technicznym parę tygodni.

Jak widać posłużono się najsłabszym ogniwem w systemie zabezpieczeń – człowiekiem. W tym przypadku pracownikiem banku. Dlatego tak ważnym elementem profilaktyki stały się cykliczne szkolenia pracowników. Nie tylko w formie obowiązkowych szkoleń, lecz także coraz częściej interaktywnych gier, filmów czy spotkań, dzięki którym w bardziej kontrolowany sposób można dotrzeć i zweryfikować stan świadomości pracowników.

Bardzo pomocne są wszelakie studia przypadku pokazujące jak proste zaniedbania lub rutyna mogą doprowadzić do przeniknięcia niepożądanego oprogramowania do sieci banku. Im bardziej *case study* jest oparta na realnych osobach i sytuacjach zaczerpniętych z życia danej instytucji, tym większe jest zrozumienie zagrożenia i potencjalnych implikacji infiltracji. Pokazanie na prostych przykładach, jak drobne błędy, takie jak otwieranie nieznanych linków, dokumentów i wiadomości czy też korzystanie z prywatnego niezabezpieczonego sprzętu do celów służbowych może zakończyć się wymiernymi stratami dla banku.

Raport Accenture i HfS Research *The State of Cybersecurity and Digital Trust 2016*[8] na temat stanu cyberbezpieczeństwa w cyfrowej gospodarce identyfikuje pięć głównych luk w tym obszarze:

- Brak odpowiednio wykształconych zasobów ludzkich - chociaż wraz ze wzrostem automatyzacji prac operacyjnych jego ważność będzie malała.
- Problem z szybko rosnącym zagrożeniem i technologią, która umożliwiałaby szybką reakcję w przypadku wystąpienia takiego zagrożenia – remedium mogą być nowe technologie z obszaru bezpieczeństwa często oparte o uczenie maszynowe czy sztuczną inteligencję.
- Brak zrównoważonego rozwoju pomiędzy regionami powoduje, że organizacje przestępcze przeniosą swoje działania do krajów o mniejszych rygorach i stamtąd będą uderzały w kraje wysokorozwinięte.
- Braki odpowiednich nakładów, wynikające z presji rynku do obniżania cen produktów i usług, mogą powodować zmniejszenie nakładów na inwestycje w bezpieczeństwo.
- Luka w zrozumieniu tematów bezpieczeństwa pomiędzy specjalistami i kadrą kierowniczą.

8 https://www.accenture.com/t20160704T014005__w__/us-en/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Report-June.pdf

Raport pokazuje, że 69% respondentów miało do czynienia z atakami przeprowadzonymi przez osoby z wewnątrz organizacji w ciągu ostatniego roku. Pozytywnym komunikatem płynącym z raportu jest rosnąca świadomość wagi cyfrowego bezpieczeństwa zarówno w aspekcie ochrony fizycznych zasobów, jak i informacji w nich zawartych. Według raportu możemy oczekiwać w nadchodzących latach zagrożenia ze strony zorganizowanych grup przestępczych, które oceniane jest jako wysokie lub krytyczne przez 48% respondentów, natomiast wewnętrzne (bieżących lub byłych pracowników) tylko przez 28%, co w porównaniu do 31% oceniających zagrożenie ze strony kontraktorów i partnerów biznesowych oraz dostawców usług pokazuje wiarę i zaufanie do własnych pracowników.

Marcin Spychała
Dział Security, IBM

W ciągu ostatnich lat zajmował się projektowaniem systemów cyberbezpieczeństwa dla klientów IBM. W swojej pracy łączy praktyczną wiedzę o łamaniu zabezpieczeń z dobrym zrozumieniem rzeczywistych potrzeb klientów.
Wielki fan socjotechniki, co często demonstruje podczas konferencji oraz wydarzeń typu live hacking.
Posiada również głęboką wiedzę z zakresu regulacji prawnych dotyczących ochrony danych osobowych oraz legislacji dotyczącej cyberbezpieczeństwa w obrębie Unii Europejskiej.

Marcin Spychała, IBM

Medytacje o bezpieczeństwie pierwszym

Przechodząc ostatnio przez kontrolę bezpieczeństwa w Zurichu zostałem poproszony przez oficera bezpieczeństwa o wypakowanie wszystkich rzeczy z plecaka. Ku mojemu zdziwieniu z plecaka wyjąłem dawno zapomnianą butelkę perfum (co ważne: 125 mililitrów), z którą latałem od dobrych kilku miesięcy. Oczywiście perfumy musiałem zostawić na bramce bezpieczeństwa z poczuciem, że nie trafi ona wcale do kosza na śmieci. Ze złością (na bezduszne procedury bezpieczeństwa) zacząłem iść w stronę swojej bramki do wylotu, kiedy uderzyła mnie paradoksalność tej sytuacji. Przez kilkanaście miesięcy latałem po całej Europie z butelką perfum w bagażu podręcznym, która jawnie łamała podstawową regułę bezpieczeństwa lotów i byłem zadowolony, że nikt na nią nie zwraca uwagi, a zezłościłem się na to jedno lotnisko, gdzie poważnie i profesjonalnie potraktowano przepisy bezpieczeństwa. Przypomniało mi to historię sprzed kilku miesięcy, kiedy na prośbę znajomego zabezpieczyłem mu komputer dość podstawowymi acz skutecznymi środkami ochrony przeciw złośliwemu oprogramowaniu. Już dzień później ochroniło go to przed całkiem sprytnie pomyślanym atakiem typu *watering hole*. W ramach podziękowań zostałem poproszony o jak najszybsze odinstalowanie zabezpieczeń, gdyż cytuję „teraz na tym komputerze w ogóle nie da się pracować". Jak później odkryłem naprawdę chodziło o problemy z odtwarzaniem filmów w formacie Adobe Flash, którego to obsługę w przeglądarkach zawszę z przyzwyczajenia wyłączam.

Obie powyższe sytuacje uzmysłowiły mi, że powtarzana mantra o tym, że człowiek jest dla siebie największym zagrożeniem w Internecie jest nie tylko w dalszym ciągu prawdziwa, ale wraz z rozwojem technologii staje się coraz bardziej uciążliwa. Użytkownicy sieci, mimo że coraz bardziej świadomi zagrożeń, w dalszym ciągu jednak rozwijają swoją świadomość niebezpieczeństw dużo wolniej niż rozwijają się same zagrożenia. Sam zawodowo spędzam dużo czasu na poznawaniu nowych technik eksfiltracji danych i wiem, że nawet dla profesjonalisty ogarnięcie całości ekosystemu zagrożeń jest niemożliwe. Co dopiero dla laika. Z dobrych informacji, jest to również niemożliwe do ogarnięcia dla przeciętnego cyberprzestępcy, co jest zresztą powodem na coraz częstszą specjalizację usług podziemia cyberprzestępczego. Ale to jest temat na osobny artykuł.

Z perspektywy instytucji finansowej świadomość socjologicznych motywów reakcji ich klientów na utratę pieniędzy może się więc okazać kolejnym wielkim wyzwaniem. Tak samo jak ja nie doczekałem się podziękowania od znajomego, którego stację roboczą ochroniłem przed infekcją, tak samo bank może narazić się na negatywny PR zarówno jak utraci pieniądze klienta – ale, co ważniejsze – również kiedy w tym skutecznie przeszkodzi. Znalezienie złotego środka jest równie łatwe jak w dowcipie o mechaniku, który na prośbę klienta o usługę dobrą, tanią i szybką umożliwia wybranie dowolnych dwóch z powyższych charakterystyk. Niestety współczesny klient, który jest stale online wymaga i oczekuje usługi szybkiej, taniej i bezpiecznej. I ją często dostaje. A raczej wydaje mu się, że ją dostaje do momentu, kiedy pierwszy lepszy *overlay malware* wyprowadzi wszystkie środki z konta przez aplikację mobilną.

W latach 2015 i 2016 przy kilku okazjach miałem okazję wyrazić swoje zdanie na temat przyszłości cyberedukacji w kontekście ochrony bankowości elektronicznej. Zawsze byłem zwolennikiem podejścia mechanistycznego. Uważałem, że temat fraudów finansowych będzie można rozwiązać posiadając dostatecznie dużą ilość danych i odpowiednie modele. Obecnie jednak skłaniam się bardziej do podejścia humanistycznego, gdzie rola edukacji jednostki na nowo jawi się jako podstawowe remedium na wszechobecne cyberniebezpieczeństwa. Skupmy się zatem przez chwilę nad przyszłością. Na tym, w którym kierunkach powinna ewoluować edukacja społeczeństw w dobie informacyjnej. Współczesny dyskurs nad jakością tej edukacji, uwzględniający wielość kontekstów bezpieczeństwa jako domeny, powinien sprzyjać umiejętności planowania działań oświatowych na rzeczy stworzenia

bezpieczniejszej kultury i higieny pracy z Internetem. Warunkiem *sine qua non* będzie więc poznanie i zrozumienie istoty transformacji odbywającej się w przestrzeni cyberzagrożeń.

Będzie więcej tego, co już było

Spośród wszystkich pytań, jakie regularnie dostaję, jedno trafia do mnie zdecydowanie najczęściej. Jest to pytanie o najnowsze i przyszłe zagrożenia dla naszego bezpieczeństwa w sieci. Pytanie jakkolwiek bardzo trafne z perspektywy akademickiej, ale całkowicie niewłaściwe w kontekście najpopularniejszych zagrożeń. To trochę jak ze statystykami wypadków drogowych. Zdajemy sobie wprawdzie sprawę, że technicznie możliwe jest już zdalne przejęcie kontroli nad samochodem i spowodowanie nim wypadku – ale nadal za większość wypadków i ofiar śmiertelnych odpowiada prowadzenie po alkoholu i niedostosowanie szybkości do warunków drogowych[1]. Tak samo jest w przypadku cyberzagrożeń. Dlatego moją standardową odpowiedzią na to pytanie jest – „będzie więcej tego, co widzimy dotychczas". Więcej *phishingu*, więcej i lepiej sprofilowanych ataków socjotechnicznych oraz więcej *malware* finansowego opartego na znanym wcześniej, ale zmodyfikowanym kodzie[2]. Skoro tego typu ataki są w dalszym ciągu tak skuteczne, to nie spodziewam się, żeby w najbliższym czasie miało nagle dojść do przetasowania w czołówce tego peletonu zagrożeń.

Jest jeszcze jeden ważny powód, dla którego będziemy obserwować zalew znanych lub lekko zmodyfikowanych zagrożeń. Jeszcze kilka lat temu umiejętne przeprowadzenie ataku na aplikację bankową wymagało wiedzy, pieniędzy i zasobów informatycznych. Przestępca musiał kontrolować całość lub większą część infrastruktury ataku, co siłą rzeczy zawężało ilość osób mogących taki atak wykonywać. Globalizacja Internetu wraz z upowszechnieniem się usług i sieci anonimizujących umożliwiła większej ilości cyberprzestępców bezpośredni dostęp do komponentów cyberataku dostępnych coraz częściej w formie usługi „…as a Service". Wypożyczenie botnetu, kupienie złośliwego kodu, dostęp do centrum *Command & Control* na potrzeby przeprowadzenia ataku – to wszystko jest teraz prawie ogólnodostępne. Jak skutecznie przestępcy dbają o swoich klientów może świadczyć przykład kampanii

1 http://statystyka.policja.pl/st/ruch-drogowy/76562,Wypadki-drogowe-raporty-roczne.html

2 https://github.com/ytisf/theZoo/tree/master/malwares/Binaries

Dyre z 2014 i 2015 r., podczas której w anonimowej sieci I2P[3] działało centrum wsparcia ataku w trybie 24/7.

Obecnie jesteśmy w sytuacji, w której większość przestępców, tak samo zresztą, jak i większość użytkowników Internetu lub innych usług sieciowych opartych na WiFi, Bluetooth czy chociażby NFC, nie są w pełni świadomi zasad ich działania. To powoduje powstanie zagrożeń, z których nawet specjaliści w tych tematach nie zawsze zdają sobie sprawę. Chociaż w jednym przypadku akurat większość z nich jest i była zgodna.

„Powiedz swojemu telewizorowi, żeby przestał hakować moją lodówkę…"

Kiedy 22 września 2016 r. z sieci zniknęła strona Krebs on Security (http://krebsonsecurity.com/) niewielu chyba zdawało sobie sprawę z powagi tego pojedynczego zdarzenia. Ot, kolejny autor i bloger bezpieczeństwa padł ofiarą ataku DDoS. Jednak, jak się później okazało, wybór tego konkretnego celu ataku nie był przypadkowy. Pierwotnie sporo osób myślało, że jest to rodzaj zemsty na Brianie Krebsie w związku z aresztowaniem dwójki izraelskich hakerów prowadzących serwis do zlecania ataków DDoS – vDOS[4], jednak z czasem stało się jasne, że wybrano stronę jednego z najbardziej znanych blogerów i badaczy cyberbezpieczeństwa z powodów PR-owych. Zleceniodawca chciał rozreklamować swój nowy produkt – botnet/malware Mirai i wiedział, że zablokowanie strony Briana Krebsa na 4 dni da mu światową sławę. Tak się też stało. I mimo, że z czasem pojawiało się coraz więcej dowodów na to, że za stworzeniem Miraia stał producent rozwiązań Anti DDoS[5], to problem urządzeń IoT podłączonych do Internetu zyskał swoje pięć minut i, niestety, wcale nie został rozwiązany.

Dla przypomnienia – Botnet Mirai jest kolejną odsłoną botnetów atakujących urządzenia IoT przyłączone do sieci. Od 2014 r. widzieliśmy już przynajmniej kilka prób stworzenia światowej sieci zainfekowanych urządzeń IoT[6], ale dopiero Mirai udało się uzyskać odpowiednią skalę działania. Dzięki przyłączeniu do botnetu kilku milionów urządzeń możliwe było przeprowadzenie

3 *The Invisible Internet Project* – podobna do TORa sieć anonimowa o mniejszym zasięgu. https://geti2p.net/pl/comparison/tor

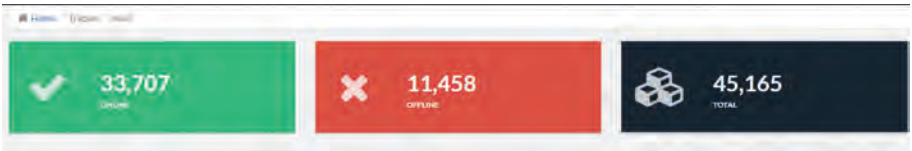
4 http://www.themarker.com/technation/1.3063772

5 https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/

6 Na przykład Bashlite, Gafgyt, Qbot, Remaiten czy Torlus

ataku DDoS o łącznej sile 620 Gbps na stronę Krebsa, o sile 1 Tbps na stronę OHV oraz znaczącego wkładu w październikowy atak na dostawcę usług DNS – Dyn. Z końcem stycznia br. do botnetu przyłączonych było jedynie około 38 000[7] urządzeń, więc sam w sobie nie stanowił już większego zagrożenia, ale należy pamiętać, że jego kod źródłowy jest publicznie dostępny w sieci, więc każdy posiadający wystarczającą wiedzę lub umiejący posługiwać się YouTubem może sobie w każdej chwili zrobić własny botnet.[8]

Rys. 1. Statystyki Botnetu Mirai (stan na 30 stycznia 2017 r.)



Zwłaszcza, że podstawowy problem z tym zagrożeniem nie został i prawdopodobnie nie zostanie wyeliminowany.

Świat IoT jest niesamowicie różnorodnym i rozwijającym się w niesamowitym tempie fenomenem. Mimo że samo określenie ma dopiero 19 lat[9], to Gartner przewiduje, że do 2020 r. do sieci będzie podpiętych ponad 20 mld urządzeń. Osobiście uważam te estymacje za zbyt ostrożne. I tak jak opracowanie standardów WWW znacząco przyśpieszyło propagację Internetu, tak upowszechnienie się niskoenergetycznych standardów WiFi i Bluetooth znacząco wpłynęło na rozwój urządzeń IoT podpiętych do sieci. I w chwili obecnej mamy ponad pięć mln de facto komputerów podpiętych do sieci na których, upraszczając, nie można w większości przypadków ani zainstalować oprogramowania antywirusowego ani przeprowadzić patchowania wykrytych luk. Tego typu beztroska w przypadku komputerów stacjonarnych podpiętych do sieci wydaje się nieprawdopodobna. Zresztą najlepszym przykładem obrazującym powagę sytuacji jest właśnie szybkość i łatwość infekcji urządzeń w ramach botnetu Mirai. Mirai komunikuje się z urządzeniami wykorzystując w większości przypadków protokół telnet oraz hasła standardowe lub konta serwisowe. Aby zainfekować ponad 7 mln urządzeń na całym

7 https://intel.malwaretech.com/botnet/mirai/?t=24h&bid=all

8 https://www.youtube.com/watch?v=A0Z-6rnL1zw

9 Pierwszy użył tego określenia Kevin Ashton w 1999 odnosząc się do sieci urządzeń komunikujących się w standardzie RFID

świecie (szczytowa wielkość botnetu), autor wykorzystał i na sztywno wpisał w kod *malware* jedynie 68 par użytkownik/hasło.

Rys. 2. Użytkownicy i hasła malware Mirai[10]

```
// Set up passwords
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                 // root     xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x48\x58\x5A\x54", 9);                      // root     vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x48\x4C", 8);                      // root     admin
add_auth_entry("\x43\x46\x4F\x48\x4C", "\x43\x46\x4F\x48\x4C", 7);                  // admin    admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                  // root     888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x48\x52\x41", 5);              // root     xmhdipc
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);              // root     default
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);          // root     juantech
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);                  // root     123456
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                      // root     54321
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);  // support  support
add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                          // root     (none)
add_auth_entry("\x43\x46\x4F\x48\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);      // admin    password
```

Kiedy kilka lat temu zaczynałem publicznie mówić o cyberbezpieczeństwie – przykładem niebezpiecznego zachowania było pozostawienie standardowego użytkownika i hasła na routerze w sieci domowej. Dzisiaj powinno się raczej zadać pytanie czy zmienione zostało hasło administratora w telewizorze w salonie, kamerze internetowej i lalce Barbie, którą córka dostała pod choinkę.[11]

„Proszę zresetować nazwisko panieńskie matki…"

Kiedy w 2014 r. na konferencji *Chaos Communication* Jan Krissler zademonstrował, jak za pomocą zdjęć w wysokiej rozdzielczości można skopiować odciski palców i oszukać urządzenia do biometrycznego uwierzytelniania[12], jasnym się stało, że rynek uwierzytelnień czeka burzliwy czas. Z perspektywy instytucji finansowej jednoznaczne uwierzytelnienie osoby realizującej transakcje jest oczywiście kluczowe. Samą teorię uwierzytelniania mamy bardzo dobrze opisaną – problem tkwi nie w samej teorii, ale w jej implementacji i poprawnym stosowaniu. A jak wcześniej pisałem, założenie, że usługi finansowe mają być szybkie, dobre i bezpieczne nie uwzględnia niestety miejsca

10 https://github.com/jgamblin/Mirai-Source-Code/blob/master/mirai/bot/scanner.c

11 https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children

12 https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands

dla rozbudowanych polityk bezpieczeństwa. Co więcej, banki już dawno mają techniczną możliwość quasi-biometrycznego identyfikowania swoich klientów (np. sposoby interakcji z interfejsem, pisania na klawiaturze czy ruszania myszką). Są to typowe przypadki dynamicznej charakterystyki biometrycznej. Niemniej jednak wykorzystując tego typu narzędzia wchodzimy w delikatny i nie do końca zdefiniowany prawnie obszar prywatności i dostępu do danych wrażliwych. W 2018 r. po wejściu w życie regulacji GDPR dane biometryczne (wreszcie) będą podlegały ochronie jako dane osobowe, więc przynajmniej w ramach EU będzie ustanowiony wspólny standard. Ale wcale nie jest powiedziane, że użytkownicy usług sieciowych, coraz mniej chętnie zgadzający się na zbieranie o nich danych w sieci, będą chcieli poświęcić tę część prywatności na rzecz dodatkowego biometrycznego uwierzytelnienia. Są pewne przesłanki mówiące, że tak będzie. Przede wszystkim to, co jest najważniejsze z perspektywy uwierzytelnienia biometrycznego – wygoda, która w tym przypadku jest niedościgniona. Zawsze i wszędzie mamy samego siebie ze sobą. Dodatkowo dane biometryczne są (przynajmniej na razie) trudniejsze do pozyskania niż nasze hasła czy dane karty kredytowej. I, co nie mniej ważne, danych do uwierzytelnienia nie jesteśmy w stanie przekazać innej osobie, tak jak PIN do karty.

Niestety, są też poważne zagrożenia idące z powszechnym stosowaniem pojedynczego uwierzytelniania biometrycznego. Po pierwsze, na razie nie wymyślono działającego rozwiązania problemu resetowania danych biometrycznych na wypadek chociażby wycieku takich danych do sieci. Oczekiwanie, że tego typu dane nie wyciekną, jest zwykłą naiwnością. Są pewne propozycje rozwiązania tego problemu[13], ale nie widziałem ich nigdzie wdrożonych produkcyjnie. Po drugie, brakuje w dalszym ciągu poważnej dyskusji o konsekwencjach błędów uwierzytelnienia biometrycznego. Jak rozpoznać prawowite uwierzytelnienie odciskiem palca od uwierzytelnienia transakcji płatniczej przez 6-latkę używającą palca śpiącej matki[14], pozostaje otwarte.

Dodatkową przeszkodą w powszechnym stosowaniu danych biometrycznych jest też fakt, że już teraz mogą być one pobierane i przetwarzane całkowicie bez naszej zgody a nawet wiedzy, czego najlepszym przykładem jest wspomniane przeze mnie skopiowanie odcisków palca ze zdjęcia. Jeszcze

13 http://www3.wcoomd.org/files/2.%20Event%20files/PDFs/Biometrics/13-ratha.pdf

14 https://securityintelligence.com/hacked-by-a-kid-a-story-to-illustrate-the-state-of-authentication-today/

łatwiej jest zebrać dane z dowolnej restauracji lub kawiarni, gdzie zostawiamy przecież nasze odciski na szklankach czy sztućcach. Nie wspominając już o wszechobecnych kamerach, które zbierają dane nie tylko o wyglądzie naszej twarzy, ale również o sposobie chodzenia.

Popularyzacja uwierzytelnienia biometrycznego wydaje się nieunikniona. Co za tym idzie, spopularyzują się również ataki na tego typu zabezpieczenia. Świadomość i sposoby ochrony danych biometrycznych muszą się stać przedmiotem ogólnospołecznej dyskusji. Zarówno dla popularyzacji idei, jak i dla zaadresowania możliwych lęków społecznych powstałych chociażby po rewelacjach Edwarda Snowdena. Wielopoziomowe kształtowanie świadomości jednostek powinno być tutaj podstawową troską procesów edukacyjnych, gdyż warunkuje treść, kierunek i metody ludzkich działań. Co pozostaje nie bez znaczenia w konsekwencji takich programów, jak np. Indyjski Aadhaar[15].

Pański portfel kryptowaluty… nie mamy go już

Po tym, jak w październiku 2016 r. z sieci zniknęła polska giełda Bitcoin Bitcurex wraz ze wszystkimi środkami zgromadzonymi w portfelach uczestników, do masowej świadomości trafiła informacja, że pomimo iż sam *bitcoin* (a raczej protokół *blockchain*) oparty jest na zaawansowanych algorytmach kryptograficznych – nadal istnieje niezerowa szansa na zostanie okradzionym.[16]

Patrząc z perspektywy ostatnich ośmiu lat myślę, że nawet sam Satoshi Nakamoto nie przewidywał sukcesu zaproponowanej przez niego kryptowaluty. Obecnie łączna kapitalizacja rynku kryptowalut to ponad 14 mld dolarów. Wprawdzie mocno dominującą pozycję z tym zestawieniu zajmuje Bitcoin[17], to na świecie obecnie mamy w obrocie 719 kryptowalut. Dla porównania, walut w klasycznym tego słowa rozumieniu mamy obecnie 180[18]. I to wszystko w niecałe osiem lat od opublikowania krótkiego 8-stronicowego tekstu „*Bitcoin: A Peer-to-Peer Electronic Cash System*".

Ciężko jednoznacznie określić, które z istniejących zagrożeń dla kryptowalut okaże się dominujące w najbliższej przyszłości. Na chwilę obecną najbardziej zagraża jej to, co również przez wielu jest postrzegane jako największy

15 https://en.wikipedia.org/wiki/Aadhaar

16 Najprościej wpisać frazę „bitcoin exchange shuts down" w dowolnej wyszukiwarce

17 Szacuje się że około 85% kapitalizacji kryptowalut stanowi Bitcoin

18 https://en.wikipedia.org/wiki/List_of_circulating_currencies

plus kryptowalut – jej niezależność od uregulowanego rynku finansowego. Obecnie każdy może stworzyć własną kyptowalutę a nawet giełdę kryptowalut bez większych problemów i niczyich zgód. Nieuregulowanie tego rynku jest jego największą zaletą, ale również przyciąga przez to osoby o nieuczciwych zamiarach. Jest to niejako naturalna konsekwencja faktu, że kryptowaluty (przy wszystkich swoich korzyściach w legalnych zastosowaniach) stały się de facto standardem w płatnościach za nielegalny towar i usługi w sieci.

Patrząc na zagrożenia dla kryptowalut z perspektywy technologicznej mamy również do czynienia z kilkoma możliwymi zagrożeniami. Pierwszym i najpoważniejszym problemem dla wszystkich PUBLICZNYCH usług opartych na *blockchainie* będzie zapewnienie odpowiedniej skali przetwarzania. Jedną z największych korzyści stosowania technologii łańcucha bloków jest jego niezaprzeczalność. Każdy blok łańcucha zawiera w sobie hash poprzedniego, przez co podrobienie któregokolwiek z jego elementów jest od razu widoczne. Tak długo jak większość (a konkretnie przynajmniej 51% użytkowników łańcucha) jest uczciwa – jego bezpieczeństwo i niezaprzeczalność są zapewnione. Problem pojawia się, kiedy atakujący posiada przynajmniej 51% mocy obliczeniowej w łańcuchu. Wtedy ma możliwość manipulowania powstającymi hashami (tak zwany atak 51%). Ta czysto matematyczna możliwość ataku została, niestety, już praktycznie udowodniona w czerwcu 2016 r., kiedy nastąpił udany atak 51% na dwie platformy oparte na Ethereum – Krypton (KR) i Shift (SHF). Do ataku na oba serwisy została wykorzystana moc obliczeniowa wydzierżawiona od dostawców usług obliczeniowych w chmurze[19]. To pokazuje, że obecnie takie ataki są całkowicie wykonalne. Co więcej, przy odpowiedniej skali, opłacalne jest wykorzystanie mocy obliczeniowej superkomputerów, coraz tańszego przetwarzania w chmurze czy ostatecznie przetwarzania w oparciu o komputery kwantowe. Sam *Bitcoin*, właśnie ze względu na swoją skalę, wydaje się odporny na tego typu ataki, ale pozostaje jeszcze przeszło 700 walut działających w dużo mniejszych społecznościach. Szczęśliwie zaczynają się pojawiać teoretyczne modele zabezpieczenia sieci kryptowalut przez atakiem typu 51%.[20] Musimy jedynie zaczekać na ich praktyczną implementację i weryfikację przez rynek. Niemniej jednak wymyślono już sposoby kradzieży kryptowalut, w tym Bitcoina, przed którymi tak naprawdę trudno się zabezpieczyć. Na szczęście są to przypadki na tyle

19 Paradoksalnie był to NiceHash – jedna z największych koparek kryptowalut

20 https://eprint.iacr.org/2016/716.pdf

trudne do zaimplementowania, że z perspektywy całego rynku można uznać je za pomijalne. Na razie.

W 2014 r. zespół badaczy z laboratorium SecureWorks podał do wiadomości, że wykrył sposób na kradzież strumienia wykopanych kryptowalut bezpośrednio z sieci z wykorzystaniem dobrze znanego teoretycznego zagrożenia dla protokołu BGP (*BGP Hijacking*). *BGP Hijacking* był już dyskutowany jako potencjalne zagrożenie dla Internetu, kiedy w 1998 r. grupa hakerów L0pht opowiedziała przed Amerykańskim Kongresem o możliwości wyłączenia całego Internetu w niecałe 30 minut. Schemat ten zyskał również chwilową popularność w 2008 r. na konferencji DefCon oraz w 2012 r., kiedy spora część ruchu internetowego została czasowo (i w dość tajemniczy sposób) przekierowana z USA do Islandii i na Białoruś. Ta sama podatność została teraz wykorzystana przez przestępców w celu wyprowadzania z sieci bitcoin, dogecoin i worldcoin waluty w tempie 9 000 USD dziennie. Wszyscy są w miarę zgodni, że będziemy obserwować więcej tego typu ataków w przyszłości.

Najpierw w lewo potem w prawo i jeszcze raz w lewo

Nasze dzieci świetnie wiedzą, jak bezpiecznie przechodzić przez ulicę. Nie wszystkie to praktykują, ale kiedy trzeba, potrafią się do tego dostosować. Dlaczego tak się dzieje? Bo mają tę wiedzę wpajaną od najmłodszych lat zarówno prze rodziców, jak i przez edukację instytucjonalną i programy społeczne. Z zagrożeniami w cyberprzestrzeni jest podobnie i tu także trzeba przyjąć podobne metody edukacji, żeby wychować cyberbezpieczne pokolenie. Jest to o tyle trudniejsze, że wśród starszego pokolenia wiedza o cyberzagrożeniach dopiero się kształtuje. Najlepszym przykładem są coroczne zestawienia najpopularniejszych haseł stosowanych w Internecie. Od lat niekwestionowanym liderem haseł (którego definicją jest w końcu: „ciąg znaków stosowany powszechnie jako *tajny* parametr w kryptografii oraz uwierzytelnianiu") jest 123456 oraz 12345678. Oparcie jakiegokolwiek zabezpieczenia na tego typu haśle zakrawa na szaleństwo – a jednak. Zresztą brak instynktów samozachowawczych użytkowników w sieci można zaobserwować każdorazowo przy wycieku haseł z jakiegokolwiek serwisu internetowego. Ponad 30% haseł do serwisu Ashley Madison zostało złamanych w pierwszych 10 dniach od wycieku, a ich analiza[21] pokazuje, że nawet osoby, które chcą ukryć swoją tożsa-

21 http://www.zdnet.com/article/these-are-the-top-100-passwords-from-the-ashley-madison-hack/

mość nie rozumieją podstawowych zasad konstrukcji mocnych zabezpieczeń. Inna sprawa, że badania Lorrie Faith Cranor[22] z Uniwersytetu Carnegie Mellon pokazują, iż wymagalność stosowania skomplikowanych zabezpieczeń nie poprawia wcale stopnia bezpieczeństwa chronionych zasobów.

Jaka więc czeka nas przyszłość? Na razie w miarę spokojna i przewidywalna co do możliwych zagrożeń. Ciekawiej zacznie się dziać w momencie, kiedy testowana obecnie sztuczna inteligencja zacznie być wykorzystywana do automatyzowania procesu przełamywania zabezpieczeń. Wydarzenia takie jak *DARPA Cyber Grand Challenge*[23] czy projekty *Google Brain* zabezpieczania komunikacji metodami niezrozumiałymi dla człowieka[24] pokazują, że poszukiwanie zabezpieczeń ostatecznych w oparciu o komputery niepopełniające ludzkich błędów jest już na wyciągnięcie ręki. Nadzieja, że osiągnięcia te nie zostaną wykorzystane również do łamania zabezpieczeń jest mocno naiwna. Na końcu i tak wygra ten, kto będzie miał większy komputer.

Wracając więc jeszcze raz do mojej przygody z kontrolą bezpieczeństwa w Zurichu. Po chwili refleksji musiałem sam przed sobą się przyznać, że mimo utraty perfum i spędzeniu na kontroli większej niż zwykle ilości czasu, to właśnie takie podejście sprawiło, że czułem się bezpieczniej. Jednak fakt, że przez chwilę sam kwestionowałem zasady bezpieczeństwa na potrzeby własnej wygody dał mi sporo do myślenia, ile jeszcze mamy do zrobienia w kwestii edukacji cyberzagrożeń. I to zarówno w kwestii edukacji społeczeństwa, jak i dopasowywania legislacji (zaczynając od nieszczęsnego art. 269b KK).

22 https://www.ted.com/talks/lorrie_faith_cranor_what_s_wrong_with_your_pa_w0rd

23 http://www.darpa.mil/news-events/2016-08-05a

24 https://arxiv.org/abs/1610.06918

Aleksander P. Czarnowski
Prezes AVET Information and Network Security sp. z o.o.

Jego firma od 17 lat zajmuje się konsultingiem w zakresie bezpieczeństwa informacji w Polsce, Rumunii, Holandii i Wielkiej Brytanii oraz na Ukrainie i Słowacji. On sam jest Członkiem 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 Information and Network Security

Ochrona danych osobowych a bezpieczeństwo rozwiązań bankowych

Ochrona danych osobowych zawsze była istotnym elementem zarządzania bezpieczeństwem informacji w sektorze bankowym. Jednak zmiany legislacyjne i technologiczne powodują, że zagadnienie to staje się coraz większym wyzwaniem, zwłaszcza na rok przed wejściem w życie GDPR (General Data Protection Regulation, znane także jako RODO – Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/67 z dnia 27 kwietnia 2016 r. w sprawie ochrony danych osobowych) a także PSD II na horyzoncie.

Istotne zmiany wprowadzane przez GDPR

Wysokopoziomowo GDPR wprowadza trzy istotne zmiany względem dotychczasowych regulacji:

1. Wysokie kary finansowe: 20 mln euro lub 4% globalnego obrotu.
2. Powiadomienie (notyfikację) o naruszeniu bezpieczeństwa danych osobowych zarówno organ nadzorujący, jak i osoby, których bezpieczeństwo danych zostało naruszone.
3. Bezpieczeństwo oraz ochrona prywatności mają być domyślne i wbudowane w systemy przetwarzające dane.

Już z powyższej listy wynika, że nawet jeśli dzisiaj dysponujemy opinią o zgodności z aktualnie obowiązującym prawem, zgodność ta w większości

przypadków nie oznacza braku potrzeby dodatkowych działań. W praktyce bowiem, i to nie tylko w sektorze bankowym, ale także i poza nim, nikt nie implementował wcześniej np. mechanizmów do notyfikacji. Niewiele też systemów było projektowanych i budowanych według zasady *secure by default* lub – bardziej w nomenklaturze GDPR – *privacy by design and by default*, czyli wymogu zapewnienia ochrony danych osobowych zawsze i w sposób domyślny. W tym miejscu warto zaznaczyć, że dużymi wygranymi okazali się ci dostawcy i odbiorcy, którzy zaczęli kilka lat temu wprowadzać programy typu *Secure Development Lifecycle* (SDL), pozwalające ustanowić wewnątrz organizacji proces wytwarzania bezpiecznego oprogramowania. Udaje się to zarówno w modelu *waterfall*, który już po woli odchodzi do lamusa, jak i aktualnie popularnym podejściu *agile*. W każdym programie SDL u jego podstaw leżą bowiem obie zasady wspomniane powyżej. Co więcej proces wytwarzania bezpiecznego oprogramowania zawiera w sobie fazę jego projektowania, dzięki czemu bez większych problemów można dodać na tym etapie nowe wymogi GDPR.

Innym ważnym spostrzeżeniem, jakiego należy dokonać jest fakt, że właściwie tylko podejście oparte o zarządzanie ryzykiem ma szanse – z biznesowego punktu widzenia – wytrzymać zderzenie z rzeczywistością. Dla sektora bankowego to z pewnością dobra wiadomość, bo proces zarządzania ryzykiem operacyjnym nie jest niczym nowym. Konsekwencją tego spostrzeżenia musi być więc selekcja zabezpieczeń na podstawie szacowania ich siły oraz analizy ryzyka. Jest to element od kilku lat pojawiający się w normie ISO 27001, ale podejście to pojawiło się częściowo także w systemach zarządzania jakością ISO 9001.

Należy także zwrócić uwagę na bardziej szczegółowe zmiany, jakie niesie za sobą wejście w życie GDRP, a w szczególności:

- Szczegółowy przepływ danych osobowych: kto, kiedy, gdzie, jak i po co ma do nich dostęp.
- Rozliczność w zakresie dostępu do danych osobowych i ich przetwarzania.
- Właściwa polityka logowania zdarzeń i ślad audytu.
- Aktualne inwentaryzacja zasobów w odniesieniu do przetwarzania danych osobowych.
- Stałe monitorowanie bezpieczeństwa.

- Ochrona danych osobowych poprzez ich szyfrowanie. Nie jest to jednak jedyne wymagane zabezpieczenie – należy w tym miejscu podkreślić, że GDPR wymaga mechanizmów kontrolnych o wysokiej efektywności. Samo wdrożenie szyfrowania nie uchroni nas od kary finansowej w przypadku incydentu, jeśli okaże się, że zabezpieczenie zostało błędnie wdrożone lub tylko po to, aby zadowolić regulatora.

Mikroserwisy, kontenery i ochrona danych

Jednym z ważnych trendów w tworzeniu aplikacji jest obecnie wykorzystanie mikroserwisów. Jest to podejście odwrotne do tego stosowanego jeszcze niedawno, kiedy to do działania aplikacji wymagane było tylko kilka serwisów sieciowych, takich jak DNS czy HTTP. Dzisiaj aplikacje budowane są z gotowych klocków, a każdy z nich może składać się z jednego lub więcej mikroserwisów. Czasami nawet pojedynczy widok w aplikacji webowej lub mobilnej do prawidłowego funkcjonowania potrzebuje bowiem więcej niż jednego.

Do mikroserwisów idealnie pasują kontenery, do popularyzacji których z pewnością przyczynił się pakiet Docker. Obecnie zarówno system Linux, jak i Windows natywnie wspierają kontenery, co powoduje dalszy wzrost ich popularności. Można je także uruchamiać bez większego problemu u wszystkich czołowych dostawców chmury.

Czym jest kontener? Wyobraźmy sobie, że wszystkie istotne elementy potrzebne do działania danego serwisu mamy zamknięte w jednym pudełku. Co więcej, zawiera ono komponenty charakterystyczne tylko dla tego właśnie serwisu i to bez elementów wspólnych z innymi. W przypadku, gdy serwis potrzebuje zewnętrznego, złożonego zasobu, jakim jest np. system bazodanowy może on być także zamknięty w osobnym, dedykowanym pudełku, czyli oddzielnym kontenerze. Wszystkie one częściowo współdzielą zasoby systemu operacyjnego, korzystając przykładowo z dostępnego systemu plików i wolnej przestrzeni, jednak nie będąc od siebie zależnymi, chyba, że zostały ten sposób skonfigurowane. Jeśli nie, to nie mogą współdzielić z innymi kontenerami swoich zasobów. Ta możliwość izolacji od siebie komponentów, danych, serwisów i aplikacji wpływa bardzo korzystnie na możliwość zmniejszania powierzchni ataku. Im jest bowiem ona mniejsza, tym mniejsze ryzyko wystąpienia incydentu, a w konsekwencji także niższe ryzyko operacyjne.

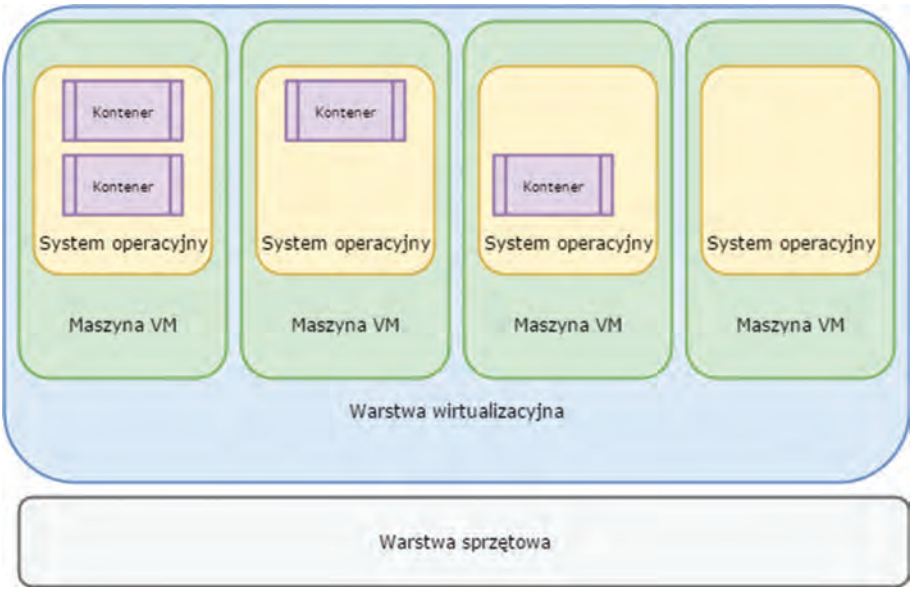
Koncepcja powierzchni ataku ma także istotne zastosowanie w kontekście wymagań GDPR. Proszę zwrócić uwagę, że koncepcja separacji od siebie komponentów nie pochodzi tylko z obszaru ochrony danych osobowych. Jest to także elementarny wymóg w przypadku ochrony informacji niejawnych oraz danych kartowych w myśl *PCI DSS*.

Należy jednak zwrócić uwagę na fakt, że – zgodnie z teorią bezpieczeństwa systemów IT – im większa liczba serwisów, tym większa jest powierzchnia ataku. Okazuje się więc, że w praktyce zalety z perspektywy bezpieczeństwa kontenerów nie zawsze mogą zrównoważyć wzrostu ryzyka związanego z rosnącą liczbą (mikro)serwisów.

Po drugie, separacja za pomocą kontenerów niesie za sobą jeszcze dwa istotne problemy:

- Wraz ze wzrostem liczby kontenerów rośnie złożoność procesów administrowania nimi. Bez adekwatnych mechanizmów automatyzujących ten proces praktycznie nie można mówić np. o działającym procesie *patch management*. Z kolei rozwiązania służące do instrumentacji lub zarządzania kontenerami są wymarzonym – podobnie jak interfejsy administracyjne platform wirtualizacyjnych – celem ataków. Przejęcie kontroli nad elementem zapewniającym scentralizowane zarządzanie praktycznie powoduje przełamanie większości, jeśli nie wszystkich zabezpieczeń.
- Ochrona danych osobowych wymaga ich bezpiecznego usunięcia po zakończeniu przetwarzania. W teorii kontenery są idealnym rozwiązaniem tego problemu, ponieważ można je tworzyć i niszczyć na zawołanie. Raz zniszczonego kontenera nie można już odzyskać. Niestety, na skutek wewnętrznej implementacji może okazać się, że dane – przynajmniej częściowo, np. w pamięci *swap* – jednak przetrwały zniszczenie kontenera. Dlatego tak istotne jest wprowadzanie wielowarstwowości zabezpieczeń. Drugim problemem jest rozliczalność: jeśli zniszczono kontener a nie dokonano eksportu logów z niego, zniszczono tym samym ślad audytu. Podobny problem występuje w przypadku incydentu: jeśli atakujący zniszczy kontenery, które spenetrował, zatrze też dość skutecznie dużą cześć dowodów.

Rys. 1. Relacja pomiędzy warstwą wirtualizacyjną, systemem operacyjnym a kontenerami



Szyfrowanie danych

Umyślnie rozpocząłem dyskusję od mikrosewisów i kontenerów przesuwając zabezpieczenia kryptograficzne na dalszy plan, ponieważ panuje powszechne, chociaż błędne przekonanie o tym, że szyfrowanie danych to definitywna odpowiedź na wszystkie kłopoty związane z ochroną danych osobowych.

Szyfrowanie jest niezwykle ważnym zabezpieczeniem i ma zastosowanie nie tylko w przypadku transmisji danych, np. pomiędzy przeglądarką a systemem bankowości elektronicznej, ale także np. na poziomie maszyn wirtualnych, baz danych (lub wybranych tabel, kolumn a nawet wierszy) czy systemów plików a także pamięci typu *swap*. W dalszej kolejności szyfrowanie może obejmować kopie zapasowe, środowiska testowe i zapasowe itd.

Niektóre z wymienionych mechanizmów szyfrowania są już dostępne od dawna w określonych rozwiązaniach a nawet domyślnie włączone. Dotyczy to np. wielu systemów operacyjnych i szyfrowania pamięci *swap*.

Największą słabością każdego zabezpieczenie kryptograficznego jest to, że w wielu przypadkach dane zaszyfrowane muszą być co jakiś czas

rozszyfrowywane. Na szczęście nie zawsze tak się musi dziać. W przypadku porównania hasła podczas uwierzytelnienia można np. wyliczyć jego funkcję skrótu i tylko uzyskany wynik porównywać z zaszyfrowanymi hasłami w bazie danych. Oczywiście, takie podejście ma pewne wady, np. w przypadku wykorzystania wielu permutacji haseł maskowanych. Z perspektywy bezpieczeństwa ma jednak oczywistą zaletę.

Zazwyczaj jednak dane w ramach przetwarzania muszą być rozszyfrowane. Jeśli na tym etapie atakujący uzyska do nich dostęp lub po prostu wycieknią, mechanizmy kryptograficzne stają się bezużytecznym zabezpieczeniem. Innym problemem jest potencjalny wyciek sekretu używanego do szyfrowania lub podpisywania danych oraz generowania np. certyfikatów. Jeśli atakujący uzyska dostęp do tej informacji będzie mógł nie tylko odszyfrować zaszyfrowane dane, ale także np. składać ważne podpisy elektroniczne czy generować pełnoprawne certyfikaty.

Biorąc pod uwagę powyższe słabe punkty każdego kryptosystemu widać wyraźnie, że z perspektywy bezpieczeństwa a nie tylko samej ochrony danych osobowych wymagane są także inne zabezpieczenia, pozwalające skutecznie zapobiegać i wykrywać próby opisanych ataków.

Należy przy tym zwrócić uwagę, że w implementacjach rozwiązań kryptograficznych także potrafią się znajdować podatności i to nierzadko niezwykle groźne. Idealnym przykładem może być biblioteka OpenSSL oraz podatność *heartbleed*, która trzy lata po jej opublikowania nadal występuje w setkach tysięcy urządzeń podłączonych do internetu.

Podsumowując, szyfrowanie nie może być jedynym mechanizmem kontroli dostępu. Może jednak doskonale wspierać inne zabezpieczenia w tym obszarze, np. gdy dane są w tranzycie.

Ochrona danych osobowych a Polski sektor bankowy

W tym miejscu warto zwrócić uwagę na pewne istotne, charakterystyczne tylko dla polskiego sektora bankowego trendy. Nie jest to kompleksowa analiza sytuacji w zakresie ochrony danych osobowych, bowiem takie opracowanie wymagałoby odrębnej, znacznie obszerniejszej publikacji, która, zapewne, gdyby była kompletna, po dniu jej publikacji byłaby już nieaktualna. W zamian za to są praktyczne spostrzeżenia wybrane w sposób subiektywny przez autora.

Konsolidacja sektora i połączenie z sektorem ubezpieczeniowym

Jesteśmy świadkami silnej konsolidacji polskiego sektora bankowego oraz sektora bankowego z sektorem ubezpieczeniowym. Ma to istotne znaczenie z perspektywy przetwarzania i ochrony danych osobowych – oto banki w pośredni lub bezpośredni sposób zyskują dostęp do danych wrażliwych, takich jak dane medyczne. Następuje więc koncentracja zbiorów danych osobowych – zarówno od strony właścicielskiej, jak i, w konsekwencji, także systemowej. Koncentracja niesie ze sobą jeszcze jeden problem: otóż rośnie liczba systemów i aplikacji, które wymagają ochrony, monitorowania i zapewnienia zgodności chociażby z GDPR. Po drugie, rośnie także liczba systemów *legacy* w pojedynczych organizacjach, które obecnie stanowią w bankowości olbrzymi problem z perspektywy zarządzania bezpieczeństwem.

Chmura jest „be"

Polski sektor finansowy, a w szczególności bankowy nie lubi chmury, a zwłaszcza chmury publicznej. Rodzi to ciekawą schizofrenię polegająca na tym, że w wielu bankach słyszy się tę samą, ale nieprawdziwą, opinię, że korzystanie z chmury jest zabronione prawnie. Z drugiej strony, ten sam bank kupuje oprogramowanie pracujące tylko w chmurze, bo nie ma dostępnych już innych wersji. Nie wiem skąd bierze się to mylne przekonanie – zwłaszcza w dużych bankach komercyjnych – o niemożliwości korzystania z chmury na skutek regulacji prawnych.

Na drugim krańcu spektrum są niektóre Banki Spółdzielcze, które często jako pierwsze korzystały z outsourcingu i dzisiaj także potrafią brać udział w ciekawych projektach chmurowych. Banki Zrzeszające także prowadzą lub mają pomysły na takie projekty. Innym przypadkiem są Banki Samochodowe: w ich przypadku zdarza się, że w ramach BCP/DRP świadczą one usługi odtworzeniowe dla zagranicznych oddziałów. Nadal jednak wykorzystanie chmury w polskim sektorze bankowym jest niezwykle ograniczone – nie jest to jednak cecha charakterystyczna sektora bankowego. Sektor publiczny i rządowy wyglądają w Polsce jeszcze gorzej pod tym względem. Co ciekawe, istnieją dzisiaj standardy pozwalające bezpiecznie przetwarzać dane w chmurze, np. ISO 27017 i 27018. Aktualna wersja Rekomendacji D także definiuje pojęcie *cloud computing*.

Być może tę sytuację zmienią fintechy, które na skutek akwizycji przez banki będą także wnosiły chmurę z dobrodziejstwem inwentarza. Trudno bowiem sobie dzisiaj wyobrazić startup, który nie korzystałby z chmury a budował całą infrastrukturę sieciową i aplikacyjną od zera u siebie. To z kolej rodzi problem ochrony danych osobowych, które można bezpiecznie i zgodnie z prawem przetwarzać w chmurze, ale po spełnieniu określonych warunków.

Blockchain

Z blockchainem jest jak z chmurą – wszyscy o niej mówią, ale mało kto w polskim sektorze bankowym z niej korzysta. Dlatego ograniczę się tylko do stwierdzenia, że konstrukcja blockchain może wydawać się bardzo atrakcyjna z perspektywy bezpieczeństwa. Jednak w ujęciu danych osobowych może przysporzyć pewnych trudności, podobnie jak było w przypadku chmury. Rozproszona struktura ułatwia ochronę przed atakami, zwłaszcza klasy DoS/DDoS, ale nie ułatwia identyfikacji miejsc, w których dane są przetwarzane. Z drugiej strony, wiele z tego typu potencjalnych problemów rozwiązano już przy okazji chmury, gdzie np. pojawia się definicja danych w tranzycie. Niektóre zagadnienia są jednak nadal dyskutowane, także na poziomie Komisji Europejskiej. Dobrym przykładem może być wspomniana już kilkakrotnie tematyka bezpiecznego usuwania danych.

SIEM jako spełnienie wymogów GDPR

Systemy klasy SIEM na poważnie pojawiły się w polskich bankach na skutek punktu 20.7 Rekomendacji D KNF, kiedy to nagle okrzyknięto, że każdy z nich musi go posiadać. Rekomendacja ta jest jednak z goła odmienna: mówi ona, że bank powinien przeanalizować zasadność użycia takiego systemu. I brać się za jego wdrożenie dopiero wtedy, gdy okaże się, że jest to konieczne. Niezrozumienie tego spowodowało, że prawie wszystkie banki w Polsce, w tym Banki Spółdzielcze, wdrożyły takie systemy z bardzo różnym skutkiem.

Systemy klasy SIEM wyglądają atrakcyjnie z perspektywy wymagań GDPR w obszarze potencjalnego zastosowania ich do wykrywania incydentów a następnie notyfikacji. Niestety, rzeczywistość jest bardziej skomplikowana. Otóż, aby systemy te były użyteczne, tzn. mogły pomóc cokolwiek wykryć najpierw muszą być spełnione minimum dwa warunki:

- Źródła zdarzeń, które są pobierane do systemu SIEM muszą być dobrej jakości i ustabilizowane.
- Aplikacje, które przetwarzają dane osobowe muszą zapewniać właściwy audyt zdarzeń.

Okazuje się, że wiele – w tym kluczowych – systemów nie oferuje adekwatnego audytu zdarzeń z perspektywy GDPR. Co więcej, w przypadku systemów *legacy* nie ma szansy na zmianę tego stanu rzeczy. Innym problemem przy skali działalności banku i jego systemów może być kwestia pobierania zdarzeń do aplikacji SIEM. Mamy klientów, których dane, np. z Active Directory, są dostępne tylko kilka minut, po czym zostają nadpisane przez nowsze dzienniki zdarzeń. Jeśli w tym czasie nie zostały one pobrane do analizy, to przepadły bezpowrotnie.

Wniosek z tego jest następujący: SIEM może ułatwić osiągnięcie zgodności z GDPR, ale posiadanie systemu tej klasy nie może być traktowane jako zapewnienie jej w 100%, podobnie zresztą jak ma to miejsce w przypadku szyfrowania danych.

Nie tylko GDPR

Niezwykle istotne jest zrozumienie, że wymóg ochrony przetwarzanych informacji, a w szczególności danych osobowych, nie wynika (i nigdy nie wynikał) tylko z dyrektywy GDPR lub jej lokalnych odpowiedników w krajach członkowskich UE. W praktyce od dawna obszar ochrony danych osobowych, jak i powiązanych z nią zabezpieczeń, typu polityka bezpieczeństwa, czy też bardziej niskopoziomowych, jak np. zarządzanie mechanizmami kryptograficznymi, pojawia się w wielu standardach i najlepszych praktykach.

Poniżej warto wskazać kilka wybranych standardów popularnych w sektorze bankowym:

- **Rodzina norm ISO 27000** – jeszcze w czasach standardu 17799 wskazywano takie zabezpieczenia jak: polityka bezpieczeństwa, zarządzanie kryptografią, fizyczna ochrona dostępu, wystrefowanie obiektów, bezpieczne usuwanie danych oraz zdawanie sprzętu czy wreszcie ochrona danych osobowych i zgodność z obowiązującym prawem. Dzisiaj rodzina ISO 27000 posiada także dedykowane standardy w zakresie ochrony danych osobowych, np. w chmurze – ISO 27018.

- **Standard PCI DSS** w obszarze ochrony danych kartowych także dotyka obszaru związanego z danymi osobowymi, co więcej, wymaga także podobnych zabezpieczeń, jak szyfrowania, filtrowania ruchu sieciowego, separacji systemów czy monitorowania bezpieczeństwa.
- **COBIT 5** – w dodatku *Information Security* czytamy: "*Confidentiality means preserving authorised restrictions on access and disclosure, including means for protecting privacy and proprietary information*". Dalej jest zwrócenie uwagi na potrzebę identyfikacji oraz właściwego zarządzania wymaganiami zgodności, m.in. w zakresie ochrony danych osobowych i prywatności.

W kontekście polskiego sektora bankowego, nie można zapomnieć także o Rekomendacji D KNF. Aktualna jej wersja powołuje się na ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 j.t. z późn. zm.). W samej rekomendacji obszar danych osobowych jest dotykany w wielu miejscach, czasem bardzo szczegółowo, jak np. w rekomendacji 9.20:

> *„Eksploatowane przez bank skanery sieciowe wykorzystywane do skanowania dokumentów zawierających dane osobowe lub takich, których nieuprawnione ujawnienie mogłoby narazić bank na znaczne straty, powinny być zabezpieczone przed możliwością wycieku informacji (np. poprzez przesyłanie danych w formie zaszyfrowanej). Rozwiązania banku w tym zakresie powinny również zapewniać, aby zeskanowane dokumenty były dostępne jedynie dla upoważnionych osób*".

Warto zwrócić uwagę, że np. wcześniejsza rekomendacja 9.19 dotycząca drukowania także dotyczy danych osobowych, choć nie wymienia ich explicite. Podobna sytuacja występuje w wielu innych miejscach Rekomendacji D. Jest to ważne spostrzeżenie, bo powoduje, że analiza rekomendacji za pomocą funkcji „znajdź" i szukania wyrazu „osobowe" nie przyniesie właściwego efektu.

Innym wartym odnotowania spostrzeżeniem związanym z Rekomendacją D jest sugerowanie wykorzystania standardu SSAE 16. Taki zapis znajduje się w rekomendacji 10.7 odnośnie kontroli dostawców. Należy w tym miejscu wyjaśnić, że SSAE 16 został stworzony przez księgowych z myślą o badaniu zapisów księgowych. W praktyce, gdzie następuje zderzenie wymagań prawnych, procesów biznesowych i technologii takie standardy raportowania bardzo marnie się sprawdzają w mojej ocenie. Niezwykle trudno jest w format takiego raportu „włożyć" wszystkie istotne informacje, zwłaszcza te bardzo techniczne. Dlaczego to może być problemem? Otóż chociażby z perspektywy wspomnianego już wcześniej GDPR. Dyrektywa ta wymaga w praktyce dużo więcej środków technicznej ochrony niż wcześniejsze regulacje.

PSD II i ochrona danych osobowych

Niewątpliwie PSD II może stanowić istotne wyzwanie dla ochrony danych osobowych. Z jednej strony potrzebna jest kontrola wszystkich dostawców i stron którym udostępnia się lub powierza przetwarzanie danych osobowych, a z drugiej dostęp do przynajmniej części z nich musi być zapewniony i otwarty, jak nigdy dotychczas. Niezwykle istotny jest w tym przypadku proces monitorowania bezpieczeństwa oraz rozliczalność. Większość startup'ów, których pomysł biznesowy opiera się na PSD II będzie korzystało – co już wcześnie zostało wskazane – z chmury publicznej. Korzystanie z niej przy przetwarzaniu danych osobowych jest możliwe, jednak po spełnieniu określonych warunków.

Niewątpliwie wysokość kar wynikających z GDPR stanowi realne zagrożenie dla stratup'ów a zarazem doskonały argument, aby nawet niewielkie, młode firmy dbały o bezpieczeństwo danych osobowych.

Podsumowanie

Spełnienie wymogów GDPR może być dużym wyzwaniem dla banków, w niektórych przypadkach być może większym nawet niż przygotowanie się do ostatniej aktualizacji Rekomendacji D KNF.

To co GDPR zmienia, to wymuszenie zmiany podejścia do procesu zarządzania bezpieczeństwem w organizacji. Nie da się już dłużej traktować bezpieczeństwa, jego monitorowania i procesu *patch management* po macoszemu. To znaczy da się, ale kary finansowe szybko zmienią taki trend.

Niezwykle istotnym – i zazwyczaj pomijanym w większości analiz – jest wdrożenia procesu wytwarzania bezpiecznego oprogramowania (SDL). Co istotne, można go wdrożyć u siebie nie będąc producentem oprogramowania a tylko klientem dostawców. W takim przypadku SDL polegać będzie na zdefiniowaniu właściwych praktyk przy wytwarzania oprogramowania oraz wymuszenia podejścia *secure by default and by design* dla wszystkich dostarczanych do banku aplikacji. Jeszcze kilka lat temu musieliśmy do wdrażania SDL przekonywać prawie każdą organizację, z którą przyszło mi współpracować. Dzisiaj, w obliczu ryzyka tak wysokich kar, percepcja ulega istotnej zmianie. Z perspektywy bezpieczeństwa danych osobowych nas wszystkich jest to niezwykle pozytywny trend.

Maciej Gawroński
Partner zarządzający kancelarii Gawronski & Partners

Radca prawny, jeden z pięciu ekspertów Technologii, Mediów i Telekomunikacji rekomendowanych przez Ranking Kancelarii Prawniczych Rzeczypospolitej 2016, ekspert Komisji Europejskiej ds. kontraktów cloud computingowych, europejski ekspert ds. międzynarodowych transferów danych osobowych i cyberbezpieczeństwa, autor wielu publikacji z tych dziedzin. Był też wiodącym prawnikiem największego wdrożenia informatycznego w polskim sektorze finansowym. Od 20 lat doradza bankom i instytucjom finansowym w sprawach regulacyjnych, korporacyjnych, komercyjnych i spornych.

Maciej Gawroński, Gawronski & Partners

Odpowiedzialność za cyberbezpieczeństwo w banku w czasach reformy ochrony danych

Przed wszystkimi instytucjami w Unii Europejskiej stoi obecnie wyzwanie wdrożenia nowych zasad ochrony danych osobowych wynikających z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), czyli z tak zwanego RODO. Stosowanie RODO ma formalnie zacząć się 25 maja 2018 r. Nieprzyjemne znaczenie tego faktu polega na tym, że z dniem tym stosować będzie można i trzeba drakońskie kary przewidziane Rozporządzeniem. Zważywszy, że dostosowanie się do RODO jest procesem wymagającym, w praktyce RODO właśnie zaczyna obowiązywać.

Wyzwania cyberrzeczywistości

Przed bankami piętrzy się fala cyberzagrożeń. Przestępcy nieuchronnie i coraz bardziej wkraczają w cyberprzestrzeń. Wyzwaniem dla banków staje się połączenie dostępności cyfrowej z zabezpieczeniem się przed ingerencją w ich systemy, nadążanie za rozwijającymi się technikami cyberataków oraz ochrona klienta. Wreszcie, wobec zderzenia rosnących wymogów prawa z rosnącymi zagrożeniami, wyzwaniem dla banków, ich kadry zarządzającej i służb bezpieczeństwa stać się może wykazanie dopełnienia odpowiedzialności za cyberbezpieczeństwo.

W tym artykule nie staram się przedstawić kompleksowego krajobrazu pola bitwy czy teatru działań wojennych, ale raczej wskazuję na perfidną grę pomiędzy wymaganiami prawa, wyzwaniami rzeczywistości a możliwościami i wynikające z tego zagrożenia dla osób odpowiedzialnych w bankach za cyberbezpieczeństwo.

Unijna reforma zasad ochrony danych

RODO stawia przed instytucjami, także przed bankami, nowe wyzwania, takie jak:

- podejście oparte na ryzyku,
- uwzględnienie prywatności w projektowaniu swojej działalności,
- założenie ochrony prywatności (*privacy by default*),
- zapewnienie przenoszalności danych,
- kontrola cyklu życia danych (usuwanie danych, proporcjonalność przetwarzania),
- ograniczenie profilowania,
- raportowanie naruszeń ochrony danych,
- drakońskie kary, których wysokość można pewnie będzie mitygować, ale które co do zasady będą nieuchronne,
- zwiększona odpowiedzialność za dostawców (chociaż skłonność banków do śrubowania wymogów względem nich może zwrócić się przeciwko samym bankom – nie będzie bowiem uzasadnienia, dla którego bank miałby stosować niższy poziom zabezpieczenia danych niż ten, którego wymaga od swojego dostawcy).

Warto zauważyć, że banki tradycyjnie przyzwyczajone są do ochrony danych klientów – tych objętych tajemnicą bankową. RODO jednak nie czyni rozróżnienia pomiędzy klientami, pracownikami czy personelem dostawców. Wszystkie te dane są danymi osobowymi i muszą podlegać nowym zasadom ochrony.

Kary po raz pierwszy

Można byłoby powiedzieć, że temat kar jest już oklepany i że wszyscy wiedzą, iż od przyszłego roku możliwe będzie karanie za naruszenia ochrony danych

osobowych. Można też oczywiście powiedzieć, że za niewłaściwe zabezpieczenie danych osobowych grozi niższy wymiar kary, to jest „tylko" do 2% światowego obrotu, ale nie mniej niż do 10 mln euro. Problem jednak w tym, że w przypadku stwierdzenia naruszenia przepisów RODO kary nie będzie można uniknąć. Możliwa będzie tylko dyskusja z jej wymiarem, którego górna granica jest zapewne wystarczająco przerażająca dla wszystkich przedsiębiorstw w tym kraju. Dlatego właśnie zaczynam od kar.

Adekwatna ochrona danych

Wśród przepisów, za których naruszenie grozi kara, znajduje się artykuł 32 RODO dotyczący bezpieczeństwa przetwarzania. Zgodnie z tym przepisem należy wdrożyć techniczne i organizacyjne środki ochrony danych, odpowiadające wyważonemu ryzyku naruszenia praw i wolności osób, których dane dotyczą, przy uwzględnieniu kosztów ochrony i pozostałego kontekstu przetwarzania.

Wśród środków ochrony RODO wymienia szyfrowanie, zapewnienie bezpieczeństwa informacji i systemów (cyberbezpieczeństwo), gotowość zapobiegania skutkom katastrof oraz testowanie przyjętych rozwiązań.

Wydaje się, że szczególnie trudne a równocześnie najbardziej potrzebne będzie wykazanie adekwatności zastosowanych rozwiązań w przypadku wycieku danych osobowych. W takiej sytuacji będziemy stali przed kolejnym trudnym zadaniem. Trzeba będzie przecież wykazać, że pomimo wycieku nie doszło do naruszenia przepisów o ochronie danych osobowych…

Analiza ryzyka przetwarzania danych

RODO wymaga przeprowadzania analiz przetwarzania danych. Większość znanych mi poglądów koncentruje się na przepisie artykułu 35 RODO (tzw. PIA czyli *Privacy Impact Assessement*), zgodnie z którym analizę wpływu przeprowadza się, gdy istnieje wysokie ryzyko naruszenia praw i wolności osób fizycznych. Wyrażane są poglądy, że tylko nowe rodzaje przetwarzania danych wymagają takiej analizy – np. wdrażanie nowych rozwiązań IT, a co więcej, że obowiązek PIA powstanie dopiero z datą rozpoczęcia stosowania RODO (czyli 25 maja 2018 r.).

Jednak implikacje wyżej wspomnianego artykułu 32 RODO są dalej idące. Zadaniem karkołomnym w przypadku wycieku danych będzie wykazanie, że

zastosowano odpowiednie środki ochrony, jeśli uprzednio nie udokumentuje się analizy adekwatności środków ochrony danych, a w tym analizy ryzyka naruszenia praw i wolności, o którym mowa w art. 32 RODO.

Stąd obawiam się, że banki w ramach przygotowań do RODO powinny dokonać oceny ryzyka przetwarzania poszczególnych klas danych osobowych. Już tu można powiedzieć, że wydaje się, iż wyciek danych klienckich rodziłby zagrożenia o wielkiej wadze. Równie niebezpieczny byłby też wyciek danych o wynagrodzeniach pracowniczych. Sądzę, że w takiej sytuacji regulator nie dałby się przekonać za pomocą argumentów o niskim prawdopodobieństwie wystąpienia takiego zdarzenia. Banki nie są bowiem ofiarą syndromu oblężonej twierdzy – banki są oblężoną twierdzą, która musi być świadoma tego, że jest poddawana ciągłym cybernetycznym atakom.

Jaki z tego wniosek? Otóż taki, że jeśli w nowej rzeczywistości dojdzie do wycieku danych osobowych z banku, to będzie on musiał wytłumaczyć się, dlaczego nie zastosował wszystkich możliwych środków ich ochrony. Zakładać przy tym należy, że w pierwszej kolejności zostanie odpytany o środki przewidziane w RODO, a wśród nich tak naprawdę tylko jeden wskazany jest wprost – szyfrowanie.

Zgłoszenie naruszenia

Wyzwaniem, przed którym stają także banki, jest konieczność zgłaszania naruszeń ochrony danych, które grożą naruszeniem praw i wolności osób fizycznych.

Zasadniczo chodzi tu o wycieki danych, przy czym zarówno zewnętrzne (nie tylko wskutek ataku, ale także np. zagubienia nośnika danych – telefonu, pamięci flash, laptopa, dokumentacji papierowej, przesłania emaila pod niewłaściwy adres, itp.), jak i wewnętrzne (np. nieuprawniony dostęp personelu własnego).

Zgłoszenie do GIODO[1] powinno nastąpić w ciągu 72 godzin lub krócej. Trudnością jest nie tylko konieczność szybkiego działania, w tym ustalenia szczegółów zdarzenia, oceny wpływu, propozycji środków zaradczych. Dużym wyzwaniem będzie zbudowanie świadomości co do tego, co jest naruszeniem ochrony danych oraz kultury, w której takie zdarzenia nie będą ukrywane.

1 Czy też do Prezesa Urzędu Ochrony Danych Osobowych, zgodnie z projektem nowej ustawy.

W przypadku wycieków dotykających dużą liczbę osób fizycznych (szczególnie klientów) odrębnym problemem będzie konieczność ich powiadomienia o zaistniałej sytuacji. Jeśli wyciek może być groźny (np. gdy utracone dane mogłyby być wykorzystane przeciwko osobom fizycznym a nie były zaszyfrowane), konieczne jest poinformowanie zagrożonych osób. Problemem będzie szczególnie poinformowanie tych, z którymi bank nie ma kontaktu elektronicznego czy telefonicznego. Problem ten może mieć dwojaką naturę: finansową – koszt szybkiego doręczenia zawiadomień papierowych może być bardzo duży, oraz reputacyjną – w alternatywie bank może zdecydować się na nadawanie publicznego komunikatu o wycieku.

Kary po raz drugi

Jak widać, na polu cyberbezpieczeństwa jest wiele min, na które wpaść może bank, gdy zdarzy się najgorsze i będzie je trzeba sprawdzić w ustawowe 72 godziny. Dlatego warto poświęcić czas, uwagę i inne zasoby, aby w ciągu najbliższych kilkunastu miesięcy przygotować mapę tego pola minowego oraz koncepcję podejścia do problemu, którego konieczność prędzej czy później nastąpi.

Wśród pytań, które będziemy musieli sobie zadać i na nie odpowiedzieć, są nie tylko o te szkody, które wyrządzić może wyciek różnych posiadanych przez nas danych osobowych, o koszty zapewnienia ich bezpieczeństwa, o środki, które możemy podjąć w celu ich zabezpieczenia i czy powinniśmy je podjąć, ale także o to, czy możemy tych środków, takich jak np. szyfrowanie, nie podjąć. Niby powinniśmy zadać sobie też o prawdopodobieństwo wycieku, czyli naruszenia ochrony danych. Ale nadziei w odpowiedzi na to pytanie bym nie upatrywał. Specjaliści z dziedziny bezpieczeństwa twierdzą, że obecnie nie można już liczyć na to, że naruszenie się nie zdarzy. Należy zakładać, że do niego dojdzie i przygotowywać plan reagowania.

Im gorzej będziemy przygotowani na wypadek zaistnienia wycieku danych, tym trudniej będzie nam obniżyć wymiar kary, która zostanie na nas nałożona. Liczyć na to, że zostaną uznani za niewinnych, praktyczni ludzie nie powinni. W przypadku wycieku katastrofalnego kara też grozić będzie katastrofalna.

Jaki z tego wniosek? O ile dotychczas incydenty cyberbezpieczeństwa nie rodziły drastycznych konsekwencji względem osób odpowiedzialnych

w bankach za ten obszar[2], po 25 maja 2018 r. poszukiwanie winnego wejdzie w zupełnie nowy wymiar.

Odpowiedzialność za cyberbezpieczeństwo

Nie wchodząc w tym tekście w szczegóły, odpowiedzialność za bezpieczeństwo danych osobowych opiera się na zasadzie winy i jest to odpowiedzialność za staranne działanie.

Obecnie są silne argumenty by uznać, że prawo wymaga szczególnej staranności do zabezpieczenia danych osobowych oraz tych objętych tajemnicą bankową, co jest podkategorią tych pierwszych. Wątpliwe, aby nowa ustawa o ochronie danych wprowadziła niższy standard staranności. Na pewno Prawo bankowe nie obniży też standardu ochrony tajemnicy bankowej[3].

Odpowiedzialność rozkłada się i przesuwa (często z powrotem do góry) według łańcucha dowodzenia. W banku będzie ona rozkładać się głównie na linii od członka zarządu odpowiedzialnego za bezpieczeństwo danych poprzez departament bezpieczeństwa i departament informatyki, na końcu dochodząc do pozostałych działów, tzn. biznesu, kadr itd. Odpowiedzialność może zahaczać o dział zgodności, a osobno może spoczywać też na administratorze bezpieczeństwa informacji, który w nowej rzeczywistości stanie się zapewne IODą, czyli inspektorem ochrony danych.

Ważnym jest, że już w tej chwili istnieją przepisy przypisujące odpowiedzialność karną za przestępstwa nieumyślne związane z niedołożeniem odpowiedniej staranności w ochronie danych (względem osób za to odpowiedzialnych) lub w dbałości o interesy przedsiębiorcy (względem kadry kierowniczej). Na ten temat coraz częściej zdarza mi się prowadzić prezentacje. Ciekawe, jakie nowe przepisy karne pojawią się w nowej ustawie o ochronie danych?

Jakie ma to znaczenie praktyczne? Ano takie, że gdy bank będzie prowadził śledztwo wewnętrzne, GIODO będzie prowadził śledztwo i postępowanie „o ukaranie", wyciek zostanie ujawniony poszkodowanym lub co gorsza publicznie, a wtedy jest całkiem prawdopodobne, że ktoś zdecyduje się złożyć zawiadomienie o popełnieniu przestępstwa, nazwijmy je, „niezabezpieczenia danych".

W takiej sytuacji zagrożone osoby bronić się będą na dwa sposoby.

2 Choć były one wykorzystywane już do rozgrywek personalnych.

3 Nie jestem zwolennikiem teorii, że Prawo bankowe wyłącza przepisy o ochronie danych osobowych w odniesieniu do danych klienckich.

Wskazując, że wina leży po stronie kolegi, przełożonego lub podwładnego bądź, że zastosowano odpowiednie, starannie dobrane i stosowane, organizacyjne i techniczne środki ochrony danych.

Problem jednak będzie polegał na tym, że standardem staranności zapewne będzie staranność szczególna. Tylko co to znaczy?

Pewien znakomity prawnik, luminarz prawa nowych technologii oraz mój dobry kolega, wiele lat temu zwykł awanturować się podczas negocjacji, gdy żądałem, aby jego klient zobowiązał się do staranności szczególnej. Mój kolega perfidnie pytał się, co to właściwie ta szczególna staranność jest. Ja równie perfidnie odpowiadałem mu, żeby sobie poszukał w przepisach i orzecznictwie i jeszcze perfidniej dostarczałem na następne spotkanie wyciąg z nich. Z biegiem lat praktyki i przemyśleń doszedłem jednak do następującego, dość konkretnego spojrzenia na tę sprawę. Staranność najwyższa oznacza zrobienie wszystkiego, co można byłoby wymyśleć i zrobić w danej sytuacji. Staranność zwykła oznacza zrobienie tego, co zwykle się w takiej sytuacji robi. Staranność profesjonalna oznacza zrobienie tego, co zwykle zrobiłby profesjonalista.[4] Zaś staranność szczególna oznacza zrobienie nie tego, co zrobi większość, ale tego, co robią prymusi.

Proponuję, aby teraz czytelnicy przeprowadzili sobie taki intelektualny test, a mianowicie, czy robią to, co robią prymusi cyberbezpieczeństwa bankowego. Odpowiedź na to pytanie będzie odwrotnie proporcjonalna do zagrożenia odpowiedzialnością w razie wystąpienia dużego wycieku danych, szczególnie jeśli będą to dane klienckie, o uwierzytelniających lepiej nawet nie myśleć.

Szyfrowanie

Myśląc o bezpieczeństwie danych nie wolno nam się zamknąć w idealnym świecie procedur bezpieczeństwa. Powinniśmy myśleć jak zwykły użytkownik, dla którego nasze procedury są największą uciążliwością. Wiara w ich wypełnianie powinna być okolicznością obciążającą. Stąd dużą rolę powinny pełnić mechanizmy wymuszone, obliczone i przewidziane na błędy ludzkie. Takim mechanizmem, środkiem przewidzianym w RODO, jest szyfrowanie. Tam, gdzie jest to możliwe, chrońmy w ten sposób dane. Po drugie, bo jest to

4 Z racji problemów z jakością usług w naszym kraju warto na marginesie nadmienić, że nie chodzi tu o to, co zwykle zrobiłby tzw. „fachowiec", tylko o to, co zwykle zrobiłby prawdziwy fachowiec.

chyba jeden z podstawowych sposobów zabezpieczenia danych w cyfrowym świecie. Po pierwsze zaś, bo RODO wprost odwołuje się do szyfrowania, więc w razie wypadku nieuchronnie zostaniemy o nie zapytani.

Warto pamiętać, że GIODO w opinii w sprawie bezpieczeństwa danych przekazywanych przy użyciu poczty elektronicznej opublikowanej dnia 10 marca 2017 r. zwraca uwagę na coraz powszechniejsze ryzyka związane z posługiwaniem się nią i rekomenduje szyfrowanie nie tylko jej treści, ale także kanałów komunikacji oraz dbanie o odpowiednie uwierzytelnianie się (do czego również wykorzystuje się metody kryptograficzne). Z prawdopodobieństwem graniczącym z pewnością szyfrowanie znajdzie królewskie miejsce wśród dobrych praktyk zabezpieczania danych, które nowy organ – Prezes Urzędu Ochrony Danych Osobowych – będzie publikował zgodnie z kompetencją, którą planuje się mu przyznać.

Podsumowanie

Celem tego tekstu nie jest przedstawienie wszystkich zagadnień związanych z wejściem w życie czy też rozpoczęciem stosowania RODO. Nad tym pracuje cała grupa robocza w Związku Banków Polskich. Chciałem natomiast pokazać czytelnikom, że kończą się żarty z ochroną danych osobowych i cyberbezpieczeństwem. Sektor bankowy powinien cechować się bardzo wysoką wrażliwością na te kwestie, jednak w praktyce obserwujemy różne podejście do bezpieczeństwa w bankach. Czasem składane jest ono w ofierze na ołtarzu wygody, często jest traktowane wstydliwie oraz jako centrum kosztów. Nieśmiałe głosy w tych sprawach słyszę od lat. Wydaje się, że teraz nadszedł najwyższy czas, aby zastanowić się, w jaki sposób wykażemy, że szczególnie postaraliśmy się o bezpieczeństwo danych i że cokolwiek złego tym danym się zdarzyło lub mogło zdarzyć, to nie nasza wina...

Andrzej Kawiński
Country Manager Banknote Processing w Giesecke & Devrient GmbH

Absolwent Politechniki Warszawskiej i Automatyki Procesów 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.
Od 1 marca 2014 r. pracuje w firmie Giesecke & Devrient GmbH, gdzie jest odpowiedzialny za Polskę oraz kraje skandynawskie. W przeszłości zarządzał firmami Wincor Nixdorf, Siemens Nixdorf oraz 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.

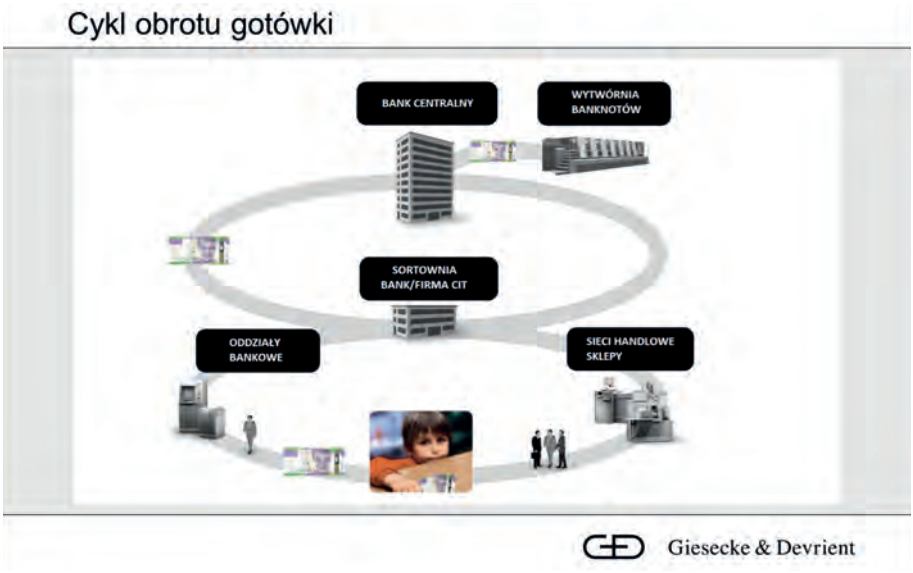
Andrzej Kawiński, Giesecke & Devrient GmbH

Zarządzanie gotówką w krajach europejskich

Od wielu lat, profesjonalnie zajmując się obrotem gotówkowym, mam unikalną okazję porównania procesów związanych z jej zarządzaniem w krajach europejskich. Mogłoby się wydawać, że obrót gotówką powinien wyglądać w każdym kraju identycznie. Praktyka pokazuje jednak, że jest inaczej. Liczba krajów, jak i modeli jest zbyt duża, aby omówić je wszystkie w tym artykule, postaram się jednak porównać rozwiązania wdrożone w Polsce z krajami Europy Zachodniej oraz Skandynawią.

Różnice w obrocie gotówkowym pomiędzy krajami wynikają z przepisów oraz przyzwyczajeń społeczeństwa. Jednym z czynników wpływających na różnice między nimi jest chęć ograniczenia przez rządy kosztów obrotu gotówkowego. Również w tzw. Strefie Euro, regulowanej przez Europejski Bank Centralny, występują istotne różnice w modelach stosowanych przez poszczególne kraje.

Gotówka od czasu wynalezienia jej przez Fenicjan w VII w p.n.e do dnia dzisiejszego pozostaje najbardziej uniwersalną formą zapłaty i jest jednym z symboli swobód obywatelskich. Obrót gotówki na dużym poziomie ogólności można opisać w postaci prostego schematu.



Standardowo gotówka krąży w dwóch obiegach:

- Zamkniętym, gdzie gotówka jest przekazywana pomiędzy skarbcami Banku Centralnego a skarbcami banków lub firmami CIT, które w imieniu banków odbierają i przechowują gotówką.
- Otwartym, gdzie gotówka przepływa pomiędzy skarbcami banku, obywatelami i przedsiębiorcami.

Producenci banknotów oraz mennice na zlecenie Banków Centralnych dostarczają banknoty i monety do skarbców Banku Centralnego. Banki i instytucje płatnicze pobierają gotówkę z Banku Centralnego celem zasilenia swoich oddziałów i bankomatów. Klienci banków, posiadający dostępne środki, wypłacają gotówkę w bankomacie lub oddziale bankowym. Zakup towarów lub usług powoduje przekazanie gotówki do przedsiębiorcy, a ci deponują ją w oddziałach banków. Zwykle odbiór oraz przeliczenie gotówki w imieniu banku wykonują wyspecjalizowane firmy CIT (*Cash in Transit*). Banki nadmiar gotówki odprowadzają do Banku Centralnego, który tę dobrej jakości (tzw. obiegową) po przeliczeniu wprowadza do ponownego obrotu, a złej (tzw. destrukty) utylizuje.

Poszczególni uczestnicy procesu obrotu gotówki mają różne priorytety, które powodują zmiany w przedstawionym powyżej modelu. Krajowe

regulacje, przyzwyczajenie społeczeństwa do gotówki, jak również warunki geograficzne mają wpływ na występujące w Europie różnice.

Zadaniem Banku Centralnego jest zapewnienie odpowiedniej ilości gotówki na rynku. Istotnym priorytetem Narodowego Banku Polskiego jest nadzór nad jakością banknotów i monet znajdujących się w obiegu. NBP dla zapewnienia właściwej jakości banknotów wprowadzanych do obrotu, 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, opublikował 17 sierpnia 2016 r. Zarządzenie nr 19/2016 w sprawie sposobu i trybu przeliczania, sortowania, pakowania i oznaczania opakowań banknotów i monet oraz wykonywania czynności związanych z zaopatrywaniem banków w te znaki.

Banki komercyjne, przechowując środki klientów, muszą im zapewnić możliwość zdeponowania, jak i pobrania gotówki. Realizując swoje działania dbają o jak najniższe koszty związane z jej przeliczaniem, transportem i przechowywaniem.

Firmy CIT profesjonalnie zajmujące się transportem, przeliczaniem i przechowywaniem gotówki zarabiają oferując swoje usługi na rynku. W Polsce ich klientami są przeważnie banki, w krajach skandynawskich podpisują one natomiast bezpośrednie umowy z przedsiębiorcami. Ich głównym celem działania jest generowanie jak największych zysków dla swoich właścicieli.

Obywatele chcą mieć bezpłatny i jak najprostszy sposób dostępu do gotówki.

Z kolei dla przedsiębiorców priorytetem jest jak najszybsze i jak najtańsze zdeponowanie gotówki na rachunku bankowym.

Model Polski

W strukturach NBP funkcjonuje 16 Oddziałów Okręgowych zlokalizowanych w każdym mieście wojewódzkim. Odbiór i transport gotówki z nich na zlecenie banków realizują firmy CIT. Oprócz firm komercyjnych czynności te wykonuje również Poczta Polska.

Odebrana gotówka jest przewożona do sortowni. Większość banków czynność przechowywania oraz przeliczania gotówki powierzyła firmom zewnętrznym. Sortownie przygotowują zasiłki dla oddziałów bankowych oraz kasety do bankomatów.

Klienci banków, po wypłacie gotówki, kupują towary lub usługi przekazując gotówkę przedsiębiorcom.

Przedsiębiorcy deponują gotówkę w oddziałach bankowych, wrzutniach nocnych lub we wpłatomatach. Często, również na zlecenie banków, firmy CIT odbierają gotówkę bezpośrednio ze sklepów.

Gotówka wraca do sortowni, gdzie zwykle w bardzo krótkim okresie czasu musi być przeliczona. Firmy CIT procesują gotówkę powierzoną im przez banki, dlatego też gotówka jednego banku nie może być mieszana z gotówką innego. W sortowniach, zgodnie z rozporządzeniem Prezesa NBP, banknoty są dzielone według nominałów oraz orientacji, następnie paczkowane po 100 sztuk i wiązkowane (10 paczek banknotów o tym samym nominale). Monety są również dzielone według nominałów a następnie rolowane lub pakowane w foliowe opakowania zbiorcze (saszetki).

W sortowniach CIT banknoty są również dzielone na obiegowe i destrukty. Dopiero od niedawna na rynku polskim obowiązuje rozporządzenie NBP Nr 19/2016, szczegółowo definiujące różnice pomiędzy banknotem obiegowym a destruktem. Rozporządzenie, co prawda, określa maszynowy sposób sortowania banknotów, ale dopuszcza również możliwość ręcznego ich dzielenia na obiegowe i destrukty. Regulacje stosowane w Strefie Euro, ale także w innych krajach europejskich, np. w Czechach, zobowiązują sortownie do maszynowego sortowania banknotów. Europejski Bank Centralny, ale również Banki Centralne innych krajów podjęły się zadania certyfikacji urządzeń pod kątem obiegowości. Wprowadzenie do ponownego obiegu zniszczonego banknotu (destruktu) jest karalne. Polskie regulacje nie wymuszają maszynowego sortowania banknotów. Również wprowadzenie do obrotu destruktu nie pociąga za sobą kar finansowych.

Przeliczona i posortowana gotówka obiegowa, zgodnie z decyzją banku, może wrócić do obrotu (zasiłki dla oddziałów, zasilenia bankomatów) lub jest odprowadzana do sortowni Banku Centralnego. Brak konieczności maszynowego sortowania jakości banknotów powoduje ręczne oddzielanie destruktów. Zniszczone banknoty (destrukty) są odprowadzane do Banku Centralnego. W przypadku, gdy jeden z banków ma do odprowadzenia gotówkę do Banku Centralnego a drugi potrzebuje się w tym dniu zasilić, nie ma możliwości przekazania gotówki w sortowniach firm CIT. W takiej sytuacji musi ona odwieźć, w imieniu pierwszego banku, gotówkę do Banku Centralnego, a następnie pobrać ją w imieniu tego drugiego.

Gotówka przychodząca do Banku Centralnego jest przeliczana na dużych sorterach przemysłowych, które jednoznacznie dzielą banknoty na obiegowe i destrukty. Banknoty obiegowe są paczkowane i wiązkowane. Destrukty są automatycznie po przeliczeniu niszczone.

Opisany proces, ze względu na swoją złożoność, wymaga zaangażowania wielu pracowników zarówno w sortowniach firm CIT, jak i po stronie Banku Centralnego. Banknoty są co najmniej kilka razy przeliczane na sorterach w celu:

- przeliczenia depozytu klienta,
- ponownej weryfikacji w przypadku wystąpienia różnicy,
- podziału według nominałów,
- podziału według obiegowości,
- ułożenia w jednej orientacji.

Każde przepuszczenie banknotu przez urządzenie wymaga obecności pracownika, zajmuje czas oraz ma wpływ na żywotność banknotu. Wszystkie te elementy są składowymi kosztów obrotu gotówkowego.

Model stosowany w Strefie Euro

Cykl obiegu gotówki w Strefie Euro jest podobny do obrotu w Polsce, nie jest jednak jednolity we wszystkich krajach. Krajowe Banki Centralne stosują lokalne regulacje, których celem jest obniżenie kosztów obrotu gotówkowego dla wszystkich podmiotów funkcjonujących na rynku.

Istotną różnicą stosowaną w strefie Euro jest brak regulacji związanych z orientacją banknotów. Ze względu na zaszyte w papierze zabezpieczenie nie mają one jednolitej grubości, dlatego też preferowane jest mieszanie ich orientacji. Regulacja ta ma duży wpływ na zmniejszenie pracochłonności w sortowniach zarówno banków oraz firm CIT, jak i w Banku Centralnym. W Polsce obowiązek orientacji banknotów wymusza konieczność zakupu większych sorterów (wyposażonych w większą liczbę kieszeni) lub kilkukrotnego przeliczenia banknotów przez mniejsze urządzenia celem ich odpowiedniego ułożenia (większa pracochłonność).

Podejście do podziału banknotów na obiegowe i destrukty jest różne zależnie od kraju. We Francji oraz w Niemczech wszystkie banknoty odebrane od klientów trafiają za pośrednictwem firm CIT do Banku Centralnego.

Nie wymagają one przy tym sortowania jakościowego w sortowniach banków lub firm komercyjnych. Sortowanie jakościowe jest realizowane w sortowniach Banków Centralnych przy przeliczaniu dostarczonych depozytów. Ta metoda gwarantuje, że w obiegu znajdują się tylko banknoty dobrej jakości. Zaletą jest również oszczędność inwestycji i pracochłonności po stronie sortowni komercyjnych. Mniejsza liczba przejścia banknotów przez sortery ma wpływ na ich żywotność.

Bardzo ciekawym rozwiązaniem, stosowanym w Niemczech, jest brak obowiązku paczkowania i wiązkowania banknotów w sortowniach komercyjnych. Przeliczone banknoty są układane w standardowe kontenery, przy czym każdy z nich ma swój unikalny kod paskowy. Dodatkowo zabezpieczony jest plombą, również z indywidualnym numerem. Wartość banknotów znajdujących się w kontenerze jest wprowadzana do systemu informatycznego. Niemiecki Bank Centralny odczytując numer kontenera i plomby otrzymuje informacje o wartości. Po przeliczeniu banknotów znajdujących się w kontenerze uznaje wartość na rachunkach klientów, a w przypadku różnicy automatycznie obciąża konto firmy CIT.

To rozwiązanie wyniknęło z chęci oszczędzenia pracochłonności po stronie Banku Centralnego. Obecnie w Polsce banknoty przeliczone w sortowni firmy CIT są paczkowane (opaskowane) i wiązkowane (pakowane w folie). Opaska m.in. zawiera informacje o dniu przeliczenia i osobie, która była za to odpowiedzialna. Sortownie ze względu na podpisane umowy wykonują te czynności głównie w godzinach nocnych. W ciągu dnia pakiety te są dostarczane do sortowni NBP, gdzie przed przeliczeniem zdejmowane jest opakowanie z folii, a następnie zrywane są opaski z poszczególnych paczek.

System wdrożony w Niemczech oszczędza pracochłonność po stronie firmy CIT, bo nie ma tam konieczności nakładania opasek i pakowania banknotów w wiązki, jak również pracochłonność po stronie Banku Centralnego z powodu braku konieczności rozrywania wiązek i zdejmowania opasek. Efektem dodatkowym jest ekologia, bo nie korzysta się z folii i papierowych opasek.

We Francji wszystkie banknoty odbierane od klientów są również dostarczane do sortowni Banku Centralnego. W modelu francuskim dla przekazywania wartości stosowane są standardowe jednorazowe koperty bezpieczne. Obecnie rozważany jest projekt zastąpienia foliowych opakowań kontenerami wielokrotnego użytku.

W Polsce transport gotówki pomiędzy sortowniami jest realizowany w workach jutowych wydawanych przez NBP. Opakowania te były stosowane przed laty również w innych krajach. Obecnie prawie wszystkie kraje zastąpiły worki standardowymi kontenerami, kasetami lub bezpiecznymi kopertami. Kontenery, oprócz ułatwień związanych z pakowaniem i transportem, w odróżnieniu do worków są czyste. Worki jutowe z dużą ilością banknotów lub monet, ze względu na swój ciężar, są przesuwane a nie przenoszone, dlatego też są bardzo podatne na zbieranie kurzu. Duże jego stężenie w sortowniach ma wpływ nie tylko na zdrowie pracowników, ale również na większą awaryjność sorterów.

Francuski Bank Centralny rozważa obecnie wdrożenie modelu tzw. recyclingu. W jego ramach sortownie komercyjne będą miały prawo sortowania jakościowego banknotów i ponownego przekazywania do obiegu tych o dobrej jakości. Warunkiem wdrożenia tego modelu jest posiadania przez sortownię odpowiednich certyfikowanych urządzeń do sortowania jakościowego.

Fiński Bank Centralny, ze względu na małą liczbę oddziałów, już kilka lat temu pozwolił sortowniom firm komercyjnych na przechowywanie w swoich skarbcach depozytów Banku Centralnego. Ta regulacja związana jest z obowiązkiem sortowania jakościowego banknotów przy użyciu certyfikowanych sorterów. Gotówka odebrana od klientów po przeliczeniu i posortowaniu według jakości jest przenoszona do skarbca firmy komercyjnej jako depozyt Banku Centralnego. Banknoty zniszczone są przesyłane do Banku Centralnego celem ich utylizacji. Wdrożony model pozwolił na oszczędności związane z transportem gotówki pomiędzy sortowniami komercyjnymi a Bankiem Centralnym. Brak konieczności ponownego przeliczania gotówki w jego sortowni jest dodatkową oszczędnością kosztów obrotu gotówkowego.

Model Skandynawski

Kraje skandynawskie, mimo ogólnej opinii krajów bezgotówkowych, w dalszym ciągu w dosyć istotny sposób posługują się gotówką. Płatności bezgotówkowe są tam jednak bardzo popularne. Kartą można płacić w taksówce, w kawiarni czy za parkowanie. Karta bywa czasami jedynym identyfikatorem uiszczenia opłaty za przejazd metrem. Jednym z elementów, które miało wpływ na popularyzację płatności bezgotówkowych, są duże odległości w stosunku do niewielkiej liczby mieszkańców. Przy takich uwarunkowaniach

koszt obrotu gotówkowego był bardzo wysoki. Od wielu lat instytucje rządowe wspierają idee płatności bezgotówkowych.

Gotówka, będąca synonimem wolności obywatelskich, w dalszym ciągu w krajach skandynawskich funkcjonuje. Wartym podkreślenia jest fakt, że w ostatnich latach Szwedzki Bank Centralny (Riksbank) wypuścił nowa emisję szwedzkich banknotów i monet wymieniając dotychczasowe nominały. A to tylko potwierdza, że zapotrzebowanie na gotówkę w dalszym ciągu jest duże. Mimo marketingowych zapowiedzi, że w roku 2020 Szwecja będzie pierwszym społeczeństwem bezgotówkowym, działania Riksbanku wspierają obrót gotówkowy w tym kraju. Wymiana emisji banknotów jest również planowana w tym roku w Norwegii, a w Danii nastąpi w najbliższych latach.

Model obrotu gotówkowego wdrożony w krajach skandynawskich znacznie różni się od modeli stosowanych w innych krajach europejskich. Banki Centralne bardzo ograniczyły tam swoją rolę w procesie, przekazując szereg kompetencji firmom CIT, które stały się ich partnerami biznesowymi. Bardzo wyraźnym przykładem takiej współpracy jest fakt, że w Norwegii jedna z firm CIT posiada prawo do niszczenia banknotów nieobiegowych. Zwykle Banki Centralne nie oddają tego typu usługi firmom zewnętrznym.

Zdecydowana większość obrotu gotówkowego w krajach skandynawskich jest realizowana bez udziału banków. Oddziały bankowe nie obsługują operacji gotówkowych kierując klientów do urządzeń samoobsługowych. Firmy CIT stały się w tych krajach Instytucjami Płatniczymi. Zmiana ta spowodowała, że umowy na odbiór gotówki podpisywane są bezpośrednio pomiędzy sklepami a firmami CIT. Gotówka trafiająca do sortowni staje się gotówką firmy CIT, dzięki czemu proces rozliczania i sortowania jest prostszy oraz tańszy.

Bardzo istotnym obowiązkiem, kontrolowanym przez Bank Centralny, jest sortowanie jakościowe banknotów. Bank Centralny przyjmuje tylko zniszczone banknoty, a banknoty obiegowe pozostają w skarbcach firm CIT albo wracają z powrotem do obrotu. Już wiele lat temu Banki Centralne w Skandynawii wdrożyły model przechowywania swojej gotówki w skarbcach firm komercyjnych. Ta regulacja umożliwiła im zamknięcie swoich oddziałów ograniczając koszty obrotu gotówkowego.

Wysokie koszty pracy, w połączeniu ze znacznymi świadczeniami socjalnymi wobec pracowników, przełożyły się na wysoki stopień automatyzacji procesów związanych z przeliczaniem i sortowaniem banknotów. Rozwiązania wdrożone w sortowniach krajów skandynawskich są jednymi

z najnowocześniejszych na świecie. Nowe sortownie, wybudowane obok centrów logistycznych (zwykle poza miastami), charakteryzują się bardzo wysokim poziomem zabezpieczeń. Z wypowiedzi przedstawicieli firm CIT wynika, że liczba przeliczanych banknotów i monet rośnie.

Rola firm CIT w procesie obrotu gotówkowego

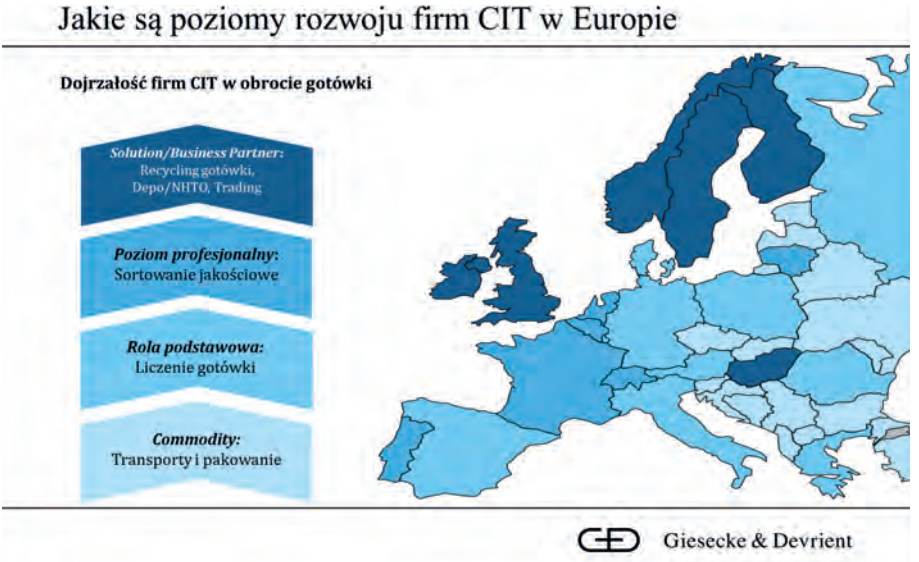
Działania banków związane z ograniczeniem kosztów obrotu gotówki przekładają się na zwiększenie roli firm CIT. Już obecnie w niektórych krajach to firmy CIT stały się partnerem dla Banków Centralnych zastępując instytucje finansowe. Niektóre usługi, takie jak transport gotówki, stały się na tyle powszechne, że obecnie nie przynoszą zysków. W Polsce mamy kilkadziesiąt podmiotów oferujących usługę transportu gotówki przy pięciu komercyjnych firmach oferujących przeliczanie i sortowanie gotówki.

Pozycja firm CIT w danym kraju wynika z wielu czynników. Składają się na nie m.in. obwiązujące regulacje Banku Centralnego w zakresie obrotu gotówki oraz skłonność banków do outsourcingu tych procesów. Przejęcie większego zakresu obowiązków związanych z obrotem gotówkowym przez firmy CIT zwykle przekłada się na większe zyski.

W Europie można określić cztery poziomy zaawansowania roli firm CIT w krajowym obrocie gotówki:

- **Commodity** – model, w którym firmy CIT ograniczają się do transportu i pakowania gotówki.
- **Podstawowy** – firmy CIT świadczą usługi rozliczania depozytów.
- **Profesjonalny** – dodatkową usługą oferowaną na rynku przez firmy CIT jest sortowanie jakościowe banknotów i monet.
- **Solution/Business Partner** – firmy CIT stają się partnerami Banków Centralnych zajmując się recyclingiem gotówki i przechowywaniem depozytów Banku Centralnego, zastępując w tym obszarze instytucje finansowe.

Niniejsza grafika poglądowo pokazuje poziom rozwoju firm CIT w krajach europejskich.



Sytuacje w poszczególnych krajach są tu jednak przedstawione w sposób uproszczony. Już teraz w polskich sortowniach część przeliczonej gotówki ponownie wraca do obrotu. Sortowanie jakościowe banknotów realizowane jest na bazie wiedzy i doświadczenia pracowników a nie wynika z jednoznacznej definicji oraz maszynowego sortowania. Nowe rozporządzenie nr 19/2016 w zakresie maszynowgo sortowania banknotów i monet wejdzie w życie po 1 lipca 2018 r. Rozporządzenie dopuszcza jednak również sortowanie ręczne. Obecnie jedynym wyznacznikiem jakościowego sortowania banknotów jest Narodowy Bank Polski, który posiadając jedną platformę sprzętową wydaje banknoty tej samej jakości niezależnie od lokalizacji.

Podsumowanie

Polska, mimo silnego lobby obrotu bezgotówkowego, jest w dalszym ciągu krajem, gdzie obrót gotówkowy stanowi główną formę płatności. Konkurencja pomiędzy firmami CIT przełożyła się na niską zyskowność ich działalności. Wprowadzone przepisy dotyczące wysokości płacy minimalnej powodują konieczność renegocjacji umów na obsługę gotówki. Trudności z pozyskaniem pracowników będą się przekładać na pogorszenie jakości poziomu obsługi. Niski poziom zysku przekłada się na wstrzymanie decyzji inwestycyjnych dotyczących unowocześnienie sortowni.

Jak przerwać to zamknięte koło? Jedynym wyjściem z tej sytuacji jest zwiększenie zakresu świadczonych usług połączone z uproszczeniem procesów i większą ich automatyzacją. Rola firm CIT w procesie obrotu gotówki w najbliższych latach będzie się zwiększać.

Koszty obrotu gotówkowego są znane, tak więc wdrożenie nowych modeli może je ograniczyć. Płatności bezgotówkowe, będące przykładem transakcji, gdzie instytucje finansowe zarabiają coraz częściej, stają się kosztem a nie przychodem. Plany polskiego rządu, związane z likwidacją opłaty *interchange*, zwiększą koszty obrotu bezgotówkowego. Nowym dużym kosztem ponoszonym przez nas wszystkich a związanym ze wzrostem płatności bezgotówkowych są inwestycje w bezpieczeństwo transakcji. Przeważnie koszty są księgowane na innych kontach i nie stanowią kosztu obrotu bezgotówkowego. Cyberzagrożenia stale rosną, więc i wydatki na bezpieczeństwo będą się zwiększać. Czy na pewno w przyszłości koszty obrotu bezgotówkowego będą niższe niż gotówka? Odpowiedź poznamy za kilka lat.

Sebastian Ptak
Członek Zarządu Blue Media S. A.

Odpowiada m.in. 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 2009 r. uhonorowany przez Związek Banków Polskich tytułem Ambasadora Gospodarki Elektronicznej, rok później Odznaką Honorową ZBP, a w 2016 r. Medalem Mikołaja Kopernika w uznaniu szczególnych zasług w budowie i rozwoju sektora bankowego.

Sebastian Ptak, Blue Media

Czy bankowcy śnią o elektronicznych płatnościach?

Twórcy książek i filmów fantastyczno-naukowych przewidzieli wiele współczesnych innowacji – telefony komórkowe, ekrany dotykowe, biometryczną autoryzację, a nawet satelity. W klasyce science fiction nie znajdziemy jednak wielu pomysłów na to, jak ludzie mogliby płacić w przyszłości. Dlaczego? Bo ludzie będą kupować, ale nie będą płacić.

Sektor finansowy, a w szczególności bankowy, goni za nowinkami. Jednak banki wprowadzają innowacje nie tylko po to, by zwiększać przychody, ale by bronić swojej pozycji i udziałów w rynku – a zarazem swoich przychodów – przed firmami fintechowymi. Obszarem, w którym banki muszą liczyć się z coraz silniejszą konkurencją ze strony światowych fintechów są płatności.

Fintechy to – w uproszczeniu – innowacyjne firmy oferujące w oparciu o rozwiązania internetowe usługi finansowe, które są wygodne i dostosowane do potrzeb internetowych i mobilnych klientów. Najczęściej próbują wykorzystywać infrastrukturę bankową, np. rachunki bankowe i w oparciu o nią tworzyć usługi wygodniejsze i tańsze. Spółki te mocno podgryzają sektor bankowy, gdyż ich strategia często polega na odebraniu bankom „ostatniej mili", czyli dostępu do klienta.

Wejście na rynek płatniczy technologicznych gigantów, dysponujących znaną i lubianą przez klientów marką, zasięgiem swoich urządzeń i systemów operacyjnych może ograniczyć pozycję banków. Te, ograniczone do funkcji dostarczycieli pieniądza, stracą źródło dochodów, jakim jest obsługa płatności. Jest jednak możliwy i drugi scenariusz – współpraca banków i fintechów. W Polsce mamy długą tradycję współpracy firm technologicznych

z instytucjami finansowymi. Jeżeli obie strony utrzymają tę współpracę, wszyscy na tym skorzystamy.

Gdzie kończy się pęd za nowymi rozwiązaniami, a zaczyna rzeczywistość?

Mechanizm elektronicznych płatności właściwie nie zmienił się od kilkudziesięciu lat. Opiera się albo na zastosowaniu karty płatniczej (znanej już od półwiecza!) albo polecenia przelewu. I chociaż co pewien czas pojawiają się nowe schematy i rozwiązania płatnicze, np. działające w oparciu o tzw. wirtualne portmonetki albo o kryptowaluty, to wciąż daleko im do popularności.

Mimo głośnych dyskusji o innowacjach w obszarze płatności należy mieć więc świadomość, że w rzeczywistości dyskutujemy niemal wyłącznie o „interfejsach", tzn. o fizycznym doświadczeniu dokonywania płatności. Dlatego innowacje w obszarze elektronicznych płatności można dziś dostrzec na trzech głównych poziomach.

Pierwszy z nich to identyfikacja i autoryzacja z rosnącym znaczeniem biometrii. Wykorzystywanie danych biometrycznych jako metody w procesach autoryzacji i uwierzytelniania klienta nie jest niczym nadzwyczajnym. Logowanie do aplikacji bankowych przez odcisk palca powoli staje się standardem, także w Polsce. Odciskiem palca możemy autoryzować płatności, np. korzystając z usługi Android Pay, Apple Pay czy aplikacji Identity Check Mobile od MasterCard'a przy okazji zakupów internetowych. Ponadto na świecie testowane są już rozwiązania autoryzujące płatności w oparciu o identyfikację głosową (rozwija je np. polska spółka VoicePIN) lub rozpoznanie kształtu twarzy klienta (tzw. selfie pay od MasterCard'a).

Poziom drugi to zmiana głównego nośnika informacji o płatności z plastiku (karty) na telefon. Biorąc pod uwagę fakt, że dzisiejsze smartfony mają więcej pamięci niż pierwszy prom kosmiczny Columbia, nie dziwi ich masowe wykorzystanie do agregowania wielu funkcji jednocześnie. I to właśnie dzięki tym możliwościom telefon wygrywa.

Smartfon stał się ekwiwalentem fizycznego oddziału banku – dzięki aplikacjom mobilnym możemy zlecać przelewy, otwierać lokaty czy starać się o kredyt. Nie musimy już odwiedzać lokalnych oddziałów naszych banków. Smartfony, dzięki różnorakim aplikacjom płatniczym od BLIK-a po Android Pay, stają się powoli także nowym rodzajem fizycznej karty płatniczej.

Prędko, prędzej, automatycznie

Poziom trzeci dotyczy szybkości i wygody przelewów. Zgodnie z unijną zasadą „D+1", zlecenie przelewu musi zostać zrealizowane przez dostawcę usług płatniczych najpóźniej do końca następnego dnia roboczego po złożeniu dyspozycji polecenia przelewu. Coraz więcej banków idzie o krok dalej i oferuje swoim klientom płatności ekspresowe, czyli takie, które pozwalają natychmiast bądź prawie natychmiast przenieść środki finansowe na wybrany rachunek. Kolejnym etapem przyspieszenia płatności będzie… zniknięcie procesu płacenia. Płatności będą bowiem odbywały się automatycznie.

Innowacje związane z szybkością i wygodą płatności to z mojej perspektywy szczególnie interesujący wątek. Opierają się one na prostym założeniu, że ludzie chcą kupować, ale nie chcą – a wręcz nienawidzą – płacić. Bo o ile kupowanie może sprawiać przyjemność, o tyle płacenie nie wywołuje już takich doznań. Dlatego sama płatność powinna być jak najszybsza, a jej moment jak najmniej zauważalny dla klienta. Dzięki automatyzacji to możliwe. Nowoczesne formy płatności staną się niewidoczne.

Amazon pod koniec 2016 r. pokazał, jak mogą wyglądać automatyczne płatności przyszłości, prezentując bezobsługowy sklep Amazon Go. Zasada działania jest bardzo prosta: klient wchodzi, wybiera produkty i wychodzi, bez stania w kolejce do kasy i fizycznego płacenia. Jak to możliwe? Wchodząc do sklepu należy zeskanować w terminalu smartfon wyposażony w aplikację Amazon Go. Wybór produktów i kompletowanie koszyka odbywa się pod czujnym okiem kamer oraz czujników zamontowanych w sklepie. Na koniec w aplikacji pojawia się lista zakupów. W momencie wychodzenia ze sklepu należność pobierana jest automatycznie z konta klienta.

Spójrzmy na Ubera – jednym kliknięciem załatwiamy wszystkie czynności związane z zamówieniem przejazdu. Sam proces płacenia jest niezauważalny, odbywa się niejako w tle. To samo dotyczy takich usług jak Spotify czy Netflix – przyzwyczailiśmy się mówić „mam Spotify", a nie „płacę ze Spotify", mimo że faktycznie co miesiąc płacimy abonament za dostęp do niego.

Popularyzacja bezobsługowych płatności to kwestia czasu. Tym bardziej, że zautomatyzowane płatności z elementem kontroli (w każdej chwili można cofnąć lub zareklamować płatność) są na rękę wszystkim: klientom, bankom, wydawcom kart płatniczych i dostawcom usług.

Wydaje się, że wszyscy powinni szukać sposobów na to, by proces płatności w ogóle zniknął.

Płatności biometryczne – przyszłość, która nadeszła

O ile wcześniej omawialiśmy rozwiązania już istniejące, to teraz zabawimy się w futurologów. Z czasem do płacenia nie będzie nam potrzebny żaden smartfon, karta czy zegarek. Nie będzie potrzebne żadne urządzenie. Reklamy już teraz przypominają, że gdy zapomnimy portfel, to zawsze możemy sięgnąć po telefon. A co jeśli zapomnę i portfela, i telefonu? Nic się nie stanie, bo do płacenia wystarczy mój palec, oko, twarz, głos albo moje zachowanie. Skoro wszystkie urządzenie są niczym innym jak substytutem tego, że to ja osobiście mogę zarządzać swoimi środkami, to spokojnie można wyeliminować tych „pośredników" i autoryzować płatności zgodnie z tym, kim jestem.

To właśnie wokół biometrii pojawia się najwięcej futurystycznych innowacji płatniczych. Chociażby Fingopay – rozwiązanie autorstwa brytyjskiej firmy Sthaler, współpracującej z Visą i Hitachi. Fingopay do dokonywania płatności wykorzystuje biometrię naczyń krwionośnych i nie wymaga posiadania fizycznego nośnika – wystarczy rejestracja danych biometrycznych i powiązanie ich z numerem karty płatniczej Visy. Transakcja odbywa się po przyłożeniu palca do czytnika naczyń krwionośnych. Co ciekawe, do przyjęcia i zautoryzowania takiej płatności po stronie sprzedawcy wystarczy jedynie tablet z odpowiednim oprogramowaniem.

Z kolei w Korei Południowej jeszcze w tym roku mają rozpocząć się testy nowego biometrycznego systemu płatności o nazwie BioPay, działającego w oparciu o technologię *palm vein* (skan naczyń krwionośnych dłoni). Po rejestracji wzoru dłoni w bankomacie czy terminalu POS zaopatrzonym w skaner naczyń krwionośnych i po powiązaniu go z numerem karty użytkownicy BioPay będą mogli płacić poprzez zwykłe przyłożenie dłoni do terminala.

Choć powyższe rozwiązania są lub w niedługim czasie będą testowane, to droga do ich umasowienia jest bardzo długa. Podstawowe pytanie brzmi, czy klienci będą skłonni, by rejestrować swoje dane biometryczne. Wydaje się, że tak – dziś mało kto pamięta, że wielu bankowców było przekonanych, iż ludzie nie zechcą udostępniać swoich wrażliwych danych telefonowi. Tymczasem klienci wręcz wymusili na bankach wprowadzenie aplikacji bankowych.

Podsumowanie

Płacenie nie jest naturalną czynnością dla człowieka, w przeciwieństwie do gromadzenia dóbr. W jakim kierunku zmierza rynek płatności, można dostrzec, przyglądając się historii płatności. To nic innego, jak historia stopniowego pozbywania się w procesie płacenia fizycznej reprezentacji wartości nabywanego lub zbywanego dobra lub usługi – od wymiany barterowej, przez reprezentację wartości w kruszcu, gotówkę, kartę płatniczą, smartfon aż do technologii pozwalających płacić bez jakiegokolwiek fizycznego nośnika.

Czy zatem bankowcy powinni cały czas myśleć o innowacjach płatniczych? Nie! Internet komercyjny ma ćwierć wieku, smartfony – dziesięć lat. W tym czasie pojawiło się więcej innowacji w obszarze płatności niż kiedykolwiek wcześniej. Czy dekadę temu przewidywaliśmy, że telefon tak bardzo zmieni świat finansów? Raczej nie. Nie powinniśmy szukać innowacji płatniczych na siłę, powinniśmy raczej obserwować nowe technologie i wyciągać wnioski, jak one zmienią nasz świat.

W sytuacji upowszechnienia się automatycznych płatności jest możliwe, że banki stracą bezpośredni kontakt z klientem. Dlatego bankowcy zamiast śledzić świat fintechów powinni brać z nich przykład i po prostu obserwować ludzi. Jeśli usługi bankowe, w tym płatnicze, mają realnie odpowiadać na potrzeby swoich klientów, banki muszą śledzić nawyki swoich klientów poza sferą bankową.

Jeśli chcemy wiedzieć, jak proces płatności będzie wyglądał za 5–10 lat, musimy zrozumieć nie tylko millenialsów, ale również ich młodszych, nastoletnich kolegów i koleżanki. Co istotne, dla tych pokoleń ważniejsze od regulacji rynkowych staje się zaufanie do samej marki. Z ubiegłorocznego badaniu Blue Media „Podejście Polaków do fintechu" wynika, że aż 72 proc. polskich millenialsów ufa koncernom technologicznym, takim jak Google, Facebook czy Apple. Z kolei według amerykańskiego badania „The Millennial Disruption Index" 73 proc. ankietowych większym entuzjazmem darzy usługi finansowe oferowane przez firmy technologiczne niż banki. Dlaczego? Bo w świecie tych marek są zanurzeni w sposób naturalny, na co dzień.

Musimy szukać odpowiedzi nie tylko na pytanie, jak i gdzie klienci płacą, ale jak zmienia się ich życie pod wpływem technologii.

Postęp technologiczny w fundamentalny sposób wpływa na funkcjonowanie zarówno całego otoczenia, w jakim żyjemy jak i na nas samych. Zmiany technologiczne i związane z nimi innowacje determinują również w wielu elementach działanie sektora finansowego. Jednocześnie, technologia powoduje konwergencję sektorów i zmniejsza bariery wejścia innych podmiotów w tradycyjne obszary działalności banków. Klienci, w wyniku postępującej digitalizacji i zmieniających się oczekiwań generacji tzw. millenialsów, są coraz bardziej wymagający. Jest już pewne, że w wyniku postępujących technologii, takich jak sztuczna inteligencja czy automatyzacja, dojdzie do zasadniczych zmian na rynku pracy i, w konsekwencji, także w sektorze finansowym.

W tej rzeczywistości obszar informatyki jest kluczowy, by wyzwania stojące przed bankami wynikające z tych megatrendów zmieniły w wykorzystane szanse. Zaawansowane technologie służące wygodnej, prostej komunikacji z bankiem, ale odporne na cyberataki, to dzisiaj podstawowy standard, którego oczekują klienci. Jednocześnie, aby dostarczać klientom dodatkową wartość, banki wykorzystują i analizują olbrzymie zbiory danych i wykorzystują najnowsze trendy technologiczne. Na bieżąco też instytucje finansowe muszą spełniać cały szereg nowych regulacji wynikających ze zmian technologicznych.

Niniejsza publikacja „Wyzwania informatyki bankowej" stanowi bardzo cenny przegląd najważniejszych zagadnień w zakresie zmian technologicznych, przed którymi stoi obecnie sektor bankowy. A zagadnień tych jest wiele, począwszy od wpływu zmieniających się potrzeb klientów, przez szereg nowych regulacji, jak na przykład PSD II czy ochrona danych osobowych, zmiany modelów biznesowych, sposobów dokonywania płatności, cyberbezpieczeństwo, na nowych technologiach takich jak Blockchain skończywszy. To, co wyróżnia tę publikację w sposób szczególny, to spojrzenie na te najważniejsze obecnie obszary informatyki bankowej w sposób prosty i zrozumiały, adresowany do szerokiego grona odbiorców.

Iwona Kozera
Partner EY
Lider Doradztwa Biznesowego w Europie Wschodniej i Środkowej

ISBN 978-83-945091-1-8