Wyzwania informatyki bankowej

Pod redakcją Andrzeja Kawińskiego i Andrzeja Sieradza

Wyzwania Informatyki Bankowej

– Materiał przygotowany na podstawie seminariów „IT w instytucjach finansowych'' organizowanych przez Gdańską Akademię Bankową

GDAŃSK 2014

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

Redaktorzy: Andrzej Kawiński, Andrzej Sieradz

Opracowanie redakcyjne: Wojciech Gryciuk

Projekt graficzny: TOFU

Skład: Łukasz Sitko

ISBN 978-83-88835-20-9

CIP - Biblioteka Narodowa

Wyzwania informatyki bankowej : materiał przygotowany na podstawie seminariów IT w instytucjach finansowych organizowanych przez Gdańską Akademię Bankową / [red. Andrzej Kawiński, Andrzej Sieradz]. - Gdańsk : Instytut Badań nad Gospodarką Rynkową, 2014

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

Spis treści

Wstęp ... 7

Justyna Kesler, Ewa Hadasz
Zarządzanie oczekiwaniami biznesu wobec IT ... 11

Maciej Majewski
Big Data w bankowości – wyzwania ... 21

Bartłomiej Nocoń, Bartosz Zborowski
Bankowość mobilna i płatności mobilne ... 35

Maciej Gawroński
Aspekty prawne cloud computingu w odniesieniu do sektora bankowego (regulacje EU) ... 45

Andrzej Pyka
Pokolenie Y: nowy rodzaj pracowników – szanse i zagrożenia ... 61

Andrzej Gibas
Efektywny model bankowości ... 71

Maciej Kaniewski
Metodyka Agile – blaski i cienie ... 81

Aleksander P. Czarnowski
Obecne zagrożenia w bankowych systemach IT ... 95

Andrzej Koweszko
Zagrożenia sektorowe płatności natychmiastowych ... 119

Grzegorz Kuliszewski, Andrzej Sieradz
Przyszłość centralnych systemów bankowych ... 133

Rafał Burzyński, Tomasz Rzepa, Jakub Chadysz
FATCA – analiza porozumienia IGA wynegocjowanego przez Polskę ... 149

Marek Grajek
Uwierzytelnianie klienta banku w rozwoju cyfryzacji sektora publicznego ... 161

Wstęp

Pomysł niniejszego opracowania został zainspirowany dorocznym spotkaniem Rady Programowej Konferencji „IT - w instytucjach finansowych", poprzedzającym przygotowania do tego wydarzenia.

Co roku, i to już od dziewiętnastu lat, przedstawiciele sektora finansowego spotykają się pod auspicjami Gdańskiej Akademii Bankowej w celu przedyskutowania najważniejszych wyzwań, jakie stoją przed instytucjami finansowymi w Polsce. Zwykle owocem prezentacji i szerokiej dyskusji, jaka im towarzyszy, jest kilka rekomendacji dotyczących zagadnień ważnych dla rozwoju usług finansowych, co do których, według opinii uczestników, należy podjąć inicjatywy sektorowe. Dyskusja nad agendą tegorocznego spotkania, jako również chęć przedstawienia wieloletniego dorobku tego uznanego na rynku seminarium, uświadomiła nam konieczność odniesienia się do kilkunastu zagadnień, które pojawiają się w naszych dyskusjach od kilku lat, a które uznaliśmy za wyjątkowo ważne z punktu widzenia rozwoju technologii informacyjnych w bankowości. Przyglądając się ponownie wyzwaniom, jakie stoją przed nowoczesnym sektorem finansowym, doszliśmy do wniosku, że wiele z nich już staje się naszą rzeczywistością. Wielokrotnie wyzwania prezentowane przez uczestników konferencji stały się codziennością, która umożliwiła rozwój biznesowy instytucji finansowych. Cześć nowych jest konsekwencją dynamicznie rozwijających się usług bankowych opartych na nowych technologiach IT, w szczególności technologiach mobilnych. Postanowiliśmy zatem podjąć próbę problemowego zaadresowania tych zagadnień, które według naszej opinii będą decydowały o dalszym rozwoju usług i produktów sektora finansowego. Naszym zamierzeniem nie było powtarzanie wniosków z dyskusji i prezentowanie potencjalnych rozwiązań. Chcieliśmy raczej odnieść się

do szeregu wyzwań i potencjalnych problemów, z jakimi większość instytucji finansowych w Polsce będzie musiała się zmierzyć w nadchodzących latach. Intencją podjęcia prezentowanych zagadnień było zatem odniesienie się do nich z punktu widzenia przyszłości usług finansowych, a nie pojedynczego uczestnika rynku, jakim jest np. bank. Znalazły się wśród nich takie zagadnienia, jak bankowość mobilna, bezpieczeństwo transakcji płatniczych, współpraca z pozabankowymi uczestnikami rynku płatniczego czy wymiana technologiczna związana z wielokanałowością dystrybucji produktów i usług finansowych.

Funkcjonowanie instytucji finansowych obecnie nie jest możliwe bez informatyki. Prawidłowe współdziałanie i wzajemne zrozumienie departamentów informatycznych z departamentami biznesowymi jest podstawą rozwoju i sukcesu na konkurencyjnym rynku bankowym. Przygotowując publikację, chcieliśmy w sposób przystępny zaprezentować zagadnienia, które omawiamy w wąskim gronie informatycznym, adresując je szerszemu gronu odbiorców, szczególnie tym którzy są użytkownikami tego typu rozwiązań. Zależało nam aby poruszone w publikacji zagadnienia stosunkowo szeroko omawiały wyzwania, które stoją przed informatyką bankową. Tematy zawarte w publikacji nie zamykają listy wszystkich wyzwań, które będą tematami kolejnych seminariów.

Swoją propozycję przekrojowego zaadresowania ważnych problemów sektora finansowego skierowaliśmy do osób, które aktywnie uczestniczyły w poprzednich konferencjach oraz które z racji pełnionych funkcji zawodowych zajmują się tymi zagadnieniami. Z tego miejsca chcemy im bardzo serdecznie podziękować za włożony trud w przygotowanie niniejszej publikacji. Mamy nadzieję, że lektura poniższego zbioru artykułów będzie dla Państwa inspiracją do własnych przemyśleń i decyzji w zakresie prezentowanych wyzwań.

Wyrazy podziękowania chcielibyśmy przekazać prof. Leszkowi Pawłowiczowi za cenne uwagi w czasie przygotowywania publikacji.

Andrzej Kawiński
Andrzej Sieradz

Justyna Kesler
Wiceprezes Zarządu ING Banku Śląskiego odpowiedzialna za obszary IT, operacji, usług i zarządzanie zmianą. Absolwentka Szkoły Głównej Planowania i Statystyki w Warszawie (obecnie Szkoła Główna Handlowa) na kierunku cybernetyka ekonomiczna i informatyka.

Ewa Hadasz
Dyrektor departamentu w ING Bank Śląski, odpowiedzialna za rozwój i utrzymanie aplikacji dla klienta korporacyjnego i strategicznego.
Od kilkunastu lat związana z obszarem IT, w ramach którego przeszła ścieżkę od analityka do zarządzającego realizacją wielowątkowych, złożonych projektów informatycznych. Posiada certyfikat Project Management Professional PMP. Ma duże praktyczne doświadczenie we współpracy z biznesem w kreowaniu i wdrażaniu procesów *demand management*, zdobyte m.in. w trakcie pełnienia roli Account Managera IT.

Justyna Kesler, Ewa Hadasz, ING Bank Śląski

Zarządzanie oczekiwaniami biznesu wobec IT

Rynek usług bankowych jest rynkiem o długiej tradycji funkcjonowania, ale wciąż dynamicznie się rozwijającym i mocno konkurencyjnym. Jednocześnie jest to obszar podlegający restrykcyjnym regulacjom prawnym.

Bardzo duży wpływ na działalność banków ma aktualna sytuacja makroekonomiczna. Instytucje finansowe jako podmioty gospodarcze muszą reagować na globalne czynniki ekonomiczne, jak np. tempo wzrostu PKB, poziom obrotów z zagranicą, popyt krajowy oraz bezpośrednio na nie wpływające instrumenty polityki pieniężnej, np. wysokości stóp procentowych czy wysokość rezerw obowiązkowych.

Jednocześnie, będąc instytucjami zaufania publicznego, banki zobowiązane są do minimalizacji ryzyka działalności, ściśle przestrzegając narzuconych przez regulatorów rozmaitych zaleceń i rekomendacji sztywno określających ramy działalności. Jako przykład można podać rekomendację S dotyczącą zarządzania obszarem kredytów hipotecznych, rekomendację M dotyczącą zarządzania ryzykiem operacyjnym czy rekomendację D z obszaru IT.

W ostatnich czasach narastają na sile inne elementy w zasadniczy sposób determinujące kierunki działania banków i wymuszające nowe spojrzenie na oferowane produkty i rozwiązania.

Jednym z najważniejszych jest nowy typ konkurencji, który w usługach bankowych zaczyna wykraczać poza instytucje bankowe. Bill Gates w 1994 roku stwierdził, że „Bankowość jest niezbędna, ale banki nie".[1] Ten trend jest już mocno zauważalny. Realizację płatności mobilnych zaczynają przejmować operatorzy telekomunikacyjni czy instytucje płynnościowe i nie tylko dokonują przelewów.

---

1 K. Brett, *Bank 3.0. Nowy Wymiar Bankowości*, Wydawnictwo Studio Emka, Warszawa 2013, str. 57.

Równocześnie jesteśmy świadkami niesamowitego przyspieszenia postępu technologicznego, np. przeciętny mainframe (superkomputer) z lat 70., który kosztował ponad 1 mln USD, miał mniejszą moc obliczeniową niż dzisiejszy, średniej klasy smartfon. Pojawiają się też produkty wykorzystujące rozwiązania NFC (*Near Field Communication*), BLW (*Bluetooth Low Energy*), pisane RWD (*Responsive Web Design*), itd.

Wzrastający poziom informatyzacji społeczeństwa jest bardzo zauważalny w sektorze bankowości. W 2010 roku ponad 16,2 mln klientów miało podpisane umowy na korzystanie z bankowości elektronicznej, a 3 lata później już 21,5 mln,[2] co stanowi prawie 60% ludności Polski.

Postęp, jaki się wciąż dokonuje obrazuje również poniższy przykład dotyczący roku 2012, który zakończył się liczbą 350 tys. zagrożeń wymierzonych w system Android. Stosunek przyrostu liczby nowych złośliwych aplikacji na Androida w porównaniu do nowych złośliwych aplikacji wymierzonych w pecety wynosił wtedy 14:3. Android potrzebował jedynie trzech lat, by dotrzeć do poziomu złośliwego oprogramowania, do którego pecety dotarły w ciągu lat czternastu.[3]

Dodatkowo niesamowicie wzrosła świadomość i oczekiwania klientów. Dzisiejszy klient, bardzo często korzystający z nowych technologii, poszukuje rozwiązań wygodnych, funkcjonalnych, często „szytych na miarę", a nade wszystko niezawodnych. Sprostanie jego oczekiwaniom wymaga ciągłych zmian w procesach i aplikacjach, jakie się mu udostępnia. Klient ma możliwość oceniania jakości produktów i jakości obsługi głównie poprzez media społecznościowe i coraz częściej z tego korzysta. Stwarza to dla banków nowe możliwości, bo dzięki temu tworzy się istotny kanał dla lepszego zrozumienia jego potrzeb i oczekiwań, ale jednocześnie czas reakcji na potrzeby klienta ulega dalszemu skróceniu.

Powyższe czynniki determinujące działalność banków w bezpośredni lub pośredni sposób znajdują odzwierciedlenie w oczekiwaniach wobec IT, stawianych przez jednostki biznesowe tworzące rozwiązania dla klienta. Niniejszy artykuł stawia sobie za cel przedstawienie, jak takimi oczekiwaniami może zarządzać IT.

Można wymienić kilka obszarów działania IT, względem których są stawiane oczekiwania biznesu:

---

2 Raport NetB@nk, ZBP http://zbp.pl/raporty/raport-netb-nk

3 2012 Annual Security Roundup, *Evolved threats in a "post-PC" world – Trend-Micro* http://www.trendmicro.pl/security-intelligence/research/index.html

I. Działalność utrzymaniowa.
II. Efektywność kosztowa.
III. Wdrażanie nowych rozwiązań.
IV. Inspirowanie do nowych produktów, innowacyjność.

I. Działalność utrzymaniowa

Pod tym terminem rozumie się przede wszystkim zapewnienie ciągłości pracy systemów, obsługę Help Desk oraz obsługę operacyjną narzędzi pracy dostępnych dla pracowników banku.

Oczekiwania jednostek biznesowych wobec tego aspektu działania IT to: jak najwyższa dostępność systemów i ich niezawodność, jak najmniejsza liczba awarii, a w przypadku problemów szybkość reakcji i możliwość błyskawicznego wypracowania rozwiązań zastępczych. Niezmiernie ważna jest też jakość i profesjonalizm obsługi.

W dużym stopniu te oczekiwania przekładają się na konkretne miary, stąd głównymi metodami zarządzania tym obszarem oczekiwań jest SLA (*Service Level Agreement*) pomiędzy biznesem i IT. Odpowiednio ustawione KPI (*Key Performance Indicators*) wzmacniają istotność tego jednego z kluczowych czynników.

Sądzimy, że miarą sukcesu działania IT i poziomu zadowolenia biznesu, a przede wszystkim klienta w obszarze działalności utrzymaniowej jest niezauważalność tego elementu. Im mniej się o tym mówi wewnątrz banku i wśród klientów (np. na forach społecznościowych), tym lepiej działa IT. Taka niezauważalność jest niezbędną podstawą dla funkcjonowania IT w dzisiejszej rzeczywistości. Peter Hinssen stwierdził, iż „dzisiaj jest zero tolerancji dla awarii”[4] i trudno się z tym nie zgodzić.

II. Efektywność kosztowa

Dzisiaj chyba nikt nie może sobie wyobrazić funkcjonowania banku bez IT. Z jednej strony dobre IT jest niezbędne dla skutecznego działania banku, z drugiej jest jednak istotnym i coraz większym czynnikiem kosztowym. Niestety, często jest tak odbierane – szczególnie, jeżeli za nakładami na IT nie podążają właściwej wielkości przychody biznesu.

4 P. Hinssen, *The New Normal explore the limits of the digital world*, ACROSS Technology, s. 46–48.

Zatem oczekiwania jednostek biznesowych w tym elemencie koncentrują się przede wszystkim na obniżeniu kosztów działania i szukaniu optymalnych rozwiązań pozwalających zatrzymać tendencje wzrostowe.

Zarządzanie kosztami bezpośrednio po stronie IT jest realizowane poprzez szukanie tańszych platform i bardziej efektywnych rozwiązań, optymalizacje *backupów*, które dzisiaj stanowią istotny koszt, automatyzacje procesów wytwórczych (integracji, testów, instalacji), outsourcing, efektywne wykorzystywanie dostawców zewnętrznych, *body leasing* versus rozwój wewnętrzny, rozszerzenie stosowania *End User Computing*, itd.

Możliwości podnoszenia efektywności kosztowej jest wiele, natomiast istotnym elementem ułatwiającym zarządzanie oczekiwaniami biznesu w tym zakresie jest transparenty układ i przejrzystość podziału kosztów na każdym poziomie: jednostki biznesowej, poszczególnych aplikacji, procesów i nawet w warstwie produktów. Właściwa alokacja pełnych kosztów IT powinna wpływać na bardziej racjonalne decyzje inwestycyjne po stronie biznesu oraz ułatwiać identyfikację obszarów do optymalizacji. W tym bardzo nam pomagają coraz tańsze technologie, które dotychczas uważano za użyteczne jedynie dla osób fizycznych, a nie dla dużych korporacji.

Świadomość po stronie biznesu wielkości i struktury kosztów IT oraz czynników je determinujących ma niebagatelne znaczenie dla podejmowania również przyszłych decyzji biznesowych zarówno przy zakupie gotowych rozwiązań, jak i przy projektowaniu nowych. A świadomość ta rośnie, jeśli IT dostarcza rzetelnej, przejrzystej i zrozumiałej informacji o kosztach swoich usług.

III. Wdrażanie nowych rozwiązań

Uważamy, że czynniki zewnętrzne, o których wspominałyśmy na wstępie, wywierają szczególnie duży wpływ na działanie IT.

Oczekiwaniem biznesu jest tutaj szybkość reagowania na potrzeby klienta, przygotowywanie rozwiązań łatwych w korzystaniu, intuicyjnych oraz, szczególnie po stronie klientów korporacyjnych, rozwiązań „szytych na miarę". Realizacja tych celów w dzisiejszej rzeczywistości nie jest możliwa bez bezpośredniej współpracy pomiędzy jednostkami biznesowymi, jednostkami operacyjnymi i IT, która jest oparta na zdecydowanie partnerskich i równoprawnych relacjach. Każda ze stron wnosi tu niezbędną wiedzę i doświadczenie dla wypracowania najlepszych rozwiązań. Jednostki biznesowe – przede

wszystkim znajomość potrzeb klienta, jednostki operacyjne – wiedzę jak zastosować efektywnie proces, a IT – technologię i finalną realizację. Słowa Vince Lombardiego, coacha futbolu amerykańskiego, dobrze to obrazują: „osiągnięcia organizacji są rezultatem wspólnego wysiłku każdego z jej członków z osobna".[5]

Bardzo bliski i ścisły model pracy wymaga pojawienia się nowych ról w relacjach biznes – IT, wdrożenia nowych metod realizacji zmian a nade wszystko ludzi z określonym profilem kompetencji. Zarządzanie potrzebami biznesowymi realizowane jest na różnych płaszczyznach współpracy.

Struktura organizacyjna

Patrząc z tej perspektywy konieczne jest jeszcze większe nakierowanie i skoncentrowanie jednostek IT na poszczególnych liniach biznesowych, tak aby w najlepszy sposób zrozumieć potrzeby i oczekiwania klientów.

Skutecznym rozwiązaniem może być ustanowienie funkcji, która zarządza relacją IT – biznes. Panuje nad całością realizowanych zadań bez wchodzenia w zbytnie szczegóły oraz otwiera „właściwe drzwi" po obu stronach, aby szybko i skutecznie realizować szczególnie priorytetowe zadania. Skraca do minimum czas konieczny na znalezienie po obu stronach właściwych adresatów tematów, czasami również rozładowuje napięcia we współpracy IT i biznesu.[6]

Funkcja ta może się przerodzić w strukturę IT ułożoną per linia biznesowa, czyli w utworzenie jednostek dedykowanych poszczególnym liniom biznesowym bądź przynajmniej wyznaczeniem roli opiekuna linii biznesowej AM (*Account Manager*) – tzw. koncepcji BRM (*Business Relationship Management*). Pełniejszą formą jest dedykowana jednostka IT, wówczas znajomość specyfiki klienta jest „wzmocniona" na każdym poziomie współpracy IT z biznesem, co w efekcie przyczynia się do ciągłych, bliskich relacji i zdecydowanie lepszego ukierunkowania na klienta.

Taką ścieżką podąża właśnie nasza organizacja. Przez kilka lat za kontakty z biznesem odpowiadała grupa Account Managerów: trzy osoby reprezentujące cztery główne linie biznesowe i jedna odpowiedzialna za jednostki wsparcia. Pomimo pozytywnych efektów funkcjonowania takiego modelu

5 P. Hinssen, *The New Normal...*, ACROSS Technology, s. 122.

6 Sz. Augustyniak, *Uwaga! BRM zmienia podejście biznesu do IT*, CIO nr 03/2012.

podjęto decyzję o wyodrębnieniu dedykowanych jednostek reprezentujących biznes, aby jeszcze bardziej wzmocnić współpracę pomiędzy jednostkami biznesowymi i IT. Póki co nie można jeszcze mówić o jej efektach – zmiana funkcjonuje od początku tego roku.

Organizacja pracy

Dla lepszego zarządzania oczekiwaniami IT – biznes nie wystarczą jednak tylko nowe role czy struktury, konieczna jest również zmiana metod pracy. Tradycyjne metody *waterfall'owe* coraz częściej są wypierane przez bardzo obecnie popularne metody *agile'owe*. Chociaż jest ich kilka (*Scrum*, *Dynamic Systems Development Methodology – DSDM*, *Feature Driven Development – FDD*, *Crystal*, *Lean*, *Extreme Programming*[7]), coraz bardziej popularna staje się ta pierwsza. Przy pełnej formie realizacji zadań element ścisłej, interakcyjnej współpracy nabiera jeszcze większego znaczenia i przy dużej zmienności otoczenia jest po prostu niezbędny. Przy realizacji tematów trudnych, gdzie wyzwaniem jest duża liczba niewiadomych, można małymi interakcjami uzyskać najlepsze efekty. Prototypowanie, co jest często wykorzystywane w *scrumach*, z jednej strony jest ciągłą weryfikacją potrzeb, a z drugiej zmniejsza koszt nietrafionych rozwiązań. Oczekiwania klienta są wspólnie i na bieżąco aktualizowane. Przy tym podejściu zaangażowanie strony biznesowej w realizację zadania musi być jeszcze większe niż w tradycyjnych metodach realizacji.

Oczywiście, przejście na formę pracy *scrum* nie jest proste. Wymaga nie tylko zmian organizacyjnych po stronie IT, ale również po stronie jednostek biznesowych. Niezbędna jest dojrzałość wewnętrzna organizacji oraz zaakceptowanie sytuacji, gdy na początku prac nie ma z góry określonych trzech podstawowych elementów – czasu, pieniędzy i zakresu.

W naszym przypadku większość prac rozwojowych jest już aktualnie realizowana metodami *scrum'owymi*, przy czym proces wygląda różnie w poszczególnych obszarach. Związane jest to przede wszystkim z różnym poziomem oczekiwań jednostek biznesowych, możliwościami jego zaangażowania się w proces oraz dojrzałością zespołu. Niemniej jednak, bazując na prawie dwóch latach doświadczeń w posługiwaniu się tą metodą, można stwierdzić, iż jest ona skuteczna, sprawdziła się i przynosi spodziewane efekty.

7 M. Chrapko, *SCRUM o zwinnym Zarządzaniu Projektami*, Helion, Gliwice 2013, s. 44–49.

Ludzie

Obok nowych ról i procesów zarządzanie oczekiwaniami jednostek biznesowych wobec IT wymaga ludzi z określonymi kompetencjami. Oczywiście, na każdym poziomie struktury organizacyjnej występuje inne zapotrzebowanie na różne kompetencje, niemniej jednak jest możliwe określenie kilku głównych, wspólnych dla wszystkich cech. Można do nich zaliczyć zdolności komunikacyjne, umiejętność jasnego formułowania swoich opinii, odwaga, pewność siebie i umiejętność pracy w zespole. W przypadku wspólnej pracy, gdzie zderzenie różnych poglądów i opinii jest codziennością, cechy takie są niezbędne. W zapomnienie przechodzi już obraz pracownika IT, który siedząc przy biurku coś realizuje, ale nie wiadomo co i na kiedy. Dzisiaj ma to być osoba otwarta, komunikatywna i nastawiona na współpracę.

IV. Inspirowanie do nowych produktów, innowacyjność

Ostatnim obszarem oczekiwań biznesu wobec IT jest inspirowanie i wyszukiwanie nowości, które pozwalają tworzyć nowe, innowacyjne rozwiązania. W tym aspekcie IT ma bardzo duże pole do działania. W strukturach IT jest wielu doskonałych specjalistów znających nowinki technologiczne i mających dużą wiedzę, dla których świat nowych technologii to często pasja. Mamy również architektów IT, którzy koncentrują się dzisiaj nie tylko na aspektach technologicznych, ale również, a może przede wszystkim, wyszukują w IT nowe trendy i rozwiązania, które mogą mieć wartość dla biznesu. W gąszczu informacji konieczna jest umiejętność przedstawienia i „zarażenia" pomysłami strony biznesowej. Dalej idąc, jeżeli temat zostanie „kupiony", bycie gotowym na realizację zarówno od strony merytorycznej jak i organizacyjnej. Również, a może przede wszystkim, ten obszar oczekiwań biznesu wobec IT wymaga ścisłej wzajemnej współpracy, ponieważ szybka reakcja i wdrożenie nowatorskich rozwiązań daje szanse na wypracowanie przewagi konkurencyjnej na rynku. Mamy świadomość, że świat pędzi do przodu i za chwilę ktoś inny wymyśli coś nowego, lepszego. Natomiast brak realizacji nowatorskich rozwiązań może w dłuższej perspektywie być bolesne.

Podsumowanie

Reasumując powyższe rozważania: zarządzanie oczekiwaniami jest realizowane przy wykorzystaniu różnych narzędzi i różnymi metodami. Dzisiejsza rzeczywistość wymaga ciągłego doskonalenia, ciągłej zmiany i nade wszystko pracy zespołowej. Sądzimy, że w każdym z tych aspektów osiągnięcie sukcesu wymaga partnerskich relacji, otwartości, transparentności oraz klarownej i jasnej komunikacji, a także brania na siebie odpowiedzialności, decyzyjności i wspólnego dążenia do jednego celu. I takie właśnie zadania bierze na siebie nowoczesne i efektywne IT.

dr Maciej Majewski
Prezes Zarządu Pentacomp S.A.
Ma 30-letnie doświadczenie w realizacji i zarządzaniu projektami informatycznymi, zdobyte na kilku kontynentach. Przez wiele lat pracował w firmach doradczych. Wcześniej, pracując za granicą u producentów wysokich technologii IT, współtworzył rozwiązania bazodanowe oraz zastosowania sztucznej inteligencji w zarządzaniu. Od lat kieruje projektami wdrożeń systemów transakcyjnych oraz systemów decyzyjnych informacji zarządczej. Specjalizuje się w sektorach bankowości, finansów oraz sprzedaży detalicznej. Kierując obecnie firmą specjalizującą się w projektowaniu i wdrażaniu złożonych rozwiązań informatycznych w coraz większym stopniu korzysta z technologii i metod związanych z dziedziną Big Data.

dr Maciej Majewski, Pentacomp

Big Data w bankowości – wyzwania

Dziennikarze kochają sensacje! Toteż nie powinno nikogo dziwić, że zapowiedź wprowadzenia nowoczesnego systemu powiadamiania klientów w zależności od miejsca, w którym akurat przebywają, zostało podchwycone jako sensacyjna próba permanentnego śledzenia klientów przez banki. Skojarzenie z orwellowskim Big Brother nasuwało się prawie automatycznie. A jako, że zastosowana technologia wywodzi się z szeroko pojętej tematyki Big Data to nietrudno o natychmiastowe skojarzenie: Big Data to Big Brother! Mniej więcej rok temu polskie media podchwyciły te hasła i niestety tematyka Big Data źle się od tego czasu kojarzy.[1]

Oczywiście nie chodziło o inwigilację klientów. System miał udzielać korzystnych dla klienta podpowiedzi, np. o tym, że w mijanym właśnie sklepie przysługuje mu 10% rabatu na wszystkie zakupy. Bank wysyłający taką wiadomość chciał ułatwić decyzję zakupu. Klient korzystający z tej usługi może ją też w każdej chwili wyłączyć. Warto o tym pamiętać i ciągle o tym przypominać, że nic nie dzieje się bez woli klienta! W oparciu o własne doświadczenia mogę twierdzić, że jako klient wysoko cenię sobie wszelkiego rodzaju usługi dodane, ułatwiające życie, pracę i zakupy. Sądzę też, że jest nas więcej.

Można też zastanowić się, jaką faktyczną wartość dla banku miałby pełen zestaw danych o trasie, po której poruszają się klienci. Załóżmy, że dane lokalizacyjne wysyłane są przez smartfon w odstępach 10-sekundowych, co daje w ciągu doby 8 640 informacji o położeniu. Dla miliona klientów dane z jednej tylko doby to blisko 10 mld rekordów. Jeżeli bank zapamiętuje tylko numer klienta i położenie w postaci współrzędnych WGS84 używanych przez

1 *Alior Bank i „permanentna inwigilacja". Czy powinniśmy już zacząć się bać tego pana?*, Gazeta Wyborcza, 19.02.2013.

popularny system Android to możemy przyjąć, że jeden taki rekord zawiera ok. 80 bajtów. Tak więc już po roku wielkość bazy „surowych" danych zbliża się do wielkości 300 terabajtów. Dla klientów największego polskiego banku byłoby to ponad dwa petabajty! Odpowiedź na pytanie, co bank miałby zrobić z tym „bogactwem" pozostawiam autorom tytułowej zbitki: Big Data = Big Brother.

Z powyższego przykładu wypływa jednak jeden ważny wniosek. Upowszechnienie smartfonów jest jedną z ważnych przyczyn zjawiska nazwanego „tsunami danych". Dane lokalizacyjne, wpisy na forach społecznościowych, setki milionów zdjęć i filmów publikowanych codziennie w sieci to tylko wierzchołek tej fali. Masowa produkcja danych na niewyobrażalną do tej pory skalę prowadzi prostą drogą do zjawiska Big Data. Ignorowanie tego zjawiska lub sprowadzanie do niepoważnych porównań typu Big Brother jest równoznaczne z zamknięciem oczu na jedną z największych zmian, jakie technologia wprowadziła do naszego życia z perspektywy całej historii ludzkości.

Czy obecne systemy bankowe spełniają definicję Big Data?

Już kilkanaście lat temu, bo w 2001 roku META Group (obecnie Gartner) opublikowała raport[2], który definiuje Big Data jako bardzo duże zbiory danych spełniające kryterium nazwane 3V. Te trzy V to:

- *Volume* – duża ilość danych,
- *Velocity* – duża zmienność danych,
- *Variety* – duża różnorodność danych.

Dla banków, które już od ponad dziesięciu lat realizują zalecenia Nowej Umowy Kapitałowej, znanej jako Bazylea 2, pierwsze z kryteriów nie jest trudne do spełnienia. Większość stworzyła bowiem hurtownie danych, w których przechowuje historie transakcji klientów służące w pierwszej kolejności do badania zdolności kredytowej. Będąc zasilane codziennie lub nawet częściej przez bankowe systemy transakcyjne oraz osiągając wielkość nawet setek terabajtów są na ogół posadowione na relacyjnych bazach danych, które zapewniają spójność oraz bezpieczeństwo dostępu do danych. Określone zapytania, kierowane do tych baz przez pracowników sprzedających kredyty, pozwalają z bardzo niewielkim opóźnieniem (kilkanaście sekund do kilku

2 Laney Douglas, *3D Data Management: Controlling Data Volume, Velocity and Variety*, Gartner, 6.02.2001.

minut) udzielić odpowiedzi na zapytanie o możliwość uzyskania kredytu wnioskowanego przez klienta.

Znacznie trudniej spełnić bazom bankowym kryterium dużej różnorodności. W zasadzie wszystkie aplikacje finansowe oparte są o statyczne modele danych, dzięki czemu każde użyte pole zawierające informację jest dobrze zdefiniowane i opisane. Numer IBAN ma 26 znaków i dla Polski zawsze zaczyna się od tych samych dwóch znaków: PL. Dla zapewnienia blisko 100-procentowej spójności, integralności i zgodności stosuje się różnego rodzaju dodatkowe mechanizmy: sumy sprawdzające, listy dopuszczalnych wartości, itp. Dzięki temu osiąga się wysoką wiarygodność, co jest absolutnie niezbędne zarówno w relacjach z klientami, jak i w sprawozdaniach dla regulatora. Ceną, jaką banki płacą za dokładność, są sztywne schematy danych. A te są wręcz zaprzeczeniem różnorodności. Tymczasem różnorodność danych Big Data nie stoi w sprzeczności z podstawowym mechanizmem korzystania z tych danych, jakim są analizy statystyczne. Wynikiem analizy jest zwykle wartość określonej funkcji prawdopodobieństwa, która wyliczana jest w oparciu o wielką (Big) liczbę działań na wielkiej liczbie danych. Dla tak obliczanej funkcji nie wszystkie dane wejściowe muszą być kompletne, spójne i dokładne. Część z nich może zostać odrzucona, a mimo to będziemy w stanie podjąć poprawną decyzję, gdy wspiera ją najwyższe prawdopodobieństwo osiągnięcia pożądanego skutku. Tego rodzaju podejście nie jest akceptowane w raportach finansowych, często ze stratą dla ich jakości, czytelności i wartości. Statystyki realizowane na Big Data przy tych samych statystykach na danych w typowej hurtowni to jak delektowanie się widokiem Słoneczników Vincenta van Gogha przy oglądaniu tysiąca pikseli wyjętych z tego obrazu. Typowe raporty dotyczą przeszłości i mogą być tworzone w dłuższym okresie czasu.

W przypadku zastosowań Big Data analiza często dotyczy przyszłości i służy wsparciu decyzji, które muszą być podjęte natychmiast.

Aby uwzględnić ten główny obszar zastosowania technik Big Data, w roku 2012 Gartner uzupełnił podaną wcześniej definicję 3V wskazując, iż:

„Big Data to zbiory informacji o dużej objętości, dużej zmienności i/lub dużej różnorodności, które wymagają nowych form przetwarzania w celu wspomagania podejmowania decyzji, odkrywania nowych zjawisk oraz optymalizacji procesów".[3]

---

3 Laney Douglas: *The Importance of "Big Data": A Definition*, Gartner, 21.06.2012.

W kolejnym rozdziale rozwiniemy temat nowych form przetwarzania mających na celu wspomaganie podejmowania decyzji.

Big Data ma zastosowanie wszędzie tam, gdzie dużej ilości cyfrowych danych towarzyszy potrzeba zdobywania nowych informacji lub wiedzy. Szczególne znaczenie odgrywa wzrost dostępności internetu oraz usług świadczonych drogą elektroniczną, które w naturalny sposób są przystosowane do wykorzystywania baz danych.

Z ostatnim kryterium „dużej zmienności" polskie instytucje finansowe stykają się jedynie marginalnie. Wyjątkiem jest warszawska Giełda Papierów Wartościowych, która od 15 kwietnia 2013 roku działa w oparciu o nowy system informatyczny.

Duża zmienność to przede wszystkim ogromna prędkość z jaką nowe dane powstają, a więc muszą też być zapisywane. Jest też ona wyzwaniem dla analityków, którzy muszą błyskawicznie przeliczać szybko narastające stosy nowych danych. Świetną ilustracją kryterium zmienności jest HFT – *High Frequency Trading* – prowadzony przykładowo na giełdach amerykańskich. Poszczególne rynki rozsyłają swoje zlecenia przez zbiorczy mechanizm CQS (*Consolidated Quote System*), który w teorii powinien zapewnić równy dostęp dla wszystkich zarejestrowanych graczy. System ten charakteryzuje się określoną przepustowością, która w chwili obecnej sięga ponad 580 tys. notowań na sekundę. Poprzez CQS rozprzestrzeniane jest ok. 95% notowań a wszyscy gracze, jak powiedziano, powinni mieć do niego równy dostęp. Jednakże firmy specjalizujące się w HFT znalazły sposób na CQS. Przede wszystkim korzystają z tzw. kolokacji w pobliżu NYSE. Polega ona na ustawianiu komputerów HFT grających na giełdzie jak najbliżej jej serwerów. Krótsze światłowody łączące giełdę z komputerami HFT dają tym drugim przewagę kilkuset milisekund nad resztą rynku. A to już wystarczy na wygenerowanie korzystnych zleceń.

Tak więc spośród trzech kryteriów V jedynie pierwsze, tj. duży wolumen danych, jest spełnione przez dzisiejsze systemy bankowe. Aby opanować Big Data banki muszą stworzyć kompetencje technologiczne odpowiadające nowej generacji narzędzi do tej pory nieużywanych przez informatyków.

Wybrane przykłady nowych narzędzi do przetwarzania Big Data

Kilkanaście lat temu duża zmienność danych stanowiła wyzwanie i jednocześnie okazję biznesową wykorzystaną najpierw przez firmy oferujące wyszukiwarki internetowe a wkrótce potem firmy tworzące media społecznościowe.

Dla tych pierwszych optymalizacji podlegała trafność wyszukiwania oraz czas odpowiedzi. Dla drugich do dziś dnia wyzwaniem jest wolumen nowych wpisów przekraczający 100 megabajtów na sekundę. Te nowe muszą być bowiem zapisane a w chwilę później dostępne dla milionów użytkowników.

Nic dziwnego, że firmy te musiały stworzyć nowe narzędzia , które pomogły im pokonać bariery technologiczne wynikające z dużej liczby danych w połączeniu z ich zmiennością. Dla firm rozwijających je ważniejsze od zachowania własności intelektualnej było szybkie pozyskanie jak największej liczby utalentowanych programistów. Dzięki temu wiele narzędzi było tworzone jako software ogólnodostępny. Są one również otwarte dzisiaj.

Dobrym przykładem jest MapReduce – platforma do przetwarzania równoległego bardzo dużych zbiorów danych w klastrach komputerów, stworzona przez firmę Google. Nazwa była zainspirowana funkcjami *map* i *reduce* z programowania funkcyjnego, a same operacje realizowane są podczas dwóch kroków.

W kroku *map* główny program (*master node*) pobiera dane z wejścia i dzieli je na mniejsze podproblemy, po czym przesyła je do robotników (*worker nodes*). Każdy z robotników może albo dokonać kolejnego podziału na podproblemy, albo przetworzyć problem i zwrócić odpowiedź do głównego programu.

W kroku *reduce* główny program bierze odpowiedzi na wszystkie podproblemy i łączy je w jeden wynik stanowiący odpowiedź na główny problem.

Główną zaletą MapReduce jest umożliwienie łatwego rozproszenia operacji. Zakładając, że każda z operacji *map* jest niezależna od pozostałych, może być ona realizowana na osobnym serwerze. Dzięki temu rozwiązaniu Google zdobył dominującą pozycję wśród wyszukiwarek! Część platformy została opatentowana w USA.[4]

Apache Hadoop[5] jest otwartą implementacją paradygmatu MapReduce Google. Umożliwia tworzenie działających w rozproszeniu aplikacji, które przeprowadzają obliczenia na dużych ilościach danych. Jest jednym z projektów rozwijanych przez fundację Apache. Jeszcze zanim osiągnął wydanie stabilne, był już wykorzystywany w poważnych zastosowaniach (Amazon, AOL, Facebook, Yahoo). Autorem projektu jest Doug Cutting.

Obok Hadoop fundacja Apache może być źródłem szeregu innych otwartych rozwiązań przydatnych w opanowaniu Big Data. Polecanym rozwiązaniem jest baza danych Cassandra pozwalająca błyskawicznie zapisywać

---

4 US Patent 7,650,331: *System and method for efficient large-scale data processing*.

5 http://hadoop.apache.org/#What+Is+Apache+Hadoop%3F

i poddawać analizie wielkie ilości danych. Aby uzyskać nieosiągalną do tej pory szybkość musiano zrezygnować z relacyjności, w tym z języka SQL, co jest pierwszą skuteczną na taką skalę próbą podważenia prawie absolutnego do tej pory paradygmatu.

R jak Ross i jak Robert

Analitycy ilościowi lubią Nową Zelandię nie tylko za witaminy dostarczane w owocach kiwi.

Drugim ważnym powodem sympatii jest otwarta biblioteka R[6] zawierająca ogromne bogactwo gotowych funkcji stosowanych w analizie danych.

R została stworzona w 1993 roku przez Rossa Ihaka i Roberta Gentlemana z Uniwersytetu Auckland. Nazwa odpowiada imionom twórców. Panowie R wymyślili nowy język, który miał ułatwić ich studentom naukę analizy danych. Język rozprzestrzenił się bardzo szybko w innych ośrodkach akademickich i już w 1995 roku twórcy podjęli decyzję o powszechnym udostępnieniu go na zasadach Fundacji Wolnego Oprogramowania: GNU *General Public Licence*.

Wokół R szybko powstało grono entuzjastów statystyków i programistów, którzy pochodzili z różnych ośrodków na świecie. Obecnie stanowią oni zespół nadzorujący dalszy rozwój biblioteki programów służących najróżniejszym zastosowaniom statystyki. Warto podkreślić, że niezależny pomiar popularności pokazał, iż R jest dwukrotnie częściej cytowana i używana niż jakakolwiek inna biblioteka lub pakiet komercyjny. Dzięki koncepcji otwartego software'u R rozprzestrzenia się jak „wirus". Dzisiaj ta wspólnota składa się z wielu tysięcy autorów oraz milionów użytkowników na całym świecie.

Wspólnota statystyków zgrupowanych wokół R stanowi dzisiaj rodzaj ogromnej fabryki software'u. Codziennie powstają nowe pakiety, które natychmiast mogą być ściągnięte i użyte przez analityków na całym świecie. Istniejące funkcje są poprawiane i rozszerzane, a w chwilę potem mogą już być użyte przez szerokie grono użytkowników.

Wspólnota R jest źródłem niebywałego sukcesu w zastosowaniu metod analizy statystycznej do problemów biznesowych takich jak: bezpośredni marketing, badanie nastrojów klientów i konsumentów, a także w makroekonomii.

---

6 http://www.r-project.org/

R zawiera również bardzo potężny pakiet funkcji wizualizacyjnych, dzięki którym analitycy przedstawiają uzyskane wyniki w ciekawy i przekonywujący sposób.

Zastosowania R w ubezpieczeniach sięgają końca lat 90., kiedy to dzięki statystyce znacznie ulepszono proces akceptacji umów pokrywających określone ryzyka.

Jak rozpocząć pracę z Big Data?

W oparciu o przykłady nowych narzędzi informatycznych możemy sformułować dwie tezy ważne dla instytucji chcących wykorzystać zjawisko Big Data w biznesie.

Po pierwsze, wykorzystanie Big Data to nie jest typowe i znane informatykom wyzwanie technologiczne. Na szczęście dostępne są już liczne narzędzia ułatwiające pracę w tym zakresie. Istnieje cały szereg narzędzi oferowanych przez firmy technologiczne na zasadach komercyjnych, ale największą popularność zyskały zbiory narzędzi dostępnych poprzez otwarte platformy, takie jak Apache Foundation. Oznacza to, że na początek, a w wielu przypadkach nawet w ogóle nie trzeba inwestować poważnych środków w licencje.

Po drugie, bez inwestycji jednak się nie obejdzie. Najtrudniej jest zdobyć wiedzę i kwalifikacje związane z tym nowym zjawiskiem. Na dodatek konieczne jest niestandardowe podejście do tematu. W tradycyjnym podejściu informatycy kupowali narzędzia i szkolenia pozwalające zdobyć kwalifikacje do ich obsługi. Dzięki temu np. narzędzia klasy Business Intelligence pozwoliły częściowo zautomatyzować raportowanie dotyczące przeszłości: zestawienia, wyniki w różnych przekrojach, raporty obowiązkowe i zarządcze. Dzięki zjawisku Big Data pojawiła się nowa, dotąd praktycznie nieosiągalna możliwość, jaką jest optymalizacja przyszłości. Tym razem to nie zakup narzędzi i szkoleń umożliwi nam rozpoczęcie prac. Potrzebni są ludzie z wyobraźnią i odwagą naukowca stawiającego pytania dotyczące zachowania się biznesu w przyszłości. I szukający odpowiedzi na te pytania w języku rachunku prawdopodobieństwa. Ten nowy gatunek ludzi wspierających decyzje dotyczące przyszłości nosi nazwę naukowcy danych (*data scientists*).[7]

Potrzebni też będą decydenci, którzy w oparciu o zaprezentowane wyniki analizy ilościowej podejmą strategiczne decyzje biznesowe.

---

7 Thomas Davenport and D.J.Patil: *Data Scientist: the Sexiest Job of the 21st Century*, Harvard Business Review, October 2012

Ażeby dobrać się do wiedzy o przyszłości tkwiącej w danych niezbędne jest konsekwentne stosowanie kilku prostych mechanizmów analizy predykcyjnej, o czym mowa będzie w następnym rozdziale.[8]

Klucz do przyszłości – analiza predykcyjna

Wszystkie zastosowania analizy predykcyjnej zaczynają się od sformułowania pytania, na które aplikacja ma udzielić odpowiedzi, np. co skłania kredytobiorcę kredytu hipotecznego do przedterminowej spłaty całości (re-finansowania)? Właściwa odpowiedź ma dla kredytującego banku dużą wartość równą wielkości utraconych przyszłych odsetek.

Jeżeli znajdziemy właściwą odpowiedź to dla uniknięcia negatywnych skutków niezbędne będzie konkretne działanie.

Tak więc predykcję można sprowadzić do dwóch elementów zrozumiałych dla każdego menedżera: co chcemy przewidzieć i jakie działanie wykonamy zdobywszy tę wiedzę.

Aby wykonać analizę naukowiec danych musi zbudować model predykcyjny, który przetwarzając dostępne dane dokona oceny (skoringu) poszczególnych opcji. Model ten stara się odwzorować zachowanie pojedynczej osoby, np. kupno towaru, kliknięcie myszą, uchylenie się od spłaty. Model pobiera wartości zmiennych opisujących osobę i na tej podstawie wylicza prawdopodobieństwo (*skore*) określonego zachowania. W naszym przykładzie model predykcyjny wykazał, że najistotniejszym zagrożeniem zachowania przedterminowej spłaty jest wysokość oprocentowania. Jeżeli jest ona niższa niż 7,94% (wartość przykładowa) to ryzyko jest równe 3,8%, w przeciwnym przypadku wzrasta do 19,2%. Jak widać, tylko to jedno kryterium pozwala pięciokrotnie (!) zmniejszyć prawdopodobieństwo wystąpienia ryzyka.

Dobry model predykcyjny ma również zdolność do uczenia się. Kolejne rekordy danych przetwarzane przez model prowadzą do jego doskonalenia się zarówno, jeżeli chodzi o głębię analizy, jak i wartości progowe dotyczące poszczególnych kryteriów. W naszym przykładzie okazuje się, że przy oprocentowaniu poniżej progu 7,94% drugim z kolei czynnikiem jest wysokość zarobków kredytobiorcy. Natomiast powyżej progu 7,94% decyduje nie przychód kredytobiorcy, lecz całkowita wartość kredytu. Kredyty o dużej wartości i dużym oprocentowaniu obarczone są nawet 36-proc. prawdopodobieństwem przedterminowej spłaty. To jest co trzeci kredyt!

8 Eric Siegel: *Predictive Analytics*, John Wiley & Sons, 2013.

Dzięki wbudowanej funkcji uczenia się nasz model może się dalej rozwijać (uczyć) przyjmując kształt potężnie rozbudowanego drzewa binarnego. Dane spoza bankowych systemów transakcyjnych mogą znacznie rozszerzyć zakres modelu i jego moc przewidywania.

Ważną cechą modeli analizy predykcyjnej jest ich addytywność. Pracę nad nimi można podzielić między zespoły. Model końcowy będący sumą modeli opracowanych przez poszczególne zespoły odznacza się zawsze wyższą jakością i trafnością skoringu, aniżeli modele składowe. W tym przypadku tłum jest zawsze mądrzejszy od najmądrzejszej jednostki.

Teraz menedżerowie muszą podjąć działanie w oparciu o pozyskaną wiedzę. Czy są gotowi obniżyć oprocentowanie poniżej 7,94% mając na uwadze możliwość całkowitej utraty przyszłych odsetek? Gdzie leży ich próg ryzyka? Odpowiedź na te pytania wciąż jeszcze należy do ludzi.[9]

Analiza predykcyjna nie jest sztuką dla sztuki. Jej wykorzystanie w biznesie jest bardzo opłacalne, gdyż znakomicie uzupełnia doświadczenie i naturalne odruchy w sytuacjach, w których doświadczenie nie jest dobrym doradcą. Poniżej przytaczam kilka wybranych przypadków zastosowania z dziedziny bankowości.

Analiza predykcyjna zarabia na siebie

Pierwszy przykład dotyczy zachowania klientów indywidualnych korzystających z wielu produktów jednego z banków. Okazuje się, że kierowanie do takich klientów kolejnych ofert zmniejsza szansę sprzedania tych produktów. Każda nowa oferta działa destrukcyjnie i to w dwojakim sensie. Koszt oferty jest wydatkiem, który z wysokim prawdopodobieństwem się nie zwróci. Ponadto ci klienci, którzy otrzymują ofertę z dużym prawdopodobieństwem skorzystają z porównywarki internetowej i być może znajdą korzystniejszą ofertę u konkurencji.

Wniosek i działanie wynikające z analizy to zaprzestanie marketingu bezpośredniego do tej kategorii klientów.

Przewidywanie zachowania jest szczególnie trudne z uwagi na zasadniczą cechę ludzi jaką jest wolna wola. Modelowanie odpowiedzi konsumentów na określone impulsy i zachęty wymaga wielkiej dyscypliny w wyciąganiu wniosków dotyczących konkretnych działań. W powyższym przykładzie większość

9 Andrew McAfee and Erik Brynjolfsson: *Big Data: The Management Revolution*, Harvard Business Review, October 2012.

osób odpowiedzialnych za sprzedaż produktów bankowych zaryzykowałaby wysłanie oferty lub rozmowę telefoniczną kierując się instynktem i usprawiedliwieniem „a co to szkodzi".

Drugi przykład dotyczy analizy ryzyka kredytowego małych i średnich firm będących własnością jednej lub kilku osób fizycznych. Okazuje się, że analiza zachowania właściciela jako konsumenta jest znacząco ważniejsza od analizy sytuacji biznesowej jego firmy. Z jednej strony, małe firmy z reguły nie prowadzą nadmiernie dokładnej ewidencji księgowej, co powoduje, że możliwość analizy sytuacji biznesowej jest ograniczona. Z drugiej strony, można założyć, że firma zachowa się w stosunku do banku dokładnie tak jak jej właściciel.

Wniosek i rekomendowane działania to wyjątkowo atrakcyjna oferta banku na prowadzenie zarówno rachunku firmy, jak i rachunków właściciela jako osoby fizycznej. Daje to możliwość uzyskania z pierwszej ręki danych na temat zachowania właściciela jako konsumenta.

Trzeci przykład dotyczy korelacji określonych miejsc płatności kartą kredytową z wiarygodnością kredytobiorcy. Okazuje się, że płatności kartą u dentysty oznaczają niższe ryzyko niespłacenia kredytu. Natomiast częste opłaty kartą za wyroby alkoholowe korelują z podwyższonym ryzykiem. Lista miejsc płatności, które warto uwzględnić w analizie ryzyka jest bardzo długa.

Wniosek i działanie to rozszerzenie aplikacji skoringu kredytowego o analizę miejsc płatności kartą kredytową.

Egzotyczny przykład dotyczy niespłacania mikropożyczek o wartości 25 USD udzielanych projektodawcom w krajach rozwijających się przez serwis www.kiva.org. KIVA jest przykładem zbiorowego finansowania za pośrednictwem platformy, która łączy indywidualnych pożyczkodawców z pożyczkobiorcami. Analiza tekstu aplikacji pożyczkowej pozwala określić dwukrotnie podwyższony poziom ryzyka, jeżeli w aplikacji brak jest słów kluczowych takich jak *szkoła, maszyna* lub *urządzenie*.

Rekomendowane działanie to unikanie finansowania projektów, których opisy zostały nisko ocenione.

Kolejny przykład dotyczy wpływu nastrojów społecznych na notowania giełdowe.[10] Początkowa analiza ponad 600 tys. blogów, w których autorzy opisywali swoje nastroje pozwoliła na stworzenie modelu predykcyjnego zbiorowego niepokoju, który wyliczał zmienną nazwaną indeksem niepokoju.

10 Eric Gilbert and Karrie Karahalios: *Widespread Worry and the Stock Market*, *Assiociation of the Advancement of Artificial Intelligence*, 12.03.2010

Codzienne zasilanie modelu wpisami z blogosfery pozwoliło na przedstawienie rozwoju tego indeksu w czasie. Okazało się, że istnieje związek indeksu niepokoju z zachowaniem amerykańskiego indeksu giełdowego Standard & Poor's 500 (S&P 500). Zmiany indeksu niepokoju wyprzedzają o dwa dni zmiany indeksu S&P 500. Tak więc wzrost niepokoju poprzedza spadek indeksu giełdowego a spadek niepokoju wyprzedza o dwa dni wzrost indeksu.

Co do rekomendowanego działania należy w tym przypadku zachować ostrożność. Powyższy przykład nie jest instrukcją funkcjonowania automatu do robienia pieniędzy na giełdzie. Spadek niepokoju niekoniecznie musi być podstawą do niekontrolowanych zleceń kupna w oczekiwaniu na automatyczny wzrost indeksu giełdowego. Na indeks ten mogą mieć znacznie bardziej decydujący wpływ inne czynniki oprócz nastrojów społecznych.

Innowacyjność zaprezentowanego podejścia polega na powiązaniu wiedzy zdobytej z analizy amerykańskiej blogosfery z ważnym wskaźnikiem gospodarczym, jakim jest indeks giełdowy. Jest to też pierwszy naukowy dowód na to, że nastroje społeczne mają jednoznaczny wpływ na gospodarkę. Ten wpływ może być zgodny z naszą intuicją, ale dopiero analiza ilościowa stanowi niepodważalny dowód.

Ostatni przykład dotyczy bezpieczeństwa placówek bankowych. Okazuje się, że bandyci chętnie uderzają w tej samej okolicy. Analiza geograficznego rozkładu napadów na placówki prowadzona z użyciem technik Big Data pokazuje jednoznacznie, że udany (z punktu widzenia przestępcy) napad na jedną placówkę znacznie zwiększa prawdopodobieństwo powtórzenia napadu na inną placówkę w tej samej okolicy.

Wniosek jest oczywisty i dotyczy wzmożenia ochrony placówek sąsiadujących z miejscem popełnienia udanego napadu.

Powyższe przykłady można uzupełnić długą listą zastosowań analizy predykcyjnej w ubezpieczeniach majątkowych, zdrowotnych i życiowych oraz w zastosowaniu do zarządzania aktywami. Ważne, by zawsze trzymać się zasady, iż analiza dotyczy zagadnień ważnych dla biznesu, dzięki czemu jej koszty będą wielokrotnie spłacone dzięki podjętym w oparciu o nią działaniom.

Wnioski dla banków

W odróżnieniu od Nowej Umowy Kapitałowej za Big Data nie stoi wymóg Komisji Nadzoru Finansowego. Jest to czysta decyzja biznesowa.

Bankowe działy informatyki z pewnością mają szereg pilniejszych potrzeb, takich jak rozwój płatności mobilnych, całościowe zarządzanie relacjami z klientami CRM czy liczne rekomendacje wspomnianego już regulatora. Informatycy podchodzą do Big Data z rezerwą, gdyż plany działów rozwoju aplikacji są wypełnione po brzegi a w dodatku biznes nie domaga się rozwiązań Big Data. Jest to typowa martwa pętla innowacji.

Jedyna szansa wyjścia z niej to zainteresowanie tematyką Big Data menedżerów marketingu, sprzedaży, ryzyka a nawet HR. Jeżeli znajdą się interesujące pytania, to znajdą się sposoby i środki na poprowadzenie innowacyjnych inicjatyw i projektów. Jak już wspomniałem wcześniej, banki posiadają znaczne zasoby danych na temat klientów i transakcji. Dane te z pewnością mogą być wykorzystane do analizy predykcyjnej, która da odpowiedź na interesujące biznes pytania.

Historia dowodzi, że z innowacją nie warto czekać. Banki, które na serio podeszły do wymagań Nowej Umowy Kapitałowej były dobrze przygotowane na kryzys finansowy roku 2008. Były też wielkie banki, takie jak Lehman Brother's, które zignorowały wymagania kapitałowe. Dzisiaj należą one do historii.

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 roku, odpowiedzialny za realizację strategii wielokanałowej obsługi oraz rozwój bankowości elektronicznej i mobilnej Pekao24/PekaoFirma24 dla klientów indywidualnych oraz małych i średnich przedsiębiorstw. Członek Rady Nadzorczej Contact Center – Centrum Bankowości Bezpośredniej Sp. z o.o.

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

Bartosz Zborowski

Dyrektor Biura Projektów Strategicznych w Pionie Bankowości Detalicznej Banku Pekao S.A. Absolwent Akademii Ekonomicznej w Krakowie na kierunku finanse i bankowość oraz studiów podyplomowych „Zarządzanie Projektami Internetowymi" w Szkole Przedsiębiorczości i Zarządzania AE w Krakowie.

Przez 14 lat kariery zawodowej uczestniczył w licznych projektach z obszaru bankowości detalicznej i działalności brokerskiej. Na obecnym stanowisku od 2007 roku, zaangażowany m.in w połączenie Banków BPH i Pekao S.A., organizację aktywności Banku na EURO2012, wdrożenie operacyjnego CRM i innowacyjnego systemu płatności mobilnych PeoPay.

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

Bankowość mobilna i płatności mobilne

Jeszcze dziesięć lat temu rozważając kierunki, w których rozwinie się korzystanie z telefonów komórkowych trudno byłoby przewidzieć, że urządzenia te będą w stanie rzeczywiście oferować tak szerokie możliwości jak komputery osobiste. To, co wówczas wydawało się mało prawdopodobne, stało się faktem w stosunkowo krótkim czasie. Wraz z prezentacją pierwszego iPhone'a przez firmę Apple w 2007 roku zmianie uległ globalny wizerunek telefonu. Urządzenie postrzegane do tej pory jako narzędzie służące jedynie do prowadzenia rozmów i wysyłania wiadomości tekstowych zostało wzbogacone o szerokie możliwości multimedialne i, przede wszystkim, wygodny dostęp do internetu. Telefon stał się smartfonem.

Na rozwój smartfonów złożyło się równolegle kilka czynników: postęp technologiczny pozwalający oferować klientom coraz to szybsze, bardziej ergonomiczne, wyposażone w technologię dotykową urządzenia, upowszechnianie się szybkiego dostępu do internetu mobilnego, a także konkurencja pomiędzy dostawcami, powodująca obniżanie cen nowych technologii oraz samych smartfonów. W ciągu kilku lat historii smartfona zapomnieliśmy już o osobnych budzikach, papierowych mapach, odtwarzaczach CD, dyktafonach, aparatach cyfrowych i zapewne kilku innych rzeczach, które pochłonęło to małe, ale jakże wygodne urządzenie, które nosimy zawsze ze sobą.

Rozwój technologii mobilnych najlepiej obrazują statystyki dotyczące tego typu urządzeń. Podczas gdy w 2008 roku sprzedano na świecie 139,3 mln smartfonów[1], to w 2011 roku było to już 472 mln urządzeń i stanowiły one 31%

1 http://www.gartner.com/newsroom/id/910112

wszystkich sprzedanych telefonów, które trafiły na rynek[2], a w 2013 roku – ponad miliard, co stanowiło 55,1% udziału w sprzedaży telefonów.[3]

W Polsce w 2008 roku smartfony stanowiły zaledwie 3% rynku telefonów, podczas gdy w 2011 roku – 27,1%.[4] W styczniu 2014 roku smartfony zdobyły 44% rynku, a szacuje się, że do 2015 roku osiągną 60%.[5]

Mobilność w finansach – bankowość mobilna

Wraz z upowszechnieniem się technologii mobilnych również banki dostrzegły możliwość wprowadzania do swojej oferty nowych rozwiązań. Zaproponowały klientom łatwiejszy dostęp do usług bankowych przez urządzenia mobilne i od tego czasu rozwiązania te są określane jako bankowość mobilna.

Czym jest bankowość mobilna? Mimo niedługiej historii, doczekała się ona wielu definicji. Wspólnym mianownikiem tej formy bankowości jest umożliwienie klientowi dostępu do rachunków i wykonywania transakcji bezpośrednio z urządzenia mobilnego. Do niedawna w skład bankowości mobilnej zaliczane były usługi SMS oraz WAP, jak również serwisy telefoniczne (np. automatyczna obsługa klienta IVR). Obecnie przez bankowość mobilną, nazywaną po angielsku *mobile banking* lub *m-banking*, rozumie się zestaw narzędzi, które za pomocą telefonu lub innego urządzenia mobilnego z dostępem do internetu (np. tabletu) umożliwiają korzystanie z usług bankowych poprzez dedykowaną aplikację mobilną lub mobilny serwis www.

Technologie mobilne w bankowości są wykorzystywane przez banki od ponad dekady. Początkowo przybierały formę kontaktów telefonicznych z bankowym call center (IVR) oraz operacji bankowych realizowanych poprzez SMS. Dopiero szersza dostępność mobilnego internetu spowodowała, że banki zaczęły wprowadzać do swoich ofert bankowość mobilną w formie lekkich stron internetowych i aplikacji mobilnych. Początkowo banki inwestowały w tworzenie stron internetowych dostępnych przy pomocy protokołu WAP. W Polsce pierwsze tego typu rozwiązania pojawiły się w latach 2000–2002 i umożliwiały sprawdzanie salda, historii operacji czy zlecenie zdefiniowanych przelewów.

---

2 http://www.gartner.com/newsroom/id/1924314

3 http://www.telix.pl/artykul/idc-ponad-miliard-smartfonow-sprzedanych-w-2013-roku-3,59229.html

4 Natalia Hatalska, Penetracja smartfonów w Polsce – dane za 2011, http://hatalska.com/2012/02/13/penetracja-smartfonow-w-polsce-dane-za-2011/

5 Monika Mikowska, Raport Marketing mobilny w Polsce 2013/2014, mobee dick, s. 38

Kolejnym krokiem były tzw. *serwisy light*, które są zredukowaną do podstawowych funkcjonalności bankowością internetową. Wprowadzenie *serwisów light* spowodowało wycofanie się przez banki z usług WAP.

Wraz z upowszechnieniem smartfonów i tabletów banki stopniowo wprowadzają rozwiązania oparte o aplikacje mobilne, które cieszą się coraz większą popularnością. Obecnie większość z nich zarówno w Polsce, jak i na świecie decyduje się na udostępnianie bankowości mobilnej właśnie w postaci dedykowanych aplikacji mobilnych. Aplikacje wykorzystują nowoczesne funkcje dostępne w urządzeniach mobilnych (np. GPS, kamerę czy czujniki położenia), aby zaoferować klientom unikalne możliwości podczas korzystania z usług bankowych. Przykładem takich zastosowań jest możliwość geolokalizacji bankomatów lub placówek bankowych wraz ze wskazaniem ich położenia bezpośrednio na obrazie z kamery czy skanowania kodów QR do wykonywania płatności[6]. Dziś aplikacje mobilne zapewniają użytkownikom praktycznie taki sam zakres operacji jak tradycyjna bankowość internetowa.

Mobilna bankowość przeżywa obecnie okres intensywnego rozwoju, głównie w formie aplikacji mobilnych. Nowoczesne „bankowanie" nie oznacza już tylko korzystania z bankowości internetowej, gdyż dostęp do niej stał się standardem rynkowym. Bankowość mobilna stanowi rozwinięcie aktualnej oferty bankowości elektronicznej i w perspektywie najbliższych lat ma szansę stać się podstawowym kanałem dostępu do usług bankowych.

Kolejny krok – płatności mobilne

Płatności mobilne są naturalną konsekwencją i rozwinięciem bankowości mobilnej, opartym na założeniu, że również płacenie telefonem ma duży potencjał rozwoju. Obserwowana różnorodność wdrożonych dotychczas i testowanych na świecie sposobów dokonywania płatności mobilnych pokazuje, że wciąż brak jest konsensusu co do jednego rozwiązania, które znajdzie akceptację użytkowników.

Kolorytu tej sytuacji dodaje także fakt, że do walki o płatności mobilne przystąpiły nie tylko banki i organizacje kartowe, ale także podmioty dotychczas nie kojarzone z płatnościami: operatorzy telekomunikacyjni, dostawcy usług internetowych czy duże sieci detaliczne. Dzięki ich zaangażowaniu powstało

6 Kod QR (Quick Response) – dwuwymiarowy kod kreskowy w formie białych i czarnych kwadratów, który może być nośnikiem informacji, np. w płatnościach mobilnych czy marketingu.

wiele systemów oraz aplikacji pozwalających płacić, zbierać punkty, przekazywać pieniądze pomiędzy użytkownikami telefonów czy też akceptować płatności mobilne przy użyciu smartfona, stron internetowych czy terminali w sklepach.

Rodzaj technologii wykorzystanych w systemach płatności wynika m.in. ze stopnia „mobilnego" rozwoju poszczególnych regionów świata, dostępnej infrastruktury, a także ze stopnia dostępności usług bankowych. W Azji, Stanach Zjednoczonych czy Europie dominują technologie zbliżeniowe NFC (*Near Field Communication* – łączność bliskiego zasięgu) i kody QR. Na uwagę zasługują projekty wdrożeń takich firm jak: NTT DoCoMo w Japonii, PayBox w Austrii czy Starbucks w Stanach Zjednoczonych.

Z kolei w niektórych krajach afrykańskich płatności mobilne rozwinęły się w oparciu o specjalną aplikację połączoną z rachunkiem na karcie SIM dostarczaną przez operatora, umożliwiającą przesyłanie pieniędzy czy opłacanie rachunków poprzez tzw. „bezpieczne SMS-y". Ta forma rozliczeń (na przykładzie M-PESA w Kenii) stała się bardzo popularna ze względu na słabo rozwiniętą infrastrukturę bankową, a stosunkowo dużą liczbę telefonów komórkowych wśród społeczeństwa. Na przykład kenijski operator telefonii komórkowej Safaricom ma19 mln użytkowników w swoim kraju.[7] Dla porównania z rachunków bankowych korzystało w 2013 roku 5,4 mln Kenijczyków, a z płatności mobilnych 11,5 mln.[8]

Na osobną uwagę zasługuje istotne zaangażowanie w projekty płatności mobilnych największych organizacji kartowych. Wdrażają one własne rozwiązania oparte na kartach płatniczych: V.me oraz MasterPass. Współpracują również z firmami technologicznymi, operatorami i bankami przy budowie dedykowanych rozwiązań. Przykłady współpracy z VISA to wdrożenie zbliżeniowych płatności mobilnych w Hiszpanii wspólnie z bankiem La Caixa oraz operatorami Vodafone, Orange i Telefonica, we Francji usługi Orange Cash, projektu z bankiem Garanti w Turcji oraz operatorem komórkowym Turkcell.[9] Natomiast w marcu 2014 roku MasterCard i węgierski OTP Bank ogłosiły wprowadzenie OTPay – pierwszego w Europie elektronicznego portfela korzystającego z rozwiązania MasterPass.

---

7 Rzeczpospolita, http://www.ekonomia.rp.pl/artykul/1009338.html

8 FinAccess, National Survey 2013, *Profiling developments in financial access and usage in Kenya*, October 2013, s. 18.

9 VISA Polska, *Płatności mobilne Visa w Europie nabierają rozmachu*, http://prnews.pl/wiadomosci/platnosci-mobilne-visa-w-europie-nabieraja-rozmachu-6548665.html

Wykorzystanie kart zbliżeniowych i standardu NFC w płatnościach mobilnych może rozwinąć się dzięki wdrożeniu technologii polegającej na zabezpieczeniu płatności NFC w chmurze za pomocą HCE (*Host Card Emulation*), co otwiera nowe możliwości dla wszystkich uczestników zaangażowanych w płatności mobilne na świecie i pozwala na rezygnację z uciążliwej technologii opartej na rozwiązaniu SIM-centric[10].

Rozwój płatności mobilnych w Polsce

Początkiem płatności mobilnych w Polsce była firma mPay, która zaczęła oferować płatności mobilne w 2007 roku głównie w oparciu o technologię USSD i IVR oraz portmonetkę elektroniczną we współpracy z operatorem telefonii komórkowej sieci Plus. Zbliżone usługi udostępniła także firma SkyCash w oparciu o rozwiązanie aplikacyjne. Dzięki tym rozwiązaniom Polacy mogą opłacać parking, kupić bilet komunikacji miejskiej, doładować telefon na kartę lub wypłacić pieniądze z bankomatu.

Duże znaczenie dla rozwoju płatności mobilnych w Polsce miała „zbliżeniowa rewolucja". W 2007 roku Polska, jako pierwszy kraj w Europie Centralnej, udostępniła karty płatnicze w technologii zbliżeniowej. Mimo, że początkowo zarówno banki, jak i klienci podchodzili do płatności zbliżeniowych z dużą rezerwą, dzięki licznym kampaniom edukacyjnym zarówno ze strony systemów płatniczych jak i banków – wydawców kart – płatności zbliżeniowe upowszechniły się na szeroką skalę. Masowe wdrożenia płatności zbliżeniowych miały miejsce w latach 2010–2011. Z jednej strony rosła liczba zbliżeniowych instrumentów płatniczych w portfelach klientów, a z drugiej zwiększała się liczba urządzeń akceptujących te płatności. Na przestrzeni lat Polska stała się liderem płatności zbliżeniowych w Europie, o czym świadczą statystyki. Na koniec III kwartału 2013 r. w obiegu znajdowało się ok. 19,8 mln kart z funkcją zbliżeniową, co stanowi 56,7% wszystkich kart płatniczych.[11]

Rosnąca dostępność miejsc akceptujących płatności zbliżeniowe w połączeniu z pojawieniem się na rynku telefonów wyposażonych w technologię zbliżeniową NFC sprawiła, że pod koniec 2012 roku na rynku pojawiły się usługi Cash Orange oraz MyWallet T-Mobile. W tych rozwiązaniach, klient

---

10 SIM-centric – rozwiązanie płatności mobilnych wykorzystujące element bezpieczny wbudowany w kartę SIM wydawaną przez operatora

11 Dane NBP, Informacja o kartach płatniczych III kwartał 2013 r., s. 11, http://www.nbp.pl/home.aspx?f=/systemplatniczy/karty/informacje_kwartalne.html

posiadający odpowiedni model telefonu obsługujący standard NFC oraz specjalną kartę SIM z zapisanymi danymi karty płatniczej może dokonywać płatności zbliżeniowych w terminalach POS. Mimo że płacenie zbliżeniowe jest już standardem w polskich płatnościach kartowych, powyższe rozwiązania nie osiągnęły dużej popularności przede wszystkim ze względu na wciąż ograniczoną liczbę smartfonów wyposażonych w moduł NFC, ograniczenie dostępności tylko do wybranego operatora i skomplikowaną procedurę uaktywniania usługi, wynikającą z konieczności synchronizacji działań po stronie banku i operatora.

Systemy płatnicze oprócz współpracy z bankami i telekomami rozwijają swoje własne rozwiązania. VISA promuje portfel elektroniczny V.me, w którego rozwój zaangażowanych jest kilka banków członkowskich. MasterCard przyczynił się natomiast do rozpowszechnienia usługi MasterCard Mobile, która jest obecna w czterech bankach w Polsce, a firmami współpracującymi są takie podmioty jak mPay, SkyCash czy uPaid.

Znaczącym wydarzeniem 2013 roku na rynku płatności mobilnych w Polsce było niewątpliwie ogłoszenie startu czysto bankowych rozwiązań: IKO (PKO Bank Polski) i PeoPay (Bank Pekao S.A.).

Klienci korzystający z PeoPay czy IKO podłączają swoje aplikacje bezpośrednio do rachunku bankowego, ale mają też możliwość zdalnego utworzenia rachunku prepaid. Po zakończeniu rejestracji uzyskują możliwość płacenia w sklepach wyposażonych w terminal kartowy oraz w internecie, a także przekazywania pieniędzy pomiędzy użytkownikami używając jedynie numeru telefonu odbiorcy czy też wypłacania pieniędzy z bankomatów bez konieczności posiadania karty.

Dodatkowo w przypadku PeoPay płatność możliwa jest nie tylko za pomocą 6-cyfrowego kodu tymczasowego (używanego jako metoda autoryzacji w IKO), ale też poprzez skanowanie kodu QR wyświetlanego na terminalu kartowym, na stronie internetowej lub też bezpośrednio na smartfonie przedsiębiorcy wyposażonym w dedykowaną do akceptacji płatności mobilnych aplikację PeoPay mPOS.

Warto wspomnieć o możliwości zapłacenia bezpośrednio w komórce przy nabyciu aplikacji w Google Play czy App Store za pomocą wcześniej zdefiniowanej karty płatniczej czy dołączeniu płatności do faktury operatora (Google Play, operator Play). Inną propozycję przygotowała i ogłosiła na koniec 2013 roku firma PayU w postaci usługi PayU Express umożliwiającej płatność

z wykorzystaniem rachunku bankowego bez logowania się do bankowości internetowej.

Wszystkie powyższe rozwiązania charakteryzują się brakiem powszechności, która wynika z ograniczonej liczby punktów akceptujących tego typu płatności w porównaniu do kart płatniczych. Musi upłynąć trochę czasu zanim wyklarują się standardy, które będą zarówno wygodne w użyciu dla klientów i sklepów, jak i szeroko akceptowane i to nie tylko tam, gdzie już teraz można płacić kartami płatniczymi.

Trendy i przyszłość

Trudno jest jednoznacznie rozstrzygać, jakie zmiany czekają nas w najbliższych latach w świecie technologii mobilnych. Mamy bowiem do czynienia z wieloma rozwiązaniami, zarówno w zakresie samego korzystania z urządzenia (różne sposoby nawigacji – dotyk, fizyczne klawiatury), jak i ich oprogramowania. Podczas gdy na tradycyjnych komputerach dominuje system operacyjny Windows, to w przypadku urządzeń mobilnych o prymat walczy co najmniej kilku dużych graczy jak Android, iOS czy Windows Phone.

Obecnie rozwijanych jest wiele różnych technologii, takich jak: rozszerzona rzeczywistość (AR) czy *wearable devices* (np. inteligentne zegarki typu *smartwatch*, Google Glass), które mogą ukształtować rynek mobilny w najbliższych latach. Znaczącą nowością są usługi opierające się na sterowaniu głosem – Siri firmy Apple, Google Now firmy Google czy Cortana firmy Microsoft, które mają szanse upowszechnić się jako sposób obsługi urządzeń mobilnych. Niedawno do nowinek technologicznych dołączyło także HCE.

Ze względu na fakt, że trendy i rozwiązania stosowane na rynku mobilnym są bardzo dynamiczne problemem jest także jednoznaczne wskazanie kierunków rozwoju bankowości mobilnej. W ostatnim czasie obserwujemy wzrost zainteresowania głównie w zakresie:

- wykorzystania kamery urządzenia do rozszerzonej rzeczywistości i szybkiej lokalizacji, np. punktu rabatowego czy skanowania kodów QR z faktury do przeniesienia danych płatności do formularza przelewu w bankowości mobilnej,
- sterowania głosowego, czyli wykorzystania mechanizmów rozpoznawania mowy do obsługi bankowości mobilnej, co może być interesujące szczególnie dla kierowców,

- dedykowanych aplikacji dla tabletów – w odróżnieniu od aplikacji dostępnych na smartfony tablety pozwalają na wykorzystanie większej powierzchni ekranu i zaprezentowanie informacji w bardziej atrakcyjnej i czytelnej formie, a oprócz tego oferują użytkownikowi możliwość korzystania z internetu w sposób daleko bardziej wygodny zarówno od komputerów, jak i smartfonów, dzięki czemu klienci coraz częściej zaczynają używać ich jako podstawowych urządzeń nie tylko do bieżącej obsługi, ale także do zarządzania swoimi finansami.

Interesujące wyzwania dla bankowości mobilnej niosą wspomniane już *wearable devices* czyli technologie wykorzystujące okulary Google Glass czy inteligentne zegarki typu *smartwatch*. Wybrane banki już zaczynają przygotowywać rozwiązania dedykowane dla tych urządzeń, np. hiszpański Banco Sabadell, który testuje bankowość dla okularów Google czy nowozelandzki Bank Westpac, który pracuje nad rozwiązaniem dla inteligentnych zegarków.

To co jest pewne to fakt, że instytucje finansowe, a w szczególności banki muszą stale monitorować rynek i przewidywać trendy rozwoju technologii mobilnych.

Podsumowanie

Bankowość mobilna i płatności mobilne na stałe wpisały się w krajobraz usług bankowych i coraz częściej stanowią podstawę strategii rozwoju instytucji finansowych. Wraz z rosnącą popularnością smartfonów i tabletów banki bardzo szybko dostrzegły konieczność zbudowania wygodnych dla klienta rozwiązań opartych na technologiach mobilnych. Bankowość mobilna, jeszcze do niedawna postrzegana jedynie jako ciekawostka, zaczyna stanowić podstawowy element oferty banków. Wśród klientów instytucji finansowych rośnie też świadomość możliwości, jakie oferuje ten rodzaj bankowości. Dla klientów, którzy oczekują nowoczesności i preferują kontakt poprzez nowe technologie o wyborze oferty konkretnego banku decyduje posiadanie przez niego wygodnej i funkcjonalnej bankowości mobilnej.

Naturalnym krokiem rozwoju w obszarze usług finansowych opartych o technologie mobilne stają się płatności mobilne. Na świecie prognozuje się wysoką dynamikę wzrostu *m-payments*, dzięki czemu w rozwój płatności mobilnych zaangażowały się firmy nie mające do tej pory żadnego związku z rynkiem płatności. Obecnie zarówno w Polsce, jak i na świecie rozwijanych jest wiele inicjatyw w tym zakresie. Systemy płatności mobilnych działają

w oparciu o różne technologie: w systemach zamkniętych z udziałem operatorów telefonii komórkowej czy też na platformach otwartych. Trudno jest na tym etapie jednoznacznie określić, które staną się powszechnie obowiązującym standardem, a które pozostaną jedynie eksperymentem.

Pewne natomiast jest to, że w najbliższych latach rozbudowana sieć akceptacji płatności i wypracowanie wiodącego rozwiązania zdecydują o upowszechnieniu się płatności mobilnych wśród użytkowników. Banki mają dużą rolę do odegrania w tym procesie, gdyż to one są najbliżej obszaru płatności i mają szerokie możliwości edukacji klientów.

Mając na uwadze dynamiczny wzrost liczby urządzeń mobilnych i prognozy dotyczące tego rynku możemy być pewni, że przyszłość mobilności w usługach finansowych będzie niezwykle interesująca.

Maciej Gawroński

Partner zarządzający Bird & Bird. Ma 20-letnie doświadczenie w doradztwie z zakresu prawa nowych technologii, IT, jak również outsourcingu oraz bankowości i finansów. Doradzał przy ponad 100 projektach wdrożeń informatycznych, w tym przy największym wdrożeniu w sektorze finansowym w Polsce.

Od 2009 roku zajmuje się zagadnieniami *cloud computingu* i jest jednym z najbardziej poważanych ekspertów w tym obszarze w Polsce. Ekspert Komisji Europejskiej ds. Kontraktów Cloud Computingowych i konsultant Grupy Roboczej Artykułu 29. Redaktor i współautor Raportu Związku Banków Polskich „Cloud Computing w sektorze finansowym – regulacje i standardy" (2011), współautor raportu Związku Banków Polskich „Cloud computing 2013". Współautor analizy wykonalności wdrożenia *cloud computingu* w administracji publicznej w Polsce (2014). Jest także wykładowcą studiów podyplomowych Szkoły Głównej Handlowej „Zastosowanie technologii cloud computingu w modelowaniu biznesowym" (2013/14).

Maciej Gawroński, Bird & Bird

Aspekty prawne cloud computingu w odniesieniu do sektora bankowego (regulacje EU)

W artykule omawiam rozwiązania prawne na poziomie Unii Europejskiej, które będą miały wpływ i mogą pomóc bankom w szerokim wykorzystaniu przetwarzania danych w chmurze.

Dla oceny wpływu *cloud computingu* na gospodarkę, a w ramach niej na sektor finansowy, warto na początek spojrzeć wstecz. Sektor bankowy jest mocno zinformatyzowany, przy czym szczególnie dużo inwestował on w informatykę na przełomie wieków. Wdrażano wtedy duże rozwiązania sprofilowane pod każdy bank osobno, oparte na niezależnych zasobach sprzętowych. Każdy z nich posiadał własne centra przetwarzania danych i tak zostało do tej pory. Informatyzacja na skalę przemysłową wymagała w owym czasie wielkich nakładów, dlatego dostępna była dla nielicznych. Sektor finansowy dysponował stosownymi zasobami, a że od wieków zajmuje się głównie zapisywaniem liczb, był zatem predestynowany do korzystania z narzędzi IT.

„IT doesn't matter"

Początek XXI wieku i tzw. „bańka internetowa" na nowojorskiej giełdzie w połączeniu z rozwojem telekomunikacji doprowadziły do zmiany reguł gry. Część czytelników może nie pamiętać niesamowitej hossy z początku lat 2000 na akcje firm internetowych z Amazonem na czele. Równocześnie Amazon[1] był wymieniany w owym czasie jako najbardziej przeceniona firma w historii. Pęknięcie bańki internetowej pozbawiło wielu inwestorów pieniędzy i nadziei, jednak inwestycje kapitałowe w infrastrukturę teleinformatyczną pozostały realne. Wielkie nakłady finansowe zostały zainwestowane w centra

1 Amazon jest obecnie jednym z liderów oferty *cloud computingowej*.

przetwarzania danych, a tradycyjne myślenie o zasobach informatycznych doprowadziło do drastycznego przerostu dostępnej mocy obliczeniowej względem istniejących potrzeb. Te zdarzenia, w połączeniu z konsumencko-naukowym cloudem SETI@home,[2] stworzonym na potrzeby programu poszukiwania obcych cywilizacji SETI, doprowadziły do przełamania tradycyjnego myślenia o zasobach informatycznych i uwolnienia mocy obliczeniowej. Obecnie Amazon jest największym na świecie uniwersalnym dostawcą chmury.

W 2003 roku Nicolas G. Carr opublikował w Harvard Business Review artykuł *IT doesn't matter*, w którym dowodził, że informatyka straciła swój przełomowy charakter i że stała się dostępną każdemu technologią „infrastrukturalną", podobnie jak energia elektryczna, ogrzewanie czy telekomunikacja (a w jej ramach ostatnio transmisja danych). Tezy postawione w tym artykule stały się rzeczywistością. Rozwój oferty *cloud computingu* w istotnej mierze sprawił, że posiadanie na własność mocy obliczeniowej straciło na znaczeniu. Obecnie, wg McKinsey, posiadanie serwera jest trzy razy droższe niż jego wynajmowanie w chmurze, a, co więcej, szybkość serwerów podwaja się co osiemnaście miesięcy.[3]

W tym samym czasie świat przestępczy, zapewne dzięki skopiowaniu idei SETI@home, również uzyskał dostęp do wielkiej mocy obliczeniowej przez tzw. sieci zombie – pojedyncze komputery przyłączone do internetu, które zostały zarażone wirusami komputerowymi. Za ich pomocą pojedyncza osoba może wykonać skoordynowany atak np. na system bankowy.

Czy jest bezpiecznie?

W takim krajobrazie CIO, CFO i CEO banku zastanawiają się obecnie wspólnie (i pod czujnym okiem regulatora), jak podejść do oferty *cloud computingowej* i czy traktować ją jeszcze jako zagrożenie, czy już jako okazję, co może różnie przedstawiać się z perspektywy każdego z nich. Wyrażane są obawy co do bezpieczeństwa rozwiązań *cloud computingowych*, transparentności podejścia do bezpieczeństwa, a także co do zakresu odpowiedzialności prawnej. Dostawcy chmury odpowiadają, wskazując na przewagę budżetów i przemysłowego podejścia do bezpieczeństwa po ich stronie, że problem transparentności zderza się z obowiązującą w bezpieczeństwie zasadą „wiedzy koniecznej",

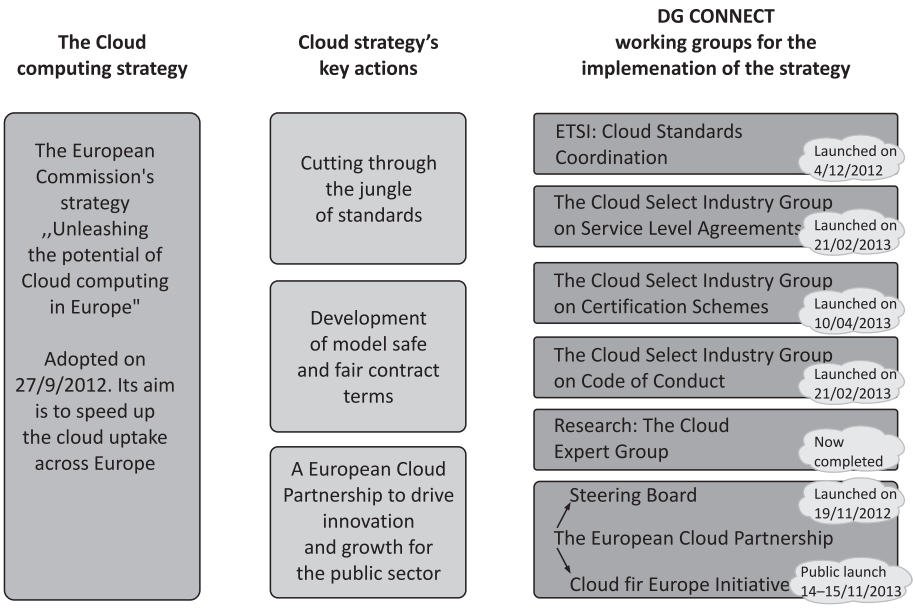
2 http://pl.wikipedia.org/wiki/SETI@home

3 http://www.businessinsider.com/mckinsey-disruptive-technology-report-2013-6

a kwestia odpowiedzialności prawnej powstaje jako zagadnienie do rozwiązania na drodze praktycznej – np. poprzez ubezpieczenia oraz operacyjne ograniczenie ryzyka uzależnienia od jednego dostawcy.

Europejski entuzjazm cloudowy

Komisja Europejska dokonała już oceny *cloud computingu*, w sposób jednoznaczny uznając ten trend technologiczno-biznesowy za okazję dla Europy do zwiększenia swojej konkurencyjności. Jej stanowisko zostało zawarte w dokumencie o wymownym tytule *Unleashing the potential of cloud computing in Europe.*[4] Cały czas prowadzi też prace zgrupowane w kilku wątkach w tym celu, aby usunąć bariery do rozwoju rynku *cloud computingu* na terenie UE. Poniższy diagram obrazuje organizację prac Komisji Europejskiej.[5]



4 Wspólny komunikat Komisji Europejskiej do Parlamentu Europejskiego, Rady Europejskiej, Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Strategia bezpieczeństwa cybernetycznego Unii Europejskiej z 7 lutego 2013 r.; Wspólny komunikat Komisji Europejskiej do Parlamentu Europejskiego, Rady Europejskiej, Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Wykorzystanie Potencjału Chmury Obliczeniowej w Europie" COM(2012) 529, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:PL:PDF

5 http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy#safe-and-fair-contract-terms-and-conditions

Prace Komisji Europejskiej trwają, ich aktualny stan można śledzić w miarę publikacji materiałów na stronach Komisji pod adresem http://ec.europa.eu/digital-agenda/en/telecoms-and-internet/cloud-computing. Sam biorę w nich udział, jako ekspert Komisji Europejskiej, w wątku dotyczącym opracowania warunków kontraktów cloudowych, oraz jako konsultant Grupy Roboczej Art. 29 w obszarze ochrony danych osobowych.

Sektor informatyczny artykułuje obawy, że podejście Komisji Europejskiej jest zbyt zorientowane na konsumenta, gubiąc przy tym podstawowy cel prac nad *cloud computingiem*, jakim ma być akceleracja jego wykorzystania. Na dzisiaj jednak istotny jest sam fakt prowadzenia przez Komisję Europejską działań zmierzających do przyspieszenia wykorzystania *cloud computingu* w europejskiej gospodarce (w tym w sektorze administracji publicznej). Nadto obawy sektora powinny zaowocować wspólnymi pracami i opracowaniami, które przedstawiać będą zrównoważone poglądy i pełne konsekwencje przyjmowania zbyt spolaryzowanego podejścia przez regulatora. Takie działania wpisują się w mądrze rozumiane pojęcie *co-opetition* (co można przetłumaczyć jako konkuperacja lub współkonkurencja), którego dobrym przykładem są, w mojej ocenie, prace nad *cloud computingiem* Forum Technologii Bankowych przy Związku Banków Polskich, w których uczestniczyłem. Ciekawą inicjatywą może okazać się także ostatnio otwarte Microsoft Cloud Computing Research Centre w Brukseli. 2 kwietnia 2014 roku także Microsoft uzyskał aprobatę Grupy Roboczej Art. 29 dla warunków ochrony danych osobowych, które będzie oferował klientom swoich usług chmurowych. Wydaje się więc, że tymi ruchami Microsoft wysunął się na pozycję lidera sektora informatycznego w promocji czytelnych zasad *cloud computingu* w UE.

Czym jest cloud computing dla prawnika?

Dla ustrukturyzowania obrazu prawnych aspektów *cloud computingu* oprzyjmy się na założeniu, że, z punktu widzenia prawnika[6], *cloud computing* to kontraktowe: (1) powierzenie przetwarzania danych, (2) powierzenie tajemnicy, (3) outsourcing procesu.

Warto przy tym zauważyć, że u podstaw regulacji, które stosują się do *cloud computingu*, kryją się paradygmaty wiedzy o bezpieczeństwie informacji i ciągłości działania.

6 W relacjach z konsumentami dochodzi cała lawina regulacji konsumenckich. Aspekt ten szczęśliwie możemy jednak pozostawić poza ramami tego artykułu.

Regulacje unijne

Najważniejszym obszarem prawnym, który na obszarze Unii Europejskiej stosuje się do *cloud computingu* jest ochrona danych osobowych. Obszar ten regulowany jest przez Dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 roku w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych[7] („Dyrektywa o ochronie danych").

Dyrektywa o ochronie danych posługuje się znanym już wcześniej pojęciem administratora danych (*controller*) oraz przetwarzającego dane (*processor*) na zlecenie administratora danych. W klasycznej relacji B2B dostawca chmury jest *processorem*[8], a klient chmury (np. bank) – *data controllerem*.

Legalność *cloud computingu*. W przeszłości wyrażane były wątpliwości co do ogólnej legalności modelu *cloud computingu* w świetle zasad ochrony danych osobowych w UE, w szczególności wobec wymogu posiadania wiedzy o lokalizacji danych przez podmioty, które powierzają je do przetwarzania (tzn. administratorów danych). W chwili obecnej dość zgodnie już przyjmuje się, że jako wiedza o położeniu danych wystarczy ta o lokalizacji infrastruktury dostawcy chmury, tj. centrów przetwarzania danych. Także i w tym zakresie są jednak pewne rozbieżności. Na przykład w ramach rządowego programu G-Cloud w Wielkiej Brytanii, związanego z przetwarzaniem danych o znaczeniu strategicznym, lokalizację centrów przetwarzania danych dostawców chmury ujawnia się tylko powołanym do tego celu służbom, a to dlatego, by ograniczyć ryzyko ataku lub fizycznej infiltracji.

Wieloreżimowa zgodność chmury w EOG. Dyrektywa jest narzędziem, które nie zapewnia pełnej jednolitości prawa w całej UE, natomiast narzuca minimalne wymogi harmonizacyjne. Z punktu widzenia dostawcy chmury kierującego ofertę do klientów w innych państwach Europejskiego Obszaru Gospodarczego (EOG) oznacza to w praktyce, że jest 28 zbliżonych, ale jednak różniących się szczegółami porządków prawnych, z którymi jego usługa powinna być zgodna. Jest tak, ponieważ do przetwarzania danych osobowych stosuje się zasady obowiązujące administratora danych (*controllera*), a dodatkowo należy stosować zasady zabezpieczenia danych miejsca siedziby przetwarzającego (*processora*). W praktyce oznacza to, że chmura obliczeniowa

---

7 Dz.U. L 281z 23.11.1995.

8 Uznałem, że omawiając regulacje unijne oraz cloud computing warto posługiwać się przyjętym żargonem.

oferowana bankom z różnych krajów powinna spełniać kumulatywnie wymagania w zakresie bezpieczeństwa danych określone przez prawa stosujące się do tych banków, a zatem oferować to bezpieczeństwo na odpowiednio wysokim poziomie.

Swoboda przepływu danych w EOG. Ważne jest także, że prawo unijne nie wymaga zgód administracyjnych dla przekazywania danych na terenie Europejskiego Obszaru Gospodarczego. Daje to dużą przewagę dostawcom chmury, którzy mają swoją infrastrukturę zlokalizowaną na terenie EOG.

Chmura pozaunijna

Eksport danych poza Europejski Obszar Gospodarczy, co do zasady, wymaga spełnienia dodatkowych obowiązków, w szczególności uzyskania zezwolenia odpowiedniego organu ochrony danych osobowych (w Polsce Generalnego Inspektora Ochrony Danych Osobowych GIODO).

Dodatkowych obowiązków nie trzeba spełniać jedynie wtedy, gdy prawo kraju spoza EOG, do którego dane mają być przekazywane, zapewnia ochronę danych osobowych adekwatną do poziomu unijnego lub jeśli podmiot, który dostarcza chmurę, posiada certyfikat *Safe Harbor* (Bezpieczna Przystań), o którym mowa dalej.

Teoretycznie eksporter danych powinien dokonać samodzielnej oceny czy państwo, do którego zamierza eksportować dane zapewnia adekwatną ochronę danych osobowych. W praktyce taka subiektywna ocena nie jest możliwa. W przypadku niewłaściwej oceny eksporterowi danych będzie groziło poniesienie odpowiedzialności administracyjnej, a nawet karnej. Jedynie w przypadku krajów, które zgodnie z decyzją Komisji Europejskiej zapewniają adekwatną ochronę danych osobowych eksporterzy będą mieć pewność, że mogą transferować dane bez konieczności spełnienia dodatkowych wymogów. Do tej pory Komisja wydała takie decyzje w odniesieniu do kilkunastu krajów (jednak nie zawsze w pełnym zakresie), w tym np. względem Szwajcarii, Kanady, Izraela, Argentyny i Australii.

Safe Harbor

Stany Zjednoczone, co do zasady, nie zapewniają adekwatnego poziomu ochrony danych osobowych. Pomiędzy Unią Europejską a USA została jednak wynegocjowana umowa międzynarodowa, na podstawie której amerykańskie

przedsiębiorstwa mogą zobowiązywać się do zapewniania adekwatnego poziomu ochrony danych. Przesyłanie danych do takich przedsiębiorstw (tzw. *Safe Harborytów*) może następować bez konieczności spełnienia dodatkowych prawnych wymogów. Należy pamiętać, że przedsiębiorstwa z USA mają jednak możliwość selektywnego przystępowania do programu *Safe Harbor*, np. tylko w odniesieniu do własnych danych pracowniczych.

Niestety, ujawnienie przez Edwarda Snowdena inwigilacji przez Amerykańską Agencję Bezpieczeństwa (NSA) częściowo podważyło zaufanie do umowy *Safe Harbor*. Może to mieć jednak pozytywne skutki dla Europy, gdyż z pewnością stanowić będzie dodatkowy impuls do rozwijania oferty *cloud computingu* na terenie Europejskiego Obszaru Gospodarczego i do korzystania z usług europejskich dostawców. Równocześnie, w przypadku korzystania z rozwiązań chmurowych oferowanych przez korporacje amerykańskie, wskazany jest wybór ofert tych podmiotów, które zapewniają, że dane przetwarzane w ofercie europejskiej nie podlegają monitoringowi NSA.

Zgoda GIODO na eksport danych

Podmiot, który zamierza eksportować dane do kraju trzeciego, może ubiegać się o uzyskanie zgody na transfer danych od odpowiedniego organu do spraw ochrony danych osobowych (w Polsce zgodnie z art. 8 ust. 1 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych[9] („**uodo**") organem tym jest GIODO). Zgoda jest udzielona na konkretny eksport danych i do konkretnego odbiorcy, w zakresie wskazanym we wniosku. GIODO nie udziela generalnej zgody na eksport wszystkich kategorii danych bez ich dookreślenia. Jeśli eksporter danych chciałby zatem rozszerzyć zakres eksportowanych danych, np. w związku z rozszerzeniem oferty dostawcy chmury, musi ponownie wystąpić do GIODO o zgodę.

Standardowe Klauzule Umowne i Wiążące Reguły Korporacyjne. W celu uniknięcia komplikacji i przyspieszenia procedury uzyskania zgody GIODO na transfer danych do kraju trzeciego eksporter może zawrzeć w odpowiedniej umowie opublikowane przez Komisję Europejską standardowe klauzule umowne (*Standard Contractual Clauses* – w skrócie SCC), stanowiące zestaw odpowiednich wzorcowych postanowień umownych zapewniających adekwatny poziom ochrony danych osobowych przy ich przekazaniu poza

9 Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 Nr 133 poz. 883 z późn. zm.)

Unię Europejską. W takiej sytuacji GIODO niejako z automatu przyjmuje wzorzec wypracowany przez Komisję Europejska, badając jedynie takie elementy, jak cel i zakres danych (czy przetwarzanie danych jest zgodne z prawem, adekwatne) oraz czy odbiorca danych zobowiązał się do przestrzegania odpowiednich środków zabezpieczających.

Możliwe, że zgoda GIODO na transfer na podstawie standardowych klauzul umownych nie będzie w przyszłości wymagana. Rząd pracuje obecnie nad nowelizacją ustawy o ochronie danych osobowych, która ma znieść ten formalizm.[10]

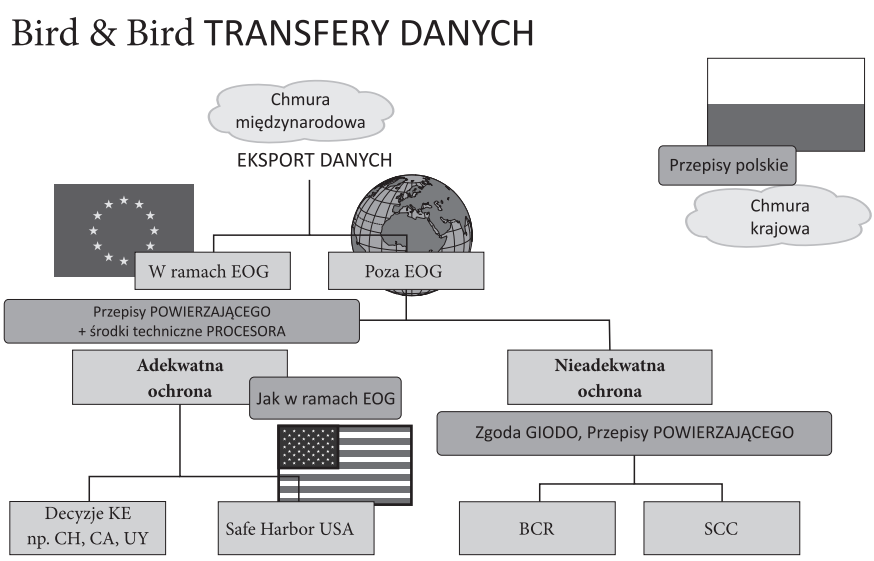
Komisja Europejska opracowała dodatkowo inny mechanizm zapewnienia adekwatnej ochrony danych osobowych polegający na przyjęciu przez daną międzynarodową korporację (a konkretnie spółki takiej korporacji położone na terenie EOG jako administratorów danych) wiążących reguł korporacyjnych (*Binding Corporate Rules* – w skrócie BCR), stanowiących wewnętrzny „regulamin" ochrony danych osobowych w spółkach takiej korporacji. W przypadku przyjęcia tych reguł i ich zatwierdzenia przez odpowiednie organy ochrony danych osobowych korporacja jest traktowana jak bezpieczny obszar przetwarzania danych, w którym dane osobowe są chronione na poziomie wymaganym w UE.

Transfery danych – schemat

Rysunek na następnej stronie obrazuje regulacje UE dotyczące transferów danych osobowych, o których mowa było powyżej.

Zagadnienia omawiane powyżej opisane są także na stronach GIODO pod adresem: http://www.giodo.gov.pl/163/id_art/1519/j/pl/.

10 Projekt jest częścią pakietu deregulacyjnego i jest dostępny na stronie www.legislacja.rcl.gov.pl



Rozporządzenie EU o ochronie danych osobowych

Równolegle do prac nad przyspieszeniem europejskiej chmury toczą się prace nad pełnym ujednoliceniem europejskiego prawa ochrony danych osobowych, czyli nad projektem ogólnego rozporządzenia UE o ochronie danych osobowych.

W dniu 12 marca 2014 roku Parlament Europejski przyjął projekt Rozporządzenia. Komisarz Vivienne Reading zapowiedziała, że oczekuje wzmożonej pracy nad reformą w 2014 roku.

Rozporządzenie przejmuje z Dyrektywy o ochronie danych koncepcję administratora danych i przetwarzającego, a także powierzenia przetwarzania danych osobowych, a w tym ich przechowywania.

Podobnie, jak to jest określone w uodo, odpowiedzialność administracyjna przetwarzającego (dostawcy chmury bankowej) będzie ograniczała się do zapewnienia gwarancji wdrożenia środków i procedur technicznych i organizacyjnych.

Projekt Rozporządzenia określa dość ogólnie środki techniczne i organizacyjne zabezpieczenia danych. Europejska Rada Ochrony Danych Osobowych (*European Data Protection Board*) ma zostać upoważniona do określenia szczegółowych środków technicznych i organizacyjnych w drodze wytycznych, rekomendacji i dobrych praktyk.

Szerszy jest katalog zobowiązań przetwarzającego wobec administratora, np. przetwarzający udostępnia administratorowi i organowi nadzorczemu wszelkie informacje niezbędne dla kontroli zgodności z niektórymi obowiązkami przetwarzającego, umożliwia administratorowi inspekcję, usuwa dane osobowe po zakończeniu współpracy (art. 26 pkt 2 Projektu Rozporządzenia). Te regulacje będą miały znaczenie dla sposobu ułożenia stosunków między klientem chmury a jej dostawcą.

W kontekście chmury obliczeniowej warto wspomnieć o następujących rozwiązaniach proponowanych w Rozporządzeniu:

- ***Privacy impact assessment* (PIA)**. Co do zasady, w przypadku przetwarzania danych osobowych w kontekście chmury obliczeniowej administrator danych będzie zobowiązany do przeprowadzenia oceny ryzyka takiego przetwarzania dla praw i wolności podmiotów danych. Ocena taka powinna obejmować: opis przetwarzania danych, ocenę ryzyka dla praw i wolności podmiotów danych, środki przewidziane w celu sprostania ryzykom, gwarancje, środki i mechanizmy bezpieczeństwa mające zagwarantować ochronę danych osobowych oraz wykazać zgodność z Projektem Rozporządzenia, uwzględniając prawa i słuszne interesy podmiotów danych i innych zainteresowanych osób. Już teraz Grupa Robocza art. 29 ds. Ochrony Danych i inne organy ochrony danych rekomendują przeprowadzenie PIA w przypadku korzystania z rozwiązań chmurowych.
- ***Privacy by design.*** Administrator danych powinien uwzględnić ochronę danych już w fazie projektowania (*privacy by design*) oraz chronić dane jako opcję domyślną (*privacy by default*). Uwzględniając najnowsze osiągnięcia techniczne oraz koszty wdrożenia administrator, zarówno w momencie ustalania środków niezbędnych do przetwarzania, jak i w momencie samego przetwarzania, wdraża odpowiednie środki i procedury techniczne i organizacyjne, tak by przetwarzanie odpowiadało wymogom Rozporządzenia oraz gwarantowało ochronę praw podmiotu danych. Także przetwarzający będzie zobowiązany do uwzględnienia ochrony danych już w fazie projektowania (*privacy by design*) oraz zakładać ochronę prywatności jako opcję domyślną (*privacy by default*). Obecne rozwiązania chmurowe nie były na ogół projektowane pod tym kątem.
- **Przenoszalność danych.** Według art. 18 Projektu Rozporządzenia podmiot danych będzie miał prawo do uzyskania od administratora kopii danych w przyjętym i użytecznym formacie. Banki powinny zwrócić uwagę na to zobowiązanie, gdyż łatwo sobie wyobrazić jego zastosowanie względem

banku traktowanego przez klienta bankowości internetowej jako dostawcę chmury. Zagadnienie przenoszalności danych było przedmiotem mojego referatu podczas prac Grupy Ekspertów Komisji Europejskiej ds. kontraktów *cloud computingowych*.

- **Zawiadomienie o naruszeniu (***data breach notification***)**. W przypadku naruszenia bezpieczeństwa danych osobowych administrator będzie zobowiązany niezwłocznie powiadomić nadzorujący go organ ochrony danych. Jeśli może dojść do naruszenia prywatności konkretnej osoby, administrator powinien powiadomić także tę osobę. Niezależnie trwają także prace nad Rozporządzeniem Komisji Europejskiej w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych.[11] Rozporządzenie będzie miało także zastosowanie do usługodawców świadczących usługi drogą elektroniczną, np. do komercyjnych operatorów chmury obliczeniowej.
- **Współadministratorzy.** Rozporządzenie dopuszcza instytucję współadministratorów (*joint controllers*). W przypadku wspólnego określenia przez dwóch administratorów celów, warunków i środków przetwarzania danych osobowych przez współadministratorów określają oni zakres odpowiedzialności za zgodność z obowiązkami wynikającymi z Rozporządzenia i spoczywającymi na każdym z nich, w szczególności jeśli chodzi o procedury i mechanizmy praw podmiotu danych w drodze ustaleń. To rozwiązanie może być przydatne przy korzystaniu przez banki z chmury sektorowej (*community cloud*).
- **Kary.** „Last but not least", w przypadku naruszenia organ nadzorczy uprawniony będzie do nałożenia następujących kar: (i) listu ostrzegawczego w przypadku pierwszego nieumyślnego naruszenia, (ii) regularnych audytów danych osobowych, (iii) grzywny do wysokości 100 mln EUR lub 5% światowego przychodu grupy w zależności od tego, która sankcja będzie bardziej dotkliwa. Obecnie GIODO ma możliwość nałożenia kar tylko w przypadku niewykonania jego decyzji nakazującej zaniechanie naruszeń do łącznej wysokości 200 tys. zł. Wbrew pozorom ta „nowinka" może spowodować skokowy wzrost zainteresowania usługami *cloud computingowymi*. Osoby zainteresowane dowiedzeniem się, dlaczego tak się stanie, zachęcam do bezpośredniej rozmowy ze mną.

---

11 Rozporządzenie Komisji (UE) NR 611/2013 z dnia 24 czerwca 2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej (Dz.U. UE L 173/2 z dnia 26 czerwca 2013 r.)

Polski outsourcing bankowy

Prawo bankowe, podobnie jak inne obecnie obowiązujące w Polsce przepisy, nie reguluje wprost *cloud computingu*. Do przetwarzania chmurowego będą jednak miały zastosowanie wymogi prawne dla tzw. outsourcingu w działalności bankowej, które określa Ustawa z 29 sierpnia 1997 r. Prawo bankowe[12] („Prawo bankowe"), w szczególności art. 6a-6d oraz art. 104 Prawa bankowego.

Można jednoznacznie stwierdzić, że polska ustawa jest najbardziej wrogą *cloud computingowi* regulacją w UE w sektorze finansowym. Prawo bankowe, co do zasady, zakazuje wprowadzania ograniczeń odpowiedzialności odszkodowawczej outsourcera (dostawcy chmury). Ograniczenia takie nie są znane systemom prawnym krajów zachodnich i stoją na przeszkodzie wykorzystania potencjału chmury obliczeniowej przez polski sektor bankowy. Relatywnie nikły koszt korzystania z niej względem korzyści, które dzięki temu realizuje dana organizacja powodują, że dostawcy chmury nie są chętni do akceptowania nieograniczonej odpowiedzialności za ewentualne problemy z zapewnieniem odpowiedniej jakości swoich usług.

Takie podejście jest racjonalne paradoksalnie także z punktu widzenia klienta chmury. Dobrze skonstruowana i monitorowana chmura obliczeniowa zapewnia poziom bezpieczeństwa informacji przekraczający to, co może osiągnąć wewnętrzny dział IT, nie mówiąc o dużo większej efektywności kosztowej. Drogą do jej racjonalnego wykorzystania w sektorze bankowym nie jest utrzymywanie rygorystycznej odpowiedzialności prawnej potencjalnych dostawców chmury. Obecnie obowiązujący zakaz ograniczeń odpowiedzialności w outsourcingu bankowym może skutkować poczuciem fałszywego bezpieczeństwa po stronie banków, przez które będą może zwracać mniejszą uwagę na zapewnienie rzeczywistego bezpieczeństwa informacji i ciągłości działania przez dostawców chmury, kontentując się iluzoryczną możliwością uzyskania odszkodowania, które i tak nie zrekompensuje szkód reputacyjnych mogących powstać w razie utraty ciągłości usługi chmurowej. Powstaje też dodatkowe ryzyko systemowe w przypadku korzystania z usług jednego dostawcy chmury przez wiele banków. Problemy dotyczące relacji pomiędzy tym dostawcą a daną jednostką mogłyby prowadzić do upadłości dostawcy i w rezultacie „zarazić" relacje pomiędzy nim a innymi jego klientami. Już w tej chwili w polskim systemie bankowym istnieją infrastrukturalni dostawcy usług IT, których upadłość jest z punktu widzenia sektora bankowego niedopuszczalna.

12 Ustawa z 29 sierpnia 1997 r. Prawo Bankowe (Dz.U.02.72.665 z późn. zm.)

Prawidłowego rozwiązania zagadnienia relacji z dostawcą usługi chmurowej poszukiwać należy w innych obszarach niż iluzja nieograniczonej odpowiedzialności. Rozwiązaniem takim może być zapewnienie sobie przez bank zapasowego rozwiązania umożliwiającego utrzymanie działania istotnej usługi (brak zależności operacyjnej) lub przynajmniej możliwość przywrócenia ciągłości w rozsądnym czasie. Bank może też rozważyć poleganie na audytach jakości bezpieczeństwa informacji i ciągłości działania danej chmury, które powinny przeprowadzać niezależne podmioty zaufane.[13] Można oczekiwać rozsądnej wysokości ubezpieczenia OC jako dodatkowej gwarancji, że ubezpieczyciel będzie wykonywał jakościową kontrolę bezpieczeństwa i ciągłości działania ubezpieczonej chmury. Nie można pomijać także stricte kontraktowej odpowiedzialności. Co więcej, rozsądnym jest oczekiwanie, że zagrożenie naruszenia bezpieczeństwa informacji ze strony outsourcera jest niższe niż ze strony personelu wewnętrznego (szacuje się, że 80% zagrożeń bezpieczeństwa powodują insiderzy) oraz że interes dostawcy chmury ma charakter stricte finansowy, a zatem że dostawcy chmury zależeć będzie na zapewnieniu bezpieczeństwa informacji i ciągłości działania swojej usługi, gdyż w innym wypadku stworzy zagrożenie dla własnej egzystencji.

Podsumowanie

Przed sektorem bankowym stoją obecnie wyzwania w zakresie zapewnienia niezawodności działania i szybkości reakcji na trendy rynkowe, ale też i oczekuje się zwiększonej efektywności finansowej samego sektora. Mówi się, ze sektor bankowy zapewnia krwioobieg gospodarki. Im będzie on sprawniejszy i im mniej krwi będzie potrzebował na własne funkcjonowanie, tym więcej pozostanie jej dla reszty krajowego gospodarczego organizmu.

W tej chwili 80% wydatków informatycznych banków pochłania samo utrzymanie systemów IT, a tylko 20% jest inwestowane w rozwój. Powierzenie części powtarzalnych procesów dostawcom zewnętrznym, którzy efektywniej wykonywać je będą na rzecz wielu odbiorców, umożliwiłoby bankom uwolnienie zasobów wewnętrznych. A te można byłoby przekierować do pracy nad rozwojem rozwiązań, którymi banki chciałyby zapewnić sobie przewagę rynkową (nie tylko względem konkurentów z sektora bankowego, ale i wobec zewnętrznej konkurencji wkraczającej na pole usług finansowych) oraz do doskonalenia się w nadzorze bezpieczeństwa działania swoich dostawców.

13 Audyty takie warto rozważyć także w odniesieniu do wewnętrznej infrastruktury teleinformatycznej banku.

Od *cloud computingu* nie ma odwrotu. Efektywność kosztowa, szybkość reakcji, elastyczność, budżet na bezpieczeństwo oraz zdolność do ściągnięcia najlepszych zasobów ludzkich tworzą nieuchronną przewagę tego modelu świadczenia usług IT względem zapewniania ich sobie wewnętrznie przez organizację.

Pozostaje pytanie, czy Polska i polski sektor bankowy powinny być awangardą, naśladowcami dobrych wzorców w tym zakresie, czy raczej staną się europejską ariergardą w tym obszarze.

Andrzej Pyka
Dyrektor Pionu Consulting and Systems Integration w firmie Atos od października 2013 roku. Z wykształcenia inżynier po Wydziale Elektroniki i Telekomunikacji na Politechnice Wrocławskiej, jest też absolwentem IESE Business School na Uniwersytecie w Nawarze.
Może się pochwalić ponad 17-letnim doświadczeniem w prowadzeniu projektów transformacyjnych, implementacji systemów oraz konsultingu operacyjnym. Wcześniej pracował w Accenture (1999–2013) i Accenture Consulting (1995–99) oraz w InterAms (1994), obsługując wiele instytucji z sektora bankowego, ubezpieczeń oraz telekomunikacji.

Andrzej Pyka, Atos

Pokolenie Y: nowy rodzaj pracowników – szanse i zagrożenia

Zacznijmy od przytoczenia krótkiej sceny z Targów Pracy na SGH, gdzie, jak co roku, prezentowały się międzynarodowe korporacje i globalne firmy doradcze, tradycyjnie uważane za najlepszy możliwy start w życie zawodowe i szczyt marzeń absolwenta planującego karierę w zarządzaniu. Prezentację jednej z firm prowadził Partner noszący liczne atrybuty luksusu. Po jej zakończeniu podszedł do niego jeden ze studentów i zapytał:

— A więc przyjmujecie tylko najlepszych z najlepszych?
— Dokładnie tak.
— I pracując u was będę podróżował po stolicach Europy, rozwiązywał najciekawsze dylematy wielkiego biznesu i miał dostęp do najnowszych narzędzi i wiedzy?
— Jak najbardziej.
— Będę pracował 14 godzin na dobę, a za dziesięć lat będzie mnie stać na wszystko i będę wyglądał mniej więcej tak jak Pan?
— Bardzo możliwe.
— Eee..., to ja dziękuję.

Wiemy, że kilka lat wcześniej taki finał rozmowy byłby nie do pomyślenia. Student ochoczo przystąpiłby do szeregu testów, symulacji pracy grupowej i rozmów kwalifikacyjnych, a następnie, jeżeli rzeczywiście byłby najlepszy, rozpocząłby pracę w 14-godzinnym reżimie i uważał się za szczęśliwca.

Tymczasem po rozmowie z Partnerem nasz student rozpoczął odprężające popołudnie. Włożył do uszu białe słuchawki smartfona i zainteresował się pogodą w Warszawie. Choć mógł ją sprawdzić spoglądając w niebo, odczytał ją z aplikacji. Następnie w drodze na przystanek autobusowy *czatując* przez *Facebooka* wymienił z kolegami wrażenia z Targów i umówił się do kina. Choć spotkał się z nimi w kawiarni vis-a-vis kinowych kas, bilety kupił przez kinowy

app i zapłacił za nie przez *SkyCash* (inny *app*). Wchodząc na salę kinową wyświetlił bilet na ekranie smartfona.

Przytoczone tu sceny są autentyczne. Świadczą one, że tak zwane Pokolenie Y zagościło na dobre w wielkomiejskich ośrodkach w Polsce a jego przedstawiciele weszli wiek, w którym mają ogromne znaczenie jako konsumenci, klienci i pracownicy.

Kto to jest

Nazwa Pokolenie Y (*Generation Y*) pojawiła się po raz pierwszy w roku 1993 w wydawanym w USA tygodniku *Advertising Age*, by określić młodzież urodzoną w tym kraju po roku 1982 i wykazującą charakterystyczne podejście do życia, zachowania i gusty. Pojęcie to zostało rozwinięte i doprecyzowane przez socjologów Williama Straussa i Neila Howe, którzy przedstawiają historię USA i świata anglosaskiego jako sekwencję pokoleń o cyklicznie powtarzających się cechach. W najnowszej historii USA wyróżniają oni cztery pokolenia:

Pokolenie	Daty urodzenia	Charakterystyka
Baby boomers	1943–1960	• pokolenie powojennego wyżu demograficznego, żyjące w nadziei na przebudowę świata na lepszy • doświadczyli szybkiej poprawy statusu materialnego w sytuacji powojennego wzrostu gospodarczego • pracowali w korporacji lub własnym biznesie • gadżet: radio tranzystorowe, telewizor
Pokolenie X	1961–1981	• doświadczyli spowolnienia wzrostu gospodarczego i co najmniej jednego kryzysu • nowe technologie doprowadziły do wyzwolenia się przedsiębiorczości i innowacyjności • gadżet: odtwarzacz wideo, komputer osobisty
Pokolenie Y, „Millenials”[1]	1982–2004	• sceptyczni wobec instytucji, lojalni wobec znajomych i przyjaciół • pewni siebie, narcystyczni, optymistyczni • otwarci na odmienność • od dziecka korzystający z komputera i internetu • gadżet: iPod, smartfon
Pokolenie Z, „Homeland”	2005– do dziś	• ukształtowani poprzez atak na WTC, wojnę w Afganistanie i światowy kryzys gospodarczy • codziennie korzystający z Internetu, sieci społecznościowych, komunikatorów i telefonów komórkowych

1 Słowo Millenials oznacza osoby wyrastające z dzieciństwa na przełomie tysiącleci.

Pokolenie Y zostało szeroko opisane w książce *Millennials Rising: The Next Great Generation*[2]. Bardzo dobrą syntezę podaje artykuł firmy Deloitte[3]:

Co ich ukształtowało – doświadczenia:

- niespotykana wcześniej opieka rodzicielska: udział ojców w wychowaniu dzieci i wsparcie materialne i mentalne rodziców udzielane nawet po osiągnięciu przez nie dojrzałości,
- wojna w Iraku i zagrożeni nuklearne ze strony Korei,
- atak na WTC,
- wielkie skandale korporacyjne (Enron, WorldCom),
- pojawienie się nowych potęg gospodarczych (Chiny, Indie).

Co ich ukształtowało – technologia:

- nie znają życia bez komputera,
- odwrócona akumulacja wiedzy – „im jesteś młodszy, tym więcej wiesz",
- cała wiedza i cały świat są „na wyciągniecie komputerowej myszki".

Ich przekonania:

- edukacja jest wartością,
- wewnętrzną spójność jest godna podziwu,
- rodzice stanowią wzorzec.

Jacy są:

- komfortowo posługują się technologią,
- połączeni ze światem 24/7,
- pewni siebie,
- optymistyczni,
- niezależni,
- polegający na sobie,
- przedsiębiorczy,
- otwarci na odmienność,
- ważny jest dla nich styl życia,
- zorientowani na sukces.

Jacy są w pracy:

- świetnie odnajdują się w pracy zespołowej, najlepiej z przyjaciółmi,
- innowacyjni i zaradni,

---

2 William Strauss, Neil Howe, *Millennials Rising: The Next Great Generation*, ISBN 0-375-70719-0.

3 Deloitte Consulting, *Who are the Millenials*.

- chcą tworzyć coś wartościowego i zmieniać rzeczywistość,
- otwarci na częste i szybkie zmiany,
- chcą być doceniani i szanowani,
- akceptują mentorów,
- niecierpliwi.

Pokolenie Y osiągnęło obecnie dorosłość a jego preferencje i nawyki kształtują rynek konsumencki i rynek pracy świata zachodniego. Stanowi ono nie lada wyzwanie dla przełożonych przyzwyczajonych do zarządzania poprzez nakazy i kontrolę oraz do podwładnych, którzy „żyli, by pracować".

Globalizacja gospodarcza i kulturowa początku XXI wieku sprawiła, że odpowiedniki amerykańskiego Pokolenia Y odnajdujemy na całym świecie, w tym w Indiach, Europie i bardzo wyraźnie również w Polsce.

Pokolenie Y w Polsce

Kształtowanie się postaw i zachowań pokoleniowych w Polsce jest oczywiście uwarunkowane historycznie. Polski odpowiednik Pokolenia X, które poprzedza Pokolenie Y, to osoby, które swoją młodość przeżyły w socjalizmie i w stanie wojennym. Doświadczyły one nieefektywności, niedostatków i absurdów dawnego systemu. Ich edukacja i nabyte wzorce okazały się mało przydatne w życiu zawodowym lat 90., kształtowanym przez zachodnie korporacje i rodzimy biznes. Szansa na szybki awans materialny oraz osobisty rozwój przy wykorzystaniu wzorców, szkoleń i kontaktów w ramach firmy sprawiała, że wiele osób głęboko zaangażowało się i wniknęło w korporacyjne tryby.

Pierwsza dekada XXI wieku przyniosła dwie fale kryzysu, które zaowocowały zmniejszeniem budżetów na podróże, szkolenia i rozwój oraz redukcjami zatrudnienia. Wyższe stanowiska kierownicze zostały już wypełnione i możliwości szybkiego awansu znacznie się ograniczyły. Wielkie korporacje straciły swój blask. Jednocześnie pojawiło się wiele małych, lecz dobrze prosperujących firm.

Żyjący w dużych miastach Polacy, urodzeni po roku 1982, kształtowali się w warunkach podobnych do swoich rówieśników w świecie zachodnim. Podobnie jak ich rówieśnicy, mogą w razie potrzeby skorzystać ze wsparcia materialnego i rad rodziców, którzy już mocno okrzepli w nowej rzeczywistości i „starają się zapewnić dzieciom to, czego nie mieli sami". Nie ma barier w przepływie treści kulturowych i wzorców zachowań. Umożliwiają go internet, do którego nie ma już trudności w dostępie, międzynarodowe stacje

telewizyjne oraz wyjazdy organizowane przez rodziców, szkoły i uczelnie. Znajomość języka angielskiego jest powszechna. Żadnych barier nie stanowi cena laptopa, tableta lub smartfona.

Nic dziwnego więc, że z punktu widzenia zachowań konsumenckich lub zarządzania kapitałem ludzkim, żyjący w dużych miastach i urodzeni po 1982 roku Polacy nie różnią się znacząco od swoich rówieśników z Europy czy USA i tak też są traktowani przez międzynarodowe firmy.

Mamy do czynienia z jednym globalnym Pokoleniem Y.

Stosunek Pokolenia Y do banków jako potencjalnych pracodawców

Branża bankowa, wstrząśnięta kryzysem finansowym i z nadszarpnięta reputacją, stoi dziś przed koniecznością transformacji kulturowej i wizerunkowej. Nośnikami zmian kultury organizacyjnej są młodzi liderzy, którzy szybko awansują do szczebli zarządczych. Jednak oczekiwania dzisiejszych absolwentów wobec pracodawców rozmijają się istotnie z ich percepcją branży bankowej. Trudno zatem oczekiwać, że najbardziej utalentowani wybiorą bank jako miejsce stabilnej kariery.

Niedawne globalne badanie firmy Deloitte[4], przeprowadzone wśród studentów, którzy rozważają karierę w bankowości wykazało, że choć w ich percepcji banki posiadają cztery ważne atrybuty, czyli:

- dają szansę na wysokie zarobki w przyszłości,
- stanowią dobrą referencję na dalszych etapach kariery,
- oferują prace pełna wyzwań,
- oraz w pewnym stopniu umożliwiają szkolenia i rozwój zawodowy,

to zdecydowanie nie spełniają oczekiwań pod kątem:

- możliwości pracy z liderami, którzy będą wspierać rozwój młodego pracownika,
- nagradzania za rzeczywiste rezultaty (merytokracja),
- środowiska pracy wspierającego kreatywność i dynamizm,
- elastyczności czasu pracy,
- równowagi między życiem osobistym i zawodowym.

Biorąc pod uwagę, że planowany przez absolwentów okres pracy u pierwszego pracodawcy to najczęściej dwa lub trzy lata, należy się obawiać, że praca

4 Deloitte. Universum. *Generation why? Attracting the bankers of the future.*

w banku jest traktowana głownie jako etap przejściowy służący zbudowaniu umiejętności i podstaw do dalszej kariery.

Jak „zagospodarować" Pokolenie Y

Pojawienie się pokolenia Y niesie dla pracodawcy liczne szanse oraz wyzwania:

Szanse	Wyzwania
• umiejętność pracy zespołowej • skłonność do dzielenia się wiedzą • otwartość na zmiany i szybkość uczenia się • ambicja i dbałość o własny rozwój • umiejętność pracy projektowej • umiejętność pracy w środowisku wielokulturowym • umiejętność jednoczesnego prowadzenia wielu tematów • sprawne posługiwanie się nowoczesnymi narzędziami komunikacji i zarządzania wiedzą • sprawne wyszukiwanie informacji i rozwiązań • podatność na motywację pozafinansową.	• słabe przygotowanie do samodzielnego podejmowania decyzji i ponoszenia odpowiedzialności • słaba podatność na tradycyjne systemy motywacyjne • skłonność do angażowania się wyłącznie w tematy ciekawe i rozwijające, a jednocześnie niechęć do zadań żmudnych • rygorystyczna dbałość o własny czas wolny • odrzucanie autorytetu przełożonych, które wynika jedynie ze stanowiska. • niska lojalność i duże prawdopodobieństwo odejścia, co dla pracodawcy oznacza utratę kompetencji i inwestycji poczynionych w szkolenia • postawy roszczeniowe.

W literaturze oraz wewnętrznych instrukcjach międzynarodowych firm powtarza się zestaw wskazań, które mają pozwolić wykorzystać unikalne cechy Pokolenia Y, podnieść ich produktywność i zaangażowanie oraz uchronić pracodawcę przed ich frustracją i odejściem.

Zgodnie z nimi należy:

- narzucić strukturę i nadać kierunek – w pewnym sensie przejmując rolę rodzica,
- nieustannie stymulować poprzez nowe wyzwania,
- dawać częsty i szybki *performance feedback*, nie czekając z premiowaniem lub nagradzaniem,
- rozliczać z rezultatów, a nie z trzymania się utartych sposobów i procedur,
- wykorzystywać do komunikacji media elektroniczne (komunikatory, portale, SMS),
- umożliwić wykorzystanie do celów zawodowych ich własnych urządzeń (tabletów, smartfonów),

- polegać na zdolności do pracy zespołowej i wielozadaniowości,
- słuchać, brać pod uwagę ich punkt widzenia i starać się korzystać z ich pomysłów,
- w miarę możliwości zapewnić im wygodę funkcjonowania (np. zezwalając na elastyczne godziny pracy i pracę z domu).

Banki, które chcą przyciągnąć i zagospodarować najbardziej utalentowanych absolwentów i młodych pracowników mają przed sobą szczególne zadanie. Powinny one uwzględnić w swoich strategiach specyfikę Pokolenia Y i zlikwidować rozdźwięk pomiędzy jego oczekiwaniami a dzisiejszym wizerunkiem banku. W szczególności, powinny:

- zaakcentować inwestycje w szkolenia i rozwój pracowników,
- zbudować długoterminowe atrakcyjne ścieżki kariery,
- przekonywująco odbudować wizerunek banku jako instytucji zaufania społecznego opartej na wartościach i etyce.

Środowisko pracy wyzwalające zbiorową energię i kreatywność

Życie społeczne Pokolenia Y odbywa się w Internecie i za pośrednictwem internetu. Tam są gromadzone i publikowane informacje (np. zdjęcia, filmy czy muzyka), tamtędy przesyłane są wiadomości, tam wyraża się opinie i emocje , tam nawiązuje się znajomości i tworzy współdziałające ze sobą grupy. Portal społecznościowy coraz częściej stanowi podstawowy punkt wejścia do kanałów z rozrywką, usług i zakupów w sieci.

Wg badań McKinsey[5], osoby w wieku 18–24 lata wykorzystują urządzenia mobilne przede wszystkim do aktywności na portalu społecznosciowym (wg ilości spędzonego czasu). Komputery używane są w pierwszej kolejności do przeglądania stron internetowych, a już w drugiej do dostępu do portali społecznościowych. Wysyłanie i odbieranie poczty zajmuje osobom w tym wieku zdecydowanie najmniej czasu (mniej niż 10%), przy czym stopień korzystania z poczty elektronicznej wyraźnie maleje z wiekiem respondenta.

W tym świetle tradycyjne środowisko pracy oparte na telefonie, poczcie elektronicznej i przechowywaniu plików na dyskach wydaje się archaiczne i ograniczające. Przekraczając drzwi firmy przedstawiciel Pokolenia Y poczuje się w nim, jak gdyby czas cofnął się o 10 lat.

---

5 McKinsey. *The Young and Digital*.

Pełne zagospodarowanie unikalnych cech przedstawicieli Pokolenia Y będzie możliwe tylko, jeżeli umieści się ich w środowisku, które te cechy ukształtowało, czyli w środowisku firmowej sieci społecznościowej, dostępnej 24 godziny na dobę również przez smartfon i tablet. Dodatkowo, taka sieć powinna wykraczać poza formalne granice firmy, obejmując klientów, dostawców i partnerów.

Rozpiętość wiekowa pracowników firmy typowo obejmuje dwa pokolenia. Obok *Millenials* w organizacjach pracuje przytłaczająca większość, dla której normą komunikowania się są telefon oraz e-mail, a także osoby, które najwyżej cenią sobie napisane na maszynie memorandum opatrzone podpisem i pieczątką, a to może istotnie hamować adopcję i popularyzację nowych narzędzi pracy.

Niektóre firmy podejmują wysiłek przyspieszenia wewnętrznej transformacji kulturowej, aby „wytworzyć przestrzeń" dla nawyków Pokolenia Y oraz usprawnić współpracę i komunikację w zespołach. Atos, wiodąca europejska firma informatyczna, wdraża koncepcję „Zero email™ Company"[6]. Firma jest przekonana, że usunięcie poczty elektronicznej i zastąpienie jej zunifikowaną elektroniczną platformą współpracy obejmującą sieć społecznościową, komunikator i repozytoria plików podniesie produktywność o 20%.

Podsumowanie

Pokolenie Y, obecnie stanowiące silną grupę konsumentów i nabierające znaczenia na rynku pracy, jest pierwszym jednolitym pokoleniem globalnej gospodarki. Zostało ono ukształtowane przez rozczarowanie światem wielkich korporacji, który rozkwitł w latach 90., a następnie uległ serii kryzysów i skandali. *Millenials* to pierwsze pokolenie, które nie zna życia bez komputera i doskonale odnajduje się w świecie internetu. Cechuje je sceptycyzm i brak lojalności wobec instytucji. Ponad wynagrodzenie finansowe ceni sobie możliwość samorealizacji i komfort. Jest ambitne, optymistyczne i narcystyczne. Ma tendencję do polegania na sobie, ale również swobodnie korzysta ze wsparcia rodziców. W relacji z pracodawcą bywa roszczeniowe i kapryśne. Posiada za to niespotykaną umiejętność pracy zespołowej i adaptacji do zmian.

Banki nie są przezeń postrzegane jako preferowane miejsce rozwoju zawodowego. Istnieje bowiem rozdźwięk między dzisiejszym wizerunkiem banków

6 Atos. *Enterprise social collaboration for a better way of working*.

a potrzebami i oczekiwaniami Pokolenia Y (np. potrzebą spójności między wartościami własnymi, a wartościami firmy, potrzebą rozwoju pod kierunkiem mentora czy potrzebą równowagi między życiem osobistym i zawodowym).

Aby pozyskać talent Pokolenia Y i skorzystać z jego unikalnych cech banki muszą dostosować wewnętrzne praktyki, kulturę organizacyjną i wizerunek oraz stworzyć długoterminowe ścieżki karier dla pracowników nowego typu.

Pełniejsze zagospodarowanie kreatywności, otwartości i zbiorowej energii Pokolenia Y dla potrzeb firm i instytucji naszych czasów będzie możliwe dzięki stworzeniu im środowiska pracy podobnego do sieci społecznościowej, ułatwiającego swobodne dzielenie się informacją w dowolnej formie i stałą wymianę komunikatów w maksymalnie dogodny dla nich sposób, tak jak to ma miejsce w sferze prywatnej.

Andrzej Gibas

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

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

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

Andrzej Gibas, Microsoft

Efektywny model bankowości

Bez wątpienia żyjemy w ciekawych czasach, w których stare schematy, reguły i przyzwyczajenia są kwestionowane i wiele z nich bezpowrotnie przemija. Niestabilność rynków finansowych, kolejne fazy kryzysu finansowego, ale przede wszystkim nowe zjawiska społeczne i formy komunikacji definiują naszą dzisiejszą codzienność. Zachodzące przemiany mogą być źródłem nowych możliwości, ale jednocześnie realnym zagrożeniem dla wielu przedsiębiorstw. Bez cienia wątpliwości dotyczy to także banków i innych instytucji finansowych.

Sektor bankowy stanowiący swoisty krwiobieg światowej gospodarki jest szczególnie czuły i reaguje niemal natychmiast na zachodzące w naszym otoczeniu zmiany. Jednocześnie, ze względu na jego umiejscowienie w obiegu gospodarczym, ewentualne błędy w wyborze strategii mogą mieć olbrzymie skutki nie tylko dla samego sektora bankowego, ale na całe gałęzie gospodarki lub wręcz sytuację finansową państw. Stąd nie dziwi fakt, że w tym środowisku stale podejmowana jest dyskusja na temat poszukiwania bardziej efektywnego modelu bankowości. To poszukiwanie powinno uwzględniać wiele opisanych również poniżej zjawisk. W rozważaniach tego artykułu najistotniejsze jednak są pytania dotyczące przyszłej współpracy lub konkurencji banków i innych instytucji finansowych z przedstawicielami innych branż. Wydaje się, że to odpowiedni moment, by odpowiedzieć sobie na istotne pytanie – czy istnieją synergie w zakresie współpracy banków z przedsiębiorstwami reprezentującymi inne sektory? Jeśli tak, to współpraca z jakimi branżami będzie najefektywniejsza? Czy może wręcz przeciwnie – zainteresowanie innych sektorów usługami finansowymi może być źródłem zagrożenia dla banków?

Wyzwania stojące przed sektorem usług finansowych

Zacznijmy jednak od początku i przyjrzyjmy się bliżej wyzwaniom, jakie przed sektorem finansowym stawiają zmiany nawyków i oczekiwań konsumentów. Zastanówmy się, czy współczesny konsument, dla którego Internet jest podstawowym medium komunikacji, nadal potrzebuje tradycyjnych banków czy już tylko bankowości elektronicznej?

„W roku 2011 w USA internet prześcignął pod względem popularności telewizję i gazety, stając się dla młodego pokolenia głównym źródłem informacji" – takim zdaniem Brett King zaczął, wydaną w 2013 roku, książkę „Bank 3.0 Nowy wymiar bankowości"[1]. I to potwierdza, w czym autor swoistej biblii nowoczesnej bankowości upatruje największego wpływu na sektor finansowy w najbliższych czasach. Internet i technologie mobilne bez wątpienia zupełnie zmieniają zachowania konsumentów.

Nowe możliwości i wyzwania dla sektora bankowego wg Microsoft

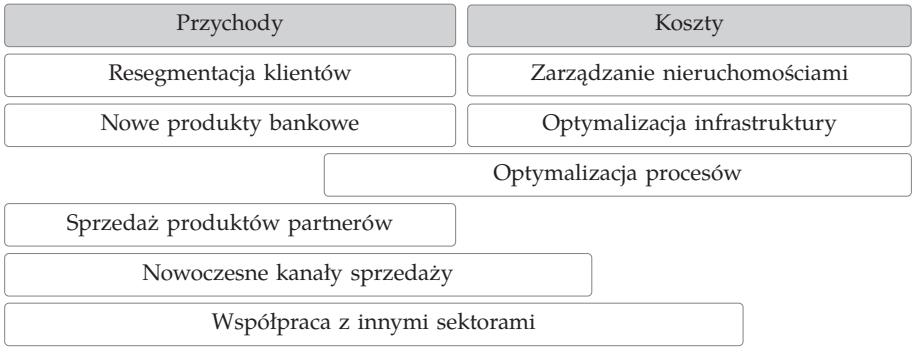
Zjawisko wykorzystania internetu jako podstawowego medium komunikacji ma wielki wpływ na wiele aspektów prowadzenia działalności bankowej i jest wyzwalaczem dyskusji na wiele istotnych tematów. Rozwój kanałów bankowości mobilnej to już codzienność, ale ponieważ niesie za sobą zarówno nowe okazje, jak i zagrożenia dla banków, wciąż pozostaje tematem ożywionej dyskusji branży. Kwestią najbardziej nurtującą środowisko jest jednak rola oddziałów w systemie bankowym. Bo jeśli konsument potrzebuje tylko usług bankowych, ale już niekoniecznie banku, to czy oddziały powinny przyjmować nowoczesne, nafaszerowane technologią formy, czy wręcz przeciwnie –

1 Brett King, *Bank 3.0 Nowy wymiar bankowości*, Studio Emka, czerwiec 2013, str. 20.

nie warto w nie inwestować, gdyż ich znaczenie spadnie w przyszłości? Wydaje się, że konsumenci szukają dzisiaj przede wszystkim lepszego doświadczenia w relacji z sektorem finansowym. Czy jednak oznacza to wizyty w oddziałach, czy raczej pozostawanie w stałym kontakcie z bankiem i pełną obsługę za pośrednictwem mediów elektronicznych? Trendy konsumenckie obserwowane są przez wszystkich uczestników rynku. Dlatego nie powinno dziwić, że przedsiębiorstwa z innych branż, niekojarzonych dotychczas z bankowością lub innymi usługami finansowymi, uświadamiają sobie, iż takie usługi mogą znaleźć się w kręgu ich zainteresowań. Z kolei takie zainteresowanie może być dla banków nową okazją, kiedy będą widziały w nim szansę na współpracę i rozszerzenie swojego zasięgu, lub zagrożeniem, jeśli będą postrzegały je jako działania konkurencyjne.

Efektywny model bankowości – o co chodzi?

Poszczególne branże w różny sposób opisują efektywność swojej działalności. Przykładowo w sektorze energetycznym i telekomunikacyjnym szczególnie istotny jest wskaźnik zysku przed potrąceniem odsetek od zaciągniętych kredytów, podatków oraz amortyzacji (EBITDA), w sektorze telekomunikacyjnym mierzy się wskaźnik średniego przychodu na użytkownika (ARPU), wskaźnik utraty klientów (*churn*), itd. Wskaźniki efektywności typowe dla bankowości to wskaźniki rentowności kapitałów i aktywów – ROA, ROE, a także wskaźniki dotyczące oceny ryzyka. Wydaje się jednak, że wspólnym dla wszystkich branż i jednocześnie jednym z łatwiejszych do analizy jest wskaźnik poziomu kosztów (C/I – *Cost to Income),* analizujący koszty operacyjne do przychodów. Używając takiego wskaźnika można sprowadzić myślenie o dowolnej działalności gospodarczej do uproszczonego modelu, w którym chodzi o to, aby w swojej działalności przy minimalnych kosztach maksymalizować przychody, a co się z tym wiąże – zysk. Rozmaite działania podejmowane przez przedsiębiorstwa mogą wpływać na stronę kosztową lub przychodową ich działalności. Wydaje się, że współpraca z przedsiębiorstwami reprezentującymi inne branże może być przykładem strategii, która może pozytywnie wpływać zarówno na tę pierwszą, jak i drugą.



Przykłady podejmowanych działań i ich oddziaływanie na wskaźnik C/I

Współpraca z innymi sektorami – szansa czy zagrożenie?

Zarówno na światowym, jak i polskim rynku można już znaleźć wiele przykładów współpracy sektora finansowego z innymi branżami.

11 grudnia 2013 roku T-Mobile Polska zawarł strategiczny alians z Alior Bankiem. Według oficjalnego komunikatu główne cele współpracy obu podmiotów to oferowanie obsługi bankowej klientom T-Mobile Polska poprzez zapewnienie im najnowocześniejszych rozwiązań technologii internetowej i mobilnej, bankowości transakcyjnej oraz produktów i usług, które łączyć będą unikalne korzyści wynikające ze współpracy banku i firmy telekomunikacyjnej. T-Mobile zamierza zaproponować abonentom sieci prowadzenie rachunków bankowych, depozytów, kredytów, pożyczek i limitów kredytowych oraz kart płatniczych. Usługi będą dostępne w punktach sprzedaży T-Mobile za pośrednictwem urządzeń mobilnych, serwisów internetowych, Contact Center oraz Wirtualnego Oddziału i oferowane pod marką powiązaną z nazwą operatora.

Tu zatem postawiono na współpracę i szansę na rozwój. Alior Bank zyskuje dostęp do dużej części 16 mln klientów T-Mobile Polska i dodatkowo jeden tysiąc punktów sprzedaży w ramach sieci operatora. Z kolei T-Mobile pozyskuje bogatą paletę produktów, którymi jako operator telekomunikacyjny nie dysponował. Partnerstwo takie oczywiście może mieć także pozytywny wpływ na stronę kosztową. Nie dziwi zatem decyzja Banku o zaprzestaniu rozbudowy sieci własnych placówek Alior Express[2].

2 http://m.forsal.pl/branze/technologie/t-mobile-i-alior-bank-stworza-nowy-projekt-alior-sync-zniknie-z-rynku

Warto zauważyć, że T-Mobile dosyć konsekwentnie realizuje swoją strategię wejścia w świat usług finansowych. Przykładowo w USA uruchomiony został projekt T-Mobile Money Services we współpracy z The Bancorp, określającym siebie jako *„jedną z niewielu firm z branży usług finansowych na świecie, specjalizującą się w dostarczaniu rozwiązań bankowych i technologii w ramach modelu «private label» dla firm «pozabankowych»"*. T-Mobile Money Services proponuje swoim klientom podstawowy rachunek bankowy wraz z przedpłaconą kartą Visa, dostępem do sieci darmowych bankomatów, brakiem opłat miesięcznych, brakiem wymogów dotyczących minimalnego salda czy brakiem overdraftu (i związanych z nim opłat). To daje wyobrażenie o tym, co w przyszłości zaoferuje nowy alians powołany na rynku polskim z Alior Bankiem. Andrew Sherrard, odpowiadający za marketing T-Mobile w USA, powiedział, że *„usługi finansowe w ofercie telekomu mają za zadanie przede wszystkim wzmocnić lojalność klienteli, nie muszą być w krótkim okresie dochodowe"*[3]. Dlatego w ofercie położono nacisk na atut niskich kosztów. Komunikat jest czytelny – „chcesz tanich usług bankowych, przystąp do T-Mobile". Jednak czy przy wyśrubowanych kosztach może pojawić się chęć presji na partnera? Wydaje się, że takiej presji może sprostać dostawca usługi „private label" czy „white label". Czy zatem nie istnieje ryzyko dla Alior Banku, że w przyszłości jego partner będzie chciał go zepchnąć wyłącznie do takiej roli? To niewątpliwie kwestia, która musi zostać wnikliwie przeanalizowana już na etapie budowania strategii partnerstwa.

Kolejną inicjatywę w sektorze telekomunikacyjnym w Polsce obserwujemy obecnie w grupie Zygmunta Solorza, w której w drugim kwartale 2014 roku Plus Bank ma uruchomić nową ofertę, dedykowaną dla dotychczasowych klientów Invest Banku, ale także milionów klientów operatora Plus i Cyfrowego Polsatu.

Inną branżą, z którą od lat już współpracuje sektor bankowy jest branża pocztowa. W Polsce współpracę w tym zakresie realizuje Poczta Polska i Bank Pocztowy. Dla Banku Pocztowego współpraca z Pocztą Polską przynosi korzyści związane przede wszystkim z obniżeniem kosztów dotarcia do klientów i nakładów na rozwój sieci placówek. W ramach współpracy urzędy pocztowe oferują konta osobiste banku, lokaty, kredyty, jednostki funduszy inwestycyjnych PKO BP TFI i PZU TFI. Tym samym Bank Pocztowy dał dostęp

3 Michał Kisiel, „T-Mobile chce być bankiem", 24 stycznia 2014 r., http://prnews.pl/hydepark/t-mobile-chce-byc-bankiem-3045705.html

swoim klientom do największej w kraju sieci punktów (ok. 10 tys. placówek), w których mogą bez prowizji wypłacić gotówkę, a dodatkowo w ponad trzech tysiącach urzędów umieścił terminale do wypłaty gotówki. Poczta Polska próbuje także swoich sił na polu sprzedaży ubezpieczeń. To dzięki tej ofercie klienci Poczty Polskiej będą korzystać z możliwości zakupu ubezpieczenia on-line u listonoszy wyposażonych w nowoczesne urządzenia mobilne. Przedstawione powyżej działania są realizowane wewnątrz Grupy Poczty Polskiej. Jest to de facto transformacja samej Poczty do przedsiębiorstwa lepiej odpowiadającego na wyzwania obecnego świata. Wydaje się, że Poczta Polska dobrze przeanalizowała trendy na rynkach europejskich i zrozumiała, że wejście na rynek usług finansowych jest dla niej wielką szansą. Przykładowo we Włoszech, BancoPosta, bank należący do włoskiego operatora pocztowego Poste Italiane, jest kluczowym kontrybutorem do wyników włoskiej grupy pocztowej. Z kwoty 21,6 mld EUR przychodów włoskiej poczty tylko 4,8 mld EUR pochodzi z usług pocztowych, a reszta to sprzedaż kont, kart, kredytów i ubezpieczeń. W dodatku to usługi finansowe są jedyną dochodową działalnością włoskiej poczty – ma z nich 1,4 mld EUR zysku operacyjnego, gdy z działalności pocztowej generuje 200 mln EUR straty. Ponadto okazuje się, że znacznie łatwiej udaje się zwiększać udział przychodów z działalności finansowej tym pocztom, które mają własne banki niż tym, które żyją z partnerstwa strategicznego z zewnętrznymi bankami komercyjnymi. Przykładowo we Francji udział przychodów z działalności bankowej tamtejszego operatora pocztowego wynosi 24%, a w Wielkiej Brytanii lub Belgii, gdzie poczty udostępniają jedynie zewnętrznym partnerom swoje sieci placówek, to zaledwie 6–8%. Wydaje się zatem, że dla banków komercyjnych Poczta Polska staje się coraz silniejszym, konkurencyjnym graczem oferującym swoim klientom „bankowość bez banku" i de facto tworzy dla nich nowe zagrożenie.

Inne ciekawe inicjatywy w zakresie poszukiwania synergii różnych branż pojawiają się na styku bankowości i sektora paliwowego. Przykładowo w Austrii Erste Bank i Sparkasse podjęły współpracę z paliwowym gigantem OMV. Poza udostępnieniem bankomatów, co dzisiaj jest powszechną praktyką na stacjach benzynowych, zakres współpracy obejmuje oferowanie usług bankowych dostępnych na 170 stacjach paliw OMV ze sklepem VIVA. W przedstawionym powyżej modelu podstawowe korzyści dla banku dotyczą zarówno strony kosztowej – relatywnie taniego zwiększenia swojej sieci, jak i przychodowej – możliwości sprzedaży swoich produktów do klientów sieci stacji paliw.

Kolejną branżą, która wydaje się mieć spore możliwości w zakresie poszukiwania korzyści ze współpracy jest branża energetyczna. Branża ta, podobnie jak sektor telekomunikacyjny, wnosi do aliansu z instytucją finansową dostęp do milionów swoich klientów. Co ciekawe, na świecie obserwuje się mniejszą liczbę projektów realizowanych na styku bank – przedsiębiorstwo energetyczne niż aliansów z przedstawicielami sektora komunikacyjnego. Wydaje się, że telekomy poddane niezwykle silnej presji konkurencji i stale malejąca EBITDA są bardziej zmuszone do poszukiwań nowych pomysłów na biznes i stąd ich otwartość na współpracę z sektorem finansowym. Uwalnianie rynku energetycznego przyczyni się niewątpliwie również do tego, że po stronie firm energetycznych wzrośnie zainteresowanie usługami finansowymi. Również wymogi smart meeteringu i gromadzenie wielkiej liczby danych o konsumentach mogą w przyszłości podwyższyć atrakcyjność tego sektora dla banków.

Ciekawym przykładem współpracy z sektorem energetycznym wydaje się egzotyczny alians Barclays Bank of Botswana i Botswana Power Corporation. Instytucje te zjednoczyły się, aby zaoferować swoim klientom przedpłaconą energię elektryczną. Korzyści dla firmy energetycznej to ułatwienie odsprzedaży energii elektrycznej. Rola Barclays to udostępnienie internetowej platformy bankowej, za pośrednictwem której bank sprzedaje przedpłaconą energię elektryczną. Na razie jeszcze nie pojawiają się sygnały, że polskie banki podejmują bliższą współpracę z sektorem energetycznym. W lukę tę wchodzą inni przedsiębiorcy. Energię elektryczną sprzedają już Ruch SA we współpracy z BillBird SA, właścicielem oraz operatorem sieci VIA™ – Moje Rachunki. Usługa dostępna jest dla klientów TAURON (na terenie Górnego Śląska), Energa SA (woj. pomorskie, część warmińsko-mazurskiego i kujawsko-pomorskiego, część zachodniopomorskiego i wielkopolskiego) oraz PGE O/Łódź (na terenie woj. łódzkiego i mazowieckiego). Z kolei Duon sprzedaje prąd we wszelkich możliwych kanałach dystrybucyjnych, w tym także w internecie, m.in.: Gruper, Groupon, Allegro, w salonach prasowych Inmedio, jak również poprzez dziennik „Super Express".

Synergia wewnątrz sektora – współpraca czy rywalizacja

Innym ciekawym pomysłem i alternatywą dla współpracy z innymi branżami jest poszukiwanie synergii wewnątrz sektora bankowego. Przykładem tego typu inicjatywy jest Skandinavisk Data Center (SDC). SDC to organizacja udostępniająca Centralny System Bankowy dla 125 instytucji finansowych

zlokalizowanych w 4 krajach. Skandynawska inicjatywa to nie tylko przykład współpracy wewnątrz sektora bankowego, ale także skutecznej metody poszukiwania synergii z wykorzystaniem najnowocześniejszej technologii. SDC, obsługując tak wielu klientów, realizuje w praktyce chmurowy model udostępniania usług, na który firmy technologiczne kładą szczególny nacisk w ostatnich latach. Bez wątpienia to właśnie nowe technologie dają możliwości poszukiwania kolejnych synergii instytucji finansowych także z partnerami z branży technologicznej. Jeszcze kilka lat temu koszt inwestycji w nowy projekt był wysoki, a ryzyko duże ze względu na konieczność zakupu wielu elementów infrastruktury. Obecnie można wynająć wiele elementów niezbędnych do realizacji projektu i zrezygnować z nich w razie niepowodzenia. Modele działania Infrastructure as a Service (IaaS), Platform as a Service (PaaS) lub najbardziej zaawansowany Software as a Service (SaaS) pozwalają na zamianę inwestycyjnych nakładów kapitałowych na wydatki operacyjne.

Przedstawione powyżej przykłady to oczywiście wąski wycinek inicjatyw podejmowanych na świecie. Poszukiwanie synergii pomiędzy światem usług finansowych a innymi sektorami nie zawęża się jedynie do branż powyżej omówionych. Od lat znane są projekty realizowane na innych rynkach, np. współpraca z sektorem sprzedaży detalicznej, rynkiem ubezpieczeniowym, liniami lotniczymi, producentami samochodów, itd. Wydaje się jednak, że warta jest dyskusji i refleksji obecna sytuacja sektora bankowego w kontekście poszukiwania synergii z innymi sektorami, zwłaszcza w konfrontacji z nowymi trendami i wyzwaniami. Bez wątpienia przy poszukiwaniu efektywnego modelu bankowego współistnienia z innymi sektorami warto analizować – zarówno pod kątem szans, jakie niesie, jak i potencjalnego ryzyka. Jedno jest pewne: konsumenci i dynamika zmian społecznych nie pozwolą nam stać w miejscu. Konieczne jest poszukiwanie nowych, efektywnych modeli biznesowych i sposobów docierania do konsumenta i zaspokajania jego potrzeb.

Maciej Kaniewski
Współwłaściciel firmy EOS istniejącej od 1992 r.
Świadczy usługi informatyczne dla sektora automotive i finansowego, prowadzi projekty w Polsce i w Niemczech oraz wykłada zarządzanie projektami, m.in. na University of Applied Sciences w Berlinie. Posiada certyfikaty PMP (od 2003 r.), Agile Project Management Foundation i Agile Project Management Registered Practitioner.

Maciej Kaniewski, EOS

Metodyka Agile – blaski i cienie

Metodyki typu Agile, określane często w polskiej literaturze mianem zwinnych, pojawiły się jako odpowiedź na bolączki tradycyjnych metod wytwarzania oprogramowania i zarządzania projektami informatycznymi, w szczególności metod opartych na modelu wodospadowym. Podejście wodospadowe wygląda mniej więcej tak: z początku odbiorca systemu informatycznego opracowuje specyfikację wymagań, być może przy wsparciu analitycznym ze strony zewnętrznych doradców. W następnym kroku inny zespół – zapewne już po stronie dostawcy systemu – opracowuje projekt techniczny, potem kolejny zespół buduje zgodny z tym projektem system informatyczny, który po wykonaniu rygorystycznych testów i usunięciu błędów zostaje wdrożony na produkcję. Przejście od jednego etapu do następnego wymaga „zaliczenia" punktu kontrolnego, obudowanego zazwyczaj rygorystycznymi procedurami, wiążącymi się m.in. z przeglądem opracowanej wcześniej, stosownej dokumentacji.

Model ten sam w sobie jest logiczny i wewnętrznie spójny, jednak to, co znakomicie się sprawdzało w przypadku klasycznych projektów inżynierskich (np. budowlanych czy konstrukcyjnych) okazywało się i nadal okazuje swą słabość w projektach informatycznych. Precyzyjne i ostateczne określenie oraz zakomunikowanie wymagań dla systemu informatycznego od zawsze było obarczone większym błędem niż określenie analogicznych wymagań dla budynku. Wśród częstych przyczyn takiego stanu rzeczy można wymienić brak powszechnie obowiązujących standardów analizy wymagań, dotyczących zarówno procesu analizy, jak i zapisu wyników, niepełny stan wiedzy zespołów

dziedzinowych w początkowych fazach projektu, a także dynamiczny rozwój technologii informatycznej powodujący – zwłaszcza w długoterminowych projektach – nieadekwatność wymagań osadzonych we wcześniejszej rzeczywistości technologicznej.

Konieczność późniejszych uzupełnień i zmian skutkowała tym, że projekty przekraczały terminy i budżet (co jest zresztą nadal nagminne), dostarczenie realnej wartości dla biznesu odbywało się zbyt późno, a zmiany można było uwzględniać tylko pod rygorem kosztownej i skomplikowanej procedury zgłaszania, akceptacji i realizacji. Kierownicy projektu, rozliczani w pierwszym rzędzie z utrzymania harmonogramu i budżetu, z natury rzeczy dążyli do zamknięcia na czas fazy analizy wymagań oraz do minimalizacji zmian w późniejszych fazach projektu.

Rynek wymusza jednak coraz szybszą realizację projektów, gdyż oznacza to szybkie dostarczenie korzyści biznesowych. Pojawia się pytanie, w jaki sposób można zyskać na szybkości nie zwiększając nadmiernie ryzyka projektowego i nie idąc na niepotrzebne kompromisy w obszarze jakości?

Filozofia zwinności

W 2001 roku grupa siedemnastu wybitnych inżynierów oprogramowania opublikowała tzw. *Manifesto for Agile Software Development*.[1] Autorzy manifestu od jakiegoś czasu stosowali już alternatywne metodyki tworzenia oprogramowania, a wielu z nich uczestniczyło w ich tworzeniu.[2] Manifest nie miał na celu przedstawienia konkretnej metody, lecz sformułowanie fundamentalnych zasad, których przestrzeganie pozwoliłoby tworzyć szybko, dobrze i skutecznie. Podstawowe założenie polega na przesunięciu punktu ciężkości projektów w kierunku klienta, uznając nadrzędność jego perspektywy i konieczności nieustannej współpracy z nim. W ujęciu tym przyjmuje się, że klient chce w pierwszym rzędzie otrzymać funkcjonalny system informatyczny, który zaspokoi jego potrzeby biznesowe za przewidywalną cenę i w terminie adekwatnym z biznesowego punktu widzenia. W tym celu jest gotowy działać elastycznie i pragmatycznie, podjąć stosowny wysiłek i ponosić ryzyko związane ze zmianami.

---

1 *The Agile Manifesto*, www.agilemanifesto.org

2 Przykładowo Ken Schwaber, jeden z autorów manifestu, opracował wraz z Jeffem Sutherlandem metodykę SCRUM.

W deklaracji wartości *(value statements)* stanowiącej część manifestu autorzy wyrażają wprost swoją preferencję dla:

- osób i interakcji ponad procesy i narzędzia,
- działającego oprogramowania ponad wyczerpującą dokumentację,
- współpracy z klientem ponad negocjację umowy,
- reagowania na zmiany ponad stosowanie się do planu,

dostrzegając zarazem wartość w elementach znajdujących się po prawej stronie porównania. W tym drugim wypadku trudno zresztą, żeby było inaczej. Najbardziej nawet zwinny projekt musi być realizowany w obrębie konkretnych uwarunkowań, takich jak struktura organizacyjna czy polityki i procedury, a relacje pomiędzy partnerami biznesowymi muszą zostać uregulowane kontraktowo. Nielubiana dokumentacja w końcu też powinna powstać. Wartości po lewej stronie nie są zatem sprzeczne z wartościami po prawej. Co więcej, uporządkowane procesy i dojrzałe narzędzia powinny pomóc w interakcjach na linii klient – dostawca. Oznacza to, że Agile bynajmniej nie stoi w pryncypialnej opozycji do podejścia tradycyjnego. Analogicznie, nacisk na zaspokojenie potrzeb biznesowych i osiągnięcie tym samym zadowolenia klienta nie jest obce podejściom bardziej tradycyjnym (por. utrzymanie ciągłego uzasadnienia biznesowego – *continuous business justification* – w metodyce PRINCE2, podniesione do rangi pierwszej z podstawowych zasad w edycji z 2009 roku[3]).

Koncepcja Agile rozpoczęła swój triumfalny pochód w czasach, kiedy „klasycznym" podejściom do zarządzania projektami, takim jak PRINCE2 czy też metodykom wywodzącym się z PMBOK[4] rzeczywiście można było zarzucić niepotrzebny formalizm. Niekoniecznie wynikał on zresztą z samej metodyki, lecz raczej z nadmiernie rygorystycznej interpretacji jej zaleceń. Obecnie także w podejściach tradycyjnych podkreśla się konieczność dostosowania wszelkiej „biurokracji" do realiów i potrzeb projektu. Przykładowo, jedną z siedmiu wiodących zasad projektów zgodnych z PRINCE2 jest *tailoring*[5], czyli obowiązkowe dostosowanie metodyki do potrzeb projektu i organizacji. Z kolei

---

3 Andy Murray i in., *Managing Successful Projects with PRINCE2*, Office of Government Commerce, The Stationery Office, 2009, str. 27.

4 PMBOK definiuje się jako standard, zatem jako metodykę zarządzania projektami można potraktować konkretny zestaw procesów i procedur opierających się na tym standardzie.

5 Andy Murray i in., *Managing Successful Projects with PRINCE2*, Office of Government Commerce, The Stationery Office, 2009, str. 30.

według PMBOK decyzja dotycząca odpowiedniej metody realizacji projektu leży w gestii kierownika projektu i zespołu, naturalnie z uwzględnieniem uwarunkowań organizacyjnych.[6]

Naturalnie Agile nie oznacza preferencji dla działań *ad hoc* aż do braku metodyki włącznie ani nie jest sprytnym sposobem na zamaskowanie chaosu w zarządzanym projekcie. Wręcz przeciwnie: każde konkretne podejście Agile wymaga szczególnie rygorystycznego przestrzegania zasad. Biorąc pod uwagę konieczność zbudowania efektywnie współpracującego zespołu, często z hierarchiczną kulturą organizacyjną w tle, można uznać Agile za podejście pracochłonne i wymagające szczególnej dyscypliny. Metodyka SCRUM – jedno z najbardziej rozpowszechnionych podejść Agile – określana jest wprost mianem „zarządzania o wysokiej intensywności".[7] Jak podkreślają wszystkie podręczniki metodyk Agile, wybiórcze stosowanie elementów metodyki ma negatywny wpływ na sukces projektu.[8]

Podejście zwinne nie neguje także konieczności tworzenia systemu informatycznego zgodnie z zasadami sztuki. Dostawca musi dysponować procesem zapewniającym jakość tworzonego oprogramowania, obejmującą m.in. spójność tworzonego systemu, jednolitość standardu kodowania, uwzględnienie aspektów niefunkcjonalnych (odpowiedniej obsługi błędów, bezpieczeństwa, itp.) i inne aspekty zgodne z zasadami sztuki. Z drugiej strony, klient powinien zapewnić jakość „wygenerowanych" wymagań, a także spójność i kompletność scenariuszy testowych. Odbiór tworzonego systemu pozostaje zagadnieniem dla obu stron kluczowym: po stronie klienta gwarantuje uzyskanie systemu spełniającego jego potrzeby biznesowe, po stronie dostawcy gwarantuje uzyskanie płatności.

Reasumując, stosując podejście zwinne nadal musimy dysponować kryteriami określającymi, czy praca została wykonana i czy produkt projektu został wykonany dobrze. Kryterium jego akceptacji powinno być ustalone a priori, niezależnie od poziomu formalizacji. Metodyka SCRUM posługuje się

---

6 *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Fifth Edition*, Project Management Institute, Inc., Newtown Square, 2013, str. 35: *Within those constraints* (tzn. ramowych zasad project governance – przyp. M.K.), *as well as the additional limitations of time and budget, it is up to the project manager and the project team to determine the most appropriate method of carrying out the project*.

7 K. H. Pries, J. M. Quigley, *Scrum Project Management*, CRC Press, Boca Raton, 2011.

8 Przykładowo, rozluźnienie rygoru dotyczącego czasu trwania pojedynczych przebiegów (sprintów, timeboksów, itp.) powoduje, że zamiast jednej zmiennej – zakres projektu – mamy dwie: zakres i czas.

pojęciem *definition of „done"*, tzn. definicji kryteriów określających, że zadanie zostało zrealizowane. Taka definicja musi zostać w ramach projektu precyzyjnie sformułowana.

Pojawia się pytanie, w jaki sposób można skonstruować kontrakt dla projektu typu Agile. Pomijając hipotetyczny przypadek braku ograniczeń budżetowych i czasowych, w umowie musimy nadal określić budżet i harmonogram. Uwzględniając wymiary ograniczeń projektowych (czas, zakres, koszty i jakość) oznacza to takie zarządzanie projektem, aby dopuszczając zmiany zakresu zmieścić się w kosztach i budżecie przy żądanym poziomie jakości.

Agile jako sposób... na co?

Główne korzyści z podejścia Agile biorą się z usprawnienia komunikacji – podejmowania decyzji nie spowalniają bowiem formalne, proceduralne ograniczenia (np. konieczność zarejestrowania i „przeprocesowania" żądań zmian) – oraz z pozytywnego podejścia do zmian.

Wybór podejścia Agile można najlepiej uzasadnić w przypadku projektów, w których występuje jeden lub kilka z następujących czynników:

- projekt toczy się w nowym obszarze biznesowym, wymagającym eksploracji, charakteryzującym się wysokim poziomem niepewności i niewystarczającą wiedzą na początku projektu, skutkującą trudnością w zdefiniowaniu wymagań,
- kluczowym elementem projektu jest budowa systemu informatycznego opartego na silnej interakcji z użytkownikiem (co powoduje szczególną istotność wymagań użytkowych), lecz powiązanego z innymi systemami w stopniu umiarkowanym,
- projekt znajduje się pod dużą presją czasu, spowodowaną koniecznością szybkiego dostarczenia i wdrożenia jego produktów,
- częste zmiany w trakcie projektu są prawdopodobne i oczekiwane,
- istnieje realna możliwość ścisłej współpracy pomiędzy zespołem dostawcy i klienta, np. z wykorzystaniem kolokacji.

Trudnościom w definiowaniu wymagań warto zresztą poświęcić nieco więcej uwagi. Typowe problemy, z którymi autor stykał się w swoich projektach, można pogrupować następująco:

- dotarcie do wszystkich źródeł wymagań, w szczególności uwzględnienie wszystkich interesariuszy, co wiąże się często z trudnością w prawidłowym

zamodelowaniu procesów biznesowych, które mają być wspomagane przez system informatyczny – zwłaszcza w sytuacji, gdy proces jest nowy i nie do końca zbadany,
- niski poziom wiedzy, którą trzeba pogłębiać w trakcie pracy nad wymaganiami, często przy wykorzystaniu zewnętrznych ekspertów,
- przekroczenie czasu wynikające z konieczności pogłębionej analizy wymagań,
- ryzyko formułowania wymagań zbyt abstrakcyjnych, oderwanych od procesu biznesowego, lub przeciwnie – zbyt szczegółowych, niejawnie zakładających już określone rozwiązania technologiczne,
- sprzeczne wymagania formułowane przez różne grupy użytkowników lub interesariuszy, nierzadko wynikające z odmiennych celów lub interesów,
- trudność w zidentyfikowaniu takiej formy zapisu wymagań, która zapewni ich zrozumiałość i kompletność, a zarazem, nie ograniczając procesu pozyskiwania wiedzy, ułatwi jej systematyzację.

W tych wszystkich przypadkach pomaga usprawnienie komunikacji i uruchomienie skutecznej pracy zespołowej w ścisłym powiązaniu klienta i dostawcy, dlatego sytuacje te stanowią szczególne pole popisu dla podejścia zwinnego.

Z praktycznego punktu widzenia można także rozważyć zastosowanie Agile do części projektu lub też do określonych pakietów prac, zarządzając całym projektem w sposób tradycyjny. Przykładowo, projektem biznesowym – np. założeniem nowego przedsiębiorstwa – można zarządzać zgodnie z jedną z metod tradycyjnych, wykorzystując jednak Agile do budowy systemu informatycznego.

Wdrożenie Agile w przedsiębiorstwie

Zarówno klasyczne, jak i zwinne metodyki zarządzania projektami poruszają się w ramach realiów organizacyjnych, zarządczych i technologicznych przedsiębiorstwa. Pojawiło się w związku z tym szereg koncepcji mających na celu uplasowanie podejścia Agile w kontekście dojrzałej, stabilnej organizacji, np. podejście *Disciplined Agile Delivery*[9] opracowane w IBM oraz DSDM[10]

9 S.W. Ambler, M. Lines, *Disciplined Agile Delivery – A Practitioner's Guide to Agile Software Delivery in the Enterprise*, IBM Press Pearson plc, Boston, 2013.

10 A. Craddock i in., *Agile Project Management Handbook*, DSDM Consortium, Kent, 2012.

Agile Project Management opracowane przez brytyjską organizację DSDM[11] Consortium i stanowiącej element całościowego podejścia DSDM Atern.

W ramach niniejszego artykułu odniesiemy się do drugiego z tych podejść, czyli DSDM Agile Project Management. Punktem wyjścia metodyki są dwa założenia:

- projekty częściej ponoszą porażkę z przyczyn ludzkich niż technologicznych,
- nic nie powstaje za pierwszym razem w formie doskonałej.

W związku z tym DSDM stawia sobie za priorytet umożliwienie efektywnej współpracy, podobnie zresztą jak inne podejścia zwinne. Ponieważ przyjęto rozsądne założenie, że jakość nie może podlegać dyskusji, a czas i koszty są sztywne, jedyną zmienną niezależną pozostaje w związku z tym zakres projektu. Dlatego podstawowe narzędzie tej metodyki związane jest z zarządzaniem zakresem – jest to spriorytetyzowana lista wymagań *(prioritized requirements list)*. Wymagania zapisane na niej są opatrzone priorytetami zgodnie z zasadą MoSCoW: niezbędne *(must have)*, pożądane *(should have)*, opcjonalne *(could have)* i świadomie pominięte *(won't have)*. Optymalna mieszanka wymagań powinna składać się z nie więcej niż ok. 60% wymagań niezbędnych.[12] Dostawca zobowiązuje się do realizacji wszystkich wymagań typu *must* i *should*. Realizacja wymagań typu *could* nie jest gwarantowana, natomiast może zostać osiągnięta przy sprzyjającym przebiegu projektu.

U podstaw podejścia DSDM leży osiem zasad:

- skupienie na potrzebie biznesowej: zrozumienie prawdziwych priorytetów, ustanowienie zdrowego uzasadnienia biznesowego *(business case)*, zapewnienie ciągłego zaangażowania biznesu i zagwarantowanie dostarczenia minimalnego, zdatnego do użycia podzbioru wymagań *(minimum usable subset)*,
- dostarczanie produktów na czas – organizacja pracy w stałych odcinkach czasowych *(timeboxes)*, skupienie na priorytetach nadanych przez biznes i przestrzeganie terminów,
- współpraca: zaangażowanie odpowiednich interesariuszy we właściwym czasie, zapewnienie, aby członkowie zespołów byli uprawomocnieni do podejmowania decyzji w imieniu reprezentowanych przez siebie osób lub

11 Skrót od Dynamic System Development Method.

12 Procentowy udział dotyczy przewidywanego wysiłku niezbędnego do zrealizowania wymagań.

grup, aktywne zaangażowanie przedstawicieli strony biznesowej oraz budowa kultury wspólnego zespołu *(one-team culture),*

- bezkompromisowa jakość: zdefiniowanie żądanego jej poziomu od początku, zapewnienie, że nie stanie się ona zmienną projektu, odpowiednie projektowanie, dokumentowanie i testowanie, wbudowanie jakości poprzez ciągłe przeglądy, wczesne i ciągłe testowanie rozwiązania,
- inkrementalna budowa rozwiązania na solidnych podstawach: dążenie do wczesnego dostarczenia korzyści biznesowych wszędzie tam, gdzie jest to możliwe, ciągłe potwierdzanie, że budowane jest właściwe rozwiązanie, formalna, ponawiana ocena priorytetów i dalszego uzasadnienia biznesowego dla projektu po każdym inkremencie,
- praca iteracyjna: prace projektowe na początku powinny być wystarczające, aby zapewnić solidny fundament, iteracyjne podejście do budowy wszystkich produktów, informacje zwrotne od klienta w każdej iteracji, przyjęcie do wiadomości, że szczegóły będą się pojawiać później (a nie wcześniej), pozytywne podejście do zmiany, kreatywność, eksperymentowanie, nauka i rozwój,
- ciągła i przejrzysta komunikacja: codzienne spotkania zespołu na stojąco, warsztaty wspomagane *(facilitated workshops)*, techniki wzbogaconej komunikacji (np. modelowanie i prototypowanie), wczesne i częste przedstawianie kolejnych instancji tworzonego rozwiązania, zwięzła i cały czas aktualna dokumentacja, zarządzanie wymaganiami interesariuszy przez cały czas trwania projektu, zachęcanie do nieformalnej, bezpośredniej komunikacji na wszystkich poziomach,
- demonstrowanie kontroli: wykorzystanie odpowiedniego poziomu sformalizowania do celów śledzenia i raportowania, plany i postęp prac widoczne dla wszystkich, pomiar postępu prac poprzez skupienie na dostarczeniu produktów (a nie na zakończeniu czynności), zarządzanie proaktywne, analiza dalszego uzasadnienia dla projektu na podstawie celów biznesowych.

Zarządzanie projektami według DSDM wykorzystuje pięć podstawowych praktyk:

- warsztaty wspomagane *(faciliated workshops),*
- ustalanie priorytetów według zasady MoSCoW *(MoSCoW prioritization),*
- iteracyjne podejście do budowy produktów *(iterative development),*
- modelowanie *(modelling),*
- praca w stałych odcinkach czasu *(timeboxing).*

Dojście do spriorytetyzowanej listy wymagań, o wdzięcznym skrócie PRL, odbywa się w kilku etapach. Na etapie przedprojektowym *(pre-project)* zostaje zidentyfikowany cel biznesowy projektu. Jeżeli projekt jest dobrze uzasadniony, następuje przejście do etapu analizy wykonalności *(feasibility)*, w ramach którego następuje sprawdzenie, czy istnieje pomysł na rozwiązanie sformułowanego wcześniej celu biznesowego. Jeśli tak jest, istotne cechy rozwiązania zostają naszkicowane i przeanalizowane, m.in. pod kątem ryzyka, a rozwiązanie biznesowe zostaje dopracowane.

W wyniku kolejnego etapu tworzenia podwalin *(foundation)* powstaje zarówno lista wymagań, jak i bardziej szczegółowe plany. Na tym etapie definiuje się „szerokość" wymagań, czyli opisuje zakres funkcjonalny rozwiązania na poziomie dość ogólnym, np. w odniesieniu do wspieranych przez system procesów biznesowych. Pula wymagań do zrealizowania rozdzielana jest pomiędzy inkrementy, tzn. etapy projektu skutkujące dostarczeniem kolejnych, wdrażalnych wersji działającego produktu *(deployments)*. Wymagania do zrealizowania w ciągu inkrementu są analizowane i rozdzielane na sekwencję krótkich (np. tygodniowych) jednostek czasowych o równej długości, zwanych *timeboxes*. Timebox może służyć dogłębnemu zbadaniu i zdekomponowaniu wymagań (jest to wówczas tzw. *exploration timebox)*, wytwarzaniu produktu na bazie wymagań (tzw. *engineering timebox)*, a może także stanowić połączenie obu tych obszarów. Tutaj wchodzi się w wymiar „głębokości" wymagań, tzn. formułuje szczegółowe wytyczne dla systemu. Szerokość wymagań powinna pozostać stała w czasie projektu, natomiast zmiany będą się pojawiać podczas analizy głębokości wymagań.

Każdy timebox rozpoczyna się spotkaniem inicjującym *(kickoff)*, po którym następują fazy: badania problemu *(investigation)*, doskonalenia rozwiązania *(refinement)* i konsolidacji *(consolidation)*, a następnie zakończenia *(closeout)*. Podczas tej ostatniej fazy następuje ocena wykonanych prac i podjęcie decyzji dotyczących tych prac, których wykonać się nie dało. Decyzją może być nie tylko przeniesienie prac do następnych timeboksów, ale także całkowite usunięcie prac z danego inkrementu.

Planowanie projektu zarządzanego w duchu DSDM odbywa się na kilku poziomach, którym towarzyszą różne poziomy szczegółowości w definicji wymagań. Utworzenie planu inkrementów i rozdzielenie wymagań pomiędzy nie posługuje się wymaganiami na poziomie listy PRL. Rozdział inkrementów na timeboxy wymaga bardziej szczegółowej analizy wymagań. Najbardziej szczegółowa analiza wymagań powstaje na poziomie planowania timeboksu.

Planowanie release'ów (wydań systemu) odbywa się w sposób „klasyczny", natomiast priorytetyzacja wymagań i dochodzenie do ostatecznej wersji systemu – w sposób zwinny. Jest to odzwierciedlenie znanej z innych podejść zasady planowania kroczącego.

Już z tego krótkiego opisu można wywnioskować, że metodykę *DSDM Agile Project Management* trudno określić jako prostą, a jej stosowanie wymaga nie lada dyscypliny. Jej zaletą jest jednak zarówno porządek w planowaniu projektu, jak i gwarancja powstania odpowiedniej dokumentacji. Metodykę można zatem dostosować do wymogów polityk korporacyjnych.

Tworzenie kultury Agile

Podstawową „sztuczką" podejścia Agile jest budowa zespołu składającego się z przedstawicieli dostawcy i z przedstawicieli klienta, opartego na pełnym przepływie informacji i wzajemnym zaufania. Częstym problemem zespołów mieszanych jest oczekiwanie od dostawcy, że przejmie na siebie identyfikację i analizę wymagań w miejsce klienta. Jednak to nie będzie działać, ponieważ perspektywa dostawcy jest zasadniczo inna od perspektywy klienta, gdyż dąży on zazwyczaj do tego, aby wdrożyć system za określoną cenę przy minimalnej liczbie funkcjonalnych dostosowań. Dlatego też nieodzowne jest precyzyjne zdefiniowanie ról przede wszystkim po stronie klienta. Role właściciela biznesowego i analityka biznesowego są w tym kontekście kluczowe.

Podstawowe czynniki umożliwiające zastosowanie Agile to kultura oparta na zaufaniu, określone metody bezpośredniej komunikacji (np. spotkania *stand-up*) oraz praca zespołowa, zakładająca integrację zespołu biznesowego po stronie klienta z zespołem po stronie dostawcy. Kolejnym istotnym założeniem jest także samoorganizacja zespołu, który będzie razem poszukiwał rozwiązań. Taki zespół musi składać się ze zmotywowanych osób. W tym kontekście przeszkadzać we wdrożeniu podejścia Agile może myślenie silosowe, tak często spotykane w firmach o bardziej skomplikowanej strukturze organizacyjnej, a także autorytarny model zarządzania.

Tymczasem nowoczesne zarządzanie stanowi dwustronny proces pomiędzy prowadzącym i prowadzonym, opierający się na podstawie wzajemnego zaufania.[13] Przełożony jest przede wszystkim wewnętrznym usługodawcą, który wspiera i promuje swoich współpracowników. Dlatego też powinien –

13 T. Daigeler i in., *Führungstechniken*, Haufe-Lexware GmbH und Co. KG, Freiburg, 2012.

działając w pewnej mierze jako ich coach – unikać dostarczania współpracownikom prostych odpowiedzi, jeśli tylko sytuacja na to pozwala. Powinien ich raczej zachęcać do przejęcia odpowiedzialności za sytuację i samodzielnego przeanalizowania problemu – w ten sposób przełożony stwarza im możliwość, aby sami szukali rozwiązań. Takie podejście wspiera kulturę Agile.

Kultura organizacyjna przedsiębiorstwa stanowi wypadkową wielu czynników, wśród których istotną rolę odgrywają tendencje kulturowe dominujące w danym kraju. Podejście Agile powstało w środowisku amerykańskim i brytyjskim. Odniesienia do warunków polskich mogą dostarczyć badania Geerta Hofstede[14], który opracował model sześciu wymiarów kultury i przeanalizował wyniki w wielu krajach świata. W wymiarze dystansu Polska ma stosunkowo wysoki wynik 68. Oznacza to, że przeciętny Polak akceptuje porządek hierarchiczny, w którym każdy ma swoje miejsce i który nie wymaga dalszego uzasadnienia. Hierarchia w organizacji jest postrzegana jako odzwierciedlenie wbudowanych nierówności, popularna jest centralizacja, pracownicy oczekują, że im się powie, co mają robić, a idealny szef jest dobrotliwym autokratą. Dla porównania, Stany Zjednoczone na tej samej skali uzyskały wynik 35, a Niemcy 40, co oznacza o wiele mniejszy dystans władzy, a co za tym idzie – mniejsze przywiązanie do hierarchii. Jednocześnie Polacy są społeczeństwem indywidualistycznym (wynik 60), choć w trochę mniejszym stopniu, niż Niemcy (67) i znacznie mniejszym niż Stany Zjednoczone (91). Istnieje tu pewna sprzeczność pomiędzy poczuciem hierarchii a indywidualizmem. Menedżer może ją rozwiązać poprzez bezpośredni kontakt ze wszystkimi osobami w strukturze, przekazując informację, że każda osoba jest równie ważna, nawet jeśli zajmuje niskie miejsce w hierarchii.

Zaskakiwać może wysoka wartość wskaźnika unikania niepewności (93) w porównaniu z Niemcami (65) i USA (46). Odmiennie, niż wskazywałby na to stereotyp ułańskiej fantazji Polaków i ich zdolności do improwizacji, Polacy mają według tej oceny silną potrzebę norm i reguł (nawet, jeśli te ostatnie niezbyt działają), niechętnie widzą zachowania odbiegające od normy, a bezpieczeństwo stanowi jeden z najważniejszych osobistych motywatorów. Dlatego zachęta do przekraczania reguł poprzez spontaniczne, kreatywne działania musi być explicite wyartykułowana przez kierownictwo.

Ujęte w tym modelu różnice kulturowe pomiędzy Polską a Stanami Zjednoczonymi – ojczyzną podejścia Agile – są zauważalne. Można by zatem

14 The Hofstede Centre, http://www.hofstede.com

oczekiwać, że wdrożenie podejścia zakorzenionego w amerykańskiej kulturze biznesowej będzie wymagało szczególnego wsparcia i zachęty ze strony przełożonych. Autor wymieniłby tutaj następujące obszary:

- budowanie kultury opartej na otwartej, bezpośredniej komunikacji niezależnie od poziomów hierarchii,
- nagradzanie postaw kontestujących aktualny porządek z intencją usprawnień (np. w duchu *kaizen*),
- powoływanie zespołów zadaniowych odpowiedzialnych za autonomiczne rozwiązywanie zagadnień, przy czym rola przełożonych sprowadzałaby się do wsparcia,
- ustanowienie systemu motywacji powiązanego z wynikami pracy zespołowej,
- niezależne doradztwo w trakcie projektu, pozwalające rozpoznać sytuacje niekorzystne z punktu widzenia wymagań decyzyjnych i komunikacyjnych podejścia Agile.

Podsumowując należy podkreślić, że podejścia zwinne już w ubiegłej dekadzie przeszły z kategorii nowości do żelaznego repertuaru kierowników projektów i zespołów wytwórczych. Dostarczają istotnych korzyści pod względem jakości komunikacji, szybkości tworzenia sensownych rozwiązań informatycznych i usprawnienia procesów decyzyjnych, stanowiąc zarazem wyzwanie zarówno dla kierowników projektów, jak i zespołów. Skuteczne wdrożenie podejścia typu Agile wymaga gruntownego rozpoznania własnej kultury organizacyjnej, usunięcia przeszkód i przestrzegania założeń metodycznych, co zakłada ścisłe zaangażowanie kierownictwa.

Aleksander P. Czarnowski
Prezes AVET Information and Network Security sp. z o.o., spółki zajmującej się od 17 lat konsultingiem w zakresie bezpieczeństwa informacji w Polsce, Rumunii, Holandii i Wielkiej Brytanii oraz na Ukrainie i Słowacji.
Członek Komisji Technicznej 182, która w Polskim Komitecie Normalizacyjnym odpowiada za rodzinę standardów ISO 27000, a także rady programowej Zakładu Systemów Jakości i Zarządzania działającego w ramach Wojskowej Akademii Technicznej. Od 2013 r. ekspert w grupie eksperckiej odpowiedzialnej za kontraktowanie usług cloud computing 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

Obecne zagrożenia w bankowych systemach IT

W dobie gdy wszyscy myślą o aplikacjach mobilnych i każdy bank rozbudowuje swoją ofertę w tym zakresie, warto jest pamiętać o tym, że każdy kanał bankowości elektronicznej wymaga adekwatnego zabezpieczenia. Nie jest to proste zadanie biorąc pod uwagę równie dynamiczny rozwój nowych technologii IT co metod ataku. Coraz większe wymagania względem czasu dostarczania nowych rozwiązań z pewnością nie ułatwiają sytuacji.

Rekomendacja D: stara i nowa rzeczywistość

Wprowadzenie nowej rekomendacji D z pewnością przyczyniło się do wielu pytań o to, czy obecny sposób zarządzania bezpieczeństwem IT w banku jest poprawny. Niewątpliwie dobrą wiadomością jest większe otwarcie się na usługi outsourcingowe – coś co w USA i Europie Zachodniej stało się w bankowości już dawno. Po raz pierwszy pojawiło się także pojęcie *cloud computingu* wraz z jego definicją. Biorąc pod uwagę, że obecnie każdy poważny gracz na rynku usług dla sektora bankowego buduje jak najszerszą ofertę z wykorzystaniem pojęcia *cloud computing* (umyślnie nie korzystam z polskiego tłumaczenia „chmura obliczeniowa", bo czyż usługi polegające na oferowaniu storage'u są oparte przede wszystkim o moc obliczeniową?). Definicja znajdująca się w rekomendacji D umożliwi więc stwierdzenie, czy dana oferta w myśl nowych wymagań faktycznie jest chmurą a, co za tym idzie, jakie wymogi z perspektywy bezpieczeństwa musi ona spełniać. To co, niestety, w mojej ocenie zostało pominięte to podział na chmury prywatne i publiczne. Czytając rekomendację D wydaje się, że autorom chodziło przede wszystkim o chmury publiczne oferowane przez zewnętrznych dostawców. Tymczasem w bankach istnieją

już projekty prywatnych chmur oferowanych w ramach grupy kapitałowej. Czasami za ich utrzymanie odpowiadają, co prawda, zewnętrzne spółki, ale będące w 100 procentach własnością banku. O ile z perspektywy prawnej jest to zewnętrzny podmiot, o tyle z perspektywy chmury już niekoniecznie. Ma to, oczywiście, wpływ na ocenę ryzyka i sposób zarządzania nim. Wracając jednak do braku podziału na chmury prywatne i publiczne, panuje mylne przeświadczenie o tym, że chmury prywatne są bezpieczne (a przynajmniej bezpieczniejsze od publicznych), bo przecież znajdują się „w środku" organizacji. Konsekwencją tego jest pełna kontrola nad miejscem przetwarzania danych i sposobem ich zabezpieczenia oraz ograniczenie liczby osób mających dostęp do zarówno infrastruktury, aplikacji, jak i danych. Niestety, taki sposób myślenia jest błędny i prowadzi do braku adekwatnych zabezpieczeń, co opisuję w punkcie „Bezpieczeństwo chmury z perspektywy banku".

Niewątpliwie krótkie okno czasowe, jakie dostały banki na dostosowanie się do nowej rekomendacji D stanowi istotny problem zarówno dla banku, jak i jego dostawców IT. Wielu systemów nie da się bowiem dostosować i wdrożyć ich aktualnej wersji na czas.

PCI DSS

Historia tego standardu potwierdza po raz kolejny stawianą wcześniej tezę, że na skutek dynamiki zmian w technologiach IT, a w konsekwencji w systemach bankowych, standardy mają problem z adekwatnym adresowaniem zarówno zagrożeń, jak i zabezpieczeń. Dwa kardynalne przykłady z jego przeszłości to:

- kwestia dopuszczenia używania sieci WiFi,
- wymóg praktycznie galwanicznej separacji od siebie poszczególnych komponentów systemów w dobie rozpowszechnionej wirtualizacji.

Oczywiście, po pewnym czasie wymogi PCI DSS są aktualizowane i część problemów zostaje zaadresowana. W międzyczasie pojawiają się jednak nowe zagrożenia oraz nowa funkcjonalność zabezpieczeń. Efektem ubocznym jest ciągła pogoń za zgodnością z wymogami. Niestety, może to skutkować – w ekstremalnym przypadku – zbudowaniem systemu zgodnego z wymogami nawet wielu standardów i rekomendacji naraz, który nadal nie będzie bezpiecznym z technologicznego punktu widzenia.

ISO 27001

O ile rekomendacja D czy PCI DSS to przykłady standardów i regulacji z sektora finansowego, o tyle ISO 27001, wywodzące się z brytyjskiego standardu BS 7799, którego korzenie sięgają armii, jest zbiorem najlepszych praktyk w zakresie zarządzania bezpieczeństwem, skierowanym w swoim zamyśle do jak najszerszego grona odbiorców. Nie przeszkodziło to jednak sektorowi bankowemu adaptować go na skalę globalną na swoje potrzeby. Może dlatego, że standard ten jest zbiorem najlepszych praktyk w zakresie zarządzania bezpieczeństwem informacji w ujęciu systemowym, chociaż to od wdrażającego i stosującego go zależy, z których praktyk i w jakim zakresie będzie korzystał. Zapewne ta elastyczność, w połączeniu z wykorzystaniem podejścia opartego o zarządzanie ryzykiem, skłoniła instytucje finansowe, w tym banki, do tak szerokiego jego stosowania.

W 2013 roku pojawiła się nowa wersja standardu ISO 27001:2013, która zmieniła w istotny sposób tzw. Deklarację Stosowania (SOA – *Statement Of Applicability*) względem wersji z 2007 roku. O ile u jej podstaw nadal leży podejście procesowe i zarządzanie ryzykiem wraz z elastycznością w doborze stosowanych zabezpieczeń, zmieniło się poważnie nazewnictwo. Silna ewolucja objęła także obszary związane z urządzeniami mobilnymi. Zmiany takie wystarczyły, aby wiele organizacji pozostało jeszcze przynajmniej na jakiś czas przy wersji z 2007 roku. Niewątpliwie aktualizacja do ISO 27001:2013 jest dobrym pomysłem podczas aktualizacji procedur wymuszonych przez rekomendację D.

Bezpieczeństwo chmury z perspektywy banku

Poziom bezpieczeństwa usług oferowanych w ramach cloud computingu ma krytyczne znaczenie dla banku decydującego się korzystać z takiego rozwiązania. W tym miejscu należy zaznaczyć, że o ile dzisiaj możliwa jest jeszcze decyzja o niekorzystaniu z rozwiązań mających w nazwie „chmura", to w przyszłości może się to okazać niemożliwe na skutek zmian rynkowych, jakie obecnie zachodzą.

Niewątpliwie – powtarzając za rekomendacją D – z perspektywy banku istotne jest monitorowanie chmury oraz jakości i dostępności usług w niej oferowanych. W końcu jedną z podstawowych zalet chmury ma być jej wysoka dostępność i niezawodność oraz skalowalność na żądanie. W praktyce

wielu dostawców nadal nie udostępnia jednak wystarczających mechanizmów monitorowania. Nakłada to na bank albo wymuszenie ich na dostawcy albo implementację ich we własnym zakresie po swojej stronie.

Ponieważ w dużych chmurach publicznych zazwyczaj przetwarzanie danych jest odmiejscowione, zbieranie danych w ramach procesu *forensic analysis* może być niezwykle trudne zarówno w sferze technologicznej, jak i prawnej.

Należy także pamiętać, że wiele współczesnych zabezpieczeń technicznych pasuje do bardziej tradycyjnych rozwiązań. To, że w nazwie danego produktu mającego zapewnić bezpieczeństwo występuje wyraz „chmura" lub „*cloud*" nie oznacza, że tak naprawdę jest przystosowany do pracy w takim modelu.

Bankowość mobilna

Dzisiaj bankowość mobilna to najważniejszy kanał dostępowy z perspektywy rozwoju. Pojawienie się smartfonów oraz tabletów zmieniło kompletnie postrzeganie tych urządzeń na skutek bardzo szybkiej ich akceptacji przez rynek konsumencki. Z perspektywy bezpieczeństwa rodzi to jednak wiele zagrożeń.

Po pierwsze, żadne z tych urządzeń nie było projektowane pod kątem bezpieczeństwa, czego efektem jest to, że ich bezpieczeństwo fizyczne może pozostawiać wiele do życzenia. Ponieważ urządzenia te nadal mają ograniczone zasoby w porównaniu z notebookami, to projektanci systemów operacyjnych dla rozwiązań mobilnych musieli z czegoś zrezygnować i najczęściej były to funkcjonalności zabezpieczeń. Nie ma się zresztą czemu dziwić, gdyż konsumenci nie kupują tych urządzeń akurat z powodu poziomu bezpieczeństwa. Kolejnym problemem w przypadku zabezpieczeń jest fakt, że zarówno kontrola operacji, jak i wszystkie operacje kryptograficzne są kosztowne z perspektywy procesora. W przypadku urządzeń mobilnych oznacza to, że są niekoniecznie optymalne z perspektywy zużycia energii, a to przecież jest niezwykle istotne. I znów z perspektywy konsumenta łatwiej jest zaakceptować brak zabezpieczeń niż na przykład wolniejsze przetwarzanie grafiki.

Kolejnym problemem jest model dystrybucji aplikacji na urządzeniach mobilnych. Dwie dominujące platformy systemowe – Android i iOS – posiadają własne AppStory, które istotnie różnią się poziomem bezpieczeństwa. Oznacza to, że potencjalnemu atakującemu może być łatwiej zaatakować tylko jedną platformę.

Należy też pamiętać, że bezpieczeństwo w przypadku modelu dystrybucji aplikacji poprzez rozwiązania typu AppStore jest przede wszystkim postrze-

gane z perspektywy jego właściciela. Zaimplementowane zabezpieczenia mają zapewnić stały przychód i kontrolę nad użytkownikami oraz developerami właścicielowi sklepu. Bezpieczeństwo konsumenta nie jest tutaj w dłuższej perspektywie w ogóle brane pod uwagę. Dowodem na to są niezwykle wysokie uprawnienia, jakich żądają dopuszczone do dystrybucji instalowane aplikacje. Oczywiście, proces dopuszczania aplikacji do rozpowszechniania w danym sklepie i sposób podpisywania aplikacji mają krytyczny wpływ na to, czy dana platforma może zostać łatwo zaatakowana.

Pojawia się tutaj pierwsze bardzo poważne zagrożenie z perspektywy banku – nie ma on żadnej kontroli nad tym, jakie inne aplikacje (oraz z jakimi uprawnieniami) są instalowane na urządzeniach mobilnych (świadomie lub nie) przez klientów banku. Oczywiście, problem ten jest już znany od dawna w przypadku komputerów klientów, jednak urządzenia mobilne mają coraz częściej większy dostęp do danych poufnych użytkownika niż komputery stacjonarne.

Proces zabezpieczania aplikacji mobilnych przez developera

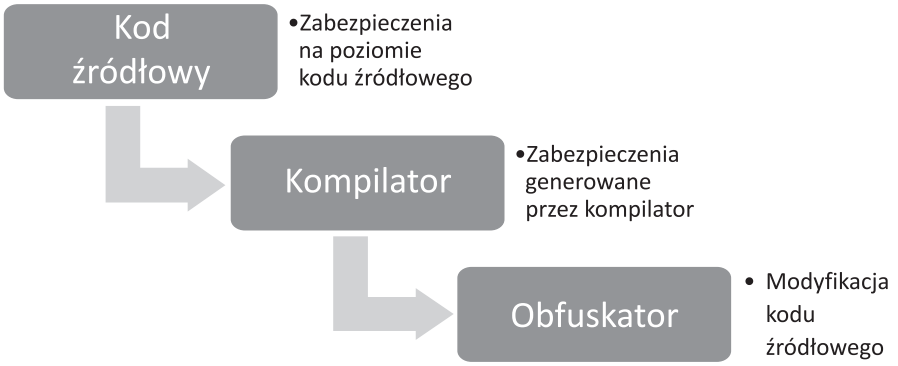
Aby zrozumieć lepiej zagrożenia i wektory ataku, trzeba przyjrzeć się zabezpieczeniom jakie są stosowane przez developerów aplikacji mobilnych.

Na model bezpieczeństwa aplikacji składają się następujące elementy:

- zabezpieczenia udostępniane przez system operacyjny, chociaż należy przy tym pamiętać, że rożne wersje mogą mieć inny ich zestaw,
- zabezpieczenia udostępniane przez kompilator, których celem jest przeciwdziałanie błędom popełnianym przez programistów, np. poprzez wychwytywanie ataków typu przepełnienie bufora (mechanizm *stack cookie* lub *stack canary* opisany w dalszej części),
- dodatkowe zabezpieczenia wybrane i dodane do aplikacji przez developera – do tej klasy należą m.in.:
  - szyfrowanie danych za pomocą własnych mechanizmów (wbudowanych lub poprzez wykorzystanie API systemowego),
  - obfuskacja kodu (opisana dalej),
  - sprawdzenie czy aplikacja uruchamia się na urządzeniu z zainstalowanym *jailbreak'iem* – i jeśli *jailbrake* zostanie wykryty, odmówienie uruchomienia się.
- Dodatkowe zabezpieczenia narzucone przez sklep odpowiedzialny za dystrybucję aplikacji, np. wymóg podpisania aplikacji przed upublicznieniem.

W tym miejscu należy zauważyć, że nawet zabezpieczenia generowane automatycznie bądź domyślnie przez kompilatory, jak np. ochrona stosu, aby mogły funkcjonować efektywnie, muszą być rozumiane i świadomie stosowane przez developerów. Aplikacje „bezpieczne przez przypadek" nie istnieją. W końcu każdą opcję można „niechcący" wyłączyć, nie zdając sobie sprawy z konsekwencji dla docelowego modelu bezpieczeństwa.

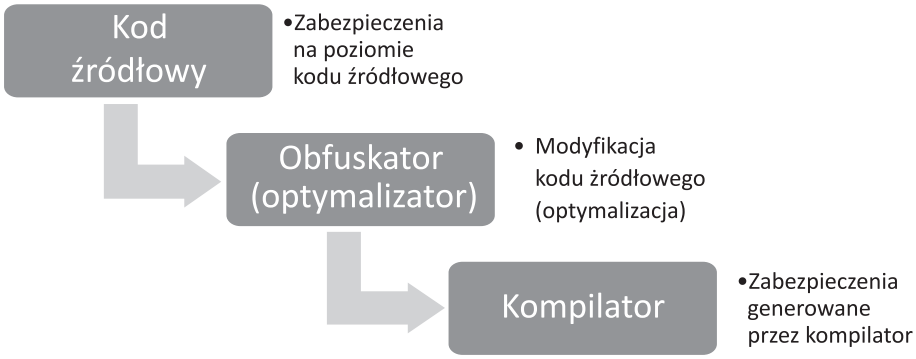
Z drugiej strony developerzy bardzo lubią automatyczne generowanie – czyli bez ich udziału – zabezpieczeń i pokładają w nich zazwyczaj wielokrotnie większą wiarę niż w rzeczywistości one oferują. Dodatkowo każde zabezpieczenie używane domyślne jest oczywiście doskonale znane atakującym i natychmiast obchodzone.



Rys 1: Typowy uproszczony proces produkcji aplikacji

W trakcie procesu tworzenia aplikacji mobilnej odpowiedzialność za poszczególne zabezpieczenia jest następująca:

- zabezpieczenia na poziomie kodu źródłowego zależą od developera i jego wiedzy,
- zabezpieczenia generowane przez kompilator dotyczą kodu wynikowego a nie źródłowego – do tej kategorii zaliczamy:
  - ochronę stosu,
  - ochronę sterty,
  - umożliwienie kontroli integralności i autentyczności poprzez podpisanie aplikacji.
- dodatkowe zabezpieczenia operujące na gotowym kodzie wynikowym – zazwyczaj stosowane są tutaj narzędzia typu obfuscator, których celem jest utrudnienie dekompilacji bądź deasemblacji kodu, co w konsekwencji ma utrudnić identyfikację wewnętrznych algorytmów oraz podatności.



Rys. 2: Typowy model produkcji aplikacji dla platformy Android

Zabezpieczenia dodawane do natywnego kodu przez kompilator w trakcie procesu kompilacji[1] stanowią naturalne uzupełnienie zabezpieczeń przed nadużyciami oferowane przez platformę systemową. System zabezpieczeń platform mobilnych przypomina więc wielowarstwowość zabezpieczeń tradycyjnych systemów operacyjnych (więcej o tym zagadnieniu znajduje się w punkcie „Przeglądarka – idealny cel").

Wiele obfuskatorów nie spełnia w praktyce swojego zadania. Niektóre z tych narzędzi mogą być automatycznie usunięte z atakowanego pliku wynikowego aplikacji. Inne wymagają mniejszych lub większych nakładów manualnych – nadal jednak w większości przypadków udaje się uzyskać dostęp do kodu przydatnego do analizy.

Z drugiej natomiast strony, obfuskacja kodu utrudnia inżynierię wsteczną badanego rozwiązania[2], jednak należy pamiętać, że tylko kwestią czasu i zastosowanych nakładów jest kompletne lub przynajmniej częściowe odwzorowanie wewnętrznych mechanizmów aplikacji. Warto jest o tym fakcie pamiętać podczas przeprowadzania testów bankowości mobilnej bez dostępu

---

1 Dla uproszczenia przyjmujemy, że na proces kompilacji składa się kompilacja, konsolidacja i ewentualne podpisanie aplikacji. W przypadku aplikacji mobilnych aplikacje wraz ze wszystkimi potrzebnymi plikami znajdują się w jednym archiwum. Proces tworzenia tego archiwum w tym przypadku także zaliczamy do procesu kompilacji.

2 Zgodnie z opisem rozwiązania ProGuard, będącego częścią pakietu Android-SDK: *"The ProGuard tool shrinks, optimizes and obfuscates your code by removing unused code and renaming classes, fields and methods with semantically obscure names. The result is a smaller sized .apk file that is more difficult to reverse engineer. (...)"* – http://developer.android.com/tools/help/proguard.html

do kodów źródłowych, gdyż prawdziwi atakujący, w przeciwieństwie do audytorów, dysponują nieograniczonym czasem pozwalającym na przeprowadzenie skutecznego ataku. Powyższa uwaga ma ważne konsekwencje dla banku podczas podpisywania umów na dostawy aplikacji bankowych: ich kod źródłowy powinien być dostępny dla banku i audytorów przez nich wynajmowanych do oceny poziomu bezpieczeństwa.

Przeglądarka – idealny cel

Przeglądarki internetowe stały się praktycznie mini systemami operacyjnymi – w ich kontekście można uruchamiać nie tylko aplikacje webowe, ale także różnego rodzaju wtyczki, a dzięki ostatniej wersji standardu HTML – nawet tworzyć połączenia sieciowe. Dodatkowo pojawiły się aplikacje, które wykorzystują silnik renderujący przeglądarki. Z perspektywy bezpieczeństwa oznacza to, że:

- przeglądarka jest uruchamiania w kontekście użytkownika a więc zazwyczaj dziedziczy wszystkie jego uprawnienia,
- przeglądarka jest niezwykle skomplikowaną aplikacją, która ze względu na wyścig w wydawaniu nowych wersji pomiędzy producentami jest zazwyczaj aplikacją pełną błędów, które prowadzą do podatności.

W efekcie powyższej charakterystyki przeglądarka internetowa stała się idealnym celem ataku. Biorąc pod uwagę, że przeglądarki zarządzają także danymi uwierzytelnienia i muszą je przynajmniej tymczasowo trzymać w formie otwartej w pamięci, wstrzykiwanie złośliwego kodu (np. techniką *DLL injection*) w przestrzeń adresową procesu stało się „naturalnym" wektorem ataku. Należy w tym miejscu zauważyć, że wewnętrzna architektura przeglądarki nie ma dla naszych rozważań aż tak dużego znaczenia, np. przeglądarka Chrome w systemie Windows nie uruchamia wielu dodatkowych wątków z jednego procesu lecz kolejne procesy, które są lżejsze od jednego z wieloma wątkami.

Producenci platform systemowych oraz przeglądarek zdają sobie sprawę z powyższej sytuacji i starają się wprowadzać coraz doskonalsze zabezpieczenia. W efekcie dzisiaj użytkownik ma do dyspozycji co najmniej cztery poziomy zabezpieczeń na poziomie:

1. systemu operacyjnego,
2. kompilatora użytego do kompilacji przeglądarki internetowej oraz wtyczek i innych komponentów,[3]
3. przeglądarki internetowej,
4. transmisji danych.

Poniższa tabela systematyzuje istotne klasy zabezpieczeń dla danego obszaru na przykładzie platformy Windows 7 dla procesorów x64. Wybór platformy i jej wersji został podyktowany miażdżącą popularnością systemu Windows w porównaniu z konkurentami na rynku komputerów osobistych.

Lp.	Obszar	Wybrane przykłady dostępnych zabezpieczeń
1.	Zabezpieczenia na poziomie systemu operacyjnego	• DEP (*Date Execution Prevention*), • ASLR (*Address Space Layout Randomization*), • UAC (*User Access Control*), • kontrola dostępu za pomocą list ACL do obiektów systemowych, w tym m.in. do plików i rejestrów, • kontrola nad uprawnieniami użytkowników,[4] • podpisywanie sterowników, • Windows Resource Protection (zastąpił od Windows Vista mechanizm Windows File Protection).
2.	Zabezpieczenia na poziomie kompilatora użytego do kompilacji przeglądarki internetowej oraz wtyczek i innych komponentów	• ochrona stosu (*stack cookie / stack canary*), • ochrona łańcucha SEH (SafeSEH).
3.	Zabezpieczenia na poziomie przeglądarki internetowej	• ochrona ciasteczek, • ochrona danych uwierzytelnienia.
4.	Zabezpieczenie transmisji danych	• protokół SSL/TLS.

3 Do tej grupy zaliczamy także, dla uproszczenia, model bezpieczeństwa i zabezpieczenia oferowane przez maszyny wirtualne, np. Java.

4 W systemie Windows, podobnie jak w systemach Unix/Linux, serwisy systemowe także są uruchamiane w kontekście określonego konta. Serwis otrzymuje więc uprawnienia i prawa dostępu, jakie zostały zdefiniowane dla konta, z którego korzysta.

W tym miejscu należy zwrócić uwagę na bardzo istotne zagrożenie, jakim jest koniec wsparcia dla systemu Microsoft Windows XP[5] od 14 kwietnia 2014 roku. Stanowi to istotny problem dla sektora bankowego z perspektywy bezpieczeństwa. Koniec wsparcia oznacza także koniec wydawania poprawek, także adresujących problemy z bezpieczeństwem w formie *hotfiksów* i *service packów*. Brak poprawek nie jest czymś, co domowych użytkowników powstrzyma od korzystania lub zmusi do zmiany wersji systemu operacyjnego, zwłaszcza że rynek aplikacji dla tego systemu jest na tyle duży, iż wycofanie się Microsoftu ze wsparcia nie oznacza wycofania się w tym samym momencie także innych dostawców.

Wracając do tematu przeglądarki, jak zaznaczono wcześniej są to coraz bardziej złożone aplikacje o niezwykle szerokiej funkcjonalności. Zgodnie z praktyką bezpieczeństwa: im bardziej złożona i większa funkcjonalność, tym większa jest powierzchnia ataku. Jedną z technologii stosowanych obecnie we wszystkich popularnych przeglądarkach wspieranych przez systemy bankowości elektronicznej jest kompilacja JIT (*just-in-time compilation*). Mechanizm JIT jest używany przez przeglądarki m.in. podczas uruchamiania kodu JavaScript i ActionScript. Spowodowało to opracowanie techniki ataku o nazwie *„JIT spraying"*. Technika ta polega na ominięciu zabezpieczeń przed wykonaniem nielegalnie kodu (w przypadku Windows jest to ominięcie między innymi mechanizmu DEP i ASLR) poprzez skierowanie procesora na wykonanie kodu znajdującego się np. w stałych lub zmiennych skryptu, na którym kompilator JIT pracuje. Zaletą atakowania w ten sposób kompilatorów JIT przez atakującego jest to, że na wejściu kompilator otrzymuje dane, które w efekcie końcowym zamienia na natywny kod. Podczas procesu translacji i kompilacji, o ile dane nie wymagają przechowywania w stronach pamięci z prawem wykonania kodu, o tyle wynik działania kompilatora już takiego prawa wymaga.

Technika ta nie musi dotyczyć tylko atakowania przeglądarki, jest ona także z powodzeniem wykorzystywana do atakowania aplikacji obsługujących format PDF.

JIT spraying jest pochodną techniki *heap spraying* – w tym przypadku atakujący alokuje duże obszary pamięci na stercie, aby w odpowiednich obszarach adresowych umieścić kod exploita, co ma zapewnić jego wykonanie.

HTML5 umożliwia przeprowadzenie powyższego ataku niezwykle sprawnie.

---

5 Pełna lista dat zakończenia wsparcia dla różnych wersji systemów Windows jest dostępna pod adresem: http://windows.microsoft.com/en-us/windows/products/lifecycle

Router brzegowy, access point i firmware

Firmware dla urządzeń sieciowych to jeden z najczęściej pomijanych komponentów podczas audytów i testów penetracyjnych. Tymczasem, kto przejmie kontrolę nad firmwarem lub wgra własny, ten przejmuje pełną kontrolę nad urządzeniem. W konsekwencji atakujący może:

- przekierować dowolnie ruch poprzez routingi,
- przekierować dowolnie ruch poprzez podstawienie swoich serwerów DNS,
- monitorować i podsłuchiwać ruch sieciowy użytkownika,
- uniemożliwić użytkownikowi dostęp do urządzenia poprzez zmianę metod uwierzytelnienia oraz danych wymaganych do uwierzytelnienia,
- zatrzeć ślady swojej obecności poprzez skasowanie firmware'u i logów (jeśli logowanie zdarzeń zostało włączone na urządzeniu), co może istotnie utrudnić późniejsza analizę incydentu.

Typowe wektory ataku to:

- użycie domyślnych, ustawionych przez producenta lub dostawcę usługi danych uwierzytelniających,
- użycie nieudokumentowanych kont lub funkcji dostępu serwisowego,
- atak brutalną siłą na domyślne konto administratora – w urządzeniach sieciowych zazwyczaj występuje tylko jedno konto i to z wysokimi uprawnieniami,
- użycie podatności w jednej z udostępnianych usług przez urządzenie – dobrym przykładem mogą być podatności w serwerach usług sieciowych służących do administracji i/lub monitorowania, np. tftp (często używanych do aktualizacji firmware'u) czy wbudowanych serwerów http.

BIOS i UEFI

Problem ataków na firmware nie jest ograniczony tylko do urządzeń wbudowanych i mobilnych, lecz dotyka także komputerów stacjonarnych i serwerów. W najpopularniejszej dzisiaj architekturze PC, opartej o procesory x64, firmware odgrywa tak samo krytyczną rolę, jak w urządzeniach mobilnych. W oryginalnej architekturze PC, zaproponowanej przez firmę IBM, rolę tego, co dzisiaj nazywamy firmwarem odgrywał BIOS zapisany w pamięci ROM. W tamtych czasach nie istniało zagrożenie jego nieautoryzowanej modyfikacji w sposób programowy. Wraz ze wzrostem złożoności architektury wymuszonej

przez jej ewolucję i dynamicznie rozwijający się rynek niezależnych dostawców sprzętu rosła też złożoność samego BIOSu. Konsekwencją tego było także pojawienie się innych niż IBM dostawców BIOSów dla producentów płyt głównych. Pierwszą istotną modyfikacją z perspektywy bezpieczeństwa – poza wewnętrzną złożonością kodu[6] tworzącego BIOS – było dodanie możliwości jego modyfikacji poprzez umieszczenie go w pamięci flash. Oznaczało to nie tylko możliwość skasowania go i uczynienia systemu nieużywalnym (co próbował robić wirus CIH, znany także jako Czarnobyl), ale przede wszystkim jego nieautoryzowaną modyfikację. Ponieważ pierwszym kodem, jaki jest uruchamiany po włączeniu komputera to właśnie *firmware*, jego nieautoryzowana modyfikacja ma daleko idące konsekwencji w ujęciu bezpieczeństwa całego systemu. Kto pierwszy uruchomi swój kod ten przejmuje całkowitą kontrolę nad systemem. Zasada ta w dobie powszechnej wirtualizacji i *hypervisorów* jest jeszcze bardziej aktualna.

Na skutek problemów z architekturą BIOSu Intel, wprowadzając na rynek procesory z rodziny Itanium, zaproponował nowy standard EFI (*Extensible Firmware Interface*). Zaadoptowała go także firma Apple do swoich produktów. Dzisiaj miejsce EFI zajęła jego nowsza wersja UEFI (*Unified Extensible Firmware Interface*).

UEFI to de facto dedykowany system operacyjny, którego zadaniem oprócz inicjalizacji sprzętu, na którym się go uruchamia jest... aktywowanie docelowego systemu operacyjnego.

W ramach inicjalizacji sprzętu UEFI wykonuje m.in.:

- inicjalizację pozostałych procesorów w systemach wieloprocesorowych,
- inicjalizację kontrolera pamięci,
- inicjalizację kontrolera przerwań,
- inicjalizację kontrolera IO,
- inicjalizację mostków: północnego i południowego (*north* i *south bridge*)
- inicjalizację kart rozszerzeń oraz kontrolerów dysków itp. poprzez sterowniki UEFI lub tzw. OPTION ROM znajdujące się na kartach PCI/PCIe,
- inicjalizację aplikacji mikrokodu dla procesorów.

---

6 Złożoność ta ma kilka źródeł, a jednym z nich jest fakt, że w momencie startu systemu nie jest zainicjalizowany kontroler pamięci, więc nie jest dostępny stos. W niektórych przypadkach BIOS używa więc wewnętrznego cache'u procesora jako pamięci RAM. Innym powodem jest wewnętrzna kompresja kodu wynikająca z ograniczeń przestrzeni adresowej x86 oraz potrzeby zachowania wstecznej kompatybilności.

Ta ostatnia czynność jest niezwykle istotna dla bezpieczeństwa całego systemu, gdyż mikrokod wpływa na zachowanie procesora – nieautoryzowana modyfikacja miałaby katastrofalne skutki dla bezpieczeństwa nie tylko całego systemu, ale także każdej aplikacji.

Innym elementem krytycznym dla bezpieczeństwa systemu operacyjnego, który ma być załadowany przez UEFI, są sterowniki i serwisy UEFI. Oprócz nieautoryzowanej modyfikacji tych komponentów architektury UEFI, innym wektorem ataku może być mechanizm OPTION ROM znajdujący się na kartach PCI/PCIe. Kod zawarty w OPTION ROM na karcie znajdującej się w systemie jest domyślnie uruchamiany przez BIOS. W przypadku UEFI – upraszczając bardzo proces – tak się dzieje tylko w przypadku, gdy sterownik UEFI nie obsługuje danej karty i musi wykorzystać przestarzałą metodę jej inicjalizacji. W architekturze UEFI odpowiada za to CSM (*Compatibility Support Module*). Oczywiście w takim przypadku nieautoryzowana modyfikacja kodu znajdującego się w OPTION ROM będzie skutkować jego wykonaniem. W przypadku BIOSu taki kod może przejąć kontrolę nad całym systemem, w przypadku UEFI jest to bardziej skomplikowane.

W wersji 2.2 standardu UEFI dodano protokół nazywany „*Secure boot*". Jego zadaniem jest uniemożliwienie załadowania do pamięci loaderów i sterowników systemu operacyjnego, które nie są podpisane lub które są podpisane, ale ich integralność została naruszona.

Mechanizm ten jest obecnie wspierany przez Windows 8, Windows Server 2012 oraz niektóre dystrybucje systemu Linuksa.

Niestety, pojawienie się znacznie lepiej zaprojektowanego pod kątem bezpieczeństwa UEFI nie oznacza jeszcze całkowitej śmierci BIOSu. Tradycyjny BIOS nadal żyje, np. w wielu platformach wirtualizacyjnych. Jego modyfikacja jest nawet łatwiejsza niż w przypadku prawdziwego sprzętu – wystarczy zmodyfikować plik, w którym się znajduje[7]. Inną możliwością ataku jest włączenie na platformie wirtualizacyjnej serwera debugowania. Na przykład środowisko VMWare oferuje serwer gdb, za pomocą którego można zdalnie przejąć kontrolę nad maszyną wirtualną i w konsekwencji wpłynąć na wykonywany w jej obrębie kod. Nic nie stoi na przeszkodzie, aby zastosować taką technikę w odniesieniu do BIOSu. Ponieważ jest on pozbawiony wszelkich zabezpieczeń przed tego typu atakami, atakujący ma bardzo ułatwione zadanie.

7 W niektórych rozwiązaniach wirtualizacyjnych BIOS nie jest przechowywany w formie osobnego pliku, lecz jako zasób (*resource*) w pliku wykonywalnym. Tak się dzieje np. w VMWare Player.

W przypadku środowiska VMWare ESX wystarczy zmodyfikować 2 linijki pliku konfiguracyjnego maszyny wirtualnej, aby taki zdalny atak był możliwy.

Podobny atak można przeprowadzić z użyciem opisanego już wcześniej mechanizmu OPTION ROM dla kart PCI/PCIe – platformy wirtualizacyjne muszą bowiem zawierać BIOS np. karty graficznej, sieciowej czy sterownika SCSI. W praktyce każdy z nich jest trzymany w pliku i jego modyfikacja może mieć wpływ na wszystkie uruchamiane maszyny wirtualne.

Środowisko wykonania aplikacji webowej

W poprzednich akapitach poruszony został głównie temat omijania zabezpieczeń znajdujących się po stronie klienta systemu bankowości elektronicznej. Teraz skupimy się na wektorach ataków dotyczących infrastruktury, która znajduje się tylko po stronie banku. Oczywiście, zdefiniowanie „banku" jako strony, która zarządza infrastrukturą oraz samą aplikacją bankowości elektronicznej jest daleko idącym uproszczeniem. Nawet ograniczenie się tylko do rynku polskiego nie umniejsza roli outsourcingu w przypadku bankowości elektronicznej. Banki korzystają zarówno z outsourcingu oferowanego przez spółki ze swojej grupy kapitałowej lub zrzeszenia (w przypadku banków spółdzielczych) bądź korzystają z rozwiązań dostarczanych przez zewnętrznych dostawców. Nie zmienia to wcale faktu, że o końcowym poziomie bezpieczeństwa systemu bankowości elektronicznej decyduje także środowisko wykonania aplikacji. Kwestie związane z bezpieczeństwem aplikacji webowych zostały omówione w dalszej części.

Na środowisko wykonania aplikacji składa się kilka warstw:

- infrastruktura sieciowa,
- infrastruktura serwerowa,
- infrastruktura wirtualizacyjna,
- serwery http/https,
- serwery aplikacyjne,
- serwery bazodanowe.

Każda z tych warstw wymaga adekwatnych zabezpieczeń. Dużym problemem jest monitorowanie bezpieczeństwa w sposób ciągły, zwłaszcza z perspektywy wykonywanych w tych systemach działań. Powodem są problemy wydajnościowe wielu komponentów w momencie włączenia pełnego audytu zdarzeń.

Przejęcie kontroli nad infrastrukturą wirtualizacyjną pozwala przejąć kontrolę nad całą aplikacją oraz bazami danych, z których korzysta. Jest to więc potencjalne pojedynczy punkt, który wymaga dokładnej ochrony.

Innym newralgicznym elementem są bazy danych i dzieje się tak z kilku powodów. Po pierwsze, poprzez ataki typu *SQL Injection* i *Blind SQL Injection* dostęp do przynajmniej wybranych pól bazy danych może być zapewniony zdalnie za pośrednictwem podatnej na atak aplikacji bankowości elektronicznej. Po drugie, silniki bazodanowe oferują wiele interfejsów do zarządzania oraz rozszerzania funkcjonalności: przykładem może być mechanizm procedur składowanych i rozszerzonych procedur składowanych w Microsoft SQL Server. Bazy danych Oracle oferują rozszerzenia funkcjonalności np. za pomocą Javy. Oznacza to, że atakujący może uruchomić nielegalnie własny kod i uzyskać dostęp do danych. Jeśli aplikacja korzysta z konta o wysokich uprawnieniach, to atakujący może nie tylko uzyskać dostęp do danych, ale także wykonać polecenia w kontekście uprawnień systemu bazodanowego i w konsekwencji dokonać całkowitej penetracji systemu bazodanowego wraz z platformą systemową.

Istotnym problemem ostatnich dwóch lat są ataki *DDoS* (*Distributed Denial of Service*). O ile sama koncepcja ataku i pierwsze udane próby sięgają lat 1999/2000 to na skutek kilku(nastu) spektakularnych ataków oraz istotnego zwiększania przychodów z kanałów elektronicznych problem stał się znów bardzo istotny.

Problem ataków typu DDoS jest o tyle ważny, że do jego przeprowadzenia nie trzeba żadnej specjalistycznej wiedzy a tylko nieco pieniędzy. Na świecie istnieje bowiem wiele organizacji oferujących gotowe sieci, tzw. botnety, umożliwiające każdemu przeprowadzenie takiego ataku. Organizacje te oferują nawet swoim „klientom" wsparcie w języku polskim.

Drugim istotnym problemem ataków DDoS jest fakt, że zaatakowany może zostać każdy i bez pełnej współpracy pomiędzy nim, a providerami praktycznie nie ma skutecznej metody obrony – w końcu każde łącze, każdy system i każda aplikacja ma ograniczoną pulę dostępnych zasobów, które w końcu można wyczerpać. Zresztą, dla biznesów internetowych nawet samo spowolnienie czasu reakcji usługi jest już zdarzeniem mogącym generować straty. Oczywiście, jak w przypadku każdego innego ataku, także i tutaj występuje po stronie ofiary ryzyko utraty reputacji.

Jest kilka podejść do ochrony przed atakami DDoS:

- budowa odpowiedniej infrastruktury po stronie banku,
- powierzenie ochrony zewnętrznemu podmiotowi oferującemu tzw. *scrubbing center*,
- podejście mieszane oparte o dwa powyższe.

W przypadku odsyłania ruchu sieciowego do trzeciej strony (czyli *scrubing center*) w celu odfiltrowania „niedobrych" pakietów należy pamiętać o ograniczeniach legislacyjnych. Otóż bez odpowiedniego przygotowania tego procesu od strony prawnej nie można np. wysyłać danych osobowych do innych państw. Istotna jest więc lokalizacja *scrubbing center* – w przypadku rozwiązania pracującego w chmurze określenie lokalizacji może jednak nie być takie łatwe.

Drugim problemem jest inspekcja ruchu zaszyfrowanego przy użyciu SSL/TLS. Jeśli *scrubbing center* nie prowadzi inspekcji wewnątrz niego, nie może wyczyścić w pełni tej komunikacji ze złych pakietów. Jeśli prowadzi taką inspekcję – co wymaga odszyfrowania ruchu – to uzyskuje automatycznie dostęp do danych osobowych i finansowych.

Z drugiej strony, bank (lub usługodawca świadczący usługę bankowości elektronicznej) może część zabezpieczeń wdrożyć po swojej stronie – niektóre są proste w implementacji, jak np.:

- filtrowanie pakietów *spoofowanych*,
- *bogon filter*,
- monitoring czasu odpowiedzi aplikacji,
- wypracowane procedury reakcji z dostawcami internetu.

Niezależnie od stosowanego podejścia bank musi być przede wszystkim przygotowany na taki atak, zanim on nastąpi. Oznacza to nie tylko zabezpieczenia techniczne, ale także odpowiedni proces monitorowania dostępności i wydajności usług oraz poszczególnych komponentów systemów, jak też odpowiednie procedury na wypadek ataku wraz z odpowiednio przeszkolonym zespołem. Brak symulacji tego typu ataków i zbadania reakcji ludzi na działania w przypadku stresowej sytuacji zawsze prowadzi do popełniania błędów podczas prawdziwego incydentu.

Aplikacja webowa

Do tej pory omówiliśmy ataki na infrastrukturę sieciową i aplikacje mobilne. Czas na aplikacje webowe. Wydawać by się mogło, że ten kanał bankowości elektronicznej istnieje już na tyle długo, że udało się w nim wyeliminować przynajmniej te klasy krytycznych podatności, które znane są co najmniej od kilku lat. Można do nich zaliczyć podatności typu:

- XSS
- CSRF

Obie klasy podatności znajdują się na aktualnej liście OWASP Top10, która stara się regularnie prezentować najczęściej występujące problemy z bezpieczeństwem w aplikacjach webowych.

Tymczasem tylko w I kwartale 2014 roku podczas prowadzonych przez AVET INS testów penetracyjnych i audytów bezpieczeństwa systemów bankowości elektronicznej udało się zidentyfikować wszystkie te problemy. Co ciekawe, podatności te występowały zarówno w nowych, właśnie wdrażanych aplikacjach, jak i starych, które w skrajnych przypadkach były już wcześniej kontrolowane pod kątem bezpieczeństwa.

Biorąc pod uwagę, że nie były to jedyne klasy podatności odkryte podczas tych projektów, należy stwierdzić na podstawie danych empirycznych, że:

- stare klasy podatności w aplikacjach webowych „nie umierają" tak szybko jakbyśmy sobie tego życzyli,
- zabezpieczenia typu *Web Application Firewall* (WAF) nie są stosowane poprawnie lub nie są skonfigurowane poprawnie, a w skrajnych przypadkach stwierdza się nawet ich brak,
- pojedyncza kontrola aplikacji wcale nie musi ujawnić wszystkich krytycznych podatności,
- brak kontroli istotnych zmian w aplikacji – zwłaszcza gdy nie jest to aplikacja podstawowa – nie jest czymś niespotykanym i zdarza się regularnie.

Na przestrzeni lat w wyścigu zbrojeń bezpieczeństwa z perspektywy webowych systemów bankowości elektronicznej najbardziej ewoluowały mechanizmy uwierzytelnienia i autoryzacji: zaczynając od statycznych haseł po wielostopniowe, wieloetapowe rozwiązania. Oczywiście, aby te metody były skuteczne muszą być one:

- poprawnie zaimplementowane z perspektywy modułu uwierzytelnienia bądź autoryzacji,

- poprawnie zintegrowane z mechanizmami zarządzania sesją,
- poprawnie osadzone w logice aplikacji pełniącej funkcję systemu bankowości elektronicznej.

Dodatkowo *workflow* związany z zarządzaniem całym cyklem dostępu do systemu musi być poprawny.

W praktyce tylko połączenie wszystkich tych czterech elementów gwarantuje bezpieczeństwo systemu bankowości elektronicznej, lecz tylko w warstwie pierwotnego uwierzytelnienia. Dzieję się tak dlatego, że po poprawnym uwierzytelnieniu wobec systemu atakujący nadal może wykorzystywać typowe dla aplikacji webowych podatności typu SQL Injection, CSRF czy błędy w logice lub niepoprawne usuwanie plików tymczasowych. Każda z tych klas podatności może zapewnić atakującemu dostęp do danych innych klientów lub wręcz wykonanie operacji w ich kontekście.

Jak już wcześniej wskazano, niezwykle istotne jest poprawne zarządzanie sesją. Należy pamiętać, że protokół HTTP jest bezstanowy, co z perspektywy każdego mechanizmu autoryzacji jest dużym problemem. Gdy tylko zdano sobie sprawę z tego ograniczenia, zaczęto „naprawiać" je na wiele różnych sposobów. Rozwój przeglądarek internetowych, wbudowanie JavaScriptu i wsparcie dla HTML5 umożliwiło wykorzystanie technologii takich jak AJAX i tworzenie dynamicznych, śledzących stan aplikacji na bezstanowym protokole HTTP/HTTPS.

Ponieważ mechanizmy zarządzania sesją są dzisiaj wbudowane na poziomie serwerów aplikacyjnych, nie każdy system bankowości elektronicznej musi je rozszerzać lub używać odrębnych, własnych metod. Oczywiście, niezależne od implementacji mechanizmu zarządzania sesją musi on być poprawnie zintegrowany z mechanizmami uwierzytelnienia i autoryzacji. Ponieważ do zarządzania sesją używa się między innymi ciasteczek (*cookies*) ich ochrona przez przeglądarkę i aplikację jest wymagana. Aplikacja (lub serwer aplikacyjny) może na przykład ustawić flagę SECURE. W przypadku aplikacji bankowości elektronicznej taka konfiguracja jest de facto wymogiem bezpieczeństwa.

Aktualna wersja OWASP Top 10 (z lutego 2014 roku):

- A1. *Injection*.
- A2. *Broken Authentication and Session Management*.
- A3. *Cross-Site Scripting (XSS)*.
- A4. *Insecure Direct Object References*.

- A5. *Security Misconfiguration*.
- A6. *Sensitive Data Exposure*.
- A7. *Missing Function Level Access Control*.
- A8. *Cross-Site Request Forgery (CSRF)*.
- A9. *Using Components with Known Vulnerabilities*.
- A10. *Unvalidated Redirects and Forwards*.

Klasyfikacja a bezpieczeństwo aplikacji webowych

Należy pamiętać, że podatności w aplikacjach webowych mogą być bardziej złożone niż to przedstawia lista OWASP Top10. Zresztą niektóre klasy problemów na tej liście nie występują w ogóle, co oznacza, że test pod kątem podatności z listy OWASP Top10 nie może być nigdy uznawany za wystarczający.

Doskonałym przykładem problemów, które tylko częściowo i to w ograniczonej formie występują na liście OWASP Top10 są podatności wynikające z błędnych założeń projektowych lub procesowych. Nie są to więc stricte techniczne podatności, które łatwo usystematyzować i wykryć za pomocą automatycznych narzędzi. Wykrywanie takich podatności wymaga manualnego testowania.

Oto przykład z I kw. 2014 roku: testowana aplikacja miała całkiem rozbudowany, wielostopniowy mechanizm uwierzytelnienia i autoryzacji. Dotyczył on jednak tylko nowych obiektów – usunięcie obiektu i utworzenie nowego w miejsce poprzednika umożliwiało pomięcie autoryzacji.

Kolejnym istotnym zagadnieniem jest fakt, że podatności można składać w jedną większą podatność. Ich połączenie może być znacznie bardziej niebezpieczne niż każda z nich osobno rozpatrywana.

Przykładem, z którym zetknęliśmy się w jednej z aplikacji webowych dla sektora finansowego była podatność umożliwiająca dostęp do bazy danych. Autorzy ograniczyli prawa użytkownika, z którego korzystała aplikacja, więc nie można było od razy uzyskać praw administratora. Nie zablokowali jednak prawa uruchomienia procedury składowanej modyfikującej prawa użytkownika. Po dodaniu odpowiednich uprawnień, użytkownik aplikacyjny stał się administratorem. W tym przypadku dwie różne podatności w różnych komponentach i dotyczące rożnych technologii umożliwiły praktycznie pełną penetrację systemu.

W przypadku pierwszej podatności atak nie wymagał żadnego dedykowanego narzędzia – można go było przeprowadzić używając samej aplikacji. W drugim przypadku potrzebne było proxy oraz znajomość zastosowanego silnika bazodanowego.

Ataki na użytkownika

Poza atakami na przeglądarki internetowe, urządzenia mobilne i urządzenia sieciowe nie poruszyliśmy innych ataków na użytkowników systemów bankowości elektronicznej. Umyślnie ich omówienie zostawiłem na koniec, ponieważ są one doskonale opisane i znane w sektorze bankowym. Dlatego tylko dla kompletności niniejszej publikacji przedstawię ich (niepełną) listę:

- ataki typu *Man-in-the-Middle* (MITM),
- instalacja fałszywych certyfikatów SSL/TLS,
- przekierowanie ruchu sieciowego,
- modyfikacja adresów IP serwerów DNS,
- ataki *phishingowe*,
- ataki z użyciem złośliwego oprogramowania: *keyloggery*, *boty*, narzędzia do zdalnej administracji, itp.

Należy zwrócić uwagę, że nie każdy atak wymaga zmian w systemie użytkownika, a więc nawet aktualne oprogramowanie antywirusowe może nic nie wykryć.

Innym problemem jest fakt, że systemy użytkowników nie zawsze są atakowane i infekowane w celu przejęcia kontroli nad kontem w systemie bankowości elektronicznej tego konkretnego użytkownika. Atak może mieć na celu wykorzystanie samego systemu – bez wiedzy użytkownika – do ataku na inne systemy i innych użytkowników. Tak się dzieje w przypadku sieci typu *botnet* używanych przy atakach DDoS.

Ataki wewnętrzne

Do tej pory większość opisanych ataków była realizowane z zewnątrz – wyjątkiem może być nieautoryzowana modyfikacja *firmware'u* na poziomie infrastruktury obsługującej system bankowości elektronicznej. Niestety, nie wyczerpuje to listy możliwych wektorów ataków. Ponieważ katalog takich ataków wykracza daleko poza ramy niniejszej publikacji, zostaną podane tylko wybrane wektory:

- Ataki na systemy bazodanowe – od lat są one najsłabiej zabezpieczonymi komponentami systemów bankowości elektronicznej. Dzieje się tak dlatego, że są schowane za kolejnymi warstwami aplikacji i infrastruktury sieciowej. Tymczasem dostęp do zarówno ich kontekstu, jak i zawartości jest możliwy np. na skutek podatności typu *SQL Injection* w sposób zdalny i to także w przypadku, gdy zaatakowana aplikacji używa ORM (*Object-Relational Mapping*). Używanie tej technologii jako jedynego skutecznego zabezpieczenia przed błędami prowadzącymi do podatności typu Injection to często popełniany błąd przed developerów. Drugim powodem jest powszechne przekonanie, że pracownik nie zmodyfikuje wnętrza tabel baz, ponieważ ich struktura jest zbyt skomplikowana, aby pominąć np. księgę główną. W praktyce można się z tą tezą zgodzić pod warunkiem, że zakładamy iż modyfikacja zostanie dokonana ręcznie. Jeśli jednak atakujący zautomatyzuje proces za pomocą odpowiednich narzędzi, to teoretycznie niemożliwy atak staje się praktycznie wykonalny.
- Kopie zapasowe – niezależnie od ich formy i procesu ich wykonywania muszą być przynajmniej częściowo odtwarzane w ramach testu. Oznacza to, że nawet jeśli kopia była zaszyfrowana to w ramach weryfikacji musi zostać odtworzona a w konsekwencji także odszyfrowana. Atakujący ma więc wtedy możliwość uzyskania dostępu do danych w formie otwartej. Ponieważ odtworzenia dokonuje się na systemach testowych, które zazwyczaj są słabiej chronione niż systemy produkcyjne, ryzyko powodzenia szansy takiego ataku rośnie. W systemach testowych zazwyczaj nie ma także pełnego audytu zdarzeń, co może prowadzić do braku wykrycia wystąpienia ataku.

Podsumowanie

Wraz ze wzrostem złożoności oferowanych produktów finansowych i liczby kanałów, w których są one udostępniane rośnie także poziom ryzyka. Powyższe opracowanie wskazało jedynie najczęstsze i najciekawsze według autora zagrożenia. To że część z nich jest dzisiaj z perspektywy sektora bankowego w sferze teoretycznych rozważań, gdyż nikt jeszcze takiego przypadku publicznie nie zaraportował, nie oznacza że należy tego typu wektory ignorować. Niewątpliwie sektor bankowy w Polsce stoi przed poważnym wyzwaniem: z jednej strony czasu do wdrożenia rekomendacji D pozostało bardzo mało, z drugiej jest ona oparta o obraz idealnego banku, który w praktyce nie występuje z wielu różnych powodów. W coraz bardziej dynamicznie zmieniającym

się i wymagającym coraz krótszego czasu reakcji świecie zagrożeń proste rozwiązania oparte o wyidealizowany obraz rzeczywistości na dłuższą metę się, niestety, nie sprawdzą. Należy także pamiętać, że dynamika zmian w obszarze technologii IT powoduje, że – jak wskazano na samym początku – standardy i prawo nie nadążają za nimi.

Niewątpliwie smutny jest fakt, że w Polsce nadal nie cieszą się popularnością usługi takie jak audyty kodów źródłowych. Tym bardziej dziwi to w odniesieniu do całego sektora finansowego, który rozumie przecież doskonale proces zarządzania ryzykiem. Tymczasem audyty i przeglądy kodu źródłowego pozwalają bardzo dokładnie modelować zagrożenia i oceniać ryzyko poprzez np. izolację interesujących fragmentów logiki oraz bardzo dokładne testy wybranego obszaru. Efektem końcowym – w przypadku oczywiście poprawnie przeprowadzonego procesu – jest niezwykle efektywne zarządzanie ryzykiem operacyjnym w obszarze bezpieczeństwa aplikacyjnego.

Podziękowania

Chciałbym podziękować zespołowi AVET Information and Network Security, z którym mam przyjemność pracować razem od wielu lat. Gdyby nie nasza praca zespołowa i pomoc, ta publikacja z pewnością nie byłaby tak dobra. Niemniej wszystkie błędy są błędami autora i tylko mi proszę je przypisywać.

Andrzej Koweszko
Dyrektor ING Banku Śląskiego odpowiedzialny za obszar zarządzania ryzykiem: operacyjnym, Compliance i przeciwdziałania oszustwom. Jako doradca wspierał proces organizacji struktur zarzadzania ryzykiem operacyjnym w bankach ING w: Indiach, Australii, Tajlandii i w Turcji.
Jako wiceprzewodniczący Komitetu Bezpieczeństwa ZBP reprezentował Polskę w stałych grupach roboczych Europejskiego Stowarzyszenia Banków. W toku wieloletniej pracy w sektorze bankowym i w M.O.P.K INTERPOL zebrał szerokie doświadczenie w zakresie zapobiegania i ujawniania działań na szkodę instytucji finansowych. Jest autorem szeregu publikacji w tej dziedzinie.

Andrzej Koweszko, ING Bank Śląski S.A.

Zagrożenia sektorowe płatności natychmiastowych

Rosnące tempo pracy i życia rodzi apetyt na nowe rozwiązania technologiczne. Ta zasada znajduje odzwierciedlenie w oczekiwaniach klientów instytucji finansowych. Dokonując wyboru banku klienci najczęściej oceniają koszt i jakość obsługi, całodobową dostępność usług bankowych oraz czas niezbędny do realizacji transakcji.

Oczekiwania klientów są jednym z najważniejszych czynników budowy strategii produktowej i technologicznej banków. Zwłoka w przedstawieniu atrakcyjnej oferty prowadzi do pogorszenia wyników finansowych i obniżenia konkurencyjności. Dlatego wdrożenie płatności natychmiastowych, zapewniających transfer środków w trybie rzeczywistym pomiędzy instytucjami finansowymi spotkało się z życzliwym poparciem menedżerów biznesu i zainteresowaniem klientów.

Niestety, do ich entuzjastów szybko dołączyli też cyberprzestępcy. Równie szybko jak bankowcy opracowali i wdrożyli własne biznesplany, wykorzystując przelewy błyskawiczne do zwiększenia opłacalności ich procederu i poprawienia bezpieczeństwa organizatorów i pośredników, często określanych mianem „mułów".

Zapoczątkowany w 2012 roku proces wdrażania tej formy płatności rozpowszechnił się w bankach i instytucjach parabankowych w roku 2013. Dostępność przelewów natychmiastowych dynamicznie rośnie ku zadowoleniu klientów i przestępców oraz umiarkowanej satysfakcji pracowników banków odpowiedzialnych za zarządzanie bezpieczeństwem instytucji finansowych. Menedżerowie biznesu finansowego są też coraz bardziej świadomi, że ten nowy produkt wymaga nowych inwestycji w środki bezpieczeństwa ograniczające ryzyko strat finansowych i reputacyjnych.

W ten sposób po raz kolejny w historii bankowości najpierw dostarczono klientom atrakcyjny i dochodowy dla banków produkt, aby następnie rozpocząć prace nad ograniczeniem zagrożeń wynikających z jego wykorzystania.

Można sobie w tym miejscu postawić pytanie, czy proces wdrożenia płatności natychmiastowych mógł zostać poprzedzony analizami bezpieczeństwa oraz zmianami w przepisach prawa i kampaniami informacyjnymi podnoszącymi poziom świadomości zagrożeń wśród przyszłych użytkowników. Praktyka biznesu i konkurencji pomiędzy dostawcami usług finansowych dowodzi, że odwrócenie kolejności implementacji tej szczególnej formy przelewów nie było nawet prawdopodobne.

Stare przysłowie głosi „lepiej późno niż wcale". Dlatego warto się zastanowić nad kierunkami i formami podniesienia bezpieczeństwa przelewów natychmiastowych.

Kanał z przyszłością, ale bez historii i oceny ryzyka

Uwzględniając czynniki pragmatyczne można śmiało postawić hipotezę, że w okresie najbliższych 2–3 lat przelewy natychmiastowe upowszechnią się i stopniowo będą wypierały z rynku przelewy tradycyjne. Będzie to spowodowane kolejnym etapem walki konkurencyjnej w sektorze finansowym.

Obecnie głównym czynnikiem zniechęcającym klientów do korzystania z tej usługi jest cena przelewów. Patrząc wstecz na historię opłat za tradycyjne przelewy elektroniczne nasuwa się wniosek, że każdy z dostawców będzie dążył do pozyskania nowych użytkowników obniżając koszt przelewu i rozszerzając paletę usług realizowanych w czasie rzeczywistym. Będą one świadczone na różnych platformach sprzętowych i popularnych systemach operacyjnych Windows, Android, iOS lub nowych, jakie dopiero pojawią się na rynku w przyszłości.

Bezpieczeństwo operacji natychmiastowych będzie doskonalone w procesie uczenia się na błędach, a także na podstawie wniosków ze szczegółowych analiz ryzyka.

Pierwsze przykre doświadczenia wielu polskich i zagranicznych banków wskazują, iż kluczowym czynnikiem ryzyka jest ograniczony czas reakcji na kradzież środków z konta ofiary. Tradycyjny model płatności elektronicznych opierał się na kilku sesjach realizowanych w dni robocze. Warto tu wspomnieć, że tradycja przelewów „opóźnionych" ma też stosunkowo krótką, bo liczącą dopiero 16 lat historię. Taki przebieg procesu pozostawiał bankom spory

margines czasu na podjęcie działań zabezpieczających przelane środki przed ich wypłatą przez przestępców.

Przed kilkunastu laty zastanawiano się szeroko czy bankowość elektroniczna jest dostatecznie bezpieczna, aby stanowić konkurencję dla bankowości bezpośredniej. Bez względu na prezentowane wtedy argumenty dzisiejsza rzeczywistość pokazuje, że postępu technologicznego nie da się zatrzymać tylko na ich podstawie. Klienci zaakceptowali przelewy natychmiastowe i trzeba się przygotować do ich skutecznego zabezpieczenia przed atakami hackerów. Wymaga to dokonania oceny obszarów ryzyka związanych z takimi płatnościami oraz zaproponowania działań ograniczających ryzyko strat dla banków i klientów.

Ocena ryzyka operacyjnego, ryzyka braku zgodności oraz zagrożeń i skutków procesu transakcji natychmiastowych nie może zostać przeprowadzona w oderwaniu od środowiska biznesowego i technologicznego w konkretnej instytucji finansowej. Powinna też ona objąć użytkowników i pośredników uczestniczących w realizacji całego procesu.

Z tego powodu przedstawione w tab. 1 obszary i czynniki ryzyka oraz środki zaradcze wymagają rozwinięcia i uszczegółowienia w trakcie zintegrowanej analizy ryzyka, która powinna towarzyszyć okresowej ocenie tego kanału w każdym banku.

Tab. 1. Wybrane obszary ryzyka operacyjnego i ryzyka braku kontroli szczególnie narażone na zagrożenia z tytułu transakcji natychmiastowych

Obszar ryzyka	Zakres ryzyka	Zakres analizy ograniczającej ryzyko wynikające z przelewów natychmiastowych (sfery wymagające szczególnej oceny)
ryzyko braku kontroli	• spóźniona reakcja na zagrożenie, wynikająca z tempa przebiegu procesu • nieadekwatne do szybkości procesu mechanizmy kontrolne	• automatyzacja procesu typowania (wyłapywania) podejrzanych operacji • monitoring on-line wszystkich transakcji natychmiastowych • wychodzenie z monitorowaniem poza strukturę informatyczną banku – interakcja z infrastrukturą IT klienta
działania nieautoryzowane	• nieuprawniony dostęp do systemów IT	• zapewnienie bezpieczeństwa systemów banku przed atakiem z wewnątrz lub z zewnątrz • analiza i archiwizacja logów i matryc dostępu • jakość reakcji na naruszenia procedur bezpieczeństwa i przekraczanie uprawnień

ryzyko procesowe	• błędy w procesach transakcyjnych	• ocena skutków finansowych w przypadku opóźnienia wykonania przelewu natychmiastowego: ○ roszczenia odszkodowawcze klienta ○ straty reputacyjne banku
praktyki zatrudnienia, bezpieczeństwo miejsca pracy	• zatrudnianie niewłaściwych pracowników w obszarach przeciwdziałania oszustwom	• oszacowanie wiedzy specjalistycznej personelu banku w zakresie przeciwdziałania i reagowania na cyberataki • ocena umiejętności pracowników w zakresie „miękkiej" komunikacji z klientami-ofiarami ataków i pozyskania ich do współpracy z bankiem w celu zabezpieczenia dowodów, w tym nieznanego szkodliwego oprogramowania lub form działania sprawców
oszustwa wewnętrzne i zewnętrzne	• korupcja personelu • niski poziom świadomości klientów w zakresie samoobrony przed atakiem na własny sprzęt informatyczny • powolne procedury reakcji na cyberataki	• ocena słabości systemu doboru i kontroli pracowników posiadających dostęp do wrażliwych danych • ocena zakresu i form komunikowania klientom stanu zagrożenia oraz sygnalizowania bankowi ataków • ocena jakości i zakresu współpracy z innymi bankami, przede wszystkim przy wykorzystaniu specjalistycznych systemów powiadamiania, zespołów zagadnieniowych Związku Banków Polskich i sieci osób kontaktowych
ryzyko braku zgodności (*Compliance*)	• reakcja na atak lub działania ograniczające jego skutki prowadzone w sposób naruszający prawo	• ocena podatności na niezgodne z wymogami prawa i regulacjami banku działania związane z wymianą informacji z innymi instytucjami finansowymi lub organami ścigania (tzw. informacje operacyjne) • ocena zawartości umów z klientami pod kątem ich adekwatności do działań ograniczających ryzyko kradzieży środków przez hackerów wykorzystujących przelewy natychmiastowe • ocena ryzyka strat finansowych i reputacyjnych z powodu niedotrzymania terminów realizacji transakcji
bezpieczeństwo personelu i zasobów	• zagrożenia pracowników banku szantażem lub atakiem ze strony	• ocena systemu sygnalizowania zagrożeń przez pracowników i procedur zwiększających ich bezpieczeństwo osobiste oraz zasady raportowania zagrożeń organom ścigania

Niektóre z zaproponowanych powyżej sfer zintegrowanej analizy ryzyka, która następnie posłuży do budowy planu, zostało sformułowanych na podstawie doświadczeń zdobytych w trakcie budowy systemu przeciwdziałania przestępstwom cybernetycznym w dużym polskim uniwersalnym banku komercyjnym.

Wprowadzenie oferty przelewów natychmiastowych nastąpiło w warunkach istnienia sprawnej struktury organizacyjnej, ukierunkowanej na przeciwdziałanie tej formie przestępczości. Jednostka koordynująca te działania od dawna szeroko współpracowała ze wszystkimi liniami biznesowymi oraz strukturami sprzedaży i operacji. Praktyka wykazała jednak, że ochrona procesu przelewów natychmiastowych wymagała modyfikacji szeregu procedur wewnętrznych, rozwinięcia współpracy międzybankowej prowadzonej pod auspicjami ZBP oraz wdrożenia nowych narzędzi informatycznych umożliwiających automatyzację generowania alertów o podejrzanych transakcjach.

Wśród zagadnień wzbudzających szczególną uwagę znalazła się kwestia zakresu kontroli, jaką bank może wykonywać w celu wykrywania szkodliwego oprogramowania umieszczonego przez hackerów na urządzeniach używanych przez klientów do realizacji płatności. Dążąc do ograniczenia ryzyka obu stron – klienta i banku – docieramy do delikatnej granicy poszanowania prywatności. Interakcja banku z infrastrukturą IT klienta, prowadząca do ustalenia symptomów działania szkodliwego oprogramowania, wymaga jeszcze dodatkowych uregulowań prawnych. Sam fakt oraz zakres sondowania stacji, z której dochodzi do logowania do systemu banku powinien być określony w umowie z klientem.

Istotne znaczenie dla prawidłowych relacji pomiędzy bankiem a klientem korzystającym z przelewów natychmiastowych ma sprawa opóźnień w realizacji transakcji spowodowanych koniecznością analizy przypadku podejrzenia, że transakcja została wykonana bez wiedzy klienta. W sytuacji, gdy z różnych względów, leżących najczęściej po stronie zlecającego przelew, nie ma możliwości kontaktu telefonicznego klient może rościć wobec banku żądania zwrotu utraconych korzyści, które mógłby uzyskać, gdyby transakcja została przeprowadzona bezzwłocznie. Przykładem takich strat mogą być transakcje związane z wymianą znacznych kwot walut w kantorach internetowych.

Z drugiej znów strony klienci, którzy padli ofiarą cyberprzestępców wygłaszają opinie, że bank nie dołożył należytej staranności, aby zadbać o bezpieczeństwo ich pieniędzy.

Wymienione powyżej ryzyka wskazują na potrzebę dokonania zmian w warunkach świadczenia przelewów elektronicznych poprzez uszczegółowienie zapisów odnoszących się do przelewów natychmiastowych. Umożliwi to istotne obniżenie ryzyka strat z tytułu przegranych procesów z klientami zarówno o charakterze finansowym, jak również reputacyjnym.

Ważnym czynnikiem ograniczającym wysokość strat jest identyfikacja szkodliwego oprogramowania, Trojana lub wirusa wprowadzonego do komputera potencjalnej lub rzeczywistej ofiary. Wielu klientów obawia się udostępnienia specjalistom z banku lub firmom wynajętym przez banki dostępu do ich sprzętu IT, wychodząc z założenia, że jeśli bank potwierdzi istnienie wirusa to w konsekwencji doprowadzi to do odmowy zwrotu skradzionych środków. Taka sytuacja stwarza zagrożenie, że bank, nie wiedząc czym dysponują przestępcy, traci możliwość odpowiedniego rozpoznania charakteru ataku i zabezpieczenia przed jego skutkami innych klientów.

Dlatego tak ważne są umiejętności pracowników wyspecjalizowanych w zwalczaniu zagrożeń dla bankowości internetowej w zakresie „miękkiej" komunikacji z klientami-ofiarami ataków i zachęcenia ich do współpracy z bankiem w celu pozyskania próbki szkodliwego oprogramowania do dalszych analiz. Intensywne szkolenia bankowych specjalistów IT w tym zakresie spowodowały niemal stuprocentową skuteczność w uzyskiwaniu zgód klientów.

W publikacjach poświęconych metodom działania cyberprzestępców autorzy wielokrotnie przywołują przykłady psychotechnik stosowanych przez hackerów, usiłujących nakłonić swoje przyszłe ofiary do wykonania czynności umożliwiających dokonania przestępstwa. Psychotechnika, jako nauka praktyczna stosowana zgodnie z prawem i zasadami etyki, może znaleźć zastosowanie w celu uzyskania pożytecznej zmiany w postawach i zachowaniach klientów. Umiejętnie budowane programy uświadamiające klientom zagrożenia oraz wskazujące pożądane przez instytucje finansowe formy zachowań ostrożnościowych mogą stanowić skuteczną formę przeciwdziałania zagrożeniom w bankowości elektronicznej, w tym tych wynikających z wprowadzenia przelewów natychmiastowych. Skuteczność kampanii informacyjnych dla klientów jest większa, jeżeli w jej propagowaniu uczestniczy wiele banków. Dobry przykład w tym zakresie stanowią komunikaty Rady Bankowości Elektronicznej (RBE) czy Związku Banków Polskich (ZBP) dotyczące nowych zagrożeń dla klientów korzystających z bankowości elektronicznej, które są publikowane w systemie SWOZ (System Wczesnego Ostrzegania o Zagrożeniach).

W dziale „Dla Klientów" → „Bezpieczny Bank" → „Aktualności" można odnaleźć szereg linków odnoszących się do najbardziej aktualnych zagrożeń związanych m.in. ze szkodliwym oprogramowaniem, atakujących klientów korzystających z przelewów natychmiastowych.

Należy tu uwzględnić komunikaty dotyczące Trojana Banapter podmieniającego rachunki bankowe wklejane ze „schowka"[1] oraz ostrzeżenia dla klientów wykorzystujących karty mikroprocesorowe do uwierzytelniania przelewów przez Internet[2], a także wskazówki jak korzystać z przelewów błyskawicznych oferowanych przez podmioty niebędące bankami czy też sposobów zabezpieczenia przed atakiem routerów bezprzewodowych Wi-Fi.

Szczególnie interesującą formą informowania obywateli, a wśród nich klientów banków, o zagrożeniach w cyberprzestrzeni są rządowe portale informacyjne przygotowywane we współpracy administracji z instytucjami komercyjnymi oraz organizacjami pozarządowymi.

W wielu krajach europejskich i w USA agencje rządowe prowadzą specjalne strony internetowe zawierające wskazówki dotyczące bezpieczeństwa transakcji bankowych wykonywanych za pośrednictwem sieci. Takie porady można znaleźć też na stronach polskiej policji. Autorzy tych portali, kierując się hasłem „zbyt piękne, żeby było prawdziwe", zamieszczają opisy zuchwałych ataków i ogólne rady jak się przed nimi ustrzec.

Jednak szczególnie ciekawym przykładem nowoczesnej, ciekawej i łatwej w odbiorze edukacji jest brytyjska strona internetowa przygotowana w ramach międzyresortowego programu bezpieczeństwa pod nazwą „*Be Cyber Streetwise*".[3]

Kampania informacyjna sfinansowana została przez Narodowy Program Bezpieczeństwa Cybernetycznego (*The National Cyber Security Programme*). Materiały dydaktyczne dostarczyły prywatne firmy z różnych sektorów gospodarki. Całym przedsięwzięciem kieruje Ministerstwo Spraw Wewnętrznych (*Home Office*) wraz z wyspecjalizowaną agendą rządową ds. rozwoju (*The Department for Business, Innovation & Skills*) oraz *Cabinet Office* będącym odpowiednikiem polskiego Urzędu Rady Ministrów. Celem kampanii jest istotne ograniczenie zagrożeń i poprawa bezpieczeństwa zachowań klientów indywidualnych i drobnych przedsiębiorców.

---

1 http://zbp.pl/dla-konsumentow/bezpieczny-bank/aktualnosci/komunikat-trojan-banapter

2 http://zbp.pl/dla-konsumentow/bezpieczny-bank/aktualnosci

3 www.cyberstreetwise.com

Bezwzględność i skuteczność ataków na klientów banków, często o charakterze transgranicznym, oraz ograniczone w aktualnym stanie prawnym możliwości mogą wywoływać u pracowników zajmujących się ograniczaniem tego ryzyka frustrację i budzić pokusę wykorzystania nieformalnych środków przeciwdziałania. W ramach analiz wykonywanych przez jednostki odpowiedzialne w bankach za zapewnienie zgodności (*Compliance*) powinny być systematycznie prowadzone oceny zagrożeń związanych z monitorowaniem i wymianą informacji o przestępczych transakcjach natychmiastowych z innymi podmiotami i organami ścigania. Nie chodzi tu oczywiście o stwarzanie barier ograniczających uprawniony przepływ informacji, ale o zapewnienie zgodności z prawem i właściwie rozumianą ochroną interesów banków i klientów. Pisząc o udziale funkcji *Compliance* w ograniczaniu ryzyka związanego z przelewami natychmiastowymi warto zwrócić uwagę, że w istotny sposób ograniczają one możliwość realizacji blokad Generalnego Inspektora Informacji Finansowej zlecanych bankom w ramach ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu. Często decyzja o blokadzie środków dociera do banku w chwili, gdy konto zostało już opróżnione poprzez przelewy natychmiastowe.

Nowe produkty bankowe – nowe wyzwania

Wprowadzenie przelewów natychmiastowych spowodowało istotny wzrost strat banków z tytułu zwrotu środków skradzionych klientom, którzy dopuścili do zarażenia ich sprzętu Trojanami lub wirusami albo padli ofiarą wyrafinowanych socjotechnik. Obecnie w krajach Unii Europejskiej wyraźnie wyodrębniają się dwa rozbieżne nurty rozpatrywania reklamacji poszkodowanych klientów.

Pierwszą, znaczną liczebnie tworzą banki zwracające klientom zagrabione im poprzez oszukańcze przelewy środki finansowe. Kierownictwo tych banków wychodzi z założenia, że dostarczając klientom kanał transakcji internetowych ponosi odpowiedzialność biznesową za ich bezpieczeństwo. Broniąc swojej reputacji godzą się na ponoszenie strat. Do tej grupy instytucji finansowych należą najczęściej duże banki, które dzięki wprowadzeniu efektywnych systemów wykrywania i reakcji nie doświadczyły szczególnie skutecznych ataków hackerskich.

Druga grupę tworzą banki, których zarządy stoją na stanowisku, że przestępcy, wykorzystujący szkodliwe oprogramowanie mogli wyprowadzić środki z rachunku bankowego tylko w wyniku interakcji z klientem lub zainfekować jego niewłaściwie zabezpieczony przed wirusami sprzęt. Zaistniałą kradzież wiążą jednoznacznie z brakiem dochowania przez klienta należytej staranności w zakresie bezpieczeństwa własnych zasobów, zapewniając, że po analizie nie stwierdzono naruszenia zabezpieczeń banku.

Oba podejścia generują problemy spowodowane stratami finansowymi, procesami sądowymi lub ryzykiem utraty reputacji. Dotychczas brak jest jednoznacznych regulacji prawnych uzasadniających wybór jednej z wyżej opisanych opcji rozpatrywania reklamacji klientów. Dlatego szczególnie istotne znaczenie ma dokonanie przeglądu i ewentualnej renegocjacji warunków umów z klientami pod kątem adekwatności zapisów dotyczących kradzieży środków przez hackerów wykorzystujących przelewy elektroniczne.

Przelewy natychmiastowe – nowy kanał, stare formy przestępstw

Przelewy elektroniczne z kont klientów indywidualnych i korporacyjnych pozostają jednym z głównych narzędzi, jakimi posługują się doskonale zorganizowane i działające w sferze międzynarodowej grupy przestępcze. Hackerzy systematycznie udoskonalają kolejne wersje szkodliwego oprogramowania, podnoszą jakość oszukańczych stron internetowych i formułują bardziej przekonywujące komunikaty kierowane do ich potencjalnych ofiar. Do czasu wprowadzenia przelewów ekspresowych straty banku zależały przede wszystkim od efektywności jednostki zwalczania nadużyć i jakości współdziałania z innymi bankami kooperującymi w zabezpieczaniu wytransferowanych nielegalnie środków. W efekcie banki nie inwestowały w systemy monitorujące a raczej rozwijały współpracę międzybankową w celu podniesienia skuteczności blokad. Istotne znaczenie odgrywał czas przetrzymywania środków na koncie „słupa". Z dużym prawdopodobieństwem można było założyć, że znaczna część skradzionych środków zostanie zabezpieczona przed ich wyprowadzeniem poza systemy krajowych instytucji finansowych. Niskie straty rzeczywiste ograniczały apetyty zarządów na zakup systemów informatycznych monitorujących na bieżąco wszystkie transakcje elektroniczne.

Doświadczenia jednego z dużych polskich banków wskazują, że przelewy ekspresowe całkowicie zmieniły ten stan.

W latach 2009–2010 środki skradzione w wyniku oszukańczych przelewów elektronicznych zostały w 100% odzyskane po wcześniejszym zablokowaniu ich na kontach bankowych.

W latach 2011–2012 odzyski spadły wprawdzie o 3%, ale to ze względu na przelewy do małych banków lub instytucji parabankowych, które nie współpracują z bankami przy blokowaniu zagrabionych pieniędzy.

Jednak w roku 2013 po wprowadzeniu przelewów błyskawicznych procentowy odzysk zmniejszył się o 79%, a w pierwszych dwóch miesiącach 2014 roku spadł do 78%. Średni czas wypłaty środków skradzionych z krajowego banku w 2013 roku skrócił się do 11 minut.

Jakość ataków zdolnych do pokonania zabezpieczeń powiązanych z uwierzytelnieniem użytkownika kartą chip lub tokenem spowodowała, że w fazie największego nasilenia ataku zachodziła potrzeba czasowego ograniczenia dostępności jednego z systemów, aby umożliwić pełną weryfikację zlecanych transakcji natychmiastowych. Ataki te wykonują zorganizowane grupy wysoko wyspecjalizowanych hackerów, którzy nierzadko są ekspertami w zakresie programowania i łamania zabezpieczeń.

Umożliwienie klientom dokonywania transakcji natychmiastowych nie wywołało żadnych zmian w procedurach reakcji i prowadzenia postępowań przez organy ścigania. Szczególne znaczenie ma tu czas podejmowania decyzji przez prokuratury o blokadach środków na kontach pośredników. Ponieważ część tych pieniędzy przekazywana jest na konta w innych krajach, wnioskowanie o blokady w ramach wniosków o międzynarodową pomoc prawną dodatkowo obniża szanse na skuteczny zwrot skradzionych pieniędzy poszkodowanym.

Cyberprzestępcy szybko docenili zalety przelewów natychmiastowych szczególnie przy atakach wymierzonych w średniej wielkości klientów firmowych, dysponujących na kontach znacznymi kapitałami, lecz nieprzywiązującymi dostatecznej wagi do zabezpieczenia sprzętu i procedur bezpieczeństwa przy realizacji przelewów elektronicznych. Sondaż wśród klientów wskazuje, że wprowadzenie limitu kwot dopuszczonych do natychmiastowego transferu byłoby odczytane jako przejaw słabości banków i zachęcało do korzystania z systemów pozabankowych.

Dokąd zmierzamy

Dążąc do ograniczenia skutków ataków z wykorzystaniem elektronicznych transferów, zarówno błyskawicznych, jak i tradycyjnych, warto skupić wysiłki ZBP i poszczególnych banków na:

- Doskonaleniu mechanizmów aktywnej współpracy i wymiany informacji między partnerami z sektora bankowego, firm informatycznych, administracji rządowej, organów ścigania i wymiaru sprawiedliwości. Banki muszą być przygotowane kadrowo i technologicznie do szybkiego rozpoznawania i ograniczenia ataku. Administracja rządowa powinna wspierać ochronę systemu bankowego jako elementu infrastruktury krytycznej państwa.
- Delegowaniu uprawnień do podejmowania decyzji w zakresie reakcji na atak na niskie szczeble kompetentnej struktury banku. Potrzeba szybkiego reagowania to jedna z ważnych lekcji wyciągniętych z zaistniałych ataków. Pracownicy zarządzający systemami monitorowania systemów transakcyjnych mają bardzo mało czasu na rozpoznanie ataku i podjęcie działań ograniczających. Ich decyzje zyskują czas na uruchomienie wcześniej przygotowanych procedur ostrzegania klientów oraz neutralizację szkodliwego oprogramowania.
- Dzieleniu się informacjami pomiędzy sektorem bankowym i publicznym jest kluczowym czynnikiem sukcesu, pomimo że istniejące ograniczenia prawne, biznesowe i kulturowe tworzą ku temu szereg barier. Niekiedy banki obawiają się utraty pozycji rynkowej, jeśli publicznie przyznałyby, że ich klienci padli ofiarami zmasowanego ataku hackerskiego. Nawet dzielenie się informacjami o zastosowanych środkach obrony wzbudza obawy, bo takie informacje mogłyby zostać wykorzystane przy przełamywaniu zabezpieczeń.
- Doskonaleniu form współpracy pomiędzy bankami, organami ścigania i administracji rządowej. Rozszerzanie już funkcjonujących struktur, jak np. konferencje w WSP w Szczytnie, jest metodą na budowę zaufania i dzielenia się przez banki wiedzą o nowych zagrożeniach. Na takich forach buduje się z biegiem czasu zaufanie wypracowywane dzięki dobrej współpracy w konkretnych sprawach. Konkurujące banki przynoszą większe dochody dzięki temu, że wspólnie rozwiązują problemy zanim ich słabe punkty zostaną wykorzystane przez przestępców.

Podsumowanie

Nadrzędnym wyzwaniem dla banków związanym z przeciwdziałaniem cyberprzestępczości, a w tym również przestępstwom natychmiastowym jest doskonalenie standardowych praktyk współpracy i wymiany doświadczeń, systematyczne rozwijanie zaawansowanych technologicznie systemów obronnych i analitycznych oraz lobbowanie na rzecz zmian w prawie krajowym i dobrego wykorzystania przez polski rząd międzynarodowych konwencji, których stroną jest nasz kraj.

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

Andrzej Sieradz
Wiceprezes Zarządu Banku BGŻ. Ukończył Politechnikę Warszawską. 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, 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, obsługi klienta oraz zarządzanie projektami. W latach 2002–2006 związany z ING Bank Śląski S.A., najpierw jako dyrektor zarządzający. W latach 1997–2002 piastował stanowiska kierownicze w Coca-Cola Beverages Polska sp. z o.o.

Grzegorz Kuliszewski, IBM
Andrzej Sieradz, Bank BGŻ

Przyszłość centralnych systemów bankowych

Zanim systemy centralne oparte na zaawansowanych systemach teleinformatycznych na dobre pojawiły się w bankowej rzeczywistości, instytucje bankowe zachowywały się podobnie jak inne przedsiębiorstwa. Pod koniec tygodnia po prostu zamykały swoje „okienka bankowe", aby znowu je otworzyć w poniedziałek rano. Klienci w tamtych czasach byli przyzwyczajeni do „chodzenia do banku" i to najczęściej do jednego oddziału. Szef Finansowy lub Główny Księgowy niejednego przedsiębiorstwa traktował wizytę w banku jako niezbywalną część swojej aktywności zawodowej. Wszystkim, jak dziś, była potrzebna bankowość i banki, a raczej oddziały banku. W tamtych czasach, nie tak znowu odległych, oddziały banku opierały swój model biznesowy wyłącznie na sieci swoich oddziałów. Oprócz tradycyjnych okienek banki posługiwały się dokumentami papierowymi a przelewy między bankami potrafiły „wędrować" nawet tygodniami. Stopniowo jednak, z chwilą pojawienia się najpierw terminali a następnie komputerów osobistych, sytuacja zaczęła się zmieniać. Początkowo technologia informatyczna pojawiała się w oddziałach banku traktowanych jako niezależne części banku. W przypadku polskiego rynku bankowego system oddzielnych systemów oddziałowych został np. wdrożony w 1998 roku w Banku Śląskim. Chodziło tu o system firmy Fiserv, którego implementację rozpoczęto w roku 1994. Jego budowa przebiegała w dwóch etapach. Na początku utworzono dziewięć rejonowych systemów IT. Jeden z rejonów, nazywany rejonem centralnym, został zbudowany jako baza dla zamierzonej w następnym etapie konsolidacji. Sam proces centralizacji w jeden skonsolidowany system na koniec 1998 roku obsługiwał on-line ponad 200 oddziałów Banku oraz prawie 300 bankomatów.

Centralizacja systemów IT była bardzo widoczna dla klientów banków na przełomie XX i XXI wieku i dotyczyła głównie systemów ewidencyjno-księgowych, z których korzystały banki. Lata 90. to bardzo ciekawy czas w polskiej bankowości – era systemów centralnych. I mimo że tak naprawdę to ona ukształtowała naszą bankowość, jej wystąpienie bezpośrednio wynika ze zmian ustrojowych, jakie zaszły w Polsce.

Kluczem do zmian, jakie nastąpiły był podział Narodowego Banku Polskiego w 1989 roku, kiedy to powstały:

- Państwowy Bank Kredytowy w Warszawie (PBK, ob. Bank BPH),
- Bank Przemysłowo-Handlowy w Krakowie (BPH, ob. Bank BPH),
- Bank Śląski w Katowicach (BŚ, ob. ING Bank Śląski),
- Wielkopolski Bank Kredytowy w Poznaniu (WBK, ob. Bank Zachodni WBK),
- Pomorski Bank Kredytowy w Szczecinie (ob. Bank Polska Kasa Opieki),
- Bank Depozytowo-Kredytowy w Lublinie (ob. Bank Polska Kasa Opieki),
- Powszechny Bank Gospodarczy w Łodzi (PBG, ob. Bank Polska Kasa Opieki),
- Bank Gdański S.A. (BG, ob. Bank Millennium),
- Bank Zachodni we Wrocławiu (BZ, ob. Bank Zachodni WBK),

a następnie rozpoczęta w 1992 roku prywatyzacja poszczególnych banków wraz z przejęciem znaczących pakietów przez banki międzynarodowe.

Prawdziwa rewolucja w bankowości pojawiła się wtedy, gdy możliwe stało się scentralizowanie systemów księgowych. Z czasem, przy modułowej budowie systemu, można by było porównać je do systemów ERP, które równolegle zaczęły się pojawiać w przedsiębiorstwach. Bezpośrednimi przyczynami popularności systemów centralnych w tamtym okresie były udogodnienia dla klienta:

- odmiejscowienie rachunku bankowego, co umożliwiało klientom obsługę konta bankowego w dowolnym oddziale banku,
- zwiększenie szybkości przesyłania płatności i środków pomiędzy bankami,
- powszechne zakładanie kont typu ROR dla pracowników, co zmniejszało koszty przedsiębiorstw związanych z procesem wypłat wynagrodzeń.

Po stronie banku wprowadzenie systemu centralnego umożliwiało bankom:

- adresowanie rosnącej kompleksowości bankowości detalicznej i korporacyjnej,
- prowadzenie księgowości bankowej, specyficznej dla banku i operacji wykonywanych w banku,
- księgowanie dzienne operacji klienta i stanu jego kont oraz kont, które go obsługują po stronie banku,

- zmniejszenie pracochłonności wewnętrznej banków przy wzrastającej na początku lat 90. aktywności gospodarczej Polaków.

Pierwsze wdrożenia adresowały głównie potrzeby banków w początkowym okresie modernizacji sektora bankowego w Polsce. Należy jednak pamiętać, że technologie informatyczne tamtego okresu odnosiły się do jedynego znanego w tamtym czasie kanału dystrybucji, jakim były oddziały banku. Rewolucja, która pojawiła się w bankowości z chwilą upowszechniania się internetu i telefonii mobilnej spowodowała zupełnie inne wymagania do bankowych systemów centralnych.

Wdrożenia systemów centralnych

Bankowy system centralny pełni w banku funkcję „serca". Jest to główne i jedyne miejsce, gdzie przechowywane są dane dotyczące klienta, depozytów, kredytów i większości transakcji. Odpowiada również za wszystkie interakcje pomiędzy danymi banku i innymi uczestnikami rynku. Głównym celem początkowym było zbieranie informacji o klientach i ich rachunkach, by łatwiej nimi zarządzać. Pozytywnym skutkiem tej centralizacji, istotnym zwłaszcza dla klientów banków, było odmiejscowienie rachunków, czyli ich uniezależnienie od fizycznego umiejscowienia w konkretnej jednostce organizacyjnej banku. Pionierem w tej dziedzinie był Bank Rozwoju Eksportu SA, który w 1992 roku wdrożył system scentralizowany, a tym samym uniezależnił klienta od konkretnego oddziału.[1]

Systemy informatyczne dostępne w polskich bankach na początku lat 90. były jednorodne i nakierowane na obsługę księgową operacji w pojedynczym oddziale banku. Zostały one stworzone wewnętrznymi siłami banku lub pochodziły od krajowych dostawców. Wykonywanie operacji między oddziałami było utrudnione, a odmiejscowienie rachunków nie istniało.

Wchodzący kapitał zagraniczny przynosił ze sobą doświadczenia z Europy, gdzie korzystano z osobnych systemów kredytowych i depozytowych, dostępnych jednakowoż w ramach całego banku. Transakcje pomiędzy nimi były powolne – rozliczenia następowały z kilkudniowym opóźnieniem. Tymczasem w Polsce, w związku z powstałą w 1991 roku Krajową Izbą Rozliczeniową, rozliczenia międzybankowe realizowane jednego dnia stały się oczekiwanym przez rynek standardem. Wobec braku dobrych wzorców, zarówno

1 W. Chmielarz, *Komputer i bank*, Warszawa, 1997 r.

krajowych, jak i europejskich, większość banków zdecydowała się na wdrożenie niesprawdzonych w Europie gotowych rozwiązań, opartych o bankowość anglosaską i proponowanych przez firmy międzynarodowe.

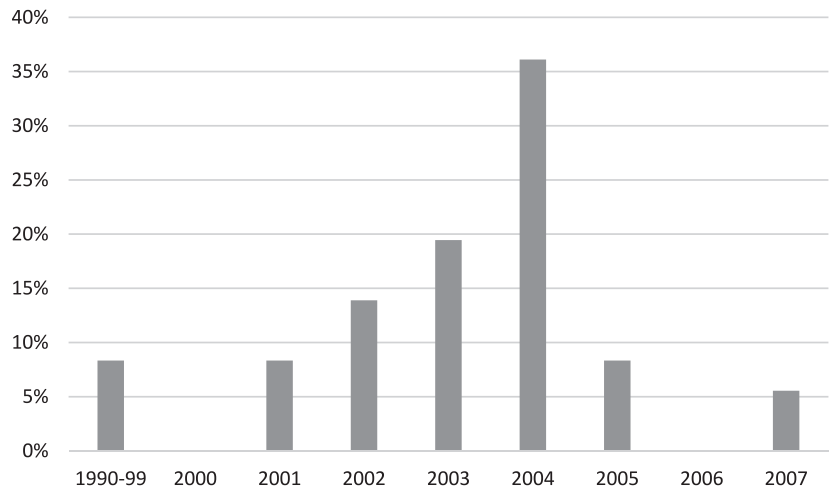
Projekty wdrożeniowe nie były łatwe. Przeciętnie przekraczały początkowo zakładany harmonogram o cztery lata, a budżet czterokrotnie. Wśród kluczowych przyczyn takiego stanu rzeczy należałoby wskazać:

- brak doświadczenia banków we wdrażaniu tak dużych rozwiązań informatycznych,
- przyzwyczajenia pochodzące z systemów oddziałowych, stawiające na pierwszym miejscu aspekty księgowe, prowadzące do ogromnej liczby modyfikacji do funkcjonalności,
- chęć posiadania w nowym systemie wszystkich produktów obecnie wykorzystywanych oraz posiadanych przez konkurencyjne banki, co prowadziło do niesamowitego wzrostu zakresu wdrożeń,
- unikatowe dla rynku polskiego rozwiązania produktowe – w tym przede wszystkim ROR z linią kredytową,
- ograniczoną świadomość dla ogromu zmian organizacyjnych i procesowych, wynikających z wdrożenia systemu centralnego, w tym przede wszystkim:
  - drastycznego ograniczenia roli back-office'u w oddziałach i związanego z tym zmniejszenia wielkości zatrudnienia w pojedynczym oddziale z 50–100 osób w 1990 roku do kilkunastu 10 lat później,
  - wzrostu znaczenia front-office'u w oddziałach i odwrócenia trendu, w którym awansem w banku było przejście z lady na zaplecze,
  - braku gotowości departamentów biznesowych centrali do przyjęcia wykonalności informatycznej jako istotnego parametru podczas budowania nowych produktów,
  - konieczności znaczącego wzrostu wiedzy o działaniu systemu informatycznego w departamentach biznesowych centrali.

Początkowe wdrożenia systemów centralnych, podobnie jak systemów klasy ERP na początku lat 90., przewidywały cykl życia systemu w granicach 12–15 lat. Niestety, w miarę pojawiania się nowych wymagań, zarówno biznesowych, jak i regulacyjnych, banki miały do wyboru dwie drogi. Unikać drogich i długotrwałych upgradów i modyfikacji systemów centralnych albo adresować nowe wymagania poza systemami centralnymi, integrując aplikacje biznesowe z wykorzystaniem narzędzi typu *middleware*.

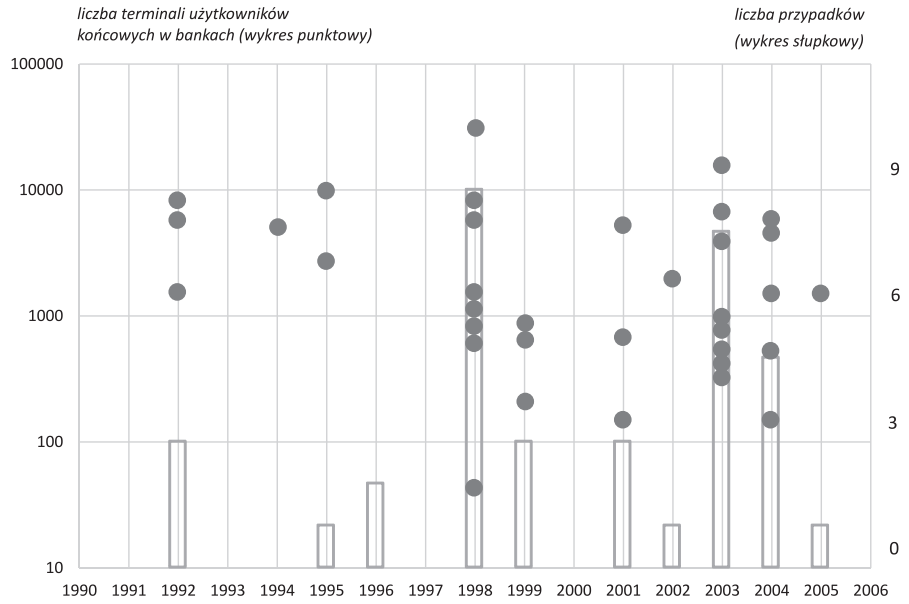
Powszechnie wybierano tańsze i szybsze rozwiązania, co spowodowało traktowanie systemu centralnego jako *„back-office'u"* aplikacji bankowych przeznaczonych do obsługi np. wielokanałowości. Doprowadzało to do konieczności albo wymiany lub unowocześnienia systemu centralnego. Na rys 1. zaprezentowano rozkład takich migracji. Największa ich liczba przypada na lata 2003–2004. Drugim efektem tych migracji było zmniejszenie się grupy systemów na rynku polskim.

Rys. 1:
Migracje aplikacji krytycznych w bankach według daty wymiany (1990–2007)



Źródło: DiS, 2008 (100% = 36 przypadków)

Rys. 2:
Migracje krytycznych aplikacji bankowych w funkcji wielkości banków i lat eksploatacji w okresie 1990–2006



Źródło: DiS, 2008

Jak wynika z rys. 2, zdecydowana większość systemów centralnych w polskiej bankowości jest wykorzystywana już od 8–15 lat.

Problemy, na jakie natknęły się pierwsze banki wdrażające systemy centralne istotnie wpłynęły na procesy przetargowe w kolejnych. Wymagania dotyczące referencji z wdrożeń w Polsce, zgodności z regulacjami księgowymi oraz wsparcia funkcjonalnego dla ROR'u z linią kredytową spowodowały, że obecnie na polskim rynku reprezentowanych jest zaledwie kilka systemów:

- Profile – Bank BPH, Alior Bank, Kredyt Bank,
- Alnova – PKO Bank Polski, Pekao SA, mBank,
- Fileserv – Bank Millennium, Bank Zachodni WBK, ING Bank Śląski,
- Temenos – Raiffeisen Bank, mBank, Nordea Polska,
- Def 3000 – Getin Bank, BOŚ Bank.

Co interesujące, jedynie ostatni jest produkcji krajowej.

Proces wdrażania systemów centralnych zakończył się ok. 2005 roku (porównaj rys. 2). Podobny czas wdrożenia systemów doprowadził do stworzenia pewnego wspólnego standardu, który pozwolił na powszechne udostępnienie następujących funkcjonalności:

- możliwość realizacji operacji w każdej placówce banku (odmiejscowienie rachunku),
- utrzymywanie w czasie rzeczywistym salda księgowego i dostępnego rachunków klienta (co najmniej w czasie dnia),
- wykonywanie transakcji w ramach jednego banku w czasie rzeczywistym,
- wykonywanie transakcji pomiędzy bankami w ramach jednego dnia biznesowego (przy udziale mechanizmów zapewnionych przez KIR).

Polska bankowość na początku XXI wieku zaliczała się do najnowocześniejszych na świecie, oferując klientowi informację, wygodę i prędkość dokonywania operacji niespotykaną w krajach bardziej rozwiniętych.

Nowe kanały dystrybucji (internet, IVR, mobile banking)

To, co było przewagą konkurencyjną polskiej bankowości 10 lat temu, dziś powoli staje się ograniczeniem jej rozwoju. Wdrażane rozwiązania zakładały, że centralne systemy bankowe będą obsługiwały wszystkie produkty i całość potrzeb klienta – jedynym „zewnętrznym" produktem działającym w trybie 24/7 była wówczas karta płatnicza i obsługa sieci bankomatów.[2] Ekspansja dodatkowych kanałów dystrybucji, najpierw IVR'u i bankowości internetowej, a następnie bankowości mobilnej i płatności P2P ukazały niedoskonałość architektury systemów centralnych.

Wiele systemów, wobec wielości kanałów wejściowych, ma problem z utrzymywaniem salda dostępnego szczególnie podczas operacji przetwarzania nocnego. Dodatkowo integracja poszczególnych kanałów z systemem centralnym w celu standaryzacji wymaga wdrożenia szyny danych. Obecnie wymagania dotyczące wielokanałowości powodują stawianie przed bankami kolejnych wyzwań. Dostępność usług w trybie 24/7 oznacza w praktyce, że bank nigdy nie jest zamknięty. Im bardziej scentralizowany staje się cały system informatyczny banku, tym bardziej rośnie ryzyko związane z przetwarzaniem danych.

2 Obecnie bankomaty w większości mniejszych banków są outsource'owane.

Dziś nie mamy już banków, które nie posiadałyby rozwiązań umożliwiających obsługiwanie klientów bez przerw. Ośrodki zapasowe z głównymi aplikacjami, w tym systemem centralnym, rozwiązania telekomunikacyjne, czy wsparcie techniczne on-line są dziś niekwestionowaną potrzebą biznesową. Bankowość jest dziś dostępna w dowolnym czasie i z dowolnego miejsca na świecie.

To rodzi pytanie, jak poradzić sobie np. z tradycyjnym zamknięciem dnia, które łączy się z tak podstawowym zadaniem, jak naliczanie odsetek od depozytów klientów, itp. Dodatkowo gwałtownie powiększa się grupa użytkowników systemu centralnego. Poza pracownikami banku są to teraz bezpośrednio klienci banku. To oznacza dodatkowe systemy wspierające do autentykacji i autoryzacji, a wraz z nimi skomplikowany system bezpieczeństwa operacyjnego banku związanego z codzienną działalnością operacyjną.

Tak więc, 10 lat po zakończeniu wdrożeń systemów centralnych, jesteśmy dokładnie tam, gdzie bankowcy z krajów Europy – mamy gmatwaninę systemów realizujących poszczególne operacje klienta, które są połączone, w najlepszym wypadku, szyną danych. Systemy centralne przestały pełnić rolę podstawowego repozytorium wiedzy o kliencie i są krok po kroku ograniczane do roli back-office'owego rejestratora operacji.

Równolegle presja konkurencyjna, w tym nowi gracze wchodzący do niektórych, wcześniej zarezerwowanych dla banków nisz, powodują ciągłą presję na rozwój systemów front-office'owych, rozwiązań wspierających analizę danych o kliencie, dynamiczne naliczanie opłat i prowizji, elastyczne taryfy czy personalizowany marketing zarówno w ruchu wchodzącym, jak i wychodzącym. Wszystkie powyższe elementy wpływają na znaczący wzrost kosztów funkcjonowania banków, niekoniecznie dając im możliwość dodatkowego przychodu.

Wzrost stopnia skomplikowania (poza transakcyjnością systemu centralnego)

Jednocześnie rosną oczekiwania klientów. Obecnie od banków oczekuje się dostępności 24/7, pełnej widoczności wszystkich operacji w czasie rzeczywistym, identycznej funkcjonalności niezależnie od kanału dostępu oraz transakcji w czasie rzeczywistym. Jednocześnie uniwersalność dostępu do banku powoduje poważne zagrożenia po stronie bezpieczeństwa nie tylko transakcji, ale również środków pieniężnych klientów.

Zagrożenia te wynikają także z przyspieszenia operacji (obecnie przy zastosowaniu tzw. Płatności Natychmiastowych przelew jest wykonywany i zaksięgowany po stronie odbiorcy w kilkadziesiąt sekund) oraz zagrożeń wynikających z cyberprzestępczości. Ponadto regulacje mające na celu ochronę przed tymi zagrożeniami powodują dodatkowy stopień skomplikowania systemów kontrolnych czy też zapasowych działających w czasie rzeczywistym. Klient po wykonaniu transakcji może natychmiast przekonać się, że została zaksięgowana.

Dodatkowym wyzwaniem dla systemów centralnych są wymagane obecnie wyrafinowane systemy autoryzacji i autentykacji klientów lub użytkowników systemu, które muszą ze sobą współpracować w czasie rzeczywistym. Przykładem takiej współpracy jest powszechnie wykorzystywany system potwierdzeń transakcji w kanale internetowym przy pomocy SMS-a. Ponadto zmieniają się zachowania klientów. Wzrasta częstotliwość interakcji z klientami banku przy pomocy kanałów zdalnych, co tym bardziej zwiększa nacisk na niezawodność i pełną dostępność systemów banków.

I co dalej

Problem wymiany bankowych systemów jest nie tylko problemem polskiego sektora bankowego. Penny Crosman z American Banker[3] ocenia, że wśród amerykańskich banków wiele wykorzystuje systemy zakupione blisko 30 lat temu, „obudowując je" rozwiązaniami na potrzeby bankowości internetowej i mobilnej.

Ocenia on, że wartość rynku systemów centralnych wzrośnie z 2,9 mld USD obecnie do 3,3 mld USD w 2017 roku i trend ten będzie kontynuowany w latach kolejnych. Banki poszukują teraz systemów „totalnie otwartych", ponieważ rozwiązania, które będą musiały wybrać, muszą przetrwać następnych 20–30 lat.

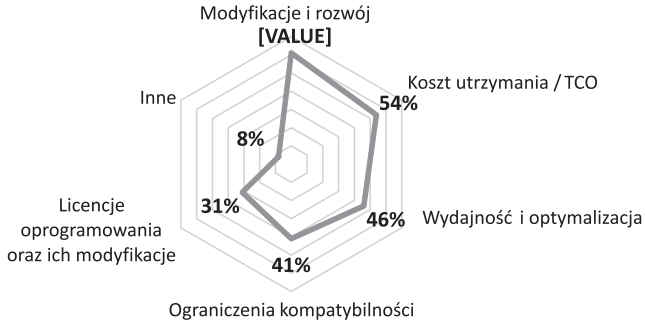
Systemy te muszą spełniać szerokie spektrum wymagań i będą „narażone„ nie tylko na integrację z systemami innych banków czy systemami rozliczeniowymi, ale także na konieczność uczestniczenia w procesach budowania wartości, same będąc niewidocznymi. Ponadto większość systemów centralnych wykorzystywanych w bankach po dzień dzisiejszy została zaprojektowana po koniec lat 70. ubiegłego wieku. Ich cechą wspólną jest to, że w większości zostały oparte o tradycyjne pojmowanie transakcji bankowej i wokół tego jest zbudowana ich funkcjonalność.

3 Crosman [2013], s. 1–4.

Ponieważ były projektowane, kiedy nie było wielokanałowości, koncentrowały się na definicji produktów i usług. Obecnie nowoczesne systemy bankowe muszą koncentrować się na kliencie i procesach związanych z jego obsługą lub aktywnością.

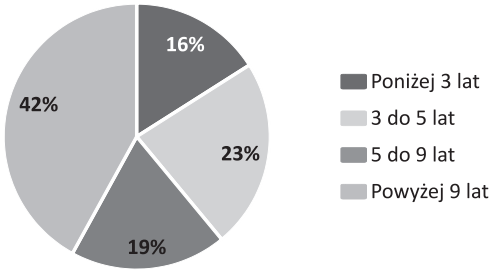
Banki będą musiały zderzyć się z tymi problemami wcześniej czy później. Zwykle trudno znaleźć powody biznesowe, które uzasadniałyby taką wymianę połączoną z ogromnymi kosztami i bardzo długim okresem przygotowania projektu. Taka decyzja jest odwlekana tak długo, jak się da. Na rys. 3 przedstawiono najważniejsze trudności, na jakie narażone są banki wykorzystujące wysłużone wersje systemów centralnych.

Rys. 3:
Najważniejsze wyzwania związane z istniejącymi systemami centralnymi banków



źródło: Kendler [2001], s. 2.

Rys. 4:
Ile lat mają Państwa systemy centralne?



źródło: Kendler [2011], s. 3 – dane zebrane od 255 przedstawicieli banków w ramach badania UBM TechWeb Surwey.

Zanim jednak banki będą zmuszone do podjęcia decyzji w sprawie kosztownej wymiany systemów centralnych, może warto zastanowić się na rozwiązaniami alternatywnymi.

Warstwa komunikacji – *middleware*

Jednym z nich jest zaproponowana przez IBM postępująca (ale stopniowo) transformacja środowiska systemów bankowych z wykorzystaniem narzędzi *middleware*. Przykładowo, aplikacja bankowości mobilnej łączy się z warstwą komunikacyjną (middleware) 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.

Ograniczenie funkcji systemu centralnego

W wielu dużych bankach, takich jak ABN, Barcleys czy JPMorgan, funkcje systemu centralnego są od lat minimalizowane do podstawowych funkcji, głównie księgowych. Rozwiązanie takie powoduje, że banki są w stanie przygotowywać nowe produkty i usługi bankowe poza systemem centralnym. W ten sposób banki stopniowo przygotowują się do wymiany systemu, jednocześnie będąc w stanie zarządzać równolegle „starymi" i „nowymi" aplikacjami. W przypadku dużych banków lub takich, które mają skomplikowaną, odziedziczoną architekturę systemów IT, takie rozwiązanie zdecydowanie zmniejsza ryzyko i bezpośredni czas potrzebny na wymianę systemu centralnego.[4]

Mark Gunning z firmy Temendos uważa, że do 2020 roku większość projektów wymiany systemu centralnego banku będzie wykonywana w technologii „chmury", choć jednocześnie zaznacza, iż duże banki będą wykorzystywały do tego celu własną. Dużo zależy od regulatorów sektora finansowego. Holenderski Bank Centralny (DNB) zgodził się na wykorzystywanie przez banki platformy **Amazon Web Services** po tym, jak kilkanaście z nich próbowało

4 Groenfeldt (2013), s. 2–3.

uzyskać pozwolenie na wykorzystywanie usług w „chmurze".[5] Oznacza to, że banki holenderskie mogą podjąć działalność bankową w Europie wykorzystując usługi „chmury". Oczywiście spodziewane jest istotne zmniejszenie ich kosztów.

Nic jednak nie wskazuje na zmianę trendu wzrostu kosztów informatyki w bankowości. Oznaczać to może równoległą realizację następujących procesów:

- konsolidacji sektora bankowego w celu wzmocnienia efektu skali,
- przekształcania poszczególnych elementów systemów informatycznych, w tym systemu centralnego, w usługi wymieniające informacje poprzez szynę danych,
- rosnącej presji na obniżenie kosztów informatyki.

Najwięcej różnorodnych kierunków działań może dostarczyć ta ostatnia opcja. Możemy spodziewać się postępującej specjalizacji mniejszych banków, propozycji uproszczeń produktów i procesów, jak również ograniczania oferowanej funkcjonalności. Alternatywą, choć trudno powiedzieć czy już uświadomioną, jest obniżanie jakości serwisu lub podnoszenie opłat za utrzymanie tej jakości.

Możliwy jest również znaczący wzrost roli outsourcingu w bankowości związany z koncentracją na działalności podstawowej. Banki, które uznają, że informatyka przestała być źródłem ich przewagi konkurencyjnej mogą w ten sposób poszukiwać uproszczeń i ograniczania kosztów.

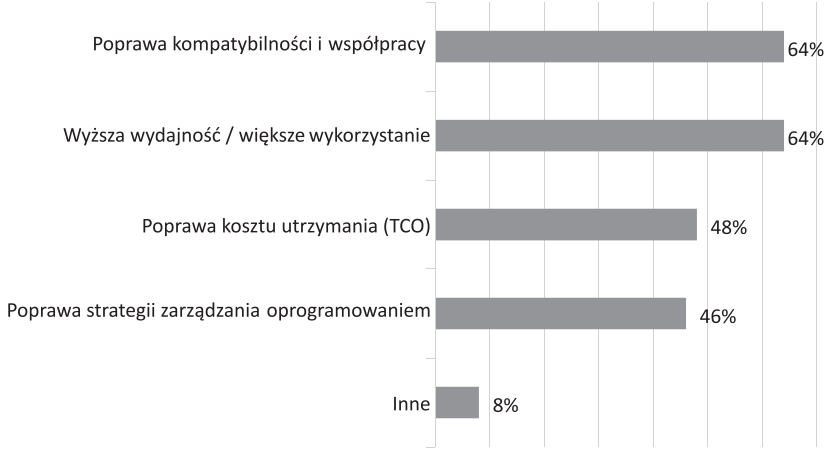
Niezależnie od kierunku, w którym podąży świat bankowy określenie „System Centralny" należy odsunąć do lamusa – dziś powinniśmy nazywać je „Systemami Transakcyjnymi".

Zanim ruszysz w daleką drogę...

Peggy Kendler z UBS Web Tech przeprowadziła badanie na temat odniesionych korzyści wymiany systemu centralnego, w którym uczestniczyło 250 menedżerów IT i użytkowników biznesowych. Wyniki badania zostały przedstawione na rys. 5.

5 Ibidem.

Rys. 5:
Jakie są kluczowe korzyści, jakie odnieśli Państwo w efekcie wdrożenia systemu centralnego?



źródło: Kendler [2001], s. 4.

David Boyle i James Roberts z firmy Ernst&Young opracowali poradnik z najważniejszymi miarami sukcesu dla wymiany systemów centralnych, zebranymi na podstawie obserwowanych projektów.[6] W swojej pracy umieścili dziewięć najważniejszych, spośród których najważniejsze to:

1. Najważniejszym wyzwaniem jest odpowiedź na pytanie, czy mamy w organizacji dostatecznie dużą, wszechstronną grupę ludzi, którzy są w stanie podołać takiemu projektowi.
2. Należy opracować model współdzielenia ryzyka takiego projektu ze wszystkimi dostawcami. Projekty tego typu trwają od 3 do 5 lat w zależności od wielkości banku i stopnia skomplikowania architektury IT.
3. Należy opracować model stanu obecnego i dokładnie komunikować kompleksowość obecną oraz model końcowy projektu.
4. Upraszczaj, upraszczaj, upraszczaj!!!
5. W projekcie powinni brać udział najlepsi ludzie, jakimi dysponujemy w organizacji. Jest to problem zarządzania krótko- i długoterminowymi celami organizacji. Ten aspekt poczytuje się, jako główny „opóźniacz" projektów wymiany systemów centralnych.

6 Oczywiście nie jest to jedyny taki poradnik, bo oferuje je większość dostawców i firm konsultingowych. Zamieszczony przykład jest w opinii autorów najbardziej uniwersalny.

Bibliografia

Boyle, D. Roberts, J., 2012, *Key to success for core systems modernization in financial services*.
Chmielarz W., 1997, *Komputer i bank*, Warszawa.
Crosman P., 2013, *Can big four core banking vendors oligopoly be broken*, American Banker, 01.10.2013, s. 1–4.
Dziuba D. T., 2003, *Systemy informatyczne w bankowości detalicznej*, Uniwersytet Warszawski, Warszawa.
Groenfeldt T., 2012, *Replacing legacy core banking systems – SAP has limited success*, Forbes, 18/12/2012.
Groenfeldt T., 2013, *Core banking replacement reminds locked in the future*, Forbes 9/10/2013.
Kendler P., 2011, *Core Banking Systems Transformation*, UBM Tech Web.

Rafał Burzyński

Senior Manager w firmie doradczej KPMG. Z wykształcenia magister ekonomii po Akademii Ekonomicznej we Wrocławiu. Ukończył też Podyplomowe Studium Podatków i Prawa Podatkowego na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego. Licencjonowany Doradca Podatkowy numer 10508.

Członek Krajowej Grupy Wsparcia w zakresie projektów FATCA. Specjalizuje się w doradztwie podatkowym dla instytucji finansowych. Jego profesjonalne doświadczenie obejmuje m.in. doradztwo w zakresie automatyzacji kalkulacji podatku VAT i cen transferowych, jak również w zakresie podatku CIT i VAT oraz podatku od czynności cywilnoprawnych.

Tomasz Rzepa

Senior Manager w KPMG Tax M. Michna sp. k. Z wykształcenia magister prawa po Uniwersytecie Warszawskim, absolwent Szkoły Prawa Amerykańskiego na University of Florida, Licencjat z Ekonomii na SGH.

Specjalizuje się w doradztwie podatkowym dla branży finansowej, w szczególności banków. Zakres jego doświadczenia obejmuje zarówno bieżące doradztwo podatkowe i przeprowadzanie kompleksowych przeglądów rozliczeń podatkowych, jak również prowadzenie postępowań podatkowych. Prowadził kompleksowe projekty mające na celu wprowadzenie procedur podatkowych i sprawozdawczych w bankach i innych instytucjach finansowych. W ramach swojej pracy zajmuje się także doradztwem podatkowym w zakresie wdrożenia regulacji FATCA w bankach i zakładach ubezpieczeń, m.in. Grupa DnB, Grupa PZU, a oprócz tego prowadzi liczne szkolenia z zakresu obowiązków wynikających z przepisów FATCA oraz jest autorem publikacji w tym zakresie.

Jakub Chadysz

Senior Manager w firmie doradczej KPMG. Z wykształcenia magister inżynier po Politechnice Warszawskiej.

Doświadczony menedżer projektów, inżynier systemowy oraz doradca w zakresie bezpieczeństwa systemów informatycznych. Jego doświadczenie obejmuje liczne projekty wdrożeniowe, audyty systemów informatycznych, przeglądy polityk bezpieczeństwa oraz doradztwo przy przetargach na usługi IT (systemy, outsourcing, itp.). Ostatnio zaangażowany w projekty dla sektora finansowego związane z implementacją systemów stworzonych przez KPMG. Wspierają one procesy back-office'owe w zakresie zapewnienia zgodności z MSR 39 (IFRS Calculator) oraz procesy podatkowe (TaxTool).

Rafał Burzyński, Tomasz Rzepa, Jakub Chadysz, KPMG

FATCA – analiza porozumienia IGA wynegocjowanego przez Polskę

Nie ma już praktycznie żadnych wątpliwości, iż od 1 lipca 2014 roku polskie instytucje finansowe będą zobowiązane do wdrożenia regulacji FATCA, zgodnie z którą będą one zobowiązane do identyfikacji czy ich klienci są amerykańskimi rezydentami podatkowymi i w rezultacie do raportowania do organów podatkowych posiadanych przez nich rachunków finansowych.

FATCA – stan prawny

Analizując rys historyczny tej regulacji należy wskazać w szczególności, iż jej źródło związane jest z nadużyciami dokonywanymi przez podatników amerykańskich, które w ocenie Kongresu Stanów Zjednoczonych powodują straty wpływów podatkowych na poziomie 100 mld USD rocznie. Mając powyższe na uwadze podjęto prace legislacyjne, które spowodowały przyjęcie przez Kongres Stanów Zjednoczonych 28 marca 2010 roku Ustawy o ujawnianiu kont zagranicznych dla celów podatkowych FATCA (*Foreign Account Tax Compliance Act*).

Zgodnie z pierwotnymi założeniami regulacja FATCA miała dotyczyć bezpośrednio wszystkich zagranicznych instytucji (*Foreign Financial Institutions*), które prowadzą rachunki finansowe dla podatników amerykańskich, poprzez podpisanie z amerykańskimi organami podatkowymi (*Internal Revenue Service – IRS*) umowy cywilnoprawnej. Instytucje finansowe, które nie podporządkowałyby się temu obowiązkowi zostałyby obciążone podatkiem w wysokości 30% od wszystkich płatności dokonywanych na ich rzecz (w tym na rzecz ich klientów) i mających swoje źródło w USA, m.in. dywidend i odsetek.

Biorąc jednak pod uwagę, iż bezpośrednie zastosowanie się zagranicznych instytucji finansowych do amerykańskiej regulacji FATCA, niebędącej częścią lokalnego systemu prawnego, pozostawało w sprzeczności z prawem większości państw na świecie, w szczególności w zakresie ochrony danych osobowych, Stany Zjednoczone zaproponowały wdrożenie regulacji FATCA poprzez zawarcie umów międzyrządowych, tzw. IGA (*Intergovernmental Agreement*), które jako pierwsza podpisała Wielka Brytania we wrześniu 2012 roku. Mając na uwadze negatywne konsekwencje związane z brakiem przystąpienia do IGA, a w szczególności istotne ryzyko, że wszystkie płatności ze źródeł amerykańskich dokonywane przy udziale polskich instytucji finansowych obciążone będą 30% podatkiem w USA, Polska parafowała 10 września 2013 roku umowę międzyrządową IGA, której podpisanie planowane jest na koniec I kwartału 2014 roku. Powyższe umożliwi instytucjom finansowym rejestrację na portalu internetowym IRS i traktowanie ich jako uczestniczące instytucje finansowe (PFFI).

W tym miejscu należy wskazać, iż choć zgodnie z założonymi przez stronę amerykańską terminami FATCA ma zacząć obowiązywać w praktyce od 1 lipca 2014 roku, Polska z uwagi na opóźnienia nie zakłada ratyfikowania IGA w tym terminie a tym bardziej dostosowania regulacji krajowych do zakresu informacji, które mają być gromadzone i raportowane przez polskie instytucje finansowe. Powyższe podejście, choć może w praktyce powodować pewne trudności, znajduje pewne uzasadnienie z uwagi na opóźnienia w uzgodnieniu treści IGA, jak również konieczność wdrożenia zmian w prawie krajowym w kształcie uwzględniającym nie tylko wymogi FATCA, ale również opublikowanego 13 lutego 2014 roku przez OECD projektu regulacji o automatycznej wymianie informacji o rachunkach finansowych (*Common Reporting Standard*), którego wdrożenie planowane jest na początek roku 2016 roku.

Biorąc pod uwagę, iż od 1 lipca 2014 roku instytucje finansowe powinny rozpocząć jedynie identyfikację klientów z perspektywy ich rezydencji podatkowej w USA (odrębnie dla klientów nowych i istniejących), zaś obowiązki związane z raportowaniem do IRS za pośrednictwem polskich organów podatkowych rozpoczną się od 30 czerwca 2015 roku (lub później w zależności od terminów ustalonych w finalnej wersji IGA), wiele wskazuje na to, iż możliwe będzie dostosowanie prawa krajowego do nowych regulacji. Pewne wątpliwości w tym zakresie może budzić stanowisko Generalnego Inspektora Ochrony Danych Osobowych (GIODO), co do możliwości gromadzenia przez instytucje finansowe informacji wymaganych przez FATCA od 1 lipca 2014 roku bez

zmian w prawie krajowym, niemniej, jak zapewnia Ministerstwo Finansów, kwestia ta zostanie doprecyzowana. Dodatkową wątpliwością jest wystąpienie 18 listopada 2013 roku Rzecznika Praw Obywatelskich do Ministra Finansów, w którym w związku z planowym podpisaniem IGA wyraził on zaniepokojenie *„czy konieczne do realizacji tych zobowiązań zmiany polskiego prawa będą dopuszczalne w związku z konstytucyjnymi wymaganiami wobec ograniczeń wolności i praw człowieka i obywatela"*.

Podstawowe definicje

Odnosząc się do treści regulacji IGA należy zaznaczyć, iż dotyczy ona polskich instytucji finansowych, które mogą zostać zakwalifikowane do jednej z następujących kategorii:

- instytucja powiernicza (*Custodial institution*),
- instytucja przyjmująca depozyty (*Depository institution*),
- podmiot inwestycyjny (*Investment entity*),
- określona instytucja ubezpieczeniowa (*Specified insurance company*).

Przez instytucję powierniczą należy rozumieć podmiot, którego znaczna część działalności skupia się na utrzymywaniu aktywów finansowych na rachunek innych podmiotów. Jako instytucję przyjmującą depozyty przepisy IGA definiują każdy podmiot, który przyjmuje depozyty w toku prowadzonej działalności bankowej lub działalności podobnej. Podmiot inwestycyjny został zdefiniowany jako ten prowadzący działalność (lub jako zarządzany przez podmiot prowadzący działalność) polegającą na wykonywaniu na rzecz lub w imieniu klienta: obrotu instrumentami rynku pieniężnego (czekami, wekslami, certyfikatami depozytowymi lub derywatami i podobnymi instrumentami), walutą, instrumentami odzwierciedlającymi kurs walut, wartość indeksów lub stóp procentowych, zbywalnymi papierami wartościowymi lub kontraktami na wartość surowców, zarządzania indywidualnym lub zbiorowym portfelem aktywów, innych form inwestowania oraz zarządzania lub dysponowania środkami pieniężnymi w imieniu innych osób. Natomiast określona instytucja ubezpieczeniowa to każdy podmiot będący firmą ubezpieczeniową (lub spółką holdingową takiej spółki), który zawiera umowy ubezpieczenia posiadające wartość pieniężną („*cash value*") lub umowy typu *annuities* (umowy renty) albo jest zobligowany do dokonywania płatności w zakresie takich umów.

Wśród instytucji finansowych, które mogą podlegać wyłączeniu z zakresu regulacji FATCA należy wskazać tzw: *Exempt Beneficial Owners* oraz *Deemed-Compliant Financial Institutions*. Do pierwszej kategorii zaliczyć należy podmioty rządowe i samorządowe, Bank Centralny, organizacje międzynarodowe i ich jednostki oraz fundusze emerytalne. Natomiast jako *Deemed-Compliant Financial Institutions* mogą zostać uznane m.in. instytucje finansowe z lokalną bazą klientów lub lokalne banki z niewielką wartością rachunków (brak rachunku powyżej 50 tys. USD), określone podmioty inwestycyjne oraz kwalifikowani wydawcy kart kredytowych.

Kwestią, która może budzić szczególne zainteresowanie w odniesieniu do możliwości zastosowania wskazanych powyżej zwolnień są instytucje finansowe z lokalną bazą klientów. Aby instytucje finansowe, np. SKOK-i lub banki spółdzielcze, mogły zostać objęte tym zwolnieniem muszą spełnić łącznie 9 kryteriów, wśród których należy wskazać m.in. na takie wymogi jak:

- instytucja finansowa i każdy podmiot z nią powiązany zmusi być zarejestrowany w kraju,
- instytucji finansowej nie wolno starać się zdobywać klientów nie zamieszkałych na terytorium kraju,
- co najmniej 98% rachunków musi być posiadana przez podmioty krajowe lub innego państwa członkowskiego Unii Europejskiej,
- instytucja finansowa najpóźniej 1 lipca 2014 roku musi wdrożyć procedury ukierunkowane na sprawdzenie czy prowadzi rachunki dla (i) konkretnych osób z USA, które nie zamieszkują na terenie kraju, (ii) instytucji finansowych niewywiązujących się z zapisów IGA ani (iii) pasywnych niefinansowych jednostek zagranicznych, gdzie osoby sprawujące kontrolę to obywatele lub mieszkańcy USA.

Instytucja finansowa niepodlegająca zwolnieniu, zaliczona do jednej z czterech kategorii wskazanych powyżej, będzie zobowiązana do weryfikacji czy jej klienci posiadający rachunki finansowe w rozumieniu FATCA są rezydentami podatkowymi USA i – w przypadku identyfikacji takich rachunków według ściśle określonych procedur *due diligence* – do raportowania ich do IRS za pośrednictwem polskich organów podatkowych.

Jeśli chodzi o definicję rachunków finansowych to jego pojęcie w rozumieniu IGA może być obszerniejsze niż mogłoby to wynikać z lokalnej praktyki i obejmować przykładowo udziały kapitałowe lub udziały w zyskach spółki inwestycyjnej. Co do zasady jednak IGA wskazuje na 4 kategorie rachunków finansowych, tj. konta depozytowe, konta powiernicze, instrumenty dłużne lub

udziały kapitałowe oraz ubezpieczenia typu cash value/umowy renty. Wśród rachunków wyłączonych z definicji rachunku finansowego wskazać należy m.in. na te związane z zabezpieczeniem emerytalnym lub korzyściami podatkowymi przewidzianymi przez prawo krajowe, rachunki escrow, rachunki w posiadaniu masy majątkowej, niektóre umowy ubezpieczenia na życie, rachunki w krajach, które podpisały IGA oraz wyłączone z definicji rachunku finansowego zgodnie z przepisami odpowiedniej IGA.

Obowiązki identyfikacji i raportowania wynikające z FATCA

W tym miejscu należy krótko omówić, jakie obowiązki w zakresie identyfikacji i raportowania nałożone zostaną na polskie instytucje finansowe i w jakich terminach zobowiązane będą je wykonywać. Pierwszym i najistotniejszym obowiązkiem jest konieczność identyfikowania każdego nowego klienta (tj. takiego, który otwiera rachunek finansowy w rozumieniu FATCA 1 lipca bieżącego roku lub później) pod kątem tego czy spełnia on przesłanki definicji podatnika amerykańskiego. Identyfikacja ta wyglądać będzie inaczej w przypadku klientów indywidualnych czyli osób fizycznych (w tym prowadzących działalność gospodarczą), inaczej zaś w przypadku klientów instytucjonalnych. W przypadku klientów indywidualnych identyfikacja ta składać się będzie z dwóch elementów. Po pierwsze, od każdego pojawiającego się po 1 lipca klienta, który nabywać będzie produkt objęty FATCA, instytucja finansowa będzie zobowiązana pobrać oświadczenie, w którym klient wskaże czy jest podatnikiem amerykańskim, czy też nie. Oświadczenie to może mieć formę jednostronnego dokumentu z właściwym polem do odznaczenia przez klienta. Co więcej, jak wskazuje praktyka innych krajów, oświadczenie takie mogłoby być złożone także za pośrednictwem kanałów zdalnych. Część instytucji finansowych już jednak zakłada, iż pobierać będzie od klientów bardziej skomplikowane formularze, odpowiadające kształtem amerykańskiemu formularzowi podatkowemu W-8 lub W-9. Drugim natomiast elementem tej identyfikacji będzie sprawdzenie przez instytucję finansową wiarygodności złożonego przez klienta oświadczenia. Powyższy proces sprowadzał się będzie do sprawdzenia czy w danych posiadanych przez instytucję nie występują określone przesłanki wskazujące na podejrzenie, iż klient może być jednak podatnikiem amerykańskim. Te przesłanki, określane w IGA terminem *U.S. Indicia*, to chociażby amerykański adres klienta, miejsce urodzenia w USA, amerykański numer telefonu, amerykański adres pełnomocnika

do rachunku czy też stałe zlecenie transferu środków na rachunek w USA. W przypadku znalezienia takiej przesłanki, instytucja finansowa nie może bazować na oświadczeniu złożonym przez klienta i ma obowiązek traktować takiego klienta jak podatnika amerykańskiego, chyba że klient dostarczy określone dodatkowe dokumenty na potwierdzenie prawidłowości złożonego oświadczenia.

Nieco inaczej będzie wyglądał proces identyfikacji nowych klientów instytucjonalnych. W tym przypadku każdy klient powinien zostać zidentyfikowany pod kątem spełnienia przesłanek definicji jednej z kategorii klienta instytucjonalnego, jakie wymienia FATCA. Klient może być więc przykładowo amerykańskim podatnikiem (*Specified U.S. Person*), co obejmuje m.in. spółki mające siedzibę w USA lub założone na podstawie prawa amerykańskiego. Jeśli klient spełnia przesłanki definicji podatnika amerykańskiego, dane o jego rachunku będą podlegały raportowaniu do amerykańskich organów podatkowych. Klient może również zaliczać się do kategorii instytucji finansowych, przy czym należy odróżnić tutaj te zgodne z FATCA (czy jest ona zgodna z FATCA, będzie można sprawdzić na portalu uruchomionym przez Amerykanów specjalnie dla celów FATCA) oraz niezgodne z nią (np. instytucje z krajów, które nie podpisały IGA, czy też instytucje skreślone z listy zamieszczonej na portalu IRS w wyniku poważnych zaniedbań w realizacji obowiązków wynikających z FATCA). Rachunki należące do instytucji finansowych nie podlegają obowiązkowi raportowania, jednakże instytucje finansowe współpracujące z instytucjami finansowymi niezgodnymi z FATCA zobowiązane będą raportować płatności dokonywane na ich rzecz w latach 2015 i 2016. Ostatnią kategorią klientów, którzy nie są ani podatnikami amerykańskimi, ani instytucjami finansowymi są tzw. niefinansowe podmioty zagraniczne (*Non-Financial Foreign Entity* - w skrócie NFFE). W ich przypadku instytucje finansowe będą miały obowiązek sprawdzić, czy podmioty te mają, zgodnie z definicjami stosowanymi przez FATCA, charakter pasywny czy aktywny. Pasywnym zagranicznym podmiotem finansowym są podmioty, które osiągają większość swoich dochodów z tzw. źródeł pasywnych (dywidendy, odsetki, sprzedaż papierów wartościowych, należności licencyjne i tym podobne) i jednocześnie nie łapią się w jedną ze wskazanych przez FATCA kategorii wyłączeń (tj., przykładowo, nie są pasywnymi NFFE podmioty notowane na giełdzie lub powiązane z takimi podmiotami, nie są też nimi spółki w likwidacji, spółki rozpoczynające dopiero działalność czy spółki świadczące wyłącznie usługi finansowe w ramach swojej grupy kapitałowej). Jeśli dany podmiot zostanie

uznany za pasywne NFFE, instytucja finansowa będzie dodatkowo zobowiązana sprawdzić czy posiada on beneficjentów rzeczywistych, którymi są osoby fizyczne będące amerykańskimi podatnikami. Jeśli znajdzie się choć jeden beneficjent, który jest podatnikiem USA, dane takiego podmiotu wraz z danymi beneficjentów rzeczywistych podlegać będą raportowaniu. Na jakiej podstawie należy klasyfikować klientów do jednej z ww. kategorii? FATCA daje tutaj kilka możliwości. Wśród nich jest opieranie się na danych gromadzonych już obecnie przez instytucje finansowe w ramach procedur AML/KYC, wykorzystywanie informacji publicznie dostępnych, np. strony internetowej klienta, czy też po prostu wystąpienie do klienta o złożenie oświadczenia, w którym on sam określi do jakiego typu instytucji się zalicza.

Niezależnie od obowiązków identyfikacji klientów, którzy nawiążą pierwszą relację z daną instytucją dopiero od 1 lipca b.r., instytucja finansowa będzie zobowiązana dokonać przeglądu klientów, którzy już posiadają u niej produkty będące w zakresie FATCA. W tym przypadku będzie ona mogła zastosować określone limity salda lub wartości rachunku, powyżej których dopiero wymagana będzie identyfikacja. Limity te to generalnie 50 tys. USD w przypadku klientów indywidualnych (w przypadku umów ubezpieczenia limit ten jest jednakże wyższy – 250 tys. USD) i 250 tys. USD w przypadku klientów instytucjonalnych. Klienci, którzy nie przekroczą ww. progów na 30 czerwca 2014 r. nie będą musieli być identyfikowani, chyba że na koniec któregokolwiek następnego roku saldo lub wartość ich rachunku przekroczy 1 mln USD. Identyfikacja istniejących klientów indywidualnych zasadniczo odbywać się będzie w oparciu o dane w systemach informatycznych i sprowadzać się będzie do wyszukiwania wspomnianych wyżej *U.S. Indicia*. W odniesieniu do rachunków o wyższej wartości (powyżej 1 mln USD) konieczne będzie dodatkowo przeszukanie dokumentacji papierowej klienta z ostatnich pięciu lat i weryfikacja informacji posiadanych przez opiekuna klienta. W przypadku znalezienia przesłanki wskazującej na możliwe spełnienie przesłanek definicji podatnika amerykańskiego rachunek tego klienta będzie raportowany, chyba że klient przedstawi dodatkowe dokumenty dowodzące, że mimo znalezienia takiej przesłanki, nie jest on podatnikiem USA. Natomiast w przypadku klientów instytucjonalnych weryfikacja może odbywać się zarówno na podstawie danych, w których posiadaniu instytucja finansowa już jest (np. gromadzonych w ramach procedur AML/KYC), jak również danych publicznie dostępnych oraz oświadczenia składanego przez klienta.

Kluczowe decyzje biznesowe, jakie należy podjąć

Wdrażając FATCA instytucje finansowe powinny przemyśleć kilka istotnych kwestii, które mogą istotnie wpłynąć nie tylko na efektywność i koszty nowych procesów identyfikacji, ale także na relacje z klientami. Pierwszą taką kwestią, nad którą instytucje finansowe powinny się zastanowić jest stosowanie limitów identyfikacji klientów także w odniesieniu do nowych. Takie limity (na wzór opisanych wyżej limitów w odniesieniu do identyfikacji klientów istniejących) dotyczyć mogą wyłącznie rachunków depozytowych oraz umów ubezpieczenia i tylko w sytuacji, kiedy produkty te nabywają klienci indywidualni. W obu przypadkach limit ten wynosi 50 tys. USD na koniec danego roku. Decydując się na stosowanie limitów identyfikacji, instytucje finansowe nie dokonują zatem identyfikacji klienta już na starcie w momencie podpisywania przez niego umowy, lecz czekają do końca roku i następnie rozpoczynają odpowiednie procedury jedynie odnośnie tych klientów, których saldo lub wartość rachunku na koniec roku przekroczy wspomniany limit. Na pierwszy rzut oka wydawałoby się, iż skorzystanie z tego limitu jest korzystne, ograniczy bowiem liczbę nowych klientów, którzy podlegać będą procedurom identyfikacji. Może to być jednak korzyść iluzoryczna. Przerzucenie identyfikacji na czas po zakończeniu danego roku powodować bowiem będzie przede wszystkim konieczność dodatkowego kontaktu z klientem w celu pobrania od niego oświadczenia lub innych dokumentów, a to może oznaczać dodatkowe koszty w porównaniu do sytuacji, kiedy klient podpisując umowę od razu dokonuje samoidentyfikacji.

Kolejną decyzją, jaką instytucje finansowe powinny podjąć jest sposób postępowania z klientami, którzy odmówią dostarczenia określonych dokumentów koniecznych dla celów identyfikacji wymaganej przez FATCA. Klienci ci w regulacjach FATCA noszą nazwę tzw. klientów „opornych" (*recalcitrant*). Kwestią, jaką należy tutaj rozważyć jest czy otwierać takiemu klientowi rachunek, czy też wprowadzić politykę, iż klienci niedostarczający dokumentów wymaganych dla celów identyfikacji FATCA nie mogą w ogóle nabyć nowego produktu.

Następną kwestią, nad którą instytucja finansowa powinna się zastanowić jest jak daleko posunąć się w działaniach mających na celu identyfikację klienta. Wyobraźmy sobie sytuację, kiedy w odniesieniu do klienta indywidualnego instytucja finansowa zidentyfikuje chociażby amerykański adres korespondencyjny lub miejsce urodzenia w USA, czyli jedną z tzw.

U.S. Indicia, która wskazuje, że potencjalnie klient może być podatnikiem USA. Zgodnie z regulacjami FATCA w takiej sytuacji instytucja finansowa ma już prawo zaraportowania klienta do amerykańskich organów podatkowych. Ma ona jednak też możliwość wystąpienia do klienta z prośbą o dostarczenia dodatkowych dokumentów, takich jak kopia dokumentu tożsamości, certyfikat rezydencji czy dokument poświadczający utratę amerykańskiego obywatelstwa, tak aby klient mógł wyjaśnić swoją sytuację.

Fundamentalnym pytaniem jest także gdzie w strukturze instytucji finansowej umiejscowić procesy identyfikacji klienta. Czy weryfikacja klienta powinna odbywać się od razu na tzw. „ladzie" przez pracowników rejestrujących dane nowego klienta? Za takim rozwiązaniem przemawiałaby oszczędność czasu, z drugiej strony jednak strony rozwiązanie takie rodziłoby konieczność przeprowadzenia szczegółowych szkoleń z zakresu regulacji FATCA dla pracowników front-office, co zwiększy koszty. Dodatkowo, takie podejście zwiększałoby ryzyko błędów w identyfikacji.

To tylko kilka z najistotniejszych kwestii, jakie należy mieć na uwadze zastanawiając się nad sposobem wdrożenia w danej instytucji regulacji FATCA. Od podjęcia decyzji w tych kluczowych kwestiach zależeć będzie kształt przyszłych procedur czy też rozwiązań w zakresie nowych funkcjonalności informatycznych. Trzeba też pamiętać, że takie procedury identyfikacji klientów, jakich wymaga FATCA już wkrótce trzeba będzie stosować także względem podatników z krajów Unii Europejskiej, a w dalszym horyzoncie – podatników krajów OECD. W 2016 roku, a być może już w 2015 wprowadzone zostaną regulacje w zakresie automatycznej wymiany informacji dla celów podatkowych, wynikające z tzw. *Common Reporting Standard OECD* wzorowanego właśnie na rozwiązaniach FATCA, a także przepisy wynikające z nowelizacji europejskiej dyrektywy dotyczącej wymiany informacji dla celów podatkowych. O tym już teraz należy pomyśleć projektując przyszłe procesy i rozwiązania informatyczne dla celów FATCA.

Wpływ FATCA na IT

FATCA, podobnie jak wszystkie inne regulacje wprowadzające nowy rodzaj raportowania, ma wpływ na systemy informatyczne w instytucjach objętych tą regulacją. Wpływ ten skupia się wokół trzech obszarów funkcjonalnych:

- danych klienta,
- danych rachunków,
- raportowania.

Zmiany w obszarze danych klienta wynikają z obowiązku identyfikacji klientów będących amerykańskimi rezydentami podatkowymi. Z pozoru prosty proces identyfikacji amerykańskiego podatnika nie jest tak oczywisty, gdy wejdziemy w szczegóły regulacji. IGA przewiduje inne podejście do identyfikacji podatnika amerykańskiego dla klientów istniejących na dzień wejścia regulacji w życie (30-06-2014), a inne dla zupełnie nowych klientów. W ramach tego podziału dodatkowo inne podejście stosujemy dla klientów indywidualnych a inne dla klientów instytucjonalnych. W tym też miejscu pojawia się kolejna komplikacja. Takie formy działalności gospodarczej jak spółka cywilna czy też jednoosobowa działalność gospodarcza, standardowo traktowane jako klienci instytucjonalni, w rozumieniu IGA powinny być traktowane jako klienci indywidualni. Nie wchodząc w kolejne opisane wcześniej szczegóły regulacji, najistotniejsze potencjalne zmiany w systemach odpowiedzialnych za rejestrację i utrzymujących danych klienta wynikające z regulacji IGA to:

- rozszerzenie kartoteki klienta o dane wymagane do prawidłowej oceny klienta (np. oświadczenia klienta wyjaśniające status FATCA, finalna ocena klienta pod kątem FATCA, dane do weryfikacja przesłanek),
- funkcjonalność badania przesłanek „*US Indicia*" występujących na kartotekach klientów indywidualnych oraz w przypadku wykrycia przesłanki automatyczna modyfikacja danych kartoteki klienta i nadanie właściwego statusu FATCA.

Do zakresu potencjalnych zmian w obszarze rachunków wchodzą:

- kalkulacja zagregowanego salda rachunków FATCA klienta,
- dodatkowa klasyfikacja produktów pod kątem FATCA wynikająca z potrzeby agregacji i kalkulacji salda FATCA klienta,
- modyfikacja kartoteki klienta na podstawie wyliczonego salda rachunków FATCA.

Dodatkowo, z uwagi na nowe procesy związane z oceną klienta pod kątem FATCA (np. weryfikacja dokumentów papierowych pod kątem występowania przesłanek), które nie mogą być w pełni zautomatyzowane, należy rozważyć wdrożenie (rozszerzenie) rozwiązań wspierających procesy back-office'owe instytucji (np. rozwiązania BPM).

Jeśli chodzi o zmiany w zakresie raportowania FATCA to konieczne będzie gromadzenie danych niezbędnych do raportowania oraz stworzenie funkcjonalności odpowiedzialnej za generowanie raportów w formacie wymaganym przez regulatora. Istotne jest, aby już na etapie projektowania rozwiązania

uwzględnić rozszerzający się z każdym kolejnym rokiem zakres raportowania. W pierwszych latach są to jedynie podstawowe dane klienta oraz salda jego rachunków, jednak w kolejnych latach zakres się rozszerza i obejmuje takie dane jak przychody odsetkowe klienta czy dywidendy, a także dane niezwiązane bezpośrednio z klientami amerykańskim, a dotyczące transferu środków (niezależnie od źródła) do nieuczestniczących instytucji finansowych (raportowanie danych o klientach będących instytucjami finansowymi).

Oczywiście, wszelkie zmiany w systemach informatycznych powinny być poprzedzone wnikliwą analizą, tak aby ich zakres i miejsce implementacji były optymalne dla danej instytucji. Szczegółowy zakres zmian zależeć będzie od obecnych procesów funkcjonujących w organizacji, skali działalności, ilości oferowanych produktów FATCA oraz wstępnej analizy obecnych klientów pod kątem salda ich rachunków FATCA oraz zidentyfikowanych przesłanek *US Indicia*.

Analiza przedwdrożeniowa FATCA pomoże odpowiedzieć na takie pytania jak:

- Na ile procesy FATCA w danej instytucji wymagają automatyzacji (np. z uwagi na małą liczbę rachunków FATCA lub znikomą ilość potencjalnych klientów amerykańskich proces weryfikacji może być przeprowadzany ręcznie lub półautomatycznie)?
- Z jaką częstotliwością wykonywać automatyczne badanie danych klientów?
- Jaki powinien być poziom wsparcia dla procesów manualnych?
- W jakich systemach implementować poszczególne zmiany?

Podsumowując, można stwierdzić, że FATCA wiąże się ze zmianami w systemach informatycznych, jednak same zmiany powinny być poprzedzone analizą, tak aby ich zakres był optymalny dla danej instytucji.

Źródła

- *http://www.hmrc.gov.uk/drafts/uk-us-fatca-guidance-notes.pdf*
- *http://www.treasury.gov/resource-center/tax-policy/treaties/Documents/FATCA-Reciprocal-Model-1A-Agreement-Preexisting-TIEA-or-DTC-11-4-13.pdf*
- *http://www.treasury.gov/resource-center/tax-policy/treaties/Documents/FATCA-Annex-I-to-Model-1-Agreement-11-4-13.pdf*
- *http://www.treasury.gov/resource-center/tax-policy/treaties/Documents/FATCA-Annex-II-to-Model-1-Agreement-11-4-13.pdf*

dr Marek Grajek
Niezależny konsultant. Z wykształcenia ekonomista, ale także kryptolog, historyk i pisarz.
Jeden z pionierów polskiego rynku kapitałowego. W swojej pracy wykorzystuje doświadczenia zebrane w projektach IT realizowanych w globalnej skali na rzecz instytucji finansowych, specjalizując się w zarządzaniu tożsamością i innych zastosowaniach kryptologii w biznesie.

Marek Grajek, niezależny konsultant

Uwierzytelnianie klienta banku w rozwoju cyfryzacji sektora publicznego

Większość procesów biznesowych realizowanych w sektorze finansowym znajduje naturalne odpowiedniki w sektorze publicznym. Zarówno instytucje finansowe, jak i publiczne cieszą się specjalnym statusem instytucji zaufania publicznego. Ich kontrpartnerami bywają te same grupy podmiotów: osoby fizyczne lub podmioty gospodarcze. Procesy biznesowe realizowane w sposób tradycyjny przybierają w obu sferach podobną strukturę. Jest więc pewnym zaskoczeniem, że tempo akceptacji przez oba sektory rozwiązań charakterystycznych dla cywilizacji cyfrowej różni się zasadniczo w większości krajów rozwiniętych. Wydaje się, że jedną z istotnych przyczyn tego zjawiska jest różnica w postrzeganiu ryzyk związanych z identyfikacją i uwierzytelnieniem partnerów.

Aby udokumentować tę tezę przedstawię poniżej przegląd typowych rozwiązań w zakresie infrastruktury zaufania na styku sektora publicznego i prywatnego, dokonam analizy aktualnego stanu usług zaufania w Polsce, a w charakterze podsumowania przedstawię niektóre uwarunkowania ich dalszego rozwoju, w szczególności w świetle ewolucji prawa europejskiego.

Modele cyfrowej infrastruktury zaufania

W świecie tradycyjnym państwo i jego agendy są pierwotnym i w zasadzie jedynym autorytatywnym źródłem usług zaufania.[1] Administrowane przezeń atrybuty zaufania (w formie dokumentów tożsamości) są akceptowane

1 W duchu projektowanej regulacji UE w niniejszym tekście zastępuję liczne stosowane mniej lub bardziej fortunnie pojęcia „identyfikacja", „autentykacja", „autoryzacja" itd. preferowanymi w niej i obejmującymi szerszą sferę zagadnień pojęciami „usług zaufania" i „infrastruktury zaufania".

w sektorze publicznym i prywatnym na równi i na tyle powszechnie, że potrzeba dystrybucji alternatywnych atrybutów dotyczy drugoplanowych obszarów działalności człowieka. Wynika to z naturalnej roli państwa w organizacji społeczeństwa: (t)*ylko państwo, poprzez swoje struktury, może powiązać tożsamość z osobą. Żadne inne ciało nie może, w początku XXI stulecia, stworzyć legalnej tożsamości. „Tożsamość" nieutworzona przez państwo nie jest prawdziwa ani legalna, lub też maskuje prawdziwą tożsamość i jest w konsekwencji fałszywa. W ogólności musi istnieć prawdziwe jądro tożsamości, na którym oparta jest tożsamość różnych ról. Zaletą tej metody jest fakt, że zapewnia ona praktyczną unikalność tożsamości.*[2] Do spostrzeżenia natury filozoficznej dodajmy argument prawny – art. 18 ust. 2 i 3 Traktatu UE. Ust. 2 pozwala Radzie UE przyjąć prawa gwarantujące realizację traktatowej swobody ruchu osób, lecz ust. 3 uściśla, że *(u)stęp 2 nie znajduje zastosowania w odniesieniu do paszportów, dokumentów tożsamości lub rezydencji i innych dokumentów (...)*, zastrzeżonych do wyłącznej kompetencji krajów członkowskich. Wydaje się bezsporne, że na gruncie filozofii, prawa, teorii organizacji i innych przesłanek budowa i administracja infrastrukturą zaufania jest w pierwszym rzędzie zadaniem państwa.

Dlatego pewnym zaskoczeniem były rozwiązania przyjęte w Dyrektywie 1999/93/EC, określającej zasady funkcjonowania podpisu elektronicznego, fundamentu paneuropejskiej infrastruktury zaufania w cyberprzestrzeni. Nie wskazując w niej *explicite* kategorii podmiotów odpowiedzialnych za realizację funkcji dostawców usług certyfikacji, autorzy ukształtowali strukturę dyrektywy zakładając w czytelny sposób, że rolę tę będą pełnić podmioty sektora prywatnego. Wynikało to zapewne z braku w sektorze publicznym kompetencji, kapitału i technologii niezbędnych do budowy nowych usług. Dokonała się tym samym częściowa prywatyzacja usług zaufania, do tej pory zastrzeżonych dla sektora publicznego. Prywatyzacja nieskuteczna, bowiem dopuszczając udział sektora prywatnego w rodzącym się rynku usług zaufania sektor publiczny narzucił jego aktorom wyśrubowane standardy techniczne. Przełożyły się one na wysoką cenę usług i produktów, co na płytkim rynku spowodowało ich faktyczne odrzucenie.

W rezultacie rynek usług zaufania zaczął ulegać procesowi stopniowej dywersyfikacji. W niektórych krajach państwo postanowiło powrócić do swej tradycyjnej roli, rozciągając ją także na cyberprzestrzeń. Dobrymi przykładami takiej polityki w Europie są Belgia i Niemcy, które wdrożyły elektroniczne

2 Grayson, Timothy R.D., *Philosophy of identity*, http://timothygrayson.com/PDFs/PhilosophyofID.pdf.pdf (wszystkie tłumaczenia tekstów źródłowych autora).

dokumenty tożsamości, umożliwiając sektorowi prywatnemu wykorzystanie ich funkcjonalności. W Belgii Rada Ministrów podjęła w lipcu 2001 r. decyzję o konstrukcji państwowej, elektronicznej infrastruktury zaufania BelPIC. Elementami tej infrastruktury stała się m.in. państwowa agencja technologii ICT, Fedict, oraz państwowy urząd certyfikacji FedPKI. W 2003 roku rozpoczęła się techniczna realizacja projektu, a w 2004 roku ruszyła dystrybucja nowych dokumentów tożsamości. Do 2011 roku BelPIC objął zasięgiem 9 mln obywateli i rezydentów Belgii, a na jego bazie dostarcza się obecnie ponad 600 usług sektora publicznego i prywatnego.

W Niemczech elektroniczny dokument tożsamości (*neuer Personalausweis* – w skrócie nPA) wszedł do użytku 1 listopada 2010 roku. Jego premiera była ukoronowaniem około 10-letniego procesu planowania i projektowania, skomplikowanego koniecznością dokonania zmian w konstytucji. Ustawa o dowodzie osobistym i elektronicznym poświadczeniu tożsamości została uchwalona 18 czerwca 2009 roku. W styczniu 2010 roku opublikowano specyfikację techniczną dokumentu tożsamości oraz zainicjowano podprojekt projektu nPA, którego celem było wdrożenie przez wybranych partnerów usług elektronicznych bazujących na funkcjonalnościach dokumentu. Publiczna premiera dokumentu miała miejsce 1 listopada 2010 roku w trakcie targów CeBIT. Na użytek nPA opracowano szereg interesujących standardów technicznych, których część została przyjęta przez europejskie instytucje standaryzacyjne. Z drugiej strony, zawarte w nPA rozwiązania i funkcjonalności wykraczają poza i ponad normy dotyczące klasycznego podpisu elektronicznego, potwierdzając tym samym ograniczenia tego ostatniego.

W krajach, w których sektor publiczny nie podjął wyzwania cyberprzestrzeni próżnię wypełniły instytucje sektora prywatnego. W Danii bank centralny zainicjował prace nad nowym rozwiązaniem w zakresie uwierzytelnienia, a ich owocem, zaakceptowanym następnie w skali duńskiego sektora bankowego oraz w administracji publicznej i w niektórych internetowych serwisach sektora prywatnego, jest system NemID. System opracowany przez firmę należącą do banku centralnego został zainaugurowany 1 czerwca 2010 roku. Umożliwia on dwuczynnikową procedurę uwierzytelnienia, opartą na znanym jedynie użytkownikowi haśle statycznym oraz hasłach jednorazowych pobieranych z posiadanej karty lub sprzętowego tokena. W 2011 roku identyfikatory NemID posiadało ok. 3 mln mieszkańców Danii. Rozwiązanie jest uważane za przykład harmonijnej współpracy sektora publicznego i prywatnego.

Innym rozwiązaniem, powstałym w sektorze finansowym i uznanym następnie przez sektor publiczny, jest szwedzki system BankID, który został wdrożony przez grupę wiodących banków skandynawskich i uruchomiony w 2003 roku. BankID bazuje na standardach technicznych PKI zgodnych z dyrektywą EU, a każdy z 9 banków pełni rolę kwalifikowanego dostawcy usług certyfikacyjnych. Pozwala to w naturalny sposób rozciągnąć zastosowanie systemu także na instytucje sektora publicznego. W efekcie z systemu korzysta obecnie ponad 3 mln osób, a na jego bazie skonstruowano ponad 1 tys. usług zarówno dla sektora prywatnego, jak i publicznego.

Także ze Skandynawii pochodzi kolejny przykład twórczego podejścia do usług zaufania, stanowiącego hybrydę usług realizowanych przez sektor publiczny i prywatny. Rząd Norwegii oferuje dostawcom usług elektronicznych usługę sfederowanej tożsamości w postaci portalu ID-Porten. Portal ten pozwala rządowi, ok. 300 gminom norweskim i prywatnym dostawcom usług na wdrożenie jednolitego podejścia do identyfikacji i uwierzytelnienia, niezależnie od typu poświadczenia tożsamości. ID-Porten akceptuje poświadczenia tożsamości wydawane zarówno przez sektor publiczny (MinID – norweski odpowiednik polskiego profilu zaufanego), jak i prywatny (omówiony powyżej BankID, Buypass wydawany w formie karty przez narodową loterię oraz Commfides – certyfikat PKI wydawany w formie tokena USB). Federacja usług zaufania różnego pochodzenia jest jednym z najgorętszych trendów w zarządzaniu tożsamością, toteż norweski przykład zasługuje na uwagę.

Powyższy przegląd pozwala zidentyfikować kilka typowych modeli realizacji usług zaufania:

1. Świadczone przez sektor publiczny:
   a) na użytek własny,
   b) adresowane także do sektora prywatnego.
2. Świadczone przez:
   a) dostawcę na użytek własny,
   b) dostawcę na użytek powszechny, w tym w sektorze publicznym (np. BankID, PKI),
   c) grupę dostawców na użytek własny,
   d) grupę dostawców na użytek powszechny, w tym w sektorze publicznym (np. NemID).
3. Sfederowane:
   a) w ramach sektora prywatnego,
   b) z udziałem sektora publicznego.

A tymczasem u nas...

W Polsce, zarówno w sektorze publicznym, jak i prywatnym, dominują elementarne modele struktury zaufania. W sektorze publicznym rozwinął się jedynie model opisany powyżej jako 1a, przy czym nie osiągnięto ujednolicenia rozwiązań – obok profilu zaufanego funkcjonują rozwiązania sektorowe, np. poświadczenia tożsamości stosowane przez ZUS lub NFZ. W sektorze prywatnym dominują rozwiązania typu 2a, w większości realizowane w standardach niepozwalających uzyskać akceptacji poza domeną dostawcy, oraz, w ograniczonym zakresie, 2b, czyli standardowa infrastruktura PKI.

W swoim czasie nadzieję na zmianę tego pejzażu dawała realizacja projektu pl.ID. Jednym z jego planowanych efektów miało być wyposażenie obywateli Polski w nowoczesny dokument tożsamości, którego warstwa elektroniczna miała zapewnić co najmniej dwa różne sposoby uwierzytelnienia w systemach teleinformatycznych. Pierwszym był tzw. podpis osobisty, wydawany bezpłatnie przez wystawcę dokumentu, którego użycie w systemach sektora publicznego miało być równoważne podpisowi tradycyjnemu. Ustawa przewidywała także możliwość uznania podpisu osobistego przez podmioty spoza sektora publicznego. Oprócz tego dokument tożsamości miał zawierać obszar zarezerwowany dla osadzenia tradycyjnego podpisu elektronicznego w standardzie PKI, wystawianego przez kwalifikowany urząd certyfikacji.[3] Realizacja projektu w jego pierwotnej strukturze pozwoliłaby osiągnąć efekt przewyższający znaczenie projektów BelPIC lub nPA, zapewniając wspólną infrastrukturę zaufania sektora publicznego i prywatnego. Skala i znaczenie projektu przyciągały zainteresowanie wielu instytucji, a ich wpływ na strukturę projektu nie zawsze miał na celu umacnianie zaufania do dokumentu. W pierwotnej wersji ustawy o dowodzie osobistym przyjęto np. rozwiązania wprowadzające w zakamuflowany sposób szczególną strukturę podpisu osobistego, pozwalającą na szeroką inwigilację jego użytkowników, a także uniemożliwiającą należytą ochronę klucza prywatnego użytkownika. Mimo wyeliminowania większości słabości w toku dalszych prac legislacyjnych, projekt został ostatecznie poważnie zmodyfikowany pod wpływem powszechnie znanego, związanego z jego realizacją skandalu korupcyjnego. Efektem

---

3 Sfera potencjalnych zastosowań dokumentu pl.ID była w istocie szersza i zakładała m.in. osadzenie na wspólnym nośniku funkcjonalności karty ubezpieczenia zdrowotnego oraz innych funkcjonalności, niezdefiniowanych w momencie personalizacji dokumentu, konfigurowanych w trakcie użytkowania dokumentu.

finalnych modyfikacji była m.in. całkowita rezygnacja z warstwy elektronicznej dokumentu, a w konsekwencji – związanych z nią usług zaufania.

W rezultacie przyjętych zmian w pl.ID jedynym składnikiem powszechnej infrastruktury zaufania sektora publicznego jest obecnie tzw. profil zaufany (PZ). Liczne słabości PZ powalały traktować go jedynie jako rozwiązanie przejściowe przed wdrożeniem pl.ID. Po rezygnacji z warstwy elektronicznej w pl.ID administracja publiczna z konieczności promuje użycie PZ, podejmując jednocześnie działania obliczone na doraźne podniesienie jego bezpieczeństwa. Ma temu służyć m.in. przesyłanie haseł jednorazowych innym kanałem (SMS) niż zasadniczy kanał komunikacji.[4] Nie zmienia to faktu, że PZ lokuje się zaledwie na drugim poziomie wiarygodności w rozumieniu normy ISO 29115, a z przyczyn natury strukturalnej brak możliwości dalszego podniesienia poziomu jego bezpieczeństwa. Po modyfikacjach PZ będzie właściwym narzędziem do uwierzytelniania w usługach publicznych o charakterze wyłącznie informacyjnym. Jego poziom bezpieczeństwa pozostanie niewystarczający dla składania z jego wykorzystaniem oświadczeń woli. Wydaje się, że administracja publiczna była świadoma problemu zlecając wydzielenie funkcjonalności PZ ze struktury platformy ePUAP.[5] Krok ten nie przyczynia się do podniesienia bezpieczeństwa, jest jednak konieczną przesłanką zastąpienia w przyszłości PZ przez inną metodę identyfikacji i uwierzytelnienia. PZ nie cieszy się zaufaniem ze strony innych instytucji sektora publicznego: konstruując Platformę Usług Elektronicznych ZUS przewidział emisję własnego profilu PUE, a NFZ wymaga dla dostępu do Zintegrowanego Informatora Pacjenta uzyskania indywidualnego konta ZIP. Powyższe obserwacje nie pozwalają prognozować akceptacji i szerokiego zastosowania PZ. Tym samym w przewidywalnym okresie administracja publiczna w Polsce nie będzie dysponować bezpieczną i powszechnie akceptowaną infrastrukturą zaufania, której wykorzystanie mogłaby zaoferować podmiotom spoza sektora publicznego.

Niekonsekwencji działań w sektorze publicznym towarzyszy sektorowy charakter projektów podejmowanych w sektorze prywatnym. Walor powszechności posiadają jedynie podpisy elektroniczne certyfikowane przez kwalifikowane urzędy certyfikacji w ramach infrastruktury PKI. Niestety, zakres ich zastosowania i wykorzystania wynika w większym stopniu z przymusu administracyjnego (por. składanie deklaracji ZUS) niż rzeczywistej użyteczności.

4 Zamówienie publiczne 56-CPI-ZZP-2244/12 CPI MAiC.

5 Zamówienie publiczne 42-CPI-ZZP-2244/12 CPI MAC.

Poza infrastrukturą PKI podmioty prywatne preferują budowę własnej infrastruktury zaufania, dostosowanej do realizowanych procesów biznesowych i nieakceptowanej poza ich sferą. W tym zakresie przejawiają sporą kreatywność, oferując rodzaje identyfikacji i uwierzytelnienia reprezentujące większość metod znanych z teorii i praktyki. Ich zróżnicowanie może wynikać w znacznej mierze z przeniesienia na grunt krajowy praktyk stosowanych przez zagraniczne instytucje–matki. W dłuższej perspektywie czasowej nie stanowi ono czynnika sprzyjającego integracji.

W polskiej praktyce pojawiła się dotąd jedna, i to jedynie nieformalna, próba konstrukcji sfederowanego systemu zarządzania tożsamością. Mowa o uwierzytelnieniu klientów banków przez realizację symbolicznych przelewów z innych instytucji, w których dany podmiot posiada rachunek. System bazuje na założeniu, że właściwa identyfikacja klienta nastąpiła w innej instytucji finansowej w wyniku zastosowania przepisów ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.[6] System jest funkcjonalny, wydaje się jednak, że opisana procedura uwierzytelnienia nie jest perspektywiczna. Cechują ją liczne ograniczenia: słaba podstawa prawna, wysoki koszt realizacji w wypadku potwierdzania tożsamości w czasie rzeczywistym, brak mechanizmów autokorekcji, tendencja do propagacji skutków ew. błędów i nadużyć, ograniczona użyteczność poza sektorem finansowym.

Ważne są tylko te dni, których jeszcze nie znamy...

W nadchodzących latach zasadniczym czynnikiem kształtującym infrastrukturę zaufania w krajach UE będą prace wokół projektu regulacji dotyczącej *elektronicznej identyfikacji i usług zaufania dla transakcji elektronicznych*.[7] Samo podjęcie prac nad nową regulacją dowodzi przeświadczenia, że wcześniejsze akty dotyczące tego obszaru wyczerpały swój potencjał, nie nadążając za rozwojem technologii i rynku. Warto zwrócić uwagę na kilka ogólnych aspektów dotyczących projektu. Po pierwsze, Unia Europejska zdecydowała się tym razem sięgnąć po formułę regulacji, a nie dyrektywy. Regulacja, obowiązująca na terenie UE wprost, bez konieczności transpozycji jej postanowień do prawa krajowego, jest narzędziem dalece bardziej skutecznym i natychmiastowym w działaniu od dyrektywy. Jak się wydaje, UE ma świadomość

6 Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, Dz. U. 2010 nr 46, poz. 276, art. 8b, ust. 3, p. 1.

7 COM(2012) 238 final.

rozchodzenia się praktyki funkcjonowania usług zaufania w krajach UE z celami określonymi w Agendzie Cyfrowej 2020. Po drugie, projekt w obecnej formie znacząco poszerza listę usług zaufania w stosunku do wcześniejszej legislacji. Obok tradycyjnego podpisu elektronicznego w projekcie pojawiają się koncepcje cyfrowej pieczęci (art. 28), elektronicznych znaczników czasu (art. 32), dokumentów elektronicznych (art. 34), elektronicznych usług dostarczania informacji (art. 35) i autentykacji serwisów internetowych (art. 37). W tym kontekście objęcie ich wspólną nazwą usług zaufania jest całkowicie uzasadnione. Po trzecie, projekt pozwala nadać moc wiążącą także niekwalifikowanym poświadczeniom tożsamości na podstawie analizy ryzyka związanego z ich obszarem zastosowania. Po czwarte i najważniejsze z punktu widzenia poniższej analizy, projekt zasadniczo przesuwa akcenty odpowiedzialności za realizację usług zaufania.

Struktura aktualnie obowiązujących aktów prawnych powierza budowę infrastruktury zaufania w zasadzie instytucjom sektora prywatnego, zastrzegając dla państwa regulację i nadzór. Art. 2 ust.1 nowego projektu stanowi, że *(r)egulacja dotyczy usług elektronicznej identyfikacji świadczonych przez kraj członkowski, w jego imieniu lub na jego odpowiedzialność*. Art. 5, 6 i 7 projektu przewidują budowę zintegrowanej, paneuropejskiej infrastruktury zaufania złożonej z komponentów krajowych, których funkcjonowanie zostało notyfikowane Komisji Europejskiej w sposób opisany w art. 7 regulacji. Istotne jest, że notyfikacji podlegają wyłącznie *środki identyfikacji elektronicznej wydawane przez kraj członkowski, w jego imieniu lub na jego odpowiedzialność*. Innymi słowy, Unia Europejska stoi obecnie na stanowisku, że usługi zaufania stanowią część ogólnej infrastruktury publicznej, za której budowę i utrzymanie odpowiedzialne są kraje członkowskie, przy czym następuje zasadnicze przesunięcie odpowiedzialności za jej konstrukcję z sektora prywatnego na publiczny. Jednocześnie uznając, że sektor publiczny niektórych krajów członkowskich może nie być zainteresowany lub nie posiadać kompetencji dla budowy infrastruktury zaufania, projektowana regulacja pozwala powierzyć realizację zadania innym podmiotom, także reprezentującym sektor prywatny. Jeśli jednak dostarczane przez nie usługi mają stanowić część paneuropejskiej infrastruktury zaufania, muszą być realizowane w imieniu lub na odpowiedzialność państwa.

Projektowana regulacja pozwala państwom stosować w ramach sektora publicznego rozwiązania prostsze i tańsze niż kwalifikowane podpisy cyfrowe (art. 20 ust. 4). W takim przypadku metoda uwierzytelnienia jest dopuszczana do użytku w innych krajach członkowskich wyłącznie w odniesieniu do

usług, które na podstawie analizy ryzyka wymagają użycia metod o zbliżonym poziomie bezpieczeństwa. W projekcie zawarto delegacje dla Komisji Europejskiej wydania aktów wykonawczych określających standardy techniczne opisanych w regulacji usług (art. 38 i inne). Art. 39 przewiduje, że Komisja będzie w tym zakresie współpracować z komitetem reprezentującym kraje członkowskie, sytuacja będzie zatem odmienna od zaistniałej wskutek przyjęcia Dyrektywy 1999/93/EC. Wtedy państwa określały wymogi regulacyjne wobec nadzorowanych podmiotów prywatnych. Tym razem KE przy współudziale przedstawicieli krajów członkowskich określi wymogi techniczne wobec usług realizowanych przez same kraje lub w ich imieniu. Pozwala to mieć nadzieję, że wymagania zostaną określone w racjonalny sposób, na podstawie rzetelnej analizy potrzeb i ryzyk.

Powyższe spostrzeżenia potwierdzają, że decyzję o rezygnacji z warstwy elektronicznej w pl.ID podjęto bez uwzględnienia kierunków prac legislacyjnych UE i ich długofalowych skutków dla rozwoju elektronicznej gospodarki i cyfrowego społeczeństwa w naszym kraju. Jeżeli Polska będzie aspirować do uczestnictwa w paneuropejskiej infrastrukturze zaufania (a rezygnując zeń obniży konkurencyjność podmiotów krajowego sektora prywatnego oraz skomplikuje życie milionom Polaków), w ciągu najbliższych kilku lat polska administracja publiczna będzie musiała zbudować powszechny system elektronicznej identyfikacji lub powierzyć jego konstrukcję i zarządzanie instytucjom sektora prywatnego. Nie będzie to łatwe zadanie. Ukształtowanie konsensusu dotyczącego struktury uwierzytelnienia w pl.ID pomiędzy ówczesnym MSWiA i Ministerstwem Gospodarki kosztowało sporo wysiłku i czasu. Obecnie udział trzeciego gracza, Ministerstwa Administracji i Cyfryzacji, komplikuje zadanie jeszcze bardziej, bowiem nadzór nad sferami związanymi z różnymi usługami zaufania określonymi w projekcie regulacji jest podzielony pomiędzy całą trójkę. Zważywszy ponadto, że głównymi konsumentami usług zaufania w sektorze publicznym będą inne resorty lub podległe im podmioty (m.in. MF i aparat skarbowy, ZUS, NFZ), uzgodnienie wspólnego kształtu usług zaufania, a tym bardziej jego implementacja i zarządzanie infrastrukturą, mogą okazać się zadaniem ponad siły sektora publicznego.

Oznacza to wyzwanie i szansę dla sektora prywatnego, który może stać się partnerem państwa w tworzeniu infrastruktury zaufania służącej obu sferom: publicznej i prywatnej. Szansa ta otwiera się w szczególności przed sektorami, które dysponują już własną, rozbudowaną infrastrukturą zaufania, niezbędną dla realizacji kluczowych procesów biznesowych: sektorem bankowym oraz

operatorami telefonii mobilnej. Nie oznacza to jednak, że droga do współpracy sektora prywatnego i publicznego w tym zakresie jest prosta i wolna od przeszkód. Zasadniczą przeszkodą jest odmienne postrzeganie problemów, jakie rozwiązują usługi zaufania i tym samym odmienny charakter proponowanych rozwiązań. Biznes, a w jego ramach szczególnie sektor usług finansowych ma bogate doświadczenie w stosowaniu wobec planowanych przedsięwzięć analizy ryzyka. Definiując miarę akceptowalnego ryzyka menedżer poszukuje najtańszych rozwiązań technicznych i organizacyjnych, pozwalających prowadzić daną działalność bez przekraczania założonego progu. Większość metod uwierzytelnienia stosowanych obecnie w sektorze bankowym nie należy do górnych dwóch grup wiarygodności w rozumieniu normy ISO 29115, tym niemniej ich zastosowanie pozwala utrzymać poziom błędu w założonych ramach. Administracja publiczna stosuje podejście z gruntu odmienne. Jedynym rodzajem ryzyka, które jest skłonna mierzyć, jest ryzyko polityczne, wymierne słupkami notowań w sondażach. We wszystkich innych sferach sektor publiczny wykazuje wręcz doskonałą awersję wobec ryzyka, w każdej sferze i w każdych okolicznościach preferując rozwiązania pozwalające całkowicie uniknąć podejmowania ryzyka lub przynajmniej jako takie przedstawiane. Naturalna dla administracji postawa ulegnie zapewne spotęgowaniu przy dyskusji nad usługami, *nomen omen*, zaufania. Metody uwierzytelnienia uważane za wystarczające dla celów biznesowych prawie bez wyjątku okażą się nie dość bezpieczne dla sektora publicznego. Luka, która pojawi się między stanowiskami sektora publicznego i prywatnego nie będzie rezultatem nieracjonalnego uporu z którejkolwiek strony, lecz naturalnej różnicy ról partnerów. Powstanie wspólnej infrastruktury zaufania dla sektora publicznego i prywatnego nie jest w tej sytuacji przesądzone, choć z pewnością jej funkcjonowanie byłoby tańsze niż utrzymanie odrębnych rozwiązań dla każdej sfery. Co więcej, udział sektora prywatnego pozwoliłby na bardziej efektywne zarządzanie powstałą infrastrukturą. Wymaga to jednak ze strony sektora prywatnego gotowości do zaakceptowania rozwiązań wykraczających poza jego własne potrzeby biznesowe, a ze strony sektora publicznego – rezygnacji z rozwiązań ingerujących w prywatność obywateli i poufność procesów biznesowych w sektorze prywatnym.

Zamiast podsumowania pokuśmy się o krótką analizę atutów i słabości dwóch głównych pretendentów do roli partnera administracji w budowie infrastruktury zaufania: sektora bankowego i operatorów mobilnych. Dla sektora bankowego zaufanie, nie tylko w rozumieniu identyfikacji i uwierzytelnienia,

jest zasadniczym aktywem. Regulacje dotyczące potwierdzania tożsamości klientów są w przypadku banków bardziej rygorystyczne niż w wypadku operatorów: założenie anonimowego lub pseudonimowego rachunku bankowego jest zasadniczo trudniejsze, o ile w ogóle możliwe, od uzyskania karty SIM niepowiązanej z prawdziwą tożsamością użytkownika. W efekcie praktyka banków w zakresie potwierdzania tożsamości klientów jest dalece bardziej rozwinięta niż w wypadku operatorów. Pod pewnymi względami przewyższa także doświadczenia sektora publicznego: bankowy zbiór dokumentów zastrzeżonych może aspirować do roli rejestru referencyjnego także dla administracji.

Ale operatorzy mobilni także mogą wyciągnąć kilka atutów. Skala penetracji rynku z ich strony przewyższa osiągnięcia banków: w Polsce zarejestrowano większą liczbę kart SIM niż wynosi ludność kraju. Sektor bankowy nie zdołał dotąd wypracować wspólnych i powszechnych mechanizmów uwierzytelnienia; po stronie operatorów unifikacja wynika wprost z wykorzystania tych samych standardów technicznych i interoperacyjności systemów. W wypadku wykorzystania bardziej zaawansowanych metod uwierzytelnienia w sektorze bankowym każdego klienta trzeba wyposażyć w odpowiedni sprzęt; w przypadku operatorów mobilnych niezbędny sprzęt większość klientów nosi już w kieszeni. W przypadku protokołów uwierzytelnienia online operator mobilny zapewnia klientom łączność w ramach zasadniczej usługi. Z drugiej strony – obecnie rozprowadzane karty SIM nie zawierają funkcjonalności pozwalających wykorzystać je wprost do bezpiecznego uwierzytelnienia. Próba budowy powszechnej infrastruktury zaufania na bazie zasobów operatorów wiązałaby się z wymianą wszystkich kart SIM, przedsięwzięciem nie tyle kosztownym, ile złożonym logistycznie.

Reasumując, atuty obu sektorów wydają się wyrównane. Zważywszy coraz większe zainteresowanie operatorów płatnościami mobilnymi z jednej strony, a instytucji finansowych – bankowością mobilną z drugiej, można prognozować umacnianie synergii pomiędzy nimi. Obszar usług zaufania jest dobrym terenem dla poszukiwania nowych form współpracy.