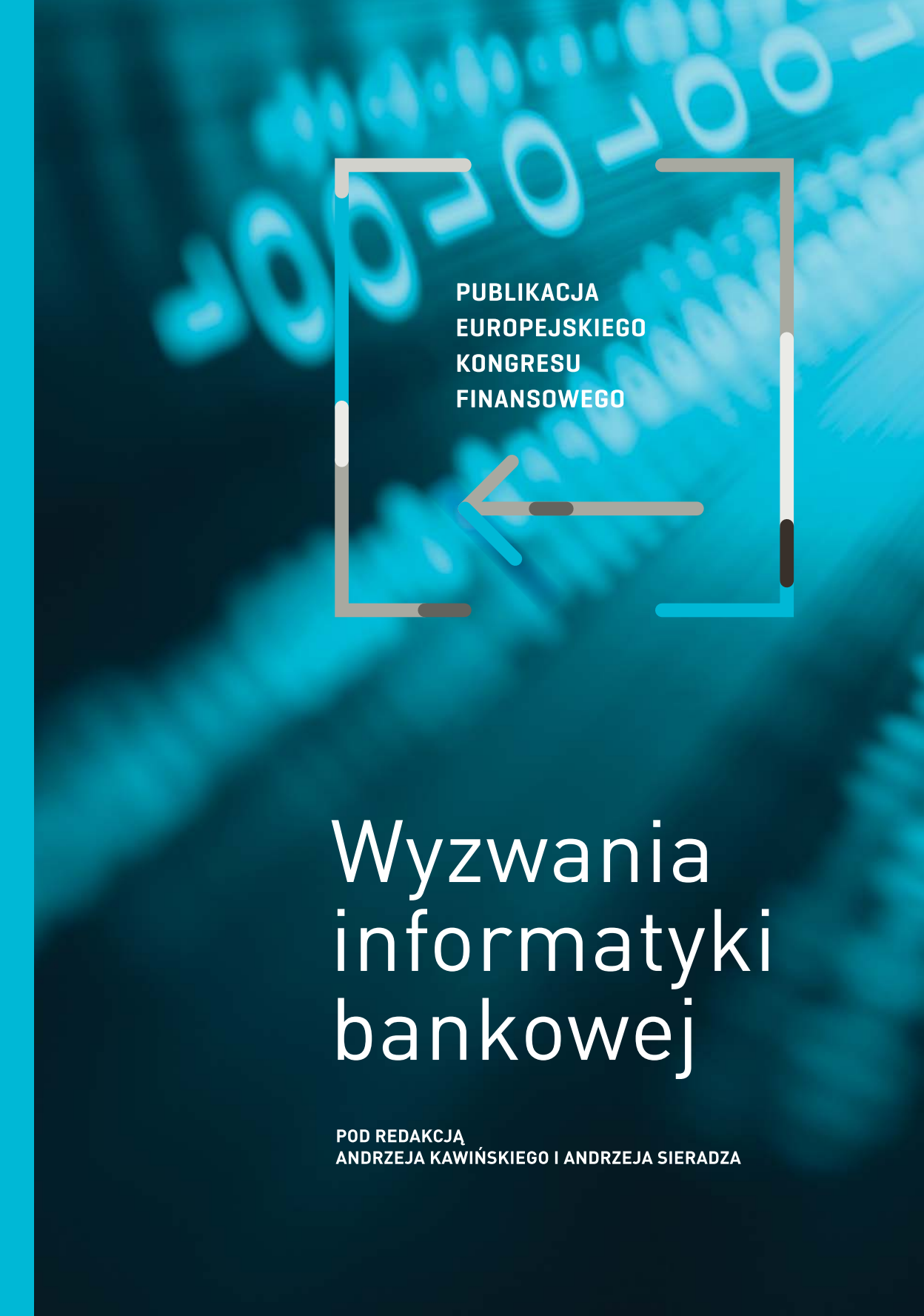


PUBLIKACJA
EUROPEJSKIEGO
KONGRESU
FINANSOWEGO

Wyzwania informatyki bankowej

POD REDAKCJĄ
ANDRZEJA KAWIŃSKIEGO I ANDRZEJA SIERADZA

EUROPEAN
FINANCIAL
CONGRESS

Wyzwania Informatyki Bankowej

– Materiał przygotowany na podstawie seminariów IT w Instytucjach Finansowych organizowanych przez Gdańską Akademię Bankową

GDAŃSK 2015

© 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 978-83-88835-24-7

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

Spis treści

Wstęp 7

Bartłomiej Nocoń, Bartosz Zborowski
Bankowość mobilna i płatności mobilne 11

Andrzej Pyka, Andrzej Sieradz
Bank Detaliczny ery „Digital" 21

Maciej Majewski
Big Data w walce z atakami cyfrowymi 31

Robert Gajda, Maciej Gawroński, Andrzej Gibas
Czas na chmurę w sektorze finansowym w Polsce! 47

Maciej Kaniewski
Metodyki Agile – blaski, cienie i szare strefy 61

Dina Dąbrowska, Bartłomiej Owczarek
Zwinne zarządzanie programami 79

Aleksander P. Czarnowski
Obecne zagrożenia w bankowych systemach IT 91

Joanna Gałajda, Maciej Gawroński
Aktualne trendy regulacji technologii bankowych 119

Anna Baryła, Rafał Burzyński, Tomasz Rzepa
Common Reporting Standard 133

Grzegorz Kuliszewski, Andrzej Sieradz
Banki – platforma cyfrowa dla usług administracji państwowej? 145

Marek Grajek
Uwierzytelnianie klienta banku w rozwoju cyfryzacji sektora publicznego 163

Andrzej Kawiński
Zarządzanie gotówką 181

Wstęp

Oddajemy w Państwa ręce drugie opracowanie będące kontynuacją pomysłu z roku 2014, a zainspirowane wynikiem dorocznych dyskusji i spotkań środowiska przedstawicieli sektora finansowego oraz dostawców rozwiązań IT dla tegoż sektora w ramach konferencji „IT – w instytucjach finansowych", które poprzedziło przygotowania do tego wydarzenia.

W tym roku konferencja odbyła się po raz dwudziesty, a w jej trakcie przedstawiciele sektora finansowego spotkali się pod auspicjami Gdańskiej Akademii Bankowej w celu przedyskutowania najważniejszych wyzwań i zjawisk, przed jakimi stoją instytucje finansowe w Polsce. Ożywiona dyskusja i prezentacje, które inicjują tę dyskusję mają za zadanie zaadresowanie ważnych zagadnień i wypracowanie w toku dyskusji kilka rekomendacji dotyczących tematów ważnych dla rozwoju usług finansowych w Polsce, co do których, stosownie do opinii uczestników konferencji, należałoby podjąć inicjatywy sektorowe.

Dyskusja nad opracowaniem zagadnień w poprzednim wydaniu przekonała nas co do konieczności kontynuacji inicjatywy wydawania i rozszerzenia listy zagadnień, jakie wydają się być interesujące dla całego sektora finansowego.

Podobnie, jak w zeszłym roku, cześć zagadnień jest ciągle aktualna i wymaga uaktualnienia, stąd też tegoroczna lista publikacji zawiera cześć artykułów, które są rozszerzoną wersją publikacji z zeszłego roku. Doszły też nowe zagadnienia i tematy, które będą odgrywać coraz większe znaczenie w najbliższych latach.

Przyglądając się, jak co roku, wyzwaniom, jakie stoją przed nowoczesnym sektorem finansowym, jak i nowym zjawiskom na rynku, zmieniającym w dynamicznym stopniu w naszym przekonaniu dotychczasowy model biznesowy

tego sektora, doszliśmy do wniosku, że wiele z nich już staje się naszą rzeczywistością i dokonują się zmiany fundamentalne dla przyszłości sektora finansowego. Współpraca i wzajemne zrozumienie zagadnień pomiędzy deparatamentami biznesu, informatyki i bezpieczeństwa jest obecnie głównym motorem jego rozwoju.

Cześć nowo obserwowanych produktów i usług finansowych, czasami oferowanych niekoniecznie przez „typowe" i „tradycyjne" organizacje finansowe od dawna funkcjonujące na rynku, są konsekwencją dynamicznie rozwijających się usług opartych na nowych technologiach IT, a w szczególności technologiach mobilnych.

Coraz powszechniej mówi się o konieczności zastosowania koncepcji całkowitej zmiany podejścia do klienta i przeniesienia usług finansowych do przestrzeni określanej jako „digital", podążając za klientami i współtworząc razem z nimi nowe rozwiązania.

Postanowiliśmy zatem podjąć próbę problemowego zaadresowania szerokiego wachlarza 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.

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

Intencją podjęcia prezentowanych zagadnień było zatem odniesienie się do nich z punktu widzenia przyszłości usług finansowych, a nie pojedynczego uczestnika rynku. Znalazły się wśród nich takie zagadnienia, jak bankowość mobilna, bezpieczeństwo transakcji płatniczych, współpraca spoza-bankowymi uczestnikami rynku płatniczego czy wymiana technologiczna związana z wielokanałowością dystrybucji produktów i usług finansowych.

Funkcjonowanie instytucji finansowych obecnie nie jest możliwe bez informatyki. Aktualne trendy rynkowe i możliwe technologie umożliwiają jednocześnie zmniejszenie kosztów IT w instytucjach finansowych i przyspieszenie cyklu rozwoju produktów i usług oferowanych klientom. Tym bardziej ważne jest i będzie coraz ważniejsze sprawne współdziałanie i wzajemne zrozumienie departamentów informatycznych z działami biznesowymi oraz ds. bezpieczeństwa.

Przygotowując tegoroczną publikację naszą intencją było przedstawienie skomplikowanych zagadnień, które omawiamy w wąskim gronie informatycznym, w sposób prosty i zrozumiały, 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 i mamy nadzieję że to się nam udało.

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

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

Andrzej Kawiński
Andrzej Sieradz

Bartłomiej Nocoń

Dyrektor Zarządzający Departamentem Bankowości Elektronicznej w Pionie Bankowości Detalicznej Banku Pekao S.A. Absolwent Akademii Ekonomicznej w Krakowie (obecnie Uniwersytet Ekonomiczny) na kierunku międzynarodowe stosunki gospodarcze i polityczne (specjalność handel zagraniczny) oraz stypendysta The Swedish School of Economics and Business Administration w Helsinkach.

Z obszarem bankowości elektronicznej i mobilnej oraz zarządzaniem finansami on-line związany od początku swojej kariery zawodowej. Na obecnym stanowisku od grudnia 2007 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% wszystkich sprzedanych telefonów, które trafiły na rynek[2]. W 2014 roku

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

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

– na rynek trafiło 1,3 mld smartfonów, a więc prawie 30% więcej niż w roku poprzednim.[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 w 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. Kolejnym krokiem były tzw. *serwisy light*, które są zredukowaną

3 http://www.idc.com/getdoc.jsp?containerId=prUS25407215

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

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, producenci urządzeń mobilnych, dostawcy systemów operacyjnych, dostawcy usług internetowych czy duże sieci detaliczne. Dzięki ich zaangażowaniu powstało wiele systemów oraz aplikacji pozwalających płacić, zbierać punkty, przekazywać

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.

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 w 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.

W tym kontekście warto zaznaczyć, że standard płatności zbliżeniowych, opartych na NFC, ze względu na swoją wygodę staje się jedną z najistotniej-

---

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

szych metod płacenia telefonem. Płatności zbliżeniowe dokonywane za jego pomocą to naturalna konsekwencja udanego trendu zapoczątkowanego przez karty zbliżeniowe.

Pierwszym krokiem łączącym telefon i kartę zbliżeniową były stickery, czyli naklejane na telefon mini-karty zbliżeniowe. Kolejnym etapem była integracja danych zapisanych na chipie karty płatniczej z danymi na karcie SIM posiadacza telefonu, co pozwoliło dokonywać płatności telefonem, bez konieczności fizycznego posiadania karty. Tak powstała technologia SIM-centric[10].

Rosnąca popularność technologii NFC sprawiła, że nawet firma Apple, która przez wiele lat opierała się wdrożeniu modułów tego typu w swoich urządzeniach, udostępniła usługę Apple Pay, która pozwoli użytkownikom najnowszego iPhone'a 6 płacić zbliżeniowo z wykorzystaniem kart płatniczych wydanych przez banki w Stanach Zjednoczonych.

Chyba najważniejszego jednak kroku w rozwoju płatności zbliżeniowych dokonał Google, producent najpopularniejszego na świecie systemu operacyjnego na smartfony Android, który umożliwił jeszcze łatwiejszą metodę tworzenia zbliżeniowych aplikacji płatniczych. Nowa technologia nazywa się HCE (*Host Card Emulation*) i umożliwia przechowanie danych poufnych na serwerze Banku, co znacznie upraszcza proces realizowania płatności i uniezależnia użytkownika od operatora telefonii komórkowej.

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 i kolejowej, 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

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

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 IV kwartału 2014 r. w obiegu znajdowało się ok. 25,7 mln kart z funkcją zbliżeniową, co stanowiło 71,3% 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 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. Rozwinięciem MasterCard Mobile jest usługa MasterPass, która ma mieć zasięg globalny i pokrywać cały e-commerce.

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

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

11 Dane NBP, *Informacja o kartach płatniczych IV kwartał 2014 r.*, s. 10, http://www.nbp.pl/systemplatniczy/karty/q_04_2014.pdf

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.

W grudniu 2014 roku Bank Pekao S.A., jako pierwszy w Polsce i jeden z pierwszych na świecie, uruchomił mobilne płatności zbliżeniowe telefonem w technologii HCE. Nowe rozwiązanie pozwoliło użytkownikom PeoPay płacić zbliżeniowo w terminalach z funkcją zbliżeniową PayPass[12] bez konieczności wiązania się z konkretnym operatorem komórkowym.

W kontekście płatności mobilnych należy wspomnieć o PSP (Polski Standard Płatności sp. z o.o.) powołanym przez 6 banków: Alior Bank, Bank Millennium, Bank Zachodni WBK, ING Bank Śląski, mBank oraz PKO Bank Polski, którego celem jest tworzenie mobilnego standardu pod nazwą BLIK. System ma zapewnić możliwość podłączania aplikacji mobilnych różnych banków oraz agentów rozliczeniowych.

Wszystkie powyższe rozwiązania charakteryzują się brakiem powszechności, która wynika z ograniczonej liczby punktów akceptujących tego typu płatności w porównaniu do kart płatniczych. Musi upłynąć jeszcze 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 dynamicznie rozwijającym się rynkiem, oferującym wiele rozwiązań, zarówno w zakresie stosowanych technologii, jak również oprogramowania. Obecnie rozwijanych jest wiele różnych technologii, takich jak chociażby:

12 Rozwiązanie dostępne dla posiadaczy smartfonów z systemem operacyjnym Android min. 4.4 (KitKat) oraz wyposażonych w antenę NFC.

wearable devices (np. inteligentne zegarki typu *smartwatch*, okulary HoloLens Microsoftu), usługi osobistych asystentów (Siri firmy Apple, Cortana firmy Microsoft) czy wreszcie technologie biometryczne, coraz śmielej stosowane w urządzeniach mobilnych (np. Apple Touch ID, czytnik linii papilarnych w Samsungu Galaxy S5/6). Do nowinek technologicznych dołączyło także wspomniane wcześniej 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 geolokalizacji w celu prezentowania użytkownikom ofert na podstawie informacji o miejscu, w jakim użytkownik się znajduje (np. zniżki na kawę w pobliskiej restauracji przy płatności kartą danego banku),
- sterowania głosowego, czyli wykorzystania mechanizmów rozpoznawania mowy do obsługi bankowości mobilnej, a także biometrii do logowania czy autoryzacji operacji np. odcisku palca w ramach płatności mobilnych (Apple Pay),
- 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,
- m-commerce – co trzeci kupujący w internecie korzysta ze smartfona, a co piąty – z tabletu[13], co stwarza szerokie możliwości rozwoju bankowości mobilnej (głównie w obszarze płatności mobilnych), która ma szansę stać się jednym z głównych filarów m-commerce łącząc ofertę, możliwość dokonania za nią zakupu i program lojalnościowy w ramach jednej aplikacji – tak jak czynią to obecnie sklepy tradycyjne.

Interesujące wyzwania dla bankowości mobilnej niosą wspomniane już *wearable devices* czyli technologie wykorzystujące inteligentne okulary czy zegarki typu *smartwatch*. Wybrane banki już zaczynają przygotowywać rozwiązania

13 Gemius Polska, *E-commerce w Polsce 2014. Gemius dla e-Commerce Polska*, http://www.infomonitor.pl/download/e-commerce-w-polsce-2014.pdf, s. 144

dedykowane dla tych urządzeń, np. nowozelandzki Bank Westpac, który udostępnił rozwiązanie dla inteligentnych zegarków (Cash Tank dla zegarka Sony SmartWatch).

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.

Andrzej Pyka

Dyrektor Pionu Consulting and Systems Integration odpowiedzialny za klientów z sektora finansowego w Europie Środkowo-Wschodniej w firmie Atos, gdzie pracuje od października 2013 roku. Z wykształcenia inżynier po Wydziale Elektroniki i Telekomunikacji na Politechnice Wrocławskiej i University of Nottingham. Jest też absolwentem IESE Business School na Uniwersytecie w Nawarze.

Może się pochwalić 20-letnim doświadczeniem w prowadzeniu projektów transformacyjnych, implementacji systemów oraz konsultingu operacyjnym. Wcześniej pracował w Accenture (1999–2013) i Andersen Consulting (1995–99), obsługując wiele instytucji z sektora bankowego, ubezpieczeń oraz telekomunikacji.

dr Andrzej Sieradz

Wiceprezes Zarządu Banku BGŻ. Doktor nauk ekonomicznych Uniwersytetu Gdańskiego. Ukończył Politechnikę Warszawską w 1983. Uzyskał również tytuł MBA Business International School w Warszawie oraz ukończył studia podyplomowe z zakresu finansów i bankowości w Szkole Głównej Handlowej. Zanim związał się z Bankiem BGŻ, w latach 2006–2010 był dyrektorem operacyjnym i członkiem zarządu ING Towarzystwo Ubezpieczeń na Życie S.A. oraz członkiem zarządu ING Usługi Finansowe S.A., gdzie odpowiadał za dział informatyki, obsługę klienta oraz zarządzanie projektami. W latach 2002–2006 związany z ING Bank Śląski S.A., najpierw jako dyrektor zarządzający. W latach 1997–2002 pracował w Coca-Cola HBC w Polsce i w centrali w Wiedniu.

Andrzej Pyka, Andrzej Sieradz

Bank Detaliczny ery „Digital”

Jednoczesny rozwój technologii i zmiana nawyków konsumentów oraz wejście w wiek dojrzały Pokolenia Y i Pokolenia Z[1] wykształciły nowy model klienta banku – klienta ery cyfrowej.

Jego oczekiwania i przyzwyczajenia zostały ukształtowane przez wszechobecny mobilny internet, popularność smartfonów i mediów społecznościach. Branża bankowa nie jest pionierem rewolucji cyfrowej. Klient ery cyfrowej został ukształtowany przez firmy takie jak Amazon.com, branżę telekomunikacyjną i firmy usługowe.

Amazon.com od wielu lat potrafi w ułamku sekundy podpowiedzieć klientowi produkty odpowiadające jego profilowi, przeprowadzić transakcję i (jeżeli są to książki, filmy czy muzyka) dostarczyć je natychmiast klientowi na czytnik Kindle lub inne urządzenie.

Firmy telekomunikacyjne stale przygotowują nowe pakiety usług i promują je w czasie rzeczywistym w zależności od profilu i kontekstu klienta (np. pakiet roamingowy przy przekroczeniu granicy) oraz aktywują je i deaktywują w trybie natychmiastowym 24 x 7.

Linie lotnicze odeszły od papierowych biletów i kart pokładowych. Umożliwiają przeprowadzenie całego procesu rezerwacji, zakupu biletu i check-in za pomocą smartfona, przy okazji sprzedają ubezpieczenia, oferują hotele i zapisują punkty frequent flyer.

„Wychowany” w ten sposób klient ery cyfrowej ma następujące nawyki i oczekiwania:

- nieograniczona interakcja z dostawcą produktów i usług w trybie 24x7 za pośrednictwem smartfona i/lub internetu,
- oczekiwanie spersonalizowanej oferty i mała tolerancja na „spam” (czyli propozycje nietrafione),

---

1 Opisane w artykule: Pokolenie Y: Nowy rodzaj pracowników – szanse i zagrożenia

- samodzielne poszukiwanie, ocena i porównywanie ofert od wielu konkurujących dostawców,
- pozyskiwanie opinii i rekomendacji od „znajomych",
- natychmiastowa realizacja (dostawa) lub aktywacja usługi,
- prostota i wygoda.

Współczesny bank musi dostosować sposób interakcji z klientami, swoje wewnętrzne procesy, technologię oraz pracowników do zmieniających się wymagań klienta i swojego otoczenia. Innymi słowy – musi stać się bankiem ery cyfrowej.

Definicja

„Cyfrowa Bankowość" to nowa koncepcja w obszarze bankowości elektronicznej, która ma na celu wzbogacenie standardowych usług online i bankowości mobilnej poprzez integrację technologii cyfrowych, na przykład strategicznych narzędzi interakcji analityki mediów społecznych, innowacyjnych rozwiązań płatniczych, technologii mobilnych i skupienie się na doświadczeniu użytkownika.

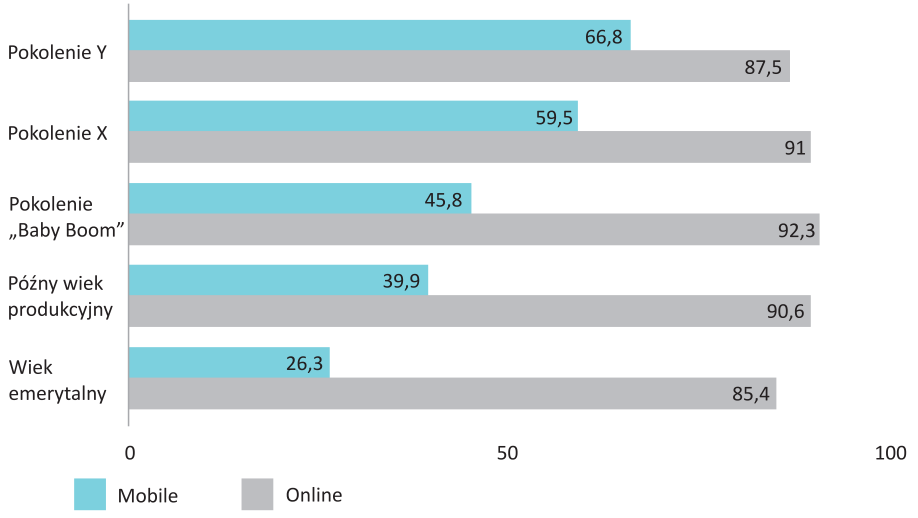
Rola banku i klienta

Oczekiwanie współczesnych klientów, co do możliwości nabywania produktów i usług bankowych oraz realizowania dostępu do tych zasobów, wskazują na potrzebę dostosowywania ich w tzw. Modelu Omni-Channel (czytaj: wielokanałowość) co oznacza, że klienci mogą realizować te same funkcjonalności we wszystkich kanałach, jakie bank oferuje. Dzisiejsza technologia umożliwia realizację pełnej interakcji z klientami przy pomocy kanałów zdalnych za pomocą dowolnych urządzeń, zarówno mobilnych, jak i stacjonarnych. Do klienta należy decyzja, w jaki sposób chce realizować tę interakcję. Podobnie dzieje się z bankami. Tradycyjna transakcyjna (i nie tylko) bankowość w oddziale banku znika z rynku. Klienci przyzwyczajeni do bankowości internetowej dziś oczekują pełnego zakresu produktowego i serwisowego w kanale mobilnym. Dzieje się tak dlatego, że rewolucja mobilna polegająca na powszechnym wykorzystywaniu smartfonów i tabletów czyni z tych urządzeń swoistego rodzaju „cockpit" dla każdego konsumenta. Nie ma odwrotu, wcześniej czy później urządzenia mobilne będą w 100% w użyciu dzisiejszych konsumentów. To kwestia 2–3 lat i kolejnej fazy zmiany technologicznej w grupie urządzeń mobilnych. Niedługo przestaniemy pamiętać, jak

wyglądał „telefon" tylko do wykonywania połączeń telefonicznych. Zmiana funkcjonalności urządzeń mobilnych jest nieunikniona, a wraz z nią wręcz nieograniczone możliwości wykorzystywania tych urządzeń w życiu codziennym konsumentów, w tym bankowości.

Nowe funkcje mobilne oferują nowe formy integracji z użytkownikiem––klientem: zupełnie inny dostęp do danych informacji i zupełnie inne zachowania klientów. Powoduje to zatem zupełnie inne oczekiwania konsumentów „mobilności" co do usług udostępnianych na platformach mobilnych. Oczekiwana jest pełna funkcjonalność: „on-line" w trybie 7/24/365. Usługa mobilna po prostu zawsze towarzyszy konsumentowi tam, gdzie w danej chwili się znajduje. Oczekiwana jest mobilność połączona z prostotą obsługi, co czyni wyzwanie „digital banking" jeszcze większym. Jednocześnie oczekiwana jest zminimalizowana interakcja z samym urządzeniem mobilnym. Bez zbędnego wpisywania danych, logowania, naciskania klawiszy, po prostu, jeśli tylko się da, usługa ma być „one click away". Era cyfrowa będzie wymagać prostoty na poziomie dwulatka połączonej z zakresem funkcjonalności odpowiadającej wymagającemu konsumentowi–użytkownikowi.

Udział respondentów, którzy obecnie używają lub rozważają używanie kanałów bankowych typu „mobile" lub „on-line" (w proc.)



Źródło: *PWC Digital Tipping Point Survey 2011.*

Implikacje dla banków

Oczekiwania klientów oznaczają dla banków zupełnie inne podejście do wielu aspektów nie tylko oferowania produktów i usług, ale również do przeorganizowania dostępu do danych i zmianę procesów biznesowych.

Główne aspekty, które będą definiować tzw. „Digital Banking" to:

- mobilność i ciągła dostępność,
- łatwość obsługi i prostota rozwiązań,
- zapewnienie bezpieczeństwa,
- indywidualna oferta produktowo-serwisowa na dowolnym urządzeniu, zgodna z zachowaniem klienta,
- decyzje klientów w czasie rzeczywistym,
- połączenie usług bankowych z szeroką grupą usług innych dostawców,
- możliwości e-commerce,
- wszystkie czynności bankowe łącznie z pełną obsługą wniosków kredytowych,
- łączenie karty bankowej, karty zdrowia, kart lojalnościowych i prawa jazdy,
- zestawy aplikacji, które pozwolą urządzeniom mobilnym zastąpić kasjerów banku.

Bankowość cyfrowa staje się rzeczywistością

Przykład pionierskiego rozwiązania daje słynący z innowacyjności Commonwealth Bank of Australia, który klientom poszukującym nowej nieruchomości oferuje *app* znacznie upraszczający proces zakupu i pozyskania kredytu hipotecznego. Przy jego użyciu klient banku może kierując kamerę smartfona na daną nieruchomość zidentyfikować ją, pozyskać informacje o jej stanie prawnym i poprzednich transakcjach zakupu oraz natychmiast uzyskać od banku ofertę finansowania dostosowaną do swojej zdolności kredytowej. W ten sposób klient oszczędza czas potrzebny na pozyskiwanie informacji od agenta nieruchomości, czytanie ksiąg wieczystych oraz przygotowywanie wniosku kredytowego. Przy tym otrzymuje od banku ofertę na kluczowy produkt dokładnie w chwili i w miejscu, kiedy emocjonalnie jest najbardziej gotowy na skorzystanie z niej.

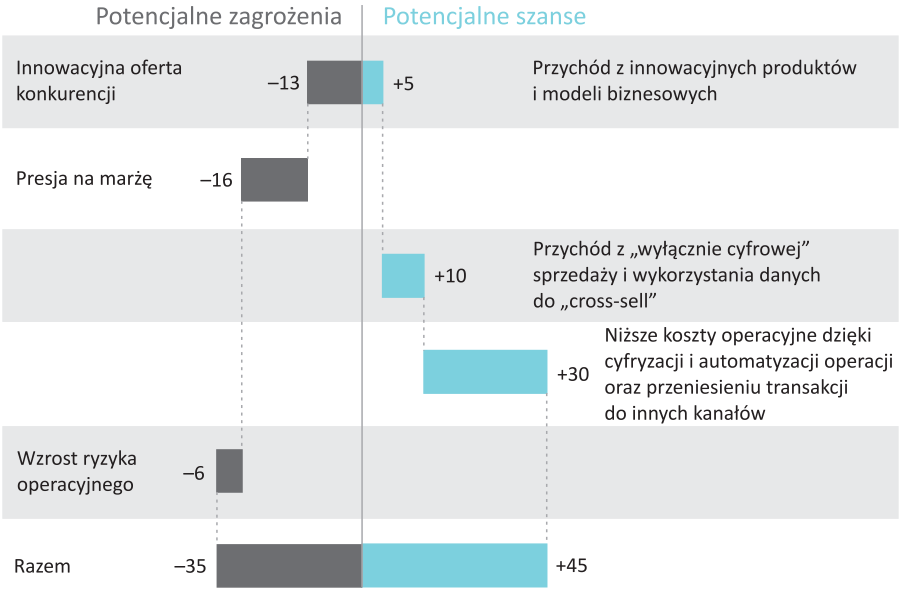
Innym przykładem jest iberyjski potentat BBVA, który całkowicie przeprojektował format placówki i wielokanałową interakcję z klientem. Kanał

cyfrowy jest podstawowym kanałem komunikacji klienta z bankiem. Wszystkie urządzenia – smartfony, tablety, bankomaty i stanowiska samoobsługowe w placówkach działają i wyglądają w sposób jednolity. W placówce zamiast typowych stanowisk kasjerskich i doradczych znajdują się loże do samodzielnej pracy klienta z dużym ekranem dotykowym. Pracownicy placówki przestali być „dysponentami" i pomagają klientom w korzystaniu z cyfrowych środków komunikacji lub doradzają z w złożonych zagadnieniach planowania finansowego. Możliwy jest także kontakt wideo z ekspertami z centrali banku.

Źródła wartości „digital banking"

Dlaczego, „digital banking" jest koniecznością dla banków? Pomijając zmieniające się zachowania klientów, pierwsze banki realizujące takie podejście już obserwują korzyści. Z analizy porównawczej firmy McKinsey wynika, że liczyć się będą dla banków w przyszłości główne: innowacje w zakresie nowych produktów i modeli biznesowych oraz doskonałość operacyjna wynikająca z dalszego postępu automatyzacji.

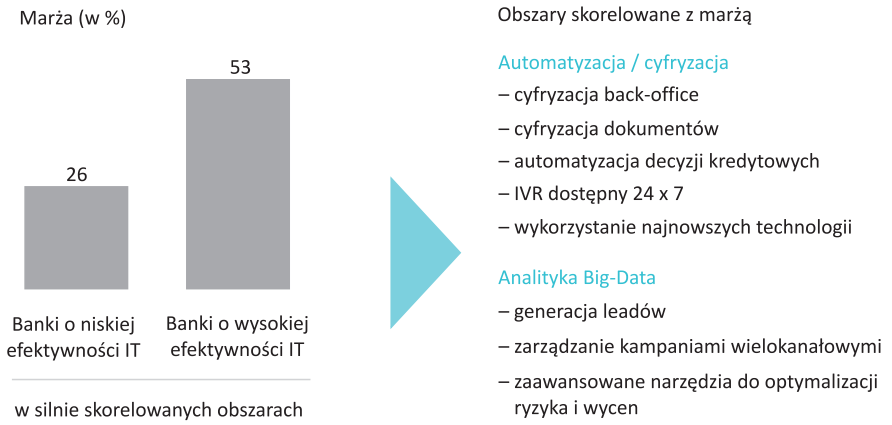
Wpływ transformacji cyfrowej jako % zysku netto banku



Źródło: *Analiza McKinsey*

Banki te obserwują nawet 2,5-krotny wzrost interakcji klientów z wykorzystaniem urządzeń mobilnych a to stwarza większe możliwości sprzedaży produktów i usług. Dodatkowy strumień dochodów pojawia się w obszarze zwiększonego wolumenu płatności o małej wartości, a do tego nowe możliwości przychodowe w obszarze aktywności przed- i posprzedażnych.

Banki osiągające wysokie marże przodują w wybranych obszarach cyfryzacji i analityki



Źródło: *Analiza dostarczona przez McKinsey Horison360*

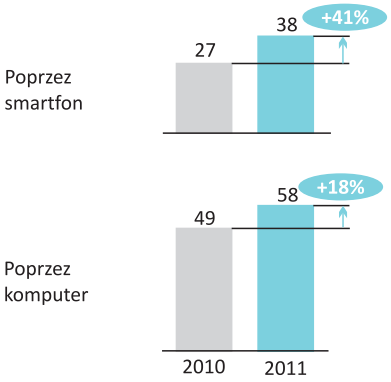
Zmieniają się zasady gry na rynku bankowym wynikające ze zmieniających się zachowań klientów. Według PwC[2] 61% konsumentów chce i poszukuje aktywnie nowych usług w przestrzeni cyfrowej, a 42% chce kupować te usługi i produkty samodzielnie, bez doradztwa. Ten sam raport ostrzega przed złą obsługą w świecie cyfrowym. Na podstawie badań z każdych pięciu niezadowolonych klientów banku dwóch zmieni bank na inny, a aż 45% będzie aktywnie odradzać propozycje banku wykorzystując serwisy i media społecznościowe w świecie cyfrowym.

2 Raport PwC, Retail BANKING 2020.

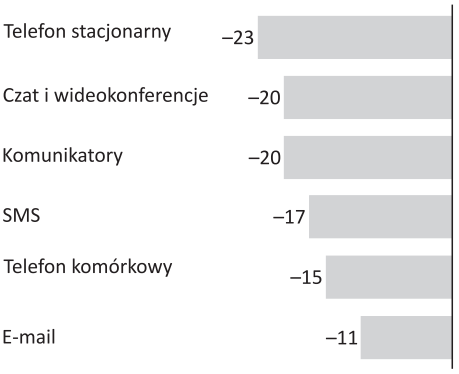
Korzystanie z mediów społecznościowych doprowadziło do spadku wykorzystania innych form komunikacji

Średnia europejska

Procent właścicieli urządzeń, którzy używają mediów społecznościowych co najmniej raz w tygodniu



W jakim stopniu korzystanie z mediów społecznościowych wpłynęło na korzystanie przez ciebie z innych sposobów komunikowania się? (w %)



Źródło: *McKinsey iConsumer (Europa 2011)*

Miejsce banku w cyfrowym ekosystemie

Gospodarka ery cyfrowej to sieć połączonych w trybie on-line dostawców usług, dostawców łączności, mediów społecznościach i mechanizmów płatności. Przyszła rola banku detalicznego w ekosystemie nie jest ustalona. Wydaje się, że banki mogą zajmować różne w nim różne miejsca i będzie to kluczowy wybór strategiczny.

Jedną z opcji jest wyjście banku poza rolę instytucji finansowej i ekspansja do roli „agregatora wartości" i stanie się „one-stop-shop" dla klienta. W tej roli bank, który:

- jest obecny przy każdej czynności ekonomicznej, gdyż obsługuje skojarzoną z nią płatność,
- ma dostęp do bardzo bogatych danych o kliencie, zwłaszcza o jego operacjach finansowych,
- cieszy się zaufaniem klienta

będzie starał się obsługiwać maksymalnie dużo potrzeb klienta angażując innych uczestników ekosystemu i aranżując ich cząstkowe usługi w sposób dogodny i optymalny dla klienta.

Inną opcją jest pozostanie banku w tradycyjnej roli. Niektóre jego usługi będą wtedy zastępowane przez analogiczne usługi instytucji nie-bankowych (finansowanie, płatności) lub będą oferowane rynkowi na zasadzie white-label, gdyż aranżerem transakcji będzie inny uczestnik ekosystemu.

Zadania dla banku w czasach „digital"

Jednym z głównych elementów, z którym banki będą musiały się zmierzyć to integracja danych ze wszystkich podsystemów bankowych, prowadząca do zwiększenia możliwości decyzyjnych klienta i umożliwiająca mu podejmowanie decyzji „poparte danymi" przy jednoczesnym zachowaniu bezpieczeństwa i poufności danych. Nie będzie to łatwe zadanie. Dzisiejsze procesy przetwarzania danych w bankach ewaluowały zgodnie z procesami biznesowymi wewnątrz bankowymi. Obecny świat mobilny i „cyfrowość w bankach" będzie wymagała znacznego procesu przebudowy rozwiązań IT. Dodatkowo same procesy biznesowe i decyzyjne będą musiały ulec zmianie: inne modele przychodowe i cenowe adresujące zmiany w zachowaniu się klientów i inna kultura w postrzeganie usług bankowych. Muszą się pojawić również inne modele szacowania ryzyka kredytowego oparte o informacje, jak klienci się zachowują, co ich interesuje oraz kim są, które w połączeniu z analizą Deep Data, będą w stanie sprostać rosnącym oczekiwaniom klientów. Dzisiaj nie wszystkie banki są w stanie sprostać tym wyzwaniom.

Dodatkowo banki będą musiały zaakceptować lub pogodzić się w niektórych relacjach biznesowych, zarówno po stronie klienta, jak i po stronie firm z nimi współpracującymi, z nie zawsze główną rolą w dostarczaniu wartości dodanej. W świecie cyfrowym wiele podmiotów zaczyna odgrywać w zależności od sytuacji biznesowej rolę dostawcy i jednocześnie rolę odbiorcy w połączonych łańcuchach wartości budowanych dla klienta końcowego. Ta rola czasami będzie limitowana w przypadku banku do niewielkiego udziału. Podstawowym pytaniem jest czy banki mentalnie są gotowe na przyjęcie w świecie „digital" takiej podwójnej roli.

Czy banki są gotowe na cyfrową rewolucję?

Według badań PwC, obecne 75% banków ponosi znaczne inwestycje w obszarze zmian modelu biznesowego, dążąc do modelu całkowicie zorientowanego na klienta, ale jednocześnie tylko 17% organizacji uważa w opinii menedżerów, że są już dostatecznie przygotowane.

W szczególności era cyfrowa wymagać będzie:

- rozbudowy zdolności analitycznych (*real-time advanced analytics*), tak by w móc czasie rzeczywistym analizować sygnały o zachowaniach klienta i w sposób oszczędny, tj. unikając zalewania ich bodźcami, proponować im przez właściwy kanał „next best action",
- zmiany sposobu współpracy Działów Marketingu i IT – przejścia na model „agile", tak by umożliwić stałą innowację i częste eksperymentowanie z pomysłami na kampanie,
- efektywnej współpracy między silosami organizacyjnymi, takimi jak kanały dystrybucji, marketing, zakupy, IT,
- budowy kompetencji w zakresie transformacji cyfrowej (częściowo poprzez przejęcie z rynku ekspertów wykształconych przez inne branże, częściowo poprzez kształcenie własnych kadr „w walce" i częściowo poprzez współpracę z firmami doradczymi),
- sponsorowania transformacji cyfrowej przez CEO.

Niezależnie od tego, czy dany bank uważa się za lidera w obszarze „digital", czy też podąża ze swoimi rozwiązaniami za rynkiem elementy sukcesu pozostają te same:

- doskonałość operacyjna,
- przejrzysta wartość dodana dla konsumenta,
- kultura organizacji zorientowana na klienta,
- ciągłe doskonalenie produktów i usług, obecnie razem z klientami.

Era „Digital" wkroczyła w nasze życie i tego procesu nie da się ignorować. Nowy model interakcji z klientami, nie tylko bankowymi, zmienia przestrzeń biznesową wręcz na naszych oczach. Czy i jak ten model zostanie zaakceptowany przez sektor bankowy jest tylko kwestą czasu i jego wyobraźni biznesowej. Oby tylko nie trwało to zbyt długo, bo konkurenci wyręczą banki w zapewnieniu potrzeby bankowania dla klientów mobilnych.

Źródła:

The rise of the digital bank – McKinsey & Company
The digital battle that banks must win – McKinsey & Company
The bank of the future – McKinsey & Company
Retail Banking 2020 – PwC
The Everyday Bank – Accenture
McKinsey iCustomer Europe, 2011
PwC Digital Tipping Point Survey, 2011

.

dr Maciej Majewski

Prezes Zarządu Pentacomp S.A.

Posiada 40 lat doświadczenia zawodowego zdobytego na kilku kontynentach w realizacji i zarządzaniu projektami informatycznymi. Przez wiele lat pracował w firmach doradczych. Wcześniej, pracując za granicą u producentów wysokich technologii IT, współtworzył bezpieczne rozwiązania bazodanowe oraz techniczne zastosowania sztucznej inteligencji. Od lat specjalizuje się w sektorach bankowości, finansów oraz sprzedaży detalicznej.

Obecnie kieruje firmą specjalizującą się w projektowaniu i wdrożeniu złożonych rozwiązań informatycznych oraz bezpiecznych rozwiązań opartych na biometrii i PKI. Jest audytorem wiodącym ISO 27001.

dr Maciej Majewski, Pentacomp

Big Data w walce z atakami cyfrowymi

Skok wart miliard dolarów

New York Times z 14 lutego 2015 roku publikuje obszerny artykuł oparty o raport firmy Kaspersky Lab. Według niego w ostatnim roku grupa cyberprzestępców zrealizowała największy w historii schemat przestępczy skierowany przeciwko bankom. Ponad 100 instytucji finansowych w 30 krajach poniosło straty szacowane na miliard dolarów!

Cyberprzestępcy stosowali skomplikowane metody wirtualnej obserwacji poszczególnych banków. Do systemów komputerowych wprowadzano „konia trojańskiego" – oprogramowanie o nazwie *Carbanak*, pozwalające na śledzenie mechanizmów ich działania. Następnie, wzorując się na procedurach stosowanych przez normalnych pracowników banków, przestępcy transferowali pieniądze z kont, które wytypowali do okradzenia. Każdy akt kradzieży poprzedzała uważna obserwacja wirtualna, trwająca zwykle od 2 do 4 miesięcy. Podkreślam, że zaatakowane banki przez wiele miesięcy nie zidentyfikowały zagrożenia! Według raportu z każdego banku skradziono od 2,5 do ponad 10 mln dolarów. Poszkodowane są instytucje finansowe w Europie Wschodniej, Rosji, USA i w Azji.

Polskie instytucje nie mają zwyczaju publikować danych o atakach, ale autor ma powody aby sądzić, że nad Wisłą i Odrą podobne incydenty również miały miejsce. Jest oczywiste, że banki nie są zainteresowane publikacją informacji o incydentach tego rodzaju. Typowe komunikaty marketingowe starają się raczej utwierdzać klientów w przekonaniu, że wszystkie produkty i kanały dostępu są absolutnie bezpieczne. Przykładem może być ubiegłoroczna dyskusja na temat screen-scrapingu. Przedstawiciele banków używających tego

mechanizmu zapewniali, że przy zachowaniu pewnych reguł jest to w pełni bezpieczny mechanizm wirtualnego zakładania lokat. Jednak z punktu widzenia zarządzania bezpieczeństwem nie może być prawdziwe założenie, że masowy konsument trzyma się procedury. Doświadczenie uczy, że w dużej grupie znajdzie się pokaźna liczba ludzi, którzy postąpią wbrew ustalonym regułom. Dlatego bezpieczeństwo musi być wbudowane w proces i być utrzymane niezależnie od dobrej woli czy samopoczucia użytkowników.

Świadomość i odporność

Rosnąca liczba doniesień medialnych o atakach cyfrowych powoduje, że powoli rośnie poziom świadomości zagrożeń zarówno wśród konsumentów, jak i decydentów instytucji finansowych.

Nie dziwi więc, że 62% prezesów badanych[1] polskich firm postrzega cyberbezpieczeństwo jako główne wyzwanie biznesowe na bieżący rok. I to jest naprawdę dobra wiadomość, jako że świadomość zagrożeń jest powszechnie uważana za główny czynnik zapobiegania i ochrony przed skutkami tychże. Jej wagę potwierdza najnowsza norma ISO 27001:2013, która mówi, że *„najwyższe kierownictwo powinno wykazywać przywództwo i zaangażowanie w odniesieniu do systemu zarządzania bezpieczeństwem informacji"*[2].

Świadomość powinna być siłą sprawczą wypracowania skutecznej strategii obrony przed zagrożeniami. To dzięki niej organizacja zdobywa się na podjęcie inwestycji w narzędzia, wiedzę i niezbędne działania.

Zgodnie z systematyką proponowaną przez firmę Deloitte,[3] skuteczna strategia w obszarze ryzyka cyfrowego to zdobywanie kolejnych stopni dojrzałości od *bezpieczny* poprzez *czujny* aż do *odporny*.

Tradycyjnie zarządzanie bezpieczeństwem koncentruje się na obronie przed znanymi i możliwymi do przewidzenia zagrożeniami. Ważna jest też zgodność z regulacjami i standardami bezpieczeństwa. Pozwala to zameldować zarządowi, że jesteśmy organizacją *bezpieczną*. Niestety, poziom *bezpieczny* to za mało w dzisiejszym, przesyconym technologią informatyczną, świecie, w którym atak może być zainicjowany na przykład przez „inteligentną" klimatyzację. Lawinowo rosnąca liczba rzeczy podłączonych do Internetu oraz

1 Raport badania „CEO Survey 2015" firmy doradczej PWC.

2 Polski Komitet Normalizacyjny „PN-ISO/IEC 27001: 2014-12".

3 Raport „Transforming security" z lutego 2014 firmy doradczej Deloitte.

związane z tym ogromne nasycenie cyfrowe wszystkiego co robimy w pracy, domu i w czasie wolnym powoduje, że źródłem ataku może być najmniej podejrzewany obiekt w naszym otoczeniu, np. pilot, telewizor czy zabawka dziecka[4].

Czujna jest organizacja, która dzięki wysokiemu poziomowi świadomości i nieustannemu monitoringowi potrafi szybko wykryć anomalie i potencjalne zagrożenia. Jeżeli uwzględnić fakt, że 50% ataków odnosi sukces w ciągu minut a pozostałe 50% w ciągu godzin i porównać to ze zdolnością organizacji do jego wykrycia, co z reguły zajmuje dni a nawet miesiące, to widać, że z czujnością nie jest najlepiej. Potwierdziły to wyniki symulacji, w której brały udział polskie urzędy związane z bezpieczeństwem cyfrowym oraz firmy sektora telekomunikacyjnego[5]. Szczególnie niepokoi niezdolność części organizacji biorących udział w ćwiczeniu do przeprowadzenia szybkiej i skutecznej analizy złośliwego oprogramowania. Jeżeli zespół fachowców zmobilizowanych i działających w warunkach „laboratoryjnych" ma problem z bardzo szybkim diagnozowaniem, to jak wygląda to w warunkach „normalnych"? O tym, jak jest źle świadczy średni czas potrzebny na wykrycie zaawansowanego ataku, który wynosi ok. 200 dni[6]. Jakie straty mogą być spowodowane przez szkodliwy software, który działa w ukryciu przez ponad pół roku? To retoryczne pytanie powinno dać impuls do radykalnej zmiany podejścia do kwestii bezpieczeństwa. Pokażemy, jak metody analityczne stosowane w zagadnieniach Big Data mogą być pomocne w osiągnięciu poziomu *czujny*.

Odporność – to najwyższy stopień dojrzałości, którego podstawą jest zdolność do przewidywania i takiego działania w trybie awaryjnym, które zapewnia kontynuację działania nawet w sytuacji złożonego ataku. Osiągnięcie stopnia *odporny* należy traktować jako długofalowy cel. Szybko zmieniające się metody ataków oraz ogromne korzyści, jakie te udane przynoszą przestępcom powodują, że organizacja odporna dzisiaj może stracić odporność w obliczu nowego rodzaju ataku. Dlatego należy przyjąć, że zachowanie najwyższego stopnia *odporności* jest procesem ciągłego doskonalenia i rozwoju metod przewidywania i reakcji na atak. A trwałe utrzymanie *odporności* powinno być wspieranie działaniami z zakresu Big Data.

---

4 Michael R. Porter, James E. Heppelman „How Smart, Connected Products Are Transforming Competition", Harvard Business Review, November 2014.

5 Raport „Cyber-exe Polska 2014", Fundacja Bezpieczna Cyberprzestrzeń, 2015.

6 Raport „Mandiant M-Trends", FireEye, 2013 r.

Nie ma odporności bez szybkiej reakcji

Masowe stosowanie inteligentnych urządzeń powoduje gwałtowny wzrost liczby źródeł potencjalnych zagrożeń. Jednocześnie urządzenia te wytwarzają dane na niewyobrażalną do tej pory skalę co prowadzi prostą drogą do zjawiska Big Data. Dlatego naturalne jest sięgnięcie do metod Big Data w celu uzyskania odporności. Dodatkowym argumentem jest duża dynamika wielu ataków, która może być zaadresowana w kategorii zmienności.

Zjawisko Big Data zostało dostrzeżone już kilkanaście lat temu, gdy w 2001 roku META Group (obecnie Gartner) opublikowała raport[7], który definiuje Big Data jako bardzo duże zbiory danych spełniające kryterium nazwane 3V. Te trzy V to:

- Volume – duża ilość danych,
- Variety – duża różnorodność danych,
- Velocity – duża zmienność 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. Zasilane są one codziennie lub nawet częściej przez bankowe systemy transakcyjne. Hurtownie osiągające wielkość nawet setek terabajtów są na ogół posadowione na relacyjnych bazach danych, które zapewniają spójność oraz bezpieczeństwo oparte o prawa dostępu. Dzięki relacyjnej organizacji danych można z niewielkim opóźnieniem (kilkanaście sekund do kilku minut) udzielić odpowiedzi na standardowe zapytania, np. o możliwość uzyskania kredytu 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 dwóch znaków: PL. Dla zapewnienia blisko 100% 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 za dokładność są sztywne schematy danych. A te są wręcz zaprzeczeniem

---

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

różnorodności. Tymczasem różnorodność danych Big Data nie stoi w sprzeczności z podstawowym mechanizmem korzystania z nich, 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. Pewne dane mogą zostać odrzucone 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.

Na podkreślenie zasługuje fakt, że czas oczekiwania na tradycyjne raporty nie jest czynnikiem krytycznym. Odwrotnie jest w wielu zastosowaniach Big Data, gdy analiza 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"*[8].

Te nowe zjawiska to zarówno poszlaki dotyczące oszustw, jak i sytuacji nadzwyczajnych, jakimi są ataki cyfrowe. A trafione decyzje podjęte szybko pozwalają uniknąć strat lub ograniczyć ich wielkość. W kolejnych rozdziałach rozwiniemy temat nowych metod stosowanych w analizie i diagnozowaniu zagrożeń.

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 ogromne tempo, z jakim powstają, a więc muszą też być zapisywane, nowe dane. Duża zmienność jest też wyzwaniem dla analityków, którzy muszą błyskawicznie przeliczać szybko narastające stosy nowych danych.

---

8 Laney Douglas: The Importance of 'Big Data': A Definition, Gartner, 21.06.2012.

Ekstremalną 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 charakteryzuje się określoną przepustowością, w chwili obecnej sięgającą ponad 580 tys. notowań na sekundę.

Duża zmienność jest również wyzwaniem dla analityków pracujących w zespołach reagowania na ataki cyfrowe. Duża liczba potencjalnych źródeł ataku oraz lawinowo rosnący wolumen danych przesyłanych poprzez Internet komplikują szybkie ich rozpoznanie.

Dlatego obecnie osiągany czas rozpoznania rzędu godzin musi ulec radykalnej redukcji. Nieuprawnione zajęcie wolnych zasobów w czasie ataku typu DDoS (Distributed Denial of Service) powoduje, że każda sekunda braku dostępności kosztuje krocie!

Aby móc stosować metody Big Data, banki potrzebują kompetencji technologicznych odpowiadających nowej generacji narzędzi. Jednak to nie kwestie techniczne stanowią główne wyzwanie. Do osiągnięcia odporności potrzeba ludzi z wyobraźnią i odwagą naukowca stawiającego nietypowe pytania. I szukających odpowiedzi na te pytania w języku rachunku prawdopodobieństwa. Ten nowy gatunek ludzi wspierających odporność firmy na nietypowe ataki nosi nazwę „naukowcy danych" – data scientists[9]. Naukowcy potrzebują laboratorium wyposażonego w przyrządy i tym specyficznym dla Big Data wyposażeniem zajmiemy się poniżej.

Big Data jest synonimem ultra szybkiego przetwarzania

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 podlegały trafność wyszukiwania oraz czas odpowiedzi. Dla drugich do dziś dnia wyzwaniem jest wolumen nowych wpisów przekraczający 100 megabajtów na sekundę. Te nowe wpisy muszą być zapisane a w chwilę później dostępne dla milionów użytkowników na całym świecie.

Nic dziwnego, że firmy musiały stworzyć nowe narzędzia technologiczne, które pomogły im pokonać bariery przetwarzania wynikające z dużej liczby

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

danych połączone z ich zmiennością. Co charakterystyczne, dla firm rozwijających nowe narzędzia ważniejsze od zachowania własności intelektualnej było szybkie pozyskanie jak największej liczby utalentowanych programistów. Dzięki temu wiele narzędzi było tworzone jako software ogólnodostępny w domenie publicznej. Pozostają one również otwarte dzisiaj.

Dobrym przykładem jest **MapReduce** – stworzona przez firmę Google platforma do przetwarzania równoległego bardzo dużych zbiorów danych w klastrach komputerów. Nazwa była zainspirowana funkcjami „map" i „reduce" z programowania funkcyjnego. 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! Podobne zrównoleglenie można co do zasady zastosować również dla przyspieszenia diagnozy ataku cyfrowego.

Część platformy została opatentowana w USA[10], ale istnieje jej otwarta implementacja jaką jest Apache Hadoop[11]. Umożliwia ona tworzenie działających w rozproszeniu aplikacji, które przeprowadzają obliczenia na dużych ilościach danych. Jest jednym z projektów rozwijanych przez fundację Apache. Jeszcze zanim osiągnęła wydanie stabilne, była już wykorzystywana 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 i poddawać analizie wielkie ilości danych. Aby uzyskać nieosiągalną do tej pory szybkość, musiano zrezygnować z relacyjności, w tym z języka SQL, co

---

10 US Patent 7,650,331: „System and method for efficient large-scale data processing"

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

jest pierwszą skuteczną na taką skalę próbą podważenia prawie absolutnego do tej pory paradygmatu.

Komercyjna wersja narzędzi Apache umożliwiających szybkie przetwarzanie oferowana jest poprzez firmę HortonWorks (www.hortonworks.com).

Zwracamy uwagę na ogromną przydatność tych rozwiązań dla tworzenia baz, w których możliwe jest rejestrowanie wszystkich zdarzeń systemowych tradycyjnie przechowywanych w logach systemowych. Dzięki ogromnej szybkości dostępu możliwe jest powiązanie zdarzeń systemowych ze zdarzeniami występującymi w różnorodnych aplikacjach biznesowych. Przykładem może być powiązanie danych aplikacji rejestrującej czas pracy z informacją dotyczącą adresów portali odwiedzanych przez pracownika. Pracownik, który w nietypowych godzinach odwiedza poradniki, które uczą jak zbudować botnet powinien co najmniej wzbudzić zainteresowanie.

Nasze laboratorium prócz narzędzi szybkiego przetwarzania potrzebuje jeszcze narzędzi służących do analizy statystycznej, bardzo wydajnego silnika przetwarzania reguł i przyjaznej wizualizacji wyników.

R jak reguły

Naukowcy danych cenią Nową Zelandię nie tylko za witaminy dostarczane w owocach kiwi.

Drugim ważnym powodem sympatii jest otwarta biblioteka R[12] zawierająca ogromne bogactwo gotowych funkcji stosowanych w analizie danych.

R zostało stworzone w 1993 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 do innych ośrodków akademickich i już w 1995 roku twórcy podjęli decyzję o powszechnym udostępnieniu go na zasadach Fundacji Wolnego Oprogramowania: GNU General Public Licence.

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

Wokół R szybko powstało grono entuzjastów statystyków i programistów, którzy pochodzili z różnych ośrodków na świecie. Warto podkreślić, że niezależny pomiar popularności pokazał, że R jest dwukrotnie częściej cytowana

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

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 R jest źródłem niebywałego sukcesu w zastosowaniu metod analizy statystycznej do problemów biznesowych takich jak bezpośredni marketing, badanie nastrojów klientów i konsumentów oraz w zarządzaniu ryzykiem.

Z naszego punktu widzenia szczególnie interesująca jest możliwość tworzenia niesłychanie szybko działających drzew decyzyjnych[13]. Drzewa takie są podstawą reguł pozwalających diagnozować poszlaki dotyczące podejrzanego zachowania pracowników i systemów oraz diagnozować ataki cyfrowe. R zawiera również bardzo potężny pakiet funkcji wizualizacyjnych, dzięki którym analitycy przedstawiają uzyskane wyniki w łatwy do interpretacji a więc przekonywujący sposób.

Komercyjna wersja R, która zawiera szereg interfejsów umożliwiających łatwą integrację z innymi elementami wyposażenia laboratorium dostępna jest poprzez www.revolutionanalytics.com.

Dobrze wyposażone laboratorium pomoże skutecznie dobrać się do wiedzy tkwiącej w danych. Właściwą metodą ich stosowania jest analizy predykcyjna[14].

Analiza predykcyjna

Wszystkie zastosowania analizy predykcyjnej zaczynają się od sformułowania nośnego pytania, na które aplikacja ma udzielić odpowiedzi. Zacznijmy od relatywnie prostego przykładu związanego z ryzykiem kredytowym.

Pytanie: co skłania kredytobiorcę kredytu hipotecznego do przedterminowej spłaty całości (refinansowania)? 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.

---

13 Revolution Analytics White Paper, „Big Data Decision Trees with R", 2012

14 Eric Siegel: Predictive Analytics, John Wiley & Sons, 2013

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. uchylenie się od spłaty, oszustwo, zemsta na pracodawcy czy współpraca z cyfrowym przestępcą.

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 polegającego na przedterminowej spłacie jest wysokość oprocentowania kredytu. Jeżeli jest ona niższa niż 7,94% (wartość przykładowa) to ryzyko jest równe 3,8%, a przeciwnym przypadku to 19,2%. Jak widać, odkrycie tylko jednego kryterium otwiera drogę do pięciokrotnego(!) zmniejszenia prawdopodobieństwa wystąpienia tego 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% prawdopodobieństwem przedterminowej spłaty. To jest co trzeci kredyt!

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 modelem można podzielić pomiędzy niewielkie 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.

Gdy naukowcy przedstawią fakty, kolej na decyzje menedżerów. To oni muszą podjąć działanie w oparciu o pozyskaną wiedzę. Czy są gotowi zrezygnować z marży przez obniżenie oprocentowania poniżej 7,94% mając na uwadze możliwość całkowitej utraty przyszłych odsetek? Gdzie leży próg ich

apetytu na ryzyko? Odpowiedzi na te pytania nie da się zautomatyzować – to ciągle domena ludzi[15].

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 intuicja oparta na doświadczeniu nie jest dobrym doradcą. Poniżej przytaczam kilka wybranych przypadków zastosowania z dziedziny bezpieczeństwa.

Odporność dzięki działaniom opartym na przewidywaniu

Zacznijmy od przykładu, w którym analizowane jest fizyczne bezpieczeństwo placówek bankowych. Analiza wielu tysięcy zdarzeń wykazała, 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. Warto podkreślić, że wynik analizy przeczy obiegowej „mądrości".

Wniosek do działania jest oczywisty i dotyczy wzmożenia fizycznej ochrony placówek sąsiadujących z miejscem popełnienia udanego napadu oraz częstszych patroli policji.

Następny bardziej złożony przykład związany jest z przygotowaniem na ataki typu APT (Advanced Persistent Threat), w których instytucja atakowana jest w sposób zdecydowany i zarządzany przez nieznaną centralę przestępczą. Analiza dowodzi, że ataki takie bardzo często wspomagane są przez osoby pracujące wewnątrz organizacji. Osoby te są albo delegowane przez przestępców albo rekrutowane spośród pracowników podatnych na współpracę.

Nie należy się spodziewać, że kolaboranci sami zgłoszą się do działu bezpieczeństwa. To w praktyce oznacza, że każdy pracownik może być podejrzany. Nie chodzi też o to, by w instytucji tworzyć psychozę zagrożenia i podejrzeń. Aby ograniczyć listę podejrzanych, należy dyskretnie łączyć ze sobą wszelkie informacje o sytuacjach i zachowaniu pracowników, sprzyjające współpracy z przestępcami, z informacjami pochodzącymi z zapisów zdarzeń systemów i aplikacji. W ten sposób tworzymy reguły pozwalające na identyfikację zachować oraz zdarzeń, które można zakwalifikować jako poszlaki. Przykładem

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

sytuacji może być pominięcie w awansie, brak podwyżki, nagana, sygnalizowana chęć zmiany pracodawcy. Typowe zdarzenia to logowanie o nietypowych porach, dostęp z zewnątrz do chronionych aktywów IT, częste tworzenie i usuwanie kont w ramach grup uprawnień.

Mogą to więc być sytuacje i zdarzenia takie jak: pracownik w okresie wypowiedzenia ściąga duże pliki na swoje urządzenie mobilne lub podczas urlopu kopiuje pliki zawierające dane klienta. Niektóre sytuacje mogą być prawdziwym zaskoczeniem. Okazuje się, że zmiana stanu cywilnego też zwiększa podatność na współpracę z przestępcami.

Innowacyjność zaprezentowanego podejścia polega na powiązaniu wiedzy zdobytej z analizy danych personalnych, danych z systemów rejestracji czasu pracy, kontroli dostępu do aplikacji i typowych danych o zdarzeniach systemowych uzyskiwanych z logów systemu operacyjnego, baz danych i aplikacji internetowych. Różnorodność formatów, bardzo duża liczba rekordów oraz tempo z jakim nowe sytuacje i zdarzenia muszą być filtrowane przez zestaw reguł wymagają przetwarzania typowego dla Big Data.

Powyższe przykłady można uzupełnić długą listą zastosowań analizy predykcyjnej w zwalczaniu oszustw kredytowych, kartowych, ubezpieczeń majątkowych i zdrowotnych. Zagadnienia te są tak wartościowe dla biznesu, że koszty utrzymania laboratorium będą wielokrotnie spłacone dzięki podjętym działaniom.

Adaptacja organizacji do Big Data

W oparciu o doświadczenia liderów możemy sformułować trzy tezy ważne dla instytucji chcących wykorzystać zjawisko Big Data dla uzyskania wyższego stopnia bezpieczeństwa.

Po pierwsze, wykorzystanie Big Data jest typowym projektem badawczo-rozwojowym a nie projektem informatycznym. Głównym wyzwaniem dla organizacji jest stworzenie odpowiednich warunków działania dla naukowców danych zatrudnionych w laboratorium.

Idealnym miejscem dla laboratorium jest SOC – Security Operations Center. W organizacji SOC naukowcy danych stanowiliby jeden z zespołów analitycznych obsługujących SIEM czyli Security Information and Event Management. Naukowcy stawiając pytania i poszukując odpowiedzi pracują w trybie zasadniczo różnym od monitoringu, do jakiego przywykły zespoły zajmujące się bezpieczeństwem. Obok pokoju sytuacyjnego, w którym czeka się na alarmy,

pojawia się laboratorium. Zespół analityczny przekazywałby spostrzeżenia i wyniki analiz do zespołów reagowania.

Niestety, większość polskich instytucji ciągle jest na etapie dyskutowania celowości poniesienia wydatków na SOC z prawdziwego zdarzenia.

Po drugie, bardzo trudno jest o wiedzę i kwalifikacje związane z nowym zjawiskiem, jakim jest Big Data. Aby móc prognozować i wyprzedzać rozwój wypadków potrzebni są naukowcy danych, których brak jest na rynku pracy.

Po trzecie, potrzeba decydentów, którzy w oparciu o zaprezentowane wyniki analizy podejmą odpowiednie decyzje, nawet jeżeli są one sprzeczne z intuicją.

Wnioski dla banków

Stosowanie technik analitycznych i narzędzi z dziedziny Big Data nie jest wyraźnie rekomendowane w Rekomendacji D Komisji Nadzoru Finansowego[16]. Rekomendacja mówi jedynie o obowiązku stosowania automatycznych zabezpieczeń, które w zaproponowanej powyżej skali odpowiadają najniższemu stopniowi – *bezpieczny*. Wprawdzie mówi ona również o tym, by zapewnić „odpowiednią ochronę środowiska teleinformatycznego", ale nie mówi jak interpretować słowo „odpowiednią".

Szansą jest odnotowane[17] większe zainteresowanie tematyką bezpieczeństwa ze strony zarządów, które ponoszą przecież odpowiedzialność przed akcjonariuszami. Zachętą powinny być coraz liczniejsze doniesienia o kolejnych rekordowych stratach banków ponoszonych w wyniku ataków cyfrowych. Rachunek zysków i strat powinien być również przekonywujący dla akcjonariuszy, którzy w końcu przestaną akceptować wzrastające koszty braku odpowiednich zabezpieczeń.

Jeżeli znajdą się interesujące pytania dotyczące bezpieczeństwa, to znajdą się sposoby i środki na poprowadzenie innowacyjnych inicjatyw i projektów analitycznych. Jak już wspomniałem wcześniej, banki posiadają znaczne zasoby danych na temat zdarzeń, zachowań i transakcji. Dane te z pewnością mogą być wykorzystane do analizy predykcyjnej, która pozwoli zwiększyć odporność na zagrożenia.

---

16 Komisja Nadzoru Finansowego, „Rekomendacja D: dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach", Warszawa, styczeń 2013.

17 Raport badania „CEO Survey 2015" firmy doradczej PWC.

Historia dowodzi, że z innowacją nie warto czekać. Jeden dobrze umocowany pracownik Nick Leeson był w stanie doprowadzić do upadku najstarszy brytyjski bank inwestycyjny. Przy okazji bankructwa Banku Baringsa wysokie straty poniosła również rodzina królewska. Można sobie wyobrazić jakie szkody jest w stanie spowodować celny atak przeprowadzony drogą elektroniczną.

A historia lubi się powtarzać, choć na ogół w zmodyfikowanej postaci.

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.

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 kilkuset 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". Autor publikacji „Aspekty prawne cloud computingu w odniesieniu do sektora bankowego (regulacje EU)" (2014). Współautor analizy wykonalności wdrożenia *cloud computingu* w administracji publicznej w Polsce (2014). Jest także wykładowcą studiów podyplomowych Szkoły Głównej Handlowej „Zastosowanie technologii cloud computingu w modelowaniu biznesowym".

Robert Gajda

Odpowiedzialny za sprzedaż i rozwój rynku w obszarze zaawansowanych technologii w sektorze dużych przedsiębiorstw, rynku finansowego i sektora publicznego w polskim oddziale Microsoft. Posiada ponad 20 letnie doświadczenie w branży IT. Absolwent Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie oraz Wyższej Szkoły Zarządzania i Prawa w Warszawie. Posiada tytuł MBA University of Illinois.

Andrzej Gibas, Maciej Gawroński, Robert Gajda

Czas na chmurę w sektorze finansowym w Polsce!

Od co najmniej pięciu lat temat przetwarzania w chmurze (z ang. cloud computing) jest tematem stale dyskutowanym w środowisku związanym z informatyką w sektorze finansowym w Polsce. Ta wieloletnia dyskusja przyczyniła się do pogłębienia wiedzy na ten temat. Koncepcja dostarczania usług informatycznych w trybie przetwarzania w chmurze oraz liczne korzyści wypływające z implementacji takich rozwiązań są dzisiaj powszechnie zrozumiałe nie tylko wśród informatyków, ale także wśród menedżerów biznesowych, zarządzających ryzykiem, bezpieczeństwem czy wreszcie finansami w bankach i innych instytucjach sektora finansowego.

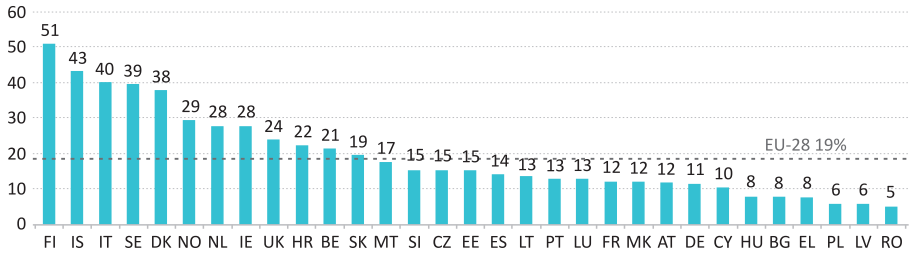
Awersja do ryzyka i wynikające z niej opóźnienia

Pomimo znacznego wzrostu świadomości oraz gwałtownego rozwoju technologii chmurowych we wspomnianym okresie, sektor finansowy w Polsce wciąż z wielką ostrożnością podchodzi do rzeczywistej implementacji modelu chmurowego. Z jednej strony jest to zrozumiałe, gdyż akceptacja chmury w pierwszej kolejności następuje wśród konsumentów, następnie wśród małych i średnich firm, a dopiero na końcu wśród największych przedsiębiorstw. Z drugiej jednak strony sektor finansowy w Polsce prezentuje pewne opóźnienie w tym obszarze zarówno w porównaniu do innych branż w Polsce, jak i do podobnych organizacji w Europie czy Ameryce Północnej.

Wydaje się, że przyczyn należy szukać w dwóch źródłach. Pierwsze to generalnie niższa akceptacja koncepcji przetwarzania w chmurze przez polskie przedsiębiorstwa na tle innych krajów. Przykładowo, wg. Eurostat jedynie 6% polskich przedsiębiorstw korzystało w 2014 r. z takiego modelu, co na tle

średniej europejskiej – 18% – plasuje Polskę na końcu całej stawki z wielkimi zaległościami do lidera, Finlandii, gdzie chmura jest używana przez ponad połowę przedsiębiorstw.

Rys. 1.
Korzystanie z usług cloud computingu w 2014 roku (jako % przedsiębiorstw)



Źródło: *Eurostat (isoc_cicce_use)*

Być może przyczyną wstrzemięźliwości polskich przedsiębiorstw we wdrażaniu rozwiązań chmurowych jest paradoksalnie dobra, zwłaszcza na tle innych krajów, sytuacja polskiej gospodarki. Być może nieźle radzące sobie polskie przedsiębiorstwa wciąż nie odczuwają potrzeby wdrożenia nowych, innowacyjnych i oszczędnych rozwiązań, które jednak w pierwszym okresie wymagają wysiłku wdrożenia, reorganizacji procesów czy wręcz zmianę korporacyjnej kultury.

W przypadku instytucji sektora finansowego na ogólną wstrzemięźliwość polskich przedsiębiorstw nakłada się dodatkowa trudność – chętnie wspominana przez przedstawicieli tej branży – związana z obowiązkiem zgodności z wymagającymi regulacjami tego rynku.

Idą trudne czasy – czas na zmiany

Bez wątpienia sektor finansowy jest poddany bardziej rygorystycznym wymogom regulacji niż inne branże w Polsce. Wydaje się jednak, że w przypadku niektórych instytucji z tego sektora wymóg zgodności z obowiązującymi przepisami był dotychczas wykorzystywany jako swoiste usprawiedliwienie braku podejmowania wysiłku w przygotowaniu wdrożenia rozwiązań chmurowych. W wielu miejscach można usłyszeć takie argumenty, jak: „popatrzymy jak się

uda innym", „nie chcemy być pionierami", „nie dostaniemy zgody od działu bezpieczeństwa" itp.

Rok 2015 i lata kolejne będą trudnym okresem dla sektora bankowego w Polsce. Banki między innymi będą musiały zmierzyć się z następującymi wyzwaniami:

- drastyczne podwyższenie składki na Bankowy Fundusz Gwarancyjny – konsekwencja upadku SKOK-ów,
- spadająca marża odsetkowa,
- kryzys „frankowy" – powszechne oczekiwanie zarówno ze strony konsumentów, jak i sporej grupy polityków, aby banki finansowo partycypowały w kwestii rozwiązania problemu spłaty kredytów hipotecznych udzielonych we frankach szwajcarskich z dużym prawdopodobieństwem odbije się negatywnie na wyniku sektora,
- stała presja na koszty, związana ze strategią poprawy wskaźnika C/I także w kontekście przygotowania się banków do kolejnej fali konsolidacji rynku,
- wzrost wewnętrznej konkurencyjności na rynku bankowym w Polsce, w tym związana z kurczeniem się rezerw prostych; znaczny wzrost „ubankowienia" polskiego społeczeństwa; dalsze pozyskiwanie klientów jest związane z ich przejęciem od konkurentów,
- pojawienie się konkurencji w postaci ofert usług finansowych z instytucji z innych branż,
- wzrost wymagań ze strony klientów, w tym związanych ze zmianami kultury i metod komunikacji w konsekwencji powszechności użycia technologii internetowych.

Wydaje się, że czas „strategii na przeczekanie" mija – dotychczasowe metody poszukiwania oszczędności związane np. z optymalizacją, konsolidacją i wirtualizacją zasobów informatycznych nie przyniosą dalszych znaczących efektów. Wydaje się także, że nadchodzi czas na bardziej zdecydowane ruchy i wdrożenia kolejnych innowacyjnych rozwiązań. Przetwarzanie w chmurze może być właśnie takim znaczącym krokiem, umożliwiającym dalsze znaczne redukcje kosztów przy jednoczesnej poprawie efektywności procesów biznesowych instytucji finansowej, poprawie wydajności zatrudnianych pracowników, poprawie oferowanego doświadczenia klienta oraz poprawie wskaźników finansowych banków, w tym C/I i ROE.

Oczekiwane korzyści wynikające z implementacji rozwiązań chmurowych, zwłaszcza w kontekście wyzwań rynkowych, przyczynią się do podjęcia trudu

wdrożeń spełniających wszystkie wymogi obowiązujących przepisów. Nagrodą za ten trud będzie umocnienie pozycji rynkowej instytucji i zbudowanie przewag konkurencyjnych na nadchodzące lata w stosunku do tych instytucji finansowych, które tego trudu nie podejmą.

Główne wyzwania regulacyjne

Mając na uwadze możliwość wykorzystania usług opartych o przetwarzanie w chmurze mierzymy się z reguły z następującymi wyzwaniami:

- ochrona prywatności, w tym ochrona danych osobowych,
- przetwarzanie danych za granicą,
- zasady leżące u podstaw umowy na usługi w chmurze,
- rola dostawcy i podwykonawcy usług w chmurze,
- bezpieczeństwo – w tym zabezpieczenie ciągłości działania, zgodność z międzynarodowymi standardami, itp.

W przypadku sektora finansowego w Polsce zagadnienia związane z wykorzystaniem usług przetwarzania w chmurze regulowane są między innymi przez następujące dokumenty:

- przepisy Unii Europejskiej,
- prawo bankowe, ustawa z dnia 29 sierpnia 1997 r. (tekst jednolity Dz. U. z 2012 r. Nr 0, poz. 1376),
  - w tym przepisy dot. outsourcingu czynności bankowych,
- rekomendacja D KNF.

Ochrona prywatności stanowi jeden z głównych aspektów do dyskusji, pojawiający się w momencie rozważania wykorzystania przetwarzania w chmurze. Zagadnienie to zostało opisane Dyrektywą UE o ochronie danych (95/46/WE), która określa ścisłe wymagania dotyczące obsługi danych osobowych w Unii Europejskiej. Zgodnie z prawem europejskim usługobiorca jest kontrolerem danych klientów, a usługodawca pełni funkcję organizacji przetwarzającej dane. Aby umożliwić ciągły przepływ informacji niezbędny do prowadzenia międzynarodowej działalności gospodarczej (w tym transfer danych osobowych przez granice), firmy działają zgodnie z zasadami bezpiecznego transferu danych (z ang. Safe Harbor Framework) między USA i UE na podstawie porozumienia Komisji Europejskiej z Departamentem Handlu USA. Certyfikat Safe Harbor umożliwia zgodne z prawem przesyłanie danych

osobowych z Unii Europejskiej poza obszar Unii Europejskiej do ośrodków przetwarzania danych usługodawcy w celu ich przetwarzania.

Aspekt ochrony i przekazywania danych osobowych do podmiotów przetwarzających dane, które mają siedzibę w państwach trzecich, decyzją Komisji Europejskiej z dnia 5 lutego 2010 r. został określony na podstawie tzw. standardowych klauzul umownych na mocy Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady[1].

Powyższe opisuje stan prawny rozważanego zagadnienia w kontekście przepisów europejskich. Czy przepisy obowiązujące w Polsce narzucają jakieś szczególne, dodatkowe ograniczenia w zakresie przetwarzania danych osobowych w chmurze? Obecnie nie ma takich ograniczeń, które stanowiłyby istotny problem dla korzystania z cloud computingu. Ścieżki w tym obszarze zostały już przetarte w Unii Europejskiej i w Polsce. Pewien kłopot organizacyjny sprawiać może wymaganie złożenia podpisu na papierowej umowie o powierzeniu przetwarzania danych osobowych. Jednak w relacjach B2B trudność taką można zaakceptować i jej sprostać. Niesprostanie temu wymogowi też nie będzie rodzić bezpośrednich negatywnych konsekwencji, o ile umowa o powierzenie przetwarzania danych zostanie zawarta w jakikolwiek sposób, bo pozostanie ona ważna. Wreszcie liczymy, że w końcu w roku 2015 wejdą w życie w Polsce przepisy o formie dokumentowej, wymagającej jedynie utrwalenia oświadczenia woli i że wymóg formy pisemnej względem umowy o powierzenie przetwarzania danych zostanie zastąpiony wymogiem formy dokumentowej.

Również w zakresie eksportu danych poza Europejski Obszar Gospodarczy nastąpiły w Polsce zmiany eliminujące wcześniejsze bariery. Do niedawna eksport danych do państw, które nie zapewniają adekwatnej ochrony wymagał w każdym przypadku zgody wydanej przez GIODO. Obecnie, od 1 stycznia 2015 roku zgoda taka nie jest wymagana przy zawarciu przez strony standardowych klauzul umownych, o których mowa powyżej. W innych przypadkach, np. przy zawarciu wiążących reguł korporacyjnych (ang. binding corporate rules) zgoda GIODO na eksport danych nadal jest wymagana.

To, co wyróżnia Polskę na tle innych krajów Unii Europejskiej to regulacje dotyczące outsourcingu istotnych czynności bankowych. Polskie Prawo Bankowe zakazuje ograniczania odpowiedzialności outsourcerów. Podobny zakaz spotykamy w przepisach ustawy o funduszach inwestycyjnych i o obrocie

---

1 (http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF).

instrumentami finansowymi (w obu tych ustawach zakaz nie dotyczy outsourcingu nieistotnego). Zakaz ograniczenia odpowiedzialności dostawcy nie pojawia się w żadnej zachodnioeuropejskiej regulacji. Przepisy unijne nie zezwalają instytucjom finansowym na powołanie się na outsourcing dla zwolnienia się z odpowiedzialności. Polski ustawodawca rozszerzył ten wymóg na dostawców sektora. Wydaje się, że przeniesienie odpowiedzialności na dostawcę usług jest ogranicznikiem rozwoju rynku. Zakaz ograniczenia odpowiedzialności outsourcera (dostawcy chmury w naszym przypadku) stoi na przeszkodzie pełnego wykorzystania usług cloud computingu przez polski sektor bankowy. Globalna kultura prawna usług informatycznych opiera się na założeniu ograniczonej odpowiedzialności. Takie podejście wydaje się szczególnie uzasadnione w przypadku usług chmurowych. Globalni dostawcy, co do zasady nie akceptują nieograniczonej odpowiedzialności. Jednocześnie uwzględniając ich pozycję rynkową oraz możliwość utraty reputacji podejmują wszelkie możliwe działania ograniczające do minimum ryzyka związane z wykorzystaniem usług w modelu chmurowym.

Zamiast zakładać pełną odpowiedzialność dostawcy chmury, tworzącą iluzoryczne poczucie bezpieczeństwa po stronie banku, należałoby raczej skupić się na zapewnieniu bezpieczeństwa operacyjnego dla procesu powierzonego dostawcy chmury i przewidzeniu planu alternatywnego na wypadek utraty ciągłości działania dostawcy. Na nic bankowi odszkodowanie a tym bardziej doprowadzenie do upadłości swojego dostawcy. Nie zrekompensuje to a wręcz dodatkowo nadszarpnie reputację banku, która jest jego głównym kapitałem.

Wraz z uregulowaniem kwestii outsourcingu w Prawie bankowym w Polsce w 2004 r. pojawiły się wątpliwości co do dopuszczalności podoutsourcingu. Doprowadziło to do tworzenia skomplikowanych struktur tzw. outsourcingu gwiaździstego. Co gorsza, w związku z zakazem ograniczeń odpowiedzialności outsourcerów, drastycznie utrudniło i przedłużyło to proces zawierania tych umów. Po nowelizacji Prawa Bankowego w 2011 r. podoutsourcing został uregulowany ustawowo. Nie może on obejmować całości świadczeń objętych umową a dodatkowo powinien być przewidziany w umowie outsourcingowej. Bank powinien wyrazić na piśmie zgodę na konkretne podzlecenie, bądź może ono nastąpić incydentalnie dla odwrócenie skutków katastrofy lub innego przypadku siły wyższej. Inne ustawy sektorowe nie regulują podoutsourcingu wprost. Z chwilą, gdy w Prawie bankowym uregulowano podoutsourcing, prawnicy z sąsiednich subsektorów dostrzegli u siebie lukę i zaczęło dominować przekonanie o tym, że w tych podsektorach podoutsourcing nie jest

dozwolony. Rodzi to spore problemy interpretacyjne i analityczne przy „wtłaczaniu" poszczególnych usług cloudowych w ramy przepisów. Czasami się to udaje, a czasami nie.

PRZYKŁADY WYMOGÓW DOTYCZĄCYCH PRZETWARZANIA W CHMURZE W SEKTORZE FINANSOWYM W POLSCE		
Obowiązek	**Podstawa prawna**	**Trudności w realizacji / możliwe rozwiązania**
Umowa powierzenia przetwarzania danych musi być podpisana	Ustawa o ochronie danych osobowych	Trzeba uzyskać podpis dostawcy chmury.
Zakaz ograniczeń odpowiedzialności outsourcera	Ustawa Prawo bankowe	Ogranicza możliwość korzystania z największych chmur obliczeniowych; tworzy preferencję dla lokalnych rozwiązań o większym ryzyku operacyjnym; rodzi ryzyko „zakażenia" w przypadku sporu między jednym klientem chmury a dostawcą – upadłość dostawcy pozbawi usług wszystkich klientów („too small to fail"). Zaadresowanie tego wyzwania regulacyjnego nie jest proste. Wymagałoby, aby dostawca chmury nie miał dostępu do danych klienckich przetwarzanych w chmurze przez bank a równocześnie, żeby bank posiadał awaryjne rozwiązanie niezależne od dostawcy chmury na wypadek problemów z jego ciągłością działania. W naszej ocenie potrzebna jest ingerencja ustawodawcy i deregulacja – usunięcie zakazu ograniczeń odpowiedzialności, który jest nadregulacją względem wymogów UE. W obecnym stanie prawnym rozwiązaniem mogłaby być pseudonimizacja lub szyfrowanie danych umieszczanych w chmurze kluczami posiadanymi tylko przez bank – klienta chmury.
Podoutsourcing bankowy	Ustawa Prawo bankowe	Prawo bankowe zezwala jedynie na tzw. podoutsourcing pomocniczy i podoutsourcing awaryjny. Nie można natomiast podzlecić wykonania części głównego świadczenia. Rodzi to wątpliwości w przypadku, gdy elementem usługi miałaby być współpraca kilku centrów danych. Rozwiązaniem tego problemu, trafnym w naszej ocenie, byłoby przyjęcie, że skoro jedno CPD jest w stanie zapewnić usługę, to drugie CPD pełni rolę podoutsourcera, zwiększającego tylko pewność usługi.

Obowiązek	Podstawa prawna	Trudności w realizacji / możliwe rozwiązania
Zakaz ograniczenia odpowiedzialności outsourcera istotnego	Ustawa o funduszach inwestycyjnych	Jeśli fundusz całość swojego istotnego procesu chciałby w pełni oprzeć na zewnętrznej chmurze, umowa nie mogłaby ograniczać odpowiedzialności dostawcy tej chmury. Jednak jeśli fundusz posiadałby rozwiązanie awaryjne niezależne od dostawcy chmury podstawowej, można byłoby rozważać, że nie zachodzi tzw. outsourcing istotny.
Brak regulacji podoutsourcingu	Ustawa o działalności ubezpieczeniowej; Ustawa o funduszach inwestycyjnych; Ustawa o organizacji i funkcjonowaniu funduszy emerytalnych	Z interpretacji przepisów wysnuwa się wniosek, że instytucja finansowa musi zawrzeć umowy bezpośrednio z podwykonawcami bezpośredniego outsourcera. Rodzi to poważne problemy organizacyjne dla modelu cloud computingu. Możliwe rozwiązania: (i) obstawać przy „starej" wykładni, że brak regulacji nie oznacza zakazu; (ii) tworzyć skomplikowane struktury umowne tzw. „outsourcingu gwiaździstego" – czyli podpisywać umowy ze wszystkimi uczestnikami łańcucha dostawy (niekiedy podejście to może być uzasadnione względami bezpieczeństwa operacyjnego, szczególnie przy usługach SaaS); (iii) dokonać szczegółowej analizy konkretnej usługi w celu oceny, w jakich rolach uczestniczą w niej poszczególne podmioty, czy jest to rola podwykonawcy, wsparcia technicznego niebędącego podwykonawstwem czy potencjalnego wsparcia ("podwykonawca uśpiony").

WYBRANE ZAGADNIENIA ZWIĄZANE Z PRZETWARZANIEM W CHMURZE I ICH REGULACJA W POLSCE W ROZBICIU NA POSZCZEGÓLNE SUBSEKTORY

	Outsourcing	Podoutsourcing	Tajemnica sektorowa	Ograniczenie odpowiedzialności
Banki	Uregulowany	Uregulowany, dozwolone są: podoutsourcing pomocniczy i podoutsourcing awaryjny	Zobowiązanie do zachowania tajemnicy (art. 104 ust. 2 pkt. 2a)	Zakaz ograniczenia odpowiedzialności outsourcera (art. 6b)

	Outsourcing	Podoutsourcing	Tajemnica sektorowa	Ograniczenie odpowiedzialności
Ubezpieczyciel	Uregulowany	Nieuregulowany	Zobowiązanie do zachowania tajemnicy (art.19 ust.1)	Brak możliwości wyłączenia odpowiedzialności zakładu ubezpieczeń wynikającej z powierzenia przetwarzania danych, ale istnieje możliwość ograniczenia odpowiedzialności przetwarzającego (art. 19 ust. 3).
Fundusze inwestycyjne	Uregulowany	Nieuregulowany	Zobowiązanie do zachowania tajemnicy	Brak zakazu wyłączenia odpowiedzialności. Nie dotyczy outsourcingu nieistotnego.
Fundusze emerytalne	Uregulowany	Nieuregulowany	Zobowiązanie do zachowania tajemnicy	Brak zakazu wyłączenia odpowiedzialności.

Co na to dostawcy Cloud Computing?

Aby skutecznie oferować usługi w modelu chmurowym trzeba dysponować nie tylko odpowiednimi kompetencjami, produktami, infrastrukturą, ale przede wszystkim skalą, czyli potencjałem organizacyjnym i finansowym. Takim dysponują firmy działające w skali globalnej, które, ze względu na atrakcyjność potencjalnego rynku, w pierwszej kolejności starają sprostać wytycznym Komisji Europejskiej. Przykładem jest chociażby firma Microsoft. Inspektorzy ochrony danych osobowych z 28 krajów UE – tzw. Grupa Robocza Art. 29 (w tym polski Generalny Inspektor Ochrony Danych Osobowych), którzy kontrolują firmy prowadzące działalność biznesową na terenie Unii Europejskiej opublikowali **wspólne stanowisko**, wyrażając swoje poparcie dla prawidłowych rozwiązań kontraktowych firmy Microsoft w zakresie usług chmurowych dla biznesu.

W skrócie, w tym konkretnym przypadku dla usługobiorców, oznacza to aprobatę unijnego regulatora dla podejścia Microsoftu do ochrony prywatności i bezpieczeństwa danych obywateli europejskich oraz zapewnienie, że jakiekolwiek zmiany w innych standardach ochrony (takich jak umowa Safe

Harbor pomiędzy UE i USA odnośnie przypływu danych) nie wpłyną na możliwość używania biznesowych usług chmurowych Microsoftu. Po drugie, jest to uznanie dla w/w zobowiązań kontraktowych dotyczących transferów danych na całym świecie (podczas gdy umowa Safe Harbor dotyczy specyficznie tylko transferów danych między Europą a USA). Dodatkowo niektórzy usługodawcy oferują możliwość wyboru regionu geograficznego, na którym będą przetwarzane dane dla poszczególnych usług chcąc zawęzić go np. do Unii Europejskiej.

Firmy zajmujące się dostarczaniem usług opartych na przetwarzaniu w chmurze dążą do zachowania przejrzystości swoich działań w zakresie prywatności, udostępniania klientom możliwości wyboru opcji związanych z ochroną prywatności oraz odpowiedzialnego zarządzania przechowywanymi danymi. Jako gwarancję tych działań przyjmuje się odpowiednie procedury oraz politykę bezpieczeństwa wdrożone po stronie usługodawcy potwierdzone niezależnymi certyfikatami (np. zgodności z normą 27001/27002: 2013, która jest powszechnie stosowaną międzynarodową normą dotyczącą zarządzania bezpieczeństwem informacji, ISO/IEC 27018 w aspekcie ochrony danych PII czy atest Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) opisujący podstawowe zasady zabezpieczeń, którymi powinni kierować się dostawcy) oraz procedurami audytorskimi zgodnymi ze światowymi standardami (np. SOC 1 typu 2 i SOC 2 typu 2 w obszarze audytu).

Kierując się najlepszymi praktykami oraz standardami rynkowymi związanymi z zarządzaniem bezpieczeństwem informacji usługodawcy zwracają szczególną uwagę na następujące mechanizmy zabezpieczeń:

- fizyczne systemy sprzętowe monitorowane przez 24 godziny na dobę,
- zasady bezpieczeństwa dotyczące tożsamości federacyjnych i logowania jednokrotnego po stronie klienta, uwierzytelniania dwuskładnikowego oraz izolacje danych klientów,
- zautomatyzowana obsługa,
- szyfrowanie danych i bezpieczeństwo infrastruktury logicznej,
- ochrona przed złośliwym oprogramowaniem.

Starając się w sposób jak najbardziej efektywny doskonalić mechanizmy zabezpieczeń chroniące przed nieuprawnionym dostępem do informacji, usługodawcy niejednokrotnie stosują mechanizmy pozwalające symulować rzeczywiste ataki, stale monitorować zabezpieczenia oraz ćwiczyć reagowanie na incydenty związane z zabezpieczeniami.

Jak już wcześniej wspomniano, w realiach rynku polskiego dostawcom usług chmurowych najtrudniej jest sprostać wymogom regulacyjnym dotyczącym outsourcingu. Niektóre metody radzenia sobie z tym wyzwaniem to:

- powołanie dedykowanej spółki do świadczenia usług outsourcingowych – w takim przypadku ograniczeniem odpowiedzialności jest de facto kapitał zakładowy spółki,
- odsprzedaż usług chmurowych poprzez lokalnego partnera i przejęcie odpowiedzialności przez tego partnera,
- wyniesienie do chmury tych procesów, które nie są kluczowymi czynnościami bankowymi – i wówczas reguła nieograniczonej odpowiedzialności nie ma zastosowania,
- wykorzystanie możliwości technologii chmurowych i budowanie tzw. chmur prywatnych – i wówczas kwestia outsourcingu w ogóle się nie pojawia.

Co w Polsce już udało się wdrożyć?

Mimo wspomnianych ograniczeń w polskim sektorze finansowym, obserwujemy pierwsze wdrożenia rozwiązań chmurowych. Wszędzie tam, gdzie istnieje odpowiednia skala, rozwiązania takie dają wymierne korzyści. Zwykle instytucje finansowe sięgają po chmurę prywatną – w jej przypadku nie istnieje problem wyśrubowanych polskich regulacji w zakresie outsourcingu, więc takie projekty relatywnie łatwo jest uruchomić od strony formalnej. Często uzasadnieniem do budowania chmury prywatnej jest efekt synergii, polegający na utworzeniu centrum usług wspólnych dostarczającego te usługi do grupy kapitałowej.

Przykładem takiego podejścia do chmury prywatnej jest wdrożenie w ING Services Polska (ISP), dostawcy usług IT na rzecz podmiotów Grupy ING działających na całym świecie. W zakres usług dostarczanych przez ISP wchodzi tradycyjny hosting, zdalne zarządzanie infrastrukturą i aplikacjami oraz usługi związane z bezpieczeństwem IT. Centrum zatrudnia 500 pracowników i obsługuje ponad 70 klientów w 15 krajach.

Szybki rozwój firmy spowodował konieczność wdrożenia rozwiązania automatyzującego procesy tworzenia i zarządzania wirtualnymi maszynami, które są dostarczane klientom w ramach usługi hostingu zasobów systemowych. Rozwiązanie chmury prywatnej doskonale odpowiedziało na obecny popyt szefów IT w Europie, podczas gdy mechanizmy federacji umożliwią przejście na chmurę hybrydową w przyszłości[2].

2 http://www.ingservicespolska.pl/pl/13,case-study.html

W Polsce pojawiają się również wdrożenia usług dostarczanych w modelu chmury publicznej. W takich przypadkach, podejmując decyzje o wyborze rozwiązania chmurowego, banki wybierają te procesy biznesowe, które nie są traktowane jako outsourcing istotnych procesów bankowych w rozumieniu polskiego prawa bankowego. Często dotyczy to tych, które nie wymagają przetwarzania danych osobowych. Przykładem takiego podejścia są wdrożenia w polskim sektorze finansowym rozwiązania MS Office 365 lub MS CRM Online. W tych wdrożeniach w grupach finansowych wyselekcjonowano podmioty, które nie są regulowane ustawą o prawie bankowym lub wybrano procesy i zadania, które nie są istotnymi procesami bankowymi. Przykładowo CRM serwowany z chmury wykorzystywany jest do zarządzania tzw. długim kanałem, czyli partnerami handlowymi współpracującymi z daną instytucją finansową. O wyborze usług Microsoftu zdecydowały m.in. stosowane przez daną firmę zasady i mechanizmy bezpieczeństwa i zarządzania danymi oraz spełnienie wymagań dotyczących obsługi danych osobowych na terenie Unii Europejskiej (zgodność z dyrektywą UE o ochronie danych 95/46/WE).

Świetlana przyszłość?

Reasumując – w chwili obecnej polskie regulacje sektora finansowego na tle innych krajów Unii Europejskich – głównie ze względu na sposób uregulowania kwestii outsourcingu – są najbardziej wymagające względem koncepcji dostarczania usług w chmurze. Pomimo tych trudności, korzyści z takiego modelu dostarczania usług są tak istotne, że w Polsce zrealizowano w sektorze finansowym pierwsze wdrożenia rozwiązań chmurowych. Trudno jednak ukryć, że wdrożenia te realizowane są dzięki wyjątkowej determinacji zarówno klientów, jak i dostawców tego typu usług. Dzisiaj udaje się wtłoczyć konkretne usługi cloudowe w ramy polskich regulacji sektora finansowego, jednak wymaga to żmudnej analizy i połączonej wiedzy specjalistycznej z dziedziny prawa i architektury poszczególnych rozwiązań informatycznych.

Istniejąca od 2004 roku regulacja outsourcingu w sektorze finansowym dryfuje w złym kierunku, wprowadzając rozwiązania niespotykane na tle przepisów innych państw europejskich. Zakaz ograniczeń odpowiedzialności outsourcera bankowego jest niespotykany w innych krajach i sprzeczny z globalną kulturą prawną obszaru informatyki. Uregulowanie podoutsourcingu bankowego w 2011 roku nie dość, że zostało zredagowane w sposób dezorientujący, to rykoszetem uderzyło w inne podsektory, np. powodując restrykcyjną zmianę podejścia do podoutsourcingu w sektorze ubezpieczeniowym.

W zakresie ograniczeń odpowiedzialności w dobrym kierunku idą rozwiązania przedstawione w Rekomendacji D Komisji Nadzoru Finansowego, która główną wagę przykłada do podejścia do ryzyka operacyjnego i jego konsekwencji dla banku, oraz widzi w outsourcingu do podmiotu profesjonalnego także sposób skutecznego zarządzania takim ryzykiem. Należy mieć jedynie nadzieję, że KNF nie tylko w dezyderatach, ale również w sposobie nadzoru nad prawidłowym wykonywaniem założeń Rekomendacji będzie w podobny sposób podchodzić do zarządzania ryzykiem przetwarzania informacji. W takim też kierunku powinna iść regulacja ustawowa. Profesjonalne usługi cloudowe często (jeśli nie na ogół) zapewniają bowiem dużo większe bezpieczeństwo i kontrolę nad danymi niż można uzyskać wewnątrz własnej organizacji lub dużo większą efektywność bezpieczeństwa (rozumianą jako relację pomiędzy poziomem bezpieczeństwa a nakładami na jego utrzymanie).

Dalszy rozwój rynku usług chmurowych w sektorze finansowym w Polsce wymaga większego zaangażowania liderów innowacji przede wszystkim po stronie zamawiających. W dłuższej perspektywie istnieje potrzeba zarówno zmiany świadomości, jak i zmian regulacyjnych w tym zakresie. Główni interesariusze i regulatorzy sektora bankowego, tacy jak Związek Banków Polskich i Komisja Nadzoru Finansowego, powinni wypracować razem z dostawcami usług informatycznych, w drodze wspólnego dialogu, platformę, która pozwoli nowoczesnym technologiom informatycznym nadać kolejny impuls wzrostu wydajności i konkurencyjności w tym sektorze, wzorem działań podejmowanych w latach 90. ubiegłego stulecia. Dzięki tamtym działaniom polski sektor bankowy jest nadal postrzegany jako jeden z najbardziej technologicznie zaawansowanych w Europie, lecz dla podtrzymania tego wizerunku konieczne są warunki do wdrażania nowoczesnych technologii dnia dzisiejszego.

Maciej Kaniewski

Jest architektem rozwiązań informatycznych dla jednego z koncernów motoryzacyjnych, prowadzi projekty w Polsce i w Niemczech w dziedzinie automotive i autofinance oraz wykłada zarządzanie projektami na University of Applied Sciences w Berlinie. Jest współwłaścicielem firmy EOS, którą założył w 1992 roku. Posiada certyfikaty PMP (od 2003 roku), Agile Project Management Foundation i Agile Project Management Registered Practitioner. Jest także wieloletnim członkiem Project Management Institute oraz od niedawna członkiem International Institute for Business Analysis.

Maciej Kaniewski, EOS

Metodyki Agile – blaski, cienie i szare strefy

Metodyki typu Agile, określane w polskiej literaturze mianem zwinnych[1], powstały pierwotnie w wyniku niezadowolenia z niedostatków tradycyjnych metod wytwarzania oprogramowania i zarządzania projektami informatycznymi, w szczególności metod opartych na modelu wodospadowym. Podejście wodospadowe wygląda w skrócie tak: z początku odbiorca systemu informatycznego opracowuje specyfikację wymagań, być może przy wsparciu analitycznym ze strony zewnętrznych doradców. W następnym kroku inny zespół – często już po stronie dostawcy systemu – opracowuje projekt techniczny, potem zespół wykonawczy buduje zgodny z tym projektem system informatyczny, który po wykonaniu rygorystycznych testów technicznych i użytkowych oraz usunięciu błędów zostaje wdrożony na produkcję. Przejście od jednego etapu do następnego wymaga „zaliczenia" odpowiedniego punktu kontrolnego, a w jego ramach mniej lub bardziej ścisłych procedur weryfikujących, wiążących się m.in. z przeglądem opracowanej wcześniej dokumentacji stosownej do danego etapu.

Konstrukcja tego modelu postępowania jest logiczna i wewnętrznie spójna, jednakże coś, co znakomicie się sprawdzało w przypadku klasycznych projektów inżynierskich (np. budowlanych czy konstrukcyjnych) zaczęło wykazywać słabości w kontekście projektów informatycznych. Precyzyjne opisanie i zakomunikowanie definitywnych wymagań dla systemu informatycznego od razu na początku projektu jest obarczone większym prawdopodobieństwem błędów niż określenie analogicznych wymagań dla budynku lub obrabiarki. Przyczyn takiego stanu rzeczy można szukać w niepełnym stanie wiedzy

1 W PMBOK użyto zastępczo także pojęcia „Adaptive Life-Cycles" w odróżnieniu od „Predictive Life-Cycles", jednak nie w odniesieniu do całościowej metody zarządzania projektem, lecz tylko do cyklu życia projektowego.

zespołów dziedzinowych w początkowych fazach projektu, braku powszechnych standardów analizy wymagań, dotyczących zarówno procesu analizy jak i zapisu wyników oraz zrozumiałych dla wszystkich uczestników analizy, a także w dynamicznym rozwoju technologii informatycznej, powodującym – zwłaszcza w długoterminowych projektach – nieadekwatność wymagań osadzonych we wcześniejszej rzeczywistości technologicznej.

Konieczność późniejszych uzupełnień i modyfikacji 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?

Filozoficzne założenia zwinności

W 2001 roku grupa siedemnastu wybitnych inżynierów oprogramowania opublikowała tzw. *Manifesto for Agile Software Development*[2]. Jego autorzy od jakiegoś czasu stosowali już alternatywne metodyki tworzenia oprogramowania, a wielu z nich uczestniczyło w ich tworzeniu[3]. 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 zaspokajający 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.

2 The Agile Manifesto, www.agilemanifesto.org

3 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,
- współpracę z klientem ponad negocjację umowy,
- reagowanie na zmiany ponad stosowanie się do planu,

dostrzegając zarazem wartość w elementach znajdujących się z prawej strony 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, polityki i procedury, a relacje pomiędzy partnerami biznesowymi muszą zostać uregulowane kontraktowo. Nielubiana dokumentacja w końcu też powinna powstać. Wartości z lewej strony porównania nie są zatem sprzeczne z wartościami z prawej strony. 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 (predykcyjnego). Analogicznie, nacisk na zaspokojenie potrzeb biznesowych i osiągnięcie tym samym zadowolenia klienta nie są obce podejściom bardziej tradycyjnym (porównaj utrzymanie ciągłego uzasadnienia biznesowego – *continuous business justification* – w metodyce PRINCE2, podniesione do rangi pierwszej z podstawowych zasad w edycji z 2009 roku[4]).

Koncepcja Agile rozpoczęła swój triumfalny pochód w czasach, kiedy „klasycznym" podejściom do zarządzania projektami, takim jak PRINCE2 czy też metodyki wywodzące się z PMBOK[5], 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*[6], czyli obowiązkowe dostosowanie metodyki do potrzeb projektu i organizacji. Z kolei według PMBOK decyzja dotycząca odpowiedniej metody realizacji

---

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

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

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

projektu leży w gestii kierownika projektu i zespołu, naturalnie z uwzględnieniem uwarunkowań organizacyjnych.[7]

Agile ani nie oznacza preferencji dla działań *ad hoc* aż do braku metodyki włącznie, ani też nie jest sprytnym sposobem na zamaskowanie chaosu w zarządzanym projekcie. Wręcz przeciwnie: każde konkretne podejście Agile wymaga 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"[8]. Jak podkreślają wszystkie podręczniki metodyk Agile, wybiórcze stosowanie elementów metodyki ma negatywny wpływ na sukces projektu.[9]

Podejście zwinne nie neguje także konieczności tworzenia systemu informatycznego zgodnie z zasadami sztuki inżynierskiej. Z jednej strony, u dostawcy muszą funkcjonować procesy zapewniające jakość tworzonego oprogramowania w aspektach takich, jak spójność tworzonego systemu, jednolitość standardu kodowania, uwzględnienie wymagań pozafunkcjonalnych (przechwytywanie i obsługa błędów, bezpieczeństwo itp.) i inne. Z drugiej strony, klient powinien zapewnić jakość „wygenerowanych" wymagań, a także spójność i kompletność scenariuszy testowych. Odbiór tworzonego systemu pozostaje zagadnieniem kluczowym dla obu stron: po stronie klienta gwarantuje uzyskanie systemu spełniającego jego potrzeby biznesowe, po stronie dostawcy gwarantuje możliwość rozliczenia.

Reasumując, przy podejściu zwinnym nadal musimy dysponować kryteriami określającymi, czy praca została wykonana i czy produkt projektu został wykonany dobrze. Kryterium akceptacji produktu powinno być ustalone a priori, niezależnie od poziomu formalizacji metodyki zarządzania i metodyki wytwórczej. Metodyka SCRUM posługuje się pojęciem *definition of*

---

7 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.

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

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

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

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 produktów projektu,
- 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. W następnych podrozdziałach zagadnienie komunikacji pomiędzy interesariuszami zostanie przedstawione bardziej szczegółowo.

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.

Świat potrzeb interesariuszy

W kontekście rozważań nad międzyludzkim wymiarem zarządzania projektami i tworzenia rozwiązań informatycznych warto sobie zadać (lub raczej – nieustannie zadawać) trzy pytania: czy w projektach rozmawiamy z właściwymi ludźmi, czy rozmawiamy we właściwy sposób i czy ci ludzie rozmawiają też między sobą nawzajem. Pojęcia-klucze, które otworzą tu niejedne drzwi, to zarządzanie interesariuszami projektu i analiza biznesowa, w obu wypadkach stanowiące obszary wiedzy rozwijające się dynamicznie częściowo na styku z, a częściowo wewnątrz dyscypliny zarządzania projektami.

Zainteresowanie obszarem związanym z interesariuszami stanowi naturalną konsekwencję faktu, że oczekiwania względem projektu nie biorą się tylko

z jednego źródła (np. sponsora), ale stanowią wypadkową życzeń, preferencji i obaw szerszej grupy ludzi, a także uwarunkowań i ograniczeń, w ramach których projekt się znajduje. Kształt projektu zaczyna się zazwyczaj klarować na długo wcześniej zanim zostanie on porządnie zdefiniowany i formalnie uruchomiony. W podejściach Agile wykorzystujemy zazwyczaj listę wymagań w postaci *backlog'u* funkcjonalności, którego zawartość jest dynamicznie przyporządkowywana do kolejnych etapów (sprintów, inkrementów itp.). Sytuacja, kiedy kierownik projektu dysponuje takim *backlog'iem*, jest już jednak stosunkowo komfortowa – tylko jak należy najskuteczniej do powstania tego *backlog'u* doprowadzić?

Z jednej strony zadanie polega nie tylko na zidentyfikowaniu czy też zgromadzeniu wymagań *(collect requirements)*, ale na ich pozyskaniu *(elicit requirements)* poprzez identyfikację potrzeb. Subtelna różnica pomiędzy tymi dwoma pojęciami odzwierciedla zasadniczo odmienną perspektywę analityczną. W pierwszym przypadku analityk musi tylko przepytać odpowiednie osoby i usystematyzować informacje, które od nich uzyskał, starając się zapewnić zadowalającą formalną postać wymagań, np. żeby były zgodne z zasadami SMART[10]. W przypadku wydobycia wymagań analityk musi sięgnąć głębiej, mianowicie do potrzeb, które mają swoje źródło w założeniach biznesowych – niekoniecznie precyzyjnie zapisanych – zakorzenionych w wizji i misji przedsiębiorstwa lub organizacji. Aby do tych potrzeb dotrzeć, analityk musi wiedzieć, z jakimi grupami osób – interesariuszami projektu – się kontaktować. W tym celu niezbędna jest identyfikacja interesariuszy i opracowanie sposobu postępowania z nimi. Aby z kolei poprawnie zidentyfikować ich potrzeby i przetworzyć je na wymagania, analityk musi posłużyć się różnymi technikami z obszaru analizy biznesowej, adekwatnymi dla danego interesariusza i dla poziomu szczegółowości, na którym rozpoczyna działania.

Zwróćmy uwagę na to, że powszechnie stosowana definicja analizy biznesowej brzmi następująco:[11] analiza biznesowa jest zestawem zadań i technik wykorzystywanych jako sposób **łączności pomiędzy interesariuszami**

---

10 SMART stanowi akronim od specific (konkretne), measurable (mierzalne), attainable (osiągalne), realistic (realistyczne) i time-related (ograniczone w czasie); istnieją też inne interpretacje, por. http://en.wikipedia.org/wiki/SMART_criteria

11 „Business analysis is the set of tasks and techniques used to work as a liaison among stakeholders in order to understand the structure, policies, operation of an organization, and to recommend solutions that enable the organization to achieve its goal", w: A Guide to the Business Analysis Body of Knowledge (BABOK Guide) – Version 2.0, praca zbiorowa, International Institute of Business Analysis, Toronto 2009; tłumaczenie własne.

[wyróżnienie M.K.] w celu zrozumienia struktury, polityk i działalności organizacji oraz zalecenia rozwiązań, które umożliwią organizacji osiągnięcie swojego celu.

Można zatem oczekiwać, że analiza biznesowa z założenia powinna wspierać interakcję i porozumienie pomiędzy interesariuszami, a nie stanowić tylko sposobu na przekształcenie wiedzy pojedynczych interesariuszy w wymagania.

Temat niniejszego artykułu nie pozwala na przedstawienie pełnego spektrum technik analizy biznesowej, a zatem skupmy się na jednej, szczególnie popularnej w metodykach Agile, mianowicie *user stories* (opowieściach użytkownika). *User stories* mają na celu dotarcie do wymagań poprzez przedstawienie perspektywy poszczególnych interesariuszy w kontekście oczekiwanych zachowań systemu. Mogą być wykorzystywane przez analityków, ale także użytkowników systemu, deweloperów i testerów. Rozpowszechnione podejście do *user story* polega na sformułowaniu opisu w następującej postaci:

Jako (tu: określona rola lub aktor) potrzebuję (tu: cechy lub zachowania systemu), po to, aby (tu: oczekiwana wartość lub korzyść biznesowa).

Do takiego opisu często dodaje się priorytet, reguły biznesowe uściślające zapis oraz kryteria, według których można ocenić poprawność zachowania systemu. Prawidłowa *user story* jest skonstruowana w zgodności z modelem INVEST[12]:

- ***I**ndependent* (niezależna) – zmniejszona liczba zależności powoduje, że łatwiej jest ją zaplanować.
- ***N**egotiable* (negocjowalna) – szczegóły opowieści dodaje się poprzez kolaborację i konsensus.
- ***V**aluable* (wartościowa) – powinna zawsze dostarczać wartości klientowi końcowemu[13].
- ***E**stimable* (możliwa do oszacowania) – nie powinna być zbyt długa lub zbyt ogólna, ponieważ to nie pomoże w oszacowaniu.
- ***S**mall* (mała) – powinna nadawać się do realizacji przez zespół w krótkiej perspektywie czasowej,
- ***T**estable* (zdatna do testów) – *user stories* powinny być zawsze wsparte jasnymi, dobrze sformułowanymi kryteriami akceptacji.

---

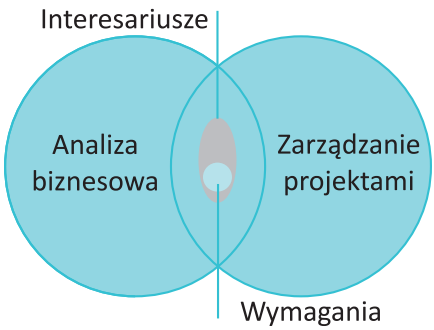
12 J. Cadle i in., Business Analysis Techniques, 99 essential tools for success, BCS Learning & Development Ltd., Swindon (UK), 2014, technika nr 69.

13 Warto zwrócić uwagę, że pojęcie „klienta końcowego" nie musi być jednoznaczne dla wszystkich interesariuszy.

Skuteczne zastosowanie tej techniki wymaga zidentyfikowania wszystkich ról i aktorów, które znajdują odzwierciedlenie co najmniej w podzbiorze najważniejszych interesariuszy oraz nakłonienie ich do zdefiniowania swoich *user stories*. Jednocześnie, ponieważ interesariusze mogą mieć różne perspektywy i różne potrzeby, należy przeprowadzić konsolidację rozbieżnych lub sprzecznych *user stories*.

Przykład: projekt ma na celu stworzenie portalu bankowego, pozwalającego klientowi na samodzielną obsługę umów kredytowych i płatności. Jednym z celów marketingu może być dodatkowa promocja marki poprzez oferty marketingowe i różne funkcjonalne dodatki – co można odzwierciedlić w *user story*. W *user story* pisanej z perspektywy użytkownika nadrzędnym celem może być z kolei szybkość działania i prostota. Dział back office chciałby zwiększenia poziomu automatyzacji obsługi umów i zmniejszenia obciążenia pracowników, a dział windykacji – możliwości szybszej lub bardziej skutecznej komunikacji z klientem. Można się spodziewać, że oczekiwania marketingu będą stały w pewnej sprzeczności z oczekiwaniami klienta, które z kolei w dużej mierze mogą się pokrywać z oczekiwaniami back office, a oczekiwania back office – z oczekiwaniami działu windykacji. Dlatego też zarządzanie projektem powinno uwzględnić proces takiego uzgadniania oczekiwań interesariuszy, aby doprowadzić do powstania spójnego zestawu wymagań – co w podejściu Agile przekłada się na spójny *backlog*.

Celem powyższych rozważań było ukazanie przenikania się świata zarządzania projektami i analizy biznesowej z dwoma punktami przecięcia: interesariuszami i wymaganiami, tak jak na poniższej ilustracji:



Zauważmy, że oba te punkty przecięcia są obecne zarówno w standardzie PMBOK, jak i w czołowym standardzie z obszaru analizy biznesowej,

tj. przywołanym Business Analysis Body of Knowledge[14]. W tym drugim dokumencie wystarczy zwrócić uwagę na dziedzinę wiedzy *Business Analysis Planning and Monitoring*, a konkretnie punkt *2.2 Stakeholder Analysis*, oraz na całą dziedzinę *Requirements Management and Communication*. Project Management Institute z kolei od niedawna oferuje certyfikat zawodowy *Professional in Business Analysis (PMI-PBA)*, co pokazuje rosnące uznanie PMI dla tej dziedziny w kontekście zarządzania projektami.[15]

Konwergencja obu światów może tylko cieszyć kierowników projektów. Powiązanie to nie było niegdyś wcale oczywiste, gdyż tematykę wymagań traktowano raczej jako należącą do sfery dziedzinowej (wytwórczej), leżącej poza obszarem zainteresowania zarządzania projektami. Przykładowo, proces gromadzenia wymagań *(collect requirements)* dodano do PMBOK dopiero w edycji czwartej z 2008 roku. W tej samej edycji dość ogólny proces zarządzania interesariuszami *(manage stakeholders)* został rozdzielony na identyfikację interesariuszy *(identify stakeholders)* i zarządzanie oczekiwaniami interesariuszy *(manage stakeholder expectations)*, lecz czym oba te procesy pozostawały przyporządkowane do dziedziny zarządzania komunikacją w projekcie. Dopiero w edycji piątej z 2013 roku dokonał się awans wszystkich procesów związanych z interesariuszami do osobnej dziedziny *Project Stakeholder Management*, tj. na tym samym poziomie strategicznym, co zarządzanie czasem, zakresem, jakością, ryzykiem itp. Warto zwrócić przy okazji uwagę na przesunięcie punktu ciężkości definicji interesariusza. W edycji trzeciej PMBOK interesariuszy definiuje się jako:

„Osoby i organizacje takie jak klienci, sponsorzy, organizacja realizująca projekt oraz inne podmioty spoza projektu, które są aktywnie zaangażowane w projekt lub których interesy podlegają korzystnym lub niekorzystnym wpływom wynikającym z realizacji lub zakończenia projektu".[16]

---

14 A Guide to the Business Analysis Body of Knowledge (BABOK), Version 2.0, International Institute of Business Analysis, Version 2.0, Toronto, 2009; nowa edycja 3.0 zostanie opublikowana 15 kwietnia 2015, już po dacie złożenia do druku niniejszego artykułu.

15 „Business analysis helps you work with stakeholders to define their business requirements so you can shape the output of projects and drive successful business outcomes." – cytat ze strony http://www.pmi.org/Certification/PMI-Professional-in-Business-Analysis-PMI-PBA.aspx, stan z dnia 2015-03-09

16 „Persons and organizations such as customers, sponsors, performing organization and the public, that are actively involved in the project, or whose interests may be positively or negatively affected by execution or completion of the project and its deliverables"; tłumaczenie polskie z „Kompendium wiedzy o zarządzaniu projektami", Management Training and Development Center, Warszawa 2006, str. 377.

Natomiast w edycji piątej mamy już:

„Jednostka, grupa lub organizacja, która może wpłynąć, podlegać wpływowi lub postrzegać się jako podlegająca wpływowi decyzji, czynności lub wyniku projektu."[17]

Zwróćmy uwagę na fakt, że w edycji piątej interakcja interesariusza z projektem rozpoczyna się już na poziomie podejmowania decyzji projektowych (w rzeczywistości jeszcze przed rozpoczęciem projektu), a nie dopiero w chwili zakończenia projektu. Podkreślono też subiektywną ocenę wpływu projektu przez interesariusza.

Czy adepci podejścia zwinnego mogą skorzystać na uwzględnieniu trendu ściślejszego zjednoczenia dziedziny analizy biznesowej i zarządzania projektami? Zdaniem autora mogą skorzystać dwojako: z jednej strony poprzez bardziej strukturalne podejście do identyfikacji interesariuszy i analizy ich potrzeb, z drugiej poprzez dostosowanie narzędzi interakcji i komunikacji z interesariuszami i pomiędzy interesariuszami do etapu projektu (łącznie z etapem przedprojektowym) i do charakteru samych interesariuszy.

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 umożliwienie zastosowania podejścia Agile w typowej, stabilnej organizacji o charakterze hierarchicznym. Jako przykład takiego podejścia może posłużyć podejście Disciplined Agile Delivery[18] opracowane w IBM oraz DSDM[19] Agile Project Management opracowane przez brytyjską organizację DSDM[20] Consortium i stanowiące składową 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, oba zresztą intuicyjnie oczywiste:

---

17 W oryginale: „An individual, group or organization who may affect, be affected by, or perceive itself to be affected by a decision, outcome or activity of a project"; tłumaczenie własne.

18 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.

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

20 Skrót od „Dynamic System Development Method".

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

Autorzy DSDM postawili sobie za priorytet umożliwienie i wspieranie efektywnej współpracy. Ponieważ przyjęto rozsądne założenie, że kompromisy w kwestii jakości są w projektach niepożądane, a ograniczenia czasowe i kosztowe raczej sztywne, toteż jedyną zmienną niezależną pozostaje zakres projektu. Dlatego podstawowe narzędzie tej metodyki wiąże się z zarządzaniem zakresem i jest to tzw. spriorytetyzowana lista wymagań *(prioritized requirements list)*. Wszystkie wymagania ujęte w tej liście otrzymują 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 około 60% wymagań niezbędnych[21], co gwarantuje wystarczającą elastyczność zakresu. Dostawca rozwiązania informatycznego zobowiązuje się jedynie do realizacji wszystkich wymagań typu *must* i *should* w założonym czasie i budżecie. Realizacja wymagań typu *could* nie jest już gwarantowana, lecz niewykluczone przy sprzyjającym przebiegu projektu.

U podstaw podejścia DSDM leży osiem zasad:

- koncentracja na **potrzebie biznesowej**: zrozumienie rzeczywistych priorytetów, ustanowienie zdrowego uzasadnienia biznesowego *(business case)*, zapewnienie ciągłego zaangażowania biznesu w projekt 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 grup, aktywne zaangażowanie przedstawicieli strony biznesowej oraz budowa kultury wspólnego zespołu *(one-team culture)*,
- **bezkompromisowa jakość**: zdefiniowanie żądanego poziomu jakości od początku, zapewnienie, że jakość nie stanie się zmienną projektu,

21 Procentowy udział dotyczy przewidywanego wysiłku niezbędnego do zrealizowania wymagań.

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 (nie na zakończeniu czynności), zarządzanie proaktywne, analiza dalszego uzasadnienia dla projektu na podstawie celów biznesowych.

Zarządzanie projektami według DSDM wykorzystuje cztery podstawowe praktyki:

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

Uzyskanie wspomnianej spriorytetyzowanej listy wymagań o wdzięcznym skrócie PRL odbywa się w kilku etapach. Na etapie przedprojektowym *(pre-project)* zostaje zidentyfikowany cel biznesowy projektu. Już w tym momencie

do gry wchodzą zatem metody analizy interesariuszy i metody analizy biznesowej. Jeżeli projekt uznano za uzasadniony biznesowo, 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 zakończenia 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 inkrementy posługuje się wymaganiami na poziomie listy PRL. Rozdział inkrementów na timeboxy wymaga bardziej szczegółowej analizy wymagań. Najbardziej szczegółowa analiza wymagań powstaje na poziomie planowania timeboxu. 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. Metodę 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 – zwróćmy przy tym uwagę na wspomnianą wcześniej konieczność identyfikacji interesariuszy i zapewnienia współpracy między nimi. 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[22]. Przełożony jest przede wszystkim wewnętrznym usługodawcą,

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

który wspiera i promuje swoich współpracowników. Dlatego też powinien – 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[23], 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 z wszystkimi osobami w strukturze, przekazujący 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.

---

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

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

Dina Dąbrowska
Associate w Goldenberry. Posiada wieloletnie doświadczenie przy realizacji oraz zarządzaniu projektami w obszarze IT. Jest certyfikowanym Scrum Masterem i autorem publikacji na temat metod zwinnych, w tym „Scrum w dużych organizacjach".

Bartłomiej Owczarek
Partner w Goldenberry. Odpowiada za obszar strategii Goldenberry. Zajmuje się również nadzorem nad rozwojem nowych technologii w ramach przedsięwzięć startupowych.

Dina Dąbrowska, Bartłomiej Owczarek, Goldenberry

Zwinne zarządzanie programami

Technologia ma coraz większe znaczenie dla wartości dostarczanej przez banki klientom. Dostrzegły to nawet firmy technologiczne i to do tego stopnia, że niektóre mają coraz większy apetyt na wypchnięcie z łańcucha usług finansowych samych banków. W końcu, jak stwierdził Marc Andreessen, „finanse to czysta informacja", czyli coś, z czym firmy technologiczne radzą sobie najlepiej.

Nic dziwnego, że banki podjęły informatyczny wyścig zbrojeń, czego na polskim rynku przykładem są inwestycje takie jak nowy mBank lub jeszcze nowszy bank SMART. W czasie, gdy coraz rzadziej wykorzystywane przez przeciętnego klienta oddziały znikają, „twarzą" banku stają się widoczne dla klienta technologie.

Z drugiej strony, technologiczne zbrojenia są kosztowne, a w warunkach wzrastającej konkurencji oszczędności stają się coraz ważniejsze. Wydatki na IT nie są tu wyjątkiem. Oprócz szybkiego wprowadzania nowości na rynek (lub spełniania w terminie kolejnych regulacyjnych wymagań) od IT oczekuje się równocześnie obniżenia kosztów.

W tej rzeczywistości tradycyjne podejście do produkcji nowych technologii w bankach – szczególnie duże, kosztowne programy, które efekty przynoszą po latach od rozpoczęcia pierwszych analiz – przestaje spełniać współczesne wymagania. Banki stopniowo, rozpoczynając od pilotażowych projektów, często w „nowych" obszarach, takich jak technologie mobilne adoptują metody zwinne, które pozwalają na szybki rozwój produktu i przemycają ideologię „lean", wymuszając uelastycznienie struktury organizacyjnej.

Metody zwinne (ang. „agile") zakładają rytmiczny, iteracyjny charakter pracy, interdyscyplinarne zespoły i aktywny udział (oraz odpowiedzialność) właściciela biznesowego za rozwój produktu.

Po pierwszych pozytywnych doświadczeniach z pilotażowych projektów pojawia się pytanie o przeniesienie zwinnego podejścia na poziom całych programów złożonych z wielu równoległych produktów. Wtedy jednak pojawiają się trudności, ponieważ metody zwinne tak naprawdę wymagają zmiany sposobu działania całej organizacji, nie ograniczając się tylko do programistów IT. Innymi słowy metody zwinne nie są tylko „sposobem, w jaki może pracować IT" i wymagają też zmiany podejścia biznesu.

Zmiana kulturowa

Przenoszenie doświadczeń z firm technologicznych, które najszybciej zaadoptowały metody zwinne, obarczone jest ryzykiem – ponieważ bank, mimo wszystko, nie jest firmą technologiczną, a co za tym idzie osoby odpowiedzialne za obszary biznesowe widzą w rozwiązaniach IT tylko narzędzie, a nie końcowy produkt dla klienta. Oczekiwania pełnego zaangażowania w jego rozwój zderzają się więc z rzeczywistością „właścicieli biznesowych", których codzienne obowiązki operacyjne mają wyższy priorytet niż stały nadzór nad rozwojem produktu technologicznego.

O ile w przypadku pilotażowego projektu przygotowanie wszystkich zaangażowanych w niego stron, łącznie z jednym właścicielem produktu, nie jest tak dużym wyzwaniem, w przypadku dużych programów zaangażowana jest zwykle niemal cała organizacja. To oznacza, że istnieje szerokie grono kadry zarządzającej, które musi zostać przygotowane do nowego podejścia – w tym do rzeczywistości, w której znikają tradycyjne ramy negocjacji „kontraktu" pomiędzy zamawiającym biznesem a wykonującym IT, a biznes staje się współodpowiedzialny za projekty.

Jak przedstawiamy dalej, usuwane są czynności uznawane za zbędne w podejściu zwinnym, na przykład skomplikowane raportowanie, a co za tym idzie zbędne są niektóre role, takie jak PMO, zajmujące się często przede wszystkim utrzymywaniem skomplikowanych planów i aktualizacją statusów postępu prac na prezentacjach dla wielu interesariuszy.

Chociaż z dystansem traktujemy licznych guru metod zwinnych, którzy niemalże z religijnym zapałem chcieliby zmienić każde stanowisko w organizacji i każdy termin niezgodny z ortodoksją („nie prowadzimy już projektów, tylko rozwijamy produkty!"), to jednak trzeba zdawać sobie sprawę z konieczności poparcia najwyższego kierownictwa dla głębszych zmian.

Zwinne podejście do programów: po pierwsze unikać

Metodyki zwinne zostały udoskonalone w mniejszych, wyizolowanych inicjatywach, takich jak nowe firmy. Można jednak stosować je także w warunkach działania banku, gdzie projekty są ze sobą ściśle powiązane i z tego powodu często łączone w programy.

Tworzenie skomplikowanych, dużych inicjatyw, z wieloma współzależnymi projektami, samo w sobie jest działaniem, którego zwinne organizacje unikają, jeśli tylko jest to możliwe. Oprócz wysokich kosztów związanych z koordynacją, których, niezależnie od metodyki, nie można uniknąć, trudniej jest również o inkrementalny rozwój całościowego produktu.

Czasem uniknięcie tworzenia programu nie jest jednak możliwe. Dzieje się tak na przykład wtedy, gdy inicjatywa dotyczy połączenia banków lub jej zakres zawiera zmiany narzucane przez regulatora. Programy takie również można zorganizować w podejściu zwinnym, jednak trzeba się do tego dobrze przygotować.

Często tworzenie przerośniętych struktur wynika bardziej z zastanego sposobu myślenia i inercji biurokratycznej (zgodnie z zasadą, że większa organizacja zawsze wymyśli sobie pracę), niż z obiektywnych przyczyn. Inicjatywy IT cierpią również z utożsamiania produkcji oprogramowania z fizycznym procesem, w którym nakład pracy da się z góry ocenić, a większa liczba zaangażowanych osób proporcjonalnie skraca czas wykonania zadania.

Oprogramowanie to jednak produkcja kreatywna i jeden bardzo dobry członek zespołu może być bardziej produktywny niż pięciu słabych. Dodatkowo, z powodu zaangażowania dużej liczby osób pojawiają się koszty koordynacji, a powstałe środowisko pracy, w którym więcej czasu spędza się na pisaniu raportów dla kolejnych szczebli zarządzania niż na pracy kreatywnej, zniechęca najlepszych pracowników.

Pierwszym krokiem dla większej zwinności organizacji może być więc powtórne spojrzenie na zasadność tworzenia inicjatyw-kolosów oraz zmiana akcentu ze zwiększania stanu osobowego na koncentrację na małych zespołach złożonych z najbardziej utalentowanych specjalistów na rynku.

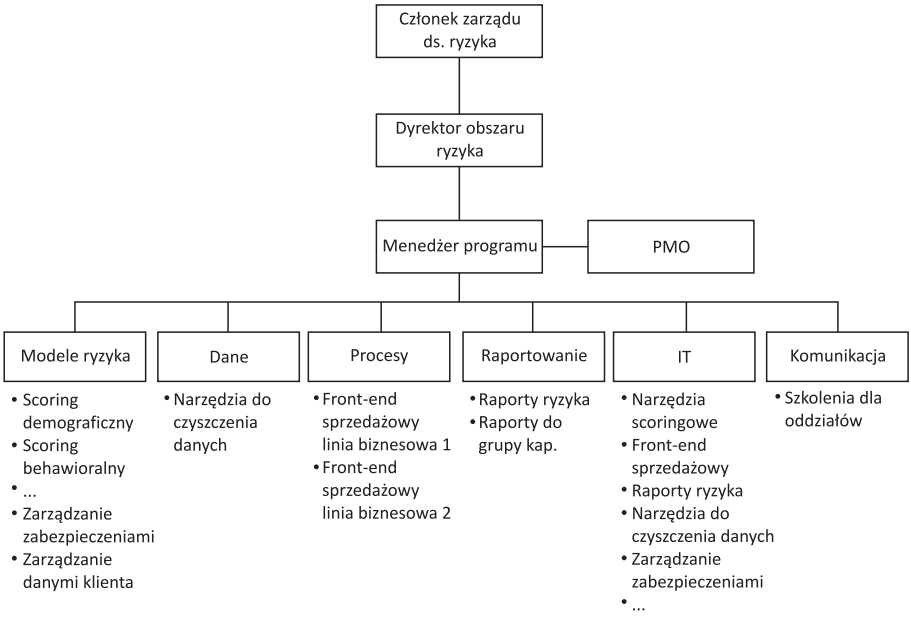
Przykład tradycyjnego programu IT

Wracając do zarządzania programami IT, dla porównania dobrze jest zacząć od szkicu, jak taki program wyglądałby w podejściu tradycyjnym, aby

skierować uwagę na problemy i koszty, których w podejściu zwinnym chcielibyśmy uniknąć.

Wybrany przez nas przykład to program związany z wdrożeniem nowej metody zarządzania ryzykiem kredytowym w średniej wielkości banku. Zarządzanie inicjatywą jako programem jest konieczne, ponieważ związane z nią zmiany wymagają dostosowań niemal w całej strukturze banku – od sprzedaży, przez ryzyko aż po operacje. Zmiany w IT dotykają odpowiednio wszystkich istotnych elementów architektury, w tym budowę nowych aplikacji dla użytkowników pierwszej linii, wprowadzenie szyny integracyjnej i przebudowę hurtowni danych.

Rysunek 1.
Struktura przykładowego programu w podejściu tradycyjnym



Program angażuje ponad 30 osób po stronie biznesu, głównie pracowników z obszaru ryzyka kredytowego, oraz 15 osób po stronie IT: analityków, architektów, testerów i administratorów. Oprócz tego zaangażowanych jest wielu dostawców IT.

W programie bierze również udział menedżer programu, 6 kierowników obszarów oraz 5-osobowe PMO, zajmujące się koordynacją i raportowaniem do grupy kapitałowej. Program podzielony jest na strumienie funkcjonalne (np. strumień IT, strumień procesów). W każdym strumieniu uruchomionych jest od kilku do kilkunastu projektów. Menedżer projektu raportuje do dyrektora odpowiedzialnego za obszar ryzyka, a ten z kolei do odpowiedniego członka zarządu.

Projekty dotyczące systemów IT prowadzone są w podejściu kaskadowym. Zaakceptowana przez użytkowników biznesowych dokumentacja trafia do dostawców zewnętrznych odpowiedzialnych za aplikacje, w których zmiana jest wymagana. Po serii testów technicznych użytkownicy biznesowi weryfikują jakość oprogramowania i spełnienie przez nie wymagań.

Program musi zakończyć się w określonym przez regulatora terminie, dlatego wszelkie zmiany w zaplanowanym zakresie są niepożądane. Zmian jednak nie da się uniknąć, ponieważ analiza nie jest doskonała, a warunki biznesowe zmieniają się szybko.

Każda zmiana zakresu musi być przeanalizowana na odpowiednich szczeblach i uzgodniona wspólnie z zarządem, przez co wydłuża się czas jej wprowadzenia. Powstała wcześniej dokumentacja również jest „produktem", który w takiej sytuacji należy zaktualizować.

Odpowiedzialność za powodzenie programu spoczywa na zarządzie, który najczęściej nie jest bezpośrednio zaangażowany w prace projektowe. Członkowie zarządu polegają najczęściej na podsumowaniu z licznych raportów, których przygotowanie zajmuje znaczną część czasu kierowników strumieni i menedżera programu. Jednocześnie wśród zespołów, które pracują najbliżej tworzonego produktu (użytkownicy biznesowi, programiści) zaobserwować można brak poczucia współodpowiedzialności za finalny produkt. Pracownicy są bowiem przyzwyczajeni do ciągłej kontroli przez kierownika strumienia i niechętnie podejmują własne inicjatywy, które wykraczają poza sformalizowany zakres obowiązków.

Częstym problemem w projektach obejmujących zakresem zmiany IT są również relacje z dostawcami oprogramowania. Jeżeli programiści znajdują się w innej lokalizacji niż, na przykład, użytkownicy biznesowi banku, utrudniona jest komunikacja pomiędzy nimi. Brak częstej i łatwej komunikacji sprawia natomiast, że jakość dostarczanego oprogramowania jest niezadowalająca – nie wszystkie wymagania biznesowe są zrealizowane zgodnie z oczekiwaniami biznesu, występuje dość dużo błędów. Ponieważ za przeprowadzenie

wcześniejszych analiz odpowiadały inne osoby niż te, które dostarczają samo oprogramowanie, powstaje szerokie pole do przerzucania odpowiedzialności w przypadku problemów.

Szczególnie trudne są jednak relacje pomiędzy uczestnikami biznesowymi a pracownikami IT. Obie strony mają tendencję do obwiniania się wzajemnie za trudności i niepowodzenia związane z wdrażaniem aplikacji. Zespoły przyzwyczajone są do pracy w swoich obszarach i po wykonaniu swojej części zadania uznawania jej za skończoną.

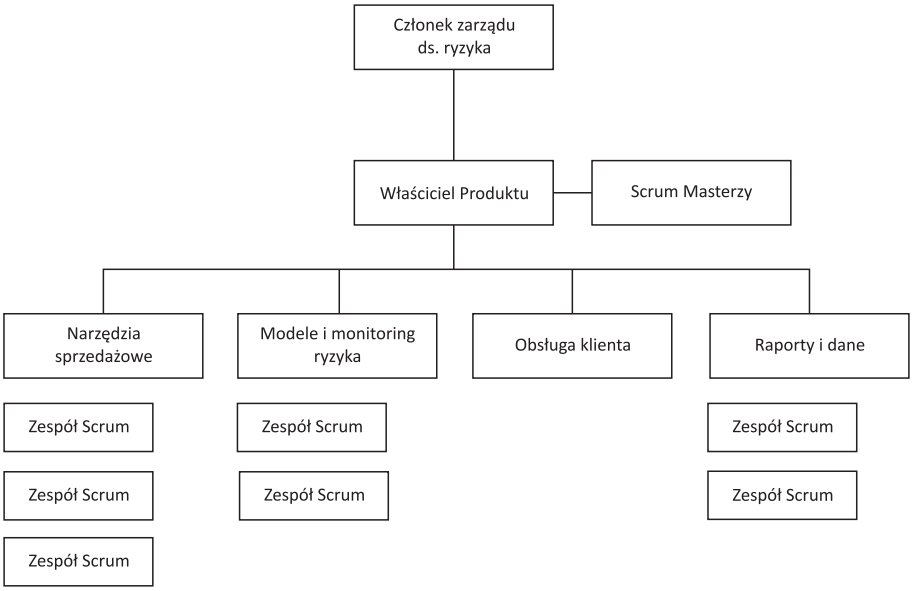
Program IT zarządzany zwinnie

Jak wspomnieliśmy, wprowadzenie metod zwinnych nie zlikwiduje w magiczny sposób wszystkich narzutów związanych z wprowadzeniem programu – w przypadku powiązanych ze sobą projektów konieczna jest wymiana informacji i koordynacja prac (np. uzgadnianie sposobu integracji).

Koszty, których można uniknąć w zwinnej strukturze organizacyjnej, obejmują koszt niepotrzebnego raportowania i koordynacji przez role niewnoszące wartości w rozwój produktu (tradycyjne PMO). Ze względu na rezygnację ze sztywnych faz projektów zmniejszają się koszty wynikające z inercji akceptacji dokumentacji przez użytkowników biznesowych oraz koszty wprowadzania zmian na dalszych etapach projektu – w podejściu zwinnym zmiany są czymś oczekiwanym.

Zarządzanie zwinne w większej skali wymaga modyfikacji podejścia znanego z pojedynczego projektu. Znane metodyki stosowane w tym celu to między innymi SAFe (Scaled Agile Framework), oraz LeSS (Large Scale Scrum), promowany przez Craiga Larmana. W naszym przykładzie trzymamy się linii LeSS, która przekłada zasady zwinne na większą skalę starając się minimalizować niezbędne zmiany formalne w podejściu. Na poziomie ideologii, inspirowanej *lean*, obie szkoły są niemal zbieżne, natomiast porównanie szczegółów podejścia to temat na oddzielną rozprawę.

Rysunek 2.
Struktura przykładowego programu w metodyce zwinnej



Podstawową rolą w podejściu zwinnym pełni Właściciel Produktu. Wywodzi się on z biznesu, który będzie odbiorcą nowych lub zmienionych aplikacji i procesów. Podejmuje bieżące decyzje co do priorytetów i kierunku rozwoju produktu. Jego rola obejmuje dualizm tradycyjnego programu, w którym oddzielny manager odpowiada za „zarządzanie" programem, komunikując się ze stojącym obok właścicielem biznesowym. W przypadku naszego programu Właścicielem byłby dyrektor odpowiedzialny za obszar ryzyka.

Ponieważ piszemy o dużym programie w przeciwieństwie do pojedynczego projektu, musimy zaadresować fakt, że jeden Właściciel Produktu nie będzie w stanie pełnić swojej roli dla całego programu. Idąc za LeSS, za poszczególne części produktu powinni wtedy odpowiadać Właściciele Obszarów Produktu, którzy będą bezpośrednio współpracować z zespołami.

Drugą istotną zmianą są interdyscyplinarne i samoorganizujące się zespoły. Zespoły Scrum powinny posiadać wszystkie niezbędne kompetencje (analityczne, architektoniczne, programistyczne, testerskie, projektowania UX itd.), aby samodzielnie tworzyć swoje obszary produktu. Każdy zespół wspierany jest przez Scrum Mastera (na przykład pochodzącego z IT), którego zadaniem

jest ułatwianie pracy zespołu poprzez usuwanie pojawiających się przeszkód (np. brak informacji, licencji itp.) i dbanie o poprawność stosowania zasad Scrum.

Zespół Scrum (wraz z Właścicielem Produktu lub Właścicielem Obszaru Produktu) posiada pełną odpowiedzialność za tworzony produkt. Oznacza to, że zespół taki nie posiada kierownika projektu, który rozlicza poszczególnych członków zespołu z wykonanych zadań. Jedną z podstawowych zasad Scrum jest samoorganizowanie się zespołu, co z jednej strony zwiększa motywację i poczucie odpowiedzialności za tworzony produkt, z drugiej jednak jest jednym z najtrudniejszych aspektów Scrum.

Dzięki interdyscyplinarnym zespołom zmniejsza się dystans pomiędzy pracownikami pochodzącymi z biznesu, IT i dostawcami zewnętrznymi, co znacznie ułatwia komunikację i szybkie reagowanie na ewentualne problemy. Zespoły Scrum pracują w krótkich (dwu-, trzy- lub czterotygodniowych) iteracjach, na koniec których prezentują efekty prac Właścicielowi Produktu. Ma on więc okazję na bieżąco śledzić rozwój produktu oraz na wczesnym etapie przekazać uwagi, jeśli produkt odbiega od oczekiwań.

Zwiększenie aktywnej komunikacji w zespole oraz przyspieszenie dostarczania ukończonych części produktu sprawia, że zespoły są w stanie zrealizować więcej funkcjonalności, niż ma to miejsce w podejściu kaskadowym. Krótkie iteracje pozwalają też na bardziej dynamiczne dostosowywanie realizowanego zakresu do aktualnych potrzeb biznesowych.

Planowanie prac na bieżąco wymaga również ciągłego przeglądu priorytetów realizowanych funkcjonalności, dzięki czemu tworzone jest tylko to, co na chwilę obecną jest niezbędne z punktu widzenia biznesu. Pozwala to na uniknięcie tworzenia funkcjonalności „na przyszłość", których utrzymanie jest kosztowne ze względu, na przykład, na konieczność aktualizowania wersji i utrzymywania dokumentacji.

Kierowanie bez kierowników i raportów

Taka organizacja projektu wymaga jednak zaakceptowania przez organizację pewnych zmian. Przede wszystkim, jest to zgoda kierownictwa na przeniesienie kontroli nad postępem tworzenia produktu na niższe poziomy: Właściciela Produktu, Właścicieli Obszarów Produktu i zespoły. Dotychczasową formę kontroli pracowników, polegającą na analizowaniu danych z raportów, ocen

okresowych itp., zastępują bezpośrednie interakcje Właściciela Produktu z zespołami, zgodnie z zasadą „Go See" wywodzącą się z praktyk zarządzania *lean*.

Rola menedżerów i kierowników w Scrum nie występuje. Stają się oni Właścicielami Produktu, Właścicielami Obszarów Produktu, Scrum Masterami lub ekspertami merytorycznymi. Ich zadaniem nie jest już rozliczanie pracowników z wykonanych zadań, lecz aktywne uczestniczenie w tworzeniu produktu we właściwej dla siebie roli.

Podobnie „role" programistów, analityków i testerów zamieniają się w członków zespołu, którzy reprezentują określone profile kompetencji. Nie mogą jednak dłużej używać wymówki swojego „zakresu obowiązków" do unikania podejmowania zadań popychających projekt do przodu.

Wbrew opiniom o tym, że podejście zwinne zakłada mniejszą dyscyplinę prowadzenia projektów, tak naprawdę wymagana jest wyższa dyscyplina niż w podejściu kaskadowym, w tym dbanie o stały rytmu pracy i utrzymywanie w dobrym stanie najważniejszych narzędzi, takich jak Rejestr Produktu.

W Scrum każda iteracja, zwana sprintem, trwa określoną liczbę tygodni i, co do zasady, jej długość nie zmienia się. Każdy sprint rozpoczyna się planowaniem, na którym tworzony jest rejestr sprintu, zawierający zadania do wykonania przez zespół do zakończenia iteracji. Na koniec sprintu zespoły przeprowadzają prezentację stworzonego produktu oraz retrospekcję, czyli wspólną analizą sposobu pracy zespołu oraz próbę jej doskonalenia. W trakcie sprintu zespół planuje pracę co 24 godziny na codziennych spotkaniach, zwanych Daily Scrum. Utrzymywany jest rejestr produktu, określający zakres wymagań zarówno funkcjonalnych, jak i niefunkcjonalnych, który jest na bieżąco aktualizowany i uzupełniany przez Właściciela Produktu (lub Właścicieli Obszarów Produktu).

Podejmując decyzję o stosowaniu Scrum organizacja powinna liczyć się z tym, że wymagana przez to podejście dyscyplina zajmuje czas pracowników. Niemniej, prawidłowo przebiegające spotkania w Scrum angażują wszystkich jego uczestników, a zespół nie ma poczucia, że są one nadmiarowe i powodują przestoje w pracy.

Wszyscy pracownicy muszą zaangażować się w zmianę

Podejście zwinne wymaga transformacji całej organizacji projektowej. Korzyści nie będą mogły być osiągnięte, jeśli dotychczasowa struktura projektów

czy programów zostanie utrzymana, a zmienią się tylko nazwy ról poszczególnych pracowników. Niezbędna jest zmiana mentalności zarówno zarządu, menedżerów, jak i zespołów. Dlatego tak ważne są intensywne szkolenia i coaching, szczególnie na początku pracy w podejściu zwinnym. Za dbałość o przestrzeganie zasad Scrum odpowiadają Scrum Masterzy, którzy powinni mieć odpowiednią wiedzę, doświadczenie i umiejętności uczenia innych.

Należy się liczyć z tym, że nie wszyscy pracownicy banku, którzy przez lata pracowali w strukturze silosowej, będą skłonni poddać się tak głębokim zmianom i przestawić się z myślenia o swojej pracy jako o wąskim wycinku obowiązków na poczucie współodpowiedzialności za cały produkt. Dobór odpowiednich osób do zespołów, chętnych do rozwoju i adaptowania zmian, jest kolejnym kluczowym czynnikiem powodzenia w zmianie podejścia projektowego.

Pilotaż vs. zmiana całej organizacji

Częstym pytaniem zadawanym przez osoby zainteresowane podejściem zwinnym jest sposób rozpoczęcia takiej inicjatywy. Nie istnieje jednak uniwersalna metoda. Ścieżka, którą wybierze bank, powinna być decyzją strategiczną i zależeć od gotowości zarządu do wprowadzenia i aktywnego wspierania zmiany, obszaru działalności banku, który ma być objęta transformacją, skłonności banku do podejmowania ryzyka oraz wielu innych czynników.

Jednym ze sposobów rozpoczęcia budowy podejścia zwinnego w organizacji jest wybranie jednego lub kilku projektów, które będą prowadzone w ten sposób. Taki pilotaż pozwala wąskiej grupie osób zbudować wiedzę i umiejętności oraz przekonać się o korzyściach, jakie przynosi realizowanie projektów w podejściu zwinnym. Osoby te mogą potem rozszerzać dobre praktyki na całą organizację i wspierać mniej doświadczone zespoły.

Rozpoczęcie wdrażania podejścia zwinnego od niedużych i, w miarę możliwości, wyizolowanych inicjatyw pozwala też na identyfikację, jakie przeszkody specyficzne dla działalności danej organizacji należy brać pod uwagę przy późniejszej budowie ram i planu transformacji całej firmy.

Pierwsze sukcesy mogą pomóc przekonać do tej metody bardziej sceptycznych menedżerów, dlatego dobry start z metodykami zwinnymi jest niezwykle istotny w organizacji. Ze względu na to, że projekty prowadzone w podejściu zwinnym nie wymagają dużych nakładów na rozpoczęcie, a iteracje są krótkie i kończą się prezentacją produktu, pilotaż przeprowadzony na wybranych

projektach daje możliwość szybkiej i taniej weryfikacji, czy organizacja jest gotowa na większe zmiany procesowe i kulturowe.

Innym pomysłem na przeprowadzenie takiej zmiany jest podejście całościowe, czyli pełna transformacja struktury portfela projektów banku. Podejście to będzie miało szanse powodzenia tylko wtedy, jeśli zarząd i menedżerowie wyższego szczebla udzielą mu silnego poparcia od samego początku inicjatywy. Istotne jest, aby kierownictwo miało głębokie zrozumienie zasad podejścia zwinnego, a także kosztów i korzyści, jakie się z nim wiążą.

Wdrażanie metod zwinnych na szerszą skalę pozwala na stosowanie od początku prawidłowych zasad, bez tworzenia pośrednich rozwiązań, które mogą być potrzebne wtedy, gdy tylko niewielka część projektów działa w podejściu zwinnym. Rozwiązania pośrednie, które z założenia powinny być tymczasowe, utrwalają się w organizacji, a ich zmiana jest trudna i czasochłonna. Poza tym, próby modyfikacji zasad podejścia zwinnego i dostosowywania ich do istniejących formalności w organizacji mogą doprowadzić do budowania skomplikowanych metodyk, które zupełnie odbiegają od idei upraszczania pracy oraz mogą zniechęcić organizację do dalszego inwestowania we wdrażanie potrzebnych zmian.

Aleksander P. Czarnowski

Prezes AVET Information and Network Security sp. z o.o., spółki zajmującej się od 17 lat konsultingiem w zakresie bezpieczeństwa informacji w Polsce, Rumunii, Holandii i Wielkiej Brytanii oraz na Ukrainie i Słowacji. Członek Komisji Technicznej 182, która w Polskim Komitecie Normalizacyjnym odpowiada za rodzinę standardów ISO 27000, a także rady programowej Zakładu Systemów Jakości i Zarządzania działającego w ramach Wojskowej Akademii Technicznej. Od 2013 r. ekspert w grupie eksperckiej odpowiedzialnej za kontraktowanie usług cloud computingu dla sektora SMB przy Komisji Europejskiej, gdzie odpowiada m.in. za zagadnienia związane z dostępnością i ciągłością działania. Wieloletni autor i wykładowca, doskonale znany czytelnikom magazynu i uczestnikom konferencji Virus Bulletin.

Aleksander P. Czarnowski, AVET

Obecne zagrożenia w bankowych systemach IT

Publikacje na temat bezpieczeństwa IT mają jedną przykrą cechę: niezwykle szybko się starzeją, a często za tym idzie także ich merytoryczna dewaluacja. Z jednej strony od publikacji poprzedniej wersji tego artykułu minął zaledwie rok, jednak z perspektywy technologii to aż rok. Co więcej, gdy powstawała pierwsza wersja, nowa Rekomendacja D KNF nie weszła jeszcze w życie. Jesteśmy więc bogatsi nie tylko o doświadczenia wynikające z nowych technik ataku, ale także z procesu kompleksowego wdrażania nowych wymogów bezpieczeństwa w bankach.

Z drugiej strony – pomimo postępu technologicznego i zmian legislacyjnych – mamy do czynienia z pewną niezmiennością. To co z pewnością nie zmieniło się przez ostatni rok, to nacisk na mobilność, dostępność i *end user experience*. Oczywiście każdy z powyższych atrybutów wymaga adekwatnych mechanizmów kontrolnych. Bez efektywnych zabezpieczeń, nie da się dzisiaj zbudować konkurencyjnego produktu na rynku finansowym.

Rekomendacja D: obecna rzeczywistość

Relatywnie krótkie okno czasowe na wprowadzenie zaleceń nowej rekomendacji D z pewnością miało wpływ na sposób implementacji zabezpieczeń w bankach. Nie każdy zdążył z pełną implementacją na czas. Efektem ubocznym, w niektórych przypadkach, był brak adekwatnych analiz. Wielu sprzedawców systemów SIEM lansowało na przykład pogląd, że rekomendacja D wymaga tej klasy systemu. W rzeczywistości taki system jest wymagany jeśli analiza banku wskaże potrzebę jego wdrożenia.

Wprowadzenie pojęcia *cloud computingu* przyniosło w mojej ocenie kilka dobrych zmian, takich jak na przykład budowa elastycznych środowisk testowych w modelu chmury prywatnej lub publicznej. Do tej pory budowa

środowisk testowych o podobnych parametrach co środowiska produkcyjnego była trudnym tematem z perspektywy... finansowej. Tymczasem model rozliczenia *on-demand* na podstawie zużytych faktycznie zasobów, takich jak moc obliczeniowa, przepustowość czy *storage* pozwala budować w miarę tanio nawet rozległe środowiska testowe.

Z jednej strony, jednoznaczne zdefiniowanie terminu *cloud computingu* w rekomendacji D zawęziło potencjalną ofertą zewnętrznych dostawców, co jest pozytywnym efektem, ponieważ dzisiaj praktycznie każdy dostawca, niezależnie od swojej wielkości i specjalizacji, oferuje „chmurę", która niekoniecznie ma cokolwiek wspólnego z tym pojęciem. Co więcej, rekomendacja D określa także część wymogów bezpieczeństwa stawianych przed dostawcą i jego usługą. Niestety, to co zostało pominięte przy tej okazji to wprowadzenie przynajmniej podziału na chmurę prywatną i publiczną. Model prywatny rządzi się innymi prawami z perspektywy np. legislacji i dlatego warto byłoby go uwzględnić. Innym obszarem niezwykle istotnym jest kwestia audytu i kontroli środowiska – w przypadku chmury prywatnej wiele zapisów z umowy SLA nie występuje w porównaniu z chmurą publiczną. Oczywiście istnieje wiele punktów wspólnych dla obu modeli – np. tzw. *cloud lock-in* (zwany także *vendor lock-in*) czyli problem eksportu/transferu danych do innego środowiska/dostawcy w przypadku zakończenia korzystania z aktualnie używanej chmury.

Rozpatrując kwestie modelu chmury z perspektywy polskiego rynku usług IT dla banków należy także wziąć pod uwagę fakt, że niektóre banki w swojej grupie kapitałowej posiadają wyspecjalizowane spółki IT, które dostarczają lub mogą dostarczyć usługę typu *cloud computing*. W takim przypadku należy sobie odpowiedzieć na pytanie, czy chmura udostępniana przez spółkę, której w 100% udziałowcem jest bank i która jest udostępniana tylko na jego potrzeby jest rozwiązaniem publicznym czy prywatnym. Odpowiedź wcale nie musi być oczywista – w końcu z perspektywy prawa usługę świadczy zewnętrzny podmiot. Z drugiej strony zdarza się, że usługa jest świadczona na... środowisku IT, którego właścicielem jest bank. Podobne scenariusze można mnożyć praktycznie do woli.

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.

Biorąc pod uwagę rosnącą liczbę elektronicznych środków płatności, które nie są kartami płatniczymi w rozumienie standardu PCI DSS, należy zadać sobie pytanie, czy nie jesteśmy świadkami zmierzchu tego standardu a zarazem tradycyjnej karty płatniczej. Nawet gdy ograniczymy się tylko do rodzimego rynku, od 2014 roku można wskazać co najmniej kilka dużych projektów związanych z elektronicznymi środkami płatności, w których uczestniczą banki, a w których standard PCI DSS (ani jego pochodna dla producentów rozwiązań płatniczych PA DSS) nie ma zastosowania.

ISO/IEC 27001

Rekomendacja D czy PCI DSS to przykłady standardów i regulacji dedykowanych dla sektora finansowego. Z kolei standard ISO/IEC 27001, wywodzący 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. Elastyczność, podejście procesowe oraz zarządzanie ryzykiem będące integralną częścią tego standardu z pewnością przyczyniło się do jego globalnego zaadaptowania przez sektor bankowy. Warto zauważyć, że wiele zabezpieczeń opisanych w ramach ISO/IEC 27001 ma swoje odzwierciedlenie w rekomendacji D KNF.

W 2013 roku pojawiła się nowa wersja standardu ISO/IEC 27001:2013, która zmieniła w istotny sposób zakres dokumentacji koniecznej do certyfikacji, w tym na przykład tzw. Deklarację stosowania (SOA– *Statement Of Applicability*) względem wersji z 2007 roku. Należy zauważyć, że dokonane zmiany nie

są rewolucją, lecz ewolucją. Oznacza to, że podstawowe, wysokopoziomowe założenia standardu nie uległy zmianie, i oprócz wskazanej powyżej charakterystyki, nadal organizacja stosująca tą normę posiada dowolność w doborze zabezpieczeń, jak i w sposobie ich implementacji. Brak zrozumienia tych zasad to zresztą jeden z najczęściej popełnianych błędów przez organizacje starające się uzyskać zgodność.

Co w takim razie się zmieniło?

Już na pierwszy rzut oka widać, że układ rozdziałów części głównej normy. Nie bazuje on, jak poprzednio, na cyklu PDCA, lecz na układzie treści, który został przyjęty dla wszystkich norm wprowadzających systemy zarządzania (tych istniejących, jak i tych które powstaną w przyszłości). Nie oznacza to jednak, że podejście procesowe zostało skreślone – wręcz przeciwnie. Efektywne zarządzanie bezpieczeństwem nie jest możliwe w innym modelu.

W konsekwencji zmian treści w normie ISO/IEC 27002:2013, stanowiącej zbiór zaleceń do ISO/IEC 27001, modyfikacji uległa lista sugerowanych mechanizmów kontrolnych (zabezpieczeń) oraz w pewnym stopniu ich nazewnictwo, co wpływa na zawartość SOA.

Kolejna istotna różnica występuje w obszarze zarządzania ryzykiem. Obecna wersja standardu wskazuje ISO 31000 jako podstawę do budowania efektywnego procesu zarządzania ryzykiem w organizacji, zamiast dotychczas używanej normy ISO/IEC 27005. Jest to zmiana dyskusyjna, która zwiększa liczbę strategii postępowania z ryzykiem z 4 do 7 wprowadzając pojęcie „szansy" („ryzyka pozytywnego"). Jest to ułatwienie dla organizacji, ale jednocześnie utrudnienie dla audytorów, przyzwyczajonych do uwzględniania w analizie ryzyka takich aspektów jak prawdopodobieństwo zagrożeń, siła zabezpieczeń, podatności i wpływy. To także utrudnia mapowanie wyników np. ze skanerów zabezpieczeń czy manualnych testów penetracyjnych na proces analizy ryzyka. Co więcej, wiele organizacji wdrażając wcześniejsze wersje standardu ISO/IEC 27001 niekoniecznie kierowało się wszystkimi wytycznymi normy ISO/IEC 27005. W konsekwencji organizacje te – w tym także banki – posiadają proces analizy ryzyka w obszarze ISMS, który może wymagać adaptacji w kontekście nowych zapisów.

Ważne zmiany dotyczą także zarządzania ciągłością działania – niewątpliwie kluczowego obszaru z perspektywy banku. Nowa wersja standardu praktycznie zostawia kluczowe elementy BCM/DRP innym normom, koncentrując się tylko na aspektach bezpieczeństwa informacji w ciągłości działania.

Można więc powiedzieć, że nastąpiło „rozluźnienie" względem starszych wersji normy, choć w praktyce zapisy dla tej części standardu zawsze były bardzo wysokopoziomowe.

Kolejną ważną zmianą jest brak możliwości certyfikacji od 2015 roku na bazie wersji standardu z 2007. Oznacza to, że organizacje które rozpoczęły proces wdrażania ISO 27001:2007 muszą dokonać aktualizacji przed rozpoczęciem procesu certyfikacji.

Omawiając zmiany jakie zaszły w ramach standardu ISO/IEC 27001 nie można także pominąć relatywnie nowych norm z rodziny 27000 w kontekście bezpieczeństwa chmury:

- ISO 27017 „Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services" – opisuje wymagania dotyczące zabezpieczeń chmury z perspektywy dostawcy, jak i klienta,
- ISO 27018:2014 „Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors" – opisuje wymagania w obrębie ochrony danych osobowych oraz prywatności w chmurze.

Należy zwrócić uwagę, że legislacja w wielu krajach zmierza w kierunku akceptacji zgodności z wymogami prawa w przypadku, gdy dostawca chmury przetwarza dane zgodnie z ISO 27018.

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

W tym miejscu warto wspomnieć o debacie jaka toczy się od pewnego czasu, także na poziomie Komisji Europejskiej, w zakresie listy lokalizacji centrów przetwarzania danych, które są częścią określonej usługi w chmurze. Wielu dostawców stoi na stanowisku, że lista lokalizacji jest zbędna lub wręcz niemożliwa do przedstawienia ponieważ dane mogą być przetwarzane równolegle w wielu lokalizacjach naraz lub być w ciągłym tranzycie pomiędzy nimi. Z perspektywy sektora finansowego, takie rozwiązanie jest w praktyce nie do przyjęcia z kilku powodów:

- lista lokalizacji musi być znana z przyczyn legislacyjnych – np. w obszarze ochrony danych osobowych,
- lista lokalizacji musi być znana z przyczyn kontrolnych i nadzoru – jak ocenić bezpieczeństwo fizyczne nieznanych lokalizacji,
- transgraniczny eksport danych i informacji może być także problemem legislacyjnym.

Innym powiązanym zagadnieniem z danymi w tranzycie jest problem bezpiecznego usuwania danych. Dane powinny zostać usunięte w sposób uniemożliwiający ich odtworzenie w każdej instancji i lokalizacji. Sytuacja, w której dane w tranzycie nie podlegają usunięciu jest z perspektywy prawnej w sektorze bankowym niedopuszczalna. Dlatego niezwykle istotne jest posiadanie adekwatnej umowy *SLA*, regulującej te jak i inne zagadnienia. Dodatkowo, w przypadku chmury publicznej, z perspektywy bezpieczeństwa niezwykle istotna jest lista lokalizacji, gdzie dane są przetwarzane. Należy w tym miejscu zwrócić uwagę na fakt, iż jeśli dostawca posiada tylko jedną lokalizację trudno mówić o jego rozwiązaniu jako pracującym w chmurze. U podstaw koncepcji chmury leży przecież zapewnienie wysokiej dostępności oraz niezawodności. Trudno o spełnienie takich postulatów dysponując tylko jedną lokalizacją. Przy okazji brak dodatkowej lokalizacji może być niezgodny zarówno z sektorowymi, jak i właścicielskimi wymogami.

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 on przystosowany do pracy w takim modelu.

Bankowość mobilna

Dzisiaj bankowość mobilna to najważniejszy kanał dostępowy z perspektywy rozwoju. Pojawienie się smartfonów oraz tabletów zmieniło 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 poziom bezpieczeństwa fizycznego 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.

Na szczęście rozwój technologii trochę zmienił rynek tych urządzeń – dzisiaj na przykład standardowa dystrybucja systemu Android posiada rozszerzenie SELinux, które jeszcze do niedawna było spotykane w instalacjach systemów Linux na serwerach. SELinux pozwala na separację procesów oraz granularną kontrolę nad uprawnieniami, znacznie bardziej rozbudowaną niż w tradycyjnym systemie Linux. Efektem tego jest możliwość obniżania uprawnień aplikacjom, co w przypadku ich penetracji np. na skutek błędu w ich kodzie ogranicza zasięg ataku.

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 postrzegane z perspektywy jego właściciela. Zaimplementowane zabezpieczenia mają zapewnić mu stały przychód i kontrolę nad użytkownikami oraz developerami. 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

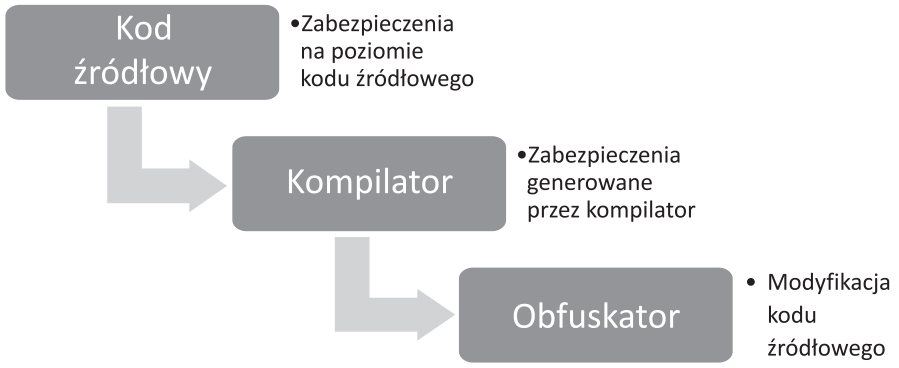
mogły funkcjonować efektywnie, muszą być rozumiane i świadomie stosowane przez developerów. Aplikacje „bezpieczne przez przypadek" nie istnieją. W końcu każdą opcję można „niechcący" wyłączyć, nie zdając sobie sprawy z konsekwencji dla docelowego modelu bezpieczeństwa.

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.

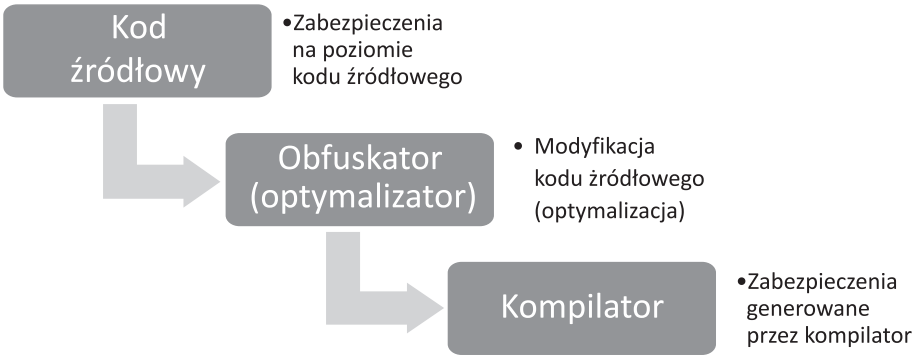
Rys. 1 przedstawia uproszczony proces tworzenia aplikacji mobilnej:

- 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.

Rysunek 1.
Typowy uproszczony proces produkcji aplikacji



Rysunek 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 obfuscatorów 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 do kodów źródłowych, gdyż prawdziwi atakujący, w przeciwieństwie do

1 Dla uproszczenia przyjmujemy, że na proces kompilacji składa się kompilacja, konsolidacja i ewentualne podpisanie aplikacji. W przypadku aplikacji mobilnych znajdują się one wraz ze wszystkimi potrzebnymi plikami 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

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

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.

W zeszłym roku mieliśmy do czynienia z zakończeniem wsparcia dla Windows XP (zakończyło się ono 14 kwietnia 2014 roku). 14 lipca 2015 roku kończy się z kolei wsparcie dla Windows 2003 Server. Dla banku brak po tym terminie poprawek i nowych service pack'ów od producenta może stanowić problem nie tylko w kontekście bezpieczeństwa, ale także zgodności z rekomendacją D.

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.

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 stosowaną 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.

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 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[5] tworzącego BIOS – było dodanie możliwości jego modyfikacji poprzez umieszczenie go w pamięci flash. Oznaczało

5 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 przestrzenia adresowej x86 oraz potrzeby zachowania wstecznej kompatybilności.

to nie tylko możliwość skasowania go i uczynienia systemu nieużywalnym (co próbował robić wirus CIH, znany także jako Czarnobyl), ale przede wszystkim jego nieautoryzowaną modyfikacją. 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 których się uruchamia jest... uruchomienie docelowego systemu operacyjnego.

W ramach inicjalizacji sprzętu UEFI wykonuje inicjalizację m.in.:

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

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[6]. 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. 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. Warto zauważyć, że w przypadku mechanizmu OPTION ROM niektóre BIOSy stosują zabezpieczenia starające się ograniczyć ten wektor ataku. Przykładem może być np. implementacja emulatora procesora x86 w pakiecie coreboot (opcja *Secure Mode* w *Option ROM Execution type*). Zastosowanie emulatora do uruchomienia kodu nie pozwala np. na instalację hypervisora lub modułu SMM przez

6 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.

fałszywy lub zainfekowany ROM. Efektem ubocznym jest wolniejszy start systemu, jednak w wielu przypadkach ten problem jest pomijalny.

Jeśli wszystko powyższe wydaje się być fantazją lub wybieganiem w przyszłość, to z przykrością należy stwierdzić, że opisane wektory ataku są wykorzystywane w realnym świecie coraz powszechniej. Na początku 2015 roku ujawniono, że National Security Agency instalowała zmodyfikowany firmware w dyskach twardych niektórych producentów. Dzięki temu oprogramowanie szpiegujące startowało zanim kontrolę przejmował system operacyjny oraz oprogramowanie antywirusowe i szyfrujące dane. Należy zwrócić uwagę, że infekcje lub umyślne modyfikowanie *firmware'u* już na etapie produkcji sprzętu komputerowego może oznaczać, że nie ma możliwości usunąć zagrożenia z poziomu systemu operacyjnego. W praktyce usunięcie jest możliwe tylko poprzez wymianę zainfekowanego komponentu lub całego urządzenia.

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) lub korzystają z rozwiązań dostarczanych przez zewnętrznych dostawców. Nie zmienia to wcale faktu, że o końcowym poziomie bezpieczeństwa systemu bankowości elektronicznej decyduje także środowiska wykonania aplikacji. Kwestie związane z bezpieczeństwem aplikacji webowych zostały omówione w dalszej części.

Na środowiska 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 aplikacja 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 2015 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 kwartału 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. Tego typu błędy są dzisiaj aktywnie wykorzystywane także przez złośliwe oprogramowanie. Przykłady takiego wykorzystania zostały opisane w dalszej części.

Kolejnym istotnym zagadnieniem jest fakt, że kilka 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.

Przykłady ataków z użyciem złośliwego oprogramowania

Wraz z rozwojem zabezpieczeń po stronie użytkownika jak i systemów bankowości elektronicznej następuje ewolucja złośliwego oprogramowania. W ciągu ostatniego roku mieliśmy kilka przykładów zmasowanych ataków na konkretne systemy bankowości elektronicznej. Oznacza to, że myślenie, iż produkty ograniczone do wybranych rynków nie są lub nie będą atakowane przez złośliwe oprogramowanie, nie ma i nigdy nie miało racji bytu. Drugim ważnym

faktem jest to, że każde nowe zabezpieczenia po stronie systemu bankowości elektronicznej powoduje jego próbę obejścia lub neutralizacji. Oznacza to, że zabezpieczenia muszą ewoluować razem ze złośliwym oprogramowaniem i wykorzystywanymi metodami ataku. Tutaj pojawia się – lansowana przez kilku dostawców – pokusa korzystania z rozwiązań bazujących na analizie i przewidywaniu. Chodzi o rozwiązania typu *threat intelligence* i pochodne. Praktyka pokazuje zgoła inny obraz: nikt nie jest w stanie przewidzieć dokładnie ataku. Nie oznacza to, że bank musi pozostać bezbronny: efektywny, wielowarstwowy model zabezpieczeń w połączeniu z odpowiednimi procedurami oraz treningiem personelu pozwala skutecznie się bronić.

Jedną z popularnych w 2014 roku metod ataku na systemy bankowości elektronicznej była próba nieautoryzowanej zmiany numeru rachunku w przelewach zdefiniowanych. Otóż nie każdy system domyślnie wymaga autoryzacji takiej operacji. Co więcej niektóre systemy dają możliwość wyłączenia przez użytkownika autoryzacji zmiany numery rachunku. Złośliwe oprogramowanie potrafi taką „funkcjonalność" idealnie wykorzystać. Oczywiście nie jest to jedyna wykorzystywana metoda. Jednak obrazuje ona, że złośliwe oprogramowanie coraz częściej posiada wiedzę na temat konkretnych aplikacji, które próbuje atakować. Do innych popularnych metod ataku można także zaliczyć metody stosowane przez złośliwe oprogramowanie z rodziny VBKlip. Idea jest prosta – podmiana rachunku następuje w momencie kopiowania ze schowka (ang. *clipboard*) systemu Windows prawdziwego numeru rachunku na inny. Okazuje się, że sporo użytkowników posługuje się schowkiem do wpisywania danych w formularzy operacji przelewu. VBKlip 2.0 nie wykorzystuje już schowka do podmiany numery rachunku. W zamian za to, po instalacji w systemie, przeszukuje on listę procesów systemu Windows, aby odnaleźć przeglądarkę internetową. Jeśli *malware* znajdzie taki proces, rozpoczyna przeszukanie jego przestrzeni adresowej w poszukiwaniu 26 znakowego ciągu cyfr (ciąg może zawierać spacje). Jeśli ciąg zostanie odnaleziony w przestrzeni adresowej procesu, następuje jego podmiana na inny – pobrany z serwera C&C.

Opisane powyżej przypadki są dobrze udokumentowane, więc publicznie znane. Tymczasem w skali roku mamy też do czynienia z rosnącą liczbą ataków za pomocą dedykowanego złośliwego oprogramowania na systemy bankowe. Ataki te często są na tyle ograniczone do wybranego banku lub grupy klientów, że standardowe oprogramowanie antywirusowe nawet 12 miesięcy po odkryciu *malware'u* nie wykrywa go. Nie można więc oprzeć

strategii bezpieczeństwa tylko na rozwiązaniach antywirusowych – potrzebna jest, co zresztą już wcześniej zaznaczono, wielowarstwowość zabezpieczeń. W tym miejscu także objawia się kolejna wada rozwiązań *threat intelligence*. Do udanego ataku nie zawsze potrzebny jest efekt skali wywołany masowość zdarzenia. Bez odpowiedniej np. liczby infekcji lub innych incydentów modele oparte o statystyki i analizę/korelację zdarzeń są kompletnie bezradne.

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 aplikacja 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

Aktualizacja rekomendacji D ma duży wpływ na zabezpieczenia stosowane w bankach działających na licencji KNF. Niewątpliwie otwarcie się na outsourcing i cloud computing jest dobrym kierunkiem, pozwalającym obniżać koszty IT przy jednoczesnym zapewnieniu wymaganego poziomu bezpieczeństwa. Nie oznacza to jednak, że w obszarze bezpieczeństwa zrobiono już wszystko i można spocząć na laurach. Rosnąca liczba fraudów, jak i zaawansowanych ataków jawnie takiemu stwierdzeniu przeczy.

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. Na szczęście w przypadku aplikacji mobilnych dostęp do kodu źródłowego jest mniej istotny i posiadając odpowiednie doświadczenie oraz narzędzia można szybko i sprawnie dokonać ich oceny pod kątem bezpieczeństwa.

Podziękowania

Chciałbym podziękować zespołowi AVET Information and Network Security, z którym mam przyjemność pracować od wielu lat.

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 kilkuset 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 Bankow Polskich „Cloud computing 2013". Autor publikacji „Aspekty prawne cloud computingu w odniesieniu do sektora bankowego (regulacje EU)" (2014).Współautor analizy wykonalności wdrożenia *cloud computingu* w administracji publicznej w Polsce (2014). Jest także wykładowcą studiów podyplomowych Szkoły Głównej Handlowej „Zastosowanie technologii cloud computingu w modelowaniu biznesowym".

Joanna Gałajda

Prawnik w zespole IT i Transakcji handlowych w warszawskim biurze Bird & Bird. Główny obszar jej zainteresowań zawodowych stanowią zagadnienia związane z cyberbezpieczeństwem oraz *cloud computingiem*, w szczególności wykorzystanie rozwiązań cloudowych w instytucjach finansowych oraz ochrona danych osobowych w chmurze. Współautorka wielu artykułów z tego obszaru.

Pracuje dla klientów z sektora IT, finansowego oraz ubezpieczeniowego. Doradzała w sporach związanych z wdrażaniem dużych projektów IT.

Uczestniczyła w licznych konferencjach poświęconych *cloud computingowi*, ochronie danych osobowych oraz cyberbezpieczeństwu.

Maciej Gawroński, Joanna Gałajda, Bird & Bird

Aktualne trendy regulacji technologii bankowych

W obecnej edycji „Wyzwań informatyki bankowej", aby nie powtarzać znaczącej części zeszłorocznego tekstu, postanowiłem zamieścić, wraz ze współautorką, nieco szerszy przegląd regulacji, które w opinii mojej i moich kolegów z Bird & Bird będą miały wpływ na sposób, w jaki banki będą korzystały z technologii.

1. Nowelizacja ustawy o ochronie danych osobowych

1 stycznia 2015 roku weszły w życie istotne zmiany ustawy o ochronie danych osobowych („uodo"). Ułatwiono tzw. eksport danych, czyli przekazywanie danych osobowych do państwa trzeciego, które nie zapewnia odpowiedniego poziomu ochrony danych osobowych; zmieniono również istotnie rolę Administratora Bezpieczeństwa Informacji („ABI").

Międzynarodowe transfery danych. Nowelizacja ustawy zniosła dotychczasowy obowiązek uzyskania zgody Generalnego Inspektora Ochrony Danych Osobowych (GIODO) na transfer danych do państwa niezapewniającego adekwatnej ochrony, jeżeli eksporter i importer zawrą umowę opartą na Standardowych Klauzulach Umownych UE.

Standardowe Klauzule Umowne to zatwierdzone przez Komisję Europejską wzorce klauzul umownych określających prawa i obowiązki eksportera oraz importera danych osobowych. Dotychczas Komisja przyjęła dwa rodzaje SCC (ang. *Standard Contractual Clauses*): pomiędzy administratorem danych a przetwarzającym (ang. *Controller to Processor, C2P*) oraz pomiędzy administratorem danych a administratorem danych (ang. *Controller to Controller, C2C*). W opracowaniu są SCC dla relacji pomiędzy przetwarzającym a podprzetwarzającym (ang. *Processor to Processor, P2P*), które mogą być szczególnie istotne na przykład dla dostawców globalnych usług przetwarzania chmurowego.

Projekt SCC P2P opracowany przez Grupę Robocza Artykułu 29 (czyli rzeczników ochrony danych osobowych Krajów Członkowskich Unii Europejskiej) miałem okazję konsultować na zaproszenie GIODO. Rekomendowałem wtedy wprowadzenie postanowień dotyczących przenoszalności danych (ang. *data portability*), czyli tematu, za którego opracowanie byłem współodpowiedzialny w Grupie Ekspertów Komisji Europejskiej ds. Umów Przetwarzania Chmurowego (ang. *European Commission Expert Group on Cloud Computing Contracts*). Jakie będą losy projektu i moich rekomendacji, czas pokaże.

Na zmianie przepisów skorzystają zapewne korporacje międzynarodowe, które nie będą musiały ubiegać się o zgodę GIODO przy wprowadzaniu nowych produktów lub usług IT wymagających przekazywania danych osobowych do państwa trzeciego.

Ze zwolnienia z konieczności uzyskania zgody Generalnego Inspektora mogą teoretycznie skorzystać też banki, które chciałyby sięgnąć po najświeższe lub najbardziej zaawansowane usługi informatyczne dostępne na globalnym rynku. Należy pamiętać jednak, że na przeszkodzie mogą stanąć polskie przepisy dotyczące outsourcingu, a w szczególności zakaz ograniczania odpowiedzialności głównego outsourcera w outsourcingu bankowym lub niekiedy brak konkretnych regulacji dotyczących podoutsourcingu. Nie zawsze przepisy staną na przeszkodzie skorzystaniu z takich usług, na pewno jednak konieczna będzie szczegółowa analiza konkretnego przypadku.

Wiążące Reguły Korporacyjne. Do tej pory ustawa o ochronie danych osobowych nie regulowała wprost wiążących reguł korporacyjnych (ang. *Binding Corporate Rules*, *BCR*). Wiążące Reguły Korporacyjne to jakby regulamin ochrony danych osobowych międzynarodowej grupy kapitałowej, który po zatwierdzeniu przez europejskich rzeczników ochrony danych osobowych umożliwia transfer danych w ramach grupy niezależnie od położenia spółek z tej grupy, tak jakby wszystkie znajdowały się na terenie Unii Europejskiej. W praktyce Generalny Inspektor wydawał zgody na transfer danych na podstawie BCR. Nowelizacja zawiera nową podstawę prawną upoważniającą GIODO do zatwierdzania BCR jako podstawy do transferu danych w ramach tej samej organizacji w państwie trzecim nieposiadającym odpowiedniego poziomu ochrony.

Niektóre międzynarodowe korporacje obecne w Polsce, w tym znany bank, skorzystały z możliwości wdrożenia Wiążących Reguł Korporacyjnych. Narzędzie to może ułatwiać na przykład korzystanie z wewnątrzgrupowych centrów informatycznych położonych poza terytorium UE – a więc – inaczej to nazywając, z globalnej prywatnej chmury obliczeniowej.

Zainteresowanie polskich podmiotów tym specyficznym instrumentem prawnym może wzrosnąć dzięki temu, że ujęto go bezpośrednio w polskich przepisach ochrony danych osobowych. Szczególnie zainteresowane mogą być polskie firmy, w tym instytucje finansowe, które dokonują ekspansji na wschód – poza teren Unii Europejskiej.

Administrator Bezpieczeństwa Informacji

Nowelizacja ustawy o ochronie danych osobowych wprowadza zmianę dotyczącą powoływania i roli Administratora Bezpieczeństwa Informacji („ABI") przez administratora danych.

Zgodnie z nowymi przepisami organizacje będą mogły bądź powołać ABI i zgłosić go do GIODO, bądź nie wyznaczać ABI w ogóle. Wyznaczenie ABI przez daną organizację (administratora danych) zwolni tę organizację z obowiązku rejestracji zbiorów danych. Jest ot pewne udogodnienie. Jednak warto zastanowić się, czy gra jest warta świeczki, zważywszy, że powołanie ABI rodzi też nowe obowiązki.

Według nowych przepisów ABI będzie zobowiązany do zapewnienia zgodności organizacji z prawem ochrony danych osobowych, między innymi poprzez: (i) sprawdzanie zgodności przetwarzania danych osobowych z przepisami ustawy o ochronie danych osobowych oraz przygotowanie sprawozdania dla administratorów/przetwarzających; (ii) nadzorowanie, opracowywanie i aktualizowanie obowiązkowej dokumentacji dotyczącej zabezpieczenia danych; (iii) zapewnienie zapoznania się osób upoważnionych do przetwarzania danych z przepisami uodo; (iv) prowadzenie przez ABI rejestru informacji o zbiorach danych.

Jednak to następujące nowe obowiązki administratora bezpieczeństwa informacji wywołują wiele obaw: (i) możliwość nałożenia przez GIODO obowiązku przeprowadzenia przez ABI wewnętrznego „audytu" ochrony danych osobowych i przekazania sprawozdania z audytu do GIODO; (ii) obowiązek ABI informowania w formie sprawozdań administratora danych osobowych o stanie ochrony danych osobowych w organizacji.

Wyznaczenie ABI przez organizację będzie sygnałem dla kontrahentów, że dana organizacja zapewnia wysoki poziom ochrony danych osobowych. Z drugiej strony, mnogość nowych obowiązków ABI, w tym obowiązki związane z periodyczną weryfikacją zgodności organizacji z przepisami o ochronie danych osobowych, dokumentowaniem wyników takiej weryfikacji, prawem GIODO do dostępu do takiej dokumentacji, związane z tym koszty bieżące

oraz ryzyka mogą skutecznie „odstraszyć" nie tylko małych i średnich przedsiębiorców, ale i duże organizacje.

Znawcy prawa ochrony danych osobowych wyrażają też niepokój co do ryzyka odpowiedzialności karnej administratora bezpieczeństwa informacji[1]. Wszystko to powoduje, że w prywatnych organizacjach, w tym tych dużych z sektora finansowego pojawiła się tendencja do rezygnacji z wyznaczania administratora bezpieczeństwa informacji na korzyść powołania „Specjalisty" lub „Głównego Specjalisty ds. ochrony danych osobowych".

2. Nowe Rozporządzenie UE

Obecnie w Parlamencie Europejskim trwają prace nad projektem ogólnego rozporządzenia UE o ochronie danych osobowych[2] ("Rozporządzenie UE"). Wejście w życie Rozporządzenia UE planowane jest na rok 2017/2018. Podstawowe zasady ochrony danych, które będą wprowadzone Rozporządzeniem UE, opisaliśmy w pierwszej edycji „Wyzwań informatyki bankowej". Ostatnia wersja Rozporządzenia UE została opublikowana przez Komisję w grudniu 2014 r.

Poniżej przedstawiamy najnowszą wersję zapisów Rozporządzenia UE mających znaczenie dla chmury obliczeniowej.

- **Analiza wpływu** (***data protection impact assessment***). Administrator danych będzie zobowiązany przeprowadzić przed przetwarzaniem danych osobowych ocenę wpływu przetwarzania danych na zakres ich ochrony. Oceny skutków w zakresie ochrony danych administrator musi dokonać, jeśli operacje przetwarzania danych, w szczególności przetwarzanie z wykorzystaniem nowych technologii, stwarzają szczególne ryzyko dla praw i wolności podmiotów danych z racji swego charakteru, zakresu lub jeżeli cele przetwarzania mogą wiązać się z wysokim ryzykiem dla praw i wolności osób fizycznych, takich jak dyskryminacja, kradzież tożsamości, oszustwo, straty finansowe, szkody dla reputacji (naruszenie pseudonimowości), utrata poufności danych chronionych tajemnicą zawodową lub inną niekorzystną sytuacją gospodarczą lub społeczną.

---

1 Patrz: http://prawo.rp.pl/artykul/1174998.html – artykuł dr Pawła Litwińskiego w dzienniku Rzeczpospolita z dnia 28 stycznia 2015 roku pt. „Być albo nie być – admiratorem".

2 Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych).

- **Ochrony prywatności na etapie projektowania oraz ochrona prywatności jako wartość domyślna** *(privacy by design and privacy by default***).** Administrator danych powinien uwzględnić ochronę danych już w fazie projektowania (*privacy by design*) oraz chronić dane jako opcję domyślną (*privacy by default*). Administrator będzie zobowiązany podjąć odpowiednie środki techniczne oraz organizacyjne odpowiednie do przetwarzania danych oraz celów przetwarzania (w tym minimalizację i pseudonimizację danych), biorąc pod uwagę dostępną technologię oraz koszty realizacji oraz uwzględniając charakter, zakres, kontekst i cel przetwarzania, a także prawdopodobieństwo wystąpienia i nasilenia zagrożeń dla praw i wolności osób fizycznych związane z przetwarzaniem. Wdrożenie odpowiednich środków technicznych i organizacyjnych powinno odpowiadać wymogom Rozporządzenia i zapewniać ochronę prywatności. Proces powinien rozpoczynać się już w fazie projektowania np. nowej usługi cloud computingu a także w trakcie procesu.
- **Przenoszalność danych** *(data portability).* W najnowszej wersji projektu został usunięty zapis o prawie podmiotu danych do uzyskania od administratora kopii danych w przyjętym i użytecznym formacie. Zmiana ta ma istotne znaczenie z punktu widzenia instytucji finansowych, działających jako przetwarzający dane. Należałoby się zastanowić, czy w takim wypadku instytucje finansowe nie powinny wypracować systemu umożliwiającego dostarczanie na prośbę swoich klientów kopii ich danych osobowych.

Przenoszalność danych jest jednym z istotniejszych zagadnień z punktu widzenia kontroli nad danymi przekazywanymi do chmur obliczeniowych oraz zaufania do rynku cloud computingu i jako takie jest przedmiotem zainteresowania Komisji Europejskiej. Zagadnienie to omawialiśmy w ramach prac Grupy Ekspertów Komisji Europejskiej ds. Umów Cloud Computingowych, gdzie przygotowałem rekomendacje przepisów lub najlepszych praktyk w tym zakresie.

- **Zawiadomienie o naruszeniu (***data breach notification***)**. W przypadku naruszenia bezpieczeństwa danych osobowych, administrator będzie zobowiązany powiadomić nadzorujący go organ ochrony danych o naruszeniu oraz o okolicznościach naruszenia w przeciągu 72 godz. Jeżeli nie będzie możliwe dostarczenie informacji o okolicznościach naruszenia w przeciągu 72 godz., administrator będzie zobowiązany zrobić to niezwłocznie po uzyskaniu takich informacji. Jeśli może dojść do naruszenia prywatności konkretnej osoby, administrator powinien także niezwłocznie powiadomić tę osobę, ale tylko w przypadku naruszeń o istotnym wpływie na

ochronę danych. W nowym projekcie, jako naruszenie o istotnym wpływie na ochronę danych podano naruszenie pseudonimizacji (*breach of pseudonymity*). Został również zmieniony katalog okoliczności, kiedy administrator nie ma obowiązku informowania o naruszeniu danych. Jako takie okoliczności wprowadzono sytuację, kiedy naruszałoby to ważny interes publiczny oraz kiedy wiązałoby się to z nieproporcjonalnym nakładem.

- **Współadministratorzy.** Rozporządzenie dopuszcza instytucję współadministratorów (*joint controllers*). W przypadku wspólnego określenia przez dwóch administratorów celów 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.
- **Kary.** W Rozporządzeniu przewidziano możliwość nałożenia kary pieniężnej przez organy nadzorcze na podmiot naruszający. W ostatnim projekcie Rozporządzenia nie określono jednak jeszcze szczegółowych wartości kar. Wiadomo jedynie, że będzie to wartość procentowa od obrotu światowego. Znamienne jest usunięcie z projektu zapisu o możliwości wystosowania przez organ nadzorczy listu ostrzegawczego w przypadku pierwszego nieumyślnego naruszenia oraz nałożenia obowiązku przeprowadzenia regularnych audytów.

3. Cybersecurity

Zagadnienie cybersecurity coraz częściej znajduje się w centrum zainteresowania regulatorów. Powstaje coraz więcej dokumentów dotyczących strategii cyberbezpieczeństwa narodowego i tego, w jaki sposób powinno być ono budowane i oceniane. Obecnie wiele krajów podjęło współpracę w celu zwiększenia bezpieczeństwa w cyberprzestrzeni. W styczniu 2015 r. Stany Zjednoczone i Wielka Brytania ogłosiły plan wzmożonej współpracy w zakresie cyberbezpieczeństwa. Zakres współpracy obejmuje: poprawę infrastruktury krytycznej, wzmocnienie współpracy w zakresie obrony przed atakami cybernetycznymi oraz wspieranie badań naukowych dotyczących cyberbezpieczeństwa.

Prace regulacyjne w Unii Europejskiej i Stanach Zjednoczonych

Unia Europejska. 7 lutego 2013 r. został wydany wspólny komunikat Komisji Europejskiej do Parlamentu Europejskiego, Rady Europejskiej, Komitetu

Ekonomiczno-Społecznego i Komitetu Regionów o nazwie Strategia bezpieczeństwa cybernetycznego Unii Europejskiej („Strategia"). Celem Strategii jest m.in. upowszechnienie usług elektronicznych, w tym cloud computingu. Częścią Strategii jest projekt Dyrektywy w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii („Dyrektywa"), nad którym trwają obecnie prace w Komisji Europejskiej. Przyjęcie Dyrektywy planowane jest na rok 2015, z kolei wejście w życie na rok 2017. Obowiązki określone w Dyrektywie będą mieć wymiar zarówno krajowy, jak i międzynarodowy. Zgodnie z projektem, państwa członkowskie będą zobligowane do przyjęcia narodowych strategii dotyczących cyberbezpieczeństwa, ustanowienia odpowiednich organów nadzoru nad bezpieczeństwem systemów informatycznych (national competent authority „NCA") oraz do utworzenia komputerowego zespołu szybkiego reagowania na naruszenie bezpieczeństwa systemów informatycznych. Na poziomie międzynarodowym dyrektywa nakłada obowiązek współpracy pomiędzy Komisją a NCA, przekazywanie wczesnych ostrzeżeń o pojawiających się zagrożeniach przez Komisję lub NCA oraz uzgodnienie wspólnych działań w zakresie pojawiających się zagrożeń.

Z perspektywy instytucji finansowych istotne jest, to, że znalazły się one w kręgu operatorów rynkowych objętych szczególnymi obowiązkami. Zarówno organy administracji publicznej, jak i operatorzy w określonych krytycznych sektorach (kluczowe usługi świadczone drogą elektroniczną, energetyka, transport, bankowość, infrastruktura rynków finansowych oraz służba zdrowia) będą zobowiązane do dokonywania oceny zagrożeń, na jakie są narażone oraz do przyjęcia odpowiednich środków mających na celu zapewnienie bezpieczeństwa sieci telekomunikacyjnych i przetwarzanych w nich informacji. Podmioty te będą również zobowiązane do zgłaszania właściwym organom wszelkich incydentów zagrażających sieciom telekomunikacyjnym i systemom informatycznym oraz mogących znacząco zakłócić ciągłość krytycznych usług i dostaw towarów. Informacje o incydentach będą również musiały być podawane do publicznej wiadomości, a zarówno organy administracji, jak i operatorzy będą zobligowani do poddawanie się audytowi w zakresie bezpieczeństwa sieci telekomunikacyjnej i systemów informatycznych.

Celem obu dokumentów jest wzmocnienie poziomu ochrony cybernetycznej na rynku europejskim, co może podnieść jego atrakcyjność. Nowe regulacje wzmocnią zaufanie wobec usług cyfrowych, co umożliwi ich pełniejsze wykorzystanie przez obywateli, jak i sektor prywatny oraz publiczny.

Stany Zjednoczone. Również w Stanach Zjednoczonych podjęto wzmożone prace nad regulacjami dotyczącymi cyberbezpieczeństwa. 12 stycznia 2015 r. prezydent Barack Obama przedstawił propozycję dokumentu *The Personal Data Notification and Protection Act*, w którym określone zostały ogólnokrajowe zasady dotyczące notyfikacji o naruszeniu danych osobowych. Dokument m.in. nakłada na organizacje obowiązek notyfikacji o naruszeniu w przeciągu 30 dni. Zawiadomienie powinno być skierowane zarówno do osoby, której dane dotyczą, jak i ogłoszone w mediach. Ogłoszenie o naruszeniu w mediach powinno nastąpić w przypadku, gdy naruszone zostały dane ponad 5 tys. osób w danym stanie.

W lutym 2015 r. National Institution of Standards and Technology ("NIST") opublikował dokument *Wytyczne dotyczące cyberbezpieczeństwa* (NIST Cybersecurity Framework), który jest zbiorem najlepszych praktyk w zakresie zapewnienia bezpieczeństwa cybernetycznego w organizacjach. Implementacja wytycznych NIST jest dobrowolna, jednakże można oczekiwać, że ich przyjęcie będzie zalecane lub nawet nakazane organizacjom, które przechowują wrażliwe dane klienckie bądź dane poufne.

Działania Białego Domu w zakresie cyberbezpieczeństwa są odpowiedzią na coraz częstsze ataki cybernetyczne, takie jak chociażby na Sony Pictures w listopadzie 2014 r., czy na bank JP Morgan Chase, który spowodował utratę poufności danych ponad 80 milionów klientów. Amerykański sektor finansowy jest szczególnie narażony na ataki cybernetyczne. W związku z tym niebezpieczeństwem Federalna Komisja Nadzoru nad Instytucjami Finansowymi (The Federal Financial Institutions Examination Council – FFIEC) stworzyła Grupę Roboczą do spraw związanych z cyberbezpieczeństwem i infrastrukturą krytyczną (Cybersecurity and Critical Infrastructure Working Group) w celu zwiększenia współpracy w zakresie cyberbezpieczeństwa pomiędzy poszczególnymi instytucjami sektora finansowego.

Zalecenia dla organizacji w zakresie cyberbezpieczeństwa

Powstaje pytanie, jakie działania powinny podjąć organizacje, aby uniknąć lub przynajmniej zminimalizować groźby ataków cybernetycznych. Takimi działaniami może być np. wprowadzenie systemu monitorowania oprogramowania, regularne przeprowadzanie ocen ryzyka, odpowiednie zabezpieczenie dostępu do systemu przez osoby nieuprawnione, przeprowadzanie odpowiednich szkoleń wśród pracowników w zakresie cyberbezpieczeństwa, ustanowienie odpowiedniego zespołu do spraw cyberbezpieczeństwa. Jednym

z ważniejszych zaleceń dla organizacji jest stworzenie odpowiedniego systemu nadzoru pracowników. Z ostatnich danych jasno wynika, że największy odsetek ataków cybernetycznych to tzw. *ataki insiderskie*, a więc takie, których źródłem jest personel wewnętrzny organizacji. Należy wdrożyć takie mechanizmy kontroli, które wyeliminują ryzyko przeprowadzenie ataku przez pracownika.

4. Nowe standardy dla cloud computingu

W ostatnim czasie powstało kilka nowych standardów istotnych z punktu widzenie dostawców usług cloudowych. Komisja Europejska opracowała w tym zakresie dwa dokumenty: Code of conduct for cloud service providers (”Code of conduct”) oraz Cloud Service Level Agreement Standardisation Guidelines (”SLA”). Z kolei ISO wydało najnowszy standard ISO/IEC 27018:2014 Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (”ISO 27018”).

Code of conduct. Cloud Select Industry Group opracowała w ostatnim czasie Code of Conduct dla dostawców usług chmurowych. Celem kodeksu było wypracowanie ujednoliconego modelu stosowania przepisów o ochronie danych osobowych. Kodeks jest zbiorem obowiązków dostawców chmury jako przetwarzających dane osobowe i ma umożliwić klientom chmury łatwiejszy wybór dostawców.

Code of Conduct w założeniu ma być stosowany dobrowolnie i możliwe są odstępstwa od niego wraz z ich wyjaśnieniami. Code of conduct został opracowany w dużej mierze przy udziale przedstawicieli usług SaaS i budzi kontrowersje dostawców usług IaaS. Jakie będą jego dalsze losy, zobaczymy.

Cloud Service Level Agreement. Założeniem twórców SLA (Cloud Select Industry Group) było stworzenie uniwersalnych mierników usług cloudowych. W rezultacie bolesnego i długotrwałego procesu powstał dokument o wysokim stopniu ogólności. W moim osobistym odczuciu – średnio przydatny. Wśród kolegów i znawców zagadnień cloud computingu znam również entuzjastów tego dokumentu.

ISO/IEC 27018:2014. Nowa norma ISO 27018 jest uzupełnieniem dwóch poprzednich norm ISO/IEC 27002 (Code of pratice for information security control) oraz ISO/IEC 29100 (Privacy Framework). Jest to pierwszy standard, który bezpośrednio skupia się na zapewnieniu bezpieczeństwa danych w chmurze.

Przedmiotem standardu ISO 27018 jest wprost ochrona danych osobowych (dokładnie tłumacząc: informacji, które mogą zostać powiązane z konkretną osobą) w chmurach obliczeniowych działających jako przetwarzający dane osobowe. Jego istotność dla cloud computingu jest więc oczywista.

Standard ten adresuje sporo istotnych zagadnień, które wywołują wątpliwości przy przetwarzaniu danych osobowych w chmurach obliczeniowych. Określa on podstawowe rodzaje środków bezpieczeństwa, które powinni przyjąć dostawcy chmury, w tym szyfrowanie i kontrolę dostępu. Wydaje się on bardzo przydatnym narzędziem do określenia *par excellence* standardu ochrony danych osobowych w chmurach obliczeniowych. Wdrożenie ISO 27018 przez dostawców zapewni większe bezpieczeństwo danych w chmurze, co może przyczynić się do ogólnego wzrostu zaufania organizacji do usług cloudowych.

W lutym 2015 r. Microsoft, jako pierwsza firma na świecie, uzyskał certyfikat ISO 27018. Zapewne w najbliższym czasie więcej organizacji zdecyduje się na podobny krok.

5. Zmiana regulacji outsourcingu w usługach finansowych

Outsourcing – zakaz ograniczania odpowiedzialności

Zakaz ograniczania odpowiedzialności outsourcerów spotykamy w Polskim Prawie Bankowym oraz w przepisach ustawy o funduszach inwestycyjnych i o obrocie instrumentami finansowymi (w obu tych ustawach zakaz nie dotyczy outsourcingu nieistotnego).

Podobny zakaz ograniczenia odpowiedzialności dostawcy nie pojawia się w żadnej zachodniej regulacji. Przepisy unijne nie zezwalają instytucjom finansowym na powołanie się na outsourcing dla zwolnienia się z odpowiedzialności. Polski ustawodawca „bankowy" twórczo rozszerzył ten wymóg na dostawców sektora. Chytrość, jaką wykazał się tutaj polski ustawodawca, jest jednak w naszej opinii krótkowzroczna. Zakaz ograniczenia odpowiedzialności outsourcera stoi na przeszkodzie pełnego wykorzystania usług cloud computingowych przez polski sektor bankowy. Globalna kultura prawna usług informatycznych opiera się na założeniu ograniczonej odpowiedzialności.

Zamiast zakładać pełną odpowiedzialność dostawcy chmury, tworzącą iluzoryczne poczucie bezpieczeństwa po stronie banku, należałoby raczej skupić się na zapewnieniu bezpieczeństwa operacyjnego dla procesu powierzonego takiemu dostawcy (chmurze) i przewidzeniu planu alternatywnego na

wypadek utraty ciągłości działania dostawcy. Na nic bankowi bowiem będzie odszkodowanie a już tym bardziej doprowadzenie do upadłości swojego dostawcy – nie zrekompensuje to a wręcz dodatkowo nadszarpnie reputację banku, która jest jego głównym kapitałem.

Podoutsourcing – dopuszczalność i regulacja

Outsourcing został uregulowany w Prawie Bankowym w 2004 r. Wraz z uregulowaniem outsourcingu pojawiły się wątpliwości co do dopuszczalności podoutsourcingu. Doprowadziło to do tworzenia skomplikowanych struktur tzw. outsourcingu gwiaździstego. Co gorsza, w związku z zakazem ograniczeń odpowiedzialności outsourcerów drastycznie utrudniło i przedłużyło to proces zawierania tego typu umów.

Dopiero po nowelizacji Prawa Bankowego w 2011 roku podoutsourcing został uregulowany ustawowo. Obecnie nie może on obejmować całości świadczeń objętych umową a dodatkowo powinien być bądź przewidziany w umowie outsourcingowej oraz bank powinien wyrazić na piśmie zgodę na konkretne podzlecenie, bądź może nastąpić incydentalnie dla odwrócenie skutków katastrofy lub innego przypadku siły wyższej.

Inne ustawy sektorowe nie regulują podoutsourcingu wprost. Z chwilą gdy w Prawie Bankowym uregulowano podoutsourcing, prawnicy z sąsiednich subsektorów dostrzegli u siebie lukę i zaczęło dominować przekonanie o tym, że w tych podsektorach podoutsourcing nie jest dozwolony. Rodzi to spore problemy interpretacyjne i analityczne przy „wtłaczaniu" poszczególnych usług cloudowych w ramy przepisów. Czasami się to udaje, a czasami nie.

Podsumowanie

Nie ma odwrotu od informatyzacji i usieciowienia usług finansowych. Postęp technologiczny zwiększa możliwości dostarczania takich usług, zwiększa tempo i wygodę ale i rodzi ryzyka, indywidualne i systemowe. Zarówno rzeczywistość, jak i regulatorzy stawiają przed bankami kolejne wyzwania z obszaru rzeczywistości cyfrowej.

W naszej ocenie obecny gorset przepisów Prawa bankowego i ustaw regulujących pozostałe podsektory finansowe (np. ubezpieczenia, fundusze inwestycyjne) utrudnia zwinne i odpowiednie dostosowywanie się banków do postępującej rzeczywistości cyfrowej. Ograniczenia dotykające korzystanie przez banki z dostawców technologii w istocie utrudniają odpowiadanie na

zagrożenia bezpieczeństwa operacyjnego. Banki i ich dostawcy muszą koncentrować się na ryzyku współpracy bardziej niż na ryzykach, którym ta współpraca ma zapobiegać. Przykładem jest tu np. coraz częstsze oferowanie cyberbezpieczeństwa jako usługi chmurowej. Gdy dostawca takiej usługi monitoruje internet i w swojej infrastrukturze chmurowej gromadzi, przetwarza i reaguje na zagrożenia pojawiające się i dotykające społeczność jego klientów. Globalni dostawcy takich usług (a te usługi z natury swoje mają charakter globalny) nie chcą naginać się do – jak je widzą – lokalnych oczekiwań prawa polskiego w zakresie odpowiedzialności czy struktury organizacyjnej swojej usługi. Mając silną pozycję rynkową i oferując wysokiej jakości usługę wolą odciąć niszowy rynek niż narażać się na jak to widzą ryzyko egzotycznego prawa.

Banki tracą też w wyścigu o klienta np. z firmami pożyczkowymi. Te ostatnie, nie będąc krępowane żadnymi szczególnymi regulacjami, potrafią w szybszy sposób i dotrzeć do klienta i ocenić ryzyko klienta, w tym z użyciem takich narzędzi jak weryfikacja profilu w sieciach społecznościowych.

Wydaje się, że nastał czas, w którym regulacje dotyczące korzystania z technologii i usług technologicznych przez firmy z sektora finansowego powinny zostać poluzowane lub – raczej – urealnione. Sektor finansowy obecnie jest świadomy ryzyka technologicznego i ryzyka operacyjnego i mitygowanie tych właśnie ryzyk wymaga bardziej elastycznych ram prawnych.

Rafał Burzyński

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.

Anna Baryła

Absolwentka prawa na Uniwersytecie Warszawskim, autorka pracy magisterskiej poświęconej tematyce stosowania FATCA w polskim porządku prawnym.

Jako konsultantka w KPMG Tax M. Michna sp. k. zajmuje się wdrażaniem FATCA i CSR w polskich instytucjach finansowych, w szczególności projektowaniem procesów i procedur niezbędnych dla implementacji powyższych regulacji, analizą prawną możliwych w tym zakresie rozwiązań, a także przeprowadzaniem szkoleń z zakresu FATCA i CRS. Specjalizuje się także w doradztwie podatkowym dla podmiotów z sektora finansowego w zakresie CIT, VAT i cen transferowych.

Rafał Burzyński, Tomasz Rzepa, Anna Baryła, KPMG

Common Reporting Standard

W ostatnim okresie byliśmy świadkami bezprecedensowej aktywności społeczności międzynarodowej w zakresie walki ze zjawiskiem uchylania się od opodatkowania. Szczególnie eksploatowanym narzędziem w tym zakresie jest automatyczna wymiana informacji podatkowych, która, w odróżnieniu od wymiany spontanicznej czy wymiany na wniosek, polega na cyklicznym i systematycznym przekazywaniu danych dotyczących różnych kategorii dochodu podatnika pomiędzy państwem źródła a państwem rezydencji[1].

Pierwszym przedsięwzięciem wykorzystującym automatyczną wymianę informacji na niespotykaną dotąd skalę był amerykański akt prawny, powszechnie znany pod nazwą FATCA (*Foreign Account Tax Compliance Act*). W Polsce implementacja obowiązków wynikających z FATCA nastąpiła[2] w formie podpisanej w dniu 7 października 2014 r. Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie poprawy wypełniania międzynarodowych obowiązków podatkowych oraz wdrożenia ustawodawstwa FATCA (dalej: Umowa IGA)[3]. Dostosowanie się do przepisów wskazanej umowy okazało się dla instytucji polskiego sektora bankowego skomplikowanym i kosztownym przedsięwzięciem, wpływającym na relacje z klientami, obowiązujące w bankach procedury i systemy informatyczne.

---

1 S. Merle, S. Hemkar, K. Dautrich-Reynolds, *The global harmonization of exchange of information*, International Tax Review, Tom 25, nr 3, s. 3.

2 Należy zaznaczyć, iż komentowana umowa międzynarodowa implementująca FATCA nie stanowi, w chwili pisania niniejszych słów, obowiązującego prawa w Polsce. Przedmiotowa umowa została podpisana przez rząd Rzeczypospolitej Polskiej, jednakże nie została jeszcze ratyfikowana i opublikowana w Dzienniku Ustaw.

3 Dostępna: http://www.finanse.mf.gov.pl/documents/766655/10779436/FATCA.pdf, data dostępu: 26.02.2015 r.

Mechanizm gromadzenia i wymiany informacji opracowany w ramach FATCA, chociaż z jednej strony spotkał się z ogromną falą krytyki ze względu na istotne obciążenia, jakie nakłada zarówno na podmioty sektora prywatnego, jak i na administrację publiczną, został wykorzystany do opracowania regulacji *Common Reporting Standard* (CRS)[4], która już w najbliższej przyszłości stanie się kolejnym wyzwaniem dla polskich instytucji finansowych. CRS, chociaż wyraźnie inspirowany umowami międzyrządowymi implementującymi FATCA[5], istotnie odróżnia się tym, że w założeniu ma mieć ogólnoświatowy charakter.

Fakt, że już 52 kraje, w tym Polska, podpisały wielostronne porozumienie, w którym zobowiązały się do wdrożenia CRS już od 1 stycznia 2016 r. wskazuje, iż automatyczna wymiana informacji podatkowych może wkrótce objąć większość państw świata[6].

Historia CRS i aktualny stan prawny

W kwietniu 2013 r. państwa należące od G5 (tj. Francja, Niemcy, Włochy, Hiszpania i Wielka Brytania) zainicjowały pilotażowy projekt automatycznej wymiany informacji podatkowej mający na celu zwiększenie wykrywalności i przeciwdziałanie oszustwom podatkowym. Państwa te wezwały pozostałych członków Unii Europejskiej do przyłączenia się do programu, a jednym z pierwszych państw, które na to wezwanie odpowiedziało, była Polska[7]. Autorzy wskazanej inicjatywy nie ukrywali, że jest ona inspirowana regulacją FATCA. Podkreślano jednocześnie, iż społeczność międzynarodowa stanęła przed niepowtarzalną okazją do przejścia od modelu wymiany informacji w oparciu o umowy dwustronne, jak miało to miejsce w ramach FATCA, do

4 Standard for Automatic Exchange of Financial Account Information – Common Reporting Standard, dostępny: http://www.oecd.org/ctp/exchange-of-tax-information/automatic-exchange-financial-account-information-common-reporting-standard.pdf, data dostępu: 26.02.2015 r.

5 Przez umowy implementujące FATCA rozumie się tu Model 1 Umowy międzyrządowej o poprawie międzynarodowej zgodności podatkowej i implementacji FATCA, dostępną: http://www.treasury.gov/resource-center/tax-policy/treaties/Pages/FATCA.aspx, data dostępu: 26.02.2015 r.

6 Wskazane porozumienie zostało podpisane 29 października 2014 r., co potwierdza komunikat na portalu internetowym OECD: http://www.oecd.org/tax/exchange-of-tax-information/multilateral-competent-authority-agreement.ht, data dostępu: 26.02.2015 r.

7 Źródło: http://biznes.pap.pl/pl/news/search/info/13801340,polska-jako-1-kraj-regionu-przylaczyla-sie-do-g5-ws-podatkow-rostowsk, data dostępu: 26.02.2015 r.

opracowania rozwiązania globalnego. Uważano, iż jedno, wielostronne narzędzie, jako alternatywa dla wielu konkurujących ze sobą podstaw do wymiany informacji, pozwoli na zminimalizowanie zjawiska fragmentaryczności otrzymywanych informacji, występowania luk prawnych, a także znacząco obniży koszty implementacji zarówno dla administracji jak i dla sektora prywatnego[8]. Prace w ramach powyższej inicjatywy odbywały się następnie na forum G8 i G20, by ostatecznie to OECD zostało wyposażone w mandat do prac nad jednym, wielostronnym standardem wymiany informacji. W efekcie na szczycie G20 w Sydney, który odbył się w dniach 22–23 lutego 2014 r., OECD przedstawiło projekt *Common Reporting Standard* oraz modelowego porozumienia (*Competent Authority Agreement*, CAA), które miało stać się podstawą do wdrożenia CRS w poszczególnych państwach. 29 października 2014 r. 52 kraje, w tym Polska, podpisały *Competent Authority Agreement* w którym zobowiązały się do wdrożenia CRS od 1 stycznia 2016 r.[9] Chociaż CRS wymaga jeszcze implementacji do polskiego prawa, wskazany planowany termin wejścia w życie CRS oznacza, iż już od 1 stycznia 2016 r. instytucje finansowe w Polsce będą zobowiązane do rozpoczęcia procedury identyfikacji klientów, natomiast do końca roku 2016 będą musiały zakończyć przegląd niektórych rodzajów rachunków. Data pierwszej wymiany informacji (raportowania) została zaplanowana na 30 września 2017 roku. Krótki okres czasu, jaki pozostał do wdrożenia wymogów CRS oznacza, iż polskie instytucje finansowe powinny już w chwili obecnej podjąć kroki w celu zmodyfikowania wewnętrznych procesów, procesów, dokumentacji wydawanej klientom oraz systemów informatycznych, aby być przygotowanym na wypełnianie nowych obowiązków od 1 stycznia 2016 r.

Ogólna charakterystyka CRS

CRS zakłada, iż instytucje finansowe z państw, które do niego przystąpiły wdrożą określone w nim procedury weryfikacji klientów, a dane zidentyfikowanych przy ich użyciu podmiotów przekażą za pośrednictwem krajowych organów administracyjnych do kraju rezydencji podatkowej tych podmiotów.

8 Statement on the pilot multilateral automatic information exchange facility, dostępne: https://www.gov.uk/government/publications/statement-on-the-pilot-multilateral-automatic-information-exchange-facility, data dostępu: 26.02.2015 r.

9 Podpisana przez Ministra Finansów CAA dostępna: http://www.mf.gov.pl/documents/764034/1161631/Poland_Signing_Package+rev1.pdf, dostęp: 26.02.2015 r.

Zakresem podmiotowym CRS, podobnie jak miało to miejsce w ramach Umowy IGA, zostały objęte następujące typy instytucji finansowych:

- instytucja powiernicza (*Custodial Institution*),
- instytucja depozytowa (*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 CRS definiują każdy podmiot, który przyjmuje depozyty w toku prowadzonej działalności bankowej lub działalności podobnej. Podmiot inwestycyjny został zdefiniowany jako 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 lub umowy typu *annuities* (umowy renty) albo jest zobligowany do dokonywania płatności w zakresie takich umów[10].

Wymaga podkreślenia, iż w przypadku, gdy organ administracji, który otrzyma dane podlegające raportowaniu, stwierdzi ich niekompletność lub niepoprawność powinien powiadomić o tym fakcie właściwą władzę z kraju siedziby instytucji finansowej, która przekazała błędne lub niepełne dane. Władza ta będzie zobowiązana do *„podjęcia wszystkich niezbędnych działań i środków przewidzianych prawem krajowym zmierzających do usunięcia tych błędów lub niezgodności*[11]. W przeciwieństwie do FATCA, CRS nie przewiduje koncepcji poboru podatku w związku z niezgodnością z przepisami CRS lub od płatności do instytucji z państw, które nie przystąpiły do CRS. Powyższe

10 CRS, Załącznik, Art. VIII.

11 CRS, s. 16.

rozwiązanie wzbudza uzasadnione wątpliwości wobec faktu, iż zachęca instytucje finansowej do przenoszenia się do jurysdykcji, które nie przystąpiły do CRS, natomiast klientów do korzystania z usług takich instytucji. W konsekwencji, jeżeli istotna część instytucji finansowych znajdzie się poza systemem wymiany informacji przewidzianym przez CRS, skuteczność i efektywność tego narzędzia może zostać postawiona pod znakiem zapytania[12].

Instytucje finansowe, rodzące niewielkie ryzyko wykorzystywania w celu unikania opodatkowania, zostały wyłączone z obowiązków raportowanych przewidzianych przez CRS. Każde państwo może zaproponować własną listę takich instytucji[13].

CRS, podobnie jak Umowa IGA, zachowuje podział na klientów nowych i klientów istniejących oraz na klientów indywidualnych i instytucjonalnych, uzależniając procedury identyfikacyjne jakie mają być zastosowane od danego klienta od tego, do której z ww. kategorii jest on zakwalifikowany. Datą rozgraniczającą klientów istniejących od nowych jest 1 stycznia 2016 roku. W odniesieniu do rachunków prowadzonych dla klientów przed wskazaną datą instytucje finansowe będą zobowiązane do weryfikacji danych pod kątem przesłanek wskazujących na posiadanie przez nich rezydencji podatkowej w innym państwie. Co się zaś tyczy pozostałych klientów, będą oni zobowiązani do przedłożenia instytucji finansowej, w chwili otwierania rachunku, oświadczenia o ich rezydencji podatkowej. Instytucja finansowa będzie natomiast zobowiązana do okresowego weryfikowania wiarygodności tych oświadczeń.

Zidentyfikowani w powyższy sposób klienci będą podlegali corocznemu raportowaniu do właściwej władzy krajowej, która następnie przekaże ich dane do kraju ich rezydencji. Do danych klienta podlegających raportowaniu, do których uzyskania zobowiązana jest instytucja finansowa, należy zaliczyć:

- imię i nazwisko,
- adres,
- numer identyfikacji podatkowej,
- datę urodzenia (w przypadku osób fizycznych),
- numer rachunku,

12 P. Radcliffe, *The OECD's Common Reporting Standard: The Next Step in the Global Fight against Tax evasion*, Derivatives & Financial Instruments, 2014 (Volume 16), No. 4, s. 162.

13 K. Marsoul, *FATCA and Beyond: Global Information Reporting and Withholding Tax Relief*, Derivatives & Financial Instruments, 2014 (Volume 16), No. 1, s. 13.

- saldo lub wartość rachunku,
- w przypadku rachunków powierniczych: wartość brutto kwot lub wpływów brutto na rachunek w danym roku,
- w przypadku rachunków depozytowych: wartość brutto odsetek wpłaconych lub naliczonych względem rachunku,
- w przypadku pozostałych rachunków: wartość brutto kwot wpłaconych lub naliczonych względem rachunku, włączając w to łączną sumę płatności tytułem umorzenia.

Jeżeli instytucje finansowe nie będą w posiadaniu powyższych danych, będą one zobowiązane do podjęcia uzasadnionych działań w celu ich uzyskania[14].

CRS a Umowa IGA – porównanie

Twórcy CRS nie odżegnywali się od jego podobieństwa z Umową IGA. Przeciwnie, w preambule do CRS wskazano, iż mając na uwadze zarówno efektywność proponowanej regulacji, jak i minimalizację kosztów jej implementacji dla instytucji finansowych, CSR został oparty na rozwiązaniach już wypracowanych dla celów FATCA z uwzględnieniem jednak różnic wynikających z wielostronnego charakteru CSR oraz zastosowania w umowach implementującej FATCA rozwiązań uwzględniających specyfikę prawa podatkowego Stanów Zjednoczonych.

Do najważniejszych różnic miedzy CRS a Umową IGA należy zaliczyć:

- brak limitów sald, poniżej których identyfikacja rachunków nie jest konieczna,
- inne definicje osób objętych raportowaniem,
- różnice w zakresie dokumentacji wymaganej od klientów,
- różnice w klasyfikacji podmiotów i produktów,
- inny zakres weryfikowanych i raportowanych danych,
- inne procedury wymagane względem funduszy inwestycyjnych.

Jedną z najistotniejszych modyfikacji względem Umowy IGA przewidzianą w CRS jest brak limitów sald, poniżej których identyfikacja istniejących rachunków finansowych nie jest wymagana. W przypadku Umowy IGA, instytucje finansowe miały prawo zrezygnować z identyfikacji istniejących rachunków indywidualnych, których saldo nie przekraczało 50 tys. dolarów (lub

14 P. Radcliffe, *The OECD's Common Reporting Standard...* s. 163

250 tys.). W praktyce, większość instytucji finansowych działających w Polsce skorzystało ze wskazanej możliwości. Niestety, CRS nie przewiduje takiego wyłączenia spod obowiązku identyfikacji.

Inną bardzo istotną różnicą między analizowanymi regulacjami jest fakt, iż CRS przewiduje inną definicję osoby raportowanej oraz inną dokumentację wymaganą od klientów w celu wyjaśnienia ich rezydencji podatkowej. Jak już wskazano, podczas gdy wiele rozwiązań i procedur przewidzianych w Umowie IGA bazowało na prawie amerykańskim, na potrzeby CRS musiały zostać wypracowane inne, bardziej uniwersalne narzędzia. Z uwagi na fakt, iż amerykański system prawa podatkowego zakłada, iż osobą podlegającą nieograniczonemu obowiązkowi podatkowemu w Stanach Zjednoczonych jest również obywatel USA (a nie tylko amerykański rezydent podatkowy, jak ma to miejsce w większości państw świata) dla potrzeb CRS okazało się konieczne wypracowanie innej niż w Umowie IGA koncepcji osoby raportowanej.

W konsekwencji przewidziana w CRS definicja odwołuje się do prawa krajowego każdego poszczególnego państwa uczestniczącego w systemie wymiany informacji z uwagi na fakt, że celem CRS jest zidentyfikowanie rezydentów podatkowych tych państw. W rezultacie przesłanki, jakie należałoby zbadać w ramach weryfikacji klientów przewidzianej w CRS nie będą takie same jak przy identyfikacji dokonywanej dla potrzeb Umowy IGA.

W związku z powyższą zmianą koncepcji osoby raportowanej, CRS przewiduje również inną dokumentację wymaganą od klientów w związku z dokonywaną weryfikacją. W szczególności, zgodnie z CRS, klienci mogą składać wyjaśnienia odnoście ich statusu dla celów CRS i ich rezydencji podatkowej, których wiarygodność powinna być weryfikowana przez osoby wyposażone w wiedzę merytoryczną w powyższym zakresie. Powyższe poszerzenie zakresu weryfikacji, w połączeniu ze znacznie większą liczbą rezydencji podatkowych możliwych do przypisania klientom, skutkuje koniecznością opracowania nowych i modyfikacji już istniejących procedur dla celów CRS.

Wiele spośród statusów przewidzianych w Umowie IGA nie znajduje swoich odpowiedników w CRS. W tym zakresie ważną zmianą jest brak w CRS pojęcia nieuczestniczącej instytucji finansowej, co przekłada się np. na konieczność identyfikacji i raportowania do państwa rezydencji beneficjentów rzeczywistych funduszy inwestycyjnych z państw, które nie przystąpiły do CRS. Dodatkowo, definicje wielu zachowanych statusów uległy zmianie. Przykładowo, na gruncie CRS zmodyfikowano pojęcie podmiotów inwestycyjnych, poszerzając jego zakres.

Również definicje rachunków finansowych dla celów CRS i Umowy IGA nie pokrywają się. Istotną zmianą w CRS jest objęcie funduszy inwestycyjnych zamkniętych publicznych zakresem pojęcia rachunek finansowy.

Ponadto duże wątpliwości budzi zakres produktów, a także podmiotów zwolnionych z CRS ze względu na brak precyzyjne zdefiniowanych warunków zastosowania zwolnienia.

Co więcej, różnice pomiędzy CRS i Umową IGA uwidoczniają się także w zakresie danych zbieranych i raportowanych przez instytucje finansowe. Poszerzenie zakresu danych klientów objętych obowiązkiem zgromadzenia i raportowania w CRS uzasadnia się zwiększeniem poprawności dopasowywania raportowanych dochodów do konkretnego podatnika[15].

Zatem, mimo iż obowiązki weryfikacyjne i sprawozdawcze nałożone na instytucje finansowe przez Common Reporting Standard w ogólnej konstrukcji przypominają procedury należytej staranności przewidziane w Umowie IGA, wykazują też wiele istotnych różnic, które spowodują, że instytucje finansowe będą musiały podjąć szereg działań w celu dostosowania swoich procedur i dokumentacji do CRS.

Nie należy też zapominać, iż na gruncie CRS instytucje finansowe będę zobowiązane do badania klientów pod kątem bardzo wielu możliwych rezydencji podatkowych. Dodatkowo, podczas gdy, jak wskazuje praktyka instytucji finansowych, raportowanie dla potrzeb Umowy IGA objęłoby bardzo niewielką grupę ich klientów, obowiązki sprawozdawcze przewidziane przez CRS, jak się wydaje, mogą dotknąć dość znaczącej części klientów instytucji finansowych.

Dyrektywa w sprawie współpracy administracyjnej w dziedzinie opodatkowania

Mimo iż niniejszy artykuł koncentruje się na analizie CRS, należy zaznaczyć, iż nie jest on jedyną regulacją, która nakłada na instytucje finansowe obowiązki w zakresie identyfikacji i wymiany informacji o klientach będących zagranicznymi rezydentami. W ostatnim czasie także Komisja Europejska zintensyfikowała swoje działania w zakresie przeciwdziałania uchylaniu się od opodatkowania, czego rezultatem jest m.in. przyjęta w dniu 9 grudnia 2014 r. Dyrektywa Rady z dnia 9 grudnia 2014 r. nr 2014/107/UE zmieniająca

15 Ibidem, s. 162.

Dyrektywę nr 2011/16/UE w zakresie obowiązkowej automatycznej wymiany informacji w dziedzinie opodatkowania[16].

Dyrektywa 2014/107/UE powiela rozwiązania znane już z FATCA i CRS. Powyższe wynika z przyjętych przez Unię Europejską założeń minimalizacji kosztów i obciążeń nakładanych zarówno na państwa członkowskie, jak i podmioty gospodarcze[17]. W konsekwencji celem Dyrektywy jest coroczne przekazywanie przez instytucje finansowe określonych danych o rachunkach prowadzonych dla nierezydentów za pośrednictwem krajowych organów administracji do kraju ich rezydencji podatkowej.

Należy podkreślić, iż w założeniu Dyrektywa 2014/107/UE ma nie obciążać instytucji finansowych z państw członkowskich dodatkowymi wymaganiami w stosunku od tych, które wynikają z CRS. W preambule do Dyrektywy wskazano, iż aby osiągnąć ten cel, państwa członkowskie powinny wymagać od swoich instytucji finansowych wdrożenia zasad sprawozdawczych i zasad należytej staranności w pełni zgodnych z zasadami określonymi w Common Reporting Standard. Oczekuje się ponadto, iż każde państwo członkowskie będzie miało tylko jeden wykaz określonych wewnętrznie „nieraportujących instytucji finansowych" i typów wyłączonych rachunków finansowych, który to wykaz dane państwo wykorzystywałoby zarówno do wdrożenia niniejszej dyrektywy, jak i dla celów CRS[18].

Jednakże o rzeczywistej spójności wymagań nałożonych na instytucje finansowe dla celów CRS i Dyrektywy 2014/107/UE będzie można przekonać się dopiero wtedy, gdy oba wskazane akty zostaną implementowane do polskiego prawa. W przypadku Dyrektywy przyjęcie przez Polskę odpowiednich aktów ustawodawczych i wykonawczych ją transponujących ma odbyć się do końca 2015 r. W rezultacie instytucje finansowe rozpoczną stosowanie obu analizowanych aktów jednocześnie – począwszy od 1 stycznia 2016 r.[19]

Jak instytucje finansowe powinny przygotować się do CRS?

W pierwszej kolejności instytucje finansowe powinny przeanalizować istniejące procedury, a w szczególności rozwiązania wypracowane dla potrzeb

16 Dz. U. UE seria L 359/1, dalej: „Dyrektywa 2014/107/UE" lub „Dyrektywa"

17 Patrz pkt. 9 preambuły do Dyrektywy 2014/107/UE

18 Ibidem.

19 Art. 2 Dyrektywy 2014/107/UE

Umowy IGA w celu określenia, jak dalece mogą być one wykorzystywane do wypełniania obowiązków nałożonych przez CRS i jakich modyfikacji będą wymagały. Niewykluczone, że ze względu na występujące w niektórych obszarach istotne rozbieżności miedzy Umową IGA a CRS niekiedy konieczne będzie opracowywanie nowych rozwiązań.

Niewątpliwie niezbędne będą także modyfikacje systemów informatycznych instytucji finansowych, aby uwzględnić dodatkowe dane zbierane dla celów CRS, a przede wszystkim algorytmy identyfikacji klientów wymagane przez CRS. Jeżeli instytucja finansowa nie zdecyduje się na automatyzację procesu identyfikacji klientów, istotne może okazać się gruntowane przeszkolenie personelu celem prawidłowego wypełniania obowiązków wynikających z CRS, w szczególności w obliczu faktu, iż w skutek większej uznaniowości pozostawionej instytucjom finansowych w przedmiocie oceny wiarygodności danych przedstawionych przez klientów, CRS będzie wymagał bardziej specjalistycznej wiedzy niż Umowa IGA.

Wdrożenie CRS nie obędzie się bez zmian w dokumentacji instytucji finansowych, takich jak procedury, formularze, oświadczenia czy umowy. Instytucje finansowe będą mogły zmodyfikować istniejące oświadczenia zbierane od klientów dla potrzeb Umowy IGA, tak by odzwierciedlały one wymagania przewidziane przez CRS lub zdecydować się na stosowanie dwóch oddzielnych oświadczeń. Podobnych dylematów i decyzji biznesowych do podjęcia jest wiele.

Instytucje finansowe przy opracowaniu rozwiązań dla potrzeb CRS muszą uwzględnić konieczność zapewnienia ich elastyczności. Wymóg ten wiąże się z jednej strony z faktem, iż ostateczny kształt regulacji, którą stosować będą instytucje finansowe w Polsce nie jest jeszcze znany, z drugiej natomiast z potrzebą wzięcia pod uwagę, iż do CRS będą przystępować kolejne państwa.

Podobnie, jak miało to miejsce w przypadku Umowy IGA, instytucje finansowe staną przed wyzwaniem opracowania rozwiązań, które będą minimalizowały negatywne skutki dla relacji z biznesowych oraz ich obciążania przy zapewnieniu pełnej zgodności z regulacją CRS.

Podsumowanie

Przeprowadzona analiza nowej regulacji, jak również doświadczenie autorów niniejszego artykułu we wdrożeniu projektów FATCA wykazują, że CRS będzie oddziaływał na obowiązujące obecnie w instytucjach finansowych

procesy i procedury biznesowe, a także wspierające je systemy IT w znacznie szerszym zakresie niż miało to miejsce w przypadku Umowy IGA.

Istotne zaangażowanie Polski w jak najszybszą implementację postanowień nowych regulacji nie pozostawia wątpliwości, że CRS stanie się w niedługim czasie elementem polskiego porządku prawnego. W kontekście krótkiego horyzontu czasowego, jaki pozostał do deklarowanego przez Polskę wdrożenia CRS oraz Dyrektywy 2014/107/UE (tj. 1 stycznia 2016 r.), instytucje finansowe w Polsce staną w najbliższym czasie przed koniecznością dokonania analizy rozwiązań i narzędzi wypracowanych dla potrzeb FATCA w celu określania, jak dalece mogą one wspierać implementację CRS, a także opracowania nowych rozwiązań wymaganych w celu wdrożenia komentowanej regulacji.

Andrzej Sieradz

Wiceprezes Zarządu Banku BGŻ. Doktor nauk ekonomicznych Uniwersytetu Gdańskiego.Ukończył Politechnikę Warszawską w 1983. Uzyskał również tytuł MBA Business International School w Warszawie oraz ukończył studia podyplomowe z zakresu finansów i bankowości w Szkole Głównej Handlowej.Zanim związał się z Bankiem BGŻ, w latach 2006–2010 był dyrektorem operacyjnym i członkiem zarządu ING Towarzystwo Ubezpieczeń na Życie S.A. oraz członkiem zarządu ING Usługi Finansowe S.A., gdzie odpowiadał za dział informatyki, obsługę klienta oraz zarządzanie projektami. W latach 2002–2006 związany z ING Bank Śląski S.A., najpierw jako dyrektor zarządzający. W latach 1997–2002 pracował w Coca-Cola HBC w Polsce i w centralii w Wiedniu.

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 i Grzegorz Kuliszewski

Banki – platforma cyfrowa dla usług administracji państwowej?

Administracja cyfrowa (ang. E-Government) to wykorzystanie przez instytucje rządowe informatyki i telekomunikacji do przekazywania informacji i świadczenia usług obywatelom[1]. Oznacza to wykorzystywanie rozwiązań informatycznych w celu integracji procesów, efektywnego zarządzania danymi i informacją, poprawy jakości usług, otwarcia na nowe kanały komunikacyjne oraz zwiększenia zaangażowania i współpracy z obywatelami. Wśród wykorzystywanych w ostatnich latach narzędzi należy wskazać portale internetowe, media społecznościowe, analizy typu „big data", aplikacje mobilne czy też rozwiązania chmurowe. Niemniej jednak, mówiąc o administracji cyfrowej zawsze mamy na myśli co najmniej trzy rodzaje interakcji:

- pomiędzy jednostkami rządowymi – government-to-government (G2G),
- pomiędzy administracją a biznesem – government-to-business (G2B),
- pomiędzy administracją a obywatelem – government-to-consumer (G2C).

Zbiór dobrych praktyk wskazuje następujące czynniki konieczne do efektywnego uruchomienia projektu wdrożenia administracji cyfrowej:

- wola polityczna,
- współzarządzanie i współodpowiedzialność jednostek administracji publicznej,
- obywatelo-centryczny model zarządzania Państwem,
- strategia informatyzacji Państwa,
- budowanie poczucia usługowej roli Państwa.

1 Global E-Government Readiness Report 2004.

Natomiast udana realizacja takiego przedsięwzięcia wymaga dodatkowo:

- otwartości, przejrzystości, odpowiedzialności i zaangażowania urzędów oraz urzędników,
- efektywnej platformy informatycznej i telekomunikacyjnej,
- odpowiednich zasobów ludzkich,
- przyjaznych dla użytkowników systemów dostępowych.

W najnowszym rankingu ONZ *„e-Government Survey 2014"*[2], dotyczącym informatyzacji zarządzania państwami, Polska została sklasyfikowana na 42. miejscu na 193 analizowane państwa, podczas gdy jeszcze dwa lata temu było to miejsce 47. – czyli awans, choć niewielki. Niestety, bliższy wgląd w niniejszą klasyfikację pokazuje mniej pozytywny obraz – *„Im bardziej Puchatek zaglądał do środka, tym bardziej Prosiaczka tam nie było."*[3]. 42. miejsce na świecie – czyli za Malta i Słowenią, a przed Andorą i Katarem, to zaledwie 28 miejsce w Europie. W rankingu europejskim Polska pokonała takie mocarstwa informatyczne jak: Albania, Andora, Białoruś, Bośnia i Hercegowina, Bułgaria, Chorwacja, Czarnogóra, Czechy, Macedonia, Mołdawia, Rumunia, San Marino, Serbia, Słowacja i Ukraina (kolejność alfabetyczna). Liderami rankingu światowego są Korea Południowa, Australia, Singapur i Francja.

W tym samym zestawieniu średni zintegrowany współczynnik usług administracji cyfrowej dla krajów UE wynosi 0,73 przy 0,65 osiągniętym przez Polskę. Najlepiej przygotowanym do administracji cyfrowej państwem UE jest Francja z blisko 90% udziałem usług administracyjnych dostępnych dla obywateli przez Internet.

---

2 UNITED NATIONS E-GOVERNMENT SURVEY 2014, E-Government for the Future We Want, str. 34, 202, 210

3 Alan Alexander Milne – „Chatka Puchatka"

Tablica 1.
Stopień zaawansowania usług e-governmentowych w krajach Europy

Kraj	Region	EGDI*	Miejsce w rankingu w 2012 r.	Miejsce w rankingu w 2014 r.	Zmiana rankingu
		Bardzo wysokie EGDI			
Francja	Europa Zachodnia	0,8938	6	4	2
Holandia	Europa Zachodnia	0,8897	2	5	-3
Wielka Brytania	Europa Północna	0,8695	3	8	-5
Finlandia	Europa Północna	0,8449	9	10	-1
Hiszpania	Europa Południowa	0,8410	23	12	11
Szwecja	Europa Północna	0,8225	14	7	-7
Estonia	Europa Północna	0,8180	20	15	5
Dania	Europa Północna	0,8162	4	16	-12
Austria	Europa Zachodnia	0,7912	21	20	1
Niemcy	Europa Zachodnia	0,7864	17	21	-4
Irlandia	Europa Północna	0,7810	34	22	12
Włochy	Europa Południowa	0,7593	32	23	9
Luksemburg	Europa Zachodnia	0,7591	19	24	-5
Belgia	Europa Zachodnia	0,7564	24	25	-1
		Wysokie EGDI			
Litwa	Europa Północna	0,7271	29	29	
Łotwa	Europa Północna	0,7178	42	31	11
Grecja	Europa Południowa	0,7118	37	34	3
Portugalia	Europa Południowa	0,6900	33	37	-4
Węgry	Europa Wschodnia	0,6637	31	39	-8
Malta	Europa Południowa	0,6518	35	40	-5
Słowenia	Europa Południowa	0,6505	25	41	-16
Polska	Europa Wschodnia	0,6482	47	42	5
Chorwacja	Europa Południowa	0,6282	30	47	-17
Słowacja	Europa Wschodnia	0,6148	53	51	2
Czechy	Europa Wschodnia	0,6070	46	53	-7
Cypr	Azja Zachodnia	0,5958	45	58	-13
Rumunia	Europa Wschodnia	0,5632	62	64	-2
Bułgaria	Europa Wschodnia	0,5421	60	73	-13
średnia dla UE		0,7300			
średnia dla regionu		0,6936			
średnia światowa		0,4712			

* EGDI – The E-Government Readiness Index

Źródło: *United Nations E-government Survey 2014*, s. 54

Warto poznać dokonania poszczególnych państw, aby zrozumieć, jakie działania przez nie podjęte pozwoliły im zająć czołowe miejsca w rankingu.

Oczekiwania obywateli

Badania oczekiwań, co do administracji cyfrowej, prowadzane w UE i w Polsce zasadniczo się pokrywają. Obywatele oczekują:

- Bezpieczeństwa danych i informacji – i, co więcej, ważkość tego wymagania rośnie wraz ze wzrostem zagrożeń informatycznych oraz świadomości obywateli.
- Dostępności usług w wirtualnej przestrzeni dla obywateli, kiedy chcą i gdziekolwiek się znajdują, wykorzystując urządzenie, jakie wybiorą lub dysponują. Internet jest zatem postrzegany tylko jako medium.
- Zawartości (ang. content), która jest dobrze zaprojektowana, z łatwą nawigacją. Treść informacyjna jest napisana prostym językiem, umożliwiającym szybkie i skuteczne wyszukanie oraz skorzystanie z informacji.
- Transakcyjności, umożliwiającej realizację procesów od początku do końca z cyfrowym uwierzytelnieniem tożsamości i płatnością (jeśli jest potrzebna).

Szczególnej uwagi wymaga oczekiwanie dotyczące prostoty nawigacji i języka. Dane pokazują, że organizacje rządowe myślą i działają silosowo, co powoduje, iż sprawne poruszanie się po stronach rządowych wymaga znajomości „oferty". Dodatkowo formalny i urzędowy język komunikacji powoduje, że wykonanie nawet najprostszej czynności może być wyzwaniem[4].

Doświadczenia poszczególnych Państw

Wielka Brytania wdrożyła portal „GOV.UK", którego zadaniem było zapewnienie obywatelom i firmom prostego i efektywnego dostępu do informacji i usług. Portal uruchomiony w 2012 roku zastąpił setki stron poszczególnych departamentów i urzędów publicznych[5].

W celu realizacji oczekiwań związanych z bezpieczeństwem dostępu rząd *Niemiec* w swojej strategii „eGovernment 2.0" zdefiniował następujące wymagania:

---

4 Paving the way for the next generation of eservices: How the public sector can meet Canadians' expectations www.pwc.com/ca/CitizenCompass, str.6.

5 The eGovernment factsheets United Kingdom, May 2014, http://epractice.eu, str. 23.

- bezpieczna wymiana informacji elektronicznej,
- skuteczna autentykacja,
- stałe i bezpieczne przechowywanie dokumentów elektronicznych i innych danych[6].

Należy zwrócić tutaj uwagę, że skuteczna i bezpieczna autentykacja nie musi oznaczać jednej metody dla wszystkiego. Badania pokazują, że oczekiwania obywateli wobec kontroli dostępu do danych podstawowych (imię, nazwisko, adres) są inne niż wobec np. danych zdrowotnych.

W ***Wielkiej Brytanii*** jako jeden z filarów programu eGovernment wdrożono centralną platformę identyfikacji (ang. *Government Gateway*) służącą do autentykacji operacji. W zależności od typu operacji identyfikacja użytkowników jest oparta o certyfikat cyfrowy lub ID i hasło udostępnione przez platformę[7].

Podobne rozwiązanie zastosowała ***Estonia***, która już w 1999 roku wdrożyła chipowy dowód osobisty wraz z ID i pinem dla każdego obywatela[8]. Korzystając z kart obywatele Estonii mogą sięgać do zasobów rządowych, wykonywać operacje bankowe, podpisywać wiadomości w poczcie elektronicznej, czy tez głosować w wyborach. Świadomość, że już w 2011 r. 25% obywateli Estonii głosowało elektronicznie[9] była szczególnie przykra obserwując zamieszanie po wyborach samorządowych w Polsce jesienią zeszłego roku.

Odwrotne podejście zastosowały niektóre instytucje ***Kanady***. Zezwoliły one obywatelom na wykorzystanie dostępów do bankowości elektronicznej (ID oraz hasło) w celu dostępu do transakcyjnych części aplikacji rządowych. Uznano, że olbrzymią zaletą jest wygoda obywatela, który nie musi pamiętać kolejnych ID, pinów i haseł, a na dodatek wykorzystano istniejącą infrastrukturę bezpiecznego dostępu stworzoną przez kanadyjskie banki[10]. Urzędy wyciągnęły lekcję z doświadczeń kanadyjskiej bankowości. Adopcja kanałów samoobsługowych w bankach (bankowość elektroniczna, bankomaty) była powolna. Ludzie nie byli przyzwyczajeni do samodzielnego wykonywania operacji, a obszar bezpieczeństwa budził obawy. Dopiero uświadomienie sobie wygody, poczucie wzrostu poczucia bezpieczeństwa oraz wsparcie

---

6 eGovernment 2.0 The Programme of the Federal Government, www.verwaltung-innovativ.de, str. 21.

7 The eGovernment factsheets United Kingdom, May 2014, http://epractice.eu, str. 24.

8 e-Economy and e-Government in Estonia, 05.01.2006, Ain Järv, CEO, Sertifitseerimiskeskus (SK).

9 http://estonia.eu/about-estonia/economy-a-it/e-estonia.html

10 Paving the way for the next generation... str. 6.

pracowników banku spowodowały masową migrację klientów do kanałów samoobsługowych. Obecnie Kanadyjczycy są oswojeni z kanałami elektronicznymi i takiego rodzaju obsługi oczekują od urzędów.

Rząd ***Stanów Zjednoczonych Ameryki*** w celu realizacji oczekiwania związanego ze swobodnym wyborem urządzeń zdecydował się udostępnić setki API, które mogą być wykorzystywane przez firmy prywatne do tworzenia nowych aplikacji i usług. Udostępnione API dotyczyły zarówno trendów zużycia energii przez obywateli i przedsiębiorstwa, jak i informacji w czasie rzeczywistym o trzęsieniach ziemi, czy też o pogodzie na Marsie przekazywane z lądownika Curiosity. Poszczególne agencje rządowe udostępniły strony dla deweloperów, tak aby ułatwić wykorzystanie udostępnionych interfejsów, a administracja centralna uruchomiła program wsparcia tworzenia aplikacji mobilnych[11].

Bariery

Kluczową umiejętnością, jaką poszczególne kraje muszą posiąść jest całościowe spojrzenie na dostęp elektroniczny do zasobów oraz zdolność rozlicznych rządowych i pozarządowych organizacji do wymiany oraz integracji informacji pomiędzy sobą. Wyzwaniem jest tutaj gotowość do wymiany informacji, a nie, jak to nastąpiło w wielu przypadkach, koncentracja na zagadnieniach technologicznych, takich jak standardy czy protokoły. Technologia jest oczywiście konieczna, ale niewystarczająca dla stworzenia społeczeństwa informacyjnego. Rozwiązania informatyczne muszą zapewnić bezpieczeństwo wymiany informacji poufnych i zdobyć zaufanie obywateli. Najważniejszym zadaniem systemów back-office'owych jest zapewnienie wygody, prostoty i dostępności dla użytkowników. Obywateli nie interesuje, która agencja czy ministerstwo dostarcza daną usługę, lecz gdzie ją znaleźć i czy jest ona wygodna w użyciu[12].

Należy pamiętać, że cała koncepcja administracji cyfrowej nie jest celem samym w sobie, a narzędziem do realizacji celu w sposób oparty na współpracy. Z punktu widzenia usług można wskazać cztery pryncypia, na których powinno budować się takie rozwiązania:

- wysoka jakość, która może być określona jako dostępność usług publicznych w sposób wygodny dla obywateli (prościej, szybciej, bez konieczności wypełniania dokumentów papierowych, ...),

11 United Nations E-government Survey 2014, str. 108.

12 United Nations E-government Survey 2014, str. 90.

- łatwy dostęp, czyli taki rozwój usług, który prowadzi do ograniczenia liczby wykluczonych,
- efektywność kosztowa, bo to w końcu nasze pieniądze,
- obywatelo-centryczność wraz z mechanizmami do zbierania i wykorzystywania uwag i wniosków użytkowników oraz włączania ich w proces poprawiania rozwiązań.

Trzeba zwrócić uwagę, że ścisła integracja pomiędzy jednostkami administracyjnymi nie powinna być celem samym w sobie. Jest nim dostarczanie wartości dla obywatela, a nie integracja dla integracji. Przykładem mogą być tu doświadczenia z sektora usług medycznych, które pokazały, że integracja usług medycznych z innymi usługami administracyjnymi nie jest ani oczekiwana, ani potrzebna, gdyż obywatele traktują ten obszar działań rozłącznie od innych, stawiając jednocześnie znacznie wyższe oczekiwania związane z prywatnością i zabezpieczeniem ich danych.

Istnieje wiele politycznych, organizacyjnych i technicznych wyzwań, które utrudniają szeroką współpracę jednostek rządowych z otoczeniem. Wśród najważniejszych należy wskazać:

- brak jednolitej wizji i praktycznej gotowości do pokonywania przeszkód,
- słabe przywództwo i silosowe myślenie,
- zachowawcze struktury decyzyjne,
- fragmentacja pozioma i pionowa,
- niewystarczające mechanizmy zapewniające, wspierające współodpowiedzialność przy współpracy pomiędzy jednostkami,
- brak zaufania pomiędzy jednostkami i urzędami,
- brak zaufania do jakości, niezawodności i bezpieczeństwa infrastruktury technicznej[13].

Administracja cyfrowa w Polsce

W rankingu ONZ Polska zajęła 22 miejsce wśród 28 krajów Unii Europejskiej, przy czym w ciągu ostatnich dwóch lat „przeskoczyliśmy" Chorwację, Czechy i Cypr. Czy to już pora osiąść na laurach? Kiedy uznamy, że osiągnęliśmy sukces?

---

13 United Nations E-government Survey 2014, str. 79.

Według Ministerstwa Administracji i Cyfryzacji wypełnienie celów będzie mierzone odsetkiem obywateli i przedsiębiorców korzystających z e-usług administracji publicznej. Wzrost tego wskaźnika do 2020 r. powinien pozwolić Polsce być w pierwszej siódemce krajów Unii Europejskiej. Brzmi ambitnie biorąc pod uwagę dotychczasowe osiągnięcia w tym zakresie oraz świadomość, że inne kraje Unii też mają swoje plany w tym zakresie.

Według badań Ministerstwa Administracji i Cyfryzacji ponad połowa obywateli Polski aktywnie korzystających z Internetu ciągle woli załatwiać urzędowe sprawy „osobiście", czyli bezpośrednio w urzędzie. Jednocześnie zwiększa się liczba tych obywateli, którzy „podejmują próbę" załatwiania spraw urzędowych przez Internet. Według danych GUS z „elektronicznych usług" urzędów korzysta nie więcej, niż co czwarty Polak. Sama definicja „korzysta" wymaga oddzielnego omówienia, na które w niniejszym artykule nie ma miejsca.

Powstaje pytanie dlaczego tak się dzieje? Jak przyznają badani internauci – wielu urzędowych spraw nie da się załatwić przez Internet w sposób kompleksowy. Stąd też dystans, jaki dzieli Polskę od wielu krajów Unii Europejskiej, a także – od unijnej średniej. Tymczasem oczekiwania Polaków, jak przedstawiono powyżej, są typowe i jak wszędzie indziej rosną.

Dzięki technologiom cyfrowym zadania państwa mogą być realizowane w sposób bardziej efektywny, spersonalizowany i partycypacyjny. Polskie społeczeństwo przechodzi intensywną przemianę spowodowaną rozwojem cywilizacyjnym oraz stałym wzrostem roli Internetu i technologii cyfrowych w stosunkach społecznych. Państwo i administracja muszą w tym kontekście dotrzymać kroku obywatelom i wykorzystać szanse związane z cyfryzacją do lepszej realizacji zadań. Celem drugorzędnym, niemniej jednak istotnym, jest „uproszczenie" państwa i zmniejszenie kosztów administracji państwowej. Ale ostrożnie, wcale tak nie musi być. Ciekawym przykładem jest wspomniana już Francja, będąca liderem Europy w zakresie cyfrowego państwa, a jednocześnie zatrudniająca procentowo największą liczbę pracowników administracji w Europie. Publikacje MAiC nie odnoszą się jasno do celów dotyczących efektywności kosztowej administracji państwowej.

Cyfrowa rzeczywistość to w praktyce nie tylko obsługa zdalna procedur administracyjnych, ale przebudowa relacji rząd – obywatel – samorząd – organizacje pozarządowe w kierunku większego partnerstwa, a w konsekwencji transformacji modelu funkcjonowania państwa. Dzięki koncepcji „otwartego rządu" można będzie w większym stopniu włączać obywateli w podejmowanie

decyzji oraz wykorzystywać ich wiedzę i umiejętności. Przynajmniej teoretyczne. Poprzestańmy zatem na celach związanych z łatwiejszym dostępem do procedur administracyjnych wykonywanych przez obywateli zdalnie.

Sukces w podatkach i ZUS

Za największy sukces administracji cyfrowej w Polsce należy uznać system rozliczeń podatkowych obywateli. Deklarację podatkową PIT za rok 2013 złożyło w systemie e-Deklaracje kilka milionów Polaków. Warto od razu zauważyć, że przez lata usługa ta nie mogła być uruchomiona ze względu na ułomności procesu weryfikacji uwierzytelnienia wypełniającego deklarację PIT. Obecnie bardzo prosty mechanizm weryfikacji umożliwia skorzystanie z tej formy składania PIT wielu Polakom.

Działa też Centralna Ewidencja i Informacja o Działalności Gospodarczej (CEiDG) – rejestr, który umożliwia zakładanie działalności gospodarczej (choć w wielu sytuacjach wizyty w urzędach nie sposób uniknąć). System ten pozwala też sprawdzać dokumenty związane z jej prowadzeniem. Sprawnie działa system elektronicznych ksiąg wieczystych oraz platforma ZUS.

Wdrożenie nowego Systemu Rejestrów Państwowych miało nastąpić 1 stycznia 2015 r. Zostało przesunięte o dwa miesiące i system prawdopodobnie ruszy bez dalszych opóźnień, a więc 1 marca 2015 r. Co to zmieni dla obywatela?

System Rejestrów Państwowych (SRP) połączy rejestry PESEL, dowodów osobistych i aktów stanu cywilnego. Oznacza to pewne pozytywne zmiany z punktu widzenia obywatela. Do tej pory każda gmina pracowała na odrębnym systemie, tzn. urzędnicy nie mieli dostępu do wszystkich danych zawartych m.in. w zbiorze PESEL czy ewidencji dowodów osobistych. Mieli za to dostęp do informacji o mieszkańcach gminy. Z tego właśnie powodu, jeśli chciało się wyrobić dowód osobisty, trzeba było stawić się w urzędzie właściwym dla miejsca zameldowania. Informacje wprowadzane w systemach lokalnych trafiały z opóźnieniem do centralnego zbioru PESEL, a instytucje takie jak ZUS czy NFZ otrzymywały je z jeszcze większym opóźnieniem. SRP ma sprawić, że urzędnicy będą mieli dostęp do wszystkich informacji zgromadzonych w kluczowych rejestrach państwowych. Dlatego możliwe będzie załatwianie prostych spraw urzędowych w dowolnej gminie oraz (części z nich) online. Dzięki integracji rejestrów procedury powinny być dużo łatwiejsze – zamiast dostarczać góry dokumentów, wystarczające będzie podanie numeru PESEL.

Nie da się ukryć, że ogromnym ułatwieniem będzie też możliwość uzyskania odpisu aktu stanu cywilnego w dowolnym mieście. Obecnie obywatele są zmuszani do pokonywania setek kilometrów, aby dotrzeć do właściwego urzędu i uzyskać np. akt urodzenia. Trzeba się stawić w godzinach pracy urzędu, więc w praktyce trzeba brać urlop na takie okazje.

Czy jest to już wizja świata idealnego? Niestety, nie! Osoby, które chciałyby korzystać z administracji cyfrowej największy problem mają z weryfikacją swojej tożsamości. W tej chwili Jan Kowalski, chcąc załatwiać sprawy w różnego rodzaju urzędach – na przykład w swojej gminie – powinien zarejestrować się na platformie ePUAP i uzyskać tzw. profil zaufany (taki profil ma nieco ponad 350 tys. osób). Chcąc komunikować się z ZUS przez Internet, musi mieć profil PUE (ok. 900 tys. osób). Jeśli chce sprawdzić, za jakie świadczenia zapłacił w jego imieniu lekarzom Narodowy Fundusz Zdrowia, musi mieć profil w Zintegrowanym Informatorze Pacjenta (ZIP). Posiadanie oddzielnego systemu autoryzacji do wielu rejestrów administracji państwowej wydaje się być niewygodne i niepraktyczne. Może to być jedna z barier szerokiego stosowania systemu przez obywateli. A może to działanie celowe, gdyż istnieje wątpliwość, czy ePUAP w obecnej konfiguracji obsłuży 1 milion klientów, a co dopiero 20 milionów.

Najwięcej do zrobienia jest w tej chwili w obszarze ochrony zdrowia, gdzie już działają ZIP (dane na temat leczenia i finansowania usług) i eWUŚ (ewidencja ubezpieczonych), ale ciągle nie ma systemu eZdrowie, tzw. Platformy P1. Platforma ta ma ułatwić życie lekarzom, NFZ, ZUS – i przede wszystkim pacjentom. Gdy powstanie, lekarze będą wystawiać recepty, zwolnienia oraz skierowania drogą elektroniczną. Dużo łatwiejsza będzie ich kontrola, sprawniejszy obieg dokumentów.

Problem integracji rozwiązań dla administracji cyfrowej

Dotychczasowy proces informatyzacji charakteryzował się rozwiązaniami wyspowymi, które odpowiadały zapotrzebowaniom poszczególnych sektorów administracji publicznej, jednak nie zapewniały dostatecznej interoperacyjności systemów, co mogło mieć negatywny wpływ na realizację usług elektronicznych. W związku z powyższym niezbędne stało się wprowadzenie nowego instrumentu planowania i koordynacji informatyzacji działalności podmiotów publicznych, którym jest ustanawiany w drodze uchwały Rady

Ministrów, Program Zintegrowanej Informatyzacji Państwa w skrócie PZIP[14]. Obok Narodowego Planu Szerokopasmowego jest dokumentem wykonawczym dla strategii rozwoju, czyli strategii Sprawne Państwo 2020 (SP2020).

W ostatnich dniach grudnia 2014 ogłoszono pierwszy konkurs z Programu Polska Cyfrowa. Do wydania jest 945 mln złotych. Pieniądze zostaną wydane na usługi cyfrowe w administracji publicznej. Nabór wniosków ruszył 27 lutego br. i będą mogły go składać do 4 maja przede wszystkim urzędy państwowe, sądy i jednostki prokuratury. Wnioskodawcami mogą być też partnerstwa, jakie te instytucje utworzą z firmami, jednostkami naukowymi, instytucjami związanymi z ochroną zdrowia lub organizacjami pozarządowymi. Bezpośrednimi odbiorcami wsparcia będą natomiast obywatele. Cel jest jeden: budowa nowoczesnych cyfrowych usług publicznych, zarówno dla obywateli, jak i dla przedsiębiorców. Typowanie w ramach konkursu najlepszych pomysłów na nowoczesne usługi cyfrowe nie gwarantuje niestety budowania przemyślanej struktury powszechnych usług administracji w całym kraju.

Potencjalne rozwiązania dla Polski

Informatyzacja państwa ma wspierać budowanie modelu państwa 2.0 poprzez kreowanie i rozwój usług administracji publicznej – rządowej i samorządowej oraz monitorowanie i poprawę ich jakości – uwzględniając nowe możliwości, jakie pojawiają się w związku z dynamicznym rozwojem technologii cyfrowych oraz rozbudową cyfrowych zasobów i treści.

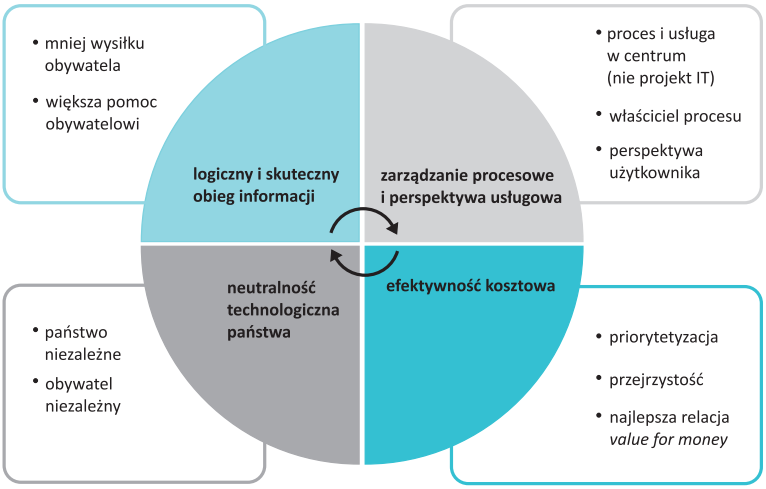
Celem programu informatyzacji w Polsce jest zapewnienie obywatelom i przedsiębiorcom, ale również samej administracji, dostępu do narzędzi użytecznych, bezpiecznych, prostych w stosowaniu, powszechnie dostępnych i neutralnych technologicznie. Z punktu widzenia obywatela najważniejsza jest wygoda załatwiania spraw urzędowych (w tym związanych z prowadzeniem działalności gospodarczej), związanych z ochroną zdrowia, poszukiwaniem pracy, regulowaniem należności, zdobywaniem wiedzy i wykształcenia. Obsługa klientów urzędów, w tym w szczególności usługi elektroniczne, powinny zapewnić oszczędność czasu oraz uwolnić obywateli od konieczności wizyty w obsługującej jednostce z wyłączeniem przypadków, kiedy osobiste stawienie się jest niezbędne. Przy wykorzystaniu usług elektronicznych

14 Dokument dostępny na stronach ministerstwa MAiC

powinno być możliwe załatwianie spraw niezależnie od miejsca pobytu i rodzaju stosowanej technologii służącej do korzystania z sieci (sprzętu, oprogramowania).

Według dokumentu „Informatyzacja zintegrowanych usług" opublikowanego przez MAiC powinna opierać się na czterech filarach (porównaj rysunek poniżej), z których trzy są krytyczne dla obywatela:

1. Informatyzacja państwa (różne szczeble administracji) podporządkowana jest obiegowi informacji. Logiczny i skuteczny obieg informacji, pomaga obywatelowi w realizacji jego obowiązków na rzecz państwa oraz wspiera go w realizacji jego aspiracji.
2. Koncentracja na procesach w administracji publicznej i usługach, jakie ona zapewnia, nie zaś projektach informatycznych. Właścicielem każdego procesu jest organ władzy publicznej, działający poprzez urzędnika urzędu, który realnie odpowiada za kontakty na linii państwo-obywatel.
3. Neutralność technologiczna, która gwarantuje, że dostęp do usług i dostaw dla administracji nie jest ograniczany i wynika jedynie z potrzeb funkcjonalnych. Dobór rozwiązania zapewnia możliwość zmiany dostawcy rozwiązań informatycznych, jeśli współpraca z obecnym nie gwarantuje spełnienia oczekiwań strony publicznej[15].



15 Raport „Państwo 2.0". Nowy start dla e-administracji.

Wykorzystanie rozwiązań z bankowości

Popularyzacja administracyjnych usług cyfrowych mogłaby zostać wielokrotnie zwiększona gdyby większość tych usług była oferowana obywatelom w łatwej i zrozumiałej formie. Od wielu lat banki promują bankowość w kanałach zdalnych, w tym głównie z wykorzystaniem dostępu do konta bankowego i usług bankowych przez Internet. Należy przypomnieć, że początki były trudne, ale dziś powszechność dostępu do konta o dowolnej porze jest niekwestionowana. Polska należy do niewielu krajów Europy o tak nowoczesnej infrastrukturze bankowej. Dziś niektóre banki już stosują rozwiązania, które umożliwiają klientom podpisanie umowy bankowej (np. kredytowej) bez konieczności osobistej wizyty w oddziale banku. W wielu aspektach takie podejście jest podobne do wykonania czynności administracyjnej na linii obywatel – administracja państwa, a opisane we wcześniejszych rozdziałach doświadczenia z Kanady można wykorzystać.

E-podpis czy popularne uwierzytelnienie bankowe

Według danych Ministerstwa Gospodarki od początku istnienia podpisu elektronicznego (czyli od 2002 roku) firmy wydały w sumie ponad milion certyfikatów kwalifikowanych. Obecnie w użyciu pozostaje ok. 300 tys. podpisów elektronicznych. Ograniczona popularność bezpiecznego podpisu elektronicznego wynika z faktu odpłatności za jego używanie, ograniczonego zakresu usług obsługiwanych przez ten mechanizm oraz z funkcjonowania elektronicznej Platformy Usług Administracji Publicznej (ePUAP). Platforma ta służy również do kontaktowania się z instytucjami administracyjnymi online i jest bezpłatna. Wystarczy tylko założyć „profil zaufany", co od kilku miesięcy można zrobić choćby na poczcie. Problem jednak polega na tym, że posługiwanie się tym profilem przez „przeciętnego" obywatela nie jest zrozumiałe. Tym bardziej trudno jest wytłumaczyć szerokiej grupie istotne zagadnienia związanie z bezpieczeństwem posługiwania się takim profilem. Profil zaufany to mniej niż bezpieczny podpis elektroniczny. Tylko ten drugi sposób pozwala, na przykład, podpisywać umowy, brać udział w zamówieniach publicznych czy składać wnioski do Krajowego Rejestru Sądowego przez Internet. Niezwykle istotnym zadaniem będzie określenie modelu uwierzytelniania w systemach teleinformatycznych, co w konsekwencji doprowadzi do zrównania podpisu elektronicznego z odręcznym wszędzie tam, gdzie będzie to zasadne i możliwe.

Powstaje zatem pytanie czy banki nie mogłyby pośredniczyć, jako jeden z zaufanych partnerów, w relacjach pomiędzy „obywatelem–klientem banku" a różnymi urzędami administracyjnymi, takimi jak: urzędy skarbowe, ZUS czy inne inne rejestry już dostępne. Z jednej strony można by stosować metody uwierzytelnienia i autoryzacji stosowane w bankach bez konieczności stosowania indywidualnych kont dodatkowo dla każdego klienta banku. Z drugiej strony zapytanie lub zgłoszenie się po usługę administracyjną „autoryzowane" przez banki i jednocześnie gwarantujące, że pochodzi ono od uprawnionego obywatela zapewniłoby odpowiedni poziom bezpieczeństwa danych.

Szyna usług i wspólna platforma komunikacyjna

Sprawne posługiwanie się usługami administracji cyfrowej musi zakładać powszechną uniwersalność oferowanych usług niezależnie od podziału terytorialnego kraju, jednocześnie zapewniając pełną interoperacyjność pomiędzy uczestnikami systemu i źródłami danych. To oznacza w praktyce realizację koncepcji „szyny serwisowej", spełniającej rolę pośrednika komunikacyjnego pomiędzy uczestnikami systemu i gwarantującego bezpieczna formę wymiany danych. Szyny serwisowa, poza funkcjami komunikacyjnymi, musiałaby zapewniać uwierzytelnienie już nie pojedynczych obywateli, a raczej agend rządowych lub pozarządowych upoważnionych lub zobowiązanych do oferowania usług. Podobną koncepcję wdraża się w Szwecji, stopniowo określając rejestry danych, które powinny być oferowane obywatelom w formie elektronicznej usługi czy w USA wystawiając API dla deweloperów aplikacji.

Podsumowanie wnioski

Bankowe platformy dostępu do usług finansowych mogłoby zostać wykorzystane jako wspólna platforma do komunikacji pozabankowej. W szczególności platforma mogłaby być zastosowana do zapewnienia, tak jak to zrobiono w Kanadzie, dostępu do usług administracji cyfrowej. Korzyści z takiego podejścia byłyby wielorakie:

- zmniejszenie kosztów infrastruktury informatycznej, jaka już istnieje w bankach, a która mogłaby być współdzielona do komunikacji i wymiany informacji na linii obywatel–państwo,
- zintegrowany system bezpieczeństwa danych osobowych (ze względu na regulacje, którymi banki są objęte od dawna),

- zapewnienie wysokiego stopnia bezpieczeństwa danych obywateli z wykorzystaniem wszystkich elementów Rekomendacji D, obowiązującej od 1 stycznia 2015,
- zmniejszenie kosztów administracyjnych,
- zmniejszenie kosztów wdrożenia administracji cyfrowej,
- zapewnienie terminowości administracji cyfrowej przy wykorzystaniu procesów automatyzacji, jakie już istnieją w bankach,
- krok wstępny do wdrożenia opracowywanego europejskiego programu przeciwdziałania wkluczeniom.

Polska jest obecnie w trakcie planowania inicjatyw w ramach kolejnej perspektywy budżetowej środków unijnych przeznaczonych dla e-administracji. Trwa proces zgłaszania inicjatyw jednostek administracyjnych i przyznawania tym inicjatywom budżetu. Trochę martwi fakt, że ten proces nie musi gwarantować pomyślnego wdrożenia oraz ujednolicenia świadczonych usług. Może warto przynajmniej część tych środków przeznaczyć na systemy IT i rozwiązania użyteczne dla wszystkich obywateli niezależnie od miejsca zamieszkania i połączyć je z już istniejącymi rozwiązaniami. Takimi systemami IT są obecnie istniejące systemy bankowe. Obawiamy się, że przyjęty proces nie zapewni minimalnego zestawu usług administracyjnych dla ogółu obywateli oraz potrzebnego stopnia integracji tych usług. Czas pokaże, czy nasze obawy były przesadzone czy też nie.

Niniejsze opracowanie wyraża prywatną opinię autorów i nie może być traktowane jako stanowisko firm, w jakich są lub byli zatrudnieni.

Bibliografia:

1. eGovernment 2010 Action Plan -Accelerating eGovernment in Europe for the Benefit of All, retrieved from:http://europa.eu/legislation_summaries/information_society/strategies/index_en.htm, 2012
2. M. Popiołek, E-Government in Poland- selected issues; Journal of Education Culture and Society No.2_2013.
3. United Nation E-Government Survey 2014, ISBN 978-92-1-1231984.
4. Program Zintegrowanej Informatyzacji Państwa, Ministerstwo Administracji i Cyfryzacji, Warszawa marzec 2013.
5. eGovernment in Poland, Edition 16.0; March 2014, European Dynamics. S.A.
6. Global E-Government Readiness Report 2004.

7. Paving the way for the next generation of eservices: How the public sector can meet Canadians' expectations www.pwc.com/ca/CitizenCompass.
8. The eGovernment factsheets United Kingdom, May 2014, http://epractice.eu
9. eGovernment 2.0 The Programme of the Federal Government, www.verwaltung-innovativ.de
10. e-Economy and e-Government in Estonia, 05.01.2006, Ain Järv, CEO, Sertifitseerimiskeskus (SK).
11. http://estonia.eu/about-estonia/economy-a-it/e-estonia.html
12. Raport „Państwo 2.0". Nowy start dla e-administracji.

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

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. Mimo tego tempo akceptacji przez oba sektory rozwiązań charakterystycznych dla cywilizacji cyfrowej różni się zasadniczo. 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 pierwotnym i w zasadzie jedynym autorytatywnym źródłem usług zaufania są państwo i jego agendy[1]. Administrowane przez nie atrybuty zaufania są akceptowane w sektorze publicznym i prywatnym na równi i na tyle powszechnie, że potrzeba dystrybucji alternatywnych atrybutów

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

dotyczy drugoplanowych obszarów działalności człowieka. Wynika to z przyjętej 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 dorzućmy 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 oczywiste, że na gruncie filozofii, prawa, teorii organizacji i innych przesłanek działania państwa i jego agend stanowią punkt wyjścia dla budowy infrastruktury zaufania.

Rozwiązania zawarte w Dyrektywie 1999/93/EC określającej zasady funkcjonowania podpisu elektronicznego poszły jednak w odmiennym kierunku. Nie wskazując *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. Skutkiem przyjęcia dyrektywy była 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 standardy techniczne i organizacyjne, które przełożyły się na wysoką cenę usług i produktów, co na płytkim początkowo rynku spowodowało ich faktyczne odrzucenie.

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

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

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 milionów 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*, nPA) wszedł do użytku 1 listopada 2010 roku. Jego premiera była ukoronowaniem około 10-letniego procesu planowania i projektowania, skomplikowanego koniecznością dokonania po drodze 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. 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 jego ograniczenia.

W krajach, w których sektor publiczny nie podjął wyzwania cyberprzestrzeni, próżnię wypełniły instytucje sektora finansowego. 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 nośnika sprzętowego. W 2011 roku identyfikatory NemID posiadało około trzech milionów 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. Bazuje on na standardach technicznych PKI zgodnych z dyrektywą EU, a każdy z dziewięciu banków pełni rolę kwalifikowanego dostawcy usług certyfikacyjnych. Pozwala to w naturalny sposób rozciągnąć zastosowanie systemu także na instytucje sektora publicznego. W efekcie z systemu korzystają obecnie ponad 3 miliony osób, a na jego bazie skonstruowano ponad 1 tys. usług zarówno sektora prywatnego, jak publicznego.

Wykorzystanie dla celów uwierzytelnienia poświadczeń zarządzanych przez podmiot zewnętrzny, publiczny lub prywatny stanowi formę federalizacji usług zaufania, która stanowi jeden z najgorętszych trendów w dyskutowanym obszarze. Wykorzystanie tożsamości sfederowanej (*federated identity*, lub usług sfederowanego zarządzania tożsamością, *federated identity management*) pozwala dostawcom usług elektronicznych oferować je bez konieczności budowy własnych mechanizmów identyfikacji, polegając na usługach świadczonych przez podmiot zewnętrzny (*identity provider*). Popularność usług sfederowanego zarządzania tożsamością doprowadziła do opracowania szeregu protokołów komunikacji pomiędzy stronami tego procesu. Wśród nich największą popularnością w sektorze B2B cieszy się protokół SAML (*Security Assertion Markup Language*), podczas gdy obszarze usług B2C coraz większą popularność zyskuje standard OpenID promowany przez OpenID Foundation.

Przykładem systemu sfederowanego zarządzania tożsamością jest portal ID-Porten stworzony przez rząd Norwegii. Portal ten pozwala rządowi, około 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 prywatny (omówiony powyżej BankID, Buypass wydawany w formie karty przez narodową loterię oraz Commfides – certyfikat PKI wydawany w formie nośnika USB). Na poziomie technicznym uczestnicy systemu ID-Porten wymieniają komunikaty w standardzie SAML 2.0. Portal świadczy obecnie usługi na rzecz ponad 3 milionów użytkowników.

Najbardziej obecnie znaczącym zarządcą tożsamości w oparciu o standard OpenID jest korporacja Google. Każdy posiadacz konta pozwalającego na korzystanie z dowolnej usługi Google może powiązać atrybuty tożsamości tego konta z unikalnym identyfikatorem OpenID, pozwalającym na łatwą identyfikację w systemach usługodawców zewnętrznych wspierających ten standard.

Google wydaje się dbać o podwyższenie poziomu bezpieczeństwa identyfikacji, od 2014 roku wspierając identyfikację dwuczynnikową, w której rolę drugiego czynnika może pełnić element sprzętowy – klucz USB Fido (*Fast Identity Online*, standard zarządzany przez FIDO Alliance) oferujący identyfikację w standardzie U2F (*Universal Second Factor*). Ograniczeniem zakresu jej zastosowania jest obecnie fakt, że wsparcie dla klucza Fido jest obecnie dostępne jedynie wewnątrz przeglądarki internetowej Chrome.

Tymczasem w Polsce...

Zarówno w sektorze publicznym, jak i prywatnym dominują elementarne modele struktury zaufania. W sektorze publicznym rozwinął się model autarkiczny, w którym każdy usługodawca buduje własną strukturę zaufania. Nie udało się osiągnąć ujednolicenia rozwiązań w gronie instytucji sektora publicznego; obok profilu zaufanego platformy ePUAP funkcjonują rozwiązania sektorowe (np. poświadczenia tożsamości stosowane przez ZUS, NFZ oraz wdrażane przez Pocztę Polską). Zapewne można by usprawiedliwić opisany stan rzeczy, gdyby poświadczenia tożsamości wdrażane przez różne podmioty reprezentowały odmienne poziomy bezpieczeństwa. Tak jednak nie jest: wymienione rozwiązania reprezentują analogiczny poziom bezpieczeństwa w rozumieniu standardu ISO/IEC 29115, w związku z czym większość z nich należy uznać za nadmiarowe. Także w sektorze prywatnym dominują rozwiązania budowane wyłącznie na własne potrzeby, w większości realizowane w standardach niepozwalających uzyskać akceptacji poza domeną dostawcy. Standardowa infrastruktura PKI, teoretycznie uniwersalna, jest wykorzystywana w ograniczonym zakresie, a zakres jej zastosowań stymulują raczej wymogi natury administracyjnej niż użyteczność biznesowa.

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 państwa, przy czym nie wszystkie uznawały umacnianie bezpieczeństwa i zaufania do dokumentu za cel pierwszoplanowy. 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. Wady merytoryczne projektu w jego pierwotnej wersji nie stały się przedmiotem szerszej dyskusji, całkowicie przesłonięte głośnym skandalem korupcyjnym związanym z realizacją innych projektów w pakiecie ówcześnie zarządzanym przez MSWiA. W toku dalszych prac legislacyjnych i technicznych wady pierwotnej koncepcji zostały usunięte, a projekt w znowelizowanej postaci doprowadzony do stadium pozwalającego wdrożyć nowy dokument oraz powiązane z nim elektroniczne usługi zaufania. Mimo tego administracja rządowa podjęła decyzję o rezygnacji z wdrożenia produktów projektu i rozpoczęciu prac nad nową koncepcją, w której nie przewidziano w dokumencie tożsamości warstwy elektronicznej, a w konsekwencji – zrezygnowano z pierwotnie planowanych, powiązanych z dokumentem usług zaufania.

W rezultacie zmian w projekcie pl.ID jedynym składnikiem powszechnej infrastruktury zaufania sektora publicznego jest obecnie tzw. profil zaufany (PZ). Liczne słabości PZ powalały traktować go dotąd jedynie jako rozwiązanie przejściowe przed wdrożeniem pl.ID. Po rezygnacji z warstwy elektronicznej w pl.ID administracja publiczna z konieczności stara się promować użycie PZ, podejmując jednocześnie działania obliczone na doraźne podniesienie jego bezpieczeństwa. Ma temu służyć m.in. przesyłanie haseł jednorazowych innym niż zasadniczy kanałem komunikacji (SMS). Nie zmienia to faktu, że PZ lokuje się obecnie na drugim poziomie wiarygodności (*level of assurance*, LoA2) w rozumieniu normy ISO 29115, a implementowane zmiany mogą podnieść jego wiarygodność do poziomu LoA3. Po modyfikacjach PZ będzie właściwym narzędziem do uwierzytelniania w usługach publicznych o charakterze

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.

informacyjnym, jednocześnie jego poziom bezpieczeństwa pozostanie niewystarczający dla składania oświadczeń woli. Administracja publiczna jest świadoma problemu zlecając wydzielenie funkcjonalności PZ ze struktury platformy ePUAP. Krok ten nie przyczynia się samoistnie do podniesienia poziomu bezpieczeństwa, jest jednak przesłanką zastąpienia w przyszłości PZ przez inną metodę identyfikacji i uwierzytelnienia. PZ nie cieszy się zaufaniem innych instytucji sektora publicznego: np. 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.

Premiera projektu pl.ID w nowej strukturze miała miejsce 1 marca 2015 r.[4]. Zasadniczą zmianą w stosunku do stanu poprzedniego jest odmiejscowienie procesów związanych z obsługą dokumentu tożsamości oraz akt stanu cywilnego. Obywatele RP mogą odtąd załatwić sprawy związane z obu obszarami w dowolnym urzędzie administracji na terenie kraju, niezależnie od aktualnego miejsca zameldowania lub zamieszkania. Zmiana, niewątpliwie korzystna dla obywateli, ma jedynie marginalne znaczenie dla ich aktywności poza sferą publiczną. Drugim efektem projektu jest wdrożenie nowego wzoru dokumentu tożsamości, w którym wprowadzono nowe zabezpieczenia o charakterze materialnym oraz ograniczono zakres informacji dotyczących posiadacza. W stosunku do dokumentu obowiązującego obecnie zabraknie informacji o adresie zameldowania posiadacza, wzroście, kolorze oczu oraz wzoru podpisu. Potencjalne skutki wprowadzonych zmian omówiono poniżej.

Nowe zabezpieczenia materialne stanowią konieczność wobec okresu życia obowiązującego wzoru dokumentu i postępu technicznego w zakresie technik umożliwiających jego naśladownictwo. Można jednak żywić wątpliwości, czy zakres wprowadzonych zmian będzie stanowić czynnik istotnie utrudniający lub ograniczający możliwości fałszerstwa. W ciągu ostatnich miesięcy pojawiały się doniesienia prasowe dotyczące internetowego handlu naśladownictwami polskiego dokumentu tożsamości, określanymi przez sprzedawców

4 Pierwotna data premiery, planowana na 1 stycznia 2015 r., została przesunięta na 1 marca 2015 r. wobec braku gotowości technicznej systemów obsługujących nowy dokument.

jako egzemplarze kolekcjonerskie. Równolegle prasa informowała o skutecznym wykorzystaniu sfałszowanych dowodów osobistych w ramach czynności prawnych dokonywanych m.in. z udziałem notariusza. Podrobione dokumenty oferowane w Internecie z pewnością zostaną rozpoznane jako fałszerstwa w trakcie badania prowadzonego przez przeszkolonego fachowca. Praktyka potwierdza jednak, że rozwiązania techniczne dostępne fałszerzom pozwalają na produkcję naśladownictw dowodu osobistego, które są i będą akceptowane w trakcie rutynowych czynności, także tych realizowanych z udziałem funkcjonariuszy publicznych zobowiązanych do zachowania szczególnej staranności. Wszelkie nowinki w zakresie zabezpieczeń o charakterze materialnym będą szybko równoważone przez postęp w zakresie technik produkcji, w szczególności spektakularny rozwój technik druku trójwymiarowego. W tej sytuacji wydaje się bezsporne, że wprowadzany wzór dokumentu tożsamości szybko ulegnie moralnemu zużyciu i zaistnieje konieczność zastąpienia go nowym dokumentem, łączącym zabezpieczenia o charakterze materialnym i informacyjnym. Bulwersującym aspektem wdrożenia nowego wzoru dokumentu jest spóźniona notyfikacja jego wzoru agendom UE, w której konsekwencji w okresie przejściowym posiadacze nowego dowodu mogą być narażeni na niedogodności, z deportacją do kraju włącznie.

Brak w dokumencie informacji o kolorze oczu i wzroście nie ma istotnego znaczenia. Potencjalnie ważniejsza jest zmiana wymagań dotyczących fotografii posiadacza dokumentu: do wniosku o wydanie nowego dowodu osobistego należy dołączyć fotografię w standardzie obowiązującym dotąd w odniesieniu do zdjęć paszportowych, pozwalającą na określenie cech biometrycznych wizerunku posiadacza. Potencjalnie istotna nowość jest jednak pozbawiona znaczenia praktycznego zważywszy, że brak warstwy elektronicznej nie pozwala na zapisanie w dokumencie opisu biometrycznego, a w konsekwencji wykorzystania metod biometrii dla potwierdzenia tożsamości posiadacza.

Najbardziej ożywioną dyskusję budzi brak w nowym wzorze dokumentu adresu zameldowania i wzoru podpisu posiadacza. Ustawa o ewidencji ludności z 2010 r.[5] przewidywała, że 1 stycznia 2014 r. nastąpi zniesienie obowiązku meldunkowego, zaś jej nowelizacja z 2012 r.[6] przesunęła tę datę na 1 stycznia 2016 r. W tym stanie prawnym logiczna była decyzja zespołu pracującego nad wzorem nowego dokumentu tożsamości o rezygnacji z uwzględnienia adresu

5 Dz. U. 2010 nr 217 poz. 1427.

6 Dz. U. 2012 nr 0 poz. 1407.

zameldowania w jego treści. Jednakże po zatwierdzeniu wzoru nowego dokumentu sytuacja ulegała (i ulega) dynamicznym zmianom. W końcówce 2014 r. międzyresortowy zespół powołany do oceny skutków rezygnacji z obowiązku meldunkowego zauważył, że jego konsekwencją winna być zmiana ponad 100 ustaw zawierających odniesienia do adresu zameldowania, ponadto rezygnacja z adresu zameldowania utrudnia lub uniemożliwia realizację niektórych zadań państwa (m.in. w sferze obronności, wyborów, obowiązku szkolnego, itd.). W efekcie zespół rekomendował utrzymanie obowiązku meldunkowego. Bezpośrednio przed oddaniem niniejszego tekstu do druku media przyniosły jednak informację, że wbrew rekomendacji MSW rozważa zastąpienie adresu zameldowania inną formą rejestracji miejsca zamieszkania, obligując zespół międzyresortowy do opracowania jej propozycji.

Dyspozycję tę należy przyjąć z satysfakcją: jeżeli państwo nie może obejść się bez jakiejś formy kontaktu z obywatelem, nie musi to być forma w swej istocie represyjna[7], odziedziczona po dawnym systemie politycznym. O ile niektóre zadania państwa istotnie wymagają znajomości miejsca zamieszkania obywatela, dla realizacji większości wystarczające jest określenie go w rozumieniu przepisów Kodeksu Cywilnego, tj. z dokładnością do miejscowości. Większość czynności administracyjnych, prawnych i faktycznych wymaga nie tyle znajomości adresu zameldowania lub zamieszkania strony, ile określenia sposobu powiadamiania zapewniającego skuteczność prawną doręczeń. Pozostaje mieć nadzieję, że wiedza i wyobraźnia zespołu międzyresortowego okażą się wystarczające, by dopuścić możliwość deklarowania jako rejestrowanego adresu dla powiadomień także adresu elektronicznego. Będzie to możliwe m.in. dzięki opisanym w następnym rozdziale usługom rejestrowanego doręczenia elektronicznego, przewidzianym w Rozporządzeniu Parlamentu Europejskiego i Rady UE 910/2014.

Jakiekolwiek rozwiązania przyjmie w przyszłości MSW w dyskutowanym obszarze, eliminacja adresu posiadacza z treści dokumentu tożsamości oznacza okres trudności dla obywateli RP i sektora prywatnego. Podmioty komercyjne zostaną zmuszone do przeglądu procedur operacyjnych i uwzględnienia w nich dwóch wariantów weryfikacji adresu klientów – dla posiadaczy dowodów osobistych starego i nowego wzoru. W przypadku posiadaczy dowodów

7 Świeżym przykładem represyjności systemu jest opisywany w mediach przypadek odmowy nadania dziecku numeru Pesel ze względu na brak stałego adresu zameldowania jego rodziców (wynikający z kolei z braku zgody na meldunek ze strony właściciela wynajmowanego przez nich lokalu).

nowego wzoru możliwa będzie weryfikacja adresu zameldowania w trybie określonym w art. 44h ust. 5 i 6 ustawy o ewidencji ludności i dowodach osobistych. Zgodnie z przepisami ustawy dane z rejestrów udostępniane będą podmiotom, które *posiadają urządzenia umożliwiające identyfikację osoby uzyskującej dane w systemie oraz zakresu, daty i celu ich uzyskania* oraz *zabezpieczenia techniczne i organizacyjne uniemożliwiające wykorzystanie danych niezgodnie z celem ich uzyskania*. Ustawa przewidziała określenie przez Radę Ministrów wzorów wniosków o udostępnienie lub weryfikację danych oraz wysokości i trybu wnoszenia opłat z ich tytułu. Nie przewidziano natomiast określenia wymagań dotyczących identyfikacji osób uzyskujących informacje oraz stosowanych zabezpieczeń. Aby uniknąć arbitralnych decyzji w zakresie udostępniania i weryfikacji danych konieczne będzie jednak wypracowanie jednolitych kryteriów, które w istniejącym stanie formułowane będą już w toku stosowania przepisów ustawy. Warto też zauważyć, że weryfikacja danych osobowych będzie czynnością odpłatną – rozporządzenie RM[8] określiło wysokość opłaty za jednostkową weryfikację na 30 groszy. Inną potencjalną niedogodnością dla instytucji finansowych będzie konieczność weryfikacji w dwóch niezależnych źródłach, czy przedstawiany dowód osobisty nie został zarejestrowany w zbiorze dokumentów zastrzeżonych. W odniesieniu do dokumentów wydawanych dotąd zbiorem referencyjnym takich dokumentów był rejestr prowadzony przez banki pod auspicjami ZBP. W nowym systemie MSW będzie prowadzić ewidencję wydanych i unieważnionych dowodów osobistych, która w zamyśle winna zastąpić rejestr prowadzony przez banki. Tym niemniej, w znaczącym okresie przejściowym obie ewidencje będą uzupełniać się nawzajem.

Mimo oczekiwanych, przejściowych niedogodności związanych z nowym wzorem dowodu należy docenić potencjalne zalety braku danych adresowych i wzoru podpisu w dokumencie tożsamości. W przeszłości ukształtowała się praktyka, w myśl której dane zawarte w przedstawionym dokumencie tożsamości uznawano za wystarczające dla realizacji licznych czynności prawnych, np. zawarcia umowy rachunku bankowego. W rezultacie utracony lub skradziony dowód osobisty (jeżeli nie został wystarczająco prędko zarejestrowany w bazie dokumentów zastrzeżonych), ewentualnie dokument sfałszowany na tyle profesjonalnie, by nie wzbudzić wątpliwości pracownika pierwszego

8 Rozporządzenie Rady Ministrów z dnia 12.09.2011 r. w sprawie opłat za udostępnienie danych z rejestrów mieszkańców, rejestrów zamieszkania cudzoziemców oraz rejestru PESEL, Dz. U. nr 195 poz. 1153.

kontaktu, okazywały się wystarczające dla realizacji czynności bez weryfikacji zawartych w nim danych. Brak w dokumencie istotnych informacji zmusza stronę czynności do pozyskania ich ze źródeł zewnętrznych i/lub weryfikacji informacji podanych przez osobę legitymującą się dokumentem. Jeżeli MSW zdoła zaprojektować procedury gromadzenia i udostępniania danych adresowych w sposób inteligentny i uwzględniający potrzeby biznesu, system jako całość stanie się bardziej odporny na próby nadużyć.

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 (deklaracje ZUS i wymóg sygnowania nimi począwszy od 2015 r. sprawozdań PIT i CIT) niż rzeczywistej użyteczności. 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, nieformalna i wysoce niefortunna próba konstrukcji systemu sfederowanego zarządzania tożsamością. Mowa o uwierzytelnieniu klientów banków przez realizację przelewów z innej instytucji, w której dany podmiot posiada rachunek. System bazuje na założeniu, że właściwa identyfikacja klienta nastąpiła w źródłowej instytucji finansowej w wyniku zastosowania przepisów ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[9]. Praktyka potwierdza, że system jest funkcjonalny, jednak funkcjonalność stanowi jego jedyną zaletę. Jego działanie nie opiera się na jasno sprecyzowanych przepisach prawa, a jedynie na ich daleko idącej interpretacji. System nie zawiera żadnych mechanizmów pozwalających na korektę i ograniczenie skali propagacji pierwotnego błędu lub nadużycia. Obserwujemy coraz liczniejsze przypadki kradzieży tożsamości i/lub przejęcia przez cyberprzestępców kontroli nad rachunkiem bankowym ofiary.

9 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.

Funkcjonowanie opisanego systemu identyfikacji pozwala przekształcić incydentalne włamanie w łańcuch rachunków powiązanych z tożsamością ofiary, zakładanych bez ograniczeń w kolejnych instytucjach finansowych i wykorzystywanych dla dalszej, przestępczej działalności. Potencjalny efekt kaskadowy takiego procederu rodzi poważne ryzyko dla sektora finansowego, dlatego milcząca akceptacja jego nadzorców dla funkcjonowania kontrowersyjnego schematu zarządzania tożsamością jest niezrozumiała. Byłoby niefortunne, gdyby na rozwiązanie problemu przyszło czekać do chwili, gdy rachunek bankowy znaczącego polityka zostanie przejęty, sklonowany i wykorzystany np. dla działalności związanej z praniem brudnych pieniędzy lub finansowaniem terroryzmu. Z drugiej strony sam fakt funkcjonowania systemu, z którym wiąże się wysoki poziom ryzyka, ilustruje pilną potrzebę stworzenia powszechnie akceptowanego systemu zarządzania elektroniczną tożsamością.

eIDAS

W nadchodzących latach zasadniczym czynnikiem kształtującym infrastrukturę zaufania w krajach UE będą prace związane z implementacją Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie *identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych*[10]. Rozporządzenie zostało przyjęte wcześniej od oczekiwań ekspertów, jednak jego szybka akceptacja była możliwa w głównej mierze dzięki przeniesieniu większości problemów wymagających rozwiązania do aktów wykonawczych oraz założeniu sfinalizowania w porę prowadzonych równolegle prac nad uzupełnieniem struktury standardów technicznych. Formalnie rozporządzenie eIDAS weszło w życie z dniem 17 września 2014 roku, jednak sekwencja zdarzeń, które mają doprowadzić do jego pełnego zastosowania jest złożona:

- rozporządzenie przewiduje wydanie jednego aktu delegowanego i do 28 aktów wykonawczych[11],
  - przewiduje się, że prace nad przepisami dotyczącymi proceduralnych warunków ułatwiania współpracy między państwami członkowskimi (art. 12.7 eIDAS) zostaną zakończone do 18 marca 2015 roku,

10 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, skrótowo określane mianem eIDAS.

11 Niektóre z aktów wykonawczych przewidzianych w rozporządzeniu mają charakter opcjonalny, toteż ich wydanie nie jest przesądzone.

- do 1 lipca 2015 roku KE winna ogłosić przepisy dotyczące funkcjonowania znaku zaufania UE dla kwalifikowanych usług zaufania; wcześniej, 23 kwietnia 2015, ma nastąpić ogłoszenie wyników konkursu na formę graficzną znaku,
- do 18 września 2015 roku winno nastąpić ogłoszenie przepisów dot. ram interoperacyjności eID (art. 12.8), poziomów zaufania eID (art. 8.3), numerów referencyjnych norm dotyczących zaawansowanych podpisów elektronicznych (art. 27.4), technicznych specyfikacji i formatów dotyczących zaufanych list (art. 22.5) oraz numerów referencyjnych norm dotyczących zaawansowanych pieczęci elektronicznych (art. 37.4),

- z dniem 18 września 2015 roku przewidziano możliwość dobrowolnego uznania przez państwa członkowskie schematów identyfikacji stosowanych w innych krajach,
- z dniem 1 lipca 2016 roku wejdą w życie przepisy dotyczące usług zaufania,
- z dniem 18 września 2018 roku uznanie schematów identyfikacji stosowanych w innych państwach członkowskich stanie się obligatoryjne.

O ile wydanie w założonych terminach samych przepisów wykonawczych do rozporządzenia wydaje się realne, terminarz skorelowania z przepisami eIDAS istniejących i zatwierdzenia brakujących standardów technicznych jest napięty. W ramach przygotowań do wdrożenia eIDAS KE już w 2009 r. nadała europejskim organizacjom normatywnym (CEN, CELEC i ETSI) mandat M/460 dotyczący przeglądu istniejącej bazy standardów technicznych w obszarze usług zaufania i przygotowania jej racjonalizacji pod kątem planowanego rozporządzenia. W ramach przeglądu CEN i ETSI uznały, że istniejące standardy techniczne w analizowanym obszarze tworzą złożoną mozaikę o niejasnej strukturze, w wielu obszarach zachodząc wzajemnie na swoje sfery oddziaływania. W rezultacie obie organizacje stworzyły plan racjonalizacji struktury standardów, zakładający precyzyjne rozgraniczenie pomiędzy sześcioma obszarami dotyczącymi następujących sfer oddziaływania:

- zarządcy list określających status dostawców usług zaufania,
  - dostawcy usług podpisu elektronicznego,
  - dostawcy złożonych usług zaufania (w szczególności rejestrowana poczta elektroniczna i przechowanie informacji),
- tworzenie i weryfikacja podpisów elektronicznych,
  - bezpieczne urządzenia do tworzenia podpisu,
  - biblioteki kryptograficzne.

Samo podjęcie prac nad nową strukturą regulacji i standardów 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 aktu:

1. Unia Europejska zdecydowała się sięgnąć po formułę rozporządzenia, a nie dyrektywy. Rozporządzenie, obowiązujące na terenie UE wprost, bez konieczności transpozycji jego postanowień do prawa krajowego, jest narzędziem bardziej skutecznym od dyrektywy i natychmiastowym w działaniu. Jak się wydaje, UE ma świadomość rozchodzenia się praktyki funkcjonowania usług zaufania w krajach UE z celami określonymi w Agendzie Cyfrowej 2020.
2. Rozporządzenie znacząco poszerza listę usług zaufania w stosunku do wcześniejszej legislacji. Obok tradycyjnego podpisu elektronicznego (sekcja IV) w rozporządzeniu pojawiają się koncepcje cyfrowej pieczęci (sekcja V), elektronicznych znaczników czasu (sekcja VI), usług rejestrowanego doręczenia elektronicznego (sekcja VII) i uwierzytelniania witryn internetowych (sekcja VIII).
3. Rozporządzenie pozwala stosować różne schematy identyfikacji i uwierzytelnienia (w tym także niekwalifikowane) po przeprowadzeniu analizy ryzyka ich zastosowania i w zakresie zgodnym z wynikami tej analizy (zgodnie z poziomami bezpieczeństwa określonymi w ISO 29115 i projekcie Stork).
4. Rozporządzenie pozwala stosować nowe, nieprzewidziane w dotychczasowej dyrektywie schematy identyfikacji i uwierzytelnienia, m.in. w formie zakładającej powierzanie kwalifikowanych urządzeń do składania podpisu elektronicznego stronie trzeciej (*server-side signatures*).
5. Konsekwencją rozporządzenia jest stworzenie pan-europejskiej infrastruktury usług zaufania, współtworzonej przez usługi notyfikowane KE przez poszczególne kraje członkowskie. Notyfikowane usługi z definicji są uznawane we wszystkich krajach UE, pod warunkiem, że *notyfikujące państwo członkowskie zapewnia dostępność uwierzytelniania online, tak aby każda strona ufająca mająca siedzibę na terytorium innego państwa członkowskiego mogła potwierdzić dane identyfikujące osobę otrzymane w postaci elektronicznej*.

Najważniejszą innowacją jest jednak zasadnicze przesunięcie akcentów odpowiedzialności za realizację usług zaufania. Struktura dyrektywy o podpisie elektronicznym powierzała budowę infrastruktury zaufania w zasadzie instytucjom sektora prywatnego, zastrzegając dla państwa regulację i nadzór.

Art. 2 ust.1 nowego rozporządzenia stanowi, że *rozporządzenie ma zastosowanie do systemów identyfikacji elektronicznej, które zostały notyfikowane przez państwo członkowskie, oraz do dostawców usług zaufania mających siedzibę w Unii*. Art. 7 precyzuje, że przedmiotem notyfikacji może być system identyfikacji elektronicznej, w którym środki identyfikacji są wydawane *przez notyfikujące państwo członkowskie* (...), *na mocy upoważnienia od notyfikującego państwa członkowskiego* (lub)*niezależnie od notyfikującego państwa członkowskiego* (lecz)*są uznawane przez to państwo członkowskie* (oraz)*mogą być używane w celu uzyskania dostępu do co najmniej jednej usługi świadczonej przez podmiot sektora publicznego.* Przyjmując rozporządzenie UE zajęła stanowisko zgodnie z którym usługi zaufania stanowią część ogólnej infrastruktury publicznej, za której budowę i utrzymanie odpowiedzialne są kraje członkowskie; 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 uznane przez państwo i akceptowane jako środek dostępu do co najmniej jednej usługi publicznej.

Wśród usług zaufania przewidzianych w rozporządzeniu najbardziej istotną nowością wydaje się być usługa rejestrowanego doręczenia elektronicznego, stanowiąca elektroniczny odpowiednik tradycyjnej, pocztowej przesyłki rejestrowanej (listu poleconego). Systemy o funkcjonalności rejestrowanego doręczenia elektronicznego funkcjonują już w kilku krajach europejskich. W Norwegii administratorem takiego systemu jest ten sam podmiot, który zarządza opisanym wcześniej systemem sfederowanej tożsamości ID-Porten. Warto zauważyć, że na mocy ustawy Stortingu wszelka komunikacja pomiędzy obywatelem i agendami administracji publicznej jest realizowana standardowo w trybie elektronicznym, choć obywatel dysponuje opcją *opt-out*, pozwalającą przywrócić tradycyjny tryb. W Niemczech 2 maja 2011 roku weszła w życie ustawa tworząca podstawy prawne dla funkcjonowania systemu DE-Mail, pozwalającego na elektroniczną wymianę wiążących prawnie dokumentów pomiędzy obywatelami, podmiotami publicznymi i prywatnymi. Definiując standardy techniczne i aspekty prawne funkcjonowania systemu państwo nie pełni jednocześnie roli dostawcy usługi. W chwili obecnej dostawcami usług DE-Mail są cztery podmioty prywatne, trwa akredytacja

w systemie następcy prawnego dawnej poczty państwowej, Deutsche Post AG. Warto zauważyć, że struktura systemu ePUAP umożliwia względnie łatwą organizację usługi rejestrowanego doręczenia elektronicznego na bazie jego funkcjonalności. Ewentualne, przyszłe dostosowanie struktury ePUAP do standardów technicznych wydanych w kontekście rozporządzenia eIDAS może samo przez się zapewnić biznesowe uzasadnienie dla dalszego funkcjonowania platformy (przy założeniu, że prace wspomnianego wyżej zespołu międzyresortowego dopuszczą adres elektroniczny jako rejestrowany adres dla powiadomień oraz że funkcjonalność skrzynki ePUAP stanie się dostępna także dla podmiotów niepublicznych).

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 itd.), 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, 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, preferując rozwiązania pozwalające całkowicie uniknąć jego podejmowania 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.

Andrzej Kawiński

Country Manager Banknote Processing w firmie Giesecke & Devrient GmbH od 1 marca 2014 roku. Absolwent Politechniki Warszawskiej i Automatyki Procesów Technologicznych. W 2005 r. ukończył studia Executive MBA w Gdańskiej Fundacji Kształcenia Menedżerów we współpracy z Rotterdam School of Management i Uniwersytetem Gdańskim.

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

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

Andrzej Kawiński

Zarządzanie obrotem gotówki – nowe wyzwania proceduralne i technologiczne

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

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

Wytwarzanie monet ze złota i srebra było bardzo kosztowne, a ilość dostępnych metali do produkcji monet nie zaspokajała potrzeb. Bezpieczeństwo przechowywania dużych ilości monet stawało się problemem, zaczęto więc zastawiać zasoby u złotników otrzymując jako potwierdzenie kwit depozytowy. Regulował on wzajemne zobowiązania pomiędzy złotnikiem a właścicielem monet. Z czasem kwit depozytowy stał się dokumentem, na podstawie którego złotnik wypłacał należność okazicielowi. Ludzie coraz częściej regulowali swoje zobowiązania za ich pomocą. Złotnicy, którzy stali się pierwszymi bankierami wystawiali je nie tylko potwierdzając zdeponowanie kruszców, ale również udzielając pożyczek. Odsetki od wystawionych w ten sposób

kwitów depozytowych stały się dodatkowym dochodem bankierów. Wydawane kwity depozytowe zostały zatwierdzone przez Państwo i stały się przodkiem dzisiejszego pieniądza papierowego. Państwa zaczęły wydawać rozporządzenia regulujące obrót kwitami depozytowymi, jednocześnie ustanawiając bank będący emitentem kwitów. Regulacje te miały na celu likwidację chaosu powstałego przez emisję różnych banknotów indywidualnie przez każdy z banków. Z czasem banki emitujące pieniądze zostały upaństwowione, wiążąc je z centralną władzą monetarną.

Historię weksli datuje się na XVI wiek. Dopiero w tym okresie czasu we Włoszech zaczęto odróżniać weksle trasowane, płatne w jakimś określonym terminie, od weksli trasowanych płatnych za okazaniem, czyli płatnych w każdej chwili. Jeśli trasat, czyli ten, który miał zapłacić za weksel, był mocnym i znanym bankierem, weksle te nazywano czekami (od nazwiska rodu włoskiego Ceccinich). Czeki, w odróżnieniu do weksli, stały się środkiem płatniczym początkowo używanym we Włoszech, ale z czasem stały się popularnym narzędziem również w krajach Europy Zachodniej, głównie Belgii, Holandii i Anglii. 19 marca 1931 roku w Genewie zostały uchwalone konwencje w przedmiocie wprowadzenia jednolitego prawa czekowego. Na konwencjach tych oparta jest obowiązująca do dnia dzisiejszego w Polsce ustawa z dnia 28 kwietnia 1936 roku – Prawo czekowe.

Pierwsze karty płatnicze pojawiły się w Stanach Zjednoczonych na początku XX wieku. Były one wystawiane przez sieci sklepów i stacje benzynowe. Umożliwiały wydanie towaru i zapisanie kredytu na poczet klienta. W roku 1914 firma Western Union wprowadziła pierwsze karty obciążeniowe. Dopiero w roku 1950 powstała firma Diners Club, która zajmowała się wydawaniem kart umożliwiających bezgotówkowe regulowanie płatności w hotelach i restauracjach.

Najnowszą formą zapłaty są płatności telefonem komórkowym (płatności mobilne). Ta forma płatności znana jest od kilku lat, a Polska stała się w tej dziedzinie światowym liderem. W roku 2013 jako pierwszy na skalę ogólnokrajową taką formę płatności wprowadził Bank PKO BP (system IKO), a kilka miesięcy później Bank Pekao S.A. oferując system PeoPay.

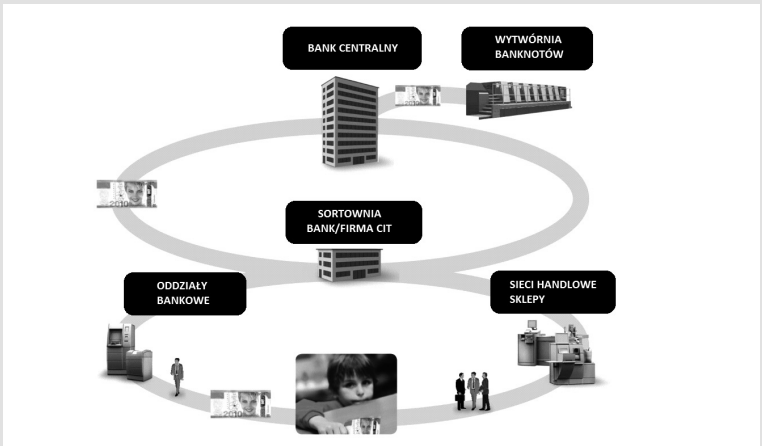
Czy nowe formy płatności są w stanie zastąpić gotówkę? Szybkość transakcji, bezpieczeństwo a także rewolucja mobilna to czynniki, za pomocą których instytucje finansowe starają się przekonać społeczeństwo do zmiany dotychczasowych zwyczajów płatniczych. Duża sieć terminali płatniczych z technologią płatności bezstykowych jest jedną z cech mającą wpływ na szybkość

transakcji. Starsze modele płatności kartą, związane z czasem trwania autoryzacji, przegrywały z szybką płatnością gotówką. Bezpieczeństwo transakcji, szczególnie w kanale mobilnym, będzie jednym z trendów technologicznych instytucji finansowych w najbliższych latach. Zbudowanie świadomości klientów, jak bezpiecznie realizować transakcje w kanale mobilnym może zapobiec dużej liczbie fraudów i przekonać użytkowników do realizowania swoich zobowiązań tą metodą. Płatności mobilne w sposób naturalny zastępować będą płatności kartowe, wyzwaniem będzie jednak zmniejszenie liczby płatności gotówkowych. Historia pokazuje, że całkowite zastąpienie gotówki innymi formami płatności jest niemożliwe.

Cykl obrotu gotówki w gospodarce

Typowy cykl obrotu gotówki można przedstawić za pomocą następującego schematu.

Cykl obrotu gotówki



Giesecke & Devrient

W Polsce Państwowa Wytwórnia Papierów Wartościowych (PWPW) na zlecenie Narodowego Banku Polskiego produkuje banknoty. Narodowy Bank Polski wprowadza pieniądze do obrotu zasilając banki. Większość instytucji finansowych w Polsce już od kilku lat zleciła procesowanie gotówki wyspecjalizowanym firmom CIT (Cash in Transit). Firmy te na zlecenie banków

odbierają gotówkę z Narodowego Banku Polskiego, a następnie w swoich sortowniach przygotowują zasiłki oddziałów bankowych i bankomatów. Społeczeństwo, pobierając gotówkę w oddziałach bankowych oraz bankomatach, uzyskuje środki do realizacji swoich potrzeb. Zapłata za towary powoduje przekazanie gotówki od obywateli do przedsiębiorcy będącego dostawcą towaru. Przedsiębiorcy deponują gotówkę w banku. Funkcję tą typowo świadczą firmy CIT, które na zlecenie banku odbierają gotówkę od przedsiębiorców, przeliczają wpłaty i księgują na odpowiednich kontach. Firmy CIT odbierają również gotówkę wpłaconą w oddziałach bankowych. Gotówka przeliczana w sortowniach jest dzielona na pieniądze o dobrej jakości, które mogą wrócić do ponownego obrotu w gospodarce, i destrukty, które muszą być przekazane do Narodowego Banku Polskiego. Każdego dnia banki podejmują decyzję, jaka część odebranej z rynku gotówki jest nadmiarowa i powinna być przekazana do depozytu NBP, zmniejszając w ten sposób obowiązkową rezerwę. Pozostałe środki wracają do ponownego obiegu w gospodarce (zasilenia oddziałów i bankomatów). Usługę transportu wykonują na zlecenie banków firmy CIT.

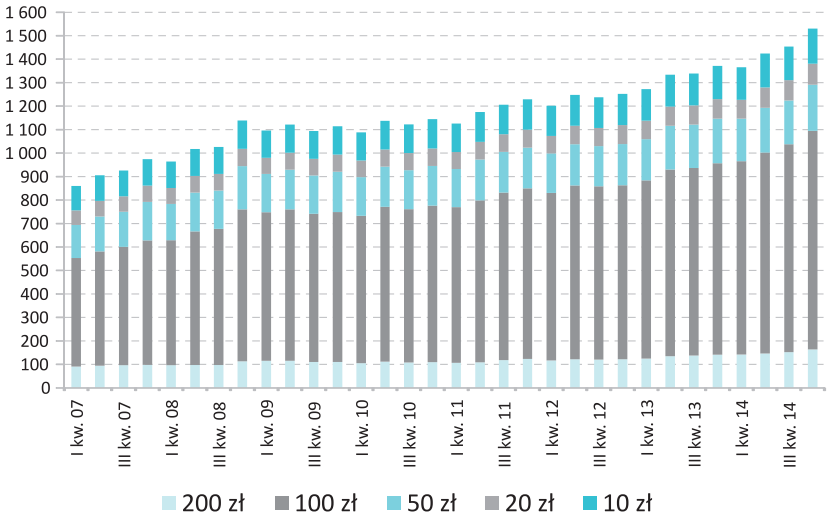
Firmy CIT realizują usługi dla wielu instytucji finansowych. Każda z sortowni przyjmuje depozyty różnych banków. Gotówka jednego banku nie może być fizycznie mieszana z gotówką innego banku. Przeliczone i spakowane banknoty przechowywane są w skarbcu w oddzielnych szafach. Gotówka deponowana w Narodowym Banku Polskim po przeliczeniu i sprawdzeniu jakościowym wraca ponownie do obiegu. Depozyty NBP przechowywane są przez Bank Centralny i usługa ta nie jest obecnie zlecana firmom zewnętrznym zajmującym się procesowaniem gotówki.

Przedstawiony model obrotu gotówki jest typowy również dla innych państw. Analizując poszczególne etapy można szukać optymalizacji kosztów, np. zmniejszając strumień pieniędzy wracających do Banku Centralnego. Wymaga to jednak zrozumienia przedstawionych dalej zadań Narodowego Banku Polskiego, oczekiwań instytucji finansowych oraz firm zajmujących się transportem i liczeniem gotówki.

Ilość gotówki w obiegu

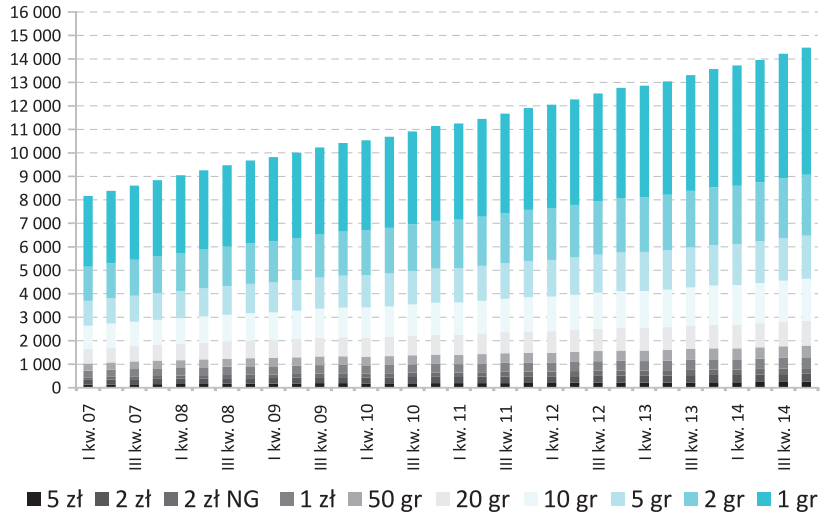
W lutym 2015 roku Departament Emisyjno-Skarbcowy Narodowego Banku Polskiego opublikował strukturę (liczbę oraz wartości) banknotów i monet będących w powszechnym obiegu w Polsce.

Struktura obiegu banknotów w mln szt.:



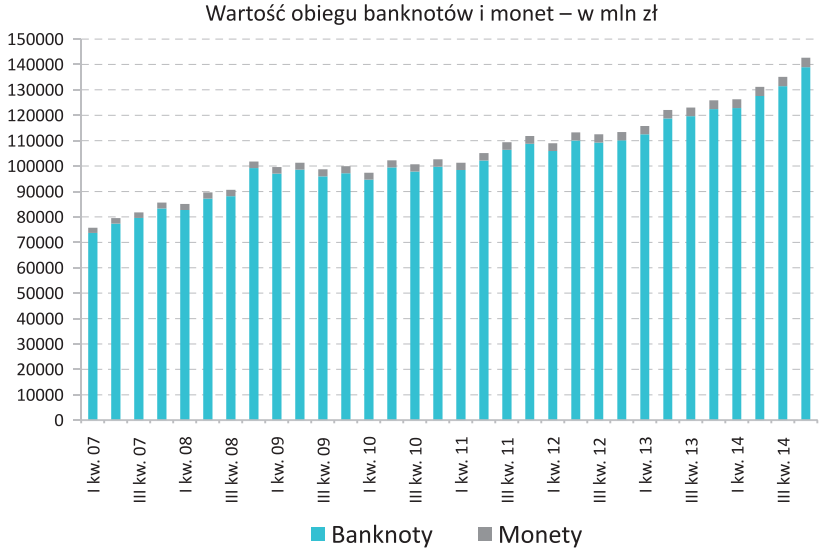
Podane dane wskazują, że liczba banknotów w obiegu w ciągu ostatnich siedmiu lat prawie się podwoiła. Na koniec pierwszego kwartału 2007 roku, według danych NBP, w obiegu było 860 mln banknotów, natomiast na koniec czwartego kwartału 2014 roku 1530,3 mln. Oznacza to średni roczny wzrost na poziomie 10%.

Struktura obiegu monet w mln szt.:



W tym samym okresie liczba monet w obiegu również wzrosła. Na koniec pierwszego kwartału 2007 roku według danych NBP w obiegu było 8 162,7 mln sztuk, a na koniec czwartego kwartału 2014 roku – 14 480,6 mln. Dane te wskazują również na średni roczny wzrost w wysokości 10%.

Narodowy Bank Polski publikuje również dane dotyczące wartości gotówki będącej w obiegu.



Podane przez NBP dane wskazują wzrost wartości z poziomu 75 776,5 mln zł na koniec pierwszego kwartału 2007 roku do poziomu 142 661 mln zł na koniec czwartego kwartału 2014 roku. Średni roczny wzrost to około 12%.

Dane statystyczne wskazują na stale rosnącą liczbę gotówki w obiegu. Automatyzacja procesów liczenia oraz lepsze zarządzanie cyrkulacją gotówki wydają się jedyną drogą do ograniczenia kosztów obrotu gotówkowego w gospodarce.

Zgodnie z raportem opracowanym przez Tomasza Koźlińskiego i opublikowanym przez Departament Systemu Płatniczego NBP w maju 2013 roku gotówka jest dominującym sposobem płatności Polaków z blisko 82% udziałem w ogólnej liczbie płatności dokonywanych przez osoby fizyczne. Analizy prezentowanych przez firmę Deloitte w czasie Seminarium „IT w Instytucjach Finansowych" w marcu 2014 roku prognozują spadek udziału płatności gotówkowych w najbliższych latach do poziomu 61% w roku 2017. Czas pokaże,

czy zaprezentowana analiza stanie się rzeczywistością. Ostatni kryzys światowy po upadku Banku Lehman Brothers spowodował zwiększenie transakcji gotówkowych kosztem pozostałych form zapłaty. Innym przykładem może być sytuacja w Japonii, gdzie duża liczba dziennych wypłat i wpłat gotówki spowodowała rozwój bankomatów recyclingowych z zamkniętym obiegiem.

Średnia wartość transakcji gotówkowej według analiz NBP wynosi 38 zł, a transakcje do kwoty 20 zł stanowią połowę wszystkich transakcji gotówkowych.

Zadania Narodowego Banku Polskiego

Narodowy Bank Polski (NBP) zapewnia sprawne działanie systemu płatniczego, umożliwiającego szybki i bezpieczny przepływ pieniędzy zarówno pomiędzy obywatelami, jak i podmiotami gospodarczymi. NBP ma wyłączne prawo emitowania znaków pieniężnych Rzeczypospolitej Polskiej. Oznacza to, że jest jedyną instytucją uprawnioną do wprowadzania do obiegu pieniężnego złotych i groszy jako prawnych środków płatniczych na obszarze Polski. Mają one ustawową moc zwalniania ze wszystkich zobowiązań i nikt nie może odmówić ich przyjęcia jako zapłaty.

Znakami pieniężnymi emitowanymi przez NBP są banknoty i monety. Monety emitowane są w dwóch grupach. Pierwszą tworzą monety powszechnego obiegu, a drugą monety kolekcjonerskie o niskich nakładach.

Narodowy Bank Polski ustala też zasady wymiany zużytych i uszkodzonych znaków pieniężnych oraz zatrzymywania fałszywych znaków pieniężnych. Znaki zużyte lub uszkodzone tracą moc prawnego środka płatniczego i podlegają wymianie. Fałszywe znaki pieniężne są natomiast zatrzymywane bez prawa zwrotu ich równowartości.

W przyszłości, po przyjęciu euro jako prawnego środka płatniczego emitentem banknotów będzie Europejski Bank Centralny, natomiast NBP pozostanie emitentem monet.

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

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

Wymieniona rekomendacja jest pierwszym tego typu dokumentem tak szczegółowo opisującym standard banknotów, które trafiają do obiegu. W strefie Euro, jak również w innych krajach takie regulacje obowiązują już od kilku lat. Brak do tej pory w Polsce tak szczegółowych standardów powodował, że ocena stanu jakości banknotu była bardzo subiektywna i w różnych sortowniach różnie interpretowana. Ustawienie sorterów i zdefiniowanie poziomu jakości banknotów obiegowych zależało od indywidualnych preferencji kierownika sortowni.

Zmiana standardu obsługi w oddziałach bankowych

W ostatnich latach wygląd oddziałów bankowych uległ dużej zmianie. Te tradycyjne „ciężkie", z dużą powierzchnią, zostały zastąpione „lekkimi" małymi placówkami. Niskie koszty utrzymania oraz możliwość szybkiego zamknięcia lub przeniesienia placówki z jednej strony oraz zmiana charakteru funkcjonalnego z drugiej to główne czynniki kształtujące wygląd obecnych oddziałów bankowych. W tradycyjnych placówkach podstawą był skarbiec, gdzie przechowywano między innymi środki pieniężne. Koszt oraz czas budowy skarbca uniemożliwiał szybką relokację placówki. Obecne nowoczesne placówki bankowe nie są wyposażane w skarbce. Potrzebna dla codziennej obsługi klientów gotówka jest deponowana w szafie transferowej przez firmy konwojujące. W ciągu dnia gotówka jest przechowywana w szafkach kasjerskich (multisejfy) lub w dyspenserach. Certyfikowane klasy sejfów tych urządzeń zapewniają bezpieczny poziom przechowywania wartości.

Powszechność wypłat w bankomatach oraz stale rosnąca liczba płatności elektronicznych powoduje, że obsługa gotówki nie jest głównym zadaniem placówki bankowej. Obecnie oddziały bankowe to miejsca sprzedaży usług finansowych. Zamiast kasjerki, instytucje finansowe zatrudniają sprzedawców lub konsultantów, których zadaniem jest sprzedaż produktów bankowych. Otwarta przestrzeń, kontakt przez biurko, rozmowa na siedząco to czynniki, które mają wpływ na zwiększenie sprzedaży. Zdeponowanie lub podjęcie gotówki przez klienta nie jest podstawową funkcją oddziału. Celem realizacji

tych czynności oddziały bankowe są wyposażane w urządzenia do liczenia, rozpoznawania oraz przechowywania gotówki.

Firmy Cash in Transit

Zmiana wyglądu i ilości placówek bankowych, jak również stale zwiększająca się liczba urządzeń samoobsługowych spowodowała powstanie nowych usług związanych z przeliczaniem i sortowaniem gotówki. Zwiększyła się również ilość, określonych odpowiednimi przepisami, usług konwojowania gotówki. Większość banków zdecydowała się w tym zakresie na zlecenie tych usług podmiotom zewnętrznym – tzw. firmom CIT (Cash in Transit). Zakres oferowanych przez te firmy usług jest coraz szerszy i obejmuje między innymi:

- obsługę gotówkową oddziałów bankowych – rozliczenia, transport, sortowanie nominałów, przygotowywanie zasiłków,
- obsługę gotówkową urządzeń samoobsługowych – rozliczenie urządzeń, ładowanie gotówki do kaset, transport i załadunek kaset,
- obsługę gotówkową klientów banków – odbiór zamkniętych depozytów, rozliczenia i księgowanie depozytów, sortowanie nominałów, przygotowywanie zasiłków,
- przechowywanie gotówki banku w skarbcach,
- transport gotówki pomiędzy sortownią a oddziałami NBP.

Szeroki zakres oferowanych usług i scedowanie większości procesów związanych z obsługą gotówki przez banki na rzecz firm CIT spowodował, że dzisiaj te firmy są odpowiedzialne za jakość wprowadzanych na rynek banknotów. W całym obiegu gotówki można wskazać procesy, w których banknoty wpłacane do banku a następnie wprowadzane na rynek nie mają kontaktu z pracownikiem banku.

Firmy CIT zainwestowały w stworzenie profesjonalnych sortowni, wyposażonych w szereg nowoczesnych zabezpieczeń, światowej klasy urządzenia do rozpoznawania i liczenia wartości pieniężnych oraz systemy monitoringu. Odpowiednie międzynarodowe certyfikaty potwierdzają wdrożenie procedur związanych z bezpieczeństwem sortowania i przechowywania gotówki. Odpowiedni dobór kadr daje gwarancję jakości usług wykonywanych na rzecz Banków.

Konkurencja banków oraz walka o klienta w obszarze bankowości korporacyjnej spowodowały erozję cen za usługi związane z transportem, przeli-

czaniem i ewidencjonowaniem gotówki. Coraz większe wymagania dużych klientów handlowych wprowadziło szereg nowych procesów zwiększających pracochłonność. W praktyce proces rozliczania każdego dużego klienta banku jest inny.

Koszty obrotu gotówki w Instytucji Finansowej

Roczny koszt gotówki w banku stanowi dużą pozycję w budżecie każdej instytucji finansowej. Składowymi tej pozycji jest koszt zamrożonej gotówki (między innymi gotówka w bankomatach) oraz koszty procesowania gotówki czyli transportów i liczenia. Instytucje finansowe nie publikują takich danych, szacuje się jednak, że około połowy kosztów obrotu gotówki w banku stanowią koszty zamrożonej gotówki a drugą połowę koszty jej procesowania. Dla średniej wielkości banku całkowity budżet kosztu gotówki to kwota z przedziału od 16 do 20 mln złotych rocznie. Tak duże kwoty, jak również chęć ich ograniczenia potwierdzają promowany przez banki rozwój bankowości elektronicznej oraz płatności bezgotówkowych. Koszty zamrożonej gotówki są pochodną stóp procentowych i kosztów transportu. Każdy z banków analizuje czy częściej zasilać bankomaty mniejszymi kwotami, czy też ograniczyć koszty transportu na rzecz większej ilości gotówki zamrożonej w urządzeniu. Znalezienie najtańszej opcji jest trudnym zadaniem, wspieranym przez systemy informatyczne, ale bazującym na historii i doświadczeniach pracowników. Obydwie składowe w ostatnich latach ulegały zmianie. Rada Polityki Pieniężnej reagując na sytuację ekonomiczną zmniejszała stopy procentowe. Konkurencja pomiędzy firmami CIT, prowadzone przez instytucje finansowe postępowania przetargowe, mimo rosnących cen paliw, doprowadziły do redukcji kosztów transportu.

Obowiązujące w Polsce niskie stopu procentowe i związane z tym niskie koszty zamrożenia gotówki dodatkowo mają wpływ na obniżenie kosztów gotówki w banku. Sytuacja w przyszłości może ulec zmianie. Zgodnie z zapowiedziami Marka Belki, Prezesa Narodowego Banku Polskiego, stopy procentowe mogą w przyszłości oscylować w granicach 3% przez długie lata, a taka sytuacja zwiększa koszty gotówki w instytucjach finansowych. Dlatego już dzisiaj należy zastanowić się nad działaniami mającymi wpływ na obniżenie tych kosztów, np. przez automatyzację i standaryzację procesów.

Kondycja finansowa firm CIT

Analizując kondycję finansową firm CIT należy rozdzielić usługi związane z transportem wartości pieniężnych od usług związanych z liczeniem i przechowywaniem gotówki. W obszarze transportu gotówki na rynku polskim występuje wiele podmiotów oferujących ten typ usługi. Banki, dywersyfikując ryzyko, mają możliwość zawarcia umów z wieloma podmiotami. W obszarze liczenia i przechowywania gotówki liczba podmiotów w ostatnich latach się zmniejszyła. Z rynku polskiego wycofały się międzynarodowe korporacje G4S i Brinks, jako powód wskazując m.in. niepowodzenie ekonomiczne oraz znaczące odstępstwa od europejskich standardów w kwestii oczekiwań rynku. Przejęcia i łączenia doprowadziły do sytuacji, że obecnie na rynku polskim są trzy podmioty oferujące usługę w pełnym zakresie. Centrum Usług Koncesjonowanych Poczty Polskiej to czwarty podmiot oferujący bankom usługi zarządzania gotówką.

14 sierpnia 2014 roku Polska Organizacja Firm Obsługi Gotówki, skupiająca największe podmioty zajmujące się obrotem gotówki, opublikowała pismo dotyczące sytuacji ekonomicznej w branży. Wzrost średniej płacy oraz kosztów paliwa z jednej strony oraz presja na obniżenie cen przez Banki z drugiej doprowadziła do złej sytuacji ekonomicznej firm zajmujących się obsługą gotówki. Najważniejszą pozycją kosztową firm CIT są koszty personalne. Oferowany w branży poziom wynagrodzeń dla podstawowych pracowników powoduje liczne rotacje personelu. Niski poziom motywacji pracowników może przekładać się na bezpieczeństwo oraz jakość oferowanych usług. Wymagania banków, jak również końcowych klientów przekładają się na brak standaryzacji zakresu usług. Wiele działań jest w ramach zawartych umów wykonywanych bezpłatnie. Nie udało się zdefiniować standardu podstawowej usługi i katalogu usług dodatkowych. Brak standaryzacji przekłada się na duży udział pracy manualnej oraz zwiększenie kosztów osobowych. Na razie branża korzysta z sytuacji rynkowej dającej możliwość znalezienie kandydatów gotowych na wykonywanie pracy za tak niski poziom wynagrodzeń. Sytuacja może się jednak zmienić, wzrost ekonomiczny będzie skutkował wzrostem poziomu wynagrodzeń, a taki scenariusz może się przełożyć podniesieniem stawek dla Banków lub bankructwem podmiotów.

Automatyzacja procesów warunkiem utrzymania kosztów procesowania gotówki

Wynagrodzenia pracowników są głównym kosztem działalności firm CIT. Duży stopień prac wykonywanych manualnie, wynikający z braku standaryzacji procesów, powoduje konieczność zaangażowania dużej liczby personelu. W polskich sortowniach liczba przeliczonych dziennie banknotów na jednego pracownika jest kilka razy mniejsza niż w sortowniach niemieckich, francuskich, bułgarskich czy czeskich. Każdy banknot zanim zostanie odwieziony do Narodowego Banku Polskiego lub ponownie trafi do obiegu jest kilka razy procesowany przez urządzenia w sortowni. Typowo w pierwszym kroku banknoty są przeliczane i orientowane (układane w jednym kierunku) na małych sorterach stanowiskowych. Urządzenia te nie umożliwiają obrócenia banknotu, więc, aby odpowiednio go zorientować, należy czasami kilkakrotnie wyjąć banknot z kieszeni odrzutów i ponownie w innym położeniu umieścić w podajniku. W drugim kroku, zorientowane banknoty dzielone są na nominały w kategoriach obiegowe i destrukty. Również w czasie drugiego przeliczania banknoty mogą być kilka razy przetwarzane przez sorter. Tak zorganizowany proces liczenia wymaga zaangażowania dużej liczby osób. Wielokrotne przekładanie banknotu ma wpływ na cykl jego żywotności oraz jakość trafiających do obiegu środków.

Wdrożenie urządzeń, które w czasie jednego obiegu umożliwią zorientowanie (ułożenie banknotów w jednym kierunku), podział na nominały oraz na banknoty obiegowe i destrukty spowoduje przyśpieszenie procesu liczenia oraz ograniczenie personelu. Taki proces ma również wpływ na większą żywotność banknotu.

Aby wdrożyć proces liczenia w jednym obiegu niezbędne są zmiany procedur nie tylko w firmach CIT, ale również w bankach, które zlecają tą usługę. Jednym z zagadnień jest dokumentowanie różnic. Częstym przypadkiem jest sytuacja, gdzie klient błędnie przeliczył deponowaną wartość. W przypadku wykazania w sortowni różnicy pomiędzy deklarowaną a rzeczywistą wartością, pieniądze muszą być pod nadzorem ponownie przeliczone. Z reguły na życzenie klienta, banki, a w ich imieniu firmy CIT, udostępniają nagranie video z przeliczenia depozytu. Dzienna liczba protokołów różnic to kilkadziesiąt dokumentów, co stanowi nawet 5% liczby procesowanych depozytów. Wdrożenia procesu liczenia w jednym obiegu powoduje, po przeliczeniu, wymieszanie banknotów różnych depozytów. Raporty generowane przez sortery

zawierając szczegółowe informacje dotyczące wartości depozytu w rozbiciu na nominały i ilości.

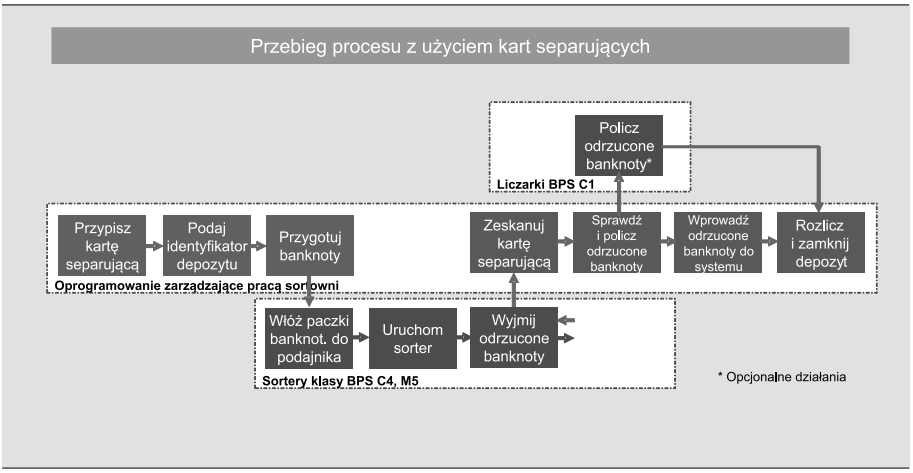
Instytucje finansowe w umowach zawieranych z klientami gwarantują sobie prawo zaksięgowania wartości przeliczonej przez bank, a nie podanej przez klienta. Banki regularnie audytują sortownie firm CIT. Wszystkie obecne w Polsce firmy CIT posiadają certyfikaty wystawione przez międzynarodowe instytucje w zakresie bezpieczeństwa i zarządzania procesami. Konieczność dodatkowego dokumentowania różnic jest istotnym elementem blokującym wdrożenie szybszego i bardziej efektywnego procesu liczenia gotówki.

Światowym standardem w procesie liczenia gotówki jest wdrożenie systemu kart separujących. Standard ten nie został wdrożony w żadnej polskiej sortowni firm CIT, jak również w sortowniach Poczty Polskiej. Przebieg takiego procesu jest trzystopniowy.

W pierwszym etapie przygotowawczym otwierana jest koperta z depozytem. Pieniądze, bez ich liczenia, przypisywane są w systemie informatycznym do indywidualnej karty separującej. Operator oddziela poszczególne depozyty za pomocą specjalnie zaprojektowanych kart.

Etap drugi polega na przeliczeniu, posortowaniu i ułożeniu banknotów. Operator zasila sorter paczkami banknotów, które składają się z wielu depozytów przedzielonych kartami separującymi. Sorter po rozpoznaniu karty separującej rozpoczyna proces liczenia nowego depozytu. Wszystkie banknoty tylko jeden raz są przetwarzane przez sorter. Gotowe paczki lub wiązki (10 paczek, każda po 100 banknotów) są efektem końcowym liczenia w tym etapie. Ewentualne nierozpoznane banknoty, przedzielone kartami separującymi, lądują w kieszeni odrzutów.

W trzecim etapie następuje rozliczenie i zaksięgowanie depozytów. Operator po wprowadzeniu numeru karty separującej może porównać przeliczoną kwotę z kwotą zadeklarowaną przez klienta. Ewentualne nierozpoznane banknoty (przeważnie kilka sztuk) są ręcznie doksięgowane. Po zamknięciu depozytu następuje automatyczne uznanie rachunku klienta.



Giesecke & Devrient

Tak zorganizowany proces liczenia umożliwia maksymalnie efektywne wykorzystanie sortera przy minimalnym zaangażowaniu personelu. Jednocześnie na każdym etapie procesowania w systemie informatycznym jest informacja dotycząca miejsca oraz stopnia zaawansowania procesu liczenia danego depozytu. Zintegrowanie procesu z systemem video umożliwia zaawansowane śledzenie każdego z depozytów.

Informatyka w procesie obrotu gotówki

Analizując zakres wsparcie informatycznego w procesach obrotu gotówki, należy wziąć pod uwagę parę aspektów:

- obsługę odbioru gotówki od Klientów Banków,
- procesowanie gotówki w sortowniach,
- księgowanie przeliczonych pakietów w systemach bankowych,
- prognozowanie i zamawianie gotówki,
- przyszłe rozwiązania związane z zarządzaniem depozytami NBP.

Usługę odbioru gotówki od klientów na zlecenie banku wykonują firmy CIT. Model deponowania gotówki jest elementem umowy zawartej pomiędzy bankiem a klientem. Stosowanych jest kilka metod:

- odbiór gotówki bezpośrednio od klienta w jego siedzibie; klient przekazuje gotówkę w zamkniętej bezpiecznej kopercie,
- klient przekazuje zamkniętą bezpieczną kopertę w oddziale Banku,
- klient deponuje kopertę we wrzutni,
- klient wpłaca gotówkę do wpłatomatu.

Zarówno pierwsza, jak i druga metoda obecnie nie jest wspierana rozwiązaniami informatycznym. Odbiory wykonywane są według ustalonych reguł, a konwojenci nie są wyposażeni w urządzenia umożliwiające identyfikację i śledzenie pakietów. Nie stosowane są również rozwiązania do awizowania gotówki przez klientów. Banki nie oferują klientom narzędzi, które umożliwiają zadeklarowanie w systemie kwoty oraz numeru bezpiecznej koperty. Ta prosta funkcjonalność usprawnia monitorowanie depozytów oraz na bardzo wczesnym etapie daje informację dotyczącą spodziewanego poziomu gotówki w Banku. Wrzutnie elektroniczne przed zdeponowaniem pakietu wymagają czynności związanych z podaniem wyżej wymienionych danych. Informacje te jednak z reguły nie są przekazywane do sortowni. Ostatnia metoda bezpośrednio informuje właściciela wpłatomatu o poziomie gotówki w urządzeniu.

Awizacja numeru bezpiecznej koperty przez klienta daje możliwość wyposażenia konwojentów w urządzenia do elektronicznego potwierdzenia odbioru pakietu i on-linowego monitorowania statusu. Obecnie bywają sytuacje, kiedy konwojenci po otwarciu wrzutni depozytowej spędzają kilkadziesiąt minut ręcznie spisując numery pakietów, które przejmują.

Brak awizowania przesyłek wymusza dodatkową pracę w centrach gotówki. Obecnie na etapie przyjmowania depozytów do sortowni dyspozytor tworzy listę zawierająca numery kopert i kwotę spisaną z opakowania koperty. Bywają sytuacje, gdy taka lista tworzona jest w arkuszach kalkulacyjnych typu Excel a sortownie nie stosują specjalizowanych systemów informatycznych do zarządzania procesem. Awizowanie przesyłek, oprócz wspomnianego wcześniej monitorowania pakietów, przyśpiesza proces przyjęcie w sortowni.

System zarządzania procesami w sortowni jest kolejnym wyzwaniem informatycznym. Niektóre podmioty na rynku polskim nie posiadają wdrożonego oprogramowania do zarządzania tym procesem lub ma ono ograniczoną funkcjonalność. W takich przypadkach po otwarciu koperty operator swoim podpisem na papierowych dokumentach potwierdza zgodność przeliczonej gotówki z kwotą zadeklarowaną przez klienta. Brak systemu wymusza personalną odpowiedzialność operatora od momentu otrzymania pakietu do momentu rozliczenia całości gotówki (uporządkowanej według orientacji

i nominałów) na koniec zmiany. Wprowadzenie systemu daje możliwość wykonywania poszczególnych elementów procesu przez różnych pracowników, usprawniając i przyśpieszając proces liczenia i sortowania.

Integracja systemu zarządzania sortownią z systemem banku daje możliwość księgowania depozytu bezpośrednio po jego przeliczeniu. Obecnie potwierdzony przez operatora bankowy dowód wpłaty jest ręcznie przez pracowników firmy CIT księgowany w systemie banku.

Zarządzanie gotówką, w tym planowanie i zamawianie, to kolejny obszar wspomagany rozwiązaniami informatycznymi. Analiza poziomów zamrożonej gotówki w relacji do stóp procentowych oraz kosztów transportu to codzienne zadania banków. Jaki harmonogram ładowania bankomatów przyjąć: czy bardziej opłacalnym jest załadowanie kaset większą ilością gotówki i rzadsze transporty, czy też na odwrót? Bieżąca informacja dotycząca poziomu gotówki znajdującej się w sortowni umożliwia lepsze zarządzanie stanem gotówki w banku. W tym zakresie niezbędne są interfejsy pomiędzy systemami zarządzania procesami w sortowni, a systemami prognozowania gotówki w instytucjach finansowych.

Przechowywanie depozytów Banku Centralnego w skarbcach firm procesujących gotówkę musi być również wsparte wdrożeniem rozwiązań informatycznych. Transakcje deponowania oraz pobrania gotówki w Banku Centralnych może być realizowane elektronicznie, a droga gotówki z Banku A do Banku B nie musi fizycznie przechodzić przez skarbiec Banku Centralnego. Aby zarządzać takimi transakcjami, niezbędna jest platforma informatyczna pozwalająca zarządzić ruchami i stanami gotówki.

Automatyzacja i związana z tym standaryzacja procesów dla wszystkich instytucji finansowych, wsparta rozwiązaniami informatycznymi, jest drogą rozwiązania przedstawionych problemów w przyszłości.

Zmiany w zakresie transportu gotówki

Większość prac sortowni wykonywana jest w godzinach nocnych. Taki sposób pracy wynika z odbiorów depozytów wieczorem oraz umów z klientem do przeliczenia wartości w jak najkrótszym czasie. Dodatkowym elementem powodującym pracę nocną jest konieczność odwiezienia w godzinach rannych nadmiaru gotówki do Narodowego Banku Polskiego. Instytucje finansowe dążą do jak najszybszego zdeponowania środków w NBP. Pieniądze zdeponowane w Narodowym Banku Polskim pracują (są oprocentowane) lub stają

się częścią obowiązkowej rezerwy. Banki potrzebujące gotówki zasilają się w NBP, zlecając ta usługę często tym samym podwykonawcom, z których korzystają banki odprowadzające gotówkę. W obecnym czasie wprowadzania elektronicznych form rozliczeń, taka forma rozliczeń i przesuwania gotówki jest anachroniczna. Jednym z zadań NBP jest dbanie o jakość banknotów i monet znajdujących się w obiegu. Brak szczegółowych technicznych regulacji w tym zakresie powodował, że Bank Centralny odbierając pieniądze od jednego banku i wydając je kolejnemu mógł oddzielić destrukty. Wydana 5 stycznia 2015 r. rekomendacja jest jednym z kroków w kierunku zmiany tego trybu postępowania. Docelowym rozwiązaniem, mogłyby być depozyty NBP fizycznie przechowywane w skarbcach firm CIT. Warunkiem niezbędnym ograniczenia transportów pomiędzy sortowniami a NBP jest wprowadzenie regulacji dotyczących maszynowego oddzielania nominałów obiegowych od destruktów. Obecne regulację powodują, że podział na nominały obiegowe i destrukty praktycznie zależy od doświadczenia kierownika sortowni.

Podsumowanie

Wynaleziona w VII w. p.n.e przez Fenicjan gotówka do dzisiaj pozostaje głównym środkiem płatności w transakcjach wykonywanych przez osoby fizyczne. Na przestrzeni wieków próby zastąpienia gotówki inną formą płatności nie odniosły sukcesu. Niektóre rozwiązania, takie jak czeki, znikają z rynku i są zastępowane przelewem, płatnością kartą lub telefonem. Nowoczesne metody płatności są stosunkowo młode i, jak na razie, nie wyeliminowały obrotu gotówkowego.

Statystyki publikowane przez Narodowy Bank Polski wskazują na systematyczny wzrost ilości gotówki znajdującej się w obiegu. Koszty zarządzania gotówką stanowią dużą pozycję w budżetach instytucji finansowych. Środowisko bankowe ograniczając koszty aktywnie wspiera elektroniczne formy płatności. Większość banków korzysta z zewnętrznych podmiotów w zakresie transportów, przeliczania i przechowywania gotówki. Wzajemna konkurencja tych firm doprowadziła rentowność działalności na granicę opłacalności. Zwrotne przejęcie procesowania gotówki przez instytucje finansowe wydaje się nierealne. Usystematyzowanie procesów, automatyzacja i lepsze zarządzanie wdrażając rozwiązania informatyczne wydaje się jedyną drogą do utrzymania kosztów na obecnym poziomie. W dłużej perspektywie takie działania przyniosą wymierne oszczędności związane z kosztami procesowania gotówki.

Wzajemna współpraca Narodowego Banku Polskiego, banków, firm CIT oraz dostawców technologii, jest warunkiem usprawnienia procesów przy jednoczesnym zapewnieniu bezpieczeństwa obrotu gotówkowego w Polsce. Niższe koszty obsługi gotówki dla Banków, zmniejszenie obciążenia dla gospodarki kraju oraz obniżenie pracochłonności w sortowniach to wspólne cele które powinny przyświecać zmianom w obrocie gotówkowym w najbliższych latach.

Bibliografia:

http://pl.wikipedia.org/wiki/Pieniądz
http://pieniadze.fakt.pl/pieniadze-w-historii-jak-ludzie-placili-w-dawnych czasach,artykuly,459857,1.html
http://www.weksel.pl/historia-weksli.html
http://www.nbp.pl/home.aspx?f=/statystyka/pieniezna_i_bankowa/struktura-obiegu.html

© 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 Studio
SKŁAD:
Łukasz Sitko
ISBN: 978-83-88835-24-7
CIP – Biblioteka Narodowa

Bank = informatyka + ludzie + informatyka. To prowokacyjnie proste równanie staje się powoli dogmatem dla menedżerów zarządzających instytucjami finansowymi. To efekt dynamicznego postępu technologicznego, coraz większej roli „cyfrowych konsumentów" oraz wzrostu konkurencji m.in. poprzez wchodzenie na rynek usług bankowych przez podmioty z innych branż, zwłaszcza technologicznych, np. telekomy czy firmy internetowe. Choć tytuł publikacji, której najnowszą edycję trzymają Państwo w rękach, sugeruje że dotyczy ona tylko jednego – informatycznego – komponentu przywołanej na początku „recepty na bank", to jest to wrażenie pozorne. Mobile, Big Data, cloud computing – z tymi pojęciami jest już zaznajomiony każdy bankowiec, nie tylko pracujący w dziale IT. Autorzy artykułów zawartych w niniejszej książce rozumieją to bardzo dobrze, pisząc w przystępny sposób, interesujący dla szerokiego spektrum odbiorców. Ciekawym aspektem publikacji są również prognozy i rekomendacje dotyczące prawdopodobnych kierunków rozwoju bankowości. Szczególną uwagę warto zwrócić na możliwe do uzyskania synergie płynące ze współpracy instytucji finansowych z administracją publiczną m.in. w zakresie uwierzytelniania użytkowników w systemach informatycznych i przenoszenia procesów ze świata realnego do cyfrowego. Zachęcam Państwa do zapoznania się z książką i podejmowania zarysowanych w niej „Wyzwań Informatyki Bankowej" w codziennej rzeczywistości biznesowej.

Zbigniew Jagiełło, Prezes Zarządu PKO Banku Polskiego

Przez sektor finansowy przechodzi fala fundamentalnych przeobrażeń. Banki redefiniują swoje strategie by móc stawić czoła konkurentom spoza branży, którzy dzięki innowacyjności oraz znajomości dynamicznie zmieniających się potrzeb konsumentów potrafią dostosować ofertę produktów finansowych do ich indywidualnych oczekiwań.
Dzisiaj ważny jest nie tylko sposób gromadzenia i przetwarzania danych, ale także ich wymiana i współdzielenie. Era inteligentnego oprogramowania staje się faktem, platformy cyfrowe, spersonalizowane aplikacje i zaawansowane narzędzia informatyczne wykorzystywane są na coraz szerszą skalę. Kluczem do sukcesu staje się zorganizowanie instytucji w taki sposób by pozwalała na bliską współpracę i wymianę wiedzy z innymi podmiotami na rynku. Właśnie takie zjawisko zostało nazwane przez Accenture „We Economy". „Wyzwania Informatyki Bankowej" – publikacja przygotowana przez Gdańską Akademię Bankową przedstawia szerokie spektrum zagadnień związanych z bankowością w erze cyfrowej. Trafnie definiuje wyzwania, przed którymi stoi sektor oraz przedstawia przykłady rozwiązań praktycznych jak i warstwę teoretyczną. Dzięki analizie poruszanych tematów jest to pozycja, która powinna znaleźć się w polu zainteresowań każdego specjalisty IT pracującego w instytucjach finansowych.

Jarosław Kroc, Prezes Zarządu Accenture Polska

ISBN 978-83-88835-24-7