Partnerzy raportu

cloudware

pwc

Bank bez chmury nie istnieje

Wydawcy raportu

Centrum Procesów Bankowych i Informacji
cpb.pl

BANK
MIESIĘCZNIK FINANSOWY

BANK.PL

Chmura w biznesie
Liderzy widzą wartość

Sektor finansowy

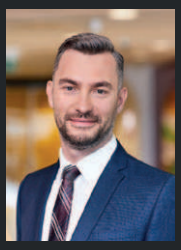
Które z następujących stwierdzeń najlepiej opisuje operacje Twojej organizacji w chmurze?

Wszystkie nasze operacje są w chmurze

PL	CEE	EMEA	USA
14%	18%	23%	42%

Wszystkie nasze operacje będą w chmurze w ciągu najbliższych 2 lat

PL	CEE	EMEA	USA
46%	41%	53%	51%



Sondaż wskazuje, że już 35% instytucji finansowych wdrożyło chmurę we wszystkich lub większości obszarów swojej działalności, a 46%, które obecnie nie stawiają na chmurę, planuje przenieść całą swoją działalność do niej w ciągu najbliższych 2 lat. Te dane wyraźnie wskazują, że sektor jest w ciągłym procesie migracji do chmury, a najbliższe dwa lata pokażą z jakim efektem.

Przemysław Paprotny
Partner, Lider usług dla sektora finansowego | PwC Polska

Mariusz Chudy
Partner, CEE Cloud & Digital Leader | PwC Polska

35%
instytucji finansowych wdrożyło chmurę we wszystkich lub większości obszarów swojej działalności

46%
organizacji, które obecnie nie stawiają na chmurę, planuje przenieść całą swoją działalność do chmury w ciągu najbliższych 2 lat

30%
instytucji finansowych wykorzystuje przede wszystkim chmurę do modernizacji, a tylko jedna na cztery stosuje holistyczne i wieloaspektowe podejście, które pozwala usprawnić im swoją działalność

Zeskanuj kod QR jeśli chcesz przeczytać pełną wersję raportu

Bank bez chmury nie istnieje

Fot. Ar_TH/stock.adobe.com

Dr hab. Mateusz Folwarski
PROFESOR UNIWERSYTETU EKONOMICZNEGO W KRAKOWIE, ZASTĘPCA DYREKTORA INSTYTUTU FINANSÓW UNIWERSYTETU EKONOMICZNEGO W KRAKOWIE. DYREKTOR STUDIÓW PODYPLOMOWYCH REALIZOWANYCH W KSB UEK – BANKOWOŚĆ I FINANSE CYFROWE. OD KILKU LAT WSPÓŁPRACUJE DYDAKTYCZNIE I NAUKOWO Z WYDZIAŁEM ZARZĄDZANIA I KOMUNIKACJI SPOŁECZNEJ UNIWERSYTETU JAGIELLOŃSKIEGO. AUTOR LICZNYCH PUBLIKACJI Z ZAKRESU BANKOWOŚCI, INNOWACJI CYFROWYCH ORAZ SEKTORA FINTECH. UCZESTNIK PROJEKTÓW DOTYCZĄCYCH WSPÓŁPRACY NAUKI Z BIZNESEM, M.IN. DLA MINISTERSTWA ROZWOJU, ZBP, WIB. CZŁONEK RADY NADZORCZEJ SYSTEMU OCHRONY ZRZESZENIA BPS.

1. Chmura obliczeniowa – problemy definicyjne, rola i istota

Usługi rynkowe i usługi administracji publicznej przechodzą z platform stacjonarnych na platformy mobilne, przez co stają się coraz bardziej wszechobecne. Zmiany te wymagają ustanowienia unijnych ram regulacyjnych dla przetwarzania w chmurze, transgranicznego dostępu do treści i transferu danych mobilnych bez granic, przy jednoczesnej ochronie prywatności, danych osobowych i zagwarantowaniu cyberbezpieczeństwa. Dlatego też na obszarze Unii Europejskiej ustanowiono m.in. akt o rynkach cyfrowych oraz akt o usługach cyfrowych, które zrewolucjonizują jednolity rynek cyfrowy w nadchodzących latach[1]. W akcie o rynkach cyfrowych (DMA) ustanowiono ściśle zdefiniowane obiektywne kryteria kwalifikowania dużej platformy internetowej jako „strażnika dostępu" (kontrolującego dostęp do informacji i usług). Akt o usługach cyfrowych (DSA) koncentruje się na tworzeniu bezpieczniejszej przestrzeni cyfrowej dla użytkowników cyfrowych i firm, poprzez ochronę praw podstawowych online[2].

Problematyka rozwiązań chmurowych zainicjowana została w Stanach Zjednoczonych jeszcze w latach 60 XX wieku. Wskazuje to na charakterystyczną cechę innowacji finansowych na globalnym rynku finansowym – tj. nowe zastosowanie istniejących już technologii. Początkowo zasoby teleinformatyczne jako usługa użyteczności publicznej klasyfikowane były jako jedna z trzech koncepcji: *cluster*, *grid* oraz *cloud computing*. I to właśnie chmura obliczeniowa (*cloud computing*), rozumiana jako system równoległego i rozporoszonego →

1 Powszechny jednolity rynek cyfrowy, https://www.europarl.europa.eu/factsheets/pl/sheet/43/powszechny-jednolity-rynek-cyfrowy, dostęp z dnia 3.11.2023.

2 Szerzej: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_pl, dostęp z dnia 3.11.2023. https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020PC0842, dostęp z dnia 3.11.2023. https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32022R2065, dostęp z dnia 3.11.2023.

zasobu obliczeniowego zyskuje w dzisiejszym cyfrowym świecie bankowości coraz większe znaczenie. W literaturze przedmiotu bardzo często następuje odwołanie do początkowych prób określenia i zdefiniowania chmury obliczeniowej i jej silnych związków z internetem – zwłaszcza że początkowo te pojęcia były tożsame[3]. Jednym z prekursorów sformułowania definicji chmury obliczeniowej był **Ramalingam Chellappa**, który określił ją jako połączenie komputerów tworzących światową sieć internetu, w ramach której miejsce i obszar przechowywania danych nie jest widoczny dla użytkownika[4]. Najogólniej definicję chmury obliczeniowej można ująć jako usługi związane z przenoszeniem danych. Wśród licznych prób definiowania chmury obliczeniowej można wskazać na jej różne elementy, m.in.: zbioru połączonych i wirtualnych komputerów, skalowalne usługi informatyczne, wirtualne zasoby obliczeniowe, współdzielenie zasobów, outsorcing infrastruktury, zaangażowanie podmiotów trzecich. Pomimo funkcjonowania wielu definicji chmury obliczeniowej, jedną z najpopularniejszych jest określenie jej jako modelu świadczenia usług swobodnego dostępu na żądanie do zasobów teleinformatycznych zarządzanych przez jeden bądź wiele różnych podmiotów[5]. Taki model oparty na usługach oferowanych w chmurze obliczeniowej posiada kilka głównych cech, m.in.[6]:

- oferowanie usług na żądanie,
- szeroki dostęp za pomocą internetu,
- wymiana zasobów teleinformatycznych zlokalizowanych w różnych miejscach,
- mierzalność usług.

Dynamiczny rozwój zainteresowania rozwiązań opartych na chmurze obliczeniowej nastąpił po roku 2008, kiedy to w raporcie Gartnera wykazano że w USA coraz więcej firm rezygnuje z wykorzystania własnego sprzętu i przenosi swoje rozwiązania do chmury obliczeniowej. Rozwój zainteresowania przedsiębiorstw na rynku amerykańskim doprowadził do zintensyfikowanych działań dostawców rozwiązań chmurowych oferowanych przez międzynarodowe instytucje z sektora IT.

W związku z tym, również na rynku europejskim podjęto działania zmierzające do popularyzacji chmury obliczeniowej. Rozwój rozwiązań chmurowych na rynku finansowym w Europie jest oparty na jednym z podstawowych dokumentów prawnych określającym cechy chmury obliczeniowej na rynku europejskim wg Komisji Europejskiej[7]. W ramach kierunku rozwoju chmury obliczeniowej do głównych jej cech można zaliczyć:

- własność zasobów teleinformatycznych dostawcy chmury obliczeniowej,
- migracja danych i optymalne wykorzystanie dostępnego sprzętu,
- brak jednej lokalizacji do przechowywania i przetwarzania danych,
- rozbudowana architektura chmury obliczeniowej, wskazująca na kilka poziomów,
- powszechny dostęp do usług, bez względu na lokalizację,
- względnienie preferencji użytkownika chmury obliczeniowej – w zależności od jego potrzeb.

W ramach legislacyjnych w UE nad ustawą o usługach cyfrowych (DSA), wskazano m.in. na istotną rolę w zakresie zasad dotyczących usług pośrednictwa online, oferowanych przez liczne podmioty na rynku finansowym. W ramach istotnych podmiotów i kierunków zmian w zakresie rynku finansowego w szczególny sposób podkreślono rolę rozwiązań chmurowych – jako przyszłego standardu przetwarzania danych przez instytucje finansowe. W ramach piramidy istotności podmiotów świadczących usługi online przedstawiono istotność rozwiązań pod względem roli, wielkości i wpływu na europejski ekosystem online.

Chmura obliczeniowa jest jedną ze strategicznych technologii cyfrowych uważanych za kluczowy element funkcjonowania instytucji finansowych – zwiększa produktywność i świadczy bardziej spersonalizowane usługi. Przedsiębiorstwa wykorzystują chmurę obliczeniową do optymalizacji wykorzystania zasobów oraz budowania modeli biznesowych i strategii rynkowych, które umożliwią im rozwój, innowacje i zwiększenie konkurencyjności. Regulacje prawne na rynkach europejskich m.in. Ustawa o usługach cyfrowych i europejska strategia w zakresie danych, mają na celu umożliwienie i ułatwienie szybszego przyjęcia chmury obliczeniowej we wszystkich sektorach gospodarki. W istotny sposób może to

3 J. W. Rittinghouse, J.F. Ransome, *Cloud computing. Implementation, Management and Security*, CRC Press 2010.

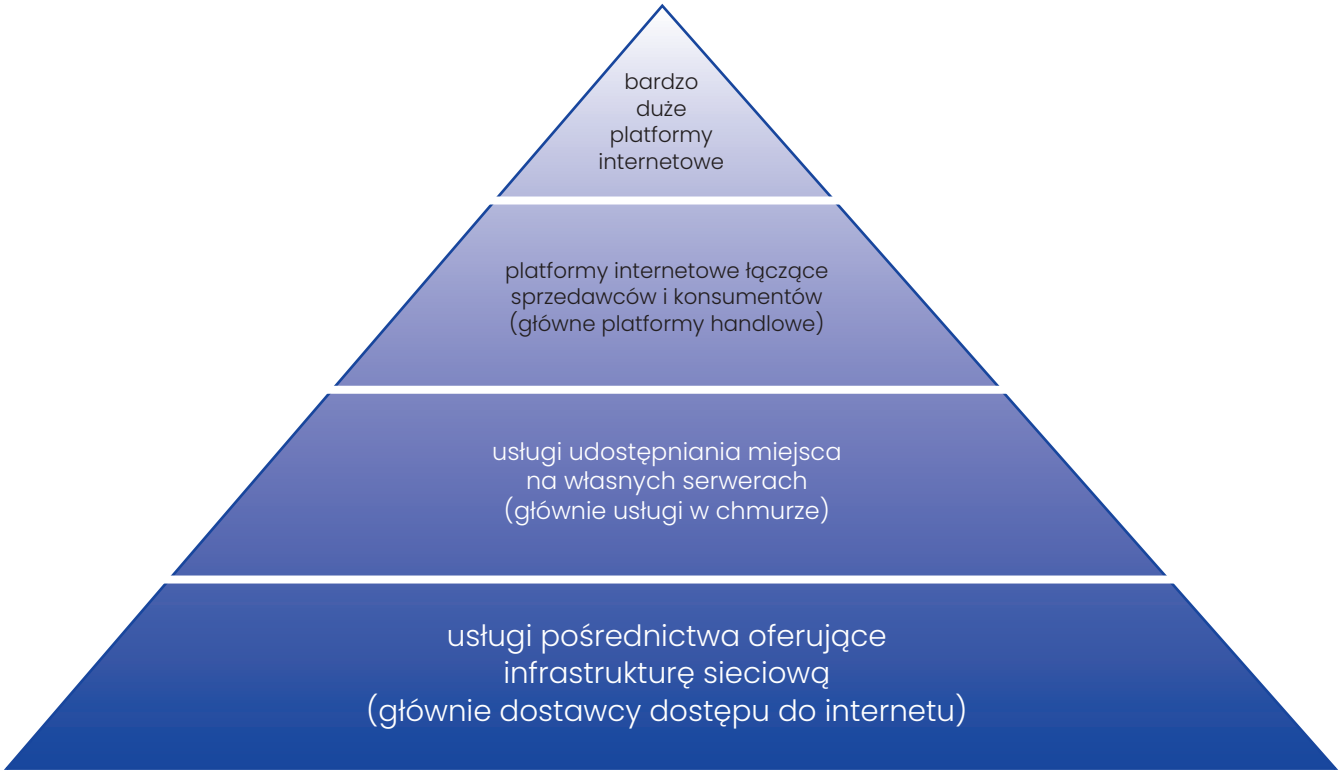
4 T. Fickert, *Entwicklungen des Cloud Computing im Ueberblick – Aktuelle und kuenftige rechtliche Probleme* [w:] Inside the Cloud – Neue Herausforderungen fuer das Informationsrect, J. Taeger, A. Wiebe, Tagungsbank Herbstakademie 2009.

5 P. Mell, T. Grance, *The NIST Definition of Cloud Computing*. Recommendations of the National Institute of Standards and Technology.

6 Szerzej: A. Krasuski, *Chmura obliczeniowa, Prawne aspekty zastosowania*, Wolters Kluwer, Warszawa 2018.

7 Szerzej: KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY, EUROPEJSKIEGO KOMITETU EKONOMICZNO-SPOŁECZNEGO I KOMITETU REGIONÓW Wykorzystanie potencjału chmury obliczeniowej w Europie /* COM/2012/0529 final.

Schemat 1 . Piramida istotności podmiotów świadczących usługi online wg UE



Źródło: opracowanie własne. Szerzej: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en, dostęp z dnia 3.11.2023.

obniżyć koszty ICT, a w połączeniu z nowymi cyfrowymi praktykami biznesowymi istotnie zwiększyć produktywność, a także wzrost gospodarczy i zatrudnienie w europejskich gospodarkach[8].

Ze względu na zasięg usług oferowanych w chmurze obliczeniowej można wyróżnić chmurę publiczną, prywatną, hybrydową, korporacyjną oraz społecznościową. Chmura publiczna dostępna jest dla wszystkich użytkowników, nie posiada ograniczenia geograficznego oraz nie jest związana z konkretnym dostawcą usług opartych na chmurze. Dlatego też chmura publiczna bardzo często nazywana jest również chmurą zewnętrzną, którą cechuje publiczny dostęp do usługi telekomunikacyjnej. Chmura prywatna cechuje się ograniczeniem do określonego jej użytkownika. W zależności od ujęcia definicyjnego w tym przypadku istotna jest kwestia kontroli nad infrastrukturą. W zależności od podejścia użytkownik może być jedynym użytkownikiem takiej chmury, którą kontroluje lub to zarządzanie może być zależne od podmiotu trzeciego. Istotnym elementem chmury prywatnej jest kontrola użytkownika nad całą infrastrukturą teleinformatyczną, a co za tym idzie kwestiami związanymi z bezpieczeństwem przechowywania i przetwarzania danych.

Fundamentem chmury hybrydowej jest chmura prywatna, która zawiera elementy chmury publicznej. Kluczowym jej elementem jest bezpieczeństwo danych użytkownika, które mogą funkcjonować na zasadach chmury prywatnej. Ponadto jedną z przewag użytkownika chmury hybrydowej nad innymi rozwiązaniami chmurowymi jest możliwość wykorzystania chmury prywatnej w celu publicznym (np. strona internetowa banku).

Chmura korporacyjna jest chmurą prywatną, w której tym samym podmiotem jest zarówno jej dostawca, jak i jej użytkownik. To rozwiązanie opiera się na zapewnieniu całkowitej kontroli nad chmurą w danej organizacji, bez możliwości dostępu podmiotów trzecich do zasobów i danych. →

8 Szerzej: COMMUNICATION TO THE COMMISSION, European Commission digital strategy. Next generation digital Commission, Brussels, 30.6.2022 C (2022) 4388 final. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

Chmura społecznościowa opiera się na świadczeniu usług dla ściśle określonej grupy użytkowników. Może ona być tworzona przez kilka podmiotów, które współpracują nad np. danym projektem. W tym modelu to użytkownicy wspólnie podejmują decyzje w zakresie zarówno bezpieczeństwa, kontroli, jak i zarządzania chmurą obliczeniową. Chmury społecznościowe są chmurami prywatnymi o większej liczbie użytkowników aniżeli chmury korporacyjne.

Przedsiębiorstwa korzystają z chmur obliczeniowych głównie ze względu na oszczędności, jakie są związane z jej wykorzystaniem w prowadzonej działalności. Ponadto jedną z kluczowych różnic pomiędzy korzystaniem z rozwiązań chmurowych i tradycyjnych platform jest to, że urządzenie użytkownika nie odgrywa żadnej roli w przetwarzaniu i przechowywaniu danych w chmurze obliczeniowej. Każdy użytkownik z dowolnym urządzeniem zdolnym do połączenia się z tymi centrami danych może uzyskać dostęp i udostępniać swoje usługi w dowolnym momencie[9].

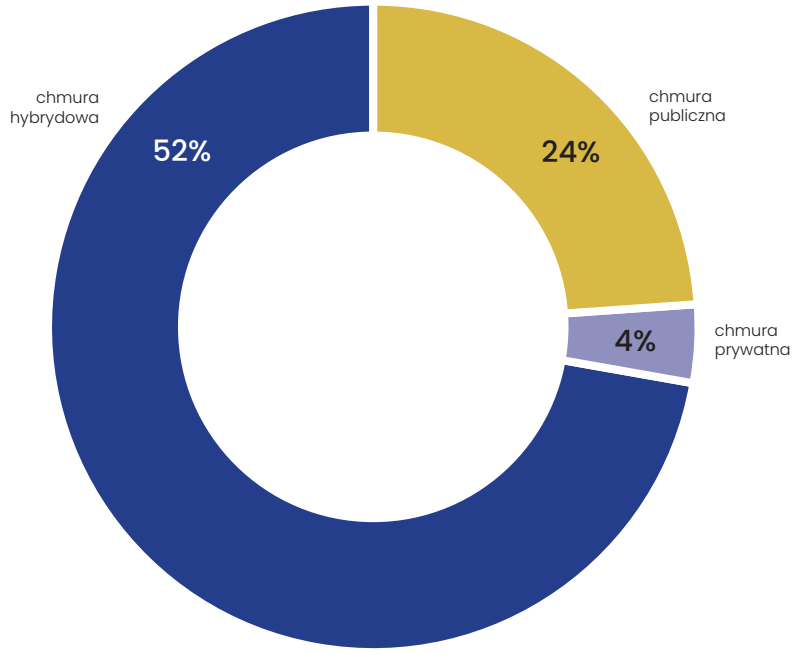
Usługi oferowane w chmurze obliczeniowej klasyfikowane są najczęściej poprzez model, który jest przedmiotem świadczenia usług, tj.:

- infrastruktura jako usługa (*Infrastructures as a Service*: IaaS),
- platforma jako usługa (*Platform as a Service*: PaaS),
- aplikacja jako usługa (*Software as a Service*: SaaS),
- sieć jako usługa (*Network as a Service*: NaaS),
- inne usługi (*Everyfhing as a Service*: XaaS).

W literaturze przedmiotu wyróżnia się trzy poziomy świadczenia usług: Iaas, PaaS, SaaS. Na najniższym poziomie klasyfikowana jest infrastruktura jako usługa w chmurze obliczeniowej (IaaS), gdyż zakres oferowanych usług jest stosunkowo najmniejszy. Model IaaS opiera się na sprzęcie komputerowym jako przedmiocie oferowanej usługi. Ich świadczenie, ze względu na swój charakter, umożliwia wysoki poziom skalowalności i istotnie ogranicza wydatki związane z IT. Wykorzystanie infrastruktury jako usługi w chmurze obliczeniowej umożliwia świadczenie nie tylko podstawowych usług, ale również usług związanych z mocą obliczeniową, przechowywaniem danych oraz kompleksowych usług telekomunikacyjnych. Niemniej to użytkownik w tym modelu jest odpowiedzialny za zarządzanie serwerami i oprogramowaniem – wraz z instalowaniem i dodawaniem dowolnych aplikacji w zależności od preferencji. Ponadto to użytkownik jest odpowiedzialny za bezpieczeństwo danych. Musi on wykazywać się wysokim poziomem wiedzy i doświadczeniem w zakresie administrowania i zarządzania siecią teleinformatyczną oraz systemem operacyjnym i aplikacjami.

W modelu IaaS obowiązkiem dostawcy usług jest głównie zapewnienie infrastruktury sprzętowej, która może być indywidualnie dostosowywana do potrzeb użytkownika. Do niezbędnych elementów dostarczanej infrastruktury zaliczyć należy m.in. sprzęt komputerowy w celu zapewnienia skalowalności, sieć komputerową, dostęp do internetu, platformy wirtualizacyjne – w celu efektywnego zarządzania zasobami, umowy typu service – *level agreements* oraz rozwiązania dotyczące naliczania opłat[10].

Wykres 1. Skala wykorzystania chmury publicznej i prywatnej



Źródło: opracowanie własne na podstawie raportu Flexera: 2023 State of the Cloud Report,dostęp z dnia 3.11.2023.

9 F. Li, H. Lu, M. Hou, K. Cui, M. Darbandi, *Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality*, Technology in Society 64 (2021) 101487.

10 A. Krasuski, *Chmura obliczeniowa, Prawne aspekty zastosowania*, Wolters Kluwer, Warszawa 2018, s. 64–68.

Kolejnym poziomem w zakresie świadczenia usług jest model oparty na platformie jako usłudze (PaaS). Odnosi się on do dostarczania przez dostawcę rozwiązań chmurowych narzędzi programistycznych oraz zintegrowanego środowiska programistycznego. W związku z tym użytkownik chmury obliczeniowej w tym modelu nie posiada narzędzi do zarządzania infrastrukturą. Platforma jako usługa w chmurze obliczeniowej związana jest z udostępnieniem przez dostawcę platform oprogramowania i systemu operacyjnego. W ramach tego modelu użytkownikom udostępniane są gotowe rozwiązania, które umożliwiają dalsze ich wdrożenia – np. tworzenie aplikacji. Platforma jako usługa umożliwia klientowi kontrolę nad wdrożonymi aplikacjami, ale nie daje dostępu do systemu operacyjnego oraz sieci.

Trzecim poziomem klasyfikacji usług oferowanych w chmurze obliczeniowej jest świadczenie usług jako oprogramowania (SaaS). Usługi oferowane w tym modelu są najbardziej powszechne w zakresie świadczenia rozwiązań opartych na chmurze. Istotną przewagą tego modelu nad pozostałymi jest brak konieczności ponoszenia początkowych kosztów związanych m.in. z zakupem sprzętu i oprogramowania, jak i różnego rodzaju opłat licencyjnych. W tym modelu użytkownik nie zarządza ani nie jest odpowiedzialny za kontrolę infrastruktury sieciowej, serwerów oraz systemów operacyjnych. Nie jest również odpowiedzialny za aplikacje – tak jak jest to charakterystyczne dla modeli IaaS i PaaS.

Warto podkreślić istotę zastosowania rozwiązań chmurowych w sektorze finansowym, które są coraz częściej wdrażane w międzynarodowych instytucjach finansowych. Według raportu *International Data Corporation* (IDC) *Worldwide Software and Public Cloud Services Spending Guide*, światowe wydatki na usługi w chmurze obliczeniowej osiągną w roku 2027 wartość 1,35 bln USD. Wśród zidentyfikowanych 28 branż trzema najistotniejszymi segmentami w roku 2027, w których zastosowanie będzie miała chmura obliczeniowa, będą: bankowość, oprogramowanie i usługi informacyjne oraz telekomunikacja. Łącznie będą stanowić 326 mld USD wydatków na usługi w chmurze obliczeniowej[11].

2. Poziom rozwoju innowacyjności w Polsce

Banki w Polsce – zarówno w sektorze komercyjnym, jak i spółdzielczym zmagają się ostatnio z licznymi wyzwaniami w zakresie prowadzenia działalności bankowej – m.in. zwłaszcza w kwestii ryzyka systemowego oraz istotnych zmian regulacyjnych. Niestabilne otoczenie makroekonomiczne istotnie wpływa na decyzje podejmowane przez sektor bankowy. Niemniej, pandemia COVID-19, jak i działania wojenne na świecie, były w pewnym sensie kamieniami milowymi w rozwoju cyfryzacji rynku bankowego w Polsce. →

11 Szerzej: IDC, *International Data Corporation*, https://www.idc.com/getdoc.jsp?containerId=prUS51179523, dostęp z dnia 3.11.2023.

Tabela 1. Zakres odpowiedzialności dostawcy usług i użytkownika w modelach świadczenia usług w chmurze

Infrastruktura jako usługa (model IaaS)		Platforma jako usługa (model PaaS)		Oprogramowanie jako usługa (model SaaS)	
dostawca usługi	użytkownik	dostawca usługi	użytkownik	dostawca usługi	użytkownik
umiejscowienie infrastruktury sprzętowej	system operacyjny	umiejscowienie infrastruktury sprzętowej	aplikacje	umiejscowienie infrastruktury sprzętowej	interfejs
sieć telekomunikacyjna	zestaw oprogramowania	sieć telekomunikacyjna	interfejs	sieć telekomunikacyjna	
sprzęt (m.in. serwery, nośniki danych)	aplikacje	sprzęt (m.in. serwery, nośniki danych)		sprzęt (m.in. serwery, nośniki danych)	
oprogramowanie stosowane do wirtualizacji maszyn, komputerów, aplikacji	interfejs	oprogramowanie stosowane do wirtualizacji maszyn, komputerów, aplikacji		oprogramowanie stosowane do wirtualizacji maszyn, komputerów, aplikacji	
		system operacyjny		system operacyjny	
		zestaw oprogramowania		zestaw oprogramowania	
				aplikacje	

Źródło: opracowanie własne na podstawie: A. Krasuski, Chmura obliczeniowa, Prawne aspekty zastosowania, Wolters Kluwer, Warszawa 2018, s. 61–75.

Po roku 2009, w którym na całym świecie rozpoczęto procesy doregulowania sektora bankowego, pojawiły się nowe podmioty na rynku finansowym, które zrewolucjonizowały strategie tradycyjnych banków w podejściu do klienta rynku finansowego. Nowe podmioty, m.in. fintechy, challenger banki, neobanki, w wyniku postępującego procesu smartfonizacji społeczeństwa po 2010 roku – stały się konkurencją dla tradycyjnych instytucji finansowych. Niemniej pandemia COVID-19 zmusiła tradycyjne instytucje do przeniesienia w większym stopniu świadczenia usług i produktów finansowych do zdalnych kanałów dystrybucji. To w istotny sposób wpłynęło nie tylko na oszczędności w zakresie niższych kosztów prowadzenia działalności, ale również – a może i przede wszystkim – na zmianę postrzegania banków; jako nowoczesnych podmiotów, które nie konkurują z fintechami, ale z nimi współpracują. W wyniku tych działań – zwłaszcza młodzi uczestnicy rynku finansowego, zauważyli, że tradycyjny bank ma konkurencyjną ofertę w porównaniu do usług świadczonych przez neobanki czy challeger banki. Dlatego też banki, stawiając klienta rynku finansowego w centrum swojej uwagi, umocniły swoją pozycję na rynku finansowym.

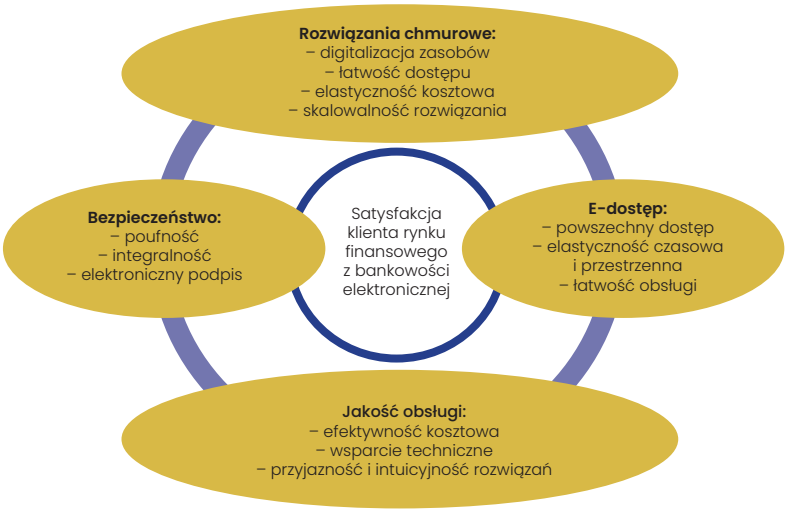
Zadowolenie konsumenta jest istotnym czynnikiem pomagającym bankom utrzymać przewagę konkurencyjną. W literaturze przedmiotu zidentyfikowano cztery kluczowe czynniki, które mogą wpływać na zadowolenie klientów korzystających z bankowości elektronicznej: usługi w chmurze, bezpieczeństwo, e-dostęp i jakość usług.

Kolejnym istotnym wyzwaniem dla sektora bankowego w ostatnim czasie były działania wojenne na świecie i konieczność dostosowania się do wysokiej stopy inflacji, a co za tym idzie wysokich oczekiwań płacowych pracowników. Spełnienie tych oczekiwań było w dużej mierze możliwe poprzez osiągane wysokie wyniki finansowe sektora bankowego, które były możliwe przy wysokich stopach banku centralnego. Niemniej jednak zapoczątkowana w Polsce seria obniżek stóp procentowych we wrześniu 2023 roku oraz zapowiedzi braku kolejnych podwyżek stóp procentowych przez najważniejsze banki centralne na świecie – będą stanowiły w kolejnych latach istotne wyzwanie w zakresie generowania wysokiego wyniku finansowego, co przy względnie rosnących kosztach prowadzenia działalności będzie wymagało od zarządów banków poszukiwania nowych segmentów, w których można będzie zaoszczędzić, zwłaszcza przy niskiej innowacyjności polskiej gospodarki. Według badań *European Innovation Scoreboard* opublikowanych w lipcu 2023 roku, Polska gospodarka jest traktowana jako wschodzący innowator (ostatni koszyk krajów)

Schemat 2. Kluczowe elementy nowej generacji innowacji cyfrowych w bankowości

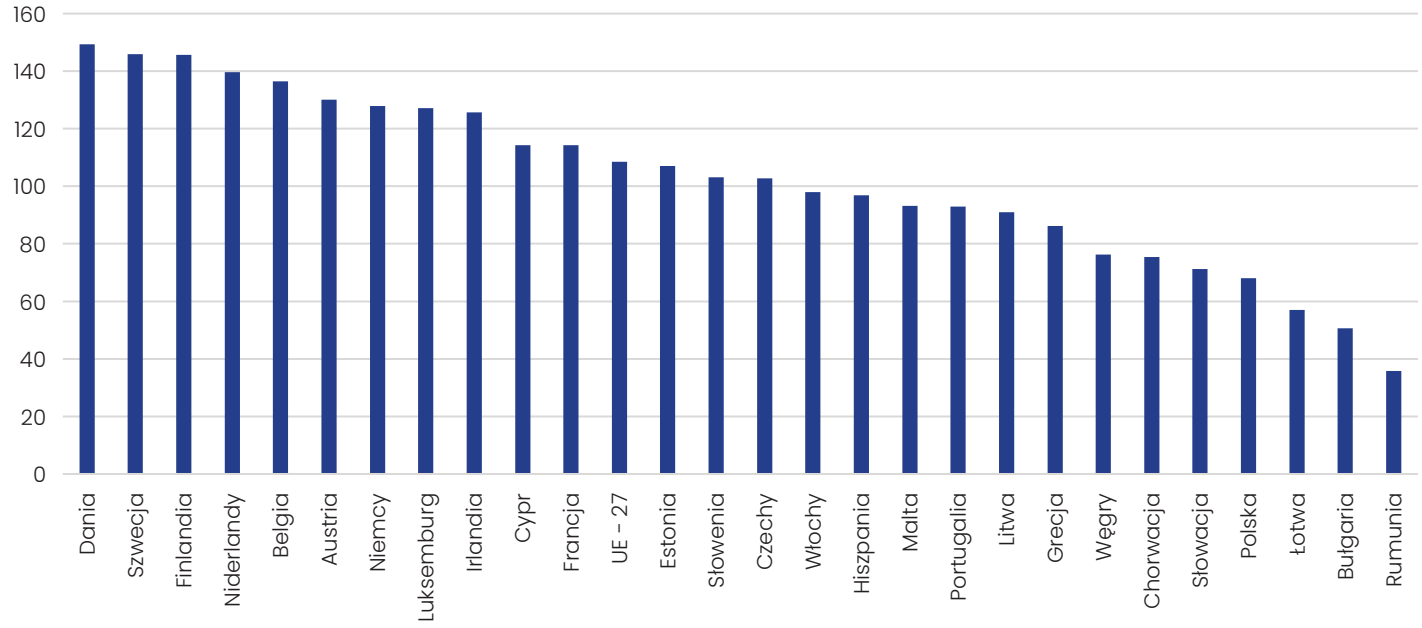
Źródło: M. Folwarski, Innowacje cyfrowe w bankowości a włączenie cyfrowe i finansowe społeczeństwa, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2021, s. 33.

Schemat 3. Kluczowe elementy satysfakcji klienta rynku finansowego w związku z wykorzystaniem zdalnych kanałów dostępu



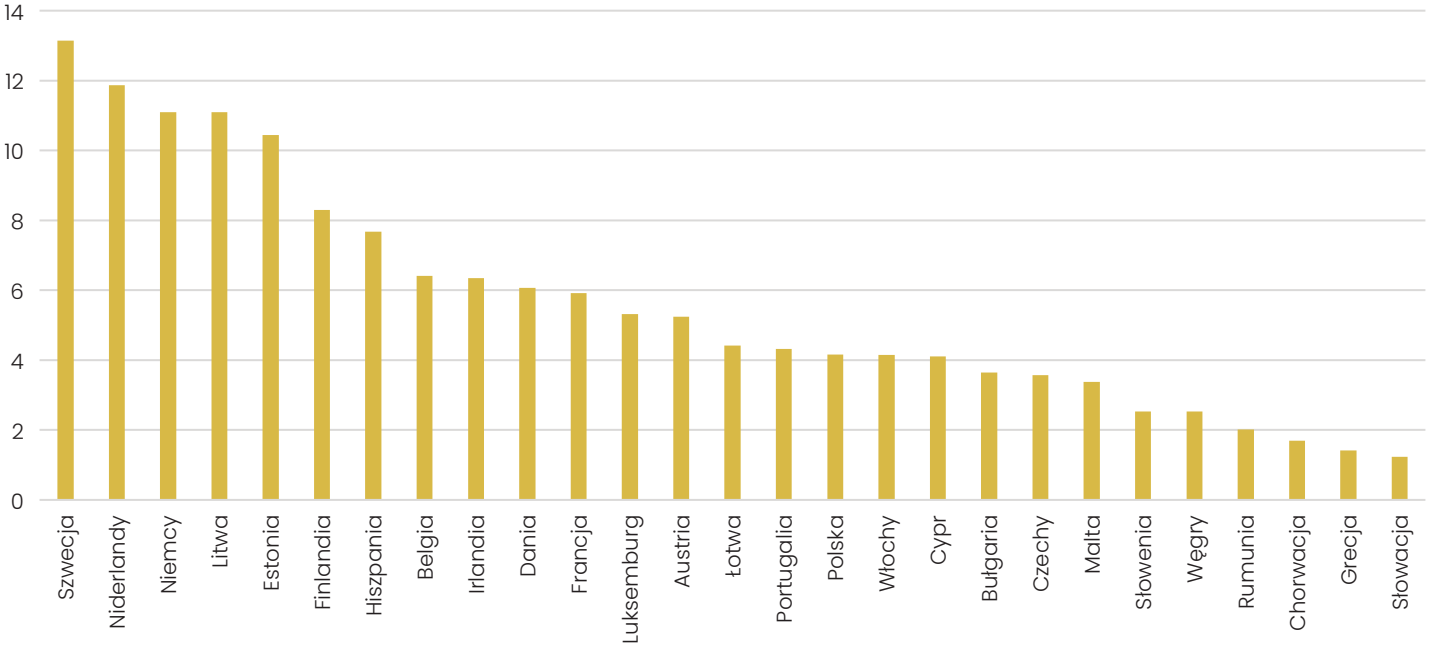
Źródło: opracowanie własne na podstawie: F. Li, H. Lu, M. Hou, K. Cui, M. DarbandiCustomer satisfaction with bank services: The role of cloud services, security,e-learning and service quality, Technology in Society 64 (2021) 101487.

Wykres 2. Indeks innowacyjności gospodarek UE (European Innovation Scoreboard), rok 2023



Źródło: opracowanie własne na podstawie: https://ec.europa.eu/research-and-innovation/en/statistics/performance-indicators/european-innovation-scoreboard/eis, dostęp z dnia 3.11.2023.

Wykres 3. Wskaźnik fintechizacji gospodarek UE (The Global Fintech Index, Findexable)



Źródło: opracowanie własne na podstawie: https://gfi.findexable.com/fintechs, dostęp z dnia 3.11.2023.

– wraz z gospodarkami Chorwacji, Słowacji, Łotwy, Bułgarii i Rumunii[12].

Innowacyjność całej gospodarki może nie oddawać poziomu innowacyjności sektora finansowego (chociaż stanowi on jej istotny element, gdy chodzi o unowocześnianie). Dlatego też, skupiając się na poziomie rozwoju innowacji w sektorze finansowym, warto zwrócić uwagę na indeks fintechizacji europejskich gospodarek. Ogólny poziom rozwoju krajowych gospodarek w zakresie wdrażania rozwiązań z sektora *financial technology* wskazuje na średni poziom rozwoju fintechów w Polsce.

3. W poszukiwaniu pobudzenia innowacyjności banku – rozwiązania chmurowe

Głównym kierunkiem zmian na w zakresie finansów cyfrowych na europejskich rynkach finansowych jest[13]:

- rozwój innowacyjnych modeli biznesowych banków,
- wspieranie wdrażania nowych technologii, takich jak blockchain, sztuczna inteligencja i usługi w chmurze w sektorze finansowym,
- zwiększanie poziomu cyberbezpieczeństwa i integralności systemu finansowego.

Analizując poziom rozwoju innowacyjności oraz indeks fintechizacji, można zauważyć istotną przestrzeń do rozwoju innowacyjności polskiego sektora bankowego. Najdynamiczniej rozwijającym się segmentem rynku w zakresie innowacyjności jest rynek płatności (22% ogólnej liczby fintechów w tym zakresie działa w Polsce)[14]. Dlatego też banki powinny poszukiwać nowych form – zwłaszcza współpracy z innowacyjnymi podmiotami. Jednym z takich rozwiązań jest technologia, która zarówno odpowiada preferencjom konsumentom usług finansowych, jak i umożliwia obniżenie kosztów prowadzenia działalności przez banki – np. rozwiązania chmurowe, które są przełomowymi technologiami w zakresie cyfryzacji rynku bankowego.

Co warte podkreślenia, banki bardzo często już współpracują z podmiotami, które oferują w swojej grupie takie rozwiązania, w związku z tym poszerzenie współpracy w tym zakresie mogłoby być dokonane w stosunkowo krótkim czasie, z korzyścią dla całego rynku finansowego. Głównymi globalnym podmiotami jeśli chodzi o świadczenie rozwiązań chmurowych są bigtechy, które w ostatnich latach oferują coraz więcej usług i produktów na rynku

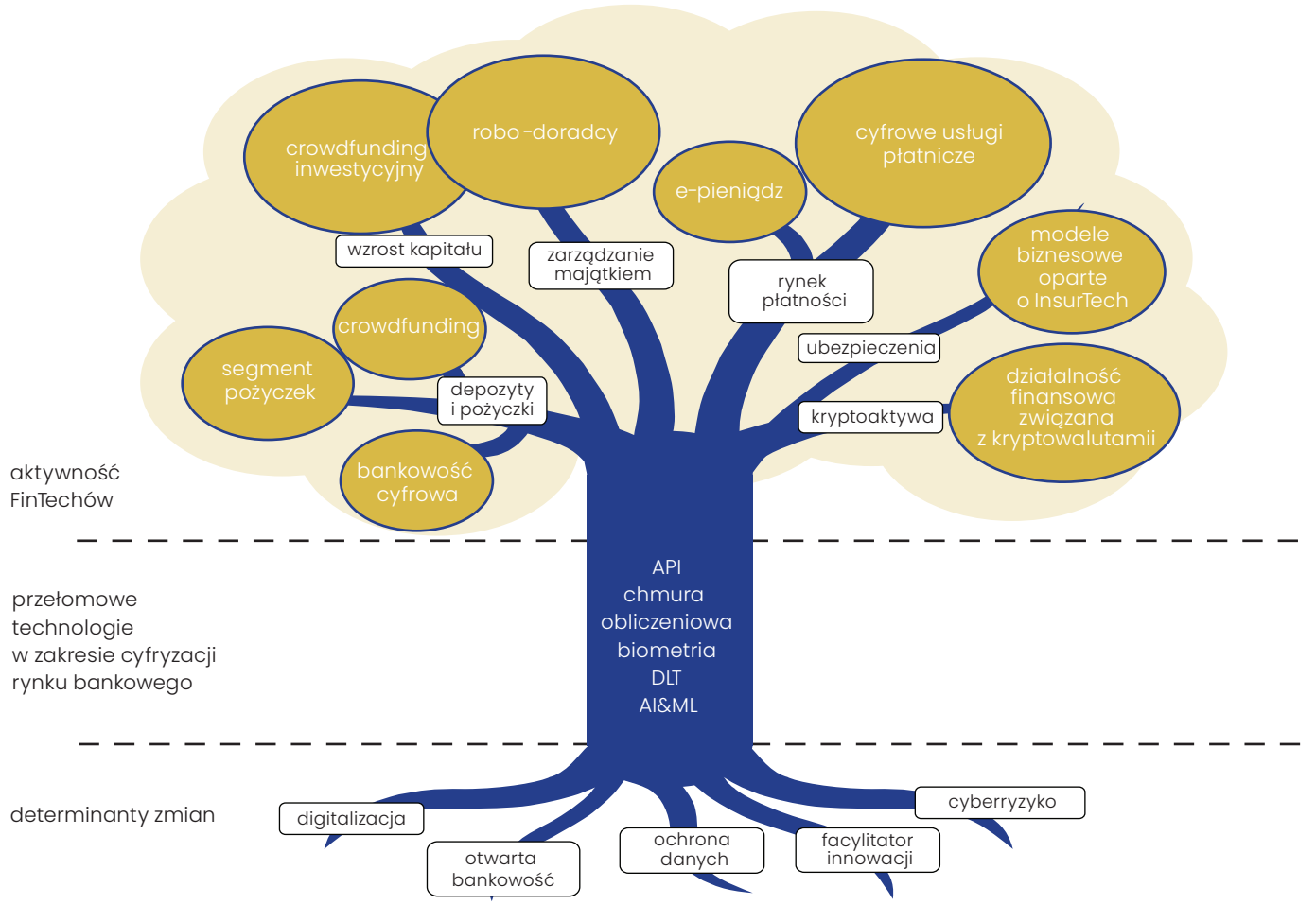
12 Szczegółowa metodologia przeprowadzanego badania wg *European Innovation Scoreboard* https://research-and-innovation.ec.europa.eu/system/files/2023-07/ec_rtd_eis-2023-methodology-report.pdf, dostęp z dnia 3.11.2023.

13 *Digital Finance*, European Commission, https://finance.ec.europa.eu/digital-finance/what-digital-finance_en, dostęp z dnia 3.11.2023.

14 Szerzej: *Mapa polskiego FinTechu*, cashless.pl, https://www.cashless.pl/13778-mapa-polskiego-fintechu-2023-cashless-fintech-2023, dostęp z dnia 3.11.2023.

Fot. Linus/stock.adobe.com

Schemat 4. Drzewo wskazujące na kierunek rozwoju sektora cyfryzacji rynku finansowego



Źródło: Szerzej: J. Ehrentraud, D. G. Ocampo, L. Garzoni, M. Piccolo, Policy Responses to Fintech: a Cross-Country Overview, BIS, 30 January 2020, s. 6.

finansowym. Dodatkowo mocnymi ich stronami, zwłaszcza spółek wdrażających rozwiązania w zakresie cyfryzacji usług bankowych, są[15]:

- bardzo wysokie zasoby finansowe,
- przewaga technologiczna (np. w usługach chmury obliczeniowej, systemów),
- dopasowanie usług do potrzeb i preferencji klienta,
- bogata baza danych o klientach i możliwości big data i data analytics,
- ciągła obecność w mediach, umiejętny marketing, szeroka promocja, PR,
- stały kontakt z liczną grupą klientów, którzy już korzystają z określonych usług GAFA(M), GANDALF, BAT,
- dobre nastawienie do firmy wśród licznej grupy klientów (chociaż nie brakuje też osób z negatywnym nastawieniem),
- doświadczenie poza świadczeniem usług finansowych.

W związku z istotnymi nakładami finansowymi związanymi z budowaniem lub rozbudowywaniem własnych infrastruktur IT, sektor bankowy może w efektywniejszy sposób wykorzystać istniejące już rozwiązania chmurowe oferowane przez duże firmy technologiczne. Obecnie korzystanie z chmury obliczenio- →

15 J. Górka, *Banki, GAFAM, FinTech w gospodarce współdzielenia – equalibrium współpracy i konkurencji*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, 2018, nr 531, s. 155–156.

Tabela 1. Procent firm wykorzysujących rozwiązania chmurowe w krajach UE

	2018	2020	2021
Szwecja	57,2	69,5	75,4
Finlandia	65,3	75,5	75,3
Niderlandy	48,2	52,6	64,9
Dania	55,6	66,9	64,8
Włochy	22,5	59,1	60,5
Irlandia	45,2	50,9	58,8
Estonia	33,9	56,3	57,5
Malta	36,5	52,2	57,1
Belgia	40,2	53,2	53,0
Cypr	26,6	34,6	50,3
Czechy	26,5	28,9	43,8
Słowenia	26,3	38,6	42,7
Niemcy	22,4	33,3	41,6
UE – 27	23,9	36,1	41,0
Austria	23,3	38,1	40,4
Chorwacja	30,7	39,0	39,2
Słowacja	21,1	25,6	36,1
Portugalia	24,7	29,0	34,7
Litwa	22,6	30,8	33,6
Luksemburg	24,5	29,1	33,5
Hiszpania	22,0	26,2	30,9
Francja	19,4	26,9	29,4
Polska	11,5	24,4	28,7
Łotwa	14,5	21,3	28,5
Węgry	18,0	25,2	26,4
Grecja	12,8	16,7	20,7
Rumunia	10,3	15,7	14,1
Bułgaria	8,3	10,9	12,8

Źródło: opracowanie własne na podstawie danych Eurostat: https://ec.europa.eu/eurostat/databrowser/view/isoc_cicce_use/default/table?lang=en, dostęp z dnia 3.11.2023.

wej i zastępowanie tradycyjnych platform tymi nowymi technologiami jest jednym z kluczowych wyzwań na globalnym rynku finansowym[16].

Niemniej, wg danych Eurostatu, zaledwie 29% firm w Polsce aktywnie wykorzystywało rozwiązania chmurowe, co jest dużo niższym wynikiem aniżeli średnia dla krajów UE (41%). Dlatego też Polska jest rynkiem wschodzącym, który w zakresie wdrażania rozwiązań chmurowych w instytucjach finansowych ma wiele szans na poprawienie innowacyjności.

Rozwiązania chmurowe są coraz bardziej powszechne. Coraz więcej instytucji na całym świecie przenosi swoje dane do chmury. Aczkolwiek wśród globalnych trendów można zauważyć, że kluczowym elementem nie jest już migracja danych, a szybkie wdrażanie coraz to nowszych usług w chmurze17. Ponadto, na podstawie licznych badań, wskazuje się jeszcze jedną kluczową cechę dotyczącą skuteczności wdrożenia rozwiązań chmurowych w instytucji – zwłaszcza finansowej. Sugeruje się, że przed wprowadzeniem nowych technologii, zwłaszcza takich jak *cloud computing*, powinno się przeprowadzić wiele szkoleń personelu. Wskazuje się, że kultura korporacji i poziom świadomości pracowników są decydującymi czynnikami w zakresie skuteczności stosowania tej technologii[18]. Dlatego też przed rynkiem bankowym w Polsce stoją liczne wyzwania związane z wdrażaniem rozwiązań chmurowych, które – jeśli zostaną przeprowadzone w efektywny sposób – istotnie wpłyną na konkurencję polskich banków na rynku krajowym i międzynarodowym. •

---

16 M. Darbandi, S. Haghgoo, M. Hajiali, A. Khabir, *Prediction and estimation of next demands of cloud users based on their comments in CRM and previous usages*, in: 2018 International Conference on Communication, Computing and Internet of Things (IC3IoT), IEEE, 2018, pp. 81–86.

K. Zanbouri, N.J.I.J. o C S Jafari Navimipour, *A cloud service composition method using a trust-based clustering algorithm and honeybee mating optimization algorithm 33* (5) (2020) e4259.

17 *State of Cloud 2023, How organizations are maturing in the cloud*, https://learn.pluralsight.com/resource/offers/2023/state-of-cloud?utm_source=google&utm_medium=paid search&utm_campaign=upskilling-and-reskilling&utm_term=b2b-emea-whitepaper-state-of-cloud&utm_content=whitepaper-cloud&gad_source=1&gclid=CjwKCAjw7o-eqBhBwEiwALyHLM8IdGqyRDsKMeU-roVKiRi5HDZ-54WEkCCmKlP7hY_7v2Qj-wYYIdZRoCEcMQAvD_BwE, dostęp z dnia3.11.2023.

18 H. Hamidi, S. H. Seyed Lotfali, *Analysis of Role of Cloud Computing in Providing Internet Banking Services: Case Study Bank Melli Iran*, International Journal of Engineering, Transactions B: Applications, Vol. 35, No. 05, (2022) pp. 1082–1088.

Moda czy konieczność?

Potrzeba zapewnienia funkcjonowania infrastruktury krytycznej przez banki nawet w warunkach trwającej wojny to jeden z argumentów za wykorzystaniem chmury obliczeniowej. Dodatkowym czynnikiem skłaniającym do migracji jest atrakcyjność kosztowa rozwiązań cloudowych w stosunku do tradycyjnych.

Korzystanie z usług związanych z przetwarzaniem w chmurze wymaga zmiany w sferze mentalnej i zaakceptowania przez biznes, że nie wszystko, co jest potrzebne do prowadzenia działalności musi być własnością firmy. Łatwiej będzie wtedy zarządom podejmować decyzje o wykorzystywaniu chmury. Nie będą musiały martwić się kosztami związanymi z lokalnym hostingiem danych, zarówno gdy chodzi o wdrażanie, jak i utrzymanie niezbędnej do tego infrastruktury. Oferowany przez dostawców chmury model pay-as-you-go pozwala firmom płacić za te usługi, z których korzystają, co zmniejsza koszty.

Fot. Gorodenkoff/stock.adobe.com

Od cloudu nie ma odwrotu

W opublikowanym przez Straits Research badaniu dotyczącym rynku chmury obliczeniowej, całkowity adresowalny rynek dla cloudu w 2022 r. wyceniono na 337,76 mld USD i założono że do 2031 r. osiągnie on wartość 1412,39 mld USD, rosnąc w tym czasie średnio co roku o 17,23%.

Zgodnie z prognozami Gartnera, opublikowanymi 29 listopada 2023 r., do 2028 r. chmura stanie się koniecznością biznesową, a całkowite wydatki na globalne usługi w chmurze publicznej w 2024 r. wyniosą 679 mld USD. Natomiast za cztery lata przetwarzanie w niej przestanie być przełomem technologicznym i stanie się niezbędnym elementem utrzymania konkurencyjności biznesu. Jak podano, wydatki na usługi IT w chmurze publicznej stale rosną i w 2027 r. przekroczą 1 bln USD.

Gartner podał także, że w 2024 r. największy wzrost wydatków użytkowników końcowych odnotuje infrastruktura jako usługa (IaaS) – 26,6% oraz platforma jako usługa (PaaS) – 21,5%. Innym ważnym trendem napędzającym wydatki na chmurę jest systematyczny wzrost popularności branżowych platform chmurowych. Uwzględniają one istotne dla danych branż wyniki biznesowe, łącząc podstawowe usługi oprogramowania jako usługi SaaS, PaaS i IaaS w kompleksową ofertę produktów z możliwościami ich komponowania. Gartner przewiduje, że do 2027 r. ponad 70% przedsiębiorstw będzie korzystać z branżowych platform chmurowych, podczas gdy w 2023 r. czyniło tak mniej niż 15%.

Ostatnie lata były złotym wiekiem dla przetwarzania w chmurze, a trend ten zyskuje na popularności w każdej branży. Usługi w chmurze stają się coraz częściej priorytetem firm na całym świecie, dzięki nim mogą one ograniczyć wydatki na infrastrukturę i zwiększyć elastyczność operacyjną. Wątpliwości dotyczących potrzeby rozwijania przetwarzania w chmurze nie ma także Komisja Europejska. Jest ono, jej zdaniem, kluczowe dla zwiększenia suwerenności Europy.

Chmura w Polsce

Opublikowany 14 lutego 2023 r. raport PMR przewiduje wysokie tempo wzrostu rynku chmury obliczeniowej – 3,6 mld zł w tym roku (w 2022 r. rynek osiągnął wartość 2,9 mld zł). Stwierdzono w nim, że rynek chmury obliczeniowej w Polsce po raz kolejny wykazał wysokie tempo wzrostu, rosnąc w 2022 r. o blisko 28%. Średni roczny wzrost w latach 2023–2028 ma nie spadać poniżej 20%, przy czym większy wzrost odnotuje model chmury publicznej.

Analitycy wśród czynników wpływających na wzrost rynku wymieniają takie zjawiska, jak pandemia i związany z nią gwałtowny wzrost inwestycji w narzędzia usprawniające pracę zdalną →

i bezpieczeństwo zasobów firmy oraz postępującą transformację cyfrową przedsiębiorstw w Polsce i związane z tym zwiększone zapotrzebowania na narzędzia i usługi korzystające z tej technologii. Z badań PMR, przeprowadzonych na potrzeby tegorocznej edycji raportu, wynika, że wojna w Ukrainie spowodowała zmianę nastawienia do chmury ok. 30% przedsiębiorstw w Polsce. W przypadku dużych firm, co piąta przyznała, że to właśnie wojna jest czynnikiem, wpływającym na decyzję o migracji do chmury.

Jeśli chodzi o sektor finansowy, w tym banki, to regulatorzy jeszcze nie tak dawno podchodzili z rezerwą do takich rozwiązań, ale sytuacja zmieniła się wraz z opublikowaniem przez UKNF 23 stycznia 2020 r. komunikatu dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej.

Bankowość w chmurze

Do korzystania z rozwiązań chmurowych nie trzeba przekonywać przedstawicieli bankowości niezmiernie szybko przecież implementującej nowe technologie. Które z nich są dziś dla banków szczególnie atrakcyjne? **Bernard Marr** w artykule opublikowanym na portalu „Forbes" w październiku 2022 r. podkreślił, że wśród pięciu najważniejszych trendów w chmurze obliczeniowej priorytetem w roku 2023 będą wydatki na cyberbezpieczeństwo i budowanie odporności na wszelkie możliwe zagrożenia. Jednym z rozwiązań je zwiększających jest wykorzystanie sztucznej inteligencji i technologii predykcyjnej do wykrywania zagrożeń, zanim spowodują one problemy. Rozwiązaniem mogą być rozwiązania chmurowe typu Security as a Service. Dzięki nim możliwe jest np. stałe monitorowanie incydentów bezpieczeństwa i szybka reakcja na nie.

Najwięksi dostawcy usług chmurowych, jak Amazon, Google i Microsoft, rozwijają własne technologie sztucznej inteligencji i udostępniają klientom nowe usługi, co umożliwia budowanie rozwiązań z ich wykorzystaniem. Szybko rozwijają się w chmurze usługi typu low-code i no-code, które pozwalają na zaprojektowanie prawie każdego rodzaju rozwiązań cyfrowych, także z wykorzystaniem sztucznej inteligencji i uczenia maszynowego, przy coraz mniejszym bezpośrednim zaangażowaniu własnych specjalistów i infrastruktury.

Eksperci Straits Research zwracają uwagę na segment analityki biznesowej. Dostawcy usług w chmurze prześcigają się w opracowywaniu nowoczesnych narzędzi analitycznych dla klientów korporacyjnych. Wśród znaczących dostawców chmurowych platform analitycznych są takie firmy, jak IBM, Google, SAS, Microsoft i Salesforce.

Nawet duże banki mogą w najbliższych latach mieć problem z samodzielnym rozwijaniem wymienionych powyżej technologii, nie mówiąc już o związanych z tym kosztach. Pewne wątpliwości związane z migrowaniem do chmury budzą opóźnienia, przepustowość łączy i bezpieczeństwo. Obecnie modne są chmury hybrydowe, na popularności zyskują też modele wielochmurowe. W przypadku infrastruktury multicloud korzysta się z usług kilku dostawców, co pozwala lepiej rozłożyć obciążenia w wielu środowiskach i poprawić zarządzanie ryzykiem.

Rozwiązaniem, o którym dużo się ostatnio mówi, jest edge computing, czyli przetwarzanie brzegowe. To kolejny krok w kierunku optymalizacji, a zarazem technologia, która umożliwia przetwarzanie i przechowywanie danych w centrach zlokalizowanych w pobliżu sieci użytkowników. Połączenie chmury i przetwarzania brzegowego daje wiele korzyści. Należą do nich zwiększona prędkość przetwarzania danych, niskie lub zerowe opóźnienia czasu na uzyskanie odpowiedzi oraz mniejsze wykorzystanie przepustowości. Wśród zalet wymienia się też zwiększone bezpieczeństwo danych oraz niższe koszty związane z ich przesyłaniem, przechowywaniem i przetwarzaniem w chmurze.

Na stronach Komisji Europejskiej podano, że choć przetwarzanie w chmurze odbywa się obecnie głównie w dużych centrach danych, to do 2025 r. tendencja ta się odwróci i 80% wszystkich informacji będzie przetwarzanych w inteligentnych urządzeniach bliżej użytkownika, to znaczy z wykorzystaniem edge computing.

Z chmury obliczeniowej instytucje finansowe albo już korzystają lub zamierzają to zrobić. Tak wynika z sondażu PwC po raz pierwszy przeprowadzonego w regionach CEE (Europa Środkowo-Wschodnia) i EMEA (Europa, Bliski Wschód i Afryka) oraz po raz drugi w Polsce. Zgodnie z tym badaniem już 35% instytucji finansowych wdrożyło chmurę we wszystkich lub w większości obszarów swojej działalności, a 46%, które obecnie nie stawiają na nią, planuje przenieść całą działalność do niej w ciągu najbliższych dwóch lat. Raport wskazuje, że 24% instytucji stosuje holistyczne i wieloaspektowe podejście do chmury, co pozwala im usprawnić działalność.

W obecnych uwarunkowaniach organizacje, w tym banki, nie mogą sobie pozwolić na zignorowanie cloudu – co do tego nikt nie ma wątpliwości. Podstawowe technologie związane z przetwarzaniem w chmurze są już dojrzałe i sprawdzone. Wśród głównych graczy na tym rynku wymienia się takie firmy, jak Adobe, Google, IBM, Microsoft, NTT Communication, Oracle, Alibaba, AWS, CenturyLink, Fujitsu, Rackspace, SAP, Verizon i Vmware. Dodatkowym argumentem za przetwarzaniem w chmurze jest nie tylko bardziej wydajne uruchamianie aplikacji, ale także to, że funkcjonujące w niej centrum danych wytwarza mniejsze ilości dwutlenku węgla niż jego odpowiednik działający lokalnie. To kolejny krok do osiągnięcia przez organizację celów zrównoważonego rozwoju.

Oczywiście są też przeszkody na drodze do osiągnięcia przez branżę finansową wymiernych wartości z technologii chmurowych. Przedstawiciele polskiego sektora finansowego odpowiadając na pytania umieszczone w ankiecie PwC wskazywali głównie na wyzwania związane z dostawcami usług w chmurze (41% odpowiedzi), ograniczenia budżetowe i/lub inwestycje (41%), lukę talentów (35%). Natomiast za najważniejsze kompetencje, które należy rozwijać w ciągu najbliższych 12 miesięcy uznali: gromadzenie wymagań dotyczących chmury, zarządzanie projektami migracyjnymi, rozwój i integrację natywną dla chmury oraz cyberbezpieczeństwo. **(Oprac. BoSz)**

Nowa filozofia funkcjonowania

Korzyści wynikające z migracji do chmury nie ograniczają się do optymalizacji procesów i kosztów funkcjonowania instytucji finansowej. Przenoszenie zasobów bankowych na serwery zewnętrzne wymaga zredefiniowania modelu biznesowego i operacyjnego organizacji, jednak rekompensują to zwiększenie bezpieczeństwa i odporności instytucji na zagrożenia.

Fot. fotomek/stock.adobe.com

Otrzymuje ona m.in. dostęp do szeregu narzędzi, umożliwiających – co istotne dla instytucji finansowych – dynamiczne dostosowywanie oferty do szybkich i nie zawsze dających się przewidzieć zmian realiów rynkowych. Dzięki temu mogą one osiągnąć znaczącą przewagę konkurencyjną. Choć jednak banki są zainteresowane migracją, to tak naprawdę dopiero się ona zaczyna. Decydującą rolę odgrywają tu kwestie technologiczne; czasami bowiem dostosowanie systemów wykorzystywanych w bankach do środowiska chmurowego wymaga szeregu działań, choćby weryfikacji możliwości ich przeniesienia z uwagi na zapisy licencji etc.

Śpiesz się powoli

W normalnych warunkach przygotowania do przeniesienia zasobów do chmury z reguły zajmują trochę czasu. Banki powinny przeprowadzić analizę obecnych systemów IT, a niekiedy zrealizować business case – oczywiście we współpracy z partnerami, w tym dostawcami usług chmurowych. Dzięki temu migrację będzie można odpowiednio zaplanować. W chmurze Amazon Web Services (AWS) występują programy typu map, wspierające zainteresowane przenosinami instytucje w tworzeniu business case'ów czy systemów typu landing zone, albo modelu operacyjnego, który uwzględniać będzie nie tylko kwestie technologiczne, ale również niezbędne zmiany w ich kulturze organizacyjnej, w procesach i sposobie obsługi. Wszystko po to, by migrację zrealizować jak najefektywniej.

Dlaczego przy budowie business case dla wybranych systemów instytucje finansowe powinny skorzystać z pomocy dostawców usług chmurowych oraz ich partnerów? Po prostu dlatego, że posiadają oni sprawdzone rozwiązania, które ułatwiają przeanalizowanie infrastruktury banku oraz określenie co należy wykonać od strony technologii, aby migracja zakończyła się sukcesem. Przy czym w trakcie analizy pod uwagę powinny zostać wzięte zarówno aspekty techniczne, jak i biznesowe – czyli określenie jakie procesy w ramach banku, jego systemów monitoringu, compliance, governance, bezpieczeństwa należy dostosować do chmury.

Skoro zostanie to ustalone, należy dobrać rozwiązania, które w ramach chmury powinny funkcjonować. Migracja związana jest ze zmianą kultury oraz systemów, aby zatem niepotrzebnie nie podwyższać kosztów, warto przeprowadzić szkolenia obecnego zespołu, powołać Cloud Center of Excellence (Centrum Doskona- →

łości w Chmurze) oraz określić sposoby jego prowadzenia. Wszystko to rzecz jasna w ścisłej współpracy z dostawcą usług chmurowych oraz partnerem technologicznym – co znacząco usprawni proces migracji do chmury, zwłaszcza publicznej.

Ostrożności nigdy za wiele

Bezpieczeństwo, compliance oraz zarządzanie ryzykiem w chmurze wyglądają inaczej niż w środowisku on premise. Tu rejestrowane są wszystkie zdarzenia, każde dołączenie nowego serwera, dostęp do wybranej aplikacji, jej wdrożenie pozostawiają ślad cyfrowy, co w trybie rzeczywistym może owocować odpowiednią akcją czy reakcją. Warto także wdrożyć tzw. metodykę continuous compliance, która zapewnia zgodność wszelkich systemów bankowych z założeniami ustalonymi przez działy compliance. Można też zwiększyć bezpieczeństwo – czyli wpływać na konfigurację aplikacji, które mają zbyt „niski" poziom bezpieczeństwa lub nie przestrzegają reguł korporacyjnych. Jeśli developerzy nie przestrzegają podanych przez instytucję zasad, można uniemożliwiać propagację ich rozwiązań na wyższe środowiska.

To istotne, bowiem przy wydawaniu komunikatu chmurowego, Komisja Nadzoru Finansowego kierowała się intencją, by banki podejmujące decydujące się na migrację do chmury dochowały wysokich standardów bezpieczeństwa; zdawały sobie sprawę, z czym ona się wiąże; potrafiły zaadresować wszystkie ryzyka, wiążące się z utrzymaniem systemów w chmurze oraz odpowiednio przygotowały i wykształciły kadrę.

Nowa kultura pracy

Chmura umożliwia diametralną zmianę kultury pracy. Umożliwia testowanie nowych pomysłów biznesowych i szybkie wycofanie się w przypadku stwierdzenia, że nie zostaną one dobrze przyjęte przez rynek. Transformacja chmurowa powinna stanowić czynnik wyzwalający głębsze zmiany w organizacji, te zaś umożliwią pełne wykorzystanie możliwości, jakie daje cloud – podkreśla **Maciej Jeruzal**, dyrektor Biura Automatyzacji Procesów w Departamencie Transformacji Cyfrowej Nest Banku. Przyjęcie takiego założenia sprawia, iż migracja zasobów banku do chmury nie może być traktowana jedynie w kategoriach zmiany technologicznej, tylko, jak wskazuje **Tomasz Fryc**, dyrektor Departamentu Infrastruktury IT i Chmury Obliczeniowej w Alior Banku, powinna się wpisywać w holistyczny proces, ukierunkowany na osiągnięcie celów typowo biznesowych, w rodzaju poprawy efektywności funkcjonowania banku. Dlatego i sam wybór rozwiązania chmurowego czy modelu funkcjonowania tej formy outsourcingu nie może przebiegać bezrefleksyjnie. Nie można zgodzić się z **Krzysztofem Opalińskim**, menedżerem dyscypliny Cloud Advisory w Formacji Transformacji Chmurowej PKO Banku Polskiego, iż przyjmując kurs na chmurę, bankowcy powinni uwzględnić wszelkie aspekty opłacalności tego przedsięwzięcia, a więc oprócz finansowych również i te trudniej mierzalne, jak choćby operacyjne, organizacyjne czy wreszcie technologiczne.

Maksymalnie wykorzystać możliwości cloudu

Nabierają one szczególnego znaczenia z uwagi na dotychczasowe zasoby IT instytucji finansowych, które siłą rzeczy generują dług technologiczny. Słusznie uważa Maciej Jeruzal, iż nie każdy system wdrożony 12 lat temu lub jeszcze wcześniej będzie się kwalifikować do migracji, stąd też planując jej przebieg, lepiej w pierwszej kolejności budować w chmurze całkiem nowe narzędzia, przy równoczesnej optymalizacji i adaptacji dotychczasowych, o ile będą one spełniać warunki do przeniesienia. Zdaniem **Amadeusza Paliwody**, Program Manager Programu Chmurowego Grupy Raiffeisen Bank International, część legacy software da się adaptować do funkcjonowania w cloudzie przy stosunkowo niewielkich nakładach. Z tych właśnie przyczyn rozwiązania lift & shift co do zasady nie sprawdzają się w transformacji chmurowej, stanowiąc, jak to określa Krzysztof Opaliński, jej najgorszy wariant, za każdym razem priorytetem powinno wszak być maksymalne wykorzystanie nowych możliwości, jakie daje cloud, choćby w zakresie skalowalności czy szybkości działania.

W ślad za ową gruntowną zmianą podejścia do budowy, rozwoju i utrzymania rozwiązań IT w duchu DevOps musi następować podobna metamorfoza w obszarze organizacyjnym, eliminująca chociażby główną barierę rozwoju instytucji finansowej w postaci skostniałej, silosowej struktury. Rzecz w tym, że w niektórych obszarach, jak choćby w przypadku analityki, alternatywy dla chmury w zasadzie nie ma. Zdaniem **Elżbiety Żebrowskiej-Poziemskiej**, dyrektor Departamentu Customer Intelligence w VeloBanku, możliwości działania w modelu on premise zostały praktycznie wyczerpane, zatem jeśli myśli się poważnie o spożytkowaniu uczenia maszynowego, to przejście do cloudu staje się niejako naturalną koniecznością. Aspektem, na który warto zwrócić szczególną uwagę, jest optymalne zagospodarowanie zasobów ludzkich, co zwłaszcza w dobie triumfalnego postępu robotyzacji i upowszechniania rozwiązań bazujących na AI nabiera szczególnego znaczenia. I nie chodzi tu tylko o wychowanie kadr do obsługi procesów outsourcingowych, ale – jak uważa **Grzegorz Pędzisz**, CIO w Volkswagen Financial Services – skłonienie do długofalowej współpracy z bankiem specjalistów z młodszych generacji, dla których aplikacje chmurowe stanowią codzienne narzędzie pracy. W ten kontekst wpisuje się też potrzeba reskillingu

Fot. ipopba/stock.adobe.com

i upskillingu dotychczasowych kadr, co – jak sugeruje przedstawiciel PKO Banku Polskiego – winno towarzyszyć technologicznej stronie migracji.

Pięć kluczowych czynników dobrej transformacji

Dyskusję o optymalnym modelu transformacji chmurowej w sektorze finansowym komplikuje fakt, iż bank bankowi nierówny. **Bartosz Kublik**, wiceprezes Związku Banków Polskich, który przez kilkanaście lat szefował Bankowi Spółdzielczemu w Ostrowi Mazowieckiej, jednej z największych lokalnych instytucji finansowych w Polsce, zwraca uwagę, iż różnice dotyczą zarówno zasobów finansowych, ludzkich, jak i technologicznych, a nawet modelu funkcjonowania. Szczególnie spółdzielcy, dysponując relatywnie niewielkimi zasobami finansowymi, mogą mieć problem z zakupem najnowszych technologii, a chmura może być dla nich szansą.

Dlatego, zdaniem wiceprezesa ZBP, planując przeniesienie zasobów do cloudu, należy zwrócić uwagę na pięć istotnych czynników. Pierwszy z nich to analiza ryzyka w zakresie ciągłości działania, obejmująca możliwość zapewnienia przez instytucję zasobów w tak dynamicznie zmieniającym się otoczeniu. Z kwestią tą wiąże się wydajność i skalowalność dotychczas posiadanych zasobów i koszt ich modernizacji, co nierzadko przemawia za chmurą – zdaniem Bartosza Kublika, sama tylko wymiana serwerowni co kilka lat może pochłonąć środki liczone w milionach złotych, co dla lokalnego banku stanowi lwią część zasobów finansowych na obszar IT. Niezwykle istotną wartością dodaną, jaką zapewnia środowisko chmurowe, jest nieporównanie większa elastyczność, w tym możliwość skuteczniejszego i szybszego testowania wdrażanych rozwiązań, co z kolei wydatnie skraca time to market.

Z punktu widzenia bankowości szczególną rolę odgrywają względy bezpieczeństwa, w tym również możliwość pozyskania na własną rękę wykwalifikowanych specjalistów z obszaru cybersecurity, co zwłaszcza w przypadku instytucji finansowych o zasięgu lokalnym i regionalnym stanowić może wyzwanie ponad siły, a to z uwagi na postępujący deficyt talentów IT. Do tego wszystkiego dochodzi aspekt kosztowy, a tu nie ma wątpliwości, iż własne zasoby stają się coraz droższe w porównaniu z narzędziami oferowanymi w cloudzie. Wydaje się zatem, iż alternatywy dla chmury po prostu brak. →

Sukces niejedno ma oblicze

Jak zatem ocenić, czy i na ile migracja do środowiska chmurowego przyniosła oczekiwany efekt? Zdaniem bankowców, trudno byłoby wskazać uniwersalne mierniki powodzenia transformacji. Elżbieta Żebrowska-Poziemska wskazuje, iż nawet w ramach jednej instytucji możemy mieć dziesiątki wskaźników odnoszących się do funkcjonowania poszczególnych aplikacji i systemów w nowych uwarunkowaniach. Według Amadeusza Paliwody, istotnym kryterium będą strategiczne cele przeprowadzonej migracji, takie jak skrócenie time to market, redukcja zbyt rozbudowanych zasobów IT czy optymalizacja wykorzystania kadr, a właściwe zdefiniowanie owych zadań stanowić będzie punkt odniesienia do oceny przebiegu całego procesu. Pewnym wspólnym kryterium dla wszystkich instytucji finansowych, na które zwraca uwagę Tomasz Fryc, może się okazać swoboda wyboru pomiędzy oferowanymi rozwiązaniami chmurowymi i on premise.

Oczywiście, można też postawić pytanie, czy w ogóle powinniśmy mówić o sukcesie wdrożenia cloudu w rozumieniu działania jednorazowego, bowiem, jak słusznie sugeruje Krzysztof Opaliński, mamy do czynienia raczej z pewnym procesem o charakterze ciągłym. W tym rozumieniu sukcesem jest już samo podjęcie rękawicy, fakt ten wskazuje bowiem, iż bankowcy zdają sobie sprawę z rozlicznych korzyści, jakie zapewnia migracja. Ewentualnym, choć trudno mierzalnym wskaźnikiem, może być też moment, w którym przejście do chmury stało się naturalnym elementem, determinującym dalsze funkcjonowanie organizacji.

Praktyczne przykłady takiego właśnie sukcesu są w stanie wskazać dostawcy usług chmurowych. **Sylwia Samulczyk**, dyrektor Centrum Usług Operacyjnych w firmie Asseco Poland, podaje przykład migracji do chmury publicznej, która odbyła się w tym roku i spełniła oczekiwania klienta w dziedzinie skalowalności oraz rozwoju biznesu, w tym przypadku bazującego na udzielaniu mikropożyczek, a zatem wymagającego szybkiego podejmowania licznych decyzji. Alternatywnym przykładem wskazywanym przez przedstawicielkę Asseco Poland jest bank podlegający procesowi restrukturyzacji, tu priorytety z oczywistych względów były całkiem inne, zatem projekt dało się wdrożyć w chmurze prywatnej Asseco w kilka miesięcy. Generalnie przesłankami świadczącymi o powodzeniu migracji będą kwestie typowo biznesowe, w rodzaju lepszego customer experience czy też szybszego time to market. Sukces osiąga się wówczas, gdy cloud uzupełnia ofertę, pozwalając szybciej reagować w określonych aspektach.

Regulacje: koniec niepewności

Punktem zwrotnym dla całej polskiej bankowości, jeśli chodzi o transformację chmurową, był wspomniany już, wydany z początkiem roku 2020 komunikat KNF dotyczący przetwarzania informacji w cloudzie. Krzysztof Opaliński nie ma wątpliwości, iż dokument ten zakończył wieloletni okres niepewności, któremu towarzyszyła potrzeba dogłębnej analizy każdego projektu migracji bez jednoznacznego punktu odniesienia. Są oczywiście obszary, w których podejście regulatora pozostało restrykcyjne, tak jest choćby w odniesieniu do rozwiązań typu SaaS, jednak, zdaniem bankowca, ma to swoje dobre strony, łatwiej wszak zniuansować jednoznaczny i precyzyjny przepis aniżeli dopuścić do anarchii w tak istotnej sferze. Dotyczy to również sztucznej inteligencji, która – zdaniem przedstawicielki VeloBanku – daje na tyle nieograniczone możliwości użycia danych, że niezbędna jest silna ochrona konsumenta na poziomie regulacyjnym.

Mec. **Michał Kulesza**, partner kierujący zespołem technologii finansowych i ekspert od cloudu w Kancelarii Rymarz Zdort Maruta, ukazuje jeszcze jeden pozytywny efekt przyjęcia przez polski nadzór komunikatu chmurowego, uświadomił on wszak instytucjom potrzebę wykonywania rzetelnej analizy ryzyk towarzyszących migracji. Doświadczenie to przynosi profity już obecnie, kiedy banki i inne podmioty obowiązane są do analizowania ryzyka – zarówno technologicznego, jak i organizacyjnego – przez rozporządzenie DORA, a już niebawem podobne wymogi stawiać będzie przed sektorem AI Act.

Obydwa te przepisy będą miały rangę rozporządzenia, a więc, jak podkreśla ekspert, ich stosowanie co do zasady będzie mieć charakter jednolity na całym terenie Unii Europejskiej, to zaś powinno skrócić procesy negocjacyjne w przypadku ewentualnych zakupów rozwiązań software, w tym również w sferze outsourcingu. Jego zdaniem łatwiej jest wspierać klientów, jeśli można bazować na wypracowanych wcześniej dokumentach, zamiast tworzyć wszystko od podstaw. Unijne ustawodawstwo umożliwia przede wszystkim określenie pewnego minimalnego, acz nieuchronnego poziomu ryzyka, który należy zaakceptować, by nie zamykać się na innowacje.

Opinię tę podziela Bartosz Kublik, jego zdaniem na samym początku tworzenia regulacji mamy nierzadko do czynienia z rozmijaniem się podejścia regulatora i rynku, jednak ostatecznym sprawdzianem dojrzałości regulacyjnej jest wypracowanie swoistej mapy drogowej, co miało miejsce również i w tym przypadku. Nie ma zatem wątpliwości, iż droga w chmury daje sektorowi bankowemu coraz większą szansę na lepszą przyszłość, – od zaangażowania poszczególnych instytucji zależy, czy faktycznie będzie ona świetlana.

Artykuł powstał na podstawie debaty eksperckiej, która odbyła się 15 listopada 2023 r. podczas konferencji IT@BANK 2023. Partnerem debaty była firma Asseco Poland. (**Oprac. ALa; KaJMo**)

Zdaniem bankowych praktyków

Jakie doświadczenia towarzyszyły wdrażaniu technologii chmurowych w polskich bankach? W których obszarach działania na rzecz migracji do cloudu napotykały na największe wyzwania, a także co wpływało na formułowanie strategii chmurowych? Z tym pytaniem zwróciliśmy się do przedstawicieli sektora, biorących aktywny udział we wdrażaniu nowych rozwiązań.

Fot. Lila DK/stock.adobe.com

Tomasz Hołubowicz
DYREKTOR BIURA USŁUG CHMUROWYCH, BANK PEKAO S.A.:

Analizując „Hype Cycle for Cloud Computing", opracowany przez Gartnera na rok 2023, można z pewnością stwierdzić, że Bank Pekao S.A. doskonale wpisuje się w obecne trendy chmurowe. Warto podkreślić, że podejście naszego banku jest racjonalne, co oznacza, że realizujemy te projekty, które przynoszą nam wymierne korzyści biznesowe i przyspieszają transformację cyfrową. Istotny jest również aspekt ludzki – chmura nie tylko sprawia, że nasze miejsce pracy staje się atrakcyjne dla pracowników, ale także przyciąga utalentowane jednostki, które chcą pracować z najnowszymi technologiami.

Bank operuje już w tej chwili produkcyjnie w dwóch chmurach publicznych, Google Cloud Platform oraz Microsoft Azure. Aby dojść do tego poziomu, przyjęliśmy strategię stworzenia ram przyjęcia chmury (tzw. landing zone), która obejmowała opracowanie strukturalnego podejścia do wdrażania nowych technologii w sposób zgodny z unikalnymi potrzebami banku i wymaganiami sektora finansowego. Prace obejmowały wprowadzenie solidnej architektury bezpieczeństwa i zaadresowania kwestii prywatności danych, bezpieczeństwa i zgodności. Następnie rozpoczęliśmy równoczesny rozwój platform chmurowych, który był skorelowany z pierwszymi migracjami systemów banku. To podejście umożliwiło nam szybkie korzystanie z zalet chmur publicznych, zabezpieczając jednocześnie bank przed ewentualną koniecznością przeprojektowania architektury platform chmurowych w przyszłości, w miarę wzrostu skali przemieszczonych systemów.

Obszarem chmur publicznych w banku zarządzają dedykowane zespoły chmurowe, funkcjonujące w modelu „Cloud Center of Excellence". Zespoły stale rozwijają platformy chmurowe, kładąc szczególny nacisk na powtarzalność wykorzystania produktów swojej pracy. Obejmuje to tworzenie wielokrotnie używanych modułów do powoływania zasobów oraz opracowanie uniwersalnej dokumentacji niezbędnej do spełnienia wymagań regulacyjnych i operacyjnych banku. Jednym z kluczowych zadań CCoE →

jest także rozwijanie kompetencji chmurowych w IT banku, a także w jednostkach biznesowych.

Warto podkreślić, że korzystamy ze wszystkich możliwości oferowanych przez dostawców chmur publicznych, takich jak dostęp do platform edukacyjnych, rekomendowane ścieżki rozwoju i certyfikacyjne. Organizujemy także meetUp'y oraz jesteśmy obecni na innych ogólnofirmowych platformach i forach wymiany wiedzy i doświadczeń. Pracownikom bardziej zainteresowanym chmurami udostępniamy również środowiska typu „sandbox" nauki, testowania, uczenia się poprzez praktykę. W przypadku zespołów odpowiedzialnych za utrzymanie systemów zmigrowanych do chmury, zapewniamy wsparcie kompetencyjne zawsze, gdy tylko tego potrzebują.

W Banku Pekao S.A. powszechne są już migracje systemów do chmur, a każdy nowy system jest rozważany do przeniesienia do jednej z dwóch chmur publicznych. W procesie modernizacji, systemy są również rozwijane w kierunku „cloud ready", umożliwiając przyszłą relatywnie łatwą i szybką migrację do chmur publicznych. Obecnie widzimy największy potencjał chmur dla systemów frontowych oraz systemów typu „data". Dlatego też bank już umieścił w chmurze niektóre systemy tego typu i kontynuuje migrację kolejnych.

Na szczycie „Hype Cycle", w obszarze największych oczekiwań, obecnie znajdują się usługi „Generative AI". W Banku Pekao, zarówno IT, jak i jednostki biznesowe, mają wysokie oczekiwania względem tej technologii. Dzięki łatwej dostępności dużej mocy obliczeniowej, niezbędnej m.in. do trenowania modeli oraz możliwości szybkiego rozpoczęcia pracy z GenAI, wiele jednostek biznesowych banku aktualnie testuje tego typu usługi w bezpiecznych piaskownicach oraz równolegle analizuje potencjalne korzyści biznesowe z ich wdrożenia. Warto zaznaczyć, że dostrzegamy również ogromny potencjał w usługach chmurowych typu ML/AI, starając się komercjalizować nasze pomysły oparte na tych usługach.

Podsumowując doświadczenia Banku Pekao S.A z chmurami publicznymi – mamy je, aktywnie je wykorzystujemy, rozwijamy kompetencje w obszarze coraz to nowszych usług, jesteśmy zgodni w trendami rynkowymi, a jednocześnie nieustannie rozbudowujemy platformy, dbając szczególnie o bezpieczeństwo danych naszych klientów.

Hubert Tarnowski
KIERUJĄCY WYDZIAŁEM INŻYNIERII DANYCH I MARIUSZ GROMADA, DYREKTOR DEPARTAMENTU CUSTOMER INTELLIGENCE, BANK MILLENNIUM:

W Banku Millennium, podróż z analityką w chmurze rozpoczęła się od implementacji platformy raportowej PowerBI, działającej w modelu hybrydowym (SaaS z utrzymaniem pełnej kontroli nad danymi). To doświadczenie pozwoliło zgłębić aspekty związane z compliance i bezpieczeństwem danych. Naszym kolejnym krokiem była implementacja platformy analitycznej AI („MilleAI" oparta na open-source i wykorzystywana w data science). Projekt dostarczył cennych wniosków dotyczących infrastruktury i integracji. Obecnie skupiamy się na strategicznej inicjatywie hiperpersonalizacji, która stawia przed nami wyzwanie związane z architekturą real-time multi-cloud, głównie w modelu SaaS.

Bazując na naszych bankowych doświadczeniach, możemy stwierdzić, że **kluczowymi wyzwaniami są**:

- **Bezpieczeństwo, Compliance i FinOps**: W naszej ocenie stanowią one główną część czasu dedykowanego na wdrożenie projektu chmurowego. Bezpieczeństwo danych, zarówno w trakcie przesyłania, jak i przechowywania, wymaga szczególnej uwagi. Wymagania compliance, wynikające z regulacji KNF oraz RODO, obejmują szczegółowe procedury dostępu do danych oraz zapewnienia ciągłości biznesowej. Niezbędne jest również ponowne przemyślenie modelu zarządzania budżetem. Są to zadania angażujące wiele działów w banku, co ma wpływ na złożoność realizacji projektów chmurowych w porównaniu do projektów realizowanych „lokalnie".
- **Użycie usług chmurowych**: ta pozostała część projektu, obejmuje infrastrukturę, taką jak sieć, dostarczenie i przechowywanie danych, dobór i konfigurację mocy obliczeniowej, implementację monitoringu, a także dostosowanie usług do specyficznych potrzeb biznesowych.

Naszym zdaniem, w kontekście strategii chmurowych, **kluczowe znaczenie mają**:

- **Modele subskrypcji**: Każdy z modeli ma swoje zalety i wyzwania, szczególnie w kontekście compliance i zarządzania.
  1) **Model IaaS** (Infrastructure as a Service): ten model jest najbliższy tradycyjnej infrastrukturze IT, zapewniając elastyczność rozbudowy i kontrolę nad środowiskiem sprzętowym. Jednakże, choć jest podobny do rozwiązań on-prem, niesie ze sobą wyzwania finansowe. Bank musi wciąż ponosić koszty zarządzania logiczną infrastrukturą, co może nie być opłacalne w dłuższej perspektywie.
  2) **Model PaaS** (Platform as a Service): jest bardziej efektywny z punktu widzenia zarządzania i compliance. Ułatwia tworzenie aplikacji bez konieczności zarządzania infrastrukturą na niższym poziomie. Jednakże wymaga od organizacji wysiłku podobnego do podejścia DevOps w modelu on-prem, co wiąże się z koniecznością dostosowania umiejętności i procedur.
  3) **Model SaaS** (Software as a Service): jest najbardziej zgodny z filozofią „cloud native", oferuje szybkie dostarczanie roz-

Fot. ipopba/stock.adobe.com

wiązań i wartości biznesowej. Jednakże ze względu na ograniczoną kontrolę nad przetwarzaniem danych, stanowi wyzwanie w kontekście compliance. Konieczna jest także dokładna weryfikacja, np. poprzez testy PoC (Proof of Concept), aby ustalić, w jakim stopniu usługa SaaS rzeczywiście minimalizuje potrzebę nadzoru ze strony banku.

4) **Multi-cloud**: Aby skutecznie wdrożyć strategię multi-cloud, ważne jest najpierw dokładne zrozumienie możliwości i „nauczenie się" jednego dostawcy chmurowego.

- **Optymalizacja kosztów**: storage w chmurze jest stosunkowo tani i idealnie nadaje się do przechowywania danych archiwalnych. Natomiast compute jest opłacalny przy okresowym wykorzystaniu, ale już znacznie mniej przy ciągłym dużym obciążeniu.

Podsumowując – technologia chmurowa zdecydowanie zyskała na znaczeniu, ale wiąże się z nowymi wyzwaniami, takimi jak nowe kompetencje i zmiana podejścia, dostosowanie procedur, wyzwania związane z architekturą multi-cloud, bezpieczeństwem oraz integracją z infrastrukturą lokalną. Mimo tych trudności chmura oferuje elastyczność oraz wartość poprzez dostęp do nowoczesnych usług i platform biznesowych (np.: automatyzacja marketingu, zarządzanie contentem, generatywna sztuczna inteligencja) dostarczanych przez światowych liderów, często niedostępnych w innych formach.

Sebastian Hutny
DYREKTOR DEPARTAMENTU DOSTARCZANIA USŁUG IT, CREDIT AGRICOLE BANK POLSKA:

Na rynku powszechne jest twierdzenie, że banki to instytucje technologiczne z licencją finansową. IT w obszarze finansowym wykracza poza rolę operatora technologii i dostarcza realnego wkładu do rozwoju biznesowego i oferowanych produktów. Doskonale to widać, gdy śledzi się wchodzenie nowoczesnych technologii do instytucji finansowych i ich rosnący udział w kreowaniu produktów biznesowych. Wydawałoby się, że dynamika rozwoju IT w bankach i oczekiwana elastyczność powinny skutkować masowym przenoszeniem swoich zasobów do chmury, tymczasem instytucje finansowe robią to ostrożnie i obok definicji chmury publicznej, prywatnej i hybrydowej możemy spotkać się z pojęciem chmury selektywnej. Czy jest to odwrócenie trendu chmurowego? Accenture w swoim badaniu z 2021 r. „Accenture Technology Vision"[1] wskazywało, że 94% CIO w bankowości przewiduje przeniesienie w ciągu trzech lat co najmniej 50% biznesu do chmury. Uwzględniając punkt startowy z 2021 r., w którym tylko 12% zasobów w Ameryce Północnej i 5% zasobów w Europie było przetwarzanych w chmurze, powinniśmy mieć obecnie wysyp projektów związanych z wykorzystywaniem chmury. Żeby odpowiedzieć na pytanie o stan obecny, możemy zajrzeć do strategii IT banków w Polsce. Każdy z naszych rodzimych banków wymienia chmurę jako jeden z czynników różnicujących tempo rozwoju technologii.

Za możliwościami wykorzystywania chmury przemawiają też rosnące doświadczenia rynku związane z zapewnieniem zgodności z wymaganiami prawa bankowego oraz coraz bardziej precyzyjne przepisy pochodzące m.in. z europejskiej regulacji DORA (Digital Operational Resilience Act) i obowiązującego komunikatu chmurowego UKNF. Dlaczego więc cloud ma być selektywny? Odpowiedzią jest strona finansowa projektów dotyczących chmury. Wszystkie duże banki mają swoje data center, w których moc obliczeniowa kosztuje mniej. Jako ryzyko postrzegane są elementy wysokiego poziomu skomplikowania modeli cenników w chmurze i ich wielopoziomowa zależność (np. nie tylko od ilości wykorzystywanej mocy obliczeniowej, lecz również klasy rozwiązania, wielkości →

transferów danych itp.). Ponadto działy prawne i zespoły odpowiedzialne za efektywność zakupów zwracają uwagę na możliwości modyfikacji cennika przez operatora chmury i wysokie koszty przenoszenia rozwiązań do innego operatora – o ile nie jest to proces zaprojektowany od początku (tzw. multicloud). Poza sytuacjami kryzysowymi, jak np. konieczność zabezpieczenia danych na terenach Ukrainy, projekty chmurowe są realizowane w oparciu o szczegółowo zbadany business case i zabezpieczają obszary technologii, w których wymagana jest duża ilość lub specyficzny rodzaj mocy obliczeniowej. Takimi projektami jest m.in. analityka i związany z tym trend hiperpersonalizacji danych, gdzie punktowo potrzeba dużej ilości mocy obliczeniowej (np. ponad 1000 corów na okres do 1 tygodnia w miesiącu). Duże znaczenie odgrywa również AI (artificial intelligence) i rosnąca rola botów typu GPT (Generative Pre-trained Transformer), które najlepiej skalują się, bazując na mało popularnych w bankowych data center procesorach graficznych.

Zarządy banków mają dużą świadomość roli technologii i chmury, która poprzez swoją elastyczność wspiera osiąganie przewagi rynkowej. Selektywne podejście do chmury oznacza dużo szersze spojrzenie niż tylko migracja mocy obliczeniowej i stawia większe wymagania przed dostawcami i integratorami chmury, którzy obok technologii muszą oferować kontekst biznesowy swoich rozwiązań.

1 Badanie Accenture: https://bankingblog.accenture.com/banking-cloud-altimeter-magazine/volume-1-what-does-banking-cloud-mean

Maciej Appelt
DYREKTOR DEPARTAMENTU ZARZĄDZANIA DANYMI, SGB-BANK SA:

Tworząc zrzeszeniową hurtownię danych w Spółdzielczej Grupie Bankowej, chcieliśmy osiągnąć cele, które SGB-Bank określił w swojej strategii na najbliższe lata, czyli m.in. zwiększyć naszą cyfrową moc oraz efektywność. Z drugiej strony, celem było połączenie wszystkich danych banków należących do zrzeszenia SGB oraz budowa w naszej organizacji świadomości nowego wymiaru gromadzenia, bezpieczeństwa i użyteczności tych danych.

Dodatkowo ujednolicamy sprawozdawczość, zarówno regulacyjną, jak i zarządczą, zwiększamy bezpieczeństwo infrastruktury oraz przechowywanych danych poprzez wykorzystanie rozwiązań centralnych projektowanych dla wszystkich banków zrzeszenia. Finalnie będzie to służyło redukcji kosztów zarówno sprzętu, jak i pozyskiwania informacji.

Aby osiągnąć te cele, musieliśmy wykonać szereg prac o charakterze nietechnicznym, których wymaga od instytucji finansowej państwowy regulator. Mowa oczywiście o szerokim obszarze compliance. W ubiegłym roku SGB-Bank przeszedł przez procedurę zgodności komunikatu chmurowego KNF. Dzięki temu doświadczeniu, przygotowaliśmy koncepcję chmury społecznościowej, czyli hybrydowej formy chmury prywatnej, która jest budowana i zarządzana pod konkretną grupę docelową, a w naszym przypadku tą grupą są banki spółdzielcze SGB.

Przygotowaliśmy standard chmury społecznościowej w zrzeszeniu, który jest zbiorem reguł, procedur oraz dokumentacji, stanowiących realne wsparcie podczas przechodzenia procesu komunikatu chmurowego przez pojedynczy bank spółdzielczy.

Sam proces dotyczący wytycznych KNF to nie tylko zakres prawny i zarządzania zgodnością. To także szereg kwestii technicznych i koncepcyjnych, które musiały być spełnione, aby rozpocząć budowę zrzeszeniowej hurtowni danych.

Zaprojektowaliśmy zatem całą architekturę i przeprowadziliśmy bardzo wiele testów, które utwierdziły nas w przekonaniu, że droga transformacji z rozwiązań *on premises* na rozwiązania chmurowe jest słusznym wyborem. Ostatecznie więc na początku roku uruchomiliśmy produkcyjne zasilenia z kluczowych systemów źródłowych w banku, a całość rozwiązania oparliśmy na dedykowanych komponentach Google Cloud Platform. Zrobiliśmy to jako jeden z pierwszych banków w Polsce.

Jak wygląda obecnie stan rozwiązań chmurowych, jak planujemy rozwój? Mamy gotową HD w zakresie zasilania oraz przechowywania danych ze wszystkich systemów źródłowych w banku. Zbudowaliśmy mechanizmy, pozwalające dowolnie rozszerzać tę architekturę oraz podłączać kolejny bank z zachowaniem separacji danych. Pracujemy obecnie nad warstwą biznesową, w tym nad ujednoliconym słownikiem pojęć biznesowych oraz wspólnym dla całego zrzeszenia modelem biznesowym. Finalnie chcemy być organizacją data driven i wierzymy, że budowany produkt w ekosystemie Google przybliży nas do tego celu.

Jakie efekty dają bankom spółdzielczym SGB rozwiązania chmurowe? Wdrożenie nowoczesnej hurtowni danych w środowisku chmurowym umożliwia przede wszystkim centralizację danych z różnych systemów bankowych, poprawia efektywność, bezpieczeństwo oraz integralność architektury IT, usprawnia raportowanie i analizowanie danych, a także pozwala na konsolidację informacji o kliencie.

Korzystanie z rozwiązań chmurowych oznacza nie tylko wymierne efekty finansowe, ale także szansę na olbrzymi skok technologiczny i praktyczne wykorzystanie wszystkich możliwości nowych technologii informatycznych w obszarze bezpieczeństwa, sprawności i szybkości działania banków spółdzielczych. •

QRadar Suite, czyli kompleksowe wsparcie dla banków w zapewnieniu bezpieczeństwa

Rozmowa z ŁUKASZEM KUFLEWSKIM, Identity Manager Architect w Cloudware Polska.

Fot. ipopba/stock.adobe.com

Jak upowszechnienie rozwiązań bazujących na AI i uczeniu maszynowym zmieniło mapę zagrożeń dla instytucji finansowych oraz ich klientów? Chodzi zarówno o same strategie przestępcze, jak też skuteczność dotychczas używanych środków bezpieczeństwa.

– Wyścig zbrojeń pomiędzy światem przestępczym a twórcami zabezpieczeń dla sektora bankowego trwa od zawsze. W czasach, gdy to kasiarze stanowili główne zagrożenie dla instytucji finansowych, odpowiedzią ze strony tych ostatnich były coraz bardziej przemyślane sejfy, skarbce i systemy alarmowe. Wraz z digitalizacją gospodarki rywalizacja pomiędzy złodziejami a bankowcami przenosiła się do cyberprzestrzeni. Tu sporą przewagę zyskała jasna strona mocy, przeznaczając kolosalne nakłady finansowe na tworzenie skutecznych systemów bezpieczeństwa cyfrowego, czy też wdrażając odpowiednie polityki antyfraudowe i w zakresie AML/KYC. W ślad za przemianami natury technologicznej i organizacyjnej postępowała edukacja pracowników instytucji finansowych odnośnie ewentualnych zagrożeń, co przyczyniło się do budowy ich świadomości w tym zakresie.

Najsłabszym ogniwem w całym łańcuchu pozostał konsument, przeciętny Kowalski korzystający z usług finansowych, który – pomimo licznych kampanii uświadamiających zagrożenie cyberprzestępczością – w dalszym ciągu jest najbardziej podatny na coraz bardziej wyrafinowane kampanie socjotechniczne, wspomagane najnowszymi rozwiązaniami IT. Niekiedy wystarczy jedno kliknięcie czy otwarcie trefnego załącznika, by utracić całe oszczędności życia, zwłaszcza jeśli po drugiej stronie mamy oszustów posługujących się deepfake czy innymi narzędziami bazującymi na uczeniu maszynowym, których skuteczność przewyższa doświadczonego hakera. Rosnąca liczba zaawansowanych prób oszukańczych z użyciem botów sprawia, że instytucje finansowe przejmują na siebie część odpowiedzialności za zabezpieczenie zdalnych kanałów komunikacji z bankiem, z których korzystają ich klienci. →

Działania te stymulowane są zarówno wewnętrznym poczuciem odpowiedzialności społecznej kadry zarządzającej banków, jak i presją ze strony regulatorów, zarówno na szczeblu krajowym, jak i europejskim.

– Przykładem mogą być bardzo prokonsumenckie zapisy polskiej ustawy o usługach płatniczych, przewidujące rozpatrywanie reklamacji na nieautoryzowaną transakcję, zapisy o podobnej treści znalazły się w projekcie unijnego rozporządzenia PSR, które miałoby zastąpić obecnie obowiązującą dyrektywę PSD2. Budzą one kontrowersje, niemniej kierunek, w jakim zmierza europejski regulator, jest poniekąd zrozumiały, gdyż nie sposób wymóc na wszystkich bez wyjątku klientach instytucji bankowych, by posługiwali się bardziej zaawansowanymi rozwiązaniami antyfraudowymi, kiedy korzystają ze zdalnego dostępu do banku dosłownie na co dzień, płacąc smartfonem w restauracji czy sklepie, a także w kanałach e-commerce. Tymczasem banki są w stanie wdrożyć odpowiednie narzędzia, maksymalnie ograniczające ryzyko podszywania się osoby niepowołanej pod użytkownika rachunku bankowego, a w sukurs przychodzi im sztuczna inteligencja.

Algorytmy z obszaru analizy zachowań użytkownika (user behaviour analytics) są w stanie bardzo szybko i z olbrzymim prawdopodobieństwem zweryfikować, czy po drugiej stronie mamy do czynienia z tą samą osobą, co zwykle, a także, czy i na ile jej zachowanie w danej chwili odbiega od dotychczasowych doświadczeń. Do tego dochodzą elementy kontekstu samego uwierzytelniania, w tym weryfikacja, z jakiego urządzenia i z jakiego regionu następuje połączenie. Dzięki temu można wykryć przypadki, kiedy niewzbudzająca podejrzeń transakcja wykonywana jest o godzinie 14.00 z Warszawy, a za 15 minut z tego samego konta i przy użyciu tych samych poświadczeń przeprowadzana jest operacja z odległego miejsca. Możliwości narzędzia user behaviour analytics nie ograniczają się do weryfikacji interakcji klientów z urządzeniem, ale są również w stanie wychwycić anomalie wewnątrz infrastruktury danej instytucji. Chodzi o sytuacje, kiedy logowanie administratora czy innego pracownika następuje w nietypowym czasie, albo próbuje on uzyskać dostęp do zasobów, z których nigdy dotąd nie korzystał. Każdy taki przypadek, zgłoszony przez system, należy oczywiście zweryfikować i odpowiednio zareagować.

Skoro już mówimy o kompleksowej zmianie podejścia do kwestii cyberbezpieczeństwa, w którym obszarze sektor finansowy wymaga największych zmian, by skutecznie stawiać czoło zagrożeniom XXI wieku: technologicznym, organizacyjnym czy regulacyjnym?

– Zacznę od końca. Regulatorzy wymagają coraz większej odpowiedzialności, przerzucając ją na poszczególne sektory poprzez wymuszanie określonych działań w celu minimalizacji ryzyka, co – jak już wcześniej wspomniałem – wynika poniekąd z rosnącej świadomości zagrożeń. W tej sferze nie upatrywałbym jakichś szczególnych wyzwań. Pod względem organizacyjnym bankowość ma szczególnie rozwiniętą świadomość adresowania problemów, związanych z szeroko pojętym bezpieczeństwem, jest to niejako wpisane w DNA instytucji finansowych już od początków transformacji cyfrowej. Najwięcej uwagi wymagać będzie zatem odświeżenie czy też raczej aktualizacja wykorzystywanych technologii, które są w stanie wspomóc sektor i jego klientów w obszarze bezpieczeństwa.

Systemy, jakich używają w tym celu banki, nie zawsze należą do najświeższych, bywa i tak, że przedstawiciele instytucji oceniają dotychczasowe rozwiązania, nierzadko skrojone pod ich indywidualne potrzeby, jako wystarczające, tymczasem świat cyberataków cały czas się rozwija. Jesteśmy świadkami nie tylko powstawania nowych schematów przestępczych działań, ale i ewolucji dotychczasowych, w dalszym ciągu najczęstszym atakiem wymierzonym w dane jest ransomware, zaś najpowszechniejsza taktyka przestępcza służąca wykradaniu poświadczeń to phishing. Te zagrożenia nie pojawiły się miesiąc czy pół roku temu, są znane od dawna, tylko stają się coraz bardziej wyrafinowane. Aby im przeciwdziałać, potrzeba narzędzi, które będą w stanie nie tylko reagować na znane zagrożenia, ale korzystając z analityki pewnych czynności, wskażą, że coś niepokojącego się dzieje bądź za chwilę może się wydarzyć.

Podstawą sukcesu każdego rozwiązania, wykorzystującego uczenie maszynowe, jest dostęp do danych. Jak skutecznie zarządzać wewnętrznymi zbiorami danych banku i agregować je z informacjami pozyskiwanymi z zewnątrz, by w oparciu o te zasoby stworzyć skuteczną zaporę antyfraudową?

– Wszystko zależy od tego, jak w tym kontekście rozumiemy fraud. Jeśli chodzi o dane, to kluczowe znaczenie ma ich zabezpieczenie. Banki, podobnie jak inne instytucje finansowe, przechowują mnóstwo informacji o swoich klientach, i są to wszystko dane chronione, zatem w pierwszej kolejności należy zapobiegać ich wyciekom. W tym celu zaś nie wystarczy wdrożenie odpowiednich polityk bezpieczeństwa ani zakup zaawansowanego pakietu cybersecurity. Niezbędna jest świadomość, gdzie i jakie dane posiadamy, bo przy obecnym natłoku informacji nietrudno doprowadzić do sytuacji, w której dana instytucja traci panowanie nad tym, co i gdzie gromadzi, a w konsekwencji również, które zbiory należy chronić w szczególny sposób. To pierwszy krok do powstania luki w systemie bezpieczeństwa i potencjalnego ryzyka dostania się do tych danych czy przechwycenia ich przez osoby niepowołane.

Fot. tippapatt/stock.adobe.com

Jednym z głównych kierunków digitalizacji banków jest migracja do środowisk chmurowych. Jak powinny wyglądać poszczególne etapy wdrażania cloudu z punktu widzenia bezpieczeństwa, by osiągnąć optymalny efekt? Pamiętajmy, że przenoszenie zasobów do chmury jest niczym przebudowa samolotu w trakcie lotu, gdyż instytucja finansowa jako element infrastruktury krytycznej musi utrzymywać ciągłość działania.

– Transformacja chmurowa w ostatnim czasie się nasiliła, a rozwiązania chmurowe są coraz popularniejsze także z uwagi na bezpieczeństwo przechowywania danych. Mamy zapewnione backupowanie, dostępność i skalowalność, a to wszystko przy wydatnie niższych nakładach finansowych niż w przypadku klasycznej architektury. Należy jednak pamiętać, że cloud cloudowi nierówny. Mamy rozwiązania bazujące na chmurze prywatnej, wdrażane przez organizację wyłącznie na potrzeby własne i funkcjonujące we własnym środowisku, ale również chmury hybrydowe czy publiczne. W przypadku tych ostatnich należy po pierwsze odpowiednio zabezpieczyć serwery, one powinny być aktualne i posiadać wdrożone odpowiednie polityki, jak najbardziej ograniczające dostęp, bo pamiętajmy, że całe zasoby mogą być wówczas dostępne z internetu.

Odrębnym wyzwaniem jest to, że w powszechnie dostępnych chmurach swoje rozwiązania i swoje usługi mają różne organizacje, zatem zasoby banku trzeba odpowiednio odseparować i zabezpieczyć sieci. Z tych wymogów raczej wszyscy zdają sobie sprawę, niemniej trzeba jeszcze pamiętać o odpowiednim monitoringu bezpieczeństwa tych wszystkich rozwiązań. Zarówno chmury publiczne, jak i nawet prywatne, udostępniają pewne zasoby logów, które wypadałoby odpowiednio gromadzić i przetwarzać, a przede wszystkim skorelować z tym, co się dzieje w wewnętrznym środowisku, czy też na styku pomiędzy on premise a rozwiązaniem chmurowym. Przede wszystkim trzeba dbać o bezpieczeństwo danych, czemu służą odpowiednie narzędzia, które szyfrują dane, kontrolują dostęp, monitorują wykorzystanie zasobów danych, żeby wychwycić podejrzany ruch i odpowiednio zareagować. Do tego dochodzą elementy związane z rozwiązaniami opartymi →

na sztucznej inteligencji, które się tego wszystkiego uczą, analizują i sygnalizują, jeśli coś odbiega od normy.

Na czym polega zatem specyfika narzędzi takich, jak IBM Security QRadar i IBM Cloud Pak for Security, w kontekście podnoszenia poziomu ochrony instytucji finansowych, a w szczególności jak radzą sobie one z nowymi, nieznanymi dotychczas schematami przestępczych działań?

– Mamy do dyspozycji cały pakiet QRadar Suite, stanowi on zestaw rozwiązań, wspierających instytucję finansową w zapewnieniu odpowiedniego poziomu bezpieczeństwa. Należy zacząć od QRadar SIEM, narzędzia odpowiedzialnego za zbieranie informacji o całej aktywności w środowisku, zarówno jeśli chodzi o ruch sieciowy, logi bezpośrednio z systemów, aplikacji bazodanowych, czy wreszcie feedback z każdego urządzenia, przełącznika sieciowego czy firewalla. Rozwiązania tej klasy służą po to, by w infrastrukturze zbierać dane z mnóstwa końcówek, ale również korelować je, budować informacje o tym, co po kolei się działo, co z czego wynika, by w konsekwencji uzyskać pełny obraz danej sytuacji. Te skorelowane już informacje pozwalają wyodrębnić potencjalne incydenty, w przypadku tego rozwiązania określane jako offence.

Oczywiście należy pamiętać, iż nie każda informacja zgłoszona przez system musi być od razu zagrożeniem. Wdrażając takie rozwiązanie, określamy sytuacje typowe i standardowe, które normalnie występują w codziennej pracy całego środowiska, a odstępstwa od tej normy są klasyfikowane jako potencjalny incydent bezpieczeństwa, którym trzeba by się zająć, choć niekonieczne zareagować. To jest istota pracy z narzędziem, nie wystarczy je wdrożyć i mieć święty spokój. Zagrożeń przybywa, a więc trzeba pracować nad tego typu rozwiązaniem, konfigurować i aktualizować pod kątem tego, co się dzieje u nas w środowisku.

Bardzo mocno powiązane z QRadar SIEM jest rozwiązanie QRadar SOAR (Security Automation, Orchestration and Response), które bazuje na informacjach pochodzących ze SIEM-a, a jego zadaniem jest przesyłanie wskazanych przez SIEM, potencjalnie ryzykownych sytuacji do odpowiednich grup wsparcia. Nie chodzi jednak wyłącznie o samo zaprezentowanie incydentu i zapewnienie jego obsługi, ale również automatyczne zadziałanie poprzez tak zwane playbooki, czyli skrypty, które reagują odpowiednio na określoną sytuację potencjalnego zagrożenia. Zadaniem takiego playbooku jest np. sprawdzenie, w oparciu o feedback otrzymany od SIEM, czy trwa jakiś proces, który wskazuje bezpośrednio na atak, czy można w danej sytuacji zablokować dostęp, a jeśli już doszło np. do zaszyfrowania zasobu danych, to odtworzyć je z ostatniego możliwego backupu, żeby zminimalizować postój całego środowiska.

W ramach narzędzia występują też moduły oparte na sztucznej inteligencji, które wspierają operatora, automatycznie wzbogacając informacje o zagrożeniu. Można np. sprawdzić, czy domena, z której jest wykonywany ruch, nie została zarejestrowana wczoraj, co już stanowi istotny sygnał ostrzegawczy. Ale możliwe jest również skanowanie wiadomości mailowych, które przychodzą do pracowników banku, pod kątem załączników zawierających malware, czy URL-i, przekierowujących na domeny nieznane bądź z innych względów oznaczone jako niebezpieczne. Takie rozwiązanie jest w stanie poprowadzić osobę, która obsługuje dany incydent krok po kroku, żeby wykonała wszystkie niezbędne czynności, od potwierdzenia, że faktycznie trzeba w jakiś sposób zareagować, chociażby poprzez zgłoszenie naruszenia bezpieczeństwa, jeśli przepisy tego wymagają. To może nas wspomóc w wykonaniu wszystkich kroków, niezbędnych w ramach pełnej obsługi incydentu. Działania te mogą być realizowane po części automatycznie, a po części przez operatora.

Dysponujemy jeszcze jednym elementem wspomagającym całe nasze środowisko, QRadar NDR (Network Detection and Response). To moduł odpowiadający za szczegółową analizę ruchu sieciowego, włącznie z analizą pakietów, które krążą w sieci w danym środowisku IT. Mamy rozwiązanie QRadar EDR (Endpoint Detection and Response) przeznaczone do zabezpieczeń końcówek, czyli poszczególnych urządzeń, które jest w stanie upewnić się, że nie trwa żaden niepożądany proces, nikt nie próbuje zmanipulować danych, zaszyfrować ich czy bezpośrednio zaatakować danej końcówki.

Jeśli chodzi o Cloud Pak for Security, jest to rozwiązanie uzupełniające, dedykowane wspomnianym wcześniej środowiskom chmurowym. Zawiera ono elementy SIEM, jak i SOAR, i jest przeznaczone po to, by z jednej strony korelować wszystkie informacje, które jesteśmy w stanie zebrać z cloudu i połączyć je ze zdarzeniami, które mamy w SIEM-ie obsługującym infrastrukturę lokalną – po to, żeby mieć pełny pogląd na to, co się dzieje już na naszym całym środowisku, żeby jedno środowisko nie było oderwane od drugiego. Pamiętajmy, że zasoby chmurowe nierzadko współpracują z naszym środowiskiem lokalnym, i dlatego Cloud Pak for Security spaja te dwa oddzielne środowiska. IBM udostępnia swoje usługi związane z bezpieczeństwem, polegające na dostępie do wiedzy i bazy wszystkich aktualnych zagrożeń. Baza zabezpieczeń jest na bieżąco uaktualniana, żeby być cały czas na bieżąco ze wszystkimi zagrożeniami, zatem bank czy inna instytucja, korzystając z tych narzędzi, nie jest osamotniona w walce z szeroko rozumianymi cyberatakami. •

Czy Industry Cloud zastąpi uniwersalne rozwiązania „klasycznej” chmury publicznej?

Według najnowszego badania PwC „Chmura w biznesie, liderzy widzą wartość”[1] aż 30% instytucji finansowych wykorzystuje chmurę do modernizacji, a tylko jedna na cztery stosuje holistyczne i wieloaspektowe podejście, które pozwala usprawnić im swoją działalność. To w tych 25% możemy dostrzec potencjał tego, czego rynek finansowy oczekuje od chmury – wysokiej efektywności oraz nowych funkcji biznesowych i wszystkiego, co mieści się w definicji nowej wartości czy holistycznych transformacji obszaru biznesu. Rynek chce definiować chmurę jako nośnik cyfrowej transformacji XXI wieku – katalizator innowacji i prędkości, coś, co buduje wartość.

Fot. Ar_TH/stock.adobe.com

Fot. PwC

Przemysław Galiński
CLOUD & DIGITAL DIRECTOR,
PWC POLSKA

Oczekiwania sektora finansowego w kontekście wartości generowanej technologią wskazują jednoznacznie na rozwiązania, które nie będą generyczne czy uniwersalne. Oczekuje się wysoko wyspecjalizowanych rozwiązań dedykowanych dla określonego sektora. Jest to scenariusz, gdzie zwycięża pragmatyzm biznesowy i adekwatność rozwiązań.

Dostosowanie do potrzeb

Na pytanie, jakiej chmury potrzebujemy, obecnie wielu odpowie „dostosowanej do unikalnych potrzeb i wymagań stawianych naszej organizacji przez klientów czy też całe otoczenie rynkowe”. Uzupełnieniem tej odpowiedzi w obszarze rozwiązań technologicznych może być Industry Cloud i rozwiązania dedykowane dla sektorów i branż. Gartner w swoim najnowszym raporcie „Top Strategic Technology Trends 2024”[1] wskazuje właśnie Industry Cloud jako jeden z dziesięciu istotnych oraz obiecujących trendów i zjawisk wpływających na wszystkie organizacje i cały rynek. Gartner pozycjonuje zresztą chmurę branżową – zarówno w zbiorze szeroko →

1 https://emt.gartnerweb.com/ngw/globalassets/en/publications/documents/2024-gartner-top-strategic-technology-trends-ebook.pdf?_gl=1*dgw8tr*_ga*OTcyOTkwOTc2LjE2OTQ2Nzg4NjU.*_ga_R1W5CE5FEV*MTcwMTI1OTc0MC4xNy4wLjE3MDEyNTk3NDMuNTcuMC4w

Fot. idambeer/stock.adobe.com

pojętego zabezpieczenia, czy zagwarantowania zwrotu z już poniesionych inwestycji, ale także w kontekście komponentów, gotowych prefabrykatów służących do budowy biznesu przyszłości.

Pojęcie Industry Cloud czy Chmury Branżowej pojawia się w obszarze rozmów o transformacji chmurowej już od dawna. Zwrot ten przenika niejako pojęcie chmury hybrydowej czy też prywatnej, które na infrastrukturze „chmurowej" są oferowane dla danego sektora. Bardzo częsty przykład rozwiązań Industry Cloud to rozwiązania dla sektora finansowego. Pojęcie Chmury Branżowej jest niezwykle pojemne i dotyczy nie tylko wskazanego portfolio wyselekcjonowanych usług dostępnych tylko i wyłącznie np. w modelu PaaS, ale dość szerokiej gamy rozwiązań, które mają dwie wspólne płaszczyzny. Jedną z tych płaszczyzn jest dowolna forma uchmurowienia (as a service), może to być właśnie PaaS (Platform as a Service) jako wyselekcjonowane mikroserwisy, ale także infrastruktura IaaS (Infrastructure as a Service), czy też dedykowane oprogramowanie SaaS (Software as a Service). Drugą płaszczyzną jest obszar kierunkowej funkcjonalności, użyteczności czy adekwatności specyficznej dla danej branży, np. finansowej. Funkcjonalność tą rozumiemy czy przez funkcje biznesowe, czy całe obszary biznesowe (np. dla bankowości może to być obszar biznesu korporacyjnego, detalu, treasury albo elementów dotyczących funkcji systemów corowych banków). Wszystko to, co ma w szeroko pojętym biznesie określone zadanie, może być w modelu „as a service" wsparte albo wręcz zamienione funkcjonalnością dostępną jako gotowe rozwiązanie (np. business process as a service) w chmurze.

Nie specjalizującym się w archeologii technologii, ciężko odnaleźć pierwsze rozwiązania wpisane w tę szeroką definicję i znaleźć moment, w którym Industry Cloud zaczęło być tak nazywane. Na pewno jednym z prekursorów podejścia była firma IBM ze swoją chmurą IBM Cloud, która została zmodyfikowana w kierunku spełnienia zgodności regulacyjnej dla sektora finansowego. To wszystko zostało przedstawione rynkowi i oferowane jako IBM Cloud for Financial Services[2]. I tu pierwsze rozwiązania tworzone właśnie w oparciu o chmurę tego dostawcy zostały opracowane i dostarczane w ten sposób, aby działały zgodne z wymaganiami regulacyjnymi instytucji finansowych, co ciekawe zarówno dla rynku Stanów Zjednoczonych, jak i Europy.

Kluczowe w tym modelu było także to, że dostawca nie wymyślał i nie tworzył rozwiązań na nowo. Zapewniał platformę, na której inni dostawcy technologii, np. ISV (Independent Software Vendor), mogli oferować swoje rozwiązania dla sektora bankowego w pełnej zgodności, zapewnianej przez chmurę tego dostawcy.

2 https://www.ibm.com/cloud/financial-services

Od modułu po pełne rozwiązanie

Wykorzystując analogię klocków, budowano modele z wystandaryzowanych, bezpiecznych (zgodnych z regulacjami) elementów, które dostarczała chmura za to funkcjonalności były i są zapewniane przez dostawcę rozwiązania docelowego. Model ten jest nad wyraz prosty w projektowaniu, a przy tym optymalny, jest też stosowany przez innych dostawców chmury. Jest on również przykładem budowania rozwiązań dla konkretnych sektorów na technologii, która „by design" jest zgodna z wymaganiami regulatora albo charakterystycznych dla danego sektora. Jest on dość uniwersalny i popularny u niemal wszystkich hyperscalerów. Ten model tworzenia Industry Cloud wskazuje zresztą Gartner we wspomnianym wcześniej raporcie, gdzie obszar Marketplace stanowi immanentny element szerokiej definicji i kierunek rozwoju chmury branżowej. Nie jedyny, ale istotny. Stanowi też najczęściej pierwszy poziom adopcji takiej chmury w organizacjach.

Analizując rynek chmury, bez wyjątku wszyscy hiperskalerzy starają się oferować rozwiązania w oparciu o model Industry Cloud. Wyjątku nie stanowi tu również Microsoft[3], który w swoim portfolio klasyfikuje co najmniej kilka klastrów podejścia Industry Cloud, adresując sektory takie, jak Retail, Healthcare, Manufacturing czy Financial Services – nie jest to zresztą unikalne wyłącznie u tego dostawcy. Co naturalne, mamy tutaj podobny podział rozwiązań, od infrastruktury (certyfikowane pod wymagania branży, np. dla sektora branży zdrowotnej HIPAA, HHS czy dla sektora finansowego PCI DSS), czy serwisy platformy PaaS aż po dedykowane, pełne i skończone rozwiązania adresujące funkcje „end to end". Zwłaszcza tu np. dla rozwiązań Cloud for Healthcare dostępne są gotowe moduły czy pełne rozwiązania dla szpitali i klinik adresujące właściwie całą ścieżkę interakcji z pacjentem. Wszystko w oparciu o chmurę, która w tym przypadku jest zgodna z wymaganiami dotyczącymi przetwarzania i ochrony danych medycznych. Jesteśmy tu o krok od modelu znanego w bankowości i określanego jako „bank in the box", będącego zresztą rozwinięciem idei Industry Cloud. Nie oceniając sukcesu komercyjnego takich rozwiązań, warto odnotować taki trend. Podobny kierunek do Microsoft przybiera również Amazon Web Services oferujący predefiniowane pod sektor bankowy rozwiązania w obszarze choćby AML czy inne rozwiązania zasilane przez AI oferowane przez AWS. Rozwiązania Google Cloud nie pozostają tu w tyle, oferując bardzo zbliżone portfolio usług i rozwiązań dedykowane dla sektora finansowego, choćby tych spełniających wysokie i specyficzne dla bankowości wymagania bezpieczeństwa.

Remedium na wiele wyzwań

Wyjątkowym i namacalnym przykładem rozwiązań Industry Cloud, które już działają i spotykają się z ogromnym zainteresowaniem oraz pozytywnym odbiorem, jest szeroka agenda technologiczna dla obszaru zrównoważonego rozwoju Cloud for Sustainability – gdzie niezależnie od branży adresowane są specyficzne wymagania , zwłaszcza regulacyjne i raportowe. Zresztą ten obszar w ramach działań Industry Cloud jest bardzo intensywnie eksploatowany w instytucjach finansowych. Banki szukają takich rozwiązań, które będą adekwatne nie tylko dla tego wszystkiego, co stoi za akronimem ESG, ale będą adekwatne dla sektora. I to tu sektor bankowy dopatruje się remedium na wiele wyzwań wynikających z nowych regulacji oraz intensywności ich zmian. Warto wspomnieć, że także i tu sama agenda regulacji, ogromu pozyskiwanych oraz analizowanych danych, ich charakterystyk, audytowalności czy spójności jest dużym wyzwaniem. Jeśli chodzi o wspomniane wcześniej gotowe rozwiązania technologiczne, są one tylko wycinkiem determinowanej przez regulacje (np. CSRD) transformacji czy rozszerzonego raportowania niefinansowego. Właśnie w takim modelu rozszerzonym holistycznym podejściem, programy realizowane przy wykorzystaniu rozwiązań wpisujących się w Industry Cloud są w stanie zaadresować wymagania stawiane instytucjom finansowym szybciej, lepiej i efektywniej. Przykładem rozszerzonego Industry Cloud dla ESG jest metodyka PwC. Rozwiązanie ESG Hub, w którym centralnym miejscem jest wspomniane wcześniej narzędzie Cloud for Sustainability, natomiast otoczone jest integracją z zewnętrznymi i wewnętrznymi systemami, zasilającymi pośrednio strukturę danych, ale przede wszystkim adresującymi określony dla branży finansowej kluczowy model danych – powstały w oparciu o unikalną branżową wiedzę. Całe rozwiązanie oparte na chmurze, przynosi określoną wysoką wartość. Wszystko to w modelu specyficznym dla instytucji finansowych.

Industry Cloud to również dedykowane rozwiązanie inne niż infrastruktura, przykłady rozwiązań można mnożyć, np. Microsoft 365 czy platforma Dynamics 365 dla tego przykładu dostarczane w reżimie regulacji dla sektora finansowego. I to m.in. w tych rozwiązaniach „silnik branżowy" odpowiada za procesy wsparcia, szyfrowanie czy szeroko pojętą odpowiedzialność dostawcy.

Rozwiązań jest wiele

Wariantów, scenariuszy czy modeli jest znacznie więcej. Kolejnym przykładem branży, która chce adoptować takie rozwiązania jest branża ubezpieczeniowa, która działa w oparciu →

3 https://www.microsoft.com/en-us/industry

Fot. Thitichaya/stock.adobe.com

o inny model niż sektor bankowy. To w niej można odnaleźć charakterystyki specyficznych modeli ryzyk czy separacji określonych części biznesu (np. majątek i życie) czy też działania na styku organizacja–agenci, którzy pełnią kluczową kluczową rolę w modelu dotarcia do klienta końcowego. Tu znów z pomocą przychodzą rozwiązania firm trzecich, które dostarczają swoje funkcjonalności w oparciu o platformę chmury branżowej. W tym przykładzie dedykowaną dla regulacji ubezpieczeniowych. Tworząc jako całość homogeniczny wariant Industry Cloud dla sektora ubezpieczeń.

Jeszcze innym poziomem Industry Cloud są również dedykowane, wysoce specjalizowane czy wręcz unikalne na rynku, niszowe rozwiązania oferowane przez dostawców chmury, a dotyczące modelu, w którym chmura jest dostarczana „w całości". Oracle Dedicated Cloud ze swoimi charakterystycznymi usługami w obszarze „Dedicated Region" czy „Isolated Region" idealnie nadają się do scenariusza, w którym chmura uruchamiana jest w wymiarze prywatności i zabezpieczeń wcześniej niedostępnych dla chmury publicznej, łącznie z galwaniczną separacją zasobów. Powyższe może stanowić kolejny wymiar Industry Cloud dla sektorów krytycznych dla bezpieczeństwa.

Wariantów oraz modeli, które możemy odnaleźć w koncepcji Industry Cloud jest wiele, wszystkie powinny cechować się możliwie niezachwianą elastycznością, charakteryzującą niezmiennie chmurę publiczną, potencjalnie niską barierą wejścia, ale przede wszystkim być skrojone pod potrzeby specyficzne dla branży lub obszaru. Błędem jest zamykanie definicji Industry Cloud tylko wokół regulacji i bezpieczeństwa, choć to z tego kierunku się ona wywodzi i tam się zaczynała.

Chmura branżowa może mieć zupełnie innych adresatów, ambasadorów technologii w organizacjach – podczas gdy „klasyczna" chmura to wciąż w dominującej części adresaci obszaru IT. Industry Cloud to często adresaci biznesowi albo przynajmniej udział w kreowaniu potrzeb stawianych technologii jest w dużej mierze oparty na biznesie i to właśnie biznes może być największym zwolennikiem chmury, zwłaszcza branżowej.

Czy Industry Cloud zastąpi uniwersalne rozwiązania „klasycznej" chmury publicznej? Na pewno nie, stanowić będzie jej uzupełnienie, wydaje się jednak, że na stałe zagości w cyfrowej agendzie sektora bankowego i nie tylko tego sektora. •

FinOps: strategiczne podejście do zarządzania kosztami chmury nowoczesnej bankowości

W dobie szybko rozwijających się technologii cyfrowych sektor usług finansowych (FSI) stoi przed nowymi wyzwaniami. Innowacyjne firmy fintech odpowiadają na rosnące oczekiwania klientów dobrze orientujących się w technologii, zmuszając tradycyjne instytucje finansowe do rywalizacji na coraz bardziej konkurencyjnym rynku.

Fot. PwC

Ernest Orłowski
SENIOR MANAGER
PWC POLSKA

Fot. PwC

Agnieszka Bochacka
MANAGER
PWC POLSKA

Złożone warunki geopolityczne i ekonomiczne wymuszają na liderach branży FSI ostrożne podejście do wdrażania nowych rozwiązań, skłaniając ich do unikania ryzykownych eksperymentów. Pomimo tego, to właśnie chmura pozostaje kluczowym elementem innowacyjnym branży – 46% instytucji finansowych, które obecnie nie konsumują usług chmurowych, planuje rozpocząć drogę do chmury w ciągu najbliższych dwóch lat[1]. Obserwujemy również rosnące zainteresowanie rozwiązaniami hybrydowymi, które pozwalają na dostarczanie nowych i jeszcze bardziej kompleksowych doświadczeń dla klientów banków.

W obliczu tych wyzwań, FinOps, czyli procesy, narzędzia i wiedza dają pewność kadrze zarządzającej, że każda „złotówka" wydana na usługi chmurowe została wydana efektywnie i na właściwe usługi.

Co to jest FinOps?

FinOps, będąc połączeniem słów „*Finance*" (Finanse) i „*Operations*" (Operacje), reprezentuje dynamicznie rozwijającą się dziedzinę zarządzania finansami chmury. Jest to wynik rosnącej potrzeby organizacji odnośnie lepszego zarządzania kosztami i efektywnością usług chmurowych, które stały się kluczowym elementem w wielu branżach, zwłaszcza w sektorze IT. Geneza FinOps wywodzi się z wyzwań, jakie niosły ze sobą inwestycje w technologie chmurowe, szczególnie w kontekście monitorowania i optymalizacji wydatków.

W centrum filozofii FinOps leży współpraca między różnymi działami w organizacji, w tym zespołami finansowymi, technologicznymi , biznesem i zakupami. Ta synergia jest kluczowa dla skutecznego zarządzania zasobami chmurowymi i związanymi z nimi kosztami. FinOps kładzie duży nacisk na podejmowanie decyzji opartych na danych, co oznacza analizowanie i interpretowanie informacji dotyczących wykorzystania chmury w celu podejmowania świadomych decyzji.

Głównym celem FinOps jest optymalizacja kosztów związanych z chmurą. Nie chodzi tutaj tylko o ich redukcję, ale o pewność, że każda „złotówka" wydana na usługi chmurowe została wydana efektywnie i w biznesowo uzasadniony sposób. FinOps jest dynamiczne, wymagające ciągłej adaptacji do zmieniających się warunków rynkowych i technologicznych.

Dlaczego FinOps jest tak ważne w sektorze finansowym?

Firmy z sektora usług finansowych (FSI) aby utrzymać wysokie tempo wdrażania innowacji i nowych usług cyfrowych – coraz częściej zaczynają swoją strukturą przypominać firmy technologiczne. Banki stały się poniekąd software-house'ami a chmura publiczna stała się kluczowym elementem innowacyjności w branży.

Jednakże, bez odpowiedniego zarządzania, może to prowadzić do utraty kontroli nad budżetowaniem i poziomem kosztów. Wynika to z lawinowo rosnącej konsumpcji usług chmurowych oraz (skądinąd pożądanego) oddawania w ręce deweloperów i biznesu narzędzi i mechanizmów do powoływania nowych usług w chmurze.

Właśnie tu z pomocą przychodzi FinOps – metodyczne i kompleksowe podejście do efektywnego zarządzania kosztami usług chmury publicznej.

Wdrażanie FinOps – trzy poziomy dojrzałości

Wdrożenie FinOps w organizacji można podzielić na trzy główne etapy rozwoju, znane jako model dojrzałości FinOps: Crawling (Pełzanie), Walking (Chodzenie) i Running (Bieganie). →

1 Raport PwC Polska: „*Chmura w biznesie, liderzy widzą wartość – sektor finansowy*" 2023.

Crawling (Pełzanie): Pierwszy etap to początkowe zrozumienie i monitorowanie wydatków na chmurę. Organizacje skupiają się na podstawowym śledzeniu i raportowaniu kosztów, ucząc się korzystać z danych do pierwszych prób optymalizacji. Jest to etap, w którym firmy zdobywają fundamentalną wiedzę na temat swoich zasobów chmurowych i ich wykorzystania.

Walking (Chodzenie): Na tym etapie organizacje posiadają już pewną wiedzę i doświadczenie w zarządzaniu kosztami chmury. Zaczynają stosować bardziej zaawansowane strategie, takie jak budżetowanie, prognozowanie i optymalizacja wydatków. To etap, w którym firmy zaczynają aktywnie zarządzać swoimi zasobami chmurowymi, starając się osiągnąć lepszą efektywność kosztową.

Running (Bieganie): Ostatni etap to pełna kontrola i zaawansowane zarządzanie wydatkami na chmurę. Organizacje wykorzystują zaawansowane narzędzia analityczne, automatyzację i integrację z innymi systemami biznesowymi, aby zmaksymalizować efektywność kosztową i wspierać strategiczne decyzje biznesowe. Na tym poziomie zarządzanie chmurą staje się integralną częścią strategii biznesowej firmy.

Dzięki FinOps, firmy z sektora finansowego mogą nie tylko optymalizować koszty, ale przede wszystkim maksymalizować wartość biznesową, jaką chmura wnosi do ich działalności.

Globalne trendy i rozwój FinOps

Na całym świecie FinOps zyskuje na popularności, stając się niezbędnym elementem w organizacjach konsumujących usługi chmury publicznej. Jednocześnie jest to młoda i dynamicznie rozwijana metodyka, a liczba certyfikowanych ekspertów na rynku z praktycznym doświadczeniem bardzo ograniczona.

Na uwagę zasługuje również fakt, że projekty FinOps w organizacjach są przekrojowe - dotyczą kilku działów – które zazwyczaj mają różne cele i priorytety. Dlatego zaangażowanie certyfikowanych ekspertów (np. z PwC) w celu dostosowania modelu i sposobu jego wdrożenia w danej organizacji pozwala znacząco przyspieszyć osiągnięcie pierwszych mierzalnych wyników.

Podsumowanie

FinOps stał się globalnym rynkowym standardem zarządzania finansowym kontekstem usług chmurowych. Pozwala rozwiać wątpliwości członków zarządu (CFO, CIO), które pojawiają się wraz z rosnącymi fakturami od dostawcy chmurowego oraz dać pewność i gwarancję maksymalnej wartości biznesowej z każdego dolara wydanego na usługi chmury publicznej. Wdrożenie FinOps w organizacji jest niemałym wyzwaniem ale współpraca z doświadczonym partnerem może znacząco przyspieszyć osiągnięcie mierzalnych efektów. •

Fot. Naphat/stock.adobe.com

Bank bez chmury nie istnieje

Raport przygotowany przez
Centrum Procesów Bankowych i Informacji

© Copyright by Centrum Procesów Bankowych i Informacji

Centrum Procesów Bankowych i Informacji
cpb.pl

Partnerzy raportu:

cloudware

pwc

Warszawa, listopad 2023
Wydawnictwo Centrum Procesów Bankowych i Informacji

BANK.PL

PORTAL FINANSOWY

O bankowości warto wiedzieć więcej!