TECHNOLOGIE DLA FINANSÓW

Ochrona danych osobowych w cyberprzestrzeni

Kradzież tożsamości w i nternecie to z perspektywy globalnej bardzo powszechne zjawisko. Badania wskazują, że każdego roku około 9 mln Amerykanów jest narażonych na cyberprzestępstwo. W naszym kraju dochodzi rocznie do 1,5 mln przypadków naruszenia danych. Liczba rośnie z roku na rok, niosąc za sobą różne konsekwencje.

Piotr **Siwiec**

prezes zarządu, AIQLabs

Fałszerstwa w sieci dosięgają wielu płaszczyzn. Jedne są relatywnie niegroźne jak na przykład wykorzystanie kodu pocztowego do rozsyłania spamu. Inne natomiast mogą być bardzo poważne, uwzględniając realne straty finansowe. Jak wynika z raportu Związku Banków Polski, cyberprzestępcy wyłudzają rocznie nawet 60 mln zł. Kradzież tożsamości, określana także fałszerstwem tożsamości lub defraudacją tożsamości, to przestępstwo opierające się na wykorzystaniu cudzych danych, jak imię, nazwisko, PESEL, adres domowy lub wizerunek, bez zgody właściciela. Ich zdobycie umożliwia przestępcy podszywanie się pod ofiarę i podejmowanie działań w jej imieniu bez jej wiedzy.

Odpowiedzialna obecność w sieci

Każda tożsamość ma unikalny charakter, także, a może nawet przede wszystkim, w internecie. Dokumenty oraz dane osobowe są czymś, czego nie można wypożyczyć. Powinny być one chronione przed niepowołanym dostępem. Należy mieć to na uwadze, również w trakcie obecności w sieci. Jak wynika z raportu GUS „Społeczeństwo informacyjne w Polsce", ponad 90 proc. gospodarstw domowych ma dostęp do internetu i regularnie z niego korzysta. Każda z osób, bez wyjątku, zostawia w sieci swój cyfrowy ślad. Dane zbierane online służą do różnych celów – wykorzystuje się je na przykład do zapamiętywania preferencji lub tworzenia anonimowych statystyk odwiedzanych serwisów. Wystarczy przeglądać strony internetowe, robić zakupy w e-commerce, korzystać z poczty mailowej, mediów społecznościowych czy popularnych komunikatorów. W sieci nikt nie jest zupełnie anonimowy, co z kolei stanowi duże udogodnienie dla cyberprzestępców.

Ochrona prywatności w internecie jest czymś, o czym należy pamiętać każdego dnia, w trakcie każdej aktywności podejmowanej online. W celu ograniczenia ryzyka narażenia się na cyberprzestępstwo warto uruchomić czujność i ograniczyć potencjalne zagrożenie. Mniejsza liczba publikacji na forach czy kanałach social media to mniej treści o charakterze publicznym. Kluczowym aspektem jest natomiast używanie unikalnych haseł. Warto również uruchomić dwuskładnikowe uwierzytelnianie. Równie ważnym aspektem jest czytanie polityki prywatności, korzystanie z wiarygodnych i zweryfikowanych aplikacji, a także zmiana ustawień przeglądarki na tryb prywatny lub incognito. Dzięki podjęciu wskazanych działań można skutecznie ochronić się przed cyberatakiem. Należy jednak zwracać uwagę na wszelkie niepokojące sygnały.

Nie brakuje przypadków, w których to właśnie sam użytkownik jest „słabym ogniwem". Trywialne hasła lub używanie podobnych ciągów autoryzacyjnych naraża go na realne niebezpieczeństwo. Każda, nawet najlepsza i wysoce zabezpieczona usługa, jest narażona na cyberatak. Te narzędzia, które są najmocniej ufortyfikowane, mają oczywiście mniejsze szanse na to, że zostaną złamane przez hakera, lecz nigdy nie możemy mieć maksymalnej pewności. Podmioty, które obracają danymi, muszą jednak zapewnić możliwie najwyższy poziom bezpieczeństwa. Przykładem jest inwestycja w nowoczesne i zaawansowane narzędzia jak dane znajdujące się w zbiornikach opartych o Blockchain, czyli rozwiązania kryptograficzne.

Fundament bezpieczeństwa

Obecnie wiele spraw można sprawnie załatwić w e-urzędzie lub placówce online. Zdalne wyrobienie nowego dowodu osobistego lub nowego meldunku już nikogo nie dziwi i stało się standardem szczególnie w czasach pandemii. Bankowość również coraz rzadziej wymaga osobistej wizyty, którą coraz skuteczniej zastępują zaawansowane aplikacje do zarządzania kontem osobistym. Nie trzeba wychodzić z domu, aby otworzyć lokatę, wziąć kredyt lub pożyczkę. Wiąże się to jednak z pewnym ryzykiem, o którym warto pamiętać, tym bardziej że wspomniane dane dotyczące rozwoju cyberprzestępstw wymagają wzmożonej czujności. Fundamentem bezpieczeństwa w internecie jest przede wszystkim wiedza na temat tego, jakie zachowania w sieci są ryzykowne. Kwestie związane z cyberbezpieczeństwem dotyczą również prób wyłudzenia kredytu. Według raportu o infoDOK wydanego przez Związek Banków Polskich, w drugim kwartale 2022 roku zablokowano 1,8 tys. prób wyłudzeń kredytów na łączną kwotę 54,4 mln zł. Jednocześnie zastrzeżono ponad 37 tys. skradzionych lub zgubionych dokumentów tożsamości. W ostatnim kwartale baza Systemu DOKUMENTY ZASTRZEŻONE wzrosła dokładnie o 37 112 szt. – to niemal dokładnie tyle samo, jak w analogicznym okresie rok temu. Statystycznie do bazy trafiało 408 szt. dziennie. Ograniczone do minimum formalności i możliwość zaciągnięcia pożyczki bez jakichkolwiek zaświadczeń to duże udogodnienie dla osób chcących jak najszybciej zdobyć dofinansowanie na dowolny cel. Uproszczone procedury przyznawania pożyczek czy nawet kredytów w bankach to także pewne ułatwienie dla złodziei tożsamości.

Ograniczenie ryzyka

Dowód osobisty jest przydatny podczas załatwiania formalności w urzędach, ale nie tylko. Dokument ten wykorzystywany jest również w innych sytuacjach, np. podczas meldowania się w hotelu czy wypożyczania sprzętu sportowego. Zdarza się także, że oszuści podają się za pracowników banku i wysyłają maila z prośbą o aktualizację danych osobowych lub też dzwoniąc w tej sprawie do potencjalnej ofiary wyłudzenia. Inną stosowaną przez nich praktyką jest oferowanie atrakcyjnej pracy, najczęściej zdalnej na podstawie umowy o dzieło. Właśnie dlatego tak istotne jest, aby nie podawać danych osobowych osobom do tego nieupoważnionym i nie udostępniać informacji niezbędnych do zawarcia umowy o pracę, jeśli istnieją podstawy ku temu, że potencjalny pracodawca jest nieuczciwy.

Sposoby reakcji

Kradzież lub zgubienie dowodu osobistego należy jak najszybciej zgłosić na policji, a także w bankach i firmach pożyczkowych, w których zaciągnęliśmy zobowiązania. Poza tym należy udać się do urzędu gminy i poprosić o zaświadczenie potwierdzające utratę dokumentu tożsamości, którym będzie można posługiwać się aż do wyrobienia nowego. Oprócz wspomnianych wyżej czynności warto też zastrzec dowód osobisty w internecie. Najłatwiejsze zadanie mają osoby zarejestrowane na stronie BIK – wówczas można zrobić to za pomocą jednego kliknięcia. Jest to bezpłatne dla wszystkich użytkowników.

Bezpieczeństwo danych i rozwój priorytetami w sektorze finansowym

W obliczu niestabilnej sytuacji gospodarczej i wahań na rynku finansowym, zmieniających się uregulowań, oczekiwań konsumentów, nowych technologii oraz alternatywnych modeli biznesowych, instytucje finansowe wdrażają strategie, które pomagają im przygotować się na przyszłość oraz zwiększyć ich możliwości szybkiego dostosowania się do powyższych zmian.

Robert **Czarniewski**
CFO, Polcom

Jeszcze kilka lat temu mówiono o tym, że instytucje finansowe dopiero będą się digitalizować. Obecnie możemy ocenić, że proces ten jest już w zaawansowanej fazie. Digitalizacja, oprócz licznych korzyści, to jednak także szereg nowych ryzyk, których nie można pominąć.

Dostosować infrastrukturę do nowych wyzwań

Przy zwiększonej aktywności niemal każdej firmy w internecie nie dziwi rosnąca ilość cyberzagrożeń. Jak wynika z danych Check Point Research z ub.r. sektor finansowy jest atakowany ok. 1000 razy w ciągu tygodnia. Ważnym aspektem jest szybkie dostosowywanie infrastruktury do nowych wyzwań, a także regulacji branżowych. Na przykład, w związku z PSD2 banki muszą udostępniać dane klientów poprzez dedykowany interfejs API. Ma to pozwolić na ich integrację z różnymi systemami innych podmiotów. Dyrektywa umożliwia także wdrożenie wielu innowacyjnych rozwiązań w zakresie usług płatniczych i bankowych.

Przy czym, wykorzystywanie PSD2 przez sektor finansowy oraz zmiana nawyków klientów np. poprzez wzrost transakcji bezgotówkowych, to także powód do pewnych obaw. Wynikają one z dwóch kwestii. Oznacza to, że znacznie wzrośnie liczba danych, które trzeba przetwarzać i odpowiednio zabezpieczyć, także przed atakami hakerów. Wg szacunków już w 2025 r. liczba danych, które powstaną na całym świecie przekroczy 175 zettabajtów. Tym samym, będzie ich prawie pięć razy więcej, niż dzisiaj. Po drugie, już 2019 roku w badaniu KPMG i Związku Banków Polskich, aż 76 proc. przedstawicieli banków wyraziło opinię, że spodziewa się zwiększonej liczby cyberataków po wdrożeniu unijnej dyrektywy.

Niesie to za sobą konieczność rozbudowy środowisk informatycznych, by były odpowiednio wydajne oraz znalezienia odpowiedniej kadry pracowników. Po drugie wszystkie dane będą wymagać dodatkowych zabezpieczeń. I tu pojawia się kolejna kwestia do rozważenia. Według Gartnera w 2023 r. wydatki na IT urosną na świecie o zaledwie 2,4 proc., do 4,5 bln dolarów – to mniej niż wcześniej prognozowali eksperci.

Z szerokiej perspektywy

Z mojego doświadczenia wynika, że firmy często myślą, że bezpieczeństwo organizacji to tak naprawdę jakieś rozwiązanie dostępne z „pudełka". Będąc głównym dostawą usług chmurowych w Polsce, mamy nieco szerszą perspektywę i widzimy na co dzień pełne spektrum różnego typu ataków, ich różnorodność technologiczną i funkcjonalną. Stąd nasuwa się wniosek, że prawdziwie bezpieczne organizacje to takie, które patrzą na ten aspekt w sposób holistyczny, a nie jak na jakiś pakiet niepowiązanych ze sobą rozwiązań. Właśnie dlatego działania w tym zakresie powinny być częścią wszystkich procesów na poszczególnych szczeblach organizacji. Wymaga to odpowiednich środków oraz wdrożenia rozwiązań technologicznych, a także monitoringu zagrożeń i podatności w systemach informatycznych, rozwiązań proceduralno-organizacyjnych oraz zaangażowania ekspertów.

Obserwujemy, że chcąc zachować zgodność z regulacjami branżowymi i bezpieczeństwo IT, a jednocześnie

> Ważnym aspektem jest szybkie dostosowywanie infrastruktury do nowych wyzwań, a także regulacji branżowych.

zwiększyć elastyczność biznesową sektor finansowych coraz częściej sięga po chmurę. Chmura pomaga instytucjom we wdrażaniu nowych modeli biznesowych i operacyjnych wynikających z aktualnych potrzeb klientów oraz dostosowaniu się do wytycznych regulatorów takich jak np. KNF. Pozwala też na szybkie i skuteczne dostarczanie produktów istotnych dla klientów banków i instytucji finansowych, pomocy w monetyzacji aktywów związanych z danymi oraz zapewnieniu odpowiedniego poziomu ich bezpieczeństwa.

W Polcom już teraz dostarczamy usługę cloud computingu do co najmniej 20 czołowych, polskich i zagranicznych instytucji finansowych. Widzimy, że rodzimy sektor finansowy coraz bardziej otwiera się na usługi chmurowe, szczególnie świadczone przez polskich usługodawców. Niemniej należy mieć świadomość, że w tej kwestii jest jeszcze sporo do nadrobienia, ponieważ – jak wskazują dane zebrane przez PwC Polska w raporcie „Chmura i jej wartość. Oczekiwania vs. rzeczywistość: wyniki dla sektora finansowego" aż 65 proc. instytucji finansowych ocenia swoją dojrzałość chmurową jako niską.

Instytucje finansowe na celowniku hakerów

Firmy z branży finansowej są narażone na cyberataki 300 razy częściej niż przedsiębiorstwa działające w innych obszarach. Instytucje finansowe przetwarzają cenne dane dotyczące m.in. aktywów i transakcji, dlatego cyberprzestępczość jest dla nich poważnym zagrożeniem. Zapobieganie atakom utrudnia też złożoność systemów informatycznych stosowanych w instytucjach finansowych.

Niklas **Enge**
dyrektor regionalny
Nordics i Polska, Progress

Naruszenia systemów bezpieczeństwa w firmach z branży finansowej stają się coraz bardziej powszechne, a ich skutki – coraz bardziej poważne. Hakerzy biorą na celownik w szczególności amerykańskie firmy finansowe – 27 proc. globalnych cyberataków jest wymierzona właśnie w przedsiębiorstwa z USA. W następnej kolejności atakowane są instytucje finansowe z Wielkiej Brytanii, Japonii i Rosji. Również polskie instytucje finansowe narażone są na niebezpieczeństwo. Według danych Komisji Nadzoru Finansowego z lutego zeszłego roku, przeciętne polskie przedsiębiorstwo z sektora bankowego jest atakowane około tysiąc razy w tygodniu. Wprost proporcjonalnie do liczby cyberataków rosną też koszty związane z usuwaniem ich skutków. Badanie Accenture wykazało, że średni roczny koszt związany z naruszeniem danych w firmach z sektora usług finansowych wynosi już 18,5 miliona dolarów. Jednocześnie trudno oszacować wpływ, jaki cyberataki mają na reputację organizacji. Ryzyko związane z bezpieczeństwem danych dotyczy całego procesu obsługi klienta – od korzystania z aplikacji, poprzez obsługę w placówkach finansowych, po procedurę udzielania kredytu. Wraz z rozpowszechnieniem się bankowości mobilnej klienci oczekują całodobowego dostępu do swojego konta. Dodatkowo w Polsce bardzo prężnie działają fintechy, które oferują np. wygodne opcje płatności w internecie. Tymczasem według danych ImmuniWeb, 92 proc. mobilnych aplikacji bankowych zawiera co najmniej jedną lukę bezpieczeństwa średniego ryzyka.

Monitorowanie sieci ułatwia zarządzanie bezpieczeństwem

Odpowiedzią firm na coraz częstsze i bardziej niebezpieczne cyberataki jest zwiększanie działań w zakresie bezpieczeństwa danych. Inwestują w rozszerzony monitoring infrastruktury IT, aby skanować dane w poszukiwaniu przypadków naruszeń bezpieczeństwa, awarii, złośliwego oprogramowania i innych anomalii systemowych. Co więcej, firmy wprowadzają narzędzia, które mogą zautomatyzować procesy bezpieczeństwa. Biorąc pod uwagę zwiększającą się liczbę ataków na systemy finansowe, automatyzacja to niezbędna funkcja. Hakerzy nie przestaną wprowadzać innowacji i szukać nowych dróg dostępu do sieci finansowych. Dostępne są jednak rozwiązania eliminujące problemy, z którymi zespoły IT w sektorze usług finansowych borykają się najczęściej. Należy do nich kompleksowy monitoring IT, czyli jedno, dobrze dobrane narzędzie, które pozwala na szczegółową obserwację infrastruktury IT, czyli serwerów, routerów, rozwiązań w chmurze, aplikacji i systemów pamięci masowej. Kolejne rozwiązanie to inteligentne powiadomienia, czyli system alertów, który natychmiast sygnalizuje każdą niepokojącą aktywność. Należy pamiętać, że zbyt duża liczba alertów może przytłoczyć zespół IT. Według badań przeprowadzonych przez Ovum, ponad jedna trzecia (37 proc.) banków dziennie otrzymuje średnio 200 tys. powiadomień związanych z bezpieczeństwem. Ważne jest także szczegółowe monitorowanie ruchu sieciowego, aby sprawdzić, którzy użytkownicy, aplikacje i urządzenia zużywają najwięcej pasma. Nietypowe wykorzystanie i skoki aktywności mogą wskazywać na problem z bezpieczeństwem. Instytucje finansowe nie mogą zapomnieć o konfiguracji sieci w celu zabezpieczenia się przed przypadkowymi lub złośliwymi zmianami konfiguracji urządzeń sieciowych. Istotne jest również zarządzanie logami – monitorowanie ich i ustawianie alertów dla meta trendów, takich jak zmiany objętości oraz filtrowanie i archiwizowanie logów przez dowolny okres przechowywania, aby spełnić wymagania prawne.

Dodatkowe środki bezpieczeństwa

Monitorowanie infrastruktury IT to podstawowa linia obrony instytucji finansowej przed cyberatakami. Firmy mogą korzystać z własnej polityki alertów w połączeniu z możliwościami AI i uczenia maszynowego, aby dowiedzieć się skąd pochodzą ataki i przewidzieć problemy zanim się pojawią. Innym rodzajem monitoringu jest rozwiązanie Network Detection and Response (NDR), które bada przepływ ruchu w sieci. NDR to wielowarstwowe podejście do bezpieczeństwa, wykorzystujące analizę zachowań, algorytmy, uczenie maszynowe czy dane dotyczące reputacji firmy. Może być używane do przewidywania i automatyzacji reakcji na wykryte zagrożenia, które ominęły ochronę obwodową i zaczęły się rozprzestrzeniać w sieci. Oczywiście, sam monitoring sieci nie jest jedynym rozwiązaniem. Ważną rolę odgrywają zaktualizowane zasady dotyczące haseł, dwuskładnikowe uwierzytelnianie oraz kampanie edukacyjne dla użytkowników.

Szkolenia dla pracowników i weryfikowanie ich wiedzy związanej z bezpieczeństwem są równie istotne, aby mieć pewność, że zespoły specjalistów mają bieżące informacje na temat zagrożeń i sposobów ich zapobiegania.

Źródła:
Raport Federal Reserve Bank of New York, „Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis"
Raport Chinatechtreat.com, „High-Tech Heist: Chinese government, it vendors, and the threat to US banks"
Badanie Accenture, „Unlocking the Value of Improved Cybersecurity Protection"
Raport Związku Przedsiębiorstw Finansowych I EY Polska, „Nadużycia w sektorze finansowym. Edycja 2022"
Badanie ImmuniWeb, State of Application Security at S&P Global World's 100 Largest Banks

O TRANSFORMACJI CYFROWEJ W FINANSACH, CZYLI NA CO ZWRÓCIĆ UWAGĘ, ABY ODNIEŚĆ SUKCES

Jak optymalizować procesy i przeprowadzać jednostki biznesowe przez cyfrową transformację? Nowoczesne rozwiązania wsparciem dla instytucji finansowych.

Katarzyna **Wojda**

dyrektor finansowy, ING Hubs Poland

Transformacja cyfrowa bezsprzecznie zwiększa potencjał przedsiębiorstwa, znajdując rozwiązania dla potrzeb wynikających ze zmieniającej się rzeczywistości i rozwijającego się technologicznie otoczenia rynkowego czy rosnących oczekiwań klientów, a także prowadzi do większej efektywności procesów wewnętrznych.
Z punktu widzenia finansów, pozwala nie tylko na docelową maksymalizację zysku przez zwiększanie przewagi wśród konkurencji, ale przede wszystkim jest sposobem na optymalizowanie procesów w przedsiębiorstwie czy instytucji finansowej.
Czym jednak jest transformacja, jak przez nią przeprowadzić przedsiębiorstwo i czy to proces jednorazowy – o tym poniżej.

> Najkrótsza definicja transformacji cyfrowej to przekształcenie procesów analogowych w cyfrowe za pomocą technologii, czyli wykorzystanie technologii w celu poprawy procesów biznesowych związanych ze sprzedażą, z obsługą klienta czy zarządzaniem łańcuchem dostaw. Inaczej mówiąc, to wdrożenie i właściwe wykorzystanie rozwiązań opartych na nowoczesnych technologiach cyfrowych.

Czym jest transformacja cyfrowa

Najkrótsza definicja transformacji cyfrowej to przekształcenie procesów analogowych w cyfrowe za pomocą technologii, czyli wykorzystanie technologii w celu poprawy procesów biznesowych związanych ze sprzedażą, z obsługą klienta czy zarządzaniem łańcuchem dostaw. Inaczej mówiąc, to wdrożenie i właściwe wykorzystanie rozwiązań opartych na nowoczesnych technologiach cyfrowych.
W przypadku instytucji finansowych często skupiamy się na kliencie i poprawie jego zadowolenia ze sposobu, w jaki korzysta z produktów czy łatwości dostępu do nich.
Z kolei z punktu widzenia wewnętrznych zespołów finansowych dążymy na przykład do skrócenia czasu niezbędnego na pozyskanie danych oraz ich przetworzenie, ale także eliminujemy nieefektywności związane z papierową dokumentacją i pracą manualną.
Należy też podkreślić, że chociaż transformacja cyfrowa bierze swoją nazwę od nowych – częściowo lub całościowo cyfrowych procesów, to tak naprawdę jest kompleksową transformacją firmy, wymuszającą przemyślenie i przeprojektowanie zasadniczo wszystkich procesów w ramach przedsiębiorstwa czy instytucji finansowej. To zmiana technologiczna, ale także zmiana organizacyjna i kulturowa w przedsiębiorstwie, wywołująca inne wykorzystanie zasobów i zmianę sposobu myślenia o sposobie, w jaki realizujemy swoje cele biznesowe.

Transformacja cyfrowa, czyli poprawa wydajności

Przede wszystkim taka transformacja pozwala na poprawę wydajności. Cyfryzacja danego procesu, jak choćby wprowadzenie podpisów elektronicznych, pozwala skrócić czas niezbędny do przeprowadzenia danego procesu do minimum. To oznacza także poprawę zarządzania zasobami: zużyjemy mniej papieru i zaangażujemy mniej ludzi i urządzeń, by osiągnąć ten sam cel – a zasoby wykorzystamy efektywniej. Zmieniając w ten sposób model biznesowy, polepszamy standard obsługi klientów i budujemy swoją markę jako firmy nowoczesnej. Z kolei pracownicy dzięki przejściu na technologię cyfrową uzyskują lepszy komfort pracy, zwłaszcza teraz w okresie po pandemii, gdy w dużej mierze pracujemy zdalnie lub w modelach hybrydowych.

Jak przeprowadzić firmę przez cyfryzację

Przede wszystkim należy zdefiniować obszary, które powinny być poddane transformacji cyfrowej. Zmiany przełożą się na całą firmę, ale określenie celu szczegółowego pozwoli na kolejne kroki planu – zaplanowanie działań i określenie budżetu.
Wskazanie potrzeb daje możliwość przeprowadzenia analizy tego, co faktycznie powinno ulec zmianie, aby osiągnięcie celu było możliwe, a to z kolei pozwala na skonkretyzowanie rozwiązań, które pomogą dokonać tej zmiany. Wybór narzędzi i sposobu ich implementacji zależy od specyfiki przedsiębiorstwa czy instytucji finansowej oraz aktualnego stanu technologicznego. Samo określenie obszaru działań jest zależne od potrzeb organizacji (obecnych i przyszłych) i może obejmować zarówno wdrożenie prostego oprogramowania IT, jak i wprowadzenie rozwiązań bazujących np. na sztucznej inteligencji, analiz Big Data czy rozwiązań chmurowych.
Gdy określimy już, czego potrzebujemy i jakimi metodami chcemy osiągnąć cel, należy przeprowadzić szczegółową analizę rozwiązań dostępnych na rynku oraz zapewnić finansowanie projektu. Ma to na celu znalezienie najlepszego rozwiązania w ramach dostępnego budżetu, ale także pod kątem spodziewanych korzyści z transformacji, zarówno wymiernych (mierzonych np. zmniejszonym zużyciem zasobów), jak i częściowo wymiernych lub niewymiernych (jak komfort pracowników czy klientów, lub wizerunek przedsiębiorstwa na rynku).
Finalnie, konieczny jest szczegółowy plan w czasie i zapewnienie zasobów niezbędnych do realizacji tego planu, przy czym konieczna jest też pamięć o odpowiednim zarządzeniu zmianą, bez którego nawet najlepszy plan może napotykać trudności. Zarządzanie zmiana będzie zatem kolejną kompetencją, którą należy zapewnić w transformowanej instytucji. Trzeba mieć na uwadze szczególnie to, jak pracownicy adaptują się do nowego procesu, w którym ich role ulegają modyfikacji. Pewne elementy procesu zostaną zastąpione przez automatyzację, a inne wymagają nauczenia się zupełnie nowych umiejętności czy przestawienia się na inny model pracy, skupiających się wokół komunikacji, pracy zespołowej i utrzymaniu wysokiej produktywności.

> Przede wszystkim należy zdefiniować obszary, które powinny być poddane transformacji cyfrowej. Zmiany przełożą się na całą firmę, ale określenie celu szczegółowego pozwoli na kolejne kroki planu – zaplanowanie działań i określenie budżetu.

> Chociaż transformacja cyfrowa bierze swoją nazwę od nowych – częściowo lub całościowo cyfrowych procesów, to tak naprawdę jest kompleksową transformacją firmy, wymuszającą przemyślenie i przeprojektowanie zasadniczo wszystkich procesów w ramach przedsiębiorstwa czy instytucji finansowej.

Jedna transformacja i gotowe? Nie.

Czytając artykuły na temat transformacji cyfrowej, możemy się natknąć na stwierdzenie, że to „cyfrowa rewolucja", co jest nawiązaniem do szybkości zachodzących zmian wymuszających dostosowanie do rynku (lub lepiej – wyjście o krok przed konkurencję). Natomiast należy pamiętać, że sukcesu związanego z transformacją cyfrową nie odnosi się w jeden dzień, zwłaszcza że już w momencie planowania zmiany powinniśmy mieć świadomość, że codziennie pojawiają się nowe dostępne rozwiązania. To oznacza, że wybrane narzędzia się starzeją i są wypierane przez inne. Transformacja jest długotrwałym procesem – jednak nie w sensie czasu potrzebnego do implementacji pojedynczych zmian, chociaż oczywiście to także zależy od kompleksowości procesu i narzędzi, które zmieniamy. Długotrwałość wynika bowiem z konieczności stałej gotowości do zmian i nieustannego ich śledzenia i poszukiwania. Warto jednak, bo odpowiednie technologie w połączeniu z ludźmi i zoptymalizowanymi procesami, umożliwiają przedsiębiorstwom i instytucjom finansowym reagowanie na potrzeby klientów i zmiany na rynku, a także na stymulowanie przyszłego rozwoju.
Praca w modelu „Continuous improvement" (ciągłe udoskonalanie) to jedyne rozwiązanie, które pozwala na ewolucję po tym, jak dokonujemy „rewolucji".

Chmura rozwiąże problemy działów finansowych w bankach

W erze transformacji cyfrowej banki muszą wprowadzać innowacje znacznie szybciej niż kiedyś. W obliczu trendów, takich jak np. otwarta bankowość, banki muszą świadczyć klientom nowe rodzaje usług, aby utrzymać konkurencyjność. Klienci coraz częściej korzystają z bankowości mobilnej – w związku z tym banki muszą dysponować elastycznymi środowiskami informatycznymi, które można szybko zaktualizować lub rozszerzyć i które umożliwiają realizację nowych projektów w ciągu tygodni, a nie miesięcy czy lat.

Marcin **Odrowąż-Sypniewski**

Lead Account Manager, Financial Services, Oracle Polska

Obecnie klienci oczekują od swoich dostawców usług finansowych czegoś więcej niż tylko obsługi transakcji. Chcą, by banki dostarczały im nowe i lepsze rozwiązania do zarządzania ich sprawami finansowymi. W dzisiejszych czasach klienci nie widzą specjalnej różnicy między usługami bankowymi a innymi. Po prostu oczekują wygody i najwyższego poziomu bezpieczeństwa. Klientów nie obchodzi także kwestia zgodności z przepisami.

Aby sprostać tym oczekiwaniom, przed działami finansowymi w bankach pojawia się nowe wyzwanie: współpracować z kierownikami poszczególnych działów w celu szybszego uzyskiwania informacji o znaczeniu strategicznym oraz przeprowadzania analiz predykcyjnych umożliwiających rozwój banku. Dotychczas głównym zadaniem działu finansowego było zapewnienie obsługi transakcji. Obecnie dyrektorzy generalni banków oczekują, że ich dyrektorzy finansowi będą poświęcać więcej czasu na działania napędzające rozwój instytucji. Realizacja tej misji jest możliwa dzięki współpracy w chmurze.

Nowy model operacyjny dla elastycznych działów finansowych

Działy finansowe w bankach i innych branżach tradycyjnie skupiają się na księgowości, budżetach, prognozach i śledzeniu wskaźników KPI. Ale obecnie coraz częściej oczekuje się od nich zaangażowania we wprowadzanie innowacji i tworzenie wartości przy jednoczesnym obniżaniu ogólnych kosztów działalności. Oczywiste jest, że wymaga to nowego podejścia do funkcjonowania działów finansowych.

Współczesna branża finansowa ewoluuje, a jej model działania coraz częściej zapewnia elastyczność, jaką daje przetwarzanie w chmurze. Już niedługo usługi finansowe zmienią swoje oblicze. Złożone, przestarzałe systemy zostaną zastąpione platformami chmurowymi, realizującymi funkcje raportowania, planowania, prognozowania i analizowania i dostarczającymi dane osobom odpowiedzialnym za podejmowanie decyzji w przedsiębiorstwie. Z kolei technologia Blockchain może zrewolucjonizować przetwarzanie transakcji i zarządzanie kontrahentami bez udziału pośredników.

Uczenie maszynowe i systemy automatyzacji umożliwią automatyzację wielu rutynowych procesów biznesowych, co pozwoli zespołom ds. finansowych poświęcać więcej czasu na wspieranie podejmowania decyzji i analizy predykcyjne z wykorzystaniem sztucznej inteligencji oraz danych dostarczonych przez statystyków, analityków, specjalistów ds. ekonomii behawioralnej, a nawet antropologów. Liderzy działów finansowych oraz ich zespoły wykorzystują te możliwości na wiele sposobów. Poszerzają swoją wiedzę informatyczną i wdrażają technologie, które umożliwiają im dokonywanie analiz i wspieranie osób zarządzających w podejmowaniu decyzji. Może to obejmować na przykład wykrywanie trendów, wskazywanie możliwości rozwoju oraz proponowanie nowych produktów.

Elastyczne działy finansowe tworzą nowe modele finansowe i sposoby pracy. Formują zintegrowane, realizujące wiele zróżnicowanych zadań zespoły, które są skupione w centrach doskonałości lub centrach usług współużytkowanych. Zespoły te muszą jednak w swojej pracy zmierzyć się z wieloma wyzwaniami – takimi jak:

- Kwestie strukturalne: działy finansowe muszą centralizować funkcje, aby móc uzyskiwać szybki i łatwy dostęp do danych.
- Niewydajne systemy: z czasem systemy informatyczne działów finansowych stają się coraz bardziej złożone i scentralizowane – zwłaszcza, gdy bank staje się większy w wyniku przejęcia. Uproszczone i zintegrowane systemy przetwarzania w chmurze są łatwiejsze w utrzymaniu i aktualizowaniu oraz zapewniają lepszy dostęp do danych.
- Ludzie i kompetencje: specjaliści ds. finansowych muszą być lepiej zaznajomieni z nowymi technologiami, by móc z nich korzystać. Zakresy obowiązków i kryteria rekrutacji zmieniają się w odpowiedzi na zapotrzebowanie na wiedzę specjalistyczną dotyczącą technologii w branży finansowej.

Działy finansowe o zoptymalizowanej strukturze, dysponujące odpowiednimi systemami i zespołami pracowników, są w stanie obniżyć koszty finansowania przy jednoczesnym tworzeniu większej wartości. Elastyczne działy finansowe skupiają się w większym stopniu na działaniach przynoszących większe korzyści biznesowe dzięki wykorzystaniu zintegrowanej analizy i możliwości drążenia danych, planowaniu i modelowaniu predykcyjnemu oraz wizualizacji danych. Wszystkie powyższe korzyści zapewniają środowiska IT działające w chmurze, ponieważ model cloud computing zapewnia doskonałą widoczność danych w całym przedsiębiorstwie.

> Działy finansowe w bankach i innych branżach tradycyjnie skupiają się na księgowości, budżetach, prognozach i śledzeniu wskaźników KPI. Ale obecnie coraz częściej oczekuje się od nich zaangażowania we wprowadzanie innowacji i tworzenie wartości przy jednoczesnym obniżaniu ogólnych kosztów działalności.

Podsumowanie

Dzięki przejściu do chmury działy finansowe banków stają się bardziej elastyczne, a pracownicy tych działów pracują szybciej i efektywniej przy niższych kosztach. Na przykład projekty rozwojowe mające na celu dostarczenie bardziej zintegrowanych danych mogą być realizowane znacznie szybciej niż typowy okres 12-18 miesięcy. Projektowanie, utrzymywanie i modernizacja efektywnych systemów przetwarzania w chmurze zajmuje mniej czasu, co pozwala działom finansowym w bankach zmniejszyć wysokie koszty finansowania.

Integracja danych w chmurze umożliwia ich zaawansowaną analizę, co pozwala działom finansowym w bankach skupić się na tworzeniu strategii rozwoju nowych produktów i zwiększania wzrostu. Dzięki agregacji danych w chmurze sztuczna inteligencja oraz uczenie maszynowe pozwalają szybciej identyfikować trendy, a tym samym wspierać prognozowanie. Także analiza wielkich zbiorów danych jest bardziej efektywna, gdy zintegrowane dane są przechowywane w chmurze. Umożliwia to działom finansowym współpracę z innymi działami w celu realizacji programów rozwojowych, takich jak spersonalizowane kampanie marketingowe, w ramach których klienci uzyskują informacje o produktach i usługach finansowych odpowiadających ich potrzebom.