TOMASZ KWICZOR
Dyrektor ds. Usług Outsourcingowych w Talex SA

Specjalista w zakresie zapewnienia ciągłości działania i outsourcingu IT. Doświadczony Project Manager w projektach kolokacyjnych, Cloud Computing oraz wsparcia użytkownika. Od 2002 r. pracuje w Talex SA, gdzie pełnił funkcje kierownika zespołu Help Desk oraz dyrektora data center.

WSZYSTKO, CO KAŻDY MENEDŻER W BANKU POWINIEN WIEDZIEĆ O BEZPIECZNYM DATA CENTER

Polska bankowość uważana jest za jedną z najlepiej rozwiniętych na świecie, zwłaszcza w obszarze bankowości elektronicznej. Mimo to większość banków nadal posiada własne data center (model *on-premise*). Jakie są tego konsekwencje? Czy własne data center rzeczywiście gwarantuje bankowi bezpieczeństwo i ciągłość działania?

Dotychczas w bankach dane przetwarzano zazwyczaj lokalnie, na własnym sprzęcie. Jest to tzw. model *on-premise*. Takie podejście z jednej strony było wynikiem przekonania, że tylko własny ośrodek przetwarzania danych zapewni pełną kontrolę nad infrastrukturą, a co za tym idzie bezpieczeństwo i wysoką dostępność usług. Z drugiej strony wynikało ono z braku profesjonalnych dostawców usług data center oraz braku regulacji prawnych i jasnych wytycznych, które określałyby, czy można korzystać w tym obszarze z usług zewnętrznego dostawcy oraz jakie powinien on spełniać kryteria.

WADY I ZALETY POSIADANIA PRZEZ BANK WŁASNEGO DATA CENTER

Posiadanie przez bank własnego data center ma pewne zalety, ale też wiele wad. Wśród zalet należy przede wszystkim wymienić pełną,

nieprzerwaną kontrolę nad całą infrastrukturą IT znajdującą się w przestrzeni zarządzanej przez bank. W modelu *on-premise* bank posiada własny zespół IT doskonale orientujący się w całej infrastrukturze. Z punktu widzenia banku takie rozwiązanie wydaje się gwarantować maksymalne bezpieczeństwo i ciągłość działania. Jednakże w praktyce ośrodki data center banków często nie spełniają podstawowych wymogów bezpieczeństwa pod względem lokalizacji oraz architektury i konstrukcji budynków, zwykle adaptowanych, a nie projektowanych od początku jako centra przetwarzania danych. Zdarza się również, że bank posiada podstawowy ośrodek data center i ośrodek zapasowy w zbyt małej odległości od siebie, co generuje dodatkowe ryzyko przerwania ciągłości działania.

Wśród wielu wad posiadania własnego data center wymienić należy przede wszystkim konieczność poniesienia wysokich nakładów inwestycyjnych (CAPEX). Dziś otoczenie rynkowe zmienia się dynamicznie, więc ponoszenie dużych nakładów finansowych na rozwój własnej infrastruktury, a w szczególności inwestowanie w nieruchomości, może być ryzykowne.

Bywa to jednak niezbędne, jeśli chce się sprostać aktualnym wymaganiom norm bezpieczeństwa. Dodatkowo istnieje ryzyko, że bank z różnych względów będzie zmuszony zmienić lokalizację ośrodka zanim poniesione nakłady w pełni się zamortyzują. Myśląc o budowie własnego data center, uwzględnić należy także stałe koszty jego bieżącego funkcjonowania (zużycie mediów, przeglądy, serwisy itp.) oraz koszty utrzymania zespołu specjalistów i obsługi ośrodka. Co jakiś czas infrastruktura wymaga także zazwyczaj kosztownych modernizacji i ponoszenia kolejnych nakładów finansowych.

> Dziś otoczenie rynkowe zmienia się dynamicznie, więc ponoszenie dużych nakładów finansowych na rozwój własnej infrastruktury, a w szczególności inwestowanie w nieruchomości, może być ryzykowne.

Jednak największym wyzwaniem dla banku jest spełnienie wszystkich norm bezpieczeństwa data center rekomendowanych przez regulatorów. Prowadzenie centrum przetwarzania danych nie należy do podstawowej działalności banku, ale z pewnością od prawidłowego i bezpiecznego funkcjonowania ośrodka zależą kluczowe dla instytucji procesy.

CO DZIŚ OZNACZA BEZPIECZNE DATA CENTER?

Data center gwarantujące bezpieczeństwo danych i zapewniające ciągłość działania musi spełniać określone normy i standardy. Dzisiaj trzy powszechnie akceptowane to:

- **Data Center Infrastructure Tier Standard** – standard opracowany przez Uptime Institute,
- **ANSI/TIA-942Telecommunications Infrastructure Standard for Data Centers** – standard opracowany przez The Telecommunications Industry Association (TIA),
- **EN 50600: Information Technology – Data Centre Facilities and Infrastructures** – seria norm opracowana przez European Committee For Electrotechnical Standardization (CENELEC).

Standard Data Center Infrastructure Tier opisuje sposób funkcjonowania data center i definiuje cele, jakie należy osiągnąć na etapie projektowania, a następnie budowy ośrodka. Nie podaje jednak sposobów prowadzących do ich osiągnięcia. Standard koncentruje się na infrastrukturze zasilania i chłodzenia, pomijając zupełnie kwestie bezpieczeństwa fizycznego czy infrastruktury sieciowej. Dodatkowo krytykowany jest za swój komercyjny charakter i brak jednoznacznych reguł klasyfikacji.

Standard ANSI/TIA-942 pierwotnie dotyczył wyłącznie okablowania i infrastruktury telekomunikacyjnej. W kolejnych etapach został rozszerzony o zagadnienia związane z redundancją i niezawodnością, które zostały przejęte ze standardu opracowanego przez Uptime Institute. Nie bez znaczenia pozostaje fakt, że standard TIA-942

został przygotowany przez instytucję amerykańską z myślą o rynku amerykańskim, a nie europejskim.

Standard EN 50600 opracowany został przez Europejski Komitet Normalizacyjny Elektrotechniki (CENELEC). Został przyjęty przez Komisję Europejską, a następnie ratyfikowany i przyjęty przez kraje członkowskie Unii Europejskiej,

> Prowadzenie centrum przetwarzania danych nie należy do podstawowej działalności banku, ale z pewnością od prawidłowego i bezpiecznego funkcjonowania ośrodka zależą kluczowe dla instytucji procesy.

w tym przez Polski Komitet Normalizacyjny jako norma PN/EN 50600 (BS/EN 50600 w Wielkiej Brytanii, DIN/EN 50600 w Niemczech itd.). Standard ten składa się z serii szczegółowych norm, które kompleksowo obejmują zagadnienia data center. Zapisy standardu nawiązują do innych oficjalnych norm stosowanych na obszarze Unii Europejskiej i są w stosunku do nich komplementarne.

W przypadku instytucji finansowych standard EN 50600 zasługuje na szczególną uwagę. Pojawia się on bowiem w wielu dokumentach wydanych jako wytyczne dla bezpiecznego przetwarzania danych. Wymienia go między innymi w swoich rekomendacjach Urząd Komisji Nadzoru Finansowego, Związek Banków Polskich oraz uchwała Rady Ministrów.

Spełnienie przez data center banku rygorystycznych wymogów normy EN 50600 jest trudne, czasochłonne i kosztowne. Alternatywą jest więc znalezienie dostawcy zewnętrznego, którego centra przetwarzania danych posiadają certyfikat zgodności z normą EN 50600.

JAKIE MOŻLIWOŚCI MA BANK, KORZYSTAJĄC Z ZEWNĘTRZNEGO DATA CENTER?

Dzisiaj dostawcy usług data center oferują szeroki wachlarz możliwości. Dlatego tak ważne jest, aby rozpocząć od analizy problemów, z jakimi mierzy się dana instytucja finansowa. Dopiero prawidłowe zidentyfikowanie potrzeb pozwala na wybranie najlepszego dla danego banku rozwiązania.

Decydując się na skorzystanie z usług zewnętrznego data center, bank ma do wyboru dwie podstawowe możliwości: **kolokację** oraz usługi **cloud computing**.

Kolokacja polega na ulokowaniu własnej infrastruktury technologicznej banku (własny sprzęt i oprogramowanie) w centrum przetwarzania danych należącym do zewnętrznego dostawcy. W jej przypadku bank pozostaje jedynym właścicielem infrastruktury technologicznej służącej do przechowywania i przetwarzania danych. Profesjonalny dostawca usług data center zapewnia nie tylko optymalne warunki pracy sprzętu IT, ale także dba o bezpieczeństwo sprzętu i danych, uniemożliwiając dostęp do nich osobom nieuprawnionym. Ciągłość działania ośrodka data center gwarantuje redundantna infrastruktura, a wszystkie systemy nadzorowane są przez całodobowy monitoring. Utrzymanie takiego środowiska pracy we własnym centrum przetwarzania danych byłoby dla banku niezwykle kosztowne i wymagające. Ponadto banki bardzo często nie są w stanie spełnić rygorystycznych norm bezpieczeństwa data center na takim poziomie, jak certyfikowane ośrodki przetwarzania danych należące do firm wyspecjalizowanych w tym zakresie. Z tych względów kolokacja jest doskonałym rozwiązaniem – bank ma zagwarantowane właściwe parametry środowiskowe oraz ciągłość działania infrastruktury IT bez konieczności ponoszenia nakładów inwestycyjnych na budowę własnego ośrodka data center. Skorzystanie z usługi kolokacji pozwala więc uwolnić środki finansowe i przeznaczyć je na finansowanie podstawowej działalności banku. Dodatkowo ograniczane są w ten sposób koszty związane z bieżącym utrzymaniem własnego data center, a odpowiedzialność za zabezpieczenie danych przeniesiona zostaje na dostawcę.

Cloud computing to usługa polegająca na przetwarzaniu i przechowywaniu danych w data center należącym do zewnętrznego dostawcy. Kierowana jest więc do wszystkich instytucji, które nie

chcą ponosić kosztów związanych z inwestycją nie tylko w nieruchomości, ale także w sprzęt IT czy oprogramowanie. Usługi opłacane są w ramach abonamentu (koszty klasyfikowane jako wydatki operacyjne – OPEX). Cloud computing to elastyczne rozwiązanie pozwalające dopasować zasoby IT do aktualnego zapotrzebowania.

W ramach cloud computing bank może korzystać z najnowocześniejszych platform sprzętowych czołowych producentów i dzięki temu wdrażać nowe rozwiązania informatyczne, jednocześnie w pełni kontrolując koszty.

Usługa ta umożliwia szybką migrację danych lub systemów na lepiej dostosowany do aktualnych wymagań banku sprzęt oraz zwalnia bank z konieczności modernizacji infrastruktury IT i zabezpieczenia fizycznego dostępu do danych. Korzystając z usługi cloud computing w certyfikowanym data center, bank może szybko podnieść swoje standardy bezpieczeństwa bez ponoszenia ogromnych nakładów inwestycyjnych (CAPEX). Przenosi również pełną odpowiedzialność za utrzymanie ciągłości działania oraz bezpieczeństwo danych i systemów należących do banku na zewnętrznego dostawcę.

Usługi cloud computing można podzielić na:

- chmurę prywatną,
- chmurę publiczną,
- chmurę hybrydową.

Chmura prywatna to usługa, w której cała udostępniona na cele przetwarzania danych infrastruktura jest dedykowana dla jednego klienta. Zapewnia ona pełną kontrolę nad dostępem fizycznym do sprzętu, cyfrowym do danych i nad całą architekturą bezpieczeństwa. W tym modelu nie występuje współdzielenie zasobów fizycznych (serwerów, macierzy dyskowych itp.). Korzystając z chmury prywatnej, można uzyskać od dostawcy usługi gwarancje związane z SLA (*Service Level Agreement*) oraz jasno określić miejsce, w którym sprzęt jest zainstalowany, a co za tym idzie – dokładną lokalizację przetwarzania danych. Jest to szczególnie istotne w przypadku instytucji finansowych, które zgodnie z rekomendacjami KNF powinny przechowywać i przetwarzać dane na terenie Rzeczypospolitej Polskiej.

Chmura publiczna charakteryzuje się współdzieleniem infrastruktury przez wielu klientów. Należy tutaj jednak jasno rozgraniczyć chmurę publiczną rozumianą jako współdzieloną przez kilku klientów u lokalnego dostawcy (klient nadal wie, gdzie fizycznie przetwarzane i składowane są jego dane) od chmury publicznej oferowanej przez takich dostawców, jak np. Amazon czy Google. Z infrastruktury tego typu firm korzystają miliony użytkowników, a serwery ulokowane są na całym świecie. Nigdy nie ma więc stuprocentowej pewności, gdzie dane są przechowywane i przetwarzane. Aby uniknąć wieloznaczności terminu „chmura publiczna", w dalszej części artykułu na określenie chmury publicznej oferowanej przez lokalnego dostawcę, przyjęto pojęcie **chmury współdzielonej**.

Chmurę współdzieloną bank może rozważyć dla procesów, które mają charakter pomocniczy i nie są związane z krytycznymi danymi. Mogą to być przykładowo środowiska testowe, deweloperskie lub wpierające pracę użytkownika końcowego. Należy jednak pamiętać, że mimo, iż procesy te nie mają kluczowego – z punktu widzenia działalności banku – znaczenia, to nadal dostawca chmury podlega wszystkim restrykcjom wskazanym przez regulatora.

Chmura hybrydowa to rozwiązanie, które łączy w sobie chmurę prywatną i publiczną. W tym wariancie klient część danych przechowuje i przetwarza na dedykowanej, wydzielonej infrastrukturze, a część na infrastrukturze współdzielonej. Rozwiązanie hybrydowe to także połączenie zasobów banku z chmurą u zewnętrznego dostawcy. W przypadku posiadania chmury prywatnej i publicznej u jednego, zewnętrznego dostawcy, dodatkową korzyścią jest lepsze zabezpieczenie danych – obie chmury mogą być ze sobą połączone fizycznie, na poziomie sprzętu, bez użycia sieci publicznej.

> W przypadku banków istotne jest, aby usługi chmurowe zawsze świadczone były z konkretnego, znanego bankowi data center, a ośrodek ten spełniał wszystkie normy wskazane przez regulatora.

W przypadku instytucji finansowych usługi cloud computing mogą stanowić uzupełnienie mocy obliczeniowych wykorzystywanych wewnątrz organizacji. Oznacza to, że bank może korzystać z rozwiązań chmurowych dla wybranych procesów lub usługi. Wybór takiej drogi nie wymaga migracji wszystkich systemów bankowych do chmury. Kluczowe dla banku systemy mogą nadal mieścić się w data center banku lub w kolokacji, a pozostałe w chmurze.

W każdym wariancie usług cloud computing – w chmurze prywatnej, współdzielonej oraz hybrydowej – korzystać z niej można w trzech modelach:

- IaaS – *Infrastructure as a Service* – usługa polega na udostępnieniu samej mocy obliczeniowej, która obejmuje w szczególności moc procesora, pamięć RAM i pamięć dyskową;
- PaaS – *Platform as a Service* – usługa polega na udostępnieniu mocy obliczeniowej oraz platform systemowych, w tym przykładowo systemu operacyjnego lub silnika bazy danych;
- SaaS – *Software as a Service* – najbardziej zaawansowana usługa polegająca na udostępnieniu konkretnej aplikacji – po stronie dostawcy jest zapewnienie wszystkich komponentów sprzętowych oraz oprogramowania niezbędnych do jej udostepnienia.

Niezależnie od wybranego modelu, **w przypadku banków istotne jest, aby usługi chmurowe zawsze świadczone były z konkretnego, znanego bankowi data center, a ośrodek ten spełniał wszystkie normy wskazane przez regulatora.**

Dzisiaj banki mają wiele możliwości w zakresie korzystania z zewnętrznych data center. Mogą do nich przenieść zarówno swoje podstawowe centrum przetwarzania danych, rezygnując z modelu *on-premise*, jak i jedynie ośrodek zapasowy, podstawowy nadal zachowując u siebie. Mogą również przenieść tylko część procesów pomocniczych do chmury, poprawiając swoją efektywność.

CZYM POWINIEN SIĘ CHARAKTERYZOWAĆ DOSTAWCA USŁUG DATA CENTER I CLOUD COMPUTING DLA BANKU?

Do niedawna brak wyraźnych wytycznych dotyczących wykorzystania zewnętrznych data center i usług chmurowych w bankowych procesach przetwarzania danych, powodował sceptyczne podejście do korzystania z tego typu usług. W ostatnim czasie pojawiły się jednak regulacje dotyczące przetwarzania danych w data center z uwzględnieniem przetwarzania w chmurze. Są to m.in. „Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach" Komisji Nadzoru Finansowego, Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa", „Komunikat Urzędu Komisji Nadzoru Finansowego z dnia 23 stycznia 2020 roku dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej" oraz „Standard wdrożeń przetwarzania informacji w chmurze obliczeniowej" opracowany przez Związek Banków Polskich.

W przywołanych rekomendacjach i standardach wskazano kilka elementów kluczowych dla wyboru odpowiedniego dostawcy usług data center i cloud computing. Zgodnie z zaleceniami KNF bank powinien przechowywać i przetwarzać dane na terenie Europejskiego Obszaru Gospodarczego, przy czym w pierwszej kolejności powinien wybrać centrum przetwarzania danych na terenie Polski. Kolejne wytyczne doprecyzowują nie tylko miejsce przetwarzania danych, ale i szeroko pojęte standardy bezpieczeństwa. **We wszystkich dokumentach zaleca się korzystanie z ośrodków data center spełniających wymagania normy EN 50600.**

Obecnie seria norm EN 50600 uważana jest za najbardziej kompleksową i wymagającą normę w Europie, przyjętą do stosowania w państwach członkowskich Unii Europejskiej. Mieszczące się w Poznaniu i we Wrocławiu **centra przetwarzania danych firmy Talex jako jedyne w Polsce posiadają certyfikat potwierdzający spełnianie rygorystycznych wymogów normy EN 50600** na najwyższym zdefiniowanym w nich poziomie, we wszystkich obszarach, tj. dostępności – klasa 4 (najwyższa), bezpieczeństwa fizycznego – klasa 4 (najwyższa), efektywności energetycznej – poziom 3 (najwyższy). Warto wspomnieć, że KNF rekomenduje wybór dostawcy usług data center spełniającego wymagania normy EN 50600 minimum klasy 3, co oznacza, że Talex gwarantuje jeszcze większe bezpieczeństwo i niezawodność (EN 50600 klasy 4).

CO W PRAKTYCE OZNACZA SPEŁNIANIE WYMOGÓW NORMY EN 50600?

Spełnienie wymogów normy EN 50600 przez określone data center obejmuje wiele aspektów – od jego lokalizacji i projektu architektonicznego, przez konstrukcję i wyposażenie, po jego utrzymanie i zabezpieczenie. Najlepiej przedstawić to na przykładzie data center spółki Talex, która jest dostawcą usług data center i cloud computing dla banków. Jako jedyna w Polsce posiada centra przetwarzania danych z certyfikatem EN 50600. Położone są w oddalonych od siebie o 200 km, bezpiecznych lokalizacjach wolnych od zagrożeń środowiskowych w Poznaniu i we Wrocławiu. Wszystkie elementy data center, czyli infrastruktura fizyczna, rozwiązania techniczne i systemowe, procedury operacyjne i oferowane usługi są zdublowane w obu ośrodkach. Jednocześnie oba data center są ze sobą połączone i zarządzane tak, by mogły stanowić jeden spójny organizm. Dzięki takiemu podejściu, firma może skutecznie reagować w przypadku wystąpienia nieprzewidzianych zdarzeń, utrzymując wymagany poziom usług, w szczególności funkcji o znaczeniu krytycznym. Wszystkie urządzenia wspierające pracę Talex data center zostały dostarczone i zainstalowane przez światowych liderów oferujących najnowsze rozwiązania technologiczne. Oba ośrodki są neutralne telekomunikacyjnie, co pozwala na podłączenie do wszystkich większych operatorów telekomunikacyjnych. W każdym z ośrodków światłowody operatorów doprowadzono różnymi drogami do dwóch niezależnych pomieszczeń *meet-me-room*, które stanowią punkt styku operatorów telekomunikacyjnych oraz infrastruktury teletechnicznej data center. Oba ośrodki zaliczają się także do tzw. *green data centers*. Zostały zaprojektowane i zbudowane z wykorzystaniem najnowszych technologii energooszczędnych.

W data center firmy Talex wdrożony został system zarządzania ciągłością biznesu. Składają się na niego

plany zachowania ciągłości działania na wypadek lokalnych kataklizmów, masowych awarii sprzętu, masowej niedostępności pracowników, długotrwałego braku dostaw prądu i innych mediów, braku dostępu do usług telekomunikacyjnych i innych sytuacji kryzysowych. Wdrożona polityka zachowania ciągłości działania zakłada także przeprowadzanie okresowych ćwiczeń i testów – wszystkie są odpowiednio dokumentowane. System zarządzania ciągłością działania jest w pełni zgodny z wymogami normy ISO 22301. Oba centra przetwarzania danych są obsługiwane przez dedykowane zespoły specjalistów dyżurujących na miejscu w trybie 24/7 i monitorujących na bieżąco parametry środowiskowe.

Oba ośrodki data center firmy Talex zapewniają bezpieczeństwo na wielu poziomach, począwszy od lokalizacji budynków, ich architektury i budowy, a kończąc na bezpieczeństwie energetycznym oraz bezpieczeństwie fizycznym.

Bezpieczna lokalizacja data center

- w miejscu o małym natężeniu ruchu komunikacyjnego, jednocześnie z zapewnieniem wygodnego dojazdu;
- poza centrum miasta;
- z dala od obiektów mogących generować zagrożenie, np. instytucji finansowych (napady), zakładów chemicznych, stadionów sportowych;
- poza korytarzami powietrznymi komunikacji lotniczej;
- na terenie odpowiednio odwodnionym;
- z dala od środowiskowych zagrożeń (powodzie, osuwiska, itp.);
- rozproszone rozmieszczenie zasobów (serwerownie w różnych budynkach);

Bezpieczna konstrukcja data center

- konstrukcja żelbetowa z elementami hydrobetonu;
- układ sejfu – wewnątrz głównej strefy przetwarzania umieszczone są dedykowane poszczególnym klientom kapsuły o godzinnej odporności ogniowej;
- dedykowany, redundantny system klimatyzacji dla każdej wydzielonej strefy przetwarzania (kapsuły);
- technologia zamkniętych zimnych korytarzy zwiększająca wydajność systemu klimatyzacji;
- innowacyjna technologia freecoolingu umożliwiająca wykorzystanie niskiej temperatury zewnętrznej do schłodzenia wnętrza strefy przetwarzania;

Bezpieczeństwo energetyczne data center

- dwie niezależne linie zasilające średniego napięcia (SN);
- dwie stacje transformatorowe;
- dwie dwusekcyjne rozdzielnie elektryczne z układem sprzęgającym (awaria jednej linii SN, jednej stacji transformatorowej powoduje przełączenie odbiorników na drugą linię SN);
- dwa zestawy zasilaczy UPS dla każdego toru zasilania, każdy w układzie nadmiarowym (N+1), pozwalające utrzymać rygorystyczne parametry zasilania podczas przełączania między źródłami zasilania;
- dwa układy agregatów prądotwórczych wyposażone w system umożliwiający tankowanie w trakcie działania;

Bezpieczeństwo fizyczne data center

- zaawansowana kontrola elektroniczna obejmująca m.in. biometryczną kontrolę dostępu;
- niezależna kontrola dostępu do kapsuł dedykowanych dla poszczególnych klientów;
- system telewizji przemysłowej CCTV,
- system sygnalizacji włamania i napadu oraz sprawdzania statusu drzwi;
- niezależne łącza telekomunikacyjne;
- dedykowany dla każdej kapsuły system gaszenia gazem;
- możliwość instalacji własnych elektronicznych systemów bezpieczeństwa
- całodobowa ochrona fizyczna;

Wykorzystywane w data center procesy zostały wypracowane przez firmę Talex w trakcie ponad 30-letniej współpracy z klientami z sektora finansowego. Aby zapewnić szeroki wachlarz usług data center – od kolokacji po różnego rodzaju rozwiązania cloud computing (chmura prywatna, współdzielona, hybrydowa) – i świadczyć je na najwyższym poziomie, Talex wykorzystuje swoje multidyscyplinarne kompetencje i ogromne doświadczenie. Stanowi to dużą wartość dla klientów zarówno na etapie planowania usługi (analiza potrzeb klienta, rozpoznanie technologii, dobór najlepszego rozwiązania technologicznego oraz jego zaprojektowanie), jak i jej wdrożenia (implementacja opracowanego rozwiązania), a następnie migracji środowiska klienta. Na potrzeby obsługi klientów już korzystających z usług kolokacji w data center lub cloud computing, Talex zaadaptował sprawdzone przez siebie procesy w pełni zgodne z międzynarodowymi normami ISO, m.in. ISO 20000, ISO 27001, ISO 18295.

PODSUMOWANIE

Dla banków zapewnienie bezpieczeństwa danych oraz ciągłości działania jest kluczowe, a jednocześnie nie stanowi podstawowej działalności. Mało prawdopodobne jest, aby bank mógł we własnych ośrodkach data center (zarówno w podstawowym, jak i w zapasowym) spełnić wymogi norm bezpieczeństwa w takim stopniu, jak firmy zewnętrzne specjalizujące się w tym zakresie. Skorzystanie z usług renomowanego, posiadającego stosowny certyfikat data center jest dzisiaj bardzo dobrym rozwiązaniem. Z jednej strony gwarantuje najwyższe bezpieczeństwo i przenosi odpowiedzialność na dostawcę, a z drugiej strony jest najlepszym rozwiązaniem pod względem ekonomicznym, gdyż eliminuje konieczności ponoszenia wydatków na inwestycje (CAPEX), a za usługę płaci się w ramach okresowych opłat (OPEX).

Obecnie najpopularniejszym rozwiązaniem udostępnianym przez zewnętrznych dostawców data center jest usługa kolokacji. Budzi ona najmniej obaw co do bezpieczeństwa danych i wiele instytucji myśląc dziś o outsourcingu, nadal koncentruje się na kolokacji, pomijając inne dostępne i warte uwagi alternatywy. Dzisiaj dostawcy usług data center oferują o wiele więcej i kolokacja może być zaledwie pierwszym krokiem w kierunku outsourcingu, który część polskich banków ma już za sobą. Światowe trendy pokazują, że banki poszukują nowych rozwiązań pozwalających optymalizować koszty i zapewniających skalowalność oraz zwiększenie operacyjnej efektywności. Niektóre z nich całkowicie zrezygnowały z własnego data center i wszystkie procesy przeniosły do chmury.

Dzisiaj przewagą może stać się korzystanie z infrastruktury, dzięki której banki będą mogły sprawniej prowadzić projekty

Opinia eksperta

dr Jacek Truszkowski
Prezes Truszkowski Consulting Group

Doradzając strategicznie instytucjom finansowym widzimy, że bezpowrotnie minęły czasy, gdy banki konkurowały między sobą wyłącznie na poziomie oferty. Dzisiaj klienci często wybierają dany bank ze względu na możliwości, jakie oferuje jego platforma bankowości elektronicznej. Wykorzystanie przez bank chmury pozwala szybciej reagować na zmiany w otoczeniu konkurencyjnym i sprawnie wprowadzać nowe rozwiązania technologiczne.

i szybciej wdrażać nowe biznesowe rozwiązania. Usługi outsourcingowe cały czas ewoluują i także banki powoli widzą korzyści z oddawania części swoich procesów na zewnątrz.

Instytucje finansowe muszą jednak spełniać szereg wymogów nakładanych przez regulatora i audyty, szczególnie w zakresie bezpieczeństwa. Zatem nie każde rozwiązanie chmurowe będzie stanowiło dla nich interesującą alternatywę. Należy zatem rozważyć, który model współpracy i który dostawca usług cloud computing będzie dla banku najlepszy.

CASE STUDY

Data center firmy Talex rozwiązaniem dla instytucji finansowych

WYZWANIE

Jeden z większych działających w Polsce banków komercyjnych posiadał własne centra przetwarzania danych (data center). Dynamicznie zmieniające się otoczenie rynkowe, rosnące wymogi regulacyjne i chęć korzystania z najnowszych rozwiązań technologicznych skłoniły bank do rozważenia budowy nowych ośrodków data center. Po szczegółowej analizie okazało się jednak, że budowa własnych centrów przetwarzania danych wiązałaby się z poniesieniem bardzo wysokich nakładów inwestycyjnych (CAPEX), a dodatkowo zajęłaby dużo czasu.

ROZWIĄZANIE

Rozwiązaniem pozbawionym wskazanych wyżej wad było, coraz popularniejsze w branży bankowej na świecie, wykorzystanie powierzchni w profesjonalnym data center spełniającym stosowne normy i wymagania regulatora rynku. Ostatecznie bank podjął decyzję o przeniesieniu swojego sprzętu do cata center firmy Talex.

Chcąc ograniczyć ewentualne ryzyko związane ze zmianą wykorzystywanego wcześniej modelu działania w zakresie IT, bank podjął decyzję o przeniesieniu w pierwszym kroku jednego ze swoich centrów przetwarzania danych do data center firmy Talex. W tym celu opracowany został szczegółowy plan, obejmujący nie tylko relokację posiadanych zasobów, ale także optymalizację środowiska IT poprzez zastąpienie części infrastruktury rozwiązaniami najnowszej generacji. Ponieważ cały proces przeniesienia i uruchomienia nowego ośrodka był drobiazgowo zaplanowany i odbywał się etapami, w żaden sposób nie wpłynął on na działalność operacyjną banku.

Po przeniesieniu swojego centrum danych, bank cyklicznie przeprowadzał audyty weryfikujące jakość świadczonej usługi. Ich wyniki potwierdziły spełnienie przez data center firmy Talex wysokich standardów i wymagań stawianych przez bank i regulatorów.

Dzięki temu w kolejnym etapie bank zdecydował się na poszerzenie zakresu współpracy ze spółką Talex. W drugim kroku przeniósł swoje kolejne centrum przetwarzania danych do drugiego ośrodka tej firmy. Podobnie, jak przy pierwszej relokacji, przygotowany został plan stopniowego przenoszenia zasobów IT do nowej lokalizacji. Duże doświadczenie oraz kompetencje zespołu firmy Talex pozwoliły na kompletną relokację infrastruktury z zachowaniem pełnej ciągłości działania banku.

KORZYŚCI DLA BANKU

Od wielu lat urządzenia banku działają nieprzerwanie w data center spółki Talex. Oba centra danych, zgodnie z rekomendacją KNF, posiadają certyfikaty EN 50600 i zostały zbudowane z dala od zagrożeń środowiskowych. W obu ośrodkach bank korzysta z dedykowanej powierzchni całkowicie odseparowanej od pozostałych przestrzeni data center. Kapsuły zabezpieczono niezależnymi układami chłodzenia i gaszenia. Dane są bezpieczne, a bank nie musiał ponosić dużych kosztów inwestycji na budowę własnej, nowej infrastruktury. Odpowiedzialność za nieprzerwane działanie data center została przeniesiona z banku na firmę Talex.