

PKO Bank Polski inwestuje w mobilną przyszłość

Artur Król

Bank PKO BP jest jednym z pierwszych w Polsce, który zdecydował się na masowe wdrożenie mobilnej floty smartfonów, zarządzanych z poziomu zaawansowanego systemu klasy MDM (*Mobile Device Management*).

Systemy mobilne stają się nieodzowną częścią infrastruktury informatycznej dużych firm i korporacji. Znaczna liczba pracowników, niezadko rozbudowana sieć zdalnych oddziałów, niemal wymusza zastosowanie rozwiązań ułatwiających realizację kluczowych potrzeb, związanych np. z szybką wymianą informacji, wspierających obieg dokumentów, pocztę elektroniczną itp. Nieodzowne stają się systemy mobilne, gwarantujące wysoki poziom bezpieczeństwa przy odpowiednio miarodajnym poziomie wydajności. I funkcjonalności infrastruktury IT.

Jeszcze w październiku ubiegłego roku PKO Bank Polski zdecydował się na wymianę posiadanej floty urządzeń BlackBerry na smartfony Lumia, sygnowane przez Microsoft. Obecnie pracownicy banku posiadają 2500 urządzeń tej marki. Skąd taki wybór? – Wybraliśmy Microsoft Lumia, ponieważ PKO Bank Polski ściśle współpracował z firmą Microsoft nad dostosowaniem modelu Lumii do potrzeb naszej organizacji. Najważniejsze dla banku były kwestie bezpieczeństwa, dlatego niektóre z funkcji zostały wyłączone, np. czytniki SD – odpowiada Andrzej Leszczyński, dyrektor Pionu Eksploatacji i Infrastruktury w PKO BP.

Należy jednak dodać, że bank korzystał z infrastruktury Microsoft już wcześniej, tak więc wybór tej właśnie platformy nie był przypadkowy. Większość firm decyduje się obecnie na jednolitą infrastrukturę informatyczną, ponieważ taka umożliwia zachowanie wielu korzyści, unifikację oprogramowania, jednolitość stosowanych narzędzi do zarządzania oraz bezpieczeństwa. Podobne cele stawia sobie PKO BP, który w utworzeniu jednego, kompleksowego rozwiązania CRM dostępnego na wszystkie typy urządzeń (komputer, tablet, telefon) upatruje korzyści, tj. podniesienia jakości obsługi, skrócenia dystansu do klienta i zwiększenia efektywności sprzedaży. Podejście takie jest również korzystne ze względu na optymalizację procesów i kosztów utrzymania całego środowiska teleinformatycznego. Od samego początku zakładano, że wdrożenie rozwiąże kluczowe potrzeby banku – zdalny dostęp do zasobów informacyjnych, dostęp do e-maili czy pracę grupową. Bardzo ważne były kwestie bezpieczeństwa, w tym możliwość zdalnego usuwania zawartości danych z mobilnego urządzenia. Istotę przedsięwzięcia stanowiło bowiem zachowanie

pełnej kontroli nad przekazanymi zdalnie danymi, które można w dowolnym momencie zaszyfrować czy usunąć. Każdorazowy dostęp do zasobów firmowych banku wymaga podania loginu i hasła. W przypadku kradzieży lub zagubienia aparatu wymiana kary SIM powoduje natychmiastowy reset urządzenia i wyczyszczenie pamięci.

Lumia pod baczny okiem banku

Bank miał szczególne wymagania, dlatego też dostarczone smartfony zostały wręcz uszyte na miarę. Dla zapewnienia najwyższego możliwego poziomu bezpieczeństwa wprowadzono rozwiązania ograniczające do minimum możliwości nieautoryzowanego dostępu do danych czy wycieku informacji, zablokowano możliwość stosowania kart Dual SIM, zablokowano korzystanie z kart SD. Przedstawiciele banku byli głównymi testerami nowych smartfonów Nokii dostosowanych do wymogów stawianych przez duże korporacje. Zanim jednak zapadła ostateczna decyzja zastanawiano się nad przyjęciem innych rozwiązań.

– Rozważaliśmy platformy iOS, Android, BlackBerry i Windows Phone. Po przeanalizowaniu kosztów i możliwości, PKO Bank Polski zdecydował się na telefon z systemem operacyjnym Microsoftu. Jedną z jego zalet jest inter-

fejs kafelkowy na telefonie i komputerach osobistych. W dalszej perspektywie bank planuje wprowadzenie tabletów, korzystających z tego samego oprogramowania – dodaje Andrzej Leszczyński:

Platforma iOS jest najczęściej wybieranym rozwiązaniem w przypadku dużych firm i korporacji, a to ze względu na jej hermetyczność i bardzo wysokiej klasy zabezpieczenia. W systemach Windows wykorzystywanych w PKO BP dodatkowo zastosowano oddzielny system zarządzania mobilną flotą MDM (*Mobile Device Management*) firmy AirWatch. Pozwoliło to na stworzenie własnego sklepu Windows Store, w którym przechowywane są aplikacje dozwolone przez bank do instalacji na telefonach pracowników. MDM – podpięty do rozwiązania typu SIEM (*Security Information and Event Management*) – raportuje próby niedozwolonych działań. Zastosowanie systemu MDM wyeliminowało konieczność stosowania rozwiązań VPN do zdalnego łączenia się z siecią przedsiębiorstwa. Uwierzytelnienie połączenia z bankiem odbywa się poprzez przyznane użytkownikom certyfikaty oraz konta domenowe. Systemy MDM zaczynają ogrywać podstawową rolę wszędzie tam, gdzie serio rozważane jest wdrożenie licznych mobilnych urządzeń. *Mobile Device Management* jest wspólnym obszarem dla administracji



Foto: Fotolia.com

i nadzoru, bezpieczeństwa, monitorowania oraz integracji dla urządzeń mobilnych – smartfonów, tabletów, komputerów przenośnych. Zadaniem tych systemów jest optymalizacja funkcjonalności i bezpieczeństwa urządzeń mobilnych w przedsiębiorstwie i jednocześnie ochrona sieci firmowej. W dobrze przygotowanym środowisku narzędzia MDM realizują funkcje zarządzania aplikacjami, zapewniają synchronizację plików i udostępnianie danych, gwarantują bezpieczeństwo oraz wsparcie dla urządzeń należących do firmy, ale także i dla tych, które są własnością prywatną pracowników. Za sprawą trendu BYOD (*Bring Your Own Device* – wykorzystywanie prywatnych smartfonów, tabletów czy komputerów, również stacjonarnych, do celów komunikacji z siecią firmową) o systemach MDM mówi się w szerszym kontekście zarządzania całą mobil-

nością firmy – EMM (*Enterprise Mobility Management*).

Celem była praca grupowa

W przypadku instytucji finansowych, gdzie szczególnie istotna jest szybka wymiana informacji, stosowane są rozwiązania pozwalające na wykorzystanie wielu kanałów komunikacji do interakcji z klientami. Szybkość wymiany informacji jest tutaj podstawą, jest to istotne również ze względu na konieczność sprostania ostrej rywalizacji konkurencyjnej. Nic więc dziwnego, że instytucje finansowe szczególnie chętnie inwestują obecnie w systemy mobilne, jako najbardziej rozwojowe.

– Na obecnym etapie pracownicy mają dostęp do poczty korporacyjnej, odpowiednio przydzielonych zasobów firmowych oraz aplikacji systemu płatności mobilnych IKO – mówi Andrzej Leszczyński.

Bank myśli o rozbudowie w przyszłości systemu o kolejne funk-

cjonalności, a pozwala mu na to otwarta architektura samego rozwiązania. PKO BP korzysta m.in. z pakietu biurowego Office 365, który jest rozwiązaniem przystosowanym do pracy w tzw. chmurze i zapewnia łatwe zdalne udostępnianie lub współdzielenie plików. Dzięki temu możliwe jest wdrożenie zaawansowanych mechanizmów pracy grupowej. PKO BP testuje też komunikator Lync na komputerach stacjonarnych. Jest to – zdaniem jego przedstawicieli – bardzo użyteczne rozwiązanie ze względu na fakt, że wiadomo, kiedy dany pracownik jest przy biurku (funkcja Lync Presence); a jeśli go akurat przy nim nie ma, można wówczas „wydzwonić” go za pomocą Lync. Po fazie testów zostanie on zapewne zainstalowany także na smartfonach Lumia. Każde rozwiązanie musi jednak przede wszystkim przynieść swojej organizacji realne korzyści. Zdaniem Andrzeja Leszczyń-

skiego, chodzi przede wszystkim o zwiększenie efektywności pracy działów IT i osób odpowiedzialnych za ciągłość procesów bankowych. Pracownicy mają dostęp do poczty firmowej i specjalnie przygotowanej wersji sklepu Windows Store, dzięki czemu stali się mobilni i mogą pracować w różnych miejscach. Warto podkreślić, że urządzenia są bezpieczne – telefon w stanie spoczynku automatycznie się blokuje. Oprogramowanie AirWatch umożliwiło sprawne wdrożenie i zarządzanie nowoczesnymi urządzeniami mobilnymi w technologii Microsoft Windows Phone. Dzięki niemu pracownicy banku zyskali możliwość prezentacji klientom aplikacji do płatności mobilnych, dostępu do konta bankowego za pomocą IKO oraz do zasobów korporacyjnych. Udostępnienie poczty korporacyjnej na urządzeniach, które nie posiadają rozwiązania takiego jak AirWatch, jest bardzo ryzykowne. ■