Quest Dystrybucja
Dystrybutor Dell Software w Polsce

Case study
06.2014

Zwiększenie bezpieczeństwa IT i dostępności aplikacji w Banku BGŻ

Bank BGŻ jest uniwersalnym bankiem komercyjnym, z blisko 100-letnią tradycją. Od lat zajmuje miejsce w czołówce największych banków w Polsce. Oferta produktowa banku to zarówno rozwiązania dla sektora rolno-spożywczego (rachunki, finansowanie działalności, ubezpieczenia, leasing), jak i dla klientów indywidualnych oraz przedsiębiorców. Klienci banku mają do dyspozycji sieć blisko 400 oddziałów w całym kraju. Z usług banku można korzystać również za pomocą nowoczesnych i wygodnych rozwiązań bankowości elektronicznej m.in. bankowości mobilnej eBGŻ Lite, systemu bankowości internetowej eBGŻ, obsługi telefonicznej TeleBGŻ oraz Home Banking. Dostęp do tych usług odbywa się poprzez zaawansowane technologie informatyczne.

Bardzo ważnym elementem środowiska informatycznego w Banku BGŻ jest Active Directory (AD). Usługa AD stanowi centralny punkt uwierzytelniania, bazę danych zasobów sieciowych i użytkowników. Poprawne działanie AD wpływa na dostępność najważniejszych aplikacji wspierających główne funkcje i procesy biznesowe oraz inne usługi w Banku BGŻ. Dlatego zapewnienie właściwej dostępności, wydajności, bezpieczeństwa oraz stabilności AD ma istotny wpływ na funkcjonowanie całego Banku.

Obszary podlegające usprawnieniom

Szczegółowa kontrola bezpieczeństwa i monitorowanie zmian w bardzo rozbudowanej infrastrukturze IT były znacznie ograniczone. Zadania te bardzo obciążały administratorów IT i zajmowały im dużo czasu. Potencjalne błędy administracyjne lub awarie stanowiły duże zagrożenie dla ciągłości działania AD i bezpieczeństwa Banku. Niezwykle istotne jest również zapewnienie zgodności z odpowiednimi zewnętrznymi i wewnętrznymi regulacjami, w tym z rekomendacjami Komisji Nadzoru Finansowego (KNF). Brak lub nieodpowiednie mechanizmy zabezpieczania i monitorowania bezpieczeństwa mogłyby spowodować istotne naruszenie polityk bezpieczeństwa. Standardowe narzędzia dostarczane z systemami operacyjnymi nie zapewniały kompleksowego podglądu wszystkich zmian i logów zdarzeń, które były rozproszone w wielu lokalizacjach i formatach. Administratorzy nie dysponowali także szczegółowym wglądem w dane na temat bezpieczeństwa środowiska IT, co pozwoliłoby im podjąć proaktywne działania w przypadku naruszenia polityki bezpieczeństwa. Ponadto monitorowanie zdarzeń logowania i raportowanie zmian było konieczne do spełnienia wymogów audytorów i ładu korporacyjnego.

„Active Directory to krytyczny i bardzo istotny, jeżeli nie najważniejszy element infrastruktury IT w Banku BGŻ. Wykonywanie zadań związanych z monitorowaniem

„Szybka instalacja, prosta i intuicyjna obsługa w przejrzystej konsoli graficznej, a przede wszystkim ogromna funkcjonalność i elastyczność tych rozwiązań zaskakiwały nas pozytywnie od samego początku." - Janusz Bogusz, zastępca Kierownika Wydziału Zarządzania Systemami w Banku BGŻ.

Opis

Bank BGŻ jest uniwersalnym bankiem komercyjnym, od lat zajmującym miejsce w czołówce największych banków w Polsce. Dysponuje siecią blisko 400 oddziałów i zatrudnia ponad 5 tys. osób.

Korzyści

- Poprawa kontroli i zwiększenie bezpieczeństwa środowiska IT
- Zautomatyzowanie i usprawnienie zarządzania środowiskiem AD
- Zapewnienie ciągłości działania, monitorowania i diagnostyki AD
- Spełnienie wymagań zewnętrznych regulacji i wewnętrznych polityk

Rozwiązania

- InTrust Enterprise Edition
- Change Auditor for Active Directory Suite:
  - Change Auditor for AD
  - Change Auditor for LDAP
  - Change Auditor for Windows File Server
- Availability Suite for Active Directory:
  - Recovery Manager for AD
  - Spotlight on AD

i analizowaniem środowiska AD zajmowało administratorom dużo czasu. Tworzone przez nich raporty często nie były wystarczająco szczegółowe i dokładne. Bez odpowiednich, dodatkowych narzędzi informatycznych bardzo trudno było też przewidywać i wykrywać pojawiające się problemy. Dlatego konieczne było jak najszybsze zautomatyzowanie i uproszczenie czynności związanych ze śledzeniem zmian i raportowaniem środowiska AD.

Potrzebne do tego były rozwiązania, które ułatwiłyby analizy i audyt dużej ilości informacji zawartych w logach systemowych oraz wpłynęłyby na poprawę kontroli bezpieczeństwa środowiska IT." - powiedział Tadeusz Rubin - Dyrektor Departamentu Operacji IT w Banku BGŻ.

Rozwiązania Dell Software

Konieczność spełnienia wymagań zewnętrznych regulacji oraz wewnętrznych polityk, a przede wszystkim zapewnienia ciągłości działania, monitorowania i diagnostyki AD zdecydowała o zakupie i wdrożeniu dodatkowych rozwiązań. We wrześniu 2011 Bank BGŻ zakupił pakiet zintegrowanych narzędzi firmy Dell Software: **InTrust Enterprise Edition**, **ChangeAuditor for Active Directory Suite** oraz **Availability Suite for Active Directory**. Wdrożenie oprogramowania trwało 5 dni i objęło: 10 kontrolerów domeny na systemie Windows 2008, 4 serwery plików Windows 2008 oraz 7700 aktywnych kont AD.

„Decyzję o wyborze odpowiednich rozwiązań informatycznych poprzedziła dokładna analiza naszych potrzeb. Zależało nam na tym, żeby wdrożone oprogramowanie zapewniło właściwą dostępność, wydajność, stabilność oraz bezpieczeństwo AD także w dalszej perspektywie czasu. Szukaliśmy rozwiązań, które mogłyby być niezależne od pozostałej infrastruktury IT i miały niewielkie wymagania systemowe. Nasze oczekiwania spełniła firma Quest Dystrybucja i zaproponowane przez nią rozwiązania Dell Software. Szybka instalacja, prosta i intuicyjna obsługa w przejrzystej konsoli graficznej, a przede wszystkim ogromna funkcjonalność i elastyczność tych rozwiązań zaskakiwały nas pozytywnie od samego początku." - Janusz Bogusz - zastępca Kierownika Wydziału Zarządzania Systemami w Banku BGŻ.

Monitorowanie logów

Wdrożone w Banku BGŻ rozwiązanie **InTrust** pozwoliło na wprowadzenie w czasie rzeczywistym monitoringu środowiska AD. **InTrust** dostarcza informacje niezbędne do zapewnienia bezpieczeństwa środowiska IT w Banku i pozwala spełnić wymagania zewnętrznych regulacji oraz wewnętrznych polityk. Umożliwia kolekcjonowanie, przechowywanie i przeglądanie informacji zawartych w logach systemowych. Wykrywa również nietypowe sytuacje mogące naruszać bezpieczeństwo AD i natychmiast powiadamia administratorów IT o nienaturalnych zachowaniach użytkowników, takich jak próba dostępu do danych poza godzinami pracy, nieudane próby logowania, wielokrotne nieudane próby zmiany hasła oraz o innych wydarzeniach, krytycznych z punktu widzenia bezpieczeństwa Banku. Rozwiązanie **InTrust** pozwala także na generowanie raportów na podstawie zebranych logów oraz umożliwia pełny audyt i wewnętrzną kontrolę nad środowiskiem IT, m.in. poprzez monitorowanie dostępu do krytycznych danych systemu oraz śledzenie nadawania dostępu i jego wykorzystywania przez użytkowników.

Audyt zmian AD i Windows

Uwierzytelnianie logowania i autoryzacja użytkowników w Banku BGŻ odbywa się w oparciu o Microsoft Active Directory. Zakup i wdrożenie pakietu **ChangeAuditor for Active Directory Suite** (**ChangeAuditor for AD**, **ChangeAuditor for LDAP**, **ChangeAuditor for Windows File Servers**) pozwoliło stworzyć infrastrukturę

całkowicie niezależną od Microsoft, umożliwiającą monitorowanie zmian zachodzących w Active Directory oraz Windows File System i ochronę krytycznych obiektów.

Rozwiązanie **ChangeAuditor** zapewnia śledzenie i audyt zmian w czasie rzeczywistym dla AD, LDAP, serwerów plików Windows, rejestrów systemowych, usług, lokalnych grup i użytkowników. Za pomocą prostej w obsłudze centralnej konsoli do zarządzania, administratorzy IT mogą przeglądać logi zmian i filtrować widoki według atrybutów (użytkownik, komputer, czas i typ zdarzenia). Dzięki temu możliwe jest szybkie wykrywanie problemów i lokalizowanie ich źródła.

ChangeAuditor for Active Directory zapewnia szczegółowe śledzenie w czasie rzeczywistym ustawień AD i Group Policy. Pozwala na natychmiastowe powiadomienie o naruszeniu procedur bezpieczeństwa i umożliwia podjęcie odpowiedniej akcji zapobiegającej niepożądanym zmianom AD. Zapewnia także zgodność z regulacjami zewnętrznymi poprzez śledzenie aktywności w środowisku AD, zmian w konfiguracji AD, schemacie oraz DNS. Rozwiązanie umożliwia tworzenie szczegółowych raportów na temat aktywności użytkowników, wdrożonych polityk bezpieczeństwa i innych wymogów audytu. Dodatkowo, rozwiązanie **ChangeAuditor for Windows File Server** zapewnia inspekcję dostępu do plików i folderów. Pozwala na zbieranie i raportowanie informacji o utworzeniu pliku, zmianie nazwy, uprawnień, przeniesieniu czy skasowaniu. Tym samym pomaga zwiększyć bezpieczeństwo i kontrolę compliance dla serwerów plików Windows. Dzięki rozwiązaniu **ChangeAuditor** administratorzy mogą natychmiast reagować na zdarzenia i nieprawidłowości, zapewniając ochronę krytycznych danych przed wprowadzeniem przypadkowych lub niedozwolonych zmian. Wpływa to na poprawę kontroli i zwiększenie bezpieczeństwa środowiska IT w Banku BGŻ oraz pozwala spełnić wymagania i regulacje (compliance).

Bezpieczne zarządzanie środowiskiem AD

Dodatkowo Bank BGŻ wdrożył pakiet **Availability Suite for Active Directory**, który obejmuje dwa rozwiązania: **Recovery Manager for Active Directory** oraz **Spotlight on Active Directory**. Narzędzia te pozwoliły zwiększyć funkcjonalność zarządzania środowiskiem AD, zapewniając ciągłość działania, niezawodność i diagnostykę AD.

Recovery Manager for Active Directory zapewnia zautomatyzowany backup, archiwizację i szybkie odtwarzanie (w kilka minut!) utraconych obiektów i atrybutów w trybie online. Może przywrócić każdy, przypadkowo skasowany lub zmieniony obiekt AD. Dzięki **Recovery Manager for AD** użytkownicy mają zapewniony ciągły i niezakłócony dostęp do zasobów AD nawet w czasie procesu przeprowadzania backupu czy odtwarzania danych. Rozwiązanie wpływa także na przyspieszenie i usprawnienie przeprowadzania backupu środowiska AD, zapewniając przy tym ciągłą dostępność bieżących danych oraz możliwość współpracy z istniejącą już w banku infrastrukturą tworzącą kopie bezpieczeństwa.

Rozwiązanie **Spotlight on Active Directory** umożliwia szczegółową analizę i diagnostykę środowiska AD w czasie rzeczywistym. Zapewnia wgląd we wszystkie procesy i komponenty środowiska AD. Administratorzy mogą teraz proaktywnie wykrywać przyczyny powstawania problemów związanych z replikacją, wydajnością, synchronizacją czy dostępnością. Pozwala administratorom na szybkie wykrywanie i rozwiązywanie problemów wydajnościowych zanim wpłyną na pracę użytkowników i procesy biznesowe w Banku BGŻ.

Efekty

Rozwiązania Dell Software w krótkim czasie od wdrożenia wpłynęły na poprawę kontroli bezpieczeństwa środowiska IT w Banku BGŻ. W krótkim czasie udało się zautomatyzować

i uprościć czynności związane ze śledzeniem zmian. Analiza i audyt dużej ilości informacji zawartych w logach systemowych stały się łatwiejsze, a czynności te zajmują administratorom mniej czasu. Ponadto szczegółowy wgląd w dane na temat bezpieczeństwa środowiska IT pozwala podjąć proaktywne działania w przypadku naruszenia polityki bezpieczeństwa. Wdrożone rozwiązania przyczyniły się do zapewnienia ciągłości działania i pełnej diagnostyki AD, spełnienia wymagań zewnętrznych regulacji oraz wewnętrznych polityk oraz przede wszystkim wpłynęły na zwiększenie bezpieczeństwa

---

Bank BGŻ jest uniwersalnym bankiem komercyjnym, od lat zajmującym miejsce w czołówce największych banków w Polsce. Specjalizuje się w finansowaniu rolnictwa, gospodarki żywnościowej oraz infrastruktury regionalnej. Bank dysponuje siecią blisko 400 oddziałów i zatrudnia ponad 5 tys. osób. W 2013 roku Grupa Banku BGŻ wypracowała zysk netto w wysokości 160,1 mln zł, co oznacza wzrost o 23% w porównaniu z 2012 rokiem.

Historia banku sięga 1919 roku. Powstał wtedy Polski Bank Rolny (od 1921 roku - Państwowy Bank Rolny, od 1948 roku - Bank Rolny), który małym i średnim gospodarstwom rolnym oferował m.in. kredyt krótkoterminowy, kredyt na kupno gruntu i inwestycje oraz zarządzanie funduszami. W 1975 roku w wyniku połączenia Centralnego Związku Spółdzielni Oszczędnościowo-Pożyczkowych i Państwowego Banku Rolnego powstaje państwowo-spółdzielczy Bank Gospodarki Żywnościowej. W 1994 r. Bank został przekształcony w spółkę akcyjną. Większościowym udziałowcem BGŻ jest holenderski Rabobank.

Quest Dystrybucja Sp. z o.o. –Dystrybutor i Elite/Premiere Partner oraz Partner Wsparcia Technicznego (Support Providing Partner) firmy Dell Software w Polsce, dostarcza innowacyjne rozwiązania do zarządzania systemami IT w środowiskach fizycznych, wirtualnych i w chmurze oraz zapewnia wsparcie w zakresie implementacji i wykorzystania oferowanego oprogramowania. Spółka działa na polskim rynku oprogramowania narzędziowego już ponad dziesięć lat, rozpoczynając działalność jako wyłączny przedstawiciel i dystrybutor produktów firmy Quest Software. W wyniku przejęcia Quest Software przez firmę Dell w 2012 r., Quest Dystrybucja Sp. z o.o. pozostała dystrybutorem oprogramowania narzędziowego, oferując polskim klientom rozwiązania z szerokiej oferty Dell Software.

Produkty Dell Software pomagają zredukować koszty IT, osiągnąć większą wydajność oraz zapewnić kompleksowe zarządzanie następującymi obszarami:
Zarządzanie Bazami Danych, Zarządzanie Środowiskami Microsoft, Bezpieczeństwo i Kontrola Dostępu, Monitoring Systemów i Aplikacji, Ochrona Danych, Zarządzanie Wirtualizacją oraz Zarządzanie Stacjami Roboczymi.

Klientami Quest Dystrybucja w Polsce są firmy reprezentujące wszystkie sektory gospodarki, m.in. finansowy, telekomunikacyjny, energetyczny, przemysłowy oraz instytucje rządowe. W realizacji wymagań klientów firma współpracuje zarówno z dostawcami i producentami głównych platform systemowych, jak i największymi firmami integratorskimi.

Więcej informacji: www.quest-pol.com.pl