Załącznik nr 2 do ogłoszenia

DZIAŁANIE 2.2. ROZWÓJ ELEKTRONICZNYCH USŁUG PUBLICZNYCH

PRIORYTET II. SPOŁECZEŃSTWO INFORMACYJNE

REGIONALNEGO PROGRAMU OPERACYJNEGO WOJEWÓDZTWA ŚLĄSKIEGO
NA LATA 2007-2013

Wstępny opis planowanego zamówienia „Wdrożenie systemu zarządzania zasobami IT wraz ze sprzętową infrastrukturą serwerową, systemem archiwizacji i backupu”.

BACK OFFICE

System Back Office w Komendzie Wojewódzkiej będzie obejmował stworzenie i wdrożenie zintegrowanego systemu wspomagania zarządzania.

W związku ze specyficzną działalnością każdego wydziału zostanie on podzielony na dwie części:

- system zarządzania oraz obiegu dokumentów Laboratorium Kryminalistycznego (120 użytkowników)
- system zarządzania zasobami IT w Policji w całym województwie śląskim

Projektowane rozwiązanie będzie wykorzystywało wspólną infrastrukturę serwerową.

System zarządzania zasobami IT

Policja obecnie eksploatuje 2 niezależne sieci komputerowe Policyjna Sieć Transmisji Danych (PSTD) i odseparowana od niej sieć z dostępem do internetu. Takie rozwiązanie zapewnia bezpieczeństwo danych w PSTD jednak konieczne jest zarządzanie dwoma odrębnymi sieciami. Garnizon śląski składa się z 133 lokalizacji tj.: Komenda Wojewódzka Policji w Katowicach, 32 Komendy Miejskie/Powiatowe Policji i 84 Komisariaty Policji. Osobowo garnizon śląski liczy ok. 13 tys. policjantów i pracowników policji. Wykorzystywanych jest aktualnie ok 6900 komputerów.

System zarządzania zasobami IT obejmie wszystkich użytkowników obecnie istniejących dwóch sieci, wszystkie stacje robocze, system zarządzania wydrukiem oraz konieczną infrastrukturę sprzętową przechowywania danych i ich archiwizację.
System zostanie stworzony z wykorzystaniem usług katalogowych active directory i będzie obejmował:

- Scentralizowane zarządzanie wszystkimi usługami i komputerami – zrealizowanie zaleceń w zakresie polityki bezpieczeństwa dotyczących użytkowników sieci komputerowej, sprzętu i oprogramowania komputerowego.

- Kompleksowe zarządzanie infrastrukturą komputerową, a tym samym usprawnienie przeprowadzenia cyklicznych audytów bezpieczeństwa obejmujących zasoby teleinformatyczne całego garnizonu śląskiej Policji
- Zminimalizowanie strat wywołanych przez awarie sprzętu.
- Sprzętową i programową ochronę danych.
- Udostępnienie do pracy grupowej zasobów IT (pliki, urządzenia wielofunkcyjne, drukarki).
- Pełna kontrolę dostępu wraz z historią działań.
- Ujednolicenie procesu logowania i związaną z tym redukcję czasowo - kosztową zarządzania kontami.
- Ograniczenie liczby interwencji serwisu.
- Spójną administrację zasobami.
- Automatyzację procesów instalacji nowych zasobów i użytkowników.
- Możliwość zdalnego i automatycznego instalowania i aktualizowania oprogramowania.
- Możliwość instalowania centralnych systemów teleinformatycznych, które w połączeniu z nowoczesną strukturą łączności światłowodowej między jednostkami, pozwolą na szybką i pełna reakcję.

Zbudowane środowisko usług katalogowych z uwagi na dwie odseparowane od siebie sieci komputerowe stworzone zostanie w postaci dwóch osobnych domen. Ze względu na ten podział, w ramach prac konieczne jest wykonanie dwóch projektów logowania i procedur migracji danych. Całość infrastruktury serwerowej i zasobów Active Directory użytkowana byłaby w jednej lokalizacji. Kopie zapasowe tych danych byłyby przesyłane do drugiej lokalizacji. Projektowana infrastruktura serwerowo – sprzętowa powinna zapewnić pełną separację sieci.
Pierwszy etap projektu obejmuje wykonanie struktury logowania, które obejmie:

- Opracowanie konwencji nazewniczej dla całej organizacji uwzględniającej dopuszczalne standardy nazw dla:
  - Oddziałów,
  - Jednostek organizacyjnych,
  - Zasad grup (GPO),
  - Kont użytkowników, komputerów (stacji roboczych, serwerów),
  - Grup administracyjnych i zasobowych,
  - Kont funkcyjnych i serwisowych,
  - Zasobów,
  - Drukarek i urządzeń peryferyjnych.
- Opracowanie zasad tworzenia i stosowania grup do zarządzania systemem oraz zasobami.
- Projekt struktury logicznej Active Directory
  - Architektura i poziom funkcjonalności domen,
  - Struktura kontenerów AD grupująca obiekty tj. konta komputerów,użytkowników, grupy,
  - Określenie sposobu zarządzania kontami użytkowników, komputerów,
  - Konfiguracja uprawnień administracyjnych dla jednostek organizacyjnych w domenie.
- Projekt topologii (struktury fizycznej) Active Directory

  - Topologia siedzib Active Directory,
  - Rozmieszczenie i funkcje kontrolerów domenowych,
  - Konfiguracja replikacji usługi Active Directory,
  - Synchronizacja czasu,
  - Konfiguracja serwerów.
- Konfiguracja ustawień bezpieczeństwa.
  - Ustawienia Zasady Grup (GPO) dla domeny,
  - Ochrona antywirusowa,
  - Zarządzanie poprawkami,
  - Audyt zmian w konfiguracji usług katalogowych.
- Projekt usług sieciowych
  - Konfiguracja usług DHCP i DNS.
- Zarządzanie środowiskiem pracy użytkownika
  - Zasady Grup – Group Policy,
  - Uprawnienia do zarządzania stacjami roboczymi.
- Koncepcja zarządzania zasobami plikowymi
  - Organizacja zasobów sieciowych (folder domowy, repozytoria).
- Model administrowania dla Systemu
  - Administrowanie domeną,
  - Administrowanie systemem,
  - Role administracyjne,
  - Zadania i zakres uprawnień administratorów.

Dla zapewnienia wymaganego poziomu bezpieczeństwa użytkownicy sieci policyjnej zostaną objęci systemem silnego uwierzytelniania opartego o karty inteligentne, na których będą zapisane certyfikaty X509. Początkowo system uwierzytelniania będzie obejmował logowanie do domeny Active Directory, jednak docelowo będzie można rozszerzyć go o inne systemy i aplikacje (np. sieci VPN, sieci WIFI).

System silnego uwierzytelniania zostanie zaprojektowany w taki sposób, aby maksymalnie wykorzystać produkty i rozwiązania informatyczne obecnie eksploatowane w KWP w Katowicach i w KGP w Warszawie. W skład systemu uwierzytelniania wejdą wykorzystywane już:

1. Centrum Certyfikacji Kluczy Centaur CCK, który będzie odpowiedzialny za wystawianie, zawieszanie i unieważnianie certyfikatów X509 v3 dla użytkowników kart inteligentnych. System zarządzany przez KGP Warszawa.
2. Sprzętowy moduł kryptograficzny CompCrypt Delta-1 służący do bezpiecznego generowania i przechowywania materiału kryptograficznego.
3. Karty mikroprocesorowe CryptoCard multiSIGN.

CryptoCard multiSIGN jest specjalizowaną kryptograficzną kartą mikroprocesorową przeznaczoną do realizacji kwalifikowanego i niekwalifikowanego podpisu elektronicznego oraz funkcji identyfikacji i silnego uwierzytelniania użytkowników. Obecnie KWP w Katowicach posiada ok. 4000 kart (sieć policyjna)

4. CryptoCard Suite - programowanie middleware do obsługi i zarządzania kartami elektronicznymi CryptoCard multiSIGN.
5. Czytniki kart – wykorzystywane obecnie czytniki kart mikroprocesorowych.

Dalsze etapy projektu obejmują wdrożenie usług poprzez instalację, konfigurację kompletnego środowiska usług katalogowych zgodnie z powyższymi założeniami i funkcjonalnością wraz z przygotowaniem planów migracji i integracji istniejącego środowiska komputerowego.

Wprowadzenie systemu pozwoli na:

- wprowadzenie centralnego kompleksowego zarządzania infrastrukturą teleinformatyczną
- automatyzację procesów administracyjnych
- zapewnienie pełnego bezpieczeństwa zgodnego ze standardami
- ograniczenie i przyspieszenie interwencji serwisowych

Sprzętowa Infrastruktura serwerowa, system archiwizacji i backupu.

Wszystkie rozwiązania projektowane są jako wirtualne i zostaną one zainstalowane w projektowanym środowisku wirtualnym zapewniającym wymaganą niezawodność i odporność na awarie.

Do stworzenia infrastruktury systemu zostanie zastosowana technologia serwerowa typu blade wraz z wirtualizacją.

Koncepcja zakłada następujące elementy, które zostały podzielone ze względu na fizyczną lokalizację:

Podstawowe centrum przetwarzania danych:

- oprogramowanie do wirtualizacji
- macierz dyskową w technologii fiber Chanel
- oprogramowanie zarządzające
- osiem serwerów typu blade
- dwa przełączniki SAN w technologii Fibre Channel
- system backupu

Zapasowe centrum przetwarzania danych:

- zapasowa macierz dyskowa
- zapasowy system backupu

Środowisko zostanie zbudowane przy użyciu fizycznych serwerów typu blade. Architektura oparta o technologię blade charakteryzuje się wysokim stopniem zagęszczenia serwerów przy jednoczesnej minimalizacji kosztów okablowania, zasilania i klimatyzacji. W ramach jednej obudowy otrzymujemy kompletne środowisko sprzętowe wraz z infrastrukturą sieciową Ethernet oraz FibreChannel. Obudowę można później doposażyć o kolejne serwery oraz moduły komunikacyjne.

W ramach farmy, na każdym serwerze zostanie zainstalowany preinstalowany system operacyjny, tzw. hypervisor, który stanowi podstawę pracy serwera w klastrze. Całe środowisko wirtualne będzie zarządzane przy pomocy konsoli zarządzającej. Każdy z serwerów będzie miał dostęp do macierzy dyskowej, która udostępni (współdzielone między

serwerami) zasoby pod przyszłe maszyny wirtualne. Przy pomocy oprogramowania do wirtualizacji, klaster zostanie zabezpieczony przed awariami fizycznymi serwerów oraz zostaną ustawione priorytety umożliwiające relokację maszyn wirtualnych w przypadku nadmiernego obciążenia systemu. Technologia proponowanej macierzy pozwoli na pełną współpracę ze środowiskiem wirtualizacji serwerów tak aby administrator dysponował pojedynczą konsolą do środowiska wirtualnego i dyskowego (storage). Sama macierz wyposażona zostanie w funkcjonalności umożliwiające dynamiczną zmianę parametrów pracy w zależności od warunków obciążenia środowiska (thin provisioning, virtual provisioning, fast cache, tiering itp.).

Cała architektura jest w pełni redundantna, czyli posiada podwójne moduły komunikacyjne, interfejsy do serwerów oraz zdublowane zasoby dyskowe na poziomie samych macierzy. W ramach projektu wydzielona zostanie zapasowa fizyczna lokalizacja, która posłuży do replikacji danych w calu szybkiego przełączenia zasobów serwerowych. Dopełnieniem całej architektury jest również zastosowanie wydajnego systemu kopii zapasowych i archiwizacji. Proponujemy do tego celu system backupu dyskowego typu avamar. Podstawą tej architektury jest backup z de-duplikacją. Backup odbywa się na medium dyskowe w postaci wydzielonej przestrzeni dyskowej RAID. Najważniejszą zaletą systemu jest fakt, iż w systemie tym przechowywane będą tylko nowe fragmenty danych (plików, baz danych, maszyn wirtualnych). Dzięki de-duplikacji przenoszenie pełnej kopii zapasowej wymaga transmisji 1 -3% oryginalnych produkcyjnych i jest wykonywana w bardzo krótkim czasie (krótkie okno backupu). System potrafi wykonywać backup plikowy, aplikacyjny (MS Active Directory, bazy danych itp.) oraz całych maszyn wirtualnych. Jest to rozwiązanie kompletne i zarządzane z jednej konsoli administracyjnej. System potrafi na granularne odtwarzanie danych na poziomie usług katalogowych MS ADDS (odtwarzania pojedynczych obiektów AD) lub pojedynczych plików całych maszyn wirtualnych (nawet jeśli maszyna jest wyłączona). Proponowane rozwiązanie charakteryzuje się bardzo elastycznym modelem licencjonowania (na pojemność) przez co można na początku objąć backupem środowisko maszyn wirtualnych oraz aplikacji np. SQL a w późniejszym etapie dołączyć stacje robocze użytkowników. W założeniach proponowanej architektury, system backupu znajdować się będzie w podstawowym centrum przetwarzania danych, natomiast w zapasowym centrum znajdować się będzie jego replika. Dane synchronizowane są na bieżąco, a przez zastosowane algorytmy deduplikacji system w sposób minimalny obciąży sieć. System zbudowany zostanie przy pomocy wydajnej architektury klastrowej RAIN.

Zasoby stworzonej infrastruktury zostaną wykorzystane we wszystkich wdrażanych w ramach projektu systemach typu Back Office