Załącznik nr 1 do Umowy

OPIS PRZEDMIOTU ZAMÓWIENIA

1. System zarządzania uprawnieniami

Wdrożenie systemu zarządzania uprawnieniami - kontrola dostępu do dokumentów o rożnych poziomach wrażliwości jest jednym z kluczowych wymagań systemu wspomagającego pracę Urzędu.

1. System ma zapewnić zarzadzanie uprawnieniami dostępu do systemów informatycznych i dokumentów o rożnych poziomach wrażliwości zgodnie z Polityki Bezpieczeństwa Informacji Urzędu Miasta Gorzowa Wielkopolskiego (Załącznik nr 1).
2. System ma posiadać interfejs w języku polskim.
3. System ma zostać zintegrowany z usługami Active Directory.
4. System ma zostać zainstalowany w oparciu o infrastrukturę Zamawiającego na serwerze wirtualnym w oparciu o darmową bazę danych np. PostgreSQL.
5. System pozwala na zawansowane zarządzanie uprawnieniami w oparciu o użytkowników, stanowiska, komórki organizacyjne i role.
6. Struktura organizacyjna oraz przypisane role mają być głównym nośnikiem uprawnień w systemie.
7. System ma umożliwić odwzorowanie struktury organizacyjnej.
8. System informuje użytkowników o zadaniach wysyłając powiadomienie e-mail oraz umożliwia podpięcie bramki SMS.
9. System ma umożliwić utrzymanie bazy aktywów informatycznych (systemów itp.), typów dokumentów i pomieszczeń.
10. System ma umożliwić wypełnienie i wygenerowanie metryki zasobu zawierający minimum:
    - nazwę,
    - typ,
    - właściciela,
    - zasoby podrzędne i nadrzędny,
    - uprawnienia.
11. System ma umożliwić przypisanie działania do zasobu wraz ze wskazaniem terminu wykonania oraz opisem.
12. System ma umożliwić wskazanie kalendarza działań dla aktywa np. przegląd uprawnień, co skutkować będzie przypomnieniem o działaniu i możliwością raportowania wykonania działania i wprowadzenia wyniku.
13. System ma automatyzować obsługę wniosku o nadanie / zmianę / wycofanie uprawnień poprzez możliwość wypełnienia wniosku, zatwierdzenia, potwierdzenia nadania lub modyfikacji uprawnień.
14. System ma prezentować rejestry wniosków wraz z ich statusami.
15. System ma przechowywać i tworzyć rejestr aktywnych uprawnień wraz z powiązaniem do zasobu osoby czy wniosku, w ramach którego został nadany / zmodyfikowany.
16. System monitoruje realizację działań poprzez przypomnienia i mechanizm eskalacji zadań.

17. System ma posiadać mechanizmy zarządzania repozytorium dokumentów z zarządzaniem uprawnieniami do nich, ich wersjonowaniem i zapewnieniem informowania o dokumentach i wymuszaniem zapoznania.
18. System ma wspierać przegląd uprawnień i umożliwiać generowanie raportów.
19. System posiada predefiniowane raporty z możliwością wygenerowania pliku: pdf, xls, doc.
20. System posiada generowanie i automatyczną dystrybucję raportów w wybranych formatach do wytypowanych użytkowników oraz dystrybucję via e-mail, oraz w ramach oferowanego systemu.
21. Wymagania co do modelu licencjonowania rozwiązania:
    - Wykonawca dostarczy minimum 650 licencji wieczystych.
22. Zamawiający wymaga:
    a. Instalacji systemu w oparciu o infrastrukturę Zamawiającego,
    b. Integracji z Active Directory Zamawiającego,
    c. Przeprowadzenia szkoleń dla Administratorów merytorycznych systemu (maksymalnie do 6 osób),
    d. Uruchomienia toutoriala / szkolenia dla użytkowników końcowych,
    e. Produkcyjnego uruchomienia systemu.

2. Infrastruktura PKI (Infrastruktura Klucza Publicznego)

Wdrożenie infrastruktury klucza publicznego w domenie lokalnej (jednej wskazanej przez Zamawiającego).

1. Zamawiający zapewni:

   a. dostarczenie 2 serwerów w formie maszyn wirtualnych:

      1. server Root CA
      system operacyjny: Windows 2016
      procesor 1 core
      pamięć: 4GB
      storage 32GB
      2. server issuing CA
      system oepracyjny: Windows 2016
      procesor 2 core
      pamięć 8G
      storage 64GB

   b. udostępnienie konta Administrator domeny na czas wdrożenia.

2. Wykonawca zapewni:

   a. stosowne licencje dla powyższej infrastruktury,
   b. 2 licencje: system operacyjny Windows 2019 lub 2022 Standard 2 Core, język angielski.

W ramach zamówienia Wykonawca wykona instalacje dwupoziomowego PKI, w ramach którego zrealizuje zadania:

1. Instalacja serwera Root CA (poza domeną), opublikowanie certyfikatu cyfrowego w AD.
2. Instalacja i konfiguracja roli Active Directory Ceriticate Services.
3. Instalacja serwera SUB CA (prywatny klucz 2048, algorytm SHA256).
4. Konfiguracja kryptografii, nazwy PKI, procesu żądania certyfikatów.
5. Konfiguracja certyfikatów SUB CA.
6. Publikacja certyfikatów SUB CA w magazynie AD (magazyn zaufanych głównych urzędów certyfikacji).
7. Uruchomienie usług PKI oraz publikacja listy CRL.
8. Konfiguracja usługi NDES (obsługa protokołu SCEP).
9. Konfiguracja portalu do żądań certyfikatów instalacja na oddzielnym serwerze lub na SUB CA (zostanie ustalone po weryfikacji przygotowanego środowiska).
10. Konfiguracja funkcji automatycznego odnawiania certyfikatów dla komputerów w AD.
11. Szkolenie w zakresie wystawiania certyfikatów dla typowych 3 szablonów. Prezentacja jak przygotować własny szablon na bazie natywnych rozwiązań Microsoft-u.
12. Zaprojektowanie backup-u infrastruktury PKI.

3. Ochrona przed wyciekiem informacji wraz z modelowaniem zasad i reguł DLP

1. Oprogramowanie musi wspierać co najmniej systemy operacyjne:
   a. Windows 8,
   b. Windows 8.1,
   c. Windows 10,
   d. Windows Server min. 2003 (32/64 bit),
   e. Windows Server 2019 (32/64 bit).

2. Zarządzanie systemem DLP musi posiadać, co najmniej poniższe funkcjonalności:
   a. Interfejs zarządzania oparty na Microsoft Management Console.
   b. Rozwiązanie musi zapewniać integrację z Active Directory (AD), co oznacza, że elementy składowe AD (w tym szczególnie: jednostki organizacyjne, grupy, komputery, użytkownicy) mogą być importowane na serwer systemu DLP. Dodatkowo wymagana jest możliwość włączenia mechanizmu synchronizacji zmian z AD. Instalacja agenta na wszystkich komputerach w sieci musi być wykonywana w sposób zautomatyzowany, bez angażowania użytkownika stacji końcowych. Nie dopuszcza się instalowania oprogramowania na kontrolerach AD.W przypadku braku połączenia sieciowego pomiędzy serwerem, a stacją końcową, powinna być możliwość ustawień alternatywnych, używanych w danym przypadku.
   c. Definiowanie ustawień dla stacji końcowych zdalnie.
   d. Zarządzanie poszczególnymi ustawieniami dostępu (np. do portów USB) definiowane jest dla komputerów, grup użytkowników oraz użytkowników.
   e. Możliwość zmodyfikowania komunikatów pojawiających się na stacjach końcowych w przypadku naruszenia polityki.
   f. Audyt pozwalający na monitorowanie, kiedy i w jakich godzinach były dokonywane modyfikacje w konsoli.
   g. Możliwość zdefiniowania czy w pasku zadań Windows (tzw. Tray) ma być widoczna dla standardowego użytkownika ikona, informująca o działaniu oprogramowania DLP.
3. System DLP musi posiadać, co najmniej poniższe funkcjonalności:

a. Oprogramowanie zezwala na kontrolę dostępu do protokołów FTP, HTTP, IBM Notes, SMTP, MAPI, SMB, Telnet oraz innych na podstawie przynależności do grup domenowych lub bezpośrednio wybierając użytkowników.
b. Oprogramowanie zezwala na utworzenie „białych list" protokołów pozwalających na selektywne dopuszczenie komunikacji sieciowej.
c. Oprogramowanie zezwala na utworzenie reguł, blokujących przesyłanie plików na podstawie ich zawartości.
d. Oprogramowanie w przypadku naruszenia reguł ma możliwość skopiowania pliku, który naruszył politykę, celem wglądu w zawartość przez administratora zarządzającego konsolą oprogramowania DLP.
e. Zarządzanie dostępem do plików na podstawie zawartości dokumentów.
f. Tworzenie białych list dla urządzeń USB, zezwalające na dopuszczenie używania tylko wyznaczonych
g. Możliwość zablokowania podłączania innych urządzeń niż urządzeń wejścia, pokroju: mysz, klawiatura.
h. Wsparcie dla języka polskiego dla systemu OCR zezwalającego na sprawdzanie zawartości pliku
i. Wsparcie systemu OCR również dla plików graficznych znajdujących się wewnątrz dokumentów np. Microsoft Word.
j. Możliwość zdefiniowania w jakich godzinach oraz dniach dany użytkownik może skorzystać z predefiniowanych protokołów lub podłączyć urządzenie do danego portu, a w jakich godzinach ma to być zabronione.
k. Dla blokowania przesyłania plików na podstawie zawartości, system powinien posiadać predefiniowaną funkcję, umożliwiającą rozpoznanie w treści numeru PESEL.
l. Możliwość wykrycia sprzętowych keyloggerów oraz zdefiniowanie czynności, uniemożliwiających przechwycenie danych użytkownika wpisywanych przez klawiaturę.

4. Wymagania co do modelu licencjonowania rozwiązania:
   a. Model licencjonowania oparty na liczbie maszyn fizycznych lub wirtualnych (brak limitów na chronioną ilość danych).
   b. Wykonawca dostarczy minimum 650 licencji na minimum 2 lata.
5. Zamawiający wymaga:
   a. Dostawy odpowiedniej liczby licencji.
   b. Instalacji systemu w oparciu o infrastrukturę Zamawiającego.
   c. Wdrożenia oprogramowania, np. poprzez konfiguracje odpowiednich polityk / reguł
   d. Przeszkolenia administratorów: maksymalnie do 4 osób.
6. Wymagania systemowe:
   a. Konsole zarządzania dla administratorów.
   b. Agenci na stacjach.
   c. Windows 7/8/8.1/10/11/Server 2003-2019 (32/64-bit).
   d. Microsoft RDS, Citrix XenDesktop/XenApp, XenServer, VMware Horizon View VMware Workstation, VMware Player, Oracle VM VirtualBox.
   e. Windows Server 2003-2019 (32/64-bit).
   f. Integracja katalogów:
      – Microsoft AD (w pełni natywna),
      – dowolny LDAP (import obiektów).
   g. Bazy danych

- Microsoft SQL Server/Server Express 2014 lub nowszy,
- PostgreSQL 11 lub nowszy.