

Opis Przedmiotu Zamówienia – część numer 2

Zakup oprogramowania do zarządzania tożsamością i dostępem w Urzędzie Miasta i Gminy w Kunowie

1. Oprogramowanie do zarządzania tożsamością i dostępem

1. Wymagania ogólne

Mechanizm ma za zadanie poprawić znacznie bezpieczeństwo systemów poprzez zwiększenie kontroli nad dostępem, minimalizacją zagrożeń związanych z zarządzaniem hasłami i redukcję ryzyka ataków na konta użytkowników. Zapewnia centralne zarządzanie kontami użytkowników i dostępem do zasobów.

2. Wymagania niefunkcjonalne

1. Dostępność i wydajność: Zapewnienie szybkiego i niezawodnego mechanizmu logowania, aby użytkownicy mogli rozpocząć pracę z systemem bez opóźnień i problemów technicznych.
2. Bezpieczne przechowywanie danych uwierzytelniających: Hasła i dane autoryzacyjne powinny być przechowywane w sposób bezpieczny z wykorzystaniem silnych algorytmów kryptograficznych, aby uniemożliwić odzyskanie oryginalnego hasła w przypadku naruszenia dostępu do systemu.
3. Odporność na ataki: Mechanizm logowania powinien ograniczać liczbę prób nieudanych logowań aby uniemożliwić lub utrudnić atakującemu próby odgadnięcia hasła metodą brute force (np. blokada po 3 nieudanych próbach na 5 minut).
4. Wymuszanie bezpieczeństwa: Mechanizm powinien umożliwić definiowanie własnej polityki bezpieczeństwa, tj wymagania co do długości hasła, złożoności (np. wymóg zawierania wielkich liter, małych liter, cyfr i znaków specjalnych) oraz okresowej zmiany hasła.
5. Szyfrowanie danych: Wszystkie dane przesyłane w procesie logowania powinny być szyfrowane w celu ochrony przed przechwyceniem przez osoby trzecie.
6. Bezpieczne zarządzanie sesjami: Mechanizm powinien umożliwić ograniczenie czasu trwania sesji oraz usuwać ją całkowicie po wylogowaniu użytkownika.
7. Monitorowanie aktywności: Mechanizm powinien rejestrować i monitorować aktywność logowania, w tym udane i nieudane próby logowania, aby wykrywać potencjalne próby naruszenia bezpieczeństwa.
8. Współpraca: Mechanizm bezpiecznego logowania powinien mieć możliwość konfiguracji i uruchomienia z kontrolerem domeny na środowisku z systemem Windows Serwer (np. Windows

Serwer 2022) oraz Linux (Debian ≥ 12). Stacja końcowa (kliencka) musi być wyposażona w system Windows wpierający integrację z domeną tj. Professional bądź Enterprise.

3. Zakres integracji z obecnym systemem dziedziny

1. W wyniku integracji mechanizmu bezpiecznego logowania z systemem dziedziny Respons autoryzacja użytkownika powinna nastąpić po uprzedniej skutecznej autoryzacji użytkownika na stacji roboczej, bez konieczności ponownego logowania bezpośrednio w systemie dziedziny.
2. Pojedyncze logowanie powinno wyeliminować konieczność posiadania wielu różnych kont przez użytkowników.
3. Integracja powinna być parametryzowana i opcjonalna.

4. Lista czynności dot. wdrożenia mechanizmu

1. Aktualizacja systemu dziedziny na potrzeby uruchomienia mechanizmu bezpiecznego logowania.
2. Wsparcie przy konfiguracji i mapowaniu użytkowników systemu dziedziny Respons z użytkownikami domeny.
3. Instruktaże oraz asystę stanowiskową dla administratora.
4. Świadczenie pomocy technicznej dotyczącej mechanizmu bezpiecznego logowania.
5. Świadczenie usług utrzymania i konserwacji dla dostarczonego mechanizmu.
6. Dostarczenie nowych wersji dokumentacji użytkownika wraz z nowymi wersjami systemu dziedziny i mechanizmu bezpiecznego logowania.