OPZ 2 - Moduł SSO (Bezpieczne logowanie)

Moduł SSO (Bezpieczne logowanie)

## Wymagania ogólne

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

## Wymagania szczegółowe

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 przez 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 bezpieczeństw.
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).

## Zakres integracji z obecnym systemem dziedzinowym

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

## Lista czynności dot. wdrożenia mechanizmu

1. Aktualizacja systemu dziedzinowego na potrzeby uruchomienia mechanizmu bezpiecznego logowania.
2. Wsparcie przy konfiguracja i mapowaniu użytkowników systemu dziedzinowego 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 dziedzinowego i mechanizmu bezpiecznego logowania.