Ćwiczenie 5a. Group Policy Object (GPO) cz 1.

Przywróć maszyny wirtualne po poprzednich ćwiczeniach

Scenariusz

Kontynuujesz pracę jako administrator w firmie „KEJA Corp". Kierownik działu IT zlecił

wykonanie pewnych czynności związanych z GPO

Zadania do wykonania

Zadanie 1

Zapoznaj się z funkcjonowaniem Group Policy. Zapoznaj się z tworzeniem i edytowaniem Obiektów GPO, z Blokowaniem dziedziczenia, z wymuszaniem Polis itp.

Zadanie 2

- Polityki w firmie dotyczące kont komputerów powinny zaczynać się od **C_**
- Polityki w firmie dotyczące kont użytkowników powinny zaczynać się od **U_**
- Polityka **Default Domain Policy** nie powinna być zmieniana - wyjątek stanowi polityka haseł i polityka blokowania kont po nieudanych próbach logowania.
- Polityki w firmie dotyczące zarówno kont komputerów jak i użytkowników powinny zaczynać się od **A_** (polityki niepolecane)
- **Nazwa polityki** powinna określać na co dana polityka ma wpływ
- Zaleca się tworzenie osobnych polityk do niezależnych funkcjonalności.

1. Polityka haseł dla użytkowników domeny jest następująca:
    - Historia haseł 15
    - Maksymalny okres ważności hasła 30
    - Minimalny okres ważności hasła 2
    - Minimalna długość hasła 10
    - Hasła muszą spełniać wymogi co do złożoności
2. Polityka blokowania konta: Po 3 nieudanych próbach konto powinno zostać trwale zablokowane. Licznik nieudanych prób ma się zresetować po 120 minutach.
3. Poniższe ustawienia mają być **zawsze wdrażane** dla wszystkich komputerów w firmie
    a. Always wait for the network at computer startup and logon
    b. Default Logon domain: keja.msft
    c. Logowania lokalne nie powinny być cache'owane na serwerach - innymi słowy każdorazowe logowanie wymaga uwierzytelnienia przez kontroler domeny.
    d. Grupa Administratorów powinna dodawana do profil przechodnich użytkowników (Add the Administrators security group to roaming user profiles)
    e. Właściciel profili przechodnich nie powinien być sprawdzany (Do not check for user ownership of Roaming Profile Folders)
    f. Automatyczne wylogowywanie użytkowników po czasie 120 s. bezczynności.
    g. Wyłączanie dostępu do portów USB.
    h. Ograniczenie dostępu do rejestru.

1. Poniższe ustawienia mają być **zawsze wdrażane** dla wszystkich użytkowników w firmie
    a. Wyłączenie dostępu do Panelu sterowania i ustawień.
    b. Ograniczenie dostępu do określonych dysków (np. dysku C:)
    c. Blokada dostępu do Menedżera zadań.
    d. Wyłączenie możliwości uruchamiania wybranych aplikacji (np. cmd.exe, powershell.exe).
    e. Zablokowanie możliwości zmiany tapety.

Testowanie ustawień

- Dla następujących użytkowników ma być włączony system starzenia się haseł: **ewa**, **ala**, **grzegorz** – włącz go używając np. AD Users and Computers lub PowerShell
- Przetestuj powyższe ustawienie. m.in. Spróbuj zalogować się na **CL1** jako **ala**. Po zalogowaniu zmień hasło. – Udało się ?
- Zaloguj się jako Grzegorz po czym wyloguj się i spróbuj się kilkukrotnie zalogować z błędnym hasłem.
- Przeprowadź inne testy.
- Sprawdź czy polityki zostały wdrożone zarówno na komputer

Zadanie 3

1. Server **SVR1** został przeniesiony do **Katowic**, skoryguj jego lokalizację w **AD**
2. Dla wszytkach serwerów w firmie należy wprowadzić następujące ustawienie (przygotuj odpowiednie polityki i je udokumentuj)
    a. Zarządzać serwerami powinni jedynie:
        - administrator lokalny
        - administratorzy domenowi
        - członkowie grupy IT

        ustawienie to powinno nadpisać ewentualne inne polityki.
    b. Prawo do **wyłączania komputera** oraz **logowania lokalnego**, oraz możliwość łączenia się przed **RDP** mają tylko wskazani w poprzednim punkcie użytkownicy
    c. Użytkownicy powinni być powiadamiani 7 dni przed wygaśnięciem hasła.
    d. Na wszystkich serwerach ma zostać wyłączone serwis „windows audio”.

Testowanie ustawień: Przetestuj powyższe ustawienia na serwerze SVR1

Zadanie 4

1. Komputer **CL1** został przeniesiony do **Opola**, skoryguj jego lokalizację w **AD**.
2. Dla wszytkach komputerów klienckich mają zostać wdrożone następujące ustawienia
    a. Zarządzać komputerami klienckimi powinni jedynie:
        - administrator lokalny
        - administratorzy domenowi
        - członkowie grupy IT
    b. Serwisy
        - Windows Remote Management WinRm powinien być włączony automatycznie
        - Microsoft ISCSI Initiator powinien być włączony automatycznie

3. Dla komputerów klienckich w **Opolu** lokalnie logować mogą się członkowie lokalnej grupy administratorów i działu **HR**.
4. Dla wszytkach pracowników działu **HR** powinny być wdrożone następujące ustawienia
    a. Zabronienie dostępu do Control Panel i PC Settings
    b. ScreenServer: Włącza się po 2 minutach bezczynności, Wymaga podania hasła aby odblokować komputer
    c. Pracownicy nie powinni móc zmieniać wyglądu swojego Windowsa (desktop,Theme itp.)
    d. Na dysku C: powinien być zawsze dostępny folder TEMPFILE

Testowanie ustawień: Przetestuj powyższe ustawienia na kliencie **CL1** i koncie należącym do działu **HR**

Cele dydaktyczne. Po zakończeniu ćwiczenia powinieneś umieć:

- Tworzyć i edytować Obiekty GPO
- Wyszukiwać niezbędne ustawienia w obiektach GPO
- Decydować o kolejności wdrażania GPO

Uzupełnienie Teoretyczne

1. Wprowadzenie do Group Policy Object (GPO)

Group Policy Object (GPO) to mechanizm zarządzania i konfiguracji systemów operacyjnych, aplikacji oraz ustawień użytkowników w środowisku Windows. Dzięki GPO administratorzy mogą scentralizować i automatyzować zarządzanie politykami w domenach Active Directory (AD). GPO umożliwia kontrolowanie wielu aspektów systemu, takich jak instalacja oprogramowania, konfiguracja zabezpieczeń, ustawienia sieciowe i zarządzanie sesjami użytkowników.

Podstawowe elementy GPO:

- **Local Group Policy** (polityka lokalna) – polityka dotycząca tylko lokalnego komputera.
- **Domain-based Group Policy** – polityka stosowana w ramach domeny Active Directory.
- **GPOs** mogą być przypisane do:
    - **Site** (witryny),
    - **Domain** (domeny),
    - **Organizational Units (OU)** (jednostki organizacyjne).

Typy ustawień w GPO:

- **Computer Configuration** – ustawienia, które są stosowane do komputerów (niezależnie od użytkownika, który jest zalogowany).
- **User Configuration** – ustawienia, które są stosowane do użytkowników (niezależnie od komputera, na którym są zalogowani).

2. Dziedziczenie GPO

Domyślnie GPO mają charakter dziedziczny. Oznacza to, że polityki przypisane do wyższego poziomu struktury AD (np. domeny) są dziedziczone przez obiekty na niższych poziomach (np. jednostki organizacyjne – OU).

Przykład:

> Jeśli przypiszemy GPO do domeny, to polityka ta będzie automatycznie stosowana do wszystkich obiektów (komputerów i użytkowników) wewnątrz tej domeny, chyba że dziedziczenie zostanie wyłączone lub zmienione.

3. Blokowanie dziedziczenia GPO (Block Inheritance)

Administratorzy mogą zablokować dziedziczenie GPO w jednostkach organizacyjnych (OU) poprzez opcję **Block Inheritance**. Gdy ta opcja jest włączona dla konkretnej OU, wszystkie polityki z wyższego poziomu struktury AD nie będą stosowane do obiektów w tej OU.

Przykład:

> Blokowanie dziedziczenia może być użyteczne, gdy w jednej z jednostek organizacyjnych potrzebne są zupełnie inne polityki niż te, które są przypisane do całej domeny.

4. Force GPO (Wymuszanie polityki)

Aby przeciwdziałać **Block Inheritance**, można użyć opcji **Enforce (Force GPO)**. Ustawiając politykę jako wymuszoną, sprawiamy, że będzie ona stosowana do wszystkich obiektów poniżej, nawet jeśli dziedziczenie zostało zablokowane.

Przykład:

> Możemy wymusić stosowanie polityki zabezpieczeń w całej domenie, aby zapewnić jednolite zasady bezpieczeństwa na wszystkich poziomach organizacyjnych.

Gpupdate:

gpupdate to narzędzie wiersza poleceń w systemach Windows, które umożliwia wymuszenie natychmiastowego odświeżenia zasad grupowych (**Group Policy**), zamiast czekać na domyślny cykl odświeżania (co 90 minut). Przy jego użyciu można zaktualizować zarówno ustawienia komputera, jak i użytkownika.

Przykład użycia:

> ***gpupdate /force***

Polecenie to wymusi natychmiastowe przetwarzanie polityk dla zarówno konfiguracji komputera, jak i użytkownika. Dodatkowe przełączniki, jak np. /logoff, mogą wymusić wylogowanie po aktualizacji polityk, jeśli to wymagane.

Gpresult:

gpresult to narzędzie wiersza poleceń, które pozwala wyświetlić szczegółowe informacje na temat zastosowanych polityk grupowych na danym komputerze i dla zalogowanego użytkownika. Służy do

analizy i diagnostyki, jakie zasady GPO zostały zastosowane, które polityki zostały zablokowane i z jakiego źródła pochodzą.

Przykład użycia:

gpresult /r

Polecenie to wyświetli podsumowanie polityk dla bieżącego użytkownika i komputera, w tym ich źródło oraz czas ostatniego odświeżenia.

Podsumowanie:

- gpupdate służy do **natychmiastowego odświeżenia GPO**.
- gpresult pozwala na **sprawdzenie wyników stosowania polityk GPO**, co jest użyteczne w diagnozowaniu problemów z GPO.