Ćwiczenie 5d. Group Policy Object (GPO) cz 4.

Zadanie A1: Wdrożenie polityki zarządzania aktualizacjami systemu

Cel: Skonfiguruj GPO, aby zarządzać aktualizacjami systemu w firmie.

Kroki:

1. Utwórz nową GPO o nazwie **A_Updates_Policy**.
2. W sekcji **Computer Configuration → Administrative Templates → Windows Components → Windows Update**, skonfiguruj następujące ustawienia:
    - **Configure Automatic Updates**: Ustaw na „Auto download and notify for install".
    - **Specify intranet Microsoft update service location**: Wskaż serwer WSUS (jeśli jest dostępny).
    - **No auto-restart with logged on users for scheduled automatic updates installations**: Włącz.
3. Przetestuj działanie polityki na komputerze CL1, sprawdzając, czy ustawienia zostały poprawnie wdrożone.

Zadanie A2: Konfiguracja zaawansowanych zasad bezpieczeństwa dla komputerów

Cel: Zastosowanie dodatkowych polityk bezpieczeństwa, które będą dotyczyć komputerów w firmie.

Kroki:

1. Utwórz nową GPO o nazwie **C_Security_Policy**.
2. W sekcji **Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options**, skonfiguruj następujące ustawienia:
    - **Interactive logon: Do not display last user name**: Włącz.
    - **Interactive logon: Message text for users attempting to log on**: Dodaj informację o polityce bezpieczeństwa firmy.
    - **Interactive logon: Message title for users attempting to log on**: Dodaj tytuł wiadomości.
3. Skonfiguruj dodatkowo politykę, która zmusza do uruchomienia **ekranu blokady** po 5 minutach nieaktywności (w sekcji **Computer Configuration → Administrative Templates → Control Panel → Personalization → Enable Screen Saver**).
4. Przetestuj ustawienia na jednym z komputerów w domenie.

Zadanie A3: Filtrowanie GPO przy użyciu WMI

Cel: Kursanci nauczą się, jak stosować GPO tylko dla określonej grupy komputerów za pomocą filtrów WMI.

Kroki:

1. Utwórz nową GPO o nazwie **C_WMI_Filtered_Policy**.
2. W sekcji **Computer Configuration**, skonfiguruj dowolną politykę, np. wyłącz **Windows Defender** na komputerach.
3. Utwórz nowy filtr WMI, który ograniczy stosowanie tej polityki tylko dla komputerów z systemem Windows 10.
    - Filtr WMI: SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.%" AND ProductType = "1".
4. Przypisz ten filtr WMI do stworzonego GPO.
5. Przetestuj politykę na komputerach z Windows 10 oraz innymi wersjami Windows (Windows 7, Windows Server) i upewnij się, że działa tylko na Windows 10.

Zadanie A4: Przygotowanie polityki dla stacji roboczych z dostępem VPN

Cel: Zastosowanie specjalnej polityki dla komputerów korzystających z VPN.

Kroki:

1. Utwórz nową GPO o nazwie **C_VPN_Security_Policy**.
2. W sekcji **Computer Configuration → Windows Settings → Security Settings → Windows Firewall with Advanced Security**, skonfiguruj zasady dla połączeń VPN:
    - Ustaw regułę, która zezwala na połączenia przychodzące tylko przez port 443 (HTTPS).
    - Zablokuj inne nieautoryzowane połączenia przychodzące.
3. Skonfiguruj politykę wymuszającą użycie określonego serwera DNS dla komputerów łączących się przez VPN.
4. Przetestuj politykę na komputerze CL1, konfigurując połączenie VPN i sprawdzając, czy reguły firewall są poprawnie stosowane.

Zadanie A5: Zastosowanie polityki logowania i audytowania aktywności użytkowników

Cel: Wdrożenie polityki logowania oraz konfiguracja audytu aktywności użytkowników.

Kroki:

1. Utwórz nową GPO o nazwie **U_Audit_Logon_Policy**.
2. W sekcji **Computer Configuration → Windows Settings → Security Settings → Advanced Audit Policy Configuration**, skonfiguruj następujące zasady:
    - **Audit Logon**: Włącz.
    - **Audit Account Lockout**: Włącz.
    - **Audit Account Logon Events**: Włącz.
3. Skonfiguruj politykę, która rejestruje wszystkie próby nieudanych logowań.
4. Przetestuj politykę na komputerze CL1 poprzez wielokrotne nieudane próby logowania i sprawdź, czy zdarzenia są rejestrowane w dzienniku zdarzeń (Event Viewer).

Zadanie A6: Przygotowanie polityki do ograniczenia dostępu do urządzeń USB

Cel: Ograniczenie użycia pamięci masowych USB na komputerach w firmie.

Kroki:

1. Utwórz nową GPO o nazwie **C_USB_Restriction_Policy**.
2. W sekcji **Computer Configuration → Administrative Templates → System → Removable Storage Access**, skonfiguruj następujące ustawienia:
    - **Deny write access to removable drives not protected by BitLocker**: Włącz.
    - **Deny read access to removable drives**: Włącz.
3. Skonfiguruj wyjątki dla administratorów lokalnych, aby mieli pełny dostęp do urządzeń USB.
4. Przetestuj politykę na komputerze CL1, podłączając urządzenie USB i sprawdzając dostępność do odczytu i zapisu.