Zasada IGDLA (dawniej AGDLP) – Zastosowanie i Korzyści

1. Co to jest IGDLA?

IGDLA (ang. Identity > Global group > Domain Local group > Access) to nowoczesne podejście do zarządzania uprawnieniami w środowisku opartym na Active Directory. Zastępuje ono starszą zasadę AGDLP (Account > Global > Domain Local > Permission), rozszerzając ją o aspekt tożsamości (Identity) jako punkt wyjścia dla nadawania uprawnień.

2. Rozwinięcie skrótu IGDLA

- I – Identity: użytkownicy i konta serwisowe (własność tożsamości)
- G – Global group: grupy globalne, do których przypisywane są konta użytkowników
- DL – Domain Local group: grupy lokalne domeny, którym przypisuje się dostęp do zasobów
- A – Access: rzeczywisty dostęp (uprawnienia NTFS, udziały sieciowe, role aplikacji itp.)

3. Jak działa IGDLA?

IGDLA opiera się na warstwowym przypisywaniu ról i dostępu. Zamiast przypisywać użytkowników bezpośrednio do zasobów, tworzy się logiczne grupy reprezentujące role lub zespoły (G), które następnie są członkami grup reprezentujących dostęp (DL). Te z kolei mają przypisane konkretne uprawnienia (A). Dzięki temu struktura jest bardziej przejrzysta, skalowalna i łatwa w utrzymaniu.

4. Przykład zastosowania

Przykład: Pracownicy działu HR potrzebują dostępu do folderu \\domena\zasoby\HR.
- Utwórz grupę globalną: GG_HR_Users
- Dodaj użytkowników działu HR do GG_HR_Users
- Utwórz grupę lokalną: DL_Folder_HR_RW (Read/Write)
- Dodaj GG_HR_Users do DL_Folder_HR_RW
- Przypisz DL_Folder_HR_RW do folderu HR z odpowiednimi uprawnieniami NTFS

W ten sposób dostęp jest kontrolowany centralnie i można łatwo go modyfikować.

5. Korzyści ze stosowania IGDLA

- Skalowalność: łatwe zarządzanie dużą liczbą użytkowników
- Przejrzystość: jasna struktura przypisań i dostępów
- Audyt: łatwość w śledzeniu, kto i dlaczego ma dostęp
- Bezpieczeństwo: brak bezpośrednich przypisań użytkowników do zasobów
- Elastyczność: łatwe przenoszenie ról i użytkowników między zespołami

6. Uwagi końcowe

Zasada IGDLA jest zalecana jako standardowy model zarządzania dostępem w środowiskach Active Directory, szczególnie w większych organizacjach. Ułatwia zgodność z politykami bezpieczeństwa i wspiera efektywne zarządzanie tożsamościami.