T: Zasady tworzenia nowych kont użytkowników.

Przydzielanie komuś konta upoważnia go do:
- zalogowania się w systemie,
- korzystania z usług świadczonych przez system.

Każde konto w systemie składa się z:
- zarejestrowanej w systemie nazwy użytkownika i hasła,
- katalogu macierzystego,
- prawa dostępu do systemu.

Ogólne zasady tworzenia nowych kont użytkowników:
- rozpoznanie przeznaczenia konta i związanych z tym potrzeb (dostęp do systemu, programów, sieci, czas pracy itp.),
- zebranie danych personalnych użytkownika (informacje niezbędne do utworzenia konta),
- analiza istniejących w systemie grup (w celu późniejszego przypisanie użytkownika do właściwych grup),
- tworzenie konta (w zależności od potrzeb: lokalnego lub w domenie) i przypisywanie go do grup,
- modyfikacja niezbędnych zabezpieczeń w systemie plików NTFS oraz udostępnianiu zasobów sieciowych,
- jeżeli jest to potrzebne konfiguracja zasad zabezpieczeń,
- sprawdzenie poprawności funkcjonowania konta,
- przekazanie użytkownikowi informacji o zasadach korzystania z konta.

Wszystkie obiekty w Active Directory powinny być odpowiednio nazywane. Standard nazewnictwa powinien być opracowany w formie konwencji łatwej i zrozumiałej dla wszystkich użytkowników i administratorów.

Usługa Active Directory zapewnia organizacji bezpieczne środowisko katalogu, korzystając z wbudowanych funkcji uwierzytelniania logowania i autoryzacji użytkowników. Aby dodatkowo zabezpieczyć usługę Active Directory po jej wdrożeniu, należy wziąć pod uwagę podane niżej zalecenia:
- Ustanów relację zabezpieczeń między dwoma lasami i uprość administrowanie zabezpieczeniami oraz uwierzytelnianie w lasach.
- Wymuś na użytkownikach domeny używanie silnych haseł.
- Włącz zasady inspekcji. Dzienniki zdarzeń inspekcji mogą powiadamiać o czynnościach stwarzających ryzyko związane z zabezpieczeniami.
- Przypisz prawa użytkownika nowym grupom zabezpieczeń, aby mieć możliwość przypisania użytkownikowi określonej roli administracyjnej w domenie.
- Wymuś blokadę kont użytkowników, aby zmniejszyć prawdopodobieństwo złamania zabezpieczeń domeny przez powtarzanie prób logowania.
- Wymuś tworzenie historii haseł do kont użytkowników, aby zmniejszyć prawdopodobieństwo złamania zabezpieczeń domeny.
- Wymuś minimalny i maksymalny okres ważności haseł do kont użytkowników, aby zmniejszyć prawdopodobieństwo złamania zabezpieczeń domeny.
- Weryfikuj i uwierzytelniaj każdego użytkownika, stosując kryptografię klucza publicznego.
- Jeśli nie jest to konieczne, uruchamiaj komputer bez poświadczeń administracyjnych, co jest bezpieczniejsze dla środowiska pracy.
- Ogranicz dostęp użytkowników, grup i komputerów do zasobów udostępnionych i określ ustawienia filtrowania zasad grupy.
- Zapobiegnij atakom złośliwych użytkowników, którzy mogliby próbować udzielić szerszych praw użytkownika innemu kontu użytkownika.
- Zapewnij zabezpieczone przed penetracją uwierzytelnianie użytkowników i bezpieczeństwo poczty e-mail.
- Zastosuj techniki silnego szyfrowania w celu zabezpieczenia informacji o kontach na komputerach lokalnych, serwerach członkowskich lub kontrolerach domeny.