Metody zabezpieczenia zasobów sieciowych

Cel ogólny lekcji: Nauczanie metod zabezpieczania zasobów sieciowych w Windows Server 2019.

Cele szczegółowe lekcji:

1. Zrozumienie kontroli dostępu do plików i folderów na poziomie systemu plików NTFS w celu zapewnienia bezpieczeństwa zasobów sieciowych.
2. Zrozumienie roli szyfrowania plików i folderów na poziomie systemu plików NTFS w zapobieganiu nieuprawnionemu dostępowi do zasobów sieciowych.
3. Zrozumienie roli audytowania zdarzeń na serwerze plików w celu monitorowania i rejestrowania działań użytkowników oraz wykrywania prób nieuprawnionego dostępu do zasobów sieciowych.
4. Zrozumienie roli wbudowanego firewalla w Windows Server 2019 w celu kontrolowania ruchu sieciowego przychodzącego i wychodzącego oraz chronienia serwera przed nieuprawnionymi atakami.
5. Zrozumienie roli zabezpieczania zdalnego dostępu, w tym protokołów VPN, RDP i SSH, w celu zapewnienia bezpieczeństwa zasobów sieciowych, które są dostępne z zewnątrz.
6. Zrozumienie roli regularnych aktualizacji systemu operacyjnego i oprogramowania zainstalowanego na serwerze plików w celu zapewnienia bezpieczeństwa poprzez instalowanie poprawek zabezpieczeń i usuwanie luk w zabezpieczeniach.
7. Zrozumienie roli oprogramowania antywirusowego w celu wykrywania i usuwania wirusów i innych szkodliwych plików na serwerze plików.
8. Zrozumienie roli definiowania i stosowania polityk zabezpieczeń w celu określenia, jakie działania są dozwolone na serwerze plików i zapewnienia bezpieczeństwa zasobów sieciowych

Windows Server 2019 oferuje szereg narzędzi i metod zabezpieczania zasobów sieciowych. Oto kilka przykładów:

1. **Kontrola dostępu** - Używając systemu plików NTFS można zastosować kontrole dostępu na poziomie pliku lub folderu. W ten sposób można określić, kto ma dostęp do pliku, kto może go modyfikować lub kto może go tylko odczytywać. Można również ustawić atrybuty bezpieczeństwa dla plików i folderów, aby uniemożliwić nieuprawniony dostęp.
2. **Szyfrowanie** - System plików NTFS umożliwia szyfrowanie plików i folderów. Szyfrowanie danych pomaga w ochronie przed nieuprawnionym dostępem. Dzięki temu, jeśli ktoś uzyska dostęp do pliku lub folderu, bez klucza szyfrowania nie będzie w stanie go odczytać.
3. **Audytowanie** - Windows Server 2019 pozwala na audytowanie zdarzeń, które mają miejsce na serwerze plików, na przykład próby dostępu do zasobów sieciowych. Audytowanie pozwala na monitorowanie i rejestrowanie działań użytkowników, co ułatwia wykrycie prób nieuprawnionego dostępu.
4. **Firewall** - Windows Server 2019 zawiera wbudowany firewall, który umożliwia kontrolowanie ruchu sieciowego przychodzącego i wychodzącego. Dzięki temu można chronić serwer przed nieuprawnionymi atakami.

5. **Zabezpieczanie zdalnego dostępu** - Jeśli serwer plików jest dostępny z zewnątrz, należy zadbać o odpowiednie zabezpieczenie zdalnego dostępu. Windows Server 2019 oferuje kilka metod zabezpieczania zdalnego dostępu, w tym protokoły VPN, RDP oraz SSH.
6. **Aktualizacje** - Regularne aktualizacje systemu operacyjnego i oprogramowania zainstalowanego na serwerze plików są kluczowe dla zapewnienia bezpieczeństwa. Aktualizacje mogą zawierać poprawki zabezpieczeń i usuwać luki w zabezpieczeniach.
7. **Antywirus** - Warto zainstalować na serwerze plików odpowiednie oprogramowanie antywirusowe, które pomoże w wykryciu i usunięciu wirusów i innych szkodliwych plików.
8. **Polityki zabezpieczeń** - Windows Server 2019 pozwala na definiowanie i stosowanie polityk zabezpieczeń, które określają, jakie działania są dozwolone na serwerze plików. Dzięki temu można na przykład zablokować dostęp do niektórych typów plików lub ograniczyć dostęp do zasobów sieciowych tylko dla określonych użytkowników.

Wykonaj poniższe czynności:

1. Zapoznaj się z artykułem na temat najlepszych praktyk w zakresie zabezpieczeń usługi Active Directory.
2. Zapoznaj się z tematami związanymi z zabezpieczeniami usługi AD omówionymi w tym przewodniku.
3. Wykonaj testy dla 6 z punktów omówionego w przewodniku na jedną lekcje (12 na 2 lekcje), udokumentuj je. Użyj serwer z funkcją kontrolera domeny *_dc2019 i Windows 10 jako klienta.
4. Zanotuj w zeszycie prawidłowe dla każdego z wykonanych punktów rozwiązania i wnioski.

zgłoszenie

Przywróć pierwszy punkt kontrolny

Podsumowanie:

Po wykonaniu wszystkich czynności z powyższej instrukcji przeczytaj ponownie z zrozumieniem cel ogólny i cele szczegółowe, które znajdują się na pierwszej stronie instrukcji. Jeżeli one zostały niezrealizowane to powtarzaj wykonie tej instrukcji w szkole lub/i w domu do momentu zrealizowania.