Wnioski po przeprowadzeniu testów zabezpieczeń zasobów sieciowych:

1. **Kontrola dostępu:**

- **Rozwiązanie:** Skonfigurowanie kontroli dostępu do określonych plików i folderów na serwerze za pomocą systemu plików NTFS.

- **Wnioski:** Zrozumienie, jak precyzyjnie zarządzać uprawnieniami użytkowników do zasobów, co pozwala na ochronę danych przed nieautoryzowanym dostępem.

2. **Szyfrowanie plików:**

- **Rozwiązanie:** Zastosowanie szyfrowania plików i folderów na poziomie systemu plików NTFS.

- **Wnioski:** Zabezpieczenie danych poprzez zastosowanie szyfrowania, co utrudnia dostęp do informacji nawet w przypadku fizycznego dostępu do nośnika.

3. **Audytowanie zdarzeń:**

- **Rozwiązanie:** Konfiguracja audytowania zdarzeń na serwerze plików w celu monitorowania działań użytkowników.

- **Wnioski:** Śledzenie i rejestrowanie działań użytkowników umożliwia szybkie wykrywanie prób nieautoryzowanego dostępu oraz dostarcza informacji dla analizy incydentów.

4. **Firewall:**

- **Rozwiązanie:** Skonfigurowanie wbudowanego firewalla w Windows Server 2019 do kontrolowania ruchu sieciowego.

- **Wnioski:** Zapewnienie dodatkowej warstwy ochrony przed nieuprawnionym ruchem sieciowym i atakami z zewnątrz.

5. **Zabezpieczanie zdalnego dostępu:**

- **Rozwiązanie:** Skonfigurowanie bezpiecznego zdalnego dostępu, np. przy użyciu protokołów VPN, RDP, czy SSH.

- **Wnioski:** Zrozumienie, jak właściwie zabezpieczyć zdalny dostęp, co jest kluczowe, jeśli zasoby sieciowe są dostępne z zewnątrz.

6. **Aktualizacje systemu i oprogramowania:**

- **Rozwiązanie:** Regularne przeprowadzanie aktualizacji systemu operacyjnego i oprogramowania zainstalowanego na serwerze plików.

- **Wnioski:** Utrzymywanie systemu w najnowszej wersji zabezpiecza przed znanymi lukami w zabezpieczeniach, co jest kluczowe dla ochrony przed atakami.

7. **Oprogramowanie antywirusowe:**

- **Rozwiązanie:** Instalacja i konfiguracja oprogramowania antywirusowego na serwerze plików.
- **Wnioski:** Ochrona przed wirusami i innymi szkodliwymi plikami, co stanowi istotny element zabezpieczeń zasobów sieciowych.

8. **Polityki zabezpieczeń:**

- **Rozwiązanie:** Definiowanie i stosowanie polityk zabezpieczeń, które określają dozwolone działania na serwerze plików.
- **Wnioski:** Ustalanie reguł i ograniczeń, które zapewniają kontrolę nad operacjami na zasobach sieciowych, zgodnie z politykami bezpieczeństwa organizacji.

Podsumowanie: Przeprowadzone testy potwierdzają skuteczność różnych metod zabezpieczania zasobów sieciowych w Windows Server 2019. Zrozumienie i praktyczne zastosowanie tych środków zabezpieczających są kluczowe dla utrzymania bezpieczeństwa w środowisku sieciowym.