

Zadanie 1 - Trudne początki

Wnioski:

- Uczniowie powinni zauważyć, że po odjęciu dziedziczonych uprawnień dla folderu, nawet inny zaawansowany użytkownik (User_adv2) nie może edytować uprawnień w folderze User_adv1. To potwierdza, że nadane uprawnienia są skonfigurowane tylko dla użytkownika User_adv1, co chroni folder przed modyfikacjami przez innych użytkowników.

Zadanie 2 - Zabieramy jednym, dajemy drugim.

Wnioski:

- Uczniowie powinni zauważyć, że nadawanie i odbieranie różnych uprawnień wpływa na możliwości użytkownika User_adv2 w odniesieniu do plików i folderów w C:\User_adv1. Kontrolowanie szczegółowych uprawnień umożliwia dostosowanie poziomu dostępu dla różnych użytkowników.

Zadanie 3 Administrator i tak może wszystko!

Wnioski:

- Uczniowie powinni zrozumieć, że administrator może przejąć kontrolę nad folderem, zmieniając właściciela. W przypadku braku dostępu, zmiana właściciela na grupę Administratorzy pozwoliła na późniejszą modyfikację uprawnień. Teraz konto admin ma pełny dostęp do folderu C:\User_adv1 i jego zawartości, co pokazuje, że administrator ma uprawnienia do zarządzania wszystkimi zasobami systemowymi.

Zadanie 4 Użytkownicy mają prawa, ale

Wnioski:

- Uczniowie powinni zrozumieć, że możliwości zarządzania uprawnieniami są związane z właścicielstwem i kontem administratora. W przypadku ograniczania dostępu dla innych użytkowników, konieczne jest zalogowanie się jako administrator lub właściciel, aby dokonać zmian w uprawnieniach. Odpowiednie manipulacje uprawnieniami pozwalają kontrolować dostęp do folderów i plików na komputerze.

Zadanie 5 Jak za pomocą uprawnień zablokować Painta ?

Wnioski:

- Zadanie polegało na ograniczeniu uprawnień grupy „Użytkownicy” dla pliku Paint.exe, co skutkowało niemożnością uruchomienia Painta przez użytkownika. Procedury takie pozwalają administratorowi systemu na kontrolowanie dostępu do konkretnych aplikacji, co może być istotne w przypadku chęci zabezpieczenia pewnych programów przed użytkownikami.

Zadanie 6 Awansujemy!

Wnioski:

- Zadanie polegało na dodaniu specyficznych uprawnień dla grupy „Użytkownicy zaawansowani” do folderu C:\User. Jednak, aby zmienić te uprawnienia, konieczne było posiadanie uprawnień „Zmiana uprawnień”, które musiało zostać nadane przez konta Administratora. To ukazuje, jak ważne jest, aby odpowiednie uprawnienia były nadawane przez osoby mające dostęp do bardziej zaawansowanych działań w systemie.

Zadanie 7 Sprawdzamy

Wnioski:

- Po wykonaniu powyższych kroków uczniowie mogą zauważyć, że czynne uprawnienia różnią się w zależności od użytkownika i folderu.
- Dostęp do poszczególnych folderów zależy od nadanych uprawnień dla danego użytkownika.
- Można zobaczyć, że administrator (admin) może mieć bardziej rozszerzone uprawnienia w porównaniu do innych użytkowników.
- Różnice w czynnych uprawnieniach wynikają z konfiguracji systemu, a także z przypisanych uprawnień dla poszczególnych użytkowników.

Zadanie 8 - Wnioski:

1. Zasada najmniejszych uprawnień:

- Nadanie zbyt szerokich uprawnień, zwłaszcza dla folderów systemowych, może prowadzić do ryzyka naruszenia bezpieczeństwa.
- Warto przestrzegać zasady najmniejszych uprawnień, aby użytkownicy i grupy miały tylko te uprawnienia, które są niezbędne do wykonywania ich zadań.

2. Mechanizm dziedziczenia uprawnień:

- Koncepcja dziedziczenia uprawnień jest istotna, umożliwia określenie, które uprawnienia są dziedziczone z folderu nadrzędnego, a które można definiować na niższym poziomie.

3. Wpływ nadania/uprzedzenia uprawnień:

- Nadanie zbyt rygorystycznych uprawnień, zwłaszcza dla folderów systemowych, może prowadzić do ograniczeń w dostępie do plików i folderów, a nawet do problemów z działaniem systemu operacyjnego.

4. Blokowanie dostępu do folderu WINNT:

- Blokowanie pełnej kontroli grupie „Wszyscy” dla folderu WINNT może skutkować niemożnością odczytu, zapisu, wykonywania, usuwania lub modyfikowania plików i folderów wewnątrz tego folderu.

5. Folder WINNT a historia systemu operacyjnego Windows:

- Folder WINNT jest ważny dla systemu operacyjnego Windows od wersji NT 3.1 wydanej w 1993 roku.

- Zawiera kluczowe pliki, takie jak ntoskrnl.exe, ntdll.dll, win.ini, boot.ini, które są niezbędne do poprawnego działania systemu.

6. Różnice między systemami operacyjnymi:

- W przypadku Windows 11, zmiana uprawnień dla folderu Windows jest utrudniona z powodu mechanizmu Kontroli Konta Użytkownika (UAC).
- Folder Windows zawiera pliki systemowe niezbędne dla Windows 11, a próba zmiany uprawnień skutkuje prośbą o zezwolenie administratora.

7. Wpływ błędów w zarządzaniu uprawnieniami:

- Błędy w zarządzaniu uprawnieniami, takie jak nadanie zbyt rygorystycznych uprawnień, mogą prowadzić do problemów, takich jak brak dostępu do plików czy niezdolność do uruchamiania programów.

8. Bezpieczeństwo konta administratora:

- Znaczenie ochrony dostępu do konta administratora, aby uniknąć niepożądanych zmian w systemie.

9. Praktyczne umiejętności w zarządzaniu uprawnieniami:

- Wykonanie ćwiczeń daje praktyczne doświadczenie w zarządzaniu uprawnieniami, co może być przydatne w pracy z danymi i w kontekście bezpieczeństwa.

10. Rola właściciela plików i folderów:

- Właściwe zarządzanie uprawnieniami podkreśla znaczenie koncepcji właściciela plików i folderów, co jest istotne w kontekście zarządzania uprawnieniami.

Wniosek ogólny: Bezpieczne i skuteczne zarządzanie uprawnieniami jest kluczowe dla utrzymania integralności systemu operacyjnego i ochrony danych przed nieautoryzowanym dostępem czy modyfikacjami.