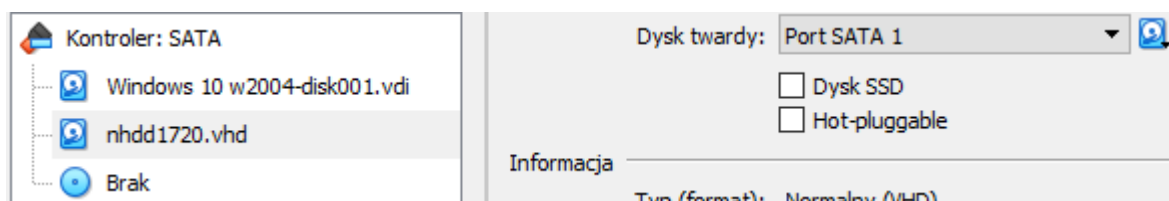


Zadanie: - Uprawnienia w systemie plików NTFS.

Czynności wykonuj według podanej w zadaniu kolejności, jeżeli wykonasz dowolną czynność poza kolejnością pobierz nową maszynę wirtualną i wykonaj ćwiczenie od początku.

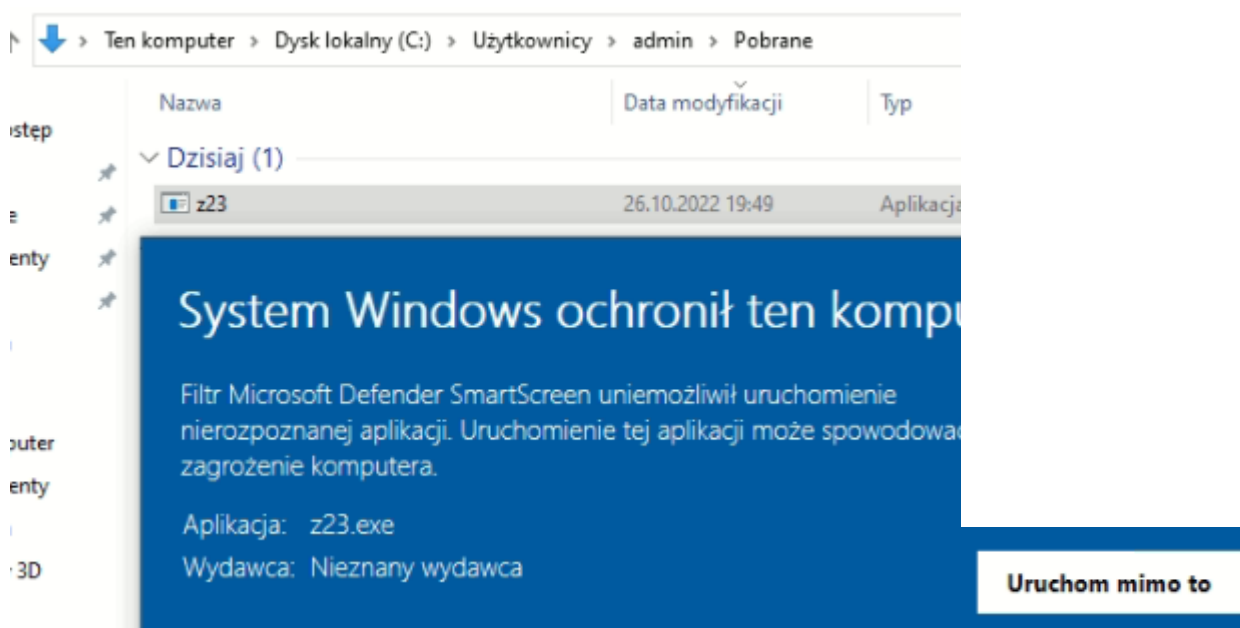
1. W folderze z materiałami znajduje się plik:

- a) **nhdd1720.zip** należy rozpakować do przygotowanego wcześniej folderu z maszyną wirtualną a następnie **nhdd1720.vhd** podłączyć jako drugi dysk do maszyny wirtualnej.



2. W maszynie wirtualnej z strony z materiałami pobierz pliki **z23.exe**.

3. Plik **z23.exe** uruchom jako administrator

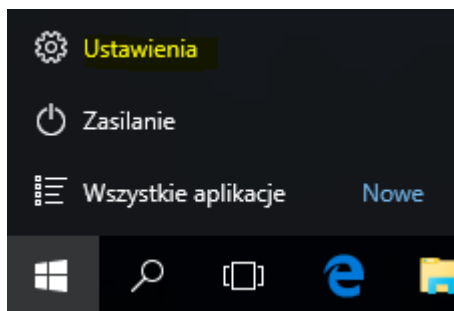


Każdą czynność wykonaną w zadaniach zgłoś prowadzącemu na etapie wskazanym w zadaniu.

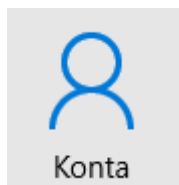
Zaloguj się do konta domyślnego z hasłem zaq1@WSX

Ćwiczenie 1.1. Tworzenie kont użytkowników

W celu utworzenia nowego konta użytkownika:



1. Z menu Start > wybierz

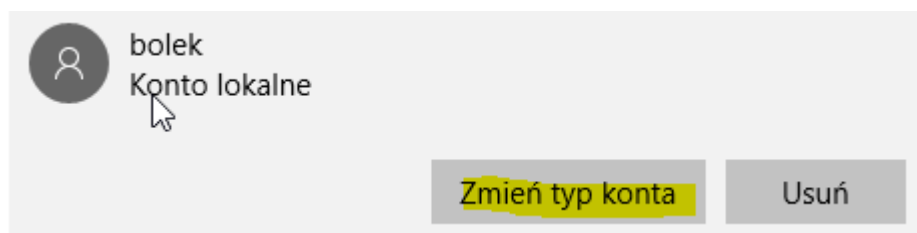


2.



3.

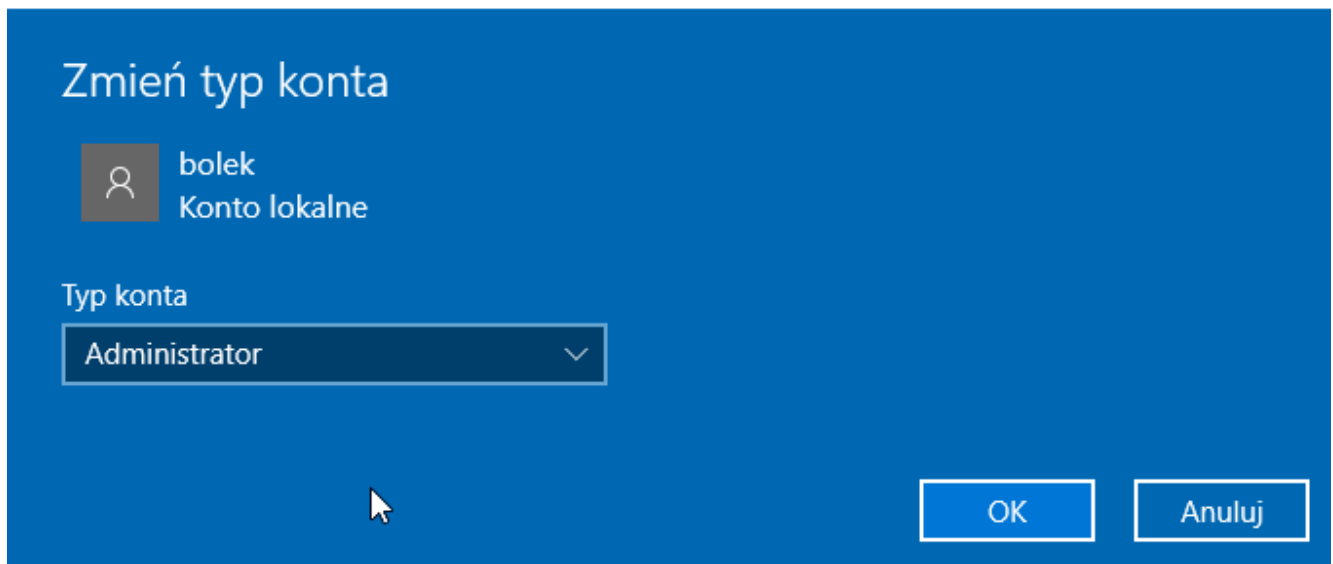
4. Wpisz nazwę nowo utworzonego konta **bolek**.



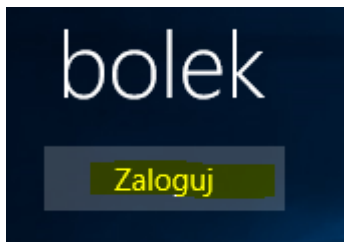
5.

6. Określ typ konta - do wyboru są dwie opcje: Użytkownik standardowy lub Administrator. Zaznacz opcje **Administrator**.

7. Naciśnij przycisk **OK**. *Kreator dodawania nowego konta* zostanie zamknięty, a nowe konto utworzone.



8. Zaloguj się do konta **bolek**



9. Powtórz utworzenie konta użytkownika.

- a. Utwórz konto **lolek**,
- b. Określ typ konta - **Użytkownik standardowy**.

10. W zeszycie zapisz wnioski z wyżej wymienionych czynności uwzględniające sposób tworzenia konta w Windows. Dlaczego podczas utworzenia konta tą metodą nie można dodać konta do grupy Użytkownicy zaawansowani.

(zgłoszenie) 1

Ograniczenie dostępu do danych

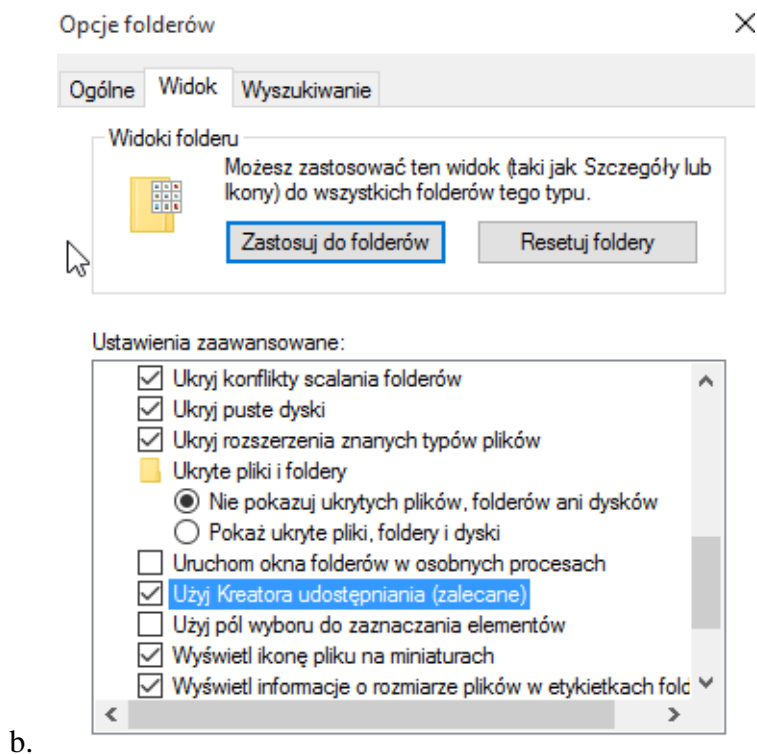
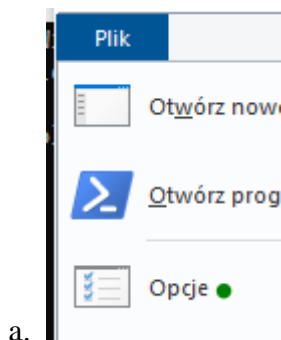
Ćwiczenie 1.2. Folder - modyfikacja uprawnień

Każdy plik i folder umieszczony na dysku NTFS jest „własnością” jednego z użytkowników.

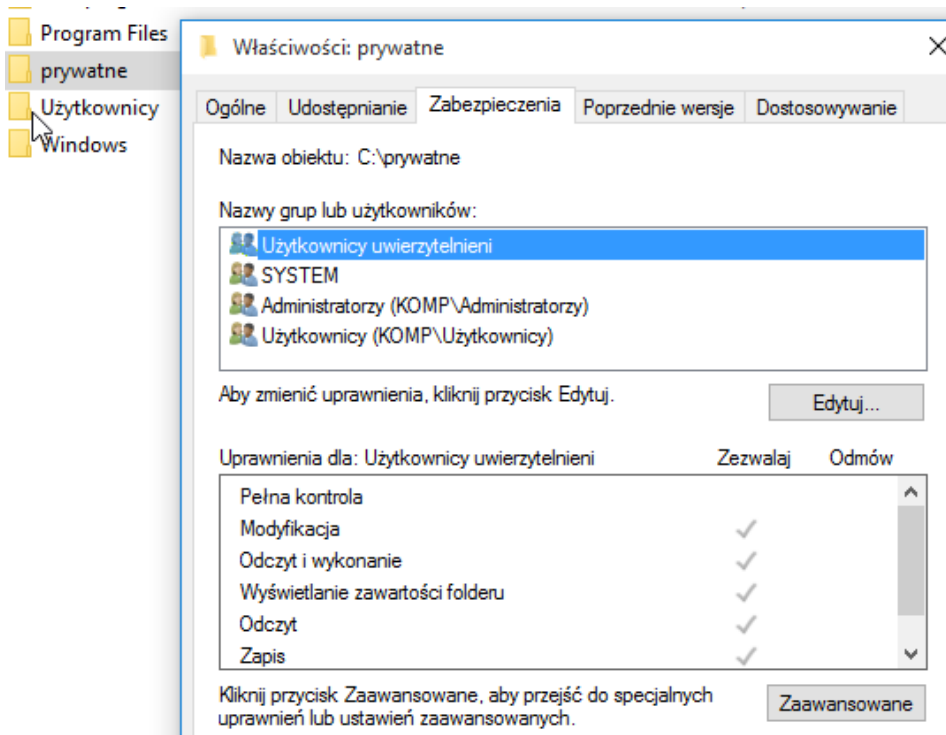
Właściciel folderu może w pełni nim zarządzać, w tym zabronić innym użytkownikom modyfikowania danych umieszczonych w tym folderze.

1. Upewnij się, że jesteś zalogowany do konta **bolek** bez hasła.
2. Na **C:\lokalnym** dysku NTFS utwórz nowy folder o nazwie **prywatne**.

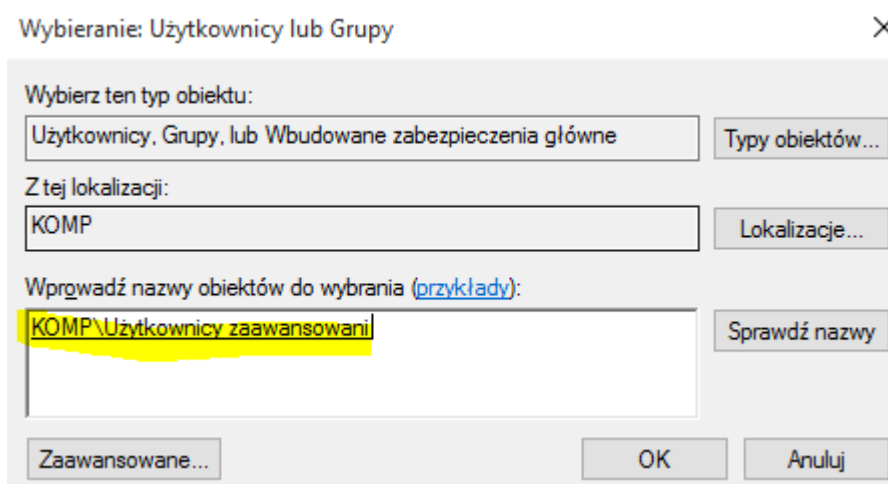
3. Przejdź do folderu **prywatne**.
4. Ustaw kursor myszki tak, aby nie wskazywał żadnego z elementów okna i naciśnij prawy przycisk myszy.
5. Z menu podręcznego wybierz opcję **Nowy | Dokument tekstowy**. W folderze zostanie utworzony nowy plik.
6. Przejdź do obiektu **Dysk lokalny C:** jest folder o nazwie **prywatne**.
Jeżeli w oknie właściwości nie znajduje się zakładka **Zabezpieczenia**:



7. Kliknij prawym przyciskiem myszy na folderze **prywatne** i z podręcznego menu wybierz opcję **Właściwości**.



8. W oknie **Właściwości: prywatne** wybierz zakładkę **Zabezpieczenia > Edytuj**.
9. Naciśnij przycisk **Dodaj**. W polu Wprowadź nazwę obiektów do wybrania wpisz (wklej) **Użytkownicy zaawansowani** i naciśnij **OK**.



10. Wyczyść pola **Zezwalaj** dla wierszy **Odczyt i wykonanie** oraz **Wyświetlanie zawartości folderu** i naciśnij przyciski **Zastosuj** i **OK**.
11. Sprawdź czy użytkownik **tola** nie może modyfikować danych umieszczonych w folderze **C:\prywatne**.
12. W zeszycie zapisz wnioski z wyżej wymienionych czynności.

(zgłoszenie) 2

Ćwiczenie 1.3. Odebranie uprawnień do folderu danej grupie użytkowników

Ponieważ użytkownik może być członkiem więcej niż jednej grupy odznaczenie opcji Zezwalaj dla niektórych tylko grup, w których znajduje się konto użytkownika nie powoduje odebranie mu praw do pliku lub folderu.

Dla kont użytkowników **bolek**, **lolek**, **tola** sprawdź który z użytkowników nadal ma dostęp do folderu **prywatne** i zapisz to w zeszycie.

1. Zaloguj się do konta **bolek**.
2. Kliknij prawym przyciskiem myszy na folderze **prywatne** i z menu podręcznego wybierz opcję **Właściwości > Zabezpieczanie**.
3. W polu Nazwy grupy lub użytkownika zaznacz **Użytkownicy zaawansowani > Edytuj**. Tytuł dolnego okna zostanie zmieniony na Uprawnienia dla Użytkownicy zaawansowani.
4. Zaznacz pole **Odmów** dla wiersza **Modyfikacja**. Ponieważ pozostałe uprawnienia (z wyjątkiem uprawnienia Pełna kontrola) zależą od uprawnienia do modyfikacji, system automatycznie potwierdzi odebranie tych uprawnień.
5. Naciśnij przycisk **Zastosuj**. Zostanie wyświetlony komunikat ostrzegający przed konsekwencjami jawnego odbierania uprawnień. Naciśnij przycisk **TAK > potwierdź**.
6. Sprawdź czy użytkownik **tola** nie będzie mógł modyfikować danych umieszczonych w tym folderze.
7. W zeszycie zapisz wnioski z wyżej wymienionych czynności.

(zgłoszenie) 3

Ćwiczenie 1.4. Nadawanie uprawnień do danego pliku

1. Przejdź do folderu **prywatne**.
2. Ustaw kursor myszki tak, aby nie wskazywał żadnego z elementów okna i naciśnij prawy przycisk myszy.
3. Z menu podręcznego wybierz opcję **Nowy | Obraz - mapa bitowa**. W folderze zostanie utworzony nowy plik.
4. Kliknij prawym przyciskiem myszy na ikonie nowego pliku i z podręcznego menu wybierz opcję **Właściwości**.
5. W polu **Właściwości: Nowy obraz – mapa bitowa** wybierz opcję **Zabezpieczenia**.

6. Naciśnij przycisk Edytuj > **Dodaj**. W polu **Wprowadź nazwę obiektów do wybrania** wpisz nazwę konta **lolek**.

Ponieważ to konto należy do pewnej grupy, automatycznie ma nadane, takie same jak grupa, uprawnienia do wszystkich obiektów znajdujących się w katalogu **prywatne**. Zaznacz opcję **Odmów** dla wiersza **Pełna kontrola**.

7. Naciśnij przycisk **Zastosuj** i **OK**.

8. W zeszycie opowiedz na pytania.

- Do jakich grup należy konto **lolek**?
- Jakie uprawnienia użytkownika konta **lolek** do pliku **Nowy obraz – mapa bitowa** zostały odebrane?
- Sprawdź czy po zalogowaniu do konta **lolek** w katalogu *poufne* jest niemożliwa modyfikacja pliku **Nowy obraz – mapa bitowa**?


(zgłoszenie) 4

Kopiowanie plików i folderów

Ponieważ każdy obiekt (taki jak plik lub folder) „dziedziczy” uprawnienia od folderu nadrzędnego, to podczas kopiowania i przenoszenia obiektów uprawnienia te mogą ulec zmianie.

Ćwiczenia 1.5. Zmiana właściwości kopiowanych obiektów

Kopiuwane lub przenoszone pomiędzy dyskami NTFS obiekty otrzymują uprawnienia nadrzędnego obiektu docelowego. Jedynym wyjątkiem od tej zasady jest przenoszenie obiektów w ramach pojedynczej partycji - wtedy obiekt zachowuje wszystkie swoje uprawnienia. Aby sprawdzić prawdziwość powyższej reguły:

1. Zaloguj się ponownie do konta **bolek**.
2. Otwórz folder **prywatne**.
3. Wyświetl i zapamiętaj uprawnienia poszczególnych grup i użytkowników do pliku **Nowy obraz – mapa bitowa**. Zapisz w zeszycie. (wykonaj zrzut ekranu)
4. Skopiuj plik do głównego katalogu na **D:** (inny dysk NTFS).
5. Wybierz 
6. Wyświetl uprawnienia do pliku **Nowy obraz – mapa bitowa**. (wykonaj zrzut ekranu)

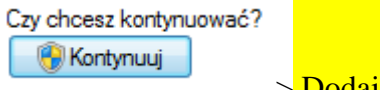
7. Zapisz w zeszycie zabezpieczenia i **wykonaj zrzut ekranu**, na którym będą okna **Zabezpieczenia** obydwu plików (**C:\ prywatne\ Nowy obraz – mapa bitowa** i **D:\ Nowy obraz – mapa bitowa**)
8. Na liście, którego pliku nie ma grupy **Użytkownicy zaawansowani** i użytkownika konta **lolek**
9. W zeszycie wyjaśnij, dlaczego na liście wskazanego pliku nie ma grupy **Użytkownicy zaawansowani** i użytkownika konta **lolek**.

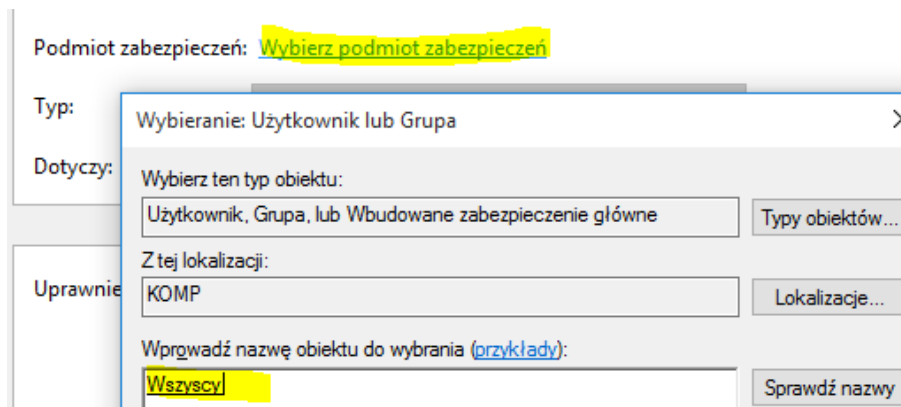
(zgłoszenie) 5

Inspekcja dostępu do danych

Ćwiczenie 1.6 Monitorowanie dostępu do katalogu

Celem ćwiczenia jest włączenie inspekcji dostępu do folderu **prywatne**.

1. Upewnij się, że jesteś zalogowany do konta **bolek**.
2. Uruchom menu **Start | Uruchom ... | secpol.msc**.
3. Rozwiń folder **Zasady lokalne** i wybierz opcję **Zasady inspekcji**.
4. Dwukrotnie kliknij zasadę **Przeprowadź inspekcję dostępu do obiektów**.
5. Zaznacz opcje **Sukces** oraz **Niepowodzenie**.
6. Naciśnij klawisz **OK** i zamknij okno konsoli **Zasady zabezpieczeń lokalnych**.
7. Kliknij prawym przyciskiem myszki na folderze **prywatne** i z menu podręcznego **Właściwości:prywatne** wybierz opcję **Zabezpieczanie**.
8. Wybierz opcje **Zabezpieczenia | Zaawansowane | Inspekcja**.
9. Kliknij przycisk  > **Dodaj**.
10. W polu **Wprowadź nazwę obiektów do wybrania** wpisz **Wszyscy**. Sprawdź poprawność nazwy i naciśnij **OK**.



11. Zostanie wyświetlone okno **Wpis inspekcji dla prywatne**. Zaznacz opcję **Powodzenie** i **Niepowodzenie** dla wiersza **Pełna kontrola**.

Uprawnienia podstawowe:

- Pełna kontrola
- Modyfikacja
- Odczyt i wykonanie
- Wyświetlanie zawartości folderu
- Odczyt
- Zapis
- Uprawnienia specjalne

12. Naciśnij klawisz **OK**. Zostanie zamknięte okno **Zaawansowane ustawianie zabezpieczeń dla prywatne**.
13. Naciśnij przycisk **OK**.

W praktyce nie stosuje się tak dokładnej modyfikacji obiektu. Monitorowanie dla każdego użytkownika zarówno udanych, jak i nieudanych prób dostępu w krótkim czasie skończyłoby się zapełnieniem **Dziennika zabezpieczenia**.

14. W zeszycie wyjaśnij jaka modyfikacja zawartości folderu **prywatne** zostanie odnotowana w **Dzienniku zabezpieczenia**.

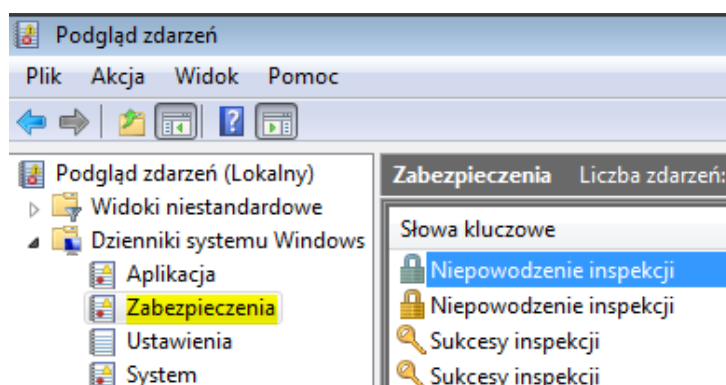
(zgłoszenie) 6

Ćwiczenie 1.7 Przeglądanie Dziennika zabezpieczenia

Aby sprawdzić kto modyfikował zawartość folderu **prywatne**:

1. Upewnij się, że jesteś zalogowany do konta **bolek**.
2. Uruchom menu **Start | Uruchom ... | eventvwr.msc | Podgląd zdarzeń**.

- Wybierz **Dziennik Zabezpieczenia**. W oknie po prawej stronie zostanie wyświetlona lista zarejestrowanych zdarzeń.



- Aby poznać więcej szczegółów o konkretnym zdarzeniu kliknij na nim dwukrotnie lewym przyciskiem myszki.
- W zeszycie wyjaśnij szczegóły konkretnego zdarzenia dotyczącego modyfikacji zawartości folderu **prywatne** które zostanie odnotowane w podglądzie zdarzeń *dziennika Zabezpieczenia*.

(zgłoszenie) 7

Zadania do samodzielnego wykonania

Ćwiczenie 1.8 Zaprojektuj w zeszycie, a następnie stwórz w systemie Windows strukturę katalogową w katalogu E:\1720 spełniającą następujące wytyczne

- bolek** pracuje w marketingu i zwykle zapisuje pliki w katalogu marketing.
- lolek** pracuje w finansach i zwykle zapisuje pliki w katalogu finanse.
- Użytkownicy **bolek** i **lolek** nie mogą zapisywać plików i katalogów poza katalogami: marketing, finanse.
- Użytkownicy **bolek** i **lolek** nie mogą zmieniać nazw i usuwać plików i katalogów poza katalogami: marketing, finanse.
- Użytkownicy **bolek** i **lolek** mogą pracować na wspólnych plikach w katalogach: marketing, finanse.
- W katalogach marketing i finanse znajdują się podkatalogi sekret, które zawierają pliki dostępne tylko dla (odpowiednio) marketingu i finansów.

(zgłoszenie) 8