Zabezpieczanie dostępu do plików katalogów - prawa NTFS.

Za pomocą systemu plików NTFS można ograniczyć dostęp do katalogów i plików znajdujących się na serwerze sieci Web. Można również skonfigurować poziom dostępu określonego użytkownika lub grupy do pliku i katalogów na serwerze czy stacji roboczej. Aby zaprojektować prawa dostępu należy zdawać sobie sprawę z następujących cech praw zaimplementowanych w NTFS.

Cechy praw NTFS

1. **Prawa się dziedziczą** - oznacza to, ze prawo nadane do folderu nadrzędnego obowiązuje w folderach podrzędnych.

    - Dane - User1 otrzymuje tu prawo ***Odczyt i Wykonanie***
      |-- Folder1
      |--Folder2
      | |PodfolderA
      | |
      |

    Dzięki dziedziczeniu prawo *Odczyt i wykonanie* obowiązuje również w folderze Folder1, Folder2, PodfolderA oraz folderach, które będą dopiero utworzone. Stosowanie dziedziczenia i poprawne rozmieszczenie plików w strukturze folderów zdecydowanie zmniejsza ilość miejsc, w których trzeba nadawać prawa.

2. **Istnieje równoważność zabezpieczeń** - oznacza iż jeden obiekt np. użytkownik ma prawa takie jak inny obiekt np. grupa.

    Jeżeli przypiszemy prawa grupie, to takie same prawa mają użytkownicy przypisani do grupy.

    - Dane - Grupa Pracownicy otrzymuje tu prawo ***Odczyt i Wykonanie***
      |-- Folder1
      |--Folder2
      | |PodfolderA

| |

|

Dzięki dziedziczeniu prawo *Odczyt i wykonanie* obowiązuje również w folderze Folder1, Folder2, PodfolderA oraz folderach, które zostaną dopiero utworzone. Ponadto dzięki równoważności zabezpieczeń wielu użytkowników (wszyscy członkowie grupy *Pracownicy*) otrzymuje prawa do folderu Dane.

3. **Prawa się sumują** - uprawnienia otrzymane dzięki przynależności do różnych grup sumują się dając prawa efektywne.

   - Dane - Grupa Pracownicy otrzymuje tu prawo ***Odczyt i Wykonanie***
     |-- Folder1
     |--Folder2 - grupa Kierownicy otrzymuje prawo ***Odczyt i Wykonanie***, ***Zapis***.
     | |--PodfolderA -
     | | |

   Prawa efektywne użytkownika, członka grupy *Pracownicy* i *Kierownicy* to suma praw obu grup czyli *Odczyt i wykonanie* oraz *Zapis*

   - Dane - Grupa Pracownicy otrzymuje tu prawo ***Odczyt i Wykonanie***
     |-- Folder1
     |--Folder2 - grupa Kierownicy otrzymuje prawo ***Zapis***.
     | |--PodfolderA -
     | | |

   Prawa efektywne użytkownika, członka grupy *Pracownicy* i *Kierownicy* to suma praw obu grup czyli *Odczyt i wykonanie* oraz *Zapis*

4. **Istnieją dwa rodzaje praw: Zezwalaj i Odmów** - jeżeli użytkownik ma obydwa prawa np. *zezwolenie na odczyt* oraz *odmówienie odczytu* to ważniejsze jest prawo odmów - użytkownik nie ma prawa na czytanie pliku. Jeżeli prawo zezwalaj jest nadane jawnie, a prawo odmów jest odziedziczone, to prawo zezwalaj ma pierwszeństwo.

- Dane - grupa Pracownicy otrzymuje tu prawo ***odmów Zapis.***
  | - grupa Użytkownicy otrzymuje tu prawo ***Odczyt i Wykonanie*** oraz ***Zapis***.
  |-- Folder1
  |--Folder2
  | |--PodfolderA
  | | |

Prawa efektywne użytkownika, członka grupy *Pracownicy* i *Użytkownicy* w folderze *Dane* to suma praw obu grup czyli: zezwalaj *Odczyt i wykonanie, Zapis,* odmów *Zapis.* Ponieważ użytkownik ma *zezwalaj Zapis i odmów Zapis* to prawo odmów ma pierwszeństwo i użytkownik nie może zapisać pliku w PodfolderA.

- Dane - Grupa Pracownicy otrzymuje tu prawo ***Odczyt i Wykonanie***
  oraz ***odmów Zapis.***
  |-- Folder1
  |--Folder2 - Grupa Kierownicy otrzymuje prawo **- zezwalaj *Zapis.***
  | |--PodfolderA | | |

Prawa efektywne użytkownika, członka grupy *Pracownicy* i *Kierownicy* w folderze *Folder2* to suma praw obu grup czyli: zezwalaj *Odczyt i wykonanie,* odmów *Zapis, zezwalaj Zapis.* Ponieważ użytkownik ma *zezwalaj Zapis i odmów zapis* to prawo odmów ma pierwszeństwo i użytkownik nie może zapisać pliku w PodfolderA. **To jest zła interpretacja. W tym przypadku prawo zezwalaj zostało nadane jawnie, to znaczy do folderu PdfolderA, a prawo odmów jest dziedziczone, więc pierwszeństwo ma prawo zezwalaj i użytkownik może czytać zawartość plików w Podfolder2 i poniżej.**

5. Właściciel pliku lub folderu w NTFS, może zmienić prawa do tego pliku lub folderu. Może dodać nowy obiekt do ACL lub zmienić prawa już tam istniejącego obiektu.

Operacje na plikach i katalogach a prawa NTFS

Wykonanie czynności na plikach typu zapisanie zmian w pliku, odczytanie zawartości pliku itp. wymagają odpowiednich praw. Tabela poniżej przedstawia niezbędne prawa do wykonania typowych zadań.

Tabela 1 Niezbędne prawa do wykonywania czynności na plikach i folderach.

Czynność / prawa	WZF	WZF, O	OiW	OiW, Z	M	PK
Zobaczyć listę plików i folderów	**T**	**T**	**T**	**T**	**T**	**T**
Zobaczyć atrybuty	**T**	**T**	**T**	**T**	**T**	**T**
Zobaczyć uprawnienia	F-**T**, P-N	**T**	**T**	**T**	**T**	**T**
Odczytać zawartość pliku	N	**T**	**T**	**T**	**T**	**T**
Uruchomić program	N	N	**T**	**T**	**T**	**T**
Zmienić atrybuty	N	N	N	**T**	**T**	**T**
Zapisać plik	N	N	N	**T**	**T**	**T**
Stworzyć plik	N	N	N	**T**	**T**	**T**
Stworzyć folder	N	N	N	**T**	**T**	**T**
Zmienić nazwę	N	N	N	N	**T**	**T**
Usunąć plik	N	N	N	N	**T**	**T**
Usunąć folder pusty	N	N	N	N	**T**	**T**
Usunąć folder z zawartością	N	N	N	N	**T**	**T**
Zmienić uprawnienia *	N	N	N	N	N	**T**
Przejąć na własność	N	N	N	N	N	**T**

* - niezależnie od przydzielonych praw na liście ACL właściciel pliku lub katalogu może zmienić uprawnienia obiektów znajdujących się w ACL oraz dodać nowy obiekt i nadać mu prawa. Jest to problem trudny do obejścia.

Legenda:
WZF - wyświetlanie zawartości folderu, **O** - odczyt, **OiW** - odczyt i wykonanie, **Z** - zapis, **M** - modyfikacja, **PK** - pełna kontrola, **P** - plik, **F** - folder

Jak uniemożliwić właścicielowi zmianę uprawnień do plików i katalogów?

Jest to proste w przypadku danych umieszczonych w udziale sieciowym, jeżeli użytkownik nie może zalogować się na serwerze lokalnie lub pulpitem zdalnym. Nadaj grupie Wszyscy tylko prawo **Zmiana** w ACL w zakładce *Udostępnianie* pod przyciskiem *Uprawnienia*.

Zasady nadawania praw do plików i katalogów

Aby użytkownicy mogli wykonywać swoje zadania, a administrator miał jak najmniej pracy przy nadawaniu uprawnień należy stosować następujące zasady:

1. Nadawaj minimum praw niezbędnych użytkownikowi do wykonania swojej pracy

2. Planuj rozmieszczenie danych w folderach tak, aby można było stosować dziedziczenie oraz nadawać niskie uprawnienia na górze drzewa do coraz większych w katalogach podrzędnych

3. Stosuj równoważność zabezpieczeń (nie nadawaj praw obiektom użytkownik)

4. Staraj się nie używać prawa odmów

5. Staraj się nie przerywać dziedziczenia. Przerywanie dziedziczenia i stosowanie prawa odmów komplikują zarządzanie uprawnieniami.

Wskazania przy stosowaniu uprawnień

- Uprawnienia należy przypisywać raczej grupom, a nie użytkownikom. Ponieważ bezpośrednie zarządzanie kontami użytkowników jest nieefektywne, przypisywanie uprawnień bezpośrednio użytkownikom należy stosować w sytuacjach wyjątkowych.

- Jeśli jest to możliwe, należy unikać zmieniania domyślnych uprawnień dla obiektów systemu plików, szczególnie w przypadku folderów systemowych i folderów głównych. Zmiana uprawnień domyślnych może spowodować nieoczekiwane problemy z dostępem lub obniżyć poziom bezpieczeństwa.

- Nigdy nie należy odmawiać dostępu do obiektu grupie Wszyscy. Jeśli grupa Wszyscy nie będzie miała dostępu do obiektu, obejmie to również administratorów. Lepszym rozwiązaniem jest usunięcie grupy Wszyscy, pod warunkiem, że uprawnienia do tego obiektu będą przydzielane innym użytkownikom, grupom lub komputerom. Może być również konieczne udzielenie uprawnienia Pełna kontrola grupie Administratorzy i kontu System lokalny.

- Dziedziczone uprawnienia Odmów nie uniemożliwiają dostępu do obiektu, jeśli obiekt ma jawny wpis uprawnienia Zezwalaj. Jawne uprawnienia mają wyższy priorytet od uprawnień odziedziczonych, nawet od odziedziczonych uprawnień Odmów.

- Uprawnienia Odmów powinny być używane tylko w następujących szczególnych przypadkach:

    - Aby wykluczyć podzbiór grupy mającej uprawnienia Zezwalaj.

    - Aby wykluczyć jedno specjalne uprawnienie, gdy użytkownikowi lub grupie zostało już przypisane uprawnienie Pełna kontrola.

- Należy zachować ostrożność podczas konfigurowania uprawnień NTFS dla witryny sieci Web. Niewłaściwie ustawione uprawnienia mogą uniemożliwić uprawnionym użytkownikom dostęp do żądanych plików i katalogów. Na przykład nawet jeśli użytkownik ma właściwe prawa do oglądania i wykonywania programu, może nie

mieć uprawnień do dostępu do określonej biblioteki DLL, wymaganej do uruchomienia tego programu. Aby zagwarantować użytkownikom bezpieczny i niezakłócony dostęp do plików, należy umieścić powiązane ze sobą pliki w tym samym katalogu, a następnie przypisać odpowiednie uprawnienia NTFS do katalogu.

Problemy początkujących administratorów

1. Użytkownik otrzymał prawo w udziale sieciowym Modyfikacja, a nie może utworzyć pliku, zapisać ani usunąć.

   Wyjaśnienie - Użytkownik doświadcza praw zdefiniowanych w zakładce Zabezpieczenia - NTFS oraz Uprawnienia - dostęp przez sieć. Domyślnie w Zakładce Udostępnianie pod przyciskiem Uprawnienia znajdziemy obiekt *Wszyscy* z uprawnieniami *Odczyt*. Użytkownik posiadający prawa do pliku w NTFS i zakładce Udostępnianie doświadcza praw bardziej restrykcyjnych - nie sumy. Odczyt odpowiada Odczytowi i Wykonaniu w NTFS, Zmiana Modyfikacji, a Pełna Kontrola Pełnej Kontroli. Na przykład prawa w NTFS Modyfikacja, przez sieć Odczyt daje razem prawo Odczyt i Wykonanie.

   Rozwiązanie - w zakładce udostępnianie pod przyciskiem Uprawnienia zdefiniowane są prawa dostępu przez sieć. Nadaj obiektowi Wszyscy prawo zezwalaj Zmiana. Zmiana odpowiada Modyfikacji , a Pełna kontrola Pełnej kontroli. Domyślnie w ACL występuje obiekt wszyscy z uprawnieniami Odczyt.

2. Użytkownik posiada prawa w ACL NTFS Odczyt i Wykonanie, a pomimo to może tworzyć pliki i katalogi.

   Wyjaśnienie- zapomniano o sumowaniu praw i równoważności zabezpieczeń. Każdy użytkownik należy do grupy Użytkownicy, do której jest dodawany przez system w czasie operacj tworzenia użytkownika. W systemie plików w katalogu głównym grupa Użytkownicy ma prawo do tworzenia folderów, a w podkatalogach również do tworzenie plików. Tak więc członek grupy, która ma prawo Wyświetlanie Zawartości Folderów jest zwykle członkiem grypy Użytkownicy i dzięki dziedziczeniu, równoważności zabezpieczeń oraz sumowaniu praw jego prawa efektywne umożliwiają tworzenie plików i katalogów.

   Rozwiązanie - Przerwij dziedziczenie praw z katalogu nadrzędnego, usuń z ACL grupę użytkownicy, nadaj prawa według potrzeb.

3. Grupa Użytkownicy ma prawo Odczyt i wykonanie oraz prawo specjalne Tworzenie plików i Tworzenie folderów, a pomimo to może usuwać stworzone foldery i pliki.

   Wyjaśnienie - Domyślnie w ACL katalogu głównego istnieje grupa Twórca/Właściciel. Standardowo ma przydzielone prawo *Pełna kontrola*. Do tej grupy, w stosunku do utworzonego katalogu lub pliku, należy użytkownik który stworzył plik lub katalog. Tak więc, użytkownik tworzy plik posiadając np. prawo *Wyświetlanie zawartości folderu* i *Tworzenie folderu* dzięki grupie Twórca/Właściciel posiada do stworzonego folderu pełne prawa.

   Rozwiązanie - przerwij dziedziczenie praw i usuń grupę Twórca/Właściciel lub przerwij dziedziczenie i zmień prawa grupy Twórca/Właściciel na odpowiednie do potrzeb. Nie zapomnij, że Właściciel folderu/pliku może zmieniać uprawnienia, czyli może je sobie lub innym obiektom podwyższyć.