T: Kontrolowany dostęp.

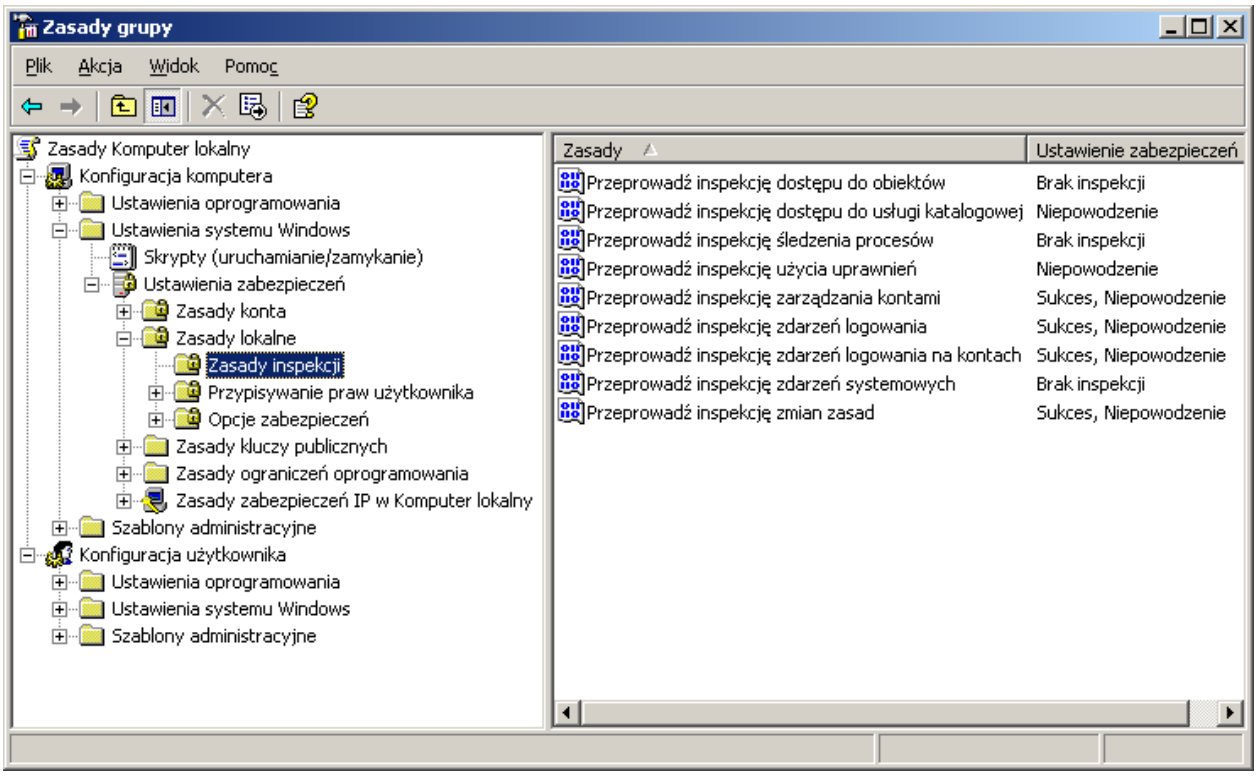
W środowisku domenowym Windows użytkownik, logując się do domeny, uzyskuje automatycznie dostęp do zasobów tej domeny. Podczas logowania się klient podaje nazwę konta i hasło. Zanim ktokolwiek zostanie dopuszczony przez system do korzystania z zasobów, musi zostać uwierzytelniony przez kontroler domeny. W zależności od wyniku tego procesu użytkownik otrzymuje (bądź nie) prawo do korzystania z sieci.

Z każdym kontem użytkownika (a także grupą) jest skojarzony numer ID zabezpieczeń (SID-Security IDentification Number). SID jest generowany w chwili tworzenia konta i jednoznacznie je identyfikuje przez cały okres jego istnienia. System wykorzystuje ten unikatowy numer, a nie nazwę konta, przy sterowaniu dostępem użytkownika do wszystkich zasobów. Usunięcie i ponowne utworzenie obiektu (np. konta użytkownika) sprawia, że konto ma zupełnie inny identyfikator, czyli z punktu widzenia systemu jest to całkowicie nowy obiekt.

Gdy użytkownik logujący się do domeny Windows zostaje uwierzytelniony, wówczas tworzona jest dla niego przepustka dostępu (Access Token), zawierająca ciąg informacji wykorzystywanych później przy ubieganiu się użytkownika o dostęp do zasobów systemu. Znajduje się w niej m.in. identyfikator SID użytkownika oraz identyfikatory SID wszystkich grup, do których użytkownik należy. Przepustka dostępu identyfikuje użytkownika w sieci przez cały czas trwania sesji. Ponieważ Access Token jest tworzony podczas logowania, więc jeśli zmienimy przynależność użytkownika do grup, zmiana ta zacznie obowiązywać dopiero po ponownym zalogowaniu użytkownika.

Każdy program oraz proces uruchomiony w kontekście konta użytkownika wyposażony jest w kopię jego przepustki. Jeśli klient żąda dostępu do obiektu, przepustka jest wykorzystywana do sprawdzenia, jakie uprawnienia do tego obiektu ma użytkownik. Porównuje się w tym celu identyfikatory użytkownika i grup, do których przynależy z listą kontroli dostępu obiektu (ACL Access Control List).

Każdy obiekt (plik, folder) ma listę kontroli dostępu ACL, zawierającą spis wszystkich użytkowników i grup mających prawa do tego obiektu wraz z uprawnieniami. Lista ta jest porównywana z przepustką użytkownika żądającego dostępu do zasobu. Jeśli na liście znajduje się identyfikator użytkownika lub grupy, do której on należy, klient uzyskuje dostęp do zasobu, zgodnie z należnym mu poziomem uprawnień. W odróżnieniu od Access Token, jeśli zmieniamy uprawnienia do obiektu, zmiana będzie oczywiście obowiązywać od razu, w



trakcie tej samej sesji, przy próbie ponownego dostępu do obiektu, gdyż Access Control List będzie wtedy ponownie porównana z Access Token.

W Windows XP dostęp do obiektu może być kontrolowany poprzez różnego rodzaju uprawnienia (read, write, change, no access i inne). W celu sprawdzenia, jak wygląda lista kontroli dostępu dowolnego obiektu, należy wybrać kartę Zabezpieczenia z opcji Właściwości danego obiektu.

Więcej informacji na: http://www.pckurier.pl/archiwum/art0.asp?ID=4319

Zagadnienia warte uwagi
- W celu zwiększenia bezpieczeństwa należy włączyć rejestrację zdarzeń w systemie za pomocą zasad zabezpieczeń. Informacje zarejestrowane przez system zostaną zapisane w plikach zlokalizowanych domyślnie w katalogu **%windir%\system32\config**. Odczytanie zarejestrowanych informacji umożliwia narzędzie administracyjne **Podgląd zdarzeń**.

Active Directory jest składnikiem Local Security Authority. Składniki podsystemu bezpieczeństwa działają w kontekście procesu Lsass.exe i zawierają następujące elementy:
- Local Security Authority,
- usługa Net Logon,
- usługa Security Accounts Manager,
- usługa LSA Server,
- Secure Sockets Layer,
- protokoły uwierzytelniania Kerberos V5 i NTLM.

Podsystem bezpieczeństwa monitoruje założenia bezpieczeństwa i w efekcie ma wpływ na cały system operacyjny.

Local Security Authority (LSA) jest modułem chronionym, który utrzymuje bezpieczeństwo lokalne systemu (zwane założeniami bezpieczeństwa lokalnego - Local Security Policy). Generalnie LSA pełni cztery podstawowe funkcje:
- zarządza założeniami bezpieczeństwa lokalnego,
- dostarcza interaktywnych usług logowania użytkownika,
- generuje znaczniki, zawierające informacje o użytkownikach i grupach, dotyczące przywilejów użytkownika w zakresie bezpieczeństwa,
- zarządza zasadami i ustawieniami nadzorowania oraz zapisuje ostrzeżenia do właściwego dziennika systemowego.

Więcej informacji na: http://technet2.microsoft.com/windowsserver/pl/library/7364fdca-ae55-4f9a-a8e9-88b71b45cd021045.mspx?mfr=true

Kontrola dostępu w usłudze Active Directory
Dla celów zabezpieczeń administratorzy mogą używać kontroli dostępu do zarządzania dostępem użytkowników do zasobów udostępnionych. W usłudze Active Directory kontrolą dostępu administruje się na poziomie obiektu, ustawiając różne poziomy (inaczej uprawnienia) dostępu do obiektów, takie jak Pełna kontrola, Zapis, Odczyt lub Brak dostępu. Kontrola dostępu w usłudze Active Directory określa, w jaki sposób różni użytkownicy mogą korzystać z obiektów usługi Active Directory. Domyślnie uprawnienia do obiektów w usłudze Active Directory są ustawione na wartości najbezpieczniejsze.
Do elementów, które określają uprawnienia kontroli dostępu do obiektów usługi Active Directory, należą: deskryptory zabezpieczeń, dziedziczenie uprawnień do obiektów i uwierzytelnianie użytkowników.

Deskryptory zabezpieczeń
Przez przypisywanie uprawnień kontroli dostępu do obiektów udostępnionych i obiektów usługi Active Directory można sterować tym, w jaki sposób różni użytkownicy mogą korzystać z każdego obiektu. Obiekt udostępniony, inaczej zasób udostępniony, to obiekt używany za pośrednictwem sieci przez jednego lub wielu użytkowników. Takim obiektem może być plik, drukarka, folder lub usługa. Zarówno obiekty udostępnione, jak i obiekty usługi Active Directory przechowują uprawnienia kontroli dostępu w deskryptorach zabezpieczeń.

Deskryptor zabezpieczeń zawiera dwie listy kontroli dostępu (ACL) używane do przypisywania i śledzenia informacji o zabezpieczeniach dla każdego obiektu: listę arbitralnej kontroli dostępu (DACL) i listę systemowej kontroli dostępu (SACL).

- Listy arbitralnej kontroli dostępu (DACL). Listy DACL identyfikują użytkowników i grupy, którym udzielono lub odmówiono uprawnień dostępu do obiektu. Jeśli lista DACL w sposób jawny nie identyfikuje użytkownika ani żadnych grup, których członkiem jest użytkownik, użytkownikowi odmawiany jest dostęp do danego obiektu. Domyślnie listę DACL kontroluje właściciel lub twórca obiektu i zawiera ona wpisy kontroli dostępu (ACE), które określają poziom dostępu użytkownika do obiektu.
- Listy systemowej kontroli dostępu (SACL). Listy SACL identyfikują użytkowników i grupy, których pomyślne i niepomyślne próby uzyskania dostępu do obiektów mają być poddane inspekcji. Inspekcja jest używana do monitorowania zdarzeń związanych z zabezpieczeniami systemu lub sieci, do identyfikowania przypadków złamania zabezpieczeń oraz do określania rozmiaru i lokalizacji wszelkich szkód. Domyślnie listę SACL kontroluje właściciel lub twórca obiektu. Lista SACL zawiera wpisy kontroli dostępu (ACE), które określają, czy mają być rejestrowane pomyślne lub niepomyślne próby uzyskania dostępu do obiektu przez użytkownika z danym uprawnieniem, na przykład Pełna kontrola lub Odczyt.

Aby wyświetlić listy DACL i SACL obiektów usługi Active Directory za pomocą przystawki Użytkownicy i komputery usługi Active Directory, w menu Widok kliknij polecenie Opcje zaawansowane, a następnie kartę Zabezpieczenia dla każdego obiektu. Do zarządzania listami kontroli dostępu w usłudze Active Directory można również używać narzędzia obsługi DSACLS.
Domyślnie listy DACL i SACL są skojarzone z każdym obiektem usługi Active Directory, co zmniejsza niebezpieczeństwo ataków złośliwych użytkowników na sieć i przypadkowych pomyłek użytkowników domeny. Jeśli jednak złośliwy użytkownik uzyska nazwę użytkownika i hasło dowolnego konta z poświadczeniami administracyjnymi dla usługi Active Directory, las będzie narażony na ataki. Z tego powodu należy wziąć pod uwagę zmianę nazwy lub wyłączenie domyślnego konta administratora.

Dziedziczenie uprawnień do obiektów
Domyślnie obiekty usługi Active Directory dziedziczą wpisy ACE deskryptora zabezpieczeń ich obiektu nadrzędnego (kontenera). Dziedziczenie pozwala na stosowanie informacji kontroli dostępu określonych dla kontenera w usłudze Active Directory do deskryptorów zabezpieczeń jego dowolnych obiektów podrzędnych, w tym innych kontenerów i ich obiektów. Eliminuje to konieczność stosowania uprawnień za każdym razem, gdy jest tworzony obiekt podrzędny. Jeśli to konieczne, odziedziczone uprawnienia można zmienić. Zaleca się jednak, aby unikać zmieniania uprawnień domyślnych i odziedziczonych ustawień obiektów usługi Active Directory.