Bezpieczeństwo w Windows Server 2003. Kompendium

Autor: Roberta Bragg
Tłumaczenie: Paweł Gonera, Piotr Pilch
ISBN: 83-246-0232-1
Tytuł oryginału: Windows Server 2003 Security: A Technical Reference
Format: B5, stron: 1170

We współczesnym świecie, w którym informacja jest najcenniejszym towarem, bezpieczeństwo danych to jedno z najważniejszych zagadnień spędzających sen z powiek administratorom serwerów i systemów. Mechanizmy zabezpieczeń oferowane przez system operacyjny powinny zostać odpowiednio skonfigurowane i wykorzystane we właściwy sposób. Sama wiedza na ich temat to zdecydowanie za mało. Należy poznać nie tylko zagadnienia związane z ich stosowaniem, ale również zasady ogólnej polityki bezpieczeństwa, doboru identyfikatorów i haseł sieciowych oraz korzystania z zabezpieczeń takich, jak klucze publiczne.

Książka „Bezpieczeństwo w Windows Server 2003. Kompendium" to praktyczny przewodnik po tych kwestiach. Autorka książki, ceniona specjalistka w zakresie bezpieczeństwa systemów operacyjnych z rodziny Windows, przedstawia w niej informacje niezbędne, aby skutecznie zabezpieczyć sieć i serwery. Porusza wszystkie zagadnienia związane z projektowaniem, wdrażaniem, diagnozowaniem lub konfigurowaniem zabezpieczeń systemu Windows Server 2003 lub sieci, w których znajdują się komputery z tym systemem.

W książce poruszono między innymi:

- Zasady bezpieczeństwa informacji
- Uwierzytelnianie za pomocą protokołów LM i Kerberos
- Kontrola dostępu na poziomie uprawnień
- Zabezpieczanie aplikacji i danych
- Wykorzystanie usługi Active Directory
- Tworzenie, wdrażanie i diagnozowanie zasad grupy
- Stosowanie mechanizmów klucza publicznego (PKI)
- Zabezpieczanie zdalnego dostępu do serwera
- Archiwizacja i odtwarzanie danych
- Wykrywanie włamań i reagowanie na ataki

Zmień swoją sieć w twierdzę nie do zdobycia

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

ROZDZIAŁ 4.

Ograniczanie dostępu do oprogramowania i kontrolowanie dostępu aplikacji do zasobów

Celem wielu obecnie przeprowadzanych ataków zakończonych powodzeniem jest warstwa aplikacji. Jest to wynikiem wykorzystywania luk występujących w oprogramowaniu innym niż system operacyjny. Choć tego typu ataki powodują spore problemy, wiele innych, równie poważnych jest wywoływanych przez przypadkowe działania użytkowników, takie jak klikanie załączników do wiadomości pocztowych, pobieranie aplikacji z internetu i niewłaściwe korzystanie z nich. Wymienione operacje mogą doprowadzić do przypadkowego usunięcia danych, utraty ich integralności i dostępu do zaszyfrowanych danych. Choć trzeba zwiększać poziom zabezpieczeń w celu ochrony aplikacji przed szkodliwymi atakami, konieczne jest tworzenie oprogramowania pozbawionego luk i szkolenie użytkowników pod kątem podejmowania lepszych decyzji. Trzeba się też zastanowić nad tym, czy można lepiej projektować aplikacje i zarządzać nimi.

Być może rozwiązaniem jest uniemożliwianie stosowania określonych aplikacji. Może powinno się tak konfigurować systemy, aby dozwolone było uruchamianie wyłącznie zaakceptowanego oprogramowania. To może być pomocne. W końcu,

gdy szkodliwy program nie może zostać uaktywniony, nie będzie w stanie spowodować szkód. Być może lepsze rezultaty od tworzenia kodu źródłowego aplikacji zgodnie z regułami bezpieczeństwa przyniesie zastosowanie w oprogramowaniu środków pozwalających zarządzać na poziomie aplikacji prawami użytkownika i dostępem do zasobów. Można to osiągnąć przy użyciu składników systemu Windows Server 2003 takich jak:

- **Listy kontroli dostępu ACL plików, rejestru, drukarek i obiektów usługi Active Directory**. Definiując dla pliku programu wykonywalnego odpowiednią listę ACL, uniemożliwi się jego uruchomienie przez nieupoważnione osoby. Z kolei konfigurując listy ACL plików, obiektów usługi Active Directory i rejestru, można zapobiec wykonywaniu przez nieupoważnione osoby określonych zadań za pomocą aplikacji, a także uniemożliwić im kopiowanie plików w inne miejsca dysku twardego. Listy ACL plików i rejestru wstępnie omówiono w rozdziale 3. Więcej informacji na ich temat można znaleźć w rozdziale 5.

- **Narzędzie *Menedżer autoryzacji***. Będące nowością w systemie Windows Server 2003 narzędzie umożliwia projektantom uwzględnianie w tworzonych aplikacjach modelu zabezpieczeń opartego na rolach. Zarządzanie przez administratorów eksploatacją takiej aplikacji polega na dodawaniu użytkowników do grup systemu Windows, a także grup aplikacji, podstawowych grup aplikacji i grup kwerend LDAP. Narzędzie *Menedżer autoryzacji* pozwala również decydować o tym, kto będzie mógł uaktywniać określone składniki aplikacji funkcjonującej w systemie.

- **Zasady ograniczeń oprogramowania**. Tego typu zasady, będące nowością w systemach Windows XP Professional i Windows Server 2003, umożliwiają blokowanie uruchamiania wybranych aplikacji lub mogą być użyte do tego, aby na komputerze mogło być uaktywniane wyłącznie zidentyfikowane oprogramowanie.

- **Konsola *Usługi składowe* — uprawnienia i role dla aplikacji COM+**. Aplikacje mogą być zarządzane za pomocą narzędzia *Usługi składowe*. Aby aplikacje COM+ były w pełni efektywne, trzeba je projektować z uwzględnieniem zdefiniowanych ról. W przeciwnym razie administrator będzie jedynie mógł modyfikować uprawnienia związane z uruchamianiem i poziomy uwierzytelniania. Nowością w systemie Windows Server 2003 jest możliwość określenia poziomu zabezpieczeń ograniczających aplikację COM+ bezpośrednio w oknie jej właściwości.

- **Przystawka *Zasady grupy***. Wiele aplikacji może być zarządzanych za pomocą przystawki *Zasady grupy*. Odpowiednie ustawienia nadzorujące systemowe aplety są zlokalizowane w węźle *Szablony administracyjne* znajdującym się w oknie przystawki *Zasady grupy*.

Dla produktów takich jak Microsoft Office są dostępne specjalne szablony administracyjne. Korzystanie z szablonów zawartych w oknie przystawki *Zasady grupy* omówiono w rozdziale 7.

- **System EFS (*Encrypting File System*)**. Pliki aplikacji mogą być szyfrowane za pomocą systemu EFS. Podstawowe informacje na jego temat zamieszczono w rozdziale 6.

Do trzech podstawowych narzędzi zarządzających oprogramowaniem w systemie Windows Server 2003 zaliczają się: program *Menedżer autoryzacji*, zasady ograniczeń oprogramowania i konsola *Usługi składowe*. W niniejszym rozdziale opisano je i wyjaśniono, w jaki sposób ich używać.

Narzędzie Menedżer autoryzacji

Narzędzie *Menedżer autoryzacji* umożliwia projektowanie aplikacji RBAC (*Role-Based Access Control*) kontrolujących dostęp w oparciu o role, a także pozwala na administrowanie nimi. Tworząc aplikacje RBAC i definiując używane przez nie role użytkowników, projektanci korzystają z interfejsu API (*Application Programming Interface*) narzędzia *Menedżer autoryzacji*. Aby móc zarządzać aplikacjami, co polega na przypisywaniu grupom użytkowników definicji ról, administratorzy posługują się przystawką *Menedżer autoryzacji* konsoli MMC (*Microsoft Management Console*).

Zanim będzie można administrować aplikacjami RBAC, trzeba zrozumieć, w jaki sposób są projektowane i jak działają. Kluczem do opanowania narzędzia *Menedżer autoryzacji* jest uświadomienie sobie, że w jego przypadku odpowiedzialność za podział dostępu do zasobów przechodzi z administratora na aplikację.

Aplikacja zgodna z narzędziem *Menedżer autoryzacji* jest tak zaprojektowana, aby reagować na rolę użytkownika, który z niej korzysta. Rola, będąca częścią aplikacji, ma na celu przekazanie praw i uprawnień zezwalających posiadaczowi roli wykonać powierzone mu zadania i nic ponadto. Przykładowo, rola może umożliwiać uaktywnianie wybranych składników aplikacji, a także pozwalać na odczyt określonych danych i jednocześnie zapisywanie, usuwanie lub przetwarzanie innych danych. Początkowo można odnieść wrażenie, że rola umożliwia projektantowi sprawowanie nadzoru nad zasobami komputera. Jednak w przypadku właściwie zarządzanego środowiska projektowania programiści bazują na specyfikacjach opracowanych przez właścicieli danych i muszą ich przestrzegać. Przykładowo, aplikacja stworzona w celu drukowania listy płac może dysponować rolą pracownika i kierownika, którzy są za to odpowiedzialni. Pracownicy działu obsługującego listy płac muszą przygotować specyfikacje określające, na

wykonanie jakich operacji w programie poszczególne role zezwalają, a także jakie pliki i drukarki zostaną udostępnione rolom użytkowników. Kierownictwo działu zatwierdza następnie specyfikacje i powiadamia informatyków, którym pracownikom i jakie powinni przydzielić role. Administrator systemu zarządza aplikacją, przypisując jej role odpowiednim użytkownikom.

Dla porównania, zwykła aplikacja kiepsko sobie radzi z nadawaniem i odbieraniem dostępu do zasobów. Taka aplikacja postrzega magazyn danych jako „szary krajobraz" złożony z obiektów, które mogą być przetwarzane lub nie, co przede wszystkim zależy od kontekstu zabezpieczeń użytkownika. Gdy zwykła aplikacja musi komunikować się z wewnętrznymi procesami komputera, przełącza kontekst i działa zgodnie z tym, jak ją zaprogramowano, ignorując kontekst zabezpieczeń użytkownika. A zatem zarządzanie taką aplikacją jest ułomne. Upoważnianie do uruchomienia aplikacji jest niezależne od praw dostępu do zasobów. Aby zarządzać zwykłymi aplikacjami, administrator systemu musi jedynie zdecydować, kto będzie mógł je uaktywniać. Oddzielnie zarządza się zasobami, do których program będzie mógł uzyskać dostęp. Administrator chroni zasoby, określając, jakie prawa powinny być użytkownikowi nadane lub odebrane i do których obiektów powinno mu się udzielić dostępu. Autoryzacja powiązana z aplikacją i zasobami jest rozłączona. Co więcej, choć administrator może przypisać użytkownikowi uprawnienie pozwalające mu uruchamiać określony program, może nie być w stanie przydzielić mu prawa do uaktywniania wybranego składnika aplikacji i jednocześnie zablokować dostęp do jej pozostałych komponentów. Istnieją wyjątki. Zarówno programy bazodanowe, jak i aplikacje COM+ mogą dysponować rolami, które zdefiniowano w ich strukturze. Administratorzy bazy danych przypisują użytkownikom role bazodanowe.

W dobrze zdefiniowanym i dość statycznym środowisku administrator systemu może radzić sobie z zarządzaniem zwykłą aplikacją i zadaniami związanymi z nadawaniem praw i uprawnień. W dobrze zarządzanym środowisku właściciele danych określają, kto i jak może je przetwarzać, natomiast administrator jest w stanie do tych wymagań dostosować model uwierzytelniania stosowany przez system operacyjny. W dość statycznym środowisku zmiany zachodzą powoli, dlatego dysponuje się czasem pozwalającym na podjęcie decyzji dotyczących nowych aplikacji i rozważenie ich wpływu na starsze programy. Jednak wiele organizacji nie posiada dobrze zdefiniowanego lub w miarę statycznego środowiska. Zmiany zachodzą w nich szybko, natomiast posiadacze danych i administratorzy czasami nie współpracują ze sobą odpowiednio. Ponadto często akceptuje się aplikacje, które wymagają zwiększenia przywilejów, nie dlatego, że są im niezbędne do funkcjonowania, ale ze względu na to, że są kiepskiej jakości.

Receptą na udane zastosowanie narzędzia *Menedżer autoryzacji* jest uświadomienie sobie, że nie rozwiąże ono problemów powstałych w przeszłości. Nie może zarządzać nieobliczalnymi aplikacjami lub w magiczny sposób sprawić, że

administrator zostanie zwolniony z obowiązku nadawania praw i uprawnień. Narzędzie *Menedżer autoryzacji* jest w stanie zaoferować infrastrukturę, z myślą o której mogą być projektowane aplikacje. Infrastruktura pozwoli zmienić model zarządzania, którym posługiwał się dotąd administrator. W przypadku aplikacji zgodnych z narzędziem *Menedżer autoryzacji* administrator nie musi udzielać dostępu do obiektów poszczególnym użytkownikom lub grupom. Wystarczy, że dostosuje się do specyfikacji właścicieli aplikacji, w której określą, kto i jaką może w nich pełnić rolę.

Jeśli takie rozwiązanie jest zadowalające, trzeba będzie rozpocząć współpracę z właścicielami danych i projektantami aplikacji, aby uzyskać programy, które będą mogły być zarządzane za pomocą narzędzia *Menedżer autoryzacji*. Omawianie tworzenia aplikacji RBAC wykracza poza zakres książki, natomiast zarządzanie nimi przy użyciu narzędzia *Menedżer autoryzacji* będzie tu omówione. Może się okazać, że zostanie się poproszonym o administrowanie tego typu aplikacją lub będzie się miało duży wpływ na to, czy tworzone aplikacje będą zgodne z narzędziem *Menedżer autoryzacji*, a tym samym czy zapewnią kontrolę dostępu opartą na rolach.

UWAGA: Dostępność narzędzia *Menedżer autoryzacji* w przypadku innych wersji systemu Windows

Interfejs API narzędzia *Menedżer autoryzacji* dla systemu Windows 2000 umożliwiający tworzenie aplikacji RBAC można pobrać pod adresem *http://www.microsoft.com/downloads/details.aspx?FamilyID=7edde11f-bcea-4773-a292--84525f23baf7&display-lang=en*. Aplikacje zgodne z tym narzędziem mogą być zarządzane wyłącznie za pomocą przystawki *Menedżer autoryzacji* oferowanej przez system Windows Server 2003 lub Windows XP Professional (z zainstalowanym pakietem Windows Server 2003 Administration Tools Pack). Aby możliwe było utworzenie w bazie danych usługi Active Directory magazynów narzędzia *Menedżer autoryzacji*, dla domeny musi być ustawiony poziom funkcjonalności systemu Windows Server 2003.

KONTROLA DOSTĘPU W SYSTEMIE WINDOWS OPARTA NA ROLACH

Bez wymogu użycia narzędzia *Menedżer autoryzacji* kontrola dostępu oparta na rolach jest dostępna w systemach Windows wykorzystujących technologię NT. Zastosowanie tego typu kontroli w poprzednich wersjach systemu Windows wymagało od administratorów zdefiniowania ról. W tym celu musieli wykonać następujące operacje:

- Utworzenie grup systemu Windows.
- Przypisanie grupom odpowiednich praw użytkownika.
- Zdefiniowanie list kontroli dostępu ACL dla zasobów takich jak pliki, foldery, klucze rejestru i obiekty usługi Active Directory.

- Dodanie kont do utworzonych grup lub ich usunięcie, gdy poszczególne osoby zaczynają pracę w firmie lub z niej odchodzą bądź zmieniają stanowiska.
- Uwzględnienie w aplikacjach niestandardowych ról w ramach współpracy z programistami. Dotyczy to aplikacji .NET, aplikacji COM+ i programów opartych na starszych modelach programistycznych.

Nie ma nic złego w tego typu modelu postępowania. Jednak powodzenie jego wdrożenia w dużej mierze zależało od zarządzania uprawnieniami dużej liczby obiektów. Gdy jest to dobrze robione, użytkownicy mogą wykonywać powierzone im obowiązki. Ale gdy tak nie jest, niewłaściwe osoby często uzyskują dostęp, którym nie powinny dysponować, natomiast użytkownicy faktycznie wymagający praw i uprawnień mogą nie być w stanie pracować. Frustracja staje się częścią dnia każdego administratora i użytkownika. Ostatecznie w zabezpieczeniach mogą zostać utworzone luki tylko dlatego, aby użytkownicy mogli wykonać swoje zadania. Skalowanie tego typu modelu jest szczególnie utrudnione, gdy ma miejsce wysoki poziom zmian kadrowych i szybko pojawiają się nowe stanowiska. Choć model jest bardzo elastyczny i w zakresie uprawnień do obiektów umożliwia szczegółową kontrolę, nie pozwala na precyzyjne zarządzanie sposobem wykorzystania oprogramowania.

Problem nie polegał na konieczności znalezienia metody kontrolowania aplikacji RBAC, ale bardziej na tym, w jaki sposób powinny być realizowane następujące zadania:

- Definiowanie ról. Kto, co, na jakich komputerach i za pomocą jakich aplikacji może robić? Czym się zajmują poszczególne osoby?
- Translacja pełnionej funkcji na zestaw uprawnień do obiektów. Które programy wymagają dostępu do których plików, drukarek lub kluczy rejestru w przypadku poszczególnych ról?
- Zdefiniowanie odpowiedzialności za odwzorowywanie funkcji, praw, uprawnień. Kto powinien się tym wszystkim zająć?
- Określenie odpowiedzialności za wdrażanie, zarządzanie i audyt ról, a także ich przypisywanie. Kto tak naprawdę powinien konfigurować komputer, sprawdzać, czy wszystko działa zgodnie z oczekiwaniami, i przeprowadzać inspekcję ról i ich przydzielania? Czy właściwym osobom przypisano odpowiednie role? Czy role prawidłowo zdefiniowano?

Narzędzie *Menedżer autoryzacji* zwalnia administratora systemu z konieczności definiowania szczegółów związanych z rolami. Projektanci tworzą aplikacje posiadające role zdefiniowane na podstawie specyfikacji dostarczonych przez osoby wiedzące, w jaki sposób nowe programy powinny funkcjonować. W ramach definicji ról aplikacji projektanci przypisują uprawnienia do obiektów i prawa umożliwiające jej uruchamianie. Po zdefiniowaniu rola może zostać przydzielona grupie. Aby użytkownikom lub członkom grup systemu Windows umożliwić wykonanie powierzonych zadań, administratorzy muszą jedynie dodać ich do grup, którym przypisano role. Administratorzy i właściciele danych mogą brać udział w projektowaniu aplikacji i jej ról. Właściciele danych określają, jakie role zostaną przydzielone osobom pracującym w organizacji.

Dla porównania, listy ACL próbują zarządzać ograniczeniami dotyczącymi aplikacji, ustawiając uprawnienia takie jak „wykonaj" lub „zablokuj możliwość wykonania". W przypadku zasad ograniczeń oprogramowania wykorzystuje się specjalne wyznaczniki, które zezwalają na uruchomienie aplikacji lub to uniemożliwiają. Aplikacje zgodne z narzędziem *Menedżer autoryzacji* definiują role, które następnie są tak ograniczane, że pozwalają na wykonanie w programie niektórych operacji. W przypadku autoryzacji nie tylko określa się, kto może uruchomić aplikację, ale również jaka rola zostanie mu w niej przydzielona. Oznacza to, że użytkownicy nie tylko są ograniczeni do korzystania z wybranych aplikacji, ale też mogą uaktywniać jedynie niektóre ich składniki. Dla ról można także określić podzbiór zasobów używanych przez aplikację, z których będą mogły korzystać, i przypisać im uprawnienia ograniczające zakres, w jakim mogą przetwarzać zasoby. *Menedżer autoryzacji* jest narzędziem administracyjnym umożliwiającym konfigurowanie partycji aplikacji, ról i zasobów, a także przydzielanie użytkownikom ról. Zastosowanie dobrze zdefiniowanych ról do kontrolowania dostępu do systemu określa się mianem zabezpieczania opartego na rolach.

Zamieszczone poniżej informacje mogą być pomocne w zrozumieniu podstaw dotyczących narzędzia *Menedżer autoryzacji* i kroków, które muszą być wykonane, aby można było z niego skorzystać.

Podstawowe informacje na temat narzędzia Menedżer autoryzacji

Narzędzie *Menedżer autoryzacji* oferuje jeden interfejs, za pomocą którego administratorzy mogą zarządzać wieloma aplikacjami. Tego typu aplikacje muszą być tak tworzone, aby zawierały składniki niezbędne do bardziej precyzyjnej kontroli dostępu.

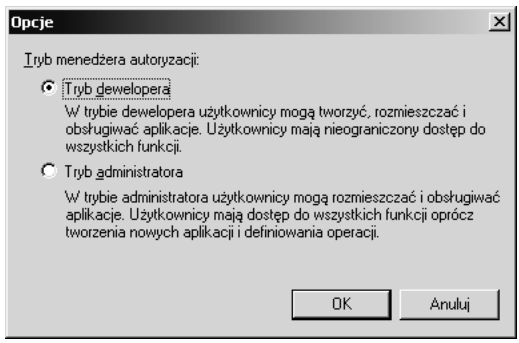
Projektanci aplikacji tworzą komponenty definiujące role. Program instalacyjny aplikacji uaktywnia zasadę autoryzacji, która jest zestawem reguł definiujących role aplikacji. Zasada autoryzacji jest przechowywana w magazynie autoryzacji i udostępniana administratorowi za pośrednictwem przystawki *Menedżer autoryzacji*. Jeśli program instalacyjny nie uwzględni zasady autoryzacji, jej składniki mogą zostać utworzone bezpośrednio w oknie przystawki *Menedżer autoryzacji*.

UWAGA: Rola administratora

Administrator jest przede wszystkim odpowiedzialny za przypisywanie ról grupom aplikacji oraz grupom i użytkownikom systemu Windows. Dodatkowo musi dodawać do tych grup użytkowników, przez co wiąże ich z odpowiednimi rolami. Administratorzy powinni też wiedzieć, na czym polega cały proces, aby nie były dla nich zaskoczeniem prawa i uprawnienia przypisywane w zarządzanych przez nich systemach użytkownikowi posiadającemu rolę.

Aby ułatwić zrozumienie zasad funkcjonowania aplikacji zgodnych z narzędziem *Menedżer autoryzacji*, w dalszej części rozdziału zdefiniowano składniki i zamieszczono instrukcje wyjaśniające, w jaki sposób można je utworzyć w oknie przystawki *Menedżer autoryzacji*. Aby możliwe było wykonanie wielu operacji, konieczna będzie zmiana trybu pracy magazynu autoryzacji z trybu administratora na tryb dewelopera. Administratorzy nie mogą definiować aplikacji, magazynów autoryzacji lub operacji, a także modyfikować nazw aplikacji lub numerów ich wersji. W celu uaktywnienia trybu dewelopera do konsoli MMC należy dodać przystawkę *Menedżer autoryzacji*, a następnie wykonać następujące kroki:

1. Prawym przyciskiem myszy kliknąć węzeł *Menedżer autoryzacji* i z menu wybrać pozycję *Opcje*.
2. Kliknąć opcję *Tryb dewelopera* (rysunek 4.1).



Rysunek 4.1. *To, jakie operacje będą mogły być wykonane za pomocą narzędzia Menedżer autoryzacji, zależy od ustawionego trybu*

3. Kliknąć przycisk *OK*.

Kompletna aplikacja zgodna z narzędziem *Menedżer autoryzacji* wymaga zdefiniowania następujących komponentów:

- **Magazyn autoryzacji**. Służy do przechowywania zasad zabezpieczeń.
- **Grupy**. Jednostki, którym można przypisać role.
- **Aplikacja**. Definiuje relację między aplikacjami, które mają być zarządzane za pomocą narzędzia *Menedżer autoryzacji*, i magazynem autoryzacji.
- **Zakres**. Folder lub inny zasób używany przez aplikację.
- **Role**. Zbiór powiązanych zadań, które muszą być wykonane.
- **Zadania**. Zbiór operacji.

- **Skrypty autoryzacji**. Skrypty autoryzujące użytkownika, który zamierza wykonać zadanie.
- **Operacje**. Zestaw uprawnień na poziomie systemu operacyjnego.

Magazyn autoryzacji

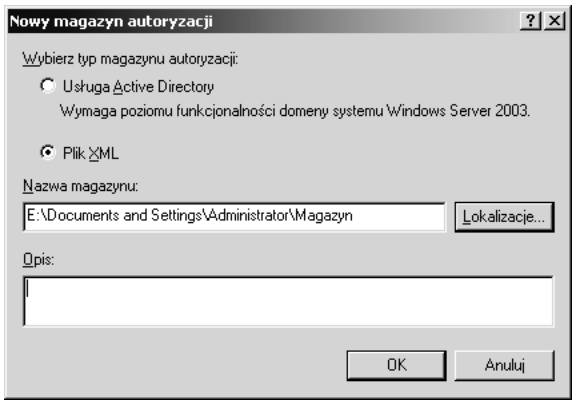
Aplikacja zgodna z narzędziem *Menedżer autoryzacji* w czasie uruchamiania swoją zasadę zabezpieczeń pobiera z magazynu autoryzacji, z którym jest powiązana. Zasada zabezpieczeń składa się z reguł określających, na co wybrana rola pozwala. Nie istnieje domyślny magazyn autoryzacji. Jest on tworzony w określonym celu. Magazyny autoryzacji mogą znajdować się w bazie danych usługi Active Directory lub w pliku XML systemu plików NTFS (lokalnym lub zdalnym). Plik taki jest zabezpieczany przy użyciu listy ACL. W tabeli 4.1 wymieniono różnice występujące między dwoma typami magazynów.

Tabela 4.1. *Definicja magazynu autoryzacji*

	Usługa Active Directory	Plik XML
Obsługa delegowania	Obsługa na poziomie magazynu autoryzacji, aplikacji i zakresu.	Brak obsługi. Plik XML jest zabezpieczany przez wpisy ACE listy ACL.
Definiowanie autoryzacji	Adres URL z prefiksem *MMSLDAP://* lub nazwa wyróżniająca LDAP, taka jak *CN=magazyn,CN=dane,DN=firma* (lub *DN=com*).	Adres URL z prefiksem *MSXML://* lub ścieżka, taka jak *C:\magazyny\ten_magazyn.xml* lub *\\serwer\udział_a\ten_magazyn.xml*.
Zgodność z systemem Windows	Tylko poziom funkcjonalny domeny systemu Windows Server 2003.	Partycja NTFS (łącznie ze znajdującymi się na serwerach z systemem Windows 2000).
Obsługa inspekcji fazy wykonywania	Obsługa na poziomie magazynu autoryzacji i aplikacji.	Obsługa na poziomie magazynu autoryzacji i aplikacji.
Obsługa inspekcji modyfikacji magazynu autoryzacji	Obsługa na poziomie magazynu autoryzacji, aplikacji i zakresu.	Obsługa wyłącznie na poziomie magazynu autoryzacji.

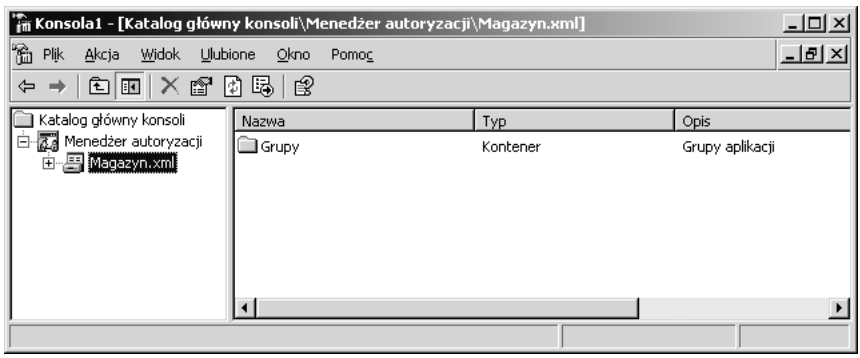
Magazyn autoryzacji można zdefiniować programowo lub ręcznie w oknie przystawki *Menedżer autoryzacji*. Gdy w oknie przystawki są tworzone takie elementy jak grupy, role, operacje zadań, ich dane trafiają do magazynu autoryzacji. W celu zdefiniowania magazynu należy wykonać następujące kroki:

1. Uruchomić przystawkę *Menedżer autoryzacji*.
2. Prawym przyciskiem myszy kliknąć węzeł *Menedżer autoryzacji* i z menu wybrać pozycję *Nowy magazyn autoryzacji*.
3. Zdecydować, czy magazyn autoryzacji znajdzie się w pliku XML, czy w bazie danych usługi Active Directory, a następnie określić nazwę i lokalizację magazynu.
4. Wprowadzić opis (rysunek 4.2).



Rysunek 4.2. *Tworzenie magazynu autoryzacji polega na zdefiniowaniu jego nazwy i lokalizacji*

5. W celu dodania magazynu kliknąć przycisk *OK*. Na rysunku 4.3 pokazano magazyn zdefiniowany w oknie przystawki *Menedżer autoryzacji*.



Rysunek 4.3. *Po utworzeniu magazyn autoryzacji jest widoczny w oknie przystawki Menedżer autoryzacji*

UWAGA: Delegowanie

Delegowanie w przypadku usługi Active Directory jest metodą nadawania uprawnień administracyjnych użytkownikom, którzy nie są członkami grupy *Administratorzy*. Operacja polega na przypisywaniu grupie użytkowników uprawnień do obiektów usługi Active Directory. Ponieważ magazyn autoryzacji znajdujący się w bazie usługi Active Directory też jest obiektem, można delegować uprawnienia do niego i umieszczonych w nim obiektów. Magazyny autoryzacji przechowywane w pliku XML nie są obiektami usługi Active Directory, dlatego nie pozwalają na delegowanie.

Grupy

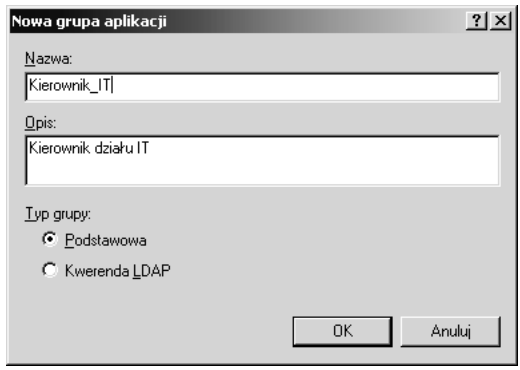
Grupy służą do przypisywania ról użytkownikom. Role są przydzielane grupom, natomiast administratorzy dodają do nich konta użytkowników. W oknie przystawki *Menedżer autoryzacji* mogą być tworzone specjalne grupy. Można też użyć grup systemu Windows. Jeśli zastosuje się grupy narzędzia *Menedżer autoryzacji*, można je tak zdefiniować, aby były wykorzystywane tylko przez aplikację, a nawet jej zakres. Terminologia związana z grupami jest następująca:

- **Grupa aplikacji**. Grupa użytkowników aplikacji zgodnej z narzędziem *Menedżer autoryzacji*. Tego typu grupy mogą być tworzone na wszystkich trzech poziomach (magazynu autoryzacji, aplikacji i zakresu) dostępnych w oknie przystawki *Menedżer autoryzacji*. Grupa zdefiniowana na wyższym poziomie może być stosowana na niższym. Jednak grupa utworzona na niższym poziomie nie może być użyta na wyższym. Grupy aplikacji dzielą się na podstawowe i grupy kwerend LDAP.
- **Podstawowa grupa aplikacji**. Grupa posiada listę członków i listę składającą się z tych, którzy nie są członkami. Ta druga lista służy do blokowania dostępu do określonego podzbioru uprawnień grupy, która zezwala na szerszy dostęp. W związku z tym tego typu grupa może oferować dostęp do aplikacji i blokować go w przypadku niektórych jej składników. Druga lista ma pierwszeństwo przed pierwszą. Podstawowymi grupami aplikacji mogą być grupy i użytkownicy systemu Windows lub grupy kwerend LDAP.
- **Grupa kwerendy LDAP (*Lightweight Directory Access Protocol*)**. Tego typu grupa jest dynamicznie generowana przez kwerendę LDAP. W skład takiej kwerendy może wchodzić dowolny atrybut użytkownika. Przykładowo, grupa kwerendy może uwzględniać wszystkich użytkowników mieszkających na obszarze miasta Kraków. Z czasem grupa może ulegać modyfikacjom. Inne grupy mogą być bardziej zmienne. Przykładem mogłaby być grupa, której członkami są wszyscy, którzy mają urodziny w bieżącym miesiącu.
- **Grupy i użytkownicy systemu Windows**. Są to standardowe konta użytkowników i grup (domyślne lub utworzone przez użytkowników). Decydując się na przypisanie roli grupie, można skorzystać z grup i użytkowników systemu Windows lub grupy aplikacji.

Aby dodać grupę, należy wykonać następujące kroki:

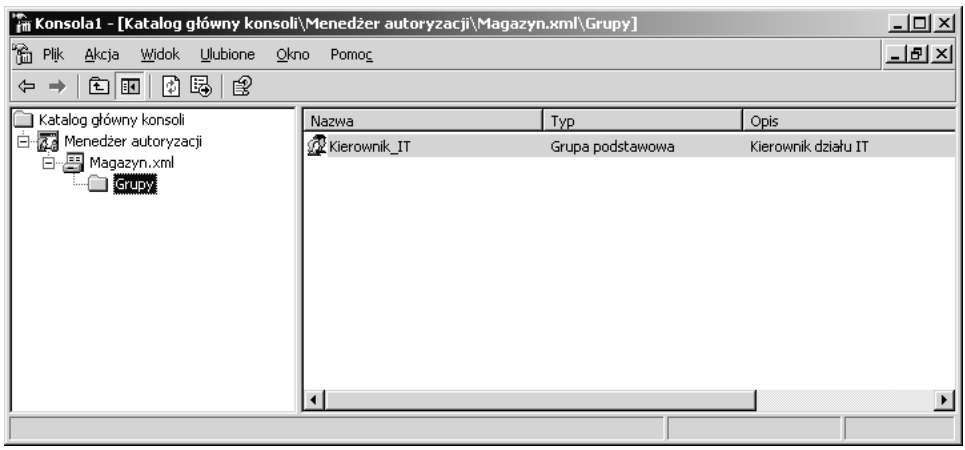
1. Prawym przyciskiem myszy kliknąć węzeł *Grupy* znajdujący się w kontenerze magazynu autoryzacji, aplikacji lub zakresu, a następnie z menu wybrać pozycję *Nowa grupa aplikacji*.
2. Podać nazwę i opis grupy aplikacji.

3. Określić typ grup identyfikowany przez opcję *Kwerenda LDAP* lub *Podstawowa* (rysunek 4.4).



Rysunek 4.4. *Typ grupy jest określany w trakcie jej tworzenia*

4. Kliknąć przycisk *OK* i sprawdzić zdefiniowaną grupę (rysunek 4.5).



Rysunek 4.5. *Grupy są zlokalizowane w kontenerze Grupy*

Aplikacja

W trakcie projektowania aplikacji zgodnej z narzędziem *Menedżer autoryzacji* jest określane, na co będą pozwalały jej role. Przypisując do grup role i użytkowników, definiuje się, kto i jakie będzie mógł realizować zadania. Obiekt aplikacji tworzony w oknie przystawki *Menedżer autoryzacji* jest umieszczany w powiązanym z nią magazynie autoryzacji. Obiekt aplikacji zawiera obiekty definiujące zastosowaną w niej kontrolę dostępu opartą na rolach. Choć aplikacja może znajdować się tylko w jednym magazynie autoryzacji, on sam może zawierać wiele

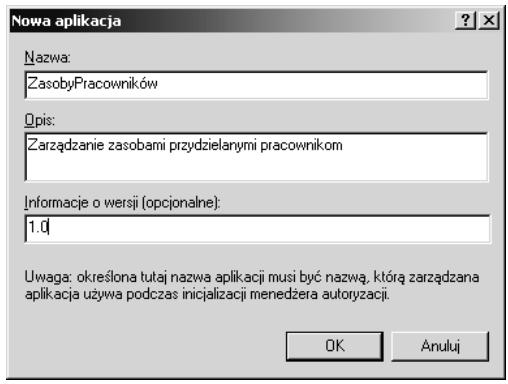
aplikacji. W tabeli 4.2 wymieniono typowe operacje obsługiwane przez aplikację zgodną z narzędziem *Menedżer autoryzacji* i porównano je z tymi, na których wykonanie pozwalają zwykłe programy.

Tabela 4.2. *Porównanie operacji wykonywanych przez aplikacje*

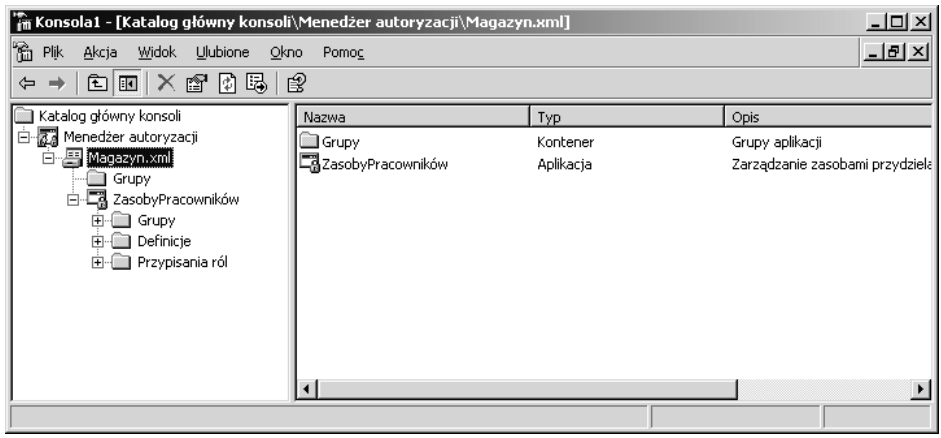
Aplikacja zarządzająca autoryzacją	Zwykła aplikacja
1. Faza projektowania aplikacji: definiowanie ról, wdrażanie operacji i łączenie ich w zadania.	Choć pozwala na definiowanie ról, w praktyce zwykle nie korzysta się z tego. Definicje ról mogą zezwalać administratorom na uruchamianie niektórych aplikacji lub wykonywanie operacji, natomiast im i jednocześnie użytkownikom na uaktywnianie innych programów.
2. Podczas instalacji aplikacji jest definiowany magazyn autoryzacji, operacje, zadania i role. Dodatkowo są tworzone pliki lub bazy służące do przechowywania danych.	Proces instalacji definiuje pliki lub bazy przechowujące dane aplikacji, a także umieszcza dane konfiguracyjne w rejestrze lub w pliku.
3. W czasie pracy aplikacja korzysta z narzędzia *Menedżer autoryzacji*, aby połączyć się z magazynem autoryzacji i wczytać zasadę zabezpieczeń.	Po uruchomieniu aplikacja może sprawdzić dane konfiguracyjne znajdujące się w plikach lub gałęziach rejestru. W czasie pracy autoryzacja przeprowadzana w celu udzielenia lub zablokowania dostępu do obiektów polega na sprawdzeniu praw użytkownika i uprawnień przypisanych przez administratora.
4. Gdy z aplikacją połączy się klient, zostanie utworzony kontekst aplikacji.	Gdy użytkownik uruchamia aplikację, korzysta ona z jego kontekstu zabezpieczeń.
5. Zanim klient będzie mógł użyć aplikacji, w oparciu o role wykona ona odpowiednie czynności. To, jaki interfejs zostanie udostępniony użytkownikowi w czasie pracy, zależy od jego roli.	Zanim klient będzie mógł użyć aplikacji, wykona ona odpowiednie czynności głównie na podstawie praw i uprawnień udzielonych użytkownikowi do obiektów. Jeśli prawa i uprawnienia użytkownika nie będą zgodne z wymaganymi do uruchomienia aplikacji, interfejs może wyświetlić komunikaty o błędach.
6. Gdy klient próbuje wykonać operację, jest wykonywana kontrola dostępu mająca na celu stwierdzenie, czy rola użytkownika dysponuje prawem zezwalającym mu na to.	Gdy aplikacja próbuje wykonać operację, jest przeprowadzana kontrola dostępu mająca na celu stwierdzenie, czy użytkownik dysponuje wymaganym prawem lub uprawnieniem.

Gdy zarządza się aplikacją zgodną z narzędziem *Menedżer autoryzacji* lub bierze się udział w jej projektowaniu, rolami można administrować w inny bardzo naturalny sposób. W celu utworzenia w oknie przystawki *Menedżer autoryzacji* obiektu aplikacji należy wykonać następujące kroki:

1. Prawym przyciskiem myszy kliknąć węzeł magazynu autoryzacji i z menu wybrać pozycję *Nowa aplikacja*.
2. Wprowadzić nazwę, opis i numer wersji aplikacji (rysunek 4.6).
3. Kliknąć przycisk *OK* i sprawdzić zdefiniowaną aplikację widoczną w oknie przystawki *Menedżer autoryzacji* (rysunek 4.7).



Rysunek 4.6. *Aplikacje są kontenerami tworzonymi w celu przechowywania zasad zabezpieczeń mających postać ról, grup, operacji i zadań*



Rysunek 4.7. *Aplikacje są tworzone w magazynie autoryzacji*

Zakres

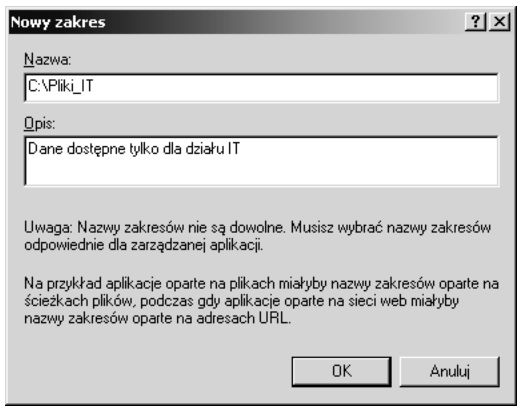
Zakresy są tworzone dla każdej aplikacji w celu ograniczenia dostępu do zasobów. Zakres identyfikuje takie zasoby, jak foldery systemu plików, kontenery usługi Active Directory, różnego typu pliki (np. wszystkie pliki **.doc*), adresy URL i gałęzie rejestru. Zamiast z aplikacją, tworzone grupy narzędzia *Menedżer autoryzacji*, przypisania i definicje ról bądź definicje zadań kojarzy się z zakresem aplikacji. Jednak operacje nie mogą być definiowane na poziomie zakresu.

Grupy tworzone w obrębie zakresu dysponują dostępem do zasobów określonych dla zakresu. Z kolei grupy zdefiniowane na poziomie aplikacji mogą uzyskać dostęp do zasobów całej aplikacji, łącznie z jej zakresem. Użycie zakresów jest dobrą metodą ograniczania dostępu wybranym użytkownikom i zwiększania go innym.

Zakresem może być folder systemu plików NTFS, kontener usługi Active Directory, zbiór plików identyfikowanych przez maskę, taką jak na przykład *.*doc*, adres URL itd. Wymienione obiekty znajdują się w kontenerze aplikacji zlokalizowanym w oknie przystawki *Menedżer autoryzacji*.

W celu utworzenia zakresu należy wykonać następujące kroki:

1. Prawym przyciskiem myszy kliknąć węzeł aplikacji i z menu wybrać pozycję *Nowy zakres*.
2. Wprowadzić nazwę i opis zakresu (rysunek 4.8). Warto zauważyć, że nazwa ma postać ścieżki folderu. Nazwy muszą reprezentować rzeczywiste lokalizacje.



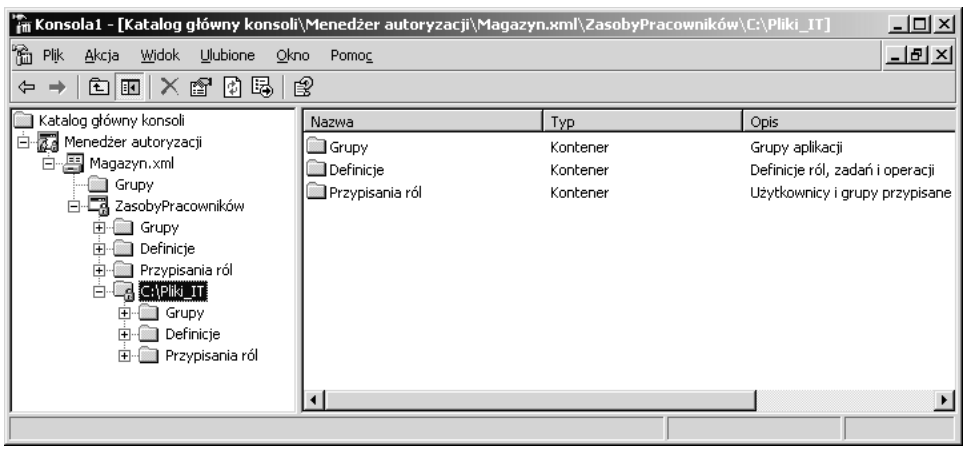
Rysunek 4.8. *Nazwy zakresów muszą reprezentować rzeczywiste lokalizacje*

3. Kliknąć przycisk *OK*.

Definiując zakresy, trzeba zadbać o to, aby identyfikowały zasoby w sposób zrozumiały dla aplikacji. Trzeba tu wspomnieć o dwóch istotnych rzeczach. Po pierwsze, zasób powinien być identyfikowany przez lokalizację, określaną na przykład przy użyciu ścieżki pliku, gałęzi rejestru lub kompletnego adresu URL. Zasób może też być identyfikowany przez istniejące jednostki organizacyjne usługi Active Directory. Po drugie, sama aplikacja musi być w stanie obsługiwać zasób. W roli identyfikatorów zakresu aplikacje internetowe mogą używać adresów URL, natomiast programy oparte na systemie plików mogą korzystać ze ścieżek plików.

Aby skutecznie ograniczyć dostęp do zasobów, korzystając z ich lokalizacji, należy wykonać następujące kroki:

1. Utworzyć zakresy dla zasobów wymagających bardziej szczegółowej ochrony.
2. W zakresach zdefiniować grupy aplikacji. Na rysunku 4.9 pokazano zakres *C:\Pliki_IT* utworzony w obrębie aplikacji *ZasobyPracowników*. Warto zwrócić uwagę na to, w jaki sposób kontenery grup są definiowane na poziomie magazynu autoryzacji, aplikacji i zakresu, a także jak są tworzone definicje i przypisania ról zarówno na poziomie zakresu, jak i aplikacji. Na rysunku widać, że wszystkie grupy umieszczone w kontenerze *Grupy* zakresu *C:\Pliki_IT* mogą uzyskać dostęp tylko do plików powiązanych z tym poziomem. Z kolei grupom utworzonym na poziomie aplikacji może być udzielony dostęp do wszystkich jej zasobów. Grupy zdefiniowane w kontenerze magazynu autoryzacji uzyskają dostęp do zasobów wszystkich aplikacji znajdujących się w magazynie.



Rysunek 4.9. *Lokalizacja grupy decyduje o tym, z jakich zasobów będą mogli korzystać jej członkowie*

3. Do odpowiednich grup przypisać użytkowników, którzy powinni dysponować dostępem do określonych zasobów.
4. Utworzyć grupy na poziomie aplikacji.
5. Do grup poziomu aplikacji dodać użytkowników, którzy powinni dysponować dostępem do wszystkich zasobów aplikacji.
6. Zdefiniować grupy na poziomie magazynu autoryzacji. Dołączyć do nich użytkowników, którzy muszą uzyskać dostęp do wszystkich aplikacji zlokalizowanych w magazynie.

UWAGA: Dlaczego warto korzystać z grup narzędzia *Menedżer autoryzacji*

Grupy narzędzia *Menedżer autoryzacji* należy stosować z dwóch powodów. Po pierwsze, dzięki takim grupom można lepiej kontrolować dostęp do obiektów. Po drugie, gdy są używane tego typu grupy, łatwiejsze będzie wykorzystanie aplikacji zarówno w środowisku grupy roboczej, jak i domeny. Jest to istotne dlatego, że komputery wchodzące w skład grupy roboczej posiadają grupy systemu Windows różniące się od tych oferowanych przez usługę Active Directory obsługującą domeny. Aplikacja, którą stworzono by z myślą o grupach usługi Active Directory, nie mogłaby być zastosowana w środowisku grupy roboczej. Warto jednak zauważyć, że aplikacja zaprojektowana dla środowiska usługi Active Directory może nie być w ogóle przydatna w przypadku grupy roboczej. Biorąc pod uwagę wymagania aplikacji, powinno się podjąć decyzję dotyczącą typów grup, które zostaną zastosowane.

Role, zadania, skrypty autoryzacji i operacje

W aplikacji zgodnej z narzędziem *Menedżer autoryzacji* role są definiowane przez zadania, operacje i skrypty autoryzacji. Zadania składają się z zadań niższego poziomu, operacji i skryptów autoryzacji. Operacje są elementami niższego poziomu związanymi z funkcjonalnością systemu operacyjnego. Przykładowo, zadanie wykonywane przez dział wsparcia może polegać na resetowaniu hasła dla użytkowników, których konta znajdują się w określonej jednostce organizacyjnej. Zadaniu takiemu zdefiniowanemu w aplikacji można nadać nazwę *ResetowanieHasła*. Operacja, która też jest tworzona w aplikacji, uwzględnia odwołanie do wartości identyfikującej rzeczywisty kod programu umożliwiający operatorowi zresetowanie haseł użytkowników należących do określonej jednostki organizacyjnej. Operacja jest przypisywana do zadania, które przydziela się roli pełnionej przez pracowników działu wsparcia. Po zdefiniowaniu roli wiąże się ją z grupą utworzoną w celu reprezentowania użytkowników, którym zostanie przydzielona rola pracowników działu wsparcia.

W trakcie tworzenia aplikacji operacje są kodowane. Gdy projektuje się aplikację zgodną z narzędziem *Menedżer autoryzacji*, są definiowane elementy każdej roli. Podczas instalowania aplikacji zadania i operacje definiujące rolę są umieszczane w oknie narzędzia *Menedżer autoryzacji* wraz z grupami i innymi składnikami programu.

W oknie przystawki *Menedżer autoryzacji* można ręcznie dodawać role, skrypty autoryzacji, zadania i operacje. Wystarczy wiedzieć, że elementy te muszą być powiązane z kodem aplikacji, natomiast wartości określone w operacjach muszą tworzyć łącza między narzędziem *Menedżer autoryzacji* i kodem.

Role

Zanim za pomocą ról będzie można kontrolować autoryzację, trzeba je zdefiniować. W tym celu do ról należy dodać utworzone zadania i operacje. Role można definiować dla wielu aplikacji i zarządzać nimi z jednego miejsca. Role mogą też dotyczyć tylko wybranych aplikacji, a nawet być ograniczone do ich niektórych zasobów.

Pierwszy krok polega na zidentyfikowaniu wymaganych ról. Aby utworzyć role, należy je potraktować jak abstrakcję odpowiadającą rzeczywiście wykonywanym operacjom i zadaniom. Pracownik działu wsparcia i administrator systemu są rolami, które można zdefiniować, gdy aplikację stworzono w celu nadzorowania operacji systemowych. Osoba zajmująca się listami płac, księgowy i główny księgowy są rolami, które można utworzyć na potrzeby programu księgującego. Na etapie projektowania aplikacji jest określana specyfikacja, która uwzględnia rzeczywiste zadania realizowane przez każdego typu pracownika. Wszystkie zadania są dzielone na mniejsze jednostki lub operacje.

Dobrze zdefiniowana rola odwzorowuje kategorię stanowiska lub zakres odpowiedzialności. Choć z łatwością w nazwach stanowisk można doszukać się ogólnej definicji ról, w celu stwierdzenia, co faktycznie robi osoba pełniąca określone stanowisko, konieczne będzie przeprowadzenie dokładniejszej analizy. Trzeba pamiętać, że wielu pracowników jest zaangażowanych w specjalne procesy biznesowe, natomiast nazwy stanowisk nie zawsze odpowiadają określonym rolom aplikacji. Proces tworzenia roli w obrębie aplikacji składa się z następujących operacji:

- Wybranie nazwy.
- Określenie definicji.
- Utworzenie zadań niższego poziomu, ról i operacji wchodzących w skład nowej roli. Reguły autoryzacji mogą być definiowane za pomocą skryptów, takich jak skrypty VBScript. Zadania stają się częścią definicji roli i mogą być dodawane do kontenera *Definicje ról*, a także w nim przeglądane.

Choć zatwierdzanie listy członków określonej roli aplikacji nie jest zadaniem administratora, samo przypisywanie kont użytkowników do roli już tak. Jak zwykle, krytyczne znaczenie ma zrozumienie, jakie w ramach takiej operacji przydziela się prawa i dostęp. Trzeba wiedzieć, kiedy dostęp udzielany użytkownikowi i wykonywane przez niego operacje są normalne i zatwierdzone, a kiedy realizowane działania naruszają reguły, tak jak w przypadku ataku, którego celem jest system.

UWAGA: Istnieje więcej metod tworzenia roli

Oczywiście najpierw można zdefiniować wszystkie operacje, a następnie utworzyć poszczególne zadania i przypisać do nich operacje. Zgodnie z tą zasadą po utworzeniu ról należy do nich dodać zadania.

W celu zdefiniowania roli za pomocą przystawki *Menedżer autoryzacji* w pierwszej kolejności trzeba utworzyć zadania i operacje, a następnie odpowiednio je przypisać. Pierwszym krokiem procedury tworzenia roli jest określenie jej definicji. W tym celu należy wykonać następujące kroki:

1. Zlokalizować kontener aplikacji, a następnie rozwinąć zawartość węzła *Definicje*.
2. Prawym przyciskiem myszy kliknąć węzeł *Definicje ról* i z menu wybrać pozycję *Nowa definicja roli*.
3. Dla roli wprowadzić nazwę i opis (rysunek 4.10).

Rysunek 4.10. *Role są definiowane przez powiązane z nimi zadania i tworzone skrypty autoryzacji*

4. Jeśli dla roli utworzono role niższego poziomu, zadania lub skrypty autoryzacji, za pomocą przycisku *Dodaj* dodać je do definicji roli.
5. Kliknąć przycisk *OK*.

Zadania

Role składają się z zadań. Zadania są zbiorem operacji, skryptów autoryzacji i ewentualnie innych zadań. Zadania muszą być dobrze zdefiniowane i powiązane z rolami. Dobrze zdefiniowane zadania reprezentują rozpoznawalne elementy pracy. Oto przykłady takich zadań:

- zmiana hasła,
- uaktywnienie konta,
- utworzenie konta użytkownika,
- przedstawienie kosztów,
- zatwierdzenie kosztów,
- podpisanie czeku.

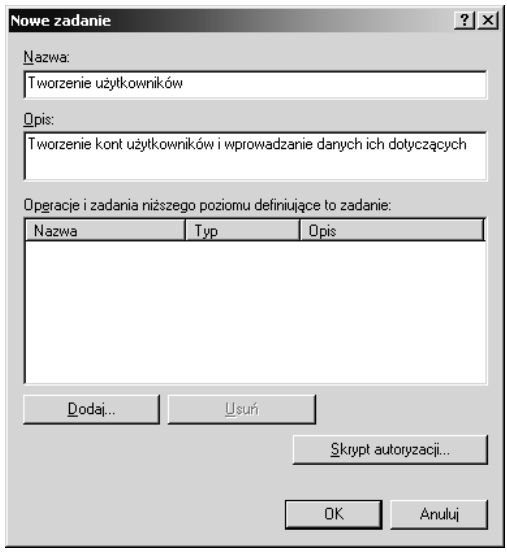
Oto przykłady zadań, które nie są dobrze zdefiniowane:

- zarządzanie pracownikami,
- kierowanie działem księgowym,
- udzielanie użytkownikom pomocy w zakresie obsługi komputerów.

Aby stwierdzić, jakie zadania powinny zostać zdefiniowane dla wybranej roli, trzeba będzie zidentyfikować elementy pozwalające określić, jakie są obowiązki osoby pełniącej rolę. Przykładowo, administrator sieci może modyfikować listy ACL routera. Pracownik działu wsparcia może zmieniać hasła lub resetować zablokowane konta. Podobnie jak role, zadania są definiowane w oknie przystawki *Menedżer autoryzacji*. Polega to na podaniu nazwy i opisu. Zadanie składa się z zadań niższego poziomu lub operacji, a także skryptów autoryzacji.

W celu utworzenia zadania należy wykonać następujące kroki:

1. Prawym przyciskiem myszy kliknąć kontener *Definicje zadań* i z menu wybrać pozycję *Nowa definicja zadania*.
2. Wprowadzić nazwę i opis zadania (rysunek 4.11).
3. Jeśli dla zadania utworzono zadania niższego poziomu, operacje lub skrypty autoryzacji, dodać je za pomocą przycisku *Dodaj*.
4. Kliknąć przycisk *OK*.



Rysunek 4.11. *Zadania składają się z operacji i skryptów autoryzacji*

Operacje

Operacje są zbiorem uprawnień powiązanych z procedurami zabezpieczeń na poziomie systemu lub interfejsu API. Przykładowe uprawnienia to odczyt lub zapis atrybutów. Operacje pełnią rolę elementów tworzących zadania. Operacje są definiowane na poziomie aplikacji. W przypadku poziomu magazynu autoryzacji lub zakresu nie jest to możliwe. Definicja operacji uwzględnia nazwę, opis i wartość. Wartość identyfikuje operację w obrębie aplikacji. Ma ona istotne znaczenie, ponieważ wiąże ze sobą wszystkie działania mające miejsce między narzędziem *Menedżer autoryzacji* i aplikacją. Ze względu na to, że operacje wchodzą w skład zadań, role identyfikują zadania, które mogą być wykonane, natomiast grupom są przydzielane role, po dodaniu do grupy użytkownik będzie mógł realizować wszystkie operacje tworzące zadania przypisane rolom.

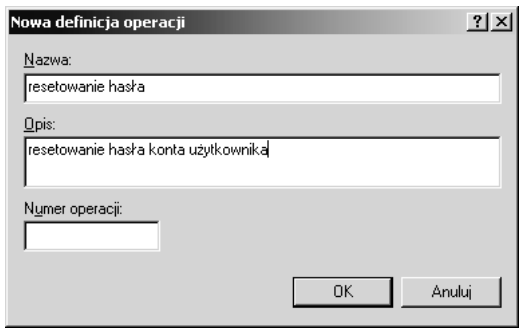
OSTRZEŻENIE: Unikanie błędów dotyczących wartości operacji

Wartość musi być liczbą całkowitą z przedziału od 0 do 2147483647. Jeśli trzeba ręcznie podać wartość, należy sprawdzić, czy poprawnie ją wprowadzono. Nieprawidłowa wartość spowoduje wystąpienie błędu w aplikacji.

Jeśli na przykład kilka operacji definiujących niskopoziomowe czynności niezbędne do sformatowania dysku twardego tworzy zadanie „formatowanie dysku", które z kolei jest przypisane roli *Zarządca serwera* powiązanej z grupą aplikacji *Zarządca_serwera*, po dodaniu do niej użytkownika umożliwi mu się sformatowanie dysku.

W celu zdefiniowania operacji należy wykonać następujące kroki:

1. Prawym przyciskiem myszy kliknąć kontener *Definicje operacji* i z menu wybrać pozycję *Nowa definicja operacji*.
2. Wprowadzić nazwę, opis i numer operacji (rysunek 4.12). Numer operacji musi znajdować się w kodzie aplikacji.



Rysunek 4.12. *Operacje są identyfikowane przez numer*

3. Kliknąć przycisk *OK*.

Tworzenie skryptów autoryzacji

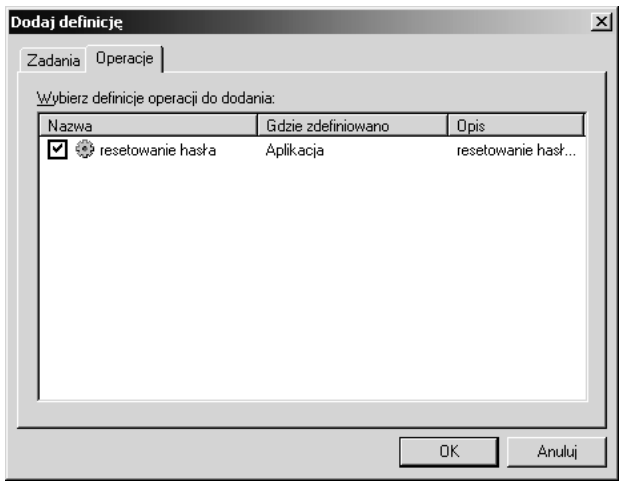
Skrypty autoryzacji są tworzone w celu zastosowania reguł autoryzacji. Reguła taka sprawdza warunki, aby stwierdzić, czy użytkownik dysponuje prawem lub uprawnieniem niezbędnym do zrealizowania określonego zadania. Przykładowo, użytkownicy mogą należeć do grupy, której przypisano rolę. Rola jest definiowana przez zadania, które umożliwiają posiadaczowi roli sfinalizowanie określonej czynności, takiej jak odczyt pliku. Reguła autoryzacji może posłużyć do uwzględnienia praw systemu operacyjnego i uprawnień do obiektów przypisanych użytkownikowi. Jeśli uprawnienia nie zezwalają użytkownikowi na odczytanie pliku, nie będzie mógł tego zrobić, nawet gdy członkowie jego grupy aplikacji zgodnej z narzędziem *Menedżer autoryzacji* standardowo mają taką możliwość. Skrypty mogą być tworzone przy użyciu języka VBScript lub JScript. Zwykle są pisane przez programistów.

Definiowanie zadań

Aby zdefiniować zadanie, co polega na przypisaniu operacji, należy wykonać następujące kroki:

1. Dwukrotnie kliknąć zadanie, które ma być zdefiniowane.
2. Uaktywnić zakładkę *Definicja*, kliknąć przycisk *Dodaj* i uaktywnić zakładkę *Operacje*.

3. Zaznaczyć operacje, które są niezbędne do zdefiniowania zadania (rysunek 4.13).



Rysunek 4.13. *Do zadania są dodawane operacje*

4. Kliknąć przycisk *OK*.

Definiowanie ról

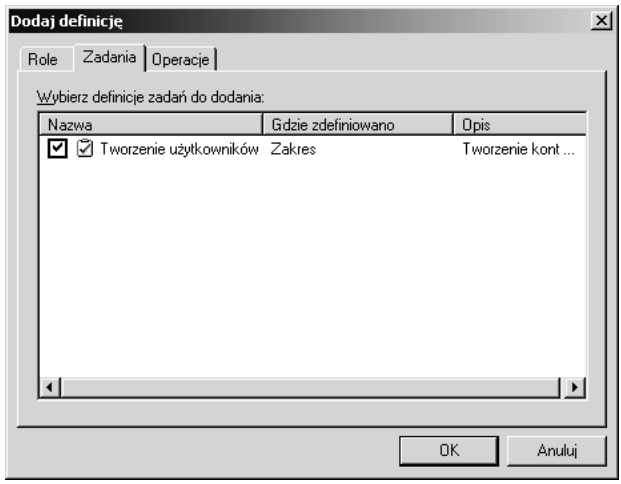
Aby zdefiniować rolę, co polega na przypisaniu jej listy zadań, należy wykonać następujące kroki:

1. Dwukrotnie kliknąć rolę, która ma być zdefiniowana.
2. Uaktywnić zakładkę *Definicja*, kliknąć przycisk *Dodaj* i uaktywnić zakładkę *Zadania*.
3. Zaznaczyć zadania definiujące role (rysunek 4.14).
4. Jeśli istnieją skrypty autoryzacji, które powinny zostać dołączone, kliknąć przycisk *Skrypt autoryzacji*. Wprowadzić kod źródłowy skryptu lub ścieżkę identyfikującą jego położenie, a następnie kliknąć przycisk *OK*.
5. Kliknąć przycisk *OK*.

Przypisywanie ról do grup

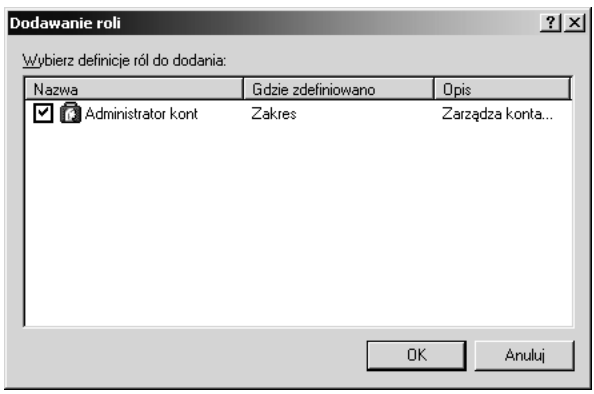
W celu przydzielenia grupom ról należy wykonać następujące kroki:

1. Prawym przyciskiem myszy kliknąć kontener *Przypisania ról* i z menu wybrać pozycję *Przypisz role*.



Rysunek 4.14. *Do ról są dodawane zadania*

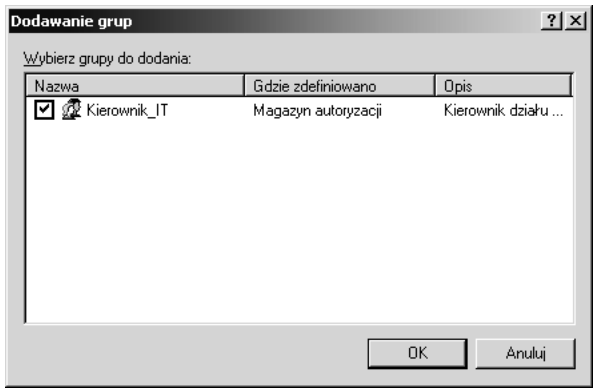
2. W oknie dialogowym *Dodawanie roli* zaznaczyć role (rysunek 4.15), a następnie kliknąć przycisk *OK*.



Rysunek 4.15. *Umieszczanie zdefiniowanych ról w kontenerze Przypisania ról*

3. Role zostaną umieszczone w kontenerze *Przypisania ról*. Prawym przyciskiem myszy kliknąć rolę, która ma być przypisana grupie, i z menu wybrać pozycję *Przypisz grupy aplikacji* lub *Przypisz użytkowników i grupy systemu Windows*.

4. Po wybraniu pozycji *Przypisz grupy aplikacji* zaznaczyć grupę aplikacji (rysunek 4.16).



Rysunek 4.16. *Przypisywanie odpowiednich grup do poszczególnych ról*

5. Gdy kliknięto pozycję *Przypisz użytkowników i grupy systemu Windows*, za pomocą narzędzia służącego do wybierania obiektów zaznaczyć grupę lub użytkowników, którym zostanie przypisana rola.
6. Kliknąć przycisk *OK*.

Podstawowe informacje dotyczące narzędzia Menedżer autoryzacji — podsumowanie

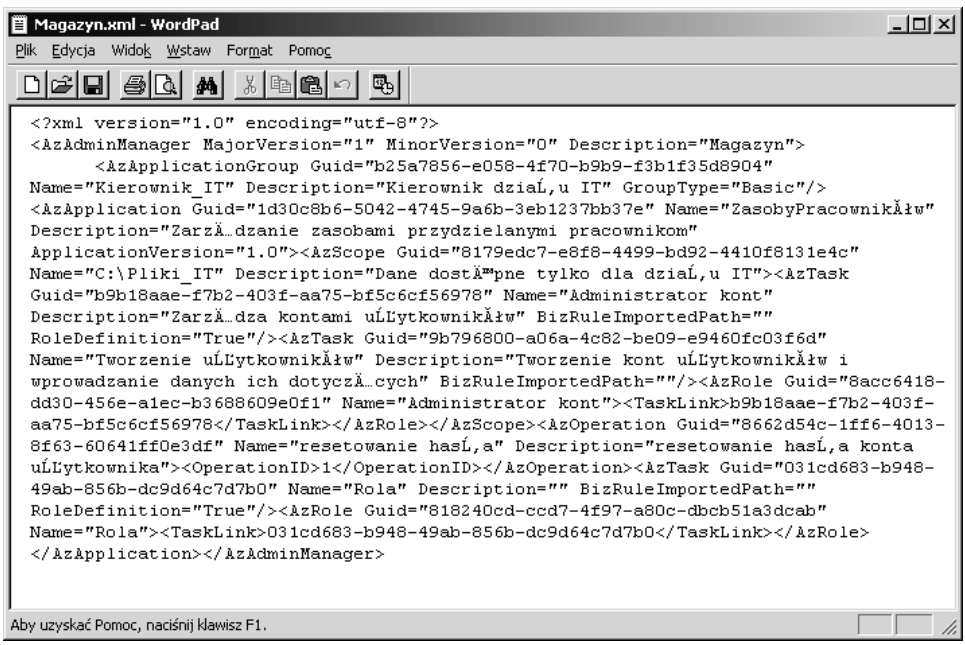
W obrębie narzędzia *Menedżer autoryzacji* i określonych aplikacji każdej roli jest przypisywane prawo do wykonywania zadań i operacji. Rola jest przydzielana grupie będącej interfejsem, za pomocą którego administrator będzie upoważniał użytkowników lub grupy systemu Windows do używania aplikacji i przetwarzania zasobów. Zamiast zarządzać zasobami aplikacji nadzoruje się działania i obieg zadań. Przykładowo, zamiast korzystać z narzędzia *Kreator delegowania kontroli* bądź bezpośrednio przypisywać kontu użytkownika lub grupy uprawnienie pozwalające na resetowanie haseł kont znajdujących się w jednostce organizacyjnej, wystarczy konto użytkownika dodać do grupy narzędzia *Menedżer autoryzacji*, której przydzielono rolę pracownik działu wsparcia.

Jeśli zdefiniuje się dostęp do obiektów i prawa pozwalające na uaktywnianie składników aplikacji, rola administracyjna będzie prosta. Zamiast wykonywać tysiące niezależnych czynności polegających na tworzeniu grup systemu Windows i przypisywaniu im praw, a także uprawnień do obiektów usługi Active Directory, plików, gałęzi rejestru i innych zasobów, wystarczy jedynie konta użytkowników lub grup systemowych dodać do grup, z którymi powiązano role.

UWAGA: Administratorzy muszą o tym wiedzieć

Administratorzy nie są odpowiedzialni za tworzenie aplikacji zgodnych z narzędziem *Menedżer autoryzacji*, definiowanie ról, pisanie skryptów wykonujących zadania lub autoryzację operacji. Są to zadania należące do projektantów, które mogą być zrealizowane za pomocą kodu lub przy użyciu przystawki *Menedżer autoryzacji* działającej w trybie dewelopera. Główną powinnością administratora jest przypisywanie ról grupom aplikacji lub grupom i użytkownikom systemu Windows, a także dodawanie do tych grup użytkowników, dzięki czemu będą mogli pełnić odpowiednią rolę. Jednak administratorzy powinni też wiedzieć, na czym polega cały proces, aby były dla nich zrozumiałe prawa i uprawnienia nadawane użytkownikowi w systemie, gdy stanie się posiadaczem roli.

W magazynie autoryzacji znajdują się informacje niezbędne do stworzenia dla aplikacji zasady zabezpieczeń i reprezentowania jej w oknie przystawki *Menedżer autoryzacji*. Gdy magazyn autoryzacji jest zlokalizowany w systemie plików NTFS, ma postać pliku XML. Na rysunku 4.17 pokazano zawartość pliku XML, który utworzono przez dodanie obiektów zdefiniowanych w niniejszym punkcie.



Rysunek 4.17. *Plik XML magazynu autoryzacji zawiera zasadę zabezpieczeń aplikacji*

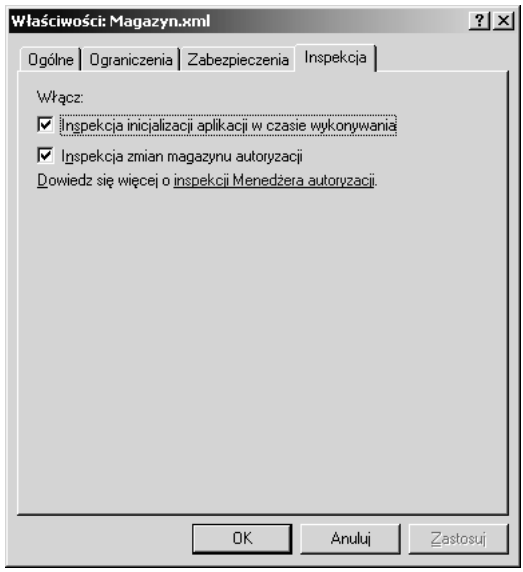
Inspekcja narzędzia Menedżer autoryzacji

Możliwe jest skonfigurowanie inspekcji zdarzeń narzędzia *Menedżer autoryzacji*, które będą rejestrowane w dzienniku zdarzeń *Zabezpieczenia*. Można wyróżnić dwa typy inspekcji narzędzia *Menedżer autoryzacji*:

- **Inspekcja fazy wykonywania**. Inspekcja ma miejsce, gdy zastosuje się zasadę zabezpieczeń zdefiniowaną w magazynie autoryzacji. Inspekcja może informować zarówno o udanych, jak i nieudanych operacjach. Zakresem inspekcji jest też objęte sprawdzanie kontekstu użytkownika i dostępu. Tego typu inspekcja może być zastosowana na poziomie magazynu autoryzacji i aplikacji, natomiast na poziomie zakresu nie.
- **Inspekcja zmian magazynu autoryzacji**. Wpisy inspekcji są generowane po zmodyfikowaniu magazynu autoryzacji, niezależnie od jego lokalizacji. W przypadku magazynu autoryzacji znajdującego się w bazie danych usługi Active Directory inspekcja może być zdefiniowana na poziomie magazynu, aplikacji i zakresu. Gdy magazyn autoryzacji jest zlokalizowany w pliku XML, inspekcję można skonfigurować tylko na poziomie magazynu.

W celu uaktywnienia inspekcji należy użyć opcji umieszczonych w zakładce *Inspekcja* (rysunek 4.18). Jeśli określonego typu inspekcja nie jest dostępna, powiązana z nią opcja nie pojawi się. Jeśli nie są widoczne opcje udanych (*Sukces*) i nieudanych (*Niepowodzenie*) operacji, oznacza to, że inspekcję zdefiniowano na wyższym poziomie. Aby to zmienić, trzeba będzie najpierw stwierdzić, gdzie inspekcja jest zarządzana (lokalnie lub za pomocą zasad grupy na poziomie domeny lub jednostki organizacyjnej) i wprowadzić modyfikacje. Dziedziczone będą wszystkie możliwe inspekcje obiektów. Przykładowo, dziedziczona jest inspekcja dostępu do obiektu zdefiniowana dla pliku systemu plików, będącego zasobem magazynu autoryzacji. W celu skonfigurowania inspekcji muszą zostać spełnione następujące wymagania:

- trzeba dysponować przywilejem *Generowanie zdarzeń inspekcji zabezpieczeń*;
- trzeba posiadać przywilej *Zarządzanie inspekcją i dziennikiem zabezpieczeń*;
- inspekcja dostępu do obiektów musi zostać uaktywniona za pomocą przystawki *Edytor obiektów zasad grupy* lub *Zasady zabezpieczeń lokalnych*.

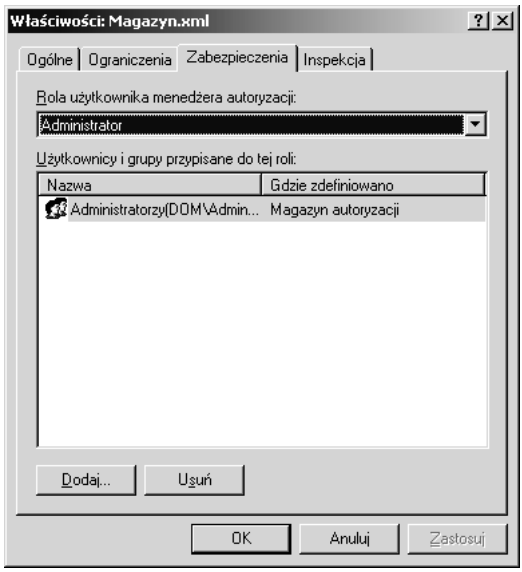


Rysunek 4.18. *Inspekcja jest definiowana w oknie właściwości magazynu autoryzacji i aplikacji*

Zarządzanie narzędziem Menedżer autoryzacji

Zarządzanie aplikacjami zgodnymi z narzędziem *Menedżer autoryzacji* jest prostym zadaniem, gdy administratorzy zrozumieją, na czym to polega i w jaki sposób funkcjonują takie aplikacje. Podstawowym zadaniem jest przypisywanie użytkowników do grup powiązanych z rolami. Administrator może być zmuszony do przypisywania ról grupom i wykonywania innych zadań, gdy kod aplikacji nie będzie się tym zajmował. Jednak tak jak w przypadku większości zadań administracyjnych proste czynności mogą kryć w sobie złożone operacje. Spostrzegawczy administrator zauważy konsekwencje z tym związane, przeprowadzi inspekcję czynności i zapobiegnie powielaniu lub usuwaniu wyników. Korzystając z posiadanych możliwości, osiągnie to przez przekazanie dostępu do zasobów i praw aplikacji, która powinna nimi zarządzać.

Rozważne może być ograniczenie liczby administratorów, którzy mogą korzystać z narzędzia *Menedżer autoryzacji*. W tym celu należy zdefiniować grupy i użytkowników dysponujących dostępem do narzędzia na poziomie administratora. Przy użyciu zakładki *Zabezpieczenia* okna właściwości magazynu autoryzacji można dodawać lub usuwać grupy i użytkowników (rysunek 4.19).



Rysunek 4.19. *Określanie administratorów, którzy mogą zarządzać aplikacjami zgodnymi z narzędziem Menedżer autoryzacji*

Zasady ograniczeń oprogramowania

Można sobie wyobrazić, że mogłoby się uniemożliwić nowemu wirusowi uaktywnienie w zarządzanych systemach nawet przed przygotowaniem sygnatury przez producenta oprogramowania antywirusowego i jej publicznym udostępnieniem. A może byłoby możliwe zapobiegnięcie uruchomieniu w systemie przez dowolną osobę ogólnie znanego, lecz zabronionego oprogramowania, takiego jak gry lub narzędzia administracyjne. Być może dałoby się całkowicie wyeliminować możliwość załadowania jeszcze nieznanego szkodliwego programu. Czy podjęłoby się decyzję o zakupie produktu pozwalającego na to wszystko?

Wcale nie trzeba tego robić. Jeśli dysponuje się systemem Windows Server 2003 lub Windows XP Professional, już można skorzystać z takiego produktu. Zasady ograniczeń oprogramowania są składnikiem dołączonym po raz pierwszy do systemu Windows XP Professional i umożliwiającym zarządzanie komputerem. Korzystając z systemu Windows Server 2003, można utworzyć zasady grupy, które będą kontrolowały pojedynczy serwer lub stację roboczą bądź tysiące komputerów z systemem Windows XP Professional i Windows Server 2003. Poniżej wyjaśniono, na czym to polega.

Możliwości zasad ograniczeń oprogramowania

Jeśli nie zrozumie się w pełni, na co zasady ograniczeń oprogramowania pozwalają, a na co nie, można je niepoprawnie skonfigurować lub oczekiwać od nich poziomu zabezpieczeń, którego nie są w stanie zapewnić. W obu przypadkach zasady mogą nie zadziałać w oczekiwany sposób lub, co gorsza, spowodować, że błędnie będzie się traktowało zabezpieczenia. Można być przekonanym, że dysponuje się komputerami chronionymi przed szkodliwymi programami lub takimi, które pozwalają jedynie na uruchomienie autoryzowanych aplikacji, gdy w rzeczywistości tak nie jest. Właściwie zdefiniowane zasady ograniczeń oprogramowania mogą zapewnić zwiększony poziom zabezpieczeń, gdy ma się świadomość ich możliwości i gdy się je uwzględni. Powinno się zapoznać z poniżej wymienionymi ograniczeniami zasad.

W przypadku trybu awaryjnego zasady ograniczeń oprogramowania nie mają żadnego wpływu

Gdy system komputera załaduje się w trybie awaryjnym, zasady ograniczeń oprogramowania nie będą miały żadnego znaczenia.

OSTRZEŻENIE: Tryb awaryjny

Gdy uaktywni się tryb awaryjny, zasady ograniczeń oprogramowania nie będą odgrywały żadnej roli. Jeśli użytkownik jest w stanie uruchomić system w trybie awaryjnym, może pominąć zasady ograniczeń oprogramowania.

Zasady ograniczeń oprogramowania dotyczą każdego użytkownika komputera

Zasady ograniczeń oprogramowania definiowane w oknie przystawki *Zasady zabezpieczeń lokalnych* będą obowiązywały tylko dla lokalnego komputera. Ze względu na to, że zasady dotyczą całego systemu, mają wpływ na każdego użytkownika, pod warunkiem że nie zostały tak skonfigurowane, aby nie uwzględniały członków grupy *Administratorzy*. Jeśli użyje się zasad ograniczeń oprogramowania dostępnych w oknie przystawki *Edytor obiektów zasad grupy*, można je skonfigurować dla komputera lub użytkowników, korzystając z węzła *Ustawienia zabezpieczeń*. Aby określić, kogo zasady będą dotyczyły, wystarczy powiązać je z jednostkami organizacyjnymi, w których znajdują się wybrane konta użytkowników lub komputerów, bądź dla obiektu GPO (*Group Policy Object*) aplikacji zastosować filtrowanie polegające na usunięciu dla żądanych grup użytkowników uprawnienia powodującego uwzględnienie zasady grupy.

Na niektóre aplikacje zasady ograniczeń oprogramowania nie oddziałują

Zasady ograniczeń oprogramowania nie mają wpływu na następujące oprogramowanie:

- sterowniki lub inne programy trybu jądra;
- programy uruchamiane przy użyciu konta *SYSTEM*;
- makra dokumentów stworzonych za pomocą pakietów Microsoft Office 2000 lub XP (makrami zarządza się za pomocą odpowiednich ustawień zabezpieczeń);
- programy tworzone dla środowiska wykonawczego CLR (*Common Language Runtime*), korzystające z narzędzia *Code Access Security Policy*.

Istnieją metody omijania reguł

Zasady ograniczeń oprogramowania uwzględniają reguły, które uniemożliwiają użycie określonej aplikacji lub zezwalają na to. Jednak skuteczność każdej reguły jest ograniczona. Nie oznacza to, że nie można definiować reguł, które efektywnie nie pozwalają na zastosowanie oprogramowania. Wskazuje to jedynie, że trzeba zapoznać się z ograniczeniami każdej reguły i odpowiednio je stosować. Oto przykładowe ograniczenia reguł:

- gdy kod aplikacji ulegnie modyfikacji, reguła mieszania nie będzie już obowiązywała;
- gdy zmianie ulegnie ścieżka aplikacji, ścieżka zdefiniowana w regule nie będzie już ważna;
- reguły stref internetowych dotyczą wyłącznie aplikacji instalowanych za pomocą instalatora systemu Windows;
- reguły certyfikatów bazują na tym, że certyfikaty uzyskano od zaufanych wystawców.

W podrozdziale „Tworzenie i stosowanie zasad ograniczeń oprogramowania" zamieszczono więcej informacji na temat reguł.

Podstawowe informacje dotyczące zasad ograniczeń oprogramowania

Ograniczanie dostępu do oprogramowania nie wydaje się być trudnym zadaniem. Sprowadza się jedynie do tego, aby nie instalować określonych aplikacji i nie zezwalać innym na coś takiego. Problem polega na tym, że można nie mieć

możliwości dokładnego kontrolowania tego, jakie oprogramowanie powinno być instalowane, kto może wykonywać taką operację, a także kto będzie mógł uruchamiać programy już znajdujące się na komputerze. Pomocne będą niektóre domyślnie przypisane prawa systemu Windows. Aby zainstalować aplikację uwzględniającą usługę, użytkownik będzie musiał dysponować prawami administratora. Jednak wiele aplikacji nie korzysta z usług, dlatego do przeprowadzenia ich instalacji nie są wymagane prawa administratora. Jeśli użytkownik może skopiować plik na dysk, tak prosta operacja może być wszystkim, co jest niezbędne do zainstalowania aplikacji. Ponieważ wiele aplikacji, takich jak narzędzia, których skróty znajdują się w menu *Narzędzia administracyjne*, musi być obecnych w systemie, powinno się uniemożliwić zwykłym użytkownikom korzystanie z nich. Dostęp do takich programów jest kontrolowany za pomocą nadanych i narzuconych praw użytkownika i uprawnień. Przykładowo, zwykli użytkownicy nie są w stanie tworzyć lub edytować obiektów GPO. Domyślnie inne aplikacje systemowe i powiązane z nimi wpisy rejestru są chronione przed określonego typu użytkownikami. Zasady grupy, listy ACL obiektów i dokładne nadzorowanie praw użytkowników można wykorzystać do kontrolowania dostępu do obiektów. Jednak w przypadku kiepskiej jakości aplikacji może być konieczne nadanie użytkownikom praw administratora komputerów, z których korzystają.

Jeśli użytkownikowi ograniczy się dostęp do takich zasobów jak pliki i wpisy rejestru, można zmniejszyć ilość szkód, które mogą być spowodowane na skutek uruchomienia nieautoryzowanych aplikacji. Jeśli użytkowników zapozna się z odpowiednimi zasadami postępowania i dokładnie będzie się wymuszało przestrzeganie zasad zabezpieczeń, można też zapobiec instalowaniu aplikacji. Jednak żadne z tych rozwiązań nie jest w stanie całkowicie wyeliminować możliwości instalacji lub użycia szkodliwego oprogramowania.

UWAGA: Definiowanie zasad ograniczeń oprogramowania

Pod adresem *http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/rstrplcy.mspx* jest dostępny znakomity dokument *Using Software Restriction Policies to Protect Against Unauthorized Software*, który poświęcono definiowaniu zasad ograniczeń oprogramowania. W dokumencie uwzględniono zastosowanie zasad w przypadku usług terminalowych i biznesowych komputerów PC, a także omówiono użycie innych zasad dla różnych użytkowników.

Korzystając z zasad ograniczeń oprogramowania, poszerza się i ulepsza domyślne ustawienia, a także definiuje mechanizm pozwalający kontrolować to, czego domyślne zasady i inne operacje nie są w stanie nadzorować. Za pomocą zasad ograniczeń oprogramowania można zrealizować następujące zadania:

- uniemożliwienie uruchomienia dowolnej aplikacji i niezależne autoryzowanie każdego składnika wymaganego oprogramowania;
- zezwolenie na uruchomienie wszystkich aplikacji, a następnie blokowanie możliwości uaktywniania wybranych programów.

Wymienione powyżej podstawowe poziomy zabezpieczeń początkowo określają, czy oprogramowanie będzie można uruchomić, czy nie. Po wybraniu poziomu zabezpieczeń zasady ograniczeń oprogramowania będą mogły identyfikować aplikacje za pomocą wartości mieszania, ścieżki, adresu URL lub certyfikatu do podpisywania kodu. Na podstawie identyfikacji oprogramowania zasady będą też zezwalać na jego uruchomienie lub je uniemożliwiać. Aby można było zdefiniować zasadę pozwalającą na uaktywnienie aplikacji lub blokującą taką możliwość, nie musi się ona znajdować wcześniej w komputerze.

OSTRZEŻENIE: Automatycznie generowane reguły ścieżek

Tego typu reguły pełnią rolę ochrony przed zablokowaniem wszystkim użytkownikom możliwości korzystania z systemu. Reguły te są zawsze widoczne w kontenerze *Reguły dodatkowe*. Oto one:

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%.exe*

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\System32.exe*

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\ProgramFilesDir%

Ogólna zasada mówi, że nie powinno się modyfikować tych reguł, jeśli nie dysponuje się bardzo dużą wiedzą na temat rejestru i dostępu wymaganego przez sam system.

Tworzenie i stosowanie zasad ograniczeń oprogramowania

Aby zdefiniować zasady ograniczeń oprogramowania, trzeba najpierw utworzyć podstawowe zasady, a następnie reguły. W tym celu należy wykonać następujące kroki:

1. Utworzyć zasadę ograniczeń oprogramowania.
2. Ustalić poziom zabezpieczeń.
3. Określić zakres obowiązywania zasady.
4. Zdefiniować typy plików identyfikujące pliki wykonywalne.

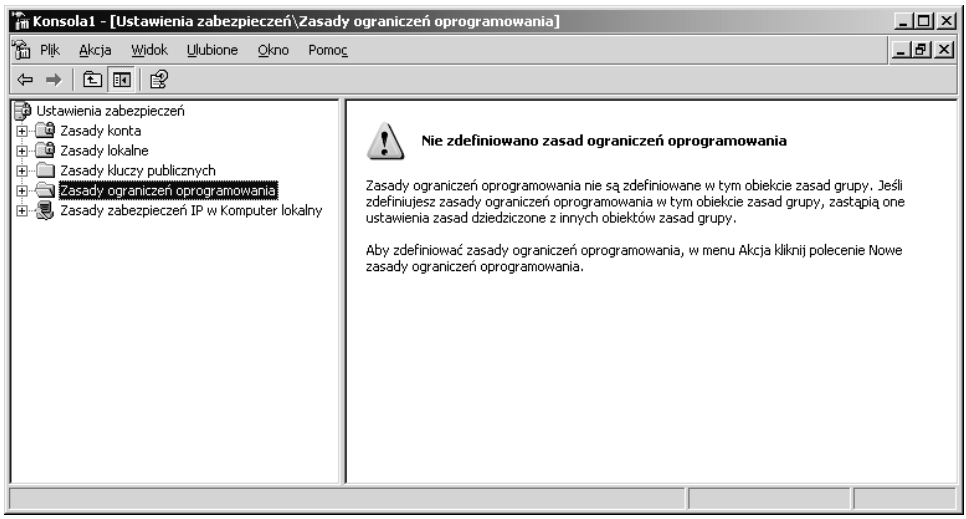
Tworzenie zasady ograniczeń oprogramowania

Zasada ograniczeń oprogramowania jest tworzona w kontenerze *Zasady ograniczeń oprogramowania* znajdującym się w oknie narzędzia *Ustawienia zabezpieczeń lokalnych* lub przystawki *Edytor obiektów zasad grupy* (w przypadku usługi Active Directory). Lokalne zasady dotyczą tylko komputera, na którym je zastosowano, natomiast zasady grupy usługi Active Directory mogą być powiązane z domenami i jednostkami organizacyjnymi, dzięki czemu są w stanie w jednakowy sposób oddziaływać na wiele systemów i użytkowników. Decyzja dotycząca miejsca przypisania zasady wymaga przemyślenia i będzie uzależniona od zaprojektowanej struktury usługi Active Directory. Więcej informacji na ten temat zamieszczono w rozdziale 7. Niezależnie od tego, gdzie zasada zostanie zdefiniowana, powinno się ją sprawdzić na jednym komputerze testowym posiadającym konfigurację, z której korzysta się podczas normalnej eksploatacji. Jeśli zasada zostanie zastosowana na wielu komputerach domeny, trzeba ją dokładnie sprawdzić w testowej domenie lub jednostce organizacyjnej. Trzeba pamiętać o dużych możliwościach zasad ograniczeń oprogramowania. Możliwe jest zdefiniowanie zasady, która uniemożliwi używanie oprogramowania znajdującego się na komputerze. Można sobie wyobrazić, co by się stało po wdrożeniu takiej zasady dla tysięcy komputerów organizacji. Jak zwykle, kwestie związane z wdrażaniem są najbardziej złożone. Definiowanie zasady dla jednego komputera jest prostym zadaniem. W celu zdefiniowania lokalnej zasady ograniczeń oprogramowania należy wykonać następujące kroki:

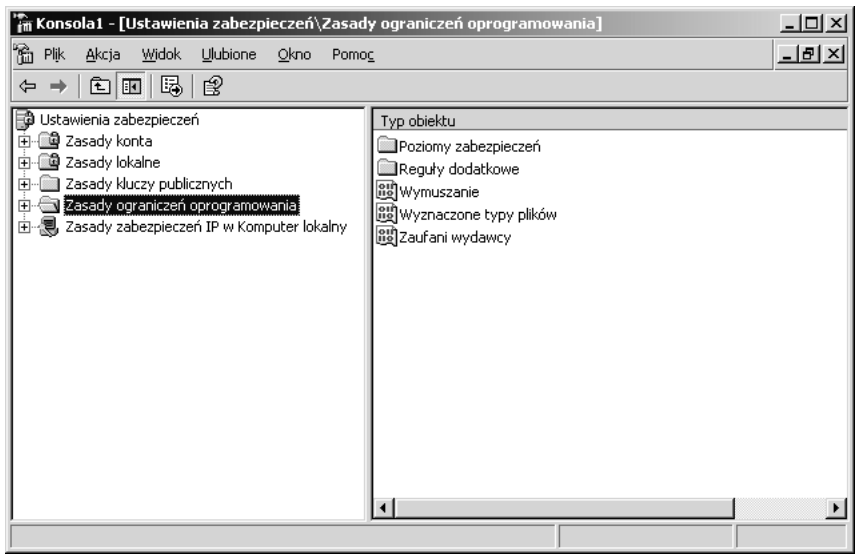
1. Z menu *Start* wybrać pozycję *Uruchom* i w polu *Otwórz* wprowadzić łańcuch `secpol.msc`. Alternatywnie z menu *Start* wybrać pozycję *Wszystkie programy/Narzędzia administracyjne/Zasady zabezpieczeń lokalnych*.
2. Zaznaczyć kontener *Zasady ograniczeń oprogramowania*.
3. Jeśli nie istnieje żadna zasada (rysunek 4.20), prawym przyciskiem myszy kliknąć kontener *Zasady ograniczeń oprogramowania* i z menu wybrać pozycję *Nowe zasady ograniczeń oprogramowania*.
4. Zostaną utworzone domyślne kontenery i obiekty pokazane na rysunku 4.21.

Ustalanie poziomu zabezpieczeń

Poziom zabezpieczeń określa, czy wszystkie aplikacje będą mogły być uruchamiane bez ograniczeń (niektóre z nich będą identyfikowane jako te, których nie można załadować), czy żaden program nie będzie mógł być uaktywniony (część aplikacji będzie identyfikowana jako te, które można uruchomić). Czy nie jest to proste? Niezależnie od podjętej decyzji trzeba będzie trochę się natrudzić. Ponadto trochę niezrozumiały może być używany interfejs.



Rysunek 4.20. *Domyślnie nie istnieje żadna zasada ograniczeń oprogramowania*



Rysunek 4.21. *Operacja definiowania zasad powoduje wygenerowanie kontenerów*

Aby umożliwić uruchamianie wszystkich programów, a następnie zablokować taką możliwość dla niektórych z nich, trzeba zastosować poziom zabezpieczeń *Bez ograniczeń* (nie ma on wcale innej nazwy, takiej jak na przykład „uruchamianie umożliwione", „OK" lub „możliwe uaktywnienie oprogramowania, gdy inaczej nie wskazano"). Domyślnie właśnie ten poziom jest aktywny. Można stwierdzić, że być może taka nazwa ma sens. W końcu są to zasady ograniczeń oprogramowania.

Dopóki dla oprogramowania nie zdefiniowano ograniczeń, jest bez ograniczeń. Jednak alternatywny poziom zabezpieczeń nosi nazwę *Niedozwolone*, a nie „ograniczone". Gdy wszystkie aplikacje są ograniczone, jest aktywny poziom *Niedozwolone*.

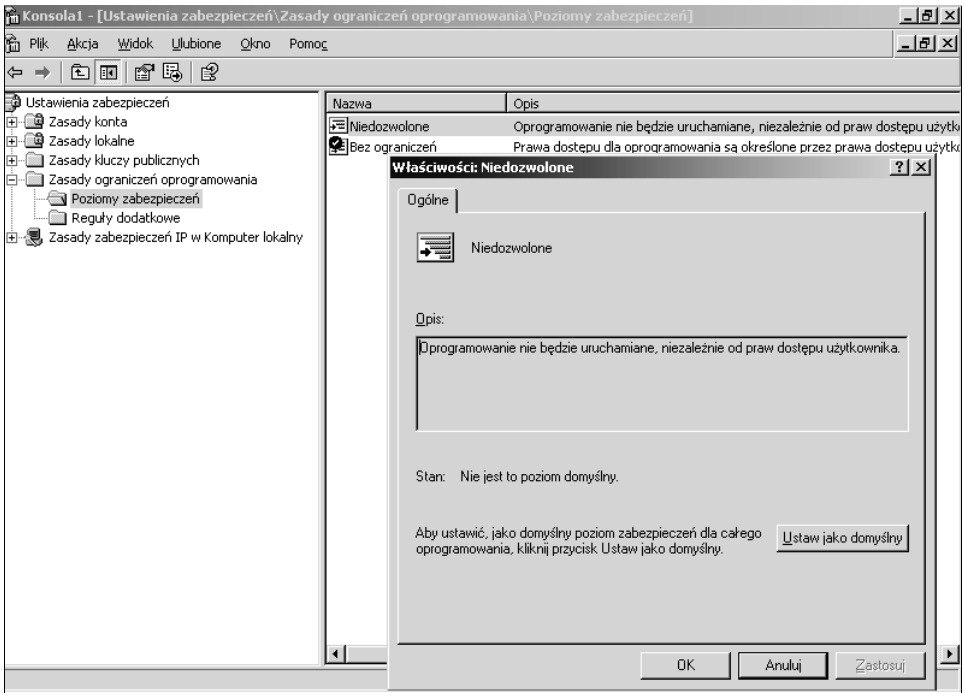
Tego typu problem z nazewnictwem występuje też w przypadku reguł. Każda reguła posiada własny poziom zabezpieczeń — *Niedozwolone* lub *Bez ograniczeń*. Więcej na ten temat będzie przy okazji omawiania poszczególnych typów reguł. Jeśli tylko zrozumie się znaczenie oficjalnie stosowanych nazw, uniknie się sytuacji, w której tysiące użytkowników nie będzie mogło skorzystać ze swoich komputerów. Trzeba pamiętać, że *Bez ograniczeń* oznacza, że można uruchomić wszystko, co nie zostało ograniczone. Z kolei *Niedozwolone* oznacza, że nic nie można uruchomić, jeśli nie zostanie to umożliwione. W praktyce poziom zabezpieczeń *Niedozwolone* powinno się ustawiać tylko wtedy, gdy znane są wszystkie aplikacje, które muszą być uruchomione. W przeciwnym razie należy zastosować poziom zabezpieczeń *Bez ograniczeń*, który domyślnie jest aktywny. Paradoksalnie, ustawienie poziomu zabezpieczeń *Niedozwolone*, a następnie usunięcie ograniczeń tylko dla tych programów, które mogą być uruchamiane, pozwala uzyskać bezpieczniejsze środowisko. Jednak jest to trudniejsze do osiągnięcia, niż mogłoby się początkowo wydawać.

W celu ustawienia poziomu zabezpieczeń dla zasady należy wykonać następujące kroki:

1. Rozwinąć węzeł *Zasady ograniczeń oprogramowania*.
2. Dwukrotnie kliknąć kontener *Poziomy zabezpieczeń*.
3. W prawym panelu pojawią się dostępne poziomy. Ikona poziomu, który w danej chwili jest domyślny, będzie opatrzona symbolem zaznaczenia. Jeśli zamierza się dokonać zmian, dwukrotnie należy kliknąć żądany poziom zabezpieczeń (*Bez ograniczeń* lub *Niedozwolone*).
4. Aby poziomowi zabezpieczeń przypisać rolę domyślnego, należy kliknąć przycisk *Ustaw jako domyślny* (rysunek 4.22).
5. Kliknąć przycisk *OK*.

Określanie zakresu obowiązywania zasady

Lokalne zasady ograniczeń oprogramowania dotyczą komputera, natomiast zasady ograniczeń oprogramowania dostępne w oknie przystawki *Edytor obiektów zasad grupy* obowiązują dla komputera lub użytkownika. Aby administratorzy nie byli objęci zakresem oddziaływania zasad, należy zastosować regułę wymuszania *Wszyscy użytkownicy oprócz administratorów lokalnych*. Można również uaktywnić regułę *Wszyscy użytkownicy*, co spowoduje, że zasada będzie dotyczyła



Rysunek 4.22. *Możliwa jest zmiana domyślnego poziomu zabezpieczeń*

wszystkich użytkowników, łącznie z członkami grupy *Administratorzy*. Jeśli użytkownicy muszą być na swoich komputerach członkami lokalnej grupy *Administratorzy*, nie wolno stosować reguły wymuszania *Wszyscy użytkownicy oprócz administratorów lokalnych*.

Inny typ reguły wymuszania decyduje o tym, czy będą ograniczone biblioteki oprogramowania, które są plikami z kodem nie uruchamianymi, lecz wykorzystywanymi przez pliki wykonywalne. W większości przypadków są to pliki bibliotek DLL. Należy zastosować regułę wymuszania *Wszystkie pliki oprogramowania oprócz bibliotek (takich jak DLL)* lub *Wszystkie pliki oprogramowania*. Użycie pierwszej reguły pozwala uprościć tworzenie zasady i zapobiega spadkowi wydajności. Reguła *Wszystkie pliki oprogramowania oprócz bibliotek (takich jak DLL)* zakłada, że gdy umożliwi się uruchomienie aplikacji, mają być dostępne jej biblioteki. Z kolei gdy zamierza się uniemożliwić uaktywnienie aplikacji, reguła zakłada, że jej biblioteki nie mają być dostępne. Reguła nie zarządza bibliotekami. Można też wymagać bardziej ścisłej kontroli. Jednak w tym przypadku trzeba pamiętać, że sprawdzanie biblioteki DLL może przyczynić się do spadku wydajności. Każda aplikacja uruchamiana przez użytkownika spowoduje sprawdzenie powiązanej z nią zasady. Gdy uruchomi się 10 programów, będzie miało miejsce

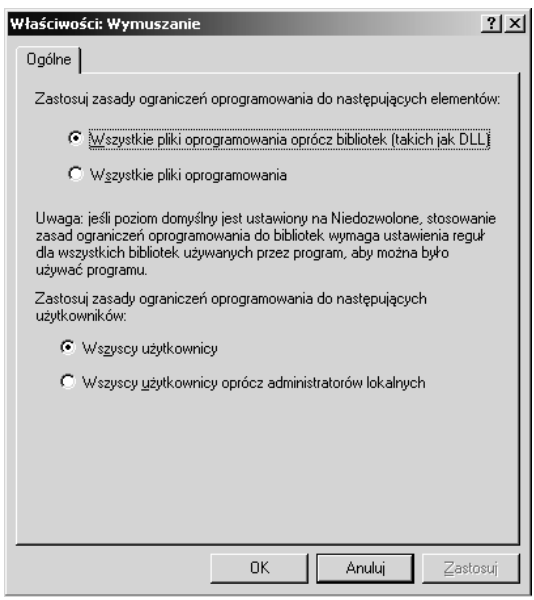
10 takich operacji. Jeśli każda aplikacja użyje 15 bibliotek DLL i uaktywni się regułę wymuszającą ich sprawdzanie, w sumie zostanie wykonanych 150 sprawdzeń. Biblioteki zawierają kod, do którego dostęp może być udzielony innym, niezarządzanym aplikacjom. Jeśli użycie bibliotek może spowodować przypadkowe lub celowe szkody, to aby je kontrolować, należy uaktywnić regułę wymuszania *Wszystkie pliki oprogramowania*.

OSTRZEŻENIE: Zastosowanie reguły *Wszystkie pliki oprogramowania* wiąże się z dodatkowym nakładem pracy polegającej na identyfikowaniu bibliotek DLL i zapisywaniu reguł

Trzeba wiedzieć, że gdy ustawi się poziom zabezpieczeń *Niedozwolone* i zastosuje regułę wymuszania *Wszystkie pliki oprogramowania*, to w celu umożliwienia uruchomienia określonej aplikacji konieczne będzie zidentyfikowanie wszystkich jej bibliotek i przypisanie im poziomu *Bez ograniczeń*. Może to być uciążliwe zadanie.

W celu skonfigurowania reguły wymuszania należy wykonać następujące kroki:

1. Zaznaczyć i rozwinąć węzeł *Zasady ograniczeń oprogramowania*.
2. W prawym panelu dwukrotnie kliknąć obiekt *Wymuszanie*, co spowoduje wyświetlenie okna właściwości (rysunek 4.23).

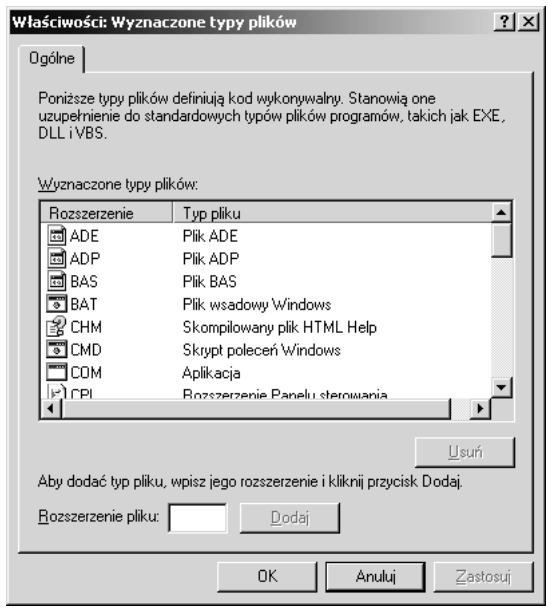


Rysunek 4.23. *Definiowanie dla zasady reguł wymuszania*

3. Określić regułę wymuszania zasad ograniczeń oprogramowania dla składników aplikacji.
4. Określić regułę wymuszania zasad ograniczeń oprogramowania dla użytkowników.
5. Kliknąć przycisk *OK*, aby zamknąć okno *Właściwości: Wymuszanie*.

Definiowanie typów plików identyfikujących pliki wykonywalne

Co definiuje plik wykonywalny? Jakiego typu pliki będą ograniczone, gdy ustawi się poziom zabezpieczeń *Niedozwolone*? Aby uzyskać odpowiedzi na te pytania, należy wyświetlić okno właściwości obiektu *Wyznaczone typy plików* powiązanego z zasadą (rysunek 4.24).



Rysunek 4.24. *W oknie Wyznaczone typy plików znajdują się typy plików wykonywalnych obsługiwanych przez zasadę ograniczeń oprogramowania*

W oknie można przeglądać, dodawać lub usuwać typy plików wykonywalnych programów objętych zakresem zasady. Dzięki temu oknu można uaktualniać zasady, gdy nowa aplikacja będzie korzystała z nowego typu plików wykonywalnych. Dostęp do tego okna konfiguracyjnego powinien być chroniony. Wynika to stąd, że użytkownik ze złymi intencjami, który będzie w stanie usunąć z okna rozszerzenie pliku, może ominąć zasady ograniczeń oprogramowania.

Aby sprawdzić lub zmodyfikować wyznaczone typy plików wykonywalnych, należy wykonać następujące kroki:

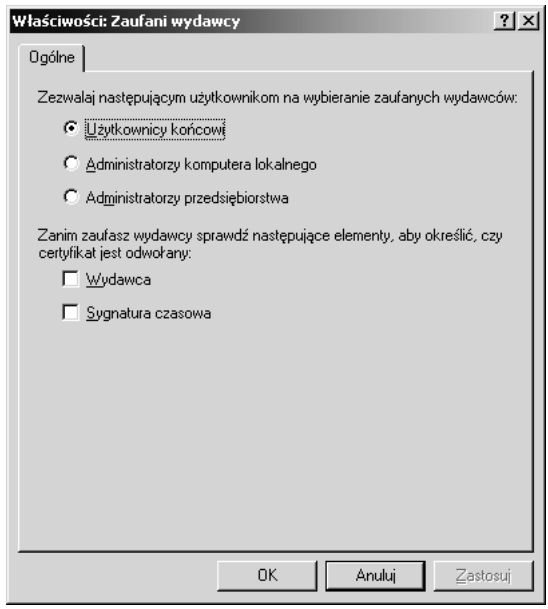
1. Zaznaczyć węzeł *Zasady ograniczeń oprogramowania*.
2. W prawym panelu dwukrotnie kliknąć obiekt *Wyznaczone typy plików* znajdujący się w węźle *Zasady ograniczeń oprogramowania*.
3. Przewinąć zawartość okna pokazanego na rysunku 4.24, aby zorientować się, jakie typy plików są identyfikowane jako składniki oprogramowania.
4. W celu usunięcia typu pliku zaznaczyć go, a następnie kliknąć przycisk *Usuń*. Kliknąć przycisk *Tak*, aby zamknąć wyświetlone okno komunikatu.
5. W celu dodania typu pliku w polu *Rozszerzenie pliku* podać jego rozszerzenie i kliknąć przycisk *Dodaj*.
6. Kliknąć przycisk *OK*, aby zamknąć okno.

Określanie ustawień obiektu Zaufani wydawcy

Zaufanymi wydawcami są organizacje, którym się ufa w zakresie udostępniania bezpiecznego kodu. Obiekt *Zaufani wydawcy* dotyczy jedynie kontrolek ActiveX i innych danych opatrzonych podpisem. Zaufane aplikacje są identyfikowane w systemie za pomocą ich certyfikatów. Aplikacje takie swój kod podpisują przy użyciu klucza prywatnego. Określając zaaprobowanych i zaufanych wydawców, można kontrolować to, czy na komputerze można uruchamiać oprogramowanie z podpisem i bez niego. W celu dodania zaufanych wydawców ich certyfikat należy zaimportować do kontenera *Zaufani wydawcy* znajdującego się w magazynie certyfikatów komputera.

Opcje obiektu *Zaufani wydawcy* widoczne na rysunku 4.25 umożliwiają zdecydowanie, kto może wybierać wydawców certyfikatów i co powinno zostać sprawdzone przed uznaniem certyfikatu za ważny.

W celu ustalenia, kto będzie upoważniony do wybierania zaufanych wydawców, należy kliknąć opcję *Użytkownicy końcowi*, *Administratorzy komputera lokalnego* lub *Administratorzy przedsiębiorstwa*. Domyślnie w przypadku całych domen lub grup komputerów tylko administratorzy domeny i przedsiębiorstwa mogą określać zaufanych wydawców. Jeśli zasada nie jest kontrolowana na wyższym poziomie, w lokalnym systemie akceptowaniem oferowanych certyfikatów jako zaufanych mogą się zajmować lokalni użytkownicy i administratorzy. Jeśli możliwością zatwierdzania certyfikatów będą dysponowali wyłącznie administratorzy, użytkownicy nie będą mogli kliknąć przycisku *OK*, gdy podczas pobierania lub instalowania oprogramowania zostanie im zaoferowany certyfikat. Gdy zastosuje się takie ograniczenie, uniemożliwi się na przykład użytkownikom podejmowanie decyzji dotyczących ufania kontrolkom ActiveX, które mogą próbować pobrać



Rysunek 4.25. *Opcje obiektu Zaufani wydawcy pozwalają określić, kto może akceptować wydawców, których obdarzy się zaufaniem*

z internetu lub otrzymać w załączniku wiadomości pocztowej. W końcu nikt nie musi przejść testu etycznego, aby zakupić lub uzyskać certyfikat podpisujący kod. Certyfikat umożliwia jedynie uwierzytelnienie w określony sposób podpisującego. Tworząc reguły certyfikatów, można w szerszym zakresie wykorzystać certyfikaty do kontrolowania oprogramowania.

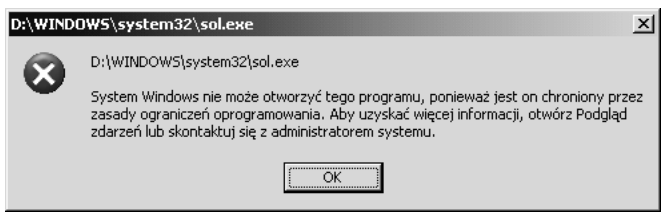
W celu określenia ważności certyfikatu można wymagać zastosowania informacji na temat wydawcy (opcja *Wydawca*), sygnatury czasowej (opcja *Sygnatura czasowa*) lub obu. Zaznaczenie opcji *Wydawca* spowoduje, że konieczne będzie sprawdzenie, czy certyfikat nie został anulowany. Z kolei kliknięcie opcji *Sygnatura czasowa* sprawi, że zostanie sprawdzone, czy certyfikat nie stracił ważności.

Definiowanie reguł zasad ograniczeń oprogramowania

Reguły zasad ograniczeń oprogramowania dotyczą określonych aplikacji (wykorzystując reguły mieszania, certyfikatów, ścieżek i adresów URL), ich lokalizacji (reguły ścieżek i adresów URL), a także wpisów rejestru. Z każdym typem reguły są związane zalety i wady. Przykładowo, jedna reguła ścieżek może zezwalać na uruchamianie dużej grupy aplikacji lub uniemożliwiać to. Jeśli jednak użytkownik będzie mógł skopiować plik w inne miejsce, może być w stanie wykonać kod.

PRZYKŁAD OGRANICZANIA OPROGRAMOWANIA

W firmie, z którą współpracowałam, pracownik sam zarządzał własnym komputerem. Pobierał z internetu fajne narzędzia i sterowniki, przynosił oprogramowanie z domu i spędzał wiele godzin przy grze *Pasjans* lub *FreeCell*. Pracownik przekonał nawet osoby dysponujące odpowiednimi możliwościami do tego, że jego konto musi być członkiem lokalnej grupy administratorów systemu Windows XP Professional. Później firma zastosowała zasady ograniczeń oprogramowania. Pierwszą rzeczą, którą pracownik zauważył, było to, że nie mógł grać w grę *Pasjans*. Po dwukrotnym kliknięciu skrótu programu *sol.exe* znajdującego się na pulpicie pojawiał się komunikat ostrzeżenia widoczny na rysunku 4.26. W związku z tym pracownik skopiował plik programu do innego folderu, aby mieć możliwość zagrania. Również to zakończyło się niepowodzeniem. Pracownik był mocno poirytowany. Stwierdził, że wiele innych dotychczasowych rozrywek stało się nieaktualnych. Nie można już było pobierać dowolnej aplikacji, a także okazało się, że pracownik nie dysponował pełnymi przywilejami administratora komputera. Utracił kontrolę nad nim i nie mógł znaleźć sposobu na ominięcie restrykcji. W końcu sfrustrowany pracownik dowiedział się, że przyczyną kłopotów jest nowy administrator, który przekonał zarząd do zastosowania zasad ograniczeń oprogramowania. Pracownik próbował dokonać sabotażu skierowanego przeciwko zasadom i nowemu administratorowi. W tym celu zaczął usuwać pliki wykonywalne aplikacji, których uruchamianie przypuszczalnie było mu umożliwione, lub przenosił programy w miejsce identyfikowane przez ścieżki objęte zakresem zasad ograniczających. Gdy pracownikowi nie udało się uruchomić programów, informował o tym i dołączał wszystkie komunikaty o błędzie, które udało mu się wygenerować.



Rysunek 4.26. *Gdy użytkownik spróbuje uruchomić ograniczone oprogramowanie, pojawi się komunikat ostrzeżenia*

Nowy administrator omal nie stracił pracy, natomiast zasady ograniczeń oprogramowania były obwiniane za problemy. Na szczęście administrator mógł uaktywnić inspekcję komputera pracownika i stwierdzić, jakie działania podejmował. Ponieważ dysponował takim dowodem, to pracownik musiał odejść z firmy.

Od tego czasu wszystkie zasady ograniczeń oprogramowania były wspierane przez odpowiednie listy ACL plików, które uniemożliwiały wykonanie szkodliwych operacji, wspomagały ograniczanie (odmowa wykonywania) i rejestrowały próby uzyskania przez użytkownika dostępu i przeprowadzenia ewentualnych ataków.

Każda reguła mieszania może być użyta tylko dla jednego pliku wykonywalnego, uniemożliwiając użytkownikowi jego uruchomienie niezależnie od tego, jaka będzie źródłowa lokalizacja pliku, jego ścieżka lub nazwa. Jeśli jednak oprogramowanie zmieni się (wirus ulegnie mutacji lub pojawi się nowa wersja gry), konieczne będzie utworzenie kolejnej reguły. Najlepiej nie polegać tylko na jednym typie reguły, a zwłaszcza nie definiować reguł i nie pozostawać w przekonaniu, że nigdy nie będzie trzeba ich ponownie konfigurować. Ponadto warto nawet zastosować listy ACL plików, aby dodatkowo kontrolować dostęp użytkownika do obiektów wykonywalnych.

Tworzone mogą być następujące cztery typy reguł:

- reguły mieszania,
- reguły certyfikatów,
- reguły ścieżki uwzględniające reguły ścieżek plików i rejestru,
- reguły strefy internetowej.

Aby sfinalizować definiowanie zasad ograniczeń oprogramowania, trzeba utworzyć reguły. Najpierw należy stwierdzić, które programy muszą być uruchamiane, a które nie. W dalszej kolejności należy określić typ użytych reguł, a następnie je utworzyć. Zadanie polegające na zidentyfikowaniu aplikacji, które powinny i nie powinny być uaktywniane, nie jest proste. Konieczne będzie sprawdzenie zasady zabezpieczeń i zadań realizowanych przez użytkowników komputerów, a następnie skonsultowanie się z zarządem. Sugestie zamieszczone w tabeli 4.3 mogą być pomocne w podjęciu decyzji dotyczącej typu reguł, które zostaną użyte.

Tabela 4.3. *Najlepsze praktyki dotyczące określania typów reguł*

Reguła	Przeznaczenie
Reguła mieszania	Zezwala na uruchomienie pliku programu posiadającego określoną wartość mieszania lub uniemożliwia to.
Reguła strefy	Umożliwia instalowanie oprogramowania pochodzącego z zaufanych witryn WWW strefy internetowej.
Reguła ścieżki	Zezwala na uruchomienie pliku programu, który zawsze jest instalowany w tym samym miejscu lub uniemożliwia to.
Reguła certyfikatu	Identyfikuje zestaw skryptów, które mogą być wykonywane.
Reguła ścieżki rejestru	Zezwala na uruchomienie pliku programu, którego ścieżka jest przechowywana w rejestrze lub uniemożliwia to.
Reguła ścieżki zgodnej z formatem UNC (np. *\\SERWER\udział*)	Zezwala na uruchomienie zestawu skryptów zlokalizowanych na serwerze lub uniemożliwia to.
Dwie reguły ścieżki — **.vbs* z ustawionym poziomem zabezpieczeń *Niedozwolone* i *\\LOGIN-XRV\udział*.vbs* z określonym poziomem *Bez ograniczeń*	Dwie reguły ścieżki uniemożliwiają uruchomienie wszystkich plików skryptów *.vbs* z wyjątkiem skryptów logowania.
Reguła ścieżki *flcss.exe* z ustawionym poziomem *Niedozwolone*	Uniemożliwia uaktywnienie nowego wirusa, którego plik zawsze nosi nazwę *flcss.exe*.

Gdy wiele reguł dotyczy tego samego pliku programu, kolejność ich stosowania będzie zależeć od ustalonej zasady pierwszeństwa. Kolejność reguł (według pierwszeństwa) jest następująca:

- reguła mieszania,
- reguła certyfikatu,
- reguła ścieżki,
- reguła strefy internetowej.

Jeśli na przykład w przypadku zasady, dla której ustawiono poziom zabezpieczeń *Bez ograniczeń*, reguła ścieżki uniemożliwia uruchomienie oprogramowania, natomiast reguła mieszania pozwala na to, pierwszeństwo będzie mieć druga reguła, dzięki czemu aplikację będzie można uaktywnić. Gdy zastosuje się wiele reguł ścieżek, jako pierwsza zostanie użyta najbardziej restrykcyjna. Jeśli na przykład regułę ścieżki zdefiniowano dla folderu *C:\moje_oprogramowanie*, uniemożliwi ona uruchomienie aplikacji (dla reguły jest ustawiony poziom zabezpieczeń *Niedozwolone*). Jeśli jednak dla folderu *C:\moje_oprogramowanie\zatwierdzone* zdefiniowano kolejną regułę ścieżki i ustawiono poziom zabezpieczeń *Bez ograniczeń*, będzie można uruchomić programy zlokalizowane w tym folderze.

UWAGA: Reguły dotyczące wirusów

Zasady ograniczeń oprogramowania nie mają zastępować programów antywirusowych. Trzeba pamiętać o tym, że reguły mieszania nie zadziałają, gdy pliki zostaną zmodyfikowane (wirusy często się mutują). Ponadto często zmieniają się nazwy wirusów. Programy antywirusowe rozpoznają wzorce lub sygnatury wirusów i są bardziej skuteczne w zapobieganiu infekcji. Warto jednak utworzyć zasadę ograniczeń oprogramowania, która zwiększy poziom ochrony, gdy zidentyfikuje się nowy wirus, dla którego producent programu antywirusowego nie opracował jeszcze sygnatury.

Przed zastosowaniem reguły w systemach produkcyjnych powinno się ją sprawdzić w środowisku testowym. Po skonfigurowaniu reguły, lecz jeszcze przed rozpoczęciem testowania jej należy ponownie uruchomić system, aby mieć pewność, że reguła zaczęła obowiązywać.

Reguły mieszania

Działanie reguł mieszania polega na generowaniu wartości mieszania dla pliku wykonywalnego. Funkcja mieszania jest w stanie pobrać dowolną ilość informacji i zredukować ją do unikatowej wartości mieszania o standardowym rozmiarze. W idealnej sytuacji żadne dwa pliki programów przetworzone przez ten sam algorytm mieszania nie spowodują wygenerowania identycznej wartości mieszania.

Za pomocą reguły mieszania można ograniczać programy dysponujące podpisem i pozbawione go. W przypadku podpisanego programu wartość mieszania może być generowana za pomocą algorytmu MD5 lub SHA-1. Tworzona reguła mieszania użyje dowolnej możliwej wartości mieszania. Jeśli plik nie jest podpisany, zostanie użyty algorytm mieszania MD5. Reguła mieszania zawiera wartość mieszania, długość pliku i identyfikator określający zastosowany algorytm mieszania.

UWAGA: Zawsze należy wybierać algorytmy mieszania odporne na kolizję

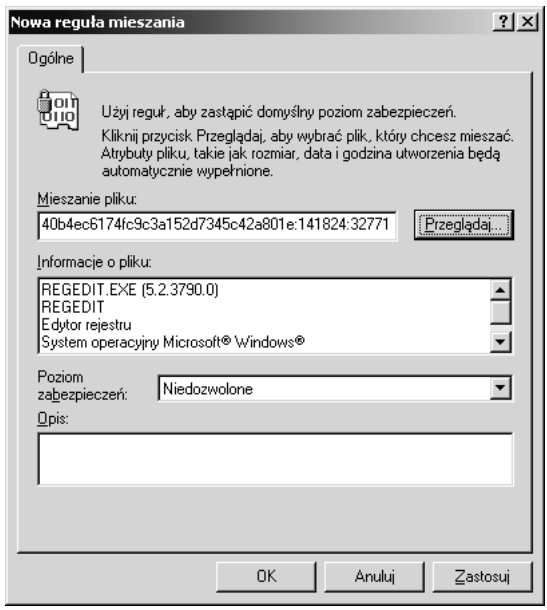
Choć kolizja (wygenerowanie dla różnych danych identycznej wartości mieszania) jest zawsze możliwa, jej wystąpienie jest mało prawdopodobne. Wybierając algorytmy mieszania, projektanci powinni rozważyć te, które w danej chwili są uważane ze mniej podatne na kolizje. To samo powinni uwzględnić administratorzy wybierający aplikacje. W celu uzyskania dodatkowych informacji należy zapoznać się z dokumentem dostępnym pod adresem *http://www.rsasecurity.com/rsalabs/node.asp?id=2738*, w którym zamieszczono wyniki badań przeprowadzonych w 2004 r., dotyczących kolizji związanych ze stosowaniem algorytmu MD5.

Gdy użytkownik próbuje uruchomić program, dla którego zdefiniowano regułę mieszania, jest generowana nowa wartość mieszania i porównywana z wartością znajdującą się w regule. Jeśli wartości okażą się zgodne i dla reguły mieszania ustawiono poziom zabezpieczeń *Niedozwolone*, program nie zostanie uaktywniony, niezależnie od tego, skąd dokonano próby jego uruchomienia. Jeśli na przykład regułę mieszania utworzono dla programu *sol.exe*, będzie dla niego obowiązywała, niezależnie od lokalizacji pliku wykonywalnego lub miejsca, z którego spróbuje się go uaktywnić. Nadal tak będzie, nawet gdy zmieni się nazwę pliku programu. Użytkownicy nie mogą obejść reguły, kopiując plik do innego folderu. Jeśli jednak plik wykonywalny zostanie zmodyfikowany, wartość mieszania wygenerowana przy próbie jego uruchomienia nie będzie zgodna z wartością mieszania żadnej z reguł, co spowoduje uaktywnienie programu. W celu zdefiniowania reguły mieszania należy wykonać następujące kroki:

1. Wyświetlić zawartość węzła *Zasady ograniczeń oprogramowania*.
2. Prawym przyciskiem myszy kliknąć kontener *Reguły dodatkowe* i z menu wybrać pozycję *Nowa reguła mieszania*.
3. W oknie dialogowym *Nowa reguła mieszania* kliknąć przycisk *Przeglądaj*.
4. Odszukać i wybrać plik wykonywalny, dla którego zostanie zdefiniowana reguła mieszania.

5. Kliknąć przycisk *Otwórz*, aby zatwierdzić wybór pliku i powrócić do okna dialogowego.

6. Dla pliku zostanie wygenerowana wartość mieszania i umieszczona w polu tekstowym *Mieszanie pliku*. Pole *Informacje o pliku* zostanie automatycznie wypełnione (rysunek 4.27).



Rysunek 4.27. *Po odszukaniu pliku wartość mieszania zostanie skopiowana z cyfrowego podpisu pliku lub wygenerowana*

7. W polu *Poziom zabezpieczeń* wybrać wartość *Niedozwolone* lub *Bez ograniczeń*. Jeśli aktualnym poziomem jest *Bez ograniczeń*, w celu uniemożliwienia uruchomienia określonego programu należy ustawić wartość *Niedozwolone*. Gdy jest aktywny poziom zabezpieczeń *Niedozwolone*, po wybraniu wartości *Bez ograniczeń* możliwe będzie uruchomienie programu. Trzeba pamiętać o tym, że poziom *Niedozwolone* uniemożliwia uaktywnienie programu, natomiast poziom *Bez ograniczeń* zezwala na to.

8. Wprowadzić opis reguły.

9. Kliknąć przycisk *OK*, aby zakończyć tworzenie reguły i powrócić do okna zasad ograniczeń oprogramowania.

UWAGA: Jeśli plik wykonywalny ulegnie zmianie, związana z nim reguła mieszania przestanie obowiązywać

Trzeba pamiętać, że gdy plik wykonywalny zostanie zmodyfikowany, związana z nim reguła mieszania przestanie obowiązywać. Nie jest istotne, jak znacząca jest zmiana. Dostępne są proste i darmowe narzędzia, które umożliwiają wprowadzenie niewielkich modyfikacji. Program *reshack.exe* jest przykładem takiego narzędzia. Często jest stosowany do modyfikowania zasobów (takich jak ikona) pliku wykonywalnego systemu Windows. Zdeterminowany użytkownik może z łatwością znaleźć takie narzędzie i opanować jego obsługę. Powoduje to konieczność uświadomienia w zakresie zasad bezpieczeństwa. Nie powinno się wyjaśniać użytkownikom, w jaki sposób wprowadzać tego typu zmiany, lecz poinformować administratorów, że coś takiego jest możliwe, by mogli opracować alternatywne techniczne rozwiązania przeciwdziałające temu. W takim przypadku lepszym wariantem będzie najpierw uniemożliwienie uaktywnienia wszystkich aplikacji, a następnie zezwalanie na uruchomienie tylko zaakceptowanych plików wykonywalnych.

Reguły certyfikatów

Reguły certyfikatów mogą zezwalać na uruchomienie oprogramowania lub blokować taką możliwość na podstawie cyfrowego podpisu powiązanego z plikiem. Reguła certyfikatu identyfikuje certyfikat wydawcy podpisujący kod aplikacji. Reguła sprawdza plik, korzystając z wartości mieszania znajdującej się w podpisie pliku. Położenie pliku nie ma znaczenia. Jeśli aplikację podpisano przy użyciu jednego z certyfikatów określonych w regułach certyfikatów, dla pliku wykonywalnego zostanie zastosowany poziom zabezpieczeń ustawiony dla reguły. Regułę certyfikatu można wykorzystać, gdy zasady zabezpieczeń firmy wymagają, aby wszystkie skrypty ActiveX były podpisane za pomocą określonego cyfrowego podpisu.

Reguły certyfikatów obowiązują tylko typy plików zdefiniowane w elemencie *Wyznaczone typy plików*. Aby zdefiniować tego typu regułę, trzeba dysponować kopią certyfikatu powiązanego z podpisanymi plikami. Reguły certyfikatów można też uaktywniać za pomocą przystawki *Zasady grupy*. Przykładowo, aby zastosować regułę certyfikatu zezwalającą na wykonanie tylko tych skryptów języka Visual Basic, które zostały podpisane przy użyciu certyfikatu organizacji, należy wykonać następujące operacje:

- umożliwienie za pomocą przystawki *Zasady grupy* stosowania reguł certyfikatów;
- podpisanie skryptów języka Visual Basic;
- umieszczenie kopii certyfikatu w dostępnej lokalizacji;

- zdefiniowanie reguły ścieżki uniemożliwiającej wykonanie wszystkich skryptów tego typu (**.vbs*);
- utworzenie reguły certyfikatu identyfikującej certyfikat i ustawienie dla niej poziomu zabezpieczeń *Bez ograniczeń*.

Aby umożliwić stosowanie reguł certyfikatów, należy wykonać następujące kroki:

1. Uruchomić edytor zasad grupy obowiązujących dla lokalnego komputera (przystawka *Edytor obiektów zasad grupy* w przypadku domeny usługi Active Directory lub narzędzie *Zasady zabezpieczeń lokalnych*, gdy korzysta się z autonomicznego komputera).
2. Zlokalizować węzeł *Ustawienia zabezpieczeń/Zasady lokalne/Opcje zabezpieczeń*.
3. Dwukrotnie kliknąć zasadę *Ustawienia systemowe: użyj reguł certyfikatów plików wykonywalnych systemu Windows dla Zasad ograniczeń oprogramowania*.
4. Zaznaczyć opcję *Włączone* (rysunek 4.28).

Rysunek 4.28. *W celu umożliwienia użycia reguł certyfikatów trzeba uaktywnić odpowiednią opcję zabezpieczeń*

5. Kliknąć przycisk *OK*, aby zamknąć okno i uaktywnić nową opcję zabezpieczeń.

W celu utworzenia reguły certyfikatu należy wykonać następujące kroki:

1. Wyświetlić zawartość węzła *Zasady ograniczeń oprogramowania*.
2. Prawym przyciskiem myszy kliknąć kontener *Reguły dodatkowe* i z menu wybrać pozycję *Nowa reguła certyfikatu*.
3. Za pomocą przycisku *Przeglądaj* zlokalizować certyfikat.

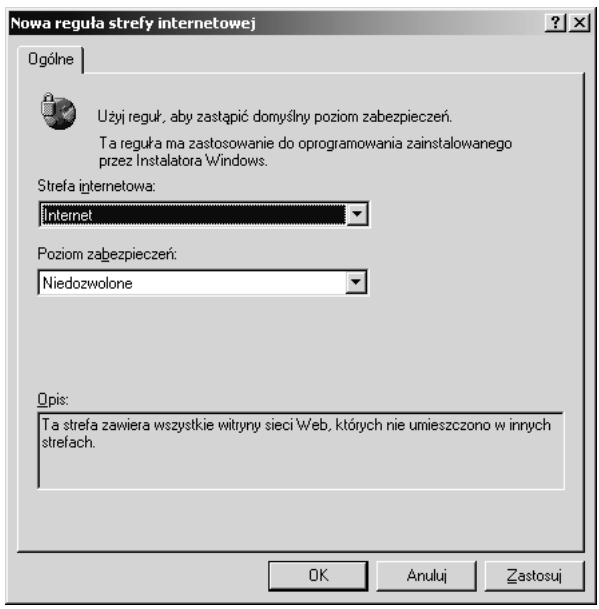
4. Ustalić poziom zabezpieczeń.
5. Kliknąć przycisk *OK*, aby zakończyć definiowanie reguły.

Reguły strefy internetowej

Reguły strefy internetowej dotyczą aplikacji instalowanych za pomocą instalatora systemu Windows. Tego typu reguły określają, czy można zainstalować aplikację pochodzącą z witryny WWW należącej do strefy internetowej. Można wybierać takie strefy jak *Komputer lokalny*, *Internet*, *Lokalny intranet*, *Witryny z ograniczeniami* i *Zaufane witryny*.

Aby zdefiniować regułę strefy internetowej, należy wykonać następujące kroki:

1. Wyświetlić zawartość węzła *Zasady ograniczeń oprogramowania*.
2. Prawym przyciskiem myszy kliknąć kontener *Reguły dodatkowe* i z menu wybrać pozycję *Nowa reguła strefy internetowej*.
3. Wybrać strefę, która będzie kontrolowana.
4. Ustalić dla reguły poziom zabezpieczeń (rysunek 4.29).



Rysunek 4.29. *Reguły strefy internetowej określają, czy można zainstalować aplikację pochodzącą z witryny WWW należącej do kontrolowanej strefy*

5. Kliknąć przycisk *OK*, aby zakończyć definiowanie reguły.

Reguły ścieżek plików i rejestru

Reguły ścieżek są powiązane z zasadami ograniczającymi aplikacje, których pliki wykonywalne znajdują się w miejscu identyfikowanym przez określoną ścieżkę. Można wyróżnić reguły ścieżek plików i rejestru. Definiując systemową ścieżkę plików, można zastosować znaki wieloznaczne, takie jak * i ?, a także zmienne środowiskowe, takie jak `%ProgramFiles%` lub `%SystemRoot%`. Jeśli lokalizacja pliku systemowego może być inna na poszczególnych komputerach, a znana jest ścieżka rejestru identyfikująca jego położenie, można utworzyć regułę ścieżki rejestru. Ścieżki rejestru muszą być zawarte w znakach %, natomiast identyfikowane przez nie wpisy muszą być typu `REG_SZ` lub `REG_EXPAND_SZ`. Nie można w ścieżce rejestru umieszczać skrótów, takich jak *HKLM* lub *HKCU*.

Jeśli dysponuje się programami, które muszą być uruchamiane podczas ładowania systemu, i realizuje się to za pomocą klucza rejestru *Run*, dla ścieżki rejestru *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run* należy utworzyć regułę ścieżki i ustawić dla niej poziom zabezpieczeń *Bez ograniczeń*.

Jeśli programy nie mają być uruchamianie podczas ładowania systemu, powinno się zdefiniować identyczną regułę ścieżki jak powyższa i ustawić dla niej poziom zabezpieczeń *Niedozwolone*.

W celu utworzenia reguły ścieżki należy wykonać następujące kroki:

1. Wyświetlić zawartość węzła *Zasady ograniczeń oprogramowania*.
2. Prawym przyciskiem myszy kliknąć kontener *Reguły dodatkowe* i z menu wybrać pozycję *Nowa reguła ścieżki*.
3. Wprowadzić ścieżkę (rysunek 4.30).
4. Kliknąć przycisk *OK*, aby zamknąć okno i zakończyć definiowanie zasady.

„HAKOWANIE" POZIOMÓW ZABEZPIECZEŃ ZASAD OGRANICZAJĄCYCH OPROGRAMOWANIE

Administratorzy często są w delikatny sposób przekonywani do tego, aby ufać kontrolkom służącym do zarządzania, znajdującym się w graficznym interfejsie użytkownika, a także publicznie dostępnej dokumentacji dotyczącej narzędzi wiersza poleceń i modyfikowania rejestru. Często zapominają o sporej ilości kodu umieszczonego pod udostępnianym interfejsem, który w równym stopniu mógł zostać napisany przez osoby mające dobre, jak i osoby mające złe intencje. Słowo „hakowanie" zawarte w powyższym nagłówku nie powinno być kojarzone z nielegalnymi działaniami lub lekceważeniem potrzeby właściwego testowania i planowania. Słowo ma pełnić rolę ostrzeżenia. Nie sugeruje się w ten sposób Czytelnikowi, aby spróbował nielegalnie zdobyć kod źródłowy systemu Windows lub zastosować dla niego inżynierię odwrotną.

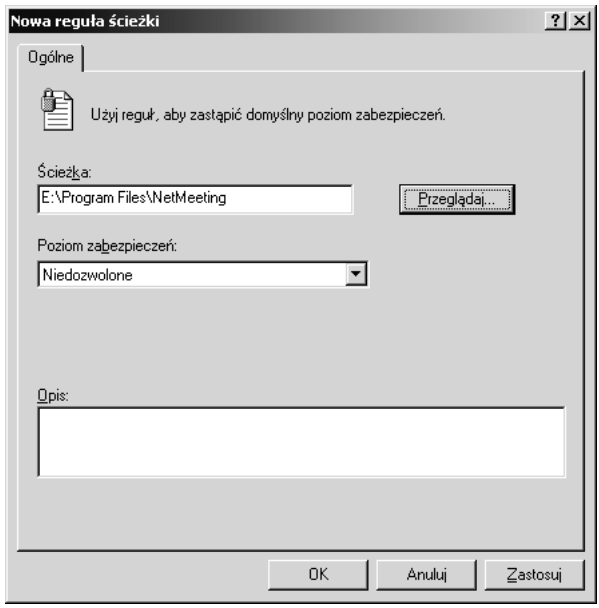
Podobnie jak w przypadku każdego dobrego „haka", tu omówiony nie jest przeznaczony dla każdego administratora systemu Windows ani nadający się do zastosowania w dowolnej sytuacji. Ponadto wymaga dokładnego sprawdzenia w zarządzanym środowisku w celu stwierdzenia, czy będzie się nadawał. Trzeba uprzedzić, że poniższy „hak" może uszkodzić aplikacje. Zalecane jest szczegółowe zapoznanie się z artykułami dostępnymi pod adresami *http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dncode/html/secure11152004.asp* i *http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dncode/html/secure01182005.asp*. W artykułach omówiono inne metody ograniczania praw użytkowników bez stosowania niezależnej tożsamości użytkownika. Zawarto w nich też ostrzeżenie, że wymienione technologie mogą ulec zmianie w przyszłych wersjach systemu Windows.

„Hak" polega na zmodyfikowaniu rejestru w taki sposób, że dostępne stają się trzy nowe poziomy zabezpieczeń zasad ograniczeń oprogramowania. Oto one:

- ***Użytkownik podstawowy***. Użytkownik nie dysponuje prawami administratora lub użytkownika zaawansowanego.
- ***Z ograniczeniami***. Gałąź rejestru *HKEY_CURRENT_USER* jest tylko do odczytu. Zmienna środowiskowa `%USERPROFILE%` jest niedostępna. Nie działają niektóre operacje kryptograficzne, takie jak negocjowanie związane z protokołem SSL.
- ***Niezaufane***. Jeszcze większe ograniczenia niż w przypadku poziomu *Z ograniczeniami*. Jednak nie są udokumentowane.

Każdy z wymienionych poziomów umożliwia uruchomienie programu, dla którego ustalono poziom zabezpieczeń *Bez ograniczeń*, z tym że zmniejszając przywileje użytkownika, ogranicza zakres operacji, które może wykonać. Jest to ważne, ponieważ użytkownicy mogą wymagać określonych praw do uruchomienia wybranych aplikacji, ale też będą w stanie uaktywnić wiele innych programów, nie posiadając tych uprawnień. Uruchamianie dowolnej aplikacji z jak najmniejszymi przywilejami zawsze będzie uważane za polecaną praktykę dotyczącą zabezpieczeń. Przykładowo, nie jest dobrym pomysłem uruchomienie programu Internet Explorer z uprawnieniami administratora w celu przeglądania stron internetowych. Aby ograniczyć to, kto może korzystać z przeglądarki Internet Explorer, należy zastosować zasadę ograniczeń oprogramowania i ustawić poziom zabezpieczeń *Użytkownik podstawowy*.

W celu udostępnienia w węźle *Zasady ograniczeń oprogramowania* nowego poziomu zabezpieczeń *Użytkownik podstawowy* należy zmodyfikować rejestr. Po uruchomieniu programu *Edytor rejestru* należy odszukać klucz *HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers*, a następnie utworzyć wpis typu `DWORD` o nazwie *Levels* i wartości *0x00031000*.



Rysunek 4.30. *Reguły ścieżki plików i rejestru identyfikują lokalizacje, z których aplikacje mogą być uruchamiane lub nie*

Rozwiązywanie problemów związanych z zasadami ograniczeń oprogramowania

Wiele problemów dotyczących zasad ograniczeń oprogramowania jest wynikiem tego, że administratorzy lub użytkownicy nie rozumieją, w jaki sposób zasady są tworzone. Może wystąpić kilka następujących problemów:

- Użytkownicy narzekają, że na ich komputerach pojawia się komunikat *System Windows nie może otworzyć tego programu, ponieważ jest on chroniony przez zasady ograniczeń oprogramowania*. Może być on zgodny z oczekiwaniami, gdy użytkownicy nie powinni mieć możliwości uruchomienia aplikacji. Zanim zmodyfikuje się zasadę ograniczeń oprogramowania, należy zastanowić się, dlaczego ją zdefiniowano. Jeśli użytkownik powinien być w stanie uaktywnić aplikację, należy poszukać konfliktów, które mogą występować między zasadami (należy sprawdzić kolejność ich stosowania) i stwierdzić, czy zasadę zdefiniowano dla właściwej jednostki organizacyjnej, domeny usługi Active Directory lub komputera (dotyczy lokalnych zasad zabezpieczeń).

- Użytkownik zgłasza, że nie może uruchomić aplikacji, mimo że słusznie dysponuje odpowiednim prawem. W przypadku domeny istnieje kilka zasad ograniczających oprogramowanie, które mogą obowiązywać dla użytkownika. Sprawdzając identyfikator GUID powiązany z regułą, która jest przyczyną problemu, można zidentyfikować zasadę sprawiającą kłopoty. Każdej regule zasad ograniczających oprogramowanie jest przypisywany unikatowy identyfikator GUID. Identyfikator ten będzie zawarty w zdarzeniu dziennika dotyczącym użytkownika. Uruchamiając program `gpresult` wchodzący w skład pakietu Resource Kit systemu Windows lub narzędzie *Wynikowy zestaw zasad* (RSoP, *Resultant Set of Policy*), można zidentyfikować zasadę grupy zawierającą identyfikator GUID, a tym samym regułę. Inspekcja zasady ograniczeń oprogramowania pozwala wykryć pomyłkę, którą można następnie usunąć.
- Administratorzy narzekają na to, że przy próbie uruchomienia narzędzia z poziomu wiersza poleceń pojawia się komunikat `System nie może wykonać określonego programu`. Przyczyną tego problemu może być zasada ograniczeń oprogramowania, ponieważ taki komunikat jest generowany, gdy zasada uniemożliwia uruchomienie programu z poziomu wiersza poleceń. W tym przypadku należy sprawdzić, czy administrator dysponuje prawami do uruchamiania aplikacji i poszukać ewentualnych konfliktów. Jeśli administrator powinien mieć możliwość uaktywnienia programu, natomiast użytkownicy nie, po otwarciu okna właściwości obiektu *Wymuszanie* należy kliknąć opcję *Wszyscy użytkownicy oprócz administratorów lokalnych*.
- Zasada ograniczeń oprogramowania znajdująca się w oknie narzędzia *Ustawienia zabezpieczeń lokalnych* nie została uwzględniona. Zasady ograniczeń oprogramowania zdefiniowane w przypadku usługi Active Directory będą miały pierwszeństwo przed lokalnymi zasadami. Należy sprawdzić, czy w bazie danych usługi Active Directory istnieje zasada ograniczeń oprogramowania.
- Lokalna zasada zabezpieczeń jest stosowana, nawet pomimo tego, że istnieje zasada zdefiniowana na poziomie domeny. W tym przypadku należy upewnić się, czy zostały uwzględnione modyfikacje zasady usługi Active Directory. Dodatkowo należy sprawdzić, czy lokalny komputer pobiera zasadę z kontrolera domeny.
- Modyfikacja zasad ograniczeń oprogramowania spowodowała, że nikt nie może się zalogować na komputerze. Powodem takiego stanu rzeczy może być to, że zdefiniowano regułę, która uniemożliwia uruchomienie programów, od których zależy udane załadowanie systemu, w tym okienka logowania. Aby przywrócić możliwość poprawnego uruchomienia systemu, należy skorzystać z trybu awaryjnego, zalogować się jako lokalny administrator i poprawić zasadę. Po włączeniu trybu awaryjnego zasady ograniczeń oprogramowania są nieaktywne.

- Reguła stworzona w celu ograniczenia określonej aplikacji nie jest używana. Być może powodem jest to, że typu pliku programu nie uwzględniono w obiekcie *Wyznaczone typy plików* znajdującym się w węźle *Zasady ograniczeń oprogramowania*. Typ pliku należy dodać do listy.

Często w identyfikacji przyczyny problemów z zasadami ograniczeń oprogramowania pomocny będzie zdrowy rozsądek, przeglądanie ustawień i odwoływanie się do typowych problemów, o których wcześniej wspomniano. Jednak gdy wszystko to nie umożliwi wykrycia przyczyny problemu, można uaktywnić rozszerzone rejestrowanie, które pozwala na zapisywanie każdej operacji związanej z zasadami ograniczeń oprogramowania. W celu włączenia rejestrowania należy wykonać następujące kroki:

1. Utworzyć klucz rejestru *HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\Codeidentifiers*.
2. Zdefiniować wpis *LogFileName* o wartości ciągu.
3. Wprowadzić wartość, którą jest ścieżka pliku dziennika.

Aby wyłączyć rejestrowanie, wpis należy usunąć z rejestru.

Najlepsze praktyki dotyczące zasad ograniczeń oprogramowania

Tworząc zasady ograniczeń oprogramowania, dąży się do uzyskania jak najlepszych rezultatów. Zasady mogą być narzędziem o dużych możliwościach, umożliwiającym kontrolowanie tego, jakie programy będzie można uruchamiać na komputerze. Jednak zasady mogą również ograniczyć produktywność i uniemożliwiać wykonanie powierzonych zadań. Microsoft zaleca korzystanie z następujących praktyk dotyczących zasad ograniczeń oprogramowania:

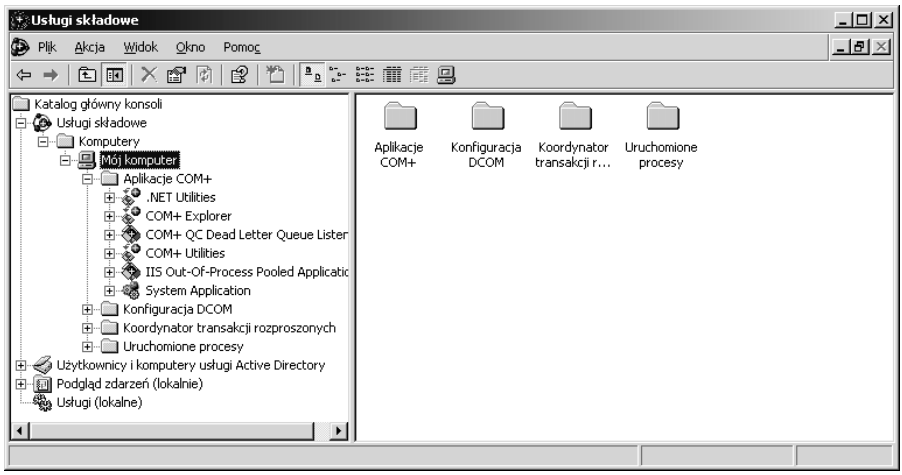
- W przypadku użycia zasad ograniczeń oprogramowania w domenie nie wolno ich definiować w obiekcie GPO domeny. Zawsze dla takich zasad należy tworzyć oddzielny obiekt GPO. Ze względu na to, że domyślnie nie są definiowane żadne zasady ograniczeń oprogramowania, w celu wycofania nieprawidłowej zasady można ją usunąć lub wyłączyć, a następnie zezwolić na ponowne zastosowanie obiektu GPO domeny.
- Nie należy tworzyć łącza z zasadą ograniczeń oprogramowania innej domeny, ponieważ spowoduje to spadek wydajności.

- Należy stosować filtrowanie interfejsu WMI. Można zdefiniować filtr, który ograniczy zakres oddziaływania obiektu GPO na przykład do komputerów, na których zainstalowano określoną wersję dodatku Service Pack. Filtry interfejsu WMI są definiowane w oknie właściwości obiektu GPO.
- Należy stosować filtrowanie zabezpieczeń. Można określić, dla jakich grup użytkowników będzie obowiązywała zasada. Polega to na umieszczeniu grup na zakładce *Zabezpieczenia* znajdującej się w oknie właściwości obiektu GPO i sprawdzeniu (gdy dla grup nie mają obowiązywać zasady oprogramowania), czy nie dysponują uprawnieniem powodującym zastosowanie zasad grupy. Jeśli zadba się o to, aby grupy nie posiadały uprawnienia umożliwiającego odczytywanie zasady, można zwiększyć wydajność. Gdy grupy nie będą miały takiego uprawnienia, obiekt GPO zasady nie zostanie pobrany na komputer użytkowników należących do tej grupy.
- Jeśli pojawią się problemy z zasadami ograniczeń oprogramowania, system należy załadować w trybie awaryjnym. Gdy tryb ten jest aktywny, tego typu zasady nie obowiązują. Dzięki temu można zalogować się jako administrator, a następnie zmodyfikować zasadę, uaktualnić ją za pomocą narzędzia `gpupdate` i ponownie uruchomić komputer.
- Jeśli zamierza się zmienić domyślny poziom zabezpieczeń na poziom *Niedozwolone*, w oknie obiektu *Wymuszanie* należy pozostawić aktywną opcję *Wszyscy użytkownicy oprócz administratorów lokalnych*, przynajmniej dopóki można diagnozować system. Ustawienie poziomu zabezpieczeń *Niedozwolone* spowoduje, że każdorazowo w celu umożliwienia uruchomienia aplikacji trzeba będzie definiować zasadę.
- W połączeniu z zasadami ograniczeń oprogramowania należy stosować listy kontroli dostępu powiązane z plikami i rejestrem. Użytkownicy będą próbowali obejść zasady, przenosząc pliki, nadpisując je lub umieszczając ich kopie w innych miejscach. Można uniemożliwić im wykonywanie takich działań.
- Przed wdrożeniem zasad należy je sprawdzić w środowisku testowym. Jeśli zasady będą użyte w domenie, należy je sprawdzić w domenie testowej.
- Nie należy zgadywać, jakie będą efekty określenia ograniczeń dla plików. Uniemożliwienie uruchomienia wybranych plików może doprowadzić do braku możliwości załadowania systemu lub jego niestabilności.
- W przypadku domeny należy filtrować zakres stosowania zasad ograniczeń oprogramowania, odbierając użytkownikom uprawnienia do odczytu i używania zasad powiązane z obiektem GPO domeny.

- Należy zarządzać obiektem *Wyznaczone typy plików*, który określa, jakie typy plików poza *.exe* i *.dll* będą uważane za pliki programów. Jeśli zastosuje się reguły z ustawionym poziomem zabezpieczeń *Niedozwolone* (uniemożliwia uruchomienie wszystkich aplikacji) i określony typ pliku nie zostanie zdefiniowany w obiekcie *Wyznaczone typy plików*, plik wykonywalny tego typu będzie można uaktywnić. Uzależnione są od tego reguły ścieżki.
- W przypadku autonomicznych serwerów w obiekcie *Zaufani wydawcy* zamiast domyślnej opcji *Użytkownicy końcowi* należy uaktywnić opcję *Administratorzy komputera lokalnego*. Gdy serwery znajdują się w domenie, należy zaznaczyć opcję *Administratorzy komputera lokalnego* lub *Administratorzy przedsiębiorstwa*.
- Należy zadbać o to, aby użytkownicy musieli się co jakiś czas wylogowywać z systemu i ponownie w nim logować. Gdy wdroży się nową zasadę ograniczeń oprogramowania lub zmodyfikuje istniejącą, użytkownik musi się wylogować i jeszcze raz zalogować, aby zmiany zaczęły dla niego obowiązywać.
- Jeśli użytkownicy są członkami lokalnej grupy administratorów komputerów, z których korzystają, obiekt *Wymuszanie* należy tak skonfigurować, aby zasady dotyczyły administratorów.
- Dla folderu załączników wiadomości pocztowych (są w nim tymczasowo umieszczane załączniki i mogą być z niego uruchomione) należy utworzyć regułę ścieżki. Jeśli dla reguły ustawi się poziom *Niedozwolone*, nie będzie można przypadkowo uaktywnić załącznika, dzięki czemu być może uniknie się kolejnego załącznika zawierającego wirus. Jeśli załącznikiem jest program niebudzący podejrzeń i wymagany przez odbiorcę wiadomości, musi go zapisać w innym folderu, z którego umożliwiono uruchamianie aplikacji.

Zabezpieczanie aplikacji COM, COM+ i DCOM za pomocą usługi Usługi składowe

Aplikacje COM (*Component Object Model*), COM+ i DCOM (*Distributed Component Object Model*) są zarządzane przy użyciu konsoli *Usługi składowe* pokazanej na rysunku 4.31. Zabezpieczeniami tych aplikacji można zarządzać w takim zakresie, na jaki pozwalają odpowiednie interfejsy przez nie oferowane. Przykładowo, aplikacja COM+ może definiować role dysponujące w jej obrębie specyficznymi przywilejami i uprawnieniami. Jeśli role utworzono w aplikacji, można nimi zarządzać za pomocą konsoli.



Rysunek 4.31. *Konsola Usługi składowe służy do zarządzania zabezpieczeniami aplikacji COM i COM+*

Zabezpieczanie aplikacji COM, COM+ i DCOM składa się z następujących czynności:

- definiowanie praw użytkownika, inspekcji i uprawnień zasobów, które na przykład określa się dla folderów i plików systemu plików NTFS;
- definiowanie właściwości systemowych używanych przez wszystkie aplikacje, którymi nie będzie się zarządzało indywidualnie;
- określenie właściwości dla każdej aplikacji, która będzie zarządzana indywidualnie;
- przypisanie użytkowników i grup do ról aplikacji COM+, które mogą nimi dysponować;
- zadbanie o to, aby tylko administratorzy mogli modyfikować ustawienia aplikacji i dodawać użytkowników do ról;
- ograniczenie liczby administratorów, którzy mogą modyfikować zabezpieczenia aplikacji COM+.

OSTRZEŻENIE: Nie wolno modyfikować właściwości istniejącej aplikacji COM+

Nie jest zalecane modyfikowanie ustawień istniejącej aplikacji, ponieważ może zawierać kod wymagający wartości domyślnych. Dokonanie zmian może spowodować, że aplikacja przestanie działać, będzie niestabilna lub mniej bezpieczna. Jeśli nie zrozumie się dokładnie zasad funkcjonowania aplikacji i nie wie, dlaczego zmiana ustawień może zwiększyć poziom zabezpieczeń, nie powinno się ich modyfikować. Domyślne ustawienia najlepiej modyfikować na etapie projektowania aplikacji.

Konfigurowanie zabezpieczeń aplikacji COM i COM+

Można skonfigurować właściwości powiązane z kilkoma następującymi kategoriami:

- poziom uwierzytelnienia wywołań,
- autoryzacja,
- poziom zabezpieczeń,
- personifikacja,
- identyfikacja,
- uprawnienia zezwalające na uruchamianie,
- uprawnienia zezwalające na dostęp.

Poziom uwierzytelnienia wywołań

Tożsamość jest właściwością, taką jak identyfikator użytkownika lub nazwa komputera. Uwierzytelnianie jest procesem, w ramach którego tożsamość potwierdza, że jest tym, za kogo się podaje. Możliwość wywoływania komponentów COM+ można ograniczyć do użytkowników przypisanych do określonej roli. W tym przypadku uwierzytelnianie będzie miało na celu stwierdzenie, czy użytkownik jest faktycznie tym, za kogo się podaje. Gdy tak będzie, w dalszej kolejności zostanie sprawdzone członkostwo użytkownika w grupach.

UWAGA: Źródło informacji

Można uzyskać więcej informacji na temat zarządzania aplikacjami COM+, korzystając z pakietu SDK (*Software Development Kit*). Można go pobrać z witryny MSDN (*http:// msdn.microsoft.com*).

Poziom uwierzytelniania można określić w konsoli *Usługi składowe* lub przy użyciu kodu zawierającego funkcje administracyjne pakietu SDK. Uwierzytelnienia mogą wymagać aplikacje serwera i klienta COM+. Można zdefiniować różny poziom uwierzytelniania, począwszy od jego braku, a skończywszy na szyfrowaniu każdego pakietu i wszystkich parametrów wywołania metody. Poniższa lista zaczyna się od poziomu, w przypadku którego nie zachodzi uwierzytelnianie, a kończy na najwyższym poziomie uwierzytelniania. Sposób uwierzytelniania jest negocjowany przez klienta i serwer. Zostaną użyte bezpieczniejsze ustawienia, którymi dysponuje jedna z dwóch stron. Kontrolowanie uwierzytelniania po stronie serwera może polegać na ustawieniu dla procesu najwyższego żądanego poziomu. Jeśli dla aplikacji nie określono poziomu uwierzytelniania, zostaną użyte ustawienia komputera (domyślnym poziomem jest poziom łączenia). Można wyróżnić następujące poziomy uwierzytelniania:

- ***Brak***. Proces uwierzytelniania nie jest realizowany.
- ***Łączenie***. Dane uwierzytelniające są sprawdzane tylko w trakcie nawiązywania połączenia.
- ***Wywołanie***. Dane uwierzytelniające są sprawdzane na początku każdego wywołania.
- ***Pakiet***. Dane uwierzytelniające są sprawdzane i ma miejsce weryfikacja mająca na celu stwierdzenie, czy odebrano wszystkie dane żądane w ramach wywołania.
- ***Integralność pakietów***. Dane uwierzytelniające są sprawdzane i ma miejsce weryfikacja mająca na celu stwierdzenie, czy żądane dane nie zostały zmodyfikowane podczas transferu.
- ***Prywatność pakietów***. Dane uwierzytelniające są sprawdzane i ma miejsce weryfikacja mająca na celu stwierdzenie, czy zaszyfrowano wszystkie informacje znajdujące się w pakiecie, łącznie z tożsamością i sygnaturą nadawcy.

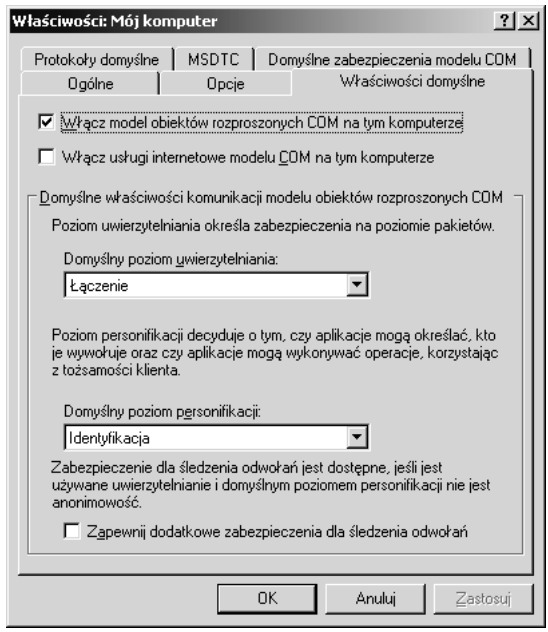
W celu ustalenia dla komputera poziomu uwierzytelniania należy wykonać następujące kroki:

1. Uruchomić narzędzie administracyjne *Usługi składowe*.
2. Prawym przyciskiem myszy kliknąć kontener *Komputery* i z menu wybrać pozycję *Właściwości*.
3. Uaktywnić zakładkę *Właściwości domyślne* pokazaną na rysunku 4.32.
4. Sprawdzić, czy na zakładce jest zaznaczona opcja *Włącz model obiektów rozproszonych COM na tym komputerze*.
5. W polu *Domyślny poziom uwierzytelniania* ustawić wartość.
6. Kliknąć przycisk *OK*.

Autoryzacja

Jeśli aplikacja COM+ jest zabezpieczana przy użyciu ról, należy uaktywnić przeprowadzanie autoryzacji. Zanim użytkownicy będą mogli wykonać w aplikacji jakąkolwiek operację, w trakcie uzyskiwania do niej dostępu zostanie sprawdzone ich członkostwo w rolach. W celu uaktywnienia przeprowadzania autoryzacji należy wykonać następujące kroki:

1. Uruchomić konsolę *Usługi składowe*.
2. Prawym przyciskiem myszy kliknąć aplikację COM+ i z menu wybrać pozycję *Właściwości*.



Rysunek 4.32. *Zakładka Właściwości domyślne pozwala na zastosowanie aplikacji posiadających role*

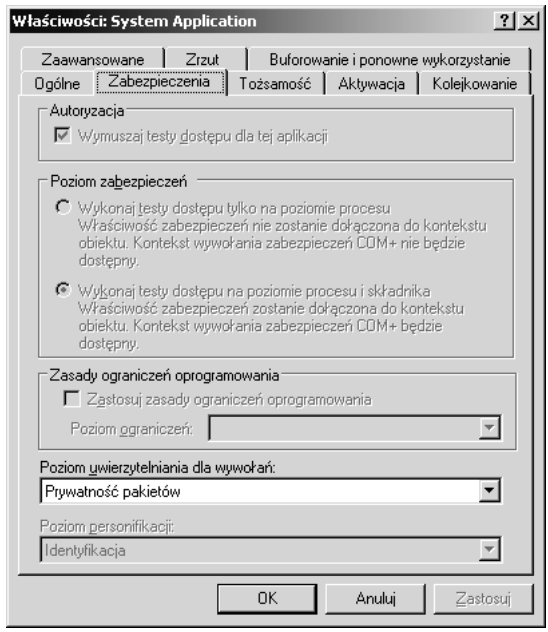
3. Uaktywnić zakładkę *Zabezpieczenia*.
4. W sekcji *Autoryzacja* zaznaczyć opcję *Wymuszaj testy dostępu dla tej aplikacji* (rysunek 4.33).
5. Kliknąć przycisk *OK*.

Poziom zabezpieczeń

Poziom zabezpieczeń określa, na jakim poziomie aplikacje COM+ dysponujące rolami będą sprawdzały dostęp. Kontrola dostępu może być realizowana na poziomie komponentu lub procesu. Role umożliwiają zdefiniowanie sprawdzania dostępu na poziomie komponentu. Role można przypisać komponentom, interfejsom i metodom aplikacji COM+. Sprawdzanie dostępu na poziomie procesu obowiązuje jedynie w obrębie aplikacji.

W celu ustawienia poziomu zabezpieczeń należy wykonać następujące kroki:

1. Uruchomić konsolę *Usługi składowe*.
2. Prawym przyciskiem myszy kliknąć aplikację i z menu wybrać pozycję *Właściwości*.



Rysunek 4.33. *Za pomocą zakładki Zabezpieczenia można określić poziom uwierzytelniania, poziom zabezpieczeń i poziom personifikacji*

3. Uaktywnić zakładkę *Zabezpieczenia*.
4. W sekcji *Poziom zabezpieczeń* (rysunek 4.33) zaznaczyć opcję *Wykonaj testy dostępu tylko na poziomie procesu* lub opcję *Wykonaj testy dostępu na poziomie procesu i składnika*.
5. Kliknąć przycisk *OK*.
6. Ponownie uruchomić aplikację, aby dokonane zmiany zostały uwzględnione.

Personifikacja i delegowanie

Gdy serwer realizuje wywołanie w imieniu klienta, korzystając z jego danych uwierzytelniających zamiast ze swoich, ma miejsce personifikacja. Zależnie od tego, co umożliwiono użytkownikowi, dostęp do zasobów może zostać rozszerzony lub zmniejszony. Przykładowo, może być wymagane, aby aplikacja serwera uzyskała dostęp do danych znajdujących się w bazie, a ponadto żeby były to dowolne dane, do których dostępem dysponuje klient.

Można wyróżnić następujące poziomy personifikacji:

- ***Anonim***. Z punktu widzenia serwera klient jest anonimowy. Serwer może personifikować klienta, ale w żetonie personifikacji nie ma żadnych informacji dotyczących klienta.
- ***Identyfikacja***. Domyślny poziom, w przypadku którego serwer może użyć tożsamości klienta i go personifikować. Używany na potrzeby ustalania poziomów kontroli dostępu.
- ***Personifikacja***. Domyślny poziom w przypadku aplikacji serwerowych COM+. Serwer może personifikować klienta, ale ma ograniczone możliwości. Serwer jest w stanie uzyskać dostęp do identycznych zasobów komputera, co klient. Jeśli serwer znajduje się na tym samym komputerze, co klient, będzie mógł uzyskiwać dostęp do zasobów sieciowych w imieniu klienta. W przeciwnym razie serwer może jedynie korzystać z zasobów zlokalizowanych na komputerze, na którym się znajduje.
- ***Delegowanie***. Serwer może personifikować klienta, niezależnie od tego, czy znajduje się na tym samym komputerze, co klient, czy nie. Dane uwierzytelniające klienta mogą zostać przekazane dowolnej liczbie komputerów.

Aby ustawić poziom personifikacji, należy wykonać następujące kroki:

1. Uruchomić konsolę *Usługi składowe*.
2. Prawym przyciskiem myszy kliknąć aplikację i z menu wybrać pozycję *Właściwości*.
3. Uaktywnić zakładkę *Zabezpieczenia*.
4. W polu *Poziom personifikacji* widocznym na rysunku 4.33 ustawić poziom personifikacji.
5. Kliknąć przycisk *OK*.
6. Ponownie uruchomić aplikację, aby dokonane zmiany zostały uwzględnione.

Delegowanie jest specjalną odmianą personifikacji stosowaną w sieci. Korzysta się z niej, gdy serwer i klient nie znajdują się na tym samym komputerze, a ponadto serwer używa danych uwierzytelniających klienta w celu uzyskania dostępu do zasobów innego komputera. Delegowanie jest kontrolowane przez usługę Active Directory. Aby dowiedzieć się, jak definiować delegowanie, należy zapoznać się z rozdziałem 8. Muszą zostać spełnione następujące dwa wymagania:

- tożsamość używana przez uruchomiony serwer (konto stosowane przez serwer do uaktywnienia swojej usługi) musi być zaufana w kwestii delegowania;
- aplikacja klienta musi zostać uaktywniona przy użyciu tożsamości, dla której nie zaznaczono opcji *Konto jest poufne i nie może być delegowane*.

Identyfikacja

Aplikacje COM i COM+ mogą działać jako usługi. Gdy tak jest, korzystają z kontekstu zabezpieczeń konta lub tożsamości *System lokalny*. Jeśli aplikacje nie są usługami, mogą personifikować tożsamość lub korzystać z uprawnień konta użytkownika, za pomocą którego zostały uruchomione.

Tożsamość aplikacji jest określana podczas jej instalacji i dotyczy wyłącznie aplikacji serwerowych. Tożsamość jest kontem użytkownika wykorzystywanym przez aplikację do uruchomienia i wykonywania wywołań dotyczących innych aplikacji i zasobów. W przypadku bibliotek tożsamość nie jest stosowana. Biblioteki COM+ używają tożsamości hosta. Zastosowanie konkretnego konta (konta *System lokalny* lub przydzielonego konta użytkownika) jest bezpieczniejsze od zezwolenia na użycie interaktywnej tożsamości. Interaktywność oznacza, że aplikacje COM+ są uruchamiane z uprawnieniami zalogowanego użytkownika. Jeśli na przykład jest zalogowany lokalny administrator, aplikacje COM+ mogłyby zostać uaktywnione z jego przywilejami, a także posłużyć do wykonania wywołań i uzyskania dostępu do zasobów, nawet w imieniu klientów. Jeśli nikt nie jest zalogowany, aplikacje nie mogą zostać uruchomione. Można wyróżnić następujące rodzaje tożsamości:

- ***Interaktywna***. Aktualnie zalogowany użytkownik.
- ***Usługa lokalna***. Konto z minimalnymi uprawnieniami pozwalającymi na uruchamianie lokalnie dostępnej usługi.
- Określone ważne konto użytkownika.

OSTRZEŻENIE: Przechowywanie hasła tożsamości używanej przez aplikację COM+

Aplikacja COM+ przechowuje hasła w tajnej bazie podsystemu LSA, co oznacza, że administrator może je pobrać. Należy użyć konta, które utworzono tylko na potrzeby aplikacji COM+, i uniemożliwić lokalne logowanie za jego pomocą.

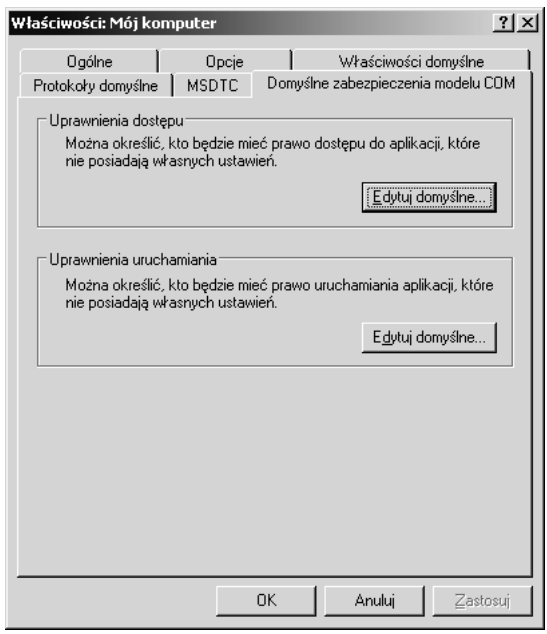
Uprawnienia zezwalające na uruchamianie

Uprawnienia uruchamiania identyfikują listę użytkowników, którym może być nadane lub odebrane uprawnienie zezwalające na uaktywnienie aplikacji COM. Gdy tego typu uprawnienia zdefiniuje się dla komputera, będą obowiązywały

wszystkie aplikacje, które nie posiadają własnych list uprawnień uruchamiania. Domyślnie na liście znajdują się grupa *Interaktywna* (uwzględnia wszystkich lokalnie zalogowanych użytkowników) i konto *SYSTEM*, a także grupa *Administratorzy*.

Aby zdefiniować uprawnienia uruchamiania, należy wykonać następujące kroki:

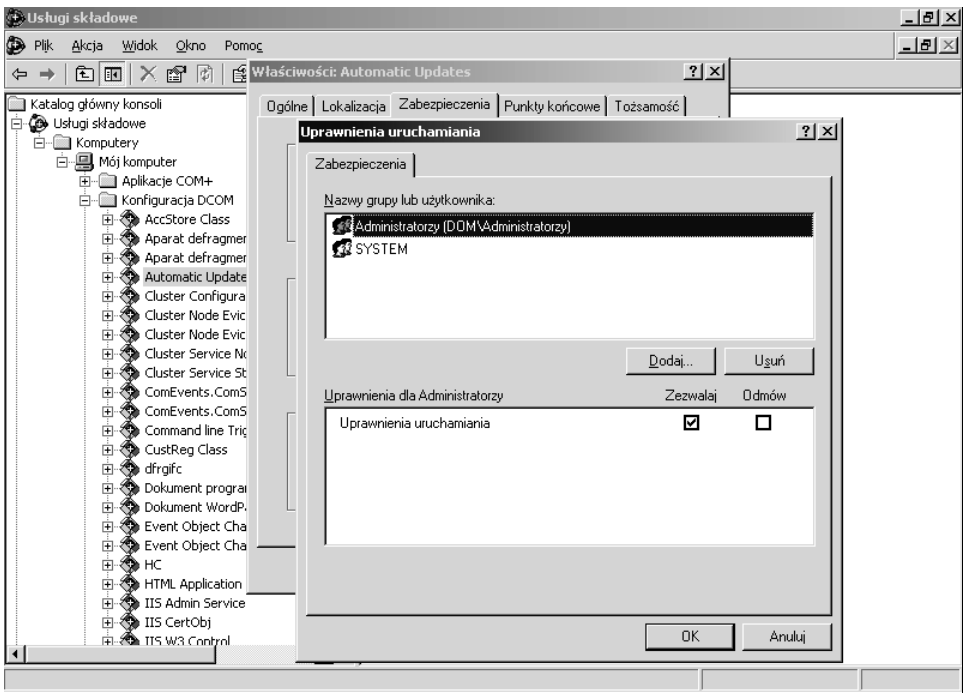
1. Uruchomić konsolę *Usługi składowe*.
2. Prawym przyciskiem myszy kliknąć komputer, dla którego zostaną określone uprawnienia obowiązujące w całym systemie, i z menu wybrać pozycję *Właściwości*.
3. Uaktywnić zakładkę *Domyślne zabezpieczenia modelu COM*.
4. Kliknąć przycisk *Edytuj domyślne* znajdujący się w sekcji *Uprawnienia uruchamiania* (rysunek 4.34).



Rysunek 4.34. *Zakładka Domyślne zabezpieczenia modelu COM umożliwia zdefiniowanie uprawnień uruchamiania*

5. Dodać grupy użytkowników i przypisać im uprawnienia uruchamiania, zaznaczając opcję *Zezwalaj* lub *Odmów*.

Uprawnienia uruchamiania można zdefiniować dla poszczególnych aplikacji. Po sprawdzeniu kilku aplikacji dojdzie się do wniosku, że najprościej będzie zastosować domyślne ustawienia. Jednak są wyjątki. Jeśli wyświetli się właściwości aplikacji *Automatic Updates* (*Aktualizacje automatyczne*) (rysunek 4.35), okaże się, że zmodyfikowano domyślną konfigurację uprawnień uruchamiania. Uprawnienia przypisano jedynie kontu *SYSTEM* i grupie *Administratorzy*. Domyślnie uprawnienia są nadawane grupie *Interaktywna* i kontu *SYSTEM*, a także grupie *Administratorzy*.



Rysunek 4.35. *Dla aplikacji Automatic Updates określono niestandardową konfigurację uprawnień uruchamiania*

Zdefiniowanie uprawnień uruchamiania jest dobrym sposobem ograniczenia możliwości korzystania z aplikacji. Uprawnienia można określić dla dowolnej aplikacji widocznej w oknie konsoli *Usługi składowe* i umożliwić jej uruchamianie tylko niektórym użytkownikom. Przykładowo, w przypadku programu *Media Player* domyślnie uprawnienia uruchamiania nadano kontom *Administrator*, *SYSTEM* i *Interaktywna*. Jeśli zamierza się ograniczyć możliwości uruchamiania (uprawnienia uruchamiania), używania (uprawnienia dostępu) i konfigurowania (uprawnienia konfiguracji) aplikacji, odpowiednie zmiany można wprowadzić w oknie konsoli.

OSTRZEŻENIE: Modyfikowanie ustawień

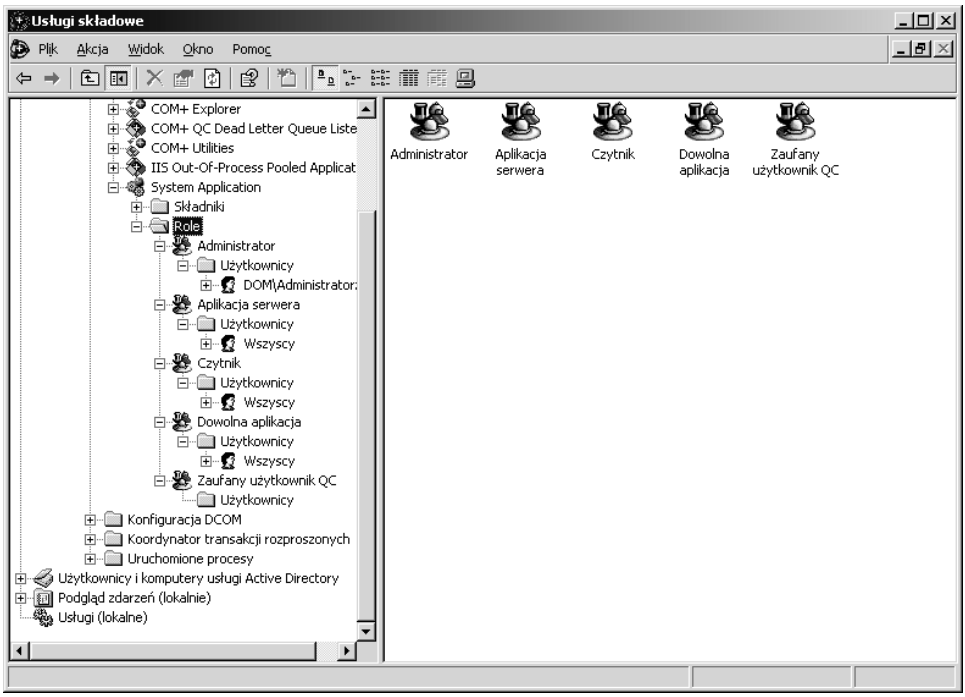
Zanim się zacznie modyfikować ustawienia, trzeba wiedzieć, jaki będzie efekt takiej operacji. Jeśli nie jest wiadome, na czym polega działanie aplikacji, nie należy zmieniać jej ustawień. Gdy taką wiedzą się dysponuje, można się zastanowić, w jakim zakresie można ograniczyć możliwość korzystania z aplikacji. Jeśli nie ma potrzeby tak dokładnego zarządzania programem *Media Player*, może będzie tak w przypadku aplikacji *NetMeeting*? Czy powinno być możliwe uruchamianie sesji tego programu na serwerze? Czy aplikację będzie można uaktywnić na stacji roboczej? Czy będzie mogła to zrobić każda osoba? W ramach rozbudowanej strategii stosowania zasad zabezpieczeń z łatwością można ograniczać aplikacje za pomocą konsoli *Usługi składowe*. Trzeba tylko zadbać o to, aby nie stało się to częścią strategii, która sprawi, że systemy będą bezużyteczne.

Ograniczanie przywilejów przez utworzenie aplikacji będącej biblioteką

Można wyróżnić dwa typy aplikacji COM+ — aplikacje i biblioteki. Biblioteki są obsługiwane przez inny proces. Oznacza to, że mogą korzystać z zabezpieczeń hosta, a nie zabezpieczeń własnej tożsamości (konta użytkownika). Biblioteki dysponują tylko takimi przywilejami, jakie przypisano ich hostowi. Choć domyślnie biblioteki mogą brać udział w uwierzytelnianiu, można je tak skonfigurować, aby proces ten nie był realizowany (nie jest to zalecane). Gdy aplikację COM+ świadomie zaprojektuje się jako bibliotekę, można ograniczyć jej możliwości. Biblioteka będzie mogła użyć tylko tych zasobów, do których dostępem dysponuje jej klient, czyli proces hosta. Klientami będą wywołania wykonywane poza obrębem aplikacji lub dostęp do zasobów, takich jak pliki, zależny od deskryptora zabezpieczeń. Jeśli tworzy się aplikację, która będzie realizowała istotne operacje, i zależy nam, aby mogły z niej korzystać tylko te osoby, które dysponują uprawnieniami do wykonywania takich operacji, należy zaprojektować bibliotekę.

Przypisywanie użytkowników do ról

Role identyfikują kategorie użytkowników i są definiowane przez projektanta aplikacji. Podobnie jak aplikacje zgodne z narzędziem *Menedżer autoryzacji* aplikacje COM+ mogą zawierać role określające, jaki użytkownik jakie operacje może wykonywać po uruchomieniu programu. Role wymuszają przestrzeganie zasady kontroli dostępu zdefiniowanej dla aplikacji i są w niej umieszczane przez projektantów. Administratorzy przypisują do ról aplikacji użytkowników i grupy systemu Windows. Przykładowe role aplikacji COM+ można przejrzeć w oknie konsoli *Usługi składowe*. W tym celu po uruchomieniu konsoli należy rozwinąć węzeł *Mój komputer/Aplikacje COM+/System Application/Role*. W dalszej kolejności należy rozwijać zawartość każdej roli i znajdującego się w niej kontenera *Użytkownicy*. Wyniki operacji pokazano na rysunku 4.36.



Rysunek 4.36. *Poniżej węzła System Application są widoczne zdefiniowane role, którym w wielu przypadkach przypisano grupy systemu Windows*

Każda rola zawiera opis objaśniający, co będzie mógł zrobić użytkownik, któremu się ją przypisze. W tabeli 4.4 wymieniono role znajdujące się w węźle *System Application* wraz z ich opisem i przypisanymi grupami użytkowników.

Tabela 4.4. *Role znajdujące się w węźle System Application*

Rola	Opis	Domyślni użytkownicy
Administrator	Umożliwia skonfigurowanie aplikacji COM+ znajdującej się w systemie.	Lokalni administratorzy
Dowolna aplikacja	Identyfikuje tożsamości, za pomocą których można uruchomić dowolną aplikację znajdującą się na lokalnym komputerze.	Wszyscy
Zaufany użytkownik QC	Rola dysponuje zaufaniem w zakresie przesyłania w imieniu innych użytkowników komunikatów dotyczących kolejkowanych komponentów.	Rola nie jest przypisana żadnemu użytkownikowi.
Czytnik	Rola pozwala sprawdzać konfigurację elementów i przeglądać informacje dotyczące wydajności uruchomionych aplikacji.	Wszyscy
Aplikacja serwera	Identyfikuje tożsamości, za pomocą których są uruchamiane aplikacje COM+ znajdujące się na lokalnym komputerze.	Wszyscy

Aplikacja korzystająca z zabezpieczeń opartych na rolach sprawdza członkostwo użytkownika każdorazowo, gdy zamierza on użyć dowolnego jej składnika. Jeśli użytkownik nie posiada roli, która upoważnia do uzyskania dostępu do zasobu lub wykonania wywołania, operacja nie powiedzie się. Z uwagą należy przypisywać użytkowników do ról, które odpowiadają rzeczywistym stanowiskom. Dokumentacja aplikacji powinna wyraźnie identyfikować znaczenie każdej roli, a także prawa i uprawnienia, jakimi dysponuje w obrębie aplikacji. Administratorzy muszą wiedzieć, jakie obowiązki służbowe użytkowników odpowiadają zdefiniowanej roli. Gdy ten warunek nie zostanie spełniony, może dojść do tego, że użytkownik nie będzie w stanie wykonać zleconych mu zadań lub jakaś nieupoważniona osoba uzyska dostęp, którego posiadać nie powinna.

CZY ZAMIESZANIE Z ROLAMI APLIKACJI MOŻE SPOWODOWAĆ ODMOWĘ USŁUGI?

Donna Advertius pracująca w niewielkiej firmie konsultingowej Advanced Services Corporation, zlokalizowanej w środkowo-zachodniej części Stanów Zjednoczonych, otrzymała polecenie zmodyfikowania systemu PBX. System został właśnie uaktualniony do systemu Windows Server 2003 i korzysta z serwera Microsoft SQL Server, na którym znajduje się baza danych użytkowników, właściwości komunikatów, reguł i ograniczeń. Godną uwagi zaletą systemu PBX jest możliwość rejestrowania odebranych połączeń i przesyłania ich do serwera Exchange Server, dzięki czemu posiadacze skrzynek pocztowych mogą na swoich komputerach PC odsłuchiwać wiadomości głosowe. Firma stwierdziła, że ta funkcja będzie szczególnie przydatna dla podróżujących konsultantów, ponieważ sprawdzając skrzynkę wiadomości pocztowych, jednocześnie mogliby odsłuchać otrzymane wiadomości głosowe. Ponadto funkcja zaoferowałaby wszystkim użytkownikom bardziej elastyczny dostęp do wiadomości. Kolejną zaletą byłoby to, że bez wprowadzania numeru telefonu można by było od razu oddzwaniać.

Choć dokumentacja była skromna, Donna zapoznała się z systemami PBX i bardzo dobrze obsługiwała system Windows Server 2003, a także serwery Exchange i SQL Server. Wyglądało na to, że musi jedynie skonfigurować narzędzie *SQL Mail* i dokonać kilku innych drobnych modyfikacji. Choć konfiguracja narzędzia *SQL Mail* nie jest złożona, wymaga wykonania kilku kroków, z których jeden polega na utworzeniu konta dla usługi i zdefiniowaniu profilu dla konta. Korzystając z tego konta, narzędzie *SQL Mail* będzie wysyłało wiadomości do dowolnego konta użytkownika. Po wprowadzeniu kilku niewielkich modyfikacji narzędzie *SQL Mail* zadziałało.

W dokumentacji systemu PBX zalecano, aby używane przez niego konto usługi było tym samym, które jest wykorzystywane przez narzędzie *SQL Mail*. Czy Czytelnik już wie, o czym mowa? System PBX miałby rejestrować wiadomość i za pomocą narzędzia *SQL Mail* umieszczać ją w skrzynce pocztowej użytkownika. Donna z łatwością zmieniła konto i usługa systemu PBX od razu zaczęła wykonywać taką operację. Donna z zadowoleniem spojrzała na zegarek, ponieważ stwierdziła, że szybko przetestuje system i około północy będzie już w domu.

W ramach testu systemu postanowiła wykręcić własny numer, używając telefonu znajdującego się w serwerowni, a następnie odsłuchać wiadomość na swoim komputerze. Nie była w stanie nawiązać połączenia. Nie było sygnału wybierania. Zupełnie nic. Donna sprawdziła co najmniej tuzin numerów telefonów. Cały czas nie było sygnału. Sprawdziła wszystkie numery, jakimi dysponowała. Czy wystąpił jakiś nowy problem z systemem Windows Server 2003? Czy w dokumentacji nie wymieniono jakichś kroków? Czy Donna zrobiła coś niepoprawnie?

W pewnym momencie pomyślała, czy przypadkiem role aplikacji COM+ nie są przyczyną problemów? Uruchomiła konsolę *Usługi składowe* zupełnie pewna, że znajdzie w niej aplikację systemu PBX. Dostępna była rola *Administrator*, którą przydzielono tylko kontu *SYSTEM*. Po sprawdzeniu uprawnień uruchamiania stwierdziła, że je również przypisano wyłącznie kontu *SYSTEM*. Ze względu na to, że w początkowej konfiguracji usługa systemu PBX korzystała z konta *System lokalny*, działał on bez zarzutów. Gdy Donna zmieniła konto, system PBX utracił uprawnienia do własnych komponentów. Oznaczało to niedostępność usług telefonicznych. Aby można było z nich ponownie korzystać, trzeba było jedynie zmodyfikować przypisanie roli *Administrator* i nadać uprawnienia uruchamiania nowemu kontu usługi.

Nawet gdy nie zamierza się konfigurować zabezpieczeń aplikacji COM+ lub nie dysponuje takimi, które mają wbudowane role pozwalające na zarządzanie, powinno się administrować rolami znajdującymi się w węźle *System Application*. Role te określają, kto może instalować aplikacje COM+, a także kto może zarządzać nimi i ich środowiskiem. Domyślnie członkiem ról jest lokalna grupa *Administratorzy*. Choć tylko członkowie grupy *Administratorzy* mogą zarządzać zabezpieczeniami aplikacji COM+, można jeszcze bardziej to ograniczyć. W tym celu należy wykonać następujące kroki:

1. Uruchomić konsolę *Usługi składowe* (z menu *Start* należy wybrać pozycję *Wszystkie programy/Narzędzia administracyjne/Usługi składowe*).
2. Rozwinąć węzeł *System Application*, a następnie *Role*.
3. Rozwinąć węzeł roli.
4. Prawym przyciskiem myszy kliknąć kontener *Użytkownicy* znajdujący się poniżej roli, a następnie z menu *Nowy* wybrać pozycję *Użytkownik*.
5. W oknie *Wybieranie: Użytkownicy, Komputery lub Grupy* wprowadzić nazwę użytkownika lub kliknąć przycisk *Zaawansowane*, a następnie przycisk *Znajdź teraz*, aby z listy użytkowników i grup lokalnego komputera wybrać użytkownika bądź grupę.
6. Ponownie uruchomić komputer, aby dokonane zmiany zostały uwzględnione.

Definiowanie zasad ograniczeń oprogramowania dla aplikacji COM+

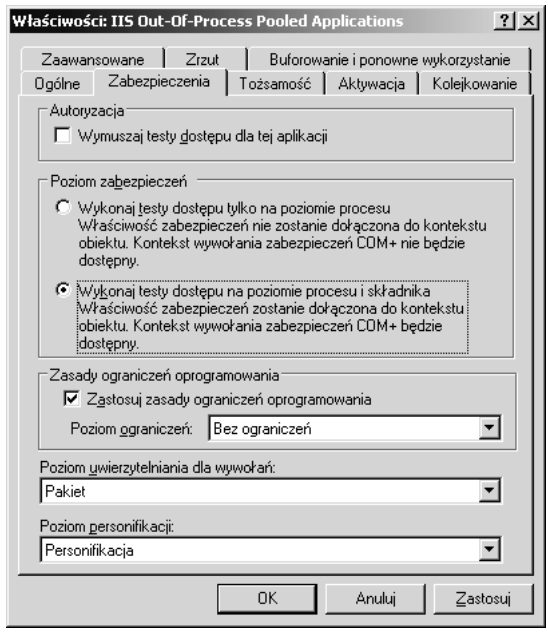
Zasada ograniczeń oprogramowania może być zdefiniowana bezpośrednio w oknie właściwości aplikacji COM+ znajdującej się na serwerze z systemem Windows Server 2003. Domyślnie dla wszystkich aplikacji serwerowych jest ustawiany identyczny systemowy poziom zabezpieczeń zasady ograniczeń oprogramowania. Wynika to stąd, że wszystkie są obsługiwane przez ten sam program *dllhost.exe*. Jeśli zamierza się zmodyfikować zasadę ograniczeń oprogramowania dla określonych aplikacji COM+, można to zrobić bezpośrednio w oknie ich właściwości. Zasady ograniczeń oprogramowania zdefiniowane w tym oknie mają pierwszeństwo przed zasadami obowiązującymi w całym systemie.

W celu zdefiniowania dla aplikacji COM+ zasad ograniczeń oprogramowania należy wykonać następujące kroki:

1. Z menu *Narzędzia administracyjne* wybrać pozycję *Usługi składowe*.
2. Prawym przyciskiem myszy kliknąć aplikację COM+, którą zamierza się zarządzać i wybrać *Właściwości*.
3. Uaktywnić zakładkę *Zabezpieczenia*.
4. W sekcji *Zasady ograniczeń oprogramowania* zaznaczyć opcję *Zastosuj zasady ograniczeń oprogramowania*, aby umożliwić ustawienie poziomu zabezpieczeń (rysunek 4.37). Jeśli opcja jest wyłączona, będą obowiązywały systemowe zasady ograniczeń oprogramowania.
5. Jako poziom zabezpieczeń ustawić wartość *Niedozwolone* (aplikacja będzie mogła ładować zaufane i pozbawione zaufania składniki, lecz nie będzie mogła skorzystać z pełnych przywilejów użytkownika) lub *Bez ograniczeń* (aplikacja dysponuje nieograniczonym dostępem do przywilejów użytkownika; w obrębie aplikacji będzie można używać tylko tych składników, dla których ustawiono poziom *Bez ograniczeń*).

Podsumowanie

Choć dostępnych jest wiele metod, które można zastosować do ograniczenia możliwości uruchamiania aplikacji, to aby operacja była precyzyjnie wykonana, niezbędne jest zastosowanie w aplikacji zabezpieczeń mających postać ról. Aby role były skuteczne i łatwe w zarządzaniu, powinny odwzorowywać rzeczywiste stanowiska zajmowane przez użytkowników.



Rysunek 4.37. *Zasady ograniczeń oprogramowania mogą być zdefiniowane dla aplikacji COM+ w jej oknie właściwości*

Jeśli nawet zdefiniuje się zaawansowane zabezpieczenia aplikacji, warto pamiętać o tym, że pierwszą linią obrony mogą być listy ACL plików, folderów i kluczy rejestru. Listy kontroli dostępu ACL całkowicie uniemożliwiają uruchomienie przez kogoś aplikacji. Jeśli do tego się dąży, to mimo że dysponuje się bardziej zaawansowanymi narzędziami konfigurującymi zabezpieczenia, warto dodatkowo zdefiniować listy ACL plików. W kolejnym rozdziale omówiono listy ACL plików, folderów i kluczy rejestru.