

Rozdział 9: Wdrażanie zasad zabezpieczeń w systemie Windows 2000

Spis treści

Przegląd zagadnień	1
Zabezpieczanie pulpitów i usług przy wykorzystaniu zasad zabezpieczeń	2
Laboratorium A: Konfigurowanie zabezpieczeń w systemie Windows 2000	15
Inspekcja dostępu do zasobów systemowych	23
Laboratorium B: Konfigurowanie inspekcji	32
Podsumowanie	41



Zastrzega się prawo wprowadzania zmian do treści niniejszego dokumentu bez uprzedniego powiadomienia. Wszelkie nazwy firm, nazwiska i imiona osób oraz inne dane wykorzystywane w przykładach są fikcyjne, o ile nie zaznaczono, że jest inaczej. Odpowiedzialność za przestrzeganie wszelkich praw autorskich ponosi użytkownik. Niniejszego dokumentu ani jego części nie wolno powielać w żadnej formie, ani przekazywać za pomocą jakichkolwiek nośników elektronicznych lub mechanicznych, z wyjątkiem przypadków, gdy uzyskano na to pisemną zgodę firmy Microsoft Corporation. Jeżeli użytkownik ma dostęp do tego dokumentu wyłącznie w formie elektronicznej, zezwala się na wydrukowanie jednego egzemplarza tego dokumentu.

Firma Microsoft może mieć patenty lub rozpoczęte postępowania patentowe, znaki towarowe, prawa autorskie lub inne prawa związane z własnością intelektualną, które odnoszą się do treści zawartej w tym dokumencie. Otrzymanie tego dokumentu nie oznacza udzielenia licencji na patenty, znaki towarowe, prawa autorskie lub inne prawa związane z własnością intelektualną, z wyjątkiem wyraźnie określonych przypadków zawartych w pisemnych umowach licencyjnych firmy Microsoft.

© 2000 Microsoft Corporation. Wszelkie prawa zastrzeżone.

Microsoft, Active Desktop, Active Directory, ActiveX, BackOffice, DirectX, FrontPage, JScript, MS-DOS, NetMeeting, PowerPoint, Visual Basic, Visual Studio, Windows, Windows Media, and Windows NT są zastrzeżonymi znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Microsoft Corporation zarejestrowanymi w USA i/lub w innych krajach.

Wszelkie inne nazwy firm i produktów wymienione w niniejszym dokumencie mogą być znakami towarowymi zarejestrowanymi przez ich właścicieli.

Project Lead: Rick Selby

Instructional Designers: Kelly Bowen, Victoria Fodale (ComputerPREP),
H. James Toland III (ComputerPREP), Kathryn Yusi (Independent Contractor),
Barbara Pelletier (S&T Onsite)

Lead Program Manager: Andy Ruth (Infotec Commercial Systems)

Program Manager: Chris Gehrig (Infotec Commercial Systems),
Joern Wettern (Wettern Network Solutions)

Graphic Artist: Kimberly Jackson (Independent Contractor)

Editing Manager: Lynette Skinner

Editor: Kelly Baker (The Write Stuff)

Copy Editor: Kathy Toney (S&T Consulting)

Online Program Manager: Debbi Conger

Online Publications Manager: Arlo Emerson (Aditi)

Online Support: David Myka (S&T Consulting)

Multimedia Development: Kelly Renner (Entex)

Courseware Test Engineers: Jeff Clark, H. James Toland III (ComputerPREP)

Testing Developer: Greg Stemp (S&T OnSite)

Compact Disc Testing: Data Dimensions, Inc.

Courseware Testing: Data Dimensions, Inc.

Production Support: Carolyn Emory (S&T Consulting)

Manufacturing Manager: Rick Terek (S&T OnSite)

Manufacturing Support: Laura King (S&T OnSite)

Lead Product Manager, Development Services: Bo Galford

Lead Product Manager: Gerry Lang

Group Product Manager: Robert Stewart

Simulation and interactive exercises were built with Macromedia Authorware

Opracowanie wersji polskiej: DC Edukacja Sp. z o.o. Sopot

Współpraca: P.S.I. Sp. z o.o. Kielce

Zespół tłumaczy: Przemysław Dąbkowski, Sylwester Nowicki, Marcin Sworzyński

Konsultacja: Waldemar Pierścioneek, Witold Stajura, Piotr Zejer

Uwagi dla wykładowcy

Prezentacja:
60 minut

W tym rozdziale przedstawiono wiadomości i działania niezbędne do wdrażania założeń bezpieczeństwa w środowisku systemu Microsoft® Windows® 2000, przy wykorzystaniu zasad zabezpieczeń i inspekcji zdarzeń.

Laboratoria:
60 minut

Po zrealizowaniu tego rozdziału słuchacz będzie potrafił:

- Zabezpieczyć pulpity i usługi, przy wykorzystaniu zasad zabezpieczeń.
- Monitorować dostęp do zasobów systemowych.

Materiały i sposób przygotowania

W sekcji tej opisano sposób przygotowania wykładowcy oraz materiały niezbędne do właściwej prezentacji rozdziału.

Wymagane materiały

Do przedstawienia tego rozdziału wykładowcy potrzebne będą następujące materiały:

- Plik Microsoft PowerPoint® 2152B_09.ppt.

Przygotowanie

Aby przygotować się do przedstawienia tego rozdziału należy:

- Przeczytać wszystkie materiały związane z tym rozdziałem.
- Wykonać ćwiczenia.

Strategia przedstawiania rozdziału

Wskazówki dotyczące prezentacji rozdziału:

- Zabezpieczanie pulpitów i usług przy wykorzystaniu zasad zabezpieczeń

W tej sekcji zawarto informacje dotyczące procedur wdrażania zasad zabezpieczeń. Należy wyjaśnić, że czynniki mające wpływ na konfigurację i rozpowszechnianie zasad zabezpieczeń zależą od rozmiaru i potrzeb organizacji. Przedstawić narzędzia używane przy konfiguracji zasad zabezpieczeń, rozpoczynając od opisu dwóch podstawowych metod ich wdrażania. Wyjaśnić, w jaki sposób tworzyć i wykorzystywać szablony, jak analizować konfigurację zabezpieczeń oraz w jaki sposób wykorzystywać narzędzie Secedit.

- Inspekcja dostępu do zasobów systemowych

W tej sekcji zawarto informacje dotyczące procedur wdrażania zasad inspekcji. Należy wyjaśnić przyczyny stosowania inspekcji. Przedstawić zdarzenia, które w systemie Windows 2000 mogą być monitorowane oraz na co może wskazywać wystąpienie zdarzenia. Wyjaśnić, jak zaplanować zasady inspekcji oraz jak je zastosować. Na zakończenie, należy pokazać zastosowanie zasad inspekcji dla pliku.

Informacje uzupełniające

W sekcji tej opisane są wymagania dotyczące instalacji laboratorium dla tego rozdziału oraz zmiany w konfiguracji, które zachodzą na komputerach słuchaczy w trakcie realizacji laboratorium. Informacje te będą pomocne w powielaniu lub dostosowywaniu materiałów szkoleniowych MOC (Microsoft Official Curriculum).

Ważne Aby możliwe było wykonanie laboratorium, zawartego w tym rozdziale, konieczne jest odpowiednie skonfigurowanie pracowni, zgodnie z uwagami znajdującymi się w sekcji Informacje uzupełniające, zamieszczonej w rozdziale Przygotowanie pracowni do kursu 2244A, *Wdrażanie systemów operacyjnych Microsoft Windows 2000 Professional i Microsoft Windows 2000 Server*.

Przygotowanie laboratorium

Aby przygotować komputery słuchaczy do laboratorium w tym rozdziale, należy ukończyć rozdział 1, „Instalacja lub uaktualnianie do Windows 2000” kursu 2244A, *Wdrażanie systemów operacyjnych Microsoft Windows 2000 Professional i Microsoft Windows 2000 Server*. Każdy z komputerów słuchaczy powinien być serwerem członkowskim w domenie nwtraders.msft.

Rezultaty laboratorium

Wykonanie ćwiczeń z tego rozdziału spowoduje następujące zmiany w konfiguracji komputerów słuchaczy:

- Utworzenie lokalnego szablonu zabezpieczeń *Server Security Template* (gdzie *Server* jest nazwą komputera słuchacza).
- Skonfigurowanie i włączenie inspekcji na komputerze każdego słuchacza.

Przegląd zagadnień

Cel slajdu

Przedstawienie tematów i celów rozdziału.

Wprowadzenie

W tym rozdziale przedstawiono tworzenie i konfigurację zasad zabezpieczeń na komputerze pracującym w systemie Windows 2000.

- Zabezpieczanie pulpitów i usług przy wykorzystaniu zasad zabezpieczeń
- Inspekcja dostępu do zasobów systemowych

Utrata informacji może negatywnie wpłynąć na działalność organizacji. Solidne założenia bezpieczeństwa są w przedsiębiorstwie podstawowym elementem ochrony komputerów użytkowników oraz całej sieci. System Microsoft® Windows® 2000 zapewnia zasady bezpieczeństwa oraz narzędzia służące do ich monitorowania, zarówno w stosunku do jednego komputera jak i całego przedsiębiorstwa. System Windows 2000 zapewnia również możliwość inspekcji, pozwalającej na określenie sposobu, w jaki zasoby są wykorzystywane.

Po zrealizowaniu tego rozdziału słuchacz będzie potrafił:

- Zabezpieczać pulpity i usługi przy wykorzystaniu zasad bezpieczeństwa.
- Prowadzić inspekcję dostępu do zasobów.

◆ Zabezpieczanie pulpitów i usług przy wykorzystaniu zasad zabezpieczeń

Cel slajdu

Wprowadzenie do zagadnień związanych z zabezpieczaniem pulpitów i usług.

Wprowadzenie

Zasady zabezpieczeń określają wymagania organizacji dotyczące właściwego wykorzystania komputera oraz procedury zabezpieczania sieci, związane ze zdarzeniami zagrażającymi jej bezpieczeństwu.

- Wdrażanie zasad zabezpieczeń
- Modyfikowanie zabezpieczeń
- Predefiniowane szablony zabezpieczeń
- Tworzenie własnego szablonu zabezpieczeń
- Analiza zabezpieczeń
- Konfiguracja i analiza zabezpieczeń z poziomu wiersza poleceń

Zasady zabezpieczeń są wykorzystywane do wymuszenia odpowiedniego poziomu bezpieczeństwa w sieci korporacyjnej. Określają one wymagania organizacji, dotyczące właściwego wykorzystania komputera oraz procedury zabezpieczania sieci, związane ze zdarzeniami zagrażającymi jej bezpieczeństwu. Dlatego też, niezmiennie istotne jest zabezpieczenie przez administratora pulpitów i usług na stacjach roboczych. Poprzez zastosowanie zasad zabezpieczeń można zapobiec uszkodzeniu komputera przez użytkownika oraz zabezpieczyć szczególnie wrażliwe obszary sieci komputerowej. Najbardziej efektywnym sposobem osiągnięcia tego celu jest wykorzystanie *szablonów zabezpieczeń*. Szablon zabezpieczeń jest plikiem tekstowym, zawierającym ustawienia zabezpieczeń, które można użyć do skonfigurowania komputera. W systemie Windows 2000 zawarte są również narzędzia konfiguracji zabezpieczeń, pomagające analizować i konfigurować zabezpieczenia dla komputerów i użytkowników.

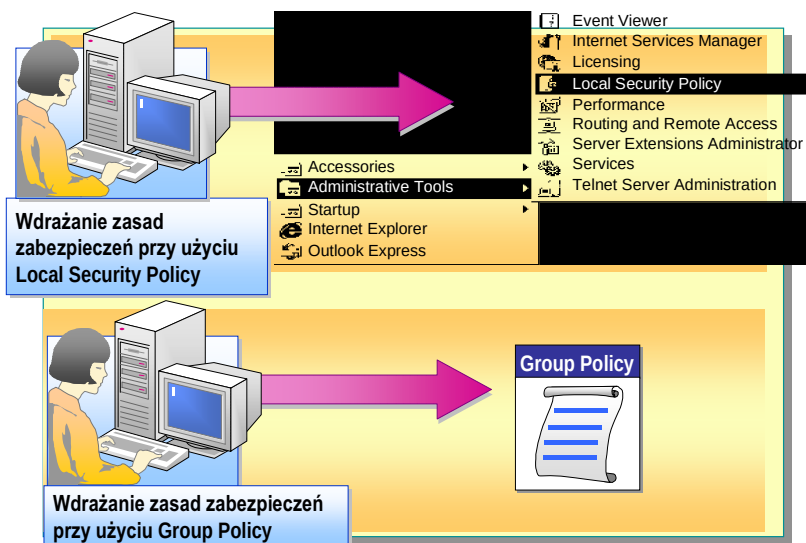
Wdrażanie zasad zabezpieczeń

Cel slajdu

Prezentacja dwóch sposobów wdrażania zasad zabezpieczeń.

Wprowadzenie

Zasady zabezpieczeń mogą być wdrażane na poziomie komputera, lokalizacji, domeny lub jednostki organizacyjnej OU, przy wykorzystaniu Group Policy.



Wdrażanie zasad zabezpieczeń można przeprowadzić na dwa różne sposoby: przez zasady zabezpieczeń lokalnych, na pojedynczym komputerze lub przez Group Policy na poziomie domeny, dla wielu komputerów. Wykorzystywana metoda zależy do rozmiaru organizacji i wymaganego poziomu bezpieczeństwa. W mniejszych organizacjach lub w tych, w których nie używa się usługi Active Directory™, można skonfigurować zasady zabezpieczeń ręcznie, w zależności od indywidualnych wymagań. Jeśli jednak organizacja jest duża lub wymagany jest wysoki poziom bezpieczeństwa, należy rozważyć wykorzystanie Group Policy, w celu rozpowszechnienia zasad zabezpieczeń.

Wyjaśnij, że ustawianie zasad zabezpieczeń zostanie przedstawione w dalszej części rozdziału.

Uwaga Ustawienia Group Policy określają składniki środowiska użytkownika, które są zarządzane przez administratora. Ustawienia Group Policy są zawarte w obiektach GPO (Group Policy Object) i są powiązane z obiektami usługi Active Directory. Więcej informacji na temat Group Policy i Active Directory znajduje się w programie kursu 2154A *Implementing and Administering Microsoft Windows 2000 Directory Services*.

Wdrażanie zabezpieczeń na komputerze lokalnym

Wdrażanie zabezpieczeń na komputerze lokalnym, który nie należy do domeny, jest możliwe przez konfigurację zasad zabezpieczeń lokalnych. Można to zrobić korzystając z programu Local Security Policy, z menu **Administrative Tools**.

Aby skonfigurować zasady zabezpieczeń lokalnych na komputerze pracującym w systemie Windows 2000, należy:

1. Uruchomić, z menu **Administrative Tools**, program Local Security Policy.
2. W drzewie konsoli rozwinąć kontener, odpowiadający zakresowi ustawianych zabezpieczeń, na przykład, **Account Policy**, a następnie **Password Policy**, w celu wyświetlenia ustawień dostępnych dla haseł.
3. Zaznaczyć odpowiedni element, aby w panelu szczegółów wyświetlić zasady zabezpieczeń.
4. W oknie szczegółów wybrać zasadę, aby skonfigurować ustawienia. Każda z zasad posiada unikalne, możliwe do konfiguracji opcje. Wprowadzić wymagane ustawienia konfiguracyjne.
5. Wybrać przycisk **OK**, aby zapisać nowe ustawienia.

Wdrażanie zabezpieczeń na wielu komputerach

Zagadnienie kluczowe Ustawienia lokalnych zasad zabezpieczeń są nadpisywane przez ustawienia skonfigurowane na poziomie lokalizacji, domeny lub OU.

Administratorzy sieci, w której wykorzystywana jest usługa Active Directory, mogą znacznie zaoszczędzić czas, wykorzystując Group Policy do dystrybucji zasad zabezpieczeń. Istnieje możliwość edycji ustawień zabezpieczeń, umieszczonych w obiektach GPO, dla dowolnej lokalizacji (site), domeny lub jednostki organizacyjnej OU. Podczas edycji obiektu GPO, należy rozwinąć kontener **Computer Configuration** lub **User Configuration**, następnie **Windows Settings** i odszukać wymagane opcje zasad zabezpieczeń.

Ważne Ustawienia Group Policy są stosowane w następującej kolejności: na początku ustawienia lokalne, następnie ustawienia dla lokalizacji i domeny, a na końcu ustawienia dla jednostki organizacyjnej OU.

Modyfikacja zasad zabezpieczeń

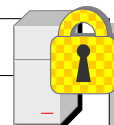
Cel slajdu

Prezentacja możliwych do skonfigurowania zabezpieczeń.

Wprowadzenie

Ustawienia zabezpieczeń można modyfikować, w celu ustalenia i wymuszenia bezpieczeństwa w sieci.

Account policies	Konfiguracja zabezpieczeń haseł i kont
Local policies	Konfiguracja inspekcji, praw użytkownika i opcji zabezpieczeń
Public key policies	Konfiguracja agentów odzyskiwania zaszyfrowanych danych, domeny głównej, zaufanych centrów obsługi certyfikatów, itp.
IPSec policies	Konfiguracja zabezpieczeń protokołu IP
Event log	Konfiguracja dzienników aplikacji, systemowego i zabezpieczeń
Restricted groups	Konfiguracja członkostwa w grupach, istotnych ze względu na bezpieczeństwo systemu
System services	Konfiguracja zabezpieczeń i ustawień początkowych dla usług pracujących na komputerze
Registry	Konfiguracja zabezpieczeń kluczy rejestru
File system	Konfiguracja zabezpieczeń obiektów systemu plików



Zagadnienie kluczowe

W programie Local Security Policy dostępne są tylko zasady zabezpieczeń kont, lokalne, kluczy publicznych i IPsec.

Ustawienia hasła, blokowania konta i protokołu Kerberos V5 są dostępne tylko na poziomie domeny.

Poniżej opisano ustawienia zasad zabezpieczeń, które można konfigurować dla komputera, przy wykorzystaniu programu Local Security Policy lub rozszerzenia Security Settings w Group Policy:

- *Account policies.* Zabezpieczenia konta umożliwiają konfigurację zasad dotyczących haseł, blokowania konta oraz protokołu Kerberos w wersji 5 dla domeny. Protokół Kerberos V5 jest podstawowym protokołem stosowanym przy bezpiecznym uwierzytelnianiu w domenie.
- *Local policies.* Zabezpieczenia lokalne z definicji odnoszą się tylko do komputera lokalnego. Zawierają zasady prowadzenia inspekcji, przypisywania praw użytkownikom i różne inne opcje zabezpieczeń, możliwe do skonfigurowania lokalnie.

Ważne Nie należy mylić zasad zabezpieczeń lokalnych z lokalnym ustawianiem zasad. Jak wszystkie pozostałe, także i zasady lokalne można konfigurować przy użyciu Local Security Policy jak i Group Policy.

- *Public key policies.* Zabezpieczenia kluczy publicznych pozwalają na konfigurację agentów odzyskiwania zaszyfrowanych danych oraz zaufanych centrów obsługi certyfikatów. Certyfikaty są programową usługą obsługi uwierzytelnienia, wykorzystywaną przy dostępie do poczty elektronicznej, w sieci Web i uwierzytelnianiu z wykorzystaniem kart typu Smart Card. Zasady kluczy publicznych są ustawiane tylko w kontenerze **User Configuration**.
- *IP Security policy.* Zabezpieczenia protokołu IP (Internet Protocol) pozwalają na konfigurację protokołu IPSec (Internet Protocol Security). Protokół IPSec jest przemysłowym standardem szyfrowania danych podczas transmisji za pomocą protokołu TCP/IP (Transmission Control Protocol/Internet Protocol) i zabezpieczania połączeń w Internecie oraz poprzez Internet, w ramach sieci VPN (Virtual Private Networks).

Wymienione niżej zasady zabezpieczeń mogą być skonfigurowane tylko przy wykorzystaniu rozszerzenia Security Settings w Group Policy:

- *Event log.* Konfiguracja dzienników zdarzeń pozwala na określenie rozmiaru, sposobu dostępu oraz parametrów przechowywania dzienników aplikacji, systemu i zabezpieczeń.
- *Restricted groups.* Zarządzanie członkostwem w grupach wbudowanych, posiadających predefiniowany zestaw praw, takich jak Administrators i Power Users czy grup domenowych, takich jak Domain Admins. Istnieje możliwość dodawania do zestawu grup o ograniczonym członkostwie innych grup, wraz z wszelkimi informacjami o ich członkach. Pozwala to na zarządzanie i śledzenie tych grup poprzez założenia bezpieczeństwa.

Poza członkostwem w grupie można również monitorować i konfigurować wsteczne członkostwo każdej grupy. W kolumnie Member Of wyświetlane są grupy, do których należy bieżąca grupa.

- *System services.* Zasady bezpieczeństwa dla usług systemowych pozwalają na konfigurację zabezpieczeń i ustawień startowych dla usług zainstalowanych na komputerze. Zawierają one także ustawienia ważne dla systemu, takie jak ustawienia usług sieciowych, usług plików i wydruku, usług telefonicznych i faksowych oraz usług internetowych i intranetowych. Ogólne ustawienia określają sposób uruchomienia usługi (automatyczny, ręczny, wyłączona) oraz jej zabezpieczenia.
- *Registry.* Zasady dla rejestru pozwalają na konfigurację zabezpieczeń kluczy rejestru. Rejestr jest centralną bazą danych, zawierającą informacje niezbędne do konfiguracji systemu Windows 2000 dla użytkowników, aplikacji oraz urządzeń.
- *File System.* Zasady bezpieczeństwa dla systemu plików pozwalają na konfigurację zabezpieczeń konkretnego pliku.

Predefiniowane szablony zabezpieczeń

Cel slajdu

Prezentacja interfejsu do organizacji i edycji szablonów zabezpieczeń.

Wprowadzenie

Aby w systemie Windows 2000 zastosować wcześniej skonfigurowane zasady zabezpieczeń dla komputera, można wykorzystać predefiniowane szablony zabezpieczeń.

	■ Podstawowy poziom zabezpieczeń dla systemu Windows 2000.
	■ Wyższy poziom zabezpieczeń, niż dostępny w szablonie podstawowym, zapewniający działanie wszystkich elementów aplikacji biurowych.
	■ Wysoki poziom zabezpieczeń, nie zapewniający działania wszystkich składników standardowych aplikacji biurowych.
	■ Maksymalny poziom zabezpieczeń w systemie Windows 2000, nie uwzględniający funkcjonowania aplikacji.

Zagadnienie kluczowe

Predefiniowane szablony zabezpieczeń dostarczane z systemem Windows 2000 w coraz większym stopniu modyfikują domyślne ustawienia zabezpieczeń.

Predefiniowane szablony nie powodują instalacji domyślnych ustawień zabezpieczeń.

Aby w systemie Windows 2000 zastosować własny, wymagany zestaw ustawień, można utworzyć szablon zabezpieczeń lub wykorzystać jeden z gotowych szablonów, co spowoduje zastosowanie predefiniowanych ustawień na komputerze. Wykorzystanie gotowego szablonu w znacznym stopniu modyfikuje konfigurację zabezpieczeń, zwiększając bezpieczeństwo systemu. Załadowanie predefiniowanych szablonów zabezpieczeń *nie* powoduje instalacji ustawień domyślnych.

Ważne Domyślne zasady zabezpieczeń są stosowane tylko dla instalacji systemu Windows 2000 na partycji NTFS. Jeżeli komputer jest uaktualniany z systemu Microsoft Windows NT® w wersji 4.0, zabezpieczenia nie są modyfikowane. Jeśli system Windows 2000 jest instalowany na partycji FAT nie można zastosować zasad zabezpieczeń dla komputera.

Wykorzystanie predefiniowanych szablonów zabezpieczeń

Predefiniowane szablony często zapewniają dobry punkt wyjścia przy dostosowaniu konfiguracji zabezpieczeń do wymaganego poziomu. Przed zastosowaniem takiego szablonu, należy najpierw sprawdzić, czy nie zawiera niekorzystnych ustawień dla aplikacji sieciowych lub sposobów połączeń. Predefiniowane szablony zabezpieczeń zostały tak przygotowane, aby odpowiadały najczęstszym wymaganiom, dotyczącym bezpieczeństwa. Zawierają cztery poziomy zabezpieczeń: podstawowy, zgodny, bezpieczny i wysoki.

Podstawowy

Szablon podstawowy jest tak zdefiniowany, aby zapewniał podstawowy poziom zabezpieczeń dla systemu Windows 2000. Może być wykorzystany jako podstawa do analizy zabezpieczeń i powinien być stosowany jako domyślne ustawienia zabezpieczeń przy konfiguracji komputerów aktualizowanych do systemu Windows 2000.

Predefiniowane podstawowe szablony zabezpieczeń są następujące:

- Domyślny dla stacji roboczej (basicwk.inf)
- Domyślny dla serwera (basicsv.inf)
- Domyślny dla kontrolera domeny (basicdc.inf)

Szablony podstawowe można znaleźć w folderze `systemroot\security\templates`.

Zgodny

Konfiguracja określona w szablonie zgodnym zapewnia wyższy poziom bezpieczeństwa, ale jednocześnie umożliwia działanie wszystkich standardowych aplikacji biurowych. Szablon ten jest wspólny dla stacji roboczej i serwera (compatws.inf).

Bezpieczny

Szablon bezpieczny określa konfigurację wysokiego poziomu zabezpieczeń, ale jego wykorzystanie nie daje pewności, że wszystkie funkcje standardowych aplikacji biurowych będą działać. Predefiniowane bezpieczne szablony zabezpieczeń są następujące:

- Bezpieczny dla stacji roboczej lub serwera (securews.inf)
- Bezpieczny dla kontrolera domeny (securedc.inf)

Wysoki

Zastosowanie szablonu wysokiego bezpieczeństwa zapewnia maksymalny poziom zabezpieczeń w systemie Windows 2000, lecz poprawna praca aplikacji nie jest brana pod uwagę. Szablon ten został utworzony do testowania i rozwijania aplikacji wysokiego poziomu bezpieczeństwa. Predefiniowane szablony wysokiego bezpieczeństwa określają następujące konfiguracje:

- Wysoce bezpieczną stację roboczą lub serwer (hisecws.inf)
- Wysoce bezpieczny kontroler domeny (hisecdc.inf)

Stosowanie szablonu

Szablon zabezpieczeń można zastosować bezpośrednio do lokalnych zasad komputera pod warunkiem, że komputer nie pracuje w domenie. System jest natychmiast konfigurowany z nowymi ustawieniami szablonu.

Aby zastosować szablon bezpieczeństwa do komputera lokalnego należy:

1. W konsoli Security Configuration and Analysis prawym przyciskiem myszy wskazać **Security Configuration and Analysis**.
2. Wybrać polecenie **Open Database**, aby wskazać aktualną bazę danych. (Wskazanie bazy danych jest potrzebne dla określonego szablonu tylko raz.)
3. Wybrać przycisk **Import Template**, wskazać plik szablonu zabezpieczeń i wybrać przycisk **Open**.
4. Prawym przyciskiem myszy wskazać **Security Configuration and Analysis** i wybrać polecenie **Configure System Now**.

Uwaga W środowisku Active Directory można importować szablon zabezpieczeń do obiektu GPO, aby dowolny komputer czy użytkownik w lokalizacji, domenie lub OU, do którego obiekt Group Policy został zastosowany, otrzymał ustawienia szablonu zabezpieczeń. Więcej informacji na temat Group Policy i Active Directory znajduje się w programie kursu 2154A, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

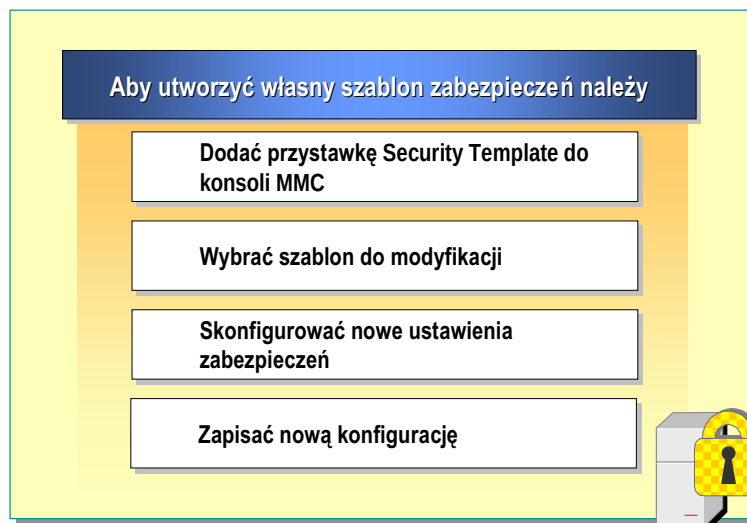
Tworzenie własnego szablonu zabezpieczeń

Cel slajdu

Prezentacja sposobu eksportu szablonu z konsoli Local Security Policy.

Wprowadzenie

Istnieją dwie sugerowane metody tworzenia własnego szablonu zabezpieczeń dla sieci: eksportowanie szablonu z poprawnie skonfigurowanego komputera lub edycja szablonu w programie Security Templates.



Jeśli okaże się, że żaden z predefiniowanych szablonów zabezpieczeń nie spełnia wymagań bezpieczeństwa, należy utworzyć własny szablon. Do dostosowania szablonu należy wykorzystać narzędzie Security Templates. Po dołączeniu narzędzia Security Templates do konsoli MMC (Microsoft Management Console), należy rozpocząć tworzenie własnego szablonu, bez żadnych ustawień początkowych lub zmodyfikować szablon predefiniowany, zapisując go pod inną nazwą.

Aby zmodyfikować predefiniowany szablon wykorzystując program Security Templates, należy:

1. W drzewie konsoli Security Templates rozwinąć gałąź lokalizacji szablonów lub wprowadzić nową ścieżkę. Domyślna ścieżka do szablonów to `systemroot\Security\Templates`.
2. Prawym przyciskiem myszy wskazać szablon przeznaczony do skopiowania i z menu podręcznego wybrać polecenie **Save As**.
3. Wprowadzić nową nazwę szablonu i wybrać przycisk **Save**. Szablon z nową nazwą zostanie wyświetlony w kontenerze z szablonami.
4. Rozwinąć nowy szablon, aby wskazać konfigurowane zasady. Na przykład, aby skonfigurować maksymalny czas ważności hasła, należy rozwinąć **Account Policies** i wybrać **Password Policy**.
5. Wybrać nazwę zasady przeznaczoną do konfiguracji, a następnie przycisk **OK**, aby zapisać w szablonie wprowadzone zmiany.

Nowy szablon jest natychmiast dostępny i można go zastosować do konfiguracji zasad zabezpieczeń dowolnego obiektu GPO.

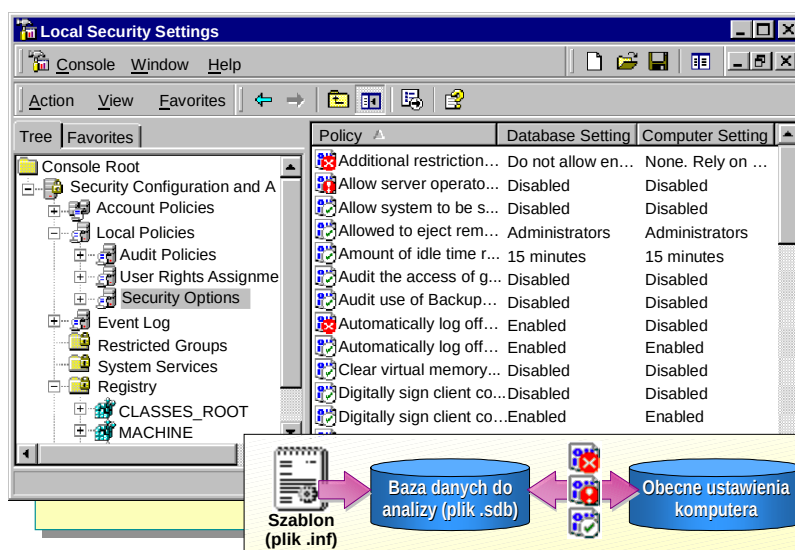
Analiza zabezpieczeń

Cel slajdu

Prezentacja interfejsu wykorzystywanego do analizy zabezpieczeń i terminów z tym związanych.

Wprowadzenie

Program Security Configuration and Analysis pozwala na utworzenie hipotetycznego scenariusza, w celu zapoznania się z efektami zastosowania szablonu do istniejącej konfiguracji zabezpieczeń.



Przed wdrożeniem szablonu zabezpieczeń na dużej liczbie komputerów należy przeanalizować wynik zastosowania szablonu, aby sprawdzić, czy nie powstaną żadne niekorzystne efekty w odniesieniu do aplikacji, połączeń czy zabezpieczeń. Wykorzystanie analizy pomaga w odnalezieniu luk w systemie zabezpieczeń oraz odstępstw od konfiguracji standardowej. Przystawka Security Configuration and Analysis umożliwia utworzenie i przetestowanie hipotetycznego scenariusza działań oraz pozwala na dokonanie zmian w konfiguracji.

Analiza zabezpieczeń

Za pomocą programu Security Configuration and Analysis można porównać konfigurację zabezpieczeń komputera lokalnego z alternatywną konfiguracją, pobraną z szablonu (plik .inf) i przechowywaną w osobnej bazie danych (plik .sdb). Pozwala to upewnić się, że komputer jest skonfigurowany zgodnie z zasadami bezpieczeństwa firmy.

Aby porównać dwie konfiguracje zabezpieczeń, należy:

1. Dodać do konsoli MMC przystawkę Add the Security Configuration and Analysis.
2. Wybrać z menu podręcznego **Security Configuration and Analysis** polecenie **Open database**.
3. Wskazać istniejący plik bazy danych lub utworzyć nową bazę o unikalnej nazwie, a następnie wybrać przycisk **Open**.
4. Istniejąca baza danych zawiera już importowane ustawienia. Jeśli jest tworzona nowa baza, zostanie wyświetlone okno dialogowe **Import Template**. Należy wówczas wybrać bazę danych, a następnie przycisk **Open**.

5. Wskazać prawym przyciskiem myszy **Security Configuration and Analysis** i z menu podręcznego wybrać polecenie **Analyze Computer Now**.
6. W oknie **Perform Analysis** wprowadzić lokalizację dla dziennika analizy i wybrać przycisk **OK**.

Rozpocznie się porównanie dwóch konfiguracji oraz wyświetlanie stanu zaawansowania operacji. Gdy proces zostanie zakończony, należy przejrzeć drzewo ustawień, w celu zapoznania się z rezultatami. Rozbieżności zostaną oznaczone czerwonym znacznikiem. Podobieństwa będą oznaczone znacznikiem zielonym. Zasady nie oznaczone żadnym znacznikiem nie są skonfigurowane w bazie danych.

Konfiguracja zabezpieczeń

Po zakończeniu analizy można przystąpić do zastosowania szablonu, w celu ponownej konfiguracji zabezpieczeń systemu. Aby to zrobić, należy:

- Usunąć różnice poprzez skonfigurowanie ustawień w bazie danych tak, by odpowiadały aktualnym ustawieniom komputera. Zmiany ustawień w bazie danych można wykonywać w panelu szczegółów konsoli.
- Importować inny plik szablonu, scalić jego ustawienia i nadpisać te, przy których wystąpił konflikt. Aby dokonać importu innego pliku szablonu, należy wskazać prawym przyciskiem myszy **Security Configuration and Analysis** i z menu podręcznego wybrać polecenie **Import Template**.
- Eksportować aktualne ustawienia bazy danych do pliku szablonu. Aby eksportować ustawienia do pliku szablonu, należy wskazać prawym przyciskiem myszy **Security Configuration and Analysis** i z menu podręcznego wybrać polecenie **Export Template**.

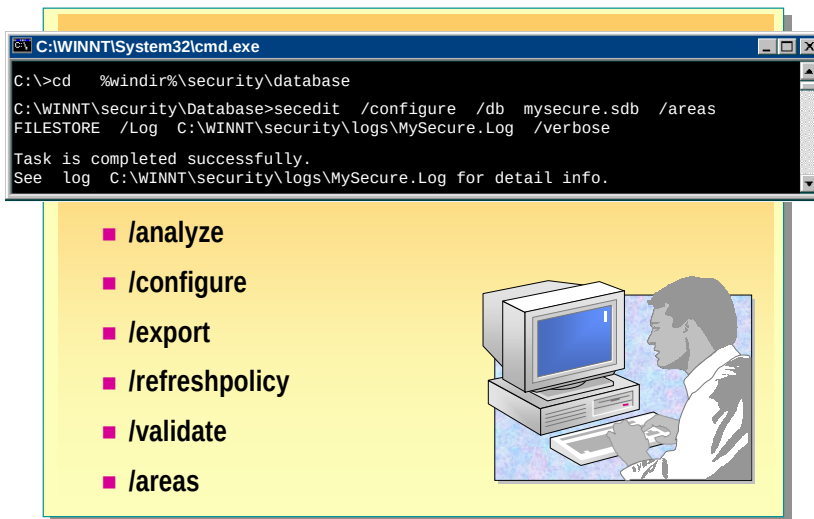
Konfiguracja i analiza zabezpieczeń z poziomu wiersza poleceń

Cel slajdu

Prezentacja wykorzystania polecenia **secedit**.

Wprowadzenie

Zarządzanie zasadami zabezpieczeń można prowadzić także z poziomu wiersza poleceń.



- **/analyze**
- **/configure**
- **/export**
- **/refreshpolicy**
- **/validate**
- **/areas**

Operacje wykonywane w wierszu poleceń pozwalają na konfigurację zabezpieczeń przy wykorzystaniu skryptów, w przeciwieństwie do graficznego interfejsu użytkownika (GUI). Dodatkowo, polecenie Secedit.exe umożliwia wykorzystanie pewnych cech niedostępnych w interfejsie graficznym, jak na przykład, odświeżanie zasad zabezpieczeń.

Wykorzystanie polecenia Secedit

Jest pięć operacji wysokiego poziomu, które można wykonać za pomocą polecenia Secedit.exe:

- Przełączniki **/analyze**, **/configure** i **/export** odpowiadają tym samym zadaniom, które są dostępne w programie Security Configuration and Analysis. Funkcje te wymagają wskazania wykorzystywanej bazy danych przełącznikiem **/db**. Można także, przełącznikiem **/cfg**, wskazać szablon przeznaczony do importu. Funkcje te obsługują także tryby **/verbose** i **/quiet**, które nie są dostępne w programie Security Configuration and Analysis.
- Przełącznik **/refreshpolicy** pozwala na wymuszenie propagacji zdarzeń Group Policy, co zwykle ma miejsce w czasie uruchomienia komputera, a później co 60 – 90 minut lub gdy zasady zabezpieczeń lokalnych zostaną zmienione przy użyciu rozszerzenia Security Settings konsoli Group Policy. Aby spowodować odświeżenie zasad zabezpieczeń niezależnie od tego, kiedy uległy one zmianom, należy dołączyć przełącznik **/enforce**.
- Przełącznik **/validate** powoduje sprawdzanie poprawności składni szablonu tworzonego przy użyciu Security Templates.

Wykorzystanie przełącznika /areas

Unikalny dla polecenia Secedit.exe jest również przełącznik **/areas**, który pozwala na eksport wybranego obszaru ustawień zabezpieczeń. Obszary te opisano w poniższej tabeli.

Obszar	Opis
securitypolicy	Zasady lokalne i zasady domenowe dla systemu, zawierają zasady kont, inspekcji i tym podobne elementy.
group_mgmt	Ustawienia zasad dla grup o ograniczonym członkostwie, dla dowolnych grup wskazanych w szablonie zabezpieczeń.
user_rights	Przypisywanie użytkownikom praw, w tym prawa logowania.
regkeys	Zabezpieczenia lokalnych kluczy rejestru.
filestore	Zabezpieczenia przechowywania plików lokalnych.
services	Zabezpieczenia dla wszystkich zdefiniowanych usług.

Na przykład, należy skonfigurować zabezpieczenia na lokalnym komputerze wykorzystując następujące parametry:

- Ustawienia, które będą konfigurowane, znajdują się w pliku bazy danych Mysecure.sdb.
- Skonfigurowane powinny zostać tylko prawo użytkownika do logowania i zabezpieczenia przechowywania lokalnych plików.
- Wymagany jest szczegółowy dziennik, zapisany w pliku o nazwie Mysecure.log.
- Lokalizacja folderu systemowego Windows 2000 to C:\Winnt.

Aby skonfigurować zabezpieczenia według podanych parametrów, należy skorzystać z następującego polecenia:

```
secedit /configure /db mysecure.sdb /areas USER_RIGHTS FILESTORE  
/log c:\winnt\security\logs\Mysecure.log /verbose
```

Uwaga Aby obejrzeć pełną składnię polecenia Secedit.exe, należy skorzystać z systemu pomocy Windows 2000.

Laboratorium A: Konfigurowanie zabezpieczeń w systemie Windows 2000

Cel slajdu

Omówienie laboratorium.

Wprowadzenie

W tym laboratorium zostaną wdrożone zasady zabezpieczeń przy użyciu zestawu narzędzi Security Configuration Tool.



Wyjaśnij cel laboratorium

Cele laboratorium

Po zrealizowaniu tego laboratorium słuchacz będzie potrafił:

- Utworzyć szablon zabezpieczeń.
- Przeanalizować i skonfigurować ustawienia zabezpieczeń komputera przy wykorzystaniu szablonów zabezpieczeń.

Wymagania wstępne

Przed rozpoczęciem tego laboratorium, należy zapoznać się z prawami użytkowników oraz usługami systemu Windows 2000.

Przygotowanie laboratorium

Do wykonania tego laboratorium niezbędne są:

- Komputer pracujący w systemie Windows 2000 Advanced Server skonfigurowany jako serwer członkowski w domenie nwtraders.msft.
- Konto użytkownika Adminx (gdzie x jest numerem stanowiska).
- Domenowe konto użytkownika bez przywilejów administratorskich.

Przewidywany czas ukończenia laboratorium: 30 minut

Ćwiczenie 1

Tworzenie szablonu zabezpieczeń

Scenariusz

W założeniach bezpieczeństwa Twojej firmy wymagane jest okresowe przeglądanie ustawień zabezpieczeń na komputerach oraz wymuszenie ustawień zabezpieczeń, zawartych w firmowych założeniach. W tym celu, opisano zasady zabezpieczeń, określające szereg ustawień, które muszą być zastosowane dla serwerów w sieci. Musisz skonfigurować w szablonie zabezpieczeń następujące zasady, które zostaną wykorzystane do konfiguracji serwerów:

- Tylko administratorzy są uprawnieni do zamknięcia systemu.
- Przy próbie logowania powinna być wyświetlana informacja, ostrzegająca przed tym, że nieautoryzowany dostęp do komputera jest zabroniony.
- Nazwa ostatnio zalogowanego użytkownika nie powinna być wyświetlana w oknie **Log on to Windows**, aby zapobiec poznawaniu nazw kont użytkowników przez nieupoważnione osoby.
- Usługa Telnet powinna zostać zablokowana.

Cel

W tym ćwiczeniu utworzysz konsolę MMC, z dołączonymi przystawkami Security Configuration and Analysis i Security Template. Następnie, utworzysz nowy szablon zabezpieczeń i skonfigurujesz w nim ustawienia zabezpieczeń wymienione w scenariuszu.

Zadania	Szczegółowe kroki
1. Zaloguj się do domeny nwtraders.msft jako Studentx (gdzie x jest numerem Twojego stanowiska) z hasłem domain i utwórz konsolę MMC, zawierającą przystawki Security Configuration and Analysis i Security Template. Przypisz konsoli nazwę Security Tools i zapisz ją na pulpicie.	a. Zaloguj się, wykorzystując następujące informacje: User name: Studentx (gdzie x jest numerem Twojego stanowiska) Password: domain Log on to: nwtraders b. Rozwiń menu Start i wybierz polecenie Run. c. W oknie Open wpisz mmc i wybierz przycisk OK. d. W oknie Console1, z menu Console wybierz polecenie Add/Remove Snap-in. e. W oknie Add/Remove Snap-in wybierz przycisk Add. f. W oknie Add Standalone Snap-in, na liście Available Standalone Snap-ins wskaż Security Configuration and Analysis i wybierz przycisk Add, a następnie wskaż Security Templates i wybierz przycisk Add. g. Wybierz przycisk Close, aby zamknąć okno Add Standalone Snap-in, a następnie przycisk OK, aby zamknąć okno Add/Remove Snap-in. h. Z menu Console wybierz polecenie Save As. i. W oknie Save in odszukaj pulpit. j. W polu File name wpisz Security Tools i wybierz przycisk Save. k. Zamknij okno Security Tools.

(ciąg dalszy)

Zadania	Szczegółowe kroki
2. Wykorzystaj przygotowaną konsolę do utworzenia szablonu zabezpieczeń, nazwanego <i>Server Security Template</i> (gdzie <i>Server</i> jest nazwą Twojego komputera).	a. Na pulpicie wskaż prawym przyciskiem myszy Security Tools i wybierz polecenie Run as. b. W oknie Run As Other User, w polu User name wpisz Adminx (gdzie x jest numerem Twojego komputera). c. W polu Password wpisz domain d. W polu Domain wpisz nwtraders.msft i wybierz przycisk OK. e. W drzewie konsoli rozwiń Security Templates i prawym przyciskiem myszy wskaż C:\WINNT\Security\Templates, a następnie wybierz polecenie New Template. f. W oknie C:\WINNT\Security\Templates, w polu Template name wpisz Server Security Template (gdzie <i>Server</i> jest nazwą Twojego komputera). g. W polu Description wpisz Corporate Standard Server Settings i wybierz przycisk OK.
3. Skonfiguruj szablon zabezpieczeń tak, aby jedynie administrator mógł zamknąć system.	a. W drzewie konsoli rozwiń C:\WINNT\Security\Templates, następnie Server Security Template (gdzie <i>Server</i> jest nazwą Twojego komputera), a następnie Local Policies. b. Wskaż User Rights Assignment i w oknie szczegółów wybierz Shut down the system. c. W oknie Template Security Policy Setting wybierz opcję Define these policy settings in the template, a następnie przycisk Add. d. W oknie Add user or group wybierz przycisk Browse. e. W oknie Select Users or Groups, w polu Look in sprawdź, czy zaznaczony jest Twój komputer. f. Na liście Name wybierz grupę Administrators, następnie przycisk Add i przycisk OK. g. Wybierz przycisk OK, aby zamknąć okno Add user or group i ponownie przycisk OK, aby zamknąć okno Template Security Policy Setting.  <i>Zauważ, że w oknie szczegółów, przy zasadzie Shut down the system widoczna jest teraz grupa Administrators.</i>
4. Skonfiguruj szablon zabezpieczeń, aby zapobiec wyświetleniu w oknie Log on to Windows ostatnio używanej nazwy użytkownika.	a. W drzewie konsoli wskaż Security Options, a w oknie szczegółów wybierz Do not display last username in logon screen. b. W oknie Template Security Policy Setting zaznacz opcję Define these policy settings in the template, wybierz opcję Enabled i przycisk OK.  <i>Zauważ, że w panelu szczegółów przy zasadzie Do not display last username in logon screen wyświetlany jest napis Enabled.</i>
5. Skonfiguruj szablon zabezpieczeń, aby przy logowaniu wyświetlana była następująca informacja: LEGAL NOTICE: Authorized Users Only.	a. W panelu szczegółów wybierz Message text for users attempting to log on. b. W oknie Template Security Policy Setting wybierz opcję Define these policy settings in the template. c. Wpisz Unauthorized access is prohibited. If you are not an authorized user, do not attempt to log on i wybierz przycisk OK.

(ciąg dalszy)

Zadania	Szczegółowe kroki
5. (ciąg dalszy)	d. W oknie szczegółów wybierz Message title for users attempting to log on. e. W oknie Template Security Policy Setting wybierz opcję Define these policy settings in the template. f. Wpisz LEGAL NOTICE: Authorized Users Only i wybierz przycisk OK.  <i>Zauważ, że w panelu szczegółów wyświetlane są ustawienia zdefiniowanej wiadomości.</i>
6. Skonfiguruj szablon zabezpieczeń, aby zablokować usługę Telnet i zapisz szablon.	a. W drzewie konsoli wskaż System Services i w oknie szczegółów wybierz Telnet. b. W oknie Template Security Policy Setting wybierz opcję Define these policy settings in the template.  <i>Zostało wyświetlone okno Security for Telnet, które jest wykorzystywane do wskazania użytkowników i grup, dla których ma zastosowanie ta zasada.</i> c. Wybierz przycisk OK, aby zamknąć okno. d. W oknie Template Security Policy Setting upewnij się, że na liście Select service startup mode wybrana jest opcja Disabled i wybierz przycisk OK.  <i>Zauważ, że w kolumnie Startup wyświetlany jest napis Disabled for the Telnet service.</i> e. W drzewie konsoli wskaż prawym przyciskiem myszy Server Security Template (gdzie Server jest nazwą Twojego komputera) i z menu podręcznego wybierz polecenie Save.

Ćwiczenie 2: Analiza i konfiguracja zasad bezpieczeństwa komputera przy użyciu szablonu zabezpieczeń

Scenariusz

Zanim rozpoczniesz modyfikację ustawień zabezpieczeń dla komputera, warto najpierw porównać obecną konfigurację zabezpieczeń z konfiguracją zawartą w nowym szablonie. Gdy przekonasz się, że obecny poziom bezpieczeństwa komputera jest niewystarczający, będziesz musiał skonfigurować komputer ponownie, wykorzystując utworzony przez siebie szablon zabezpieczeń. Następnie sprawdzić skonfigurowane ustawienia.

Cel

W tym ćwiczeniu utworzysz bazę danych zabezpieczeń, wykorzystując utworzony szablon zabezpieczeń, a następnie dokonasz analizy obecnego poziomu bezpieczeństwa komputera. Skonfigurujesz komputer, wykorzystując utworzony szablon zabezpieczeń i dokonasz ponownej analizy poziomu bezpieczeństwa. Następnie, przez zalogowanie się jako użytkownik domeny, sprawdzisz, czy nowe ustawienia zabezpieczeń zostały wymuszone w całej domenie.

Zadania	Szczegółowe kroki
1. Utwórz bazę danych zabezpieczeń.	a. W drzewie konsoli wybierz Security Configuration and Analysis. b. Wskaż prawym przyciskiem myszy Security Configuration and Analysis i z menu podręcznego wybierz polecenie Open database. c. W oknie Open database, w polu File name wpisz Server (gdzie Server jest nazwą Twojego komputera) i wybierz przycisk Open. d. W oknie Import Template wskaż Server Security Template i wybierz przycisk Open.  Zauważ, że w panelu szczegółów wyświetlana jest informacja, wskazującą na możliwość konfiguracji lub analizy systemu.
2. Dokonaj analizy zabezpieczeń komputera przy użyciu utworzonego szablonu bezpieczeństwa.	a. W drzewie konsoli wskaż prawym przyciskiem myszy Security Configuration and Analysis i z menu podręcznego wybierz polecenie Analyze Computer Now. b. W oknie Perform Analysis wybierz przycisk OK, aby zaakceptować domyślny dziennik błędów oraz rozpocząć analizę. c. Gdy analiza zakończy się, rozwiń Security Configuration and Analysis.
 Które z poniższych ustawień zabezpieczeń są poprawnie skonfigurowane? (Podpowiedź: Przejdź do lokalizacji poniżej Local Policies w drzewie konsoli, aby zobaczyć ustawienia skonfigurowane w poprzednim ćwiczeniu. Nieprawidłowo skonfigurowane ustawienia są oznaczone czerwonym znakiem x.) Żadne. ☐ Local Policies\Users Rights Assignment\Shut down the system ☐ Local Policies\Security Options\Do not display last username in logon screen ☐ Local Policies\Security Options\Message text for users attempting to log on ☐ Local Policies\Security Options\Message title for users attempting to log on ☐ System Services\Telnet	

(ciąg dalszy)

Zadania	Szczegółowe kroki
3. Skonfiguruj system przy użyciu szablonu utworzonego w Ćwiczeniu 1.	a. W drzewie konsoli wskaż prawym przyciskiem myszy Security Configuration and Analysis i wybierz polecenie Configure Computer Now. b. W oknie Configure System wybierz przycisk OK, aby zaakceptować domyślną ścieżkę dziennika błędów i rozpocząć konfigurację.  Program <i>Security Configuration Manager</i> wyświetli komunikat Configuring System Security, który pokazuje postęp procesu konfiguracji, informując, które obszary są konfigurowane.
4. Dokonaj analizy komputera przy użyciu szablonu zabezpieczeń utworzonego w Ćwiczeniu 1.	a. W drzewie konsoli wskaż prawym przyciskiem myszy Security Configuration and Analysis i wybierz polecenie Analyze Computer Now. b. W oknie Perform Analysis wybierz przycisk OK, aby zaakceptować domyślną ścieżkę dziennika błędów i rozpocząć analizę. c. Po zakończeniu analizy, jeśli to konieczne, rozwiń Security Configuration and Analysis.
? Które z poniższych zabezpieczeń są poprawnie skonfigurowane? Wszystkie ustawienia są skonfigurowane, tak jak wskazano to w szablonie zabezpieczeń. ✓ Local Policies\Users Rights Assignment\Shutdown the system ✓ Local Policies\Security Options\Do not display last username in logon screen ✓ Local Policies\Security Options\Message text for users attempting to log on ✓ Local Policies\Security Options\Message title for users attempting to log on ✓ System Services\Telnet	
4. (ciąg dalszy)	d. Zamknij okno Security Tools, zapisując ustawienia konsoli i wyloguj się.
5. Sprawdź, czy importowane zasady zostały właściwie zastosowane. Zaloguj się do domeny nwtraders.msft jako Studentx (gdzie x jest numerem Twojego stanowiska) z hasłem domain .	a. W czasie wyświetlania okna Welcome to Windows wciśnij kombinację klawiszy CTRL+ALT+DELETE.
? Czy jest wyświetlana informacja z tytułem i treścią skonfigurowanymi wcześniej? Tak. _____ _____ _____ _____	
5. (ciąg dalszy)	b. Wybierz przycisk OK .

(ciąg dalszy)

Zadania	Szczegółowe kroki
? Czy w oknie Log On to Windows wyświetlana jest nazwa ostatnio zalogowanego użytkownika? Nie.	
5. (ciąg dalszy)	c. Zaloguj się, wykorzystując następujące informacje: User name: Studentx (gdzie x jest numerem Twojego stanowiska) Password: domain Log on to: nwtraders d. Z menu Administrative Tools uruchom Computer Management. e. W drzewie konsoli rozwiń Services and Applications i wybierz Services. f. W oknie szczegółów wyświetl wpis dla usługi Telnet.
? Jaki jest typ uruchomienia usługi Telnet? Disabled.	
5. (ciąg dalszy)	g. Zamknij program Computer Management.

Ćwiczenie 3

Usuwanie Group Policy

Scenariusz

Musisz usunąć serwer z sieci i przenieść go do innej. Zasady zabezpieczeń sieci docelowej są inne niż dotychczasowej. Przed przeniesieniem komputera musisz usunąć zasady zabezpieczeń.

Cel

W tym ćwiczeniu, poprzez zastosowanie szablonu podstawowego, usuniesz ustawienia zabezpieczeń przypisane w poprzednim ćwiczeniu.

Zadania	Kolejne kroki
1. Wykorzystaj polecenie Run As dla konsoli MMC Security Tools, umieszczonej na pulpicie, podając jako nazwę użytkownika Adminx (gdzie x jest numerem Twojego stanowiska), hasło domain , a nazwę domeny nwtraders.msft. Skonfiguruj system za pomocą podstawowego szablonu zabezpieczeń.	a. Na pulpicie, wskaż prawym przyciskiem myszy Security Tools i wybierz z menu podręcznego polecenie Run as . b. W oknie Run As Other User , w polu User name wpisz Adminx (gdzie x jest numerem Twojego stanowiska). c. W polu Password wpisz domain d. W polu Domain wpisz nwtraders.msft i wybierz przycisk OK . e. W oknie szczegółów konsoli Security Tools wskaż prawym przyciskiem myszy Security Configuration and Analysis i wybierz polecenie Import Template . f. W oknie Import Template wskaż szablon basicsv i wybierz przycisk Open . g. W drzewie konsoli wskaż prawym przyciskiem myszy Security Configuration and Analysis i z menu podręcznego wybierz polecenie Configure Computer Now . h. W oknie Configure System wybierz przycisk OK , aby zaakceptować domyślne położenie dziennika i rozpocząć konfigurację. i. Gdy konfiguracja zostanie zakończona, zamknij okno Security Tools nie zapisując ustawień konsoli i wyloguj się.
2. Zaloguj się, aby sprawdzić, czy wyświetlany jest komunikat ostrzegawczy i nazwa konta logującego się poprzednio użytkownika.	a. Przy wyświetlonym oknie Welcome to Windows wciśnij klawisze CTRL+ALT+DELETE.
 Czy przed wyświetleniem okna Log On to Windows został wyświetlony komunikat ostrzegawczy? Czy nazwa ostatnio zalogowanego użytkownika jest wyświetlana w polu User name? Nie. Komunikat ostrzegawczy nie jest wyświetlany przed wyświetleniem okna Log On to Windows, a nazwa ostatnio zalogowanego użytkownika również nie jest wyświetlana w polu User name okna logowania. _____ _____ _____	
2. (ciąg dalszy)	b. Wybierz przycisk Cancel aby zamknąć okno Log On to Windows .

◆ Inspekcja dostępu do zasobów systemowych

Cel slajdu

Wprowadzenie do zagadnień związanych z wdrażaniem zasad inspekcji.

Wprowadzenie

Aby śledzić wybrane zdarzenia i utrzymać bezpieczeństwo systemu, można wdrożyć zasady inspekcji.

- Wprowadzenie do inspekcji
- Wybór zdarzeń do inspekcji
- Planowanie zasad inspekcji
- Ustawianie zasad inspekcji
- Inspekcja dostępu do zasobów

W systemie Windows 2000 jest możliwe śledzenie aktywności użytkowników i systemu operacyjnego. Pozwala to ocenić całkowity poziom bezpieczeństwa systemu. Zrozumienie, w jaki sposób wdrożyć inspekcję i monitorować zdarzenia systemowe, jest niezwykle ważne dla wykrywania prób nieautoryzowanego dostępu do danych w sieci.

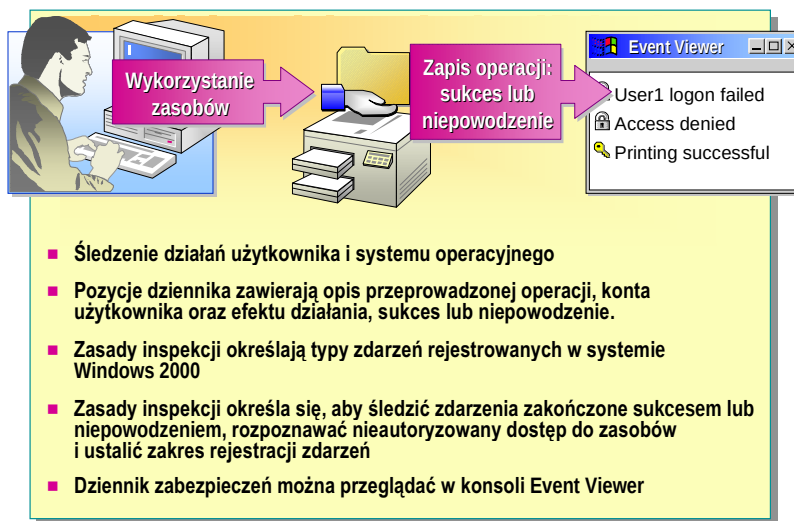
Wprowadzenie do inspekcji

Cel slajdu

Prezentacja celów inspekcji.

Wprowadzenie

Inspekcja jest mechanizmem, wykorzystywanym przez administratorów, do monitorowania bezpieczeństwa sieci.



Zagadnienie kluczowe

Wykorzystaj inspekcję do śledzenia zdarzeń systemowych. W opisie zdarzenia umieszczane są informacje o rodzaju zdarzenia, użytkownika oraz czasie wykonania działania.

W systemie Windows 2000 inspekcja jest procesem śledzenia na komputerze przejawów aktywności (nazywanych zdarzeniami) użytkownika i systemu operacyjnego. Gdy wystąpi śledzone zdarzenie, dokonywany jest wpis w dzienniku zabezpieczeń.

Wpisy inspekcji

Wpis w dzienniku zabezpieczeń (security) zawiera:

- Identyfikację wykonanego działania.
- Nazwę użytkownika przeprowadzającego działania.
- Informację, czy działanie zostało zakończone sukcesem czy niepowodzeniem.
- Dodatkowe informacje, takie jak nazwa komputera, z którego użytkownik próbował wykonać działanie.

Zasady inspekcji

Zasady inspekcji określają typ zdarzeń, których wystąpienie spowoduje umieszczenie wpisu w dzienniku zabezpieczeń komputera. W systemie Windows 2000 zdarzenia zapisywane są do dziennika komputera, na którym miały miejsce.

Zasady inspekcji ustawia się, aby:

- Śledzić zdarzenia zakończone sukcesem lub niepowodzeniem, takie jak próby logowania, próby odczytania pliku przez konkretnego użytkownika, zmiany odnoszące się do konta użytkownika lub członkostwa w grupach, zmiany w ustawieniach zabezpieczeń.
- Zmniejszyć ryzyko nieautoryzowanego wykorzystania zasobów.
- Otrzymać spis działań użytkowników i administratora.

Przeglądanie zdarzeń

Aby w systemie Windows 2000 przejrzeć zdarzenia wpisane do dziennika systemowego, należy użyć programu Event Viewer. Aby ustalić trendy długoterminowe, można archiwizować pliki dziennika. Pomaga to w określeniu, na przykład, wykorzystania drukarek, dostępu do plików lub weryfikacji prób nieautoryzowanego wykorzystania zasobów.

Wybór zdarzeń do inspekcji

Cel slajdu
Identyfikacja zdarzeń, które podlegają inspekcji w systemie Windows 2000.

Wprowadzenie
Wdrożenie zasad inspekcji musi poprzedzać wskazanie typu zdarzenia, które ma być śledzone.

Zdarzenie	Przykład
Account Logon	Żądanie uwierzytelnienia konta użytkownika przez kontroler domeny
Account management	Tworzenie, usuwanie lub modyfikacja konta użytkownika lub grupy przez administratora
Directory Service Access	Dostęp użytkownika do obiektu usługi Active Directory
Logon	Wylogowanie lub logowanie użytkownika do lokalnego komputera
Object Access	Dostęp użytkownika do pliku, folderu lub drukarki
Policy Change	Dokonanie zmian w opcjach zabezpieczeń użytkownika, prawach użytkownika lub zasadach inspekcji
Privilege Use	Korzystanie z uprawnień, takich jak przejęcie pliku na własność
Process Tracking	Wykonanie operacji przez aplikację
System	Zamknięcie lub ponownie uruchomienie systemu

Pierwszym krokiem przy wdrażaniu zasad inspekcji jest wskazanie typu zdarzeń przeznaczonych do śledzenia. W poniższej tabeli znajduje się opis zdarzeń, które w systemie Windows 2000 można poddać inspekcji.

Zdarzenie	Przykład
Account Logon	Nazwa i hasło użytkownika są weryfikowane w bazie danych zabezpieczeń. Gdy użytkownik loguje się do komputera lokalnego, zdarzenie logowania jest zapisywane w dzienniku komputera lokalnego. Gdy użytkownik loguje się do domeny, zdarzenie logowania jest zapisywane na kontrolerze uwierzytelniającym.
Account Management	Administrator tworzy, modyfikuje lub usuwa konto użytkownika lub grupy. Konto użytkownika jest blokowane lub odblokowywane, zmieniana jest nazwa konta lub hasło.
Directory Service Access	Użytkownik uzyskuje dostęp do obiektów usługi Active Directory. Aby zapisywać te zdarzenia, należy najpierw wskazać obiekty przeznaczone do inspekcji.
Logon	Użytkownik loguje się lub wylogowuje z lokalnego komputera, tworzy lub usuwa połączenie sieciowe ze zdalnym komputerem. Zdarzenie jest zapisywane na komputerze, do którego użytkownik uzyskał dostęp, niezależnie od tego, czy wykorzystywane jest konto lokalne czy domenowe.
Object Access	Użytkownik uzyskuje dostęp do pliku, folderu lub drukarki. Administrator musi skonfigurować odpowiedni plik, folder lub drukarkę do inspekcji.
Policy Change	Została wykonana zmiana opcji zabezpieczeń użytkownika (opcji hasła, ustawień logowania), praw użytkownika lub zasad inspekcji.
Privilege Use	Użytkownik wykorzystał swoje prawa, takie jak zmiana czasu systemowego (nie są w tym zawarte prawa odnoszące się do logowania) lub administrator przejął plik na własność.

(ciąg dalszy)

Zdarzeniet	Przykład
Process Tracking	Aplikacja wykonała działanie. Ta informacja jest w zasadzie istotna tylko dla programistów, którzy chcą śledzić etapy wykonywania aplikacji.
System	Użytkownik ponownie uruchamia bądź wyłącza komputer, lub zachodzi dowolne zdarzenie oddziałujące na bezpieczeństwo systemu Windows 2000 lub dziennik zabezpieczeń.

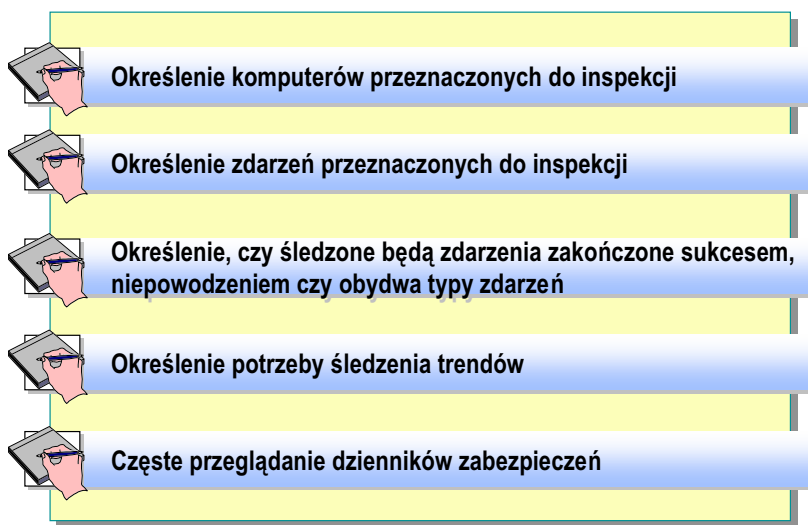
Planowanie zasad inspekcji

Cel slajdu

Prezentacja planowania strategii inspekcji i określenie zdarzeń przeznaczonych do inspekcji.

Wprowadzenie

Przed ustanowieniem inspekcji, należy określić zdarzenia przeznaczone do śledzenia oraz czy monitorować działania zakończone sukcesem, czy niepowodzeniem.



Wskazówka

Pokaż słuchaczom, jakie zdarzenia mogą podlegać inspekcji w systemie Windows 2000.

Poinformuj ich, że można śledzić tylko zdarzenia skonfigurowane w zasadach inspekcji oraz, że dzienniki zdarzeń powinny być regularnie sprawdzane, ponieważ dopiero wtedy uzyskane informacje mogą być cenne dla firmy.

Inspekcja zbyt dużej ilości typów zdarzeń może spowodować przepełnienie dzienników. Wskazane jest prowadzenie inspekcji tylko tych zdarzeń, które zapewnią informacje przydatne w analizie zabezpieczeń. Przy planowaniu zasad inspekcji, należy wziąć pod uwagę poniższe wskazówki:

- Należy określić komputery przeznaczone do inspekcji. Zaplanować inspekcję dla każdego z komputerów, gdyż w systemie Windows 2000 zdarzenia zapisywane są dla każdego komputera z osobna. Dzięki temu można będzie częściej sprawdzać komputery zawierające ważne dane, a rzadziej wykorzystywane tylko do uruchamiania aplikacji.
- Określić typy zdarzeń podlegające inspekcji:
 - Dostęp do plików i folderów
 - Logowanie i wylogowywanie użytkowników
 - Zamykanie i ponowne uruchamianie komputerów z systemem Windows 2000 Server
 - Zmiany dotyczące kont użytkowników i grup
- Określić, czy śledzone będą działania zakończone sukcesem czy niepowodzeniem. Śledzenie zdarzeń zakończonych sukcesem wskazuje jak wielu użytkowników korzystało z konkretnego pliku lub drukarki, co można wykorzystać do planowania rozmieszczenia zasobów. Śledzenie zdarzeń zakończonych niepowodzeniem pozwala wychwycić próby naruszenia bezpieczeństwa systemu.
- Określić, czy potrzebne jest wyznaczanie trendów wykorzystania systemu. Jeśli tak, warto zaplanować archiwizowanie dzienników zdarzeń. Część organizacji wymaga przechowywania zapisów dotyczących zasobów i dostępu do danych.
- Często przeglądać dzienniki zabezpieczeń. Warto wyznaczyć harmonogram przeglądania dzienników zabezpieczeń. Poprzestanie tylko na konfiguracji, nie spowoduje zwrócenia uwagi na próby naruszenia bezpieczeństwa.

Ustawianie zasad inspekcji

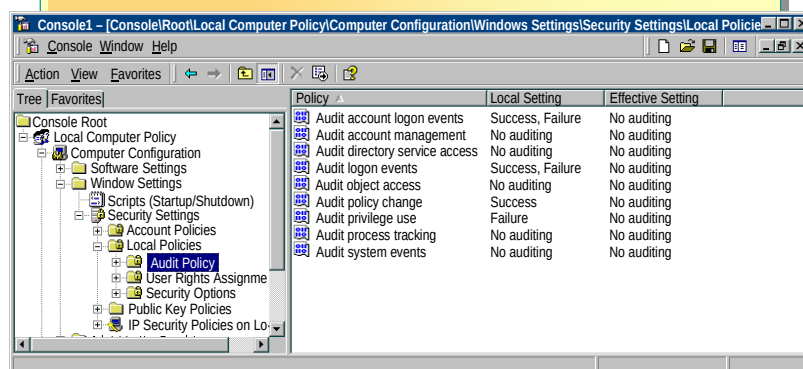
Cel slajdu

Prezentacja sposobu ustawiania zasad inspekcji.

Wprowadzenie

Zanim zostaną wskazane zdarzenia podlegające inspekcji, należy przygotować zasady inspekcji.

- Przypisanie ustawień zabezpieczeń dla pojedynczego komputera przez konfigurację ustawień w Local Policy lub Group Policy
- Przypisanie ustawień zabezpieczeń dla wielu komputerów przez utworzenie obiektu Group Policy Object



Wskazówka

Zaprezentuj sposób przygotowania zasad inspekcji.

Po przygotowaniu zasad inspekcji na pojedynczym komputerze, można wdrożyć inspekcję systemu plików, obiektów Active Directory i drukarek. Aby zastosować zasady inspekcji za pojedynczym komputerze, należy skonfigurować ustawienia zasad inspekcji dla komputera, w gałęzi Local Policies konsoli Group Policy. Zasady inspekcji mogą też zostać przygotowane jako część szablonu zabezpieczeń i przy wykorzystaniu narzędzia Security Configuration and Analysis rozpowszechnione w sieci. Inny sposób to import szablonu do obiektów Group Policy.

Aby przygotować zasady inspekcji należy:

1. Utworzyć konsolę MMC, dodając do niej przystawkę Group Policy, a następnie wybrać **Local Computer** jako obiekt Group Policy.
2. W drzewie konsoli Local Computer Policy rozwinąć kolejno: **Computer Configuration, Windows Settings, Security Settings, Local Policies** i wybrać **Audit Policy**.

W oknie szczegółów zostaną wyświetlone aktualne ustawienia zasad inspekcji.

3. Wskazać typ zdarzenia do śledzenia i wybrać polecenie **Security** z menu **Action**.
4. Zaznaczyć pole opcji **Success, Failure** lub oba i wybrać przycisk **OK**.

Ważne Zasady inspekcji mogą być konfigurowane tylko przez członków grupy Administrators.

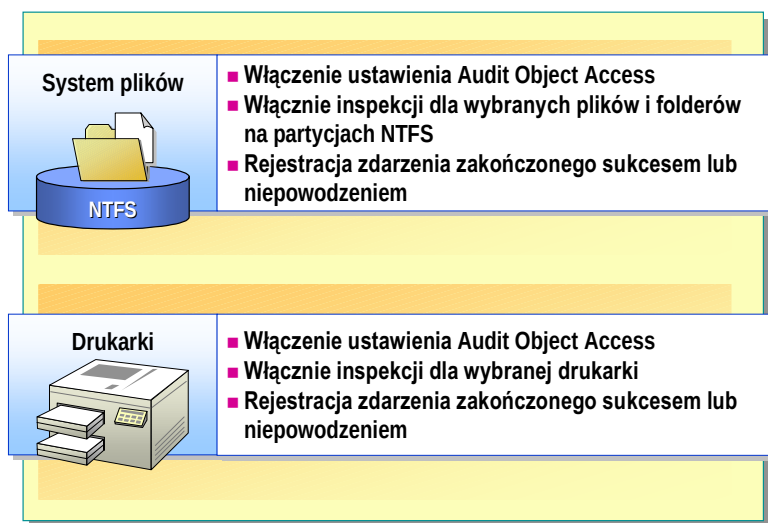
Inspekcja dostępu do zasobów

Cel slajdu

Prezentacja procedury inspekcji dostępu do systemu plików i drukarek.

Wprowadzenie

Aby zostać ostrzeżonym przed możliwością naruszenia bezpieczeństwa, należy skonfigurować inspekcję plików, folderów i drukarek.



Wskazówka

Zaprezentuj, jak należy przygotować inspekcję dla pliku.

Przy prowadzeniu inspekcji w celach bezpieczeństwa, standardowo śledzony jest dostęp do systemu plików i drukarek.

Inspekcja dostępu do systemu plików

Aby monitorować dostęp użytkowników do systemu plików należy:

- Skonfigurować zasady inspekcji do prowadzenia inspekcji dostępu do obiektów, w tym plików i folderów.
- Włączyć inspekcję wybranych plików i folderów oraz wskazać typ zdarzeń do inspekcji. Inspekcja dostępu do plików i folderów może być prowadzona tylko na partycjach NTFS. System plików FAT nie umożliwia inspekcji.

Zagadnienie kluczowe

Inspekcja może być prowadzona tylko dla plików i folderów na partycjach NTFS.

Przy określeniu ustawień inspekcji systemu plików można korzystać z poniższych wskazówek:

- Rejestrować niepowodzenie operacji Read, do określenia użytkowników próbujących uzyskać dostęp do plików, do których nie mają przypisanych uprawnień.
- Rejestrować zakończone sukcesem i niepowodzeniem operacje Delete, przy inspekcji plików poufnych i archiwalnych.
- Rejestrować zakończone sukcesem i niepowodzeniem operacje Change Permissions i Take Ownership, dla poufnych i osobistych plików użytkownika. Wystąpienie takich operacji może sugerować próbę zmiany zabezpieczeń dostępu do danych. Jeśli administrator przejmie na własność plik użytkownika, aby zezwolić sobie na dostęp do tego pliku, takie ustawienie pozwoli zarejestrować to zdarzenie.
- Rejestrować zakończone sukcesem i niepowodzeniem operacje prowadzone przez grupę Guests. Szczególnie powinno być to konfigurowane dla zasobów, do których grupa Guest nie ma dostępu.
- Prowadzić inspekcję plików i folderów na wszystkich komputerach zawierających udostępniane dane, które powinny być zabezpieczone.

Inspekcja dostępu do drukarek

Można też śledzić dostęp do drukarek, aby monitorować dostęp użytkowników do kosztownych w utrzymaniu urządzeń. Aby prowadzić inspekcję drukarek, należy:

- Skonfigurować zasady inspekcji do prowadzenia inspekcji dostępu do obiektów, w tym do drukarek.
- Włączyć inspekcję wybranych drukarek oraz wskazać typ zdarzeń do inspekcji.

Przy określaniu ustawień inspekcji drukarek, można korzystać z poniższych wskazówek:

- Rejestrować niepowodzenie operacji Print na zastrzeżonych drukarkach, takich jak wykorzystywane do wydruku faktur.
- Rejestrować zakończone sukcesem i niepowodzeniem operacje Full Control, w celu aktualizacji dzienników, gdy na drukarce wykonywane są zadania administratorskie.
- Rejestrować zakończone sukcesem operacje Delete, wykonywane na drukarkach ogólnodostępnych, w celu sprawdzenia, czy niekompletny wydruk bądź usunięcie zadania drukowania nastąpiło w wyniku działań administratorskich, czy błędu sprzętu.
- Rejestrować zakończone sukcesem operacje Change Permissions i Take Ownership na zastrzeżonych drukarkach. Pozwala to na rejestrację działań administratorskich, w celu późniejszej konsultacji przy rozbieżnościach w ocenie stanu bezpieczeństwa.

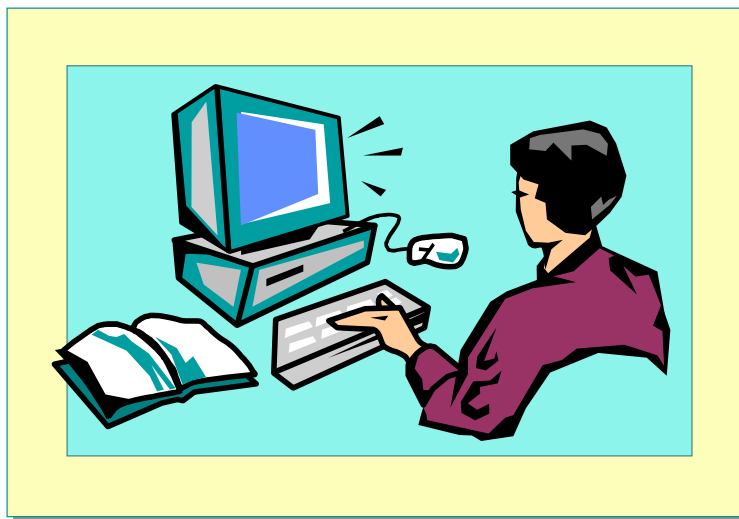
Laboratorium B: Konfigurowanie inspekcji

Cel slajdu

Omówienie laboratorium.

Wprowadzenie

W tym laboratorium zostaną zaplanowane zasady inspekcji, skonfigurowane ustawienia inspekcji, przygotowane ustawienia inspekcji plików i drukarek oraz utworzony i przejrany dziennik zabezpieczeń.



Wyjaśnij cel laboratorium.

Cele laboratorium

Po zrealizowaniu tego laboratorium słuchacz będzie potrafił:

- Zaplanować zasady inspekcji.
- Skonfigurować ustawienia inspekcji.
- Przygotować inspekcję plików i drukarek.
- Przeglądać wpisy w dzienniku zabezpieczeń.

Wymagania wstępne

Przed rozpoczęciem tego laboratorium należy:

- Zapoznać się z typami ustawień inspekcji, dostępnymi w systemie Windows 2000.
- Zapoznać się z przypisywaniem uprawnień do plików i drukarek.
- Zapoznać się ze sposobami konfiguracji drukarek.

Przygotowanie laboratorium

Do wykonania tego laboratorium niezbędne są:

- Komputer pracujący w systemie Windows 2000 Advanced Server, skonfigurowany jako serwer członkowski w domenie nwtraders.msft.
- Konto użytkownika Adminx (gdzie x jest numerem stanowiska).
- Drukarka nazwana jako Color Printer.
- Folder C:\MOC\Win2152b\Labfiles\Lab09, który zawiera plik Bronte.txt.

Przewidywany czas ukończenia laboratorium: 30 minut

Ćwiczenie 1

Planowanie zasad inspekcji

Scenariusz

Twoja firma właśnie zakończyła wewnętrzny przegląd zabezpieczeń i wdrożyła, w oparciu o wyniki przeglądu, kilkanaście zasad zabezpieczeń. Aby sprawdzić, że wdrożone zabezpieczenia zapewnią wymagany poziom bezpieczeństwa, zaplanowałeś prowadzenie inspekcji. Założenia inspekcji obejmują:

- Rejestrację nieudanych prób dostępu do sieci.
- Rejestrację nieautoryzowanego dostępu do plików tworzących bazę danych klientów.
- Monitorowanie wykorzystania kolorowej drukarki, przeznaczonej do drukowania rachunków.
- Monitorowanie prób zmian konfiguracji sprzętowej serwera.
- Rejestrację działań administratorskich, prowadzonych w celu śledzenia nieautoryzowanych zmian.

Cel

Przed przypisaniem ustawień inspekcji do zasobów serwera, musisz opisać konfigurację zasad inspekcji, określając:

- Typ zdarzeń przeznaczonych do inspekcji.
- Czy inspekcji będą podlegały operacje zakończone sukcesem, niepowodzeniem lub wszystkim.

W poniższej tabeli wprowadź swoje propozycje ustawień inspekcji, które będą odpowiadały scenariuszowi.

Operacje przeznaczone do inspekcji	Sukces	Niepowodzenie
Zdarzenia Account Logon	☐	☐
Account management	☐	☐
Directory service access	☐	☐
Zdarzenia Logon	☐	☐
Object access	☐	☐
Policy change	☐	☐
Privilege use	☐	☐
Process tracking	☐	☐
Zdarzenia System	☐	☐

Zadania	Szczegółowe kroki
	❓ Upewnij się, że Twoje propozycje, zawarte w powyższej tabeli, odpowiadają odpowiedziom przedstawionym przez prowadzącego zajęcia. Wymień poprawne odpowiedzi, jeśli jest to konieczne. Account Logon: Niepowodzenie (dla prób dostępu do sieci). Account management: Sukces (dla operacji administratorskich). Directory service access: Brak ustawień. Logon: Niepowodzenie (dla prób dostępu do sieci). Object access: Sukces (dla użycia drukarki), i Niepowodzenie (dla nieautoryzowanego dostępu). Policy change: Sukces (dla operacji administratorskich). Priveledge use: Sukces (dla operacji administratorskich i procedur archiwizacji). Process tracking: Brak ustawień. Zdarzenia System: Sukces i Niepowodzenie (dla prób włamania do serwera).

Ćwiczenie 2

Konfigurowanie ustawień inspekcji

Scenariusz

Po określeniu firmowych zasad inspekcji, powinieneś skonfigurować serwer poprzez zastosowanie dla niego odpowiednich zasad inspekcji.

Cel

W tym ćwiczeniu skonfigurujesz i zastosujesz zasady inspekcji dla swojego komputera.

Zadania	Szczegółowe kroki
1. Zaloguj się do domeny nwtraders.msft jako Adminx (gdzie x jest numerem Twojego stanowiska) z hasłem domain. Wykorzystaj konsolę Computer Management do skonfigurowania zasad inspekcji, odpowiadających Twoim zasadom zabezpieczeń.	a. Zaloguj się, wykorzystując następujące informacje: User name: Adminx (gdzie x jest numerem Twojego stanowiska) Password: domain Log on to: nwtraders b. Z menu Administrative Tools otwórz konsolę Local Security Policy. c. W drzewie konsoli rozwiń Local Policies i wybierz Audit Policy. d. W oknie szczegółów konsoli wybierz każdy z atrybutów inspekcji i w oknie Local Security Policy Setting zaznacz pole opcji Success lub Failure, zgodnie z poniższą listą. • Audit account logon event – Brak inspekcji • Audit account management - Success • Audit directory service acces – Brak inspekcji • Audit logon events - Failure • Audit object acces – Success, Failure • Audit policy change - Success • Audit priveledge use - Success • Audit process tracking – Brak inspekcji • Audit system events – Success, Failure
2. Wymuś natychmiastowe odświeżenie zasad zabezpieczeń dla komputera.	a. W wierszu poleceń wpisz runas /user:nwtraders.msft\adminx "secedit /refreshpolicy machine_policy" (gdzie x jest numerem Twojego stanowiska). b. Wciśnij klawisz ENTER, wpisz domain i ponownie wciśnij klawisz ENTER.  Zostanie wyświetlony komunikat wskazujący na odświeżanie zasad zabezpieczeń dla komputera. c. Zamknij okno wiersza poleceń i konsolę Local Security Settings.

Ćwiczenie 3

Ustanawianie inspekcji plików i drukarek

Scenariusz

Twój komputer został przygotowany zgodnie z firmowymi zasadami inspekcji. Należy teraz skonfigurować właściwości inspekcji dla tych plików i drukarek, dla których chcesz rejestrować zdarzenia.

Cel

Skonfigurujesz ustawienia inspekcji i zmodyfikujesz uprawnienia do pliku. Następnie skonfigurujesz ustawienia inspekcji dla drukarki Color Printer.

Zadania	Szczegółowe kroki
1. Ustanowisz inspekcję dla pliku Bronte.txt, umieszczonego w folderze C:\MOC\Win2152b\Labfiles\Lab09. Monitoruj następujące rodzaje dostępu dla wszystkich użytkowników: • Create Files / Write Data • Delete • Change Permissions • Take Ownership	a. W programie Windows Explorer przejdź do folderu C:\MOC\Win2152b\Labfiles\Lab09 i wyświetl okno Properties pliku Bronte.txt. b. W oknie Bronte Properties, na karcie Security wybierz przycisk Advanced. c. W oknie Access Control Settings for Bronte, na karcie Auditing wybierz przycisk Add. d. W oknie Select User, Computer, or Group upewnij się, że w polu Look in znajduje się wpis nwtraders.msft; na liście Name wskaż Everyone, a następnie wybierz przycisk OK. e. W oknie Auditing Entry for Bronte zaznacz pola opcji Successful i Failed dla każdego z poniższych typów dostępu: • Create Files / Write Data • Delete • Change Permissions • Take Ownership f. Wybierz przycisk OK, aby zamknąć okno Auditing Entry for Bronte i ponownie przycisk OK, aby zamknąć okno Access Control Settings for Bronte.  <i>Zwróć uwagę, że nazwa grupy Everyone widnieje na liście Auditing Entries.</i>
2. Zmień uprawnienia do pliku Bronte.txt na Read dla grupy Everyone.	a. W oknie Bronte Properties, na karcie Security usuń zaznaczenie pola opcji Allow inheritable permissions from parent to propagate to this object i po wyświetleniu okna komunikatu wybierz przycisk Copy. b. W oknie Bronte Properties przypisz grupie Everyone uprawnienie Read (jako jedyne uprawnienie). c. Wybierz przycisk OK, aby zamknąć okno Bronte Properties, a następnie zamknij okno programu Windows Explorer.

(ciąg dalszy)

Zadania	Kolejne kroki
3. Skonfiguruj inspekcję drukarki Color Printer, aby rejestrować wszystkie wydruki.	a. Rozwiń menu Start, wskaż Settings, a następnie Printers. b. Wyświetl okno Properties dla drukarki Color Printer. c. Na karcie Security wybierz przycisk Advanced. d. W oknie Access Control Settings for Color Printer, na karcie Auditing wybierz przycisk Add. e. W oknie Select User, Computer, or Group na liście Name wskaż Everyone, a następnie wybierz przycisk OK. f. W oknie Auditing Entry for Color Printer zaznacz pola opcji Successful dla wszystkich typów dostępu, a następnie wybierz przycisk OK.  <i>Zwróć uwagę, że nazwa grupy Everyone widnieje na liście Auditing Entries.</i> g. Wybierz przycisk OK, aby zamknąć okno Access Control Settings for Color Printer. h. Wybierz przycisk OK, aby zamknąć okno Color Printer Properties, a następnie zamknij okno folderu systemowego Printers.

Ćwiczenie 4

Tworzenie i przeglądanie wpisów dziennika zabezpieczeń

Scenariusz

Twój komputer został skonfigurowany zgodnie z firmowymi zasadami bezpieczeństwa, inspekcja została ustanowiona dla plików i drukarek. Sprawdzisz czy działania, które chcesz monitorować są rejestrowane, przeprowadzając te operacje i obserwując efekty.

Cel

Wyczyścisz dziennik zabezpieczeń swojego komputera. Następnie wygenerujesz zdarzenia na swoim komputerze, uzyskując dostęp do obiektów przeznaczonych do inspekcji i modyfikując ich właściwości. Przeglądniesz dziennik zabezpieczeń swojego komputera, aby sprawdzić, które zdarzenia są rejestrowane.

Zadania	Kolejne kroki
1. Wyczyść dziennik zabezpieczeń swojego komputera.	- Z menu Administrative Tools uruchom program Event Viewer. - W drzewie konsoli, wskaż prawym przyciskiem myszy Security Log i z menu podręcznego wybierz polecenie Clear all Events. - W oknie komunikatu Event Viewer wybierz przycisk No i zamknij konsolę Event Viewer.
2. Utwórz wpis w dzienniku komputera lokalnego, przeglądając zawartość pliku Bronte.txt i próbując dokonać w nim zmian.	- W oknie programu Windows Explorer przejdź do folderu C:\MOC\Win2152b\Labfiles\Lab09, otwórz plik Bronte.txt i zamknij go bez modyfikacji jego zawartości. - Otwórz ponownie plik Bronte.txt, zmodyfikuj zawartość pliku i spróbuj zapisać zmiany. - Zamknij plik bez zapisywania zmian i zamknij okno programu Windows Explorer.
3. Utwórz wpis w dzienniku komputera lokalnego, zmieniając priorytet drukarki Color Printer.	- Otwórz menu Start wskaż Settings i wybierz Printers. - Otwórz okno Properties dla drukarki Color Printer. - Na karcie Advanced w polu Priority wpisz 9 i wybierz przycisk OK. - Zamknij folder Printers.
4. Utwórz wpis w dzienniku komputera lokalnego, uruchamiając go ponownie i próbując zalogować się z błędnym hasłem lub na nieistniejące konto użytkownika. Następnie zaloguj się do domeny nwtraders.msft jako Adminx (gdzie x jest numerem Twojego stanowiska) z hasłem domain i ponownie uruchom komputer.	- Ponownie uruchom komputer. - Spróbuj zalogować się, wykorzystując następujące informacje: User name: Starter Password: domain Log on to: nwtraders - Spróbuj zalogować się, wykorzystując następujące informacje: User name: Administrator Password: Windows Log on to: <i>Server</i> (gdzie <i>Server</i> jest nazwą Twojego komputera) - Zaloguj się, wykorzystując następujące informacje: User name: Adminx (gdzie x jest numerem Twojego stanowiska) Password: domain Log on to: nwtraders - Uruchom ponownie komputer.

(ciąg dalszy)

Zadania	Kolejne kroki
5. Zaloguj się do domeny nwtraders.msft jako Adminx (gdzie x jest numerem Twojego stanowiska) z hasłem domain i przejrzyj dziennik zabezpieczeń Twojego komputera, analizując zdarzenia powstałe w wyniku Twojej działalności.	a. Zaloguj się, wykorzystując następujące informacje User name: Adminx (gdzie x jest numerem Twojego stanowiska) Password: domain Log on to: nwtraders b. Z menu Administrative Tools otwórz program Event Viewer. c. W drzewie konsoli wybierz dziennik Security Log. d. Przejrzyj dziennik, wykorzystując polecenia Filter i Find z menu View, aby odpowiedzieć na poniższe pytania:
? Czy zdarzenia Logon/Logoff zostały zarejestrowane? Jeśli tak, to czy te zakończone sukcesem, czy niepowodzeniem? Tak. Zdarzenia zakończone niepowodzeniem zostały zarejestrowane.	
? Czy zdarzenia ObjectAccess zostały zarejestrowane dla pliku Bronte.txt? Jeśli tak, to czy te zakończone sukcesem czy niepowodzeniem? Tak. Zdarzenia zakończone niepowodzeniem zostały zarejestrowane.	
? Czy zdarzenia ObjectAccess zostały zarejestrowane dla drukarki Color Printer? Jeśli tak, to czy te zakończone sukcesem czy niepowodzeniem? Tak. Zdarzenia zakończone sukcesem zostały zarejestrowane.	

(ciąg dalszy)

Zadania	Kolejne kroki
 Czy zdarzenia PrivilegeUse zostały zarejestrowane? Jeśli tak, to czy te zakończone sukcesem czy niepowodzeniem? Tak. Zamknięcia systemu zakończone sukcesem zostały zarejestrowane.	
5. (ciąg dalszy)	e. Zamknij okno konsoli Event Viewer i wyloguj się.

Podsumowanie

Cel slajdu

Podsumowanie celów rozdziału poprzez przypomnienie zagadnień kluczowych.

Wprowadzenie

Pytania podsumowujące dotyczą głównych tematów omówionych w rozdziale.

- Zabezpieczanie pulpitów i usług przy wykorzystaniu zasad zabezpieczeń
- Inspekcja dostępu do zasobów systemowych

1. W przedsiębiorstwie poproszono Administratora o zabezpieczenie wybranych komputerów w sieci. Jakiego narzędzia należy użyć, aby w najprostszy sposób wprowadzić ustawienia zabezpieczeń na tych komputerach?

Security Configuration and Analysis.

2. Administrator chciałby zabezpieczyć komputer z systemem Windows 2000 Professional. Chce wykorzystać w tym celu najbezpieczniejszą metodę, ale bez tworzenia nowego szablonu. W jaki sposób może to osiągnąć?

W konsoli Security Configuration and Analysis, importując predefiniowany szablon zabezpieczeń dla wysokiego poziomu bezpieczeństwa stacji roboczej lub serwera (hisecls.inf).

3. Istnieje podejrzenie, że pracownik nocnej zmiany próbuje, logując się do komputera sekretarki, uzyskać dostęp do tajnych danych. W jaki sposób należy wdrożyć zasady inspekcji i jakie zdarzenia monitorować?

Należy skonfigurować inspekcję na komputerze sekretarki i monitorować zarówno udane jak i nieudane próby logowania.

4. Użytkownik próbuje ustanowić inspekcję folderu na swoim komputerze, ale gdy usiłuje obejrzeć ustawienia kontroli dostępu Access Control, karta **Audit** nie jest widoczna. Dlaczego?

Aby karta Audit była widoczna, wymagany jest system plików NTFS, a użytkownik musi mieć prawa administratorskie dla lokalnego komputera.

