#### T: Inspekcja dostępu do zasobów systemowych.

## Przed implementacją zasad inspekcji utwórz plan inspekcji.

- Zdecyduj, jaki rodzaj informacji ma być uzyskiwany przez zbieranie zdarzeń inspekcji:
  - Przy wykrywaniu włamań śledzeniu prób uzyskania dostępu przez użytkowników do obszarów, do których nie mają oni uprawnień można prowadzić inspekcję niepowodzeń. Włączenie inspekcji niepowodzeń może jednak stwarzać zagrożenie dla organizacji. Jeśli użytkownicy próbują uzyskać dostęp do zasobu, do którego nie mają uprawnień, mogą utworzyć tyle zdarzeń, że dziennik zabezpieczeń zapełni się i komputer nie będzie mógł zbierać więcej informacji o inspekcji. Gdy jest włączone ustawienie zasad Inspekcja: zamknij system natychmiast, jeśli nie można rejestrować wyników inspekcji, użytkownicy mogą przeprowadzić atak typu "odmowa usługi".
  - W przypadku działań śledczych określania za pomocą dziennika inspekcji, co dokładnie dzieje się w organizacji można dokonywać inspekcji sukcesów i niepowodzeń.
- Należy rozważyć zasoby dostępne do zbierania i przeglądania dziennika inspekcji. Zdarzenia inspekcji zajmują miejsce na komputerach, zabierają także czas administratora i pracowników organizacji. Nie należy dokonywać inspekcji zdarzeń, które faktycznie nie stanowią obiektu zainteresowania.

#### Zadanie1:

Zapoznaj się z informacjami publikowanymi na stronie http://technet2.microsoft.com/windowsserver/pl/library/5658fae8-985f-48cc-b1bf-bd47dc2109161045.mspx?mfr=true

Inspekcja jest elementem stosowanym w serwerach Windows od dawna. Jednak poprzednio administrator musiał ją włączyć ręcznie. Ze względów bezpieczeństwa w Windows Server 2003 inspekcja jest włączona domyślnie. Oznacza to, że w dzienniku Zabezpieczenia zaraz po zakończeniu instalacji pojawiają się wpisy związane z działaniem użytkowników. Dzięki temu pewne poczynania są odnotowywane od samego początku pracy serwera. Instalacja systemu operacyjnego uruchamia samoczynnie tylko część zasad inspekcji. Jeśli dodatkowo chcemy wiedzieć, jak eksploatowane są zasoby albo kto bezskutecznie usiłował się podłączyć do serwera, musimy włączyć te działania audytu. W tym celu wybieramy Start | Narzędzia administracyjne | Zasady zabezpieczeń kontrolera domeny i zmieniamy parametry folderu Ustawienia zabezpieczeń | Zasady lokalne | Zasady inspekcji. W zależności od tego, co chcemy obserwować, należy dwukrotnie kliknąć odpowiednią opcję. We właściwościach zaznaczamy Definiuj następujące ustawienia zasad i wybieramy Sukces lub Niepowodzenie. Naturalnie podczas uruchamiania zasad musimy wiedzieć, jaki typ zdarzenia nas interesuje. W niektórych przypadkach bardziej uzasadnione jest obserwowanie prób zakończonych sukcesem, np. inspekcja zmian zasad. Niekiedy warto odnotowywać niepowodzenia, np. nieudane próby logowania. W razie potrzeby możemy przenosić do dziennika informacje zarówno o sukcesach, jak i o niepowodzeniach.

Uruchomienie audytu po zaznaczeniu sukcesu lub niepowodzenia powoduje zapisywanie informacji w Poglądzie zdarzeń. Od tej reguły są wyjątki. Jeśli chcemy śledzić dostęp do zasobów serwera lub Active Directory, samo włączenie zasad inspekcji nie wystarcza. Dodatkowo musimy poinformować system, jakie zasoby ma monitorować. Oprócz źródła danych należy jeszcze określić, kogo i w jakim zakresie monitorujemy. Możemy włączyć na przykład monitorowanie dostępu do pliku cmd.exe (źródło) przez użytkowników z grupy Wszyscy, na poziomie powodzenia i niepowodzenia prób wykonywania (uruchomiania), usuwania lub zmiany uprawnień. Parametry te określamy we właściwościach zasobu, w wypadku plików wybieramy Właściwości | Zabezpieczenia | Zaawansowane | Inspekcja. W celu włączenia audytu Rejestru uruchamiamy edytor Regedit.exe. Następnie zaznaczamy gałąź lub klucz, który chcemy obserwować, i z menu wybieramy Edycja | Uprawnienia | Zabezpieczenia | Zaawansowane | Inspekcja i dodajemy określone obiekty. Ustawienia monitorowania drukarek przebiegają dość podobnie. Otwieramy folder Drukarki i faksy, zaznaczamy odpowiednią drukarkę i z menu wybieramy Właściwości. Na koniec w znany już sposób przechodzimy przez kartę Zabezpieczenia | Zaawansowane | Inspekcja. Nieco więcej kłopotu przysparza ustawienie audytu w obiektach usługi Active Directory. Uruchamiamy przystawkę Użytkownicy i komputery usługi Active Directory. Ponieważ domyślnie karta Zabezpieczenia jest ukryta, aby dostać się do inspekcji, musimy najpierw zaznaczyć Opcje zaawansowane w menu Widok. Dalej wszystko pójdzie jak z płatka. Zaznaczamy domenę, obiekt lub jednostkę organizacyjną i przechodzimy przez Zabezpieczenia | Zaawansowane | Inspekcja.

Audyt związany z folderami i plikami jest możliwy wyłącznie w systemie plików NTFS. Konfiguracja inspekcji dostępu do obiektów oraz do usługi katalogowej powinna być gruntownie przemyślana.

Tomasz Greszata

- Koszalin 2012 -

http://greszata.pl

Uruchomienie obserwacji zbyt wielu obiektów może generować dużo zdarzeń i zmniejszyć wydajność systemu. Interpretacja zdarzeń inspekcji i wyszukanie interesujących informacji może być kłopotliwe. W przypadku trudności z interpretacją zdarzenia warto sięgnąć do opublikowanego na stronach Microsoftu dokumentu: Windows Server 2003 Security Guide. Natomiast podczas wyszukiwania pamiętajmy o dostępnych w Poglądzie zdarzeń filtrach oraz opcji Znajdź. Dzięki nim szybko odnajdziemy istotne informacje. Jeśli zdarzeń jest naprawdę wiele, zawartość dziennika można wyeksportować do pliku tekstowego (TXT) lub rozdzielanego przecinkami (CSV), a następnie zaimportować do dowolnego arkusza lub bazy danych.

Najważniejszym zaleceniem przed fizyczną konfiguracją zasad inspekcji jest określenie zakresu monitorowania. W wypadku narażonych na niebezpieczeństwo serwerów inspekcja powinna dotyczyć przede wszystkim zasad: logowania (sukces, niepowodzenie), zarządzania kontami (sukces, niepowodzenie), zmiany zasad (sukces, niepowodzenie), zdarzeń systemowych (sukces, niepowodzenie), użycia uprawnień (niepowodzenie) i części plików systemowych (niepowodzenie).

W celu włączenia monitorowania wskazanych zasad po kolei klikamy Start | Narzędzia administracyjne| Zasady zabezpieczeń kontrolera domeny | Ustawienia zabezpieczeń | Zasady lokalne | Zasady inspekcji. Tutaj rozpoczynamy od dwukrotnego kliknięcia opcji Przeprowadź inspekcję dostępu do obiektów, następnie zaznaczamy Definiuj następujące ustawienia zasad oraz Sukces i Niepowodzenie. W ten sposób konfigurujemy zalecane wyżej ustawienia lub te, które nam najbardziej odpowiadają. Po zamknięciu przystawki możemy jeszcze odświeżyć zasady poleceniem wiersza poleceń gpudate.

#### Zadanie2:

Wykorzystując narzędzia do edycji zabezpieczeń Zasady grupy oraz sprawdzania zabezpieczeń systemu plików skonfiguruj następujące ustawienia inspekcji:

- Przeprowadź inspekcję zdarzeń logowania dla Sukcesu i Niepowodzenia.
- Przeprowadź inspekcję zarządzania kontami dla Sukcesu i Niepowodzenia.
- Przeprowadź inspekcję dostępu do obiektów dla Niepowodzenia.

Następnie dokonaj takich działań w systemie, które spowodują zapisanie zdarzeń dotyczących konta Administratora, konta Gościa oraz programu cmd.exe. Gdzie odszukasz informacji na temat tych zdarzeń? Opisz w zeszycie działania rozwiązujące powyższe zadanie.

#### Uwaga:

W ramach pomocy posłuż się dostępną w systemie Windows Pomocą i obsługą techniczną podając jako kryterium wyszukiwania "Opisy ustawień zabezpieczeń".

Konfiguracja zasad grupy dotyczących zasad inspekcji:

🚰 Zasady grupy			
Plik Akcja Widok Pomoc			
🛐 Zasady Komputer lokalny	Zasady 🔺	Ustawienie zabezpieczeń	
🖻 🌆 Konfiguracja komputera	🐯 Przeprowadź inspekcję dostępu do obiektów	Niepowodzenie	
I Istawienia oprogramowania	🕮 Przeprowadź inspekcję dostępu do usługi katalogowej	Niepowodzenie	
Ustawienia systemu windows	👸 Przeprowadź inspekcję śledzenia procesów	Brak inspekcji	
E Strawienia zabeznieczeń	👸 Przeprowadź inspekcję użycia uprawnień	Niepowodzenie	
The Constant and C	👸 Przeprowadź inspekcję zarządzania kontami	Sukces, Niepowodzenie	
Zasady lokalne	👸 Przeprowadź inspekcję zdarzeń logowania	Sukces, Niepowodzenie	
庄 🔂 Zasady inspekcji	Przeprowadź inspekcję zdarzeń logowania na kontach	Sukces, Niepowodzenie	
🕀 🧰 Przypisywanie praw użytkownika	Przeprowadź inspekcję zdarzeń systemowych	Brak inspekcji	
🕀 🧰 Opcje zabezpieczeń	Przeprowadź inspekcję zmian zasad	Sukces, Niepowodzenie	
🗈 📄 Zasady kluczy publicznych	Właściwości: Przeprowadź inspekcję dostępu do obiektó	w ?×	
I III Zasady ograniczeń oprogramowania	Listawianie zabeznieczeń lokalnuch		
E Sashlopu administracuino		1	
Finizia Szabiony administracyjne	Przeprowadź inspekcję dostępu do obiektów		
I Ustawienia systemu Windows			
🗄 🛅 Szablony administracyjne			
	Dokonuj inspekcji tych prób:		
	🔲 Sukces		
	Vienowodzenie		
1			

Tomasz Greszata

- Koszalin 2012 -

### Konfiguracja zasad inspekcji dla zasobów dyskowych:

Właściwości: exctrlst.exe 2	Zaawansowane	e ustawienia zabe	zpieczeń dla exctrlst.exe	<u>?</u> ×
Ogólne   Wersja   Zgodność   Zabezpieczenia   Pod Nazwy grupy lub użytkownika:	Uprawnienia Aby wyświetlia	Inspekcja   Właścio ć więcej informacji na	iel Czynne uprawnienia   temat specjalnych wpisów inspekcji, zaznacz wpis inspekcji, a	
Administratorzy (BIELEK\Administratorzy) SYSTEM	następnie klik Wpisy inspeki	nij przycisk Edytuj. cji:		
🐼 Użytkownicy (BIELEK\Użytkownicy)	Typ Wszystko	Nazwa Wszyscy	Dostęp Odziedziczone po Przechodzenie <nie odziedziczone=""></nie>	
Vpis inspekcji dla exctrlst.exe		? ×		
Obiekt Nazwa: Wszyscy Zastosuj dla: Tylko ten obiekt Dostęp:	Powodzenie	Zmień		Þ
Pełna kontrola Przechodzenie przez folder/Wykonywanie pliku Wyświetlanie zawartości folderu/Odczyt danych Odczyt atrybutów Odczyt atrybutów rozszerzonych Tworzenie plików/Zapis danych Tworzenie folderów/Dołączanie danych Zapis atrybutów			ym wpisy inspekcji stosowane do obiektów podrzędnych. Uwzględn anymi	ii je
Zapis atrybutów rozszerzonych			OK Anuluj Zasto	osuj

# Odczyt wpisów w dzienniku systemowym dotyczących inspekcji:

🔜 Zarządzanie komputerem			Właściwości: Zdarzenie				? ×	
具 Plik Akcja Widok Okno	Pomoc		Zdarzenie					
	) <b>E</b>		Data:	2009-10-19	Źródło:	Security	•	
📃 Zarządzanie komputerem (loka	Тур	Data	Godzina:	07:39:27	Kategoria:	Wykorzystanie przywilejó		
🖻 🌇 Narzędzia systemowe	💰 Inspekcja sukcesów	2009-10-19	Тур:	Inspekcja	Identyfikator		+	
Podgląd zdarzeń	矿 Inspekcja sukcesów	2009-10-19			zdarzenia:	577		
Antivirus	矿 Inspekcja sukcesów	2009-10-19	Użytkowni	k: BIELEK\tom	ek			
Aplikacja	💕 Inspekcja sukcesów	2009-10-19	Komputer:	BIELEK				
	🕑 Inspekcja sukcesów	2009-10-19	Opis:					
System	💰 Inspekcja sukcesów -	2009-10-19	Wywołan	a uprzywilejowa	na usługa:			
E Poldery udostępnione	2009-10-19							
🕀 🔬 Użytkownicy i grupy lo	🖥 Inspekcja niepow	2009-10-19		Podstawowa na	azwa użytkowr	nika: tomek		
🕀 🐺 Dzienniki wydajności i 🗤	矿 Inspekcja sukcesów -	2009-10-19		Podstawowa do	omena: BIELEI			
🔜 Menedżer urządzeń	矿 Inspekcja sukcesów	2009-10-19		Podstawowy idi Nazwa użutkow	entyrikator logo unika klienta: -	owania: (UXU,UXZUEDB)		
📮 🖆 Magazyn	of Inspekcja sukcesów	2009-10-19	Domena klienta: - Identyfikator logowania klienta: -					
🕀 🙀 Magazyn wymienny	🖬 Inspekcja niepow	2009-10-19						
Defragmentator dyskć	🖬 Inspekcja niepow	2009-10-19	1	Przywileje: SeS	ecurityPrivilege	9	<u> </u>	
Zarządzanie dyskami	🖬 Inspekcja niepow	2009-10-19	Dane: 🙃	Baity 🔿 Słov	va			
⊞~ <b>S</b> Usrugi i aplikacje	🗑 Inspekcja sukcesów	2009-10-19						
	🕤 Inspekcja sukcesów	2009-10-19						
	ogr Inspekcja sukcesów	2009-10-19					<b>_</b>	
	🐨 Inspekcja sukcesów –	2009-10-19						
	•						Zastosui	
							Zastosuj	