XP z zasadami

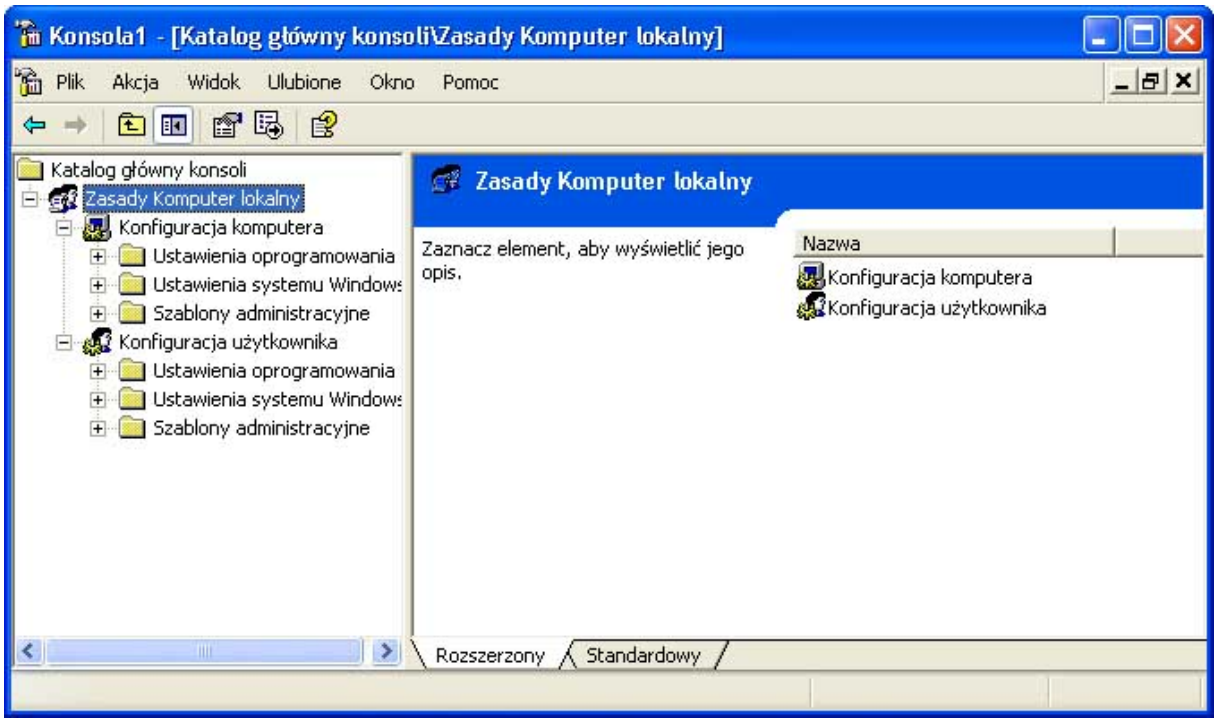
Jacek Ścisławski
PC World Komputer

Każdy wie, jak ważną rolę w zabezpieczeniach komputera odgrywają hasła. Wiadomo również, że - zgodnie ze starym przysłowiem - sprawdzać to znaczy wiedzieć. Administratorzy Windows XP Professional mogą tak skonfigurować system, żeby wymuszał hasła o wysokim poziomie bezpieczeństwa oraz kontrolował dostęp do plików, drukarek czy komputera. Czynności te są możliwe dzięki usłudze Zasady grupy i stanowią jedynie mały fragment jej przebogatych możliwości.

Zabezpieczanie systemu pracującego pod kontrolą Windows XP nie opiera się wyłącznie na przypisaniu skomplikowanego hasła do konta Administratora albo uruchomieniu wbudowanej zapory połączenia internetowego. W zasięgu ręki znajduje się silne narzędzie do kompleksowego konfigurowania ustawień oraz zabezpieczeń systemu. Uruchamiając przystawkę Zasady grupy, przekonujemy się, ile parametrów można ustawić, by zwiększyć funkcjonalność systemu. Z pozoru skomplikowana struktura usługi, po bliższym poznaniu okazuje się całkiem znośna w obsłudze i zarządzaniu.

Na czym polegają Zasady grupy?

Ujmując najprościej, Zasady grupy to zespół ustawień konfigurujących system operacyjny. Ustawienia te dotyczą bardzo szerokiego spektrum parametrów i obejmują między innymi takie elementy, jak ustawienia aplikacji Windows XP, ustawienia zabezpieczeń, ustawienia Pulpitu, ustawienia środowiska systemu i wiele innych.



Konfiguracja komputera i użytkownika z użyciem zasad lokalnych

Po zainstalowaniu Windows XP otrzymujemy produkt gotowy do pracy. Instalator przenosi na system operacyjny ustawienia związane z obiektami w menu Start, parametrami logowania, czy chociażby ustawieniami Eksploratora Windows. Jeśli nie odpowiada nam domyślna konfiguracja, możemy zmodyfikować ustawienia wielu obiektów wchodząc w ich właściwości. Dotyczy to na przykład paska zadań oraz menu Start. Jednak opcje dostępne we właściwościach tych elementów, to jedynie część parametrów, jakie możemy narzucić systemowi. Inne, bardziej zawansowane, są wprowadzane właśnie przez Zasady grupy.

Główna funkcja Zasad grup to ujednolicenie i zabezpieczenie środowiska pracy użytkowników. Dodatkowo dzięki nim można dystrybuować oprogramowanie w sieci oraz wypływać na to, do jakich komponentów Windows użytkownicy będą mieli dostęp. W zależności od miejsca pracy Windows zadania założeń grup mogą się nieco różnić oraz mieć inny rozmiar.

Najlepiej ich wykorzystanie sprawdza się w sieciach pracujących pod kontrolą Windows 2000 Server z zaimplementowaną usługą Active Directory. W takich środowiskach administrator definiuje dla wszystkich stacji jedną zasadę (grupę parametrów), która podczas startu zostanie automatycznie zastosowana do każdego komputera. Podobnie dzieje się z założeniami środowiska pracy użytkowników - jeśli to konieczne, można centralnie wyłączyć np. dostęp do konfiguracji ekranu.

W sieciach bezdomenowych, opartych na grupach roboczych, wdrożenie zasad grup jest nieco utrudnione, ale w pełni możliwe. Kłopot polega na tym, że w sieciach peer-to-peer nie ma wyspecjalizowanego serwera, który by nadzorował dystrybucję ustawień. Rozwiązaniem tego problemu jest zastosowanie pewnej cechy zasad grup, czyli możliwości zapisu zmienianych parametrów w szablonie. Wystarczy wówczas przygotować jeden plik konfiguracyjny, a następnie przyłożyć go do wszystkich komputerów małej sieci.

Duża część ustawień odnosi się do lokalnego środowiska systemu operacyjnego, dlatego znajomość konfiguracji zasad sprawdza się doskonale podczas pracy na indywidualnych stacjach roboczych. Tu zadanie założeń grup koncentruje się głównie na określaniu zabezpieczeń systemu. Tym niemniej można je również zastosować do określania parametrów pracy na tych stacjach, które są wykorzystywane przez wielu użytkowników.

Rodzaje zasad

Ustawienia przypisywane przez zasady mogą być określane na różnych poziomach. Jeśli system pracuje w domenie Windows 2000, zasady grupy są utrzymywane przez usługi katalogowe (Active Directory). Podczas startu Windows XP pobiera je z serwera i wplata w rejestr. Active Directory gromadzą informacje o zasobach sieci, np. komputerach oraz użytkownikach. Ponieważ struktura usługi jest wielopoziomowa, zasady mogą być stosowane do kilku typów obiektów: domen, lokacji i jednostek organizacyjnych. Na przykład przypisanie zasad do domeny powoduje, że są one przenoszone na wszystkie komputery i użytkowników do niej należących.

Koncentrujemy się na zabezpieczeniach Windows XP, który niekoniecznie musi pracować w domenie Windows 2000 lub 2003, ale warto zaznaczyć, że są jeszcze założenia lokalne, przechowywane na każdym komputerze, na którym zostały zdefiniowane. Swoim zasięgiem obejmują wyłącznie parametry własnej stacji i zalogowanego użytkownika. Jeśli komputer

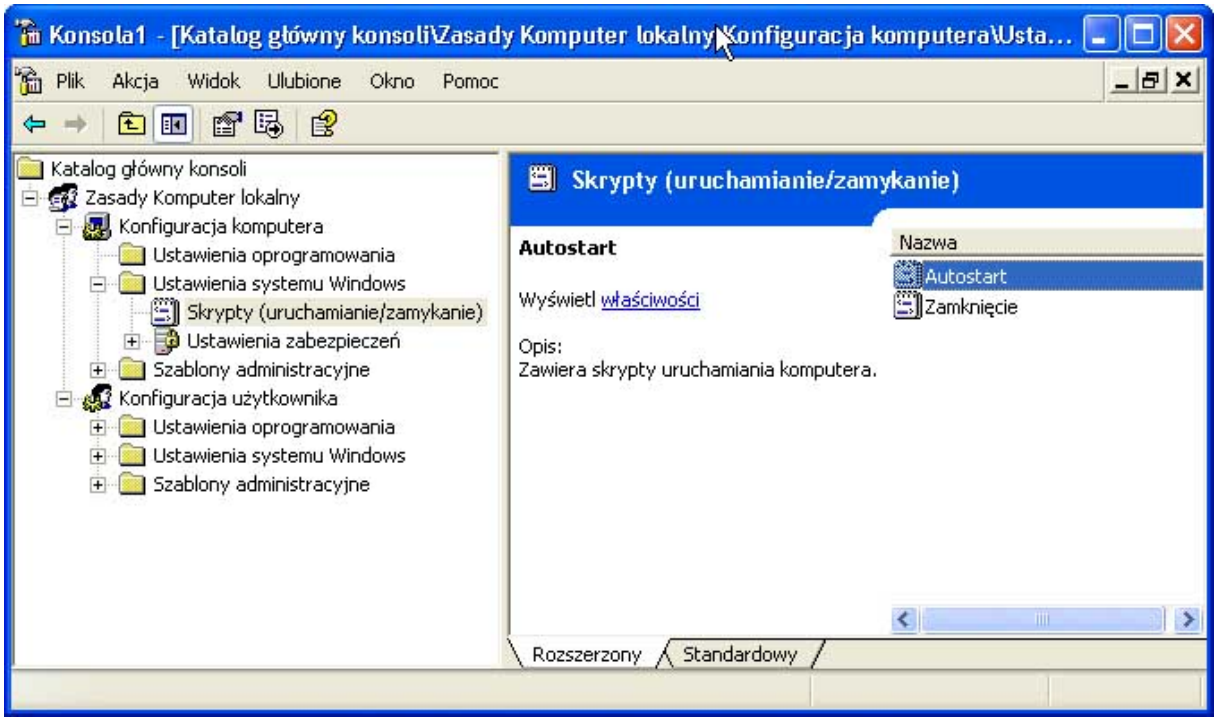
jest podłączony do domeny, wówczas ewentualne ustawienia sieciowe biorą górę i nadpisują ustawienia lokalne. Windows XP przechowuje zasady grupy w rejestrze. Część parametrów zapisana jest w katalogu katalog_systemowy\system32\GroupPolicy. Pobierane stamtąd dane są wtłaczane w rejestr podczas startu komputera lub logowania użytkownika.

Zasady grupy obejmują użytkowników oraz komputery. Każdemu z nich przypisane są niezależne ustawienia, które odnoszą się do poszczególnych elementów systemu. Na przykład dla komputera są to parametry monitorowania, a dla użytkownika ustawienia pulpitu. Podział ten wynika ze sposobu utrzymywania informacji o konfiguracji Windows. Rejestr systemu składa się z kilku oddzielnych części, tzw. gałęzi. Ich lokalizacja obejmuje dwa miejsca: katalog_systemowy\system32\config, oraz lokalny katalog profilu każdego z użytkowników. W profilach zawarte są informacje o indywidualnych preferencjach osób korzystających z Windows, takich jak parametry ekranu, myszy itp. Dlatego też, co innego przechowywane jest w obiekcie Użytkownik zasad grupy, a co innego w obiekcie Komputer. Ustawienia nadane komputerowi są stosowane zawsze, niezależnie od tego, który użytkownik w danej chwili pracuje na stacji. Parametry użytkownika mogą być odmienne dla każdej z osób.

Zanim przejdziemy do przypisywania ustawień konfiguracji zasad komputerowi lub użytkownikowi, należy powiedzieć, kiedy są implementowane. Najpierw - podczas startu Windows XP, zanim pojawi się okno logowania - wprowadzane są ustawienia maszyny. Po uwierzytelnieniu implementowane są zasady konfigurujące środowisko użytkownika.

Co konfigurują zasady?

Struktura Zasad grupy przypomina nieco układ katalogów i plików, gdzie do katalogów można porównać zespoły ustawień obejmujące parametry Windows, a do plików, poszczególne opcje konfiguracyjne. Każdy z obiektów zasad, węzeł użytkownika czy komputera, zawiera trzy foldery: Ustawienia oprogramowania, Ustawienia systemu Windows oraz Szablony administracyjne.



Okno przypisywania plików skryptów

Ustawienia oprogramowania to folder pozwalający na konfigurację dystrybucji oprogramowania w domenach sieci Windows. Przypisanie oprogramowania do folderu Konfiguracja komputera powoduje, że aplikacja będzie dostępna na wszystkich maszynach, do których zastosowano Zasady grupy. Inne znaczenie ma przypisanie aplikacji do konfiguracji użytkownika - oprogramowanie zostanie udostępnione tylko osobom, do których odnosi się zasada. Więcej informacji o dystrybucji oprogramowania można znaleźć w pomocy systemów Windows 2000 Server oraz Windows 2003 Server.

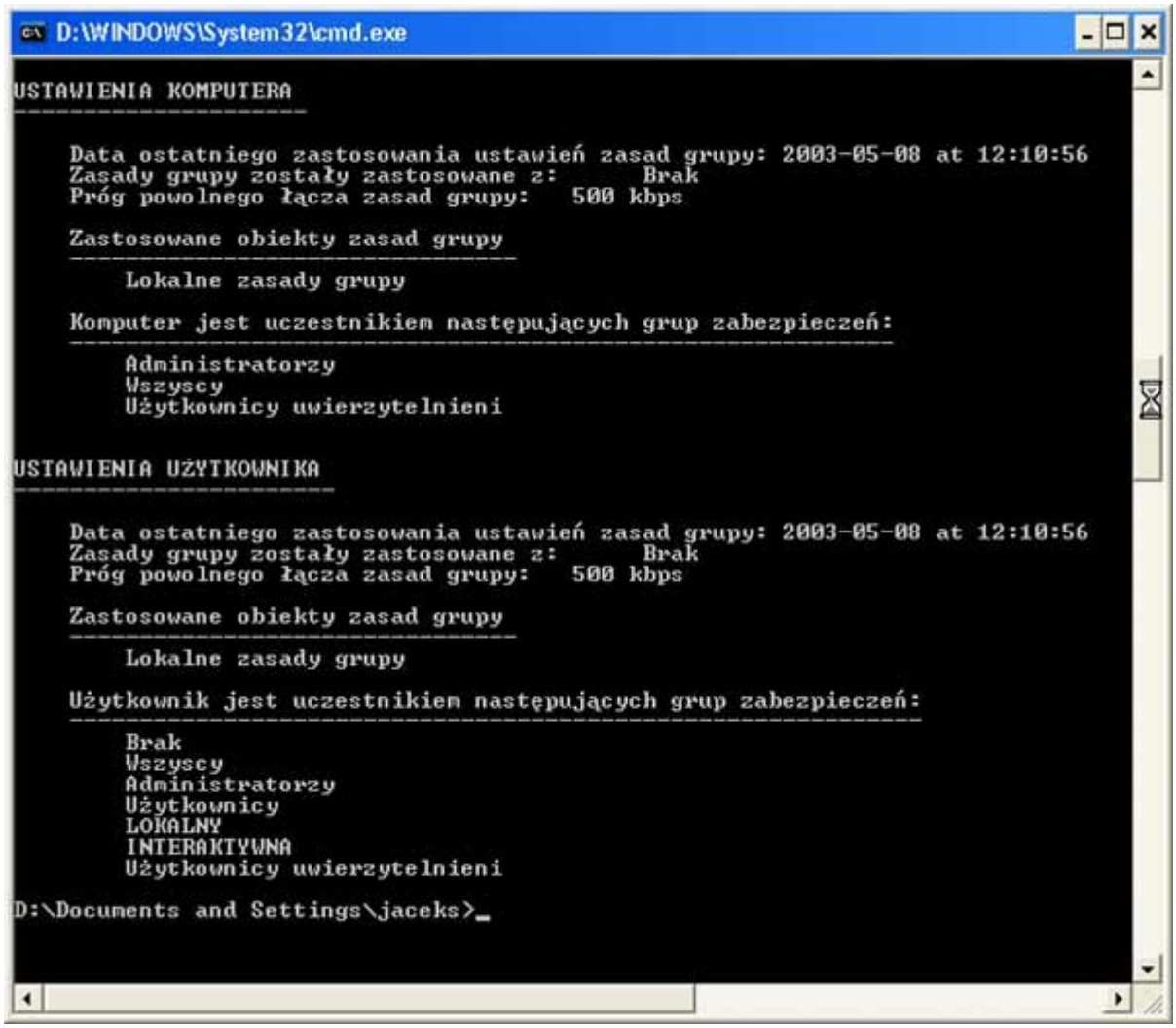
W wypadku zabezpieczeń szczególnie istotne są ustawienia ukryte w folderze Ustawienia systemu Windows. Zasady dotyczące obiektu komputer zawierają dwa elementy: konfiguracje skryptów oraz Ustawienia zabezpieczeń. Jeśli sięgniemy do ikony Skrypty, będziemy mogli przypisać w niej pliki, które mają być uruchamiane podczas startu i zamykania systemu. Analogicznie w części związanej z użytkownikiem można określić pliki wykonywane podczas logowania i wylogowywania z systemu.

Dzięki opcjom dostępnym w Ustawieniach zabezpieczeń można konfigurować ustawienia haseł, ustawienia praw, zasady inspekcji i wiele innych elementów. Szerzej konfiguracja tego folderu zostanie opisana w dalszej części artykułu. W węźle obejmującym konfigurację użytkownika umieszczony został dodatkowo folder Konserwacja programu Internet Explorer. Pozwala on na dostosowanie takich parametrów przeglądarki internetowej, jak opcje połączenia, lista ulubionych witryn czy parametry zabezpieczeń.

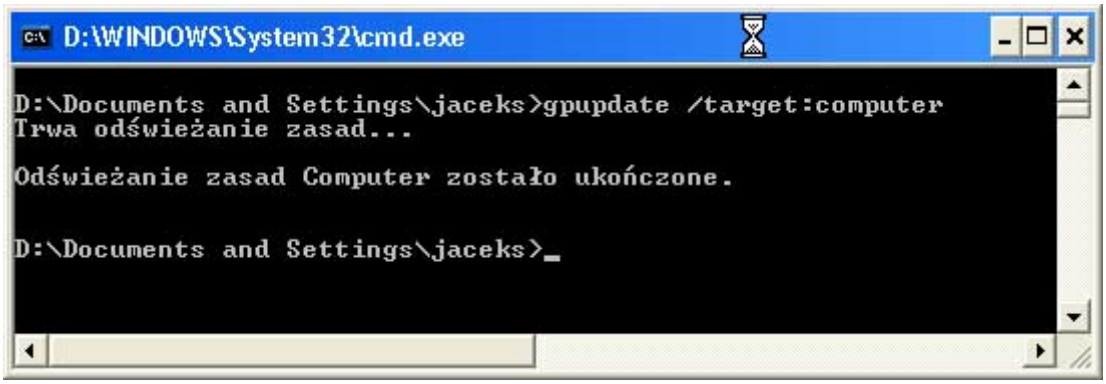
Najwięcej ustawień zawiera folder Szablony administracyjne - opcje bezpośrednio związane ze środowiskiem pracy komputera oraz użytkownika. Dla maszyny będą to parametry modyfikujące Składniki systemu Windows, System, Sieć oraz Drukarki. W części dotyczącej Użytkownika wymienione są grupy: Składniki systemu Windows, menu Start i pasek zadań, pulpit, Panel sterowania, Foldery udostępnione, Sieć i System.

Narzędzia do konfiguracji zasad

Starsze systemy rodziny Windows do konfiguracji odpowiedników zasad grup wykorzystywały narzędzie poledit.exe. Program ten można jeszcze odnaleźć w Windows 2000, ale w Windows XP do konfigurowania zasad grupy służą zupełnie inne narzędzia. Pierwszym i najważniejszym jest przystawka konsoli MMC - Zasady grupy. Pozwala ona na ustawienie wszystkich parametrów zasad, zarówno dla środowiska domenowego, jak i lokalnego. Kolejnym narzędziem są Zasady zabezpieczeń lokalnych. Ta przystawka MMC stanowi jedynie wycinek Zasad grupy, obejmujący zabezpieczenia lokalne komputera. Dodatkowo są do dyspozycji narzędzia wiersza poleceń: gpresult.exe, gpupdate.exe i secedit.exe.



Przykład wykonania polecenia gpresult.exe



Przykład działania polecenia gpupdate.exe

Do konfiguracji zasad najlepiej wykorzystać przystawkę Zasady grupy. Można ją łatwo wywołać, wpisując gpedit.msc w oknie edycji polecenia Uruchom. Innym sposobem jest załadowanie konsoli MMC, wybranie Dodaj/Usuń przystawkę i wskazanie obiektu Zasady grupy.

Po otworzeniu przystawki zobaczysz okno podzielone na dwa panele. Pierwszy z nich (lewy), zawiera ustawienia użytkownika i komputera. Rozwijając poszczególne obiekty (tak jak w Eksploratorze Windows), możesz się poruszać po folderach grupujących odpowiednie opcje. W prawym panelu są poszczególne opcje konfiguracyjne. Na w karcie Wyjaśnij (właściwości obiektu) znajdują się opisy poszczególnych ustawień. Innym sposobem uzyskania pomocy jest wybranie rozszerzonego widoku przystawki MMC. Powoduje to wyświetlenie opisu poszczególnych funkcji bezpośrednio w prawym panelu konsoli.

W przeciwieństwie do przystawki Zasady grupy, która została niejako "ukryta" przed użytkownikami Windows XP, dostęp do Zasad zabezpieczeń lokalnych jest jawny. Aby odnaleźć tę przystawkę, wystarczy otworzyć Narzędzia administracyjne w Panelu sterowania. Po uruchomieniu Zasad zabezpieczeń lokalnych zauważysz pewne podobieństwo do Zasad grupy. Po bliższym przyjrzeniu się przystawce widać, że konsola ta jest jedynie wycinkiem Zasad grupy. Obejmuje on wyłącznie parametry zabezpieczeń obiektu komputer. Jeśli chcesz uruchomić Zasady zabezpieczeń lokalnych poleceniem Uruchom, wpisz secpol.msc.

Konfiguracja poszczególnych opcji

Zasad grupy polega na wprowadzeniu odpowiedniej wartości parametru lub określeniu położenia przełącznika. Aby zmienić ustawienie, kliknij dwukrotnie wybrany obiekt. Dla większości parametrów związanych z zabezpieczeniami wpisuje się żądaną wartość lub wybiera ją z listy. W ten sposób określasz na przykład minimalną liczbę znaków w haśle systemu. Nieco inaczej przebiega zmiana parametrów Szablonów administracyjnych - nadanie ustawień polega na zmianie stanu przełącznika. System daje do wyboru trzy wartości: Włączone, Wyłączone i Nie skonfigurowano. Aby wyjaśnić, do czego służą, posłużmy się przykładem. Wśród ustawień związanych z menu Start i paskiem zadań znajduje się parametr Usuń menu Wyszukaj z menu Start. Jeśli przypiszesz mu wartość Włączone, Wyszukaj zniknie z menu Start, jeśli zaś wybierzesz Wyłączone, powróci ono na swoje miejsce. Ustawienie Nie skonfigurowano można przyjąć za neutralne albo obojętne. Jego zalety najlepiej widać w środowiskach sieciowych, gdzie zasady mogą napływać z wielu poziomów. Jeśli lokalnie zastosujesz Włączone, a dla domeny Wyłączone, opcja Wyszukaj będzie widoczna w menu. Zapewnia to kolejność stosowania zasad, w których ustawienia domenowe

są ważniejsze. Gdyby jednak w zasadach domenowych pozostawić domyślne Nie skonfigurowano, wówczas menu Start byłoby pozbawione polecenia Wyszukaj.

Narzędzia wiersza poleceń

Jeśli chcesz wykonywać część zadań związanych z zasadami grupy poprzez skrypty lub podłączyć się zdalnie do systemu niezbędne ci będą narzędzia wiersza poleceń. Trzy główne narzędzia wiersza poleceń to: gpresult.exe, secedit.exe oraz gpupdate.exe.

Gpresult.exe służący do wyświetlania konfiguracji oraz do generowania wynikowego zestawienia zasad. Zastosowanie Gpresult jest niezmiernie istotne, gdy zasady spływają z wielu źródeł. Możesz wówczas w prosty sposób ustalić, które ustawienia są efektywne.

Na największą uwagę zasługują parametry /v oraz /z narzędzia, zwiększające liczbę wyświetlanych informacji, i parametr /s, dzięki któremu można pobrać informacje z innego komputera.

Secedit.exe jest tekstowym odpowiednikiem przystawki Konfiguracja i analiza zabezpieczeń. Służy do analizowania i przypisywania ustawień zasad zgromadzonych w plikach szablonów. Jeśli zechcesz zastosować szablon, przeanalizować jego użycie czy sprawdzić poprawność składni, wystarczy wpisać secedit.exe z odpowiednim parametrem. Narzędzie sprawdza się najlepiej w zadaniach związanych z nadawaniem zasad na komputerach zdalnych.

Ostatnie z narzędzi - gpupdate.exe - służy do odświeżania zasad przypisanych użytkownikowi lub komputerowi. Domyślnie system automatycznie aktualizuje zmiany nanoszone w założeniach systemowych co określony interwał. Zarówno komputery, jak i użytkownicy mają po 90 minut. Jeśli chcesz, aby zasady odświeżane były szybciej, zmień parametry ustawień Konfiguracja komputera | Szablony administracyjne | System | Zasady grupy | Interwał odświeżania zasad grupy dla komputerów oraz Konfiguracja użytkownika | Szablony administracyjne | System | Zasady grupy | Interwał odświeżania zasad grupy dla użytkowników. Polecenie gpupdate.exe służy do wymuszenia natychmiastowej aktualizacji zasad. Jeśli na przykład dokonasz istotnej aktualizacji ustawień komputera i zechcesz ją jak najszybciej zastosować, wpisz w wierszu poleceń: gpupdate/target:computer. Wydanie polecenia bez parametrów aktualizuje ustawienia dla użytkownika i komputera.

Konfiguracja zabezpieczeń

W systemie niepodłączonym do sieci najważniejszą rolą zasad grup jest wpływanie na ustawienia zabezpieczeń. Po uruchomieniu Lokalnych zasad zabezpieczeń widać pięć obiektów: Zasady konta, Zasady lokalne, Zasady kluczy publicznych, Zasady ograniczeń oprogramowania i Zasady zabezpieczeń IP. W dalszej części szerzej zostaną opisane Zasady konta i Zasady lokalne, natomiast teraz skoncentrujemy się na pozostałych trzech folderach.

W Windows XP Proffesional folder Zasady kluczy publicznych jest związany z systemem szyfrowania plików (EFS). Jeśli dane zostaną zaszyfrowane, nawet kradzież dysku nie pozwala na dostęp do informacji. Zaszyfrowane pliki mogą być otwierane jedynie przez osoby, które je zaszyfrowały, albo przez tzw. agenty odzyskiwania danych. Folder Zasady

kluczy publicznych służy właśnie do określania, które konto w systemie operacyjnym ma pełnić funkcję agenta. W przeciwieństwie do Windows 2000, Windows XP pozwala na szyfrowanie danych nawet wtedy, gdy tych agentów nie ma.

Zasady ograniczeń oprogramowania zabezpieczają system przed uruchamianiem nieuprawnionych programów. Zastosowanie tej funkcji pozwala administratorom określić, które aplikacje użytkownicy mogą uruchamiać na swoich stacjach, a których nie. Dostęp do Internetu wiąże się z poważnym zagrożeniem, automatycznego instalowania i uruchamiania szkodliwych programów, więc ta opcja jest wyjątkowo przydatna. Aplikacje konfiguruje się, stosując określone przez administratora reguły. Więcej na temat zasad ograniczeń oprogramowania można znaleźć w pomocy systemu Windows XP.

Zasady zabezpieczeń IP pozwalają, dzięki zastosowaniu protokołu IPSec, na ochronę informacji przesyłanych przez sieć. Jeśli na przykład jest zagrożenie podsłuchania komunikacji sieciowej, użytkownicy systemów Windows XP mogą zdefiniować odpowiednie reguły weryfikujące integralność lub szyfrujące przesyłane dane. Domyślnie system oferuje trzy rodzaje zasad protokołu IPSec: Klient, Serwer oraz Serwer z zabezpieczeniami. Włączenie jednej z tych opcji nakazuje Windows XP stosować bezpieczną komunikację na odpowiednim poziomie.

Zasady konta

W zabezpieczaniu komputerów niebagatelną rolę odgrywają hasła dostępu. Im mocniejsze hasło, tym trudniej je złamać. Zasady konta przechowywane w Lokalnych zasadach zabezpieczeń pozwalają na skonfigurowanie parametrów związanych z siłą haseł oraz blokowaniem dostępu do stacji.

Przeznaczenie obiektów Ustawień zabezpieczeń

Folder Zasad zabezpieczeń lokalnych	Konfigurowane ustawienia.
Zasady konta	Służą do definowania ustawień haseł, blokady kont oraz parametrów protokołu Kerberos.
Zasady lokalne	Służą do definowania ustawień inspekcji, praw użytkownika oraz opcji zabezpieczeń
Zasady kluczy publicznych	Służą do zarządzania agentami odzyskiwania danych.
Zasady ograniczeń oprogramowania	Służą do kontrolowania możliwości uruchamiania programów na komputerze lokalnym.
Zasady zabezpieczeń IP	Służą do konfigurowania ustawień bezpieczenej komunikacji sieciowej.

Parametry zasad haseł

Parametr	Działanie
Hasło musi spełniać wymagania co do złożoności	Wymusza na użytkownikach stosowanie trudnych haseł.
Maksymalny okres ważności hasła	Określa, ile dni można używać hasła, zanim system będzie wymagał jego zmiany.
Minimalna długość hasła	Określa minimalną liczbę znaków, jaką musi zawierać hasło.
Minimalny okres ważności hasła	Określa, ile dni hasło musi obowiązywać.
Wymuszaj tworzenie historii haseł	Określa liczbę unikatowych haseł.
Zapisz hasła dla wszystkich użytkowników w domenie, korzystając z szyfrowania odwracalnego	Narzuca zapisywanie haseł przy użyciu szyfrowania odwracalnego.

Jeśli chcesz, aby twój komputer wymuszał stosowanie mocnych zasad zabezpieczeń, skorzystaj z opcji dostępnych w Zasadach haseł. Pozwalają one określić: złożoność, długość hasła, okres jego ważności oraz pamiętanie historii haseł. Opcja Hasło musi spełniać

wymagania co do złożoności jest jednym z bardziej istotnych ustawień systemu. Jej włączenie powoduje, że użytkownicy mają obowiązek stosować hasła o wysokim poziomie skomplikowania. Aby system je zaakceptował, wymagane jest spełnienie trzech, czterech warunków: hasło musi zawierać co najmniej jedną wielką literą, małą literę, cyfrę lub znak spoza grupy znaków alfanumerycznych.

Poniżej zasad związanych z hasłami znajdują się zasady blokady konta. Ich ustawienie powoduje, że użytkownicy mają ograniczoną możliwość popełniania błędów podczas logowania. Folder ten zawiera jedynie trzy opcje: czas trwania blokady konta, próg blokady konta oraz czas, po jakim licznik blokady konta ma zostać wyzerowany. Jeśli ustalisz, że próg blokady to trzy pomyłki, a czas w obu wypadkach to 15 minut, użytkownicy logujący się do systemu w ciągu 15 minut będą mogli pomylić się jedynie dwa razy, trzecia pomyłka zakończy się zablokowaniem konta na 15 minut.

Konfigurując zasady konta, należy zachować rozwagę. Jeśli wprowadzisz zbyt restrykcyjne ustawienia, np. czas blokady 999 minut, możesz mieć kłopoty. Aby usunąć restrykcje nałożone na logowanie, należy wejść na konto administratora i we właściwościach zablokowanego użytkownika usunąć zaznaczenie opcji Konto jest zablokowane. Administrator to jedyny użytkownik, którego dostęp do stacji nie jest blokowany nawet po wielu pomyłkach podczas logowania.

Zasady lokalne

Folder Zasady lokalne zawiera kluczowe ustawienia związane z bezpieczeństwem systemu. Oferuje przede wszystkim, możliwość konfiguracji praw użytkowników. Inna ważna grupa to Opcje zabezpieczeń. Trzeci obiekt, Zasady inspekcji, służy do włączania monitorowania wykorzystania systemu oraz dostępu do zasobów.

Prawa użytkowników Windows XP to zespół zasad określających, jakie czynności w obrębie systemu operacyjnego, mogą wykonywać użytkownicy i grupy. Nie należy mylić praw z uprawnieniami do obiektów. Uprawnienia są ściśle związane z czynnościami dozwolonymi dla użytkowników w odniesieniu do danego obiektu (folder, drukarka itp.). Można na przykład określić, który użytkownik ma uprawnienie do drukowania na wskazanej drukarce, a który nie. Prawa natomiast są związane z działalnością wykonywaną w obrębie całego komputera, np. prawo do zamykania systemu. W folderze Przypisywanie praw użytkownika możesz nadawać użytkownikom szereg "przywilejów" realizacji poszczególnych zadań. W celu zmiany ustawień wskazanego prawa, należy wejść w jego właściwości (podwójne kliknięcie obiektu) i dodać lub usunąć użytkownika albo grupę z listy kont. Zarządzanie prawami wymaga szczególnej ostrożności, łatwo bowiem spowodować luki w zabezpieczeniach komputera, nieostrożnie nadając przywileje. Posługiwanie się konfiguracją praw powinno być ostatecznością. W wypadku stacji lokalnych wiele funkcji administratora można wykonać, niekoniecznie zmieniając ustawienia praw. Chcąc na przykład, żeby użytkownik nie mógł się zalogować do komputera, wystarczy zablokować konto w zarządzaniu systemem, zamiast przypisywać mu ograniczenie Odmowa logowania lokalnego.

Opcje zabezpieczeń służą do konfiguracji dodatkowych parametrów zwiększających bezpieczeństwo systemu. Obejmują kilka grup ustawień związanych z takimi elementami, jak konta, logowanie, dostęp sieciowy i wiele innych. Przed przestawieniem jakiejkolwiek opcji dokładnie zapoznaj się z jej opisem. Podobnie jak w wypadku konfiguracji praw,

nieprzemyślana zmiana ustawień może spowodować, że komputer stanie się bardzo podatny na ataki z zewnątrz. Nie jest na przykład wskazana zmiana ustawień opcji Stan konta gościa albo Zezwalaj na stosowanie uprawnień Wszyscy do anonimowych użytkowników. W trosce o większe bezpieczeństwo warto natomiast zmienić nazwę konta Administratora lub uaktywnić opcję Logowanie interakcyjne: nie wyświetlaj nazwy ostatniego użytkownika. Dla użytkowników o mniejszym doświadczeniu zalecanym sposobem na zwiększenie bezpieczeństwa systemu jest posłużenie się gotowymi szablonami Zasady grupy.

Folder związany z zasadami inspekcji pozwala na wskazanie, jakie zachowania i zasoby systemu mają być monitorowane przez Windows XP. Monitorowanie obejmuje grupę kategorii odnoszących się do różnych obiektów systemu, może to być na przykład ăszpiegowanieÓ dostępu do plików i folderów, logowania i wylogowywania ze stacji itp.

Inspekcja polega na odnotowywaniu w Podglądzie zdarzeń informacji o dostępie do zasobów oraz wystąpieniu zdarzenia systemowego. Administrator określa, jaką część systemu chce monitorować i czy interesują go próby dostępu lub zmiany konfiguracji zakończone sukcesem, czy niepowodzeniem. Jeśli chcesz nadzorować użycie plików lub drukarek, musisz jeszcze odpowiednio skonfigurować sam zasób. Otwórz właściwości obiektu i wskaż, jaki dostęp ma być śledzony. Na przykład we właściwościach drukarki kliknij kartę Zabezpieczenia | Zaawansowane | Inspekcja i wybierz typ dostępu (sukces, porażka), rodzaj (np. drukowanie, odczyt uprawnień) i konta użytkowników, których chcesz obserwować (np. Wszyscy).

Uwaga! Karta Zabezpieczenia jest dostępna tylko dla drukarek oraz danych przechowywanych na wolumenach NTFS, po wyłączeniu ustawienia Użyj prostego udostępniania plików w Opcje folderów | Mój komputer | Narzędzia.

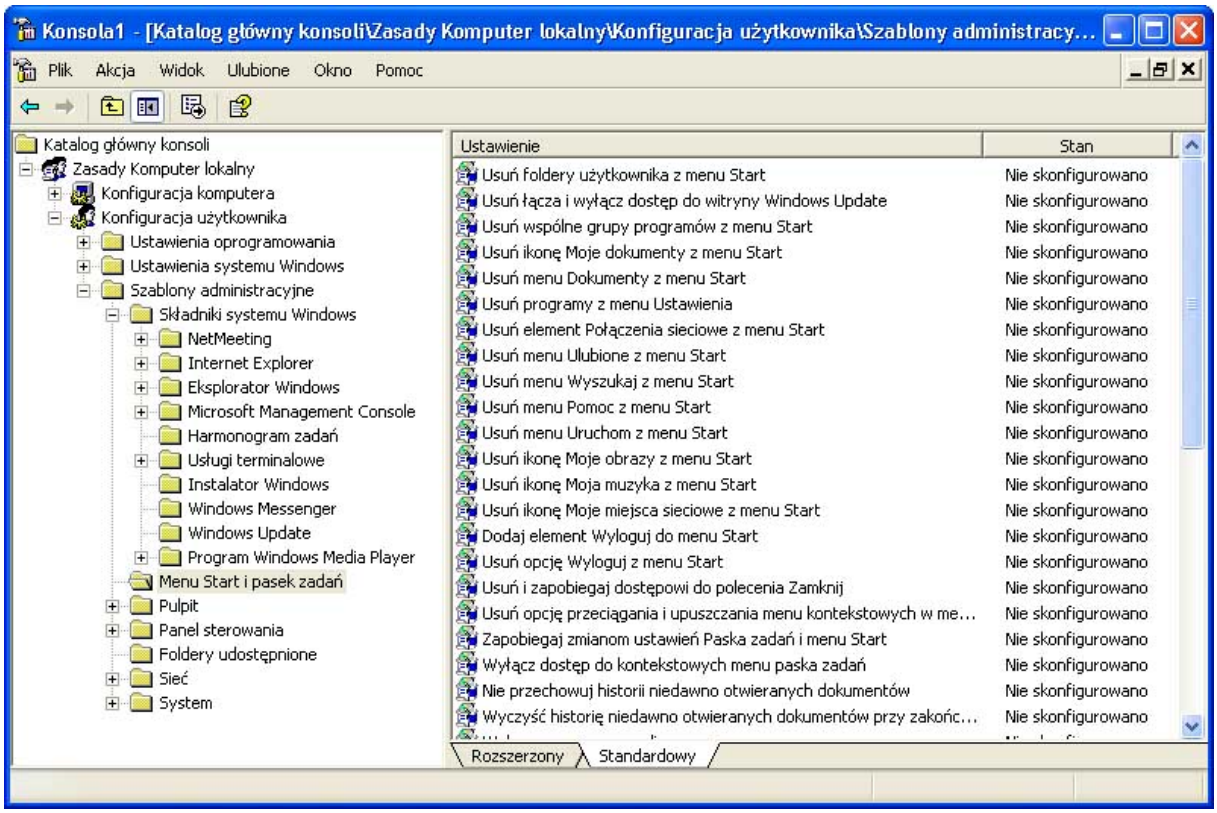
Folder Szablony administracyjne

Ustawienia wprowadzane przez Zasady zabezpieczeń lokalnych nie są jedynym źródłem zwiększania bezpieczeństwa systemu. Wiele przydatnych opcji znajduje się w folderze Szablony administracyjne. Co prawda, większość z nich nie wpływa bezpośrednio na ochronę systemu, lecz pozwala ograniczyć dostęp do obiektów Windows XP. Wspomniane parametry można przypisać zarówno do obiektu komputer, jak i użytkownik. Ponieważ liczba ustawień związanych z tymi obiektami jest pokaźna, skoncentrujemy się na opcjach najważniejszych, dotyczących bezpieczeństwa.

Konfiguracja komputera obejmuje takie elementy, jak Składniki systemu Windows, System, Sieć i Drukarki. Przeglądając ich zawartość, można natrafić jedynie na kilka parametrów mogących mieć wpływ na ograniczenia dostępu do pewnych komponentów Windows: Internet Explorer, Usługi terminalowe, NetMeeting itp. Przykładem niech będzie opcja Internet Explorera - Strefy zabezpieczeń: Nie zezwalaj użytkownikowi na zmianę zasad, która zabrania wprowadzania zmian do właściwości stref zabezpieczeń przeglądarki internetowej.

Konfiguracja użytkownika jest folderem dającym administratorowi większe pole do popisu. Ustawienia w szablonach administracyjnych mogą istotnie ograniczyć to, co użytkownicy będą widzieli na pulpicie oraz do czego będą mieli dostęp. Znaczna większość opcji rozpoczyna się od groźnie brzmiących słów, np. Panel sterowania: Zabroń dostępu do Panelu

sterowania, System: Zapobiegaj dostępowi do narzędzi edycji rejestru, menu Start i pasek zadań: Usuń i zapobiegaj dostępowi do polecenia Zamknij.



Przykładowe parametry konfiguracyje dla użytkownika

Nakładanie tych ograniczeń najlepiej sprawdza się w domenach Windows 2000 lub 2003, gdzie parametry są pobierane z kontrolerów domeny. W wypadku komputera lokalnego przypisanie odmiennych ustawień logującym się użytkownikom jest nieco skomplikowane. Najłatwiej można wpłynąć na to, komu zasady zostaną zaimplementowane, przypisując odpowiednie uprawnienia do folderu GroupPolicy (katalog_systemowy\system32). Jeśli system został zainstalowany w wolumenie NTFS, należy wyłączyć proste udostępnianie folderów w Opcjach folderów, następnie we właściwościach katalogu GroupPolicy określić, że np. grupa Administratorzy nie ma uprawnień do odczytywania jego zawartości. Jeżeli nie masz uprawnień, nie zostaną zastosowane zasady. Trzeba jednak pamiętać, że odebranie sobie uprawnień nie pozwala również na zmianę zasad. Gdy zajdzie konieczność modyfikacji ustawień, należy uprawnienia przywrócić. Nie jest to może najbardziej elastyczne rozwiązanie, ale na pewno na swój sposób skuteczne. Innym, lepszym sposobem ograniczania użytkowników jest wtapianie w rejestr ich profilu odpowiednich ustawień. Tu konieczna jest dokładna znajomość parametrów rejestru oraz duża ostrożność. Nieumiejętne posługiwanie się Edytorem rejestru może być bardzo szkodliwe. Żeby odnaleźć informacje o tym, gdzie i jakie wpisy wykonać w rejestrze, należy poszperać nieco na stronach internetowych firmy Microsoft lub np. skorzystać z wyszukiwarki Google.

Szablony Zasad grupy

Omówiony do tej pory sposób konfigurowania Zasad grupy jest nie tyle skomplikowany, co uciążliwy. Przebrnięcie przez ponad setkę ustawień, szczegółowe wczytywanie się w pomoc dotyczącą każdego parametru wymaga bardzo wiele czasu. W celu ułatwienia i przyśpieszenia konfiguracji systemu możesz się posłużyć szablonami Zasad grupy.

Typy i zadania szablonów Zasad grupy

Nazwa szablonu	Zastosowanie
CompatWS	Szablon usuwa wszystkich użytkowników z grupy Użytkownicy zawansowani, dodatkowo zwiększa uprawnienia grupy. Użytkownicy w celu umożliwienia uruchamiania aplikacji niedostosowanych do zabezpieczeń systemu XP.
HisecWS	Szablon zawiera wszystkie ustawienia nanoszone przez SecureWS oraz dodatkowe zabezpieczenia związane z uwierzytelnieniem i komunikacją sieciową.
SecureWS	Zwiększa szereg parametrów zabezpieczeń systemu np. ustawienia blokowania kont, haseł, zasad inspekcji.
RootSec	Przywraca domyślne uprawnienia katalogu głównego dysku systemowego.
Setup security	Zawiera domyślne ustawienia zabezpieczeń przypisywane po instalacji Windows XP.

Szablony to zdefiniowane przez projektantów firmy Microsoft ustawienia zasad, zapisane w pliku. Wystarczy je zaimportować do systemu i cała konfiguracja jest zakończona. Ponieważ wymagania użytkowników Windows XP mogą być odmienne, przygotowano grupę szablonów, z których każdy pozwala na ustawienie stacji na różnym poziomie zabezpieczeń. Dodatkowo użytkownicy mogą definiować własne szablony do późniejszego wykorzystania na innych komputerach.

Do kompleksowej pracy z szablonami potrzebne są dwie przystawki konsoli MMC: Konfiguracja i analiza zabezpieczeń oraz Szablony zabezpieczeń. Aby je uruchomić, należy uruchomić konsolę MMC i dodać do niej wymienione obiekty (polecenie Dodaj/Usuń przystawkę).

Przystawka Szablony zabezpieczeń służy do modyfikacji oraz tworzenia własnych ustawień zasad grupy. Fizycznie szablony to pliki z rozszerzeniem INF, przechowywane w katalogu folder_systemowy\security\templates. Po uruchomieniu przystawki zobaczysz listę dostępnych szablonów systemu. Rozwijając każdy z nich, sprawdzisz, jakie parametry są przez niego nanoszone. Jeśli chcesz zdefiniować własny szablon, kliknij prawym przyciskiem myszy folder z plikami szablonów i wybierz opcję Nowy szablon.

Lista ustawień wprowadzanych do XP jest nieco inna od tego, co zawierała przystawka Zasady zabezpieczeń lokalnych. Warto o nich wspomnieć, ponieważ dostępnych jest kilka dodatkowych parametrów. Po pierwsze, można konfigurować opcje Dziennika zdarzeń. Zmiana parametrów narzuci Windows XP takie ustawienia, jak maksymalny rozmiar poszczególnych plików dziennika, sposoby reakcji systemu na przepełnienie dziennika oraz zezwolenie na dostęp do danych przez grupę Goście. Następna opcja - Grupy z ograniczeniami służy do wymuszania członkostwa w grupach. Jeśli w systemie są grupy, których członkostwo powinno być przez ciebie z góry określone i niezmienne, możesz się posłużyć tym ustawieniem. Jeśli chcesz na przykład, żeby jedynymi członkami grupy Użytkownicy zaawansowani byli Gosia i Marcin, dodaj tę grupę, wraz z wymienionymi kontami, do folderu Grupy z ograniczeniami. Gdy zapiszesz ustawienia szablonu, a w dalszej kolejności zastosujesz jego ustawienia do swojego komputera, obecni członkowie grupy Użytkownicy zaawansowani zostaną usunięci i zastąpieni kontami Gosia i Marcin. Kolejny folder pozwala na wykorzystanie szablonu do konfiguracji usług systemowych. Podczas optymalizacji i zabezpieczania systemu często wyłącza się automatyczne uruchamianie niepotrzebnych serwisów. W tym celu w przystawce Usługi (Panel sterowania | Narzędzia administracyjne) należy zmienić parametry startowe. Zastosowanie szablonów pomoże

ujednolicić ten proces. Jeśli na dostępnej liście usług zmienisz ustawienia uruchamiania, implementacja szablonu wykona za ciebie całą pracę. Ostatnie dwa foldery, Rejestr i System plików, funkcjonują w podobny sposób. Ich zadaniem jest ujednolicenie uprawnień do zasobów. Po określeniu w szablonie, jakie czynności mogą wykonywać użytkownicy na wybranych kluczach w rejestrze oraz plikach na partycjach NTFS, uprawnienia te zostaną nadane podczas zastosowania szablonu.

Przystawka Szablony zabezpieczeń pozwala na definiowanie oraz modyfikację szablonów przystawki Zasady grupy. W celu wdrożenia przygotowanych ustawień posłuż się przystawką Konfiguracja i analiza zabezpieczeń. Dzięki niej nie tylko łatwo przeniesiesz skonfigurowane opcje do systemu, ale także będziesz mógł przeanalizować, jakie różnice występują między ustawieniami komputera a tym, co zostanie przypisane przez szablon. Po załadowaniu przystawki konieczne jest utworzenie bazy danych analizy. W tym celu kliknij prawym przyciskiem myszy główny folder Konfiguracji i analizy zabezpieczeń, a następnie wybierz polecenie Otwieranie bazy danych. Baza analizy służy do porównywania bieżących ustawień komputera z tymi, które będą wprowadzone przez szablon. Po wprowadzeniu nazwy nowej bazy wskaż szablon, który chcesz do niej zaimportować. Następnie możesz bezpośrednio nanieść zmiany konfiguracji w komputerze albo przeprowadzić analizę różnic w ustawieniach. Bardzo zalecane jest wcześniejsze skontrolowanie nanoszonych ustawień, gdyż po załadowaniu zmian nie ma prostego sposobu odwrócenia tej operacji. Rezultatem wykonanej analizy jest raport tekstowy i graficzny. Tekstowy odnotowuje zmiany w dzienniku (domyślnie nazwa_szablonu.log), natomiast graficzny wyświetla okno z ustawieniami, przy których pojawiają się ikony reprezentujące zgodność lub niezgodność modyfikowanych opcji.