Windows 7 PL. Zaawansowana administracja systemem

Autor: Andrzej Szeląg
ISBN: 978-83-246-2461-4
Format: 158x235, stron: 360

Komfortową metodę wprowadzenia w zaawansowane zagadnienia związane z zarządzaniem nowym środowiskiem firmy Microsoft oferuje książka Windows 7 PL. Zaawansowana administracja systemem. Dzięki niej poznasz m.in. dostępne wersje systemu Windows 7 PL oraz dowiesz się, jakie wprowadzono w nich nowości, a także dobierzesz najlepszy sposób instalacji tego środowiska. Poza tym nauczysz się korzystać z narzędzi administracyjnych, systemowych i narzędziowych oraz zdobędziesz wiadomości na temat zaawansowanego zarządzania dyskami i systemami plików w Windows 7 PL. Łatwo opanujesz też administrację kontami użytkowników i grup oraz poznasz tematykę bezpieczeństwa środowiska i zagadnienia związane z korzystaniem z sieci.

- Wprowadzenie do systemu Windows 7 PL
- Wybór wersji i instalacja środowiska
- Zarządzanie komputerem z systemem Windows 7 PL
- Administracja dyskami i systemami plików
- Zarządzanie kontami użytkowników i grupami
- Zaawansowana konfiguracja i używanie narzędzi do ochrony danych
- Zarządzanie ustawieniami sieci i dostępem do internetu
- Konfiguracja zabezpieczeń systemu
- Monitorowanie i optymalizacja działania Windows 7 PL

Już dziś zostań profesjonalnym administratorem systemu Windows 7 PL

Helion SA
ul. Kościuszki 1c
44-100 Gliwice
tel. 032 230 98 63
e-mail: helion@helion.pl

Spis treści

8.4.2. Konfigurowanie inspekcji zdarzeń logowania na kontach

Inspekcja zdarzeń logowania na kontach rejestruje zdarzenia logowania i wylogowywania użytkowników na komputerze pracującym pod kontrolą systemu Windows 7 Professional, a wyniki jej pracy zapisywane są w dzienniku systemowym *Zabezpieczenia*.

Aby skonfigurować inspekcję zdarzeń logowania na kontach w komputerze pracującym pod kontrolą systemu Windows 7 Professional, należy z poziomu przystawki *Edytor lokalnych zasad grupy* przejść do wspomnianej wcześniej gałęzi oraz wykonać (jako lokalny administrator) przedstawione poniżej kroki.

1. Zaznaczamy w środkowym panelu zasadę *Przeprowadź inspekcję zdarzeń logowania na kontach* (*Audit Account Logon Events*).
2. Z menu *Akcja* (*Action*) wybieramy polecenie *Właściwości* (*Properties*).
3. W oknie przedstawionym na rysunku 8.27 zaznaczamy opcję *Niepowodzenie* (*Failure*) i klikamy przycisk *OK*.
4. Zamykamy przystawkę *Edytor lokalnych zasad grupy*.

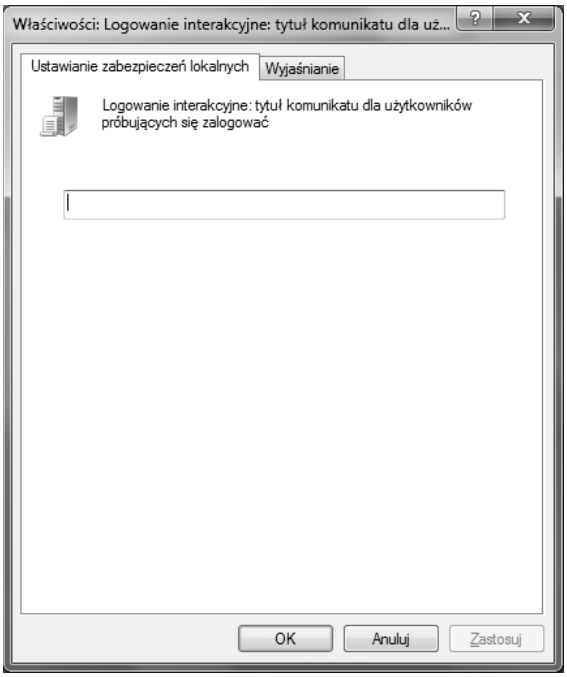
Ustawienie zabezpieczeń *Przeprowadź inspekcję zdarzeń logowania na kontach* pozwala określić (zgodnie z rysunkiem 8.27), czy każda weryfikacja poświadczeń konta na lokalnym komputerze (aktywna opcja *Niepowodzenie* [*Failure*]) ma być poddawana inspekcji w systemie Windows 7 Professional.

8.5. Zaawansowane konfigurowanie zabezpieczeń w Windows 7

Zaawansowane konfigurowanie zabezpieczeń w systemie Windows 7 Professional można przeprowadzić z poziomu przystawki *Edytor lokalnych zasad grupy* w gałęzi *Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady lokalne\Opcje zabezpieczeń* (*Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options*). W powyższej lokalizacji można znaleźć szereg przydatnych ustawień zabezpieczeń. Niektóre z nich zostały przedstawione w dalszej części książki.

8.5.1. Logowanie interakcyjne: tytuł komunikatu dla użytkowników próbujących się zalogować

Ustawienie zabezpieczeń lokalnych w postaci zasady *Logowanie interakcyjne: tytuł komunikatu dla użytkowników próbujących się zalogować* (*Interactive logon: Message title for users attempting to lon on*), które zostało pokazane na rysunku 8.28, zezwala na określenie tytułu wypisywanego użytkownikowi podczas logowania się — zanim zostanie wyświetlony ekran logowania systemu Windows 7 Professional.



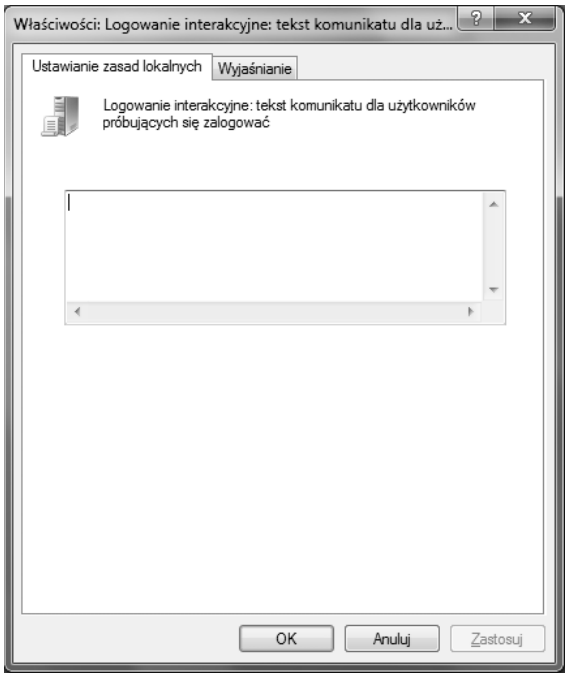
Rysunek 8.28. *Okno dialogowe Właściwości: Logowanie interakcyjne: tytuł komunikatu dla użytkowników próbujących się zalogować*

8.5.2. Logowanie interakcyjne: tekst komunikatu dla użytkowników próbujących się zalogować

Ustawienie zabezpieczeń lokalnych w postaci zasady *Logowanie interakcyjne: treść komunikatu dla użytkowników próbujących się zalogować* (*Interactive logon: Message text for users attempting to lon on*), które zostało pokazane na rysunku 8.29, zezwala na określenie treści komunikatu wyświetlanego każdemu użytkownikowi podczas logowania się — zanim zostanie wyświetlony ekran logowania systemu Windows 7 Professional. To rozwiązanie jest często wykorzystywane w dużych przedsiębiorstwach oraz organizacjach z przyczyn prawnych, np. w celu ostrzeżenia użytkowników o konsekwencjach nieprawidłowego wykorzystania informacji firmowych lub możliwości poddania inspekcji czynności, które użytkownicy wykonują na komputerze.

8.5.3. Klient sieci Microsoft: podpisuj cyfrowo komunikację (zawsze)

Wszystkie edycje systemu Windows 7 obsługują do 20 połączeń z wykorzystaniem protokołu o nazwie *Blok komunikatów serwera* (*Server Message Block*) w wersji *2.0*. Protokół *SMB* jest podstawą mechanizmu udostępniania danych i drukarek w systemach Windows 7 Professional oraz operacji sieciowych, takich jak np. zdalne administrowanie.



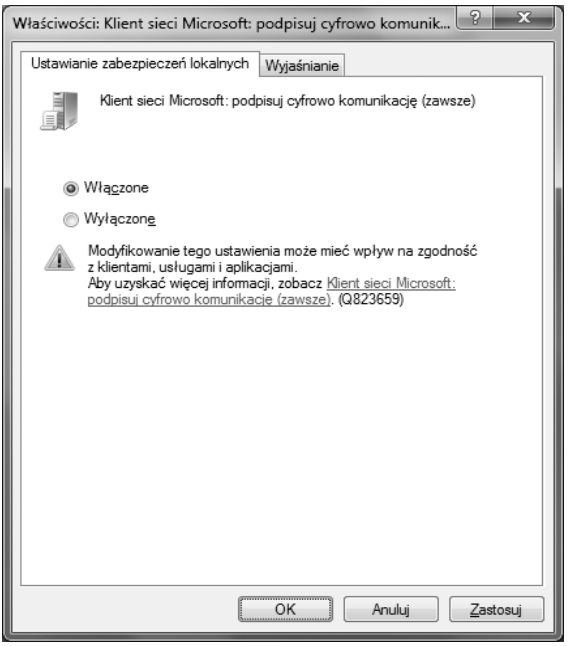
Rysunek 8.29. *Okno dialogowe Właściwości: Logowanie interakcyjne: treść komunikatu dla użytkowników próbujących się zalogować*

Aby zapobiec atakom pochodzącym wnętrza sieci, które polegają np. na modyfikowaniu transmitowanych pakietów *SMB*, wspomniany wcześniej protokół *SMB* obsługuje cyfrowe podpisywanie tych pakietów. Służy do tego zasada ustawienia zabezpieczeń lokalnych o nazwie *Klient sieci Microsoft: podpisuj cyfrowo komunikację (zawsze)* (*Microsoft network client: Digitally sign communications (always)*), której dwie opcje zostały pokazane na rysunku 8.30. Po włączeniu tego ustawienia pakiety *SMB* będą podpisywane cyfrowo przez system Windows 7 Professional. Warto wiedzieć, że klient sieci firmy Microsoft nie będzie mógł komunikować się np. z serwerem sieci firmy Microsoft, dopóki serwer ten nie zgodzi się na podpisywanie pakietów *SMB*.

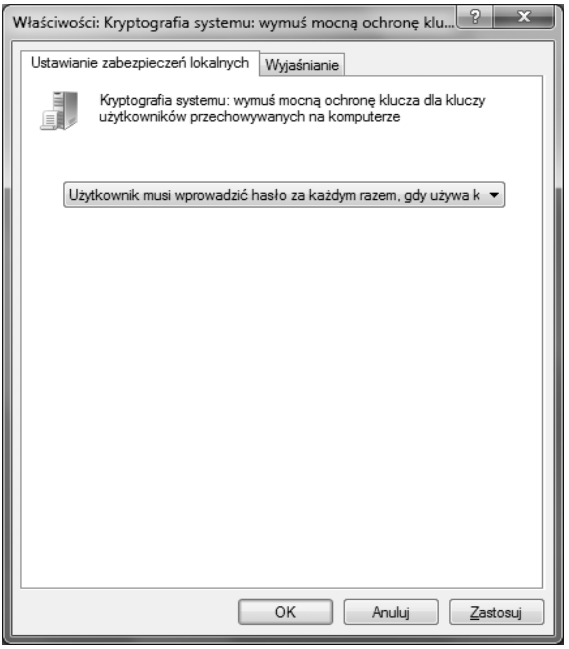
8.5.4. Kryptografia systemu: wymuś mocną ochronę klucza dla kluczy użytkowników przechowywanych na komputerze

Ustawienie zabezpieczeń lokalnych w postaci zasady *Kryptografia systemu: wymuś mocną ochronę klucza dla kluczy użytkowników przechowywanych na komputerze* (*System cryptography: Force strong key protection for user keys stored on the computer*), której jedna z opcji została przedstawiona na rysunku 8.31, określa, czy użycie kluczy prywatnych użytkowników wymaga podania hasła. Dostępne są takie opcje jak:

- *Wprowadzenie danych przez użytkownika nie jest wymagane przy zachowaniu i używaniu nowych kluczy* (*User input is not required when new keys are stored and used*),



Rysunek 8.30. *Okno dialogowe Właściwości: Klient sieci Microsoft: podpisuj cyfrowo komunikację (zawsze)*

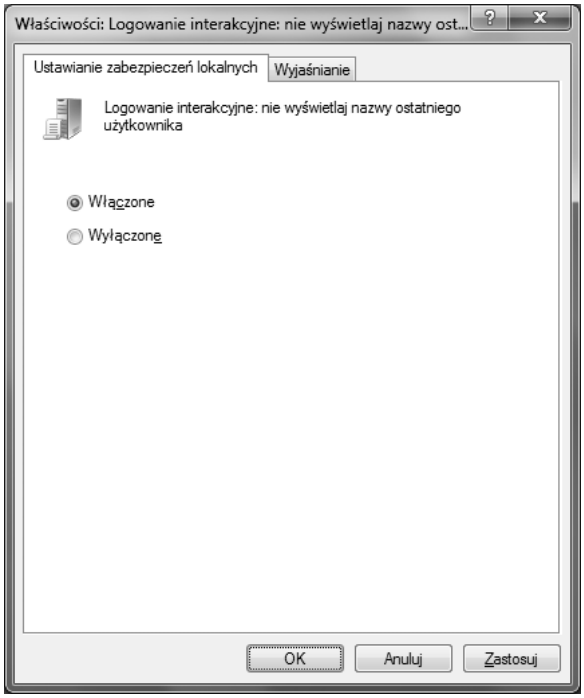


Rysunek 8.31. *Okno dialogowe Właściwości: Kryptografia systemu: wymuś mocną ochronę klucza dla kluczy użytkowników przechowywanych na komputerze*

- *Użytkownik jest monitowany przy pierwszym użyciu klucza* (*User is prompted when the key is first used*),
- *Użytkownik musi wprowadzić hasło za każdym razem, gdy używa klucza* (*User must enter a password each time they use a key*).

8.5.5. Logowanie interakcyjne: nie wyświetlaj nazwy ostatniego użytkownika

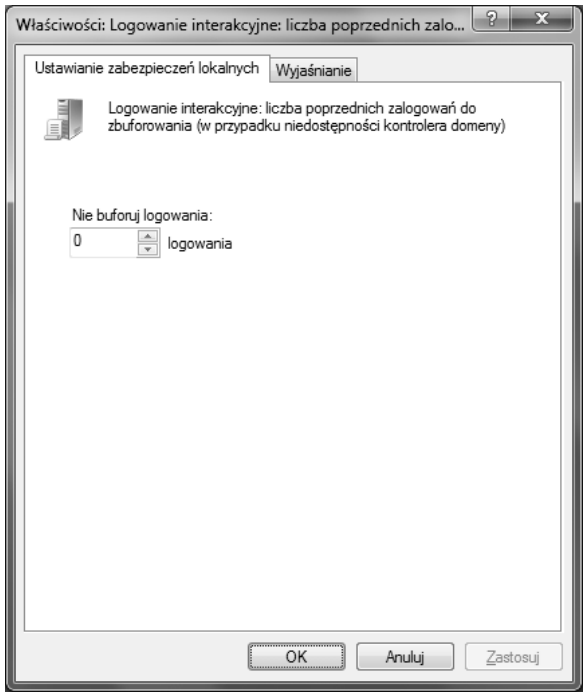
Ustawienie zabezpieczeń lokalnych w postaci zasady *Logowanie interakcyjne: nie wyświetlaj nazwy ostatniego użytkownika* (*Interactive logon: Do not display last user name*), które zostało przedstawione na rysunku 8.32, określa, czy na ekranie logowania systemu Windows 7 Professional będzie wyświetlana nazwa użytkownika, który ostatnio zalogował się na komputerze. Jej brak nie pozwala intruzowi poznać nazwy użytkownika, który ma konto w systemie. Potencjalny intruz nie tylko będzie musiał odkryć nazwę użytkownika, ale i jego hasło, co dodatkowo chroni dostęp do systemu Windows 7 Professional.



Rysunek 8.32. *Okno dialogowe Właściwości: Logowanie interakcyjne: nie wyświetlaj nazwy ostatniego użytkownika*

8.5.6. Logowanie interakcyjne: liczba pośrednich zalogowań do zbuforowania (w przypadku niedostępności kontrolera domeny)

Ustawienie zabezpieczeń lokalnych w postaci zasady *Logowanie interakcyjne: liczba pośrednich zalogowań do zbuforowania (w przypadku niedostępności kontrolera domeny)* (*Interactive logon: Numbers of previous logons to cache (in case domain controller is not available)*), które zostało pokazane na rysunku 8.33, określa, czy będzie możliwe pracowanie na kontach domenowych przy jednoczesnym braku dostępu do jakiegokolwiek



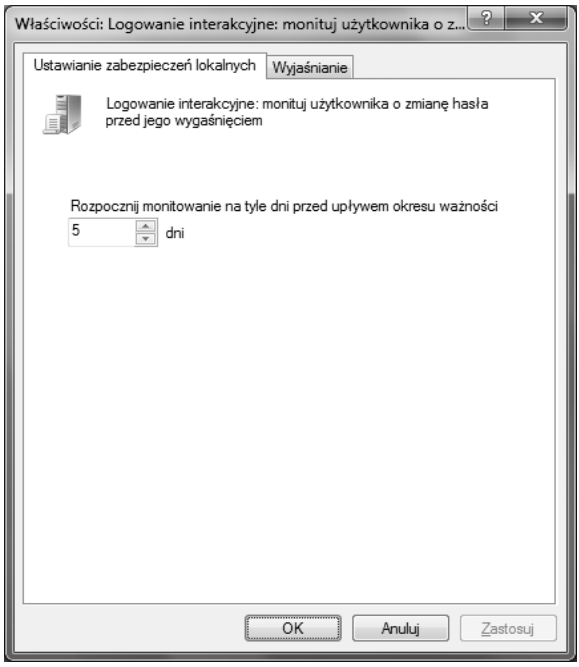
Rysunek 8.33. *Okno dialogowe Właściwości: Logowanie interakcyjne: liczba pośrednich zalogowań do zbuforowania (w przypadku niedostępności kontrolera domeny)*

kontrolera domeny. Ustawienie w tej zasadzie wartości *0* spowoduje wyłączenie buforowania lokalnego kont domenowych, a tym samym niemożność pracy na tego typu koncie przy braku możliwości skontaktowania się z kontrolerem domeny.

Alternatywna metoda zmiany domyślnej wartości poświadczeń kont domenowych przechowywanych w buforze lokalnego komputera została zaprezentowana w rozdziale 7. tej publikacji i polegała na edycji rejestru systemu Windows, a dokładniej ciągu *CachedLogonsCount* typu *REG_SZ* znajdującego się w kluczu *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon*.

8.5.7. Logowanie interakcyjne: monituj użytkownika o zmianę hasła przed jego wygaśnięciem

Ustawienie zabezpieczeń lokalnych w postaci zasady *Logowanie interakcyjne: monituj użytkownika o zmianę hasła przed jego wygaśnięciem* (*Interactive logon: Prompt user to change password before expiration*), które zostało przedstawione na rysunku 8.34, określa, z jakim wyprzedzeniem (w dniach) użytkownicy będą ostrzegani o wygaśnięciu hasła dostępowego. Dzięki temu będą mieli czas na przygotowanie tzw. silnego hasła. W systemie Windows 7 Professional jest to okres 14 dni. Można go zmienić na inny, np. 5 dni.



Rysunek 8.34. *Okno dialogowe Właściwości: Logowanie interakcyjne: monituj użytkownika o zmianę hasła przed jego wygaśnięciem*

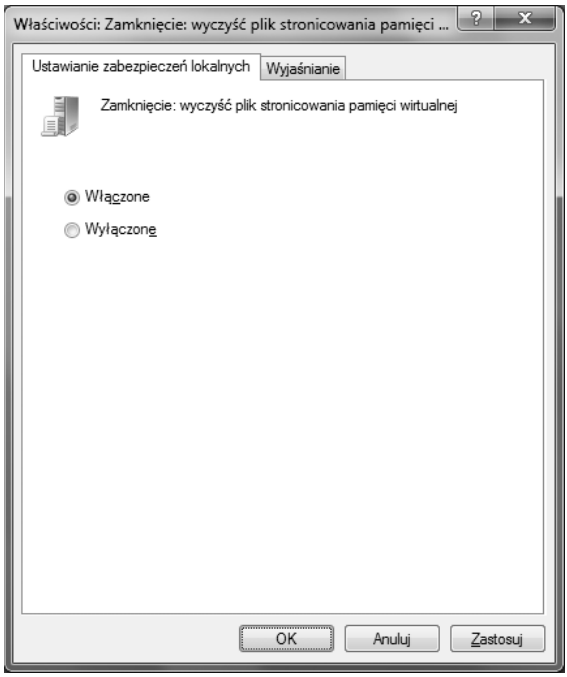
8.5.8. Zamknięcie: wyczyść plik stronicowania pamięci wirtualnej

Plik stronicowania pamięci wirtualnej *pagefile.sys* używany jest przez funkcje obsługi pamięci wirtualnej do zapisywania na dysku twardym nieużywanych stron pamięci fizycznej. W poprawnie działającym systemie Windows 7 Professional plik ten jest chroniony oraz otwierany wyłącznie przez system operacyjny. Jednakże w systemach, w których została skonfigurowana możliwość rozruchu innych systemów operacyjnych, może być konieczne zagwarantowanie, że plik stronicowania jest czyszczony podczas zamykania systemu. Tego typu zabieg ma na celu głównie uniemożliwienie dostępu nieautoryzowanym użytkownikom (intruzom) do poufnych informacji z pamięci procesów, które mogły zostać zapisane w pliku stronicowania na dysku twardym, nawet wtedy, kiedy uda im się uzyskać bezpośredni dostęp do tego systemowego pliku.


Uwaga

Plik stronicowania to obszar dysku twardego używany przez system Windows 7 Professional tak, jakby była to pamięć fizyczna.

Ustawienie zabezpieczeń lokalnych w postaci zasady o nazwie *Zamknięcie: wyczyść plik stronicowania pamięci wirtualnej* (*Shutdown: Clear virtual memory pagefile*), które zostało pokazane na rysunku 8.35, określa, czy plik stronicowania pamięci wirtualnej będzie czyszczony podczas zamykania systemu Windows 7 Professional. Włączenie tej zasady powoduje czyszczenie systemowego pliku stronicowania pamięci wirtualnej podczas zamykania systemu operacyjnego, przez co samo jego zamykanie wydłuża się nieznacznie.



Rysunek 8.35. *Okno dialogowe Właściwości: Zamknięcie: wyczyść plik stronicowania pamięci*