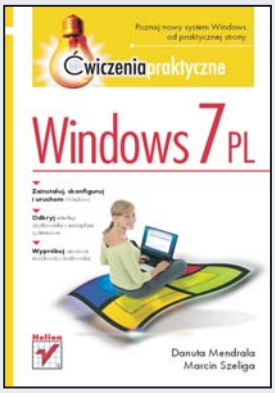
Windows 7 PL. Ćwiczenia praktyczne



Autorzy: Danuta Mendrala, Marcin Szeliga
ISBN: 978-83-246-2426-3
Format: A5, stron: 192

Poznaj nowy system Windows od praktycznej strony

- Zainstaluj, skonfiguruj i uruchom Windows
- Odkryj interfejs użytkownika i narzędzia systemowe
- Wypróbuj sieciowe możliwości środowiska

Użytkownicy systemów tworzonych przez firmę Microsoft długo czekali na nową wersję najpopularniejszego na świecie graficznego środowiska operacyjnego. Wraz z pojawieniem się Windows 7 ich cierpliwość została wreszcie nagrodzona, a wymagania całkowicie zaspokojone. Ostatnia edycja „okienek" oferuje bowiem szereg ciekawych funkcji, bardzo atrakcyjny wygląd i niespotykany do tej pory poziom bezpieczeństwa.

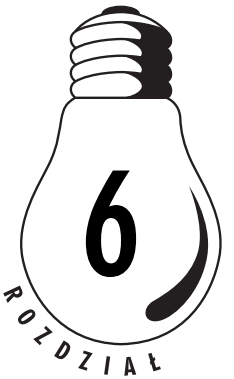
Aby móc w pełni skorzystać z tych możliwości, potrzebujesz jednak odpowiedniej wiedzy. W przystępny sposób dostarczy Ci ją książka „Windows 7 PL. Ćwiczenia praktyczne", stanowiąca niezbędną pozycję w biblioteczce każdego, kto rozpoczyna swoją przygodę z tym środowiskiem lub chce szybko i bez problemów przesiąść się na nową wersję systemu. Lektura poparta wykonaniem kolejnych ćwiczeń umożliwi Ci praktyczne poznanie procesu instalacji i konfiguracji Windows 7, zaznajomi z graficznym interfejsem użytkownika środowiska i przybliży sposoby przeprowadzania podstawowych działań na systemie plików. Z książki dowiesz się również, jak podłączyć swój komputer do sieci i korzystać z zasobów internetu, a także nauczysz się właściwie zabezpieczyć Windows przed typowymi zagrożeniami.

- Instalacja i aktualizacja systemu do wersji 7
- Podstawowe operacje w środowisku Windows
- Praca z oknami i innymi elementami interfejsu
- Konfiguracja i optymalizacja systemu
- Tworzenie, kontrolowanie i usuwanie kont użytkowników
- Zarządzanie plikami i folderami
- Podłączanie do sieci i korzystanie z jej zasobów
- Sposoby zabezpieczania systemu przed wirusami i atakami z zewnątrz

Dowiedz się, co może Ci zaoferować Windows 7

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

Spis treści



Bezpieczeństwo

Jeśli podłączyłeś do sieci niezabezpieczony komputer, to sam prosisz się o kłopoty. Wystarczy, że raz nie dopisze Ci szczęście i zostaniesz ofiarą ataku — w takim przypadku musisz liczyć się z utratą lub ujawnieniem Twoich danych i z kosztownymi awariami. Na szczęście Windows 7 został opracowany z myślą o poprawie bezpieczeństwa jego użytkowników.

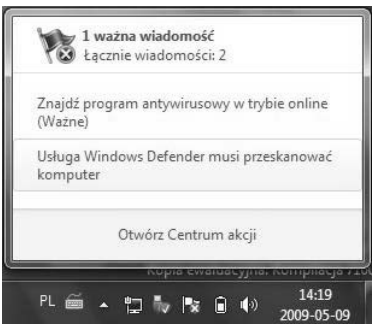
ĆWICZENIE

6.1 Centrum akcji

Centrum akcji zastąpiło Centrum zabezpieczeń z Visty i jest miejscem, w którym można szybko sprawdzić stan komputera i skonfigurować najważniejsze dla jego bezpieczeństwa opcje, takie jak zapora sieciowa, aktualizacje automatyczne, ochrona przed niebezpiecznymi programami i ochrona kont użytkowników. Dodatkowo Centrum akcji zawiera informacje o problemach z samym systemem Windows, np. o błędnie wykonanej kopii zapasowej czy niewłaściwe skonfigurowanych urządzeniach.

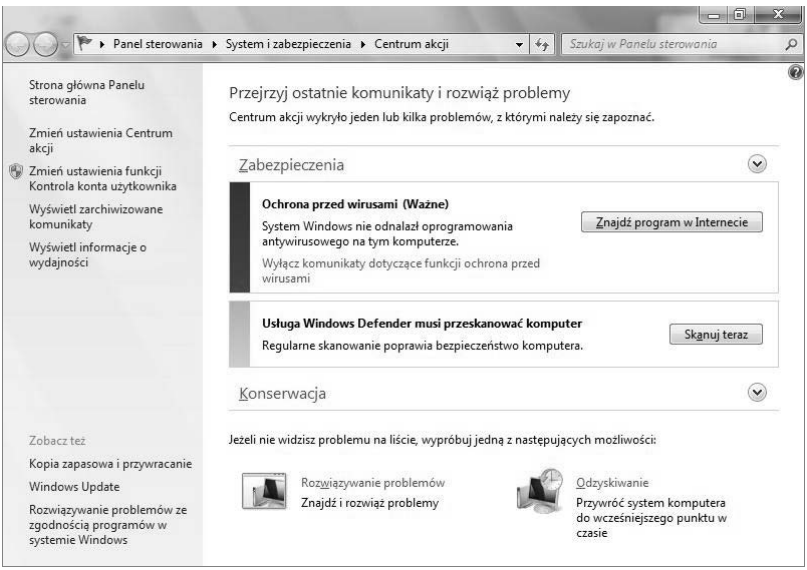
Dopóki komputer jest bezpieczny i działa prawidłowo, nie ma powodu do odwiedzania Centrum akcji. Gdy pojawi się jakiś problem z komputerem lub jego bezpieczeństwem Centrum akcji wyświetli odpowiednie powiadomienie.

1. Kliknij widoczną w obszarze powiadomień ikonę białej flagi — jeżeli dodatkowo zawierała ona czerwony znak ostrzeżenia, zostanie wyświetlone okienko z wiadomościami od Centrum akcji (rysunek 6.1).



Rysunek 6.1. *Dopóki komputer jest bezpieczny, w obszarze powiadomień będzie widoczna biała ikona Centrum akcji — w tym przypadku wykryte zostały dwa problemy i przy ikonie flagi pojawił się czerwony znak ostrzeżenia*

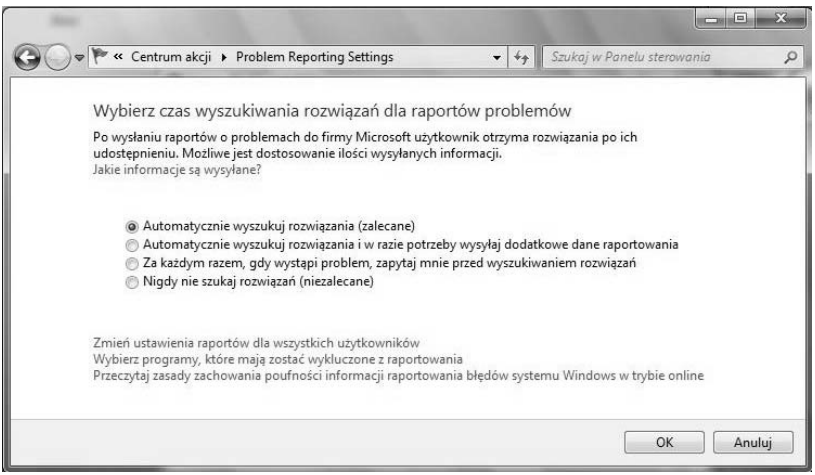
2. Kliknij odnośnik *Otwórz Centrum akcji*.
3. Kwestie, które wymagają Twojej natychmiastowej uwagi, zaznaczone są na czerwono. W tym przypadku system nie wykrył skanera antywirusowego. Mniej poważne problemy (takie jak potrzeba przeskanowania komputera przez usługę Windows Defender) zaznaczone są na żółto (rysunek 6.2).
4. W lewej części okna Centrum akcji znajdują się odnośniki do typowych zadań — kliknij odnośnik *Zmień ustawienia Centrum akcji*.
5. Domyślnie Centrum akcji monitoruje:
   a. Stan usługi Windows Update — jeżeli komputer nie jest automatycznie aktualizowany, zostanie wyświetlone ostrzeżenie.
   b. Ustawienia zabezpieczeń internetowych — jeżeli bieżąca konfiguracja przeglądarki Internet Explorer jest mniej bezpieczna niż konfiguracja domyślna, zostanie wyświetlone ostrzeżenie.
   c. Stan zapory sieciowej — jeżeli zostanie ona wyłączona, zostanie wyświetlone ostrzeżenie.
   d. Stan ochrony przed niechcianymi i szpiegowskimi programami — jeżeli usługa Windows Defender zostanie wyłączona, zostanie wyświetlone ostrzeżenie.



Rysunek 6.2. *Podstawowa ochrona komputera nigdy nie była tak prosta — wystarczy dbać o to, żeby Centrum akcji nie miało żadnych zastrzeżeń do poziomu bezpieczeństwa Twojego komputera*

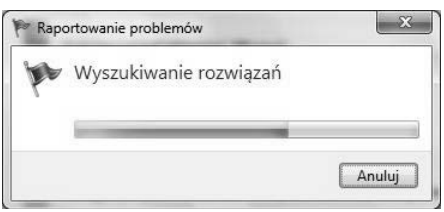
   e. Stan mechanizmu kontroli konta użytkownika — jeżeli zostanie on wyłączony, zostanie wyświetlone ostrzeżenie.
   f. Stan ochrony przed wirusami — jeżeli nie będziemy mieli aktualnego skanera antywirusowego, zostanie wyświetlone ostrzeżenie.

6. Kliknij znajdujący się w sekcji *Pokrewne ustawienia* odnośnik *Ustawienia raportowania problemów* (rysunek 6.3).
7. Zamknij okno konfiguracji usługi raportowania o błędach i kliknij odnośnik *Ustawienia Programu poprawy jakości obsługi klienta*.
8. Domyślnie każdy użytkownik systemu Windows bierze udział w programie polegającym na przesyłaniu do firmy Microsoft danych na temat konfiguracji jego komputera i działania systemu operacyjnego. Przesyłane dane nie zawierają żadnych poufnych informacji i służą wyłącznie do udoskonalania kolejnych wersji Windows.
9. Zdecyduj, czy chcesz uczestniczyć w tym programie, i wróć do okna Centrum akcji.



Rysunek 6.3. *Domyślnie skonfigurowany system Windows 7 zbiera informacje o wszystkich błędach (np. o zawieszaniu się jakiegoś programu) i wysyła je do firmy Microsoft w celu sprawdzenia, czy dany problem został już rozwiązany. Jeżeli tak, znalezione rozwiązanie zostanie nam przesłane*

10. Rozwiń sekcję *Konserwacja* i kliknij odnośnik *Wyszukaj rozwiązania* (rysunek 6.4).



Rysunek 6.4. *Jeżeli masz jakiekolwiek problemy z komputerem, w pierwszej kolejności sprawdź, czy nie są znane ich rozwiązania*

ĆWICZENIE

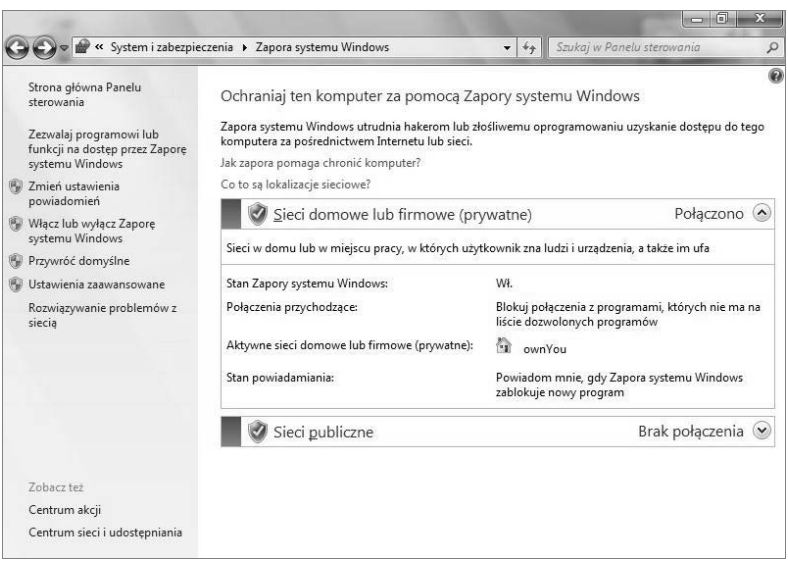
6.2 Zapora sieciowa

Użytkownicy systemu Windows 7 powinni ochronić się przed atakami sieciowymi za pomocą zintegrowanej z systemem zapory połączenia internetowego.

Instalowana z systemami Windows XP SP1 i Windows 2003 zapora służyła jedynie do filtrowania nadchodzących połączeń — proces wysyłania danych z komputera nie był przez nią monitorowany. Zapora systemu Windows 7 umożliwia blokowanie zarówno odbieranych, jak i wysyłanych danych, ale domyślnie zezwala ona na wszystkie połączenia wychodzące.

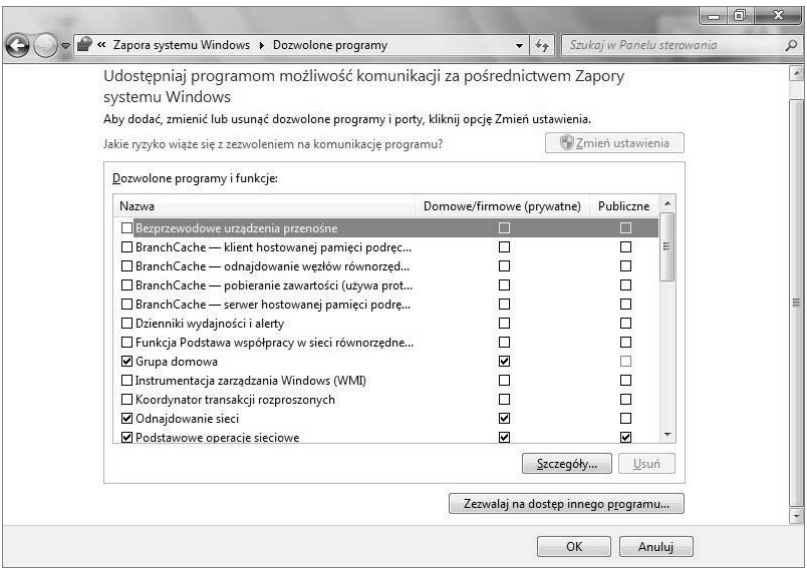
Domyślne ustawienia zapory są odpowiednie dla komputerów, na których nie jest uruchomiony żaden serwer sieciowy, tj. program, który oczekuje na nadchodzące od innych komputerów dane, przetwarza je i wysyła odpowiedzi. Jeżeli Twój komputer pełni funkcję jakiegoś serwera sieciowego, należy tak skonfigurować zaporę połączenia internetowego, aby zezwalała na połączenia z innymi komputerami. W tym celu:

1. Jeżeli okno Centrum akcji nie zostało zamknięte, wpisz w polu wyszukiwania *Zapora* i kliknij odnośnik *Zapora systemu Windows*. W przeciwnym wypadku rozwiń menu *Start*, uruchom *Panel sterowania*, wpisz w polu wyszukiwania *Zapora* i kliknij odnośnik *Zapora systemu Windows* (rysunek 6.5).



Rysunek 6.5. *Jedną z nowości w systemie Windows 7 jest możliwość jednoczesnego używania kilku profili sieciowych. Dzięki czemu, jeżeli komputer jest jednocześnie połączony z siecią publiczną i — poprzez połączenie VPN — z siecią firmową, każde z tych połączeń może mieć inne ustawienia zabezpieczeń*

2. Kliknij odnośnik do zadania *Zezwalaj programowi lub funkcji na dostęp przez Zaporę systemu Windows*.
3. Zostanie wyświetlona lista programów, które mogą wymieniać dane poprzez sieć. Jeżeli interesujący nas program jest na tej liście, wystarczy zaznaczyć odpowiednie pole wyboru (rysunek 6.6).



Rysunek 6.6. *Każdy program może być odblokowany osobno w sieciach prywatnych i publicznych*

4. Gdyby w sieciach prywatnych (domowych lub firmowych) używany był zdalny pulpit, należałoby odblokować tę funkcję poprzez zaznaczenie odpowiedniego pola wyboru.
5. Aby zezwolić na komunikację sieciową wybranemu programowi:
   a. Kliknij przycisk *Zezwalaj na dostęp innego programu*.
   b. Zostanie wyświetlona lista zainstalowanych aplikacji — zaznacz program, który będzie mógł działać w sieciach prywatnych, i kliknij *OK* (rysunek 6.7).
   c. Jeżeli programu nie ma liście, kliknij *Przeglądaj* i wskaż lokalizację głównego pliku programu.
   d. Po kliknięciu *OK* program zostanie dodany do listy wyjątków i będzie poprawnie działał przez sieć.

Rysunek 6.7. *Aby wybrane programy mogły komunikować się w sieciach publicznych, kliknij przycisk Typy lokalizacji sieciowych i wybierz sieci publiczne*

6. Aby zablokować program, któremu wcześniej zezwoliliśmy na komunikację przez sieć:
   a. Zaznacz ten program.
   b. Kliknij przycisk *Usuń*.
   c. Po potwierdzeniu decyzji program zostanie zablokowany przez Zaporę systemu Windows.
7. Aby zablokować wszystkie programy i przywrócić domyślną (bezpieczną) konfigurację Zapory systemu Windows:
   a. Wyświetl okno Zapora systemu Windows.
   b. Kliknij odnośnik *Przywróć domyślne*.
   c. Kliknij przycisk *Przywróć domyślne* i potwierdź swoją decyzję, klikając *Tak*.
8. Kończąc ćwiczenie, zamknij okno Zapory systemu Windows.

ĆWICZENIE

6.3 Automatyczna aktualizacja systemu

W celu lepszego zrozumienia, jak ważne jest regularne uaktualnianie używanego oprogramowania, zapoznaj się z cyklem życia aktualizacji zabezpieczeń:

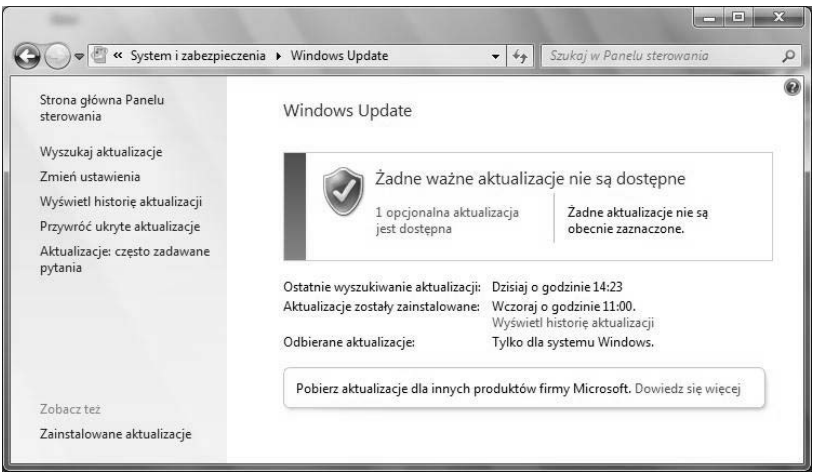
1. Analityk bezpieczeństwa wykrywa lukę i zgłasza ten fakt firmie Microsoft. Opublikowanie przez niego w tym momencie odkrycia w internecie naraziłoby wszystkich korzystających z danego oprogramowania użytkowników na poważne straty.
2. Microsoft rozpoczyna pracę nad przygotowaniem i przetestowaniem eliminującej wykrytą lukę aktualizacji zabezpieczeń. Na tym etapie wyłącznie raportujący i producent oprogramowania wiedzą o błędzie.
3. Microsoft informuje użytkowników o przygotowanym uaktualnieniu. W tym momencie rozpoczyna się wyścig pomiędzy osobą, która chce wykorzystać powszechnie już znaną lukę, a użytkownikiem komputera.
4. Udostępniona aktualizacja zabezpieczeń jest analizowana i na podstawie tych badań (nazywanych wsteczną inżynierią) atakujący dowiaduje się o eliminowanej przez tę aktualizację luce.
5. Po stworzeniu i udostępnieniu kodu exploita hakerzy opracowują wykorzystującego go wirusa. Gotowy wirus zostaje rozpowszechniony w internecie, a niezabezpieczone komputery stają się jego łatwą ofiarą.

Kończąc instalację systemu Windows 7, należało zdecydować, czy włączone będą wszystkie mechanizmy zabezpieczeń, w tym mechanizm automatycznych aktualizacji. Jeżeli wybrałeś zalecaną opcję, system codziennie sprawdzi, czy dostępne są nowe aktualizacje zabezpieczeń, i jeżeli są, pobierze je.

Nie należy zmieniać domyślnego harmonogramu codziennego instalowania pobranych aktualizacji. Chociaż większość aktualizacji zabezpieczeń jest udostępniania raz na miesiąc, to aktualizacje krytyczne są udostępniane natychmiast po ich przygotowaniu i powinny być zainstalowane w ciągu 24 godzin od udostępnienia.

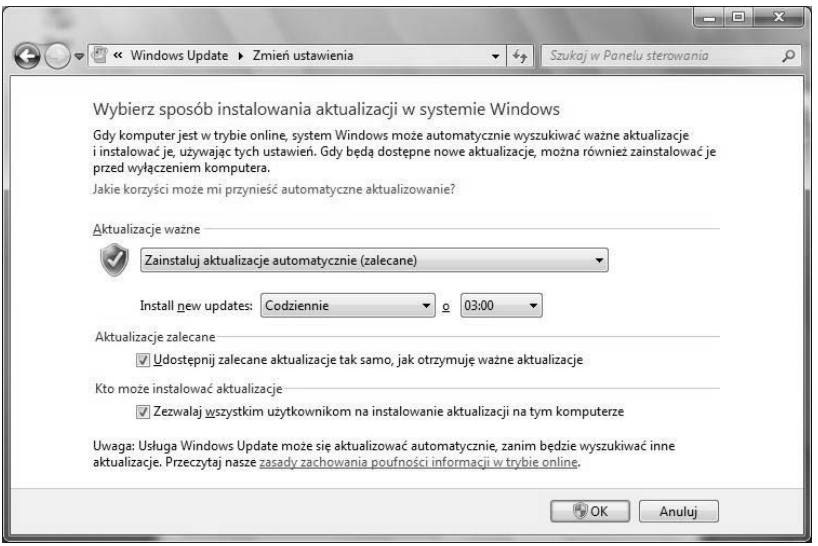
Aby sprawdzić i skonfigurować aktualizacje automatyczne:

1. Otwórz okno Centrum akcji.
2. Kliknij znajdujący się z lewej strony odnośnik *Windows Update*.
3. O ile bieżące ustawienia są takie jak na rysunku 6.8 (czyli system codziennie sprawdza dostępne aktualizacje), ich ręczne sprawdzanie jest niepotrzebne.



Rysunek 6.8. *W oknie Windows Update możesz m.in. przejrzeć i odinstalować wybrane aktualizacje. Możesz też włączyć automatyczne aktualizowanie innych programów, m.in. pakietu Office i niektórych skanerów antywirusowych*

4. Kliknij odnośnik *Zmień ustawienia*. Najwygodniejsze i najbezpieczniejsze jest automatyczne instalowanie pobranych aktualizacji (rysunek 6.9) — wystarczy tylko wybrać właściwą godzinę przeprowadzania tej operacji. Możesz jednak zdecydować się na automatyczne pobieranie i ręczną instalację albo na ręczne pobieranie i instalowanie aktualizacji.
5. Wróć do okna Windows Update.
6. Aktualizowany powinien być nie tylko system Windows, ale również zainstalowane w nim programy — **to w programy, a nie systemy operacyjne wymierzona jest większość ataków**.
7. Kliknij znajdujący się w polu *Pobierz aktualizacje dla innych produktów Microsoft* odnośnik *Dowiedz się więcej*.
8. Zostanie wyświetlona strona WWW usługi Microsoft Update. Zaakceptuj jej regulamin i kliknij przycisk *Zainstaluj*.
9. Zostanie wyświetlone okno kontroli konta użytkownika z pytaniem, czy chcesz zezwolić programowi Windows Update na zmianę konfiguracji Twojego komputera. Kliknij przycisk *Tak*.
10. Usługa Windows Update sprawdzi, czy nie ma dostępnych aktualizacji dla zainstalowanych na Twoim komputerze programów firmy Microsoft.



Rysunek 6.9. *Taka konfiguracja aktualizacji spowoduje, że będą one rzeczywiście automatyczne instalowane — Windows 7 jest pierwszą wersją systemu Windows, w której aktualizacje mogą być instalowane przez standardowych użytkowników (a nie tylko przez administratorów), w dodatku jeżeli komputer będzie o zaplanowanej godzinie aktualizacji uśpiony, zostanie obudzony na czas instalacji aktualizacji*

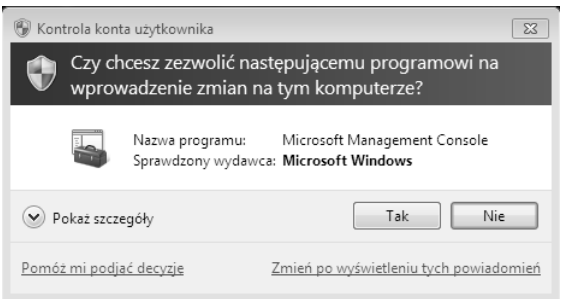
Aktualizując komputer, nie zapominaj o zainstalowanych programach firm trzecich — bardzo często to właśnie one są celem ataków.

ĆWICZENIE

6.4 Kontrola konta użytkownika

Zasada minimalnych uprawnień to jedna z podstawowych, najważniejszych zasad bezpieczeństwa komputerowego. Według tej zasady użytkownik powinien mieć tylko takie uprawnienia, jakie są mu potrzebne do pracy z komputerem — i żadnych więcej. Niestety, w systemach Windows większość użytkowników ma uprawnienia administracyjne, a prawie wszyscy administratorzy na co dzień, podczas sprawdzania poczty czy przeglądania stron WWW, korzystają z konta administratora. Firma Microsoft, chcąc rozwiązać ten problem, w systemie Windows 7 wprowadziła domyślnie ograniczone uprawnienia również dla administratorów.

Wykonanie niektórych ćwiczeń z tej książki wymagało potwierdzenia posiadania uprawnień administratora — w takich sytuacjach wyświetlane było okienko podobne do pokazanego na rysunku 6.10.



Rysunek 6.10. *Jedną z najbardziej krytykowanych funkcji Visty była konieczność ciągłego potwierdzania uprawnień administracyjnych — w skrajnych przypadkach skasowanie jednego pliku wymagało nawet czterokrotnego potwierdzenia posiadanych uprawnień*

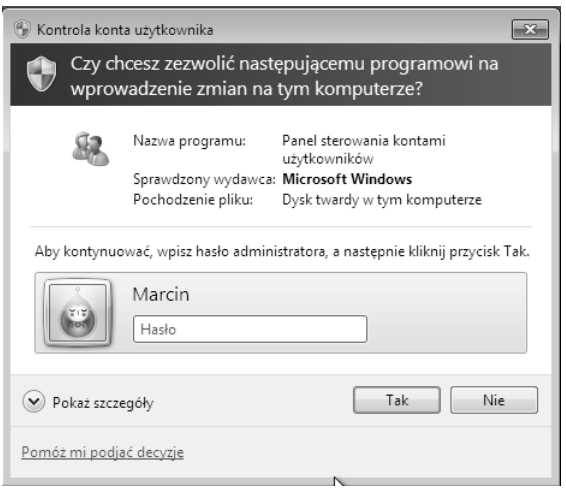
W systemie Windows 7 mechanizm kontroli konta użytkownika został znacznie ulepszony, w związku z czym możemy tygodniami pracować z komputerem i ani razu nie zobaczyć pytania o zezwolenie programowi na wprowadzenie zmian w komputerze. Mechanizm ten jednak nadal chroni nasz komputer.

Aby się o tym przekonać:

1. Zaloguj się do systemu na konto standardowego użytkownika.
2. Wyświetl *Panel sterowania* i kliknij *Dodaj lub usuń konta użytkowników* — ponieważ zarządzanie kontami wymaga uprawnień administratora, zostaniesz poproszony o podanie odpowiedniego hasła (rysunek 6.11).
3. Po podaniu hasła administratora będziesz mógł tworzyć, modyfikować i usuwać konta użytkowników systemu.
4. Wyloguj się i zaloguj na konto administratora.

Działanie mechanizmu kontroli konta użytkownika może być dostosowane do indywidualnych potrzeb:

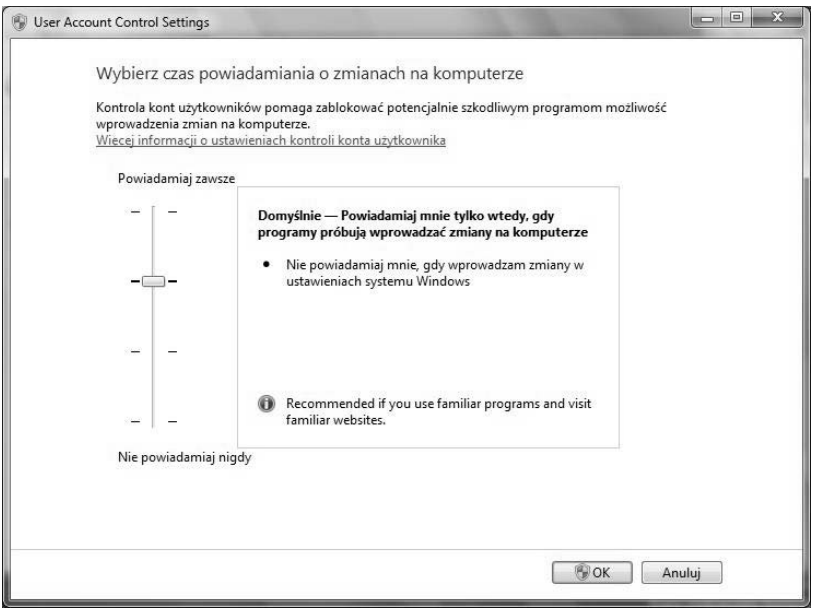
1. Wyświetl okno Centrum akcji.
2. Kliknij odnośnik do zadania *Zmień ustawienia funkcji Kontrola konta użytkownika*.



Rysunek 6.11. *Standardowi użytkownicy przed uruchomieniem programu wymagającego uprawnień administratora zostaną poproszeni o podanie hasła użytkownika posiadającego takie uprawnienia*

3. Zostanie wyświetlone okno pozwalające wybrać operacje, których wykonanie będzie wymagało potwierdzenia posiadania uprawnień administracyjnych[1] (rysunek 6.12).
4. Domyślnie powiadomienia funkcji kontroli konta użytkownika są wyświetlane na bezpiecznym pulpicie — dopóki nie odpowiemy na pytanie, czy zgadzamy się na uruchomienie programu czy narzędzia systemu Windows, pulpit użytkownika będzie zablokowany. W przypadku administratorów powiadomienie może być wyświetlone:
   a. za każdym razem, gdy zmieniane są ustawienia komputera, ustawienia systemowe oraz podczas instalowania programów (najbezpieczniejsza opcja *Zawsze powiadamiaj*),
   b. tylko gdy zmieniane są ustawienia komputera (opcja domyślna),
   c. tylko gdy zmieniane są ustawienia komputera, ale pytanie będzie wyświetlone w standardowym oknie dialogowym a nie na bezpiecznym pulpicie (opcja *Nie przyciemniaj pulpitu*),
   d. nigdy (opcja *Nie powiadamiaj*).
5. Jeżeli nie musisz, nie obniżaj poziomu działania funkcji kontroli konta użytkownika i kliknij *Anuluj*.

[1] W finalnej wersji systemu Windows 7 to okno będzie całkowicie spolszczone i może wyglądać nieco inaczej.



Rysunek 6.12. *W Viście funkcję kontroli konta użytkownika można było włączyć albo wyłączyć, a nieliczne zmiany w jej działaniu trzeba było wprowadzać za pomocą konsoli MMC Zasady grupy. W Windows 7 konfiguracja tej funkcji jest znacznie prostsza*

Wirusy

Wirusy zagrażają wszystkim komputerom działającym pod kontrolą systemów Microsoft Windows, nie tylko tym podłączonym do sieci lokalnych — łącząc się poprzez modem z internetem, odczytując e-maile, odwiedzając stronę WWW czy uruchamiając skopiowany na płytę program, możesz nieświadomie zainfekować swój komputer.

Jedyną skuteczną ochroną przed wirusami jest nieuruchamianie niezaufanych programów, nieodwiedzanie niezaufanych stron WWW, nieotwieranie nieoczekiwanych załączników w e-mailach (również tych otrzymanych od znanych nam osób) i nieklikanie znajdujących się w tych wiadomościach odnośników do stron WWW.

ĆWICZENIE

6.5 Skaner antywirusowy

Pewną ochronę przed wirusami daje bezustanne sprawdzanie, czy uruchamiane i kopiowane pliki nie zostały wcześniej zainfekowane. Zadanie to wykonują skanery antywirusowe — programy, które chronią przed znanymi wirusami i które umożliwiają sprawdzenie, czy na dyskach twardych nie znajdują się zainfekowane pliki.

Programy tego typu, zarówno komercyjne (płatne), jak i darmowe, są powszechnie dostępne — wystarczy wpisać w ulubionej przeglądarce internetowej frazę `Skaner antywirusowy` albo `Ochrona przed wirusami`, aby uzyskać tysiące adresów. Wśród pierwszych dwudziestu będzie znajdować się co najmniej kilka adresów firm oferujących tego typu programy. My zdecydowaliśmy się na skaner ESET Smart Security firmy ESET — demonstracyjną, 30-dniową wersję tego skanera można pobrać pod adresem *http://www.eset.com/download/free_trial_download_int.php*.

Nigdy nie instaluj programów antywirusowych pochodzących z nieznanych źródeł. W ciągu ostatnich lat miało miejsce kilkanaście ogólnoświatowych ataków polegających na próbie nakłonienia użytkowników — z reguły za pomocą wyświetlania fałszywych ostrzeżeń o zainfekowaniu komputera wieloma groźnymi wirusami — do zainstalowania fałszywego programu antywirusowego. Takie programy nie tylko nie chronią przed wirusami, ale same instalują na komputerach wrogie programy (np. programy pozwalające atakującemu przejęcie zdalnej kontroli nad naszym komputerem). Coraz częściej takie fałszywe programy antywirusowe próbują też wyłudzić pieniądze poprzez nakłanianie użytkowników do ich zarejestrowania, a więc do zapłacenia atakującemu za program, który nie chroni, tylko umożliwia zaatakowanie komputera.

1. Jeżeli nie wybrałeś jeszcze programu antywirusowego, kliknij powiadomienie *Centrum akcji*, a następnie wiadomość *Znajdź program antywirusowy w trybie online*.
2. Wybierz program antywirusowy — zostanie wyświetlona strona jego producenta.
3. Pobierz i zainstaluj przeznaczony dla Twojej wersji systemu Windows 7 program antywirusowy. W dalszych punktach tego ćwiczenia i dwóch następnych ćwiczeniach jako przykładowy program antywirusowy został przedstawiony ESET Smart Security Business Edition.

4. Po uruchomieniu programu instalacyjnego skanera antywirusowego zaakceptuj umowę licencyjną i wybierz standardową instalację.
5. Podaj nazwę użytkownika i hasło lub wybierz opcję pozwalającą na podanie tych danych w późniejszym czasie.
6. Włącz dodatkową ochronę przed niechcianymi programami.
7. Po zakończeniu instalacji skaner wykryje połączenie sieciowe i zapyta, czy jest to sieć prywatna czy publiczna. Wybierz odpowiednią opcję (w sieciach publicznych udostępnianie plików jest blokowane).
8. Windows 7 domyślnie ukrywa ikony, które programy próbują umieścić w obszarze powiadomień paska zadań — jeżeli chcesz, żeby znalazła się tam ikona skanera antywirusowego:
   a. Kliknij znajdujący się na pasku zadań przycisk *Pokaż ukryte ikony*.
   b. Kliknij *Dostosuj*.
   c. Znajdź ikonę skanera antywirusowego i wybierz opcję *Pokaż ikony i powiadomienia*.
9. Uruchom skaner antywirusowy — można to zrobić albo z menu *Start*, albo klikając jego wyświetloną na pasku zadań ikonę.
10. Przeskanuj cały komputer — skaner sprawdzi, czy jakikolwiek ze znajdujących się na lokalnym dysku plików nie jest zainfekowany, i jeśli znajdzie wirusy, spróbuje je usunąć z pliku (ta opcja najczęściej nazywa się wyleczeniem pliku).
11. Jeśli wyleczenie pliku będzie niemożliwe, skaner zaproponuje usunięcie całego pliku lub objęcie go kwarantanną, czyli przeniesienie do specjalnego folderu.

ĆWICZENIE

6.6 Aktualizacja bazy znanych wirusów

Skanery antywirusowe rozpoznają wirusy poprzez porównanie kodów programów z sygnaturami (cechami charakterystycznymi) znanych wirusów. **Jeżeli wykorzystywana do porównywania baza sygnatur nie będzie zawierała danych o określonych wirusach, to nie zostaną one wykryte**. Z tego powodu każdy skaner antywirusowy posiada opcję aktualizacji bazy znanych wirusów, umożliwiającą pobranie dostępnego w internecie pliku, w którym zostały zapisane sygnatury wszystkich znanych wirusów.

Jeżeli dysponujesz stałym dostępem do internetu, powinieneś codziennie aktualizować sygnatury wirusów. W innym przypadku możesz pozwolić sobie na ich aktualizację co dwa lub trzy dni, nie rzadziej jednak niż dwa razy w ciągu tygodnia.

1. Uruchom skaner antywirusowy.
2. Wybierz opcję aktualizacji bazy wirusów (w przypadku programu ESET przed aktualizacją konieczne jest podanie nazwy użytkownika i hasła).
3. Upewnij się, czy włączona jest automatyczna aktualizacja bazy znanych wirusów — większość skanerów antywirusowych aktualizuje swoje bazy według specjalnego harmonogramu i wystarczy upewnić się, czy jest on włączony.

Niechciane i fałszywe programy

Wirusy to tylko jedne z wielu niechcianych (tj. takich, których użytkownik świadomie nie uruchomiłby na swoim komputerze) programów. Obok nich do tej kategorii zaliczamy:

1. Programy szpiegowskie (ang. *SpyWare*) — ich działanie polega na zbieraniu informacji, które mogą ułatwić atak na komputer albo być wykorzystane przeciwko jego użytkownikowi, takich jak hasła do systemu operacyjnego, odwiedzanych stron internetowych czy serwerów pocztowych, numery kart kredytowych, dane o konfiguracji systemu operacyjnego czy po prostu sekwencje naciskanych przez użytkownika klawiszy.
2. Programy dodatkowe (ang. *AdWare*) — instalowane albo z darmowymi bądź demonstracyjnymi wersjami najróżniejszych programów, albo automatycznie, bez wiedzy odwiedzającego strony WWW użytkownika, programy o najróżniejszym działaniu — od wyświetlania reklam, poprzez zbieranie informacji o odwiedzanych stronach WWW, aż po zmiany w ustawieniach programów i systemu operacyjnego.
3. Konie trojańskie (ang. *Trojan horse*) — programy, które umożliwiają atakującemu przejęcie zdalnej kontroli nad komputerem.

Niektóre z takich programów są wykrywane i usuwane przez skanery antywirusowe, jednak zdecydowana większość nie jest uznawana za wirusy, co nie oznacza, że nie są one niebezpieczne. Dlatego oprócz skanera antywirusowego każdy komputer powinien być chroniony za pomocą specjalnego antyszpiegowskiego programu.

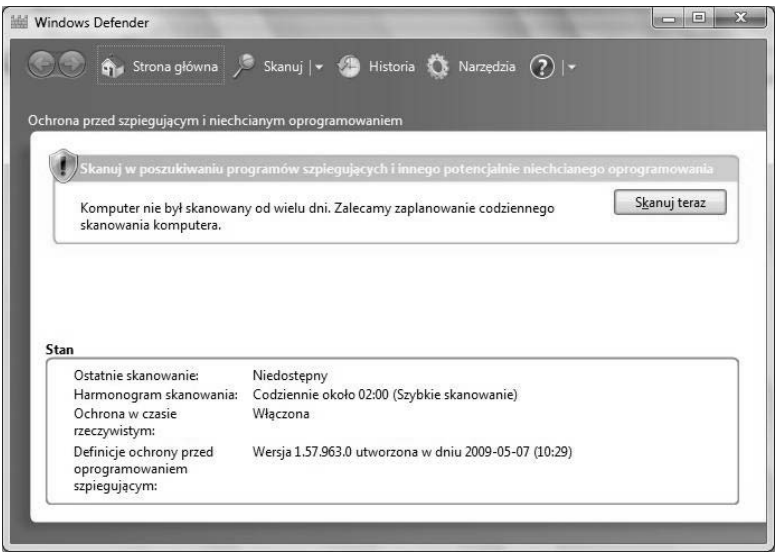
Niechciane i fałszywe programy są często dołączane do darmowych, dostępnych w internecie programów, takich jak zestawy kodeków czy odtwarzacze multimediów. Odradzamy pobieranie i uruchamianie pochodzących z niezaufanych źródeł programów — próbując zaoszczędzić kilkadziesiąt złotych, możemy stracić kontrolę nad własnym komputerem i przechowywanymi w nim danymi.

ĆWICZENIE

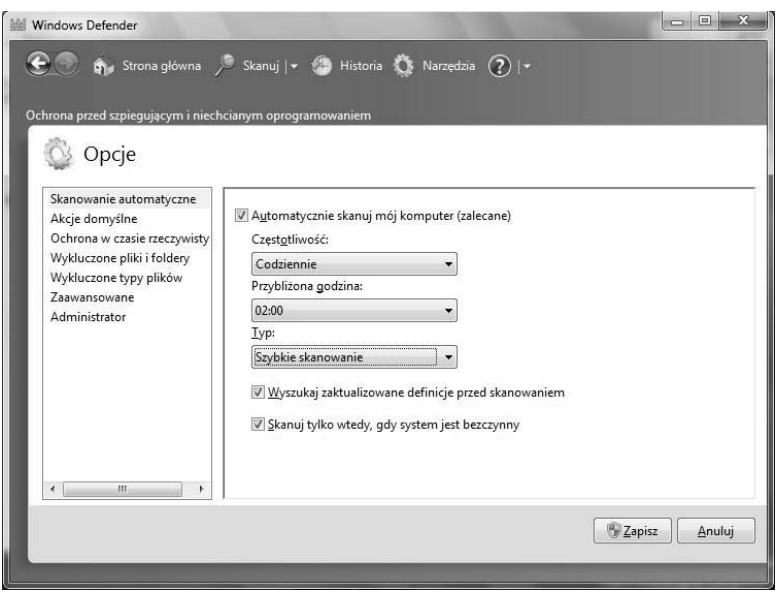
6.7 Windows Defender

Windows Defender to usługa systemu Windows 7 chroniąca go przed niechcianymi programami i niepożądanymi zmianami w jego konfiguracji.

1. Aby wyświetlić okno konfiguracyjne usługi *Windows Defender*, wyświetl główne okno *Panelu sterowania*, wpisz w polu wyszukiwania `Defender` i kliknij znaleziony odnośnik *Windows Defender*.
2. Na głównej zakładce znajdziesz informacje, na które powinieneś zwrócić szczególną uwagę (rysunek 6.13). Przy każdej z informacji znajdziesz przycisk lub wskazówki dotyczące tego, jak rozwiązać dany problem.
3. Kliknij przycisk *Skanuj teraz* — rozpocznie się wyszukiwanie niechcianych programów. Jeżeli jakieś zostaną znalezione, zaakceptuj domyślną akcję i usuń je.
4. Kliknij znajdujący się na pasku narzędzi przycisk *Narzędzia* i kliknij odnośnik *Opcje*. W tym podzielonym na sekcje oknie możesz ustawić najważniejsze opcje usługi.
5. Wybierz, o której godzinie i jak często przeprowadzany będzie test systemu, i upewnij się, czy zaznaczone jest pole sprawdzania dostępnych aktualizacji przed rozpoczęciem testów oraz czy test będzie przeprowadzany tylko w czasie bezczynności komputera (rysunek 6.14).

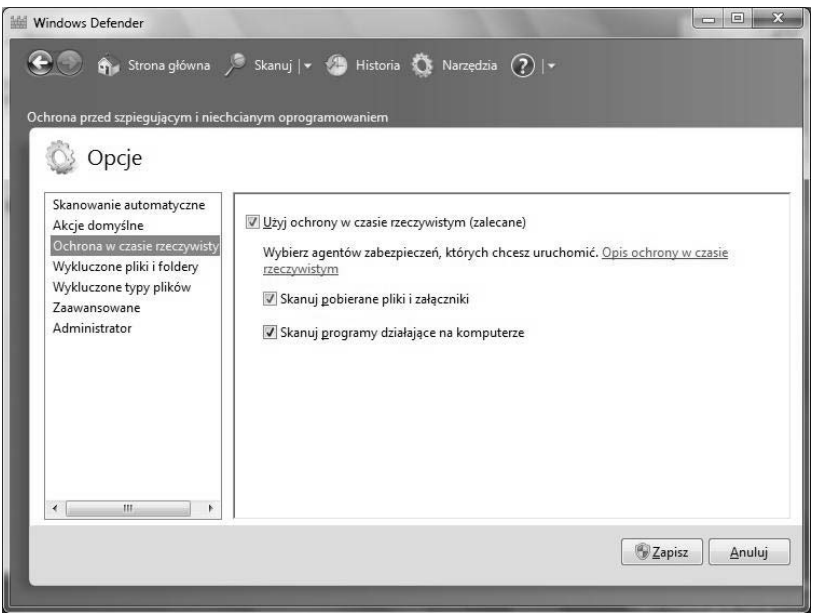


Rysunek 6.13. *W tym przypadku komputer od kilku tygodni nie był sprawdzany pod kątem obecności niechcianych programów*



Rysunek 6.14. *Jeżeli codzienne sprawdzanie komputera będzie przeprowadzane tylko w czasie jego bezczynności, to nawet tego nie zauważymy*

6. Przejdź do sekcji *Ochrona w czasie rzeczywistym* i upewnij się, że włączone są wszystkie mechanizmy ochrony systemu w czasie rzeczywistym. Jeżeli któryś z nich był wyłączony, włącz go (rysunek 6.15).



Rysunek 6.15. *Windows Defender nie tylko wyszukuje niechciane programy, ale również chroni najważniejsze składniki systemu — takie jak rejestr, sterowniki czy listę automatycznie uruchamianych programów — przed nieautoryzowanymi zmianami. To właśnie ochrona w czasie rzeczywistym jest główną zaletą tej usługi*

7. Przejdź do sekcji *Zaawansowane* i zaznacz pola wyboru *Skanuj pocztę e-mail* (to w e-mailach można znaleźć wiele niechcianych programów) oraz *Skanuj dyski wymienne* (coraz więcej niechcianych programów rozprzestrzenia się właśnie poprzez napędy USB).
8. Zatwierdź wprowadzone zmiany klawiszem *Zapisz*.