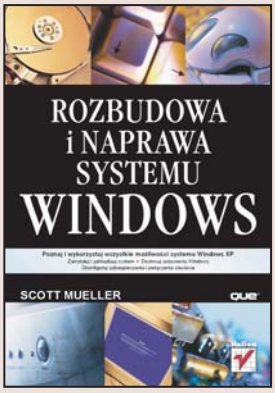
Rozbudowa i naprawa systemu Windows



Autor: Scott Mueller
Tłumaczenie: Paweł Gonera, Piotr Pilch, Przemysław Szeremiota
ISBN: 83-246-0269-0
Tytuł oryginału: Upgrading and Repairing Microsoft Windows
Format: B5, stron: 912

Poznaj i wykorzystaj wszystkie możliwości systemu Windows XP

- Zainstaluj i zaktualizuj system.
- Dostosuj ustawienia Windows.
- Skonfiguruj zabezpieczenia i połączenia sieciowe.

Windows XP jest dziś najpopularniejszym systemem operacyjnym dla komputerów PC. Korzystają z niego zarówno użytkownicy domowi, jak i przedsiębiorstwa. Jednak mimo tak ogromnej popularności, Windows XP nie posiada dokumentacji, która szczegółowo opisywałaby wszystkie jego możliwości. Większość dostępnych na rynku pozycji książkowych koncentruje się na podstawowych zagadnieniach, niemal całkowicie pomijając tematy zaawansowane oraz opisy rzadziej wykorzystywanych narzędzi i funkcji. Tymczasem coraz więcej użytkowników tego systemu wykorzystuje wiele dotychczas nieopisanych funkcji.

Książka „Rozbudowa i naprawa systemu Windows" to podręcznik kompleksowo opisujący system Windows XP. Czytając tę książkę, poznasz działanie i funkcje systemu Windows bez potrzeby przebijania się przez rozbudowane opisy najprostszych procedur. Znajdziesz tu szczegółowe omówienie procesu instalacji i aktualizacji systemu oraz konfigurowania go tak, aby pracował z największą wydajnością. Nauczysz się zarządzać kontami użytkowników, woluminami dyskowymi i sprzętem oraz dowiesz się, w jaki sposób wykonywać kopie zapasowe i przywracać z nich dane. Przeczytasz także o przystosowywaniu systemu operacyjnego Windows do pracy w sieci oraz o dobieraniu parametrów zabezpieczeń systemowych tak, aby naprawdę pomagały chronić komputer, a nie przeszkadzały użytkownikowi w pracy.

- Instalowanie systemu
- Przenoszenie ustawień z innych komputerów
- Pobieranie i instalacja aktualizacji
- Zarządzanie użytkownikami i urządzeniami
- Dostrajanie wydajności systemu
- Edycja rejestru
- Konfiguracja ustawień sieciowych
- Praca z konsolą tekstową i tworzenie plików wsadowych oraz skryptów
- Odzyskiwanie utraconych danych

Odkryj prawdziwą potęgę systemu Windows XP

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

Spis treści

Rozdział 8

Ochrona i zabezpieczenia systemu Windows

Wraz ze wzrostem liczby złośliwego oprogramowania krążącego w internecie, ochrona i zabezpieczanie komputera staje się coraz ważniejszym problemem. Dni, kiedy wystarczyło tylko zainstalować najnowsze aktualizacje zabezpieczeń dla systemu Windows, już nie wrócą. Niemal codziennie są wykrywane nowe słabe punkty w systemie bezpieczeństwa, a napisanie i przetestowanie poprawek łatających te dziury trwa w firmie Microsoft kilka dni, o ile nie tygodni. Długi czas reakcji firm produkujących oprogramowanie, połączony z tym, że większość słabych punktów nie jest powszechnie znana do momentu ataku na tysiące komputerów, powoduje, że niezbędne jest opracowanie aktywnych działań pozwalających chronić komputery działające pod kontrolą systemu Windows.

Korzystając z różnych technik i narzędzi, można znacznie zredukować możliwości ataku na komputer, nawet jeżeli zostanie wykryty nowy słaby punkt systemu.

Zastosowanie aktywnych metod ochrony komputera pozwala łatwo chronić komputer przed trzema głównymi typami zagrożeń:

- wirusami, które mogą zainfekować dokumenty, a nawet skasować ważne pliki systemu operacyjnego;
- oprogramowaniem szpiegowskim, które monitoruje działanie komputera i często jest wykorzystywane do wyświetlania irytujących reklam;
- koniami trojańskimi, które pozwalają napastnikowi uzyskać pełny dostęp do plików komputera.

Zagrożenia te są oczywiście poważnym problemem dla administratorów sieci korporacyjnych, ale również dla domowych użytkowników systemu Windows XP. Podjęcie kroków opisanych w tym rozdziale, które mają za zadanie chronić komputery z systemem Windows, jest ważnym elementem ochrony danych oraz stabilności systemu. Pierwszym z ważnych kroków jest upewnienie się, że wszystkie konta użytkowników komputera są chronione hasłami.

Hasła Windows

Hasła są pierwszą linią obrony przed lokalnymi i zdalnymi atakami na komputer. Jednak ogromna większość użytkowników domowych nie korzysta z haseł do swoich kont użytkowników w Windows. Dla niektórych jest to mało wygodne, inni nie widzą potrzeby korzystania z haseł, ponieważ ufają każdemu (rodzinie i przyjaciołom), kto ma fizyczny dostęp do komputera. Jeżeli komputer nie jest podłączony do dowolnego typu sieci, w tym do internetu, nie stanowi to problemu. Jeżeli jednak, jak większość użytkowników komputerów, podłączają się oni do internetu za pomocą łącza dowolnego typu, nawet jeżeli jest to jedynie kilka minut połączenia modemowego, pozostawiają szeroko otwarte drzwi do systemu.

Umieszczenie komputera w bezpiecznej lokalizacji (w domu, biurze i tak dalej), zapewnia zabezpieczenie fizycznego dostępu do komputera. Jednak w momencie podłączenia do internetu lub innej sieci (na przykład szerokopasmowej) potencjalnie możemy udostępnić wszystkie pliki danych całemu światu. Właściwie każdy, kto zna nazwę użytkownika, może

korzystać z takiego komputera. Nawet jeżeli nazwa nie jest znana, sprytnemu napastnikowi jej ustalenie zajmuje niewiele czasu.

Z tego właśnie powodu z roku na rok rośnie ilość przypadków kradzieży tożsamości. Wiele osób nie podejmuje żadnych kroków w celu ochrony swoich poufnych danych. Hasła ustawione dla wszystkich kont użytkowników komputera nie rozwiązują wszystkich problemów z zabezpieczeniami, ale jest to niezbędny pierwszy krok na długiej drodze do zabezpieczenia dostępu do komputera, który pozwala zamknąć drzwi napastnikom szukającym łatwej ofiary.

Jeżeli wszystkie konta użytkowników nie mają ustawionych haseł, bardzo łatwo to zmienić. Wystarczy otworzyć *Panel sterowania* i kliknąć ikonę *Konta użytkowników*. Następnie należy kliknąć nazwę konta i wybrać *Utwórz hasło*. Aby ustawić hasło użytkownika, należy kliknąć prawym przyciskiem myszy nazwę konta i wybrać *Ustawianie hasła*. Zarządzanie kontami użytkowników jest opisane w rozdziale 5., „Zarządzanie systemem Windows".

W Windows 2000 i XP można po prostu wpisać *lusrmgr.msc* w wierszu poleceń lub oknie *Uruchom* (kliknąć *Start/Uruchom*). Powoduje to uruchomienie konsoli *Użytkownicy i grupy lokalne*.

Należy pamiętać, że hasła muszą być na tyle dobre, aby napastnik nie mógł ich odgadnąć lub złamać za pomocą dowolnego programu łamiącego metodą *brute-force*. Poniżej przedstawione są cechy charakteryzujące dobre hasło:

- hasło zawiera cyfry i znaki specjalne, takie jak)(*&^%$#;
- hasło zawiera małe i wielkie litery;
- nie są używane popularne słowa;
- nie są używane dane osobiste, takie jak nazwisko, adres czy numer telefonu;
- hasło powinno mieć długość ponad 8 znaków;
- hasło należy zmieniać co najmniej dwa razy w roku.

Oprócz tych wskazówek, zalecane jest wykorzystywanie różnych haseł dla każdego z kont w sieci. Korzystanie z jednego hasła można porównać do używania jednego klucza do samochodu, domu, biura i sejfu. Jeżeli ktoś odkryje to hasło, w niebezpieczeństwie jest wiele danych osobistych oraz finansowych.

Korzystanie ze wskazówek dotyczących dobrych haseł oraz używanie różnych haseł dla każdego z kont w sieci może dać w wyniku wiele haseł do zapamiętania. Przy korzystaniu z kilkunastu kont w sieci, zapamiętanie ich wszystkich jest niemal niemożliwe. W przypadku korzystania z wielu haseł lub jeżeli ktoś ma kłopoty z ich zapamiętywaniem, można skorzystać z bezpłatnego programu o nazwie Password Safe, który jest dostępny pod adresem *http://passwordsafe.sourceforge.net/*. To przydatne narzędzie pozwala bezpiecznie przechowywać w jednej lokalizacji wszystkie hasła do używanych kont, wykorzystując do tego celu zaszyfrowany plik.

Sposób implementacji haseł przez system Windows

Wczesne wersje systemu Windows korzystały z zupełnie innej metody implementacji haseł niż systemy bazujące na systemie NT, czyli NT, 2000 i XP. W Windows 98/Me hasła były szyfrowane bardzo słabą metodą, a następnie zapisywane w pliku haseł znajdującym się w systemie plików, który był dostępny dla każdego, kto miał na to ochotę. Było to bardzo mało bezpieczne, ponieważ każdy mógł po prostu skasować plik haseł i mieć pełen dostęp do komputera.

Począwszy od Windows NT, hasła są przechowywane w bardziej bezpieczny sposób. Obecnie, w Windows 2000 oraz Windows XP Home i Professional, hasła użytkowników są przechowywane w magazynie nazywanym Security Account Manager, określanym również skrótem SAM, którego działanie jest podobne do mechanizmu ochrony haseł w systemie Unix. Baza SAM jest umieszczona w zastrzeżonej części rejestru systemowego i może być wykorzystywana tylko przez konto systemowe. Nie pozwala to użytkownikom, ani lokalnym, ani zdalnym, na uruchomienie edytora rejestru i odczytanie danych hasła. Aby jeszcze bardziej zwiększyć bezpieczeństwo, hasła są zapisywane w 128-bitowej tablicy mieszającej z algorytmem jednokierunkowym z zastosowaniem standardowej metody szyfrowania nazywanej MD4 Message Digest. Powoduje to, że hasła są bardzo trudne do złamania, nawet jeżeli ktoś w jakiś sposób uzyska dostęp do bazy SAM.

Więcej informacji na temat haseł użytkowników i zarządzania kontami znajduje się w rozdziale 5., „Zarządzanie systemem Windows”, w punkcie „Zarządzanie użytkownikami”.

Odzyskiwanie utraconego hasła

Zapomnienie hasła do konta na komputerze może być bardzo frustrujące. W Windows 2000/XP nowy mechanizm zabezpieczeń bazujący na Windows NT zastąpił bardzo mało skuteczny mechanizm używany w systemach Windows 98 i Me. W przypadku Windows 98 i Me bardzo łatwo można dostać się na dowolne konto komputera. Przy wykorzystaniu dyskietki z systemem DOS, można było skasować plik haseł Windows. Ponieważ Windows 2000 oraz XP bazują na jądrze NT, działa tu solidniejszy i bezpieczniejszy system.

System ten powoduje, że niemal niemożliwe jest zorientowanie się, gdzie są hasła użytkowników, ponieważ wszystkie dane haseł są zaszyfrowane. Teoretycznie można skorzystać z aplikacji, która będzie próbowała „złamać” szyfr danych haseł i odkryć faktyczne hasło. Jednak przy dużej liczbie bitów wykorzystywanych przez stosowane obecnie szyfry może to zająć kilka lat, o ile zostanie zastosowany najszybszy sprzęt. Jeżeli nie mamy własnego superkomputera, nie jest to właściwe rozwiązanie.

Jeżeli znamy hasło użytkownika Administrator, można zalogować się do komputera, korzystając z tego konta, i uruchomić konsolę *Użytkownicy i grupy lokalne*, wpisując w wierszu poleceń *lusrmgr.msc* (lub uruchomić ją z *Panelu sterowania*). Po tej operacji można kliknąć prawym przyciskiem myszy nazwę konta i zmienić jego hasło.

Jeżeli nie znamy hasła konta *Administrator*, jedyną możliwą metodą skorzystania z konta jest użycie programu narzędziowego, który nadpisuje dane hasła. Nie powoduje to odzyskania hasła, ale pozwala skorzystać z dowolnego konta komputera, ponieważ konta mają przypisane nowe hasła.

W Windows XP konto *Administrator* nie jest wyświetlane na ekranie powitalnym. Aby zalogować się na konto Administrator w Windows XP, należy nacisnąć kombinację klawiszy *Ctrl+Alt+Del* dwukrotnie, co powoduje wyświetlenie ekranu logowania takiego jak w Windows 2000. Następnie należy ręcznie wpisać nazwę użytkownika i hasło.

Zastosowanie programu firmy trzeciej do nadania nowego hasła jest proste, ale wymaga wykonania wielu operacji. Wszystkie te programy korzystają z podobnej metody, ale mogą być zapisywane na dyskietce lub dysku CD-ROM pozwalającym uruchomić komputer. Zazwyczaj trzeba uruchomić komputer z dyskiem narzędziowym umieszczonym w napędzie, dzięki czemu komputer uruchomi system operacyjny programu zamiast Windows. Następnie wykonywana jest zamiana haseł.

Można skorzystać z setek takich programów. Jedne są bezpłatne, inne kosztują setki dolarów. Większość z tych narzędzi działa tak podobnie, że nie warto płacić za coś, co jest powszechnie dostępne w Sieci. Osobiście wybrałem dwa programy pozwalające na zastępowanie haseł w Windows. Pierwszy wymaga uruchomienia systemu z dyskietki, drugi wypalenia płyty CD-ROM i uruchomienia komputera z tej płyty.

Zanim zaczniemy, konieczne jest poinformowanie o konsekwencjach wymiany hasła do konta użytkownika. Z powodu solidniejszego systemu zabezpieczeń w systemie Windows 2000/XP, po zamianie hasła użytkownika wszystkie zaszyfrowane pliki, foldery i zapisane hasła zostaną utracone. Pliki nadal istnieją, ale są zaszyfrowane innym kluczem niż dostępny po zmianie hasła, co powoduje, że są one niedostępne, a w praktyce stracone.

Zastosowanie dyskietki uruchomieniowej do zmiany hasła

Do zamiany haseł użytkowników z wykorzystaniem dyskietki uruchomieniowej zalecam użycie programu Offline NT Password & Registry Editor, który można pobrać z witryny *http://home.eunet.no/~pnordahl/ntpasswd/*. Choć nie jest to narzędzie najbardziej przyjazne użytkownikowi, jest jednym z najpopularniejszych i najbardziej niezawodnych programów tej klasy.

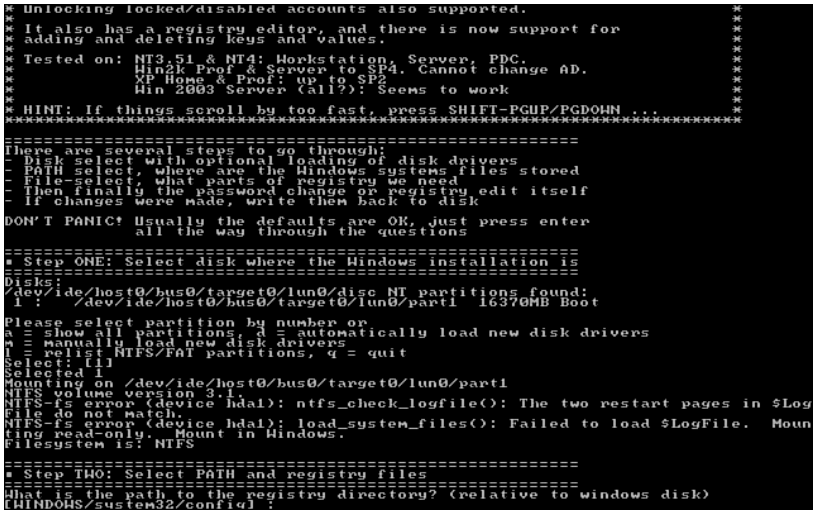
1. Na początku należy odwiedzić witrynę i pobrać obraz dysku, do którego prowadzą łącza umieszczone na dole strony. Jeżeli komputer posiada dyski SCSI, należy pamiętać o pobraniu tej wersji, która posiada sterownik obsługujący dyski tego typu.
2. Po pobraniu prawidłowej wersji należy rozpakować plik *zip* w dowolnym katalogu. Następnie w napędzie dyskietek należy umieścić pustą, sformatowaną dyskietkę i z katalogu, w którym został rozpakowany plik *zip*, uruchomić plik wsadowy *install.bat*. Gdy program poprosi o podanie litery dysku docelowego (*Target Disk Drive*), należy podać literę oznaczającą dysk skojarzony ze stacją dyskietek (zwykle jest to dysk *A*). Po potwierdzeniu wyboru napędu program rozpoczyna kopiowanie obrazu uruchomieniowego na dyskietkę.
3. Po zakończeniu tej operacji dyskietka przywracania haseł jest gotowa i można już z niej korzystać. Dyskietkę tę należy umieścić w stacji dysków komputera, którego hasła chcemy zastąpić. Następnie komputer ten należy włączyć i już powinien rozpocząć procedurę uruchamiania z dyskietki. Jeżeli komputer będzie

uruchamiał się tak jak zwykle, należy sprawdzić w ustawieniach BIOS, czy dyskietka jest pierwszym napędem w kolejności uruchamiania.

◀◀ Więcej informacji na temat tworzenia dysków do kasowania haseł znajduje się w punkcie „Lokalne konta i dyskietki resetowania hasła" — strona 248 rozdział 5.

4. Po zakończeniu ładowania programu znajdującego się na dysku, należy podać dysk, na którym jest zainstalowany system Windows. Należy podać odpowiedni numer z wyświetlonej na ekranie listy napędów. Domyślna wartość *1* powinna działać na większości instalacji Windows, szczególnie gdy system posiada tylko jeden dysk i partycję. Jeżeli nie widać żadnych napędów, należy nacisnąć *d* i *Enter*, co spowoduje załadowanie większej liczby sterowników. Po wybraniu napędu i naciśnięciu *Enter* można wykonać następną operację.

5. Następnie na ekranie pojawia się pytanie o miejsce przechowywania rejestru, co jest pokazane na rysunku 8.1. Dla Windows XP odpowiednim katalogiem jest *Windows/System32/Config*. Użytkownicy Windows 2000 powinni wpisać *Winnt/System32/Config*. Na ekranie znajduje się katalog domyślny dla Windows XP, więc jeżeli komputer działa pod kontrolą tego systemu, wystarczy nacisnąć *Enter*.



Rysunek 8.1. *Wybór lokalizacji rejestru systemowego w programie Offline NT Password & Registry Editor*

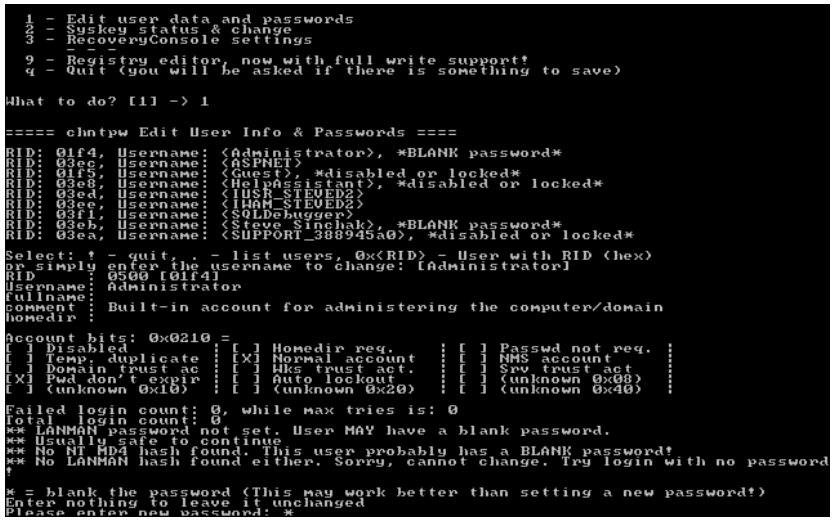
6. Następnie trzeba określić, którą część rejestru należy załadować. Ponieważ chcemy pracować na hasłach, należy nacisnąć *1*, a następnie *Enter*.

7. Powoduje to załadowanie danych haseł z rejestru. Następnie należy nacisnąć *1* (aby modyfikować dane haseł użytkowników) i *Enter*, aby zmienić hasło użytkownika.

8. Na ekranie pojawia się lista kont użytkowników utworzonych w systemie. Należy wpisać hasło użytkownika, którego hasło chcemy zmienić, i nacisnąć *Enter*. Jeżeli chcemy zmienić hasło użytkownika *Administrator*, wystarczy nacisnąć *Enter*, ponieważ jest to wartość domyślna.

9. Następnie należy podać nowe hasło lub, jak zaleca program, wprowadzić znak * jako puste hasło, co jest pokazane na rysunku 8.2 (można zawsze zmienić hasło po zalogowaniu do Windows). Aby przejść do następnego kroku, należy nacisnąć *Enter*.

Rysunek 8.2. *Wprowadzanie znaku * jako pustego hasła*



10. Aby potwierdzić wprowadzenie zmian, należy nacisnąć *y*.

11. Następnie należy zakończyć działanie programu i zapisać zmiany w rejestrze. Nacisnąć *!* i *Enter*, co spowoduje powrót do głównego menu. Następnie naciśnięcie *q* i *Enter* powoduje zakończenie pracy programu do zmiany haseł.

12. W tym momencie pojawia się pytanie o zapis zmian w rejestrze. Należy nacisnąć *y*, a następnie *Enter*. Operacja ta może potrwać kilka minut. Gdy na ekranie pojawi się komunikat ***** *Edit Complete* *****, należy wyjąć dyskietkę z napędu i ponownie uruchomić komputer.

Jeżeli wszystko zostało wykonane bezbłędnie, po uruchomieniu komputera powinniśmy mieć możliwość zalogowania się na zmieniane konto, korzystając z pustego lub wprowadzonego hasła.

Jeżeli w czasie działania programu Offline NT Password & Registry Editor na ekranie pojawiają się błędy lub aplikacja po prostu nie działa, należy zapoznać się z listą często zadawanych pytań, która znajduje się pod adresem *http://home.eunet.no/~pnordahl/ntpasswd/faq.html*.

Zastosowanie uruchomieniowego dysku CD-ROM do zmiany hasła

Jeżeli użycie dyskietki nie wchodzi w grę lub po prostu w komputerze nie ma zainstalowanej stacji dyskietek, istnieją inne narzędzia pozwalające na zresetowanie hasła użytkownika. Osobiście korzystam z zestawu narzędzi o nazwie Emergency Boot CD. EBCD to zbiór przydatnych narzędzi, których można użyć do naprawienia komputera po różnego

rodzaju katastrofach. Dostępna jest również funkcja resetowania hasła, dzięki czemu jest to świetne narzędzie dla profesjonalistów branży IT lub zaawansowanych użytkowników.

Emergency Boot CD wymaga użycia programu pozwalającego wypalać płyty CD, na przykład Nero Burning ROM firmy Ahead Software lub Easy CD Creator firmy Roxio.

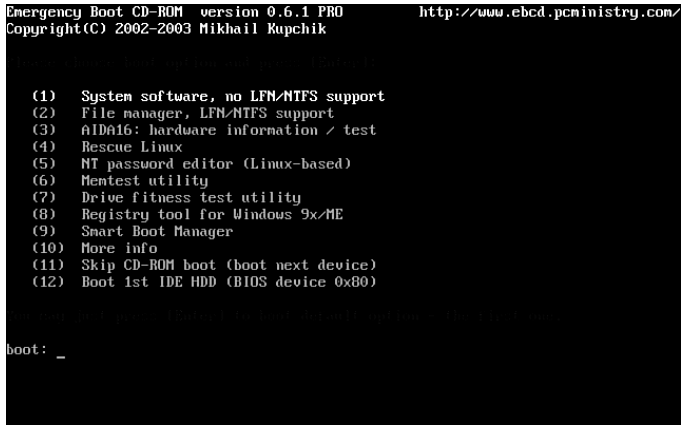
Aby stworzyć własny uruchomieniowy dysk CD-ROM i za jego pomocą zamienić hasła użytkowników, należy wykonać następujące operacje:

1. Otworzyć witrynę *http://ebcd.pcministry.com/* i pobrać z niej wersję *lite* lub *pro* dysku CD. Jedyną różnicą między tymi odmianami jest to, że wersja pro zawiera dodatkowe narzędzia, niepotrzebne do wykonania tego zadania (być może jednak okażą się one przydatne).
2. Po pobraniu odpowiedniej wersji dysku CD należy uruchomić plik, co spowoduje rozpakowanie plików na dysku. Ponieważ można określić zawartość dysku CD, nie jest jeszcze tworzony obraz dysku. Należy przejść do folderu, w którym zostały rozpakowane pliki, i uruchomić program *makeebcd.exe*, który utworzy plik obrazu.
3. Na dysku zostanie utworzony obraz ISO płyty CD. Następnie należy użyć jednego z kilku popularnych programów do nagrywania płyt CD i wypalić plik ISO na płycie CD-R lub CD-RW.
4. Po wypaleniu pliku obrazu dysku, należy włożyć utworzony dysk do komputera, na którym chcemy zmienić hasła. Uruchomić komputer, a jeżeli w BIOS-ie ustawione jest uruchamianie systemu z dysku CD, komputer powinien zamiast Windows załadować program z CD. Jeżeli komputer nie uruchomi się z dysku CD, należy sprawdzić, czy BIOS jest właściwie skonfigurowany i czy obsługuje uruchamianie z napędu CD-ROM.

Więcej informacji na temat BIOS-u oraz procesu uruchamiania systemu Windows znajduje się w rozdziale 4., „Uruchamianie systemu Windows”.

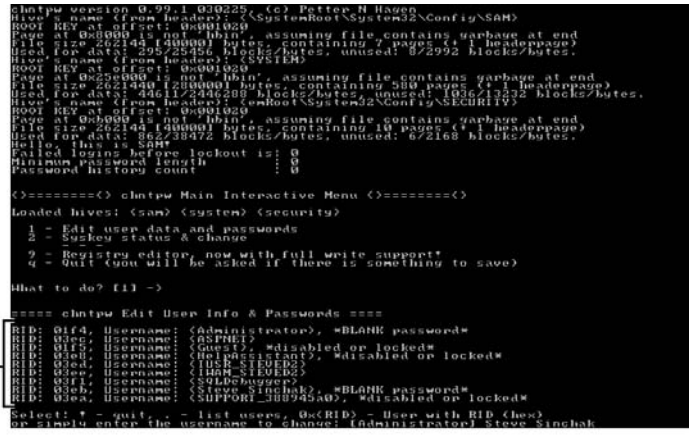
5. Gdy komputer uruchomi się z dysku CD, należy uruchomić NT Password Utility przez naciśnięcie *5* a następnie *Enter*, jak jest to pokazane na rysunku 8.3.
6. Po załadowaniu programu należy nacisnąć *Enter*, aby zamknąć ekran powitalny. Następnie wyświetlane jest pytanie o wykonanie wykrywania dysków SCSI; jeżeli w komputerze nie są zamontowane dyski SCSI, należy nacisnąć *n*, a następnie *Enter*.
7. Na ekranie zostanie wyświetlona lista partycji dyskowych. Należy podać pełną nazwę partycji, na której jest zainstalowany system Windows, i nacisnąć *Enter*. Większość użytkowników może po prostu nacisnąć *Enter*, co spowoduje wybranie wyświetlanej na ekranie domyślnej partycji */dev/hda1*.
8. Następnie należy podać położenie danych rejestru Windows (porównać z krokiem 5. z poprzedniego punktu). Ponownie większość użytkowników może nacisnąć *Enter*, co powoduje wybranie wyświetlanego na ekranie katalogu *Windows/System32/Config* — domyślnego dla systemu Windows XP.

Rysunek 8.3. *Wybranie opcji 5 z Emergency Boot CD-ROM powoduje uruchomienie edytora haseł*



9. Następnie należy podać *hive*, czyli lokalizację rejestru, do edycji. Domyślna wartość jest taka sama dla wszystkich, więc można po prostu nacisnąć *Enter*.
10. Aby edytować hasła, należy wybrać opcję *1* i nacisnąć *Enter*.
11. Wpisać nazwę użytkownika, którego hasło należy zmienić, i nacisnąć *Enter* (patrz rysunek 8.4).

Rysunek 8.4. *Użycie dysku Emergency Boot CD do zmiany hasła konta użytkownika Windows*



12. Aby wprowadzić puste hasło, należy wpisać znak *, a następnie nacisnąć *Enter*. Można również wpisać nowe hasło, ale program zaleca ustawienie pustego hasła.
13. Na ekranie potwierdzenia należy nacisnąć *Y* oraz *Enter*. Aby wyjść z trybu edycji haseł, należy nacisnąć *!* i *Enter*, a aby zakończyć aplikację NT Password, należy wpisać `q` i nacisnąć *Enter*, co spowoduje zapisanie zmian.
14. Następnie należy jeszcze dwa razy nacisnąć *Y*, aby potwierdzić zapisanie zmian w rejestrze. Po wykonaniu tej operacji zadanie jest zakończone.

Po wykonaniu operacji resetowania hasła dla konta dobrze jest zalogować się i zmienić hasło na takie, które spełnia wspomniane wcześniej zalecenia, dzięki czemu dane pozostaną bezpieczne.

Usługa Windows Update

Jak zostało to wspomniane na początku rozdziału, cały czas są odkrywane nowe słabe punkty Windows. Z tego powodu ważnym zadaniem jest stała aktualizacja systemu, co zabezpiecza nas przed wykorzystaniem przez kogoś nowo odkrytych słabych punktów. Korzystając z bezpłatnych usług takich jak Microsoft Windows Update można łatwo utrzymywać aktualność oprogramowania komputera. Dodatkowo system Windows XP może być tak skonfigurowany, aby automatycznie szukał aktualizacji i sam pobierał poprawki, bez konieczności wykonywania dodatkowych operacji.

Krótka historia bezpieczeństwa systemu Windows

W całej historii systemu Windows, Microsoft musiał uruchomić kilka metod usuwania różnych problemów z bezpieczeństwem, jakie były wykrywane w jego systemach. Po wykryciu zagrożenia zaczynała się praca nad opracowaniem łatki usuwającej ten problem. Po przejściu łatki przez wewnętrzne testy, Microsoft udostępniał ją poprzez Windows Update lub Microsoft TechNet. Z czasem ta metoda udostępniania poprawek zabezpieczeń została zmieniona z losowych wydań w czasie miesiąca na udostępnianie wielu poprawek naraz. Obecnie Microsoft udostępnia poprawki raz w miesiącu, chyba że niezbędne jest natychmiastowe opublikowanie poprawki.

Co około dwa lata Microsoft zbiera wszystkie poprawki zabezpieczeń oraz dodatkowe funkcje opracowane w tym czasie i udostępnia je wszystkie razem w dużym pakiecie nazywanym service pack. Pakiet ten pozwala na znacznie prostszą aktualizację systemu, który nie był nigdy łatany, ponieważ konieczne jest zainstalowanie tylko jednej aktualizacji, a nie kilkudziesięciu pojedynczych poprawek i dodatkowych pakietów oprogramowania. Ostatnio Microsoft wykorzystuje pakiety service pack, takie jak Windows XP Service Pack 2, do wprowadzania do systemu operacyjnego poważnych zmian. W przypadku Windows XP Service Pack 2 wiele komponentów Windows zostało zmienionych, aby działały w bardziej bezpieczny sposób, oraz dodane zostały nowe funkcje, takie jak bardziej inteligentna zapora, która zapewnia lepszą ochronę komputera.

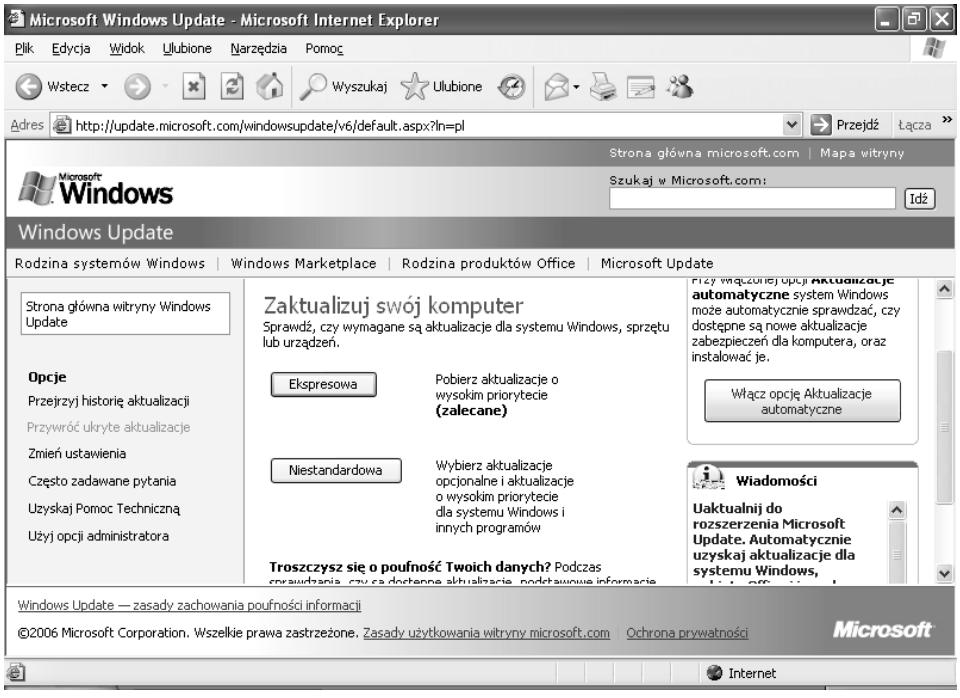
Usługa Windows Update jest wartościowym narzędziem pomagającym w pobieraniu miesięcznych poprawek zabezpieczeń udostępnianych przez Microsoft (jak również pojawiających się czasami krytycznych aktualizacji). Wykorzystując Windows Update, zapewniamy, że komputer będzie miał instalowane aktualizacje od razu po ich udostępnieniu, co minimalizuje czas, przez który komputer jest potencjalnie wrażliwy na ataki.

Użycie Windows Update

Usługa Windows Update jest bardzo prosta w użyciu. Może być wykorzystywana przez system Windows na kilka sposobów. Można wywołać ją, korzystając ze skrótu Windows Update znajdującego się na górze menu *Start/Wszystkie Programy*, przez otwarcie programu Internet Explorer i wybranie *Narzędzia/Windows Update* lub przez przejście bezpośrednio do witryny *www.WindowsUpdate.com*.

Jeżeli witryna ta dawno nie była odwiedzana lub jest otwierana po raz pierwszy, może być konieczne zainstalowanie specjalnej kontrolki wykrywającej poprawki, jakie muszą być zainstalowane na danym komputerze. Kontrolka ta jest często aktualizowana, więc w dłuższym okresie może być konieczne wielokrotne wyrażanie zgody na jej instalację.

Po załadowaniu witryny i inicjalizacji kontrolki dostępne są dwie opcje, *Ekspresowa* i *Niestandardowa*, które pozwalają ręcznie zainstalować na komputerze najnowsze poprawki zabezpieczeń i dodatkowe aplikacje, co jest pokazane na rysunku 8.5.



Rysunek 8.5. *Opcje Windows Update*

Jeżeli nie mamy czasu lub nie chcemy się zastanawiać, które aktualizacje należy zainstalować i dlaczego, należy wybrać instalację ekspresową. Wybór instalacji niestandardowej pozwala sprawdzić dokładnie, które aktualizacje są dostępne dla danego systemu, i wybrać opcje do instalacji. Osobiście korzystam z instalacji niestandardowej, ponieważ lubię sprawdzać, jakie poprawki są dostępne.

Po wybraniu metody aktualizacji komputera, usługa Windows Update uruchamia program aktualizacji, który wyszukuje poprawki odpowiednie dla danego komputera. Jeżeli są dostępne aktualizacje, są one wyświetlane. Jeżeli zostanie wybrana opcja instalacji ekspresowej, wystarczy kliknąć przycisk *Instaluj* i rozpocznie się proces instalacji wszystkich dostępnych aktualizacji. Jeżeli zostanie wybrana instalacja niestandardowa, należy przejrzeć dostępną listę aktualizacji i kliknąć przycisk *Dodaj* dla każdej aktualizacji, którą chcemy pobrać i zainstalować na komputerze. Po zakończeniu wybierania należy kliknąć przycisk *Instaluj*.

Spowoduje to uruchomienie programu pobierającego, który automatycznie pobierze aktualizacje i jedna po drugiej je zainstaluje. Jeżeli będzie potrzebne ponowne uruchomienie komputera, będzie można wybrać opcję natychmiastowego przeładowania systemu lub odłożenia tej operacji na później.

Czasami musi być zainstalowana aktualizacja samej usługi Windows Update, bez pobierania żadnych innych aktualizacji. W takim przypadku można zauważyć, że usuwane jest zaznaczenie wszystkich pozostałych aktualizacji i nie można zaznaczyć żadnej innej. W takim przypadku należy pobrać i zainstalować tę jedną aktualizację i wykonać wymagane ponowne uruchomienie systemu. Po przeładowaniu systemu należy ponownie uruchomić usługę Windows Update i zaznaczyć pozostałe aktualizacje, które powinny zostać zainstalowane.

Więcej informacji na temat Windows Update oraz pakietów Windows Service Pack znajduje się w rozdziale 2., „Instalowanie Windows".

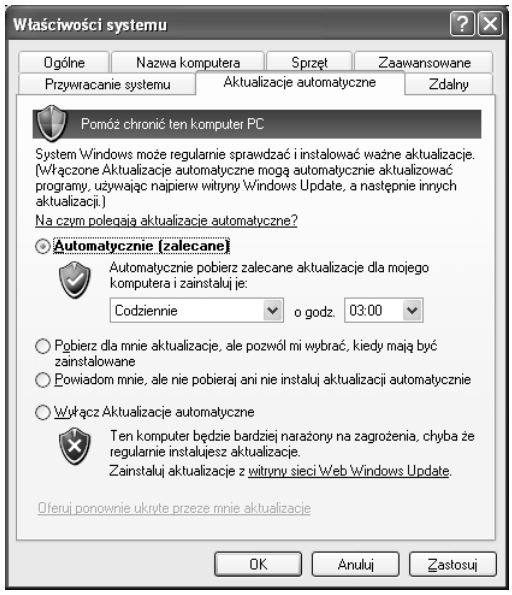
Konfiguracja aktualizacji automatycznych

Aktualizacja automatyczna to jedna ze świetnych funkcji Windows XP, która była rozszerzana w kolejnych pakietach service pack. Konfiguracja systemu, aby automatycznie się aktualizował, jest najlepszą metodą pobierania najnowszych poprawek zabezpieczeń, a jeżeli zainstalowany jest Service Pack 2, jest to bardzo łatwe do wykonania.

Jeżeli na komputerze nie jest jeszcze zainstalowany Windows XP Service Pack 2, należy ręcznie uruchomić Windows Update, co jest opisane we wcześniejszej części rozdziału, i wybrać service pack do zainstalowania. Aktualizacja ta zawiera wiele mechanizmów zabezpieczeń i poprawia działanie wielu funkcji Windows XP.

Jeżeli nie był wcześniej instalowany Windows XP Service Pack 2, w ostatniej fazie instalacji można włączyć opcję automatycznej aktualizacji. Jeżeli opcja ta nie została włączona w czasie instalacji, można w dowolnym momencie ją uaktywnić, korzystając z następującej procedury:

1. Otworzyć *Panel sterowania*, klikając *Start/Panel sterowania*.
2. Jeżeli nie jest włączony widok klasyczny, należy go włączyć przez kliknięcie łącza *Przełącz do widoku klasycznego*, które znajduje się w lewym panelu. Następnie kliknąć ikonę *System*, co spowoduje otwarcie okna *Właściwości systemu*.
3. Następnie kliknąć zakładkę *Aktualizacje automatyczne*, aby pokazać ustawienia aktualizacji, jak jest to pokazane na rysunku 8.6. Na tym ekranie mamy cztery różne opcje aktualizacji. Można tu wybrać, aby system Windows:
   - w wyznaczonym czasie w pełni automatycznie pobierał i instalował aktualizacje,
   - automatycznie pobierał aktualizacje, ale żądał potwierdzenia instalacji,
   - tylko informował o nowych aktualizacjach,
   - nie korzystał z automatycznych aktualizacji.



Rysunek 8.6. *Na zakładce Aktualizacje automatyczne okna dialogowego Właściwości systemu można określać sposób aktualizacji systemu Windows XP*

Jako absolutne minimum należy przyjąć automatyczne pobieranie najnowszych aktualizacji i informowanie w momencie, gdy są gotowe do instalacji. Najlepszym rozwiązaniem jest automatyczne pobieranie i instalowanie aktualizacji przez system Windows.

4. Po wybraniu metody aktualizacji należy kliknąć *OK*.

Większość użytkowników wie, że aktualizacje automatyczne są świetną funkcją w Windows XP, ale wielu z nich nie wie lub zapomina wykorzystać fakt, że Microsoft posiada podobne usługi aktualizacji innych programów, takich jak pakiet Office. Wysoce zalecane jest odwiedzanie witryny Microsoft Update, która jest nową centralną lokalizacją dla poprawek do wszystkich produktów firmy Microsoft, dzięki czemu można być pewnym, że poprawione zostaną również znane słabe punkty we wszystkich produktach firmy Microsoft. Usługa Microsoft Update jest dostępna poprzez główną stronę witryny *http://www.microsoft.com*.

Aktualizacja całego oprogramowania, zaczynając od systemu operacyjnego, jest bardzo ważna dla zabezpieczania komputera. Jeżeli nawet system operacyjny jest bezpieczny, słaby punkt w dowolnej aplikacji działającej w tym systemie pozwoli napastnikowi znaleźć inne wejście do systemu.

Zapory sieciowe

W momencie gdy komputer w dowolny sposób zostaje podłączony do internetu, staje się narażony na niemal dowolne ataki z tego źródła. Każdy, kto zna adres IP takiego komputera lub skanuje bloki adresów IP, może wykorzystać znane i nieznane słabe punkty do włamania się do danej instalacji Windows. Dosyć często nasze komputery są skanowane przez

wirusy i konie trojańskie, które zainfekowały inne komputery i teraz próbują rozprzestrzenić się na kolejne systemy.

Adres IP to wartość przydzielona komputerowi przez dostawcę usług internetowych w celu identyfikacji tego komputera w sieci lokalnej lub rozległej (takiej jak internet). Więcej informacji na temat adresów IP znajduje się w rozdziale 7., „Sieć w Windows".

Bardzo duża część ruchu w internecie jest generowana przez trojany, wirusy i napastników. Aplikacje, które filtrują większość tych śmieci i nie pozwalają tym programom na dostanie się do właściwego systemu operacyjnego, są nazywane zaporami sieciowymi (często określane są też jako firewalle). Te bardzo inteligentne programy ściśle współpracują z różnymi warstwami oprogramowania realizującego komunikację sieciową. Gdy dane są przesyłane w sieci za pośrednictwem jednego z popularnych protokołów, pomiędzy komputerami jest zestawiane połączenie między określonymi numerami portów. Na przykład, gdy otwieramy witrynę, komputer podłącza się do portu 80 w komputerze, na który wskazuje nazwa domeny. Program zapory blokuje możliwość podłączenia się do wszystkich portów komputera poza tymi, które użytkownik rozmyślnie odblokował.

Przez zastosowanie zapory można znacznie ograniczyć liczbę sposobów ataku na komputer z internetu. Nawet jeżeli zostaną odkryte nowe słabe punkty, zastosowanie zapory może ochronić komputer, ponieważ napastnik lub wirusy nie będą w stanie podłączyć się do tego portu komputera, w którym istnieje słaby punkt, bo połączenie zostanie zablokowane przez zaporę. Jak widać, zapora jest jednym z najlepszych sposobów ochrony przed atakami z internetu.

Na rynku są dostępne dwie różne odmiany zapór: zapory sprzętowe oraz zapory programowe. Zapory sprzętowe i programowe zachowują się i działają podobnie; różnią się one tym, że zapora sprzętowa jest osobnym fizycznym urządzeniem zainstalowanym w sieci, które filtruje cały ruch sieciowy wchodzący do sieci. Zapory programowe są specjalnymi aplikacjami, które działają na danym komputerze, korzystając z systemu operacyjnego. Zaletą zapór sprzętowych jest to, że mogą chronić wiele komputerów, natomiast zapory programowe mogą chronić tylko ten komputer, na którym są zainstalowane. W tej książce zajmiemy się wyłącznie zaporami programowymi.

Jak zapory programowe chronią komputer przed atakami?

Wszystkie zapory programowe działają na tej samej zasadzie. Wszystkie dane kierowane do komputera i wychodzące z niego przechodzą przez *porty*. Program zapory programowej monitoruje te porty i pozwala na ruch tylko w tych portach, które zostały włączone, a komunikacja w pozostałych portach jest blokowana. Gdy zdalny komputer próbuje podłączyć się do komputera na porcie blokowanym przez zaporę, nie da się zestawić połączenia. Większość zapór programowych domyślnie nie ma żadnych otwartych portów, czyli wszystkie są zablokowane. Zabezpiecza to komputer przed atakami, ponieważ nawet jeżeli komputer posiada znaną dziurę w systemie bezpieczeństwa, zdalny komputer próbujący ją wykorzystać nie może się wcale podłączyć.

Oczywiście blokowanie wszystkich portów w systemie przez cały czas jest niepraktyczne. Całkowite zablokowanie całego ruchu w systemie będzie powodowało problemy z każdą

aplikacją, która wykorzystuje sieć LAN lub internet, w tym przeglądarek, komunikatorów lub gier sieciowych. Możliwe jest więc otwarcie portów, co pozwala na realizację potrzebnej komunikacji sieciowej. Większość zapór pozwala na ustawianie uprawnień dla określonych programów dla określonych portów i blokowanie pozostałych portów. Jednak gdy otworzymy port, mogą być przez niego przesyłane zarówno dobre, jak i złe dane.

Aby zwalczyć ten problem, większość nowoczesnych zapór posiada funkcję nazywaną *inspekcją pakietów*. Mechanizm inspekcji pakietów analizuje pakiety przechodzące przez port, szukając w nich śladów wykorzystania znanych słabych punktów. Jest to dobra funkcja, ponieważ pomaga chronić komputer nawet w przypadku otwarcia znanych słabych punktów po otwarciu portów w zaporze. Obecnie zapora dostarczana w systemie Windows XP nie posiada tej funkcji.

Większość zapór programowych innych firm analizuje nie tylko ruch wchodzący, ale również wysyłane dane. Jest to ważna funkcja, ponieważ istnieje wiele sposobów na zainfekowanie systemu przez wirusa lub konia trojańskiego, które to programy później wysyłają dane do internetu. Zapora monitorująca ruch wychodzący blokuje wszystkie nieznane transmisje do momentu, gdy użytkownik zezwoli na nie.

Konfigurując zaporę programową należy pamiętać, że najlepszą zasadą jest blokowanie wszystkiego. Należy otworzyć tylko te porty, których niezbędnie potrzebujemy!

Zapora systemu Windows

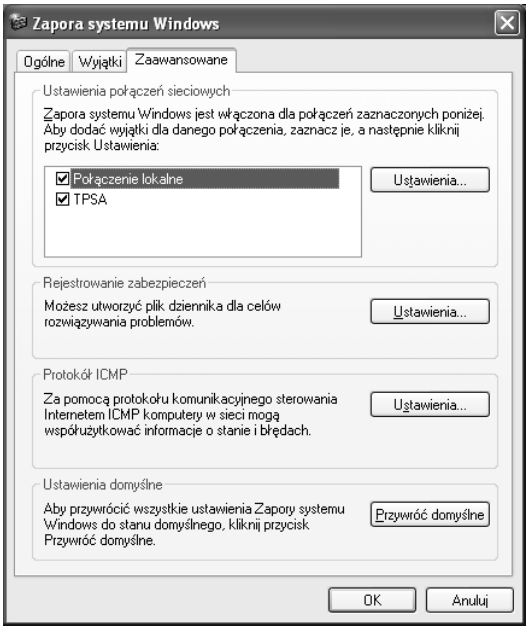
Każdy użytkownik podłączony do internetu powinien mieć uruchomioną jakąkolwiek zaporę chroniącą komputer przed zewnętrznym światem. Zapora systemu Windows jest świetnym rozwiązaniem dla większości użytkowników komputerów.

Windows XP był wyposażony w zaporę już w momencie jego wypuszczenia na rynek i był to pierwszy system operacyjny Windows wyposażony w takie oprogramowanie. Jednak ponieważ zapora nie była domyślnie włączona, wielu użytkowników nie wiedziało, że można było za jej pomocą chronić komputer. Początkowo była ona znacznie słabsza niż dostępne zapory innych firm. W Windows XP Service Pack 2 do zapory wprowadzono wiele zmian. Stała się ona znacznie lepsza i bardziej efektywna. Dodatkowo znacznie łatwiej ją włączyć, ponieważ użytkownicy mieli możliwość wykonania tej operacji w czasie instalacji Service Pack 2.

Zapora systemu Windows jest bardzo prosta, jeżeli porówna się ją do pozostałych programów. Bardziej zaawansowane zapory nie tylko monitorują ruch przychodzący, ale również ruch wychodzący i mogą informować, jeżeli jakiś program, na przykład program kradnący nasze informacje osobiste, próbuje wysłać dane bez naszej wiedzy.

Jeżeli na komputerze nie została jeszcze włączona zapora systemu Windows, bardzo łatwo można ją aktywować. Na początek należy upewnić się, że komputer korzysta z systemu Windows XP z zainstalowanym pakietem Service Pack 2. Następnie należy otworzyć *Panel sterowania* w widoku klasycznym i kliknąć ikonę *Zapora systemu Windows*. Wybrać *Włącz* i kliknąć *OK*.

Konfiguracja zapory systemu Windows jest również bardzo prosta, ponieważ jest to podstawowa zapora. Aby skonfigurować jej opcje, należy ponownie otworzyć ustawienia zapory za pomocą ikony w *Panelu sterowania* i wybrać zakładkę *Zaawansowane*. Określa się tu, które połączenia mają być chronione przez zaporę, ustawienia portów dla każdego połączenia, ustawienia protokołu ICMP, dane rejestrowania, możliwe jest też przywrócenie domyślnych ustawień; okno to jest pokazane na rysunku 8.7.



Rysunek 8.7. *Zaawansowane funkcje zapory systemu Windows*

Ustawienia indywidualnych połączeń

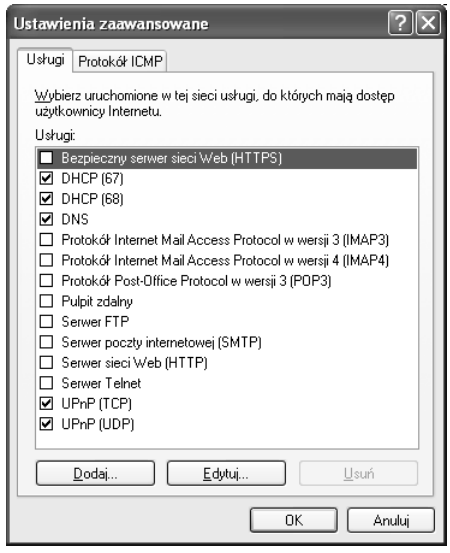
Każde z połączeń sieciowych, które ma włączoną zaporę, może być konfigurowane osobno i może mieć inne otwarte i zamknięte porty. Pozwala to uruchamiać na komputerze różne usługi, na przykład serwer FTP lub WWW, i zezwolić na dostęp z zewnętrznej sieci do wybranych danych z komputera chronionego zaporą.

Jeżeli komputer posiada więcej niż jedno połączenie, na przykład sieć przewodową i bezprzewodową, można skonfigurować je osobno, dzięki czemu można otworzyć porty tylko w połączeniu wykorzystywanym przez określoną aplikację, co zwiększa poziom bezpieczeństwa. Na przykład, będąc w domu i korzystając z połączenia kablowego, można grać na komputerze w gry sieciowe, które wymagają otwarcia określonych portów. Otwarcie tych samych portów dla połączenia bezprzewodowego nie jest w tej sytuacji potrzebne i tworzy słaby punkt w systemie bezpieczeństwa.

Aby umożliwić komputerom w sieci korzystanie z usług uruchomionych na danym komputerze, należy otworzyć „dziury" w zaporze, co powoduje, że ruch na danych portach nie jest filtrowany. Otwarcie portów w zaporze systemu Windows jest bardzo proste. Należy otworzyć okno ustawień zapory i przejść na zakładkę *Zaawansowane*, zaznaczyć na liście połączenie, dla którego chcemy wykonać operację, i kliknąć przycisk *Ustawienia*. Powoduje

to wyświetlenie okna *Ustawienia zaawansowane*, pokazanego na rysunku 8.8, gdzie wymienione są predefiniowane usługi, których zaznaczenie powoduje otwarcie dostępu w zaporze.

Rysunek 8.8. *Ustawienia usług zapory systemu Windows*



Aby otworzyć dostęp do usługi, należy zaznaczyć kratkę obok tej usługi, o ile znajduje się ona na liście. Jeżeli w liście nie ma interesującej nas usługi, należy utworzyć nową pozycję, klikając przycisk *Dodaj*.

Po kliknięciu przycisku *Dodaj* należy w polu *Opis usługi* podać nazwę aplikacji otwierającej port. Następnie potrzebny numer portu należy wpisać w polach dla portu wewnętrznego i zewnętrznego i kliknąć *OK* (port ten powinien być specyficzny dla producenta oprogramowania).

Ustawienia protokołu ICMP

Nazwa ICMP jest skrótem od Internet Control Message Protocol, co oznacza protokół wykorzystywany zwykle przez administratorów systemu do monitorowania i diagnozowania problemów z siecią. Niestety, polecenia te mogą być wykorzystywane również do tworzenia nadmiernego ruchu w sieci, co powoduje znaczny spadek szybkości działania. Jednym z najpopularniejszych poleceń ICMP, o którym prawdopodobnie wszyscy słyszeli, jest polecenie `ping`.

Polecenie to, pokazane na rysunku 8.9, może być bardzo przydatne do testowania i konfigurowania sieci lokalnej lub połączenia internetowego, ale nie ma praktycznego zastosowania w normalnej pracy i korzystaniu z internetu.

Z powodu natury działania tego polecenia najlepiej zablokować je w zaporze, chyba że czasami jest ono wykorzystywane. Aby wyłączyć polecenie `ping`, na zakładce `Zaawansowane` okna właściwości zapory Windows należy kliknąć przycisk *Ustawienia* znajdujący się w sekcji *Protokół ICMP*. Następnie należy zaznaczyć lub usunąć zaznaczenie dla różnych typów komunikatów.

Rysunek 8.9. *Ustawienia protokołu ICMP dla zapory systemu Windows*

Ograniczenia zapory systemu Windows

Zapora systemu Windows jest bardzo mało zaawansowana. Monitoruje ona jedynie ruch przychodzący i nie pozwala na monitorowanie ruchu wychodzącego, na co pozwalają inne programowe zapory. Dodatkowo, zapora nie posiada zaawansowanej funkcji analizy pakietów, która pozwala sprawdzić, co faktycznie jest przesyłane. Funkcja ta jest dostępna w bardziej zaawansowanych produktach innych firm. Pomimo tego, że zapora systemu Windows posiada swoje ograniczenia, nadal jest bardzo pomocna przy zabezpieczaniu komputera i oferuje znacznie lepszą ochronę, niż mamy w przypadku, gdy z niej nie korzystamy.

Zapory innych firm

Na rynku jest dostępnych bardzo dużo różnych zapór programowych. Większość z tych programów jest płatna, ale oferuje znacznie wyższy poziom ochrony niż zapora systemu Windows dostarczana w Windows XP. Niektórymi z często spotykanych funkcji zapewniających wyższy poziom ochrony są:

- Systemy wykrywania włamań. Są to zaawansowane systemy inspekcji pakietów, szukające sygnatur „złych" danych, które są przesyłane na chroniony komputer.
- Monitorowanie komunikacji procesów. System PCM kontroluje dane przesyłane między usługami działającymi na danym komputerze.
- Monitorowanie danych wychodzących. Zapory z tą funkcją kontrolują wszystkie dane wysyłane z chronionego komputera. Wiele zapór blokuje tylko dane wchodzące, ale zapory z tą funkcją mogą również blokować dane wychodzące. Może być to szczególnie przydatne, jeżeli na komputerze zostanie zainstalowane oprogramowanie szpiegujące. W takim przypadku program szpiegujący nie będzie w stanie wysłać do swojego właściciela naszych danych osobistych.

Norton Personal Firewall 2005

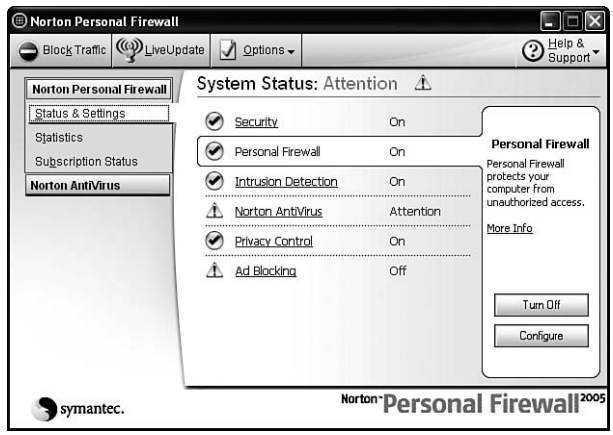
Norton Personal Firewall, dostępny jako część pakietu aplikacji Norton Internet Security, jest jednym z najpopularniejszych zapór wykorzystywanych do ochrony Windows. Posiada on wszystkie funkcje dostępne w zaporze systemu Windows, a dodatkowo inteligentne filtrowanie pakietów, system wykrywania włamań oraz monitorowanie całego ruchu wychodzącego, co zapewnia, że żaden z naszych plików ani inne ważne dane nie zostaną wysłane do internetu bez naszej wiedzy.

W wersji Norton Personal Firewall 2005 zostały dodane nowe funkcje pomagające chronić użytkowników przed rosnącą liczbą nadużyć typu *phishing scams*. W przypadku Norton Personal Firewall 2005, gdy osobiste dane są wysyłane do witryny, zapora kontroluje, czy dane trafią do witryny, która jest skonfigurowana jako zaufana. Teraz, gdy użytkownik otrzyma jedną z tych fałszywych przesyłek e-mail i weźmie ją za prawdziwą, zapora zauważy nadużycie.

Phishing scam to fałszywa witryna, która ma za zadanie oszukać użytkownika i spowodować, aby podał swoje dane osobiste, na przykład numer PESEL lub numer konta bankowego. Innym atakiem typu *phishing scam* jest przesyłka e-mail od osoby przedstawiającej się jako przedstawiciel banku, w której użytkownik jest proszony o zalogowanie się na witrynie i sprawdzenie danych konta. Po kliknięciu łącza uruchamiana jest nie prawdziwa witryna, ale fałszywa, wyglądająca bardzo podobnie.

Użycie programu Norton Personal Firewall jest dosyć proste. Po zainstalowaniu aplikacji, jej główny interfejs jest integrowany z pozostałymi programami firmy Symantec, zainstalowanymi na tym komputerze. Na rysunku 8.10 pokazany jest główny ekran programu Norton Personal Firewall zintegrowany z Norton AntiVirus.

Rysunek 8.10. *Norton Personal Firewall*

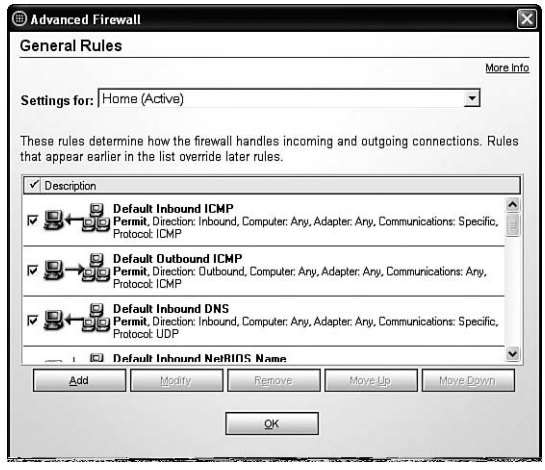


W porównaniu z innymi programami zapór, konfigurowanie Norton Personal Firewall jest bardzo proste. Wystarczy zaznaczyć w głównym oknie programu obszar programu, jaki należy skonfigurować, i kliknąć przycisk *Configure*.

Konfiguracja zapory może być wykonywana osobno dla lokalizacji, co jest bardzo przydatne w przypadku laptopów, które są przenoszone pomiędzy różnymi sieciami. Oczywiste

jest, że chcemy, by laptop działający w publicznej sieci Wi-Fi w kawiarni był lepiej zabezpieczony niż w firmowej sieci korporacyjnej. Dodatkowo, nasze potrzeby mogą być różne w różnych lokalizacjach, więc dużą zaletą jest możliwość konfigurowania otwartych portów zapory w zależności od lokalizacji.

Aby ułatwić zarządzanie zaporą, w ustawieniach konfiguracji dostępne są wstępnie skonfigurowane poziomy bezpieczeństwa. Jednak otwarcie specyficznego portu dla usługi, na przykład serwera WWW lub FTP, jest nieco trudniejsze i ukryte w aplikacji. Aby otworzyć specyficzny port, należy na głównym ekranie wybrać Personal Firewall i po kliknięciu przycisku *Configure* przejść na zakładkę *Advanced* i kliknąć przycisk *General*. Na tym ekranie należy kliknąć przycisk *Add* widoczny na rysunku 8.11 i dodać reguły do wybranych ustawień połączenia sieciowego. Tworzenie nowej reguły pozwalającej otworzyć wybrany port w zaporze ułatwia prosty w użyciu kreator.



Rysunek 8.11. *Otwarcie portu w zaporze Norton Personal Firewall*

Norton Personal Firewall nie jest dostępny za darmo, ale jego cena kształtuje się w dolnym zakresie dla komercyjnych zapór. Choć posiada niektóre z najlepszych funkcji komercyjnych zapór programowych, brakuje mu elastyczności i kontroli nad regułami zapory, z jakiej można korzystać w innych zaporach.

Próbną wersję, jak również więcej informacji na temat programu Norton Personal Firewall, można znaleźć na witrynie *http://www.symantec.com*.

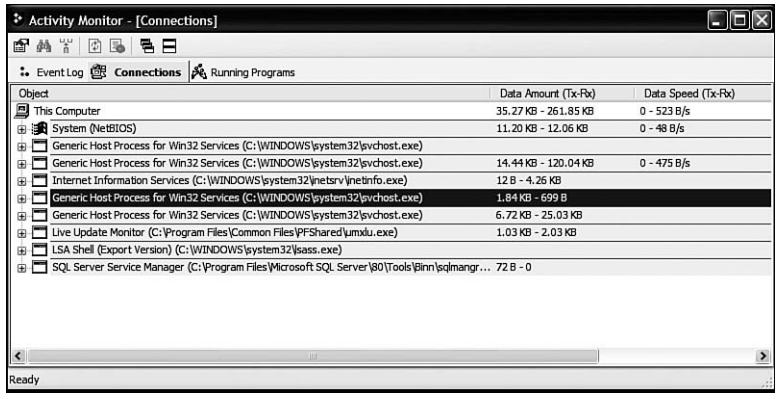
Tiny Personal Firewall Professional 2005

Tiny Personal Firewall jest zaawansowaną zaporą przeznaczoną dla użytkowników, którzy żądają pełnej kontroli nad konfigurowaniem zasad ruchu, zarówno dla pakietów przychodzących, jak i wychodzących. Program ten jest produkowany przez firmę Tiny Software i może być pobrany z witryny *http://www.TinySoftware.com*. Tiny Personal Firewall jest jedną z najdroższych programowych zapór — kosztuje niemal 100 dolarów.

Tiny Personal Firewall posiada wszystkie podstawowe funkcje dostępne w zaporze systemu Windows, a dodatkowo ma funkcję automatycznego filtrowania ruchu wychodzącego. Jedną z przyjemnych cech programu Tiny Personal Firewall jest to, że zawsze wie, które

procesy działające w komputerze wchodzą w skład systemu operacyjnego, i automatycznie umieszcza je na liście zaufanych procesów. Pozwala to uniknąć bombardowania wieloma pytaniami dotyczącymi blokowania lub udostępnienia określonego typu komunikacji, jak w przypadku innych zapór. Jeżeli jednak chcemy zablokować cały ruch, niezależnie czy jest on legalny, czy nie, funkcja ta może być bardzo kłopotliwa.

Główną częścią zapory jest Activity Monitor, który pokazuje wszystkie bieżące połączenia sieciowe, zarówno wychodzące, jak i wychodzące. Osobiście korzystam z zakładki *Connections*, na której pokazane są wszystkie zestawione połączenia do oraz z komputera, wyświetlona ilość wysłanych i otrzymanych danych oraz bieżąca szybkość przesyłu, tak jak na rysunku 8.12.



Rysunek 8.12. *Informacje o połączeniach sieciowych w programie Tiny Personal Firewall*

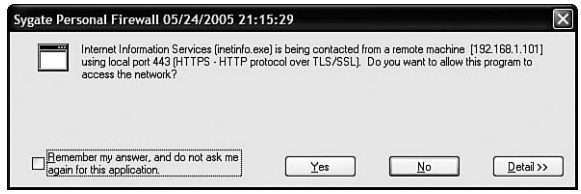
Administration Center to okno pozwalające na zarządzanie wszystkimi zasadami dostępu. Zarządzanie zasadami sieciowymi jest podobne do zastosowanego w korporacyjnej zaporze programowej firmy Microsoft noszącej nazwę ISA Server. Każdy, kto jest zaznajomiony z tym systemem, powinien sobie poradzić w domu z Tiny Personal Firewall. Jednak korzystanie z rozbudowanych opcji programu może być frustrujące i denerwujące dla niektórych użytkowników.

Ponieważ w porównaniu do innych programowych zapór administracja jest tu znacznie bardziej skomplikowana i rozbudowana, zalecam użycie zapory prostszej do konfiguracji, takiej jak Norton Personal Firewall lub bezpłatny Sygate Personal Firewall, jeżeli potrzebne są tylko podstawowe funkcje rozszerzone o monitorowanie i kontrolę ruchu wychodzącego. Jeżeli wymagana jest maksymalna elastyczność i kontrola nad połączeniem sieciowym, Tiny Personal Firewall jest właściwym wyborem.

Sygate Personal Firewall

Sygate Personal Firewall (wersja nieprofesjonalna) jest bezpłatną zaporą programową, która zawiera wszystkie funkcje wbudowanej zapory Windows, ale dodatkowo posiada możliwość blokowania ruchu wychodzącego dla wszystkich lub wybranych aplikacji.

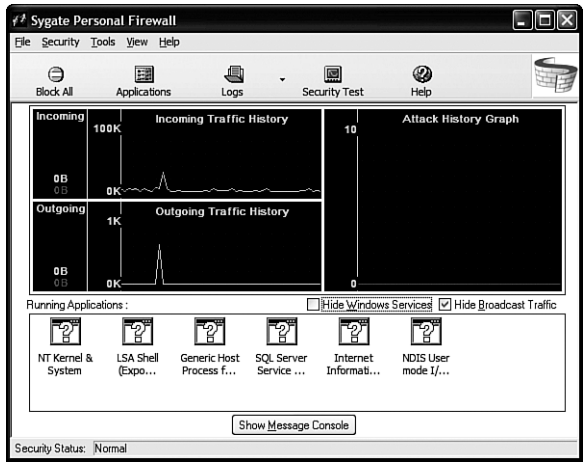
Po zainstalowaniu zapory można być zaskoczonym, jak wiele procesów działających w komputerze żąda dostępu do internetu. Za każdym razem gdy proces próbuje sięgnąć do internetu, na ekranie jest wyświetlane okno pokazane na rysunku 8.13.



Rysunek 8.13. *Sygate Personal Firewall — potwierdzenie dostępu aplikacji do sieci*

Jak widać na rysunku 8.13, użytkownik ma możliwość zareagowania na kilka sposobów. Po kilku pierwszych uruchomieniach komputera, ogromna liczba potwierdzeń zacznie spadać, ponieważ program uczy się, co jest normalnym ruchem sieciowym.

Inną funkcją programu Sygate Personal Firewall są wykresy graficzne pokazane na rysunku 8.14 oraz obszerne dzienniki, w których zapisane są zablokowane próby dostępu z wewnątrz i z zewnątrz komputera.



Rysunek 8.14. *Sygate Personal Firewall w działaniu*

Firma Sygate oferuje również profesjonalną wersję tego programu, która posiada dodatkowe funkcje podobne do tych, które są dostępne w programach Norton Personal Firewall oraz Tiny Personal Firewall. Cena tego programu jest podobna do innych „profesjonalnych wersji" zapór. Więcej informacji na temat programu Sygate Personal Firewall, zarówno bezpłatnego, jak i profesjonalnego, można znaleźć na witrynie *http://smb.sygate.com/*[1].

Wirusy

Wirusy są znane od bardzo długiego czasu, ale choć w internecie jest nadal wiele tych niebezpiecznych programów, straciły one nieco na znaczeniu na rzecz innych odmian destrukcyjnych programów i oprogramowania szpiegującego. Na szczęście, ze wszystkich zagrożeń komputerowych, przeciwko wirusom można się stosunkowo najłatwiej obronić. Dzięki

[1] Firma Sygate została wykupiona przez Symantec i od 30 listopada 2005 roku program Sygate Personal Firewall jest niedostępny — *przyp. tłum.*

postępowi w dziedzinie programów antywirusowych, potrzebujemy tylko dobrego i często aktualizowanego programu antywirusowego.

Początkowo oprogramowanie antywirusowe chroniło komputery w sposób bardziej pasywny. Programy te na żądanie mogły przeskanować wybrany plik. W końcu producenci oprogramowania antywirusowego zorientowali się, że potrzebne jest bardziej proaktywne rozwiązanie. Obecnie programy te można tak skonfigurować, aby skanowały wszystkie pliki, jakie komputer próbuje odczytać lub uruchomić, jak również automatycznie blokowały metody wykorzystywane przez większość wirusów do rozprzestrzeniania się. Jest to bardzo przydatne, ponieważ większość programów antywirusowych wykrywa wirusy bazując na definicjach, które muszą być stale aktualizowane, aby mogły być wykrywane nowe wirusy. Przez zablokowanie dołączania do przesyłek e-mail plików o określonych rozszerzeniach oraz blokowanie uruchamiania określonych typów skryptów, oprogramowanie to może chronić przed potencjalnymi wirusami, których definicje nie zostały jeszcze dostarczone.

Jeżeli pracujemy na komputerze, który nie ma zainstalowanego żadnego oprogramowania antywirusowego, i chcemy szybko sprawdzić system, można skorzystać z witryny dostępnej pod adresem *http://housecall.trendmicro.com*, na której dostępny jest bezpłatny, sieciowy skaner antywirusowy. Następnie należy wybrać program antywirusowy, który będzie aktywnie chronił komputer.

AVG Anti-Virus Free

Istnieje wiele firm, które dostarczają programów antywirusowych, ale bardzo niewiele udostępnia programy bezpłatnie. AVG Anti-Virus Free firmy Grisoft to standardowy program antywirusowy. Posiada wszystkie podstawowe funkcje programów antywirusowych dostępnych na rynku i do zastosowań domowych jest bezpłatny. Dostępna jest również profesjonalna wersja programu AVG Anti-Virus przeznaczona do użytku komercyjnego; za tę wersję trzeba zapłacić.

Jeżeli jednak szukamy dobrego programu antywirusowego do komputera domowego i nie chcemy płacić za Norton Anti-Virus lub Mcafee Anti-Virus, to AVG jest dobrym wyborem.

Na początek należy odwiedzić witrynę *http://free.grisoft.com* i pobrać najnowszą wersję programu.

Aby zainstalować, skonfigurować i zaktualizować program AVG Anti-Virus, należy wykonać następujące operacje:

1. Pobrać i zainstalować AVG Anti-Virus. Po zakończeniu działania programu instalacyjnego zostanie automatycznie uruchomiona aplikacja i kreator *First Run*. Mogą się również pojawić komunikaty informujące o tym, że wewnętrzna baza wirusów jest nieaktualna. Na razie należy zignorować te komunikaty; wkrótce zaktualizujemy bazę danych. W kreatorze *First Run* należy kliknąć *Next*.
2. Teraz należy zaktualizować bazę danych; wystarczy kliknąć przycisk *Check for Updates*. Następnie należy kliknąć przycisk *Internet*, aby automatycznie pobrać aktualizacje z serwera firmy Grisoft.

3. Jeżeli zostaną znalezione nowe aktualizacje, zostaną one wyświetlone. Należy je zaznaczyć (o ile nie są automatycznie zaznaczone) i kliknąć *Update*, aby zainicjować pobieranie i instalację aktualizacji.
4. Po zakończeniu instalacji i aktualizacji, wracamy do kreatora *First Run*. Jeszcze raz należy kliknąć przycisk *Next*.
5. W tym momencie mamy możliwość utworzenia dyskietek ratunkowych wykorzystywanych do naprawienia komputera, jeżeli wirus zainfekuje niektóre pliki systemowe. Krok ten nie jest wymagany, ale jego wykonanie jest zalecane. Należy kliknąć przycisk *Create Rescue Disks* i postępować zgodnie z instrukcjami kreatora. Należy upewnić się, że mamy kilka wolnych dyskietek. Po zakończeniu operacji lub jej pominięciu należy kliknąć *Next*.

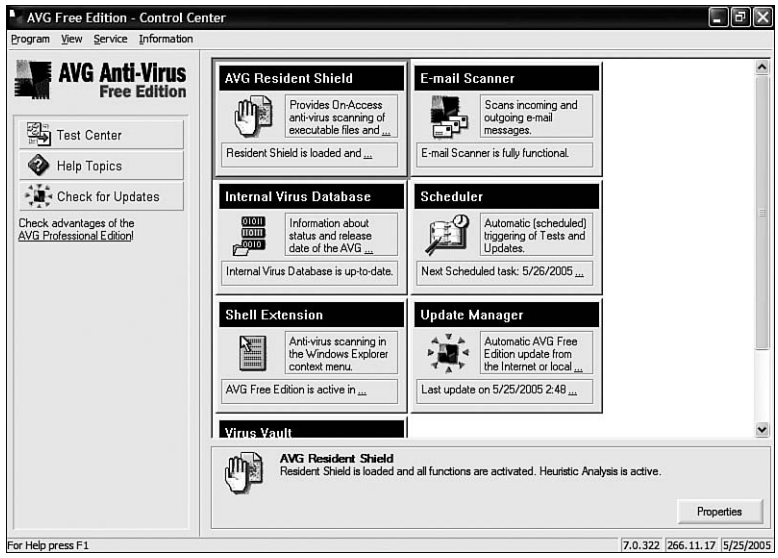
Nie da się utworzyć ratunkowego dysku CD za pomocą tego procesu.

6. Jeżeli oprogramowanie antywirusowe jest instalowane na tym komputerze po raz pierwszy, dobrym pomysłem jest wykonanie pierwszego skanowania, które przeanalizuje wszystkie pliki komputera, aby upewnić się, że są wolne od wirusów. W tym celu należy kliknąć przycisk *Scan Computer!*. Pierwsze skanowanie antywirusowe może potrwać od kilku minut do ponad godziny, w zależności od ilości plików na dysku. Po zakończeniu skanowania zostaną wyświetlone wyniki, jak również opcja usunięcia znalezionych wirusów. Gdy wszystko zostanie zakończone, należy kliknąć *Next*, aby przejść do następnego ekranu kreatora *First Run*.
7. Ostatnim etapem konfiguracji jest rejestracja. Wykonanie tego kroku jest opcjonalne, ponieważ zarejestrowanie bezpłatnej wersji nie daje żadnych korzyści poza przekazaniem danych osobistych do firmy Grisoft. Po zakończeniu rejestracji należy kliknąć *Next*, a następnie na ostatnim ekranie kreatora *Continue*.

Po wykonaniu tych operacji AVG Anti-Virus jest zainstalowany i działa na naszym komputerze. Domyślnie uruchomione są wszystkie moduły monitorujące, takie jak skaner aktywnych plików, który automatycznie skanuje wszystkie otwarte dokumenty w edytorze, czy też skaner załączników w programie pocztowym. Jeżeli chcemy ręcznie zmienić ustawienia tych agentów, należy w głównym oknie *Test Center* kliknąć *Control Center*. Po załadowaniu okna *Control Center* widzimy wszystkich agentów ochrony, jak jest to pokazane na rysunku 8.15.

Należy kliknąć dowolny przycisk agenta, a następnie przycisk *Properties* lub inną opcję dostępną w dolnej części okna.

Utrzymanie aktualności bazy danych wirusów jest krytyczne dla działania tego programu. AVG Anti-Virus posiada program harmonogramu, który domyślnie jest skonfigurowany w taki sposób, aby codziennie szukał aktualizacji i skanował system w poszukiwaniu nowych wirusów.



Rysunek 8.15. *Okno Control Center programu AVG Anti-Virus*

Norton AntiVirus 2005

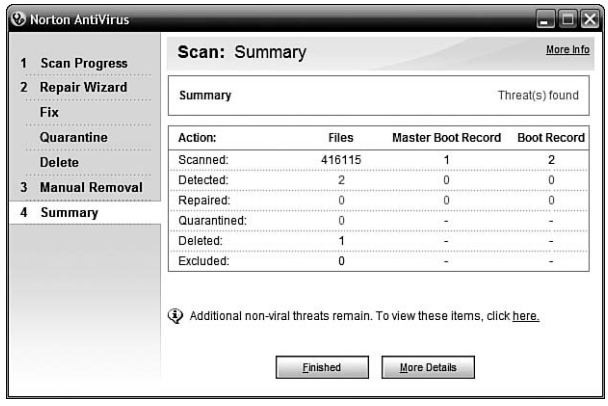
Wiodącym programem antywirusowym dla Windows jest Norton AntiVirus. Posiada on wszystkie funkcje AVG Anti-Virus Free, a dodatkowo bardziej zaawansowaną bazę danych, dzięki której może wykrywać trojany, robaki i inne typy szkodliwego oprogramowania. Producentem tego programu jest firma Symantec, a można go kupić za około 150 zł. Użycie programu Norton AntiVirus jest podobne do użycia innych programów antywirusowych, ponieważ monitorują one pliki w taki sam sposób, korzystają tylko z innego silnika.

Podobnie jak w przypadku pozostałych programów antywirusowych, utrzymanie aktualności bazy danych jest niezwykle ważne. Norton AntiVirus korzysta z usługi LiveUpdate formy Symantec, aby co tydzień pobierać nowe definicje. Instalacja i konfiguracja programu Norton AntiVirus jest równie prosta. Wystarczy wykonać następującą procedurę:

1. Po zakupieniu i rozpoczęciu instalowania programu Norton AntiVirus, przeprowadzone zostaje wstępne skanowanie antywirusowe. Procedura ta została umieszczona w programie instalacyjnym, aby przed zainstalowaniem programu system był wyczyszczony z istniejących wirusów, które mogą próbować sabotować instalację. Krok ten nie jest wymagany, więc można po prostu kliknąć *Next*, aby kontynuować pracę. Jednak zalecane jest naciśnięcie przycisku *Start Scan*, aby upewnić się, że komputer jest czysty i nic nie będzie przeszkadzać w instalacji.
2. Po zakończeniu skanowania można kontynuować instalację przez naciśnięcie przycisku *Next*. Po zakończeniu instalacji należy ponownie uruchomić komputer.
3. Po uruchomieniu komputera i zalogowaniu się, uruchomiony zostaje kreator konfiguracji. Na ekranie początkowym należy kliknąć *Next*, aby rozpocząć konfigurowanie programu Norton AntiVirus.
4. Na następnym ekranie można aktywować oprogramowanie i wprowadzić klucz, jaki Symantec dołączył do zakupionego oprogramowania.

5. Na ekranie zabezpieczeń mamy możliwość włączenia funkcji współdzielenia statusu programu z innymi produktami. Najlepiej zaznaczyć tę opcję i przejść dalej.
6. Kreator kończy pracę, ale uruchomiony zostaje moduł Live Update, który pozwala aktualizować oprogramowanie i pobierać najnowsze definicje wirusów. Po sprawdzeniu oprogramowania przez moduł Live Update i wyświetleniu listy dostępnych aktualizacji, kliknięcie przycisku *Next* powoduje ich pobranie i automatyczne zainstalowanie. Czas wykonywania tej operacji zależy od szybkości działania połączenia internetowego. W zależności od zainstalowanej poprawki, może zaistnieć konieczność ponownego uruchomienia komputera.
7. Zazwyczaj po ponownym uruchomieniu komputera Norton AntiVirus automatycznie uruchamia ponowne skanowanie wszystkich plików komputera, ale tym razem korzysta z najnowszych definicji wirusów, koni trojańskich i robaków. Po zakończeniu skanowania konfiguracja jest ukończona.

Po zakończeniu pełnego skanowania wyświetlone zostanie okno podobne do przedstawionego na rysunku 8.16.



Rysunek 8.16. *Norton AntiVirus — znaleziony wirus*

W większości przypadków Norton AntiVirus automatycznie usuwa wszystkie znalezione wirusy. Jeżeli chcemy zobaczyć szczegóły skanowania i sprawdzić, jaki wirus został znaleziony, należy kliknąć przycisk *More Details*.

Jeżeli konieczne jest wyłączenie dodatkowych funkcji, takich jak ochrona przed robakami czy ochrona komunikatora, ponieważ przeszkadzają one aplikacji przez blokowanie dostępu do sieci, można je na stałe wyłączyć, klikając przycisk *Options* znajdujący się na górze głównego okna.

Oprogramowanie szpiegujące

Oprogramowanie szpiegujące (ang. *spyware*) jest obecnie najszybciej rosnącym problemem dla użytkowników komputerów. Rzadko można znaleźć komputer, który nigdy nie był zarażony jakimkolwiek programem szpiegującym. Ponieważ słabe punkty zostały odkryte w większości przypadków w programie Internet Explorer, a oprogramowanie szpiegujące

jest dołączane do niektórych popularnych aplikacji, jest ono zwykle instalowane na komputerze bez powiadamiania użytkownika. Pierwszym symptomem, który informuje użytkownika o istnieniu oprogramowania szpiegującego w systemie, jest nagłe otwieranie okien z reklamami, które w pewien sposób dotyczą operacji wykonywanych na komputerze. W innych przypadkach oprogramowanie szpiegujące może tylko zapisywać to, co dzieje się na komputerze, na przykład odwiedzane witryny, i w żaden sposób się nie ujawniać.

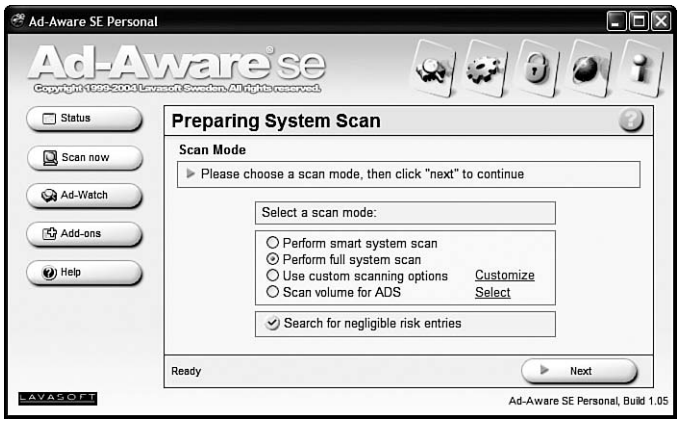
Ponieważ oprogramowanie szpiegujące jest często bardzo trudne do wykrycia przez zwykłego użytkownika, może być niezbędne zastosowanie narzędzi do wykrywania i usuwania tego typu szkodników. Obecnie dostępnych jest kilkanaście programów do usuwania oprogramowania szpiegującego. Co dziwniejsze, niektóre z nich również są programami szpiegującymi. Wydaje się, że każdy chce trochę zarobić na zastosowaniu oprogramowania szpiegującego. Na szczęście istnieje kilka programów, które są bezpłatne, a są najlepszymi programami do usuwania szpiegów z komputerów i ochrony przed przyszłą infekcją.

Podobnie do oprogramowania antywirusowego, programy wykrywają oprogramowanie szpiegowskie, korzystając z bazy znanych programów. Baza danych każdego programu jest aktualizowana w różnych momentach. Powoduje to, że aby być pewnym, że system jest wolny od oprogramowania szpiegującego, należy skorzystać z kombinacji kilku programów. Programy te stają się coraz lepsze, lecz dosyć często po oczyszczeniu systemu przez Ad-Aware wykonywałem skanowanie za pomocą Spybot Search & Destroy i Spybot czasami znajdował kolejne rzeczy do usunięcia. Ta sama sytuacja zdarza się, gdy korzystamy z tych programów w odwrotnej kolejności. Nie jest to spowodowane tym, że jeden program jest lepszy od drugiego, ale tym, że w ich bazach danych znajdują się inne dane.

LavaSoft Ad-Aware

LavaSoft Ad-Aware SE Personal Edition to bezpłatna wersja popularnego programu Ad-Aware do usuwania oprogramowania szpiegującego, którą można pobrać z witryny *http://www.lavasoftusa.com*. Ad-Aware SE Personal Edition jest świetnym programem do wyszukiwania i usuwania programów szpiegujących z komputera. Aby skorzystać z programu Ad-Aware, należy sprawdzić, czy na komputerze została zainstalowana kopia programu Ad-Aware SE Personal Edition, i wykonać następującą procedurę:

1. Uruchomić Ad-Aware i włączyć pobieranie najnowszej wersji bazy danych definicji. Po pobraniu i automatycznym zainstalowaniu definicji, wyświetlony zostaje główny ekran aplikacji. Ponieważ definicje są aktualne, należy wykonać pełne skanowanie systemu. W tym celu należy kliknąć przycisk *Scan Now*.
2. Po tej operacji na ekranie pokazują się różne typy operacji skanowania, jakie można wykonać za pomocą programu Ad-Aware. Jeżeli jest to pierwsze skanowanie, najlepiej wykonać pełne skanowanie systemu, jak jest to pokazane na rysunku 8.17. W przyszłości można wykonać sprytne skanowanie systemu, które wyszukuje oprogramowanie szpiegujące w najczęściej spotykanych miejscach, a nie na całym dysku. Jak łatwo zgadnąć, ta metoda skanowania jest znacznie szybsza. Na razie jednak należy wybrać *Perform full system scan* i kliknąć *Next*, aby rozpocząć operację.
3. Po zakończeniu skanowania należy kliknąć *Next*, aby przejrzeć wyniki. Na zakładce *Critical Objects* wyświetlane jest znalezione oprogramowanie szpiegujące.



Rysunek 8.17. *Pełne skanowanie systemu w programie Ad-Aware SE Personal Edition*

Aby usunąć je, należy zaznaczyć każdą z tych pozycji lub kliknąć prawym przyciskiem myszy listę i z menu wybrać pozycję *Select All Objects*. Następnie należy kliknąć *Next*, aby usunąć oprogramowanie szpiegujące.

4. Na ekranie wyświetlane jest okno, w którym należy potwierdzić, czy faktycznie chcemy usunąć znalezione oprogramowanie. Po kliknięciu *OK* operacja zostaje zakończona.

Zalecane jest ręczne wyszukiwanie oprogramowania szpiegującego raz w tygodniu, aby zapewnić, że osobiste dane są bezpieczne i komputer jest czysty. Dodatkowo przed każdym skanowaniem należy upewnić się, że pobrane są najnowsze definicje.

Definicje dla programu Ad-Aware SE Personal Edition można pobrać przez kliknięcie ikony globusa znajdującej się na głównym ekranie. Po wyświetleniu okna *Web Update* należy kliknąć przycisk *Connect* w celu wyszukania i pobrania nowych aktualizacji.

Spybot Search & Destroy

Innym bezpłatnym i bardzo popularnym programem wykrywającym oprogramowanie szpiegujące jest Spybot Search & Destroy, którego autorem jest Patrick Kolla. Spybot działa w ten sam sposób co Ad-Aware, ale ma również możliwość konfiguracji programu Internet Explorer, aby automatycznie blokował niektóre znane aplikacje szpiegujące.

Korzystanie z programu Spybot różni się od korzystania z Ad-Aware, ale jest równie proste. Należy odwiedzić witrynę *http://www.safernetworking.org*, skąd należy pobrać program Spybot, zainstalować go, a następnie wykonać następującą procedurę skanowania i naprawy komputera:

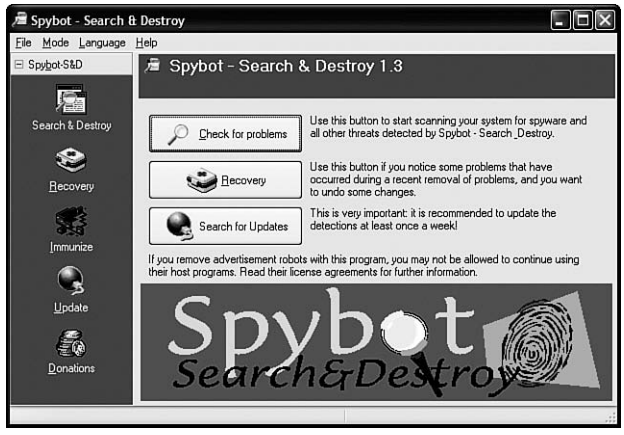
1. Uruchomić Spybot S&D Wizard z menu *Start* (lub ikony na pulpicie). Jeżeli jest to pierwsze uruchomienie programu Spybot Search & Destroy, załadowany zostanie kreator *Spybot S&D Wizard*. Na pierwszym ekranie mamy możliwość utworzenia kopii rejestru. Jest to bardzo przydatne, jeżeli po usunięciu aplikacji szpiegującej komputer przestanie prawidłowo działać. W takiej sytuacji można skorzystać z wykonanej kopii w celu przywrócenia stanu sprzed zmian

wprowadzonych do rejestru. Jeżeli program ma wykonać kopię, należy kliknąć przycisk *Create registry backup*. W przeciwnym razie, kliknąć *Next*, aby przejść dalej.

2. Na następnym ekranie kreatora dostępna jest opcja wyszukania aktualizacji przed wykonaniem skanowania komputera. Aby pobrać listę najnowszych poprawek oraz aktualizacji definicji, należy kliknąć *Search for Updates*. Jeżeli dostępne są aktualizacje, należy kliknąć przycisk *Download all available updates*.

3. Po zainstalowaniu aktualizacji program Spybot uruchomi się ponownie i zostanie wyświetlony główny ekran (patrz rysunek 8.18). Aby rozpocząć skanowanie komputera, należy kliknąć przycisk *Check for problems*.

Rysunek 8.18. *Program Spybot Search & Destroy*



4. Po zakończeniu wyszukiwania oprogramowania szpiegującego, jeżeli coś zostanie znalezione, na ekranie zostanie wyświetlona lista zidentyfikowanych programów. Aby usunąć wszystkie znalezione programy, należy kliknąć przycisk *Fix Selected Problems*. Spybot utworzy punkt przywracania systemu, a następnie usunie wszystkie znalezione programy szpiegujące. W niektórych sytuacjach Spybot może nie być w stanie usunąć wszystkich plików. Zwykle dzieje się tak, gdy plik jest używany i Spybot nie może zakończyć korzystającego z niego procesu. W takich przypadkach Spybot informuje, że aby usunąć program spyware, komputer musi być przeładowany. Po ponownym uruchomieniu komputera, natychmiast po zalogowaniu zostanie uruchomiony program Spybot S&D i automatycznie zostanie wybrana opcja naprawienia wszystkich problemów. Tym razem, ponieważ jest to pierwsza uruchomiona aplikacja, wstrzymuje ona pozostałe uruchamiane programy i żaden inny proces, w tym program szpiegujący, nie zostanie uruchomiony, co umożliwia usunięcie plików.

Spybot Search & Destroy zawsze powinien być aktualizowany przed skanowaniem, aby zapewnić, że wyszuka najnowsze programy szpiegujące, jakie zostały zainstalowane na komputerze. Po uruchomieniu aplikacji należy kliknąć przycisk *Search for Updates* w celu automatycznego pobrania najnowszych definicji.

Po zakończeniu operacji wyszukiwania i usuwania przez program Spybot Search & Destroy oprogramowania szpiegującego z komputera, można skorzystać z zaawansowanych funkcji w celu zabezpieczenia programu Internet Explorer i zablokowania możliwości instalacji znanego oprogramowania szpiegującego.

Aby zastosować zaawansowane funkcje programu Spybot, należy uruchomić program Spybot i kliknąć przycisk *Immunize* znajdujący się w panelu po lewej stronie okna. Program może automatycznie blokować ponad 2000 różnych aplikacji szpiegujących w przeglądarce Internet Explorer. Aby włączyć ochronę, wystarczy kliknąć przycisk *Immunize* z dużym znakiem plusa.

Jeżeli w przyszłości zdarzą się problemy, na przykład strony, które normalnie działały, przestaną być prawidłowo wyświetlane w programie Internet Explorer, można wycofać operację *Immunize* z programu Spybot. Realizuje się to przez kliknięcie przycisku *Undo* w sekcji *Immunize*.

Microsoft Windows AntiSpyware

Microsoft Windows AntiSpyware to odpowiedź firmy Microsoft na rosnącą ilość oprogramowania szpiegującego, które instaluje się w systemie Windows. Program, początkowo opracowany w firmie Giant Software, która została przejęta przez Microsoft w roku 2004, jest obszernym i bezpłatnym pakietem oferującym nie tylko usuwanie oprogramowania szpiegującego, ale również aktywną ochronę realizowaną w podobny sposób do funkcji Auto Protect wykorzystywanej w programie Norton AntiVirus do ochrony przed wirusami.

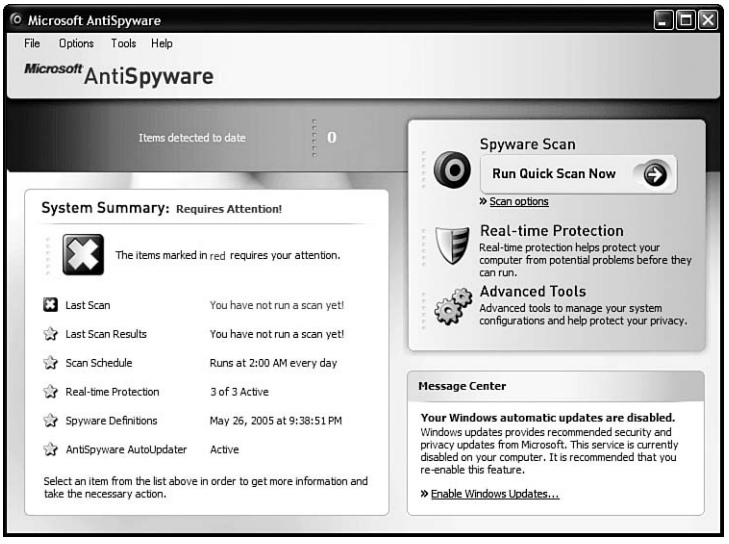
Jeżeli na komputerze działa Microsoft AntiSpyware i użytkownik odwiedzi stronę, która będzie usiłowała zainstalować jakikolwiek kod, wyświetlony zostanie komunikat informujący o tym fakcie i użytkownik będzie mógł zezwolić na tę operację lub ją zablokować, jak jest to pokazane na rysunku 8.19. Podobne powiadomienia są również wyświetlane, jeżeli dowolna aplikacja będzie próbowała zmodyfikować listę automatycznie uruchamianych programów lub zmienić ustawienia połączenia internetowego. Jest to bardzo efektywny wskaźnik pozwalający natychmiast dowiedzieć się, że komputer może być zainfekowany przez program szpiegujący, jak również uniemożliwiający nieautoryzowaną zmianę jakichkolwiek ustawień konfiguracji.

Rysunek 8.19. *Powiadomienie programu Microsoft Windows AntiSpyware*

Instalacja programu Microsoft Windows AntiSpyware jest bardzo prosta. Należy zacząć od odwiedzenia witryny *http://www.microsoft.com* i pobrania programu instalacyjnego. Po zainstalowaniu programu AntiSpyware należy uruchomić program przez kliknięcie ikony na pulpicie i wykonać przedstawione poniżej operacje mające na celu skonfigurowanie Anti-Spyware:

1. Po uruchomieniu Microsoft AntiSpyware załadowany zostanie Setup Assistant, który prowadzi użytkownika przez proces konfigurowania ochrony przeciw programom szpiegującym. Kliknąć *Next*, aby przejść dalej.
2. W kroku 1. z 3 kreator zadaje pytanie o włączenie funkcji AutoUpdate. Funkcja AutoUdate regularnie pobiera najnowsze definicje oprogramowania szpiegującego; opisane wcześniej programy nie posiadają takiej funkcji. Włączenie tej opcji jest wysoce zalecane; następnie należy kliknąć przycisk *Next*.
3. W następnym kroku można włączyć lub wyłączyć agentów ochrony w czasie rzeczywistym, którzy realizują wspomnianą wcześniej funkcję blokowania zmiany ustawień internetowych do momentu wyrażenia na to zgody przez użytkownika. Jest to jedna z najlepszych funkcji programu Microsoft Windows AntiSpyware i zdecydowanie powinna być włączona. Kliknąć *Next*, aby przejść do ostatniego kroku.
4. W ostatnim kroku można wziąć udział w czymś, co zostało nazwane SpyNet. SpyNet jest właściwie metodą pozwalającą na przesyłanie raportów z wyników skanowania do firmy Microsoft, dzięki czemu informacje te mogą być wykorzystane do aktualizacji bazy danych definicji. Najlepiej, gdyby wszyscy korzystali z tej funkcji, ponieważ definicje byłyby lepsze, ale użytkownicy mający wątpliwości dotyczące prywatności mogą wyłączyć tę funkcję. Tak czy inaczej, kliknięcie *Finish* powoduje zamknięcie kreatora Setup Assistant.
5. Na następnym ekranie można uruchomić funkcję pełnego skanowania systemu. Sugeruję kliknięcie przycisku *Run Scan Later*, ponieważ wcześniej warto zaktualizować definicje.
6. Po załadowaniu głównego interfejsu należy kliknąć menu *File*, a następnie wybrać opcję *Check for Updates*. Jeżeli są dostępne aktualizacje, zostaną one automatycznie zainstalowane. Aby kontynuować, należy kliknąć *Close*.
7. Po tej operacji można wykonać wyszukiwanie oprogramowania szpiegującego. Aby rozpocząć skanowanie, należy kliknąć przycisk *Run Quick Scan Now*.
8. Po zakończeniu skanowania, o ile nic nie zostanie znalezione, na ekranie wyświetlane jest podsumowanie wyników. Aby przejrzeć szczegóły oraz usunąć znalezione programy szpiegujące, należy kliknąć przycisk *View Report*.
9. Na ekranie *Scan Results* znajduje się lista znalezionych elementów, która zawiera listy rozwijane zawierające zalecane akcje, jakie należy wykonać (*Ignore*, *Quarantine*, *Remove* lub *Always remove* — Ignoruj, Kwarantanna, Usuń lub Zawsze usuwaj). Domyślnie Microsoft AntiSpyware wybiera zalecaną akcję w zależności od stopnia złośliwości programu. Zawsze można zmienić ten wybór przez wybranie nowej opcji z listy rozwijanej znajdującej się z lewej strony elementu. Po zaznaczeniu wszystkich akcji należy kliknąć *Continue*. Kliknięcie następnie *Yes* na ekranie potwierdzenia powoduje wykonanie akcji.

Rysunek 8.20. *Microsoft Windows AntiSpyware*



Microsoft AntiSpyware zawiera wiele funkcji, których nie spodziewamy się w programie do zwalczania oprogramowania szpiegującego. Wiele przydatnych narzędzi można znaleźć w sekcji *System and Privacy* dostępnej po kliknięciu ikony *Advanced Tools*.

Przywracanie po przejęciu przeglądarki

Dla naszej wygody oprogramowanie szpiegujące często zmienia naszą stronę startową w Internet Explorer, jak również domyślną stronę wyszukiwania. Przez to zaraz po otwarciu przeglądarki lub próbie wyszukiwania jesteśmy bombardowani kolejnymi możliwościami złapania szpiega. Choć czasami operacje te są zupełnie nieszkodliwe, to jednak znacznie częściej przekraczają one wszelkie granice, co motywuje użytkowników do odzyskania kontroli nad swoją przeglądarką.

Przywracanie po przejęciu przeglądarki przez oprogramowanie szpiegujące jest często bardzo irytującym zajęciem. Dosyć często uruchamiamy program do usuwania oprogramowania szpiegującego z naszego systemu, które powraca po otwarciu przeglądarki, ponieważ program usuwający nie potrafił wykryć modyfikacji w przeglądarce. Projektanci oprogramowania szpiegującego są zwykle bardzo skuteczni w swojej pracy i tworzą programy, które nie zawsze dają się usunąć bez walki. Na szczęście za pomocą Microsoft Windows AntiSpyware bardzo łatwo można przywrócić domyślne ustawienia programu Internet Explorer, dzięki czemu można skasować wszystkie zmiany wprowadzone przez program szpiegujący. Oczywiście powoduje to utratę wszystkich własnych usprawnień wprowadzonych do przeglądarki.

Funkcja, która pomaga w wykonaniu tej operacji, jest zaszyta w aplikacji. Należy uruchomić Microsoft Windows AntiSpyware, kliknąć ikonę *Advanced Tools* znajdującą się w prawym górnym narożniku okna i wykonać następującą procedurę:

1. Znaleźć i kliknąć ikonę *Browser Restore* znajdującą się w sekcji *System Tools*.
2. Kliknąć pole wyboru *Check All*, jak jest to pokazane na rysunku 8.21.

Rysunek 8.21. *Przywracanie ustawień przeglądarki w programie Microsoft Windows AntiSpyware*

3. Następnie należy kliknąć przycisk *Restore* i wszystkie ustawienia zostaną przywrócone do stanu początkowego.

Przywracanie po przejęciu przeglądarki nigdy nie było prostsze.

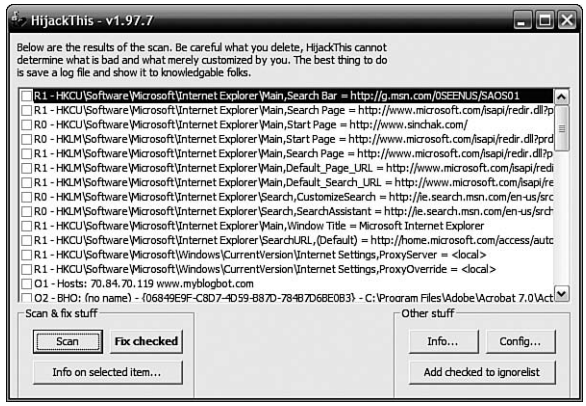
Co robić, gdy automatyczne procedury zawiodą?

Oprogramowanie szpiegujące stale się rozwija i próbuje być o krok przed programami przeznaczonymi do jego usuwania. Jednym z największych problemów programów usuwających spyware jest to, że w znacznym stopniu opierają się na znanych definicjach. Choć to pasywne podejście może być efektywne i jest znacznie lepsze od zaniechania działania, oznacza to, że nowe szkodliwe oprogramowanie musi narobić szkód, aby stało się znane. Aby usunąć oporne oprogramowanie szpiegujące, konieczna jest pomoc kogoś, kto ma duże doświadczenie w usuwaniu tego typu programów.

Aby pomóc niezliczonym ofiarom programów spyware, na różnych witrynach można uzyskać wsparcie w ich zwalczaniu. Większość z tych witryn korzysta z popularnego oprogramowania diagnostycznego o nazwie HijackThis. HijackThis to świetny program analizujący różne składniki konfiguracji systemu oraz ustawienia programu Internet Explorer i wyświetlający ich bieżące wartości. Program ten pozwala użytkownikowi zapisać kopię wyników, które mogą być wysłane na różne witryny korzystające z tego narzędzia. Wybrane osoby, które poświęcają swój czas na pomaganie za pośrednictwem tych witryn przeglądają nadesłane wyniki i pomagają zorientować się, które wpisy powodują problemy. Następnie, ponownie uruchamiając program HijackThis, można w łatwy sposób sprawdzić ten wpis i usunąć go w celu rozwiązania problemu.

Na początek należy otworzyć witrynę *http://www.merijn.org* i pobrać najnowszą wersję programu HijackThis. Następnie wykonać następującą procedurę w celu wygenerowania wyników:

1. Po pobraniu programu HijackThis należy uruchomić aplikację (nie wymaga ona instalacji).
2. Kliknąć przycisk *Scan*, aby wyświetlić wyniki działania (patrz rysunek 8.22).



Rysunek 8.22. *Generowanie wyników w programie HijackThis*

3. Następnie kliknąć przycisk *Save Log*, aby zapisać wyniki skanowania komputera do pliku tekstowego.

Następnie, mając plik z wynikami skanowania, należy go wysłać do jednej z popularnych witryn, które mają dedykowane wsparcie dla HijackThis:

- *http://forum.tweakxp.com*
- *http://forums.spywareinfo.com*
- *http://forums.tomcoyote.org*

Po wysłaniu wyników działania HijackThis na jedną lub kilka z tych witryn, najprawdopodobniej otrzymamy odpowiedź w przeciągu jednego dnia. Gdy winowajca zostanie zidentyfikowany, wystarczy otworzyć program HijackThis, zaznaczyć pole obok wiersza do usunięcia i kliknąć *Fix Checked*. Następnie, aby wykonać operację, należy ją dodatkowo potwierdzić. Po ponownym uruchomieniu komputera problem powinien być rozwiązany.