ABC ochrony przed wirusami

Autor: Radosław Sokół
ISBN: 83-7361-399-4
Format: B5, stron: 188

Wirusy stają się coraz poważniejszym zagrożeniem. W dobie internetu, gdy większość komputerów połączona jest globalną siecią, wirusy rozpowszechniają się w zastraszającym tempie. Efekty ich działania mogą być różne – od całkiem trywialnych żartów, aż do całkowitego zniszczenia plików znajdujących się na dysku twardym zainfekowanego komputera. Możliwe jest również wykorzystanie tego komputera do przeprowadzenia ataku na serwery internetowe lub do przekazywania informacji o działaniach podejmowanych przez użytkownika komputera.

Na atak narażony jest każdy z nas, dlatego niezwykle istotną rzeczą jest umiejętność zabezpieczania się przez wirusami, jak również ich zwalczania. Książka „ABC ochrony przed wirusami" zawiera omówienie obu tych tematów. Czytając ją, dowiesz się:

- Czym naprawdę są wirusy komputerowe
- Jakie rodzaje niepożądanych plików mogą zainfekować Twój komputer
- Jak bronić się przed atakami wirusów, wykorzystując mechanizmy zaimplementowane w Windows XP
- Jak korzystać z programów realizujących funkcje „zapór ogniowych"
- W jaki sposób usunąć z komputera „szpiegowskie" oprogramowanie
- Jak korzystać z internetowych skanerów antywirusowych
- W jaki sposób zainstalować i skonfigurować najpopularniejsze pakiety antywirusowe oraz korzystać z nic

Jedyną rzeczą związaną z wirusami, która pozostaje niewyjaśniona są intencje kierujące ich twórcami. Wszystkiego innego dowiesz się z tej książki.

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Rozdział 5.

Norton AntiVirus 2004

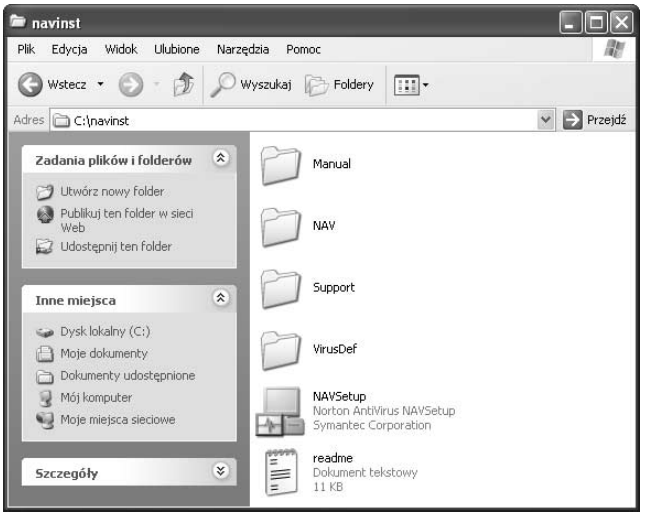
W przeciwieństwie do opisywanego przed chwilą internetowego skanera antywirusowego MkS_Vir, którego działanie — jako skanera pasywnego — za każdym razem wiąże się z łączeniem z Internetem i samodzielnym uruchamianiem procesu skanowania, Norton AntiVirus 2004 jako skaner aktywny cały czas czuwa nad bezpieczeństwem Twojego komputera. Poza tym zakres usług, które udostępnia NAV (tak brzmi skrócona nazwa programu Norton AntiVirus) jest o wiele szerszy i obejmuje:

- aktywne skanowanie w tle wszystkich przeprowadzanych operacji dyskowych,
- skanowanie zawartości archiwów plików,
- przeglądanie zawartości wiadomości pocztowych,
- automatyczną aktualizację bazy informacji o wirusach,
- skanowanie heurystyczne, umożliwiające wykrywanie nieznanych programowi szczepów wirusów.

Jedyną wadą pakietu Norton AntiVirus — w porównaniu z darmowym skanerem MkS_Vir — jest fakt, iż aby stać się legalnym posiadaczem programu, należy zakupić jego kopię. Jeśli opis funkcjonalności programu zawarty w tym rozdziale nie przekona Cię jeszcze, czy warto zainwestować pieniądze, firma Symantec — producent pakietu — daje do dyspozycji wersję testową (*trial*) programu, zachowującą pełną funkcjonalność przez 15 dni od daty instalacji.

Instalacja pakietu

Instalację pakietu rozpoczynasz, klikając dwukrotnie ikonę programu instalacyjnego, zatytułowaną *NAVSetup* (rysunek 5.1). Ponieważ instalowanie programu w zawirusowanym systemie operacyjnym mogłoby zmienić pakiet Norton AntiVirus w siedlisko wirusów, pierwszy krok instalacji polega na wstępnym przeskanowaniu systemu w poszukiwaniu najbardziej rozpowszechnionych wirusów.



Rysunek 5.1. *Dwukrotne kliknięcie ikony zatytułowanej NAVSetup rozpocznie proces instalacji pakietu Norton AntiVirus 2004-01-08*

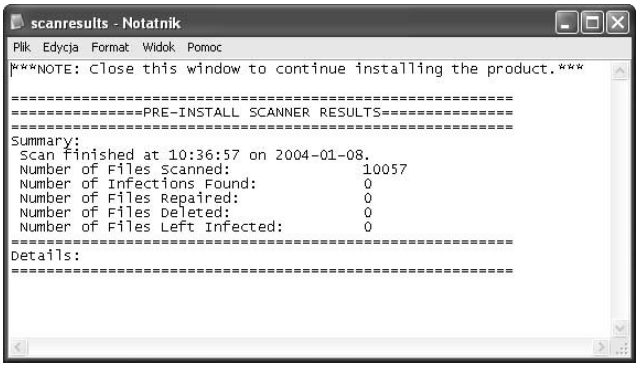
Ponieważ to wstępne skanowanie zajmuje sporo czasu i nie zawsze jest potrzebne, program instalacyjny daje możliwość rezygnacji z jego przeprowadzenia (rysunek 5.2). Jeśli jesteś pewien, że Twój system operacyjny jest czysty — na przykład instalujesz pakiet NAV w dopiero co zainstalowanym systemie operacyjnym, na komputerze pozbawionym dostępu do Internetu — możesz w oknie dialogowym *Scan for viruses?* kliknąć przycisk *Nie* i od razu przejść do instalacji. Jeśli jednak masz jakiekolwiek wątpliwości, bez wahania kliknij *Tak* i poczekaj, aż program instalacyjny sprawdzi wszystkie pliki i foldery przechowywane na dyskach twardych Twojego komputera (rysunek 5.3); w zależności od szybkości komputera oraz liczby zapisanych plików takie skanowanie może trwać od kilku do kilkudziesięciu minut.

Rysunek 5.2. *Już w czasie instalacji pakietu Twój komputer może zostać sprawdzony pod kątem obecności wirusów*

Rysunek 5.3. *Trwa poszukiwanie wirusów na dyskach twardych Twojego komputera*

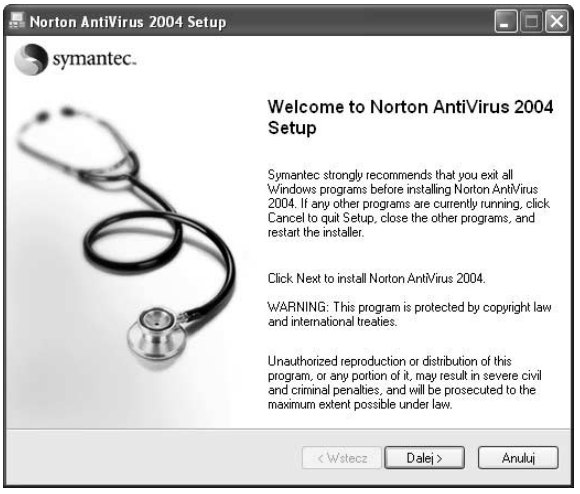
O zakończeniu poszukiwań poinformuje pojawienie się na ekranie okna programu *Notatnik*, wyświetlającego raport wygenerowany przez skaner antywirusowy (rysunek 5.4). Najważniejsza informacja — liczba wykrytych infekcji — wyświetlana jest w linii *Number of Infections Found*; obyś zawsze widział tam zero.

Rysunek 5.4. *Raport podsumowujący poszukiwania*



Aby kontynuować instalację, zamknij okno Notatnika i poczekaj chwilę na uruchomienie właściwego programu instalacyjnego (rysunek 5.5). Po planszy powitalnej — którą pominiesz, klikając przycisk *Dalej* — zostaniesz poproszony o przeczytanie i zaakceptowanie umowy licencyjnej, określającej warunki korzystania z programu. Jeśli zgadzasz się z jej warunkami i chcesz kontynuować instalację, umieść znacznik w polu *I accept the License Agreement* i kliknij przycisk *Dalej*.

Rysunek 5.5. *Plansza powitalna programu instalacyjnego pakietu Norton AntiVirus 2004*



Zaakceptowanie umowy licencyjnej jest warunkiem koniecznym instalacji programu.

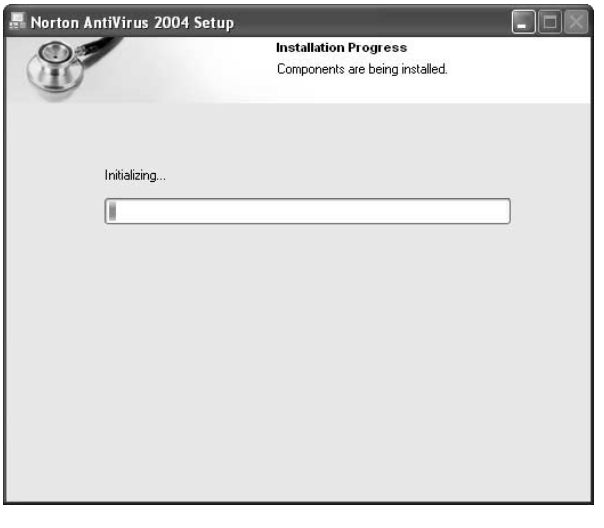
Kolejna plansza programu instalacyjnego pozwala określić nazwę folderu instalacyjnego programu (rysunek 5.6). W olbrzymiej większości przypadków standardowo zaproponowana nazwa (*C:\Program Files\Norton AntiVirus*) będzie jak najbardziej

Rysunek 5.6. *Wybór folderu instalacyjnego*

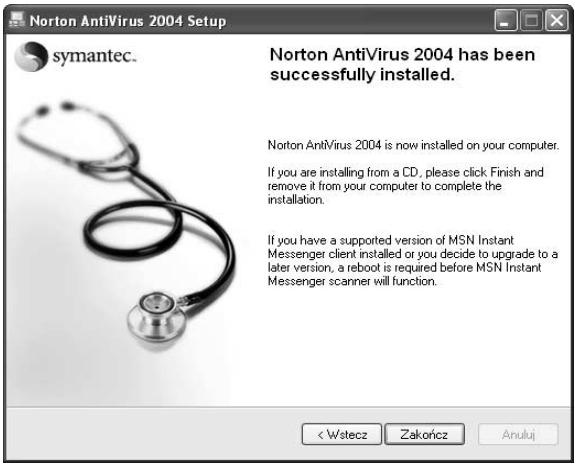
odpowiednia; gdybyś mimo to chciał zainstalować program w folderze o innej nazwie lub umieszczonym na innej partycji dyskowej, wprowadź nową nazwę w polu *Destination Folder* lub kliknij przycisk *Browse*, by wskazać folder docelowy na liście wyświetlanej w odrębnym oknie dialogowym. Wybór folderu zatwierdzisz, klikając przycisk *Dalej*, co jednocześnie wznowi proces instalacji.

Teraz w oknie programu instalacyjnego wyświetlone zostanie podsumowanie zebranych informacji. Sprawdź je dokładnie: kliknięcie przycisku *Dalej* natychmiast rozpocznie kopiowanie plików pakietu Norton AntiVirus na dysk twardy Twojego komputera oraz ich instalację (rysunek 5.7). Z kolei kliknięcie przycisku *Wstecz* pozwoli cofnąć się do jednego z poprzednich etapów instalacji i wprowadzić zmiany w podanych informacjach.

Rysunek 5.7. *Trwa instalacja pakietu*



Jeśli zdecydowałeś się na dokończenie instalacji i kliknąłeś przycisk *Dalej*, poczekaj parę minut. W tym czasie wszystkie potrzebne pliki zostaną skopiowane do folderu przeznaczenia i zarejestrowane w systemie; o aktualnym stanie procesu instalacji informować będzie pasek postępu, wyświetlany w oknie programu instalacyjnego. Po zakończeniu kopiowania na ekranie pojawi się jeszcze tekst zawierający najważniejsze informacje dotyczące produktu (pominiesz go, klikając przycisk *Dalej*) oraz plansza pożegnalna, informująca o pomyślnym zakończeniu całego procesu instalacji (rysunek 5.8).



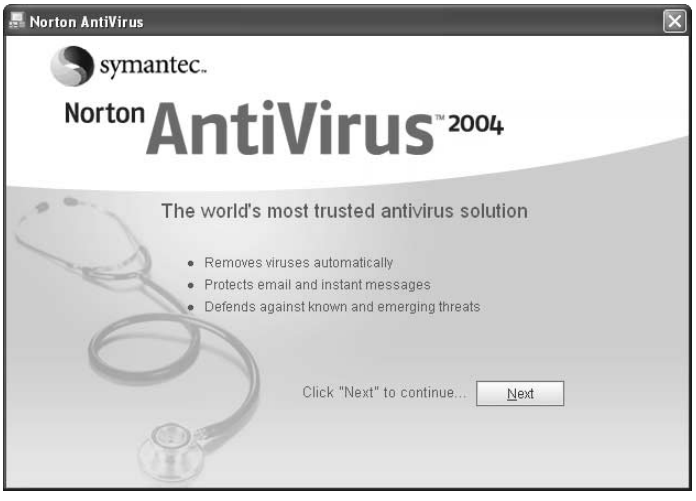
Rysunek 5.8. *Instalacja pakietu zakończyła się sukcesem!*

Choć instalację pakietu masz już za sobą, zanim zaczniesz korzystać z funkcji programu Norton AntiVirus, musisz przeprowadzić jego wstępną konfigurację i aktualizację. Kliknij przycisk *Zakończ* i poczekaj chwilę, aż na pulpicie otwarte zostanie okno powitalne automatycznego programu konfiguracyjnego.

Wstępna konfiguracja i aktualizacja pakietu

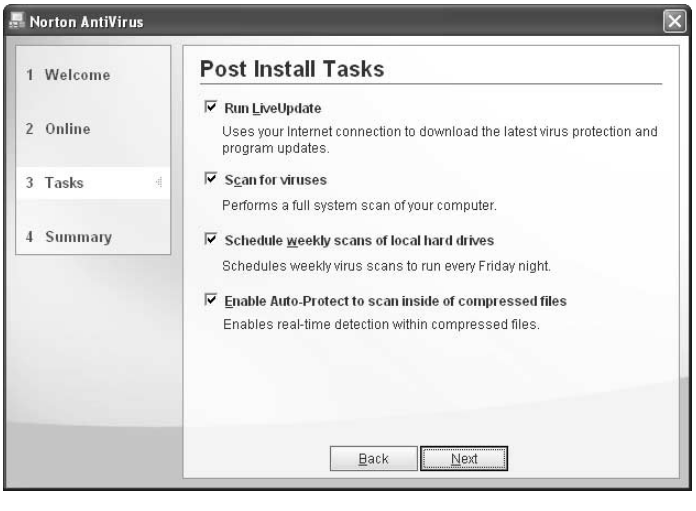
Aby ułatwić korzystanie z pakietu początkującym użytkownikom i zwiększyć bezpieczeństwo ich komputerów, firma Symantec zadecydowała, że zaraz po zakończeniu instalacji pakietu Norton AntiVirus powinien uruchamiać się moduł automatycznie konfigurujący i aktualizujący oprogramowanie oraz bazę informacji o wirusach. Dzięki temu nawet użytkownik, który nie jest świadom konieczności regularnego aktualizowania oprogramowania antywirusowego, w momencie instalowania pakietu zawsze będzie dysponował w miarę aktualną bazą informacji o wirusach — na pewno bardziej odpowiednią, niż dołączona do wersji instalacyjnej programu.

Chwilę po tym, jak z ekranu zniknie okno *Norton AntiVirus 2004 Setup*, należące do programu instalacyjnego, ujrzysz nowe okno dialogowe, zatytułowane tym razem po prostu *Norton AntiVirus* (rysunek 5.9). Jego zadaniem jest przeprowadzenie przez proces wyboru aktywnych modułów programu oraz przez pierwszą aktualizację bazy informacji o wirusach.



Rysunek 5.9. *Plansza powitalna automatycznego modułu konfiguracyjnego pakietu*

Kliknij przycisk *Next*, by pominąć planszę powitalną. Jeśli zainstalowałeś program w wersji testowej, wyświetlona zostanie informacja o liczbie dni testowania programu, które masz jeszcze do dyspozycji — zaakceptujesz ją, klikając przycisk *Next*; w wersji pełnej od razu wyświetlona zostanie lista zadań, które program Norton AntiVirus może wykonać po zakończeniu instalacji (rysunek 5.10).



Rysunek 5.10. *Zaraz po zakończeniu instalacji możesz uaktualnić bazę informacji o wirusach oraz przeskanować system*

Poszczególne zadania będą wykonane, jeśli w polu po lewej stronie ich nazw umieszczony będzie znacznik. Standardowo zaznaczone są wszystkie pozycje i nie powinieneś usuwać żadnego ze znaczników, by zapewnić swojemu komputerowi najwyższy poziom bezpieczeństwa.

- Pole *Run LiveUpdate* aktywuje natychmiastową aktualizację bazy informacji o wirusach oraz samego kodu programu; dzięki temu skaner antywirusowy pakietu Norton AntiVirus od razu będzie dysponował maksymalną skutecznością i nie zostanie zaskoczony przez „mikroba" nieznanego w czasie pisania programu.

- Pole *Scan for Viruses* zezwala na przeprowadzenie gruntownego skanowania komputera w poszukiwaniu wirusów; tak, zaraz przed instalacją został on już sprawdzony, teraz jednak skanowanie będzie znacznie dokładniejsze, a ponadto, jeśli zgodziłeś się na automatyczną aktualizację bazy informacji o wirusach — co bardzo polecam — w czasie tego skanowania zostanie użyta możliwie najbardziej aktualna wersja bazy, co nie pozostanie bez wpływu na skuteczność poszukiwań.
- Pole *Schedule weekly scans of local hard drives* kontroluje mechanizm automatycznego skanowania zasobów komputera w poszukiwaniu wirusów; jeśli pozostawisz w nim znacznik, Norton AntiVirus jeden raz w tygodniu z własnej inicjatywy przeskanuje wszystkie pliki i foldery zapisane na dyskach twardych Twojego komputera.

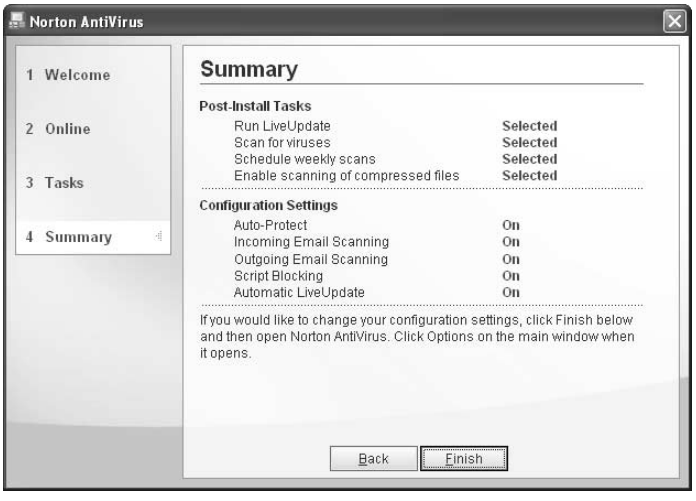
Jeśli jesteś zdania, że program komputerowy nie powinien samodzielnie decydować o rozpoczęciu wykonania tak obciążającej maszynę operacji jak skanowanie wszystkich plików i folderów, możesz wyłączyć tę opcję. Pamiętaj jednak, by jej brak zrównoważyć regularnym, najlepiej częstszym niż raz na tydzień ręcznym skanowaniem plików i folderów.

- Pole *Enable Auto-Protect to scan inside of compressed files* zezwala automatycznemu, aktywnemu skanerowi pakietu Norton AntiVirus na skanowanie zawartości otwieranych, kopiowanych i rozpakowywanych archiwów plików; pozwala to wykryć wirusy nawet wtedy, gdy ukryte są w skompresowanym archiwum plików, i powiadomić Cię o tym, zanim spróbujesz wydobyć zainfekowane pliki z archiwum i uruchomić je.

Skanowanie skompresowanych archiwów plików może stanowić poważne obciążenie obliczeniowe dla Twojego komputera, ponieważ przy każdym skanowaniu program Norton AntiVirus będzie musiał wydobyć wszystkie pliki z archiwum i przeskanować je. Ponieważ aktywny skaner antywirusowy i tak wykryje obecność wirusa podczas wydobywania zainfekowanego pliku z archiwum, na wolniejszych komputerach możesz wyłączyć tę opcję, zastępując ją większą własną czujnością.

Gdy zdecydujesz się już, które opcje chcesz pozostawić włączone, a z których możesz zrezygnować, kliknij przycisk *Next*. Po chwili oczekiwania na zastosowanie Twojego wyboru — w tym czasie na ekranie wyświetlane będzie okno dialogowe proszące o cierpliwość — program Norton AntiVirus wyświetli planszę podsumowującą wybór (rysunek 5.11).

Teraz pozostaje tylko kliknąć przycisk *Finish* i nadzorować wykonywanie zaplanowanych przed chwilą zadań. Pierwszym z nich będzie aktualizacja oprogramowania oraz bazy informacji o wirusach. Zajmuje się tym osobny moduł, wspólny dla wszystkich programów firmy Symantec i noszący nazwę LiveUpdate. Pozwala to za jednym zamachem zaktualizować wszystkie posiadane produkty tej firmy, a dzięki współdzieleniu części kodu między programami zaktualizowanie jednego z nich automatycznie aktualizuje też fragment pozostałych. Nie muszę chyba specjalnie podkreślać, że znacząco zmniejsza to ilość danych, które musisz pobrać z Internetu, a więc — jeśli łączysz się za pomocą modemu — również rachunki za połączenia telefoniczne.



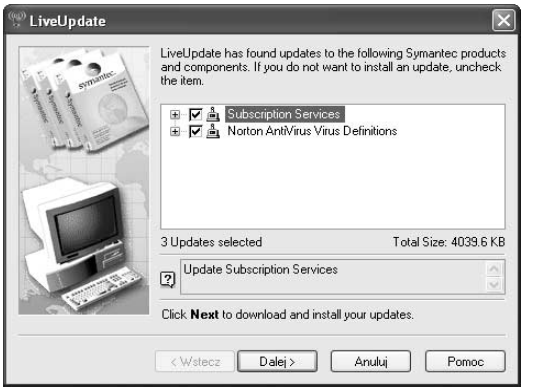
Rysunek 5.11. *Oto lista zadań, które pozostały jeszcze do wykonania, oraz informacja o uaktywnionych opcjach skanera antywirusowego*

Pierwsza plansza programu LiveUpdate prezentuje listę znanych modułowi programów i bibliotek firmy Symantec, zainstalowanych na Twoim komputerze (rysunek 5.12). Wystarczy, byś posiadał program Norton AntiVirus, a na liście tej znajdzie się już kilkanaście pozycji; na szczęście tylko dwie lub trzy z nich wymagają regularnej aktualizacji.

Rysunek 5.12. *Moduł LiveUpdate odpowiada za automatyczną aktualizację bazy danych o wirusach oraz kodu pakietu*

Pomiń planszę powitalną, klikając przycisk *Dalej*. Program LiveUpdate rozpocznie pobieranie z Internetu listy zaktualizowanych wersji pakietów oprogramowania; o postępie tej procedury informować będzie pasek postępu, wyświetlany u dołu okna *LiveUpdate* (rysunek 5.13). Po kilkunastu lub kilkudziesięciu sekundach zawartość okna samoczynnie się zmieni i będzie teraz wyświetlać listę modułów wymagających aktualizacji (rysunek 5.14). Standardowo wszystkie pozycje listy będą zaznaczone; jeśli koniecznie chcesz zabronić aktualizacji jednego z pakietów, usuń znacznik z lewej strony odpowiadającego mu wiersza listy.

Rysunek 5.13. *Trwa pobieranie informacji o dostępnych zaktualizowanych pakietach oprogramowania*

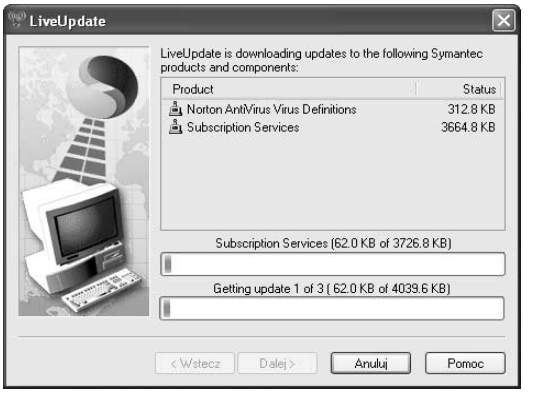


Rysunek 5.14. *Moduł LiveUpdate stwierdził możliwość zaktualizowania dwóch pakietów — w tym bazy informacji o wirusach*

Po prawej stronie okna *LiveUpdate*, poniżej listy pakietów wymagających aktualizacji, wyświetlana jest sumaryczna objętość danych, które zostaną pobrane z Internetu. Najczęściej nie będziesz zmuszany do pobierania dużej ilości danych — aktualizacje bazy informacji o wirusach nie mają dużego rozmiaru. Jedynie od czasu do czasu — gdy firma Symantec zaktualizuje jeden ze składników programu — będziesz musiał nieco przedłużyć czas korzystania z Internetu.

Zadecydowałeś już, na aktualizację których pakietów oprogramowania możesz sobie pozwolić? W takim razie kliknij przycisk *Dalej* i czekaj cierpliwie, gdyż LiveUpdate przeprowadza aktualizację. O postępie procedury aktualizacji będziesz na bieżąco informowany za pomocą dwóch pasków postępu wyświetlanych w oknie *LiveUpdate* (rysunek 5.15):

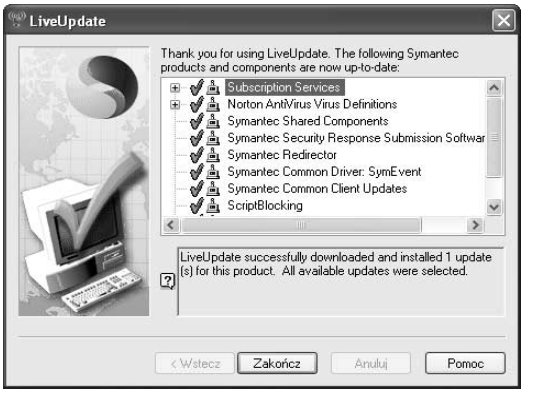
- górny z nich informuje o stopniu zaawansowania procesu pobierania z Sieci aktualizowanego składnika; powyżej paska wyświetlana jest informacja o liczbie już pobranych bajtów danych oraz o sumarycznym rozmiarze tego jednego pakietu,
- dolny informuje o stopniu zaawansowania procesu pobierania z Sieci wszystkich aktualizowanych składników; powyżej paska wyświetlana jest informacja o liczbie zaktualizowanych pakietów oprogramowania, liczbie już pobranych bajtów danych oraz o sumarycznym rozmiarze wszystkich aktualizowanych modułów.



Rysunek 5.15. *Trwa pobieranie zaktualizowanych pakietów oprogramowania z Internetu*

Sfinalizowanie pobierania zaktualizowanych pakietów oprogramowania z Internetu to jeszcze nie koniec procesu aktualizacji. Dopiero w momencie, gdy wszystkie zaktualizowane pakiety zostaną bezpiecznie zapisane na dysku twardym Twojego komputera i sprawdzona zostanie ich poprawność, program LiveUpdate przystąpi do zastępowania starych wersji plików nowymi. Również o postępie tego procesu będzie informował w swoim oknie za pomocą paska postępu.

Gdy cała aktualizacja zakończy się sukcesem, a poprawność jej wykonania zostanie zweryfikowana, ujrzysz ostatnią już planszę programu LiveUpdate, wyświetlającą ponownie listę zainstalowanych pakietów oprogramowania wraz z graficznymi symbolami (rysowanymi w każdym wierszu listy) określającymi, czy dysponujesz najnowszą wersją danego pakietu. Kliknij przycisk *Zakończ*, by zamknąć okno programu *LiveUpdate* i definitywnie zakończyć aktualizację (rysunek 5.16).



Rysunek 5.16. *Aktualizacja zakończona! Dysponujesz najnowszymi wersjami wszystkich składników pakietu Norton AntiVirus*

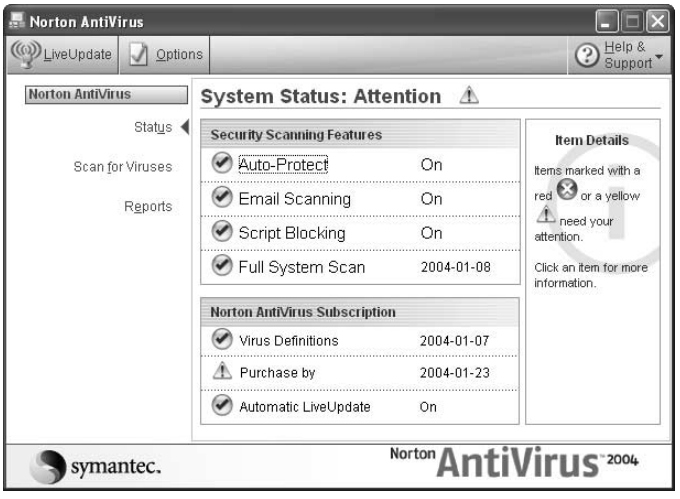
W tym momencie program Norton AntiVirus jest już aktywny, a najnowsza dostępna wersja bazy informacji o wirusach pozwala aktywnemu skanerowi antywirusowemu możliwie najskuteczniej chronić Twój komputer przed infekcją elektronicznych „mikrobów". O aktywności programu świadczy ikona aktywnego skanera antywirusowego, wyświetlana na pasku zadań systemu Windows, w prawym dolnym rogu ekranu — .

Aktywny skaner antywirusowy programu Norton AntiVirus będzie uruchamiał się samoczynnie za każdym razem, gdy włączysz komputer i załadujesz na nowo system operacyjny.

Zmiana konfiguracji pakietu

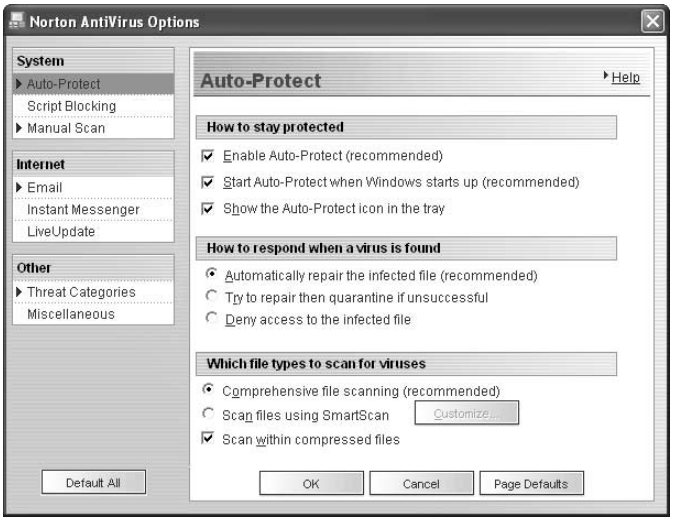
Chociaż w czasie instalacji pakietu Norton AntiVirus masz okazję dostosować go do własnych potrzeb, wyłączając zbędne opcje, możliwości konfiguracji programu sięgają znacznie dalej. Początkujący użytkownik, odwiedzający po raz pierwszy okno ustawień programu, może poczuć się wręcz przytłoczony olbrzymią liczbą dostępnych opcji. Jakie szczęście, że w zasadzie żadnej z nich nie musisz zmieniać, a sięgnięcie po nie konieczne jest tylko wtedy, gdy chcesz zmienić jakiś aspekt funkcjonowania pakietu.

Okno konfiguracji pakietu możesz uruchomić na dwa sposoby. Jeśli otworzysz główne okno programu, zatytułowane *Norton AntiVirus* (dwukrotnie klikając ikonę programu, wyświetlaną w prawym dolnym rogu ekranu na pasku zadań systemu Windows lub klikając tę ikonę prawym przyciskiem myszy i w menu kontekstowym wskazując pozycję *Open Norton AntiVirus*), wystarczy kliknąć przycisk *Options*, znajdujący się w jego lewym górnym rogu (rysunek 5.17). Istnieje też prostsza droga: kliknij prawym przyciskiem myszy ikonę programu wyświetlaną na systemowym pasku zadań i z menu kontekstowego wybierz pozycję *Configure Norton AntiVirus*.



Rysunek 5.17. *Kliknięcie przycisku Options pozwoli rozpocząć konfigurację programu*

Niezależnie od wybranej metody na ekranie powinno pojawić się okno dialogowe *Norton AntiVirus Options* (rysunek 5.18). Podzielone jest ono na szereg zakładek, których etykiety wyświetlane są — jedna pod drugą — w lewym panelu okna. Zauważ, że po prawej stronie niektórych etykiet znajduje się mały ciemny trójkącik: oznacza to, że kliknięcie etykiety nie tylko wyświetli w prawym panelu okna nową planszę ustawień, ale też odsłoni na liście kategorii ustawień dodatkowe etykiety zakładek.



Rysunek 5.18. *Opcje automatycznej ochrony antywirusowej*

Pamiętaj, że w każdej chwili możesz cofnąć wprowadzone zmiany — nawet gdybyś zapomniał, które opcje zmieniłeś. Przycisk *Default All* pozwoli wrócić do domyślnej konfiguracji całego programu, zaś przycisk *Page Defaults* przywraca domyślne wartości opcji wyświetlanych na aktywnej planszy okna dialogowego *Norton AntiVirus Options*.

Zakładka AutoProtect

Poszczególne pola zakładki *AutoProtect* — zawierającej podstawowe opcje konfiguracyjne aktywnego skanera antywirusowego Norton AntiVirus, non stop czuwającego nad bezpieczeństwem Twoich plików — mają następujące znaczenie (rysunek 5.18).

Grupa How to stay protected

- *Enable Auto-Protect* — uruchamia aktywny skaner antywirusowy, monitorujący wszystkie pliki zapisywane na dysku twardym i z niego odczytywane.
- *Start Auto-Protect when Windows starts up (recommended)* — powoduje uruchamianie aktywnego skanera antywirusowego zaraz po starcie systemu Windows.
- *Show the Auto-Protect icon in the tray* — włącza opcję wyświetlania ikony programu Norton AntiVirus na pasku zadań systemu Windows, w prawym dolnym rogu ekranu.

Jeśli ukryjesz ikonę pakietu Norton AntiVirus, usuwając znacznik z pola *Show the Auto-Protect icon in the tray*, dostęp do funkcji pakietu będziesz mógł wciąż uzyskać z poziomu menu *Start* systemu Windows lub za pomocą ikony programu, umieszczonej na pulpicie.

Grupa How to respond when a virus is found

- *Automatically repair the infected file (recommended)* — gdy aktywny skaner antywirusowy wykryje wirusa, natychmiast — bez pytania o zgodę — usunie go z pliku, przywracając oryginalną zawartość zbioru.
- *Try to repair then quarantine if unsuccessful* — gdy aktywny skaner antywirusowy wykryje wirusa, przeprowadzi próbę usunięcia go (przywracając oryginalną zawartość zainfekowanego pliku), a gdy się to nie powiedzie — zastosuje wobec zainfekowanego pliku kwarantannę, uniemożliwiając Ci dostęp do niego.
- *Deny access to the infected file* — w razie wykrycia przez aktywny skaner antywirusowy wirusa wewnątrz pliku, dostęp do tego pliku zostanie zablokowany, lecz plik pozostanie nienaruszony; usunięcie wirusa będzie mogło nastąpić dopiero na skutek ręcznego uaktywnienia funkcji skanowania plików (skanera pasywnego).

Grupa which file types to scan for viruses

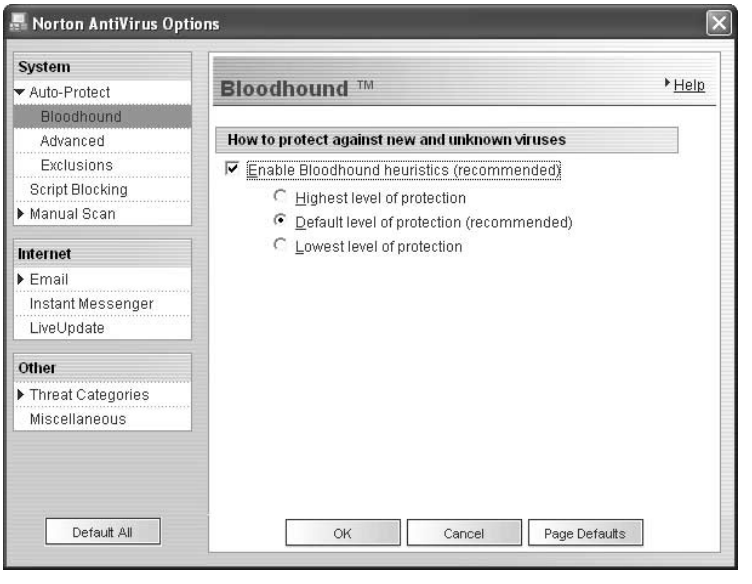
- *Comprehensive file scanning (recommended)* — aktywny skaner antywirusowy będzie analizował wszystkie pliki, niezależnie od ich typu; umożliwi to wykrycie wirusa nawet, jeśli zainfekowany plik będzie miał niestandardowe rozszerzenie nazwy.
- *Scan files using SmartScan* — skanowane będą tylko wybrane, najbardziej zagrożone infekcją typy plików.
- *Scan within compressed files* — włączenie tej opcji umożliwi aktywnemu skanerowi antywirusowemu wydobywanie plików z wnętrza otwieranych archiwów i analizowanie ich; pozwala to na wykrywanie infekcji, zanim jeszcze spróbujesz wydobyć zainfekowane pliki z archiwum i zapisać je na dysku twardym, zwiększa jednak znacznie obciążenie obliczeniowe komputera i może wyraźnie pogorszyć jego wydajność.

Zakładka AutoProtect: Bloodhound

Poszczególne pola zakładki *AutoProtect: Bloodhound* — zawierającej opcje konfiguracyjne heurystycznego aktywnego skanera antywirusowego — mają następujące znaczenie (rysunek 5.19).

Grupa How to protect against new and unknown viruses

- *Enable Bloodhound heuristics (recommended)* — uaktywnia heurystyczny skaner antywirusowy, który analizuje kod programów i poszukuje w nich fragmentów, które przypominają kod wirusów; umożliwia to wykrywanie nowych, nieznanych jeszcze programowi wirusów na podstawie poszlak, może jednak również powodować, że zaawansowane programy narzędziowe będą rozpoznawane jako wirusy.



Rysunek 5.19. *Opcje aktywnego heurystycznego skanera antywirusowego*

Pola *Highest level of protection*, *Default level of protection* oraz *Lowest level of protection* pozwolą przesunąć próg, od którego program traktuje niebezpieczny kod jako wirusa. Obniżając poziom bezpieczeństwa (pole *Lowest level of protection*), zmniejszasz prawdopodobieństwo wykrycia nowych typów wirusów, jednak unikasz sytuacji, w której normalny, niezainfekowany program nie będzie mógł funkcjonować. Z kolei podniesienie poziomu bezpieczeństwa (pole *Highest level of protection*) pozwoli czuć się bezpieczniej, może jednak spowodować kłopoty z użytkowaniem niektórych programów.

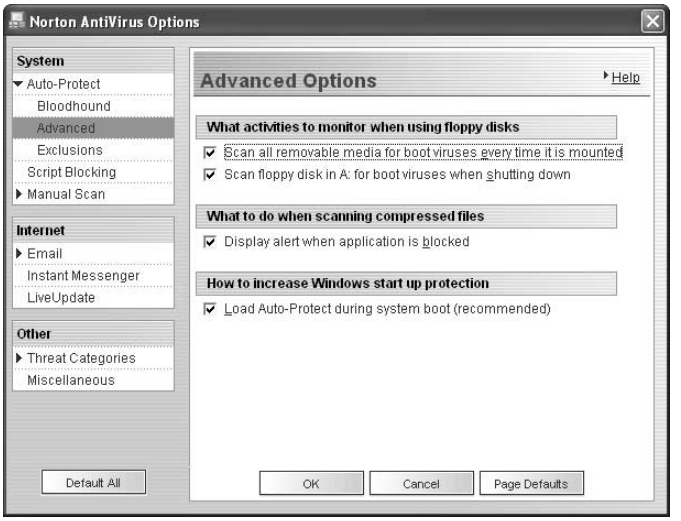
Pamiętaj, że nawet jeśli aktywny heurystyczny skaner antywirusowy zablokuje dostęp do jakiegoś programu, co do którego masz pewność, że nie jest zainfekowany, zawsze możesz wyłączyć ten program z zakresu działania aktywnego skanera antywirusowego. O definiowaniu wyjątków dowiesz się już za chwilę.

Zakładka AutoProtect: Advanced

Poszczególne pola zakładki *AutoProtect: Advanced* — zawierającej zaawansowane opcje konfiguracyjne aktywnego skanera antywirusowego Norton AntiVirus — mają następujące znaczenie (rysunek 5.20).

Grupa What activities to minotor when using floppy disks

- *Scan all removable media for boot viruses every time it is mounted* — włącza opcję sprawdzania używanych dyskietek pod kątem występowania w ich sektorze rozruchowym wirusów uaktywniających się w razie próby uruchomienia systemu operacyjnego z dyskietki.



Rysunek 5.20. *Zaawansowane opcje aktywnego skanera antywirusowego*

Wirusy, które uruchamiają się podczas próby załadowania systemu operacyjnego z dyskietki lub płyty CD-ROM, stanowią dobry powód, by w programie konfiguracyjnym płyty głównej uniemożliwić ładowanie systemu operacyjnego z nośników innych niż dysk twardy. Uruchamianie systemu operacyjnego z dyskietki lub płyty CD-ROM potrzebne jest tylko w czasie instalowania systemu operacyjnego; zaraz po udanej instalacji powinieneś tę opcję wyłączyć, by przypadkiem pozostawiona w napędzie zainfekowana dyskietka lub płyta CD nie stała się zaczątkiem infekcji.

- *Scan floppy disk in A: for boot viruses when shutting down* — włącza opcję skanowania dyskietki włożonej do stacji dysków w czasie, gdy system operacyjny kończy swoją pracę i przygotowuje się do wyłączania lub ponownego uruchomienia komputera; zabezpiecza to przed zainfekowaniem komputera wirusem znajdującym się w sektorze rozruchowym dyskietki, która pozostawała włożona do stacji dysków, z której jednak użytkownik w ogóle nie korzystał (a więc nie została sprawdzona mimo aktywności opcji *Scan all removable media for boot viruses every time it is mounted*).

Grupa What to do when scanning compressed files

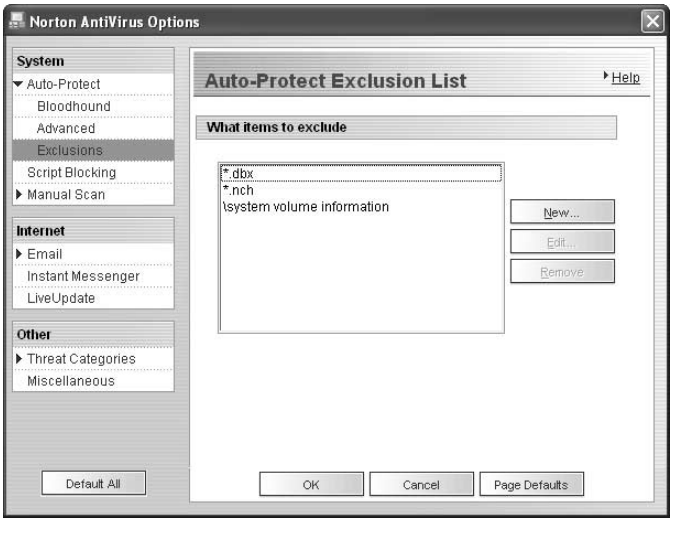
- *Display alert when application is blocked* — umożliwia pakietowi Norton AntiVirus wyświetlanie okna informującego o zablokowaniu programu, który usiłował otworzyć archiwum plików zawierające zainfekowane pliki.

Grupa How to increase Windows start up protection

- *Load Auto-Protect during system boot* — powoduje włączanie aktywnego skanera antywirusowego już w czasie pierwszych etapów uruchamiania systemu operacyjnego, co może zapobiec zainfekowaniu komputera przez bardziej rozbudowane wirusy.

Zakładka AutoProtect: Exclusions

Zakładka *Auto-Protect Exclusions* umożliwia określenie listy plików, których aktywny skaner antywirusowy nigdy nie będzie próbował skanować (rysunek 5.21). Choć opcja ta pociąga za sobą potencjalną możliwość pogorszenia ochrony antywirusowej komputera, prawidłowo używana może znacznie podnieść wydajność komputera, nie zwiększając jednocześnie znacząco zagrożenia ze strony wirusów.



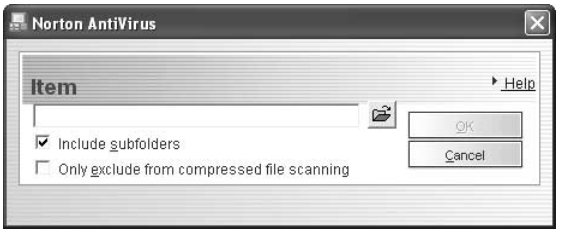
Rysunek 5.21. *Lista plików i folderów, których aktywny skaner antywirusowy nie powinien nigdy analizować*

Zawsze lepiej prawidłowo skonfigurować program antywirusowy, by nie skanował niepotrzebnie plików, które nie powinny zostać zainfekowane, niż wyłączać całkowicie aktywny skaner antywirusowy w czasie, gdy potrzebna jest cała moc obliczeniowa komputera.

Lista wyświetlana na środku okna dialogowego prezentuje definicje elementów, których aktywny skaner antywirusowy nie będzie próbował skanować. Standardowo zawiera ona wpisy blokujące skanowanie skrzynek pocztowych programu Microsoft Outlook Express (**.dbx*, **.nch*) — poczta elektroniczna i tak jest skanowana pod kątem obecności wirusów, powtórne skanowanie byłoby zatem wyłącznie stratą czasu — oraz folder *System Volume Information*, w którym przechowywane są często wykorzystywane informacje systemowe (skanowanie plików znajdujących się w tym folderze spowodowałby znaczące pogorszenie wydajności komputera).

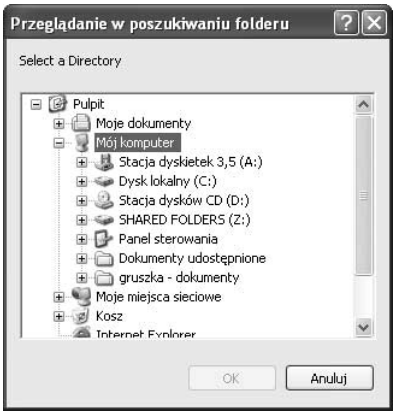
Folder *System Volume Information* i tak jest wprost niedostępny dla użytkowników komputera — włączając w to użytkowników o uprawnieniach administratora — zatem zainfekowanie plików, które się w nim znajdują, jest mało prawdopodobne.

Aby dodać nowy element do listy elementów wykluczonych z działania aktywnego skanera antywirusowego, kliknij przycisk *New*. Na ekranie pojawi się okno dialogowe *Norton AntiVirus*, pozwalające wprowadzić nazwę wykluczanego elementu (rysunek 5.22).



Rysunek 5.22. *Określanie elementów, które mają być wykluczone z działania aktywnego skanera antywirusowego*

Definicje wieloznaczne — na przykład definicję `*.txt`, wyłączającą ze skanowania wszystkie pliki, których nazwa kończy się znakami *.txt* — musisz wprowadzić z klawiatury bezpośrednio w polu *Item*. Definicje dotyczące pojedynczych plików lub folderów możesz utworzyć za pomocą okna dialogowego *Przeglądanie w poszukiwaniu folderu*, dającego możliwość wskazania elementu na liście (rysunek 5.23): kliknij przycisk , by wywołać to okno dialogowe, podświetl na liście plik lub folder, który chcesz wykluczyć z zakresu poszukiwań aktywnego skanera antywirusowego, po czym kliknij przycisk *OK*, aby nazwa wskazanego elementu została skopiowana do pola *Item* okna dialogowego *Norton AntiVirus*.



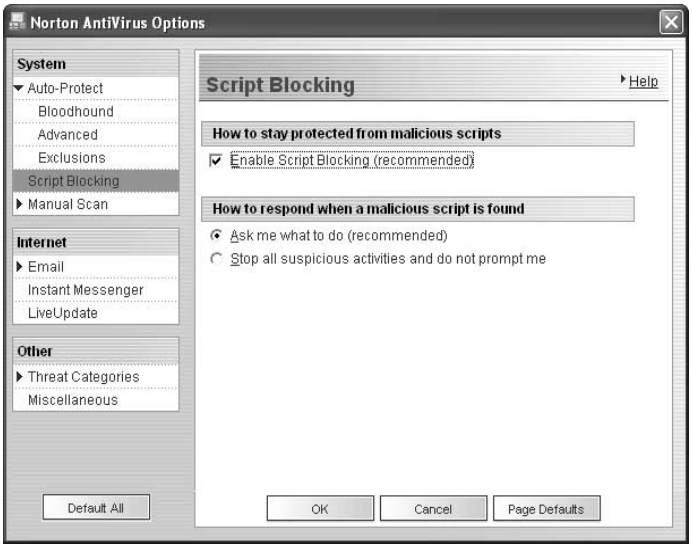
Rysunek 5.23. *Wybór elementu — grupy plików lub folderów — z listy*

Jeśli elementem, który wykluczasz z zakresu skanowania, jest folder, możesz nakazać wykluczenie nie tylko plików znajdujących się w tym folderze, ale również wszystkich folderów podrzędnych wraz z ich zawartością. Aby to uczynić, umieść znacznik w polu *Include subfolders*. Jeśli z kolei Twoim zamiarem jest jedynie uniemożliwienie skanowania archiwów plików, składowanych we wskazanym folderze (co jest czynnością bardzo czasochłonną), umieść znacznik w polu *Only exclude from compressed file scanning*: spowoduje to, że wewnątrz wybranego folderu skanowane będą tylko i wyłącznie pojedyncze pliki, podczas gdy skompresowane archiwa plików będą ignorowane.

Klikając przycisk *OK*, spowodujesz zakończenie tworzenia definicji, zamknięcie okna dialogowego *Norton AntiVirus* oraz dodanie definicji do listy wykluczeń. Jeśli w czasie tworzenia definicji pomyliłeś się i dopiero teraz to zauważyłeś, nic straconego! Przycisk *Edit* pozwoli wprowadzić dowolne zmiany w definicji, zaś przycisk *Remove* — usunąć podświetlony element listy.

Zakładka Script Blocking

Poszczególne pola zakładki *Script Blocking* — zawierającej opcje konfiguracyjne skanera wykrywającego niebezpieczne skrypty — mają następujące znaczenie (rysunek 5.24).



Rysunek 5.24. *Opcje blokowania groźnych skryptów*

Grupa How to stay protected from malicious scripts

- *Enable Script Blocking (recommended)* — uaktywnia blokadę, która uniemożliwia skryptom JavaScript i Visual Basic (zarówno tym uruchamianym bezpośrednio przez system operacyjny, jak i wykonywanym pod kontrą przeglądarki internetowej) uzyskanie dostępu do zawartości dysku twardego, a więc pobieranie i niszczenie Twoich danych; wyłączaj tę opcję, tylko jeśli często używasz sprawdzonych skryptów, które muszą korzystać z plików dyskowych, i nie chcesz za każdym razem udzielać zgody na kontynuowanie pracy skryptu.

Grupa How to respond when a malicious script is found

- *Ask me what to do (recommended)* — w razie wykrycia potencjalnie niebezpiecznego skryptu program Norton AntiVirus wyświetli okno dialogowe proszące o decyzję kontynuowania pracy skryptu; pozwoli to uniknąć przerywania pracy pożytecznych skryptów, świadomie uruchomionych.
- *Stop all suspicious activities and do not prompt me* — blokuje działanie wszystkich potencjalnych skryptów, daje w ten sposób najwyższy stopień bezpieczeństwa, choć ogranicza możliwość tworzenia prostych skryptów automatyzujących codzienne czynności.