McAfee®

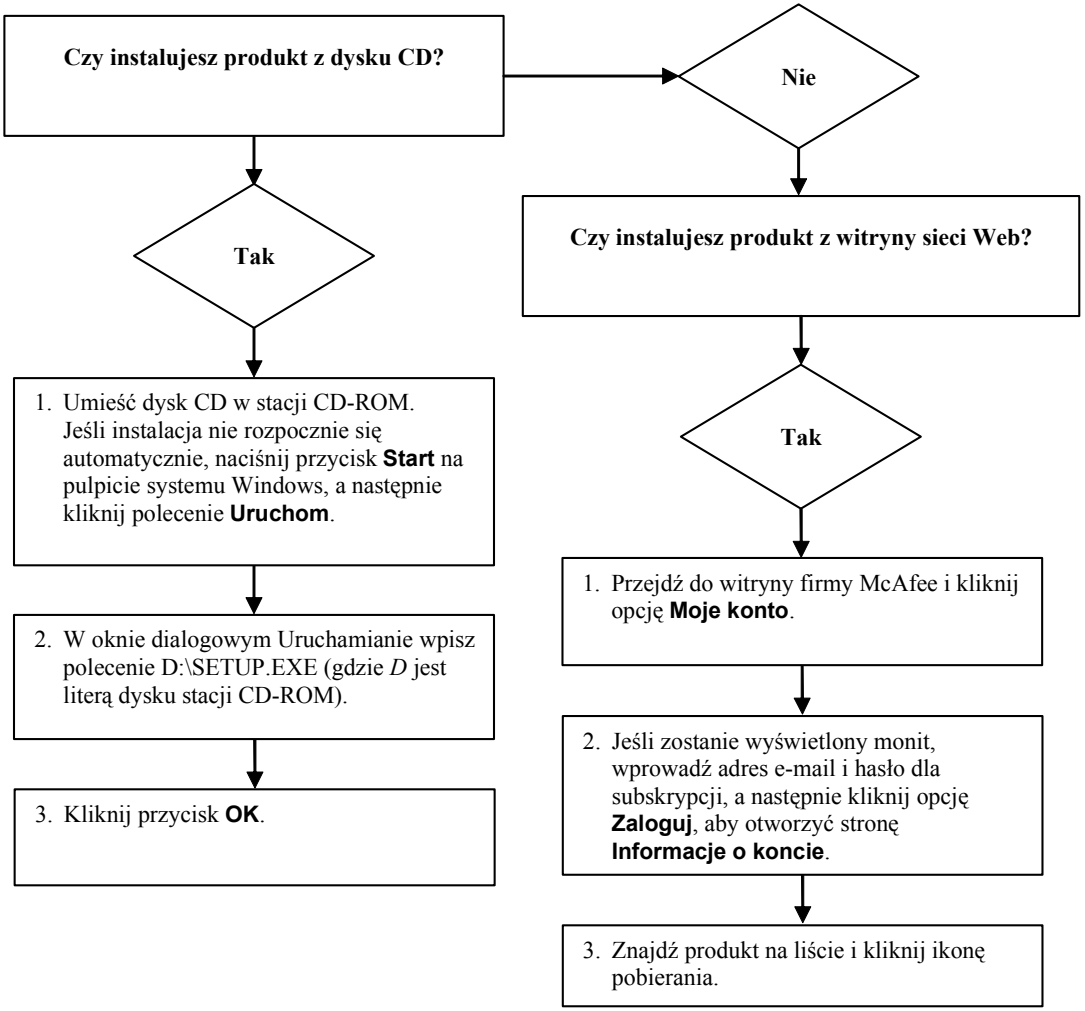
virusscan®

Podręcznik użytkownika

McAfee®

Karta Szybki start

Wydrukowanie tej wygodnej w użyciu strony pomocy może przydać się podczas instalacji produktu z dysku CD-ROM lub witryny sieci Web.



Więcej informacji

Do przeglądania podręczników użytkownika zamieszczonych na dysku CD-ROM produktu wymagany jest zainstalowany program Acrobat Reader. Jeśli program ten nie został zainstalowany, należy zainstalować go teraz z dysku CD-ROM produktu firmy McAfee.

1. Włóż dysk CD-ROM produktu do stacji dysków CD-ROM.
2. Otwórz Eksploratora Windows: na pulpicie systemu Windows kliknij przycisk **Start**, a następnie kliknij polecenie **Wyszukaj**.
3. Znajdź folder Manuals i kliknij dwukrotnie plik .PDF podręcznika użytkownika, który chcesz otworzyć.

Korzyści z rejestracji

Firma McAfee zaleca wykonanie prostej procedury (dostępnej w produkcie) w celu wysłania rejestracji bezpośrednio do naszej firmy. Rejestracja zapewnia otrzymanie na czas odpowiedniej pomocy technicznej oraz następujące korzyści:

- BEZPŁATNA elektroniczna pomoc techniczna.
- Aktualizacje pliku definicji wirusów (.DAT) przez jeden rok po zainstalowaniu zakupionego oprogramowania VirusScan.

  Cennik oferty dodatkowego roku pobierania sygnatur wirusów znajduje się w witrynie http://www.mcafee.com/.
- 60-dniowa gwarancja wymiany dysku CD-ROM z oprogramowaniem w przypadku wystąpienia uszkodzeń lub błędów.
- Aktualizacje filtru SpamKiller przez jeden rok po zainstalowaniu zakupionego oprogramowania SpamKiller.

  Cennik oferty dodatkowego roku aktualizacji filtru znajduje się w witrynie http://www.mcafee.com/.
- Aktualizacje zakupionego oprogramowania McAfee Internet Security Suite przez jeden rok po jego zainstalowaniu.

  Cennik oferty dodatkowego roku aktualizacji treści znajduje się w witrynie http://www.mcafee.com/.

Pomoc techniczna

Aby uzyskać pomoc techniczną, należy odwiedzić witrynę

http://www.mcafeehelp.com/.

W witrynie tej przez całą dobę dostępny jest łatwy w użyciu Kreator odpowiedzi umożliwiający rozwiązanie najczęściej spotykanych problemów.

Doświadczeni użytkownicy mogą także korzystać z opcji zaawansowanych, takich jak wyszukiwanie według słowa kluczowego lub drzewo pomocy. Jeśli rozwiązanie nie zostanie znalezione, użytkownik może skorzystać z bezpłatnych opcji Chat Now! i E-mail Express! firmy McAfee. Korzystając z tych narzędzi, można szybko i bezpłatnie skontaktować się przez Internet z wykwalifikowanymi pracownikami pomocy technicznej. W przeciwnym wypadku informacje na temat telefonicznej pomocy technicznej można uzyskać w witrynie

http://www.mcafeehelp.com/.

Spis treści

Karta Szybki start iii

1 Wprowadzenie 7

Nowe funkcje 7
Wymagania systemowe 8
Testowanie programu VirusScan 9
Testowanie programu ActiveShield 9
Testowanie funkcji skanowania 10
Korzystanie z programu McAfee SecurityCenter 11

2 Korzystanie z programu McAfee VirusScan 13

Korzystanie z programu ActiveShield 13
Włączanie i wyłączanie programu ActiveShield 13
Konfigurowanie opcji programu ActiveShield 14
Jak działa system generowania alertów zabezpieczeń 25
Ręczne skanowanie komputera 28
Ręczne skanowanie w poszukiwaniu wirusów i innych zagrożeń 28
Automatyczne skanowanie w poszukiwaniu wirusów i innych zagrożeń 32
Jak działa system wykrywania zagrożeń 34
Zarządzanie plikami poddanymi kwarantannie 35
Tworzenie dyskietki ratunkowej 36
Zabezpieczanie dyskietki ratunkowej przed zapisem 37
Korzystanie z dyskietki ratunkowej 38
Aktualizacja dyskietki ratunkowej 38
Automatyczne przesyłanie informacji o wirusach 38
Przesyłanie raportu do mapy ataków wirusowych na świecie 38
Przeglądanie mapy ataków wirusowych na świecie 39
Aktualizacja programu VirusScan 41
Automatyczne sprawdzanie aktualizacji 41
Ręczne sprawdzanie aktualizacji 41

Skorowidz 43

Wprowadzenie 1

McAfee VirusScan - Zapraszamy!

Program McAfee VirusScan to udostępniana w drodze subskrypcji usługa zapewniająca kompleksową, niezawodną ochronę antywirusową przed najnowszymi zagrożeniami. Dzięki wykorzystaniu wielokrotnie nagradzanej technologii skanowania opracowanej przez firmę McAfee program VirusScan zabezpiecza system przed wirusami, robakami, końmi trojańskimi, podejrzanymi skryptami, atakami hybrydowymi i innymi zagrożeniami.

Funkcje programu:

ActiveShield - skanuje pliki w momencie, gdy użytkownik lub system próbuje uzyskać do nich dostęp.

Skanowanie - wyszukiwanie wirusów i innych zagrożeń na dyskach twardych, dyskietkach oraz w pojedynczych plikach i folderach.

Kwarantanna - powoduje zaszyfrowanie i tymczasowe odizolowanie podejrzanych plików w folderze kwarantanny do momentu, gdy będzie można podjąć odpowiednie działanie.

Wykrywanie wrogiej działalności - monitorowanie pracy komputera w poszukiwaniu objawów działalności wirusów, robaków i podejrzanych skryptów.

Nowe funkcje

W bieżącej wersji programu VirusScan dostępne są następujące nowe funkcje:

- **Usuwanie oprogramowania szpiegującego i reklamowego**
  Program VirusScan rozpoznaje i usuwa oprogramowanie szpiegujące i reklamowe, a także wszelkie inne programy narażające prywatność użytkownika i spowalniające pracę komputera.
- **Codzienne automatyczne aktualizacje**
  Codzienne automatyczne aktualizacje programu VirusScan zapewniają ochronę przed najnowszymi zagrożeniami bezpieczeństwa - zarówno znanymi, jak tymi, których jeszcze nie zidentyfikowano.
- **Szybkie skanowanie w tle**
  Szybkie i nieprzeszkadzające w pracy skanowanie identyfikuje i usuwa wirusy, konie trojańskie, robaki, oprogramowanie szpiegujące i reklamowe oraz dialery i inne zagrożenia.

- **Ostrzeganie o zagrożeniach bezpieczeństwa w czasie rzeczywistym**
  Alerty zabezpieczeń powiadamiają o epidemiach wirusowych i zagrożeniach bezpieczeństwa oraz udostępniają opcje reagowania w celu usunięcia, zneutralizowania lub uzyskania dodatkowych informacji na temat zagrożenia.

- **Wykrywanie i czyszczenie w wielu punktach ataku**
  Program VirusScan monitoruje i czyści w kluczowych punktach ataku w komputerze: skanowane są przychodzące wiadomości e-mail i ich załączniki, załączniki do wiadomości błyskawicznych, a także pliki pobierane z Internetu.

- **Monitorowanie poczty e-mail w poszukiwaniu działalności robaków**
  Program WormStopper™ monitoruje podejrzane zmasowane wysyłanie wiadomości e-mail oraz powstrzymuje wirusy i robaki internetowe przed przenoszeniem się poprzez pocztę elektroniczną na inne komputery.

- **Monitorowanie skryptów w poszukiwaniu działalności robaków**
  Program ScriptStopper™ monitoruje podejrzane wykonania skryptów oraz powstrzymuje wirusy i robaki internetowe przed przenoszeniem się poprzez pocztę elektroniczną na inne komputery.

- **Bezpłatna pomoc techniczna udzielana za pośrednictwem poczty e-mail i wiadomości błyskawicznych**
  Ekipa pomocy technicznej zapewnia szybką i przystępną pomoc za pośrednictwem poczty elektronicznej i wiadomości błyskawicznych.

Wymagania systemowe

- System operacyjny Microsoft® Windows 98, Windows Me, Windows 2000 lub Windows XP
- Komputer osobisty z procesorem zgodnym z Pentium
  System operacyjny Windows 98, 2000: 133 MHz lub szybszy
  System operacyjny Windows Me: 150 MHz lub szybszy
  System operacyjny Windows XP (Home i Professional): 300 MHz lub szybszy
- Pamięć RAM
  System operacyjny Windows 98, Me, 2000: 64 MB
  System operacyjny Windows XP (Home i Professional): 128 MB
- 40 MB miejsca na twardym dysku
- Przeglądarka Microsoft® Internet Explorer w wersji 5.5 lub nowszej

  UWAGA
  Aby pobrać najnowszą wersję przeglądarki Internet Explorer, odwiedź witrynę firmy Microsoft http://www.microsoft.com/worldwide/.

Obsługiwane programy pocztowe

- Zgodne z protokołem POP3 (Outlook Express, Outlook, Eudora, Netscape)

Obsługiwane programy wiadomości błyskawicznych

- AOL Instant Messenger w wersji 2.1 lub nowszej
- Yahoo Messenger w wersji 4.1 lub nowszej
- Microsoft Windows Messenger w wersji 3.6 lub nowszej
- MSN Messenger w wersji 6.0 lub nowszej

Testowanie programu VirusScan

Przed pierwszym uruchomieniem programu VirusScan warto sprawdzić poprawność jego instalacji. Aby przetestować osobno działanie programu ActiveShield i funkcji skanowania, wykonaj opisane poniżej czynności.

Testowanie programu ActiveShield

UWAGA
Aby sprawdzić poprawność działania programu ActiveShield, korzystając z karty VirusScan w programie SecurityCenter, kliknij opcję **Testuj program VirusScan**. Spowoduje to wyświetlenie witryny sieci Web z wykazem często zadawanych pytań dotyczących procedury testowej.

Aby przetestować program ActiveShield:

1. W swojej przeglądarce internetowej przejdź do witryny http://www.eicar.com/.
2. Kliknij łącze **The AntiVirus testfile eicar.com** (Plik testowy eicar.com dla programów antywirusowych).
3. Przejdź do dolnej części strony. Pod nagłówkiem **Pobierz** znajdują się cztery łącza:
4. Kliknij łącze **eicar.com**.

Jeśli program ActiveShield działa prawidłowo, wykryje plik eicar.com natychmiast po kliknięciu łącza. Można także spróbować usunąć wykryte pliki lub poddać je kwarantannie, aby sprawdzić, jak program ActiveShield radzi sobie z potencjalnymi zagrożeniami. Szczegółowe informacje znajdziesz w rozdziale *Jak działa system generowania alertów zabezpieczeń* na stronie 25.

Testowanie funkcji skanowania

Przed przetestowaniem funkcji skanowania musisz wyłączyć program ActiveShield, aby zapobiec wykrywaniu przez niego plików testowych, zanim zrobi to funkcja skanowania. Następnie pobierz pliki testowe.

Aby pobrać pliki testowe:

1. Wyłącz program ActiveShield: kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Wyłącz**.
2. Pobierz pliki testowe EICAR z witryny internetowej EICAR:
   a. Przejdź do witryny http://www.eicar.com/.
   b. Kliknij łącze **The AntiVirus testfile eicar.com** (Plik testowy eicar.com dla programów antywirusowych).
   c. Przejdź do dolnej części strony. Pod nagłówkiem **Pobierz** znajdują się następujące łącza:

      eicar.com - jest to plik zawierający wiersz tekstu wykrywany przez program VirusScan jako kod wirusa.

      eicar.com.txt (opcjonalnie) - jest to ten sam plik zapisany pod inną nazwą, aby mogli go pobrać użytkownicy, którzy mają problem z pobraniem pierwszego pliku. Po pobraniu pliku należy zmienić jego nazwę na „eicar.com”.

      eicar_com.zip - jest to kopia zbioru testowego umieszczona w skompresowanym pliku ZIP (archiwum w formacie WinZip™).

      eicarcom2.zip - jest to kopia zbioru testowego umieszczona w skompresowanym pliku ZIP, który znajduje się w innym skompresowanym pliku ZIP.

   d. Kliknij odpowiednie łącze, aby pobrać żądany plik. Spowoduje to otwarcie okna dialogowego **File Download** (Pobieranie pliku).
   e. Kliknij kolejno przyciski **Zapisz** i **Utwórz nowy folder**, a następnie zmień nazwę folderu na **VSO Scan Folder**.
   f. Kliknij dwukrotnie folder **VSO Scan Folder**, a następnie kliknij ponownie przycisk **Zapisz** w każdym oknie dialogowym **Zapisz jako**.
3. Po pobraniu w ten sposób wszystkich plików zamknij przeglądarkę Internet Explorer.
4. Włącz program ActiveShield: kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Włącz**.

Aby przetestować funkcję skanowania:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Skanuj**.
2. Za pomocą drzewa katalogów dostępnego w okienku po lewej stronie przejdź do folderu **VSO Scan Folder**, w którym zostały zapisane pliki:
   a. Kliknij znak **+** obok ikony dysku C.
   b. Kliknij folder **VSO Scan Folder**, aby go wyróżnić (nie należy klikać znajdującego się obok znaku **+**).

      W ten sposób do skanowania zostanie wybrany tylko ten folder. Można również skopiować pliki testowe do dowolnych lokalizacji na dysku twardym, aby przeprowadzić skanowanie w warunkach zbliżonych do rzeczywistych.
3. Upewnij się, że zaznaczone są wszystkie opcje dostępne w obszarze **Opcje skanowania** okna dialogowego **Skanowanie**.
4. Kliknij przycisk **Skanuj** w prawym dolnym rogu okna dialogowego.

   Program VirusScan skanuje folder **VSO Scan Folder**. Pliki testowe EICAR zapisane w tym folderze pojawią się w obszarze **Lista wykrytych plików**. Jeśli tak się stało, funkcja skanowania działa poprawnie.

Można także spróbować usunąć wykryte pliki lub poddać je kwarantannie, aby sprawdzić, jak funkcja skanowania radzi sobie z potencjalnymi zagrożeniami. Szczegółowe informacje znajdziesz w rozdziale *Jak działa system wykrywania zagrożeń* na stronie 34.

Korzystanie z programu McAfee SecurityCenter

Program McAfee SecurityCenter pełni rolę centrum zabezpieczeń i jest dostępny za pomocą ikony znajdującej się na pasku zadań lub z pulpitu systemu Windows. Dzięki niemu możliwe jest wykonywanie następujących zadań:

- Uzyskanie darmowej analizy zabezpieczeń komputera.
- Uruchamianie, zarządzanie i konfigurowanie za pomocą jednej ikony wszystkich subskrypcji produktów firmy McAfee.
- Przeglądanie stale aktualizowanych alertów o wirusach oraz najnowszych informacji o produkcie.
- Szybki dostęp do łączy do często zadawanych pytań oraz szczegółowych informacji o koncie w witrynie sieci Web firmy McAfee.

> **UWAGA**
> Aby uzyskać więcej informacji na temat funkcji tego programu, należy kliknąć przycisk **Pomoc** w oknie dialogowym **SecurityCenter**.

Jeśli włączono wszystkie zainstalowane aplikacje firmy McAfee, po uruchomieniu programu SecurityCenter na pasku zadań systemu Windows zostanie wyświetlona czerwona ikona z literą M  . Jest to obszar zawierający zegar, znajdujący się zazwyczaj w prawym dolnym rogu pulpitu systemu Windows.

Jeśli chociaż jedna z zainstalowanych na komputerze aplikacji firmy McAfee zostanie wyłączona, ikona programu McAfee zmieni kolor na czarny  .

Aby otworzyć okno programu McAfee SecurityCenter:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee  .
2. Kliknij polecenie **Otwórz program SecurityCenter**.

Aby uzyskać dostęp do funkcji programu VirusScan:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee  .
2. Wskaż polecenie **VirusScan**, a następnie kliknij nazwę funkcji, której chcesz użyć.

Korzystanie z programu McAfee VirusScan 2

Korzystanie z programu ActiveShield

Po uruchomieniu (załadowaniu do pamięci komputera) i włączeniu program ActiveShield zapewnia ciągłą ochronę komputera. Skanuje on pliki w momencie, gdy użytkownik lub system próbuje uzyskać do nich dostęp. Kiedy program ActiveShield wykryje podejrzany plik, automatycznie podejmuje próbę jego wyczyszczenia. Jeśli program ActiveShield nie jest w stanie usunąć wirusa, zainfekowany plik można poddać kwarantannie lub usunąć.

Włączanie i wyłączanie programu ActiveShield

Program ActiveShield jest domyślnie włączony (o czym informuje czerwony kolor ikony na pasku zadań systemu Windows). Jest on uruchamiany (ładowany do pamięci komputera), gdy zakończona zostanie instalacja, a komputer uruchomi się ponownie.

Jeśli program ActiveShield zostanie zatrzymany (nie załaduje się) lub wyłączony (o czym informuje czarny kolor ikony), można go uruchomić ręcznie i skonfigurować w taki sposób, aby samoczynnie rozpoczynał działanie zaraz po uruchomieniu systemu Windows.

Włączanie programu ActiveShield

Aby włączyć program ActiveShield tylko na czas trwania danej sesji systemu Windows:

Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Włącz**. Kolor ikony programu McAfee zmieni się na czerwony .

Jeśli program ActiveShield jest skonfigurowany tak, aby samoczynnie rozpoczynał działanie po uruchomieniu systemu Windows, zostanie wyświetlony komunikat informujący o uaktywnieniu ochrony komputera przed zagrożeniami. W przeciwnym wypadku pojawi się okno dialogowe umożliwiające skonfigurowanie programu ActiveShield w taki sposób, aby rozpoczynał działanie automatycznie zaraz po uruchomieniu systemu Windows (Ilustracja 2-1 na stronie 14).

Wyłączanie programu ActiveShield

Aby wyłączyć program ActiveShield tylko na czas trwania danej sesji systemu Windows:

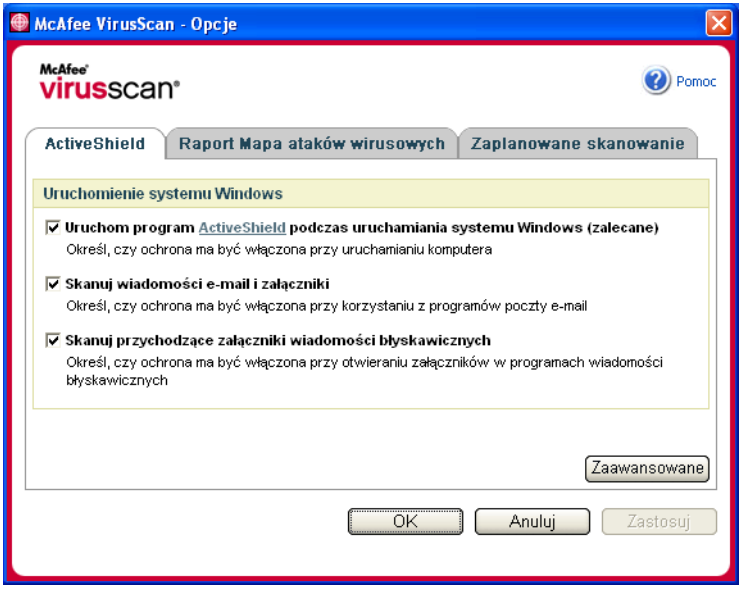
1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Wyłącz**.
2. Kliknij przycisk **Tak**, aby potwierdzić ustawienie.

   Kolor ikony programu McAfee zmieni się na czarny .

Jeśli program ActiveShield jest skonfigurowany tak, aby samoczynnie rozpoczynał działanie po uruchomieniu systemu Windows, uaktywni się automatycznie po ponownym uruchomieniu komputera.

Konfigurowanie opcji programu ActiveShield

Opcje programu ActiveShield dotyczące uruchamiania i skanowania można modyfikować z poziomu karty **ActiveShield** dostępnej w oknie dialogowym **Opcje programu VirusScan** (Ilustracja 2-1). Okno to można otworzyć za pomocą ikony programu McAfee wyświetlanej na pasku zadań systemu Windows.



Ilustracja 2-1. Opcje programu ActiveShield

Uruchamianie programu ActiveShield

Program ActiveShield jest domyślnie włączony (o czym informuje czerwony kolor ikony ). Jest on uruchamiany (ładowany do pamięci komputera), gdy zakończona zostanie instalacja, a komputer uruchomi się ponownie.

Jeśli program ActiveShield zostanie zatrzymany (o czym informuje czarny kolor ikony ), można skonfigurować go tak, aby samoczynnie rozpoczynał działanie zaraz po uruchomieniu systemu Windows (zalecane).

> **UWAGA**
> W trakcie aktualizowania programu VirusScan **Kreator aktualizacji** może tymczasowo wyłączyć program ActiveShield, aby zainstalować nowe pliki. Kiedy **Kreator aktualizacji** wyświetli monit o kliknięcie przycisku **Zakończ**, program ActiveShield zostanie uruchomiony ponownie.

Aby program ActiveShield rozpoczynał działanie automatycznie po uruchomieniu systemu Windows:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Opcje**.

   Zostanie otwarte okno dialogowe **Opcje programu VirusScan** (Ilustracja 2-1 na stronie 14).

2. Zaznacz pole wyboru **Uruchom program ActiveShield podczas uruchamiania systemu Windows (zalecane)** i kliknij przycisk **Zastosuj**, aby zapisać zmiany.

3. Kliknij przycisk **OK**, aby potwierdzić ustawienia, a następnie jeszcze raz kliknij przycisk **OK**.

Zatrzymywanie programu ActiveShield

> **OSTRZEŻENIE**
> Jeśli program ActiveShield zostanie zatrzymany, komputer nie będzie chroniony przed zagrożeniami. Jeśli wymagane jest zatrzymanie programu ActiveShield w innym celu, niż aktualizacja oprogramowania VirusScan, należy się upewnić, że komputer nie jest połączony z Internetem.

Aby wyłączyć opcję automatycznego uruchamiania programu ActiveShield po uruchomieniu systemu Windows:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Opcje**.

   Zostanie otwarte okno dialogowe **Opcje programu VirusScan** (Ilustracja 2-1 na stronie 14).

2 Usuń zaznaczenie pola wyboru **Uruchom program ActiveShield podczas uruchamiania systemu Windows (zalecane)** i kliknij przycisk **Zastosuj**, aby zapisać zmiany.

3 Kliknij przycisk **OK**, aby potwierdzić ustawienia, a następnie jeszcze raz kliknij przycisk **OK**.

Skanowanie wiadomości e-mail i załączników

Domyślnie funkcja skanowania i automatycznego czyszczenia wiadomości e-mail jest włączona, tzn. zaznaczona jest opcja **Skanuj wiadomości e-mail i załączniki** (Ilustracja 2-1 na stronie 14).

Gdy ta opcja jest zaznaczona, program ActiveShield automatycznie skanuje i czyści wykryte wiadomości e-mail - zarówno przychodzące (POP3), jak i wychodzące (SMTP) - oraz załączniki dla większości klientów poczty elektronicznej, w tym:

- Microsoft Outlook Express w wersji 4.0 lub nowszej,
- Microsoft Outlook w wersji 97 lub nowszej,
- Netscape Messenger w wersji 4.0 lub nowszej,
- Netscape Mail w wersji 6.0 lub nowszej,
- Eudora Light w wersji 3.0 lub nowszej,
- Eudora Pro w wersji 4.0 lub nowszej,
- Eudora w wersji 5.0 lub nowszej,
- Pegasus w wersji 4.0 lub nowszej.

UWAGA

W przypadku następujących programów do obsługi poczty elektronicznej funkcja skanowania wiadomości e-mail nie jest dostępna: klienci oparci na sieci Web, klienci AOL, aplikacje wykorzystujące protokoły IMAP lub POP3 SSL oraz program Lotus Notes. Załączniki takie są jednak skanowane przez program ActiveShield w momencie ich otwierania.

Jeśli opcja **Skanuj wiadomości e-mail i załączniki** zostanie wyłączona, automatycznie wyłączane są także opcje dotyczące funkcji skanowania wiadomości e-mail i programu WormStopper (Ilustracja 2-2 na stronie 18). Wyłączenie opcji skanowania poczty wychodzącej powoduje zdezaktywowanie opcji powiązanych z aplikacją WormStopper.

Aby zmiany wprowadzone w opcjach skanowania wiadomości e-mail zostały uwzględnione, należy ponownie uruchomić klienta poczty e-mail.

Przychodzące wiadomości e-mail

W przypadku wykrycia przychodzącej wiadomości e-mail lub przychodzącego załącznika program ActiveShield podejmie następujące działania:

- Próbuje wyczyścić wykrytą wiadomość e-mail.
- Próbuje poddać kwarantannie lub usunąć wiadomość e-mail, której nie udało się wyczyścić.
- Dołącza do wiadomości przychodzącej plik alertu informujący użytkownika o działaniach podjętych w celu usunięcia potencjalnego zagrożenia.

Wychodzące wiadomości e-mail

W przypadku wykrycia wychodzącej wiadomości e-mail lub wychodzącego załącznika program ActiveShield podejmuje następujące działania:

- Próbuje wyczyścić wykrytą wiadomość e-mail.
- Próbuje poddać kwarantannie lub usunąć wiadomość e-mail, której nie udało się wyczyścić.

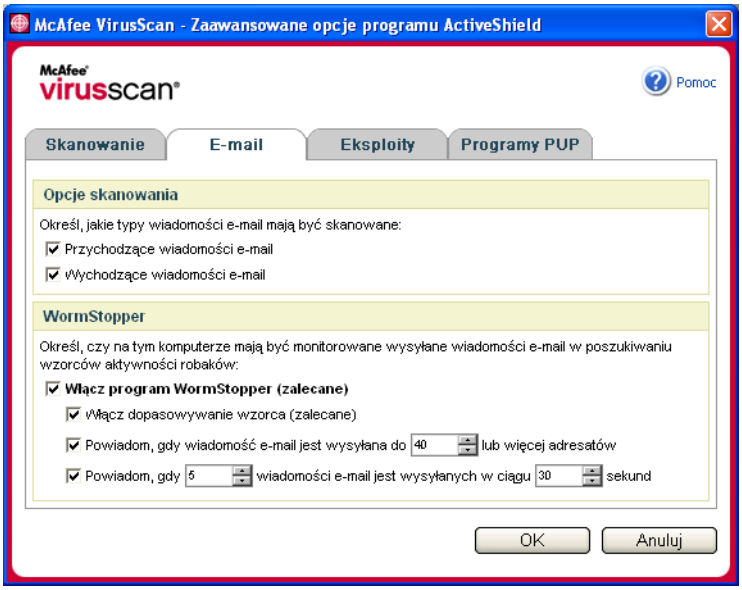
> **UWAGA**
> Szczegółowe informacje o błędach występujących podczas skanowania wychodzących wiadomości e-mail można znaleźć w pomocy w trybie online.

Wyłączanie opcji skanowania wiadomości e-mail

Program ActiveShield domyślnie skanuje przychodzące i wychodzące wiadomości e-mail. Istnieje jednak możliwość skonfigurowania go w taki sposób, aby skanował tylko wiadomości wychodzące lub tylko wiadomości przychodzące.

Aby wyłączyć opcję skanowania wychodzących lub przychodzących wiadomości e-mail:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Opcje**.
2. Kliknij przycisk **Zaawansowane**, a następnie kliknij kartę **Skanowanie wiadomości e-mail** (Ilustracja 2-2).
3. Usuń zaznaczenie pola wyboru **Przychodzące wiadomości e-mail** lub **Wychodzące wiadomości e-mail**, po czym kliknij przycisk **OK**.



Ilustracja 2-2. Zaawansowane opcje programu ActiveShield - karta E-mail

Skanowanie w poszukiwaniu robaków

Program VirusScan monitoruje działanie komputera, wykrywając podejrzaną działalność, która może oznaczać, że komputer jest zagrożony. Jego zadaniem jest oczyszczenie systemu z wirusów i innych zagrożeń. Zadaniem programu WormStopper™ jest uniemożliwienie dalszego rozprzestrzeniania się wirusów i robaków.

„Robak" to samopowielający się wirus, który ładuje się do aktywnej pamięci komputera i rozsyła swoje kopie za pomocą poczty e-mail. Jeśli komputer nie jest chroniony przez program WormStopper, obecność robaka można stwierdzić tylko wtedy, gdy jego niekontrolowane powielanie się zużywa znaczną część zasobów systemowych, spowalniając pracę lub wstrzymując wykonywane przez komputer zadania.

Mechanizm ochronny WormStopper wykrywa i blokuje podejrzaną działalność i informuje o niej użytkownika. Przejawami podejrzanej działalności mogą być następujące operacje:

- Próba wysłania wiadomości e-mail do dużej liczby odbiorców, których adresy znajdują się w książce adresowej.
- Następujące krótko po sobie próby przesłania dalej wielu wiadomości e-mail.

Jeśli dla programu ActiveShield uaktywniono domyślną opcję **Włącz program WormStopper (zalecane)** dostępną w oknie dialogowym **Opcje zaawansowane**, aplikacja WormStopper monitoruje działanie klienta poczty e-mail w poszukiwaniu podejrzanych wzorców i alarmuje użytkownika, gdy w określonym przedziale czasowym zostanie przekroczona ustalona liczba wiadomości e-mail lub odbiorców.

Aby program ActiveShield skanował wysyłane wiadomości e-mail w poszukiwaniu działalności robaków:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Opcje**.
2. Kliknij przycisk **Zaawansowane**, a następnie kliknij kartę **E-mail**.
3. Kliknij opcję **Włącz program WormStopper (zalecane)** (Ilustracja 2-3).

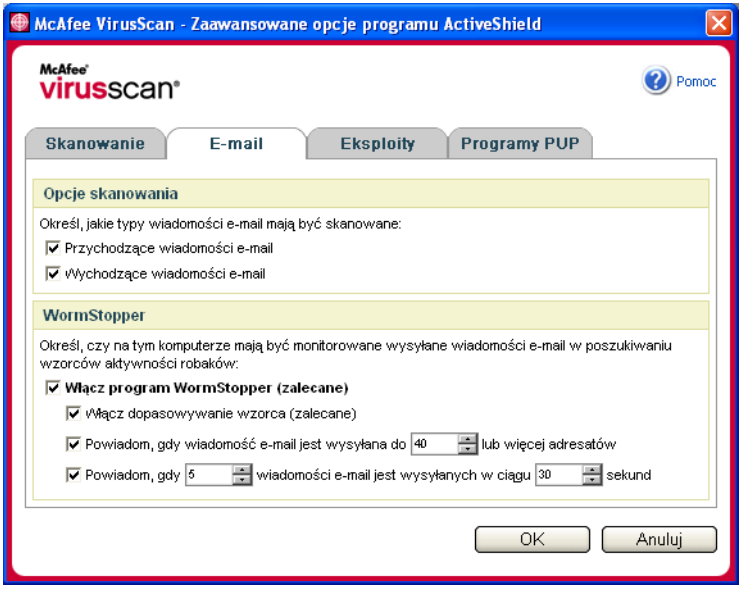
   Domyślnie włączone są następujące opcje:

   - dopasowywanie wzorca w celu wykrycia podejrzanej działalności;
   - powiadamianie, gdy wiadomość e-mail jest wysyłana do co najmniej 40 adresatów;
   - powiadamianie, gdy co najmniej 5 wiadomości e-mail jest wysyłanych w ciągu 30 sekund.

     UWAGA
     Zmiana wartości określającej liczbę adresatów lub sekund używanej przy monitorowaniu wysyłanych wiadomości e-mail może spowodować błędy w wykrywaniu zagrożeń. Firma McAfee zaleca kliknięcie przycisku **Nie** w celu zachowania ustawienia domyślnego. Aby zastąpić wartości domyślne własnymi, kliknij przycisk **Tak**.

Następująca opcja może zostać automatycznie włączona po pierwszym wykryciu potencjalnego robaka (szczegółowe informacje można znaleźć w rozdziale *Zarządzanie potencjalnymi robakami* na stronie 26):

- Automatyczne blokowanie podejrzanych wychodzących wiadomości e-mail



Ilustracja 2-3. Zaawansowane opcje programu ActiveShield - karta E-mail

Skanowanie przychodzących załączników wiadomości błyskawicznych

Domyślnie skanowanie załączników przychodzących z wiadomościami błyskawicznymi jest włączone, tzn. zaznaczona jest opcja **Skanuj przychodzące załączniki wiadomości błyskawicznych** (Ilustracja 2-1 na stronie 14).

Gdy ta opcja jest zaznaczona, program VirusScan automatycznie skanuje i czyści wykryte załączniki przychodzące z wiadomościami błyskawicznymi dla większości programów wiadomości błyskawicznych, w tym:

- MSN Messenger w wersji 6.0 lub nowszej,
- Yahoo Messenger w wersji 4.1 lub nowszej,
- AOL Instant Messenger w wersji 2.1 lub nowszej.

UWAGA
Ze względów bezpieczeństwa nie można wyłączyć opcji automatycznego czyszczenia załączników przychodzących z wiadomościami błyskawicznymi.

W przypadku wykrycia załącznika przychodzącej wiadomości błyskawicznej program VirusScan podejmie następujące działania:

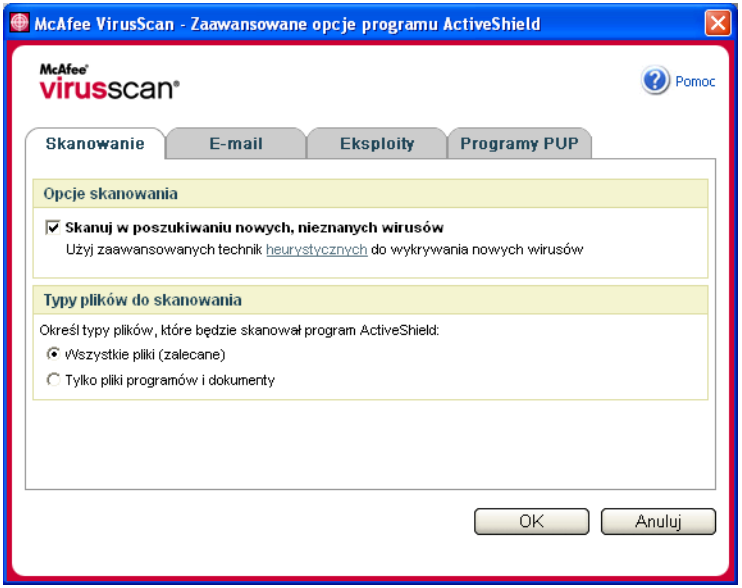
- Spróbuje wyczyścić wykrytą wiadomość.
- Wyświetli monit o poddanie kwarantannie lub usunięcie wiadomości, której nie udało się wyczyścić.

Skanowanie wszystkich plików

Jeśli dla programu ActiveShield zostanie włączona domyślna opcja **Wszystkie pliki (zalecane)**, skanowane będą wszystkie typy plików używane przez komputer. Pliki będą skanowane przy próbie użycia ich przez komputer. Opcji tej należy użyć, jeśli komputer ma być skanowany możliwie jak najdokładniej.

Aby włączyć w programie ActiveShield skanowanie wszystkich typów plików:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Opcje**.
2. Kliknij przycisk **Zaawansowane**, a następnie kliknij kartę **Skanowanie** (Ilustracja 2-4 na stronie 21).
3. Kliknij opcję **Wszystkie pliki (zalecane)**, a następnie kliknij przycisk **OK**.



Ilustracja 2-4. Zaawansowane opcje programu ActiveShield - karta Skanowanie

Skanowanie jedynie plików programów i dokumentów

W przypadku włączenia dla programu ActiveShield opcji **Tylko pliki programów i dokumenty** skanowane są wyłącznie pliki programów i dokumenty. Pozostałe pliki są pomijane. Najnowszy plik sygnatur wirusów (plik DAT) określa typy plików skanowane przez program ActiveShield. Aby wybrać dla programu ActiveShield opcję skanowania wyłącznie plików programów i dokumentów:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Opcje**.
2. Kliknij przycisk **Zaawansowane**, a następnie kliknij kartę **Skanowanie** (Ilustracja 2-4).
3. Kliknij opcję **Tylko pliki programów i dokumenty**, a następnie kliknij przycisk **OK**.

Skanowanie w poszukiwaniu nowych, nieznanych wirusów

Jeśli dla programu ActiveShield jest włączona domyślna opcja **Skanuj w poszukiwaniu nowych, nieznanych wirusów (zalecane)**, wykorzystuje on zaawansowane techniki heurystyczne porównujące pliki z sygnaturami znanych wirusów i wyszukujące dowodów obecności niezidentyfikowanych wirusów w plikach.

Aby wybrać dla programu ActiveShield opcję skanowania w poszukiwaniu nowych, nieznanych wirusów:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Opcje**.
2. Kliknij przycisk **Zaawansowane**, a następnie kliknij kartę **Skanowanie** (Ilustracja 2-4).
3. Kliknij opcję **Skanuj w poszukiwaniu nowych, nieznanych wirusów (zalecane)**, a następnie kliknij przycisk **OK**.

Skanowanie w poszukiwaniu skryptów

Program VirusScan monitoruje działanie komputera, wykrywając podejrzaną działalność, która może oznaczać, że komputer jest zagrożony. Jego zadaniem jest oczyszczenie systemu z wirusów i innych zagrożeń. Zadaniem programu ScriptStopperTM jest uniemożliwienie koniom trojańskim uruchamiania skryptów tworzących nowe kopie wirusa.

„Koń trojański” to podejrzany program udający nieszkodliwą aplikację. Nie jest on wirusem, ponieważ nie potrafi tworzyć własnych kopii, ale stanowi równie poważne zagrożenie.

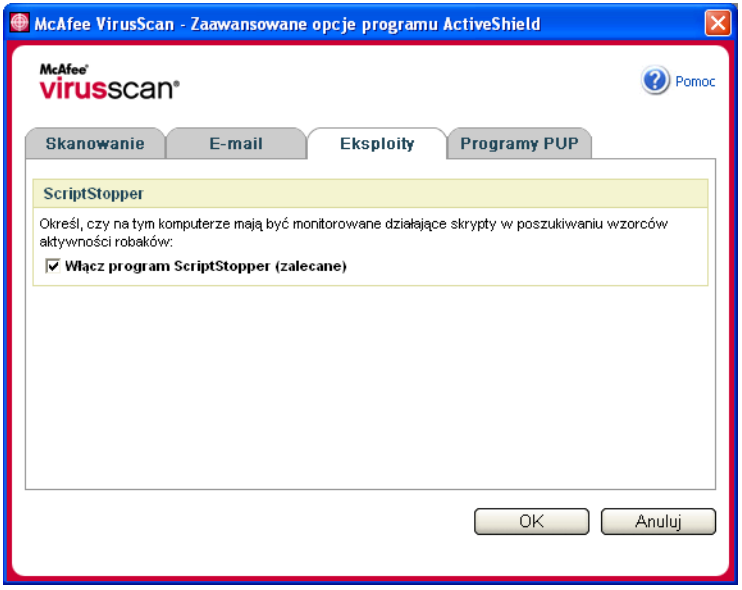
Mechanizm ochronny ScriptStopper wykrywa i blokuje podejrzaną działalność i informuje o niej użytkownika. Przejawem podejrzanej działalności może być następująca operacja:

- Wykonanie skryptu prowadzące do utworzenia, skopiowania lub usunięcia plików albo otwarcia rejestru systemu Windows.

Jeśli dla programu ActiveShield uaktywniono domyślną opcję **Włącz program ScriptStopper (zalecane)** dostępną w oknie dialogowym **Opcje zaawansowane**, aplikacja ScriptStopper śledzi wykonywanie skryptów w poszukiwaniu podejrzanych wzorców i alarmuje użytkownika, gdy w określonym przedziale czasowym zostanie przekroczona ustalona liczba wiadomości e-mail lub odbiorców.

Aby program ActiveShield skanował uruchamiane skrypty w poszukiwaniu działalności robaków:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Opcje**.
2. Kliknij przycisk **Zaawansowane**, a następnie kliknij kartę **Eksploity** (Ilustracja 2-5).
3. Kliknij opcję **Włącz program ScriptStopper (zalecane)**, a następnie kliknij przycisk **OK**.



Ilustracja 2-5. Zaawansowane opcje programu ActiveShield - karta Eksploity

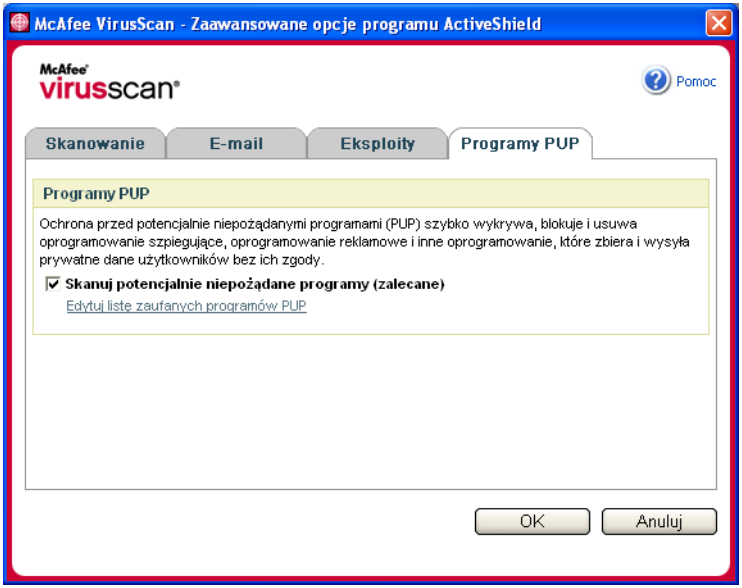
Skanowanie w poszukiwaniu potencjalnie niepożądanych programów (PUP)

UWAGA
Program McAfee AntiSpyware kontroluje wszystkie działania potencjalnie niepożądanych programów na komputerze, na którym go zainstalowano. Uruchom program McAfee AntiSpyware i skonfiguruj jego opcje.

Jeśli dla programu ActiveShield uaktywniono domyślną opcję **Skanuj potencjalnie niepożądane programy (zalecane)** dostępną w oknie dialogowym **Opcje zaawansowane**, mechanizm ochrony przed programami PUP szybko wykrywa, blokuje i usuwa oprogramowanie szpiegujące i reklamowe, a także inne aplikacje, które gromadzą i wysyłają prywatne dane użytkowników bez ich zgody.

Aby program ActiveShield skanował komputer w poszukiwaniu programów PUP:

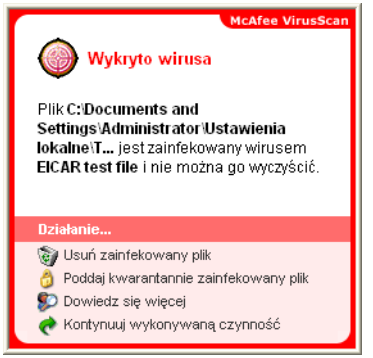
1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Opcje**.
2. Kliknij przycisk **Zaawansowane**, a następnie kliknij kartę **Programy PUP** (Ilustracja 2-6).
3. Kliknij opcję **Skanuj potencjalnie niepożądane programy (zalecane)**, a następnie kliknij przycisk **OK**.



Ilustracja 2-6. Zaawansowane opcje programu ActiveShield - karta Programy PUP

Jak działa system generowania alertów zabezpieczeń

Jeśli program ActiveShield znajdzie wirusa, wyświetlany jest alert o wirusie podobny do przedstawionego tutaj: Ilustracja 2-7. Jeśli wykryte zostanie zagrożenie, program ActiveShield podejmie automatycznie próbę wyczyszczenia pliku i wyświetli alert. Dzieje się tak w przypadku większości wirusów, koni trojańskich i robaków. W przypadku potencjalnie niepożądanych programów (PUP) program ActiveShield wykrywa plik, po czym automatycznie go blokuje i wyświetla alert.



Ilustracja 2-7. Alert o wirusie

Użytkownik może zdefiniować działania podejmowane przez program po wykryciu plików, wiadomości e-mail lub podejrzanych skryptów, a także potencjalnych robaków i programów PUP. Możliwe jest także włączenie lub wyłączenie opcji przesyłania pliku do zespołu AVERT firmy McAfee.

Po wykryciu przez program ActiveShield podejrzanego pliku ze względów bezpieczeństwa wyświetlany jest monit o niezwłoczne przeskanowanie całego systemu. Jeśli nie zostanie wybrana opcja ukrycia tego monitu, co jakiś czas będą wyświetlane przypomnienia - do momentu przeskanowania systemu.

Zarządzanie wykrytymi plikami

1. Jeśli program ActiveShield jest w stanie wyczyścić plik, można zignorować alert lub zażądać dodatkowych informacji:
   - Kliknij opcję **Dowiedz się więcej**, aby poznać nazwę i lokalizację wykrytego pliku oraz nazwę wirusa.
   - Kliknij opcję **Kontynuuj wykonywaną czynność**, aby zignorować alert i zamknąć jego okno.
2. Jeśli program ActiveShield nie jest w stanie wyczyścić pliku, kliknij opcję **Poddaj kwarantannie wykryty plik**, aby zaszyfrować i tymczasowo odizolować podejrzane pliki w folderze kwarantanny do momentu, gdy będzie można podjąć odpowiednie działanie.

Zostanie wyświetlony komunikat potwierdzenia i monit o sprawdzenie komputera pod kątem występowania zagrożeń bezpieczeństwa. Kliknij przycisk **Skanuj**, aby zakończyć proces poddawania plików kwarantannie.

3 Jeśli program ActiveShield nie jest w stanie poddać pliku kwarantannie, kliknij opcję **Usuń wykryty plik**, aby spróbować usunąć plik.

Zarządzanie wykrytymi wiadomościami e-mail

Domyślnym działaniem skanowania wiadomości e-mail jest próba automatycznego wyczyszczenia wykrytych wiadomości e-mail. Do wiadomości przychodzących dołączany jest plik alertu informujący użytkownika, czy dana wiadomość została wyczyszczona, poddana kwarantannie czy też usunięta.

Zarządzanie podejrzanymi skryptami

Jeśli program ActiveShield wykryje podejrzany skrypt, użytkownik może uzyskać dodatkowe informacje o tym skrypcie, a także zatrzymać jego wykonanie zainicjowane wbrew swojej woli:

- Kliknij opcję **Dowiedz się więcej**, aby poznać nazwę, lokalizację i opis działania związanego z podejrzanym skryptem.
- Kliknij opcję **Zatrzymaj ten skrypt,** aby zapobiec wykonaniu podejrzanego skryptu.

Jeśli masz pewność, że skrypt pochodzi z zaufanego źródła, możesz zezwolić na jego uruchomienie:

- Kliknij opcję **Zezwól tym razem na wykonanie tego skryptu,** aby pozwolić na jednorazowe uruchomienie wszystkich skryptów zawartych w jednym pliku.
- Kliknij opcję **Kontynuuj wykonywaną czynność**, aby zignorować alert i zezwolić na wykonanie skryptu.

Zarządzanie potencjalnymi robakami

Jeśli program ActiveShield wykryje potencjalnego robaka, użytkownik może uzyskać dodatkowe informacje o podejrzanej wiadomości i przerwać zainicjowane wbrew swojej woli działanie klienta poczty e-mail:

- Kliknij opcję **Dowiedz się więcej**, aby poznać listę odbiorców, temat i treść wiadomości oraz opis podejrzanych działań związanych z wykrytą wiadomością e-mail.
- Kliknij opcję **Zatrzymaj tę wiadomość e-mail,** aby zapobiec wysłaniu podejrzanej wiadomości i usunąć ją z kolejki.

Jeśli masz pewność, że działania podjęte przez klienta poczty e-mail są bezpieczne, kliknij opcję **Kontynuuj wykonywaną czynność**, aby zignorować alert i zezwolić na wysłanie wiadomości.

Zarządzanie programami PUP

Jeśli aplikacja ActiveShield wykryje i zablokuje potencjalnie niepożądany program (PUP), użytkownik może uzyskać dodatkowe informacje o tym programie i usunąć go, jeśli nie ma zamiaru go instalować:

- Kliknij opcję **Dowiedz się więcej**, aby poznać nazwę i lokalizację programu PUP oraz zalecane działanie.
- Kliknij opcję **Usuń ten program PUP**, aby usunąć program, jeśli nie chcesz go instalować.

  Zostanie wyświetlony komunikat potwierdzenia.

  - Jeżeli (a) nie rozpoznajesz programu PUP lub (b) dany program PUP nie został zainstalowany w ramach większego pakietu ani nie zaakceptowano jego umowy licencyjnej, kliknij przycisk **OK**, aby usunąć ten program za pomocą oprogramowania firmy McAfee.

  - W przeciwnym wypadku kliknij przycisk **Anuluj**, aby przerwać proces automatycznego usuwania. Program można będzie usunąć później, korzystając z dezinstalatora producenta.
- Kliknij opcję **Kontynuuj wykonywaną czynność**, aby zignorować alert i tymczasowo zablokować program.

- Jeżeli (a) rozpoznajesz program PUP lub (b) dany program PUP mógł zostać zainstalowany w ramach większego pakietu albo mogła zostać zaakceptowana jego umowa licencyjna, można zezwolić na uruchamianie tego programu.

- Kliknij opcję **Ufaj temu programowi PUP**, aby dodać program do białej listy i zawsze zezwalać na jego uruchamianie.

  Szczegółowe informacje znajdziesz w rozdziale *Zarządzanie zaufanymi programami PUP*.

Zarządzanie zaufanymi programami PUP

Programy dodane do listy Zaufane programy PUP nie są wykrywane przez program McAfee VirusScan.

W razie potrzeby żądany program PUP można z tej listy usunąć.

Jeśli lista Zaufane programy PUP jest pełna, nie można do niej dodać kolejnej pozycji, o ile wcześniej nie zostanie zwolniona część miejsca na liście.

Aby usunąć program z listy zaufanych programów PUP:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Opcje**.
2. Kliknij przycisk **Zaawansowane**, a następnie kliknij kartę **Programy PUP**.
3. Kliknij łącze **Edytuj listę zaufanych programów PUP**, zaznacz pole wyboru przed wybraną nazwą pliku, a następnie kliknij przycisk **Usuń**. Po zakończeniu usuwania pozycji z listy kliknij przycisk **OK**.

Ręczne skanowanie komputera

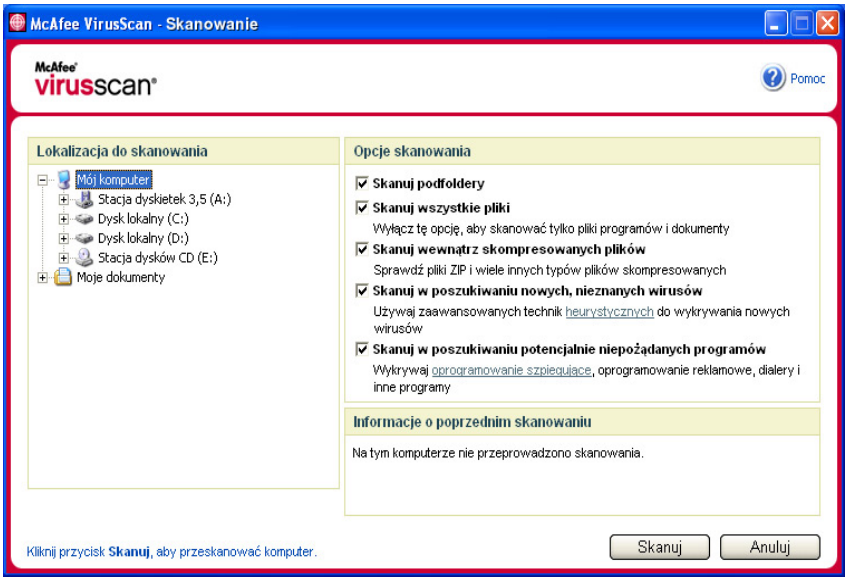
Funkcja skanowania pozwala przeskanować wybrane dyski twarde, dyskietki oraz pojedyncze pliki i foldery w poszukiwaniu wirusów i innych zagrożeń. Jeżeli w trakcie skanowania zostanie wykryty podejrzany plik, program automatycznie spróbuje go wyczyścić, o ile plik ten nie jest potencjalnie niepożądanym programem. Jeśli funkcja skanowania nie jest w stanie wyczyścić pliku, można go poddać kwarantannie lub usunąć.

Ręczne skanowanie w poszukiwaniu wirusów i innych zagrożeń

Aby przeskanować komputer:

1 Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Skanuj**.

Zostanie wyświetlone okno dialogowe **Skanowanie** (Ilustracja 2-8).



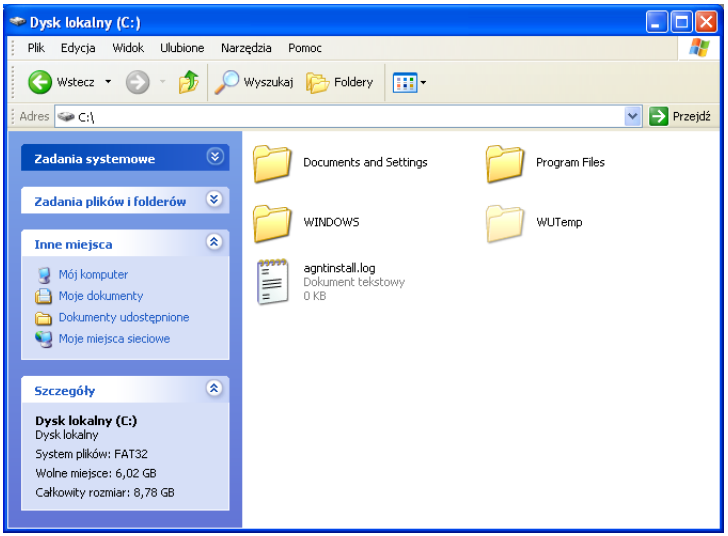
Ilustracja 2-8. Okno dialogowe Skanowanie

2 Kliknij dysk, folder lub plik, który chcesz przeskanować.

3 Wybierz **Opcje skanowania**. Standardowo zaznaczone są wszystkie ustawienia domyślne dostępne w obszarze **Opcje skanowania**, co zapewnia największą możliwą dokładność skanowania (Ilustracja 2-8).

- **Skanuj podfoldery** - użyj tej opcji, aby skanować pliki zawarte w podfolderach. Usuń zaznaczenie tego pola wyboru, aby zezwolić na skanowanie jedynie plików widocznych po otwarciu folderu lub dysku.

Przykład: Jeśli usuniesz zaznaczenie pola wyboru **Skanuj podfoldery**, zostaną przeskanowane wyłącznie pliki widoczne tutaj: Ilustracja 2-9. Foldery i ich zawartość nie zostaną przeskanowane. Aby je przeskanować, musisz pozostawić zaznaczenie tego pola wyboru.



Ilustracja 2-9. Zawartość lokalnego dysku

- **Skanuj wszystkie pliki** - opcja pozwala dokładnie przeskanować pliki wszystkich typów. Usuń zaznaczenie tego pola wyboru, aby skrócić czas skanowania (skanowane będą jedynie pliki programów i dokumenty).

- **Skanuj wewnątrz skompresowanych plików** - użyj tej opcji ustawienia, aby wykryć zainfekowane pliki ukryte w plikach ZIP i innych skompresowanych plikach. Usuń zaznaczenie tego pola wyboru, aby wyłączyć sprawdzanie plików lub archiwów zapisanych wewnątrz skompresowanego pliku.

  Zdarza się, że autorzy wirusów umieszczają je w plikach .ZIP, które z kolei są dodawane do innych zbiorów .ZIP w celu oszukania skanerów antywirusowych. Zaznaczenie opisywanej opcji umożliwia funkcji skanowania wykrywanie takich wirusów.

- **Skanuj w poszukiwaniu nowych, nieznanych wirusów (zalecane)** - użyj tej opcji, jeśli chcesz, aby wykrywane były najnowsze wirusy, dla których mogą jeszcze nie istnieć metody ich usuwania. Wykorzystuje ona zaawansowane techniki heurystyczne porównujące pliki z sygnaturami znanych wirusów i wyszukujące dowodów obecności niezidentyfikowanych wirusów w plikach.

  Wyszukiwane są też cechy plików pozwalające zwykle wykluczyć obecność wirusa. Minimalizuje to szanse zaklasyfikowania przez funkcję skanowania niezainfekowanego pliku jako wirusa. Niemniej jednak pliki, które zostały uznane przez skanowanie heurystyczne za potencjalne wirusy, powinny być traktowane z taką samą ostrożnością, jak inne wykryte wirusy.

Opcja skanowania w poszukiwaniu nowych, nieznanych wirusów zapewnia największą dokładność skanowania, ale wiąże się z wydłużeniem czasu skanowania.

- **Skanuj w poszukiwaniu potencjalnie niepożądanych programów** - użyj tej opcji, jeśli chcesz, aby wykrywane było oprogramowanie szpiegujące i reklamowe oraz inne programy, które gromadzą i wysyłają prywatne dane użytkowników bez ich zgody.

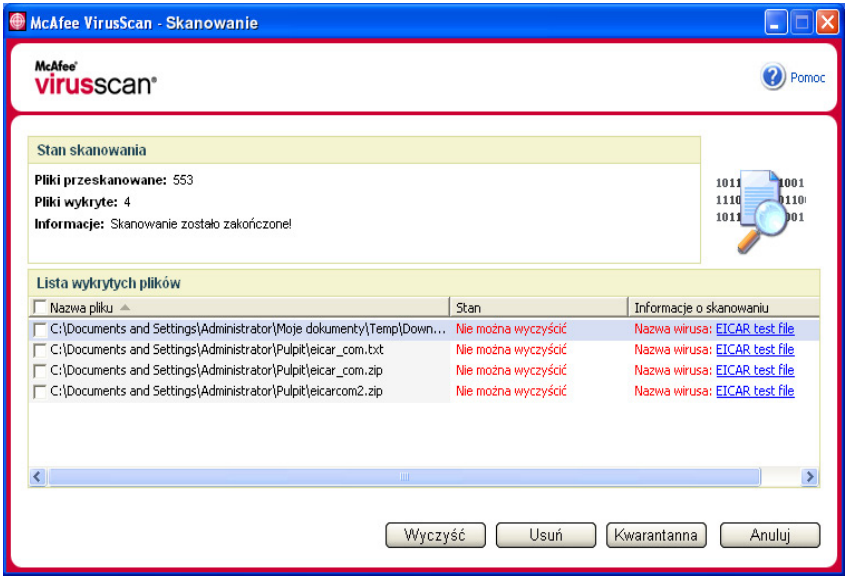
UWAGA

Zalecane jest zaznaczenie wszystkich opcji, aby komputer był skanowany jak najdokładniej. Przy takiej konfiguracji sprawdzany jest każdy plik na wybranym dysku lub w wybranym folderze, w związku z czym do przeprowadzenia skanowania wymagana jest znaczna ilość czasu. Im większy jest dysk twardy i im więcej zawiera plików, tym dłużej trwa skanowanie.

4 Kliknij przycisk **Skanuj,** aby rozpocząć skanowanie plików.

Po zakończeniu skanowania wyświetlane jest podsumowanie przedstawiające liczbę przeskanowanych plików, wykrytych plików, potencjalnie niepożądanych programów i wykrytych plików, które zostały automatycznie wyczyszczone.

5 Kliknij przycisk **OK**, aby zamknąć podsumowanie i obejrzeć listę wykrytych plików w oknie dialogowym **Skanowanie** (Ilustracja 2-10).



Ilustracja 2-10. Wyniki skanowania

UWAGA
Każdy plik skompresowany (tj. zbiór .ZIP, .CAB itp.) uwzględniany w liczbie plików wyświetlanych pod pozycją **Pliki przeskanowane** jest liczony jako jeden plik. Ponadto wyświetlana liczba przeskanowanych plików może być inna niż w rzeczywistości, jeśli w okresie, jaki upłynął od ostatniego skanowania, usunięto tymczasowe pliki internetowe.

6 Jeśli w trakcie skanowania nie zostały wykryte żadne wirusy ani inne zagrożenia, kliknij przycisk **Wstecz**, aby wybrać inny dysk lub folder do sprawdzenia lub kliknij przycisk **Zamknij**, aby zamknąć okno dialogowe. W przeciwnym razie zapoznaj się z rozdziałem *Jak działa system wykrywania zagrożeń* na stronie 34.

Skanowanie z poziomu Eksploratora Windows

W programie VirusScan dostępne jest menu podręczne umożliwiające rozpoczęcie skanowania w poszukiwaniu wirusów i innych zagrożeń w wybranych plikach, folderach lub na dyskach bezpośrednio z Eksploratora Windows.

Aby skanować pliki z poziomu Eksploratora Windows:

1 Otwórz Eksploratora Windows.

2 Kliknij prawym przyciskiem myszy dysk, folder lub plik, który ma zostać przeskanowany, a następnie kliknij przycisk **Skanuj**.

Zostanie otwarte okno dialogowe **Skanowanie** i rozpocznie się skanowanie plików. Standardowo zaznaczone są wszystkie ustawienia domyślne dostępne w obszarze **Opcje skanowania**, co zapewnia optymalną dokładność skanowania (Ilustracja 2-8 na stronie 28).

Skanowanie z poziomu programu Microsoft Outlook

Ikona dodawana do paska narzędzi przez program VirusScan pozwala przeskanować z poziomu programu Microsoft Outlook 97 lub nowszego wybrane magazyny wiadomości i ich podfoldery, a także foldery skrzynki pocztowej i wiadomości e-mail zawierające załączniki w poszukiwaniu wirusów i innych zagrożeń.

Aby skanować z poziomu programu Microsoft Outlook:

1 Otwórz program Microsoft Outlook.

2 Kliknij żądany magazyn wiadomości, folder lub wiadomość e-mail z załącznikiem, a następnie kliknij ikonę skanowania wiadomości e-mail na pasku narzędzi  .

Zostanie otwarty skaner wiadomości e-mail i rozpocznie się skanowanie plików. Standardowo zaznaczone są wszystkie ustawienia domyślne dostępne w obszarze **Opcje skanowania**, co zapewnia największą możliwą dokładność skanowania (Ilustracja 2-8 na stronie 28).

Automatyczne skanowanie w poszukiwaniu wirusów i innych zagrożeń

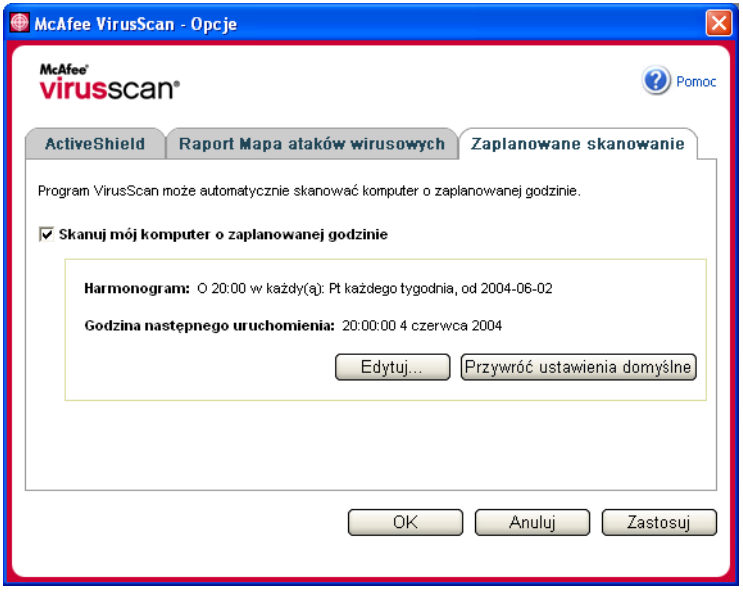
Chociaż program VirusScan skanuje na bieżąco pliki, z których chce skorzystać użytkownik lub komputer, za pomocą usługi Harmonogram zadań systemu Windows można zaplanować skanowanie automatyczne, aby w ustalonych odstępach czasu sprawdzać, czy komputer jest wolny od wirusów i innych zagrożeń.

Aby zaplanować skanowanie:

1 Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Opcje**.

Zostanie otwarte okno dialogowe **Opcje programu VirusScan**.

2 Kliknij kartę **Zaplanowane skanowanie** (Ilustracja 2-11 na stronie 32).



Ilustracja 2-11. Opcje zaplanowanego skanowania

3 Zaznacz pole wyboru **Skanuj mój komputer o zaplanowanej godzinie**, aby włączyć skanowanie automatyczne.

4 Zdefiniuj harmonogram skanowania automatycznego:

- Aby zaakceptować harmonogram domyślny (w każdy piątek o godzinie 20:00), kliknij przycisk **OK**.
- Aby przeprowadzić edycję harmonogramu:

  a. Kliknij przycisk **Edytuj**.

  b. Określ, jak często komputer ma być skanowany, wybierając odpowiednią pozycję z listy **Zaplanuj zadanie**, po czym wybierz dodatkowe opcje w obszarze dynamicznym poniżej:

  Codziennie - określ, co ile dni komputer ma być skanowany.

  Cotygodniowo (domyślnie) - określ, co ile tygodni komputer ma być skanowany oraz wybierz żądane dni tygodnia.

  Comiesięcznie - określ, w którym dniu miesiąca komputer ma być skanowany. Kliknij przycisk **Wybierz miesiące**, aby wskazać miesiące, w których komputer ma być skanowany, a następnie kliknij przycisk **OK**.

  Raz - określ datę skanowania.

  UWAGA
  Następujące opcje usługi Harmonogram zadań systemu Windows nie są obsługiwane:
  Przy uruchamianiu systemu, **W czasie bezczynności** oraz **Pokaż wiele harmonogramów**. Ostatni zgodny harmonogram pozostanie aktywny, dopóki użytkownik nie wybierze dozwolonej opcji.

  c. W polu **Godzina rozpoczęcia** wybierz porę dnia, o której ma się rozpocząć skanowanie komputera.

  d. Aby wybrać zaawansowane opcje, kliknij przycisk **Zaawansowane**.

  Zostanie wyświetlone okno dialogowe **Zaawansowane opcje harmonogramu**.

  i. Podaj datę rozpoczęcia, datę zakończenia, czas trwania i godzinę zakończenia, a także określ, czy zadanie ma zostać zatrzymane o ustalonej godzinie, jeśli nadal będzie trwać skanowanie.

  ii. Kliknij przycisk **OK**, aby zapisać zmiany i zamknąć okno dialogowe. W przeciwnym razie kliknij przycisk **Anuluj**.

5 Kliknij przycisk **OK**, aby zapisać zmiany i zamknąć okno dialogowe. W przeciwnym razie kliknij przycisk **Anuluj**.

6 Aby przywrócić harmonogram domyślny, kliknij przycisk **Przywróć ustawienia domyślne**. W przeciwnym razie kliknij przycisk **OK**.

Jak działa system wykrywania zagrożeń

Funkcja skanowania podejmie automatycznie próbę wyczyszczenia pliku w przypadku większości wirusów, koni trojańskich i robaków. Użytkownik może zdefiniować działania podejmowane przez program po wykryciu zagrożenia oraz włączyć lub wyłączyć opcję przesyłania pliku do zespołu AVERT firmy McAfee. Jeśli funkcja skanowania wykryje potencjalnie niepożądany program, można spróbować wyczyścić, poddać kwarantannie lub usunąć plik ręcznie (nie ma możliwości przesłania pliku do zespołu AVERT).

Postępowanie w przypadku wykrycia wirusa lub potencjalnie niepożądanego programu:

1. Jeśli plik jest wyświetlany w obszarze **Lista wykrytych plików**, zaznacz go, klikając odpowiadające mu pole wyboru.

   UWAGA
   Jeśli na liście figuruje więcej niż jeden plik, wystarczy zaznaczyć pole wyboru przed listą **Nazwa pliku**, aby wybrać wszystkie pliki. Można także kliknąć nazwę pliku na liście **Informacje o skanowaniu**, aby wyświetlić szczegółowe informacje z Biblioteki informacji o wirusach.

2. Jeśli plik jest potencjalnie niepożądanym programem, można kliknąć przycisk **Wyczyść**, aby spróbować go wyczyścić.

3. Jeśli funkcja skanowania nie jest w stanie wyczyścić pliku, możesz kliknąć opcję **Kwarantanna**, aby zaszyfrować i tymczasowo odizolować podejrzane pliki w folderze kwarantanny do momentu, gdy będzie można podjąć odpowiednie działanie. (Szczegółowe informacje znajdziesz w rozdziale *Zarządzanie plikami poddanymi kwarantannie* na stronie 35).

4. Jeśli funkcja skanowania nie jest w stanie wyczyścić pliku ani poddać go kwarantannie, można wykonać jedną z następujących czynności:

   - Kliknij przycisk **Usuń**, aby usunąć plik.
   - Kliknij przycisk **Anuluj**, aby zamknąć okno dialogowe bez wykonywania jakichkolwiek dalszych czynności.

Jeśli funkcja skanowania nie jest w stanie wyczyścić wykrytego pliku ani go usunąć, należy poszukać dodatkowych informacji w Bibliotece informacji o wirusach - pod adresem http://us.mcafee.com/virusInfo/default.asp - aby dowiedzieć się, jak usunąć wirusa ręcznie.

Jeżeli wykryty plik uniemożliwia połączenie się z Internetem lub korzystanie z komputera, spróbuj uruchomić komputer za pomocą dyskietki ratunkowej. Dyskietka ratunkowa pozwala często uruchomić komputer, z którego nie można było normalnie korzystać z powodu infekcji. Szczegółowe informacje znajdziesz w rozdziale *Tworzenie dyskietki ratunkowej* na stronie 36.

Więcej pomocnych informacji można znaleźć w witrynie sieci Web firmy McAfee poświęconej obsłudze klienta pod adresem http://www.mcafeehelp.com/.

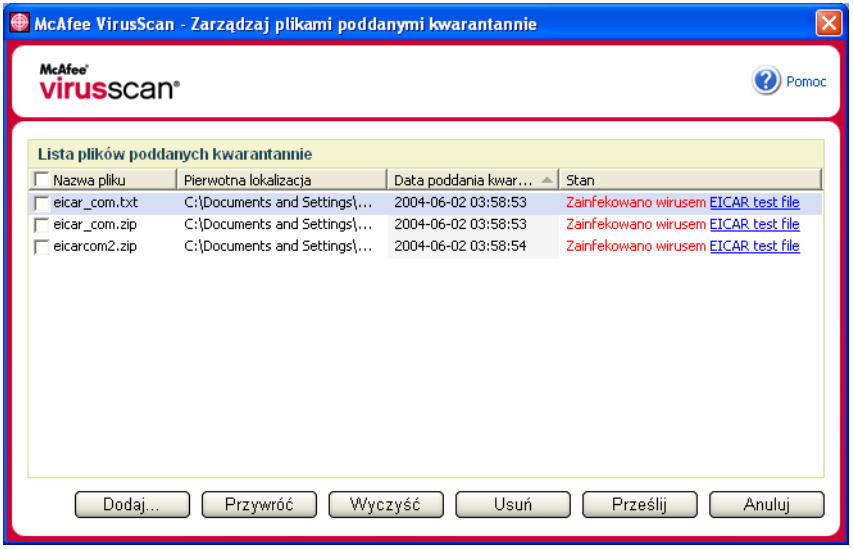
Zarządzanie plikami poddanymi kwarantannie

Funkcja kwarantanny powoduje zaszyfrowanie i tymczasowe odizolowanie podejrzanych plików w folderze kwarantanny do momentu, gdy będzie można podjąć odpowiednie działanie. Po wyczyszczeniu plik poddany kwarantannie może zostać przywrócony do oryginalnej lokalizacji.

Aby zarządzać plikami poddanymi kwarantannie:

1 Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Zarządzaj plikami poddanymi kwarantannie**.

Zostanie wyświetlona lista plików poddanych kwarantannie (Ilustracja 2-12).



Ilustracja 2-12. Okno dialogowe Zarządzaj plikami poddanymi kwarantannie

2 Zaznacz pola wyboru znajdujące się przy nazwach plików, które chcesz wyczyścić.

UWAGA
Jeśli na liście figuruje więcej niż jeden plik, wystarczy zaznaczyć pole wyboru przed listą **Nazwa pliku**, aby wybrać wszystkie pliki. Można także kliknąć nazwę wirusa na liście **Stan**, aby wyświetlić szczegółowe informacje z Biblioteki informacji o wirusach.

Ewentualnie kliknij przycisk **Dodaj**, zaznacz podejrzany plik, który chcesz dodać do listy plików objętych kwarantanną, kliknij przycisk **Otwórz**, a następnie zaznacz plik na liście.

3 Kliknij przycisk **Wyczyść**.

4 Jeśli plik został wyczyszczony, kliknij przycisk **Przywróć**, aby przenieść go z powrotem do oryginalnej lokalizacji.

5 W przypadku, gdy program VirusScan nie jest w stanie wyczyścić pliku z wirusa, kliknij przycisk **Usuń**, aby usunąć plik.

6 Jeżeli program VirusScan nie może wyczyścić ani usunąć pliku, który nie jest potencjalnie niepożądanym programem, plik ten można przesłać do zespołu szybkiego reagowania AVERT™ firmy McAfee, który dokona jego analizy:

   a Zaktualizuj pliki sygnatur wirusów, jeśli są one starsze niż dwa tygodnie.

   b Dokonaj weryfikacji subskrypcji.

   c Wybierz plik i kliknij przycisk **Prześlij**, aby przekazać go zespołowi AVERT.

   Program VirusScan wysyła plik poddany kwarantannie w postaci załącznika do wiadomości e-mail zawierającej adres e-mail użytkownika, nazwę kraju, wersję oprogramowania, informacje o systemie operacyjnym oraz oryginalną nazwę i lokalizację pliku. Maksymalna wielkość wysyłanych danych to jeden plik dziennie o rozmiarze 1,5 MB.

7 Kliknij przycisk **Anuluj**, aby zamknąć okno dialogowe bez wykonywania jakichkolwiek dalszych czynności.

Tworzenie dyskietki ratunkowej

Za pomocą narzędzia Dyskietka ratunkowa można utworzyć własną dyskietkę rozruchową pozwalającą uruchomić i przeskanować komputer, jeśli wirus uniemożliwia normalne uruchomienie systemu.

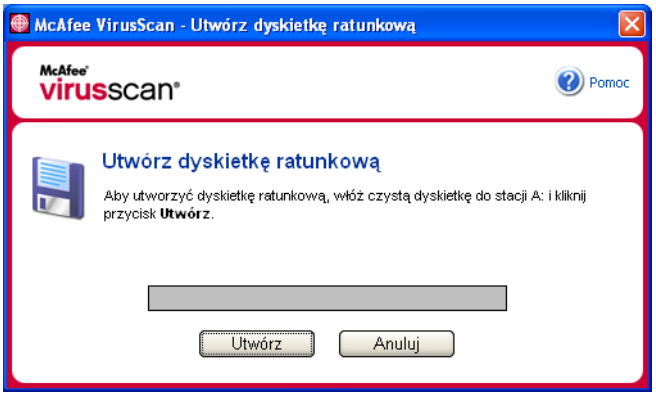
UWAGA
Aby można było pobrać obraz dyskietki ratunkowej, należy połączyć się z Internetem. Obraz ten jest dostępny jedynie w wersji przeznaczonej dla komputerów z partycjami FAT (FAT 16 i FAT 32). Nie jest potrzebny w przypadku partycji NTFS.

Aby utworzyć dyskietkę ratunkową:

1 Na niezainfekowanym komputerze włóż wolną od infekcji dyskietkę do stacji A. Możesz użyć funkcji skanowania, aby upewnić się, że na komputerze i dyskietce nie ma wirusów. (Szczegółowe informacje znajdziesz w rozdziale *Ręczne skanowanie w poszukiwaniu wirusów i innych zagrożeń* na stronie 28).

2 Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Utwórz dyskietkę ratunkową**.

Zostanie wyświetlone okno dialogowe **Utwórz dyskietkę ratunkową** (Ilustracja 2-13).



Ilustracja 2-13. Okno dialogowe Utwórz dyskietkę ratunkową

3 Kliknij przycisk **Utwórz**, aby utworzyć dyskietkę ratunkową.

Jeśli dyskietka ratunkowa tworzona jest po raz pierwszy, wyświetlany jest komunikat informujący o konieczności pobrania pliku obrazu dla dyskietki ratunkowej. Kliknij przycisk **OK**, aby pobrać ten składnik. Jeśli plik obrazu ma zostać pobrany później, kliknij przycisk **Anuluj**.

Wyświetlony zostanie komunikat ostrzegawczy z informacją, że zawartość dyskietki zostanie utracona.

4 Kliknij przycisk **Tak**, aby kontynuować tworzenie dyskietki ratunkowej.

W oknie dialogowym **Utwórz dyskietkę ratunkową** wyświetlany jest stan tworzenia dyskietki ratunkowej.

5 Po wyświetleniu komunikatu „Dyskietka ratunkowa została utworzona pomyślnie” kliknij przycisk **OK**, a następnie zamknij okno dialogowe **Utwórz dyskietkę ratunkową**.

6 Wyjmij dyskietkę ratunkową ze stacji dysków, zabezpiecz ją przed zapisem i umieść w bezpiecznym miejscu.

Zabezpieczanie dyskietki ratunkowej przed zapisem

Aby zabezpieczyć dyskietkę ratunkową przed zapisem:

1 Odwróć dyskietkę etykietą w dół (u góry powinno znaleźć się metalowe kółko).

2 Odszukaj plastikowy uchwyt blokady zapisu. Przesuń go tak, aby odsłonić otwór.

Korzystanie z dyskietki ratunkowej

Aby skorzystać z dyskietki ratunkowej:

1. Wyłącz zainfekowany komputer.
2. Włóż dyskietkę ratunkową do stacji dyskietek.
3. Włącz komputer.

   Pojawi się szare okno, a w nim kilka opcji.
4. Wybierz najbardziej odpowiadającą opcję, naciskając klawisz funkcyjny (np. F2, F3).

UWAGA
Jeśli w ciągu 60 sekund nie zostanie naciśnięty żaden klawisz funkcyjny, dyskietka ratunkowa zostanie uruchomiona automatycznie.

Aktualizacja dyskietki ratunkowej

Dyskietkę ratunkową powinno się aktualizować w regularnych odstępach czasu. Procedura aktualizacji tej dyskietki jest identyczna jak w przypadku tworzenia nowej dyskietki ratunkowej.

Automatyczne przesyłanie informacji o wirusach

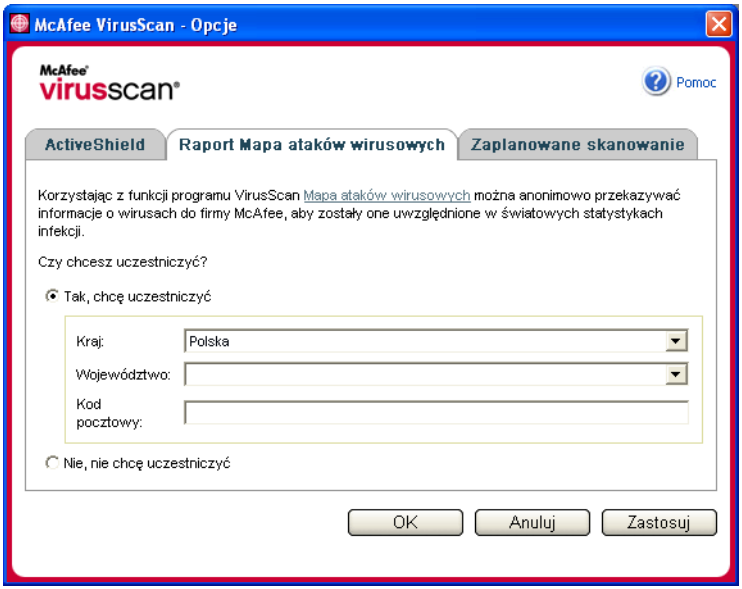
Istnieje możliwość anonimowego przekazywania do naszej mapy ataków wirusowych na świecie informacji pozwalających śledzić wirusy. Tę bezpłatną i całkowicie bezpieczną usługę można zarejestrować automatycznie podczas instalacji programu VirusScan (w oknie dialogowym **Tworzenie raportu o mapie ataków wirusowych**) albo ręcznie - korzystając z karty **Tworzenie raportu o mapie ataków wirusowych** w oknie dialogowym **Opcje programu VirusScan**.

Przesyłanie raportu do mapy ataków wirusowych na świecie

Aby automatycznie przesyłać informacje o wirusach do mapy ataków wirusowych na świecie:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Opcje**.

   Zostanie otwarte okno dialogowe **Opcje programu VirusScan**.
2. Kliknij kartę **Tworzenie raportu o mapie ataków wirusowych** (Ilustracja 2-14).



Ilustracja 2-14. Opcje tworzenia raportu o mapie ataków wirusowych

3 Zaakceptuj ustawienie domyślne **Tak, chcę uczestniczyć**, jeśli chcesz, aby do firmy McAfee były anonimowo przesyłane informacje o wirusach, które będą uwzględniane w światowych statystykach wykrywanych zagrożeń. W przeciwnym wypadku zaznacz opcję **Nie, nie chcę uczestniczyć**. Z komputera nie będą wówczas wysyłane powyższe informacje.

4 Jeśli przebywasz w Stanach Zjednoczonych, wybierz stan, w którym znajduje się komputer i wprowadź odpowiedni kod pocztowy. W przeciwnym razie program VirusScan automatycznie próbuje wybrać kraj, w którym znajduje się komputer.

5 Kliknij przycisk **OK**.

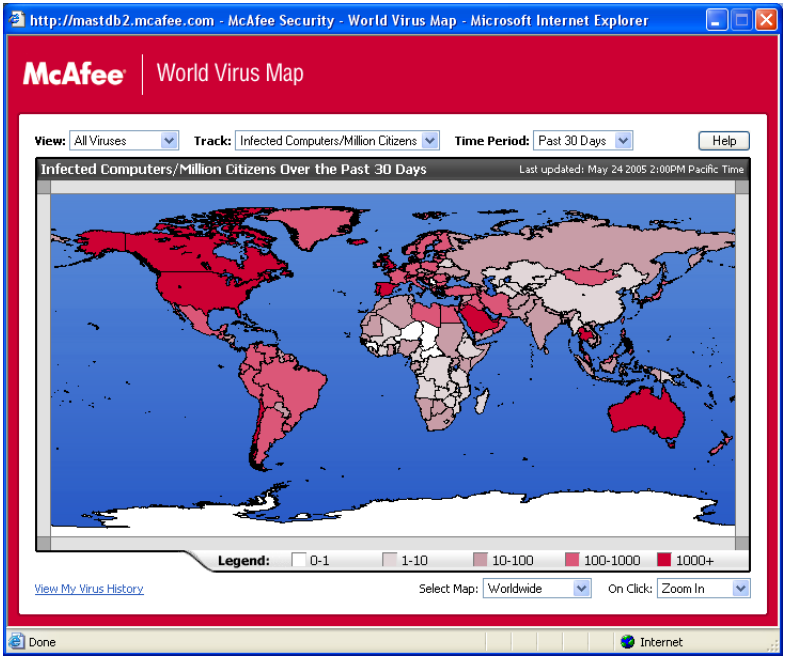
Przeglądanie mapy ataków wirusowych na świecie

Niezależnie od tego, czy uczestniczysz w programie tworzenia mapy ataków wirusowych na świecie, możesz korzystać ze światowych statystyk wykrywanych zagrożeń - dostępnych pod ikoną programu McAfee na pasku zadań systemu Windows.

Aby obejrzeć mapę ataków wirusowych na świecie:

- Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Mapa ataków wirusowych na świecie**.

Zostanie wyświetlona strona sieci Web **World Virus Map** (Ilustracja 2-15).



Ilustracja 2-15. World Virus Map

Domyślnie mapa ataków wirusowych pokazuje liczbę komputerów z całego świata, na których w ciągu ostatnich 30 dni wykryto podejrzane pliki, oraz czas ostatniej aktualizacji danych. Można zmienić widok mapy, aby sprawdzić liczbę wykrytych plików; możliwe jest także zapoznanie się z danymi z innego okresu - tylko z ostatnich 7 dni lub ostatnich 24 godzin.

W obszarze **Śledzenie wirusów** przedstawiane są sumaryczne informacje o liczbie przeskanowanych plików oraz wykrytych plików i zawierających podejrzane pliki komputerów, o których otrzymano raporty we wskazanym terminie.

Aktualizacja programu VirusScan

Gdy komputer jest połączony z Internetem, program VirusScan co cztery godziny automatycznie sprawdza dostępność aktualizacji, po czym automatycznie pobiera i instaluje cotygodniowe aktualizacje definicji wirusów, nie przerywając pracy użytkownika.

Pliki definicji wirusów mają rozmiar około 100 KB, w związku z czym ich pobieranie ma minimalny wpływ na wydajność systemu.

W przypadku wykrycia aktualizacji produktu lub epidemii wirusowej wyświetlany jest alert. Można wtedy wybrać opcję zaktualizowania programu VirusScan w celu usunięcia zagrożenia epidemią.

Automatyczne sprawdzanie aktualizacji

Program McAfee SecurityCenter jest skonfigurowany w ten sposób, aby co cztery godziny automatycznie sprawdzać aktualizacje wszystkich usług McAfee, gdy komputer jest połączony z Internetem, a następnie powiadomić użytkownika za pomocą alertów i dźwięków. Domyślnie program SecurityCenter automatycznie pobiera i instaluje wszystkie dostępne aktualizacje.

UWAGA
W niektórych przypadkach może zostać wyświetlony monit o ponowne uruchomienie komputera w celu dokończenia aktualizacji. Przed powtórnym uruchomieniem komputera należy pamiętać o zapisaniu pracy i zamknięciu wszystkich otwartych aplikacji.

Ręczne sprawdzanie aktualizacji

Oprócz możliwości automatycznego sprawdzania aktualizacji co cztery godziny, gdy komputer jest połączony z Internetem, istnieje możliwość ręcznego sprawdzenia aktualizacji w dowolnym momencie.

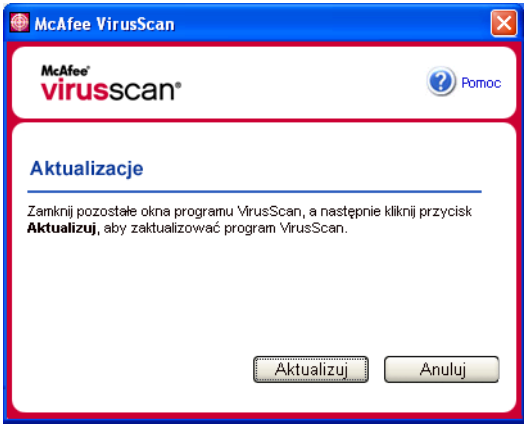
Aby ręcznie sprawdzić dostępność aktualizacji programu VirusScan:

1. Upewnij się, że komputer jest połączony z Internetem.
2. Kliknij prawym przyciskiem myszy ikonę programu McAfee i wybierz polecenie **Aktualizacje**.

   Zostanie wyświetlone okno dialogowe **SecurityCenter - Aktualizacje**.
3. Kliknij przycisk **Sprawdź teraz**.

   Jeśli jest dostępna aktualizacja, zostanie otwarte okno dialogowe **VirusScan - Aktualizacje** (Ilustracja 2-16 na stronie 42). Aby kontynuować, kliknij przycisk **Aktualizuj**.

Jeśli nie ma dostępnych aktualizacji, zostanie otwarte okno dialogowe z informacją, że program VirusScan nie wymaga uaktualnienia. Kliknij przycisk **OK**, aby zamknąć to okno dialogowe.



Ilustracja 2-16. Okno dialogowe Aktualizacje

4 W przypadku wyświetlenia monitu zaloguj się w witrynie sieci Web. **Kreator aktualizacji** automatycznie zainstaluje aktualizację.

5 Kliknij przycisk **Zakończ**, gdy instalacja aktualizacji dobiegnie końca.

UWAGA
W niektórych przypadkach może zostać wyświetlony monit o ponowne uruchomienie komputera w celu dokończenia aktualizacji. Przed powtórnym uruchomieniem komputera należy pamiętać o zapisaniu pracy i zamknięciu wszystkich otwartych aplikacji.

Skorowidz

A

ActiveShield
- czyszczenie wirusa, 25
- domyślne ustawienie skanowania, 15, 18 do 24
- opcje skanowania, 14
- skanowanie jedynie plików programów i dokumentów, 22
- skanowanie przychodzących załączników wiadomości błyskawicznych, 20
- skanowanie w poszukiwaniu nowych, nieznanych wirusów, 22
- skanowanie w poszukiwaniu potencjalnie niepożądanych programów (PUP), 23
- skanowanie w poszukiwaniu robaków, 18
- skanowanie w poszukiwaniu skryptów, 22
- skanowanie wiadomości e-mail i załączników, 16
- skanowanie wszystkich plików, 21
- skanowanie wszystkich typów plików, 21
- testowanie, 9
- uruchamianie, 15
- włączanie, 13
- wyłączanie, 14
- zatrzymywanie, 15

aktualizacja
- dyskietka ratunkowa, 38
- VirusScan
  - automatycznie, 41
  - ręcznie, 41

alerty
- dotyczące podejrzanych skryptów, 26
- dotyczące potencjalnych robaków, 26
- dotyczące programów PUP, 27
- dotyczące wykrytych plików, 25
- dotyczące wykrytych wiadomości e-mail, 26
- w poszukiwaniu wirusów, 25

B

biała lista, programy, 27

D

dyskietka ratunkowa
- aktualizacja, 38
- korzystanie, 34, 38
- tworzenie, 36
- zabezpieczanie przed zapisem, 37

E

edytowanie białych list, 27
Eksplorator Windows, 31

K

Karta Szybki start, iii
konfigurowanie
- VirusScan
  - ActiveShield, 13
  - Skanowanie, 28

konie trojańskie
- alerty, 25
- wykrywanie, 34

korzystanie z dyskietki ratunkowej, 38
Kreator aktualizacji, 15
Kwarantanna
- czyszczenie plików, 35
- dodawanie podejrzanych plików, 35
- przesyłanie podejrzanych plików, 36
- przywracanie wyczyszczonych plików, 35 do 36
- usuwanie plików, 35
- usuwanie podejrzanych plików, 36
- zarządzanie podejrzanymi plikami, 35

L

lista wykrytych plików (funkcja skanowania), 30, 34
Lista zaufanych programów PUP, 27

M

Mapa ataków wirusowych na świecie
przeglądanie, 39
raportowanie, 38
McAfee SecurityCenter, 11
Microsoft Outlook, 31

N

nowe funkcje, 7

O

opcje skanowania
ActiveShield, 14, 21 do 22
Skanowanie, 28

P

planowanie skanowania, 32
pomoc techniczna, 34
potencjalnie niepożądane programy (PUP), 23
alerty, 27
czyszczenie, 34
poddawanie kwarantannie, 34
usuwanie, 27, 34
wykrywanie, 34
zaufany, 27
przesyłanie podejrzanych plików do zespołu AVERT, 36
przychodzące załączniki wiadomości błyskawicznych
czyszczenie automatyczne, 20
skanowanie, 20

R

robaki
alerty, 25 do 26
wykrywanie, 25, 34
zatrzymywanie, 26

S

ScriptStopper, 22
Skanowanie
automatyczne skanowanie, 32
czyszczenie wirusa lub potencjalnie niepożądanego programu, 34
poddanie kwarantannie wirusa lub potencjalnie niepożądanego programu, 34
ręczne skanowanie, 28
ręczne skanowanie z poziomu Eksploratora Windows, 31
ręczne skanowanie z poziomu paska narzędzi programu Microsoft Outlook, 31
Skanuj podfoldery, opcja, 28
Skanuj w poszukiwaniu nowych nieznanych wirusów, opcja, 29
Skanuj w poszukiwaniu potencjalnie niepożądanych programów, opcja, 30
Skanuj wewnątrz skompresowanych plików, opcja, 29
Skanuj wszystkie pliki, opcja, 29
testowanie, 10 do 11
usuwanie wirusa lub potencjalnie niepożądanego programu, 34
skanowanie
planowanie automatycznego skanowania, 32
podfoldery, 28
skompresowane pliki, 29
tylko pliki programów i dokumenty, 22
w poszukiwaniu nowych, nieznanych wirusów, 29
w poszukiwaniu potencjalnie niepożądanych programów (PUP), 23
w poszukiwaniu robaków, 18
w poszukiwaniu skryptów, 22
wszystkie pliki, 21, 29
z poziomu Eksploratora Windows, 31
z poziomu paska narzędzi programu Microsoft Outlook, 31
Skanuj podfoldery, opcja (funkcja skanowania), 28
Skanuj w poszukiwaniu nowych nieznanych wirusów, opcja (funkcja skanowania), 29
Skanuj w poszukiwaniu potencjalnie niepożądanych programów, opcja (funkcja skanowania), 30
Skanuj wewnątrz skompresowanych plików, opcja (funkcja skanowania), 29
Skanuj wszystkie pliki, opcja (funkcja skanowania), 29
skrypty
alerty, 26
zatrzymywanie, 26
zezwalanie na wykonanie, 26
stosowanie białych list
programy PUP, 27

T

testowanie programu VirusScan, 9
tworzenie dyskietki ratunkowej, 36

V

VirusScan
- automatyczna aktualizacja, 41
- automatyczne przesyłanie informacji o wirusach, 38 do 39
- planowanie skanowania, 32
- ręczna aktualizacja, 41
- skanowanie z poziomu Eksploratora Windows, 31
- skanowanie z poziomu paska narzędzi programu Microsoft Outlook, 31
- testowanie, 9
- wprowadzenie, 7

W

wiadomości e-mail i załączniki
- czyszczenie automatyczne
  - włączanie, 16
- skanowanie
  - błędy, 17
  - włączanie, 16
  - wyłączanie, 17

wirusy
- alerty, 25
- automatyczne przesyłanie informacji, 38 do 39
- czyszczenie, 25, 34
- poddanie kwarantannie wykrytych plików, 25
- poddawanie kwarantannie, 25, 34
- usuwanie, 25, 34
- usuwanie programów PUP, 27
- usuwanie wykrytych plików, 26
- wykrywanie, 34
- wykrywanie za pomocą programu ActiveShield, 25
- zatrzymywanie podejrzanych skryptów, 26
- zatrzymywanie potencjalnych robaków, 26
- zezwalanie na wykonanie podejrzanych skryptów, 26

WormStopper, 18
wprowadzenie do programu VirusScan, 7
wymagania systemowe, 8

Z

zabezpieczanie dyskietki ratunkowej przed zapisem, 37
zespół AVERT, przesyłanie podejrzanych plików do, 36