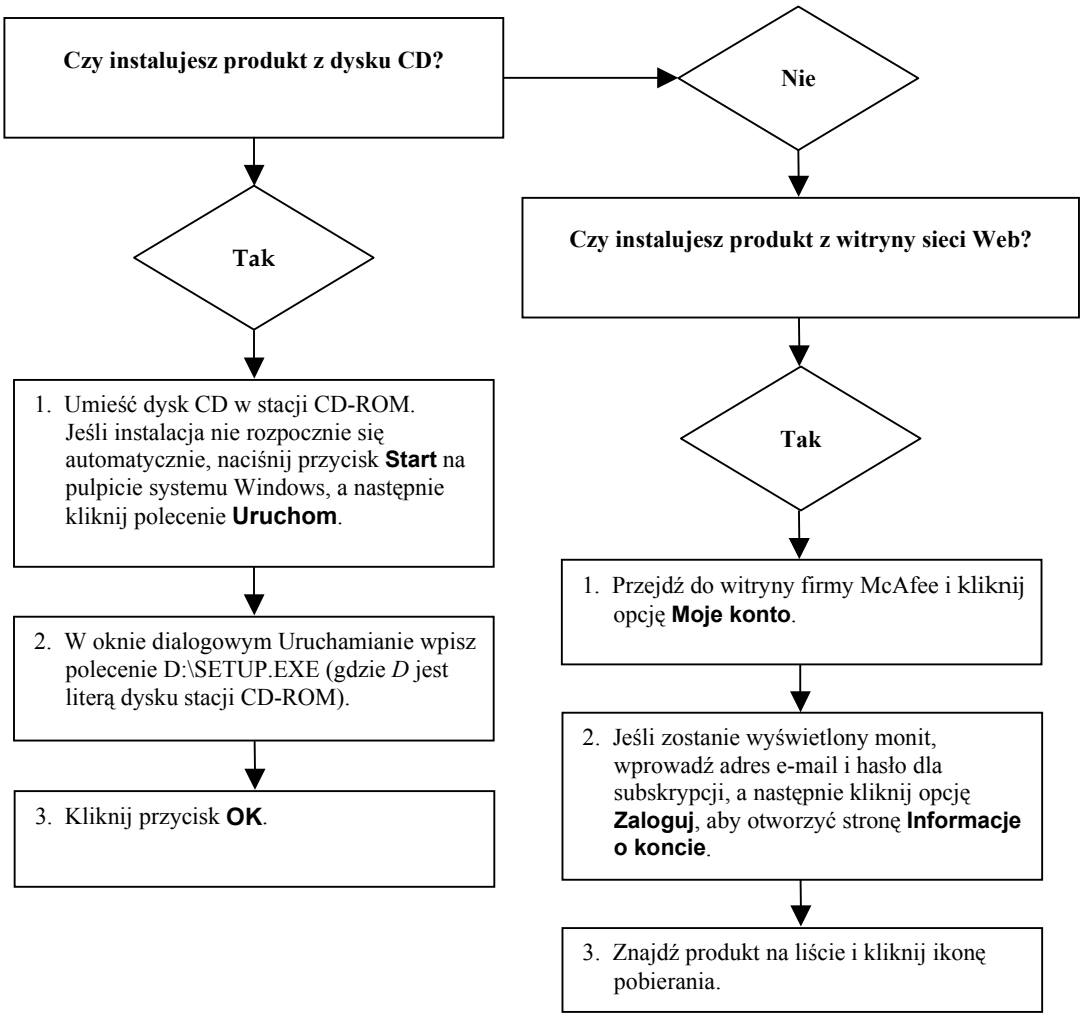
internetsecuritysuite

Podręcznik użytkownika

McAfee®

Karta Szybki start

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



Dodatkowe informacje

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

1. Włóż dysk CD 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 wysyłania rejestracji bezpośrednio do naszej firmy. Rejestracja zapewnia otrzymanie na czas odpowiedniej pomocy technicznej oraz następujące korzyści:

- DARMOWA 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 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 jest dostępny łatwy w obsłudze Kreator odpowiedzi umożliwiający rozwiązanie najczęściej spotykanych problemów.

Doświadczeni użytkownicy mogą także korzystać z opcji zaawansowanych, takich jak drzewo pomocy lub wyszukiwanie według słów kluczowych. W przypadku problemów ze znalezieniem rozwiązania można skorzystać z BEZPŁATNYCH usług Chat Now! i E-mail Express! firmy McAfee. Dzięki tym narzędziom można szybko i bezpłatnie skontaktować się przez Internet z wykwalifikowanymi pracownikami pomocy technicznej. Informacje na temat telefonicznej pomocy technicznej można także uzyskać w witrynie

http://www.mcafeehelp.com/.

Spis treści

Wprowadzenie 1

Internet jest niewyczerpanym źródłem informacji i rozrywki. Jednakże po połączeniu z siecią komputer jest narażony na różnego rodzaju próby naruszenia prywatności i zagrożenia bezpieczeństwa. Chroń swoją prywatność i zabezpiecz komputer oraz dane za pomocą programu McAfee Internet Security Suite. Opracowany w oparciu o nagradzane technologie firmy McAfee program McAfee Internet Security Suite jest jednym z najbardziej wszechstronnych zestawów narzędzi ochrony prywatności i bezpieczeństwa. Program McAfee Internet Security Suite niszczy wirusy, udaremnia wysiłki hakerów, zabezpiecza informacje osobiste, zapewnia prywatność podczas przeglądania witryn sieci Web, blokuje wyświetlanie reklam i wyskakujących okien, zarządza plikami cookie i hasłami, chroni pliki, foldery i dyski użytkownika, filtruje niepożądaną zawartość oraz zapewnia kontrolę nad przychodzącymi i wychodzącymi połączeniami komputera z Internetem.

Program McAfee Internet Security Suite jest sprawdzonym rozwiązaniem, które zapewnia doskonałą ochronę współczesnym użytkownikom Internetu.

Pakiet McAfee Internet Security Suite składa się z następujących produktów:

- *McAfee VirusScan* na str. 17
- *McAfee Personal Firewall Plus* na str. 51
- *McAfee Privacy Service* na str. 85
- *McAfee SpamKiller* na str. 109

Oprogramowanie McAfee Internet Security

- **McAfee SecurityCenter -** ocenia podatność komputera na ataki, podaje informacje na ten temat i ostrzega użytkownika o lukach w zabezpieczeniach. Każdy wskaźnik zabezpieczeń pozwala szybko ocenić podatność na próby naruszenia bezpieczeństwa i zagrożenia związane z dostępem do Internetu, a następnie udziela zaleceń umożliwiających szybkie i dokładne zabezpieczenie komputera.
- **McAfee VirusScan -** skanuje komputer w poszukiwaniu wirusów internetowych, a po wykryciu usuwa je. Można dostosować proces skanowania do własnych potrzeb, a także określić reakcję po wykryciu wirusa i czynności, jakie mają być podjęte. Można też skonfigurować program VirusScan tak, aby rejestrował wszystkie wykonywane na komputerze działania związane z wykrywaniem wirusów.
- **McAfee Personal Firewall Plus -** chroni komputer, gdy jest on podłączony do Internetu, oraz zabezpiecza wychodzące i przychodzące połączenia komputera z Internetem.
- **McAfee Privacy Service -** chroni informacje osobiste, blokuje reklamy internetowe i umożliwia filtrowanie zawartości. Program ten zabezpiecza informacje osobiste, zapewniając równocześnie większą kontrolę nad korzystaniem z Internetu przez rodzinę. Program McAfee Privacy Service gwarantuje, że informacje poufne nie są narażone na zagrożenia, i chroni całą rodzinę przed nieodpowiednimi publikacjami dostępnymi w Internecie.
- **McAfee SpamKiller -** ponieważ codziennie do przedsiębiorstw i odbiorców indywidualnych, zarówno dorosłych, jak i dzieci, przesyłana jest ogromna liczba fałszywych, nieodpowiednich i obraźliwych wiadomości, ochrona przed spamem jest podstawowym składnikiem strategii zabezpieczeń komputera.

Wymagania systemowe

- Microsoft® Windows 98, Me, 2000 lub XP
- Komputer z procesorem zgodnym z Pentium
  - Windows 98, 2000: 133 MHz lub lepszy
  - System Windows Me: 150 MHz lub lepszy
  - Windows XP (Home/Professional): 300 MHz lub lepszy
- RAM
  - Windows 98, Me, 2000: 64 MB
  - Windows XP (Home/Professional): 128 MB

- 100 MB miejsca na twardym dysku
- Microsoft® Internet Explorer 5.5 lub nowszy

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)
- Zgodne z interfejsem MAPI (Outlook)
- Internetowe (MSN/Hotmail lub konto e-mail oparte na protokole POP3)

Wymagania dotyczące dodatku plug-in paska narzędzi

- Outlook Express 6.0 lub nowszy
- Outlook 98, 2000 z dodatkiem SP3, 2003 lub XP
- Internet Explorer w wersji 6.0 lub nowszej

Obsługiwane programy wiadomości błyskawicznych

- AOL Instant Messenger 2.1 lub nowszy
- Yahoo Messenger 4.1 lub nowszy
- Microsoft Windows Messenger 3.6 lub nowszy
- MSN Messenger 6.0 lub nowszy

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 bezpłatnej analizy zabezpieczeń komputera;
- Uruchamianie, zarządzanie i konfiguracja 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 internetowej firmy McAfee.

> **UWAGA**
> Aby uzyskać więcej informacji na temat funkcji programu SecurityCenter, 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 i 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  na pasku zadań systemu Windows.
2. Kliknij polecenie **Otwórz program SecurityCenter**.

Aby uzyskać dostęp do produktu McAfee:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee  na pasku zadań systemu Windows.
2. Wskaż odpowiedni produkt firmy McAfee i wybierz funkcję, której chcesz użyć.

Usuwanie pakietu oprogramowania Internet Security Suite

W niektórych przypadkach może wystąpić potrzeba usunięcia pakietu Internet Security Suite lub niektórych jego aplikacji.

UWAGA
Do odinstalowania programów pakietu Internet Security Suite wymagane są uprawnienia administratora.

1. Zapisz pracę i zamknij wszystkie otwarte aplikacje.
2. Otwórz **Panel sterowania**.
   - Na pasku zadań systemu Windows kliknij przycisk **Start**, wskaż polecenie **Ustawienia**, a następnie kliknij opcję **Panel sterowania** (w systemach Windows 98, ME i 2000).
   - Na pasku zadań systemu Windows kliknij przycisk **Start**, a następnie kliknij polecenie **Panel sterowania** (w systemie Windows XP).
3. Kliknij opcję **Dodaj/Usuń programy**.
4. Wybierz kreatora odinstalowywania programów firmy McAfee, a następnie wybierz jeden lub więcej programów i kliknij opcję **Odinstaluj**. Aby usunąć wszystkie produkty wchodzące w skład pakietu Internet Security, kliknij opcję **Zaznacz wszystko**, a następnie opcję **Odinstaluj**.
5. Aby kontynuować usuwanie, kliknij opcję **Tak**.
6. Po wyświetleniu monitu uruchom komputer ponownie.

McAfee VirusScan 2

McAfee VirusScan - Zapraszamy!

McAfee VirusScan to udostępniane w drodze subskrypcji rozwiązanie antywirusowe zapewniające kompleksową i niezawodną ochronę komputera opartą na często aktualizowanych plikach sygnatur. 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.

Program ma następujące funkcje:

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 i 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 komputer w kluczowych punktach ataku na niego: skanowane są wiadomości e-mail i wiadomości błyskawiczne, załączniki do nich 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**
  Zespół pomocy technicznej zapewnia szybką i przystępną pomoc za pośrednictwem poczty elektronicznej i wiadomości błyskawicznych.

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, kliknij na karcie VirusScan w programie SecurityCenter 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 na ten temat można znaleźć w sekcji *Jak działa system generowania alertów zabezpieczeń* na str. 33.

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 zapisano 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 przeskanuje 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 na ten temat można znaleźć w sekcji *Jak działa system wykrywania zagrożeń* na str. 42.

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 bezpłatnej analizy zabezpieczeń komputera;
- uruchamianie, zarządzanie i konfiguracja 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 internetowej 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 (w obszarze powiadomień systemu Windows XP) zostanie wyświetlona czerwona ikona z literą M  . Jest to obszar zawierający zegar i 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 ActiveShield

Po uruchomieniu (załadowaniu do pamięci komputera) i włączeniu program ActiveShield zapewnia ciągłą ochronę systemu. 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) po zakończeniu instalacji i ponownym uruchomieniu komputera.

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 mechanizmu 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 23).

Wyłączanie programu ActiveShield

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

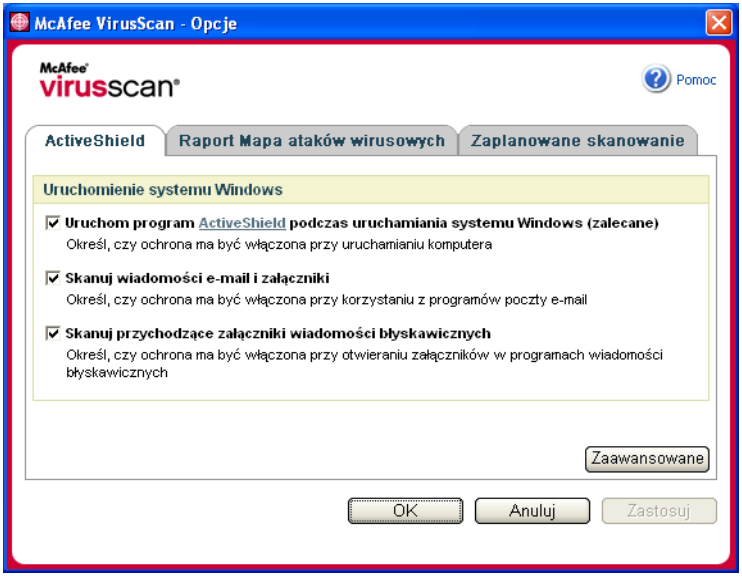
1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Wyłącz**.
2. Kliknij przycisk **Tak**, aby potwierdzić ustawienie.

   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 23).

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 podłączony do Internetu.

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 23).

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 23).

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.

Po wyłączeniu opcji **Skanuj wiadomości e-mail i załączniki** automatycznie wyłączane są także opcje dotyczące funkcji skanowania wiadomości e-mail i programu WormStopper (Ilustracja 2-2 na stronie 26). Wyłączenie opcji skanowania poczty wychodzącej powoduje automatyczne wyłączenie opcji aplikacji 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 podejmuje następujące działania:

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

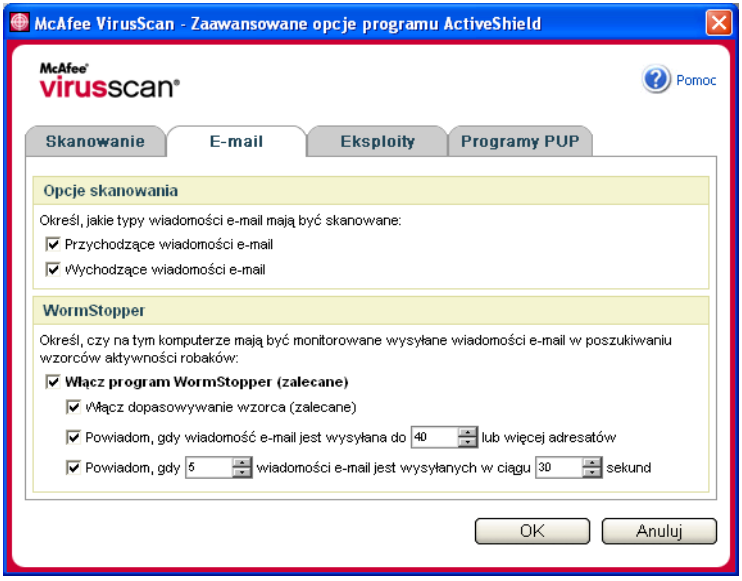
> **UWAGA**
> Szczegółowe informacje o błędach występujących podczas skanowania wychodzących wiadomości e-mail można znaleźć w pomocy w trybie online.

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).

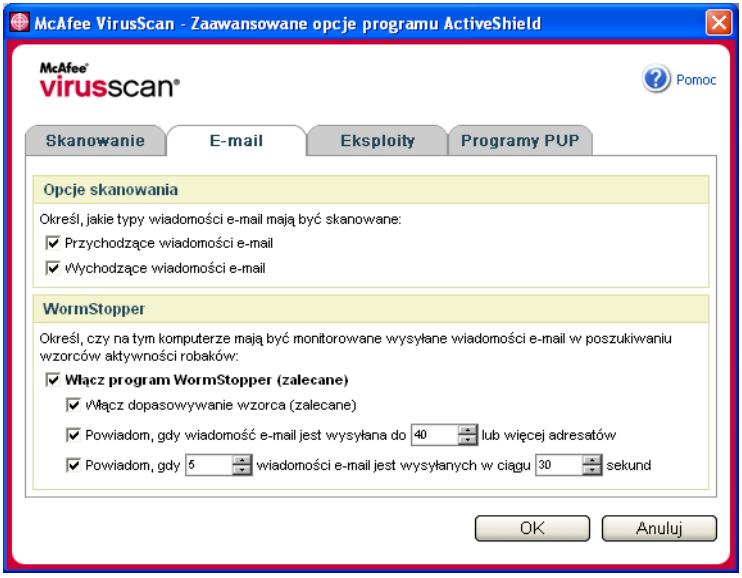
   Domyślnie włączone są następujące opcje:

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

   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**, gdy wyświetlony zostanie monit. Pozwoli to zachować ustawienia domyślne. Aby zastąpić wartości domyślne własnymi, kliknij przycisk **Tak**.

Następującą opcję można włączyć automatycznie po pierwszym wykryciu potencjalnego robaka (szczegółowe informacje znajdują się w rozdziale *Zarządzanie potencjalnymi robakami* na str. 34):

- 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 23).

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 do przychodzącej wiadomości błyskawicznej program VirusScan podejmie następujące działania:

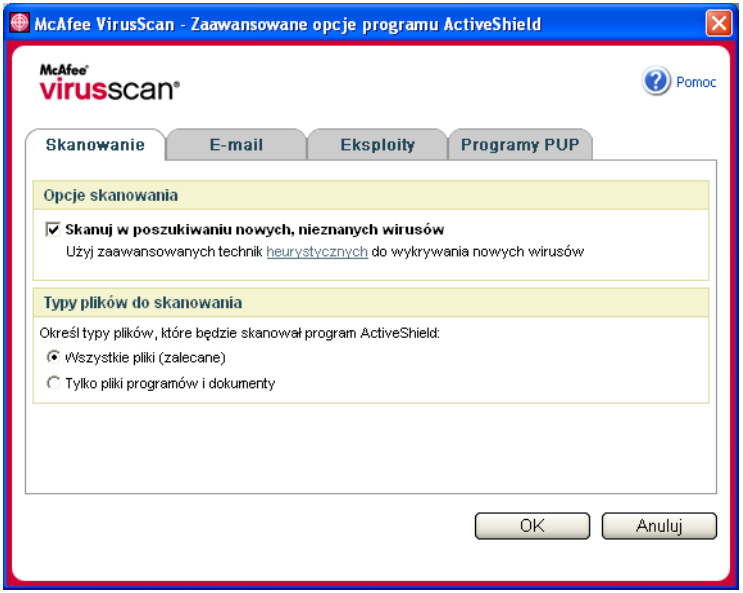
- Spróbuje wyczyścić wykrytą wiadomość.
- wyświetli monit o poddanie kwarantannie lub usunięcie wiadomości, której nie udało się wyczyścić.

Skanowanie wszystkich plików

Jeśli dla programu ActiveShield uaktywniono domyślną opcję **Wszystkie pliki (zalecane)**, skanowane będą wszystkie typy plików używane przez komputer. Pliki będą skanowane przy próbie użycia ich przez komputer. Opcji tej należy użyć, aby zapewnić jak najdokładniejsze skanowanie komputera.

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 29).
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 ustawienia w programie 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 uaktywniono domyślną opcję **Skanuj w poszukiwaniu nowych, nieznanych wirusów (zalecane)**, będzie on stosował zaawansowane techniki heurystyczne porównujące pliki z sygnaturami znanych wirusów i wyszukujące oznak 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.

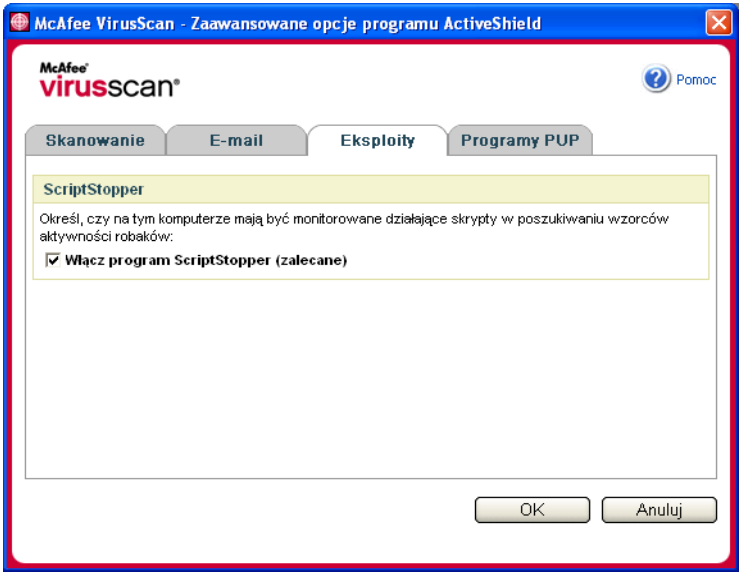
Mechanizm ochronny ScriptStopper wykrywa i blokuje podejrzaną działalność i informuje o niej użytkownika. Przejawem podejrzanej działalności może być następująca operacja:

- 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

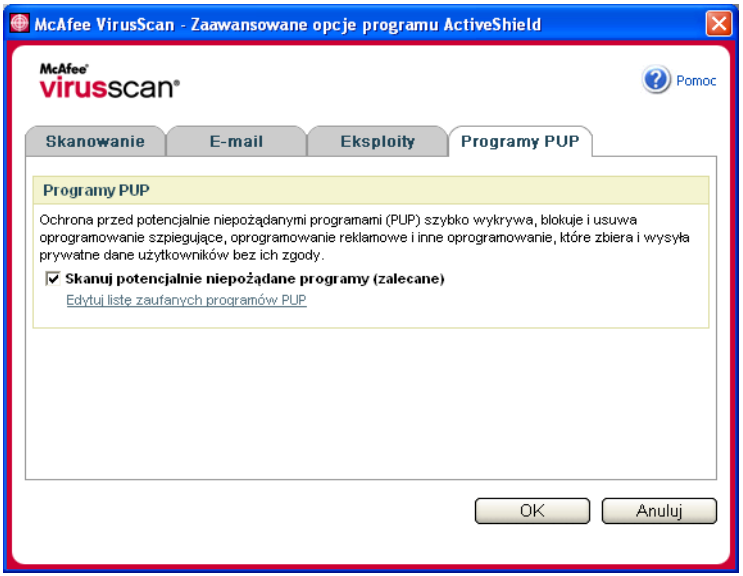
Skanowanie w poszukiwaniu potencjalnie niepożądanych programów (PUP)

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:

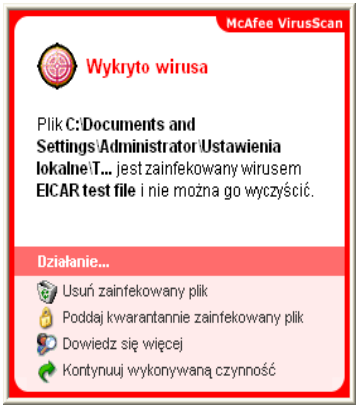
1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **VirusScan**, a następnie kliknij polecenie **Opcje**.
2. Kliknij przycisk **Zaawansowane**, a następnie kliknij kartę **Programy PUP** (Ilustracja 2-6).
3. Kliknij opcję **Skanuj potencjalnie niepożądane programy (zalecane)**, 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, wyświetli alert o wirusie podobny do przedstawionego tutaj: Ilustracja 2-7. W przypadku większości wirusów, koni trojańskich i robaków program ActiveShield podejmie próbę wyczyszczenia pliku automatycznie i wyświetli alert. 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 podejrzanych plików, wiadomości e-mail lub skryptów, a także potencjalnych robaków i programów PUP. Możliwe jest także włączenie lub wyłączenie opcji przekazywania 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 skanera poczty e-mail jest próba automatycznego wyczyszczenia wykrytych wiadomości e-mail. Plik alertu dołączany do wiadomości przychodzących informuje 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 potencjalnie niepożądanymi 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 z potwierdzeniem.

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

  - W przeciwnym razie kliknij przycisk **Anuluj**, aby przerwać proces automatycznego usuwania. Program można będzie usunąć także 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 został zainstalowany w ramach większego pakietu albo zaakceptowano umowę licencyjną zawierającą wymóg jego zainstalowania, 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 znajdują się w rozdziale *Zarządzanie zaufanymi programami PUP*.

Zarządzanie zaufanymi programami PUP

Programy dodane do listy Zaufane programy PUP nie będą 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 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

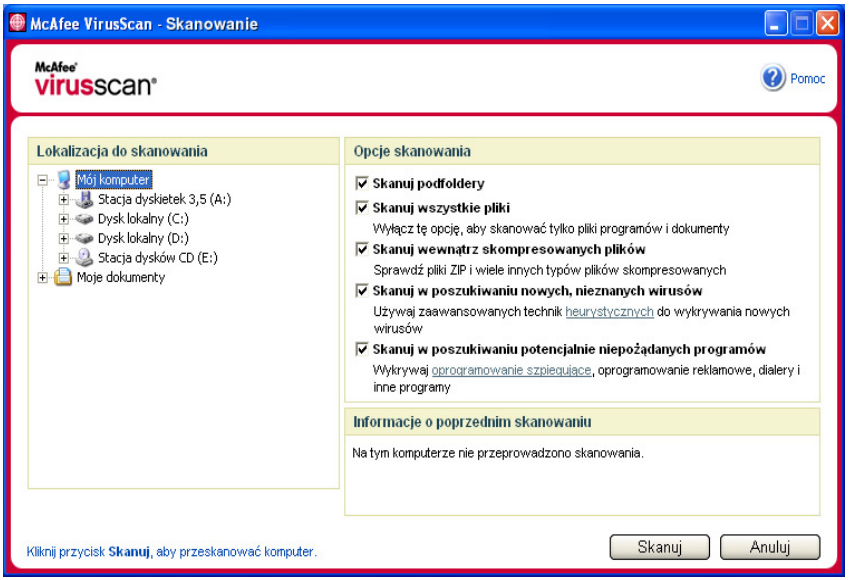
Funkcja skanowania pozwala przeskanować wybrane dyski twarde, dyskietki oraz pojedyncze pliki i foldery w poszukiwaniu wirusów i innych zagrożeń. Jeżeli w trakcie skanowania zostanie wykryty podejrzany plik, program automatycznie spróbuje go wyczyścić, o ile plik ten nie jest potencjalnie niepożądanym 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).



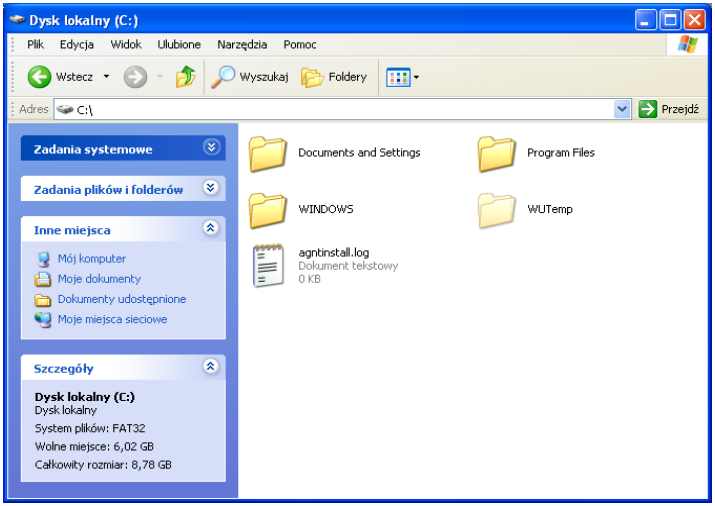
Ilustracja 2-8. Okno dialogowe Skanowanie

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

3 Wybierz żądane ustawienia w obszarze **Opcje skanowania**. Domyślnie zaznaczone są wszystkie ustawienia dostępne w obszarze **Opcje skanowania**, co zapewnia optymalną 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 ani ich zawartość nie zostaną przeskanowane. Aby je przeskanować, należy pozostawić zaznaczenie tego pola wyboru.



Ilustracja 2-9. Zawartość lokalnego dysku

- **Skanuj wszystkie pliki** - użyj tej opcji, aby 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 tej opcji umożliwia funkcji skanowania wykrywanie takich wirusów.

- **Skanuj w poszukiwaniu nowych, nieznanych wirusów** - użyj tej opcji, jeśli chcesz, aby wykrywane były najnowsze wirusy, dla których z dużą dozą prawdopodobieństwa nie opracowano jeszcze metody leczenia. Opisywana opcja wykorzystuje zaawansowane techniki heurystyczne porównujące pliki z sygnaturami znanych wirusów i wyszukujące dowodów obecności w plikach niezidentyfikowanych wirusów.

  Wyszukiwane są też cechy plików pozwalające zwykle wykluczyć obecność wirusa. Zmniejsza to ryzyko zidentyfikowania przez funkcję skanowania niezainfekowanego pliku jako wirusa. Pliki, które skanowanie heurystyczne wskazało jako potencjalne wirusy, należy traktować 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.

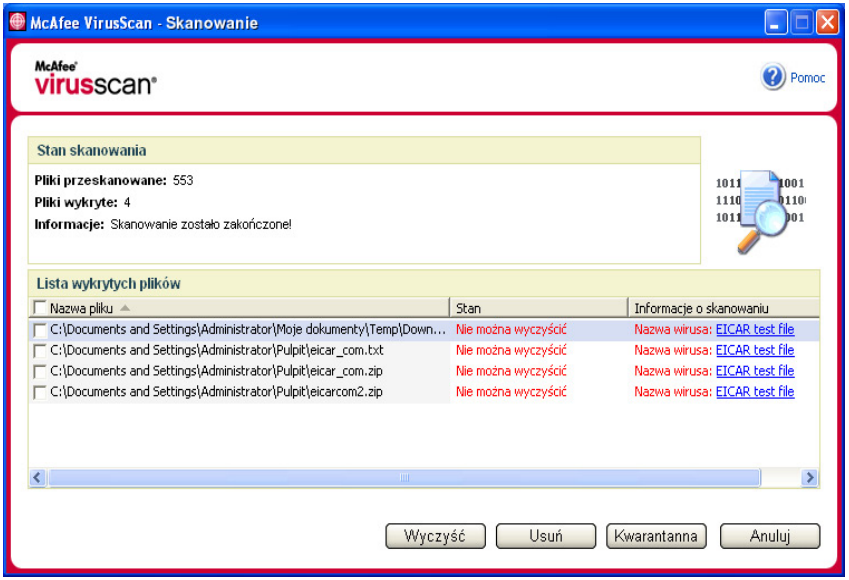
UWAGA

Zalecane jest zaznaczenie wszystkich opcji, aby komputer był skanowany jak najdokładniej. W 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 (.ZIP, .CAB itp.) zostaje uwzględniony w liczbie plików wyświetlanych pod pozycją **Pliki przeskanowane** 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 str. 42.

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 największą możliwą dokładność skanowania (Ilustracja 2-8 na stronie 36).

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 przeskanować wiadomości e-mail z poziomu programu Microsoft Outlook:

1 Otwórz program Microsoft Outlook.

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

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 36).

Automatyczne skanowanie w poszukiwaniu wirusów i innych zagrożeń

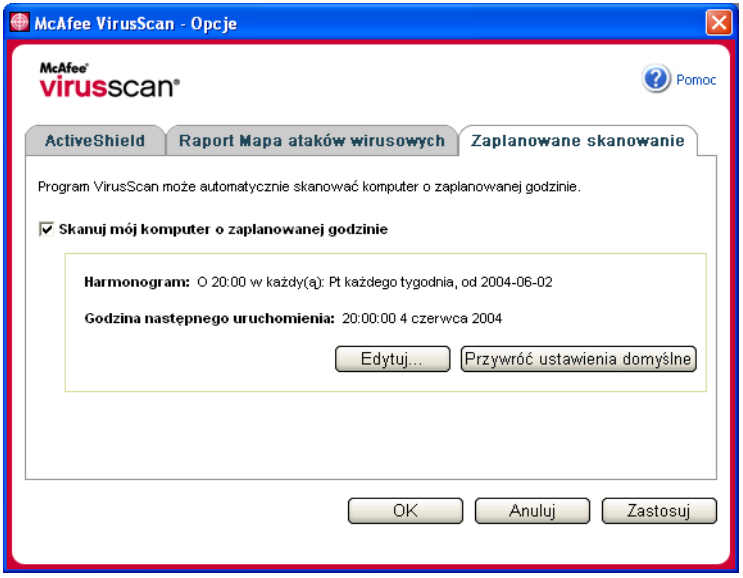
Chociaż program VirusScan skanuje na bieżąco pliki, z których chce skorzystać użytkownik lub komputer, za pomocą usługi Harmonogram zadań systemu Windows można zaplanować skanowanie automatyczne, aby w ustalonych odstępach czasu sprawdzać, czy komputer jest wolny od wirusów i innych zagrożeń.

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 40).



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** i **Pokaż wiele harmonogramów**. Ostatnio wybrany obsługiwany harmonogram pozostanie włączony do momentu wybrania prawidłowej opcji.

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

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

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

  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 str. 43).

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 na ten temat można znaleźć w sekcji *tworzenie dyskietki ratunkowej* na str. 45.

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

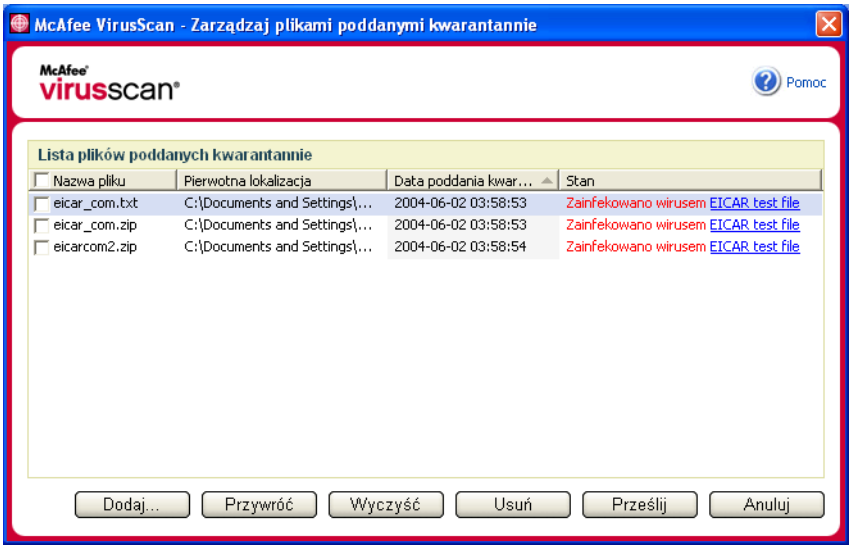
Zarządzanie plikami poddanymi kwarantannie

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 można przywrócić w pierwotnej jego 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 pierwotnej 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 (PUP), plik ten można przesłać do zespołu szybkiego reagowania AVERT™ firmy McAfee, który dokona jego analizy, w następujący sposób:

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 pierwotną 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.

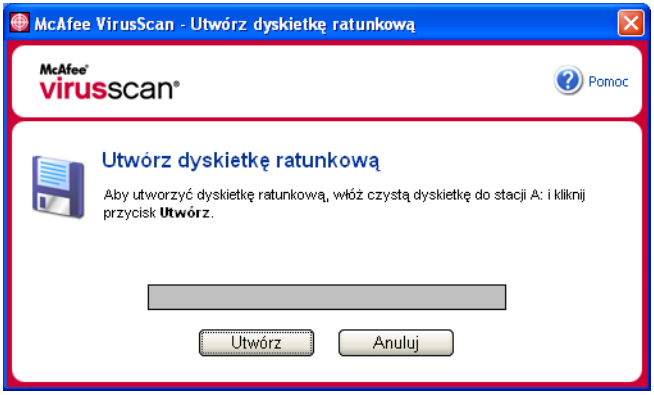
> **UWAGA**
> Aby można było pobrać obraz dyskietki ratunkowej, należy być podłączonym do Internetu. Obraz ten jest dostępny jedynie w wersji przeznaczonej dla komputerów z partycjami FAT (FAT 16 i FAT 32). Nie jest potrzebny w przypadku partycji NTFS.

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 str. 36).

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, wyświetlony zostanie komunikat informujący o konieczności pobrania pliku obrazu dla dyskietki ratunkowej. Kliknij przycisk **OK**, aby pobrać ten składnik, lub kliknij przycisk **Anuluj**, aby pobrać go później.

   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 odpowiednią opcję, naciskając klawisz funkcyjny (np. F2, F3).

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

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

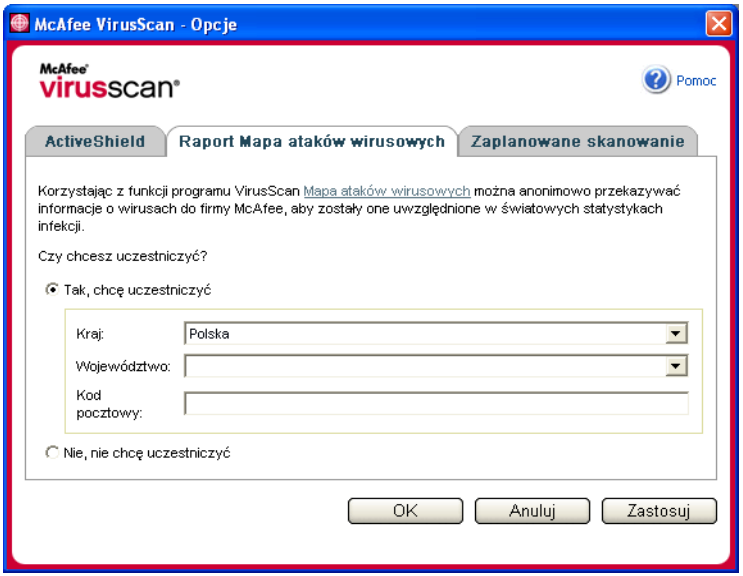
Przesyłanie raportu do mapy ataków wirusowych na świecie

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 dla mapy ataków wirusowych

3 Zaakceptuj ustawienie domyślne **Tak, chcę uczestniczyć**, jeśli chcesz, aby do firmy McAfee były anonimowo przekazywane informacje o wirusach znalezionych na Twoim komputerze. Informacje te będą uwzględniane w światowych statystykach infekcji. W przeciwnym razie 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 spróbuje wybrać kraj, w którym znajduje się komputer.

5 Kliknij przycisk **OK**.

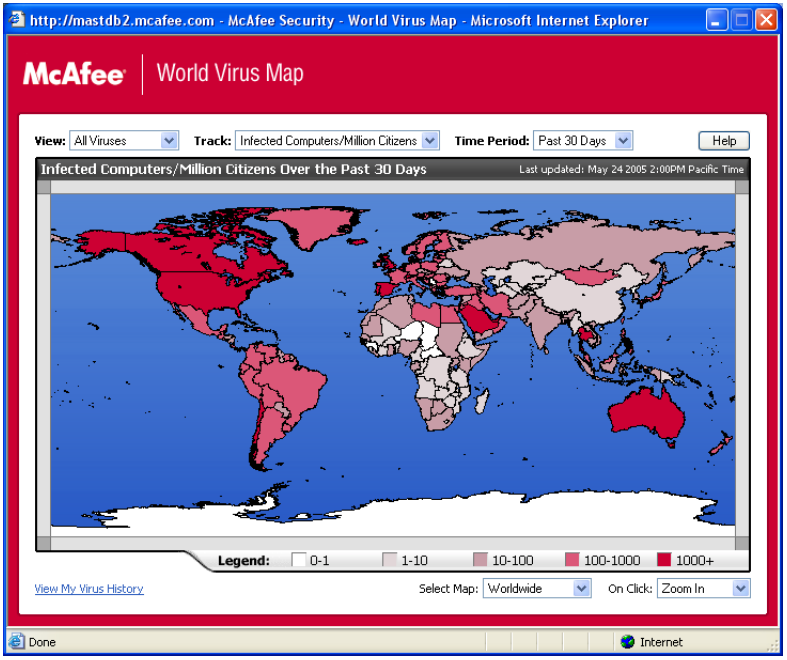
Przeglądanie mapy ataków wirusowych na świecie

Niezależnie od tego, czy uczestniczysz w programie tworzenia mapy ataków wirusowych na świecie, możesz korzystać ze światowych statystyk infekcji 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 **World Virus Map**.

  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 wirusową.

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. Należy pamiętać o zapisaniu pracy i zamknięciu wszystkich otwartych aplikacji przed ponownym uruchomieniem komputera.

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.

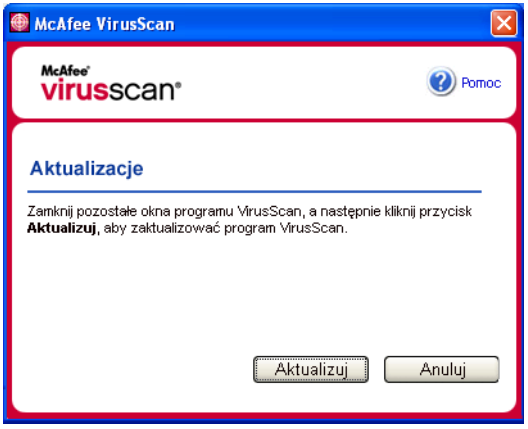
2 Kliknij prawym przyciskiem myszy ikonę programu McAfee i wybierz polecenie **Aktualizacje**.

Zostanie wyświetlone okno dialogowe **SecurityCenter - Aktualizacje**.

3 Kliknij przycisk **Sprawdź teraz**.

Jeśli aktualizacja jest dostępna, zostanie otwarte okno dialogowe **VirusScan - Aktualizacje** (Ilustracja 2-16 na stronie 50). 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 Po wyświetleniu monitu zaloguj się w witrynie sieci Web. **Kreator aktualizacji** zainstaluje aktualizację automatycznie.

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. Należy pamiętać o zapisaniu pracy i zamknięciu wszystkich otwartych aplikacji przed ponownym uruchomieniem komputera.

McAfee Personal Firewall Plus 3

McAfee Personal Firewall Plus - zapraszamy!

Oprogramowanie McAfee Personal Firewall Plus zapewnia zaawansowaną ochronę komputera oraz osobistych informacji użytkownika. Program Personal Firewall tworzy barierę między komputerem a Internetem, dyskretnie monitorując ruch internetowy w poszukiwaniu podejrzanych działań.

Program ma następujące funkcje:

- Obrona przed potencjalnymi próbami włamań i atakami hakerów.
- Uzupełnia ochronę antywirusową.
- Monitoruje ruch internetowy i sieciowy.
- Ostrzega o potencjalnie niebezpiecznych zdarzeniach.
- Informuje szczegółowo o podejrzanym ruchu internetowym.
- Integracja funkcji witryny HackerWatch.org łącznie z raportowaniem zdarzeń, narzędziami do samodzielnego testowania systemu oraz możliwością przesyłania zgłoszonych zdarzeń pocztą elektroniczną do innych ekspertów online.
- Zawiera funkcje szczegółowego śledzenia oraz badania zdarzeń.

nowe funkcje

- **Udoskonalona obsługa gier**
  Program McAfee Personal Firewall Plus chroni komputer przed próbami włamań i podejrzanymi działaniami podczas pełnoekranowej sesji gry, ale w razie ich wykrycia może ukrywać alerty. Alerty czerwone pojawią się po wyjściu z gry.

- **Udoskonalone zarządzanie dostępem**
  Program McAfee Personal Firewall Plus umożliwia użytkownikom dynamiczne przyznawanie aplikacjom tymczasowego dostępu do Internetu. Dostęp jest ograniczony do czasu między uruchomieniem aplikacji a jej zamknięciem.
  Gdy produkt Personal Firewall wykryje nieznany program próbujący komunikować się z Internetem, czerwony alert umożliwia przyznanie tej aplikacji tymczasowego dostępu do sieci.

- **Ulepszone sterowanie zabezpieczeniami**
  Funkcja blokowania dostępna w programie McAfee Personal Firewall Plus umożliwia natychmiastowe zablokowanie całego przychodzącego i wychodzącego ruchu sieciowego między komputerem a Internetem. Użytkownicy mogą włączać i wyłączać funkcję blokowania z trzech miejsc w programie.

- **Udoskonalona obsługa sytuacji awaryjnych**
  Za pomocą polecenia Resetuj ustawienia można automatycznie przywrócić ustawienia domyślne. Jeśli program Personal Firewall będzie działać w sposób niepożądany, którego użytkownik nie będzie mógł poprawić, może on przywrócić domyślne ustawienia produktu.

- **Ochrona połączeń z Internetem**
  Aby zapobiec przypadkowemu zablokowaniu połączeń z Internetem przez użytkownika, opcja zabraniania dostępu z adresu internetowego jest wyłączona w alercie niebieskim, jeśli program Personal Firewall wykryje, że źródłem połączenia jest serwer DHCP lub DNS. Jeśli ruch przychodzący nie pochodzi z serwera DHCP lub DNS, opcja pojawi się na alercie.

- **Ulepszona integracja z witryną HackerWatch.org**
  Raportowanie o potencjalnych hakerach jest prostsze niż kiedykolwiek. Program McAfee Personal Firewall Plus poszerza funkcjonalność witryny HackerWatch.org, umożliwiając między innymi wysyłanie do bazy danych informacji o podejrzanych zdarzeniach.

- **Rozszerzona inteligentna obsługa aplikacji**
  Gdy aplikacja próbuje uzyskać dostęp do Internetu, program Personal Firewall sprawdza najpierw, czy aplikacja ta jest uważana za zaufaną czy szkodliwą. Jeśli zostanie rozpoznana jako zaufana, program Personal Firewall automatycznie zezwoli jej na dostęp do Internetu bez konieczności podejmowania działań przez użytkownika.

- **Zaawansowane wykrywanie koni trojańskich**
  Program McAfee Personal Firewall Plus łączy zarządzanie połączeniami aplikacji z ulepszoną bazą danych. Umożliwia to wykrycie większej liczby potencjalnie szkodliwych aplikacji mogących przekazywać dane osobiste, takich jak konie trojańskie, i zablokowanie im dostępu do Internetu.

- **Udoskonalone śledzenie wizualne**
  Zawiera ono przejrzyste mapy graficzne pokazujące źródło ataków i przepływ danych na całym świecie, w tym szczegółowe informacje kontaktowe/informacje o właścicielu pochodzące z jego adresu IP.

- **Większa prostota używania**
  Program McAfee Personal Firewall Plus zawiera Asystenta konfiguracji i Samouczek użytkownika, które zawierają informacje o konfigurowaniu zapory i korzystaniu z niej. Pomimo, że produkt został zaprojektowany do działania bez jakiejkolwiek interwencji, firma McAfee dostarcza użytkownikom bogate zasoby pozwalające zrozumieć i docenić zalety działania zapory.

- **Ulepszony system wykrywania włamań**
  System wykrywania włamań (IDS, Intrusion Detection System) programu Personal Firewall wykrywa typowe wzorce ataków oraz inne podejrzane działania. Monitoruje on każdy przychodzący pakiet danych w poszukiwaniu podejrzanych transferów danych lub metod przesyłania oraz rejestruje je w dzienniku zdarzeń.

- **Ulepszona analiza ruchu**
  Program McAfee Personal Firewall Plus umożliwia użytkownikom wgląd zarówno w dane przychodzące, jak i wychodzące z ich komputerów. Pokazuje też połączenia aplikacji oraz programy, które aktywnie „nasłuchują” w oczekiwaniu na otwarcie połączeń. Umożliwia to użytkownikom zauważenie i podjęcie działań w stosunku do aplikacji, które mogą być narażone na włamania.

Usuwanie zapór innych firm

Przed rozpoczęciem instalacji oprogramowania McAfee Personal Firewall Plus na komputerze, należy odinstalować inne zapory. W tym celu należy postępować zgodnie z instrukcją odinstalowania tych programów.

UWAGA
W przypadku korzystania z systemu Windows XP nie jest konieczne wyłączenie wbudowanej zapory przed zainstalowaniem oprogramowania McAfee Personal Firewall Plus. Jednakże jest to zalecane. Pozostawienie włączonej wbudowanej zapory uniemożliwi rejestrowanie zdarzeń w dzienniku zdarzeń przychodzących programu McAfee Personal Firewall Plus.

Ustawianie domyślnej zapory

Program McAfee Personal Firewall może zarządzać uprawnieniami i ruchem aplikacji internetowych na komputerze, nawet jeśli wykryje uruchomioną zaporę systemu Windows.

Po zainstalowaniu program McAfee Personal Firewall automatycznie wyłącza Zaporę systemu Windows i ustawia się jako zapora domyślna. Od tej chwili użytkownik korzysta tylko z funkcji i komunikatów programu McAfee Personal Firewall. Jeśli następnie użytkownik włączy Zaporę systemu Windows za pomocą Centrum zabezpieczeń systemu Windows lub Panelu sterowania, pozwalając na działanie na komputerze obu zapór, może to doprowadzić do częściowej utraty rejestrowanych danych przez program McAfee Personal Firewall, a także do powielania się komunikatów o stanie i alertów.

UWAGA

Jeśli włączone są obie zapory, program McAfee Personal Firewall nie pokazuje na karcie Zdarzenia przychodzące wszystkich zablokowanych adresów IP. Zapora systemu Windows przechwytuje i blokuje większość z tych zdarzeń, uniemożliwiając ich wykrycie i rejestrowanie przez program McAfee Personal Firewall. Program McAfee Personal Firewall może jednakże blokować dodatkowy ruch w oparciu o inne czynniki bezpieczeństwa i taki ruch będzie rejestrowany.

Rejestrowanie jest domyślnie wyłączone w Zaporze systemu Windows, ale jeśli użytkownik wybierze włączenie obu zapór, może również włączyć rejestrowanie w Zaporze systemu Windows. Domyślnym plikiem dziennika Zapory systemu Windows jest plik C:\Windows\pfirewall.log.

Aby być pewnym, że komputer jest chroniony przez co najmniej jedną zaporę, Zapora systemu Windows zostaje automatycznie włączona ponownie po odinstalowaniu programu McAfee Personal Firewall.

Jeśli użytkownik wyłączy program McAfee Personal Firewall lub ustawi ustawienie zabezpieczeń na poziomie **Otwarty** bez ręcznego włączenia Zapory systemu Windows, komputer zostanie pozbawiony całej ochrony z wyjątkiem wcześniej zablokowanych aplikacji.

Ustawianie poziomu zabezpieczeń

Istnieje możliwość skonfigurowania opcji zabezpieczeń określających sposób reagowania programu Personal Firewall w momencie wykrycia niepożądanego ruchu. Domyślnie włączony jest **Standardowy** poziom zabezpieczeń. W przypadku **Standardowego** poziomu zabezpieczeń zezwolenie aplikacji na dostęp do Internetu przydziela jej pełny dostęp. Pełny dostęp umożliwia aplikacji zarówno wysyłanie danych, jak również pozwala na odbieranie niepożądanych danych poprzez porty niesystemowe.

Aby skonfigurować ustawienia zabezpieczeń:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Opcje**.
2. Kliknij ikonę **Ustawienia zabezpieczeń**.
3. Ustaw poziom zabezpieczeń przesuwając suwak na żądany poziom.

   Możliwe jest ustawienie w zakresie od poziomu Blokowanie do poziomu Otwarty.

   - **Blokowanie -** Wszystkie połączenia komputera z Internetem są zamknięte. Ustawienie to można wykorzystać do zablokowania portów skonfigurowanych jako otwarte na stronie Usługi systemowe.

- **Wyższy poziom zabezpieczeń -** Gdy aplikacja żąda określonego typu dostępu do Internetu (na przykład dostępu tylko dla połączeń wychodzących), użytkownik może zezwolić lub zabronić aplikacji na takie połączenie. Później, jeśli aplikacja zażąda pełnego dostępu, można go jej przyznać lub ograniczyć tylko dla połączeń wychodzących.

- **Zabezpieczenia standardowe (zalecane) -** Gdy aplikacja zażąda i uzyska dostęp do Internetu, to uzyska dostęp pełny umożliwiający obsługę ruchu przychodzącego i wychodzącego.

- **Zabezpieczenia zaufania -** Podczas pierwszej próby uzyskania dostępu do Internetu wszystkie aplikacje są automatycznie traktowane jako zaufane. Można jednakże skonfigurować program Personal Firewall, aby za pomocą alertów użytkownik był powiadamiany o nowych aplikacjach w komputerze. Ustawienie to można wykorzystać w przypadku, gdy nie działają niektóre gry lub multimedia strumieniowe.

- **Otwarty -** Zapora jest wyłączona. Ustawienie to pozwala na przechodzenie całego ruchu internetowego przez program Personal Firewall bez filtrowania.

  UWAGA
  Zablokowane wcześniej aplikacje są dalej blokowane, kiedy zapora jest ustawiona w trybie zabezpieczeń **Otwarty** lub **Blokowanie**. Aby temu zapobiec, można zmienić uprawnienia aplikacji na **Zezwalaj na pełny dostęp** lub usunąć regułę **Zablokowane** z listy **Aplikacje internetowe**.

4 Wybierz dodatkowe ustawienia zabezpieczeń:

  UWAGA
  Jeśli na komputerze zainstalowany jest system operacyjny Windows XP i dodano wielu użytkowników systemu XP, opcje te będą dostępne wyłącznie po zalogowaniu jako administrator.

- **Rejestruj zdarzenia wykrywania włamań (IDS) w dzienniku zdarzeń przychodzących -** Po wybraniu tej opcji zdarzenia wykryte przez system IDS będą się pojawiały w dzienniku zdarzeń przychodzących. System wykrywania włamań wykrywa typowe rodzaje ataków oraz inne podejrzane działania. Funkcja wykrywania włamań monitoruje każdy przychodzący i wychodzący pakiet danych w poszukiwaniu podejrzanych transferów danych lub metod przesyłania. Są one porównywane z bazą „sygnatur” i pakiety pochodzące od atakującego komputera zostają automatycznie odrzucone.

  System IDS poszukuje określonych wzorców ruchu sieciowego stosowanego przez intruzów. System IDS sprawdza każdy pakiet przychodzący do komputera w celu wykrycia ruchu charakterystycznego dla podejrzanych lub znanych ataków. Na przykład, jeżeli program Personal Firewall napotka pakiety ICMP, analizuje je w poszukiwaniu podejrzanych wzorców ruchu sieciowego przez porównanie ruchu ICMP z wzorcami znanych ataków.

- **Akceptuj żądania ICMP ping** - Ruch ICMP służy głównie do badania adresów i wysyłania poleceń ping. Polecenie ping jest często używane do przeprowadzania szybkich testów przed próbą zainicjowania połączeń. Pakiety ping mogą być bardzo często wysyłane do komputera, na którym zainstalowano program typu P2P do udostępniania plików. Po wybraniu tej opcji program Personal Firewall będzie zezwalał na wszystkie żądania poleceń ping bez ich rejestrowania w dzienniku zdarzeń przychodzących. Jeśli opcja ta nie zostanie wybrana program Personal Firewall będzie blokował wszystkie żądania poleceń ping i będzie je rejestrował w dzienniku zdarzeń przychodzących.
- **Zezwalaj użytkownikom z ograniczeniami na zmianę ustawień programu Personal Firewall** - Jeżeli na komputerze zainstalowany jest system Windows XP lub Windows 2000 z wieloma użytkownikami, wybranie tej opcji pozwoli użytkownikom z ograniczeniami na modyfikowanie ustawień programu Personal Firewall.

5 Po zakończeniu wprowadzania zmian kliknij przycisk **OK**.

Testowanie programu McAfee Personal Firewall Plus

Istnieje możliwość przetestowania instalacji programu Personal Firewall pod kątem istnienia możliwych luk w zabezpieczeniach umożliwiających włamanie oraz podejrzane działanie.

Aby przetestować instalację programu Personal Firewall za pomocą ikony McAfee na pasku zadań:

- Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, a następnie wybierz polecenie **Testuj zaporę**.

Program Personal Firewall otworzy przeglądarkę Internet Explorer i przejdzie do obsługiwanej przez firmę McAfee witryny http://www.HackerWatch.org/. Aby przetestować program Personal Firewall, należy postępować zgodnie z poleceniami wyświetlanymi na stronie Probe (Sondowanie) witryny HackerWatch.org.

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 bezpłatnej analizy zabezpieczeń komputera;
- Uruchamianie, zarządzanie i konfiguracja 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 internetowej firmy McAfee.

> **UWAGA**
> Aby uzyskać więcej informacji na temat funkcji 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 (w obszarze powiadomień systemu Windows XP) zostanie wyświetlona czerwona ikona z literą M  . Jest to obszar zawierający zegar i 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 uruchomić program McAfee SecurityCenter:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee  , a następnie wybierz polecenie **Otwórz program SecurityCenter**.

Aby uruchomić program Personal Firewall z poziomu aplikacji McAfee SecurityCenter:

1. W programie SecurityCenter kliknij kartę **Personal Firewall Plus**.
2. Z menu Działanie wybierz właściwe zadanie.

Aby uruchomić program Personal Firewall z poziomu systemu Windows:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee  znajdującą się na pasku zadań systemu Windows, a następnie wskaż pozycję **Personal Firewall**.
2. Wybierz zadanie

Aby otworzyć program Personal Firewall:

- Kliknij prawym przyciskiem myszy ikonę programu McAfee  znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz zadanie.

Informacje o stronie Podsumowanie

Podsumowanie w programie Personal Firewall zawiera cztery strony podsumowania:

- Podsumowanie główne
- Podsumowanie aplikacji
- Podsumowanie zdarzeń
- Podsumowanie witryny HackerWatch

Na stronach podsumowania dostępne są różne raporty na temat ostatnich zdarzeń przychodzących, stanu aplikacji oraz raporty witryny HackerWatch.org dotyczące ogólnoświatowej aktywności w zakresie włamań. Znajdują się tu również łącza do typowych zadań wykonywanych w programie Personal Firewall.

Aby otworzyć stronę Podsumowanie główne w programie Personal Firewall:

- Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Wyświetl podsumowanie** (Ilustracja 3-1).

Ilustracja 3-1. Strona Podsumowanie główne

Aby przejść do innych stron podsumowania, należy kliknąć opisane poniżej elementy.

Pozycja	Opis
Zmień widok	Aby otworzyć listę ze stronami podsumowania, należy kliknąć łącze **Zmień widok**. Następnie należy wybrać z listy stronę podsumowania, która ma zostać wyświetlona.
 Strzałka w prawo	Aby wyświetlić następną stronę podsumowania, należy kliknąć ikonę strzałki w prawo,
 Strzałka w lewo	Aby wyświetlić poprzednią stronę podsumowania, należy kliknąć ikonę strzałki w lewo.
 Początek	Aby powrócić do strony **Podsumowanie główne**, należy kliknąć ikonę strony głównej (z rysunkiem domu).

Na stronie Podsumowanie główne można znaleźć następujące informacje.

Pozycja	Opis
Ustawienie zabezpieczeń	Stan ustawienia zabezpieczeń określa ustawiony poziom zabezpieczeń zapory. Po kliknięciu łącza można zmienić poziom zabezpieczeń.
Zablokowane zdarzenia	Stan zablokowanych zdarzeń wyświetla liczbę zdarzeń zablokowanych w bieżącym dniu. Po kliknięciu łącza wyświetlane są szczegóły zdarzenia ze strony Zdarzenia przychodzące.
Zmiany reguł aplikacji	Stan reguł aplikacji wyświetla liczbę zmienionych ostatnio reguł aplikacji. Kliknięcie łącza wyświetla listę aplikacji z przyznanym i zablokowanym dostępem oraz umożliwia modyfikację uprawnień aplikacji.
Nowości	Po kliknięciu łącza **Nowości** wyświetlana jest aplikacja, która jako ostatnia uzyskała prawo pełnego dostępu do Internetu.
Ostatnie zdarzenie	W sekcji **Ostatnie zdarzenie** są wyświetlane ostatnie zdarzenia przychodzące. Po kliknięciu łącza można przeprowadzić śledzenie zdarzenia lub umieścić adres IP na liście zaufanych adresów. Umieszczenie adresu IP na liście zaufanych adresów zezwoli na cały ruch z tego adresu IP do lokalnego komputera.
Raport dzienny	W sekcji **Raport dzienny** jest wyświetla liczba zablokowanych przez program Personal Firewall zdarzeń przychodzących w bieżącym dniu, tygodniu oraz miesiącu. Po kliknięciu łącza wyświetlane są szczegóły zdarzenia ze strony Zdarzenia przychodzące.
Aktywne aplikacje	W sekcji **Aktywne aplikacje** są wyświetlane aplikacje, które w danej chwili są uruchomione na komputerze i korzystają z połączenia z Internetem. Kliknięcie nazwy aplikacji pozwala wyświetlić adresy IP, z którymi dana aplikacja nawiązuje połączenia.
Typowe zadania	Kliknięcie łącza znajdującego się w sekcji **Typowe zadania** umożliwia przejście do stron programu Personal Firewall, na których można przeglądać działanie zapory i wykonywać zadania.

Aby wyświetlić stronę Podsumowanie aplikacji:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Wyświetl podsumowanie**.
2. Kliknij łącze **Zmień widok**, a następnie wybierz opcję **Podsumowanie aplikacji**.

Na stronie Podsumowanie aplikacji można znaleźć następujące informacje.

Pozycja	Opis
Monitor ruchu	W sekcji **Monitor ruchu** są wyświetlane przychodzące i wychodzące połączenia z Internetem nawiązane w ciągu ostatnich piętnastu minut. Aby wyświetlić szczegóły monitorowania ruchu, należy kliknąć wykres.
Aktywne aplikacje	W sekcji **Aktywne aplikacje** są wyświetlane informacje o wykorzystaniu przepustowości pasma przez najbardziej aktywne aplikacje na komputerze w ciągu ostatnich dwudziestu czterech godzin. **Aplikacja** - Aplikacja uzyskująca dostęp do Internetu. **%** - Procentowa wartość wykorzystania przepustowości pasma przez aplikację. **Uprawnienie** - Typ dostępu do Internetu dozwolony dla aplikacji. **Utworzona reguła** - Data utworzenia reguły dla aplikacji.
Nowości	Po kliknięciu łącza **Nowości** wyświetlana jest aplikacja, która jako ostatnia uzyskała prawo pełnego dostępu do Internetu.
Aktywne aplikacje	W sekcji **Aktywne aplikacje** są wyświetlane aplikacje, które w danej chwili są uruchomione na komputerze i korzystają z połączenia z Internetem. Kliknięcie nazwy aplikacji pozwala wyświetlić adresy IP, z którymi dana aplikacja nawiązuje połączenia.
Typowe zadania	Kliknięcie łącza znajdującego się w sekcji **Typowe zadania** umożliwia przejście do stron programu Personal Firewall, na których można przeglądać stan aplikacji i wykonywać związane z aplikacjami zadania.

Aby wyświetlić stronę Podsumowanie zdarzeń:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Wyświetl podsumowanie**.
2. Kliknij łącze **Zmień widok**, a następnie wybierz opcję **Podsumowanie zdarzeń**.

Na stronie Podsumowanie zdarzeń można znaleźć następujące informacje.

Pozycja	Opis
Porównanie portów	W sekcji **Porównanie portów** jest wyświetlany wykres kołowy najczęściej wykorzystywanych portów w komputerze w ciągu ostatnich 30 dni. Kliknięcie nazwy portu spowoduje wyświetlenie szczegółów ze strony Zdarzenia przychodzące. Umieszczenie wskaźnika myszy nad numerem portu spowoduje wyświetlenie opisu tego portu.
Najczęstsze ataki	W sekcji **Najczęstsze ataki** są wyświetlane najczęściej blokowane adresy IP, czas wystąpienia ostatniego zdarzenia przychodzącego dla każdego adresu oraz ogólna liczba zdarzeń przychodzących z ostatnich trzydziestu dni dla każdego adresu. Kliknięcie zdarzenia wyświetla jego szczegóły ze strony Zdarzenia przychodzące.
Raport dzienny	W sekcji **Raport dzienny** jest wyświetla liczba zablokowanych przez program Personal Firewall zdarzeń przychodzących w bieżącym dniu, tygodniu oraz miesiącu. Kliknięcie liczby wyświetla szczegóły zdarzenia z dziennika zdarzeń przychodzących.
Ostatnie zdarzenie	W sekcji **Ostatnie zdarzenie** są wyświetlane ostatnie zdarzenia przychodzące. Po kliknięciu łącza można przeprowadzić śledzenie zdarzenia lub umieścić adres IP na liście zaufanych adresów. Umieszczenie adresu IP na liście zaufanych adresów zezwoli na cały ruch z tego adresu IP do lokalnego komputera.
Typowe zadania	Kliknięcie łącza znajdującego się w sekcji **Typowe zadania** umożliwia przejście do stron programu Personal Firewall, na których można przeglądać szczegóły zdarzeń i wykonywać związane ze zdarzeniami zadania.

Aby wyświetlić stronę Podsumowanie witryny HackerWatch:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Wyświetl podsumowanie**.
2. Kliknij łącze **Zmień widok**, a następnie wybierz opcję **HackerWatch**.

Na stronie Podsumowanie witryny HackerWatch można znaleźć następujące informacje**.**

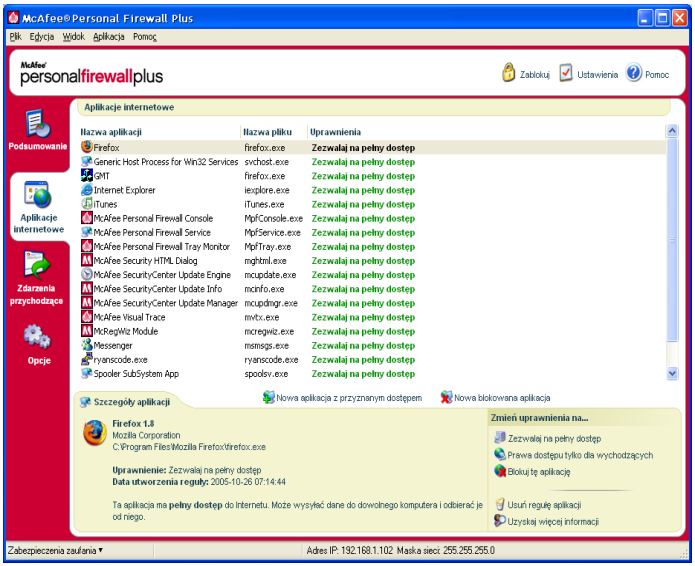
Pozycja	Opis
Globalna aktywność	W sekcji **Globalna aktywność** wyświetlana jest mapa świata z zaznaczoną ostatnio zablokowaną działalnością monitorowaną przez witrynę HackerWatch.org. Kliknij mapę, aby otworzyć mapę analizy zagrożeń globalnych w witrynie HackerWatch.org.
Śledzenie zdarzeń	W sekcji **Śledzenie zdarzeń** jest wyświetla liczba zdarzeń przychodzących przesłanych do witryny HackerWatch.org.
Globalna aktywność portów	W sekcji **Globalna aktywność portów** są wyświetlane najczęściej atakowane porty w ciągu ostatnich pięciu dni (potencjalne zagrożenia). Kliknięcie portu wyświetla jego numer i opis.
Typowe zadania	Kliknięcie łącza znajdującego się w sekcji **Typowe zadania** umożliwia przejście do stron witryny HackerWatch.org, gdzie można uzyskać informacje na temat aktywności hakerów na całym świecie.

Informacje o stronie Aplikacje internetowe

Strona Aplikacje internetowe umożliwia wyświetlanie listy aplikacji z przyznanym oraz zablokowanym dostępem.

Aby otworzyć stronę Aplikacje internetowe:

- Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Aplikacje** (Ilustracja 3-2).



Ilustracja 3-2. Strona Aplikacje internetowe

Strona Aplikacje internetowe zawiera następujące informacje:

- Nazwy aplikacji
- Nazwy plików
- Bieżące poziomy uprawnień
- Szczegóły aplikacji: nazwa i wersja aplikacji, nazwa firmy, ścieżka dostępu do aplikacji, poziom uprawnień aplikacji, znaczniki czasowe oraz objaśnienia poszczególnych typów uprawnień.

Zmiana reguł aplikacji

Program Personal Firewall umożliwia zmienianie reguł dostępu aplikacji.

Aby zmienić regułę aplikacji:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż opcję **Personal Firewall**, a następnie wybierz polecenie **Aplikacje internetowe**.
2. Na liście **Aplikacje internetowe** prawym przyciskiem myszy kliknij regułę aplikacji i wybierz inny poziom:
   - **Zezwalaj na pełny dostęp -** Pozwala aplikacji na ustanawianie wychodzących i przychodzących połączeń z Internetem.
   - **Prawa dostępu tylko dla wychodzących -** Pozwala aplikacji na ustanawianie wyłącznie wychodzących połączeń z Internetem.
   - **Blokuj tę aplikację -** Blokuje aplikacji dostęp do Internetu.

     UWAGA
     Zablokowane wcześniej aplikacje są dalej blokowane, kiedy dla zapory ustawiono poziom zabezpieczeń **Otwarty** lub **Blokowanie**. Aby temu zapobiec, można zmienić regułę dostępu tej aplikacji na **Zezwalaj na pełny dostęp** lub usunąć regułę **Zablokowane** z listy **Aplikacje internetowe**.

Aby usunąć regułę aplikacji:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Aplikacje internetowe**.
2. Na liście **Aplikacje internetowe** prawym przyciskiem myszy kliknij regułę aplikacji i wybierz polecenie **Usuń regułę aplikacji**.

Następnym razem, gdy aplikacja zażąda dostępu do Internetu, będzie można ponownie ustawić jej poziom uprawnień w celu dodania jej do listy.

Przyznawanie dostępu i blokowanie aplikacji internetowych

Aby zmienić listę aplikacji internetowych z przyznanym dostępem i zablokowanych:

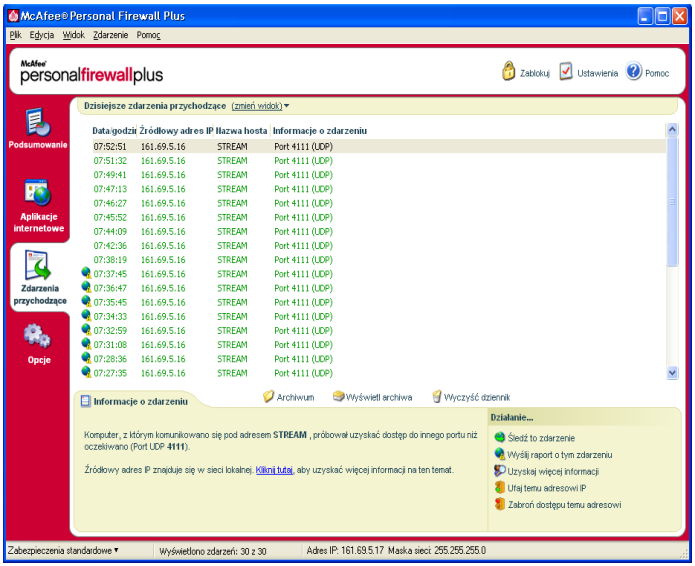
1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Aplikacje internetowe**.
2. Na stronie Aplikacje internetowe kliknij jedną z następujących opcji:
   - **Nowa aplikacja z przyznanym dostępem** - Zezwala aplikacji na pełny dostęp do Internetu.
   - **Nowa blokowana aplikacja** - Blokuje aplikacji dostęp do Internetu.
   - **Usuń regułę aplikacji** - Usuwa regułę aplikacji.

Informacje o stronie Zdarzenia przychodzące

Strona Zdarzenia przychodzące służy do wyświetlania dziennika zdarzeń przychodzących generowanego w momencie blokowania przez program Personal Firewall niepożądanych połączeń internetowych.

Aby otworzyć stronę Zdarzenia przychodzące:

- Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące** (Ilustracja 3-3).



Ilustracja 3-3. Strona Zdarzenia przychodzące

Na stronie Zdarzenia przychodzące znajdują się następujące informacje:

- Znaczniki czasu
- ródłowe adresy IP
- Nazwy hostów
- Nazwy usług lub aplikacji
- Szczegóły zdarzenia: typy połączenia, porty połączenia, nazwa lub adres IP hosta oraz wyjaśnienia zdarzeń występujących na tych portach.

Omówienie zdarzeń

Informacje o adresach IP

Adresy IP składają się z czterech liczb, każda z zakresu od 0 do 255. Liczby te identyfikują określone miejsce w Internecie, do którego można skierować ruch sieciowy.

Typy adresów IP

Pewna liczba adresów IP traktowana jest inaczej z różnych przyczyn:

Nierutowalne adresy IP - znane również jako „prywatna przestrzeń adresowa IP". Te adresy IP nie mogą być używane w Internecie. Prywatne bloki IP to 10.x.x.x, 172.16.x.x- 172.31.x.x oraz 192.168.x.x.

Pętlowe adresy IP - wykorzystywane są w celach testowych. Ruch sieciowy wysłany do takiego bloku adresów IP wraca do urządzenia, które wygenerowało pakiet. Nigdy nie opuszcza tego urządzenia i przeważnie służy do testowania sprzętu i oprogramowania. Pętlowy blok IP to 127.x.x.x.

Pusty adres IP - jest to adres nieprawidłowy. Jego wykrycie przez program Personal Firewall oznacza, że ruch sieciowy użył pustego adresu IP. Często oznacza to, że nadawca celowo ukrywa źródło ruchu. Nadawca nie będzie w stanie odebrać żadnych odpowiedzi na generowany ruch sieciowy, chyba że pakiet zostanie odebrany przez aplikację, która zrozumie zawartość tego pakietu zawierającą instrukcje specyficzne dla tej aplikacji. Wszystkie adresy rozpoczynające się liczbą 0 (0.x.x.x) są adresami pustymi. Na przykład 0.0.0.0 jest pustym adresem IP.

Zdarzenia z adresu 0.0.0.0

Występowanie zdarzeń pochodzących z adresu IP 0.0.0.0 ma zazwyczaj dwie przyczyny. Pierwszą, a zarazem najczęstszą, jest otrzymanie przez komputer nieprawidłowo skonstruowanego pakietu. Internet nie jest zawsze w 100% niezawodny i możliwe jest występowanie błędnych pakietów. Program Personal Firewall przechwytuje pakiety zanim protokół TCP/IP może je sprawdzić, więc pakiety takie mogą być raportowane jako zdarzenie.

Inna sytuacja ma miejsce, gdy źródłowy adres IP jest fałszywy lub ktoś się pod niego podszywa. Występowanie pakietów podszywających się może być znakiem, że ktoś przeprowadza skanowanie komputera w poszukiwaniu koni trojańskich. Program Personal Firewall blokuje tego typu działania, więc komputer pozostaje bezpieczny.

Zdarzenia z adresu 127.0.0.1

Czasami zdarzenia mają źródłowy adres IP 127.0.0.1. Jest on nazywany adresem pętlowym lub hostem lokalnym.

Wiele normalnych programów wykorzystuje adres pętlowy do komunikowania się ze swoimi składnikami. Na przykład, wiele osobistych serwerów poczty e-mail lub WWW można skonfigurować poprzez interfejs sieci Web. Aby uzyskać do nich dostęp, należy wpisać „http://localhost/" w przeglądarce sieci Web.

Jednakże program Personal Firewall pozwala na ruch z tych programów, jeśli więc pojawiają się zdarzenia spod adresu 127.0.0.1, najprawdopodobniej taki źródłowy adres IP jest fałszywy lub ktoś się pod niego podszywa. Występowanie pakietów podszywających się oznacza zazwyczaj, że inny komputer przeprowadza skanowanie w poszukiwaniu koni trojańskich. Program Personal Firewall blokuje próby włamań tego typu, więc komputer pozostaje bezpieczny.

Niektóre programy, a zwłaszcza Netscape w wersji 6.2 i nowszej, wymagają dodania adresu 127.0.0.1 do listy zaufanych adresów IP. Składniki tego programu komunikują się ze sobą w taki sposób, że Personal Firewall nie może określić, czy ma do czynienia z ruchem lokalnym czy nie.

Biorąc dalej jako przykład program Netscape 6.2, jeśli adres 127.0.0.1 nie zostanie dodany do listy zaufanych adresów, nie będzie możliwe korzystanie z listy znajomych. Dlatego jeśli w dzienniku pojawi się ruch z adresu 127.0.0.1, a wszystkie aplikacje w komputerze działają normalnie, to ruch ten można bezpiecznie zablokować. Jednakże jeśli jakiś program (np. Netscape) działa niestabilnie, należy dodać adres 127.0.0.1 do listy zaufanych adresów IP programu Personal Firewall.

Jeśli dodanie adresu 127.0.0.1 do listy zaufanych adresów IP usunęło problem, należy rozważyć związane z tym kwestie. jeśli użytkownik doda adres 127.0.0.1 do listy zaufanych, program będzie działał, ale zwiększy się niebezpieczeństwo wystąpienia ataków z wykorzystaniem podszywania się. Jeśli użytkownik nie doda adresu do listy zaufanych, jego program nie będzie działał, ale komputer pozostanie chroniony przed takim złośliwym ruchem sieciowym.

Zdarzenia pochodzące z komputerów w sieci LAN

Zdarzenia mogą być generowane przez komputery w sieci lokalnej (LAN) użytkownika. Aby pokazać, że zdarzenia te są generowane przez sieć, program Personal Firewall wyświetla je w kolorze zielonym.

W przypadku ustawień większości firmowych sieci LAN powinno zostać wybrane ustawienie **Ufaj wszystkim komputerom w sieci LAN** w opcjach Zaufane adresy IP.

W niektórych sytuacjach sieć lokalna może być tak samo niebezpieczna jak Internet. Szczególnie w przypadku, gdy komputer pracuje w szerokopasmowej sieci wykorzystującej modem DSL lub kablowy. W takim przypadku nie należy wybierać opcji **Ufaj wszystkim komputerom w sieci LAN**. Zamiast tego należy dodać adresy IP komputerów lokalnych do listy zaufanych adresów IP.

Zdarzenia pochodzące z prywatnych adresów IP

Adresy IP w formacie 192.168.xxx.xxx, 10.xxx.xxx.xxx oraz 172.16.0.0- 172.31.255.255 są tak zwanymi nierutowalnymi lub prywatnymi adresami IP. Adresy te nie powinny nigdy opuścić lokalnej sieci i w większości przypadków można im zaufać.

Blok 192.168.xxx.xxx jest wykorzystywany przez usługę udostępniania połączenia internetowego (ICS) firmy Microsoft. Jeśli w przypadku korzystania z usługi ICS w dzienniku znajdują się zdarzenia z tego bloku IP, to adres IP 192.168.255.255 można dodać do listy zaufanych adresów IP. Spowoduje to przyznanie zaufania do całego bloku 192.168.xxx.xxx.

Jeśli użytkownik nie korzysta z sieci prywatnej, a zdarzenia z tych zakresów adresów IP pojawiają się w dzienniku, wówczas źródłowy adres IP może być fałszywy lub ktoś się pod niego podszywa. Występowanie pakietów podszywających się jest zazwyczaj znakiem, że ktoś przeprowadza skanowanie w poszukiwaniu koni trojańskich. Należy pamiętać o istotnym fakcie, że taka próba została zablokowana przez program Personal Firewall, więc komputer pozostaje bezpieczny.

W związku z tym, że prywatne adresy IP odnoszą się do różnych komputerów w zależności od sieci, w której pracuje komputer użytkownika, zgłaszanie tego typu zdarzeń nie przyniesie żadnych rezultatów, tak więc nie jest to konieczne.

Wyświetlanie zdarzeń w dzienniku zdarzeń przychodzących

Dziennik zdarzeń przychodzących wyświetla zdarzenia na różne sposoby. Domyślny widok wyświetla zdarzenia tylko z bieżącego dnia. Można również wyświetlić zdarzenia z ostatniego tygodnia lub wyświetlić cały dziennik.

Program Personal Firewall pozwala również na wyświetlenie zdarzeń przychodzących z określonych dni, określonych adresów internetowych (adresów IP) lub zdarzeń zawierających identyczne informacje.

Aby uzyskać informacje o zdarzeniu, należy kliknąć to zdarzenie, a informacje pojawią się w okienku **Informacje o zdarzeniu**.

Wyświetlanie zdarzeń z bieżącego dnia

Ta opcja służy do przeglądania zdarzeń z bieżącego dnia.

Aby wyświetlić zdarzenia z bieżącego dnia:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. W dzienniku zdarzeń przychodzących kliknij wpis prawym przyciskiem myszy, a następnie kliknij polecenie **Pokaż dzisiejsze zdarzenia**.

Wyświetlanie zdarzeń z bieżącego tygodnia

Ta opcja służy do przeglądania zdarzeń tygodniowych.

Aby wyświetlić zdarzenia z bieżącego tygodnia:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. W dzienniku zdarzeń przychodzących kliknij wpis prawym przyciskiem myszy, a następnie kliknij polecenie **Pokaż zdarzenia z tego tygodnia**.

Wyświetlanie całego dziennika zdarzeń przychodzących

Ta opcja służy do przeglądania wszystkich zdarzeń.

Aby wyświetlić wszystkie zdarzenia z dziennika zdarzeń przychodzących:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż opcję **Personal Firewall**, a następnie kliknij polecenie **Zdarzenia przychodzące**.
2. W dzienniku zdarzeń przychodzących kliknij wpis prawym przyciskiem myszy, a następnie kliknij polecenie **Pokaż cały dziennik**.

   Wyświetlone zostaną wszystkie zdarzenia z dziennika zdarzeń przychodzących.

Wyświetlanie zdarzeń z określonego dnia

Ta opcja służy do przeglądania zdarzeń z określonego dnia.

Aby pokazać zdarzenia z wybranego dnia:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. W dzienniku zdarzeń przychodzących kliknij wpis prawym przyciskiem myszy, a następnie kliknij polecenie **Pokaż tylko zdarzenia z tego dnia**.

Wyświetlanie zdarzeń z określonego adresu Internetowego

Opcja ta służy do przeglądania innych zdarzeń pochodzących z określonego adresu internetowego.

Aby pokazać zdarzenia dla adresu internetowego:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie kliknij polecenie **Zdarzenia przychodzące**.
2. W dzienniku zdarzeń przychodzących kliknij wpis prawym przyciskiem myszy, a następnie kliknij polecenie **Pokaż tylko zdarzenia dla wybranego adresu internetowego**.

Wyświetlanie zdarzeń zawierających identyczne informacje o zdarzeniu

Opcja ta służy do przeglądania innych zdarzeń w dzienniku zdarzeń przychodzących, które w kolumnie Informacje o zdarzeniu zawierają takie same informacje jak wybrane zdarzenie. W ten sposób można uzyskać informacje o liczbie wystąpień tego zdarzenia oraz czy pochodzi ono z tego samego źródła. W kolumnie Informacje o zdarzeniu znajduje się opis zdarzenia oraz, jeśli jest znany, typowy program lub usługa korzystająca z tego portu.

Aby pokazać zdarzenia zawierające identyczne informacje o zdarzeniu:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie kliknij polecenie **Zdarzenia przychodzące**.
2. W dzienniku zdarzeń przychodzących kliknij wpis prawym przyciskiem myszy, a następnie kliknij polecenie **Pokaż tylko zdarzenia z tymi samymi informacjami o zdarzeniu**.

Reagowanie na zdarzenia przychodzące

Poza przeglądaniem szczegółowych informacji o zdarzeniach w dzienniku zdarzeń przychodzących użytkownik może przeprowadzić wizualne śledzenie adresów IP zdarzenia z dziennika zdarzeń przychodzących lub uzyskać szczegółowe informacje na temat tego zdarzenia w witrynie ochrony przed włamaniami społeczności online HackerWatch.org.

Śledzenie wybranego zdarzenia

Dla zdarzenia znajdującego się w dzienniku zdarzeń przychodzących można spróbować przeprowadzić wizualne śledzenie za pomocą aplikacji Visual Trace.

Aby prześledzić wybrane zdarzenie:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. W dzienniku zdarzeń przychodzących kliknij prawym przyciskiem myszy zdarzenie, które ma być śledzone, a następnie kliknij polecenie **Śledź wybrane zdarzenie**. Można również rozpocząć śledzenie, klikając zdarzenie dwukrotnie.

Program Personal Firewall domyślnie rozpoczyna wizualne śledzenie przy użyciu zintegrowanego programu Personal Firewall Visual Trace.

Uzyskiwanie porad z witryny HackerWatch.org

Aby uzyskać poradę z witryny HackerWatch.org:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż opcję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. Na stronie Zdarzenia przychodzące wybierz wpis zdarzenia, a następnie w panelu **Działanie** kliknij łącze **Uzyskaj więcej informacji**.

Zostanie uruchomiona domyślna przeglądarka sieci Web i otworzy się witryna HackerWatch.org, z której można pobrać informacje na temat danego typu zdarzenia oraz uzyskać poradę dotyczącą jego raportowania.

Raportowanie zdarzenia

Aby wysłać raport na temat zdarzenia, które mogło być atakiem na komputer:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. Kliknij zdarzenie, o którym raport ma zostać wysłany, a następnie w panelu **Działanie** kliknij łącze **Wyślij raport o tym zdarzeniu**.

Program Personal Firewall wyśle raport o zdarzeniu do witryny HackerWatch.org, używając unikatowego identyfikatora użytkownika.

Rejestrowanie się w witrynie HackerWatch.org

Po pierwszym otwarciu strony Podsumowanie program Personal Firewall skontaktuje się z witryną HackerWatch.org w celu wygenerowania unikatowego identyfikatora użytkownika. Jeśli użytkownik będzie już zarejestrowany, jego dane rejestracyjne zostaną sprawdzone automatycznie. W przypadku nowego użytkownika w celu korzystania z funkcji filtrowania/przesyłania pocztą e-mail zdarzeń do witryny HackerWatch.org należy podać przydomek oraz adres e-mail, a następnie kliknąć na sprawdzające łącze znajdujące się w potwierdzającej wiadomości e-mail przesłanej z tej witryny.

Zdarzenia można zgłaszać w witrynie HackerWatch.org z pominięciem etapu sprawdzania identyfikatora użytkownika. Rejestracja jest jednak wymagana, aby można było filtrować i przesyłać zdarzenia pocztą elektroniczną do znajomych.

Zarejestrowanie się w tej usłudze pozwala na śledzenie zgłoszeń oraz na powiadamianie użytkownika w przypadku, gdy witryna HackerWatch.org będzie potrzebowała więcej informacji lub dalszych działań ze strony użytkownika. Aby jakakolwiek uzyskana informacja była użyteczna, musi istnieć możliwość jej potwierdzenia, co zapewnia wymagana rejestracja użytkowników.

Wszystkie adresy e-mail przekazane do witryny HackerWatch.org są przechowywane jako dane poufne. Jeśli dostawca usług internetowych żąda dodatkowych informacji, żądanie takie jest kierowane do witryny HackerWatch.org; adres e-mail użytkownika nigdy nie jest ujawniany.

Ufanie adresowi

Aby dodać adres IP do listy zaufanych adresów IP i umożliwić trwałe połączenie, można skorzystać ze strony Zdarzenia przychodzące.

Jeśli na stronie Zdarzenia przychodzące znajduje się zdarzenie zawierające adres IP, z którego dostęp ma być dozwolony, program Personal Firewall można skonfigurować tak, aby zawsze zezwalał na połączenia z tego adresu.

Aby dodać adres IP do listy zaufanych adresów IP:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. Kliknij prawym przyciskiem myszy zdarzenie, którego adres IP ma zostać dodany do adresów zaufanych, a następnie kliknij polecenie **Ufaj źródłowemu adresowi IP**.

Sprawdź, czy adres IP wyświetlany w oknie dialogowym Ufaj temu adresowi IP jest poprawny, a następnie kliknij przycisk **OK**. Adres IP zostanie dodany do listy Zaufane adresy IP.

Aby sprawdzić, czy adres IP został dodany:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Opcje**.
2. Kliknij ikonę **Zaufane i zabronione adresy IP**, a następnie kliknij kartę **Zaufane adresy IP**.

Adres IP pojawi się jako zaznaczony na liście Zaufane adresy IP.

Zabranianie dostępu adresowi

Jeśli w dzienniku zdarzeń przychodzących pojawia się adres IP oznacza to, że ruch z tego adresu został zablokowany. Zabronienie dostępu do adresu nie daje zatem dodatkowej ochrony, chyba że za pomocą usług systemowych celowo pozostawiono otwarte porty lub na komputerze uruchomiona jest aplikacja mająca uprawnienie do odbierania ruchu.

Dodanie adresu IP do listy zabronionych adresów jest uzasadnione tylko wówczas, gdy co najmniej jeden port pozostaje celowo otwarty, oraz jeśli istnieją powody, aby uważać, że dostęp do otwartych portów z tego adresu musi być zablokowany.

Jeśli na stronie Zdarzenia przychodzące znajduje się zdarzenie zawierające adres IP, który ma być zabroniony, program Personal Firewall można skonfigurować tak, aby nigdy nie zezwalał na połączenia z tego adresu.

Aby zabronić dostępu do adresu IP, co do którego istnieje przypuszczenie, że jest źródłem podejrzanej lub niepożądanej aktywności internetowej, można skorzystać ze strony Zdarzenia przychodzące zawierającej listę adresów IP całego przychodzącego ruchu internetowego.

Aby dodać adres IP do listy zabronionych adresów IP:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. Na stronie Zdarzenia przychodzące znajduje się lista adresów IP dla całego przychodzącego ruchu internetowego. Wybierz adres IP, a następnie wykonaj jedną z poniższych czynności:
   - Kliknij prawym przyciskiem myszy adres IP, a następnie wybierz polecenie **Zabroń dostępu źródłowemu adresowi IP**.
   - W menu **Działanie** kliknij polecenie **Zabroń dostępu temu adresowi**.
3. W oknie dialogowym Dodaj regułę zabronionego adresu IP zastosuj co najmniej jedno z następujących ustawień, aby skonfigurować regułę zabronionego adresu IP:
   - **Pojedynczy adres IP**: Adres IP, do którego dostęp ma zostać zabroniony. Domyślnie jest to adres IP wybrany ze strony Zdarzenia przychodzące.
   - **Zakres adresów IP**: Adresy IP zawarte między adresem określonym w polu Od adresu IP, a adresem IP określonym w polu Do adresu IP.
   - **Niech ta reguła wygasa**: Data i godzina, o której wygaśnie reguła zabronionego adresu IP. Wybierz datę i godzinę z odpowiedniego menu rozwijanego.
   - **Opis**: Opcjonalnie opisuje nową regułę.
   - Kliknij przycisk **OK**.
4. W oknie dialogowym kliknij przycisk **Tak**, aby potwierdzić ustawienie. Kliknij przycisk **Nie**, aby powrócić do okna dialogowego Dodaj regułę zabronionego adresu IP.

Jeśli program Personal Firewall wykryje zdarzenie z zabronionego połączenia internetowego, zostanie wyświetlony alert zgodnie z metodą określoną na stronie Ustawienia alertu.

Aby sprawdzić, czy adres IP został dodany:

1. Kliknij kartę **Opcje**.
2. Kliknij ikonę **Zaufane i zabronione adresy IP**, a następnie kartę **Zabronione adresy IP**.

Adres IP pojawi się jako zaznaczony na liście Zabronione adresy IP.

Zarządzanie dziennikiem zdarzeń przychodzących

Strona Zdarzenia przychodzące umożliwia zarządzanie zdarzeniami w dzienniku zdarzeń przychodzących generowanymi w momencie blokowania przez program Personal Firewall niepożądanego ruchu internetowego.

Archiwizowanie dziennika zdarzeń przychodzących

Dziennik zdarzeń przychodzących można zarchiwizować, aby zapisać wszystkie rejestrowane zdarzenia, łącznie z ich datą i godziną, źródłowymi adresami IP, nazwami hostów, portów i informacjami o zdarzeniu. Aby zapobiec nadmiernemu powiększaniu się dziennika zdarzeń przychodzących, zaleca się jego okresowe archiwizowanie.

Aby zarchiwizować dziennik zdarzeń przychodzących:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. Na stronie Zdarzenia przychodzące kliknij łącze **Archiwizuj**.
3. W oknie dialogowym Archiwizuj dziennik kliknij przycisk **Tak**, aby kontynuować operację.
4. Kliknij przycisk **Zapisz**, aby zapisać archiwum w domyślnej lokalizacji lub wybierz lokalizację do zapisania archiwum.

Uwaga: Domyślnie program Personal Firewall automatycznie tworzy archiwum dziennika zdarzeń przychodzących. Zaznacz lub usuń zaznaczenie pola wyboru **Automatycznie archiwizuj rejestrowane zdarzenia** znajdujące się na stronie Ustawienia dziennika zdarzeń, aby włączyć lub wyłączyć tę opcję.

Przeglądanie zarchiwizowanego dziennika zdarzeń przychodzących

Można wyświetlać wszystkie wcześniej zarchiwizowane dzienniki zdarzeń przychodzących. Zapisane archiwum zawiera datę i godzinę, źródłowe adresy IP, nazwy hostów, porty i informacje o zdarzeniu.

Aby wyświetlić zarchiwizowany dziennik zdarzeń przychodzących:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. Na stronie Zdarzenia przychodzące kliknij łącze **Wyświetl archiwa**.
3. Wybierz lub znajdź nazwę pliku archiwum i kliknij przycisk **Otwórz**.

Czyszczenie dziennika zdarzeń przychodzących

Można wyczyścić wszystkie informacje znajdujące się w dzienniku zdarzeń przychodzących.

OSTRZEŻENIE
Po wyczyszczeniu dziennika zdarzeń przychodzących nie ma możliwości odtworzenia jego zawartości. Jeśli dziennik zdarzeń ma być wykorzystywany w przyszłości, powinien zostać zarchiwizowany.

Aby wyczyścić dziennik zdarzeń przychodzących:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż opcję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. Na stronie Zdarzenia przychodzące kliknij opcję **Wyczyść dziennik**.
3. Kliknij przycisk **Tak** w oknie dialogowym, aby wyczyścić dziennik.

Kopiowanie zdarzenia do schowka

Zdarzenie można skopiować do schowka w celu wklejenia go do pliku tekstowego za pomocą Notatnika.

Aby skopiować zdarzenia do schowka:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż opcję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. Prawym przyciskiem myszy kliknij zdarzenie z dziennika zdarzeń przychodzących.
3. Kliknij polecenie **Kopiuj wybrane zdarzenie do schowka**.
4. Uruchom program Notatnik.
   - Wpisz tekst `notepad` w wierszu polecenia lub kliknij przycisk **Start** systemu Windows, wskaż polecenie **Programy**, a potem polecenie **Akcesoria**. Następnie wybierz polecenie **Notatnik**.
5. Kliknij menu **Edycja**, a następnie polecenie Wklej. Tekst zdarzenia pojawi się w Notatniku. Powtarzaj tę czynność, aż do skopiowania wszystkich koniecznych zdarzeń.
6. Zapisz plik Notatnika w bezpiecznym miejscu.

Usuwanie wybranego zdarzenia

Istnieje możliwość usuwania zdarzeń z dziennika zdarzeń przychodzących.

Aby usunąć zdarzenia z dziennika zdarzeń przychodzących:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. Na stronie Zdarzenia przychodzące kliknij wpis zdarzenia, które chcesz usunąć.
3. W menu Edycja kliknij polecenie **Usuń wybrane zdarzenie**. Zdarzenie zostanie usunięte z dziennika zdarzeń przychodzących.

Informacje o alertach

Stanowczo zaleca się zaznajomienie z rodzajami alertów występującymi w trakcie korzystania z programu Personal Firewall. Przejrzenie poniższych rodzajów alertów oraz możliwych reakcji na nie umożliwi użytkownikowi świadome reagowanie na wyświetlony alert.

UWAGA
Zalecenia zawarte w alertach pomagają w podjęciu decyzji dotyczącej sposobu obsługi zdarzenia wywołującego alert. W celu wyświetlania zaleceń w alertach kliknij kartę **Opcje**, kliknij ikonę **Ustawienia alertów**, a następnie z listy **Inteligentne zalecenia** wybierz opcję **Użyj inteligentnych zaleceń**(domyślnie) lub **Wyświetlaj tylko inteligentne zalecenia**.

Alerty czerwone

Alerty czerwone zawierają ważne informacje wymagające natychmiastowej uwagi:

- **Zablokowano aplikację internetową** - Ten alert jest wyświetlany, gdy program Personal Firewall zablokuje aplikacji dostęp do Internetu. Na przykład, jeśli wyświetlony zostanie alert o programie będącym koniem trojańskim, zapora McAfee automatycznie odmówi temu programowi dostępu do Internetu i zaleci przeskanowanie komputera w poszukiwaniu wirusów.
- **Aplikacja żąda dostępu do Internetu -** Alert ten jest wyświetlany, gdy program Personal Firewall wykryje ruch internetowy lub sieciowy wywołany przez nową aplikację.
- **Zmodyfikowano aplikację -** Ten alert zostaje wyświetlony w przypadku, gdy program Personal Firewall wykryje, że aplikacja, której wcześniej zezwolono na dostęp do Internetu, zmieniła się. Jeśli dana aplikacja nie była ostatnio uaktualniana, należy zachować ostrożność w przyznawaniu takiej zmodyfikowanej aplikacji uprawnień dostępu do Internetu.

- **Aplikacja żąda dostępu w roli serwera -** Ten alert zostaje wyświetlony, gdy program Personal Firewall wykryje, że aplikacja, której wcześniej zezwolono na dostęp do Internetu, zażądała dostępu do Internetu w roli serwera.

  UWAGA
  W systemie operacyjnym Windows XP SP2 domyślne ustawienie aktualizacji automatycznych powoduje pobieranie i instalowanie aktualizacji systemu operacyjnego Windows oraz innych uruchomionych na komputerze programów firmy Microsoft bez powiadamiania użytkownika. Jeśli aplikacja została zmodyfikowana w wyniku jednej z takich cichych aktualizacji systemu Windows, to program McAfee Personal Firewall wyświetli alert przy następnym uruchomieniu takiej aplikacji firmy Microsoft.

  WAŻNE
  Aplikacjom wymagającym dostępu do Internetu w celu aktualizacji produktu w trybie online (na przykład usługom firmy McAfee) należy przyznać odpowiednie uprawnienia dostępu.

Alert Zablokowano aplikację internetową

Jeśli wyświetlony zostanie alert o programie będącym koniem trojańskim (Ilustracja 3-4), program Personal Firewall automatycznie odmówi temu programowi dostępu do Internetu i zaleci przeskanowanie komputera w poszukiwaniu wirusów. Jeśli program McAfee VirusScan nie został zainstalowany, można uruchomić program McAfee SecurityCenter.

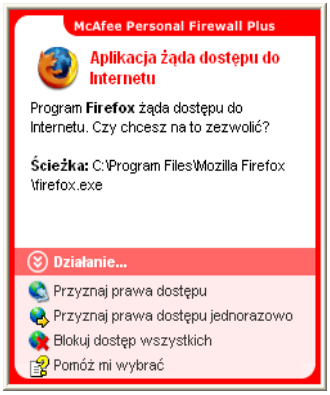
Ilustracja 3-4. Alert Zablokowano aplikację internetową

Należy zapoznać się z krótkim opisem tego zdarzenia, a następnie wybrać jedną z następujących opcji:

- Kliknij polecenie **Dowiedz się więcej** w celu uzyskania szczegółowych informacji o zdarzeniu za pośrednictwem dziennika zdarzeń przychodzących (aby uzyskać więcej informacji, patrz *Informacje o stronie Zdarzenia przychodzące* na str. 65).
- Kliknij przycisk **Uruchom program McAfee VirusScan**, aby przeskanować komputer w poszukiwaniu wirusów.
- Kliknij przycisk **Kontynuuj wykonywaną czynność**, jeśli nie chcesz podejmować dalszych działań poza tymi, które zostały już podjęte przez program Personal Firewall.
- Kliknij przycisk **Przyznaj prawa dostępu dla wychodzących**, aby zezwolić na połączenie wychodzące (**Wyższy** poziom zabezpieczeń).

Alert Aplikacja żąda dostępu do Internetu

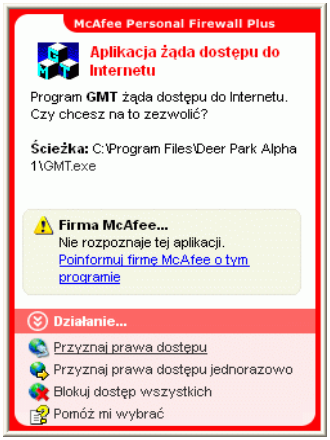
Jeśli w opcjach Ustawienia zabezpieczeń wybrano poziom zabezpieczeń **Standardowy** lub **Wysoki**, program Personal Firewall wyświetli alert (Ilustracja 3-5) w momencie wykrycia połączeń internetowych lub sieciowych dla nowych lub zmodyfikowanych aplikacji.



Ilustracja 3-5. Alert Aplikacja żąda dostępu do Internetu

Po wyświetleniu alertu zalecającego zachowanie ostrożności przed przyznaniem aplikacji dostępu do Internetu użytkownik może uzyskać dodatkowe informacje o tej aplikacji, klikając łącze **Kliknij tutaj, aby dowiedzieć się więcej**. Opcja ta pojawi się w alercie tylko wówczas, gdy program Personal Firewall zostanie skonfigurowany do korzystania z funkcji Inteligentne zalecenia.

Zapora McAfee może nie rozpoznać aplikacji próbującej uzyskać dostęp do Internetu (Ilustracja 3-6).



Ilustracja 3-6. Alert Nierozpoznana aplikacja

Z tego powodu zapora McAfee nie może podać zalecanego sposobu postępowania z daną aplikacją. Do firmy McAfee można wysłać raport na temat tej aplikacji, klikając łącze **Poinformuj firmę McAfee o tym programie**. Spowoduje to wyświetlenie strony sieci Web umożliwiającej podanie informacji związanych z aplikacją. Należy wprowadzić jak najwięcej znanych informacji.

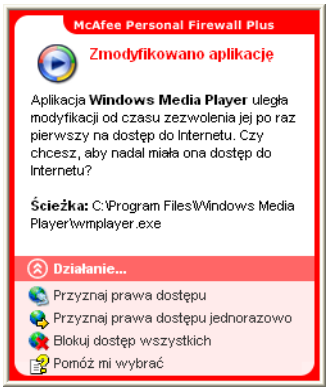
Przesyłane informacje w połączeniu z innymi narzędziami badawczymi są używane przez operatorów HackerWatch do określenia, czy aplikacja powinna zostać umieszczona w bazie danych znanych aplikacji, a jeśli tak, to w jaki sposób ma być traktowana przez program Personal Firewall.

Należy zapoznać się z krótkim opisem tego zdarzenia, a następnie wybrać jedną z następujących opcji:

- Kliknij przycisk **Przyznaj prawa dostępu**, aby zezwolić aplikacji na wychodzące i przychodzące połączenia internetowe.
- Kliknij przycisk **Przyznaj prawa dostępu jednorazowo**, aby zezwolić aplikacji na tymczasowe połączenie internetowe. Dostęp jest ograniczony do czasu między uruchomieniem aplikacji a jej zamknięciem.
- Kliknij przycisk **Blokuj dostęp wszystkich**, aby zabronić połączenia z Internetem.
- Kliknij przycisk **Przyznaj prawa dostępu dla wychodzących**, aby zezwolić na połączenie wychodzące (**Wyższy** poziom zabezpieczeń).
- Kliknij przycisk **Pomóż mi wybrać**, aby wyświetlić Pomoc online dotyczącą uprawnień dostępu aplikacji.

Alert Zmodyfikowano aplikację

Jeśli opcjach Ustawienia zabezpieczeń wybrano poziom zabezpieczeń **Zaufany**, **Standardowy** lub **Wysoki**, program Personal Firewall wyświetla alert (Ilustracja 3-7) w momencie wykrycia zmiany w aplikacji, która wcześniej uzyskała zezwolenie na dostęp do Internetu. Jeśli dana aplikacja nie była ostatnio uaktualniana, należy zachować ostrożność w przyznawaniu takiej zmodyfikowanej aplikacji uprawnień dostępu do Internetu.



Ilustracja 3-7. Alert Zmodyfikowano aplikację

Należy zapoznać się z krótkim opisem tego zdarzenia, a następnie wybrać jedną z następujących opcji:

- Kliknij przycisk **Przyznaj prawa dostępu**, aby zezwolić aplikacji na wychodzące i przychodzące połączenia internetowe.
- Kliknij przycisk **Przyznaj prawa dostępu jednorazowo**, aby zezwolić aplikacji na tymczasowe połączenie internetowe. Dostęp jest ograniczony do czasu między uruchomieniem aplikacji a jej zamknięciem.
- Kliknij przycisk **Blokuj dostęp wszystkich**, aby zabronić połączenia z Internetem.
- Kliknij przycisk **Przyznaj prawa dostępu dla wychodzących**, aby zezwolić na połączenie wychodzące (**Wyższy** poziom zabezpieczeń).
- Kliknij przycisk **Pomóż mi wybrać**, aby wyświetlić Pomoc online dotyczącą uprawnień dostępu aplikacji.

Alert Aplikacja żąda dostępu w roli serwera

Jeśli w opcjach ustawień zabezpieczeń wybrano poziom zabezpieczeń **Wysoki**, program Personal Firewall wyświetla alert (Ilustracja 3-8), gdy aplikacja, której wcześniej zezwolono na dostęp do Internetu, zażąda dostępu do Internetu w roli serwera.

Ilustracja 3-8. Alert Aplikacja żąda dostępu w roli serwera

Na przykład, alert zostanie wyświetlony, gdy program MSN Messenger zażąda dostępu w roli serwera, aby podczas rozmowy wysłać plik.

Należy zapoznać się z krótkim opisem tego zdarzenia, a następnie wybrać jedną z następujących opcji:

- Kliknij przycisk **Przyznaj prawa dostępu jednorazowo**, aby zezwolić aplikacji na tymczasowy dostęp do Internetu. Dostęp jest ograniczony do czasu między uruchomieniem aplikacji a jej zamknięciem.
- Kliknij przycisk **Przyznaj prawa dostępu w roli serwera**, aby zezwolić aplikacji na wychodzące i przychodzące połączenie z Internetem.
- Kliknij przycisk **Ogranicz do praw dostępu dla wychodzących**, aby zabronić przychodzącego połączenia internetowego.
- Kliknij przycisk **Blokuj dostęp wszystkich**, aby zabronić połączenia z Internetem.
- Kliknij przycisk **Pomóż mi wybrać**, aby wyświetlić Pomoc online dotyczącą uprawnień dostępu aplikacji.

Alerty zielone

Alerty zielone informują użytkownika o zdarzeniach występujących w programie Personal Firewall takich jak aplikacje, którym automatycznie przyznano dostęp do Internetu.

Program uzyskał prawo dostępu do Internetu - Ten alert zostaje wyświetlony, gdy program Personal Firewall automatycznie umożliwia dostęp do Internetu wszystkim nowym aplikacjom, a następnie powiadamia o tym użytkownika (**Zaufany** poziom zabezpieczeń). Przykładem zmodyfikowanej aplikacji jest aplikacja posiadająca zmodyfikowane reguły automatycznie zezwalające jej na dostęp do Internetu.

Alert Aplikacja uzyskała dostępu do Internetu

Po wybraniu poziomu zabezpieczeń **Zaufany** w opcjach Ustawienia zabezpieczeń program Personal Firewall automatycznie przyznaje dostęp do Internetu wszystkim nowym aplikacjom, a następnie powiadamia o tym zdarzeniu użytkownika w alercie (Ilustracja 3-9).

Ilustracja 3-9. Program uzyskał prawo dostępu do Internetu

Należy zapoznać się z krótkim opisem tego zdarzenia, a następnie wybrać jedną z następujących opcji:

- Kliknij polecenie **Wyświetl dziennik aplikacji** w celu uzyskania szczegółowych informacji o zdarzeniu za pośrednictwem dziennika aplikacji internetowych (aby uzyskać więcej informacji, patrz *Informacje o stronie Aplikacje internetowe* na str. 63).
- Kliknij polecenie **Wyłącz ten rodzaj alertów**, aby zapobiec wyświetlaniu alertów tego typu.
- Kliknij przycisk **Kontynuuj wykonywaną czynność**, jeśli nie chcesz podejmować dalszych działań poza tymi, które zostały już podjęte przez program Personal Firewall.
- Kliknij przycisk **Blokuj dostęp wszystkich**, aby zabronić połączenia z Internetem.

Alert Zmodyfikowano aplikację

Po wybraniu poziomu zabezpieczeń **Zaufany** w opcjach Ustawienia zabezpieczeń program Personal Firewall automatycznie przyznaje dostęp do Internetu wszystkim zmodyfikowanym aplikacjom. Należy zapoznać się z krótkim opisem tego zdarzenia, a następnie wybrać jedną z następujących opcji:

- Kliknij polecenie **Wyświetl dziennik aplikacji** w celu uzyskania szczegółowych informacji o zdarzeniu za pośrednictwem dziennika aplikacji internetowych (aby uzyskać więcej informacji, patrz *Informacje o stronie Aplikacje internetowe* na str. 63).
- Kliknij polecenie **Wyłącz ten rodzaj alertów**, aby zapobiec wyświetlaniu alertów tego typu.
- Kliknij przycisk **Kontynuuj wykonywaną czynność**, jeśli nie chcesz podejmować dalszych działań poza tymi, które zostały już podjęte przez program Personal Firewall.
- Kliknij przycisk **Blokuj dostęp wszystkich**, aby zabronić połączenia z Internetem.

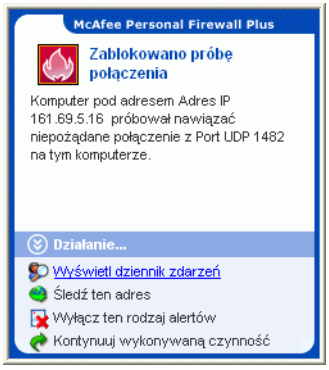
Alerty niebieskie

Alerty niebieskie mają charakter informacyjny i nie wymagają reakcji użytkownika.

- **Zablokowano próbę połączenia -** Ten alert jest wyświetlany, gdy program Personal Firewall zablokuje niepożądany ruch internetowy lub sieciowy. (Zaufany, Standardowy lub Wyższy poziom zabezpieczeń).

Alert Zablokowano próbę połączenia

Jeśli wybrano poziom zabezpieczeń **Zaufany**, **Standardowy** lub **Wyższy**, program Personal Firewall wyświetla alert (Ilustracja 3-10) w momencie zablokowania niepożądanego ruchu internetowego lub sieciowego.



Ilustracja 3-10. Alert Zablokowano próbę połączenia

Należy zapoznać się z krótkim opisem tego zdarzenia, a następnie wybrać jedną z następujących opcji:

- Kliknij polecenie **Wyświetl dziennik zdarzeń** w celu uzyskania szczegółowych informacji o zdarzeniu za pośrednictwem dziennika zdarzeń przychodzących programu Personal Firewall (aby uzyskać więcej informacji, patrz *Informacje o stronie Zdarzenia przychodzące* na str. 65).
- Kliknij przycisk **Śledź ten adres**, aby przeprowadzić wizualne śledzenie adresów IP dla tego zdarzenia za pomocą aplikacji Visual Trace.
- Kliknij przycisk **Zabroń dostępu temu adresowi**, aby zablokować dostęp do komputera z danego adresu. Adres zostanie dodany do listy zabronionych adresów IP.
- Kliknij przycisk **Ufaj temu adresowi**, aby zezwolić na dostęp do komputera z danego adresu IP.
- Kliknij polecenie **Kontynuuj wykonywaną czynność**, jeśli nie chcesz podejmować dalszych działań poza tymi, które zostały już podjęte przez program Personal Firewall.

McAfee Privacy Service 4

Dziękujemy za zakup programu McAfee® Privacy Service™. Oprogramowanie McAfee Privacy Service zapewnia zaawansowaną ochronę użytkownika, całej rodziny, informacji osobistych i komputera.

Funkcje

Ta wersja programu McAfee Privacy Service udostępnia następujące funkcje:

- Reguły korzystania z Internetu - określanie dni i godzin, w których użytkownicy mogą uzyskać dostęp do Internetu.
- Filtrowanie na podstawie niestandardowych słów kluczowych - tworzenie reguł dotyczących słów kluczowych w celu kontrolowania dostępu użytkowników do witryn sieci Web.
- Tworzenie kopii zapasowej i przywracanie danych programu Privacy Service - możliwość zapisania ustawień programu Privacy Service i ich przywrócenia w dowolnym momencie.
- Blokowanie pluskiew internetowych - możliwość blokowania pluskiew (obiektów pochodzących z potencjalnie niebezpiecznych witryn sieci Web) i niedopuszczenia do ich załadowania w wyświetlanych witrynach sieci Web.
- Blokowanie wyskakujących okien - zapobieganie wyświetlaniu wyskakujących okien podczas korzystania z Internetu.
- Shredder - program McAfee Shredder chroni prywatność użytkownika poprzez szybkie i bezpieczne wymazywanie niepożądanych plików.

Administrator

Administrator określa, którzy użytkownicy mogą korzystać z Internetu, kiedy mogą uzyskiwać dostęp oraz jakie czynności mogą wykonywać w Internecie.

UWAGA
Przyjmuje się, że administratorem jest osoba dorosła, która ma dostęp do wszystkich witryn sieci Web. Jednak przed przesłaniem informacji osobistych umożliwiających identyfikację użytkownika administrator jest pytany o to, czy zezwolić na tę czynność, czy uniemożliwić ją.

Konfigurowanie programu Privacy Service

Asystent konfiguracji umożliwia utworzenie konta administratora, zarządzanie ustawieniami globalnymi, wprowadzanie informacji osobistych i dodawanie użytkowników.

Hasło administratora i odpowiedź na pytanie zabezpieczające należy zapamiętać. W przeciwnym razie nie będzie można zalogować się do programu Privacy Service. Jeśli nie można się zalogować, nie można też korzystać z programu Privacy Service i Internetu. Administrator powinien zachować hasło w tajemnicy, aby nikt inny nie mógł zmieniać ustawień programu Privacy Service. Niektóre witryny sieci Web wymagają do prawidłowego działania włączenia obsługi plików cookie. Program Privacy Service zawsze akceptuje pliki cookie pochodzące z witryny McAfee.com.

UWAGA
Jeśli program Privacy Service został zainstalowany przez producenta komputera, niektóre z poniższych czynności zostaną pominięte. Aby uzyskać dodatkowe informacje, patrz *Konfigurowanie programu Privacy Service zainstalowanego przez producenta komputera* na str. 86. Zapoznaj się także z dokumentacją komputera dostarczoną przez jego producenta.

Konfigurowanie programu Privacy Service zainstalowanego przez producenta komputera

Jeżeli program Privacy Service został zainstalowany przez producenta na komputerze z systemem Windows XP, można go skonfigurować pod warunkiem zalogowania się do systemu Windows przy użyciu konta administratora systemu Windows.

Aby skonfigurować program Privacy Service zainstalowany przez producenta komputera:

1. Jeżeli dotychczas tego nie zrobiono, należy uruchomić Asystenta konfiguracji przy użyciu jednej z następujących metod:
   - Kliknij prawym przyciskiem myszy ikonę programu McAfee na pasku zadań systemu Windows, wskaż polecenie **Privacy Service**, a następnie wybierz polecenie **Konfiguracja programu Privacy Service**.
   - W menu **Start** systemu Windows wskaż polecenie **McAfee**, a następnie wybierz polecenie **McAfee Privacy Service**.
   - Kliknij dwukrotnie ikonę **McAfee Privacy Service** na pulpicie.
   - Uruchom program McAfee SecurityCenter, kliknij kartę **Privacy Service**, a następnie kliknij opcję **Konfiguracja programu Privacy Service**, aby uruchomić Asystenta konfiguracji.
2. Następnie należy postępować zgodnie z poszczególnymi instrukcjami.

UWAGA
Aby anulować konfigurację, kliknij przycisk **Anuluj**.

Pobieranie hasła administratora

W przypadku zapomnienia hasła administratora można uzyskać do niego dostęp, korzystając z informacji o zabezpieczeniach wprowadzonych podczas tworzenia profilu administratora.

Aby pobrać hasło administratora:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee na pasku zadań systemu Windows, wskaż opcję **McAfee Privacy Service**, a następnie wybierz polecenie **Zarejestruj**.
2. Z menu rozwijanego **Nazwa użytkownika** wybierz opcję **Administrator**.
3. Kliknij opcję **Nie pamiętasz hasła.**
4. Wpisz odpowiedź na wyświetlone pytanie, a następnie kliknij opcję **Pobierz hasło**. Zostanie wyświetlony komunikat zawierający hasło. Jeśli zapomnisz odpowiedzi na pytanie zabezpieczające, konieczne będzie odinstalowanie programu McAfee Privacy Service przy użyciu trybu awaryjnego (tylko w systemach Windows 2000 i Windows XP).

Usuwanie programu Privacy Service w trybie awaryjnym

Aby odinstalować program Privacy Service w trybie awaryjnym:

1. Kliknij przycisk **Start** i wskaż polecenie **Zamknij**. Zostanie wyświetlone okno dialogowe **Zamykanie systemu Windows**.
2. Wybierz z menu opcję **Wyłącz**, a następnie kliknij przycisk **OK**.
3. Zaczekaj na wyświetlenie komunikatu **Można bezpiecznie wyłączyć komputer** i wyłącz komputer.
4. Włącz ponownie komputer.
5. Natychmiast zacznij naciskać co dwie sekundy klawisz **F8**, aż zostanie wyświetlone menu **Uruchamianie systemu Windows**.
6. Wybierz opcję **Tryb awaryjny** i naciśnij klawisz **Enter**.
7. Podczas uruchamiania systemu Windows zostanie wyświetlony komunikat zawierający informacje na temat trybu awaryjnego. Kliknij przycisk **OK**.
8. Kliknij ikonę **Dodaj/Usuń programy** w Panelu sterowania systemu Windows. Po zakończeniu operacji uruchom ponownie komputer.
9. Zainstaluj ponownie program McAfee Privacy Service i ustaw hasło administratora. Zanotuj wprowadzone hasło.

UWAGA
Program Privacy Service można odinstalować w trybie awaryjnym tylko w systemach Windows 2000 i Windows XP.

Użytkownik startowy

Użytkownik startowy jest automatycznie rejestrowany w programie Privacy Service po uruchomieniu komputera.

Może nim być na przykład użytkownik korzystający z komputera lub z Internetu częściej niż inni (włącznie z administratorem). Kiedy użytkownik startowy korzysta z komputera, nie musi rejestrować się w programie Privacy Service.

Jeśli z komputera korzystają małe dzieci, najmłodsze z nich może być użytkownikiem startowym. W ten sposób, gdy starszy użytkownik korzysta z komputera, może wylogować się z konta młodszego użytkownika, a następnie ponownie się zalogować przy użyciu własnej nazwy użytkownika i hasła. Takie rozwiązanie uniemożliwia młodszym użytkownikom oglądanie niewłaściwych witryn sieci Web.

Wybieranie administratora jako użytkownika startowego

Aby wybrać administratora jako użytkownika startowego:

1. W oknie dialogowym **Zarejestruj** wybierz użytkownika z menu rozwijanego **Nazwa użytkownika**.
2. W polu **Hasło** wpisz hasło.
3. Zaznacz opcję **Ustaw tego użytkownika jako użytkownika startowego** i dokonaj rejestracji.

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. Umożliwia dostęp do programu Privacy Service i wykonywanie innych zadań:

- uzyskanie bezpłatnej analizy zabezpieczeń komputera;
- Uruchamianie, zarządzanie i konfiguracja 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 internetowej firmy McAfee.

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

Jeśli włączono wszystkie zainstalowane aplikacje firmy McAfee, po uruchomieniu programu SecurityCenter na pasku zadań systemu Windows (w obszarze powiadomień systemu Windows XP) zostaje wyświetlona czerwona ikona z literą M . Jest to obszar zawierający zegar i 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 uruchomić program McAfee SecurityCenter:

Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, a następnie wybierz opcję **Otwórz program SecurityCenter**.

Uruchamianie programu McAfee Privacy Service

Po zainstalowaniu programu McAfee Privacy Service na pasku zadań systemu Windows obok zegara systemowego pojawi się ikona programu McAfee . Po kliknięciu ikony McAfee można uzyskać dostęp do programów McAfee Privacy Service, McAfee SecurityCenter i innych produktów firmy McAfee zainstalowanych na komputerze.

UWAGA
Jeżeli oprogramowanie zostało zainstalowane przez producenta komputera, należy je najpierw skonfigurować. Aby uzyskać dodatkowe informacje, patrz *Konfigurowanie programu Privacy Service zainstalowanego przez producenta komputera* na str. 86.

Uruchamianie programu Privacy Service i rejestrowanie się w nim

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee na pasku zadań systemu Windows, wskaż polecenie **McAfee Privacy Service**, a następnie wybierz polecenie **Zarejestruj**.
2. Z menu rozwijanego **Nazwa użytkownika** wybierz swoją nazwę użytkownika.
3. Wprowadź hasło w polu **Hasło**.
4. Kliknij przycisk **Zarejestruj**.

Wyłączanie programu Privacy Service

Do wyłączenia programu Privacy Service wymagane są uprawnienia administratora.

Aby wyłączyć program Privacy Service:

- Kliknij prawym przyciskiem myszy ikonę programu McAfee na pasku zadań systemu Windows, wskaż opcję **McAfee Privacy Service**, a następnie wybierz polecenie **Wyrejestruj**.

  UWAGA
  Jeśli zamiast opcji **Wyrejestruj** jest dostępna opcja **Zarejestruj**, wyrejestrowanie zostało już przeprowadzone.

Aktualizacja programu McAfee Privacy Service

Gdy komputer jest włączony i podłączony do Internetu, narzędzie McAfee SecurityCenter regularnie sprawdza dostępność aktualizacji programu Privacy Service. Jeśli aktualizacja jest dostępna, narzędzie McAfee SecurityCenter wyświetli monit o aktualizację programu Privacy Service.

Aby ręcznie sprawdzić dostępność ewentualnych aktualizacji:

- Kliknij ikonę **Aktualizacje** w górnym okienku.

Usuwanie i ponowne instalowanie programu Privacy Service

Do odinstalowania programu Privacy Service wymagane są uprawnienia administratora.

Jeżeli program Privacy Service firmy McAfee został zainstalowany przez producenta komputera, instrukcje dezinstalacji i ponownej instalacji można znaleźć w dokumentacji dostarczonej przez tego producenta.

UWAGA
Usunięcie programu Privacy Service powoduje także skasowanie wszystkich jego danych.

Usuwanie programu Privacy Service

Aby odinstalować program Privacy Service:

1. Zapisz pracę i zamknij wszystkie otwarte aplikacje.
2. Otwórz Panel sterowania:
   - Windows 98, Windows Me i Windows 2000: Kliknij przycisk **Start**, wskaż opcję **Ustawienia**, a następnie kliknij polecenie **Panel sterowania**.
   - Windows XP: Kliknij przycisk **Start** na pasku zadań systemu Windows, a następnie kliknij polecenie **Panel sterowania**.
3. Otwórz okno dialogowe **Dodaj/Usuń programy**:
   - Windows 98, Me i 2000: Kliknij dwukrotnie ikonę **Dodaj/Usuń programy**.
   - Windows XP: Kliknij polecenie **Dodaj lub usuń programy**.
4. Zaznacz pozycję Privacy Service na liście programów, a następnie kliknij przycisk **Zmień/Usuń**.
5. Gdy zostanie wyświetlony monit o potwierdzenie operacji, kliknij przycisk **Tak**.
6. Po wyświetleniu monitu o ponowne uruchomienie systemu kliknij przycisk **Zamknij**. Komputer zostanie uruchomiony ponownie w celu zakończenia procesu dezinstalacji.

Instalowanie programu Privacy Service

Aby zainstalować program Privacy Service:

1. Przejdź do witryny sieci Web firmy McAfee, a następnie do strony programu Privacy Service.
2. Kliknij łącze **Pobierz** na stronie programu Privacy Service.
3. Kliknij przycisk **Tak** we wszystkich oknach dialogowych z pytaniami, czy chcesz pobrać pliki z witryny sieci Web firmy McAfee.
4. Kliknij przycisk **Start Installation** (Rozpocznij instalację) w oknie instalacji programu Privacy Service.
5. Po zakończeniu pobierania kliknij przycisk **Uruchom ponownie**, aby ponownie uruchomić komputer. Jeśli chcesz zapisać pracę lub zamknąć programy, najpierw kliknij przycisk **Zamknij**, a następnie uruchom ponownie komputer. W celu poprawnej pracy programu Privacy Service działał należy ponownie uruchomić komputer.

Po ponownym uruchomieniu komputera należy znowu utworzyć konto administratora.

Jeżeli program Privacy Service firmy McAfee został zainstalowany przez producenta komputera, instrukcje ponownej instalacji można znaleźć w dokumentacji dostarczonej przez tego producenta.

Aby móc dodawać użytkowników, należy zarejestrować się w programie Privacy Service jako administrator.

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee na pasku zadań systemu Windows.
2. Wskaż polecenie **McAfee Privacy Service**, a następnie wybierz polecenie **Zarządzaj użytkownikami**. Zostanie wyświetlone okno dialogowe **Wybierz użytkownika**.
3. Kliknij przycisk **Dodaj** i wprowadź nazwę nowego użytkownika w polu **Nazwa użytkownika**.

Ustawianie hasła

1. Wprowadź hasło w polu **Hasło**. Może się ono składać z maksymalnie 50 znaków i zawierać wielkie i małe litery oraz cyfry.
2. Wprowadź ponownie hasło w polu **Potwierdź hasło**.
3. Zaznacz opcję **Ustaw tego użytkownika jako użytkownika startowego**, jeśli ten użytkownik ma być użytkownikiem startowym.
4. Kliknij przycisk **Dalej**.

Podczas przypisywania hasła należy uwzględnić wiek użytkownika. Na przykład hasło dla młodszego dziecka powinno być proste. Hasło dla starszego nastolatka lub osoby dorosłej powinno być bardziej złożone.

Ustawianie grupy wiekowej

Wybierz odpowiednie ustawienie dla grupy wiekowej, a następnie kliknij przycisk **Dalej**.

Ustawianie blokowania plików cookie

Zaznacz odpowiednią opcję, a następnie kliknij przycisk **Dalej**.

- **Odrzucaj wszystkie pliki cookie** - uniemożliwia odczytywanie plików cookie przez witryny sieci Web, które je wysłały. Niektóre witryny sieci Web wymagają do prawidłowego działania włączenia obsługi plików cookie.
- **Monituj użytkownika o zaakceptowanie plików cookie** - umożliwia użytkownikowi każdorazowe określenie, czy wysyłany plik cookie ma zostać zaakceptowany, czy odrzucony. Program Privacy Service wysyła powiadomienie, gdy odwiedzana witryna sieci Web usiłuje wysłać plik cookie do komputera. Po określeniu działania odnośnie pliku cookie użytkownik nie otrzymuje więcej zapytań na jego temat.
- **Akceptuj wszystkie pliki cookie** - umożliwia witrynom sieci Web odczytywanie plików cookie wysyłanych do tego komputera.

  UWAGA
  Niektóre witryny sieci Web wymagają do prawidłowego działania włączenia obsługi plików cookie.

  Program Privacy Service zawsze akceptuje pliki cookie pochodzące z firmy McAfee.

Ustawianie ograniczeń czasu dostępu do Internetu

Aby przyznać użytkownikowi nieograniczony dostęp do Internetu:

1. Zaznacz opcję **Dozwolone korzystanie z Internetu przez cały czas**.
2. Kliknij opcję **Utwórz**. Nowy użytkownik pojawi się na liście Wybierz użytkownika.

Aby przyznać użytkownikowi ograniczony dostęp do Internetu:

1. Zaznacz opcję **Ograniczaj dostęp do Internetu**, a następnie kliknij przycisk **Edytuj**.

2 Na stronie Ograniczenia czasu dostępu do Internetu przeciągnij myszą po siatce czasu, aby określić dni i godziny, kiedy użytkownik może korzystać z Internetu. Limity czasu można określić w odstępach co trzydzieści minut. Zielone fragmenty siatki przedstawiają okresy, kiedy można korzystać z Internetu. Czerwone fragmenty siatki przedstawiają okresy, w których użytkownik nie może łączyć się z Internetem. Jeśli użytkownik spróbuje skorzystać z Internetu poza wyznaczonym czasem, w programie Privacy Service zostanie wyświetlony komunikat informujący, że korzystanie z Internetu jest aktualnie niedozwolone. Aby zmodyfikować okresy, w których użytkownik może korzystać z Internetu, przeciągnij myszą po zielonej części siatki.

3 Kliknij przycisk **Gotowe**.

4 Kliknij opcję **Utwórz**. Nowy użytkownik pojawi się na stronie Wybierz użytkownika. Jeśli użytkownik spróbuje skorzystać z Internetu poza wyznaczonym czasem, w programie Privacy Service zostanie wyświetlony komunikat informujący, że korzystanie z Internetu jest aktualnie niedozwolone.

Aby zabronić dostępu do Internetu:

Zaznacz opcję **Ograniczaj dostęp do Internetu**, a następnie kliknij przycisk **Utwórz**. Kiedy użytkownik korzysta z komputera, będzie wyświetlany monit o zarejestrowanie się w programie Privacy Service. Możliwe jest korzystanie z komputera, ale nie z Internetu.

Tworzenie uprawnień dostępu do witryn sieci Web na podstawie słów kluczowych

Program Privacy Service obsługuje domyślną listę słów kluczowych i odpowiadających im reguł, które określają, czy użytkownik w danym wieku może oglądać witrynę sieci Web, w której występuje określone słowo kluczowe, czy też nie.

Administrator może dodawać własne dozwolone słowa kluczowe do bazy danych programu Privacy Service i przypisywać je do określonych grup wiekowych. Reguły dotyczące słów kluczowych dodane przez administratora zastępują powiązane z określonymi słowami kluczowymi reguły znajdujące się w domyślnej bazie danych programu Privacy Service. Administrator może wyszukiwać istniejące słowa kluczowe lub określać nowe słowa, które zostaną powiązane z określonymi grupami wiekowymi.

Aby utworzyć uprawnienia dostępu do witryn sieci Web na podstawie słów kluczowych:

1 Prawym przyciskiem myszy kliknij ikonę programu McAfee na pasku zadań systemu Windows, wskaż opcję **Privacy Service**, a następnie wybierz polecenie **Opcje**.

2 Kliknij kartę **Słowa kluczowe**.

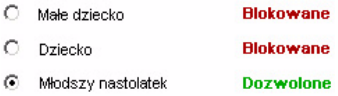
3 W polu **Wyszukaj słowa** wpisz żądane słowo.

4 W okienku **Uprawnienia** wybierz grupę wiekową, z którą ma być powiązane to słowo. Dostępne są następujące grupy wiekowe:

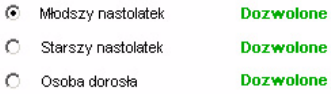
- Młodsze dziecko
- Dziecko
- Młodszy nastolatek
- Starszy nastolatek
- Dorosły

Nowe słowo kluczowe i grupa wiekowa, z którą jest ono powiązane, pojawią się na liście **Lista słów**.

Użytkownicy należący do grup wiekowych znajdujących się powyżej wybranej grupy nie będą mieć dostępu do witryn sieci Web zawierających wprowadzone słowo.



Użytkownicy z grupy wiekowej powiązanej z nowym słowem kluczowym i z grup znajdujących się poniżej będą mieć dostęp do witryn sieci Web, w których występuje dane słowo.



Aby zmienić istniejące uprawnienia dostępu do witryn sieci Web:

1 Prawym przyciskiem myszy kliknij ikonę programu McAfee na pasku zadań systemu Windows, wskaż opcję **Privacy Service**, a następnie wybierz polecenie **Opcje**.

2 Kliknij kartę **Słowa kluczowe**.

3 W polu **Wyszukaj słowa** wpisz słowo, które chcesz zmienić, a następnie kliknij opcję **Wyszukaj**. Słowo zostanie wyświetlone, jeżeli będzie zapisane w bazie danych programu Privacy Service.

Aby dokonać edycji użytkowników, należy zarejestrować się w programie Privacy Service jako administrator.

Zmiana haseł

1. Wybierz użytkownika, którego informacje mają zostać zmienione, a następnie kliknij przycisk **Edytuj**.
2. Wybierz opcję **Hasło** i wprowadź nowe hasło użytkownika w polu **Nowe hasło**. Może się ono składać z maksymalnie 50 znaków i zawierać wielkie i małe litery oraz cyfry.
3. Wprowadź to samo hasło w polu **Potwierdź hasło**, a następnie kliknij przycisk **Zastosuj**.
4. Kliknij przycisk **OK** w oknie dialogowym potwierdzenia.

UWAGA
Administrator może zmienić hasło użytkownika, nie znając jego aktualnego hasła.

Zmiana informacji o użytkowniku

1. Wybierz użytkownika, którego informacje mają zostać zmienione, a następnie kliknij przycisk **Edytuj**.
2. Wybierz opcję **Informacje o użytkowniku**.
3. Wprowadź nazwę nowego użytkownika w polu **Nowa nazwa użytkownika**.
4. Kliknij przycisk **Zastosuj**, a następnie kliknij przycisk **OK** w oknie dialogowym potwierdzenia.
5. Aby ograniczyć dostęp użytkownika tylko do wyświetlania witryn sieci Web znajdujących się na liście Dozwolone witryny sieci Web, zaznacz opcję **Ogranicz dostęp tego użytkownika do witryn z listy „Dozwolone witryny sieci Web”**.

Zmiana ustawienia blokowania plików cookie

1. Wybierz użytkownika, którego informacje mają zostać zmienione, a następnie kliknij przycisk **Edytuj**.
2. Wybierz opcję **Pliki cookie**, a następnie wybierz odpowiednią opcję.
   - **Odrzucaj wszystkie pliki cookie** - uniemożliwia odczytywanie plików cookie przez witryny sieci Web, które je wysłały. Niektóre witryny sieci Web wymagają do prawidłowego działania włączenia obsługi plików cookie.

- **Monituj użytkownika o zaakceptowanie plików cookie** - umożliwia użytkownikowi każdorazowe określenie, czy wysyłany plik cookie ma zostać zaakceptowany, czy odrzucony. Program Privacy Service wysyła powiadomienie, gdy odwiedzana witryna sieci Web usiłuje wysłać plik cookie do komputera. Po określeniu działania odnośnie pliku cookie użytkownik nie otrzymuje więcej zapytań na jego temat.
- **Akceptuj wszystkie pliki cookie** - umożliwia witrynom sieci Web odczytywanie plików cookie wysyłanych do tego komputera.

3 Kliknij przycisk **Zastosuj**, a następnie kliknij przycisk **OK** w oknie dialogowym potwierdzenia.

Edycja listy akceptowanych i odrzucanych plików cookie

1 Zaznacz opcję **Monituj użytkownika o zaakceptowanie plików cookie** i kliknij przycisk **Edytuj**, aby określić witryny sieci Web, które mogą odczytywać pliki cookie.

2 Określ modyfikowaną listę, zaznaczając opcję **Witryny sieci Web, które mogą zapisywać pliki cookie** lub **Witryny sieci Web, które nie mogą zapisywać plików cookie**.

3 W polu **http://** wprowadź adres witryny sieci Web, z której pliki cookie mają być akceptowane lub odrzucane.

4 Kliknij przycisk **Dodaj**. Witryna pojawi się na liście witryn sieci Web.

5 Po zakończeniu wprowadzania zmian kliknij przycisk **Gotowe**.

UWAGA
Niektóre witryny sieci Web wymagają do prawidłowego działania włączenia obsługi plików cookie.

Program Privacy Service zawsze akceptuje pliki cookie pochodzące z firmy McAfee.

Zmiana grupy wiekowej

1 Wybierz użytkownika, którego informacje mają zostać zmienione, a następnie kliknij przycisk **Edytuj**.

2 Wybierz opcję **Grupa wiekowa**.

3 Wybierz nową grupę wiekową dla użytkownika, a następnie kliknij przycisk **Zastosuj**.

4 Kliknij przycisk **OK** w oknie dialogowym potwierdzenia.

Zmiana ograniczeń czasu dostępu do Internetu

1. Wybierz użytkownika, którego informacje mają zostać zmienione, a następnie kliknij przycisk **Edytuj**.
2. Wybierz opcję **Limity czasowe** i wykonaj następujące czynności:

Aby zezwolić na nieograniczony dostęp do Internetu:

1. Zaznacz opcję **Dozwolone korzystanie z Internetu przez cały czas** i kliknij przycisk **Zastosuj**.
2. Kliknij przycisk **OK** w oknie dialogowym potwierdzenia.

Aby ograniczyć dostęp do Internetu:

1. Zaznacz opcję **Ograniczaj dostęp do Internetu** i kliknij przycisk **Edytuj**.
2. Na stronie Ograniczenia czasu dostępu do Internetu zaznacz zielony lub czerwony kwadrat, a następnie przeciągnij myszą po siatce czasu, aby zmienić istniejące dni i godziny, kiedy użytkownik może korzystać z Internetu.
   Limity czasu można określić w odstępach co trzydzieści minut. Zielone fragmenty siatki przedstawiają okresy, kiedy można korzystać z Internetu. Czerwone fragmenty siatki przedstawiają okresy, w których użytkownik nie może łączyć się z Internetem. Jeśli użytkownik spróbuje skorzystać z Internetu poza wyznaczonym czasem, w programie Privacy Service zostanie wyświetlony komunikat informujący, że korzystanie z Internetu jest aktualnie niedozwolone.
3. Kliknij przycisk **Zastosuj**.
4. Na stronie Limity czasowe kliknij przycisk **OK**.
5. W oknie dialogowym potwierdzenia programu McAfee Privacy Service kliknij przycisk **OK**.

Zmiana użytkownika startowego

Administrator może zmienić użytkownika startowego w dowolnym czasie. Jeśli użytkownik startowy już istnieje, nie trzeba go usuwać.

1. Wybierz użytkownika, który ma być użytkownikiem startowym, a następnie kliknij przycisk **Edytuj**.
2. Wybierz opcję **Informacje o użytkowniku**.
3. Zaznacz opcję **Ustaw tego użytkownika jako użytkownika startowego**.
4. Kliknij przycisk **Zastosuj**, a następnie kliknij przycisk **OK** w oknie dialogowym potwierdzenia.

UWAGA
Użytkownika startowego można również wybrać w oknie dialogowym **Zarejestruj**. Aby uzyskać dodatkowe informacje, patrz *Użytkownik startowy* na str. 88.

Usuwanie użytkowników

1. Wybierz użytkownika, który ma zostać usunięty, a następnie kliknij przycisk **Usuń**.
2. Kliknij przycisk **Tak** w oknie dialogowym potwierdzenia.
3. Po zakończeniu wprowadzania zmian zamknij okno programu Privacy Service.

Aby skonfigurować opcje programu Privacy Service, należy zarejestrować się w programie Privacy Service jako administrator.

Blokowanie witryn sieci Web

1. Kliknij **Opcje**, a następnie wybierz kartę **Lista blokowania**.
2. W polu **http://** wprowadź adres URL witryny sieci Web, która ma być blokowana, a następnie kliknij opcję **Dodaj**. Witryna pojawi się na liście **Blokowane witryny sieci Web**.

UWAGA
Użytkownicy (w tym administratorzy) należący do grupy wiekowej Dorosły mają dostęp do wszystkich witryn sieci Web, nawet jeśli znajdują się one na liście witryn zablokowanych. Aby przetestować blokowanie witryn sieci Web, administratorzy muszą zalogować się jako użytkownicy inni niż dorośli.

Dozwolone witryny sieci Web

Administrator może zezwolić wszystkim użytkownikom na przeglądanie określonych witryn sieci Web. Ta opcja zastępuje ustawienia domyślne programu Privacy Service i listę blokowanych witryn sieci Web.

1. Kliknij **Opcje**, a następnie wybierz kartę **Lista dozwolonych**.
2. W polu **http://** wprowadź adres URL witryny, na przeglądanie której chcesz zezwolić, a następnie kliknij opcję **Dodaj**. Witryna pojawi się na liście **Dozwolone witryny sieci Web**.

Blokowanie informacji

Administrator może uniemożliwić innym użytkownikom wysyłanie określonych informacji osobistych przez Internet (on sam nadal może je wysyłać).

W przypadku wykrycia przez program Privacy Service, że wysyłane dane zawierają informacje umożliwiające identyfikację użytkownika, wykonywane są następujące czynności:

- Jeśli użytkownik jest administratorem, zostaje wyświetlony monit z pytaniem, czy informacje mają zostać wysłane, czy nie.
- Jeśli zalogowany użytkownik nie ma uprawnień administratora, zablokowane informacje są zastępowane tekstem *MFEMFEMFE*. Na przykład jeśli w treści wiadomości e-mail znajdzie się informacja *Lance Armstrong wygrał turniej*, a słowo „Armstrong” będzie ustawione jako blokowana informacja osobista, wysłana wiadomość będzie miała postać: *Lance MFEMFEMFE wygrał turniej*.

Dodawanie informacji

1. Kliknij **Opcje**, a następnie wybierz kartę **Blokuj informacje**.
2. Kliknij przycisk **Dodaj**. Zostanie wyświetlone menu rozwijane **Wybierz typ**.
3. Wybierz typ informacji, które chcesz zablokować.
4. Wprowadź informacje w odpowiednich polach, a następnie kliknij przycisk **OK**. Wprowadzone informacje zostaną wyświetlone na liście.

Edycja informacji

1. Kliknij **Opcje**, a następnie wybierz kartę **Blokuj informacje**.
2. Wybierz informacje, które chcesz zmienić, a następnie kliknij przycisk **Edytuj**.
3. Wprowadź wymagane zmiany, a następnie kliknij przycisk **OK**. Jeżeli informacje nie wymagają zmiany, kliknij przycisk **Anuluj**.

Usuwanie informacji osobistych

1. Kliknij **Opcje**, a następnie wybierz kartę **Blokuj informacje**.
2. Wybierz informacje, które chcesz usunąć, a następnie kliknij przycisk **Usuń**.
3. Kliknij przycisk **Tak** w oknie dialogowym potwierdzenia.

Blokowanie pluskiew internetowych

Pluskwy internetowe są małymi plikami graficznymi, które mogą wysyłać wiadomości stronom trzecim, w tym informacje o zachowaniach użytkowników podczas przeglądania witryn sieci Web, lub które wysyłają informacje osobiste do zewnętrznych baz danych. Inne firmy mogą używać tych informacji do tworzenia profilów użytkowników.

Aby zapobiec ładowaniu pluskiew internetowych podczas wyświetlania stron sieci Web, zaznacz opcję **Blokuj pluskwy internetowe na tym komputerze**.

Blokowanie reklam

Reklamy są zazwyczaj obrazami przesyłanymi z domeny innej firmy do strony sieci Web lub wyskakującego okna. Program Privacy Service nie blokuje reklam przesyłanych z tej samej domeny, co strona sieci Web.

Wyskakujące okna są dodatkowymi oknami przeglądarki zawierającymi niepożądane reklamy, które pojawiają się automatycznie podczas przeglądania witryny sieci Web. Program Privacy Service blokuje tylko wyskakujące okna wyświetlane automatycznie podczas ładowania strony sieci Web. Okna wyskakujące w wyniku kliknięcia łącza nie są blokowane. Aby wyświetlić zablokowane okno wyskakujące, należy przytrzymać klawisz CTRL i odświeżyć stronę sieci Web.

Konfigurowanie programu Privacy Service w celu blokowania reklam i wyskakujących okien podczas korzystania z Internetu

1. Kliknij **Opcje**, a następnie wybierz kartę **Blokuj reklamy**.
2. Zaznacz właściwą opcję.
   - **Blokuj reklamy na tym komputerze** - umożliwia blokowanie reklam podczas korzystania z Internetu.
   - **Blokuj wyskakujące okna na tym komputerze** - umożliwia blokowanie okien wyskakujących podczas korzystania z Internetu.
3. Kliknij przycisk **Zastosuj**, a następnie kliknij przycisk **OK** w oknie dialogowym potwierdzenia.

Aby wyłączyć blokowanie wyskakujących okien, kliknij prawym przyciskiem myszy stronę sieci Web, wskaż opcję **McAfee - Blokowanie wyskakujących okien**, a następnie usuń zaznaczenie opcji **Włącz funkcję blokowania wyskakujących okien**.

Zezwalanie na pliki cookie z określonych witryn sieci Web

Jeśli niektóre witryny sieci Web nie działają prawidłowo, a ustawione jest blokowanie plików cookie lub wymaganie potwierdzenia przed ich akceptacją, należy skonfigurować program Privacy Service tak, aby witryny te mogły odczytywać pliki cookie.

1. Kliknij **Opcje**, a następnie wybierz kartę **Pliki cookie**.
2. W polu **http://** wprowadź adres witryny sieci Web, która wymaga odczytu plików cookie, a następnie kliknij opcję **Dodaj**. Adres pojawi się na liście **Witryny sieci Web z akceptacją plików cookie**.

Aby wyświetlić dziennik zdarzeń, należy zarejestrować się w programie Privacy Service jako administrator. Następnie należy wybrać opcję **Dziennik zdarzeń** i kliknąć dowolny wpis dziennika, aby wyświetlić jego szczegóły. Aby zapisać lub wyświetlić zapisany dziennik, należy wybrać kartę Zapisane dzienniki.

Data i godzina

Informacje w dzienniku zdarzeń są domyślnie wyświetlane w porządku chronologicznym, począwszy od najnowszych. Jeśli wpisy w Dzienniku zdarzeń nie są uporządkowane chronologicznie, należy kliknąć nagłówek Data i godzina.

Data jest wyświetlana w formacie miesiąc/dzień/rok, a godzina w formacie dwunastogodzinnym.

Użytkownik

Użytkownik to osoba, która zalogowała się i korzystała z Internetu w momencie zarejestrowania zdarzenia przez program Privacy Service.

Podsumowanie

Podsumowania zawierają krótki i zwięzły opis działań podejmowanych przez program Privacy Service w celu ochrony użytkowników oraz działań użytkowników w Internecie.

Szczegóły zdarzenia

Pole Szczegóły zdarzenia zawiera szczegółowe informacje o wpisie.

Zapisywanie bieżącego dziennika

Strona Bieżący dziennik zawiera informacje o ostatnio wykonanych czynnościach administracyjnych i działaniach użytkownika. Informacje te można zapisać, aby były dostępne do przeglądania w przyszłości.

Aby zapisać bieżący dziennik zdarzeń:

1. Zarejestruj się w programie Privacy Service jako administrator.
2. Wybierz opcję **Dziennik zdarzeń**.
3. Na stronie Bieżący dziennik kliknij przycisk **Zapisz dziennik**.
4. W polu **Nazwa pliku** wprowadź nazwę pliku dziennika.
5. Kliknij przycisk **Zapisz**.

Wyświetlanie zapisanych dzienników

Strona Bieżący dziennik zawiera informacje o ostatnio wykonanych czynnościach administracyjnych i działaniach użytkownika. Informacje te można zapisać, aby były dostępne do przeglądania w przyszłości.

Aby wyświetlić zapisany dziennik

1. Zarejestruj się w programie Privacy Service jako administrator.
2. Wybierz opcję **Dziennik zdarzeń**.
3. Na stronie Bieżący dziennik kliknij przycisk **Otwórz dziennik**.
4. W oknie dialogowym **Wybierz zapisany dziennik do przejrzenia** wybierz plik kopii zapasowej bazy danych i kliknij przycisk **Otwórz**.

Aby uzyskać dostęp do narzędzi, należy zarejestrować się w programie Privacy Service jako administrator, a następnie kliknąć **Narzędzia**.

Aby usunąć wybrane pliki lub foldery albo całą zawartość dysku, kliknij opcję **McAfee Shredder**. Aby zapisać ustawienia bazy danych programu Privacy Service, kliknij opcję **Kopia zapasowa**. Aby przywrócić ustawienia, kliknij opcję **Przywróć**.

Trwałe usuwanie plików za pomocą programu McAfee Shredder

Program McAfee Shredder  chroni prywatność użytkownika przez szybkie i bezpieczne wymazywanie niepożądanych plików.

Usunięte pliki można odzyskać na komputerze nawet po opróżnieniu Kosza. Gdy plik jest usuwany, system Windows oznacza tylko miejsce zajmowane przez ten plik na dysku jako nieużywane, ale plik nadal tam jest.

Dlaczego system Windows zostawia pozostałości po plikach

Aby trwale usunąć plik, należy go wielokrotnie zastąpić nowymi danymi. Gdyby system Microsoft Windows usuwał pliki w sposób bezpieczny, każda operacja na plikach byłaby bardzo wolna. Zniszczenie dokumentu nie zawsze zapobiega jego odzyskaniu, ponieważ niektóre programy tworzą tymczasowe ukryte kopie otwartych plików. W razie niszczenia tylko dokumentów widzianych w Eksploratorze ich tymczasowe kopie mogą pozostać na komputerze. Zaleca się okresowe niszczenie zawartości nieużywanego miejsca na dysku, aby mieć pewność, że te tymczasowe kopie zostały na trwałe usunięte.

UWAGA
Za pomocą komputerowych narzędzi śledczych można odzyskać zeznania podatkowe, życiorysy i inne usunięte dokumenty.

Co usuwa program McAfee Shredder

Za pomocą programu McAfee Shredder można bezpiecznie i trwale usunąć:

- Jeden lub więcej plików bądź folderów
- Całą zawartość dysku
- Ślady przeglądania sieci Web

Trwałe usuwanie plików w Eksploratorze Windows

Aby niszczyć pliki z poziomu Eksploratora Windows:

1. Otwórz Eksploratora Windows, a następnie wybierz plik lub pliki, które chcesz zniszczyć.
2. Kliknij prawym przyciskiem myszy zaznaczenie, wskaż polecenie **Wyślij do**, a następnie pozycję **McAfee Shredder**.

Opróżnianie Kosza systemu Windows

Jeśli w Koszu znajdują się pliki, program McAfee Shredder udostępnia bezpieczniejszy sposób jego opróżnienia.

Aby zniszczyć zawartość Kosza:

1. Na pulpicie systemu Windows kliknij prawym przyciskiem myszy ikonę Kosz.
2. Wybierz polecenie **Zniszcz zawartość Kosza**, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Dostosowywanie ustawień programu Shredder

Można wykonać następujące czynności:

- Określić liczbę przebiegów niszczenia.
- Wyświetlać komunikat ostrzegawczy przed zniszczeniem plików.

- Sprawdzać dysk twardy pod kątem błędów przed niszczeniem.
- Dodać program McAfee Shredder do menu Wyślij do.
- Umieścić ikonę programu Shredder na pulpicie systemu Windows.

Aby dostosować ustawienia, otwórz program McAfee Shredder, kliknij przycisk **Właściwości**, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Tworzenie kopii zapasowej bazy danych programu Privacy Service

Bazę danych programu Privacy Service można przywrócić na dwa sposoby. W przypadku uszkodzenia lub usunięcia bazy danych wyświetlany jest monit o przywrócenie bazy danych programu Privacy Service. Ustawienia bazy danych można też przywrócić podczas uruchamiania programu Privacy Service.

1. Kliknij **Narzędzia**, a następnie kliknij łącze **Kopia zapasowa**.
2. Kliknij przycisk **Przeglądaj**, aby wybrać lokalizację pliku bazy danych, a następnie kliknij przycisk **OK**.
3. Wprowadź hasło w polu **Hasło**.
4. Wprowadź ponownie hasło w polu **Potwierdź hasło**, a następnie kliknij przycisk **Kopia zapasowa**.
5. Kliknij przycisk **OK** w oknie dialogowym potwierdzenia.
6. Po zakończeniu zamknij okno programu Privacy Service.

UWAGA
Hasło należy zapamiętać i zachować w tajemnicy. Bez niego nie można przywrócić ustawień programu Privacy Service.

Przywracanie kopii zapasowej bazy danych.

1. Program Privacy Service udostępnia dwa sposoby przywracania pierwotnych ustawień:
   - Załadowanie pliku kopii zapasowej bazy danych po wyświetleniu przez program Privacy Service monitu o przywrócenie ustawień z powodu uszkodzenia lub usunięcia bazy danych.
   - Załadowanie pliku kopii zapasowej bazy danych podczas uruchamiania programu Privacy Service.

Aby przywrócić ustawienia programu Privacy Service po wyświetleniu monitu:

1. Kliknij przycisk **Przeglądaj**, aby znaleźć plik.
2. W polu **Hasło** wpisz hasło.
3. Kliknij przycisk **Przywróć**.
   Jeśli nie utworzono kopii zapasowej bazy danych programu Privacy Service, użytkownik zapomniał hasła do kopii zapasowej lub przywrócenie bazy danych nie powiodło się, należy odinstalować i ponownie zainstalować program Privacy Service.

Aby przywrócić ustawienia programu Privacy Service podczas jego uruchamiania:

1. Kliknij kartę **Narzędzia**.
2. Kliknij przycisk **Przywróć**.
3. Kliknij przycisk **Przeglądaj**, a następnie wpisz ścieżkę i nazwę pliku kopii zapasowej.
4. Kliknij przycisk **Otwórz**.
5. W polu **Hasło** wpisz hasło.
6. Kliknij przycisk **Przywróć**, a następnie kliknij przycisk **OK** w oknie dialogowym potwierdzenia programu McAfee Privacy Service.

Przedstawione instrukcje nie dotyczą administratora.

Użytkownicy mogą zmieniać swoją nazwę użytkownika i hasło. Zaleca się zmianę hasła po uzyskaniu go od administratora. Zalecane jest także zmienianie hasła raz w miesiącu lub gdy istnieje podejrzenie, że jest ono znane innym osobom. Takie postępowanie uniemożliwia innym osobom uzyskiwanie dostępu do Internetu przy użyciu cudzej nazwy użytkownika.

Zmiana hasła użytkownika

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż opcję **McAfee Privacy Service**, a następnie wybierz polecenie **Opcje**.
2. Kliknij opcję **Hasło** i wprowadź stare hasło w polu **Stare hasło**.
3. Wprowadź nowe hasło w polu **Nowe hasło**.
4. Wpisz ponownie nowe hasło w polu **Potwierdź hasło**, a następnie kliknij przycisk **Zastosuj**.
5. Kliknij przycisk **OK** w oknie dialogowym potwierdzenia. Nowe hasło zostało utworzone.

Zmiana nazwy użytkownika

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż opcję **McAfee Privacy Service**, a następnie wybierz polecenie **Opcje**.
2. Kliknij opcję **Informacje o użytkowniku**.
3. Wpisz nową nazwę użytkownika w polu **Nowa nazwa użytkownika**, a następnie kliknij przycisk **Zastosuj**.
4. Kliknij przycisk **OK** w oknie dialogowym potwierdzenia. Nowa nazwa użytkownika została utworzona.

Czyszczenie pamięci podręcznej

Zaleca się czyszczenie pamięci podręcznej, aby dzieci nie miały dostępu do stron sieci Web odwiedzanych przez innych użytkowników. Aby wyczyścić pamięć podręczną, wykonaj następujące czynności:

1. Uruchom program Internet Explorer.
2. Kliknij menu **Narzędzia**, a następnie kliknij polecenie **Opcje internetowe**. Zostanie wyświetlone okno dialogowe Opcje internetowe.
3. W sekcji **Tymczasowe pliki internetowe** kliknij przycisk **Usuń pliki**. Zostanie wyświetlone okno dialogowe Usuwanie plików.
4. Zaznacz pole wyboru **Usuń całą zawartość offline**, a następnie kliknij przycisk **OK**.
5. Kliknij przycisk **OK**, aby zamknąć okno dialogowe Opcje internetowe.

Akceptowanie plików cookie

Ta opcja jest dostępna tylko w przypadku, gdy administrator zezwala użytkownikowi na akceptowanie lub odrzucanie przechwytywanych plików cookie.

Jeśli używane witryny sieci Web wymagają plików cookie, można zezwolić im na ich odczytywanie.

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż opcję **McAfee Privacy Service**, a następnie wybierz polecenie **Opcje**.
2. Kliknij kartę **Zaakceptowane pliki cookie**.
3. W polu **http://** wprowadź adres URL witryny sieci Web, a następnie kliknij opcję **Dodaj**. Witryna pojawi się na liście **Witryna sieci Web**.

Aby usunąć witrynę sieci Web z tej listy:

1. Zaznacz adres URL witryny na liście **Witryna sieci Web**.
2. Kliknij przycisk **Usuń**, a następnie kliknij przycisk **Tak** w oknie dialogowym potwierdzenia.

Odrzucanie plików cookie

Ta opcja jest dostępna tylko w przypadku, gdy administrator zezwala użytkownikowi na akceptowanie lub odrzucanie przechwytywanych plików cookie.

Jeśli używane witryny sieci Web nie wymagają plików cookie, można je odrzucać bez wyświetlania monitu.

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż opcję **McAfee Privacy Service**, a następnie wybierz polecenie **Opcje**.
2. Kliknij kartę **Odrzucone pliki cookie**.
3. W polu **http://** wprowadź adres URL witryny sieci Web, a następnie kliknij opcję **Dodaj**. Witryna pojawi się na liście **Witryna sieci Web**.

Aby usunąć witrynę sieci Web z tej listy:

1. Zaznacz adres URL witryny na liście **Witryna sieci Web**.
2. Kliknij przycisk **Usuń**, a następnie kliknij przycisk **Tak** w oknie dialogowym potwierdzenia.

McAfee SpamKiller 5

McAfee SpamKiller - zapraszamy!

Program McAfee SpamKiller pomaga zatrzymać spam przed wtargnięciem do skrzynki odbiorczej poczty e-mail. Program ma następujące funkcje:

Opcje użytkownika

- Blokowanie spamu przy użyciu filtrów i poddawanie spamu kwarantannie poza skrzynką odbiorczą
- Przeglądanie zablokowanych i zaakceptowanych wiadomości
- Monitorowanie i filtrowanie wielu kont e-mail
- Importowanie adresów znajomych do listy znajomych
- Zwalczanie nadawców spamu (zgłaszanie spamu, składanie skarg dotyczących spamu, tworzenie niestandardowych filtrów)
- Uniemożliwianie dzieciom dostępu do wiadomości będących spamem
- Szybkie blokowanie i szybkie ratowanie wiadomości
- Obsługa znaków dwubajtowych
- Obsługa wielu użytkowników (systemy Windows 2000 i Windows XP)

Filtrowanie

- Automatyczna aktualizacja filtrów
- Tworzenie filtrów niestandardowych w celu blokowania wiadomości e-mail zawierających głównie obrazy, niewidoczny tekst lub nieprawidłowe formatowanie
- Wielowarstwowy mechanizm filtrowania
- Filtr ataków słownikowych
- Wielopoziomowe filtrowanie adaptacyjne
- Filtry zabezpieczeń

Funkcje

W tej wersji programu SpamKiller dostępne są następujące funkcje:

- Filtrowanie - zaawansowane opcje filtrowania udostępniają nowe techniki filtrowania, między innymi filtrowanie oparte na meta-znakach i identyfikację tekstu niepożądanych wiadomości.
- „Phishing” - dodatek plug-in AntiPhishing dostępny z paska narzędziowego programu Internet Explorer z łatwością identyfikuje i blokuje witryny internetowe, które mogą być źródłami ataków typu „phishing”.
- Integracja z programem Microsoft Outlook i Outlook Express - pasek narzędzi udostępnia w obrębie klienta poczty folder do bezpośredniego blokowania spamu.
- Instalacja - uproszczony proces instalacji i konfiguracji programu. Automatyczne wykrywanie kont gwarantuje bezproblemową instalację, konfigurację i integrację z istniejącymi kontami poczty e-mail.
- Aktualizacje - proces automatycznych aktualizacji dyskretnie uruchomiony w tle pozostaje zawsze czujny, aby zminimalizować podatność na zagrożenia związane ze spamem.
- Interfejs - intuicyjny interfejs użytkownika pomagający zabezpieczyć komputer przed spamem.
- Pomoc techniczna - darmowa pomoc techniczna za pośrednictwem poczty e-mail i wiadomości błyskawicznych to szybka i przystępna obsługa klienta.
- Przetwarzanie spamu - domyślnie wiadomości będące spamem są oznaczane jako [SPAM] i umieszczane w folderze SpamKiller w programie Outlook i Outlook Express lub w skrzynce odbiorczej. Wiadomości oznaczone są także wyświetlane na stronie Zaakceptowana poczta e-mail.

Górne okienko - omówienie

W górnym okienku na każdej stronie programu SpamKiller pojawiają się następujące ikony:

- Kliknij ikonę **Przełącz użytkownika**  , aby zalogować się jako inny użytkownik.

  Uwaga: Opcja **Przełącz użytkownika** jest dostępna tylko w przypadku, gdy na komputerze jest zainstalowany system operacyjny Windows 2000 lub Windows XP, do programu SpamKiller dodano wielu użytkowników, a użytkownik zalogowany w programie SpamKiller ma uprawnienia administratora.

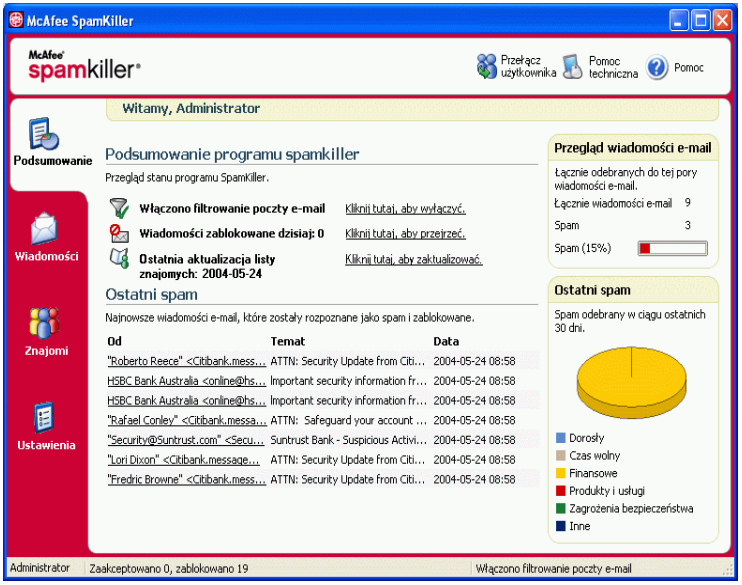
- Kliknij ikonę **Pomoc techniczna**  , aby otworzyć stronę pomocy technicznej firmy McAfee, na której znajdują się aktualne wiadomości na temat programu SpamKiller i innych produktów firmy McAfee, odpowiedzi na często zadawane pytania i wiele innych informacji. Aby uzyskać dostęp do strony pomocy technicznej, wymagane jest połączenie z Internetem.
- Kliknij ikonę **Pomoc**  , aby otworzyć pomoc w trybie online, w której znajdują się szczegółowe instrukcje dotyczące konfiguracji i używania programu SpamKiller.

Strona Podsumowanie - omówienie

Kliknij kartę **Podsumowanie**, aby otworzyć stronę Podsumowanie (Ilustracja 5-1).

- **Przegląd stanu programu SpamKiller** - wskazuje, czy włączone jest filtrowanie, informuje, kiedy ostatnio zaktualizowano listę znajomych oraz podaje liczbę wiadomości otrzymanych bieżącego dnia, które zostały rozpoznane jako spam. Na tej stronie można też wyłączyć lub włączyć funkcję filtrowania wiadomości przez program SpamKiller, zaktualizować listę znajomych oraz otworzyć stronę Zablokowana poczta e-mail.
- **Najnowsze wiadomości e-mail, które zostały rozpoznane jako spam i zablokowane** - ostatnie wiadomości zidentyfikowane jako spam i zablokowane przez program SpamKiller (wiadomości usunięte ze skrzynki odbiorczej).
- **Przegląd wiadomości e-mail** - całkowita liczba wiadomości e-mail, spamu (zablokowanych wiadomości) oraz wartość procentowa, jaką stanowią wszystkie otrzymane wiadomości rozpoznane jako spam.

- **Ostatni spam** - podział na typy spamu odebranego w ciągu ostatnich 30 dni.



Ilustracja 5-1. Strona Podsumowanie

Integracja z programami Microsoft Outlook i Outlook Express

Główne funkcje programu SpamKiller są dostępne z poziomu programów Outlook Express 6.0, Outlook 98, Outlook 2000 i Outlook XP - w menu SpamKiller lub na pasku narzędzi SpamKiller.

Pasek narzędzi programu SpamKiller jest wyświetlany na prawo od standardowych pasków narzędzi aplikacji Outlook i Outlook Express. Jeśli pasek ten nie jest widoczny, należy rozwinąć okno programu pocztowego lub kliknąć strzałki w celu wyświetlenia większej liczby pasków narzędzi.

Po pojawieniu się paska narzędzi programu SpamKiller w programie pocztowym po raz pierwszy jego polecenia można wykonywać tylko w odniesieniu do nowych wiadomości. Istniejące wiadomości zidentyfikowane jako spam należy usunąć ręcznie.

Obsługiwane programy pocztowe

- Zgodne z protokołem POP3 (Outlook Express, Outlook, Eudora, Netscape)
- Zgodne z interfejsem MAPI (Outlook)
- Internetowe (MSN/Hotmail lub konto e-mail oparte na protokole POP3)

Wymagania dotyczące dodatku plug-in paska narzędzi

- Outlook Express 6.0 lub nowszy
- Outlook 98, 2000 z dodatkiem SP3, 2003 lub XP
- Internet Explorer w wersji 6.0 lub nowszej

Korzystanie z programu McAfee SecurityCenter

Program McAfee SecurityCenter pełni rolę centrum zabezpieczeń. Bezproblemowa integracja z programem McAfee SecurityCenter zapewnia skonsolidowany widok stanu zabezpieczeń komputera oraz najnowszych alertów zabezpieczeń i alertów o wirusach. Program SecurityCenter można uruchomić za pomocą ikony McAfee znajdującej się na pasku zadań systemu Windows lub z poziomu pulpitu systemu Windows.

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

Po uruchomieniu programu SecurityCenter, jeśli na komputerze zainstalowano i włączono wszystkie funkcje oprogramowania McAfee, na pasku zadań systemu Windows (w obszarze powiadomień systemu Windows XP) zostanie wyświetlona czerwona ikona z literą **M** .

Jeśli co najmniej 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 SpamKiller:

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

Po zainstalowaniu programu SpamKiller na pasku zadań obok zegara systemowego pojawi się ikona programu McAfee . Po kliknięciu ikony McAfee można uzyskać dostęp do programów SpamKiller, McAfee SecurityCenter i innych produktów firmy McAfee zainstalowanych na komputerze.

Wyłączanie programu SpamKiller

Istnieje możliwość wyłączenia programu SpamKiller, aby zapobiec filtrowaniu poczty elektronicznej.

Aby wyłączyć filtrowanie:

Kliknij prawym przyciskiem myszy ikonę programu McAfee  , wskaż polecenie **SpamKiller**, a następnie kliknij polecenie **Wyłącz**. Można też kliknąć kartę **Podsumowanie**, a następnie opcję **Kliknij tutaj, aby wyłączyć**.

Aby włączyć filtrowanie:

Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż polecenie **SpamKiller**, a następnie kliknij polecenie **Włącz**. Można też kliknąć kartę **Podsumowanie**, a następnie opcję **Kliknij tutaj, aby włączyć**.

Dodawanie kont e-mail

Można dodawać następujące rodzaje kont e-mail:

- Standardowe konto e-mail (POP3) - z kont tego typu korzysta większość użytkowników domowych.
- Konto MSN/Hotmail - konta internetowe oferowane w ramach usługi MSN/Hotmail.

UWAGA

Jeśli na komputerze jest zainstalowany system Windows 2000 lub Windows XP i planowane jest dodanie wielu użytkowników do programu SpamKiller, użytkowników należy dodać przed dodaniem kont e-mail do ich profilów. Aby uzyskać dodatkowe informacje, patrz *Dodawanie użytkowników* na str. 122. W przypadku, gdy do programu SpamKiller dodano wielu użytkowników, konto zostanie dodane do profilu użytkownika, który jest aktualnie zalogowany do programu SpamKiller.

Dodawanie konta e-mail

1 Kliknij kartę **Ustawienia**, aby otworzyć stronę Ustawienia (Ilustracja 5-2), a następnie kliknij opcję **Konta e-mail**. Zostanie wyświetlone okno dialogowe **Konta e-mail** zawierające listę wszystkich kont e-mail dodanych do programu SpamKiller.

> **UWAGA**
> W przypadku, gdy do programu SpamKiller dodano wielu użytkowników, na liście wyświetlane są konta e-mail użytkownika, który jest aktualnie zalogowany do programu SpamKiller.

2 Kliknij przycisk **Dodaj**. Zostanie wyświetlony kreator konta e-mail.

3 Postępuj zgodnie z instrukcjami wyświetlanymi w oknach dialogowych.

W przypadku dodawania konta MSN/Hotmail program SpamKiller wyszukuje książkę adresową MSN/Hotmail, aby zaimportować ją do listy osobistych znajomych.

Ilustracja 5-2. Strona Ustawienia

Wskazywanie programu SpamKiller w kliencie poczty e-mail

Aby dodać konto, które nie jest wykrywane przez program SpamKiller (konto takie nie jest widoczne na liście w oknie dialogowym **Wybierz konto**) lub aby móc odczytywać pocztę MSN/Hotmail jak wiadomości z konta POP3 w programie SpamKiller, wskaż program SpamKiller w kliencie poczty e-mail, zmieniając serwer przychodzącej poczty e-mail.

Na przykład, jeśli serwerem poczty przychodzącej jest „mail.mcafee.com”, zmień go na „localhost”.

Usuwanie kont e-mail

Konto e-mail, które nie być już monitorowane za pomocą programu SpamKiller, należy z niego usunąć.

Usuwanie konta e-mail z programu SpamKiller

1. Kliknij kartę **Ustawienia**, a następnie opcję **Konta e-mail**. Zostanie wyświetlone okno dialogowe **Konta e-mail** zawierające listę wszystkich kont e-mail dodanych do programu SpamKiller.

   UWAGA
   W przypadku, gdy do programu SpamKiller dodano wielu użytkowników, na liście wyświetlane są konta e-mail użytkownika, który jest aktualnie zalogowany do programu SpamKiller.

2. Wybierz żądane konto, a następnie kliknij przycisk **Usuń**.

Edycja właściwości kont e-mail

Istnieje możliwość edycji informacji o koncie e-mail dodanym do programu SpamKiller. Można na przykład zmienić adres poczty e-mail, opis konta, informacje o serwerze, częstotliwość sprawdzania konta przez program SpamKiller pod kątem spamu oraz sposób łączenia się komputera z Internetem.

Konta POP3

Edycja kont POP3

1. Kliknij kartę **Ustawienia**, a następnie opcję **Konta e-mail**. Zostanie wyświetlone okno dialogowe **Konta e-mail** zawierające listę wszystkich kont e-mail dodanych do programu SpamKiller.

   UWAGA
   W przypadku, gdy do programu SpamKiller dodano wielu użytkowników, na liście wyświetlane są konta e-mail użytkownika, który jest aktualnie zalogowany do programu SpamKiller.

2. Wybierz konto POP3, a następnie kliknij przycisk **Edytuj**.

3. Kliknij kartę **Ogólne**, aby zmienić opis konta i adres e-mail.

   - **Opis** - opis konta. W tym polu można wpisać dowolne informacje.
   - **Adres e-mail** - adres e-mail konta.

4 Kliknij kartę **Serwery**, aby zmienić informacje o serwerach.

- **Przychodząca poczta e-mail** - nazwa serwera odbierającego pocztę przychodzącą.
- **Nazwa użytkownika** - nazwa użytkownika służąca w celu uzyskania dostępu do konta. Czasami używane jest określenie „nazwa konta”.
- **Hasło** - hasło używane w celu uzyskania dostępu do konta.
- **Wychodząca poczta e-mail** - nazwa serwera wysyłającego pocztę wychodzącą. Kliknij przycisk **Więcej**, aby zmienić wymagania uwierzytelniania dla serwera poczty wychodzącej.

5 Kliknij kartę **Sprawdzanie**, aby zmienić częstotliwość sprawdzania przez program SpamKiller występowania spamu na koncie:

a Zaznacz opcję **Sprawdź co** lub **Sprawdź codziennie o**, a następnie wprowadź lub wybierz wartość czasową w odpowiednim polu. W przypadku wprowadzenia zera program SpamKiller będzie sprawdzać konto tylko po nawiązaniu połączenia z Internetem.

b Wybierz dodatkowe godziny, kiedy program SpamKiller ma filtrować konto:

Sprawdź podczas uruchamiania - opcja przydatna w przypadku korzystania z łącza stałego, gdy konto ma być sprawdzane przez program SpamKiller podczas każdego uruchomienia komputera.

Sprawdź podczas wybierania numeru - opcja przydatna w przypadku korzystania z połączenia telefonicznego, gdy konto ma być sprawdzane przez program SpamKiller za każdym razem, gdy komputer nawiązuje połączenie z Internetem.

6 Kliknij kartę **Połączenie**, aby określić sposób nawiązywania połączenia z Internetem przez program SpamKiller w celu sprawdzenia, czy w skrzynce odbiorczej znajdują się nowe wiadomości do filtrowania.

- **Nigdy nie wybieraj numeru połączenia** - umożliwia wyłączenie opcji samodzielnego wybierania numeru połączenia przez program SpamKiller. W takim przypadku użytkownik musi najpierw nawiązać połączenie telefoniczne ręcznie.
- **Wybierz numer w razie potrzeby** - gdy połączenie z Internetem nie jest dostępne, program SpamKiller automatycznie podejmuje próbę nawiązania go przy użyciu domyślnego telefonicznego połączenia z Internetem.
- **Zawsze wybieraj numer** - program SpamKiller automatycznie podejmuje próbę nawiązania połączenia z Internetem przy użyciu połączenia telefonicznego zdefiniowanego przez użytkownika.
- **Utrzymaj połączenie po zakończeniu filtrowania** - komputer pozostaje połączony z Internetem po zakończeniu filtrowania.

7 Kliknij kartę **Zaawansowane**, aby zmienić opcje zaawansowane.

- **Pozostaw na serwerze wiadomości będące spamem** - umożliwia pozostawienie kopii zablokowanych wiadomości na serwerze poczty e-mail. Pocztę można przeglądać za pomocą klienta poczty elektronicznej, a także w programie SpamKiller - na stronie Zablokowana poczta e-mail. Jeśli to pole wyboru nie jest zaznaczone, zablokowane wiadomości można przeglądać tylko na stronie Zablokowana poczta e-mail.
- **Port POP3** - numer portu POP3. Serwer POP3 obsługuje wiadomości przychodzące.
- **Port SMTP** - numer portu SMTP. Serwer SMTP obsługuje wiadomości wychodzące.
- **Limit czasu serwera** - określa, jak długo program SpamKiller czeka na odebranie wiadomości e-mail, zanim upłynie limit czasu i zostanie zatrzymane jego działanie.

  W przypadku problemów z odbiorem poczty należy zwiększyć limit czasu serwera. Połączenie używane do sprawdzania poczty e-mail może mieć małą przepustowość. Dlatego zaleca się zwiększyć tę wartość, aby limit czasu upływał później.

8 Kliknij przycisk **OK**.

Konta MSN/Hotmail

Edycja kont MSN/Hotmail

1 Kliknij kartę **Ustawienia**, a następnie opcję **Konta e-mail**.

Zostanie wyświetlone okno dialogowe **Konta e-mail** zawierające listę wszystkich kont e-mail dodanych do programu SpamKiller.

> **UWAGA**
> W przypadku, gdy do programu SpamKiller dodano wielu użytkowników, na liście wyświetlane są konta e-mail użytkownika, który jest aktualnie zalogowany do programu SpamKiller.

2 Zaznacz żądane konto MSN/Hotmail, a następnie kliknij przycisk **Edytuj**.

3 Kliknij kartę **Ogólne**, aby zmienić opis konta i adres e-mail.

- **Opis** - opis konta. W tym polu można wpisać dowolne informacje.
- **Adres e-mail** - adres e-mail konta.

4 Kliknij kartę **Serwery**, aby zmienić informacje o serwerach.

- **Przychodząca poczta e-mail** - nazwa serwera odbierającego pocztę przychodzącą.
- **Hasło** - hasło używane w celu uzyskania dostępu do konta.
- **Wychodząca poczta e-mail** - nazwa serwera wysyłającego pocztę wychodzącą.
- **Użyj serwera SMTP dla wychodzącej poczty e-mail** - opcja ta umożliwia wysyłanie komunikatów o błędach bez wiersza podpisu MSN. Wiersz podpisu MSN ułatwia nadawcom spamu rozpoznanie, że komunikat o błędzie jest fałszywy.

  Kliknij przycisk **Więcej**, aby zmienić wymagania uwierzytelniania dla serwera poczty wychodzącej.

5 Kliknij kartę **Sprawdzanie**, aby określić częstotliwość sprawdzania przez program SpamKiller obecności spamu na koncie:

a Zaznacz opcję **Sprawdź co** lub **Sprawdź codziennie o**, a następnie wprowadź lub wybierz wartość czasową w odpowiednim polu. W przypadku wprowadzenia zera program SpamKiller będzie sprawdzać konto tylko po nawiązaniu połączenia z Internetem.

b Wybierz dodatkowe godziny, kiedy program SpamKiller ma filtrować konto:

Sprawdź podczas uruchamiania - zaznacz tę opcję w przypadku korzystania z łącza stałego, gdy konto ma być sprawdzane przez program SpamKiller podczas każdego uruchomienia komputera.

Sprawdź podczas wybierania numeru - zaznacz tę opcję w przypadku korzystania z połączenia telefonicznego, gdy konto ma być sprawdzane przez program SpamKiller za każdym razem, gdy komputer nawiązuje połączenie z Internetem.

6 Kliknij kartę **Połączenie**, aby określić sposób nawiązywania połączenia z Internetem przez program SpamKiller w celu sprawdzenia, czy w skrzynce odbiorczej znajdują się nowe wiadomości do filtrowania.

- **Nigdy nie wybieraj numeru połączenia** - umożliwia wyłączenie opcji samodzielnego wybierania numeru połączenia przez program SpamKiller. W takim przypadku użytkownik musi najpierw nawiązać połączenie telefoniczne ręcznie.
- **Wybierz numer w razie potrzeby** - gdy połączenie z Internetem nie jest dostępne, program SpamKiller automatycznie podejmuje próbę nawiązania go przy użyciu domyślnego telefonicznego połączenia z Internetem.
- **Zawsze wybieraj numer** - program SpamKiller automatycznie podejmuje próbę nawiązania połączenia z Internetem przy użyciu połączenia telefonicznego zdefiniowanego przez użytkownika.
- **Utrzymaj połączenie po zakończeniu filtrowania** - komputer pozostaje połączony z Internetem po zakończeniu filtrowania.

7 Kliknij przycisk **OK**.

Konfigurowanie konta Hotmail do blokowania spamu w programie Outlook lub Outlook Express

Program SpamKiller może filtrować konta Hotmail bezpośrednio. Szczegółowe informacje można znaleźć w systemie pomocy online. Blokowanie wiadomości oraz dodawanie znajomych za pomocą paska narzędzi SpamKiller w programie Outlook lub Outlook Express jest możliwe dopiero po skonfigurowaniu konta Hotmail.

1 Skonfiguruj konto Hotmail w programie McAfee SpamKiller.

2 W przypadku posiadania istniejącego konta Hotmail w programie Outlook lub Outlook Express usuń je.

3 Dodaj konto Hotmail do programu Outlook lub Outlook Express. Jako typ konta i typ serwera poczty przychodzącej wybierz **POP3**.

4 Nadaj serwerowi poczty przychodzącej nazwę **`localhost`**.

5 Wprowadź nazwę dostępnego serwera poczty wychodzącej SMTP (wymagane).

6 Dokończ proces konfiguracji konta. Można teraz blokować nowe wiadomości Hotmail zidentyfikowane jako spam oraz dodawać znajomych.

Konta MAPI

Poniżej przedstawiono warunki pomyślnej integracji programu SpamKiller z podsystemem MAPI programu Outlook:

- Program Outlook został wstępnie zainstalowany z opcją obsługi firm/grup roboczych (tylko Outlook 98).
- Pierwszym kontem e-mail jest konto MAPI (tylko Outlook 98).
- Komputer jest zalogowany do domeny.

Edycja kont MAPI

1. Kliknij kartę **Ustawienia**, a następnie opcję **Konta e-mail**. Zostanie wyświetlone okno dialogowe **Konta e-mail** zawierające listę wszystkich kont e-mail dodanych do programu SpamKiller.

   UWAGA
   W przypadku, gdy do programu SpamKiller dodano wielu użytkowników, na liście wyświetlane są konta e-mail użytkownika, który jest aktualnie zalogowany do programu SpamKiller.

2. Wybierz konto MAPI, a następnie kliknij przycisk **Edytuj**.
3. Kliknij kartę **Ogólne**, aby zmienić opis konta i adres e-mail.
   - **Opis** - opis konta. W tym polu można wpisać dowolne informacje.
   - **Adres e-mail** - adres e-mail konta.
4. Kliknij kartę **Profil**, aby zmienić informacje o profilu.
   - **Profil** - profil MAPI dla konta.
   - **Hasło** - hasło odpowiadające profilowi MAPI w przypadku jego utworzenia (nie musi to być hasło konta e-mail).
5. Kliknij kartę **Połączenie**, aby określić sposób nawiązywania połączenia z Internetem przez program SpamKiller w celu sprawdzenia, czy w skrzynce odbiorczej znajdują się nowe wiadomości do filtrowania:
   - **Nigdy nie wybieraj numeru połączenia** - umożliwia wyłączenie opcji samodzielnego wybierania numeru połączenia przez program SpamKiller. W takim przypadku użytkownik musi najpierw nawiązać połączenie telefoniczne ręcznie.
   - **Wybierz numer w razie potrzeby** - gdy połączenie z Internetem nie jest dostępne, program SpamKiller automatycznie podejmuje próbę nawiązania go przy użyciu domyślnego telefonicznego połączenia z Internetem.

- **Zawsze wybieraj numer** - program SpamKiller automatycznie podejmuje próbę nawiązania połączenia z Internetem przy użyciu połączenia telefonicznego zdefiniowanego przez użytkownika.
- **Utrzymaj połączenie po zakończeniu filtrowania** - komputer pozostaje połączony z Internetem po zakończeniu filtrowania.

6 Kliknij przycisk **OK**.

Dodawanie użytkowników

W programie SpamKiller można skonfigurować wielu użytkowników odpowiadających użytkownikom skonfigurowanym w systemie operacyjnym Windows 2000 lub Windows XP.

Podczas instalacji programu SpamKiller na komputerze dla użytkownika zalogowanego w systemie Windows program SpamKiller automatycznie tworzy profil użytkownika z uprawnieniami administratora. Jeśli podczas instalacji dodano do programu SpamKiller konta e-mail, zostaną one dodane do tego profilu użytkownika.

Przed dodaniem kolejnych kont e-mail do programu SpamKiller należy określić, czy wymagane jest dodanie nowych użytkowników programu SpamKiller. Dodanie użytkowników jest korzystne, jeśli z komputera korzysta kilku użytkowników mających własne konta e-mail. Konto e-mail każdego użytkownika jest dodawane do profilu danego użytkownika, dzięki czemu użytkownicy mogą zarządzać własnymi kontami e-mail, ustawieniami osobistymi, filtrami osobistymi i listą osobistych znajomych.

Typy użytkowników określają zadania, jakie może wykonywać użytkownik w programie SpamKiller. W poniższej tabeli przedstawiono podsumowanie uprawnień dla poszczególnych typów użytkowników. Administratorzy mogą wykonywać wszystkie zadania, natomiast użytkownicy z ograniczonymi uprawnieniami mogą korzystać jedynie z tych funkcji programu, które zdefiniowano w ich profilu osobistym. Na przykład, administratorzy mogą wyświetlać całą zawartość zablokowanych wiadomości, podczas gdy użytkownicy z ograniczonymi uprawnieniami mogą przeglądać tylko tematy.

Zadania	Administrator	Użytkownik z ograniczonymi uprawnieniami
Zarządzanie osobistymi kontami e-mail, filtrami osobistymi, listą osobistych znajomych i osobistymi ustawieniami dźwięku	X	X
Zarządzanie osobistymi stronami Zablokowana poczta e-mail i Zaakceptowana poczta e-mail	X	X
Wyświetlanie tekstu zablokowanych wiadomości	X	
Wyświetlanie tekstu zaakceptowanych wiadomości	X	X

Zadania	Administrator	Użytkownik z ograniczonymi uprawnieniami
Zarządzanie filtrami globalnymi i globalną listą znajomych	X	
Zgłaszanie spamu firmie McAfee	X	X
Wysyłanie skarg i komunikatów o błędach	X	X
Zarządzanie skargami i komunikatami o błędach (tworzenie, edycja i usuwanie szablonów wiadomości)	X	
Zarządzanie użytkownikami (tworzenie, edycja i usuwanie użytkowników)	X	
Tworzenie kopii zapasowej i przywracanie programu SpamKiller	X	
Wyświetlanie strony podsumowania dotyczącej otrzymanego spamu	X	X

Gdy nowo dodany użytkownik zaloguje się do komputera, zostanie wyświetlony monit o dodanie konta e-mail do jego profilu.

Aby dodawać użytkowników lub zarządzać nimi, muszą być spełnione następujące warunki:

- Zalogowanie się do programu SpamKiller jako administrator.
- Zainstalowany na komputerze system Windows 2000 lub Windows XP.
- Dodawani lub zarządzani użytkownicy muszą mieć konta użytkowników w systemie Windows.

Hasła użytkowników i ochrona dzieci przed spamem

Utworzenie hasła zwiększa poziom prywatności. Ustawienia osobiste, lista znajomych i lista zaakceptowanej poczty e-mail są niedostępne dla innych użytkowników bez zalogowania się z podaniem odpowiedniego hasła. Dodatkową korzyścią wynikającą z utworzenia hasła jest uniemożliwienie dzieciom dostępu do programu SpamKiller i wyświetlanie treści wiadomości rozpoznanych jako spam.

Tworzenie lub zmiana hasła istniejącego użytkownika programu SpamKiller

1. Kliknij kartę **Ustawienia**, a następnie przycisk **Użytkownicy**.
2. Zaznacz użytkownika, a następnie kliknij przycisk **Edytuj**.

3 Wpisz hasło w polu **Hasło**. Aby użytkownik mógł używać programu SpamKiller musi użyć tego hasła w celu zalogowania się.

> **WAŻNE**
> Zapomnianego hasła nie można odzyskać. Tylko administrator programu SpamKiller może utworzyć nowe hasło.

Dodawanie użytkownika do programu SpamKiller

1 Kliknij kartę **Ustawienia**, a następnie przycisk **Użytkownicy**.

2 Kliknij przycisk **Dodaj**.

Zostanie wyświetlona lista użytkowników systemu Windows. Aby dodać użytkownika, którego nie ma na liście, należy utworzyć konto użytkownika systemu Windows dla tej osoby. Następnie nowy użytkownik musi co najmniej raz zalogować się do komputera. Dopiero później można dodać go do programu SpamKiller.

> **UWAGA**
> Użytkownicy systemu operacyjnego Windows z uprawnieniami administratora mają prawa administratora programu SpamKiller.

3 Zaznacz użytkownika, którego chcesz dodać, a następnie kliknij przycisk **OK**. Nowy użytkownik zostanie dodany do programu SpamKiller, a jego nazwa pojawi się na liście użytkowników programu SpamKiller.

4 Po zakończeniu dodawania użytkowników kliknij przycisk **Zamknij**.

Aby utworzyć hasło użytkownika, zapoznaj się z sekcją *Tworzenie lub zmiana hasła istniejącego użytkownika programu SpamKiller* na str. 123.

Gdy nowo dodany użytkownik zaloguje się po raz pierwszy do komputera, zostanie wyświetlony monit o dodanie konta e-mail do jego profilu w programie SpamKiller. Konta e-mail można dodawać do profilu użytkownika w przypadku zalogowania się do programu SpamKiller jako dany użytkownik i posiadania potrzebnych informacji na temat konta. Szczegółowe informacje można znaleźć w sekcji *Dodawanie kont e-mail* na str. 114.

Edycja profilu użytkownika programu SpamKiller

1 Kliknij kartę **Ustawienia**, a następnie przycisk **Użytkownicy**. Zostanie wyświetlona lista użytkowników programu SpamKiller.

2 Zaznacz użytkownika, a następnie kliknij przycisk **Edytuj**.

3 Wprowadź nową nazwę użytkownika i hasło.

Usuwanie profilu użytkownika programu SpamKiller

OSTRZEŻENIE
Po usunięciu profilu użytkownika z programu SpamKiller usuwane są także konta e-mail danego użytkownika.

1. Kliknij kartę **Ustawienia**, a następnie przycisk **Użytkownicy**. Zostanie wyświetlona lista użytkowników programu SpamKiller.
2. Zaznacz żądanego użytkownika na liście, a następnie kliknij przycisk **Usuń**.

Logowanie do programu SpamKiller w środowisku wielu użytkowników

Po zalogowaniu do komputera i otwarciu programu SpamKiller użytkownicy są automatycznie logowani do programu SpamKiller przy użyciu ich profilu użytkowników. Jeśli przypisano im hasło programu SpamKiller, wymagane jest wpisanie hasła w wyświetlonym oknie dialogowym **Zaloguj**.

Przełączanie między użytkownikami

Zalogowanie się do programu SpamKiller jako administrator.

1. Kliknij przycisk **Przełącz użytkownika** znajdujący się u góry strony. Zostanie wyświetlone okno dialogowe **Przełącz użytkownika**.
2. Zaznacz wybranego użytkownika, a następnie kliknij przycisk **OK**. Jeśli użytkownik ma hasło, zostanie wyświetlone okno dialogowe **Zaloguj**. Wpisz hasło użytkownika w polu **Hasło**, a następnie kliknij przycisk **OK**.

Zaleca się dodanie nazwisk i adresów e-mail wszystkich swoich przyjaciół do listy znajomych. Ponieważ program SpamKiller nie blokuje wiadomości od osób znajdujących się na tej liście, dodanie znajomych gwarantuje dostarczanie chcianych wiadomości.

Program SpamKiller umożliwia dodawanie następujących informacji do list znajomych: nazwisk, adresów e-mail, domen lub list adresowych. Adresy można dodawać pojedynczo lub grupowo przez zaimportowanie książki adresowej z programu pocztowego.

Program SpamKiller korzysta z dwóch rodzajów list:

- **Globalna lista znajomych** - dotyczy wszystkich kont e-mail dla wszystkich użytkowników w programie SpamKiller. Jeśli dodano wielu użytkowników, w celu zarządzania tą listą należy zalogować się do programu SpamKiller jako administrator.
- **Lista osobistych znajomych** - dotyczy wszystkich kont e-mail skojarzonych z określonym użytkownikiem. Jeśli dodano wielu użytkowników, w celu zarządzania tą listą należy zalogować się do programu SpamKiller jako użytkownik.

Do listy znajomych dodaje się znane sobie osoby, aby mieć pewność, że wysyłane przez nie wiadomości e-mail nie będą blokowane. Na stronie Znajomi wyświetlane są nazwy i adresy dodane do listy znajomych. Widoczna jest na niej także data dodania znajomego oraz całkowita liczba otrzymanych od niego wiadomości.

Kliknij kartę **Adresy e-mail**, aby wyświetlić adresy e-mail na liście znajomych. Kliknij kartę **Domeny**, aby wyświetlić adresy domen na liście. Kliknij kartę **Listy adresowe**, aby wyświetlić listy adresowe na liście znajomych.

Aby przejść z globalnej listy znajomych na listę osobistych znajomych, kliknij strzałkę w dół znajdującą się na kartach **Adres e-mail**, **Domeny** lub **Listy adresowe**, a następnie wybierz opcję **Lista osobistych znajomych**.

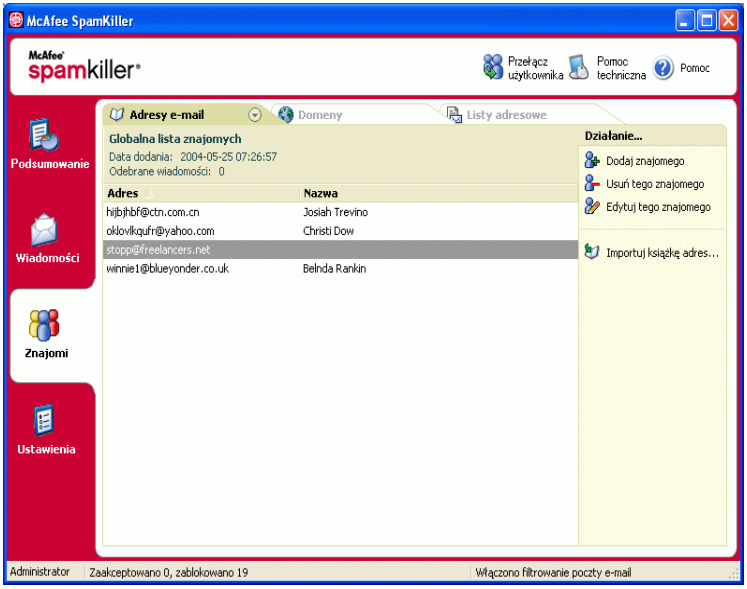
Otwieranie listy znajomych

1 Aby otworzyć listę znajomych, kliknij kartę **Znajomi**. Zostanie wyświetlona strona Znajomi (Ilustracja 5-3).

2 Kliknij kartę **Adres e-mail**, **Domeny** lub **Lista adresowa**. Zostanie wyświetlona globalna lista znajomych Aby wyświetlić listę osobistych znajomych, kliknij strzałkę w dół na jednej z tych kart, a następnie wybierz opcję **Lista osobistych znajomych**.

UWAGA

W przypadku, gdy na komputerze jest zainstalowany system operacyjny Windows 2000 lub Windows XP, a do programu SpamKiller dodano wielu użytkowników, użytkownicy z ograniczonymi uprawnieniami mogą przeglądać tylko listę osobistych znajomych.



Ilustracja 5-3. Strona Znajomi

Importowanie książek adresowych

Książki adresowe można importować do listy znajomych ręcznie lub automatycznie. Przy automatycznym importowaniu program SpamKiller może w regularnych odstępach czasu sprawdzać książki adresowe w celu wyszukania nowych adresów i automatycznie importować je do listy znajomych.

Książki adresowe można importować z następujących programów poczty e-mail:

- Microsoft Outlook (wersja 98 lub nowsza)
- Microsoft Outlook Express (wszystkie wersje)
- Netscape Communicator (wersja 6 lub nowsza, w przypadku eksportu do pliku LDIF)
- Qualcomm Eudora (wersja 5 lub nowsza)
- IncrediMail Xe
- MSN/Hotmail
- Wszystkie programy umożliwiające wyeksportowanie książki adresowej do pliku tekstowego.

Automatyczne importowanie książek adresowych

Listę osobistych znajomych można regularnie aktualizować, tworząc harmonogram importowania adresów z książek adresowych.

1. Kliknij kartę **Ustawienia**, a następnie opcję **Książki adresowe**. Zostanie wyświetlone okno dialogowe **Importuj książki adresowe** z listą książek adresowych, które są regularnie sprawdzane przez program SpamKiller i z których są importowane nowe adresy.
2. Kliknij przycisk **Dodaj**. Zostanie wyświetlone okno dialogowe **Harmonogram importowania**.
3. W polu **Typ** wybierz typ książki adresowej, która ma zostać zaimportowana, oraz jej źródło w polu **ródło**.
4. W polu **Harmonogram** wybierz, jak często program SpamKiller ma sprawdzać dostępność nowych adresów w książce adresowej.
5. Kliknij przycisk **OK**. Po zakończeniu aktualizacji nowe adresy pojawią się na liście osobistych znajomych.

Ręczne importowanie książek adresowych

Książkę adresową można ręcznie zaimportować do listy osobistych znajomych lub globalnej listy znajomych.

> **UWAGA**
> W przypadku, gdy na komputerze jest zainstalowany system operacyjny Windows 2000 lub Windows XP, a do programu SpamKiller dodano wielu użytkowników, należy zalogować się jako administrator, aby możliwe było dodanie znajomych do globalnej listy znajomych.

1. Kliknij kartę **Znajomi**, a następnie przycisk **Importuj książkę adresową**.

   Zostanie wyświetlone okno dialogowe **Importuj książkę adresową** z listą typów książek adresowych, które można zaimportować.

2. Wybierz typ książki adresowej, która ma zostać zaimportowana, lub kliknij przycisk **Przeglądaj**, aby zaimportować adresy zapisane w pliku.

   Aby zaimportować książkę adresową tylko do listy osobistych znajomych, należy zaznaczyć pole wyboru **Dodaj do listy osobistych znajomych**. Aby zaimportować książkę adresową tylko do globalnej listy znajomych, to pole wyboru nie może być zaznaczone.

3. Kliknij przycisk **Dalej**. Zostanie wyświetlona strona z monitem o potwierdzenie oraz liczbą adresów dodanych przez program SpamKiller.

4. Kliknij przycisk **Zakończ**. Adresy zostaną wyświetlone na globalnej liście znajomych lub liście osobistych znajomych.

Edycja informacji książki adresowej

Istnieje możliwość przeprowadzenia edycji informacji w książce adresowej, która została automatycznie zaimportowana.

1. Kliknij kartę **Ustawienia**, a następnie opcję **Książki adresowe**.
2. Zaznacz żądaną książkę adresową, a następnie kliknij przycisk **Edytuj**.
3. Zmień informacje w książce adresowej, a następnie kliknij przycisk **OK**.

Usuwanie książki adresowej z listy automatycznego importowania

Wpis książki adresowej można usunąć, jeśli program SpamKiller nie ma dłużej automatycznie importować z niej adresów.

1. Kliknij kartę **Ustawienia**, a następnie opcję **Książki adresowe**.
2. Zaznacz żądaną książkę adresową, a następnie kliknij opcję **Usuń**. Zostanie wyświetlone okno dialogowe z monitem o potwierdzenie.
3. Kliknij przycisk **Tak**, aby usunąć książkę adresową z listy.

Dodawanie znajomych

Aby mieć pewność, że wszystkie wiadomości wysyłane przez znajomych są odbierane, należy dodać ich nazwiska i adresy do listy znajomych. Znajomych można dodawać na następujących stronach: Znajomi, Zablokowana poczta e-mail, Zaakceptowana poczta e-mail. Do tego celu można także użyć programu Microsoft Outlook lub Outlook Express.

UWAGA
W przypadku, gdy na komputerze jest zainstalowany system operacyjny Windows 2000 lub Windows XP, a do programu SpamKiller dodano wielu użytkowników, należy zalogować się jako administrator, aby możliwe było dodanie znajomych do globalnej listy znajomych.

Dodawanie znajomych na stronach Zablokowana poczta e-mail i Zaakceptowana poczta e-mail

1. Kliknij kartę **Wiadomości**, a następnie kartę **Zablokowana poczta e-mail** lub **Zaakceptowana poczta e-mail**.

   Lub

   Z menu SpamKiller w programie Microsoft Outlook lub Outlook Express wybierz polecenie **Wyświetl blokowane wiadomości**, aby otworzyć stronę Zablokowana poczta e-mail dla danego konta.

   Zostanie wyświetlona strona Zablokowana poczta e-mail lub Zaakceptowana poczta e-mail.

2. Zaznacz wiadomość od nadawcy, który ma zostać dodany do listy znajomych, a następnie kliknij przycisk **Dodaj znajomego**.

3. W polu **Adres** wprowadź adres, który ma zostać dodany do listy znajomych. W polu **Adres** może znajdować się już adres z zaznaczonej wiadomości.

4. Wpisz imię i nazwisko znajomego w polu **Nazwa**.

5. Wybierz rodzaj adresu, który ma zostać dodany, w polu **Typ znajomego**:

   - **Pojedynczy adres e-mail** - nazwa i adres e-mail nadawcy są dodawane do sekcji Domeny na liście znajomych.
   - **Wszyscy w domenie** - nazwa domeny jest dodawana do sekcji **Domeny** na liście znajomych. Program SpamKiller akceptuje wszystkie wiadomości e-mail przychodzące ze wskazanej domeny.
   - **Lista adresowa** - adres jest dodawany do sekcji **Listy adresowe** na liście znajomych.

Aby dodać adres tylko do listy osobistych znajomych, zaznacz pole wyboru **Dodaj do listy osobistych znajomych**. Aby dodać adres tylko do globalnej listy znajomych, pozostaw to pole wyboru puste.

6 Kliknij przycisk **OK**. Wszystkie wiadomości od tej osoby zostaną oznaczone jako wiadomości od znajomego i pojawią się na stronie Zaakceptowana poczta e-mail.

Dodawanie znajomych na stronie Znajomi

1 Kliknij kartę **Znajomi**, a następnie kliknij opcję **Dodaj znajomego**. Zostanie wyświetlone okno dialogowe **Właściwości znajomego**.

2 W polu **Adres** wprowadź adres, który ma zostać dodany do listy znajomych.

3 Wpisz imię i nazwisko znajomego w polu **Nazwa**.

4 Wybierz rodzaj adresu, który ma zostać dodany, w polu **Typ znajomego**:

- **Pojedynczy adres e-mail** - nazwa i adres e-mail nadawcy są dodawane do sekcji Domeny na liście znajomych.
- **Wszyscy w domenie** - nazwa domeny jest dodawana do sekcji **Domeny** na liście znajomych. Program SpamKiller akceptuje wszystkie wiadomości e-mail przychodzące ze wskazanej domeny.
- **Lista adresowa** - adres jest dodawany do sekcji **Listy adresowe** na liście znajomych.

Aby dodać adres tylko do listy osobistych znajomych, zaznacz pole wyboru **Dodaj do listy osobistych znajomych**. Aby dodać adres tylko do globalnej listy znajomych, pozostaw to pole wyboru puste.

5 Kliknij przycisk **OK**. Wszystkie wiadomości od tej osoby zostaną oznaczone jako wiadomości od znajomego i pojawią się na stronie Zaakceptowana poczta e-mail.

Dodawanie znajomych w programie Microsoft Outlook

1 Otwórz konto poczty e-mail w programie Microsoft Outlook lub Outlook Express.

2 Zaznacz wiadomość od nadawcy, który ma zostać dodany do listy znajomych.

3 Kliknij ikonę na pasku narzędzi programu Microsoft Outlook. Wszystkie wiadomości od tej osoby zostaną oznaczone jako wiadomości od znajomego i pojawią się na stronie Zaakceptowana poczta e-mail.

Edycja znajomych

1 Kliknij kartę **Znajomi**, a następnie kartę **Adresy e-mail**, **Domeny** lub **Listy adresowe**.

Zostanie wyświetlona globalna lista znajomych Aby wyświetlić listę osobistych znajomych, kliknij strzałkę w dół na jednej z tych kart, a następnie wybierz opcję **Lista osobistych znajomych**.

UWAGA
Jeśli na komputerze jest zainstalowany system Windows 2000 lub Windows XP, a do programu SpamKiller dodano wielu użytkowników, tylko administratorzy mogą uzyskać dostęp do globalnej listy znajomych.

2 Zaznacz żądany adres na liście, a następnie kliknij przycisk **Edytuj**.

3 Zmień odpowiednie informacje, a następnie kliknij przycisk **OK**.

Usuwanie znajomych

Adresy, które nie są już potrzebne na liście znajomych, można usunąć.

1 Kliknij kartę **Znajomi**, a następnie kartę **Adresy e-mail**, **Domeny** lub **Listy adresowe**.

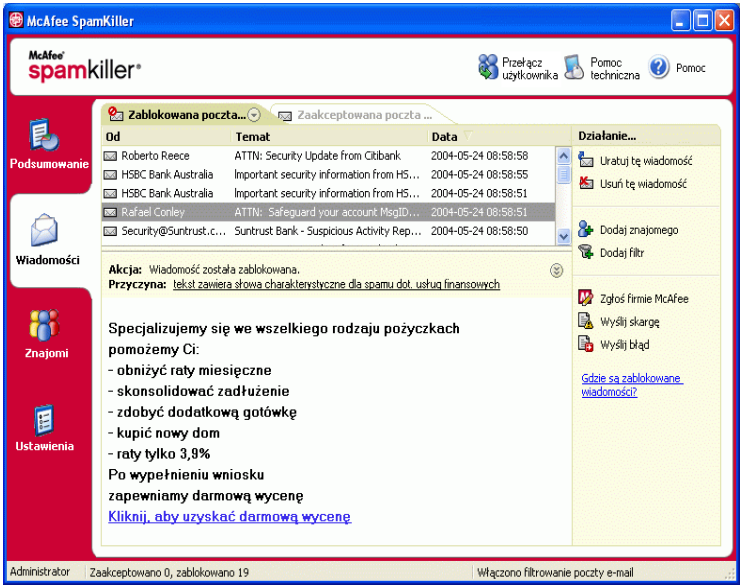
Zostanie wyświetlona globalna lista znajomych Aby wyświetlić listę osobistych znajomych, kliknij strzałkę w dół na jednej z tych kart, a następnie wybierz opcję **Lista osobistych znajomych**.

UWAGA
Jeśli na komputerze jest zainstalowany system Windows 2000 lub Windows XP, a do programu SpamKiller dodano wielu użytkowników, tylko administratorzy mogą uzyskać dostęp do globalnej listy znajomych.

2 Wybierz adres z listy, a następnie kliknij opcję **Usuń znajomego**. Zostanie wyświetlone okno dialogowe z monitem o potwierdzenie.

3 Kliknij przycisk **Tak**, aby usunąć znajomego.

Kliknij kartę **Wiadomości**, aby otworzyć stronę Wiadomości (Ilustracja 5-4) i uzyskać dostęp do zablokowanej i zaakceptowanej poczty. Strony Zablokowana poczta e-mail i Zaakceptowana poczta e-mail udostępniają podobne funkcje.



Ilustracja 5-4. Strona Wiadomości

Strona Zablokowana poczta e-mail

Kliknij kartę **Zablokowana poczta e-mail** na stronie Wiadomości, aby wyświetlić listę zablokowanych wiadomości.

> **UWAGA**
> Dostęp do zablokowanych wiadomości można także uzyskać w programie Microsoft Outlook, wybierając menu SpamKiller, a następnie klikając polecenie **Wyświetl blokowane wiadomości**.

Zablokowane wiadomości to wiadomości zidentyfikowane przez program SpamKiller jako spam, usunięte ze skrzynki odbiorczej i przeniesione na stronę Zablokowana poczta e-mail.

Na stronie Zablokowana poczta e-mail znajdują się wszystkie wiadomości będące spamem, które zostały usunięte z kont poczty e-mail. Aby wyświetlić zablokowane wiadomości e-mail dla określonego konta, należy kliknąć strzałkę w dół znajdującą się na karcie **Zablokowana poczta e-mail**, a następnie wybrać konto, które ma zostać wyświetlone.

Lista wiadomości będących spamem jest widoczna w górnym okienku komunikatów i uporządkowana według daty. Najnowsza wiadomość znajduje się na pierwszym miejscu. Dolne okienko podglądu zawiera treść zaznaczonej wiadomości.

UWAGA
Jeśli na komputerze jest zainstalowany system operacyjny Windows 2000 lub Windows XP, do programu SpamKiller dodano wielu użytkowników, a użytkownik korzystający aktualnie z programu ma ograniczone prawa, w dolnym okienku podglądu nie jest wyświetlana treść wiadomości.

W okienku środkowym znajdują się szczegółowe informacje o wiadomości. Kliknięcie strzałki w dół powoduje rozwinięcie okienka szczegółów wiadomości, umożliwiając wyświetlenie tekstu wiadomości i nagłówków w formacie macierzystym, w tym znaczników formatowania HTML. Okienko szczegółów wiadomości zawiera następujące informacje:

- **Akcja** - określa sposób przetwarzania wiadomości będącej spamem przez program SpamKiller. Akcja jest skojarzona z akcją filtru, który zablokował wiadomość.
- **Przyczyna** - określa, dlaczego program SpamKiller zablokował wiadomość. Kliknięcie przyczyny powoduje otwarcie edytora filtru i wyświetlenie filtru. W edytorze filtru można zobaczyć, czego filtr szuka we wiadomości oraz jakie działanie program SpamKiller podejmuje w odniesieniu do wiadomości znalezionych przez filtr.
- **Od** - nadawca wiadomości.
- **Data** - data wysłania wiadomości.
- **Do** - adresat wiadomości.
- **Temat** - temat wyświetlany w wierszu tematu wiadomości.

Jeśli wysłano ręcznie skargi lub komunikaty o błędach, w lewej kolumnie obok wiadomości znajdują się ikony.

- Wysłano skargę - wysłano skargę dotyczącą wiadomości.
- Wysłano komunikat o błędzie - wysłano komunikat o błędzie na adres zwrotny w wiadomości zidentyfikowanej jako spam.
- Wysłano skargę i komunikat o błędzie - wysłano zarówno skargę, jak i komunikat o błędzie.

Więcej informacji o położeniu zablokowanych wiadomości znajduje się w sekcji *Gdzie są zablokowane wiadomości* na str. 138.

Strona Zaakceptowana poczta e-mail

Kliknij kartę **Zaakceptowana poczta e-mail** na stronie Wiadomości, aby wyświetlić listę zaakceptowanych wiadomości.

Na stronie Zaakceptowana poczta e-mail są wyświetlane wszystkie wiadomości znajdujące się w skrzynkach odbiorczych wszystkich kont e-mail zalogowanego użytkownika. W przypadku kont MAPI strona Zaakceptowana poczta e-mail nie zawiera wewnętrznych wiadomości e-mail. Aby wyświetlić zaakceptowane wiadomości e-mail dla określonego konta, należy kliknąć strzałkę w dół znajdującą się na karcie **Zaakceptowana poczta e-mail**, a następnie wybrać konto, które ma zostać wyświetlone.

> **UWAGA**
> Program SpamKiller zaprojektowano do akceptowania legalnych wiadomości e-mail. Gdyby jednak na liście Zablokowana poczta e-mail znalazły się potrzebne wiadomości, można przenieść je z powrotem do skrzynki odbiorczej (oraz na listę Zaakceptowana poczta e-mail), zaznaczając wiadomości, a następnie klikając przycisk **Uratuj tę wiadomość**.

Podobnie jak w przypadku strony Zablokowana poczta e-mail, górne okienko komunikatów zawiera listę wiadomości uporządkowanych według daty. Dolne okienko podglądu zawiera treść zaznaczonej wiadomości.

W środkowym okienku wyświetlana jest informacja o tym, że wiadomość została wysłana przez osobę z listy znajomych lub że spełnia ona kryteria filtru, ale akcją filtru jest **Akceptuj** lub **Oznacz jako potencjalny spam**. Kliknięcie strzałki w dół powoduje rozwinięcie okienka szczegółów wiadomości, umożliwiając wyświetlenie tekstu wiadomości i nagłówków w formacie macierzystym, w tym znaczników formatowania HTML.

Okienko szczegółów wiadomości zawiera następujące informacje:

- **Akcja** - określa sposób przetwarzania wiadomości przez program SpamKiller.
- **Przyczyna** - jeśli program SpamKiller oznaczył wiadomość, informuje, dlaczego tak się stało.
- **Od** - nadawca wiadomości.
- **Data** - data wysłania wiadomości.
- **Do** - adresat wiadomości.
- **Temat** - temat wyświetlany w wierszu tematu wiadomości.

Obok wiadomości może pojawić się jedna z następujących ikon:

- Poczta od znajomego - program SpamKiller wykrył, że nadawca wiadomości znajduje się na liście znajomych. Wiadomość ma zostać zachowana.
- Potencjalny spam - wiadomość spełnia warunki filtru, dla którego ustawiono akcję Oznacz jako potencjalny spam.

- Wysłano skargę - wysłano skargę dotyczącą wiadomości.
- Wysłano komunikat o błędzie - wysłano komunikat o błędzie na adres zwrotny w wiadomości zidentyfikowanej jako spam.
- Wysłano skargę i komunikat o błędzie - wysłano zarówno skargę, jak i komunikat o błędzie.

Zadania dotyczące zablokowanej i zaakceptowanej poczty e-mail

W prawym okienku na stronach Zablokowana poczta e-mail i Zaakceptowana poczta e-mail znajduje się lista zadań, które można wykonać.

- **Blokuj tę wiadomość** - umożliwia usunięcie wiadomości ze skrzynki odbiorczej i przeniesienie jej na stronę Zablokowana poczta e-mail programu SpamKiller. (Ta opcja jest dostępna tylko na stronie Zaakceptowana poczta e-mail).
- **Uratuj tę wiadomość** - umożliwia umieszczenie wiadomości z powrotem w skrzynce odbiorczej (ta opcja dostępna jest tylko na stronie Zablokowana poczta e-mail). Zostanie wyświetlone okno dialogowe **Opcje ratowania**. Można automatycznie dodać nadawcę do listy znajomych i uratować wszystkie wiadomości od niego.
- **Usuń tę wiadomość** - umożliwia usunięcie zaznaczonej wiadomości.
- **Dodaj znajomego** - umożliwia dodanie imienia i nazwiska nadawcy, adresu e-mail, domeny lub listy adresowej do listy znajomych.
- **Dodaj filtr** - umożliwia utworzenie filtru.
- **Zgłoś firmie McAfee** - umożliwia poinformowanie firmy McAfee o otrzymanych wiadomościach zidentyfikowanych jako spam.
- **Wyślij skargę** - umożliwia wysłanie skargi dotyczącej spamu do administratora domeny nadawcy lub na inny wpisany adres e-mail.
- **Wyślij błąd** - umożliwia wysłanie komunikatu o błędzie na adres zwrotny wiadomości zidentyfikowanej jako spam.

Ratowanie wiadomości

Jeśli na stronie Zablokowana poczta e-mail lub w folderze SpamKiller programu Microsoft Outlook bądź Outlook Express znajdują się potrzebne wiadomości, można je przenieść z powrotem do skrzynki odbiorczej.

Ze strony Zablokowana poczta e-mail

1. Kliknij kartę **Wiadomości**, a następnie kartę **Zablokowana poczta e-mail**.

   Lub

   Z menu SpamKiller w programie Microsoft Outlook lub Outlook Express wybierz polecenie **Wyświetl blokowane wiadomości**, aby otworzyć stronę Zablokowana poczta e-mail dla danego konta.

2. Zaznacz wiadomość i kliknij przycisk **Uratuj tę wiadomość**  . Zostanie wyświetlone okno dialogowe **Opcje ratowania**.

   - **Dodaj znajomego** - pozwala dodać nadawcę do listy znajomych.
   - **Uratuj wszystko od tego nadawcy** - pozwala uratować wszystkie zablokowane wiadomości od nadawcy wybranej wiadomości.

3. Kliknij przycisk **OK**. Wiadomość zostanie z powrotem umieszczona w skrzynce odbiorczej i na stronie Zaakceptowana poczta e-mail.

W folderze SpamKiller programu Microsoft Outlook lub Outlook Express

Zaznacz żądane wiadomości i kliknij polecenie **Uratuj zaznaczenie** w menu programu SpamKiller lub na pasku narzędzi. Zaznaczone wiadomości zostaną przeniesione do skrzynki odbiorczej, a znacznik wiadomości (domyślnie [SPAM]) zostanie usunięty.

Blokowanie wiadomości

Istnieje możliwość zablokowania znajdujących się w skrzynce odbiorczej wiadomości będących spamem. Gdy wiadomość jest blokowana, program SpamKiller automatycznie tworzy filtr w celu usunięcia jej ze skrzynki odbiorczej. Wiadomości znajdujące się w skrzynce odbiorczej można blokować na stronie Zaakceptowana poczta e-mail lub w programie Microsoft Outlook bądź Outlook Express.

Ze strony Zaakceptowana poczta e-mail

1. Kliknij kartę **Wiadomości**, a następnie kliknij kartę **Zaakceptowana poczta e-mail**. Zostanie wyświetlona strona Zaakceptowana poczta e-mail z listą wiadomości znajdujących się aktualnie w skrzynce odbiorczej.
2. Zaznacz wiadomość i kliknij opcję **Blokuj tę wiadomość**. Wiadomość zostanie usunięta ze skrzynki odbiorczej i strony Zaakceptowana poczta e-mail, a jej kopia pojawi się na stronie Zablokowana poczta e-mail.

W programie Microsoft Outlook

W programie Microsoft Outlook wiadomości od użytkowników serwera Exchange są uznawane za bezpieczne i nie są filtrowane przez program SpamKiller. Filtrowane są tylko wiadomości ze źródeł zewnętrznych.

1. Otwórz skrzynkę odbiorczą programu Microsoft Outlook lub Outlook Express.
2. Zaznacz wiadomość, a następnie kliknij ikonę  . Kopia wiadomości zostanie umieszczona na stronie Zablokowana poczta e-mail.

Gdzie są zablokowane wiadomości

Domyślnie wiadomości rozpoznane jako spam są opatrywane znacznikiem [SPAM] i umieszczane w folderze SpamKiller programu Outlook lub Outlook Express albo w skrzynce odbiorczej. Wiadomości oznaczone są także wyświetlane na stronie Zaakceptowana poczta e-mail.

Ręczne usuwanie wiadomości

1. Kliknij kartę **Wiadomości**, a następnie kartę **Zablokowana poczta e-mail**.

   Lub

   Z menu SpamKiller w programie Microsoft Outlook lub Outlook Express wybierz polecenie **Wyświetl blokowane wiadomości**, aby otworzyć stronę Zablokowana poczta e-mail dla danego konta.
2. Zaznacz wiadomość, którą chcesz usunąć.
3. Kliknij opcję **Usuń tę wiadomość**. Zostanie wyświetlone okno dialogowe z monitem o potwierdzenie.
4. Kliknij przycisk **Tak**, aby usunąć wiadomość.

Zmiana sposobu przetwarzania wiadomości zidentyfikowanych jako spam

Wiadomość zidentyfikowana jako spam jest oznaczana lub blokowana. Spam jest usuwany z serwera za każdym razem, gdy program SpamKiller łączy się z nim.

Oznaczanie

W wierszu tematu wiadomości e-mail dodawana jest informacja [SPAM], a wiadomość jest przesyłana do skrzynki odbiorczej lub - w przypadku korzystania z programów Microsoft Outlook lub Outlook Express - folderu programu SpamKiller.

Blokowanie

Wiadomość jest usuwana i umieszczana na stronie Zablokowana poczta e-mail. Jeśli zablokowana została nieprawidłowa wiadomość, można ją uratować (patrz sekcja Ratowanie wiadomości).

Po upływie 15 dni program SpamKiller automatycznie usuwa zablokowane wiadomości ze strony Zablokowana poczta e-mail. Można jednak samodzielnie określić częstotliwość usuwania zablokowanych wiadomości.

Program SpamKiller nie usuwa automatycznie wiadomości ze strony Zaakceptowana poczta e-mail, ponieważ na tej stronie są wyświetlane wiadomości aktualnie znajdujące się w skrzynce odbiorczej.

Modyfikowanie sposobu przetwarzania wiadomości zidentyfikowanych jako spam przez program SpamKiller

1. Kliknij kartę **Ustawienia**, a następnie ikonę **Opcje filtrowania**.
2. Kliknij kartę **Przetwarzanie**.
   - **Umieść spam w skrzynce Zablokowana poczta e-mail** - wiadomości zidentyfikowane jako spam są usuwane ze skrzynki odbiorczej i przenoszone na stronę Zablokowana poczta e-mail programu SpamKiller.
   - **Oznacz jako spam i zachowaj w skrzynce odbiorczej** - jest to ustawienie domyślne. Wiadomości zidentyfikowane jako spam pozostają w skrzynce odbiorczej, ale w ich wierszu tematu dodawana jest informacja [SPAM].

     Zachowaj zablokowane wiadomości e-mail przez ____ dni - zablokowane wiadomości pozostają na stronie Zablokowana poczta e-mail przez określony czas.

     Zachowaj zaakceptowane wiadomości e-mail przez ____ dni - zaakceptowane wiadomości pozostają na stronie Zaakceptowana poczta e-mail przez określony czas.
3. Kliknij przycisk **OK**.

Korzystanie z filtru AntiPhishing

Niechciana poczta e-mail jest klasyfikowana jako spam (wiadomości e-mail nakłaniające do zakupów) lub phishing (wiadomości e-mail nakłaniające do podania informacji osobistych fałszywej lub potencjalnie fałszywej witrynie sieci Web).

Filtr McAfee AntiPhishing zabezpiecza użytkownika przed witrynami sieci Web znajdującymi się na czarnej liście (witrynami sieci Web, które są źródłami ataków typu „phishing", lub podobnymi fałszywymi witrynami) lub na szarej liście (witryn zawierających niebezpieczną treść lub łącza do witryn sieci Web na czarnej liście).

W przypadku wykrycia próby przejścia na fałszywą lub potencjalnie fałszywą witrynę sieci Web następuje przekierowanie na stronę filtru McAfee AntiPhishing.

Aby zmienić ustawienia AntiPhishing, wykonaj następujące czynności:

1. Uruchom program Internet Explorer.
2. W menu **Narzędzia** wybierz opcję **McAfee AntiPhishing Filter**.

- **Włącz filtrowanie witryn sieci Web** - ta opcja jest domyślnie włączona. Aby wyłączyć filtrowanie AntiPhishing, należy usunąć zaznaczenie tego pola wyboru.
- **Zezwalaj na dostęp do witryn sieci Web na czarnej liście** - umieszcza łącze na stronie przekierowania umożliwiające dostęp do witryn na czarnej liście. Kliknięcie tego łącza powoduje przejście na żądaną witrynę sieci Web.
- **Zezwalaj na dostęp do witryn sieci Web na szarej liście** - umieszcza łącze na stronie przekierowania umożliwiające dostęp do witryn na szarej liście. Kliknięcie tego łącza powoduje przejście na żądaną witrynę sieci Web.

3. Po zakończeniu kliknij przycisk **OK**.

Dodawanie kontaktów do listy znajomych

Patrz *Dodawanie znajomych na stronach Zablokowana poczta e-mail i Zaakceptowana poczta e-mail* na str. 130.

Dodawanie filtrów

Więcej informacji o filtrach zamieszczono w temacie *Korzystanie z filtrów* w systemie pomocy w trybie online.

1. Aby utworzyć filtr globalny, kliknij kartę **Ustawienia**, zaznacz opcję **Filtry globalne** i kliknij przycisk **Dodaj**.

   Lub

   Aby utworzyć filtr osobisty, kliknij kartę **Ustawienia**, zaznacz opcję **Filtry osobiste** i kliknij przycisk **Dodaj**.

Lub

Kliknij kartę **Wiadomości**, następnie kliknij kartę **Zablokowana poczta e-mail** lub **Zaakceptowana poczta e-mail**, po czym kliknij opcję **Dodaj filtr**.

2 Kliknij przycisk **Dodaj**, aby rozpocząć tworzenie warunku filtru. Zostanie wyświetlone okno dialogowe **Warunek filtru**.

3 Utwórz warunek filtru, wykonując poniższe czynności:

Warunek filtru to wyrażenie określające, czego program SpamKiller ma szukać w wiadomości. W przykładowym warunku „Tekst wiadomości zawiera: hipoteka" filtr wyszukuje wiadomości zawierające słowo „hipoteka". Więcej informacji o warunkach filtru zamieszczono w temacie *Warunki filtru* w systemie pomocy w trybie online.

a Wybierz typ warunku w pierwszym polu.

b Wybierz lub wprowadź wartości w następnych polach.

c Jeśli dostępne są poniższe opcje, zaznacz odpowiednie pola wyboru, aby dokładniej zdefiniować warunek filtru.

Szukaj także w kodach formatowania - ta opcja dostępna jest tylko wtedy, gdy zażądano przeszukiwania tekstu wiadomości. Po zaznaczeniu tego pola wyboru program SpamKiller wyszukuje wskazany tekst zarówno w tekście wiadomości, jak i kodach formatowania wiadomości.

Dopasuj warianty - ta opcja umożliwia programowi SpamKiller wykrywanie słów, które zostały celowo błędnie napisane przez nadawców spamu. Na przykład słowo „normalny" może zostać błędnie zapisane jako „n0rma1ny" w celu oszukania filtrów.

Wyrażenia regularne - ta opcja umożliwia określenie wzorów znaków używanych w warunkach filtru. Aby sprawdzić dany wzór znaków, kliknij opcję **Testuj wyrażenie regularne**.

Rozróżnianie wielkości znaków - ta opcja jest dostępna tylko w przypadku warunków z wprowadzoną wartością. Jeśli to pole wyboru zostanie zaznaczone, program SpamKiller będzie rozróżniał wielkie i małe litery we wpisanej wartości.

d Kliknij przycisk **OK**.

4 Utwórz inny warunek filtru zgodnie z poniższymi instrukcjami lub przejdź do sekcji krok 5, aby wybrać akcję filtru.

   a Kliknij przycisk **Dodaj**, a następnie utwórz warunek filtru. Po zakończeniu tworzenia warunku filtru kliknij przycisk **OK**.

   Oba warunki filtru są widoczne na liście Warunki filtru i są połączone operatorem **and**. Operator **and** wskazuje, że program SpamKiller będzie wyszukiwał wiadomości spełniające *obydwa* warunki filtru. Jeśli program SpamKiller ma wyszukiwać wiadomości spełniające tylko jeden ze zdefiniowanych warunków, należy zmienić operator **i** na **lub**. W tym celu należy kliknąć operator **i**, a następnie wybrać **lub** w wyświetlonym polu.

   b Kliknij przycisk **Dodaj**, aby utworzyć inny warunek, lub przejdź do sekcji krok 5, aby wybrać akcję filtru.

   W przypadku utworzenia trzech lub więcej warunków filtru można je pogrupować i utworzyć frazy. Przykłady grupowania można znaleźć w temacie *Grupowanie filtrów* w systemie pomocy w trybie online.

   Aby zgrupować warunki filtru, zaznacz wybrany warunek filtru, a następnie kliknij opcję **Grupuj**. Aby rozgrupować warunki filtru, zaznacz zgrupowany warunek, a następnie kliknij opcję **Rozgrupuj**.

5 Wybierz akcję filtru w polu **Akcja**. Akcja filtru określa, jak program SpamKiller ma przetwarzać wiadomości znalezione przez filtr. Więcej informacji można znaleźć w temacie *Akcje filtru* w systemie pomocy w trybie online.

6 Kliknij przycisk **Zaawansowane**, aby wybrać zaawansowane opcje filtru (wybór opcji zaawansowanych nie jest wymagany). Więcej informacji można znaleźć w temacie *Zaawansowane opcje filtrów* w systemie pomocy w trybie online.

7 Po zakończeniu tworzenia filtru kliknij przycisk **OK**.

UWAGA
Aby przeprowadzić edycję warunku, zaznacz go i kliknij opcję **Edytuj**. Aby usunąć warunek, zaznacz go i kliknij opcję **Usuń**.

Wyrażenia regularne

Wyrażenia regularne są dostępne tylko w przypadku następujących warunków filtru: **Temat**, **Tekst wiadomości**, **Co najmniej jedno z następujących wyrażeń**.

Podczas definiowania warunków filtru można użyć poniższych sekwencji lub znaków specjalnych jako wyrażeń regularnych. Na przykład:

- Wyrażenie regularne **[0-9]*\,[0-9]+** powoduje wyszukanie liczb zmiennopozycyjnych w zapisie bez wykładnika. Powyższe wyrażenie regularne znajdzie następujące elementy: „12,12”, „.1212” i „12,0”, ale nie „12” i „12”.
- Wyrażenie regularne **\D*[0-9]+\D*** powoduje wyszukanie wszystkich słów zawierających liczby: „SpamKi11er” i „V1AGRA”, ale nie „SpamKiller” i „VIAGRA”.

****

Oznacza następny znak jako znak specjalny lub literał. Na przykład „n” powoduje wyszukanie znaku „n”. „\n” oznacza znak nowego wiersza. Sekwencja „\\” powoduje wyszukanie znaku „\”, natomiast „\(” - znaku „(”.

^

Oznacza początek ciągu.

$

Oznacza koniec ciągu.

*****

Wyszukuje znak poprzedzający powtarzający się zero lub więcej razy. Na przykład „zo*” powoduje wyszukanie „z” lub „zoo”.

+

Wyszukuje znak poprzedzający powtarzający się jeden lub więcej razy. Na przykład „zo+” powoduje wyszukanie „zoo”, ale nie „z”.

?

Wyszukuje znak poprzedzający występujący powtarzający się zero lub jeden raz. Na przykład „m?ig?” powoduje wyszukanie „ig” w wyrazie „nigdy”.

.

Oznacza dowolny jeden znak z wyjątkiem znaku nowego wiersza.

(wzór)

Wyszukuje wzór i zapamiętuje znalezione wystąpienie. Wyszukany podłańcuch można uzyskać z wynikowej kolekcji wyszukanych wystąpień za pomocą numeru [0]...[n]. Aby wyszukać znaki nawiasów ( ), należy użyć wyrażenia „\(” lub „\)”.

x|y

Wyszukuje wartość x lub y. Na przykład „s|tama” powoduje wyszukanie „s” lub „tama”. „(s|t)ama” powoduje wyszukanie „sama” lub „tama”.

{n}

n jest liczbą całkowitą nieujemną. Wyszukuje sekwencję dokładnie n powtórzeń. Na przykład „o{2}” nie powoduje wyszukania „o” w wyrazie „Robert”, ale powoduje wyszukanie pierwszych dwóch o w wyrazie „goooool”.

{n,}

n jest liczbą całkowitą nieujemną. Wyszukuje sekwencję co najmniej n powtórzeń. Na przykład „o{2,}” nie powoduje wyszukania „o” w wyrazie „Robert”, ale powoduje wyszukanie wszystkich o w wyrazie „goooool”. Wyrażenie „o{1,}” jest równoważne wyrażeniu „o+”. „o{0,}” jest równoważne wyrażeniu „o*”.

{n,m}

m oraz n są liczbami całkowitymi nieujemnymi. Wyszukuje sekwencję co najmniej n i maksymalnie m powtórzeń. Na przykład „o{1,3}” powoduje wyszukanie pierwszych trzech o w wyrazie „goooool”. Wyrażenie „o{0,1}” jest równoważne wyrażeniu „o?”.

[xyz]

Zestaw znaków. Wyszukuje dowolny ze znaków w nawiasie kwadratowym. Na przykład „[abc]” powoduje wyszukanie „a” w wyrazie „jasny”.

[^xyz]

Wykluczenie zestawu znaków. Wyszukuje dowolny ze znaków, który nie jest wymieniony w nawiasie. Na przykład „[^abc]” powoduje wyszukanie „p” w wyrazie „paczka”.

[a-z]

Zakres znaków. Wyszukuje dowolny ze znaków w określonym zakresie. Na przykład „[a-z]” powoduje wyszukanie dowolnej małej litery alfabetu w zakresie od „a” do „z”.

[^m-z]

Wykluczenie przedziału znaków. Wyszukuje dowolny ze znaków, który nie znajduje się w określonym przedziale. Na przykład „[^m-z]” powoduje wyszukanie dowolnego znaku, który nie znajduje się w przedziale od „m” do „z”.

\b

Wyszukuje granicę słowa, czyli miejsce pomiędzy słowem a spacją. Na przykład „er\b” powoduje wyszukanie „er” w słowie „rower”, ale nie powoduje wyszukania „er” w słowie „roweru”.

\B

Wyszukuje granicę, która nie jest granicą słowa. „we*r\B” powoduje wyszukanie „wer” w wyrażeniu „nowa wersja”.

\d

Oznacza cyfrę Równoważne wyrażeniu [0-9].

\D

Oznacza znak inny niż cyfra Równoważne wyrażeniu [^0-9].

\f

Oznacza znak końca strony.

\n

Oznacza znak nowego wiersza.

\r

Oznacza znak powrotu karetki.

\s

Oznacza dowolny odstęp, taki jak znak spacji, znak tabulacji, znak końca strony itd. Równoważne wyrażeniu „[\f\n\r\t\v]”.

\S

Oznacza dowolny znak niebędący odstępem. Równoważne wyrażeniu „[^ \f\n\r\t\v]”.

\t

Oznacza znak tabulacji.

\v

Oznacza znak tabulatora w pionie.

\w

Oznacza dowolny znak alfanumeryczny lub podkreślenie. Równoważne wyrażeniu „[A-Za-z0-9_]”.

\W

Oznacza dowolny znak, który nie występuje w słowie. Równoważne wyrażeniu „[^A-Za-z0-9_]”.

\num

Wstawia wartość określoną przez num, gdzie num jest dodatnią liczbą całkowitą. Odwołuje się do zapamiętanych wyników wyszukiwania. Na przykład „(.)\1” powoduje wyszukanie dwóch kolejnych identycznych znaków.

\n

Oznacza znak określony przez wartość n, gdzie n jest liczbą ósemkową. Liczby ósemkowe muszą zawierać 1, 2 lub 3 cyfry. Na przykład zarówno „\11”, jak i „\011” oznaczają znak tabulatora. „\0011” jest równoważne wyrażeniu „\001” & „1”. Wartości ósemkowe nie mogą być większe niż 256. W przeciwnym razie wyrażenie tworzą tylko dwie pierwsze cyfry. Umożliwia używanie kodów ASCII w wyrażeniach regularnych.

\xn

Oznacza znak określony przez wartość n, gdzie n jest liczbą szesnastkową. Liczby szesnastkowe muszą zawierać dokładnie dwie cyfry. Na przykład „\x41” oznacza znak „A”. „\x041” jest równoważne wyrażeniu „\x04” & „1”. Umożliwia używanie kodów ASCII w wyrażeniach regularnych.

Zgłaszanie spamu firmie McAfee

Spam można zgłosić firmie McAfee, która przeprowadzi odpowiednie analizy i przygotuje aktualizacje filtrów.

1. Kliknij kartę **Wiadomości**, a następnie kartę **Zablokowana poczta e-mail** lub **Zaakceptowana poczta e-mail**. Zostanie wyświetlona strona Zablokowana poczta e-mail lub Zaakceptowana poczta e-mail.
2. Zaznacz wiadomość, a następnie kliknij opcję **Zgłoś firmie McAfee**. Zostanie wyświetlone okno dialogowe z monitem o potwierdzenie.
3. Kliknij przycisk **Tak**. Wiadomość zostanie wysłana automatycznie do firmy McAfee.

Ręczne wysyłanie skarg

Wysłanie skargi do nadawcy spamu zapobiega wysyłaniu przez niego kolejnych niechcianych wiadomości. Więcej informacji o skargach znajduje się w temacie *Wysyłanie skarg i komunikatów o błędach* w systemie pomocy w trybie online.

1. Kliknij kartę **Wiadomości**, a następnie kartę **Zablokowana poczta e-mail** lub **Zaakceptowana poczta e-mail**. Zostanie wyświetlona lista wiadomości.
2. Zaznacz wiadomość, na którą chcesz złożyć skargę, a następnie kliknij opcję **Wyślij skargę**. Zostanie wyświetlone okno dialogowe **Wyślij skargę**.
3. Wybierz, do kogo ma zostać wysłana skarga.

   OSTRZEŻENIE
   W większości przypadków nie należy wybierać opcji **Nadawca**. Wysłanie skargi do nadawcy spamu potwierdza poprawność adresu e-mail, co może skutkować otrzymywaniem większej liczby niechcianych wiadomości od danego nadawcy.
4. Kliknij przycisk **Dalej**, a następnie postępuj zgodnie z instrukcjami wyświetlanymi w oknach dialogowych.

Wysyłanie komunikatów o błędach

Więcej informacji o komunikatach o błędach znajduje się w temacie *Wysyłanie skarg i komunikatów o błędach* w systemie pomocy w trybie online.

Wysłanie komunikatu o błędzie do nadawcy spamu pozwala zapobiec wysyłaniu przez niego kolejnych niechcianych wiadomości.

Ręczne wysyłanie komunikatu o błędzie

1. Kliknij kartę **Wiadomości**, a następnie kartę **Zablokowana poczta e-mail** lub **Zaakceptowana poczta e-mail**. Zostanie wyświetlona lista wiadomości.
2. Aby wysłać komunikat o błędzie dotyczący konkretnej wiadomości będącej spamem, zaznacz tę wiadomość, a następnie kliknij opcję **Wyślij błąd**. Komunikat o błędzie zostanie wysłany na adres zwrotny wiadomości rozpoznanej jako spam.

Program SpamKiller nie może skomunikować się ze swoim serwerem

Komunikacja z serwerem jest niemożliwa, jeśli serwer programu SpamKiller nie może zostać uruchomiony lub jest blokowany przez inną aplikację.

Ręczne uruchamianie serwera SpamKiller

Poniższe informacje dotyczą tylko użytkowników systemów Microsoft Windows 2000 i XP.

1. Kliknij przycisk **Start** i wybierz polecenie **Uruchom**.
2. Wpisz SERVICES.MSC i kliknij przycisk **OK**.
3. Kliknij prawym przyciskiem myszy opcję McAfee SpamKiller Server i wybierz polecenie **Uruchom**. Zostanie uruchomiona usługa serwera.

Serwer SpamKiller jest blokowany przez zaporę lub program do filtrowania danych z Internetu

Jeśli usługa SpamKiller Server jest uruchomiona i działa, należy wykonać następujące czynności

1. Sprawdź, czy program SpamKiller Server i/lub program MSKSrvr.exe mają pełny dostęp do wszystkich zainstalowanych zapór programowych, w tym McAfee Personal Firewall.
2. Sprawdź, czy LocalHost i/lub adres 127.0.0.1 nie są blokowane lub nie jest do nich zabroniony dostęp przez zainstalowane zapory, w tym program McAfee Personal Firewall.
3. Wyłącz programy zapewniające ochronę prywatności w Internecie lub filtrujące dane pobierane z Internetu.

Nie można połączyć się z serwerem poczty elektronicznej

Jeśli usługa SpamKiller Server bezskutecznie próbuje nawiązać połączenie z serwerem POP3, należy wykonać poniższe czynności.

Sprawdzanie połączenia z Internetem

Połączenie telefoniczne

1. Kliknij przycisk **Kontynuuj wykonywaną czynność** w oknie komunikatu o błędzie (w razie potrzeby).
2. Nawiąż połączenie z Internetem.
3. Utrzymaj połączenie przez co najmniej 15 minut, aby sprawdzić, czy komunikat zostanie ponownie wyświetlony.

Połączenie szerokopasmowe (kablowe, DSL)

1. Kliknij przycisk **Kontynuuj wykonywaną czynność** w oknie komunikatu o błędzie (w razie potrzeby).
2. Sprawdź, czy komputer jest połączony z Internetem, otwierając dowolną witrynę sieci Web.

Sprawdzanie adresu serwera POP3 do obsługi programu SpamKiller

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż polecenie **SpamKiller**, a następnie wybierz polecenie **Ustawienia**.
2. Kliknij opcję **Konta e-mail**.
3. Zaznacz konto e-mail podane w oknie komunikatu o błędzie.
4. Kliknij przycisk **Edytuj**.
5. Wybierz kartę **Serwery**.
6. Sprawdź adres serwera w polu **Przychodząca poczta e-mail** i porównaj go z adresem serwera poczty przychodzącej wskazanym przez dostawcę usług internetowych (ISP) do obsługi konta poczty e-mail. Adresy serwera powinny być takie same.
7. Sprawdź poprawność hasła, ponownie wprowadzając hasło podane przez dostawcę usług internetowych dla danego konta e-mail.
8. Kliknij przycisk **OK**.
9. Kliknij przycisk **Zamknij**.

Skorowidz

E

F

H

I

K

L

M

N

O

P

R

S

T

U

W

Z