McAfee®

Total Protection 2008

Podręcznik użytkownika

Spis treści

ROZDZIAŁ 1

McAfee Total Protection

Pakiet McAfee Total Protection zapewnia wszechstronną profilaktyczną ochronę 12 w 1, zabezpieczając to, co cenne. Program McAfee SiteAdvisor Plus osłania komputer przed interakcjami z niebezpiecznymi witrynami sieci Web. Dzięki stałym automatycznym aktualizacjom usługa firmy McAfee ułatwia zapobieganie atakom hakerów przy użyciu najnowszej ochrony. Ponadto umożliwia tworzenie kopii zapasowych i przywracanie danych w przypadku awarii komputera lub niefortunnych pomyłek.

Pakiet McAfee Total Protection udostępnia funkcje ochrony rodzicielskiej w środowisku wielu użytkowników oraz zapewnia ochronę przed kradzieżą tożsamości, spamem i oszustwami. Dzięki usłudze zabezpieczeń firmy McAfee zawsze dostępne są najnowsze rozszerzenia i aktualizacje informacji o zagrożeniach umożliwiające blokowanie wirusów i oprogramowania szpiegującego. Dostępna jest też zapora, której celem jest eliminowanie zagrożeń ze strony hakerów.

W tym rozdziale

ROZDZIAŁ 2

Program McAfee SecurityCenter

Program McAfee SecurityCenter umożliwia monitorowanie stanu zabezpieczeń komputera, przedstawia na bieżąco informacje o tym, czy usługi ochrony przed wirusami, oprogramowaniem szpiegującym, ochrona poczty e-mail oraz zapora są aktualne, a także podejmuje odpowiednie działania w celu zabezpieczenia przez powstaniem potencjalnych luk w zabezpieczeniach. Zawiera narzędzia i elementy nawigacyjne potrzebne do koordynowania wszystkich obszarów ochrony komputera i zarządzania nimi.

Przed rozpoczęciem konfigurowania mechanizmów ochrony komputera i zarządzania nimi należy zapoznać się z interfejsem oprogramowania SecurityCenter i przeanalizować różnice między stanami ochrony, jej rodzajami oraz usługami. Następnie należy zaktualizować program SecurityCenter w celu uzyskania z firmy McAfee najnowszej wersji mechanizmów ochronnych.

Po zakończeniu wstępnych zadań konfiguracyjnych można używać programu SecurityCenter do monitorowania stanu ochrony komputera. Jeśli ten pakiet wykryje problem dotyczący ochrony, ostrzega użytkownika, aby ten mógł go wyeliminować lub zignorować (w zależności od stopnia zagrożenia). Można również przeglądać w dzienniku zdarzenia programu SecurityCenter, takie jak zmiany w konfiguracji skanowania w poszukiwaniu wirusów.

Uwaga: Program SecurityCenter zgłasza krytyczne i niekrytyczne problemy dotyczące ochrony natychmiast po ich wykryciu. Jeśli potrzebna jest pomoc w diagnozowaniu problemów dotyczących ochrony, można uruchomić narzędzie McAfee Virtual Technician.

W tym rozdziale

Funkcje programu SecurityCenter

Program SecurityCenter jest wyposażony w następujące funkcje:

Uproszczone informacje o stanie ochrony

Łatwe przeglądanie informacji o stanie ochrony komputera, sprawdzanie dostępności aktualizacji i usuwanie potencjalnych problemów związanych z ochroną.

Zautomatyzowane aktualizacje i uaktualnienia

Automatyczne pobieranie i instalowanie aktualizacji zarejestrowanych programów. Gdy tylko zostaje udostępniona nowa wersja zarejestrowanego programu firmy McAfee, użytkownik w okresie subskrypcji otrzymuje ją bezpłatnie w sposób automatyczny, co zapewnia ciągłą skuteczną ochronę przed najnowszymi zagrożeniami.

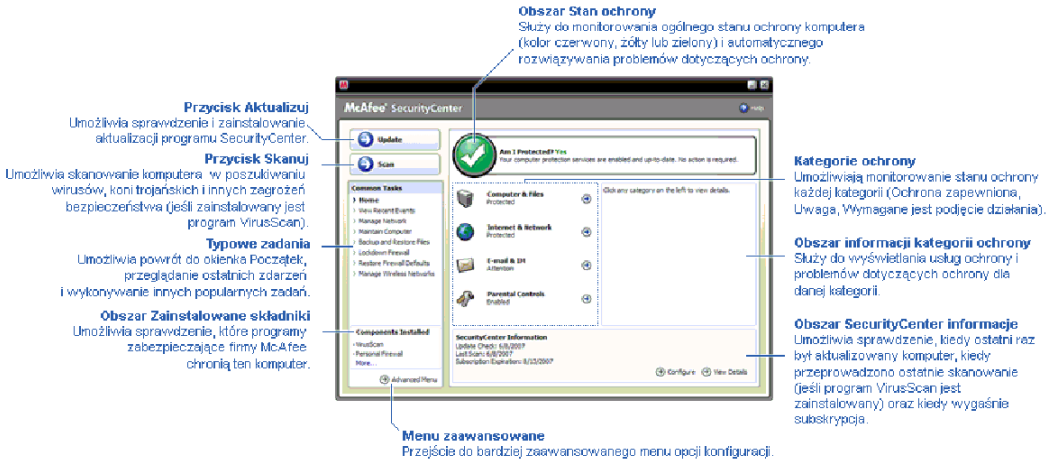
Wyświetlanie na bieżąco alertów

Alerty zabezpieczeń powiadamiają o epidemiach wirusowych i zagrożeniach bezpieczeństwa oraz umożliwiają usunięcie, zneutralizowanie zagrożenia i uzyskanie dodatkowych informacji na jego temat.

ROZDZIAŁ 3

Korzystanie z programu SecurityCenter

Przed rozpoczęciem korzystania z programu SecurityCenter należy zapoznać się ze wszystkimi składnikami i obszarami konfiguracji, które służą do zarządzania stanem ochrony komputera. Aby uzyskać więcej informacji na temat terminologii użytej na tej ilustracji, zobacz część *Jak działa stan ochrony* (strona 8) i część *Jak działają kategorie ochrony* (strona 9). Następnie można przejrzeć informacje na temat konta McAfee i sprawdzić ważność subskrypcji.



W tym rozdziale

Jak działa stan ochrony

Informacje o stanie ochrony komputera są widoczne w obszarze stanu ochrony w okienku Początek programu SecurityCenter. W tym miejscu można się dowiedzieć, czy komputer jest całkowicie chroniony przed najnowszymi zagrożeniami bezpieczeństwa i czy na jego stan mogą mieć wpływ zewnętrzne ataki, inne programy zabezpieczające oraz programy, które korzystają z sieci Internet.

Stanowi ochrony komputera mogą odpowiadać kolory: czerwony, żółty lub zielony.

Stan ochrony	Opis
Czerwony	Komputer nie jest chroniony. Obszar stanu ochrony w okienku Początek programu SecurityCenter jest czerwony, co oznacza, że komputer nie jest chroniony. Program SecurityCenter zgłasza co najmniej jeden problem z zabezpieczeniami o znaczeniu krytycznym. W celu uzyskania pełnej ochrony należy wyeliminować wszystkie problemy z zabezpieczeniami o znaczeniu krytycznym należące do wszystkich kategorii ochrony (stan kategorii problemu jest wyświetlany jako **Wymagane jest podjęcie działania**, również w kolorze czerwonym). Aby uzyskać więcej informacji na temat sposobu rozwiązywania problemów z ochroną, zobacz część *Naprawianie problemów dotyczących ochrony* (strona 18).
Żółty	Komputer jest częściowo chroniony. Obszar stanu ochrony w okienku Początek programu SecurityCenter jest żółty, co oznacza, że komputer nie jest chroniony. Program SecurityCenter zgłasza co najmniej jeden problem z zabezpieczeniami o znaczeniu mniejszym niż krytyczne. W celu uzyskania pełnej ochrony należy wyeliminować lub zignorować niekrytyczne problemy z zabezpieczeniami należące do wszystkich kategorii ochrony. Aby uzyskać więcej informacji na temat sposobu rozwiązywania lub ignorowania problemów z zabezpieczeniami, zobacz część *Naprawianie lub ignorowanie problemów dotyczących ochrony* (strona 17).
Zielony	Komputer jest w pełni chroniony. Obszar stanu ochrony w okienku Początek programu SecurityCenter jest zielony, co oznacza, że komputer jest chroniony. Program SecurityCenter nie zgłasza żadnego problemu z zabezpieczeniami o znaczeniu krytycznym lub mniejszym. Poszczególne kategorie ochrony zawierają listy usług, które chronią komputer.

Jak działają kategorie ochrony

Usługi ochrony oprogramowania SecurityCenter dzielą się na cztery kategorie: Komputer i pliki, Internet i sieć, Poczta e-mail i wiadomości błyskawiczne oraz Funkcje ochrony rodzicielskiej. Te kategorie ułatwiają przeglądanie i konfigurowanie usług związanych z zabezpieczeniami, które chronią komputer.

Po kliknięciu nazwy kategorii można skonfigurować należące do niej usługi związane z zabezpieczeniami oraz wyświetlić informacje o problemach wykrytych przez te usługi. Jeśli stan ochrony komputera jest czerwony lub żółty, co najmniej w jednej kategorii jest wyświetlany komunikat *Wymagane jest podjęcie działania* lub *Uwaga*, co wskazuje na wykrycie problemu w danej kategorii przez program SecurityCenter. Aby uzyskać więcej informacji na temat stanu ochrony, zobacz część *Jak działa stan ochrony* (strona 8).

Kategoria ochrony	Opis
Komputer i pliki	Kategoria Komputer i pliki umożliwia skonfigurowanie następujących usług ochrony: ▪ Ochrona przed wirusami ▪ Ochrona przed programami potencjalnie niepożądanymi ▪ Monitory systemu ▪ Ochrona systemu Windows
Internet i sieć	Kategoria Internet i sieć umożliwia skonfigurowanie następujących usług ochrony: ▪ Ochrona przy użyciu zapory ▪ Ochrona tożsamości
Poczta e-mail i wiadomości błyskawiczne	Kategoria Poczta e-mail i wiadomości błyskawiczne umożliwia skonfigurowanie następujących usług ochrony: ▪ Ochrona poczty e-mail ▪ Ochrona przed spamem
Funkcje ochrony rodzicielskiej	Kategoria Funkcje ochrony rodzicielskiej umożliwia skonfigurowanie następujących usług ochrony: ▪ Blokowanie zawartości

Jak działają usługi ochrony

Usługi ochrony są podstawowymi składnikami programu SecurityCenter. Są one konfigurowane przez użytkownika w celu zapewnienia ochrony komputera. Usługi ochrony odpowiadają bezpośrednio programom firmy McAfee. Na przykład po zainstalowaniu programu VirusScan stają się dostępne następujące usługi: Ochrona przed wirusami, Ochrona przed programami potencjalnie niepożądanymi, Monitory systemu oraz Ochrona systemu Windows. Aby uzyskać szczegółowe informacje na temat tych konkretnych usług ochrony, zobacz Pomoc oprogramowania VirusScan.

Domyślnie wszystkie usługi ochrony związane z programem są włączone po jego zainstalowaniu, można jednak każdą z nich wyłączyć w dowolnym momencie. Na przykład po zainstalowaniu programu Privacy Service są włączane usługi Blokowanie zawartości oraz Ochrona tożsamości. Jeśli użytkownik nie zamierza używać usługi Blokowanie zawartości, może wyłączyć ją całkowicie. Można również tymczasowo wyłączyć usługę ochrony, wykonując zadania konfiguracyjne lub konserwacyjne.

Zarządzanie kontem McAfee

Kontem McAfee można łatwo zarządzać za pomocą programu SecurityCenter, uzyskując dostęp do informacji o koncie i przeglądając je oraz sprawdzając bieżący stan subskrypcji.

Uwaga: Jeśli programy firmy McAfee zostały zainstalowane z dysku CD, należy zarejestrować je w witrynie sieci Web firmy McAfee, aby umożliwić skonfigurowanie lub zaktualizowanie konta McAfee. Tylko wtedy użytkownik jest upoważniony do otrzymywania regularnych automatycznych aktualizacji programu.

Zarządzanie kontem McAfee

Dostęp do informacji o koncie McAfee (Moje konto) można łatwo uzyskać za pomocą programu SecurityCenter.

1. W obszarze **Typowe zadania** kliknij opcję **Moje konto**.
2. Zaloguj się na koncie McAfee.

Weryfikowanie subskrypcji

Weryfikacja subskrypcji ma na celu upewnienie się, że jej okres nie minął.

- Kliknij prawym przyciskiem myszy ikonę programu SecurityCenter znajdującą się w obszarze powiadomień, z boku po prawej stronie paska zadań, następnie kliknij polecenie **Weryfikuj subskrypcję**.

ROZDZIAŁ 4

Aktualizowanie oprogramowania SecurityCenter

Program SecurityCenter zapewnia najnowszą wersję zarejestrowanych programów firmy McAfee poprzez sprawdzanie ich dostępności i instalowanie aktualizacji w trybie online co cztery godziny. W zależności od zainstalowanych i zarejestrowanych programów aktualizacje online mogą obejmować najnowsze definicje wirusów oraz uaktualnienia dotyczące działalności hakerów, spamu, programów szpiegujących oraz ochrony prywatności. Sprawdzenie dostępności aktualizacji jest możliwe w dowolnym momencie w trakcie domyślnego okresu czterogodzinnego. Gdy program SecurityCenter sprawdza dostępność aktualizacji, użytkownik może kontynuować wykonywanie innych zadań.

Sposób, w jaki program SecurityCenter sprawdza i instaluje aktualizacje, można zmienić, ale nie jest to zalecane. Na przykład można skonfigurować program SecurityCenter tak, aby aktualizacje były pobierane, ale nie instalowane, bądź aby użytkownik był powiadamiany przed pobraniem lub zainstalowaniem aktualizacji. Można również wyłączyć automatyczne aktualizowanie.

Uwaga: Jeśli programy firmy McAfee zostały zainstalowane z dysku CD, regularne, automatyczne aktualizacje tych programów nie będą dostępne do momentu zarejestrowania ich na witrynie sieci Web firmy McAfee.

W tym rozdziale

Sprawdzanie dostępności aktualizacji

Domyślnie program SecurityCenter automatycznie sprawdza dostępność aktualizacji co cztery godziny, gdy komputer jest podłączony do sieci Internet. Użytkownik może jednak sprawdzić dostępność aktualizacji w dowolnym momencie. Po wyłączeniu automatycznych aktualizacji należy regularnie sprawdzać dostępność aktualizacji.

- W okienku Początek programu SecurityCenter kliknij przycisk **Aktualizuj**.

Wskazówka: Dostępność aktualizacji można sprawdzać bez konieczności uruchamiania programu SecurityCenter, klikając prawym przyciskiem myszy ikonę programu SecurityCenter znajdującą się w obszarze powiadomień, z boku po prawej stronie paska zadań, a następnie klikając polecenie **Aktualizacje**.

Konfigurowanie automatycznych aktualizacji

Gdy komputer jest podłączony do Internetu, program SecurityCenter domyślnie co cztery godziny automatycznie sprawdza, czy są dostępne aktualizacje, i instaluje je. Aby zmienić ten domyślny sposób działania, można skonfigurować program SecurityCenter do automatycznego pobierania aktualizacji i powiadamiania użytkownika, gdy aktualizacje są gotowe do zainstalowania, lub do powiadamiania przed pobraniem aktualizacji.

Uwaga: W celu sygnalizowania gotowości aktualizacji do pobrania lub zainstalowania program SecurityCenter używa alertów. Z poziomu alertów można pobrać aktualizacje, zainstalować je lub odroczyć. W przypadku aktualizowania programów z poziomu alertu może się pojawić monit o zweryfikowanie subskrypcji przed pobraniem i zainstalowaniem aktualizacji. Aby uzyskać więcej informacji, zobacz *Praca z alertami* (strona 23).

1 Otwórz okienko Konfiguracja programu SecurityCenter.

   Jak to zrobić?

   1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
   2. W prawym okienku w obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.

2 W okienku Konfiguracja programu SecurityCenter w obszarze **Opcja automatycznych aktualizacji jest wyłączona** kliknij przycisk **Włączone**, a następnie kliknij przycisk **Zaawansowane**.

3 Kliknij jeden z poniższych przycisków:

   - **Instaluj aktualizacje automatycznie i powiadamiaj mnie, gdy usługi zostaną zaktualizowane (zalecane)**
   - **Pobieraj aktualizacje automatycznie i powiadamiaj mnie, gdy są gotowe do zainstalowania**
   - **Powiadamiaj przed pobieraniem aktualizacji**

4 Kliknij przycisk **OK**.

Wyłączanie automatycznych aktualizacji

Wyłączywszy automatyczne aktualizacje, użytkownik sam odpowiada za regularne sprawdzanie dostępności aktualizacji — w przeciwnym razie komputer nie będzie mieć najnowszych zabezpieczeń. Aby uzyskać informacje na temat ręcznego sprawdzania dostępności aktualizacji, zobacz *Sprawdzanie aktualizacji* (strona 13).

1 Otwórz okienko Konfiguracja programu SecurityCenter.

   Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W prawym okienku w obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.

2 W okienku Konfiguracja programu SecurityCenter w obszarze **Opcja automatycznych aktualizacji jest włączona** kliknij przycisk **Wyłączone**.

Wskazówka: Automatyczne aktualizacje włącza się przez kliknięcie przycisku **Włączone** bądź wyczyszczenie pola wyboru **Wyłącz aktualizacje automatyczne i zezwól na ręczne sprawdzanie aktualizacji** w okienku Opcje aktualizacji.

ROZDZIAŁ 5

Naprawianie lub ignorowanie problemów dotyczących ochrony

Program SecurityCenter zgłasza krytyczne i niekrytyczne problemy dotyczące ochrony natychmiast po ich wykryciu. Krytyczne problemy dotyczące ochrony wymagają niezwłocznego działania i powodują obniżenie stanu ochrony (kolor jest zmieniany na czerwony). Niekrytyczne problemy dotyczące ochrony nie wymagają niezwłocznego działania i nie muszą, choć mogą, skutkować obniżeniem stanu ochrony (zależy to od typu problemu). Aby osiągnąć zielony stan ochrony, należy naprawić wszystkie problemy krytyczne oraz naprawić lub zignorować wszystkie problemy niekrytyczne. Jeśli potrzebna jest pomoc w diagnozowaniu problemów dotyczących ochrony, można uruchomić narzędzie McAfee Virtual Technician. Aby uzyskać więcej informacji na temat narzędzia McAfee Virtual Technician, zobacz Pomoc tego narzędzia.

W tym rozdziale

Naprawianie problemów dotyczących ochrony

Większość problemów dotyczących zabezpieczeń jest naprawiana automatycznie, ale niektóre problemy wymagają interwencji użytkownika. Na przykład, jeśli ochrona przy użyciu zapory jest wyłączona, program SecurityCenter może ją włączyć automatycznie, lecz jeśli nie jest zainstalowana, trzeba ją zainstalować samodzielnie. W poniższej tabeli opisano kilka innych działań podejmowanych w przypadku ręcznego naprawiania problemów dotyczących ochrony:

Problem	Action (Akcja)
Pełne skanowanie systemu nie zostało wykonane w przeciągu ostatnich 30 dni.	Ręczne przeskanowanie komputera. Aby uzyskać więcej informacji, zobacz Pomoc narzędzia VirusScan.
Pliki sygnatur wykrywania (DAT) są nieaktualne.	Ręczna aktualizacja zabezpieczeń. Aby uzyskać więcej informacji, zobacz Pomoc narzędzia VirusScan.
Program nie jest zainstalowany.	Instalacja programu z witryny sieci Web firmy McAfee lub dysku CD.
Brakuje pewnych składników programu.	Ponowna instalacja programu z witryny sieci Web firmy McAfee lub dysku CD.
Program nie jest zarejestrowany i nie może uzyskać pełnej ochrony.	Rejestracja programu w witrynie sieci Web firmy McAfee.
Ważność programu wygasła.	Sprawdzenie stanu swojego konta w witrynie sieci Web firmy McAfee.

Uwaga: Często jeden problem dotyczący ochrony jest związany z więcej niż jedną kategorią ochrony. W takim przypadku naprawienie problemu w jednej kategorii powoduje usunięcie go z pozostałych kategorii.

Automatyczne naprawianie problemów dotyczących ochrony

Program SecurityCenter automatycznie naprawia większość problemów dotyczących ochrony. Zmiany konfiguracji wprowadzane przez program SecurityCenter podczas automatycznego naprawiania problemów dotyczących ochrony nie są rejestrowane w dzienniku zdarzeń. Aby uzyskać więcej informacji na temat zdarzeń, zobacz *Przeglądanie zdarzeń* (strona 29).

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Strona główna programu SecurityCenter w obszarze stanu ochrony kliknij przycisk **Napraw**.

Ręczne naprawianie problemów dotyczących ochrony

Jeśli jakieś problemy występują nadal mimo prób ich automatycznego naprawienia, można je naprawić ręcznie.

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Strona główna programu SecurityCenter kliknij kategorię ochrony, której dotyczy problem zgłaszany przez program SecurityCenter.
3. Kliknij łącze znajdujące się po opisie problemu.

Ignorowanie problemów dotyczących ochrony

Problem niekrytyczny wykryty przez program SecurityCenter można naprawić lub zignorować. Inne problemy niekrytyczne (np. brak zainstalowanego oprogramowania antyspamowego lub produktu Privacy Service) są ignorowane automatycznie. Zignorowane problemy nie są wyświetlane w obszarze informacji danej kategorii ochrony w okienku Strona główna programu SecurityCenter, chyba że stan ochrony komputera jest zielony. Jeśli użytkownik zdecyduje, że zignorowany problem jednak powinien być wyświetlany w obszarze informacji danej kategorii ochrony, gdy stan ochrony komputera nie jest zielony, może włączyć jego wyświetlanie.

Ignorowanie problemu dotyczącego ochrony

Jeśli użytkownik nie chce naprawić problemu niekrytycznego wykrytego przez program SecurityCenter, może go zignorować. Zignorowanie spowoduje usunięcie problemu z obszaru informacji danej kategorii ochrony w oknie programu SecurityCenter.

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Strona główna programu SecurityCenter kliknij kategorię ochrony, której dotyczy zgłoszony problem.
3. Kliknij łącze **Ignoruj** znajdujące się obok tego problemu dotyczącego ochrony.

Wyświetlanie lub ukrywanie zignorowanych problemów

Zignorowany problem dotyczący ochrony można wyświetlać lub ukrywać, w zależności od stopnia zagrożenia.

1. Otwórz okienko Opcje alertów.

   Jak to zrobić?

   1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
   2. W prawym okienku w obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
   3. W obszarze **Alerty** kliknij przycisk **Zaawansowane**.
2. W okienku Konfiguracja programu SecurityCenter kliknij opcję **Zignorowane problemy**.
3. W okienku Zignorowane problemy wykonaj następujące czynności:
   - Aby ignorować problem, zaznacz jego pole wyboru.
   - Aby problem był zgłaszany w obszarze informacji danej kategorii ochrony, wyczyść jego pole wyboru.

4 Kliknij przycisk **OK**.

Wskazówka: Problem można zignorować także przez kliknięcie łącza **Ignoruj** znajdującego się obok zgłoszonego problemu w obszarze informacji danej kategorii ochrony.

ROZDZIAŁ 6

Praca z alertami

Alerty to małe wyskakujące okna dialogowe wyświetlane w prawym dolnym rogu ekranu, gdy wystąpią określone zdarzenia programu SecurityCenter. Alert udostępnia szczegółowe informacje o zdarzeniu, a także zalecenia i opcje dotyczące rozwiązywania problemów, które mogą być związane z danym zdarzeniem. Niektóre alerty zawierają też łącza do dodatkowych informacji o zdarzeniu. Łącza te umożliwiają otwarcie ogólnoświatowej witryny sieci Web firmy McAfee lub wysłanie informacji do firmy McAfee w celu uzyskania rozwiązania problemu.

Dostępne są trzy typy alertów: czerwony, żółty i zielony.

Typ alertu	Opis
Czerwony	Czerwony alert to krytyczne powiadomienie, które wymaga reakcji użytkownika. Czerwone alerty występują, gdy program SecurityCenter nie może określić, jak automatycznie rozwiązać dany problem dotyczący ochrony.
Żółty	Żółty alert to niekrytyczne powiadomienie, które zazwyczaj wymaga odpowiedzi ze strony użytkownika.
Zielony	Zielony alert to niekrytyczne powiadomienie, które nie wymaga reakcji użytkownika. Zielone alerty udostępniają podstawowe informacje o zdarzeniu.

Ponieważ alerty są tak istotne dla monitorowania stanu ochrony i zarządzania nim, nie można ich wyłączyć. Można jednak określić, czy alerty informacyjne pewnych typów mają być wyświetlane, a także skonfigurować niektóre opcje alertów (na przykład, czy program SecurityCenter ma odtwarzać dźwięk, wyświetlając alert, lub czy podczas uruchamiania systemu ma być wyświetlany ekran powitalny programu firmy McAfee).

W tym rozdziale

Wyświetlanie i ukrywanie alertów informacyjnych

Alerty informacyjne powiadamiają o wystąpieniu zdarzeń, które nie powodują zagrożenia bezpieczeństwa komputera. Na przykład, jeśli została skonfigurowana ochrona przy użyciu zapory, alert informacyjny jest domyślnie wyświetlany za każdym razem, gdy jakiś program na komputerze uzyska dostęp do Internetu. Jeśli alert informacyjny pewnego typu nie ma być wyświetlany, można go ukryć. Jeśli żadne alerty informacyjne nie mają być wyświetlane, można ukryć je wszystkie. Można też ukryć wszystkie alerty informacyjne na czas korzystania z gier w trybie pełnoekranowym. Gdy użytkownik zakończy grę i zamknie tryb pełnoekranowy, program SecurityCenter ponownie zacznie wyświetlać alerty informacyjne.

Jeśli jakiś alert informacyjny zostanie ukryty przez pomyłkę, w każdej chwili można ponownie włączyć jego wyświetlanie. Domyślnie program SecurityCenter wyświetla wszystkie alerty informacyjne.

Wyświetlanie lub ukrywanie alertów informacyjnych

Program SecurityCenter można skonfigurować tak, aby wyświetlał niektóre alerty informacyjne, a ukrywał inne, lub aby ukrywał wszystkie alerty informacyjne.

1 Otwórz okienko Opcje alertów.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W prawym okienku w obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
3. W obszarze **Alerty** kliknij przycisk **Zaawansowane**.

2 W okienku Konfiguracja programu SecurityCenter kliknij opcję **Alerty informacyjne**.

3 W okienku Alerty informacyjne wykonaj następujące czynności:

- Aby alert informacyjny był wyświetlany, wyczyść odpowiadające mu pole wyboru.
- Aby ukryć alert informacyjny, zaznacz odpowiadające mu pole wyboru.
- Aby ukryć wszystkie alerty informacyjne, zaznacz pole wyboru **Nie pokazuj alertów informacyjnych**.

4 Kliknij przycisk **OK**.

Wskazówka: Alert informacyjny można ukryć także przez zaznaczenie pola wyboru **Nie wyświetlaj tego alertu ponownie** w samym oknie alertu. Aby później ponownie włączyć wyświetlanie tego alertu informacyjnego, należy wyczyścić odpowiednie pole wyboru w okienku Alerty informacyjne.

Wyświetlanie lub ukrywanie alertów informacyjnych na czas korzystania z gier

Alerty informacyjne można ukryć na czas korzystania z gier w trybie pełnoekranowym na komputerze. Gdy użytkownik zakończy grę i zamknie tryb pełnoekranowy, program SecurityCenter ponownie zacznie wyświetlać alerty informacyjne.

1 Otwórz okienko Opcje alertów.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W prawym okienku w obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
3. W obszarze **Alerty** kliknij przycisk **Zaawansowane**.

2 W okienku Opcje alertów zaznacz lub wyczyść pole wyboru **Pokaż alerty informacyjne, gdy zostanie wykryty tryb gier**.

3 Kliknij przycisk **OK**.

Konfigurowanie opcji alertów

Wygląd i częstotliwość alertów są konfigurowane przez program SecurityCenter; można jednak zmieniać niektóre podstawowe opcje alertów. Na przykład można włączyć odtwarzanie dźwięku wraz z alertem lub wyłączyć wyświetlanie ekranu powitalnego alertu podczas uruchamiania systemu Windows. Można też ukryć alerty powiadamiające o epidemiach wirusowych i innych zagrożeniach bezpieczeństwa społeczności online.

Włączanie odtwarzania dźwięku podczas wyświetlania alertów

Jeśli wyświetleniu alertu ma towarzyszyć sygnał dźwiękowy, można skonfigurować program SecurityCenter do odtwarzania dźwięku w przypadku każdego alertu.

1 Otwórz okienko Opcje alertów.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W prawym okienku w obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
3. W obszarze **Alerty** kliknij przycisk **Zaawansowane**.

2 W okienku Opcje alertów w obszarze **Dźwięk** zaznacz pole wyboru **Odtwórz dźwięk przy wystąpieniu alertu**.

Ukrywanie ekranu powitalnego podczas uruchamiania

Domyślnie podczas uruchamiania systemu Windows jest przez krótką chwilę wyświetlany ekran powitalny programu firmy McAfee, powiadamiając użytkownika, że komputer jest chroniony przez program SecurityCenter. Ekran ten można jednak ukryć, jeśli się nie chce, by był wyświetlany.

1 Otwórz okienko Opcje alertów.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W prawym okienku w obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
3. W obszarze **Alerty** kliknij przycisk **Zaawansowane**.

2 W okienku Opcje alertów w obszarze **Ekran powitalny** wyczyść pole wyboru **Pokazuj ekran powitalny firmy McAfee przy uruchamianiu systemu Windows**.

Wskazówka: W każdej chwili można ponownie włączyć wyświetlanie ekranu powitalnego, zaznaczając pole wyboru **Pokazuj ekran powitalny firmy McAfee przy uruchamianiu systemu Windows**.

Ukrywanie alertów o epidemiach wirusowych

Alerty powiadamiające o epidemiach wirusowych i innych zagrożeniach bezpieczeństwa społeczności online można ukryć.

1 Otwórz okienko Opcje alertów.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W prawym okienku w obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
3. W obszarze **Alerty** kliknij przycisk **Zaawansowane**.

2 W okienku Opcje alertów wyczyść pole wyboru **Powiadom, gdy pojawi się wirus lub zagrożenie bezpieczeństwa**.

Wskazówka: W każdej chwili można ponownie włączyć wyświetlanie alertów o epidemiach wirusowych, zaznaczając pole wyboru **Powiadom, gdy pojawi się wirus lub zagrożenie bezpieczeństwa**.

ROZDZIAŁ 7

Przeglądanie zdarzeń

Zdarzenie jest akcją lub zmianą konfiguracji, która ma miejsce w ramach kategorii ochrony i jest związana z usługami ochrony. W przypadku różnych usług ochrony są rejestrowane różnego typu zdarzenia. Na przykład program SecurityCenter rejestruje zdarzenie, jeśli usługa ochrony zostanie włączona lub wyłączona, funkcja ochrony przed wirusami rejestruje zdarzenie za każdym razem, gdy wirus zostanie wykryty i usunięty, a funkcja ochrony przy użyciu zapory rejestruje zdarzenie za każdym razem, gdy zostanie zablokowana próba ustanowienia połączenia internetowego. Aby uzyskać więcej informacji na temat kategorii ochrony, zobacz *Jak działają kategorie ochrony* (strona 9).

Zdarzenia można przeglądać w celu rozwiązywania problemów z konfiguracją i przeglądania operacji wykonywanych przez innych użytkowników. Wielu rodziców monitoruje zachowania swoich dzieci w Internecie właśnie za pomocą dziennika zdarzeń. Jeśli chce się sprawdzić tylko ostatnie 30 zdarzeń, można wyświetlić tylko ostatnie zdarzenia. Jeśli chce się sprawdzić pełną listę wszystkich zdarzeń, można wyświetlić wszystkie zdarzenia. Dla potrzeb wyświetlenia wszystkich zdarzeń program SecurityCenter uruchamia dziennik zdarzeń posortowany według kategorii ochrony, w których dane zdarzenia miały miejsce.

W tym rozdziale

Wyświetlanie ostatnich zdarzeń

Jeśli chce się sprawdzić tylko ostatnie 30 zdarzeń, można wyświetlić tylko ostatnie zdarzenia.

- W obszarze **Typowe zadania** kliknij opcję **Przeglądaj ostatnie zdarzenia**.

Wyświetlanie wszystkich zdarzeń

Jeśli chce się sprawdzić pełną listę wszystkich zdarzeń, można wyświetlić wszystkie zdarzenia.

1 W obszarze **Typowe zadania** kliknij opcję **Przeglądaj ostatnie zdarzenia**.

2 W okienku Ostatnie zdarzenia kliknij opcję **Wyświetl dziennik**.

3 W lewym okienku okna dziennika zdarzeń kliknij typ zdarzeń, które chcesz przejrzeć.

ROZDZIAŁ 8

McAfee VirusScan

Zaawansowane usługi wykrywania i ochrony udostępniane przez program VirusScan bronią użytkownika i jego komputer przed najnowszymi zagrożeniami bezpieczeństwa, takimi jak wirusy, konie trojańskie, śledzące pliki cookie, oprogramowanie szpiegujące, oprogramowanie reklamowe i inne potencjalnie niepożądane programy. Ochrona wykracza poza pliki i foldery znajdujące się na komputerze, eliminując zagrożenia z różnych punktów wejścia — poczty e-mail, wiadomości błyskawicznych i sieci Web.

Dzięki programowi VirusScan ochrona komputera działa natychmiastowo i stale (nie są wymagane żadne uciążliwe czynności administracyjne). Gdy użytkownik pracuje, korzysta z gier, przegląda sieć Web i sprawdza pocztę e-mail, program ten działa w tle, monitorując, skanując i wykrywając potencjalne zagrożenia w czasie rzeczywistym. Okresowo, według harmonogramu, jest wykonywane wszechstronne skanowanie w celu sprawdzenia komputera przy użyciu bardziej zaawansowanego zestawu opcji. Sposób działania programu VirusScan w tym zakresie można dostosowywać, lecz jeśli użytkownik nie skorzysta z tej możliwości, komputer i tak będzie chroniony.

Podczas normalnego użytkowania komputera mogą się do niego dostać wirusy, robaki i inne potencjalne źródła zagrożenia. Gdy tak się stanie, program VirusScan powiadamia użytkownika o zagrożeniu, ale zwykle sam sobie radzi z problemem, czyszcząc i poddając kwarantannie zainfekowane elementy, zanim dojdzie do uszkodzenia systemu. Czasami mogą być konieczne dodatkowe działania. W takich przypadkach program VirusScan pozostawia użytkownikowi decyzję, co robić (ponownie wykonać skanowanie po następnym uruchomieniu komputera, zachować wykryty element czy usunąć go).

Uwaga: Program SecurityCenter zgłasza krytyczne i niekrytyczne problemy dotyczące ochrony natychmiast po ich wykryciu. Jeśli potrzebna jest pomoc w diagnozowaniu problemów dotyczących ochrony, można uruchomić narzędzie McAfee Virtual Technician.

W tym rozdziale

Funkcje programu VirusScan

Program VirusScan jest wyposażony w następujące funkcje.

Wszechstronna ochrona przed wirusami

Zaawansowane usługi wykrywania i ochrony udostępniane przez program VirusScan bronią użytkownika i jego komputer przed najnowszymi zagrożeniami bezpieczeństwa, takimi jak wirusy, konie trojańskie, śledzące pliki cookie, oprogramowanie szpiegujące, oprogramowanie reklamowe i inne potencjalnie niepożądane programy. Ochrona wykracza poza pliki i foldery znajdujące się na komputerze, eliminując zagrożenia z różnych punktów wejścia — poczty e-mail, wiadomości błyskawicznych i sieci Web. Nie są wymagane żadne uciążliwe czynności administracyjne.

Opcje skanowania z rozpoznawaniem zasobów

Jeśli skanowanie przebiega powoli, można wyłączyć opcję używania minimalnych zasobów komputera, pamiętając jednak, że wówczas ochrona przed wirusami będzie miała priorytet przed innymi zadaniami. Program VirusScan umożliwia dostosowywanie opcji skanowania w czasie rzeczywistym i skanowania ręcznego, lecz jeśli użytkownik nie skorzysta z tej możliwości, komputer i tak będzie chroniony.

Automatyczne naprawy

Jeśli podczas skanowania w czasie rzeczywistym lub skanowania ręcznego aplikacja VirusScan wykryje zagrożenie bezpieczeństwa, próbuje automatycznie je usunąć w sposób odpowiedni dla rodzaju zagrożenia. Dzięki temu większość zagrożeń może być wykrywana i neutralizowana bez udziału użytkownika. Czasami program VirusScan może nie być w stanie zneutralizować zagrożenia. W takich przypadkach program VirusScan pozostawia użytkownikowi decyzję, co robić (ponownie wykonać skanowanie po następnym uruchomieniu komputera, zachować wykryty element czy usunąć go).

Wstrzymywanie zadań w trybie pełnoekranowym

Podczas oglądanie filmów i korzystania z gier lub podczas wykonywania innych czynności, które zajmują cały ekran komputera, program VirusScan wstrzymuje pewną liczbę zadań, w tym aktualizacje automatyczne i skanowanie ręczne.

Włączanie ochrony przed wirusami w czasie rzeczywistym

Program VirusScan zapewnia dwa rodzaje ochrony przed wirusami: w czasie rzeczywistym i ręczną. Ochrona przed wirusami w czasie rzeczywistym stale monitoruje komputer pod kątem działalności wirusów, skanując pliki za każdym razem, gdy użytkownik lub jego komputer próbuje uzyskać do nich dostęp. Ręczna ochrona przed wirusami pozwala na skanowanie plików na żądanie. Aby mieć pewność, że komputer jest chroniony przed najnowszymi zagrożeniami bezpieczeństwa, należy pozostawić włączoną ochronę przed wirusami w czasie rzeczywistym i skonfigurować harmonogram regularnego, bardziej wszechstronnego skanowania ręcznego. Domyślnie raz w tygodniu uruchamiane jest w programie VirusScan skanowanie zaplanowane. Aby uzyskać więcej informacji na temat skanowania w czasie rzeczywistym i ręcznego, zobacz *Skanowanie komputera* (strona 59).

Czasami może być konieczne tymczasowe zatrzymanie skanowania w czasie rzeczywistym (na przykład po to, by zmienić jakieś opcje skanowania lub rozwiązać problem dotyczący wydajności). Jeśli ochrona przed wirusami w czasie rzeczywistym jest wyłączona, komputer nie jest chroniony i w programie SecurityCenter jest sygnalizowany czerwony stan ochrony. Aby uzyskać więcej informacji na temat stanu ochrony, zobacz „Jak działa stan ochrony” w Pomocy programu SecurityCenter.

Włączanie ochrony przed wirusami w czasie rzeczywistym

Domyślnie ochrona przed wirusami w czasie rzeczywistym jest włączona i chroni komputer przed wirusami, końmi trojańskimi i innymi zagrożeniami bezpieczeństwa. Jeśli ochrona przed wirusami w czasie rzeczywistym zostanie wyłączona, trzeba ją włączyć z powrotem, aby komputer był chroniony.

1. Otwórz okienko konfiguracji Komputer i pliki.

   Jak to zrobić?

   1. W okienku po lewej stronie kliknij opcję **Menu zaawansowane**.
   2. Kliknij przycisk **Konfiguruj**.
   3. W okienku konfiguracji kliknij opcję **Komputer i pliki**.

2. W polu **Ochrona przed wirusami** kliknij opcję **Włączona**.

Zatrzymywanie ochrony przed wirusami w czasie rzeczywistym

Ochronę przed wirusami w czasie rzeczywistym można tymczasowo wyłączyć, a następnie określić, kiedy ma zostać wznowiona. Ochrona może zostać wznowiona automatycznie po 15, 30, 45 lub 60 minutach, gdy komputer zostanie uruchomiony ponownie lub nigdy.

1 Otwórz okienko konfiguracji Komputer i pliki.

Jak to zrobić?

1. W okienku po lewej stronie kliknij opcję **Menu zaawansowane**.
2. Kliknij przycisk **Konfiguruj**.
3. W okienku konfiguracji kliknij opcję **Komputer i pliki**.

2 W polu **Ochrona przed wirusami** kliknij opcję **Wyłączona**.

3 W oknie dialogowym wybierz, kiedy skanowanie w czasie rzeczywistym ma zostać wznowione.

4 Kliknij przycisk **OK**.

ROZDZIAŁ 9

Uruchamianie dodatkowej ochrony

Oprócz ochrony przed wirusami w czasie rzeczywistym program VirusScan zapewnia zaawansowaną ochronę przed skryptami, oprogramowaniem szpiegującym, potencjalnie szkodliwymi wiadomościami oraz załącznikami przesyłanymi przez komunikatory internetowe. Funkcje skanowania skryptów, oprogramowania szpiegującego, wiadomości e-mail i wiadomości błyskawicznych są domyślnie włączone i zapewniają ochronę komputera.

Ochrona przez skanowanie skryptów

Ochrona przez skanowanie skryptów wykrywa potencjalnie szkodliwe skrypty i uniemożliwia ich wykonywanie na komputerze. Funkcja monitoruje komputer w poszukiwaniu podejrzanej aktywności skryptów, takiej jak tworzenie, kopiowanie i usuwanie plików czy otwieranie rejestru systemu Windows, a następnie ostrzega użytkownika przed mogącym wystąpić uszkodzeniem.

Ochrona przed oprogramowaniem szpiegującym

Ochrona przed oprogramowaniem szpiegującym wykrywa oprogramowanie szpiegujące, reklamowe i inne potencjalnie niepożądane programy. Oprogramowanie szpiegujące to potajemnie zainstalowane na komputerze programy, które monitorują zachowanie użytkownika, zbierają informacje osobiste, a nawet ograniczają kontrolę nad komputerem poprzez instalowanie dodatkowego oprogramowania czy przekierowanie żądań przeglądarki.

Ochrona poczty e-mail

Ochrona poczty e-mail wykrywa podejrzaną aktywność w wysyłanych i odbieranych wiadomościach e-mail oraz załącznikach.

Ochrona wiadomości błyskawicznych

Ochrona wiadomości błyskawicznych wykrywa potencjalnie niebezpieczne zagrożenia w odbieranych załącznikach przesyłanych przez komunikatory. Funkcja blokuje także programy wiadomości błyskawicznych przed udostępnianiem informacji osobistych.

W tym rozdziale

Uruchamianie ochrony przez skanowanie skryptów

Włączenie ochrony przez skanowanie skryptów umożliwia wykrywanie potencjalnie szkodliwych skryptów i uniemożliwia ich wykonywanie na komputerze. Ochrona przez skanowanie skryptów ostrzega użytkownika, gdy skrypt próbuje utworzyć, skopiować lub usunąć pliki na komputerze bądź wprowadzić zmiany w rejestrze systemu Windows.

1 Otwórz okienko konfiguracji Komputer i pliki.

Jak to zrobić?

1. W okienku po lewej stronie kliknij opcję **Menu zaawansowane**.
2. Kliknij przycisk **Konfiguruj**.
3. W okienku konfiguracji kliknij opcję **Komputer i pliki**.

2 W polu **Ochrona przez skanowanie skryptów** kliknij opcję **Włączona**.

Uwaga: Ochronę przez skanowanie skryptów można wyłączyć w dowolnym momencie, jednak spowoduje to, że komputer będzie narażony na działanie szkodliwych skryptów.

Uruchamianie ochrony przed oprogramowaniem szpiegującym

Włączenie ochrony przed oprogramowaniem szpiegującym umożliwia wykrywanie i usuwanie programów szpiegujących i reklamowych oraz innych potencjalnie niepożądanych programów, które gromadzą i wysyłają dane bez wiedzy i zgody użytkowników.

1 Otwórz okienko konfiguracji Komputer i pliki.

Jak to zrobić?

1. W okienku po lewej stronie kliknij opcję **Menu zaawansowane**.
2. Kliknij przycisk **Konfiguruj**.
3. W okienku konfiguracji kliknij opcję **Komputer i pliki**.

2 W polu **Ochrona przez skanowanie skryptów** kliknij opcję **Włączona**.

Uwaga: Ochronę przed oprogramowaniem szpiegującym można wyłączyć w dowolnym momencie, jednak spowoduje to, że komputer będzie narażony na działanie potencjalnie niepożądanych programów.

Uruchamianie ochrony poczty e-mail

Włączenie ochrony poczty e-mail umożliwia wykrywanie robaków, a także potencjalnych zagrożeń w wychodzących (SMTP) i przychodzących (POP3) wiadomościach e-mail oraz załącznikach.

1 Otwórz okienko konfiguracji Poczta e-mail i wiadomości błyskawiczne.

Jak to zrobić?

1. W okienku po lewej stronie kliknij opcję **Menu zaawansowane**.
2. Kliknij przycisk **Konfiguruj**.
3. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.

2 W polu **Ochrona poczty e-mail** kliknij opcję **Włączona**.

Uwaga: Ochronę poczty e-mail można wyłączyć w dowolnym momencie, jednak spowoduje to, że komputer będzie narażony na działanie zagrożeń w wiadomościach e-mail.

Uruchamianie ochrony wiadomości błyskawicznych

Włączenie ochrony wiadomości błyskawicznych umożliwia wykrywanie zagrożeń bezpieczeństwa w wychodzących i przychodzących załącznikach przesyłanych przez komunikatory internetowe.

1 Otwórz okienko konfiguracji Poczta e-mail i wiadomości błyskawiczne.

Jak to zrobić?

1. W okienku po lewej stronie kliknij opcję **Menu zaawansowane**.
2. Kliknij przycisk **Konfiguruj**.
3. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.

2 Pod polu **Ochrona wiadomości błyskawicznych** kliknij opcję **Włączona**.

Uwaga: Ochronę wiadomości błyskawicznych można wyłączyć w dowolnym momencie, jednak spowoduje to, że komputer będzie narażony na działanie szkodliwych załączników przesyłanych przez komunikatory internetowe.

ROZDZIAŁ 10

Konfigurowanie ochrony przed wirusami

Program VirusScan zapewnia dwa rodzaje ochrony przed wirusami: skanowanie w czasie rzeczywistym i ręczne. Funkcja ochrony przed wirusami w czasie rzeczywistym skanuje pliki za każdym razem, gdy użytkownik lub system próbują uzyskać do nich dostęp. Ręczna ochrona przed wirusami pozwala na skanowanie plików na żądanie. Dla każdego rodzaju ochrony można ustawić różne opcje. Na przykład, ponieważ ochrona w czasie rzeczywistym ciągle monitoruje komputer, to można wybrać dla niej pewien podstawowy zestaw opcji skanowania, zachowując bardziej szeroki zestaw opcji skanowania dla ochrony ręcznej, uruchamianej na żądanie.

W tym rozdziale

Ustawianie opcji skanowania w czasie rzeczywistym

Po uruchomieniu ochrony przed wirusami w czasie rzeczywistym program VirusScan używa domyślnego zestawu opcji, które użytkownik może zmienić stosownie do swoich potrzeb.

Aby zmienić opcje skanowania w czasie rzeczywistym, należy podjąć decyzję dotyczącą tego, co będzie sprawdzane przez program VirusScan podczas skanowania oraz określić lokalizacje i typy skanowanych plików. Na przykład można określić, czy program VirusScan ma szukać nieznanych wirusów lub plików cookie, których witryny sieci Web mogą używać do śledzenia zachowania użytkownika, lub czy ma skanować dyski sieciowe zmapowane na komputerze czy tylko dyski lokalne. Można także określić, jakie typy plików mają być skanowane (wszystkie pliki czy tylko pliki programów i dokumentów, w których wykrywanych jest najwięcej wirusów).

Zmieniając opcje skanowania w czasie rzeczywistym, należy także określić, czy ma zostać włączona funkcja ochrony bufora przed przepełnieniem. Bufor to części pamięci używana przez komputer do tymczasowego przechowywania danych. Przepełnienia buforów mogą występować, gdy ilość informacji przechowywanych w buforze przez podejrzane programy lub procesy przekracza pojemność buforu. W przypadku wystąpienia takiego przepełnienia, komputer staje się bardziej narażony na ataki na zabezpieczenia.

Ustawianie opcji skanowania w czasie rzeczywistym

Opcje skanowania w czasie rzeczywistym ustawia się, aby dostosować to, czego program VirusScan będzie szukał podczas skanowania w czasie rzeczywistym, oraz określić lokalizacje i typy skanowanych plików. Opcje obejmują skanowanie nieznanych wirusów i śledzenie plików cookie, a także ochronę przed przepełnieniem bufora. Można też skonfigurować skanowanie w czasie rzeczywistym tak, aby były sprawdzane dyski sieciowe zmapowane na komputerze.

1 Otwórz okienko Skanowanie w czasie rzeczywistym.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Komputer i pliki**.
3. W obszarze informacji kategorii Komputer i pliki kliknij opcję **Konfiguruj**.
4. Upewnij się, że w okienku konfiguracji Komputer i pliki jest włączona ochrona przed wirusami, a następnie kliknij przycisk **Zaawansowane**.

2 Określ opcje skanowania w czasie rzeczywistym, a następnie kliknij przycisk **OK**.

Aby...	Wykonaj następujące czynności:
Wykrywać nieznane wirusy i nowe warianty znanych wirusów	Zaznacz pole wyboru **Skanuj w poszukiwaniu nieznanych wirusów przy użyciu heurystyk**.
Wykrywać pliki cookie	Zaznacz pole wyboru **Skanuj i usuwaj śledzące pliki cookie**.
Wykrywać wirusy i inne potencjalne zagrożenia na dyskach sieciowych	Zaznacz pole wyboru **Skanuj dyski sieciowe**.
Chronić komputer przed przepełnieniem bufora	Zaznacz pole wyboru **Włącz ochronę przed przepełnieniem buforu**.
Określić typy plików, które będą skanowane	Zaznacz opcję **Wszystkie pliki (zalecane)** lub **Tylko pliki programów i dokumenty**.

Ustawianie opcji skanowania ręcznego

Ręczna ochrona przed wirusami pozwala na skanowanie plików na żądanie. Po uruchomieniu skanowania ręcznego program VirusScan sprawdza komputer w poszukiwaniu wirusów i innych potencjalnie szkodliwych elementów przy użyciu szerszego zestawu opcji skanowania. Aby zmienić opcje skanowania ręcznego, należy podjąć decyzję dotyczącą tego, co będzie sprawdzane przez program VirusScan podczas skanowania. Na przykład można określić, czy program VirusScan ma szukać nieznanych wirusów, potencjalnie niepożądanych programów (takich jak oprogramowanie szpiegujące i reklamowe), programów typu stealth (takich jak rootkit, które mogą przyznawać nieupoważniony dostęp do komputera) oraz plików cookie (których witryny sieci Web mogą używać do śledzenia zachowania użytkownika). Należy także zdecydować o tym, jakie typu plików mają być sprawdzane. Na przykład można określić, czy program VirusScan ma sprawdzać wszystkie pliki czy tylko pliki programów i dokumentów (w których wykrywanych jest najwięcej wirusów). Oprócz tego można określić, czy mają być skanowane pliki archiwów (np. pliki ZIP).

Domyślnie program VirusScan po uruchomieniu skanowania ręcznego sprawdza wszystkie dyski i foldery w komputerze, jednak domyślne lokalizacje można zmienić, dostosowując je do własnych potrzeb. Na przykład można skanować tylko krytyczne pliki systemowe, elementy znajdujące się na pulpicie lub w folderze Program Files. Jeśli użytkownik nie chce być odpowiedzialny za samodzielne uruchamianie skanowania ręcznego, może skonfigurować uruchamianie skanowania według harmonogramu. Zaplanowane skanowania zawsze sprawdzają cały komputer, używając domyślnych opcji skanowania. Domyślnie raz w tygodniu uruchamiane jest w programie VirusScan skanowanie zaplanowane.

Jeśli szybkość skanowania będzie mała, można rozważyć wyłączenie opcji używania minimalnych zasobów komputera, jednak należy pamiętać, że zadanie ochrony przed wirusami będzie miało wyższy priorytet niż inne zadania wykonywane na komputerze.

Uwaga: Podczas oglądanie filmów i korzystania z gier lub podczas wykonywania innych czynności, które zajmują cały ekran komputera, program VirusScan wstrzymuje pewną liczbę zadań, w tym aktualizacje automatyczne i skanowanie ręczne.

Ustawianie opcji skanowania ręcznego

Opcje skanowania ręcznego ustawia się, aby dostosować to, czego program VirusScan będzie szukał podczas skanowania ręcznego, oraz określić lokalizacje i typy skanowanych plików. Opcje obejmują skanowanie nieznanych wirusów, plików archiwów, oprogramowania szpiegującego i potencjalnie niepożądanych programów, śledzenie plików cookie oraz programów typu rootkit i stealth.

1 Otwórz okienko Skanowanie ręczne.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Komputer i pliki**.
3. W obszarze informacji kategorii Komputer i pliki kliknij opcję **Konfiguruj**.
4. Upewnij się, że w okienku konfiguracji Komputer i pliki jest włączona ochrona przed wirusami, a następnie kliknij przycisk **Zaawansowane**.
5. Kliknij opcję **Skanowanie ręczne** w okienku Ochrona przed wirusami.

2 Określ opcje skanowania ręcznego, a następnie kliknij przycisk **OK**.

Aby...	Wykonaj następujące czynności:
Wykrywać nieznane wirusy i nowe warianty znanych wirusów	Zaznacz pole wyboru **Skanuj w poszukiwaniu nieznanych wirusów przy użyciu heurystyk**.
Wykrywać i usuwać wirusy w plikach ZIP i innych archiwach	Zaznacz pole wyboru **Skanuj pliki .zip i inne pliki archiwów**.
Wykrywać oprogramowanie szpiegujące, reklamowe i inne potencjalnie niepożądane programy	Zaznacz pole wyboru **Skanuj w poszukiwaniu programów szpiegujących i potencjalnie niepożądanych**.
Wykrywać pliki cookie	Zaznacz pole wyboru **Skanuj i usuwaj śledzące pliki cookie**.
Wykrywać programy typu rootkit i stealth, które mogą zmienić i wykorzystać istniejące pliki systemu Windows	Zaznacz pole wyboru **Skanuj w poszukiwaniu programów typu rootkit i stealth**.
Wykorzystywać mniejszą moc obliczeniową procesora podczas skanowania, umożliwiając innym zadaniom (takim jak przeglądanie sieci Web czy otwieranie dokumentów) uzyskanie wyższego priorytetu	Zaznacz pole wyboru **Skanuj, używając minimalnej ilości zasobów komputera**.
Określić typy plików, które będą skanowane	Zaznacz opcję **Wszystkie pliki (zalecane)** lub **Tylko pliki programów i dokumenty**.

Ustawianie lokalizacji skanowania ręcznego

Lokalizację skanowania ręcznego ustawia się, aby określić, gdzie program VirusScan będzie szukał wirusów i innych szkodliwych elementów podczas skanowania ręcznego. Można skanować wszystkie pliki, foldery i dyski w komputerze lub ograniczyć skanowanie do konkretnych folderów i dysków.

1 Otwórz okienko Skanowanie ręczne.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Komputer i pliki**.
3. W obszarze informacji kategorii Komputer i pliki kliknij opcję **Konfiguruj**.
4. Upewnij się, że w okienku konfiguracji Komputer i pliki jest włączona ochrona przed wirusami, a następnie kliknij przycisk **Zaawansowane**.
5. Kliknij opcję **Skanowanie ręczne** w okienku Ochrona przed wirusami.

2 Kliknij opcję **Domyślna lokalizacja do skanowania**.

3 Określ lokalizację skanowania ręcznego, a następnie kliknij przycisk **OK**.

Aby...	Wykonaj następujące czynności:
Skanować wszystkie pliki i foldery w komputerze	Zaznacz pole wyboru **(Mój) Komputer**.
Skanować konkretne pliki, foldery i dyski w komputerze	Usuń zaznaczenie pola wyboru **(Mój) Komputer** i wybierz jeden albo więcej folderów lub dysków.
Skanować krytyczne pliki systemowe	Usuń zaznaczenie pola wyboru **(Mój) Komputer** i zaznacz pole wyboru **Krytyczne pliki systemowe**.

Planowanie skanowania

Możliwe jest zaplanowanie skanowania na dowolną godzinę i dzień tygodnia w celu kompleksowego sprawdzenia komputera pod kątem obecności wirusów i innych zagrożeń. Zaplanowane skanowania zawsze sprawdzają cały komputer, używając domyślnych opcji skanowania. Domyślnie raz w tygodniu uruchamiane jest w programie VirusScan skanowanie zaplanowane. Jeśli szybkość skanowania będzie mała, można rozważyć wyłączenie opcji używania minimalnych zasobów komputera, jednak należy pamiętać, że zadanie ochrony przed wirusami będzie miało wyższy priorytet niż inne zadania wykonywane na komputerze.

1 Otwórz okienko Zaplanowane skanowanie.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Komputer i pliki**.
3. W obszarze informacji kategorii Komputer i pliki kliknij opcję **Konfiguruj**.
4. Upewnij się, że w okienku konfiguracji Komputer i pliki jest włączona ochrona przed wirusami, a następnie kliknij przycisk **Zaawansowane**.
5. Kliknij opcję **Zaplanowane skanowanie** w okienku Ochrona przed wirusami.

2 Zaznacz opcję **Włącz zaplanowane skanowanie**.

3 Aby zmniejszyć moc obliczeniową procesora wykorzystywaną normalnie do skanowania, zaznacz opcję **Skanuj, używając minimalnej ilości zasobów komputera**.

4 Wybierz jeden lub większą liczbę dni.

5 Określ godzinę rozpoczęcia.

6 Kliknij przycisk **OK**.

Wskazówka: Domyślny harmonogram można przywrócić, klikając przycisk **Resetuj**.

Korzystanie z opcji aplikacji SystemGuard

Aplikacje SystemGuard monitorują, rejestrują w dzienniku i raportują potencjalnie nieupoważnione zmiany wykonane w rejestrze systemu Windows lub w krytycznych plikach systemowych oraz umożliwiają zarządzanie tymi zmianami. Nieuprawnione zmiany w rejestrze i plikach mogą spowodować uszkodzenie komputera, obniżenie poziomu jego zabezpieczeń lub zniszczenie cennych plików systemowych.

Zmiany w rejestrze i plikach są operacjami typowymi i często występującymi na komputerze. Ponieważ wiele takich zmian jest niebezpiecznych, domyślne ustawienia aplikacji SystemGuard są tak skonfigurowane, aby zapewnić pewną, inteligentną i rzeczywistą ochronę przed nieupoważnionymi zmianami, które wydają się być niebezpieczne. Na przykład gdy aplikacje SystemGuard wykryją zmiany, które są nietypowe i stwarzają potencjalnie znaczne zagrożenie, ich aktywność jest natychmiast rejestrowana w dzienniku i tworzone są raporty. Zmiany, które są bardziej typowe, ale ciągle stwarzają pewną potencjalną możliwość powstania uszkodzeń, są tylko rejestrowane. Natomiast monitorowanie zmian typowych i o niskim zagrożeniu jest domyślnie wyłączone. Technologia aplikacji SystemGuard może zostać skonfigurowana w celu rozciągnięcia ochrony na dowolne środowisko.

Istnieją trzy rodzaje aplikacji SystemGuard: Programowi strażnicy systemu, aplikacje SystemGuard z kategorii Windows oraz Strażnicy systemu dla przeglądarki.

Programowi strażnicy systemu

Programowi strażnicy systemu wykrywają potencjalnie nieupoważnione zmiany w rejestrze komputera i innych plikach krytycznych, które mają zasadnicze znaczenie dla systemu Windows. Te ważne elementy rejestru i pliki obejmują instalacje formantów ActiveX, elementy uaktywniane podczas uruchamiania systemu, uchwyty uruchamiania powłoki systemu Windows oraz opóźnione ładowanie obiektów usług powłoki. Monitorując te elementy, Programowi strażnicy systemu oprócz oprogramowania szpiegującego i potencjalnie niepożądanych programów zatrzymują także podejrzane formanty ActiveX (pobrane z Internetu), które mogą uruchamiać się automatycznie wraz ze startem systemu Windows.

Aplikacje SystemGuard z kategorii Windows

Aplikacje SystemGuard z kategorii Windows także wykrywają potencjalnie nieupoważnione zmiany w rejestrze komputera i innych plikach krytycznych, które mają zasadnicze znaczenie dla systemu Windows. Te ważne elementy rejestru i pliki obejmują programy obsługi menu kontekstowego, biblioteki DLL AppInit oraz plik Hosts systemu Windows. Monitorując te elementy, aplikacje SystemGuard z kategorii Windows pomagają w zapobieganiu przed wysyłaniem i odbieraniem nieupoważnionych informacji z komputera przez Internet. Oprócz tego pomagają także w zatrzymywaniu podejrzanych programów, które wprowadzają niepożądane zmiany do wyglądu i działania programów ważnych dla użytkowników komputera.

Strażnicy systemu dla przeglądarki

Strażnicy systemu dla przeglądarki, podobnie jak aplikacje z kategorii Program i Windows, także wykrywają potencjalnie nieupoważnione zmiany w rejestrze komputera i innych plikach krytycznych, które mają zasadnicze znaczenie dla systemu Windows. Strażnicy systemu dla przeglądarki monitorują także zmiany w ważnych pozycjach rejestru i plikach, takich jak dodatki do programu Internet Explorer, adresy URL programu Internet Explorer oraz strefy zabezpieczeń programu Internet Explorer. Monitorując te elementy, Strażnicy systemu dla przeglądarki pomagają w zapobieganiu nieupoważnionym działaniom przeglądarki, takim jak przekierowania do podejrzanych witryn sieci Web, zmiany opcji i ustawień przeglądarki bez wiedzy użytkownika czy niepożądane dodawanie podejrzanych witryn sieci Web do zaufanych.

Włącz ochronę za pomocą aplikacji SystemGuard

Włączenie aplikacji SystemGuard umożliwia wykrywanie potencjalnie nieupoważnionych zmian w rejestrze systemu Windows i plikach komputera oraz ostrzeganie przed takimi zmianami. Nieuprawnione zmiany w rejestrze i plikach mogą spowodować uszkodzenie komputera, obniżenie poziomu jego zabezpieczeń lub zniszczenie cennych plików systemowych.

1 Otwórz okienko konfiguracji Komputer i pliki.

Jak to zrobić?

1. W okienku po lewej stronie kliknij opcję **Menu zaawansowane**.
2. Kliknij przycisk **Konfiguruj**.
3. W okienku konfiguracji kliknij opcję **Komputer i pliki**.

2 W polu **Ochrona przez program SystemGuard** kliknij opcję **Włączona**.

Uwaga: Ochronę przez program SystemGuard można wyłączyć, klikając opcję **Wyłączone**.

Konfigurowanie opcji aplikacji SystemGuard

Do konfigurowania opcji ochrony i ostrzegania przed nieupoważnionymi zmianami w rejestrze i plikach związanych z plikami systemu Windows, programami i przeglądarką Internet Explorer oraz rejestrowania tych zmian w dzienniku służy okienko Programy SystemGuard. Nieuprawnione zmiany w rejestrze i plikach mogą spowodować uszkodzenie komputera, obniżenie poziomu jego zabezpieczeń lub zniszczenie cennych plików systemowych.

1 Otwórz okienko Programy SystemGuard.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Komputer i pliki**.
3. W obszarze informacji kategorii Komputer i pliki kliknij opcję **Konfiguruj**.
4. Upewnij się, że w okienku konfiguracji Komputer i pliki ochrona przez program SystemGuard jest włączona, a następnie kliknij przycisk **Zaawansowane**.

2 Wybierz z listy typ aplikacji SystemGuard.

- **Programowi strażnicy systemu**
- **Aplikacje SystemGuard z kategorii Windows**
- **Strażnicy systemu dla przeglądarki**

3 W obszarze **Działanie** wykonaj jedną z następujących czynności:

- Aby wykrywać, rejestrować i raportować nieupoważnione zmiany w rejestrze i plikach skojarzone z aplikacjami SystemGuard z kategorii Program, Windows i Przeglądarka, kliknij opcję **Pokaż alerty.**
- Aby wykrywać i rejestrować nieupoważnione zmiany w rejestrze i plikach skojarzone z aplikacjami SystemGuard z kategorii Program, Windows i Przeglądarka, kliknij opcję **Rejestruj tylko zmiany.**
- Aby wyłączyć wykrywanie nieupoważnionych zmian w rejestrze i plikach skojarzone z aplikacjami SystemGuard z kategorii Program, Windows i Przeglądarka, kliknij opcję **Wyłącz ten program SystemGuard.**

Uwaga: Aby uzyskać więcej informacji na temat aplikacji SystemGuard, zobacz *Rodzaje aplikacji SystemGuard — informacje* (strona 51).

Rodzaje aplikacji SystemGuard — informacje

Aplikacje SystemGuard wykrywają potencjalnie nieupoważnione zmiany w rejestrze komputera i innych plikach krytycznych, które mają zasadnicze znaczenie dla systemu Windows. Istnieją trzy rodzaje aplikacji SystemGuard: Programowi strażnicy systemu, aplikacje SystemGuard z kategorii Windows oraz Strażnicy systemu dla przeglądarki.

Programowi strażnicy systemu

Programowi strażnicy systemu oprócz oprogramowania szpiegującego i potencjalnie niepożądanych programów zatrzymują także podejrzane formanty ActiveX (pobrane z Internetu), które mogą uruchamiać się automatycznie wraz ze startem systemu Windows.

SystemGuard	Wykrywa...
Instalacje formantów ActiveX	Nieuprawnione zmiany w rejestrze dotyczące instalacji formantów ActiveX, które mogą spowodować uszkodzenie komputera, obniżenie poziomu jego zabezpieczeń lub zniszczenie cennych plików systemowych.
Elementy uaktywniane podczas uruchamiania systemu	Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą instalować pliki zmieniające elementy uaktywniane podczas uruchamiania systemu, umożliwiając uruchamianie podejrzanych programów podczas uruchamiania komputera.
Uchwyty uruchamiania powłoki systemu Windows	Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą instalować uchwyty uruchamiania powłoki systemu Windows, aby uniemożliwić prawidłowe działanie programów zabezpieczających.
Shell Service Object Delay Load (Opóźnione ładowanie obiektów usług powłoki)	Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące opóźnionego ładowania obiektów usług powłoki, umożliwiając uruchamianie szkodliwych plików podczas uruchamiania komputera.

Aplikacje SystemGuard z kategorii Windows

Aplikacje SystemGuard z kategorii Windows pomagają w zapobieganiu przed wysyłaniem i odbieraniem nieupoważnionych informacji z komputera przez Internet. Oprócz tego pomagają także w zatrzymywaniu podejrzanych programów, które wprowadzają niepożądane zmiany do wyglądu i działania programów ważnych dla użytkowników komputera.

SystemGuard	Wykrywa...
Programy obsługi menu kontekstowego	Nieuprawnione zmiany w rejestrze dotyczące programów obsługi menu kontekstowego w systemie Windows, które mogą spowodować zmianę wyglądu i zachowania tych menu. Menu kontekstowe umożliwiają wykonywanie na komputerze różnych akcji, na przykład po kliknięciu pliku prawym przyciskiem myszy.
Biblioteki DLL AppInit	Nieuprawnione zmiany w rejestrze dotyczące bibliotek AppInit_DLL w systemie Windows, które mogą umożliwić uruchamianie potencjalnie szkodliwych plików przy uruchomieniu komputera.
Plik Hosts systemu Windows	Oprogramowanie szpiegujące, oprogramowanie reklamowe i potencjalnie niepożądane programy, które mogą wprowadzać nieuprawnione zmiany w pliku Hosts systemu Windows, co umożliwi przekierowywanie przeglądarki do podejrzanych witryn sieci Web oraz blokowanie aktualizacji oprogramowania.
Powłoka Winlogon	Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące powłoki Winlogon, umożliwiając zastępowanie przeglądarki Windows Explorer przez inne programy.
Winlogon User Init	Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące usługi Winlogon User Init, umożliwiając uruchamianie podejrzanych programów podczas logowania użytkownika do systemu Windows.
Protokoły systemu Windows	Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące protokołów systemu Windows, wpływając na sposób wysyłania i odbierania informacji między komputerem a Internetem.
Dostawcy usługi warstwowej (Winsock)	Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące dostawców usługi warstwowej (LSP) Winsock, aby przechwytywać i zmieniać informacje wysyłane i odbierane przez Internet.

Polecenia Otwórz powłoki systemu Windows	Nieuprawnione zmiany w poleceniach Otwórz powłoki systemu Windows, które mogą umożliwić uruchamianie na komputerze robaków i innych szkodliwych programów.
Udostępniony harmonogram zadań	Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze i plikach dotyczących Udostępnionego harmonogramu zadań, umożliwiając uruchamianie potencjalnie szkodliwych plików podczas uruchamiania komputera.
Usługa Posłaniec systemu Windows	Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące usługi Windows Messenger, umożliwiając wyświetlanie niechcianych reklam i zdalne uruchamianie programów na komputerze.
Plik win.ini systemu Windows	Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w pliku Win.ini, umożliwiając uruchamianie podejrzanych programów podczas uruchamiania komputera.

Strażnicy systemu dla przeglądarki

Strażnicy systemu dla przeglądarki pomagają w zapobieganiu nieupoważnionym działaniom przeglądarki, takim jak przekierowania do podejrzanych witryn sieci Web, zmiany opcji i ustawień przeglądarki bez wiedzy użytkownika czy niepożądane dodawanie podejrzanych witryn sieci Web do zaufanych.

SystemGuard	Wykrywa...
Obiekty pomocnicze przeglądarki	Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą używać obiektów pomocniczych przeglądarki do śledzenia przeglądanych stron sieci Web i wyświetlania niechcianych reklam.
Paski przeglądarki Internet Explorer	Nieuprawnione zmiany w rejestrze dotyczące programów na pasku programu Internet Explorer, takich jak Szukaj i Ulubione, które mogą spowodować zmianę wyglądu i zachowania programu Internet Explorer.
Dodatki do programu Internet Explorer	Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą instalować dodatki do programu Internet Explorer, aby śledzić przeglądane strony sieci Web i pokazywać niechciane reklamy.
Obiekt ShellBrowser przeglądarki Internet Explorer	Nieuprawnione zmiany w rejestrze dotyczące obiektu ShellBrowser przeglądarki Internet Explorer, które mogą spowodować zmianę wyglądu i zachowania przeglądarki internetowej.

Obiekt WebBrowser przeglądarki Internet Explorer	Nieuprawnione zmiany w rejestrze dotyczące obiektu Web Browser przeglądarki Internet Explorer, które mogą spowodować zmianę wyglądu i zachowania przeglądarki.
Uchwyty wyszukiwania adresów URL przeglądarki Internet Explorer	Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące uchwytów wyszukiwania adresów URL w przeglądarce Internet Explorer, umożliwiając przekierowywanie przeglądarki do podejrzanych witryn sieci Web podczas przeszukiwania Internetu.
Adresy URL przeglądarki Internet Explorer	Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące adresów URL programu Internet Explorer, zmieniając ustawienia przeglądarki.
Ograniczenia przeglądarki Internet Explorer	Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące ograniczeń programu Internet Explorer, zmieniając ustawienia i opcje przeglądarki.
Strefy zabezpieczeń przeglądarki Internet Explorer	Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące stref zabezpieczeń programu Internet Explorer, umożliwiając uruchamianie potencjalnie szkodliwych plików podczas uruchamiania komputera.
Zaufane witryny przeglądarki Internet Explorer	Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące zaufanych witryn przeglądarki Internet Explorer, powodując, że przeglądarka będzie traktowała podejrzane witryny sieci Web jako zaufane.
Zasady przeglądarki Internet Explorer	Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące zasad przeglądarki Internet Explorer, zmieniając wygląd i zachowanie przeglądarki.

Używanie list zaufanych

Jeśli program VirusScan wykryje zmianę w rejestrze lub pliku (SystemGuard), program lub przepełnienie bufora, wyświetli monit o zaufanie wykrytemu elementowi bądź jego usunięcie. Jeśli użytkownik ufa elementowi i wskaże, że nie chce być ponownie powiadamiany o takiej aktywności, element zostanie dodany do listy zaufanych elementów, a program VirusScan nie będzie w przyszłości wykrywał ani powiadamiał o takiej aktywności. Jeśli element zostanie dodany do listy zaufanych, ale użytkownik zdecyduje, że chce blokować jego aktywność, możliwe jest późniejsze jego usunięcie z listy. Blokowanie zapobiega przed uruchomianiem elementu lub wprowadzaniem zmian w komputerze bez powiadomienia za każdym razem, gdy podejmowana jest taka próba. Element może zostać także usunięty z listy zaufanych. Usunięcie spowoduje, że program VirusScan będzie ponownie wykrywał aktywność takiego elementu.

Zarządzanie listami zaufanych

Opcje w okienku Listy zaufanych umożliwiają zezwolenie lub zablokowanie działania elementów, które zostały już wcześniej wykryte i dodane do zaufanych. Można również usuwać elementy z listy — wtedy program VirusScan wykryje je od nowa.

1 Otwórz okienko Listy zaufanych

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Komputer i pliki**.
3. W obszarze informacji kategorii Komputer i pliki kliknij opcję **Konfiguruj**.
4. Upewnij się, że w okienku konfiguracji Komputer i pliki jest włączona ochrona przed wirusami, a następnie kliknij przycisk **Zaawansowane**.
5. Kliknij opcję **Listy zaufanych** w okienku Ochrona przed wirusami.

2 Zaznacz jeden z następujących typów list zaufanych elementów:

- **Programowi strażnicy systemu**
- **Aplikacje SystemGuard z kategorii Windows**
- **Strażnicy systemu dla przeglądarki**
- **Zaufane programy**
- **Zaufane przepełnienia buforu**

3 W obszarze **Działanie** wykonaj jedną z następujących czynności:

- Aby zezwolić wykrytemu elementowi na wprowadzanie zmian w rejestrze systemu Windows lub kluczowych plikach systemowych na komputerze bez powiadamiania Cię, zaznacz opcję **Ufaj**.
- Aby zablokować wykrytemu elementowi możliwość wprowadzania zmian w rejestrze systemu Windows lub kluczowych plikach systemowych na komputerze bez powiadamiania Cię, zaznacz opcję **Zablokuj**.
- Aby usunąć wykryty element z listy zaufanych, zaznacz opcję **Usuń**.

4 Kliknij przycisk **OK**.

Uwaga: Aby uzyskać więcej informacji na temat rodzajów list zaufanych, zobacz *Typy list zaufanych — informacje* (strona 56).

Typy list zaufanych — informacje

Wpisy aplikacji SystemGuard znajdujące się w okienku Listy zaufanych adresów ukazują wcześniejsze nieautoryzowane modyfikacje rejestru i plików wykryte przez program VirusScan, które użytkownik dopuścił z poziomu komunikatu alertu lub okienka Wyniki wyszukiwania. Opcje zawarte w okienku umożliwiają zarządzanie pięcioma rodzajami list: Programowi strażnicy systemu, Aplikacje SystemGuards z kategorii Windows, Strażnicy systemu dla przeglądarki, Zaufane programy i Zaufane przepełnienia buforu.

Opcja	Opis
Programowi strażnicy systemu	Wpisy programowych strażników systemu znajdujące się w okienku Listy zaufanych adresów ukazują wcześniejsze nieautoryzowane modyfikacje rejestru i plików wykryte przez program VirusScan, które użytkownik dopuścił z poziomu komunikatu alertu lub okienka Wyniki wyszukiwania. Strażnicy ci wykrywają nieuprawnione zmiany w rejestrze i plikach związane z instalacją formantów ActiveX, elementami uaktywnianymi podczas uruchamiania systemu, uchwytami uruchamiania powłoki systemu Windows oraz opóźnionym ładowaniem obiektów usług powłoki. Opisane zmiany mogą spowodować uszkodzenie komputera, obniżenie poziomu jego bezpieczeństwa lub zniszczenie cennych plików systemowych.

Aplikacje SystemGuard z kategorii Windows	Wpisy aplikacji SystemGuard z kategorii Windows znajdujące się w okienku Listy zaufanych adresów ukazują wcześniejsze nieautoryzowane modyfikacje rejestru i plików wykryte przez program VirusScan, które użytkownik dopuścił z poziomu komunikatu alertu lub okienka Wyniki wyszukiwania. Aplikacje te wykrywają nieuprawnione zmiany w rejestrze i plikach związane z programami obsługi menu kontekstowych, bibliotekami DLL inicjowania aplikacji, plikiem Hosts systemu Windows, powłoką Winlogon, dostawcami usługi warstwowej (LSP) Winsock itd. Opisane zmiany mogą wpływać na wysyłanie i odbieranie informacji między komputerem a Internetem oraz wygląd i działanie programów, a także umożliwiać uruchamianie podejrzanych programów na komputerze.
Strażnicy systemu dla przeglądarki	Wpisy strażników systemu dla przeglądarki znajdujące się w okienku Listy zaufanych adresów ukazują wcześniejsze nieautoryzowane modyfikacje rejestru i plików wykryte przez program VirusScan, które użytkownik dopuścił z poziomu komunikatu alertu lub okienka Wyniki wyszukiwania. Strażnicy ci wykrywają nieuprawnione zmiany w rejestrze i inne podejrzane zachowania związane z obiektami pomocniczymi przeglądarek, dodatkami do przeglądarki Internet Explorer, adresami URL otwieranymi w przeglądarce Internet Explorer, strefami zabezpieczeń przeglądarki Internet Explorer itd. Opisane zmiany mogą prowadzić do wykonywania niepożądanych operacji w przeglądarce, takich jak przekierowywanie do podejrzanych witryn sieci Web, modyfikowanie ustawień i opcji przeglądarki czy obdarzanie zaufaniem podejrzanych witryn sieci Web.
Zaufane programy	Zaufane programy to potencjalnie niepożądane programy wykryte przez aplikację VirusScan, wobec których z poziomu komunikatu alertu lub okienka Wyniki wyszukiwania użytkownik określił relację zaufania.
Zaufane przepełnienia buforu	Zaufane przepełnienia buforu to wcześniejsze niepożądane działania wykryte przez program VirusScan, wobec których z poziomu komunikatu alertu lub okienka Wyniki wyszukiwania użytkownik określił relację zaufania. Przepełnienia buforów mogą spowodować uszkodzenie komputera i zniszczenie plików. Przepełnienia buforów występują, gdy ilość informacji przechowywanych w buforze przez podejrzane programy lub procesy przekracza pojemność buforu.

ROZDZIAŁ 11

Skanowanie komputera

Podczas pierwszego uruchomienia programu SecurityCenter moduł ochrony antywirusowej w czasie rzeczywistym zawarty w aplikacji VirusScan zaczyna chronić komputer przed potencjalnie szkodliwymi wirusami, koniami trojańskimi i innymi zagrożeniami bezpieczeństwa. Jeśli ów moduł ochrony pozostanie włączony, aplikacja na bieżąco monitoruje komputer w poszukiwaniu objawów aktywności wirusów, skanując pliki w reakcji na każdą operację dostępu. Skanowanie odbywa się przy użyciu opcji skanowania w czasie rzeczywistym ustawionych przez użytkownika. Aby mieć pewność, że komputer jest skutecznie chroniony przez najnowszymi zagrożeniami, moduł powinien być cały czas włączony, a dodatkowo należy przygotować harmonogram regularnych, bardziej kompleksowych skanowań ręcznych. Aby uzyskać więcej informacji na temat konfigurowania opcji skanowania w czasie rzeczywistym i skanowania ręcznego, zobacz *Konfigurowanie ochrony przed wirusami* (strona 41).

Aplikacja VirusScan zawiera zestaw bardziej szczegółowych opcji skanowania przeznaczonych dla wariantu ręcznej ochrony antywirusowej. Umożliwiają one okresowe przeprowadzanie sesji skanowania rozszerzonego. Skanowania ręczne można inicjować z poziomu programu SecurityCenter, wybierając określone lokalizacje zgodnie z ustalonym harmonogramem. W razie potrzeby skanowanie takie można zainicjować również z poziomu Eksploratora Windows, w trakcie pracy. Zaletą inicjowania skanowania z programu SecurityCenter jest możliwość zmiany opcji skanowania w trakcie sesji, jednak skanowanie za pośrednictwem Eksploratora Windows jest wygodniejsze z perspektywy bezpieczeństwa komputera.

W obu przypadkach po zakończeniu skanowania można obejrzeć jego wyniki. Dzięki temu można ustalić, czy program VirusScan wykrył, naprawił lub poddał kwarantannie wirusy, konie trojańskie, oprogramowanie szpiegujące, oprogramowanie reklamowe, pliki cookie lub inne potencjalnie szkodliwe programy. Rezultaty skanowania mogą być wyświetlane na różne sposoby. Można na przykład obejrzeć sumaryczne (ogólne) wyniki sesji albo szczegółowe informacje, obejmujące np. stan i rodzaj infekcji. Aplikacja pozwala również wyświetlić zbiorcze statystyki skanowania i wykrywania.

W tym rozdziale

Skanowanie komputera

Ręczne skanowanie komputera można zainicjować zarówno z zaawansowanego, jak i podstawowego menu programu SecurityCenter. W przypadku menu zaawansowanego przed rozpoczęciem skanowania można potwierdzić jego ustawienia. W przypadku menu podstawowego skanowanie rozpoczyna się natychmiast, z użyciem aktualnie ustawionych opcji skanowania. Skanowanie z poziomu Eksploratora Windows również bazuje na istniejących ustawieniach.

- Wykonaj jedną z następujących czynności:

  Skanowanie z poziomu programu SecurityCenter

Aby...	Wykonaj następujące czynności:
Skanować przy użyciu istniejących ustawień	W menu podstawowym kliknij opcję **Skanuj**.
Skanować przy użyciu zmodyfikowanych ustawień	W menu zaawansowanym kliknij opcję **Skanuj**, zaznacz lokalizacje, które chcesz przeskanować, wybierz opcje skanowania i kliknij przycisk **Skanuj teraz**.

  Skanowanie z poziomu Eksploratora Windows

  1. Otwórz Eksploratora Windows.
  2. Kliknij prawym przyciskiem myszy żądany plik, folder lub dysk, a następnie kliknij przycisk **Skanuj**.

Uwaga: Wyniki skanowania są wyświetlane w oknie alertu Skanowanie zostało zakończone. W wynikach znajdują się informacje o liczbie obiektów zeskanowanych, wykrytych, naprawionych, poddanych kwarantannie i usuniętych. Aby uzyskać więcej informacji o wynikach skanowania lub wykonać operacje na zainfekowanych plikach, kliknij przycisk **Wyświetl szczegóły skanowania**.

Wyświetl wyniki skanowania

Po zakończeniu skanowania ręcznego można wyświetlić jego wyniki i zobaczyć dzięki temu, jakie zagrożenia zostały wykryte oraz jaki jest obecny stan ochrony komputera. Wyniki pokazują, czy program VirusScan wykrył, naprawił lub poddał kwarantannie wirusy, konie trojańskie, oprogramowanie szpiegujące, oprogramowanie reklamowe, pliki cookie czy inne potencjalnie szkodliwe programy.

- W menu podstawowym lub zaawansowanym kliknij polecenie **Skanuj**, a następnie wykonaj jedną z następujących operacji:

Aby...	Wykonaj następujące czynności:
Wyświetlić wyniki skanowania w oknie alertu	Obejrzyj wyniki skanowania w oknie alertu Skanowanie zostało zakończone.
Wyświetlić dokładniejsze informacje o wynikach skanowania	W oknie alertu Skanowanie zostało zakończone kliknij przycisk **Wyświetl szczegóły skanowania**.
Wyświetlić streszczenie wyników skanowania	Na pasku zadań w obszarze powiadomień umieść wskaźnik myszy na ikonie **Skanowanie zostało zakończone**.
Wyświetlić statystykę skanowania i wykrywania	Na pasku zadań w obszarze powiadomień kliknij dwukrotnie ikonę **Skanowanie zostało zakończone**.
Wyświetlić szczegółowe informacje o wykrytych elementach oraz stanie i rodzaju infekcji	Na pasku zadań w obszarze powiadomień kliknij dwukrotnie ikonę **Skanowanie zostało zakończone**, a następnie w okienku Postęp skanowania: Skanowanie ręczne kliknij przycisk **Wyświetl wyniki**.

ROZDZIAŁ 12

Wykonywanie operacji na wynikach skanowania

Jeśli podczas skanowania w czasie rzeczywistym lub skanowania ręcznego aplikacja VirusScan wykryje zagrożenie bezpieczeństwa, próbuje automatycznie je usunąć w sposób odpowiedni dla rodzaju zagrożenia. Na przykład w reakcji na wykryty wirus, konia trojańskiego lub śledzący plik cookie próbuje wyczyścić zainfekowany plik. Jeśli nie można wykonać czyszczenia, plik jest poddawany kwarantannie.

W przypadku niektórych zagrożeń aplikacja VirusScan może nie być w stanie ani wyczyścić pliku, ani poddać go kwarantannie. Wtedy wyświetla monit o podjęcie działania przez samego użytkownika. Wybór zależy od rodzaju zagrożenia. Jeśli na przykład w pliku został wykryty wirus, w razie niepowodzenia obu operacji aplikacja blokuje do niego dostęp. W przypadku śledzących plików cookie użytkownik może zdecydować o ich usunięciu lub obdarzeniu zaufaniem. Gdy zostaną wykryte potencjalnie niepożądane programy, aplikacja VirusScan automatycznie nie podejmuje żadnych działań, pozostawiając użytkownikowi wybór między ustanowieniem relacji zaufania a poddaniem programu kwarantannie.

Kwarantanna polega na zaszyfrowaniu, a następnie odizolowaniu plików, programów czy plików cookie w osobnym folderze, dzięki czemu nie zagrażają one już komputerowi. Elementy poddane kwarantannie można przywracać lub trwale usuwać. Przeważnie pliki cookie poddane kwarantannie można usunąć bez szkody dla systemu, jeśli jednak kwarantanna będzie dotyczyła programu, który użytkownik zna i z którego korzysta, warto rozważyć jego przywrócenie.

W tym rozdziale

Wykonywanie operacji na wirusach i koniach trojańskich

Jeśli podczas skanowania w czasie rzeczywistym lub skanowania ręcznego aplikacja VirusScan wykryje w pliku na komputerze wirusa lub konia trojańskiego, próbuje wyczyścić taki plik. Jeśli jest to niemożliwe, próbuje poddać go kwarantannie. Jeśli również ta operacja kończy się niepowodzeniem, blokuje dostęp do takiego pliku (dotyczy tylko skanowań w czasie rzeczywistym).

1 Otwórz okienko Wyniki skanowania.

Jak to zrobić?

1. Na pasku zadań w obszarze powiadomień (prawy koniec paska) kliknij dwukrotnie ikonę **Skanowanie zostało zakończone**.
2. W okienku Postęp skanowania: Skanowanie ręczne kliknij przycisk **Wyświetl wyniki**.

2 Na liście wyników skanowania zaznacz pozycję **Wirusy i konie trojańskie**.

Uwaga: Informacje o możliwych działaniach na plikach poddanych kwarantannie przez program VirusScan znajdują się w części *Wykonywanie operacji na plikach poddanych kwarantannie* (strona 65).

Wykonywanie operacji na potencjalnie niepożądanych programach

Jeśli podczas skanowania w czasie rzeczywistym lub skanowania ręcznego aplikacja VirusScan wykryje na komputerze potencjalnie niepożądany program, oferuje możliwość usunięcia go lub obdarzenia zaufaniem. Usunięcie programu w rzeczywistości nie powoduje wykasowania go z komputera, a jedynie poddanie kwarantannie, tak aby nie uszkodził komputera lub plików.

1 Otwórz okienko Wyniki skanowania.

Jak to zrobić?

1. Na pasku zadań w obszarze powiadomień (prawy koniec paska) kliknij dwukrotnie ikonę **Skanowanie zostało zakończone**.
2. W okienku Postęp skanowania: Skanowanie ręczne kliknij przycisk **Wyświetl wyniki**.

2 Na liście wyników skanowania zaznacz pozycję **Potencjalnie niepożądane programy**.

3 Zaznacz potencjalnie niepożądany program.

4 W obszarze **Działanie** zaznacz opcję **Usuń** lub **Ufaj**.

5 Potwierdź zaznaczenie opcji.

Wykonywanie operacji na plikach poddanych kwarantannie

Kwarantanna zainfekowanych plików polega na ich zaszyfrowaniu, a następnie przeniesieniu do osobnego folderu, skąd nie zagrażają już komputerowi. Pliki poddane kwarantannie można przywracać lub trwale usuwać.

1 Otwórz okienko Pliki poddane kwarantannie.

Jak to zrobić?

1. W okienku po lewej stronie kliknij opcję **Menu zaawansowane**.
2. Kliknij opcję **Przywróć**.
3. Kliknij opcję **Pliki**.

2 Zaznacz plik poddany kwarantannie.

3 Wykonaj jedną z następujących czynności:

- Aby naprawić zainfekowany plik i przywrócić go do pierwotnej lokalizacji na komputerze, zaznacz opcję **Przywróć**.
- Aby usunąć zainfekowany plik z komputera, zaznacz opcję **Usuń**.

4 Kliknij przycisk **Tak**, aby potwierdzić wybór opcji.

Wskazówka: W jednym kroku można przywrócić lub usunąć kilka plików.

Wykonywanie operacji na programach i plikach cookie poddanych kwarantannie

Kwarantanna potencjalnie niepożądanych programów lub śledzących plików cookie polega na ich zaszyfrowaniu, a następnie przeniesieniu do chronionego folderu, skąd nie zagrażają już komputerowi. Elementy poddane kwarantannie można przywracać lub trwale usuwać. Najczęściej usunięcie takiego elementu nie powoduje negatywnych skutków w systemie.

1 Otwórz okienko Programy w folderze kwarantanny i śledzące pliki cookie.

Jak to zrobić?

1. W okienku po lewej stronie kliknij opcję **Menu zaawansowane**.
2. Kliknij opcję **Przywróć**.
3. Kliknij opcję **Programy i pliki cookie**.

2 Zaznacz program lub plik poddany kwarantannie.

3 Wykonaj jedną z następujących czynności:

- Aby naprawić zainfekowany plik i przywrócić go do pierwotnej lokalizacji na komputerze, zaznacz opcję **Przywróć**.
- Aby usunąć zainfekowany plik z komputera, zaznacz opcję **Usuń**.

4 Kliknij przycisk **Tak**, aby potwierdzić operację.

Wskazówka: W jednym kroku można przywrócić lub usunąć kilka programów/plików cookie.

ROZDZIAŁ 13

McAfee Personal Firewall

Program Personal Firewall zapewnia zaawansowaną ochronę komputera i danych osobistych. Program Personal Firewall tworzy barierę między komputerem a Internetem, dyskretnie monitorując ruch internetowy w poszukiwaniu podejrzanych działań.

Uwaga: Program SecurityCenter zgłasza krytyczne i niekrytyczne problemy dotyczące ochrony natychmiast po ich wykryciu. Jeśli potrzebna jest pomoc w diagnozowaniu problemów dotyczących ochrony, można uruchomić narzędzie McAfee Virtual Technician.

W tym rozdziale

Funkcje programu Personal Firewall

Program Personal Firewall zawiera poniższe funkcje.

Standardowy poziomy ochrony i poziomy niestandardowe

Ochrona przed włamaniami i podejrzanymi działaniami z użyciem domyślnych ustawień programu Firewall lub ustawień niestandardowych.

Wyświetlane na bieżąco zalecenia

Otrzymywanie na bieżąco zaleceń pomaga w określeniu, czy programom należy przyznać dostęp do Internetu oraz, czy dany ruch sieciowy jest godny zaufania.

„Inteligentne" zarządzanie dostępem programów

Zarządzanie dostępem programów do Internetu za pośrednictwem alertów i dzienników zdarzeń lub konfigurowanie uprawnień dostępu dla określonych aplikacji.

Niezakłócanie korzystania z gier

Zapobieganie wyświetlaniu alertów dotyczących prób włamania i podejrzanych działań w trakcie korzystania z gier na pełnym ekranie.

Ochrona komputera podczas uruchamiania

Podczas uruchamiania systemu Windows® program Firewall chroni komputer użytkownika przed próbami włamania, niepożądanymi programami i niepożądanym ruchem sieciowym.

Nadzorowanie portów usług systemowych

Zarządzanie otwartymi i zamkniętymi portami usług systemowych wymaganymi przez niektóre aplikacje.

Zarządzanie połączeniami z komputerem

Zezwalanie na zdalne połączenia między komputerem użytkownika a innymi komputerami oraz blokowanie takich połączeń.

Kompleksowe informacje w witrynie HackerWatch

Śledzenie pochodzących z całego świata wzorców ataków i włamań za pośrednictwem witryny HackerWatch, która dostarcza najświeższych wiadomości o programach działających na komputerze użytkownika oraz kompleksowych statystyk zdarzeń dotyczących bezpieczeństwa i portów internetowych.

Blokowanie programu Firewall

Natychmiastowe zablokowanie całego przychodzącego i wychodzącego ruchu sieciowego między komputerem użytkownika a Internetem.

Przywracanie ustawień programu Firewall

Natychmiastowe przywrócenie pierwotnych ustawień ochrony programu Firewall.

Zaawansowane wykrywanie koni trojańskich

Wykrywanie i blokowanie dostępu do Internetu potencjalnie złośliwych aplikacji, takich jak konie trojańskie, oraz zapobiegania przekazywaniu przez nie danych osobistych użytkownika.

Rejestrowanie zdarzeń

Śledzenie przychodzącego i wychodzącego ruchu sieciowego w ostatnim czasie oraz najnowszych zdarzeń związanych z włamaniami.

Monitorowanie ruchu internetowego

Możliwość przeglądania map geograficznych całego świata, które przedstawiają źródła wrogich ataków i ruchu na całym świecie. Ponadto można uzyskać szczegółowe informacje na temat właściciela oraz dane geograficzne źródłowych adresów IP. Można również analizować ruch przychodzący i wychodzący oraz monitorować wykorzystanie przepustowości przez programy i ich działanie.

Ochrona przed włamaniami

Ochrona prywatności użytkownika przed możliwymi zagrożeniami płynącymi z Internetu. Za pomocą funkcji zbliżonych do heurystycznych firma McAfee zapewnia trójwarstwową ochronę przez blokowanie elementów wykazujących symptomy ataków lub cechy charakterystyczne dla prób włamań.

Zaawansowana analiza ruchu

Sprawdzanie przychodzącego i wychodzącego ruchu internetowego oraz połączeń programów, m.in. takich, które aktywnie „nasłuchują” w oczekiwaniu na otwarcie połączeń. Umożliwia to zauważenie programów, które mogą być narażone na włamania, i podjęcie w stosunku do nich odpowiednich działań.

ROZDZIAŁ 14

Uruchamianie programu Firewall

Po zainstalowaniu programu Firewall komputer będzie chroniony przed włamaniami i niepożądanym ruchem sieciowym. Ponadto można obsługiwać alerty i zarządzać dostępem dla przychodzących i wychodzących połączeń z Internetem znanych i nieznanych programów. Automatycznie są włączone funkcja Inteligentne zalecenia i poziom zabezpieczeń Zaufany (z wybraną opcją zezwolenia programom na dostęp do Internetu tylko dla ruchu wychodzącego).

Jeśli zapora zostanie wyłączona w okienku Konfiguracja sieci i Internetu, komputer przestanie być chroniony przed włamaniami i niepożądanym ruchem sieciowym oraz nie będzie możliwe skuteczne zarządzanie przychodzącymi i wychodzącymi połączeniami internetowymi. Jeśli trzeba wyłączyć ochronę programu Firewall, należy to robić tymczasowo i tylko w razie potrzeby. Zaporę można również wyłączyć w panelu Konfiguracja sieci i Internetu.

Zapora automatycznie wyłącza zaporę systemu Windows® i staje się zaporą domyślną.

Uwaga: Aby skonfigurować program Firewall, należy otworzyć okienko Konfiguracja Internetu i sieci.

W tym rozdziale

Włączanie ochrony przy użyciu zapory

Włączenie ochrony programu Firewall zabezpiecza komputer przed włamaniami i niepożądanym ruchem sieciowym oraz pomaga w zarządzaniu wychodzącymi i przychodzącymi połączeniami internetowymi.

1. W okienku McAfee SecurityCenter kliknij najpierw przycisk **Internet i sieć**, a następnie przycisk **Konfiguruj**.
2. W okienku Konfiguracja Internetu i sieci, w obszarze **Ochrona przy użyciu zapory jest wyłączona** kliknij przycisk **Włącz**.

Wyłączanie ochrony przy użyciu zapory

Program Firewall można wyłączyć, jeśli zabezpieczanie komputera przed włamaniami i niepożądanym ruchem sieciowym jest zbędne. Po wyłączeniu programu Firewall nie można zarządzać przychodzącymi i wychodzącymi połączeniami internetowymi.

1. W okienku McAfee SecurityCenter kliknij najpierw przycisk **Internet i sieć**, a następnie przycisk **Konfiguruj**.
2. W okienku Konfiguracja Internetu i sieci, w obszarze **Ochrona przy użyciu zapory jest włączona** kliknij przycisk **Wyłącz**.

ROZDZIAŁ 15

Praca z alertami

Zapora wykorzystuje szereg alertów pomagających zarządzać bezpieczeństwem użytkownika. Alerty te można podzielić na trzy podstawowe typy:

- Czerwony alert
- Żółty alert
- Zielony alert

Alerty mogą także zawierać informacje pomocne w podjęciu reakcji na nie lub uzyskaniu informacji o programach działających na komputerze.

W tym rozdziale

Informacje o alertach

Zapora wykorzystuje trzy podstawowe typy alertów. Ponadto w niektórych alertach są zawarte informacje pomagające uzyskać informacje o programach działających na komputerze użytkownika.

Czerwony alert

Czerwony alert zostaje wyświetlony, gdy przy użyciu zapory wykryto a następnie zablokowano konia trojańskiego na komputerze użytkownika i zawiera zalecenie wykonania skanowania w celu wykrycia dodatkowych zagrożeń. Koń trojański sprawia wrażenie normalnego programu, lecz może zakłócić pracę komputera użytkownika, uszkodzić go lub umożliwić nieautoryzowany dostęp do niego. Ten alert występuje na wszystkich poziomach zabezpieczeń oprócz poziomu Otwarty.

Żółty alert

Najczęściej występujący typ alertu to żółty alert, który informuje o działaniu aplikacji lub zdarzeniu sieciowym wykrytym przez program Firewall. Po zaistnieniu takiej sytuacji alert podaje opis działania aplikacji lub zdarzenia sieciowego, a następnie wyświetla jedną lub kilka opcji, które wymagają podjęcia wyboru przez użytkownika. Na przykład alert **Wykryto nową sieć** jest wyświetlany, gdy komputer z zainstalowanym programem Firewall został podłączony do nowej sieci. Można wybrać czy ufać lub nie ufać tej sieci. Jeśli sieć zostanie określona jako zaufana, zapora zezwala na ruch z dowolnego komputera w tej sieci, a jej adres jest dodawany do listy Zaufane adresy IP. Jeśli inteligentne zalecenia są włączone, programy są dodawane do listy w okienku Uprawnienia programów.

Zielony alert

W większości przypadków zielony alert zawiera podstawowe informacje o zdarzeniu i nie wymaga reakcji. Zielone alerty są domyślnie wyłączone i zwykle występują na poziomach zabezpieczeń Standardowy, Zaufany, Wysoki i Ukryty.

Pomoc dla użytkownika

W wielu alertach programu Firewall zawarte są dodatkowe informacje pomagające zarządzać bezpieczeństwem komputera użytkownika, m.in.:

- **Więcej informacji na temat tego programu**: Przejście do witryny firmy McAfee poświęconej globalnemu bezpieczeństwu, gdzie można uzyskać informacje o programie wykrytym przez zaporę na komputerze użytkownika.
- **Poinformuj firmę McAfee o tym programie**: Przesłanie informacji do firmy McAfee o nieznanym pliku wykrytym przez zaporę na komputerze użytkownika.

- **Firma McAfee zaleca**: Porada na temat postępowania z alertami. Alert może np. zawierać zalecenie zezwolenia programowi na dostęp do Internetu.

ROZDZIAŁ 16

Zarządzanie alertami informacyjnymi

Podczas korzystania z programu Firewall można wyświetlać lub ukrywać alerty informacyjne, które są wyświetlane po wykryciu prób włamań lub podejrzanej aktywności podczas określonych zdarzeń, np. w trakcie korzystania z gier na pełnym ekranie.

W tym rozdziale

Wyświetlanie alertów podczas korzystania z gier

Można zezwolić na wyświetlane alertów programu Firewall dotyczących wykrycia prób włamań lub podejrzanej aktywności zaistniałej w trakcie korzystania z gier na pełnym ekranie.

1. W okienku McAfee SecurityCenter kliknij opcję **Menu zaawansowane**.
2. Kliknij przycisk **Konfiguruj**.
3. W okienku Konfiguracja programu SecurityCenter, w obszarze **Alerty** kliknij przycisk **Zaawansowane**.
4. W okienku Opcje alertów wybierz opcję **Pokazuj alerty informacyjne, gdy zostanie wykryty tryb gier**.
5. Kliknij przycisk **OK**.

Ukrywanie alertów informacyjnych

Można wyłączyć wyświetlanie alertów informacyjnych programu Firewall dotyczących wykrycia prób włamań lub podejrzanej aktywności.

1. W okienku McAfee SecurityCenter kliknij opcję **Menu zaawansowane**.
2. Kliknij przycisk **Konfiguruj**.
3. W okienku Konfiguracja programu SecurityCenter, w obszarze **Alerty** kliknij przycisk **Zaawansowane**.
4. W okienku Konfiguracja programu SecurityCenter kliknij opcję **Alerty informacyjne**.
5. W okienku Alerty informacyjne wykonaj jedną z następujących czynności:
   - Wybierz opcję **Nie pokazuj alertów informacyjnych**, aby ukryć wszystkie alerty informacyjne.
   - Aby ukryć dany alert, usuń zaznaczenie jego pola wyboru.
6. Kliknij przycisk **OK**.

ROZDZIAŁ 17

Konfigurowanie ochrony programu Firewall

Zapora oferuje wiele metod zarządzania bezpieczeństwem i dostosowania sposobu reakcji na zdarzenia i alerty dotyczące bezpieczeństwa.

Po zainstalowaniu programu Firewall po raz pierwszy ustawiany jest poziom zabezpieczeń komputera Zaufany, a aplikacje mają zezwolenie na dostęp do Internetu tylko dla ruchu wychodzącego. Jednak zapora udostępnia również inne poziomy, od bardzo restrykcyjnego do bardzo tolerancyjnego.

Zapora umożliwia również odbieranie zaleceń dotyczących alertów i dostępu programów do Internetu.

W tym rozdziale

Zarządzanie poziomami zabezpieczeń programu Firewall

Poziomy zabezpieczeń programu Firewall określają zakres zarządzania i reagowania na alerty. Alerty pojawiają się, gdy wykryje on niepożądany ruch sieciowy lub przychodzące i wychodzące połączenia internetowe. Domyślnie ustawiany jest poziom zabezpieczeń Zaufany, który zezwala na dostęp do Internetu tylko dla ruchu wychodzącego.

W przypadku ustawienia poziomu zabezpieczeń Zaufany i włączenia funkcji Inteligentne zalecenia żółte alerty są wyposażone w opcję zezwalania na dostęp lub jego blokowania nieznanym programom, która wymagają dostępu dla ruchu przychodzącego. W przypadku wykrycia znanych programów są wyświetlane zielone alerty informacyjne i następuje automatyczne zezwolenie na dostęp. Przyznanie dostępu umożliwia programowi nawiązywanie połączeń wychodzących i nasłuchiwanie w oczekiwaniu na połączenia przychodzące.

Ogólnie rzecz biorąc, im bardziej restrykcyjny poziom zabezpieczeń (poziom Ukryty i Wysoki), tym więcej jest wyświetlanych opcji i alertów, na które musi zareagować użytkownik.

W poniższej tabeli opisano sześć poziomów zabezpieczeń programu Firewall, począwszy od najbardziej restrykcyjnego do najbardziej tolerancyjnego:

Poziom	Opis
Blokada	Blokowanie wszystkich przychodzących i wychodzących połączeń sieciowych, w tym dostępu do witryn sieci Web, poczty e-mail oraz aktualizacji zabezpieczeń. Zastosowanie tego poziomu zabezpieczeń powoduje takie same skutki, jak wyłączenie połączenia z Internetem. Ustawienie to można wykorzystać do zablokowania portów ustawionych jako otwarte w okienku Usługi systemowe.
Ukryty	Blokowanie wszystkich przychodzących połączeń sieciowych z wyjątkiem otwartych portów, które powoduje ukrycie obecności komputera w Internecie. Zapora wyświetla alerty, gdy nowe programy próbują nawiązać połączenia wychodzące lub otrzymują żądania połączeń przychodzących. Zablokowane i dodane programy są wyświetlane w okienku Uprawnienia programów.
Wysoki	Wyświetlanie alertów, gdy nowe programy próbują nawiązać połączenia wychodzące lub otrzymują żądania połączeń przychodzących. Zablokowane i dodane programy są wyświetlane w okienku Uprawnienia programów. W przypadku ustawienia poziomu zabezpieczeń na Wysoki program żąda tylko tego typu dostępu, który jest mu aktualnie potrzebny, np. dostępu tylko do połączeń wychodzących, który użytkownik może przyznać lub zablokować. Później, jeśli program wymaga zarówno połączeń przychodzących, jak i wychodzących, można zezwolić mu na pełny dostęp w okienku Uprawnienia programów.

Standardowy	Monitorowanie połączeń przychodzących i wychodzących oraz wyświetlanie alertów, gdy nowe programy próbują uzyskać dostęp do Internetu. Zablokowane i dodane programy są wyświetlane w okienku Uprawnienia programów.
Zaufany	Zezwolenie programom na dostęp do Internetu albo dla połączeń przychodzących i wychodzących (pełny), albo tylko dla ruchu wychodzącego. Domyślnym poziomem zabezpieczeń jest Zaufany z wybraną opcją zezwolenia programom na dostęp do Internetu tylko dla ruchu wychodzącego. Jeśli dana aplikacja ma przyznany pełny dostęp, program Firewall automatycznie uznaje ją za zaufaną i umieszcza na liście dozwolonych aplikacji w okienku Uprawnienia programów. Jeśli dana aplikacja ma przyznany dostęp tylko dla ruchu wychodzącego, program Firewall automatycznie uznaje ją za zaufaną tylko przy nawiązywaniu wychodzącego połączenia z Internetem. Połączenie przychodzące nie jest automatycznie uznawane za zaufane.
Otwarty	Zezwalanie na wszystkie przychodzące i wychodzące połączenia internetowe.

Program Firewall umożliwia również natychmiastowe przywrócenie standardowego poziomu zabezpieczeń, czyli Zaufany (dostęp do Internetu tylko dla ruchu wychodzącego), w okienku Przywróć ustawienia domyślne ochrony przy użyciu zapory.

Ustawianie poziomu zabezpieczeń na poziom Blokada

Można ustawić poziom zabezpieczeń programu Firewall na Blokada, aby blokować wszystkie przychodzące i wychodzące połączenia sieciowe.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Poziom zabezpieczeń przesuń suwak tak, aby bieżącym poziomem był poziom **Blokada**.
4. Kliknij przycisk **OK**.

Ustawienie poziomu zabezpieczeń na Ukryty

Można ustawić poziom zabezpieczeń programu Firewall na Ukryty, aby blokować wszystkie przychodzące połączenia sieciowe z wyjątkiem otwartych portów, co powoduje ukrycie obecności komputera w Internecie.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Poziom zabezpieczeń przesuń suwak tak, aby bieżącym poziomem był poziom **Ukryty**.
4. Kliknij przycisk **OK**.

Uwaga: W trybie Ukryty program Firewall wyświetla alert, gdy nowe aplikacje żądają nawiązania wychodzącego połączenia internetowego lub otrzymują żądania nawiązania połączenia przychodzącego.

Ustawianie poziomu zabezpieczeń na Wysoki

Można ustawić poziom zabezpieczeń programu Firewall na Wysoki, aby otrzymywać alerty, gdy nowe aplikacje próbują nawiązać połączenia wychodzące lub otrzymują żądania połączeń przychodzących.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Poziom zabezpieczeń przesuń suwak tak, aby bieżącym poziomem był poziom **Wysoki**.
4. Kliknij przycisk **OK**.

Uwaga: W trybie Wysoki program żąda tylko tego typu dostępu, który jest mu aktualnie potrzebny, np. dostępu tylko do połączeń wychodzących, który użytkownik może przyznać lub zablokować. Jeśli program wymaga później zarówno połączeń przychodzących, jak i wychodzących, można przyznać mu pełny dostęp w okienku Uprawnienia programów.

Ustawianie poziomu zabezpieczeń na Standardowy

Można ustawić poziom zabezpieczeń na Standardowy, aby zapora monitorowała połączenia przychodzące i wychodzące oraz wyświetlała alerty, gdy nowe programy próbują uzyskać dostęp do Internetu.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Poziom zabezpieczeń przesuń suwak tak, aby bieżącym poziomem był poziom **Standardowy**.
4. Kliknij przycisk **OK**.

Ustawianie poziomu zabezpieczeń na poziom Zaufanie

Można ustawić poziom zabezpieczeń programu Firewall na Zaufany, aby zezwalać albo na pełny dostęp do sieci, albo na dostęp do sieci tylko dla połączeń wychodzących.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Poziom zabezpieczeń przesuń suwak tak, aby bieżącym poziomem był poziom **Zaufanie**.
4. Wykonaj jedną z następujących czynności:
   - Aby zezwolić na pełny dostęp do sieci dla połączeń przychodzących i wychodzących, wybierz opcję **Zezwalaj na pełny dostęp**.
   - Aby zezwolić na dostęp do sieci tylko dla połączeń wychodzących, wybierz opcję **Zezwalaj na dostęp tylko dla wychodzących**.
5. Kliknij przycisk **OK**.

Uwaga: Domyślna opcja to **Zezwalaj na dostęp tylko dla wychodzących**.

Ustawienie poziomu zabezpieczeń na poziom Otwarty

Można ustawić poziom zabezpieczeń programu Firewall na Otwarty, aby zezwalać na wszystkie przychodzące i wychodzące połączenia sieciowe.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Poziom zabezpieczeń przesuń suwak tak, aby bieżącym poziomem był poziom **Otwarty**.
4. Kliknij przycisk **OK**.

Konfigurowanie inteligentnych zaleceń dla alertów

Program Firewall można skonfigurować tak, aby uwzględniał, wykluczał lub wyświetlał w alertach zalecenia dotyczące wszystkich programów próbujących uzyskać dostęp do Internetu. Włączenie inteligentnych zaleceń pomaga w podejmowaniu decyzji dotyczących reakcji na alerty.

Po włączeniu funkcji Inteligentne zalecenia (gdy poziom zabezpieczeń jest ustawiony na Zaufany z włączonym dostępem do Internetu tylko dla połączeń wychodzących) program Firewall automatycznie przepuszcza lub blokuje programy i informuje użytkownika o nierozpoznanych i potencjalnie niebezpiecznych programach.

Jeśli funkcja Inteligentne zalecenia jest wyłączona, program Firewall nie przepuszcza automatycznie programów i nie blokuje dostępu do Internetu oraz nie sugeruje żadnych działań w alertach.

Jeśli dla funkcji Inteligentne zalecenia jest wybrane ustawienie Tylko wyświetl, pojawia się monit o zezwolenie na dostęp lub zablokowanie go wraz z sugestiami dotyczącymi dalszych działań.

Włączanie funkcji Inteligentne zalecenia

Można włączyć funkcję Inteligentne zalecenia, aby program Firewall automatycznie zezwalał aplikacjom na dostęp do Internetu lub blokował go oraz wyświetlał alerty dotyczące nierozpoznanych lub potencjalnie niebezpiecznych aplikacji.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Poziom zabezpieczeń, w obszarze **Inteligentne zalecenia** wybierz opcję **Włącz inteligentne zalecenia**.
4. Kliknij przycisk **OK**.

Wyłączanie funkcji Inteligentne zalecenia

Można wyłączyć funkcję Inteligentne zalecenia, aby program Firewall zezwalał aplikacjom na dostęp do Internetu lub blokował go oraz wyświetlał alerty dotyczące nierozpoznanych lub potencjalnie niebezpiecznych aplikacji. Jednak w takim przypadku alerty nie zawierają żadnych sugestii dotyczących obsługi dostępu aplikacji do Internetu. Jeśli program Firewall wykryje nową aplikację, która jest podejrzana lub stanowi ewentualne zagrożenie, automatycznie zablokuje jej dostęp do Internetu.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Poziom zabezpieczeń, w obszarze **Inteligentne zalecenia** wybierz opcję **Wyłącz inteligentne zalecenia**.
4. Kliknij przycisk **OK**.

Wyświetlanie tylko inteligentnych zaleceń

Można włączyć wyświetlanie w alertach inteligentnych zaleceń, które podpowiadają tylko odpowiednie działania, ale to użytkownik decyduje o przepuszczeniu lub zablokowaniu nierozpoznanych lub potencjalnie niebezpiecznych aplikacji.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Poziom zabezpieczeń, w obszarze **Inteligentne zalecenia** wybierz opcję **Tylko wyświetl**.
4. Kliknij przycisk **OK**.

Optymalizacja zabezpieczeń programu Firewall

Istnieje wiele zagrożeń bezpieczeństwa komputera. Na przykład niektóre programy mogą próbować połączyć się z Internetem przed uruchomieniem systemu Windows®. Ponadto zaawansowani użytkownicy mogą sprawdzić, czy komputer użytkownika jest połączony z siecią, używając polecenia ping. Program Firewall zapewnia obronę przed obydwoma typami włamań, umożliwiając włączenie ochrony podczas rozruchu i zablokowanie żądań ping. Pierwsze ustawienie blokuje dostęp programów do Internetu podczas uruchamiania systemu Windows, a drugie blokuje żądania ping umożliwiające innym użytkownikom wykrycie obecności danego komputera w sieci.

Do standardowych ustawień instalacji należy automatyczne wykrywanie najbardziej typowych prób włamań, np. ataków typu DoS (odmowa usługi) czy prób z użyciem programów wykorzystujących luki w zabezpieczeniach. Korzystanie ze standardowych ustawień instalacji gwarantuje ochronę przed tymi atakami i próbami skanowania komputera, jednak ochronę tę można wyłączyć w okienku Wykrywanie włamań.

Ochrona komputera podczas uruchamiania

Można chronić komputer podczas uruchamiania systemu Windows i blokować nowe programy, które wcześniej nie wymagały dostępu do Internetu podczas uruchamiania, a teraz wymagają. Zapora wyświetla alerty dla programów, które zażądały dostępu do Internetu, przy czym dostęp ten można przyznać lub zablokować. Aby użyć tej opcji, poziom zabezpieczeń musi być ustawiony na Otwarty lub Blokada.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Poziom zabezpieczeń, w obszarze **Ustawienia zabezpieczeń** wybierz opcję **Włącz ochronę podczas uruchamiania**.
4. Kliknij przycisk **OK**.

Uwaga: Zablokowane połączenia i włamania nie są rejestrowane, gdy włączona jest ochrona podczas uruchamiania.

Konfigurowanie ustawień żądania ping

Można zezwolić innym użytkownikom na wykrywanie tego komputera w sieci lub uniemożliwić to.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Poziom zabezpieczeń, w obszarze **Ustawienia zabezpieczeń** wykonaj jedną z następujących czynności:
   - Wybierz opcję **Zezwalaj na żądania ICMP ping**, aby umożliwić wykrywanie komputera w sieci za pomocą żądań ping.
   - Usuń zaznaczenie opcji **Zezwalaj na żądania ICMP ping**, aby uniemożliwić wykrycie komputera w sieci za pomocą żądań ping.
4. Kliknij przycisk **OK**.

Konfiguracja wykrywania włamań

Można wykrywać próby włamań w celu ochrony komputera przed atakami i nieautoryzowanym skanowaniem. Standardowe ustawienia zapory uwzględniają automatyczne wykrywanie najczęściej spotykanych prób włamań, takich jak ataki typu DoS (odmowa usługi) czy próby z użyciem programów wykorzystujących luki w zabezpieczeniach. Można jednak wyłączyć automatyczne wykrywanie jednego lub większej liczby ataków bądź prób skanowania.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Zapora kliknij opcję **Wykrywanie włamań**.
4. W obszarze **Wykryj próby włamań** wykonaj jedną z następujących czynności:
   - Wybierz nazwę, aby automatycznie wykryć atak lub skanowanie.
   - Usuń nazwę, aby wyłączyć automatyczne wykrywanie ataku lub skanowania.
5. Kliknij przycisk **OK.**

Konfiguracja ustawień stanu ochrony przy użyciu zapory

Można tak skonfigurować zaporę, aby określone problemy były ignorowane i nie były zgłaszane do programu SecurityCenter.

1. W okienku McAfee SecurityCenter w obszarze **SecurityCenter — informacje** kliknij opcję **Konfiguruj**.
2. W okienku Konfiguracja programu SecurityCenter w obszarze **Stan ochrony** kliknij opcję **Zaawansowane**.
3. W okienku Zignorowane problemy wybierz jedną lub więcej następujących opcji:
   - **Ochrona przy użyciu zapory jest wyłączona.**
   - **W zaporze ustawiono poziom zabezpieczeń Otwarty.**
   - **Usługa zapory nie została uruchomiona.**
   - **Ochrona przy użyciu zapory nie jest zainstalowana na komputerze.**
   - **Zapora systemu Windows jest wyłączona.**
   - **Ochrona ruchu wychodzącego za pomocą zapory nie jest zainstalowana na komputerze.**
4. Kliknij przycisk **OK**.

Blokowanie i odblokowywanie zapory

Blokada natychmiast blokuje cały przychodzący i wychodzący ruch sieciowy, aby ułatwić odizolowanie komputera i rozwiązanie problemu.

Natychmiastowe zablokowanie zapory

Przy użyciu zapory można natychmiast zablokować cały ruch sieciowy między komputerem a Internetem.

1. W obszarze **Typowe zadania** okienka McAfee SecurityCenter kliknij opcję **Zablokuj zaporę**.
2. W okienku Blokada zapory kliknij opcję **Blokada**.
3. Kliknij przycisk **Tak**, aby potwierdzić ustawienie.

Wskazówka: Zaporę można też zablokować, klikając prawym przyciskiem myszy ikonę programu SecurityCenter znajdującą się w obszarze powiadomień w prawej części paska zadań, a następnie klikając polecenia **Szybkie łącza** i **Zablokuj zaporę**.

Natychmiastowe odblokowanie zapory

Przy użyciu zapory można natychmiast odblokować cały ruch sieciowy między komputerem a Internetem.

1. W obszarze **Typowe zadania** okienka McAfee SecurityCenter kliknij opcję **Zablokuj zaporę**.
2. W okienku Blokada włączona kliknij opcję **Odblokuj**.
3. Kliknij przycisk **Tak**, aby potwierdzić ustawienie.

Przywracanie ustawień zapory

Można szybko przywrócić pierwotne ustawienia ochrony przy pomocy zapory. Powoduje to przywrócenie poziomu zabezpieczeń Zaufany, przyznawanie dostępu tylko dla połączeń wychodzących, włączenie inteligentnych zaleceń, przywrócenie listy domyślnych programów i ich uprawnień w okienku Uprawnienia programów, wyczyszczenie listy zaufanych i zabronionych adresów IP oraz przywrócenie usług systemowych, ustawień dziennika zdarzeń i wykrywania włamań.

1. W okienku McAfee SecurityCenter kliknij opcję **Przywróć ustawienia domyślne zapory**.
2. W okienku Przywróć ustawienia domyślne ochrony przy użyciu zapory kliknij opcję **Przywróć ustawienia domyślne**.
3. Kliknij przycisk **Tak**, aby potwierdzić ustawienie.

Wskazówka: Ustawienia domyślne zapory można też przywrócić, klikając prawym przyciskiem myszy ikonę programu SecurityCenter znajdującą się w obszarze powiadomień w prawej części paska zadań, a następnie klikając polecenia **Szybkie łącza** i **Przywróć ustawienia domyślne zapory**.

ROZDZIAŁ 18

Zarządzanie programami i uprawnieniami

Zapora umożliwia zarządzanie i tworzenie uprawnień dostępu dla istniejących i nowych programów wymagających dostępu do Internetu dla ruchu przychodzącego i wychodzącego. Zapora umożliwia kontrolowanie pełnego dostępu dla programów lub dostępu tylko dla połączeń wychodzących. Można również zablokować dostęp programów do Internetu.

W tym rozdziale

Przyznawanie dostępu programów do Internetu

Niektóre programy, na przykład przeglądarki internetowe, do prawidłowego funkcjonowania wymagają dostępu do Internetu.

Zapora umożliwia użycie strony Uprawnienia programów w celu:

- Zezwalania na dostęp dla programów
- Zezwalania programom na dostęp tylko dla połączeń wychodzących
- Zablokowania programom dostępu

Na pełny dostęp i dostęp tylko dla połączeń wychodzących do Internetu można zezwolić z poziomu dziennika Zdarzenia wychodzące i dziennika Ostatnie zdarzenia.

Zezwalanie programowi na pełny dostęp

Można zezwolić istniejącemu na komputerze zablokowanemu programowi na pełny dostęp do przychodzących i wychodzących połączeń internetowych.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Zapora kliknij opcję **Uprawnienia programów**.
4. W obszarze **Uprawnienia programów** wybierz program z opcją **Zablokowane** lub **Prawa dostępu tylko dla wychodzących**.
5. W obszarze **Akcja** kliknij opcję **Zezwalaj na dostęp**.
6. Kliknij przycisk **OK**.

Zezwalanie nowemu programowi na pełny dostęp

Można zezwolić nowemu na komputerze zablokowanemu programowi na pełny dostęp do przychodzących i wychodzących połączeń internetowych.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Zapora kliknij opcję **Uprawnienia programów**.
4. W obszarze **Uprawnienia programów** kliknij opcję **Dodaj dozwolony program**.
5. W oknie dialogowym **Dodawanie programu** znajdź i wybierz program, który chcesz dodać, a następnie kliknij przycisk **Otwórz**.

Uwaga: Uprawnienia nowo dodanego programu można zmienić tak, jak w przypadku istniejącego programu, wybierając program, a następnie w obszarze **Akcja** klikając opcję **Zezwalaj na dostęp tylko dla wychodzących** lub **Blokuj dostęp**.

Zezwalanie na pełny dostęp z poziomu dziennika Ostatnie zdarzenia

Można zezwolić istniejącemu zablokowanemu programowi pojawiającemu się w dzienniku Ostatnie zdarzenia na pełny dostęp do przychodzących i wychodzących połączeń internetowych.

1. W okienku McAfee SecurityCenter kliknij opcję **Menu zaawansowane**.
2. Kliknij opcję **Raporty i dzienniki**.
3. W okienku **Ostatnie zdarzenia** wybierz opis zdarzenia, a następnie kliknij opcję **Zezwalaj na dostęp**.
4. W oknie dialogowym Uprawnienia programów kliknij przycisk **Tak**, aby potwierdzić.

Tematy pokrewne

- *Wyświetlanie zdarzeń wychodzących* (strona 123)

Zezwalanie na pełny dostęp z poziomu dziennika Zdarzenia wychodzące

Można zezwolić istniejącemu zablokowanemu programowi pojawiającemu się w dzienniku Zdarzenia wychodzące na pełny dostęp do przychodzących i wychodzących połączeń internetowych.

1. W okienku McAfee SecurityCenter kliknij opcję **Menu zaawansowane**.
2. Kliknij opcję **Raporty i dzienniki**.
3. W obszarze **Ostatnie zdarzenia** kliknij opcję **Wyświetl dziennik**.
4. Kliknij opcję **Internet i sieć**, a następnie opcję **Zdarzenia wychodzące**.
5. Wybierz program i w obszarze **Działanie** kliknij opcję **Zezwalaj na dostęp**.
6. W oknie dialogowym Uprawnienia programów kliknij przycisk **Tak**, aby potwierdzić.

Zezwalanie programom na dostęp tylko dla połączeń wychodzących

Niektóre programy na komputerze wymagają dostępu do Internetu dla połączeń wychodzących. Korzystając z zapory, można zezwalać programom na dostęp do Internetu tylko dla połączeń wychodzących.

Zezwalanie programowi na dostęp tylko dla połączeń wychodzących

Można tak skonfigurować zaporę, aby zezwolić programowi tylko na dostęp do Internetu dla połączeń wychodzących.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Zapora kliknij opcję **Uprawnienia programów**.
4. W obszarze **Uprawnienia programów** wybierz program z opcją **Zablokowane** lub **Pełny dostęp**.
5. W obszarze **Akcja** kliknij przycisk **Zezwalaj na dostęp tylko dla wychodzących**.
6. Kliknij przycisk **OK**.

Zezwalanie na dostęp tylko dla połączeń wychodzących z dziennika Ostatnie zdarzenia

Można zezwolić istniejącemu zablokowanemu programowi pojawiającemu się w dzienniku Ostatnie zdarzenia na pełny dostęp do Internetu tylko dla połączeń wychodzących.

1. W okienku McAfee SecurityCenter kliknij opcję **Menu zaawansowane**.
2. Kliknij opcję **Raporty i dzienniki**.
3. W okienku **Ostatnie zdarzenia** wybierz opis zdarzenia, a następnie kliknij opcję **Zezwalaj na dostęp tylko dla wychodzących**.
4. W oknie dialogowym Uprawnienia programów kliknij przycisk **Tak**, aby potwierdzić.

Zezwalanie na dostęp tylko dla połączeń wychodzących z poziomu dziennika Zdarzenia wychodzące

Można zezwolić istniejącemu zablokowanemu programowi pojawiającemu się w dzienniku Zdarzenia wychodzące na pełny dostęp do Internetu tylko dla połączeń wychodzących.

1. W okienku McAfee SecurityCenter kliknij opcję **Menu zaawansowane**.
2. Kliknij opcję **Raporty i dzienniki**.
3. W obszarze **Ostatnie zdarzenia** kliknij opcję **Wyświetl dziennik**.
4. Kliknij opcję **Internet i sieć**, a następnie opcję **Zdarzenia wychodzące**.
5. Wybierz program i w obszarze **Działanie** kliknij opcję **Zezwalaj na dostęp tylko dla wychodzących**.
6. W oknie dialogowym Uprawnienia programów kliknij przycisk **Tak**, aby potwierdzić.

Blokowanie dostępu programów do Internetu

Zapora umożliwia blokowanie dostępu programów do Internetu. Należy się upewnić, że zablokowanie programu nie przerwie połączenia z siecią lub działania innego programu, który do prawidłowego funkcjonowania wymaga dostępu do Internetu.

Blokowanie dostępu programu

Można zablokować programowi dostęp do Internetu dla połączeń przychodzących i wychodzących.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Zapora kliknij opcję **Uprawnienia programów**.
4. W obszarze **Uprawnienia programów** wybierz program z opcją **Prawa pełnego dostępu** lub **Prawa dostępu tylko dla wychodzących**.
5. W obszarze **Akcja** kliknij opcję **Zablokuj dostęp**.
6. Kliknij przycisk **OK**.

Blokowanie dostępu nowego programu

Można zablokować nowemu programowi dostęp do Internetu dla połączeń przychodzących i wychodzących.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Zapora kliknij opcję **Uprawnienia programów**.
4. Na karcie **Uprawnienia programów** kliknij opcję **Dodaj zablokowany program**.
5. W oknie dialogowym Dodawanie programu przejdź do programu, który ma zostać dodany, a następnie kliknij przycisk **Otwórz**.

Uwaga: Uprawnienia nowo dodanego programu można zmienić, wybierając program, a następnie w obszarze **Akcja** klikając opcję **Zezwalaj na dostęp tylko dla wychodzących** lub **Zezwalaj na dostęp**.

Blokowanie dostępu z poziomu dziennika Ostatnie zdarzenia

Można zablokować programowi pojawiającemu się w dzienniku Ostatnie zdarzenia dostęp do Internetu dla połączeń przychodzących i wychodzących.

1. W okienku McAfee SecurityCenter kliknij opcję **Menu zaawansowane**.
2. Kliknij opcję **Raporty i dzienniki**.
3. W okienku **Ostatnie zdarzenia** wybierz opis zdarzenia, a następnie kliknij opcję **Blokuj dostęp**.
4. W oknie dialogowym Uprawnienia programów kliknij przycisk **Tak**, aby potwierdzić.

Usuwanie praw dostępu programów

Przed usunięciem uprawnienia programu należy się upewnić, że jego brak nie wpłynie negatywnie na pracę komputera lub na połączenie sieciowe.

Usuwanie uprawnienia programu

Można usunąć program z listy uprawnionych do dostępu do Internetu dla połączeń przychodzących i wychodzących.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Zapora kliknij opcję **Uprawnienia programów**.
4. W obszarze **Uprawnienia programów** wybierz program.
5. W obszarze **Akcja** kliknij opcję **Usuń uprawnienia programu**.
6. Kliknij przycisk **OK**.

Uwaga: Zapora zapobiega modyfikowaniu ustawień niektórych programów przez ograniczenie lub wyłączenie określonych działań.

Informacje o programach

Jeśli nie ma pewności, jakie uprawnienie powinien mieć program, w witrynie internetowej HackerWatch firmy McAfee można znaleźć informacje na jego temat.

Informacje o programie

W witrynie internetowej HackerWatch firmy McAfee można uzyskać informacje o programie ułatwiające podjęcie decyzji, czy należy mu zezwolić na dostęp do Internetu dla połączeń przychodzących i wychodzących, czy raczej go zablokować.

Uwaga: Należy upewnić się, że połączenie z Internetem zostało nawiązane i za pomocą przeglądarki można pomyślnie otworzyć witrynę HackerWatch firmy McAfee. Zawiera ona bieżące informacje o programach, ich wymaganiach dotyczących dostępu do Internetu i zagrożeniach bezpieczeństwa.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Zapora kliknij opcję **Uprawnienia programów**.
4. W obszarze **Uprawnienia programów** wybierz program.
5. W obszarze **Akcja** kliknij opcję **Więcej informacji**.

Informacje o programie znajdujące się w dzienniku Zdarzenia wychodzące

Z poziomu dziennika Zdarzenia wychodzące można pobrać z witryny internetowej HackerWatch firmy McAfee informacje o programie ułatwiające podjęcie decyzji, czy należy mu zezwolić na dostęp do Internetu dla połączeń przychodzących i wychodzących, czy raczej go zablokować.

Uwaga: Należy upewnić się, że połączenie z Internetem zostało nawiązane i za pomocą przeglądarki można pomyślnie otworzyć witrynę HackerWatch firmy McAfee. Zawiera ona bieżące informacje o programach, ich wymaganiach dotyczących dostępu do Internetu i zagrożeniach bezpieczeństwa.

1. W okienku McAfee SecurityCenter kliknij opcję **Menu zaawansowane**.
2. Kliknij opcję **Raporty i dzienniki**.
3. W obszarze Ostatnie zdarzenia wybierz zdarzenie, a następnie kliknij opcję **Wyświetl dziennik**.
4. Kliknij opcję **Internet i sieć**, a następnie opcję **Zdarzenia wychodzące**.
5. Wybierz adres IP, a następnie kliknij przycisk **Dowiedz się więcej**.

ROZDZIAŁ 19

Zarządzanie usługami systemowymi

Niektóre programy (w tym serwery sieci Web i programy serwerów do udostępniania plików) do swojego prawidłowego działania wymagają odbierania połączeń z innych komputerów za pośrednictwem określonych portów usług systemowych. Zazwyczaj zapora zamyka te porty usług systemowych, ponieważ to głównie one są źródłem zagrożeń w systemie użytkownika. Aby akceptować połączenia ze zdalnych komputerów, porty usług systemowych muszą być jednak otwarte.

W tym rozdziale

Konfigurowanie portów usług systemowych

Porty usług systemowych mogą być tak skonfigurowane, aby umożliwiać lub blokować zdalny dostęp do usługi sieciowej na komputerze.

Na poniższej liście przedstawiono często spotykane usługi systemowe i powiązane z nimi porty:

- Porty protokołu FTP 20–21
- Serwer poczty (IMAP) — port 143
- Serwer poczty (POP3) — port 110
- Serwer poczty (SMTP) — port 25
- Serwer Microsoft Directory Server (MSFT DS) — port 445
- Serwer Microsoft SQL Server (MSFT SQL) — port 1433
- Port protokołu Network Time 123
- Pulpit zdalny / Pomoc zdalna / Serwer terminali (protokół RDP) — port 3389
- Zdalne wywołania procedur (RPC) — port 135
- Bezpieczny serwer sieci Web (HTTPS) — port 443
- Usługa Universal Plug and Play (UPNP) — port 5000
- Serwer sieci Web (HTTP) — port 80
- Udostępnianie plików systemu Windows (NETBIOS) — porty 137–139

Porty usług systemowych mogą też zostać tak skonfigurowane, aby umożliwić komputerowi udostępnianie połączenia z Internetem innym komputerom z nim połączonym. Ta usługa, znana jako udostępnianie połączenia internetowego (ICS), umożliwia komputerowi udostępniającemu połączenie pełnienie roli bramy do Internetu wobec innych komputerów w sieci.

Uwaga: Jeśli na komputerze jest uruchomiona aplikacja akceptująca połączenia z serwerem sieci Web lub FTP, może zajść potrzeba otwarcia powiązanego portu usługi systemowej na komputerze udostępniającym połączenie i zezwolenie na przesyłanie połączeń przychodzących do tego portu.

Zezwolenie na dostęp do istniejącego portu usług systemowych

Można otworzyć istniejący port, aby zezwolić na zdalny dostęp do usługi sieciowej uruchomionej na komputerze.

Uwaga: Otwarcie portu usług systemowych może spowodować, że komputer będzie podatny na zagrożenia z Internetu. Dlatego port należy otwierać tylko wtedy, gdy jest to konieczne.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Zapora kliknij opcję **Usługi systemowe**.
4. W obszarze **Otwórz port usług systemowych** wybierz usługę systemową, której port chcesz otworzyć.
5. Kliknij przycisk **OK**.

Blokowanie dostępu do istniejącego portu usługi systemowej

Można zamknąć istniejący port, aby zablokować zdalny dostęp do usługi sieciowej uruchomionej na komputerze.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Zapora kliknij opcję **Usługi systemowe**.
4. Na liście **Otwarty port usługi systemowej** usuń zaznaczenie przy wybranej usłudze systemowej, aby zamknąć jej port.
5. Kliknij przycisk **OK**.

Konfiguracja nowego portu usług systemowych

Można skonfigurować nowy port usług systemowych, który można otworzyć lub zamknąć, aby zezwolić na zdalny dostęp do komputera lub go zablokować.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Zapora kliknij opcję **Usługi systemowe**.
4. Kliknij przycisk **Dodaj**.
5. W obszarze **Porty i usługi systemowe** okienka Usługi systemowe wprowadź następujące informacje:
   - nazwa programu,
   - porty TCP/IP połączeń przychodzących,

- porty TCP/IP połączeń wychodzących,
- porty UDP połączeń przychodzących,
- porty UDP połączeń wychodzących.

6 Aby wysyłać informacje o aktywności tego portu innym komputerom w sieci z systemem Windows używającym tego połączenia z Internetem, zaznacz opcję **Przekieruj ruch sieciowy na tym porcie do użytkowników sieci, którzy używają usługi udostępniania połączenia internetowego**.

7 Można też wprowadzić opis nowej konfiguracji.

8 Kliknij przycisk **OK**.

Uwaga: Jeśli na komputerze jest uruchomiona aplikacja akceptująca połączenia z serwerem sieci Web lub FTP, może zajść potrzeba otwarcia powiązanego portu usługi systemowej na komputerze udostępniającym połączenie i zezwolenie na przesyłanie połączeń przychodzących do tego portu. W przypadku korzystania z usługi udostępniania internetowego (ICS, Internet Connection Sharing) należy też dodać połączenie z zaufanym komputerem do listy zaufanych adresów IP. Aby uzyskać więcej informacji, zobacz temat Dodawanie połączenia z zaufanym komputerem.

Modyfikacja portu usług systemowych

Można modyfikować informacje dotyczące dostępu dla połączeń przychodzących i wychodzących dla istniejącego portu usług systemowych.

Uwaga: Jeśli informacje dotyczące portu są wprowadzone niepoprawnie, usługa systemowa nie działa.

1 W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.

2 W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.

3 W okienku Zapora kliknij opcję **Usługi systemowe**.

4 Wybierz usługę systemową, a następnie kliknij przycisk **Edytuj**.

5 W obszarze **Porty i usługi systemowe** okienka Usługi systemowe wprowadź następujące informacje:

- nazwa programu,
- porty TCP/IP połączeń przychodzących,
- porty TCP/IP połączeń wychodzących,
- porty UDP połączeń przychodzących,
- porty UDP połączeń wychodzących.

6 Aby wysyłać informacje o aktywności tego portu innym komputerom w sieci z systemem Windows używającym tego połączenia z Internetem, zaznacz opcję **Przekieruj ruch sieciowy na tym**

porcie do użytkowników sieci, którzy używają usługi udostępniania połączenia internetowego.

7 Można też wprowadzić opis zmienionej konfiguracji.

8 Kliknij przycisk **OK**.

Usuwanie portu usług systemowych

Można usunąć z komputera istniejący port usług systemowych. Po usunięciu portu usługa sieciowa na komputerze nie będzie już dostępna zdalnie.

1 W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.

2 W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.

3 W okienku Zapora kliknij opcję **Usługi systemowe**.

4 Wybierz usługę systemową, a następnie kliknij przycisk **Usuń**.

5 Po wyświetleniu monitu kliknij przycisk **Tak**, aby potwierdzić.

ROZDZIAŁ 20

Zarządzanie połączeniami z komputerem

Zaporę można skonfigurować tak, aby można było zarządzać określonymi zdalnymi połączeniami z komputerem użytkownika. W takim przypadku należy stworzyć reguły oparte na adresach protokołu internetowego (IP) przypisanych do zdalnych komputerów. Komputerom przypisanym do zaufanych adresów IP można ufać i mogą one łączyć się z komputerem użytkownika. Komputerom o nieznanych, podejrzanych lub wzbudzających nieufność adresach można blokować możliwość łączenia się z komputerem użytkownika.

Przy zezwalaniu na połączenie należy się upewnić, że zaufany komputer jest bezpieczny. Jeśli zaufany komputer jest zainfekowany robakiem lub innym mechanizmem, komputer użytkownika może również być zagrożony. Ponadto firma McAfee zaleca, aby zaufane komputery były również chronione za pomocą zapory i aktualnego programu antywirusowego. Zapora nie rejestruje ruchu ani nie generuje alertów o zdarzeniach z adresów IP znajdujących się na liście zaufanych adresów IP.

Komputerom, którym są przypisane nieznane, podejrzane lub wzbudzające nieufność adresy IP, można zabronić łączenia się z komputerem użytkownika.

Ponieważ program Firewall blokuje cały niepożądany ruch, zwykle nie jest konieczne blokowanie adresu IP. Blokowanie adresu IP ma sens tylko w przypadku, gdy użytkownik jest pewien, że połączenie internetowe stanowi określone zagrożenie. Należy upewnić się, że nie są blokowane ważne adresy IP, takie jak adresy serwerów DNS czy DHCP lub innych serwerów usługodawcy internetowego. Zależnie od ustawień zabezpieczeń program Firewall może generować alert o wykryciu zdarzenia wywołanego przez zablokowany komputer.

W tym rozdziale

Udzielanie zaufania połączeniom z komputerami

Zaufane adresy IP można dodawać, edytować i usuwać w okienku Zaufane i zabronione adresy IP w obszarze **Zaufane adresy IP**.

Lista **Zaufane adresy IP** w okienku Zaufane i zabronione adresy IP pozwala na odbieranie całego ruchu z określonego komputera przez komputer użytkownika. Program Firewall nie rejestruje ruchu ani nie generuje alertów o zdarzeniach z adresów IP znajdujących się na liście **Zaufane adresy IP**.

Zapora udziela zaufania wszystkim sprawdzonym adresom IP na liście i zawsze zezwala na ruch sieciowy z zaufanego adresu IP na każdym porcie. Działania, w których uczestniczy komputer przypisany do zaufanego adresu IP i komputer użytkownika, nie są filtrowane ani analizowane przez zaporę. Domyślnie na liście Zaufane adresy IP umieszczana jest pierwsza sieć prywatna odnaleziona przez zaporę.

Przy zezwalaniu na połączenie należy się upewnić, że zaufany komputer jest bezpieczny. Jeśli zaufany komputer jest zainfekowany robakiem lub innym mechanizmem, komputer użytkownika może również być zagrożony. Ponadto firma McAfee zaleca, aby zaufane komputery były również chronione za pomocą zapory i aktualnego programu antywirusowego.

Dodawanie połączenia z zaufanym komputerem

Można dodać połączenie z zaufanym komputerem i przypisany do niego adres IP.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Zapora kliknij opcję **Zaufane i zabronione adresy IP**.
4. W okienku Zaufane i zabronione adresy IP wybierz opcję **Zaufane adresy IP**, a następnie kliknij przycisk **Dodaj**.
5. W obszarze **Dodaj regułę zaufanego adresu IP** wykonaj jedną z następujących czynności:
   - Wybierz opcję **Pojedynczy adres IP**, a następnie wprowadź adres IP.
   - Wybierz opcję **Zakres adresów IP**, a następnie wprowadź początkowe i końcowe adresy IP w polach **Z adresu IP** i **Na adres IP**.

6 Jeśli usługa systemowa korzysta z udostępniania połączenia internetowego, można dodać następujący zakres adresów IP: od 192.168.0.1 do 192.168.0.255.

7 Można też wybrać opcję **Reguła wygasa za** i wprowadzić liczbę dni, w czasie których reguła będzie obowiązywać.

8 Dodatkowo można wprowadzić opis reguły.

9 Kliknij przycisk **OK**.

10 W oknie dialogowym **Zaufane i zabronione adresy IP** kliknij przycisk **Tak**, aby potwierdzić.

Uwaga: Aby uzyskać więcej informacji na temat udostępniania połączenia internetowego, patrz temat Konfiguracja nowej usługi systemowej.

Dodawanie zaufanego komputera z poziomu dziennika Zdarzenia przychodzące

Połączenie z zaufanym komputerem i związany z nim adres IP można dodać z poziomu dziennika Zdarzenia przychodzące.

1 W obszarze Typowe zadania okna McAfee SecurityCenter kliknij opcję **Menu zaawansowane**.

2 Kliknij opcję **Raporty i dzienniki**.

3 W obszarze **Ostatnie zdarzenia** kliknij opcję **Wyświetl dziennik**.

4 Kliknij opcję **Internet i sieć**, a następnie opcję **Zdarzenia przychodzące**.

5 Wybierz źródłowy adres IP i w obszarze **Działanie** kliknij opcję **Zaufaj temu adresowi**.

6 Kliknij przycisk **Tak**, aby potwierdzić ustawienie.

Edycja połączenia z zaufanym komputerem

Można edytować połączenie z zaufanym komputerem i przypisany do niego adres IP.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Zapora kliknij opcję **Zaufane i zabronione adresy IP**.
4. W okienku Zaufane i zabronione adresy IP wybierz opcję **Zaufane adresy IP**.
5. Wybierz adres IP, a następnie kliknij przycisk **Edytuj**.
6. W obszarze **Edytuj zaufany adres IP** wykonaj jedną z następujących czynności:
   - Wybierz opcję **Pojedynczy adres IP**, a następnie wprowadź adres IP.
   - Wybierz opcję **Zakres adresów IP**, a następnie wprowadź początkowe i końcowe adresy IP w polach **Z adresu IP** i **Na adres IP**.
7. Można też zaznaczyć opcję **Reguła wygasa za** i wpisać liczbę dni, w czasie których reguła będzie obowiązywać.
8. Dodatkowo można wprowadzić opis reguły.
9. Kliknij przycisk **OK**.

Uwaga: Nie można edytować domyślnych połączeń komputera dodanych automatycznie przez zaporę z zaufanej sieci prywatnej.

Usuwanie połączenia z zaufanym komputerem

Można usunąć połączenie z zaufanym komputerem i przypisany do niego adres IP.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Zapora kliknij opcję **Zaufane i zabronione adresy IP**.
4. W okienku Zaufane i zabronione adresy IP wybierz opcję **Zaufane adresy IP**.
5. Zaznacz adres IP, a następnie kliknij przycisk **Usuń**.
6. W oknie dialogowym **Zaufane i zabronione adresy IP** kliknij przycisk **Tak**, aby potwierdzić.

Blokowanie połączeń z komputerami

Zabronione adresy IP można dodawać, edytować i usuwać w okienku Zaufane i zabronione adresy IP w obszarze **Zabronione adresy IP**.

Komputerom, którym są przypisane nieznane, podejrzane lub wzbudzające nieufność adresy IP, można zabronić łączenia się z komputerem użytkownika.

Ponieważ program Firewall blokuje cały niepożądany ruch, zwykle nie jest konieczne blokowanie adresu IP. Blokowanie adresu IP ma sens tylko w przypadku, gdy użytkownik jest pewien, że połączenie internetowe stanowi określone zagrożenie. Należy upewnić się, że nie są blokowane ważne adresy IP, takie jak adresy serwerów DNS czy DHCP lub innych serwerów usługodawcy internetowego. Zależnie od ustawień zabezpieczeń program Firewall może generować alert o wykryciu zdarzenia wywołanego przez zablokowany komputer.

Dodawanie połączenia z zabronionym komputerem

Można dodać połączenie z zabronionym komputerem i przypisany do niego adres IP.

Uwaga: Należy upewnić się, że nie są blokowane ważne adresy IP, takie jak adresy serwerów DNS czy DHCP lub innych serwerów usługodawcy internetowego.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Zapora kliknij opcję **Zaufane i zabronione adresy IP**.
4. W okienku Zaufane i zabronione adresy IP wybierz opcję **Zabronione adresy IP**, a następnie kliknij przycisk **Dodaj**.
5. W obszarze **Dodaj regułę zabronionego adresu IP** wykonaj jedną z następujących czynności:
   - Wybierz opcję **Pojedynczy adres IP**, a następnie wprowadź adres IP.
   - Wybierz opcję **Zakres adresów IP**, a następnie wprowadź początkowe i końcowe adresy IP w polach **Z adresu IP** i **Na adres IP**.

6 Można też wybrać opcję **Reguła wygasa za** i wprowadzić liczbę dni, w czasie których reguła będzie obowiązywać.

7 Dodatkowo można wprowadzić opis reguły.

8 Kliknij przycisk **OK**.

9 W oknie dialogowym **Zaufane i zabronione adresy IP** kliknij przycisk **Tak**, aby potwierdzić.

Edycja połączenia z zabronionym komputerem

Można edytować połączenie z zabronionym komputerem i przypisany do niego adres IP.

1 W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.

2 W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.

3 W okienku Zapora kliknij opcję **Zaufane i zabronione adresy IP**.

4 W okienku Zaufane i zabronione adresy IP wybierz opcję **Zabronione adresy IP**, a następnie kliknij przycisk **Edytuj**.

5 W obszarze **Edytuj zabroniony adres IP** wykonaj jedną z następujących czynności:

- Wybierz opcję **Pojedynczy adres IP**, a następnie wprowadź adres IP.
- Wybierz opcję **Zakres adresów IP**, a następnie wprowadź początkowe i końcowe adresy IP w polach **Z adresu IP** i **Na adres IP**.

6 Można też wybrać opcję **Reguła wygasa za** i wprowadzić liczbę dni, w czasie których reguła będzie obowiązywać.

7 Dodatkowo można wprowadzić opis reguły.

8 Kliknij przycisk **OK**.

Usuwanie połączenia z zabronionym komputerem

Można usunąć połączenie z zabronionym komputerem i przypisany do niego adres IP.

1. W okienku McAfee SecurityCenter kliknij kategorię **Internet i sieć**, a następnie opcję **Konfiguruj**.
2. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
3. W okienku Zapora kliknij opcję **Zaufane i zabronione adresy IP**.
4. W okienku Zaufane i zabronione adresy IP wybierz opcję **Zabronione adresy IP**.
5. Zaznacz adres IP, a następnie kliknij przycisk **Usuń**.
6. W oknie dialogowym **Zaufane i zabronione adresy IP** kliknij przycisk **Tak**, aby potwierdzić.

Blokowanie dostępu komputerowi z poziomu dziennika Zdarzenia przychodzące

Połączenia z komputerem i związanym z nim adresem IP można zabronić z poziomu dziennika Zdarzenia przychodzące.

Adresy IP, które są wyświetlane w dzienniku Zdarzenia przychodzące, są zablokowane. Zabranianie dostępu adresowi nie zapewnia zatem żadnej dodatkowej ochrony, chyba że komputer użytkownika używa portów, które są celowo otwarte lub znajduje się na nim program, któremu zezwolono na dostęp do Internetu.

Dodanie adresu IP do listy **Zabronione adresy IP** 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.

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.

1. W obszarze **Typowe zadania** okna McAfee SecurityCenter kliknij opcję **Menu zaawansowane**.
2. Kliknij opcję **Raporty i dzienniki**.
3. W obszarze **Ostatnie zdarzenia** kliknij opcję **Wyświetl dziennik**.
4. Kliknij opcję **Internet i sieć**, a następnie opcję **Zdarzenia przychodzące**.
5. Wybierz źródłowy adres IP i w obszarze **Działanie** kliknij opcję **Zabroń dostępu temu adresowi**.
6. W oknie dialogowym **Dodaj regułę zabronionego adresu IP** kliknij przycisk **Tak**, aby potwierdzić.

Blokowanie dostępu komputerowi z poziomu dziennika Zdarzenia wykrywania włamań

Połączenia z komputerem i związanym z nim adresem IP można zabronić z poziomu dziennika Zdarzenia wykrywania włamań.

1. W obszarze **Typowe zadania** okna McAfee SecurityCenter kliknij opcję **Menu zaawansowane**.
2. Kliknij opcję **Raporty i dzienniki**.
3. W obszarze **Ostatnie zdarzenia** kliknij opcję **Wyświetl dziennik**.
4. Kliknij opcję **Internet i sieć**, a następnie kliknij opcję **Zdarzenia wykrywania włamań**.
5. Wybierz źródłowy adres IP i w obszarze **Działanie** kliknij opcję **Zabroń dostępu temu adresowi**.
6. W oknie dialogowym **Dodaj regułę zabronionego adresu IP** kliknij przycisk **Tak**, aby potwierdzić.

ROZDZIAŁ 21

Rejestrowanie, monitorowanie i analiza

Korzystając z zapory, można obszernie i w sposób czytelny rejestrować, a także monitorować i analizować zdarzenia i ruch internetowy. Zrozumienie ruchu i zdarzeń internetowych pomaga zarządzać połączeniami z Internetem.

W tym rozdziale

Rejestrowanie zdarzeń

Zapora umożliwia włączenie lub wyłączenie rejestrowania zdarzeń. Jeśli jest ono włączone, można określić, które typy zdarzeń mają być rejestrowane. Rejestrowanie zdarzeń pozwala na przeglądanie ostatnich zdarzeń przychodzących, wychodzących i związanych z próbami włamań.

Konfiguracja ustawień dziennika zdarzeń

Można określić i skonfigurować typy zdarzeń zapory, które mają być rejestrowane. Domyślnie rejestrowanie jest włączone dla wszystkich zdarzeń i działań.

1. W okienku Konfiguracja kategorii Internet i sieć w obszarze **Zapora jest włączona** kliknij opcję **Zaawansowane**.
2. W okienku Zapora kliknij opcję **Ustawienia dziennika zdarzeń**.
3. Jeśli nie jest jeszcze zaznaczona, zaznacz opcję **Włącz rejestrowanie zdarzeń**.
4. W obszarze **Włącz rejestrowanie zdarzeń** zaznacz lub usuń zaznaczenie dla typów zdarzeń które mają lub nie mają być rejestrowane. Rodzaje zdarzeń obejmują:
   - zablokowane programy,
   - żądania ICMP ping,
   - ruch z zabronionych adresów IP,
   - zdarzenia na portach usług systemowych,
   - zdarzenia na nieznanych portach,
   - przypadki wykrywania włamań (IDS).
5. Aby zapobiec rejestrowaniu na określonych portach, wybierz polecenie **Nie rejestruj zdarzeń na następujących portach**, a następnie wpisz numery poszczególnych portów oddzielone przecinkami lub zakresy portów oddzielone myślnikami. Na przykład: `137-139, 445, 400-5000`.
6. Kliknij przycisk **OK**.

Wyświetlanie ostatnich zdarzeń

Jeśli włączono rejestrowanie, można wyświetlić ostatnie zdarzenia. W okienku Ostatnie zdarzenia jest wyświetlana data i opis zdarzenia. Wyświetlane są tylko działania programów, których dostęp do Internetu został wyraźnie zablokowany.

- W **Menu zaawansowanym**, w okienku Typowe zadania kliknij opcję **Raporty i dzienniki** lub opcję **Przeglądaj ostatnie zdarzenia**. W tym celu można też kliknąć opcję **Przeglądaj ostatnie zdarzenia** w okienku Typowe zadania menu podstawowego.

Wyświetlanie zdarzeń przychodzących

Jeśli włączone jest rejestrowanie, można wyświetlić zdarzenia przychodzące. Dane zdarzeń przychodzących zawierają datę i godzinę zdarzenia, źródłowy adres IP, nazwę hosta oraz informację o typie zdarzenia.

1. Upewnij się, że włączone jest Menu zaawansowane. W okienku Typowe zadania kliknij opcję **Raporty i dzienniki**.
2. W obszarze **Ostatnie zdarzenia** kliknij opcję **Wyświetl dziennik**.
3. Kliknij opcję **Internet i sieć**, a następnie opcję **Zdarzenia przychodzące**.

Uwaga: Adres IP z dziennika zdarzeń przychodzących można uznać za zaufany, zablokować go lub śledzić.

Wyświetlanie zdarzeń wychodzących

Jeśli jest włączone rejestrowanie, można wyświetlić zdarzenia wychodzące. Dane zdarzeń wychodzących obejmują nazwę programu próbującego uzyskać dostęp na zewnątrz, datę i godzinę zdarzenia oraz lokalizację programu na komputerze.

1. W okienku Typowe zadania kliknij opcję **Raporty i dzienniki**.
2. W obszarze **Ostatnie zdarzenia** kliknij opcję **Wyświetl dziennik**.
3. Kliknij opcję **Internet i sieć**, a następnie opcję **Zdarzenia wychodzące**.

Uwaga: Programowi z dziennika Zdarzenia wychodzące można zezwolić na pełny dostęp lub dostęp tylko dla połączeń wychodzących. W dzienniku można również znaleźć dodatkowe informacje o programie.

Wyświetlanie zdarzeń wykrywania włamań

Jeśli włączone jest rejestrowanie, można wyświetlić zdarzenia przychodzące dotyczące prób włamań. Dane zdarzenia wykrywania włamań zawierają datę i godzinę zdarzenia, źródłowy adres IP, nazwę hosta oraz informacje o typie zdarzenia.

1. W okienku Typowe zadania kliknij opcję **Raporty i dzienniki**.
2. W obszarze **Ostatnie zdarzenia** kliknij opcję **Wyświetl dziennik**.
3. Kliknij opcję **Internet i sieć**, a następnie kliknij opcję **Zdarzenia wykrywania włamań**.

Uwaga: Adres IP z dziennika Zdarzenia wykrywania włamań można zablokować i śledzić.

Praca ze statystykami

Wykorzystanie poświęconej bezpieczeństwu witryny sieci Web firmy McAfee HackerWatch pozwala zaporze dostarczać użytkownikowi statystyk o globalnych zdarzeniach związanych z bezpieczeństwem Internetu i aktywnością portów.

Wyświetlanie światowych statystyk dotyczących zagrożeń bezpieczeństwa

Program HackerWatch monitoruje zagrożenia internetowe z całego świata. Dotyczące ich informacje można przeglądać w programie SecurityCenter. Informacje dotyczą przypadków przekazanych do programu HackerWatch w ciągu ostatnich 24 godzin, 7 dni i 30 dni.

1. Upewnij się, że włączone jest Menu zaawansowane, a następnie kliknij opcję **Narzędzia**.
2. W okienku Narzędzia kliknij opcję **HackerWatch**.
3. Wyświetl światowe statystyki dotyczące zagrożeń bezpieczeństwa w obszarze Monitorowanie zdarzeń.

Wyświetlanie aktywności dotyczącej portów internetowych na świecie

Program HackerWatch monitoruje zagrożenia internetowe z całego świata. Dotyczące ich informacje można przeglądać w programie SecurityCenter. Wyświetlone informacje opisują porty związane z najistotniejszymi zdarzeniami przekazanymi do programu HackerWatch w ciągu ostatnich siedmiu dni. Zazwyczaj wyświetlane są informacje o portach HTTP, TCP i UDP.

1. Upewnij się, że włączone jest Menu zaawansowane, a następnie kliknij opcję **Narzędzia**.
2. W okienku Narzędzia kliknij opcję **HackerWatch**.
3. W obszarze **Niedawna aktywność portów** wyświetl najistotniejsze zdarzenia dotyczące portów.

Śledzenie ruchu internetowego

Zapora udostępnia kilka opcji śledzenia ruchu internetowego. Umożliwiają one lokalizację komputera sieciowego, uzyskanie informacji o domenie i sieci oraz odszukanie komputerów z dzienników zdarzeń przychodzących i zdarzeń wykrywania włamań.

Lokalizowanie komputera w sieci

Programu Visual Tracer można użyć do zlokalizowania komputera, który łączy się lub próbuje połączyć się z komputerem użytkownika, przy wykorzystaniu jego nazwy i adresu IP. Przy pomocy programu Visual Tracer można również uzyskać dostęp do informacji o sieci i rejestracji. Program Visual Tracer umożliwia wyświetlenie mapy świata pokazującej najbardziej prawdopodobną drogę, którą pokonały dane z komputera źródłowego do komputera użytkownika.

1. Upewnij się, że włączone jest Menu zaawansowane, a następnie kliknij opcję **Narzędzia**.
2. W okienku Narzędzia kliknij opcję **Wątek śledzenia wizualnego**.
3. Wprowadź adres IP komputera i kliknij opcję **Zlokalizuj**.
4. W obszarze **Wątek śledzenia wizualnego** wybierz polecenie **Widok mapy**.

Uwaga: Nie można śledzić zdarzeń związanych z pętlowymi, prywatnymi lub nieprawidłowymi adresami IP.

Uzyskiwanie informacji o rejestracji komputera

Informacje o rejestracji komputera można uzyskać, korzystając z modułu Visual Trace w programie SecurityCenter. Informacje zawierają nazwę domeny, nazwę i adres rejestrującego oraz kontakt administracyjny.

1. Upewnij się, że włączone jest Menu zaawansowane, a następnie kliknij opcję **Narzędzia**.
2. W okienku Narzędzia kliknij opcję **Wątek śledzenia wizualnego**.
3. Wprowadź adres IP komputera, a następnie kliknij opcję **Zlokalizuj**.
4. W obszarze **Wątek śledzenia wizualnego** wybierz polecenie **Widok rejestracji**.

Informacje o sieci komputera

Informacje o sieci komputera można uzyskać, korzystając z modułu Visual Trace w programie SecurityCenter. Informacje o sieci zawierają szczegóły dotyczące sieci, w której znajduje się domena.

1. Upewnij się, że włączone jest Menu zaawansowane, a następnie kliknij opcję **Narzędzia**.
2. W okienku Narzędzia kliknij opcję **Wątek śledzenia wizualnego**.
3. Wprowadź adres IP komputera, a następnie kliknij opcję **Zlokalizuj**.
4. W obszarze **Wątek śledzenia wizualnego** wybierz polecenie **Widok sieci**.

Śledzenie komputera z poziomu dziennika Zdarzenia przychodzące

Z okienka Zdarzenia przychodzące można śledzić adres IP, który jest wyświetlony w dzienniku Zdarzenia przychodzące.

1. Upewnij się, że włączone jest Menu zaawansowane. W okienku Typowe zadania kliknij opcję **Raporty i dzienniki**.
2. W obszarze **Ostatnie zdarzenia** kliknij opcję **Wyświetl dziennik**.
3. Kliknij opcję **Internet i sieć**, a następnie opcję **Zdarzenia przychodzące**.
4. W okienku Zdarzenia przychodzące wybierz źródłowy adres IP, a następnie kliknij opcję **Śledź ten adres**.
5. W okienku Wątek śledzenia wizualnego kliknij jedną z następujących opcji:
   - **Widok mapy**: Geograficzna lokalizacja komputera przy użyciu wybranego adresu IP.
   - **Widok rejestracji**: Wyszukiwanie informacji o domenie przy użyciu wybranego adresu IP.
   - **Widok sieci**: Wyszukiwanie informacji o sieci przy użyciu wybranego adresu IP.
6. Kliknij przycisk **Gotowe**.

Śledzenie komputera z poziomu dziennika Zdarzenia wykrywania włamań

Z poziomu okienka Zdarzenia wykrywania włamań można śledzić adres IP, który jest wyświetlony w dzienniku Zdarzenia wykrywania włamań.

1. W okienku Typowe zadania kliknij opcję **Raporty i dzienniki**.
2. W obszarze **Ostatnie zdarzenia** kliknij opcję **Wyświetl dziennik**.
3. Kliknij opcję **Internet i sieć**, a następnie kliknij opcję **Zdarzenia wykrywania włamań**. W okienku Zdarzenia wykrywania włamań wybierz źródłowy adres IP, a następnie kliknij opcję **Śledź ten adres**.
4. W okienku Wątek śledzenia wizualnego kliknij jedną z następujących opcji:
   - **Widok mapy**: Geograficzna lokalizacja komputera przy użyciu wybranego adresu IP.
   - **Widok rejestracji**: Wyszukiwanie informacji o domenie przy użyciu wybranego adresu IP.
   - **Widok sieci**: Wyszukiwanie informacji o sieci przy użyciu wybranego adresu IP.
5. Kliknij przycisk **Gotowe**.

Śledzenie monitorowanego adresu IP

Monitorowany adres IP można śledzić w celu utworzenia widoku geograficznego pokazującego najbardziej prawdopodobną trasę danych otrzymanych z komputera źródłowego przez komputer użytkownika. Ponadto można uzyskać informacje rejestracyjne i sieciowe dotyczące danego adresu IP.

1. Upewnij się, że jest włączone menu zaawansowane, a następnie kliknij opcję **Narzędzia**.
2. W okienku Narzędzia kliknij opcję **Monitor ruchu**.
3. W obszarze **Monitor ruchu** kliknij opcję **Aktywne programy**.
4. Wybierz program, a następnie adres IP wyświetlany pod nazwą programu.
5. W obszarze **Działania programu** kliknij opcję **Śledź ten adres IP**.
6. W obszarze **Wątek śledzenia wizualnego** można wyświetlić mapę pokazującą najbardziej prawdopodobną trasę, jaką dane są przesyłane z komputera źródłowego do tego komputera. Ponadto można uzyskać informacje rejestracyjne i sieciowe dotyczące danego adresu IP.

Uwaga: Aby wyświetlić najnowsze dane statystyczne, kliknij przycisk **Odśwież** w obszarze **Wątek śledzenia wizualnego**.

Monitorowanie ruchu internetowego

Zapora umożliwia kilka sposobów monitorowania ruchu internetowego, między innymi:

- **Wykres Analiza ruchu**: Pokazuje ostatni przychodzący i wychodzący ruch internetowy.
- **Wykres Wykorzystanie ruchu**: Pokazuje wartość procentową wykorzystania przepustowości przez najbardziej aktywne programy w ciągu ostatnich 24 godzin.
- **Aktywne programy**: Pokazuje programy, które obecnie wykorzystują najwięcej połączeń sieciowych komputera oraz adresy IP, z którymi te programy się łączą.

Informacje o wykresie Analiza ruchu

Wykres Analiza ruchu jest liczbową i graficzną reprezentacją przychodzącego i wychodzącego ruchu internetowego. Ponadto Monitor ruchu wyświetla programy, które wykorzystują największą liczbę połączeń sieciowych komputera oraz adresy IP, z którymi te programy się łączą.

W okienku Analiza ruchu można obejrzeć najnowsze dane na temat przychodzącego i wychodzącego ruchu internetowego, bieżącą, średnią i maksymalną prędkość przesyłania danych. Można także sprawdzić dane dotyczące ilości przesyłanych danych, w tym ilość danych przesłanych od uruchomienia zapory i całkowitą ilość danych przesłanych w bieżącym miesiącu i w miesiącach poprzednich.

W okienku Analiza ruchu są wyświetlane na bieżąco dane o aktywności internetowej na komputerze użytkownika, w tym ilość danych przychodzącego i wychodzącego ruchu internetowego w ostatnim czasie, prędkość połączenia i całkowita ilość danych przesłanych przez Internet.

Ciągła zielona linia oznacza bieżącą szybkość transferu dla ruchu przychodzącego. Przerywana zielona linia oznacza średnią szybkość transferu dla ruchu przychodzącego. Jeśli bieżąca szybkość transferu i średnia szybkość transferu są takie same, linia przerywana na wykresie nie jest wyświetlana. Linia ciągła reprezentuje wtedy zarówno średnią, jak i bieżącą szybkość transferu.

Ciągła czerwona linia reprezentuje bieżącą szybkość transferu dla ruchu wychodzącego. Przerywana czerwona linia reprezentuje średnią szybkość transferu dla ruchu wychodzącego. Jeśli bieżąca szybkość transferu i średnia szybkość transferu są takie same, linia przerywana na wykresie nie jest wyświetlana. Linia ciągła reprezentuje wtedy zarówno średnią, jak i bieżącą szybkość transferu.

Analiza ruchu przychodzącego i wychodzącego

Wykres Analiza ruchu jest liczbową i graficzną reprezentacją przychodzącego i wychodzącego ruchu internetowego. Ponadto Monitor ruchu wyświetla programy, które wykorzystują największą liczbę połączeń sieciowych komputera oraz adresy IP, z którymi te programy się łączą.

1. Upewnij się, że włączone jest Menu zaawansowane, a następnie kliknij opcję **Narzędzia**.
2. W okienku Narzędzia kliknij opcję **Monitor ruchu**.
3. W obszarze **Monitor ruchu** kliknij opcję **Analiza ruchu**.

Wskazówka: Aby wyświetlić najnowsze dane statystyczne, kliknij przycisk **Odśwież** w obszarze **Analiza ruchu**.

Monitorowanie przepustowości wykorzystywanej przez programy

Można wyświetlić wykres kołowy, który zawiera przybliżone wartości procentowe przepustowości wykorzystywanej przez najaktywniejsze programy na komputerze w okresie ostatnich dwudziestu czterech godzin. Wykres kołowy stanowi wizualną reprezentację względnych wartości wykorzystania przepustowości pasma przez programy.

1. Upewnij się, że włączone jest Menu zaawansowane, a następnie kliknij opcję **Narzędzia**.
2. W okienku Narzędzia kliknij opcję **Monitor ruchu**.
3. W obszarze **Monitor ruchu** kliknij opcję **Analiza ruchu**.

Wskazówka: Aby wyświetlić najnowsze dane statystyczne, kliknij opcję **Odśwież** w obszarze **Wykorzystanie ruchu**.

Monitorowanie aktywności programów

Można wyświetlić dane dotyczące aktywności programu (ruch przychodzący i wychodzący) obejmujące połączenia ze zdalnych komputerów i porty.

1. Upewnij się, że włączone jest Menu zaawansowane, a następnie kliknij opcję **Narzędzia**.
2. W okienku Narzędzia kliknij opcję **Monitor ruchu**.
3. W obszarze **Monitor ruchu** kliknij opcję **Aktywne programy**.
4. Można wyświetlić następujące informacje:
   - Wykres Aktywność programu: Wybierz program, dla którego ma zostać wyświetlony wykres aktywności.
   - Połączenie nasłuchujące: Wybierz opcję Nasłuchiwanie znajdującą się pod nazwą programu.

- Połączenie komputera: Wybierz adres IP pod nazwą programu, procesem systemowym lub usługą.

Uwaga: Aby wyświetlić najnowsze dane statystyczne, kliknij opcję **Odśwież** w obszarze **Aktywne programy**.

ROZDZIAŁ 22

Informacje o bezpieczeństwie internetowym

Wykorzystanie poświęconej bezpieczeństwu witryny sieci Web firmy McAfee HackerWatch pozwala zaporze dostarczać aktualnych informacji o programach i aktywności w Internecie. W witrynie HackerWatch dostępny jest także podręcznik zapory w formacie HTML.

W tym rozdziale

Uruchamianie samouczka witryny HackerWatch

Więcej informacji na temat zapory znajduje się w samouczku witryny HackerWatch w programie SecurityCenter.

1. Upewnij się, że włączone jest Menu zaawansowane, a następnie kliknij opcję **Narzędzia**.
2. W okienku Narzędzia kliknij opcję **HackerWatch**.
3. W obszarze **Zasoby witryny HackerWatch** kliknij przycisk **Wyświetl samouczek**.

ROZDZIAŁ 23

McAfee Anti-Spam

Program Anti-Spam (dawniej SpamKiller) zatrzymuje niechciane wiadomości e-mail przed wtargnięciem do skrzynki odbiorczej przez sprawdzenie przychodzącej poczty e-mail, a potem oznaczenie jej jako spam (wiadomości e-mail nakłaniające do zakupów) lub phishing (wiadomości e-mail nakłaniające do podania informacji osobistych potencjalnie fałszywej witrynie sieci Web). Następnie wiadomości e-mail — SPAM są filtrowane i przenoszone do folderu programu McAfee Anti-Spam.

Jeśli znajomi czasami przesyłają poprawne wiadomości e-mail, mogące wyglądać jak spam, ich odfiltrowaniu zapobiegnie dodanie adresów e-mail znajomych do listy PRZYJACIELE w programie Anti-Spam. Kolejna możliwość to dostosowanie sposobu wykrywania spamu. Można na przykład filtrować wiadomości bardziej rygorystycznie, określić, co ma być poszukiwane w wiadomości lub utworzyć własne filtry.

Program Anti-Spam chroni też przed próbą dostępu do potencjalnie fałszywej witryny sieci Web za pośrednictwem łącza w wiadomości e-mail. W przypadku kliknięcia łącza do potencjalnie fałszywej witryny sieci Web następuje przekierowanie na bezpieczną stronę filtru ataków typu „phishing”. Witryny sieci Web, które nie mają być filtrowane, można dodać do białej listy (znajdujące się na tej liście witryny sieci Web nie są filtrowane).

Program Anti-Spam współpracuje z różnymi programami poczty e-mail, takimi jak konta obsługujące protokół POP3, POP3 w sieci Web, Yahoo®, MSN®/Hotmail®, Windows® Live™ Mail i MAPI (Microsoft Exchange Server). W przypadku odczytywania poczty e-mail przy użyciu przeglądarki należy dodać konto pocztowe w sieci Web do programu Anti-Spam. Wszystkie pozostałe konta są konfigurowane automatycznie i nie trzeba ich dodawać do programu Anti-Spam.

Uwaga: Program SecurityCenter zgłasza krytyczne i niekrytyczne problemy dotyczące ochrony natychmiast po ich wykryciu. Jeśli potrzebna jest pomoc w diagnozowaniu problemów dotyczących ochrony, można uruchomić narzędzie McAfee Virtual Technician.

W tym rozdziale

Funkcje programu Anti-Spam

Program Anti-Spam ma następujące funkcje.

Filtrowanie spamu

Zaawansowane filtry programu Anti-Spam zapobiegają wtargnięciu niechcianych wiadomości e-mail do skrzynki odbiorczej. Są automatycznie aktualizowane dla wszystkich kont e-mail. Można też utworzyć filtry niestandardowe, aby zapewnić odfiltrowanie całego spamu oraz zgłaszać spam firmie McAfee w celu analizy.

Filtrowanie ataków typu „phishing”

Filtr ataków typu „phishing” rozpoznaje witryny sieci Web (fałszywe) stanowiące potencjalne źródło tego typu ataków, które próbują zdobyć informacje osobiste.

Dostosowane przetwarzanie spamu

Niechciane wiadomości e-mail są oznaczane jako spam i przenoszone do folderu programu McAfee Anti-Spam, a poprawne wiadomości e-mail są oznaczane jako nie-spam i przenoszone do skrzynki odbiorczej.

Znajomi

Adresy e-mail znajomych są importowane do listy PRZYJACIELE, więc ich wiadomości e-mail nie są filtrowane.

Sortowanie elementów listy według trafności

Filtry osobiste, znajomych, książki adresowe i konta pocztowe w sieci Web można sortować według trafności (po prostu klikając nazwę odpowiedniej kolumny).

Dodatkowa obsługa

Program Anti-Spam obsługuje oprogramowanie Mozilla® Thunderbird™ 1.5 i 2.0 oraz program Windows Mail w 64-bitowej wersji systemu Windows Vista™. Ponadto nowa funkcja trybu gier zatrzymuje działające w tle procesy programu Anti-Spam, więc komputer nie jest spowalniany podczas korzystania z gier wideo lub oglądania filmów na dyskach DVD. Program Anti-Spam filtruje też konta programów Microsoft® Outlook®, Outlook Express lub Windows Mail na dowolnym porcie, łącznie z portami SSL (Secure Socket Layer).

ROZDZIAŁ 24

Konfigurowanie kont pocztowych w sieci Web

W przypadku odczytywania poczty e-mail przy użyciu przeglądarki należy skonfigurować program Anti-Spam, aby łączył się z danym kontem i filtrował wiadomości. Aby dodać konto pocztowe w sieci Web do programu Anti-Spam, należy po prostu dodać informacje o koncie podane przez operatora poczty e-mail.

Po dodaniu konta pocztowego w sieci Web można edytować informacje o nim i uzyskać więcej danych o filtrowanej poczcie z sieci Web. Jeśli konto pocztowe w sieci Web nie jest już używane lub nie ma być filtrowane, można je usunąć.

Program Anti-Spam współpracuje z różnymi programami poczty e-mail, takimi jak konta obsługujące protokół POP3, POP3 w sieci Web, Yahoo®, MSN/Hotmail, Windows Live Mail i MAPI. POP3 to najbardziej popularny typ konta i jest to standard internetowej poczty e-mail. W wypadku konta POP3 program Anti-Spam łączy się bezpośrednio z serwerem poczty e-mail i filtruje wiadomości, zanim zostaną one pobrane przez program poczty e-mail. Konta POP3 w sieci Web, Yahoo, MSN/Hotmail i Windows Mail są kontami w sieci Web. Filtrowanie kont POP3 w sieci Web jest podobne do filtrowania kont POP3. MAPI jest systemem zaprojektowanym przez firmę Microsoft, który obsługuje wiele typów komunikacji obejmujących internetową pocztę e-mail, faksowanie oraz przesyłanie wiadomości z użyciem serwera Exchange. Obecnie tylko program Microsoft Outlook współpracuje bezpośrednio z kontami MAPI.

Uwaga: Program Anti-Spam ma dostęp do konta MAPI, ale nie filtruje poczty e-mail przed pobraniem wiadomości przez program Microsoft Outlook.

W tym rozdziale

Dodawanie konta pocztowego w sieci Web

Jeśli chcesz filtrować spam w wiadomościach na koncie pocztowym w sieci Web POP3 (na przykład Yahoo), MSN/Hotmail lub Windows Mail (w pełni obsługiwana jest tylko wersja płatna), dodaj je.

1 Otwórz okienko Ochrona przed spamem.

Jak to zrobić?

1. W głównym okienku programu SecurityCenter kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
2. W obszarze informacji Poczta e-mail i wiadomości błyskawiczne kliknij przycisk **Konfiguruj**.
3. W okienku Poczta e-mail i wiadomości błyskawiczne w obszarze **Ochrona przed spamem** kliknij opcję **Zaawansowane**.

2 W okienku Ochrona przed spamem kliknij opcję **Konta pocztowe w sieci Web**.

3 W okienku Konta pocztowe w sieci Web kliknij przycisk **Dodaj**.

4 Określ *informacje o koncie* (strona 142), a następnie kliknij przycisk **Dalej**.

5 W obszarze **Opcje sprawdzania** określ, *kiedy program Anti-Spam ma sprawdzać obecność spamu na koncie* (strona 142).

6 Jeśli używasz połączenia telefonicznego, określ *sposób łączenia się programu Anti-Spam z Internetem* (strona 142).

7 Kliknij przycisk **Zakończ**.

Edytowanie konta pocztowego w sieci Web

Edycja informacji o koncie pocztowym w sieci Web jest konieczna w przypadku wystąpienia na nim zmiany. Edytuj informacje o koncie pocztowym w sieci Web, na przykład jeśli zmienisz hasło lub chcesz, aby program Anti-Spam częściej sprawdzał obecność spamu.

1 Otwórz okienko Ochrona przed spamem.

Jak to zrobić?

1. W głównym okienku programu SecurityCenter kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
2. W obszarze informacji Poczta e-mail i wiadomości błyskawiczne kliknij przycisk **Konfiguruj**.
3. W okienku Poczta e-mail i wiadomości błyskawiczne w obszarze **Ochrona przed spamem** kliknij opcję **Zaawansowane**.

2 W okienku Ochrona przed spamem kliknij opcję **Konta pocztowe w sieci Web**.

3 Wybierz konto, które ma być zmienione, a następnie kliknij przycisk **Edytuj**.

4 Określ *informacje o koncie* (strona 142), a następnie kliknij przycisk **Dalej**.

5 W obszarze **Opcje sprawdzania** określ, *kiedy program Anti-Spam ma sprawdzać obecność spamu na koncie* (strona 142).

6 Jeśli używasz połączenia telefonicznego, określ *sposób łączenia się programu Anti-Spam z Internetem* (strona 142).

7 Kliknij przycisk **Zakończ**.

Usuwanie konta pocztowego w sieci Web

Konto pocztowe w sieci Web, na którym nie trzeba już filtrować spamu w wiadomościach e-mail, należy usunąć. Jeśli konto na przykład nie jest już aktywne lub występują z nim problemy, możesz je usunąć, rozwiązując w ten sposób problem.

1 Otwórz okienko Ochrona przed spamem.

Jak to zrobić?

1. W głównym okienku programu SecurityCenter kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
2. W obszarze informacji Poczta e-mail i wiadomości błyskawiczne kliknij przycisk **Konfiguruj**.
3. W okienku Poczta e-mail i wiadomości błyskawiczne w obszarze **Ochrona przed spamem** kliknij opcję **Zaawansowane**.

2 W okienku Ochrona przed spamem kliknij opcję **Konta pocztowe w sieci Web**.

3 Wybierz konto, które ma zostać usunięte, a następnie kliknij przycisk **Usuń**.

Omówienie informacji o koncie pocztowym w sieci Web

W poniższych tabelach opisano informacje, które należy określić podczas dodawania lub edycji kont pocztowych w sieci Web.

Informacje o koncie

Informacje	Opis
Opis	Podaj swój własny opis konta. W tym polu można wpisać dowolne informacje.
Adres e-mail	Określ adres e-mail skojarzony z tym kontem e-mail.
Typ konta	Określ typ konta e-mail, które dodajesz (na przykład POP3 w sieci Web lub MSN/Hotmail).
Serwer	Określ nazwę serwera pocztowego, na którym znajduje się dane konto. Jeśli nie znasz nazwy serwera, wprowadź informacje podane przez dostawcę usług internetowych (ISP).
Nazwa użytkownika	Określ nazwę użytkownika danego konta e-mail. Jeśli adresem e-mail jest na przykład *nazwa_użytkownika*@hotmail.com, prawdopodobna nazwa użytkownika to *nazwa_użytkownika*.
Hasło	Określ hasło do danego konta e-mail.
Potwierdź hasło	Potwierdź hasło do danego konta e-mail.

Opcje sprawdzania

Opcja	Opis
Sprawdź co	Program Anti-Spam będzie sprawdzać obecność spamu na koncie w podanych odstępach czasu (w minutach). Odstęp czasu musi wynosić od 5 do 3600 minut.
Sprawdź podczas uruchamiania	Program Anti-Spam będzie sprawdzać konto podczas każdego kolejnego uruchamiania komputera.

Opcje połączenia

Opcja	Opis
Nigdy nie wybieraj numeru połączenia	Umożliwia wyłączenie opcji automatycznego wybierania numeru połączenia przez program Anti-Spam. W takim przypadku użytkownik musi najpierw ręcznie nawiązać połączenie telefoniczne.

Wybierz numer w przypadku braku połączenia	Gdy połączenie z Internetem jest niedostępne, program Anti-Spam automatycznie podejmuje próbę nawiązania go przy użyciu domyślnego telefonicznego połączenia z Internetem.
Zawsze wybieraj określony numer	Program Anti-Spam będzie zawsze próbował uzyskać połączenie przy użyciu podanego numeru telefonicznego. W przypadku uzyskania połączenia przy użyciu innego numeru telefonicznego, niż został określony, nastąpi rozłączenie.
Wybierz numer połączenia	Określ numer telefoniczny używany przez program Anti-Spam do łączenia z Internetem.
Utrzymaj połączenie po zakończeniu filtrowania	Komputer będzie utrzymywał połączenie z Internetem po zakończeniu procesu filtrowania.

ROZDZIAŁ 25

Konfigurowanie listy znajomych

Aby program Anti-Spam nie filtrował prawidłowych wiadomości e-mail od znajomych, można dodać ich adresy do listy PRZYJACIELE w programie Anti-Spam.

Najprostszym sposobem aktualizacji listy PRZYJACIELE jest dodanie książek adresowych do programu Anti-Spam. Wtedy wszystkie adresy e-mail są importowane. Po dodaniu książki adresowej jej zawartość jest automatycznie importowana w zaplanowanych odstępach czasu (codziennie, co tydzień lub co miesiąc), dzięki czemu lista PRZYJACIELE jest aktualna.

Listę PRZYJACIELE w programie Anti-Spam można też aktualizować ręcznie lub dodać całą domenę, jeśli każdy użytkownik danej domeny ma się znaleźć na liście. Po dodaniu na przykład domeny firma.com, nie będzie filtrowana żadna wiadomość e-mail z tej organizacji.

W tym rozdziale

Automatyczne konfigurowanie listy znajomych

Po dodaniu książek adresowych do programu Anti-Spam jest możliwe automatyczne aktualizowanie listy znajomych. Dodanie książki adresowej umożliwia programowi Anti-Spam import odpowiednich adresów e-mail i wypełnienie listy PRZYJACIELE.

Po dodaniu książki adresowej można zmienić częstotliwość importowania jej zawartości do listy PRZYJACIELE. Można też usunąć książkę adresową, jeśli jej zawartość nie ma już być importowana.

Dodawanie książki adresowej

Dodanie książek adresowych umożliwia automatyczne importowanie wszystkich adresów e-mail i aktualizowanie listy PRZYJACIELE w programie Anti-Spam. Dzięki temu lista PRZYJACIELE jest zawsze aktualna.

1 Otwórz okienko Ochrona przed spamem.

Jak to zrobić?

1. W głównym okienku programu SecurityCenter kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
2. W obszarze informacji Poczta e-mail i wiadomości błyskawiczne kliknij przycisk **Konfiguruj**.
3. W okienku Poczta e-mail i wiadomości błyskawiczne w obszarze **Ochrona przed spamem** kliknij opcję **Zaawansowane**.

2 W okienku Ochrona przed spamem kliknij opcję **Książki adresowe**.

3 W okienku Książki adresowe kliknij przycisk **Dodaj**.

4 Na liście **Typ** kliknij typ książki adresowej, który chcesz zaimportować.

5 Jeśli lista **Źródło** jest wypełniona, wybierz źródło książki adresowej. Jeśli masz na przykład książki adresowe programu Outlook, musisz wybrać z listy właśnie ten program.

6 Na liście **Harmonogram** kliknij opcję **Codziennie, Co tydzień** lub **Co miesiąc**, aby określić, jak często program Anti-Spam ma sprawdzać książkę adresową w poszukiwaniu nowych adresów.

7 Kliknij przycisk **OK**.

Edytowanie książki adresowej

Po dodaniu książek adresowych można zmienić informacje o ich importowaniu oraz harmonogram. Książki adresowe można edytować na przykład wtedy, jeśli program Anti-Spam ma częściej sprawdzać obecność nowych adresów.

1 Otwórz okienko Ochrona przed spamem.

Jak to zrobić?

1. W głównym okienku programu SecurityCenter kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
2. W obszarze informacji Poczta e-mail i wiadomości błyskawiczne kliknij przycisk **Konfiguruj**.
3. W okienku Poczta e-mail i wiadomości błyskawiczne w obszarze **Ochrona przed spamem** kliknij opcję **Zaawansowane**.

2 W okienku Ochrona przed spamem kliknij opcję **Książki adresowe**.

3 Wybierz książkę adresową, której ustawienia chcesz zmienić, a następnie kliknij przycisk **Edytuj**.

4 Na liście **Typ** kliknij typ książki adresowej, który chcesz zaimportować.

5 Jeśli lista **Źródło** jest wypełniona, wybierz źródło książki adresowej. Jeśli masz na przykład książki adresowe programu Outlook, musisz wybrać z listy właśnie ten program.

6 Na liście **Harmonogram** kliknij opcję **Codziennie, Co tydzień** lub **Co miesiąc**, aby określić, jak często program Anti-Spam ma sprawdzać książkę adresową w poszukiwaniu nowych adresów.

7 Kliknij przycisk **OK**.

Usuwanie książki adresowej

Usuń książkę adresową, jeśli nie chcesz już, aby program Anti-Spam automatycznie importował z niej adresy (gdy książka adresowa jest na przykład nieaktualna lub nie chcesz jej już używać).

1 Otwórz okienko Ochrona przed spamem.

Jak to zrobić?

1. W głównym okienku programu SecurityCenter kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
2. W obszarze informacji Poczta e-mail i wiadomości błyskawiczne kliknij przycisk **Konfiguruj**.
3. W okienku Poczta e-mail i wiadomości błyskawiczne w obszarze **Ochrona przed spamem** kliknij opcję **Zaawansowane**.

2 W okienku Ochrona przed spamem kliknij opcję **Książki adresowe**.

3 Wybierz książkę adresową, która ma zostać usunięta, a następnie kliknij przycisk **Usuń**.

Ręczne konfigurowanie znajomych

Lista znajomych aktualizowana jest ręcznie przez edycję poszczególnych wpisów. Na przykład po odebraniu wiadomości e-mail od znajomego, którego adresu nie ma w książce adresowej, można od razu dodać jego adres e-mail. W najprostszy sposób można to wykonać używając paska narzędzi zapewniającego ochronę przed spamem. Jeśli użytkownik nie korzysta z paska narzędzi zapewniającego ochronę przed spamem, musi podać informacje o znajomym.

Dodawanie znajomego z poziomu paska narzędzi zapewniającego ochronę przed spamem

W wypadku wykorzystywania do obsługi poczty e-mail programów Outlook, Outlook Express, Windows Mail, Eudora™ lub Thunderbird, można dodawać znajomych bezpośrednio z poziomu paska narzędzi zapewniającego ochronę przed spamem.

Aby dodać znajomego z poziomu programu...	**Zaznacz wiadomość, a następnie...**
Outlook, Outlook Express, Windows Mail	Kliknij przycisk **Dodaj znajomego**.
Eudora, Thunderbird	W menu **Anti-Spam** kliknij opcję **Dodaj znajomego**.

Ręczne dodawanie znajomego

Jeśli użytkownik nie chce dodać znajomego bezpośrednio z poziomu paska narzędzi lub zapomniał tego zrobić po odebraniu wiadomości e-mail, może nadal dodać znajomego do listy znajomych bez konieczności czekania na automatyczne zaimportowanie książki adresowej przez oprogramowanie chroniące przed spamem.

1 Otwórz okienko Ochrona przed spamem.

Jak to zrobić?

1. W głównym okienku programu SecurityCenter kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
2. W obszarze informacji Poczta e-mail i wiadomości błyskawiczne kliknij przycisk **Konfiguruj**.
3. W okienku Poczta e-mail i wiadomości błyskawiczne w obszarze **Ochrona przed spamem** kliknij opcję **Zaawansowane**.

2 W okienku Ochrona przed spamem kliknij opcję **Znajomi**.

3 W okienku Znajomi kliknij przycisk **Dodaj**.

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

5 Wybierz pozycję **Pojedynczy adres e-mail** z listy **Typ**.

6 Wprowadź adres e-mail znajomego w polu **Adres e-mail**.

7 Kliknij przycisk **OK**.

Dodawanie domeny

Jeśli do listy znajomych mają zostać dodani wszyscy użytkownicy z domeny, należy dodać do listy całą domenę. Po dodaniu na przykład domeny firma.com, nie będzie filtrowana żadna wiadomość e-mail z tej organizacji.

1 Otwórz okienko Ochrona przed spamem.

Jak to zrobić?

1. W głównym okienku programu SecurityCenter kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
2. W obszarze informacji Poczta e-mail i wiadomości błyskawiczne kliknij przycisk **Konfiguruj**.
3. W okienku Poczta e-mail i wiadomości błyskawiczne w obszarze **Ochrona przed spamem** kliknij opcję **Zaawansowane**.

2 W okienku Ochrona przed spamem kliknij opcję **Znajomi**.

3 W okienku Znajomi kliknij przycisk **Dodaj**.

4 Wpisz nazwę organizacji lub grupy w polu **Nazwa**.

5 Wybierz pozycję **Cała domena** z listy **Typ**.

6 W polu **Adres e-mail** wprowadź nazwę domeny.

7 Kliknij przycisk **OK**.

Edycja znajomego

Jeśli informacje dotyczące znajomego ulegną zmianie, można zaktualizować listę znajomych, aby mieć pewność, że wiadomości od tego znajomego nie zostaną oznaczone jako spam przez oprogramowanie chroniące przed spamem.

1 Otwórz okienko Ochrona przed spamem.

Jak to zrobić?

1. W głównym okienku programu SecurityCenter kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
2. W obszarze informacji Poczta e-mail i wiadomości błyskawiczne kliknij przycisk **Konfiguruj**.
3. W okienku Poczta e-mail i wiadomości błyskawiczne w obszarze **Ochrona przed spamem** kliknij opcję **Zaawansowane**.

2 W okienku Ochrona przed spamem kliknij opcję **Znajomi**.

3 Wybierz znajomego, którego dane mają zostać poddane edycji, a następnie kliknij przycisk **Edytuj**.

4 Zmień nazwisko znajomego w polu **Nazwa**.

5 Zmień adres e-mail znajomego w polu **Adres e-mail**.

6 Kliknij przycisk **OK**.

Edycja domeny

Jeśli informacje dotyczące domeny ulegną zmianie, można zaktualizować listę znajomych, aby mieć pewność, że wiadomości z tej domeny nie zostaną oznaczone jako spam przez oprogramowanie chroniące przed spamem.

1 Otwórz okienko Ochrona przed spamem.

Jak to zrobić?

1. W głównym okienku programu SecurityCenter kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
2. W obszarze informacji Poczta e-mail i wiadomości błyskawiczne kliknij przycisk **Konfiguruj**.
3. W okienku Poczta e-mail i wiadomości błyskawiczne w obszarze **Ochrona przed spamem** kliknij opcję **Zaawansowane**.

2 W okienku Ochrona przed spamem kliknij opcję **Znajomi**.

3 W okienku Znajomi kliknij przycisk **Dodaj**.

4 Zmień nazwę organizacji lub grupy w polu **Nazwa**.

5 Wybierz pozycję **Cała domena** z listy **Typ**.

6 Zmień nazwę domeny w polu **Adres e-mail**.

7 Kliknij przycisk **OK**.

Usuwanie znajomego

Jeśli znajomy lub domena znajdująca się na liście znajomych jest źródłem spamu, należy usunąć tego znajomego lub domenę z listy znajomych oprogramowania chroniącego przed spamem, aby wiadomości pochodzące z tego źródła mogły zostać odfiltrowane.

1 Otwórz okienko Ochrona przed spamem.

Jak to zrobić?

1. W głównym okienku programu SecurityCenter kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
2. W obszarze informacji Poczta e-mail i wiadomości błyskawiczne kliknij przycisk **Konfiguruj**.
3. W okienku Poczta e-mail i wiadomości błyskawiczne w obszarze **Ochrona przed spamem** kliknij opcję **Zaawansowane**.

2 W okienku Ochrona przed spamem kliknij opcję **Znajomi**.

3 Wybierz znajomego, który ma zostać usunięty, a następnie kliknij przycisk **Usuń.**

ROZDZIAŁ 26

Konfigurowanie wykrywania spamu

Oprogramowanie chroniące przed spamem umożliwia dostosowanie sposobu wykrywania spamu. Podczas analizowania spamu możliwe jest bardziej rygorystyczne filtrowanie wiadomości, określenie, czego należy szukać w wiadomości, i wyszukiwanie określonych zestawów znaków. Możliwe jest także utworzenie filtrów osobistych precyzyjnie określających jakie wiadomości mają być rozpoznawane jako spam przez oprogramowanie chroniące przed spamem. Jeśli na przykład nie są odfiltrowywane wiadomości zawierające słowo hipoteka, można dodać filtr zawierający to słowo.

Jeśli występują problemy związane z pocztą e-mail, jednym z elementów strategii rozwiązywania problemów może być wyłączenie ochrony przed spamem.

W tym rozdziale

Wyłączanie ochrony przed spamem

Ochronę przed spamem można wyłączyć, aby uniemożliwić oprogramowaniu chroniącemu przed spamem filtrowanie wiadomości e-mail.

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W polu **Ochrona przed spamem** kliknij opcję **Wyłączona**.

Wskazówka: Należy pamiętać o kliknięciu opcji **Włączona** w polu **Ochrona przed spamem** w celu zapewnienia ochrony przed spamem.

Konfigurowanie opcji filtrowania

Jeśli podczas analizowania spamu wiadomości mają być filtrowane bardziej rygorystycznie, jeśli użytkownik chce określić czego należy szukać w wiadomości i mają być wyszukiwane określone zestawy znaków, należy dostosować opcje filtrowania oprogramowania chroniącego przed spamem.

Poziomy filtrowania

Poziom filtrowania określa, jak bardzo rygorystycznie będą filtrowane wiadomości e-mail. Jeśli na przykład przy ustawieniu poziomu filtrowania na Średni spam nie jest filtrowany, można zmienić poziom na Wysoki. Jednak ustawienie poziomu filtrowania na Wysoki powoduje, że akceptowane są tylko wiadomości od nadawców znajdujących się na liście znajomych. Wszystkie pozostałe wiadomości są filtrowane.

Filtry specjalne

Filtr definiuje, jakich elementów ma szukać oprogramowanie chroniące przed spamem w wiadomości e-mail. Filtry specjalne wykrywają wiadomości e-mail zawierające ukryty tekst, osadzone obrazy, celowe błędy w znacznikach formatowania HTML i inne techniki używane powszechnie przez nadawców spamu. Ponieważ wiadomości e-mail posiadające te atrybuty są zwykle spamem, filtry specjalne są domyślnie włączone. Jeśli na przykład użytkownik chce odbierać wiadomości e-mail zawierające osadzone obrazy, może wyłączyć filtr specjalny dotyczący obrazów.

Zestawy znaków

Podczas analizowania spamu oprogramowanie chroniące przed spamem może wyszukiwać określone zestawów znaków. Zestawy znaków używane są do reprezentacji języka, włączając w to alfabet, liczby i inne symbole. Jeśli odbierany spam jest w języku greckim, można filtrować wszystkie wiadomości zawierające grecki zestaw znaków.

Należy jednak podchodzić ostrożnie do filtrowania zestawów znaków dla języków, w których otrzymywane są poprawne wiadomości e-mail. Jeśli na przykład mają być filtrowane tylko wiadomości w języku włoskim, należy wybrać zestaw znaków dla Europy Zachodniej, ponieważ język włoski należy do zestawu znaków dla Europy Zachodniej. Jeśli jednak poprawne wiadomości otrzymywane są w języku angielskim, wybranie zestawu znaków dla Europy Zachodniej spowoduje także odfiltrowywanie wiadomości w języku angielskim i w innych językach należących do zestawu znaków dla Europy Zachodniej. W tym przypadku filtrowanie tylko wiadomości w języku włoskim nie jest możliwe.

Uwaga: Filtrowanie wiadomości zawierających znaki należące do określonego zestawu znaków jest przeznaczone dla użytkowników zaawansowanych.

Zmiana poziomu filtrowania

Można określić, jak bardzo rygorystycznie filtrowane będą wiadomości e-mail. Na przykład, jeśli poprawne wiadomości są odfiltrowywane, można obniżyć poziom filtrowania.

1 Otwórz okienko Ochrona przed spamem.

Jak to zrobić?

1. W głównym okienku programu SecurityCenter kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
2. W obszarze informacji Poczta e-mail i wiadomości błyskawiczne kliknij przycisk **Konfiguruj**.
3. W okienku Poczta e-mail i wiadomości błyskawiczne w obszarze **Ochrona przed spamem** kliknij opcję **Zaawansowane**.

2 W okienku Ochrona przed spamem kliknij opcję **Opcje filtrowania**.

3 W opcji **Opcje filtrowania** przesuń suwak do odpowiedniego poziomu, a następnie kliknij przycisk **OK**.

Poziom	Opis
Niski	Większość wiadomości poczty e-mail jest akceptowana.
Średnio-niski	Tylko wiadomości z oczywistym spamem są odfiltrowywane.
Średni	Wiadomości e-mail są filtrowane na zalecanym poziomie.
Średnio-wysoki	Wszelkie wiadomości przypominające spam są odfiltrowywane.
Wysoki	Akceptowane są tylko wiadomości od nadawców znajdujących się na liście znajomych.

Wyłączanie filtru specjalnego

Filtry specjalne są domyślnie włączone, ponieważ służą do odfiltrowywania wiadomości wysyłanych zwykle przez nadawców spamu. Na przykład wiadomości e-mail zawierające osadzone obrazy są zwykle spamem. Jeśli jednak użytkownik często otrzymuje poprawne wiadomości e-mail z osadzonymi obrazami, może wyłączyć filtr specjalny dotyczący obrazów.

1 Otwórz okienko Ochrona przed spamem.

Jak to zrobić?

1. W głównym okienku programu SecurityCenter kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
2. W obszarze informacji Poczta e-mail i wiadomości błyskawiczne kliknij przycisk **Konfiguruj**.
3. W okienku Poczta e-mail i wiadomości błyskawiczne w obszarze **Ochrona przed spamem** kliknij opcję **Zaawansowane**.

2 W okienku Ochrona przed spamem kliknij opcję **Opcje filtrowania**.

3 W obszarze **Filtry specjalne** zaznacz odpowiednie pola wyboru lub usuń ich zaznaczenie, a następnie kliknij przycisk **OK**.

Filtr	Opis
Odfiltruj wiadomości zawierające ukryty tekst	Powoduje wyszukiwanie tekstu ukrytego, ponieważ wiadomości z tekstem ukrytym są często wykorzystywane przez nadawców spamu w celu uniknięcia wykrycia.
Odfiltruj wiadomości zawierające przede wszystkim obrazy	Powoduje wyszukiwanie osadzonych obrazów, ponieważ wiadomości z osadzonymi obrazami są zwykle spamem.
Odfiltruj wiadomości zawierające celowe błędy w znacznikach formatowania HTML	Powoduje wyszukiwanie wiadomości zawierających nieprawidłowe formatowanie, ponieważ uniemożliwia ono filtrom odfiltrowanie spamu.
Nie odfiltrowuj wiadomości większych niż	Nie wyszukuje wiadomości większych od określonego rozmiaru, ponieważ wiadomości o dużym rozmiarze mogą nie być spamem. Można tu zwiększać lub zmniejszać rozmiar wiadomości (prawidłowy zakres 0–250 KB).

Zastosuj filtry zestawów znaków

Uwaga: Filtrowanie wiadomości zawierających znaki należące do określonego zestawu znaków jest przeznaczone dla użytkowników zaawansowanych.

Można odfiltrowywać zestawy znaków dla określonego języka, jednak nie należy odfiltrowywać zestawów znaków dla języków, w których otrzymywane są poprawne wiadomości e-mail.

1 Otwórz okienko Ochrona przed spamem.

Jak to zrobić?

1. W głównym okienku programu SecurityCenter kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
2. W obszarze informacji Poczta e-mail i wiadomości błyskawiczne kliknij przycisk **Konfiguruj**.
3. W okienku Poczta e-mail i wiadomości błyskawiczne w obszarze **Ochrona przed spamem** kliknij opcję **Zaawansowane**.

2 W okienku Ochrona przed spamem kliknij opcję **Zestawy znaków**.

3 Zaznacz pola wyboru obok zestawów znaków przewidzianych do odfiltrowania.

4 Kliknij przycisk **OK**.

Używanie filtrów osobistych

Filtr definiuje, jakich elementów ma szukać oprogramowanie chroniące przed spamem w wiadomości e-mail. Po wykryciu spamu wiadomość jest oznaczana jako spam i jest pozostawiana w skrzynce odbiorczej lub przenoszona do folderu programu McAfee Anti-Spam. Więcej informacji na temat priorytetów alertów można znaleźć w *Modyfikowanie sposobu przetwarzania i oznaczania wiadomości* (strona 162).

Domyślnie oprogramowanie chroniące przed spamem stosuje wiele filtrów, jednak możliwe jest również tworzenie nowych filtrów lub edycja istniejących, aby bardzo dokładnie zdefiniować, które wiadomości mają być uznawane za spam przez oprogramowanie chroniące przed spamem. Jeśli na przykład został dodany filtr zawierający słowo hipoteka, oprogramowanie chroniące przed spamem odfiltrowuje wiadomości zawierające to słowo. Nie należy tworzyć filtrów dla popularnych słów występujących w prawidłowych wiadomościach e-mail, ponieważ będą wówczas odfiltrowywane także wiadomości niebędące spamem. Po utworzeniu filtru można poddać go edycji, jeśli okaże się, że nadal nie są wykrywane wszystkie wiadomości będące spamem. Jeśli na przykład został utworzony filtr wyszukujący słowo viagra w temacie wiadomości, ale nadal otrzymywane są wiadomości zawierające słowo viagra w treści wiadomości, można zmienić filtr tak, aby wyszukiwał słowo viagra w treści wiadomości, a nie w temacie.

Wyrażenia regularne (regular expressions — RegEx) to specjalne znaki i sekwencje, które mogą także być używane w filtrach osobistych. Jednak firma McAfee zaleca używanie wyrażeń regularnych tylko przez użytkowników zaawansowanych. Aby uzyskać więcej informacji na temat wyrażeń regularnych lub sposobu ich używania, można użyć sieci Web (na przykład pod adresem http://pl.wikipedia.org/wiki/Wyrażenia_regularne).

Dodawanie filtru osobistego

Możliwe jest także dodanie filtrów precyzyjnie określających, jakie wiadomości mają być rozpoznawane jako spam przez oprogramowanie chroniące przed spamem.

1 Otwórz okienko Ochrona przed spamem.

Jak to zrobić?

1. W głównym okienku programu SecurityCenter kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
2. W obszarze informacji Poczta e-mail i wiadomości błyskawiczne kliknij przycisk **Konfiguruj**.
3. W okienku Poczta e-mail i wiadomości błyskawiczne w obszarze **Ochrona przed spamem** kliknij opcję **Zaawansowane**.

2 W okienku Ochrona przed spamem kliknij opcję **Filtry osobiste**.

3 Kliknij przycisk **Dodaj**.

4 *Określ, co filtr osobisty ma wyszukiwać* (strona 160) w wiadomości e-mail.

5 Kliknij przycisk **OK**.

Edycja filtru osobistego

Edycja istniejących filtrów służy do precyzyjnego określenia, jakie wiadomości mają być rozpoznawane jako spam.

1 Otwórz okienko Ochrona przed spamem.

Jak to zrobić?

1. W głównym okienku programu SecurityCenter kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
2. W obszarze informacji Poczta e-mail i wiadomości błyskawiczne kliknij przycisk **Konfiguruj**.
3. W okienku Poczta e-mail i wiadomości błyskawiczne w obszarze **Ochrona przed spamem** kliknij opcję **Zaawansowane**.

2 W okienku Ochrona przed spamem kliknij opcję **Filtry osobiste**.

3 Wybierz filtr, który ma zostać zmieniony, a następnie kliknij przycisk **Edytuj**.

4 *Określ, co filtr osobisty ma wyszukiwać* (strona 160) w wiadomości e-mail.

5 Kliknij przycisk **OK**.

Usuwanie filtru osobistego

Możliwe jest trwałe usuniecie filtrów, których nie chcemy już dłużej używać.

1 Otwórz okienko Ochrona przed spamem.

Jak to zrobić?

1. W głównym okienku programu SecurityCenter kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
2. W obszarze informacji Poczta e-mail i wiadomości błyskawiczne kliknij przycisk **Konfiguruj**.
3. W okienku Poczta e-mail i wiadomości błyskawiczne w obszarze **Ochrona przed spamem** kliknij opcję **Zaawansowane**.

2 W okienku Ochrona przed spamem kliknij opcję **Filtry osobiste**.

3 Wybierz filtr, który ma zostać usunięty, a następnie kliknij przycisk **Usuń**.

4 Kliknij przycisk **OK**.

Konfigurowanie filtru osobistego

W poniższej tabeli opisano, czego szuka filtr osobisty w wiadomości e-mail.

Informacje	Opis
Element	Kliknij pozycję określającą, czy filtr ma szukać słów lub wyrażeń w tematach wiadomości, w treści, w nagłówkach, czy też w nazwach nadawców.
Stan	Kliknij pozycję określającą, czy filtr ma szukać wiadomości zawierającej podane słowa lub wyrażenia, czy wiadomości niezawierającej ich.
Słowa lub wyrażenia	Wpisz, czego należy szukać w wiadomości. Na przykład wpisanie słowa hipoteka spowoduje odfiltrowanie wszystkich wiadomości zawierających to słowo.
Filtr korzysta z wyrażeń regularnych	Określ wzory znaków używane w warunkach filtru. Aby sprawdzić dany wzór znaków, kliknij opcję **Test**.

ROZDZIAŁ 27

Filtrowanie wiadomości e-mail

Oprogramowanie chroniące przed spamem bada przychodzące wiadomości e-mail i klasyfikuje je jako spam (wiadomości e-mail nakłaniające do zakupów) lub phishing (wiadomości e-mail nakłaniające do podania informacji osobistych potencjalnie fałszywej witrynie sieci Web). Domyślnie oprogramowanie chroniące przed spamem oznacza następnie każdą niechcianą wiadomość jako spam lub phishing (w wierszu tematu wiadomości wyświetlana jest etykietka [SPAM] lub [PHISH]) i przenosi wiadomość do folderu programu McAfee Anti-Spam.

Aby dostosować sposób filtrowania wiadomości przez oprogramowanie chroniące przed spamem można oznaczać wiadomości będące lub niebędące spamem z poziomu paska narzędzi zapewniającego ochronę przed spamem, można zmieniać lokalizację, do której przenoszony jest spam lub zmieniać etykietkę wyświetlaną w wierszu tematu.

Aby zmienić sposób przetwarzania i oznaczania spamu, można dostosować lokalizację, do której przenoszone są wiadomości sklasyfikowane jako spam i phishing oraz można dostosować nazwę etykietki wyświetlanej w wierszu tematu.

Jednym z elementów strategii rozwiązywania problemów z programem poczty e-mail może być także wyłączenie pasków narzędzi zapewniających ochronę przed spamem.

W tym rozdziale

Oznaczanie wiadomości z poziomu paska narzędzi zapewniającego ochronę przed spamem

Jeśli oznaczymy wiadomość jako spam, temat wiadomości otrzyma etykietkę [SPAM] lub inną zdefiniowaną przez użytkownika i pozostanie w Skrzynce odbiorczej, folderze programu McAfee Anti-Spam (Outlook, Outlook Express, Windows Mail, Thunderbird) lub w folderze Śmieci (Eudora®). Jeśli oznaczymy wiadomość jako nie-spam, etykietka wiadomości zostaje usunięta i wiadomość zostanie przeniesiona do skrzynki odbiorczej.

Aby oznaczyć wiadomość z poziomu programu...	**Zaznacz wiadomość, a następnie...**
Outlook, Outlook Express, Windows Mail	Kliknij opcję **Oznacz jako spam** lub **Oznacz jako nie-spam**.
Eudora, Thunderbird	W menu **Anti-Spam** kliknij opcję **Oznacz jako spam** lub **Oznacz jako nie-spam.**

Modyfikowanie sposobu przetwarzania i oznaczania wiadomości

Można zmienić sposób przetwarzania i oznaczania spamu. Na przykład można zadecydować, czy wiadomość e-mail jest pozostawiana w skrzynce odbiorczej, czy przenoszona do folderu programu McAfee Anti-Spam oraz można zmienić etykietkę [SPAM] lub [PHISH] wyświetlaną w wierszu tematu wiadomości.

1 Otwórz okienko Ochrona przed spamem.

Jak to zrobić?

1. W głównym okienku programu SecurityCenter kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
2. W obszarze informacji Poczta e-mail i wiadomości błyskawiczne kliknij przycisk **Konfiguruj**.
3. W okienku Poczta e-mail i wiadomości błyskawiczne w obszarze **Ochrona przed spamem** kliknij opcję **Zaawansowane**.

2 W okienku Ochrona przed spamem kliknij opcję **Przetwarzanie**.

3 Zaznacz lub usuń zaznaczenie odpowiednich pól wyboru, a następnie kliknij przycisk **OK**.

Opcja	Opis
Oznacz jako spam i przenieś do folderu programu McAfee Anti-Spam	Jest to ustawienie domyślne. Wiadomości zawierające spam będą przenoszone do folderu programu McAfee Anti-Spam.
Oznacz jako spam i pozostaw w skrzynce odbiorczej	Wiadomości zidentyfikowane jako spam pozostaną w skrzynce odbiorczej.
Dodaj ten dostosowywany znacznik do tematu wiadomości rozpoznanych jako spam	Podany znacznik będzie dodawany do tematu każdej wiadomości e-mail zidentyfikowanej jako spam.
Dodaj ten dostosowywany znacznik do tematu wiadomości wysyłanych w ramach ataku typu phishing:	Podany znacznik będzie dodawany do tematu każdej wiadomości e-mail zidentyfikowanej jako atak typu „phishing”.

Wyłącz pasek narzędzi zapewniający ochronę przed spamem

Jeśli używany jest program Outlook, Outlook Express, Windows Mail, Eudora lub Thunderbird, możliwe jest wyłączenie paska narzędzi zapewniającego ochronę przed spamem.

1 Otwórz okienko Ochrona przed spamem.

Jak to zrobić?

1. W głównym okienku programu SecurityCenter kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
2. W obszarze informacji Poczta e-mail i wiadomości błyskawiczne kliknij przycisk **Konfiguruj**.
3. W okienku Poczta e-mail i wiadomości błyskawiczne w obszarze **Ochrona przed spamem** kliknij opcję **Zaawansowane**.

2 W okienku Ochrona przed spamem kliknij opcję **Paski narzędzi poczty e-mail.**

3 Usuń zaznaczenie pola wyboru obok paska narzędzi, który chcesz wyłączyć.

4 Kliknij przycisk **OK**.

Wskazówka: Paski narzędzi zapewniające ochronę przed spamem można włączyć ponownie, zaznaczając odpowiednie pola wyboru.

ROZDZIAŁ 28

Praca z odfiltrowanymi wiadomościami e-mail

Czasami niektóre wiadomości będące spamem mogą nie zostać wykryte. Jeśli tak się zdarzy, spam można zgłosić firmie McAfee, która przeprowadzi odpowiednie analizy i przygotuje aktualizacje filtrów.

Używając konta pocztowego w sieci Web można kopiować i usuwać odfiltrowane wiadomości oraz uzyskiwać dodatkowe informacje o nich. Jest to przydatne, jeśli nie ma pewności, że nie została odfiltrowana prawidłowa wiadomość lub jeśli użytkownik chce wiedzieć, jaka wiadomość została odfiltrowana.

W tym rozdziale

Zgłaszanie spamu firmie McAfee

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

1 Otwórz okienko Ochrona przed spamem.

Jak to zrobić?

1. W głównym okienku programu SecurityCenter kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
2. W obszarze informacji Poczta e-mail i wiadomości błyskawiczne kliknij przycisk **Konfiguruj**.
3. W okienku Poczta e-mail i wiadomości błyskawiczne w obszarze **Ochrona przed spamem** kliknij opcję **Zaawansowane**.

2 W okienku Ochrona przed spamem kliknij opcję **Wysyłanie raportów do firmy McAfee**.

3 Zaznacz odpowiednie pola wyboru, a następnie kliknij przycisk **OK**.

Opcja	Opis
Włącz raportowanie po kliknięciu opcji Oznacz jako spam	Wiadomość będzie zgłaszana firmie McAfee za każdym razem, gdy zostanie oznaczona jako spam.
Włącz raportowanie po kliknięciu opcji Oznacz jako nie-spam	Wiadomość będzie zgłaszana firmie McAfee za każdym razem, gdy zostanie oznaczona jako nie-spam.

Wyślij całą wiadomość (nie tylko nagłówek)	Podczas zgłaszania spamu firmie McAfee wysyłana będzie cała wiadomość, a nie tylko jej nagłówek.

Kopiowanie lub usuwanie odfiltrowanej wiadomości z poczty z sieci Web

Można kopiować lub usuwać wiadomości z konta poczty internetowej, które zostały odfiltrowane.

1. W obszarze **Typowe zadania** kliknij opcję **Przeglądaj ostatnie zdarzenia**.
2. W okienku Ostatnie zdarzenia kliknij opcję **Wyświetl dziennik**.
3. W lewym okienku rozwiń listę **Poczta e-mail i wiadomości błyskawiczne**, a następnie kliknij pozycję **Zdarzenia filtrowania poczty z sieci Web**.
4. Zaznacz wiadomość.
5. W obszarze **Działanie** wykonaj jedną z następujących czynności:
   - Kliknij przycisk **Kopiuj**, aby skopiować wiadomość do schowka.
   - Kliknij przycisk **Usuń**, aby usunąć wiadomość.

Wyświetlanie zdarzenia filtrowania poczty z sieci Web

Możliwe jest wyświetlenie daty i godziny odfiltrowania wiadomości e-mail oraz konta, z którego pochodzi.

1. W obszarze **Typowe zadania** kliknij opcję **Przeglądaj ostatnie zdarzenia**.
2. W okienku Ostatnie zdarzenia kliknij opcję **Wyświetl dziennik**.
3. W lewym okienku rozwiń listę **Poczta e-mail i wiadomości błyskawiczne**, a następnie kliknij pozycję **Zdarzenia filtrowania poczty z sieci Web**.
4. Wybierz dziennik, który ma zostać wyświetlony.

ROZDZIAŁ 29

Konfigurowanie ochrony przed atakami typu „phishing”

Oprogramowanie chroniące przed spamem klasyfikuje niechcianą pocztę e-mail 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). Funkcja ochrony przed atakami typu „phishing” chroni przed przechodzeniem do fałszywych witryn sieci Web. W przypadku kliknięcia w wiadomości e-mail łącza do fałszywej lub potencjalnie fałszywej witryny sieci Web, oprogramowanie chroniące przed spamem przekieruje użytkownika na stronę filtru Phishing.

Jeśli są to witryny sieci Web, które nie mają być filtrowane, należy je dodać do białej listy filtru Phishing. Można także edytować witryny sieci Web znajdujące się na białej liście lub usuwać je z listy. Nie jest konieczne dodawanie takich witryn sieci Web, jak Google®, Yahoo lub McAfee, ponieważ nie są one uznawane za szkodliwe.

Uwaga: Jeśli zainstalowany jest program SiteAdvisor, użytkownik nie otrzymuje ochrony przed atakami typu phishing ze strony oprogramowania chroniącego przed spamem, ponieważ program SiteAdvisor zapewnia już podobną ochronę.

W tym rozdziale

Dodawanie witryny sieci Web do białej listy

Jeśli istnieją witryny sieci Web, które nie mają być filtrowane, należy je dodać do białej listy.

1. Otwórz okienko Ochrona przed atakami typu „phishing”.

   Jak to zrobić?

   1. W okienku Początek programu SecurityCenter kliknij kategorię **Internet i sieć.**
   2. W obszarze informacji kategorii Internet i sieć kliknij opcję **Konfiguruj**.

2. W okienku Ochrona przed atakami typu „phishing” kliknij opcję **Zaawansowane**.
3. W obszarze **Biała lista,** kliknij opcję **Dodaj.**
4. Wpisz adres witryny sieci Web, a następnie kliknij przycisk **OK**.

Edycja witryn znajdujących się na białej liście

Jeśli witryna sieci Web została dodana do białej listy i zmienił się jej adres, zawsze można ją zaktualizować.

1 Otwórz okienko Ochrona przed atakami typu „phishing”.

Jak to zrobić?

1. W okienku Początek programu SecurityCenter kliknij kategorię **Internet i sieć.**
2. W obszarze informacji kategorii Internet i sieć kliknij opcję **Konfiguruj**.

2 W okienku Ochrona przed atakami typu „phishing” kliknij opcję **Zaawansowane**.

3 W obszarze **Biała lista,** wybierz witrynę sieci Web, którą chcesz zaktualizować, a następnie kliknij opcję **Edytuj.**

4 Przeprowadź edycję adresu witryny sieci Web, a następnie kliknij przycisk **OK**.

Usuwanie witryny sieci Web z białej listy

Jeśli witryna sieci Web została dodana do białej listy, ponieważ konieczne było uzyskanie dostępu do niej, a teraz ma być filtrowana, należy usunąć ją z białej listy.

1 Otwórz okienko Ochrona przed atakami typu „phishing”.

Jak to zrobić?

1. W okienku Początek programu SecurityCenter kliknij kategorię **Internet i sieć.**
2. W obszarze informacji kategorii Internet i sieć kliknij opcję **Konfiguruj**.

2 W okienku Ochrona przed atakami typu „phishing” kliknij opcję **Zaawansowane**.

3 W obszarze **Biała lista,** wybierz witrynę sieci Web, którą chcesz usunąć, a następnie kliknij opcję **Usuń.**

Wyłączanie ochrony przed atakami typu „phishing”

Jeśli zainstalowane jest już oprogramowanie chroniące przed atakami typu „phishing” pochodzące od firmy innej niż McAfee i występuje konflikt, można wyłączyć ochronę przed atakami typu „phishing” w oprogramowaniu chroniącym przed spamem.

1. W okienku Początek programu SecurityCenter kliknij kategorię **Internet i sieć.**
2. W obszarze informacji kategorii Internet i sieć kliknij opcję **Konfiguruj**.
3. W polu **Ochrona przed atakami typu „phishing”** kliknij opcję **Wyłączona**.

Wskazówka: Po zakończeniu należy pamiętać o kliknięciu opcji **Włączona** w polu **Ochrona przed atakami typu „phishing”**, aby zapewnić sobie ochronę przed fałszywymi witrynami sieci Web.

ROZDZIAŁ 30

McAfee Privacy Service

Oprogramowanie Privacy Service zapewnia zaawansowaną ochronę użytkownika, jego rodziny, plików osobistych i komputera. Chroni przed kradzieżą tożsamości w trybie online, blokuje wysyłanie danych osobowych i pozwalających na identyfikację użytkownika oraz filtruje w trybie online potencjalnie obraźliwą zawartość (między innymi obrazy). Oferuje również zaawansowane funkcje ochrony rodzicielskiej umożliwiające dorosłym monitorowanie, kontrolowanie i rejestrowanie nieuprawnionych zachowań podczas przeglądania sieci Web, a także bezpieczny obszar pamięci przeznaczony na hasła osobiste.

Przed rozpoczęciem korzystania z programu Privacy Service można zapoznać się z niektórymi z jego najbardziej popularnych funkcji. Szczegółowe informacje na temat konfigurowania i używania tych funkcji znajdują się w pomocy programu Privacy Service.

Uwaga: Program SecurityCenter zgłasza krytyczne i niekrytyczne problemy dotyczące ochrony natychmiast po ich wykryciu. Jeśli potrzebna jest pomoc w diagnozowaniu problemów dotyczących ochrony, można uruchomić narzędzie McAfee Virtual Technician.

W tym rozdziale

Funkcje usługi Privacy Service

Program Privacy Service udostępnia następujące funkcje:

- Funkcje ochrony rodzicielskiej
- Ochrona informacji osobistych
- Magazyn haseł

Funkcje ochrony rodzicielskiej

Funkcje ochrony rodzicielskiej umożliwiają użytkownikom usługi SecurityCenter filtrowanie potencjalnie nieodpowiednich obrazów, skonfigurowanie klasyfikacji zawartości dla poszczególnych grup wiekowych, które ograniczają możliwość dostępu do witryn sieci Web i zawartości, która może być wyświetlana przez użytkownika, a także umożliwiają ustawienie limitów czasu przeglądania sieci Web określających okres i czas, w ciągu którego użytkownik ma dostęp do sieci. Funkcje ochrony rodzicielskiej umożliwiają ograniczenie dostępu do określonych witryn sieci Web oraz umożliwiają lub blokują dostęp w oparciu o słowa kluczowe.

Ochrona informacji osobistych

Ochrona informacji osobistych umożliwia blokowanie wysyłania poufnych lub tajnych informacji (na przykład numerów kart kredytowych, numerów rachunków bankowych, adresów itp.) przez sieć Web.

Magazyn haseł

Magazyn haseł jest bezpiecznym obszarem przechowywania osobistych haseł. Umożliwia on przechowywanie haseł ze świadomością, że nikt inny (nawet Administrator) nie ma do nich dostępu.

ROZDZIAŁ 31

Konfigurowanie funkcji ochrony rodzicielskiej

Jeśli z komputera korzystają dzieci, można skonfigurować dla nich funkcje ochrony rodzicielskiej. Pomagają one w określeniu, co dzieci mogą oglądać i robić, przeglądając sieć Web. Ustawienia obejmują m.in. możliwość filtrowania obrazów, wybór grupy klasyfikacji treści oraz określenie limitów czasowych przeglądania sieci Web. Filtrowanie obrazów blokuje wyświetlanie potencjalnie nieodpowiednich obrazów, gdy dziecko przegląda sieć Web. Grupa klasyfikacji zawartości określa rodzaj zawartości i witryny sieci Web dostępne dla dziecka na podstawie jego grupy wiekowej. Natomiast ograniczenia czasu przeglądania witryn sieci Web określają, w jakich dniach i godzinach dziecko może przeglądać sieć Web. Funkcje ochrony rodzicielskiej umożliwiają także filtrowanie (blokowanie lub zezwalanie) określonych witryn sieci Web dla wszystkich dzieci.

Uwaga: Tylko Administrator może konfigurować funkcje ochrony rodzicielskiej.

W tym rozdziale

Konfigurowanie użytkowników

Aby skonfigurować funkcje ochrony rodzicielskiej, należy przypisać uprawnienia użytkownikom SecurityCenter. Domyślnie użytkownicy SecurityCenter odpowiadają użytkownikom systemu Windows skonfigurowanym w komputerze. Jednakże w przypadku aktualizacji SecurityCenter z poprzedniej wersji, która korzystała z użytkowników McAfee, użytkownicy ci i ich uprawnienia zostaną zachowane.

Uwaga: Aby skonfigurować użytkowników, należy zalogować się w programie SecurityCenter jako administrator.

Praca z użytkownikami systemu Windows

Aby skonfigurować funkcje ochrony rodzicielskiej, należy przypisać użytkownikom uprawnienia, które określają, co poszczególni użytkownicy mogą oglądać i robić w Internecie. Domyślnie użytkownicy SecurityCenter odpowiadają użytkownikom systemu Windows skonfigurowanym w komputerze. Aby dodać użytkownika, należy przeprowadzić edycję informacji o jego koncie lub usunąć go w oknie Zarządzanie komputerem w systemie Windows. Następnie można w programie SecurityCenter skonfigurować funkcje ochrony rodzicielskiej dla tych użytkowników.

W przypadku aktualizacji SecurityCenter z poprzedniej wersji, która korzystała z użytkowników McAfee zobacz sekcja *Praca u użytkownikami McAfee* (strona 176).

Praca z użytkownikami McAfee

W przypadku aktualizacji SecurityCenter z poprzedniej wersji, która korzystała z użytkowników McAfee, użytkownicy ci i ich uprawnienia zostaną zachowane automatycznie. Można wciąż konfigurować użytkowników McAfee i zarządzać nimi. Jednakże, w celu łatwiejszej obsługi programu, firma McAfee zaleca przejście na użytkowników systemu Windows. Po przejściu na użytkowników Windows nie można wrócić do obsługi użytkowników McAfee.

Jeśli użytkownicy McAfee są nadal używani, można ich dodawać, edytować i usuwać oraz zmieniać i pobierać hasło administratora McAfee.

Przełącz na użytkowników systemu Windows

W celu łatwiejszej obsługi programu firma McAfee zaleca przejście na użytkowników systemu Windows. Po przejściu na użytkowników Windows nie można wrócić do obsługi użytkowników McAfee.

1 Otwórz okienko Ustawienia użytkowników.

   Jak to zrobić?

   1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
   2. W okienku Początek programu SecurityCenter kliknij kategorię **Funkcje ochrony rodzicielskiej**.
   3. W sekcji informacji kategorii Funkcje ochrony rodzicielskiej kliknij pozycję **Konfiguruj**.
   4. W okienku Konfiguracja kategorii Funkcje ochrony rodzicielskiej kliknij opcję **Zaawansowane**.

2 W okienku Ustawienia użytkowników kliknij opcję **Przełącz**.

3 Potwierdź operację.

Dodaj użytkownika McAfee

Po utworzeniu użytkownika McAfee można skonfigurować dla niego funkcje ochrony rodzicielskiej. Aby uzyskać dodatkowe informacje, patrz pomoc do usługi Privacy Service.

1 Zaloguj się w programie SecurityCenter jako Administrator.

2 Otwórz okienko Ustawienia użytkowników.

   Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij kategorię **Funkcje ochrony rodzicielskiej**.
3. W sekcji informacji kategorii Funkcje ochrony rodzicielskiej kliknij pozycję **Konfiguruj**.
4. W okienku Konfiguracja kategorii Funkcje ochrony rodzicielskiej kliknij opcję **Zaawansowane**.

3 W okienku Ustawienia użytkowników kliknij przycisk **Dodaj**.

4 Postępuj zgodnie z wyświetlanymi na ekranie instrukcjami konfigurowania nazwy użytkownika, hasła, typu konta i funkcji ochrony rodzicielskiej.

5 Kliknij przycisk **Utwórz**.

Edytuj informacje o koncie użytkownika McAfee

Można zmienić hasło, typ konta i możliwość automatycznego zalogowania się użytkownika McAfee.

1 Zaloguj się w programie SecurityCenter jako Administrator.

2 Otwórz okienko Ustawienia użytkowników.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij kategorię **Funkcje ochrony rodzicielskiej**.
3. W sekcji informacji kategorii Funkcje ochrony rodzicielskiej kliknij pozycję **Konfiguruj**.
4. W okienku Konfiguracja kategorii Funkcje ochrony rodzicielskiej kliknij opcję **Zaawansowane**.

3 W okienku Ustawienia użytkowników kliknij nazwę użytkownika, a następnie kliknij przycisk **Edytuj**.

4 Postępuj zgodnie z wyświetlanymi na ekranie instrukcjami edycji hasła użytkownika, typu konta i funkcji ochrony rodzicielskiej.

5 Kliknij przycisk **OK**.

Usuń użytkownika McAfee

Użytkownika McAfee można usunąć w dowolnym momencie.

Aby usunąć użytkownika McAfee

1 Zaloguj się w programie SecurityCenter jako Administrator.

2 Otwórz okienko Ustawienia użytkowników.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij kategorię **Funkcje ochrony rodzicielskiej**.
3. W sekcji informacji kategorii Funkcje ochrony rodzicielskiej kliknij pozycję **Konfiguruj**.
4. W okienku Konfiguracja kategorii Funkcje ochrony rodzicielskiej kliknij opcję **Zaawansowane**.

3 W okienku Ustawienia użytkowników, w obszarze **Konta użytkowników McAfee**, wybierz nazwę użytkownika i kliknij przycisk **Usuń**.

Zmień hasło administratora McAfee

W przypadku problemów z zapamiętaniem hasła administratora McAfee lub podejrzeń, że zostało ono ujawnione nieuprawnionej osobie, można je zmienić.

1 Zaloguj się w programie SecurityCenter jako Administrator.

2 Otwórz okienko Ustawienia użytkowników.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij kategorię **Funkcje ochrony rodzicielskiej**.
3. W sekcji informacji kategorii Funkcje ochrony rodzicielskiej kliknij pozycję **Konfiguruj**.
4. W okienku Konfiguracja kategorii Funkcje ochrony rodzicielskiej kliknij opcję **Zaawansowane**.

3 W okienku Ustawienia użytkowników, w obszarze **Konta użytkowników McAfee**, wybierz opcję **Administrator** i kliknij przycisk **Edycja**.

4 W oknie dialogowym Edycja konta użytkownika wpisz nowe hasło w polu **Nowe hasło**, a następnie wprowadź je ponownie w polu **Wprowadź ponownie hasło**.

5 Kliknij przycisk **OK**.

Pobierz hasło administratora McAfee

W przypadku zapomnienia hasła administratora można je odzyskać.

1. Kliknij prawym przyciskiem myszy ikonę programu SecurityCenter  , a następnie kliknij polecenie **Przełącz użytkownika**.
2. Na liście **Nazwa użytkownika** wybierz pozycję **Administrator**, a następnie kliknij przycisk **Nie pamiętam hasła**.
3. W polu **Odpowiedź** wpisz odpowiedź na pytanie zabezpieczające.
4. Kliknij przycisk **Prześlij**.

Filtrowanie potencjalnie niepożądanych obrazów w sieci Web

W zależności od wieku lub dojrzałości użytkownika można filtrować (blokować lub zezwalać) potencjalnie nieodpowiednie obrazy, gdy użytkownik ten przegląda sieć Web. Na przykład można blokować wyświetlanie potencjalnie nieodpowiednich obrazów, gdy dzieci przeglądają sieć Web, ale zezwalać na ich wyświetlanie przez starszych nastolatków i dorosłych domowników. Domyślnie filtrowanie obrazów jest wyłączone dla wszystkich użytkowników w grupie Dorośli, co oznacza, że potencjalnie nieodpowiednie obrazy są wyświetlane, gdy użytkownicy ci przeglądają sieć Web. Więcej informacji o konfigurowaniu grup wiekowych zawiera sekcja *Ustawianie grupy klasyfikacji zawartości* (strona 181).

Filtrowanie potencjalnie niepożądanych obrazów w sieci Web

Domyślnie nowi użytkownicy są dodawani do grupy Dorośli i filtrowanie obrazów jest wyłączone. Aby zablokować wyświetlanie potencjalnie nieodpowiednich obrazów, gdy określony użytkownik przegląda sieć Web, można włączyć filtrowanie obrazów. Każdy potencjalnie nieodpowiedni obraz jest automatycznie zastępowany statycznym obrazem McAfee.

1 Otwórz okienko Ustawienia użytkowników.

Jak to zrobić?

1. W okienku Początek programu SecurityCenter kliknij kategorię **Funkcje ochrony rodzicielskiej**.
2. W sekcji informacji kategorii Funkcje ochrony rodzicielskiej kliknij pozycję **Konfiguruj**.
3. W okienku Konfiguracja kategorii Funkcje ochrony rodzicielskiej kliknij opcję **Zaawansowane**.
4. W okienku Funkcje ochrony rodzicielskiej kliknij **Ustawienia użytkowników**.

2 W okienku Ustawienia użytkowników kliknij nazwę użytkownika, a następnie kliknij przycisk **Edytuj**.

3 W oknie Edycja konta użytkownika, w obszarze **Filtrowanie obrazów**, kliknij **Wł**.

4 Kliknij przycisk **OK**.

Ustawianie grupy klasyfikacji zawartości

Użytkownik może należeć do jednej z następujących grup klasyfikacji zawartości:

- Młodsze dziecko
- Dziecko
- Młodszy nastolatek
- Starszy nastolatek
- Osoba dorosła

Program Privacy Service klasyfikuje zawartość sieci Web (blokuje ją lub zezwala na dostęp do niej) z uwzględnieniem grupy, do której należy użytkownik. Pozwala to blokować niektórym domownikom dostęp do określonych witryn sieci Web lub zezwalać im na dostęp do nich. Można np. zablokować daną witrynę sieci Web w przypadku użytkowników, którzy należą do grupy Młodsze dziecko, ale zezwolić na dostęp do niej użytkownikom należącym do grupy Młodszy nastolatek. Aby precyzyjniej klasyfikować zawartość dostępną dla użytkownika, można zezwolić mu na wyświetlanie tylko tych witryn sieci Web, które są dozwolone na liście **Filtrowane witryny sieci Web**. Aby uzyskać więcej informacji, zobacz *Filtrowanie witryn sieci Web* (strona 184).

Nowy użytkownik jest domyślnie dodawany do grupy Osoba dorosła, co umożliwia mu dostęp do pełnej zawartości sieci Web.

Ustawianie grupy klasyfikacji zawartości użytkownika

Nowy użytkownik jest domyślnie dodawany do grupy Osoba dorosła, co umożliwia mu dostęp do pełnej zawartości sieci Web. Później można zmienić grupę klasyfikacji zawartości użytkownika odpowiednio do jego wieku i poziomu dojrzałości.

1 Otwórz okienko Ustawienia użytkowników.

Jak to zrobić?

1. W okienku Początek programu SecurityCenter kliknij kategorię **Funkcje ochrony rodzicielskiej**.
2. W sekcji informacji kategorii Funkcje ochrony rodzicielskiej kliknij pozycję **Konfiguruj**.
3. W okienku Konfiguracja kategorii Funkcje ochrony rodzicielskiej kliknij opcję **Zaawansowane**.
4. W okienku Funkcje ochrony rodzicielskiej kliknij **Ustawienia użytkowników**.

2 W okienku Ustawienia użytkowników kliknij nazwę użytkownika, a następnie kliknij przycisk **Edytuj**.

3 W oknie Edytuj konto użytkownika w obszarze **Klasyfikacja zawartości** kliknij grupę wiekową, do której chcesz przydzielić użytkownika.

Aby uniemożliwić użytkownikowi przeglądanie witryn sieci Web, które są zablokowane na liście **Filtrowane witryny sieci Web**, zaznacz pole wyboru **Ten użytkownik ma dostęp tylko do witryn z listy Dozwolone witryny sieci Web**.

4 Kliknij przycisk **OK**.

Ustawianie ograniczeń czasu przeglądania witryn sieci Web

W przypadku zaniepokojenia nieodpowiedzialnym lub nadmiernym korzystaniem z Internetu przez dzieci można ustawić dla nich właściwe ograniczenia czasu przeglądania sieci Web. Po wprowadzeniu określonych ograniczeń przeglądania sieci Web można mieć pewność, że program SecurityCenter będzie je egzekwował — nawet jeśli dzieci pozostaną same w domu.

Domyślnie dziecko może przeglądać sieć Web przez całą dobę, siedem dni w tygodniu. Można jednak ograniczyć wyświetlanie witryn sieci Web do określonych godzin lub dni albo zabronić go całkowicie. Jeśli dziecko podejmie próbę przeglądania sieci Web w zabronionym okresie, oprogramowanie McAfee wyświetli powiadomienie o ograniczeniu. Po całkowitym zabronieniu przeglądania sieci Web dziecko może się wprawdzie zalogować na komputerze i korzystać z innych programów internetowych, np. poczty e-mail, komunikatorów internetowych, serwerów FTP, gier itd., ale nie może wyświetlać witryn sieci Web.

Ustawianie ograniczeń czasu przeglądania witryn sieci Web

Siatka ograniczeń czasu przeglądania sieci Web pozwala ograniczyć dziecku wyświetlanie witryn sieci Web do określonych dni i godzin.

1 Otwórz okienko Ustawienia użytkowników.

Jak to zrobić?

1. W okienku Początek programu SecurityCenter kliknij kategorię **Funkcje ochrony rodzicielskiej**.
2. W sekcji informacji kategorii Funkcje ochrony rodzicielskiej kliknij pozycję **Konfiguruj**.
3. W okienku Konfiguracja kategorii Funkcje ochrony rodzicielskiej kliknij opcję **Zaawansowane**.
4. W okienku Funkcje ochrony rodzicielskiej kliknij **Ustawienia użytkowników**.

2 W okienku Ustawienia użytkowników kliknij nazwę użytkownika, a następnie kliknij przycisk **Edytuj**.

3 W oknie Edytuj konto użytkownika w obszarze **Ograniczenia czasu dostępu do Internetu** określ za pomocą myszy dni i godziny, w których użytkownik nie może przeglądać sieci Web.

4 Kliknij przycisk **OK**.

Filtrowane witryn sieci Web

Można filtrować witryny sieci Web (blokować je lub zezwalać na dostęp do nich) dla wszystkich użytkowników z wyjątkiem należących do grupy Osoba dorosła. Daną witrynę sieci Web można zablokować, aby uniemożliwić dzieciom wyświetlanie jej podczas przeglądania sieci Web. Gdy dziecko spróbuje uzyskać dostęp do zablokowanej witryny sieci Web, zostanie wyświetlony komunikat informujący o braku możliwości uzyskania dostępu do witryny z powodu zablokowania jej przez program McAfee.

Istnieje możliwość zezwolenia dzieciom na dostęp do danej witryny sieci Web nawet, jeśli została domyślnie zablokowania przez program McAfee. Aby uzyskać więcej informacji na temat witryn sieci Web, które program McAfee blokuje domyślnie, zobacz *Filtrowanie witryn sieci Web z użyciem słów kluczowych* (strona 187). Można ponadto w dowolnym czasie aktualizować i usuwać filtrowane witryny sieci Web.

Uwaga: Użytkownicy (w tym administratorzy), którzy należą do grupy Osoba dorosła, mają dostęp do wszystkich witryn sieci Web, nawet tych zablokowanych. Aby przetestować blokowanie witryn sieci Web, należy zalogować się jako inny użytkownik niż osoba dorosła.

Blokowanie witryny sieci Web

Daną witrynę sieci Web można zablokować, aby uniemożliwić dzieciom wyświetlanie jej podczas przeglądania sieci Web. Gdy dziecko spróbuje uzyskać dostęp do zablokowanej witryny sieci Web, zostanie wyświetlony komunikat informujący o braku możliwości uzyskania dostępu do witryny z powodu zablokowania jej przez program McAfee.

1 Otwórz okienko Funkcje ochrony rodzicielskiej.

Jak to zrobić?

1. W okienku Początek programu SecurityCenter kliknij kategorię **Funkcje ochrony rodzicielskiej**.
2. W sekcji informacji kategorii Funkcje ochrony rodzicielskiej kliknij pozycję **Konfiguruj**.
3. W okienku Konfiguracja kategorii Funkcje ochrony rodzicielskiej sprawdź, czy włączono funkcję kontroli rodzicielskiej, a następnie kliknij przycisk **Zaawansowane**.

2 W okienku Funkcje ochrony rodzicielskiej kliknij przycisk **Filtrowane witryny sieci Web**.

3 W okienku Filtrowane witryny sieci Web wpisz adres witryny sieci Web w polu **http://**, a następnie kliknij przycisk **Zablokuj**.

4 Kliknij przycisk **OK**.

Wskazówka: Można zablokować dozwoloną uprzednio witrynę sieci Web, klikając jej adres na liście **Filtrowane witryny sieci Web**, a następnie klikając przycisk **Zablokuj**.

Zezwalanie na korzystanie z danej witryny sieci Web

Daną witrynę sieci Web można ustawić jako dozwoloną, co zapewni, że nie będzie ona blokowana dla żadnego użytkownika. Po ustawieniu jako dozwolonej witryny sieci Web, która została zablokowana domyślnie przez program McAfee, ustawienie domyślne zostaje zastąpione.

1 Otwórz okienko Funkcje ochrony rodzicielskiej.

Jak to zrobić?

1. W okienku Początek programu SecurityCenter kliknij kategorię **Funkcje ochrony rodzicielskiej**.
2. W sekcji informacji kategorii Funkcje ochrony rodzicielskiej kliknij pozycję **Konfiguruj**.
3. W okienku Konfiguracja kategorii Funkcje ochrony rodzicielskiej sprawdź, czy włączono funkcję kontroli rodzicielskiej, a następnie kliknij przycisk **Zaawansowane**.

2 W okienku Funkcje ochrony rodzicielskiej kliknij przycisk **Filtrowane witryny sieci Web**.

3 W okienku Filtrowane witryny sieci Web wpisz adres witryny sieci Web w polu **http://**, a następnie kliknij przycisk **Zezwalaj**.

4 Kliknij przycisk **OK**.

Wskazówka: Zablokowaną uprzednio witrynę sieci Web można ustawić jako dozwoloną, klikając jej adres na liście **Filtrowane witryny sieci Web**, a następnie klikając przycisk **Zezwalaj**.

Aktualizowanie filtrowanej witryny sieci Web

Jeśli adres danej sieci Web uległ zmianie lub został wpisany nieprawidłowo przy blokowaniu jej lub zezwalaniu na dostęp do niej, można ją zaktualizować.

1. Otwórz okienko Funkcje ochrony rodzicielskiej.

   Jak to zrobić?

   1. W okienku Początek programu SecurityCenter kliknij kategorię **Funkcje ochrony rodzicielskiej**.
   2. W sekcji informacji kategorii Funkcje ochrony rodzicielskiej kliknij pozycję **Konfiguruj**.
   3. W okienku Konfiguracja kategorii Funkcje ochrony rodzicielskiej sprawdź, czy włączono funkcję kontroli rodzicielskiej, a następnie kliknij przycisk **Zaawansowane**.

2. W okienku Funkcje ochrony rodzicielskiej kliknij przycisk **Filtrowane witryny sieci Web**.
3. W okienku Filtrowane witryny sieci Web kliknij pozycję na liście **Filtrowane witryny sieci Web**, zmień adres witryny sieci Web w polu **http://**, a następnie kliknij przycisk **Aktualizuj**.
4. Kliknij przycisk **OK**.

Usuwanie filtrowanej witryny sieci Web

Filtrowaną witrynę sieci Web można usunąć, jeśli nie ma już potrzeby blokowania jej ani zezwalania na dostęp do niej.

1. Otwórz okienko Funkcje ochrony rodzicielskiej.

   Jak to zrobić?

   1. W okienku Początek programu SecurityCenter kliknij kategorię **Funkcje ochrony rodzicielskiej**.
   2. W sekcji informacji kategorii Funkcje ochrony rodzicielskiej kliknij pozycję **Konfiguruj**.
   3. W okienku Konfiguracja kategorii Funkcje ochrony rodzicielskiej sprawdź, czy włączono funkcję kontroli rodzicielskiej, a następnie kliknij przycisk **Zaawansowane**.

2. W okienku Funkcje ochrony rodzicielskiej kliknij przycisk **Filtrowane witryny sieci Web**.
3. W okienku Filtrowane witryny sieci Web kliknij pozycję na liście **Filtrowane witryny sieci Web**, a następnie kliknij przycisk **Usuń**.
4. Kliknij przycisk **OK**.

Filtrowanie witryn sieci Web z użyciem słów kluczowych

Filtrowanie na podstawie słów kluczowych pozwala blokować użytkownikom, którzy nie są osobami dorosłymi, przeglądanie witryn sieci Web zawierających potencjalnie nieodpowiednie dla nich słowa. Po włączeniu filtrowania na podstawie słów kluczowych domyślna lista słów kluczowych i odpowiednie reguły służą do klasyfikowania zawartości dla użytkowników odpowiednio do ich grupy klasyfikacji zawartości. Użytkownicy muszą należeć do określonej grupy, aby uzyskać dostęp do witryn sieci Web zawierających wybrane słowa kluczowe. Na przykład tylko członkowie grupy Osoba dorosła mogą przeglądać witryny sieci Web zawierające słowo *porno*, a tylko członkowie grupy Dziecko (lub użytkownicy należący do starszych grup wiekowych) mogą przeglądać witryny sieci Web zawierające słowo *leki*.

Można ponadto dodawać własne słowa kluczowe do domyślnej listy i przypisywać je do konkretnych grup klasyfikacji zawartości. Dodawane reguły dotyczące słów kluczowych zastępują reguły, które mogą być już przypisane do odpowiednich słów kluczowych znajdujących się na domyślnej liście.

Wyłączanie filtrowania na podstawie słów kluczowych

Filtrowanie na podstawie słów kluczowych jest domyślnie włączone, co oznacza, że domyślna lista słów kluczowych i odpowiednie reguły służą do klasyfikowania zawartości dla użytkowników odpowiednio do ich grupy klasyfikacji zawartości. Filtrowanie na podstawie słów kluczowych można wyłączyć w dowolnej chwili, chociaż firma McAfee nie zaleca takiego postępowania.

1. Otwórz okienko Funkcje ochrony rodzicielskiej.

   Jak to zrobić?

   1. W okienku Początek programu SecurityCenter kliknij kategorię **Funkcje ochrony rodzicielskiej**.
   2. W sekcji informacji kategorii Funkcje ochrony rodzicielskiej kliknij pozycję **Konfiguruj**.
   3. W okienku Konfiguracja kategorii Funkcje ochrony rodzicielskiej sprawdź, czy włączono funkcję kontroli rodzicielskiej, a następnie kliknij przycisk **Zaawansowane**.

2. W okienku Funkcje ochrony rodzicielskiej kliknij przycisk **Słowa kluczowe**.
3. W okienku Słowa kluczowe kliknij przycisk **Wyłącz**.
4. Kliknij przycisk **OK**.

Blokowanie witryn sieci Web na podstawie słów kluczowych

Aby blokować witryny sieci Web ze względu na ich nieodpowiednią zawartość w przypadku, gdy adresy konkretnych witryn nie są znane, można blokować je na podstawie słów kluczowych. Wystarczy wpisać słowo kluczowe, a następnie określić grupy klasyfikacji zawartości, które mogą przeglądać witryny sieci Web zawierające to słowo.

1 Otwórz okienko Funkcje ochrony rodzicielskiej.

Jak to zrobić?

1. W okienku Początek programu SecurityCenter kliknij kategorię **Funkcje ochrony rodzicielskiej**.
2. W sekcji informacji kategorii Funkcje ochrony rodzicielskiej kliknij pozycję **Konfiguruj**.
3. W okienku Konfiguracja kategorii Funkcje ochrony rodzicielskiej sprawdź, czy włączono funkcję kontroli rodzicielskiej, a następnie kliknij przycisk **Zaawansowane**.

2 W okienku Funkcje ochrony rodzicielskiej kliknij przycisk **Słowa kluczowe** i upewnij się, że jest włączone filtrowanie na podstawie słów kluczowych.

3 W obszarze **Lista słów kluczowych** wpisz słowo kluczowe w polu **Szukaj**.

4 Przesuń suwak **Minimalny wiek**, aby określić grupę minimalnego wieku.
Użytkownicy z tej grupy wiekowej i z grup starszych mogą przeglądać witryny sieci Web zawierające słowo kluczowe.

5 Kliknij przycisk **OK**.

ROZDZIAŁ 32

Ochrona informacji w sieci Web

Podczas przeglądania sieci Web można chronić swoje prywatne dane i pliki, blokując informacje. Można np. uniemożliwić przesyłanie przez sieć Web danych osobistych (takich jak: nazwisko, adres, numery kart kredytowych i numery kont bankowych), dodając je do obszaru zablokowanych informacji.

Uwaga: Program Privacy Service nie blokuje przesyłania danych osobistych za pośrednictwem bezpiecznych witryn sieci Web (czyli korzystających z protokołu https://), np. witryn bankowości internetowej.

W tym rozdziale

Ochrona informacji osobistych

Należy chronić informacje osobiste (takie jak nazwisko, adres, numery kart kredytowych i numery kont bankowych) przed przesyłaniem ich przez sieć Web poprzez blokowanie ich. Jeśli program McAfee wykryje informacje osobiste zawarte w jakimś elemencie (np. w polu formularza lub w pliku), które mają zostać przesłane przez sieć Web, wykonywane są następujące czynności:

- Jeśli użytkownik jest administratorem, musi potwierdzić wysłanie informacji.
- Jeśli użytkownik nie jest administratorem, blokowana część informacji zostanie zastąpiona gwiazdkami (*). Jeśli np. szkodliwa witryna sieci Web podejmie próbę wysłania numeru karty kredytowej użytkownika do innego komputera, numer ten zostanie zastąpiony gwiazdkami.

Ochrona informacji osobistych

Można zablokować następujące informacje osobiste: nazwisko, adres, kod pocztowy, informacje o ubezpieczeniu społecznym, numer telefonu, numery kart kredytowych, numery kont bankowych, rachunki maklerskie i karty telefoniczne. Aby zablokować informacje osobiste innego typu, można ustawić typ jako **inne**.

1 Otwórz okienko Chronione informacje.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij kategorię **Internet i sieć**.
3. W sekcji informacji kategorii Internet i sieć kliknij opcję **Konfiguruj**.
4. Upewnij się, że w okienku Konfiguracja kategorii Internet i sieć włączona jest ochrona informacji osobistych, a następnie kliknij przycisk **Zaawansowane**.

2 W okienku Chronione informacje kliknij przycisk **Dodaj**.

3 Wybierz na liście typ informacji, który chcesz zablokować.

4 Wprowadź informacje osobiste, a następnie kliknij przycisk **OK**.

ROZDZIAŁ 33

Ochrona haseł

Magazyn haseł jest bezpiecznym obszarem przechowywania osobistych haseł. Umożliwia przechowywanie haseł, gwarantując, że żaden inny użytkownik (nawet administrator) nie ma do nich dostępu.

W tym rozdziale

Konfigurowanie Magazynu haseł

Przed rozpoczęciem korzystania z Magazynu haseł należy ustawić hasło do Magazynu haseł. Tylko użytkownicy, którzy je znają, mogą uzyskać dostęp do Magazynu haseł. Jeśli użytkownik zapomni to hasło, można je zresetować; jednak wszystkie hasła zapisane wcześniej w Magazynie haseł zostaną usunięte.

Po skonfigurowaniu hasła do Magazynu haseł można dodawać, edytować lub usuwać hasła z magazynu. Można również w dowolnym czasie zmienić hasło do Magazynu haseł.

Dodawanie hasła

W razie problemów z zapamiętaniem haseł można je dodać do Magazynu haseł. Magazyn haseł jest bezpiecznym miejscem dostępnym dla użytkowników znających hasło do Magazynu haseł.

1 Otwórz okienko Magazyn haseł.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij kategorię **Internet i sieć**.
3. W sekcji informacji kategorii Internet i sieć kliknij opcję **Konfiguruj**.
4. W okienku Konfiguracja kategorii Internet i sieć kliknij przycisk **Zaawansowane** w obszarze **Magazyn haseł**.

2 Wpisz hasło do Magazynu haseł w polu **Hasło**, a następnie wpisz je ponownie w polu **Wprowadź ponownie hasło**.

3 Kliknij przycisk **Otwórz**.

4 W okienku Zarządzanie magazynem haseł kliknij przycisk **Dodaj**.

5 W polu **Opis** wpisz opis hasła (na przykład do czego służy), a następnie w polu **Hasło** wpisz hasło.

6 Kliknij przycisk **OK**.

Modyfikowanie hasła

Aby pozycje w Magazynie haseł zawsze były aktualne i niezawodne, należy je aktualizować wraz ze zmianą haseł.

1 Otwórz okienko Magazyn haseł.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij kategorię **Internet i sieć**.
3. W sekcji informacji kategorii Internet i sieć kliknij opcję **Konfiguruj**.
4. W okienku Konfiguracja kategorii Internet i sieć kliknij przycisk **Zaawansowane** w obszarze **Magazyn haseł**.

2 W polu **Hasło** wpisz hasło do Magazynu haseł.

3 Kliknij przycisk **Otwórz**.

4 W okienku Zarządzanie magazynem haseł kliknij pozycję hasła, a następnie kliknij przycisk **Edytuj**.

5 W polu **Opis** zmień opis hasła (wpisując na przykład do czego służy) lub zmień hasło w polu **Hasło**.

6 Kliknij przycisk **OK**.

Usuwanie hasła

W każdej chwili można usunąć hasło z Magazynu haseł. Nie można odtworzyć hasła usuniętego z magazynu haseł.

1 Otwórz okienko Magazyn haseł.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij kategorię **Internet i sieć**.
3. W sekcji informacji kategorii Internet i sieć kliknij opcję **Konfiguruj**.
4. W okienku Konfiguracja kategorii Internet i sieć kliknij przycisk **Zaawansowane** w obszarze **Magazyn haseł**.

2 W polu **Hasło** wpisz hasło do Magazynu haseł.

3 Kliknij przycisk **Otwórz**.

4 W okienku Zarządzanie magazynem haseł kliknij pozycję hasła, a następnie kliknij przycisk **Usuń**.

5 W oknie dialogowym Potwierdzenie usunięcia kliknij przycisk **Tak**.

Zmiana hasła do Magazynu haseł

Hasło do Magazynu haseł można zmienić w dowolnym czasie.

1 Otwórz okienko Magazyn haseł.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij kategorię **Internet i sieć**.
3. W sekcji informacji kategorii Internet i sieć kliknij opcję **Konfiguruj**.
4. W okienku Konfiguracja kategorii Internet i sieć kliknij przycisk **Zaawansowane** w obszarze **Magazyn haseł**.

2 W okienku Magazyn haseł wpisz swoje obecne hasło w polu **Hasło**, a następnie kliknij przycisk **Otwórz**.

3 W okienku Zarządzanie magazynem haseł kliknij przycisk **Zmień hasło**.

4 Wprowadź nowe hasło w polu **Wybierz hasło**, a następnie wprowadź je ponownie w polu **Wprowadź ponownie hasło**.

5 Kliknij przycisk **OK**.

6 W oknie dialogowym Hasło do magazynu haseł zostało zmienione kliknij przycisk **OK**.

Resetowanie hasła do Magazynu haseł

W przypadku zapomnienia hasła do Magazynu haseł można je zresetować; jednak wszystkie wprowadzone wcześniej hasła zostaną usunięte.

1 Otwórz okienko Magazyn haseł.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij kategorię **Internet i sieć**.
3. W sekcji informacji kategorii Internet i sieć kliknij opcję **Konfiguruj**.
4. W okienku Konfiguracja kategorii Internet i sieć kliknij przycisk **Zaawansowane** w obszarze **Magazyn haseł**.

2 W obszarze **Resetowanie hasła do magazynu** wpisz nowe hasło w polu **Hasło**, a następnie wpisz je ponownie w polu **Wprowadź ponownie hasło**.

3 Kliknij opcję **Resetuj**.

4 W oknie dialogowym Potwierdzenie resetowania hasła kliknij opcję **Tak**.

ROZDZIAŁ 34

McAfee Data Backup

Programu Data Backup należy używać, aby zapobiec przypadkowej utracie danych, archiwizując pliki i foldery na dysku CD, DVD, USB, zewnętrznym dysku twardym lub dysku sieciowym. Archiwizacja lokalna pozwala na zarchiwizowanie (utworzenie kopii zapasowych) osobistych danych na dysku CD, DVD, USB, zewnętrznym dysku twardym lub dysku sieciowym. Dostarcza to użytkownikowi lokalne kopie jego danych, dokumentów i innych materiałów osobistych na wypadek ich przypadkowej utraty.

Przed przystąpieniem do użytkowania programu Data Backup można zapoznać się z jego niektórymi najczęściej używanymi funkcjami. Szczegółowe informacje na temat konfigurowania tych funkcji i korzystania z nich zamieszczono w pomocy programu Data Backup. Po przejrzeniu funkcji programu, należy upewnić się, że dostępne są odpowiednie nośniki do przeprowadzania lokalnych archiwizacji.

W tym rozdziale

Funkcje

Program Data Backup pozwala na zapisywanie i przywracanie plików z fotografiami, muzyką i innymi ważnymi informacjami.

Planowana lokalna archiwizacja danych

Zabezpiecz dane, archiwizując pliki i foldery na dysku CD, DVD, USB, zewnętrznym dysku twardym lub dysku sieciowym. Po zainicjowaniu pierwszej archiwizacji archiwizacja przyrostowa będzie później wykonywana automatycznie.

Przywracanie za pomocą jednego kliknięcia

W razie omyłkowego skasowania lub uszkodzenia plików lub folderów na komputerze, można przywrócić ich ostatnie wersje z używanych nośników archiwum.

Kompresja i szyfrowanie

Domyślnie archiwizowane pliki są kompresowane, dzięki czemu oszczędza się miejsce na nośniku. Dodatkowe zabezpieczenie archiwum zapewnia jego szyfrowanie (opcja domyślna).

ROZDZIAŁ 35

Archiwizowanie plików

Programu McAfee Data Backup można użyć w celu archiwizowania kopii plików z komputera na dysku CD, DVD, USB, zewnętrznym dysku twardym lub dysku sieciowym. Archiwizowanie plików w ten sposób pozwala na łatwe odzyskanie informacji na wypadek przypadkowej utraty danych lub ich uszkodzenia.

Przed rozpoczęciem archiwizowania plików należy wybrać domyślną lokalizację archiwum (dysk CD, DVD, USB, zewnętrzny dysk twardy lub dysk sieciowy). Firma McAfee skonfigurowała wcześniej część innych ustawień, na przykład foldery i typy plików, które mają być archiwizowane — można jednak zmienić te ustawienia.

Po skonfigurowaniu opcji archiwum lokalnego można zmienić domyślne ustawienia mówiące o tym, jak często program Data Backup ma przeprowadzać pełną lub szybką archiwizację. Archiwizowanie ręczne można uruchomić w dowolnym momencie.

W tym rozdziale

Konfigurowanie opcji archiwizowania

Przed rozpoczęciem archiwizowania danych należy skonfigurować pewne opcje archiwum lokalnego. Na przykład trzeba skonfigurować monitorowane lokalizacje i typy plików. Monitorowane lokalizacje to foldery w komputerze, które program Data Backup monitoruje pod kątem pojawienia się nowych plików lub zmian w plikach. Monitorowane typy plików to typy plików (na przykład .doc, .xls itd.) znajdujące się w lokalizacjach monitorowanych, które program Data Backup archiwizuje. Domyślnie program Data Backup monitoruje wszystkie typy plików przechowywanych w monitorowanych lokalizacjach.

Można skonfigurować dwa typy monitorowanych lokalizacji: lokalizacje monitorowane dokładnie i lokalizacje monitorowane częściowo. Po skonfigurowaniu lokalizacji monitorowanej dokładnie program Data Backup archiwizuje wszystkie pliki monitorowanych typów znajdujące się w tym folderze i jego podfolderach. Po skonfigurowaniu lokalizacji monitorowanej częściowo program Data Backup archiwizuje wszystkie pliki monitorowanych typów znajdujące się tylko w tym folderze (nie w jego podfolderach). Można również określić lokalizacje, które mają być wyłączone z lokalnego archiwum. Domyślnie pulpit systemu Windows oraz folder Moje dokumenty skonfigurowane są jako lokalizacje monitorowane dokładnie.

Po skonfigurowaniu typów monitorowanych plików i lokalizacji, należy skonfigurować lokalizację archiwum (czyli dysk CD, DVD, USB, zewnętrzny dysk twardy lub dysk sieciowy, na których będą magazynowane dane poddane archiwizacji). Lokalizację archiwum można zmienić w dowolnym momencie.

Z powodów związanych z bezpieczeństwem lub rozmiarami archiwum, dla archiwizowanych plików domyślnie włączone są opcje szyfrowania i kompresji. Zawartość szyfrowanych plików jest zamieniana z tekstu na kod, mający na celu uniemożliwienie odczytania informacji przez osoby nieznające metody jego odszyfrowania. Kompresowane pliki są kompresowane do postaci, która minimalizuje przestrzeń wymaganą do ich przechowywania lub przesyłania. Pomimo, że firma McAfee tego nie zaleca, można w dowolnym momencie wyłączyć szyfrowanie lub kompresję.

Zawieranie lokalizacji w archiwum

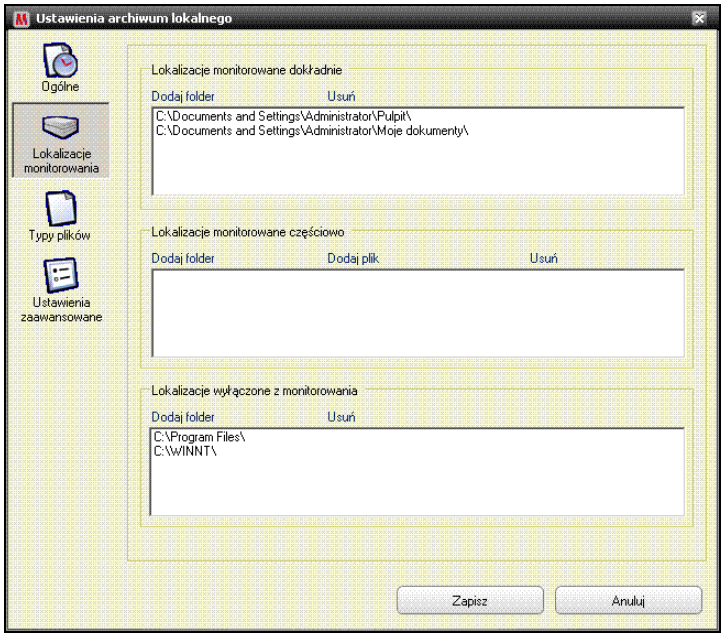
Można skonfigurować dwa typy monitorowanych lokalizacji, które będą poddane archiwizacji: dokładny i częściowy. Po skonfigurowaniu lokalizacji monitorowanej dokładnie program Data Backup monitoruje zawartość folderu oraz jego podfolderów pod kątem zmian. Po skonfigurowaniu lokalizacji monitorowanej częściowo program Data Backup monitoruje tylko zawartość folderu (nie jego podfolderów).

Aby zawrzeć lokalizację w archiwum:

1 Kliknij kartę **Archiwum lokalne**.

2 W okienku po lewej stronie kliknij przycisk **Ustawienia**.

3 W oknie dialogowym Ustawienia archiwum lokalnego kliknij przycisk **Lokalizacje monitorowania**.



4 Wykonaj jedną z poniższych czynności:

- Aby archiwizować zawartość folderu razem z zawartością jego podfolderów kliknij przycisk **Dodaj folder** w polu **Lokalizacje monitorowane dokładnie**.
- Aby archiwizować zawartość folderu, ale nie jego podfolderów, kliknij przycisk **Dodaj folder** w polu **Lokalizacje monitorowane częściowo**.

5 W oknie dialogowym Przeglądanie w poszukiwaniu folderu przejdź do folderu, który chcesz monitorować, a następnie kliknij przycisk **OK**.

6 Kliknij przycisk **Zapisz**.

Wskazówka: Jeśli program Data Backup ma monitorować folder, który nie został jeszcze utworzony, można kliknąć przycisk **Utwórz nowy folder** w oknie dialogowym Przeglądanie w poszukiwaniu folderu, aby dodać folder i jednocześnie skonfigurować go jako monitorowaną lokalizację.

Konfiguracja typów archiwizowanych plików

Można określić, jakie typy plików mają być archiwizowane w lokalizacjach monitorowanych dokładnie lub częściowo. Można wybrać z istniejącej listy typów plików lub dodać do niej nowy typ.

Aby skonfigurować archiwizowane typy plików:

1 Kliknij kartę **Archiwum lokalne**.

2 W okienku po lewej stronie kliknij przycisk **Ustawienia**.

3 W oknie dialogowym Ustawienia archiwum lokalnego kliknij przycisk **Typy plików**.

4 Rozwiń listę typów plików i zaznacz pola wyboru przy typach plików, które mają być archiwizowane.

5 Kliknij przycisk **Zapisz**.

Wskazówka: Aby dodać nowy typ plików do listy **Selected File Types** (Wybrane typy plików) wpisz rozszerzenie pliku w polu **Dodaj niestandardowy typ pliku do grupy „Inne”**, a następnie kliknij przycisk **Dodaj**. Nowy typ plików automatycznie staje się typem monitorowanym.

Wykluczenie lokalizacji z archiwum

Lokalizację wyklucza się z archiwum, jeśli nie chcemy tej lokalizacji (folderu) i jej zawartości archiwizować.

Aby wykluczyć lokalizację z archiwum:

1. Kliknij kartę **Archiwum lokalne**.
2. W okienku po lewej stronie kliknij przycisk **Ustawienia**.
3. W oknie dialogowym Ustawienia archiwum lokalnego kliknij przycisk **Watch Folders** (Monitorowane foldery).
4. Kliknij przycisk **Dodaj folder** w kategorii **Lokalizacje wyłączone z monitorowania**.
5. W oknie dialogowym Przeglądanie w poszukiwaniu folderu przejdź do folderu, który chcesz wyłączyć z monitorowania, wybierz go, a następnie kliknij przycisk **OK**.
6. Kliknij przycisk **Zapisz**.

Wskazówka: Jeśli program Data Backup ma wyłączyć z monitorowania folder, który nie został jeszcze utworzony, można kliknąć przycisk **Utwórz nowy folder** w oknie dialogowym Przeglądanie w poszukiwaniu folderu, aby dodać folder i jednocześnie wyłączyć go z monitorowania.

Zmiana lokalizacji archiwum

Gdy lokalizacja archiwum zostanie zmieniona, pliki archiwizowane wcześniej w innej lokalizacji będą oznaczone jako *Nigdy nie archiwizowano*.

Aby zmienić lokalizację archiwum:

1. Kliknij kartę **Archiwum lokalne**.
2. W okienku po lewej stronie kliknij przycisk **Ustawienia**.
3. Kliknij przycisk **Zmień lokalizację archiwum**.
4. W oknie dialogowym Lokalizacja archiwum wykonaj jedną z poniższych czynności:
   - Kliknij przycisk **Wybierz nagrywarkę CD/DVD**, na liście **Nagrywarka** kliknij znajdujący się w komputerze napęd CD lub DVD, a następnie kliknij przycisk **Zapisz**.
   - Kliknij przycisk **Wybierz lokalizację dysku**, przejdź do dysku USB, dysku lokalnego lub zewnętrznego dysku twardego, wybierz go, a następnie kliknij przycisk **OK**.
   - Kliknij przycisk **Wybierz lokalizację sieciową**, przejdź do folderu sieciowego, zaznacz go, a następnie kliknij przycisk **OK**.

5 Potwierdź nową lokalizację archiwum w polu **Wybrana lokalizacja archiwum**, a następnie kliknij przycisk **OK**.

6 W oknie dialogowym potwierdzenia kliknij przycisk **OK**.

7 Kliknij przycisk **Zapisz**.

Wyłączanie szyfrowania i kompresowania archiwum

Szyfrowanie archiwizowanych plików chroni poufność danych użytkownika, zmieniając zawartość plików tak, że stają się one nie do odczytania. Kompresowanie archiwizowanych plików pomaga zminimalizować ich rozmiar. Domyślnie zarówno szyfrowanie, jak i kompresowanie, są włączone; jednakże w dowolnej chwili można te opcje wyłączyć.

Aby wyłączyć szyfrowanie i kompresowanie archiwum:

1 Kliknij kartę **Archiwum lokalne**.

2 W okienku po lewej stronie kliknij przycisk **Ustawienia**.

3 W oknie dialogowym Ustawienia archiwum lokalnego kliknij przycisk **Ustawienia zaawansowane**.

4 Usuń zaznaczenie pola wyboru **Włącz szyfrowanie w celu zwiększenia bezpieczeństwa**.

5 Usuń zaznaczenie pola wyboru **Włącz kompresję w celu zmniejszenia ilości zajmowanego miejsca**.

6 Kliknij przycisk **Zapisz**.

Uwaga: Firma McAfee zaleca niewyłączanie szyfrowania i kompresowania podczas archiwizowania plików.

Przeprowadzanie pełnych i szybkich archiwizacji

Można przeprowadzić dwa typy archiwizacji: pełną lub szybką. Podczas przeprowadzania archiwizacji pełnej, archiwizowany jest pełen zestaw danych w zależności od skonfigurowanych monitorowanych typów plików i lokalizacji. Podczas przeprowadzania archiwizacji szybkiej, archiwizowane są tylko te monitorowane pliki, które uległy zmianie od ostatniej pełnej lub szybkiej archiwizacji.

Domyślnie program Data Backup ma zaplanowane przeprowadzanie pełnej archiwizacji monitorowanych typów plików w monitorowanych lokalizacjach w każdy poniedziałek o godzinie 9:00, a archiwizacji szybkiej co 48 godzin od ostatniej szybkiej lub pełnej archiwizacji. Ten harmonogram zapewnia utrzymywanie przez cały czas aktualnego archiwum. Jednakże, jeśli archiwizacja nie ma być przeprowadzana co 48 godzin, można ten harmonogram zmienić i dopasować do własnych potrzeb.

W każdej chwili można przeprowadzić archiwizację monitorowanych lokalizacji na żądanie użytkownika. Na przykład jeśli zmieniony został plik, który ma być archiwizowany, ale program Data Backup nie ma zaplanowanego przeprowadzania pełnej lub szybkiej archiwizacji przez najbliższe kilka godzin, można ręcznie archiwizować pliki. Gdy pliki zostaną archiwizowane ręcznie, interwał ustawiony dla automatycznych archiwizacji zostaje wyzerowany.

Można również przerwać archiwizację automatyczną lub ręczną, jeśli będzie miała ona miejsce w nieodpowiednim momencie. Na przykład jeśli użytkownik wykonuje zadanie zużywające dużo zasobów systemowych i rozpocznie się automatyczna archiwizacja, można ją zatrzymać. Gdy archiwizacja automatyczna zostanie zatrzymana, interwał ustawiony dla automatycznych archiwizacji zostaje wyzerowany.

Planowanie automatycznych archiwizacji

Można ustawić częstotliwość dokonywania pełnych i szybkich archiwizacji, aby zapewnić stałą ochronę danych.

Aby zaplanować automatyczne archiwizacje:

1. Kliknij kartę **Archiwum lokalne**.
2. W okienku po lewej stronie kliknij przycisk **Ustawienia**.
3. W oknie dialogowym Ustawienia archiwum lokalnego kliknij przycisk **Ogólne**.
4. Aby przeprowadzić pełną archiwizację co dzień, tydzień lub miesiąc, kliknij jedną z poniższych opcji w polu **Archiwizacja pełna co**:
   - **Dzień**
   - **Tydzień**
   - **Miesiąc**

5 Zaznacz pole wyboru znajdujące się obok dnia, w którym ma być przeprowadzana pełna archiwizacja.

6 Kliknij wartość na liście **O**, aby określić godzinę, o której ma być przeprowadzona pełna archiwizacja.

7 Aby przeprowadzać archiwizację szybką codziennie lub co godzinę, kliknij jedną z poniższych opcji w polu **Archiwizacja szybka**:

- **Godziny**
- **Dni**

8 Wprowadź liczbę oznaczającą częstotliwość w polu **Archiwizacja szybka co**.

9 Kliknij przycisk **Zapisz**.

Przerywanie automatycznej archiwizacji

Program Data Backup automatycznie archiwizuje pliki w monitorowanych lokalizacjach zgodnie ze zdefiniowanym przez użytkownika harmonogramem. Jednakże, jeśli użytkownik chce przerwać trwającą archiwizację, może to zrobić w dowolnym momencie.

Aby przerwać automatyczną archiwizację:

1 W okienku po lewej stronie kliknij łącze **Zatrzymaj archiwizowanie**.

2 W oknie dialogowym potwierdzenia kliknij przycisk **Tak**.

Uwaga: Łącze **Zatrzymaj archiwizowanie** pojawia się tylko wtedy, gdy trwa archiwizacja.

Ręczne przeprowadzanie archiwizacji

Pomimo, że archiwizacje automatyczne przeprowadzane są zgodnie ze zdefiniowanym wcześniej harmonogramem, można przeprowadzić szybką lub pełną archiwizację ręcznie w dowolnym momencie. Podczas przeprowadzania archiwizacji szybkiej, archiwizowane są tylko te pliki, które uległy zmianie od ostatniej pełnej lub szybkiej archiwizacji. Podczas przeprowadzania archiwizacji pełnej archiwizowane są monitorowane typy plików we wszystkich monitorowanych lokalizacjach.

Aby ręcznie przeprowadzić szybką lub pełną archiwizację:

1 Kliknij kartę **Archiwum lokalne**.

2 Aby przeprowadzić archiwizację szybką, kliknij przycisk **Archiwizacja szybka** w okienku po lewej stronie.

3 Aby przeprowadzić archiwizację pełną, kliknij przycisk **Archiwizacja pełna** w okienku po lewej stronie.

4 W oknie dialogowym Program gotowy do rozpoczęcia archiwizowania potwierdź ilość dostępnego miejsca oraz ustawienia, a następnie kliknij przycisk **Kontynuuj**.

ROZDZIAŁ 36

Praca ze zarchiwizowanymi plikami

Po zarchiwizowaniu plików do pracy z nimi można użyć programu Data Backup. Zarchiwizowane pliki prezentowane są w tradycyjnym widoku eksploratora, co pozwala je łatwo zlokalizować. Wraz z rozrastaniem się archiwum użytkownik może chcieć sortować lub wyszukiwać pliki. Można również otwierać pliki bezpośrednio w widoku eksploratora, aby obejrzeć ich zawartość bez potrzeby pobierania plików.

Pliki są pobierane z archiwum, jeśli lokalna kopia danego pliku jest nieaktualna, brakująca lub zostanie uszkodzona. Program Data Backup dostarcza również informacje potrzebne do zarządzania lokalnymi archiwami i nośnikami danych.

W tym rozdziale

Używanie eksploratora archiwum lokalnego

Eksplorator archiwum lokalnego pozwala wyświetlać i manipulować plikami zarchiwizowanymi lokalnie. Dla każdego pliku można wyświetlić jego nazwę, typ, lokalizację, rozmiar, stan (zarchiwizowany, niezarchiwizowany lub archiwizacja w toku) i datę zarchiwizowania pliku. Można również sortować pliki według dowolnego z tych kryteriów.

W przypadku posiadania dużego archiwum można szybko znaleźć plik przez jego wyszukiwanie. Można wyszukiwać plik podając całą lub część jego nazwy lub ścieżki dostępu do niego, następnie można zawęzić wyszukiwanie poprzez podanie przybliżonego rozmiaru pliku i daty jego ostatniej archiwizacji.

Po zlokalizowaniu pliku można go otworzyć bezpośrednio w eksploratorze archiwum lokalnego. Program Data Backup otwiera plik w jego macierzystym programie, pozwalając na wprowadzenie zmian bez opuszczania eksploratora archiwum lokalnego. Plik zostaje zapisany w oryginalnej monitorowanej lokalizacji na komputerze użytkownika i podlega automatycznej archiwizacji zgodnie ze zdefiniowanym przez użytkownika harmonogramem.

Sortowanie zarchiwizowanych plików

Zarchiwizowane pliki i foldery można sortować według poniższych kryteriów: nazwa, typ pliku, rozmiar, stan (czyli zarchiwizowany, niezarchiwizowany lub archiwizacja w toku), data archiwizacji pliku lub lokalizacja plików w komputerze (ścieżka).

Aby posortować zarchiwizowane pliki:

1. Kliknij kartę **Archiwum lokalne**.
2. W okienku po prawej stronie kliknij nazwę kolumny.

Wyszukiwanie zarchiwizowanego pliku

W przypadku posiadania dużego repozytorium zarchiwizowanych plików, można szybko znaleźć plik przez jego wyszukiwanie. Można szukać pliku, podając całą lub część jego nazwy lub ścieżki dostępu do niego, następnie można zawęzić wyszukiwanie poprzez podanie przybliżonego rozmiaru pliku i daty jego ostatniej archiwizacji.

Aby wyszukać zarchiwizowany plik:

1. Wprowadź całą lub część nazwy pliku w polu **Wyszukaj** na górze ekranu, a następnie naciśnij klawisz Enter.
2. Wprowadź pełną lub częściową ścieżkę w polu **Pełna lub częściowa ścieżka**.
3. Określ przybliżony rozmiar wyszukiwanego pliku, wykonując jedną z poniższych czynności:
   - Kliknij opcję **<100 kB**, **<1 MB** lub **>1 MB**.

- Kliknij przycisk **Rozmiar w kB**, a następnie podaj przybliżony rozmiar w odpowiednich polach.

4 Określ przybliżoną datę ostatniej archiwizacji online wyszukiwanego pliku, wykonując jedną z poniższych czynności:

- Kliknij przycisk **W tym tygodniu**, **W tym miesiącu** lub **W tym roku**.
- Kliknij przycisk **Określ daty**, na liście kliknij pole **Zarchiwizowane**, a następnie kliknij odpowiednie wartości daty z listy.

5 Kliknij przycisk **Wyszukaj**.

Uwaga: W przypadku, gdy przybliżony rozmiar pliku lub data jego ostatniej archiwizacji nie są znane, kliknij przycisk **Nieznane**.

Otwieranie zarchiwizowanego pliku

Można zbadać zawartość zarchiwizowanego pliku poprzez otwarcie go bezpośrednio w eksploratorze archiwum lokalnego.

Aby otworzyć zarchiwizowane pliki:

1 Kliknij kartę **Archiwum lokalne**.

2 W okienku po prawej stronie kliknij nazwę pliku, a następnie kliknij przycisk **Otwórz**.

Wskazówka: Zarchiwizowany plik można również otworzyć, klikając dwukrotnie jego nazwę.

Przywracanie zarchiwizowanych plików

Jeśli monitorowany plik zostanie uszkodzony, będzie brakujący lub zostanie omyłkowo usunięty można przywrócić jego kopię z archiwum lokalnego. Z tego powodu ważne jest regularne archiwizowanie plików. Z archiwum lokalnego można również przywrócić starsze wersje plików. Na przykład jeśli dany plik jest regularnie archiwizowany, ale zajdzie potrzeba powrotu do jego poprzedniej wersji, można tego dokonać przez zlokalizowanie pliku w lokalizacji archiwum. Jeśli lokalizacją archiwum jest dysk lokalny lub sieciowy, można je przeglądać w poszukiwaniu pliku. Jeśli lokalizacją archiwum jest zewnętrzny dysk twardy lub dysk USB, należy najpierw podłączyć dysk do komputera i dopiero później przeglądać go w poszukiwaniu pliku. Jeśli lokalizacją archiwum jest dysk CD lub DVD, należy najpierw włożyć dysk CD lub DVD do komputera, a następnie przejrzeć go w poszukiwaniu pliku.

Można również przywracać pliki zarchiwizowane na jednym komputerze z innego komputera. Na przykład jeśli zestaw plików został zarchiwizowany na zewnętrznym dysku twardym w komputerze A, można przywrócić te pliki na komputerze B. Aby to uczynić, należy zainstalować program Data Backup na komputerze B i podłączyć zewnętrzny dysk twardy. Następnie w programie Data Backup należy wykonać przeglądanie w poszukiwaniu plików i zostaną one dodane do listy **Brakujące pliki**, skąd można je przywrócić.

Więcej informacji na temat archiwizowania plików można znaleźć w sekcji Archiwizowanie plików. Jeśli monitorowany plik zostanie celowo usunięty z archiwum, można również usunąć jego wpis z listy **Brakujące pliki**.

Przywracanie brakujących plików z archiwum lokalnego

Archiwum lokalne programu Data Backup pozwala na odzyskanie brakujących danych z monitorowanego folderu na komputerze lokalnym. Na przykład jeśli plik przeniesiono lub usunięto z monitorowanego folderu, a został on już zarchiwizowany, można go przywrócić z archiwum lokalnego.

Aby przywrócić brakujący plik z archiwum lokalnego:

1. Kliknij kartę **Archiwum lokalne**.
2. Na karcie **Brakujące pliki** na dole ekranu, zaznacz pole wyboru znajdujące się przy nazwie pliku, który chcesz przywrócić.
3. Kliknij przycisk **Przywróć**.

Wskazówka: Można przywrócić wszystkie pliki z listy **Brakujące pliki**, klikając przycisk **Przywróć wszystko**.

Przywracanie starszej wersji pliku z archiwum lokalnego

Jeśli użytkownik chce przywrócić starszą wersję zarchiwizowanego pliku, może go zlokalizować i dodać do listy **Brakujące pliki**. Następnie można ten plik przywrócić, tak samo jak każdy inny plik z listy **Brakujące pliki**.

Aby przywrócić starszą wersję pliku z archiwum lokalnego:

1. Kliknij kartę **Archiwum lokalne**.
2. Na karcie **Brakujące pliki** na dole ekranu kliknij przycisk **Przeglądaj** i przejdź do lokalizacji, w której przechowywane jest archiwum.

   Nazwy folderów archiwów mają następujący format: `cre ddmmrr_gg-mm-ss_***`, gdzie `ddmmrr` jest datą archiwizacji plików, `gg-mm-ss` określa czas ich archiwizacji, a `***` zastępuje ciąg znaków `Pełna` lub `Inc`, w zależności od tego, czy przeprowadzono archiwizację pełną czy szybką.
3. Wybierz lokalizację, a następnie kliknij przycisk **OK**.

   Pliki zawarte w wybranej lokalizacji pojawią się na liście **Brakujące pliki**, skąd można je przywrócić. Więcej informacji na ten temat można znaleźć w sekcji Przywracanie brakujących plików z archiwum lokalnego.

Usuwanie plików z listy brakujących plików

Gdy zarchiwizowany plik zostanie przeniesiony lub usunięty z monitorowanego folderu, automatycznie pojawi się on na liście **Brakujące pliki**. Zwraca to uwagę użytkownika na fakt, że wystąpiła niezgodność pomiędzy plikami zarchiwizowanymi a plikami znajdującymi się w monitorowanych folderach. Jeśli plik został celowo przeniesiony lub usunięty z monitorowanego folderu, można go również usunąć z listy **Brakujące pliki**.

Aby usunąć plik z listy Brakujące pliki:

1. Kliknij kartę **Archiwum lokalne**.
2. Na karcie **Brakujące pliki** na dole ekranu, zaznacz pole wyboru znajdujące się przy nazwie pliku, który chcesz usunąć.
3. Kliknij przycisk **Usuń**.

Wskazówka: Można usunąć wszystkie pliki z listy **Brakujące pliki**, klikając przycisk **Usuń wszystko**.

Zarządzanie archiwami

W każdej chwili można wyświetlić podsumowanie pełnych i szybkich archiwizacji. Na przykład można wyświetlić informacje o ilości danych, które są w danej chwili monitorowane, ilości danych, które zostały zarchiwizowane oraz ilości danych, które są obecnie monitorowane, ale nie zostały jeszcze zarchiwizowane. Można również wyświetlić informacje dotyczące harmonogramu archiwizacji, takie jak data ostatniej i następnej archiwizacji.

Wyświetlanie podsumowania aktywności użytkownika związanej z archiwizacją

Informacje o aktywności użytkownika związanej z archiwizacją można wyświetlić w dowolnym momencie. Na przykład można zobaczyć procent zarchiwizowanych plików, rozmiar monitorowanych danych, rozmiar zarchiwizowanych danych oraz rozmiar danych, które są monitorowane, ale nie zostały jeszcze zarchiwizowane. Można również wyświetlić daty ostatniej i następnej archiwizacji.

Aby obejrzeć podsumowanie aktywności użytkownika dotyczącej kopii zapasowych:

1. Kliknij kartę **Archiwum lokalne**.
2. Na górze ekranu kliknij przycisk **Podsumowanie konta**.

ROZDZIAŁ 37

McAfee QuickClean

Program QuickClean poprawia wydajność komputera, usuwając pliki, które mogą zaśmiecać komputer. Program opróżnia Kosz i usuwa tymczasowe pliki, skróty, zagubione fragmenty plików, pliki rejestru, pliki zbuforowane, pliki cookie, pliki historii przeglądarki, wysłaną i usuniętą pocztę, listy ostatnio używanych plików, pliki ActiveX i pliki punktu przywracania systemu. Program QuickClean zapewnia także ochronę prywatności użytkownika dzięki składnikowi McAfee Shredder, który służy do bezpiecznego i trwałego usuwania elementów zawierających poufne informacje osobiste, takie jak dane osobowe użytkownika. Aby uzyskać informacje na temat niszczenia plików, zapoznaj się z opisem programu McAfee Shredder.

Defragmentator dysku rozmieszcza pliki i foldery na komputerze w sposób zapewniający ich nierozpraszanie (czyli niedzielenie na fragmenty) podczas zapisywaniu na dysku twardym komputera. Dzięki okresowemu defragmentowaniu dysku twardego można mieć pewność, że podzielone pliki i foldery zostaną połączone, co umożliwi ich szybkie pobieranie w późniejszym terminie.

Jeśli nie chcesz ręcznie obsługiwać swojego komputera, możesz zaplanować automatyczne uruchamianie programów QuickClean i Defragmentator dysku w postaci niezależnych zadań wykonywanych z dowolną częstotliwością.

Uwaga: Program SecurityCenter zgłasza krytyczne i niekrytyczne problemy dotyczące ochrony natychmiast po ich wykryciu. Jeśli potrzebna jest pomoc w diagnozowaniu problemów dotyczących ochrony, można uruchomić narzędzie McAfee Virtual Technician.

W tym rozdziale

Funkcje programu QuickClean

Program QuickClean pozwala wykonywać różne operacje oczyszczania, które usuwają niepotrzebne pliki w sposób bezpieczny i efektywny. Usuwając te pliki, użytkownik zwiększa ilość miejsca na dysku twardym komputera i poprawia jego wydajność.

Oczyszczanie komputera

Program QuickClean usuwa pliki, które mogą zaśmiecać komputer. Program opróżnia Kosz i usuwa tymczasowe pliki, skróty, zagubione fragmenty plików, pliki rejestru, pliki zbuforowane, pliki cookie, pliki historii przeglądarki, wysłaną i usuniętą pocztę, listy ostatnio używanych plików, pliki ActiveX i pliki punktu przywracania systemu. Program QuickClean usuwa te elementy, nie naruszając innych istotnych informacji.

Niepotrzebne pliki można usunąć z komputera za pomocą dowolnej operacji oczyszczania dostępnej w programie QuickClean. W poniższej tabeli opisano operacje oczyszczania dostępne w programie QuickClean:

Nazwa	Przeznaczenie
Oczyszczanie kosza	Usuwa pliki znajdujące się w Koszu.
Oczyszczanie plików tymczasowych	Usuwa pliki zapisane w folderach tymczasowych.
Oczyszczanie skrótów	Usuwa uszkodzone skróty i skróty bez skojarzonych z nimi programów.
Oczyszczanie zagubionych fragmentów plików	Usuwa z komputera zagubione fragmenty plików.
Oczyszczanie rejestru	Usuwa informacje rejestru systemu Windows® dotyczące programów nieistniejących już na komputerze. Rejestr jest bazą danych, w której system Windows przechowuje informacje dotyczące konfiguracji. Rejestr zawiera profile wszystkich użytkowników komputera, informacje o zainstalowanym sprzęcie i programach oraz ustawienia właściwości. System Windows w trakcie działania stale odwołuje się do tych informacji.
Oczyszczanie pamięci podręcznej	Usuwa buforowane pliki, które zbierają się podczas przeglądania stron sieci Web. Pliki te zwykle przechowywane są jako pliki tymczasowe w folderze pamięci podręcznej. Folder pamięci podręcznej jest miejscem zapisu tymczasowych danych komputera. Aby zwiększyć szybkość i sprawność przeglądania sieci Web, przeglądarka przy następnym wyświetlaniu strony sieci Web może ją pobierać z pamięci podręcznej (a nie ze zdalnego serwera).

Oczyszczanie plików cookie	Usuwa pliki cookie. Pliki te zwykle przechowywane są jako pliki tymczasowe. Plik cookie jest małym plikiem zawierającym informacje (najczęściej nazwę użytkownika oraz bieżącą datę i godzinę), który jest przechowywany na komputerze osoby przeglądającej sieć Web. Pliki cookie są używane przede wszystkim przez strony sieci Web w celu identyfikowania użytkowników, którzy zostali wcześniej zarejestrowani w witrynie albo ją odwiedzali. Mogą również stanowić źródło informacji dla hakerów.
Oczyszczanie historii przeglądarki	Usuwa historię przeglądanych stron sieci Web.
Oczyszczanie wiadomości e-mail programów Outlook Express i Outlook (elementy wysłane i usunięte)	Usuwa wysłane i usunięte wiadomości e-mail z programów Outlook® i Outlook Express.
Oczyszczanie ostatnio używanych elementów	Usuwa listę ostatnio używanych plików, które zostały utworzone w dowolnym z następujących programów: ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Historia systemu Windows ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®
Czyszczenie formantów ActiveX	Usuwa formanty ActiveX. ActiveX jest składnikiem oprogramowania używanym przez programy lub strony sieci Web w celu poszerzenia zakresu funkcji. Ten składnik integruje się z programem lub stroną sieci Web i działa jako zwykła część programu lub strony. Formanty ActiveX są w większości niegroźne, jednak niektóre z nich mogą przechwytywać informacje z komputera.
Oczyszczanie punktu przywracania systemu	Usuwa z komputera stare punkty przywracania systemu (poza najnowszym punktem). Punkty przywracania systemu są tworzone przez system Windows w celu oznaczania wszelkich zmian wprowadzanych do komputera, dzięki czemu w razie wystąpienia jakichkolwiek problemów można przywrócić poprzedni stan systemu.

Oczyszczanie komputera

Niepotrzebne pliki można usunąć z komputera za pomocą dowolnej operacji oczyszczania dostępnej w programie QuickClean. Po zakończeniu oczyszczania w obszarze **Program QuickClean — podsumowanie** można sprawdzić ilość miejsca odzyskanego na dysku, liczbę usuniętych plików oraz datę i godzinę uruchomienia ostatniej operacji programu QuickClean na komputerze.

1. W obszarze **Typowe zadania** okna McAfee SecurityCenter kliknij opcję **Konserwacja komputera**.
2. W obszarze **McAfee QuickClean** kliknij przycisk **Start**.
3. Wykonaj jedną z poniższych czynności:
   - Kliknij przycisk **Dalej**, aby zaakceptować domyślne operacje oczyszczania na liście.
   - Zaznacz lub usuń zaznaczenie odpowiednich operacji oczyszczania, a następnie kliknij przycisk **Dalej**. W przypadku wybrania operacji Oczyszczanie ostatnio używanych elementów można kliknąć opcję **Właściwości** w celu wybrania lub wyczyszczenia plików utworzonych ostatnio za pomocą programów znajdujących się na liście, a następnie kliknąć przycisk **OK**.
   - Kliknij przycisk **Przywróć ustawienia domyślne**, aby przywrócić domyślne operacje oczyszczania, a następnie kliknij przycisk **Dalej**.
4. Po wykonaniu analizy kliknij przycisk **Dalej**.
5. Kliknij przycisk **Dalej**, aby potwierdzić usuwanie pliku.
6. Wykonaj jedną z poniższych czynności:
   - Kliknij przycisk **Dalej**, aby zaakceptować domyślnie opcję **Nie, chcę usunąć pliki, korzystając ze standardowego sposobu usuwania plików w systemie Windows**.
   - Kliknij opcję **Tak, chcę bezpiecznie wymazać moje pliki za pomocą programu Shredder**, podaj liczbę przebiegów niszczenia (do 10), a następnie kliknij przycisk **Dalej**. W przypadku wymazywania dużych ilości informacji proces niszczenia plików może zająć dużo czasu.

7 Jeśli podczas wykonywania operacji czyszczenia niektóre pliki lub elementy zostały zablokowane, może zostać wyświetlony monit o ponowne uruchomienie komputera. Kliknij przycisk **OK**, aby zamknąć monit.

8 Kliknij przycisk **Zakończ**.

Uwaga: Pliki usunięte za pomocą programu Shredder nie mogą zostać przywrócone. Aby uzyskać informacje na temat niszczenia plików, zapoznaj się z opisem programu McAfee Shredder.

Defragmentowanie komputera

Defragmentator dysku rozmieszcza pliki i foldery na komputerze w sposób zapewniający ich nierozpraszanie (czyli niedzielenie na fragmenty) podczas zapisywania na dysku twardym komputera. Dzięki okresowemu defragmentowaniu dysku twardego można mieć pewność, że podzielone pliki i foldery zostaną połączone, co umożliwi ich szybkie pobieranie w późniejszym terminie.

Defragmentowanie komputera

W celu poprawienia dostępności plików i folderów oraz ułatwienia ich pobierania można wykonać defragmentację komputera.

1. W obszarze **Typowe zadania** okna McAfee SecurityCenter kliknij opcję **Konserwacja komputera**.
2. W obszarze **Defragmentator dysku** kliknij przycisk **Analizuj**.
3. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Uwaga: Aby uzyskać więcej informacji na temat programu Defragmentator dysku, zapoznaj się z Pomocą systemu Windows.

Planowanie zadania

Harmonogram zadań automatyzuje częstotliwość uruchamiania programów QuickClean i Defragmentator dysku na komputerze. Można na przykład zaplanować zadanie uruchamiania programu QuickClean w celu opróżniania Kosza w każdą niedzielę o godzinie 21.00 lub zadanie uruchamiania programu Defragmentator dysku w celu wykonania defragmentacji dysku twardego komputera w ostatni dzień każdego miesiąca. Takie zadanie można w dowolnym momencie utworzyć, zmodyfikować lub usunąć. Aby umożliwić uruchomienie zaplanowanego zadania, użytkownik musi być zalogowany na komputerze. Jeśli z jakiegokolwiek powodu zadanie nie zostanie uruchomione, nastąpi zmiana harmonogramu i uruchomienie zadania zostanie zaplanowane na pięć minut po zalogowaniu się użytkownika.

Planowanie zadania programu QuickClean

Istnieje możliwość zaplanowania zadania automatycznego czyszczenia komputera przy użyciu jednej lub kilku operacji oczyszczania dostępnych w programie QuickClean. Po zakończeniu wykonywania zadania w obszarze **Program QuickClean — podsumowanie** można sprawdzić datę i godzinę następnego zaplanowanego uruchomienia zadania.

1. Otwórz okienko Harmonogram zadań.

   Jak to zrobić?

   1. W obszarze **Typowe zadania** programu McAfee SecurityCenter kliknij opcję **Konserwacja komputera**.
   2. W obszarze **Harmonogram zadań** kliknij przycisk **Start**.

2. Na liście **Wybierz operację do zaplanowania** kliknij pozycję **McAfee QuickClean**.
3. W polu **Nazwa zadania** wpisz nazwę zadania, a następnie kliknij przycisk **Utwórz**.
4. Wykonaj jedną z poniższych czynności:
   - Kliknij przycisk **Dalej**, aby zaakceptować operacje oczyszczania na liście.
   - Zaznacz lub usuń zaznaczenie odpowiednich operacji oczyszczania, a następnie kliknij przycisk **Dalej**. W przypadku wybrania operacji Oczyszczanie ostatnio używanych elementów można kliknąć opcję **Właściwości** w celu wybrania lub wyczyszczenia plików utworzonych ostatnio za pomocą programów znajdujących się na liście, a następnie kliknąć przycisk **OK**.
   - Kliknij przycisk **Przywróć ustawienia domyślne**, aby przywrócić domyślne operacje oczyszczania, a następnie kliknij przycisk **Dalej**.

5 Wykonaj jedną z poniższych czynności:

- Kliknij przycisk **Harmonogram**, aby zaakceptować domyślnie opcję **Nie, chcę usunąć pliki, korzystając ze standardowego sposobu usuwania plików w systemie Windows**.
- Kliknij opcję **Tak, chcę bezpiecznie wymazać moje pliki za pomocą programu Shredder**, podaj liczbę przebiegów niszczenia (do 10), a następnie kliknij przycisk **Harmonogram**.

6 W oknie dialogowym **Harmonogram** wybierz częstotliwość uruchamiania zadania, a następnie kliknij przycisk **OK**.

7 Jeśli wprowadzono zmiany we właściwościach oczyszczania ostatnio używanych elementów, może zostać wyświetlony monit o ponowne uruchomienie komputera. Kliknij przycisk **OK**, aby zamknąć monit.

8 Kliknij przycisk **Zakończ**.

Uwaga: Pliki usunięte za pomocą programu Shredder nie mogą zostać przywrócone. Aby uzyskać informacje na temat niszczenia plików, zapoznaj się z opisem programu McAfee Shredder.

Modyfikowanie zadania programu QuickClean

Zaplanowane zadanie programu QuickClean można modyfikować, zmieniając używane operacje oczyszczania lub częstotliwość automatycznego uruchamiania zadania na komputerze użytkownika. Po zakończeniu wykonywania zadania w obszarze **Program QuickClean — podsumowanie** można sprawdzić datę i godzinę następnego zaplanowanego uruchomienia zadania.

1 Otwórz okienko Harmonogram zadań.

Jak to zrobić?

1. W obszarze **Typowe zadania** programu McAfee SecurityCenter kliknij opcję **Konserwacja komputera**.
2. W obszarze **Harmonogram zadań** kliknij przycisk **Start**.

2 Na liście **Wybierz operację do zaplanowania** kliknij pozycję **McAfee QuickClean**.

3 Wybierz zadanie z listy **Wybierz istniejące zadanie**, a następnie kliknij opcję **Modyfikuj**.

4 Wykonaj jedną z poniższych czynności:

- Kliknij przycisk **Dalej**, aby zaakceptować operacje oczyszczania wybrane dla zadania.

- Zaznacz lub usuń zaznaczenie odpowiednich operacji oczyszczania, a następnie kliknij przycisk **Dalej**. W przypadku wybrania operacji Oczyszczanie ostatnio używanych elementów można kliknąć opcję **Właściwości** w celu wybrania lub wyczyszczenia plików utworzonych ostatnio za pomocą programów znajdujących się na liście, a następnie kliknąć przycisk **OK**.
- Kliknij przycisk **Przywróć ustawienia domyślne**, aby przywrócić domyślne operacje oczyszczania, a następnie kliknij przycisk **Dalej**.

5 Wykonaj jedną z poniższych czynności:

- Kliknij przycisk **Harmonogram**, aby zaakceptować domyślnie opcję **Nie, chcę usunąć pliki, korzystając ze standardowego sposobu usuwania plików w systemie Windows**.
- Kliknij opcję **Tak, chcę bezpiecznie wymazać moje pliki za pomocą programu Shredder**, podaj liczbę przebiegów niszczenia (do 10), a następnie kliknij przycisk **Harmonogram**.

6 W oknie dialogowym **Harmonogram** wybierz częstotliwość uruchamiania zadania, a następnie kliknij przycisk **OK**.

7 Jeśli wprowadzono zmiany we właściwościach oczyszczania ostatnio używanych elementów, może zostać wyświetlony monit o ponowne uruchomienie komputera. Kliknij przycisk **OK**, aby zamknąć monit.

8 Kliknij przycisk **Zakończ**.

Uwaga: Pliki usunięte za pomocą programu Shredder nie mogą zostać przywrócone. Aby uzyskać informacje na temat niszczenia plików, zapoznaj się z opisem programu McAfee Shredder.

Usuwanie zadania programu QuickClean

Jeśli zaplanowane zadanie programu QuickClean nie ma być dłużej uruchamiane automatycznie, można je usunąć.

1 Otwórz okienko Harmonogram zadań.

Jak to zrobić?

1. W obszarze **Typowe zadania** programu McAfee SecurityCenter kliknij opcję **Konserwacja komputera**.
2. W obszarze **Harmonogram zadań** kliknij przycisk **Start**.

2 Na liście **Wybierz operację do zaplanowania** kliknij pozycję **McAfee QuickClean**.

3 Z listy **Wybierz istniejące zadanie** wybierz zadanie.

4 Kliknij przycisk **Usuń**, a następnie przycisk **Tak**, aby potwierdzić usunięcie.

5 Kliknij przycisk **Zakończ**.

Planowanie zadania programu Defragmentator dysku

Istnieje możliwość zaplanowania zadania programu Defragmentator dysku w celu określenia częstotliwości, z jaką ma być wykonywana automatyczna defragmentacja dysku twardego komputera. Po zakończeniu wykonywania zadania w obszarze **Defragmentator dysku** można sprawdzić datę i godzinę następnego zaplanowanego uruchomienia zadania.

1 Otwórz okienko Harmonogram zadań.

Jak to zrobić?

1. W obszarze **Typowe zadania** programu McAfee SecurityCenter kliknij opcję **Konserwacja komputera**.
2. W obszarze **Harmonogram zadań** kliknij przycisk **Start**.

2 Na liście **Wybierz operację do zaplanowania** kliknij pozycję **Defragmentator dysku**.

3 W polu **Nazwa zadania** wpisz nazwę zadania, a następnie kliknij przycisk **Utwórz**.

4 Wykonaj jedną z poniższych czynności:

- Kliknij opcję **Harmonogram**, aby zaakceptować domyślną opcję **Wykonaj defragmentację mimo małej ilości wolnego miejsca**.
- Usuń zaznaczenie opcji **Wykonaj defragmentację mimo małej ilości wolnego miejsca**, a następnie kliknij opcję **Harmonogram**.

5 W oknie dialogowym **Harmonogram** wybierz częstotliwość uruchamiania zadania, a następnie kliknij przycisk **OK**.

6 Kliknij przycisk **Zakończ**.

Modyfikowanie zadania programu Defragmentator dysku

Zaplanowane zadanie programu Defragmentator dysku można zmodyfikować w celu zmiany częstotliwości, z jaką zadanie ma być uruchamiane na komputerze. Po zakończeniu wykonywania zadania w obszarze **Defragmentator dysku** można sprawdzić datę i godzinę następnego zaplanowanego uruchomienia zadania.

1 Otwórz okienko Harmonogram zadań.

Jak to zrobić?

1. W obszarze **Typowe zadania** programu McAfee SecurityCenter kliknij opcję **Konserwacja komputera**.
2. W obszarze **Harmonogram zadań** kliknij przycisk **Start**.

2 Na liście **Wybierz operację do zaplanowania** kliknij pozycję **Defragmentator dysku**.

3 Wybierz zadanie z listy **Wybierz istniejące zadanie**, a następnie kliknij opcję **Modyfikuj**.

4 Wykonaj jedną z poniższych czynności:

- Kliknij opcję **Harmonogram**, aby zaakceptować domyślną opcję **Wykonaj defragmentację mimo małej ilości wolnego miejsca**.
- Usuń zaznaczenie opcji **Wykonaj defragmentację mimo małej ilości wolnego miejsca**, a następnie kliknij opcję **Harmonogram**.

5 W oknie dialogowym **Harmonogram** wybierz częstotliwość uruchamiania zadania, a następnie kliknij przycisk **OK**.

6 Kliknij przycisk **Zakończ**.

Usuwanie zadania programu Defragmentator dysku

Jeśli zaplanowane zadanie programu Defragmentator dysku nie ma być dłużej uruchamiane automatycznie, można je usunąć.

1 Otwórz okienko Harmonogram zadań.

Jak to zrobić?

1. W obszarze **Typowe zadania** programu McAfee SecurityCenter kliknij opcję **Konserwacja komputera**.
2. W obszarze **Harmonogram zadań** kliknij przycisk **Start**.

2 Na liście **Wybierz operację do zaplanowania** kliknij pozycję **Defragmentator dysku**.

3 Z listy **Wybierz istniejące zadanie** wybierz zadanie.

4 Kliknij przycisk **Usuń**, a następnie przycisk **Tak**, aby potwierdzić usunięcie.

5 Kliknij przycisk **Zakończ**.

ROZDZIAŁ 38

Program McAfee Shredder

Program McAfee Shredder w sposób trwały usuwa (niszczy) elementy znajdujące się na dysku twardym komputera. Nawet w przypadku ręcznego usunięcia plików i folderów, opróżnienia Kosza czy usunięcia tymczasowych plików internetowych, takie informacje można nadal odtworzyć za pomocą komputerowych narzędzi diagnostycznych. Ponadto istnieje możliwość odtworzenia usuniętego pliku, ponieważ niektóre programy tworzą tymczasowe, ukryte kopie otwieranych plików. Program Shredder zapewnia ochronę prywatności poprzez bezpieczne i trwałe usuwanie tych niepożądanych plików. Bardzo ważne: zniszczonych plików nie można już odtworzyć.

Uwaga: Program SecurityCenter zgłasza krytyczne i niekrytyczne problemy dotyczące ochrony natychmiast po ich wykryciu. Jeśli potrzebna jest pomoc w diagnozowaniu problemów dotyczących ochrony, można uruchomić narzędzie McAfee Virtual Technician.

W tym rozdziale

Funkcje programu Shredder

Program Shredder usuwa elementy z dysku twardego komputera, dzięki czemu nie można odtworzyć powiązanych z nimi informacji. Program zapewnia ochronę prywatności, pozwalając bezpiecznie i trwale usuwać pliki i foldery, elementy znajdujące się w Koszu i w folderze tymczasowych plików internetowych oraz całą zawartość dysków komputerowych, takich jak dyski CD wielokrotnego zapisu, zewnętrzne dyski twarde czy dyskietki.

Niszczenie plików, folderów i zawartości dysków

Dzięki programowi Shredder nie jest możliwe odtwarzanie informacji przechowywanych w usuniętych plikach i folderach, znajdujących się w Koszu i w folderze tymczasowych plików internetowych, nawet za pomocą specjalnych narzędzi. Program Shredder pozwala określić, ile razy dany element ma zostać zniszczony (maksymalnie 10 razy). Większa liczba przebiegów niszczenia zwiększa poziom bezpieczeństwa usuwania plików.

Niszczenie plików i folderów

Istnieje możliwość zniszczenia plików i folderów znajdujących się na dysku twardym komputera, w tym elementów przechowywanych w Koszu i w folderze tymczasowych plików internetowych.

1 Otwórz program **Shredder**.

Jak to zrobić?

1. W obszarze **Typowe zadania** okna McAfee SecurityCenter kliknij opcję **Menu zaawansowane**.
2. W okienku po lewej stronie kliknij opcję **Narzędzia**.
3. Kliknij opcję **Shredder**.

2 W obszarze **Działanie** okienka Zniszcz pliki i foldery kliknij opcję **Wymazywanie plików i folderów**.

3 W obszarze **Poziom niszczenia** wybierz jeden z następujących poziomów niszczenia:

- **Szybki**: Wybrane elementy są niszczone w 1 przebiegu.
- **Dokładny**: Wybrane elementy są niszczone w 7 przebiegach.
- **Niestandardowy**: Wybrane elementy są niszczone przez wykonanie do 10 przebiegów.

4 Kliknij przycisk **Dalej**.

5 Wykonaj jedną z poniższych czynności:

- Na liście **Wybierz pliki do zniszczenia** kliknij jedną z następujących pozycji: **Zawartość Kosza** lub **Tymczasowe pliki internetowe**.
- Kliknij przycisk **Przeglądaj**, przejdź do pliku, który chcesz zniszczyć, a następnie kliknij przycisk **Otwórz**.

6 Kliknij przycisk **Dalej**.

7 Kliknij opcję **Start**.

8 Po zakończeniu pracy programu Shredder kliknij opcję **Gotowe**.

Uwaga: Do czasu ukończenia tego zadania nie należy korzystać z żadnych plików.

Niszczenie całej zawartości dysku

Istnieje możliwość jednorazowego usunięcia całej zawartości dysku. Operacja niszczenia dotyczy tylko dysków wymiennych, takich jak zewnętrzne dyski twarde, dyski CD z możliwością zapisu i dyskietki.

1 Otwórz program **Shredder**.

Jak to zrobić?

1. W obszarze **Typowe zadania** okna McAfee SecurityCenter kliknij opcję **Menu zaawansowane**.
2. W okienku po lewej stronie kliknij opcję **Narzędzia**.
3. Kliknij opcję **Shredder**.

2 W obszarze **Działanie** okienka Zniszcz pliki i foldery kliknij opcję **Wymazywanie całego dysku**.

3 W obszarze **Poziom niszczenia** wybierz jeden z następujących poziomów niszczenia:

- **Szybki**: Zawartość wybranego dysku jest niszczona w 1 przebiegu.
- **Dokładny**: Zawartość wybranego dysku jest niszczona w 7 przebiegach.
- **Niestandardowy**: Zawartość wybranego dysku jest niszczona przez wykonanie do 10 przebiegów.

4 Kliknij przycisk **Dalej**.

5 Na liście **Wybierz dysk** kliknij dysk, którego zawartość chcesz zniszczyć.

6 Kliknij przycisk **Dalej**, a następnie kliknij przycisk **Tak**, aby potwierdzić ustawienia.

7 Kliknij opcję **Start**.

8 Po zakończeniu pracy programu Shredder kliknij opcję **Gotowe**.

Uwaga: Do czasu ukończenia tego zadania nie należy korzystać z żadnych plików.

ROZDZIAŁ 39

Program McAfee Network Manager

Program Network Manager przedstawia graficzną prezentację komputerów i urządzeń wchodzących w skład sieci domowej. Za jego pomocą można zdalnie monitorować stan ochrony każdego zarządzanego komputera działającego w sieci i usuwać zgłaszane luki w zabezpieczeniach tego komputera.

Przed rozpoczęciem korzystania z programu Network Manager można zapoznać się z niektórymi jego funkcjami. Szczegółowe informacje na temat konfigurowania i używania tych funkcji można znaleźć w pomocy programu Network Manager.

Uwaga: Program SecurityCenter zgłasza krytyczne i niekrytyczne problemy dotyczące ochrony natychmiast po ich wykryciu. Jeśli potrzebna jest pomoc w diagnozowaniu problemów dotyczących ochrony, można uruchomić narzędzie McAfee Virtual Technician.

W tym rozdziale

Funkcje programu Network Manager

Program Network Manager udostępnia następujące funkcje.

Graficzna mapa sieci

Mapa sieci programu Network Manager dostarcza graficznego przeglądu stanu ochrony komputerów i pozostałych elementów, z których składa się sieć domowa. Po wprowadzeniu w sieci zmian (na przykład po dodaniu komputera) mapa sieci uwzględnia je. Aby dostosować widok mapy do potrzeb, można ją odświeżać, zmieniać nazwę sieci i wyświetlać lub ukrywać jej elementy. Można również wyświetlić szczegółowe informacje na temat dowolnego składnika wyświetlanego na mapie sieci.

Zarządzanie zdalne

Mapę sieci programu Network Manager można wykorzystywać do zarządzania stanem ochrony komputerów tworzących sieć domową. Można zaprosić komputer do dołączenia do zarządzanej sieci, monitorować stan ochrony zarządzanego komputera i rozwiązywać problemy związane ze znanymi zagrożeniami bezpieczeństwa sieci pochodzącymi ze zdalnego komputera, który znajduje się w sieci.

Ikony programu Network Manager

W poniższej tabeli omówiono ikony, z jakich korzysta się zwykle w przypadku mapy sieci prezentowanej w programie Network Manager.

Ikona	Opis
	Oznacza zarządzany komputer działający w trybie online
	Oznacza zarządzany komputer działający w trybie offline
	Oznacza niezarządzany komputer, na którym zainstalowano program SecurityCenter
	Oznacza niezarządzany komputer działający w trybie offline
	Oznacza komputer działający w trybie online, na którym nie jest zainstalowany program SecurityCenter, lub oznacza nieznane urządzenie sieciowe
	Oznacza komputer działający w trybie offline, na którym nie jest zainstalowany program SecurityCenter, lub oznacza nieznane urządzenie sieciowe działające w trybie offline
	Informuje, że dany element jest chroniony i podłączony
	Informuje, że użytkownik powinien zwrócić uwagę na dany element
	Informuje, że użytkownik powinien niezwłocznie zwrócić uwagę na dany element
	Oznacza bezprzewodowy router sieci domowej
	Oznacza standardowy router sieci domowej
	Oznacza Internet, jeśli jest nawiązane z nim połączenie
	Oznacza Internet, jeśli nie jest nawiązane z nim połączenie

ROZDZIAŁ 40

Konfigurowanie zarządzanej sieci

Konfigurowanie zarządzanej sieci odbywa się za pomocą elementów naniesionych na mapę sieci oraz poprzez dodawanie do sieci składników (komputerów). Aby było możliwe zdalne zarządzanie komputerem lub przyznanie mu uprawnienia do zdalnego zarządzania innymi komputerami, musi on stać się zaufanym składnikiem sieci. Przynależność do sieci jest przyznawana nowym komputerom przez dotychczasowe składniki sieci (komputery), które mają uprawnienia administracyjne.

Można wyświetlić szczegóły dotyczące dowolnego składnika przedstawionego na mapie sieci, nawet po dokonaniu zmian w tej sieci (np. po dodaniu komputera).

W tym rozdziale

Korzystanie z mapy sieci

Po połączeniu komputera z siecią program Network Manager analizuje ją w celu określenia, czy występują w niej jakieś zarządzane lub niezarządzane składniki, oraz sprawdza atrybuty routera i stan Internetu. Jeśli nie zostaną znalezione żadne składniki, program Network Manager zakłada, że aktualnie podłączony komputer jest pierwszym komputerem w sieci i przyznaje mu status zarządzanego składnika z uprawnieniami administracyjnymi. Domyślnie nazwa sieci zawiera nazwę grupy roboczej lub domeny pierwszego komputera, który połączy się z siecią i ma zainstalowany program SecurityCenter. Nazwę sieci można jednak zmienić w dowolnym momencie.

Po wprowadzeniu zmian w sieci (np. dodaniu do niej komputera) można dostosować jej mapę. W tym celu można np. odświeżyć mapę, zmienić nazwę sieci oraz wyświetlić lub ukryć składniki na mapie. Można również wyświetlać szczegóły dotyczące dowolnego elementu przedstawionego na mapie sieci.

Uzyskiwanie dostępu do mapy sieci

Mapa sieci przedstawia w sposób graficzny komputery i komponenty tworzące sieć domową.

- W menu podstawowym lub zaawansowanym kliknij polecenie **Zarządzaj siecią**.

Uwaga: Przy pierwszym użyciu mapy sieci wyświetlany jest monit o potwierdzenie, że inne komputery w sieci są zaufane.

Odświeżanie mapy sieci

Mapę sieci można odświeżyć w dowolnym momencie, np. po dodaniu do zarządzanej sieci kolejnego komputera.

1. W menu podstawowym lub zaawansowanym kliknij polecenie **Zarządzaj siecią**.
2. W menu **Działanie** kliknij opcję **Odśwież mapę sieci**.

Uwaga: Łącze **Odśwież mapę sieci** jest dostępne tylko wówczas, gdy na mapie sieci nie jest zaznaczony żaden element. Aby usunąć zaznaczenie elementu, kliknij wybrany element lub kliknij obszar białego tła na mapie sieci.

Zmiana nazwy sieci

Domyślnie nazwa sieci zawiera nazwę grupy roboczej lub domeny pierwszego komputera, który połączy się z siecią i ma zainstalowany program SecurityCenter. Nazwę sieci można zmienić według uznania.

1. W menu podstawowym lub zaawansowanym kliknij polecenie **Zarządzaj siecią**.
2. W menu **Działanie** kliknij opcję **Zmień nazwę sieci**.
3. Wpisz nazwę sieci w polu **Nazwa sieci**.
4. Kliknij przycisk **OK**.

Uwaga: Łącze **Zmień nazwę sieci** jest dostępne tylko wówczas, gdy na mapie sieci nie jest zaznaczony żaden element. Aby usunąć zaznaczenie elementu, kliknij wybrany element lub kliknij obszar białego tła na mapie sieci.

Pokazywanie lub ukrywanie elementu na mapie sieci

Domyślnie wszystkie komputery i komponenty wchodzące w skład sieci domowej są pokazywane na mapie. Jeśli jednak część elementów została ukryta, można je wyświetlić ponownie w dowolnym momencie. Można ukryć tylko niezarządzane elementy. Zarządzanych komputerów nie można ukryć.

Aby...	W menu podstawowym lub zaawansowanym kliknij opcję **Zarządzaj siecią**, a następnie...
Ukrywanie elementu na mapie sieci	Kliknij element na mapie sieci, a następnie w menu **Działanie** kliknij opcję **Ukryj ten element**. W oknie dialogowym potwierdzenia kliknij przycisk **Tak**.
Pokazywanie ukrytych elementów na mapie sieci	W obszarze **Działanie** kliknij opcję **Pokaż ukryte elementy**.

Wyświetlanie szczegółów elementu

Można wyświetlić szczegółowe informacje o dowolnym komponencie sieci, wybierając go na mapie sieci. Informacje te obejmują nazwę komponentu, stan jego ochrony oraz inne dane niezbędne do zarządzania nim.

1. Kliknij ikonę elementu na mapie sieci.
2. W obszarze **Szczegóły** są wyświetlane informacje o tym elemencie.

Dołączanie do zarządzanej sieci

Aby było możliwe zdalne zarządzanie komputerem lub przyznanie mu uprawnienia do zdalnego zarządzania innymi komputerami, musi on stać się zaufanym składnikiem sieci. Przynależność do sieci jest przyznawana nowym komputerom przez dotychczasowe składniki sieci (komputery), które mają uprawnienia administracyjne. Aby zagwarantować, że do sieci będą dołączane tylko zaufane komputery, użytkownicy komputerów zarówno przyznających dostęp, jak i dołączających, muszą uwierzytelniać się nawzajem.

Gdy komputer dołącza do sieci, otrzymuje monit o ujawnienie swojego stanu ochrony McAfee innym komputerom w sieci. Jeśli komputer zgodzi się na ujawnienie swojego stanu ochrony, staje się zarządzanym składnikiem sieci. Jeśli komputer nie zgodzi się na ujawnienie swojego stanu ochrony, staje się niezarządzanym składnikiem sieci. Niezarządzane składniki sieci są zwykle komputerami-gośćmi, które chcą uzyskać dostęp do innych mechanizmów sieciowych (np. wysyłania plików lub współdzielenia drukarek).

Uwaga: Jeśli na komputerze są zainstalowane inne programy sieciowe firmy McAfee (np. EasyNetwork), po dołączeniu do sieci jest on ponadto rozpoznawany w tych programach jako zarządzany komputer. Poziom uprawnień, który zostanie przyznany komputerowi w programie Network Manager, obowiązuje we wszystkich programach sieciowych firmy McAfee. Więcej informacji na temat, czym są w programach sieciowych firmy McAfee uprawnienia gościa, pełne i administracyjne, można znaleźć w dokumentacji dołączonej do tych programów.

Dołączanie do zarządzanej sieci

Po otrzymaniu zaproszenia do dołączenia do zarządzanej sieci można je albo przyjąć, albo odrzucić. Można również określić, czy ten komputer i pozostałe komputery należące do sieci mają monitorować nawzajem swoje ustawienia zabezpieczeń (np. sprawdzać, czy usługi antywirusowe obecne na komputerze są aktualne).

1. Upewnij się, że pole wyboru **Zezwalaj wszystkim komputerom w tej sieci na monitorowanie ustawień zabezpieczeń** w oknie dialogowym Zarządzana sieć jest zaznaczone.
2. Kliknij przycisk **Dołącz**.
   Po przyjęciu zaproszenia zostaną wyświetlone dwie karty do gry.
3. Sprawdź, czy karty do gry są identyczne z wyświetlanymi na komputerze, który wysłał zaproszenie do dołączenia do zarządzanej sieci.
4. Kliknij przycisk **OK**.

Uwaga: Jeśli komputer, który wysłał zaproszenie do dołączenia do zarządzanej sieci, nie wyświetla takich samych kart do gry, jak wyświetlane w oknie dialogowym potwierdzenia zabezpieczeń, nastąpiło naruszenie bezpieczeństwa zarządzanej sieci. Dołączenie do sieci może spowodować zagrożenie dla komputera, dlatego w oknie dialogowym Zarządzana sieć kliknij przycisk **Odrzuć**.

Zapraszanie komputera do dołączenia do sieci zarządzanej

Jeśli komputer jest dodawany do zarządzanej sieci lub w sieci znajduje się inny niezarządzany komputer, można go zaprosić do dołączenia do zarządzanej sieci. Tylko komputery z uprawnieniami administratora w sieci mogą zapraszać inne komputery do dołączenia do sieci. Przed wysłaniem zaproszenia można również określić poziom uprawnień, który zostanie przypisany dołączającemu komputerowi.

1. Kliknij ikonę niezarządzanego komputera na mapie sieci.
2. Kliknij opcję **Monitoruj ten komputer** w obszarze **Działanie**.
3. W oknie dialogowym Zaproś komputer do dołączenia do zarządzanej sieci kliknij jedną z następujących opcji:
   - Kliknij opcję **Zezwalaj na dostęp gościa do zarządzanych programów sieciowych**, aby zezwolić komputerowi na dostęp do sieci (można użyć tej opcji dla tymczasowych użytkowników w domu).
   - Kliknij opcję **Zezwalaj na dostęp pełny do zarządzanych programów sieciowych**, aby zezwolić komputerowi na dostęp do sieci.

- Kliknij opcję **Zezwalaj na dostęp administracyjny do zarządzanych programów sieciowych**, aby zezwolić komputerowi na dostęp do sieci z uprawnieniami administracyjnymi. Opcja ta uprawnia również komputer do udzielania dostępu innym komputerom, które zamierzają dołączyć do zarządzanej sieci.

4 Kliknij przycisk **OK**.
Do komputera zostanie wysłane zaproszenie do dołączenia do zarządzanej sieci. Gdy komputer zaakceptuje zaproszenie zostaną wyświetlone dwie karty do gry.

5 Sprawdź, czy karty do gry są takie same jak te wyświetlone na komputerze zaproszonym do dołączenia do zarządzanej sieci.

6 Kliknij opcję **Przyznaj prawa dostępu**.

Uwaga: Jeśli na komputerze zaproszonym do dołączenia do zarządzanej sieci w oknie dialogowym potwierdzenia zabezpieczeń nie są wyświetlone te same karty, w zarządzanej sieci nastąpiło naruszenie bezpieczeństwa. Zezwolenie na dołączenie komputera do sieci może spowodować zagrożenie dla innych komputerów; z tego powodu kliknij przycisk **Odmów dostępu** w oknie dialogowym potwierdzenia zabezpieczeń.

Utrata zaufania do komputerów w sieci

Jeśli użytkownik zaufał innym komputerom przez pomyłkę, może cofnąć swoje zaufanie.

- Kliknij opcję **Przestań ufać komputerom w tej sieci** w obszarze **Działanie**.

Uwaga: Łącze **Przestań ufać komputerom w tej sieci** nie jest dostępne, gdy użytkownik ma uprawnienia administracyjne, a w sieci znajdują się inne zarządzane komputery.

ROZDZIAŁ 41

Zdalne zarządzanie siecią

Po skonfigurowaniu zarządzanej sieci można zdalnie zarządzać komputerami i składnikami sieci. Można monitorować stan i poziomy uprawnień komputerów i składników oraz zdalnie naprawiać większość luk w zabezpieczeniach.

W tym rozdziale

Monitorowanie stanu i uprawnień

W skład sieci zarządzanej wchodzą elementy zarządzane i niezarządzane. Elementy zarządzane zezwalają innym komputerom w sieci na monitorowanie swojego stanu ochrony McAfee, natomiast niezarządzane na to nie zezwalają. Elementy niezarządzane to zazwyczaj komputery-goście, które uzyskują dostęp do innych mechanizmów sieciowych (np. wysyłania plików lub współdzielenia drukarek). Zarządzany komputer w sieci może w dowolnym momencie zaprosić niezarządzany komputer, aby stał się zarządzanym. Podobnie zarządzany komputer może w dowolnym momencie zostać niezarządzanym.

Zarządzane komputery mają uprawnienia dostępu administracyjnego, pełnego lub typu Gość. Uprawnienia administracyjne umożliwiają zarządzanemu komputerowi zarządzanie stanem ochrony wszystkich pozostałych zarządzanych komputerów w sieci i przyznawanie innym komputerom członkostwa w sieci. Uprawnienia pełne i gościa umożliwiają komputerowi tylko uzyskanie dostępu do sieci. Poziom uprawnień komputera można modyfikować w dowolnym momencie.

Ponieważ zarządzana sieć składa się również z urządzeń (na przykład routerów), również nimi można zarządzać za pomocą programu Network Manager. Można także konfigurować i modyfikować właściwości wyświetlania urządzenia na mapie sieci.

Monitorowanie stanu ochrony komputera

Jeśli stan ochrony komputera nie jest monitorowany w sieci (komputer nie jest elementem sieci lub jest jej elementem niezarządzanym), można zażądać jego monitorowania.

1. Kliknij ikonę niezarządzanego komputera na mapie sieci.
2. Kliknij opcję **Monitoruj ten komputer** w obszarze **Działanie**.

Zakończenie monitorowania stanu ochrony komputera

Można zakończyć monitorowanie stanu ochrony zarządzanego komputera w sieci; komputer jednak staje się wówczas niezarządzany i nie można zdalnie monitorować stanu jego ochrony.

1. Kliknij ikonę zarządzanego komputera na mapie sieci.
2. Kliknij opcję **Zakończ monitorowanie tego komputera** w obszarze **Działanie**.
3. W oknie dialogowym potwierdzenia kliknij przycisk **Tak**.

Modyfikacja uprawnień zarządzanego komputera

Uprawnienia zarządzanego komputera można w dowolnym momencie zmieniać. Umożliwia to ustalenie, które komputery mogą monitorować stan ochrony innych komputerów w sieci.

1. Kliknij ikonę zarządzanego komputera na mapie sieci.
2. Kliknij opcję **Modyfikuj uprawnienia dla tego komputera** w obszarze **Działanie**.
3. W oknie dialogowym modyfikacji uprawnień zaznacz pole wyboru lub usuń jego zaznaczenie, aby określić, czy ten i inne komputery w zarządzanej sieci mogą monitorować nawzajem swój stan ochrony.
4. Kliknij przycisk **OK**.

Zarządzanie urządzeniem

Urządzeniem można zarządzać, uzyskując dostęp do jego administracyjnej strony sieci Web w programie Network Manager.

1. Kliknij ikonę urządzenia na mapie sieci.
2. Kliknij opcję **Zarządzaj tym urządzeniem** w obszarze **Działanie**.
   Administracyjna strona sieci Web urządzenia zostanie otwarta w przeglądarce sieci Web.
3. W przeglądarce sieci Web podaj informacje wymagane podczas logowania i skonfiguruj ustawienia zabezpieczeń urządzenia.

Uwaga: Jeśli urządzeniem jest bezprzewodowy router lub punkt dostępu chroniony programem Wireless Network Security, do konfiguracji ustawień zabezpieczeń urządzenia należy użyć programu Wireless Network Security.

Modyfikacja właściwości wyświetlania urządzenia

Podczas modyfikacji właściwości wyświetlania urządzenia można zmienić nazwę urządzenia wyświetlaną na mapie sieci oraz określić, czy urządzenie jest routerem bezprzewodowym.

1. Kliknij ikonę urządzenia na mapie sieci.
2. Kliknij opcję **Modyfikuj właściwości urządzenia** w obszarze **Działanie**.
3. Aby określić wyświetlaną nazwę urządzenia, wpisz ją w polu **Nazwa**.
4. Aby określić typ urządzenia, kliknij opcję **Router standardowy**, jeśli nie jest to router bezprzewodowy, lub opcję **Router bezprzewodowy** w przypadku routera bezprzewodowego.
5. Kliknij przycisk **OK**.

Naprawa luk w zabezpieczeniach

Zarządzane komputery z uprawnieniami administracyjnymi mogą monitorować stan ochrony McAfee innych zarządzanych komputerów w sieci i zdalnie naprawiać zgłoszone luki w zabezpieczeniach. Na przykład jeśli stan ochrony McAfee zarządzanego komputera wskazuje, że program VirusScan jest wyłączony, inny zarządzany komputer z uprawnieniami administracyjnymi może zdalnie włączyć program VirusScan.

Podczas zdalnego naprawiania luk w zabezpieczeniach program Network Manager naprawia najczęściej zgłaszane problemy. Jednak niektóre luki w zabezpieczeniach mogą wymagać ręcznej interwencji na lokalnym komputerze. W takim przypadku program Network Manager naprawia te problemy, które można naprawić zdalnie, a następnie monituje o naprawienie pozostałych poprzez zalogowanie do programu SecurityCenter na zagrożonym komputerze i postępowanie zgodnie z podanymi zaleceniami. W niektórych przypadkach sugerowanym sposobem naprawy jest instalacja najnowszej wersji programu SecurityCenter na zdalnym komputerze lub komputerach w sieci.

Napraw luki w zabezpieczeniach

Programu Network Manager można użyć do naprawiania większości luk w zabezpieczeniach na zdalnych zarządzanych komputerach. Jeśli na przykład program VirusScan na zdalnym komputerze jest wyłączony, można go włączyć.

1. Kliknij ikonę elementu na mapie sieci.
2. Zapoznaj się ze stanem ochrony elementu w obszarze **Szczegóły**.
3. Kliknij opcję **Napraw luki w zabezpieczeniach** w obszarze **Działanie**.
4. Po naprawieniu problemów z zabezpieczeniami kliknij przycisk **OK**.

Uwaga: Mimo iż program Network Manager automatycznie naprawia większość luk w zabezpieczeniach, niektóre naprawy mogą wymagać uruchomienia programu SecurityCenter na zagrożonym komputerze i postępowania zgodnie z podanymi zaleceniami.

Instalowanie oprogramowania zabezpieczającego McAfee na zdalnych komputerach

Jeśli jeden lub więcej komputerów w sieci nie posiada najnowszej wersji programu SecurityCenter, ich stan zabezpieczeń nie może być zdalnie monitorowany. Aby zdalnie monitorować te komputery, należy na każdym z nich zainstalować najnowszą wersję programu SecurityCenter.

1. Na komputerze, na którym ma zostać zainstalowane oprogramowanie zabezpieczające, otwórz program SecurityCenter.
2. W obszarze **Typowe zadania** kliknij opcję **Moje konto**.
3. Zaloguj się, używając tego samego adresu e-mail i hasła, które zostały użyte do rejestracji oprogramowania zabezpieczającego przy jego pierwszej instalacji.
4. Wybierz odpowiedni produkt, kliknij ikonę **Pobierz/Instaluj**, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

ROZDZIAŁ 42

Program McAfee EasyNetwork

Program EasyNetwork umożliwia bezpieczne udostępnianie plików, upraszcza ich przesyłanie i udostępnianie drukarek innym komputerom w sieci domowej. Na komputerach w sieci musi być jednak zainstalowany program EasyNetwork, aby mogły one korzystać z jego funkcji.

Przed rozpoczęciem użytkowania programu EasyNetwork można zapoznać się z niektórymi jego funkcjami. Szczegółowe informacje na temat konfigurowania tych funkcji i korzystania z nich zamieszczono w pomocy programu EasyNetwork.

Uwaga: Program SecurityCenter zgłasza krytyczne i niekrytyczne problemy dotyczące ochrony natychmiast po ich wykryciu. Jeśli potrzebna jest pomoc w diagnozowaniu problemów dotyczących ochrony, można uruchomić narzędzie McAfee Virtual Technician.

W tym rozdziale

Funkcje programu EasyNetwork

Program EasyNetwork jest wyposażony w następujące funkcje:

Udostępnianie plików

Program EasyNetwork ułatwia udostępnianie plików innym komputerom w sieci. Gdy pliki zostają udostępnione, innym komputerom zostaje przyznany dostęp pozwalający tylko na ich odczyt. Tylko komputery, którym przyznano pełny lub administracyjny dostęp do zarządzanej sieci (elementy) mogą udostępniać pliki lub uzyskiwać dostęp do plików udostępnianych przez inne elementy.

Przesyłanie plików

Można przesyłać pliki do innych komputerów, które mają pełny lub administracyjny dostęp do zarządzanej sieci (elementów). Gdy plik zostaje odebrany, pojawia się w skrzynce odbiorczej programu EasyNetwork. Skrzynka odbiorcza jest tymczasowym miejscem przechowywania dla wszystkich plików przysyłanych przez inne komputery w sieci.

Automatyczne udostępnianie drukarek

Po przyłączeniu komputera do zarządzanej sieci udostępnia on wszystkie lokalne drukarki podłączone do komputera, traktując aktualne nazwy drukarek jako nazwy drukarek udostępnionych. Ponadto wykrywa drukarki udostępniane przez inne komputery w sieci oraz umożliwia ich konfigurowanie i używanie.

ROZDZIAŁ 43

Konfigurowanie programu EasyNetwork

Przed rozpoczęciem korzystania z programu EasyNetwork należy otworzyć zarządzaną sieć i dołączyć do niej. Po dołączeniu do zarządzanej sieci można udostępniać, wyszukiwać i przesyłać pliki do innych komputerów w sieci. Można również udostępniać drukarki. Sieć można opuścić w każdej chwili.

W tym rozdziale

Uruchamianie programu EasyNetwork

Domyślnie po instalacji jest wyświetlany monit o uruchomienie programu EasyNetwork, program jednak można uruchomić także później.

- W menu **Start** wybierz polecenie **Programy**, następnie polecenie **McAfee**, a potem kliknij polecenie **McAfee EasyNetwork**.

Wskazówka: Jeśli podczas instalacji utworzono ikony na pulpicie oraz ikony szybkiego uruchamiania, program EasyNetwork można też uruchomić, klikając dwukrotnie ikonę McAfee EasyNetwork na pulpicie lub klikając ikonę w obszarze powiadomień znajdującym się w prawej części paska zadań.

Dołączanie do zarządzanej sieci

Jeśli na żadnym z komputerów, z którymi jest połączony użytkownik, nie zainstalowano programu SecurityCenter, komputer użytkownika staje się elementem sieci, a użytkownik jest proszony o określenie, czy sieć jest zaufana. Ponieważ jest to pierwszy komputer dołączany do sieci, nazwa komputera staje się częścią nazwy sieci. Nazwę sieci można jednak w każdej chwili zmienić.

Gdy komputer nawiązuje połączenie z siecią, do wszystkich pozostałych komputerów podłączonych w danej chwili do sieci jest wysyłane żądanie dołączenia do niej. Żądanie to może zostać zaakceptowane przez dowolny komputer z uprawnieniami administracyjnymi w danej sieci. Z takiego komputera można również określić poziom uprawnień dla komputerów dołączonych w danej chwili do sieci, na przykład poziom Gościa (tylko przesyłanie plików) lub poziom pełny/administracyjny (przesyłanie i udostępnianie plików). W sieci zarządzanej przez program EasyNetwork z komputerów z dostępem administracyjnym można przyznawać prawo dostępu innym komputerom oraz zarządzać uprawnieniami (podwyższać lub obniżać poziom uprawnień komputerów). Zadań administracyjnych nie można przeprowadzać z komputerów z dostępem pełnym.

Uwaga: Jeśli na komputerze są zainstalowane inne programy sieciowe firmy McAfee (np. Network Manager), po dołączeniu do sieci jest on ponadto rozpoznawany w tych programach jako zarządzany komputer. Poziom uprawnień przypisany do komputera w programie EasyNetwork dotyczy wszystkich programów sieciowych McAfee. Więcej informacji na temat, czym są w programach sieciowych firmy McAfee uprawnienia gościa, pełne i administracyjne, można znaleźć w dokumentacji dołączonej do tych programów.

Dołączanie do sieci

Gdy komputer po zainstalowaniu programu EasyNetwork po raz pierwszy nawiązuje połączenie z zaufaną siecią, wyświetlane jest pytanie, czy ma zostać dołączony do sieci zarządzanej. Gdy zostanie wyrażona zgoda na dołączenie komputera, do wszystkich pozostałych komputerów w sieci z uprawnieniami administracyjnymi jest wysyłane żądanie. Aby komputer mógł udostępniać drukarki lub pliki i wysyłać lub kopiować pliki w sieci, żądanie musi zostać zaakceptowane. Pierwszy komputer w sieci automatycznie otrzymuje uprawnienia administracyjne.

1. W oknie Udostępniane pliki kliknij opcję **Dołącz do tej sieci**. Gdy komputer administracyjny w sieci zaakceptuje to żądanie, zostanie wyświetlony komunikat z pytaniem, czy zezwolić temu komputerowi i pozostałym komputerom w sieci na wzajemne zarządzanie ustawieniami zabezpieczeń.
2. Aby zezwolić temu komputerowi i pozostałym komputerom w sieci na wzajemne zarządzanie ustawieniami zabezpieczeń, kliknij przycisk **OK**. Aby nie zezwolić na to, kliknij przycisk **Anuluj**.
3. Sprawdź, czy na komputerze akceptującym żądanie są wyświetlane karty do gry, które w danej chwili są wyświetlane w oknie dialogowym potwierdzania zabezpieczeń, a następnie kliknij przycisk **OK**.

Uwaga: Jeśli komputer, który wysłał zaproszenie do dołączenia do zarządzanej sieci, nie wyświetla takich samych kart do gry, jak wyświetlane w oknie dialogowym potwierdzenia zabezpieczeń, nastąpiło naruszenie bezpieczeństwa zarządzanej sieci. Dołączenie do sieci może spowodować zagrożenie dla komputera, dlatego w oknie dialogowym potwierdzania zabezpieczeń kliknij przycisk **Anuluj**.

Przyznawanie dostępu do zarządzanej sieci

Gdy komputer żąda dołączenia do zarządzanej sieci, do komputerów w sieci mających uprawnienia administracyjne jest wysyłany komunikat. Pierwszy komputer, który odpowie na komunikat, staje się komputerem przyznającym dostęp. Jego użytkownik jest odpowiedzialny za decyzję, który typ dostępu przyznać komputerowi: gość, pełny czy administrator.

1. W oknie alertu kliknij odpowiedni poziom dostępu.
2. W oknie dialogowym Zaproś komputer do dołączenia do zarządzanej sieci kliknij jedną z następujących opcji:
   - Kliknij opcję **Zezwalaj na dostęp gościa do zarządzanych programów sieciowych**, aby zezwolić komputerowi na dostęp do sieci (można użyć tej opcji dla tymczasowych użytkowników w domu).
   - Kliknij opcję **Zezwalaj na dostęp pełny do zarządzanych programów sieciowych**, aby zezwolić komputerowi na dostęp do sieci.

- Kliknij opcję **Zezwalaj na dostęp administracyjny do zarządzanych programów sieciowych**, aby zezwolić komputerowi na dostęp do sieci z uprawnieniami administracyjnymi. Opcja ta uprawnia również komputer do udzielania dostępu innym komputerom, które zamierzają dołączyć do zarządzanej sieci.

3 Kliknij przycisk **OK**.

4 Sprawdź, czy na komputerze są wyświetlane karty do gry, które w danej chwili są wyświetlane w oknie dialogowym potwierdzania zabezpieczeń, a następnie kliknij opcję **Przyznaj prawa dostępu**.

Uwaga: Jeśli na komputerze nie są wyświetlane te same karty, które są widoczne w oknie dialogowym potwierdzania zabezpieczeń, oznacza to, że w zarządzanej sieci doszło do naruszenia zabezpieczeń. Przyznanie temu komputerowi dostępu do sieci mogłoby stanowić zagrożenie własnego komputera, dlatego w takiej sytuacji w oknie dialogowym potwierdzania zabezpieczeń kliknij przycisk **Odmów dostępu**.

Zmiana nazwy sieci

Domyślnie nazwa sieci zawiera nazwę pierwszego komputera, który do niej dołączył. Nazwę sieci można jednak w każdej chwili zmienić. Gdy zmieniona zostaje nazwa sieci, zmienia się opis sieci wyświetlany w programie EasyNetwork.

1. W menu **Opcje** kliknij polecenie **Konfiguruj**.
2. W oknie dialogowym Konfigurowanie wpisz nazwę sieci w polu **Nazwa sieci**.
3. Kliknij przycisk **OK**.

Opuszczanie zarządzanej sieci

Jeśli użytkownik dołączy do zarządzanej sieci, a następnie zdecyduje, że nie chce już do niej należeć, może tę sieć opuścić. Po opuszczeniu zarządzanej sieci w każdej chwili można do niej ponownie dołączyć, należy jednak ponownie uzyskać prawo do tego. Więcej informacji o dołączaniu do sieci można znaleźć w sekcji *Dołączanie do zarządzanej sieci* (strona 250).

Opuszczanie zarządzanej sieci

Użytkownik może opuścić zarządzaną sieć, do której wcześniej dołączył.

1. W menu **Narzędzia** kliknij polecenie **Opuść sieć**.
2. W oknie dialogowym Opuść sieć wybierz nazwę sieci, którą chcesz opuścić.
3. Kliknij opcję **Opuść sieć**.

ROZDZIAŁ 44

Udostępnianie i wysyłanie plików

Program EasyNetwork ułatwia udostępnianie plików i wysyłanie ich do innych komputerów w sieci. Udostępniając pliki innym komputerom w sieci, przyznaje się im tylko uprawnienia do odczytu. Tylko te komputery, które należą do danej zarządzanej sieci (czyli z dostępem pełnym lub administracyjnym), mogą udostępniać pliki oraz uzyskiwać dostęp do plików udostępnianych przez inne komputery należące do tej sieci.

Uwaga: Udostępnianie dużej liczby plików może mieć wpływ na zasoby komputera.

W tym rozdziale

Udostępnianie plików

Tylko te komputery, które należą do danej zarządzanej sieci (czyli z dostępem pełnym lub administracyjnym), mogą udostępniać pliki oraz uzyskiwać dostęp do plików udostępnianych przez inne komputery należące do tej sieci. Jeśli udostępniany jest folder, udostępniane są wszystkie pliki zawarte w tym folderze i w jego podfolderach. Kolejne pliki dodawane do tego folderu nie są automatycznie udostępniane. Jeśli udostępniany plik lub folder zostaje usunięty, zostaje usunięty z okna Udostępniane pliki. Udostępnianie pliku można zakończyć w każdej chwili.

Aby uzyskać dostęp do udostępnionego pliku, otwórz plik bezpośrednio w programie EasyNetwork lub skopiuj go do swojego komputera, a następnie otwórz plik. Jeśli lista udostępnionych plików użytkownika jest długa i trudno dostrzec na niej żądany plik, można go wyszukać.

Uwaga: Do plików udostępnionych za pomocą programu EasyNetwork nie można uzyskać dostępu na innych komputerach za pomocą Eksploratora Windows, ponieważ udostępnianie plików w programie EasyNetwork wymaga bezpiecznych połączeń.

Udostępnianie pliku

Gdy plik zostaje udostępniony, staje się dostępny dla wszystkich elementów z pełnym lub administracyjnym dostępem do zarządzanej sieci.

1. W Eksploratorze Windows znajdź plik, który ma być udostępniany.
2. Przeciągnij plik z miejsca, w którym się znajduje w Eksploratorze Windows, do okna Udostępniane pliki w programie EasyNetwork.

Wskazówka: Plik można również udostępnić inaczej, klikając polecenie **Udostępnij pliki** w menu **Narzędzia**. W oknie dialogowym Udostępnianie przejdź do folderu zawierającego plik, który ma zostać udostępniony, zaznacz ten plik, a następnie kliknij opcję **Udostępnij**.

Kończenie udostępniania pliku

Jeśli plik jest udostępniany w zarządzanej sieci, udostępnianie można w każdej chwili zakończyć. Gdy udostępnianie pliku zostanie zakończone, inne komputery należącej do danej sieci zarządzanej nie będą miały do niego dostępu.

1. W menu **Narzędzia** kliknij polecenie **Zakończ udostępnianie plików**.
2. W oknie dialogowym Zakończ udostępnianie plików zaznacz plik, który ma już nie być udostępniany.
3. Kliknij przycisk **OK**.

Kopiowanie udostępnianego pliku

Udostępniany plik można skopiować, aby mieć do niego dostęp, kiedy już nie będzie on udostępniony. Można skopiować plik z każdego komputera w zarządzanej sieci.

- Przeciągnij plik z okna Udostępniane pliki w programie EasyNetwork w dowolne miejsce w Eksploratorze Windows lub na pulpit systemu Windows.

Wskazówka: Udostępniany plik można również skopiować, zaznaczając go w programie EasyNetwork, a następnie klikając polecenie **Kopiuj do** w menu **Narzędzia**. W oknie dialogowym Kopiuj do przejdź do folderu, do którego plik ma zostać skopiowany, zaznacz go, a następnie kliknij opcję **Zapisz**.

Wyszukiwanie udostępnianego pliku

Możliwe jest wyszukiwanie pliku, który został udostępniony na komputerze użytkownika lub innym komputerze należącym do danej sieci. W miarę wpisywania kryteriów wyszukiwania program EasyNetwork wyświetla odpowiadające im wyniki w oknie Udostępniane pliki.

1. W oknie Udostępniane pliki kliknij opcję **Wyszukaj**.
2. Kliknij *odpowiednią opcję* (strona 257) na liście **Zawiera**.
3. Wpisz część, całą nazwę pliku lub ścieżki na liście **Nazwa pliku lub ścieżka do pliku**.
4. Kliknij odpowiedni *typ pliku* (strona 257) na liście **Typ**.
5. Na listach **Od** i **Do** kliknij daty odpowiadające zakresowi dat utworzenia pliku.

Kryteria wyszukiwania

W poniższych tabelach opisano kryteria wyszukiwania, które można podać podczas wyszukiwania udostępnianych plików.

Nazwa pliku lub ścieżka

Zawiera:	Opis
Zawiera wszystkie słowa	Powoduje wyszukanie nazw plików lub ścieżek zawierających wszystkie słowa określone na liście **Nazwa pliku lub ścieżka do pliku**, w dowolnej kolejności.
Zawiera którekolwiek ze słów	Powoduje wyszukanie nazw plików lub ścieżek zawierających którekolwiek ze słów określonych na liście **Nazwa pliku lub ścieżka do pliku**.
Zawiera cały łańcuch znaków	Powoduje wyszukanie nazw plików lub ścieżek zawierających całą frazę określoną na liście **Nazwa pliku lub ścieżka do pliku**.

Typ pliku

Typ	Opis
Dowolna	Powoduje wyszukanie wszystkich typów udostępnianych plików.
Dokument	Powoduje wyszukanie wszystkich udostępnianych dokumentów.
Obraz	Powoduje wyszukanie wszystkich udostępnianych plików obrazów.
Wideo	Powoduje wyszukanie wszystkich udostępnianych plików wideo.
Audio	Powoduje wyszukanie wszystkich udostępnianych plików audio.
Skompresowany	Powoduje wyszukanie wszystkich skompresowanych plików (np. plików zip).

Wysyłanie plików do innych komputerów

Możliwe jest wysyłanie plików do innych komputerów należących do danej zarządzanej sieci. Przed wysłaniem pliku program EasyNetwork sprawdza, czy na komputerze odbierającym plik jest dostatecznie dużo dostępnego miejsca na dysku.

Gdy plik zostaje odebrany, pojawia się w skrzynce odbiorczej programu EasyNetwork. Skrzynka odbiorcza jest tymczasowym miejscem przechowywania dla plików przysyłanych przez inne komputery w sieci. Jeśli program EasyNetwork jest otwarty podczas odbierania pliku, plik ten natychmiast pojawia się w skrzynce odbiorczej; w przeciwnym razie wyświetlany jest komunikat w obszarze powiadomień w prawej części paska zadań systemu Windows. Jeśli użytkownik nie chce otrzymywać powiadomień (np. ponieważ przeszkadzają mu w pracy), można wyłączyć tę funkcję. Jeśli w skrzynce odbiorczej już istnieje plik o tej samej nazwie, nazwa nowego pliku zostaje zmieniona za pomocą przyrostka liczbowego. Pliki pozostają w skrzynce odbiorczej do momentu ich przyjęcia (skopiowania do komputera użytkownika).

Wysyłanie pliku do innego komputera

Możliwe jest wysłanie pliku do innego komputera w zarządzanej sieci bez jego udostępniania. Aby użytkownik na komputerze odbiorczym mógł przejrzeć plik, musi go na nim zapisać. Więcej informacji można znaleźć w sekcji *Przyjmowanie pliku z innego komputera* (strona 260).

1. W Eksploratorze Windows znajdź plik, który ma zostać wysłany.
2. Przeciągnij plik z miejsca, w którym się znajduje w Eksploratorze Windows na ikonę aktywnego komputera w programie EasyNetwork.

Wskazówka: Aby wysłać wiele plików jednocześnie do danego komputera, naciśnij klawisz CTRL podczas zaznaczania plików. Pliki można również wysyłać, klikając polecenie **Wyślij** w menu **Narzędzia**, zaznaczając pliki, a następnie klikając opcję **Wyślij**.

Przyjmowanie pliku z innego komputera

Jeśli inny komputer w zarządzanej sieci przysyła plik, musi on zostać przyjęty przez zapisanie go na lokalnym komputerze. Jeśli podczas przesyłania pliku program EasyNetwork nie jest włączony, zostanie wyświetlone powiadomienie na prawym końcu paska zadań. Kliknij komunikat z powiadomieniem, aby otworzyć program EasyNetwork i uzyskać dostęp do tego pliku.

- Kliknij opcję **Odebrane**, a następnie przeciągnij plik ze skrzynki odbiorczej programu EasyNetwork do folderu w Eksploratorze Windows.

Wskazówka: Plik z innego komputera można również odebrać, zaznaczając go w skrzynce odbiorczej programu EasyNetwork, a następnie klikając polecenie **Akceptuj** w menu **Narzędzia**. W oknie dialogowym Przyjmij do folderu przejdź do folderu, w którym mają zostać zapisane odbierane pliki, zaznacz go, a następnie kliknij opcję **Zapisz**.

Odbieranie powiadomienia o wysłaniu pliku

Użytkownik może otrzymać powiadomienie o wysłaniu do niego pliku z innego komputera w zarządzanej sieci. Jeśli program EasyNetwork nie jest uruchomiony, powiadomienie zostanie wyświetlone na prawym końcu paska zadań.

1. W menu **Opcje** kliknij polecenie **Konfiguruj**.
2. W oknie dialogowym Konfigurowanie zaznacz pole wyboru **Powiadom mnie, gdy inny komputer wysyła do mnie pliki**.
3. Kliknij przycisk **OK**.

ROZDZIAŁ 45

Udostępnianie drukarek

Po przyłączeniu komputera do zarządzanej sieci program EasyNetwork udostępnia wszystkie lokalne drukarki podłączone do komputera, traktując nazwy drukarek jako nazwy drukarek udostępnionych. Ponadto wykrywa drukarki udostępniane przez inne komputery w sieci oraz umożliwia ich konfigurowanie i używanie.

Jeśli sterownik drukarki został skonfigurowany do druku za pośrednictwem sieciowego serwera druku (na przykład bezprzewodowego serwera druku USB), program EasyNetwork traktuje taką drukarkę jako lokalną i udostępnia ją w sieci. Udostępnianie drukarki można zakończyć w każdej chwili.

W tym rozdziale

Praca z udostępnianymi drukarkami

Program EasyNetwork wykrywa drukarki udostępniane przez komputery w sieci. Jeśli program wykryje zdalną drukarkę, która nie jest podłączona do lokalnego komputera, przy pierwszym otwarciu programu EasyNetwork w oknie Udostępniane pliki pojawi się łącze **Dostępne drukarki sieciowe**. Umożliwia ono zainstalowanie dostępnych drukarek lub odinstalowanie drukarek już podłączonych do danego komputera. Można również odświeżyć listę drukarek, aby sprawdzić, czy wyświetlane informacje są aktualne.

Jeśli komputer nie został jeszcze dołączony do zarządzanej sieci, lecz już jest z nią połączony, dostęp do udostępnianych drukarek jest możliwy za pomocą panelu sterowania systemu Windows.

Kończenie udostępniania drukarki

Po zakończeniu udostępniania drukarki elementy nie mogą z niej korzystać.

1. W menu **Narzędzia** kliknij polecenie **Drukarki**.
2. W oknie dialogowym Zarządzanie drukarkami sieciowymi kliknij nazwę drukarki, której udostępnianie ma być zakończone.
3. Kliknij opcję **Nie udostępniaj**.

Instalowanie dostępnej drukarki sieciowej

Elementy zarządzanej sieci mają dostęp do udostępnianych drukarek; muszą jednak zainstalować sterowniki używane przez drukarki. Jeśli właściciel drukarki zakończy jej udostępnianie, nie można z niej korzystać.

1. W menu **Narzędzia** kliknij polecenie **Drukarki**.
2. W oknie dialogowym Dostępne drukarki sieciowe kliknij nazwę drukarki.
3. Kliknij przycisk **Zainstaluj**.

Opis

W Słowniku terminów znajdują się najczęściej stosowane w produktach firmy McAfee terminy związane z bezpieczeństwem oraz ich definicje.

Słownik

8

802.11

Zestaw standardów IEEE określających sposób przesyłania danych w sieci bezprzewodowej. Standard 802.11 określa się często mianem Wi-Fi.

802.11a

Rozszerzenie standardu 802.11 umożliwiające przesyłanie danych z prędkością do 54 Mb/s w paśmie 5 GHz. Prędkość transmisji jest większa niż w przypadku standardu 802.11b, jednak zasięg jest znacznie mniejszy.

802.11b

Rozszerzenie standardu 802.11 umożliwiające przesyłanie danych z prędkością do 11 Mb/s w paśmie 2,4 GHz. Prędkość transmisji jest mniejsza niż w przypadku standardu 802.11a, jednak zasięg jest większy.

802.1x

Standard IEEE określający sposób uwierzytelniania w sieciach przewodowych i bezprzewodowych. Standard 802.1x jest często stosowany w sieciach bezprzewodowych 802.11.

A

ActiveX, formant

Składnik oprogramowania używany przez programy lub strony sieci Web w celu poszerzenia zakresu funkcji. Formant ActiveX jest widoczny jako zintegrowany element programu lub strony sieci Web. Formanty ActiveX są w większości niegroźne, jednak niektóre z nich mogą przechwytywać informacje z komputera.

adres IP

Identyfikator komputera lub urządzenia w sieci TCP/IP. W sieciach działających na podstawie protokołu TCP/IP dane kierowane są na podstawie adresu IP miejsca docelowego. Format adresu IP to 32-bitowa wartość liczbowa zapisana jako cztery liczby oddzielone kropkami. Każda liczba mieści się w przedziale od 0 do 255 (na przykład 192.168.1.100).

Adres MAC

(Media Access Control Address, adres kontroli dostępu do nośnika) Unikatowy numer seryjny przypisany do urządzenia fizycznego z dostępem do sieci.

archiwizacja

Proces tworzenia kopii ważnych plików na dysku CD lub DVD, stacji USB, zewnętrznym dysku twardym lub dysku sieciowym.

archiwizacja pełna

Proces archiwizowania pełnego zestawu danych w zależności od skonfigurowanych typów plików i lokalizacji. Patrz także: archiwizacja szybka.

archiwizacja szybka

Proces archiwizowania tylko tych plików, które uległy zmianie od czasu ostatniej archiwizacji pełnej lub szybkiej. Zobacz też: archiwizacja pełna.

atak słownikowy

Odmiana ataku typu „brute force” wykorzystująca słownik w celu odkrycia hasła.

atak typu „brute force”

Metoda dekodowania zaszyfrowanych danych (np. haseł) przy użyciu znacznego nakładu mocy obliczeniowej (metoda „siłowa”) zamiast inteligentnych strategii. Atak typu „brute force” stanowi podejście niezawodne, ale czasochłonne. Ataki tego rodzaju określa się także mianem łamania zabezpieczeń metodą „brute force”.

atak typu „man-in-the-middle”

Metoda przechwytywania i ewentualnego modyfikowania danych przesyłanych między dwoma stronami, które nie wiedzą o tym, że łącze komunikacyjne między nimi zostało naruszone.

atak typu „phishing”

Internetowe oszustwo mające na celu kradzież cennych informacji (numerów kart kredytowych, numerów ubezpieczenia, identyfikatorów użytkownika, haseł) od niepodejrzewających niczego użytkowników w celu posłużenia się nimi jako fałszywą tożsamością.

atak typu DoS (odmowa usługi)

Typ ataku, który powoduje spowolnienie lub zatrzymanie ruchu w sieci. Atak typu DoS (odmowa usługi) występuje w sytuacji, gdy sieć jest obciążona tyloma dodatkowymi żądaniami, że zwykły ruch jest utrudniony lub zupełnie zablokowany. Zwykle nie wiąże się to z kradzieżą informacji lub wykorzystaniem innych luk w zabezpieczeniach.

B

biała lista

Lista witryn sieci Web, do których dostęp jest dozwolony, ponieważ nie są one uznawane za fałszywe.

biblioteka

Miejsce przechowywania danych w trybie online, w którym można umieścić zarchiwizowane i opublikowane pliki. Biblioteka programu Data Backup to witryna sieci Web dostępna dla wszystkich użytkowników Internetu.

brama zintegrowana

Urządzenie łączące funkcje punktu dostępu, routera i zapory. Niektóre urządzenia mogą posiadać rozszerzenia zabezpieczeń i funkcje mostkowania.

C

czarna lista

W kontekście ochrony przed atakami typu „phishing” — lista witryn sieci Web uważanych za szkodliwe.

D

DAT

Pliki DAT (pliki sygnatur) zawierają definicje używane podczas wykrywania wirusów, koni trojańskich, oprogramowania szpiegującego, oprogramowania reklamowego i innych potencjalnie niepożądanych programów na komputerze lub stacji USB.

dialer

Program, który pomaga w nawiązaniu połączenia internetowego. Dialery używane w celach destrukcyjnych mogą spowodować przekierowanie połączenia internetowego do kogoś innego niż domyślny usługodawca internetowy (ISP) bez poinformowania użytkownika o dodatkowych kosztach.

DNS

(Domain Name System) System przekształcający nazwy hostów lub domen w adresy IP. W sieci Web system DNS służy do konwertowania zrozumiałych adresów sieciowych (na przykład www.mojanazwahosta.com) w adresy IP (na przykład 111.2.3.44) w celu pobrania witryny sieci Web. Bez systemu DNS użytkownik musiałby wpisać adres IP w przeglądarce internetowej.

dodatek

Mały program współpracujący z większym programem w celu rozszerzenia jego funkcjonalności. Dodatki umożliwiają na przykład przeglądarce sieci Web dostęp i wykonywanie operacji na takich plikach osadzonych w dokumentach HTML, których format normalnie nie byłby przez nią rozpoznawany (animacje, pliki wideo, piki audio itd.).

domena

Lokalna podsieć lub deskryptor witryn w Internecie.

W sieci lokalnej (LAN) domena to podsieć składająca się z komputerów klienckich i serwerów, którymi steruje jedna baza danych zabezpieczeń. W tym kontekście domeny pomagają w zwiększeniu wydajności. W Internecie domena to element każdego adresu WWW (na przykład w adresie www.abc.com domena to abc).

dysk inteligentny

Zobacz: stacja USB.

dysk sieciowy

Dysk twardy lub napęd taśmowy podłączony do serwera sieciowego, który jest udostępniany wielu użytkownikom. Dyski sieciowe są czasem nazywane dyskami zdalnymi.

E

ESS

(Extended Service Set) Zestaw dwóch lub więcej sieci tworzących pojedynczą podsieć.

F

filtrowanie obrazów

Opcja funkcji kontroli rodzicielskiej, która umożliwia blokowanie potencjalnie niepożądanych obrazów podczas przeglądania sieci Web.

fragmenty plików

Pozostałości plików rozproszone na dysku. Do fragmentacji dochodzi podczas dodawania i usuwania plików. Fragmentacja może spowolnić działanie komputera.

Funkcje ochrony rodzicielskiej

Ustawienia pomagające decydować, co dzieci będą widzieć i jakie operacje będą mogły wykonywać w trakcie przeglądania sieci Web. Ustawienia obejmują m.in. możliwość filtrowania obrazów, wybór grupy klasyfikacji treści oraz określenie limitów czasowych przeglądania sieci Web.

G

grupy klasyfikacji zawartości

W kontekście funkcji ochrony rodzicielskiej — grupa wiekowa, do której należy użytkownik. Zawartość jest udostępniana lub blokowana w zależności od grupy klasyfikacji zawartości, do której należy dany użytkownik. Grupy klasyfikacji zawartości to: małe dziecko, dziecko, młodszy nastolatek, starszy nastolatek i dorosły.

H

hasło

Kod (zazwyczaj złożony z liter i cyfr) pozwalający na uzyskanie dostępu do komputera, programu lub witryny sieci Web.

I

Internet

Internet to ogromna liczba połączonych ze sobą sieci, które korzystają z protokołów TCP/IP do odnajdywania i przesyłania danych. Internet rozwinął się z połączonych komputerów uniwersyteckich i szkolnych (na przełomie lat 60-tych i 70-tych ubiegłego wieku). Przedsięwzięcie to zostało sfinansowane przez Departament Obrony Stanów Zjednoczonych i było znane pod nazwą ARPANET. Dziś Internet jest ogólnoświatową siecią, na którą składa się prawie 100 000 niezależnych sieci.

intranet

Prywatna sieć komputerowa stanowiąca zazwyczaj wewnętrzną sieć organizacji, do której dostęp mają wyłącznie autoryzowani użytkownicy.

K

karta PCI sieci bezprzewodowej

(PCI = Peripheral Component Interconnect) Karta sieci bezprzewodowej podłączana do gniazda PCI wewnątrz komputera.

karta sieci bezprzewodowej

Urządzenie, dzięki któremu komputer lub asystent PDA uzyskuje możliwość pracy w sieci bezprzewodowej. Podłącza się ją do portu USB, gniazda kart PC Card (CardBus), gniazda karty pamięci lub do wewnętrznej magistrali PCI.

Karta sieciowa

(NIC — Network Interface Card) Karta podłączana do komputera przenośnego lub innego urządzenia, która łączy je z siecią LAN.

karta USB sieci bezprzewodowej

Karta sieci bezprzewodowej podłączana do gniazda USB w komputerze.

klient

Aplikacja działająca na komputerze osobistym lub stacji roboczej i zależna od serwera podczas wykonywania pewnych operacji. Na przykład klient poczty e-mail to aplikacja umożliwiająca wysyłanie i odbieranie wiadomości e-mail.

klient poczty e-mail

Program uruchamiany na komputerze w celu wysyłania i odbierania wiadomości e-mail (na przykład Microsoft Outlook).

klucz

Seria liter i cyfr używana przez dwa urządzenia do uwierzytelniania ich komunikacji. Oba urządzenia muszą posiadać klucz. Patrz także: WEP, WPA, WPA2, WPA-PSK i WPA2- PSK.

kod uwierzytelniania komunikatów (MAC)

Kod zabezpieczeń służący do szyfrowania komunikatów przesyłanych między komputerami. Komunikat jest akceptowany, jeśli komputer docelowy uznaje odszyfrowany kod za poprawny.

kompresja

Proces, w wyniku którego pliki są kompresowane do postaci, w której zajmują mniej miejsca podczas przechowywania lub przesyłania.

koń trojański

Aplikacja sprawiająca wrażenie normalnego programu, ale mogąca spowodować zniszczenie cennych plików, zmniejszenie wydajności i nieuprawniony dostęp do komputera.

Kosz

Wirtualne miejsce na składowanie usuniętych plików i folderów w systemie Windows.

kwarantanna

Izolowanie. Na przykład w aplikacji VirusScan podejrzane pliki są wykrywane i poddawane kwarantannie, dzięki czemu nie stanowią już zagrożenia dla komputera ani pozostałych plików.

L

LAN

(Local Area Network, sieć lokalna) Sieć komputerowa obejmująca stosunkowo niewielki obszar (na przykład pojedynczy budynek). Komputery w sieci LAN komunikują się ze sobą i udostępniają zasoby, takie jak drukarki i pliki.

Launchpad

Składnik interfejsu platformy U3, który służy do uruchamiania programów zgodnych z platformą U3 ze stacji USB i do zarządzania tymi programami.

lista zaufanych

Zawiera wpisy elementów, którym użytkownik ufa, w związku z czym nie są one więcej wykrywane. Jeśli okaże się, że elementowi (np. potencjalnie niepożądanemu programowi lub modyfikacji rejestru) zaufano przez pomyłkę lub jeśli ma on zostać ponownie wykryty, należy usunąć go z tej listy.

lokalizacja monitorowana częściowo

Folder na komputerze, który jest monitorowany przez program Data Backup w celu wykrycia zmian. Po skonfigurowaniu lokalizacji monitorowanej częściowo program Data Backup tworzy kopie zapasowe wszystkich plików monitorowanych typów znajdujących się w tym folderze, ale pomija te w podfolderach.

lokalizacja monitorowana dokładnie

Folder na komputerze, który jest monitorowany przez program Data Backup w celu wykrycia zmian. Po skonfigurowaniu lokalizacji monitorowanej dokładnie program Data Backup tworzy kopie zapasowe wszystkich plików monitorowanych typów znajdujących się w tym folderze i jego podfolderach.

lokalizacje monitorowane

Foldery w komputerze monitorowane przez program Data Backup.

M

magazyn haseł

Bezpieczny obszar pamięci masowej przeznaczony na osobiste hasła. Umożliwia przechowywanie haseł z gwarancją, że nikt inny (nawet administrator) nie ma do nich dostępu.

mapa sieci

Graficzne przedstawienie komputerów i składników tworzących sieć domową.

MAPI

(Messaging Application Programming Interface — interfejs programowy aplikacji komunikacyjnych) Specyfikacja interfejsu firmy Microsoft umożliwiająca różnym aplikacjom komunikacyjnym i aplikacjom dla grup roboczych (między innymi do obsługi poczty e-mail, poczty głosowej i faksów) współpracę z pojedynczym klientem, takim jak klient Exchange.

MSN

(Microsoft Network) Zbiór usług internetowych oferowanych przez firmę Microsoft Corporation. Obejmuje aparat wyszukiwania, moduł poczty e-mail, moduł przesyłania wiadomości błyskawicznych oraz portal.

N

niekontrolowany punkt dostępu

Punkt dostępu, który działa nielegalnie. Niekontrolowane punkty dostępu instaluje się w bezpiecznych sieciach firmowych w celu umożliwienia dostępu do tych sieci nieuprawnionym osobom. Inne zastosowanie to stworzenie napastnikom możliwości przeprowadzenia ataków typu „man-in-the-middle”.

P

pamięć podręczna

Miejsce zapisu tymczasowych danych na komputerze. Na przykład, aby zwiększyć szybkość i sprawność przeglądania sieci Web, przeglądarka przy następnym wyświetlaniu danej strony może ją pobrać z pamięci podręcznej (a nie ze zdalnego serwera).

plik cookie

Mały plik zawierający informacje (najczęściej nazwę użytkownika oraz bieżącą datę i godzinę), który jest przechowywany na komputerze osoby przeglądającej sieć Web. Pliki cookie są używane przede wszystkim przez strony sieci Web w celu identyfikowania użytkowników, którzy zostali wcześniej zarejestrowani w witrynie albo ją odwiedzali. Mogą również stanowić źródło informacji dla hakerów.

plik tymczasowy

Plik tworzony w pamięci lub na dysku przez system operacyjny lub inny program z przeznaczeniem do użycia w ramach bieżącej sesji, a następnie usuwany.

pluskwy internetowe

Małe pliki graficzne osadzające się na stronach HTML i umożliwiające nieautoryzowanym źródłom umieszczanie plików cookie na komputerze użytkownika. Te pliki cookie mogą następnie przesyłać informacje do nieautoryzowanego źródła. Pluskwy internetowe są także nazywane sygnalizatorami sieci Web, tagami pikselowymi, czystymi lub niewidocznymi plikami GIF.

poczta e-mail

(poczta elektroniczna) Wiadomości wysyłane i odbierane elektronicznie w sieci komputerowej. Patrz także: poczta z sieci Web.

Poczta w sieci Web

Wiadomości wysyłane i odbierane elektronicznie (przez Internet). Zobacz też: e-mail.

podszywanie się pod adres IP

Fałszowanie adresu IP znajdującego się w pakiecie IP. To działanie stosowane jest w wielu typach ataków, między innymi w przechwytywaniu sesji. Często fałszowane są nagłówki wiadomości e-mail stanowiących spam, dzięki czemu nie można wyśledzić nadawcy.

POP3

(Post Office Protocol 3) Interfejs między klientem poczty e-mail a serwerem poczty e-mail. Konta POP3 (zwane również standardowymi kontami e-mail) są wykorzystywane przez większość użytkowników domowych.

port

Miejsce, przez które informacje wchodzą do komputera i z niego wychodzą. Na przykład konwencjonalny modem analogowy jest podłączony do portu szeregowego.

potencjalnie niepożądany program (PUP)

Program gromadzący i wysyłający informacje osobiste użytkownika bez jego zgody (np. oprogramowanie szpiegujące albo reklamowe).

PPPoE

(Point-to-Point Protocol Over Ethernet) Metoda wykorzystywania protokołu łączności telefonicznej (PPP), gdzie przesyłanie danych odbywa się przez sieć Ethernet.

protokół

Forma (sprzętowy lub programowy) przesyłania danych między dwoma urządzeniami. Aby komputer/urządzenie użytkownika mogły się kontaktować z innymi komputerami, musi obsługiwać odpowiedni protokół.

proxy

Komputer (lub oprogramowanie na nim uruchomione), który funkcjonuje jako bariera pomiędzy siecią a Internetem, prezentując witrynom zewnętrznym tylko pojedynczy adres sieciowy. Reprezentując wszystkie wewnętrzne komputery, serwer proxy chroni tożsamość komputerów w sieci i jednocześnie umożliwia dostęp do Internetu. Zobacz też: serwer proxy.

przeglądarka

Program używany do wyświetlana stron sieci Web w Internecie. Do popularnych przeglądarek sieci Web należą programy Microsoft Internet Explorer i Mozilla Firefox.

przepełnienie bufora

Stan występujący wtedy, gdy podejrzane programy lub procesy próbują zapisać więcej danych w buforze (miejscu zapisu tymczasowych danych na komputerze), niż może on pomieścić. Przepełnienie buforu może spowodować uszkodzenie lub nadpisanie danych w sąsiednich buforach.

przepustowość

Ilość danych, którą można przesłać w określonym czasie.

przywracanie

Proces przywracania kopii pliku z repozytorium kopii zapasowych online lub z archiwum.

publiczny punkt dostępu

Określona lokalizacja geograficzna objęta zasięgiem punktu dostępu Wi-Fi (802.11). Użytkownicy znajdujący się w zasięgu publicznego punktu dostępu z komputerem przenośnym obsługującym sieć bezprzewodową mogą nawiązać połączenie z Internetem, pod warunkiem że punkt dostępu nadaje sygnał (ujawnia swoją obecność) i nie jest wymagane uwierzytelnianie. Publiczne punkty dostępu znajdują się zwykle w miejscach, w których przebywają duże grupy ludzi, na przykład na lotniskach.

publikowanie

Proces publicznego udostępniania w Internecie pliku, który ma kopię zapasową. W celu uzyskania dostępu do opublikowanych plików należy przeszukać bibliotekę programu Data Backup.

Punkt dostępu

Urządzenie sieciowe (określane często mianem routera bezprzewodowego), które jest podłączane do przełącznika lub koncentratora sieci Ethernet w celu poszerzenia fizycznego zasięgu usługi dla użytkowników bezprzewodowych. Gdy użytkownicy bezprzewodowi przemieszczają się wraz ze swoimi urządzeniami mobilnymi, transmisja jest przekazywana z jednego punktu dostępu do innego w celu zachowania łączności.

punkt przywracania systemu

Migawka (obraz) zawartości pamięci komputera lub bazy danych. System Windows tworzy punkty przywracania systemu w regularnych odstępach czasu oraz w reakcji na poważne zdarzenia systemowe (np. przy instalacji programu lub sterownika). Użytkownik w każdej chwili może utworzyć i nazwać własny punkt przywracania.

R

RADIUS

(Remote Access Dial-In User Service) Protokół umożliwiający uwierzytelnianie użytkowników, zwykle podczas sesji zdalnego dostępu. Pierwotnie przeznaczony dla serwerów telefonicznego dostępu zdalnego, obecnie jest stosowany w wielu środowiskach uwierzytelniania, między innymi w uwierzytelnianiu 802.1x ze współdzielonym hasłem użytkownika sieci WLAN.

rejestr

Baza danych, w której system Windows przechowuje swoje informacje konfiguracyjne. Rejestr zawiera profile wszystkich użytkowników komputera, informacje o zainstalowanym sprzęcie i programach oraz ustawienia właściwości. System Windows w trakcie działania stale odwołuje się do tych informacji.

repozytorium kopii zapasowych online

Lokalizacja na serwerze online, w której są przechowywane powstające kopie zapasowe plików.

roaming

Przemieszczanie się z obszaru zasięgu jednego punktu dostępu do drugiego, bez zakłócania dostępu do usług lub utraty połączenia.

robak

Samopowielający się wirus, który ładuje się do aktywnej pamięci komputera i może rozsyłać swoje kopie za pomocą poczty e-mail. Robaki replikują się i zużywają zasoby systemu, spowalniając lub zatrzymując zadania.

rootkit

Zbiór narzędzi (programów) przyznających użytkownikowi uprawnienia administratora wobec komputera lub sieci komputerowej. Mogą to być aplikacje szpiegujące i inne potencjalnie niepożądane programy, które zagrażają bezpieczeństwu danych na komputerze lub poufności informacji osobistych.

router

Urządzenie sieciowe przekazujące pakiety danych z jednej sieci do drugiej. W oparciu o wewnętrzne tablice routingu routery analizują każdy przychodzący pakiet i na podstawie wszelkich możliwych kombinacji źródłowych i docelowych adresów oraz bieżących warunków ruchu w sieci (obciążenie, koszty połączenia, uszkodzenia łączy) wybierają sposób przekazania go. Czasami router jest nazywany „punktem dostępu”.

S

serwer

Komputer lub program, który akceptuje połączenia od innych komputerów lub programów, a następnie zwraca im właściwe odpowiedzi. Na przykład, zawsze gdy chcesz wysłać lub odebrać wiadomość e-mail, aplikacja pocztowa na Twoim komputerze łączy się z serwerem pocztowym.

serwer DNS

(serwer systemu Domain Name System) Komputer, który zwraca adres IP powiązany z nazwą hosta lub domeny. Patrz także: DNS.

serwer proxy

Składnik zapory zarządzający ruchem internetowym do i z sieci lokalnej (LAN). Serwer proxy może poprawić wydajność, dostarczając często żądane dane, takie jak popularne strony sieci Web. Może on również filtrować i odrzucać żądania uważane za niewłaściwe, takie jak żądania nieautoryzowanego dostępu do plików zastrzeżonych.

sieć

Zbiór punktów dostępu i powiązanych z nimi użytkowników, czyli środowisko ESS.

sieć domowa

Dwa lub większa liczba komputerów połączonych ze sobą w domu w celu udostępniania plików i połączenia internetowego. Patrz także: LAN.

sieć zarządzana

Sieć domowa z dwoma typami użytkowników: użytkownikami zarządzanymi i użytkownikami niezarządzanymi. Użytkownicy zarządzani zezwalają na monitorowanie swojego stanu ochrony przez inne komputery w sieci; użytkownicy niezarządzani — nie zezwalają na to.

skanowanie na żądanie

Skanowanie inicjowane przez użytkownika. W odróżnieniu od skanowania w czasie rzeczywistym skanowanie na żądanie nie jest uruchamiane automatycznie.

skanowanie w czasie rzeczywistym

Skanowanie plików i folderów w poszukiwaniu wirusów i innych przejawów aktywności w czasie, gdy użytkownik lub komputer próbuje uzyskać dostęp do tych plików/folderów.

skrót

Plik zawierający wyłącznie informację o lokalizacji innego pliku na komputerze.

skrypt

Lista poleceń, które mogą być wykonywane automatycznie (tzn. bez udziału użytkownika). W odróżnieniu od programów skrypty są zazwyczaj przechowywane w postaci zwykłego tekstu i kompilowane dopiero po wywołaniu. Mianem skryptów są również określane pliki wsadowe i makra.

słowo kluczowe

Słowo, które można przypisać do pliku posiadającego kopię zapasową w celu ustanowienia zależności lub połączenia z innymi plikami, do których przypisano to samo słowo kluczowe. Przypisywanie słów kluczowych do plików ułatwia wyszukiwanie plików opublikowanych w Internecie.

SMTP

(Simple Mail Transfer Protocol) Protokół TCP/IP służący do przesyłania wiadomości z jednego komputera w sieci do drugiego. Ten protokół jest używany w Internecie do przesyłania wiadomości e-mail.

SSID

(Service Set Identifier) Token (tajny klucz) identyfikujący sieć Wi-Fi (802.11). Identyfikator SSID jest ustalany przez administratora sieci. Użytkownicy chcący uzyskać dostęp do tej sieci muszą go podać podczas logowania.

SSL

(Secure Sockets Layer) Opracowany przez firmę Netscape protokół służący do przesyłania prywatnych dokumentów w Internecie. Protokół SSL działa, korzystając z publicznego klucza do szyfrowania danych, które są następnie przesyłane połączeniem SSL. Adresy URL wymagające połączenia SSL rozpoczynają się przedrostkiem https zamiast http.

Stacja USB

Niewielki dysk pamięci masowej wtykany do portu USB w komputerze. Stacja USB działa jak mały dysk twardy, który pozwala na sprawne przenoszenie plików między komputerami.

standardowe konto e-mail

Zobacz: POP3.

synchronizacja

Proces usuwania rozbieżności pomiędzy plikami przechowywanymi na lokalnym komputerze a ich kopiami zapasowymi. Synchronizacja jest wykonywana, gdy wersja pliku w repozytorium kopii zapasowych online jest nowsza niż ta znajdująca się w innych komputerach.

SystemGuard

Aplikacje McAfee, które wykrywają nieautoryzowane zmiany w komputerze i powiadamiają użytkownika w chwili ich wystąpienia.

szyfrowanie

Proces transformacji danych z tekstu na kod, mający na celu uniemożliwienie odczytania informacji przez osoby, które nie znają metody jego odszyfrowania. Dane przekształcone w ten sposób określa się także mianem tekstu zaszyfrowanego.

T

tekst zaszyfrowany

Tekst, który został zaszyfrowany. Tekstu zaszyfrowanego nie można odczytać, dopóki nie zostanie on przekonwertowany na zwykły tekst (odszyfrowany).

TKIP

(Temporal Key Integrity Protocol) Protokół eliminujący luki w zabezpieczeniach WEP, w szczególności podczas ponownego użycia kluczy szyfrowania. Protokół TKIP zmienia klucze tymczasowe co 10 000 pakietów, zapewniając metodę dynamicznej dystrybucji, która znacząco zwiększa bezpieczeństwo sieci. Proces zabezpieczeń TKIP rozpoczyna się 128-bitowym kluczem tymczasowym współdzielonym przez klientów i punkty dostępu. Protokół TKIP łączy klucz tymczasowy z adresem MAC komputera klienckiego, a następnie dodaje stosunkowo duży 16-oktetowy wektor inicjowania. W efekcie powstaje klucz szyfrujący dane. Ta procedura gwarantuje, że każda stacja do szyfrowania danych używa strumieni o innym kluczu. Protokół TKIP do szyfrowania używa algorytmu RC4.

tworzenie kopii zapasowej

Proces tworzenia kopii ważnych plików na bezpiecznym serwerze w trybie online.

typy monitorowanych plików

Typy plików (na przykład .doc, .xls itd.) znajdujących się w lokalizacjach monitorowanych, dla których program Data Backup tworzy kopie zapasowe lub które archiwizuje.

U

U3

(You: Simplified, Smarter, Mobile) Platforma umożliwiająca uruchamianie programów dla środowisk Windows 2000 i Windows XP bezpośrednio z dysków USB. Inicjatywa U3 została zapoczątkowana w 2004 r. przez firmy M-Systems i SanDisk. Jej celem jest stworzenie użytkownikom programów zgodnych ze standardem U3 możliwości uruchamiania programów na komputerach z systemem Windows bez konieczności wykonywania jakichkolwiek czynności konfiguracyjnych ani zapisywania danych konfiguracyjnych na tych komputerach.

udostępnianie

Umożliwianie odbiorcom wiadomości e-mail uzyskanie przez określony czas dostępu do wybranych kopii zapasowych plików. Podczas udostępniania pliku kopia zapasowa pliku jest wysyłana do określonych odbiorców wiadomości e-mail. Odbiorcy otrzymują wiadomość e-mail od programu Data Backup informującą, że udostępniono im pliki. Wiadomość e-mail zawiera również łącze do udostępnionych plików.

URL

(Uniform Resource Locator) Standardowy format adresów internetowych.

USB

(Universal Serial Bus) Ujednolicony interfejs szeregowy komputera umożliwiający podłączanie różnych urządzeń peryferyjnych: klawiatur, joysticków, drukarek itd.

uwierzytelnianie

Proces identyfikacji osoby, na ogół oparty na weryfikacji unikatowej nazwy i hasła.

V

VPN

(Virtual Private Network) Prywatna sieć skonfigurowana wewnątrz sieci publicznej i wykorzystująca jej mechanizmy zarządzania. Sieci VPN są wykorzystywane przez firmy do budowania sieci rozległych (WAN) obejmujących swoim zasięgiem duże terytoria w celu zapewnienia łączności między poszczególnymi oddziałami lub umożliwienia użytkownikom mobilnym dostępu do firmowych sieci lokalnych.

W

wardriver

Osoba, która wyszukuje sieci Wi-Fi (802.11) za pomocą komputera obsługującego ten standard oraz specjalistycznego sprzętu lub oprogramowania, jeżdżąc po mieście.

WEP

(Wired Equivalent Privacy) Protokół szyfrowania i uwierzytelniania zdefiniowany jako część standardu Wi-Fi (802.11). Wczesne wersje są oparte na algorytmach szyfrowania RC4 i mają istotne wady. Protokół WEP stara się zapewnić bezpieczeństwo poprzez szyfrowanie danych przesyłanych drogą radiową, dzięki czemu są one chronione podczas przesyłania z jednego punktu do drugiego. Jednak praktyka pokazała, że protokół WEP nie jest tak bezpieczny, jak kiedyś sądzono.

węzeł

Pojedynczy komputer podłączony do sieci.

Wi-Fi

(Wireless Fidelity) Pojęcie stosowane przez organizację Wi-Fi Alliance w odniesieniu do każdej sieci typu 802.11.

Wi-Fi Alliance

Organizacja, w której skład wchodzą najważniejsi producenci sprzętu i oprogramowania do komunikacji bezprzewodowej. Jej celem jest weryfikowanie wszystkich urządzeń sieci 802.11 pod kątem zdolności współdziałania oraz promowanie pojęcia „Wi-Fi” jako globalnej marki dla wszystkich urządzeń tworzących sieci LAN zgodne ze standardem 802.11. Organizacja działa jako konsorcjum, laboratorium testowe i izba rozrachunkowa dla dostawców, którzy chcą wspierać rozwój branży.

Wi-Fi Certified

Urządzenie sprawdzone i zatwierdzone przez organizację Wi-Fi Alliance. Produkty oznaczone logo Wi-Fi Certified uważa się za zgodne ze sobą, mimo iż mogą pochodzić od różnych producentów. Jeśli oba produkty noszą oznaczenie Wi-Fi Certified, użytkownik może korzystać z punktu dostępu dowolnego producenta w połączeniu ze sprzętem klienckim innego dowolnego producenta.

wirus

Samopowielający się program, który może modyfikować pliki lub dane użytkownika. Wirusy często sprawiają wrażenie pochodzących od zaufanego nadawcy lub zawierających nieszkodliwą zawartość.

WLAN

(Wireless Local Area Network) Sieć lokalna korzystająca z połączeń bezprzewodowych. W sieci WLAN do komunikacji pomiędzy komputerami zamiast przewodów stosuje się fale radiowe o wysokiej częstotliwości.

WPA

(Wi-Fi Protected Access) Standard znacznie zwiększający poziom ochrony danych i kontroli dostępu w istniejących i przyszłych systemach bezprzewodowej sieci LAN. Zaprojektowany do pracy na istniejącym sprzęcie jako aktualizacja oprogramowania, standard WPA pochodzi od standardu IEEE 802.11i i jest z nim kompatybilny. Po prawidłowej instalacji gwarantuje użytkownikom bezprzewodowej sieci LAN, że ich dane są chronione, a do sieci mają dostęp tylko autoryzowani użytkownicy.

WPA-PSK

Specjalny tryb WPA zaprojektowany dla użytkowników indywidualnych, którzy nie wymagają silnych zabezpieczeń klasy korporacyjnej i nie posiadają dostępu do serwerów uwierzytelniania. W tym trybie użytkownik indywidualny wprowadza hasło początkowe służące do aktywacji standardu Wi-Fi Protected Access z zastosowaniem klucza wstępnego. Hasło należy regularnie zmieniać na każdym komputerze bezprzewodowym i punkcie dostępu. Patrz także WPA2-PSK i TKIP.

WPA2

Nowsza wersja standardu zabezpieczeń WPA, bazująca na standardzie 802.11i IEEE.

WPA2-PSK

Specjalny tryb WPA bazujący na standardzie WPA2, podobny do standardu WPA-PSK. Popularną cechą urządzeń korzystających ze standardu WPA2-PSK jest ich zdolność do obsługi kilku trybów szyfrowania jednocześnie (np. AES, TKIP), podczas gdy starsze urządzenia na ogół obsługują tylko jeden tryb szyfrowania (tzn. wszystkie komputery klienckie muszą korzystać z tego samego trybu szyfrowania).

współdzielone hasło

Ciąg tekstowy lub klucz (zazwyczaj hasło) ustalony wspólnie przez dwie strony przed zainicjowaniem komunikacji. Zadaniem współdzielonego hasła jest ochrona poufnych części komunikatów RADIUS.

wyskakujące okna

Niewielkie okna pojawiające się na tle innych okien na ekranie komputera. Wyskakujące okna są często używane w przeglądarkach sieci Web do wyświetlania reklam.

Z

zapora

System (sprzętowy, programowy lub sprzętowo-programowy) zaprojektowany w celu zapobiegania nieautoryzowanemu dostępowi do lub z sieci prywatnej. Zapory są często stosowane w celu uniemożliwienia nieautoryzowanym użytkownikom Internetu uzyskania dostępu do sieci prywatnych podłączonych do Internetu, w szczególności sieci intranet. Wszystkie wiadomości wchodzące do intranetu i wychodzące z niego przechodzą przez zaporę, która analizuje każdą wiadomość i blokuje te, które nie spełniają określonych kryteriów zabezpieczeń.

zdarzenie

Zdarzenie zainicjowane przez użytkownika, urządzenie lub komputer, które wywołuje określoną reakcję. W programie McAfee zdarzenia są rejestrowane w dzienniku zdarzeń.

zewnętrzny dysk twardy

Dysk twardy znajdujący się na zewnątrz komputera.

zwykły tekst

Tekst, który nie jest zaszyfrowany. Zobacz też: szyfrowanie.

Informacje o firmie McAfee

Firma McAfee, Inc. z siedzibą w Santa Clara w Kalifornii, będąca światowym liderem w dziedzinie ochrony przed włamaniami i zarządzania ryzykiem wystąpienia zagrożeń, dostarcza proaktywne i sprawdzone rozwiązania i usługi służące zabezpieczaniu systemów i sieci na całym świecie. Dzięki bogatemu doświadczeniu w dziedzinie bezpieczeństwa oraz zaangażowaniu w dostarczanie innowacyjnych technologii firma McAfee daje użytkownikom indywidualnym, firmom i usługodawcom możliwość blokowania ataków, zapobiegania zakłóceniom oraz ciągłego śledzenia i ulepszania stanu swoich zabezpieczeń.

Copyright

Licencja

UWAGA DLA WSZYSTKICH UŻYTKOWNIKÓW: NALEŻY UWAŻNIE PRZECZYTAĆ ODPOWIEDNIĄ UMOWĘ PRAWNĄ (ZWIĄZANĄ Z NABYTĄ LICENCJĄ), W KTÓREJ OPISANE SĄ OGÓLNE WARUNKI UŻYTKOWANIA LICENCJONOWANEGO OPROGRAMOWANIA. W PRZYPADKU WĄTPLIWOŚCI CO DO TYPU UZYSKANEJ LICENCJI NALEŻY ZAPOZNAĆ SIĘ Z DOKUMENTAMI SPRZEDAŻY LUB INNYMI POKREWNYMI DOKUMENTAMI LICENCYJNYMI BĄDŹ ZAMÓWIENIAMI ZAKUPU DOŁĄCZONYMI DO OPAKOWANIA OPROGRAMOWANIA ALBO OTRZYMANYMI ODDZIELNIE W RAMACH ZAKUPU (W FORMIE KSIĄŻECZKI, PLIKU NA DYSKU CD Z PRODUKTEM ALBO PLIKU DOSTĘPNEGO NA STRONIE INTERNETOWEJ, Z KTÓREJ ZOSTAŁ POBRANY PAKIET OPROGRAMOWANIA). JEŚLI NIE SĄ AKCEPTOWANE WSZYSTKIE WARUNKI ZAWARTE W NINIEJSZEJ UMOWIE, NIE NALEŻY INSTALOWAĆ OPROGRAMOWANIA. JEŚLI JEST TO ZGODNE Z WARUNKAMI SPRZEDAŻY, W PRZYPADKU NIEZAAKCEPTOWANIA UMOWY MOŻNA ZWRÓCIĆ PRODUKT DO FIRMY MCAFEE, INC. LUB MIEJSCA ZAKUPU I OTRZYMAĆ CAŁKOWITY ZWROT KOSZTÓW.

ROZDZIAŁ 46

Biuro obsługi klienta i pomoc techniczna

Program SecurityCenter zgłasza krytyczne i niekrytyczne problemy dotyczące ochrony natychmiast po ich wykryciu. Krytyczne problemy dotyczące ochrony wymagają niezwłocznego działania i powodują obniżenie stanu ochrony (kolor jest zmieniany na czerwony). Niekrytyczne problemy dotyczące ochrony nie wymagają niezwłocznego działania i nie muszą, choć mogą, skutkować obniżeniem stanu ochrony (zależy to od typu problemu). Aby osiągnąć zielony stan ochrony, należy naprawić wszystkie problemy krytyczne oraz naprawić lub zignorować wszystkie problemy niekrytyczne. Jeśli potrzebna jest pomoc w diagnozowaniu problemów dotyczących ochrony, można uruchomić narzędzie McAfee Virtual Technician. Aby uzyskać więcej informacji na temat narzędzia McAfee Virtual Technician, zobacz Pomoc tego narzędzia.

Jeśli oprogramowanie zabezpieczające zostało kupione od partnera lub dostawcy innego niż firma McAfee, otwórz przeglądarkę sieci Web i przejdź do witryny www.mcafeepomoc.com. Następnie w sekcji Partner Links zaznacz odpowiedniego partnera lub usługodawcę, co spowoduje zainicjowanie narzędzia McAfee Virtual Technician.

Uwaga: Aby zainstalować narzędzie McAfee Virtual Technician i go używać, należy się zalogować na swoim komputerze jako administrator systemu Windows. W przeciwnym razie narzędzie może nie być w stanie rozwiązywać problemów. Aby uzyskać informacje na temat logowania się jako administrator systemu Windows, zobacz Pomoc systemu Windows. W systemie Windows Vista™ po uruchomieniu narzędzia MVT jest wyświetlany monit. W oknie monitu należy kliknąć przycisk **Akceptuję**. Narzędzie Virtual Technician nie współpracuje z przeglądarką Mozilla® Firefox.

W tym rozdziale

Korzystanie z narzędzia McAfee Virtual Technician

Narzędzie Virtual Technician, podobnie jak pracownik biura obsługi technicznej, gromadzi informacje na temat programów SecurityCenter, aby rozwiązać problemy dotyczące ochrony komputera. Po uruchomieniu narzędzie Virtual Technician sprawdza, czy programy SecurityCenter działają właściwie. W przypadku wykrycia problemów narzędzie przedstawia propozycje ich naprawienia lub szczegółowe informacje na ich temat. Po zakończeniu tego etapu narzędzie Virtual Technician wyświetla wyniki przeprowadzonej analizy i, jeśli to konieczne, pozwala uzyskać dalszą pomoc techniczną od firmy McAfee.

Aby zachować bezpieczeństwo oraz integralność komputera i plików, aplikacja nie gromadzi danych osobowych umożliwiających identyfikację użytkownika.

Uwaga: Aby uzyskać więcej informacji na temat narzędzia Virtual Technician, należy kliknąć ikonę **Pomoc** w tym narzędziu.

Uruchamianie narzędzia Virtual Technician

Narzędzie Virtual Technician gromadzi informacje na temat programów SecurityCenter, aby rozwiązać problemy dotyczące ochrony komputera. Aby chronić prywatność użytkownika, informacje te nie obejmują danych osobowych umożliwiających jego identyfikację.

1. W obszarze **Typowe zadania** kliknij opcję **McAfee Virtual Technician**.
2. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, aby pobrać i uruchomić narzędzie Virtual Technician.

Pomoc techniczna i produkty do pobrania

Aby uzyskać informacje o witrynach firmy McAfee dotyczących pomocy technicznej i produktów do pobrania (w tym podręczników użytkownika), skorzystaj z tabel zamieszczonych poniżej.

Pomoc techniczna i produkty do pobrania

Kraj	McAfee — Pomoc techniczna	McAfee — Produkty do pobrania
Australia	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brazylia	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Kanada (angielski)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Kanada (francuski)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Chiny (kontynentalne)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
Chiny (Tajwan)	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Czechy	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Dania	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Finlandia	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
Francja	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
Niemcy	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Wielka Brytania	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
Włochy	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
Japonia	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
Korea	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
Meksyk	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
Norwegia	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp

Polska	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp
Portugalia	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
Hiszpania	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Szwecja	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Turcja	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
Stany Zjednoczone	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

Podręczniki użytkownika pakietu McAfee Total Protection

Kraj	Podręczniki użytkownika oprogramowania McAfee
Australia	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brazylia	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Kanada (angielski)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
Kanada (francuski)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
Chiny (kontynentalne)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
Chiny (Tajwan)	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Czechy	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Dania	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Finlandia	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
Francja	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Niemcy	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Wielka Brytania	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
Holandia	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
Włochy	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf

Japonia	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Meksyk	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Norwegia	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
Polska	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
Portugalia	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
Hiszpania	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Szwecja	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Turcja	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
Stany Zjednoczone	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

Podręczniki użytkownika pakietu McAfee Internet Security

Kraj	Podręczniki użytkownika oprogramowania McAfee
Australia	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brazylia	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
Kanada (angielski)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
Kanada (francuski)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
Chiny (kontynentalne)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
Chiny (Tajwan)	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Czechy	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Dania	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Finlandia	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf

Francja	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
Niemcy	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf
Wielka Brytania	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Holandia	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
Włochy	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
Japonia	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
Meksyk	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Norwegia	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
Polska	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
Portugalia	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
Hiszpania	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Szwecja	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Turcja	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
Stany Zjednoczone	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

Podręczniki użytkownika programu McAfee VirusScan Plus

Kraj	Podręczniki użytkownika oprogramowania McAfee
Australia	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brazylia	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Kanada (angielski)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
Kanada (francuski)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
Chiny (kontynentalne)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf

Chiny (Tajwan)	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
Czechy	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf
Dania	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Finlandia	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
Francja	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Niemcy	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Wielka Brytania	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Holandia	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
Włochy	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Japonia	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Meksyk	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Norwegia	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
Polska	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
Portugalia	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
Hiszpania	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Szwecja	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Turcja	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
Stany Zjednoczone	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

Podręczniki użytkownika programu McAfee VirusScan

Kraj	Podręczniki użytkownika oprogramowania McAfee

Australia	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Brazylia	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
Kanada (angielski)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf
Kanada (francuski)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
Chiny (kontynentalne)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
Chiny (Tajwan)	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Czechy	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Dania	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Finlandia	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
Francja	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Niemcy	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Wielka Brytania	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
Holandia	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
Włochy	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Japonia	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Meksyk	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Norwegia	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
Polska	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
Portugalia	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
Hiszpania	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Szwecja	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Turcja	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
Stany Zjednoczone	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

W tabeli poniżej przedstawiono Centrum zagrożeń firmy McAfee oraz witryny z informacjami o wirusach dostępne w poszczególnych krajach.

Kraj	Centrala bezpieczeństwa	Informacje o wirusach
Australia	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brazylia	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Kanada (angielski)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Kanada (francuski)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Chiny (kontynentalne)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
Chiny (Tajwan)	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Czechy	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Dania	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Finlandia	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
Francja	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
Niemcy	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Wielka Brytania	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
Holandia	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
Włochy	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Japonia	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
Korea	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
Meksyk	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Norwegia	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
Polska	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
Portugalia	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
Hiszpania	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Szwecja	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Turcja	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
Stany Zjednoczone	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

W tabeli poniżej przedstawiono witryny HackerWatch dostępne w poszczególnych krajach.

Kraj	HackerWatch
Australia	www.hackerwatch.org
Brazylia	www.hackerwatch.org/?lang=pt-br
Kanada (angielski)	www.hackerwatch.org
Kanada (francuski)	www.hackerwatch.org/?lang=fr-ca
Chiny (kontynentalne)	www.hackerwatch.org/?lang=zh-cn
Chiny (Tajwan)	www.hackerwatch.org/?lang=zh-tw
Czechy	www.hackerwatch.org/?lang=cs
Dania	www.hackerwatch.org/?lang=da
Finlandia	www.hackerwatch.org/?lang=fi
Francja	www.hackerwatch.org/?lang=fr
Niemcy	www.hackerwatch.org/?lang=de
Wielka Brytania	www.hackerwatch.org
Holandia	www.hackerwatch.org/?lang=nl
Włochy	www.hackerwatch.org/?lang=it
Japonia	www.hackerwatch.org/?lang=jp
Korea	www.hackerwatch.org/?lang=ko
Meksyk	www.hackerwatch.org/?lang=es-mx
Norwegia	www.hackerwatch.org/?lang=no
Polska	www.hackerwatch.org/?lang=pl
Portugalia	www.hackerwatch.org/?lang=pt-pt
Hiszpania	www.hackerwatch.org/?lang=es
Szwecja	www.hackerwatch.org/?lang=sv
Turcja	www.hackerwatch.org/?lang=tr
Stany Zjednoczone	www.hackerwatch.org

Indeks

F

G

H

I

J

K

R

S

Ś

T

U

V

W

Z