McAfee®

VirusScan® Plus

AntiVirus, Firewall & AntiSpyware

Podręcznik użytkownika

Spis treści

ROZDZIAŁ 1

Wprowadzenie

Uzbrój komputer w połączone zabezpieczenia firmy McAfee, takie jak zapory, funkcje skanowania wirusów i technologie ochrony przed programami szpiegującymi. Program VirusScan Plus umożliwia ochronę komputera przed wirusami, monitorowanie ruchu internetowego w poszukiwaniu podejrzanych połączeń i blokowanie programów szpiegujących zagrażających integralności informacji osobistych użytkownika.

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

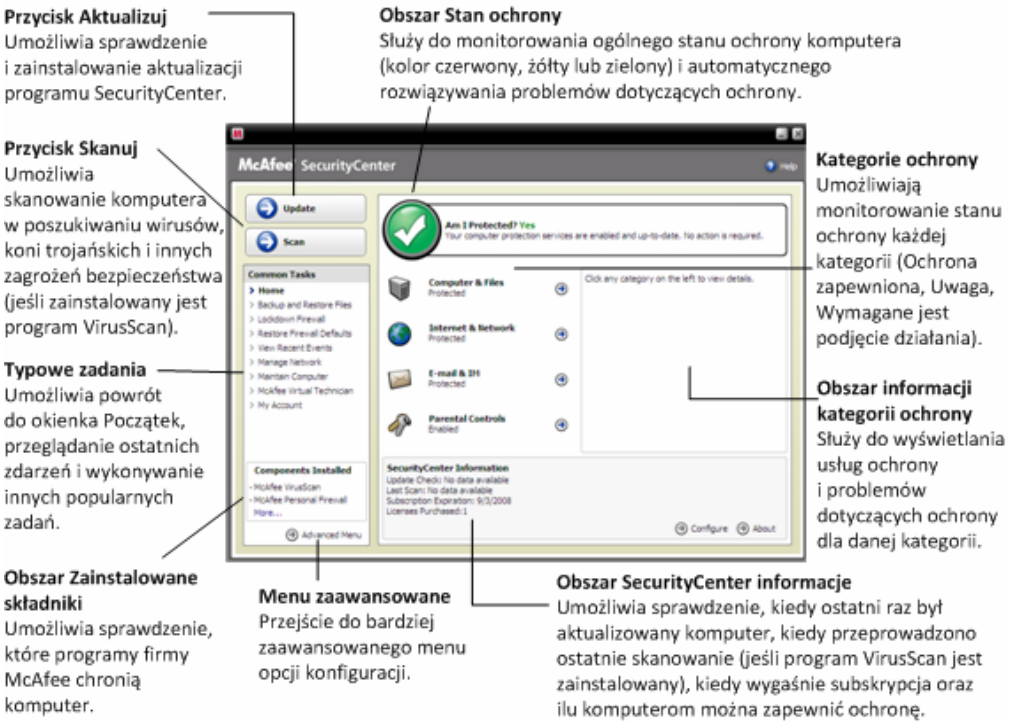
Funkcje programu SecurityCenter

Uproszczone informacje o stanie ochrony	Łatwe przeglądanie informacji o stanie ochrony komputera, sprawdzanie dostępności aktualizacji i usuwanie problemów związanych z ochroną.
Zautomatyzowane aktualizacje i uaktualnienia	Program SecurityCenter automatycznie pobiera i instaluje aktualizacje programów. Gdy tylko zostaje udostępniona nowa wersja programu firmy McAfee, jest ona dostarczana automatycznie do komputera użytkownika przez okres ważności subskrypcji w celu zapewnienia aktualnej ochrony.
Alerty wyświetlane na bieżąco	Alerty zabezpieczeń powiadamiają o masowych infekcjach wirusowych i zagrożeniach bezpieczeństwa.

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 oprogramowaniem szpiegującym ▪ SystemGuard ▪ Ochrona systemu Windows ▪ Stan komputera
Internet i sieć	Kategoria Internet i sieć umożliwia skonfigurowanie następujących usług ochrony: ▪ Ochrona przy użyciu zapory ▪ Ochrona przed atakami typu „phishing” ▪ Ochrona tożsamości
Poczta e-mail i wiadomości błyskawiczne	Kategoria Poczta e-mail i wiadomości błyskawiczne umożliwia skonfigurowanie następujących usług ochrony: ▪ Ochrona przed wirusami w wiadomościach e-mail ▪ Ochrona przed wirusami w wiadomościach błyskawicznych ▪ Ochrona przed oprogramowaniem szpiegującym w wiadomościach e-mail ▪ Ochrona przed oprogramowaniem szpiegującym w wiadomościach błyskawicznych ▪ Ochrona przed spamem
Funkcje ochrony rodzicielskiej	Kategoria Funkcje ochrony rodzicielskiej umożliwia skonfigurowanie następujących usług ochrony: ▪ Blokowanie zawartości

Jak działają usługi ochrony

Usługi ochrony to różne składniki ochrony konfigurowane przez użytkownika w celu zapewnienia ochrony komputera. Usługi ochrony odpowiadają bezpośrednio programom firmy McAfee. Na przykład po zainstalowaniu programu VirusScan dostępne są następujące usługi: Virus Protection, Spyware Protection, SystemGuards i Script Scanning. 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 ochrony rodzicielskiej 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 subskrypcjami

Każdy zakupiony produkt ochronny firmy McAfee dostarczany jest z subskrypcją pozwalającą na używanie tego produktu na określonej liczbie komputerów przez określony czas. Czas trwania subskrypcji zależy od dokonanego zakupu, ale zwykle zaczyna się od momentu aktywowania produktu. Aktywacja jest prosta i bezpłatna — wymagane jest tylko połączenie z Internetem. Jest jednak bardzo ważna, ponieważ uprawnia do otrzymywania regularnych, automatycznych aktualizacji produktu w celu zapewnienia ochrony komputera przed najnowszymi zagrożeniami.

Aktywacja jest zwykle przeprowadzana po zainstalowaniu produktu, jeżeli jednak zostanie opóźniona (na przykład z powodu braku połączenia z Internetem), można ją przeprowadzić w ciągu 15 dni. Jeżeli aktywacja nie zostanie przeprowadzona w ciągu 15 dni, dla produktu nie będą dostarczane najważniejsze aktualizacje i nie będzie wykonywane skanowanie. Przed wygaśnięciem subskrypcji będą pojawiały się okresowe powiadomienia w postaci komunikatów ekranowych. Dzięki temu można uniknąć przerw w ochronie przez jej wczesne odnowienie lub skonfigurowanie w naszej witrynie sieci Web służącej do automatycznego odnawiania subskrypcji.

Jeżeli w programie SecurityCenter widoczne jest łącze do aktywacji, oznacza to, ze subskrypcja nie została aktywowana. Datę wygaśnięcia subskrypcji można sprawdzić na stronie konta użytkownika.

Dostęp do konta McAfee

Dostęp do informacji o koncie McAfee (strona konta użytkownika) można łatwo uzyskać za pomocą programu SecurityCenter.

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

Aktywacja produktu

Aktywacja jest zwykle przeprowadzana po zainstalowaniu produktu. Jeżeli nie została przeprowadzona, w programie SecurityCenter widoczne jest łącze do aktywacji. Będą także pojawiały się okresowe powiadomienia.

- W okienku Strona główna programu SecurityCenter w obszarze **SecurityCenter — informacje** kliknij opcję **Aktywuj subskrypcję**.

Wskazówka: Możliwe jest także przejście do aktywacji z okresowo wyświetlanych alertów.

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**.

Odnawianie subskrypcji

Na krótko przed wygaśnięciem subskrypcji w programie SecurityCenter widoczne jest łącze do jej odnowienia. Będą także pojawiały się okresowe powiadomienia o wygasaniu subskrypcji.

- W okienku Strona główna programu SecurityCenter w obszarze **SecurityCenter — informacje** kliknij opcję **Odnów**.

Wskazówka: Możliwe jest także przejście do odnowienia produktu z okresowo wyświetlanych komunikatów z powiadomieniem. Alternatywnie można przejść do strony konta, na której można odnowić subskrypcję lub skonfigurować jej automatyczne odnawianie.

ROZDZIAŁ 4

Aktualizowanie oprogramowania SecurityCenter

Program SecurityCenter zapewnia najnowszą wersję zarejestrowanych programów firmy McAfee przez sprawdzanie ich dostępności i instalowanie aktualizacji w trybie online co cztery godziny. W zależności od zainstalowanych i aktywowanych programów aktualizacje online mogą obejmować najnowsze definicje wirusów oraz uaktualnienia dotyczące 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: Jeżeli produkt firmy McAfee został zainstalowany z dysku CD, aktywację należy przeprowadzić w ciągu 15 dni. W przeciwnym razie dla produktu nie będą dostarczane najważniejsze aktualizacje i nie będzie wykonywane skanowanie.

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 21).

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

Wyłączając 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**.
3. W oknie dialogowym potwierdzenia kliknij przycisk **Tak**.

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 naprawianych automatycznie, ale niektóre problemy wymagają interwencji użytkownika. Jeśli na przykład 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	Działanie
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 aktywowany i nie może uzyskać pełnej ochrony.	Aktywacja programu w witrynie sieci Web firmy McAfee.
Subskrypcja wygasła.	Sprawdzenie stanu swojego konta w witrynie sieci Web firmy McAfee. Aby uzyskać więcej informacji, zobacz Zarządzanie subskrypcjami (strona 10).

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 27).

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 ochrony rodzicielskiej) 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**.

Ukrywanie komunikatów zabezpieczeń

Możliwe jest ukrycie powiadomień o zabezpieczeniach dotyczących ochrony większej liczby komputerów w sieci domowej. Te komunikaty zawierają informacje o subskrypcji, liczbie komputerów, które można chronić przy użyciu subskrypcji, i sposobie rozszerzenia subskrypcji do ochrony większej liczby komputerów.

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 **Pokaż zalecenia dotyczące wirusów lub inne komunikaty zabezpieczeń**.

Wskazówka: Wyświetlanie komunikatów zabezpieczeń można włączyć w dowolnym momencie, zaznaczając pole wyboru **Pokaż zalecenia dotyczące wirusów lub inne komunikaty zabezpieczeń**.

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

Wszechstronna ochrona przed wirusami	Ochrona użytkownika i komputera przed najnowszymi zagrożeniami, w tym wirusami, końmi trojańskimi, śledzącymi plikami cookie, oprogramowaniem szpiegującym i reklamowym oraz innymi potencjalnie niepożądanymi programami. 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.
Uzależnione od zasobów opcje skanowania	Opcje skanowania można dostosowywać, lecz jeśli użytkownik nie skorzysta z tej możliwości, komputer i tak będzie chroniony. Jeśli skanowanie przebiega powoli, można wyłączyć opcję używania minimalnych zasobów komputera, pamiętając jednak, że wówczas ochrona przed wirusami będzie miała priorytet przed innymi zadaniami.
Automatyczne naprawy	Jeśli podczas skanowania aplikacja VirusScan wykryje zagrożenie, 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 go usunąć).
Wstrzymywanie zadań w trybie pełnoekranowym	Podczas oglądania filmów i korzystania z gier lub podczas wykonywania innych czynności, które zajmują cały ekran komputera, program VirusScan wstrzymuje pewną liczbę zadań, w tym skanowanie ręczne.

ROZDZIAŁ 9

Skanowanie komputera

Nawet przed pierwszy uruchomieniem 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 przed 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, zobacz Konfigurowanie ochrony przed wirusami (strona 49).

Aplikacja VirusScan zawiera zestaw bardziej szczegółowych opcji skanowania przeznaczonych dla ochrony antywirusowej. Umożliwiają one okresowe przeprowadzanie sesji skanowania rozszerzonego. W programie SecurityCenter można uruchamiać skanowanie pełne, szybkie, niestandardowe lub zaplanowane. Skanowanie ręczne można także zainicjować 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

Aplikacja VirusScan zawiera pełny zestaw opcji skanowania przeznaczonych dla ochrony antywirusowej, obejmujący skanowanie w czasie rzeczywistym (nieustanne monitorowanie komputera pod kątem zagrożeń), skanowanie ręczne za pośrednictwem Eksploratora Windows oraz skanowanie pełne, szybkie, niestandardowe i planowane w programie SecurityCenter.

Aby...	Wykonaj następującą czynność:
Uruchomić skanowanie w czasie rzeczywistym stale monitorujące komputer pod kątem działalności wirusów (obejmujące skanowanie plików za każdym razem, gdy komputer próbuje uzyskać do nich dostęp)	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**. **Uwaga:** Skanowanie w czasie rzeczywistym jest domyślnie włączone.
Uruchomić program QuickScan w celu szybkiego sprawdzenia komputera pod kątem występowania zagrożeń	1. W menu podstawowym kliknij opcję **Skanuj**. 2. W okienku Opcje skanowania, w obszarze Szybkie skanowanie kliknij przycisk **Uruchom**.
Uruchomić pełne skanowanie w celu dokładnego sprawdzenia komputera pod kątem występowania zagrożeń	1. W menu podstawowym kliknij opcję **Skanuj**. 2. W okienku Opcje skanowania, w obszarze Pełne skanowanie kliknij przycisk **Uruchom**.

Aby...	Wykonaj następującą czynność:
Uruchomić skanowanie niestandardowe na podstawie własnych ustawień	1. W menu podstawowym kliknij opcję **Skanuj**. 2. W okienku Opcje skanowania, w obszarze Pozwól mi wybrać kliknij przycisk **Uruchom**. 3. Dostosuj skanowanie, zaznaczając lub czyszcząc opcje: **Wszystkie zagrożenia we wszystkich plikach** **Nieznane wirusy** **Pliki archiwów** **Oprogramowanie szpiegujące oraz potencjalne zagrożenia** **Śledzące pliki cookie** **Programy typu stealth** 4. Kliknij opcję **Start**.
Uruchomić ręczne skanowanie w celu sprawdzenia plików, folderów lub dysków pod kątem zagrożeń	1. Otwórz Eksploratora Windows. 2. Kliknij prawym przyciskiem myszy żądany plik, folder lub dysk, a następnie kliknij przycisk **Skanuj**.

Aby...	Wykonaj następującą czynność:
Uruchomić zaplanowane skanowanie okresowo skanujące komputer pod kątem występowania zagrożeń	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**.

Wyniki skanowania są wyświetlane w oknie alertu informującego o zakończeniu skanowania. 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**.

Uwaga: Aby uzyskać więcej informacji na temat opcji skanowania, zobacz Typy skanowania (strona 42).

Wyświetl wyniki skanowania

Po zakończeniu skanowania 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 lub inne potencjalnie szkodliwe programy.

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

Aby...	Wykonaj następującą czynność:
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	1. Na pasku zadań w obszarze powiadomień kliknij dwukrotnie ikonę **Skanowanie zostało zakończone**. 2. Kliknij opcję **Szczegóły** w okienku Pełne skanowanie, Szybkie skanowanie, Skanowanie niestandardowe lub Skanowanie ręczne.
Wyświetlić szczegółowe informacje na temat ostatniego skanowania	Kliknij dwukrotnie ikonę **Skanowanie zostało zakończone** w obszarze powiadomień na pasku zadań i wyświetl szczegółowe informacje o ostatnim skanowaniu w obszarze Twoje skanowanie w okienku Pełne skanowanie, Szybkie skanowanie, Skanowanie niestandardowe lub Skanowanie ręczne.

ROZDZIAŁ 10

Wykonywanie operacji na wynikach skanowania

Jeśli podczas skanowania aplikacja VirusScan wykryje zagrożenie, 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. Program VirusScan przed próbą wyczyszczenia pliku zawsze poddaje go kwarantannie. Jeżeli plik nie jest czysty, 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 lub plików cookie w oddzielnym 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 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 41).

Wykonywanie operacji na potencjalnie niepożądanych programach

Jeśli podczas skanowania aplikacja VirusScan wykryje na komputerze potencjalnie niepożądany program, oferuje możliwość usunięcia go lub obdarzenia zaufaniem. Jeśli dany program jest nieznany, zalecamy rozważenie jego usunięcia. 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.

Typy skanowania

Aplikacja VirusScan zawiera pełny zestaw opcji skanowania przeznaczonych dla ochrony antywirusowej, obejmujący skanowanie w czasie rzeczywistym (nieustanne monitorowanie komputera pod katem zagrożeń), skanowanie ręczne za pośrednictwem Eksploratora Windows oraz skanowanie pełne, szybkie, niestandardowe w programie SecurityCenter lub dostosowywanie czasu przeprowadzenia skanowania. Zaletą inicjowania skanowania z programu SecurityCenter jest możliwość zmiany opcji skanowania w trakcie sesji.

Skanowanie w czasie rzeczywistym:

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. 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.

Możliwe jest ustawienie domyślnych opcji skanowania w czasie rzeczywistym, obejmujących skanowanie nieznanych wirusów oraz sprawdzanie pod kątem zagrożeń śledzących plików cookie i dysków sieciowych. Można także korzystać z ochrony przed przepełnieniem buforu, która jest domyślnie włączona (z wyjątkiem systemu operacyjnego Windows Vista w wersji 64-bitowej). Aby dowiedzieć się więcej, zobacz Ustawianie opcji skanowania w czasie rzeczywistym (strona 50).

Szybkie skanowanie

Szybkie skanowanie umożliwia sprawdzenie procesów, krytycznych plików systemu Windows i innych narażonych obszarów komputera pod kątem zagrożeń.

Pełne skanowanie

Pełne skanowanie umożliwia dokładne sprawdzenie komputera pod kątem wirusów, oprogramowania szpiegującego i innych zagrożeń mogących wystąpić na komputerze.

Skanowanie niestandardowe

Skanowanie niestandardowe umożliwia wybranie własnych ustawień skanowania komputera pod kątem zagrożeń. Opcje skanowania niestandardowego obejmują sprawdzanie wszystkich plików, plików archiwów, plików cookie oraz skanowanie pod kątem nieznanych wirusów, oprogramowania szpiegującego i programów typu stealth.

Możliwe jest ustawienie domyślnych opcji skanowania niestandardowego, obejmujących skanowanie nieznanych wirusów, plików archiwów, oprogramowania szpiegującego i potencjalnych zagrożeń, śledzących plików cookie oraz programów stealth. Można także przeprowadzać skanowanie przy minimalnym użyciu zasobów komputera. Aby dowiedzieć się więcej, zobacz Ustawianie opcji skanowania niestandardowego (strona 52).

Skanowanie ręczne

Skanowanie ręczne umożliwia szybkie sprawdzenie plików, folderów i dysków pod kątem zagrożeń bezpośrednio z Eksploratora Windows.

Skanowanie planowane

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. Aby dowiedzieć się więcej, zobacz Planowanie skanowania (strona 55).

Uwaga: Aby dowiedzieć się, jak optymalnie ustawić opcje skanowania, zobacz Skanowanie komputera (strona 34).

ROZDZIAŁ 11

Korzystanie z 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 lub w przeglądarce internetowej. 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 przez instalowanie dodatkowego oprogramowania czy przekierowanie żądań przeglądarki.

Ochrona poczty e-mail

Ochrona poczty e-mail wykrywa podejrzaną aktywność w wysyłanych 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 12

Konfigurowanie ochrony przed wirusami

Możliwe jest ustawienie różnych opcji dla skanowania planowanego, niestandardowego i skanowania w czasie rzeczywistym. Na przykład, ponieważ ochrona w czasie rzeczywistym ciągle monitoruje komputer, można wybrać dla niej pewien podstawowy zestaw opcji skanowania, zachowując szerszy zestaw opcji skanowania dla ochrony ręcznej, uruchamianej na żądanie.

Korzystając z aplikacji SystemGuard i list zaufanych, można także określić sposób, w jaki program VirusScan monitoruje i zarządza potencjalnie nieautoryzowanymi lub niepożądanymi zmianami na komputerze. 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. Listy zaufane służą do określenia, czy zaufać regułom wykrywającym zmiany w plikach lub rejestrze (SystemGuard), programy lub przepełnienia buforu, czy też usunąć te reguły. 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.

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

Zatrzymywanie ochrony przed wirusami w czasie rzeczywistym

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.

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 ponownie uruchomiony, 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**.

Ustawianie opcji skanowania niestandardowego

Niestandardowa ochrona przed wirusami pozwala na skanowanie plików na żądanie. Po uruchomieniu skanowania niestandardowego program VirusScan sprawdza komputer w poszukiwaniu wirusów i innych potencjalnie szkodliwych elementów przy użyciu szerszego zestawu opcji skanowania. Aby zmienić opcje skanowania niestandardowego, 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 i 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 typy 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 niestandardowego sprawdza wszystkie dyski i foldery na komputerze oraz wszystkie dyski sieciowe, jednak domyślne lokalizacje można zmienić, dostosowując je do własnych potrzeb. Na przykład można skanować tylko krytyczne pliki komputera, elementy znajdujące się na pulpicie lub w folderze Program Files. Jeśli użytkownik nie chce być odpowiedzialny za samodzielne uruchamianie skanowania niestandardowego, 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 oglądania 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 niestandardowe.

Ustawianie opcji skanowania niestandardowego

Opcje skanowania niestandardowego ustawia się, aby dostosować to, czego program VirusScan będzie szukał podczas skanowania niestandardowego, 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. Można także ustawić lokalizację skanowania niestandardowego, aby określić, gdzie program VirusScan będzie szukał wirusów i innych szkodliwych elementów podczas skanowania niestandardowego. Można skanować wszystkie pliki, foldery i dyski w komputerze lub ograniczyć skanowanie do konkretnych folderów i dysków.

1 Otwórz okienko Skanowanie niestandardowe.

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 niestandardowego, a następnie kliknij przycisk **OK**.

Aby...	Wykonaj następującą czynność:
Wykrywać nieznane wirusy i nowe warianty znanych wirusów	Wybierz opcję **Skanuj w poszukiwaniu nieznanych wirusów**.
Wykrywać i usuwać wirusy w plikach ZIP i innych archiwach	Wybierz opcję **Skanuj pliki archiwów**.
Wykrywać oprogramowanie szpiegujące, reklamowe i inne potencjalnie niepożądane programy	Wybierz opcję **Skanuj w poszukiwaniu programów szpiegujących i potencjalnych zagrożeń**.
Wykrywać pliki cookie	Wybierz opcję **Skanuj i usuwaj śledzące pliki cookie**.
Wykrywać programy typu rootkit i stealth, które mogą zmienić i wykorzystać istniejące pliki systemu Windows	Wybierz opcję **Skanuj w poszukiwaniu programów typu stealth**.

Aby...	Wykonaj następującą czynność:
Wykorzystywać mniejszą moc obliczeniową procesora podczas skanowania, umożliwiając innym zadaniom (takim jak przeglądanie sieci Web czy otwieranie dokumentów) uzyskanie wyższego priorytetu	Wybierz opcję **Skanuj, używając minimalnej ilości zasobów komputera**.
Określić typy plików, które będą skanowane	Zaznacz opcję **Wszystkie pliki (zalecane)** lub **Tylko pliki programów i dokumenty**.

3 Kliknij opcję **Domyślna lokalizacja do skanowania**, zaznacz lub wyczyść lokalizacje, które mają być skanowane lub pominięte, a następnie kliknij opcję **OK**:

Aby...	Wykonaj następującą czynność:
Skanować wszystkie pliki i foldery w komputerze	Wybierz opcję **(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.

Istnieje możliwość planowania skanowań, które dokładnie sprawdzają cały komputer pod kątem wirusów i innych zagrożeń bezpieczeństwa przy użyciu domyślnych opcji skanowania. Domyślnie raz w tygodniu uruchamiane jest w programie VirusScan skanowanie zaplanowane.

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 59).

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.

SystemGuard	Wykrywa...
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.

SystemGuard	Wykrywa...
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 64).

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.

Opcja	Opis
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 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

Standardowe i niestandardowe poziomy ochrony	Ochrona przed włamaniami i podejrzanymi działaniami z użyciem domyślnych ustawień programu Firewall lub ustawień niestandardowych.
Zalecenia wyświetlane na bieżąco	Otrzymywanie na bieżąco zaleceń pomaga w określeniu, czy programom należy zezwolić na dostęp do Internetu oraz czy dany ruch sieciowy jest godny zaufania.
Inteligentne zarządzanie dostępem programów	Zarządzanie dostępem programów do Internetu za pomocą alertów i dzienników zdarzeń lub konfigurowanie uprawnień dostępu dla określonych aplikacji.
Niezakłócone korzystanie z gier	Zapobieganie wyświetlaniu alertów dotyczących prób włamania i podejrzanych działań w trakcie korzystania z gier na pełnym ekranie.
Ochrona komputera podczas uruchamiania	Po uruchomieniu systemu Windows® 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 potencjalnie złośliwych aplikacji, takich jak konie trojańskie, oraz zapobieganie wysyłaniu przez nie danych osobistych użytkownika do Internetu.
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 przed potencjalnymi zagrożeniami pochodzącymi z Internetu. Za pomocą funkcji zbliżonych do heurystycznych zapewniamy 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 zapory

Po zainstalowaniu zapory 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 Automatyczny (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 przy użyciu zapory, 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 domyślną zaporą.

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.

Żółty alert

Najczęściej występujący typ alertu to żółty alert, który informuje o działaniu aplikacji lub zdarzeniu sieciowym wykrytym przez zaporę. Po zaistnieniu takiej sytuacji alert podaje opis działania aplikacji lub zdarzenia sieciowego, a następnie wyświetla jedną lub kilka opcji, które wymagają wykonania czynności przez użytkownika. Na przykład alert **Nowe połączenie sieciowe** jest wyświetlany, gdy komputer z zainstalowaną zaporą został podłączony do nowej sieci. Istnieje możliwość określenia poziomu zaufania, który ma być przypisany do nowej sieci. Pojawi się on następnie na liście sieci. Jeśli inteligentne zalecenia są włączone, znane programy są dodawane automatycznie 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.

Pomoc dla użytkownika

W wielu alertach zapory są zawarte dodatkowe informacje pomagające zarządzać bezpieczeństwem komputera użytkownika, w tym:

- **Więcej informacji na temat tego programu:** Przejście 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 przy użyciu zapory

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

Po zainstalowaniu zapory po raz pierwszy ustawiany jest poziom zabezpieczeń komputera Automatyczny, 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 zapory

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

W przypadku ustawienia poziomu zabezpieczeń Automatyczny i włączenia funkcji Inteligentne zalecenia żółte alerty są wyposażone w opcję zezwalania na dostęp lub jego blokowania nieznanym programom, które wymagają dostępu dla ruchu przychodzącego. Pomimo tego, że Zielone alerty są domyślnie wyłączone, pojawiają się w przypadku wykrycia znanych programów, gdy 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 Standardowy), tym więcej jest wyświetlanych opcji i alertów, na które musi zareagować użytkownik.

W poniższej tabeli opisano trzy poziomy zabezpieczeń zapory, począwszy od najbardziej restrykcyjnego do najbardziej tolerancyjnego:

Poziom	Opis
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.
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.
Automatyczny	Zezwolenie programom na dostęp do Internetu albo dla połączeń przychodzących i wychodzących (pełny), albo tylko dla ruchu wychodzącego. Domyślnym poziomem zabezpieczeń jest Automatyczny z wybraną opcją zezwolenia programom na dostęp do Internetu tylko dla ruchu wychodzącego. Jeśli dana aplikacja ma przyznany pełny dostęp, zapora 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, zapora automatycznie uznaje ją za zaufaną tylko przy nawiązywaniu wychodzącego połączenia z Internetem. Połączenie przychodzące nie jest automatycznie uznawane za zaufane.

Zapora umożliwia również natychmiastowe przywrócenie standardowego poziomu zabezpieczeń, czyli poziomu Automatyczny (dostęp do Internetu tylko dla ruchu wychodzącego), w okienku Przywróć ustawienia domyślne zapory.

Ustawienie poziomu zabezpieczeń na Ukryty

Można ustawić poziom zabezpieczeń zapory 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 zapora wyświetla alert, gdy nowe aplikacje żądają nawiązania wychodzącego połączenia internetowego lub otrzymują żądania nawiązania połączenia przychodzącego.

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 Automatyczny

Można ustawić poziom zabezpieczeń zapory na Automatyczny, 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 **Automatyczny**.
4. Wykonaj jedną z poniższych 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**.

Konfigurowanie inteligentnych zaleceń dla alertów

Zaporę można skonfigurować tak, aby uwzględniała, wykluczała lub wyświetlała w alertach zalecenia dotyczące wszystkich programów próbujących uzyskać dostęp do Internetu. Włączenie inteligentnych zaleceń pomaga w podejmowaniu decyzji dotyczących reakcji na alerty.

W przypadku zastosowania opcji inteligentnych zaleceń (i ustawienia poziomu zabezpieczeń na Automatyczny, który zezwala na dostęp do Internetu tylko dla ruchu wychodzącego), zapora automatycznie przepuszcza wszystkie znane programy i blokuje programy potencjalnie niebezpieczne.

Jeśli funkcja Inteligentne zalecenia nie jest zastosowana, zapora nie zezwala na dostęp ani nie blokuje dostępu do Internetu ani nie sugeruje żadnych działań w alertach.

Jeśli dla funkcji Inteligentne zalecenia jest wybrane ustawienie Pokaż, pojawia się monit o zezwolenie na dostęp lub zablokowanie go, a zapora sugeruje w alercie dalsze działania.

Włączanie inteligentnych zaleceń

Można włączyć funkcję Inteligentne zalecenia, aby zapora automatycznie zezwalała aplikacjom na dostęp do Internetu lub blokowała go oraz wyświetlała 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 **Zastosuj inteligentne zalecenia**.
4. Kliknij przycisk **OK**.

Wyłączanie inteligentnych zaleceń

Można wyłączyć funkcję Inteligentne zalecenia, aby zapora zezwalała aplikacjom na dostęp do Internetu lub blokowała go oraz wyświetlała alerty dotyczące nierozpoznanych lub potencjalnie niebezpiecznych programów. Jednak w takim przypadku alerty nie zawierają żadnych sugestii dotyczących obsługi dostępu aplikacji do Internetu. Jeśli zapora 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 **Nie stosuj inteligentnych zaleceń**.
4. Kliknij przycisk **OK**.

Wyświetlanie inteligentnych zaleceń

W ramach funkcji inteligentnych zaleceń możliwe jest ustawienie wyświetlania tylko zaleceń w alertach, co daje użytkownikowi możliwość podjęcia decyzji o przepuszczeniu lub blokowaniu nieznanych lub potencjalnie niebezpiecznych programów.

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 **Pokaż inteligentne zalecenia**.
4. Kliknij przycisk **OK**.

Optymalizacja zabezpieczeń zapory.

Istnieje wiele zagrożeń bezpieczeństwa komputera. Na przykład niektóre programy mogą próbować połączyć się z Internetem w trakcie uruchamiania systemu Windows®. Zaawansowani użytkownicy mogą również sprawdzić, czy komputer użytkownika jest połączony z siecią, używając polecenia ping. Mogą również wysłać informacje do danego komputera używając protokołu UDP w postaci jednostek wiadomości (datagramów). Zapora broni komputer przed takimi atakami, pozwalając użytkownikowi na blokowanie dostępu programów do Internetu w trakcie uruchamiania systemu Windows, blokowanie żądań ping, które pomagają innym użytkownikom wykryć komputer w sieci, i uniemożliwienie innym użytkownikom wysyłania informacji do komputera w postaci jednostek wiadomości (datagramów).

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.

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 systemu Windows**.
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 ustawień protokołu UDP

Można zezwolić innym użytkownikom komputerów w sieci na wysyłanie jednostek wiadomości do danego komputera przy użyciu protokołu UDP. Jednak można to zrobić tylko wtedy, jeżeli został zamknięty port usługi systemowej w celu zablokowania tego protokołu.

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 **Włącz śledzenie UDP**, aby umożliwić innym użytkownikom komputerów na wysyłanie jednostek wiadomości (datagramów) do danego komputera.
   - Usuń zaznaczenie opcji **Włącz śledzenie UDP**, aby uniemożliwić innym użytkownikom komputerów wysyłanie jednostek wiadomości (datagramów) do danego komputera.
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.**
   - **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 wszystkie przychodzące i wychodzące połączenia sieciowe, w tym dostęp do witryn sieci Web, pocztę e-mail oraz aktualizacje zabezpieczeń. Blokada daje taki sam rezultat, jak odłączenie kabla sieciowego od komputera. Ustawienie to można wykorzystać do zablokowania portów ustawionych jako otwarte w okienku Usługi systemowe oraz do pomocy w zidentyfikowaniu i usunięciu problemów z komputerem.

Natychmiastowa blokada zapory

Przy użyciu zapory można natychmiast zablokować cały ruch sieciowy między komputerem a dowolną siecią, w tym siecią Internet.

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

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

Natychmiastowe odblokowanie zapory

Można odblokować zaporę, aby natychmiast odblokować cały ruch sieciowy między komputerem a dowolną siecią, w tym siecią Internet.

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

Przywracanie ustawień zapory

Można szybko przywrócić pierwotne ustawienia ochrony przy pomocy zapory. Powoduje to przywrócenie poziomu zabezpieczeń Automatyczny, 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.
4. Kliknij przycisk **OK**.

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 113)

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 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 upewnić się, 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 zaufany komputer był również chroniony za pomocą zapory i aktualnego programu antywirusowego. Zapora nie rejestruje ruchu ani nie generuje alertów o zdarzeniach z zaufanych adresów IP znajdujących się na liście **Sieci**.

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

W tym rozdziale

Połączenia z komputerami

Połączenia z komputerami to połączenia, które użytkownik tworzy między swoim komputerem a innymi komputerami w dowolnej sieci. Można dodawać, edytować i usuwać adresy IP znajdujące się na liście **Sieci**. Te adresy IP są powiązane z sieciami, którym użytkownik chce przypisać poziom zaufania podczas połączenia z komputerem użytkownika: Zaufany, Standardowy i Publiczny.

Poziom	Opis
Zaufany	Zapora zezwala na odbieranie ruchu z adresu IP do komputera użytkownika przez każdy port. Działania, w których uczestniczy komputer przypisany do zaufanego adresu IP i komputer użytkownika, nie są filtrowane ani analizowane przez zaporę. Domyślnie pierwsza prywatna sieć odnaleziona przez zaporę jest wyświetlana jako zaufana na liście **Sieci**. Przykładem zaufanej sieci jest komputer lub komputery w sieci biurowej lub domowej użytkownika.
Standardowy	Zapora kontroluje ruch przychodzący z adresu IP (ale nie z każdego innego komputera w tej sieci), kiedy nawiązuje on połączenie z komputerem użytkownika, i przepuszcza lub blokuje ruch zgodnie z regułami na liście **Usługi systemowe**. Zapora rejestruje ruch i generuje alerty o zdarzeniach ze standardowych adresów IP. Przykładem sieci standardowej jest komputer lub komputery w sieci korporacyjnej.
Publiczny	Zapora kontroluje ruch z sieci publicznej zgodnie z regułami na liście **Usługi systemowe**. Przykładem sieci publicznej jest sieć internetowa w kawiarni, hotelu lub na lotnisku.

Przy zezwalaniu na połączenie należy upewnić się, 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 zaufany komputer był również chroniony za pomocą zapory i aktualnego programu antywirusowego.

Dodawanie połączenia z komputerem

Można dodać połączenie z komputerem zaufanym, standardowym lub publicznym i przypisanym do niego adresem 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 **Sieci**.
4. W okienku Sieci kliknij przycisk **Dodaj**.
5. Jeżeli połączenie komputerowe odbywa się w sieci IPv6, należy zaznaczyć pole wyboru **IPv6**.
6. W obszarze **Dodaj regułę** wykonaj jedną z następujących czynności:
   - Wybierz opcję **Pojedynczy**, a następnie wprowadź adres IP w polu **Adres IP**.
   - Wybierz opcję **Zakres**, a następnie wprowadź początkowe i końcowe adresy IP w polach **Od adresu IP** i **Do adresu IP**. Jeżeli połączenie komputerowe odbywa się w sieci IPv6, należy wprowadzić adres początkowy IP i długość prefiksu w polach **Od adresu IP** i **Długość prefiksu**.
7. W obszarze **Typ** wykonaj jedną z następujących czynności:
   - Wybierz poziom **Zaufany**, aby określić, że to połączenie komputerowe jest zaufane (np. komputer w sieci domowej).
   - Wybierz poziom **Standardowy**, aby określić, że to połączenie komputerowe (a nie inne komputery w sieci tego komputera) jest zaufane (na przykład komputer w sieci korporacyjnej).
   - Wybierz poziom **Publiczny**, aby określić, że to połączenie komputerowe jest publiczne (na przykład komputer w kawiarence internetowej, hotelu lub na lotnisku).
8. Jeśli usługa systemowa korzysta z udostępniania połączenia internetowego, można dodać następujący zakres adresów IP: od 192.168.0.1 do 192.168.0.255.
9. Można też wybrać opcję **Reguła wygasa za** i wprowadzić liczbę dni, w czasie których reguła będzie obowiązywać.
10. Dodatkowo można wprowadzić opis reguły.
11. Kliknij przycisk **OK**.

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

Dodawanie komputera z poziomu dziennika Zdarzenia przychodzące

Połączenie z zaufanym lub standardowym 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 adres źródłowy IP i w obszarze **Działanie** wykonaj jedną z następujących czynności:
   - Kliknij przycisk **Dodaj ten adres IP jako zaufany**, aby dodać ten komputer jako zaufany do listy **Sieci**.
   - Kliknij przycisk **Dodaj ten adres IP jako standardowy**, aby dodać połączenie z tym komputerem jako standardowe do listy **Sieci**.
6. Kliknij przycisk **Tak**, aby potwierdzić ustawienie.

Edycja połączenia z komputerem

Można edytować połączenie z komputerem zaufanym, standardowym lub publicznym i przypisanym do niego adresem 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 **Sieci**.
4. W okienku Sieci wybierz adres IP, a następnie kliknij przycisk **Edytuj**.
5. Jeżeli połączenie komputerowe odbywa się w sieci IPv6, należy zaznaczyć pole wyboru **IPv6**.
6. W obszarze **Edytuj regułę** wykonaj jedną z następujących czynności:
   - Wybierz opcję **Pojedynczy**, a następnie wprowadź adres IP w polu **Adres IP**.
   - Wybierz opcję **Zakres**, a następnie wprowadź początkowe i końcowe adresy IP w polach **Od adresu IP** i **Do adresu IP**. Jeżeli połączenie komputerowe odbywa się w sieci IPv6, należy wprowadzić adres początkowy IP i długość prefiksu w polach **Od adresu IP** i **Długość prefiksu**.

7 W obszarze **Typ** wykonaj jedną z następujących czynności:

- Wybierz poziom **Zaufany**, aby określić, że to połączenie komputerowe jest zaufane (np. komputer w sieci domowej).
- Wybierz poziom **Standardowy**, aby określić, że to połączenie komputerowe (a nie inne komputery w sieci tego komputera) jest zaufane (na przykład komputer w sieci korporacyjnej).
- Wybierz poziom **Publiczny**, aby określić, że to połączenie komputerowe jest publiczne (na przykład komputer w kawiarence internetowej, hotelu lub na lotnisku).

8 Można też zaznaczyć opcję **Reguła wygasa za** i wpisać liczbę dni, w czasie których reguła będzie obowiązywać.

9 Dodatkowo można wprowadzić opis reguły.

10 Kliknij przycisk **OK**.

Uwaga: Nie można edytować domyślnego połączenia z komputerem dodanego automatycznie przez zaporę z zaufanej sieci prywatnej.

Usuwanie połączenia z komputerem

Można usunąć połączenie z komputerem zaufanym, standardowym lub publicznym i przypisanym do niego adresem 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 **Sieci**.

4 W okienku Sieci wybierz adres IP, a następnie kliknij przycisk **Usuń**.

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

Blokowanie połączeń z komputerami

Zabronione adresy IP można dodawać, edytować i usuwać w okienku 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 zagrożenie. Należy upewnić się, że nie są blokowane ważne adresy IP, takie jak adresy serwerów DNS czy DHCP lub innych serwerów usługodawcy internetowego.

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 **Zabronione adresy IP**.
4. W okienku Zabronione adresy IP kliknij opcję **Dodaj**.
5. Jeżeli połączenie komputerowe odbywa się w sieci IPv6, należy zaznaczyć pole wyboru **IPv6**.
6. W obszarze **Dodaj regułę** wykonaj jedną z następujących czynności:
   - Wybierz opcję **Pojedynczy**, a następnie wprowadź adres IP w polu **Adres IP**.
   - Wybierz opcję **Zakres**, a następnie wprowadź początkowe i końcowe adresy IP w polach **Od adresu IP** i **Do adresu IP**. Jeżeli połączenie komputerowe odbywa się w sieci IPv6, należy wprowadzić adres początkowy IP i długość prefiksu w polach **Od adresu IP** i **Długość prefiksu**.
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. Kliknij przycisk **Tak**, aby potwierdzić ustawienie.

Edycja połączenia z zabronionym komputerem

Można edytować połączenie z zabronionym komputerem i przypisanym do niego adresem 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 **Zabronione adresy IP**.
4. W okienku Zabronione adresy IP kliknij opcję **Edytuj**.
5. Jeżeli połączenie komputerowe odbywa się w sieci IPv6, należy zaznaczyć pole wyboru **IPv6**.
6. W obszarze **Edytuj regułę** wykonaj jedną z następujących czynności:
   - Wybierz opcję **Pojedynczy**, a następnie wprowadź adres IP w polu **Adres IP**.

- Wybierz opcję **Zakres**, a następnie wprowadź początkowe i końcowe adresy IP w polach **Od adresu IP** i **Do adresu IP**. Jeżeli połączenie komputerowe odbywa się w sieci IPv6, należy wprowadzić adres początkowy IP i długość prefiksu w polach **Od adresu IP** i **Długość prefiksu**.

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**.

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 **Zabronione adresy IP**.

4 W okienku Zabronione adresy IP wybierz adres IP, a następnie kliknij przycisk **Usuń**.

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

Blokowanie dostępu komputerowi z poziomu dziennika Zdarzenia przychodzące

Połączenia z komputerem i związanym z nim adresem IP można zabronić z poziomu dziennika Zdarzenia przychodzące. Aby zabronić dostępu do adresu IP, co do którego istnieje przypuszczenie, że jest źródłem podejrzanej lub niepożądanej aktywności internetowej, można skorzystać z dziennika zawierającego listę adresów IP całego przychodzącego ruchu internetowego.

Dodaj adres IP do listy **Zabronione adresy IP**, jeżeli cały ruch przychodzący z tego adresu IP ma być zablokowany niezależnie od tego, czy porty usług systemowych są otwarte czy zamknięte.

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 IP**.

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

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

ROZDZIAŁ 20

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. Te porty usług systemowych mogą być otwarte lub zamknięte dla komputerów wyświetlanych jako Zaufane, Standardowe lub Publiczne na liście **Sieci**.

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

- Typowy port systemu operacyjnego 5357
- 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 dostęp zdalnej sieci do usługi systemowej 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 **Edytuj**.
6. Wykonaj jedną z poniższych czynności:
   - Aby otworzyć port dla dowolnego komputera w zaufanej, standardowej lub publicznej sieci (na przykład sieci domowej, korporacyjnej lub internetowej), wybierz opcję **Zaufane, Standardowe i Publiczne**.
   - Aby otworzyć port dla dowolnego komputera w sieci standardowej (na przykład korporacyjnej), wybierz opcję **Standardowe (zawiera Zaufane)**.
7. Kliknij przycisk **OK**.

Blokowanie dostępu do istniejącego portu usługi systemowej

Można zamknąć istniejący port, aby zablokować zdalny dostęp do usługi systemowej 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. W obszarze **Otwórz port usługi systemowej** usuń zaznaczenie przy porcie wybranej usługi systemowej, który ma być zamknięty.
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 okienku Usługi systemowe w obszarze **Dodaj regułę usługi systemowej** wprowadź następujące informacje:
   - Nazwa usługi systemowej
   - Kategoria usługi systemowej
   - Porty lokalne TCP/IP
   - Porty lokalne UDP
6. Wykonaj jedną z poniższych czynności:
   - Aby otworzyć port dla dowolnego komputera w zaufanej, standardowej lub publicznej sieci (na przykład sieci domowej, korporacyjnej lub internetowej), wybierz opcję **Zaufane, Standardowe i Publiczne**.
   - Aby otworzyć port dla dowolnego komputera w sieci standardowej (na przykład korporacyjnej), wybierz opcję **Standardowe (zawiera Zaufane)**.
7. 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 komputerów w sieci, które używają usługi udostępniania połączenia internetowego**.
8. Można też wprowadzić opis nowej konfiguracji.
9. Kliknij przycisk **OK**.

Uwaga: Jeśli na komputerze jest uruchomiony program akceptujący połączenia z serwerem sieci Web lub FTP, może zajść potrzeba otwarcia powiązanego portu usługi systemowej na komputerze udostępniającym połączenie i zezwolenia na przesyłanie połączeń przychodzących do tego portu. W przypadku korzystania z usługi udostępniania połączenia internetowego (ICS, Internet Connection Sharing) należy też dodać połączenie z zaufanym komputerem do listy **Sieci**. Aby uzyskać więcej informacji, zobacz temat Dodawanie połączenia z 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. Kliknij pole wyboru obok usługi systemowej, a następnie kliknij przycisk **Edytuj**.
5. W obszarze **Dodaj regułę usługi systemowej** okienka Usługi systemowe zmodyfikuj następujące informacje:
   - Nazwa usługi systemowej
   - Porty lokalne TCP/IP
   - Porty lokalne UDP
6. Wykonaj jedną z poniższych czynności:
   - Aby otworzyć port dla dowolnego komputera w zaufanej, standardowej lub publicznej sieci (na przykład sieci domowej, korporacyjnej lub internetowej), wybierz opcję **Zaufane, Standardowe i Publiczne**.
   - Aby otworzyć port dla dowolnego komputera w sieci standardowej (na przykład korporacyjnej), wybierz opcję **Standardowe (zawiera Zaufane)**.
7. 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 komputerów w sieci, które używają usługi udostępniania połączenia internetowego**.
8. Można też wprowadzić opis zmienionej konfiguracji.
9. 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 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 IP**.
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 IP**.
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 komputera 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 źródłowym do tego komputerem. 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. Dodatkowo Monitor ruchu pokazuje programy, które wykorzystują najwięcej 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. Dodatkowo Monitor ruchu pokazuje programy, które wykorzystują najwięcej 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 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

Czyszczenie plików	Bezpieczne i skuteczne usuwanie niepotrzebnych plików przy użyciu różnych narzędzi do usuwania. Usuwając te pliki, użytkownik zwiększa ilość miejsca na dysku twardym komputera i poprawia jego wydajność.

ROZDZIAŁ 24

Oczyszczanie komputera

Program QuickClean usuwa pliki, które mogą zaśmiecać komputer. Program opróżnia Kosz i usuwa tymczasowe pliki, skróty, zagubione fragmenty plików, pliki rejestru, buforowane pliki, 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	Funkcja
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).

Nazwa	Funkcja
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.

Nazwa	Funkcja
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.

W tym rozdziale

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 25

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

Trwałe usuwanie plików i folderów

Istnieje możliwość usunięcia elementów z dysku twardego komputera w taki sposób, aby nie można było odtworzyć powiązanych z nimi informacji. Program Shredder 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 26

Program McAfee Network Manager

Program Network Manager przedstawia graficzną prezentację komputerów i innych urządzeń wchodzących w skład sieci domowej. Za jego pomocą można zdalnie zarządzać stanem ochrony każdego zarządzanego komputera działającego w sieci i usuwać zgłaszane luki w zabezpieczeniach tych komputerów. Jeżeli został zainstalowany pakiet McAfee Total Protection, program Network Manager może także monitorować sieć pod kątem intruzów (nierozpoznanych lub niezaufanych komputerów lub urządzeń), którzy próbują połączyć się z siecią.

Przed rozpoczęciem korzystania z programu Network Manager można zapoznać się z niektórymi jego funkcjami. Szczegółowe informacje na temat konfigurowania tych funkcji i korzystania z nich zamieszczono 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

Graficzna mapa sieci	Wyświetlanie graficznego przeglądu stanu ochrony komputerów i urządzeń w sieci domowej. Po wprowadzeniu w sieci zmian (na przykład po dodaniu komputera) mapa sieci uwzględnia je. Aby dostosować jej widok do potrzeb, można ją odświeżać, zmieniać nazwę sieci i wyświetlać lub ukrywać jej elementy. Można również wyświetlić szczegółowe informacje na temat dowolnego urządzenia wyświetlanego na mapie sieci.
Zarządzanie zdalne	Zarządzanie stanem zabezpieczeń komputerów tworzących sieć domową. Można zaprosić komputer do dołączenia do sieci zarządzanej, monitorować stan ochrony zarządzanego komputera i rozwiązywać problemy ze znanymi zagrożeniami pochodzącymi ze zdalnego komputera w sieci.
Monitorowanie sieci	Jeśli program Network Manager jest dostępny, może monitorować sieci i powiadamiać o nawiązaniu połączenia przez znajomych lub intruzów. Monitorowanie sieci jest dostępne tylko w przypadku zakupu pakietu McAfee Total Protection.

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 27

Konfigurowanie sieci zarządzanej

Aby skonfigurować sieć zarządzaną, należy udzielić sieci zaufania (jeżeli jeszcze nie zostało to zrobione) i dodać do niej elementy (komputery). Aby było możliwe zdalne zarządzanie komputerem lub przyznanie mu uprawnienia do zdalnego zarządzania innymi komputerami, musi on stać się zaufanym elementem sieci. Przynależność do sieci jest przyznawana nowym komputerom przez dotychczasowe elementy sieci (komputery), które mają uprawnienia administracyjne.

Można wyświetlić szczegóły dotyczące dowolnego elementu przedstawionego na mapie sieci, nawet po dokonaniu zmian w tej sieci (np. po dodaniu komputera).

W tym rozdziale

Praca z mapą sieci

Po połączeniu komputera z siecią program Network Manager analizuje ją w celu określenia, czy występują w niej jakieś zarządzane lub niezarządzane elementy, oraz sprawdza atrybuty routera i stan Internetu. Jeśli nie zostaną znalezione żadne elementy, program Network Manager zakłada, że aktualnie podłączony komputer jest pierwszym komputerem w sieci, i przyznaje mu status zarządzanego elementu z uprawnieniami administracyjnymi. Domyślnie nazwa sieci zawiera nazwę 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. Aby dostosować widok mapy do własnych potrzeb, można na przykład ją odświeżyć, zmienić nazwę sieci i wyświetlić lub ukryć jej elementy. Można również wyświetlać szczegóły dotyczące dowolnego elementu przedstawionego na mapie sieci.

Uzyskiwanie dostępu do mapy sieci

Mapa sieci to graficzna reprezentacja komputerów i urządzeń tworzących sieć domową.

- W menu podstawowym lub zaawansowanym kliknij polecenie **Zarządzaj siecią**.

Uwaga: Jeżeli sieci nie udzielono jeszcze zaufania (przy użyciu programu McAfee Personal Firewall), przy pierwszym uzyskaniu dostępu do mapy sieci pojawia się monit o udzielenie zaufania.

Odświeżanie mapy sieci

Mapę sieci można odświeżyć w dowolnym momencie, np. po dodaniu do sieci zarządzanej 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 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 urządzenia wchodzące w skład sieci domowej są pokazywane na mapie. Jeśli jednak istnieją elementy ukryte, można je ponownie pokazać w dowolnym momencie. Ukrywać można tylko elementy niezarządzane; ukrycie komputerów zarządzanych jest niemożliwe.

Aby...	**W menu podstawowym lub zaawansowanym kliknij polecenie** Zarządzaj siecią**, a następnie...**
Ukryć element na mapie sieci	Kliknij element na mapie sieci, a następnie kliknij opcję **Ukryj ten element** w obszarze **Działanie**. W oknie dialogowym potwierdzenia kliknij przycisk **Tak**.
Wyświetlić ukryte elementy na mapie sieci	W obszarze **Działanie** kliknij opcję **Pokaż ukryte elementy**.

Wyświetlanie szczegółów elementu

Aby wyświetlić szczegółowe informacje o dowolnym elemencie sieci, należy go zaznaczyć na mapie sieci. Wyświetlane informacje obejmują: nazwę elementu, stan jego ochrony oraz inne informacje wymagane do zarządzania elementem.

1. Kliknij ikonę elementu na mapie sieci.
2. W obszarze **Szczegóły** zapoznaj się z informacjami o danym 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 sieci zarządzanej

Po otrzymaniu zaproszenia do dołączenia do sieci zarządzanej można je albo przyjąć, albo odrzucić. Można także określić, czy inne komputery w sieci mogą zarządzać ustawieniami zabezpieczeń tego komputera.

1. Upewnij się, że pole wyboru **Zezwalaj wszystkim komputerom w tej sieci na zarządzanie ustawieniami zabezpieczeń** w oknie dialogowym Zarządzana sieć jest zaznaczone.
2. Kliknij przycisk **Dołącz**.
   Po przyjęciu zaproszenia zostaną wyświetlone dwie karty do gry.
3. Potwierdź, że karty do gry są takie same jak wyświetlane na komputerze, który wysłał zaproszenie do dołączenia do sieci zarządzanej.
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 **Anuluj**.

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. Wysyłając zaproszenie, należy określić także poziom uprawnienia, który ma zostać przyznany komputerowi dołączającemu do sieci.

1. Kliknij ikonę komputera niezarządzanego na mapie sieci.
2. Kliknij opcję **Zarządzaj tym komputerem** w obszarze **Działanie**.
3. W oknie dialogowym Zapraszanie komputera do dołączenia do sieci zarządzanej 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. Potwierdź, że karty do gry są takie same jak wyświetlane na komputerze, który zapraszasz do dołączenia do sieci zarządzanej.
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 28

Zdalne zarządzanie siecią

Po skonfigurowaniu zarządzanej sieci można zdalnie zarządzać komputerami i urządzeniami składającymi się na tę sieć. Można zarządzać stanem i poziomami uprawnień komputerów i urządzeń oraz zdalnie naprawiać większość luk w zabezpieczeniach.

W tym rozdziale

Zarządzanie stanem i uprawnieniami

W skład sieci zarządzanej wchodzą elementy zarządzane i niezarządzane. Elementy zarządzane zezwalają na zarządzanie swoim stanem ochrony McAfee przez inne komputery w sieci, natomiast użytkownicy niezarządzani nie zezwalają na to. Elementy niezarządzane to zazwyczaj komputery-goście, które uzyskują dostęp do innych mechanizmów sieciowych (np. wysyłania plików lub współdzielenia drukarek). Zarządzany komputer z uprawnieniami administracyjnymi w sieci może w dowolnym momencie zaprosić niezarządzany komputer, aby stał się komputerem zarządzanym. Podobnie zarządzany komputer z uprawnieniami administracyjnymi w sieci może spowodować, że inny zarządzany komputer stanie się 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 dostępu pełnego i typu Gość pozwalają komputerowi tylko na uzyskiwanie dostępu do sieci. Poziom uprawnień komputera można zmodyfikować w dowolnym momencie.

Ponieważ zarządzana sieć składa się również z urządzeń (na przykład routerów), także nimi można zarządzać za pomocą programu Network Manager. Można także konfigurować i modyfikować ustawienia wyświetlania urządzenia na mapie sieci.

Zarządzanie stanem ochrony komputera

Jeśli stan ochrony komputera nie jest zarządzany w sieci (komputer nie jest elementem sieci lub jest jej elementem niezarządzanym), można zażądać zarządzania nim.

1. Kliknij ikonę komputera niezarządzanego na mapie sieci.
2. Kliknij opcję **Zarządzaj tym komputerem** w obszarze **Działanie**.

Kończenie zarządzania stanem ochrony komputera

Można zakończyć zarządzanie stanem ochrony zarządzanego komputera w sieci; komputer jednak staje się wówczas niezarządzany i nie można zdalnie zarządzać stanem jego ochrony.

1. Kliknij ikonę komputera zarządzanego na mapie sieci.
2. Kliknij opcję **Zakończ zarządzanie tym komputerem** w obszarze **Działanie**.
3. W oknie dialogowym potwierdzenia kliknij przycisk **Tak**.

Modyfikowanie uprawnień komputera zarządzanego

Uprawnienia zarządzanego komputera można w dowolnym momencie zmieniać. Umożliwia to ustalenie, które komputery mogą zarządzać stanem ochrony innych komputerów w sieci.

1. Kliknij ikonę komputera zarządzanego 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 nawzajem zarządzać swoim stanem ochrony.
4. Kliknij przycisk **OK**.

Zarządzanie urządzeniem

Urządzeniem można zarządzać, uzyskując dostęp do jego administracyjnej strony sieci Web na mapie sieci.

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 oknie przeglądarki sieci Web podaj informacje 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 McAfee 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 zarządzać stanem ochrony McAfee innych zarządzanych komputerów w sieci i zdalnie naprawiać zgłoszone luki w zabezpieczeniach. Jeśli na przykład 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 przez 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, nie można zdalnie zarządzać ich stanem ochrony. Aby zdalnie zarządzać tymi komputerami, należy na każdym z nich zainstalować najnowszą wersję programu SecurityCenter.

1. Na komputerze, który ma być zarządzany zdalnie, należy wykonać następujące instrukcje.
2. Przygotuj informacje logowania McAfee — są to adres e-mail i hasło, które zostały użyte podczas pierwszej aktywacji oprogramowania firmy McAfee.
3. W przeglądarce przejdź do witryny sieci Web firmy McAfee, zaloguj się i kliknij przycisk **Moje konto**.
4. Znajdź produkt, który chcesz zainstalować, i kliknij przycisk **Pobierz**, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Wskazówka: Informacje o sposobie instalowania oprogramowania zabezpieczeń firmy McAfee na zdalnych komputerach można uzyskać, otwierając mapę sieci i klikając opcję **Chroń komputery** w obszarze **Działanie**.

ROZDZIAŁ 29

Monitorowanie sieci

Jeżeli został zainstalowany pakiet McAfee Total Protection, program Network Manager monitoruje sieć pod kątem intruzów. Za każdym razem, gdy z siecią połączy się nieznany komputer lub nieznane urządzenie, użytkownik zostanie o tym powiadomiony i będzie mógł podjąć decyzję, czy jest to przyjaciel czy intruz. Przyjaciel to komputer lub urządzenie rozpoznane i zaufane, a intruz to komputer lub urządzenie nierozpoznane lub niezaufane. Jeżeli komputer lub urządzenie zostanie oznaczone jako przyjaciel, można określić, czy użytkownik będzie powiadamiany za każdym razem, gdy przyjaciel połączy się z siecią. Jeżeli komputer lub urządzenie zostanie oznaczone jako intruz, przy każdej próbie nawiązania połączenia automatycznie będzie wyświetlany alert.

Przy pierwszym połączeniu z siecią po zainstalowaniu tej wersji pakietu Total Protection lub uaktualnieniu do niej, wszystkie komputery i urządzenia zostaną oznaczone jako przyjaciele i użytkownik nie będzie w przyszłości powiadamiany o ich połączeniu z siecią. Po upływie trzech dni użytkownik będzie powiadamiany o każdym nieznanym komputerze i urządzeniu łączącym się z siecią, aby mógł oznaczyć je samodzielnie.

Uwaga: Monitorowanie sieci jest funkcją programu Network Manager dostępną tylko w pakiecie McAfee Total Protection. Więcej informacji na temat pakietu Total Protection można znaleźć w naszej witrynie sieci Web.

W tym rozdziale

Zatrzymywanie monitorowania sieci

Jeżeli monitorowanie sieci zostanie wyłączone, użytkownik nie będzie otrzymywał alertów o intruzach podłączających się do sieci domowej lub innych sieci, z którymi łączy się użytkownik.

1 Otwórz okienko Konfiguracja Internetu i sieci.

   Jak to zrobić?

   1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
   2. W okienku Początek programu SecurityCenter kliknij kategorię **Internet i sieć**.
   3. W sekcji informacji o Internecie i sieci kliknij polecenie **Konfiguruj**.

2 W polu **Monitorowanie sieci** kliknij opcję **Wyłączone**.

Ponowne włączanie powiadomień monitorowania sieci

Wyłączenie powiadomień monitorowania sieci jest możliwe, ale nie jest zalecane. Jeżeli zostanie wyłączone, użytkownik nie będzie otrzymywał informacji o nieznanych komputerach lub intruzach podłączających się do sieci. Jeżeli powiadomienia zostały wyłączone przez przypadek (na przykład w alercie użytkownik zaznaczył pole wyboru **Nie pokazuj tego alertu ponownie**), można je w dowolnym momencie ponownie włączyć.

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 Upewnij się, że w okienku Alerty informacyjne nie są zaznaczone następujące pola wyboru:

   - **Nie pokazuj alertów, gdy nowe komputery lub urządzenia łączą się z siecią**
   - **Nie pokazuj alertów, gdy intruzi łączą się z siecią**
   - **Nie pokazuj alertów o przyjaciołach, o których zwykle chcę otrzymywać powiadomienia**
   - **Nie przypominaj o wykryciu nieznanych komputerów lub urządzeń**
   - **Nie wyświetlaj alertu, gdy program McAfee zakończy wykrywanie nowych przyjaciół**

4 Kliknij przycisk **OK**.

Oznaczanie intruza

Komputer lub urządzenie w sieci należy oznaczyć jako intruza wtedy, gdy jest ono nierozpoznane lub niezaufane. Alert będzie pojawiał się automatycznie za każdym razem, gdy intruz połączy się z siecią.

1. W menu podstawowym lub zaawansowanym kliknij polecenie **Zarządzaj siecią**.
2. Na mapie sieci kliknij element.
3. W obszarze **Działanie** kliknij opcję **Oznacz jako przyjaciela lub intruza**.
4. W oknie dialogowym kliknij opcję **Intruz**.

Oznaczanie przyjaciół

Komputer lub urządzenie w sieci należy oznaczyć jako przyjaciela tylko wtedy, gdy jest ono rozpoznane i zaufane. Po oznaczeniu komputera lub urządzenia jako przyjaciela można określić, czy użytkownik ma być powiadamiany za każdym razem, gdy przyjaciel połączy się z siecią.

1. W menu podstawowym lub zaawansowanym kliknij polecenie **Zarządzaj siecią**.
2. Na mapie sieci kliknij element.
3. W obszarze **Działanie** kliknij opcję **Oznacz jako przyjaciela lub intruza**.
4. W oknie dialogowym kliknij opcję **Przyjaciel**.
5. Aby otrzymywać powiadomienia za każdym razem, gdy przyjaciel połączy się z siecią, należy zaznaczyć pole wyboru **Powiadamiaj mnie, gdy ten komputer lub urządzenie połączy się z siecią**.

Zakończenie wykrywania przyjaciół

Przez pierwsze trzy dni po połączeniu z siecią po zainstalowaniu tej wersji pakietu Total Protection każdy komputer lub urządzenie zostanie oznaczane jako przyjaciel i użytkownik nie będzie o nim powiadamiany. Automatyczne oznaczanie można zatrzymać w dowolnym momencie w ciągu tych trzech dni, ale nie można go ponownie uruchomić.

1. W menu podstawowym lub zaawansowanym kliknij polecenie **Zarządzaj siecią**.
2. W obszarze **Działanie** kliknij opcję **Zakończ wykrywanie nowych przyjaciół**.

ROZDZIAŁ 30

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 31

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

Program EasyNetwork można otworzyć z menu Start systemu Windows lub klikając ikonę na pulpicie.

- W menu **Start** wybierz polecenie **Programy**, następnie polecenie **McAfee**, a potem kliknij polecenie **McAfee EasyNetwork**.

Wskazówka: Program EasyNetwork można także otworzyć, klikając dwukrotnie ikonę McAfee EasyNetwork na pulpicie.

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 162).

Opuszczanie zarządzanej sieci

Użytkownik może opuścić zarządzaną sieć, do której wcześniej dołączył.

1. Odłącz komputer od sieci.
2. W programie EasyNetwork w menu **Narzędzia** kliknij polecenie **Opuść sieć**.
3. W oknie dialogowym Opuść sieć wybierz nazwę sieci, którą chcesz opuścić.
4. Kliknij opcję **Opuść sieć**.

ROZDZIAŁ 32

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 167) 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 167) 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 169).

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 33

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 i ich definicje.

Słownik

8

802.11

Zestaw standardów 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 określający sposób uwierzytelniania w sieciach przewodowych i bezprzewodowych. Standard 802.1x jest często stosowany w sieciach bezprzewodowych 802.11. Zobacz też uwierzytelnianie (strona 184).

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

(adres protokołu Internet Protocol) Adres służący do identyfikacji komputera lub urządzenia w sieci TCP/IP. Adres IP ma postać liczby 32-bitowej zapisanej jako cztery liczby rozdzielone kropkami. Każda liczba mieści się w przedziale od 0 do 255 (na przykład 192.168.1.100).

Adres MAC

(adres protokołu Media Access Control) Unikatowy numer seryjny przydzielany urządzeniu fizycznemu (karcie sieciowej) łączącemu się z siecią.

archiwizacja

Proces tworzenia kopii ważnych plików na dysku CD lub DVD, stacji USB, zewnętrznym dysku twardym lub dysku sieciowym. Porównaj z tworzenie kopii zapasowej (strona 183).

atak słownikowy

Odmiana ataku typu „brute force” wykorzystująca słownik w celu odkrycia hasła.

atak typu „brute force”

Metoda hakerska służąca do odgadywania haseł lub kluczy szyfrujących poprzez sprawdzanie każdej możliwej kombinacji znaków, aż do złamania szyfru.

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”

Metoda nielegalnego pozyskiwania danych osobowych, np. haseł, numerów PESEL i informacji o kartach kredytowych, poprzez wysyłanie fałszywych wiadomości e-mail, które wyglądają na pochodzące z zaufanych źródeł, np. banków lub wiarygodnych firm. W fałszywych wiadomościach e-mail znajdują się zwykle prośby o klikanie zawartych w nich łączy w celu weryfikacji lub aktualizacji danych kontaktowych lub informacji o karcie kredytowej.

atak typu DoS (odmowa usługi)

Typ ataku na komputer, serwer lub sieć, który powoduje spowolnienie lub zatrzymanie działania sieci. Zdarza się to, gdy sieć jest zasypywana tak wieloma dodatkowymi żądaniami, że zwykły ruch w niej zostaje mocno spowolniony lub wręcz przerwany. Obiekt ataku typu DoS (odmowa usługi) osiąga stan przeciążenia pod naporem fałszywych żądań połączeń, przez co zaczyna ignorować rzeczywiste żądania.

B

biała lista

Lista witryn sieci Web lub adresów e-mail uważanych za bezpieczne. Witryny sieci Web znajdujące się na białej liście należą do tych, z których użytkownik może korzystać. Adresy e-mail figurujące na białej liście są zaufanymi źródłami, z których użytkownik chce otrzymywać wiadomości. Porównaj z czarna lista (strona 175).

brama zintegrowana

Urządzenie łączące funkcje punktu dostępu, routera i zapory. Niektóre urządzenia mogą być wyposażone w rozszerzenia zabezpieczeń i funkcje mostkowania.

C

czarna lista

W oprogramowaniu antyspamowym jest to lista adresów e-mail, z których użytkownik nie chce odbierać wiadomości, ponieważ uważa je za spam. W kontekście ochrony przed atakami typu „phishing” — lista witryn sieci Web uważanych za szkodliwe. Porównaj z biała lista (strona 175).

D

DAT

Pliki z definicjami sposobu wykrywania, zwane również plikami sygnatur, zawierające dane, które pozwalają identyfikować, wykrywać i usuwać wirusy, konie trojańskie, oprogramowanie szpiegujące i reklamowe oraz inne potencjalnie niepożądane aplikacje.

dialery

Oprogramowanie, które przekierowuje połączenia internetowe do innego podmiotu niż domyślny usługodawca internetowy użytkownika, aby dostawca zawartości lub inna firma niezależna mogli uzyskiwać przychody z dodatkowych opłat za połączenia.

DNS

system nazw domen (ang. Domain Name System). System bazy danych, który tłumaczy adres IP, np. 11.2.3.44, na nazwę domeny, np. www.mcafee.com.

dodatek

Niewielki program, który wzbogaca funkcjonalność większej aplikacji lub rozszerza zakres jej działania. Dodatki umożliwiają np. przeglądarce sieci Web dostęp do i uruchamianie takich plików osadzonych w dokumentach HTML, których format normalnie nie byłby przez nią rozpoznawany, na przykład animacji, plików wideo, pików 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 Internecie domena jest częścią każdego adresu sieci Web. Na przykład w adresie www.mcafee.com domeną jest mcafee.

dysk inteligentny

Zobacz też stacja USB (strona 183).

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

(ang. Extended service set, rozszerzony zestaw usług) Zestaw dwóch lub więcej sieci tworzących pojedynczą podsieć.

F

fragmenty plików

Pozostałości plików rozproszone na dysku. Do fragmentacji dochodzi podczas dodawania i usuwania plików. Fragmentacja może spowolnić działanie komputera.

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

intranet

Prywatna sieć komputerowa stanowiąca zazwyczaj wewnętrzną sieć organizacji, do której dostęp mają wyłącznie autoryzowani użytkownicy.

K

karta PCI sieci bezprzewodowej

(ang. Peripheral Component Interconnect) Karta sieci bezprzewodowej podłączana do gniazda rozszerzeń 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

(ang. Network Interface Card, NIC) Karta podłączana do laptopa lub innego urządzenia, łącząca je z siecią LAN.

karta USB sieci bezprzewodowej

Karta sieci bezprzewodowej podłączana do portu USB w komputerze.

klient

Program działający na komputerze osobistym lub stacji roboczej i zależny od serwera podczas wykonywania pewnych operacji. Na przykład klient poczty e-mail to program umożliwiający wysyłanie i odbieranie wiadomości e-mail.

klient poczty elektronicznej

Program uruchamiany na komputerze w celu wysyłania i odbierania wiadomości e-mail (np. Microsoft Outlook).

klucz

Seria liter i cyfr używana przez dwa urządzenia do uwierzytelniania ich komunikacji. Oba urządzenia muszą posiadać klucz. Zobacz też WEP (strona 184), WPA (strona 185), WPA2 (strona 186), WPA2-PSK (strona 186) i WPA-PSK (strona 185).

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

Procedura zmniejszania wielkości plików w sposób, który minimalizuje ilość miejsca niezbędnego na ich przechowywanie lub przesyłanie.

Konta MAPI

(ang. Messaging Application Programming Interface) Specyfikacja interfejsu firmy Microsoft umożliwiająca różnym programom komunikacyjnym i aplikacjom dla grup roboczych (m.in. do obsługi poczty e-mail, poczty głosowej i faksów) współpracę z pojedynczym klientem, takim jak klient Exchange.

Konta POP3

(ang. 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.

koń trojański

Program, który nie powiela się, ale powoduje uszkodzenia lub obniża poziom bezpieczeństwa komputera. Zwykle to jakaś osoba wysyła konia trojańskiego do użytkowników, ponieważ nie rozsyła się on samodzielnie za pośrednictwem poczty elektronicznej. Można też niechcący pobrać konia trojańskiego z witryny sieci Web lub sieci typu P2P.

Kosz

Wirtualne miejsce na składowanie usuniętych plików i folderów w systemie Windows.

kwarantanna

Wymuszona izolacja pliku lub folderu, który prawdopodobnie zawiera wirusa, spam, podejrzane treści lub potencjalnie niepożądane programy. Plików i folderów poddawanych kwarantannie nie można otwierać ani uruchamiać.

L

LAN

(ang. Local Area Network, sieć lokalna) Sieć komputerowa obejmująca stosunkowo niewielki obszar (np. 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

Lista elementów, którym użytkownik ufa i 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.

lokalizacje monitorowane

Foldery na komputerze monitorowane przez program Backup and Restore.

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.

MSN

(ang. 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 zapisywania na komputerze danych tymczasowych, które były używane często lub ostatnio. 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

Niewielki plik tekstowy używany przez wiele witryn sieci Web do przechowywania informacji o odwiedzanych stronach. Jest on zapisywany na komputerze osoby przeglądającej sieć Web. Może zawierać dane logowania lub rejestracji, informacje o koszyku sklepowym albo preferencje użytkownika. Pliki cookie są używane przede wszystkim przez strony sieci Web w celu identyfikowania użytkowników, którzy zostali wcześniej zarejestrowani w witrynie albo ją odwiedzali. Mogą jednak stanowić też źródło informacji dla hakerów.

plik tymczasowy

Plik utworzony w pamięci lub na dysku przez system operacyjny lub inny program, przeznaczony do użycia w ramach bieżącej sesji, a potem 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 z sieci Web

poczta oparta na sieci Web Usługa poczty elektronicznej dostępna głównie za pośrednictwem przeglądarki sieci Web zamiast za pomocą działającego na komputerze klienta poczty e-mail, np. Microsoft Outlook. Zobacz też wiadomość e-mail (strona 185).

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, przez co nie można wyśledzić nadawcy.

port

Podzespół, przez który przepływają dane napływające do urządzenia komputerowego i wypływające z niego. Komputery osobiste są wyposażane w różnego rodzaju porty, m.in. porty wewnętrzne do podłączania napędów dyskowych, monitorów i klawiatur, jak również porty zewnętrzne do podłączania modemów, drukarek, myszy i innych urządzeń peryferyjnych.

potencjalnie niepożądany program (PUP)

Program, który może być niepożądany, mimo że użytkownik wyraził zgodę na jego pobranie. Na komputerze, na którym został zainstalowany, może zmieniać ustawienia dotyczące bezpieczeństwa i prywatności. Do potencjalnie niepożądanych programów mogą — ale nie muszą — należeć aplikacje szpiegujące i reklamowe oraz dialery, a ich pojawienie się na komputerze może nastąpić przy okazji pobierania programu, który jest przydatny użytkownikowi.

PPPoE

Akronim nazwy Point-to-Point Protocol Over Ethernet. Metoda stosowania protokołu telefonicznego Point-to-Point Protocol (PPP) z użyciem sieci Ethernet jako warstwy transportowej.

protokół

Zestaw reguł umożliwiających komputerom lub urządzeniom prowadzenie wymiany danych. W warstwowej architekturze sieciowej (model Open Systems Interconnection, OSI) każda warstwa ma własne protokoły, które określają sposób komunikacji na danym poziomie. Aby komputery lub urządzenia użytkownika mogły się kontaktować z innymi komputerami, muszą obsługiwać odpowiedni protokół. Zobacz też Open Systems Interconnection (OSI).

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 (strona 182).

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 w systemie operacyjnym lub w aplikacji, gdy podejrzane programy lub procesy próbują zapisać więcej danych w buforze (miejscu zapisu danych tymczasowych), niż może on pomieścić. Przepełnienie bufora może spowodować uszkodzenie zawartości pamięci lub nadpisanie danych w sąsiednich buforach.

przepustowość

Ilość danych, którą można przesłać w określonym czasie.

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

Procedura publicznego udostępniania w Internecie pliku, który ma kopię zapasową. W celu uzyskania dostępu do opublikowanych plików należy przeszukać bibliotekę programu Backup and Restore.

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

(ang. Remote Access Dial-In User Service) Protokół pozwalający na uwierzytelnianie użytkowników, zwykle podczas 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. Zobacz też współdzielone hasło.

rejestr

Baza danych używana przez system Windows do przechowywania jego danych konfiguracyjnych dla wszystkich użytkowników komputera, podzespołów, zainstalowanych programów i ustawień właściwości. Jest ona podzielona na klucze, dla których wprowadza się wartości. Niepożądane programy mogą zmieniać wartości kluczy rejestru lub tworzyć nowe w celu uruchamiania destrukcyjnego kodu.

roaming

Przemieszczanie się z obszaru zasięgu jednego punktu dostępu do drugiego, bez zakłócania dostępu do usług lub utraty połączenia.

robak

Wirus, który rozprzestrzenia się, tworząc swoje kopie na innych dyskach i komputerach lub w innych sieciach. Masowo wysyłane robaki mogą się rozprzestrzeniać wyłącznie z udziałem użytkownika, np. poprzez otwarcie przez niego załącznika lub uruchomienie pobranego pliku. Większość współczesnych wirusów pocztowych jest robakami. Samorozprzestrzeniający się robak może się powielać bez pomocy użytkownika. Przykładami samorozprzestrzeniających się robaków są Blaster i Sasser.

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. Routery odczytują każdy przychodzący pakiet i decydują, jak przesłać go dalej z uwzględnieniem adresu źródłowego i docelowego oraz bieżących warunków ruchu w sieci. 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 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 urządzeń opartych na protokole IP (np. routerów, przełączników, serwerów i zapór), które funkcjonują jako jednostka logiczna. Na przykład „Sieć finansowa” może obejmować wszystkie serwery, routery i komputery, które obsługują dział finansowy firmy. Zobacz też sieć domowa (strona 182).

sieć domowa

Dwa lub większa liczba komputerów połączonych ze sobą w domu w celu udostępniania plików i połączenia internetowego. Zobacz też LAN (strona 178).

skanowanie na żądanie

Zaplanowane sprawdzenie wybranych plików, aplikacji lub urządzeń sieciowych w celu wykrycia zagrożeń, luk w zabezpieczeniach lub innego potencjalnie niepożądanego kodu. Może zostać przeprowadzone natychmiast, w zaplanowanym przyszłym terminie lub z regularnymi interwałami. Porównaj ze skanowaniem podczas uzyskiwania dostępu. Zobacz też luki w zabezpieczeniach.

skanowanie w czasie rzeczywistym

Procedura skanowania 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.

SMTP

(ang. 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

(ang. 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

(ang. Secure Sockets Layer) Protokół zaprojektowany przez firmę Netscape w celu przesyłania prywatnych dokumentów przez Internet. 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 też POP3 (strona 178).

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

Metoda kodowania informacji w taki sposób, aby nie mogły uzyskać do nich dostępu żadne nieupoważnione osoby. Do kodowania danych stosuje się „klucz” i algorytmy matematyczne. Zaszyfrowanych informacji nie można odszyfrować bez odpowiedniego klucza. Wirusy korzystają czasami z szyfrowania, aby uniknąć usunięcia.

T

tekst zaszyfrowany

Tekst, który został zaszyfrowany. Tekstu zaszyfrowanego nie można odczytać, dopóki nie zostanie on przekonwertowany na zwykły tekst (odszyfrowany). Zobacz też szyfrowanie (strona 183).

TKIP

(ang. Temporal Key Integrity Protocol) Element standardu szyfrowania 802.11i dotyczącego bezprzewodowych sieci lokalnych. Szyfrowanie TKIP stanowi rozwinięcie protokołu WEP, który służy do zabezpieczania bezprzewodowych sieci lokalnych 802.11. Szyfrowanie TKIP zapewnia mieszanie kluczy w pakietach i sprawdzanie nienaruszalności wiadomości oraz udostępnia mechanizm ponownego nadawania kluczy, a ponadto eliminuje wady protokołu WEP.

tworzenie kopii zapasowej

Proces tworzenia kopii ważnych plików, zwykle na bezpiecznym serwerze w trybie online. Porównaj z archiwizacja (strona 174).

typy monitorowanych plików

Typy plików (np. DOC, XLS itd.) znajdujących się w lokalizacjach monitorowanych, które program Backup and Restore archiwizuje lub dla których tworzy kopie zapasowe.

U

U3

(ang. 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 uzyskania przez określony czas dostępu do wybranych kopii zapasowych plików. Podczas udostępniania pliku jego kopia zapasowa jest wysyłana do wskazanych przez użytkownika odbiorców wiadomości e-mail. Odbiorcy otrzymują wiadomość e-mail od programu Backup and Restore informującą, że udostępniono im pliki. Wiadomość e-mail zawiera również łącze do udostępnionych plików.

URL

Akronim nazwy Uniform Resource Locator. Standardowy format adresów internetowych.

USB

(ang. Universal Serial Bus) Standardowe złącze w większości współczesnych komputerów, które umożliwia podłączanie rozmaitych urządzeń: od klawiatur i myszy, aż po kamery internetowe, skanery i drukarki.

uwierzytelnianie

Procedura weryfikowania cyfrowej tożsamości nadawcy sygnału komunikacji elektronicznej.

V

VPN

(ang. Virtual Private Network) Prywatna sieć komunikacyjna, która jest skonfigurowana w ramach innej sieci, np. Internetu. Dane przesyłane za pośrednictwem połączenia VPN są szyfrowane i chronione skutecznymi zabezpieczeniami.

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

(ang. 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

(ang. 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. Użytkownik może korzystać z punktu dostępu dowolnego producenta w połączeniu ze sprzętem klienckim dowolnego innego producenta, jeśli oba produkty noszą oznaczenie Wi-Fi Certified.

wiadomość e-mail

(poczta elektroniczna) Wiadomości wysyłane i odbierane elektronicznie w sieci komputerowej. Zobacz też poczta z sieci Web (strona 179).

wirus

Program komputerowy, który potrafi się powielać i zarażać komputery bez wiedzy i zgody użytkowników.

WLAN

(ang. Wireless Local Area Network) Sieć lokalna korzystająca z połączenia bezprzewodowego. W sieci WLAN do komunikacji pomiędzy komputerami zamiast przewodów stosuje się fale radiowe o wysokiej częstotliwości.

WPA

(ang. 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 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 w trybie wstępnie współdzielonego klucza. Hasło należy zmieniać w wypadku każdego komputera bezprzewodowego i punktu dostępu. Zobacz też WPA2-PSK (strona 186) i TKIP (strona 183).

WPA2

Nowsza wersja standardu zabezpieczeń WPA, bazująca na standardzie 802.11i.

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. Służy on do ochrony poufnych fragmentów komunikatów RADIUS. Zobacz też RADIUS (strona 181).

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

W systemie komputerowym lub programie zajście lub wydarzenie, które może zostać wykryte przez oprogramowanie zabezpieczające zgodnie z ustalonymi kryteriami. Zdarzenie powoduje zwykle pewne działanie, np. wysłanie powiadomienia lub dodanie wpisu do dziennika zdarzeń.

zewnętrzny dysk twardy

Dysk twardy znajdujący się na zewnątrz komputera.

zwykły tekst

Tekst, który nie jest zaszyfrowany. Zobacz też szyfrowanie (strona 183).

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.

Licencja

Copyright

ROZDZIAŁ 34

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.

Aby uzyskać informacje o witrynach firmy McAfee w Twoim kraju lub regionie dotyczących pomocy technicznej i produktów do pobrania (w tym podręczników użytkownika), skorzystaj z tabel zamieszczonych poniżej.

Pomoc techniczna i produkty do pobrania

Kraj/region	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
Chiny (chiński uproszczony)	www.mcafeehelp.com	cn.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
Grecja	www.mcafeehelp.com	el.mcafee.com/root/downloads.asp
Hiszpania	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Japonia	www.mcafeehelp.jp	jp.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?langid=48
Korea	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
Meksyk	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
Niemcy	www.mcafeehilfe.com	de.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
Rosja	www.mcafeehelp.com	ru.mcafee.com/root/downloads.asp
Słowacja	www.mcafeehelp.com	sk.mcafee.com/root/downloads.asp
Stany Zjednoczone	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp
Szwecja	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Tajwan	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Turcja	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
Węgry	www.mcafeehelp.com	hu.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

Podręczniki użytkownika pakietu McAfee Total Protection

Kraj/region	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
Chiny (chiński uproszczony)	download.mcafee.com/products/manuals/zh-cn/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
Grecja	download.mcafee.com/products/manuals/el/MTP_userguide_2008.pdf
Hiszpania	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Holandia	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
Japonia	download.mcafee.com/products/manuals/ja/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
Korea	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Meksyk	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Niemcy	download.mcafee.com/products/manuals/de/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
Rosja	download.mcafee.com/products/manuals/ru/MTP_userguide_2008.pdf

Słowacja	download.mcafee.com/products/manuals/sk/MTP_userguide_2008.pdf
Stany Zjednoczone	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf
Szwecja	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Tajwan	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Turcja	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
Węgry	download.mcafee.com/products/manuals/hu/MTP_userguide_2008.pdf
Wielka Brytania	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
Włochy	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf

Podręczniki użytkownika pakietu McAfee Internet Security

Kraj/region	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
Chiny (chiński uproszczony)	download.mcafee.com/products/manuals/zh-cn/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
Grecja	download.mcafee.com/products/manuals/el/MIS_userguide_2008.pdf
Hiszpania	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Holandia	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
Japonia	download.mcafee.com/products/manuals/ja/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
Korea	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
Meksyk	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Niemcy	download.mcafee.com/products/manuals/de/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
Rosja	download.mcafee.com/products/manuals/ru/MIS_userguide_2008.pdf
Słowacja	download.mcafee.com/products/manuals/sk/MIS_userguide_2008.pdf
Stany Zjednoczone	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf
Szwecja	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Tajwan	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Turcja	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
Węgry	download.mcafee.com/products/manuals/hu/MIS_userguide_2008.pdf
Wielka Brytania	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Włochy	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf

Podręczniki użytkownika programu McAfee VirusScan Plus

Kraj/region	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
Chiny (chiński uproszczony)	download.mcafee.com/products/manuals/zh-cn/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
Grecja	download.mcafee.com/products/manuals/el/VSP_userguide_2008.pdf
Hiszpania	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Holandia	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
Japonia	download.mcafee.com/products/manuals/ja/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
Korea	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Meksyk	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Niemcy	download.mcafee.com/products/manuals/de/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
Rosja	download.mcafee.com/products/manuals/ru/VSP_userguide_2008.pdf
Słowacja	download.mcafee.com/products/manuals/sk/VSP_userguide_2008.pdf
Stany Zjednoczone	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf
Szwecja	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Tajwan	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
Turcja	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
Węgry	download.mcafee.com/products/manuals/hu/VSP_userguide_2008.pdf

Wielka Brytania	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Włochy	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf

Podręczniki użytkownika programu McAfee VirusScan

Kraj/region	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
Chiny (chiński uproszczony)	download.mcafee.com/products/manuals/zh-cn/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
Grecja	download.mcafee.com/products/manuals/el/VS_userguide.2008.pdf
Hiszpania	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Holandia	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
Japonia	download.mcafee.com/products/manuals/ja/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
Korea	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Meksyk	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Niemcy	download.mcafee.com/products/manuals/de/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
Rosja	download.mcafee.com/products/manuals/ru/VS_userguide_2008.pdf
Słowacja	download.mcafee.com/products/manuals/sk/VS_userguide_2008.pdf
Stany Zjednoczone	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf
Szwecja	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Tajwan	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Turcja	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
Węgry	download.mcafee.com/products/manuals/hu/VS_userguide.2008.pdf
Wielka Brytania	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
Włochy	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf

W tabeli poniżej przedstawiono Centrum zagrożeń firmy McAfee oraz witryny z informacjami o wirusach dostępne w poszczególnych krajach lub regionach.

Kraj/region	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
Chiny (chiński uproszczony)	www.mcafee.com/us/threat_center	cn.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
Grecja	www.mcafee.com/us/threat_center	gr.mcafee.com/virusInfo
Hiszpania	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Holandia	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
Japonia	www.mcafee.com/us/threat_center	jp.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
Korea	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
Meksyk	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Niemcy	www.mcafee.com/us/threat_center	de.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
Rosja	www.mcafee.com/us/threat_center	ru.mcafee.com/virusInfo
Słowacja	www.mcafee.com/us/threat_center	sk.mcafee.com/virusInfo
Stany Zjednoczone	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo
Szwecja	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Tajwan	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Turcja	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
Węgry	www.mcafee.com/us/threat_center	hu.mcafee.com/virusInfo
Wielka Brytania	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
Włochy	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo

W tabeli poniżej przedstawiono witryny HackerWatch dostępne w poszczególnych krajach lub regionach.

Kraj/region	HackerWatch
Australia	www.hackerwatch.org
Brazylia	www.hackerwatch.org/?lang=pt-br
Chiny (chiński uproszczony)	www.hackerwatch.org/?lang=zh-cn
Czechy	www.hackerwatch.org/?lang=cs
Dania	www.hackerwatch.org/?lang=da
Finlandia	www.hackerwatch.org/?lang=fi
Francja	www.hackerwatch.org/?lang=fr
Grecja	www.hackerwatch.org/?lang=el
Hiszpania	www.hackerwatch.org/?lang=es
Holandia	www.hackerwatch.org/?lang=nl
Japonia	www.hackerwatch.org/?lang=jp
Kanada (angielski)	www.hackerwatch.org
Kanada (francuski)	www.hackerwatch.org/?lang=fr-ca
Korea	www.hackerwatch.org/?lang=ko

Meksyk	www.hackerwatch.org/?lang=es-mx
Niemcy	www.hackerwatch.org/?lang=de
Norwegia	www.hackerwatch.org/?lang=no
Polska	www.hackerwatch.org/?lang=pl
Portugalia	www.hackerwatch.org/?lang=pt-pt
Rosja	www.hackerwatch.org/?lang=ru
Słowacja	www.hackerwatch.org/?lang=sk
Stany Zjednoczone	www.hackerwatch.org
Szwecja	www.hackerwatch.org/?lang=sv
Tajwan	www.hackerwatch.org/?lang=zh-tw
Turcja	www.hackerwatch.org/?lang=tr
Węgry	www.hackerwatch.org/?lang=hu
Wielka Brytania	www.hackerwatch.org
Włochy	www.hackerwatch.org/?lang=it

Indeks

J

K

L

M

N

O

P

R

S

Ś

T

U

V

W

Z