

McAfee®
VirusScan® 2008

Virus and Spyware Protection

Uživatelská příručka

Obsah

McAfee VirusScan	3
McAfee SecurityCenter.....	5
Funkce programu SecurityCenter	6
Použití programu SecurityCenter.....	7
Aktualizace programu SecurityCenter.....	13
Vyřešení nebo ignorování potíží ochrany	17
Práce s výstrahami	21
Zobrazení událostí.....	27
McAfee VirusScan.....	29
Funkce programu VirusScan	30
Spouštění ochrany proti virům v reálném čase	31
Spouštění další ochrany	33
Nastavení ochrany proti virům	37
Prohledávání počítače.....	55
Práce s výsledky prohledávání.....	59
McAfee QuickClean	63
Funkce programu QuickClean.....	64
Čištění počítače.....	65
Defragmentace počítače.....	68
Plánování úloh	69
McAfee Shredder	75
Funkce programu Shredder.....	76
Skartace souborů, složek a disků	77
McAfee Network Manager	79
Funkce programu Network Manager.....	80
Vysvětlení ikon programu Network Manager	81
Nastavení spravované sítě.....	83
Vzdálená správa sítě	89
Reference	94
Slovníček	95
Informace o společnosti McAfee	109
Copyright	109
Licence.....	110
Služby pro zákazníky a technická podpora.....	111
Používání nástroje McAfee Virtual Technician.....	112
Podpora a položky ke stažení.....	113
Rejstřík	121

KAPITOLA 1

McAfee VirusScan

Sada VirusScan a SiteAdvisor nabízí pokročilou detekci a ochranu, která optimalizuje ochranu počítače proti nejnovějším bezpečnostním hrozbám, včetně virů, trojských koní, sledovacích souborů cookie, spywaru, adwaru a dalších potenciálně nežádoucích programů. U programu VirusScan sahá ochrana dále než jen k souborům a složkám počítače nebo notebooku a zaměřuje se na hrozby z různých vstupních bodů, včetně e-mailů, rychlých zpráv a Internetu. Hodnocení bezpečnosti webů programu SiteAdvisor vám pomáhá vyhnout se nebezpečným webům.

V této kapitole

McAfee SecurityCenter.....	5
McAfee VirusScan.....	29
McAfee QuickClean.....	63
McAfee Shredder.....	75
McAfee Network Manager.....	79
Reference.....	94
Informace o společnosti McAfee.....	109
Služby pro zákazníky a technická podpora.....	111

KAPITOLA 2

McAfee SecurityCenter

Program McAfee SecurityCenter umožňuje sledovat stav zabezpečení počítače, má okamžitý přehled o tom, zda je ochrana počítače proti virům, spywaru, ochrana e-mailů a brána firewall aktuální, a reaguje na možná slabá místa zabezpečení. Poskytuje také navigační nástroje a ovládací prvky, které jsou pro koordinaci a správu všech oblastí ochrany počítače potřeba.

Seznamte se s rozhraním programu Security Center před tím, než začnete konfigurovat a spravovat ochranu počítače, a ujistěte se, zda chápete rozdíly mezi pojmy stav ochrany, kategorie ochrany a služby ochrany. Poté program SecurityCenter aktualizujte, abyste tak zajistili nejnovější ochranu, kterou společnost McAfee může poskytnout.

Po dokončení počátečních úkolů konfigurace používejte program SecurityCenter ke sledování stavu zabezpečení počítače. Zjistí-li program SecurityCenter problém ochrany, upozorní uživatele, takže lze podle závažnosti problém opravit nebo ignorovat. Události programu SecurityCenter (jako jsou změny konfigurace vyhledávání virů) lze zkontrolovat v protokolu událostí.

Poznámka: Program SecurityCenter informuje o závažných i méně závažných problémech ochrany ihned, jakmile problémy zjistí. Potřebujete-li pro stanovení problémů ochrany nápovědu, lze spustit nástroj McAfee Virtual Technician.

V této kapitole

Funkce programu SecurityCenter	6
Použití programu SecurityCenter	7
Aktualizace programu SecurityCenter	13
Vyřešení nebo ignorování potíží ochrany	17
Práce s výstrahami.....	21
Zobrazení událostí	27

Funkce programu SecurityCenter

Program SecurityCenter nabízí tyto funkce:

Zjednodušený stav ochrany

Slouží ke snadné kontrole stavu zabezpečení počítače, zjišťování aktualizací a odstraňování možných potíží se zabezpečením.

Automatické aktualizace a inovace

Automatické stahování a instalace aktualizací u registrovaných programů uživatele. Jakmile je k dispozici nová verze zaregistrovaného programu McAfee, získáte ji v průběhu platnosti předplatného zdarma. Vždy budete mít zajištěnou aktuální ochranu.

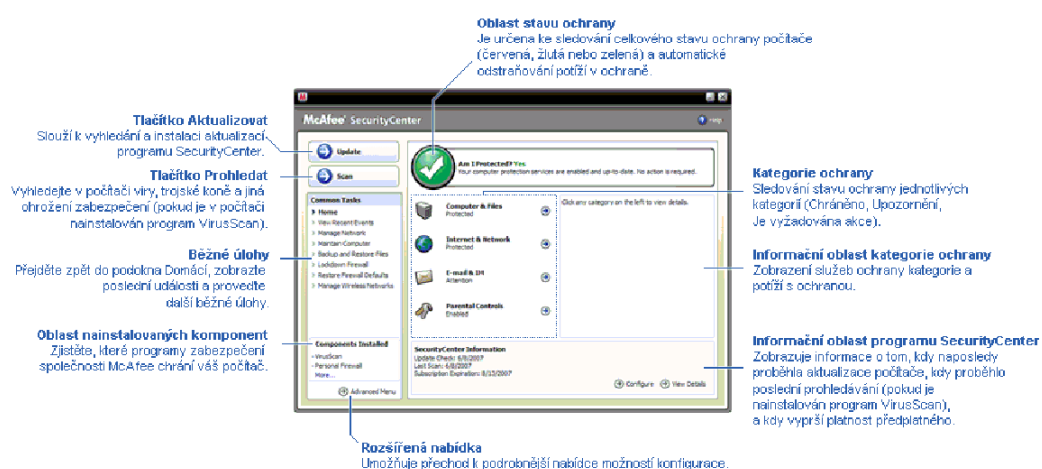
Výstrahy v reálném čase

Bezpečnostní výstrahy upozorňují na mimořádné rozšíření virů a ohrožení zabezpečení a nabízejí možnost hrozbu odstranit, neutralizovat nebo poskytnou o hrozbě další informace.

KAPITOLA 3

Použití programu SecurityCenter

S komponenty a konfiguračními oblastmi programu SecurityCenter, které budete používat ke správě stavu zabezpečení počítače, se seznámte dříve, než začnete program používat. Další informace o terminologii, který byla v tomto obrázku použita, naleznete v tématech *Vysvětlení stavu ochrany* (stránka 8) a *Vysvětlení kategorií ochrany* (stránka 9). Poté můžete zkontrolovat informace účtu McAfee a ověřit platnost vašeho předplatného.



V této kapitole

Vysvětlení stavu ochrany	8
Vysvětlení kategorií ochrany	9
Vysvětlení služeb ochrany	10
Správa účtu McAfee.....	11

Vysvětlení stavu ochrany

Stav zabezpečení počítače se zobrazuje v oblasti stavu ochrany v podokně Domácí programu SecurityCenter. Informuje o tom, zda je počítač proti nejnovějším bezpečnostním hrozbám plně chráněn. Stav ovlivňují různé okolnosti, mezi které patří vnější útoky na bezpečnost, jiné zabezpečovací programy a programy, které mají přístup k síti Internet.

Stav ochrany počítače může být červený, žlutý nebo zelený.

Stav ochrany	Popis
Červený	<p>Počítač není chráněn. Oblast stavu ochrany v podokně Domácí programu SecurityCenter je červená a oznamuje, že nejste chráněni. Program SecurityCenter hlásí minimálně jeden závažný problém zabezpečení.</p> <p>Plnou ochranu získáte tím, že opravíte všechny závažné problémy zabezpečení ve všech kategoriích ochrany (stav kategorie problému je nastaven na možnost Požadována akce a je také zobrazen červeně). Informace o tom, jakým způsobem lze problémy s ochranou vyřešit, naleznete v tématu <i>Vyřešení potíží ochrany</i> (stránka 18).</p>
Žlutý	<p>Počítač je chráněn pouze částečně. Oblast stavu ochrany v podokně Domácí programu SecurityCenter je žlutá a oznamuje, že nejste chráněni. Program SecurityCenter hlásí minimálně jeden méně závažný problém zabezpečení.</p> <p>Plnou ochranu získáte tím, že opravíte nebo budete ignorovat méně závažné problémy zabezpečení související s příslušnými kategoriemi ochrany. Informace o tom, jakým způsobem lze problémy s ochranou vyřešit nebo ignorovat, naleznete v části <i>Vyřešení nebo ignorování potíží ochrany</i> (stránka 17).</p>
Zelený	<p>Počítač je plně chráněn. Oblast stavu ochrany v podokně Domácí programu SecurityCenter je zelená a oznamuje, že jste chráněni. Program SecurityCenter nehlásí žádný závažný nebo méně závažný problém zabezpečení.</p> <p>Každá kategorie ochrany vypisuje seznam služeb, které chrání počítač.</p>

Vysvětlení kategorií ochrany

Služby ochrany programu SecurityCenter lze rozdělit do čtyř kategorií: kategorie Počítač a soubory, Internet a sítě, E-mail a rychlé zprávy a kategorie Rodičovská kontrola. Tyto kategorie pomáhají při procházení a konfiguraci služeb zabezpečení, které chrání počítač.

Klepnutím na název kategorie nakonfigurujete služby ochrany této kategorie a zobrazíte jakékoliv problémy zabezpečení, které byly pro tyto služby zjištěny. Jestliže je stav ochrany počítače červený nebo žlutý, je v jedné nebo více kategoriích zobrazena možnost *Požadována akce* nebo zpráva *Upozornění*, které informují o tom, že program SecurityCenter zjistil v této kategorii problém. Další informace o stavu ochrany naleznete v části *Vysvětlení stavu ochrany* (stránka 8).

Kategorie ochrany	Popis
Počítač a soubory	V kategorii Počítač a soubory lze nakonfigurovat následující služby ochrany: <ul style="list-style-type: none"> ▪ Antivirová ochrana ▪ Ochrana proti nevyžádaným programům (PUP) ▪ Monitorování systému ▪ Ochrana systému Windows
Internet a sítě	V kategorii Internet a sítě lze nakonfigurovat následující služby ochrany: <ul style="list-style-type: none"> ▪ Ochrana brány firewall ▪ Ochrana identity
E-mail a rychlé zprávy	V kategorii E-mail a rychlé zprávy lze nakonfigurovat následující služby ochrany: <ul style="list-style-type: none"> ▪ Ochrana e-mailů ▪ Ochrana proti nevyžádané poště
Rodičovská kontrola	V kategorii Rodičovská kontrola lze nakonfigurovat následující služby ochrany: <ul style="list-style-type: none"> ▪ Blokování obsahu

Vysvětlení služeb ochrany

Služby ochrany představují klíčové komponenty programu SecurityCenter, které lze za účelem ochrany počítače nakonfigurovat. Služby ochrany přímo odpovídají programům McAfee. Pokud například nainstalujete program VirusScan, budou k dispozici následující služby ochrany: Antivirová ochrana, Ochrana proti nevyžádaným programům (PUP), Monitorování systému a služba Ochrana systému Windows. Podrobné informace o jednotlivých službách ochrany naleznete v nápovědě programu VirusScan.

Ve výchozím nastavení jsou při instalaci programu povoleny všechny služby, které jsou programu přiřazeny. Jednotlivé služby ochrany však můžete samozřejmě kdykoliv vypnout. Pokud například nainstalujete službu Privacy Service, jsou povoleny služby Blokování obsahu a Ochrana identity. Pokud službu Blokování obsahu nechcete používat, lze službu úplně vypnout. Službu ochrany lze také dočasně vypnout tehdy, jestliže provádíte úkoly jako je instalace nebo údržba.

Správa účtu McAfee

Účet McAfee spravujte pomocí programu SecurityCenter, který nabízí snadný přístup a kontrolu informací o účtu a ověření aktuálního stavu předplatného.

Poznámka: Jestliže jste programy McAfee nainstalovali z disku CD a chcete nastavit nebo aktualizovat váš účet McAfee, je třeba programy zaregistrovat na webu McAfee. Pouze poté máte nárok na pravidelné a automatické aktualizace programů.


Správa účtu McAfee – postup

Z programu SecurityCenter je přístup k informacím o účtu McAfee (Můj účet) snadný.

- 1 V části **Běžné úkoly** klepněte na tlačítko **Můj účet**.
- 2 Přihlaste se k účtu McAfee.

Ověření předplatného

Ověření předplatného slouží k tomu, abyste se ujistili, zda předplatné nevypršelo.

- Klepněte pravým tlačítkem myši na ikonu programu SecurityCenter  v oznamovací oblasti systému Windows zcela vpravo na hlavním panelu a potom klepněte na příkaz **Ověřit předplatné**.

KAPITOLA 4

Aktualizace programu SecurityCenter

Program SecurityCenter pomocí vyhledávání a instalace aktualizací online každé čtyři hodiny zajišťuje, že jsou zaregistrované programy McAfee aktuální. V závislosti na nainstalovaných a zaregistrovaných programech mohou aktualizace online zahrnovat nejnovější definice virů a aktualizace ochrany proti hackerům, nevyžádané pošty, spywaru nebo ochrany proti krádežím identity. Chcete-li aktualizace zjišťovat dříve, než je výchozí interval čtyř hodin, lze tak učinit kdykoliv. Zatímco program Security Center zjišťuje aktualizace, můžete pokračovat v provádění dalších úkolů.

I když lze změnit způsob, jakým program SecurityCenter kontroluje a instaluje aktualizace, tento postup se nedoporučuje. Můžete například program SecurityCenter nakonfigurovat tak, aby aktualizace stahoval ale neinstaloval nebo aby vás před stahováním nebo instalací aktualizací upozornil. Automatické aktualizace lze také vypnout.

Poznámka: Jestliže jste programy McAfee nainstalovali z disku CD, je třeba programy zaregistrovat na webu McAfee a teprve poté budete získávat pravidelné a automatické aktualizace těchto programů.


V této kapitole

Zjišťování aktualizací.....	13
Konfigurace automatických aktualizací.....	14
Zakázání automatických aktualizací	14

Zjišťování aktualizací

Jestliže je počítač připojený k Internetu, zjišťuje ve výchozím nastavení program SecurityCenter aktualizace automaticky každé čtyři hodiny; pokud však chcete aktualizace zjišťovat dříve než jsou tyto čtyři hodiny, je to možné. Pokud jsou automatické aktualizace vypnuty, je pravidelné zjišťování aktualizací zodpovědností uživatele.

- V podokně Domácí programu SecurityCenter klepněte na tlačítko **Aktualizovat**.

Tip: Aktualizace lze zjišťovat, aniž by bylo potřeba spouštět program SecurityCenter. Klepněte pravým tlačítkem myši na ikonu programu SecurityCenter  v oznamovací oblasti systému Windows zcela vpravo na hlavním panelu a poté klepněte na možnost **Aktualizace**.

Konfigurace automatických aktualizací

Jestliže je počítač připojený k Internetu, program SecurityCenter kontroluje a instaluje aktualizace automaticky každé čtyři hodiny. Chcete-li toto výchozí chování změnit, lze program SecurityCenter nakonfigurovat tak, aby aktualizace stahoval automaticky a poté uživatele informoval o tom, že jsou aktualizace připraveny k instalaci, nebo aby uživatele před stahováním aktualizací informoval.

Poznámka: Program SecurityCenter pomocí výstrah oznámí, že jsou aktualizace připraveny ke stažení nebo že jsou nainstalovány. Pomocí výstrah lze aktualizace stáhnout, nainstalovat nebo odložit. Jestliže programy aktualizujete z výstrahy, můžete být před stahováním a instalací vyzváni k ověření předplatného. Další informace naleznete v tématu *Práce s výstrahami* (stránka 21).

- 1 Otevřete konfigurační podokno programu SecurityCenter.
Jak?
 1. V části **Běžné úkoly** klepněte na tlačítko **Domácí**.
 2. Klepněte v pravém podokně, v části **Informace o programu SecurityCenter**, na tlačítko **Konfigurovat**.
- 2 Klepněte v podokně Konfigurace programu SecurityCenter v rámci položky **Automatické aktualizace jsou zakázány** na možnost **Zapnout** a poté na položku **Upřesnit**.
- 3 Klepněte na jedno z následujících tlačítek:
 - **Instalovat aktualizace automaticky a upozornit, když budou služby aktualizovány (doporučeno)**
 - **Stahovat aktualizace automaticky a upozornit, jakmile budou připraveny k instalaci**
 - **Upozornit před stahováním všech aktualizací**
- 4 Klepněte na tlačítko **OK**.

Zakázání automatických aktualizací

Pokud vypnete automatické aktualizace, je pravidelné zjišťování aktualizací vaší zodpovědností, jinak nebude mít počítač nejnovější ochranu zabezpečení. Informace o ručním zjišťování aktualizací naleznete v tématu *Zjišťování aktualizací* (stránka 13).

- 1 Otevřete konfigurační podokno programu SecurityCenter.
Jak?

1. V části **Běžné úkoly** klepněte na tlačítko **Domácí**.
 2. Klepněte v pravém podokně, v části **Informace o programu SecurityCenter**, na tlačítko **Konfigurovat**.
- 2** V programu SecurityCenter klepněte v podokně Konfigurace v rámci položky **Automatické aktualizace jsou povoleny** na možnost **Vypnout**.

Tip: Automatické aktualizace povolíte klepnutím na tlačítko **Zapnout** nebo v podokně Možnosti aktualizace zrušte zaškrtnutí tlačítka **Zakázat automatické aktualizace a umožnit ruční kontrolu aktualizací**.

KAPITOLA 5

Vyřešení nebo ignorování potíží ochrany

Program SecurityCenter informuje o závažných i méně závažných problémech ochrany ihned, jakmile problémy zjistí. Závažné potíže ochrany vyžadují okamžitou nápravu a ohrožují stav ochrany (změna barvy stavu na červený). Méně závažné potíže ochrany nevyžadují okamžitou nápravu a podle toho, o jaký typ problému se jedná, nemusí (ale mohou) ohrozit stav ochrany. Chcete-li dosáhnout zeleného stavu ochrany, je třeba vyřešit všechny závažné potíže a všechny méně závažné potíže buď vyřešit nebo ignorovat. Potřebujete-li pro stanovení problémů ochrany nápovědu, lze spustit nástroj McAfee Virtual Technician. Další informace o nástroji McAfee Virtual Technician naleznete v nápovědě nástroje McAfee Virtual Technician.

V této kapitole

Vyřešení potíží ochrany	18
Ignorování potíží ochrany	20

Vyřešení potíží ochrany

Většinu potíží zabezpečení lze vyřešit automaticky. Mohou se však vyskytnout problémy, které vyžadují akci uživatele. Jestliže je například služba Ochrana brány firewall vypnuta, může službu program SecurityCenter zapnout automaticky. Pokud však služba Ochrana brány firewall není nainstalována, je třeba službu nainstalovat. Následující tabulka popisuje některé další akce, které můžete při ručním řešení potíží ochrany provést:

Problém	Akce
Během posledních 30 dnů nebylo provedeno úplné prohledávání počítače.	Prohledejte počítač ručně. Další informace naleznete v nápovědě programu VirusScan.
Soubory rozpoznávacích signatur (DAT) jsou zastaralé.	Aktualizujte ochranu ručně. Další informace naleznete v nápovědě programu VirusScan.
Program není nainstalován.	Nainstalujte program z webu McAfee nebo z disku CD.
Některé komponenty programu chybí.	Program znovu nainstalujte z webu McAfee nebo z disku CD.
Program není zaregistrován a nemůže získat plnou ochranu.	Zaregistrujte program na webu McAfee.
Platnost programu vypršela.	Zjistěte na webu McAfee stav vašeho účtu.

Poznámka: Často se stává, že má jediný problém ochrany vliv na více kategorií ochrany. V takovém případě vyřešení problému v jedné kategorii problém odstraní ze všech ostatních kategorií ochrany.

Vyřešení potíží ochrany automaticky

Většinu potíží s ochranou dokáže program SecurityCenter vyřešit automaticky. Do protokolu událostí se nezaznamenávají konfigurační změny, které program SecurityCenter provádí při automatické opravě potíží ochrany. Další informace týkající se událostí naleznete v tématu *Zobrazování událostí* (stránka 27).

- 1 V části **Běžné úkoly** klepněte na tlačítko **Domácí**.
- 2 V programu SecurityCenter klepněte v podokně Domácí na možnost **Opravit**.

Vyřešení potíží ochrany ručně

Jestliže jeden nebo více problémů zůstávají i poté, co jste zkusili tyto problémy vyřešit automaticky, lze problémy vyřešit ručně.

- 1** V části **Běžné úkoly** klepněte na tlačítko **Domácí**.
- 2** V podokně Domácí klepněte na kategorii ochrany, ve které hlásí program SecurityCenter problémy.
- 3** Klepněte na odkaz, který následuje za popisem problému.

Ignorování potíží ochrany

Zjistí-li program SecurityCenter méně závažný problém, lze problém buď vyřešit nebo ignorovat. Další méně závažné problémy jsou ignorovány automaticky (například nenainstalovaná ochrana proti nevyžádané poště nebo služba Privacy Service). Pokud je stav ochrany počítače zelený, nejsou ignorované potíže v informační oblasti kategorie ochrany v podokně Domácí zobrazovány. Ignorujete-li problém, ale později se rozhodnete tento problém v informační oblasti kategorie ochrany zobrazovat i v případě, že stav ochrany počítače není zelený, lze ignorovaný problém zobrazit.

Ignorování problému ochrany

Zjistí-li program SecurityCenter méně závažný problém a problém nechcete opravit, lze problém ignorovat. Jestliže problém ignorujete, bude problém z informační oblasti kategorie ochrany programu SecurityCenter odstraněn.

- 1 V části **Běžné úkoly** klepněte na tlačítko **Domácí**.
- 2 V podokně Domácí klepněte na kategorii ochrany, ve které je hlášen problém.
- 3 Klepněte u problému ochrany na odkaz **Ignorovat**.

Zobrazení a skrytí ignorovaných potíží

V závislosti na závažnosti potíží lze ignorované potíže ochrany zobrazit nebo skrýt.

- 1 Otevřete podokno Možnosti výstrah.
Jak?
 1. V části **Běžné úkoly** klepněte na tlačítko **Domácí**.
 2. Klepněte v pravém podokně, v části **Informace o programu SecurityCenter**, na tlačítko **Konfigurovat**.
 3. Klepněte v části **Výstrahy** na položku **Upřesnit**.
- 2 V podokně Konfigurace programu SecurityCenter klepněte na položku **Ignorované problémy**.
- 3 V podokně Ignorované problémy proveďte následující akce:
 - Chcete-li problém ignorovat, zaškrtněte políčko problému.
 - Chcete-li problém hlásit v informační oblasti kategorie ochrany, zaškrtnutí políčka problému zrušte.
- 4 Klepněte na tlačítko **OK**.

Tip: Problém také lze ignorovat tím, že klepnete vedle problému, který je hlášen v informační oblasti kategorie ochrany, na odkaz **Ignorovat**.

KAPITOLA 6

Práce s výstrahami

Výstrahy jsou malá automaticky otevíraná okna, která jsou zobrazována v pravém dolním rohu obrazovky, jestliže dojde k jistým událostem programu SecurityCenter. Výstrahy poskytují podrobné informace o události a doporučení a možnosti, jakým způsobem lze problémy související s událostí vyřešit. Součástí některých výstrah jsou také odkazy na další informace o události. Tyto odkazy spouští globální web McAfee nebo odesílají společnosti McAfee informace, které slouží k odstraňování potíží.

Existují tři typy výstrah: červená, žlutá a zelená.

Typ výstrahy	Popis
Červená	Červená výstraha představuje závažné upozornění, které vyžaduje reakci uživatele. Červená výstraha je zobrazena tehdy, jestliže nedokáže program SecurityCenter určit, jak lze vyřešit potíže automaticky.
Žlutá	Žlutá výstraha je nezávažné upozornění, které zpravidla vyžaduje reakci uživatele.
Zelená	Zelená výstraha je méně závažné upozornění, které zpravidla nevyžaduje reakci uživatele. Zelené výstrahy poskytují základní informace o události.

Výstrahy mají při sledování a správě stavu ochrany důležitou úlohu a proto je nelze zakázat. Lze však určit, zda budou určité typy informačních výstrah zobrazovány a lze nakonfigurovat některé další možnosti výstrah (jako například zda má program SecurityCenter přehrát s výstrahou zvuk nebo při spuštění zobrazovat úvodní obrazovku McAfee).

V této kapitole

Zobrazování a skrytí informačních výstrah.....	22
Konfigurace možností výstrah	24

Zobrazování a skrytí informačních výstrah

Informační výstrahy upozorňují na vzniklé události, které neohrožují zabezpečení počítače. Pokud jste například nastavili ochranu brány firewall, objeví se ve výchozím nastavení informační výstraha pokaždé, když je programu v počítači povolen přístup k Internetu. Pokud nechcete určitý typ informační výstrahy zobrazovat, lze výstrahu skrýt. Pokud nechcete zobrazovat všechny informační výstrahy, lze skrýt všechny výstrahy. Všechny informační výstrahy lze také skrýt tehdy, jestliže hrajete počítačovou hru v režimu zobrazení na celou obrazovku. Jestliže ukončíte hru a režim zobrazení na celou obrazovku, začne program SecurityCenter informační výstrahy opět zobrazovat.

Pokud informační výstrahu skryjete omylem, lze výstrahu kdykoliv opět zobrazit. Program SecurityCenter zobrazuje ve výchozím nastavení všechny informační výstrahy.

Zobrazení nebo skrytí informačních výstrah – postup

Program SecurityCenter lze nakonfigurovat tak, že bude zobrazovat některé informační výstrahy a jiné bude skrývat, nebo že bude skrývat všechny informační výstrahy.

1 Otevřete podokno Možnosti výstrah.

Jak?

1. V části **Běžné úkoly** klepněte na tlačítko **Domácí**.
2. Klepněte v pravém podokně, v části **Informace o programu SecurityCenter**, na tlačítko **Konfigurovat**.
3. Klepněte v části **Výstrahy** na položku **Upřesnit**.

2 V podokně Konfigurace programu SecurityCenter klepněte na položku **Informační výstrahy**.

3 V podokně Informační výstrahy proveďte následující akce:

- Chcete-li informační výstrahu zobrazovat, zrušte zaškrtnutí políčka výstrahy.
- Chcete-li informační výstrahu skrývat, políčko výstrahy zaškrtněte.
- Chcete-li skrývat všechny informační výstrahy, zaškrtněte políčko **Nezobrazovat informační výstrahy**.

4 Klepněte na tlačítko **OK**.

Tip: Jednotlivou informační výstrahu lze také skrýt zaškrtnutím políčka **Tuto výstrahu již příště nezobrazovat** v samotné informační výstraze. Jestliže jste výstrahu skryli, lze informační výstrahu opět zobrazit tím, že zrušíte v podokně Informační výstrahy zaškrtnutí příslušného políčka.

Zobrazení a skrytí informačních výstrah při hraní her

Informační výstrahy lze skrýt tehdy, jestliže hrajete počítačovou hru v režimu zobrazení na celou obrazovku. Jestliže hru a režim zobrazení na celou obrazovku ukončíte, začne program SecurityCenter informační výstrahy opět zobrazovat.

1 Otevřete podokno Možnosti výstrah.

Jak?

1. V části **Běžné úkoly** klepněte na tlačítko **Domácí**.
 2. Klepněte v pravém podokně, v části **Informace o programu SecurityCenter**, na tlačítko **Konfigurovat**.
 3. Klepněte v části **Výstrahy** na položku **Upřesnit**.
- 2** V podokně Možnosti výstrah zaškrtněte nebo zrušte zaškrtnutí políčka **Zobrazit informační výstrahy, pokud je zjištěn herní režim**.
- 3** Klepněte na tlačítko **OK**.

Konfigurace možností výstrah

Pomocí programu SecurityCenter lze konfigurovat vzhled a četnost výstrah. Lze však upravit pouze některé základní možnosti výstrah. Například můžete s výstrahami přehrát zvuk nebo skrýt při spuštění systému Windows zobrazování výstrahy úvodní obrazovky. Lze také skrýt výstrahy, které uživatele upozorňují na mimořádné rozšíření virů a další bezpečnostní hrozby v komunitě online.

Přehrání zvuku při zobrazení výstrahy

Chcete-li být na výskyt výstrah slyšitelně upozorněni, lze program SecurityCenter nastavit tak, aby byl s každou výstrahou přehrán určitý zvuk.

1 Otevřete podokno Možnosti výstrah.

Jak?

1. V části **Běžné úkoly** klepněte na tlačítko **Domácí**.
2. Klepněte v pravém podokně, v části **Informace o programu SecurityCenter**, na tlačítko **Konfigurovat**.
3. Klepněte v části **Výstrahy** na položku **Upřesnit**.

2 Zaškrtněte v podokně Možnosti výstrah v rámci položky **Zvuk** políčko **Při zobrazení výstrahy přehrát zvuk**.

Skrutí úvodní obrazovky při spuštění

Ve výchozím nastavení se při spuštění systému Windows krátce objeví úvodní obrazovka McAfee, která uživatele informuje o tom, že počítač chrání program SecurityCenter. Pokud však úvodní obrazovku nechcete zobrazovat, lze tuto výstrahu skrýt.

1 Otevřete podokno Možnosti výstrah.

Jak?

1. V části **Běžné úkoly** klepněte na tlačítko **Domácí**.
2. Klepněte v pravém podokně, v části **Informace o programu SecurityCenter**, na tlačítko **Konfigurovat**.
3. Klepněte v části **Výstrahy** na položku **Upřesnit**.

2 V podokně Možnosti výstrah zrušte v rámci položky **Úvodní obrazovka** zaškrtnutí políčka **Při spuštění systému Windows zobrazit úvodní obrazovku společnosti McAfee**.

Tip: Úvodní obrazovku lze kdykoliv zaškrtnutím políčka **Při spuštění systému Windows zobrazit úvodní obrazovku společnosti McAfee** opět zobrazit.

Skrytí výstrah na mimořádné rozšíření virů

Lze skrýt výstrahy, které uživatele upozorňují na mimořádné rozšíření virů a další bezpečnostní hrozby v komunitě online.

1 Otevřete podokno Možnosti výstrah.

Jak?

1. V části **Běžné úkoly** klepněte na tlačítko **Domácí**.
2. Klepněte v pravém podokně, v části **Informace o programu SecurityCenter**, na tlačítko **Konfigurovat**.
3. Klepněte v části **Výstrahy** na položku **Upřesnit**.

2 Zrušte v podokně Možnosti výstrah zaškrtnutí políčka **Upozornit, dojde-li k ohrožení viry nebo k ohrožení zabezpečení**.

Tip: Výstrahy na mimořádné rozšíření virů lze kdykoliv zaškrtnutím políčka **Upozornit, dojde-li k ohrožení viry nebo k ohrožení zabezpečení**, opět zobrazit.

KAPITOLA 7

Zobrazení událostí

Událost představuje akci nebo konfigurační změnu, ke které došlo v rámci určité kategorie ochrany a souvisejících služeb ochrany. Různé služby ochrany zaznamenávají různé typy událostí. Program SecurityCenter například zaznamená událost tehdy, jestliže je služba ochrany povolena nebo zakázána; ochrana proti virům zaznamená událost při každém zjištění a odstranění viru a ochrana brány firewall zaznamená událost při každém blokováném pokusu o přístup k Internetu. Další informace o kategoriích ochrany naleznete v tématu *Vysvětlení kategorií ochrany* (stránka 9).

Události lze zobrazit při řešení potíží s konfigurací a kontrole operací, které prováděli jiní uživatelé. Mnoha rodičům protokol události slouží ke sledování chování dětí na Internetu. Chcete-li zobrazit pouze posledních 30 událostí, ke kterým došlo, zobrazte nedávné události. Chcete-li prozkoumat vyčerpávající seznam všech událostí, ke kterým došlo, zobrazte všechny události. Jestliže zobrazujete všechny události, spustí program SecurityCenter protokol událostí, ve kterém budou události seřazeny podle kategorie ochrany, ve které k události došlo.

V této kapitole

Zobrazení nedávných událostí.....	27
Zobrazení všech událostí.....	27

Zobrazení nedávných událostí

Chcete-li zobrazit pouze posledních 30 událostí, ke kterým došlo, zobrazte nedávné události.

- V části **Běžné úkoly** klepněte na možnost **Zobrazit nedávné události**.

Zobrazení všech událostí

Chcete-li prozkoumat vyčerpávající seznam všech událost, ke kterým došlo, zobrazte všechny události.

- 1 V části **Běžné úkoly** klepněte na možnost **Zobrazit nedávné události**.
- 2 V podokně Nedávné události klepněte na položku **Zobrazit protokol**.
- 3 Klepněte v levém podokně protokolu událostí na typ událostí, které chcete zobrazit.

McAfee VirusScan

Pokročilá detekce a služby ochrany programu VirusScan chrání uživatele i počítače proti nejnovějším bezpečnostním hrozbám, včetně virů, trojských koní, sledovacích souborů cookie, spywaru, adwaru a dalších potencionálně nežádoucích programů. Ochrana sahá dále než jen na soubory a složky počítače a zaměřuje se na hrozby z různých vstupních bodů, včetně e-mailů, rychlých zpráv a Internetu.

S programem VirusScan je ochrana počítače okamžitá a neustálá a nevyžaduje únavné nastavování. Zatímco uživatel pracuje, hraje hry, prochází Internet nebo kontroluje poštu, ochrana je spuštěna na pozadí a v reálném čase sleduje, prohledává a zjišťuje možné hrozby. V pravidelných intervalech jsou spouštěna vyčerpávající prohledávání, která kontrolují počítač pomocí komplexnějších sad možností. Pokud uživatel chce, nabízí program VirusScan pružné vlastní nastavení tohoto chování. Počítač však zůstává chráněn i tehdy, jestliže tento případ nenastal.

Při běžném používání počítače mohou do počítače proniknout viry, červi a další možné hrozby. Jestliže k tomuto dojde, program VirusScan uživatele na hrozbu upozorní, ale obvykle situaci zvládne sám a nakažené položky vymaže nebo přesune do karantény dříve, než je způsobena jakákoliv škoda. V několika málo případech se může stát, že bude potřeba provést další akce. V těchto případech umožní program VirusScan uživateli rozhodnout o dalším postupu (prohledat znovu při dalším spuštění počítače, zjištěné položky ponechat nebo odebrat).

Poznámka: Program SecurityCenter informuje o závažných i méně závažných problémech ochrany ihned, jakmile problémy zjistí. Potřebujete-li pro stanovení problémů ochrany nápovědu, lze spustit nástroj McAfee Virtual Technician.

V této kapitole

Funkce programu VirusScan.....	30
Spouštění ochrany proti virům v reálném čase	31
Spouštění další ochrany.....	33
Nastavení ochrany proti virům.....	37
Prohledávání počítače	55
Práce s výsledky prohledávání	59

Funkce programu VirusScan

Program SecurityCenter nabízí tyto funkce.

Komplexní ochrana proti virům

Pokročilá detekce a služby ochrany programu VirusScan chrání uživatele i počítače proti nejnovějším bezpečnostním hrozbám, včetně virů, trojských koní, sledovacích souborů cookie, spywaru, adwaru a dalších potencionálně nežádoucích programů. Ochrana sahá dále než jen na soubory a složky počítače a zaměřuje se na hrozby z různých vstupních bodů, včetně e-mailů, rychlých zpráv a Internetu. Nevyžaduje únavné nastavování.

Možnosti prohledávání s minimálními nároky na zdroje

Jestliže je prohledávání příliš pomalé, lze možnost prohledávání s minimálními nároky na počítač zakázat. Vezměte však na vědomí, že ochrana proti virům bude mít vyšší prioritu než jiné úkoly. Pokud uživatel chce, nabízí program VirusScan pružné vlastní nastavení možností prohledávání v reálném čase a ručního prohledávání. Počítač však zůstává chráněn i tehdy, jestliže tento případ nenastal.

Automatické opravy

Jestliže program VirusScan zjistí ohrožení zabezpečení v průběhu spuštěného prohledávání v reálném čase nebo ručního prohledávání, pokusí se v závislosti na typu ohrožení zvládnout ohrožení automaticky. Tímto způsobem lze bez zásahu uživatele zjistit a neutralizovat většinu ohrožení. V několika málo případech se může stát, že program VirusScan ohrožení sám neutralizovat nedokáže. V těchto případech umožní program VirusScan uživateli rozhodnout o dalším postupu (prohledat znovu při dalším spuštění počítače, zjištěné položky ponechat nebo odebrat).

Pozastavení úkolů v režimu zobrazení na celou obrazovku

Program VirusScan určité množství úkolů (včetně automatických aktualizací a ručního prohledávání) pozastavuje tehdy, jestliže uživatel provádí jakékoli aktivity, které zaberou celou obrazovku počítače, jako je sledování filmů nebo hraní počítačových her.

Spouštění ochrany proti virům v reálném čase

Program VirusScan nabízí dva typy ochrany proti virům: ochranu v reálném čase a ruční ochranu. Ochrana proti virům v reálném čase nepřetržitě sleduje počítač, zjišťuje aktivity virů a při každém přístupu k souborům (uživatelé nebo počítačem) soubory prohledává. Ruční ochrana proti virům umožňuje prohledávat soubory na požádání. Chcete-li zajistit stálou ochranu počítače proti nejnovějším bezpečnostním hrozbám, ponechte ochranu v reálném čase zapnutou a naplánujte spouštění pravidelných a komplexnějších ručních prohledávání. Výchozím intervalem prohledávání programu VirusScan je jednou za týden. Další informace o prohledávání v reálném čase a o ručním prohledávání naleznete v tématu *Prohledávání počítače* (stránka 55).

V několika málo případech se může stát, že budete chtít prohledávání v reálném čase dočasně pozastavit (pokud chcete například některé možnosti prohledávání změnit nebo vyřešit potíže s výkonem). Jestliže je vypnuta ochrana proti virům v reálném čase, není počítač chráněn a stav ochrany programu SecurityCenter je červený. Další informace o stavu ochrany naleznete v nápovědě programu SecurityCenter v části Vysvětlení stavu ochrany.

Spouštění ochrany proti virům v reálném čase

Ochrana proti virům v reálném čase je ve výchozím nastavení zapnuta a chrání počítač proti virům, trojským koním a dalším hrozbám zabezpečení. Jestliže ochranu proti virům v reálném čase vypnete, je třeba ochranu opět zapnout, chcete-li zůstat chráněni.

- 1 Otevřete konfigurační podokno Počítač a soubory.

Jak?

1. Klepněte v levém podokně na položku **Rozšířená nabídka**.
2. Klepněte na tlačítko **Konfigurovat**.
3. V konfiguračním podokně klepněte na položku **Počítač a soubory**.

- 2 V části **Antivirová ochrana** klepněte na **Zapnout**.

Zastavení ochrany proti virům v reálném čase

Ochranu proti virům v reálném čase lze dočasně vypnout a poté zadat, kdy bude ochrana pokračovat. Ochranu lze automaticky obnovit po intervalu 15, 30, 45 nebo 60 minut, při restartování počítače nebo nikdy.

- 1 Otevřete konfigurační podokno Počítač a soubory.

Jak?

1. Klepněte v levém podokně na položku **Rozšířená nabídka**.
 2. Klepněte na tlačítko **Konfigurovat**.
 3. V konfiguračním podokně klepněte na položku **Počítač a soubory**.
- 2 V rámci položky **Antivirová ochrana** klepněte na možnost **Vypnout**.
 - 3 Vyberte v dialogovém okně čas, kdy bude prohledávání v reálném čase pokračovat.
 - 4 Klepněte na tlačítko **OK**.

KAPITOLA 9

Spouštění další ochrany

Ochranu proti virům v reálném čase programu VirusScan doplňuje pokročilá ochrana proti skriptům, spywaru a ochrana proti potenciálně škodlivým e-mailům a přílohám rychlých zpráv. Ve výchozím nastavení jsou prohledávání skriptů, ochrana proti spywaru, ochrana e-mailů a rychlých zpráv zapnuty a chrání počítač.

Prohledávání skriptů

Prohledávání skriptů zjišťuje potenciálně škodlivé skripty a zabraňuje tomu, aby byly tyto skripty spuštěny v počítači. Sleduje počítač a zjišťuje aktivity podezřelých skriptů, jako jsou například skripty, které vytváří, kopírují nebo odstraňují soubory, skripty otevírající registr systému Windows, a upozorní uživatele dříve, než je způsobena jakákoliv škoda.

Ochrana proti spywaru

Ochrana proti spywaru zjišťuje spyware, adware a další potenciálně nežádoucí programy. Spyware je software, který může být tajně nainstalován do počítače za účelem sledování chování uživatele, získávání osobních údajů nebo dokonce za účelem zásahu do ovládání počítače pomocí instalace dodatečného softwaru a přesměrování aktivit prohlížeče.

Ochrana e-mailů

Ochrana e-mailů zjišťuje podezřelé aktivity v e-mailech a přijímaných a odesílaných přílohách.

Ochrana rychlých zpráv

Ochrana rychlých zpráv zjišťuje potenciální hrozby zabezpečení, které by mohly pocházet z přijímaných příloh rychlých zpráv. Ochrana také zabraňuje tomu, aby programy rychlého zaslání zpráv sdílely osobní informace uživatele.

V této kapitole

Spuštění prohledávání skriptů	34
Spuštění ochrany proti spywaru	34
Spuštění ochrany e-mailů	34
Spuštění ochrany rychlých zpráv	35

Spuštění prohledávání skriptů

Chcete-li zjišťovat potenciálně škodlivé skripty a zabránit tomu, aby byly tyto skripty spuštěny v počítači, zapněte prohledávání skriptů. Prohledávání skriptů upozorní uživatele tehdy, jestliže se skript pokusí vytvořit, kopírovat nebo odebrat soubory z počítače nebo provést změny v registru systému Windows.

1 Otevřete konfigurační podokno Počítač a soubory.

Jak?

1. Klepněte v levém podokně na položku **Rozšířená nabídka**.
2. Klepněte na tlačítko **Konfigurovat**.
3. V konfiguračním podokně klepněte na položku **Počítač a soubory**.

2 V části **Prohledávání skriptů** klepněte na položku **Zapnout**.

Poznámka: I když můžete prohledávání skriptů kdykoliv vypnout, bude po vypnutí počítač nedostatečně zabezpečený proti škodlivým skriptům.

Spuštění ochrany proti spywaru

Chcete-li zjišťovat a odstraňovat spyware, adware a další potenciálně nežádoucí programy, které mohou bez vašeho povolení shromažďovat a odesílat data, zapněte ochranu proti spywaru.

1 Otevřete konfigurační podokno Počítač a soubory.

Jak?

1. Klepněte v levém podokně na položku **Rozšířená nabídka**.
2. Klepněte na tlačítko **Konfigurovat**.
3. V konfiguračním podokně klepněte na položku **Počítač a soubory**.

2 V části **Prohledávání skriptů** klepněte na položku **Zapnout**.

Poznámka: I když můžete ochranu proti spywaru kdykoliv vypnout, bude po vypnutí počítač nedostatečně zabezpečený proti potenciálně nežádoucím programům.

Spuštění ochrany e-mailů

Chcete-li zjišťovat červy a potenciální hrozby v příchozích (POP3) a odchozích (SMTP) e-mailových zprávách a přílohách, zapněte ochranu e-mailů.

1 Otevřete konfigurační podokno E-mailů a rychlé zprávy.

Jak?

1. Klepněte v levém podokně na položku **Rozšířená nabídka**.
2. Klepněte na tlačítko **Konfigurovat**.
3. V konfiguračním podokně klepněte na položku **E-mailly a rychlé zprávy**.

2 V části **Ochrana e-mailů** klepněte na položku **Zapnout**.

Poznámka: I když můžete ochranu e-mailů kdykoliv vypnout, bude po vypnutí počítač nedostatečně zabezpečený proti škodlivým skriptům.

Spuštění ochrany rychlých zpráv

Chcete-li zjišťovat hrozby zabezpečení, které mohou být součástí příloh příchozích rychlých zpráv, zapněte ochranu rychlých zpráv.

1 Otevřete konfigurační podokno E-mailly a rychlé zprávy.

Jak?

1. Klepněte v levém podokně na položku **Rozšířená nabídka**.
2. Klepněte na tlačítko **Konfigurovat**.
3. V konfiguračním podokně klepněte na položku **E-mailly a rychlé zprávy**.

2 V části **Ochrana rychlých zpráv** klepněte na možnost **Zapnout**.

Poznámka: I když můžete ochranu rychlých zpráv kdykoliv vypnout, bude po vypnutí počítač nedostatečně zabezpečený proti škodlivým přílohám rychlých zpráv.

KAPITOLA 10

Nastavení ochrany proti virům

Program VirusScan nabízí dva typy ochrany proti virům: ochranu v reálném čase a ruční ochranu. Ochrana proti virům v reálném čase prohledává soubory při každém přístupu k souborům (uživatelé nebo počítačem). Ruční ochrana proti virům umožňuje prohledávat soubory na požádání. Pro každý typ ochrany existují různé možnosti nastavení. Příklad: protože ochrana v reálném čase nepřetržitě sleduje počítač, lze vybrat pouze určitou sadu základních možností prohledávání a komplexnější sadu možností prohledávání vyhradit pro ruční prohledávání na požádání.

V této kapitole

Nastavení možností prohledávání v reálném čase.....	38
Nastavení možností ručního prohledávání	40
Používání možností programu Ochrana systému	44
Používání seznamů důvěryhodných položek	51

Nastavení možností prohledávání v reálném čase

Při spuštění ochrany proti virům v reálném čase program VirusScan používá pro prohledávání souborů výchozí sadu možností. Výchozí možnosti však můžete změnit a přizpůsobit vašim potřebám.

Chcete-li změnit možnosti prohledávání v reálném čase, je třeba rozhodnout o tom, co bude program VirusScan v průběhu prohledávání kontrolovat. Dále je potřeba rozhodnout o umístěních a typech prohledávaných souborů. Můžete například určit, zda bude program VirusScan kontrolovat neznámé viry a soubory cookie používané weby ke sledování chování uživatele, a zda bude program prohledávat síťové jednotky, které jsou mapovány na počítač, nebo pouze místní jednotky. Můžete také určit typy prohledávaných souborů (všechny soubory nebo pouze programové soubory a dokumenty – nejčastější umístění zjištěných virů).

Jestliže změníte možnost prohledávání v reálném čase, je třeba také určit, zda je pro počítač důležitá ochrana proti přetečení vyrovnávací paměti. Vyrovnávací paměť je část paměti, která se používá k dočasnému ukládání informací počítače. K přetečení vyrovnávací paměti může dojít tehdy, jestliže je množství informací ukládaných podezřelými programy nebo procesy do vyrovnávací paměti větší, než je kapacita paměti. Jestliže nastane tato situace, je počítač daleko více zranitelnější proti útokům na zabezpečení.

Nastavení možností prohledávání v reálném čase – postup

Nastavení možností prohledávání v reálném čase slouží k vlastnímu nastavení cílů prohledávání v reálném čase programu VirusScan a k nastavení umístění a typů prohledávaných souborů. Mezi možnosti patří prohledávání za účelem zjišťování nových virů a sledovacích souborů cookie i ochrana proti přetečení vyrovnávací paměti. Také lze nakonfigurovat prohledávání v reálném čase tak, aby byly kontrolovány síťové jednotky mapované na počítač.

1 Otevřete podokno Prohledávání v reálném čase.

Jak?

1. V části **Běžné úkoly** klepněte na tlačítko **Domácí**.
 2. V podokně Domácí programu SecurityCenter klepněte na položku **Počítač a soubory**.
 3. V informační oblasti položky Počítač a soubory klepněte na tlačítko **Konfigurovat**.
 4. V konfiguračním podokně Počítač a soubory zkontrolujte, zda je ochrana proti virům povolena a poté klepněte na tlačítko **Upřesnit**.
- 2** Určete možnosti prohledávání v reálném čase a poté klepněte na tlačítko **OK**.

Akce	Postup
Zjištění neznámých virů a nových variant virů známých	Zaškrtněte políčko Hledat neznámé viry pomocí heuristiky .
Zjišťování souborů cookie	Zaškrtněte políčko Prohledat a odstranit sledovací soubory cookie .
Zjištění virů a dalších potenciálních hrozeb na jednotkách připojených k síti	Zaškrtněte políčko Prohledat síťové jednotky .
Ochrana počítače proti přetečení vyrovnávací paměti	Zaškrtněte políčko Povolit ochranu před přetečením vyrovnávací paměti .
Určení typů prohledávaných souborů	Klepněte buď na tlačítko Všechny soubory (doporučeno) , nebo na tlačítko Pouze programové soubory a dokumenty .

Nastavení možností ručního prohledávání

Ruční ochrana proti virům umožňuje prohledávat soubory na požádání. Program VirusScan kontroluje při spuštění ručního prohledávání počítač na přítomnost virů a dalších potenciálně škodlivých položek pomocí komplexnější sady možností prohledávání. Chcete-li možnosti ručního prohledávání změnit, je třeba rozhodnout o tom, co bude program VirusScan v průběhu prohledávání kontrolovat. Můžete například určit, zda bude program VirusScan zjišťovat neznámé viry, potenciálně nežádoucí programy (jako je spyware, adware, utajené programy jako jsou správcovské sady, které mohou povolit neoprávněný přístup k počítači) a soubory cookie, které mohou weby používat ke sledování chování uživatele. Je také třeba rozhodnout o typech kontrolovaných souborů. Můžete například určit, zda bude program VirusScan kontrolovat všechny soubory nebo pouze programové soubory a dokumenty (nejčastější umístění zjištěných virů). Také lze určit, zda budou součástí prohledávání archivní soubory (například soubory ZIP).

Program VirusScan kontroluje ve výchozím nastavení při spuštění ručního prohledávání všechny jednotky a složky počítače; výchozí umístění však můžete změnit a přizpůsobit vašim potřebám. Můžete například prohledávat pouze důležité systémové soubory, položky pracovní plochy nebo položky ve složce Program Files. Pokud nechcete být odpovědní za inicializaci každého ručního prohledávání, lze nastavit pravidelné opakování prohledávání. Naplánované prohledávání vždy zkontroluje celý počítač pomocí výchozích možností prohledávání. Výchozím intervalem prohledávání programu VirusScan je jednou za týden.

Jestliže zjistíte, že je prohledávání příliš pomalé, zvažte možnost prohledávání s minimálními nároky na počítač zakázat. Vezměte však na vědomí, že ochrana proti virům bude mít vyšší prioritu než jiné úkoly.

Poznámka: Program VirusScan určité množství úkolů (včetně automatických aktualizací a ručního prohledávání) pozastavuje tehdy, jestliže uživatel provádí jakékoliv aktivity, které zaberou celou obrazovku počítače, jako je sledování filmů nebo hraní počítačových her.

Nastavení možností ručního prohledávání

Nastavení možností ručního prohledávání slouží k vlastnímu nastavení cílů ručního prohledávání programu VirusScan a k nastavení umístění a typů prohledávaných souborů. Mezi možnosti patří zjišťování neznámých virů, archivních souborů, spywaru a potenciálně nežádoucích programů, sledovacích souborů cookie, správcovských sad a utajených programů.

1 Otevřete podokno Ruční prohledávání.

Jak?

1. V části **Běžné úkoly** klepněte na tlačítko **Domácí**.
2. V podokně Domácí programu SecurityCenter klepněte na položku **Počítač a soubory**.
3. V informační oblasti položky Počítač a soubory klepněte na tlačítko **Konfigurovat**.
4. V konfiguračním podokně Počítač a soubory zkontrolujte, zda je ochrana proti virům povolena a poté klepněte na tlačítko **Upřesnit**.
5. Klepněte v podokně Antivirová ochrana na možnost **Ruční prohledávání**.

2 Určete možnosti ručního prohledávání a poté klepněte na tlačítko **OK**.

Akce	Postup
Zjištění neznámých virů a nových variant virů známých	Zaškrtněte políčko Hledat neznámé viry pomocí heuristiky .
Zjištění a odstranění virů v souborech ZIP a dalších komprimovaných souborech	Zaškrtněte políčko Prohledávat soubory ZIP a další komprimované soubory .
Zjištění spywaru, adwaru a dalších potenciálně nežádoucích programů	Zaškrtněte políčko Hledat spyware a potenciálně nežádoucí programy .
Zjišťování souborů cookie	Zaškrtněte políčko Prohledat a odstranit sledovací soubory cookie .
Zjišťování správčovských sad a utajených programů, které mohou pozměnit a zneužít stávající systémové soubory systému Windows	Zaškrtněte políčko Hledat správčovské sady a jiné utajené programy .
Menší nároky na výkon procesoru při prohledávání a zároveň přiřazení vyšší priority jiným úlohám, jako je procházení sítě Internet nebo otevírání dokumentů	Zaškrtněte políčko Prohledávat s minimálními nároky na počítač .
Určení typů prohledávaných souborů	Klepněte buď na tlačítko Všechny soubory (doporučeno) , nebo na tlačítko Pouze programové soubory a dokumenty .

Nastavení umístění ručního prohledávání

Nastavením umístění ručního prohledávání určíte, kde bude v průběhu ručního prohledávání program VirusScan vyhledávat viry a další škodlivé položky. Můžete kontrolovat všechny soubory, složky a jednotky v počítači nebo můžete prohledávání omezit pouze na určité složky a jednotky.

1 Otevřete podokno Ruční prohledávání.

Jak?

1. V části **Běžné úkoly** klepněte na tlačítko **Domácí**.
2. V podokně Domácí programu SecurityCenter klepněte na položku **Počítač a soubory**.
3. V informační oblasti položky Počítač a soubory klepněte na tlačítko **Konfigurovat**.
4. V konfiguračním podokně Počítač a soubory zkontrolujte, zda je ochrana proti virům povolena a poté klepněte na tlačítko **Upřesnit**.
5. Klepněte v podokně Antivirová ochrana na možnost **Ruční prohledávání**.

2 Klepněte na položku **Výchozí prohledávané umístění**.

3 Určete umístění ručního prohledávání a poté klepněte na tlačítko **OK**.

Akce	Postup
Prohledávání všech souborů a složek v počítači	Zaškrtněte políčko Tento počítač .
Prohledávání pouze určitých souborů, složek a jednotek počítače	Zrušte zaškrtnutí políčka Tento počítač a vyberte jednu nebo více složek nebo jednotek.
Prohledávání důležitých systémových souborů	Zrušte zaškrtnutí políčka Tento počítač a poté zaškrtněte políčko Důležité systémové soubory .

Plánování prohledávání

Jestliže naplánujete prohledávání, dosáhnete kterýkoliv den a hodinu v týdnu důkladného prohledávání počítače na přítomnost virů a dalších hrozeb. Naplánované prohledávání vždy zkontroluje celý počítač pomocí výchozích možností prohledávání. Výchozím intervalem prohledávání programu VirusScan je jednou za týden. Jestliže zjistíte, že je prohledávání příliš pomalé, zvažte možnost prohledávání s minimálními nároky na počítač zakázat. Vezměte však na vědomí, že ochrana proti virům bude mít vyšší prioritu než jiné úkoly.

1 Otevřete podokno Naplánované prohledání.

Jak?

1. V části **Běžné úkoly** klepněte na tlačítko **Domácí**.
 2. V podokně Domácí programu SecurityCenter klepněte na položku **Počítač a soubory**.
 3. V informační oblasti položky Počítač a soubory klepněte na tlačítko **Konfigurovat**.
 4. V konfiguračním podokně Počítač a soubory zkontrolujte, zda je ochrana proti virům povolena a poté klepněte na tlačítko **Upřesnit**.
 5. Klepněte v podokně Antivirová ochrana na možnost **Naplánované prohledávání**.
- 2** Vyberte možnost **Povolit naplánování prohledávání**.
- 3** Chcete-li snížit objem výkonu procesoru, který je obvykle pro prohledávání využit, vyberte možnost **Prohledávat s minimálními nároky na počítač**.
- 4** Vyberte jeden nebo více dnů.
- 5** Určete počátek spuštění.
- 6** Klepněte na tlačítko **OK**.

Tip: Výchozí naplánování obnovíte klepnutím na tlačítko **Obnovit**.

Používání možností programu Ochrana systému

Program Ochrana systému sleduje, protokoluje, hlásí a spravuje potenciálně neoprávněné změny provedené v registru systému Windows nebo v důležitých systémových souborech v počítači. Neoprávněné změny registru a souborů mohou poškodit počítač, ohrozit zabezpečení a poškodit důležité systémové soubory.

Změny registru jsou běžné a v počítači ke změnám dochází pravidelně. Hodně změn je neškodných a tak je výchozí nastavení programu Ochrana systému nakonfigurováno tak, aby poskytovalo spolehlivou, inteligentní a reálnou ochranu proti neoprávněným změnám, které mohou mít značný potenciál uživatele poškodit. Pokud například program Ochrana systému zjistí změny, které nejsou běžné a představují potenciálně závažnou hrozbu, je tato aktivita okamžitě ohlášena a zapsána do protokolu. Běžnější změny, které však přesto mají určitý potenciál škodit, jsou pouze zaprotokolovány. Ve výchozím nastavení je vypnuto sledování standardních změn a změn, které představují malé riziko. Rozsah technologie programu Ochrana systému lze nakonfigurovat tak, aby chránil jakékoliv prostředí podle přání uživatelů.

Program Ochrana systému má tři části: Ochrana systému, Ochrana systému Windows a Ochrana prohlížeče.

Ochrana systému

Ochrana systému zjišťuje potenciálně neoprávněné změny v registru počítače a dalších důležitých souborech, které jsou pro systém Windows klíčové. Mezi tyto důležité položky registru a soubory patří instalace ovládacích prvků Active X, položky Po spuštění, moduly přiřazení spuštění systému Windows a načtení zpoždění objektu služby prostředí. Technologie programu Ochrana systému sleduje tyto položky a zastavuje podezřelé programy využívající ovládacích prvků Active X (stahované ze sítě Internet). Navíc také zastavuje spyware a potenciálně nežádoucí programy, které mohou být automaticky spuštěny při spuštění systému Windows.

Ochrana systému Windows

Ochrana systému Windows také zjišťuje potenciálně neoprávněné změny v registru počítače a dalších důležitých souborech, které jsou pro systém Windows klíčové. Mezi tyto důležité položky registru a soubory patří služby místních nabídek, knihovny Applnit DLL a soubor hostitelů systému Windows. Technologie Ochrany systému Windows sleduje tyto položky a pomáhá tím zabránit tomu, aby počítač odeslal nebo přijal neoprávněné nebo osobní informace pomocí sítě Internet. Také pomáhá zastavit podezřelé programy, které mohou způsobit nežádoucí změny vzhledu a chování programů, které jsou důležité pro vás i pro vaši rodinu.

Ochrana prohlížeče

Stejně jako programy Ochrana systému a Ochrana systému Windows, také Ochrana prohlížeče zjišťuje potenciálně neoprávněné změny v registru počítače a dalších důležitých souborech, které jsou pro systém Windows klíčové. Ochrana prohlížeče ovšem sleduje změny důležitých položek registru a souborů jako jsou doplňky aplikace Internet Explorer, adresy URL aplikace Internet Explorer a zóny zabezpečení aplikace Internet Explorer. Ochrana prohlížeče sleduje tyto položky a pomáhá tím zabránit neoprávněným aktivitám prohlížeče, jako je přesměrování na podezřelé weby, změny nastavení a možností prohlížeče bez vědomí uživatele a nežádoucí důvěřování podezřelým webům.

Povolení ochrany programu Ochrana systému

Chcete-li zjišťovat a být informováni o potenciálně neoprávněných změnách v registru systému Windows a souborech, povolte ochranu programu Ochrana systému. Neoprávněné změny registru a souborů mohou poškodit počítač, ohrozit zabezpečení a poškodit důležité systémové soubory.

1 Otevřete konfigurační podokno Počítač a soubory.

Jak?

1. Klepněte v levém podokně na položku **Rozšířená nabídka**.
2. Klepněte na tlačítko **Konfigurovat**.
3. V konfiguračním podokně klepněte na položku **Počítač a soubory**.

2 V části **Ochrana systému** klepněte na možnost **Zapnout**.

Poznámka: Ochranu programu Ochrana systému lze vypnout klepnutím na tlačítko **Vypnout**.

Možnosti konfigurace programu Ochrana systému

Podokno programu Ochrana systému slouží ke konfiguraci ochrany, protokolování a možností výstrah proti neoprávněným změnám registru a souborů, které souvisí se soubory systému Windows, programy a aplikací Internet Explorer. Neoprávněné změny registru a souborů mohou poškodit počítač, ohrozit zabezpečení a poškodit důležité systémové soubory.

1 Otevřete podokno programu Ochrana systému.

Jak?

1. V části **Běžné úkoly** klepněte na tlačítko **Domácí**.
2. V podokně Domácí programu SecurityCenter klepněte na položku **Počítač a soubory**.
3. V informační oblasti položky Počítač a soubory klepněte na tlačítko **Konfigurovat**.
4. V konfiguračním podokně Počítač a soubory zkontrolujte, zda je program Ochrana systému povolen a poté klepněte na tlačítko **Upřesnit**.

2 Vyberte ze seznamu typ ochrany programu Ochrana systému.

- **Ochrana systému**
- **Ochrana systému Windows**
- **Ochrana prohlížeče**

3 V části **Požadovaná akce** proveďte jednu z následujících akcí:

- Chcete-li zjišťovat, protokolovat a hlásit neoprávněné změny registru a souborů, které souvisí s programy Ochrana systému, Ochrana systému Windows a Ochrana prohlížeče, klepněte na možnost **Zobrazit výstrahy**.
- Chcete-li zjišťovat a protokolovat neoprávněné změny registru a souborů, které souvisí s programy Ochrana systému, Ochrana systému Windows a Ochrana prohlížeče, klepněte na možnost **Změny pouze zapsat do protokolu**.
- Chcete-li vypnout zjišťování a protokolování neoprávněných změn registru a souborů, které souvisí s programy Ochrana systému, Ochrana systému Windows a Ochrana prohlížeče, klepněte na možnost **Zákaz programu Ochrana systému**.

Poznámka: Další informace o součástech programu Ochrana systému naleznete v tématu *Součásti programu Ochrana systému* (stránka 47).

Součásti programu Ochrana systému

Součásti programu Ochrana systému zjišťují potenciálně neoprávněné změny v registru počítače a dalších důležitých souborech, které jsou pro systém Windows klíčové. Program Ochrana systému má tři části: Ochrana systému, Ochrana systému Windows a Ochrana prohlížeče

Ochrana systému

Technologie programu Ochrana systému zastavuje podezřelé programy využívající ovládacích prvků Active X (stahované ze sítě Internet). Navíc také zastavuje spyware a potenciálně nežádoucí programy, které mohou být automaticky spuštěny při spuštění systému Windows.

Ochrana systému	Zjišťuje...
Instalace prvku ActiveX	Neoprávněné změny instalací ovládacích prvků ActiveX v registru, které mohou poškodit počítač, ohrozit zabezpečení a poškodit důležité systémové soubory.
Položky Po spuštění	Spyware, adware a další potenciálně nežádoucí programy, které mohou nainstalovat soubory měnící položky Po spuštění a umožnit tak spuštění podezřelých programů při spuštění počítače.
Moduly přiřazení spouštění prostředí systému	Spyware, adware a další potenciálně nežádoucí programy, které mohou nainstalovat moduly přiřazení spouštění prostředí Windows a zabránit tak zabezpečovacím programům ve správném fungování.
Načtení zpoždění objektu služby prostředí	Spyware, adware a další potenciálně nežádoucí programy, které mohou provést změny v registru pro načtení zpoždění objektu služby prostředí a umožnit spuštění nebezpečných souborů při spuštění počítače.

Ochrana systému Windows

Technologie Ochrany systému Windows pomáhá zabránit tomu, aby počítač pomocí sítě Internet odeslal nebo přijal neoprávněné nebo osobní informace. Také pomáhá zastavit podezřelé programy, které mohou způsobit nežádoucí změny vzhledu a chování programů, které jsou důležité pro vás i pro vaši rodinu.

Ochrana systému	Zjišťuje...
Obsluha místních nabídek	Neoprávněné změny obsluhy místních nabídek systému Windows v registru, které mohou mít vliv na vzhled a chování nabídek systému Windows. Místní nabídky v počítači, jako je například klepnutí pravým tlačítkem myši na soubory, slouží k provádění činností.

Knihovny Applnit DLL	Neoprávněné změny knihoven Applnit_DLL v registru, které mohou umožnit spuštění potenciálně škodlivých souborů při spuštění počítače.
Soubor hostitelů systému Windows	Spyware, adware a potenciálně nežádoucí programy, které mohou provést neoprávněné změny v souboru hostitelů systému Windows a umožnit tak přesměrování prohlížeče na podezřelé webové stránky nebo blokování aktualizací softwaru.
Prostředí přihlašování k systému Windows	Spyware, adware a další potenciálně nežádoucí programy, které mohou v registru změnit prostředí přihlašování k systému Windows a umožnit nahrazení programu Průzkumník Windows jinými programy.
Přihlašování do systému Windows – Inicializace uživatele	Spyware, adware a další potenciálně nežádoucí programy, které mohou v registru změnit inicializaci uživatele pro přihlašování k systému Windows a umožnit spuštění podezřelých programů při přihlašování k systému Windows.
Protokoly systému Windows	Spyware, adware a další potenciálně nežádoucí programy, které mohou v registru změnit protokoly systému Windows a ovlivnit způsob odesílání a přijímání informací z Internetu v počítači.
Zprostředkovatelé služeb vrstvy rozhraní Winsock	Spyware, adware a další potenciálně nežádoucí programy, které mohou nainstalovat změny v registru pro zprostředkovatele služeb vrstvy rozhraní Winsock a zachytit a změnit informace odesílané a přijímané v síti Internet.
Spuštění příkazů prostředí systému Windows	Neoprávněné změny ve spuštění příkazů prostředí systému Windows, které mohou umožnit spuštění červů a dalších nebezpečných programů v počítači.
Plánovač sdílených úloh	Spyware, adware a další potenciálně nežádoucí programy, které mohou provést změny v registru a souborech pro Plánovač sdílených úloh a umožnit spuštění potenciálně nebezpečných souborů při spuštění počítače.
Služba Windows Messenger	Spyware, adware a další potenciálně nežádoucí programy, které mohou provést v registru změny pro službu Windows Messenger a umožnit v počítači nevyžádanou reklamu a vzdáleně spuštěné programy.
Soubor Win.ini systému Windows	Spyware, adware a další potenciálně nežádoucí programy, které mohou změnit soubor win.ini a umožnit tak spuštění podezřelých programů při spuštění počítače.

Ochrana prohlížeče

Ochrana prohlížeče pomáhá zabránit neoprávněným aktivitám prohlížeče, jako je přesměrování na podezřelé weby, změny nastavení a možnosti prohlížeče bez vědomí uživatele a nežádoucí důvěřování podezřelým webům.

Ochrana systému	Zjišťuje...
Objekty BHO (Browser Helper Object)	Spyware, adware a další potenciálně nežádoucí programy, které mohou využívat objektů BHO (browser helper objects) za účelem sledování procházení Internetu a zobrazování nevyžádané reklamy.
Panel aplikace Internet Explorer	Neoprávněné změny v registru pro programy na panelu aplikace Internet Explorer, jako jsou možnosti Hledat a Oblíbené položky, které mohou mít vliv na vzhled a chování aplikace Internet Explorer.
Softwarové doplňky aplikace Internet Explorer	Spyware, adware a další potenciálně nežádoucí programy, které mohou instalovat doplňky aplikace Internet Explorer za účelem sledování procházení Internetu a zobrazování nevyžádané reklamy.
Internet Explorer ShellBrowser	Neoprávněné změny v registru pro aplikaci Internet Explorer ShellBrowser, které mohou mít vliv na vzhled a chování webového prohlížeče.
Internet Explorer WebBrowser	Neoprávněné změny v registru pro aplikaci Internet Explorer WebBrowser, které mohou mít vliv na vzhled a chování webového prohlížeče.
Moduly přiřazení adres URL aplikaci Internet Explorer	Spyware, adware a další potenciálně nežádoucí programy, které mohou v registru změnit moduly přiřazení adres URL aplikace Internet Explorer a při prohledávání webu umožnit přesměrování prohlížeče na podezřelé webové stránky.
Adresy URL aplikace Internet Explorer	Spyware, adware a další potenciálně nežádoucí programy, které mohou v registru provést změny adres URL aplikace Internet Explorer a ovlivnit tak nastavení prohlížeče.
Omezení aplikace Internet Explorer	Spyware, adware a další potenciálně nežádoucí programy, které mohou v registru provést změny omezení aplikace Internet Explorer a ovlivnit tak nastavení a možnosti prohlížeče.
Zóny zabezpečení aplikace Internet Explorer	Spyware, adware a další potenciálně nežádoucí programy, které mohou provést změny v registru pro zóny zabezpečení aplikace Internet Explorer a umožnit spuštění potenciálně nebezpečných souborů při spuštění počítače.

Důvěryhodné servery aplikace Internet Explorer	Spyware, adware a další potenciálně nežádoucí programy, které mohou v registru změnit důvěryhodné servery aplikace Internet Explorer a umožnit tak, aby prohlížeč důvěřoval podezřelým webovým serverům.
Zásady ochrany osobních údajů v aplikaci Internet Explorer	Spyware, adware a další potenciálně nežádoucí programy, které mohou v registru provést změny zásad aplikace Internet Explorer a ovlivnit tak vzhled a chování prohlížeče.

Používání seznamů důvěryhodných položek

Jestliže program VirusScan zjistí změnu registru nebo souboru (pomocí programu Ochrana systému), změnu programu nebo přetečení vyrovnávací paměti, budete vyzváni k rozhodnutí, zda chcete položce důvěřovat nebo položku odebrat. Jestliže položce důvěřujete a dáte najevo, že již nechcete příště získávat upozornění na aktivity položky, bude položka přidána do seznamu důvěryhodných položek a program VirusScan tuto položku dále nebude zjišťovat a upozorňovat na její aktivity. Jestliže byla položka přidána do seznamu důvěryhodných položek, ale rozhodli jste se její aktivitu blokovat, lze tak učinit. Položce bude díky blokování zabráněno ve spuštění nebo provádění jakýchkoliv změn v počítači a zároveň nebudete při každém pokusu upozorňováni. Položku lze také ze seznamu důvěryhodných položek odebrat. Jestliže položku odeberete, umožníte tím opětovné zjišťování aktivit položky programem VirusScan.

Správa seznamů důvěryhodných položek

Pomocí podokna Seznamy důvěryhodných položek určete, kterým dříve zjištěným a důvěryhodným položkám chcete důvěřovat a které položky chcete blokovat. Položku lze také ze seznamu důvěryhodných položek odebrat, takže program VirusScan může tuto položku opět zjišťovat.

1 Otevřete podokno Seznamy důvěryhodných položek.

Jak?

1. V části **Běžné úkoly** klepněte na tlačítko **Domácí**.
2. V podokně Domácí programu SecurityCenter klepněte na položku **Počítač a soubory**.
3. V informační oblasti položky Počítač a soubory klepněte na tlačítko **Konfigurovat**.
4. V konfiguračním podokně Počítač a soubory zkontrolujte, zda je ochrana proti virům povolena a poté klepněte na tlačítko **Upřesnit**.
5. Klepněte v podokně Antivirová ochrana na možnost **Seznamy důvěryhodných položek**.

2 Vyberte seznam z následujících typů seznamů důvěryhodných položek:

- **Ochrana systému**
- **Ochrana systému Windows**
- **Ochrana prohlížeče**
- **Důvěryhodné programy**
- **Povolené přetečení vyrovnávací paměti**

- 3** V části **Požadovaná akce** proveďte jednu z následujících akcí:
- Jestliže chcete zjištěné položce umožnit provést změny v registru systému Windows nebo v důležitých systémových souborech bez oznámení uživateli, klepněte na možnost **Důvěřovat**.
 - Jestliže chcete zjištěné položce blokovat provádění změn v registru systému Windows nebo v důležitých systémových souborech bez oznámení uživateli, klepněte na možnost **Blokovat**.
 - Chcete-li zjištěnou položku odebrat ze seznamů důvěryhodných položek, klepněte na možnost **Odebrat**.
- 4** Klepněte na tlačítko **OK**.

Poznámka: Další informace o součástech programu Ochrana systému naleznete v tématu *Součásti programu Ochrana systému* (stránka 52).

O typech seznamů důvěryhodných položek

Ochrana systému v podokně Seznamy důvěryhodných položek představuje neoprávněné změny registru a souborů, které program VirusScan zjistil dříve, ale které uživatel z výstrah nebo pomocí podokna Výsledky prohledávání povolil. Existuje pět typů seznamů důvěryhodných položek, které lze v podokně Seznamy důvěryhodných položek spravovat: Ochrana systému, Ochrana systému Windows, Ochrana prohlížeče, Důvěryhodné programy a Povolené přetečení vyrovnávací paměti.

Možnost	Popis
Ochrana systému	<p>Ochrana systému v podokně Seznamy důvěryhodných položek představuje neoprávněné změny registru a souborů, které program VirusScan zjistil dříve, ale které uživatel z výstrah nebo pomocí podokna Výsledky prohledávání povolil.</p> <p>Ochrana systému zjišťuje neoprávněné změny registru a souborů související s instalacemi ovládacích prvků ActiveX, položkami Po spuštění, moduly přiřazení spuštění systému Windows a aktivitami načtení zpoždění objektu služby prostředí. Tyto typy neoprávněných změn registru a souborů mohou poškodit počítač, ohrozit zabezpečení a poškodit důležité systémové soubory.</p>

Ochrana systému Windows	<p>Ochrana systému Windows v podokně Seznamy důvěryhodných položek představuje neoprávněné změny registru a souborů, které program VirusScan zjistil dříve, ale které uživatel z výstrah nebo pomocí podokna Výsledky prohledávání povolil.</p> <p>Ochrana systému Windows zjišťuje neoprávněné změny registru a souborů související s obsluhami místních nabídek, knihovnamy AppInit_DLL, souborem hostitelů systému Windows, prostředím přihlašování k systému Windows, zprostředkovateli služeb vrstvy rozhraní Winsock a podobně. Tyto typy neoprávněných změn registru a souborů mohou mít vliv na způsob, kterým počítač v síti Internet odesílá a přijímá informace, změnit vzhled a chování programů a umožnit, aby byly v počítači spuštěny podezřelé programy.</p>
Ochrana prohlížeče	<p>Ochrana prohlížeče v podokně Seznamy důvěryhodných položek představuje neoprávněné změny registru a souborů, které program VirusScan zjistil dříve, ale které uživatel z výstrah nebo pomocí podokna Výsledky prohledávání povolil.</p> <p>Ochrana prohlížeče zjišťuje neoprávněné změny registru a souborů a další nevyžádané chování související s objekty BHO (browser helper objects), doplňky aplikace Internet Explorer, adresami URL aplikace Internet Explorer a zónami zabezpečení aplikace Internet Explorer a podobně. Tyto typy neoprávněných změn registru mohou mít za následek nevyžádanou aktivitu prohlížeče, jako je přesměrování na podezřelé weby, změny nastavení a možností prohlížeče a důvěřování podezřelým webům.</p>
Důvěryhodné programy	<p>Důvěryhodné programy jsou potenciálně nežádoucí programy, které program VirusScan zjistil dříve, ale které uživatel označil z výstrahy nebo pomocí podokna Výsledky prohledávání za důvěryhodné.</p>
Povolené přetečení vyrovnávací paměti	<p>Povolené přetečení vyrovnávací paměti představuje dříve nevyžádanou aktivitu, kterou program VirusScan zjistil, ale kterou uživatel označil z výstrahy nebo pomocí podokna Výsledky prohledávání za důvěryhodnou.</p> <p>Přetečení vyrovnávací paměti mohou poškodit počítač a soubory. K přetečení vyrovnávací paměti dojde tehdy, jestliže je množství informací ukládaných podezřelými programy nebo procesy do vyrovnávací paměti větší, než je kapacita paměti.</p>

KAPITOLA 11

Prohledávání počítače

Při prvním spuštění programu SecurityCenter začne ochrana proti virům v reálném čase programu VirusScan chránit počítač proti potenciálně škodlivým virům, trojským koním a dalším hrozbám zabezpečení. Pokud není ochrana proti virům v reálném čase vypnuta, sleduje program VirusScan neustále počítač, zjišťuje aktivity virů a při každém přístupu k souborům (počítačem nebo uživatelem) soubory prohledává pomocí uživatelem nastavených možností prohledávání v reálném čase. Chcete-li zajistit stálou ochranu počítače proti nejnovějším bezpečnostním hrozbám, ponechte ochranu v reálném čase zapnutou a naplánujte spouštění pravidelných a komplexnějších ručních prohledávání. Další informace o nastavení možností prohledávání v reálném čase a ručním prohledávání naleznete v tématu *Nastavení ochrany proti virům* (stránka 37).

Pro ruční ochranu proti virům nabízí program VirusScan podrobnější sadu možností prohledávání a umožňuje pravidelné spouštění komplexnějších prohledávání. Ruční prohledávání lze spustit pomocí programu SecurityCenter a zaměřit v rámci nastaveného harmonogramu na specifická umístění. Ruční prohledávání lze také spustit přímo v průběhu práce na počítači z programu Průzkumník Windows. Výhodou prohledávání v programu SecurityCenter je možnost průběžně měnit možnosti prohledávání. Prohledávání z programu Průzkumník Windows zase nabízí pohodlnější přístup k zabezpečení počítače.

Ať už spouštíte ruční prohledávání z programu SecurityCenter nebo z programu Průzkumník Windows, výsledky prohledávání lze po dokončení zobrazit. Zobrazení výsledků prohledávání slouží k určení toho, zda program VirusScan zjistil, opravil nebo přesunul do karantény viry, trojské koně, spyware, adware, soubory cookie a další potenciálně nežádoucí programy. Výsledky prohledávání lze zobrazit různým způsobem. Lze například zobrazit základní přehled výsledků prohledávání nebo podrobné informace, jako je stav a typ nákazy. Další možností je zobrazení obecných statistik prohledávání a zjišťování.

V této kapitole

Prohledávání počítače – postup.....	56
Zobrazení výsledků prohledávání	56

Prohledávání počítače – postup

Ruční prohledávání lze spustit ze základní i rozšířené nabídky programu SecurityCenter. Jestliže prohledávání spouštíte z rozšířené nabídky, lze před prohledávání možnosti ručního prohledávání potvrdit. Jestliže prohledávání spouštíte ze základní nabídky, spustí program VirusScan prohledávání pomocí stávajících možností prohledávání ihned. Prohledávání můžete také spustit z programu Průzkumník Windows. Použity budou stávající možnosti prohledávání.

- Proveďte jednu z následujících akcí:

Prohledávání v programu SecurityCenter

Akce	Postup
Prohledávání za použití stávajících nastavení	Klepněte v základní nabídce na položku Prohledávat .
Prohledávání za použití změněných nastavení	Klepněte v rozšířené nabídce na možnost Prohledávat , vyberte cíl a možnosti prohledávání a poté klepněte na položku Prohledat nyní .

Prohledávání v programu Průzkumník Windows

1. Spusťte program Průzkumník Windows.
2. Klepněte na soubor, složku nebo jednotku pravým tlačítkem myši a poté klepněte na příkaz **Prohledávat**.

Poznámka: Výsledky prohledávání se zobrazí ve výstraze Prohledávání bylo dokončeno. Součástí výsledků jsou počty položek, které byly prohledány, zjištěny, opraveny, přesunuty do karantény a odebrány. Klepnutím na možnost **Zobrazit podrobnosti prohledávání** zjistíte další informace o výsledcích prohledávání a o práci s nakaženými položkami.

Zobrazení výsledků prohledávání

Zobrazení výsledků prohledávání po dokončení ručního prohledávání slouží k určení nalezených výsledků a k analýze aktuálního stavu ochrany počítače. Výsledky prohledávání slouží k určení toho, zda program VirusScan zjistil, opravil nebo přesunul do karantény viry, trojské koně, spyware, adware, soubory cookie a další potenciálně nežádoucí programy.

- Klepněte v základní nebo rozšířené nabídce na položku **Prohledávat** a poté proveďte jednu z následujících akcí:

Akce	Postup
Zobrazení výsledků prohledávání ve výstraze	Zobrazte výsledky prohledávání ve výstraze Prohledávání bylo dokončeno.

Zobrazení další informací o výsledcích prohledávání	Klepněte ve výstražce Prohledávání bylo dokončeno na možnost Zobrazit podrobnosti prohledávání .
Zobrazení rychlého přehledu výsledků prohledávání	Ukažte na ikonu Prohledávání bylo dokončeno v oznamovací oblasti hlavního panelu.
Zobrazení statistik prohledávání a zjišťování	Poklepejte na ikonu Prohledávání bylo dokončeno v oznamovací oblasti hlavního panelu.
Zobrazení podrobností o zjištěných položkách, stavu a typu nakažení.	Poklepejte na ikonu Prohledávání bylo dokončeno v oznamovací oblasti hlavního panelu a poté klepněte v podokně Průběh prohledávání: Ruční prohledávání na položku Zobrazit výsledky .

KAPITOLA 12

Práce s výsledky prohledávání

Jestliže program VirusScan zjistí ohrožení zabezpečení v průběhu spuštěného prohledávání v reálném čase nebo ručního prohledávání, pokusí se v závislosti na typu ohrožení zvládnout ohrožení automaticky. Pokud například program VirusScan zjistí v počítači virus, trojského koně nebo sledovací soubor cookie, pokusí se nakažený soubor vyčistit. Pokud soubor nelze vyčistit, přesune program VirusScan soubor do karantény.

U některých hrozeb zabezpečení nemusí být možné soubor úspěšně vyčistit nebo přesunout do karantény pomocí programu VirusScan. V takovém případě vyzve program VirusScan k vyřešení hrozby uživatele. V závislosti na typu hrozby může uživatel podniknout různé akce. Pokud má například zjištěný virus formu souboru, ale soubor nelze pomocí programu VirusScan úspěšně vyčistit nebo přesunout do karantény, bude odepřen další přístup k souboru. Jsou-li zjištěny sledovací soubory cookie, ale tyto soubory cookie nelze pomocí programu VirusScan úspěšně vyčistit nebo přesunout do karantény, může uživatel rozhodnout, zda budou odebrány nebo považovány za důvěryhodné. Jsou-li zjištěny potenciálně nežádoucí programy, nepodnikne program VirusScan žádnou akci automaticky. Namísto toho dá uživateli možnost rozhodnout, zda chce program přesunout do karantény nebo programu důvěřovat.

Při přesunu položek do karantény program VirusScan tyto položky zašifruje a izoluje ve složce, aby tak zabránil tomu, aby tyto soubory, programy nebo soubory cookie poškodily počítač. Položky přesunuté do karantény lze obnovit nebo odebrat. Ve většině případů lze soubor cookie, který byl přesunut do karantény, odstranit, aniž by to mělo na systém dopad. Pokud však program VirusScan přesunul do karantény program, který znáte a používáte, zvažte možnost tento program obnovit.

V této kapitole

Práce s viry a trojskými koňmi.....	59
Práce s potenciálně nežádoucími programy	60
Práce se soubory v karanténě	60
Práce s programy a soubory cookie v karanténě	61

Práce s viry a trojskými koňmi

Pokud program VirusScan zjistí v počítači vir nebo trojského koně během prohledávání v reálném čase nebo během ručního prohledávání, pokusí se soubor vyčistit. Pokud soubor nelze vyčistit, pokusí se program VirusScan soubor přesunout do karantény. Pokud se nezdaří i tato akce, bude odepřen přístup k souboru (pouze u prohledávání v reálném čase).

1 Otevřete podokno Výsledky prohledávání.

Jak?

1. Poklepejte na ikonu **Prohledávání bylo dokončeno** v oznamovací oblasti zcela vpravo na hlavním panelu.
 2. Klepněte v podokně Průběh prohledávání: Ruční prohledávání na tlačítko **Zobrazit výsledky**.
- 2** Klepněte v seznamu výsledků prohledávání na položku **Viry a trojské koně**.

Poznámka: Informace o práci se soubory, které program VirusScan přesunul do karantény, naleznete v tématu *Práce se soubory v karanténě* (stránka 60).

Práce s potenciálně nežádoucími programy

Pokud program VirusScan zjistí v počítači během prohledávání v reálném čase nebo během ručního prohledávání potenciálně nežádoucí program, můžete program odebrat nebo programu důvěřovat. Tím, že potenciálně nežádoucí program odeberete, program ve skutečnosti ze systému neodstraníte. Program bude namísto toho přesunut do karantény, aby bylo programu zabráněno v poškozování počítače nebo souborů.

- 1 Otevřete podokno Výsledky prohledávání.
Jak?
 1. Poklepejte na ikonu **Prohledávání bylo dokončeno** v oznamovací oblasti zcela vpravo na hlavním panelu.
 2. Klepněte v podokně Průběh prohledávání: Ruční prohledávání na tlačítko **Zobrazit výsledky**.
- 2 Klepněte v seznamu výsledků prohledávání na položku **Potenciálně nežádoucí programy**.
- 3 Vyberte potenciálně nežádoucí program.
- 4 V části **Požadovaná akce** klepněte buď na tlačítko **Odebrat** nebo **Důvěřovat**.
- 5 Potvrďte výběr.

Práce se soubory v karanténě

Při přesunu nakažených souborů do karantény program VirusScan tyto soubory zašifruje a přesune do složky, aby tak zabránil tomu, aby tyto soubory poškodily počítač. Soubory přesunuté do karantény lze poté obnovit nebo odebrat.

- 1 Otevřete podokno Soubory v karanténě.
Jak?

1. Klepněte v levém podokně na položku **Rozšířená nabídka**.
 2. Klepněte na tlačítko **Obnovit**.
 3. Klepněte na možnost **Soubory**.
- 2 Vyberte soubor v karanténě.
 - 3 Proveďte jednu z následujících akcí:
 - Chcete-li nakažený soubor opravit a vrátit do původního umístění v počítači, klepněte na tlačítko **Obnovit**.
 - Chcete-li nakažený soubor odebrat z počítače, klepněte na tlačítko **Odebrat**.
 - 4 Klepnutím na tlačítko **Ano** potvrďte vybranou možnost.

Tip: Současně lze obnovit nebo odebrat více souborů.

Práce s programy a soubory cookie v karanténě

Při přesunu potenciálně nežádoucích programů nebo sledovacích souborů cookie do karantény program VirusScan tyto položky zašifruje a přesune do chráněné složky, aby tak zabránil tomu, aby tyto programy nebo soubory cookie poškodily počítač. Položky přesunuté do karantény lze poté obnovit nebo odebrat. Ve většině případů lze položku, která byla přesunuta do karantény, odstranit, aniž by to mělo na systém dopad.

- 1 Otevřete podokno Programy a sledovací soubory cookie v karanténě.
Jak?
 1. Klepněte v levém podokně na položku **Rozšířená nabídka**.
 2. Klepněte na tlačítko **Obnovit**.
 3. Klepněte na možnost **Programy a soubory cookie**.
- 2 Vyberte program nebo soubor cookie v karanténě.
- 3 Proveďte jednu z následujících akcí:
 - Chcete-li nakažený soubor opravit a vrátit do původního umístění v počítači, klepněte na tlačítko **Obnovit**.
 - Chcete-li nakažený soubor odebrat z počítače, klepněte na tlačítko **Odebrat**.
- 4 Klepnutím na tlačítko **Ano** potvrďte operaci.

Tip: Současně lze obnovit nebo odebrat více programů a souborů cookie.

McAfee QuickClean

Program QuickClean zvyšuje výkon počítače vymazáním souborů, které mohou vymazat zbytečné soubory z počítače. Vyprázdní koš a vymaže dočasné soubory, zástupce, ztracené fragmenty souborů, cookies, soubory historie prohlížeče, odeslané vymazané e-maily, aktuálně používané soubory, soubory Active-X a soubory bodů obnovení systému. Program QuickClean také chrání vaše soukromí tím, že používá komponentu McAfee Shredder k zabezpečení a trvalému odstranění položek, které mohou obsahovat citlivé osobní údaje, jakými je např. vaše jméno nebo adresa. Další informace týkající se skartovaných souborů naleznete v části McAfee Shredder.

Program Defragmentace disku uspořádá soubory a složky v počítači, a tím zajistí, že nemohou být roztroušeny při ukládání na pevný disk počítače. Pravidelná defragmentace disku zajistí, že fragmenty souborů a složek jsou spojeny, a tím je zajištěno jejich pozdější rychlé načtení.

Nechcete-li počítač udržovat ručně, můžete naplánovat s jakoukoliv frekvencí automatické spuštění programů QuickClean a Disk Defragmenter jako nezávislých úloh.

Poznámka: Program SecurityCenter informuje o závažných i méně závažných problémech ochrany ihned, jakmile problémy zjistí. Potřebujete-li pro stanovení problémů ochrany nápovědu, lze spustit nástroj McAfee Virtual Technician.

V této kapitole

Funkce programu QuickClean	64
Čištění počítače	65
Defragmentace počítače	68
Plánování úloh.....	69

Funkce programu QuickClean

Program QuickClean poskytuje různé možnosti čištění, které vymaže bezpečně a účinně nepotřebné soubory. Vymazáním těchto souborů uvolníte prostor na pevném disku počítače a zvýšíte jeho výkon.

Čištění počítače

Program QuickClean vymaže soubory, které tvoří zbytečné soubory v počítači. Vyprázdní koš a vymaže dočasné soubory, zástupce, ztracené fragmenty souborů, cookies, soubory historie prohlížeče, odeslané vymazané e-maily, aktuálně používané soubory, soubory Active-X a soubory bodů obnovení systému. Program QuickClean vymaže tyto položky bez toho, aniž by byly ovlivněny jiné základní informace.

K vymazání nepotřebných souborů z počítače můžete použít kterýkoliv nástroj mazání programu QuickClean. Následující tabulka popisuje dostupné možnosti mazání programu QuickClean:

Název	Funkce
Čistič koše	Odstraní soubory z koše.
Čistič dočasných souborů	Odstraňuje soubory uložené v dočasných složkách.
Čistič zástupců	Odstraňuje nefunkční zástupce a zástupce, ke kterým není přidružen žádný program.
Čistič fragmentů ztracených souborů	Odstraňuje z počítače fragmenty ztracených souborů.
Čistič registru	Odstraňuje informace registru systému Windows® o programech, které již v počítači neexistují. Registr je databáze, do které systém Windows ukládá informace o konfiguraci. Registr obsahuje profily pro každého uživatele počítače a informace o hardwaru systému, nainstalovaných programech a nastavení vlastnictví. během operace systém Windows neustále odkazuje na tyto informace.
Čistič mezipaměti	Odstraňuje soubory uložené v mezipaměti, které se nashromáždí během procházení webu. Tyto soubory jsou obvykle uloženy jako dočasné soubory do složky mezipaměti. Složka mezipaměti je dočasné místo úložiště dat v počítači. Např. zvýšení rychlosti a účinnosti procházení webu, při příštím prohlížení váš prohlížeč může získat webovou stránku ze své mezipaměti (spíše než ze vzdáleného serveru).
Čistič souborů cookie	Odstraňuje soubory cookie. Tyto soubory jsou obvykle uloženy jako dočasné soubory. Cookie je malý soubor, který obsahuje informace obvykle zahrnující uživatelské jméno a aktuální datum a čas, uložený v počítači osoby procházející web. Soubory cookies jsou primárně používány webovými servery k identifikaci uživatelů, kteří byli již dříve zaregistrováni nebo web navštívili. Nicméně mohou být zdrojem informací pro hackery.

Čistič historie prohlížeče	Odstraňuje historii webového prohlížeče.
Čistič odstraněné a odeslané pošty aplikací Outlook Express a Outlook E-mail	Vymaže odstraněné a odeslané e-maily aplikací Outlook Express a Outlook E-mail.
Nedávno použitý čistič	Odstraní aktuálně používané soubory, které byly vytvořeny některým z těchto programů: <ul style="list-style-type: none"> ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Windows History ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®
Čistič prvků ActiveX	Odstraní ovládací prvky ActiveX. ActiveX je součástí softwaru využívaná programy nebo webovými stránkami dodávající funkčnost, která se jeví jako normální součást programu nebo webové stránky. Většina ovládacích prvků ActiveX je neškodná, nicméně některé mohou získávat informace z vašeho počítače.
Čistič bodů obnovení systému	Odstraňuje z počítače staré body obnovení systému (vyjma posledních). Body obnovení systému, které jsou tvořeny systémem Windows a označují změny provedené v počítači, umožňují v případě potíží návrat do předchozího stavu.

Čištění počítače

K odstranění nepotřebných souborů z počítače lze použít libovolný čistič programu QuickClean. Po dokončení čištění se v části **Souhrn programu QuickClean** zobrazí množství místa na disku uvolněného čištěním, počet odstraněných souborů a datum a čas posledního spuštění operace programu QuickClean.

- 1 V podokně McAfee SecurityCenter v části **Běžné úlohy** klepněte na položku **Údržba počítače**.
- 2 V části **McAfee QuickClean** klepněte na tlačítko **Spustit**.
- 3 Proveďte jednu z následujících akcí:
 - Klepnutím na tlačítko **Další** přijmete výchozí nastavení čištění v seznamu.

- Vyberte požadované možnosti čištění a klepněte na tlačítko **Další**. Vyberete-li čistič naposledy použitých souborů, můžete klepnutím na tlačítko **Vlastnosti** vybrat požadované soubory vytvořené programy v seznamu. Poté klepněte na tlačítko **OK**.
 - Pokud chcete obnovit výchozí nastavení možností čištění, klepněte na tlačítko **Obnovit výchozí nastavení** a na tlačítko **Další**.
- 4 Po provedení analýzy klepněte na tlačítko **Další**.
 - 5 Odstranění souborů potvrďte klepnutím na tlačítko **Další**.
 - 6 Proveďte jednu z následujících akcí:
 - Klepnutím na tlačítko **Další** přijměte výchozí nastavení **Ne, chci soubory odstranit standardním způsobem systému Windows**.
 - Klepněte na tlačítko **Ano, chci bezpečně odstranit soubory pomocí programu Shredder**, určete počet průchodů (až 10) a klepněte na tlačítko **Další**. Pokud je mazáno velké množství informací, může skartace souborů trvat poměrně dlouho.
 - 7 Byly-li při čištění některé soubory nebo složky uzamčeny, můžete být vyzváni k restartování počítače. Výzvu zavřete klepnutím na tlačítko **OK**.
 - 8 Klepněte na tlačítko **Dokončit**.

Poznámka: Soubory odstraněné pomocí programu Shredder nelze obnovit. Informace o skartaci souborů naleznete v tématu věnovaném programu McAfee Shredder.

Defragmentace počítače

Defragmentace disku zajišťuje uspořádání souborů a složek v počítači, aby nedošlo k jejich roztroušení (fragmentaci) při ukládání na pevný disk počítače. Pravidelnou defragmentací pevného disku se tyto fragmentované soubory a složky spojí, čímž se zrychlí jejich načítání.

Defragmentace počítače

Defragmentací počítače zrychlíte přístup k souborům a jejich načítání.

- 1** V podokně McAfee SecurityCenter v části **Běžné úlohy** klepněte na položku **Údržba počítače**.
- 2** V části **Defragmentace disku** klepněte na tlačítko **Analyzovat**.
- 3** Postupujte podle zobrazených pokynů.

Poznámka: Další informace o defragmentaci disku naleznete v nápovědě systému Windows.

Plánování úloh

Plánovač úloh zajišťuje pravidelné automatické spuštění programu QuickClean a defragmentace disku. Můžete například naplánovat vysypání koše programem QuickClean každou sobotu ve 21:00 nebo defragmentaci pevného disku počítače každý poslední den v měsíci. Úlohy je možné kdykoli vytvořit, upravit a smazat. Ke spuštění naplánované úlohy musíte být přihlášení k počítači. Pokud se úloha z jakéhokoli důvodu nespustí, bude znovu naplánována na dobu pět minut po přihlášení.

Naplánování úlohy programu QuickClean

Můžete naplánovat automatické vyčištění počítače pomocí jednoho či více čističů programu QuickClean. Po dokončení úlohy se v části **Souhrn programu QuickClean** zobrazí datum a čas příštího naplánovaného spuštění úlohy.

- 1 Otevřete podokno Plánovač úloh.

Jak?

 1. V části **Běžné úlohy** klepněte na tlačítko **Údržba počítače**.
 2. V části **Plánovač úloh** klepněte na tlačítko **Spustit**.
- 2 V seznamu **Vybrat operaci k naplánování** klepněte na položku **McAfee QuickClean**.
- 3 Do pole **Název úlohy** zadejte název úlohy a klepněte na tlačítko **Vytvořit**.
- 4 Proveďte jednu z následujících akcí:
 - Klepnutím na tlačítko **Další** přijmete výchozí nastavení čištění v seznamu.
 - Vyberte požadované možnosti čištění a klepněte na tlačítko **Další**. Vyberete-li čistič naposledy použitých souborů, můžete klepnutím na tlačítko **Vlastnosti** vybrat požadované soubory vytvořené programy v seznamu. Poté klepněte na tlačítko **OK**.
 - Pokud chcete obnovit výchozí nastavení možností čištění, klepněte na tlačítko **Obnovit výchozí nastavení** a na tlačítko **Další**.
- 5 Proveďte jednu z následujících akcí:
 - Klepnutím na tlačítko **Naplánovat** přijmete výchozí nastavení **Ne, chci soubory odstranit standardním způsobem systému Windows**.
 - Klepněte na tlačítko **Ano, chci bezpečně odstranit soubory pomocí programu Shredder**, určete počet průchodů (až 10) a klepněte na tlačítko **Naplánovat**.

- 6 V dialogovém okně **Plánování** zadejte frekvenci spouštění úlohy a klepněte na tlačítko **OK**.
- 7 Pokud jste provedli změny v nastavení čističe naposledy použitých souborů, můžete být vyzváni k restartování počítače. Výzvu zavřete klepnutím na tlačítko **OK**.
- 8 Klepněte na tlačítko **Dokončit**.

Poznámka: Soubory odstraněné pomocí programu Shredder nelze obnovit. Informace o skartaci souborů naleznete v tématu věnovaném programu McAfee Shredder.

Úprava úlohy programu QuickClean

U naplánované úlohy programu QuickClean lze změnit použité čističe a frekvenci automatického spouštění. Po dokončení se v části **Souhrn programu QuickClean** zobrazí datum a čas příštího naplánovaného spuštění úlohy.

- 1 Otevřete podokno Plánovač úloh.
Jak?
 1. V části **Běžné úlohy** klepněte na tlačítko **Údržba počítače**.
 2. V části **Plánovač úloh** klepněte na tlačítko **Spustit**.
- 2 V seznamu **Vybrat operaci k naplánování** klepněte na položku **McAfee QuickClean**.
- 3 Ze seznamu **Vybrat existující úlohu** vyberte úlohu a klepněte na tlačítko **Upravit**.
- 4 Proveďte jednu z následujících akcí:
 - Klepnutím na tlačítko **Další** přijmete výchozí nastavení čištění úlohy.
 - Vyberte požadované možnosti čištění a klepněte na tlačítko **Další**. Vyberete-li čistič naposledy použitých souborů, můžete klepnutím na tlačítko **Vlastnosti** vybrat požadované soubory vytvořené programy v seznamu. Poté klepněte na tlačítko **OK**.
 - Pokud chcete obnovit výchozí nastavení možností čištění, klepněte na tlačítko **Obnovit výchozí nastavení** a na tlačítko **Další**.
- 5 Proveďte jednu z následujících akcí:
 - Klepnutím na tlačítko **Naplánovat** přijmete výchozí nastavení **Ne, chci soubory odstranit standardním způsobem systému Windows**.
 - Klepněte na tlačítko **Ano, chci bezpečně odstranit soubory pomocí programu Shredder**, určete počet průchodů (až 10) a klepněte na tlačítko **Naplánovat**.

- 6 V dialogovém okně **Plánování** zadejte frekvenci spouštění úlohy a klepněte na tlačítko **OK**.
- 7 Pokud jste provedli změny v nastavení čističe naposledy použitých souborů, můžete být vyzváni k restartování počítače. Výzvu zavřete klepnutím na tlačítko **OK**.
- 8 Klepněte na tlačítko **Dokončit**.

Poznámka: Soubory odstraněné pomocí programu Shredder nelze obnovit. Informace o skartaci souborů naleznete v tématu věnovaném programu McAfee Shredder.

Odstranění úlohy programu QuickClean

Nechcete-li již automaticky spouštět naplánovanou úlohu programu QuickClean, můžete ji odstranit.

- 1 Otevřete podokno Plánovač úloh.
Jak?
 1. V části **Běžné úlohy** klepněte na tlačítko **Údržba počítače**.
 2. V části **Plánovač úloh** klepněte na tlačítko **Spustit**.
- 2 V seznamu **Vybrat operaci k naplánování** klepněte na položku **McAfee QuickClean**.
- 3 Ze seznamu **Vybrat existující úlohu** vyberte úlohu.
- 4 Klepněte na tlačítko **Odstranit** a pak klepnutím na tlačítko **Ano** potvrďte odstranění.
- 5 Klepněte na tlačítko **Dokončit**.

Naplánování úlohy defragmentace disku

Můžete naplánovat defragmentaci pevného disku počítače a určit frekvenci automatického spouštění této úlohy. Po dokončení se v části **Defragmentace disku** zobrazí datum a čas příštího naplánovaného spuštění úlohy.

- 1 Otevřete podokno Plánovač úloh.
Jak?

1. V části **Běžné úlohy** klepněte na tlačítko **Údržba počítače**.
2. V části **Plánovač úloh** klepněte na tlačítko **Spustit**.
- 2 V seznamu **Vybrat operaci k naplánování** klepněte na položku **Defragmentace disku**.
- 3 Do pole **Název úlohy** zadejte název úlohy a klepněte na tlačítko **Vytvořit**.
- 4 Proveďte jednu z následujících akcí:
 - Klepnutím na tlačítko **Naplánovat** přijměte výchozí nastavení **Provést defragmentaci, i když je málo volného místa**.
 - Zrušte zaškrtnutí políčka **Provést defragmentaci, i když je málo volného místa** a klepněte na tlačítko **Naplánovat**.
- 5 V dialogovém okně **Plánování** zadejte frekvenci spouštění úlohy a klepněte na tlačítko **OK**.
- 6 Klepněte na tlačítko **Dokončit**.

Úprava úlohy defragmentace disku

U naplánované úlohy defragmentace disku lze změnit frekvenci automatického spouštění. Po dokončení se v části **Defragmentace disku** zobrazí datum a čas příštího naplánovaného spuštění úlohy.

- 1 Otevřete podokno Plánovač úloh.

Jak?

 1. V části **Běžné úlohy** klepněte na tlačítko **Údržba počítače**.
 2. V části **Plánovač úloh** klepněte na tlačítko **Spustit**.
- 2 V seznamu **Vybrat operaci k naplánování** klepněte na položku **Defragmentace disku**.
- 3 Ze seznamu **Vybrat existující úlohu** vyberte úlohu a klepněte na tlačítko **Upravit**.
- 4 Proveďte jednu z následujících akcí:
 - Klepnutím na tlačítko **Naplánovat** přijměte výchozí nastavení **Provést defragmentaci, i když je málo volného místa**.
 - Zrušte zaškrtnutí políčka **Provést defragmentaci, i když je málo volného místa** a klepněte na tlačítko **Naplánovat**.
- 5 V dialogovém okně **Plánování** zadejte frekvenci spouštění úlohy a klepněte na tlačítko **OK**.
- 6 Klepněte na tlačítko **Dokončit**.

Odstranění úlohy defragmentace disku

Nechcete-li již automaticky spouštět naplánovanou úlohu defragmentace disku, můžete ji odstranit.

1 Otevřete podokno Plánovač úloh.

Jak?

1. V části **Běžné úlohy** klepněte na tlačítko **Údržba počítače**.
 2. V části **Plánovač úloh** klepněte na tlačítko **Spustit**.
- 2** V seznamu **Vybrat operaci k naplánování** klepněte na položku **Defragmentace disku**.
- 3** Ze seznamu **Vybrat existující úlohu** vyberte úlohu.
- 4** Klepněte na tlačítko **Odstranit** a pak klepnutím na tlačítko **Ano** potvrďte odstranění.
- 5** Klepněte na tlačítko **Dokončit**.

KAPITOLA 14

McAfee Shredder

Program McAfee Shredder odstraní trvale položky z pevného disku počítače. I když ručně odstraníte soubory i složky, vyprázdníte koš nebo vymažete složku Dočasné soubory Internetu, stále můžete obnovit informace prostřednictvím forenzních počítačových nástrojů. Vymazaný soubor lze obnovit, neboť některé programy vytváří dočasné soubory, skryté kopie otevřených souborů. Program Shredder chrání soukromí tím, že bezpečně a neustále odstraňuje nežádoucí soubory. Je důležité si pamatovat, že skartované soubory nelze obnovit.

Poznámka: Program SecurityCenter informuje o závažných i méně závažných problémech ochrany ihned, jakmile problémy zjistí. Potřebujete-li pro stanovení problémů ochrany nápovědu, lze spustit nástroj McAfee Virtual Technician.

V této kapitole

Funkce programu Shredder	76
Skartace souborů, složek a disků.....	77

Funkce programu Shredder

Program Shredder vymaže položky z pevného disku počítače tak, že přiřazené informace nelze již obnovit. Chrání vaše soukromí bezpečným a trvalým odstraněním souborů, složek a položek z koše, složek Dočasné soubory a celého obsahu disků, jakými jsou přepisovatelné disky CD, externí pevné disky nebo diskety.

Skartace souborů, složek a disků

Program Shredder zaručuje, že informace obsažené v odstraněných souborech a složkách v koši a ve složce dočasných souborů Internetu nemohou být obnoveny ani za použití speciálních nástrojů. V programu lze určit, kolikrát má být položka skartována (až 10krát). Vyšší počet průchodů skartace zvýší bezpečnost odstraňování souborů.

Skartace souborů a složek

Skartovat lze soubory a složky na pevném disku počítače včetně položek v koši a ve složce dočasných souborů Internetu.

1 Spustíte program **Shredder**.

Jak?

1. V podokně programu McAfee SecurityCenter, pod položkou **Běžné úkoly** klepněte na položku **Rozšířená nabídka**.
2. V levém podokně klepněte na položku **Nástroje**.
3. Klepněte na možnost **Shredder**.

2 V podokně Skartace souborů a složek v části **Požadovaná akce** klepněte na položku **Smazat soubory a složky**.

3 V nabídce **Úroveň skartace** klepněte na jednu z následujících úrovní:

- **Rychlá:** Skartuje vybrané položky jednou.
- **Komplexní:** Skartuje vybrané položky 7krát.
- **Vlastní:** Skartuje vybrané položky až 10krát.

4 Klepněte na tlačítko **Další**.

5 Proveďte jednu z následujících akcí:

- V seznamu **Vybrat soubory ke skartaci** klepněte na položku **Obsah koše** nebo **Dočasné soubory Internetu**.
- Klepněte na tlačítko **Procházet**, vyhledejte soubor, který chcete skartovat, vyberte jej a klepněte na tlačítko **Otevřít**.

6 Klepněte na tlačítko **Další**.

7 Klepněte na tlačítko **Spustit**.

8 Po dokončení skartace klepněte na tlačítko **Hotovo**.

Poznámka: Dokud program Shredder tuto úlohu nedokončí, nepracujte se žádnými soubory.

Skartovat celý disk

Umožňuje skartovat obsah celého disku najednou. Lze skartovat pouze vyměnitelné jednotky, jako jsou externí disky, zapisovatelné disky CD a diskety.

1 Spustíte program **Shredder**.

Jak?

1. V podokně programu McAfee SecurityCenter, pod položkou **Běžné úkoly** klepněte na položku **Rozšířená nabídka**.
 2. V levém podokně klepněte na položku **Nástroje**.
 3. Klepněte na možnost **Shredder**.
- 2** V podokně Skartace souborů a složek v části **Požadovaná akce** klepněte na položku **Smazat celý disk**.
- 3** V nabídce **Úroveň skartace** klepněte na jednu z následujících úrovní:
- **Rychlá:** Skartuje vybranou jednotku jednou.
 - **Komplexní:** Skartuje vybranou jednotku 7krát.
 - **Vlastní:** Skartuje vybranou jednotku až 10krát.
- 4** Klepněte na tlačítko **Další**.
- 5** V seznamu **Vybrat disk** klepněte na jednotku, kterou chcete skartovat.
- 6** Klepněte na tlačítko **Další** a pak klepnutím na tlačítko **Ano** potvrďte akci.
- 7** Klepněte na tlačítko **Spustit**.
- 8** Po dokončení skartace klepněte na tlačítko **Hotovo**.

Poznámka: Dokud program Shredder tuto úlohu nedokončí, nepracujte se žádnými soubory.

McAfee Network Manager

Program Network Manager poskytuje grafické zobrazení počítačů a součástí, které tvoří domácí síť. Program Network Manager lze použít ke vzdálenému sledování stavu ochrany každého spravovaného počítače v síti a ke vzdálené opravě ohlášených slabých míst zabezpečení v těchto počítačích.

Než začnete program Network Manager používat, seznamte se blíže s některými funkcemi programu. Podrobnosti o konfiguraci a používání těchto funkcí naleznete v programu Network Manager.

Poznámka: Program SecurityCenter informuje o závažných i méně závažných problémech ochrany ihned, jakmile problémy zjistí. Potřebujete-li pro stanovení problémů ochrany nápovědu, lze spustit nástroj McAfee Virtual Technician.

V této kapitole

Funkce programu Network Manager	80
Vysvětlení ikon programu Network Manager.....	81
Nastavení spravované sítě	83
Vzdálená správa sítě.....	89

Funkce programu Network Manager

Program Network Manager nabízí následující funkce.

Grafická mapa sítě














Mapa sítě programu Network Manager poskytuje grafické zobrazení stavu ochrany počítačů a součástí, které tvoří domácí síť. Pokud provedete změny v síti (pokud například přidáte další počítač), mapa sítě tyto změny rozpozná. Chcete-li přizpůsobit zobrazení, můžete aktualizovat mapu sítě, přejmenovat síť nebo zobrazit nebo skrýt součásti mapy sítě. Můžete také pro libovolnou součást na mapě sítě zobrazit podrobnosti.

Vzdálená správa

Pomocí mapy sítě programu Network Manager lze spravovat stav ochrany počítačů, které tvoří domácí síť. Můžete pozvat počítač k připojení ke spravované síti, sledovat stav ochrany spravovaného počítače nebo opravovat slabá místa zabezpečení ze vzdáleného počítače v síti.

Vysvětlení ikon programu Network Manager

Následující tabulka popisuje obvykle používané ikony na mapě sítě programu Network Manager.

Ikona	Popis
	Představuje spravovaný počítač online
	Představuje spravovaný počítač offline.
	Představuje nespravovaný počítač, ve kterém je nainstalován program SecurityCenter
	Představuje nespravovaný počítač offline.
	Představuje počítač online, ve kterém není nainstalován program SecurityCenter, nebo neznámé síťové zařízení
	Představuje počítač offline, ve kterém není nainstalován program SecurityCenter, nebo neznámé síťové zařízení offline
	Označuje, že je odpovídající položka chráněna a připojena.
	Označuje, že odpovídající položka může vyžadovat vaši pozornost
	Označuje, že odpovídající položka vyžaduje vaši okamžitou pozornost
	Představuje bezdrátový domácí směrovač.
	Představuje standardní domácí směrovač.
	Představuje síť Internet, která je připojena.
	Představuje síť Internet, která je odpojena.

KAPITOLA 16

Nastavení spravované sítě

Spravovanou síť nastavíte tak, že budete pracovat s položkami na mapě sítě a že do sítě přidáte členy (počítače). Než bude možno počítač vzdáleně spravovat, nebo než mu může být uděleno oprávnění ke vzdálené správě dalších počítačů v síti, musí se stát důvěryhodným členem sítě. Členství v síti je novým počítačům udělováno existujícími členy sítě (počítači) s oprávněními správce.

Podrobnosti související s kteroukoliv součástí, která se zobrazuje na mapě sítě, lze zobrazit i poté, co v síti provedete změny (například přidáte počítač).

V této kapitole

Práce s mapou sítě	84
Připojení ke spravované síti	86

Práce s mapou sítě

Když připojíte počítač k síti, analyzuje program Network Manager síť a zjišťuje přítomnost členů (spravovaných nebo nespravovaných), atributy směrovače a stav sítě Internet. Pokud nejsou nalezeni žádní členové, bude program Network Manager předpokládat, že aktuálně připojený počítač je první počítač v síti a vytvoří z tohoto počítače spravovaného člena s oprávněními správce. Ve výchozím nastavení název sítě zahrnuje název pracovní skupiny nebo název domény počítače, který se jako první připojí k síti a je v něm nainstalován program SecurityCenter. Síť však lze kdykoli později přejmenovat.

Pokud provedete změny v síti (pokud například přidáte další počítač), můžete mapu sítě přizpůsobit. Chcete-li přizpůsobit zobrazení, můžete například aktualizovat mapu sítě, přejmenovat síť nebo zobrazit nebo skrýt součásti mapy sítě. Můžete také zobrazit podrobnosti přidružené k libovolné součásti, která se objeví na mapě sítě.

Přístup k mapě sítě

Mapa sítě poskytuje grafickou reprezentaci počítačů a součástí, které tvoří domácí síť.

- Klepněte v základní nebo rozšířené nabídce na položku **Správa sítě**.

Poznámka: Při prvním přístupu k mapě se před zobrazením mapy sítě zobrazí výzva, zda má program důvěřovat ostatním počítačům v síti.

Obnovení mapy sítě

Mapu sítě lze kdykoliv obnovit (například poté, co se ke spravované síti připojil další počítač).

- 1 Klepněte v základní nebo rozšířené nabídce na položku **Správa sítě**.
- 2 V části **Požadovaná akce** klepněte na možnost **Obnovit mapu sítě**.

Poznámka: Odkaz **Obnovit mapu sítě** je dostupný, pouze když nejsou na mapě sítě vybrány žádné položky. Chcete-li výběr položky zrušit, klepněte na vybranou položku nebo na oblast bílého místa na mapě sítě.

Přejmenování sítě

Ve výchozím nastavení název sítě zahrnuje název pracovní skupiny nebo název domény počítače, který se jako první připojí k síti a je v něm nainstalován program SecurityCenter. Dáváte-li přednost jinému názvu, lze název změnit.

- 1 Klepněte v základní nebo rozšířené nabídce na položku **Správa sítě**.
- 2 V části **Požadovaná akce** klepněte na možnost **Přejmenovat síť**.
- 3 Zadejte název sítě do pole **Název sítě**.
- 4 Klepněte na tlačítko **OK**.

Poznámka: Odkaz **Přejmenovat síť** je dostupný, pouze když nejsou na mapě sítě vybrány žádné položky. Chcete-li výběr položky zrušit, klepněte na vybranou položku nebo na oblast bílého místa na mapě sítě.

Zobrazení a skrytí položky na mapě sítě

Ve výchozím nastavení jsou všechny počítače a součásti v domácí síti zobrazeny na mapě sítě. Skryté položky je možné kdykoli opět zobrazit. Lze skrýt pouze nespravované položky, spravované počítače nelze skrýt.

Akce	V základní nebo rozšířené nabídce klepněte na položku Správa sítě a potom proveďte následující kroky...
Skrytí položky na mapě sítě	Klepněte na položku na mapě sítě a potom v části Požadovaná akce klepněte na položku Skrýt tuto položku . V potvrzovacím dialogovém okně klepněte na tlačítko Ano .
Zobrazení skrytých položek na mapě sítě	V části Požadovaná akce klepněte na možnost Zobrazit skryté položky .

Zobrazení podrobností o položce

Podrobné informace o libovolné součásti sítě zobrazíte tím, že součást vyberete na mapě sítě. Tyto informace zahrnují název součásti, stav její ochrany a další informace požadované pro správu součásti.

- 1 Na mapě sítě klepněte na ikonu položky.
- 2 V části **Podrobnosti** zobrazíte informace o položce.

Připojení ke spravované síti

Než bude možno počítač vzdáleně spravovat, nebo než mu může být uděleno oprávnění ke vzdálené správě dalších počítačů v síti, musí se stát důvěryhodným členem sítě. Členství v síti je novým počítačům udělováno existujícími členy sítě (počítači) s oprávněními správce. Chcete-li zajistit, aby se k síti připojily pouze důvěryhodné počítače, musí se počítače udělující oprávnění a počítače, které se připojují, navzájem ověřit.

Pokud se počítač připojí k síti, je vyzván ke zveřejnění svého stavu ochrany společnosti McAfee ostatním počítačům v síti. Pokud počítač souhlasí se zveřejněním stavu ochrany, stane se spravovaným členem sítě. Pokud počítač odmítne zveřejnění stavu ochrany, stane se nespravovaným členem sítě. Nespravovanými členy sítě jsou obvykle počítače v roli hosta, které chtějí přistupovat k dalším funkcím sítě (například odeslat soubory nebo sdílet tiskárny).

Poznámka: Pokud máte nainstalovány jiné síťové programy McAfee (například program EasyNetwork), bude počítač po připojení k síti jako člen rozpoznán v těchto programech také jako spravovaný počítač. Úroveň oprávnění přiřazená počítači programem Network Manager se vztahuje na všechny síťové programy McAfee. Další informace o významu oprávnění hosta, úplného oprávnění a oprávnění správce v dalších síťových programech McAfee naleznete v dokumentaci k tomuto programu.

Připojení spravované sítě

Když obdržíte pozvání k připojení ke spravované síti, můžete pozvání přijmout nebo odmítnout. Můžete také určit, zda chcete, aby tento počítač a ostatní počítače v síti navzájem sledovaly nastavení zabezpečení (například zda jsou služby antivirové ochrany počítače aktualizované).

- 1 Ujistěte se, zda je v dialogovém okně Spravovaná síť zaškrtnuto políčko **Povolit sledování nastavení zabezpečení pro všechny počítače v této síti**.
- 2 Klepněte na příkaz **Připojit**.
Jakmile přijmete pozvání, objeví se dvě hrací karty.
- 3 Potvrďte, že tyto hrací karty jsou stejné jako karty zobrazené v počítači, který vás pozval k připojení ke spravované síti.
- 4 Klepněte na tlačítko **OK**.

Poznámka: Pokud nezobrazuje počítač, který vás pozval k připojení ke spravované síti, stejné hrací karty jako v potvrzovacím dialogovém okně zabezpečení, došlo k porušení zabezpečení ve spravované síti. Připojení jako člen k takovéto síti by mohlo počítač vystavit nebezpečí. Klepněte v dialogovém okně Spravovaná síť na tlačítko **Storno**.

Pozvání počítače k připojení ke spravované síti

Pokud je počítač přidán do spravované sítě nebo v síti existuje jiný nespravovaný počítač, můžete pozvat tento počítač k připojení jako člena ke spravované síti. Pozvat další počítače k připojení mohou pouze počítače s oprávněními správce v síti. Při odesílání pozvání také určujete úroveň oprávnění, kterou chcete přiřadit připojovanému počítači.

- 1 Na mapě sítě klepněte na ikonu nespravovaného počítače.
- 2 V části **Požadovaná akce** klepněte na možnost **Sledovat tento počítač**.
- 3 V dialogovém okně Pozvání počítače k připojení ke spravované síti proveďte některý z těchto kroků:
 - Chcete-li počítači povolit přístup k síti (pro dočasné domácí uživatele), klepněte na možnost **Povolit přístup hosta k programům spravované sítě**.
 - Chcete-li počítači povolit přístup k síti, klepněte na možnost **Povolit úplný přístup k programům spravované sítě**.
 - Chcete-li počítači povolit přístup k síti s oprávněními správce, klepněte na možnost **Povolit přístup správce k programům spravované sítě**. Tím současně umožňujete počítači udělit přístup jiným počítačům, které se chtějí ke spravované síti připojit.
- 4 Klepněte na tlačítko **OK**.
Počítači bude odesláno pozvání k připojení ke spravované síti. Jakmile počítač přijme pozvání, objeví se dvě hrací karty.
- 5 Potvrďte, že hrací karty jsou stejné jako karty zobrazené v počítači, který jste pozvali k připojení ke spravované síti jako člena.
- 6 Klepněte na tlačítko **Udělit přístup**.

Poznámka: Pokud se v počítači, kterého jste pozvali k připojení ke spravované síti, nezobrazují stejné hrací karty jako v potvrzovacím dialogovém okně zabezpečení, došlo k porušení zabezpečení ve spravované síti. Povolení připojení tohoto počítače k síti by mohlo ostatní počítače vystavit nebezpečí, proto v potvrzovacím dialogovém okně zabezpečení klepněte na tlačítko **Zamítnout přístup**.

Zastavení důvěřování počítačům v síti

Pokud jste ostatním počítačům v síti důvěřovali omylem, můžete jim přestat důvěřovat.

- V části **Požadovaná akce** klepněte na možnost **Zastavit důvěřování počítačům v této síti**.

Poznámka: Odkaz **Zastavit důvěřování počítačům v této síti** není k dispozici tehdy, jestliže máte oprávnění správce a v síti jsou další spravované počítače.

KAPITOLA 17

Vzdálená správa sítě

Po nastavení spravované sítě lze počítače a součásti, které spravovanou síť tvoří, spravovat vzdáleně. Můžete sledovat stav a úrovně oprávnění počítačů a součástí a vzdáleně opravovat většinu slabých míst zabezpečení.

V této kapitole

Sledování stavu a oprávnění.....	90
Oprava slabých míst zabezpečení	92

Sledování stavu a oprávnění

Spravovaná síť obsahuje spravované i nespravované členy. Spravování členové umožňují ostatním počítačům v síti sledovat svůj stav ochrany McAfee. Nespravování členové toto neumožňují. Nespravovanými členy sítě jsou obvykle počítače v roli hosta, které chtějí přistupovat k dalším funkcím sítě (například odeslat soubory nebo sdílet tiskárnu).

Nespravovaný počítač může být kdykoli jiným spravovaným počítačem v síti pozván, aby se stal spravovaným počítačem. Stejným způsobem se může stát spravovaný počítač kdykoli nespravovaným.

Spravované počítače mohou mít oprávnění správce, úplné oprávnění nebo oprávnění hosta. Oprávnění správce umožňují spravovanému počítači spravovat stav ochrany všech ostatních spravovaných počítačů v síti a udělovat členství v síti ostatním počítačům. Úplná oprávnění a oprávnění hosta umožňují počítači pouze přístup k síti. Úroveň oprávnění počítače lze kdykoli změnit.

Protože součástí spravované sítě mohou být také zařízení (například směrovače), můžete ke správě těchto zařízení použít program Network Manager. Lze také nakonfigurovat a upravit vlastnosti zobrazení zařízení na mapě sítě.

Sledování stavu ochrany počítače

Pokud není stav ochrany počítače v síti sledován (buď z důvodu, že počítač není členem sítě nebo že je nespravovaným členem), můžete požádat o jeho sledování.

- 1 Na mapě sítě klepněte na ikonu nespravovaného počítače.
- 2 V části **Požadovaná akce** klepněte na možnost **Sledovat tento počítač**.

Zastavení sledování stavu ochrany počítače

Sledování stavu ochrany spravovaného počítače v síti lze sice zastavit, nicméně počítač se stane nespravovaný a nebude možné vzdáleně sledovat stav ochrany tohoto počítače.

- 1 Na mapě sítě klepněte na ikonu spravovaného počítače.
- 2 V části **Požadovaná akce** klepněte na možnost **Zastavit sledování tohoto počítače**.
- 3 V potvrzovacím dialogovém okně klepněte na tlačítko **Ano**.

Úprava oprávnění spravovaného počítače

Oprávnění spravovaného počítače lze kdykoli změnit. To umožňuje upravit, které počítače mohou sledovat stav ochrany ostatních počítačů v síti.

- 1 Na mapě sítě klepněte na ikonu spravovaného počítače.
- 2 V části **Požadovaná akce** klepněte na možnost **Upravit oprávnění tohoto počítače**.
- 3 V dialogovém okně změny oprávnění zaškrtněte nebo zrušte zaškrtnutí políčka, abyste určili, zda mohou tento počítač a ostatní počítače ve spravované síti navzájem sledovat své stavy ochrany.
- 4 Klepněte na tlačítko **OK**.

Správa zařízení

Zařízení lze spravovat pomocí přístupu na jeho webovou stránku správy v programu Network Manager.

Postup správy zařízení:

- 1 Na mapě sítě klepněte na ikonu zařízení.
- 2 V části **Požadovaná akce** klepněte na možnost **Spravovat toto zařízení**.
Spustí se webový prohlížeč a zobrazí webovou stránku správy zařízení.
- 3 Ve webovém prohlížeči zadejte přihlašovací údaje a nakonfigurujte nastavení zabezpečení zařízení.

Poznámka: Je-li toto zařízení bezdrátový směrovač nebo přístupový bod chráněný programem Wireless Network Security, musíte použít ke konfiguraci nastavení zabezpečení zařízení program Wireless Network Security.

Úprava vlastností zobrazení zařízení

Při úpravě vlastností zobrazení zařízení můžete změnit název zobrazení zařízení na mapě sítě a určit, zda je zařízení bezdrátový směrovač.

- 1 Na mapě sítě klepněte na ikonu zařízení.
- 2 V části **Požadovaná akce** klepněte na možnost **Upravit vlastnosti zařízení**.
- 3 Název zobrazení zařízení určíte zadáním názvu do pole **Název**.
- 4 Typ zařízení určíte tím, že klepnete na položku **Standardní směrovač**, pokud se nejedná o bezdrátový směrovač, nebo na položku **Bezdrátový směrovač**, pokud se jedná o bezdrátový směrovač.
- 5 Klepněte na tlačítko **OK**.

Oprava slabých míst zabezpečení

Spravované počítače s oprávněními správce mohou sledovat stav ochrany McAfee ostatních spravovaných počítačů v síti a vzdáleně opravovat ohlášená slabá místa v zabezpečení. Pokud například stav ochrany McAfee spravovaného počítače uvádí, že je program VirusScan zakázán, jiný spravovaný počítač s oprávněním správce může program VirusScan vzdáleně povolit.

Pokud opravíte slabá místa zabezpečení vzdáleně, opraví program Network Manager většinu ohlášených problémů. Přesto mohou případně některá slabá místa zabezpečení vyžadovat ruční zásah v místním počítači. V takovém případě program Network Manager opraví ty problémy, které lze opravit vzdáleně, a potom vás vyzve, abyste zbývající problémy opravili přihlášením k programu SecurityCenter v počítači se slabými místy a následováním poskytnutých doporučení. V některých případech je navrženou opravou instalace nejnovější verze programu SecurityCenter ve vzdáleném počítači nebo počítačích v síti.

Oprava slabých míst zabezpečení

K opravě většiny slabých míst zabezpečení ve vzdálených spravovaných počítačích lze použít program Network Manager. Je-li například ve vzdáleném počítači zakázán program VirusScan, můžete program povolit.

- 1 Na mapě sítě klepněte na ikonu položky.
- 2 V části **Podrobnosti** zobrazte stav ochrany položky.
- 3 V části **Požadovaná akce** klepněte na možnost **Opravit slabá místa zabezpečení**.
- 4 Jakmile budou problémy se zabezpečením opraveny, klepněte na tlačítko **OK**.

Poznámka: Přestože program Network Manager automaticky opraví většinu slabých míst zabezpečení, vyžadují některé opravy spuštění programu SecurityCenter v počítači se slabými místy a následování poskytnutých doporučení.

Instalace zabezpečovacího softwaru společnosti McAfee ve vzdálených počítačích

Pokud jeden nebo více počítačů v síti nepoužívá nejnovější verzi programu SecurityCenter, nelze vzdáleně sledovat stav jejich zabezpečení. Chcete-li vzdáleně sledovat tyto počítače, je nutné v každém z nich nainstalovat nejnovější verzi programu SecurityCenter.

- 1** V počítači, do nějž chcete zabezpečovací software nainstalovat, spusťte program SecurityCenter.
- 2** V části **Běžné úkoly** klepněte na tlačítko **Můj účet**.
- 3** K přihlášení použijte e-mailovou adresu a heslo použité k registraci zabezpečovacího softwaru při první instalaci.
- 4** Vyberte vhodný produkt, klepněte na ikonu **Stáhnout/Instalovat** a postupujte podle pokynů na obrazovce.

Reference

Slovníček pojmů obsahuje seznam a definice nejpoužívanějších výrazů z terminologie zabezpečení používaných v produktech společnosti McAfee.

Slovníček

8

802.11

Sada standardů IEEE pro přenos dat prostřednictvím bezdrátové sítě. Standard 802.11 je obecně známý jako Wi-Fi standard.

802.11a

Rozšíření standardu 802.11, které se vztahuje na bezdrátové síť LAN a odesílá data rychlostí 54 Mb/s v pásmu 5 GHz. Přestože je přenosová rychlost vyšší než u standardu 802.11b, pokrytá vzdálenost je mnohem menší.

802.11b

Rozšíření standardu 802.11, který odesílá data rychlostí 11 Mb/s v pásmu 2,4 GHz. Přestože je přenosová rychlost pomalejší než u standardu 802.11a, pokrytá vzdálenost je mnohem větší.

802.1x

Standard IEEE pro ověření v drátových a bezdrátových sítích. Standard 802.1x je obvykle používán spolu se standardem 802.11 pro bezdrátové síť.

A

adresa IP

Identifikátor počítače nebo zařízení v síti TCP/IP. Síť používající protokol TCP/IP směřují zprávy na základě cílové adresy IP. Formát adresy IP je 32bitová číselná adresa napsaná jako čtyři čísla oddělená tečkami. Každé číslo může být v rozsahu od 0 do 255 (např. 192.168.1.100).

adresa MAC

(adresa Media Access Control) Jedinečné výrobní číslo přiřazené fyzickému zařízení s přístupem do sítě.

adresa URL

(Uniform Resource Locator) Jedná se o standardní formát internetových adres.

archivace

Vytvoření kopie důležitých souborů místně na discích CD, DVD, jednotce USB, externím pevném disku nebo síťové jednotce.

automaticky otevíraná okna

Malá okna zobrazovaná v popředí před ostatními okny na obrazovce počítače. Automaticky otevíraná okna jsou ve webových prohlížečích často používána k zobrazování reklam.

B

bezdrátový adaptér

Zařízení, které doplní počítač nebo PDA o bezdrátovou technologii. Je připojeno prostřednictvím portu USB, slotu pro kartu PC Card (CardBus), slotu pro paměťovou kartu nebo interně pomocí sběrnice PCI.

bod obnovení systému

Obraz (kopie) obsahu paměti počítače nebo databáze. Systém Windows vytváří pravidelně body obnovení také ve chvílích významných systémových událostí (například při instalaci ovladače nebo programu). Vytvoření a pojmenování vlastních bodů obnovení je však možné kdykoliv.

brána firewall

Systém (hardware, software nebo obojí) navržený k tomu, aby bránil neoprávněnému přístupu k soukromé síti nebo ven ze soukromé sítě. Brány firewall jsou často používány, aby bránily neoprávněným uživatelům Internetu v přístupu k sítím připojeným k Internetu, zejména v přístupu k intranetu. Všechny zprávy přicházející nebo opouštějící síť intranet prochází bránou firewall, která každou zprávu kontroluje a blokuje ty, které nesplňují specifikovaná bezpečnostní kritéria.

C

cestování

Schopnost přemístit se z pokrytí jednoho přístupového bodu (AP) k jinému bez přerušení nebo ztráty připojení.

Č

červ

Termínem červ je označován virus se schopností seberekopie, který je umístěn v aktivní paměti, a je schopen rozesílat své kopie prostřednictvím e-mailů. Červy se kopírují a spotřebovávají systémové zdroje, čímž snižují výkon nebo zastavují úlohy.

D

DAT

(Datové soubory signatur) Soubory obsahující definice, které jsou používány při detekci virů, trojských koňů, spywaru, adwaru a dalších potenciálně nežádoucích programů v počítači nebo disku USB.

dialer

Software, který pomáhá navázat připojení k Internetu. Při používání ve zlém úmyslu mohou

disk USB

Malý paměťový disk, který lze zapojit přímo do portu USB v počítači. Disk USB funguje stejně jako malá disková jednotka a umožňuje snadný přenos souborů z jednoho počítače na druhý.

DNS

(Systém názvu domény) Systém, který převádí název hostitele nebo domény na IP adresu. V prostředí Internetu je systém DNS používán k převodu snadno čitelné webové adresy (např. www.myhostname.com) na IP adresu (např. 111.2.3.44) tak, aby bylo možné zobrazit požadovanou webovou stránku. Bez systému DNS by bylo nutné zapsat do webového prohlížeče IP adresu.

dočasný soubor

Soubor vytvořený operačním systémem nebo jiným programem v paměti nebo na disku, který bude použit v průběhu relace a potom odstraněn.

domácí síť

Dva a více počítačů, které jsou doma propojeny tak, aby mohly sdílet nejen soubory, ale také přístup k Internetu. Viz také LAN.

doména

Místní podsít' nebo popis webů v Internetu.

V místní síti (LAN) je doména podsítí tvořena klienty počítači a servery, které jsou řízeny jedinou databází zabezpečení. V této souvislosti mohou domény zvýšit výkon. V prostředí Internetu je doména částí každé webové adresy (např. www.abc.com, kde "abc" je doména).

E

e-mail

(elektronická pošta) Zprávy zasílané a přijímané elektronickým způsobem prostřednictvím počítačové sítě. Viz také Webmail.

e-mailový klient

Program běžící v počítači, který umožňuje odesílání a příjem e-mailů (např. Microsoft Outlook).

ESS

(Extended Service Set) Sada dvou nebo více sítí, které tvoří jednu podsít'.

externí pevný disk

Pevný disk, který je umístěn mimo počítač.

F

falšování adres IP

Neoprávněné falšování adres IP v paketech IP. Je využíváno v mnoha typech útoků včetně zneužití relace. Často je také použito k falšování hlaviček nevyžádaných e-mailových zpráv, aby nemohly být trasovány.

filtrování obrázků

Volba Rodičovský dohled, která potenciálně blokuje zobrazení nepatřičných obrázků z Internetu.

H

heslo

Kód (obvykle alfanumerický) použitý pro získání přístupu k počítači, programu nebo na webový server.

I

integrovaná brána

Zařízení, které spojuje funkce přístupového bodu (AP), směrovače a brány firewall. Některá zařízení mohou obsahovat také vylepšení zabezpečení a funkce vytváření mostu.

Internet

Internet obsahuje velké množství vzájemně propojených sítí používajících protokoly TCP/IP pro hledání a přenos dat. Internet se vyvinul z propojení počítačů univerzit a vysokých škol (na konci 60. a začátku 70. let 20. století) financovaného Ministerstvem obrany USA a nazvaného ARPANET. Dnes Internet představuje globální síť zahrnující téměř 100 000 nezávislých sítí.

intranet

Soukromá síť, obvykle v rámci organizace, která je přístupná pouze oprávněným uživatelům.

J

Jednotka smart drive

Viz Jednotka USB.

K

karanténa

Izolace Např. v aplikaci Data Backup jsou detekovány podezřelé soubory, které jsou uloženy do karantény, aby nemohly škodit počítači nebo souborům.

karta bezdrátového adaptéru USB

Karta bezdrátového adaptéru, kterou lze zapojit přímo do patice USB v počítači.

karty bezdrátového adaptéru PCI

(Peripheral Component Interconnect) Karta bezdrátového adaptéru se zapojuje do rozšiřující patice PCI v počítači.

klíč zabezpečení

Série písmen a čísel použitých dvěma zařízeními k ověření komunikace. Klíč musí mít obě zařízení. Viz také WEP, WPA, WPA2, WPA-PSK, a WPA2-PSK.

klíčové slovo

Slovo, které můžete přiřadit k zálohovanému souboru tak, aby došlo k vytvoření vztahu nebo propojení s jinými soubory, které mají přiřazeno stejné klíčové slovo. Přiřazením klíčových slov k souborům usnadníte vyhledávání souborů, které jste publikovali v Internetu.

klient

Aplikace, která je spuštěna na osobním počítači nebo pracovní stanici a při provádění některých operací závisí na serveru. Například e-mailový klient je aplikace, která umožní odesílat a přijímat e-maily.

knihovna

Online úložná oblast pro soubory, které jste zálohovali a publikovali. Knihovna aplikace Data Backup je webový server v Internetu přístupný komukoliv s přístupem k Internetu.

komprimace

Proces, při kterém jsou soubory komprimovány do podoby minimalizující požadavky na místo pro uložení nebo na přenos.

Koš

Simulovaný koš na vymazané soubory a složky systému Windows.

L

LAN

(Local Area Network) Počítačová síť, která pokrývá relativně malou oblast (např. jediná budova). Počítače v síti LAN mohou vzájemně komunikovat a sdílet zdroje, např. tiskárny a soubory.

M

mapa sítě

Grafická reprezentace počítačů a součástí, které tvoří domácí síť.

MAPI

(Messaging Application Programming Interface) Specifikace rozhraní společnosti Microsoft, která umožňuje spolupráci různých aplikací zasílání zpráv a pracovních skupin (včetně e-mailu, hlasové pošty a faxu) s klientem, jako je například klient aplikace Exchange.

modul plug-in

Malý program, který spolu s větším programem zvýší jeho funkčnost. Moduly plug-in umožňují webovému prohlížeči přístup a spuštění souborů vložených do dokumentů HTML, které by prohlížeč normálně nerozpoznal (například animace, videa a zvukové soubory).

MSN

(Microsoft Network) Skupina webových služeb nabízených korporací Microsoft včetně vyhledávačů, elektronické pošty, zasílání rychlých zpráv a portálu.

N

NIC

(Network Interface Card) Karta, která se zapojuje do laptopu nebo do jiného zařízení a připojuje zařízení k síti LAN.

O

obnovit

Načtení kopie souboru z úložiště zálohování online nebo archivu.

odkaz

Soubor obsahující pouze informace o umístění jiného souboru v počítači.

odmítnutí služby

Typ útoku který zpomalí nebo zastaví síťový provoz. Útok typu odmítnutí služby (útok DoS) se objeví, jestliže je síť zaplavena příliš velkým počtem doplňujících požadavků a pravidelný provoz je zpomalen nebo zcela přerušen. Výsledkem obvykle není krádež informací nebo jiná slabá místa v zabezpečení.

Ochrana systému

Ochrana systému McAfee zajišťuje neoprávněné změny v počítači a při jejich výskytu zobrazuje výstrahu.

organizace Wi-Fi Alliance

Organizace vytvořená vedoucími výrobci bezdrátových zařízení a softwaru. Organizace Wi-Fi Alliance usiluje o certifikaci všech produktů založených na standardu 802.11 pro zajištění vzájemné spolupráce mezi produkty a propagace výrazu Wi-Fi jako celosvětové značky na všech trzích pro všechny produkty bezdrátových sítí LAN založené na standardu 802.11. Organizace slouží jako konsorcium, testovací laboratoř a místo pro styk dodavatelů, kteří chtějí propagovat růst průmyslu.

ověřovací kód zpráv (MAC)

Bezpečnostní kód používaný k šifrování zpráv, které jsou přenášeny mezi počítači. Tato zpráva je akceptována, jestliže počítač uzná dešifrovaná data jako platná.

ověřování

Proces identifikace jednotlivých uživatelů, obvykle na základě jedinečného jména a hesla.

ovládací prvek ActiveX

Součást softwaru využívaná programy nebo webovými stránkami dodávají funkčnost, která se jeví jako normální součást programu nebo webové stránky. Většina ovládacích prvků ActiveX je neškodná, nicméně některé mohou získávat informace z vašeho počítače.

P

platforma U3

(Vy: zjednodušená, inteligentní, mobilní) Platforma pro spuštění programů systému Windows 2000 nebo Windows XP přímo z jednotky USB. Počáteční krok pro platformu U3, která umožňuje uživatelům spustit programy U3 v počítačích s běžícím systémem Windows bez nutnosti instalace nebo uložení dat případně nastavení v počítači, byl učiněn v roce 2004 společností M-Systems a SanDisk.

podvodný server nebo zpráva (phishing)

Cílem internetových podvodů je získat cenné informace (např. čísla kreditních karet nebo sociálního pojištění, uživatelská identifikační čísla nebo hesla) od neznámých osob za účelem podvodného využití.

POP3

(Post Office Protocol 3) Rozhraní mezi programem e-mailového klienta a e-mailovým serverem. Většina domácích uživatelů má standardní e-mailový účet (POP3).

port

Místo vstupu a výstupu informací z nebo do počítače. Např. konvenční analogový modem je připojen k sériovému portu.

potenciálně nežádoucí programy (PUP)

Program, který bez svolení shromažďuje osobní informace (např. spyware nebo adware).

prohledávání na požádání

Prohledávání, které je provedeno na požádání (tzn. při spuštění operace). Na rozdíl od prohledávání v reálném čase, není prohledávání na požádání spuštěno automaticky.

prohledávání v reálném čase

Během přístupu uživatele nebo počítače k souborům jsou v souborech vyhledávány viry a jiná aktivity.

prohlížeč

Program používaný k prohlížení webových stránek na Internetu. Populárními webovými prohlížeči jsou Microsoft Internet Explorer a Mozilla Firefox.

prostý text

Text, který není šifrován. Viz také šifrování.

protokol

Formát (hardware nebo software) přenosu dat mezi dvěma zařízeními. Chcete-li komunikovat s ostatními počítači, počítač nebo zařízení musí podporovat správný protokol.

protokol PPPoE

(Point-to-Point Protocol Over Ethernet) Způsob využívající protokol s vytáčeným spojením PPP pomocí sítě Ethernet jako způsobem přenosu dat.

proxy

Počítač (nebo na něm spuštěný software), který slouží jako bariéra mezi sítí a Internetem a externím serverům prezentuje pouze jednu síťovou adresu. Server proxy tedy slouží jako prostředník představující všechny interní počítače. Zajišťuje zabezpečení identit v síti a současně umožňuje přístup k Internetu. Viz také Server proxy.

přetečení vyrovnávací paměti

Situace, která se objeví, když se programy nebo procesy pokoušejí do vyrovnávací paměti (dočasného úložiště dat) počítače uložit více dat, než je možné. Přetečení vyrovnávací paměti nebo přepis dat v přílehlých vyrovnávacích pamětech.

přípojný bod

Geografická hranice tvořená bezdrátovým (802.11) přístupovým bodem (AP). Uživatelé, kteří se dostanou s laptopem vybaveným možností bezdrátového připojení do dosahu přípojného bodu, se mohou připojit k Internetu za předpokladu, že přípojný bod signalizuje svoji přítomnost a není třeba provést ověření. Přípojné body jsou často umístěny na velmi zalidněných místech, jako jsou například letiště.

Přístupový bod

Síťové zařízení (obvykle zvané bezdrátový směrovač), které se připojí k ethernetovému hubu nebo přepínači k rozšíření fyzického rozsahu služeb pro bezdrátové uživatele. Pokud uživatelé bezdrátové technologie cestují s mobilními zařízeními, přenos dat a spojení je postupně udržováno přechodem z jednoho přístupového bodu (AP) do druhého.

publikovat

Veřejné zpřístupnění zálohovaného souboru na Internetu. Publikované soubory můžete zpřístupnit vyhledáním v knihovně aplikace Data Backup.

R

registr

Databáze, do které systém Windows ukládá informace o konfiguraci. Registr obsahuje profily pro každého uživatele počítače a informace o hardwaru systému, nainstalovaných programech a nastavení vlastnictví. Během operace systém Windows neustále odkazuje na tyto informace.

Rodičovská kontrola

Nastavení, která pomáhají usměrnit, co mohou děti sledovat při procházení Internetu. Chcete-li nastavit Rodičovský dohled, můžete zapnout nebo vypnout filtrování obrázků, zvolit skupinu hodnocení obsahu dle věkové kategorie uživatele a nastavit dobu trvání procházení Internetu.

rychlá archivace

Archivace pouze těch sledovaných souborů, které byly změněny od poslední úplné nebo rychlé archivace. Viz. také plná archivace.

S

sdílení

Operace umožňující příjemcům e-mailu po omezenou dobu přistupovat k vybraným zazálohovaným souborům. Při sdílení souboru odesíláte jeho zazálohovanou kopii určeným příjemcům e-mailu. Příjemci přijmou od aplikace Zálohování dat e-mailovou zprávu, která oznamuje, že soubory jsou s příjemci sdíleny. Tento e-mail zároveň obsahuje odkaz na dané sdílené soubory.

sdílený tajný klíč

Řetězec nebo klíč (obvykle heslo), které je sdíleno mezi dvěma komunikujícími stranami ještě před zahájením komunikace. Sdílený tajný klíč je používán k ochraně citlivých částí zpráv RADIUS.

server

Počítač nebo program, který přijme připojení jiného počítače nebo programů a vrátí odpovídající odezvu. Např. při každém odeslání nebo příjmu zpráv elektronické pošty e-mailový program provede připojení k poštovnímu serveru.

server DNS

(Domain Name System server) Počítač, který vrací IP adresu odpovídající hostitelskému názvu nebo názvu domény. Viz také DNS.

server proxy

Součást brány firewall spravující internetový provoz do sítě LAN a z ní. Server proxy může zvýšit výkon zprostředkováním často vyžadovaných dat, jako jsou oblíbené webové stránky, a může filtrovat a zakázat požadavky, které vlastník nepokládá za vhodné, například neoprávněné požadavky na přístup k soukromým souborům.

seznam důvěryhodných položek

Obsahuje položky, kterým můžete věřit a které nebyly detekovány. Pokud programu důvěřujete omylem (např. potenciálně nežádoucí program nebo změna registru) nebo chcete, aby byl zjištěn, musíte jej z tohoto seznamu odebrat.

seznam povolených serverů

Seznam webových stránek, ke kterým je povolen přístup, protože nejsou považovány za podvodné.

seznam zakázaných serverů

U ochrany proti podvodným zprávám (phishing) je uveden seznam webových stránek, které jsou považovány za škodlivé.

síť

Souhrn přístupových bodů a jejich přiřazených uživatelů ekvivalentní systému ESS.

síťová jednotka

Disková nebo pásková jednotka, která je připojena k serveru v síti sdílené více uživateli. Síťové jednotky jsou někdy nazývány vzdálené jednotky.

skript

Seznam příkazů, které mohou být automaticky provedeny (tzn. bez zásahu uživatele). Na rozdíl od programů, mohou být skripty uloženy ve formě jednoduchého textu a při každém spuštění kompilovány. Skripty jsou také nazývána makra a dávkové soubory.

skupiny hodnocení obsahu dle věkové kategorie uživatele

U rodičovské kontroly věková skupina, ke které uživatel patří. Obsah je zpřístupněn nebo blokován podle skupiny hodnocení obsahu, ke které patří uživatel. Skupiny hodnocení obsahu dle věkové kategorie uživatele obsahují tyto položky: Předškolní věk, Mladší školní věk, Starší školní věk, Mladistvý a Dospělý.

sledovaná umístění

Složky v počítači, které sleduje aplikace Zálohování dat.

sledované typy souborů

Typy souborů (například .doc, .xls atd.), které aplikace Zálohování dat archivuje ve sledovaných umístěních.

slovníkový útok

Typ útoku hrubou silou, který používá obyčejná slova k pokusu o odhalení hesla.

směrovač

Síťové zařízení, které předává pakety z jedné sítě do jiné. Směrovače jsou založeny na interních směrovacích tabulkách. Přečtou každý příchozí paket a rozhodnou, jak ho předat dále. Toto rozhodnutí je založeno na jakékoliv kombinaci zdrojové a cílové adresy zdroje, stejně jako na aktuálním objemu provozu, jako je zátěž, ceny linek, špatné linky. Směrovač je někdy nazýván přístupovým bodem (AP).

SMTP

(Simple Mail Transfer Protocol) Protokol TCP/IP pro odesílání zpráv z jednoho počítače do jiného v rámci sítě. Tento protokol je používán na Internetu ke směrování e-mailů.

soubor cookie

Malý soubor, který obsahuje informace obvykle zahrnující uživatelské jméno a aktuální datum a čas, je uložený v počítači osoby procházející web. Soubory cookies primárně používané webovými servery k identifikaci uživatelů, kteří byli již dříve zaregistrováni nebo web navštívili. Nicméně mohou být zdrojem informací pro hackery.

součásti souborů

Zbytky souboru roztroušeného na disku. Fragmentace souboru vzniká při přidávání nebo vymazání souborů a může zpomalit výkon počítače.

správcovská sada

Sada nástrojů (programů), které uživateli s přístupem na úrovni správce zajistí přístup do počítače nebo do počítačové sítě. Mohou obsahovat spyware a jiné utajené programy, které mohou způsobit další ohrožení zabezpečení nebo soukromí počítačových dat a osobních informací.

spravovaná síť

Domácí síť, která má dva typy členů: spravované členy a nespravované členy. Spravovaní členové umožňují ostatním počítačům v síti sledovat svůj stav ochrany. Nespravovaní členové toto neumožňují.

SSID

(Service Set Identifier) Token (tajný klíč), který identifikuje bezdrátovou (Wi-Fi 802.11) síť. Identifikátor SSID je nastaven správcem sítě a musí být dodán uživatelům, kteří se chtějí připojit k síti.

SSL

(Secure Sockets Layer) Protokol vyvinutý společností Netscape určený pro přenos soukromých dokumentů pomocí Internetu. Protokol SSL používá veřejný klíč k šifrování dat, která jsou přenášena pomocí připojení SSL. Adresy URL, které vyžadují spuštění připojení SSL začínají řetězcem https místo http.

standardní e-mailový účet

Viz. POP3.

Synchronizace

Slouží k odstranění nekonzistence mezi zálohovanými soubory a soubory uloženými v místním počítači. Soubory můžete synchronizovat, když verze souboru v úložišti zálohování online je novější než jeho verze na jiných počítačích.

system launchpad

Komponent rozhraní U3, které funguje jako výchozí bod pro spuštění a správu programů U3 USB.

Š

šifrování

Proces, při kterém jsou data převedena z textové podoby do kódu. To učiní informaci nečitelnou pro osoby, které nevědí, jak ji dešifrovat. Šifrovaná data jsou také známá jako zašifrovaný text.

šířka pásma

Množství dat, která mohou být přenesena za určitý časový úsek.

škodlivý přístupový bod

Neověřený přístupový bod Škodlivý přístupový bod může být nainstalován do zabezpečené podnikové sítě, kde zajistí neověřeným stranám přístup do sítě. Tyto body mohou být také vytvořeny tak, že útočníkovi umožní vést útok typu "muž uprostřed".

T

TKIP

(Temporal Key Integrity Protocol) Rychlý způsob opravy pro překonání základních slabých míst v zabezpečení WEP, zvláště opětovného použití klíčů. Protokol TKIP mění dočasné klíče po každých 10 000 paketech a takto poskytuje metodu dynamické distribuce, která značně zvyšuje úroveň zabezpečení sítě. Proces zabezpečení protokolem TKIP začíná 128bitovým dočasným klíčem, který je sdílený mezi klienty a přístupovými body (AP). Protokol TKIP spojuje dočasný klíč s adresou MAC (počítače klienta) a následně přidává poměrně velký 16 znaků dlouhý inicializační vektor v osmičkové soustavě k vytvoření klíče, který šifruje data. Tento postup zajistí, že každá stanice používá k šifrování dat různé proudy klíčů. Protokol TKIP používá k šifrování šifru RC4.

Trezor hesel

Bezpečné úložiště pro osobní hesla. Umožňuje ukládat hesla s jistotou, že k nim nebudou mít přístup žádní další uživatelé (ani správce).

Trojský kůň

Programy, které se zdají být legitimními programy, ale mohou poškodit důležité soubory, snížit výkon a umožnit neoprávněný přístup k počítači.

U

událost

Činnost aktivovaná buď uživatelem, zařízením nebo samotným počítačem, který přepíná odezvu. Program McAfee zaznamenává události do protokolu událostí.

Ú

úložiště zálohování online

Umístění na serveru online, kam jsou po zálohování ukládány soubory.

U

umístění s hloubkovým sledováním

Složka v počítači, ve které jsou změny sledovány aplikací Zálohování dat. Pokud nastavíte umístění s hloubkovým sledováním, aplikace Data Backup bude zálohovat obsah složky a jejich podsložek.

umístění s omezeným sledováním

Složka v počítači, ve které jsou změny sledovány aplikací Zálohování dat. Pokud nastavíte umístění s omezeným sledováním, aplikace Zálohování dat bude zálohovat obsah složky (podsložky archivovány nebudou).

Ú

úplná archivace

Archivace všech dat vyhovujících zadaným typům souborů a umístěním. Viz. také rychlá archivace.

U

USB

(Universal Serial Bus) Jedná se o standardizované sériové počítačové rozhraní, které umožňuje k počítači připojit taková periferní zařízení jakými jsou klávesnice, pákové ovladače nebo tiskárny.

Ú

útok hrubou silou

Způsob dekódování šifrovaných dat, jakými jsou např. hesla, prostřednictvím vyčerpávajícího úsilí (s použitím hrubé síly) namísto zapojení důmyslné strategie. Útok hrubou silou je považován za spolehlivý, přestože je to časově náročný postup. Útok hrubou silou je také nazýván jako dešifrování hrubou silou.

útok typu muž uprostřed

Způsob zachycení a možné úpravy zpráv mezi dvěma stranami bez toho, aniž by kterákoliv ze stran věděla, že jejich komunikační spojení bylo zrušeno.

U

uzel

Samostatný počítač připojený do sítě.

V

virus

Počítačové viry jsou programy se schopností sebepublikace, které mohou poškodit soubory a data. Často se zdá, že pocházejí od důvěryhodného odesílatele a mají neškodný obsah.

VPN

(Virtual Private Network) Privátní síť vytvořená v rámci veřejné sítě, jejíž výhody správy také využívá. Privátní virtuální sítě jsou využívány podniky k vytvoření sítě WAN, které zahrnují velké geografické oblasti, za účelem poskytnutí připojení firemních poboček v rámci architektury Site-to-site nebo umožní uživatelům mobilních technologií se připojit pomocí vytáčeného spojení do podnikových sítí LAN.

vyrovnávací paměť

Dočasné místo úložiště dat v počítači. Např. zvýšení rychlosti a účinnosti procházení webu, při příštím prohlížení váš prohlížeč může získat webovou stránku ze své mezipaměti (spíše než ze vzdáleného serveru).

W

wardriver

Osoba vybavená počítačem s technologií bezdrátového připojení a některým speciálním hardwarem nebo softwarem, která vyhledává bezdrátové sítě (802.11) při projíždění městy.

Webmail

Zprávy zasílané a přijímané elektronickým způsobem prostřednictvím Internetu. Viz. také e-mail.

Webové štěnice

Malé grafické soubory, které se vkládají do stránek HTML a umožňují neověřeným zdrojům nastavit v počítači soubory cookie. Tyto soubory cookie mohou přenášet informace k neověřeným zdrojům. Webové štěnice jsou také někdy označovány jako webové majáky nebo soubory GIF tvořené jedním pixelem.

WEP

(Wired Equivalent Privacy) Šifrovací a ověřovací protokol definovaný jako součást standardu 802.11. Počáteční verze jsou založeny na šifrách RC4 a mají značný počet slabých míst. Protokol WEP se snaží o poskytnutí zabezpečení pomocí šifrování dat přenášených rádiovými vlnami, aby byla chráněna během přenosu z jednoho koncového bodu do jiného. Bylo však zjištěno, že protokol WEP není tak bezpečný, jak se věřilo.

Wi-Fi

(Wireless Fidelity) Tento výraz jen obecně používán organizací Wi-Fi Alliance ve spojení s bezdrátovou sítí pro pojmenování jakéhokoliv typu sítě 802.11.

Wi-Fi Certified

Produkt byl otestován a vyzkoušen organizací Wi-Fi Alliance. Certifikované produkty Wi-Fi jsou pokládány za vzájemně spolupracující, i když pocházejí od různých výrobců. Uživatel produktu, který nese označení Wi-Fi Certified, může používat všechny značky přístupových bodů (AP) s hardwarem klienta jiné značky, pokud je také certifikován.

WLAN

(Wireless Local Area Network) Místní počítačová síť (LAN) využívající bezdrátové připojení. Síť WLAN používá ke komunikaci mezi počítači namísto kabelů vysokofrekvenční rádiové vlny.

WPA

Standard, který silně zvyšuje úroveň ochrany dat a řízení přístupu existujících a budoucích systémů LAN. Je navržen tak, aby fungoval na existujícím hardwaru jako inovace softwaru. Standard WPA pochází ze standardu IEEE 802.11i a je s ním kompatibilní. Pokud je správně nainstalován, poskytuje uživatelům síť LAN jistotu, že jejich data zůstanou chráněna a že přístup k síti budou mít pouze oprávnění uživatelé.

WPA-PSK

Speciální režim standardu WPA vytvořený pro domácí uživatele, kteří nepožadují silnou třídu zabezpečení pro velké společnosti a nemají přístup k ověřovacím serverům. V tomto režimu domácí uživatel zadává ručně spouštěcí heslo, aby aktivoval režim WPA-PSK, a měl by pravidelně měnit heslo v každém bezdrátově připojeném počítači a přístupovém bodu. Viz také WPA2-PSK a TKIP.

WPA2

Standard WPA2 je aktualizací bezpečnostního standardu WPA a je založen na standardu IEEE 802.11i.

WPA2-PSK

Speciální režim WPA2-PSK je podobný režimu WPA-PSK a je založen na standardu WPA2. Běžným rysem režimu WPA2-PSK je, že zařízení často podporují více režimů šifrování (například šifrování AES, TKIP) zároveň, zatímco starší zařízení obecně podporují pouze jeden režim šifrování ve stejnou dobu (to je když všichni klienti používají stejný režim šifrování).

Z

zabezpečení RADIUS

(Remote Access Dial-In User Service) Protokol, který uživateli umožňuje ověření, obvykle v souvislosti s dálkovým přístupem. Původně byl definován pro použití na serverech s telefonickým vzdáleným přístupem. Nyní je protokol RADIUS používán v různých prostředích ověřování, včetně ověřování 802.1x uživatelů sítě WLAN.

zálohování

Vytvoření kopie důležitých souborů na bezpečném serveru online.

zašifrovaný text

Šifrovaný text. Zašifrovaný text je nečitelný, dokud není převeden na prostý text (tzn. dešifrován).

Informace o společnosti McAfee

Společnost McAfee, Inc. se sídlem v Santa Clara v Kalifornii, která je špičkovým dodavatelem služeb pro prevenci neoprávněných vniknutí a správy rizik zabezpečení, poskytuje účinná a ověřená řešení a služby zabezpečení systémů a sítí po celém světě. Díky mimořádným zkušenostem v oblasti zabezpečení a využití nejnovějších technologií umožňuje společnost McAfee uživatelům, ať se již jedná o veřejný sektor, poskytovatele služeb, firmy či domácí uživatele, blokovat útoky, zabránit únikům informací a neustále sledovat a zlepšovat zabezpečení.

Copyright

Copyright © 2007-2008 McAfee, Inc. Všechna práva vyhrazena. Žádná část této publikace nesmí být reprodukována, přenášena, přepisována, uložena v archivačním systému ani přeložena do libovolného jazyka v žádné podobě ani žádnými prostředky bez předchozího písemného souhlasu společnosti McAfee, Inc. McAfee a další zde uvedené ochranné známky jsou registrovanými ochrannými známkami nebo ochrannými známkami společnosti McAfee, Inc. a/nebo jejich dceřiných společností v USA a/nebo dalších zemích. Červená barva McAfee Red ve spojení se zabezpečením je význačným znakem produktů společnosti McAfee. Všechny další uvedené registrované a neregistrované ochranné známky a materiály podléhající autorskému právu jsou vlastnictvím příslušných vlastníků.

OCHRANNÉ ZNÁMKY

AVERT, EPO, EPOLICY ORCHESTRATOR, FLASHBOX, FOUNDSTONE, GROUPSHIELD, HERCULES, INTRUSHIELD, INTRUSION INTELLIGENCE, LINUXSHIELD, MANAGED MAIL PROTECTION, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, MCAFEE.COM, NETSHIELD, PORTALSHIELD, PREVENTSYS, PROTECTION-IN-DEPTH STRATEGY, PROTECTIONPILOT, SECURE MESSAGING SERVICE, SECURITYALLIANCE, SITEADVISOR, THREATSCAN, TOTAL PROTECTION, VIREX, VIRUSSCAN.

Licence

POZNÁMKA PRO VŠECHNY UŽIVATELE: DŮKLADNĚ SI PŘEČTĚTE PŘÍSLUŠNOU SMLOUVU ODPOVÍDAJÍCÍ ZAKOUPENÉ LICENCI, V NÍŽ JSOU UVEDENY OBECNÉ PODMÍNKY TÝKAJÍCÍ SE UŽÍVÁNÍ LICENCOVANÉHO SOFTWARE. POKUD NEVÍTE, JAKÝ TYP LICENCE JSTE ZÍSKALI, NAJDETE POTŘEBNÉ INFORMACE V PRODEJNÍM DOKUMENTU NEBO V DALŠÍCH DOKUMENTECH SOUVISEJÍCÍCH S UDĚLENÍM LICENCE NEBO OBJEDNÁVKOU, KTERÉ JSOU DODÁNY S BALENÍM SOFTWARE NEBO KTERÉ JSTE OBDRŽELI SAMOSTATNĚ JAKO SOUČÁST NÁKUPU (VE FORMĚ PŘÍRUČKY, SOUBORU NA DISKU CD PRODUKTU NEBO SOUBORU NA WEBU, Z NĚHOŽ JSTE STÁHLI PŘÍSLUŠNÝ SOFTWAREOVÝ BALÍK). POKUD NESOUHLASÍTE SE VŠEMI PODMÍNKAMI UVEDENÝMI VE SMLouvĚ, SOFTWARE NEINSTALUJTE. MŮŽETE PRODUKT VRÁTIT SPOLEČNOSTI MCAFEE, INC. NEBO TAM, KDE JSTE JEJ ZAKOUPILI, A OBDRŽÍTE PLNOU NÁHRADU.

Služby pro zákazníky a technická podpora

Program SecurityCenter informuje o závažných i méně závažných problémech ochrany ihned, jakmile problémy zjistí. Závažné potíže ochrany vyžadují okamžitou nápravu a ohrožují stav ochrany (změna barvy stavu na červený). Méně závažné potíže ochrany nevyžadují okamžitou nápravu a podle toho, o jaký typ problému se jedná, nemusí (ale mohou) ohrozit stav ochrany. Chcete-li dosáhnout zeleného stavu ochrany, je třeba vyřešit všechny závažné potíže a všechny méně závažné potíže buď vyřešit nebo ignorovat. Potřebujete-li pro stanovení problémů ochrany nápovědu, lze spustit nástroj McAfee Virtual Technician. Další informace o nástroji McAfee Virtual Technician naleznete v nápovědě nástroje McAfee Virtual Technician.

Pokud jste zabezpečovací software nezakoupili od společnosti McAfee, ale od partnera nebo poskytovatele, otevřete webový prohlížeč a přejděte na adresu www.mcafeenapoveda.com. Poté vyberte partnera nebo poskytovatele v položce Odkazy na partnery a tím získáte přístup k nástroji McAfee Virtual Technician.

Poznámka: K instalaci a spuštění nástroje McAfee Virtual Technician musíte být k počítači přihlášení jako správce systému Windows. V opačném případě může dojít k tomu, že nástroj Virtual Technician nedokáže záležitost vyřešit. Informace o tom, jak se přihlásit jako správce systému Windows, naleznete v nápovědě systému Windows. V systému Windows Vista™ bude při spuštění nástroje Virtual Technician zobrazena výzva. Po zobrazení výzvy klepněte na tlačítko **Přijmout**. Nástroj Virtual Technician nespolupracuje s aplikací Mozilla® Firefox.

V této kapitole

Používání nástroje McAfee Virtual Technician	112
Podpora a položky ke stažení	113

Používání nástroje McAfee Virtual Technician

Nástroj Virtual Technician si lze představit jako osobního odborného zaměstnance podpory, který shromažďuje informace o programech SecurityCenter uživatele za účelem nápovědy při řešení problémů s ochranou počítače. Při spuštění nástroje Virtual Technician nástroj zkontroluje, zda programy SecurityCenter fungují správně. Zjistí-li problém, nabídne nástroj Virtual Technician možnost opravy nebo poskytne uživateli o problémech podrobnější informace. Po dokončení nástroj Virtual Technician zobrazí výsledky analýzy a v případě potřeby umožní vyhledat další technickou podporu společnosti McAfee.

Nástroj Virtual Technician za účelem udržení bezpečnosti a integrity počítače a souborů neshromažďuje osobní informace, které by mohly uživatele identifikovat.

Poznámka: Další informace o nástroji Virtual Technician získáte klepnutím na ikonu **Nápověda** v nástroji Virtual Technician.

Spuštění nástroje Virtual Technician

Nástroj Virtual Technician shromažďuje informace o programech SecurityCenter za účelem nápovědy při řešení problémů s ochranou. Abychom chránili soukromí uživatelů, neobsahuje tato informace osobní informace, které by mohly uživatele identifikovat.

- 1** V části **Běžné úkoly** klepněte na tlačítko **McAfee Virtual Technician**.
- 2** Postupujte podle pokynů na obrazovce a stáhněte a spusťte nástroj Virtual Technician.

Podpora a položky ke stažení

V následujících tabulkách naleznete informace o podpoře McAfee a serverech pro stahování, včetně uživatelských příruček pro vaši zemi.

Podpora a položky ke stažení

Stát	Podpora McAfee	Soubory McAfee ke stažení
Austrálie	www.mcafeehelp.com	au.mcafee.com/root/downloadads.asp
Brazílie	www.mcafeeajuda.com	br.mcafee.com/root/downloadads.asp
Kanada (angličtina)	www.mcafeehelp.com	ca.mcafee.com/root/downloadads.asp
Kanada (francouzština)	www.mcafeehelp.com	ca.mcafee.com/root/downloadads.asp
Čína	www.mcafeehelp.com	cn.mcafee.com/root/downloadads.asp
China (tw)	www.mcafeehelp.com	tw.mcafee.com/root/downloadads.asp
Česká republika	www.mcafeenapoveda.com	cz.mcafee.com/root/downloadads.asp
Dánsko	www.mcafeehjaelp.com	dk.mcafee.com/root/downloadads.asp
Finsko	www.mcafeehelpfinland.com	fi.mcafee.com/root/downloadads.asp
Francie	www.mcafeeaide.com	fr.mcafee.com/root/downloadads.asp
Německo	www.mcafeehilfe.com	de.mcafee.com/root/downloadads.asp
Velká Británie	www.mcafeehelp.com	uk.mcafee.com/root/downloadads.asp
Itálie	www.mcafeeaiuto.com	it.mcafee.com/root/downloadads.asp
Japonsko	www.mcafeehelp.jp	jp.mcafee.com/root/downloadads.asp
Korea	www.mcafeehelp.com	kr.mcafee.com/root/downloadads.asp
Mexiko	www.mcafeehelp.com	mx.mcafee.com/root/downloadads.asp
Norsko	www.mcafeehjelp.com	no.mcafee.com/root/downloadads.asp
Polsko	www.mcafeepomoc.com	pl.mcafee.com/root/downloadads.asp

Portugalsko	www.mcafeeajuda.com	pt.mcafee.com/root/downlo ads.asp
Španělsko	www.mcafeeayuda.com	es.mcafee.com/root/downlo ads.asp
Švédsko	www.mcafeehjalp.com	se.mcafee.com/root/downlo ads.asp
Turecko	www.mcafeehelp.com	tr.mcafee.com/root/downlo ads.asp
Spojené státy americké	www.mcafeehelp.com	us.mcafee.com/root/downlo ads.asp

Uživatelské příručky sady McAfee Total Protection

Stát	Uživatelské příručky McAfee
Austrálie	download.mcafee.com/products/manuals/en-au/MTP_userguide_20 08.pdf
Brazílie	download.mcafee.com/products/manuals/pt-br/MTP_userguide_20 08.pdf
Kanada (angličtina)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_20 08.pdf
Kanada (francouzština)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_200 8.pdf
Čína	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_20 08.pdf
Čína (Tchaj-wan)	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_20 08.pdf
Česká republika	download.mcafee.com/products/manuals/cz/MTP_userguide_2008. pdf
Dánsko	download.mcafee.com/products/manuals/dk/MTP_userguide_2008. pdf
Finsko	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.p df
Francie	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.p df
Německo	download.mcafee.com/products/manuals/de/MTP_userguide_2008. pdf
Velká Británie	download.mcafee.com/products/manuals/en-uk/MTP_userguide_20 08.pdf
Holandsko	download.mcafee.com/products/manuals/nl/MTP_userguide_2008. pdf
Itálie	download.mcafee.com/products/manuals/it/MTP_userguide_2008.p df
Japonsko	download.mcafee.com/products/manuals/ja/MTP_userguide_2008. pdf

Korea	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Mexiko	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Norsko	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
Polsko	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
Portugalsko	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
Španělsko	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Švédsko	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Turecko	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
Spojené státy americké	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

Uživatelské příručky sady McAfee Internet Security

Stát	Uživatelské příručky McAfee
Austrálie	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brazílie	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
Kanada (angličtina)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
Kanada (francouzština)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
Čína	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
Čína (Tchaj-wan)	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Česká republika	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Dánsko	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Finsko	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
Francie	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
Německo	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf

Velká Británie	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Holandsko	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
Itálie	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
Japonsko	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
Mexiko	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Norsko	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
Polsko	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
Portugalsko	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
Španělsko	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Švédsko	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Turecko	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
Spojené státy americké	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

Uživatelské příručky programu McAfee VirusScan Plus

Stát	Uživatelské příručky McAfee
Austrálie	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brazílie	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Kanada (angličtina)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
Kanada (francouzština)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
Čína	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
Čína (Tchaj-wan)	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
Česká republika	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf

Dánsko	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Finsko	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
Francie	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Německo	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Velká Británie	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Holandsko	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
Itálie	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Japonsko	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Mexiko	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Norsko	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
Polsko	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
Portugalsko	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
Španělsko	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Švédsko	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Turecko	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
Spojené státy americké	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

Uživatelské příručky programu McAfee VirusScan

Stát	Uživatelské příručky McAfee
Austrálie	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Brazílie	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
Kanada (angličtina)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf

Kanada (francouzština)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
Čína	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
Čína (Tchaj-wan)	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Česká republika	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Dánsko	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Finsko	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
Francie	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Německo	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Velká Británie	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
Holandsko	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
Itálie	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Japonsko	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Mexiko	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Norsko	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
Polsko	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
Portugalsko	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
Španělsko	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Švédsko	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Turecko	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
Spojené státy americké	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

Další informace o Centru pro hrozby společnosti McAfee a webech s informacemi o virech ve vaší zemi naleznete v následující tabulce.

Země	Centrum zabezpečení	Informace o virech
Austrálie	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brazílie	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Kanada (angličtina)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Kanada (francouzština)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Čína (tradiční čínština)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
Čína (tradiční čínština)	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Česká republika	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Dánsko	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Finsko	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
Francie	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
Německo	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Velká Británie	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
Holandsko	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
Itálie	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Japonsko	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
Korea	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
Mexiko	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Norsko	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
Polsko	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
Portugalsko	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
Španělsko	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Švédsko	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Turecko	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
Spojené státy americké	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

Další informace o webech HackerWatch ve vaší zemi naleznete v následující tabulce.

Země	HackerWatch
Austrálie	www.hackerwatch.org
Brazílie	www.hackerwatch.org/?lang=pt-br
Kanada (angličtina)	www.hackerwatch.org
Kanada (francouzština)	www.hackerwatch.org/?lang=fr-ca
Čína (tradiční čínština)	www.hackerwatch.org/?lang=zh-cn
Čína (tradiční čínština)	www.hackerwatch.org/?lang=zh-tw
Česká republika	www.hackerwatch.org/?lang=cs
Dánsko	www.hackerwatch.org/?lang=da
Finsko	www.hackerwatch.org/?lang=fi
Francie	www.hackerwatch.org/?lang=fr
Německo	www.hackerwatch.org/?lang=de
Velká Británie	www.hackerwatch.org
Holandsko	www.hackerwatch.org/?lang=nl
Itálie	www.hackerwatch.org/?lang=it
Japonsko	www.hackerwatch.org/?lang=jp
Korea	www.hackerwatch.org/?lang=ko
Mexiko	www.hackerwatch.org/?lang=es-mx
Norsko	www.hackerwatch.org/?lang=no
Polsko	www.hackerwatch.org/?lang=pl
Portugalsko	www.hackerwatch.org/?lang=pt-pt
Španělsko	www.hackerwatch.org/?lang=es
Švédsko	www.hackerwatch.org/?lang=sv
Turecko	www.hackerwatch.org/?lang=tr
Spojené státy americké	www.hackerwatch.org

Rejstřík

8

802.11	95
802.11a	95
802.11b	95
802.1x	95

A

adresa IP	95
adresa MAC	95
adresa URL	95
Aktualizace programu SecurityCenter	13
archivace	95
automaticky otevíraná okna	95

B

bezdrátový adaptér	96
bod obnovení systému	96
brána firewall	96

C

cestování	96
Copyright	109

Č

červ	96
Čištění počítače	65, 66

D

DAT	96
Defragmentace počítače	68
dialer	96
disk USB	96
DNS	96
dočasný soubor	97
domácí síť	97
doména	97

E

e-mail	97
e-mailový klient	97
ESS	97
externí pevný disk	97

F

falšování adres IP	97
--------------------------	----

filtrování obrázků	97
Funkce programu Network Manager	80
Funkce programu QuickClean	64
Funkce programu SecurityCenter	6
Funkce programu Shredder	76
Funkce programu VirusScan	30

H

heslo	97
-------------	----

I

Ignorování potíží ochrany	20
Ignorování problému ochrany	20
Informace o společnosti McAfee	109
Instalace zabezpečovacího softwaru společnosti McAfee ve vzdálených počítačích	93
integrováná brána	97
Internet	98
intranet	98

J

Jednotka smart drive	98
----------------------------	----

K

karanténa	98
karta bezdrátového adaptéru USB	98
karty bezdrátového adaptéru PCI	98
klíč zabezpečení	98
klíčové slovo	98
klient	98
knihovna	98
komprimace	98
Konfigurace automatických aktualizací	14
Konfigurace možností výstrah	24
Koš	99

L

LAN	99
Licence	110

M

mapa sítě	99
MAPI	99
McAfee Network Manager	79
McAfee QuickClean	63
McAfee SecurityCenter	5

McAfee Shredder	75
McAfee VirusScan	3, 29
modul plug-in	99
Možnosti konfigurace programu Ochrana systému	45
MSN	99

N

Naplánování úlohy defragmentace disku	71
Naplánování úlohy programu QuickClean	69
Nastavení možností prohledávání v reálném čase	38
Nastavení možností prohledávání v reálném čase – postup	38
Nastavení možností ručního prohledávání	40
Nastavení ochrany proti virům	37, 55
Nastavení spravované sítě	83
Nastavení umístění ručního prohledávání	42
NIC	99

O

O typech seznamů důvěryhodných položek	52
Obnovení mapy sítě	84
obnovit	99
odkaz	99
odmítnutí služby	99
Odstranění úlohy defragmentace disku	73
Odstranění úlohy programu QuickClean	71
Ochrana systému	99
Oprava slabých míst zabezpečení	92
organizace Wi-Fi Alliance	100
Ověření předplatného	11
ověřovací kód zpráv (MAC)	100
ověřování	100
ovládací prvek ActiveX	100

P

Plánování prohledávání	43
Plánování úloh	69
platforma U3	100
Podpora a položky ke stažení	113
podvodný server nebo zpráva (phishing)	100
POP3	100
port	100
potenciálně nežádoucí programy (PUP)	100
Použití programu SecurityCenter	7
Používání možností programu Ochrana systému	44
Používání nástroje McAfee Virtual Technician	112
Používání seznamů důvěryhodných položek	51
Povolení ochrany programu Ochrana systému	45

Pozvání počítače k připojení ke spravované síti	87
Práce s mapou sítě	84
Práce s potenciálně nežádoucími programy	60
Práce s programy a soubory cookie v karanténě	61
Práce s viry a trojskými koňmi	59
Práce s výsledky prohledávání	59
Práce s výstrahami	14, 21
Práce se soubory v karanténě	60
prohledávání na požádání	100
Prohledávání počítače	31, 55
Prohledávání počítače – postup	56
prohledávání v reálném čase	100
prohlížeč	101
prostý text	101
protokol	101
protokol PPPoE	101
proxy	101
Přehrání zvuku při zobrazení výstrahy	24
Přejmenování sítě	85
přetečení vyrovnávací paměti	101
Připojení ke spravované síti	86
Připojení spravované sítě	86
přípojný bod	101
Přístup k mapě sítě	84
Přístupový bod	101
publikovat	101

R

Reference	94
registr	101
Rodičovská kontrola	102
rychlá archivace	102

S

sdílení	102
sdílený tajný klíč	102
server	102
server DNS	102
server proxy	102
seznam důvěryhodných položek	102
seznam povolených serverů	102
seznam zakázaných serverů	102
síť	103
síťová jednotka	103
Skartace souborů a složek	77
Skartace souborů, složek a disků	77
Skartovat celý disk	78
skript	103
Skrytí úvodní obrazovky při spuštění	24
Skrytí výstrah na mimořádné rozšíření virů	25

skupiny hodnocení obsahu dle věkové kategorie uživatele	103	USB	105
sledovaná umístění	103	útok hrubou silou	106
sledované typy souborů	103	útok typu muž uprostřed	106
Sledování stavu a oprávnění	90	uzel	106
Sledování stavu ochrany počítače	90	V	
slovníkový útok	103	virus	106
Služby pro zákazníky a technická podpora ..	111	VPN	106
směrovač	103	vyrovnávací paměť	106
SMTP	103	Vyřešení nebo ignorování potíží ochrany ..	8, 17
soubor cookie	103	Vyřešení potíží ochrany	8, 18
Součásti programu Ochrana systému	46, 47	Vyřešení potíží ochrany automaticky	18
součásti souborů	103	Vyřešení potíží ochrany ručně	19
Spouštění další ochrany	33	Vysvětlení ikon programu Network Manager	81
Spouštění ochrany proti virům v reálném čase	31	Vysvětlení kategorií ochrany	7, 9, 27
Správa seznamů důvěryhodných položek	51	Vysvětlení služeb ochrany	10
Správa účtu McAfee	11	Vysvětlení stavu ochrany	7, 8, 9
Správa účtu McAfee – postup	11	Vzdálená správa sítě	89
Správa zařízení	91	W	
správcovská sada	104	wardriver	106
spravovaná síť	104	Webmail	106
Spuštění nástroje Virtual Technician	112	Webové štěnice	106
Spuštění ochrany e-mailů	34	WEP	107
Spuštění ochrany proti spywaru	34	Wi-Fi	107
Spuštění ochrany proti virům v reálném čase	31	Wi-Fi Certified	107
Spuštění ochrany rychlých zpráv	35	WLAN	107
Spuštění ochrany prohlédávání skriptů	34	WPA	107
SSID	104	WPA2	107
SSL	104	WPA2-PSK	107
standardní e-mailový účet	104	WPA-PSK	107
Synchronizace	104	Z	
systém launchpad	104	zabezpečení RADIUS	107
Š		Zakázání automatických aktualizací	14
šifrování	104	zálohování	108
šířka pásma	104	Zastavení důvěřování počítačům v síti	88
škodlivý přístupový bod	104	Zastavení ochrany proti virům v reálném čase	31
T		Zastavení sledování stavu ochrany počítače ..	90
TKIP	105	zašifrovaný text	108
Trezor hesel	105	Zjišťování aktualizací	13, 14
Trojský kůň	105	Zobrazení a skrytí ignorovaných potíží	20
U		Zobrazení a skrytí informačních výstrah při hraní her	23
událost	105	Zobrazení a skrytí položky na mapě sítě	85
úložiště zálohování online	105	Zobrazení nebo skrytí informačních výstrah – postup	22
umístění s hloubkovým sledováním	105	Zobrazení nedávných událostí	27
umístění s omezeným sledováním	105	Zobrazení podrobností o položce	85
úplná archivace	105	Zobrazení událostí	18, 27
Úprava oprávnění spravovaného počítače	91	Zobrazení všech událostí	27
Úprava úlohy defragmentace disku	72	Zobrazení výsledků prohlédávání	56
Úprava úlohy programu QuickClean	70		
Úprava vlastností zobrazení zařízení	91		

Zobrazování a skrytí informačních výstrah...22