McAfee®

Internet Security

Uživatelská příručka

Obsah

KAPITOLA 1

McAfee Internet Security

Sada Internet Security představuje domácí systém zabezpečení počítače, který chrání vás i vaši rodinu před nejnovějšími hrozbami a činí online připojení mnohem bezpečnější. Sada Internet Security chrání počítač před viry, hackery a spywarem, sleduje podezřelé aktivity v internetovém provozu, chrání soukromí vaší rodiny, hodnotí rizikové webové stránky a mnoho dalšího.

V této kapitole

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

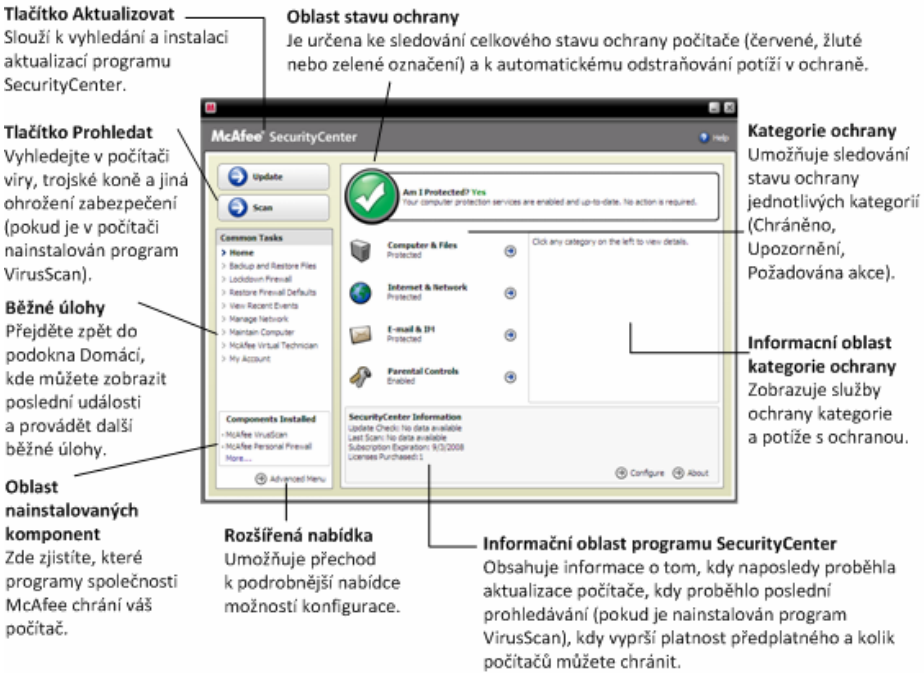
Funkce programu SecurityCenter

Zjednodušený stav ochrany	Slouží ke snadné kontrole stavu zabezpečení počítače, zjišťování aktualizací a odstraňování potíží se zabezpečením.
Automatické aktualizace a inovace	Program SecurityCenter stahuje a instaluje aktualizace programů automaticky. Jakmile je k dispozici nová verze programu McAfee, je do počítače v průběhu platnosti předplatného automaticky doručena zdarma. Vždy budete mít zajištěnou aktuální ochranu.
Výstrahy v reálném čase	O mimořádných rozšířeních virů a hrozbách zabezpečení budete informováni pomocí výstrah zabezpečení.

KAPITOLA 3

Použití programu SecurityCenter

S komponenty a konfiguračními oblastmi programu SecurityCenter, které budete používat ke správě stavu zabezpečení počítače, se seznamte dříve, než začnete program používat. Další informace o terminologii, která 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

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	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. 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 Vyřešení potíží ochrany (stránka 18).
Žlutý	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. 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 Vyřešení nebo ignorování potíží ochrany (stránka 17).
Zelený	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. Každá kategorie ochrany vypisuje seznam služeb, které chrání počítač.

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: ▪ Ochrana proti virům ▪ Ochrana proti spywaru ▪ SystemGuards ▪ Ochrana systému Windows ▪ Stav PC
Internet a sítě	V kategorii Internet a sítě lze nakonfigurovat následující služby ochrany: ▪ Ochrana brány firewall ▪ Ochrana před podvodnými zprávami (phishing) ▪ Ochrana identity
E-mail a rychlé zprávy	V kategorii E-mail a rychlé zprávy lze nakonfigurovat následující služby ochrany: ▪ Ochrana před e-mailovými viry ▪ Ochrana proti virům v rychlých zprávách ▪ Ochrana proti spywaru v e-mailových zprávách ▪ Ochrana proti spywaru v rychlých zprávách ▪ Ochrana proti spamu
Rodičovská kontrola	V kategorii Rodičovská kontrola lze nakonfigurovat následující služby ochrany: ▪ Blokování obsahu

Vysvětlení služeb ochrany

Služby ochrany jsou tvořeny různými komponenty zabezpečení, které lze za účelem ochrany počítače a souborů nakonfigurovat. Služby ochrany přímo odpovídají programům McAfee. Pokud například nainstalujete program VirusScan, budou k dispozici následující služby ochrany: Ochrana proti virům, ochrana proti spywaru, ochrana systému (program SystemGuards) a prohledávání skriptů. 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 rodičovskou kontrolu, 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 předplatného

Součástí každého zakoupeného produktu ochrany McAfee je předplatné, které umožňuje produkt používat v určitém množství počítačů po určité období. V závislosti na zakoupeném předplatném se jeho délka liší, obvykle ale začíná aktivací produktu. Aktivace je jednoduchá a bezplatná, potřebujete jedině připojení k Internetu. Na druhou stranu je ale velice důležitá, protože uživatele opravňuje k získávání pravidelných automatických aktualizací produktů, které zajišťují stálou ochranu počítače před nejnovějšími hrozbami.

K aktivaci obvykle dojde při instalaci produktu. Pokud se ale rozhodnete počkat (pokud například nemáte připojení k Internetu), máte na aktivaci 15 dnů. Pokud produkty neaktivujete do 15 dnů, nebudou již produkty získávat životně důležité aktualizace nebo provádět prohledávání. Před vypršením předplatného vás budeme pravidelně upozorňovat pomocí zpráv na obrazovce. Přerušením ochrany se lze vyhnout tím, že produkt obnovíte včas nebo nastavíte na našem webu automatické obnovování.

Jestliže je v programu SecurityCenter zobrazen odkaz s výzvou k aktivaci, nebylo předplatné aktivováno. Datum vypršení předplatného naleznete na stránce účtu.

Přístup k účtu McAfee

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

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

Aktivace produktu

K aktivaci obvykle dojde při instalaci produktu. Pokud k aktivaci nedošlo, bude v programu SecurityCenter zobrazen odkaz s výzvou k aktivaci. Také vás budeme pravidelně upozorňovat.

- V podokně Domácí programu SecurityCenter v části **Informace programu SecurityCenter** klepněte na možnost **Aktivujte své předplatné**.

Tip: Aktivaci můžete také provést z pravidelně zobrazované výstrahy.

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**.

Obnovení předplatného

Krátce před vypršením předplatného bude v programu SecurityCenter zobrazen odkaz s výzvou k obnovení. O blížícím se vypršení vás budeme také pravidelně upozorňovat pomocí výstrah.

- V podokně Domácí programu SecurityCenter v části **Informace programu SecurityCenter** klepněte na tlačítko **Obnovit**.

Tip: Produkt lze také obnovit z pravidelně zobrazované oznamovací zprávy. Také můžete přejít na svou stránku účet a provést obnovení nebo nastavit automatické obnovení zde.

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 aktivovaných programech mohou aktualizace online zahrnovat nejnovější definice virů a aktualizace ochrany proti hackerům, spamu, 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: Pokud jste produkt McAfee nainstalovali z disku CD, je třeba do 15 dnů provést aktivaci, nebo nebudou produkty získávat životně důležité aktualizace a provádět prohledávání.

V této kapitole

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**.

3. V potvrzovacím dialogovém okně klepněte na tlačítko **Ano**.

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

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 aktivován a nemůže získat plnou ochranu.	Aktivujte program na webu McAfee.
Vaše předplatné vypršelo.	Zjistěte na webu McAfee stav svého účtu. Další informace najdete v tématu Správa předplatného (stránka 10).

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 spamu nebo rodičovská kontrola). 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

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 spouštění 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**.

Skrytí 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.

Skrytí hlášení o zabezpečení

Bezpečnostní oznámení o ochraně více počítačů v domácí síti lze skrýt. Tyto zprávy poskytují informace o předplatném, počtu počítačů, které lze pomocí předplatného chránit, a o způsobu rozšíření předplatného na ochranu ještě více počítačů.

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 **Zobrazit informační zprávy o virech nebo další hlášení o zabezpečení**.

Tip: Tato hlášení o zabezpečení lze kdykoliv zaškrtnutím políčka **Zobrazit informační zprávy o virech nebo další hlášení o 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 blokovaném 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 událostí 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

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.

KAPITOLA 8

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

Komplexní ochrana proti virům	Chraňte sebe i svůj počítač 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	Pokud chcete, můžete určit vlastní možnosti prohledávání. Počítač ale zůstává chráněný i v případě, že je nenastavíte. 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.
Automatické opravy	Jestliže program VirusScan zjistí ohrožení zabezpečení v průběhu spuštěného 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 (například ruční prohledávání) pozastavuje tehdy, jestliže uživatel provádí jakékoliv aktivity, které zaberou celou obrazovku počítače, jako je sledování filmů nebo hraní počítačových her.

KAPITOLA 9

Prohledávání počítače

Dokonce i před prvním spuštěním programu SecurityCenter začne ochrana proti virům v reálném čase programu VirusScan chránit počítač proti potencionálně 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 naleznete v tématu Nastavení ochrany proti virům (stránka 47).

Pro ochranu proti virům nabízí program VirusScan podrobnější sadu možností prohledávání a umožňuje pravidelné spouštění komplexnějších prohledávání. Z programu SecurityCenter lze spustit úplné, rychlé, vlastní nebo naplánované prohledávání. 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 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 potencionálně 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

Program VirusScan nabízí na ochranu proti virům úplnou sadu možností prohledávání, mezi které patří prohledávání v reálném čase (neustálé sledování počítače a zjišťování aktivit souvisejících s hrozbami), ruční prohledávání z Průzkumníku Windows a úplné, rychlé, vlastní nebo naplánované prohledávání z programu SecurityCenter.

Akce	Postup
Spuštění prohledávání v reálném čase s cílem zajistit stálé sledování aktivit virů v počítači, při každém přístupu k souborům (počítačem nebo uživatelem) soubory prohledávat.	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 proti virům** klepněte na **Zapnout**. **Poznámka:** Prohledávání v reálném čase je ve výchozím nastavením zapnuto.
Spuštění rychlého prohledávání s cílem rychle zkontrolovat hrozby v počítači	1. Klepněte v základní nabídce na položku **Prohledávat**. 2. Klepněte v podokně Možnosti prohledávání v části Rychlé prohledávání na možnost **Spustit**.
Spuštění úplného prohledávání s cílem důkladně zkontrolovat hrozby v počítači	1. Klepněte v základní nabídce na položku **Prohledávat**. 2. Klepněte v podokně Možnosti prohledávání v části úplné prohledávání na možnost **Spustit**.

Akce	Postup
Spuštění vlastního prohledávání s uživatelským nastavením	1. Klepněte v základní nabídce na položku **Prohledávat**. 2. Klepněte v podokně Možnosti prohledávání v části Vybere uživatel na možnost **Spustit**. 3. Přizpůsobte prohledávání zaškrtnutím nebo zrušením zaškrtnutí těchto možností: **Všechna ohrožení ve všech souborech** **Neznámé viry** **Soubory archivů** **Spyware a potencionální ohrožení** **Sledovací soubory cookie** **Utajené programy** 4. Klepněte na tlačítko **Spustit**.
Spuštění ručního prohledávání s cílem zkontrolovat hrozby v souborech, složkách nebo jednotkách	1. Spusťte program Průzkumník Windows. 2. Klepněte na soubor, složku nebo jednotku pravým tlačítkem myši a poté klepněte na příkaz **Prohledávat**.

Akce	Postup
Spuštění naplánovaného prohledávání s cílem pravidelně kontrolovat hrozby v počítači	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 naplánované 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**.

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. Také zde můžete pracovat s nakaženými položkami.

Poznámka: Další informace o možnostech prohledávání naleznete v tématu Typy prohledávání (stránka 40).

Zobrazení výsledků prohledávání

Zobrazení výsledků prohledávání po dokončení 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 potencionálně 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 výstraze 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	1. Poklepejte na ikonu **Prohledávání bylo dokončeno** v oznamovací oblasti hlavního panelu. 2. Klepněte na možnost **Podrobnosti** v podoknech Plné prohledávání, Rychlé prohledávání, Vlastní prohledávání nebo Ruční prohledávání.
Zobrazení podrobností o posledním prohledávání	Poklepejte na ikonu **Prohledávání bylo dokončeno** v oznamovací oblasti hlavního panelu a zobrazte podrobnosti posledního prohledávání v části Vaše prohledávání v podoknech Plné prohledávání, Rychlé prohledávání, Vlastní prohledávání nebo Ruční prohledávání.

KAPITOLA 10

Práce s výsledky prohledávání

Jestliže program VirusScan zjistí ohrožení zabezpečení v průběhu spuštěného 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. Program VirusScan vždy umístí soubor před začátkem čištění do karantény. Pokud soubor není čistý, je přesunutý 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 potencionálně 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

Pokud program VirusScan zjistí v souboru v počítači virus nebo trojského koně, pokusí se soubor vyčistit. Pokud soubor nelze vyčistit, pokusí se program VirusScan soubor přesunout do karantény. Pokud se nezdaří ani 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 39).

Práce s potencionálně nežádoucími programy

Pokud program VirusScan zjistí v počítači potencionálně nežádoucí program, můžete program odebrat nebo programu důvěřovat. Pokud tento program neznáte, doporučujeme zvážit odebrání programu. Tím, že potencionálně 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 **Potencionálně nežádoucí programy**.

3 Vyberte potencionálně 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 potencionálně 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.

Typy prohledávání

Program VirusScan nabízí na ochranu proti virům úplnou sadu možností prohledávání, mezi které patří prohledávání v reálném čase (neustálé sledování počítače a zjišťování aktivit souvisejících s hrozbami), ruční prohledávání z Průzkumníku Windows a možnost spustit z programu SecurityCenter úplné, rychlé nebo vlastní prohledávání nebo nastavit vlastní dobu spuštění naplánovaných prohledávání. Výhodou prohledávání v programu SecurityCenter je možnost průběžně měnit možnosti prohledávání.

Prohledávání v reálném čase:

Ochrana proti virům v reálném čase nepřetržitě sleduje počítač, zjišťuje aktivity virů a při každém přístupu k souborům (uživatelem nebo počítačem) soubory prohledává. Chcete-li zajistit stálou ochranu počítače proti nejnovějším bezpečnostním hrozbám, ponechte ochranu v reálném čase zapnutou a naplánujte spouštění pravidelných a komplexnějších ručních prohledávání.

Lze nastavit výchozí možnosti prohledávání v reálném čase, mezi které patří vyhledávání neznámých virů a kontrola hrozeb ve sledovacích souborech cookie a síťových jednotkách. Můžete také využít výhody ochrany před přetečením vyrovnávací paměti, která je povolena ve výchozím nastavení (s výjimkou u 64bitového operačního systému Windows Vista). Další informace najdete v tématu Nastavení možností prohledávání v reálném čase (stránka 48).

Rychlé prohledávání

Rychlé prohledávání slouží ke kontrole aktivit souvisejících s hrozbami v procesech, důležitých souborech systému Windows a dalších citlivých oblastech počítače.

úplné prohledávání

úplné prohledávání slouží k důkladné kontrole celého počítače na přítomnost virů, spywaru a dalších hrozeb zabezpečení kdekoliv v počítači.

Vlastní prohledávání

V rámci vlastního prohledávání lze vybrat pro kontrolu aktivit souvisejících s hrozbami v počítači vlastní nastavení prohledávání. Mezi možnosti vlastního prohledávání patří, kromě vyhledávání neznámých virů, spywaru a utajených programů, také kontrola hrozeb ve všech souborech, souborech archivů a ve sledovacích souborech cookie.

Lze nastavit výchozí možnosti vlastních prohledávání, mezi které patří vyhledávání neznámých virů, spywaru, potencionálních hrozeb, sledovacích souborů cookie a utajených programů a také prohledávání souborů archivů. Můžete také prohledávat s minimálními nároky na počítač. Další informace najdete v tématu Nastavení možností vlastního prohledávání (stránka 50).

Ruční prohledávání

Ruční prohledávání slouží k rychlé kontrole hrozeb v souborech, složkách a jednotkách z Průzkumníku Windows v průběhu práce.

Naplánované prohledávání

Naplánovaná prohledávání kterýkoliv den a hodinu v týdnu důkladně zkontrolují počítač na přítomnost virů a dalších hrozeb. Naplánovaná prohledávání vždy zkontrolují 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. Další informace najdete v tématu Plánování prohledávání (stránka 52).

Poznámka: Informace o tom, jak spustit tu nejlepší možnost prohledávání pro vás, najdete v tématu Prohledávání počítače – postup (stránka 32).

KAPITOLA 11

Použití další ochrany

Ochranu proti virům v reálném čase programu VirusScan doplňuje pokročilá ochrana proti skriptům, spywaru a ochrana proti potencionálně 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 potencionálně škodlivé skripty a zabraňuje tomu, aby byly tyto skripty spuštěny v počítači nebo webovém prohlížeči. 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 potencionálně 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 odesílaných přílohách.

Ochrana rychlých zpráv

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

V této kapitole

Spuštění prohledávání skriptů

Chcete-li zjišťovat potencionálně 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 potencionálně 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 potencionálně nežádoucím programům.

Spuštění ochrany e-mailů

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

1 Otevřete konfigurační podokno E-maily 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-maily 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-maily 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-maily 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 12

Nastavení ochrany proti virům

Pro naplánované a vlastní prohledávání a prohledávání v reálném čase 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.

Pomocí programu Ochrana systému a seznamů důvěryhodných položek můžete také rozhodnout, jakým požadovaným způsobem má program VirusScan sledovat a spravovat potencionálně neoprávněné a nevyžádané změny v počítači. 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. S použitím seznamů důvěryhodných položek můžete rozhodnout, zda chcete důvěřovat nebo odebrat pravidla, která zjišťují změny souborů nebo registru (program Ochrana systému), programy nebo přetečení vyrovnávací paměti. 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.

V této kapitole

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	Vyberte možnost **Hledat neznámé viry**.
Zjišťování souborů cookie	Vyberte možnost **Prohledat a odstranit sledovací soubory cookie**.
Zjištění virů a dalších potencionálních hrozeb na jednotkách připojených k síti	Vyberte možnost **Prohledat síťové jednotky**.
Ochrana počítače proti přetečení vyrovnávací paměti	Vyberte možnost **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**.

Zastavení ochrany proti virům v reálném čase

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.

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 **Ochrana proti virům** klepněte na možnost **Vypnout**.

3 Vyberte v dialogovém okně čas, kdy bude prohledávání v reálném čase pokračovat.

4 Klepněte na tlačítko **OK**.

Nastavení vlastních možností prohledávání

Vlastní ochrana proti virům umožňuje prohledávat soubory na požádání. Program VirusScan kontroluje při spuštění vlastního prohledávání počítač na přítomnost virů a dalších potencionálně škodlivých položek pomocí komplexnější sady možností prohledávání. Chcete-li možnosti vlastního 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, potencionálně nežádoucí programy jako je spyware, adware, utajené programy a 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 vlastního prohledávání všechny jednotky a složky počítače a všechny síťové jednotky; výchozí umístění však můžete změnit a přizpůsobit vašim potřebám. Můžete například prohledávat pouze důležité soubory počítače, položky pracovní plochy nebo položky ve složce Program Files. Pokud nechcete být odpovědni za inicializaci každého vlastního 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 vlastního prohledávání) pozastavuje tehdy, jestliže uživatel provádí jakékoliv aktivity, které zaberou celou obrazovku počítače, jako je sledování filmů nebo hraní počítačových her.

Nastavení možností vlastního prohledávání

Nastavení možností vlastního prohledávání slouží k přizpůsobení cílů vlastního prohledávání programu VirusScan a k nastavení umístění a typů prohledávaných souborů. Mezi možnosti patří zjišťování neznámých virů, archivních souborů, spywaru a potencionálně nežádoucích programů, sledovacích souborů cookie, správcovských sad a utajených programů. Nastavením umístění vlastního prohledávání lze také určit, kde bude v průběhu vlastního prohledávání program VirusScan hledat 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 Vlastní 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 vlastního prohledávání a poté klepněte na tlačítko **OK**.

Akce	Postup
Zjištění neznámých virů a nových variant virů známých	Vyberte možnost **Hledat neznámé viry**.
Zjištění a odstranění virů v souborech ZIP a dalších komprimovaných souborech	Vyberte možnost **Prohledávat komprimované soubory**.
Zjištění spywaru, adwaru a dalších potencionálně nežádoucích programů	Vyberte možnost **Hledat spyware a potenciální ohrožení**.
Zjišťování souborů cookie	Vyberte možnost **Prohledat a odstranit sledovací soubory cookie**.
Zjišťování správcovských sad a utajených programů, které mohou pozměnit a zneužít stávající systémové soubory systému Windows.	Vyberte možnost **Hledat utajené programy**.

Akce	Postup
Menší nároky na výkon procesoru při prohledávání a zároveň přiřazení vyšší priority jiným úlohám, jako je procházení sítě Internet nebo otevírání dokumentů	Vyberte možnost **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**.

3 Klepněte na možnost **Výchozí prohledávané umístění** a poté vyberte nebo zrušte výběr umístění, která byste chtěli prohledat nebo přeskočit, a klepněte na tlačítko **OK**:

Akce	Postup
Prohledávání všech souborů a složek v počítači	Vyberte možnost **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**.

Naplánování 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.

Naplánovaná prohledávání vždy pomocí výchozích možností prohledávání důkladně zkontrolují celý počítač na přítomnost virů a dalších hrozeb. Výchozím intervalem prohledávání programu VirusScan je jednou za týden.

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 naplánované 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 potencionálně 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 potencionálně 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 spouštění 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 potencionálně nežádoucí programy, které mohou být automaticky spuštěny při spuštění systému Windows.

Ochrana systému Windows

Ochrana systému Windows také zjišťuje potencionálně neoprávněné změny v registru počítače a dalších důležitých souborech, které jsou pro systém Windows klíčové. Mezi tyto důležité položky registru a soubory patří obsluhy 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 potencionálně 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 potencionálně 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 57).

Součásti programu Ochrana systému

Součásti programu Ochrana systému zjišťují potencionálně 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 potencionálně 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 potencionálně 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 potencionálně 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.

Ochrana systému	Zjišťuje...
Knihovny Applnit DLL	Neoprávněné změny knihoven AppInit_DLL v registru, které mohou umožnit spuštění potencionálně škodlivých souborů při spuštění počítače.
Soubor hostitelů systému Windows	Spyware, adware a potencionálně 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 potencionálně 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 potencionálně 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 potencionálně 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 potencionálně 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 potencionálně nežádoucí programy, které mohou provést změny v registru a souborech pro Plánovač sdílených úloh a umožnit spuštění potencionálně nebezpečných souborů při spuštění počítače.
Služba Windows Messenger	Spyware, adware a další potencionálně 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 potencionálně 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 možností prohlížeče bez vědomí uživatele a nežádoucí důvěřování podezřelým webům.

Ochrana systému	Zjišťuje...
Objekty BHO (Browser Helper Object)	Spyware, adware a další potencionálně nežádoucí programy, které mohou využívat objektů BHO (browser helper objects) za účelem sledování procházení Internetu a zobrazování nevyžádané reklamy.
Panely 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 potencionálně 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 potencionálně 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 potencionálně 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 potencionálně 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 potencionálně nežádoucí programy, které mohou provést změny v registru pro zóny zabezpečení aplikace Internet Explorer a umožnit spuštění potencionálně nebezpečných souborů při spuštění počítače.
Důvěryhodné servery aplikace Internet Explorer	Spyware, adware a další potencionálně nežádoucí programy, které mohou v registru změnit důvěryhodné servery aplikace Internet Explorer a umožnit tak, aby prohlížeč důvěřoval podezřelým webovým serverům.

Ochrana systému	Zjišťuje...
Zásady ochrany osobních údajů v aplikaci Internet Explorer	Spyware, adware a další potencionálně 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 61).

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	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. Ochrana systému zjišťuje neoprávněné změny registru a souborů související s instalacemi ovládacích prvků ActiveX, položkami Po spuštění, moduly přiřazení spouštění 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.

Možnost	Popis
Ochrana systému Windows	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. Ochrana systému Windows zjišťuje neoprávněné změny registru a souborů související s obsluhami místních nabídek, knihovnami 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.
Ochrana prohlížeče	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. 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.
Důvěryhodné programy	Důvěryhodné programy jsou potencionálně nežádoucí programy, které program VirusScan zjistil dříve, ale které uživatel označil z výstrahy nebo pomocí podokna Výsledky prohledávání za důvěryhodné.
Povolené přetečení vyrovnávací paměti	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. 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.

KAPITOLA 13

McAfee Personal Firewall

Program Personal Firewall obsahuje rozšířenou ochranu počítače a osobních dat. Program Personal Firewall vytváří bariéru mezi počítačem a Internetem a skrytě v internetovém provozu vyhledává podezřelé aktivity.

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 Personal Firewall

Standardní a vlastní úrovně ochrany	Pomocí výchozích nebo vlastních nastavení ochrany brány firewall se můžete chránit proti vniknutí a podezřelým aktivitám.
Doporučení v reálném čase	Pomocí této možnosti můžete dynamicky přijímat doporučení, které vám pomohou se rozhodnout, zda je vhodné programům povolit přístup k Internetu nebo zda je vhodné důvěřovat určitému síťovému provozu.
Inteligentní správa přístupu pro programy	Umožňuje správu přístupu programů k Internetu prostřednictvím výstrah a protokolů událostí nebo konfiguraci oprávnění k přístupu pro určité programy.
Ochrana herního prostředí	Zabraňuje tomu, aby výstrahy ohledně pokusů o průnik a podezřelých aktivit vyrušovaly uživatele v průběhu hry v režimu celé obrazovky.
Ochrana při spouštění počítače	Chraňte počítač ihned po spuštění systému Windows® proti pokusům o neoprávněné vniknutí, nežádoucím programům a síťovému provozu.
Ovládání portů systémových služeb	Správa otevřených a uzavřených portů systémových služeb, které vyžadují některé programy.
Správa připojení počítače	Povolení a zakázání vzdálených připojení ostatních počítačů k vašemu.
Integrace informací serveru HackerWatch	Sledování globálních vzorků napadání a neoprávněných vniknutí prostřednictvím serveru HackerWatch, který také poskytuje informace o zabezpečení programů v počítači a stejně tak globální události zabezpečení a statistiku internetového portu.
Brána firewall s funkcí Uzamčení	Tato funkce okamžitě zablokuje veškerý příchozí a odchozí internetový provoz mezi počítačem a Internetem.
Obnovení brány firewall	Okamžitě obnoví původní nastavení ochrany u brány firewall.
Rozšířená detekce trojských koní	Zjištění a blokování potenciálně nebezpečných aplikací, například trojských koní, před přístupem k Internetu a odesíláním vašich osobních dat.
Protokolování událostí	Sleduje nedávná příchozí a odchozí neoprávněná vniknutí.
Sledování internetového provozu	Umožňuje prohlížet grafické mapy celého světa, na nichž je zobrazen zdroj nepřátelských útoků a provozu. Dále můžete nalézt podrobné informace o vlastníkovi zdrojové adresy IP a související zeměpisné údaje. Můžete také analyzovat příchozí a odchozí provoz, sledovat šířku pásma nebo činnost programů.
Prevence vniknutí	Chrání vaše soukromí před možnými internetovými hrozbami. Pomocí funkcí založených na heuristické analýze poskytujeme třetí vrstvu ochrany tím, že jsou blokovány položky vykazující charakteristiky útoku nebo pokusu o průnik do počítače.
Složitější analýzy provozu	Umožňují prohlížení příchozího i odchozího internetového provozu a připojení programů včetně těch, které aktivně naslouchají otevřeným připojením. Díky tomu lze rozpoznat programy, které se mohou stát cílem vniknutí, a adekvátně reagovat.

KAPITOLA 14

Spuštění brány firewall

Jakmile bránu firewall nainstalujete, bude počítač chráněn před neoprávněným vniknutím a nežádoucím síťovým provozem. Můžete také zpracovávat výstrahy a spravovat příchozí a odchozí internetová připojení známých a neznámých programů. Funkce Inteligentní doporučení a úroveň automatického zabezpečení (s možností volby povolení programů s pouze odchozím připojením k Internetu) jsou automaticky povoleny.

Ochranu bránou firewall lze v podokně Konfigurace sítě Internet zakázat, počítač však již nebude chráněn před neoprávněným vniknutím a nežádoucím síťovým provozem a nebude možné efektivně spravovat příchozí a odchozí internetová připojení. Musíte-li ochranu bránou firewall zakázat, zakažte ji dočasně a jen v nutných případech. Bránu firewall lze povolit také v panelu Konfigurace Internetu a sítě.

Brána firewall automaticky zakáže bránu Windows® Firewall a nastaví se jako výchozí brána firewall.

Poznámka: Chcete-li nastavit bránu Firewall, otevřete podokno Konfigurace Internetu a sítě.

V této kapitole

Spuštění ochrany bránou firewall

Povolením brány firewall ochráníte počítač před průniky a nežádoucím síťovým provozem. Pomocí brány firewall lze také spravovat příchozí a odchozí připojení k Internetu.

1. V podokně programu McAfee SecurityCenter klepněte na položku **Internet a síť** a potom klepněte na volbu **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je zakázána** klepněte na možnost **Zapnuto**.

Zakázání ochrany bránou firewall

Nechcete-li počítač chránit před pokusy o neoprávněné vniknutí a nežádoucím síťovým provozem, bránu firewall můžete zakázat. Bez ochrany brány firewall nelze spravovat příchozí a odchozí internetová připojení.

1. V podokně programu McAfee SecurityCenter klepněte na položku **Internet a síť** a potom klepněte na volbu **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na možnost **Vypnuto**.

KAPITOLA 15

Práce s výstrahami

K usnadnění správy zabezpečení používá brána firewall sadu výstrah. Tyto výstrahy je možné rozdělit na tři základní typy:

- Červená výstraha
- Žlutá výstraha
- Zelená výstraha

Výstrahy mohou také obsahovat informace, které uživateli usnadní rozhodnutí, jak s výstrahami zacházet nebo jak získat informace o programech spuštěných v počítači.

V této kapitole

Výstrahy

Brána firewall obsahuje tři základní typy výstrah. Některé výstrahy také obsahují informace, pomocí kterých se dozvíte o programech spuštěných v počítači nebo o nich získáte informace.

Červená výstraha

Červená výstraha upozorňující na trojského koně se zobrazí, pokud brána firewall v počítači zjistí a zablokuje trojského koně, a doporučí prohledat počítač kvůli dalším ohrožením. Trojský kůň se jeví jako legitimní program, ale může rušit, poškozovat nebo poskytnout neoprávněný přístup k počítači. Tato výstraha se zobrazí ve všech úrovních zabezpečení.

Žlutá výstraha

Většina obvyklých výstrah je žlutého typu. Informují o činnosti programu nebo síťové události zjištěné bránou firewall. Nastane-li tento stav, výstraha nejdříve popisuje příslušnou aktivitu programu nebo síťovou událost a následuje několik možností, na které musíte reagovat. Po připojení počítače s nainstalovanou bránou firewall do nové sítě se například zobrazí výstraha **Nové připojení sítě**. Můžete určit úroveň důvěry, kterou této nové síti přiřadíte. Tato síť se poté objeví v seznamu sítí. Pokud jsou povolena inteligentní doporučení, jsou známé programy přidány do podokna Oprávnění programů automaticky.

Zelená výstraha

Zelená výstraha většinou poskytuje základní informace o události a nevyžaduje odpověď. Zelené výstrahy jsou ve výchozím nastavení zakázány.

Pomoc uživateli

Mnoho výstrah brány firewall obsahuje další informace usnadňující správu zabezpečení počítače, které zahrnují následující informace:

- **Další informace o tomto programu**: Chcete-li získat informace o programu, který brána firewall v počítači zjistila, navštivte globální web zabezpečení společnosti McAfee.
- **Informovat společnost McAfee o tomto programu**: Odešle společnosti McAfee informace o neznámém souboru, který brána firewall v počítači zjistila.
- **Společnost McAfee doporučuje**: Rada o zpracování výstrah. Výstraha může například doporučit, abyste programu udělili přístup.

KAPITOLA 16

Správa informačních výstrah

Brána firewall umožňuje zobrazit nebo skrýt výstrahy, jestliže detekuje pokusy o průnik a podezřelé aktivity během určitých událostí, např. v režimu celé obrazovky.

V této kapitole

Zobrazení výstrah při hraní her

Bránu firewall můžete nechat zobrazovat informační výstrahy při zjištění pokusu o průnik nebo podezřelé aktivity při hraní her v režimu celé obrazovky.

1. V podokně McAfee SecurityCenter klepněte na položku **Rozšířená nabídka**.
2. Klepněte na tlačítko **Konfigurovat**.
3. V podokně McAfee SecurityCenter klepněte v části **Výstrahy** na položku **Upřesnit**.
4. V podokně Možnosti výstrah zvolte nastavení **Zobrazit informační výstrahy, pokud je zjištěn herní režim**.
5. Klepněte na tlačítko **OK**.

Skrytí informačních výstrah

Zobrazení výstrah brány firewall při zjištění pokusu o průnik nebo podezřelé aktivity můžete zabránit.

1. V podokně McAfee SecurityCenter klepněte na položku **Rozšířená nabídka**.
2. Klepněte na tlačítko **Konfigurovat**.
3. V podokně McAfee SecurityCenter klepněte v části **Výstrahy** na položku **Upřesnit**.
4. V podokně Konfigurace programu SecurityCenter klepněte na položku **Výstrahy**.
5. V podokně Informační výstrahy proveďte jednu z následujících akcí:
   - Zaškrtnutím políčka **Skrýt informační výstrahy** skryjete všechny informační výstrahy.
   - Zrušte zaškrtnutí výstrahy, kterou chcete skrýt.
6. Klepněte na tlačítko **OK**.

KAPITOLA 17

Konfigurace ochrany bránou firewall

Brána firewall poskytuje několik způsobů správy zabezpečení a přizpůsobení požadované reakce na události a výstrahy zabezpečení.

Jestliže instalujete bránu firewall poprvé, úroveň ochrany zabezpečení je nastavena na Automaticky a programům je povoleno pouze odchozí připojení k Internetu. Brána firewall však poskytuje další úrovně, od vysoce omezujících až po vysoce tolerantní.

Brána firewall také poskytuje možnost zobrazení doporučení výstrah a přístupu programů k Internetu.

V této kapitole

Správa úrovní zabezpečení bránou firewall

úroveň zabezpečení lze nastavit podle toho, do jaké míry chcete spravovat a reagovat na výstrahy. Tyto výstrahy budou zobrazeny, zjistí-li brána firewall nežádoucí síťový provoz nebo příchozí a odchozí internetová připojení. Ve výchozím nastavení je zabezpečení bránou firewall nastaveno na úroveň Automaticky a povolen je pouze odchozí přístup k Internetu.

Je-li nastavena úroveň zabezpečení Automaticky a jsou-li povolena inteligentní doporučení, poskytuje žlutá výstraha možnost povolení nebo blokování přístupu neznámým programům, které vyžadují příchozí přístup k Internetu. I když jsou ve výchozím nastavení zelené výstrahy zakázány, zobrazí se v případě, že se jedná o známé programy a přístup je povolen automaticky. Po povolení přístupu mohou programy vytvářet odchozí připojení a přijímat nevyžádaná příchozí připojení.

Obecně platí, že čím více je úroveň zabezpečení omezující (např. úroveň Utajené nebo Standardní), tím větší je množství možností a výstrah, které jsou zobrazovány a které musíte zpracovat.

Následující tabulka popisuje tři úrovně zabezpečení bránou firewall – od nejvíce omezujících k nejméně omezujícím:

úroveň	Popis
Utajené	Brána firewall blokuje všechna příchozí síťová připojení, zároveň zcela skrývá přítomnost tohoto počítače v Internetu. Brána firewall zobrazí výzvu, jakmile se nové programy pokusí o odchozí internetová připojení nebo obdrží požadavky na příchozí připojení. Blokované a přidané programy se zobrazí v podokně Oprávnění programů.
Standardní	Brána firewall sleduje příchozí a odchozí připojení a zobrazí výzvu, jakmile se nové programy pokusí o přístup. Blokované a přidané programy se zobrazí v podokně Oprávnění programů.
Automaticky	Tato úroveň zajišťuje programům buď příchozí i odchozí připojení (plné), nebo pouze odchozí připojení k Internetu. Standardní úrovní zabezpečení je úroveň Automaticky, s možností pouze odchozího připojení programů k Internetu. Má-li program nastaven plný přístup k Internetu, brána firewall programu automaticky důvěřuje a přidá jej do seznamu povolených programů v podokně Oprávnění programů. Je-li programu povoleno pouze odchozí připojení k Internetu, brána firewall programu automaticky důvěřuje pouze pro navázání odchozího připojení. Příchozí připojení k Internetu je automaticky považováno za nedůvěryhodné.

V podokně Obnovit výchozí nastavení brány firewall lze také okamžitě nastavit znovu aktuální úroveň zabezpečení na Automaticky (a udělit pouze odchozí přístup k Internetu).

Nastavení zabezpečení na úroveň Utajené

Nastavíte-li zabezpečení bránou firewall na úroveň Utajené, budou blokována všechna příchozí síťová připojení kromě otevřených portů, čímž se skryje přítomnost počítače v Internetu.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně úroveň zabezpečení nastavte posuvník tak, aby se úroveň **Utajené** zobrazila jako aktuální.
4. Klepněte na tlačítko **OK**.

Poznámka: V režimu Utajené zobrazí brána firewall při žádosti nových programů o odchozí připojení k Internetu nebo o přijetí příchozího připojení výstrahu.

Nastavení zabezpečení na úroveň Standardní

Nastavíte-li zabezpečení brány firewall na úroveň Standardní, bude brána firewall sledovat příchozí a odchozí připojení a zobrazí výstrahu, pokud se nový program pokusí o přístup k Internetu.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně Úroveň zabezpečení nastavte posuvník tak, aby se úroveň **Standardní** zobrazila jako aktuální.
4. Klepněte na tlačítko **OK**.

Nastavení zabezpečení na úroveň Automaticky

Nastavíte-li zabezpečení bránou firewall na úroveň Automaticky, bude povolen úplný přístup nebo pouze odchozí přístup k síti.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně úroveň zabezpečení nastavte posuvník tak, aby se úroveň **Automaticky** zobrazila jako aktuální.
4. Proveďte jednu z následujících akcí:
   - Chcete-li povolit příchozí a odchozí přístup k síti, vyberte možnost **Povolit úplný přístup**.
   - Chcete-li povolit pouze odchozí přístup k síti, vyberte možnost **Povolit pouze odchozí přístup**.
5. Klepněte na tlačítko **OK**.

Poznámka: Možnost **Povolit pouze odchozí přístup** je nastavena jako výchozí.

Konfigurace inteligentních doporučení pro výstrahy

Bránu firewall můžete nakonfigurovat tak, aby zahrnovala, vylučovala nebo zobrazovala doporučení výstrah při pokusu libovolného programu o přístup k Internetu. Povolení inteligentních doporučení umožňuje rozhodovat o zpracování výstrah.

Jsou-li použita inteligentní doporučení (a je nastavena úroveň zabezpečení Automaticky s povolením pouze odchozího přístupu), brána automaticky povoluje známé programy a blokuje potencionálně nebezpečné programy.

Nejsou-li inteligentní doporučení použita, brána firewall nepovoluje ani neblokuje přístup k Internetu a neposkytuje ve výstraze doporučení.

Jsou-li inteligentní doporučení nastavena na režim Zobrazit, zobrazí se výzva k povolení nebo blokování přístupu a brána firewall ve výstraze poskytuje doporučení.

Povolení inteligentních doporučení

Povolíte-li inteligentní doporučení, bude brána firewall automaticky povolovat a blokovat programy a zobrazí upozornění na neznámé a potencionálně nebezpečné programy.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně úroveň zabezpečení vyberte v části **Inteligentní doporučení** možnost **Použít funkci Inteligentní doporučení**.
4. Klepněte na tlačítko **OK**.

Zákaz inteligentních doporučení

Zakážete-li inteligentní doporučení, bude brána firewall povolovat a blokovat programy a zobrazí upozornění na neznámé nebo potencionálně nebezpečné programy. Výstrahy však nebudou obsahovat doporučení týkající se udělování přístupu programům. Zjistí-li brána firewall nový program, který je podezřelý nebo známý jako možné ohrožení, zabrání mu automaticky v přístupu k Internetu.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně úroveň zabezpečení vyberte v části **Inteligentní doporučení** možnost **Nepoužívat funkci Inteligentní doporučení**.
4. Klepněte na tlačítko **OK**.

Zobrazení inteligentních doporučení

Nastavíte-li zobrazení inteligentních doporučení ve výstraze pouze jako doporučení, budete moci rozhodnout, zda chcete povolit nebo blokovat neznámé a potencionálně nebezpečné programy.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně úroveň zabezpečení v části **Inteligentní doporučení** vyberte možnost **Zobrazit funkci Inteligentní doporučení**.
4. Klepněte na tlačítko **OK**.

Optimalizace zabezpečení bránou firewall

Existuje mnoho způsobů, jak může být zabezpečení počítače ohroženo. Některé programy se například pokouší o připojení k Internetu během spouštění systému Windows®. Zkušenější uživatelé mohou také trasováním počítače (nebo odesláním příkazu ping) určit, zda je počítač připojen k síti. Také mohou do vašeho počítače pomocí protokolu UDP odeslat informace ve formě jednotek zpráv (datagramů). Proti těmto druhům vniknutí chrání počítač brána firewall; umožňuje blokovat přístup programů k Internetu v průběhu spouštění systému Windows, blokovat požadavky na příkaz ping, který jiným uživatelům slouží ke zjištění vašeho počítače v síti, a zakázat jiným uživatelům odeslat do vašeho počítače informace ve formě jednotek zpráv (datagramů).

Standardní nastavení instalace zahrnuje automatické zjišťování většiny nejběžnějších pokusů o vniknutí, jako jsou například zneužití nebo útoky pomocí pokusu o odmítnutí služby. Použití standardních nastavení instalace zajistí, že budete chráněni před těmito útoky a prohledáváními. Automatické zjišťování však můžete pro jeden nebo více útoků zakázat v podokně Zjišťování vniknutí.

Ochrana počítače při spouštění

Při spouštění systému Windows lze počítač ochránit blokováním nových programů, které vyžadují přístup k Internetu během spouštění, i když jej dříve neměly. Brána firewall zobrazuje výstrahy týkající se programů, které požadovaly během spouštění přístup k Internetu. Můžete jim udělit přístup nebo je zablokovat.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně úroveň zabezpečení v části **Nastavení zabezpečení** vyberte možnost **Povolit ochranu během spouštění systému Windows**.
4. Klepněte na tlačítko **OK**.

Poznámka: Pokud je povolena ochrana při spouštění, nejsou protokolována zablokovaná připojení a vniknutí.

Konfigurace nastavení požadavku ping

Lze povolit nebo zabránit zjištění přítomnosti počítače v síti ostatními uživateli.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně Úroveň zabezpečení v části **Nastavení zabezpečení** proveďte jednu z následujících akcí:
   - Chcete-li umožnit detekci počítače v síti pomocí požadavků ping, vyberte možnost **Povolit požadavky ping ICMP**.
   - Chcete-li zabránit detekci tohoto počítače v síti pomocí požadavků ping, zakažte možnost **Povolit požadavky ping ICMP**.
4. Klepněte na tlačítko **OK**.

Konfigurace nastavení protokolu UDP

Můžete povolit odesílání jednotek zpráv (datagramů) pomocí protokolu UDP z jiných síťových počítačů do svého počítače. Tuto akci ale můžete provést pouze tehdy, pokud jste také zavřeli port systémové služby s cílem tento protokol blokovat.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně úroveň zabezpečení v části **Nastavení zabezpečení** proveďte jednu z následujících akcí:
   - Zaškrtnutím možnosti **Povolit sledování portu UDP** povolíte odesílání jednotek zpráv (datagramů) od jiných uživatelů do svého počítače.
   - Zrušíte-li zaškrtnutí možnosti **Povolit sledování portu UDP**, zabráníte jiným uživatelům odesílat do svého počítače jednotky zpráv (datagramy).
4. Klepněte na tlačítko **OK**.

Konfigurace detekce vniknutí

Zjišťováním pokusů o vniknutí lze počítač chránit před útoky a neoprávněným prohledáváním. Standardní nastavení brány firewall zaručuje zjištění většiny nejobvyklejších pokusů o vniknutí, jako jsou například zneužití nebo útoky pomocí pokusu o odmítnutí služby. Automatické zjišťování však můžete pro některé útoky nebo prohledávání zakázat.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně Brána firewall klepněte na položku **Zjišťování vniknutí**.
4. V podokně **Zjišťovat pokusy o vniknutí** proveďte jednu z následujících akcí:
   - Chcete-li automaticky zjistit útok nebo prohledávání, zaškrtněte políčko s jeho názvem
   - Chcete-li automatickou detekci útoku nebo prohledávání zakázat, zaškrtnutí políčka zrušte.
5. Klepněte na tlačítko **OK**.

Konfigurace možností stavu ochrany bránou firewall

Bránu firewall lze nastavit tak, aby určité problémy v počítači nebyly hlášeny programu SecurityCenter.

1. V podokně McAfee SecurityCenter v části **Informace programu SecurityCenter** klepněte na tlačítko **Konfigurovat**.
2. V podokně Konfigurace programu SecurityCenter v části **Stav ochrany** klepněte na položku **Upřesnit**.
3. V podokně Ignorované problémy vyberte jednu z následujících možností:
   - **Ochrana brány firewall je zakázána.**
   - **Služba brány firewall není spuštěna.**
   - **Brána firewall není v počítači nainstalována.**
   - **Brána firewall systému Windows je zakázána.**
   - **Brána firewall pro odchozí komunikaci není v počítači nainstalována.**
4. Klepněte na tlačítko **OK**.

Uzamčení a obnovení brány firewall

Uzamčení ihned blokuje všechna příchozí a odchozí síťová připojení včetně přístupu k webovým serverům, e-mailu a aktualizacím zabezpečení. Uzamčení se projevuje stejně, jako byste odpojili síťové kabely počítače. Pomocí tohoto nastavení lze zablokovat otevřené porty v podokně Systémové služby. Slouží také k izolování a řešení potíží v počítači.

Okamžité uzamčení brány firewall

Uzamčením brány firewall lze okamžitě zablokovat všechny síťové přenosy mezi počítačem a libovolnou sítí, včetně sítě Internet.

1. V podokně McAfee SecurityCenter v části **Běžné úkoly** klepněte na položku **Uzamčení brány firewall**.
2. V podokně Uzamčení brány firewall klepněte na tlačítko **Povolit uzamčení brány firewall**.
3. Operaci potvrďte klepnutím na tlačítko **Ano**.

Tip: Bránu firewall lze uzamknout také klepnutím pravým tlačítkem na ikonu programu SecurityCenter v oznamovací oblasti v pravé části hlavního panelu, klepnutím na položky **Rychlé odkazy** a poté na **Uzamknout bránu firewall**.

Okamžité odemknutí brány firewall

Odemknutím brány firewall lze okamžitě povolit všechny síťové přenosy mezi počítačem a libovolnou sítí, včetně sítě Internet.

1. V podokně McAfee SecurityCenter v části **Běžné úkoly** klepněte na položku **Uzamčení brány firewall**.
2. V podokně Uzamčení povoleno klepněte na tlačítko **Zakázat uzamčení brány firewall**.
3. Operaci potvrďte klepnutím na tlačítko **Ano**.

Obnovení nastavení brány firewall

Bránu firewall lze rychle obnovit do původního nastavení ochrany. Obnovením dojde k nastavení zabezpečení zpět na úroveň Automaticky, povolení pouze odchozího přístupu k síti, povolení inteligentních doporučení, obnovení seznamu výchozích programů a jejich oprávnění v podokně Oprávnění programů, odebrání důvěryhodných a zakázaných adres IP a obnovení systémových služeb, nastavení protokolu událostí a zjišťování vniknutí.

1. V podokně McAfee SecurityCenter klepněte na tlačítko **Obnovit výchozí nastavení brány firewall**.
2. V podokně Obnovení výchozího nastavení ochrany brány firewall klepněte na tlačítko **Obnovit výchozí nastavení**.
3. Operaci potvrďte klepnutím na tlačítko **Ano**.
4. Klepněte na tlačítko **OK**.

KAPITOLA 18

Správa programů a oprávnění

Brána firewall umožňuje spravovat a vytvářet oprávnění přístupu existujících a nových programů, které požadují příchozí a odchozí přístup k Internetu. Brána firewall umožňuje udělit programům úplný přístup nebo pouze odchozí přístup. Programům je také možné zablokovat přístup.

V této kapitole

Povolení přístupu programů k Internetu

Některé programy (například prohlížeče Internetu) potřebují ke správnému fungování přístup k Internetu.

Brána firewall umožňuje pomocí stránky Oprávnění programů:

- Povolit programům přístup
- Povolit programům pouze odchozí přístup
- Zablokovat programům přístup

Programům můžete povolit úplný přístup a pouze odchozí přístup také pomocí protokolu Odchozí události a Nedávné události.

Povolení úplného přístupu programu

Dříve blokovanému programu v počítači lze udělit úplný příchozí a odchozí přístup k Internetu.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně Brána firewall klepněte na položku **Oprávnění programů**.
4. V části **Oprávnění programů** vyberte program, který má nastavenu možnost **Blokováno** nebo **Pouze odchozí přístup**.
5. V části **Akce** klepněte na možnost **Povolit přístup**.
6. Klepněte na tlačítko **OK**.

Povolení úplného přístupu nového programu

Novému programu v počítači lze udělit úplný příchozí a odchozí přístup k Internetu.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně Brána firewall klepněte na položku **Oprávnění programů**.
4. V části **Oprávnění programů** klepněte na možnost **Přidat povolený program**.
5. V dialogovém okně **Přidání programu** najděte a označte program, který chcete přidat, a klepněte na tlačítko **Otevřít**.

Poznámka: Oprávnění nového programu můžete změnit stejně jako u existujícího programu jeho vybráním a klepnutím na možnost **Povolit pouze odchozí přístup** nebo **Blokovat přístup** v části **Akce**.

Povolení úplného přístupu z protokolu Nedávné události

Blokovanému programu v počítači uvedenému v protokolu Nedávné události lze povolit úplný příchozí a odchozí přístup k Internetu.

1. V podokně McAfee SecurityCenter klepněte na položku **Rozšířená nabídka**.
2. Klepněte na položku **Zprávy a protokoly**.
3. V části **Nedávné události** vyberte popis události a klepněte na tlačítko **Povolit přístup**.
4. V dialogovém okně Oprávnění programu potvrďte operaci klepnutím na tlačítko **Ano**.

Příbuzná témata

- Zobrazení odchozích událostí (stránka 105)

Povolení úplného přístupu z protokolu Odchozí události

Blokovanému programu v počítači uvedenému v protokolu Odchozí události lze povolit úplný příchozí a odchozí přístup k Internetu.

1. V podokně McAfee SecurityCenter klepněte na položku **Rozšířená nabídka**.
2. Klepněte na položku **Zprávy a protokoly**.
3. V části **Nedávné události** klepněte na položku **Zobrazit protokol**.
4. Klepněte na položku **Internet a síť** a na položku **Odchozí události**.
5. Vyberte program a v části **Požadovaná akce** klepněte na položku **Povolit přístup**.
6. V dialogovém okně Oprávnění programu potvrďte operaci klepnutím na tlačítko **Ano**.

Povolení pouze odchozího přístupu programů

Některé programy v počítači vyžadují odchozí přístup k Internetu. Brána firewall umožňuje nastavit oprávnění programu na povolení pouze odchozího přístupu k Internetu.

Povolení pouze odchozího přístupu programu

Programu lze povolit pouze odchozí přístup k Internetu.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně Brána firewall klepněte na položku **Oprávnění programů**.
4. V části **Oprávnění programů** vyberte program, který má nastavenu možnost **Blokováno** nebo **Úplný přístup**.
5. V části **Akce** klepněte na možnost **Povolit pouze odchozí přístup**.
6. Klepněte na tlačítko **OK**.

Povolení pouze odchozího přístupu z protokolu Nedávné události

Blokovanému programu v počítači uvedenému v protokolu Nedávné události lze povolit pouze odchozí přístup k Internetu.

1. V podokně McAfee SecurityCenter klepněte na položku **Rozšířená nabídka**.
2. Klepněte na položku **Zprávy a protokoly**.
3. V části **Nedávné události** vyberte popis události a klepněte na tlačítko **Povolit pouze odchozí přístup**.
4. V dialogovém okně Oprávnění programu potvrďte operaci klepnutím na tlačítko **Ano**.

Povolení pouze odchozího přístupu z protokolu Odchozí události

Blokovanému programu v počítači uvedenému v protokolu Odchozí události lze povolit pouze odchozí přístup k Internetu.

1. V podokně McAfee SecurityCenter klepněte na položku **Rozšířená nabídka**.
2. Klepněte na položku **Zprávy a protokoly**.
3. V části **Nedávné události** klepněte na položku **Zobrazit protokol**.
4. Klepněte na položku **Internet a síť** a na položku **Odchozí události**.
5. Vyberte program a v části **Požadovaná akce** klepněte na položku **Povolit pouze odchozí přístup**.
6. V dialogovém okně Oprávnění programu potvrďte operaci klepnutím na tlačítko **Ano**.

Blokování přístupu programů k Internetu

Brána firewall umožňuje zablokovat programům přístup k Internetu. Zkontrolujte, zda zablokování programu nepřeruší připojení k síti ani připojení jiného programu, který požaduje ke správnému fungování přístup k Internetu.

Blokování přístupu programu

Programu lze zablokovat příchozí a odchozí přístup k Internetu.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně Brána firewall klepněte na položku **Oprávnění programů**.
4. V části **Oprávnění programů** vyberte program, který má nastavenu možnost **Úplný přístup** nebo **Pouze odchozí přístup**.
5. V části **Akce** klepněte na možnost **Blokovat přístup**.
6. Klepněte na tlačítko **OK**.

Blokování přístupu nového programu

Novému programu lze zablokovat příchozí a odchozí přístup k Internetu.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně Brána firewall klepněte na položku **Oprávnění programů**.
4. V modulu **Oprávnění programů** klepněte na možnost **Přidat blokovaný program**.
5. V dialogovém okně Přidání programu najděte a označte program, který chcete přidat, a klepněte na tlačítko **Otevřít**.

Poznámka: Oprávnění nového programu můžete změnit jeho vybráním a klepnutím na možnost **Povolit pouze odchozí přístup** nebo **Blokovat přístup** v části **Akce**.

Blokování přístupu z protokolu Nedávné události

Programu uvedenému v protokolu Nedávné události lze zablokovat příchozí a odchozí přístup k Internetu.

1. V podokně McAfee SecurityCenter klepněte na položku **Rozšířená nabídka**.
2. Klepněte na položku **Zprávy a protokoly**.
3. V části **Nedávné události** vyberte popis události a klepněte na tlačítko **Blokovat přístup**.
4. V dialogovém okně Oprávnění programu potvrďte operaci klepnutím na tlačítko **Ano**.

Odebrání přístupových oprávnění programů

Než programu odeberete oprávnění, zkontrolujte, zda odebrání neovlivní funkčnost počítače nebo připojení k síti.

Odebrání oprávnění programu

Programu lze odebrat oprávnění k příchozímu a odchozímu přístupu k Internetu.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně Brána firewall klepněte na položku **Oprávnění programů**.
4. V části **Oprávnění programů** vyberte program.
5. V části **Akce** klepněte na možnost **Odebrat oprávnění programu**.
6. Klepněte na tlačítko **OK**.

Poznámka: Brána firewall zabraňuje změnám některých programů jejich ztemněním a znepřístupněním některých akcí.

Získání informací o programech

Pokud si nejste jisti, která oprávnění programů použít, můžete informace o programu získat na webovém serveru HackerWatch společnosti McAfee.

Získání informací o programu

Z webového serveru HackerWatch společnosti McAfee lze získat informace o programu, které vám pomohou při rozhodování, zda programu povolit či zakázat příchozí a odchozí přístup k síti.

Poznámka: Zkontrolujte, zda jste připojeni k Internetu, aby prohlížeč mohl zobrazit webový server HackerWatch společnosti McAfee, který poskytuje nejnovější informace o programech, požadavcích na připojení k Internetu a ohrožení zabezpečení.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně Brána firewall klepněte na položku **Oprávnění programů**.
4. V části **Oprávnění programů** vyberte program.
5. V části **Akce** klepněte na možnost **Další informace**.

Získání informací o programu z protokolu Odchozí události

Z protokolu Odchozí události lze získat informace o programu z webového serveru HackerWatch společnosti McAfee, které vám pomohou při rozhodování, zda programu povolit či zakázat příchozí a odchozí přístup k síti.

Poznámka: Zkontrolujte, zda jste připojeni k Internetu, aby prohlížeč mohl zobrazit webový server HackerWatch společnosti McAfee, který poskytuje nejnovější informace o programech, požadavcích na připojení k Internetu a ohrožení zabezpečení.

1. V podokně McAfee SecurityCenter klepněte na položku **Rozšířená nabídka**.
2. Klepněte na položku **Zprávy a protokoly**.
3. V části Nedávné události vyberte událost a klepněte na položku **Zobrazit protokol**.
4. Klepněte na položku **Internet a síť** a na položku **Odchozí události**.
5. Vyberte adresu IP a klepněte na tlačítko **Další informace**.

KAPITOLA 19

Správa připojení počítače

V bráně firewall je možné nakonfigurovat správu určitých vzdálených připojení k tomuto počítači vytvořením pravidel, založených na adresách IP přidružených ke vzdálenému počítači. Počítače přidružené k důvěryhodným adresám IP jsou považovány za důvěryhodné a mohou se připojit k tomuto počítači. Počítačům s neznámou, podezřelou nebo nedůvěryhodnou adresou IP může být připojení k tomuto počítači zakázáno.

Když povolujete připojení, ujistěte se, zda je důvěryhodný počítač bezpečný. Pokud je počítač, který pokládáte za důvěryhodný, napaden červem nebo jiným mechanizmem, může být i váš počítač vystaven riziku šíření virů. Společnost McAfee také doporučuje, aby byl počítač, který pokládáte za důvěryhodný, chráněn bránou firewall a aktuálním antivirovým programem. Pro důvěryhodné adresy IP uvedené v seznamu **Sítě** brána firewall nezaznamenává provoz do protokolu a negeneruje výstrahy pro události.

Počítačům, které jsou přidružené k neznámým, podezřelým nebo nedůvěryhodným adresám IP, můžete zakázat připojení k vašemu počítači.

Protože brána firewall blokuje veškerý nevyžádaný provoz, není obvykle nutné zakazovat adresy IP. Adresu IP je třeba zakázat pouze v případě, když jste si jisti, že internetové připojení představuje hrozbu. Ujistěte se, zda nejsou blokovány důležité adresy IP, například server DNS nebo DHCP či jiné servery poskytovatele služeb Internetu.

V této kapitole

Připojení počítače

Připojení počítače jsou představována připojeními, která vytvoříte mezi dalšími počítači v síti a vaším počítačem. Adresy IP v seznamu **Sítě** můžete přidat, upravit nebo odebrat. Tyto adresy IP jsou přiřazeny k sítím, pro které při připojení ke svému počítači potřebujete přiřadit úroveň důvěry (Důvěryhodná, Standardní a Veřejná).

úroveň	Popis
Důvěryhodná	Brána firewall umožňuje komunikaci síťového provozu s počítačem přes libovolný port. Aktivita mezi počítači přidruženými k důvěryhodné adrese IP a tímto počítačem není branou firewall filtrována ani analyzována. Ve výchozím nastavení je v seznamu **Sítě** uvedena jako Důvěryhodná první soukromá síť nalezená bránou firewall. Důvěryhodnou sítí může být například počítač nebo počítače v místní nebo domácí síti.
Standardní	Brána firewall řídí provoz z IP adres (ne však z jiného počítače v síti) při připojení IP adresy k počítači; provoz povoluje nebo blokuje na základě pravidel obsažených v seznamu **Systémové služby**. Brána firewall protokoluje síťový provoz a generuje výstrahy na události ze seznamu standardních adres IP. Standardní sítí může být například počítač nebo počítače v podnikové síti.
Veřejná	Brána firewall řídí provoz z veřejné sítě na základě pravidel obsažených v seznamu **Systémové služby**. Veřejnou sítí je například internetová síť v kavárně, hotelu nebo na letišti.

Když povolujete připojení, ujistěte se, zda je důvěryhodný počítač bezpečný. Pokud je počítač, který pokládáte za důvěryhodný, napaden červem nebo jiným mechanizmem, může být i váš počítač vystaven riziku šíření virů. Společnost McAfee také doporučuje, aby byl počítač, který pokládáte za důvěryhodný, chráněn bránou firewall a aktuálním antivirovým programem.

Přidání připojení počítače

Můžete přidat důvěryhodné, standardní nebo veřejné připojení počítače a k němu přidruženou adresu IP.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně Brána firewall klepněte na tlačítko **Sítě**.
4. V podokně Sítě klepněte na položku **Přidat**.

5 Pokud je připojení počítače v síti s protokolem IPv6, zaškrtněte políčko **IPv6**.

6 V části **Přidat pravidlo** proveďte jednu z následujících akcí:

- Vyberte možnost **Jediná** a pak do pole **Adresa IP** zadejte adresu IP.
- Vyberte možnost **Rozsah** a poté do polí **Od adresy IP** a **Do adresy IP** zadejte počáteční a koncovou adresu IP. Pokud je připojení počítače v síti s protokolem IPv6, zadejte do polí **Od adresy IP** a **Délka předpony** počáteční adresu IP a délku předpony.

7 V části **Typ** proveďte jednu z následujících akcí:

- Výběrem možnosti **Důvěryhodná** označíte toto připojení počítače jako důvěryhodné (například počítač v domácí síti).
- Výběrem možnosti **Standardní** označíte toto připojení počítače (ne však jiné počítače v jeho síti) jako důvěryhodné (například počítač v podnikové síti).
- Výběrem možnosti **Veřejná** označíte toto připojení počítače jako veřejné (například počítač v internetové kavárně, v hotelu nebo na letišti).

8 Pokud systémová služba používá službu Sdílení připojení k Internetu (ICS), můžete přidat následující rozsah adres IP: 192.168.0.1 až 192.168.0.255.

9 Volitelně můžete vybrat možnost **Konec platnosti pravidla** a zadat počet dnů platnosti pravidla.

10 Volitelně můžete zadat popis pravidla.

11 Klepněte na tlačítko **OK**.

Poznámka: Další informace o službě Sdílení připojení k Internetu (ICS) naleznete v části Konfigurace nové systémové služby.

Přidání počítače z protokolu Příchozí události

Z protokolu Příchozí události můžete přidat důvěryhodné nebo standardní připojení počítače a jeho přidružené adresy IP.

1. V podokně McAfee SecurityCenter v části Běžné úkoly klepněte na položku **Rozšířená nabídka**.
2. Klepněte na položku **Zprávy a protokoly**.
3. V části **Nedávné události** klepněte na položku **Zobrazit protokol**.
4. Klepněte na položku **Internet a síť** a na položku **Příchozí události**.
5. Vyberte zdrojovou adresu IP a v části **Požadovaná akce** proveďte jednu z následujících akcí:
   - Klepnutím na možnost **Přidat tuto adresu IP jako důvěryhodnou** tento počítač přidáte do seznamu **Sítě** jako důvěryhodný.
   - Klepnutím na možnost **Přidat tuto adresu IP jako standardní** toto počítačové připojení přidáte do seznamu **Sítě** jako standardní.
6. Operaci potvrďte klepnutím na tlačítko **Ano**.

úprava připojení počítače

Důvěryhodné, standardní nebo veřejné připojení počítače a k němu přidruženou adresu IP můžete upravit.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně Brána firewall klepněte na tlačítko **Sítě**.
4. Vyberte v podokně Sítě adresu IP a klepněte na tlačítko **Upravit**.
5. Pokud je připojení počítače v síti s protokolem IPv6, zaškrtněte políčko **IPv6**.
6. V části **Upravit pravidlo** proveďte jednu z následujících akcí:
   - Vyberte možnost **Jediná** a pak do pole **Adresa IP** zadejte adresu IP.
   - Vyberte možnost **Rozsah** a poté do polí **Od adresy IP** a **Do adresy IP** zadejte počáteční a koncovou adresu IP. Pokud je připojení počítače v síti s protokolem IPv6, zadejte do polí **Od adresy IP** a **Délka předpony** počáteční adresu IP a délku předpony.

7 V části **Typ** proveďte jednu z následujících akcí:

- Výběrem možnosti **Důvěryhodná** označíte toto připojení počítače jako důvěryhodné (například počítač v domácí síti).
- Výběrem možnosti **Standardní** označíte toto připojení počítače (ne však jiné počítače v jeho síti) jako důvěryhodné (například počítač v podnikové síti).
- Výběrem možnosti **Veřejná** označíte toto připojení počítače jako veřejné (například počítač v internetové kavárně, v hotelu nebo na letišti).

8 Volitelně můžete zaškrtnout možnost **Konec platnosti pravidla** a zadat počet dnů platnosti pravidla.

9 Volitelně můžete zadat popis pravidla.

10 Klepněte na tlačítko **OK**.

Poznámka: Výchozí připojení počítače automaticky přidané bránou firewall z důvěryhodné soukromé sítě nelze upravit.

Odebrání připojení počítače

Můžete odebrat důvěryhodné, standardní nebo veřejné připojení počítače a k němu přidruženou adresu IP.

1 V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.

2 V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.

3 V podokně Brána firewall klepněte na tlačítko **Sítě**.

4 Vyberte v podokně Sítě adresu IP a klepněte na tlačítko **Odebrat**.

5 Operaci potvrďte klepnutím na tlačítko **Ano**.

Zákaz připojení počítače

Zakázané adresy IP v seznamu Zakázané adresy IP můžete přidat, upravit nebo odebrat.

Počítačům, které jsou přidružené k neznámým, podezřelým nebo nedůvěryhodným adresám IP, můžete zakázat připojení k vašemu počítači.

Protože brána firewall blokuje veškerý nevyžádaný provoz, není obvykle nutné zakazovat adresy IP. Adresu IP je třeba zakázat pouze v případě, když jste si jisti, že internetové připojení představuje hrozbu. Ujistěte se, zda nejsou blokovány důležité adresy IP, například server DNS nebo DHCP či jiné servery poskytovatele služeb Internetu.

Přidání připojení zakázaného počítače

Můžete přidat připojení zakázaného počítače a přidruženou adresu IP.

Poznámka: Ověřte, zda nejsou blokovány důležité adresy IP, například server DNS nebo DHCP či jiné servery poskytovatele služeb Internetu.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně Brána firewall klepněte na položku **Zakázané adresy IP**.
4. V podokně Zakázané adresy IP klepněte na položku **Přidat**.
5. Pokud je připojení počítače v síti s protokolem IPv6, zaškrtněte políčko **IPv6**.
6. V části **Přidat pravidlo** proveďte jednu z následujících akcí:
   - Vyberte možnost **Jediná** a pak do pole **Adresa IP** zadejte adresu IP.
   - Vyberte možnost **Rozsah** a poté do polí **Od adresy IP** a **Do adresy IP** zadejte počáteční a koncovou adresu IP. Pokud je připojení počítače v síti s protokolem IPv6, zadejte do polí **Od adresy IP** a **Délka předpony** počáteční adresu IP a délku předpony.
7. Volitelně můžete vybrat možnost **Konec platnosti pravidla** a zadat počet dnů platnosti pravidla.
8. Volitelně můžete zadat popis pravidla.
9. Klepněte na tlačítko **OK**.
10. Operaci potvrďte klepnutím na tlačítko **Ano**.

úprava připojení zakázaného počítače

Můžete upravit připojení zakázaného počítače a přidruženou adresu IP.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně Brána firewall klepněte na položku **Zakázané adresy IP**.
4. V podokně Zakázané adresy IP klepněte na položku **Upravit**.
5. Pokud je připojení počítače v síti s protokolem IPv6, zaškrtněte políčko **IPv6**.
6. V části **Upravit pravidlo** proveďte jednu z následujících akcí:
   - Vyberte možnost **Jediná** a pak do pole **Adresa IP** zadejte adresu IP.
   - Vyberte možnost **Rozsah** a poté do polí **Od adresy IP** a **Do adresy IP** zadejte počáteční a koncovou adresu IP. Pokud je připojení počítače v síti s protokolem IPv6, zadejte do polí **Od adresy IP** a **Délka předpony** počáteční adresu IP a délku předpony.
7. Volitelně můžete vybrat možnost **Konec platnosti pravidla** a zadat počet dnů platnosti pravidla.
8. Volitelně můžete zadat popis pravidla.
9. Klepněte na tlačítko **OK**.

Odebrání připojení zakázaného počítače

Můžete odebrat připojení zakázaného počítače a přidruženou adresu IP.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně Brána firewall klepněte na položku **Zakázané adresy IP**.
4. Vyberte adresu IP v podokně Zakázané adresy IP a klepněte na tlačítko **Odebrat**.
5. Operaci potvrďte klepnutím na tlačítko **Ano**.

Zakázání počítače z protokolu Příchozí události

Z protokolu Příchozí události můžete zakázat připojení počítače a jeho přidružené adresy IP. Adresu IP, o níž se domníváte, že je zdrojem podezřelé nebo nežádoucí internetové aktivity, můžete zakázat pomocí tohoto protokolu, který obsahuje všechny adresy IP příchozího internetového provozu.

Pokud chcete blokovat veškerý příchozí internetový provoz z určité adresy IP bez ohledu na to, zda jsou porty systémových služeb otevřené nebo zavřené, přidejte tuto adresu do seznamu **Zakázané adresy IP**.

1. V podokně McAfee SecurityCenter v části **Běžné úkoly** klepněte na položku **Rozšířená nabídka**.
2. Klepněte na položku **Zprávy a protokoly**.
3. V části **Nedávné události** klepněte na položku **Zobrazit protokol**.
4. Klepněte na položku **Internet a síť** a na položku **Příchozí události**.
5. Vyberte zdrojovou adresu IP a v části **Požadovaná akce** klepněte na položku **Zakázat tuto adresu IP**.
6. Operaci potvrďte klepnutím na tlačítko **Ano**.

Zákaz počítače z protokolu Události zjišťování neoprávněných vniknutí

Z protokolu Události zjišťování neoprávněných vniknutí můžete zakázat připojení počítače a jeho přidružené adresy IP.

1. V podokně McAfee SecurityCenter v části **Běžné úkoly** klepněte na položku **Rozšířená nabídka**.
2. Klepněte na položku **Zprávy a protokoly**.
3. V části **Nedávné události** klepněte na položku **Zobrazit protokol**.
4. Klepněte na položku **Internet a síť** a na položku **Události zjišťování neoprávněných vniknutí (IDS)**.
5. Vyberte zdrojovou adresu IP a v části **Požadovaná akce** klepněte na položku **Zakázat tuto adresu IP**.
6. Operaci potvrďte klepnutím na tlačítko **Ano**.

KAPITOLA 20

Správa systémových služeb

Aby některé programy (včetně webových serverů a serverů pro sdílení souborů) pracovaly správně, musí prostřednictvím vyhrazených portů systémových služeb přijímat nevyžádaná připojení z jiných počítačů. Brána firewall zpravidla tyto porty systémových služeb uzavře, protože představují nejpravděpodobnější zdroj nebezpečí v systému. Aby bylo možné přijímat připojení od vzdálených počítačů, musí však být tyto porty systémových služeb otevřeny.

V této kapitole

Konfigurace portů systémových služeb

Nastavením portů systémových služeb lze povolit nebo zakázat vzdálený síťový přístup ke službě v počítači. Pro počítače, které jsou v seznamu **Sítě** uvedeny jako důvěryhodné, standardní nebo veřejné, mohou být tyto porty systémových služeb otevřené nebo zavřené.

V následujícím seznamu jsou uvedeny běžné systémové služby a přidružené porty:

- Běžný port operačního systému 5357
- Protokol FTP (File Transfer Protocol), porty 20-21
- Poštovní server (IMAP), port 143
- Poštovní server (POP3), port 110
- Poštovní server (SMTP), port 25
- Server MSFT DS (Microsoft Directory Server), port 445
- Server MSFT SQL (Microsoft SQL Server), port 1433
- Protokol NTP (Network Time Protocol), port 123
- Protokol RDP (Vzdálená plocha, Vzdálená pomoc a Terminálový server), port 3389
- Server RPC (Vzdálené volání procedur), port 135
- Zabezpečený webový server (HTTPS), port 443
- Server UPNP (Universal Plug and Play), port 5000
- Webový server (HTTP), port 80
- Rozhraní NETBIOS (Sdílení souborů systému Windows), porty 137-139

Nastavením portů systémových služeb lze povolit sdílení připojení počítače k Internetu s dalšími počítači, které se nachází ve stejné síti. Toto připojení, známé jako služba Sdílení připojení k Internetu (ICS), umožňuje počítači, který připojení sdílí, fungovat jako brána pro přístup k Internetu pro ostatní počítače.

Poznámka: Je-li v počítači nainstalována aplikace, která přijímá připojení k webovému serveru nebo serveru FTP, může být potřeba v počítačích, které připojení sdílejí, otevřít příslušný port systémové služby a povolit přesměrování příchozího připojení pro tyto porty.

Povolení přístupu ke stávajícímu portu systémových služeb

Otevřením existujícího portu lze povolit vzdálený síťový přístup k systémové službě v počítači.

Poznámka: Otevřený port systémové služby může učinit počítač zranitelný vůči bezpečnostním hrozbám na Internetu, proto porty otevírejte pouze v případě nutnosti.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně Brána firewall klepněte na položku **Systémové služby**.
4. V okně **Otevřít port systémové služby** zaškrtněte políčko systémové služby, jejíž port chcete otevřít.
5. Klepněte na tlačítko **Upravit**.
6. Proveďte jednu z následujících akcí:
   - Chcete-li port otevřít pro libovolný počítač v důvěryhodné, standardní nebo veřejné síti (například pro domácí, podnikovou nebo internetovou síť), vyberte možnosti **Důvěryhodná, Standardní nebo Veřejná**.
   - Chcete-li port otevřít pro libovolný počítač ve standardní síti (například pro podnikovou síť), vyberte možnost **Standardní (včetně Důvěryhodné)**.
7. Klepněte na tlačítko **OK**.

Blokování přístupu ke stávajícímu portu systémových služeb

Uzavřením existujícího portu lze zablokovat vzdálený síťový přístup k systémové službě v počítači.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně Brána firewall klepněte na položku **Systémové služby**.
4. V okně **Otevřít port systémové služby** zrušte zaškrtnutí políčka u portu systémové služby, který chcete zavřít.
5. Klepněte na tlačítko **OK**.

Konfigurace nového portu systémové služby

Otevřením nebo uzavřením nového portu síťové služby v počítači lze povolit nebo zablokovat vzdálený přístup k počítači.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně Brána firewall klepněte na položku **Systémové služby**.
4. Klepněte na tlačítko **Přidat**.
5. V podokně Systémové služby zadejte v části **Přidat pravidlo systémové služby** následující údaje:
   - Název systémové služby
   - Kategorii systémové služby
   - Místní porty TCP/IP
   - Místní porty UDP
6. Proveďte jednu z následujících akcí:
   - Chcete-li port otevřít pro libovolný počítač v důvěryhodné, standardní nebo veřejné síti (například pro domácí, podnikovou nebo internetovou síť), vyberte možnosti **Důvěryhodná, Standardní nebo Veřejná**.
   - Chcete-li port otevřít pro libovolný počítač ve standardní síti (například pro podnikovou síť), vyberte možnost **Standardní (včetně Důvěryhodné)**.
7. Chcete-li informace o aktivitě portu posílat na jiný síťový počítač se systémem Windows, který sdílí připojení k Internetu, vyberte možnost **Přeposlat síťovou aktivitu tohoto portu síťovým počítačům, které používají službu Sdílení připojení k Internetu** .
8. Volitelně můžete zadat popis nové konfigurace.
9. Klepněte na tlačítko **OK**.

Poznámka: Je-li v počítači nainstalován program, který přijímá připojení k webovému serveru nebo serveru FTP, může být potřeba v počítačích, které připojení sdílejí, otevřít příslušný port systémové služby a povolit přesměrování příchozího připojení pro tyto porty. Používáte-li službu Sdílení připojení k Internetu (ICS), je také potřeba přidat důvěryhodné připojení počítače do seznamu **Sítě**. Další informace naleznete v části Přidání připojení počítače.

úprava portu systémové služby

U existujícího portu systémové služby lze upravit informace o příchozím a odchozím síťovém přístupu.

Poznámka: Pokud jsou informace o portu zadány nesprávně, systémová služba nebude fungovat.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně Brána firewall klepněte na položku **Systémové služby**.
4. Zaškrtněte políčko u systémové služby a poté klepněte na tlačítko **Upravit**.
5. V podokně Systémové služby upravte v části **Přidat pravidlo systémové služby** následující údaje:
   - Název systémové služby
   - Místní porty TCP/IP
   - Místní porty UDP
6. Proveďte jednu z následujících akcí:
   - Chcete-li port otevřít pro libovolný počítač v důvěryhodné, standardní nebo veřejné síti (například pro domácí, podnikovou nebo internetovou síť), vyberte možnosti **Důvěryhodná, Standardní nebo Veřejná**.
   - Chcete-li port otevřít pro libovolný počítač ve standardní síti (například pro podnikovou síť), vyberte možnost **Standardní (včetně Důvěryhodné)**.
7. Chcete-li informace o aktivitě portu posílat na jiný síťový počítač se systémem Windows, který sdílí připojení k Internetu, vyberte možnost **Přeposlat síťovou aktivitu tohoto portu síťovým počítačům, které používají službu Sdílení připojení k Internetu** .
8. Volitelně můžete zadat popis upravené konfigurace.
9. Klepněte na tlačítko **OK**.

Odebrání portu systémové služby

Z počítače lze odebrat existující port systémové služby. Po odebrání nebudou mít vzdálené počítače k této síťové službě přístup.

1. V podokně McAfee SecurityCenter klepněte na položku **Internet a síť** a na položku **Konfigurovat**.
2. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
3. V podokně Brána firewall klepněte na položku **Systémové služby**.
4. Vyberte systémovou službu a klepněte na tlačítko **Odebrat**.
5. Po zobrazení výzvy potvrďte operaci klepnutím na tlačítko **Ano**.

KAPITOLA 21

Protokolování, sledování a analýza

Brána firewall umožňuje rozsáhlé a přehledné protokolování, sledování a analýzu událostí a provozu v síti Internet. Pochopení událostí a provozu v síti Internet usnadňuje spravování připojení k Internetu.

V této kapitole

Protokolování událostí

Brána firewall umožňuje určit, zda chcete protokolování povolit nebo zakázat, a v případě povolení typy událostí, které se mají protokolovat. Protokolování událostí umožňuje zobrazit nedávné příchozí a odchozí události a události vniknutí.

Konfigurace nastavení protokolu událostí

Můžete určit a nakonfigurovat typy událostí protokolovaných bránou firewall. Ve výchozím nastavení je povoleno protokolování všech událostí a aktivit.

1. V podokně Konfigurace Internetu a sítě v části **Ochrana brány firewall je povolena** klepněte na položku **Upřesnit**.
2. V podokně brány firewall klepněte na kartu **Nastavení protokolu událostí**.
3. Pokud není zaškrtnuto políčko **Povolit protokolování událostí**, zaškrtněte jej.
4. V části **Povolit protokolování událostí** zaškrtněte nebo zrušte zaškrtnutí políček typů událostí, které chcete nebo nechcete protokolovat. Typy událostí zahrnují následující:
   - Blokované programy
   - Pakety ICMP Ping
   - Provoz ze zakázaných adres IP
   - Události na portech systémových služeb
   - Události na neznámých portech
   - Události zjišťování neoprávněných vniknutí (IDS)
5. Chcete-li zabránit protokolování na určitých portech, vyberte možnost **Neprotokolovat události na následujících portech** a zadejte jednotlivá čísla portů oddělená čárkami nebo rozsahy portů s pomlčkami. Příklad: `137-139, 445, 400-5000`.
6. Klepněte na tlačítko **OK**.

Zobrazení nedávných událostí

Je-li povoleno protokolování, můžete zobrazit nedávné události. V podokně Nedávné události je zobrazeno datum a popis události. Je zobrazena aktivita programů, kterým byl explicitně zakázán přístup k Internetu.

- V nabídce **Rozšířená nabídka** v podokně Běžné úkoly klepněte na položku **Zprávy a protokoly** nebo **Zobrazit nedávné události**. Případně můžete klepnout na položku **Zobrazit nedávné události** v podokně Běžné úkoly v Základní nabídce.

Zobrazení příchozích událostí

Je-li povoleno protokolování, můžete zobrazit příchozí události. Příchozí události obsahují datum a čas, zdrojovou adresu IP, název hostitele a typ informace a události.

1. Zkontrolujte, zda je povolena Rozšířená nabídka. V podokně Běžné úkoly klepněte na položku **Zprávy a protokoly**.
2. V části **Nedávné události** klepněte na položku **Zobrazit protokol**.
3. Klepněte na položku **Internet a síť** a na položku **Příchozí události**.

Poznámka: Pomocí protokolu Příchozí události můžete adresu IP nastavit jako důvěryhodnou, zakázat ji nebo trasovat.

Zobrazení odchozích událostí

Je-li povoleno protokolování, můžete zobrazit odchozí události. Odchozí události obsahují název programu, který se pokouší o odchozí přístup, datum a čas události a umístění programu v počítači.

1. V podokně Běžné úkoly klepněte na položku **Zprávy a protokoly**.
2. V části **Nedávné události** klepněte na položku **Zobrazit protokol**.
3. Klepněte na položku **Internet a síť** a na položku **Odchozí události**.

Poznámka: V protokolu Odchozí události můžete programu povolit úplný nebo pouze odchozí přístup. Můžete také získat další informace o programu.

Zobrazení událostí zjišťování neoprávněných vniknutí

Je-li povoleno protokolování, můžete zobrazit události neoprávněného vniknutí. Události zjišťování neoprávněných vniknutí zobrazují datum a čas, zdrojovou adresu IP, název hostitele události a typ události.

1. V podokně Běžné úkoly klepněte na položku **Zprávy a protokoly**.
2. V části **Nedávné události** klepněte na položku **Zobrazit protokol**.
3. Klepněte na položky **Internet a síť** a **Události zjišťování neoprávněných vniknutí**.

Poznámka: Pomocí protokolu Události zjišťování neoprávněných vniknutí můžete adresu IP nastavit jako důvěryhodnou, zakázat ji nebo trasovat.

Práce se statistikami

Brána firewall ovlivňuje webovou stránku HackerWatch společnosti McAfee, na které jsou poskytovány statistiky celosvětových událostí zabezpečení sítě Internet a aktivity portů.

Zobrazení celosvětových statistik událostí zabezpečení

Server HackerWatch sleduje celosvětové události zabezpečení sítě Internet, které můžete zobrazit v programu SecurityCenter. Sledované informace uvádí seznam případů nahlášených serveru HackerWatch za posledních 24 hodin, 7 dní a 30 dní.

1. Zkontrolujte, zda je povolena Rozšířená nabídka, a klepněte na příkaz **Nástroje**.
2. V podokně Nástroje klepněte na položku **HackerWatch**.
3. V části Sledování událostí lze zobrazit události zabezpečení.

Zobrazení globální internetové aktivity portů

Server HackerWatch sleduje celosvětové události zabezpečení sítě Internet, které můžete zobrazit v programu SecurityCenter. Zobrazené informace obsahují porty s největším počtem událostí ohlášených serveru HackerWatch během posledních sedmi dní. Zpravidla jsou zobrazeny informace o portech HTTP, TCP a UDP.

1. Zkontrolujte, zda je povolena Rozšířená nabídka, a klepněte na příkaz **Nástroje**.
2. V podokně Nástroje klepněte na položku **HackerWatch**.
3. Porty s největším počtem událostí zobrazíte v části **Nedávná aktivita portů**.

Trasování internetového provozu

Brána firewall poskytuje mnoho funkcí k trasování internetového provozu. Tyto funkce umožňují geografické trasování síťového počítače, získání informací o doménách a sítích a trasování počítačů zaznamenaných v protokolech Příchozí události a Události zjišťování neoprávněných vniknutí.

Geografické trasování počítače v síti

Pomocí programu pro vizuální trasování lze počítač, který se připojuje nebo pokouší připojit k vašemu počítači, geograficky vyhledat pomocí jeho názvu nebo adresy IP. Pomocí programu pro vizuální trasování lze také získat přístup k informacím o síti a registraci. Po spuštění programu pro vizuální trasování se zobrazí mapa světa, na které je vyznačena nejpravděpodobnější trasa dat mezi zdrojovým počítačem a tímto počítačem.

1. Zkontrolujte, zda je povolena Rozšířená nabídka, a klepněte na příkaz **Nástroje**.
2. V podokně Nástroje klepněte na položku **Program pro vizuální trasování**.
3. Zadejte adresu IP počítače a klepněte na tlačítko **Trasovat**.
4. V okně **Program pro vizuální trasování** vyberte možnost **Zobrazení mapy**.

Poznámka: Události neplatných, soukromých či cyklických adres IP nelze trasovat.

Získání registračních informací počítače

Pomocí programu pro vizuální trasování lze z programu SecurityCenter získat registrační informace počítače. Informace obsahují název domény, jméno a adresu osoby, na kterou je zaregistrována, a kontaktní informace.

1. Zkontrolujte, zda je povolena Rozšířená nabídka, a klepněte na příkaz **Nástroje**.
2. V podokně Nástroje klepněte na položku **Program pro vizuální trasování**.
3. Zadejte adresu IP počítače a klepněte na tlačítko **Trasovat**.
4. V okně **Program pro vizuální trasování** vyberte možnost **Zobrazení osob žádajících o registraci**.

Získání informací o síti počítače

Pomocí programu pro vizuální trasování lze v programu SecurityCenter získat informace o síti počítače. Informace o síti obsahují podrobnosti o síti, v níž je doména umístěna.

1. Zkontrolujte, zda je povolena Rozšířená nabídka, a klepněte na příkaz **Nástroje**.
2. V podokně Nástroje klepněte na položku **Program pro vizuální trasování**.
3. Zadejte adresu IP počítače a klepněte na tlačítko **Trasovat**.
4. V okně **Program pro vizuální trasování** vyberte možnost **Zobrazení sítě**.

Trasování počítače z protokolu příchozích událostí

V podokně Příchozí události můžete trasovat adresu IP, která se zobrazí v protokolu Příchozí události.

1. Zkontrolujte, zda je povolena Rozšířená nabídka. V podokně Běžné úkoly klepněte na položku **Zprávy a protokoly**.
2. V části **Nedávné události** klepněte na položku **Zobrazit protokol**.
3. Klepněte na položku **Internet a síť** a na položku **Příchozí události**.
4. V podokně Příchozí události vyberte zdrojovou adresu IP a klepněte na položku **Trasovat tuto adresu IP**.
5. V podokně programu pro vizuální trasování klepněte na jednu z následujících položek:
   - **Zobrazení mapy**: Geografické vyhledání počítače pomocí vybrané adresy IP.
   - **Zobrazení osob žádajících o registraci**: Vyhledání informací o doméně pomocí vybrané adresy IP.
   - **Zobrazení sítě**: Vyhledání informací o síti pomocí vybrané adresy IP.
6. Klepněte na tlačítko **Hotovo**.

Trasování počítače z protokolu událostí zjišťování neoprávněných vniknutí

V podokně Události zjišťování neoprávněných vniknutí můžete trasovat adresu IP, která se zobrazí v protokolu událostí zjišťování neoprávněných vniknutí.

1. V podokně Běžné úkoly klepněte na položku **Zprávy a protokoly**.
2. V části **Nedávné události** klepněte na položku **Zobrazit protokol**.
3. Klepněte na položky **Internet a síť** a **Události zjišťování neoprávněných vniknutí**. V podokně Události zjišťování neoprávněných vniknutí vyberte zdrojovou adresu IP a klepněte na položku **Trasovat tuto adresu IP**.
4. V podokně programu pro vizuální trasování klepněte na jednu z následujících položek:
   - **Zobrazení mapy**: Geografické vyhledání počítače pomocí vybrané adresy IP.
   - **Zobrazení osob žádajících o registraci**: Vyhledání informací o doméně pomocí vybrané adresy IP.
   - **Zobrazení sítě**: Vyhledání informací o síti pomocí vybrané adresy IP.
5. Klepněte na tlačítko **Hotovo**.

Trasování sledované adresy IP

Sledovanou adresu IP je možné trasovat a získat tak zeměpisné zobrazení nejpravděpodobnější trasy dat mezi zdrojovým a vaším počítačem. Také pro tuto adresu IP můžete získat informace o síti a registraci.

1. Zkontrolujte, zda je povolena Rozšířená nabídka, a klepněte na příkaz **Nástroje**.
2. V podokně Nástroje klepněte na položku **Sledování provozu**.
3. V části **Sledování provozu** klepněte na položku **Aktivní programy**.
4. Vyberte program a adresu IP, která je uvedena pod názvem programu.
5. V části **Aktivita programů** klepněte na příkaz **Trasovat tuto adresu IP**.
6. V okně **Program pro vizuální trasování** můžete zobrazit mapu, na které je zobrazena nejpravděpodobnější trasa dat mezi zdrojovým počítačem a tímto počítačem. Také pro tuto adresu IP můžete získat informace o síti a registraci.

Poznámka: Chcete-li zobrazit aktuální statistické údaje, klepněte v podokně **Program pro vizuální trasování** na tlačítko **Aktualizovat**.

Sledování internetového provozu

Brána firewall poskytuje několik způsobů sledování internetového provozu včetně následujících způsobů:

- **Graf Analýza provozu:** Zobrazuje nedávný příchozí a odchozí internetový provoz.
- **Graf Využití provozu:** Znázorňuje procenta šířky pásma využívaná nejaktivnějšími aplikacemi v průběhu posledních 24 hodin.
- **Aktivní programy:** Zobrazuje programy, které v počítači aktuálně používají nejvíce síťových připojení, a adresy IP, ke kterým tyto programy přistupují.

O grafu Analýza provozu

Graf Analýza provozu obsahuje číselnou a grafickou reprezentaci příchozího a odchozího internetového provozu. Sledování provozu také zobrazuje programy, které v počítači používají nejvíce síťových připojení, a adresy IP, ke kterým tyto programy přistupují.

V podokně Analýza provozu můžete prohlížet nedávný příchozí a odchozí internetový provoz, aktuální, průměrné a maximální přenosové rychlosti. Současně zde můžete prohlížet objem provozu, včetně množství provozu od spuštění brány firewall, a celkový provoz pro aktuální a předchozí měsíce.

Podokno Analýza provozu zobrazuje internetovou aktivitu v počítači v reálném čase, včetně objemu a rychlosti nedávného příchozího a odchozího internetového provozu, rychlosti připojení a celkového množství bajtů, které byly přeneseny Internetem.

Nepřerušovaná zelená čára představuje aktuální rychlost přenosu příchozího provozu. Tečkovaná zelená čára představuje průměrnou rychlost přenosu příchozího provozu. Pokud jsou aktuální a průměrná rychlost přenosu stejné, tečkovaná čára nebude v grafu zobrazena. Nepřerušovaná čára představuje aktuální i průměrnou rychlost přenosu.

Nepřerušovaná červená čára představuje aktuální rychlost přenosu odchozího provozu. Tečkovaná červená čára představuje průměrnou rychlost přenosu odchozího provozu. Pokud jsou aktuální a průměrná rychlost přenosu stejné, tečkovaná čára nebude v grafu zobrazena. Nepřerušovaná čára představuje aktuální i průměrnou rychlost přenosu.

Analýza příchozího a odchozího provozu

Graf Analýza provozu obsahuje číselnou a grafickou reprezentaci příchozího a odchozího internetového provozu. Sledování provozu také zobrazuje programy, které v počítači používají nejvíce síťových připojení, a adresy IP, ke kterým tyto programy přistupují.

1. Zkontrolujte, zda je povolena Rozšířená nabídka, a klepněte na příkaz **Nástroje**.
2. V podokně Nástroje klepněte na položku **Sledování provozu**.
3. V okně **Sledování provozu** klepněte na položku **Analýza provozu**.

Tip: Chcete-li zobrazit aktuální statistické údaje, klepněte v podokně **Analýza provozu** na tlačítko **Aktualizovat**.

Sledování šířky pásma programu

Lze zobrazit kruhový graf znázorňující přibližné procento šířky pásma využité nejaktivnějšími programy v počítači za posledních 24 hodin. Kruhový graf poskytuje vizuální reprezentaci relativního množství pásma využitého programy.

1. Zkontrolujte, zda je povolena Rozšířená nabídka, a klepněte na příkaz **Nástroje**.
2. V podokně Nástroje klepněte na položku **Sledování provozu**.
3. V okně **Sledování provozu** klepněte na položku **Využití provozu**.

Tip: Chcete-li zobrazit aktuální statistické údaje, klepněte v podokně **Využití provozu** na tlačítko **Aktualizovat**.

Sledování aktivity programů

Je možné zobrazit příchozí a odchozí aktivitu programů, ve které jsou uvedena připojení k vzdáleným počítačům a porty.

1. Zkontrolujte, zda je povolena Rozšířená nabídka, a klepněte na příkaz **Nástroje**.
2. V podokně Nástroje klepněte na položku **Sledování provozu**.
3. V okně **Sledování provozu** klepněte na položku **Aktivní programy**.
4. Můžete zobrazit následující informace:
   - Graf Aktivita programů: Vyberte program, pro který chcete zobrazit graf aktivity.
   - Naslouchající připojení: Vyberte pod názvem programu položku Poslech.
   - Připojení k počítači: Vyberte adresu IP pod názvem programu, systémového procesu nebo služby.

Poznámka: Chcete-li zobrazit nejaktuálnější statistické údaje, klepněte v podokně **Aktivní programy** na tlačítko **Aktualizovat**.

KAPITOLA 22

Získání informací o zabezpečení Internetu

Brána firewall ovlivňuje webovou stránku HackerWatch společnosti McAfee, na které jsou poskytovány aktuální informace o programech a internetové aktivitě. Webová stránka HackerWatch také poskytuje výukový program ve formátu HTML o bráně firewall.

V této kapitole

Spuštění kurzu serveru HackerWatch

Chcete-li se o bráně firewall dozvědět více, můžete v programu SecurityCenter spustit kurz serveru HackerWatch.

1. Zkontrolujte, zda je povolena Rozšířená nabídka, a klepněte na příkaz **Nástroje**.
2. V podokně Nástroje klepněte na položku **HackerWatch**.
3. V nabídce **Prostředky serveru HackerWatch** klepněte na příkaz **Zobrazit kurz**.

KAPITOLA 23

McAfee Anti-Spam

Program Anti-Spam (původní název SpamKiller) zabraňuje přijetí spamu do složky Doručená pošta kontrolou příchozích e-mailů a jejich následným označením jako spamu (e-maily vyzývající k nákupu) nebo jako podvodné zprávy (phishing, e-maily vyzývající k uvedení osobních informací na potenciálně podvodném webovém serveru). Program Anti-Spam filtruje spam a přesunuje ho do složky McAfee Anti-Spam.

Pokud vám někdy přátelé posílají e-maily, které mohou vypadat jako spam, přidáním jejich e-mailových adres do seznamu přátel v programu Anti-Spam zajistíte, že tyto e-maily nebudou filtrovány. Můžete také přizpůsobit způsob zjišťování spamu. Například můžete nastavit agresivnější filtrování zpráv, určit, co má program ve zprávách hledat, nebo vytvořit vlastní filtry.

Program Anti-Spam také chrání před vstupem na potencionálně podvodný webový server prostřednictvím odkazu v e-mailové zprávě. Pokud klepnete na odkaz na potenciálně podvodný webový server, budete přesměrováni na bezpečnou stránku filtru útoků phishing. Nechcete-li některé webové servery filtrovat, můžete je přidat do seznamu povolených serverů (webové servery uvedené v tomto seznamu nejsou filtrovány).

Program Anti-Spam pracuje s různými e-mailovými programy, jako jsou například Yahoo®, MSN®/Hotmail®, Windows® Mail a Live™ Mail, Microsoft® Outlook® a Outlook Express, Mozilla Thunderbird™, i s různými e-mailovými účty, například s účty POP3, webová pošta POP3 a rozhraní MAPI (Microsoft Exchange Server). Používáte-li ke čtení e-mailů prohlížeč, je nutné do programu Anti-Spam přidat účet internetové pošty. Ostatní účty jsou nakonfigurovány automaticky a není nutné je do programu Anti-Spam přidávat.

Po instalaci programu Anti-Spam není třeba žádná konfigurace. Pokud jste však pokročilý uživatel, můžete chtít rozšířené funkce ochrany proti spamu a před podvodnými zprávami (phishing) přesněji nastavit podle sebe.

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 Anti-Spam

Filtrování spamu	Zabraňte přijetí nevyžádané pošty do složky Doručená pošta. Pokročilé filtry programu Anti-Spam jsou aktualizovány pro všechny e-mailové účty automaticky. Můžete vytvořit vlastní filtry pro zvýšení přesnosti filtrování spamu a ohlásit spam k analýze společnosti McAfee.
Filtr útoků phishing	Rozpoznává potenciálně podvodné weby (phishing), které vyžadují osobní údaje.
Přizpůsobení zpracování spamu	Nevyžádané e-maily můžete označit jako spam a přesunout je do složky programu McAfee Anti-Spam, vyžádané e-maily můžete označit jako bez spamu a přesunout je do složky Doručená pošta.
Přátelé	Importem e-mailových adres přátel do seznamu přátel lze zamezit filtrování jimi odeslaných e-mailových zpráv.

KAPITOLA 24

Konfigurace zjišťování nevyžádané pošty

Ochrana proti nevyžádané poště umožňuje vlastní nastavení způsobu zjišťování nevyžádané pošty. Můžete nastavit agresivnější filtrování zpráv, určit, co bude ve zprávách vyhledáváno, a vyhledávat při analýze nevyžádané pošty specifické znakové sady. Můžete také vytvořit osobní filtry pro přesnější určení toho, které zprávy bude ochrana proti nevyžádané poště označovat jako nevyžádané. Pokud například není filtrována nevyžádaná e-mailová zpráva, která obsahuje slovo "půjčka", lze přidat filtr, který slovo "půjčka" obsahuje.

Pokud se při práci s e-maily vyskytnou potíže, lze v rámci řešení potíží ochranu proti nevyžádané poště zakázat.

V této kapitole

Nastavení možností filtrování

Jestliže chcete nastavit agresivnější filtrování zpráv, určit způsob zpracování spamu a vyhledávat při analýze spamu specifické znakové sady, upravte možnosti filtrování programu Anti-Spam.

úroveň filtrování

úroveň filtrování určuje míru důrazu při filtrování e-mailů. Jestliže například není spam filtrován při nastavení úrovně filtrování Střední, lze úroveň nastavit na možnost Středně vysoká nebo Vysoká. Na úrovni filtrování Vysoká budou ovšem přijímány pouze e-mailové zprávy od odesilatelů ze seznamu přátel a filtrovány všechny ostatní zprávy.

Zpracování spamu

Program Anti-Spam umožňuje různá vlastní nastavení způsobu zpracování spamu. Můžete například uložit spam a podvodné zprávy do specifických složek, změnit název značky, která se objeví jako předmět spamu nebo podvodné zprávy, určit maximální filtrovanou velikost a četnost aktualizace pravidel pro spam.

Znakové sady

Ochrana proti spamu vyhledává při analýze spamu specifické znakové sady. Znaková sada slouží k reprezentaci jazyka. Zahrnuje abecedu příslušného jazyka, číslice a další symboly. Jestliže přijímáte spam v řečtině, lze filtrovat všechny zprávy, které obsahují řeckou znakovou sadu.

Buďte však opatrní a neblokujte znakové sady pro jazyky, v nichž dostáváte legitimní e-mailové zprávy. Chcete-li například blokovat zprávy v italštině, můžete vybrat možnost Západoevropské, protože se Itálie nachází v západní Evropě. Pokud však přijímáte řádné e-mailové zprávy v angličtině, bude možnost Západoevropské také filtrovat zprávy v angličtině a dalších jazycích používajících západoevropskou znakovou sadu. V takovém případě nelze filtrovat pouze zprávy, které jsou v italštině.

Poznámka: Určování filtru znakové sady je určeno pro zkušené uživatele.

Změna úrovně filtrování

Intenzitu účinnosti filtrování e-mailů je možno změnit. Pokud jsou například filtrovány legitimní zprávy, lze snížit úroveň filtrování.

1 Otevřete podokno Ochrana proti spamu.

Jak?

1. V podokně Domácí programu SecurityCenter klepněte na položku **E-maily a rychlé zprávy**.
2. V informační oblasti E-maily a rychlé zprávy klepněte na položku **Konfigurovat**.
3. V podokně Konfigurace e-mailů a rychlých zpráv v části **Ochrana proti nevyžádané poště** klepněte na položku **Upřesnit**.

2 V podokně Ochrana proti spamu klepněte na položku **Možnosti filtrování**.

3 Vyberte příslušnou úroveň v části **Zadejte úroveň filtru spamu** a klepněte na tlačítko **OK**.

úroveň	Popis
Nízká	Většina e-mailů je přijata.
Středně nízká	Je filtrován pouze zřejmý spam.
Střední (doporučená)	E-mailové zprávy jsou filtrovány na doporučené úrovni.
Středně vysoká	Každý e-mail, který se podobá spamu, je filtrován.
Vysoká	Jsou přijímány pouze zprávy od odesilatelů, kteří jsou v seznamu přátel.

Změna způsobu zpracování a označení spamu

Můžete určit složku, do které bude ukládán spam a podvodné zprávy, změnit značky [SPAM] a [PHISH], které se objevují v předmětu e-mailu, určit maximální filtrovanou velikost a četnost aktualizace pravidel pro spam.

1 Otevřete podokno Ochrana proti spamu.

Jak?

1. V podokně Domácí programu SecurityCenter klepněte na položku **E-maily a rychlé zprávy**.
2. V informační oblasti E-maily a rychlé zprávy klepněte na položku **Konfigurovat**.
3. V podokně Konfigurace e-mailů a rychlých zpráv v části **Ochrana proti nevyžádané poště** klepněte na položku **Upřesnit**.

2 V podokně Ochrana proti spamu klepněte na položku **Možnosti filtrování**.

3 Upravte nebo vyberte následující možnosti a klepněte na tlačítko **OK**.

Akce	Postup
Určení umístění ukládání spamu a podvodných zpráv	Vyberte složku v seznamu **Uložit e-mailovou zprávu se spamem do této složky**. Výchozí složkou je složka programu McAfee Anti-Spam.
Změna předmětu e-mailu se spamem	Zadejte do pole **Označit předmět e-mailové zprávy se spamem značkou** značku, která bude přidávána do předmětu e-mailové zprávy se spamem. Výchozí značkou je značka [SPAM].
Změna předmětu podvodné e-mailové zprávy	Zadejte do pole **Označit předmět podvodné e-mailové zprávy značkou** značku, která bude přidávána do předmětu podvodné e-mailové zprávy. Výchozí značkou je značka [PHISH].
Určení největší filtrované e-mailové zprávy	Zadejte do pole **Určete největší e-mailovou zprávu, kterou chcete filtrovat (velikost v kilobajtech)** největší velikost e-mailu, kterou chcete filtrovat.
Aktualizace pravidel pro spam	Vyberte položku **Aktualizovat pravidla pro spam (v minutách)** a poté zadejte frekvenci aktualizace pravidel pro spam. Doporučená frekvence je 30 minut. Pokud máte rychlé síťové připojení, lze dosáhnout lepších výsledků určením častější frekvence (například pět minut).
Vypnutí aktualizace pravidel pro spam	Vyberte možnost **Neaktualizovat pravidla pro spam**.

Použití filtrů znakových sad

Poznámka: Filtrování zpráv, které obsahují znaky specifické znakové sady, je vhodné pro zkušenější uživatele.

Lze filtrovat znakové sady určitého jazyka, avšak neblokujte znakové sady pro jazyky, v nichž dostáváte legitimní e-mailové zprávy.

1 Otevřete podokno Ochrana proti nevyžádané poště.

Jak?

1. V podokně Domácí programu SecurityCenter klepněte na položku **E-maily a rychlé zprávy**.
2. V informační oblasti E-maily a rychlé zprávy klepněte na položku **Konfigurovat**.
3. V podokně Konfigurace e-mailů a rychlých zpráv v části **Ochrana proti nevyžádané poště** klepněte na položku **Upřesnit**.

2 V podokně Ochrana proti nevyžádané poště klepněte na položku **Znakové sady**.

3 Zaškrtněte políčko vedle znakové sady, kterou chcete filtrovat.

4 Klepněte na tlačítko **OK**.

Použití osobních filtrů

Osobní filtr na základě specifických slov nebo frází určuje, zda budou e-mailové zprávy povoleny nebo blokovány. Pokud e-mailová zpráva obsahuje slovo nebo frázi nastavenou filtrem pro blokování, je zpráva označena jako spam a ponechána v Doručené poště nebo přesunuta do složky programu McAfee Anti-Spam. Další informace o způsobu zpracovávání spamu naleznete v tématu Změna způsobu zpracování a označení zpráv (stránka 122).

Program Anti-Spam obsahuje pokročilý filtr, který brání přijetí nevyžádaných e-mailových zpráv do složky Doručená pošta. Pokud však chcete nastavit přesněji, které zprávy má ochrana proti spamu označovat jako spam, lze vytvořit osobní filtr. Pokud například přidáte filtr, který obsahuje slovo „půjčka“, bude ochrana proti spamu filtrovat zprávy, které slovo „půjčka“ obsahují. Nevytvářejte filtry pro běžná slova, která se objevují v legitimních e-mailových zprávách. V takovém případě totiž budou filtrovány i e-mailové zprávy, které nejsou nevyžádané. Jestliže filtr vytvoříte a zjistíte, že filtr stále některý spam nedetekuje, lze filtr upravit. Pokud jste například vytvořili filtr, který vyhledával v předmětu zprávy slovo „viagra“, ale stále přijímáte zprávy, které slovo „viagra“ obsahují, protože se slovo objevuje v textu zprávy, změňte filtr tak, aby vyhledával slovo „viagra“ v textu zprávy namísto v předmětu zprávy.

Regulární výrazy (RegEx) jsou zvláštní znaky a posloupnosti, které lze také v osobních filtrech použít. Používání regulárních výrazů však společnost McAfee doporučuje pouze pro zkušené uživatele. Pokud s regulárními výrazy nejste obeznámeni, nebo pokud chcete další informace o způsobu používání regulárních výrazů, můžete regulární výrazy vyhledat v síti Internet (přejděte například na stránku http://en.wikipedia.org/wiki/Regular_expression).

Přidání osobního filtru

Můžete přidat osobní filtry pro přesnější určení toho, které zprávy bude ochrana proti nevyžádané poště označovat jako nevyžádané.

1 Otevřete podokno Ochrana proti nevyžádané poště.

Jak?

1. V podokně Domácí programu SecurityCenter klepněte na položku **E-maily a rychlé zprávy**.
2. V informační oblasti E-maily a rychlé zprávy klepněte na položku **Konfigurovat**.
3. V podokně Konfigurace e-mailů a rychlých zpráv v části **Ochrana proti nevyžádané poště** klepněte na položku **Upřesnit**.

2 V podokně Ochrana proti nevyžádané poště klepněte na položku **Osobní filtry**.

3 Klepněte na tlačítko **Přidat**.

4 Určete, co bude osobní filtr vyhledávat (stránka 126) v e-mailové zprávě.

5 Klepněte na tlačítko **OK**.

Úprava osobního filtru

Úpravou stávajících filtrů můžete přesněji nastavit, které zprávy jsou rozeznány jako nevyžádaná pošta.

1 Otevřete podokno Ochrana proti nevyžádané poště.

Jak?

1. V podokně Domácí programu SecurityCenter klepněte na položku **E-maily a rychlé zprávy**.
2. V informační oblasti E-maily a rychlé zprávy klepněte na položku **Konfigurovat**.
3. V podokně Konfigurace e-mailů a rychlých zpráv v části **Ochrana proti nevyžádané poště** klepněte na položku **Upřesnit**.

2 V podokně Ochrana proti nevyžádané poště klepněte na položku **Osobní filtry**.

3 Vyberte filtr, který chcete upravit, a klepněte na tlačítko **Upravit**.

4 Určete, co bude osobní filtr vyhledávat (stránka 126) v e-mailové zprávě.

5 Klepněte na tlačítko **OK**.

Odebrání osobního filtru

Filtry, které již nechcete používat, je možné natrvalo odebrat.

1 Otevřete podokno Ochrana proti nevyžádané poště.

Jak?

1. V podokně Domácí programu SecurityCenter klepněte na položku **E-maily a rychlé zprávy**.
2. V informační oblasti E-maily a rychlé zprávy klepněte na položku **Konfigurovat**.
3. V podokně Konfigurace e-mailů a rychlých zpráv v části **Ochrana proti nevyžádané poště** klepněte na položku **Upřesnit**.

2 V podokně Ochrana proti nevyžádané poště klepněte na položku **Osobní filtry**.

3 Vyberte filtr, který chcete odebrat, a klepněte na tlačítko **Odebrat**.

4 Klepněte na tlačítko **OK**.

Určení osobního filtru

Tato tabulka popisuje, co bude osobní filtr v e-mailu vyhledávat.

Akce	Postup
Určení filtrované části e-mailu	V seznamu **Část e-mailové zprávy** klepnutím na příslušnou položku určete, zda filtr vyhledává slova nebo fráze v předmětu, textu, odesílateli, záhlaví nebo v příjemci e-mailu. Pod seznamem **Část e-mailové zprávy** klepnutím na příslušnou položku určete, zda filtr vyhledává e-maily, které obsahují (nebo neobsahují) zadaná slova nebo fráze.
Určení slov nebo frází ve filtru	V poli **Slova nebo fráze** zadejte, co má program v e-mailu hledat. Pokud například zadáte slovo *hypotéka*, jsou filtrovány všechny e-maily, které obsahují toto slovo.
Určení používání regulárních výrazů ve filtru	Vyberte možnost **Tento filtr používá regulární výrazy**.
Výběr blokování nebo povolení e-mailů na základě filtrování slov nebo frází	Pro blokování nebo povolení e-mailu obsahujícího filtrovaná slova nebo fráze vyberte v části **Provést tuto akci** možnost **Blokovat** nebo **Povolit**.

Zákaz ochrany proti spamu

Chcete-li ochraně proti spamu zabránit ve filtrování e-mailů, ochranu proti spamu zakažte.

1. V rozšířené nabídce klepněte na tlačítko **Konfigurovat**.
2. V konfiguračním podokně klepněte na položku **E-maily a rychlé zprávy**.
3. V části **Ochrana proti spamu je povolena** klepněte na možnost **Vypnout**.

Tip: Nezapomeňte v části **Ochrana proti spamu je zakázána** opět klepnout na možnost **Zapnout**, takže budete chráněni proti spamu.

KAPITOLA 25

Filtrování e-mailů

Ochrana proti spamu zkoumá příchozí e-mailové zprávy a tyto zprávy rozděluje na spam (e-maily vyzývající k nákupu) a na podvodné zprávy (phishing, e-maily vyzývající k uvedení osobních informací na známém nebo potenciálním podvodném webovém serveru). Ve výchozím nastavení ochrana proti spamu označí každou nevyžádanou e-mailovou zprávu jako spam nebo podvodnou zprávu (v předmětu zprávy se objeví značka nevyžádané zprávy [SPAM] nebo podvodné zprávy [PHISH]) a zprávu přesune do složky programu McAfee Anti-Spam.

E-mail můžete pomocí panelu nástrojů programu Anti-Spam označit jako spam nebo bez spamu, můžete změnit umístění, do kterého jsou zprávy se spamem přesouvány, nebo značku, která se objeví v předmětu.

Pokud při práci s e-mailovým programem dochází k potížím, lze v rámci řešení potíží panely nástrojů ochrany proti spamu zakázat.

V této kapitole

Označení zprávy z panelu nástrojů ochrany proti spamu

Pokud označíte zprávu jako spam, je předmět zprávy označen značkou [SPAM] nebo vámi určenou značkou a zpráva je ponechána ve složce Doručená pošta, ve složce programu McAfee Anti-Spam (u aplikací Outlook, Outlook Express, Windows Mail a Thunderbird) nebo ve složce Nevyžádaná pošta (aplikace Eudora®). Pokud zprávu označíte jako bez spamu, je značka odstraněna a zpráva je přesunuta do složky Doručená pošta.

Označení zprávy v aplikaci	Postup po výběru zprávy
Outlook, Outlook Express, Windows Mail	Klepněte na možnost **Označit jako spam** nebo **Označit jako bez spamu**.
Eudora	V nabídce **Ochrana proti spamu** klepněte na tlačítko **Označit jako spam** nebo na tlačítko **Označit jako bez spamu**.
Thunderbird	V panelu nástrojů programu **Anti-Spam** ukažte na položku **M**, ukažte na možnost **Označit jako** a dále na položku **Spam** nebo na **Bez spamu**.

Zakázání panelu nástrojů ochrany proti spamu

Používáte-li e-mailové programy Outlook, Outlook Express, Windows Mail, Eudora nebo Thunderbird, můžete panel nástrojů ochrany proti spamu zakázat.

1. Otevřete podokno Ochrana proti spamu.

   Jak?

   1. V podokně Domácí programu SecurityCenter klepněte na položku **E-maily a rychlé zprávy**.
   2. V informační oblasti E-maily a rychlé zprávy klepněte na položku **Konfigurovat**.
   3. V podokně Konfigurace e-mailů a rychlých zpráv v části **Ochrana proti nevyžádané poště** klepněte na položku **Upřesnit**.

2. V podokně Ochrana proti spamu klepněte na položku **Panely nástrojů e-mailu**.
3. Zrušte zaškrtnutí políčka vedle panelu nástrojů, který chcete zakázat.
4. Klepněte na tlačítko **OK**.

Tip: Panely nástrojů ochrany proti spamu lze kdykoliv povolit zaškrtnutím příslušného políčka panelu.

KAPITOLA 26

Nastavení přátel

Protože program Anti-Spam obsahuje vylepšený filtr, který rozpoznává a povoluje legitimní e-mailové zprávy, je jen velice zřídka potřeba přidávat (ručně nebo importem z adresářů) e-mailové adresy přátel do seznamu přátel. Pokud ale přidáte e-mailovou adresu přítele a někdo ji zneužije, bude program Anti-Spam zprávy z této e-mailové adresy povolovat do složky Doručená pošta.

Pokud chcete i přesto importovat adresáře a dojde k jejich změně, je třeba import opakovat; program Anti-Spam totiž seznam přátel neaktualizuje automaticky.

Seznam přátel v programu Anti-Spam lze aktualizovat i ručně. Přidáním celé domény budou všichni uživatelé v doméně přidáni do seznamu přátel. Jestliže například přidáte doménu spolecnost.cz, nebude filtrován žádný e-mail z této společnosti.

V této kapitole

Import adresáře

Má-li program Anti-Spam přidat e-mailové adresy do seznamu přátel, importujte adresář.

1 Otevřete podokno Ochrana proti spamu.

   Jak?

   1. V podokně Domácí programu SecurityCenter klepněte na položku **E-maily a rychlé zprávy**.
   2. V informační oblasti E-maily a rychlé zprávy klepněte na položku **Konfigurovat**.
   3. V podokně Konfigurace e-mailů a rychlých zpráv v části **Ochrana proti nevyžádané poště** klepněte na položku **Upřesnit**.

2 V podokně Ochrana proti spamu klepněte na položku **Přátelé**.

3 V podokně Přátelé klepněte na položku **Importovat**.

4 V seznamu **Vybrat adresář k importu** klepněte na typ adresáře, který chcete importovat.

5 Klepněte na tlačítko **Importovat**.

Ruční nastavení přátel

Seznam přátel lze upravit ručně po jednotlivých položkách. Pokud například obdržíte e-mail od přítele, jehož adresa není v adresáři, můžete ji do něj přidat ručně. Nejjednodušším způsobem je přidání pomocí panelu nástrojů programu Anti-Spam. Pokud panel nástrojů programu Anti-Spam nepoužíváte, je nutné zadat informace o příteli.

Přidání přítele z panelu nástrojů programu Anti-Spam

Používáte-li e-mailové programy Outlook, Outlook Express, Windows Mail, Eudora™ nebo Thunderbird, můžete přátele přidat přímo z panelu nástrojů programu Anti-Spam.

Přidání přítele v aplikaci:	Postup po výběru zprávy
Outlook, Outlook Express, Windows Mail	Klepněte na tlačítko **Přidat přítele**.
Eudora	V nabídce **Anti-Spam** klepněte na položku **Přidat přítele**.
Thunderbird	V panelu nástrojů programu **Anti-Spam** ukažte na položku **M**, ukažte na možnost **Označit jako** a klepněte na položku **Přítel**.

Ruční přidání přítele

Jestliže nechcete přidat přítele přímo z panelu nástrojů nebo jste to zapomněli provést při obdržení e-mailu, lze přítele stále přidat do seznamu přátel.

1. Otevřete podokno Ochrana proti spamu.

   Jak?

   1. V podokně Domácí programu SecurityCenter klepněte na položku **E-maily a rychlé zprávy**.
   2. V informační oblasti E-maily a rychlé zprávy klepněte na položku **Konfigurovat**.
   3. V podokně Konfigurace e-mailů a rychlých zpráv v části **Ochrana proti nevyžádané poště** klepněte na položku **Upřesnit**.

2. V podokně Ochrana proti spamu klepněte na položku **Přátelé**.
3. V podokně Přátelé klepněte na položku **Přidat**.
4. Zadejte jméno přítele do pole **Jméno**.
5. V seznamu **Typ** vyberte možnost **Jediná e-mailová adresa**.
6. Do pole **E-mailová adresa** zadejte e-mailovou adresu přítele.
7. Klepněte na tlačítko **OK**.

Přidání domény

Chcete-li přidat všechny uživatele určité domény do seznamu přátel, přidejte celou doménu. Jestliže například přidáte doménu spolecnost.cz, nebude filtrován žádný e-mail z této společnosti.

1 Otevřete podokno Ochrana proti spamu.

   Jak?

   1. V podokně Domácí programu SecurityCenter klepněte na položku **E-maily a rychlé zprávy**.
   2. V informační oblasti E-maily a rychlé zprávy klepněte na položku **Konfigurovat**.
   3. V podokně Konfigurace e-mailů a rychlých zpráv v části **Ochrana proti nevyžádané poště** klepněte na položku **Upřesnit**.

2 V podokně Ochrana proti spamu klepněte na položku **Přátelé**.

3 V podokně Přátelé klepněte na položku **Přidat**.

4 Zadejte název společnosti nebo skupiny do pole **Jméno**.

5 V seznamu **Typ** vyberte možnost **Celá doména**.

6 Zadejte název domény do pole **E-mailová adresa**.

7 Klepněte na tlačítko **OK**.

úprava informací o příteli

Jestliže se informace o některém příteli změní, můžete aktualizací seznamu přátel zajistit, že ochrana proti spamu zprávy přítele neoznačí jako spam.

1 Otevřete podokno Ochrana proti spamu.

   Jak?

   1. V podokně Domácí programu SecurityCenter klepněte na položku **E-maily a rychlé zprávy**.
   2. V informační oblasti E-maily a rychlé zprávy klepněte na položku **Konfigurovat**.
   3. V podokně Konfigurace e-mailů a rychlých zpráv v části **Ochrana proti nevyžádané poště** klepněte na položku **Upřesnit**.

2 V podokně Ochrana proti spamu klepněte na položku **Přátelé**.

3 Vyberte přítele, kterého chcete upravit, a klepněte na tlačítko **Upravit**.

4 Změňte jméno přítele v poli **Jméno**.

5 V poli **E-mailová adresa** změňte e-mailovou adresu přítele.

6 Klepněte na tlačítko **OK**.

úprava informací o doméně

Jestliže se informace o doméně změní, můžete aktualizací seznamu přátel zajistit, že ochrana proti spamu zprávy domény neoznačí jako spam.

1 Otevřete podokno Ochrana proti spamu.

   Jak?

   1. V podokně Domácí programu SecurityCenter klepněte na položku **E-maily a rychlé zprávy**.
   2. V informační oblasti E-maily a rychlé zprávy klepněte na položku **Konfigurovat**.
   3. V podokně Konfigurace e-mailů a rychlých zpráv v části **Ochrana proti nevyžádané poště** klepněte na položku **Upřesnit**.

2 V podokně Ochrana proti spamu klepněte na položku **Přátelé**.

3 V podokně Přátelé klepněte na položku **Přidat**.

4 Změňte název společnosti nebo skupiny v poli **Jméno**.

5 V seznamu **Typ** vyberte možnost **Celá doména**.

6 Změňte v poli **E-mailová adresa** název domény.

7 Klepněte na tlačítko **OK**.

Odebrání přítele

Jestliže osoba nebo doména ze seznamu přátel odesílá nevyžádanou poštu, odeberte tyto adresy ze seznamu přátel ochrany proti nevyžádané poště, takže budou jejich e-mailové zprávy opět filtrovány.

1 Otevřete podokno Ochrana proti nevyžádané poště.

   Jak?

   1. V podokně Domácí programu SecurityCenter klepněte na položku **E-maily a rychlé zprávy**.
   2. V informační oblasti E-maily a rychlé zprávy klepněte na položku **Konfigurovat**.
   3. V podokně Konfigurace e-mailů a rychlých zpráv v části **Ochrana proti nevyžádané poště** klepněte na položku **Upřesnit**.

2 V podokně Ochrana proti nevyžádané poště klepněte na položku **Přátelé**.

3 Vyberte přítele, kterého chcete odebrat, a klepněte na tlačítko **Odebrat**.

KAPITOLA 27

Nastavení účtů internetové pošty

Používáte-li ke čtení e-mailů prohlížeč, je k připojení programu Anti-Spam k účtu a filtrování zpráv nutné program nakonfigurovat. účet internetové pošty přidáte do programu Anti-Spam jednoduše zadáním informací o účtu od vašeho poskytovatele e-mailu.

Po přidání účtu internetové pošty lze upravit informace o účtu a získat další informace o filtrování internetové pošty. Pokud již účet internetové pošty nepoužíváte nebo jej nechcete filtrovat, můžete jej odebrat.

Program Anti-Spam pracuje s různými e-mailovými programy, jako jsou například Yahoo!®, MSN®/Hotmail®, Windows® Mail a Live™ Mail, Microsoft® Outlook® a Outlook Express, Mozilla Thunderbird™, i s různými e-mailovými účty, například s účty POP3, internetová pošta POP3 a rozhraní MAPI (Microsoft Exchange Server). POP3 je nejobvyklejší typ účtu. Je standardní pro internetové e-mailové programy. Máte-li účet POP3, program Anti-Spam se připojí přímo k e-mailovému serveru a filtruje zprávy ještě před tím, než jsou načteny účtem internetové pošty. účty internetové pošty POP3, Yahoo, MSN/Hotmail a Windows Mail existují na Internetu. Filtrování účtů POP3 internetové pošty je podobné jako filtrování účtů POP3.

V této kapitole

Přidání účtu webové pošty

Chcete-li filtrovat nevyžádanou poštu na účtu webové pošty POP3 (například Yahoo), MSN/Hotmail nebo Windows Mail (plně podporovány jsou pouze placené verze), je potřeba jej přidat.

1 Otevřete podokno Ochrana proti nevyžádané poště.

Jak?

1. V podokně Domácí programu SecurityCenter klepněte na položku **E-maily a rychlé zprávy**.
2. V informační oblasti E-maily a rychlé zprávy klepněte na položku **Konfigurovat**.
3. V podokně Konfigurace e-mailů a rychlých zpráv v části **Ochrana proti nevyžádané poště** klepněte na položku **Upřesnit**.

2 V podokně Ochrana proti nevyžádané poště klepněte na položku **Účty webové pošty**.

3 V podokně Účty webové pošty klepněte na položku **Přidat**.

4 Zadejte informace o účtu (stránka 137) a klepněte na tlačítko **Další**.

5 V části **Možnosti kontroly** určete, kdy má program Anti-Spam kontrolovat, zda účet neobsahuje nevyžádanou poštu (stránka 137).

6 Máte-li telefonické připojení, určete způsob připojení programu Anti-Spam k Internetu (stránka 137).

7 Klepněte na tlačítko **Dokončit**.

Úprava účtu webové pošty

Dojde-li ke změně informací o účtu webové pošty, je nutné jej upravit. Účet webové pošty je potřeba upravit, pokud například změníte heslo nebo chcete, aby program Anti-Spam kontroloval nevyžádanou poštu častěji.

1 Otevřete podokno Ochrana proti nevyžádané poště.

Jak?

1. V podokně Domácí programu SecurityCenter klepněte na položku **E-maily a rychlé zprávy**.
2. V informační oblasti E-maily a rychlé zprávy klepněte na položku **Konfigurovat**.
3. V podokně Konfigurace e-mailů a rychlých zpráv v části **Ochrana proti nevyžádané poště** klepněte na položku **Upřesnit**.

2 V podokně Ochrana proti nevyžádané poště klepněte na položku **Účty webové pošty**.

3 Vyberte účet, který chcete upravit, a klepněte na tlačítko **Upravit**.

4 Zadejte informace o účtu (stránka 137) a klepněte na tlačítko **Další**.

5 V části **Možnosti kontroly** určete, kdy má program Anti-Spam kontrolovat, zda účet neobsahuje nevyžádanou poštu (stránka 137).

6 Máte-li telefonické připojení, určete způsob připojení programu Anti-Spam k Internetu (stránka 137).

7 Klepněte na tlačítko **Dokončit**.

Odebrání účtu webové pošty

Pokud již nechcete filtrovat nevyžádanou poštu z určitého účtu webové pošty, odeberte jej. Účet můžete odebrat, například pokud již účet není aktivní. Pokud se vyskytly problémy, můžete účet odebrat, dokud nebudou vyřešeny.

1 Otevřete podokno Ochrana proti nevyžádané poště.

Jak?

1. V podokně Domácí programu SecurityCenter klepněte na položku **E-maily a rychlé zprávy**.
2. V informační oblasti E-maily a rychlé zprávy klepněte na položku **Konfigurovat**.
3. V podokně Konfigurace e-mailů a rychlých zpráv v části **Ochrana proti nevyžádané poště** klepněte na položku **Upřesnit**.

2 V podokně Ochrana proti nevyžádané poště klepněte na položku **Účty webové pošty**.

3 Vyberte účet, který chcete odebrat, a klepněte na tlačítko **Odebrat**.

Vysvětlení informací o účtu webové pošty

V následující tabulce jsou uvedeny informace, které je nutné při přidání nebo úpravě účtu webové pošty zadat.

Informace o účtu

Informace	Popis
Popis	Zadejte popis účtu pro vlastní potřebu. Do tohoto pole můžete zadat jakékoli údaje.
E-mailová adresa	Určete e-mailovou adresu přidruženou k e-mailovému účtu.
Typ účtu	Vyberte typ přidávaného e-mailového účtu. (například webová pošta POP3 nebo MSN/Hotmail).
Server	Zadejte název poštovního serveru hostujícího tento účet. Pokud název serveru neznáte, naleznete jej v informacích od poskytovatele služeb Internetu (ISP).
Uživatelské jméno	Zadejte uživatelské jméno k tomuto e-mailovému účtu. Je-li vaše e-mailová adresa například *uzivatel*@hotmail.com, uživatelské jméno je pravděpodobně *uzivatel*.
Heslo	Zadejte heslo k tomuto e-mailovému účtu.
Potvrdit heslo	Ověřte heslo k tomuto e-mailovému účtu.

Možnosti kontroly

Možnost	Popis
Kontrolovat v intervalu	Program Anti-Spam bude nevyžádanou poštu na účtu kontrolovat v zadaném intervalu (počet minut). Interval musí být v rozmezí 5 a 3600 minut.
Kontrolovat při spuštění	Program Anti-Spam bude účet kontrolovat při každém restartování počítače.

Možnosti připojení

Možnost	Popis
Nikdy nenavazovat telefonické připojení	Program Anti-Spam nenaváže telefonické připojení automaticky. Telefonické připojení musíte navázat ručně.
Vytáčet, pokud není k dispozici připojení	Není-li k dispozici připojení k Internetu, pokusí se program Anti-Spam připojit pomocí vybraného telefonického připojení.
Vždy vytáčet vybrané připojení	Program Anti-Spam se pokusí připojit pomocí vybraného telefonického připojení. Budete-li připojeni pomocí jiného telefonického připojení, než je určeno, dojde k odpojení.
Vytočit toto připojení	Určete telefonické připojení, které program Anti-Spam použije pro připojení k Internetu.
Zachovat připojení po dokončení filtrování	Počítač zůstane po dokončení filtrování připojen k Internetu.

KAPITOLA 28

Práce s filtrovanými e-mailovými zprávami

Někdy se může stát, že spam nemusí být zjištěn. Pokud tato situace nastane, můžete spam nahlásit společnosti McAfee, kde bude analyzován a využit k vytvoření aktualizací filtrů.

Jestliže používáte účet internetové pošty, lze filtrované e-mailové zprávy zobrazovat, exportovat a odstraňovat. Tato možnost je užitečná tehdy, jestliže si nejste jisti, zda nebyla filtrována legitimní zpráva, nebo jestliže chcete vědět, kdy byla zpráva filtrována.

V této kapitole

Ohlášení e-mailových zpráv společnosti McAfee

Při označení zprávy jako spam nebo bez spamu lze e-mailové zprávy ohlásit společnosti McAfee, takže můžeme pomocí jejich analýzy vytvořit aktualizace filtrů.

1 Otevřete podokno Ochrana proti spamu.

   Jak?

   1. V podokně Domácí programu SecurityCenter klepněte na položku **E-maily a rychlé zprávy**.
   2. V informační oblasti E-maily a rychlé zprávy klepněte na položku **Konfigurovat**.
   3. V podokně Konfigurace e-mailů a rychlých zpráv v části **Ochrana proti nevyžádané poště** klepněte na položku **Upřesnit**.

2 V podokně Ochrana proti spamu klepněte na položku **Panely nástrojů e-mailu**.

3 Vyberte příslušná zaškrtávací políčka v rámci položky **Pomozte zlepšit program Anti-Spam** a poté klepněte na tlačítko **OK**.

Akce	Postup
Ohlásit e-mail společnosti McAfee při každém označení zprávy jako spamu.	Vyberte **Označujete e-mailové zprávy jako spam**.
Ohlásit e-mail společnosti McAfee při každém označení zprávy jako bez spamu.	Vyberte **Označujete e-mailové zprávy jako poštu, která není spam**.

Akce	Postup
Při ohlášení e-mailu bez spamu odeslat společnosti McAfee celý e-mail (ne pouze záhlaví).	Vyberte možnost **Odeslat celou e-mailovou zprávu (ne pouze záhlaví)**.

Poznámka: Když e-mail ohlásíte jako bez spamu a společnosti McAfee odešlete celý e-mail, není e-mailová zpráva šifrována.

Zobrazení, export nebo odstranění filtrované internetové pošty

Filtrované zprávy účtu internetové pošty lze zobrazit, exportovat nebo odstranit.

1. V části **Běžné úkoly** klepněte na položku **Hlášení a protokoly**.
2. V podokně Hlášení a protokoly klepněte na položku **Filtrovaná internetová pošta**.
3. Vyberte zprávu.
4. V části **Požadovaná akce** proveďte jednu z následujících akcí:
   - Klepnutím na tlačítko **Zobrazit** zprávu zobrazíte ve výchozím e-mailovém programu.
   - Klepnutím na tlačítko **Exportovat** zprávu zkopírujete do počítače.
   - Klepnutím na tlačítko **Odstranit** zprávu odstraníte.

Zobrazení události filtrované internetové pošty

Můžete zobrazit datum a čas filtrování e-mailových zpráv a účet, který zprávy přijal.

1. V části **Běžné úkoly** klepněte na možnost **Zobrazit nedávné události**.
2. V podokně Nedávné události klepněte na položku **Zobrazit protokol**.
3. V levém podokně rozbalte seznam **E-maily a rychlé zprávy** a potom klepněte na položku **Události filtrování internetové pošty**.
4. Vyberte protokol, který chcete zobrazit.

KAPITOLA 29

Konfigurace ochrany proti podvodné poště

Ochrana proti nevyžádané poště rozděluje nevyžádané e-mailové zprávy na nevyžádanou poštu (e-maily vyzývající k nákupu) a na podvodné zprávy (phishing, e-maily vyzývající k uvedení osobních informací na známém nebo potenciálním podvodném webovém serveru). Ochrana proti podvodným zprávám (phishing) chrání uživatele před přístupem k podvodným webům. Jestliže klepnete v e-mailové zprávě na odkaz na známou nebo potencionální podvodnou webovou stránku, přesměruje ochrana proti nevyžádané poště uživatele na bezpečnou stránku filtru podvodných zpráv.

Pokud existují webové stránky, které filtrovat nechcete, přidejte tyto stránky do seznamu povolených serverů ochrany proti podvodným zprávám. Weby lze také v seznamu povolených serverů upravit nebo ze seznamu odebrat. Stránky typu Google®, Yahoo nebo McAfee není třeba do seznamu přidávat, protože tyto weby za podvodné nejsou považovány.

Poznámka: Jestliže máte nainstalován program SiteAdvisor, nezískáte ochranu proti podvodným zprávám programu McAfee AntiSpam z toho důvodu, že program SiteAdvisor již obsahuje podobnou ochranu proti podvodným zprávám jako program McAfee AntiSpam.

V této kapitole

Přidání webu do seznamu povolených serverů

Pokud existují webové stránky, které filtrovat nechcete, přidejte tyto stránky do seznamu povolených serverů.

1. Otevřete podokno Ochrana proti podvodné poště.

   Jak?

   1. Klepněte v podokně Domácí programu SecurityCenter na položku **Internet a sítě**.
   2. Klepněte v informační části položky Internet a sítě na tlačítko **Konfigurovat**.

2. Klepněte v podokně Ochrana proti podvodné poště na položku **Upřesnit**.
3. Klepněte v části **Seznam povolených serverů** na tlačítko **Přidat**.
4. Zadejte adresu webové stránky a poté klepněte na tlačítko **OK**.

Úpravy serverů v seznamu povolených serverů

Pokud jste stránku přidali do seznamu povolených serverů a adresa stránky se změnila, lze adresu kdykoliv aktualizovat.

1 Otevřete podokno Ochrana proti podvodné poště.

Jak?

1. Klepněte v podokně Domácí programu SecurityCenter na položku **Internet a sítě**.
2. Klepněte v informační části položky Internet a sítě na tlačítko **Konfigurovat**.

2 Klepněte v podokně Ochrana proti podvodné poště na položku **Upřesnit**.

3 Vyberte v části **Seznam povolených serverů** stránku, kterou chcete aktualizovat, a poté klepněte na tlačítko **Upravit**.

4 Upravte adresu webové stránky a poté klepněte na tlačítko **OK**.

Odebrání stránky ze seznamu povolených serverů

Pokud jste webovou stránku přidali do seznamu povolených serverů, protože jste chtěli mít ke stránce přístup, ale nyní chcete webovou stránku filtrovat, odeberte stránku ze seznamu povolených serverů.

1 Otevřete podokno Ochrana proti podvodné poště.

Jak?

1. Klepněte v podokně Domácí programu SecurityCenter na položku **Internet a sítě**.
2. Klepněte v informační části položky Internet a sítě na tlačítko **Konfigurovat**.

2 Klepněte v podokně Ochrana proti podvodné poště na položku **Upřesnit**.

3 Vyberte v části **Seznam povolených serverů** stránku, kterou chcete odebrat, a poté klepněte na tlačítko **Odebrat**.

Zakázání ochrany před podvodnými zprávami (phishing)

Pokud již máte software ochrany před podvodnými zprávami, který nepochází od společnosti McAfee, a dochází ke konfliktu, lze ochranu před podvodnými zprávami programu McAfee Anti-Spam zakázat.

1. V podokně Domácí programu SecurityCenter klepněte na položku **Internet a síť**.
2. V informačním podokně Internet a síť klepněte na tlačítko **Konfigurovat**.
3. V části **Ochrana před podvodnými zprávami (phishing) je povolena.** klepněte na možnost **Vypnout**.

Tip: Po dokončení nezapomeňte v části **Ochrana před podvodnými zprávami (phishing)** klepnout na tlačítko **Zapnout**, takže budete před podvodnými weby opět chráněni.

KAPITOLA 30

McAfee Parental Controls

Rodičovská kontrola obsahuje rozšířenou ochranu uživatele, rodiny, osobních souborů a počítače. Pomáhá chránit před krádežemi identity online, blokuje přenos osobních údajů a filtruje možný urážlivý obsah online (včetně obrázků). Umožňuje také sledovat, kontrolovat a zaznamenávat některé zvyky při procházení neověřených webů a poskytuje bezpečné úložiště osobních hesel.

Než začnete rodičovskou kontrolu používat, seznamte se blíže s některými jejími nejoblíbenějšími funkcemi. Podrobnosti o konfiguraci a používání těchto funkcí naleznete v nápovědě rodičovské kontroly.

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 rodičovské kontroly

Rodičovská kontrola	Uživatelům programu SecurityCenter slouží k filtrování potenciálně nevhodných obrázků, umožňuje vyhledávání odpovídající věku, konfiguraci věku uživatele (na jehož základě je určen blokovaný obsah) a omezení doby procházení Internetu (ve kterých dnech nebo hodinách má uživatel přístup k Internetu). Rodičovská kontrola umožní také všeobecně omezit přístup uživatelů k určitým webovým stránkám a udělit nebo blokovat přístup v závislosti na přiřazených klíčových slovech.
Ochrana osobních údajů	Blokujte přenos citlivých nebo důvěrných informací na webu (např. čísla platebních karet, čísla bankovních účtů, adresy atd.).
Trezor hesel	Umožňuje ukládat osobní hesla s jistotou, že k nim nebudou mít přístup žádní další uživatelé (ani správce).

KAPITOLA 31

Ochrana vašich dětí

Pokud počítač používají vaše děti, lze pomocí rodičovské kontroly omezit, co mohou děti při procházení Internetu vidět a dělat. Můžete například zapnout nebo vypnout vyhledávání odpovídající věku a filtrování obrázků, zvolit skupinu hodnocení obsahu a nastavit dobu trvání procházení Internetu.

Vyhledávání odpovídající věku zajistí, že jsou zapnuty bezpečnostní filtry některých oblíbených vyhledávacích stránek, takže jsou z výsledků vyhledávání vašeho dítěte automaticky vyloučeny potenciálně nevhodné položky; filtrování obrázků umožní blokovat zobrazení potenciálně nevhodných obrázků při procházení webu dětmi; hodnocení obsahu dle věkové kategorie uživatele stanoví druh obsahu webových stránek, které jsou dítěti přístupné v závislosti na jeho věkové skupině; doba trvání procházení Internetu stanoví dny a časový interval, po který má dítě přístup k Internetu. Určité webové stránky lze také pro všechny děti filtrovat (blokovat nebo povolit).

Poznámka: Chcete-li chránit své děti a nakonfigurovat rodičovskou kontrolu, musíte se přihlásit k počítači jako správce systému Windows. Pokud jste inovovali ze starší verze produktu McAfee a stále používáte uživatele McAfee, musíte se také ujistit, zda jste přihlášeni jako správce McAfee.

V této kapitole

Filtrování webových stránek pomocí klíčových slov

Klíčová slova vám umožní blokovat nedospělým uživatelům webové stránky s obsahem tvořeným potencionálně nevhodnými slovy. Je-li aktivována funkce filtrování pomocí klíčového slova, k posouzení obsahu pro uživatele dané skupiny je využíván standardní seznam klíčových slov a odpovídajících pravidel. Aby měli uživatelé přístup k webovým stránkám se specifickými klíčovými slovy, musí náležet do určité věkové skupiny. Např. pouze členové skupiny Dospělý mohou navštívit webové stránky obsahující slovo *porno* a pouze členové skupiny Dítě (nebo starší) mohou navštívit webové stránky obsahující slovo *drogy*.

Můžete však přidat vlastní klíčová slova a přidružit je k určitým věkovým skupinám. Přidaná pravidla klíčových slov potlačí pravidlo přidružené k odpovídajícímu klíčovému slovu ve výchozím seznamu.

Blokování webových serverů podle klíčových slov

Pokud chcete blokovat webové stránky vzhledem k jejich nepřiměřenému obsahu, ale neznáte přesnou adresu serveru, můžete webové stránky blokovat na základě klíčových slov. Jednoduše zadáte klíčové slovo a určíte, které věkové skupiny mohou a které nemohou zobrazovat webové servery obsahující toto slovo.

1 Otevřete podokno Rodičovská kontrola.

Jak?

1. V podokně Domácí programu SecurityCenter klepněte na položku **Rodičovská kontrola**.
2. V informační části funkce Rodičovská kontrola klepněte na tlačítko **Konfigurovat**.
3. V konfiguračním podokně Rodičovská kontrola zkontrolujte, zda je funkce Rodičovská kontrola povolena a klepněte na tlačítko **Upřesnit**.

2 V podokně Rodičovská kontrola, klepněte na tlačítko **Klíčová slova** a zkontrolujte, zda je filtrování povoleno.

3 Pod položkou **Seznam klíčových slov** zapište do pole **Vyhledat** klíčové slovo.

4 Přesunutím posuvníku **Minimální věk** určíte nejnižší věkovou skupinu.
Uživatelé v této skupině a starších skupinách budou moci zobrazovat webové stránky, které obsahují klíčové slovo.

5 Klepněte na tlačítko **OK**.

Zákaz filtrování klíčovými slovy

Je-li aktivována funkce filtrování pomocí klíčového slova, k posouzení obsahu pro uživatele dané skupiny je využíván standardně seznam klíčových slov a odpovídajících pravidel. Přestože to společnost McAfee nedoporučuje, můžete filtrování klíčovými slovy kdykoli zakázat.

1 Otevřete podokno Rodičovská kontrola.

   Jak?

   1. V podokně Domácí programu SecurityCenter klepněte na položku **Rodičovská kontrola**.
   2. V informační části funkce Rodičovská kontrola klepněte na tlačítko **Konfigurovat**.
   3. V konfiguračním podokně Rodičovská kontrola zkontrolujte, zda je funkce Rodičovská kontrola povolena a klepněte na tlačítko **Upřesnit**.

2 V podokně Rodičovská kontrola klepněte na tlačítko **Klíčová slova**.

3 V podokně Klíčová slova klepněte na položku **Vypnuto**.

4 Klepněte na tlačítko **OK**.

Filtrování webových stránek

Pro všechny uživatele vyjma skupiny Dospělý můžete filtrovat (zakázat nebo povolit) webové stránky. Blokováním webových stránek zabráníte dětem v přístupu a procházení webu. Při pokusu dítěte o přístup k blokovaným webovým stránkám se objeví zpráva, že tento server není přístupný, protože je blokován službou McAfee.

Pokud služba McAfee určitou webovou stránku ve výchozím nastavení blokuje, ale vy chcete přístup dětem k této stránce povolit, povolte tuto webovou stránku. Více informací týkajících se webových stránek, které jsou službou McAfee blokovány ve výchozím nastavení, naleznete v části Filtrování webových stránek pomocí klíčových slov (stránka 148). Filtrovaný webový server můžete kdykoli aktualizovat nebo odebrat.

Poznámka: Uživatelé (včetně správců), kteří náleží do skupiny Dospělý, mají přístup ke všem webům, i když byly blokovány. Chcete-li vyzkoušet blokované webové stránky, je třeba se přihlásit jako uživatel v jiné skupině než ve skupině Dospělý. Nezapomeňte ale po dokončení zkoušky vymazat historii procházení webového prohlížeče.

Odebrání filtrovaných webových stránek

V případě, že již není nutné blokovat nebo povolit filtrované webové stránky, můžete je odebrat.

1. Otevřete podokno Rodičovská kontrola.

   Jak?

   1. V podokně Domácí programu SecurityCenter klepněte na položku **Rodičovská kontrola**.
   2. V informační části funkce Rodičovská kontrola klepněte na tlačítko **Konfigurovat**.
   3. V konfiguračním podokně Rodičovská kontrola zkontrolujte, zda je funkce Rodičovská kontrola povolena a klepněte na tlačítko **Upřesnit**.

2. V podokně Rodičovská kontrola, klepněte na položku **Filtrované webové stránky**.
3. V podokně Filtrované webové stránky klepněte na položku v seznamu **Filtrované webové stránky** a klepněte na tlačítko **Odebrat**.
4. Klepněte na tlačítko **OK**.

Aktualizace filtrovaných webových stránek

Pokud se adresa webových stránek změní nebo ji při přidávání k seznamu Blokované webové stránky zadáte nesprávně, můžete ji aktualizovat.

1. Otevřete podokno Rodičovská kontrola.

   Jak?

   1. V podokně Domácí programu SecurityCenter klepněte na položku **Rodičovská kontrola**.
   2. V informační části funkce Rodičovská kontrola klepněte na tlačítko **Konfigurovat**.
   3. V konfiguračním podokně Rodičovská kontrola zkontrolujte, zda je funkce Rodičovská kontrola povolena a klepněte na tlačítko **Upřesnit**.

2. V podokně Rodičovská kontrola, klepněte na položku **Filtrované webové stránky**.
3. V podokně Filtrované webové stránky klepněte na položku ze seznamu **Filtrované webové stránky**, upravte adresu webového serveru v poli **http://** a klepněte na tlačítko **Aktualizovat**.
4. Klepněte na tlačítko **OK**.

Povolení webových stránek

Chcete-li se ujistit, že webové stránky nejsou pro žádného uživatele blokovány, povolte je. Povolíte-li webové stránky, které byly službou McAfee standardně blokovány, můžete standardní nastavení potlačit.

1 Otevřete podokno Rodičovská kontrola.

Jak?

1. V podokně Domácí programu SecurityCenter klepněte na položku **Rodičovská kontrola**.
2. V informační části funkce Rodičovská kontrola klepněte na tlačítko **Konfigurovat**.
3. V konfiguračním podokně Rodičovská kontrola zkontrolujte, zda je funkce Rodičovská kontrola povolena a klepněte na tlačítko **Upřesnit**.

2 V podokně Rodičovská kontrola, klepněte na položku **Filtrované webové stránky**.

3 V podokně Filtrované webové stránky zadejte do pole **http://** adresu webového serveru a klepněte na tlačítko **Povolit**.

4 Klepněte na tlačítko **OK**.

Tip: Dříve blokované weby můžete povolit klepnutím na webovou adresu v seznamu **Filtrované webové stránky** a poté klepnutím na položku **Povolit**.

Blokování webového serveru

Blokováním webových stránek zabráníte dětem v přístupu a procházení webu. Při pokusu dítěte o přístup k blokovaným webovým stránkám se objeví zpráva, že tento server není přístupný, neboť je blokován službou McAfee.

1. Otevřete podokno Rodičovská kontrola.

   Jak?

   1. V podokně Domácí programu SecurityCenter klepněte na položku **Rodičovská kontrola**.
   2. V informační části funkce Rodičovská kontrola klepněte na tlačítko **Konfigurovat**.
   3. V konfiguračním podokně Rodičovská kontrola zkontrolujte, zda je funkce Rodičovská kontrola povolena a klepněte na tlačítko **Upřesnit**.

2. V podokně Rodičovská kontrola, klepněte na položku **Filtrované webové stránky**.
3. V podokně Filtrované webové stránky zadejte do pole **http://** adresu webového serveru a klepněte na tlačítko **Blokovat**.
4. Klepněte na tlačítko **OK**.

Tip: Dříve povolené weby můžete blokovat klepnutím na webovou adresu v seznamu **Filtrované webové stránky** a poté klepnutím na položku **Blokovat**.

Nastavení časových omezení pro web

Jestliže jste znepokojeni nezodpovědným nebo přehnaným používáním Internetu, můžete nastavit časový limit procházení webu vašimi dětmi. Pokud časově omezíte procházení webu dětmi, můžete důvěřovat, že služba SecurityCenter tato omezení uplatní, i když jste mimo domov.

Standardně je dítěti povoleno procházení webu po celý den i i noc, sedm dní v týdnu, nicméně procházení webu můžete časově omezit na určité hodiny nebo dny, případně můžete procházení webu zcela zakázat. Pokud se dítě pokusí o připojení k Internetu mimo povolenou dobu, služba McAfee jej upozorní, že připojení k Internetu není k dispozici. Jestliže přístup k webu zcela zakážete, dítě se může přihlásit a počítač používat, včetně dalších internetových programů, např. e-mail, rychlého zasílání zpráv, ftp, her atd., ale nemůže procházet web.

Nastavení časových omezení procházení webu

K časovému omezení a stanovení určitých dní a hodin přístupu dítěte k webu můžete použít mřížku časového omezení.

1 Otevřete okno Uživatelská nastavení.

Jak?

1. V podokně Domácí programu SecurityCenter klepněte na položku **Rodičovská kontrola**.
2. V informační části funkce Rodičovská kontrola klepněte na tlačítko **Konfigurovat**.
3. V konfiguračním podokně Rodičovská kontrola klepněte na tlačítko **Upřesnit**.
4. V podokně Rodičovská kontrola klepněte na položku **Uživatelská nastavení**.

2 V podokně Uživatelská nastavení klepněte na uživatelské jméno a potom klepněte na tlačítko **Upravit**.

3 V okně Upravit uživatelský účet pod položkou **Časové omezení Internetu** stisknutím a přetažením pomocí myši určete dny a hodiny, během kterých může uživatel Internet používat.

4 Klepněte na tlačítko **OK**.

Nastavení hodnocení obsahu dle věkové kategorie

Uživatel může patřit do jedné z následujících skupin hodnocení obsahu:

- Malé dítě
- Dítě
- Mladší školní věk
- Starší školní věk
- Dospělý

Rodičovská kontrola obsah webů hodnotí (blokuje nebo povoluje) na základě skupiny, do které uživatel patří. To umožní povolit nebo zakázat určité webové stránky pro určité uživatele v domácnosti. Některý webový obsah lze například blokovat uživatelům, kteří patří do skupiny Malé dítě, ale povolit pro uživatele, kteří patří do skupiny Mladší školní věk. Chcete-li hodnotit obsah pro uživatele přísněji, můžete zabránit uživatelům v prohlížení webových stránek, které nejsou povoleny v seznamu **Filtrované webové stránky**. Další informace najdete v tématu Filtrování webových stránek (stránka 149).

Nastavení skupiny hodnocení obsahu uživatele

Ve výchozím nastavení je nový uživatel přidán do skupiny Dospělý, která uživateli umožní přístup k celému obsahu webu. Potom můžete nastavit hodnocení obsahu dle věkové kategorie uživatele podle věku a úrovně vyspělosti uživatele.

1 Otevřete okno Uživatelská nastavení.

Jak?

1. V podokně Domácí programu SecurityCenter klepněte na položku **Rodičovská kontrola**.
2. V informační části funkce Rodičovská kontrola klepněte na tlačítko **Konfigurovat**.
3. V konfiguračním podokně Rodičovská kontrola klepněte na tlačítko **Upřesnit**.
4. V podokně Rodičovská kontrola klepněte na položku **Uživatelská nastavení**.

2 V podokně Uživatelská nastavení klepněte na uživatelské jméno a potom klepněte na tlačítko **Upravit**.

3 V okně Upravit uživatelský účet pod položkou **Hodnocení obsahu** klepněte na věkovou skupinu, kterou chcete uživateli přiřadit.

Chcete-li uživateli zamezit v prohlížení webových stránek, které nejsou uvedeny v seznamu **Filtrované webové stránky**, zaškrtněte políčko **Tento uživatel má přístup pouze k serverům ze seznamu Povolené webové servery.**

4 Klepněte na tlačítko **OK**.

Filtrování potenciálně nevhodných webových obrázků

V závislosti na věku nebo úrovni vyspělosti uživatele procházejícího webové stránky můžete filtrovat (zakázat nebo povolit) potenciálně nevhodné obrázky. Např. lze blokovat zobrazení potenciálně nevhodných obrázků, jestliže malé děti prochází web, ale současně umožnit starším dětem nebo dospělým zobrazení těchto obrázků. Standardně je filtrování obrázků zakázáno pro všechny uživatele skupiny Dospělý. Znamená to, že potenciálně nevhodné obrázky jsou pro tyto uživatele při procházení webu viditelné. Další informace o nastavení věkové skupiny uživatele naleznete v tématu Nastavení skupiny hodnocení obsahu uživatele (stránka 154).

Filtrování potenciálně nevhodných webových obrázků

Nový uživatel je standardně přidán do skupiny Dospělý a filtrování obrázku je zakázáno. Chcete-li zabránit zobrazení potenciálně nevhodných obrázků určitému uživateli procházejícímu web, můžete filtrování obrázků povolit. Každý potenciálně nevhodný webový obrázek je automaticky nahrazen statickým obrázkem programu McAfee.

1 Otevřete okno Uživatelská nastavení.

Jak?

1. V podokně Domácí programu SecurityCenter klepněte na položku **Rodičovská kontrola**.
2. V informační části funkce Rodičovská kontrola klepněte na tlačítko **Konfigurovat**.
3. V konfiguračním podokně Rodičovská kontrola klepněte na tlačítko **Upřesnit**.
4. V podokně Rodičovská kontrola klepněte na položku **Uživatelská nastavení**.

2 V podokně Uživatelská nastavení klepněte na uživatelské jméno a potom klepněte na tlačítko **Upravit**.

3 V okně Upravit uživatelský účet pod položkou **Filtrování obrázků**, klepněte na volbu **Zapnuto**.

4 Klepněte na tlačítko **OK**.

Povolení vyhledávání odpovídajícího věku

Některé oblíbené vyhledávací weby (jako jsou Yahoo! nebo Google) nabízí možnost „bezpečného vyhledávání“. Jedná se o nastavení vyhledávání, které zabraňuje, aby se v seznamech výsledků objevily potencionálně nevhodné výsledky vyhledávání. Tyto vyhledávací weby obvykle umožňují vybrat míru omezení pro filtrování pomocí bezpečného vyhledávání, zároveň také umožňují vám nebo dalším uživatelům toto vyhledávání kdykoliv vypnout.

Vyhledávání odpovídající věku představuje v rámci rodičovské kontroly praktický způsob, jak zajistit, že je „bezpečné vyhledávání“ při použití jednoho z následujících vyhledávacích webů pro uživatele vždy zapnuto:

- Google™
- MSN®
- Windows® Live Search
- Yahoo!®

Pokud zapnete vyhledávání odpovídající věku, zajistíme, že budou filtry bezpečného vyhledávání vyhledávacích webů pro tohoto uživatele zapnuty a nastaveny na nejvyšší míru omezení. Pokud se uživatel pokusí tyto filtry v předvolbách vyhledávacího webu nebo v rozšířených nastaveních vypnout, opět je automaticky zapneme.

Ve výchozím nastavení je vyhledávání odpovídající věku zapnuto pro všechny uživatele s výjimkou správců a uživatelů ve věkové skupině Dospělý. Další informace o nastavení věkové skupiny uživatele naleznete v tématu Nastavení hodnocení obsahu dle věkové kategorie (stránka 154).

Povolení vyhledávání odpovídajícího věku

Noví uživatelé jsou standardně přidáni do skupiny Dospělý a vyhledávání odpovídající věku je zakázáno. Pokud chcete zajistit, aby bylo filtrování pomocí bezpečného vyhledávání nabízené oblíbenými vyhledávacími weby zapnuto i pro uživatele skupiny Dospělý, lze povolit vyhledávání odpovídající věku.

1 Otevřete okno Uživatelská nastavení.

Jak?

1. V podokně Domácí programu SecurityCenter klepněte na položku **Rodičovská kontrola**.
2. V informační části funkce Rodičovská kontrola klepněte na tlačítko **Konfigurovat**.
3. V konfiguračním podokně Rodičovská kontrola klepněte na tlačítko **Upřesnit**.
4. V podokně Rodičovská kontrola klepněte na položku **Uživatelská nastavení**.

2 V podokně Uživatelská nastavení klepněte na uživatelské jméno a potom klepněte na tlačítko **Upravit**.

3 V okně Upravit uživatelský účet pod položkou **Vyhledávání odpovídající věku**, klepněte na volbu **Zapnuto**.

4 Klepněte na tlačítko **OK**.

KAPITOLA 32

Konfigurace uživatelů

Chcete-li chránit své děti a nakonfigurovat rodičovskou kontrolu, je třeba dětem v programu SecurityCenter přiřadit určitá oprávnění. Tato oprávnění určují, co může jednotlivé dítě na webu vidět a co tam může dělat.

Uživatelé programu SecurityCenter odpovídají ve výchozím nastavení uživatelům systému Windows, které jste v počítači nastavili. Inovujete-li předchozí verzi programu SecurityCenter, která obsahuje uživatele McAfee, uživatelé McAfee a jejich oprávnění zůstanou zachováni.

Poznámka: Chcete-li nastavit uživatele, musíte se k počítači přihlásit jako správce systému Windows. Pokud jste inovovali ze starší verze produktu McAfee a stále používáte uživatele McAfee, musíte se také ujistit, zda jste přihlášeni jako správce McAfee.

V této kapitole

Práce s uživateli McAfee

Inovujete-li předchozí verzi programu SecurityCenter, která obsahuje uživatele McAfee, uživatelé McAfee a jejich oprávnění zůstanou automaticky zachováni. I když lze i nadále konfigurovat a spravovat uživatele McAfee, doporučuje společnost McAfee začít používat uživatele systému Windows. Po přepnutí na uživatele systému Windows nelze přepnout zpět na uživatele McAfee.

Budete-li pokračovat v používání uživatelů McAfee, můžete uživatele přidat, upravit nebo odebrat, případně změnit nebo získat heslo správce McAfee.

Načtení hesla správce McAfee

Pokud zapomenete heslo správce, můžete je obnovit.

1. Klepněte pravým tlačítkem na ikonu programu SecurityCenter a potom klepněte na položku **Přepnout uživatele**.
2. V seznamu **Uživatelské jméno** vyberte možnost **Správce** a potom klepněte na tlačítko **Zapomenuté heslo**.
3. Do pole **Odpověď** zadejte odpověď na tajnou otázku.
4. Klepněte na tlačítko **Odeslat**.

Změna hesla správce McAfee

Pokud si nemůžete zapamatovat heslo správce McAfee nebo máte podezření, že může být ohroženo, změňte jej.

1. Do programu SecurityCenter se přihlaste jako správce.
2. Otevřete okno Uživatelská nastavení.

   Jak?

   1. V části **Běžné úlohy** klepněte na tlačítko **Domácí**.
   2. V podokně Domácí programu SecurityCenter klepněte na položku **Rodičovská kontrola**.
   3. V informační části funkce Rodičovská kontrola klepněte na tlačítko **Konfigurovat**.
   4. V konfiguračním podokně Rodičovská kontrola klepněte na tlačítko **Upřesnit**.
3. V podokně Uživatelská nastavení pod položkou **Uživatelské účty McAfee** zvolte položku **Správce** a potom klepněte na tlačítko **Upravit**.
4. V dialogovém okně Upravit uživatelský účet zadejte nové heslo do pole **Nové heslo** a potom ještě jednou do pole **Potvrdit nové heslo**.
5. Klepněte na tlačítko **OK**.

Odebrání uživatele McAfee

Odebrání uživatele McAfee můžete provést kdykoliv.

Při odebírání uživatele McAfee postupujte takto:

1. Log in to SecurityCenter as the Administrator user.
2. Otevřete okno Uživatelská nastavení.

   Jak?

   1. V části **Běžné úlohy** klepněte na tlačítko **Domácí**.
   2. V podokně Domácí programu SecurityCenter klepněte na položku **Rodičovská kontrola**.
   3. V informační části funkce Rodičovská kontrola klepněte na tlačítko **Konfigurovat**.
   4. V konfiguračním podokně Rodičovská kontrola klepněte na tlačítko **Upřesnit**.
3. V podokně Uživatelská nastavení pod položkou **Uživatelské účty McAfee** zvolte uživatelské jméno a potom klepněte na tlačítko **Odebrat**.

úprava uživatelského účtu McAfee

Můžete změnit uživatelské heslo McAfee, typ účtu nebo možnost automatického přihlášení.

1. Do programu SecurityCenter se přihlaste jako správce.
2. Otevřete okno Uživatelská nastavení.

   Jak?

   1. V části **Běžné úlohy** klepněte na tlačítko **Domácí**.
   2. V podokně Domácí programu SecurityCenter klepněte na položku **Rodičovská kontrola**.
   3. V informační části funkce Rodičovská kontrola klepněte na tlačítko **Konfigurovat**.
   4. V konfiguračním podokně Rodičovská kontrola klepněte na tlačítko **Upřesnit**.
3. V podokně Uživatelská nastavení klepněte na uživatelské jméno a potom klepněte na tlačítko **Upravit**.
4. Při úpravě uživatelského hesla, typu účtu a ochrany rodičovské kontroly postupujte podle pokynů na obrazovce.
5. Klepněte na tlačítko **OK**.

Přidání uživatele McAfee

Po vytvoření uživatele McAfee můžete pro tohoto uživatele nastavit ochranu rodičovské kontroly. Další informace naleznete v nápovědě rodičovské kontroly.

1. Do programu SecurityCenter se přihlaste jako správce.
2. Otevřete okno Uživatelská nastavení.

   Jak?

   1. V části **Běžné úlohy** klepněte na tlačítko **Domácí**.
   2. V podokně Domácí programu SecurityCenter klepněte na položku **Rodičovská kontrola**.
   3. V informační části funkce Rodičovská kontrola klepněte na tlačítko **Konfigurovat**.
   4. V konfiguračním podokně Rodičovská kontrola klepněte na tlačítko **Upřesnit**.
3. V podokně Uživatelská nastavení klepněte na položku **Přidat**.
4. Při nastavení uživatelského jména, hesla, typu účtu a ochrany rodičovské kontroly postupujte podle pokynů na obrazovce.
5. Klepněte na tlačítko **Vytvořit**.

Přepnutí na uživatele systému Windows

Společnost McAfee doporučuje z důvodu jednoduché údržby přepnout na uživatele systému Windows. Po přepnutí se ale nelze vrátit zpět k uživatelům McAfee.

1. Otevřete okno Uživatelská nastavení.

   Jak?

   1. V části **Běžné úlohy** klepněte na tlačítko **Domácí**.
   2. V podokně Domácí programu SecurityCenter klepněte na položku **Rodičovská kontrola**.
   3. V informační části funkce Rodičovská kontrola klepněte na tlačítko **Konfigurovat**.
   4. V konfiguračním podokně Rodičovská kontrola klepněte na tlačítko **Upřesnit**.
2. V podokně Uživatelská nastavení vyberte položku **Přepnout**.
3. Potvrďte operaci.

Práce s uživateli systému Windows

Uživatelé programu SecurityCenter odpovídají ve výchozím nastavení uživatelům systému Windows, které jste v počítači nastavili. Uživatele můžete přidat, upravit informace o účtu uživatele nebo uživatele odebrat ve Správě počítače systému Windows. Potom můžete pro tyto uživatele v programu SecurityCenter nastavit ochranu rodičovské kontroly.

Inovujete-li předchozí verzi programu SecurityCenter, která obsahuje uživatele McAfee, podrobnosti naleznete v části Práce s uživateli McAfee (stránka 160).

KAPITOLA 33

Ochrana informací na webu

Přidáním osobních údajů (jako je například jméno, adresa, čísla kreditních karet a čísla bankovních účtů) k oblasti chráněných informací můžete zabránit jejich přenosu prostřednictvím webu.

Poznámka: Rodičovská kontrola neblokuje přenos osobních údajů u zabezpečených webových stránek (tzn. webových stránek používajících protokol https://), například u stránek bank.

V této kapitole

Ochrana osobních údajů

Přidáním osobních údajů (jako je například jméno, adresa, čísla kreditních karet a čísla bankovních účtů) k oblasti blokovaných informací můžete zabránit v jejich přenosu prostřednictvím webu. Jestliže služba McAfee zjistí, že cokoliv, co má být odesláno prostřednictvím webu, obsahuje osobní údaje (např. pole formuláře, souboru), zobrazí se následující zpráva:

- Jste-li správce, musíte potvrdit, zda mají být informace odeslány.
- Nejste-li správce, blokovaná informace bude nahrazena hvězdičkami (*). Např. pokud se podvodný webový server pokouší odeslat číslo kreditní karty jinému počítači, číslo samo o sobě je nahrazeno hvězdičkami.

Ochrana osobních údajů

Můžete blokovat následující typy osobních údajů: jméno, adresa, poštovní směrovací číslo, rodné číslo, telefonní číslo, číslo kreditní karty, bankovního účtu, makléřského účtu a telefonních karet. Pokud chcete blokovat osobní údaje jiných typů, můžete typ nastavit na hodnotu **ostatní**.

1 Otevřete podokno Chráněné informace.

Jak?

1. V části **Běžné úlohy** klepněte na tlačítko **Domácí**.
2. V podokně Domácí programu SecurityCenter klepněte na položku **Internet a síť**.
3. V informační části Internet a síť klepněte na tlačítko **Konfigurovat**.
4. V podokně Konfigurace Internetu a sítě zkontrolujte, zda je funkce Chráněné informace povolena a klepněte na tlačítko **Upřesnit**.

2 V podokně Chráněné informace klepněte na položku **Přidat**.

3 V seznamu vyberte typ informací, které chcete blokovat.

4 Zadejte příslušné informace a pak klepněte na tlačítko **OK**.

KAPITOLA 34

Ochrana hesel

Trezor hesel představuje bezpečné úložiště osobních hesel. Umožňuje ukládat hesla s jistotou, že k nim nebudou mít přístup žádní další uživatelé (ani správce).

V této kapitole

Nastavení trezoru hesel

Před použitím trezoru hesel je nutné nastavit heslo trezoru hesel. Pouze uživatelé, kteří znají toto heslo, budou moci trezor hesel používat. Zapomenete-li heslo trezoru hesel, můžete je obnovit. Všechna hesla, která jste doposud v trezoru hesel uložili, budou však odstraněna.

Po nastavení hesla trezoru hesel můžete hesla přidat, upravit nebo z trezoru odebrat. Heslo můžete v trezoru hesel kdykoli změnit.

Obnovení hesla trezoru hesel

Zapomenete-li heslo trezoru hesel, můžete je obnovit. Všechna hesla, která jste doposud v trezoru hesel uložili, budou však odstraněna.

1 Otevřete podokno Trezor hesel.

   Jak?

   1. V části **Běžné úlohy** klepněte na tlačítko **Domácí**.
   2. V podokně Domácí programu SecurityCenter klepněte na položku **Internet a síť**.
   3. V informační části Internet a síť klepněte na tlačítko **Konfigurovat**.
   4. V podokně Konfigurace Internetu a sítě klepněte v části **Trezor hesel** na tlačítko **Upřesnit** .

2 Klepněte na položku **Zapomněli jste heslo?**.

3 Zadejte v dialogovém okně Obnovit trezor hesel do pole **Heslo** nové heslo a poté heslo znovu přepište do pole **Potvrdit heslo**.

4 Klepněte na tlačítko **Obnovit**.

5 V dialogovém okně Potvrzení obnovení hesla klepněte na tlačítko **Ano**.

Změna hesla trezoru hesel

Heslo můžete v trezoru hesel kdykoli změnit.

1 Otevřete podokno Trezor hesel.

   Jak?

   1. V části **Běžné úlohy** klepněte na tlačítko **Domácí**.
   2. V podokně Domácí programu SecurityCenter klepněte na položku **Internet a síť**.
   3. V informační části Internet a síť klepněte na tlačítko **Konfigurovat**.
   4. V podokně Konfigurace Internetu a sítě klepněte v části **Trezor hesel** na tlačítko **Upřesnit** .

2 V podokně Trezor hesel zadejte do pole **Heslo** aktuální heslo a potom klepněte na tlačítko **Otevřít**.

3 V podokně Spravovat trezor hesel klepněte na tlačítko **Změnit heslo**.

4 Nové heslo trezoru hesel zadejte do pole **Zvolte heslo** a znovu je zadejte do pole **Potvrdit heslo**.

5 Klepněte na tlačítko **OK**.

6 V dialogovém okně Došlo ke změně hesla Trezoru hesel klepněte na tlačítko **OK**.

Odstranění hesla

Heslo můžete z trezoru hesel kdykoli odebrat. Heslo, které z trezoru hesel odeberete, nelze nijak obnovit.

1 Otevřete podokno Trezor hesel.

   Jak?

   1. V části **Běžné úlohy** klepněte na tlačítko **Domácí**.
   2. V podokně Domácí programu SecurityCenter klepněte na položku **Internet a síť**.
   3. V informační části Internet a síť klepněte na tlačítko **Konfigurovat**.
   4. V podokně Konfigurace Internetu a sítě klepněte v části **Trezor hesel** na tlačítko **Upřesnit** .

2 Do pole **Heslo** zadejte heslo trezoru hesel.

3 Klepněte na tlačítko **Otevřít**.

4 V podokně Spravovat trezor hesel klepněte na položku hesla a následně klepněte na tlačítko **Odebrat**.

5 V dialogovém okně Potvrzení odebrání klepněte na tlačítko **Ano**.

Úprava hesla

Aby bylo zajištěno, že položky v trezoru hesel jsou vždy přesné a spolehlivé, je nutné je aktualizovat, jakmile se heslo změní.

1 Otevřete podokno Trezor hesel.

   Jak?

   1. V části **Běžné úlohy** klepněte na tlačítko **Domácí**.
   2. V podokně Domácí programu SecurityCenter klepněte na položku **Internet a síť**.
   3. V informační části Internet a síť klepněte na tlačítko **Konfigurovat**.
   4. V podokně Konfigurace Internetu a sítě klepněte v části **Trezor hesel** na tlačítko **Upřesnit** .

2 Do pole **Heslo** zadejte heslo trezoru hesel.

3 Klepněte na tlačítko **Otevřít**.

4 V podokně Spravovat trezor hesel klepněte na položku hesla a klepněte na tlačítko **Upravit**.

5 V poli **Popis** upravte popis hesla (například k čemu heslo slouží) a v poli **Heslo** heslo upravte.

6 Klepněte na tlačítko **OK**.

Přidání hesla

Činí-li vám potíže pamatovat si hesla, můžete je přidat do trezoru hesel. Trezor hesel je bezpečné místo, kam mohou přistupovat pouze uživatelé, kteří znají heslo trezoru hesel.

1 Otevřete podokno Trezor hesel.

Jak?

1. V části **Běžné úlohy** klepněte na tlačítko **Domácí**.
2. V podokně Domácí programu SecurityCenter klepněte na položku **Internet a síť**.
3. V informační části Internet a síť klepněte na tlačítko **Konfigurovat**.
4. V podokně Konfigurace Internetu a sítě klepněte v části **Trezor hesel** na tlačítko **Upřesnit** .

2 Do pole **Heslo** zadejte heslo trezoru hesel.

3 Klepněte na tlačítko **Otevřít**.

4 V podokně Spravovat trezor hesel klepněte na tlačítko **Přidat**.

5 Do pole **Popis** zadejte popis hesla (například k čemu heslo slouží) a heslo zadejte do pole **Heslo**.

6 Klepněte na tlačítko **OK**.

KAPITOLA 35

McAfee Backup and Restore

Aplikace McAfee® Backup and Restore zabraňuje náhodné ztrátě dat archivací souborů na disky CD, DVD, jednotku USB, externí pevný disk nebo síťovou jednotku. Místní archivace umožňuje osobní data archivovat (zálohovat) na disky CD, DVD, jednotku USB, externí pevný disk nebo síťovou jednotku. Tato funkce ochrání místní záznamy, dokumenty a jiné materiály osobní povahy před náhodnou ztrátou.

Než začnete používat aplikaci Backup and Restore, seznamte se blíže s některými jejími nejoblíbenějšími funkcemi. Podrobnosti o konfiguraci a používání těchto funkcí naleznete v nápovědě aplikace Backup and Restore. Až projdete funkce programu, zkontrolujte, zda máte dostupné odpovídající archivační médium k provedení místní archivace.

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 aplikace Backup and Restore

Místní naplánovaná archivace	Ochraňte svá data archivací souborů a složek na disk CD, DVD, jednotku USB, externí pevný disk nebo síťovou jednotku. Po založení prvního archivu se budou automaticky tvořit přírůstkové archivy.
Obnovení jedním klepnutím myší	Dojde-li omylem k odstranění nebo poškození souborů či složek v počítači, můžete je obnovit z jejich nedávno archivované verze.
Komprese a šifrování	Ve výchozím stavu jsou archivované soubory komprimovány, a tím dochází k ušetření místa na archivačním médiu. Dodatečným bezpečnostním opatřením je ve výchozím stavu zapnuté šifrování archivů.

KAPITOLA 36

Archivace souborů

Aplikaci McAfee Backup and Restore můžete použít k archivaci kopie souborů ve svém počítači na disky CD, DVD, jednotku USB, externí pevný disk nebo síťovou jednotku. Archivace souborů tímto způsobem zjednodušuje opětovné načtení informací v případě náhodné ztráty či poškození dat.

Než začnete soubory archivovat, je třeba zvolit výchozí umístění archivu (disk CD, DVD, jednotka USB, síťová jednotka nebo externí pevný disk). Společnost McAfee předvolila některá další nastavení, například složky a archivované typy souborů. Tato nastavení lze však změnit.

Po nastavení možností místní archivace můžete upravit výchozí nastavení toho, jak často bude aplikace Backup and Restore spouštět úplné nebo rychlé archivace. Ruční archivace můžete spustit kdykoli.

V této kapitole

Povolení a zakázání místní archivace

V závislosti na způsobu používání zálohování a obnovení můžete při prvním spuštění zálohování a obnovení rozhodnout, zda chcete povolit nebo zakázat místní archivaci. Jakmile se přihlásíte a začnete používat zálohování a obnovení, lze místní archivaci kdykoli povolit nebo zakázat.

Pokud nechcete kopii svých souborů v počítači archivovat na disk CD, DVD, jednotku USB, externí pevný disk nebo síťovou jednotku, lze místní archivaci zakázat.

Povolení místní archivace

Pokud chcete kopie souborů ve svém počítači archivovat na disky CD, DVD, jednotku USB, externí pevný disk nebo síťovou jednotku, povolte místní archivaci.

1. V programu SecurityCenter v části **Rozšířená nabídka** klepněte na příkaz **Konfigurovat**.
2. V konfiguračním podokně klepněte na položku **Počítač a soubory**.
3. V konfiguračním podokně Počítač a soubory klepněte v části **Místní archivace je zakázána** na možnost **Zapnout**.

Zakázání místní archivace

Pokud nechcete kopie souborů ve svém počítači archivovat na disky CD, DVD, jednotku USB, externí pevný disk nebo síťovou jednotku, zakažte místní archivaci.

1. V programu SecurityCenter v části **Rozšířená nabídka** klepněte na příkaz **Konfigurovat**.
2. V konfiguračním podokně klepněte na položku **Počítač a soubory**.
3. V konfiguračním podokně Počítač a soubory klepněte v části **Místní archivace je povolena** na možnost **Vypnout**.

Nastavení možností archivace

Než začnete archivovat soubory, musíte nastavit některé možnosti místní archivace. Například je třeba nastavit sledovaná umístění a sledované typy souborů. Sledovaná umístění jsou složky v počítači, ve kterých aplikace Backup and Restore sleduje vznik nových souborů nebo změny ve stávajících souborech. Sledované typy souborů jsou typy souborů (například .doc, .xls a podobně), které aplikace Backup and Restore ve sledovaných umístěních archivuje. Ve výchozím nastavení jsou archivovány následující typy souborů (můžete ovšem archivovat i jiné typy souborů).

- Dokumenty aplikace Microsoft® Word (.doc, .docx)
- Tabulky aplikace Microsoft Excel® (.xls, .xlsx)
- Prezentace aplikace Microsoft PowerPoint® (.ppt, .pptx)
- Soubory aplikace Microsoft Project® (.mpp)
- Soubory .pdf Adobe®
- Textové soubory .TXT
- Soubory HTML (.html)
- Soubory skupiny Joint Photographic Experts Group (.jpg, .jpeg)
- Soubor TIF (Tagged Image Format)
- Zvukový datový proud formátu MPEG III (.mp3)
- Soubory videa (.vdo)

Poznámka: Následující typy souborů nelze archivovat: .ost, a .pst.

Můžete nastavit dva typy sledovaného umístění: složky nejvyšší úrovně a podsložky nebo pouze složky nejvyšší úrovně. Pokud nastavíte umístění složek nejvyšší úrovně a podsložek, bude aplikace Backup and Restore archivovat sledované typy souborů v této složce a jejích podsložkách. Pokud nastavíte umístění složek nejvyšší úrovně, bude aplikace Backup and Restore archivovat sledované typy souborů pouze v této složce (a ne v jejích podsložkách). Lze také určit umístění, která chcete z místní archivace vyloučit. Ve výchozím nastavení jsou jako sledovaná umístění složek a podsložek nejvyšší úrovně nastavena plocha systému Windows a složka Dokumenty.

Po nastavení sledovaných typů souborů a sledovaných umístění musíte nastavit umístění archivu (tj. disk CD, DVD, jednotka USB, síťová jednotka nebo externí pevný disk). Do něj budou archivovaná data ukládána. Umístění archivu můžete kdykoli změnit.

Z bezpečnostních důvodů a kvůli snížení velikosti je ve výchozím nastavení povoleno šifrování a komprimace archivovaných souborů. Obsah šifrovaných souborů je převeden z textové podoby do kódu. To učiní informace nečitelné pro osoby, které nevědí, jak je dešifrovat. Soubory jsou komprimovány do podoby minimalizující požadavky na místo pro uložení nebo na přenos. Přestože to společnost McAfee nedoporučuje, můžete šifrování a komprimaci kdykoli zakázat.

Přidání umístění do archivu

Pro archivaci můžete nastavit dva typy sledovaného umístění: složky nejvyšší úrovně a podsložky nebo pouze složky nejvyšší úrovně. Pokud nastavíte umístění složek nejvyšší úrovně a podsložek, sleduje aplikace Backup and Restore změny obsahu v této složce a jejích podsložkách. Pokud nastavíte umístění nejvyšších složek, sleduje aplikace Backup and Restore pouze obsah složky (a ne jejích podsložek).

1. Otevřete dialogové okno Nastavení místní archivace.

   Jak?

   1. Klepněte na kartu **Místní archivace**.
   2. V levém podokně klepněte na položku **Nastavení**.

2. Klepněte na položku **Sledovat umístění**.
3. Proveďte jednu z následujících akcí:
   - Chcete-li archivovat obsah složky včetně obsahu jejích podsložek, klepněte na tlačítko **Přidat složku** v části **Archivovat složky a podsložky nejvyšší úrovně**.
   - Chcete-li archivovat obsah složky avšak ne obsah jejích podsložek, klepněte na tlačítko **Přidat složku** v části **Archivovat složky nejvyšší úrovně**.
   - Chcete-li archivovat celý soubor, klepněte v části **Archivovat složky nejvyšší úrovně** na možnost **Přidat soubor**.
4. V dialogovém okně Vyhledat složku (nebo Otevřít) přejděte do složky (nebo k souboru), kterou chcete sledovat, a klepněte na tlačítko **OK**.
5. Klepněte na tlačítko **OK**.

Tip: Pokud chcete, aby aplikace Backup and Restore sledovala složku, která dosud nebyla vytvořena, můžete přidat složku a zároveň ji nastavit jako sledované umístění klepnutím na tlačítko **Vytvořit novou složku** v dialogovém okně Vyhledat složku.

Nastavení typů archivovaných souborů

Můžete určit typy souborů, které budou archivovány v rámci umístění složek nejvyšší úrovně a jejich podsložek nebo složek nejvyšší úrovně. Je možné zvolit z již existujícího seznamu typů souborů nebo do tohoto seznamu přidat další typy.

1. Otevřete dialogové okno Nastavení místní archivace.

   Jak?

   1. Klepněte na kartu **Místní archivace**.
   2. V levém podokně klepněte na položku **Nastavení**.

2 Klepněte na možnost **Typy souborů**.

3 Rozbalte seznamy typů souborů a zaškrtněte políčka vedle typů souborů, které chcete archivovat.

4 Klepněte na tlačítko **OK**.

Tip: Chcete-li do seznamu **Vybrané typy souborů** přidat nový typ souboru, zadejte příponu typu souboru do pole **Přidat vlastní typ souboru k souborům Ostatní**, klepněte na tlačítko **Přidat** a poté na tlačítko **OK**. Nový typ souboru se automaticky stane sledovaným typem.

Vyloučení umístění z archivu

Umístění je vhodné vyloučit z archivu v případě, že toto umístění (složku) a jeho obsah nechcete archivovat.

1 Otevřete dialogové okno Nastavení místní archivace.

Jak?

1. Klepněte na kartu **Místní archivace**.
2. V levém podokně klepněte na položku **Nastavení**.

2 Klepněte na položku **Sledovat umístění**.

3 V části **Složky vyloučené ze zálohování** klepněte na možnost **Přidat složku**.

4 V dialogovém okně Vyhledat složku přejděte na složku, kterou si přejete vyloučit, a klepněte na tlačítko **OK**.

5 Klepněte na tlačítko **OK**.

Tip: Pokud chcete, aby aplikace Backup and Restore vyloučila složku, která dosud nebyla vytvořena, můžete přidat složku a zároveň ji tím vyloučit klepnutím na tlačítko **Vytvořit novou složku** v dialogovém okně Vyhledat složku.

Změna umístění archivu

Změníte-li umístění archivu, budou soubory naposledy archivované v jiném umístění vypsány jako *Nikdy nearchivováno*.

1 Otevřete dialogové okno Nastavení místní archivace.

Jak?

1. Klepněte na kartu **Místní archivace**.
2. V levém podokně klepněte na položku **Nastavení**.

2 Klepněte na položku **Změnit umístění archivu**.

3 V dialogovém okně Umístění archivu proveďte jednu z následujících akcí:

- Klepněte na položku **Vybrat zapisovací jednotku CD/DVD**, klepněte na jednotku CD nebo DVD počítače v seznamu **Zapisovací jednotka** a potom na tlačítko **OK**.
- Klepněte na položku **Vybrat umístění jednotky**, přejděte na jednotku USB, místní nebo externí pevný disk, vyberte zvolenou jednotku a klepněte na tlačítko **OK**.
- Klepněte na položku **Vybrat umístění v síti**, přejděte na síťovou složku, vyberte ji a klepněte na tlačítko **OK**.

4 Ověřte nové umístění archivu v části **Vybrané umístění archivu** a klepněte na tlačítko **OK**.

5 V potvrzovacím dialogovém okně klepněte na tlačítko **OK**.

6 Klepněte na tlačítko **OK**.

Poznámka: Změníte-li umístění archivu, budou dříve archivované soubory uvedeny jako **Nearchivováno** ve sloupci **Stav**.

Zakázání šifrování a komprimace archivu

šifrování archivovaných souborů chrání diskrétnost vašich dat zakódováním obsahu souborů tak, že se stanou nečitelnými. Komprimace archivovaných souborů pomáhá minimalizovat velikost souborů. Ve výchozím nastavení jsou šifrování i komprimace zapnuty, můžete je však kdykoli zakázat.

1 Otevřete dialogové okno Nastavení místní archivace.

Jak?

1. Klepněte na kartu **Místní archivace**.
2. V levém podokně klepněte na položku **Nastavení**.

2 Klepněte na možnost **Rozšířená nastavení**.

3 Zrušte zaškrtnutí políčka **Zvýšit zabezpečení povolením šifrování**.

4 Zrušte zaškrtnutí políčka **Snížit velikost úložiště povolením komprimace**.

5 Klepněte na tlačítko **OK**.

Poznámka: Společnost McAfee doporučuje při archivaci souborů šifrování a komprimaci nezakazovat.

Spouštění úplné a rychlé archivace

Můžete spustit dva typy archivace: úplnou nebo rychlou. Spustíte-li úplnou archivaci, archivují se všechna data vyhovující vámi nastaveným sledovaným typům souborů a umístěním. Pokud spustíte rychlou archivaci, budou archivovány pouze sledované soubory změněné od poslední úplné nebo rychlé aktualizace.

Ve výchozím nastavení má aplikace McAfee Backup and Restore naplánováno spouštění úplné archivace sledovaných typů souborů ve sledovaných umístěních na každé pondělí v 9:00 a spouštění rychlé archivace každých 48 hodin po poslední úplné nebo rychlé archivaci. Tento rozvrh zajišťuje přístupnost vždy aktuálního archivu souborů. Pokud nechcete archivaci spouštět každých 48 hodin, naplánujte si ji podle vlastních potřeb.

Chcete-li obsah sledovaných umístění archivovat na požádání, můžete tak učinit kdykoli. Pokud například změníte soubor a chcete ho archivovat, přestože aplikace Backup and Restore nebude v příštích několika hodinách provádět úplnou ani rychlou archivaci, můžete soubory archivovat ručně. Při ručním spuštění archivace je nastavený časový interval do spuštění automatické archivace vynulován.

Můžete také automatickou nebo ruční archivaci přerušit, spustí-li se v nevhodném okamžiku. Provádíte-li například úlohu intenzivně využívající prostředky počítače a spustí-li se automatická archivace, můžete ji zastavit. Při zastavení automatické archivace je nastavený časový interval do spuštění příští automatické archivace vynulován.

Naplánování automatické archivace

Můžete nastavit frekvenci spouštění úplné a rychlé archivace a zajistit tak, že vaše data budou chráněna.

1. Otevřete dialogové okno Nastavení místní archivace.

   Jak?

   1. Klepněte na kartu **Místní archivace**.
   2. V levém podokně klepněte na položku **Nastavení**.

2. Klepněte na položku **Obecné**.
3. Chcete-li spouštět úplnou archivaci každý den, týden nebo měsíc, klepněte v části **úplná archivace každý** na jednu z následujících možností:
   - **Den**
   - **Týden**
   - **Měsíc**

4 Zaškrtněte políčko vedle dne, ve kterém chcete spouštět úplnou archivaci.

5 Klepnutím na hodnotu v seznamu **V** určete čas spuštění úplné archivace.

6 Chcete-li spouštět rychlou archivaci denně nebo každou hodinu, klepněte v části **Rychlá archivace** na jednu z následujících možností:

- **Hodiny**
- **Dny**

7 Do pole **Rychlá archivace každý** zadejte číslo představující frekvenci.

8 Klepněte na tlačítko **OK**.

Poznámka: Naplánovanou archivaci zakážete výběrem možnosti **Ručně** v části **úplná archivace každý**.

Přerušení automatické archivace

Aplikace Backup and Restore automaticky archivuje data a soubory ve sledovaných umístěních podle plánu, který určíte. Pokud probíhá automatická archivace a přejete si ji ukončit, můžete tak učinit kdykoli.

1 V levém podokně klepněte na položku **Zastavit archivaci**.

2 V potvrzovacím dialogovém okně klepněte na tlačítko **Ano**.

Poznámka: Tlačítko **Zastavit archivaci** se zobrazí, pouze pokud probíhá archivace.

Ruční spuštění archivace

Přestože automatické archivace se spouštějí podle určeného plánu, můžete kdykoli spustit ruční archivaci. Rychlá archivace umožňuje archivovat pouze soubory změněné od poslední úplné nebo rychlé archivace. úplná archivace archivuje sledované soubory ze všech sledovaných umístění.

1 Klepněte na kartu **Místní archivace**.

2 Proveďte jednu z následujících akcí:

- Rychlou archivaci spustíte klepnutím na položku **Rychlá archivace** v levém podokně.
- úplnou archivaci spustíte klepnutím na položku **úplná archivace** v levém podokně.

3 V dialogovém okně Spustit archivaci ověřte místo v úložišti a nastavení a klepněte na tlačítko **Pokračovat**.

KAPITOLA 37

Práce s archivovanými soubory

Po archivaci některých souborů můžete aplikaci McAfee Backup and Restore použít pro práci s těmito soubory. Archivované soubory se zobrazují v tradičním zobrazení průzkumníku, což umožňuje jednoduché vyhledání. S narůstajícím archivem budete patrně chtít soubory třídit a vyhledávat. Soubory můžete také otevírat přímo v zobrazení průzkumníku. Tímto způsobem prověříte obsah, aniž by bylo nutné soubory načítat.

Soubory z archivu se načítají, pokud je místní kopie souboru zastaralá, poškozená nebo chybí. Aplikace Backup and Restore také poskytuje informace potřebné ke správě místních archivů a média úložiště.

V této kapitole

Používání průzkumníka místní archivace

Průzkumník místní archivace umožňuje zobrazování a manipulaci se soubory, které jste archivovali místně. Můžete zobrazit název souboru, typ, umístění, velikost, stav (archivován, nearchivován nebo probíhá archivace) a datum poslední archivace souboru. Můžete také třídit soubory podle kteréhokoli z těchto kritérií.

Máte-li velký archiv, můžete v něm soubor rychle nalézt pomocí možnosti jeho vyhledání. Můžete hledat celý nebo část názvu jeho cesty a výsledky hledání potom upřesníte určením přibližné velikosti a data poslední archivace souboru.

Po nalezení souboru jej můžete otevřít přímo nebo v průzkumníku místní archivace. Aplikace Backup and Restore otevře soubor v jeho nativním programu a umožní provést změny, aniž by bylo nutné opustit místní průzkumník archivace. Soubor je uložen v jeho původním sledovaném umístění v počítači a bude archivován automaticky podle vámi definovaného plánu archivace.

Třídění archivovaných souborů

Archivované soubory a složky můžete sdílet podle následujících kritérií: název, typ souboru, velikost, stav (tj. archivován, nearchivován nebo probíhá archivace), datum poslední archivace souborů nebo umístění souborů v počítači (cesta).

Třídění archivovaných souborů:

1. Klepněte na kartu **Místní archivace**.
2. V pravém podokně klepněte na název sloupce.

Vyhledání archivovaného souboru

Máte-li velké úložiště archivovaných souborů, můžete v něm soubor rychle nalézt pomocí možnosti jeho vyhledání. Můžete vyhledat celý nebo část názvu jeho cesty a výsledky hledání potom upřesníte určením přibližné velikosti a data poslední archivace souboru.

1. Do pole **Hledat** v horní části obrazovky zadejte část nebo celý název souboru a stiskněte klávesu Enter.
2. Do pole **Celý název nebo část názvu cesty** zadejte část nebo celou cestu k souboru.
3. Přibližnou velikost hledaného souboru určíte takto:
   - Klepněte na jednu z položek **Méně než 100 kB**, **Méně než 1 MB** nebo **Více než 1 MB**.
   - Klepněte na položku **Velikost v kB** a v seznamech zvolte odpovídající velikosti.

4 Přibližné datum poslední archivace hledaného souboru určíte takto:

- Klepněte na jednu z položek **Tento týden**, **Tento měsíc** nebo **Tento rok**.
- Klepněte na položku **Zadat data**, dále v seznamu klepněte na položku **Archivováno** a potom v seznamech klepněte na odpovídající data.

5 Klepněte na položku **Hledat**.

Poznámka: Neznáte-li přibližnou velikost nebo datum poslední archivace, klepněte na položku **Neznámé**.

Otevření archivovaného souboru

Obsah archivovaného souboru můžete prohlížet otevřením přímo v průzkumníku místní archivace.

Otevření archivovaných souborů:

1 Klepněte na kartu **Místní archivace**.

2 V pravém podokně klepněte na název souboru a klepněte na tlačítko **Otevřít**.

Tip: Archivovaný soubor můžete otevřít také poklepáním na název souboru.

Obnovení archivovaných souborů

Pokud je sledovaný soubor poškozen, chybí nebo byl omylem odstraněn, můžete ho obnovit z kopie v místním archivu. Z tohoto důvodu je důležité se ujistit, že pravidelně archivujete své soubory. Můžete také obnovit starší verze souboru z místního archivu. Pokud například pravidelně soubor archivujete, ale chcete se vrátit k jeho předchozí verzi, můžete tak učinit nalezením souboru v umístění archivu. Je-li archiv umístěn na místní nebo síťové jednotce, lze soubor nalézt procházením. Pokud je umístěn na externím pevném disku nebo jednotce USB, musíte připojit jednotku k počítači a potom soubor nalézt procházením. Je-li archiv umístěn na disku CD nebo DVD, je třeba toto médium nejdříve vložit do jednotky v počítači a soubor nalézt procházením.

Můžete také obnovit soubory archivované z jiného počítače. Pokud například archivujete nějaké soubory na externí pevný disk počítače A, můžete tyto soubory obnovit v počítači B. Chcete-li tak učinit, musíte nainstalovat aplikaci Backup and Restore do počítače B a připojit externí pevný disk. Potom v aplikaci Backup and Restore procházením najděte soubory, které budou přidány do seznamu **Chybějící soubory** k obnovení.

Další informace týkající se archivů najdete v části Archivace souborů. Pokud sledovaný soubor odstraníte úmyslně, můžete také odstranit položku v seznamu **Chybějící soubory**.

Obnovení chybějících souborů z místního archivu

Místní archiv aplikace Backup and Restore umožňuje obnovit data chybějící ve sledované složce v počítači. Je-li například soubor přesunut mimo sledovanou složku nebo je odstraněn, ale byl již předtím archivován, můžete ho znovu získat z místního archivu.

1. Klepněte na kartu **Místní archivace**.
2. Na kartě **Chybějící soubory** v dolní části obrazovky vyberte zaškrtávací políčko vedle názvu souboru, který chcete obnovit.
3. Klepněte na tlačítko **Obnovit**.

Tip: Klepnutím na tlačítko **Obnovit vše** můžete obnovit všechny soubory ze seznamu **Chybějící soubory**.

Obnovení starší verze souboru z místního archivu

Pokud chcete obnovit starší verzi archivovaného souboru, můžete ji vyhledat a přidat k seznamu **Chybějící soubory**. Potom můžete soubor obnovit jako každý jiný soubor v seznamu **Chybějící soubory**.

1. Klepněte na kartu **Místní archivace**.
2. Na kartě **Chybějící soubory** v dolní části obrazovky klepněte na **Procházet** a přejděte k umístění archivu.

   Názvy archivovaných složek se zobrazí v následujícím formátu: `cre ddmmrr_hh-mm-ss_***`, kde `ddmmrr` je datum archivace souborů, `hh-mm-ss` je čas archivace souborů a `***` je buď `Úplná` nebo `Rychlá` podle toho, zda byla provedena úplná nebo rychlá archivace.
3. Vyberte umístění a pak klepněte na tlačítko **OK**.

   Soubory obsažené ve vybraném umístění se zobrazí v seznamu **Chybějící soubory** připraveném k obnovení. Další informace získáte klepnutím na odkaz Obnovení chybějících souborů z místního archivu (stránka 184).

Odebrání souborů ze seznamu chybějících souborů

Po přesunutí nebo odstranění archivovaného souboru ze sledované složky se soubor automaticky zobrazí v seznamu **Chybějící soubory**. To je upozornění na skutečnost, že došlo k nekonzistenci mezi archivovanými soubory a soubory obsaženými ve sledovaných složkách. Pokud byl soubor přesunut nebo odstraněn ze sledované složky úmyslně, můžete jej ze seznamu **Chybějící soubory** odstranit.

Odebrání souboru ze seznamu chybějících souborů:

1. Klepněte na kartu **Místní archivace**.
2. Na kartě **Chybějící soubory** v dolní části obrazovky vyberte zaškrtávací políčko vedle názvu souboru, který chcete odebrat.
3. Klepněte na tlačítko **Odstranit**.

Tip: Můžete odebrat všechny soubory ze seznamu **Chybějící soubory** klepnutím na tlačítko **Odstranit vše**.

Správa archivů

Můžete kdykoli zobrazit souhrn informací o úplné a rychlé archivaci. Je například možné zobrazit informace o množství právě sledovaných dat, množství archivovaných dat a množství dat, která jsou právě sledována, ale nebyla dosud archivována. Můžete také zobrazit informace o plánu archivace, například datum poslední a příští archivace.

Zobrazení souhrnu aktivity archivace

Informace o aktivitě archivace můžete kdykoli zobrazit. Můžete například zobrazit podíl archivovaných souborů, velikost sledovaných dat, velikost archivovaných dat a velikost dat, které jsou sledovány, ale nebyly archivovány. Můžete také zobrazit dny posledních a následných archivací.

1. Klepněte na kartu **Místní archivace**.
2. V horní části obrazovky klepněte na položku **Souhrn účtu**.

KAPITOLA 38

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

Čištění souborů	Bezpečné a efektivní vymazání nepotřebných souborů pomocí různých možností čištění. Vymazáním těchto souborů uvolníte prostor na pevném disku počítače a zvýšíte jeho výkon.

KAPITOLA 39

Čištění počítače

Program QuickClean vymaže soubory, které tvoří zbytečné soubory v počítači. Vyprázdní koš a vymaže dočasné soubory, zástupce, fragmenty ztracených souborů, soubory registru, soubory uložené v mezipaměti, soubory cookie, soubory historie prohlížeče, odeslané a odstraněné e-maily, nedávno používané soubory, soubory ActiveX 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 webových stránek. Tyto soubory jsou obvykle uloženy jako dočasné soubory do složky mezipaměti. Složka mezipaměti je dočasné místo úložiště dat v počítači. Slouží ke zvýšení rychlosti a efektivity procházení webu. Při následujícím prohlížení může prohlížeč načíst webovou stránku nikoli ze vzdáleného serveru, ale ze své mezipaměti.

Název	Funkce
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 uživatele procházejícího web. Soubory cookie jsou primárně využívány webovými servery k identifikaci uživatelů, kteří byli již dříve zaregistrováni nebo server 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 odeslané a odstraněné e-maily aplikací Outlook® a Outlook Express.
Nedávno použitý čistič	Odstraní aktuálně používané soubory, které byly vytvořeny některým z těchto programů: ▪ 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 softwarová komponenta využívaná programy nebo webovými stránkami k rozšíření funkcí, 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.

V této kapitole

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** přijměte 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.

KAPITOLA 40

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.

KAPITOLA 41

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 přihlášeni 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 aplikaci McAfee SecurityCenter v části **Běžné úlohy** klepněte na položku **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** přijměte 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** 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 **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 aplikaci McAfee SecurityCenter v části **Běžné úlohy** klepněte na položku **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** přijměte 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** 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 **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 aplikaci McAfee SecurityCenter v části **Běžné úlohy** klepněte na položku **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 aplikaci McAfee SecurityCenter v části **Běžné úlohy** klepněte na položku **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 aplikaci McAfee SecurityCenter v části **Běžné úlohy** klepněte na položku **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 aplikaci McAfee SecurityCenter v části **Běžné úlohy** klepněte na položku **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 42

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

Trvalé vymazání souborů a složek

Odeberte položky z pevného disku počítače tak, že přiřazené informace nelze již obnovit. Tento program 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. Spusťte 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 Spusťte 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.

KAPITOLA 43

McAfee Network Manager

Program Network Manager poskytuje grafické zobrazení počítačů a dalších zařízení, které tvoří domácí síť. Program Network Manager lze použít ke vzdálené správě stavu ochrany každého spravovaného počítače v síti a ke vzdálené opravě ohlášených slabých míst zabezpečení v těchto počítačích. Pokud jste nainstalovali sadu McAfee Total Protection, lze program Network Manager také použít ke sledování sítě a zjišťování narušitelů (počítačů nebo zařízení, které neznáte a kterým nedůvěřujete), kteří se k síti pokoušejí připojit.

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

Grafická mapa sítě

Zobrazte grafické znázornění stavu ochrany počítače a zařízení, které tvoří domácí síť. Pokud provedete změny v síti (například pokud 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 libovolné zařízení na mapě sítě zobrazit podrobnosti.

Vzdálená správa

Spravujte 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 vzdáleného počítače v síti.

Sledování sítě

Pokud je program Network Manager k dispozici, používejte ho ke sledování sítě a upozornění na připojení přátele nebo narušitele. Sledování sítě je k dispozici pouze tehdy, pokud jste zakoupili sadu McAfee Total Protection.

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 44

Nastavení spravované sítě

Spravovanou síť nastavíte tak, že ji označíte jako důvěryhodnou (pokud jste tak dosud neučinili) a přidáte do ní 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 položkou, 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

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 obsahuje název 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 položky mapy sítě. Můžete také zobrazit podrobnosti přidružené k libovolné položce, která se na mapě sítě objeví.

Přístup k mapě sítě

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

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

Poznámka: Pokud jste síť ještě nenastavili jako důvěryhodnou (pomocí programu McAfee Personal Firewall), budete k tomuto kroku vyzváni při prvním přístupu k mapě sítě.

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 na mapě sítě nejsou 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 obsahuje název 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 zařízení 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 položce v síti zobrazíte tím, že položku vyberete na mapě sítě. Tyto informace zahrnují název položky, stav její ochrany a další informace požadované pro správu položky.

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 povolit ostatním počítačům v této síti spravovat nastavení zabezpečení tohoto počítače.

1. Ujistěte se, zda je v dialogovém okně Spravovaná síť zaškrtnuto políčko **Povolit správu 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 **Spravovat 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 45

Vzdálená správa sítě

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

V této kapitole

Správa stavu a oprávnění

Spravovaná síť obsahuje spravované i nespravované členy. Spravovaní členové umožňují ostatním počítačům v síti spravovat svůj stav ochrany McAfee. Nespravovaní 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 s oprávněními správce v síti pozván, aby se stal spravovaným počítačem. Obdobně může spravovaný počítač s oprávněními správce kdykoli změnit jiný spravovaný počítač na nespravovaný.

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.

Správa stavu ochrany počítače

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

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

Zastavení správy stavu ochrany počítače

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

1. Na mapě sítě klepněte na ikonu spravovaného počítače.
2. V části **Požadovaná akce** klepněte na možnost **Zastavit spravování 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 spravovat 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 spravovat své stavy ochrany.
4. Klepněte na tlačítko **OK**.

Správa zařízení

Zařízení lze spravovat pomocí přístupu na jeho webovou stránku správy z mapy sítě.

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 McAfee 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 spravovat 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 opravujete 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 navrhnutou 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 spravovat stav jejich zabezpečení. Chcete-li vzdáleně spravovat tyto počítače, je nutné v každém z nich nainstalovat nejnovější verzi programu SecurityCenter.

1. Ujistěte se, že podle těchto pokynů postupujete v počítači, který chcete vzdáleně spravovat.
2. Mějte své přihlašovací údaje McAfee snadno dostupné (e-mailovou adresu a heslo použité při první aktivaci softwaru společnosti McAfee).
3. Přejděte v prohlížeči na webový server společnosti McAfee, přihlaste se a klepněte na odkaz **Můj účet**.
4. Vyberte produkt, který chcete nainstalovat, klepněte na tlačítko produktu **Stáhnout** a postupujte podle pokynů na obrazovce.

Tip: Informace o instalaci zabezpečovacího softwaru McAfee ve vzdálených počítačích získáte také tím, že otevřete mapu sítě a v části **Požadovaná akce** klepnete na možnost **Chránit mé počítače**.

KAPITOLA 46

Sledování sítí

Pokud je nainstalována sada McAfee Total Protection, sleduje program Network Manager síť také proti narušitelům. Vždy když se k síti připojí neznámý počítač nebo zařízení, budete o něm vyrozuměni a můžete se tak rozhodnout, zda je počítač nebo zařízení přítel nebo narušitel. Přítele představuje počítač nebo zařízení, které znáte a kterému důvěřujete; narušitel je počítač nebo zařízení, které neznáte nebo kterému nedůvěřujete. Pokud počítač nebo zařízení označíte jako přítele, můžete rozhodnout, zda chcete být vyrozuměni o každém připojení přítele k síti. Pokud počítač nebo zařízení označíte jako narušitele, budete při každém připojení narušitele automaticky varováni.

Při prvním připojení k síti po instalaci nebo inovaci na tuto verzi sady Total Protection každý počítač nebo zařízení automaticky označíme jako přítele a nebudeme vás o jejich připojení k síti v budoucnu informovat. Po třech dnech vás začneme na každý připojovaný neznámý počítač nebo zařízení upozorňovat, takže je můžete označit sami.

Poznámka: Sledování sítí je funkce programu Network Manager, která je dostupná pouze se sadou McAfee Total Protection. Další informace o sadě Total Protection naleznete na našem webovém serveru.

V této kapitole

Zastavit sledování sítí

Pokud sledování sítě zakážete, nemůžeme dále zobrazovat výstrahy na případné připojení narušitelů k domácí síti nebo k libovolné jiné síti, ke které se připojujete.

1 Otevřete konfigurační podokno Internet a síť.

   Jak?

   1. V části **Běžné úlohy** klepněte na tlačítko **Domácí**.
   2. V podokně Domácí programu SecurityCenter klepněte na položku **Internet & síť**.
   3. V informační části Internet & síť klepněte na tlačítko **Konfigurovat**.

2 V části **Sledování sítě** klepněte na položku **Vypnout**.

Opakované povolení upozornění sledování sítě

I když lze upozornění sledování sítě zakázat, tuto možnost nedoporučujeme. Pokud upozornění zakážete, nebudeme vás patrně moci informovat v případě, když se k síti připojí neznámé počítače nebo narušitelé. Pokud jste tato upozornění zakázali neúmyslně (například zaškrtnutím políčka **Tuto výstrahu již příště nezobrazovat** ve výstraze), lze upozornění kdykoliv opět povolit.

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 **Výstrahy**.

3 Ujistěte se, zda jsou v podokně Informační výstrahy zrušena zaškrtnutí následujících zaškrtávacích políček:

   - **Nezobrazovat výstrahy při připojení nových počítačů nebo zařízení k síti**
   - **Nezobrazovat výstrahy při připojení narušitelů k síti**
   - **Nezobrazovat výstrahy u přátel, o kterých chci být obvykle informován**
   - **Nepřipomínat zjištěné neznámé počítače nebo zařízení**
   - **Nezobrazovat výstrahu, když program McAfee dokončí zjišťování nových přátel**

4 Klepněte na tlačítko **OK**.

Označení počítače nebo zařízení jako narušitele

Pokud počítač nebo zařízení neznáte nebo pokud jim nedůvěřujete, označte je jako narušitele. Při každém připojení narušitele k síti vás budeme automaticky varovat.

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

2 Klepněte na mapě sítě na nějakou položku.

3 V části **Požadovaná akce** klepněte na možnost **Označit jako přítele nebo narušitele**.

4 Klepněte v dialogovém okně na položku **Narušitel**.

Označení počítače nebo zařízení jako přítele

Počítač nebo zařízení označte jako přítele pouze tehdy, pokud je znáte a pokud jim důvěřujete. Když počítač nebo zařízení označíte jako přítele, můžete také rozhodnout, zda chcete nebo nechcete být vyrozuměni o každém připojení přítele k síti.

1. Klepněte v základní nebo rozšířené nabídce na položku **Správa sítě**.
2. Klepněte na mapě sítě na nějakou položku.
3. V části **Požadovaná akce** klepněte na možnost **Označit jako přítele nebo narušitele**.
4. Klepněte v dialogovém okně na položku **Přítel**.
5. Chcete-li být upozorněni na každé připojení tohoto přítele k síti, zaškrtněte políčko **Informovat, když se tento počítač nebo zařízení připojí do sítě**.

Zastavení zjišťování nových přátel

Během první tří dnů poté, co se připojíte k síti s touto nainstalovanou verzí sady Total Protection, budeme každý počítač nebo zařízení automaticky označovat jako přítele, na kterého nechcete být upozorňováni. Během těchto tří dnů můžete toto automatické označování kdykoliv zastavit, později ale už nelze restartovat.

1. Klepněte v základní nebo rozšířené nabídce na položku **Správa sítě**.
2. V části **Požadovaná akce** klepněte na tlačítko **Zastavit zjišťování nových přátel**.

KAPITOLA 47

McAfee EasyNetwork

Program McAfee® EasyNetwork umožňuje bezpečné sdílení souborů, sdílení tiskáren mezi počítači připojenými do domácí sítě a zjednodušuje přenos souborů. Tyto funkce jsou však přístupné pouze tehdy, jestliže je v počítačích sítě nainstalován program EasyNetwork.

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

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 EasyNetwork

Program EasyNetwork nabízí následující funkce.

Sdílení souborů

Program EasyNetwork usnadňuje sdílení souborů s ostatními počítači v síti. Sdílíte-li soubory, udělujete ostatním počítačům k těmto souborům přístup jen pro čtení. Pouze počítače, které jsou členy sítě (tedy počítače s úplným přístupem nebo přístupem správce), mohou sdílet soubory nebo mít přístup k souborům sdíleným ostatními členskými počítači.

Přenos souborů

Můžete soubory odesílat dalším počítačům s úplným přístupem nebo přístupem správce (členové). Pokud přijmete soubor, zobrazí se v doručené poště EasyNetwork. Doručená pošta představuje dočasné úložiště pro všechny soubory, které vám odešlou ostatní počítače v síti.

Automatické sdílení tiskárny

Připojíte-li se ke zřízené síti, program EasyNetwork automaticky sdílí všechny místní tiskárny připojené k vašemu počítači a jako název sdílené tiskárny používá aktuální název tiskárny. Program také zjišťuje tiskárny, které jsou sdíleny ostatními počítači v síti, a umožňuje tyto tiskárny konfigurovat a používat.

KAPITOLA 48

Nastavení programu EasyNetwork

Aby bylo možné program Easy Network používat, je třeba program spustit a připojit se ke spravované síti. Po připojení ke spravované síti lze sdílet, vyhledávat a odesílat soubory dalším počítačům v síti. Také můžete sdílet tiskárny. Rozhodnete-li se síť opustit, lze tak učinit kdykoliv.

V této kapitole

Spuštění programu EasyNetwork

Program EasyNetwork lze spustit pomocí nabídky Start systému Windows nebo klepnutím na ikonu na ploše.

- V nabídce **Start** přejděte na možnost **Všechny programy**, dále na možnost **McAfee** a poté klepněte na odkaz **McAfee EasyNetwork**.

Tip: Program EasyNetwork lze také spustit poklepáním na ikonu programu McAfee EasyNetwork na ploše.

Připojení spravované sítě

Pokud žádné počítače v síti, ke které jste připojeni, nemají nainstalovaný program SecurityCenter, stanete se členem sítě a jste vyzváni k určení, zda chcete této síti důvěřovat. Protože se jedná o první počítač připojený k síti, je název vašeho počítače obsažen v názvu sítě, síť však lze kdykoli přejmenovat.

Když se počítač připojí k síti, odešle do všech ostatních počítačů připojených k síti žádost o připojení. Přístup může udělit libovolný počítač v síti s oprávněními správce. Přidělující uživatel může také určit úroveň oprávnění počítače, který se připojuje k síti, například přístup hosta (pouze možnost přenosu souborů) nebo úplný přístup či přístup správce (možnost přenosu a sdílení souborů). V programu EasyNetwork mohou počítače s přístupem správce udělit přístup k ostatním počítačům a spravovat oprávnění (přesunout počítače na vyšší nebo na nižší úroveň), počítače s úplným přístupem nemohou provádět tyto úkoly správce.

Poznámka: Pokud máte nainstalovány jiné síťové programy McAfee (například program Network Manager), bude počítač po připojení k síti jako člen rozpoznán v těchto programech také jako spravovaný počítač. Úroveň oprávnění přiřazená počítači programem EasyNetwork 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 k síti

Když se počítač připojí k důvěryhodné síti poprvé po instalaci programu EasyNetwork, zobrazí se zpráva s dotazem, zda má proběhnout připojení ke spravované síti. V případě, že počítač souhlasí s připojením, je žádost o připojení odeslána do všech počítačů připojených k síti, které mají přístup správce. Dokud není požadavek schválen, nemůže počítač v síti sdílet tiskárny ani soubory ani odesílat nebo kopírovat soubory. Oprávnění správce jsou automaticky přidělena prvnímu počítači v síti.

1. V okně Sdílené soubory klepněte na tlačítko **Připojit se k této síti**. Když některý počítač s přístupem správce v síti váš požadavek schválí, zobrazí se zpráva s dotazem, zda povolit tomuto a ostatním počítačům v této síti vzájemné sledování nastavení zabezpečení.
2. Chcete-li povolit tomuto a ostatním počítačům v této síti vzájemné sledování nastavení zabezpečení, klepněte na tlačítko **OK**; v opačném případě klepněte na tlačítko **Storno**.
3. Potvrďte, že počítač udělující přístup zobrazuje stejné hrací karty, jako karty zobrazené v potvrzovacím dialogovém okně zabezpečení, a 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 potvrzovacím dialogovém okně zabezpečení na tlačítko **Storno**.

Udělení přístupu k síti

Pokud počítač požádá o členství k spravované síti, bude odeslána zpráva počítačům v síti, které mají přístup správce. První počítač, který zareaguje, se stane přidělujícím uživatelem. Jako přidělující uživatel rozhodujete o typu přístupu, který bude počítači udělen. host, úplný nebo správce.

1. Klepněte ve výstraze na příslušnou úroveň přístupu.
2. 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.

3 Klepněte na tlačítko **OK**.

4 Potvrďte, že počítač zobrazuje stejné hrací karty, jako karty zobrazené v potvrzovacím dialogovém okně zabezpečení, a poté klepněte na tlačítko **Udělit přístup**.

Poznámka: Pokud počítač nezobrazuje stejné hrací karty jako karty, které se objevily v potvrzovacím dialogovém okně zabezpečení, došlo k porušení zabezpečení ve spravované síti. Protože udělení přístupu tomuto počítači k takovéto síti může počítač vystavit nebezpečí, klepněte na tlačítko **Zamítnout přístup** v potvrzovacím dialogovém okně zabezpečení.

Přejmenování sítě

Ve výchozím nastavení název sítě obsahuje název prvního počítače, který se do sítě připojil. Síť však lze kdykoli později přejmenovat. Když přejmenujete síť, změníte popis sítě zobrazený v programu EasyNetwork.

1 V nabídce **Možnosti** klepněte na příkaz **Konfigurovat**.

2 V dialogovém okně Konfigurovat zadejte název sítě do pole **Síťový název**.

3 Klepněte na tlačítko **OK**.

Opuštění spravované sítě

Připojíte-li se ke spravované síti a později se rozhodnete, že již nechcete být jejím členem, můžete síť opustit. I když se po opuštění spravované sítě můžete vždy znovu připojit, musí vám být znovu uděleno oprávnění. Další informace o připojení naleznete v tématu Připojení ke spravované síti (stránka 228).

Opuštění spravované sítě

Spravovanou síť, ke které jste se připojili dříve, můžete opustit.

1 Odpojte počítač od sítě.

2 Klepněte v programu EasyNetwork v nabídce **Nástroje** na položku **Opustit síť**.

3 Vyberte v dialogovém okně Opustit síť název sítě, kterou chcete opustit.

4 Klepněte na příkaz **Opustit síť**.

KAPITOLA 49

Sdílení a odesílání souborů

Program EasyNetwork usnadňuje sdílení a odesílání souborů ostatním počítačům v síti. Sdílíte-li soubory, udělujete ostatním počítačům k těmto souborům přístup jen pro čtení. Pouze počítače, které jsou členy sítě (počítače s úplným přístupem nebo přístupem správce), mohou sdílet nebo mít přístup k souborům sdíleným ostatními členskými počítači.

Poznámka: Sdílení velkého množství souborů může mít vliv na prostředky počítače.

V této kapitole

Sdílení souborů

Pouze počítače, které jsou členy sítě (počítače s úplným přístupem nebo přístupem správce), mohou sdílet nebo mít přístup k souborům sdíleným ostatními členskými počítači. Sdílíte-li složku, jsou sdíleny všechny soubory obsažené v této složce a jejích podsložkách. Soubory přidané do složky dodatečně však automaticky sdíleny nejsou. Jsou-li sdílené soubory nebo složky odstraněny, jsou odebrány z okna Sdílené soubory. Sdílení souboru můžete kdykoliv zastavit.

Přístup ke sdílenému souboru získáte tím, že soubor otevřete přímo v programu EasyNetwork nebo soubor zkopírujete do počítače a otevřete z počítače. Jestliže je seznam sdílených souborů dlouhý a lze soubor obtížně nalézt, můžete soubor vyhledat.

Poznámka: K souborům, které jsou sdílené pomocí programu EasyNetwork, nelze přistupovat pomocí programu Průzkumník Windows z jiných počítačů, protože sdílení souborů programu EasyNetwork lze provozovat pouze přes zabezpečené připojení.

Sdílení souboru

Pokud sdílíte soubor, je k dispozici všem členům s úplným přístupem nebo přístupem správce ke spravované síti.

1. Pomocí Průzkumníka systému Windows vyhledejte soubor, který chcete sdílet.
2. Přesuňte soubor z jeho umístění v Průzkumníku systému Windows do okna Sdílené soubory v programu EasyNetwork.

Tip: Můžete rovněž sdílet soubor klepnutím na příkaz **Sdílet soubory** v nabídce **Nástroje**. V dialogovém okně Sdílet soubory přejděte na složku, kde je uložen soubor, který si přejete sdílet, vyberte tento soubor a klepněte na tlačítko **Sdílet**.

Zastavení sdílení souboru

Pokud ve spravované síti sdílíte soubor, můžete jeho sdílení kdykoli zastavit. Pokud zastavíte sdílení souboru, nemohou k němu ostatní členové spravované sítě přistupovat.

1. V nabídce **Nástroje** klepněte na příkaz **Zastavit sdílení souborů**.
2. V dialogovém okně Zastavit sdílení souborů zvolte soubor, jehož sdílení chcete zastavit.
3. Klepněte na tlačítko **OK**.

Kopírování sdíleného souboru

Důvodem kopírování sdíleného souboru je to, že soubor budete mít i poté, co již soubor nebude sdílen. Sdílený soubor můžete do počítače kopírovat z kteréhokoli počítače ve spravované síti.

- Přetáhněte soubor z okna Sdílené soubory v programu EasyNetwork do umístění v Průzkumníku systému Windows nebo na plochu systému Windows.

Tip: Sdílený soubor také můžete kopírovat tím, že soubor vyberete v programu EasyNetwork a poté klepnete na tlačítko **Kopírovat do** v nabídce **Nástroje**. V dialogovém okně Kopírovat do složky přejděte na složku, do které chcete soubor kopírovat, vyberte ji a klepněte na tlačítko **Uložit**.

Vyhledání sdíleného souboru

Soubor, který sdílíte nebo který sdílí některý další člen sítě, lze vyhledat. Při zadávání podmínek vyhledávání program EasyNetwork zobrazuje odpovídající výsledky v okně Sdílené soubory.

1. V okně Sdílené soubory klepněte na tlačítko **Hledat**.
2. Klepněte v seznamu **Obsahuje** na požadovanou možnost (stránka 233).
3. Zadejte část názvu nebo celý název souboru nebo cesty k němu do seznamu **Soubor nebo cesta**.
4. Klepněte v seznamu **Typ** na požadovaný typ souboru (stránka 233).
5. V seznamech **Od** a **Do** klepněte na data představující rozsah období, ve kterém byl soubor vytvořen.

Kritéria vyhledávání

Následující tabulky popisují kritéria vyhledávání, která lze pro vyhledávání sdílených souborů zadat.

Název souboru nebo cesta

Obsahuje	Popis
Obsahuje všechna slova	Vyhledává název souboru nebo cesty, který obsahuje všechna slova zadaná v seznamu **Soubor nebo cesta**, a to v libovolném pořadí.
Obsahuje jakékoliv ze slov	Vyhledává název souboru nebo cesty, který obsahuje libovolné ze slov zadaných v seznamu **Soubor nebo cesta**.
Obsahuje přesný řetězec	Vyhledává název souboru nebo cesty, který obsahuje přesný řetězec zadaný v seznamu **Soubor nebo cesta**.

Typ souboru

Typ	Popis
Jakýkoliv	Prohledá všechny sdílené typy souborů.
Dokument	Prohledá všechny sdílené dokumenty.
Obrázek	Prohledá všechny sdílené soubory obrázků.
Video	Prohledá všechny sdílené soubory videí.
Audio	Prohledá všechny sdílené zvukové soubory.
Komprimované	Prohledá všechny komprimované soubory (například soubory ZIP).

Odesílání souborů do jiných počítačů

Soubory můžete odeslat do jiných počítačů, které jsou členy spravované sítě. Před odesláním souboru program EasyNetwork potvrdí, že počítač, který daný soubor přijímá, má na disku dostatek místa.

Pokud přijmete soubor, zobrazí se v doručené poště EasyNetwork. Doručená pošta je dočasné úložiště určené pro ty soubory, které vám odešlou ostatní počítače v síti. Pokud máte při přijetí souboru spuštěn program EasyNetwork, soubor se okamžitě objeví v doručené poště; v opačném případě se zobrazí zpráva v oznamovací oblasti systému Windows zcela vpravo na hlavním panelu. Pokud nechcete přijímat tato upozornění (mohou vás například vyrušovat v práci), můžete tuto funkci vypnout. Pokud v doručené poště již existuje soubor se stejným názvem, nový soubor je přejmenován doplněním číselné přípony. Soubory jsou v doručené poště uloženy, dokud je nepřijmete (dokud soubory nezkopírujete do počítače).

Odeslání souboru do jiného počítače

Soubor můžete jinému počítači ve spravované síti odeslat, aniž byste jej sdíleli. Než bude uživatel přijímajícího počítače moci soubor zobrazit, musí být soubor uložen do místního umístění. Další informace naleznete v tématu Přijetí souboru z jiného počítače (stránka 235).

1. Pomocí Průzkumníka systému Windows vyhledejte soubor, který chcete odeslat.
2. Přesuňte soubor z jeho umístění v Průzkumníku systému Windows do ikony aktivního počítače v programu EasyNetwork.

Tip: Přidržením klávesy Ctrl během vybírání souborů můžete počítači odeslat více souborů. Soubory můžete také odeslat tím, že klepnete na položku **Odeslat** v nabídce **Nástroje**, soubory vyberete a poté klepnete na příkaz **Odeslat**.

Přijetí souboru z jiného počítače

Pokud vám jiný počítač ve spravované síti odešle soubor, musíte tento soubor přijmout a uložit do počítače. Pokud není program EasyNetwork spuštěn ve chvíli, kdy je do vašeho počítače odeslán soubor, zobrazí se zpráva v oznamovací oblasti zcela vpravo na hlavním panelu. Klepnutím na tuto zprávu spusťte program EasyNetwork a zpřístupněte soubor.

- Klepněte na tlačítko **Přijato** a poté soubor přesuňte z doručené pošty EasyNetwork do složky v Průzkumníku systému Windows.

Tip: Soubor přijatý z jiného počítače můžete také přijmout tím, že soubor vyberete v doručené poště EasyNetwork a potom klepnete v nabídce **Nástroje** na příkaz **Přijmout**. V dialogovém okně Přijmout do složky přejděte do složky, kam chcete uložit přijímané soubory, vyberte ji a klepněte na tlačítko **Uložit**.

Obdržení oznámení o odeslaném souboru

Odešle-li jiný počítač ve spravované síti vašemu počítači soubor, můžete obdržet oznámení. Pokud není spuštěn program EasyNetwork, zobrazí se zpráva v oznamovací oblasti zcela vpravo na hlavním panelu.

1. V nabídce **Možnosti** klepněte na příkaz **Konfigurovat**.
2. V dialogovém okně Konfigurace zaškrtněte políčko **Upozornit, když mi druhý počítač odesílá soubory.**
3. Klepněte na tlačítko **OK**.

KAPITOLA 50

Sdílení tiskáren

Připojíte-li se ke zřízené síti, program EasyNetwork sdílí místní tiskárny připojené k počítači a jako název sdílené tiskárny používá název tiskárny. Program EasyNetwork také zjišťuje tiskárny, které jsou sdíleny ostatními počítači v síti, a umožňuje tyto tiskárny konfigurovat a používat.

Je-li ovladač tiskárny konfigurován tak, aby tisk probíhal pomocí síťového tiskového serveru (například bezdrátového tiskového serveru USB), považuje program EasyNetwork tiskárnu za místní a sdílí ji v síti. Také sdílení tiskárny můžete zastavit kdykoliv.

V této kapitole

Práce se sdílenými tiskárnami

Program EasyNetwork zjišťuje tiskárny, které jsou počítači v síti sdíleny. Jestliže program EasyNetwork zjistí vzdálenou tiskárnu, která není k počítači připojena, zobrazí se při prvním spuštění programu EasyNetwork v okně Sdílené soubory odkaz **Dostupné síťové tiskárny**. Poté můžete dostupné tiskárny nainstalovat nebo odinstalovat tiskárny, které již jsou k počítači připojené. Také můžete seznam tiskáren aktualizovat a ujistit se, zda zobrazujete aktuální informace.

Není-li počítač členem spravované sítě, ale je k ní připojen, má přístup ke sdíleným tiskárnám ze standardního ovládacího panelu tiskáren systému Windows.

Zastavení sdílení tiskárny

Po zastavení sdílení tiskárny již členové tuto tiskárnu nemohou používat.

1. V nabídce **Nástroje** klepněte na příkaz **Tiskárny**.
2. V dialogovém okně Spravovat síťové tiskárny klepněte na název tiskárny, jejíž sdílení chcete zastavit.
3. Klepněte na tlačítko **Nesdílet**.

Instalace dostupné síťové tiskárny

Jestliže jste členem spravované sítě, máte ke sdíleným tiskárnám přístup. Je však třeba nainstalovat ovladač, který tiskárna používá. Pokud vlastník tiskárny zastaví sdílení, nemůžete tiskárnu používat.

1. V nabídce **Nástroje** klepněte na příkaz **Tiskárny**.
2. V dialogovém okně Dostupné síťové tiskárny klepněte na název tiskárny.
3. Klepněte na tlačítko **Instalovat**.

Reference

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

Slovníček

8

802.11

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

802.11a

Rozšíření standardu 802.11, které 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 nižší než u standardu 802.11a, pokrytá vzdálenost je větší.

802.1x

Standard pro ověření v drátových a bezdrátových sítích. Standard 802.1x je obvykle používán spolu se standardem 802.11 pro bezdrátové sítě. Viz také ověřování (stránka 244).

A

adresa IP

(Internet Protocol). Adresa, která slouží k identifikaci počítače nebo zařízení v síti TCP/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

(Media Access Control). Jedinečné sériové číslo přiřazené fyzickému zařízení (síťové kartě), které se připojuje k síti.

adresa URL

Adresa URL (Uniform Resource Locator). Standardní formát internetových adres.

archivace

Vytvoření kopie důležitých souborů na discích CD, DVD, jednotce USB, externím pevném disku nebo síťové jednotce. Porovnejte s heslem zálohování (stránka 252).

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

Přemísťování uživatele z oblasti pokrytí jednoho přístupového bodu (AP) k jinému bez přerušení služby nebo ztráty připojení.

Č

červ

Virus, který se šíří tak, že vytváří duplikáty sebe sama v dalších jednotkách, počítačích nebo sítích. Červ hromadné pošty vyžaduje k šíření zásah uživatele, např. otevření přílohy nebo spuštění staženého souboru. Většina současných e-mailových virů jsou červi. Červ, který může sám sebe automaticky šířit, nepotřebuje zásah uživatele. K červům, které automaticky šíří samy sebe, patří např. Blaster a Sasser.

D

DAT

(Detection Definition File). Soubory definic detekce rovněž nazývané soubory signatur obsahující definice určené k identifikaci, zjišťování a opravě virů, trojských koní, spywaru, adwaru a dalších potenciálně nežádoucích programů (PUP).

dialery

Software, který přesměruje internetová připojení na jiného účastníka, než je uživatelův výchozí poskytovatel služeb Internetu, aby tak zvýšil dodatečné poplatky za připojení pro poskytovatele obsahu, prodejce nebo jinou třetí stranu.

disk USB

Malá paměťová jednotka, kterou 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

(Domain Name System). Databázový systém, který převádí adresu IP, např. 11.2.3.44, na název domény, jako je www.mcafee.com.

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 (stránka 243).

doména

Místní podsíť nebo popis webů v Internetu. V místní síti (LAN) je doména podsítí tvořenou klientskými počítači a servery, které jsou řízeny jedinou databází zabezpečení. V Internetu je doména součástí názvu každé webové adresy. V případě adresy www.mcafee.com je doménou mcafee.

E

e-mail

Elektronická pošta. Zprávy zasílané a přijímané elektronickým způsobem prostřednictvím počítačové sítě. Viz také internetová pošta (stránka 242).

e-mailový klient

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

ESS

(Extended service set). Dvě nebo více sítí, které tvoří jednu podsíť.

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 se také používá k falšování hlaviček nevyžádaných e-mailových zpráv, aby nemohly být trasovány.

fragmenty souboru

Zbytky souboru roztrouseného na disku. K fragmentaci souboru dochází při přidávání nebo odstraňování souborů. Může způsobit zpomalení výkonu počítače.

H

heslo

Kód (obvykle alfanumerický) použitý pro získání přístupu k počítači, programu nebo k webovému serveru.

I

integrovaná brána

Zařízení, které spojuje funkce přístupového bodu (AP), směrovače a brány firewall. Některá zařízení jsou navíc vybavena funkcemi pro posílení zabezpečení a přemostění.

internetová pošta

Pošta založená na webu. Služba elektronické pošty s primárním přístupem prostřednictvím webového prohlížeče a nikoli e-mailového klienta v počítači, jako je aplikace Microsoft Outlook. Viz také e-mail (stránka 242).

intranet

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

J

Jednotka smart drive

Viz jednotka USB (stránka 241).

K

karanténa

Vynucená izolace souboru nebo složky s podezřením na obsah viru, spamu, podezřelého obsahu nebo programů PUP, aby nebylo možné tyto soubory nebo složky otevřít či spustit.

karta bezdrátového adaptéru USB

Karta bezdrátového adaptéru, kterou lze zapojit přímo do portu USB na počítači.

karta bezdrátového síťového adaptéru PCI

(Peripheral Component Interconnect). Karta bezdrátového adaptéru, kterou lze zapojit přímo do patice PCI v počítači.

klíč zabezpečení

Série písmen a čísel použitých dvěma zařízeními k ověření komunikace. Klíč musí mít obě zařízení. Viz také WEP (stránka 251), WPA (stránka 251), WPA2 (stránka 251), WPA2-PSK (stránka 251) a WPA-PSK (stránka 251).

klient

Program, který je spuštěn v 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.

komprimace

Proces, při němž dochází ke kompresi souborů do formy, která minimalizuje potřebné místo pro uložení nebo přenos.

Koš

Simulovaný koš na vymazané soubory a složky systému Windows.

L

LAN

(Local Area Network). Počítačová síť, která pokrývá relativně malou oblast (např. jedinou budovu). 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, které umožňuje spolupráci různých programů pro zasílání zpráv a pracovní skupiny (včetně e-mailu, hlasové pošty a faxu) s klientem, jako je například klient aplikace Exchange.

modul plug-in

Malý softwarový program, který přidá většímu programu funkce nebo jej rozšíří. Moduly plug-in umožňují webovému prohlížeči přístup a spuštění souborů vložených do dokumentů HTML, které by prohlížeč normálně nerozpoznal, například soubory animací, videa a zvuku.

MSN

(Microsoft Network). Skupina webových služeb nabízených společností Microsoft Corporation zahrnující vyhledávač, e-mail, zasílání rychlých zpráv a portál.

N

NIC

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

O

odkaz

Soubor obsahující pouze informace o umístění jiného souboru v počítači.

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 ověření digitální identity odesílatele při elektronické komunikaci.

ovládací prvek ActiveX

Softwarová komponenta používaná v programech nebo webových stránkách k doplnění funkčnosti, která se jeví jako normální součást programu nebo webové stránky. Většina ovládacích prvků ActiveX je neškodná, nicméně některé by mohly z počítače získávat informace.

P

platforma U3

Vy: jednodušší, inteligentnější, mobilní). Platforma pro spouštění 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)

Metoda podvodného získávání osobních údajů, jako jsou hesla, rodná čísla a informace o platebních kartách, zasíláním podvržených e-mailů, které působí dojmem, že byly odeslány z důvěryhodných zdrojů, např. bank nebo skutečných společností. Podvodné e-maily (phishing) obvykle požadují, aby příjemce klepnutím na odkaz v e-mailu potvrdil nebo aktualizoval kontaktní údaje nebo informace o platebních kartách.

POP3

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

port

Oblast hardwaru určená k předávání dat dovnitř a ven ze zařízení. Osobní počítače jsou vybaveny různými typy portů, jako jsou vnitřní porty pro připojení diskových jednotek, monitorů a klávesnic a vnější porty pro připojení modemů, tiskáren, myší a jiných periferních zařízení.

potenciálně nežádoucí programy (PUP)

Softwarové programy, které mohou být nežádoucí, přestože je možné, že uživatelé souhlasili s jejich stažením. Mohou změnit nastavení zabezpečení nebo ochrany osobních údajů v počítači, v němž jsou nainstalovány. Potenciálně nežádoucí programy mohou ale nemusí obsahovat spyware, adware a dialery a mohou být staženy spolu s programem, který uživatel chce.

prohledávání na požádání

Naplánovaná kontrola vybraných souborů, aplikací nebo síťových zařízení, která má najít hrozbu, slabé místo nebo jiný potenciálně nežádoucí kód. Může být provedena okamžitě, v naplánovaném čase v budoucnu nebo v pravidelných plánovaných intervalech. Porovnejte s prověřováním při přístupu. Viz také heslo slabé místo.

prohledávání v reálném čase

Proces zjišťování virů a jiné aktivity v souborech a složkách během přístupu uživatele nebo počítače.

prohlížeč

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

prostý text

Text, který není šifrován. Viz také šifrování (stránka 249).

protokol

Množina pravidel, která umožňuje počítačům nebo zařízením výměnu dat. Ve vícevrstvé síťové architektuře (model OSI) má každá vrstva své vlastní protokoly, které určují způsob komunikace na dané úrovni. Aby mohl váš počítač nebo zařízení komunikovat s jinými počítači, musí podporovat správný protokol. Viz také heslo OSI.

protokol PPPoE

Protokol PPP (Point-to-Point) v síti Ethernet. Metoda použití protokolu telefonického připojení PPP, která k přenosu dat využívá síť Ethernet.

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 (stránka 247)

přetečení vyrovnávací paměti

Situace, k níž dojde v operačním systému nebo aplikaci, když se podezřelé programy nebo procesy pokoušejí do vyrovnávací paměti (dočasného úložiště dat) uložit více dat, než je možné. Přetečení vyrovnávací paměti způsobuje poškození paměti nebo přepis dat v přilehlých vyrovnávacích pamětích.

přípojný bod

Geografická hranice tvořená bezdrátovým (802.11) přístupovým bodem (AP). Uživatelé, kteří s přenosným počítačem vybaveným pro bezdrátové připojení vstoupí do dosahu přípojného bodu, se mohou připojit k Internetu, pokud 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 (AP)

Síťové zařízení (obvykle zvané bezdrátový směrovač), které je připojováno k ethernetovému rozbočovači nebo přepínači, aby bylo možné rozšířit fyzický rozsah služeb pro uživatele bezdrátové sítě. Pokud uživatelé bezdrátové technologie cestují s mobilními zařízeními, spojení je udržováno převodem přenosu dat z jednoho přístupového bodu do druhého.

publikovat

Veřejně zpřístupnit zálohovaný soubor na Internetu. Publikované soubory můžete zpřístupnit vyhledáním v knihovně zálohování a obnovení.

R

registr

Databáze využívaná systémem Windows k ukládání informací o konfiguracích jednotlivých uživatelů počítače, hardwaru, nainstalovaných programů a nastavení vlastností. Databáze se dělí na klíče, pro které jsou nastaveny hodnoty. Nežádoucí programy mohou změnit hodnotu klíčů registru nebo vytvořit nové ke spuštění škodlivého kódu.

S

sdílení

Funkce, která příjemcům e-mailu umožní po omezenou dobu přistupovat k vybraným zálohovaným souborům. Jestliže sdílíte soubor, odesíláte jeho zálohovanou kopii určeným příjemcům e-mailu. Příjemci obdrží od funkce zálohování a obnovení e-mailovou zprávu, která oznamuje sdílení souborů. Tento e-mail zároveň obsahuje odkaz na sdílené soubory.

sdílený tajný klíč

Řetězec nebo klíč (obvykle heslo), které je sdíleno mezi dvěma komunikujícími stranami ještě před zahájením komunikace. Slouží k ochraně citlivých částí zpráv RADIUS. Viz také RADIUS (stránka 252).

server

Počítač nebo program, který přijme připojení jiného počítače nebo programů a vrátí odpovídající odezvu. E-mailový program se například připojí k e-mailovému serveru pokaždé, když odesíláte nebo přijímáte zprávy elektronické pošty.

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

Seznam položek, kterým můžete důvěřovat a které nebyly detekovány. Pokud důvěřujete položce (jako je např. potenciálně nežádoucí program nebo změna registru) omylem nebo chcete, aby byl zjištěn, musíte jej z tohoto seznamu odebrat.

seznam povolených serverů

Seznam webových serverů nebo e-mailových adres považovaných za bezpečné. Webové servery uvedené v seznamu povolených serverů jsou ty, k nimž mají uživatelé povolen přístup. E-mailové adresy uvedené v seznamu povolených serverů pocházejí z důvěryhodných zdrojů, jejichž zprávy chcete přijímat. Porovnejte s heslem seznam zakázaných serverů (stránka 247).

seznam zakázaných serverů

V programu Anti-Spam je to seznam e-mailových adres, z nichž nechcete přijímat zprávy, protože je předem považujete za spam. U ochrany proti podvodným zprávám (phishing) je to seznam webových serverů považovaných za podvodné. Porovnejte s heslem seznam povolených serverů (stránka 247).

síť

Skupina systémů protokolu IP (jako jsou např. směrovače, přepínače, servery a brány firewall) seskupených jako logická jednotka. Síť Finance může například zahrnovat všechny servery, směrovače a systémy, které slouží finančnímu oddělení. Viz také domácí síť (stránka 242).

síťová jednotka

Disková nebo pásková jednotka, která je připojena k serveru v síti sdílené více uživateli. Síťové jednotky jsou někdy označovány jako 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 je to věková skupina, ke které patří uživatel. Obsah je zpřístupněn nebo blokován podle skupiny hodnocení obsahu, ke které patří uživatel. Skupiny hodnocení obsahu jsou tyto: Předškolní věk, Mladší školní věk, Starší školní věk, Mladistvý a Dospělý.

sledovaná umístění

Složky v počítači, které sleduje funkce zálohování a obnovení.

sledované typy souborů

Typy souborů (například s příponou DOC, XLS atd.), které jsou funkcí zálohování a obnovení archivovány nebo zálohovány 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 čtou jednotlivé příchozí pakety a na základě adresy zdroje a cíle a aktuálních podmínek provozu rozhodují o způsobu, jakým budou přeposílány. Směrovač je někdy označován jako přístupový bod (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 textový soubor používaný mnoha webovými servery k ukládání informací o stránkách, které byly navštíveny nebo uloženy do počítače uživatele procházejícího web. Může obsahovat přihlašovací nebo registrační informace, údaje o nákupním košíku nebo předvolbách uživatele. Soubory cookie jsou primárně používány webovými servery k identifikaci uživatelů, kteří byli již dříve zaregistrováni nebo webový server navštívili. Mohou však být zdrojem informací pro hackery.

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 jsou schopny způsobit další ohrožení zabezpečení nebo soukromí počítačových dat a osobních informací.

SSID

(Service Set Identifier). Token (tajný klíč), který identifikuje bezdrátovou síť (Wi-Fi 802.11). 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 pro přenos soukromých dokumentů prostřednictvím Internetu. Protokol SSL používá veřejný klíč k šifrování dat, která jsou přenášena pomocí připojení SSL. Adresy URL, které vyžadují připojení SSL, nezačínají řetězcem HTTP ale HTTPS.

standardní e-mailový účet

Viz POP3 (stránka 245).

Synchronizace

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.

systém launchpad

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

Š

šifrování

Metoda kódování informací, která neoprávněným stranám znemožňuje jejich používání. Proces používá ke kódování klíč a matematické algoritmy. šifrované informace nelze bez příslušného klíče dešifrovat. Viry někdy používají šifrování ve snaze uniknout detekci.

šířka pásma

Množství (propustnost) dat, která mohou být přenesena za určitou dobu.

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 – vyslovováno jako tý-kip). Část standardu šifrování 802.11i pro bezdrátové sítě LAN. Protokol TKIP je další generací protokolu WEP, který slouží k zabezpečení bezdrátových sítí LAN 802.11. Protokol TKIP zajišťuje směšování klíčů po jednotlivých paketech, kontrolu integrity zprávy a mechanismus obnovy klíčů pro opravu chyb v protokolu WEP.

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

Program, který se nereplikuje, ale poškozuje nebo ohrožuje zabezpečení počítače. Trojského koně vám obvykle zašle jednotlivec, trojský kůň sám sebe neodesílá. Trojského koně je rovněž možné stáhnout nevědomky z webového serveru nebo prostřednictvím sítě peer-to-peer.

U

událost

V případě počítače nebo programu je to případ nebo výskyt, který lze zjistit softwarem zabezpečení podle předem stanovených kritérií. Událost obvykle vyvolává akci, např. odeslání upozornění nebo záznam položky do protokolu událostí.

USB

(Universal Serial Bus). Standardní konektor na většině moderních počítačů, který slouží k připojení různých zařízení od klávesnic a myší po webové kamery, skenery a tiskárny.

Ú

útok DoS (Denial of Service)

Typ útoku proti počítači, serveru nebo síti, který zpomalí nebo zastaví provoz v síti. Dochází k němu tehdy, jestliže je síť zahlcena takovým množstvím dalších požadavků, že se běžný provoz zpomalí nebo zcela zastaví. útok DoS zaplaví svůj cíl falešnými požadavky na připojení, aby cíl ignoroval oprávněné požadavky.

útok hrubou silou

Metoda hackingu používaná k vyhledávání hesel nebo šifrovacích klíčů zkoušením všech možných kombinací znaků, dokud nedojde k rozluštění šifry.

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

Počítačový program, který může kopírovat sám sebe a infikovat počítač bez svolení nebo vědomí uživatele.

VPN

(Virtual Private Network). Soukromá komunikační síť nakonfigurovaná prostřednictvím hostitelské sítě, jakou je například Internet. Data procházející připojením k síti VPN jsou zašifrována a vybavena výkonnými funkcemi zabezpečení.

vyrovnávací paměť

Dočasné úložiště dat v počítači určené pro často nebo nedávno používaná data. Slouží např. ke zvýšení rychlosti a účinnosti procházení webu, protože při následujícím prohlížení může prohlížeč načíst webovou stránku namísto ze vzdáleného serveru ze své mezipaměti.

W

wardriver

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

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, pixelové značky, čisté soubory GIF nebo neviditelné soubory GIF.

WEP

(Wired Equivalent Privacy). šifrovací a ověřovací protokol definovaný jako součást standardu Wi-Fi (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 je používán organizací Wi-Fi Alliance pro pojmenování jakéhokoliv typu sítě 802.11.

Wi-Fi Certified

Produkt byl otestován a vyzkoušen organizací Wi-Fi Alliance. U produktů s označením Wi-Fi Certified se předpokládá schopnost vzájemné spolupráce, 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 síť (LAN), v níž je používáno bezdrátové připojení. Síť WLAN používá ke komunikaci mezi počítači namísto kabelů vysokofrekvenční rádiové vlny.

WPA

(Wi-Fi Protected Access). Standard, který silně zvyšuje úroveň ochrany dat a řízení přístupu existujících a budoucích systémů LAN. Je navržen tak, aby byl na stávajícím hardwaru spouštěn jako inovace softwaru. Standard WPA pochází ze standardu 802.11i a je s ním kompatibilní. Pokud je správně nainstalován, poskytuje uživatelům sítí 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 PWA-PSK, a měl by pravidelně měnit heslo v každém bezdrátově připojeném počítači a přístupovém bodu. Viz také WPA2-PSK (stránka 251), TKIP (stránka 249).

WPA2

Aktualizace bezpečnostního standardu WPA, která vychází ze standardu 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 umožňuje ověřování uživatelů. Obvykle je používán v kontextu se vzdáleným přístupem. Původně byl definován pro použití na serverech s telefonickým vzdáleným přístupem. Nyní je používán v různých prostředích ověřování, včetně ověření sdíleného tajného klíče uživatelů sítě WLAN protokolem 802.1x. Viz také sdílený tajný klíč.

zálohování

Vytvoření kopie důležitých souborů obvykle na bezpečném serveru online. Porovnejte s heslem archivace (stránka 240).

zašifrovaný text

šifrovaný text. Zašifrovaný text je nečitelný, dokud není převeden na prostý text (tzn. dešifrován). Viz také šifrování (stránka 249).

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, zabraňovat únikům informací a neustále sledovat a zlepšovat zabezpečení.

Licence

POZNÁMKA PRO VŠECHNY UŽIVATELE: DŮKLADNĚ SI PŘEČTĚTE PŘÍSLUŠNOU SMLOUVU ODPOVÍDAJÍCÍ ZAKOUPENÉ LICENCI, V NÍŽ JSOU UVEDENY OBECNÉ PODMÍNKY TÝKAJÍCÍ SE UŽÍVÁNÍ LICENCOVANÉHO SOFTWARU. 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 SOFTWARU 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 SOFTWAROVÝ 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.

Copyright

KAPITOLA 51

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 přihlášeni jako správce systému Windows. V opačném případě může dojít k tomu, že nástroj Virtual Technician nedokáže záležitosti 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

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.

V následujících tabulkách naleznete informace o serverech podpory a serverech pro stahování společnosti McAfee včetně uživatelských příruček pro příslušnou zemi nebo oblast.

Podpora a položky ke stažení

Země nebo oblast	Podpora McAfee	Soubory McAfee ke stažení
Austrálie	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brazílie	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Česká republika	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Čína (zjednodušená čínština)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
Dánsko	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Finsko	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp

Francie	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
Itálie	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
Japonsko	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
Kanada (angličtina)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Kanada (francouzština)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp?langid=48
Korea	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
Maďarsko	www.mcafeehelp.com	hu.mcafee.com/root/downloads.asp
Mexiko	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
Německo	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Norsko	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
Polsko	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp
Portugalsko	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
Řecko	www.mcafeehelp.com	el.mcafee.com/root/downloads.asp
Rusko	www.mcafeehelp.com	ru.mcafee.com/root/downloads.asp
Slovensko	www.mcafeehelp.com	sk.mcafee.com/root/downloads.asp
španělsko	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Spojené státy americké	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp
švédsko	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Tchaj-wan	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Turecko	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
Velká Británie	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp

Uživatelské příručky sady McAfee Total Protection

Země nebo oblast	Uživatelské příručky McAfee
Austrálie	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brazílie	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Česká republika	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Čína (zjednodušená čínština)	download.mcafee.com/products/manuals/zh-cn/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.pdf
Francie	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Itálie	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
Japonsko	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf
Kanada (angličtina)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
Kanada (francouzština)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Maďarsko	download.mcafee.com/products/manuals/hu/MTP_userguide_2008.pdf
Mexiko	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Německo	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Nizozemsko	download.mcafee.com/products/manuals/nl/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
Řecko	download.mcafee.com/products/manuals/el/MTP_userguide_2008.pdf

Rusko	download.mcafee.com/products/manuals/ru/MTP_userguide_2008.pdf
Slovensko	download.mcafee.com/products/manuals/sk/MTP_userguide_2008.pdf
španělsko	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Spojené státy americké	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf
švédsko	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Tchaj-wan	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Turecko	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
Velká Británie	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf

Uživatelské příručky sady McAfee Internet Security

Země nebo oblast	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 (zjednodušená čínština)	download.mcafee.com/products/manuals/zh-cn/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
Řecko	download.mcafee.com/products/manuals/el/MIS_userguide_2008.pdf

Maďarsko	download.mcafee.com/products/manuals/hu/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
Nizozemsko	download.mcafee.com/products/manuals/nl/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
Rusko	download.mcafee.com/products/manuals/ru/MIS_userguide_2008.pdf
Slovensko	download.mcafee.com/products/manuals/sk/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
Tchaj-wan	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Turecko	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
Velká Británie	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Spojené státy americké	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

Uživatelské příručky programu McAfee VirusScan Plus

Země nebo oblast	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
Česká republika	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf

Čína (zjednodušená čínština)	download.mcafee.com/products/manuals/zh-cn/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
Itálie	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Japonsko	download.mcafee.com/products/manuals/ja/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
Korea	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Maďarsko	download.mcafee.com/products/manuals/hu/VSP_userguide_2008.pdf
Mexiko	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Německo	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Nizozemsko	download.mcafee.com/products/manuals/nl/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
Řecko	download.mcafee.com/products/manuals/el/VSP_userguide_2008.pdf
Rusko	download.mcafee.com/products/manuals/ru/VSP_userguide_2008.pdf
Slovensko	download.mcafee.com/products/manuals/sk/VSP_userguide_2008.pdf
španělsko	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Spojené státy americké	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf
švédsko	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf

Tchaj-wan	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
Turecko	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
Velká Británie	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf

Uživatelské příručky programu McAfee VirusScan

Země nebo oblast	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
Česká republika	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Čína (zjednodušená čínština)	download.mcafee.com/products/manuals/zh-cn/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
Itálie	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Japonsko	download.mcafee.com/products/manuals/ja/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
Korea	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Maďarsko	download.mcafee.com/products/manuals/hu/VS_userguide.2008.pdf
Mexiko	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Německo	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Nizozemsko	download.mcafee.com/products/manuals/nl/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
Řecko	download.mcafee.com/products/manuals/el/VS_userguide.2008.pdf
Rusko	download.mcafee.com/products/manuals/ru/VS_userguide_2008.pdf
Slovensko	download.mcafee.com/products/manuals/sk/VS_userguide_2008.pdf
španělsko	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Spojené státy americké	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf
švédsko	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Tchaj-wan	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Turecko	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
Velká Británie	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf

V následující tabulce naleznete informace o Centru pro hrozby společnosti McAfee a webech s informacemi o virech ve vaší zemi nebo oblasti.

Země nebo oblast	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
Česká republika	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Čína (zjednodušená čínština)	www.mcafee.com/us/threat_center	cn.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
Itálie	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Japonsko	www.mcafee.com/us/threat_center	jp.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
Korea	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
Maďarsko	www.mcafee.com/us/threat_center	hu.mcafee.com/virusInfo
Mexiko	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Německo	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Nizozemsko	www.mcafee.com/us/threat_center	nl.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
Řecko	www.mcafee.com/us/threat_center	gr.mcafee.com/virusInfo
Rusko	www.mcafee.com/us/threat_center	ru.mcafee.com/virusInfo
Slovensko	www.mcafee.com/us/threat_center	sk.mcafee.com/virusInfo
španělsko	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Spojené státy americké	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo
švédsko	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Tchaj-wan	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Turecko	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
Velká Británie	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo

V následující tabulce naleznete informace o webech HackerWatch ve vaší zemi nebo oblasti.

Země nebo oblast	HackerWatch
Austrálie	www.hackerwatch.org
Brazílie	www.hackerwatch.org/?lang=pt-br
Česká republika	www.hackerwatch.org/?lang=cs
Čína (zjednodušená čínština)	www.hackerwatch.org/?lang=zh-cn
Dánsko	www.hackerwatch.org/?lang=da
Finsko	www.hackerwatch.org/?lang=fi
Francie	www.hackerwatch.org/?lang=fr
Itálie	www.hackerwatch.org/?lang=it
Japonsko	www.hackerwatch.org/?lang=jp

Kanada (angličtina)	www.hackerwatch.org
Kanada (francouzština)	www.hackerwatch.org/?lang=fr-ca
Korea	www.hackerwatch.org/?lang=ko
Maďarsko	www.hackerwatch.org/?lang=hu
Mexiko	www.hackerwatch.org/?lang=es-mx
Německo	www.hackerwatch.org/?lang=de
Nizozemsko	www.hackerwatch.org/?lang=nl
Norsko	www.hackerwatch.org/?lang=no
Polsko	www.hackerwatch.org/?lang=pl
Portugalsko	www.hackerwatch.org/?lang=pt-pt
Řecko	www.hackerwatch.org/?lang=el
Rusko	www.hackerwatch.org/?lang=ru
Slovensko	www.hackerwatch.org/?lang=sk
španělsko	www.hackerwatch.org/?lang=es
Spojené státy americké	www.hackerwatch.org
švédsko	www.hackerwatch.org/?lang=sv
Tchaj-wan	www.hackerwatch.org/?lang=zh-tw
Turecko	www.hackerwatch.org/?lang=tr
Velká Británie	www.hackerwatch.org

Rejstřík

P

R

S

Š

T

U

V

W

Z