F-Secure Anti-Virus 2013

Obsah

Kapitola 1: Instalace.....5

P ed první instalací.....6
První instalace produktu.....6
Instalace a upgrady aplikací.....6
Nápov da a podpora.....7

Kapitola 2: Za ínáme.....9

Používání automatických aktualizací.....10
Kontrola stavu aktualizace.....10
Zm na nastavení p ipojení k Internetu.....10
Kontrola stavu sít ochrany v reálném ase.....11
Zobrazení inností produktu.....11
Zobrazení historie oznámení.....11
Zm na nastavení oznámení.....11
Sí ochrany v reálném ase.....12
Co je Sí ochrany v reálném ase.....12
Výhody Sít ochrany v reálném ase.....12
Jakými daty p ispíváte.....13
Jak chráníme vaše soukromí.....14
Jak se stát p isp vatelem Sít ochrany v reálném ase.....14
Dotazy týkající se Sít ochrany v reálném ase.....14
Ov ení platnosti p edplatného.....15
Centrum akcí.....15
Aktivace registrace.....16

Kapitola 3: Úvod.....17

Zobrazení celkového stavu ochrany.....18
Zobrazení statistiky produktu.....18
Práce s aktualizacemi produktu.....19
Zobrazení verzí databází.....19
Zm na nastavení mobilního širokopásmového p ipojení.....19
Co jsou viry a další malware?.....20
Viry.....20
Spyware.....20
Rootkity.....21
Riskware.....21

Kapitola 4: Ochrana po íta e proti malwaru.....23

Kontrola po íta e.....24

Automatická kontrola soubor 24

Ru ní kontrola soubor 26

Kontrola e-mail 29

Zobrazení výsledk kontroly.....29

Jak vylou it soubory z kontroly.....30

Typy vylou ených soubor 30

Vylou ení soubor podle umíst ní.....30

Zobrazení vylou ených aplikací.....31

Jak využívat karanténu?.....32

Zobrazení položek v karantén 32

Obnovení položek uložených v karantén 32

Co je DeepGuard?.....33

Zapnutí nebo vypnutí funkce DeepGuard.....33

Povolení aplikací, které funkce DeepGuard zablokovala.....33

Použití funkce DeepGuard v režimu kompatibility.....34

Co d lat p i varování na podez elé chování.....34

Kapitola

1

Instalace

Témata:

- *P ed první instalací*
- *První instalace produktu*
- *Instalace a upgrady aplikací*
- *Nápov da a podpora*

P ed první instalací

D kujeme, že jste si vybrali spole nost F-Secure.

K instalaci produktu pot ebujete:

- Instala ní disk CD-ROM nebo instala ní balí ek. Používáte-li netbook bez jednotky CD, m žete si stáhnout instala ní balí ek z webové stránky *www.f-secure.com/netbook*.
- Váš registra ní klí
- p ipojení k Internetu.

Máte-li k dispozici produkt zabezpe ení od jiného prodejce, instala ní program se ho automaticky pokusí odstranit. Pokud se tak nestane, odstra te ho ru n .

Poznámka: Pokud je v po íta i více ú t , p ihlaste se p ed instalací pomocí ú tu s oprávn ním správce.

První instalace produktu

Pokyny k instalaci produktu.

Postupujte podle t chto pokyn k instalaci produktu:

1. Vložte do po íta e disk CD-ROM nebo poklepejte na instala ní program, který jste si stáhli.
   Pokud se disk CD-ROM nespustí automaticky, p ejd te do Pr zkumníka Windows, poklepejte na ikonu CD-ROM a poklepáním na instala ní soubor spus te instalaci.
2. Postupujte podle pokyn na obrazovce.
   - Pokud jste produkt zakoupili na CD v obchod , registra ní klí najdete na obalu Stru ného pr vodce instalací.
   - Pokud jste produkt stáhli pomocí služby F-Secure eStore, registra ní klí se nachází v potvrzovacím e-mailu objednávky.

   P ed ov ením p edplatného a stažením nejnov jších aktualizací z Internetu bude možná nutné restartovat po íta . Pokud instalujete z disku CD-ROM, nezapome te ho p ed restartováním po íta e vyjmout z jednotky.

Instalace a upgrady aplikací

Pokyny k aktivaci registrace.

Podle t chto pokyn postupujte p i aktivaci nové registrace nebo p i instalaci nové aplikace pomocí hlavního panelu:

Poznámka: Ikonu hlavního panelu naleznete na hlavním panelu systému Windows.

1. P ejd te na hlavní panel a klepn te pravým tla ítkem na ikonu zcela vpravo.
   Otev e se místní nabídka.
2. Vyberte položku **Zobrazit moje registrace (View my subscriptions)**.
3. V ásti **Moje registrace (My subscriptions)** p ejd te na stránku **Stav registrace (Subscription status)** a klepn te na tla ítko **Aktivovat registraci (Activate subscription)**.
   Zobrazí se okno **Aktivovat registraci (Activate subscription)**.
4. Zadejte sv j registra ní klí pro tuto aplikaci a klepn te na tla ítko **OK**.

5. Po ov ení a aktivaci registrace klepn te na tla ítko **Zav ít (Close)**.
6. V ásti **Moje registrace (My subscriptions)** p ejd te na stránku **Stav instalace (Installation status)**. Pokud se instalace nespustí automaticky, postupujte podle t chto pokyn :
   a) Klepn te na tla ítko **Instalovat (Install)**.
      Zobrazí se okno instalace.
   b) Klepn te na tla ítko **Další**.
      Aplikace se stáhne a spustí se instalace.
   c) Po dokon ení instalace klepn te na tla ítko **Zav ít (Close)**.

Tím byla aktivována nová registrace.

Nápov da a podpora

P ístup online k nápov d produktu získáte klepnutím na ikonu nápov dy nebo stisknutím klávesy F1 na kterékoli obrazovce produktu.

Po zaregistrování licence máte nárok na další služby, jako jsou bezplatné aktualizace a podpora produktu. Registraci lze provést na stránkách *www.f-secure.com/register*.

Kapitola

2

Za ínáme

Témata:

- *Používání automatických aktualizací*
- *Zobrazení inností produktu*
- *Sí ochrany v reálném ase*
- *Ov ení platnosti p edplatného*

Informace o tom, jak za ít s produktem pracovat.

V této ásti je popsán postup p i zm n spole ných nastavení a správ registrací prost ednictvím hlavního panelu.

Spole ná nastavení jsou ta, která platí pro všechny programy nainstalované na hlavním panelu. Namísto zm n samostatných nastavení v jednotlivých programech m žete jednoduše upravit spole ná nastavení, která jsou pak využívána ve všech nainstalovaných programech.

Mezi spole ná nastavení hlavního panelu pat í:

- Stahování, kde m žete vid t informace o stažených aktualizacích a ru n kontrolovat, zda jsou k dispozici nové aktualizace.
- Nastavení p ipojení, kde lze zm nit zp sob p ipojení po íta e k Internetu.
- Oznámení, kde m žete vid t minulá oznámení a nastavit druh oznámení, která chcete zobrazit.
- Nastavení ochrany osobních dat, kde m žete vybrat, zda se po íta m že p ipojit k síti ochrany v reálném ase.

Pomocí hlavního panelu lze také spravovat registrace nainstalovaných program .

Používání automatických aktualizací

Automatické aktualizace slouží k udržování ochrany v po íta i v aktuálním stavu.

Je-li po íta p ipojen k Internetu, agent automatické aktualizace F-Secure do n j stahuje nejnov jší aktualizace. Zjiš uje p enosy v síti a neomezuje práci s Internetem ani u pomalého p ipojení.

Kontrola stavu aktualizace

Zobrazuje datum a as poslední aktualizace.

Jsou-li zapnuty automatické aktualizace, produkt v dob p ipojení k Internetu automaticky p ijímá nejnov jší aktualizace.

Ov ení instalace nejnov jších aktualizací:

1. P ejd te na hlavní panel a klepn te pravým tla ítkem na ikonu zcela vpravo.
   Zobrazí se místní nabídka.
2. Vyberte p íkaz **Otev ít spole ná nastavení**.
3. Klepn te na položku **Automatické aktualizace** > **Stahování**.
4. Klepn te na položku **Ov it nyní**.
   Produkt se p ipojí k Internetu a vyhledá nejnov jší aktualizace. Není-li ochrana aktuální, stáhne nejnov jší aktualizace.

   Poznámka: Používáte-li modem nebo máte p ipojení ISDN, je ke kontrole aktualizací pot eba, aby bylo p ipojení aktivní.

Zm na nastavení p ipojení k Internetu

Obvykle není t eba m nit výchozí nastavení, ale m žete nakonfigurovat p ipojení vašeho serveru k internetu tak, abyste mohli p ijímat aktualizace automaticky.

Zm na nastavení p ipojení k Internetu:

1. P ejd te na hlavní panel a klepn te pravým tla ítkem na ikonu zcela vpravo.
   Zobrazí se místní nabídka.
2. Vyberte p íkaz **Otev ít spole ná nastavení**.
3. Klepn te na položku **Automatické aktualizace** > **P ipojení**.
4. V seznamu **P ipojení k Internetu** vyberte zp sob p ipojení po íta e k Internetu.
   - Máte-li k dispozici nep etržité sí ové p ipojení, vyberte možnost **P edpokládat nep etržité p ipojení**.

     Poznámka: Nemá-li po íta trvalé sí ové p ipojení a je nastaveno vytá ení na vyžádání, výb r možnosti **P edpokládat nep etržité p ipojení** m že vést k opakovanému vytá ení.
   - Vybráním možnosti **Rozpoznat p ipojení** se budou aktualizace stahovat, pouze pokud produkt zjistí aktivní sí ové p ipojení.
   - Vybráním možnosti **Rozpoznat p enos** se budou aktualizace stahovat, pouze pokud produkt zjistí jiný sí ový p enos.

     Tip: Máte-li neobvyklou hardwarovu konfiguraci, která zp sobuje, že nastavení **Rozpoznat p ipojení** zjistí aktivní p enos v síti, i když žádný p enos neprobíhá, zm te nastavení na možnost **Zjistit p enosy**.
5. V seznamu **Server proxy HTTP** vyberte, zda po íta používá p ipojení k internetu *server proxy*.

- Je-li po íta p ipojen k internetu p ímo, klepn te na p epína **Bez serveru proxy HTTP**.
- Chcete-li nakonfigurovat nastavení *serveru proxy HTTP*, klepn te na p epína **Ru n konfigurovat server HTTP proxy**.
- Chcete-li použít stejné nastavení *serveru proxy HTTP*, jaké jste nakonfigurovali ve webovém prohlíže i, vyberte možnost **Použít server proxy HTTP mého prohlíže e**.

Kontrola stavu sít ochrany v reálném ase

Na p ipojení sít ochrany v reálném ase závisí správná funkce mnoha funkcí produktu.

Jestliže dochází k problém m se sítí nebo pokud brána firewall blokuje p enos sít ochrany v reálném ase, bude stav Odpojeno. Pokud nejsou nainstalovány žádné funkce produktu, které by vyžadovaly p ístup k síti ochrany v reálném ase, bude stav Nepoužíváno.

Kontrola stavu:

1. P ejd te na hlavní panel a klepn te pravým tla ítkem na ikonu zcela vpravo.
   Zobrazí se místní nabídka.
2. Vyberte p íkaz **Otev ít spole ná nastavení**.
3. Klepn te na položku **Automatické aktualizace** > **P ipojení**.

V ásti **Sí ochrany v reálném ase** se zobrazí aktuální stav sít ochrany v reálném ase.

Zobrazení inností produktu

Akce, které byly provedeny za ú elem ochrany po íta e, m žete vid t na stránce **Oznámení**.

Produkt zobrazí oznámení, když provede ur itou akci, nap . zjistí virus, který zablokuje. N která oznámení m že také zasílat p íslušný poskytovatel služeb, nap . aby vás informoval o dostupnosti nových služeb.

Zobrazení historie oznámení

Oznámení, která byla zobrazena, m žete vid t v historii oznámení.

Zobrazení historie oznámení:

1. P ejd te na hlavní panel a klepn te pravým tla ítkem na ikonu zcela vpravo.
   Zobrazí se místní nabídka.
2. Vyberte p íkaz **Otev ít spole ná nastavení**.
3. Klepn te na položku **Jiné** > **Oznámení**.
4. Klepn te na položku **Zobrazit historii oznámení**.
   Zobrazí se seznam historie oznámení.

Zm na nastavení oznámení

M žete si vybrat typ oznámení, která má produkt zobrazovat.

Zm na nastavení oznámení:

1. P ejd te na hlavní panel a klepn te pravým tla ítkem na ikonu zcela vpravo.
   Zobrazí se místní nabídka.
2. Vyberte p íkaz **Otev ít spole ná nastavení**.
3. Klepn te na položku **Jiné** > **Oznámení**.
4. Výb rem nebo zrušením výb ru možnosti **Povolit zprávy programu** zapnete nebo vypnete zprávy programu.

Po zapnutí tohoto nastavení bude produkt zobrazovat oznámení z nainstalovaných program .

5. Výb rem nebo zrušením výb ru možnosti **Povolit reklamní zprávy** zapnete nebo vypnete reklamní zprávy.
6. Klepn te na tla ítko **OK**.

Sí ochrany v reálném ase

Tento dokument popisuje Sí ochrany v reálném ase, online službu spole nosti F-Secure Corporation, která identifikuje isté aplikace a webové stránky a poskytuje ochranu p ed škodlivým softwarem a prost edky zneužití webových stránek.

Co je Sí ochrany v reálném ase

Sí ochrany v reálném ase je online služba, která poskytuje rychlou odpov proti internetovým hrozbám.

Jako p isp vatel do Sít ochrany v reálném ase nám m žete pomoci posílit ochranu proti novým hrozbám. Sí ochrany v reálném ase shromaž uje statistiky o ur itých neznámých, škodlivých nebo podez elých aplikacích a o tom, co mohou po íta i zp sobit. Tyto informace jsou anonymní a jsou zasílány spole nosti F-Secure Corporation, která provádí hromadnou analýzu shromážd ných dat. Analyzované informace používáme pro vylepšení zabezpe ení vašeho po íta e proti nejnov jším hrozbám a škodlivým soubor m.

Jak funguje Sí pro ochranu v reálném ase

Jako p isp vatel do Sít ochrany v reálném ase m žete poskytovat informace o neznámých aplikacích a webových stránkách a o škodlivých aplikacích na nich. Sí ochrany v reálném ase nesleduje vaši innost na webu ani neshromaž uje informace o webových stránkách, které již byly analyzovány. Rovn ž neshromaž uje informace o istých aplikacích, které byly na vašem po íta i nainstalovány.

Pokud nechcete tato data poskytovat, Sí ochrany v reálném ase údaje o instalovaných aplikacích ani navštívených webových stránkách shromaž ovat nebude. Avšak produkt se musí dotazovat server F-Secure na pov st aplikací, webových stránek, sd lení a dalších objekt . Dotazy se p enášejí pomocí kryptografického kontrolního sou tu, p i emž dotazovaný objekt sám se F-Secure nezasílá. Nesledujeme data podle uživatele, pouze se zvyšuje hodnota po ítadla vstupu do souboru nebo na webovou stránku.

Není možné kompletn zastavit veškerou sí ovou komunikaci se Sítí ochrany v reálném ase, protože se jedná o nedílnou sou ást ochrany poskytované produktem.

Výhody Sít ochrany v reálném ase

Se Sítí ochrany v reálném ase získáte rychlejší a p esn jší ochranu proti nejnov jším hrozbám a nebudete dostávat zbyte ná upozorn ní na podez elé aplikace, které nejsou škodlivé.

Jako p isp vatel do Sít ochrany v reálném ase nám m žete pomoci nacházet nový dosud nezjišt ný malware a odstra ovat p ípadná falešná pozitiva z naší databáze vir .

Všichni ú astníci Sít ochrany v reálném ase si navzájem pomáhají. Když Sí ochrany v reálném ase najde ve vašem za ízení podez elou aplikaci, m žete využívat výsledky analýzy, pokud již byla stejná aplikace nalezena v jiných za ízeních. Sí ochrany v reálném ase zlepšuje celkový výkon vašeho za ízení, protože nainstalovaný bezpe nostní produkt nemusí kontrolovat aplikace, které již Sí ochrany v reálném ase analyzovala a zjistila, že jsou nezávadné. Podobn jsou prost ednictvím Sít ochrany v reálném ase sdíleny informace o škodlivých webových stránkách a nevyžádaných hromadných zprávách a jsme schopni vám poskytovat ú inn jší ochranu p ed prost edky zneužití webových stránek a p ed nevyžádanými zprávami.

ím více lidí bude do Sít ochrany v reálném ase p ispívat, tím lépe budou jednotliví ú astníci chrán ni.

Jakými daty p ispíváte

Jako p isp vatel do Sít ochrany v reálném ase poskytujete informace o aplikacích uložených na vašem po íta i a webových stránkách, které navšt vujete, aby vás Sí ochrany v reálném ase mohla ochránit proti nejnov nšjím škodlivým aplikacím a podez elým webovým stránkám.

Analýza pov sti souboru

Sí ochrany v reálném ase shromaž uje pouze informace o aplikacích, jejichž pov st není známa a o souborech, které jsou podez elé nebo se o nich ví, že jsou škodlivé.

Sí ochrany v reálném ase shromaž uje anonymní informace o nezávadných a podez elých aplikacích ve vašem za ízení. Sí ochrany v reálném ase shromaž uje pouze informace o spustitelných souborech (jako jsou p enosné spustitelné soubory v platform Windows, které mají p ípony CPL, EXE, DLL, OCX, SYS, SCR a DRV).

Shromážd né informace obsahují:

- cestu k umíst ní, v n mž se nachází aplikace ve vašem za ízení,
- velikost souboru a dobu jeho vytvo ení nebo zm ny,
- atributy a oprávn ní souboru,
- informace o podpisu souboru,
- aktuální verzi souboru a spole nost, která jej vytvo ila,
- p vod souboru nebo adresu URL, odkud byl stažen,
- výsledky analýzy aplikace F-Secure DeepGuard a antivirového programu kontrolovaných soubor a
- další podobné informace.

Sí ochrany v reálném ase nikdy neshromaž uje údaje z vašich osobních dokument , pokud nejsou infikovány. U všech typ nebezpe ných soubor shromaž uje názvy infekcí a stav dezinfekce soubor .

Prost ednictvím Sít ochrany v reálném ase m žete rovn ž odesílat podez elé aplikace k analýze. Aplikace, které zašlete, musí být výhradn typu p enosného spustitelného souboru. Sí ochrany v reálném ase nikdy neshromaž uje informace o vašich osobních dokumentech a rovn ž je nikdy automaticky nezasílá k analýze.

Odeslání soubor k analýze

Pomocí sít ochrany v reálném ase m žete také odesílat podez elé aplikace k analýze.

Jednotlivé podez elé aplikace m žete odeslat ru n , když vás k tomu produkt vyzve. Odesílat lze pouze p enosné spustitelné soubory. Sí ochrany v reálném ase v žádném p ípad nenahrává osobní dokumenty.

Analýza pov sti webové stránky

Sí ochrany v reálném ase nesleduje vaši webovou aktivitu ani neshromaž uje informace o webových stránkách, které již byly analyzovány. Kontroluje, zda jsou vámi navštívené webové stránky bezpe né. Když navštívíte webovou stránku, zkontroluje Sí ochrany v reálném ase její bezpe nost a upozorní vás, když je tato stránka hodnocena jako podez elá nebo škodlivá.

Pokud webová stránka, kterou navštívíte, obsahuje škodlivý nebo podez elý obsah nebo je známa jako prost edek ke zneužití, Sí ochrany v reálném ase zaznamená celou URL adresu stránky, aby bylo možno analyzovat její obsah.

Pokud navštívíte stránku, která zatím nebyla hodnocena, Sí ochrany v reálném ase zaznamená názvy domén a poddomén a v n kterých p ípadech i cestu k navštívené stránce, aby bylo možno ji analyzovat a vyhodnotit. Všechny parametry URL, které by mohly obsahovat informace, které by mohly být jakýmkoli zp sobem spojovány s vámi a mohly by vás osobn identifikovat, budou pro ochranu vašeho soukromí odstran ny.

Poznámka: Sí ochrany v reálném ase nehodnotí ani neanalyzuje webové stránky v soukromých sítích, takže nikdy nebude zaznamenávat žádné informace z IP adres v soukromých sítích (nap íklad v podnikových intranetech).

Analýza systémových informací

Sí ochrany v reálném ase zaznamenává informace o názvu a verzi vašeho opera ního systému, o internetovém p ipojení a o statistikách využívání sít pro ochranu v reálném ase (nap íklad po et dotaz na pov st webové stránky a pr m rná doba vrácení výsledku dotazu), abychom mohli službu neustále monitorovat a vylepšovat.

Jak chráníme vaše soukromí

Všechny informace p enášíme bezpe n a automaticky odstra ujeme veškeré osobní informace, které by mohly být v datech obsaženy.

Sí ochrany v reálném ase odstra uje identifika ní údaje p ed odesláním do F-Secure a šifruje všechny shromážd né informace pro p enos, aby je chránila p ed neoprávn ným p ístupem. Shromážd né infomace se nezpracovávají individuáln , spojují se s informacemi od jiných p isp vatel do Sít ochrany v reálném ase. Všechna data jsou analyzována statisticky a anonymn , což znamená, že podle žádných dat nebude možno identifikovat vaši osobu.

Žádné informace, které by vás mohly identifikovat, se ve shromážd ných datech nenacházejí. Sí ochrany v reálném ase neshromaž uje adresy IP ani žádné jiné soukromé informace, jako jsou e-mailové adresy, uživatelská jména a hesla. A koli se snažíme ze získaných informací odstranit veškerá data, která by vás mohla identifikovat, je možné, že zde i p es tuto snahu n která z t chto dat z stanou. V takových p ípadech nebudeme takto neúmysln shromážd ná data používat k vaší identifikaci.

Uplat ujeme p ísná bezpe nostní opat ení a fyzické, administrativní a technické ochranné prost edky, abychom ochránili shromážd né informace p i p enosu, ukládání a zpracování. Informace se uchovávají v zabezpe ených úložištích a na serverech, nad nimiž máme kontrolu a které jsou umíst ny bu v našich kancelá ích nebo v kancelá ích našich subdodavatel . Ke shromážd ným informacím má p ístup pouze autorizovaný personál.

F-Secure m že shromážd ná data sdílet se svými pobo kami, subdodavateli, distributory a partnery, ale pouze v anonymním formátu, aby nemohla sloužit k identifikaci.

Jak se stát p isp vatelem Sít ochrany v reálném ase

M žete nám pomoci vylepšovat provoz Sít ochrany v reálném ase tak, že budete p ispívat informacemi o škodlivých programech a webových stránkách.

B hem instalace se m žete rozhodnout, zda se stanete p isp vatelem Sít ochrany v reálném ase. P ednastaveno je, že se p isp vatelem stanete a budete do Sít ochrany v reálném ase p ispívat svými informacemi. Toto nastavení m žete kdykoliv pozd ji zm nit.

Chcete-li zm nit nastavení Sít ochrany v reálném ase, postupujte podle následujících pokyn :

1. P ejd te na hlavní panel a klepn te pravým tla ítkem na ikonu zcela vpravo.
   Zobrazí se místní nabídka.
2. Vyberte p íkaz **Otev ít spole ná nastavení**.
3. Klepn te na položku **Jiné** > **Ochrana osobních dat**.
4. Zatrhn te polí ko ú astníka a stanete se p isp vatelem Sít ochrany v reálném ase.

Dotazy týkající se Sít ochrany v reálném ase

Kontaktní informace pro jakékoli dotazy týkající se Sít ochrany v reálném ase.

Máte-li jakékoli dotazy týkající se Sít ochrany v reálném ase, obra te se prosím na následující kontakty:

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finsko

http://www.f-secure.com/en/web/home_global/support/contact

Nejnov jší verze t chto zásad je vždy k dispozici na našem webu.

Ov ení platnosti p edplatného

Typ a stav vaší registrace se zobrazí na stránce **Stav registrace**.

Když se blíží datum vypršení platnosti registrace nebo již platnost registrace vypršela, v odpovídající ikon na hlavním panelu se zm ní celkový stav ochrany programu.

Kontrola platnosti p edplatného:

1. P ejd te na hlavní panel a klepn te pravým tla ítkem na ikonu zcela vpravo.
   Zobrazí se místní nabídka.
2. Vyberte p íkaz **Zobrazit moje registrace**.
3. Klepnutím na položku **Stav registrace** zobrazíte informace o registracích nainstalovaných program .
4. Výb rem možnosti **Stav instalace** zobrazíte programy, které jsou k dispozici pro instalaci.

Stav registrace a datum vypršení platnosti se zobrazí také na stránce **Statistika** p íslušného programu. Pokud platnost registrace vypršela, bude nutné registraci obnovit, aby bylo možné i nadále získávat aktualizace a používat produkt.

Poznámka: Ikona stavu produktu na hlavním panelu po vypršení platnosti p edplatného bliká.

Centrum akcí

V centru akcí se zobrazují veškerá d ležitá upozorn ní, která vyžadují vaši pozornost.

Pokud vypršela nebo brzy vyprší platnost vaší registrace, centrum akcí vás na to upozorní. Barva pozadí a obsah zprávy centra akcí závisí na typu a stavu registrace:

- Jestliže se blíží konec platnosti vaší registrace a jsou k dispozici bezplatné registrace, zpráva má bílé pozadí a obsahuje tla ítko **Aktivovat (Activate)**.
- Jestliže se blíží konec platnosti vaší registrace a nejsou k dispozici bezplatné registrace, zpráva má žluté pozadí a obsahuje tla ítka **Koupit (Buy)** a **Zadat klí (Enter key)**. Pokud jste již zakoupili novou registraci, m žete klepnout na tla ítko **Zadat klí (Enter key)**, zadat registra ní klí a novou registraci aktivovat.
- Pokud vypršela platnost vaší registrace a jsou k dispozici bezplatné registrace, zpráva má ervené pozadí a obsahuje tla ítko **Aktivovat (Activate)**.
- Jestliže vypršela platnost vaší registrace a nejsou k dispozici bezplatné registrace, zpráva má ervené pozadí a obsahuje tla ítka **Koupit (Buy)** a **Zadat klí (Enter key)**. Pokud jste již zakoupili novou registraci, m žete klepnout na tla ítko **Zadat klí (Enter key)**, zadat registra ní klí a novou registraci aktivovat.

Poznámka: Klepnutím na odkaz **Zobrazit historii upozorn ní (Show notification history)** v centru akcí zobrazíte seznam upozorn ní produktu, nikoli d ív jší zprávy centra akcí.

Aktivace registrace

Když vlastníte nový registra ní klí nebo kód kampan pro produkt, musíte ho aktivovat.

Aktivace registrace:

1. P ejd te na hlavní panel a klepn te pravým tla ítkem na ikonu zcela vpravo.
   Zobrazí se místní nabídka.
2. Vyberte p íkaz **Zobrazit moje registrace**.
3. Vyberte jednu z možností:
   - Klepn te na položku **Aktivovat registraci**.
   - Klepn te na položku **Aktivovat kód kampan** .
4. V dialogovém okn , které se otev e, zadejte nový registra ní klí nebo kód kampan a klepn te na tla ítko **OK**.

   Tip: Pokud jste obdrželi registra ní klí e-mailem, m žete ho zkopírovat z e-mailové zprávy a vložit ho do tohoto pole.

Po zadání nového registra ního klí e se na stránce **Stav registrace** zobrazí nové datum platnosti registrace.

Kapitola

3

Úvod

Témata:

- *Zobrazení celkového stavu ochrany*
- *Zobrazení statistiky produktu*
- *Práce s aktualizacemi produktu*
- *Co jsou viry a další malware?*

Tento produkt chrání váš po íta p ed viry a dalšími škodlivými aplikacemi.

Tento produkt prov uje soubory, analyzuje aplikace a provádí automatické aktualizace. Nevyžaduje žádné zásahy uživatele.

Zobrazení celkového stavu ochrany

Stránka **Stav** zobrazuje rychlý p ehled funkcí instalovaného produktu a jejich aktuální stav.

Otev ení stránky **Stav**:

P ejd te na hlavní stránku a klepn te na položku **Stav**.

Otev e se stránka **Stav**.

Ikony zobrazují stav programu a jeho bezpe nostních funkcí.

Ikona stavu	Název stavu	Popis
	OK	Váš po íta je chrán n. Funkce je zapnutá a pracuje správn .
	Informace	Produkt vás informuje o zvláštním stav funkce. Nap íklad probíhá aktualizace funkce.
	Varování	Váš po íta není pln chrán n. Nap íklad je možné, že produkt nebyl delší dobu aktualizován nebo stav funkce vyžaduje vaši pozornost.
	Chyba	Váš po íta není chrán n. Nap íklad vaše registrace vypršela nebo je vypnuta d ležitá funkce.
	Vypnuto	Nekritická funkce je vypnutá.

Zobrazení statistiky produktu

Akce, které produkt od své instalace provedl, jsou uvedeny na stránce **Statistika**.

Zobrazení stránky **Statistika**:

P ejd te na hlavní stránku a klepn te na položku **Statistika**.

Zobrazí se stránka **Statistika**.

- **Poslední úsp šná kontrola aktualizace** zobrazuje as poslední aktualizace.
- **Kontrola vir a spywaru** zobrazuje kolik soubor produkt od své instalace kontroloval a vy istil.
- Položka **Aplikace** zobrazuje po et program , které aplikace DeepGuard od své instalace povolila nebo zablokovala.
- V ásti **P ipojení brány firewall** je uveden po et povolených a blokovaných p ipojení od instalace.

- ást **Filtrování nevyžádané pošty a phishingu** uvádí, kolik e-mailových zpráv produkt ozna il jako platné e-mailové zprávy a kolik jako nevyžádanou poštu.

Práce s aktualizacemi produktu

Produkt ochranu aktualizuje automaticky.

Zobrazení verzí databází

as a íslo verze poslední aktualizace se zobrazuje na stránce **Aktualizace databáze**.

Otev ení stránky **Aktualizace databáze**:

1. Klepn te na hlavní stránce na možnost **Nastavení**.

   Poznámka: Zm na t chto nastavení vyžaduje oprávn ní správce.

2. Vyberte položky **Jiná nastavení** > **Verze databáze**.

Na stránce **Verze databáze** je uvedeno datum poslední aktualizace definic vir a spywaru, nástroje DeepGuard a filtrování nevyžádané pošty a phishingu a ísla jejich verzí.

Zm na nastavení mobilního širokopásmového p ipojení

Vyberte, zda chcete stahovat aktualizace zabezpe ení, pokud používáte mobilní širokopásmové p ipojení.

Poznámka: Tato možnost je dostupná pouze v opera ním systému Microsoft Windows 7.

Standardn jsou aktualizace zabezpe ení stahovány vždy v síti domácího operátora. Pokud ale navštívíte sí jiného operátora, aktualizace budou pozastaveny. D vodem je možnost odlišných cen p ipojení u r zných operátor , nap íklad v r zných zemích. Toto nastavení m žete ponechat b hem své návšt vy beze zm ny, chcete-li ušet it ší ku pásma a p ípadn i náklady.

Poznámka: Toto nastavení platí pouze pro mobilní širokopásmové p ipojení. Pokud je po íta p ipojen k pevné i bezdrátové síti, produkt je automaticky aktualizován.

Chcete-li zm nit nastavení:

1. Klepn te na hlavní stránce na možnost **Nastavení**.

   Poznámka: Zm na t chto nastavení vyžaduje oprávn ní správce.

2. Vyberte položky **Jiná nastavení** > **Mobilní širokopásmové** > **Stáhnout bezpe nostní aktualizace**.
3. Vyberte preferovanou možnost aktualizací pro mobilní p ipojení:
   - **Pouze v domácí síti operátora**

     Aktualizace jsou vždy stahovány v síti domácího operátora. Pokud navštívíte sí jiného operátora, aktualizace budou pozastaveny. Doporu ujeme, abyste zvolili tuto možnost, pokud chcete zajistit, aby byl produkt zabezpe ení stále aktualizován s o ekávanými náklady.
   - **Nikdy**

     Aktualizace nebudou staženy, pokud používáte mobilní širokopásmové p ipojení.
   - **Vždy**

     Aktualizace jsou stahovány vždy v jakékoliv síti. Vyberte tuto možnost pokud jste si jisti, že chcete mít vždy aktuální zabezpe ení po íta e bez ohledu na náklady.

4. Chcete-li se samostatn rozhodnout vždy, když opouštíte domácí sí operátora, vyberte možnost **Zobrazit dotaz vždy p i opušt ní domácí sít operátora**.

Pozastavené aktualizace zabezpe ení

Aktualizace zabezpe ení mohou být pozastaveny, pokud použijete mobilní širokopásmové p ipojení mimo domácí sí vašeho operátora.

V takovém p ípad se v pravém dolním rohu obrazovky zobrazí oznámení **Pozastaveno**. Aktualizace jsou pozastaveny, protože ceny p ipojení u r zných operátor , nap íklad v r zných zemích, se mohou lišit. Toto nastavení m žete ponechat b hem své návšt vy beze zm ny, chcete-li ušet it ší ku pásma a p ípadn i náklady. Pokud však chcete nastavení zm nit, klepn te na odkaz **Zm nit**.

Poznámka:

Tato možnost je dostupná pouze v opera ním systému Microsoft Windows 7.

Co jsou viry a další malware?

Malware jsou programy navržené speciáln za ú elem poškození po íta e, jeho zneužití k nezákonným aktivitám bez v domí uživatele nebo krádeže informací z po íta e.

Malware m že:

- získat kontrolu nad prohlíže em,
- p esm rovat pokusy o vyhledávání,
- zobrazovat nežádoucí reklamy,
- sledovat navštívené weby,
- krást osobní údaje, nap íklad bankovní,
- použít po íta k rozesílání nevyžádané pošty,
- použít po íta k útoku na jiné po íta e.

Malware také m že vést k nestabilit a snížení výkonu po íta e. Pokud je po íta náhle velmi pomalý a asto dochází k haváriím, je pravd podobné, že se v n m nachází *malware*.

Viry

Vir je obvykle program, který se p ipojí k soubor m a dále se sí í. M že m nit a p esunovat obsah jiných soubor , a tím poškodit po íta .

Vir je program, který se do po íta e obvykle nainstaluje bez v domí uživatele. Poté se vir snaží dále rozší it. Viry:

- využívají ást systémových prost edk ,
- mohou m nit nebo poškodit soubory v po íta i,
- pravd podobn se pokusí nakazit další po íta e,
- mohou umožnit zneužití po íta e k nezákonným ú el m.

Spyware

Spyware jsou programy, které získávají osobní informace uživatel .

Spyware m že shromaž ovat nap íklad následující osobní údaje:

- navštívené internetové servery,
- e-mailové adresy uložené v po íta i,
- hesla,

- ísla platebních karet.

Spyware se tém vždy instaluje bez výslovného souhlasu uživatele. Spyware m že být nainstalován spolu s užite ným programem, nebo když podvodn p im je ke klepnutí na volbu v zavád jícím p ekryvném okn .

Rootkity

Rootkity jsou programy znesnad ující nalezení *malwaru*.

Rootkity skrývají soubory a procesy, obecn proto aby skryly škodlivé aktivity v po íta i. Když rootkit skrývá *malware*, je t žké jej v po íta i odhalit.

Tento produkt obsahuje speciální kontrolu p ítomnosti rootkit , *malware* se tedy nem že skrývat.

Riskware

Riskware není navržen výslovn pro poškození po íta e, m že ho však ohrozit v p ípad zneužití.

Riskware není p esn totéž co malware. Programy ozna ené jako riskware provád jí n které užite né, avšak potenciáln nebezpe né funkce.

P íklady riskwaru mohou být následující:

- programy rychlého zasílání zpráv, nap íklad IRC (Internet relay chat),
- programy pro p enos soubor z jednoho po íta e do druhého prost ednictvím Internetu,
- programy pro telefonování prost ednictvím Internetu, nap . protokol VoIP (*Voice Over Internet Protocol*).
- software pro vzdálený p ístup, nap íklad VNC,
- scareware, který m že jednotlivce hrozbou nebo podvodem p im t k nákupu falešného bezpe nostního softwaru nebo
- software navržený k obejití kontrol CD nebo ochran proti kopírování.

Pokud jste program nainstalovali sami a správn nastavili, snižuje se pravd podobnost, že bude v po íta i škodit.

Pokud byl riskware nainstalován bez vašeho v domí, byl pravd podobn nainstalován se škodlivými úmysly a m l by být odstran n.

Kapitola

4

Ochrana po íta e proti malwaru

Témata:

- *Kontrola po íta e*
- *Jak vylou it soubory z kontroly*
- *Jak využívat karanténu?*
- *Co je DeepGuard?*

Kontrola vir a spywaru chrání po íta p ed programy, které mohou ukrást osobní informace, poškodit váš po íta nebo ho použít k nezákonným ú el m.

Program standardn ošet í všechny typy malwaru bezprost edn poté, co jsou nalezeny, takže nemohou nijak uškodit.

Dle výchozího nastavení prohledává kontrola vir a spywaru vaše lokální disky, všechna vým nná média (jako jsou p enosné jednotky a kompaktní disky) a stažený obsah automaticky. M žete také nastavit automatickou kontrolu e-mail .

Kontrola vir a spywaru také sleduje jakékoliv zm ny ve vašem po íta i indikující *malware*. Pokud jsou nalezeny jakékoliv nebezpe né zm ny systému (nap íklad systémového nastavení nebo pokusy o zm nu d ležitých systémových proces), služba DeepGuard zastaví innost programu jako by to byl *malware*.

Kontrola po íta e

Pokud je zapnuta funkce hledání vir a spywaru, po íta bude automaticky zkontrolován na škodlivé soubory. Nebo m žete soubory zkontrolovat ru n a nastavit naplánované kontroly.

Doporu ujeme nechat funkci hledání vir a spywaru vždy zapnutou. Soubory zkontrolujte ru n , chcete-li se ujistit, že se v po íta i nenachází žádné škodlivé soubory, nebo pokud chcete zkontrolovat soubory, které jste vylou ili z kontroly v reálném ase.

P i nastavení naplánované kontroly budou p i hledání vir a spywaru odstran ny z po íta e škodlivé soubory v každém zadaném ase.

Automatická kontrola soubor

Kontrola v reálném ase chrání po íta tím, že p i p ístupu kontroluje všechny soubory a blokuje p ístup k soubor m obsahujícím *malware*.

Pokud se po íta pokusí o p ístup k souboru, kontrola v reálném ase soubor zkontroluje na malware, než po íta i umožní p ístup k souboru. Pokud funkce kontroly v reálném ase zjistí jakýkoli škodlivý obsah, uložít soubor do karantény, aby nemohl zp sobit žádné škody.

Má kontrola v reálném ase vliv na výkon po íta e?

Obvykle si kontroly nevšimnete, protože trvá krátce a nevyužívá mnoho systémových prost edk . Množství asu a systémových prost edk využité kontrolou v reálném ase závisí nap íklad na obsahu, umíst ní a typu souboru.

Soubory, jejichž kontrola trvá déle:

- Soubory na vym nitelných médiích, jako jsou disky CD a DVD a p enosné jednotky USB.
- Komprimované soubory, nap íklad soubory *ZIP*.

  Poznámka: Komprimované soubory nejsou ve výchozím nastavení kontrolovány.

Kontrola v reálném ase m že po íta zpomalit v následujících p ípadech:

- máte po íta , který nespl uje systémové požadavky, nebo
- p istupujete sou asn k velkému množství soubor ; nap íklad p i otev ení adresá e, který obsahuje mnoho soubor , které je t eba zkontrolovat.

Zapnutí nebo vypnutí kontroly v reálném ase

Ponechte funkci kontroly v reálném ase zapnutou, aby mohla zabránit *malwaru* v poškození po íta e.

Zapnutí nebo vypnutí kontroly v reálném ase:

1. P ejd te na hlavní stránku a klepn te na položku **Stav**.
2. Klepn te na položku **Zm nit nastavení na této stránce**.

   Poznámka: Vypnutí bezpe nostních funkcí vyžaduje oprávn ní správce.

3. Zapn te nebo vypn te **kontrolu vir a spywaru**.
4. Klepn te na položku **Zav ít**.

Automatické ešení škodlivých soubor

Kontrola v reálném ase m že vy ešit škodlivé soubory automaticky bez jakýchkoli otázek.

Povolení automatického ešení škodlivých soubor p i kontrole v reálném ase:

1. Klepn te na hlavní stránce na možnost **Nastavení**.

   Poznámka: Zm na t chto nastavení vyžaduje oprávn ní správce.

2. Vyberte možnost **Zabezpe ení po íta e** > **Hledání vir a spywaru**.
3. Vyberte možnost **Automaticky vy ešit škodlivé soubory**.

Pokud vyberete, že se škodlivé soubory nemají ešit automaticky, kontrola v reálném ase se vás zeptá, co chcete p i zjišt ní škodlivého souboru d lat.

ešení spywaru

Hledání vir a spywaru blokuje spyware ihned, když se pokusí o spušt ní.

Než se spywarová aplikace spustí, produkt ji zablokuje a umožní vám rozhodnout se, co chcete ud lat.

Vyberte jednu z následujících akcí p i zjišt ní spywaru:

Zvolená akce	Akce provedená se spywarem
Zpracovat automaticky	Nechte produkt rozhodnout, jaká je nejvhodn jší akce pro zjišt ný spyware.
Uložit položku do karantény	P esu te spyware do karantény, kde nem že po íta poškodit.
Odstranit spyware	Odstra te z po íta e všechny spywarové soubory.
Blokovat pouze spyware	Zablokujte p ístup ke spywaru, ale ponechte jej v po íta i.
Vylou it spyware z kontroly	Umož uje spušt ní spywaru a jeho vylou ení z kontrol v budoucnu.

ešení riskwaru

Hledání vir a spywaru blokuje riskware ihned, když se pokusí o spušt ní.

Než se riskwarová aplikace spustí, produkt ji zablokuje a umožní vám rozhodnout se, co chcete ud lat.

Vyberte jednu z následujících akcí p i zjišt ní riskwaru:

Zvolená akce	Akce provedená s riskwarem
Blokovat pouze riskware	Zablokujte p ístup k riskwaru, ale ponechte jej v po íta i.
Uložit riskware do karantény	P esu te riskware do karantény, kde nem že po íta poškodit.
Odstranit riskware	Odstra te z po íta e všechny riskwarové soubory.
Vylou it riskware z kontroly	Umož uje spušt ní riskwaru a jeho vylou ení z kontrol v budoucnu.

Automatické odstran ní stopovacích soubor cookie

Odstran ním stopovacích soubor cookie zabráníte webovým stránkám sledovat stránky, které na internetu navštívíte.

Stopovací soubory cookie jsou malé soubory, které umož ují webovým stránkám zaznamenávat webové stránky, které navštívíte. Podle t chto pokyn vypn te stopovací soubory cookie v po íta i.

1. Klepn te na hlavní stránce na možnost **Nastavení**.

   Poznámka: Zm na t chto nastavení vyžaduje oprávn ní správce.

2. Vyberte možnost **Zabezpe ení po íta e** > **Hledání vir a spywaru**.
3. Vyberte možnost **Odstranit stopovací soubory cookie**.
4. Klepn te na tla ítko **OK**.

Ru ní kontrola soubor

Soubory lze zkontrolovat ru n , nap íklad pokud chcete k po íta i p ipojit externí za ízení, abyste se ujistili, že neobsahují malware.

Spušt ní ru ní kontroly

M žete zkontrolovat celý po íta , p ítomnost konkrétního typu *malwaru* nebo konkrétní umíst ní.

Pokud máte podez ení na výskyt konkrétního typu *malwaru*, m žete zkontrolovat pouze p ítomnost tohoto typu. Máte-li podez ení na konkrétní umíst ní, m žete zkontrolovat pouze tuto ást po íta e. Tyto kontroly budou provedeny mnohem rychleji než kontrola celého po íta e.

Spušt ní ru ní kontroly po íta e:

1. Na hlavní stránce klepn te na šipku pod položkou **Kontrola**.

   Zobrazí se možnosti kontroly.

2. Vyberte typ kontroly.

   Výb rem možnosti **Zm nit nastavení kontroly** optimalizujte ru ní kontrolu po íta e pro hledání vir a dalších škodlivých aplikací.

3. Poku vyberete možnost **Vybrat položku ke kontrole**, zobrazí se okno, ve kterém m žete vybrat umíst ní, které se bude kontrolovat.
   Otev e se **Pr vodce kontrolou**.

Typy kontroly

M žete zkontrolovat celý po íta , p ítomnost konkrétního typu malwaru nebo konkrétní umíst ní.

Následuje seznam r zných typ kontroly:

Typ kontroly	Co je kontrolováno?	Kdy použít tento typ?
Kontrola p ítomnosti vir a spywaru	ásti po íta e, zda neobsahují viry, spyware nebo riskware.	Tento typ kontroly je daleko rychlejší než úplná kontrola. Prohledává pouze ásti systému, které obsahují soubory instalovaných program . Tento typ kontroly se doporu uje, pokud chcete rychle zkontrolovat, zda je po íta istý, protože umož uje efektivn najít a odstranit jakýkoliv aktivní malware z vašeho po íta e.
Kontrola celého po íta e	Celý po íta (interní i externí pevné disky), zda neobsahuje viry, spyware nebo riskware.	Pokud si chcete být zcela jistí, že se v po íta i nenachází malware ani riskware. Tento typ kontroly zabírá nejvíce asu. Kombinuje rychlou kontrolu malwaru a kontrolu pevného disku. Rovn ž kontroluje položky, které by mohly být skryté rootkitem.
Vyberte položky, které se mají kontrolovat	Ur itý soubor, složka nebo jednotka, zda neobsahuje viry, spyware nebo riskware.	Máte-li podez ení, že se malware nachází v ur ité ásti po íta e, nap íklad se zde nachází soubory stažené z potencionáln nebezpe ných zdroj , jako jsou sít P2P (peer-to-peer). asová náro nost kontroly bude záviset na velikosti cíle, který kontrolujete. Kontrola prob hne rychle, pokud nap íklad kontrolujte složku, která obsahuje pouze malé množství menších soubor .
Kontrola p ítomnosti rootkit	D ležité ásti systému, v nichž by podez elá položka mohla zp sobit bezpe nostní problémy. Kontroluje skryté soubory, složky, jednotky nebo procesy	Máte-li podez ení, že je ve vašem po íta i nainstalován rootkit. Pokud byl nap íklad nedávno v po íta i zjišt n malware a chcete se ujistit, že nenainstaloval žádný rootkit.

Kontrola v programu Pr zkumník Windows

V Pr zkumníkovi Windows lze zkontrolovat, zda disk, složka nebo soubor neobsahuje *vir* , *spywaru* a *riskwaru*.

Kontrola disku, složky nebo souboru:

1. Umíst te ukazatel myši na disk, složku nebo soubor, který chcete zkontrolovat, a klepn te na n j pravým tla ítkem.
2. V nabídce zobrazené pravým klepnutím vyberte p íkaz **Zkontrolovat p ítomnost vir ve složkách**. (Název p íkazu závisí na tom, zda je zvolena kontrola disku, složky nebo souboru.)
   Otev e se okno **Pr vodce kontrolou** a spustí se kontrola.

Pokud je nalezen *vir* nebo *spyware*, **Pr vodce kontrolou** vás provede procesem odstran ní viru.

Výb r soubor ke kontrole

Vyberte typy soubor , v nichž chcete kontrolovat p ítomnost *vir* a *spywaru* p i ru ních a plánovaných kontrolách.

1. Klepn te na hlavní stránce na možnost **Nastavení**.

   Poznámka: Zm na t chto nastavení vyžaduje oprávn ní správce.

2. Vyberte položky **Jiná nastavení** > **Ru ní kontrola**.
3. Pod položkou **Možnosti kontroly** zvolte jedno z následujících nastavení:

Zkontrolovat pouze známé typy soubor	Kontrola pouze t ch typ soubor , u nichž je nejv tší pravd podobnost infekce, nap . spustitelných soubor . Výb rem této možnosti kontrolu také zrychlí. Kontrolují se soubory s t mito p íponami: `.ani`, `.asp`, `.ax`, `.bat`, `.bin`, `.boo`, `.chm`, `.cmd`, `.com`, `.cpl`, `.dll`, `.doc`, `.dot`, `.drv`, `.eml`, `.exe`, `.hlp`, `.hta`, `.htm`, `.html`, `.htt`, `.inf`, `.ini`, `.job`, `.js`, `.jse`, `.lnk`, `.lsp`, `.mdb`, `.mht`, `.mpp`, `.mpt`, `.msg`, `.ocx`, `.pdf`, `.php`, `.pif`, `.pot`, `.ppt`, `.rtf`, `.scr`, `.shs`, `.swf`, `.sys`, `.td0`, `.vbe`, `.vbs`, `.vxd`, `.wbk`, `.wma`, `.wmv`, `.wmf`, `.wsc`, `.wsf`, `.wsh`, `.wri`, `.xls`, `.xlt`, `.xml`, `.zip`, `.jar`, `.arj`, `.lzh`, `.tar`, `.tgz`, `.gz`, `.cab`, `.rar`, `.bz2` a `.hqx`.
Zkontroloval obsah komprimovaných soubor	Kontrola archivovaných soubor a složek.
Použít pokro ilo heuristiku	Použití veškeré dostupné heuristiky b hem kontroly pro lepší nalezení nového nebo neznámého malwaru. **Poznámka:** Vyberete-li tuto možnost, kontrola trvá déle a m že vést k více falešným pozitivním výsledk m (neškodné soubory jsou nahlášeny jako podez elé).

4. Klepn te na tla ítko **OK**.

Poznámka: Vylou ené soubory v seznamech vylou ených položek nebudou zkontrolovány, ani když zde vyberete, aby zkontrolovány byly.

Co d lat p i zjišt ní škodlivých soubor

Vyberte, jak chcete naložit se zjišt nými škodlivými soubory.

Chcete-li vybrat akci, která má být provedena p i zjišt ní škodlivého obsahu b hem ru ního prov ování:

1. Klepn te na hlavní stránce na možnost **Nastavení**.

Poznámka: Zm na t chto nastavení vyžaduje oprávn ní správce.

2. Vyberte položky **Jiná nastavení** > **Ru ní kontrola**.
3. V dialogu **P i zjišt ní vir nebo spywaru** vyberte jednu z následujících možností:

Možnost	Popis
Dotázat se (výchozí)	M žete vybrat akci, která má být provedena, pro všechny položky zjišt né b hem ru ního prov ování.
Vylé it soubory	Produkt se pokusí o automatické vylé ení nakažených soubor nalezených p i ru ní kontrole. **Poznámka:** Pokud produkt nem že nakažený soubor vylé it, bude uložen do karantény (krom p ípad , kdy se soubor nachází v síti nebo na vym nitelném disku),aby nemohl po íta poškodit.
Umístit soubory do karantény	Produkt p esune všechny škodlivé soubory nalezené b hem ru ní kontroly do karantény, v níž nemohou po íta poškodit.
Odstranit soubory	Produkt odstraní všechny škodlivé soubory nalezené b hem ru ního prov ování.
Pouze ohlásit	Produkt ponechá beze zm ny všechny škodlivé soubory, které byly nalezeny b hem ru ního prov ování, protože zaznamenávají výsledky ve zpráv z kontroly. **Poznámka:** Pokud vyberete tuto možnost a kontrola v reálném ase je vypnutá, p ípadný malware m že poškodit po íta .

Poznámka: P i zjišt ní škodlivých soubor b hem naplánované kontroly budou automaticky vylé eny.

Plánování kontroly

Nastavte v po íta i automatické hledání a odstran ní vir a dalších škodlivých aplikací, i když jej nepoužíváte, nebo nastavte pravidelné hledání, abyste zajistili, že po íta bude chrán n.

Postup plánování kontroly:

1. Klepn te na hlavní stránce na možnost **Nastavení**.

   Poznámka: Zm na t chto nastavení vyžaduje oprávn ní správce.

2. Vyberte položky **Jiná nastavení** > **Plánovaná kontrola**.
3. Zapn te možnost **Naplánovaná kontrola**.
4. Vyberte, kdy se má hledání spustit.

Možnost	Popis
Denn	Hledání se bude opakovat každý den.
Týdn	Po íta bude prov ován ve vybrané dny v týdnu. Vybetre dny ze seznamu.
M sí n	Po íta bude prov ován ve vybrané dny v m síci. Chcete-li vybrat dny: 1. Vyberte jednu z možností **Den**. 2. Den v m síci vyberte v seznamu vedle vybraného dne.

5. Vyberte kdy chcete spustit kontrolu vybraných dn .

Možnost	Popis
as spušt ní	Hledání se spustí ve vybraný as.
Po ne innosti po íta e po dobu	Hledání se spustí po ur ité dob ne innosti po íta e.

Naplánovaná kontrola používá nastavení ru ního prov ování p i kontrole po íta e, ale vždy prov uje také archivy a automaticky istí škodlivé soubory.

Kontrola e-mail

Kontrola e-mail vás chrání p ed škodlivými e-maily, které jsou vám zaslány.

Hledání vir a spywaru musí být zapnuto, aby byly e-maily prov ovány na viry.

Postup zapnutí kontroly e-mailu:

1. Klepn te na hlavní stránce na možnost **Nastavení**.

   Poznámka: Zm na t chto nastavení vyžaduje oprávn ní správce.

2. Vyberte možnost **Zabezpe ení po íta e** > **Hledání vir a spywaru**.
3. Vyberte možnost **Odstranit škodlivé e-mailové p ílohy**.
4. Klepn te na tla ítko **OK**.

Kdy jsou e-mailové zprávy a p ílohy kontrolovány?

Kontrola vir a spywaru m že odstranit nebezpe ný obsah z e-mail , které p ijímáte.

Kontrola vir a spywaru odstra uje nebezpe né e-mailové zprávy, které p ijímají e-mailové programy, jako nap íklad Microsoft Outlook a Outlook Express, Microsoft Mail nebo Mozilla Thunderbird. Prov uje nešifrované e-mailové zprávy a p ílohy, vždy když je e-mailový program obdrží z poštovního serveru pomocí protokolu POP3.

Funkce hledání vir a spywaru nem že zkontrolovat e-mailové zprávy ve webové pošt , které zahrnují e-mailové aplikace, které b ží ve webovém prohlíže i, jako nap íklad Hotmail, Yahoo! mail nebo Gmail. Stále budete chrán ni p ed *viry*, i když neodstraníte škodlivé p ílohy nebo používáte webovou poštu. Když e-mailovou p ílohu otev ete, kontrola v reálném ase odstraní jakékoli škodlivé p ílohy, než zp sobí jakoukoli škodu.

Poznámka: Kontrola v reálném ase chrání pouze váš po íta , ale ne vaše p átele. Kontrola v reálném ase neprov uje p ipojené soubory, pokud p ílohu neotev ete. To znamená, že pokud používáte webovou poštu a zprávu p epošlete p ed otev ením této p ílohy, m žete p átel m p eposlat nakažený e-mail.

Zobrazení výsledk kontroly

V historii vir a spywaru se zobrazují všechny škodlivé soubory, které produkt zjistil.

N kdy produkt nem že provést akci, kterou jste vybrali p i zjišt ní škodlivých položek. Nap íklad pokud vyberete, že chcete soubory vylé it, a není možné je vylé it, produkt je p esune do karantény. Tyto informace najdete v historii vir a spywaru.

Zobrazení historie:

1. Klepn te na hlavní stránce na možnost **Nastavení**.

   Poznámka: Zm na t chto nastavení vyžaduje oprávn ní správce.

2. Vyberte možnost **Zabezpe ení po íta e** > **Hledání vir a spywaru**.
3. Klepn te na možnost **Zobrazit historii odstran ní**.

V historii vir a spywaru jsou uvedeny následující informace:

- datum a as zjišt ní škodlivého souboru,
- název malwaru a jeho umíst ní v po íta i,
- provedená akce.

Jak vylou it soubory z kontroly

N kdy možná budete chtít vylou it n které soubory nebo aplikace z kontroly. Vylou ené položky nebudou zkontrolovány, dokud je neodstraníte ze seznamu vylou ených položek.

Poznámka: Seznamy vylou ených položek lze samostatn zkontrolovat v reálném ase nebo ru n . Pokud nap íklad vylou íte soubor z kontroly v reálném ase, bude zkontrolován b hem ru ní kontroly, pokud je z ru ní kontroly taktéž nevylou íte.

Typy vylou ených soubor

Když soubory vylou íte dle typu, soubory s vybranými p íponami nebudou prov eny na škodlivý obsah.

P idání nebo odstran ní soubor ur itého typu, které chcete vylou it:

1. Klepn te na hlavní stránce na možnost **Nastavení**.

   Poznámka: Zm na t chto nastavení vyžaduje oprávn ní správce.

2. Vyberte, zda chcete vylou it soubory ur itého typu z kontroly v reálném ase nebo z ru ní kontroly:
   - Výb rem položek **Zabezpe ení po íta e** > **Hledání vir a spywaru** lze z kontroly v reálném ase vylou it ur itý typ soubor .
   - Výb rem položek **Jiná nastavení** > **Ru ní kontrola** lze z kontroly v reálném ase vylou it ur itý typ soubor .
3. Kl pnete na možnost **Vylou it soubory z kontroly**.
4. Postup vylou ení typu souboru:
   a) P ejd te na kartu **Typy soubor** .
   b) Vyberte volbu **Vylou it soubory s t mito p íponami**.
   c) Napište do pole vedle tla ítka **P idat** p íponu, která p edstavuje typ soubor , které chcete vylou it.

      Chcete-li zadat soubory, které nemají p íponu, napište „.“. M žete použít zástupný znak „?“, který p edstavuje jakýkoliv samostatný znak nebo „*“, který p edstavuje libovolný po et znak .

      Chcete-li nap íklad vylou it spustitelné soubory, napište do pole exe.
   d) Klepn te na tla ítko **P idat**.
5. Opakujte p edchozí krok pro jakékoliv soubory s danou p íponou, které chcete z kontroly p ítomnosti vir vylou it.
6. Klepnutím na tla ítko **OK** zav ete dialog **Vylou it z kontroly**.
7. Chcte-li použít nové nastavení, klepn te na tla ítko **OK**.

Vybrané typy soubor budou vylou eny z p íštích kontrol.

Vylou ení soubor podle umíst ní

Když soubory vylou íte dle umíst ní, nebudou soubory ve vybraných jednotkách nebo složkách prov eny na škodlivý obsah.

P idání nebo odstran ní umíst ní soubor , které chcete vylou it:

1. Klepn te na hlavní stránce na možnost **Nastavení**.

Poznámka: Zm na t chto nastavení vyžaduje oprávn ní správce.

2. Vyberte, zda chcete vylou it umíst ní z kontroly v reálném ase nebo z ru ní kontroly:
   - Výb rem položek **Po íta** > **Kontrola vir a spywaru** vylou íte umíst ní z kontroly v reálném ase.
   - Výb rem položek **Po íta** > **Ru ní kontrola** vylou íte umíst ní z ru ní kontroly.
3. Klepn te na možnost **Vylou it soubory z kontroly**.
4. Postup vylou ení souboru, jednotky nebo složky:
   a) P ejd te na kartu **Objekty**.
   b) Vyberte položku **Vylou it objekty (soubory, složky, ...)**.
   c) Klepn te na tla ítko **P idat**.
   d) Vyberte soubor, jednotku nebo složku, které chcete vylou it z kontroly výskytu vir .

      Poznámka: N které jednotky mohou být vym nitelné, nap íklad CD, DVD nebo sí ové jednotky. Sí ové jednotky a prázdné vym nitelné jednotky nemohou být vylou eny.

   e) Klepn te na tla ítko **OK**.
5. Opakujte p edchozí krok pro vylou ení dalších soubor , jednotek nebo složek z kontroly výskytu vir .
6. Klepnutím na tla ítko **OK** zav ete dialog **Vylou it z kontroly**.
7. Klepnutím na tla ítko **OK** použijte nová nastavení.

Vybrané soubory, jednotky nebo složky budou z kontrol v budoucnu vylou eny.

Zobrazení vylou ených aplikací

M žete zobrazit aplikace, které jste vylou ili z kontroly, a odstranit je ze seznamu vylou ených položek, pokud je budete chtít zkontrolovat v budoucnu.

Pokud kontrola v reálném ase nebo ru ní kontrola zjistí aplikaci, která se chová jako spyware nebo riskware, ale víte, že se jedná o bezpe nou aplikaci, m žete ji vylou it z kontroly, aby vás produkt p ed touto aplikací již nevaroval.

Poznámka: Pokud se aplikace chová jako virus nebo jiný škodlivý software, nelze ji vylou it.

Není možné vylou it aplikace p ímo. Nové aplikace se zobrazí v seznamu vylou ených položek, pouze když je vylou íte b hem kontroly.

Postup zobrazení aplikací, které byly z kontroly vylou eny:

1. Klepn te na hlavní stránce na možnost **Nastavení**.

   Poznámka: Zm na t chto nastavení vyžaduje oprávn ní správce.

2. Vyberte, zda chcete zobrazit aplikace, které byly vylou eny z kontroly v reálném ase nebo ru ní kontroly:
   - Výb rem položek **Po íta** > **Kontrola vir a spywaru** zobrazíte aplikace, které byly z kontroly v reálném ase vylou eny.
   - Výb rem položek **Po íta** > **Ru ní kontrola** zobrazíte aplikace, které byly z ru ní kontroly vylou eny.
3. Klepn te na možnost **Vylou it soubory z kontroly**.
4. Klepn te na kartu **Aplikace**.

   Poznámka: Vylou it lze pouze spyware a riskware nikoliv viry.

5. Pokud chcete vylou ené aplikace znovu prov it:
   a) Vyberte aplikaci, kterou chcete zahrnout do kontroly.
   b) Klepn te na tla ítko **Odstranit**.

6. Klepnutím na tla ítko **OK** dialog **Vylou it z kontroly** zav ete.
7. Klepnutím na tla ítko **OK** dialog zav ete.

Jak využívat karanténu?

Karanténa slouží jako úložišt potencionáln nebezpe ných soubor .

Soubory umíst né v karantén se nemohou ší it ani poškodit po íta .

Položky *malwaru*, *spywaru* a *riskwaru* m žete uložit do karantény, pak budou neškodné. V p ípad pot eby je možné aplikace a soubory umíst né v karantén pozd ji obnovit.

Pokud soubor umíst ný v karantén nepot ebujete, m žete jej odstranit. Odstran ním položky umíst né v karantén dojde k jejímu trvalému odstran ní z po íta e.

- Obecn je možné odstranit *malware* umíst ný v karantén .
- Ve v tšin p ípad je možné odstranit *spyware* umíst ný v karantén . *Spyware* umíst ný v karantén m že být sou ástí skute ného softwarového programu a program nemusí po jeho odstran ní fungovat správn . Chcete-li program v po íta i ponechat, m žete *spyware* umíst ný v karantén obnovit.
- *Riskware* umíst ný v karantén m že fungovat jako skute ný softwarový program. Pokud jste program nainstalovali a nastavili sami, m žete jej obnovit. Pokud byl *riskware* nainstalován bez vašeho v domí, pravd podobn tak bylo u in no se škodlivými úmysly a m l by být smazán.

Zobrazení položek v karantén

M žete zobrazit další informace o položkách v karantén .

Zobrazení podrobných informací o položkách v karantén :

1. Klepn te na hlavní stránce na možnost **Nastavení**.

   Poznámka: Zm na t chto nastavení vyžaduje oprávn ní správce.

2. Vyberte možnost **Zabezpe ení po íta e** > **Hledání vir a spywaru**.
3. Klikn te na možnost **Zobrazit karanténu**.
   Na stránce **Karanténa** se zobrazuje celkový po et položek, které jsou uloženy v karantén .
4. Chcete-li zobrazit detailní informace o položkách v karantén , klepn te na položku **Detaily**.

   Obsah m žete t ídit bu podle názvu malwaru nebo podle cesty k souboru.

   Zobrazí se seznam prvních 100 položek spolu s typy položek v karantén , názvy a cestami, kam byly soubory nainstalovány.
5. Chcete-li zobrazit více informací o ur ité položce v karantén , klepn te na ikonu vedle položky ve sloupci **Stav**.

Obnovení položek uložených v karantén

Položky umíst né v karantén lze v p ípad pot eby obnovit.

V p ípad pot eby lze obnovit aplikace a soubory z karantény. Neobnovujte položky z karantény, pokud jsi nejste zcela jisti, že nejsou nebezpe né. Obnovené položky budou p esunuty do p vodního umíst ní v po íta i.

Obnovení položek uložených v karantén

1. Klepn te na hlavní stránce na možnost **Nastavení**.

   Poznámka: Zm na t chto nastavení vyžaduje oprávn ní správce.

2. Vyberte možnost **Zabezpe ení po íta e** > **Hledání vir a spywaru**.
3. Klikn te na možnost **Zobrazit karanténu**.
4. Vyberte položku karantény, kterou chcete obnovit.
5. Klepn te na položku **Obnovit**.

Co je DeepGuard?

Funkce DeepGuard analyzuje obsah soubor a chování aplikací a monitoruje aplikace, které nejsou d v ryhodné.

Funkce DeepGuard blokuje nové a nezjišt né *viry*, *ervy* a jiné nebezpe né aplikace, které se snaží provést zm ny ve vašem po íta i, a zabra uje podez elým aplikacím v p ístupu na Internet.

Když funkce DeepGuard zjistí novou aplikaci, která se snaží provést potenciáln škodlivé zm ny v systému, umož uje spustit aplikaci v bezpe né zón . V bezpe né zón nem že aplikace po íta poškodit. Funkce DeepGuard analyzuje, jaké zm ny se aplikace snaží provést, a na základ toho rozhodn , s jakou pravd podobností se jedná o *malwarovou* aplikaci. Pokud je aplikace pravd podobn *malwarová*, funkce DeepGuard ji zablokuje.

Mezi potenciáln škodlivé zm ny systému, které funkce DeepGuard zjiš uje, pat í následující:

- zm ny nastavení systému (registr systému Windows),
- pokusy o vypnutí d ležitých program systému, nap íklad program zabezpe ení jako je tento produkt,
- pokusy o úpravu d ležitých systémových soubor .

Zapnutí nebo vypnutí funkce DeepGuard

Ponechte funkci DeepGuard zapnutou, aby mohla bránit podez elým aplikacím v provád ní potenciáln škodlivých zm n systému v po íta i.

Pokud máte systém Windows XP, ujist te se, že máte nainstalovánu aktualizaci Service Pack 2, než funkci DeepGuard zapnete.

Zapnutí nebo vypnutí funkce DeepGuard:

1. P ejd te na hlavní stránku a klepn te na položku **Stav**.
2. Klepn te na položku **Zm nit nastavení na této stránce**.

   Poznámka: Vypnutí bezpe nostních funkcí vyžaduje oprávn ní správce.

3. Zapn te nebo vypn te funkci **DeepGuard**.
4. Klepn te na položku **Zav ít**.

Povolení aplikací, které funkce DeepGuard zablokovala

Je možné ídit, které aplikace funkce DeepGuard povolí a které zablokuje.

N ktery m že funkce DeepGuard zablokovat spušt ní bezpe né aplikace, i když chcete aplikaci použít a když víte, že je bezpe ná. To se stává, protože aplikace se pokouší provést zm ny systému, které by mohly být škodlivé. Také m žete aplikaci zablokovat neúmysln , když se zobrazí vyskakovací okno funkce DeepGuard.

Povolení aplikací, které funkce DeepGuard zablokovala:

1. Na hlavní stránce klepn te na možnost **Nástroje**.
2. Klepn te na položku **Aplikace**.
   Zobrazí se seznam **Monitorované aplikace**.
3. Vyhledejte aplikaci, kterou chcete povolit.

Poznámka: Klepnutím na záhlaví sloupce m žete položky v seznamu se adit. Nap íklad klepnutím na sloupec **Povolení** m žete položky v seznamu se adit do skupin povolených a zamítnutých program .

4. Vyberte možnost **Povolit** ve sloupci **Povolení**.
5. Klepn te na položku **Zav ít**.

Funkce DeepGuard umožní aplikaci znovu provést zm ny systému.

Použití funkce DeepGuard v režimu kompatibility

Aby byla zajišt na maximální ochrana, funkce DeepGuard do asn zm ní spušt né programy. N které programy kontrolují, zda nejsou poškozeny nebo zm n ny, a nemusí být s touto funkcí kompatibilní. Nap íklad online hry s anti-cheatingovými nástroji kontrolují, zda nebyly nijak upraveny, p i jejich spušt ní. V t chto p ípadech m žete zapnout režim kompatibility.

Zapnutí režimu kompatibility:

1. Klepn te na hlavní stránce na možnost **Nastavení**.

   Poznámka: Zm na t chto nastavení vyžaduje oprávn ní správce.

2. Vyberte možnost **Zabezpe ení po íta e** > **DeepGuard**.
3. Vyberte možnost **Použít režim kompatibility**.
4. Klepn te na tla ítko **OK**.

Co d lat p i varování na podez elé chování

Funkce DeepGuard monitoruje aplikace, které nejsou d v ryhodné. Pokud se monitorovaná aplikace pokusí p ipojit k Internetu, provést zm ny ve vašem po íta i nebo se chová podez ele, funkce DeepGuard ji zablokuje.

Pokud jste v nastavení funkce DeepGuard vybrali možnost **Varovat na podez elé chování**, funkce DeepGuard vás upozorní, když zjistí potenciáln škodlivou aplikaci nebo když spustíte aplikaci s neznámou pov stí.

Chcete-li se rozhodnout, co se má provést s aplikací, kterou funkce DeepGuard zablokovala:

1. Klepnutím na možnost **Podrobnosti** zobrazíte další informace o programu.
   V podrobnostech jsou uvedeny následující informace:
   - umíst ní aplikace,
   - pov st aplikace v síti s ochranou v reálném ase,
   - jak astí aplikace je.
2. Rozhodn te se, zda je možné aplikaci, kterou funkce DeepGuard zablokovala, v it:
   - Vyberte možnost **Aplikaci v ím. Je možné pokra ovat.**, pokud nechcete aplikaci blokovat.

     Aplikace je pravd podobn bezpe ná, pokud:

     - Funkce DeepGuard aplikaci zablokovala po ur ité vaší akci.
     - Aplikaci znáte.
     - Získali jste aplikaci z d v ryhodného zdroje.
   - Vyberte možnost **Aplikace nev ím. Je t eba ji ponechat blokovanou.**, chcete-li aplikaci nadále blokovat.

     Aplikace je pravd podobn nebezpe ná, pokud:

     - Aplikace není p íliš astá.
     - Pov st aplikace není známa.
     - Aplikaci neznáte.

3. Chcete-li odeslat podez elou aplikaci k analýze:

a) Klepn te na možnost **Nahlásit aplikaci spole nosti F-Secure**.
Produkt zobrazí podmínky odeslání.

b) Klepn te na možnost **P ijmout**, pokud s podmínkami souhlasíte a chcete vzorek odeslat.

Vzorek doporu ujeme odeslat v následujících p ípadech:

- Funkce DeepGuard zablokuje aplikaci, o které víte, že je bezpe ná.
- Máte podez ení, že se m že jednat o *malwarovou* aplikaci.