Kapitola 5

Viry a další havěť – postrach počítačů

5

Virová nákaza se může týkat i vašeho počítače

Důležité: Před počítačovými viry nikdy není opatrnosti nazbyt!

Ptáte se, jak se nákaze vyhnout? Hlavní zásadou je – stejně jako v životě, tak i u počítačů – především prevence! Nedůvěřovat souborům pocházejícím z neověřených a podezřelých zdrojů. Renomované servery pro stahování softwaru, jako je *Stahuj*, *Slunečnice*, *Download.com* a další, si nemohou dovolit distribuovat zavirované programy. Ale virus k vám může proniknout i při prohlížení stránek na Internetu. Měli byste dbát maximální opatrnosti při přenosu souborů z jiného počítače na váš. Potenciálně nebezpečná je jakákoliv zásilka elektronické pošty pocházející z neznámého zdroje a obsahující přílohu. Pokud je navíc připojena výzva, abyste spustili některý z připojených programů, je nebezpečí nákazy téměř jisté.

Zachovat maximální opatrnost by znamenalo odříznout počítač od Internetu i elektronické pošty a do jednotky pro práci s CD, DVD a disketami nalít epoxidovou pryskyřici. Ale k čemu by vám takový počítač byl? Proto je zapotřebí být nejen preventivně opatrný, ale mít po ruce i prostředky aktivní ochrany. A nemějte strach, není jich málo.

Prostředky a informace k boji proti virům

Důležité: Aby byla antivirová ochrana účinná, je třeba mít antivirový program s neustále aktuální virovou databází a funkční rezidentní štít.

Nejdůležitějším prvkem aktivní ochrany počítače je spolehlivý antivirový program. Ani ten však nemůže být všemocný a spoléhat na jeho stoprocentní účinnost by bylo hrubou chybou.

Antivirový program a virová databáze

Ovšem antivirový program sám od sebe nezjistí, že ten či onen soubor je nakažený. Potřebuje k tomu kartotéku „otisků prstů" jednotlivých známých virů – virovou databázi. Z toho je vidět, že antivirový program umí odhalit jen takový zdroj nákazy, který již někdo předtím identifikoval, popsal a charakteristické rysy viru zanesl do databáze. Pravda, existují již i takové programy, které mají určitou inteligenci a dokážou odhalit i viry dosud nepodchycené – ale stoprocentně se nemůžete spolehnout na nic.

Důležité: Nestačí si pořídit nějaký antivirový program, instalovat jej a jednou za měsíc spustit s pocitem bezpečí. Je zapotřebí pravidelně aktualizovat jeho virovou databázi. Ta bývá ke stažení na Internetu, na stránkách distributora programu. Antivirový program bývá schopen si aktualizované verze stahovat sám – v určitých časových intervalech, nebo dokonce mu to je od distributora oznamováno elektronickou cestou.

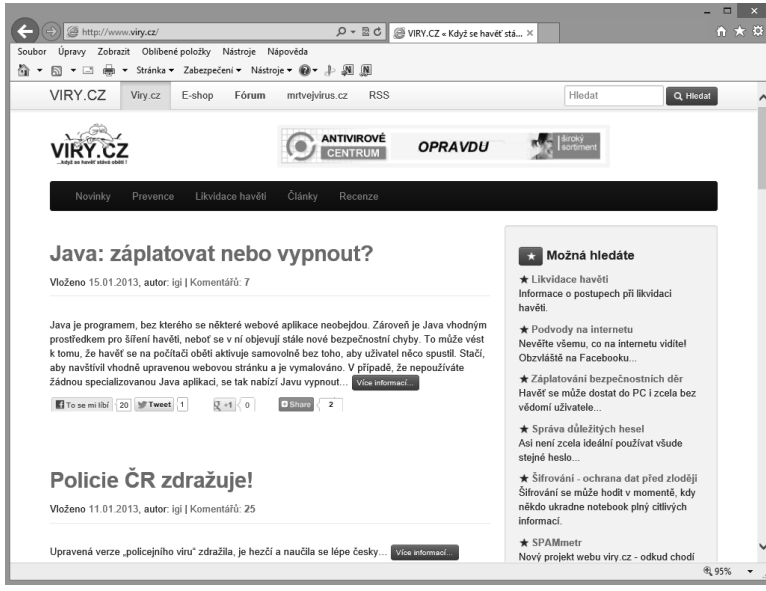
Jak konkrétně antivirový program nastavit, to se liší program od programu. Je dobré akceptovat doporučené výchozí nastavení – je v zájmu autorů takových programů, aby jejich produkty fungovaly optimálně a měly mezi lidmi dobré jméno.

Měli bychom zmínit jeden důležitý pojem. Abyste mohli mít počítač zabezpečený i během práce (v intervalu od jedné kontroly k další), bývá součástí antivirového programu takzvaný *rezidentní štít*. Ten je neustále v pohotovosti a hlídá tok dat. Jakmile by se objevilo něco podezřelého, štít vám zobrazí výstražnou zprávu, a umožní tak zareagovat dříve, než se stane neštěstí.

Poznámka: Antivirový program bývá schopen kontrolovat příchozí i odchozí zásilky elektronické pošty. Ty odchozí pak může opatřit certifikátem, že zpráva byla zkontrolována – což přispěje k většímu klidu příjemce.

Kde najdete informace o virech a boji proti nim?

Informace o virech samozřejmě najdete tam, kde jsou i viry doma – na Internetu. Zkuste třeba navštívit stránku VIRY.CZ – **http://www.viry.cz/**. Jsou tu doopravdy aktuální informace (s prodlevou ne ve dnech nebo týdnech, ale v hodinách). Dále je tu spousta opravdu zajímavých informací o virech a jejich problematice.



Obrázek 5.1 Informace o virech na Internetu

Existuje samozřejmě spousta dalších stránek. Ty výše uvedené vám poslouží i jako rozcestníky, protože obsahují další odkazy na jiné stránky atd.

Zabezpečení počítače přímo od Microsoftu

Nyní si již nemusíte lámat hlavu, jaký antivirový program si pořídit a kolik to bude stát. K dispozici je ochrana, která je již přímo integrovaná ve Windows nebo si ji můžete zdarma stáhnout. Záleží však na tom, jakou verzi Windows používáte.

1. Hledáte-li ochranu pro počítač se starší verzí Windows, můžete si k ochraně před viry, spywarem a škodlivým softwarem všeho druhu zdarma stáhnout a instalovat program Microsoft Security Essentials. Ten poskytuje pro počítače používané v domácnostech a malých firmách bezplatnou ochranu v reálném čase.
2. Pokud pracujete ve Windows 8, máte k dispozici program Windows Defender. Ten nyní poskytuje stejnou úroveň ochrany jako program Microsoft Security Essentials. Zmíněný program již nelze ve Windows 8 používat, ale to není ani potřeba – program Windows Defender ho plně nahrazuje.

Program Windows Defender

Před čím vás Windows Defender může ochránit

Důležité: Program Windows Defender nemusíte nijak instalovat, je organickou součástí Windows 8 a pomáhá chránit počítač před viry, spywarem a jiným potenciálně nežádoucím softwarem (takovým škodlivým programům se dnes souhrnně říkává *malware*).

Malware se může dostat do počítače a infikovat ho téměř odkudkoliv. Jeho zdrojem může být zásilka elektronické pošty, stránky na Internetu, zvláště pak nebezpečná je instalace aplikací z neověřených zdrojů. V tom případě pozor – malware může být naprogramován také tak, aby se spustil obecně kdykoliv, nejen ihned po instalaci.

Tomu všemu má program Windows Defender bránit dvěma způsoby:

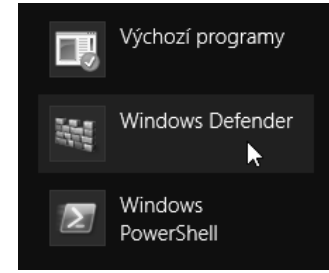
1. Zajištěním ochrany počítače přímo za jeho běhu – v reálném čase. Windows Defender dokáže rozpoznat, že se malware pokouší cosi nainstalovat do počítače nebo v něm spustit, a zabrání tomu. Upozorňuje také na to, že se některá z aplikací pokouší změnit důležitá nastavení.
2. Prohledávání počítače v požadovaném rozsahu na váš povel – v libovolném okamžiku. Tak lze dohledávat malware, který by již mohl být jakýmkoliv způsobem zavlečen do počítače. Lze naplánovat, aby takováto kontrola byla prováděna v pravidelných intervalech. Pokud jsou nalezeny podezřelé soubory, lze je z počítače buď automaticky odebírat, nebo dočasně umístit do tzv. *karantény*.

U každého antivirového programu je vrcholně důležité, aby měl k dispozici aktuální definice malwaru – prostě aby měl škodlivé programy podle čeho rozpoznávat. Proto se neustále udržuje aktuální encyklopedie možných zdrojů nákazy, která dává Windows Defenderu k dispozici potřebné údaje. Při tom se využívá automatická aktualizace a instalace definic na základě spolupráce Defenderu se službou Windows Update. Program Windows Defender se tedy sám stará, aby pracoval stále s aktuálními daty.

Důležité: Program Windows Defender není třeba nějak explicitně spouštět – běží spolu s operačním systémem, takzvaně „na pozadí", a sám na sebe upozorní jen tehdy, potřebuje-li provést nějakou akci a k tomu vyžaduje vaše rozhodnutí.

Okno programu ale můžete kdykoliv zviditelnit a vyžádat či nastavit, cokoliv potřebujete. Podívejme se, jak Windows Defender zviditelníte:

1. V okně prostředí Metro po klepnutí pravým tlačítkem myši v dolní části okna zvolte zobrazení v režimu **Všechny aplikace**.
2. Ve skupině tlačítek **Systém Windows** klepněte na tlačítko **Windows Defender**.



Obrázek 5.2 Spuštění Windows Defenderu

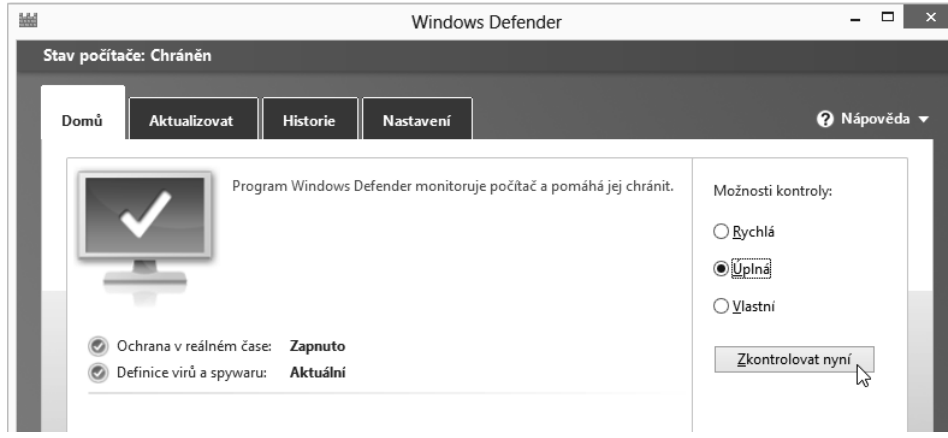
Okno Windows Defenderu se obsluhuje prostřednictvím čtveřice karet s ovladači – **Domů**, **Aktualizovat**, **Historie** a **Nastavení.**

Vyžádání okamžité kontroly počítače

Program Windows Defender si můžete v manuálním režimu práce sami vyzkoušet – vyžádejte si třeba okamžitou kontrolu svého počítače. K tomu je určena karta **Domů**.

Na této kartě jsou zobrazeny indikátory zapojení ochrany v reálném čase a aktuálnosti virové databáze. Ke kontrole počítače vyberte přepínačem **Možnosti kontroly** způsob, jak má být kontrola provedena.

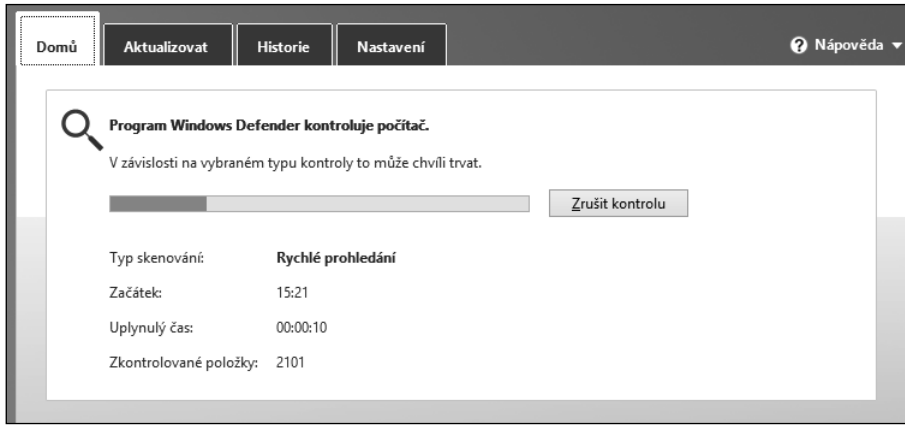
1. **Rychlá kontrola** pokryje oblasti, kde se může nákaza vyskytovat s největší pravděpodobností – je tedy opravdu rychlá, ale zdaleka nezkontroluje celý počítač.
2. Naproti tomu **Úplná kontrola** se týká všech souborů a spuštěných programů. Může však trvat, podle obsazenosti disků, i několik desítek minut.
3. Stiskem tlačítka **Zkontrolovat nyní** kontrolu spustíte.



Obrázek 5.3 – Okamžitá kontrola počítače

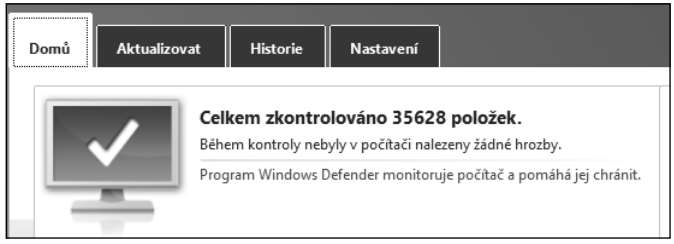
4. Jestliže použijete poslední volbu, **Vlastní**, nabídne se po stisku tlačítka **Zkontrolovat nyní** dialog, ve kterém vyberete ty části počítače, které chcete kontrolovat a které ne. Například si můžete otestovat přenosný hard disk, který jste právě k počítači připojili.

Průběh kontroly je zviditelněn pomocí indikátoru, kde přibližně můžete vidět, jak dlouho ještě kontrola potrvá.



Obrázek 5.4 Kontrola počítače probíhá

Výsledek kontroly poté vidíte na kartě **Domů**. Pokud je vše v pořádku, je údaj vypsán zeleně. Červeně by byly vypsány údaje o nalezených hrozbách.



Obrázek 5.5 Výsledek kontroly

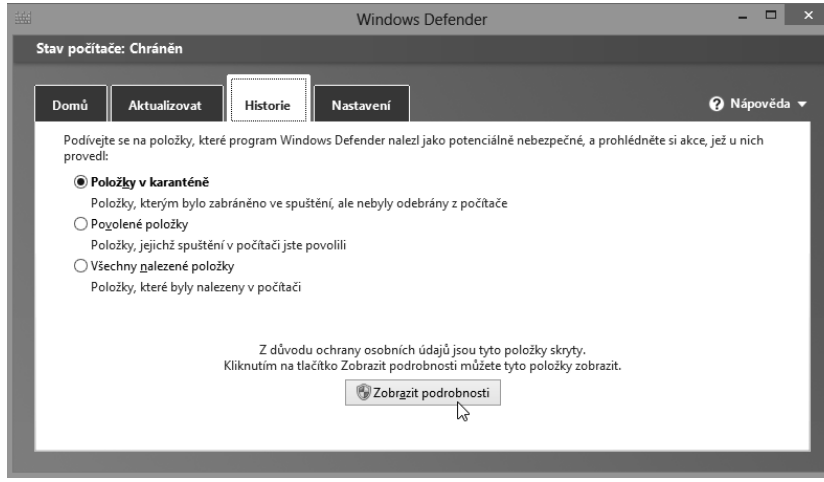
Tip: Kromě barevného rozlišení Defender přiřazuje každému rozpoznanému podezřelému malwaru stupeň výstrahy. Můžete rozhodnout, zda položku zcela odebrat, uložit do „karantény" a tam důkladněji prozkoumat, nebo nechat být, protože ji považujete za bezpečnou.

Jak na podezřelé soubory

Jak ošetřit soubory uložené v karanténě? Stane se, že program Windows Defender při kontrole nedokáže s jistotou určit, zda je rozpoznaná podezřelá položka opravdu malware nebo něco, co jste záměrně nainstalovali. V tom případě zabrání ve spuštění této položky a umístí ji do karantény. Tam sami rozhodnete, jak s položkou naložit. Postup je následující:

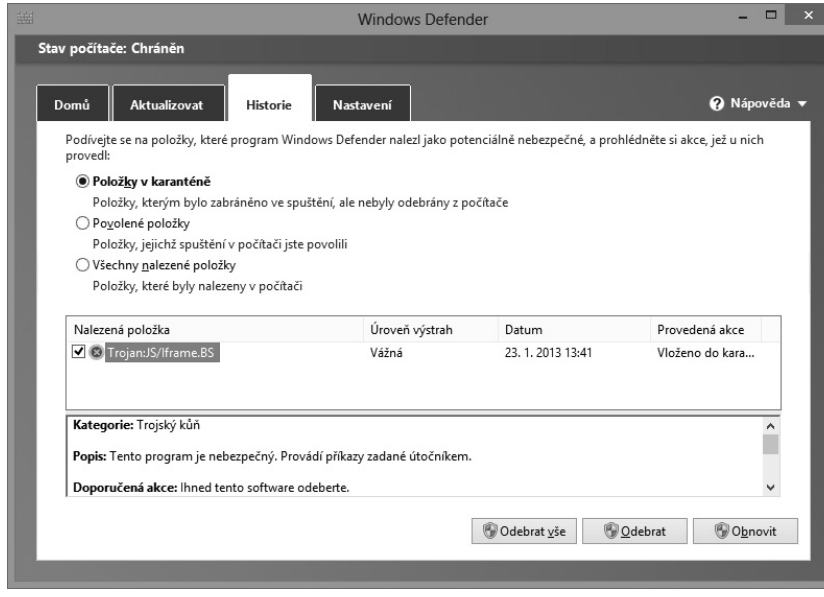
1. Na kartě **Historie** nastavte přepínač na **Položky v karanténě**.

2. Klepněte na tlačítko **Zobrazit podrobnosti**.



Obrázek 5.6 Otevření karantény

3. Proveďte jednu z následujících akcí:
   - Procházejte jednotlivé položky v karanténě. Pokud chcete daný soubor smazat, klepněte na tlačítko **Odebrat**. Pokud jste si jisti, že soubor opravdu není nakažený, klepněte na možnost **Obnovit**.
   - Chcete-li se veškerého softwaru v karanténě zbavit, klepněte na možnost **Odebrat vše**.



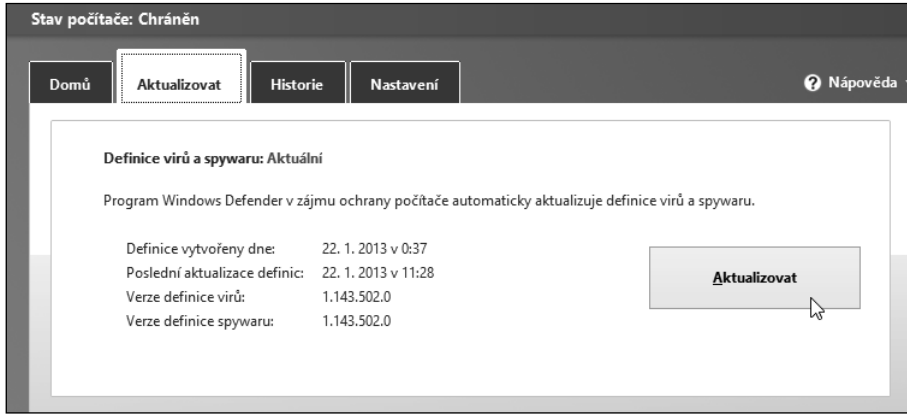
Obrázek 5.7 Infikovaný soubor v karanténě

Aktualizace virové databáze

Řekli jsme si, že se Windows Defender sám stará o to, aby jeho databáze s informacemi o virech byla stále aktuální. Za běžného provozu se tedy této otázce nemusíte věnovat. Je ale jasné, že počítač nemůže aktuálnost databáze sledovat v každém okamžiku – to by nedělal nic jiného.

Tip: Proto může být někdy užitečné, třeba před spuštěním manuální kontroly počítače, aktuálnost databáze zkontrolovat ručně.

Aktualizaci vyžádáte v okně Defenderu tak, že na kartě **Aktualizovat** stisknete stejnojmenné tlačítko.



Obrázek 5.8 Vyžádání okamžité aktualizace

Na kartě je vždy zobrazen údaj o tom, kdy byly vytvořeny používané virové definice a kdy byla databáze na vašem počítači aktualizována naposledy.

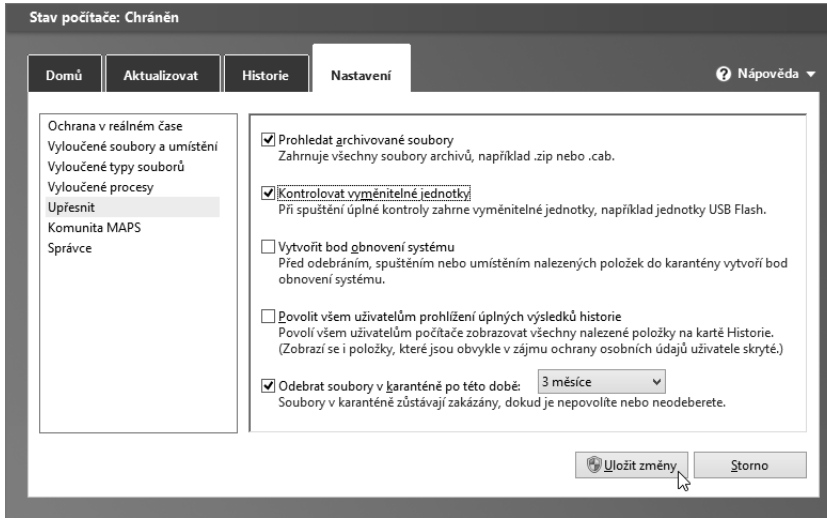
Po stisku tlačítka **Aktualizovat** je kontaktován server s definicemi, a pokud existují novější než váš počítač používá, jsou neprodleně staženy a instalovány.

Nastavení Windows Defenderu

Windows Defender jako program nabízí celou řadu volitelných nastavení. Příznivou zprávou pro ty, kdo takové manipulace nevyhledávají, je to, že program je ve výchozím stavu nastaven tak, aby co nejlépe počítač chránil i bez jakéhokoliv vašeho dodatečného zásahu. Přesto bude užitečné vědět, kde se dají některé provozní parametry nastavit. V okně Windows Defenderu k tomu otevřete kartu **Nastavení**.

Karta se ovládá tak, že v její levé části vyberete klepnutím myší okruh parametrů, které chcete nastavit, a poté v pravé části nastavíte, co je třeba. Upravené parametry pak uložíte tlačítkem **Uložit změny**.

Na kartě lze například přikázat či potlačit (což nelze doporučit) kontrolu počítače v reálném čase. Dále lze z prohledávání vyloučit určité soubory, složky, typy souborů, disky a typy procesů. Je ovšem třeba mít na zřeteli riziko, které z toho plyne.



Obrázek 5.9 Karta Nastavení

Dejte pozor – Defender nemá ve výchozím nastavení zapojenou kontrolu připojených přenosných paměťových zařízení při manuálním spuštění důkladného antivirového testu. Přitom právě tato zařízení mohou obsahovat malware ohrožující nejen daný počítač, ale i další počítače, s nimiž uživatel pracuje.

Oproti samostatně instalovaným antivirovým programům neumožňuje Windows Defender sám o sobě vlastní uživatelské naplánování preventivních antivirových testů.

Poznámka: Ještě dodejme, že Windows Defender se samočinně deaktivuje, pokud je v systému dostupný jiný antivirový program, a po jeho odstranění se případně znovu aktivuje.

Filtr Smart Screen

Důležité: Windows SmartScreen je ve Windows 8 nově koncipovanou funkcí zabezpečení. Chrání počítač před novým malwarem, který program na ochranu před škodlivým softwarem dosud nezjistil. Tak například když si stáhnete a spustíte nějakou aplikaci z Internetu, SmartScreen zhodnotí informace o pověsti této aplikace a upozorní vás, pokud aplikace není příliš známá nebo o ní reference říkají, že by mohla být škodlivá.

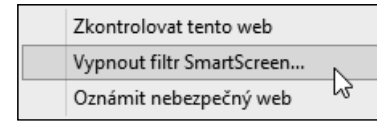
V aplikaci Internet Explorer filtr SmartScreen uživatele upozorní, pokud se chystá navštívit web nebo nějaké konkrétní místo vedené jako nebezpečné. Tak počítač pomůže chránit před škodlivým softwarem a útoky phishing.

Filtr SmartScreen pracuje na pozadí a průběžně (pozor – tedy bez vašeho souhlasu) odesílá adresy vámi navštívených internetových stránek službě SmartScreen společnosti Microsoft. Tam se adresy porovnávají se seznamem adres, ze kterých pocházejí útoky phishing a distri-

buuje se malware. Je-li vámi vyžádaná stránka v tomto seznamu, zobrazí se informace o blokování a panel Adresa bude zvýrazněn červenou barvou. Na stránce s informacemi o blokování můžete na své riziko pokračovat dál na podezřelou stránku nebo se svého úmyslu vzdát.

Jak zkontrolujete funkčnost filtru?

1. Na *Panelu příkazů* klepněte na tlačítko **Zabezpečení**.
2. V místní nabídce klepněte na položku **Filtr SmartScreen** a dále na položku **Zapnout (Vypnout) filtr SmartScreen**.
3. V dialogu **Filtr SmartScreen (od společnosti Microsoft)** zkontrolujte nastavení položky **Zapnout filtr Smart Screen** a klepněte na tlačítko **OK**.



Obrázek 5.10 Příkaz pro zapnutí nebo vypnutí filtru Smart Screen

Obrázek 5.11 Dialog pro zapnutí či vypnutí filtru

Program Microsoft Security Essentials

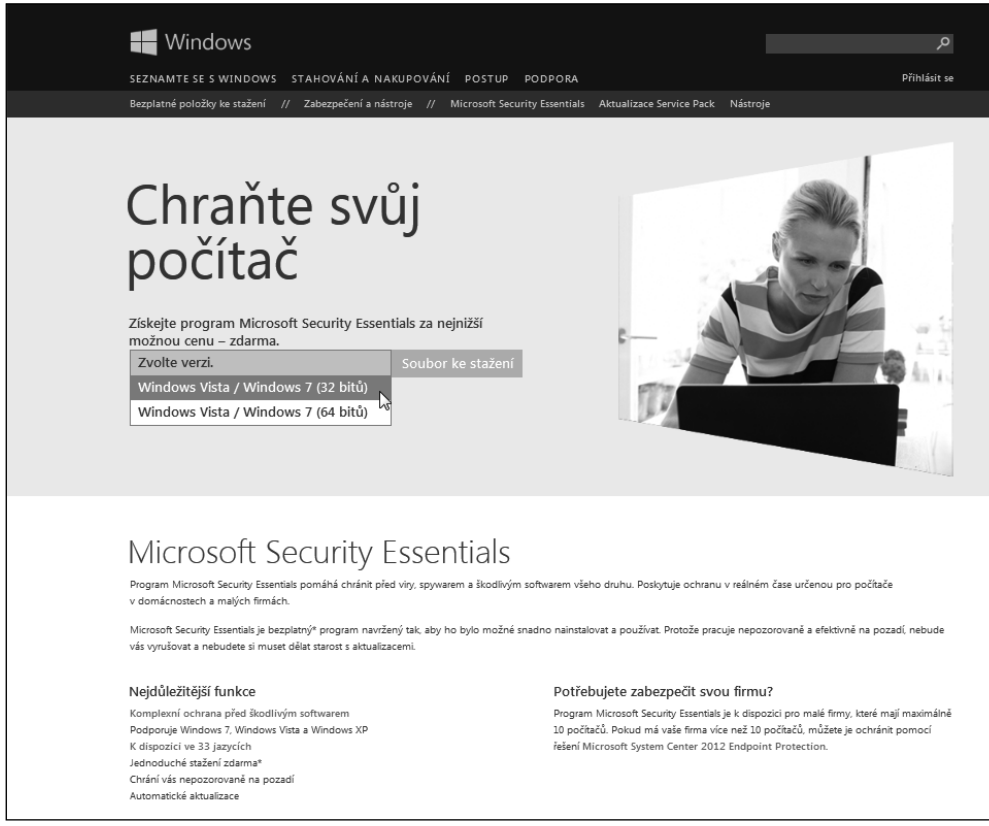
Důležité: Uživatelé Windows 8 tuto kapitolu přeskočí.

Program Microsoft Security Essentials sice nepracuje pod Windows 8, máte-li však starší verzi operačního systému, možná budete chtít tento oblíbený program instalovat. Vedle vyžádaných a naplánovaných kontrol zajišťuje pro váš počítač ochranu v reálném čase a chrání před viry, spywarem a dalším škodlivým softwarem. Po instalaci si program Microsoft Security Essentials hlídá stav své virové databáze, abyste měli jistotu, že stav ochrany je neustále aktuální. Ochrana v reálném čase běží neustále na pozadí, takže mů-

žete počítač používat běžným způsobem a naprosto bez omezení. Spustíte-li okamžitou kontrolu, poběží jako jedna z úloh ve vlastním okně bez zvláštních nároků na prostředky počítače a nebude vás nijak zdržovat.

Stáhněte si program a hned ho instalujte

Antivirový program si stáhnete ze stránek Microsoftu na adrese *http://www.microsoft.com/security_essentials/*.

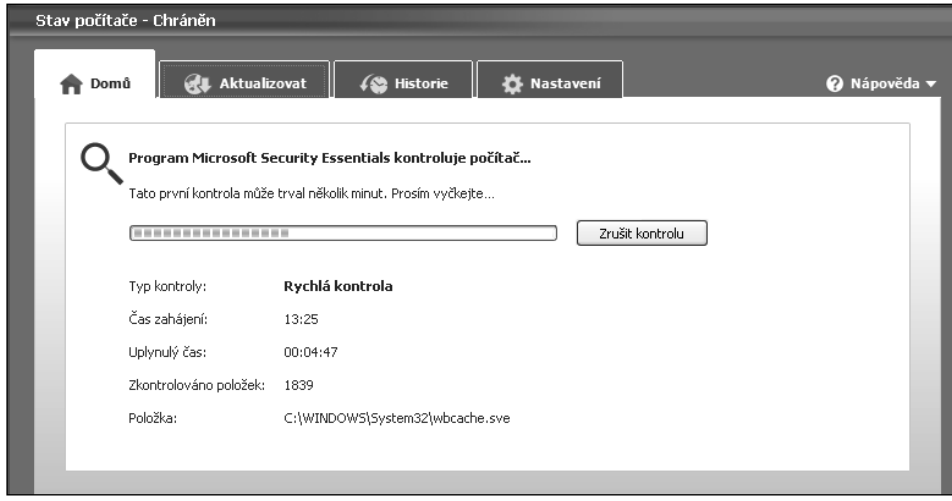


Obrázek 5.12 Stránka pro stažení antivirového programu

Stažení je jednoduché:

1. Nejprve klepněte na okénko **Zvolte verzi** a vyberte verzi operačního systému.
2. Vedla okénka klepněte na tlačítko **Soubor ke stažení**.
3. Využijte možnost uložení instalačního souboru do počítače a po ukončeném stahování přejděte klepnutím na tlačítko **Otevřít složku** přímo k instalačnímu programu.
4. Spusťte instalační program a postupujte podle zobrazovaných instrukcí. Prakticky nic nemusíte nastavit – jen „odklepáváte".

5. Nainstalovaný antivirový program se sám nakonfiguruje do základní podoby, takže nemusíte prakticky nic nastavovat. Také se hned spustí aktualizace virové databáze a poté první kontrola počítače.



Obrázek 5.13 První kontrola

Tip: Všimněte si nápisu **Stav počítače – Chráněn** v hlavičce okna. Text i zelená barva nápisu naznačují, že váš počítač je v této chvíli pod maximální možnou ochranou.

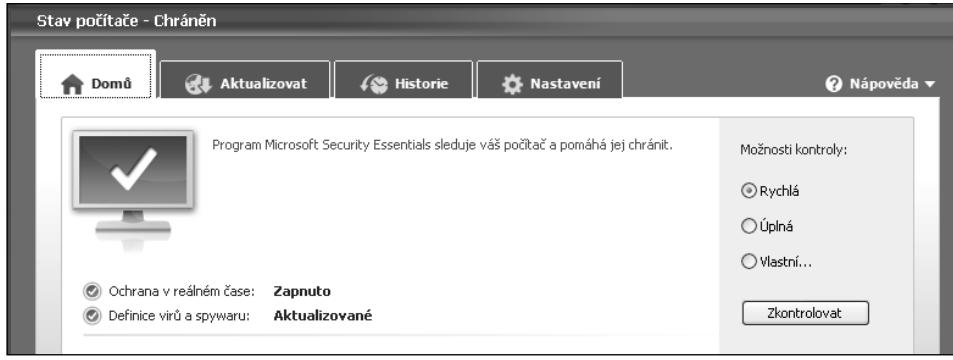
Jak budete program obsluhovat

Prostředí a obsluha jsou velice podobné obsluze programu Windows Defender pro Windows 8. Po instalaci se o program nemusíte vůbec starat – sám se spouští a vytváří „rezidentní štít" chránící vás v průběhu práce. Na rozdíl od Defenderu pro Windows 8 tu ale lze nastavit interval periodického spouštění celkové kontroly počítače, takže nemusíte dělat prakticky nic a přesto můžete mít pocit, že jste pro svůj počítač a jeho bezpečnost udělali velmi záslužný čin. Ovšem pozor – neznamená to, že můžete být lehkomyslní! Žádná ochrana není stoprocentně dokonalá; pokud ji ale posílíte vlastní opatrností, zvýší se její účinnost o hezkých pár desítek procent.

Tip: Přes „skryté působení" během práce lze otevřít okno, kde můžete nastavit některé parametry práce programu a sledovat jeho činnost. Postačí poklepat na ikonku programu na hlavním panelu Windows (zcela vpravo dole).

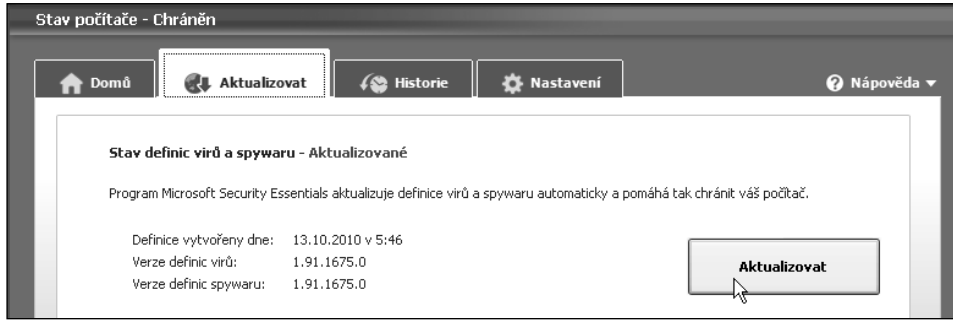
Okno programu Microsoft Security Essentials se skládá ze čtyř karet, které můžete přepínat klepnutím na jejich záložky.

1. Na kartě **Domů** vidíte informace o stavu programu a můžete také spustit okamžitou kontrolu počítače v rozsahu podle nastavení přepínače **Možnosti kontroly**.



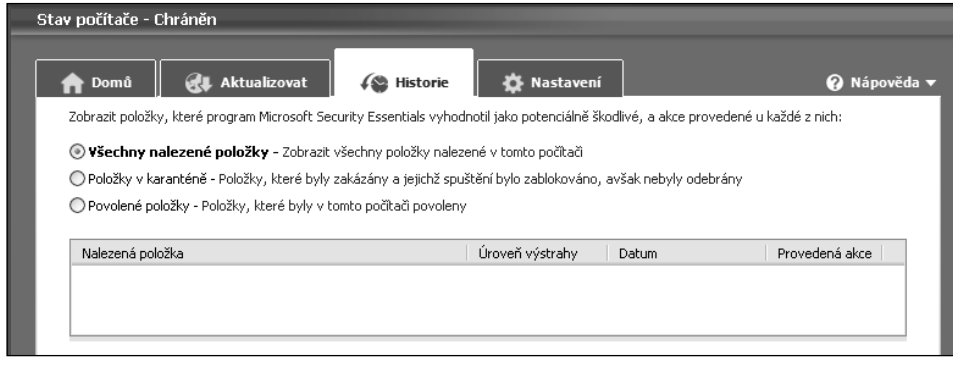
Obrázek 5.14 Karta Domů

2. Pokud kontrola právě běží, zobrazují se na této kartě informace o jejím stavu.
3. Na kartě **Aktualizovat** vidíte údaje o verzi antivirové databáze. Tlačítkem **Aktualizovat** můžete vyžádat okamžitou aktualizaci (existuje-li novější verze).



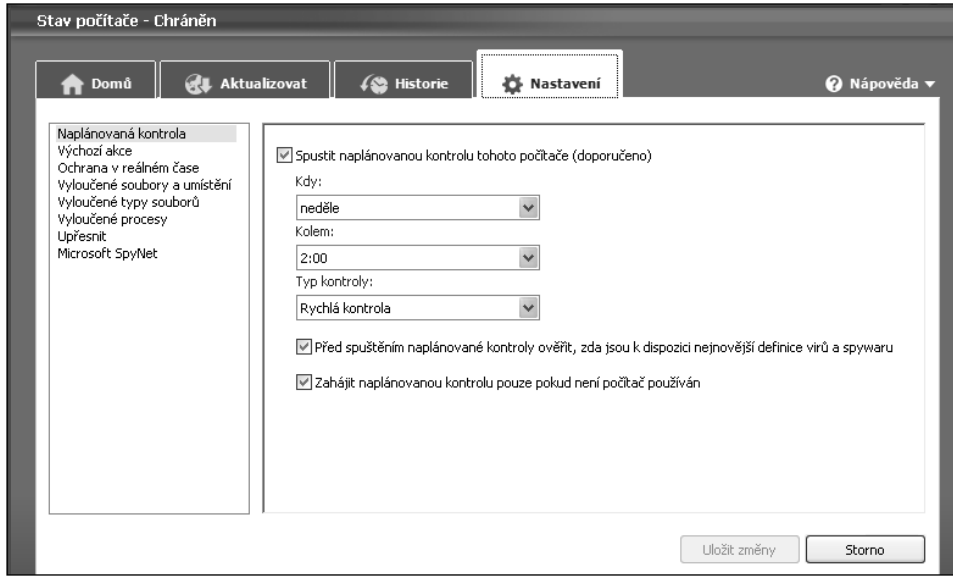
Obrázek 5.15 Karta Aktualizovat

4. Na kartě **Historie** vidíte výčet souborů, které byly v průběhu kontrol označeny jako podezřelé.



Obrázek 5.16 Karta Historie

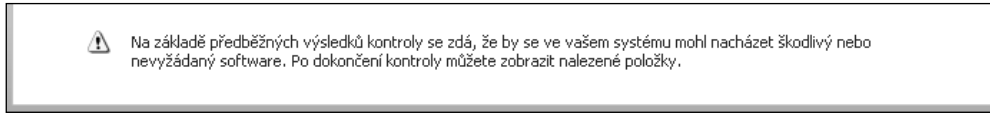
5. Poslední karta – **Nastavení** – vám umožní zkontrolovat a nastavit provozní parametry programu. Například si můžete zvolit, kdy, jak často a v jakém rozsahu má být spuštěna celková kontrola počítače ve zvoleném rozsahu.



Obrázek 5.17 Karta Nastavení

Co když se při kontrole objeví podezřelý soubor?

Pokud se v průběhu kontroly objeví podezřelý soubor, je v dolní části karty **Domů** vypsána varovná zpráva.



Obrázek 5.18 V průběhu kontroly se objevil podezřelý soubor

V takovém případě nic nepodnikejte a v klidu vyčkejte, dokud kontrola neskončí. Hlavička okna antivirového programu nese rudé upozornění **Stav počítače – Ohrožen** a na kartě **Domů** se vypíšou zprávy o tom, které soubory tento stav způsobily.

1. Buďme trochu zvědaví a klepněme na odkaz **Zobrazit podrobnosti** – bez obav, virus se tím nevzbudí.
2. V okénku vidíte podrobnosti o potenciální hrozbě – a v řádku s každým souborem je nabídnuto řešení, jak nebezpečí odstranit. Lze doporučit toto řešení přijmout.
3. Pak již máte vyhráno – zelená barva napovídá, že nebezpečí bylo zažehnáno. Zvídaví si ještě mohou po stisku tlačítka **Zobrazit podrobnosti** přečíst, jak nebezpečný soubor byl a co mohl způsobit.