



AVG Anti-Virus 2011

Uživatelský manuál

Verze dokumentace 2011.23 (6.10.2011)

Copyright AVG Technologies CZ, s.r.o. Všechna práva vyhrazena.
Všechny ostatní obchodní značky jsou majetkem jejich registrovaných vlastníků.

Tento produkt používá RSA Data Security, Inc. MD5 Message-Digest Algorithm, Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991.

Tento produkt obsahuje kód knihovny C-SaCzech, Copyright (c) 1996-2001 Jaromír Doleček (dolecek@ics.muni.cz).

Tento produkt používá kompresní knihovnu libbzip2, Copyright (c) 1996-2002 Julian R. Seward.

Tento produkt používá kompresní knihovnu zlib Copyright (C) 1995-1998 Jean-loup Gailly and Mark Adler.



Obsah

1. Úvod	6
2. Podmínky instalace AVG	7
2.1 Podporované operační systémy	7
2.2 Minimální / doporučené HW požadavky	7
3. Možnosti instalace AVG	8
4. Instalační proces AVG	9
4.1 Vítejte	9
4.2 Aktivujte vaši licenci	9
4.3 Vyberte typ instalace	10
4.4 Uživatelské volby	11
4.5 Instalovat AVG Security Toolbar	12
4.6 Postup instalace	13
4.7 Instalace byla úspěšná	13
5. Po instalaci	15
5.1 Registrace produktu	15
5.2 Otevření uživatelského rozhraní	15
5.3 Spuštění testu celého počítače	15
5.4 Test virem Eicar	15
5.5 Výchozí konfigurace AVG	16
6. Uživatelské rozhraní AVG	17
6.1 Systémové menu	18
6.1.1 Soubor	18
6.1.2 Komponenty	18
6.1.3 Historie	18
6.1.4 Nástroje	18
6.1.5 Nápověda	18
6.2 Informace o stavu zabezpečení	20
6.3 Zkratková tlačítka	21
6.4 Přehled komponent	22
6.5 Statistika	23
6.6 Ikona na systémové liště	23
6.7 Miniaplikace AVG	24



7. Komponenty AVG	27
7.1 Anti-Virus	27
7.1.1 Princip Anti-Viru	27
7.1.2 Rozhraní komponenty Anti-Virus	27
7.2 Anti-Spyware	28
7.2.1 Princip Anti-Spyware	28
7.2.2 Rozhraní komponenty Anti-Spyware	28
7.3 LinkScanner	30
7.3.1 Princip Link Scanneru	30
7.3.2 Rozhraní Link Scanneru	30
7.3.3 Search-Shield	30
7.3.4 Surf-Shield	30
7.4 Rezidentní štít	33
7.4.1 Princip Rezidentního štítu	33
7.4.2 Rozhraní komponenty Rezidentní štít	33
7.4.3 Nálezy Rezidentního štítu	33
7.5 Family Safety	37
7.6 AVG LiveKive	38
7.7 Kontrola pošty	38
7.7.1 Princip Kontroly pošty	38
7.7.2 Rozhraní komponenty Kontrola pošty	38
7.7.3 Nálezy Kontroly pošty	38
7.8 Manažer aktualizací	41
7.8.1 Princip Manažeru aktualizací	41
7.8.2 Rozhraní komponenty Manažer aktualizací	41
7.9 Licence	43
7.10 Vzdálená správa	45
7.11 Webový štít	45
7.11.1 Princip Webového štítu	45
7.11.2 Rozhraní komponenty Webový štít	45
7.11.3 Nálezy Webového štítu	45
7.12 Anti-Rootkit	48
7.12.1 Princip Anti-Rootkitu	48
7.12.2 Rozhraní komponenty Anti-Rootkit	48
7.13 PC Analyzer	50
7.14 ID Protection	52
7.14.1 Princip ID Protection	52



7.14.2 Rozhraní ID Protection	52
7.14.3 Nastavení ID Protection	52
8. AVG Security Toolbar	55
9. Pokročilé nastavení AVG	57
9.1 Vzhled	57
9.2 Zvuky	59
9.3 Ignorovat chybové podmínky	61
9.4 Virový trezor	62
9.5 PUP výjimky	62
9.6 Webový štít	65
9.6.1 Ochrana webu	65
9.6.2 Rychlé zasílání zpráv	65
9.7 LinkScanner	69
9.8 Testy	70
9.8.1 Test celého počítače	70
9.8.2 Test z průzkumníku	70
9.8.3 Test vybraných souborů či složek	70
9.8.4 Test vyměnitelných zařízení	70
9.9 Naplánované úlohy	75
9.9.1 Naplánovaný test	75
9.9.2 Plán aktualizace virové databáze	75
9.9.3 Plán programové aktualizace	75
9.10 Kontrola pošty	85
9.10.1 Certifikace	85
9.10.2 Filtrování e-mailů	85
9.10.3 Servery	85
9.11 Rezydentní štít	93
9.11.1 Pokročilé nastavení	93
9.11.2 Výjimky	93
9.12 Server vyrovnávací paměti	97
9.13 Anti-Rootkit	98
9.14 Aktualizace	99
9.14.1 Proxy	99
9.14.2 Vytáčené připojení	99
9.14.3 URL	99
9.14.4 Správa	99
9.15 Dočasné vypnutí ochrany AVG	105



9.16 Program zlepšování produktu	105
10. AVG testování	108
10.1 Rozhraní pro testování	108
10.2 Přednastavené testy	109
10.2.1 Test celého počítače	109
10.2.2 Test vybraných souborů či složek	109
10.3 Testování v průzkumníku Windows	116
10.4 Testování z příkazové řádky	117
10.4.1 Parametry CMD testu	117
10.5 Naplánování testu	119
10.5.1 Nastavení plánu	119
10.5.2 Jak testovat	119
10.5.3 Co testovat	119
10.6 Přehled výsledků testů	128
10.7 Detail výsledku testu	129
10.7.1 Záložka Přehled výsledků	129
10.7.2 Záložka Infekce	129
10.7.3 Záložka Spyware	129
10.7.4 Záložka Varování	129
10.7.5 Záložka Informace	129
10.8 Virový trezor	136
11. Aktualizace AVG	139
11.1 Úrovně aktualizace	139
11.2 Typy aktualizace	139
11.3 Průběh aktualizace	139
12. Protokol událostí	141
13. FAQ a technická podpora	143



1. Úvod

Tento uživatelský manuál je kompletní dokumentací programu **AVG Anti-Virus 2011**.

Gratulujeme k vaší volbě programu AVG Anti-Virus 2011!

AVG Anti-Virus 2011 je jedním z produktů nové řady oceňovaného bezpečnostního software AVG, jež byl navržen pro klid vaší duše a stoprocentní bezpečnost vašeho PC. Stejně jako všechny produkty nové řady AVG byl i **AVG Anti-Virus 2011** kompletně a od základů postaven tak, aby nadále dostal své pověsti uznávaného bezpečnostního programu a současně nabídl svým uživatelům zcela nové, efektivnější a vysoce uživatelsky přívětivé rozhraní. Nový **AVG Anti-Virus 2011** přináší moderní grafické rozhraní v kombinaci s agresivnějším a rychlejším testováním. Pro větší pohodlí přináší více procesů v plně automatickém režimu a nabízí nové 'inteligentní' uživatelské možnosti, které se přizpůsobí vašim potřebám.

Produkty AVG nabízejí

- Zabezpečení počítače při jakékoliv činnosti na internetu: při používání internetového bankovníctví, elektronickém nakupování, prohlížení a vyhledávání na webu, komunikaci prostřednictvím rychlého zasílání zpráv, e-mailů a sociálních sítí nebo stahování souborů
- Rychlé a efektivní zabezpečení, na které se spoléhá více než 110 milionů uživatelů a jež je podporováno odborníky z celého světa
- Nepřetržitou technickou podporu pro uživatele řady komerčních produktů



2. Podmínky instalace AVG

2.1. Podporované operační systémy

AVG Anti-Virus 2011 je určen k ochraně pracovních stanic s těmito operačními systémy:

- Windows XP Home Edice SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edice SP1
- Windows Vista (x86 a x64, všechny edice)
- Windows 7 (x86 a x64, všechny edice)

(a všechny případné vyšší servisní balíky pro jednotlivé operační systémy)

Poznámka: Komponenta [ID Protection](#) není podporována na Windows XP x64. Na tomto operačním systému lze nainstalovat AVG Anti-Virus 2011, ale pouze bez této komponenty.

2.2. Minimální / doporučené HW požadavky

Minimální hardwarové požadavky pro **AVG Anti-Virus 2011**:

- Procesor Intel Pentium 1,5 GHz
- 512 MB RAM paměti
- 750 MB volného místa na pevném disku (z instalace dříve)

Doporučené hardwarové požadavky pro **AVG Anti-Virus 2011**:

- Procesor Intel Pentium 1,8 GHz
- 512 MB RAM paměti
- 1400 MB volného místa na pevném disku (z instalace dříve)



3. Možnosti instalace AVG

AVG se instaluje buďto z instalačního souboru, který naleznete na instalačním CD, nebo si můžete stáhnout aktuální instalační soubor z webu AVG (<http://www.avg.cz/>).

Před zahájením instalačního procesu AVG doporučujeme navštívit web AVG (<http://www.avg.cz/>) a ověřit, zda se zde nenachází aktuálnější instalační soubor. Tím zajistíte, že budete instalovat vždy nejnovější dostupnou verzi AVG Anti-Virus 2011.

Během instalace budete požádáni o své licenční/prodejní číslo. Ujistěte se proto prosím, že jej máte k dispozici. Prodejní číslo najdete na CD v prodejním balení AVG. Pokud jste AVG zakoupili on-line, vaše licenční číslo vám bylo doručeno emailem.



4. Instalační proces AVG

Pro instalaci **AVG Anti-Virus 2011** na váš počítač budete potřebovat aktuální instalační soubor. Instalační soubor najdete na CD, které bylo součástí zakoupeného balení AVG, ale tento soubor může již být zastaralý. Doporučujeme vám proto navštívit web AVG (<http://www.avg.cz/>), sekce [Centrum podpory / Stáhnout](#) a nejnovější instalační soubor si odtud stáhnout.

Instalace probíhá ve sledu dialogových oken, z nichž každé vysvětluje, co je třeba v konkrétním kroku provést. Popis jednotlivých oken nyní nabízíme:

4.1. Vítejte

Instalační proces je zahájen otevřením dialogu **Vítejte**. V tomto dialogu máte možnost zvolit jazyk, v němž bude instalační proces probíhat a v němž bude následně instalován program AVG. V horní části okna najdete rozbalovací menu s nabídkou jazyků, z nichž si můžete vybrat:



Upozornění: Zde volíte jazyk instalačního procesu. V tomto jazyce bude instalován program AVG, spolu s angličtinou, která se instaluje automaticky. Pokud si přejete nainstalovat další volitelné jazyky, do nichž budete moci uživatelské rozhraní programu přepínat, budete je moci definovat v jednom z následujících dialogů [Uživatelské volby](#).

Dialog dále obsahuje plně znění závazné licenční smlouvy AVG. Text si můžete přečíst a s ním souhlasit licenčním ujednáním potvrzením stiskem tlačítka **Souhlasím**. Pokud s licenční smlouvou nesouhlasíte a stisknete tlačítko **Nesouhlasím**, instalace bude okamžitě ukončena.

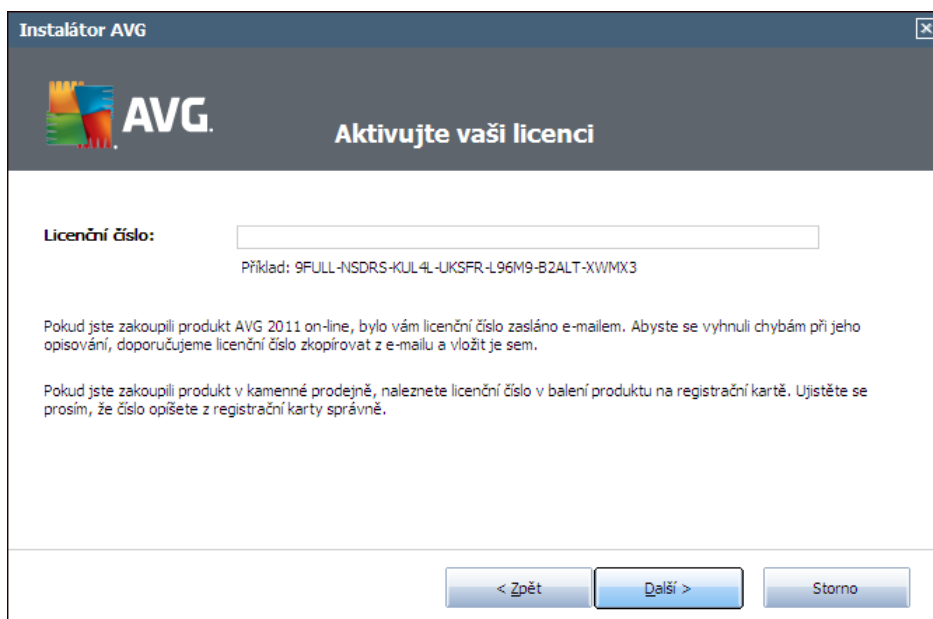
4.2. Aktivujte vaši licenci

V dialogu **Aktivujte vaši licenci** je třeba zadat do textového pole vaše licenční číslo.

Licenční číslo najdete buďto na registrační kartě v krabicovém balení **AVG Anti-Virus 2011**, anebo v potvrzovacím emailu, který jste obdrželi při zakoupení **AVG Anti-Virus 2011** on-line. Licenční číslo

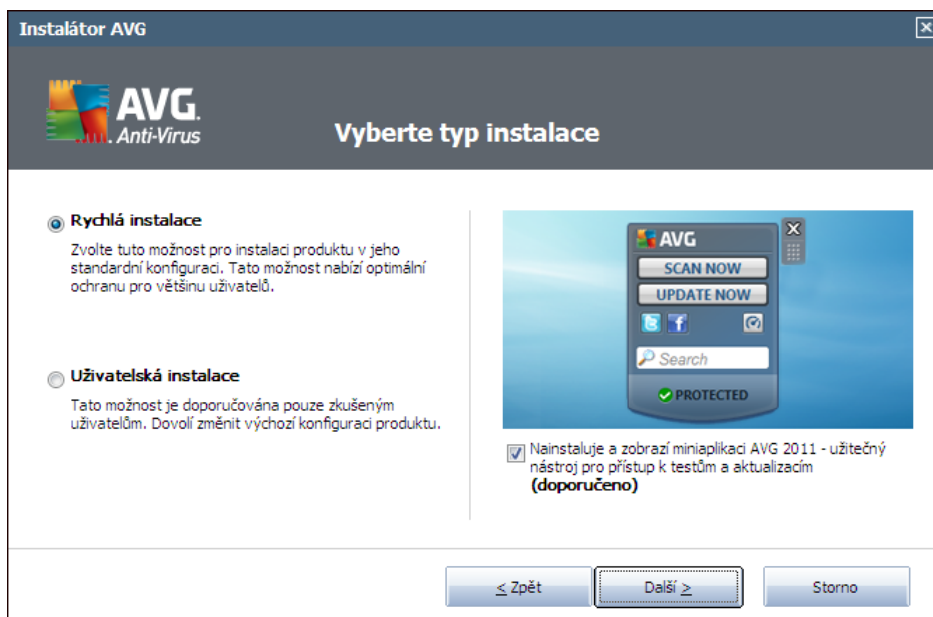


musí být zadáno naprosto přesně ve tvaru, jak je uvedeno, proto prosím věnujte velkou pozornost jeho přesnosti. Pokud máte číslo k dispozici v digitální formě, doporučujeme jej do příslušného pole zkopírovat (*metodou kopírovat a vložit*).



V instalaci pokračujte stiskem tlačítka **Další**.

4.3. Vyberte typ instalace



Dialog **Vyberte typ instalace** vám dává na výběr mezi **rychlou** a **uživatelskou** instalací.



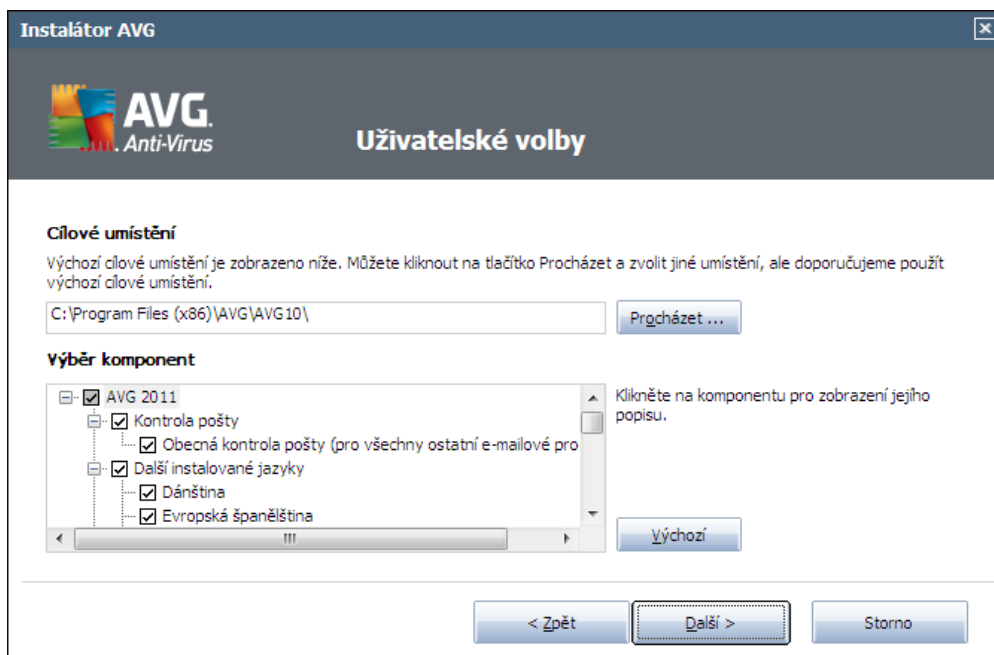
V tšín uživatel doporuujeme použít **rychlou instalaci**, kdy bude AVG nainstalován zcela automaticky s nastavením definovaným výrobcem. Toto nastavení zaručuje maximální úroveň bezpečnosti a optimální využití zdrojů. Pokud se v budoucnu vyskytne potřeba některé konkrétní nastavení změnit, budete mít vždy možnost editovat konfiguraci AVG přímo v aplikaci. Pokud se rozhodnete pro možnost **rychlé instalace**, stiskem tlačítka **Další** postoupíte k dialogu [Instalovat AVG Security Toolbar](#).

Uživatelská instalace je vhodná pouze pro pokročilé a znalé uživatele. Doporučujeme ji pouze v případě, že máte skutečnou potřebu instalovat AVG s nestandardním nastavením tak, aby vyhovovalo specifickým požadavkům vašeho systému. Jestliže zvolíte tuto možnost, po stisku tlačítka **Další** budete přesměrováni k dialogu [Uživatelské volby](#).

V pravé části dialogového okna najdete možnost povolit instalaci **miniaplikace AVG** (*miniaplikace jsou podporovány pouze na OS Windows Vista/Windows 7*). Pokud chcete instalaci miniaplikace povolit, označte příslušné políčko. **Miniaplikace AVG** pak bude dostupná z panelu Windows Sidebar a umožní vám okamžitou dostupnost nejdůležitějších funkcí **AVG Anti-Virus 2011**, a to [testování](#) a [aktualizace](#).

4.4. Uživatelské volby

Dialog **Uživatelské volby** Vám umožní nastavit dva parametry instalace:



Cílové umístění

V sekci **Cílové umístění** máte určit, kam má být program **AVG Anti-Virus 2011** instalován. Ve výchozím nastavení bude program instalován do adresáře programových souborů umístěném typicky na disku C:. Pokud si přejete toto umístění změnit, pomocí tlačítka **Procházet** zobrazíte strukturu vašeho disku a zvolíte požadovaný adresář.



Výběr komponent

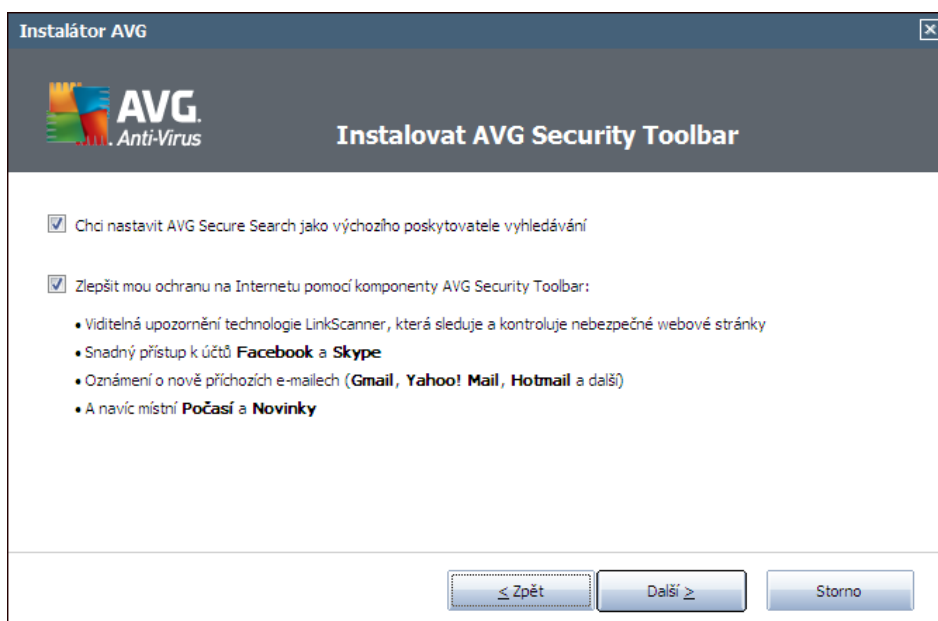
Sekce **Výběr komponent** nabízí přehled komponent **AVG Anti-Virus 2011**, které můžete nainstalovat. Pokud vám výchozí nastavení nevyhovuje, máte možnost jednotlivé komponenty odebrat/přidat.

Volíte pouze z těch komponent, které jsou zahrnuty ve vaší zakoupené licenci AVG. Pouze tyto komponenty vám také budou v dialogu nabídnuty!

Označte kteroukoliv komponentu v seznamu **Výběr komponent** a po pravé straně se zobrazí stručný popis funkčnosti této komponenty. Podrobné informace o každé jednotlivé komponentě najdete v kapitole [Přehled komponent](#). Chcete-li se vrátit k výchozí konfiguraci nastavené výrobcem, stiskněte tlačítko **Výchozí**.

Pokračujte stiskem tlačítka **Další**.

4.5. Instalovat AVG Security Toolbar



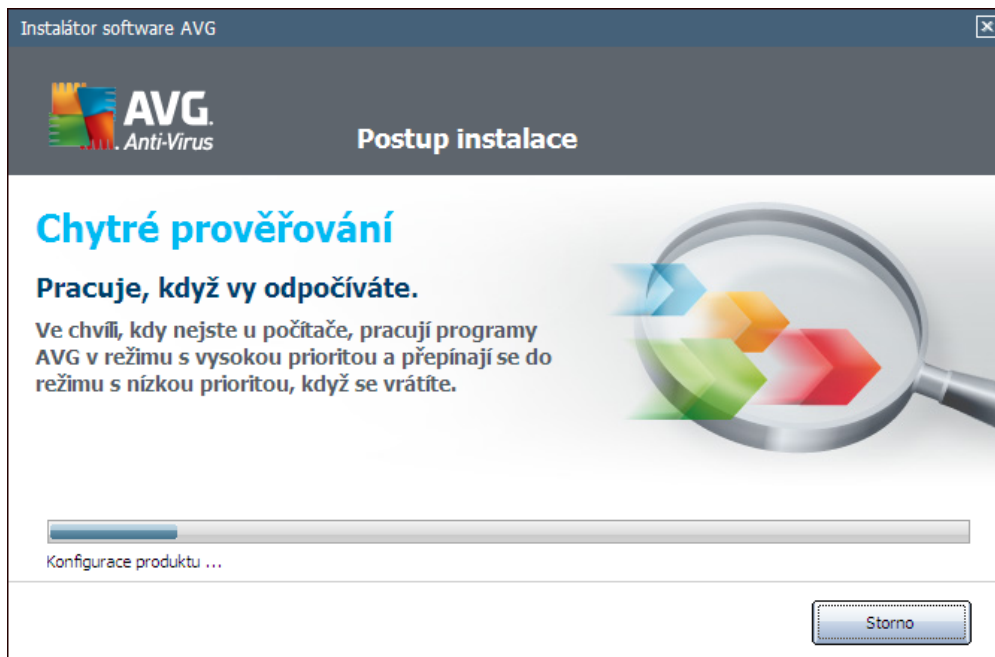
V dialogu **AVG Security Toolbar** rozhodnete, zda si v rámci **AVG Anti-Virus 2011** přejete nainstalovat i službu **AVG Security Toolbar**. Pokud nezměníte výchozí nastavení, bude tato komponenta automaticky nainstalována do vašeho internetového prohlížeče (*podporované prohlížeče jsou Microsoft Internet Explorer verze 6.0 nebo novější a Mozilla Firefox verze 3.0 nebo novější*) a zajistí kompletní on-line ochranu při prohlížení webu.

V tomto dialogu máte také možnost rozhodnout, zda si přejete nastavit Webhledani.cz jako výchozí službu vyhledávání. Pokud ano, ponechte označené příslušné políčko.



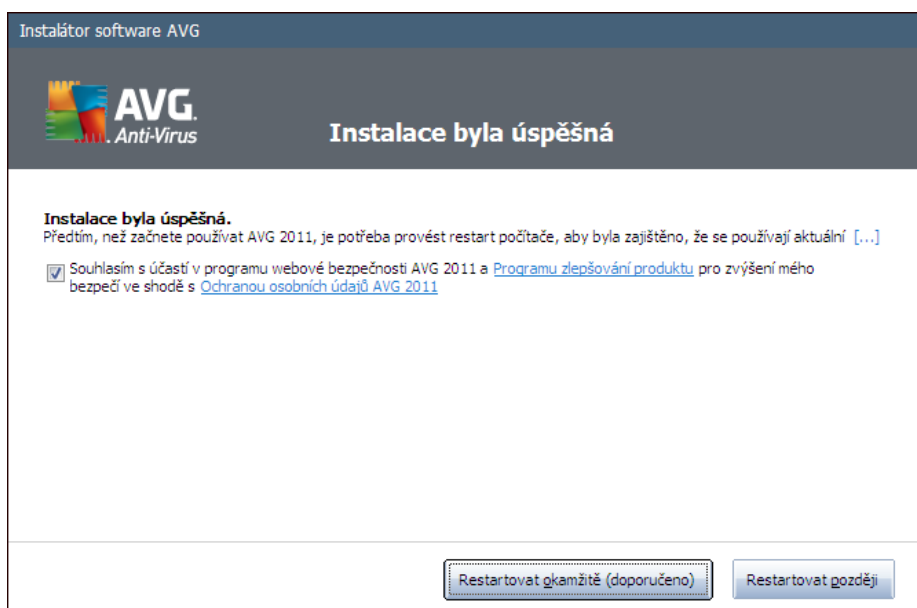
4.6. Postup instalace

Potvrzením předchozího dialogu dojde ke spuštění samotného procesu instalace, jehož průběh můžete sledovat v dialogu **Postup instalace**. Tento dialog je pouze informativní a nevyžaduje žádný váš zásah:



Po kejte prosím na dokončení instalace. Poté budete automaticky přeměnováni k následujícímu dialogu.

4.7. Instalace byla úspěšná



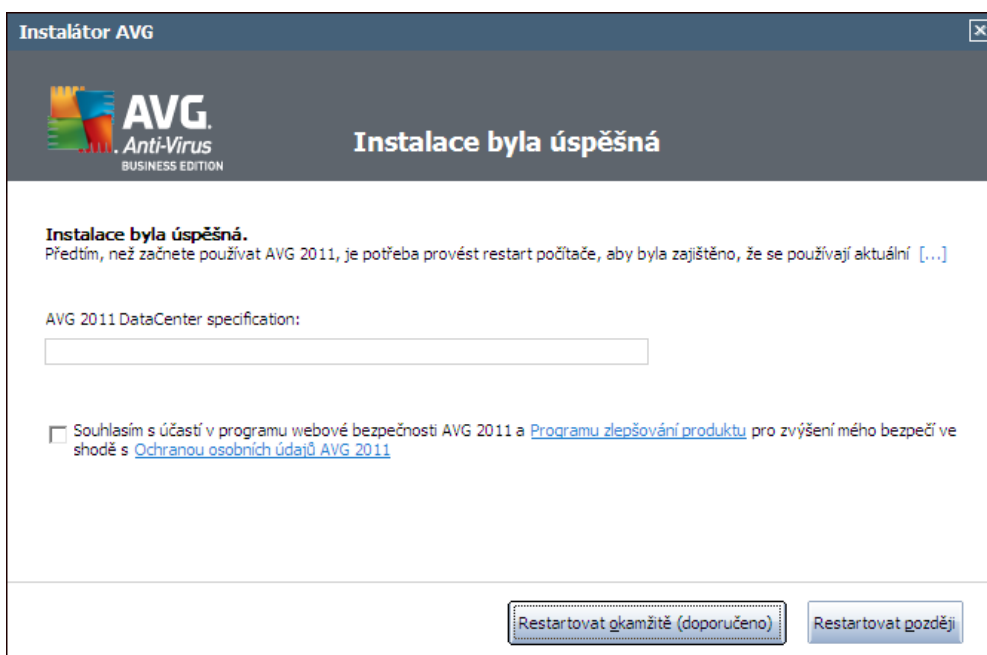


Dialog **Instalace byla úspěšná** potvrzuje, že **AVG Anti-Virus 2011** byl plně nainstalován a nastaven k optimálnímu výkonu.

V tomto dialogu uveďte prosím své kontaktní údaje, abyste mohli dostávat veškeré novinky a informace týkající se produktu. Pod registračním formulářem pak najdete následující dvě možnosti:

- **Ano, přeji si dostávat e-mailem novinky z oblasti bezpečnosti a speciální nabídky AVG 2011** - označením této volby potvrzujete, že si přejete být informováni o novinkách v oblasti internetové bezpečnosti a že chcete dostávat informace o speciálních nabídkách a novinkách v produktech AVG.
- **Souhlasím s účastí v programu webové bezpečnosti AVG 2011 a Programu zlepšování produktu ...** - označením této volby dáváte najevo svůj souhlas s účastí v Programu zlepšování produktu (podrobnosti najdete v kapitole [Pokročilé nastavení AVG / Program zlepšování produktu](#)). V rámci tohoto programu probíhá sběr anonymních informací o detekovaných hrozbách s cílem zvýšit celkovou úroveň bezpečnosti na Internetu.

Poznámka: Pokud instalujete AVG s licencí, které AVG Business Edice, a pokud jste v průběhu instalačního procesu potvrdili, že si přejete instalovat komponentu Vzdálené správy (viz [Uživatelské volby](#)), zobrazí se dialog **Instalace byla úspěšná** s následujícím rozhraním:



V tomto dialogu pak definujte parametry AVG DataCenter - zadejte připojovací adresu a port k AVG DataCenter ve tvaru server:port. Nemáte-li danou informaci momentálně k dispozici, ponechte pole zatím prázdné a později budete moci konfiguraci dokončit v dialogu [Pokročilé nastavení / Vzdálená správa](#). Pro podrobné informace o vzdálené správě AVG prosím konzultujte uživatelský manuál AVG Business Edice, který je k dispozici ke stažení na webu AVG website (<http://www.avg.cz/>).



5. Po instalaci

5.1. Registrace produktu

Po dokonění instalace **AVG Anti-Virus 2011** prosím zaregistrujte svůj produkt na webu AVG (<http://www.avg.cz/>), stránka **Registrace** (postupujte podle instrukcí uvedených na stránce). Registrace vám umožní získat přístup k uživatelskému účtu AVG, dostávat informace o aktualizacích AVG, a zprostředkuje další služby poskytované registrovaným uživateli AVG.

5.2. Otevření uživatelského rozhraní

[Uživatelské rozhraní AVG](#) je dostupné několika cestami:

- dvojklikem na [ikonu AVG na systémové liště](#)
- dvojklikem na ikonu AVG na ploše
- dvojklikem na stavový zádek umístěný ve spodní části [miniaplikace AVG](#) (Pokud jste tento [volitelný doplněk k instalaci](#). Miniaplikace AVG je podporována pouze u OS Windows Vista/Windows 7.)
- z nabídky **Start/Všechny programy/AVG 2011/Uživatelské rozhraní AVG**
- z **AVG Security Toolbaru** volbou **Spustit AVG**

5.3. Spuštění testu celého počítače

Jelikož existuje jisté riziko, že virus byl na váš počítač zavlečen již před instalací **AVG Anti-Virus 2011**, doporučujeme bezprostředně po instalaci spustit [Test celého počítače](#), který zkontroluje celý počítač a ověří přítomnost virů a potenciálně nežádoucích programů.

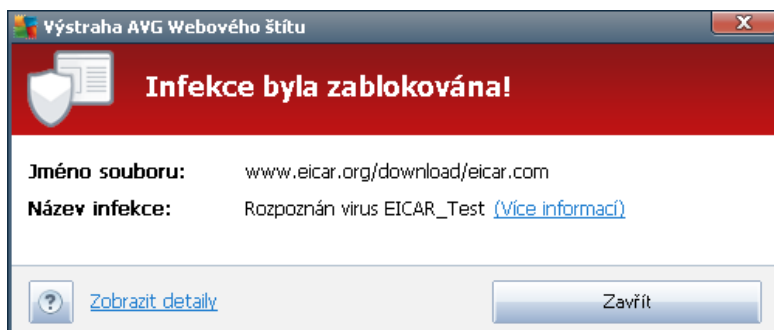
Instrukce ke spuštění testu najdete v kapitole [AVG testování](#).

5.4. Test virem Eicar

Chcete-li ověřit, že **AVG Anti-Virus 2011** byl správně nainstalován, proveďte test virem EICAR.

Test virem EICAR je standardní a naprosto bezpečnou metodou, jak zkontrolovat funkčnost antivirové ochrany AVG. 'Virus' EICAR není pravým virem a neobsahuje žádné části virového kódu. Váš produkt na něj reaguje, jako by virem byl (přestože jsou schopny jej rozpoznat a označit skutečným jménem; hlásí jeho přítomnost například takto "EICAR-AV-Test"). 'Virus' EICAR si můžete stáhnout z internetu na adrese <http://www.eicar.com>, kde také najdete všechny nezbytné informace o 'viru' samotném a testování tímto 'virem'.

Stáhněte si soubor **eicar.com** a pokuste se jej uložit na lokální disk. Ihned poté, co potvrdíte stažení testovacího souboru, zareaguje [Webový štít](#) varovným upozorněním. Toto upozornění dokazuje, že **AVG Anti-Virus 2011** na vašem počítači je správně nainstalován:



Z webu <http://www.eicar.com> můžete také stáhnout komprimovanou verzi testovacího 'viru' EICAR (například ve formátu `ecar_com.zip`). Při stahování tohoto souboru nedojde k detekci **Webovým štítem** a soubor budete moci uložit na disk, ale při jeho rozbalení jej detekuje **Rezidentní štít**. **Pokud není testovací soubor EICAR identifikován jako virus, je nutné znovu provést konfiguraci AVG Anti-Virus 2011!**

5.5. Výchozí konfigurace AVG

Ve výchozí konfiguraci (bezprostředně po instalaci AVG Anti-Virus 2011) jsou všechny komponenty a funkce **AVG Anti-Virus 2011** nastaveny výrobcem k optimálnímu výkonu bezpečnostního software.

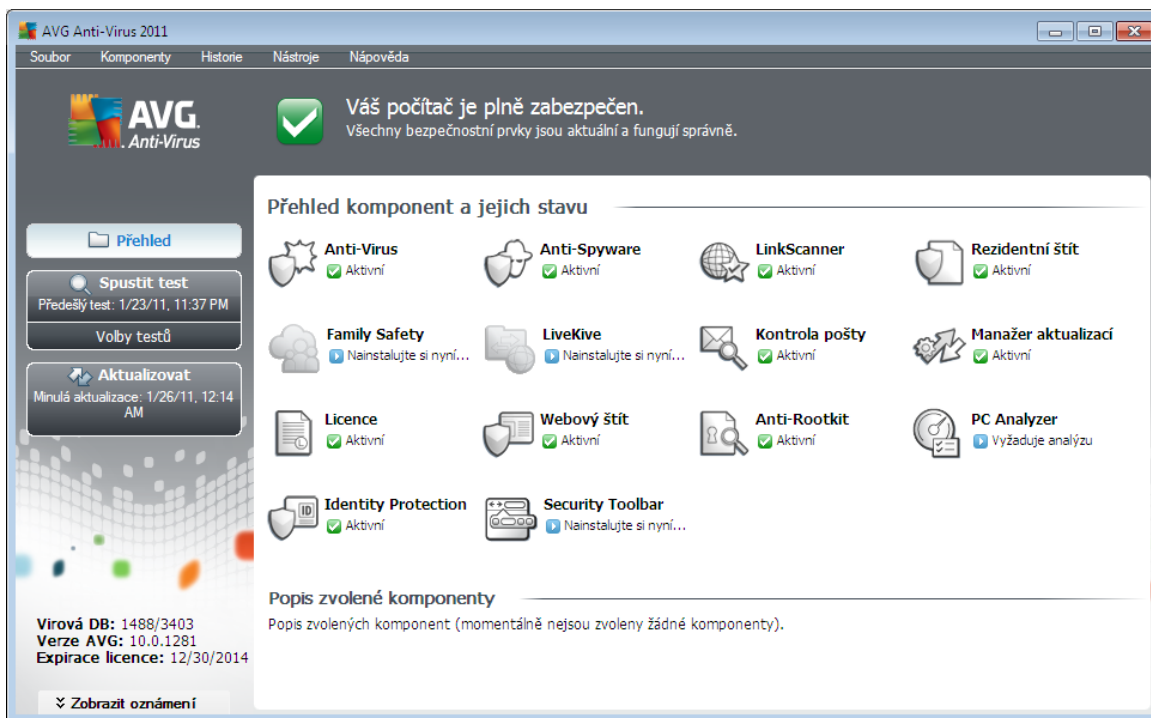
Pokud nemáte skutečný důvod jejich konfiguraci změnit, doporučujeme ponechat program v tomto nastavení! Změnu konfigurace by měl provádět pouze zkušený uživatel.

Jednoduché, spíše preferenční změny v nastavení **komponent AVG** jsou dostupné přímo z uživatelského rozhraní pro jednotlivé komponenty. Pokud se domníváte, že je nutné konfiguraci AVG přenastavit podle vašich aktuálních potřeb, proveďte editaci parametrů v **Pokročilém nastavení AVG**: zvolte ze systémového menu položku **Nástroje/Pokročilé nastavení** a editaci nastavení proveďte v nově otevřeném dialogu **Pokročilém nastavení AVG**.



6. Uživatelské rozhraní AVG

AVG Anti-Virus 2011 se otevře v tomto rozhraní:



Hlavní okno je rozděleno do několika sekcí:

- **Systémové menu** (navigace Windows zobrazená zcela nahoře) je standardní navigací, která umožňuje přístup ke všem komponentám, vlastnostem a službám AVG - [podrobnosti >>](#)
- **Informace o stavu zabezpečení** (v horní části okna) podává základní informaci o aktuálním stavu programu AVG - [podrobnosti >>](#)
- **Zkratková tlačítka** (v levé části okna) umožní rychlý přístup k nejdůležitějším a nejčastěji používaným funkcím AVG - [podrobnosti >>](#)
- **Přehled komponent** (ve střední části okna) nabízí přehled všech instalovaných komponent AVG - [podrobnosti >>](#)
- **Statistika** (vlevo dole) je stručným přehledem všech statistických dat vztahujících se k programu - [podrobnosti >>](#)
- **Ikona na systémové liště** (v pravém dolním rohu monitoru, na systémové liště) je indikátorem aktuálního stavu AVG - [podrobnosti >>](#)
- **Miniaplikace AVG** (panel Windows sidebar, podporováno pouze v OS Windows Vista/7) umožňuje rychlý přístup k testování a aktualizaci programu - [podrobnosti >>](#)



6.1. Systémové menu

Systémové menu je standardní navigací používanou ve všech oknech Windows. Je umístěno v rozhraní **AVG Anti-Virus 2011** vodorovně zcela nahoře. Prostednictvím tohoto menu můžete přistupovat k jednotlivým komponentám, vlastnostem a službám AVG.

Systémové menu je rozděleno do pěti sekcí, které se dále dělají:

6.1.1. Soubor

- **Konec** - zavírá uživatelské rozhraní **AVG Anti-Virus 2011**. Aplikace AVG však zůstává spuštěna, aby dále trvale na pozadí a váš počítač je stále chráněn!

6.1.2. Komponenty

Položka systémového menu **Komponenty** obsahuje odkazy k jednotlivým instalovaným komponentám AVG a otevírá uživatelské rozhraní vždy na jejich výchozí stránce:

- **Přehled komponent** - přepne uživatelské rozhraní na dialog **[Přehled komponent a jejich stavu](#)**
- **Anti-Virus** chrání váš počítač proti útočným virům - [podrobnosti >>](#)
- **Anti-Spyware** chrání váš počítač před spyware a adware - [podrobnosti >>](#)
- **Link Scanner** kontroluje odkazy zobrazené ve výsledcích vyhledávání ve vašem internetovém prohlížeči - [podrobnosti >](#)
- **Kontrola pošty** prověřuje všechnu přichodící i odchozí poštu na přítomnost virů - [podrobnosti >>](#)
- **Family Safety** pomáhá sledovat aktivity vašich dětí online a chránit je před nevhodným obsahem webových stránek - [podrobnosti >>](#)
- **LiveKive** automaticky zálohuje vaše data online - [podrobnosti >>](#)
- **Rezidentní štít** pracuje na pozadí a kontroluje soubory při jejich kopírování, otevírání a ukládání - [podrobnosti >>](#)
- **Manažer aktualizací** spravuje aktualizací procesy AVG - [podrobnosti >>](#)
- **Licence** zobrazuje licenční číslo, typ licence, datum expirace atd. - [podrobnosti >>](#)
- **Webový štít** kontroluje data stahovaná webovým prohlížečem - [podrobnosti >>](#)
- **Anti-Rootkit** detekuje programy a technologie, které dokáží maskovat přítomnost nebezpečného software - [podrobnosti >>](#)
- **PC Analyzer** analyzuje stav vašeho počítače a nabízí přehled zjištěných údajů - [podrobnosti >>](#)



- **Identity Protection** slouží k detekci malware a je zaměřena na prevenci zcizení osobních dat - [podrobnosti >>](#)
- **Security Toolbar** umožňuje využít funkcí AVG přímo z prostředí internetového prohlížeče - [podrobnosti >>](#)
- **Vzdálená správa** se zobrazuje pouze podmíněně v případě, že instalujete Business Edici produktu AVG a rozhodli jste se během [instalačního procesu](#) tuto komponentu doinstalovat

6.1.3. Historie

- **Výsledky test** - přepíná do testovacího rozhraní AVG, konkrétně do dialogu s přehledem výsledků testů.
- **Nálezy Rezidentního štítu** - otevírá dialog s přehledem infekcí detekovaných **Rezidentním štítem**
- **Nálezy Kontroly pošty** - otevírá dialog s přehledem příloh detekovaných jako nebezpečné komponentou **Kontrola pošty**
- **Nálezy Webového štítu** - otevírá dialog s přehledem infekcí detekovaných **Webovým štítem**
- **Virový trezor** - otevírá rozhraní karanténního prostoru (**Virového trezoru**), kam jsou přesouvány detekované infekční soubory, jež se nepodařilo automaticky vyléčit. V tomto prostoru jsou soubory zcela izolovány a tím je zajištěna naprostá bezpečnost vašeho počítače, a současně zde lze soubory uložit pro případnou další práci s nimi.
- **Protokol událostí** - otevírá rozhraní historie událostí s přehledem všech protokolovaných akcí **AVG Anti-Virus 2011**

6.1.4. Nástroje

- **Otestovat počítač** - přepíná do [testovacího rozhraní AVG](#) a přímo spouští **Test celého počítače**.
- **Otestovat zvolený adresář** - přepíná do [testovacího rozhraní AVG](#) a nabízí ve stromové struktuře vašeho disku možnost definovat ty složky, které mají být otestovány.
- **Otestovat soubor** - umožňuje spustit test na vyžádání nad samostatným souborem, který vyberete ve stromové struktuře na vašem disku.
- **Aktualizovat** - automaticky spouští proces aktualizace **AVG Anti-Virus 2011**.
- **Aktualizace z adresáře** - spustí proces aktualizace z aktualizací souboru umístěného v definovaném adresáři na lokálním disku. Tuto alternativu doporučujeme pouze jako náhradní řešení pro případ, že v danou chvíli nebude k dispozici připojení k Internetu (*např. počítač je zavirovaný a odpojený ze sítě, počítač je připojen k síti, kde není přístup k Internetu, apod.*). V nově otevřeném okně vyberte adresář, do nějž jste předešle umístili aktualizací soubory, a spusťte aktualizaci.
- **Pokročilé nastavení** - otevírá dialog **Pokročilého nastavení AVG**, kde máte možnost



editovat konfiguraci **AVG Anti-Virus 2011**. Obecnou doporučenou úroveň nastavíme na výchozí výrobcem definované nastavení aplikace.

6.1.5. Nápověda

- **Obsah** - otevírá nápovědu k programu AVG
- **Odborná pomoc online** - otevírá web AVG (<http://www.avg.cz/>) na stránce centra zákaznické podpory
- **AVG na webu** - otevírá web AVG (<http://www.avg.cz/>)
- **Informace o virech** - otevírá **Virovou encyklopedii** na webu AVG (<http://www.avg.cz/>), v níž lze dohledat podrobné informace o detekovaných nálezech
- **Reaktivovat** - otevírá dialog **Aktivace AVG**, v němž jsou již předem vyplněna data, jež jste zadali v dialogu **Registrace AVG** během **instalace programu**. V dialogu **Aktivace AVG** můžete zadat své licenční číslo, kterým budete nahradit prodejní číslo, s nímž jste AVG instalovali, nebo kterým změníte dosavadní licenční číslo za jiné, například pro jiný produkt značky AVG.
- **Registrovat** - otevírá web AVG (<http://www.avg.cz/>) na stránce **Registrace**. Vyplňte prosím své registrační údaje; pouze registrovaní zákazníci mají plný přístup k technické podpoře AVG.

Poznámka: Máte-li nainstalovanou zkušební verzi **AVG Anti-Virus 2011**, dvě poslední uvedené položky se zobrazí jako **Zakoupit** a **Aktivovat** a odkáží Vás na web AVG, kde si můžete přímou zakoupenou plnou verzi programu. Pokud máte nainstalovaný program **AVG Anti-Virus 2011** s prodejním číslem, položky se zobrazí jako **Zaregistrovat** a **Aktivovat**. Podrobnější informace o možnostech aktivace a registrace najdete v kapitole [Licence](#).

- **O AVG** - otevírá dialogové okno **Informace**, v němž na pěti záložkách najdete informace o názvu programu, verzi programu a virové databáze, parametrech systému, licenční ujednání a kontaktní informace společnosti **AVG Technologies CZ**.

6.2. Informace o stavu zabezpečení

Sekce **Informace o stavu zabezpečení** je umístěna v horní části rozhraní AVG. V této sekci najdete vždy informaci o aktuálním stavu vašeho **AVG Anti-Virus 2011**. V sekci může být zobrazena jedna z následujících ikon, jejichž význam vysvětlujeme:



- Zelená ikona informuje, že program AVG na vašem počítači je plně funkční, aktualizován a všechny instalované komponenty pracují správně. Jste zcela chráněni.



- Oranžová ikona informuje o stavu, kdy jedna (nebo více) komponent není správně nastavena. Nejedná se o kritický problém, pravděpodobně jste se sami rozhodli některou komponentu deaktivovat. V každém případě jste stále chráněni. Prosíme vás, abyste pozornost věnovali konfiguraci komponenty, která není nastavena k plné aktivitě! Jméno této

komponenty bude v sekci **Informace o stavu zabezpečení** uvedeno.

Tato ikona se zobrazí rovněž v případě, kdy jste se z nějakého důvodu v domě rozhodli [ignorovat chybový stav komponenty](#) (volba "Ignorovat stav komponenty" je dostupná z kontextového menu otevřeného pravým tlačítkem myši nad ikonou komponenty v přehledu komponent v hlavním okně AVG). Může nastat situace, kdy budete potřebovat využít této možnosti, ale rozhodně nedoporučujeme, abyste v tomto stavu setrvali déle, než je nutné.



- červená ikona informuje o kritickém stavu AVG! Na která z komponent je nefunkční a AVG nemůže plně chránit váš počítač. Vnujte prosím okamžitou pozornost opravě tohoto problému. Pokud nebudete sami schopni problém odstranit, kontaktujte oddělení [technické podpory AVG](#).

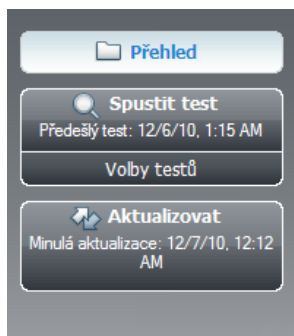
V případě, kdy AVG není nastaven k plnému a optimálnímu výkonu se vedle informace o stavu zabezpečení zobrazí tlačítko **Opravit** (případně **Opravit vše, pokud se problém týká více než jediné komponenty**), jehož stiskem AVG automaticky spustí proces kontroly a přenastavení všech parametrů k optimálnímu výkonu. Tímto tlačítkem snadno uvedete program do optimálního stavu a zajistíte tak nejvyšší úroveň bezpečnosti!

Doporučujeme, abyste v nově zobrazených údajích v sekci **Informace o stavu zabezpečení** a pokud AVG hlásí jakýkoliv problém, zaměřte se na jeho řešení. Pokud ignorujete chybová hlášení AVG, váš počítač je ohrožen!

Poznámka: Informaci o stavu AVG lze v kterémkoliv okamžiku práce na počítači získat také pohledem na [ikonu na systémové liště](#).

6.3. Zkratková tlačítka

Zkratková tlačítka (v levé části [uživatelského rozhraní AVG](#)) umožní rychlý přístup k nejdůležitějším a nejčastěji používaným funkcím AVG:



- **Přehled** - tlačítkem se z libovolného aktuálně otevřeného rozhraní AVG vrátíte do úvodní obrazovky s přehledem instalovaných komponent programu - viz kapitola [Přehled komponent >>](#)
- **Spustit test** - ve výchozím nastavení tlačítko uvádí informaci (typ testu a datum spuštění) o testu, který byl spuštěn naposledy. Můžete buďto kliknout na příkaz **Spustit test**, čímž dojde ke spuštění téhož testu, nebo na příkaz **Volba test**, čímž otevřete testovací rozhraní



AVG, kde je možné přímo spouštět testy vašeho počítače, plánovat jejich spuštění a editovat parametry testů - viz kapitola [AVG Testování >>](#)

- **Aktualizovat** - tlačítko uvádí datum posledního spuštění procesu aktualizace. Stiskem tlačítka otevřete nové rozhraní a aktualizaci přímo spustíte - viz kapitola [Aktualizace AVG >>](#)

Tato tlačítka jsou dostupná z uživatelského rozhraní v kterémkoli okamžiku práce s AVG. Spustíte-li jejich použitím libovolný proces, přepnete se do nového dialogu, ale tlačítka jsou stále k dispozici. Probíhající proces je navíc v navigační grafice znázorněn.

6.4. Přehled komponent

Sekce **Přehled komponent** je umístěna ve střední části [uživatelského rozhraní AVG](#). Tato sekce je rozdělena do dvou částí:

- Přehled všech instalovaných komponent je tvořen panelem s ikonou konkrétní komponenty a informací o tom, zda je ta která komponenta aktuálně aktivní či neaktivní
- Popisem funkcí zvolené komponenty

V rámci **AVG Anti-Virus 2011** najdete v sekci **Přehled komponent** informace o těchto komponentách:

- **Anti-Virus** chrání váš počítač proti útočným virům - [podrobnosti >>](#)
- **Anti-Spyware** chrání váš počítač před spyware a adware - [podrobnosti >>](#)
- **Link Scanner** kontroluje odkazy zobrazené ve výsledcích vyhledávání ve vašem internetovém prohlížeči - [podrobnosti >](#)
- **Kontrola pošty** prověřuje všechnu příchozí i odchozí poštu na přítomnost virů - [podrobnosti >>](#)
- **Rezidentní štít** kontroluje soubory při jejich kopírování, otevírání a ukládání - [podrobnosti >>](#)
- **Family Safety** pomáhá sledovat aktivity vašich dětí online a chránit je před nevhodným obsahem webových stránek - [podrobnosti >>](#)
- **LiveKive** automaticky zálohuje vaše data online - [podrobnosti >>](#)
- **Manažer aktualizací** spravuje aktualizací procesy AVG - [podrobnosti >>](#)
- **Licence** zobrazuje licenční číslo, typ licence, datum expirace atd. - [podrobnosti >>](#)
- **Webový štít** kontroluje data stahovaná webovým prohlížečem - [podrobnosti >>](#)
- **Anti-Rootkit** detekuje programy a technologie, které dokážou maskovat přítomnost nebezpečného software - [podrobnosti >>](#)
- **PC Analyzer** analyzuje stav vašeho počítače a nabízí přehled zjištěných údajů -



[podrobnosti >>](#)

- **Identity Protection** - slouží k detekci malware a je zaměřena na prevenci zcizení osobních dat - [podrobnosti >>](#)
- **Security Toolbar** umožňuje využití funkcí AVG přímo z prostředí internetového prohlížeče - [podrobnosti >>](#)
- **Vzdálená správa** se zobrazuje pouze podmíněně v případě, že instalujete Business Edici produktu AVG a rozhodli jste se během [instalačního procesu](#) tuto komponentu doinstalovat

Jednoduchým kliknutím na libovolnou ikonu komponenty tuto komponentu v případě vysvítíte a současně se ve spodní části uživatelského rozhraní zobrazí stručný popis funkce této komponenty. Dvojklikem na zvolenou ikonu otevřete vlastní rozhraní komponenty s pohledem základních statistických dat.

Kliknutím pravého tlačítka myši nad ikonou komponenty pak otevřete kontextové menu, které kromě možnosti otevřít grafické rozhraní komponenty nabízí ještě možnost **Ignorovat stav komponenty**. Touto volbou dáváte najevo, že jste si v domění, že se ta která [komponenta nachází v chybovém stavu](#), ale z nějakého důvodu si přejete tento stav zachovat a nebyť na něj upozorování [ikonou na systémové liště](#).

6.5. Statistika



Sekce **Statistika** je umístěna v levém spodním rohu [uživatelského rozhraní AVG](#). Statistika podává pohled o běhu programu AVG:

- **Virová DB** - informace o verzi aktuálně instalované virové databáze
- **Verze AVG** - informace o instalované verzi AVG (číslo ve tvaru 10.0.xxxx, kde 10.0 zastupuje produktovou řadu AVG a xxxx označuje číslo sestavení)
- **Expirace licence** - datum, kdy dojde k expiraci vaší licence AVG

6.6. Ikona na systémové liště

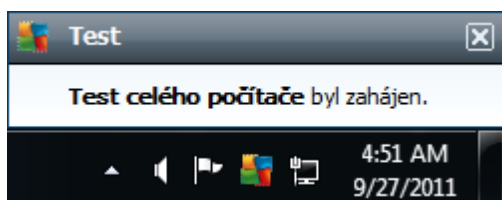
Ikona na systémové liště (vpravo dole na monitoru, na panelu Windows) ukazuje aktuální stav **AVG Anti-Virus 2011**. Ikona je viditelná v každém okamžiku vaší práce na počítači, bez ohledu na to, zda máte otevřeno uživatelské rozhraní AVG:



Jestliže je ikona zobrazena barevně , jsou všechny komponenty AVG aktivní a plně funkční. Další alternativou tohoto zobrazení je situace, kdy některá z komponent není v plně funkčním stavu, ale uživatel je si tohoto faktu v domění a v domění se rozhodl [Ignorovat stav komponenty](#). Pokud je ikona zobrazena s výkřikem , znamená to, že některá komponenta (*či více komponent*) je v chybovém stavu. Pro okamžitý přístup k editaci nastavení komponenty v chybovém stavu otevřete AVG dvojklikem na ikonu.



Systemová ikona dále poskytuje informace o aktuálním d n í v programu AVG. P í zm n stavu AVG (*automatické spušt ní naplánované aktualizace nebo testu, zm na stavu n které komponenty, p echod programu do chybového stavu, ...*) budete okamžit informováni pop-up oknem vysunutým nad ikonou na systémové lišt :

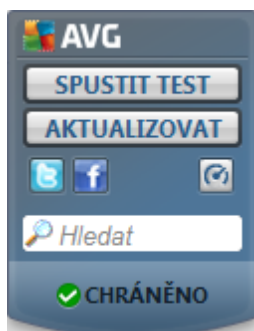


Ikonu na systémové lišt ě lze také použít pro rychlý p ístup k uživatelskému rozhraní AVG, to se otev e dvojklikem na ikonu. Kliknutí pravým tla ítkem myši nad ikonou otevírá kontextové menu s t ěmi možnostmi:



- **Otev ít uživatelské rozhraní AVG** - otev e [uživatelské rozhraní AVG](#)
- **Testy** - otev e vysunovací nabídku [p ednastavených test ě](#) ([Test celého počíta e](#), [Test vybraných soubor ů i složek](#), [Anti-Rootkit test](#)) a následnou volbou požadovaný test p ímo spustíte
- **Spustit PC Analyzer** - spustí funkci komponenty [PC Analyzer](#)
- **B žící testy** - tato položka se zobrazuje pouze tehdy, je-li aktuáln spušt n n který test. U tohoto b žícího testu pak m žete nastavit jeho prioritu, p ípadn test pozastavit nebo ukon ět. K dispozici jsou dále možnosti *Nastavit prioritu pro všechny testy*, *Pozastavit všechny testy* a *Zastavit všechny testy*.
- **Aktualizovat** - spustí okamžitou [aktualizaci](#)
- **Nápov da** - otev e soubor nápov dy na úvodní stránce

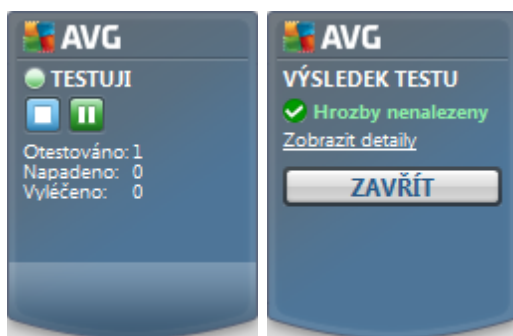
6.7. Miniaplikace AVG

Miniaplikace AVG se zobrazuje na ploše Windows (*v sekci Windows Sidebar*). Tato funkce je podporována pouze v opera ních systémech Windows Vista a Windows 7. **Miniaplikace AVG** vám umožní okamžitou dostupnost nejd ěležit ějších funkcí **AVG Anti-Virus 2011**, a to [testování](#) a [aktualizace](#):

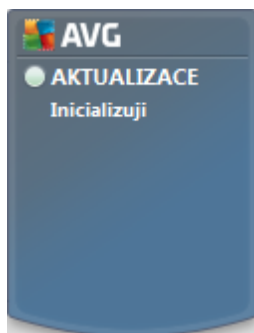



Miniaplikace AVG nabízí tyto možnosti snadného přístupu:

- **Spustit test** - kliknutím na volbu **Spustit test** spustíte přímo z prostředí miniaplikace **test celého počítače**. Jeho průběh můžete sledovat v pozmiňném rozhraní miniaplikace v jednoduchém statistickém přehledu, kde najdete informace o počtu otestovaných objektů, detekovaných hrozbách a vyléčených hrozbách. V průběhu testu můžete proces testování kdykoliv pozastavit  nebo ukončit . Podrobné informace o výsledku testu pak najdete standardně v dialogu **Přehled výsledků testu**, který lze z miniaplikace otevřít kliknutím na volbu **Zobrazit detaily** (test bude označen jako **Test z miniaplikace**).






- **Aktualizovat** - kliknutím na volbu **Aktualizovat** spustíte proces aktualizace AVG přímo z prostředí miniaplikace:



- **Twitter**  - otevírá další rozhraní **Miniaplikace AVG** s přehledem nejnovějších záznamů o AVG uveřejněných na sociální síti Twitter. Stiskem odkazu **Zobrazit všechny kanály AVG Twitter** otevřete nové okno vašeho internetového prohlížeče a budete příměrováni přímo na web Twitter, konkrétně na stránku s přehledem novinek týkajících se AVG:



- **Facebook**  - otevírá internetový prohlížeč na webu sociální sítě Facebook, konkrétně na stránce **AVG komunity**
- **LinkedIn**  - tato funkce je dostupná pouze v síťové instalaci (*instalaci s licenčním číslem* které z *AVG Business Edicí*) a otevírá internetový prohlížeč na stránce **AVG SMB Community** v rámci sociální sítě LinkedIn
- **PC Analyzer**  - otevírá uživatelské rozhraní komponenty [PC Analyzer](#)
- **Vyhledávání** - zadejte klíčové slovo a výsledky vyhledávání se zobrazí v nově otevřeném okně s prohlížečem, který obvykle používáte



7. Komponenty AVG

7.1. Anti-Virus

7.1.1. Princip Anti-Viru

Testovací jádro antivirového programu skenuje všechny soubory a jejich aktivitu (otevírání/zavírání souboru atd.) a prověřuje přítomnost známých virů. Pokud detekuje virus, okamžitě zabrání, aby mohl být aktivován a následně jej odstraní nebo přesune do virové karantény. Většina antivirových programů používá metodu heuristické analýzy, při níž jsou soubory testovány na přítomnost typických virových charakteristik. To znamená, že antivirový skener dokáže rozpoznat i nový, dosud neznámý virus podle toho, že tento virus nese určité znaky typické pro již existující viry.

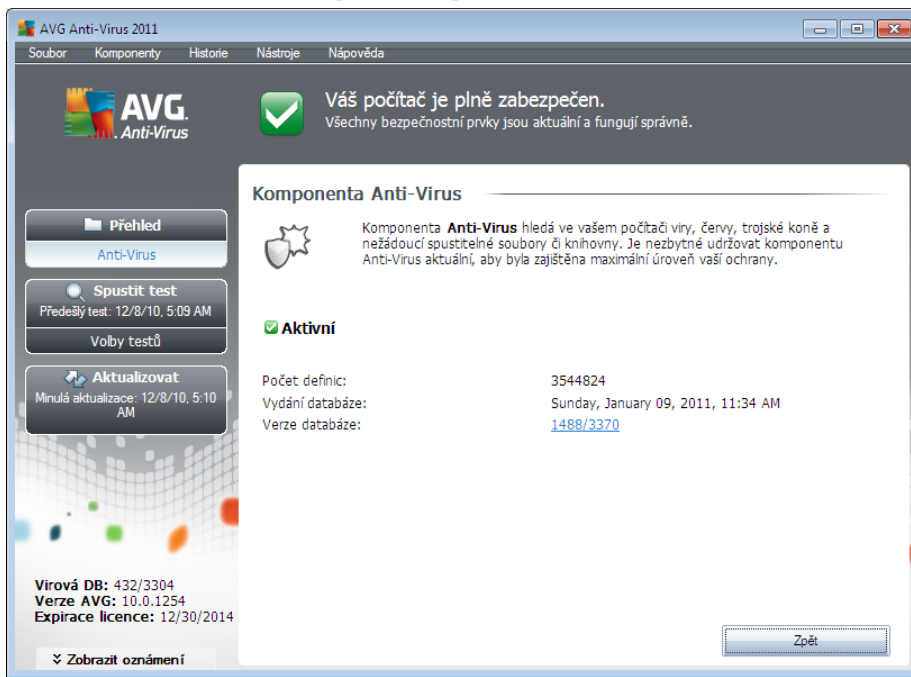
Dobrá antivirová ochrana zaručí, že na počítači nebude spuštěn žádný známý virus!

Komponenta **Anti-Virus** používá k detekci počítačových virů následující techniky:

- skenování - vyhledávání specifických znaků charakteristických pro daný virus
- heuristická analýza - dynamická emulace instrukcí testovaného objektu v prostředí virtuálního počítače
- generická detekce - statická detekce instrukcí charakteristických pro daný virus/skupinu virů

V případech, kdy použití jediné techniky nepostačí, umožňuje AVG kombinaci uvedených technik v rámci jednoho testu. Příkladem může být situace, kdy je virus zachycený skenováním přesně identifikován pomocí heuristické analýzy. AVG umí také analyzovat spustitelné programy, například DLL knihovny a určité, které z nich by mohly být potenciálně nežádoucí (jako například spyware, adware aj.). Na žádost uživatele umožní tyto programy odstranit i k nim zablokovat přístup.

7.1.2. Rozhraní komponenty Anti-Virus



Rozhraní komponenty **Anti-Virus** nabízí kromě základních informací o funkcích této komponenty také stručný statistický přehled:

- **Počet definic** - číslo udává počet virů definovaných v aktuální verzi virové databáze
- **Vydání databáze** - datum uvádí, kdy a v kolik hodin byla vydána poslední dostupná aktualizace virové databáze
- **Verze databáze** - číslo určuje aktuálně instalovanou verzi virové databáze a zvyšuje se při každé její aktualizaci

V tomto rozhraní je k dispozici jediné ovládací tlačítko (**Zpět**), kterým se vrátíte do výchozího [uživatelského rozhraní AVG](#) (přehled komponent).

7.2. Anti-Spyware

7.2.1. Princip Anti-Spyware

Spyware se obvykle definuje jako jeden z typů malware, to je software, který z vašeho počítače sbírá informace bez vašeho vědomí. Některé aplikace typu spyware mohou být nainstalovány na váš počítač záměrně; ostatním příkladem jsou třeba reklamní upoutávky, pop-up okna nebo jiné typy obtížného software.

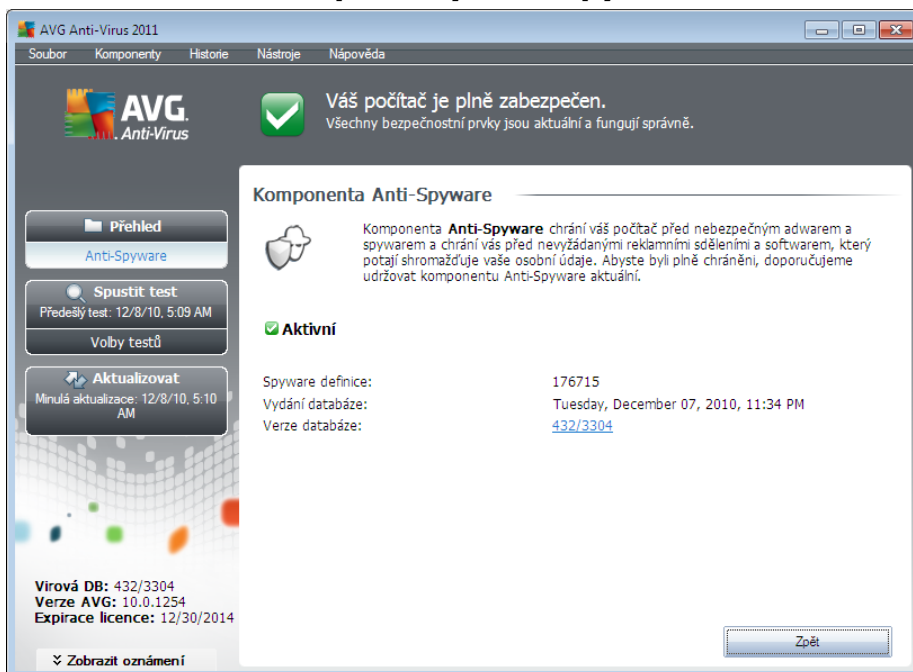
V ideálním případě byste se měli pokusit zabránit jakémukoli druhu spyware a/nebo malware v samotném průběhu na váš počítač. Nejčastějším zdrojem nákazy jsou v současné době webové



stránky s potenciálně nebezpečným obsahem. Rozšířen je i přes pomocí e-mailu nebo prostřednictvím serverů a virů. Nejdůležitějším prvkem ochrany je tedy trvale zapnutý scanner, který na pozadí, jakým je například **Anti-Spyware AVG**: pracuje nepřetržitě a na pozadí provádí veškeré aplikace, které spouštíte.

Existuje také potenciální riziko, že malware byl zavlečen na váš počítač ještě před instalací **AVG Anti-Virus 2011** nebo že jste opomněli provést [databázovou i programovou aktualizaci AVG](#). V takovém případě nabízí AVG možnost kompletní kontroly vašeho počítače na přítomnost malware/spyware za použití svých testovacích nástrojů. AVG také detekuje spící a neškodný malware, tedy malware, který již byl stažen a uložen, ale dosud neprobíhala jeho aktivace.

7.2.2. Rozhraní komponenty Anti-Spyware



Rozhraní komponenty **Anti-Spyware** uvádí stručný popis základních funkcí této komponenty, informaci o aktuálním stavu komponenty a dále statistický přehled:

- **Spyware definice** - číslo udává počet vzorků spyware definovaných v aktuální verzi spyware databáze
- **Vydání databáze** - datum udává, kdy a v kolik hodin byla vydána poslední dostupná aktualizace virové databáze
- **Verze databáze** - číslo určuje nejnovější verzi spyware databáze a zvyšuje se při každé její aktualizaci

V tomto rozhraní je k dispozici jediné ovládací tlačítko (**Zpět**), kterým se vrátíte do výchozího [uživatelského rozhraní AVG](#) (přehled komponent).



7.3. LinkScanner

7.3.1. Princip Link Scanneru

LinkScanner zajišťuje ochranu před stále rostoucím počtem nebezpečných internetových hrozeb. Tyto hrozby mohou být skryty na jakékoliv webové stránce - od stránek vládních organizací až po stránky malých firem. Pouze zřídka se vyskytují déle než 24 hodin. Jedinou náhodou technologie **LinkScanner** prohledává obsah internetových stránek a zajišťuje, že jsou stránky bezpečné v okamžiku, kdy je to nejdůležitější - když se chystáte otevřít adresu URL.

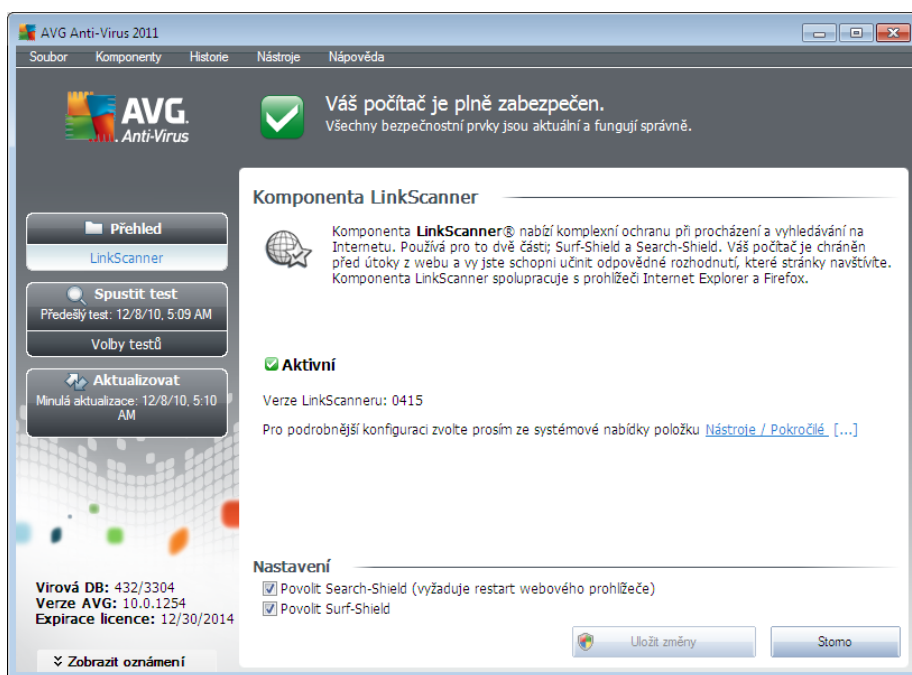
Technologie **LinkScanner** se skládá ze dvou funkcí: [Search-Shield](#) a [Surf-Shield](#):

- **Search-Shield** obsahuje seznam stránek (*URL adres*), které jsou známy jako infikované. Při hledání skrze vyhledávače Google, Yahoo! JP, WebHledání, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, a SlashDot jsou všechny výsledky zkontrolovány na základě tohoto seznamu a ke každé položce je zobrazena verdiktová ikona (*pro výsledky ve vyhledávači Yahoo! JP jsou zobrazeny tyto verdiktové ikony pouze pro infikované stránky*).
- Funkce **Surf-Shield** zabráňuje infikování počítače při nechtěném stahování nebezpečných souborů a skriptů a zároveň zajišťuje, že stránky, které navštívíte, nabízejí ve chvíli jejich otevření bezpečný obsah. Funkce testuje obsah internetových stránek, které navštívíte, bez ohledu na internetovou adresu stránky. Pokud tedy nebyla určitá stránka detekována funkcí **Search-Shield**, může být detekována a blokována právě funkcí **Surf-Shield** při přístupu na ni.

Poznámka: *LinkScanner není určen k ochraně serverů!*

7.3.2. Rozhraní Link Scanneru

Rozhraní komponenty **LinkScanner** uvádí stručný popis funkcí této komponenty a zprávu o jejím aktuálním stavu. Dále je uvedena informace o čísle verze komponenty (*Verze LinkScanneru*).



Nastavení

Ve spodní části dialogu v sekci **Nastavení** můžete editovat několik funkcí:

- **Povolit [Search-Shield](#)** - (ve výchozím nastavení zapnuto): služba je aktivní při vyhledávání na serverech Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg a SlashDot: veškeré výsledky vyhledávání jsou kategorizovány a označeny ikonou, která informuje o tom, zda je obsah odkazované stránky bezpečný či nebezpečný.
- **Povolit [Surf-Shield](#)** - (ve výchozím nastavení zapnuto): aktivní ochrana (ochrana v reálném čase) proti agresivním webovým stránkám. Kontrola stránek se provádí v okamžiku jejich načítání. Stránky s nebezpečným obsahem jsou v příslušném internetovém prohlížeči (nebo jiné aplikaci, která používá HTTP) rovnou zablokovány.


7.3.3. Search-Shield


Při prohlížení Internetu se zapnutou kontrolou **AVG Search-Shield** budou všechny výsledky vyhledávání pomocí nejrozšířenějších vyhledávačů (*Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg a SlashDot*) vyhodnoceny z hlediska bezpečnosti a rozděleny na odkazy bezpečné a nebezpečné. Označením jednotlivých odkazů grafickými ikonami vás **AVG Link Scanner** varuje před vstupem na nebezpečnou nebo podezřelou stránku.




Během vyhodnocování jednotlivých odkazů vrácených jako výsledky vyhledávání uvidíte u každého odkazu grafický symbol označující probíhající ověření odkazu. Jakmile je kontrola dokončena, u jednotlivých odkazů budou zobrazeny následující informace:

 Odkazovaná stránka je bezpečná (u výsledků dodaných z vyhledávání Yahoo! JP se tato ikona zobrazovat nebude!).

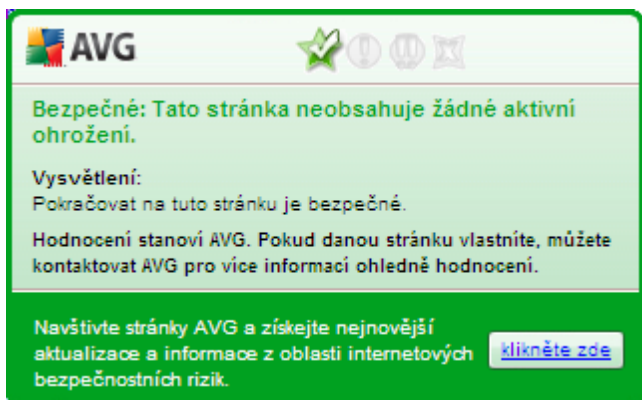
 Odkazovaná stránka neobsahuje žádné konkrétní hrozby, ale jeví se jako podezřelá (je sporný její pověst, protože ji nelze doporučit například pro aktivity typu on-line nakupování a podobně).

 Odkazovaná stránka může být sama o sobě bezpečná, ale obsahuje odkazy na jiné nebezpečné stránky. Nebo jde o stránku s podezřelým kódem.

 Odkazovaná stránka obsahuje aktivní hrozby! Pro vlastní bezpečnost vám nebude umožněno na tuto stránku vstoupit.

 Odkazovaná stránka je nepřístupná a nemohla tedy být prověřena.

Při přejetí myší nad jednotlivými ikonami s hodnocením bezpečnosti odkazu se pak zobrazí detailní informace (podrobnosti o hrozbě, pokud byla nalezena) o odkazu:



The screenshot shows a green-bordered notification box from AVG. At the top left is the AVG logo. To its right are four icons: a green star, a yellow warning icon, a yellow warning icon with an exclamation mark, and a red X icon. Below the icons, the text reads: "Bezpečné: Tato stránka neobsahuje žádné aktivní ohrožení." followed by "Vysvětlení: Pokračovat na tuto stránku je bezpečné." and "Hodnocení stanoví AVG. Pokud danou stránku vlastníte, můžete kontaktovat AVG pro více informací ohledně hodnocení." At the bottom, there is a link: "Navštivte stránky AVG a získajte najnovější aktualizace a informace z oblasti internetových bezpečnostních rizik." with a button labeled "klikněte zde".

7.3.4. Surf-Shield

Ochrana pomocí **Surf-Shield** dokáže zablokovat škodlivý obsah stránky, kterou se pokoušíte otevřít, a zabránit jeho stažení na váš počítač. Kliknete-li na odkaz, který vede na nebezpečnou stránku, nebo napíšete do adresového řádku URL nebezpečné stránky, **Surf-Shield** přístup k této stránce okamžitě zablokuje. Mějte na paměti, že váš počítač se může velmi snadno poškodit při pouhých návštěvách infikované webové stránky.

Narazíte-li na nebezpečnou webovou stránku, [AVG Link Scanner](#) vás bude varovat tímto oznámením:



Vstup na takto označenou stránku rozhodně nedoporučujeme!

7.4. Rezidentní štít

7.4.1. Princip Rezidentního štítu

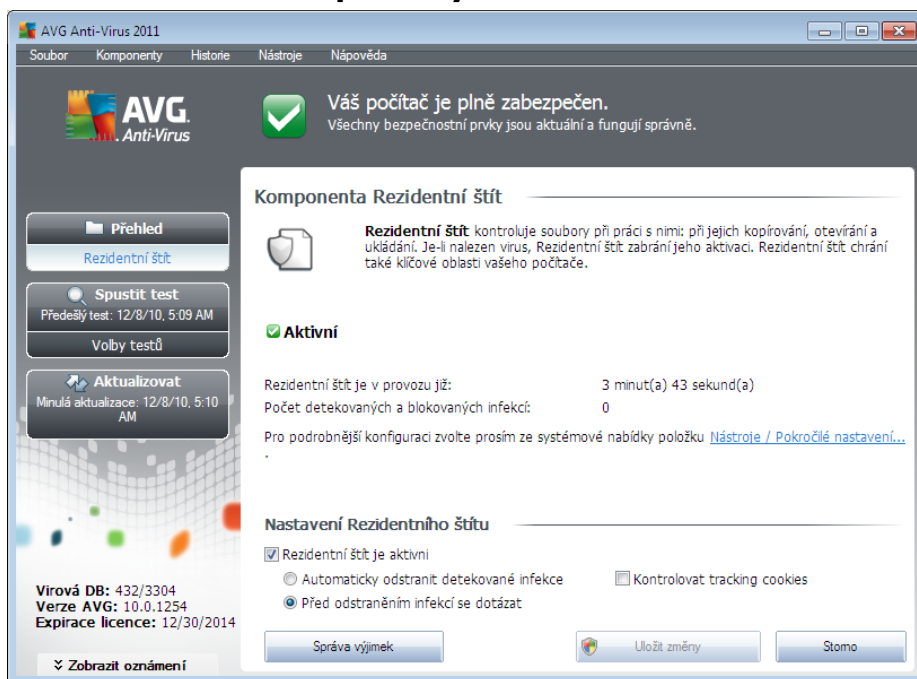
Komponenta **Rezidentní štít** poskytuje vašemu počítači nepřetržitou ochranu. Testuje všechny soubory, které otvíráte, kopírujete, ukládáte, a kontroluje také systémové oblasti počítače. V případě pozitivního nálezu v právě používaném souboru zastaví prováděnou operaci a zabrání aktivaci viru. Jelikož komponenta pracuje "na pozadí", obvykle tyto procesy ani nezaznamenáte a upozornění se vám zobrazí pouze v případě, že **Rezidentní štít** najde nějaký škodlivý kód (kterému zároveň zabrání v aktivaci).

Rezidentní štít

- testuje soubory na přítomnost různých druhů nebezpečného kódu
- testuje vyměnitelná média (*flash disky apod.*)
- testuje soubory s určitými příponami nebo i bez přípon
- povoluje výjimky, tj. soubory a adresáře, které se netestují

Upozornění: Rezidentní štít se na počítači automaticky, ihned po spuštění, a je nanejvýš důležité, aby byl zapnutý nepřetržitě!

7.4.2. Rozhraní komponenty Rezidentní štít



Rozhraní **Rezidentního štítu** nabízí kromě popisu funkce komponenty a informace o jejím aktuálním stavu také pohled na nejzákladnější statistických dat a základní možnosti nastavení. Dostupná statistika uvádí:

- **Rezidentní štít je v provozu již** - udává celkovou dobu od posledního spuštění **Rezidentního štítu**
- **Počet detekovaných a blokovanych infekcí** - uvádí počet objektů detekovaných Rezidentním štítem jako infikované (v případě potřeby, například pro statistické účely, lze tuto hodnotu vynulovat - Vynulovat hodnotu)

Nastavení Rezidentního štítu

Ve spodní části dialogového okna najdeme sekci nazvanou **Nastavení Rezidentního štítu**, v níž lze editovat některá základní nastavení funkcí komponenty (*detailní nastavení, stejně jako u ostatních komponent, je dostupné v položce Nástroje/Pokročilé nastavení*).

Volba **Rezidentní štít je aktivní** umožňuje jednoduché zapnutí / vypnutí funkce rezidentní ochrany. Ve výchozím nastavení je tato funkce zapnuta. Při zapnutí rezidentní ochrany máte dále možnost rozhodnout se, jakým způsobem mají být odstraněny detekované infekce:

- buďto automaticky (**Automaticky odstranit detekované infekce**)
- nebo po potvrzení uživatelem (**Před odstraněním infekcí se dotázat**)

Tato volba nijak neovliví úroveň bezpečnosti a pouze respektuje vaše aktuální potřeby.



V obou případech pak máte ještě možnost zvolit, zda se mají **Kontrolovat tracking cookies** (cookies = malé množství dat v protokolu HTTP, která server pošle prohlížeči, aby je uložil na počítači uživatele. Při každé další návštěvě téhož serveru pak prohlížeč tato data posílá zpět serveru, který podle nich rozlišuje jednotlivé uživatele, například při ukládání obsahu nákupního košíku, atp.). V odvolaných případech slouží tato možnost k dosažení vyššího stupně bezpečnosti, ve výchozím nastavení je však vypnuta.

Poznámka: Všechny komponenty AVG jsou výrobcem nastaveny k optimálnímu výkonu. Pokud nemáte skutečný důvod vedle jejich konfigurací, doporučujeme ponechat program ve výchozím nastavení. Změnu konfigurace by měli provádět pouze zkušení uživatelé. Chcete-li tedy změnit nastavení programu AVG, zvolte ze systémového menu položku **Nástroje / Pokročilé nastavení a editaci nastavení** provedete v nově otevřeném dialogu [Pokročilé nastavení AVG](#).

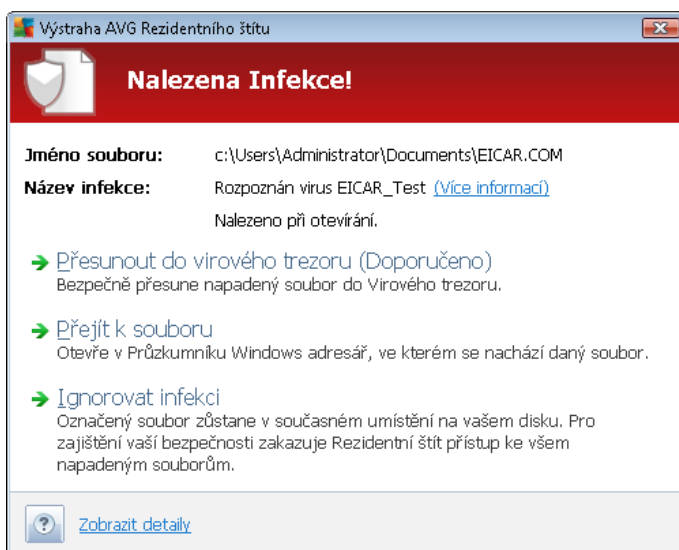
Ovládací tlačítka dialogu

Ovládací tlačítka dostupná v rozhraní komponenty **Rezidentní štít**:

- **Správa výjimek** - otevírá dialogové okno [Výjimky Rezidentního štítu](#), v němž lze definovat adresy a soubory, které mají být z kontroly [Rezidentním štítem](#) vypuštěny
- **Uložit změny** - stiskem tohoto tlačítka budou uloženy všechny v tomto dialogu provedené změny
- **Storno** - stiskem tlačítka se vrátíte do výchozího [uživatelského rozhraní AVG](#) (přehled komponent)

7.4.3. Nálezy Rezidentního štítu

Rezidentní štít kontroluje soubory při jejich otevírání, ukládání a kopírování. Jestliže detekuje virus nebo jakýkoliv podezřelý objekt, budete okamžitě varováni tímto dialogem:



V dialogu je uvedena informace o souboru, který byl detekován jako infikovaný (*Jméno souboru*) a



jméno rozpoznané infekce (*Název infekce*). Dále pak následuje odkaz do [Virové encyklopedie](#), kde najdete detailní informace o rozpoznané infekci, jsou-li tyto údaje známy (*Více informací*).

Dále je třeba, abyste se rozhodli, co se má s infikovaným souborem udělat. K dispozici jsou následující volby:

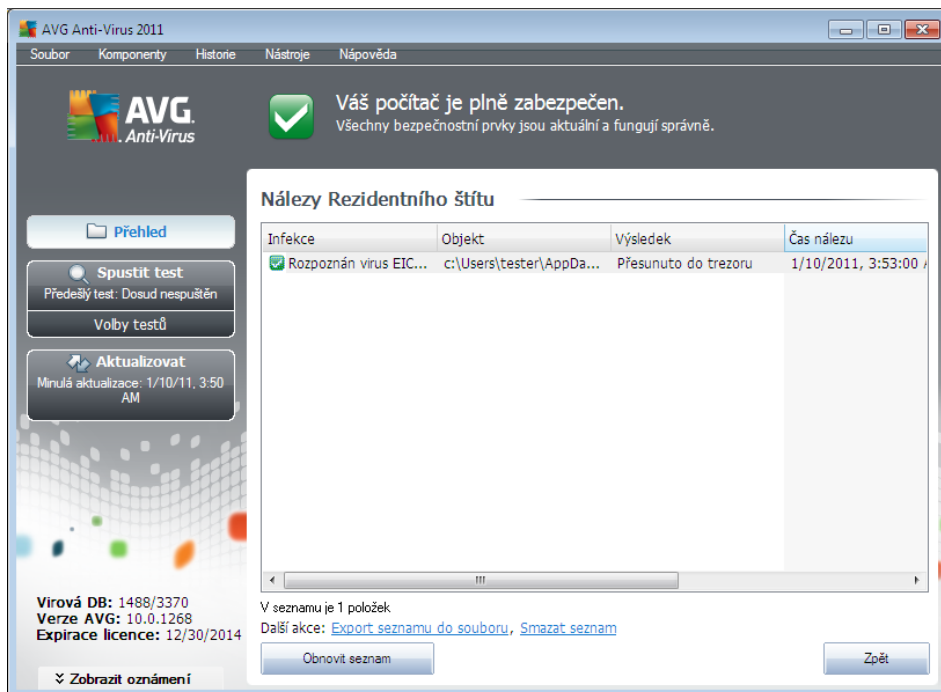
Mjte prosím na paměti, že nemusí být vždy dostupné všechny možnosti! Jednotlivé nabídky řešení se zobrazují na základě specifických podmínek (například jaký typ souboru je infikován, kde je umístěn a podobně).

- **Odstranit infekci jako uživatel s právy skupiny Power Users** - označte toto políčko, pokud se domníváte, že nemáte dostatečné oprávnění k tomu odstranit infekci jako běžný uživatel. Uživatelé skupiny Power Users mají rozšířená přístupová práva a je-li infekce detekována například v systémovém adresáři, bude nutné označit tuto volbu, aby mohla být infekce odstraněna.
- **Léčit** - toto tlačítko se zobrazí pouze v případě, že detekovaná infekce lze léčit. V takovém případě odstraní infekci ze souboru a obnoví soubor do původního stavu. V případě, že soubor jako celek je virus, bude při aplikaci této funkce vymazán (přesunut do [Virového trezoru](#))
- **Přesunout do virového trezoru** - infikovaný objekt bude přesunut do karanténního prostředí [Virového trezoru](#)
- **Přejít k souboru** - touto volbou zjistíte, kde je podezřelý objekt fyzicky umístěn (otevře se nové okno *Průzkumník Windows*)
- **Ignorovat** - tuto možnost rozhodně nedoporujujeme nikomu, kdo nemá skutečně dobrý důvod ji použít!

Poznámka: *Může se stát, že velikost detekovaného objektu bude větší než objem volného prostoru ve Virovém trezoru. V tom případě budete při pokusu o přesun infikovaného objektu vyzváni varovným hlášením o nedostatku místa ve Virovém trezoru. Objem Virového trezoru si však můžete sami nastavit. Velikost prostoru ve Virovém trezoru je dána procentuálně a závisí na celkové velikosti vašeho pevného disku. Nastavení velikosti Virového trezoru lze provést v dialogu [Virový trezor](#) v rámci [Pokročilého nastavení AVG](#), položka 'Omezit velikost Virového trezoru'.*

Ve spodní části dialogu najdete pak odkaz **Zobrazit detaily** - kliknutím na tento odkaz otevřete nové pop-up okno s detailní informací o procesu, při němž došlo k detekci infekce, a s uvedeným identifikačním číslem procesu.

Celkový přehled o všech hrozbách detekovaných [Rezidentním štítem](#) najdete v dialogu **Nález Rezidentního štítu**, který je dostupný ze systémového menu volbou [Historie/Nálezy Rezidentního štítu](#):



V dialogu najdete seznam objektů, které byly **Rezidentním štítem** detekovány jako nebezpečné a byly to vyladěny nebo přesunuty do **Virového trezoru**. U každého z detekovaných objektů jsou k dispozici následující informace:

- **Infekce** - popis (případně i jméno) detekovaného objektu
- **Objekt** - umístění detekovaného objektu
- **Výsledek** - jak bylo s detekovaným objektem naloženo
- **čas nálezu** - datum a čas detekce nebezpečného objektu
- **Typ objektu** - jakého typu je detekovaný objekt
- **Proces** - při jaké akci byl objekt detekován

Pod seznamem pak najdete informaci o celkovém počtu detekovaných objektů. Dále máte možnost exportovat celý seznam detekovaných objektů do samostatného souboru (**Exportovat seznam do souboru**) a vymazat všechny záznamy o detekovaných objektech (**Smazat seznam**). Tlačítkem **Obnovit seznam** aktualizujete seznam všech nálezů a tlačítkem **Zpět** se vrátíte do výchozího **uživatelského rozhraní AVG** (přehled komponent).

7.5. Family Safety

AVG Family Safety pomáhá ochránit vaše děti před nevhodným obsahem webových stránek, internetových médií a výsledků vyhledávání. Tato služba poskytuje přehled veškerého pohybu vašich dětí online, takže můžete nastavit příslušnou úroveň zabezpečení pro každého z uživatelů jednotlivě a sledovat jejich aktivity prostřednictvím samostatných útl.



Komponenta **AVG Family Safety** je aktivní pouze tehdy, pokud máte na svém počítači instalovaný produkt **AVG Family Safety**. Jestliže **AVG Family Safety** není nainstalován, klikněte na ikonu této komponenty v hlavním rozhraní **AVG Anti-Virus 2011** a budete přesměrováni na produktovou stránku AVG, kde najdete veškeré další podrobné informace o možnosti stažení a instalace produktu.

7.6. AVG LiveKive

AVG LiveKive automaticky zálohuje veškeré vaše dokumenty, fotografie a hudbu na bezpečném místě. V tomto záložním umístění budou vaše data dostupná odkudkoliv, z počítače i z mobilu s webovým rozhraním, a můžete se sdílet se svou rodinou i přáteli.

Komponenta **AVG LiveKive** je aktivní pouze tehdy, pokud máte na svém počítači instalovaný produkt **AVG LiveKive**. Jestliže **AVG LiveKive** není nainstalován, klikněte na ikonu této komponenty v hlavním rozhraní **AVG Anti-Virus 2011** a budete přesměrováni na produktovou stránku AVG, kde najdete veškeré další podrobné informace o možnosti stažení a instalace produktu.

7.7. Kontrola pošty

Jedním z nejčastějších zdrojů virů a trojských koní je e-mail. A díky phishingu a spamu se e-mail stává ještě v těmto zdrojích nebezpečí. Toto nebezpečí nastává obzvláště u zdarma dostupných poštovních úct (protože u těchto je použití anti-spamové technologie spíše výjimkou), které stále používá většina domácích uživatelů. Tito uživatelé také často navštíví neznámé webové stránky a nevědomky zadávají svá osobní data (nejčastěji svou e-mailovou adresu) do různých formulářů na webu, čímž ještě zvyšují riziko napadení prostřednictvím elektronické pošty. V těmto společnostem používají firemní poštovní účty a snaží se riziko minimalizovat implementací anti-spamových filtrů.

7.7.1. Princip kontroly pošty

Obecný doplněk pro kontrolu pošty slouží k automatické kontrole pošty v e-mailových klientech, které v AVG nemají svůj vlastní doplněk (ale lze jej použít i k testování pošty v klientech, pro které AVG specifický doplněk má, tedy Microsoft Outlook a The Bat). Můžete jej tedy použít primárně například ve spojení s programy Outlook Express, Mozilla, Incredimail atd.

Při [instalaci](#) AVG dojde k vytvoření automatických serverů pro kontrolu pošty - jednoho pro kontrolu příchozí pošty a druhého pro kontrolu pošty odchozí, s jejichž pomocí je následně automaticky kontrolována pošta na portech 110 a 25 (standardní porty pro příjem/odesílání pošty).

Kontrola pošty funguje jako rozhraní mezi e-mailovým klientem a e-mailovým serverem, umístěným na Internetu.

- **Příchozí pošta:** Při přijímání poštovní zprávy ze serveru otestuje komponenta **Kontrola pošty** přijímanou zprávu, odstraní případné viry a přidá certifikační text i upozornění o odstranění virové přílohy. Nalezené viry jsou umístěny do [Virového trezoru](#) (karantény). Teprve následně je zpráva předána poštovnímu klientovi.
- **Odchozí pošta:** Zpráva je odeslána z poštovního klienta do komponenty **Kontrola pošty**, kde proběhne kontrola příloh na přítomnost viru a zpráva je následně odeslána SMTP serveru (ve výchozím nastavení je kontrola odchozí pošty neaktivní a lze ji aktivovat ručně v nastavení kontroly pošty).

Poznámka: AVG Kontrola pošty není určena k ochraně poštovních serverů !

7.7.2. Rozhraní komponenty Kontrola pošty



V dialogu komponenty **Kontrola pošty** najdete stručný popis funkce komponenty, informaci o aktuálním stavu komponenty a následující statistiku:

- **Celkový počet ověřených e-mailů** - uvádí, kolik poštovních zpráv bylo po dobu spuštění této komponenty zkontrolováno (*hodnotu můžete v případě potřeby vynulovat a zařít po řádku znovu - Vynulovat hodnotu*)
- **Počet detekovaných a blokových infekcí** - udává počet infekcí, jež byly po dobu spuštění komponenty při kontrole poštovních zpráv zachyceny
- **Nainstalovaná ochrana e-mailu** - informuje o tom, který doplněk pro kontrolu pošty se používá (*informace se vztahuje k instalovanému výchozímu poštovnímu klientovi*)

Nastavení Kontroly pošty

Ve spodní části rozhraní najdete sekci **Nastavení Kontroly pošty**, v níž můžete editovat některé základní funkce této komponenty:

- **Test příchozích zpráv** - označením položky určíte, že má být prováděna kontrola všech doručených emailů. Položka je ve výchozím nastavení zapnuta, doporučujeme toto nastavení ponechat.
- **Test odchozích zpráv** - označením položky definujete, že mají být testovány veškeré odesílané emaily. Položka je ve výchozím nastavení vypnuta.



- **Zobrazit informa ní okno v systémové lišt b hem testování e-mailu** - ozna ením položky definujete, zda si p ežete zobrazit oznamovací dialog, který se objeví nad ikonou AVG na systémové lišt p i zahájení testování pošty komponentou [Kontrola pošty](#). Položka je ve výchozím nastavení zapnuta, doporu ujeme toto nastavení ponechat.

Pokro ilá editace konfigurace komponenty je k dispozici pod položkou **Nástroje/Pokro ilé nastavení**, dostupnou ze systémového menu, ale tuto editaci doporu ujeme jen zkušeným uživatel m!

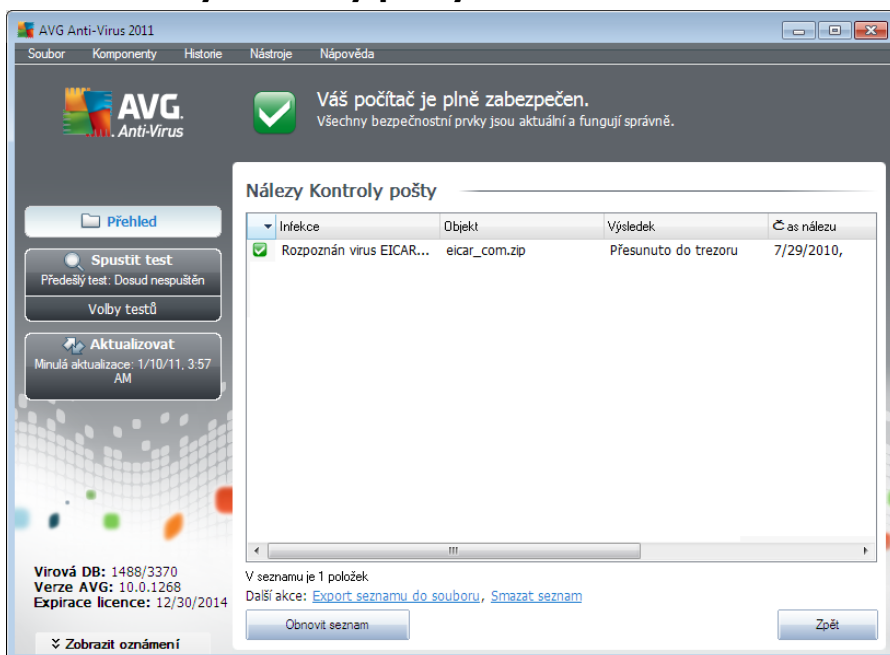
Poznámka: Všechny komponenty AVG jsou výrobcem nastaveny k optimálnímu výkonu. Pokud nemáte skute ný d vod jejich konfiguraci m nit, doporu ujeme ponechat program ve výchozím nastavení. Zm nu konfigurace by m li provád t pouze zkušení uživatelé. Chcete-li tedy zm nit nastavení programu AVG, zvolte ze systémového menu položku **Nástroje / Pokro ilé nastavení** a editaci nastavení prove te v nov oteveném dialogu [Pokro ilé nastavení AVG](#).

Ovládací tlačítka dialogu

Ovládací tlačítka dostupná v rozhraní komponenty **Kontrola pošty**:

- **Uložit změny** - stiskem tohoto tlačítka budou uloženy všechny v tomto dialogu provedené změny
- **Storno** - stiskem tlačítka se vrátíte do výchozího [uživatelského rozhraní AVG](#) (p ehled komponent)

7.7.3. Nálezy Kontroly pošty



V dialogu **Nálezy Kontroly pošty** (dostupném ze systémového menu volbou položek *Historie / Nálezy Kontroly pošty*) se bude zobrazovat seznam nález detekovaných komponentou [Kontrola](#)



pošty. U každého z detekovaných objektů jsou k dispozici následující informace:

- **Infekce** - popis (případně i jméno) detekovaného objektu
- **Objekt** - umístění detekovaného objektu
- **Výsledek** - jak bylo s detekovaným objektem naloženo
- **čas nálezů** - datum a čas detekce
- **Typ objektu** - jakého typu je detekovaný objekt

Pod seznamem pak najdete informaci o celkovém počtu detekovaných objektů. Dále máte možnost exportovat celý seznam detekovaných objektů do samostatného souboru (**Export seznamu do souboru**) a vymazat všechny záznamy o detekovaných objektech (**Smazat seznam**).

Ovládací tlačítka dialogu

Ovládací tlačítka dostupná v dialogu **Nálezy Kontroly pošty**:

- **Obnovit seznam** - aktualizuje seznam nálezů podle momentálního stavu
- **Zpět** - přejdete zpět do předchozího zobrazeného dialogu

7.8. Manažer aktualizací

7.8.1. Princip Manažeru aktualizací

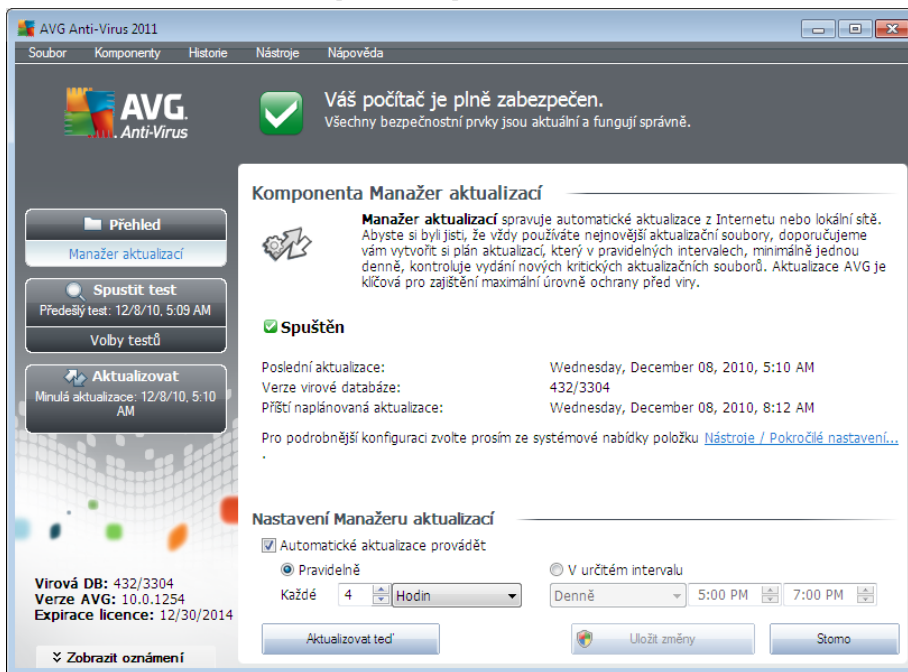
Každý bezpečnostní software musí zajistit skutečnou ochranu vašeho počítače před různými typy nebezpečí pouze tehdy, je-li pravidelně aktualizován. Autoři virů stále hledají nové a nové trhliny v operačních systémech i softwarových aplikacích a snaží se jich zneužít. Denně se objevují nové viry, nový malware, množí se internetové útoky. V reakci na tento vývoj pak výrobci software nepřetržitě vydávají nové aktualizace a bezpečnostní záplaty, aby dosáhli maximální úrovně bezpečnosti.

Je naprosto klíčové pravidelně aktualizovat AVG!

K tomu slouží komponenta **Manažer aktualizací**, s jejíž pomocí můžete naplánovat pravidelné automatické stahování aktualizací balíčků z Internetu nebo lokální sítě. Aktualizace databáze by měla být naplánována minimálně jednou denně. Méně kritické programové aktualizace mohou být naplánovány jednou týdně.

Doporučení: Pro podrobné informace o typech a úrovních aktualizací [tete prosím kapitolu Aktualizace AVG!](#)

7.8.2. Rozhraní komponenty Manažer aktualizací



Rozhraní komponenty **Manažer aktualizací** informuje o základní funkci této komponenty, aktuálním stavu komponenty a zobrazuje relevantní statistická data:

- **Poslední aktualizace** - datum uvádí, kdy a v kolik hodin byla naposledy provedena aktualizace databáze
- **Verze virové databáze** - číslo určuje verzi aktuálně instalované virové databáze a zvyšuje se při každé její aktualizaci
- **Příští naplánovaná aktualizace** - datum uvádí, kdy a v kolik hodin má být podle plánu spuštěna další aktualizace databáze

Nastavení Manažeru aktualizací

Ve spodní části dialogu v sekci **Nastavení Manažeru aktualizací** pak lze provést základní nastavení pravidel pro stahování aktualizací. Máte možnost definovat, zda si přejete stahovat aktualizace automaticky (**Automatické aktualizace provádět**) nebo pouze na vyžádání. Ve výchozím nastavení je funkce **Automatické aktualizace provádět** zapnuta a doporučujeme ji zapnutou ponechat! Pravidelné aktualizace jsou pro správné fungování bezpečnostního software naprosto klíčové!

Dále pak můžete definovat, kdy mají být aktualizace prováděny a spuštěny:

- **Pravidelně** - určete v jakém časovém intervalu
- **V určitém intervalu** - určete v kolik hodin má být aktualizace spuštěna



Ve výchozí konfiguraci je nastaveno stahování aktualizací pravidelně na každé 4 hodiny. Doporučujeme toto nastavení ponechat, pokud nemáte skutečný důvod ke změně!

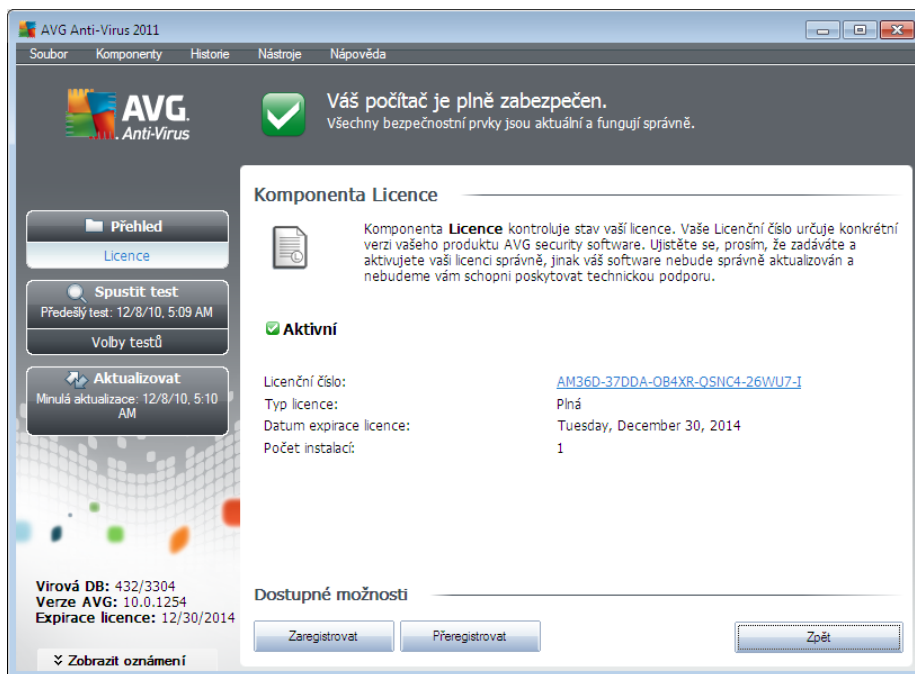
Poznámka: Všechny komponenty AVG jsou výrobcem nastaveny k optimálnímu výkonu. Změny konfigurace by měly provádět pouze zkušení uživatelé. Chcete-li tedy změnit nastavení programu AVG, zvolte ze systémového menu položku **Nástroje / Pokročilé nastavení** a editaci nastavení proveďte v nově otevřeném dialogu [Pokročilé nastavení AVG](#).

Ovládací tlačítka dialogu

Ovládací tlačítka dostupná v rozhraní komponenty **Manažer aktualizací**:

- **Aktualizovat teď** - na vyžádání okamžitě [spustí aktualizaci](#)
- **Uložit změny** - stiskem tohoto tlačítka budou uloženy všechny v tomto dialogu provedené změny
- **Storno** - stiskem tlačítka se vrátíte do výchozího [uživatelského rozhraní AVG](#) (přehled komponent)

7.9. Licence



Na rozhraní příslušné komponenty **Licence** najdete tyto informace:

- **Licenční číslo** - uvádí zkrácený tvar vašeho licenčního čísla (z bezpečnostních důvodů nejsou poslední tři znaky uvedeny). Licenční číslo je nutno zadávat vždy zcela přesně a ve tvaru, jak je definováno. Proto pro jakoukoli manipulaci s licenčním číslem doporučujeme použít metodu kopírovat/Možit.



- **Typ licence** - uvádí, o jaký typ produktu se jedná.
- **Datum expirace licence** - tímto dnem končí doba platnosti vaší licence, a pokud chcete nadále používat **AVG Anti-Virus 2011**, je třeba licenci prodloužit. Prodloužení licence lze provést on-line na [webu AVG](http://www.avg.cz).
- **Počet instalací** - číslo udává počet stanic, na nichž můžete **AVG Anti-Virus 2011** s tímto licenčním číslem oprávněně instalovat.

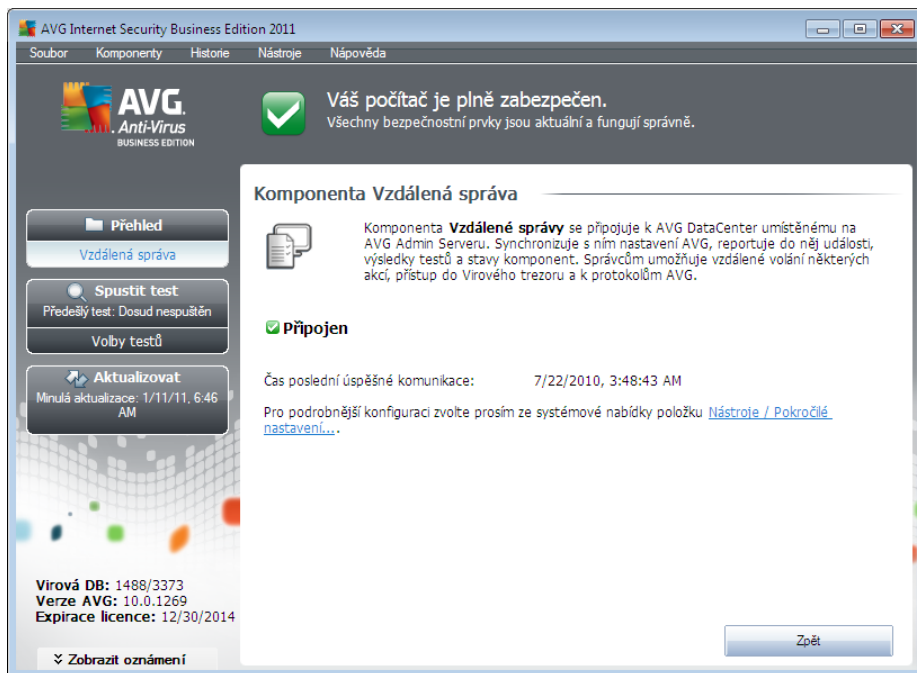
Ovládací tlačítka dialogu

- **Zaregistrovat** - otevírá web AVG (<http://www.avg.cz/>) na stránce **Registrace**. Vyplňte prosím své registrační údaje; pouze registrovaní zákazníci mají plný přístup k technické podpoře AVG.
- **Pro registrovat** - otevírá dialog **Aktivace AVG**, v němž jsou již předem vyplněna data, jež jste zadali v dialogu **Registrace AVG** během [instalačního procesu](#). V dialogu **Aktivace AVG** můžete zadat své licenční číslo, kterým budete nahradíte prodejní číslo (s nímž jste AVG instalovali), nebo kterým změníte dosavadní licenční číslo za jiné (např. při přechodu na jiný produkt značky AVG).

Poznámka: Máte-li nainstalovanou zkušební verzi **AVG Anti-Virus 2011**, tlačítka se zobrazí jako **Koupit online** a **Aktivovat** a odkáží Vás na web AVG, kde si můžete přímo zakoupit plnou verzi programu. Pokud máte nainstalovaný program **AVG Anti-Virus 2011** s prodejním číslem, tlačítka budou pojmenována **Zaregistrovat** a **Aktivovat**.

- **Zpět** - stiskem tlačítka se vrátíte do výchozího [uživatelského rozhraní AVG](#) (přehled komponent).

7.10. Vzdálená správa



Komponenta **Vzdálená správa** se v uživatelském rozhraní **AVG Anti-Virus 2011** zobrazí pouze v případě, že jste instalovali síťovou verzi produktu (viz [Licence](#)). V dialogu této komponenty najdete informaci o tom, zda je komponenta aktivní a připojena k serveru. Nastavení **Vzdálené správy** probíhá výhradně v sekci **Pokročilé nastavení / Vzdálená správa**.

Pro podrobný popis funkce a možností této komponenty a zapojení klientské stanice AVG do systému vzdálené správy vás odkazujeme na samostatnou dokumentaci v souvislosti s tímto tématem, která je ke stažení na [webu AVG \(www.avg.cz\)](http://www.avg.cz) v sekci **Centrum podpory / Stáhnout / Dokumentace**.

Ovládací tlačítka dialogu

- **Zpět** - stiskem tlačítka se vrátíte do výchozího [uživatelského rozhraní AVG](#) (přehled komponent)

7.11. Webový štít

7.11.1. Princip Webového štítu

Webový štít je typ rezidentní ochrany, která běží na pozadí a v reálném čase kontroluje obsah webových stránek nebo souborů stahovaných z Internetu. Každá stránka je prověřena ještě předtím, než je skutečně stažena a zobrazena webovým prohlížečem.

Webový štít detekuje, že stránka, kterou se chystáte navštívit, obsahuje nebezpečný javascript, a v takovém případě nebude infikovaná stránka vůbec zobrazena. Také rozpozná, že stránka obsahuje

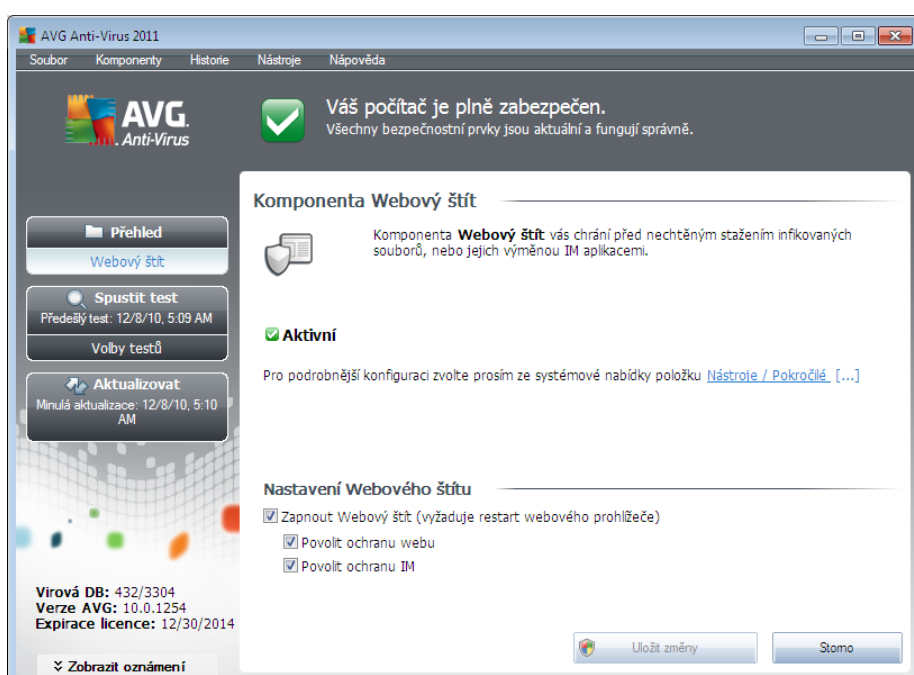


malware, který by mohl být prohlížením stránky zavlečen na váš počítač, a zabrání jeho stažení.

Poznámka: AVG Webový štít není určen k ochraně serverů!

7.11.2. Rozhraní komponenty Webový štít

Rozhraní komponenty **Webový štít** popisuje princip fungování tohoto typu ochrany, poskytuje informaci o aktuálním stavu komponenty a ve spodní části dialogu pak nabízí možnost základního nastavení funkcí této komponenty:



Základní nastavení komponenty

Především je tu možnost okamžitého zapnutí/vypnutí **Webového štítu** volbou položky **Zapnout Webový štít**. Tato položka je ve výchozím nastavení AVG zapnuta, komponenta je tedy aktivní. Pokud nemáte skutečný důvod toto nastavení změnit, doporučujeme ponechat komponentu vždy aktivní. Jestliže je položka označena a **Webový štít** spuštěn, jsou dostupné i dvě další možnosti nastavení komponenty:

- **Povolit ochranu webu** - touto volbou potvrzujete, že komponenta **Webový štít** má provádět kontrolu obsahu navštívených webových stránek.
- **Povolit ochranu IM** - touto volbou potvrzujete, že si přejete, aby byla prováděna kontrola okamžité on-line komunikace (to je komunikace pomocí programů pro okamžité zaslání zpráv, jakými jsou například ICQ, MSN Messenger, Yahoo Messenger ...).

Poznámka: Všechny komponenty AVG jsou výrobcem nastaveny k optimálnímu výkonu. Pokud nemáte skutečný důvod jejich konfiguraci změnit, doporučujeme ponechat program ve výchozím nastavení. Změnu konfigurace by měl provádět pouze zkušený uživatelé. Chcete-li tedy změnit



nastavení programu AVG, zvolte ze systémového menu položku **Nástroje / Pokro ilé nastavení a editaci nastavení** prove te v nov oteveném dialogu [Pokro ilé nastavení AVG](#).

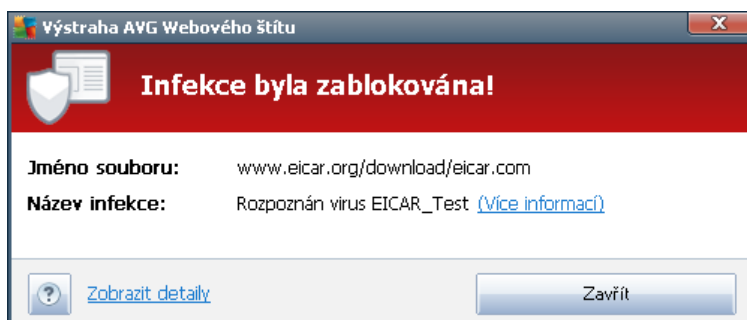
Ovládací tlačítka dialogu

Ovládací tlačítka dostupná v rozhraní komponenty **Webový štít** jsou následující:

- **Uložit změny** - stiskem tohoto tlačítka budou uloženy všechny v tomto dialogu provedené změny
- **Storno** - stiskem tlačítka se vrátíte do výchozího [uživatelského rozhraní AVG](#) (přehled komponent)

7.11.3. Nálezy Webového štítu

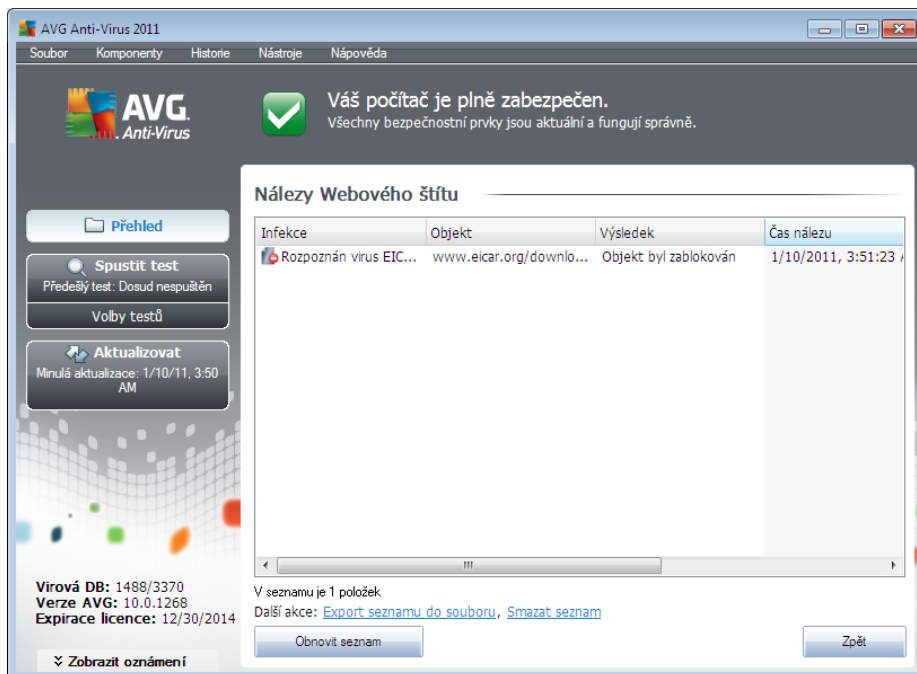
Webový štít kontroluje v reálném čase obsah webových stránek nebo soubor stahovaných z Internetu. Každá stránka je prověřena ještě předtím, než je skutečně stažena a zobrazena webovým prohlížečem. Jestliže detekuje virus nebo jakýkoliv podezřelý objekt, budete okamžitě varováni tímto dialogem:



V tomto varovném dialogu najdete informaci o souboru, který byl detekován jako infikovaný (*Jméno souboru*) a jméno rozpoznané infekce (*Název infekce*), a odkaz do [Virové encyklopedie](#), kde najdete podrobnější informace o rozpoznané infekci, jsou-li tyto údaje známy. V dialogu jsou dostupná tato tlačítka:

- **Zobrazit detaily** - kliknutím na tlačítko **Zobrazit detaily** otevře nové pop-up okno s informací o procesu, při němž došlo k detekci infekce, a s uvedeným identifikačním číslem procesu.
- **Zavřít** - tímto tlačítkem varovný dialog zavřete.

Webová stránka s podezřelým souborem nebude otevřena a záznam o detekované infekci bude zaznamenán v přehledu **Nálezy Webového štítu** - tento přehled detekovaných nálezů je dostupný ze systémového menu volbou [Historie/Nálezy Webového štítu](#).



U každého z detekovaných objektů jsou k dispozici následující informace:

- **Infekce** - popis (případně jméno) detekovaného objektu
- **Objekt** - umístění detekovaného objektu (stránka, odkud byl objekt stažen)
- **Výsledek** - jak bylo s detekovaným objektem naloženo (blokováce)
- **čas nálezu** - datum a čas, kdy došlo k detekci hrozby
- **Typ objektu** - jakého typu je detekovaný objekt
- **Proces** - při jaké akci byl objekt detekován

Pod seznamem pak najdete informaci o celkovém počtu detekovaných objektů. Dále máte možnost exportovat celý seznam detekovaných objektů do samostatného souboru (**Export seznamu do souboru**) a vymazat všechny záznamy o detekovaných objektech (**Smazat seznam**). Tlačítkem **Obnovit seznam** aktualizujete seznam všech nálezů a tlačítkem **Zpět** se vrátíte zpět do výchozího [uživatelského rozhraní AVG](#) (přehled komponent).

7.12. Anti-Rootkit

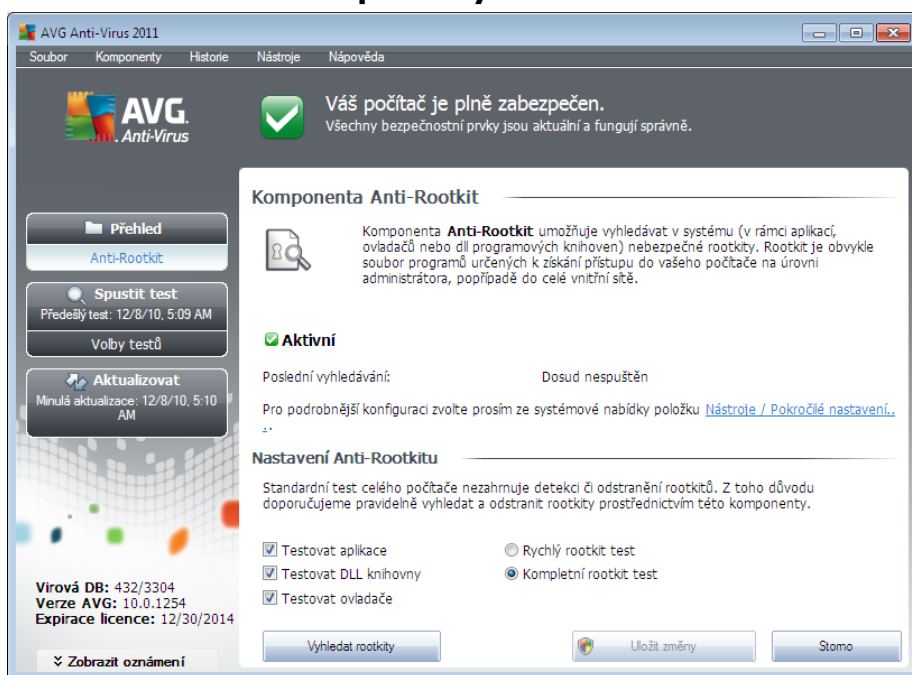
Rootkit je program speciálně vytvořený tak, aby dokázal převzít kontrolu nad vaším počítačem, aniž by požádal o jakoukoliv autorizaci. V tichosti se nepokouší ovládnout hardware, jejich cílem je ovládnout vaše operační systém. Rootkity umožňují skrývat běžící procesy, soubory a systémové údaje a upravují tedy operační systém tak, aby nebyly běžnými prostředky uživatele zjistitelné. Rootkity mají ve své škodlivého kódu poměrně výsadní postavení, jelikož pronikají hluboko do systému, přebírají požadavky systémových volání a správné výsledky nahrazují svými vlastními.



7.12.1. Princip Anti-Rootkitu

Anti-Rootkit je specializovaný nástroj pro detekci a úinné odstranění nebezpečných rootkitů, to jest programů a technologií, které dokáží maskovat přítomnost zákeřného software v počítači. Komponenta **AVG Anti-Rootkit** je schopna detekovat rootkit na základě definovaných pravidel. To znamená, že jsou detekovány všechny rootkity (nejen infikované). Dojde-li tedy k nález rootkitu, nemusí to nutně znamenat, že je počítač infikován. V některých případech mohou být rootkity použity jako ovladače nebo části korektních aplikací.

7.12.2. Rozhraní komponenty Anti-Rootkit



Rozhraní komponenty **Anti-Rootkit** uvádí stručný popis základní funkce této komponenty, informaci o stavu komponenty a dále informaci o době a času posledního spuštění komponenty (**Poslední vyhledávání**). V dialogu komponenty **Anti-Rootkit** je dále uveden odkaz [Nástroje / Pokročilé nastavení](#), kterým se přepnete do prostředí editace komponenty **Anti-Rootkit**.

Poznámka: Všechny komponenty AVG jsou výrobcem nastaveny k optimálnímu výkonu. Pokud nemáte skutečný důvod jejich konfiguraci změnit, doporučujeme ponechat program ve výchozím nastavení. Změnu konfigurace by měl provádět pouze zkušený uživatelé.

Nastavení Anti-Rootkitu

Ve spodní části rozhraní najdete sekci **Nastavení Anti-Rootkitu**, v níž můžete nastavit, které základní funkce testu na přítomnost rootkitů. Nejprve označením příslušného políčka (*jednoho nebo*



více) označte, jaké objekty mají být testovány:

- **Testovat aplikace**
- **Testovat DLL knihovny**
- **Testovat ovladače**

Dále se můžete rozhodnout, v jakém režimu si přejete test spustit:

- **Rychlý rootkit test** - testuje všechny běžící procesy, nainstalované ovladače a systémový adresář (v tšinou c:\Windows)
- **Kompletní rootkit test** - testuje všechny běžící procesy, nainstalované ovladače, systémový adresář (v tšinou c:\Windows) a také všechny lokální disky (včetně flash disku, ale bez disketové a CD mechaniky)

Ovládací tlačítka dialogu

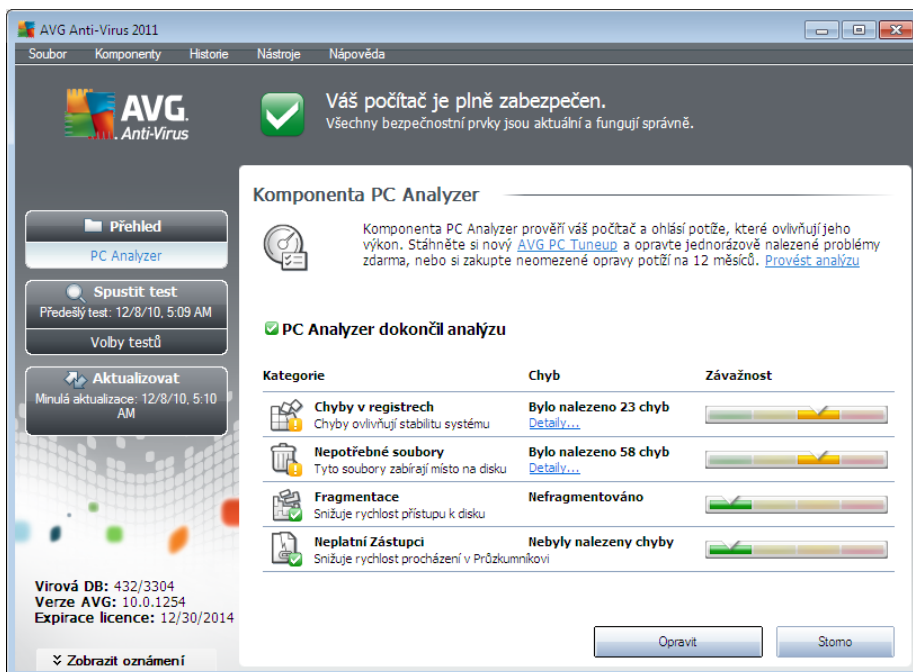
- **Vyhledat rootkity** - jelikož testování přítomnosti rootkitů není implicitní součástí [Testu celého počítače](#), slouží rozhraní komponenty **Anti-Rootkit** přímo ke spuštění samostatného testu; test spustíte stiskem tohoto tlačítka
- **Uložit změny** - stiskem tlačítka aplikujete veškeré změny v nastavení, které jste editovali v tomto dialogu, a vrátíte se do výchozího [uživatelského rozhraní AVG](#) (přehled komponent)
- **Storno** - stiskem tlačítka se bez uložení provedených změn vrátíte do výchozího [uživatelského rozhraní AVG](#) (přehled komponent)

7.13. PC Analyzer

Komponenta **PC Analyzer** provede celkovou kontrolu vašeho počítače a detekuje případné systémové chyby. V základním rozhraní komponenty najdete tabulku rozdělenou do čtyř řádků, jež odpovídají jednotlivým detekovaným kategoriím problémů:



Samotnou analýzu pak spustíte stiskem tlačítka **Provést analýzu**. Průběh kontroly budete moci sledovat přímo v tabulce, a tam budou posléze zobrazeny i výsledky analýzy:



- **Chyby v registrech** uvádí počet chyb v registrech Windows. Oprava registrů vyžaduje poměrně pokročilé znalosti, nedoporučujeme vám tudíž pouštět se do opravy na vlastní pěst.



- **Nepot ebné soubory** uvádí počet souborů, bez nichž byste se pravděpodobně obešli. Typickým příkladem mohou být různé typy dočasných souborů a soubory v odpadkovém koši.
- **Fragmentace** spočítá, jaká procentuální část vašeho pevného disku je fragmentována. Fragmentací pevného disku rozumíme skutečnost, že pevný disk se již dlouho používán a jednotlivé na něm uložené soubory jsou tedy fyzicky roztroušeny na různých částech disku. Tento problém lze odstranit použitím libovolného nástroje pro defragmentaci.
- **Poškozené odkazy** spočítá existující odkazy, které již nejsou funkční, například proto, že vedou na neexistující lokace.

V pohledu výsledků bude uveden konkrétní počet chyb nalezených v systému a rozdělených podle jednotlivých kategorií (*sloupec Chyb*). Výsledek analýzy bude také zobrazen graficky na ose ve sloupci **Závažnost**.

Ovládací tlačítka dialogu

- **Provést analýzu** - stiskem tlačítka spustíte okamžitou analýzu počítače
- **Opravit** - stiskem tlačítka přejdete na web AVG (<http://www.avg.cz/>) na stránce s podrobnými a aktuálními informacemi o komponentě PC Analyzer
- **Storno** - stiskem tlačítka můžete přerušit probíhající analýzu, anebo se vrátit do výchozího [uživatelského rozhraní AVG](#) (*přehled komponent*) po ukončení procesu analýzy

7.14. ID Protection

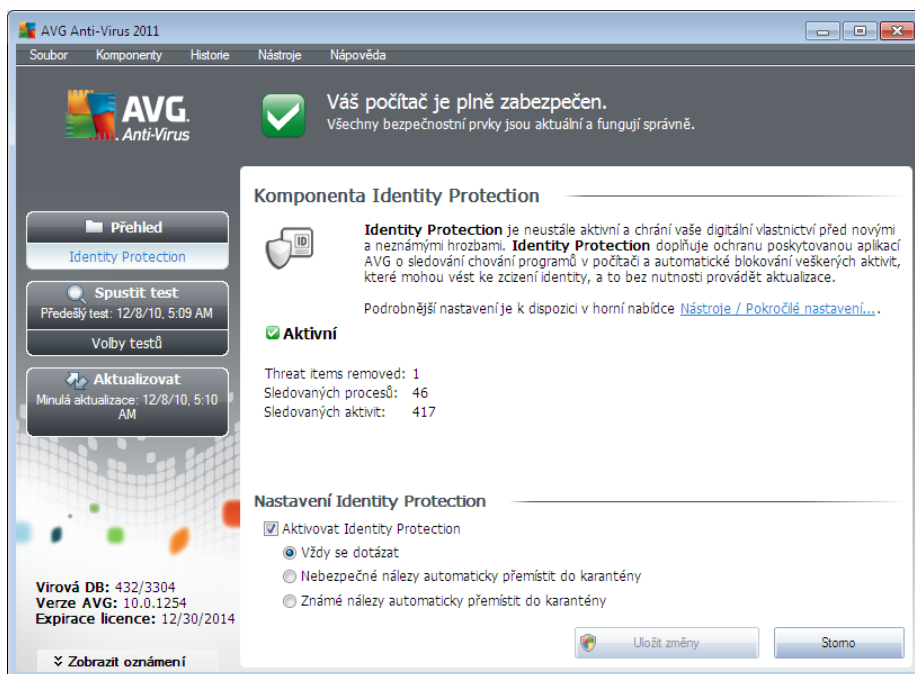
Komponenta **AVG Identity Protection** zajišťuje bezpečnost při nákupu, bankovních operacích a jiných elektronických transakcích. Slouží k detekci malware a je zaměřena na prevenci zcizení osobních dat (*přístupová hesla, bankovní údaje, čísla kreditních karet, ...*) a cenných informací prostřednictvím škodlivého software (*malware*), který útočí na váš počítač. **AVG Identity Protection** zajistí, že všechny programy běžící na vašem počítači pracují správně. **AVG Identity Protection** rozpozná jakékoliv podezřelé chování a škodlivý program zablokuje.

7.14.1. Princip ID Protection

AVG Identity Protection je novou komponentou, která přibývá a v reálném světě zajišťuje ochranu před různými druhy malware a viry, a to na bázi identifikace specifického chování těchto typů aplikací. Malware i viry se stále zdokonalují a často se s nimi lze setkat v podobě běžných programů, které se otevrou ve vašem počítači a umožní vzdálený přístup útočníkovi a zloději dat. **AVG Identity Protection** se zaměřuje právě na tento typ ochrany a je tak bezpečnostní složkou komplementární ke komponentě [AVG Anti-Virus](#), která vás chrání před známými viry detekovanými testováním za pomoci virových definic.

Pro naprostou bezpečnost vašeho počítače doporučujeme, abyste si nainstalovali obě komponenty, tedy [AVG Anti-Virus](#) i **AVG Identity Protection!**

7.14.2. Rozhraní ID Protection



Rozhraní komponenty **Identity Protection** uvádí stručný popis základních funkcí této komponenty, informaci o stavu komponenty a dále i některé další statistické údaje:

- **Odstraněných malware položek** - uvádí počet detekovaných a odstraněných aplikací hodnocených jako malware
- **Sledovaných procesů** - počet aktuálně sledovaných spuštěných aplikací
- **Sledovaných aktivit** - počet jednotlivých monitorovaných aktivit v rámci sledovaných procesů

7.14.3. Nastavení ID Protection

Ve spodní části rozhraní najdete sekci **Nastavení Identity Protection**, v níž můžete nastavit některé základní funkce komponenty:

- **Aktivovat Identity Protection** - označením této volby (ve výchozím nastavení zapnuto) aktivujete komponentu IDP a uvolníte i možnosti editace i další možnosti nastavení.

Můžete se stát, že **Identity Protection** označí zcela neškodný soubor jako podezřelý a potenciálně nebezpečný. **Identity Protection** detekuje infekce na základě chování dílčích procesů v jednotlivých aplikacích, a proto může k této chybné detekci dojít v případě, kdy se na který program snaží například monitorovat aktivitu na klávesnici, samostatně instalovat jiný program a podobně. Proto prosím zvolte jednu z následujících možností, která určuje, jak se má **Identity Protection** v případě detekce podezřelé aktivity zachovat:



- **Vždy se dotázat** - v případě detekce aplikace, která bude považována za malware, se IDP dotáže, zda si skutečně přejete tuto aplikaci zablokovat (*tato volba je zapnuta ve výchozím nastavení a pokud nemáte skutečný důvod nastavení změnit, doporučíme tuto konfiguraci ponechat*)
- **Nebezpečné nálezy automaticky přemístit do karantény** - veškeré aplikace detekované jako malware budou automaticky zablokovány
- **Známé nálezy automaticky přemístit do karantény** - zablokovány budou jen ty aplikace, o nichž lze s naprostou jistotou říci, že se skutečně jedná o malware

Ovládací tlačítka dialogu

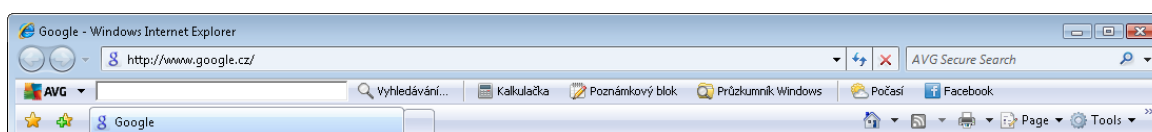
Ovládací tlačítka dostupná v rozhraní komponenty **Identity Protection**:

- **Uložit změny** - stiskem tohoto tlačítka budou uloženy všechny v tomto dialogu provedené změny
- **Storno** - stiskem tlačítka se vrátíte do výchozího [uživatelského rozhraní AVG](#) (přehled komponent)



8. AVG Security Toolbar

AVG Security Toolbar je nástroj, který úzce spolupracuje s komponentou [LinkScanner](#) a zajišťuje Vaši maximální bezpečnost při veškerém pohybu online. **AVG Security Toolbar** se v rámci **AVG Anti-Virus 2011** instaluje volitelně; možnost rozhodnout se, zda tuto komponentu chcete instalovat, jste měli v průběhu [instalace ního procesu](#). **AVG Security Toolbar** je dostupný v podobě nástrojové lišty ve vašem internetovém prohlížeči. Podporovanými prohlížeči jsou Internet Explorer (ve verzi 6.0 a vyšší) a/nebo Mozilla Firefox (ve verzi 3.0 a vyšší). Jiné prohlížeče nejsou podporovány (pokud používáte alternativní prohlížeč, například Avant browser, můžete se setkat s nekorektním chováním).



AVG Security Toolbar je tvořen těmito prvky:

- **Logo AVG** s rozbalovací nabídkou:
 - **Použít bezpečné vyhledávání AVG** - Umožňuje vyhledávání prostřednictvím vyhledávače **AVG Secure Search**, kdy jsou všechny výsledky vyhledávání jsou průběžně kontrolovány službou [Search-Shield](#) a máte tak naprostou jistotu bezpečného pohybu online.
 - **Aktuální míra ohrožení** - Otevře webovou laboratoř s grafickým znázorněním aktuální úrovně nebezpečí na Internetu.
 - **AVG Threat Labs** - Otevře stránku **AVG Threat Lab** (<http://www.avgthreatlabs.com>), kde najdete informace o bezpečnosti jednotlivých webů a aktuální úrovni online ohrožení.
 - **Nápověda k liště** - Otevírá online nápovědu k jednotlivým funkcím **AVG Security Toolbar**.
 - **Odeslat zpětnou vazbu k produktu** - Otevře stránku s online formulářem, jehož prostřednictvím nám můžete zaslat svůj názor na **AVG Security Toolbar**.
 - **O aplikaci** - Otevře samostatné okno s informací o aktuální instalované verzi **AVG Security Toolbar**.
- **Vyhledávací pole** - Při vyhledávání prostřednictvím **AVG Security Toolbar** můžete snadno prohledávat web a mít jistotu, že všechny zobrazené výsledky budou zaručeně bezpečné. Do vyhledávacího pole zadejte klíčové slovo nebo frázi a stiskněte tlačítko **Vyhledávání** nebo klávesu **Enter**. Všechny výsledky vyhledávání jsou průběžně kontrolovány službou [Search-Shield](#) (v rámci komponenty [LinkScanner](#)).
- Zkratková tlačítka pro rychlý přístup k aplikacím **Kalkulačka**, **Poznámkový blok**, **Průzkumník Windows**
- **Počasí** - Tlačítkem otevřete samostatné okno s informací o aktuálním počasí v dané lokalitě a s výhledem na následující dva dny. Tato informace je aktualizována každých 3-6 hodin. V



dialogu můžete ručně změnit požadovanou lokalitu a také rozhodnout, zda si přejete uvádět teplotu ve stupních Celsia nebo Fahrenheita.



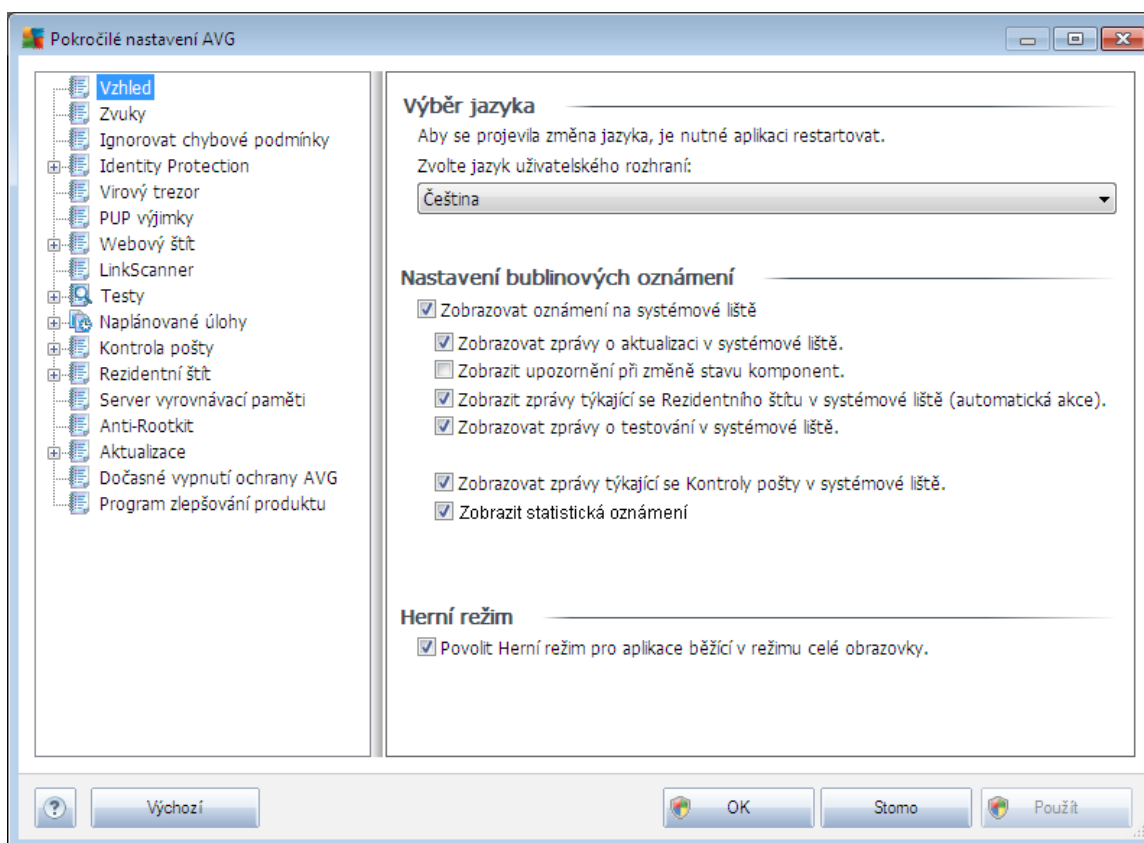
- **Facebook** - Tlačítko umožňuje přímé připojení k sociální síti [Facebook](#) z prostředí **AVG Security Toolbaru**.

9. Pokročilé nastavení AVG

Dialog pro pokročilou editaci nastavení programu **AVG Anti-Virus 2011** se otevírá v novém okně **Pokročilé nastavení AVG**. Toto okno je rozděleno do dvou částí: v levé části okna najdete přehlednou stromovou strukturu danou navigací konfigurací programu. Volbou komponenty, jejíž parametry chcete editovat (připadnou volbou konkrétní části této komponenty) otevřete v pravé části okna příslušný editační dialog.

9.1. Vzhled

První položka navigačního seznamu, **Vzhled**, se týká obecného nastavení [uživatelského rozhraní aplikace](#) a základních možností chování programu:

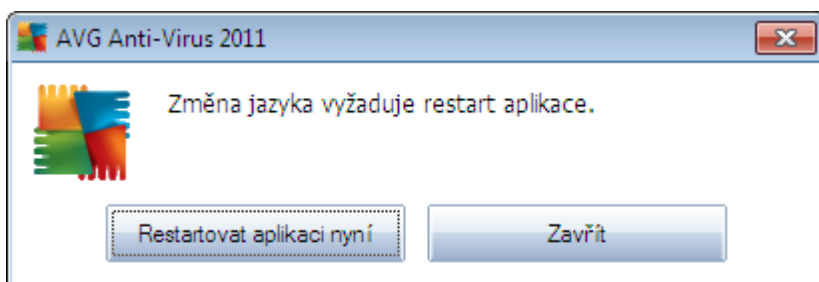


Výběr jazyka

V sekci **Výběr jazyka** můžete z rozbalovacího menu zvolit jazyk, v němž má být zobrazeno [uživatelské rozhraní AVG](#). V nabídce budou dostupné jen ty jazyky, které jste zvolili během [instalačního procesu](#) (viz kapitola [Uživatelské volby](#)) a angličtina (ta se *instaluje automaticky*). Pro zobrazení aplikace v požadovaném jazyce je však nutné uživatelské rozhraní restartovat; postupujte prosím následovně:

- Zvolte jazyk aplikace a volbu potvrďte stiskem tlačítka **Použít** (vpravo dole)

- Stiskem tlačítka **OK** zavěte editační dialog **Pokročilého nastavení AVG**
- Objeví se nový dialog s informací o tom, že pro dokončení změny jazyka uživatelského rozhraní je třeba aplikaci AVG restartovat:



Nastavení bublinových oznámení

V této sekci můžete potlačit zobrazování bublinových oznámení o aktuálním stavu aplikace. Ve výchozím nastavení programu jsou bublinová oznámení na systémové liště povolena, a doporučujeme toto nastavení ponechat! Bublinová oznámení přináší typicky informace o změně stavu některých klíčových komponent AVG a je vhodné v novat jim pozornost!

Pokud se přesto z nějakého důvodu rozhodnete, že si nepřejete být takto informováni, máte možnost kompletně potlačit zobrazování informativních oznámení, nebo zakázat pouze zobrazování informací vztahených k určité komponentě **AVG Anti-Virus 2011**. Všechny volby provádíte označením příslušné položky v takto strukturované nabídce:

- **Zobrazovat oznámení na systémové liště** - položka je ve výchozím nastavení označena, informace se zobrazují. Zrušením označení položky tedy zcela vypnete zobrazování jakýchkoliv informativních bublin. Jestliže je tato volba zapnuta, máte dále možnost definovat pravidla pro zobrazování jednotlivých typů informací:
 - **Zobrazovat zprávy o aktualizaci v systémové liště** - volbou položky rozhodnete, zda mají být zobrazena nebo naopak potlačena informativní hlášení o spuštění, průběhu a dokončení aktualizací; informace o ostatních procesech se budou zobrazovat normálně;
 - **Zobrazit upozornění při změně stavu komponent** - volbou položky rozhodnete, zda mají být zobrazena nebo naopak potlačena informativní hlášení o vypnutí/zapnutí komponenty, výskytu chyby ve funkci komponenty, ... V případě hlášení problému odpovídá tato volba změně barevnosti [ikony na systémové liště](#), které indikuje jakýkoliv problém v libovolné komponentě.
 - **Zobrazit zprávy týkající se Rezidentního štítu v systémové liště (automatická akce)** - volbou položky rozhodnete, zda mají být zobrazena nebo naopak potlačena informativní hlášení týkající se kontroly souborů při kopírování, otevírání nebo ukládání (*toto nastavení se projevuje pouze tehdy, má-li Rezidentní štít povoleno [automatické léčení detekované infekce](#)*);
 - **Zobrazovat zprávy o testování v systémové liště** - volbou položky rozhodnete, zda



mají být zobrazena nebo naopak potlačena informativní hlášení o automatickém spuštění naplánovaného testu, jeho průběhu, ukončení a výsledcích; informace o ostatních procesech se budou zobrazovat normálně;

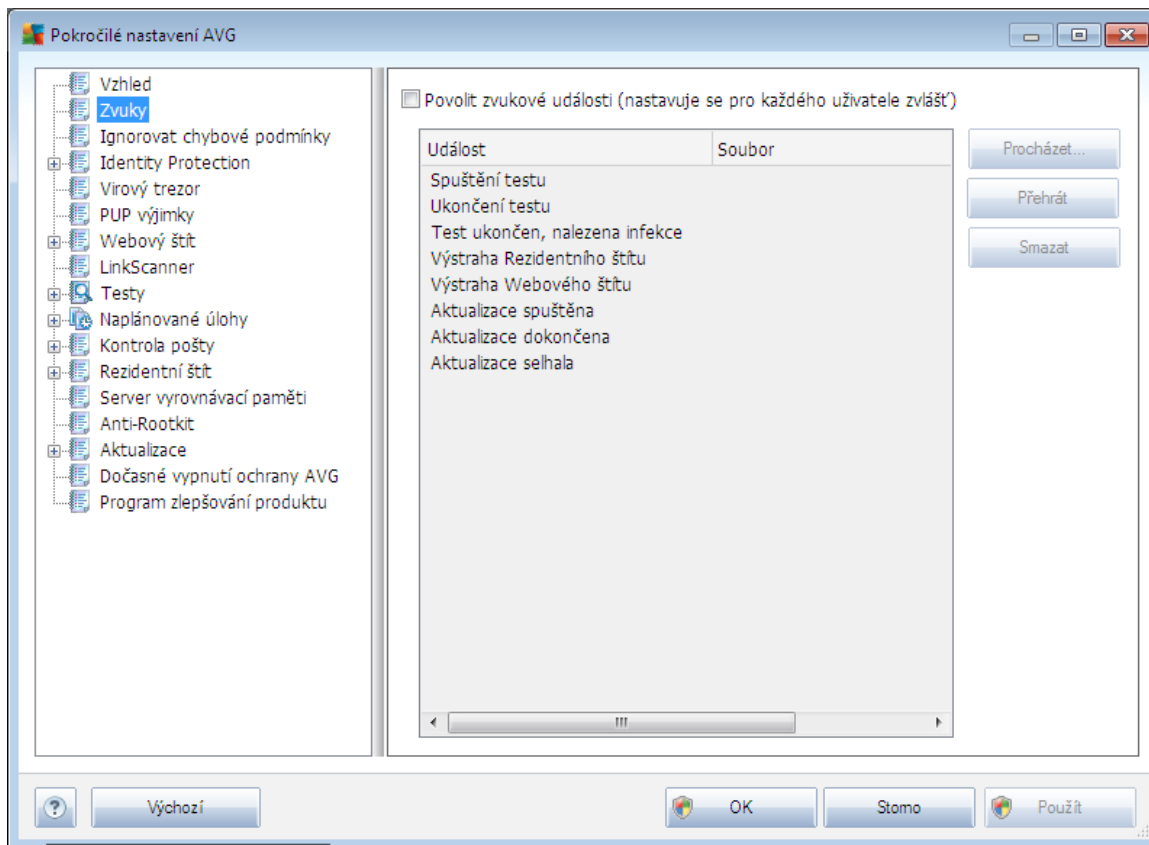
- **Zobrazovat zprávy týkající se Kontroly pošty v systémové liště** - volbou položky rozhodnete, zda mají být zobrazena nebo naopak potlačena informativní hlášení o průběhu testování příchozích a odchozích zpráv elektronické pošty; informace o ostatních procesech se budou zobrazovat normálně.
- **Zobrazit statistická oznámení** - volbou položky umožníte zobrazení pravidelného statistického přehledu v systémové liště.

Herní režim

Tato funkce je navržena s ohledem na aplikace, jež běží na celé obrazovce. Zobrazení oznámení AVG (například informace o spuštění testu apod.) by v tomto případě působilo velmi rušivě (došlo by k minimalizaci či k poškození grafiky). Abyste této situaci předešli, ponechejte prosím položku **Povolit herní mód pro aplikace běžící v režimu celé obrazovky** označenou (výchozí nastavení).

9.2. Zvuky

V dialogu **Zvuky** můžete rozhodnout, zda chcete být o jednotlivých akcích programu AVG informováni zvukovým oznámením. Pokud ano, označte prosím položku **Povolit zvukové události** (ta je ve výchozím nastavení vypnutá) a tím aktivujete seznam akcí, k nimž je možné zvukový doprovod přidat:

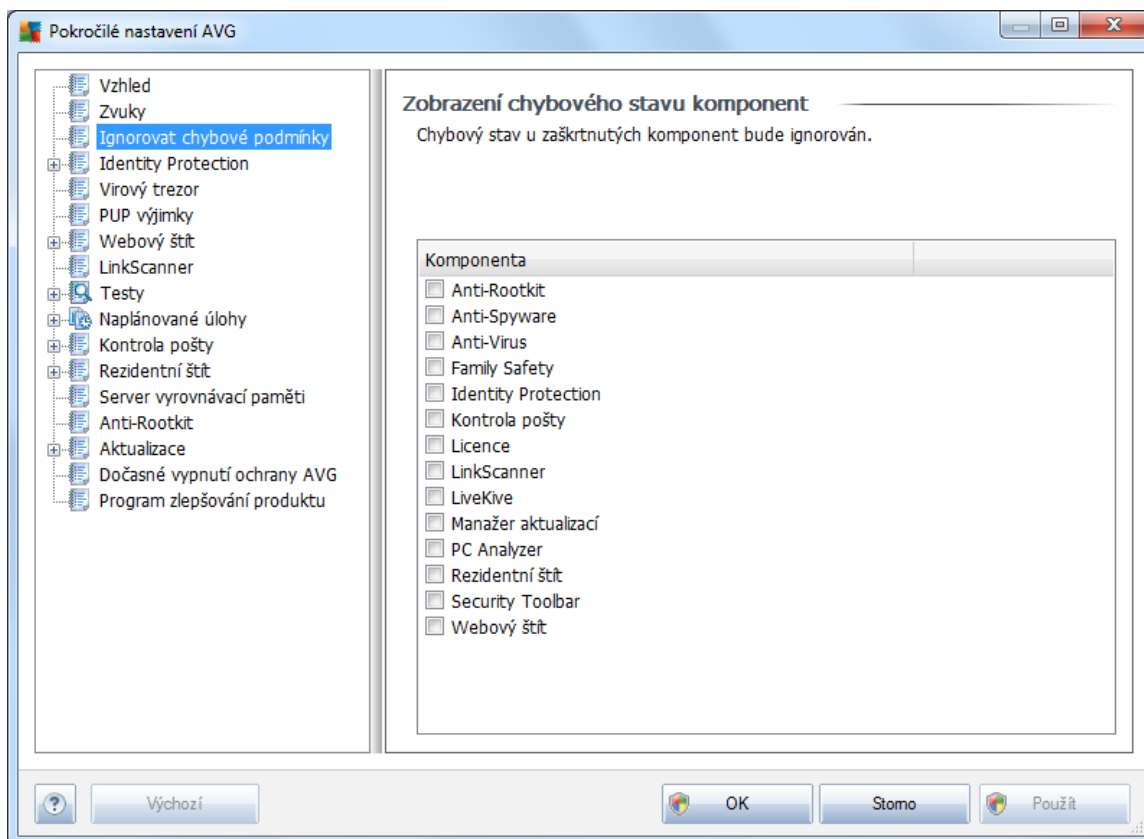


Poté vyberte ze seznamu konkrétní událost a tlačítkem **Procházet** zobrazíte strukturu svého disku, kde vyberete příslušný zvukový soubor a zvolené akci jej přidáte. Chcete-li si přehrát zvuk poslechnout, označte v seznamu příslušnou akci a stiskněte tlačítko **Přehrát**. Tlačítkem **Smazat** pak můžete zvuk přidat k zvolené akci zase odebrat.

Poznámka: V tuto chvíli jsou podporovány pouze zvukové soubory typu *.wav!

9.3. Ignorovat chybové podmínky

V dialogu **Zobrazení chybového stavu komponent** máte možnost označit ty komponenty, jejichž případný chybový stav si přejete ignorovat:



V základním nastavení programu není zvolena žádná komponenta. To znamená, že pokud dojde k jakékoliv chybě v libovolné programové komponentě, budete o tomto stavu okamžitě informováni, a to prostřednictvím:

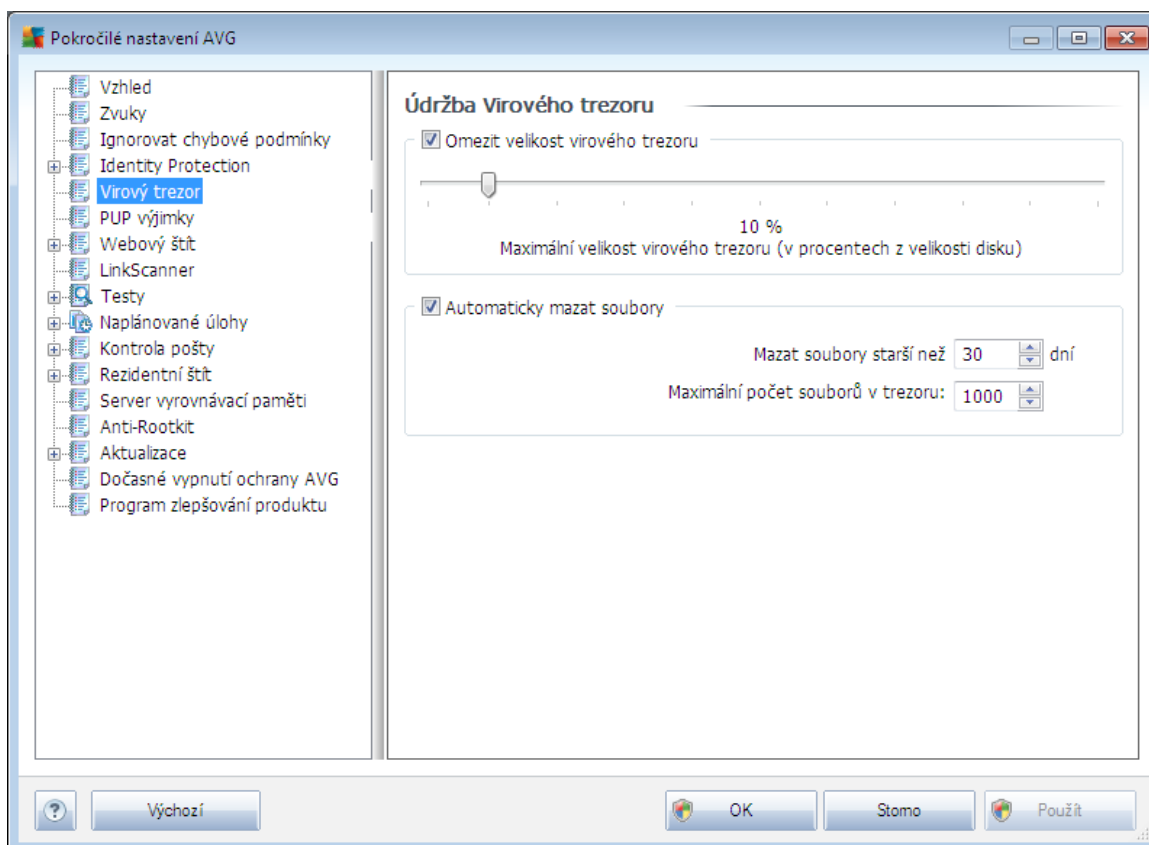
- **[ikony na systémové liště](#)** - pokud vše funguje jak má, je ikona zobrazena barevně; objeví-li se chyba, ikona se zobrazí se žlutým výkřikem
- textového popisu aktuálního problému v sekci **[Informace o stavu zabezpečení](#)** v hlavním okně AVG

Můžete se ale stát, že si z nějakého důvodu přejete dočasné deaktivovat určitou komponentu (samozřejmě doporučujeme ponechat všechny komponenty trvale zapnuté a ve výchozím nastavení, ale tato možnost existuje). Pak by ikona na systémové liště automaticky oznamovala chybový stav, který ale de facto není chybovým stavem, jelikož jste její samy navodili a jste si v domě potenciálního rizika. Zároveň by se tak zamezilo tomu, aby ikona reagovala na případnou jinou chybu v programu.

Proto máte v tomto dialogu pokročilého nastavení možnost označit ty komponenty, jejichž případný chybový stav (to znamená i jejich vypnutí) nemá být hlášen. Stejná možnost (**Ignorovat stav komponenty**) je dostupná pro jednotlivé komponenty také přímo z [přehledu komponent v hlavním](#)

[okn_AVG.](#)

9.4. Virový trezor



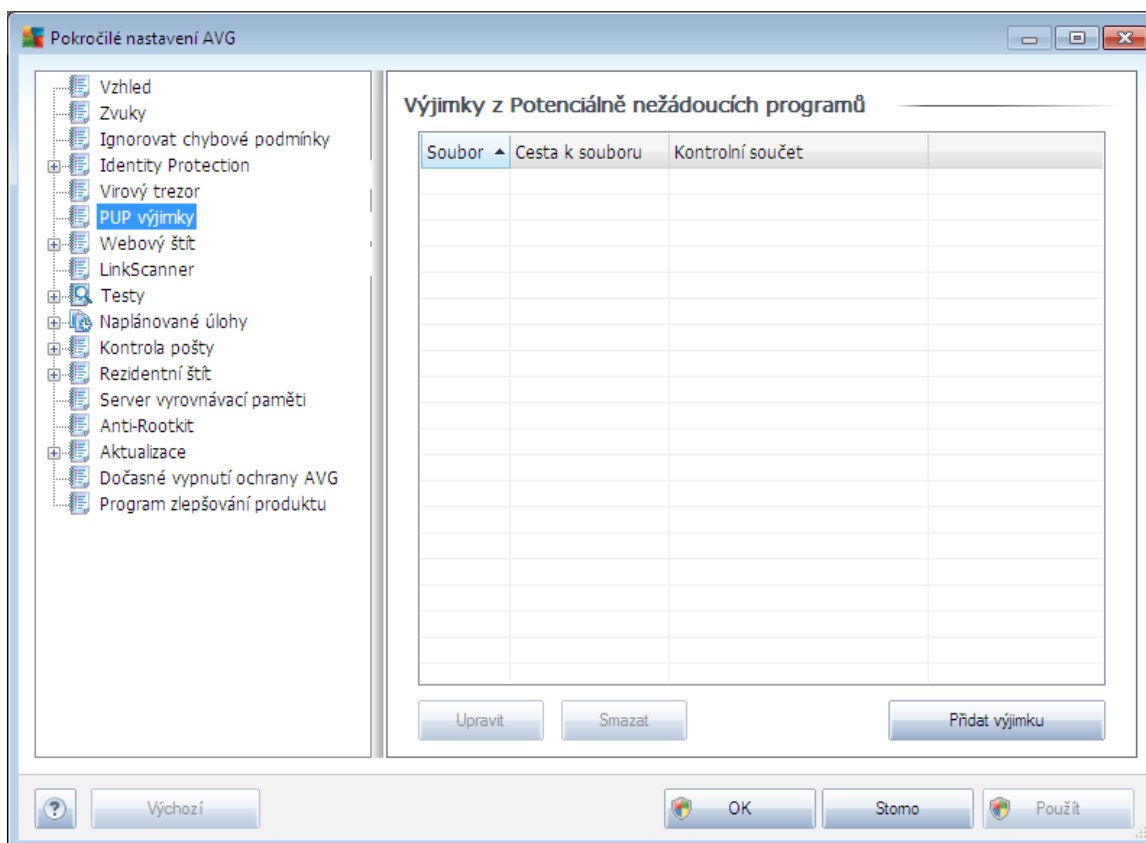
Dialog **Údržba Virového trezoru** umožňuje definovat několik parametrů souvisejících se správou objektů ve **Virovém trezoru**:

- **Omezit velikost virového trezoru** - na posuvníku můžete nastavit maximální povolenou velikost **Virového trezoru**. Velikost je určena procentuálně jako poměrná část velikosti vašeho lokálního disku.
- **Automaticky mazat soubory** - v této sekci definujete maximální dobu, po níž se mají uchovávat soubory ve **Virovém trezoru** (**Mazat soubory starší než ... dní**), a maximální počet souborů uložených ve **Virovém trezoru** (**Maximální počet souborů v trezoru**)

9.5. PUP výjimky

AVG Anti-Virus 2011 má schopnost analyzovat spustitelné programy, případně DLL knihovny, a určit, které z nich by mohly být nežádoucí (např. [spyware](#)). Může se však stát, že některé z programů detekovaných jako nežádoucí, jsou na vašem počítači nainstalovány s vaším vědomím a přejete si je používat. Příkladem může být bezplatný program, který obsahuje adware: termínem adware obecně rozumíme software generující zobrazení reklamy, obvykle přibalený jako doplněk k programu

distribuovanému zdarma. AVG může takový program při testech hlásit jako nežádoucí; pokud si však přejete jej na počítači ponechat, můžete jej definovat jako výjimku z potenciálně nežádoucích programů.



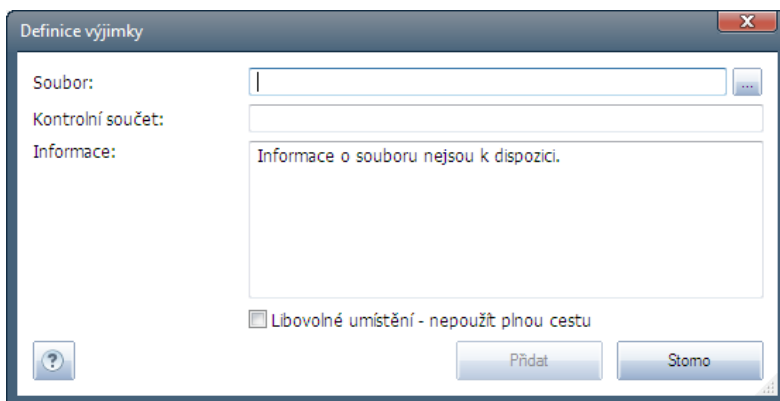
Dialog **Výjimky z Potenciálně nežádoucích programů** zobrazuje seznam již definovaných a aktuálně platných výjimek z potenciálně nežádoucích programů. Výjimku můžete editovat, smazat anebo nově přidat. Ke každé jednotlivé výjimce najdete v přehledu následující informace:

- **Soubor** - uvádí jméno konkrétní aplikace
- **Cesta k souboru** - ukazuje cestu k umístění aplikace na disku
- **Kontrolní součet** - uvádí unikátní "podpis" vybraného souboru - automaticky vygenerovaný a zec znak, který umožní jednoznačně odlišit zvolený soubor od všech ostatních. Tento součet je vygenerován a zobrazen až po úspěšném přidání dané výjimky.

Ovládací tlačítka dialogu

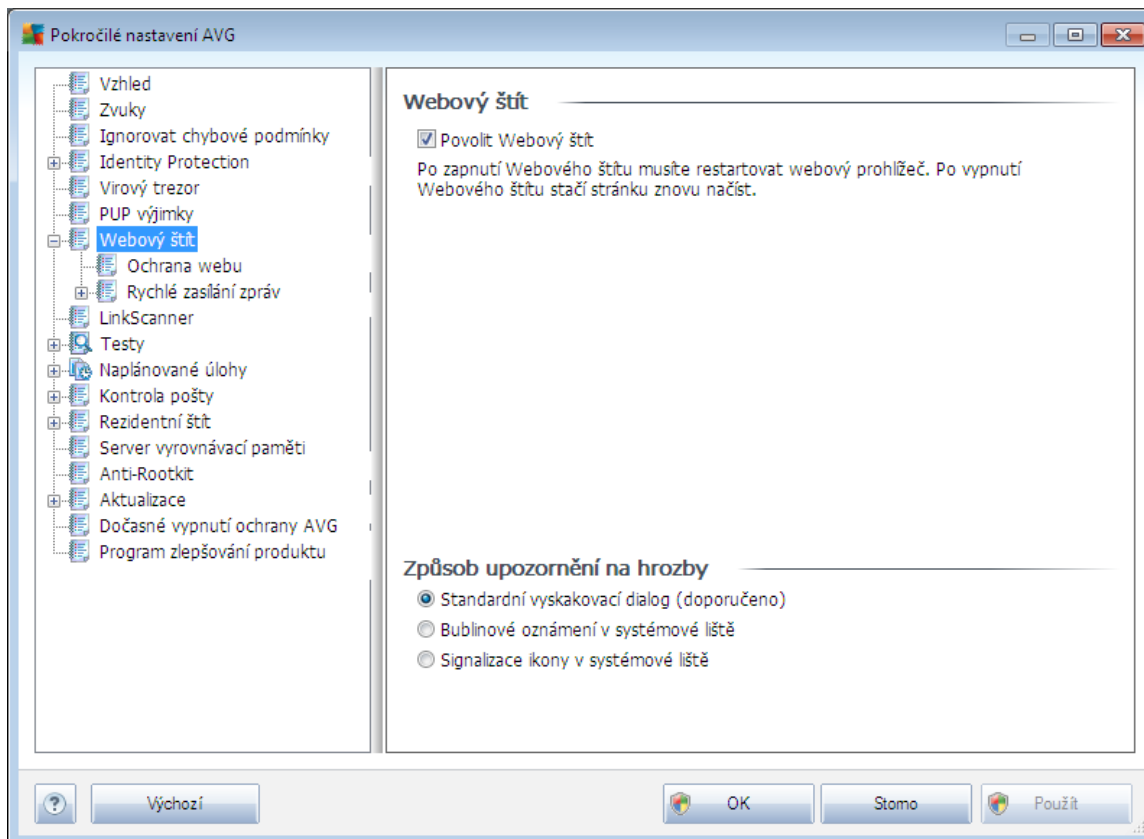
- **Upravit** - otevře editační dialog (totožný s dialogem pro zadání nové výjimky, viz níže) již definované výjimky, kde můžete nastavené parametry
- **Smazat** - odstraní označenou položku ze seznamu výjimek

- **Přidat výjimku** - otevře editační dialog, v němž můžete nastavit parametry nově definované výjimky:



- **Soubor** - zadejte plnou cestu k souboru, který chcete označit jako výjimku
- **Kontrolní součet** - uvádí unikátní "podpis" vybraného souboru - automaticky vygenerovaný řetězec znaků, který umožní jednoznačně odlišit zvolený soubor od všech ostatních. Tento součet je vygenerován a zobrazen až po úspěšném přidání dané výjimky.
- **Informace** - v této sekci se mohou zobrazovat dostupné informace o vybraném souboru (*informace o licenci, o verzi, ...*)
- **Libovolné umístění - nepoužít plnou cestu** - chcete-li uvedený soubor definovat jako výjimku pouze v tomto konkrétním umístění, ponechte položku **Libovolné umístění - nepoužít úplnou cestu** neoznačenou. Pokud položka označena, platí, že zadaný soubor je definován jako výjimka, ať už je umístěn kdekoli (*plnou cestu ke konkrétnímu souboru však musíte vyplnit v každém případě; tento soubor bude použit jako jednoznačný vzor pro případ, že by se ve vašem systému vyskytly dva odlišné soubory stejného jména*).

9.6. Webový štít



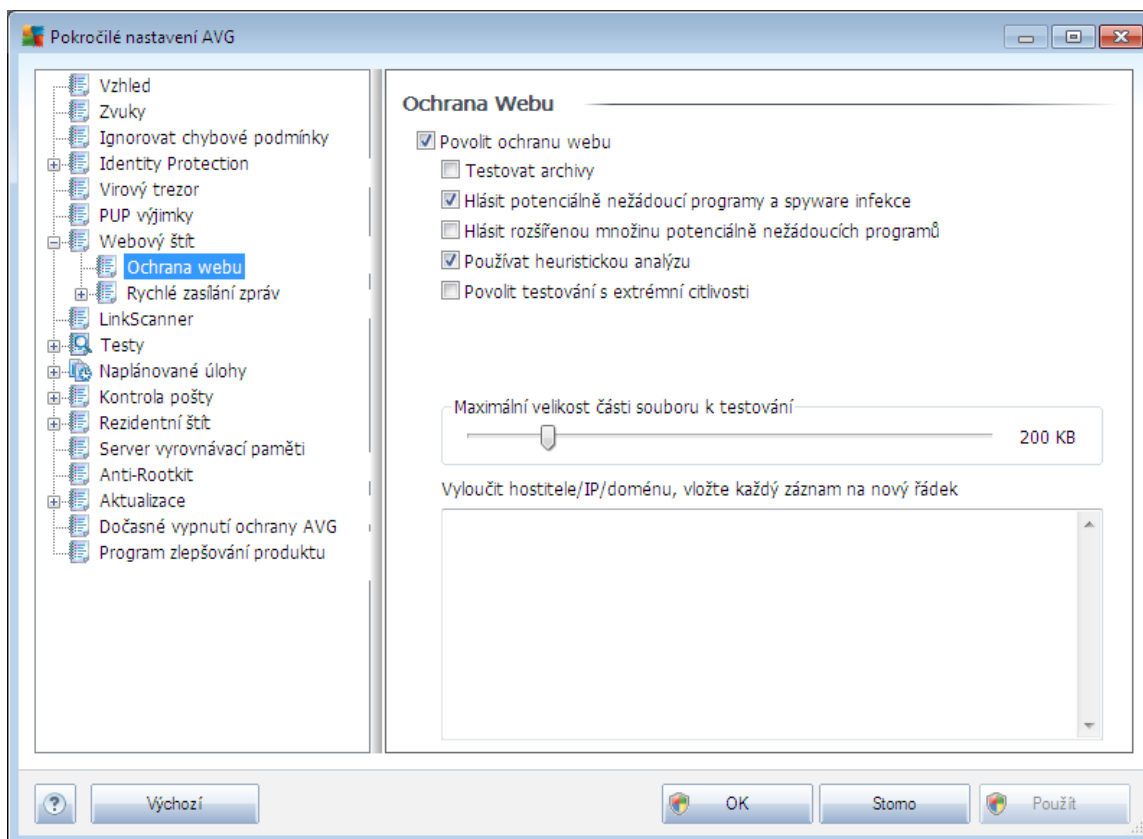
Dialog **Webový štít** nabízí možnost celkové aktivace/deaktivace komponenty **Webový štít** prostřednictvím označení položky **Povolit Webový štít** (ve výchozím nastavení zapnuto). Pokročilé nastavení této komponenty pak najdete na dalších hierarchicky uspořádaných dialozích odkazovaných z navigace.

- [Ochrana webu](#)
- [Rychlé zasílání zpráv](#)

Způsob upozornění na hrozby

Ve spodní části dialogu máte možnost zvolit si, jakým způsobem chcete být vyrozuměni o případných detekovaných hrozbách: standardním vyskakovacím dialogem, bublinovým oznámením v systémové liště nebo signalizací ikony v systémové liště.

9.6.1. Ochrana webu



V dialogu **Ochrana webu** máte možnost editovat nastavení komponenty pro kontrolu přístupu k webovým stránkám. Editace rozhraní nabízí nastavení těchto možností:

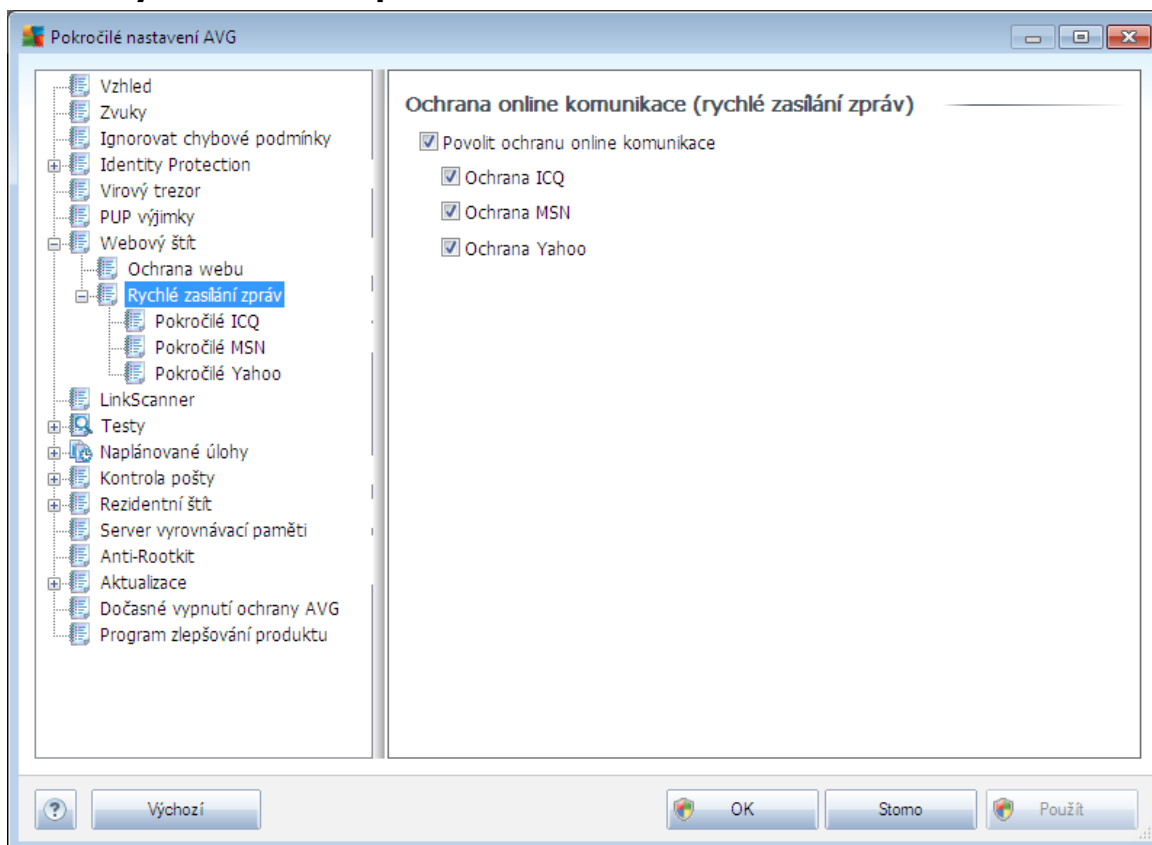
- **Povolit ochranu webu** - touto volbou potvrzujete, že v rámci komponenty **Webový štít** si přejete, aby byla prováděna kontrola obsahu navštívených www stránek. Za předpokladu, že je tato volba zapnuta (*výchozí nastavení*), můžete dále povolit nebo vypnout tyto volby:
 - **Testovat archivy** - (ve výchozím nastavení vypnuto) kontrola obsahu archivu, jež mohou být přítomny na zobrazované www stránce.
 - **Hlásit potenciálně nežádoucí programy a spyware infekce** - (ve výchozím nastavení zapnuto) kontrola přítomnosti potenciálně nežádoucích programů (spustitelné programy, které mohou fungovat jako spyware nebo adware). Zaškrtnutím tohoto políčka aktivujete **Anti-Spyware**, tj. bude se testovat přítomnost spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, protože i když v tísňovém případě program představuje bezpečenostní riziko, jsou mnohdy instalovány v domě a se souhlasem uživatele. Doporučujeme ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
 - **Hlásit rozšířenou množinu potenciálně nežádoucích programů** - (ve výchozím nastavení vypnuto) zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v podobě od výrobce



neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.

- **Používat heuristickou analýzu** - (ve výchozím nastavení zapnuto) kontrola obsahu zobrazované www stránky pomocí metody [heuristické analýzy](#) (dynamická emulace instrukcí testovaného objektu v prostředí virtuálního počítače).
- **Povolit testování s extrémní citlivostí** - (ve výchozím nastavení vypnuto) ve specifických situacích (například při podezření na infekci starším typem viru) můžete zvolit tuto metodu testování, která aktivuje nejdokladnější testovací algoritmy a velmi podrobně prohledá naprosto všechny oblasti vašeho počítače. Mějte však na paměti, že tato metoda je asociována velmi náročná.
- **Maximální velikost částí souboru k testování** - pokud jsou na zobrazované stránce přítomny vložené soubory, lze kontrolovat také jejich obsah ještě dříve, než budou staženy na váš počítač. Kontrola velkých souborů je však asociována a může výrazně zpomalit načítání www stránky. Posuvníkem tedy můžete nastavit maximální velikost souboru, který si můžete pomocí komponenty **Webový štít** testovat. I v případě, že soubor určený ke stažení bude větší než je nastavená povolená velikost souboru, a bude tudíž stažen bez kontroly [Webovým štítem](#), jste stále pod ochranou AVG: pokud by soubor byl infikován, bude okamžitě detekován [Rezidentním štítem](#).
- **Vyloučit hostitele/IP/doménu** - do textového pole můžete zadat konkrétní adresu serveru (hostitele, IP adresu, IP adresu s maskou nebo URL) i domény, jež mají být z kontroly [Webovým štítem](#) vyloučeny. Uvádějte tedy výhradně adresy hostitelů, u nichž si můžete být obsahem www stránek naprosto jisti.

9.6.2. Rychlé zasílání zpráv

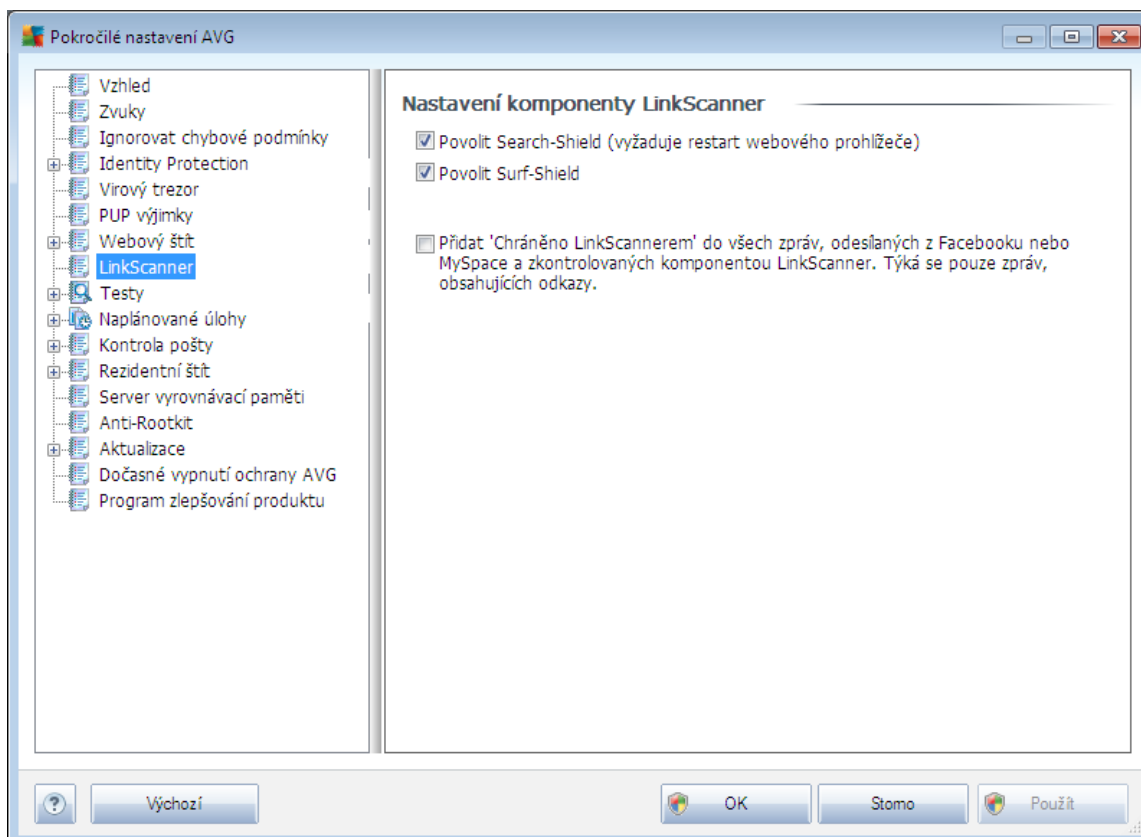


V dialogu **Ochrana online komunikace (rychlé zasílání zpráv)** můžete editovat parametry komponenty [Webový štít](#) vztahující se k online kontrole okamžité komunikace. V tuto chvíli jsou podporovány tyto tři programy pro rychlé zasílání zpráv: **ICQ**, **MSN** a **Yahoo** - označte příslušnou položku odpovídající programu, v němž chcete kontrolovat komunikaci prostřednictvím komponenty [Webový štít](#).

Podrobné nastavení seznamu povolených/zakázaných uživatelů můžete provést v příslušném dialogu (**Pokročilý ICQ**, **Pokročilý MSN**, **Pokročilý Yahoo**) a definovat **Whitelist** (seznam uživatelů, kteří mají povolenou komunikaci) a **Blacklist** (seznam uživatelů, jimž je komunikace blokována).

9.7. LinkScanner

Dialog **Nastavení komponenty [LinkScanner](#)** umožňuje zapnout i vypnout funkčnost základních složek [LinkScanner](#).



- **Povolit Search-Shield** - (ve výchozím nastavení zapnuto): služba je aktivní při vyhledávání na serverech Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg a SlashDot: veškeré výsledky vyhledávání jsou kategorizovány a označeny ikonou, která informuje o tom, zda je obsah odkazované stránky bezpečný i nebezpečný (vyžaduje restart webového prohlížeče).
- **Povolit Surf-Shield** - (ve výchozím nastavení zapnuto): aktivní ochrana proti agresivním webovým stránkám. Kontrola stránek se provádí v okamžiku jejich načítání. Stránky s nebezpečným obsahem jsou v příslušném internetovém prohlížeči (nebo jiné aplikaci, která používá HTTP) rovnou zablokovány.
- **Přidat 'Chráněno LinkScannerem' do všech zpráv ...** - označením této položky potvrdíte, že si přejete vložit certifikaci o kontrole [LinkScannerem](#) do všech zpráv odeslaných z sociálních sítí Facebook a MySpace, které obsahují aktivní odkazy na web.

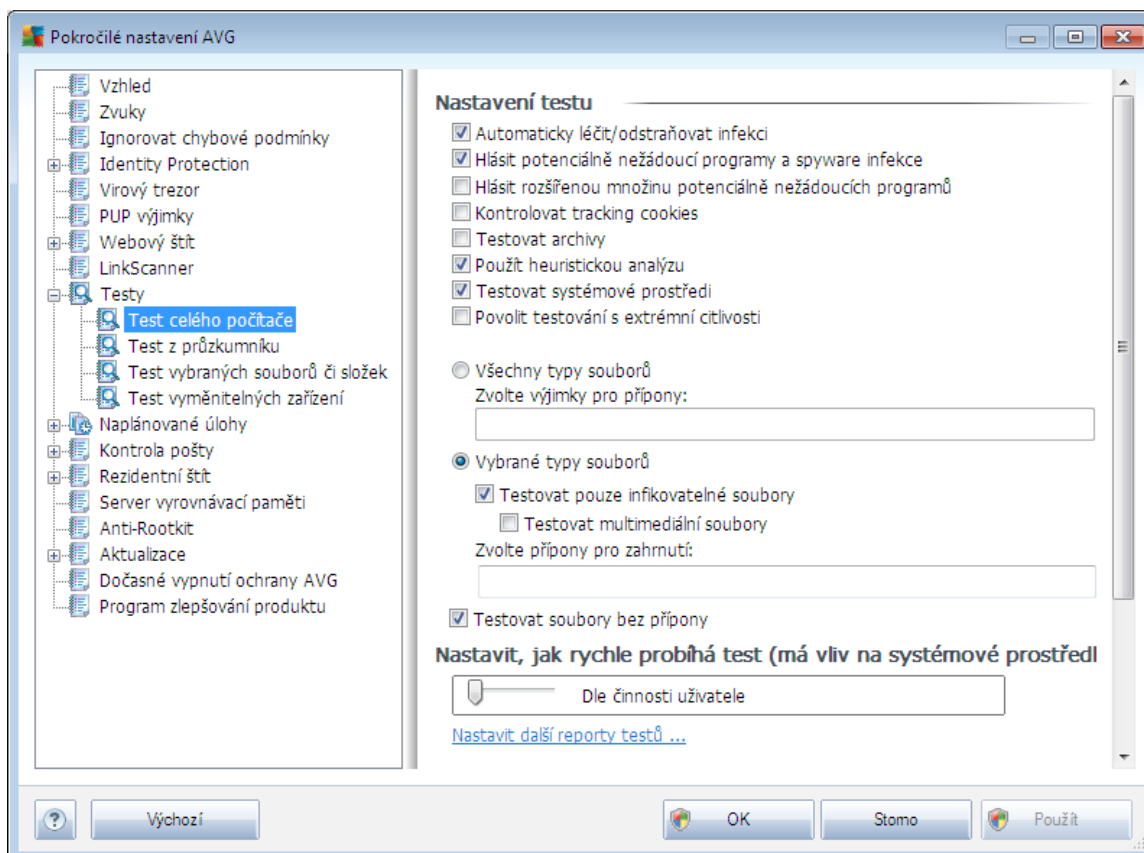
9.8. Testy

Pokročilé nastavení testů je rozděleno do čtyř kategorií, které odpovídají jednotlivým typům výrobem definovaných testů :

- [Test celého počítače](#) - výrobcem nastavený standardní test
- [Test z průzkumníku](#) - specifický test spouštěný nad zvolenými objekty přímo v prostředí Windows
- [Test vybraných souborů či složek](#) - výrobcem nastavený standardní test s možností definovat oblasti testování
- [Test vyměnitelných zařízení](#) - specifický test vyměnitelných zařízení připojených v danou chvíli k Vašemu PC

9.8.1. Test celého počítače

Položka [Test celého počítače](#) nabízí možnost editovat parametry předem nastaveného [Testu celého počítače](#):



Nastavení testu



V sekci **Nastavení testu** najdete seznam parametrů testu, které můžete podle potřeby vypínat/zapínat:

- **Automaticky léčit/odstranit infekci** (ve výchozím nastavení zapnuto) - je-li během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. Pokud virus automaticky léčit nelze, bude infikovaný objekt automaticky přesunut do [Virového trezoru](#).
- **Hlásit potenciálně nežádoucí programy a spyware infekce** (ve výchozím nastavení zapnuto) - kontrola přítomnosti [potenciálně nežádoucích programů](#) (spustitelné programy, které mohou fungovat jako spyware nebo adware). Zaškrtnutím tohoto políčka aktivujete [Anti-Spyware](#), tj. bude se testovat na přítomnost spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány v domě a se souhlasem uživatele. Doporučujeme nicméně ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
- **Hlásit rozšířenou množinu potenciálně nežádoucích programů** (ve výchozím nastavení vypnuto) - zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.
- **Kontrolovat tracking cookies** (ve výchozím nastavení vypnuto) - parametr komponenty [Anti-Spyware](#) definuje, že během testu mají být detekovány cookies (HTTP data zaslaná serverem prohlížeči a uložena na počítači uživatele; při každé další návštěvě téhož serveru prohlížeč posílá cookies zpět serveru, který podle nich rozlišuje jednotlivé uživatele).
- **Testovat archivy** (ve výchozím nastavení vypnuto) - parametr definuje, že test má kontrolovat všechny soubory zabalené v některém typu archivu, například ZIP, RAR, ...
- **Použít heuristickou analýzu** (ve výchozím nastavení zapnuto) - během testu bude použita k detekci infekce i metoda heuristické analýzy (dynamické emulace instrukcí testovaného objektu v prostředí virtuálního počítače).
- **Testovat systémové prostředí** (ve výchozím nastavení zapnuto) - test prověří i systémové oblasti vašeho počítače.
- **Povolit testování s extrémní citlivostí** (ve výchozím nastavení vypnuto) - ve specifických situacích (při podezření na infekci ve vašem počítači) můžete zvolit tuto metodu testování, která aktivuje nejdokladnější testovací algoritmy a velmi podrobně prověří naprosto všechny oblasti vašeho počítače. Mějte však na paměti, že tato metoda je časově velmi náročná.

Dále se můžete rozhodnout, zda si přejete testovat

- **Všechny typy souborů** - při němž máte zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou (po uložení se čárky změní na středníky);
- **Vybrané typy souborů** - můžete se rozhodnout, že chcete, aby se testy spouštěly pouze

nad soubory, které lze považovat za infikovatelné (soubory, které nemohou být infekcí zasaženy, se testovat nebudou - například prosté textové soubory nebo některé nespustitelné soubory), a to včetně multimediálních souborů (video, audio soubory - ponecháte-li tuto položku neoznačenou, výrazně se tím zkrátí čas testování, jelikož multimediální soubory jsou obvykle poměrně velké, ale pravděpodobnost infekce je u nich velmi nízká). I zde můžete určit výjimky a pomocí seznamu souborů definovat, které soubory mají být testovány za všech okolností.

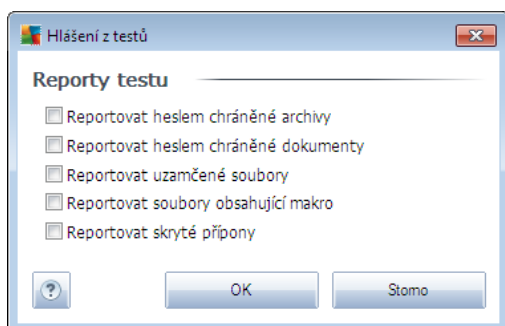
- U položky **Testovat soubory bez přípon** pak rozhodnete, zda se mají testovat i soubory se skrytou příponou nebo neznámou příponou. Tato položka je ve výchozím nastavení zapnutá a doporučujeme ji ponechat zapnutou, abyste se tohoto nastavení drželi, pokud nemáte skutečnou potřebu změnit její nastavení. Soubory bez přípon jsou obecně vysoce podezřelé a měly by být otestovány.

Nastavit, jak rychle probíhá test

V této sekci můžete nastavit požadovanou rychlost testování v závislosti na závažnosti systémových zdrojů. Ve výchozím nastavení je tato hodnota nastavena dle přání uživatele, což odpovídá střední úrovni využití systémových zdrojů. Pokud se rozhodnete pro spuštění rychlého testu, proběhne test v kratším čase, ale po dobu jeho běhu bude výrazně zvýšena závažnost systémových zdrojů, takže vaše práce na počítači bude obtížnější (tato varianta je vhodná pro situaci, kdy je počítač spuštěn, ale nikdo na něm aktuálně nepracuje). Naopak, prodloužením doby testu snížíte závažnost systémových zdrojů a vaše práce na počítači nebude téměř ovlivněna, test však bude probíhat po delší dobu.

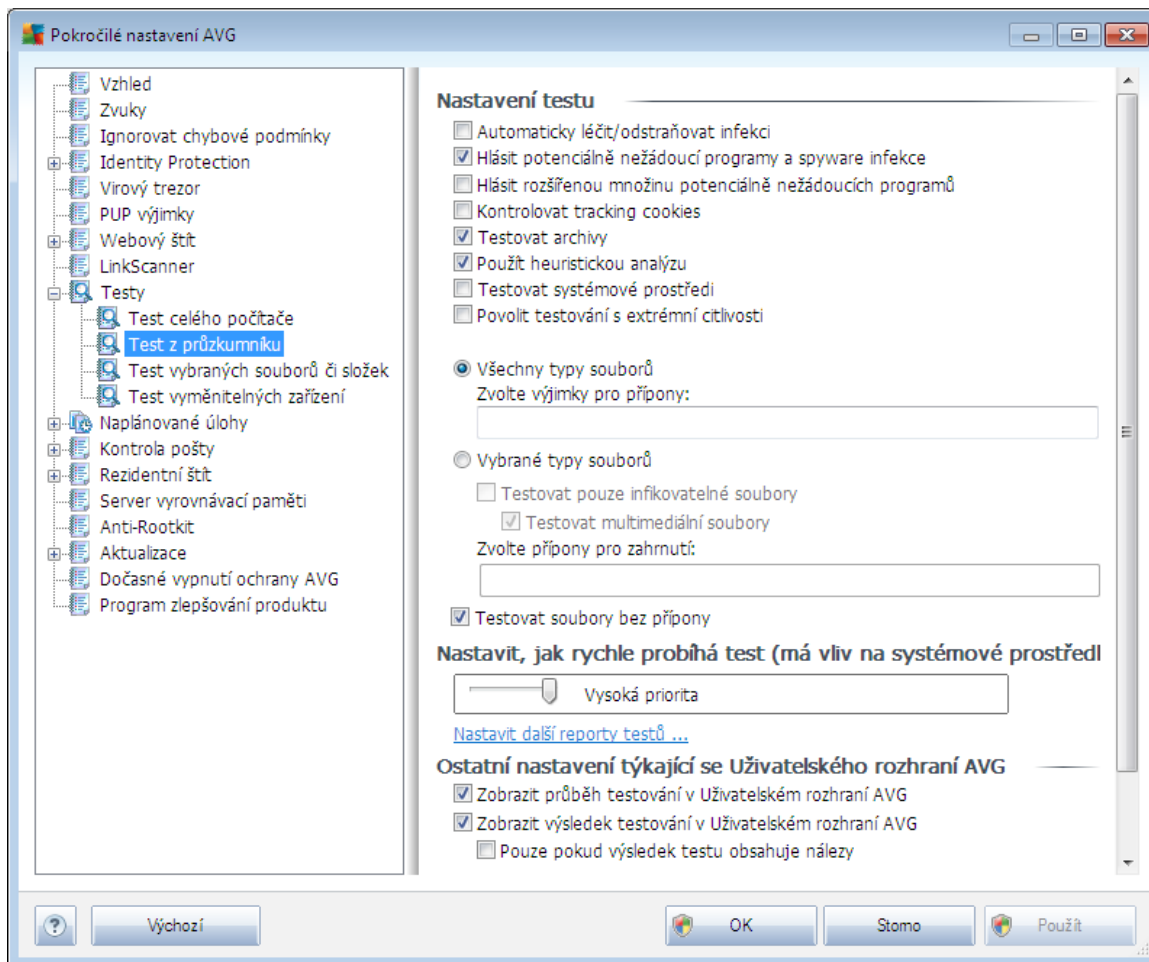
Nastavit další reporty testů ...

Kliknutím na odkaz **Nastavit další reporty testů ...** otevřete samostatné dialogové okno **Reporty testů**, v němž můžete označením příslušných položek určit situace, jejichž výskyt během testu má být hlášen:



9.8.2. Test z průzkumníku

Podobně jako předchozí položka [Test celého počítače](#) nabízí i tato položka, **Test z průzkumníku**, možnost editovat parametry výrobcem nastaveného testu. Konfigurace se tentokrát vztahuje k [testu spuštěným nad konkrétními objekty pomocí průzkumníku Windows](#) (Test z průzkumníku), viz kapitola [Testování v průzkumníku Windows](#).



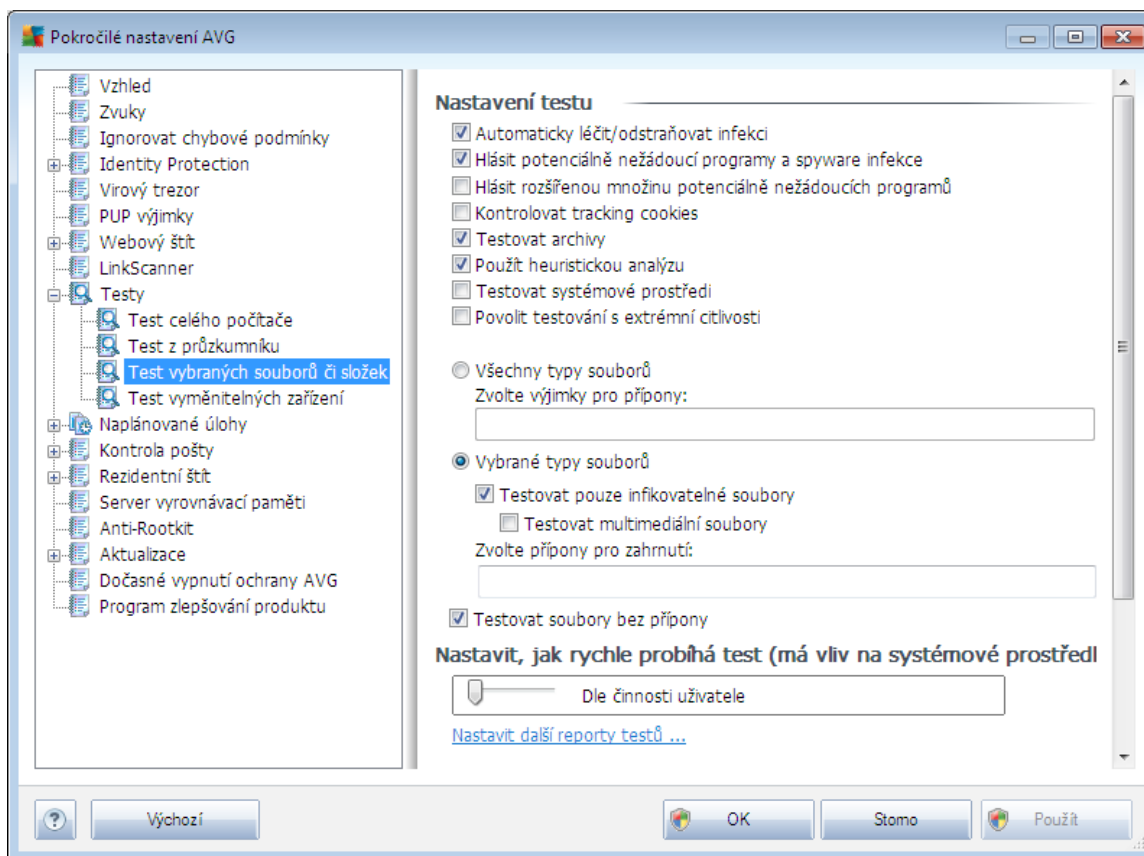
Veškeré možnosti editace parametrů testu jsou totožné s [editací parametrů Testu celého počítače](#). Odlišné je pouze výchozí nastavení těchto parametrů (například Test celého počítače ve výchozím nastavení neprovádí kontrolu archivů, ale provádí kontrolu systémového prostředí, zatímco u Testu z průzkumníku je tomu naopak).

Poznámka: Podrobný popis jednotlivých parametrů najdete v kapitole [Pokročilé nastavení AVG / Testy / Test celého počítače](#).

V dialogu [Test z průzkumníku](#) je proti [Testu celého počítače](#) navíc zahrnuta sekce **Ostatní nastavení týkající se Uživatelského rozhraní AVG**, kde máte možnost označit, zda si přejete, aby průběh testování z průzkumníku a jeho výsledek byly znázorněny v uživatelském rozhraní a odtud dostupné. Máte rovněž možnost určit, že výsledek má být zobrazen pouze v případě, že by během testu byla detekována infekce.

9.8.3. Test vybraných souborů či složek

Editace parametrů [Testu vybraných souborů či složek](#) je prakticky identická s editací parametrů [Testu celého počítače](#). Možnosti konfigurace jsou totožné, liší se pouze výchozím nastavením, které je pro [Test celého počítače](#) nastaveno striktněji:

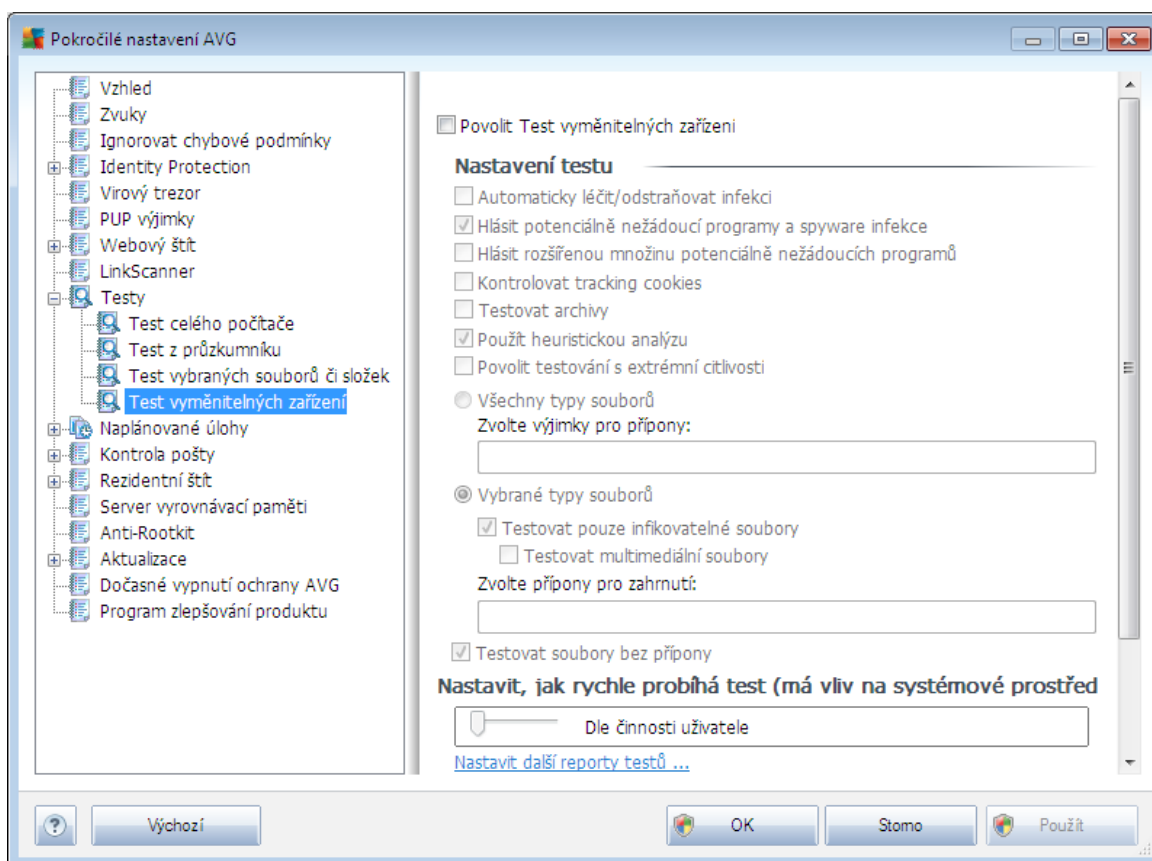


Veškeré parametry nastavené v tomto konfiguračním dialogu se vztahují pouze na ty oblasti vašeho počítače, které jste vybrali pro testování v rámci **Testu vybraných souborů či složek!**

Poznámka: Popis jednotlivých parametrů tohoto dialogu najdete v kapitole **Pokročilé nastavení / Testy / Test celého počítače.**

9.8.4. Test vyměnitelných zařízení

Editace rozhraní *Testu vyměnitelných zařízení* je také velmi podobné rozhraní [Testu celého počítače](#):



Test vyměnitelných zařízení se spouští automaticky bezprostředně po zapojení vyměnitelného zařízení k vašemu počítači. Ve výchozím nastavení je toto testování vypnuto. Testování vyměnitelných zařízení je však nanejvýš vhodné, protože právě tato média jsou významným zdrojem infekce. Chcete-li tedy využít možnosti tohoto testu, označte položku **Povolit Test vyměnitelných zařízení**.

Poznámka: Popis jednotlivých parametrů tohoto dialogu najdete v kapitole [Pokročilé nastavení / Testy / Test celého počítače](#).

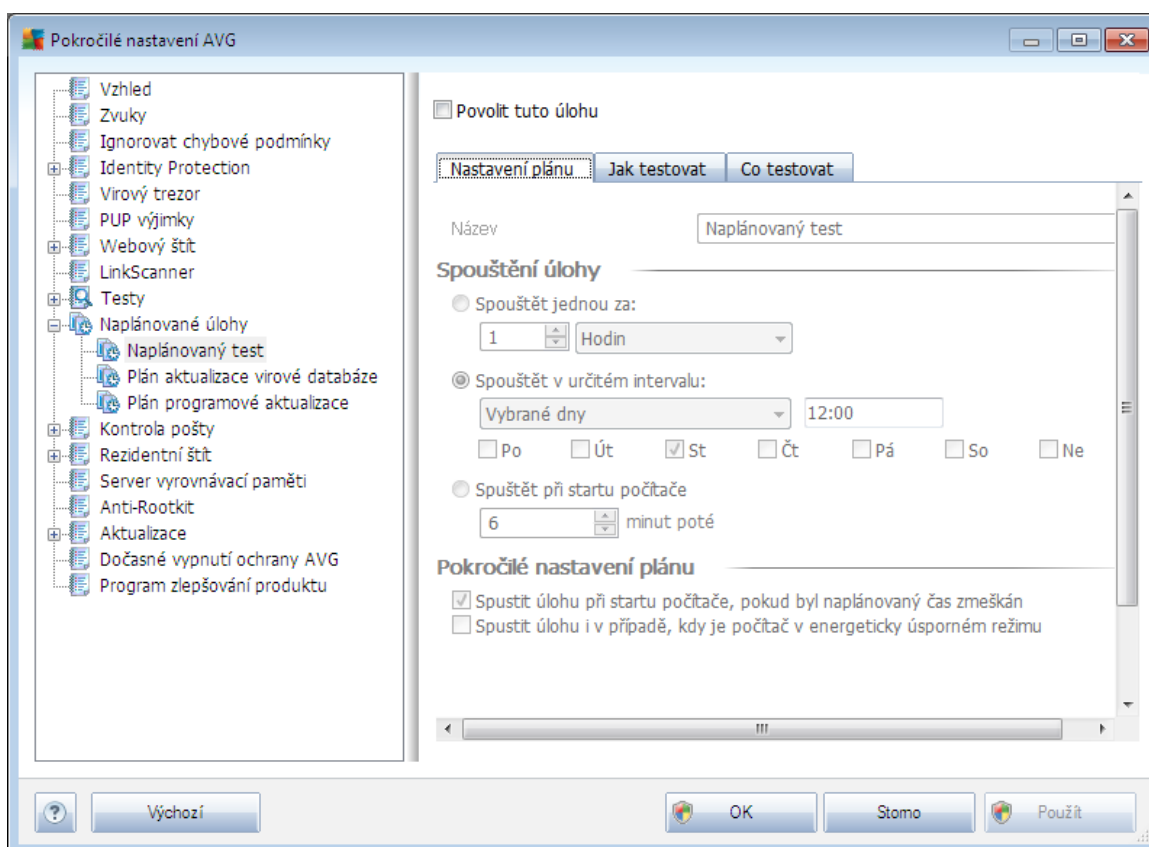
9.9. Naplánované úlohy

V sekci **Naplánované úlohy** máte možnost editace výchozího nastavení

- [Naplánovaný test](#)
- [Plánu aktualizace virové databáze](#)
- [Plánu programové aktualizace](#)

9.9.1. Naplánovaný test

Parametry naplánovaného testu můžete editovat (případně nastavit plán nový) na těchto záložkách. Na každé záložce máte nejprve možnost jednoduchým označením položky **Povolit tuto úlohu** naplánovaný test (dole) deaktivovat, a později podle potřeby znovu použít.



V textovém poli **Název** (toto pole je u všech předem nastavených plánů deaktivováno) je uvedeno jméno příslušného nastaveného testu. U nově vytvářených plánů (nový plán vytvoříte tak, že kliknete pravým tlačítkem myši nad položkou **Naplánovaný test** v levém navigačním menu) bude textové pole aktivní a dostanete možnost definovat své vlastní pojmenování plánu. Snažte se vždy používat stručné, popisné a případně názvy, abyste se později v naplánovaných úlohách snadno vyznali.

Příklad: Nevhodným názvem testu je například "Nový test" nebo "Martin v test", protože ani jeden název nevypovídá o tom, co test ve skutečnosti kontroluje. Naproti tomu správným popisným názvem testu může být například "Test systémových oblastí" nebo "Test disku C:" a podobně. Rovněž není nutné označovat testy termíny Test celého počítače versus Test vybraných souborů a složek - váš nastavený test bude vždy specifickým nastavením testu vybraných souborů a složek.

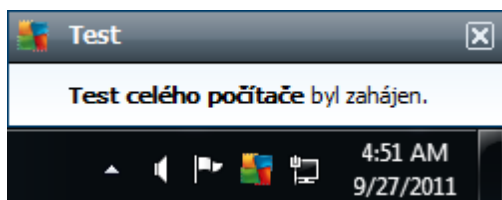
Spouštění úloh



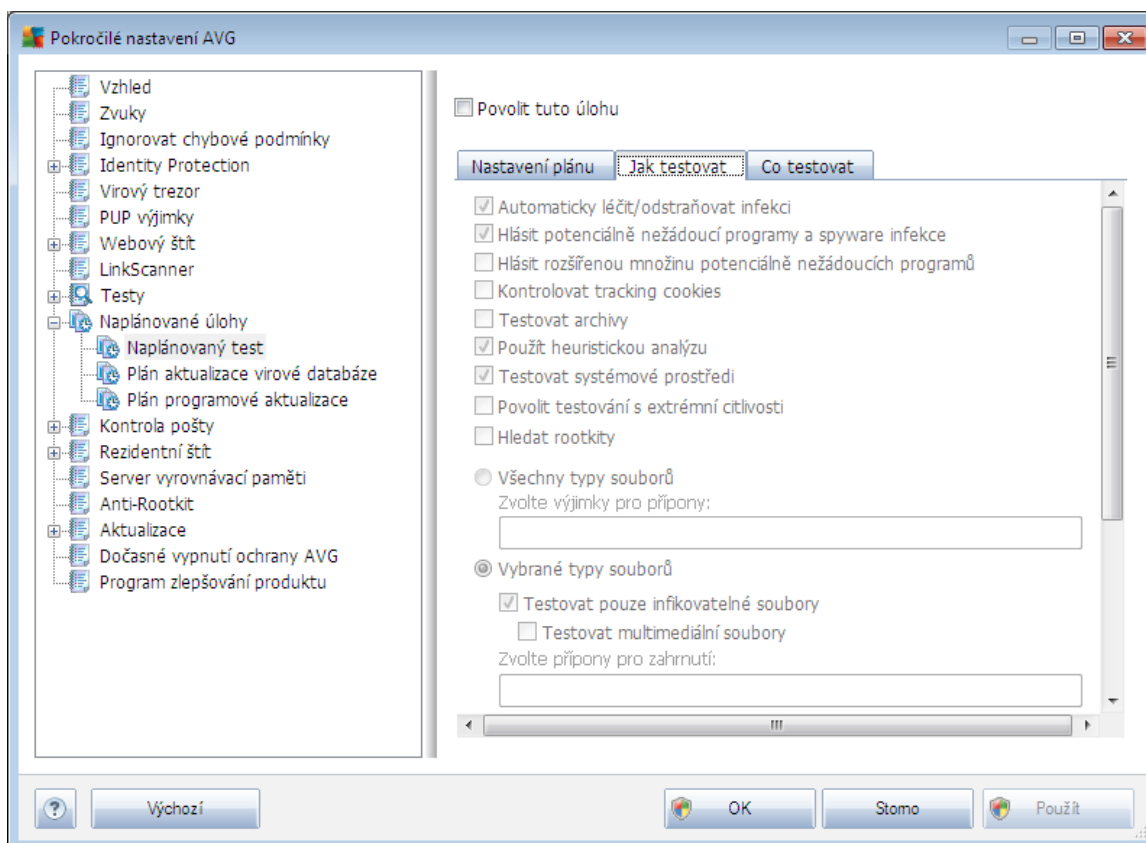
V dialogu můžete dále definovat, v jakých časových intervalech má být nově naplánovaný test spuštěn. Časové určení můžete zadat buďto opakovaným spuštěním testu po uplynutí určité doby (**Spouštět jednou za**) nebo stanovením přesného data a času (**Spouštět v určitém**), případně určit události, na niž se spuštění testu váže (**Spouštět při spuštění počítače**).

Pokročilé nastavení plánu

Tato sekce umožňuje definovat podmínky, kdy má být test spuštěn, jestliže je počítač v úsporném režimu nebo zcela vypnutý a naplánovaný test spuštění testu byl zmeškán. O automatickém spuštění testu budete v určeném čase informováni prostřednictvím pop-up okna nad [ikonou AVG na systémové liště](#):



Po zahájení testu se na systémové liště objeví [nová ikona AVG](#) (barevná s problikávajícím světlem), která vás informuje o běžícím testu. Kliknutím pravého tlačítka myši nad touto ikonou otevřete kontextové menu, z něhož můžete běžící test pozastavit nebo ukončit, a rovněž změnit prioritu právě probíhajícího testu.



Záložka **Jak testovat** nabízí seznam parametrů testu, které můžete podle potřeby vypínat/zapínat. Ve výchozím nastavení je většina parametrů zapnuta a budou tak během testu automaticky použity. Pokud nemáte skutečný důvod konfiguraci testu změnit, doporučujeme se držet výrobcem definovaného nastavení:

- **Automaticky léčit/odstraňovat infekci** (ve výchozím nastavení zapnuto): je-li během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. Pokud virus automaticky léčit nelze, bude infikovaný objekt automaticky přesunut do [Virového trezoru](#);
- **Hlásit potenciálně nežádoucí programy a spyware infekce** (ve výchozím nastavení zapnuto): kontrola přítomnosti [potenciálně nežádoucích programů](#) (spustitelné programy, které mohou fungovat jako spyware nebo adware). Zaškrtnutím tohoto políčka aktivujete [Anti-Spyware](#), tj. bude se testovat přítomnost spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány v domě a se souhlasem uživatele. Doporučujeme nicméně ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
- **Hlásit rozšířenou množinu potenciálně nežádoucích programů** (ve výchozím nastavení vypnuto): zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje



zabezpečení vašeho počítače na další úrovni, nicméně můžete také nastavit, které legální programy, proto je ve výchozím nastavení tato možnost vypnuta.

- **Kontrolovat tracking cookies** (ve výchozím nastavení vypnuto): parametr komponenty [Anti-Spyware](#) definuje, že během testu mají být detekovány cookies (*HTTP data zaslaná serverem prohlížeči a uložena na počítači uživatele; při každé další návštěvě téhož serveru prohlížeč posílá cookies zpět serveru, který podle nich rozlišuje jednotlivé uživatele*);
- **Testovat archivy** (ve výchozím nastavení vypnuto): parametr definuje, že test má kontrolovat všechny soubory, a to i takové, které jsou zabaleny v nějakém typu archivu, například ZIP, RAR, ...
- **Použít heuristickou analýzu** (ve výchozím nastavení zapnuto): během testu bude použita k detekci infekce i metoda heuristické analýzy (*dynamické emulace instrukcí testovaného objektu v prostředí virtuálního počítače*);
- **Testovat systémové prostředí** (ve výchozím nastavení zapnuto): test prověří i systémové oblasti vašeho počítače;
- **Povolit testování s extrémní citlivostí** (ve výchozím nastavení vypnuto) - ve specifických situacích (například při podezření na infekci starším typem viru) můžete zvolit tuto metodu testování, která aktivuje nejdokladnější testovací algoritmy a velmi podrobně prověří naprosto všechny oblasti vašeho počítače. Mějte však na paměti, že tato metoda je časově velmi náročná.
- **Hledat rootkity** (ve výchozím nastavení vypnuto): označením této položky zahrnete do testu i možnost detekce rootkitu, která je jinak samostatně dostupná v rámci komponenty [Anti-Rootkit](#);

Dále se můžete rozhodnout, zda si přejete testovat

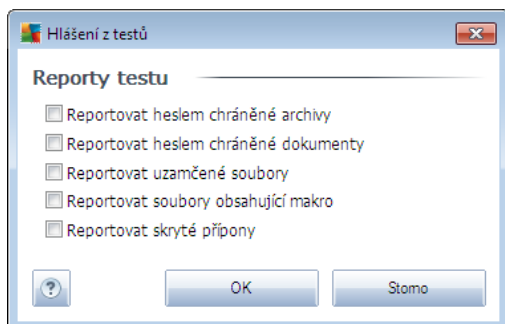
- **Všechny typy souborů** - pokud máte zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou (*po uložení se čárky změní na středníky*);
- **Vybrané typy souborů** - můžete se rozhodnout, že chcete, aby se testy spouštěly pouze nad soubory, které lze považovat za infikovatelné (*soubory, které nemohou být infekcí zasaženy, se testovat nebudou - například prosté textové soubory nebo některé nespustitelné soubory*), a to včetně multimediálních souborů (*video, audio soubory - ponecháte-li tuto položku neoznačenou, výrazně se tím zkrátí čas testování, jelikož multimediální soubory jsou obvykle poměrně velké, ale pravděpodobnost infekce je u nich velmi nízká*). I zde můžete určit výjimky a pomocí seznamu přípon definovat, které soubory mají být testovány za všech okolností.
- U položky **Testovat soubory bez přípon** pak rozhodnete, zda se mají testovat i soubory se skrytou nebo neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme, abyste se tohoto nastavení drželi, pokud nemáte skutečný důvod jej změnit. Soubory bez přípon jsou obecně vysoce podezřelé a měly by být otestovány.

Nastavit, jak rychle probíhá test

V sekci **Priorita testu** pak můžete nastavit požadovanou rychlost testování v závislosti na zátěži systémových zdrojů. Ve výchozím nastavení je tato hodnota nastavena *dle intenzity užívání počítače*. Pokud se rozhodnete pro spuštění rychlého testu, proběhne test v kratším čase, ale po dobu jeho běhu bude výrazně zvýšena zátěž systémových zdrojů, takže vaše práce na počítači bude obtížnější (*tato varianta je vhodná pro situace, kdy je počítač spuštěn, ale nikdo na něm aktuálně nepracuje*). Naopak, prodloužením doby testu snížíte zátěž systémových zdrojů a vaše práce na počítači nebude téměř ovlivněna, test však bude probíhat po delší dobu.

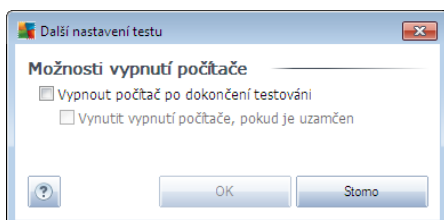
Nastavit další reporty testu

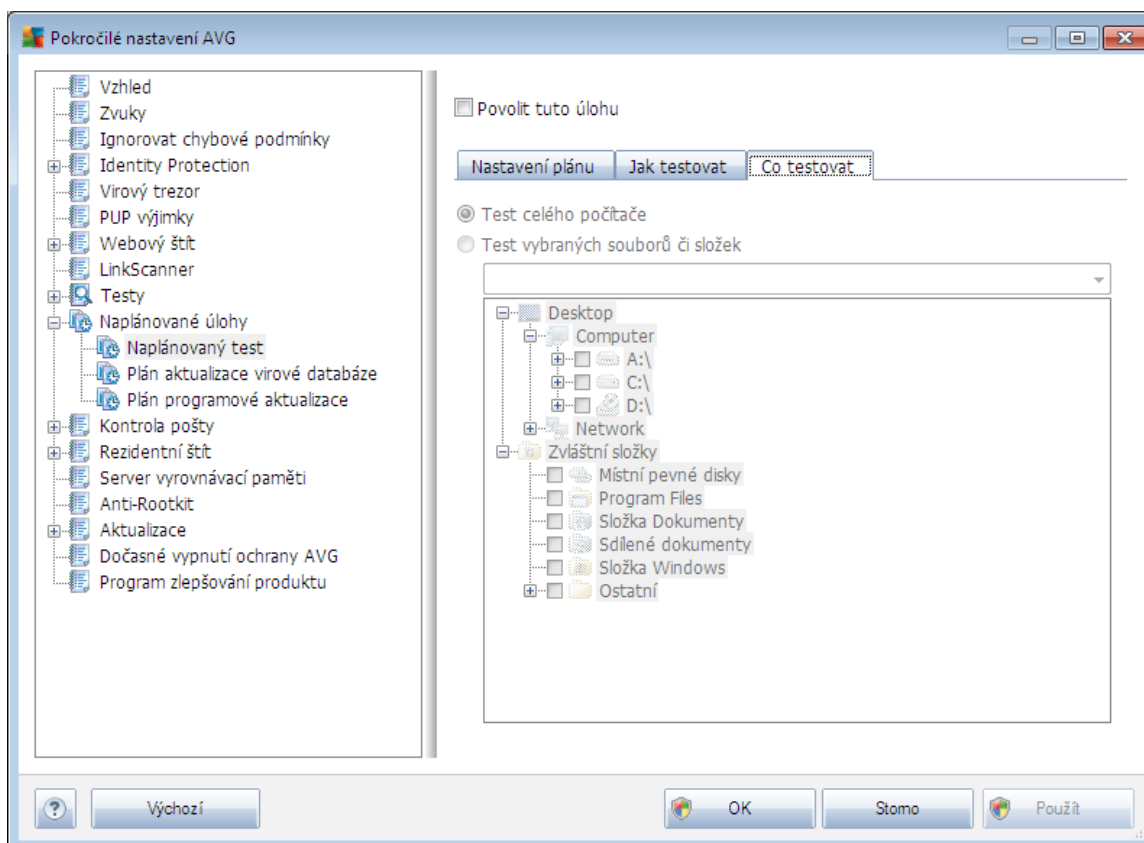
Kliknutím na odkaz **Nastavit další reporty testu ...** otevřete samostatné dialogové okno Reporty testu, v němž můžete označit situace, jejichž výskyt během testu má být hlášen:



Další nastavení testu

Kliknutím na odkaz **Další nastavení testu ...** otevřete nový dialog **Možnosti vypnutí počítače**, v němž můžete zvolit, zda má být po dokončení spuštěného testu počítač automaticky vypnut. Pokud potvrdíte tuto volbu (**Vypnout počítač po dokončení testování**), aktivuje se současně další možnost, jejímž zapnutím vynutíte vypnutí počítače i za situace, že počítač bude ve chvíli dokončení testu zamčen (**Vynutit vypnutí počítače, pokud je uzamčen**).

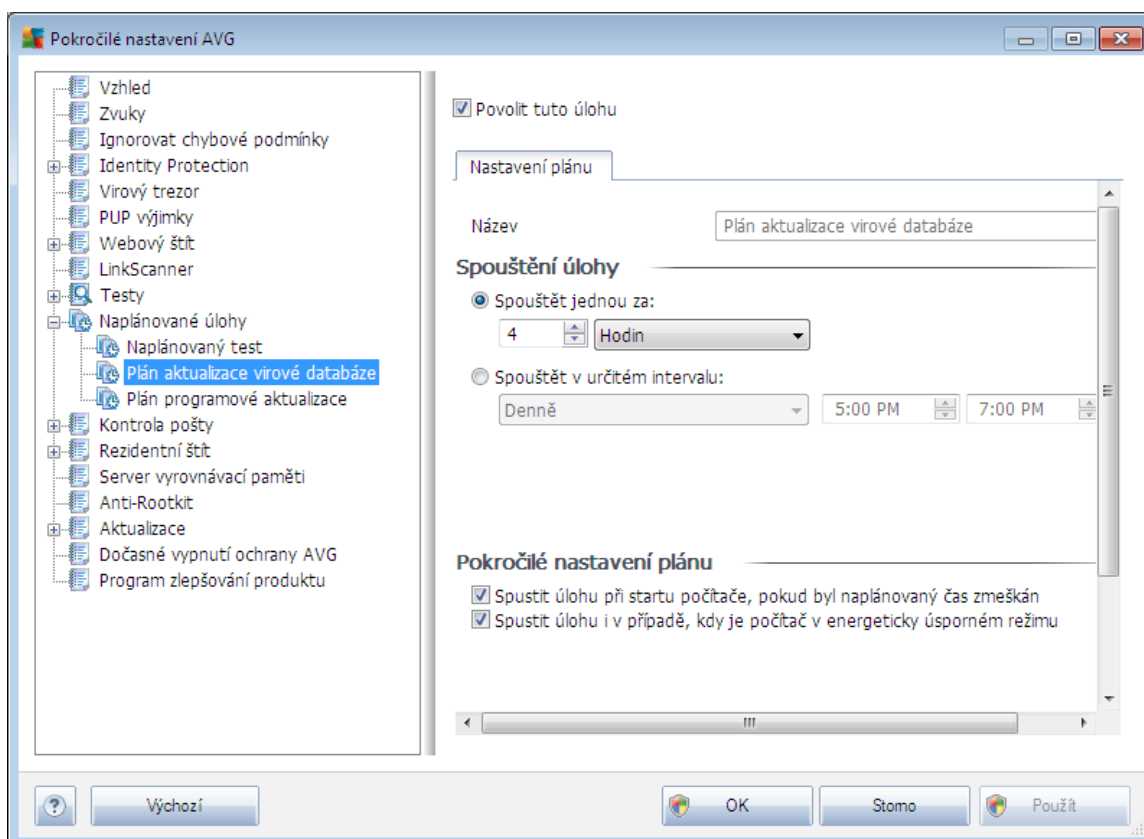




Na záložce **Co testovat** definujete, zda si přejete naplánovat **Test celého počítače** nebo **Test vybraných souborů či složek**. V případě, že se rozhodnete pro test vybraných souborů a složek, ve spodní části dialogu se aktivuje zobrazená stromová struktura vašeho disku a v ní můžete označit adresáře, jejichž obsah má být testován.

9.9.2. Plán aktualizace virové databáze

V případě **skutečně nutné** byste mohli prostým vypnutím položky **Povolit tuto úlohu** naplánovanou aktualizaci (do asn) deaktivovat, a později ji znovu zapnout:



Základní nastavení plánu aktualizace virové databáze je definováno v rámci komponenty **Manažer aktualizací**. V tomto dialogu můžete nastavit přesnější parametry plánu aktualizace. V textovém poli **Název** (toto pole je u všech předem nastavených plánů deaktivováno) je uvedeno jméno příslušného nastaveného plánu aktualizace.

Spouštění úlohy

Určete, v jakých časových intervalech má být nově naplánovaná aktualizace virové databáze provedena. Časové určení můžete zadat buďto opakovaným spuštěním aktualizace po uplynutí určité doby (**Spouštět jednou za**) nebo stanovením přesného data a času (**Spouštět v určený čas**).

Pokročilé nastavení plánu

Tato sekce umožňuje definovat podmínky, kdy má či nemá být aktualizace virové databáze spuštěna, jestliže je počítač v úsporném režimu nebo zcela vypnutý a naplánovaný čas spuštění aktualizace byl zmeškán.



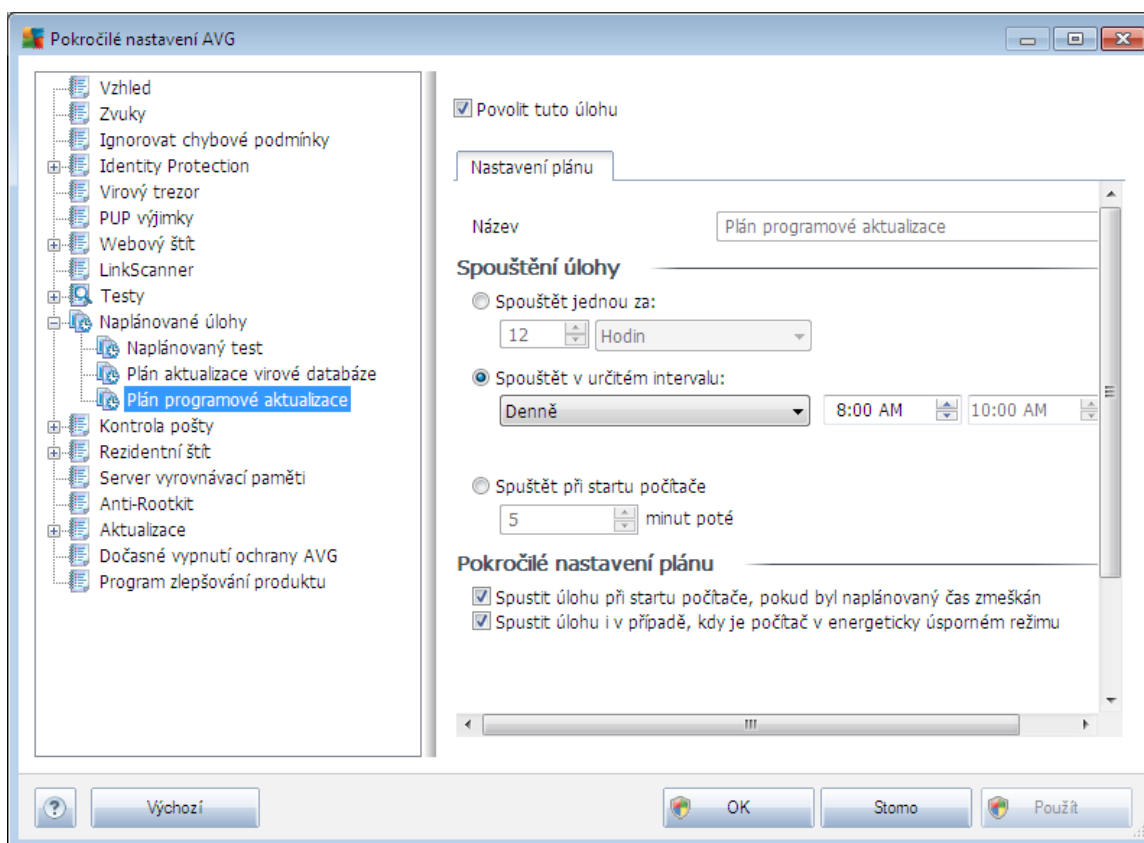
Další nastavení aktualizace

Volbou položky **Provést aktualizaci znovu po p ípojení k Internetu** zajistíte, že pokud dojde b hem aktualizace virové databáze k problém m s p ípojením a aktualizace tedy nebude moci být dokon ena, bude znovu spušt na bezprost edn po obnovení p ípojení.

O automatickém spušt ní aktualizace budete v ur eném ase informováni prost ednictvím pop-up okna nad [ikonou AVG na systémové lišt](#) (za p edpokladu, že ponecháte zapnutou volbu **Zobrazovat oznámení na systémové lišt** v [Pokro ílém nastavení/Vzhled](#)).

9.9.3. Plán programové aktualizace

V p ípad **skute n nutné** pot eby m žete prostým vypnutím položky **Povolit tuto úlohu** naplánovanou programovou aktualizací (do asn) deaktivovat, a pozd ji znovu zapnout:



V textovém poli **Název** (toto pole je u všech p edem nastavených plán deaktivováno) je uvedeno jméno p íazené práv nastavenému plánu programové aktualizace.

Spoušt ní úlohy

Ur ete, v jakých asových intervalech má být nov naplánovaná programové aktualizace provedena. asové ur ení m žete zadat bu to opakovaným spušt ní m aktualizace po uplynutí ur ené doby (



Spouštět jednou za) nebo stanovením přesného data a času (**Spouštět v určený čas**), případně určením události, na niž se spuštění aktualizace váže (**Spouštět při spuštění počítače**).

Pokročilé nastavení plánu

Tato sekce umožňuje definovat podmínky, kdy má či nemá být programové aktualizace spuštěna, jestliže je počítač v úsporném režimu nebo zcela vypnutý a naplánovaný čas spuštění aktualizace byl zmeškán.

Další nastavení aktualizace

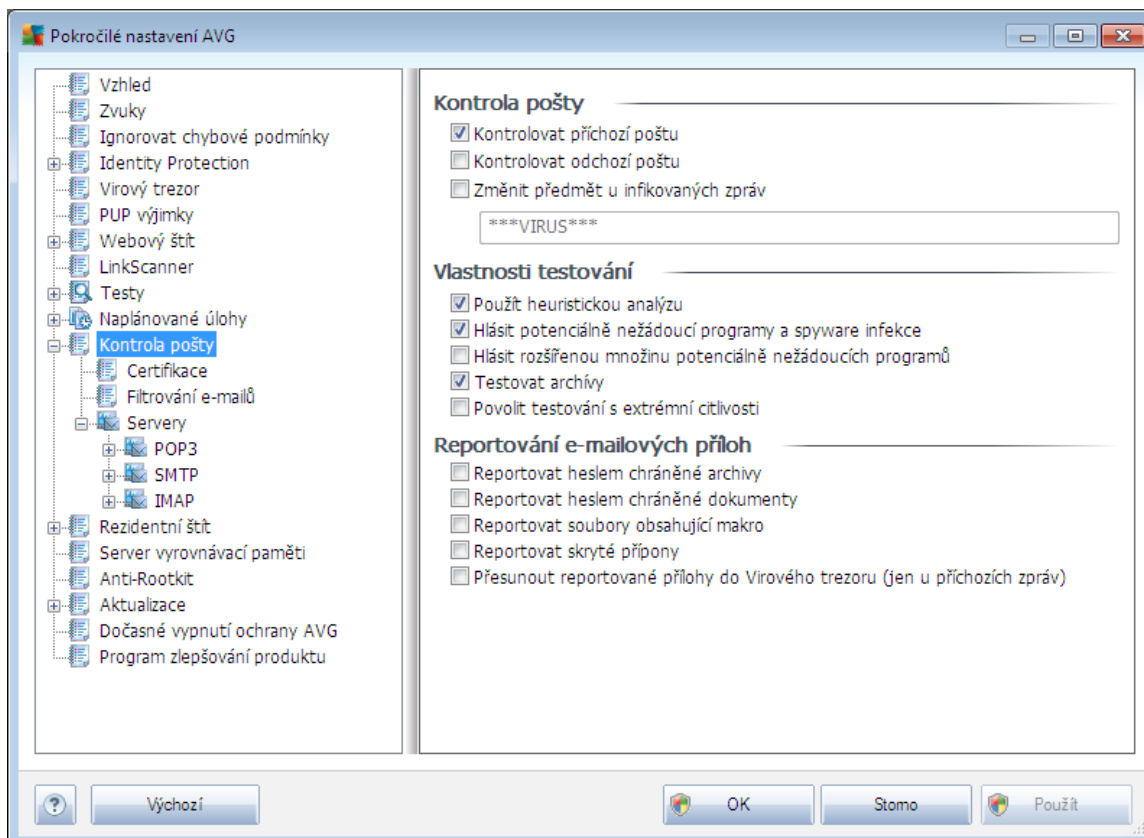
Volbou položky **Provést aktualizaci znovu po připojení k Internetu** zajistíte, že pokud dojde během programové aktualizace k problémům s připojením a aktualizace tedy nebude moci být dokončena, bude znovu spuštěna bezprostředně po obnovení připojení.

O automatickém spuštění aktualizace budete v určeném čase informováni prostřednictvím pop-up okna nad [ikonou AVG na systémové liště](#) (za předpokladu, že ponecháte zapnutou volbu **Zobrazovat oznámení na systémové liště** v [Pokročilém nastavení/Vzhled](#)).

Poznámka: Dojde-li k časovému souhrnu naplánované programové aktualizace a naplánovaného testu, proces aktualizace je považován za prioritní a test bude přerušeno.

9.10. Kontrola pošty

Dialog **Kontrola pošty** je rozdelen do tří sekcí:



Kontrola pošty

v této sekci jsou dostupná základní nastavení pro příchozí a odchozí poštu:

- **Kontrolovat příchozí poštu** (ve výchozím nastavení zapnuto) - označením zapnete/vypnete možnost testování všech příchozích e-mail
- **Kontrolovat odchozí poštu** (ve výchozím nastavení vypnuto) - označením zapnete/vypnete možnost testování všech e-mail odesílaných z vašeho útu
- **Změnit předmět u infikovaných zpráv** (ve výchozím nastavení vypnuto) - pokud si přejete být upozorněn, že otestovaná zpráva byla vyhodnocena jako infikovaná, můžete aktivovat tuto položku a do textového pole vepsat požadované označení takovéto e-mailové zprávy. Tento text pak bude přidán do pole "Předmět" u každé pozitivně detekované zprávy (slouží ke snadnější identifikaci a filtrování). Výchozí hodnota je *****VIRUS***** a doporučujeme ji ponechat.

Vlastnosti testování



V této sekci můžete určit, jak přesně e-maily testovat:

- **Použít heuristickou analýzu** (ve výchozím nastavení zapnuto) - použít heuristiku při testování e-mailů. Když je tato možnost aktivována, můžete filtrovat přilohy e-mailů nejen podle přípony, ale i podle skutečného obsahu a formátu (který příponou nemusí odpovídat). Filtrování lze nastavit v dialogu [Filtrování e-mailů](#).
- **Hlásit potenciálně nežádoucí programy a spyware infekce** (ve výchozím nastavení zapnuto) - kontrola přítomnosti [potenciálně nežádoucích programů](#) (spustitelné programy, které mohou fungovat jako spyware nebo adware). Zaškrtnutím tohoto políčka aktivujete [Anti-Spyware](#), tj. bude se testovat přítomnost spyware, nejen virů. Spyware představuje problém kvůli problematické kategorii hrozeb, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány v domě a se souhlasem uživatele. Doporučujeme nicméně ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
- **Hlásit rozšířenou množinu potenciálně nežádoucích programů** (ve výchozím nastavení vypnuto) - zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně můžete blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.
- **Testovat archivy** (ve výchozím nastavení zapnuto) - testovat obsah archivů v přílohách zpráv.
- **Povolit testování s extrémní citlivostí** (ve výchozím nastavení vypnuto) - ve specifických situacích (například při podezření na infekci starším typem viru) můžete zvolit tuto metodu testování, která aktivuje nejdokladnější testovací algoritmy a velmi podrobně prohledá naprosto všechny oblasti vašeho počítače. Mějte však na paměti, že tato metoda je časově velmi náročná.

Reportování e-mailových příloh

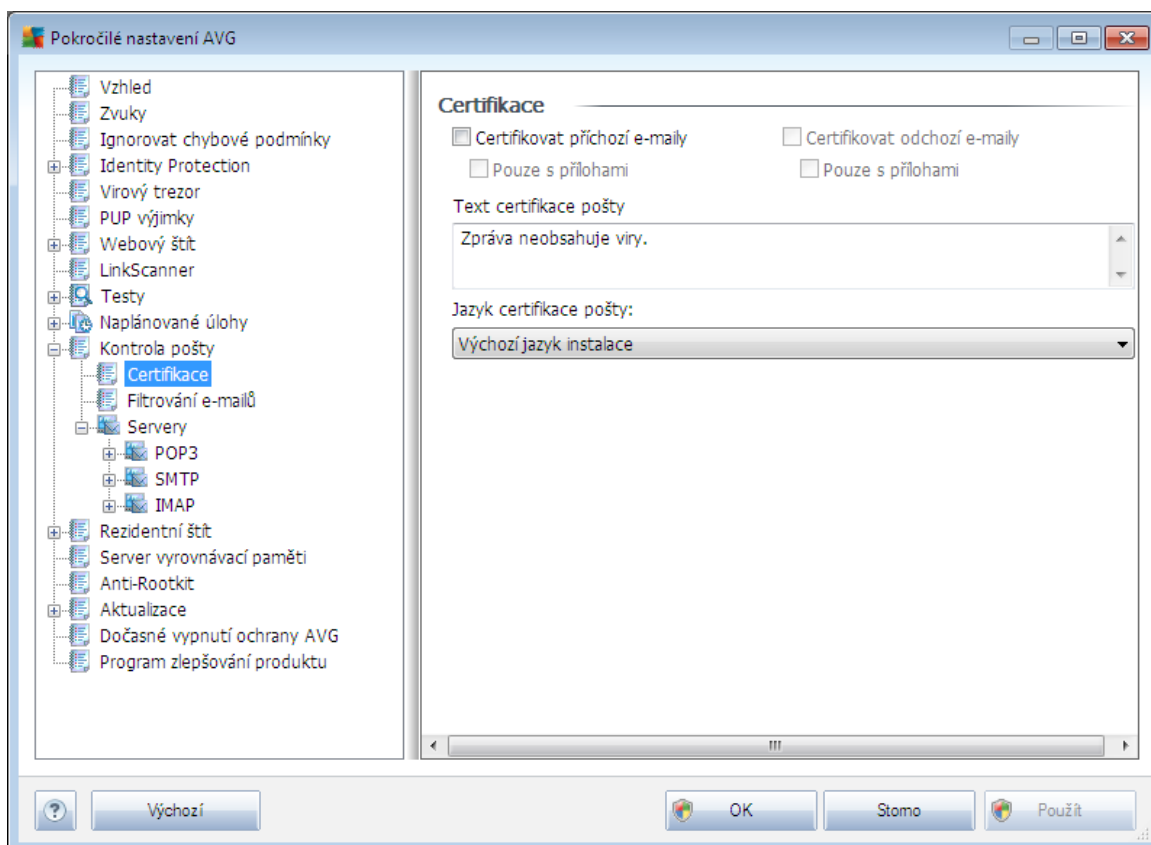
V této sekci lze nastavit reportování potenciálně nežádoucích nebo podezřelých souborů. Prosím pozor, v případě detekce takového souboru nebude zobrazen žádný dialog s varováním, e-mail bude pouze označen certifikačním textem a nález bude zaznamenán do dialogu [Nálezy Kontroly pošty](#).

- **Reportovat heslem chráněné archivy** – archivy (ZIP, RAR atd.) chráněné heslem není možné otestovat na přítomnost virů; po zaškrtnutí tohoto políčka se tyto archivy budou označovat jako potenciálně nebezpečné.
- **Reportovat heslem chráněné dokumenty** – dokumenty chráněné heslem není možné otestovat na přítomnost virů; po zaškrtnutí tohoto políčka se tyto archivy budou označovat jako potenciálně nebezpečné.
- **Reportovat soubory obsahující makro** – makro je napevno určený sled kroků, který usnadňuje uživateli často opakované složitější úkoly (makra ve Wordu jsou typickým příkladem). Makro může obsahovat různé instrukce, a to i potenciálně nebezpečné; chcete-li reportovat všechny dokumenty s makry, označte toto políčko.

- **Reportovat skryté přípony** – skryté přípony mohou podezřelý spustitelný soubor "n co.txt.exe" zamaskovat tak, aby se uživateli jevil jen jako neškodný textový soubor "n co.txt"; po zakškrtnutí tohoto políčka budou soubory se skrytými příponami reportovány jako potenciálně nebezpečné.
- Zaškrtnutím políčka **Přesunout reportované přílohy do Virového trezoru** určíte, že všechny výše vybrané soubory z příloh e-mailů se mají nejen reportovat, ale rovněž automaticky přesouvat do [Virového trezoru](#).

9.10.1. Certifikace

V dialogu **Certifikace** můžete nastavit text a jazyk certifikace pro příchozí poštu a odchozí poštu:



Certifikační text sestává ze dvou částí, uživatelské a systémové, jak si ukážeme na příkladu - v následujícím textu je první řádek uživatelskou částí, zbytek se generuje automaticky:

Zpráva neobsahuje viry.

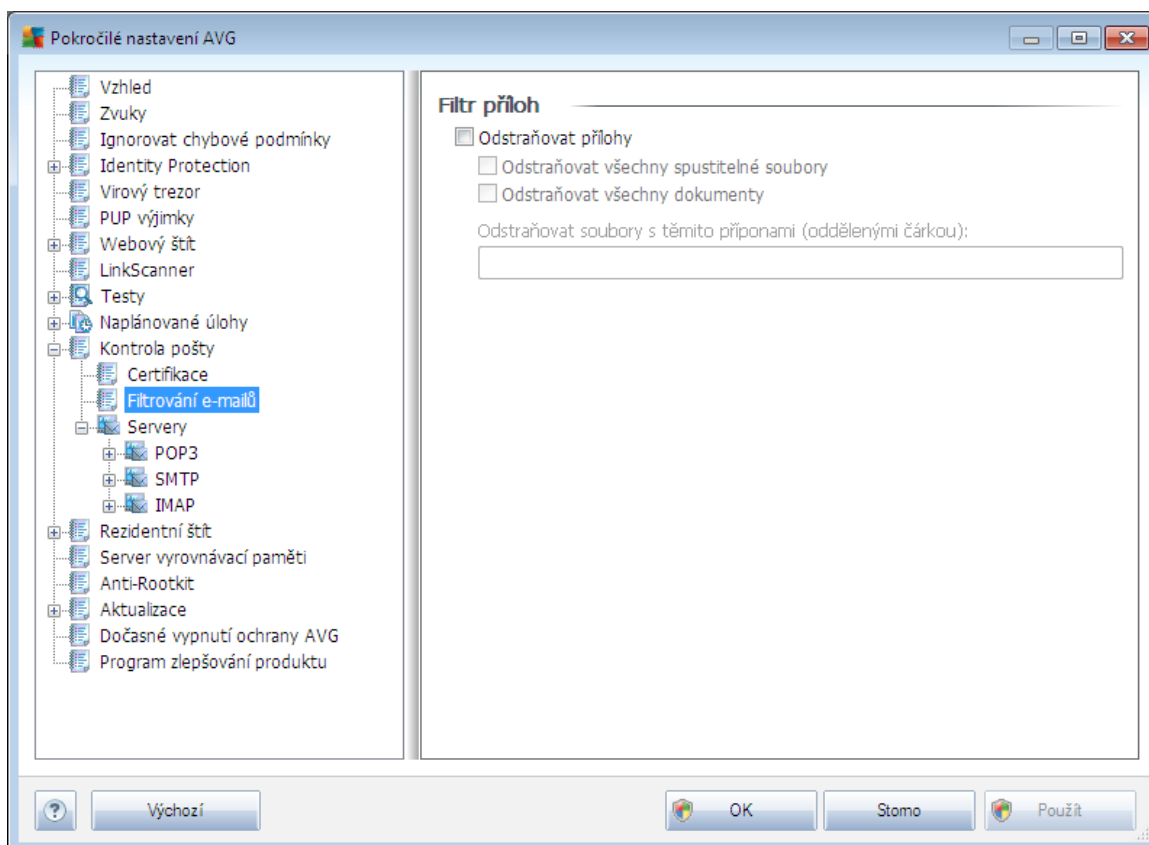
Zkontrolováno systémem AVG.

Verze: x.y.zz / Virová databáze: xx.y.z - Release Date: 12/9/2010

Pokud se rozhodnete povolit certifikaci e-mailů v příchozí nebo odchozí poště, můžete v tomto dialogu nastavit přesné znění uživatelské části certifikačního textu (**Text certifikace pošty**) a zvolit, v

jakém jazyce se má zobrazovat automaticky generovaná část certifikace (**Jazyk certifikace pošty**).

9.10.2. Filtrování e-mailů

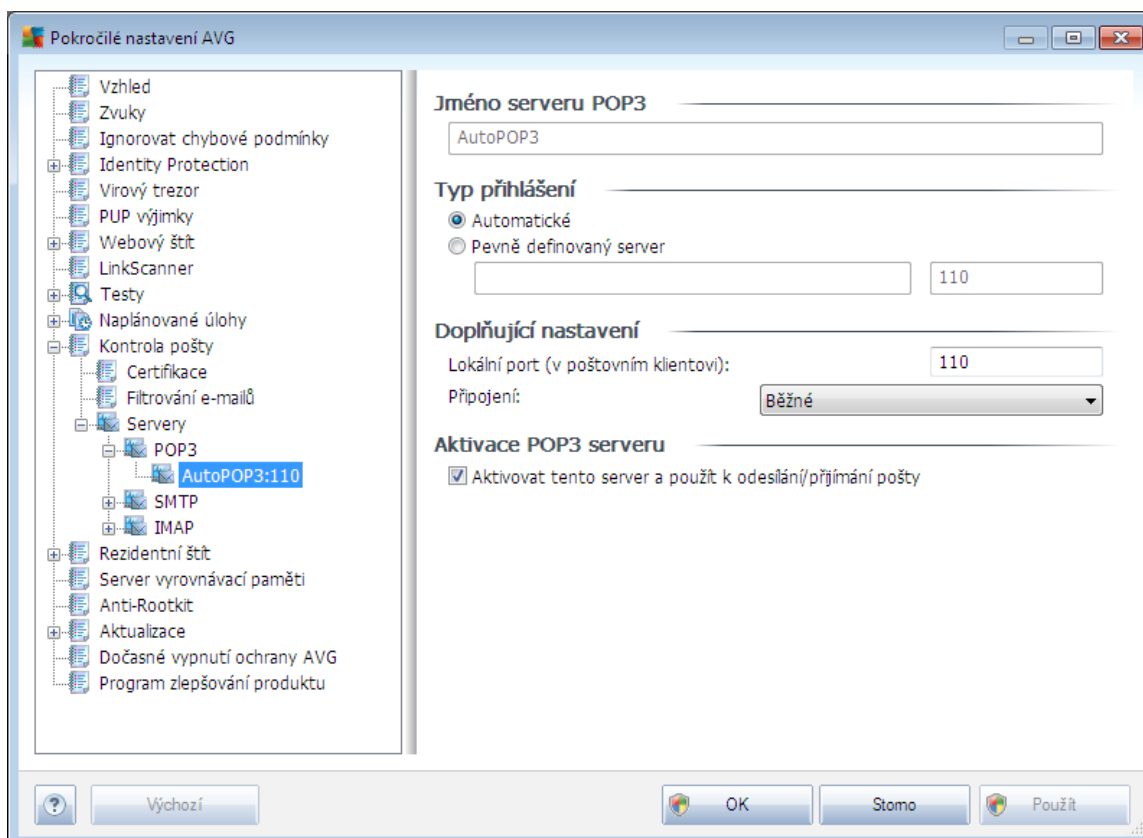


Dialog **Filtr příloh** umožňuje nastavení parametrů pro testování příloh e-mailových zpráv. Ve výchozím nastavení je možnost **Odstraňovat přílohy** vypnuta. Pokud se rozhodnete pro její aktivaci, budou automaticky odstraněny všechny přílohy zpráv, které byly detekovány jako infikované nebo potenciálně nebezpečné. Chcete-li blíže určit, které typy příloh mají být v případě pozitivní detekce odstraněny, označte příslušnou volbu:

- **Odstraňovat všechny spustitelné soubory** - odstraněny budou všechny přílohy s příponou *.exe
- **Odstraňovat všechny dokumenty** - odstraněny budou všechny přílohy s příponou *.doc, *.docx, *.xls, *.xlsx
- **Odstraňovat soubory s těmito příponami** - odstraněny budou všechny přílohy s příponami, které sami definujete

9.10.3. Servery

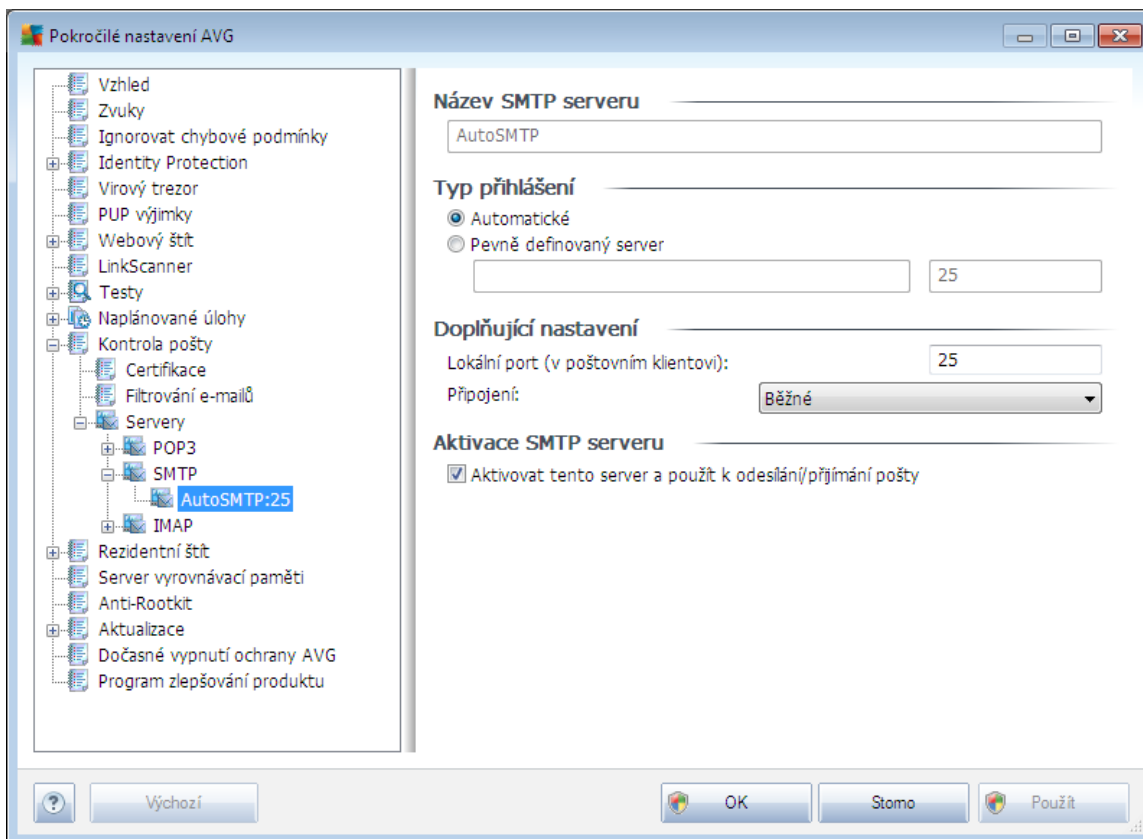
V sekci **Servery** můžete editovat parametry serverů komponenty **Kontrola pošty**, případně nastavit nový server příchozí i odchozí pošty - tlačítko **Přidat nový server**.



V tomto dialogu (odkaz **Servery / POP3**) nastavujete server **Kontroly pošty** s protokolem POP3 pro p íchozí poštu:

- **Jméno serveru POP3** - v tomto poli m žete zadat jméno nov p idaných server (server POP3 p idáte tak, že kliknete pravým tla ítkem myši nad položkou POP3 v levém naviga ním menu). U automaticky vytvo eného serveru "AutoPOP3" je toto pole deaktivováno.
- **Typ p íhlášení** - definuje, jak má být ur en poštovní server, ze kterého bude p íjímána pošta
 - **Automatické** - cílový server bude ur en podle nastavení ve vaší poštovní aplikaci; není t eba nic dále specifikovat
 - **Pevn definovaný server** - v tomto p ípad bude vždy použit konkrétní server. Je t eba zadat adresu nebo jméno vašeho poštovního serveru. P íhlašovací jméno pak z stane beze zm ny. Jako jméno je možné použít jak doménový název (nap íklad *pop.acme.com*), tak IP adresu (nap íklad *123.45.67.89*). Pokud poštovní server používá nestandardní port, lze tento port zadat za jméno serveru odd lený dvojte kou (nap . *pop.acme.com:8200*). Standardní port pro POP3 komunikaci je 110.
- **Dopl ůjící nastavení** - specifikuje další detailní parametry:

- **Lokální port** - určuje, na kterém portu lze očekávat komunikaci z poštovní aplikace. Tento port je pak také nutné v poštovní aplikaci zadat jako port pro POP3 komunikaci.
- **Typ připojení** - v této rozbalovací nabídce můžete specifikovat typ připojení (standardní/zabezpečené na vyhrazeném portu/zabezpečené na běžném portu). Pokud zvolíte zabezpečené připojení, budou posílaná data kryptována a nebude možné jejich sledování nikým jiným. I tato funkce může být aktivována pouze v případě, že ji cílový poštovní server podporuje.
- **Aktivace POP3 serveru** - zapnutím/vypnutím položky máte možnost aktivovat i deaktivovat právě nastavený POP3 server

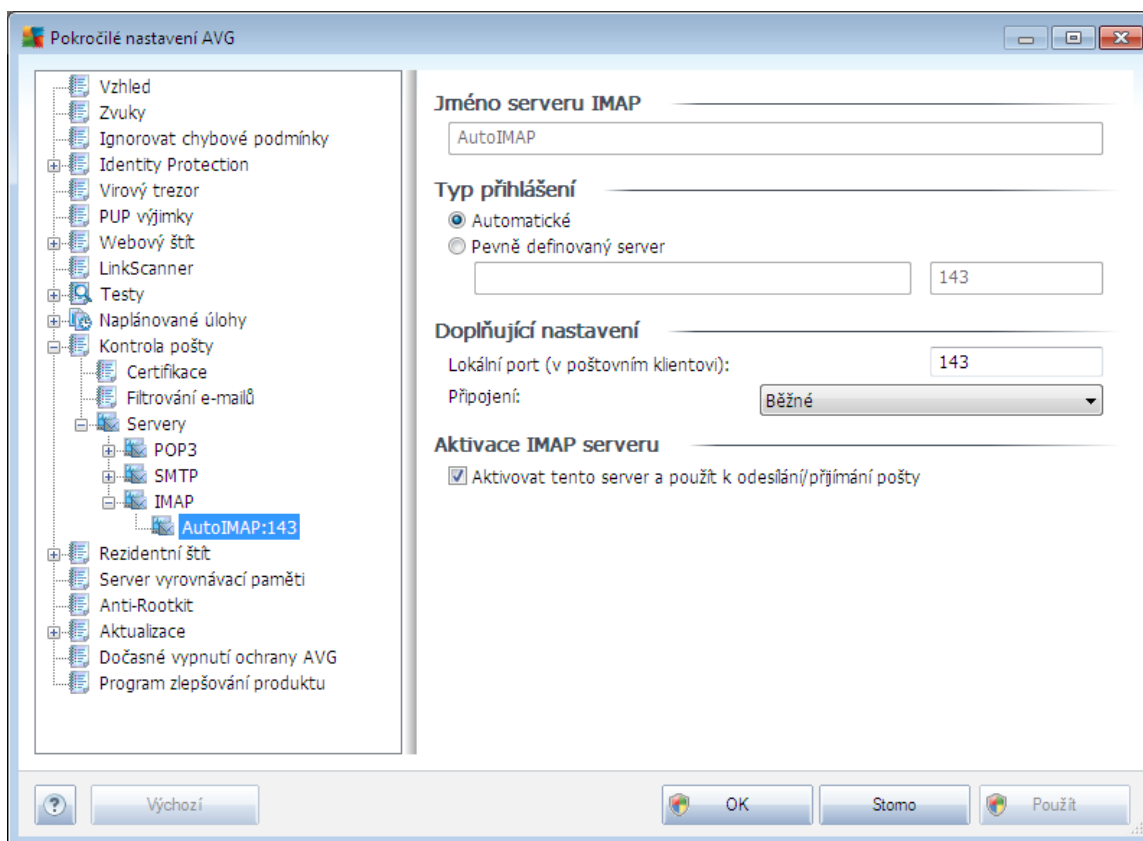


V tomto dialogu (odkaz **Servery / SMTP**) nastavujete server **Kontroly pošty** s protokolem SMTP pro odchozí poštu:

- **Název SMTP serveru** - v tomto poli můžete zadat jméno nově přidaných serverů (server SMTP přidáte tak, že kliknete pravým tlačítkem myši nad položkou SMTP v levém navigačním menu). U automaticky vytvořeného serveru "AutoSMTP" je toto pole deaktivováno.
- **Typ připojení** - definuje, jak má být určen poštovní server, ze kterého bude odesílána pošta:



- **Automatické** - cílový server bude určen podle nastavení ve vaší poštovní aplikaci; není třeba nic dále specifikovat
- **Pevně definovaný server** - v tomto případě bude vždy použit konkrétní server. Do editačního řádku je třeba zadat adresu nebo jméno vašeho poštovního serveru. Jako jméno je možné použít jak doménový název (*nap . smtp.acme.com*), tak i IP adresu (*nap . 123.45.67.89*). Pokud poštovní server používá nestandardní port, lze tento port zadat za jméno serveru oddělený dvojtečkou (*nap . smtp.acme.com:8200*). Standardní port pro SMTP komunikaci je 25.
- **Doplňující nastavení** - specifikuje další detailní parametry:
 - **Lokální port** - určuje, na kterém portu lze očekávat komunikaci z poštovní aplikace. Tento port je pak také nutné v poštovní aplikaci zadat jako port pro SMTP komunikaci.
 - **Připojení** - v této rozbalovací nabídce můžete specifikovat typ připojení (*standardní/zabezpečené na vyhrazeném portu/zabezpečené na běžném portu*). Pokud zvolíte zabezpečené připojení, budou posílaná data kryptována a nebude možné jejich sledování nikým jiným. Tato funkce může být aktivována pouze v případě, že ji cílový poštovní server podporuje.
- **Aktivace SMTP serveru** - zapnutím/vypnutím položky máte možnost aktivovat či deaktivovat právě nastavený SMTP server



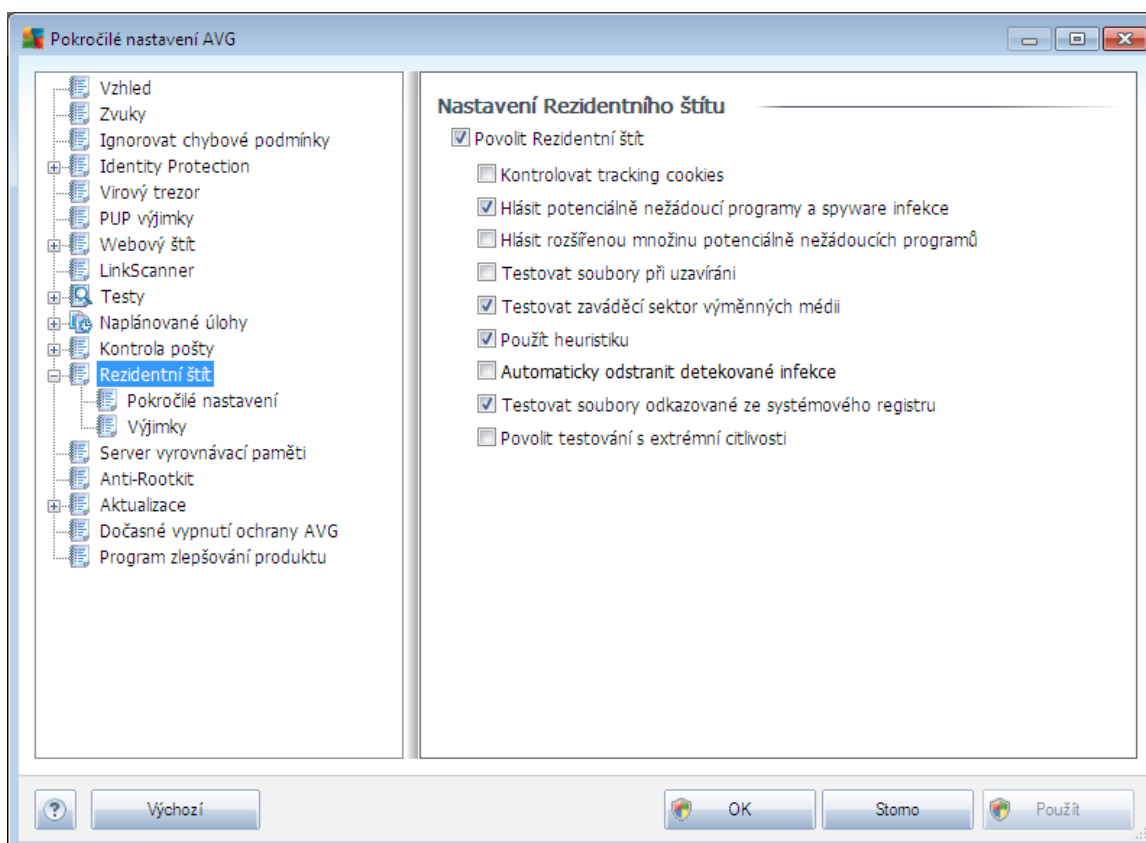
V tomto dialogu (odkaz **Servery / IMAP**) nastavujete server **Kontroly pošty** s protokolem IMAP pro odchozí poštu:

- **Jméno serveru IMAP** - v tomto poli můžete zadat jméno nově přidávaných serverů (server IMAP přidáte tak, že kliknete pravým tlačítkem myši nad položkou IMAP v levém navigačním menu). U automaticky vytvořeného serveru "AutoIMAP" je toto pole deaktivováno.
- **Typ přihlášení** - definuje, jak má být určen poštovní server, ze kterého bude odesílána pošta:
 - **Automatické** - cílový server bude určen podle nastavení ve vaší poštovní aplikaci; není třeba nic dále specifikovat
 - **Pevně definovaný server** - v tomto případě bude vždy použit konkrétní server. Do editačního řádku je třeba zadat adresu nebo jméno vašeho poštovního serveru. Jako jméno je možné použít jak doménový název (např. *imap.acme.com*), tak i IP adresu (např. *123.45.67.89*). Pokud poštovní server používá nestandardní port, lze tento port zadat za jméno serveru oddělený dvojtečkou (např. *imap.acme.com:8200*). Standardní port pro IMAP komunikaci je 143.
- **Doplňující nastavení** - specifikuje další detailní parametry:

- **Lokální port** - určuje, na kterém portu lze očekávat komunikaci z poštovní aplikace. Tento port je pak také nutné v poštovní aplikaci zadat jako port pro IMAP komunikaci.
- **Připojení** - v této rozbalovací nabídce můžete specifikovat typ připojení (*standardní/zabezpečené na vyhrazeném portu/zabezpečené na běžném portu*). Pokud zvolíte zabezpečené připojení, budou posílaná data kryptována a nebude možné jejich sledování nikým jiným. Tato funkce může být aktivována pouze v případě, že cílový poštovní server podporuje.
- **Aktivace IMAP serveru** - zapnutím/vypnutím položky máte možnost aktivovat i deaktivovat právě nastavený IMAP server

9.11. Rezidentní štít

Komponenta **Rezidentní štít** zajišťuje trvalou průběžnou ochranu souborů a složek proti virům, spyware a malware obecně.



V dialogu **Nastavení Rezidentního štítu** máte možnost celkově aktivovat i deaktivovat ochranu **Rezidentního štítu** označením i vypnutím položky **Povolit Rezidentní štít** (*tato položka je ve výchozím nastavení zapnutá*). Dále můžete prostým výběrem rozhodnout, které funkce **Rezidentního štítu** mají být aktivovány:

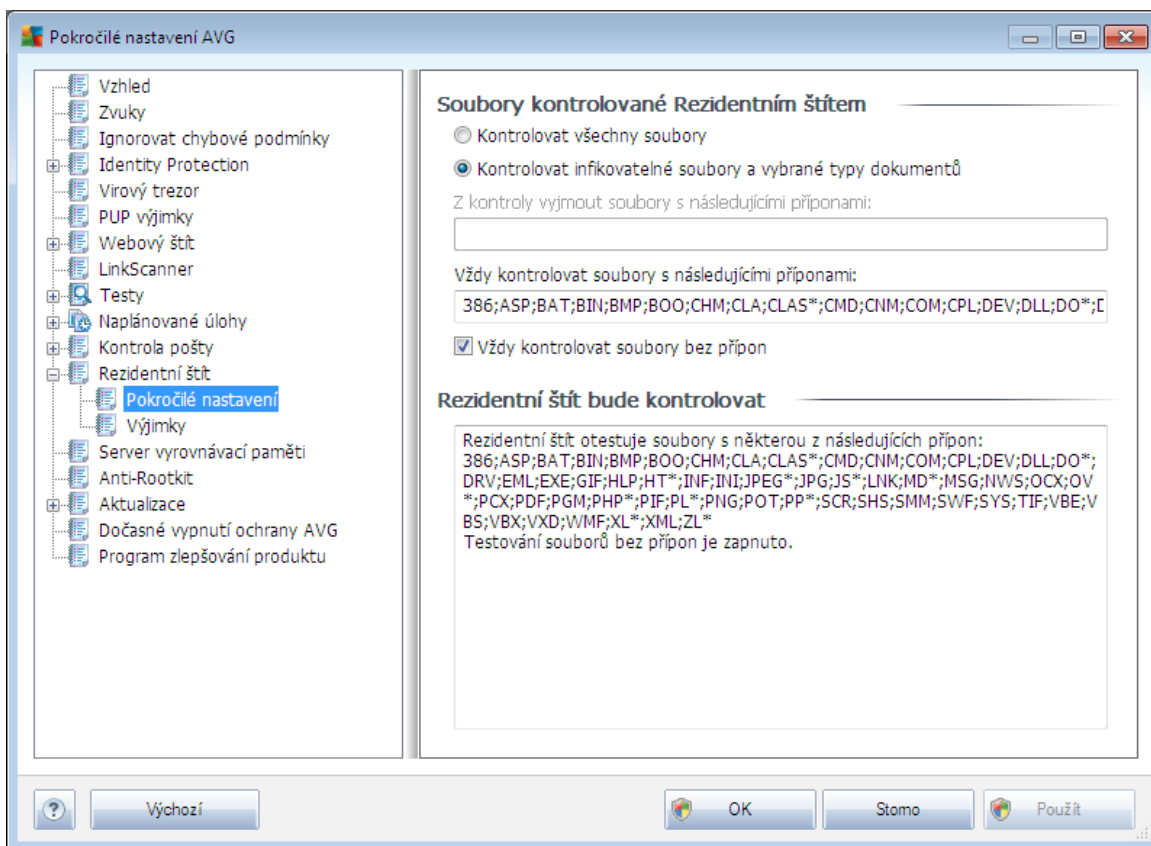
- **Kontrolovat tracking cookies** (ve výchozím nastavení vypnuto) - parametr definuje, že

mají být detekovány cookies (HTTP data zaslaná serverem prohlížeči a uložena na počítači uživatele; při každé další návštěvě téhož serveru prohlížeč posílá cookies zpět serveru, který podle nich rozlišuje jednotlivé uživatele)

- **Hlásit potenciálně nežádoucí programy a spyware infekce** (ve výchozím nastavení zapnuto) - kontrola přítomnosti [potenciálně nežádoucích programů](#) (spustitelné programy, které mohou fungovat jako spyware nebo adware). Zaškrtnutím tohoto políčka aktivujete [Anti-Spyware](#), tj. bude se testovat přítomnost spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány v domě a se souhlasem uživatele. Doporučíme nicméně ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
- **Hlásit rozšířenou množinu potenciálně nežádoucích programů** (ve výchozím nastavení vypnuto) - zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.
- **Testovat soubory při uzavírání** (ve výchozím nastavení vypnuto) - kontrola souborů při zavírání zajišťuje, že AVG testuje aktivní objekty (např. aplikace, dokumenty, ...) nejen při jejich spuštění/otevření, ale také při zavírání; tato funkce pomáhá chránit váš počítač před sofistikovanými viry
- **Testovat zavedení cílů v sítích** (ve výchozím nastavení zapnuto)
- **Použít heuristiku** (ve výchozím nastavení zapnuto) - k detekci infekce bude použita i metoda [heuristické analýzy](#) (dynamické emulace instrukcí testovaného objektu v prostředí virtuálního počítače)
- **Automaticky odstranit detekované infekce** (ve výchozím nastavení vypnuto) - detekovaná infekce bude automaticky vyléčena, jestliže je k dispozici léčba tohoto konkrétního viru; a všechny infekce, jež nelze vyléčit, budou odstraněny.
- **Testovat soubory odkazované ze systémového registru** (ve výchozím nastavení zapnuto) - AVG bude testovat všechny spustitelné soubory přidávané do systémového registru, aby tak zabránil možnému spuštění již známé infekce při prvním startu počítače.
- **Povolit testování s extrémní citlivostí** (ve výchozím nastavení vypnuto) - ve specifických situacích (mimo žádný stav ohrožení počítače) můžete zvolit tuto metodu kontroly, která aktivuje nejkvalitnější a nejpodrobnější testovací algoritmy. Mějte však na paměti, že tato metoda je časově velmi náročná.

9.11.1. Pokročilé nastavení

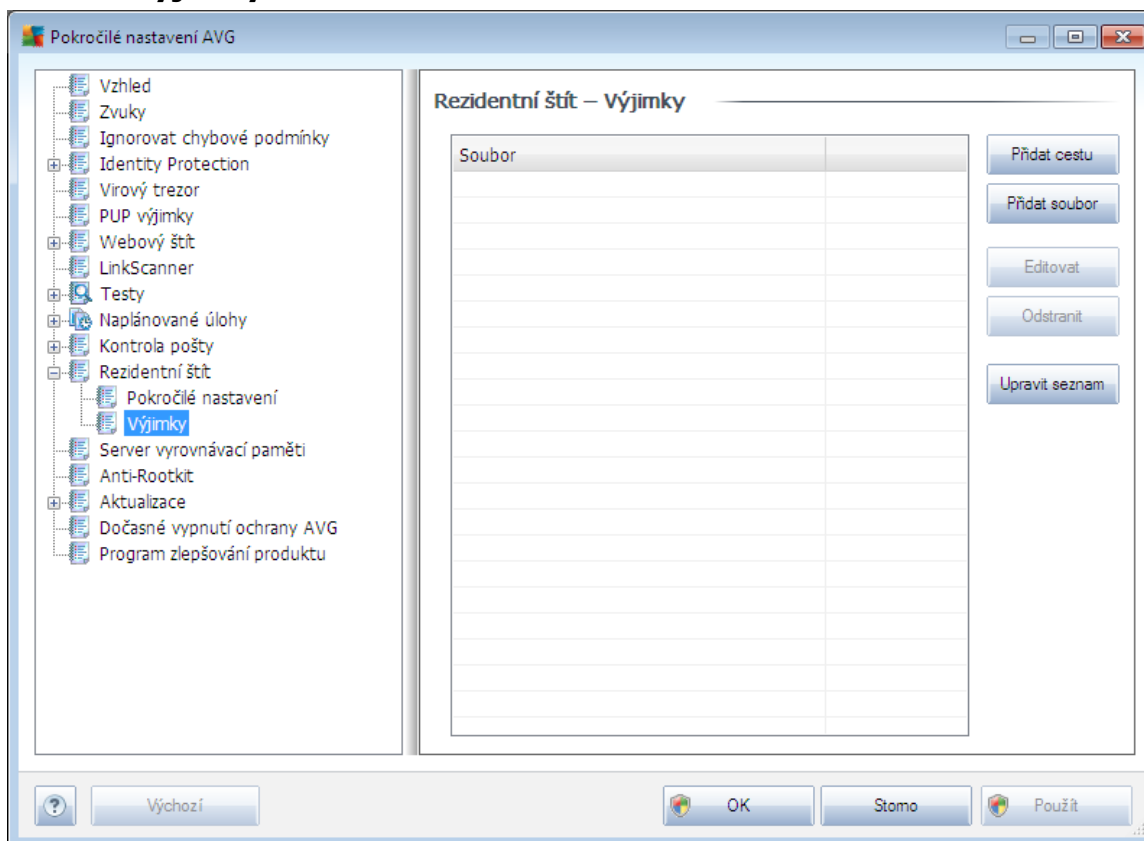
V dialogu **Soubory kontrolované Rezidentním štítem** máte možnost nastavení kontroly souborů a dokumentů vybraných typů (konkrétních přípon):



Rozhodnete, zda chcete kontrolovat všechny soubory nebo pouze infikovatelné soubory - v tom případě můžete definovat seznam přípon souborů, které mají být z kontroly vyjaty a seznam přípon souborů, které se mají kontrolovat za všech okolností.

Sekce ve spodní části dialogu nazvaná **Rezidentní štít bude kontrolovat** následně sumarizuje aktuální nastavení a zobrazuje detailní pohled všech objektů, které mají být komponentou **Rezidentní štít** kontrolovány.

9.11.2. Výjimky



Dialog **Rezidentní štít - Výjimky** nabízí možnost definovat specifické soubory nebo celé adresáře, které mají být vyaty z kontroly komponentou **Rezidentní štít**.

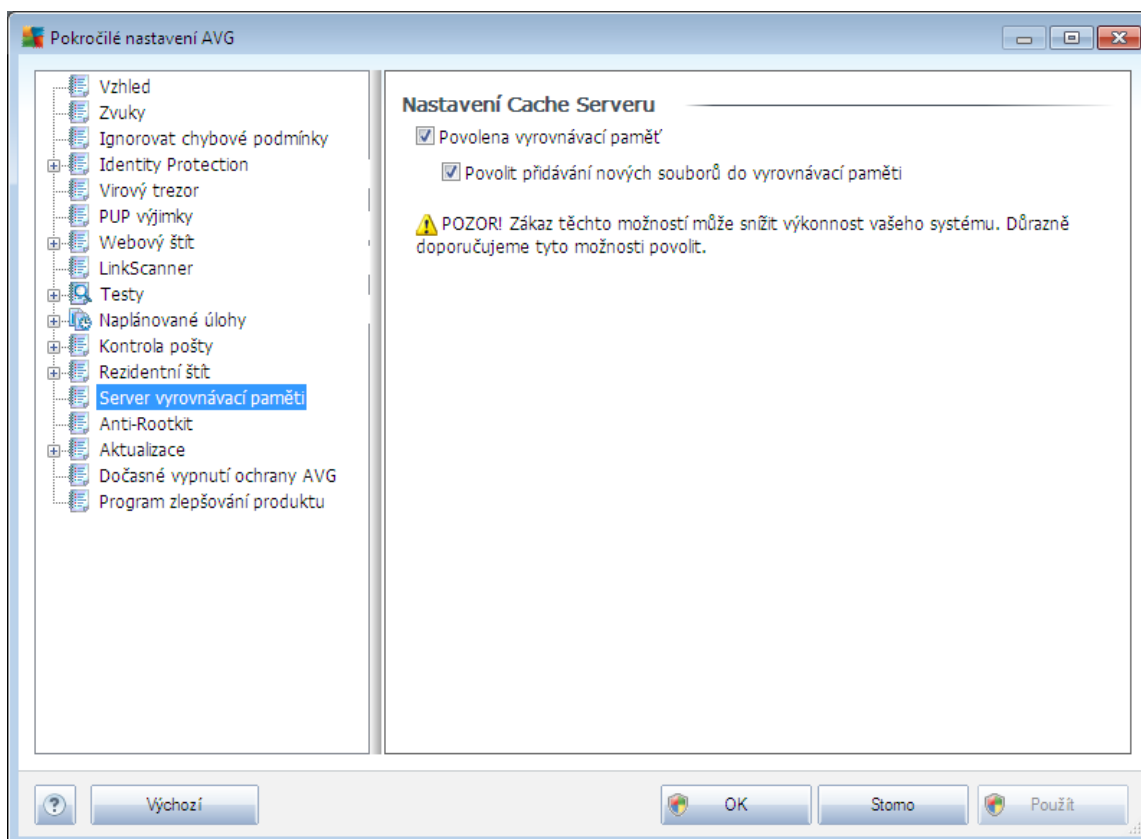
Pokud to není nezbytně nutné, doporučujeme, abyste z testování žádné položky nevyjímali!

V dialogu jsou k dispozici tato ovládací tlačítka:

- **Přidat cestu** – umožňuje vybrat z navigačního stromu lokálního disku určitou adresářovou strukturu s celým obsahem, který má být vyat z testování
- **Přidat soubor** – umožňuje vybrat z navigačního stromu lokálního disku po jednom vybrat další soubory definované jako výjimky z testování
- **Editovat** – umožňuje editovat zadání cesty ke zvolenému souboru nebo adresáři
- **Odstranit** – umožňuje odstranit cestu ke zvolenému souboru nebo adresáři

9.12. Server vyrovnávací paměti

Server vyrovnávací paměti je proces k urychlení testování (pro testy na vyžádání, naplánované testy po íta e i testy Rezidentního štítu). V rámci tohoto procesu **AVG Anti-Virus 2011** detekuje a ukládá informace o d v ryhodných souborech (tj. o systémových souborech s digitálním podpisem): tyto soubory jsou pak automaticky považovány za bezpečné a není třeba je znovu testovat.

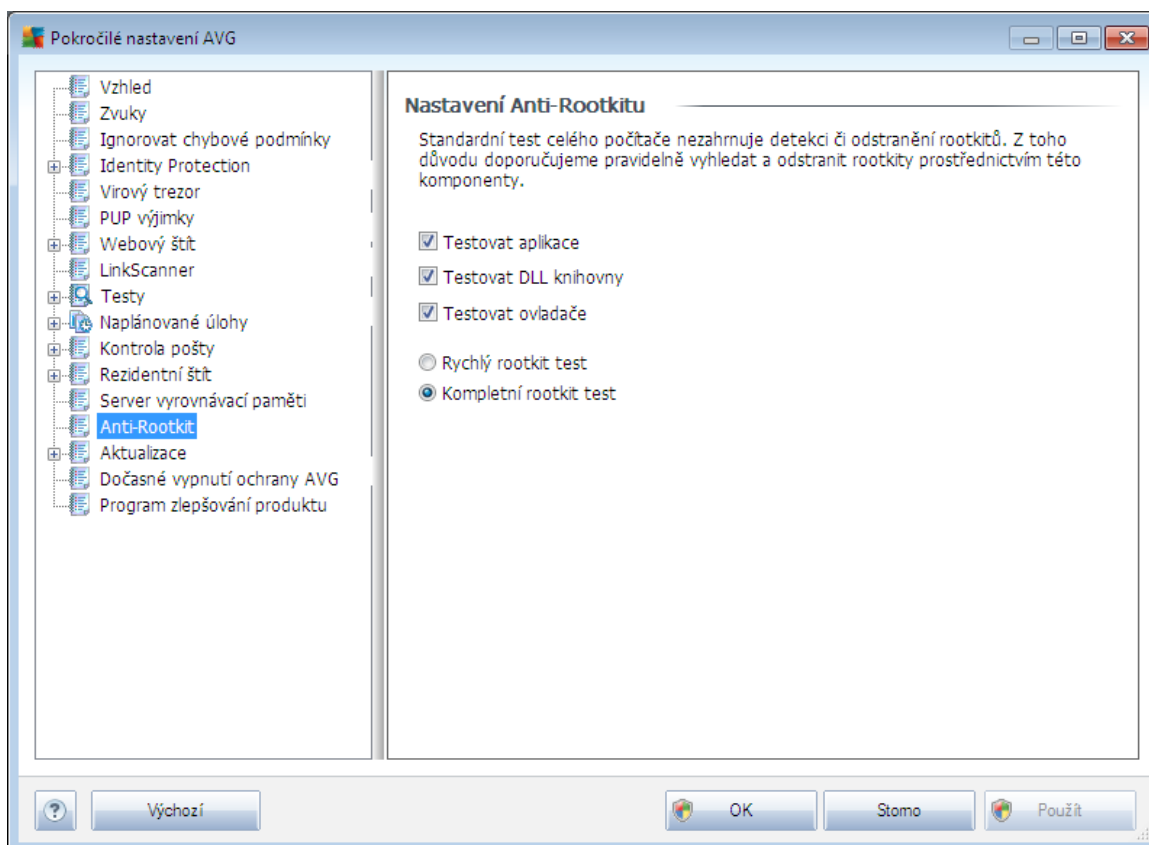


Dialog nastavení nabízí dvě možnosti:

- **Povolena vyrovnávací paměť** (ve výchozím nastavení zapnuto) - pokud tuto možnost vypnete, deaktivujete tak proces vyrovnávací paměti a vyprázdníte cache. Mějte prosím na mysli, že vypnutím tohoto procesu dojde ke zpomalení testu i celkového výkonu vašeho počítače, protože bude nutné provést test přítomnosti viru a spyware u každého jednotlivého souboru.
- **Povolit přidávání nových souborů do vyrovnávací paměti** (ve výchozím nastavení zapnuto) - pokud tuto možnost vypnete, zabráníte tak přidávání nových souborů do vyrovnávací paměti. Všechny soubory, které jsou již v paměti uloženy, budou zachovány a vynechány z testování, pokud nedojde k deaktivaci celé vyrovnávací paměti anebo do příští aktualizace virové databáze.

9.13. Anti-Rootkit

V tomto dialogu pokročilého nastavení máte možnost editovat konfiguraci komponenty [Anti-Rootkit](#).



Editace všech funkcí komponenty [Anti-Rootkit](#) uvedená v tomto dialogu je dostupná i přímo z [rozhraní komponenty Anti-Rootkit](#).

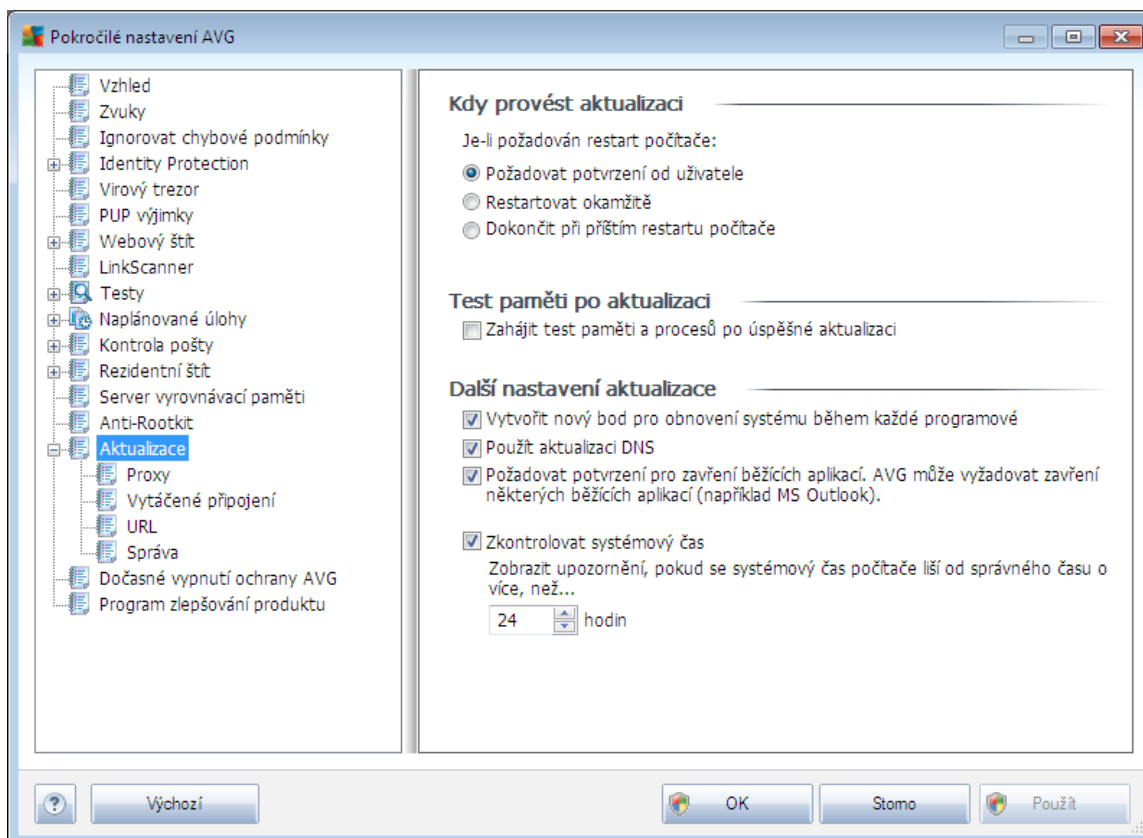
Označením příslušného políčka (*jednoho nebo více*) označíte, jaké objekty mají být testovány:

- **Testovat aplikace**
- **Testovat DLL knihovny**
- **Testovat ovladače**

Dále se můžete rozhodnout, v jakém režimu si nechat test spustit:

- **Rychlý rootkit test** - testuje všechny běžící procesy, nainstalované ovladače a systémovou adresář (v tšinou *c:\Windows*)
- **Kompletní rootkit test** - testuje všechny běžící procesy, nainstalované ovladače, systémovou adresář (v tšinou *c:\Windows*) a také všechny lokální disky (včetně flash disku, ale bez disketové a CD mechaniky)

9.14. Aktualizace



Položka navigace **Aktualizace** otevírá dialog, v němž můžete specifikovat obecné parametry související s [aktualizací AVG](#):

Kdy provést aktualizaci

V této sekci se nabízí volba alternativních možností pro případ, kdy je k dokončení aktualizace vyžadován restart počítače. Dokončení aktualizace lze naplánovat na příští restart počítače nebo můžete provést restart okamžitě:

- **Požadovat potvrzení od uživatele** (výchozí nastavení) - informativním hlášením budete upozorněni na dokončení [procesu aktualizace](#) a vyzváni k restartu
- **Restartovat okamžitě** - restart bude proveden automaticky bezprostředně po dokončení [aktualizačního procesu](#) bez vyžádání vašeho svolení
- **Dokončit při příštím restartu počítače** - restart bude dočasně odložen a [proces aktualizace](#) dokončen při příštím restartu počítače. Tuto volbu však doporučujeme použít pouze tehdy, když jste si jisti, že počítač skutečně pravidelně restartujete, a to nejméně jednou denně!



Test paměti po aktualizaci

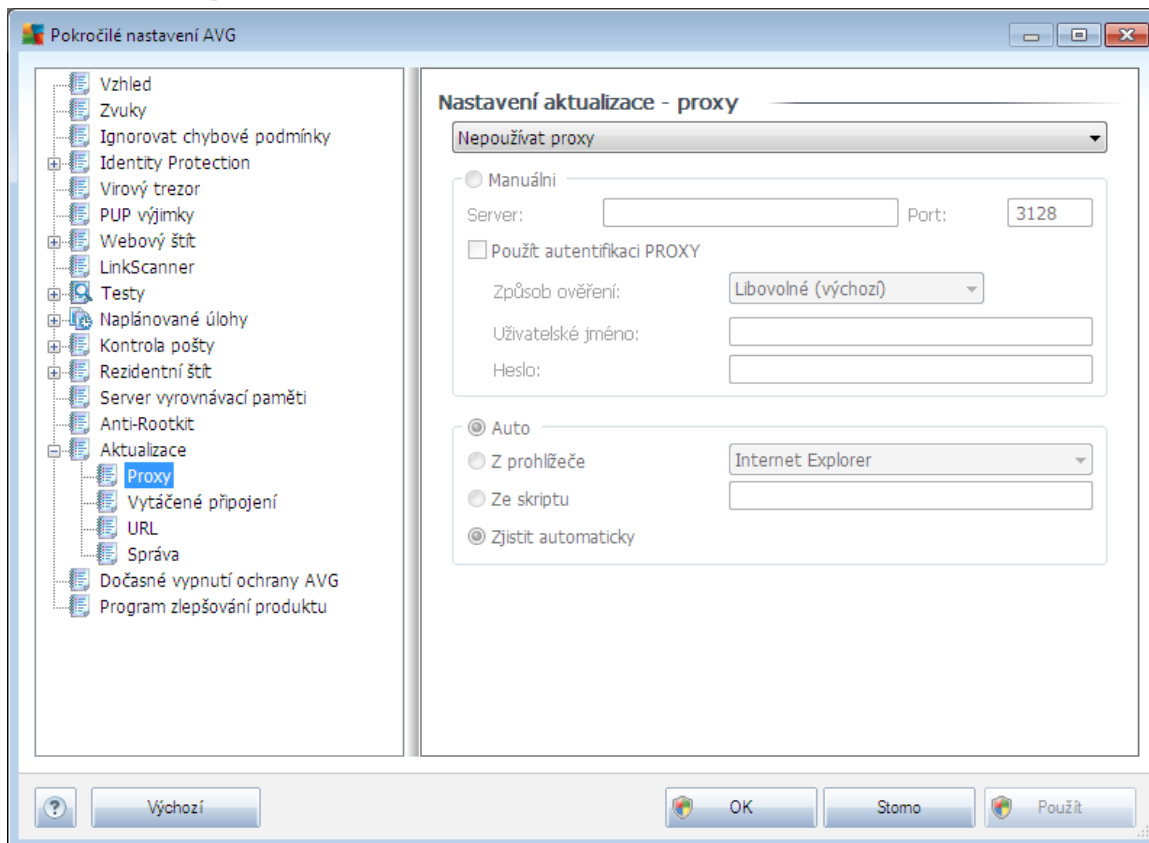
Označíte-li tuto položku, bude po každé úspěšné dokončené aktualizaci spuštěn test paměti. V případě, že by nejnovější aktualizace obsahovala nové virové definice, budou tak tyto okamžitě aplikovány během testu.

Další nastavení aktualizace

Tato sekce nabízí několik možností volby. Označením jednotlivých nabízených položek můžete označit, zda si tu kterou možnost přejete aktivovat:

- **Vytvořit nový bod pro obnovení systému ...** - před každým spuštěním programové aktualizace AVG je vytvořen takzvaný systémový bod pro obnovení systému. V případě, že aktualizací proces nebude z jakéhodůvodu dokončen a váš operační systém bude ohrožen, můžete za pomoci tohoto zálohovacího bodu obnovit OS v jeho původní konfiguraci. Tato možnost je dostupná přes volbu *Start / Všechny programy / Podpora / Systémové nástroje / Obnova systému*, ale jakékoli zásahy do tohoto nastavení lze doporučit výhradně pokročilým a zkušeným uživatelům! Chcete-li využít této možnosti, ponechtejte políčko označené.
- **Použít aktualizaci DNS (ve výchozím nastavení zapnuto)** - pokud je tato položka označena, při spuštění aktualizace **AVG Anti-Virus 2011** vyhledá na DNS serveru informaci o aktuální verzi virové databáze a aktuální verzi programu a následně stáhne pouze nejmenší nezbytně nutné aktualizací soubory. Tím se sníží celkový objem stahovaných dat a urychlí proces aktualizace.
- **Požadovat potvrzení pro zavření běžících aplikací (ve výchozím nastavení zapnutou)** zajistíte, že v případě, že bude nutné zavřít některé spuštěné aplikace, aby mohla být aktualizace dokončena, budete před jejich zavřením upozorněni varovným hlášením.
- **Zkontrolovat systémový čas** - označením této položky určíte, že si přejete, abyste byli informováni o případném rozporu mezi časem nastaveným na počítaři a skutečným časem, a to v okamžiku, kdy rozdíl těchto dvou časů dosáhne stanoveného počtu hodin.

9.14.1. Proxy



Proxy server je samostatný server nebo služba běžící na libovolném počítači, která slouží k zajištění bezpečnějšího připojení k internetu. Podle nastavení pravidel síť pak lze na Internet přistupovat buďto přímo nebo přes proxy server; obě možnosti mohou být také povoleny současně. V první položce dialogu **Nastavení aktualizace - proxy** tedy volbou z rozbalovací nabídky combo boxu určíte, zda si přejete:

- **Použít proxy**
- **Nepoužívat proxy** - výchozí nastavení
- **Zkusit připojení přes proxy a v případě selhání se připojit přímo**

Pokud zvolíte možnost, u níž se uvažuje použití proxy serveru, je třeba dále specifikovat některé další údaje. Nastavení serveru můžete provést manuálně nebo jej nechat detekovat automaticky.

Manuální nastavení

Při manuálním nastavení (volba **Manuální** aktivuje příslušnou sekci dialogu) specifikujte tyto položky:

- **Server** – zadejte IP adresu nebo jméno serveru

- **Port** – zadejte číslo portu, na němž je povolen přístup k internetu (výchozím nastavením je číslo portu 3128, ale může být nastaveno jinak – pokud si nejste jisti, obraťte se na správce vaší síť)

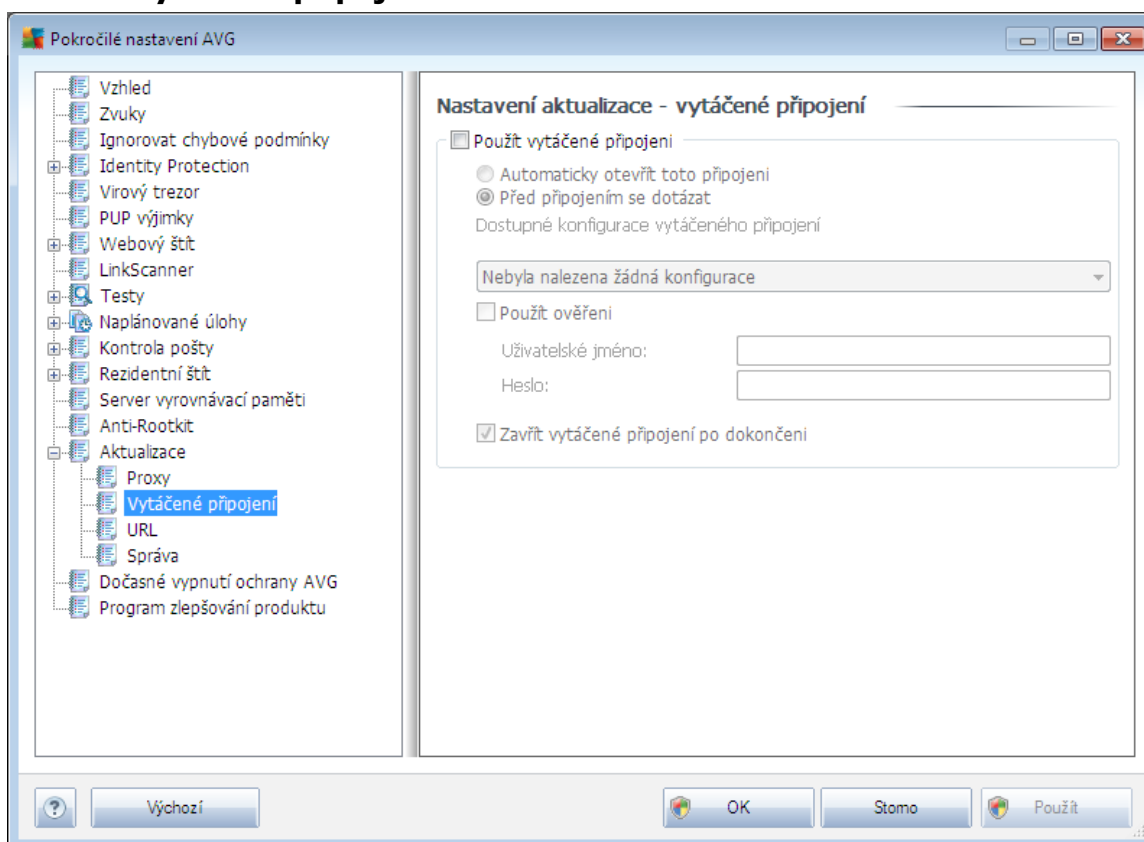
Proxy server může mít dále nastavena pravidla pro jednotlivé uživatele. Jestliže je váš proxy server takto nastaven, označte položku **Použít autentifikaci PROXY** a zadejte své **Uživatelské jméno** a **Heslo** pro připojení k internetu přes proxy server.

Automatické nastavení

Při automatickém nastavení (volba **Auto** aktivuje příslušnou sekci dialogu) prosím zvolte, odkud se má nastavení proxy serveru převzít:

- **Z prohlížeče** - nastavení se převzeme z vašeho internetového prohlížeče
- **Ze skriptu** - nastavení se převzeme ze staženého skriptu s funkcí, která vrací adresu proxy
- **Zjistit automaticky** - nastavení bude automaticky detekováno přímo na proxy serveru

9.14.2. Vytáčené připojení

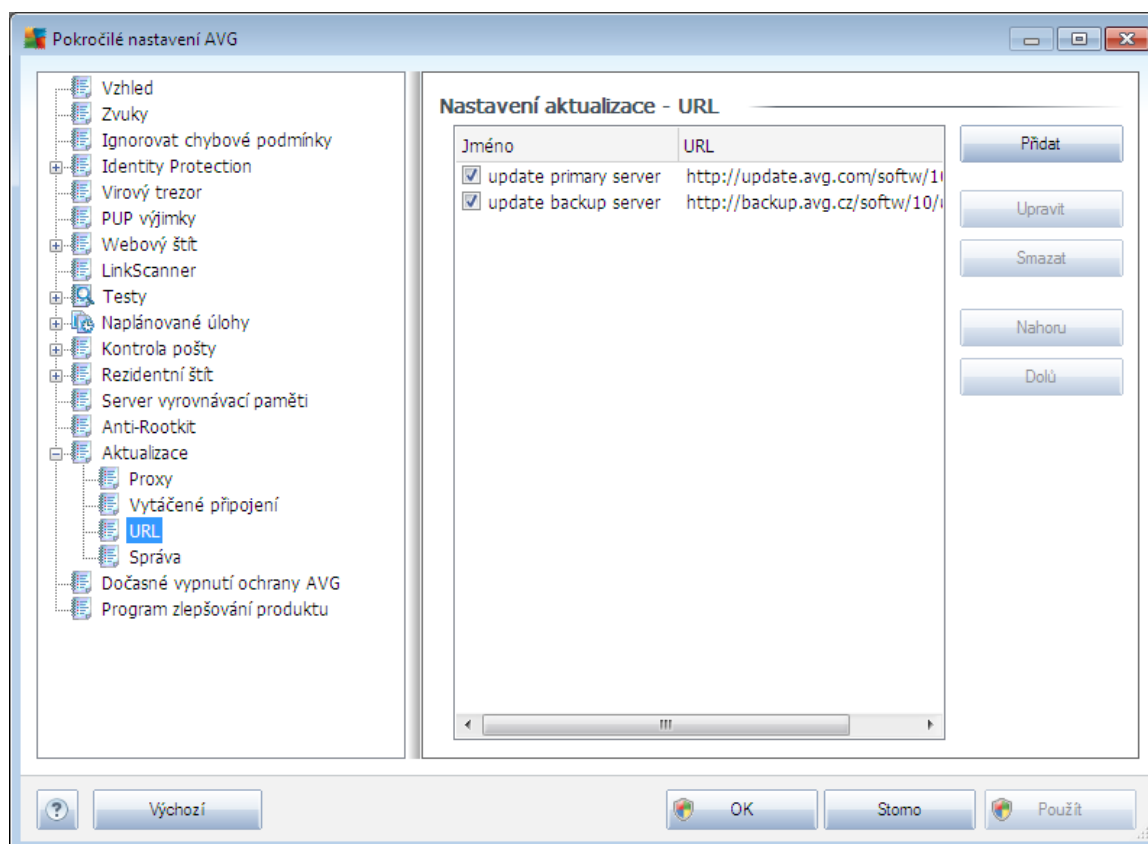


Parametry nastavované v dialogu **Nastavení aktualizace- vytáčené připojení** se vztahují k telefonickému připojení. Jednotlivá pole záložky jsou neaktivní, pokud neoznačíte položku **Použít**

vytá ené p ipojení. Touto volbou se pak aktivují ostatní pole.

Ur ete, zda má být p ipojení k internetu provedeno automaticky (**Automaticky otev ít toto p ipojení**) anebo je t eba, aby uživatel každé p ipojení potvrdil (**P ed p ipojením se dotázat**). U automatického p ipojení se dále m žete rozhodnout, zda má být p ipojení po provedení aktualizace ukon eno (**Zav ít vytá ené p ipojení po dokon ení**).

9.14.3. URL

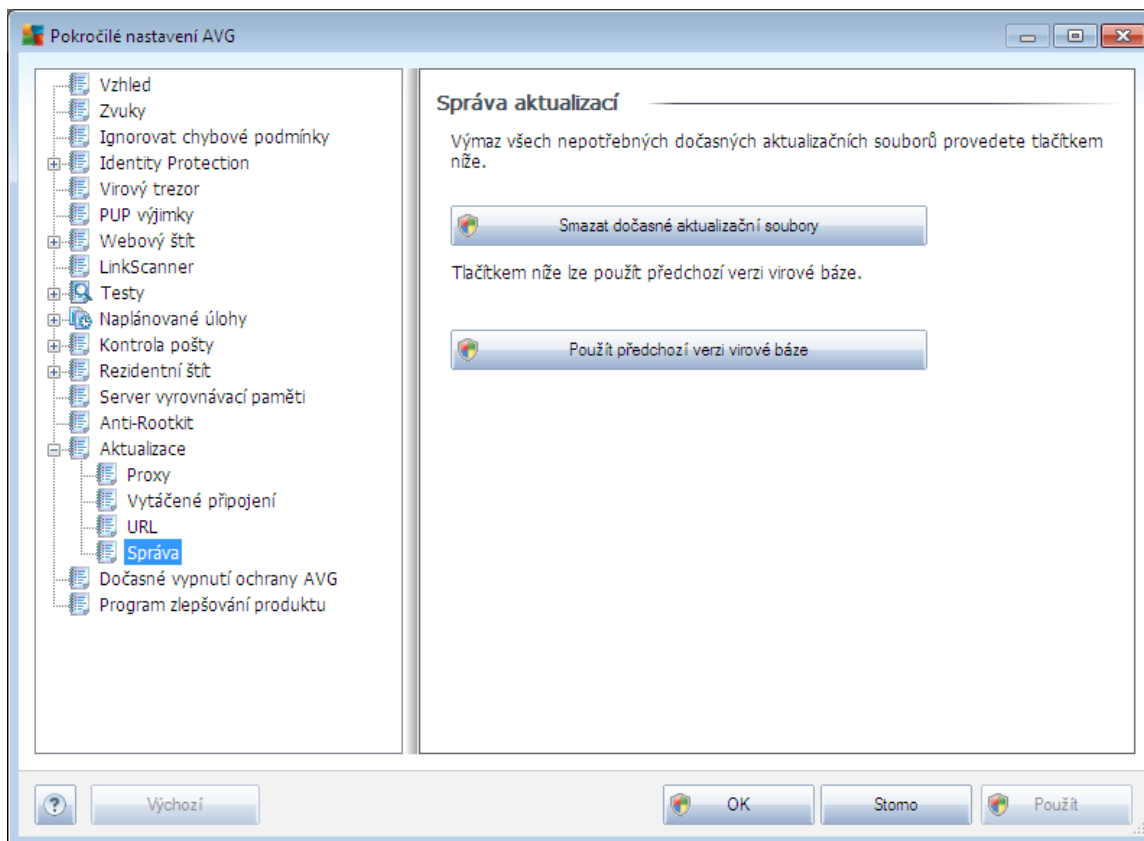


Dialog **URL** nabízí seznam internetových adres, odkud mohou být aktualizace souboru staženy. Seznam a jeho jednotlivé položky lze editovat pomocí následujících ovládacích tlačítek:

- **Přidat** – otev e dialog, kde lze specifikovat další URL k přidání do seznamu
- **Upravit** - otev e dialog, kde lze editovat parametry stávající URL
- **Smazat** – smaže zvolenou položku seznamu
- **Nahoru** – p emístí zvolenou URL na o jednu pozici v seznamu výše
- **Dolů** - p emístí zvolenou URL na o jednu pozici v seznamu níže

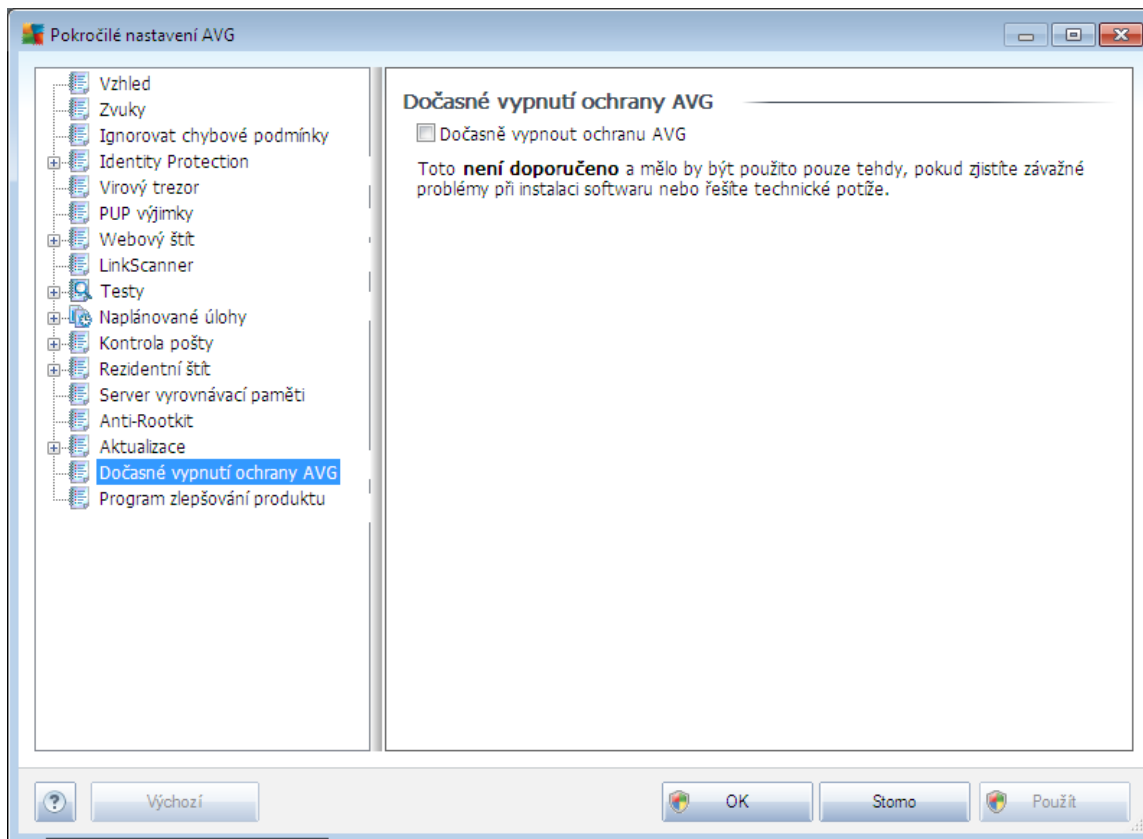
9.14.4. Správa

Dialog **Správa** obsahuje dvě možnosti volby dostupné prostřednictvím dvou tlačítek:



- **Smazat dočasná aktualizací soubory** - tímto tlačítkem odstraníte ze svého pevného disku všechny již nepotřebné soubory aktualizací (ve výchozím nastavení správy aktualizací soubor se tyto uchovávají po dobu po 30 dní)
- **Použít předchozí verzi virové báze** – tímto tlačítkem odstraníte ze svého pevného disku poslední verzi virové databáze a vrátíte se tak k předchozí uložené verzi (nová verze virové báze bude pochopitelně součástí další aktualizace)

9.15. Dočasné vypnutí ochrany AVG



V dialogu **Dočasné vypnutí ochrany AVG** máte možnost označením jediné dostupné položky jednorázově deaktivovat celou ochranu zajištěnou programem **AVG Anti-Virus 2011**.

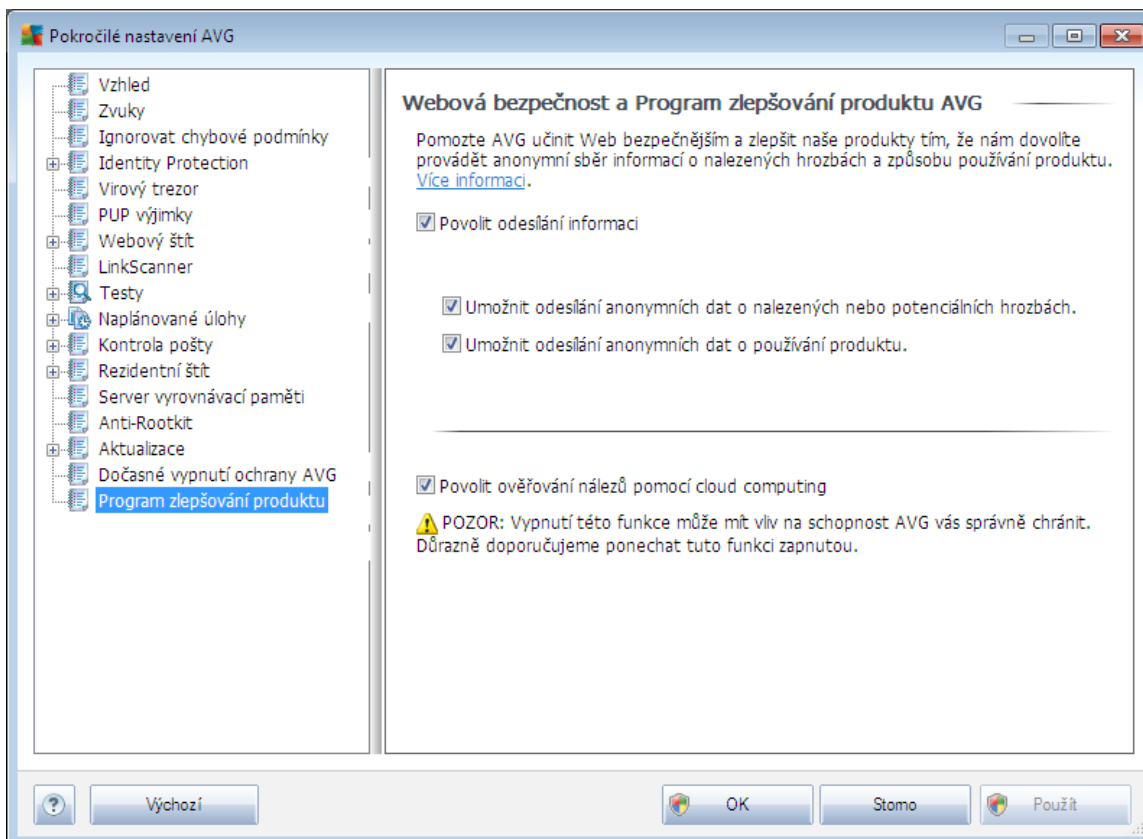
Míjte prosím na paměti, že tato volba by v žádném případě neměla být použita, pokud to není opravdu nezbytně nutné!

V naprosté většině případů **není nutné** deaktivovat AVG před instalací nového software nebo ovladače, a to ani tehdy, pokud budete během instalace vyzváni k zavěšení všech spuštěných aplikací. Pokud by v takovém případě došlo ke kolizi, pravděpodobně bude stačit deaktivovat **Residentní štít**. Jestliže budete opravdu nuceni deaktivovat AVG, zapněte jej hned, jakmile to bude možné. Pamatujte, že pokud jste připojeni k Internetu nebo k jiné síti, je váš počítač bez aktivní ochrany vysoce zranitelný.

9.16. Program zlepšování produktu

V dialogu **Webová bezpečnost a Program zlepšování produktu AVG** máte možnost zapojit se do spolupráce a podílet se na zlepšování produktu AVG a na celkovém zvýšení úrovně bezpečnosti na Internetu. Zaškrtnutím položky **Povolit odesílání informací** umožníte reportování informací o detekovaných hrozbách týmu expertů společnosti AVG. Tyto reporty nám pomáhají shromažďovat nejnovější informace o virech, spywaru i škodlivých webových stránkách a vylepšovat neustále ochranu pro všechny naše uživatele.

Reportování probíhá automaticky, takže vám nezpůsobí žádné nepohodlí, a reporty nikdy neobsahují žádná vaše soukromá data. Reportování je samozřejmě dobrovolné, nicméně vás prosíme, abyste je také aktivovali, protože nám tím výrazně pomůžete s vylepšováním ochrany vašeho počítače.



V dnešní době už de facto nemluvíme o antivirové ochraně, ale obecně o webové bezpečnosti. Na Internetu se vyskytuje obrovské množství různých hrozeb, jejichž rozsah daleko přesahuje kategorii virů. Auto i nebezpečných kódů a webových stránek jsou stále vynalézavější, a tak se denně objevují nejen nové viry, ale i zcela nové typy hrozeb, triků a technik, jak uživatele podvést a využít. Uvědomte si ty nejzáhadnější, z nichž některé ještě nemají ani české pojmenování:

- **Virus** je kód, který dokáže sám sebe kopírovat a šířit, často zcela nepozorovaně, dokud nenadělá spoustu škody. Některé viry představují vážnou hrozbu, napadají soubory, mazávají je a vymazávají z disku, jiné dělají v cíli na první pohled celkem neškodné, například přehrávají nějakou hudbu. Nebezpečné jsou však všechny viry, a to kvůli základní vlastnosti nekontrolovatelného množení – jednoduchý virus se dokáže během chvilky namnožit tak, že zabere veškerou paměť a způsobí pád systému.
- **Worm** je typ viru, který však na rozdíl od běžných virů nepotřebuje ke svému šíření jiný objekt; rozširuje sám sebe na další počítače zcela bez pomoci, nejčastěji elektronickou poštou, a tak způsobuje přetížení sítě a e-mailových serverů.
- **Spyware** je obvykle definován jako typ malware (*malware = anglická zkratka pro "malicious software", tj. škodlivé programy obecně*) a většinou zahrnuje především programy –



nejast ji tzv. *trojské kon* urené k odcizení osobních informací, hesel, ísel kreditních karet a podobn , p ípadn k proniknutí do počíta e za ú elem poskytnutí p ístupu cizí osob ; samoz ejm to vše bez v domí vlastníka počíta e.

- **Potenciáln nežádoucí programy** (z *anglického Potentially Unwanted Programs = PUP*) jsou typem spyware, který p edstavuje potenciální riziko pro váš počíta . P íkladem PUP m že být adware, to je program ur ený k distribuci reklamy. Ten se v tšinou projevuje tak, že zobrazuje v internetovém prohlíže í vyskakovací okna s reklamou, což je sice otravné, ale ne skute n ohrožující.
- **Sledovací cookies** lze rovn ž považovat za druh spyware, jelikož tyto malé soubory, uložené ve vašem internetovém prohlíže í a posílané nazp t "mate ské" webové stránce, kdykoli se na ni znovu p ípojíte, mohou obsahovat r zné osobní informace, nap íklad seznam stránek, na které jste se v poslední dob dívali, a podobn .
- **Exploit** je škodlivý kód, který využívá chyby nebo bezpe nostní skuliny v opera ním systému, internetovém prohlíže í nebo jiném ásto používaném programu.
- **Phishing** je pokus, jak získat citlivá data vydáváním se za d v ryhodnou instituci. Potenciální ob ti jsou obvykle kontaktovány hromadným e-mailem obsahujícím výzvu k aktualizaci bankovních údaj (*jinak bude konto uzav eno...*) a následuje odkaz na webovou stránku p íslušné banky, která mnohdy vypadá velmi v rn , ale je samoz ejm falešná.
- **Hoaxy** jsou et zové podvodné nebo poplašné e-maily obsahující nap íklad falešné nabídky práce, p ípadn nabídky, které pracovníky zneužijí k nelegálním aktivitám, výzvy k vybrání velké sumy pen z, podvodné loterie a podobn .
- **Nebezpe né webové stránky** dokáží nepozorovan ínstalovat škodlivé programy do vašeho počíta e, a stránky napadené hackery d lají totéž, jen se jedná o stránky p vodn íslušné a neškodné, které se však po útoku hacker chovají zcela nep edvídateln .

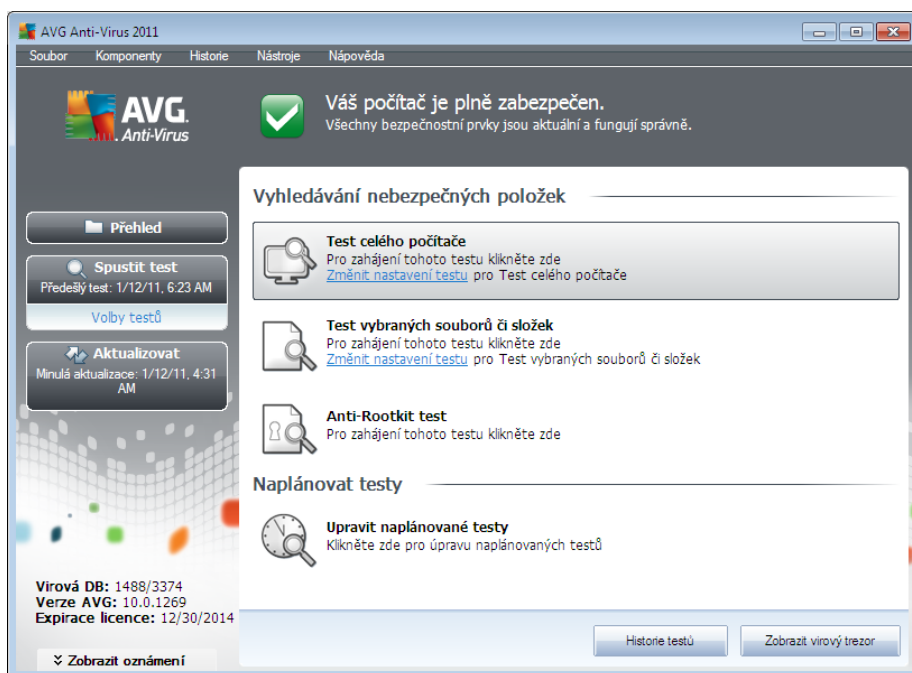
Systém AVG obsahuje ochranu proti všem zmín ným typ m hrozeb a škodlivých program :

- **[Anti-Virus](#)** chrání váš počíta p ed viry,
- **[Anti-Spyware](#)** chrání váš počíta p ed spyware,
- **[Webový štít](#)** chrání proti vir m i typ m spyware b hem prohlížení Internetu,
- **[LinkScanner](#)** chrání proti internetovým šk dc m a hrozbám uvedeným v této kapitole.

10. AVG testování

Testování je elementární součástí **AVG Anti-Virus 2011**. Testy lze spouštět na vyžádání podle okamžité situace (on-demand testy) nebo [nastavit jejich pravidelné spuštění podle plánu](#).

10.1. Rozhraní pro testování



Testovací rozhraní AVG je dostupné prostřednictvím [zkratkového tlačítka **Volby test**](#). Jeho stiskem se uživatelské rozhraní přepíná do dialogu **Vyhledávání nebezpečných položek**. V tomto dialogu najdete:

- [přehled přednastavených testů](#) - testy definované výrobcem jsou k dispozici k okamžitému spuštění na vyžádání a/nebo podle nastaveného plánu:
 - [Test celého počítače](#)
 - [Test vybraných souborů a složek](#)
 - [Anti-Rootkit test](#)
- sekci pro [naplánování testů](#) - zde můžete definovat nové testy a nastavovat jejich spuštění podle vlastního plánu.

Ovládací tlačítka dialogu

Ovládací tlačítka dostupná v testovacím rozhraní jsou:

- **Historie testů** - zobrazí dialog [Přehled výsledků testů](#) s kompletním seznamem historie



testování

- **Zobrazit virový trezor** - v novém okně otevře [Virový trezor](#) - karanténní prostor pro uložení detekovaných infekcí

10.2. Přednastavené testy

Jednou z hlavních funkcí **AVG Anti-Virus 2011** je testování na vyžádání. Testy na vyžádání jsou navrženy tak, že mohou testovat různé části vašeho počítače, kdykoliv se objeví podezření na možnost virové infekce. V každém případě však doporučujeme provádět testy pravidelně, i když považujete váš počítač za zcela virusprostý.

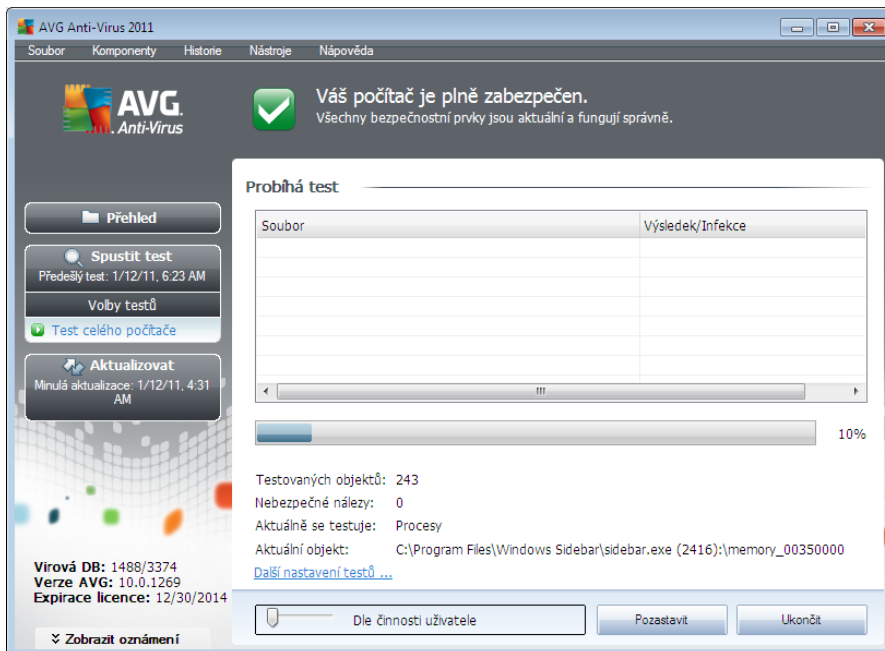
V **AVG Anti-Virus 2011** najdete tyto typy výrobcem nastavených testů:

10.2.1. Test celého počítače

Test celého počítače zkontroluje celý počítač a ověří případnou přítomnost virů a potenciálně nežádoucích programů. Test prozkoumá všechny pevné disky vašeho počítače a najde všechny viry, případně je vyčistí a přesune do [Virového trezoru](#). **Test celého počítače** by měl být na počítači naplánován minimálně jednou týdně.

Spuštění testu

Test celého počítače spusťte přímo z [rozhraní pro testování](#) kliknutím na graficky znázorněnou položku **Test celého počítače**. U tohoto testu již není potřeba žádné další specifické nastavení, test bude tedy rovnou spuštěn v dialogu **Probíhá test** (viz obrázek). Test můžete podle potřeby kdykoliv dočasně **Pozastavit** nebo **Ukončit**.



Editace nastavení testu

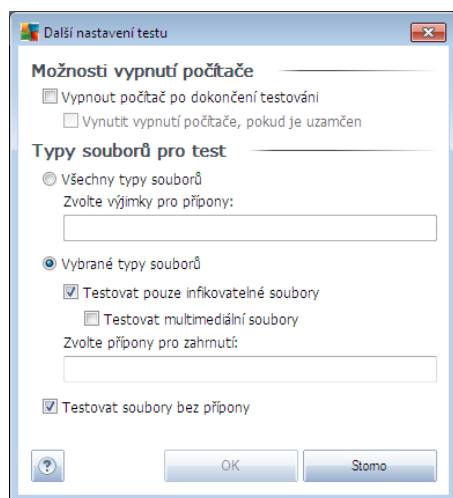
P edem definované výchozí nastavení **Testu celého počítače** máte možnost editovat v dialogu **Změnit nastavení testu pro Test celého počítače** (dostupného z [rozhraní pro testování](#) prostřednictvím odkazu **Změnit nastavení testu u Testu celého počítače**). **Pokud však nemáte skutečný vod konfiguraci testu m nit, doporu ujeme se podržet výrobcem definovaného nastavení!**



- **Parametry testu** - v seznamu parametrů testu můžete jednotlivé volby podle potřeby vypínat/zapínat:
 - **Automaticky léčit/odstraňovat infekci** - (ve výchozím nastavení zapnuto): je-li během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. Pokud virus automaticky léčit nelze, bude infikovaný objekt automaticky přesunut do [Virového trezoru](#).
 - **Hlásit potenciálně nežádoucí programy a spyware infekce** - (ve výchozím nastavení zapnuto): kontrola přítomnosti [potenciálně nežádoucích programů](#) (spustitelné programy, které mohou fungovat jako spyware nebo adware). Zaškrtnutím tohoto políčka aktivujete [Anti-Spyware](#), tj. bude se testovat přítomnost spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, protože i když v tšina tchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány v domě a se souhlasem uživatele. Doporu ujeme nicmén ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
 - **Hlásit rozšířenou množinu potenciálně nežádoucích programů** (ve výchozím nastavení vypnuto) - zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v podobě od výrobce

neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně můžete blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.

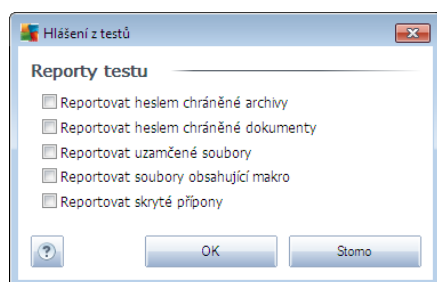
- **Kontrolovat tracking cookies** (ve výchozím nastavení vypnuto) - parametr komponenty **Anti-Spyware** definuje, že během testu mají být detekovány cookies (HTTP data zaslaná serverem prohlížeči a uložena na počítači uživatele; při každé další návštěvě téhož serveru prohlížeč posílá cookies zpět serveru, který podle nich rozlišuje jednotlivé uživatele).
 - **Testovat archivy** (ve výchozím nastavení vypnuto) - parametr definuje, že test má kontrolovat všechny soubory zabalené v některém typu archivu, například ZIP, RAR, ...
 - **Použít heuristickou analýzu** (ve výchozím nastavení zapnuto) - během testu bude použita k detekci infekce i metoda heuristické analýzy (dynamické emulace instrukcí testovaného objektu v prostředí virtuálního počítače).
 - **Testovat systémové prostředí** (ve výchozím nastavení zapnuto) - test prověří i systémové oblasti vašeho počítače.
 - **Povolit testování s extrémní citlivostí** (ve výchozím nastavení vypnuto) - ve specifických situacích (například při podezření na infekci starším typem viru) můžete zvolit tuto metodu testování, která aktivuje nejdokladnější testovací algoritmy a velmi podrobně prověří naprosto všechny oblasti vašeho počítače. Mějte však na paměti, že tato metoda je časově velmi náročná.
- **Další nastavení testu** - odkaz otevírá dialog **Další nastavení testu**, kde můžete definovat následující parametry testu:



- **Možnosti vypnutí počítače** - určete, zda má být počítač po dokončení testu automaticky vypnut. Pokud potvrdíte tuto možnost (**Vypnout počítač po dokončení testování**), aktivuje se nová volba (**Vynutit vypnutí počítače, pokud je uzamčen**), jejíž potvrzení dojde po dokončení testu k vypnutí počítače i tehdy, jestliže je

po řada momentálně zamknut.

- o **Zvolte typy soubor pro testování** - dále se můžete rozhodnout, zda si přejete testovat
 - **Všechny typy soubor** - pokud vám má být zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou;
 - **Vybrané typy soubor** - můžete se rozhodnout, že chcete, aby se testy spouštěly pouze nad soubory, které lze považovat za infikovatelné (*soubory, které nemohou být infekcí zasaženy, se testovat nebudou - například prosté textové soubory nebo některé nespustitelné soubory*), a to včetně multimediálních souborů (*video, audio soubory - ponecháte-li tuto položku neoznacenou, výrazně se tím zkrátí čas testování, jelikož multimediální soubory jsou obvykle poměrně velké, ale pravděpodobnost infekce je u nich velmi nízká*). I zde můžete určit výjimky a pomocí seznamu přípon definovat, které soubory mají být testovány za všech okolností.
 - U položky **Testovat soubory bez přípon** pak rozhodnete, zda se mají testovat i soubory se skrytou nebo neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme, abyste se tohoto nastavení drželi, pokud nemáte skutečnou důvod jej změnit. Soubory bez přípon jsou obecně vysoce podezřelé a měly by být otestovány.
- **Nastavit, jak rychle probíhá test** - posuvníkem lze změnit prioritu testu. Ve výchozím nastavení je tato hodnota nastavena *dle přání uživatele*. Tato hodnota nastavení optimalizuje rychlost testu po řadu a a vytížení systémových zdrojů. Test můžete spustit pomaleji a tedy s nižší zátěží systémových zdrojů (*vhodné, pokud potěbujete během testu na počítači pracovat a nezáleží vám tolik na celkové době testování*) nebo naopak rychleji s vyššími nároky na systémové zdroje (*například v době, kdy na počítači nikdo nepracuje*).
- **Nastavit další reporty test** - odkaz otevírá nový dialog **Reporty test**, v němž můžete označit, které typy nálezů mají být hlášeny:



Upozornění: Samotné možnosti nastavení testu jsou shodné s parametry nově definovaného testu, které jsou podrobně popsány v kapitole [AVG testování / Naplánování testu / Jak testovat](#). Pokud se rozhodnete výchozí nastavení **Testu celého počítače** změnit, můžete pak svou konfiguraci uložit jako výchozí, takže bude použita pro všechny další testy celého počítače.



10.2.2. Test vybraných souborů či složek

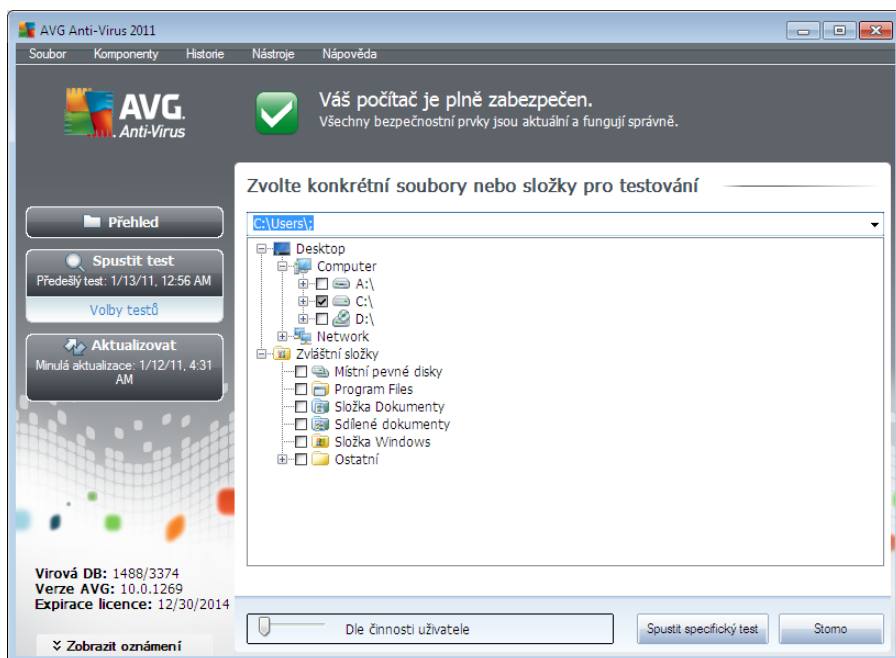
Test vybraných souborů i složek kontroluje pouze uživatelem definované oblasti počítače (zvolené složky, pevné disky, diskety, CD, optické disky, ...). Postup při nálezů a léčení / odstranění virových nákaz je stejný jako u **Testu celého počítače**: nalezené viry jsou vyléčeny nebo přesunuty do **Virového trezoru**. **Test vybraných souborů i složek** můžete s výhodou použít pro nastavení vlastních testů, jejichž spuštění nastavíte podle vašich potřeb.

Spuštění testu

Test vybraných souborů i složek spusťte přímo z [rozhraní pro testování](#) kliknutím na grafický znázorněnou položku **Test vybraných souborů i složek**. Otevře se rozhraní **Zvolte konkrétní soubory nebo složky pro testování**. V graficky znázorněné stromové struktuře vašeho počítače označte ty složky, jejichž obsah chcete nechat zkontrolovat. Cesta ke každé zvolené složce se automaticky vygeneruje v horním textovém poli dialogu.

Pokud si přejete zkontrolovat určitý adresář bez kontroly všech v něm obsažených podadresářů, napište před automaticky vygenerovanou cestu k adresáři znaménko "-". Parametrem "!" před cestou k adresáři zase určíte, že celý adresář má být z testu vypuštěn.

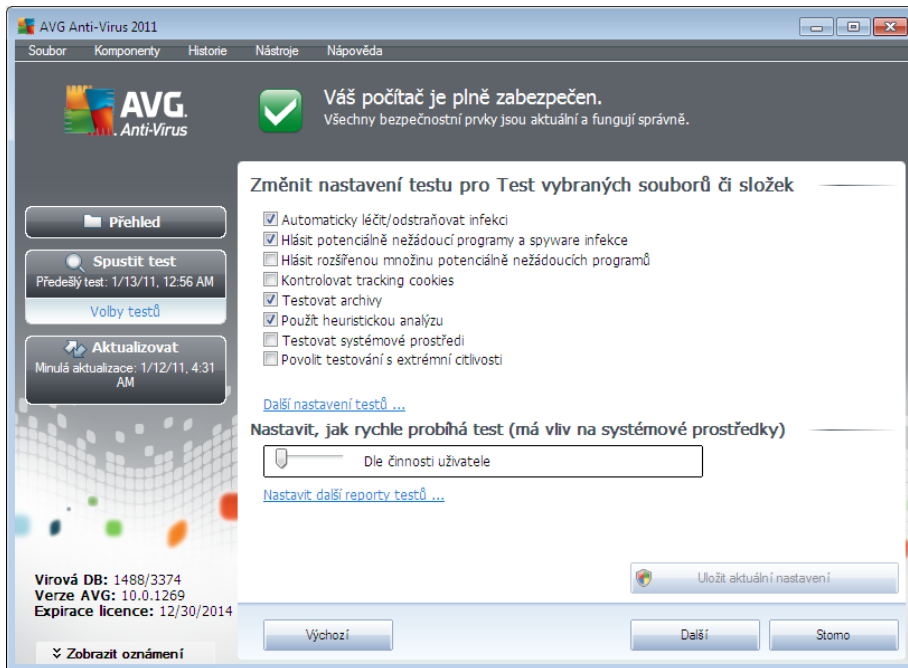
Samotný test pak spustíte stiskem tlačítka **Spustit test** a jeho průběh je identický s průběhem [Testu celého počítače](#).



Editace nastavení testu

Předem definované výchozí nastavení **Testu vybraných souborů i složek** máte možnost editovat v dialogu **Změnit nastavení testu pro Test vybraných souborů i složek** (dostupného z [rozhraní pro testování](#) prostřednictvím odkazu **Změnit nastavení testu u Testu vybraných souborů a složek**).

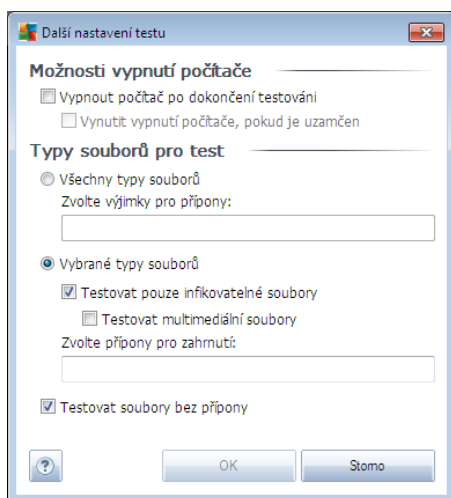
Pokud však nemáte skutečný důvod od konfiguraci testu změnit, doporučujeme se držet výrobce definovaného nastavení!



- **Parametry testu** - v seznamu parametrů testu můžete jednotlivé volby podle potřeby vypínat/zapínat:
 - **Automaticky léčit/odstraňovat infekci** - (ve výchozím nastavení zapnuto): je-li během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. Pokud virus automaticky léčit nelze, bude infikovaný objekt automaticky přesunut do [Virového trezoru](#).
 - **Hlásit potenciálně nežádoucí programy a spyware infekce** - (ve výchozím nastavení zapnuto): kontrola přítomnosti [potenciálně nežádoucích programů](#) (spustitelné programy, které mohou fungovat jako spyware nebo adware). Zaškrtnutím tohoto políčka aktivujete [Anti-Spyware](#), tj. bude se testovat přítomnost spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, protože i když v tšinu tchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány v domě a se souhlasem uživatele. Doporučujeme nicméně ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
 - **Hlásit rozšířenou množinu potenciálně nežádoucích programů** (ve výchozím nastavení vypnuto) - zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně můžete blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.
 - **Kontrolovat tracking cookies** (ve výchozím nastavení vypnuto) - parametr komponenty [Anti-Spyware](#) definuje, že během testu mají být detekovány cookies (HTTP data zaslaná serverem prohlížeči a uložena na počítači uživatele; při každé další návštěvě téhož serveru prohlížeč posílá cookies zpět serveru, který podle nich

rozlišuje jednotlivé uživatele).

- **Testovat archivy** (ve výchozím nastavení zapnuto) - parametr definuje, že test má kontrolovat všechny soubory zabalené v n kterém typu archivu, například ZIP, RAR, ...
 - **Použit heuristickou analýzu** (ve výchozím nastavení zapnuto) - během testu bude použita k detekci infekce i metoda heuristické analýzy (*dynamické emulace instrukcí testovaného objektu v prostředí virtuálního počítače*).
 - **Testovat systémové prostředí** (ve výchozím nastavení vypnuto) - test provádí i systémové oblasti vašeho počítače.
 - **Povolit testování s extrémní citlivostí** (ve výchozím nastavení vypnuto) - ve specifických situacích (při podezření na infekci zavlečenou do vašeho počítače) můžete zvolit tuto metodu testování, která aktivuje nejdokladnější testovací algoritmy a velmi podrobně provádí naprosto všechny oblasti vašeho počítače. Mějte však na paměti, že tato metoda je časově velmi náročná.
- **Další nastavení testu** - odkaz otevírá dialog **Další nastavení testu**, kde můžete definovat následující parametry testu:

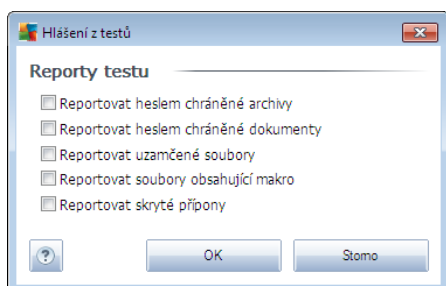


- **Možnosti vypnutí počítače** - určete, zda má být počítač po dokončení testu automaticky vypnut. Pokud potvrdíte tuto možnost (**Vypnout počítač po dokončení testování**), aktivuje se nová volba (**Vynutit vypnutí počítače, pokud je uzamčen**), při jejímž potvrzení dojde po dokončení testu k vypnutí počítače a tehdy, jestliže je počítač momentálně zamknut.
- **Zvolte typy souborů pro testování** - dále se můžete rozhodnout, zda si přejete testovat
 - **Všechny typy souborů** - pokud máte zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou;
 - **Vybrané typy souborů** - můžete se rozhodnout, že chcete, aby se testy

spouštěly pouze nad soubory, které lze považovat za infikovatelné (soubory, které nemohou být infekcí zasaženy, se testovat nebudou - například prosté textové soubory nebo některé nespustitelné soubory), a to včetně multimediálních souborů (video, audio soubory - ponecháte-li tuto položku neoznámenou, výrazně se tím zkrátí čas testování, jelikož multimediální soubory jsou obvykle poměrně velké, ale pravděpodobnost infekce je u nich velmi nízká). I zde můžete určit výjimky a pomocí seznamu připín definovat, které soubory mají být testovány za všech okolností.

➤ U položky **Testovat soubory bez připín** pak rozhodnete, zda se mají testovat i soubory se skrytou příponou nebo i s neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme, abyste se tohoto nastavení drželi, pokud nemáte skutečnou důvod jej změnit. Soubory bez připín jsou obecně vysoce podezřelé a měly by být otestovány.

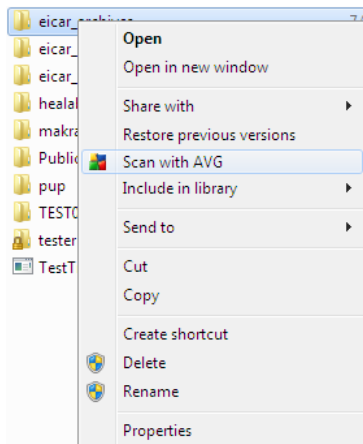
- **Priorita testu** - posuvníkem lze změnit prioritu testu. Ve výchozím nastavení je tato hodnota nastavena *dle inosti uživatele*, čímž optimalizuje rychlost testu prioritou a využitím systémových zdrojů. Test můžete spustit pomaleji a tedy s nižší zátěží systémových zdrojů (vhodné, pokud potřebujete během testu na počítači pracovat a nezáleží vám tolik na celkové době testování) nebo naopak rychleji s vyššími nároky na systémové zdroje (například v době, kdy na počítači nikdo nepracuje).
- **Nastavit další reporty testu** - odkaz otevírá nový dialog **Reporty testu**, v němž můžete označit, které typy nálezů mají být hlášeny:



Upozornění: Samotné možnosti nastavení testu jsou shodné s parametry nově definovaného testu, které jsou podrobně popsány v kapitole [AVG testování / Naplňování testu / Jak testovat](#). Pokud se rozhodnete výchozí nastavení **Testu vybraných souborů** i složek změnit, můžete pak svou konfiguraci uložit jako výchozí, takže každý další **Test vybraných souborů** nebo složek bude spuštěn s tímto nastavením a konfigurace bude také použita jako šablona pro všechny další vámi definované testy ([všechny vlastní testy vycházejí z aktuálního nastavení Testu vybraných souborů i složek](#)).

10.3. Testování v průzkumníku Windows

AVG Anti-Virus 2011 nabízí kromě přednastavených testů spuštěných nad celým počítačem nebo jeho vybranými oblastmi i možnost rychlého otestování konkrétního objektu přímo v prostředí průzkumníka Windows. Chcete-li například otevřít neznámý soubor a nejste si jisti jeho obsahem, můžete nechat tento soubor na vyžádání otestovat. Postup je následující:



- V průzkumníku Windows označte soubor (*nebo adresář*), jehož obsah chcete prověřit
- Kliknutím pravého tlačítka myši nad objektem otevřete kontextové menu
- Volbou položky **Otestovat systémem AVG** - nechte objekt otestovat programem AVG

10.4. Testování z příkazové řádky

V rámci **AVG Anti-Virus 2011** existuje také možnost spustit test z příkazové řádky. Tuto možnost využijete například na serverech nebo třeba při vytváření dávkových skriptů, které mají být spuštěny po startu počítače. Z příkazové řádky můžete spustit test s nastavením v řadě parametrů, které jsou dostupné v grafickém rozhraní AVG.

Test z příkazové řádky spustíte z adresáře, kde je nainstalovaný program AVG pomocí příkazu:

- **avgsca***n*x na 32-bitových OS
- **avgsca***n*a na 64-bitových OS

Syntaxe příkazu

Syntaxe příkazu pro spuštění testu z příkazové řádky je následující:

- **avgsca***n*x /*parametr* ... tedy například **avgsca***n*x /*comp* pro spuštění testu celého počítače
- **avgsca***n*x /*parametr* /*parametr* .. při použití více parametrů jsou tyto uvedeny za sebou a odděleny mezerou a lomítkem
- pokud parametr vyžaduje uvedení konkrétní hodnoty (například parametr **/scan** pro otestování vybraných oblastí počítače, kde musíte uvést cestu k testované oblasti), jsou jednotlivé hodnoty od sebe odděleny středníkem, například: **avgsca***n*x /*scan=C:\;D:*

Parametry příkazu



Kompletní přehled použitelných parametrů lze zobrazit příkazem pro příslušný test s parametrem /? nebo /HELP (např. **avgscanx /?**). Jediným povinným parametrem testu je /SCAN, případně /COMP, kterými určíte oblasti počítače, jež se mají testovat. Podrobný popis dostupných parametrů najdete v kapitole [Parametry CMD testu](#).

Test spustíte stiskem klávesy **Enter**. V průběhu testu lze testování zastavit stiskem kláves **Ctrl+C** nebo **Ctrl+Pause**.

Spuštění CMD testu z grafického rozhraní

Při spuštění počítače v nouzovém režimu Windows je dostupná i možnost spuštění testu z příkazové řádky prostřednictvím dialogu grafického rozhraní. Samotný text bude spuštěn z příkazové řádky; dialog **Nastavení testu z příkazové řádky** slouží pouze jako nástroj pro snadné nastavení parametrů testu, aniž byste je museli definovat v prostředí příkazové řádky.

Vzhledem k tomu, že dialog není standardně dostupný a bude zobrazen pouze v nouzovém režimu Windows, jeho podrobný popis najdete v nápovědě dostupné přímo z tohoto dialogu.

10.4.1. Parametry CMD testu

V následujícím přehledu nabízíme seznam dostupných parametrů testu:

- **/SCAN** [Test vybraných souborů i složek](#); /SCAN=path;path (například /SCAN=C:\; D:\)
- **/COMP** [Test celého počítače](#)
- **/HEUR** Použít [heuristickou analýzu](#)
- **/EXCLUDE** Z testu vynechat tuto cestu nebo soubory
- **/@** Příkazový soubor /jméno souboru/
- **/EXT** Testovat pouze soubory s těmito příponami /například EXT=EXE,DLL/
- **/NOEXT** Netestovat soubory s těmito příponami /například NOEXT=JPG/
- **/ARC** Testovat archívy
- **/CLEAN** Automaticky léčit
- **/TRASH** Přesunout infikované soubory do [Virového trezoru](#)
- **/QT** Rychlý test
- **/MACROW** Hlásit makra
- **/PWDW** Hlásit heslem chráněné soubory
- **/IGNLOCKED** Ignorovat zamčené soubory



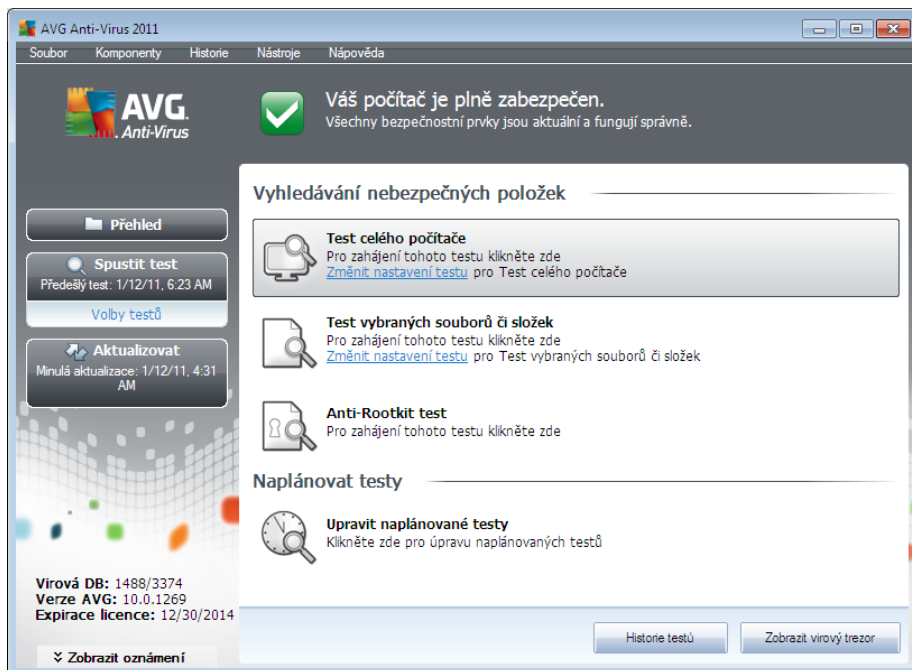
- **/REPORT** Hlásit do souboru /jméno souboru/
- **/REPAPPEND** Přidat k souboru
- **/REPOK** Hlásit neinfikované soubory jako OK
- **/NOBREAK** Nepovolit přerušení testu pomocí CTRL-BREAK
- **/BOOT** Povolit kontrolu MBR/BOOT
- **/PROC** Testovat aktivní procesy
- **/PUP** Hlásit "[Potenciálně nebezpečné programy](#)"
- **/REG** Testovat registry
- **/COO** Testovat cookies
- **/?** Zobrazit nápovědu k tomuto tématu
- **/HELP** Zobrazit nápovědu k tomuto tématu
- **/PRIORITY** Nastavit prioritu testu /Low, Auto, High/ (viz [Pokročilé nastavení / Testy](#))
- **/SHUTDOWN** Vypnout počítač po dokončení testu
- **/FORCESHUTDOWN** Vynutit vypnutí počítače po dokončení testu
- **/ADS** Testovat alternativní datové proudy (pouze NTFS)
- **/ARCBOMBSW** Hlásit opakovaně komprimované archivní soubory

10.5. Naplánování testu

Testy v **AVG Anti-Virus 2011** lze spouštět buďto na vyžádání (*například v situaci, kdy máte podezření na zavlétí infekce na váš počítač nebo z jiného zdroje*) nebo podle nastaveného plánu. Doporučujeme používat především spouštění testů podle plánu, protože tímto způsobem zajistíte svému počítači dostatečnou prevenci a budete moci pracovat bez starostí o to, zda a kdy test spustit.

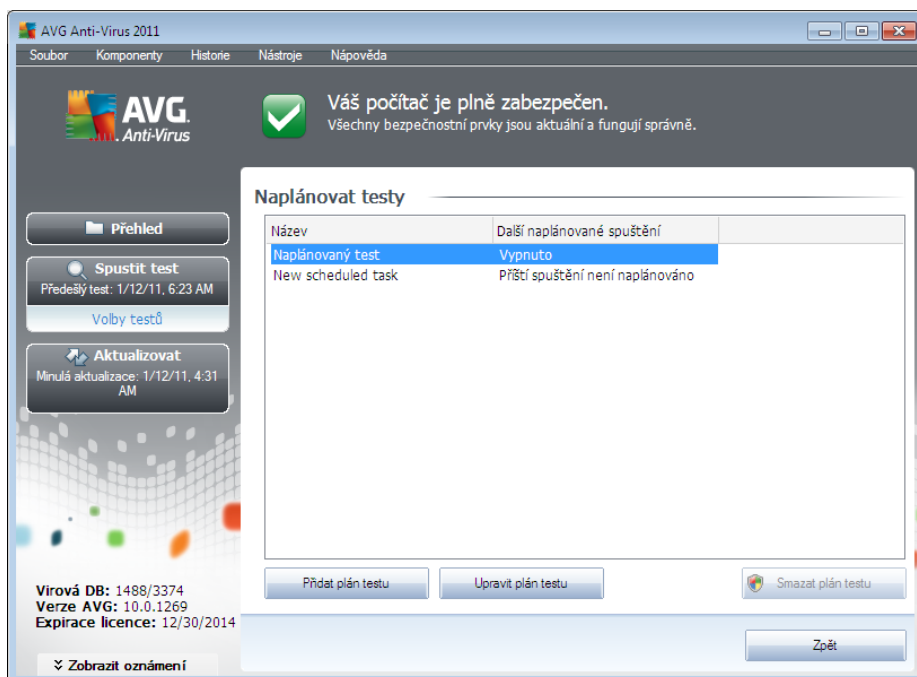
[Test celého počítače](#) by měl být spouštěn pravidelně, a to nejméně jednou týdně. Pokud vám to však provoz na vašem počítači umožní, doporučujeme spouštět test celého počítače jednou denně; tak je také ve výchozí konfiguraci nastaven plán testů. Jestliže je počítač trvale zapnutý, je vhodné naplánovat spuštění **Testu celého počítače** na dobu mimo pracovní hodiny. Pokud počítač vypínáte, nezapomeňte využít možnosti [spustit test při startu počítače, pokud byl naplánovaný a s úspěchem](#).

Plán testů lze vytvářet v [testovacím rozhraní AVG](#), kde ve spodní části dialogu najdete sekci nazvanou **Naplánovat testy**.



Naplánovat testy

Kliknutím na grafickou ikonu v sekci **Naplánovat testy** otevře nový dialog **Naplánovat testy**, v něm můžete najít přehled všech aktuálně naplánovaných testů :

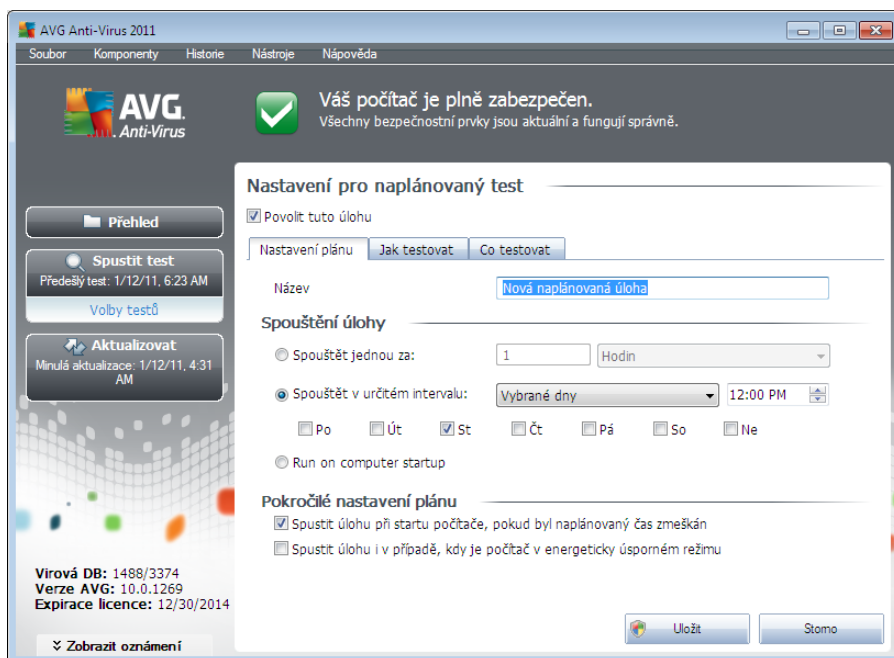


Pracovat můžete s těmito ovládacími tlačítky:

- **P idat plán testu** - tlačítkem otevřete dialog **Nastavení pro naplánovaný test**, na záložce **Nastavení plánu**. V tomto dialogu máte možnost specifikovat parametry nově definovaného testu.
- **Upravit plán testu** - tlačítkem můžete být použito pouze v případě, že jste ze seznamu naplánovaných testů vybrali již existující test. V takovém případě se tlačítko zobrazí jako aktivní a kliknutím na něj se přepnete do dialogu **Nastavení pro naplánovaný test**, na záložku **Nastavení plánu**. Zde jsou již zadány parametry stávajícího testu, které můžete editovat.
- **Smazat plán testu** - tlačítko je rovněž aktivní pouze v případě, že jste ze seznamu naplánovaných testů vybrali již existující test. Ten pak můžete být stiskem tlačítka zrušen. Odebírat však můžete jen své vlastní nastavené plány; **Plán testu celého počítače**, který je nastaven jako výchozí, smazat nelze.
- **Zpět** - návrat do [testovacího rozhraní AVG](#)

10.5.1. Nastavení plánu

Chcete-li naplánovat nový test a jeho pravidelné spuštění, vstupte do dialogu **Nastavení pro naplánovaný test** (kliknutím na tlačítko **P idat plán testu** v dialogu **Naplánování testu**). Dialog je rozdělen do tří záložek: **Nastavení plánu** - viz obrázek (výchozí záložka, na kterou budete automaticky přecházet), **Jak testovat** a **Co testovat**.



Na záložce **Nastavení plánu** máte nejprve možnost jednoduchým označením položky **Povolit tuto úlohu** naplánovaný test (dočasně) deaktivovat, a později podle potřeby znovu použít.

Dále pojmenujte test, který chcete vytvořit a naplánovat. Jméno testu zadejte do textového pole u položky **Název**. Snažte se používat stručné a souhlasné výstižné názvy testů, abyste později snadno rozeznali, o jaký test se jedná.



Příklad: Nevhodným názvem testu je například "Nový test" nebo "Martin v test", protože ani jeden název nepovídá o tom, co test ve skutečnosti kontroluje. Naproti tomu správným popisným názvem testu může být například "Test systémových oblastí" nebo "Test disku C:" a podobně. Rovněž není nutné označovat testy termíny Test celého počítače versus Test vybraných souborů a složek - vámi nastavený test bude vždy specifickým nastavením testu vybraných souborů a složek.

V tomto dialogu můžete dále definovat tyto parametry testu:

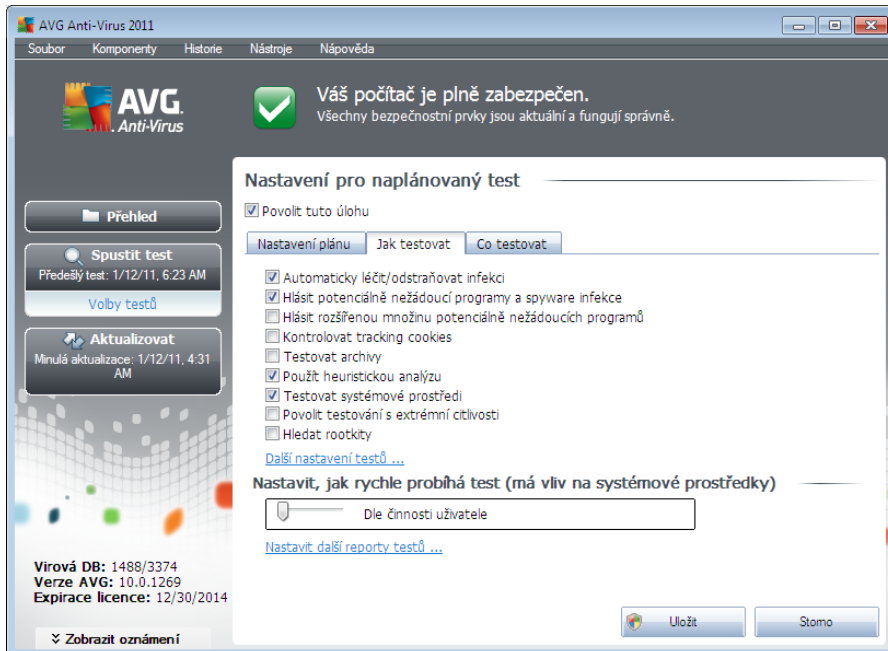
- **Spouštění úloh** - určete, v jakých časových intervalech má být nově naplánovaný test spuštěn. Časové určení můžete zadat buďto opakovaným spuštěním testu po uplynutí určité doby (**Spouštění jednou za**) nebo stanovením přesného data a času (**Spouštění v určitém čase**), případně určením události, na niž se spuštění testu váže (**Spouštění po určité události**).
- **Pokročilé nastavení plánu** - tato sekce umožňuje definovat podmínky, kdy má být spuštěn test, jestliže je počítač v úsporném režimu nebo zcela vypnutý a naplánovaný test spuštění testu byl zmeškán.

Ovládací tlačítka dialogu

Ze všech tlačítek záložek dialogu **Nastavení pro naplánovaný test (Nastavení plánu, Jak testovat a Co testovat)** jsou dostupná dvě ovládací tlačítka, jež mají stejnou funkci na kterékoli záložce dialogu:

- **Uložit** - uloží všechny změny, které jste provedli na této záložce nebo na libovolné jiné záložce dialogu pro nastavení plánu testu a přepne vás zpět do výchozího dialogu testovacího rozhraní AVG. Chcete-li tedy nastavit parametry plánu testu na všech záložkách, uložte je stiskem tohoto tlačítka teprve poté, co jste zadali všechny své požadavky.
- **Storno** - zruší veškeré změny, které jste provedli na této záložce nebo na libovolné jiné záložce dialogu pro nastavení plánu testu a přepne vás zpět do výchozího dialogu testovacího rozhraní AVG.

10.5.2. Jak testovat



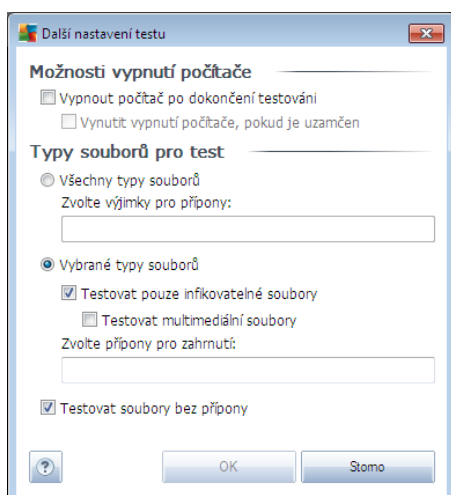
Záložka **Jak testovat** nabízí seznam parametrů testu, které můžete podle potřeby vypínat/zapínat. Ve výchozím nastavení je většina parametrů zapnuta a budou tak během testu automaticky použity. Pokud nemáte skutečný důvod konfiguraci testu změnit, doporučujeme se držet výrobcem definovaného nastavení:

- **Automaticky léčit/odstraňovat infekci** - (ve výchozím nastavení zapnuto): je-li během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. Pokud virus automaticky léčit nelze, anebo pokud se rozhodnete tuto funkci vypnout, budete o nálezu viru vyrozuměni a můžete rozhodnout, co se má dále s infikovaným objektem provést. Doporučeným postupem je přesunutí objektu do [Virového trezoru](#).
- **Hlásit potenciálně nežádoucí programy a spyware infekce** - (ve výchozím nastavení zapnuto) kontrola přítomnosti [potenciálně nežádoucích programů](#) (spustitelné programy, které mohou fungovat jako spyware nebo adware). Zaškrtnutím tohoto políčka aktivujete [Anti-Spyware](#), tj. bude se testovat přítomnost spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány v domě a se souhlasem uživatele. Doporučujeme nicméně ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
- **Hlásit rozšířenou množinu potenciálně nežádoucích programů** - (ve výchozím nastavení vypnuto): zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.

- **Kontrolovat tracking cookies** - (ve výchozím nastavení vypnuto): parametr komponenty [Anti-Spyware](#) definuje, že během testu mají být detekovány cookies (*HTTP data zaslaná serverem prohlížeči a uložena na počítači uživatele; při každé další návštěvě téhož serveru prohlížeč posílá cookies zpět serveru, který podle nich rozlišuje jednotlivé uživatele*).
- **Testovat archivy** - (ve výchozím nastavení vypnuto): parametr definuje, že test má kontrolovat všechny soubory, a to i takové, které jsou zabaleny v některém typu archivu, například ZIP, RAR, ...
- **Použít heuristickou analýzu** - (ve výchozím nastavení zapnuto): během testu bude použita k detekci infekce i metoda heuristické analýzy (*dynamické emulace instrukcí testovaného objektu v prostředí virtuálního počítače*).
- **Testovat systémové prostředí** - (ve výchozím nastavení zapnuto): test provádí i systémové oblasti vašeho počítače.
- **Povolit testování s extrémní citlivostí** (ve výchozím nastavení vypnuto) - ve specifických situacích (při podezření na infekci ve vašem počítači) můžete zvolit tuto metodu testování, která aktivuje nejdokladnější testovací algoritmy a velmi podrobně provádí naprosto všechny oblasti vašeho počítače. Mějte však na paměti, že tato metoda je časově velmi náročná.
- **Hledat rootkity** - (ve výchozím nastavení vypnuto): označením této položky zahrnete do testu i možnost detekce rootkitu, která je jinak samostatně dostupná v rámci komponenty [Anti-Rootkit](#).

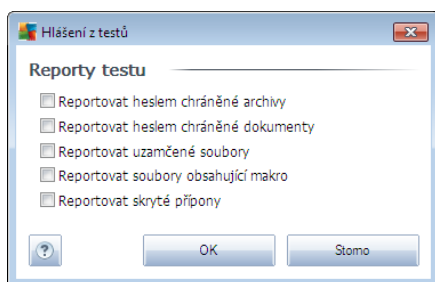
Dále máte možnost upravit konfiguraci testu tímto nastavením:

- **Další nastavení testu** - odkaz otevírá dialog **Další nastavení testu**, kde můžete definovat následující parametry testu:



- **Možnosti vypnutí počítače** - určete, zda má být počítač po dokončení testu automaticky vypnut. Pokud potvrdíte tuto možnost (**Vypnout počítač po dokončení testování**), aktivuje se nová volba (**Vynutit vypnutí počítače, pokud je uzamčen**), při jejímž potvrzení dojde po dokončení testu k vypnutí počítače i tehdy, jestliže je počítač momentálně zamknut.

- **Zvolte typy soubor pro testování** - dále se můžete rozhodnout, zda si přejete testovat
 - **Všechny typy soubor** - pokud vám má být zároveň poskytnuta možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou;
 - **Vybrané typy soubor** - můžete se rozhodnout, že chcete, aby se testy spouštěly pouze nad soubory, které lze považovat za infikovatelné (*soubory, které nemohou být infekcí zasaženy, se testovat nebudou - například prosté textové soubory nebo některé nespustitelné soubory*), a to včetně multimediálních souborů (*video, audio soubory - ponecháte-li tuto položku neoznačenou, výrazně se tím zkrátí čas testování, jelikož multimediální soubory jsou obvykle poměrně velké, ale pravděpodobnost infekce je u nich velmi nízká*). I zde můžete určit výjimky a pomocí seznamu přípon definovat, které soubory mají být testovány za všech okolností.
 - U položky **Testovat soubory bez přípon** pak rozhodnete, zda se mají testovat i soubory se skrytou nebo neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme, abyste se tohoto nastavení drželi, pokud nemáte skutečnou důvod jej změnit. Soubory bez přípon jsou obecně vysoce podezřelé a měly by být otestovány.
- **Nastavit, jak rychle probíhá test** - posuvníkem lze změnit prioritu testu. Ve výchozím nastavení je tato hodnota nastavena *dle inerce uživatele*, čímž optimalizuje rychlost testu podle zátěže a vytížení systémových zdrojů. Test můžete spustit pomaleji a tedy s nižší zátěží systémových zdrojů (*vhodné, pokud potěbujete během testu na počítači pracovat a nezáleží vám tolik na celkové době testování*) nebo naopak rychleji s vyššími nároky na systémové zdroje (*například v době, kdy na počítači nikdo nepracuje*).
- **Nastavit další reporty test** - odkaz otevírá nový dialog **Reporty test**, v němž můžete označit, které typy nálezů mají být hlášeny:



Ovládací tlačítka dialogu

Ze všech tří záložek dialogu **Nastavení pro naplánovaný test** ([Nastavení plánu](#), [Jak testovat](#) a [Co testovat](#)) jsou dostupná dvě ovládací tlačítka, jež mají stejnou funkci na kterékoli záložce dialogu:

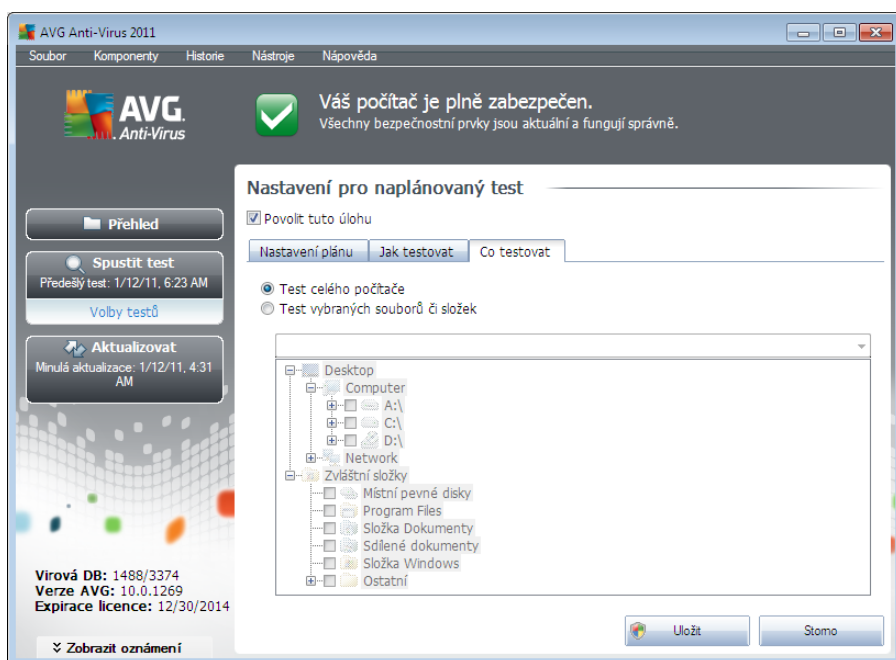
- **Uložit** - uloží všechny změny, které jste provedli na této záložce nebo na libovolné jiné záložce dialogu pro nastavení plánu testu a přepne vás zpět do [výchozího dialogu testovacího rozhraní AVG](#). Chcete-li tedy nastavit parametry plánu testu na všech



záložkách, uložte je stiskem tohoto tlačítka teprve poté, co jste zadali všechny své požadavky.

- **Storno** - zruší veškeré změny, které jste provedli na této záložce nebo na libovolné jiné záložce dialogu pro nastavení plánu testu a přepne vás zpět do [výchozího dialogu testovacího rozhraní AVG](#).

10.5.3. Co testovat



Na záložce **Co testovat** definujete, zda si přejete naplánovat [Test celého počítače](#) nebo [Test vybraných souborů a složek](#).

V případě, že se rozhodnete pro test vybraných souborů a složek, ve spodní sekci dialogu se aktivuje zobrazená stromová struktura vašeho disku a v ní můžete označit adresáře, jejichž obsah má být testován (*jednotlivé položky otevřete kliknutím na plusové znaménko dokud nenajdete požadovaný adresář*). Je také možné zvolit více adresářů označením několika příslušných zaškrtnávacích políček. Zvolené adresáře se následně zobrazí v textovém poli v horní části dialogového okna a pomocí rozbalovací nabídky se můžete vrátit k seznamu vašich předchozích výběrů. Existuje i druhá alternativa: můžete zadat cestu ke konkrétnímu adresáři přímo do textového pole ručně (*zadáte-li více cest souasně, oddíle je středníkem bez mezer*).

V zobrazené stromové struktuře je zahrnuta také vtevs označením **Zvláštní složky**. V ní najdete následující položky, jež odpovídají uvedeným lokacím, které budou při označení testovány:

- **Místní pevné disky** - všechny pevné disky počítače
- **Program files**
 - o C:\Program Files\



- o v 64-bitové verzi C:\Program Files (x86)

- **Složka Dokumenty**

- o pro Win XP: C:\Documents and Settings\Default User\My Documents\
- o pro Windows Vista/7: C:\Users\user\Documents\

- **Sdílené dokumenty**

- o pro Win XP: C:\Documents and Settings\All Users\Documents\
- o pro Windows Vista/7: C:\Users\Public\Documents\

- **Složka Windows** - C:\Windows\

- **Ostatní**

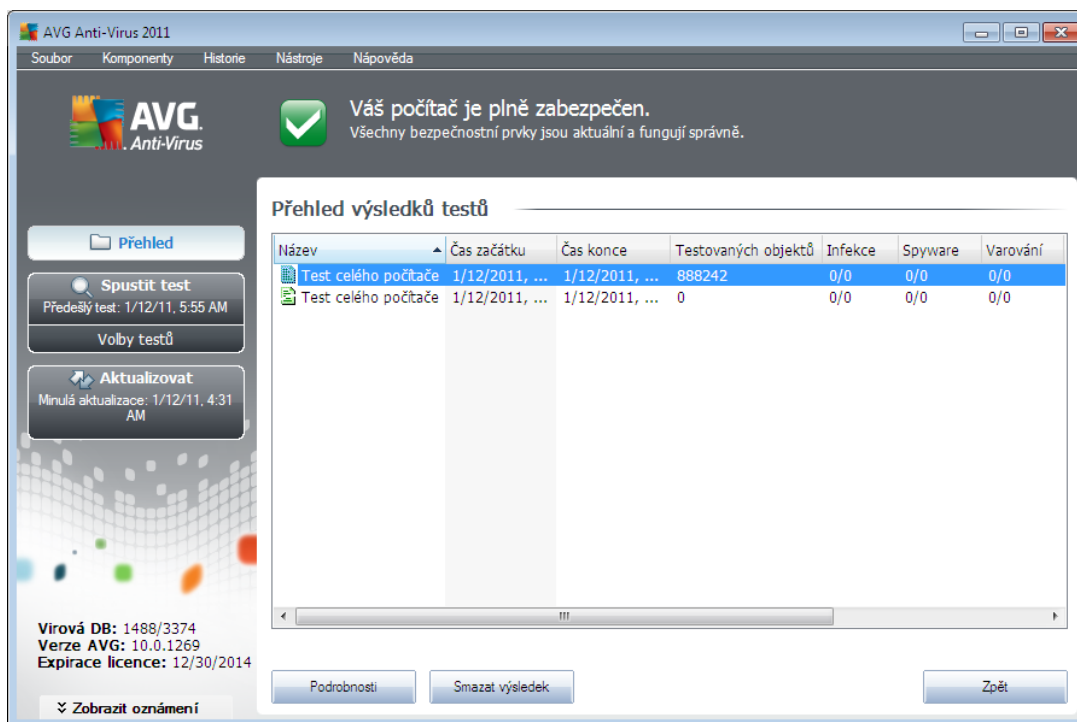
- o Systémový disk - pevný disk, na němž je instalován operační systém (obvykle C:)
- o Systémová složka - C:\Windows\System32\
- o Složka dočasných souborů - C:\Documents and Settings\User\Local\ (Windows XP) nebo C:\Users\user\AppData\Local\Temp\ (Windows Vista/7)
- o Temporary Internet Files - C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (Windows XP) nebo C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (Windows Vista/7)

Ovládací tlačítka dialogu

Ze všech tří záložek dialogu **Nastavení pro naplánovaný test** ([Nastavení plánu](#), [Jak testovat a Co testovat](#)) jsou dostupná dvě ovládací tlačítka, jež mají stejnou funkci na kterékoli záložce dialogu:


- **Uložit** - uloží všechny změny, které jste provedli na této záložce nebo na libovolné jiné záložce dialogu pro nastavení plánu testu a přepne vás zpět do [výchozího dialogu testovacího rozhraní AVG](#). Chcete-li tedy nastavit parametry plánu testu na všech záložkách, uložte je stiskem tohoto tlačítka teprve poté, co jste zadali všechny své požadavky.
- **Storno** - zruší veškeré změny, které jste provedli na této záložce nebo na libovolné jiné záložce dialogu pro nastavení plánu testu a přepne vás zpět do [výchozího dialogu testovacího rozhraní AVG](#).


10.6. Přehled výsledků testů




Dialog **Přehled výsledků testů** je dostupný z [testovacího rozhraní AVG](#) tlačítkem **Historie testů**. V tomto dialogu je zobrazen seznam všech dříve spuštěných testů společně s informacemi o jejich průběhu a výsledku:

- **Název** - označením testu může být buďto název jednoho z [přednastavených testů](#) nebo název, kterým jste sami označili [vlastní test](#). Každý název je předznamenán ikonou, která informuje o výsledku testu:

 - zelená ikona informuje, že během testu nebyla detekována žádná infekce

 - modrá ikona oznamuje, že během testu byla detekována infekce, ale podařilo se ji automaticky odstranit

 - červená ikona je varováním, že během testu byla detekována infekce, kterou se nepodařilo odstranit!

Ve všech případech může být ikona buďto celistvá nebo poloplená - celá ikona znamená, že test proběhl celý a byl úspěšně ukončen, poloplená ikona identifikuje nedokončený nebo přerušovaný test.

Poznámka: Podrobné informace o každém testu najdete v dialogu [Výsledky testů](#) dostupném přes tlačítko **Podrobnosti** (ve spodní části tohoto dialogu).

- **čas začátku** - datum a přesný čas spuštění testu



- **as konce** - datum a přesný čas ukončení testu
- **Testovaných objekt** - počet objektů, které byly během testu zkontrolovány
- **Infekce** - číslo udává počet nalezených / odstraněných [virových infekcí](#)
- **Spyware** - počet detekovaného / odstraněného [spyware](#)
- **Varování** - počet detekovaných [podezřelých objektů](#)
- **Rootkity** - počet detekovaných rootkitů
- **Informace testovacího protokolu** - údaje o průběhu testu, zejména o jeho základním i předepsaném ukončení

Ovládací tlačítka dialogu

Ovládacími tlačítky pro dialog **Přehled výsledků testu** jsou:

- **Podrobnosti** - stiskem tlačítka pak přejdete do dialogu [Výsledky testu](#), kde se zobrazí podrobné informace o testu zvoleném v přehledu
- **Smazat výsledek** - stiskem tlačítka můžete záznam o zvoleném testu v přehledu testů odstranit
- **Zpět** - přepíná zpět do výchozího dialogu [testovacího rozhraní](#)

10.7. Detail výsledku testu

Jestliže v dialogu [Přehled výsledků testu](#) vyberete jeden test ze seznamu a označíte jej, můžete stiskem tlačítka **Podrobnosti** přejít do dialogu **Výsledky testu**, v němž jsou zobrazeny detailní informace o průběhu a výsledku zvoleného testu.

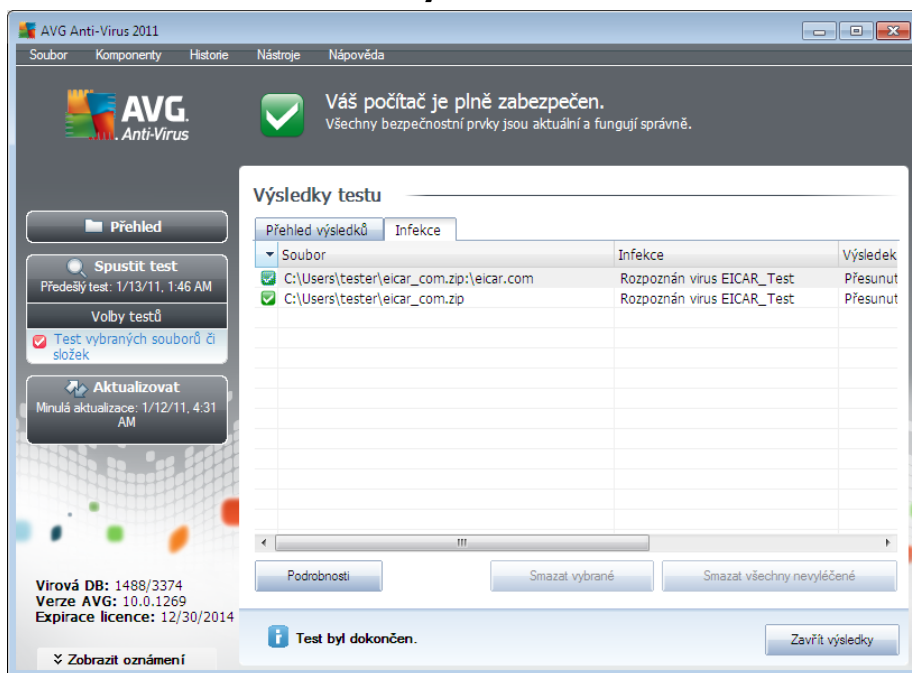
Dialog **Výsledky testu** je dále rozdělen na několik záložek:

- [Přehled výsledků](#) - záložka se zobrazuje vždy a nabízí statistická data popisující průběh testu
- [Infekce](#) - záložka se zobrazuje podmíněně tehdy, když byla během testu detekována [virová infekce](#)
- [Spyware](#) - záložka se zobrazuje podmíněně tehdy, když byl během testu detekován [spyware](#)
- [Varování](#) - záložka se zobrazuje podmíněně s upozorněním na výskyt cookies
- [Rootkity](#) - záložka se zobrazuje podmíněně tehdy, když byl během testu detekován [rootkit](#)
- [Informace](#) - záložka se zobrazuje podmíněně a zobrazuje informace (*typicky varování*)



upozornění) o nálezích, které mohou být potenciálně nebezpečné, ale nelze je klasifikovat jako konkrétní typ infekce. Rovněž se zde zobrazí případně nalezené objekty, které nemohly být otestovány (například zaheslované archivy).

10.7.1. Záložka Přehled výsledků



Na záložce **Přehled výsledků** najdete podrobnou statistiku testu s informacemi o:

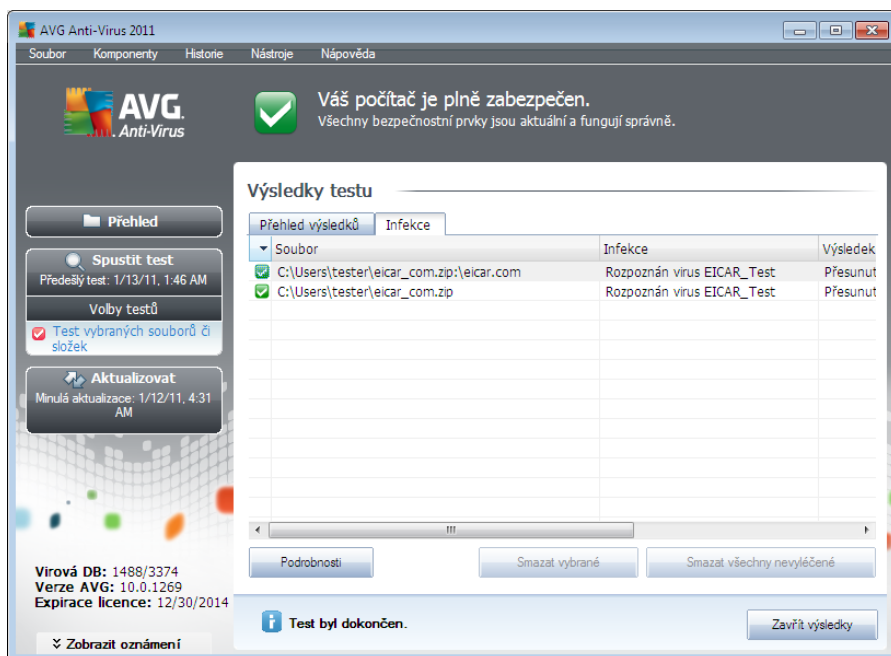
- detekovaných [virových infekcích](#) / [spyware](#)
- vyléčených [virových infekcích](#) / [spyware](#)
- počet [virových infekcích](#) / [spyware](#), které se nepodařilo odstranit nebo vyléčit

Dále jsou uvedeny informace o datu a době spuštění testu, celkovém počtu otestovaných objektů, o době trvání testu a počet chyb, k nimž během testu došlo.

Ovládací tlačítka dialogu

V dialogu je dostupné jediné ovládací tlačítko **Zpět**, kterým se vrátíte do dialogu [Přehled výsledků testu](#).

10.7.2. Záložka Infekce



Záložka **Infekce** se v dialogu **Výsledky testu** zobrazuje podmíněně v případě, že během testu byla detekována [vírová infekce](#). Záložka je rozdělena do tří sekcí a uvádí následující informace:

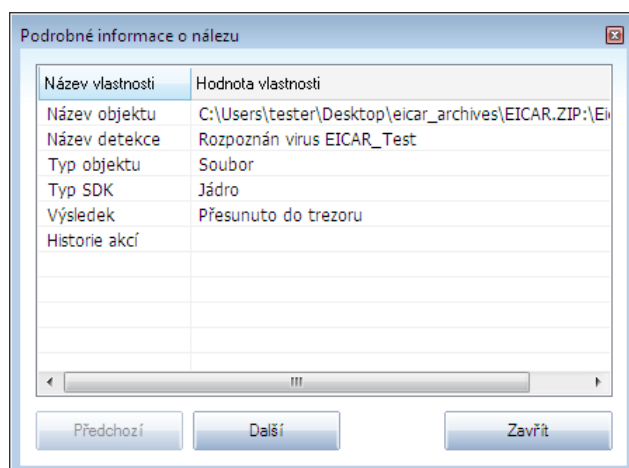
- **Soubor** - plná adresa povodního umístění infikovaného objektu na lokálním disku
- **Infekce** - jméno detekovaného [viru](#) (*podrobnosti o jednotlivých virech najdete ve [Virové encyklopedii](#)*)
- **Výsledek** - uvádí, v jakém stavu se infikovaný a během testu detekovaný objekt aktuálně nachází:
 - **Infikováno** - infikovaný objekt byl rozpoznán a zůstává ve svém povodním umístění (*například pokud máte v nastavení konkrétního testu [vypnutou možnost automatického léčení](#)*)
 - **Vyléno** - infikovaný objekt byl automaticky vyléno a ponechán ve svém povodním umístění
 - **Přesunuto do trezoru** - infikovaný objekt byl přesunut do bezpečného prostoru [Virového trezoru](#)
 - **Smazáno** - infikovaný objekt byl smazán
 - **Obnoveno** - objekt byl obnoven z [Virového trezoru](#) zpět do povodního umístění
 - **Přidáno k výjimkám PUP** - nález byl vyhodnocen jako výjimka a připojen k seznamu výjimek PUP (*výjimky lze editovat v dialogu [PUP výjimky](#) pokračujícího nastavení*)

- **Zam ený soubor - neotestován** - objekt je zam ený a nebylo možno jej otestovat
- **Potenciáln nebezpe ný objekt** - objekt je detekován jako potenciáln nebezpe ný, ale nikoli infikovaný (*m že nap íklad obsahovat makra*). Informace má tedy pouze charakter upozorn ní.
- **Pro dokon ení akce je pot eba provést restart** - infikovaný objekt nebylo možno odstranit, pro jeho odstran ní je t eba provést restart počíta e

Ovládací tlačítka dialogu

V dialogu jsou dostupná tato tlačítka:

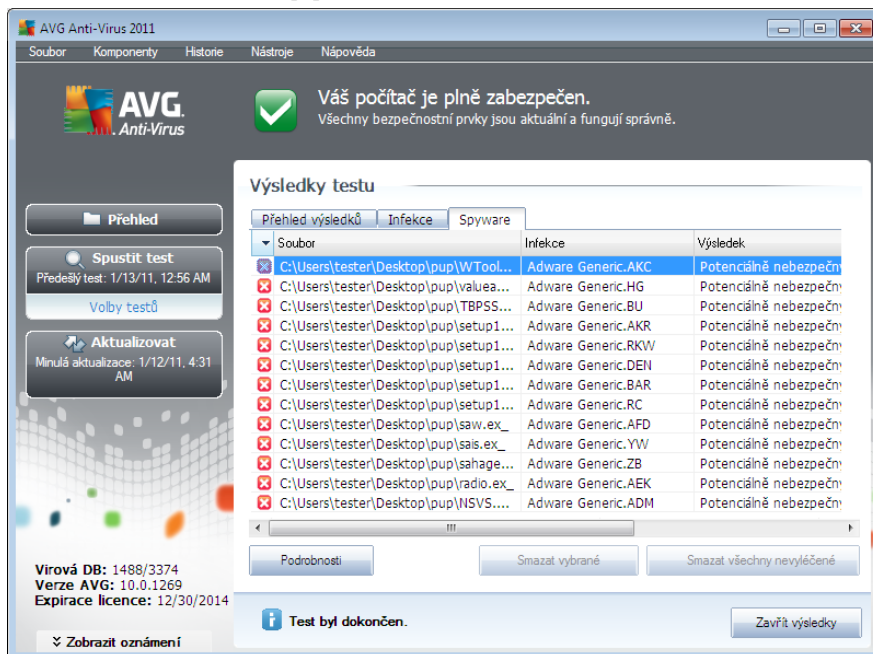
- **Podrobnosti** - tlačítko otevírá nové dialogové okno **Podrobné informace o nálezů**:



V tomto dialogu najdete detailní informace o infekci (*nap íklad umíst ní a jméno detekovaného infikovaného objektu, typ objektu, typ SDK, výsledek detekce a historii akcí provedených nad detekovaným objektem*). Pomocí tlačítek **Předchozí** / **Další** můžete postupně zobrazovat informace o jednotlivých nálezech. Tlačítkem **Zavřít** dialog zavřete.

- **Smazat vybrané** - tlačítkem přesunete v seznamu ozna ený nález do [Virového trezoru](#)
- **Smazat všechny nevylé ené** - tlačítko odstraní všechny nálezy, které nelze lé it ani nemohou být přesunuty do [Virového trezoru](#)
- **Zavřít výsledky** - zavřít detail výsledku testu a přepíná zp t do dialogu [Přehled výsledků testů](#)

10.7.3. Záložka Spyware



Záložka **Spyware** se v dialogu **Výsledky testu** zobrazuje podmíněně v případě, že během testu byl detekován [spyware](#). Záložka je rozdělena do tří sekcí a uvádí následující informace:

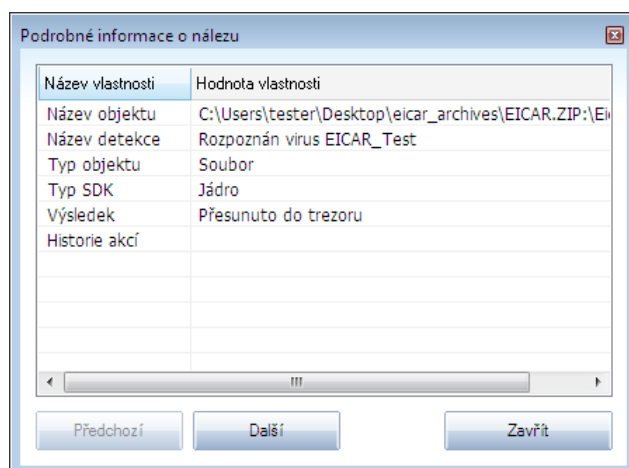
- **Soubor** - plná adresa povodního umístění infikovaného objektu na lokálním disku
- **Infekce** - jméno detekovaného spyware (*podrobnosti o jednotlivých virech najdete ve [Virové encyklopedii](#) online*)
- **Výsledek** - uvádí, v jakém stavu se infikovaný a během testu detekovaný objekt aktuálně nachází:
 - **Infikováno** - infikovaný objekt byl rozpoznán a zůstává ve svém povodním umístění (například pokud máte v nastavení konkrétního testu [vypnutou možnost automatického léčení](#))
 - **Vyléno** - infikovaný objekt byl automaticky vyléno a ponechán ve svém povodním umístění
 - **Přesunuto do trezoru** - infikovaný objekt byl přesunut do bezpečného prostoru [Virového trezoru](#)
 - **Smazáno** - infikovaný objekt byl smazán
 - **Obnoveno** - objekt byl obnoven z [Virového trezoru](#) zpět do povodního umístění
 - **Přidáno k výjimkám PUP** - nález byl vyhodnocen jako výjimka a přidán k seznamu výjimek PUP (*výjimky lze editovat v dialogu [PUP výjimky](#) pokračování nastavení*)

- **Zaměněný soubor** - neotestován - objekt je zaměněný a nebylo možno jej otestovat
- **Potenciálně nebezpečný objekt** - objekt je detekován jako potenciálně nebezpečný, ale nikoli infikovaný (může například obsahovat makra). Informace má tedy pouze charakter upozornění.
- **Pro dokončení akce je třeba provést restart** - infikovaný objekt nebylo možno odstranit, pro jeho odstranění je třeba provést restart počítače

Ovládací tlačítka dialogu

V dialogu jsou dostupná tato tlačítka:

- **Podrobnosti** - tlačítko otevírá nové dialogové okno **Podrobné informace o nálezů**:



V tomto dialogu najdete informaci o infekci (*například umístění a jméno detekovaného infikovaného objektu, typ objektu, typ SDK, výsledek detekce a historii akcí provedených nad detekovaným objektem*). Pomocí tlačítek **Předchozí** / **Následující** můžete postupně zobrazovat informace o jednotlivých nálezech. Tlačítkem **Zavřít** dialog zavřete.

- **Smazat vybrané** - tlačítkem přesunete v seznamu označený nálezu do [Virového trezoru](#)
- **Smazat všechny nevyřezané** - tlačítko odstraní všechny nálezy, které nelze léčit ani nemohou být přesunuty do [Virového trezoru](#)
- **Zavřít výsledky** - zavřít detail výsledku testu a přepíná zpět do dialogu [Přehled výsledků testu](#)

10.7.4. Záložka Varování

Záložka **Varování** zobrazuje informace o "podezřelých" objektech (*nejedná o souborech*) detekovaných během testu. Při kontrole [Rezidentním štítem](#) je k tomuto typu objektů zakázán přístup. Příkladem mohou být skryté soubory, soubory cookies, podezřelé registrové klíče, heslem chráněné dokumenty či archivy, maskovací jména atd. Takovéto soubory nepředstavují problém



hrozbu pro Váš počítač nebo bezpečnost, ale informace o nich může být užitečná v případě adware nebo spyware infekce. Pokud ve výsledku zobrazuje test AVG pouze varování, není třeba provádět žádnou akci.

Nabízíme stručný popis nejčastějších takto detekovaných objektů:

- **Skryté soubory** nejsou ve výchozím nastavení Windows viditelné. Některé viry nebo jiné hrozby se mohou vyhýbat svému odhalení právě použitím tohoto atributu pro své soubory. Pokud AVG reportuje skrytý soubor a vy máte podezření, že je infikován, můžete jej přesunout do [Virového trezoru](#).
- **Cookies** jsou textové soubory používané internetovými stránkami k ukládání uživatelských informací. Ty mohou být využívány pro volbu vlastního vzhledu stránek, vyplnění uživatelského jména, atd.
- **Podezřelé registrované klíče** - některé škodlivé programy ukládají své informace do registru pro zajištění jejich automatického spuštění po startu počítače, nebo pro rozšíření jejich vlivu na operační systém.

10.7.5. Záložka Informace

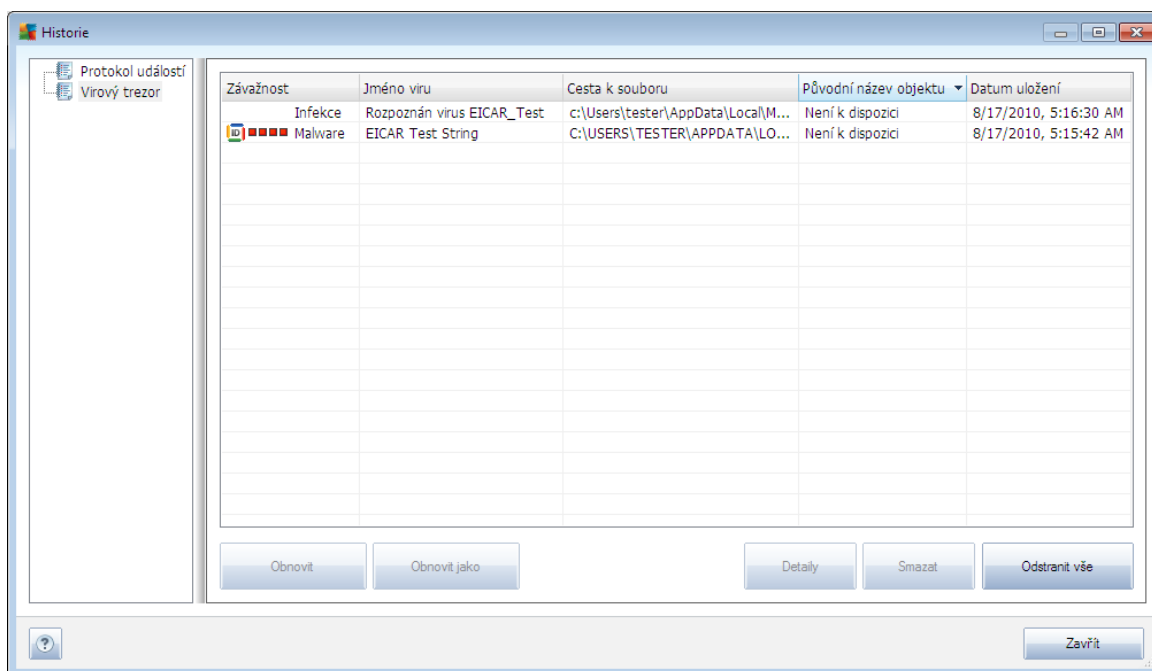
Záložka **Informace** obsahuje údaje o takových "nálezech", které nelze zařadit do kategorie infekcí, spyware, ... ani je pozitivně označit za nebezpečné, přesto zasluhují pozornost. Jsou to tedy soubory, které nejsou infikované, ale mohou být podezřelé. Takové soubory jsou hlášeny jako [Varování](#) nebo jako **Informace**.

Hlášení na záložce **Informace** může být zobrazeno z jednoho z následujících důvodů:

- **Runtime komprese**: Soubor byl zkomprimován jedním z méně běžných runtime kompresorů, což může naznačovat pokus o ochranu před otestováním takového souboru, ale rozhodně nemusí být každý takto hlášený soubor infikovaný.
- **Rekurzní runtime komprese**: Podobné jako v předchozím případě, ovšem méně často při použití u běžných aplikací. Takovéto soubory jsou podezřelé a měli byste zvážit jejich odstranění.
- **Heslem chráněné dokumenty nebo archivy**: Heslem chráněné soubory nemohou být programem AVG (ani jiným bezpečnostním programem) zkontrolovány, proto jsou označeny jako potenciálně nebezpečné.
- **Dokument s makry**: Detekovaný dokument může obsahovat škodlivé makro.
- **Skrytá pípona**: Soubory se skrytou píponou mohou představovat například obrázek, ale také mohou být spustitelné (například `obrazek.jpg.exe`). Druhá pípona je ve výchozím nastavení Windows skrytá. AVG Vás na tyto soubory upozorní, abyste předešli jejich náhodnému spuštění.
- **Soubor spuštěný z nesprávného umístění**: Pokud je některý důležitý systémový soubor spuštěný z jiného než výchozího umístění (například `winlogon.exe` spuštěný z jiné složky než Windows), AVG o této nesrovnalosti informuje. Některé viry skrývají svou přítomnost v systému použitím jmen běžných systémových procesů.

- **Zam ený soubor.** Reportovaný soubor je zam ený, a tedy nemohl být otestován programem AVG. Tato informace ve výsledku test znamená, že soubor je permanentně používán systémem (*nap . stránkový soubor*).

10.8. Virový trezor



Závažnost	Jméno viru	Cesta k souboru	Původní název objektu	Datum uložení
Infekce	Rozpoznán virus EICAR_Test	c:\Users\tester\AppData\Local\M...	Není k dispozici	8/17/2010, 5:16:30 AM
Malware	EICAR Test String	C:\USERS\TESTER\APPDATA\LO...	Není k dispozici	8/17/2010, 5:15:42 AM

Virový trezor je bezpečným prostředím pro správu podezřelých/infikovaných objektů nalezených během testu AVG. Je-li během testu detekován infikovaný objekt a AVG jej nedokáže automaticky vyléčit, budete dotázáni, co se má s tímto objektem provést. Doporučeným řešením je přesunutí objektu do **Virového trezoru** k dalšímu postupu. Hlavním smyslem **Virového trezoru** je udržovat smazané soubory po určitou dobu zejména pro případ, že byly smazány omylem. Pokud zjistíte, že jejich absence způsobuje nějaké problémy, můžete přeslušný soubor odeslat k analýze, nebo jej vrátit zpět do původního umístění.

Rozhraní **Virového trezoru** se otevírá v samostatném okně a nabízí přehled informací o infikovaných objektech uložených v karanténě :

- **Závažnost** - jestliže jste si v rámci instalace programu **AVG Anti-Virus 2011** nainstalovali také komponentu **Identity Protection**, najdete v tomto sloupci grafické znázornění závažnosti infekce přesunutě do karantény na čtyřstupeňové škále v rozptí nezávadný (■□□□) až vysoce rizikový (■□■□); zároveň je zde uvedena informace o typu nález (rozlišuje typy nález podle úrovn jejich infek nosti - objekty mohou být pozitivní / potenciálně infikované)
- **Jméno viru** - uvádí název detekované infekce viru podle **Virové encyklopedie** (on-line)
- **Cesta k souboru** - plná cesta k původnímu umístění souboru, který byl detekován jako

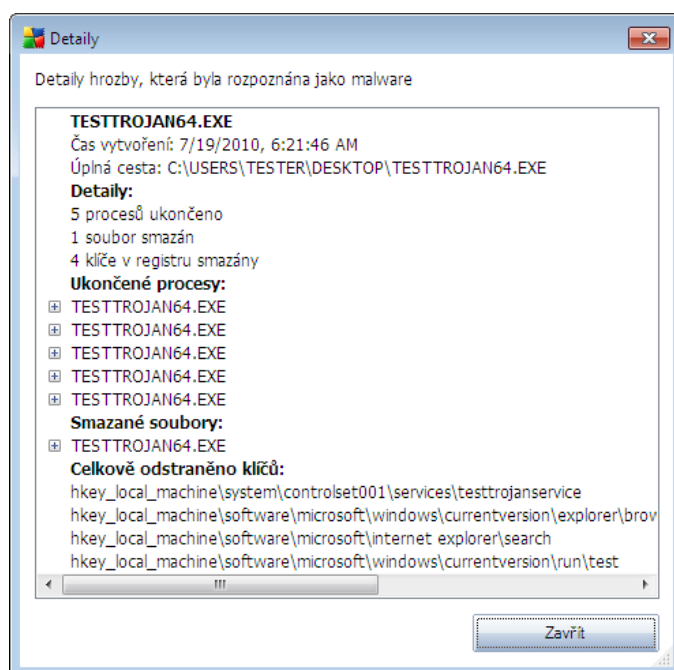
infikovaný, na lokálním disku

- **P vodní název objektu** - všechny detekované objekty v tabulce jsou uvedeny pod standardním jménem, kterým byly označeny během detekce při testování. Pokud má detekovaný objekt své vodní specifické jméno a toto jméno je známo, bude uvedeno v tomto sloupci (například příloha emailu může být označena jménem, které neodpovídá skutečnému detekovanému infekčnímu obsahu, pak budou uvedena obě jména).
- **Datum uložení** - datum a čas detekce infikovaného souboru a jeho přesunutí do **Virového trezoru**

Ovládací tlačítka dialogu

V rozhraní **Virového trezoru** jsou dostupná tato ovládací tlačítka:

- **Obnovit** - přesune infikovaný soubor z Virového trezoru zpět do vodního umístění
- **Obnovit jako** - přesune infikovaný objekt do zvoleného adresáře
- **Detaily** - toto tlačítko se týká pouze objektů nalezených komponentou **Identity Protection**. Po kliknutí se zobrazí pohled detailních informací o této hrozbě (které soubory/procesy byly dotčeny a jak, charakteristika procesu atd.). U jiných objektů než detekcí IDP je toto tlačítko neaktivní!



- **Smazat** - definitivně a nevratně vymaže infikovaný soubor z **Virového trezoru**
- **Odstranit vše** - definitivně vymaže veškerý obsah **Virového trezoru**. Touto volbou jsou všechny soubory z **Virového trezoru** nevratně smazány z disku (nebudou přesunuty do



koše).



11. Aktualizace AVG

Udržování aktuálnosti Vašeho AVG je důležité pro zajištění okamžité detekce všech nových zachycených virů.

Vzhledem k tomu že aktualizace nejsou vydávány podle pevného plánu, ale v reakci na počet a závažnost nových hrozeb, doporučujeme kontrolovat aktualizace alespoň jednou denně nebo častěji. Jedině tak zajistíte, že Váš **AVG Anti-Virus 2011** bude aktuální během celého dne.

11.1. Úrovně aktualizace

AVG rozlišuje dvě úrovně aktualizace:

- **Aktualizace definic** zahrnuje změny nezbytné pro spolehlivé fungování antivirové ochrany. Typicky neobsahuje změny v kódu aplikace a aktualizuje pouze virovou a spyware databázi.
- **Programová aktualizace** zahrnuje různé programové změny a doplňky. U klíčových systémů (souborový server) doporučujeme neprovádět aktualizaci automaticky po jejím vydání, ale nejprve ji otestovat v testovacím prostředí.

Při [nastavování plánu aktualizací](#) je možné zvolit úroveň požadované aktualizace.

Poznámka: Dojde-li k časovému soubihu naplánované programové aktualizace a naplánovaného testu, proces aktualizace je považován za prioritní a test bude přerušeno.

11.2. Typy aktualizace

Podle způsobu provedení aktualizace v rámci AVG rozlišujeme dva typy aktualizací:

- **Aktualizace na vyžádání** je okamžitou aktualizací programu a může být spuštěna kdykoli podle potřeby.
- **Naplánované aktualizace** - v rámci AVG lze také [nastavit plán aktualizací](#). Naplánovaná aktualizace se provádí periodicky podle nastavené konfigurace.

11.3. Průběh aktualizace

Proces aktualizace můžete spustit podle potřeby okamžitě [zkratkovými tlačítkem Aktualizovat](#). Toto tlačítko je vždy dostupné z kteréhokoliv dialogu [uživatelského rozhraní AVG](#). V každém případě doporučujeme provádět aktualizace i v předem určených termínech podle plánu nastaveného v [Manažeru aktualizací](#).

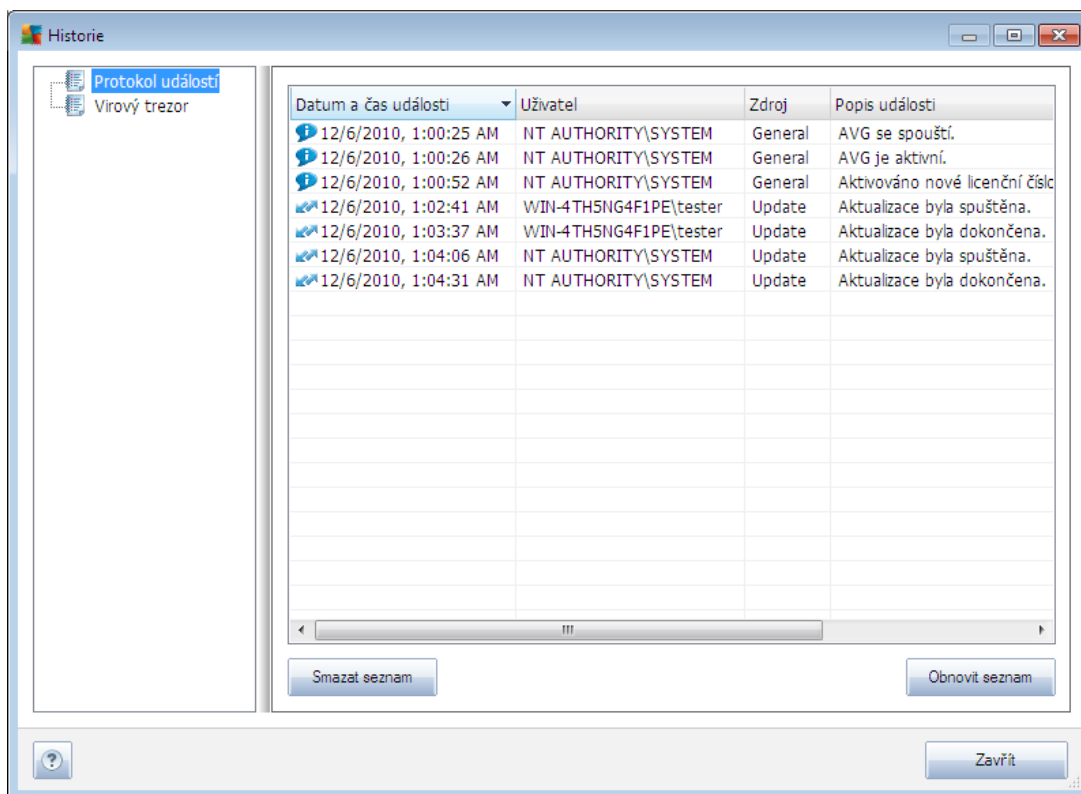
Po spuštění aktualizace dojde nejprve k ověření, zda existují nové aktualizací soubory, jež dosud nebyly aplikovány. Pokud ano, AVG zahájí jejich okamžitou stahování a spustí samotný proces aktualizace. V průběhu tohoto procesu budete přepnuti do rozhraní **Aktualizace**, kde můžete sledovat průběh aktualizace v grafickém zobrazení a současně v přehledu statistických parametrů tohoto procesu (*velikost aktualizací souboru, objem stažených dat, rychlost stahování, doba trvání, ...*).

Poznámka: Před zahájením programové aktualizace AVG dojde k vytvoření "system restore point" (záloha systému), z níž můžete v případě selhání procesu aktualizace a pádu systému váš



OS obnovit v p vodní konfiguraci. Tato možnost je dostupná p ímo v opera ním systému z menu Start / Programy / P íslušenství / Systémové nástroje / Obnova systému. Doporu ujeme pouze zkušeným uživatel m!

12. Protokol událostí



Dialog **Historie** je dostupný volbou položky [systémového menu Historie/Protokol událostí](#). V tomto dialogu najdete přehled všech dležících událostí, které nastaly v průběhu práce **AVG Anti-Virus 2011**. Zaznamenávány jsou události, mezi které patří například:

- informace o aktualizacích programu
- spuštění/ukončení/přerušování testů (včetně testů spuštěných automaticky)
- události týkající se nalezení viru ([testováním](#) i [Rezidentním štítem](#)) s uvedením konkrétního místa nálezů
- ostatní dležitá události

Ke každé události jsou evidovány následující údaje:

- **Datum a čas události** udává přesný datum a čas, kdy se událost odehrála
- **Uživatel**, který byl při hlášení v průběhu události
- **Zdroj** zobrazuje zdrojovou komponentu či jinou část AVG, která událost spustila
- **Popis události** obsahuje stručný popis události



Ovládací tlačítka dialogu

- **Smazat seznam** - vymaže veškeré protokolované záznamy ze seznamu událostí
- **Obnovit seznam** - provede aktualizaci záznamů v seznamu událostí



13. FAQ a technická podpora

Máte-li s Vaší aplikací **AVG Anti-Virus 2011** jakékoliv technické potíže nebo chcete-li položit obchodní dotaz, existuje několik způsobů, jak vyhledat pomoc. Zvolte si prosím některou z následujících možností:

- **Podpora na webu:** Pokud máte z problémů aplikace AVG můžete přejít do specifické sekce webu AVG (<http://www.avg.cz/>), která je vyhrazena zákaznické podpoře. V hlavním menu zvolte položku **Nápověda / Odborná pomoc online**. Budete automaticky přemístěni na příslušnou stránku s nabídkou dostupné podpory. Dále prosím postupujte podle pokynů uvedených na webu.
- **Centrum podpory na webu AVG:** Alternativní možností je vyhledat řešení svého problému na webu AVG (<http://www.avg.cz/>). V sekci **Centrum podpory** najdete strukturovaný přehled tematických okruhů, které řeší problémy obchodního i technického charakteru.
- **Často kladené otázky:** Na webu AVG (<http://www.avg.cz/>) najdete také samostatnou a detailnější sekci často kladených otázek. Tato sekce je dostupná volbou **Centrum podpory / FAQ**. Otázky jsou opět přehledně rozděleny do kategorií obchodní, technické a virové.
- **Informace o virech a hrozbách:** Samostatná kapitola je na webu AVG (<http://www.avg.cz/>) věnována virové tematice (*webová stránka je dostupná prostřednictvím volby Nápověda / Informace o virech v hlavním menu*). Volbou **Centrum podpory / Informace o virech a hrozbách** vstoupíte na stránku, která poskytuje strukturovaný přehled informací souvisejících s hrozbami online. Najdete zde také rady, jak odstranit viry, spyware a jak zůstat trvale chráněni.
- **Diskusní fórum:** Můžete také využít diskusního fóra pro uživatele AVG produktů na adrese <http://forums.avg.com>.