AVG 9 Anti Virus plus Firewall

Uživatelský manuál

Verze dokumentace 90.25 (23.3.2010)

Obsah

1. Úvod

Tento uživatelský manuál je kompletní dokumentací programu **AVG 9 Anti Virus plus Firewall**.

Gratulujeme k vaší volbě programu AVG 9 Anti Virus plus Firewall!

AVG 9 Anti Virus plus Firewall 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 9 Anti Virus plus Firewall** kompletně a od základů přestavěn tak, aby nadále dostál své pověsti uznávaného bezpečnostního programu a současně nabídl svým uživatelům zcela nové, efektivnější a vysoce uživatelsky přívětivé rozhraní.

Nový **AVG 9 Anti Virus plus Firewall** 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 přesně přizpůsobí vašim potřebám.

2. Podmínky instalace AVG

2.1. Podporované operační systémy

AVG 9 Anti Virus plus Firewall je určen k ochraně pracovních stanic s těmito operačními systémy:

- Windows 2000 Professional SP4 + Update Rollup 1
- 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)

2.2. Minimální / doporučené HW požadavky

Minimální hardwarové požadavky pro **AVG 9 Anti Virus plus Firewall**:

- Procesor Intel Pentium 1,5 GHz
- 512 MB RAM paměti
- 390 MB volného místa na pevném disku (*z instalačních důvodů*)

Doporučené hardwarové požadavky pro **AVG 9 Anti Virus plus Firewall**:

- Procesor Intel Pentium 1,8 GHz
- 512 MB RAM paměti
- 510 MB volného místa na pevném disku (*z instalačních důvodů*)

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 9 Anti Virus plus Firewall.

Doporučujeme Vám využít nového nástroje AVG Download Manager, který Vám pomůže sestavit instalační soubor v požadovaném jazyce!

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.

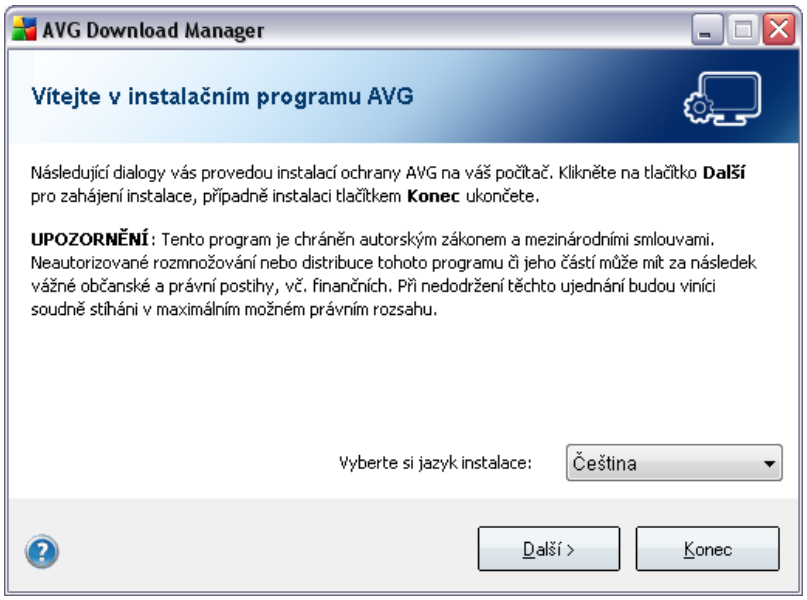
4. AVG Download Manager

AVG Download Manager je jednoduchý nástroj, který Vám pomůže vybrat a sestavit správný instalační balík pro instalaci zkušební verze Vašeho programu AVG. Na základě Vámi uvedených údajů dokáže tento nástroj zvolit správný typ produktu, typ licence, požadované komponenty a jazykovou verzi. Poté **AVG Download Manager** stáhne příslušné instalační balíky a spustí samotný proces instalace programu AVG.

Poznámka: *AVG Download Manager není určen pro stahování instalačního souboru síťových a SBS edicí a je podporován pouze na těchto operačních systémech: Windows 2000 (SP4 + SRP roll-up), Windows XP, Windows Vista a Windows 7.*

AVG Download Manager je dostupný ke stažení na webu AVG (http://www.avg.cz/). V následujících kapitolách najdete popis jednotlivých kroků, kterými Vás **AVG Download Manager** provede:

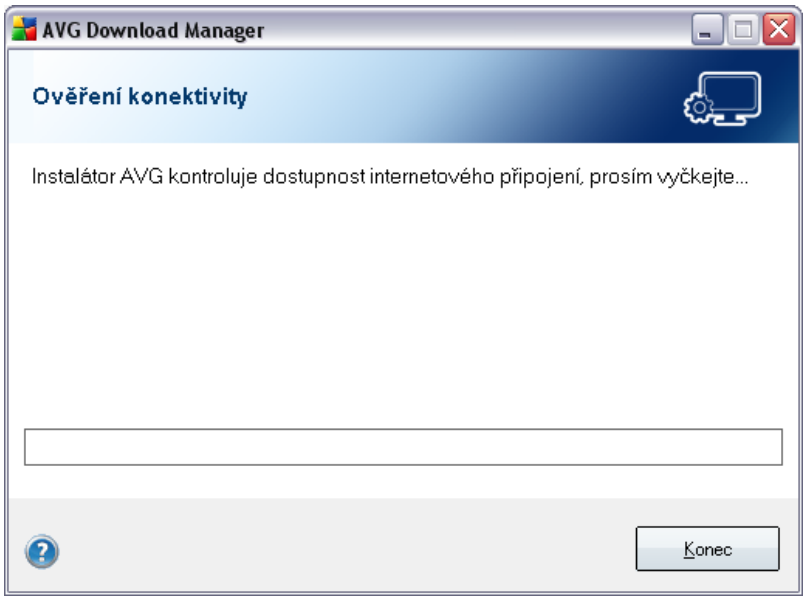
4.1. Výběr jazyka



V prvním kroku Vás **AVG Download Manager** vyzve k volbě jazyka instalace. Vyberte si z nabídky v rozbalovacím menu. Jazyk, který v tuto chvíli zvolíte, se vztahuje pouze na průběh instalačního procesu. Jazyk aplikace pak můžete kdykoliv změnit přímo v nastavení programu. Pokračujte stiskem tlačítka ***Další***.

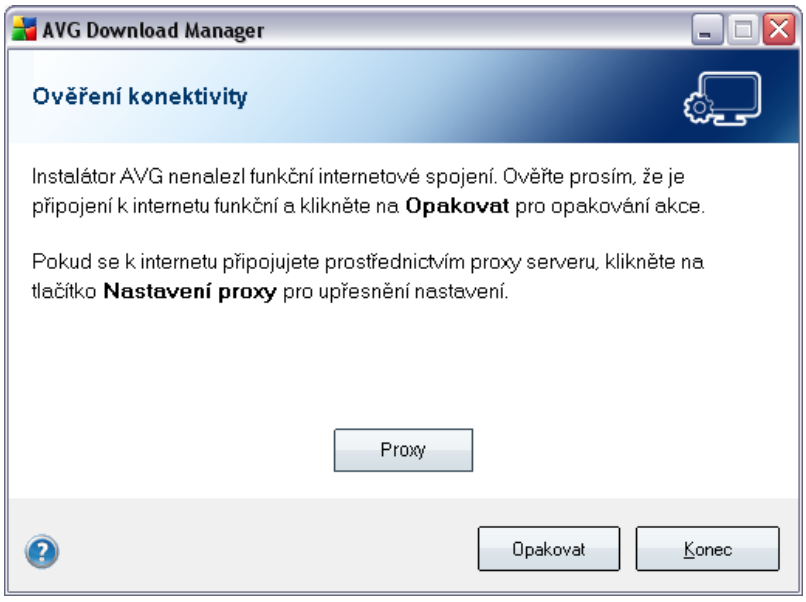
4.2. Kontrola připojení

V následujícím kroku ***Ověření konektivity*** se **AVG Download Manager** pokusí navázat spojení se sítí Internet kvůli lokalizaci aktualizačních souborů:



Po proběhnutí testu budete v dialogu vyrozuměni o jeho výsledku.

- Pokud se při testu ukáže, že spojení nelze navázat, budete o tom vyrozuměni následujícím dialogem - ověřte prosím, zda jste skutečně připojeni k Internetu a pokračujte stiskem tlačítka ***Opakovat***:

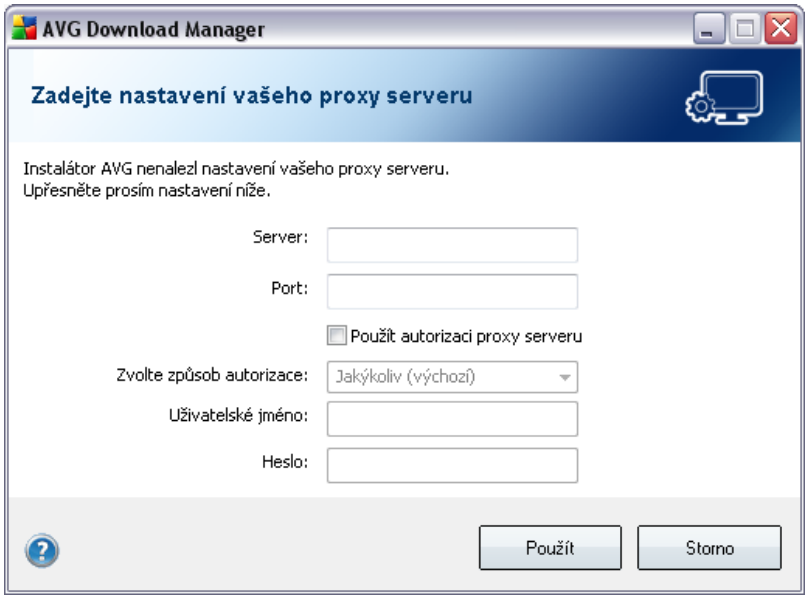


- Pokud používáte proxy a jeho nastavení nebude možno rozeznat automaticky,

objeví se tlačítko ***Proxy***. Pokračujte jeho stiskem k dialogu ***Nastavení proxy***:

- Pokud test proběhl bez potíží, **AVG Download Manager** bude pokračovat automaticky bez nutnosti vašeho zásahu a budete přesměrováni přímo k dialogu ***Stahuji instalační soubory***.

4.3. Nastavení proxy

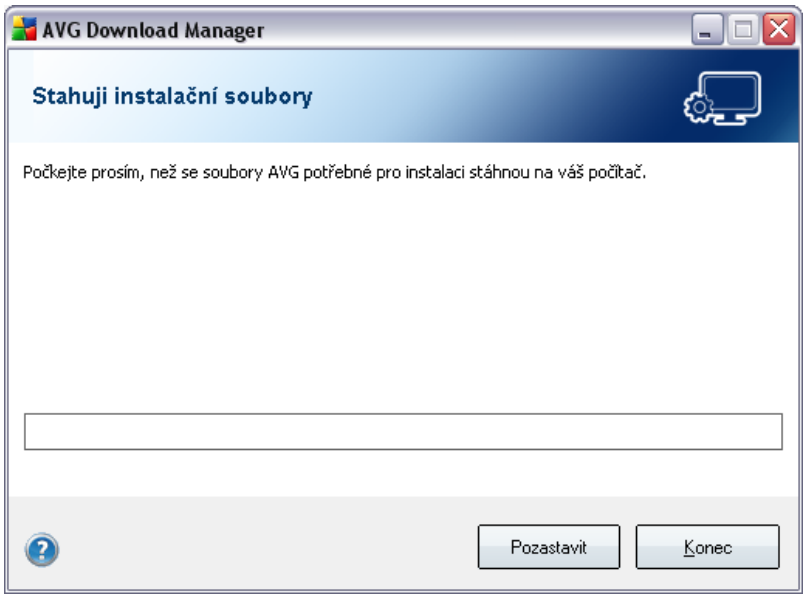


Pokud **AVG Download Manager** nedokázal identifikovat nastavení proxy serveru automaticky, je třeba je nastavit manuálně. Zadejte prosím následující data:

- ***Server***- uveďte platné jméno serveru nebo jeho IP adresu
- ***Port*** - zadejte číslo příslušného portu
- ***Použít autorizaci proxy serveru*** - pokud Váš proxy server vyžaduje autentizaci, označte tuto položku.
- ***Zvolte způsob autorizace*** - z rozbalovacího menu vyberte typ autentizace. Nejste-li skutečně zkušeným uživatelem, doporučujeme, abyste se drželi výchozího nastavení! Dále uveďte platné ***Uživatelské jméno*** a ***Heslo*** (volitelné).

Zvolené nastavení potvrďte stiskem tlačítka ***Použít*** a pokračujte k dalšímu dialogu.

4.4. Stahuji instalační soubory



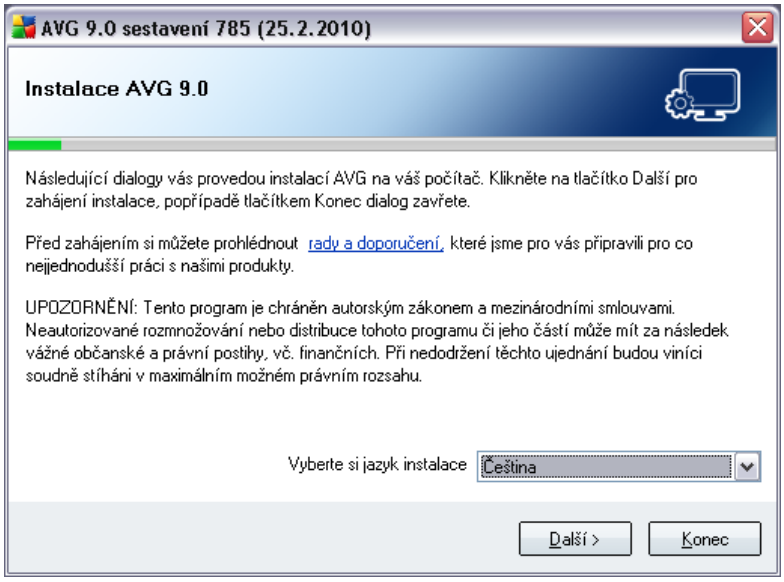
Nyní jste zadali všechny informace nutné k tomu, aby **AVG Download Manager** mohl začít stahovat instalační balík a spustit samotnou instalaci programu AVG.

5. Instalační proces AVG

Pro instalaci **AVG 9 Anti Virus plus Firewall** na váš počítač potřebujete 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 anebo využít pomoci nástroje ***AVG Download Manager***, který Vám sestaví potřebný instalační soubor podle Vašich požadavků, stáhne jej a samotný proces instalace spustí.

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

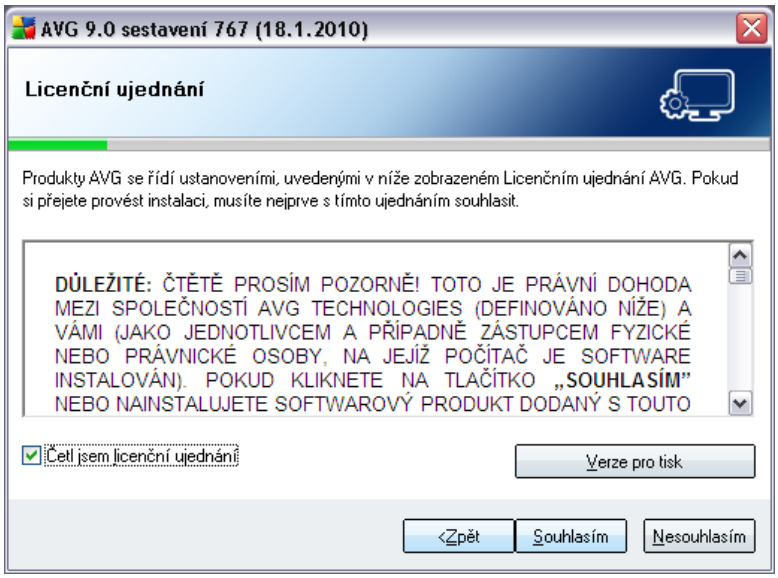
5.1. Spuštění instalace



Instalační proces je zahájen otevřením dialogu ***Instalace AVG Free 9.0***. V tomto dialogu máte možnost zvolit jazyk, v němž bude instalační proces probíhat a v němž bude následně instalován program AVG. V dolní části okna u položky ***Vyberte si jazyk instalace*** zvolte z rozbalovacího menu jazyk, v němž chcete komunikovat, a volbu potvrďte stiskem tlačítka ***Další***.

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, můžete je definovat v dialogu Uživatelská instalace - Zvolte komponenty,*

5.2. Licenční ujednání



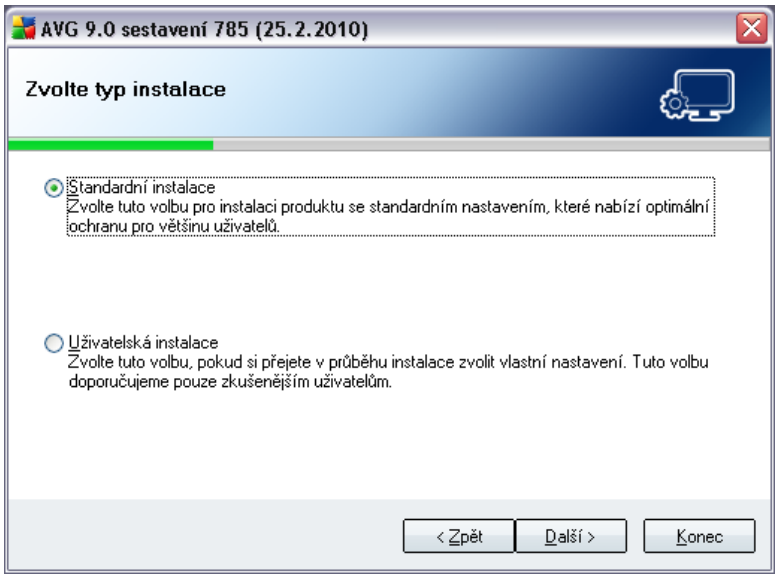
V dialogu ***Licenční ujednání*** najdete plné znění závazné licenční smlouvy AVG. Text si přečtěte a svůj souhlas s licenčním ujednáním potvrďte označením položky ***Četl jsem licenční ujednání*** a stiskem tlačítka ***Souhlasím***.

Pokud s licenční smlouvou nesouhlasíte a stisknete tlačítko ***Nesouhlasím***, instalace bude okamžitě ukončena.

5.3. Zjišťování stavu

Po potvrzení licenčního ujednání přejdete do dialogu ***Probíhá zjišťování stavu***. Tento dialog nevyžaduje žádný váš zásah; po dobu jeho zobrazení probíhá kontrola stavu vašeho systému před zahájením instalace AVG. Vyčkejte prosím dokončení tohoto procesu a budete automaticky přesměrováni do následujícího dialogu.

5.4. Zvolte typ instalace



Dialog ***Zvolte typ instalace*** vám dává na výběr mezi ***standardní*** a ***uživatelskou*** instalací.

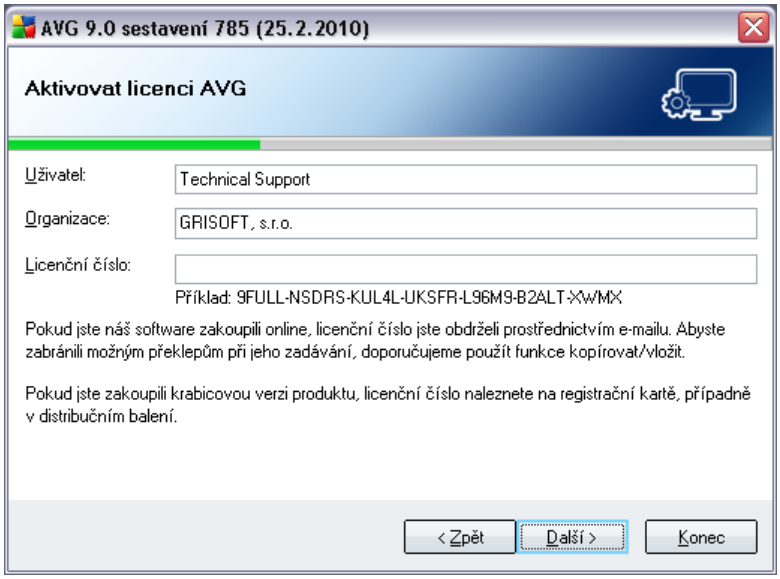
Většině uživatelů doporučujeme použít ***standardní instalaci***, kdy bude AVG nainstalován zcela automaticky s nastavením definovaným výrobcem. Toto nastavení zaručuje maximální úroveň bezpečnosti a optimální využití zdrojů. Pokud se v budoucnu vyskytne potřeba některé konkrétní nastavení změnit, budete mít vždy možnost editovat konfiguraci AVG přímo v aplikaci.

Uživatelská instalace je vhodná pouze pro pokročilé a znalé uživatele. Doporučit ji lze v případě, že máte skutečný důvod instalovat AVG s nestandardním nastavením tak, aby vyhovovalo specifickým požadavkům vašeho systému.

5.5. Aktivovat licenci AVG

V dialogu ***Aktivovat licenci AVG*** je třeba vyplnit vaše registrační údaje.

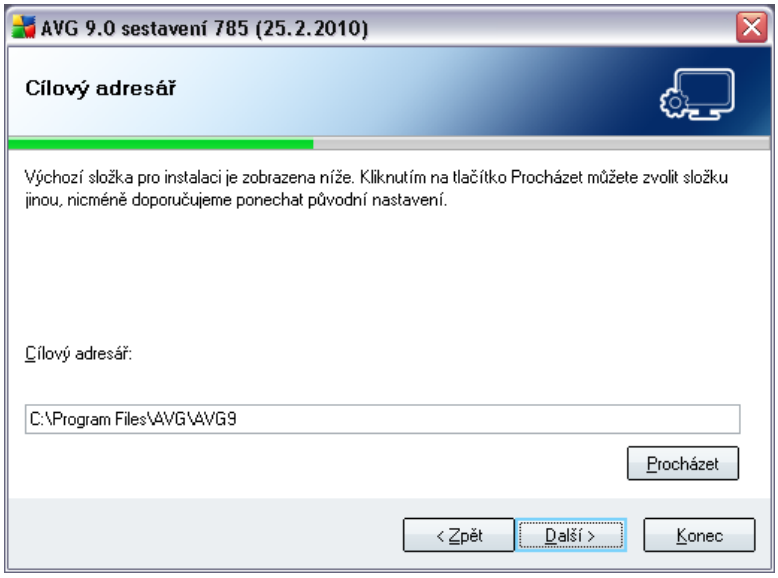
Vepište své jméno (pole ***Uživatel***) a název vaší organizace (pole ***Organizace***). Do položky ***Licenční číslo*** pak zadejte své licenční číslo. Toto číslo najdete buďto na registrační kartě v krabicovém balení **AVG 9 Anti Virus plus Firewall**, anebo v potvrzovacím emailu, který jste obdrželi při zakoupení **AVG 9 Anti Virus plus Firewall** on-line. Licenční číslo musí být zadáno naprosto přesně ve tvaru, jak je uvedeno, proto prosím věnujte velkou pozornost jeho přepisu. Pokud máte číslo k dispozici v digitální formě, doporučujeme jej do příslušného pole zkopírovat (*metodou kopírovat a vložit*).



V instalaci pokračujte stiskem tlačítka ***Další***.

Pokud jste v předchozím kroku zvolili standardní instalaci, přejdete rovnou do dialogu ***AVG Security Toolbar***. Při volbě uživatelské instalace budete pokračovat dialogem ***Cílový adresář***.

5.6. Uživatelská instalace - Cílový adresář

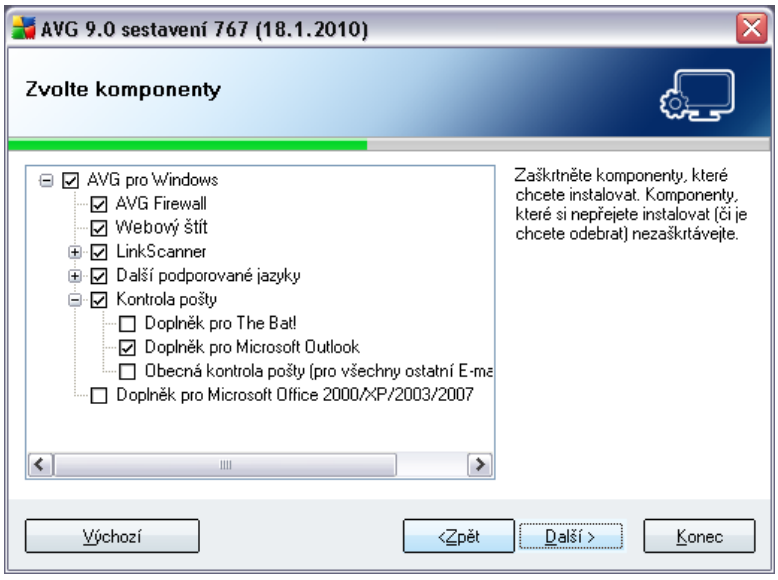


Dialog ***Cílový adresář*** vám dává možnost určit, kam má být program **AVG 9 Anti Virus plus Firewall** instalován. Ve výchozím nastavení bude program instalován do adresáře programových souborů umístěném typicky na disku C:. Pokud tento adresář ještě neexistuje, budete novým dialogem vyzváni, abyste potvrdili, že si přejete adresář vytvořit.

Pokud si přejete toto umístění změnit, pomocí tlačítka ***Procházet*** zobrazte strukturu vašeho disku a zvolte požadovaný adresář.

Svou volbu potvrďte stiskem tlačítka ***Další***.

5.7. Uživatelská instalace - Zvolte komponenty



V dialogu ***Zvolte komponenty*** je zobrazen přehled komponent **AVG 9 Anti Virus plus Firewall**, které můžete nainstalovat. Pokud vám výchozí nastavení nevyhovuje, máte možnost jednotlivé komponenty odebrat/přidat.

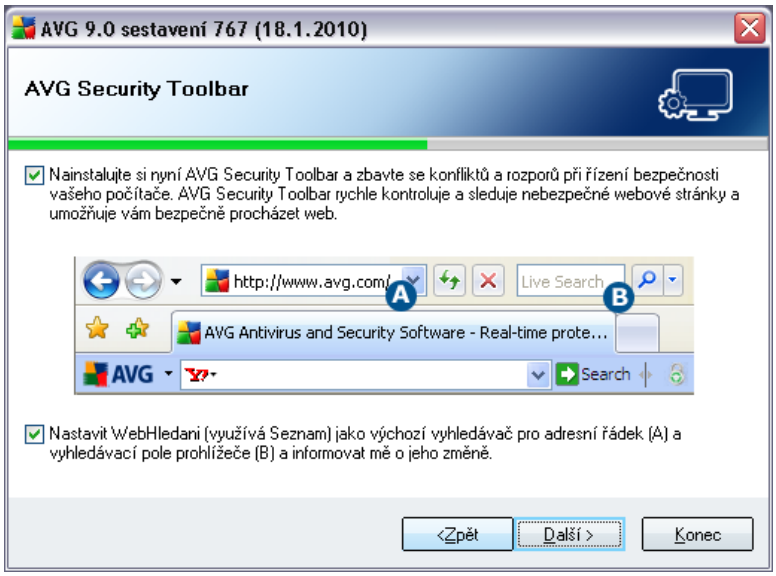
Volit můžete pouze z těch komponent, které jsou zahrnuty ve vámi zakoupené licenci AVG. Pouze tyto komponenty vám také budou v dialogu nabídnuty!

- ***Volba jazyka*** - v přehledu instalovaných komponent máte v tuto chvíli možnost definovat, jaké jazyky mají být v programu AVG instalovány (*jde o jazyky, do nichž budete mít možsnot nainstalovaný program přepínat*). Program se vždy nainstaluje v angličtině a v aktuálním jazyce instalce, ostatní jazyky můžete doinstalovat volitelně. Rozbalte položku ***Další podporované jazyky*** a požadované jazyky vyberte z příslušné nabídky.

- ***Doplňky Kontroly pošty*** - pod položkou ***Kontrola pošty*** máte možnost rozhodnout se, jakým způsobem má být zajištěna kontrola vaší elektronické pošty. Ve výchozím nastavení bude instalován doplněk, který odpovídá poštovnímu programu automaticky detekovanému na vašem počítači, a to buďto ***Doplněk pro Microsoft Outlook, Doplněk pro The Bat!*** Pokud nemáte na svém PC ani jeden z těchto poštovních programů, bude nainstalována ***Obecná kontrola pošty***, která pokrývá všechny ostatní poštovní klienty (*například Qualcomm Eudora, atd.*). Jednotlivé doplňky pro konkrétní poštovní klienty můžete rovněž volitelně doinstalovat.

Pokračujte stiskem tlačítka ***Další***.

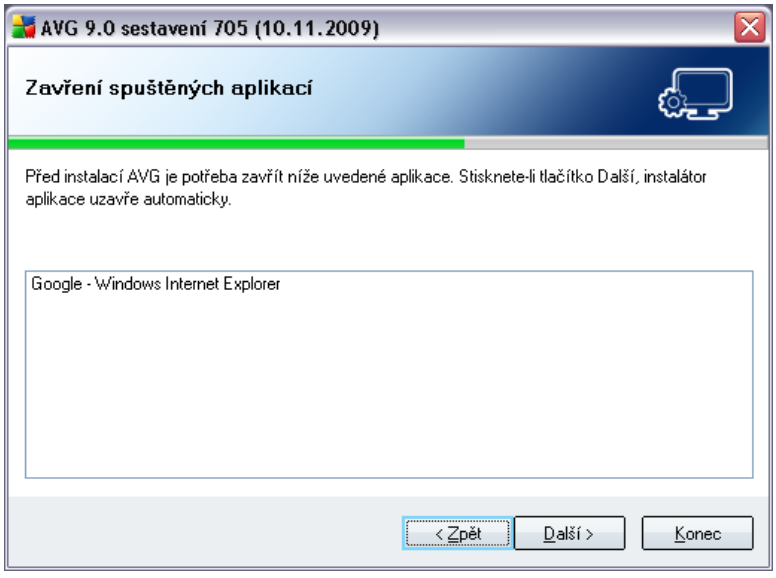
5.8. AVG Security Toolbar



V dialogu ***AVG Security Toolbar*** rozhodněte, zda si v rámci **AVG 9 Anti Virus plus Firewall** 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 v. 6.0 nebo novější a Mozilla Firefox v. 3.0 nebo novější*) a zajistí kompletní on-line ochranu při prohlížení webu.

V tomto dialogu máte také možnost rozhodnout, zda si přejete nastavit WebHledání jako výchozí službu vyhledávání. Pokud ano, prosím, označte příslušné políčko.

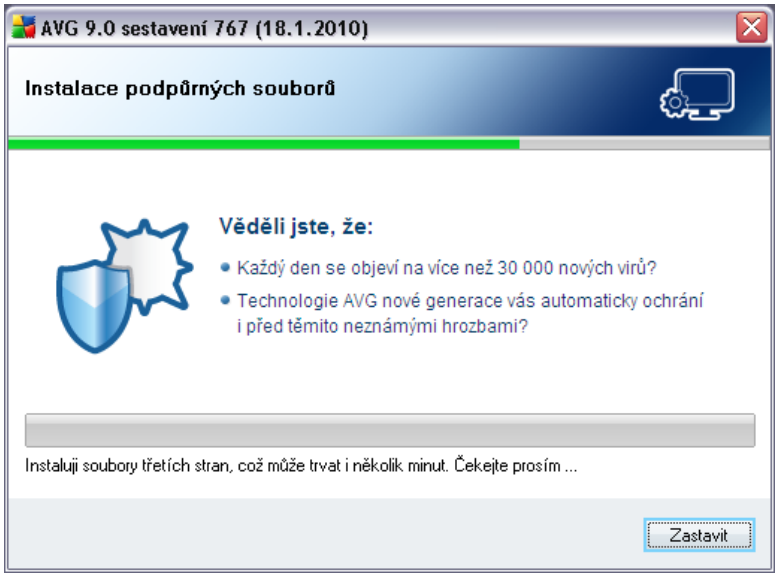
5.9. Zavření spuštěných aplikací



Dialog ***Zavření spuštěných aplikací*** se v průběhu instalačního procesu zobrazí pouze tehdy, když instalace koliduje s některými programy, které aktuálně běží na Vašem počítači. V takovém případě bude seznam těchto programů v dialogu uveden a stiskem tlačítka ***Další*** potvrdíte, že souhlasíte s tím, aby uvedené aplikace byly uzavřeny. Současně tak postoupíte k dalšímu kroku instalačního procesu.

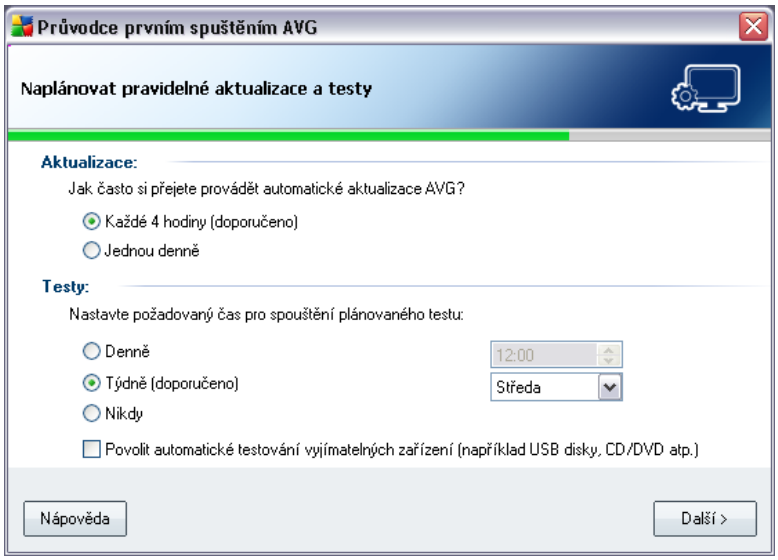
5.10. Probíhá instalace

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



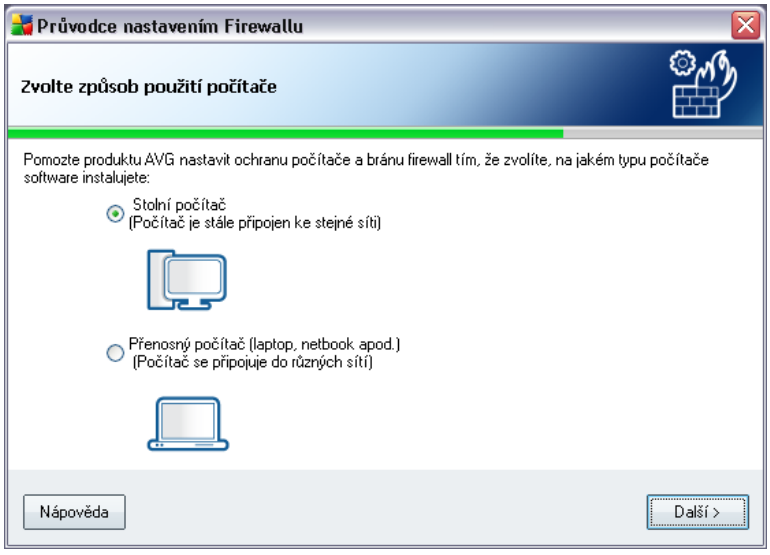
Počkejte prosím na dokončení instalace, aktualizaci virových databází a aktualizaci programu. Poté budete automaticky přesměrováni k následujícímu dialogu.

5.11. Nastavení pravidelných aktualizací a testů



V dialogu ***Naplánovat pravidelné aktualizace a testy*** určete časový interval stahování nových aktualizačních souborů a čas spuštění plánovaného testu. Doporučujeme podržet se výchozího nastavení. Pokračujte stiskem tlačítka ***Další***.

5.12. Zvolte způsob použití počítače



V tomto dialogu se ***Průvodce nastavením Firewallu*** ptá, jaký druh počítače používáte. Je zřejmé, že například notebook, s nímž se připojujete k Internetu na nejrůznějších místech (*letiště, hotel*) vyžaduje, aby byla bezpečnostní pravidla nastavena přísněji než počítač nacházející se v doméně. Podle zvoleného typu pak budou nastavena výchozí pravidla ***Firewallu*** a jim příslušná úroveň zabezpečení.

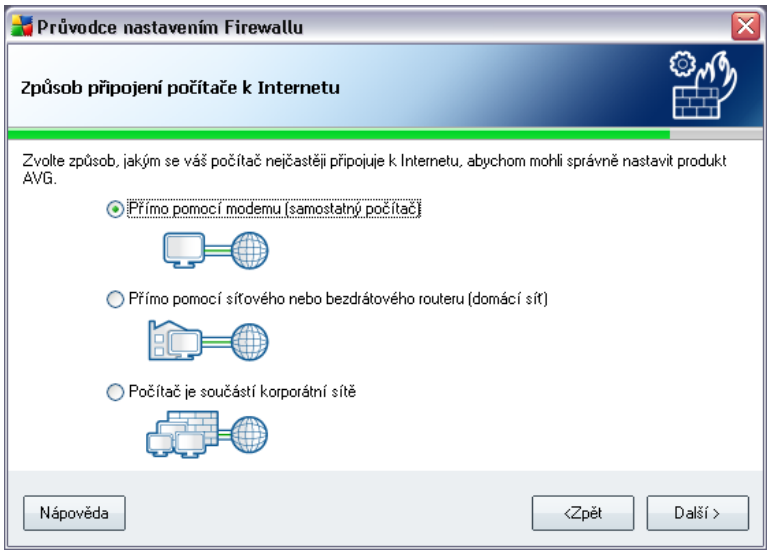
Můžete si vybrat ze dvou možností:

- ***Stolní počítač*** *- pokud zvolíte tuto alternativu, budete přesměrování k následujícímu dialogu nazvanému Způsob připojení počítače k síti*
- ***Přenosný počítač*** *- při této volbě pokračujete již k závěrečnému dialogu instalačního procesu, Konfigurace ochrany AVG je kompletní*

Volbu potvrďte stiskem tlačítka ***Další***.

5.13. Způsob připojení počítače k síti

Tento dialog se zobrazí pouze v případě, že jste v předchozím kroku (*dialog Zvolte způsob použití počítače*) označili variantu stolní počítač:



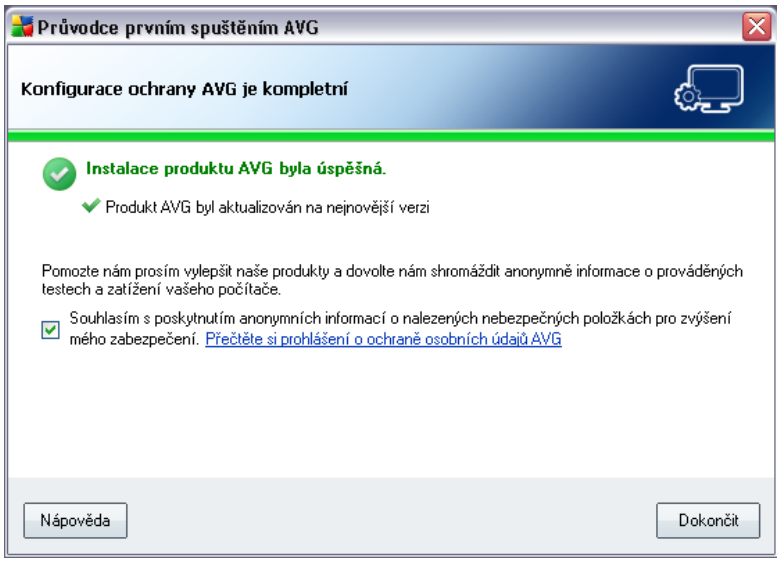
Průvodce nastavením Firewallu se v tomto dialogu dotazuje na způsob připojení vašeho počítače k Internetu. Podle zvoleného typu připojení pak budou výchozí pravidla ***Firewallu*** definována s různou mírou úrovně zabezpečení.

K výběru se nabízejí tyto tři možnosti:

- ***Přímo pomocí modemu***
- ***Přímo pomocí síťového nebo bezdrátového routeru***
- ***Počítač je součástí korporátní sítě***

Vyberete možnost, která nejlépe popisuje způsob připojení Vašeho počítače k Internetu. Svou volbu potvrďte stiskem tlačítka ***Další***.

5.14. Konfigurace ochrany AVG je kompletní



Konfigurace vašeho **AVG 9 Anti Virus plus Firewall** je nyní nastavena k optimálnímu výkonu.

V tomto dialogu máte možnost rozhodnout se, zda chcete aktivovat možnost anonymního reportování nebezpečných nálezů do virové laboratoře AVG. Pokud se tak rozhodnete, označte prosím volbu ***Souhlasím s poskytnutím ANONYMNÍCH informací o nalezených nebezpečných položkách pro zvýšení mého zabezpečení*** .

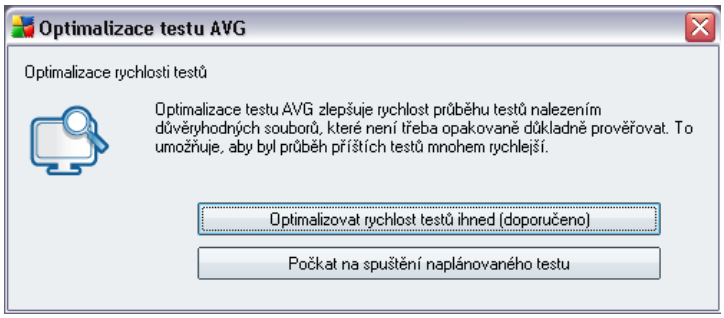
Proces instalace a konfigurace uzavřete stiskem tlačítka ***Dokončit***. Abyste mohli začít pracovat s aplikací AVG, bude vyžadován restart počítače.

6. Po instalaci

6.1. Optimalizace testu

Funkce optimalizace testů spočívá v prohledání adresářů *Windows* a *Program Files*, v nichž najde vhodné soubory (*momentálně se jedná o digitálně podepsané soubory typu *.exe, *.dll a *.sys*) a informaci o nich uloží. Při příštím přístupu nebude tyto soubory nutné automaticky testovat: označené soubory budou otestovány pouze v případě, že **AVG 9 Anti Virus plus Firewall** detekuje změnu kontrolního součtu. Pokud bude kontrolní součet beze změn, není třeba soubor znovu prověřovat, takže se významně zkrátí doba testování.

Po dokončení instalačního procesu budete vyzváni samostatným dialogem k optimalizaci rychlosti testů:



Doporučujeme potvrdit tuto volbu stiskem tlačítka ***Optimalizovat rychlost testů ihned***.

6.2. Registrace produktu

Po dokončení instalace **AVG 9 Anti Virus plus Firewall** 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 uživatelům AVG.

6.3. Otevření uživatelského rozhraní

Uživatelské rozhraní AVG je dostupné několika cestami:

- dvojklikem na ikonu AVG na systémové liště
- dvojklikem na ikonu AVG na ploše
- z nabídky ***Start/Všechny programy/AVG 9.0/Uživatelské rozhraní AVG***
- z ***AVG Security Toolbaru*** volbou ***Spustit AVG***

6.4. Spuštění testu celého počítače

Jelikož existuje jisté riziko, že virus byl na váš počítač zavlečen již před instalací **AVG 9 Anti Virus plus Firewall**, doporučujeme bezprostředně po instalaci spustit ***Test celého počítače***, který zkontroluje celý počítač a ověří případnou přítomnost virů a potenciálně nežádoucích programů.

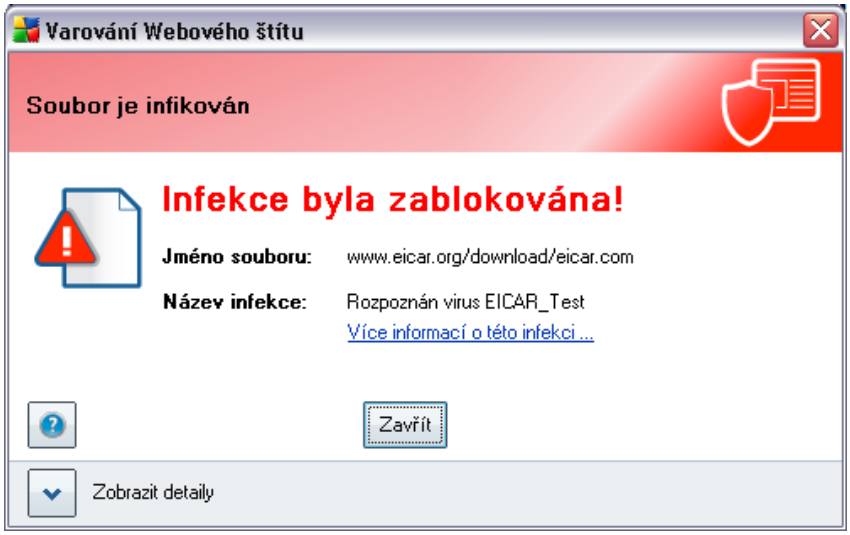
Instrukce ke spuštění testu najdete v kapitole ***AVG testování***.

6.5. Test virem Eicar

Chcete-li ověřit, že **AVG 9 Anti Virus plus Firewall** 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. Většina produktů 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 9 Anti Virus plus Firewall** na vašem počítači je správně nainstalován:



Z webu http://www.eicar.com můžete také stáhnout komprimovanou verzi testovacího 'viru' EICAR (*například ve formátu eicar_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 prověřit konfiguraci AVG 9 Anti Virus plus Firewall!**

6.6. Výchozí konfigurace AVG

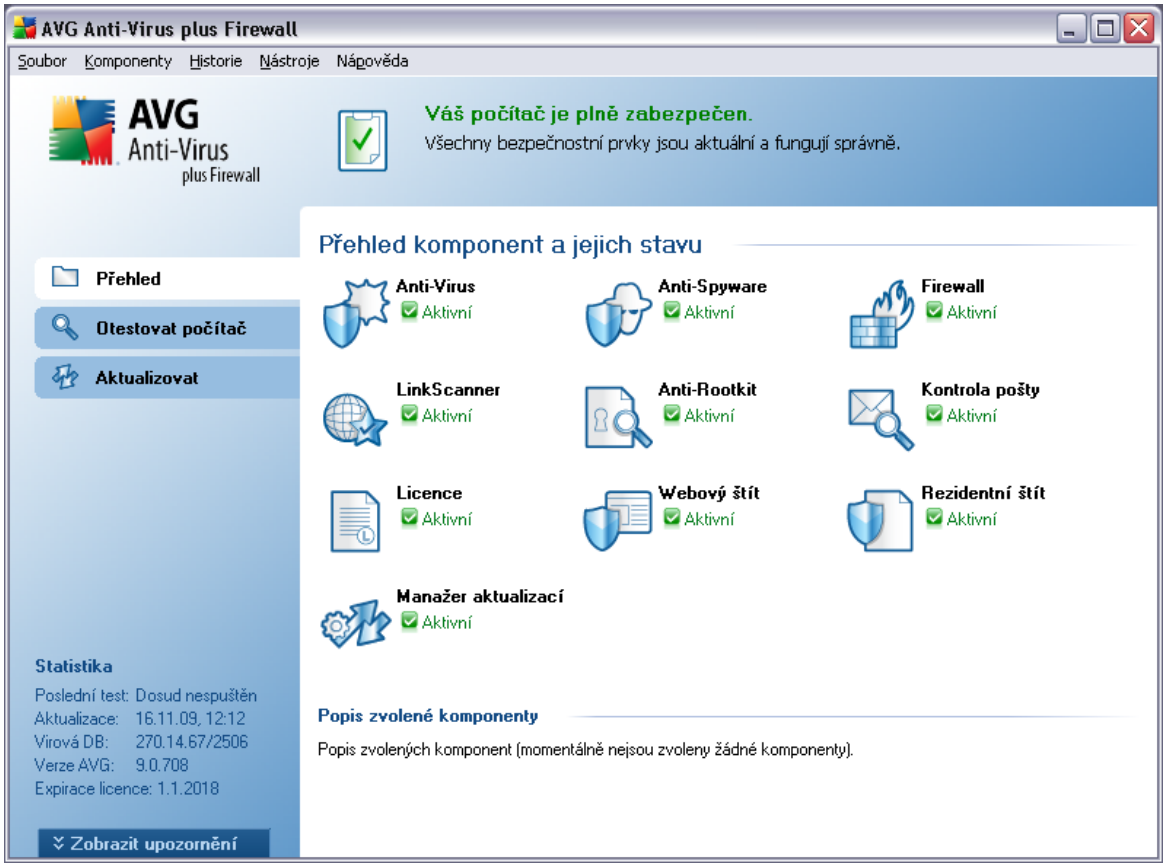
Ve výchozí konfiguraci (bezprostředně po instalaci **AVG 9 Anti Virus plus Firewall**) jsou všechny komponenty a funkce **AVG 9 Anti Virus plus Firewall** nastaveny výrobcem k optimálnímu výkonu bezpečnostního software.

Pokud nemáte skutečný důvod jejich konfiguraci měnit, doporučujeme ponechat program v tomto nastavení! Změnu konfigurace by měli provádět pouze zkušení uživatelé.

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***.

7. Uživatelské rozhraní AVG

AVG 9 Anti Virus plus Firewall 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)* umožňují 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 běhu programu - podrobnosti >>
- ***Ikona na systémové liště*** *(v pravém dolním rohu monitoru, na systémové liště)* je indikátorem aktuálního stavu AVG -podrobnosti >>

7.1. Systémové menu

Systémové menu je standardní navigací používanou ve všech oknech Windows. Je umístěno v rozhraní **AVG 9 Anti Virus plus Firewall** vodorovně zcela nahoře. Prostřednictvím tohoto menu můžete přistupovat k jednotlivým komponentám, vlastnostem a službám AVG.

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

7.1.1. Soubor

- ***Konec*** - zavírá uživatelské rozhraní **AVG 9 Anti Virus plus Firewall**. Aplikace AVG však zůstává spuštěna, běží trvale na pozadí a váš počítač je stále chráněn!

7.1.2. 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*** - otevírá výchozí dialog pro komponentu ***Anti-Virus***
- ***Anti-Rootkit*** - otevírá výchozí dialog pro komponentu ***Anti-Rootkit***
- ***Anti-Spyware*** - otevírá výchozí dialog pro komponentu ***Anti-Spyware***
- ***Firewall*** - otevírá výchozí dialog pro komponentu ***Firewall***
- ***Link Scanner*** - otevírá výchozí dialog pro komponentu ***Link Scanner***
- ***Kontrola pošty*** - otevírá výchozí dialog pro komponentu ***Kontrola pošty***
- ***Licence*** - otevírá výchozí dialog pro komponentu ***Licence***
- ***Webový štít*** - otevírá výchozí dialog pro komponentu ***Webový štít***
- ***Rezidentní štít*** - otevírá výchozí dialog pro komponentu ***Rezidentní štít***
- ***Manažer aktualizací*** - otevírá výchozí dialog pro komponentu ***Manažer aktualizací***

7.1.3. Historie

- ***Výsledky testů*** - 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 9 Anti Virus plus Firewall**

- ***Firewall*** - otevírá rozhraní ***Nastavení Firewallu*** na záložce ***Protokoly*** se záznamem o všech akcích Firewallu

7.1.4. 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 9 Anti Virus plus Firewall**

- ***Aktualizovat z adresáře*** - spustí proces aktualizace z aktualizačního 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 předem umístili aktualizační soubory, a spusťte aktualizaci.

- ***Pokročilé nastavení*** - otevírá dialog ***Pokročilého nastavení AVG***, kde máte možnost editovat konfiguraci **AVG 9 Anti Virus plus Firewall**. Obecně doporučujeme podržet výchozí výrobcem definované nastavení aplikace.

- ***Nastavení Firewallu*** - otevírá samostatný dialog pro pokročilou konfiguraci komponenty ***Firewall***

7.1.5. 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 instalačního procesu. V dialogu ***Aktivace AVG*** můžete zadat své licenční číslo, kterým buďto nahradíte prodejní číslo, s nímž jste AVG instalovali, nebo kterým změníte dosavadní licenční číslo za jiné, např. při přechodu na jiný produkt z řady 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 9 Anti Virus plus Firewall***, dvě posledně uvedené položky 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 9 Anti Virus plus Firewall** *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***.

7.2. 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 9 Anti Virus plus Firewall** . 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. Přesto prosím věnujte pozornost 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 vědomě 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 setrvávali déle, než je nutné.

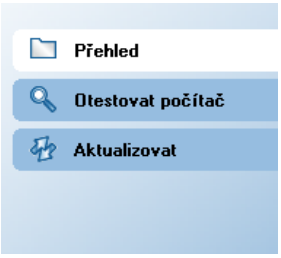

Červená ikona informuje o kritickém stavu AVG! Některá z komponent je nefunkční a AVG nemůže plně chránit váš počítač. Věnujte prosím okamžitou pozornost opravě tohoto problému. Pokud nebudete sami schopni problém odstranit, kontaktujte oddělení technické podpory AVG.

Důrazně doporučujeme, abyste věnovali pozornost informaci zobrazené 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.*

7.3. Zkratková tlačítka

Zkratková tlačítka *(v levé části uživatelského rozhraní AVG)* umožňují 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 >>***
- ***Otestovat počítač*** - tlačítko otevírá testovací rozhraní AVG, kde je možné přímo spouštět testy vašeho počítače, plánovat jejich spuštění či editovat parametry testů - viz kapitola ***AVG Testování >>***
- ***Aktualizovat*** - tlačítko otevírá nové rozhraní a současně okamžitě spouští aktualizační proces - 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 navigaci graficky znázorněn.

7.4. 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 funkčnosti zvolené komponenty

V rámci **AVG 9 Anti Virus plus Firewall** najdete v sekci ***Přehled komponent*** informace o těchto komponentách:

- ***Anti-Virus*** chrání váš počítač proti útočícím virům - podrobnosti >>
- ***Anti-Spyware*** chrání váš počítač před spyware a adware - podrobnosti >>
- ***Firewall*** řídí výměnu dat mezi vaším počítačem a ostatními stanicemi v lokální síti nebo v síti Internetu - podrobnosti >>
- ***Link Scanner*** kontroluje odkazy zobrazené ve výsledcích vyhledávání ve vašem internetovém prohlížeči - podrobnosti >>
- ***Anti-Rootkit*** detekuje programy a technologie, které dokáží maskovat přítomnost nebezpečného software - podrobnosti >>
- ***Kontrola pošty*** prověřuje všechnu příchozí i odchozí poštu na přítomnost virů - podrobnosti >>
- ***Licence*** zobrazuje licenční číslo, typ licence, datum expirace atd. - podrobnosti >>
- ***Webový štít*** kontroluje data stahovaná webovým prohlížečem - podrobnosti >>
- ***Rezidentní štít*** pracuje na pozadí a kontroluje soubory při jejich kopírování, otevírání a ukládání - podrobnosti >>
- ***Manažer aktualizací*** spravuje aktualizační procesy AVG - podrobnosti >>

Jednoduchým kliknutím na libovolnou ikonu komponenty tuto komponentu v přehledu vysvítíte a současně se ve spodní části uživatelského rozhraní zobrazí stručný popis funkce této komponenty. Dvojklikem na zvolenou ikonu otevřete vlastní rozhraní komponenty s přehledem 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 vědomi faktu, že se ta která komponenta nachází v chybovém stavu, ale z nějakého důvodu si přejete tento stav zachovat a nebýt na něj upozorňováni ikonou na systémové liště.

7.5. Statistika

Sekce ***Statistika*** je umístěna v levém spodním rohu uživatelského rozhraní AVG. Statistika podává přehled o běhu programu AVG:

- ***Poslední test*** - datum posledního spuštění testu
- ***Aktualizace*** - datum posledního spuštění aktualizace
- ***Virová DB*** - informace o verzi aktuálně instalované virové databáze
- ***Verze AVG*** - informace o instalované verzi AVG *(číslo ve tvaru 9.0.xxx, kde 9.0 zastupuje produktovou řadu AVG a xxx označuje číslo sestavení)*
- ***Expirace licence*** - datum, kdy dojde k expiraci vaší licence AVG

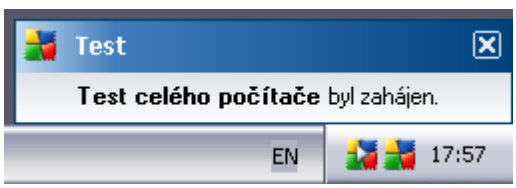
7.6. Ikona na systémové liště

Ikona na systémové liště (*vpravo dole na monitoru, na panelu Windows*) ukazuje aktuální stav **AVG 9 Anti Virus plus Firewall**. Ikona je viditelná v každém okamžiku vaší práce na počítači, bez ohledu na to, zda máte či nemáte 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 vědom a vědomě se rozhodl ***Ignorovat stav komponenty***.

Pokud je ikona zobrazena s vykřičníkem , 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.

Systémová ikona dále poskytuje informace o aktuálním dění v programu AVG. Při změně stavu AVG (*automatické spuštění naplánované aktualizace nebo testu, přepnutí profilu Firewallu, změna stavu některé komponenty, přechod programu do chybového stavu, ...*) budete okamžitě informováni pop-up oknem vysunutým nad ikonou na systémové liště:



Ikonu na systémové liště lze také použít pro rychlý přístup k uživatelskému rozhraní

AVG, to se otevře dvojklikem na ikonu. Kliknutí pravým tlačítkem myši nad ikonou otevírá kontextové menu s těmito možnostmi:

- ***Otevřít uživatelské rozhraní AVG*** - otevře uživatelské rozhraní AVG
- ***Testy*** - otevře vysunovací nabídku přednastavených testů (*Test celého počítače*, *Test vybraných souborů či složek*, *Anti-Rootkit test*) a následnou volbou požadovaný test přímo spustíte
- ***Firewall*** - otevře vysunovací nabídku s možnostmi nastavení Firewallu, z níž můžete přímo měnit nejdůležitější parametry, a to status Firewallu (*Firewall spuštěn/Firewall zastaven/Pohotovostní režim*), přepínání herního režimu a profily Firewallu
- ***Aktualizovat*** - spustí okamžitou aktualizaci
- ***Nápověda*** - otevře soubor nápovědy na úvodní stránce

8. Komponenty AVG

8.1. Anti-Virus

8.1.1. Princip Anti-Viru

Testovací jádro antivirového programu skenuje všechny soubory a jejich aktivitu (otevírání/zavírání souboru atd.) a prověřuje případnou 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.

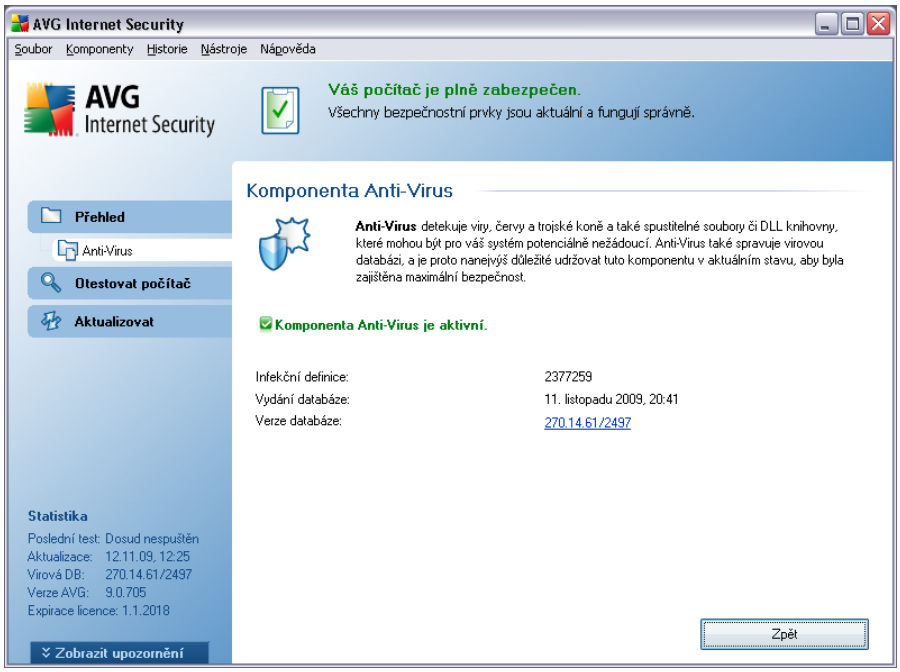
Dobrá antivirová ochrana zaručí, že na počítači nebude spuštěn žádný známý virus!

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

- skenování - vyhledávání řetězců 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, případně DLL knihovny a určit, které z nich by mohly být potenciálně nežádoucí (jako například spyware, adware aj.). Na žádost uživatele umožní tyto programy odstranit či k nim zablokovat přístup.

8.1.2. Rozhraní komponenty Anti-Virus



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

- ***Infekční definice*** - 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).

8.2. Anti-Spyware

8.2.1. Princip Anti-Spyware

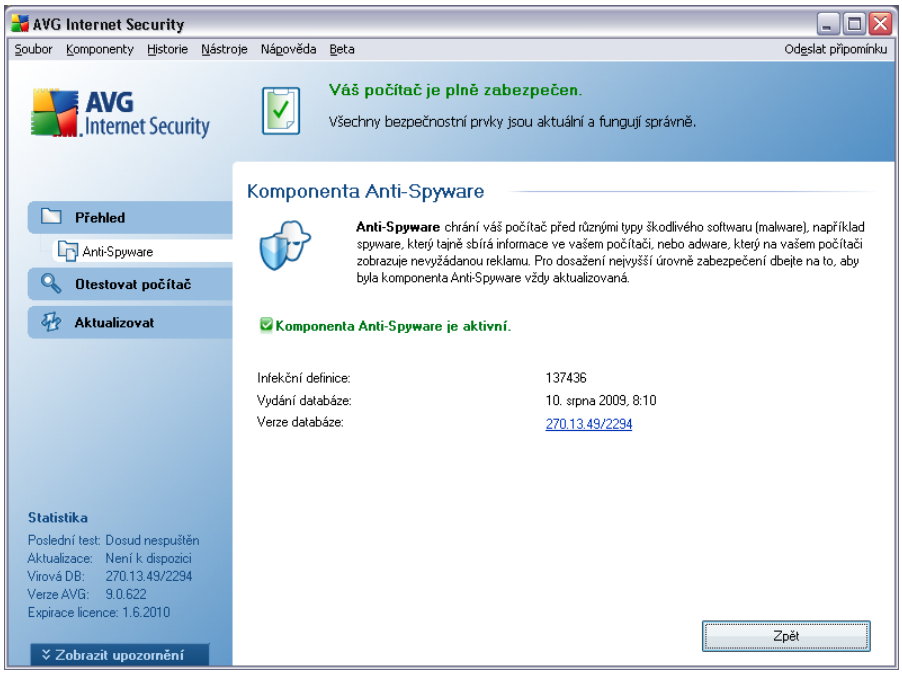
Spyware se obvykle definuje jako jeden z typů malware, to jest software, který z vašeho počítače sbírá informace bez vašeho vědomí. Některé aplikace typu spyware mohou být nainstalovány na váš počítač záměrně; častým příkladem jsou třeba reklamní upoutávky, pop-up okna nebo jiné typy obtížného software.

V ideálním případě byste se měli pokusit zabránit jakémukoli druhu spyware a/nebo malware v samotném průniku na váš počítač. Nejčastějším zdrojem nákazy jsou v současné době webové stránky s potenciálně nebezpečným obsahem. Rozšířen je i

přenos pomocí e-mailu nebo prostřednictvím červů a virů. Nejdůležitějším prvkem ochrany je tedy trvale zapnutý scanner běžící na pozadí, jakým je například ***Anti-Spyware AVG***: pracuje nepřetržitě a na pozadí prověřuje veškeré aplikace, které spouštíte.

Existuje také potenciální riziko, že malware byl zavlečen na váš počítač ještě před instalací **AVG 9 Anti Virus plus Firewall** nebo že jste opomněli provést databázovou či 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 neproběhla jeho aktivace.

8.2.2. Rozhraní komponenty Anti-Spyware



Rozhraní komponenty ***Anti-Spyware*** uvádí stručný popis základních funkcí této komponenty, informaci o aktuálním stavu komponenty (*Komponenta Anti-Spyware je aktivní.*) a dále statistický přehled:

- ***Spyware definice*** - číslo udává počet vzorků spyware definovaných v aktuální verzi spyware databáze

- ***Vydání databáze*** - datum uvádí, 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).

8.3. Firewall

Počítače, jež nejsou chráněny firewallem, se stávají snadným cílem počítačových hackerů a různých zlodějů dat.

Obecně lze firewall definovat jako systém, který pomocí blokování/povolování přístupu řídí provoz mezi dvěma nebo více sítěmi. Firewall obsahuje pravidla, jež chrání vnitřní síť před útokem zvenčí (nejčastěji z internetu) a řídí veškerou komunikaci probíhající na jednotlivých síťových portech. Tu vyhodnocuje podle pravidel, jež má nastaveny, a rozhoduje, zda je komunikace vyhovující či nevyhovující. Pokud narazí na pokusy o proniknutí, zabrání jejich průniku dovnitř počítače.

Firewall je nastaven tak, aby povolil nebo zablokoval interní či externí komunikaci (oběma směry, dovnitř nebo ven) na předem definovaných portech a pro vybrané softwarové aplikace. Například můžete Firewall nastavit tak, aby propouštěl data stahovaná z Internetu pouze za použití prohlížeče MS Internet Explorer. Jakýkoliv jiný pokus o stažení dat pomocí jiného prohlížeče bude zablokován.

Firewall vám pomůže udržet si své soukromí a zaručí, že vaše osobní informace nebudou, byť náhodně, odeslány z vašeho počítače bez vašeho svolení. Firewall průběžně kontroluje výměnu dat mezi vaším počítačem a ostatními počítači v lokální síti nebo na internetu. V rámci firmy pak firewall zajistí ochranu jednotlivého počítače před útoky vedenými z vnitřní sítě.

Doporučení: *Obecně není doporučeno na jednom počítači používat více firewallů. Instalací více firewallů není dosaženo větší bezpečnosti, ale naopak je pravděpodobné, že bude docházet mezi těmito aplikacemi ke konfliktům. Proto vám doporučujeme používat vždy pouze jeden firewall a ostatní deaktivovat, aby byl případný konflikt a jeho následky eliminovány.*

8.3.1. Princip Firewallu

V systému AVG řídí komponenta ***Firewall*** veškerý provoz na všech síťových portech vašeho počítače. Podle předem nastavených pravidel vyhodnocuje jednak aplikace, které běží na vašem počítači (a pokoušejí se o komunikaci do sítě Internetu nebo do lokální sítě), a také aplikace, které se snaží navázat komunikaci s vaším počítačem zvenčí. Každé z těchto aplikací ***Firewall*** komunikaci na síťových portech buďto povolí nebo zakáže. Ve výchozím nastavení platí, že pokud jde o neznámou aplikaci (tedy aplikaci, pro niž ještě nebylo v rámci ***Firewallu*** definováno pravidlo), ***Firewall*** se zeptá, zda si přejete tento pokus o komunikaci povolit nebo zablokovat.

Poznámka: *AVG Firewall není určen k ochraně serverů!*

Co umí AVG Firewall

- Automaticky povoluje nebo blokuje pokusy o komunikaci aplikacím, pro něž má definované pravidlo, nebo se dotáže a požádá o potvrzení volby
- Pracuje s profily nastavenými podle definovaných pravidel, jež reflektují vaše potřeby

- Automaticky přepíná profily podle aktuálního připojení k síti nebo podle aktuálně použitých síťových adaptérů

8.3.2. Profily Firewallu

Firewall umožňuje definovat specifická bezpečnostní pravidla na základě toho, zda je váš počítač umístěn v doméně nebo jde o samostatný počítač, případně o notebook. Každá z těchto možností vyžaduje jinou úroveň ochrany a jednotlivé úrovně jsou reprezentovány konkrétními profily. V krátkosti lze říci, že profil ***Firewallu*** je specifickou konfigurací ***Firewallu*** a můžete používat několik takových předem definovaných konfigurací.

Dostupné profily

- ***Povolit vše*** - systémový profil ***Povolit vše*** je přednastaveným profilem a je k dispozici za všech okolností. Jestliže je tento profil aktivován, je povolena veškerá komunikace a nejsou uplatňována žádná bezpečnostní pravidla, jako kdyby byl ***Firewall*** vypnutý *(tj. jsou povoleny všechny aplikace, ale kontrola na bázi paketů stále probíhá - chcete-li zcela zrušit jakékoliv filtrování, je nutné Firewall vypnout)*. Tento systémový profil nelze duplikovat, smazat ani modifikovat.

- ***Blokovat vše*** - systémový profil ***Blokovat vše*** je přednastaveným profilem a je k dispozici za všech okolností. Jestliže je tento profil aktivován, je veškerá komunikace zakázána a počítač není dostupný z vnějších sítí ani sám nemůže žádnou komunikaci směrem ven navázat. Tento systémový profil nelze duplikovat, smazat ani modifikovat.

- ***Uživatelské profily***:

  - ***Přímé připojení k Internetu*** – vhodný pro běžné domácí počítače připojené přímo k Internetu nebo notebooky používané mimo chráněnou firemní síť. Tuto možnost zvolte například tehdy, pokud máte počítač připojený z domova nebo se jedná o malou firemní síť bez centrální správy. Tato alternativa je rovněž vhodná pro připojení pomocí notebooku z různých neznámých a pravděpodobně naprosto nezabezpečených míst (*internetová kavárna, hotelový pokoj atd.*). Budou využita poměrně restriktivní pravidla, protože se nedá předpokládat přítomnost dalších bezpečnostních řešení a úkolem ***AVG Firewallu*** je zajistit pokud možno co nejvyšší úroveň ochrany uživatele.

  - ***Počítač v doméně*** – vhodný pro počítače v lokální síti, například ve škole nebo ve firmě. Dá se předpokládat, že taková síť je chráněna dalšími prostředky (*například softwarovým nebo hardwarovým firewallem*) a úroveň její bezpečnosti je vyšší než u samostatně připojeného počítače. Proto budou nastavená pravidla méně restriktivní.

  - ***Malá domácí nebo kancelářská síť*** – vhodný pro počítače v malé síti, například doma nebo v menší firmě. Typicky se jedná jen o několik propojených počítačů bez možnosti centrální správy.

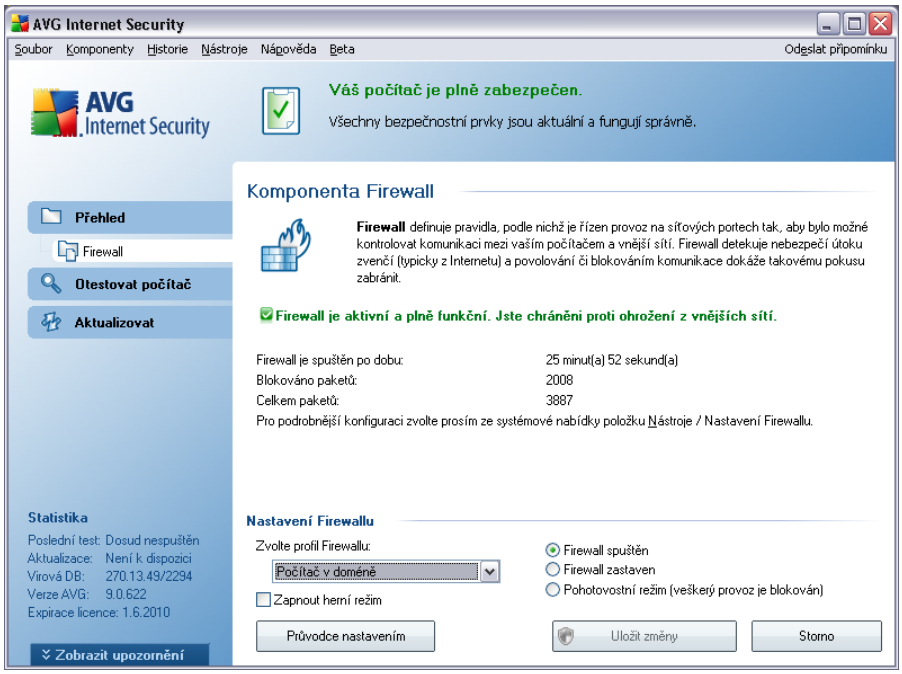
Přepínání profilů

Funkce přepínání profilů umožňuje ***Firewallu*** při použití určitého síťového adaptéru nebo při připojení k určité síti automatické přepnutí na definovaný profil. Pokud nebyl dané oblasti sítě dosud žádný profil přiřazen, pak bude při příštím připojení k této oblasti zobrazen dialog Firewallu, v němž budete vyzváni k přiřazení profilu.

Profily ,můžete přiřazovat všem lokálním síťovým rozhraním nebo oblastem a podrobné nastavení pak definovat v dialogu ***Profily sítí a adaptérů***, kde lze tuto vlastnost také zcela vypnout, pokud ji nechcete používat (*pak bude pro jakékoli připojení použit výchozí profil*).

Dá se předpokládat, že této vlastnosti využijí uživatelé s notebookem, kteří se připojují k mnoha různým sítím. Používáte-li nepřenosný stolní počítač a jste připojení vždy stejným typem připojení (*například kabelovým připojením k Internetu*), nemusíte se přepínáním profilů v podstatě vůbec zabývat.

8.3.3. Rozhraní komponenty Firewall



Rozhraní komponenty ***Firewall*** nabízí kromě základních informací o funkci komponenty také stručný statistický přehled:

- ***Firewall je spuštěn po dobu*** - celkový čas od posledního spuštění Firewallu
- ***Blokováno paketů*** - počet zablokovaných paketů z celkového počtu kontrolovaných
- ***Celkem paketů*** - celkový objem paketů kontrolovaných po dobu běhu Firewallu

Základní nastavení komponenty

- ***Zvolte profil Firewallu*** - v rozbalovací nabídce zvolte jeden z definovaných profilů - dva profily jsou dostupné vždy (*výchozí profil* ***Povolit vše*** *a* ***Blokovat vše***), další profily jste přidali ručně editací profilů v dialogu ***Profily*** v ***Nastavení Firewallu***

- ***Zapnout herní režim*** - chcete-li zajistit, aby v průběhu práce s aplikacemi, jež běží na celé obrazovce (hry, PowerPointové prezentace atd.) ***Firewall*** nezobrazoval dialogy s dotazy na povolení či zablokování komunikace u neznámých aplikací, označte tuto položku. Je-li tato volba zapnuta a dojde k situaci, kdy se neznámá aplikace pokusí navázat síťovou komunikaci, ***Firewall*** tento pokus zablokuje či povolí automaticky podle nastavení v aktuálně použitém profilu.

- ***Stav komponenty Firewall***:

  - ***Firewall spuštěn*** - touto volbou umožníte komunikaci těm aplikacím, pro něž je v pravidlech definovaných v rámci zvoleného profilu ***Firewall*** provoz povolen

  - ***Firewall zastaven*** - touto volbou vypnete ***Firewall***, veškerý síťový provoz je povolen a není kontrolován!

  - ***Nouzový režim (veškerý provoz je blokován)*** - touto volbou můžete v případě potřeby zastavit veškerý provoz na všech síťových portech; ***Firewall*** zůstává spuštěn, ale veškerý síťový provoz je blokován

Poznámka: *Všechny komponenty AVG jsou výrobcem nastaveny k optimálnímu výkonu. Pokud nemáte skutečný důvod jejich konfiguraci měnit, doporučujeme ponechat program ve výchozím nastavení. Změnu konfigurace by měli provádět pouze zkušení uživatelé. Chcete-li tedy změnit nastavení komponenty Firewall, zvolte ze systémového menu položku* ***Nástroje/Nastavení Firewallu*** *a editaci nastavení proveďte v nově otevřeném dialogu Nastavení Firewallu.*

Ovládací tlačítka dialogu

- ***Průvodce nastavením*** - tlačítkem přejdete do příslušného dialogu (***Zvolte způsob použití počítače***) v rámci instalačního procesu, v němž jste nastavovali konfigurací komponenty ***Firewall***

- ***Uložit změny*** - stiskem tlačítka budou uloženy všechny v tomto dialogu provedené změny

- ***Storno*** - stiskem tlačítka se vrátíte do výchozího uživatelského rozhraní AVG (*přehled komponent*)

8.4. LinkScanner

8.4.1. Princip Link Scanneru

Komponenta ***LinkScanner*** poskytuje ochranu proti internetovým stránkám, které byly vytvořeny záměrně za účelem infikování vašeho počítače přes internetový prohlížeč. Technologie ***LinkScanner*** se skládá ze dvou funkcí: ***AVG Search Shield*** a ***AVG Active Surf-Shield***.

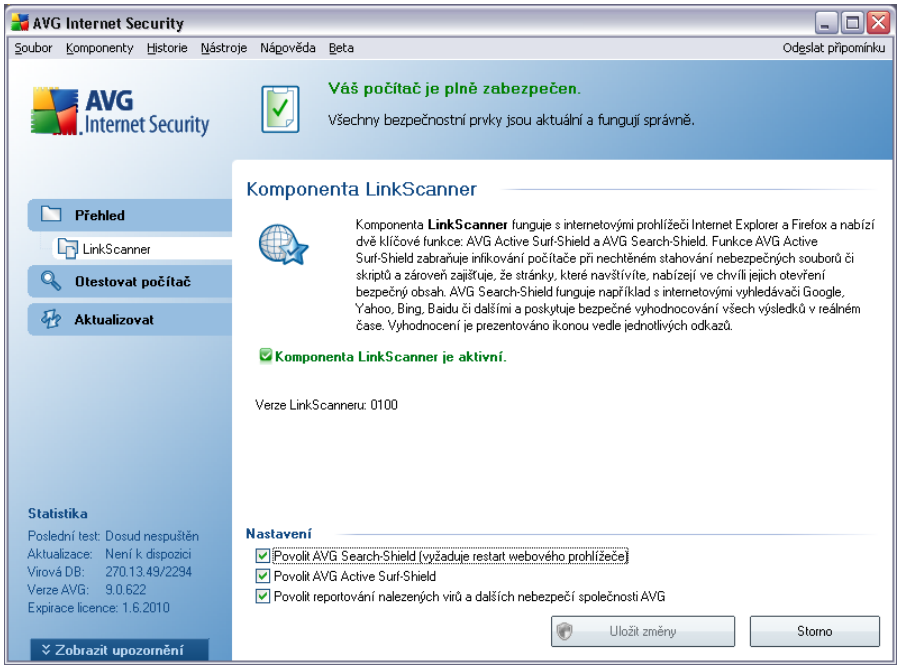
- ***AVG Search Shield*** obsahuje seznam stránek (*URL adres*), které jsou známy jako infikované. Při hledání skrze vyhledávače Google, Yahoo!, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, a SlashDot jsou všechny výsledky zkontrolovány na základě tohoto seznamu a ke každé položce je zobrazena verdiktová ikona (*pro výsledky ve vyhledávači Yahoo! jsou zobrazeny tyto verdiktové ikony pouze pro infikované stránky*).

- Funkce ***AVG Active Surf-Shield*** zabraňuje infikování počítače při nechtěném stahování nebezpečných souborů či skriptů a zároveň zajišťuje, že stránky, které navštívíte, nabízejí ve chvíli jejich otevření bezpečný obsah. Funkce testuje obsah internetových stránek, které navštěvujete, bez ohledu na internetovou adresu stránky. Pokud tedy nebyla určitá stránka detekována funkcí ***AVG Search Shield***, může být detekováná a blokována právě funkcí ***AVG Active Surf-Shield*** při přístupu na ni.

Poznámka: *AVG LinkScanner není určen k ochraně serverů!*

8.4.2. Rozhraní Link Scanneru

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



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

- ***Povolit AVG Search-Shield*** - (*ve výchozím nastavení zapnuto*): služba je aktivní při vyhledávání na serverech Google, Yahoo!, 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 AVG Active 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.

- ***Povolit reportování nalezených virů a dalších nebezpečí společnosti AVG*** - označte tuto položku, pokud se chcete zapojit do projektu zpětného reportování nebezpečných www stránek do databáze.

8.4.3. AVG Search-Shield

Při prohlížení Internetu se zapnutou kontrolou ***AVG Search-Shield*** budou všechny výsledky vyhledávání pomocí nejrozšířenějších vyhledavačů (Google, Yahoo!, 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! v rámci služby AVG Security Toolbar se tato ikona zobrazovat nebude!*).

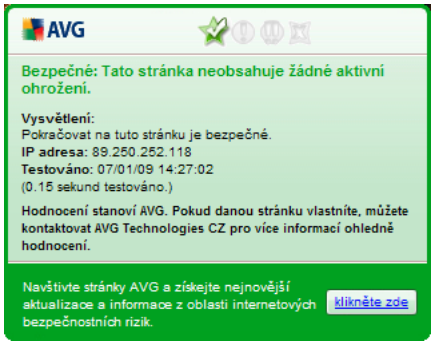
Odkazovaná stránka neobsahuje žádné konkrétní hrozby, ale jeví se jako podezřelá (*je sporný její původ či účel, proto ji nelze doporučit například pro aktivity typu on-line nakupování a podobně*).

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 přejezdu myší nad jednotlivými ikonami s hodnocením bezpečnosti odkazu se pak zobrazí detailní informace (*podrobnosti o hrozbě, pokud byla nalezena, IP adresa odkazu a datum kontroly odkazu službou AVG Search-Shield*) o odkazu:



Ikona VeriSign

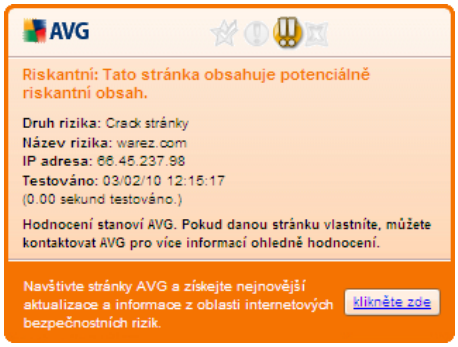
Kromě uvedených verdiktových ikon ***AVG Search Shieldu*** může být v prohlížeči zobrazena také ikona ***VeriSign*** . Její zobrazení se však vztahuje pouze ke stránkám, které jsou součástí programu Verisign Seal. Ikona ***VeriSign*** může být zobrazena vedle kteréhokoli odkazu ve výsledku hledání nebo vedle sponzorovaných odkazů. Například, pokud je stránka bezpečná, bude vedle zelené ikony ***AVG Search Shield*** zobrazena také ikona ***VeriSign***. Pokud je stránka vyhodnocena jako potenciálně riziková, budete o tom informováni obvyklou ikonou AVG.

Ikony ***VeriSign*** jsou podporovány v těchto vyhledávačích: Altavista, AOL, Ask, Baidu, Bing, Earthlink, Google, Seznam, Webhledani, Yandex a Yahoo!

8.4.4. AVG Active Surf-Shield

Ochrana pomocí ***AVG Active 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, ***AVG Active Surf-Shield*** přístup k této stránce okamžitě zablokuje. Mějte na paměti, že váš počítač se může velmi snadno poškodit při pouhé návštěvě infikované webové stránky.

Narazíte-li na nebezpečnou webovou stránku, ***AVG Link Scanner*** vás bude varovat tímto oznámením:

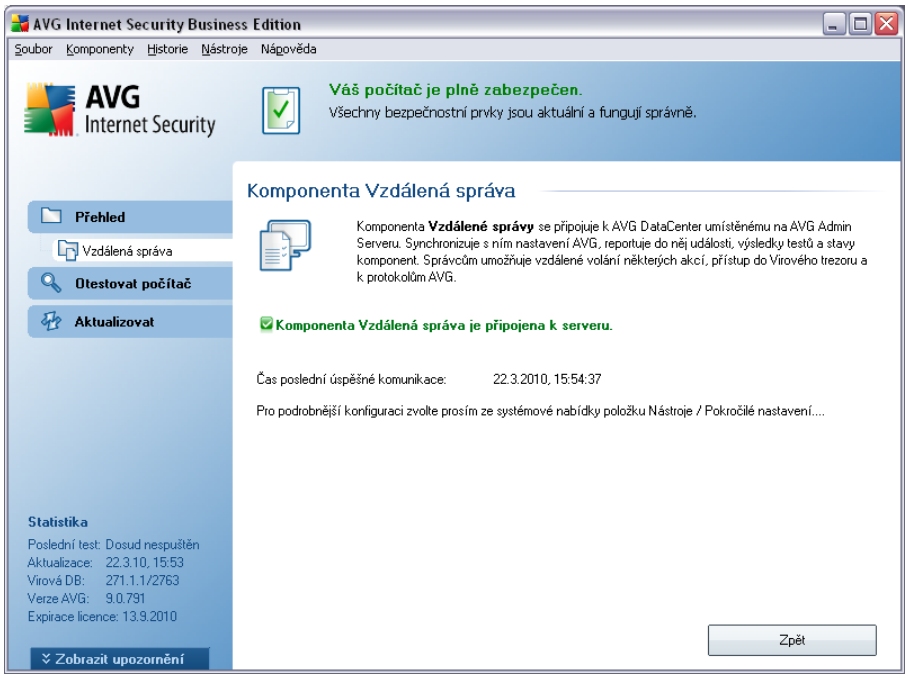


Vstup na takto označenou stránku rozhodně nedoporučujeme!

8.5. Anti-Rootkit

Rootkit je program speciálně vytvořený tak, aby dokázal převzít kontrolu nad vaším počítačem, aniž by požádal o jakoukoliv autorizaci. Většinou se nepokouší ovládnout hardware, jejich cílem je ovládnout vás 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 světě škodlivého kódu poměrně výsadní postavení, jelikož pronikají hluboko do systému, přebírají požadavky systémových volání a správné výsledky nahrazují svými vlastními.

8.6. Vzdálená správa



Komponenta ***zdálená správa*** se v uživatelském rozhraní **AVG 9 Anti Virus plus Firewall** 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 věnující se tomuto tématu, která je ke staženi na webu AVG (www.avg.cz) v sekci ***Centrum podpory / Stáhnout / Dokumentace***.

Ovládací tlačítka dialogu

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

8.7. Kontrola pošty

Jedním z nejčastějších zdrojů virů a trojských koní je e-mail. A díky phishingu a spamu se e-mail stává ještě větším zdrojem nebezpečí. Toto nebezpečí narůstá obzvláště u zdarma dostupných poštovních účtů (*protože u těch je použití anti-spamové technologie spíše výjimkou*), které stále používá většina domácích uživatelů. Tito uživatelé také často navštěvují neznámé webové stránky a nezřídka zadávají svá osobní data (*nejčastěji svou e-mailovou adresu*) do různých formulářů na webu, čímž ještě zvyšují riziko napadení prostřednictvím elektronické pošty. Větší společnosti většinou používají firemní poštovní účty a snaží se riziko minimalizovat implementací

anti-spamových filtrů.

8.7.1. 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 přijímání/odesílání pošty*).

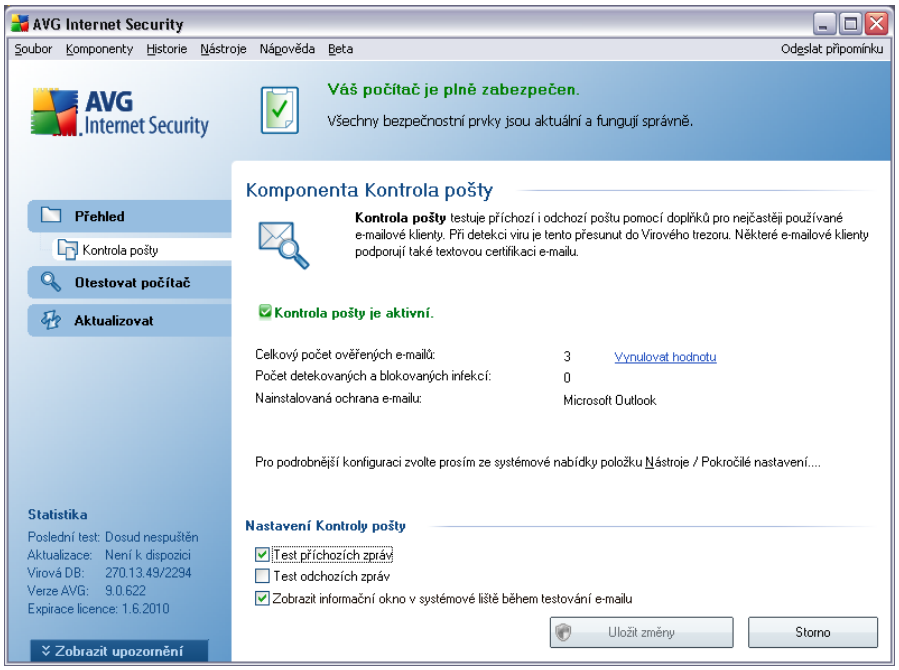
Kontrola pošty funguje jako rozhraní mezi e-mailovým klientem a e-mailovým serverem, umístěným na Internetu.

- ***Příchozí pošta***: Při přijímání poštovní zprávy ze serveru otestuje komponenta ***Kontrola pošty*** přijímanou zprávu, odstraní případné viry a přidá certifikační text či upozornění o odstranění virové přílohy. Nalezené viry jsou přemístěny 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!*

8.7.2. Rozhraní komponenty Kontrola pošty



V dialogu komponenty ***Kontrola pošty*** najdete stručný popis funkce komponenty, informaci o aktuálním stavu komponenty (*Komponenta Kontrola pošty je aktivní*) 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 začít počítat znovu - Vynulovat hodnotu*)
- ***Počet detekovaných a blokovaných 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*)

Základní nastavení komponenty

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 informační ikonu během testu e-mailu*** - označením položky definujete, zda si přejete zobrazit oznamovací dialog, který se objeví nad ikonou AVG na systémové liště při zahájení testování pošty komponentou ***Kontrola pošty***. Položka je ve výchozím nastavení zapnuta, doporučujeme toto nastavení ponechat.

Pokročilá editace konfigurace komponenty je k dispozici pod položkou ***Nástroje/ Pokročilé nastavení***, dostupnou ze systémového menu, ale tuto editaci doporučujeme jen zkušeným uživatelům!

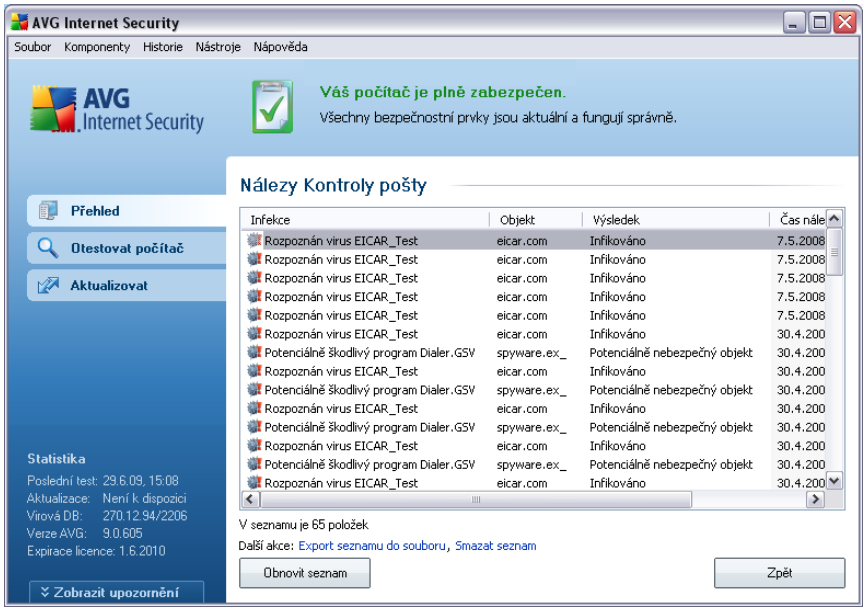
Poznámka: *Všechny komponenty AVG jsou výrobcem nastaveny k optimálnímu výkonu. Pokud nemáte skutečný důvod jejich konfiguraci měnit, doporučujeme ponechat program ve výchozím nastavení. Změnu konfigurace by měli provádět pouze zkušení uživatelé. Chcete-li tedy změnit nastavení programu AVG, zvolte ze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

8.7.3. Nálezy Kontroly pošty



V dialogu ***Nálezy Kontroly pošty*** (*dostupném ze systémového menu volbou položek Historie / Nálezy Kontroly pošty*) se bude zobrazovat seznam nálezů 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 nálezu*** - datum a čas detekce
- ***Typ objektu*** - jakého typu je detekovaný objekt

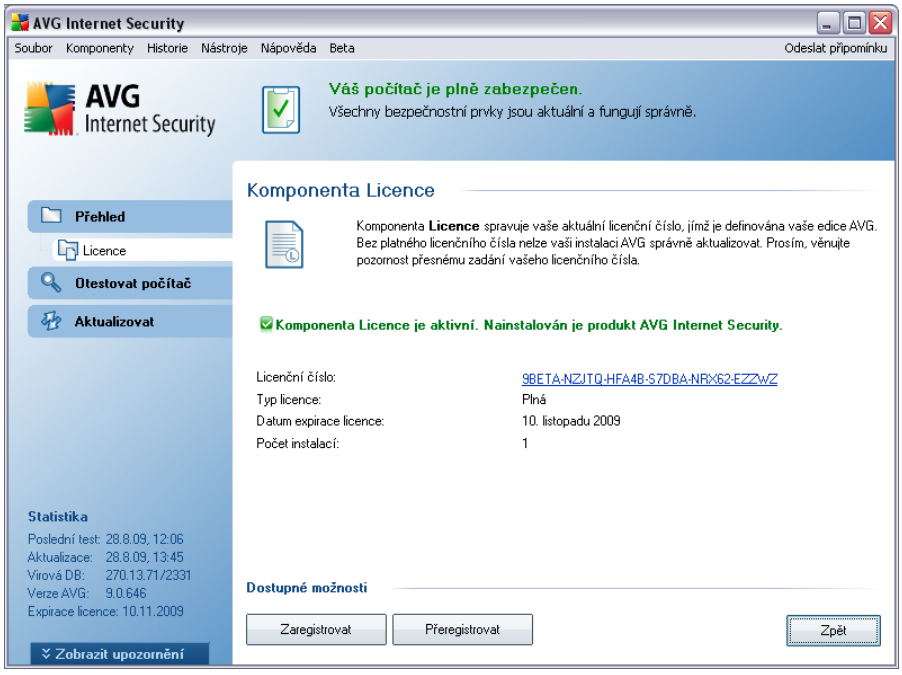
Pod seznamem pak najdete informaci o celkovém počtu detekovaných objektů. Dále máte možnost exportovat celý seznam detekovaných objektů do samostatného souboru (***Export seznamu do souboru***) a vymazat všechny záznamy o detekovaných objektech (***Smazat seznam***).

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

8.8. Licence



Na rozhraní příslušném komponentě ***Licence*** najdete tyto informace:

- ***Licenční číslo*** - uvádí zkrácený tvar vašeho licenčního čísla (*z bezpečnostních důvodů nejsou poslední čtyři 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/vložit.

- ***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 9 Anti Virus plus Firewall**, je třeba licenci prodloužit. Prodloužení licence lze provést on-line na webu AVG.

- ***Počet instalací*** - číslo udává počet stanic, na něž můžete **AVG 9 Anti Virus plus Firewall** 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.

- ***Přeregistrovat*** - 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 buďto nahradíte prodejní číslo (*s nímž jste AVG instalovali*), nebo kterým změníte dosavadní licenční číslo za jiné (*např. při přechodu na jiný produkt z řady AVG*).

Poznámka*: Máte-li nainstalovanou zkušební verzi* **AVG 9 Anti Virus plus Firewall***, 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 9 Anti Virus plus Firewall** *s prodejním číslem, tlačítka budou pojmenována* ***Zaregistrovat*** *a* ***Aktivovat****.*

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

8.9. Webový štít

8.9.1. 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!*

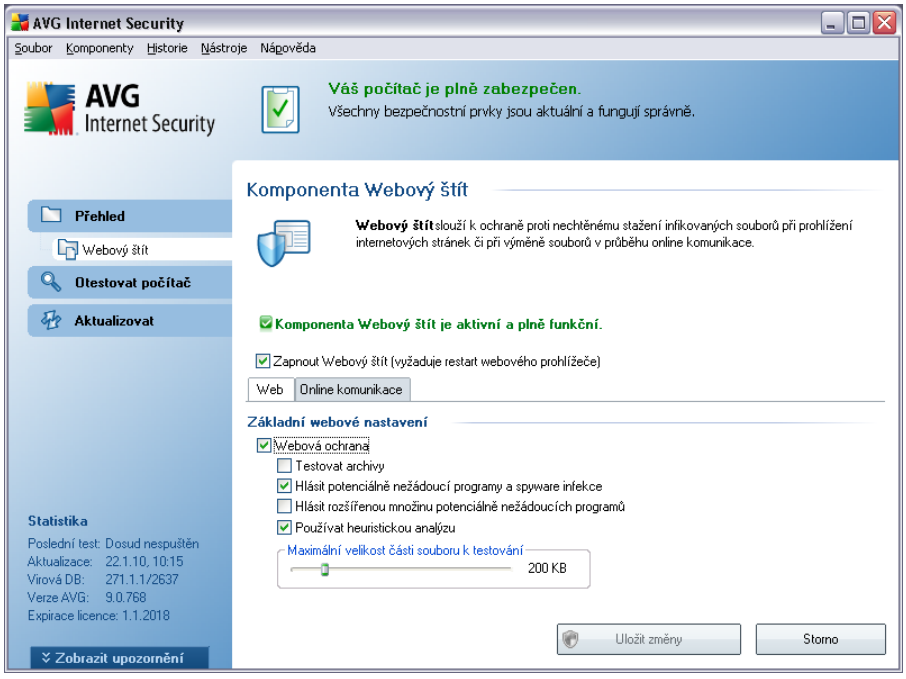
8.9.2. Rozhraní komponenty Webový štít

Rozhraní komponenty ***Webový štít*** popisuje princip fungování tohoto typu ochrany, poskytuje informaci o aktuálním stavu komponenty (*Komponenta Webový štít je aktivní a plně funkční.*) 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*** pomocí volby položky ***Zapnout Webový štít***. Tato položka je ve výchozím nastavení AVG zapnuta, komponenta je tedy aktivní. Pokud nemáte skutečný důvod toto nastavení měnit, doporučujeme ponechat komponentu vždy aktivní. Jestliže je položka označena a ***Webový štít*** spuštěn, jsou dostupné i další možnosti nastavení komponenty. Editace je rozdělena do dvou záložek:

- ***Web*** - zde máte možnost editovat nastavení komponenty pro kontrolu přístupu k webovým stránkám. Editační rozhraní nabízí nastavení těchto základních možností:



  - ***Webová ochrana*** - touto volbou potvrzujete, že v rámci komponenty ***Webový štít*** si přejete, aby byla prováděna kontrola obsahu navštěvovaných www stránek. Za předpokladu, že je tato volba zapnuta

(*výchozí nastavení*), můžete dále povolit nebo vypnout tyto volby:

- ***Testovat archívy*** - 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 malware, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány vědomě a se souhlasem uživatele. Doporučujeme nicméně ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.

- ***Hlásit rozšířenou množinu potenciálně nežádoucích programů*** - zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v původní 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*** - při testování webových stránek a stahovaných souborů používat detekční metodu heuristické analýzy, která spočívá v simulaci kódu v prostředí virtuálního počítače, takže lze tímto způsobem odhalit i škodlivý kód, který zatím není popsán ve virové databázi. (*viz Princip Anti-Viru*)

- ***Maximální velikost kontrolovaného souboru*** - 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 časově náročná a může výrazně zpomalit načítání www stránky. Posuvníkem tedy můžete nastavit maximální velikost souboru, který si přejete 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***.

- ***On-line komunikace*** - umožňuje editaci nastavení komponenty pro ochranu při on-line komunikaci (*to je pomocí programů pro okamžité zasílání zpráv, jakými jsou například ICQ, MSN Messenger, Yahoo ...*)

- ***Ochrana on-line komunikace*** - touto volbou potvrzujete, že v rámci komponenty ***Webový štít*** si přejete, aby byla prováděna kontrola on-line komunikace. Za předpokladu, že je tato volba zapnuta, můžete dále určit, pro který program pro rychlé zasílání zpráv má být kontrolován - v tuto chvíli **AVG 9 Anti Virus plus Firewall** podporuje aplikace ICQ, MSN a Yahoo.

Poznámka: *Všechny komponenty AVG jsou výrobcem nastaveny k optimálnímu výkonu. Pokud nemáte skutečný důvod jejich konfiguraci měnit, 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 proveďte v nově otevřeném dialogu Pokročilé nastavení AVG.*

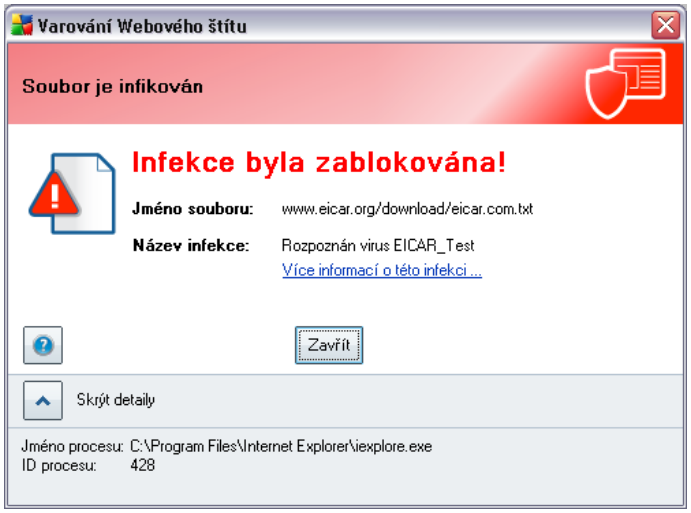
Ovládací tlačítka dialogu

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*)

8.9.3. Nálezy Webového štítu

Webový štít kontroluje v reálném čase obsah webových stránek nebo souborů 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:

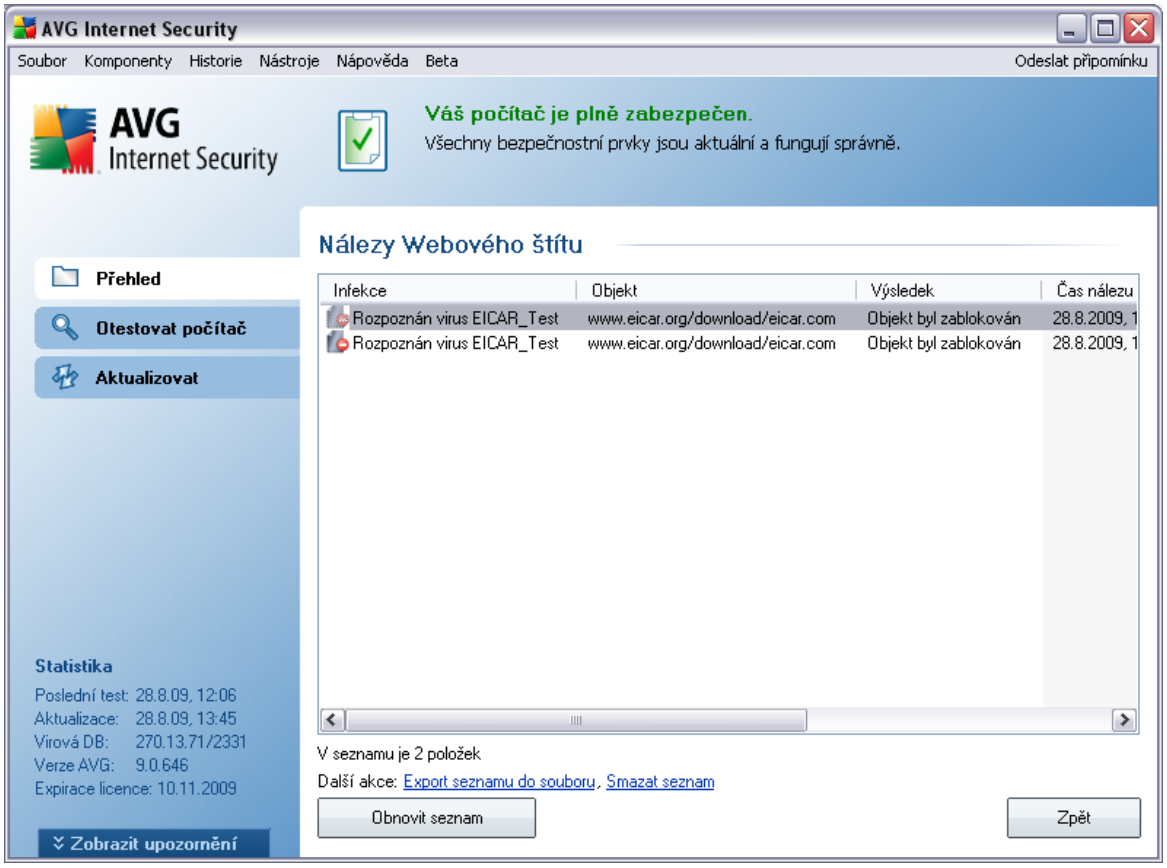


V tomto varovném dialogu najdete informaci o souboru, který byl detekován jako infikovaný (*Jméno souboru*) a jméno rozpoznané infekce (*Název infekce*), a odkaz do ***Virové encyklopedie***, kde najdete podrobnější informace o rozpoznané infekci, jsou-li tyto údaje známy. V dialogu jsou dostupná tato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

- ***Zobrazit/Skrýt detaily*** - kliknutím na tlačítko ***Zobrazit detaily*** otevřete v dolní části dialogu novou sekci s informací o procesu, při němž došlo k detekci infekce, a s uvedeným identifikačním číslem procesu. Tlačítkem ***Skrýt detaily*** pak můžete tuto sekci dialogu opět zavřít.

- ***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 i jméno*) detekovaného objektu
- ***Objekt*** - umístění detekovaného objektu (*stránka, odkud byl objekt stažen*)
- ***Výsledek*** - jak bylo s detekovaným objektem naloženo (*blokace*)
- ***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 (***Exportovat seznam do souboru***) a vymazat všechny záznamy o detekovaných objektech (***Smazat seznam***). Tlačítkem ***Obnovit seznam*** aktualizujete seznam všech nálezů a tlačítkem ***Zpět*** přejdete zpět do výchozího uživatelského rozhraní AVG (přehled komponent).

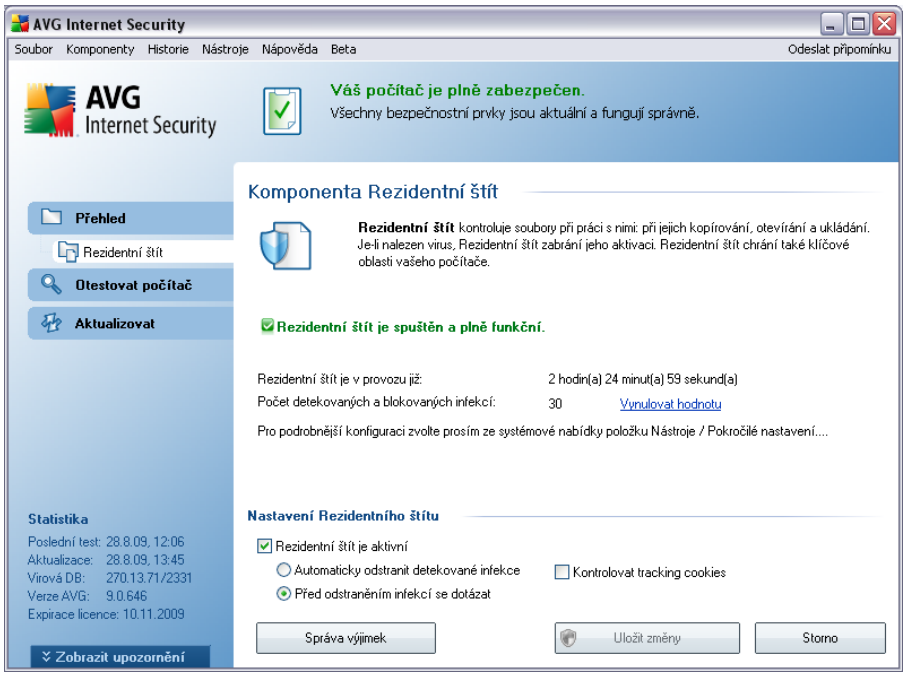
8.10. Rezidentní štít

8.10.1. 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*).

Upozornění: Rezidentní štít se načte do paměti počítače automaticky, ihned po spuštění, a je nanejvýš důležité, aby byl zapnutý nepřetržitě!

8.10.2. Rozhraní komponenty Rezidentní štít



Rozhraní ***Rezidentního štítu*** nabízí kromě popisu funkce komponenty a informace o jejím aktuálním stavu (*Rezidentní štít je spuštěn a plně funkční.*) také přehled nejdůležitějších 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 blokovaných infekcí -*** uvádí počet objektů detekovaných Rezidentním štítem jako infikované (*v případě potřeby, například pro statistické účely, lze tuto hodnotu vynulovat - Vynulovat hodnotu*)

Základní nastavení komponenty

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 neovlivňuje 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 odůvodněných 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 jejich konfiguraci měnit, 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 proveďte v nově otevřeném dialogu Pokročilé nastavení AVG.*

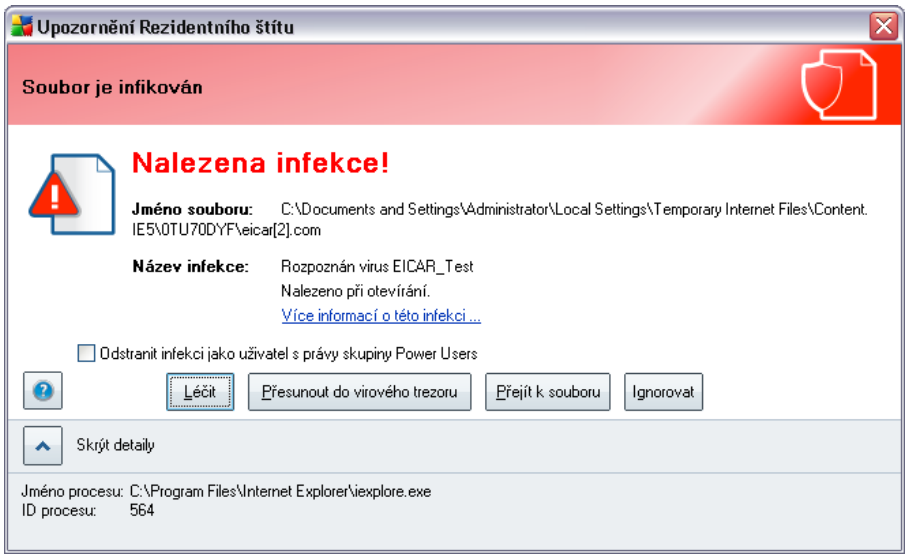
Ovládací tlačítka dialogu

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

- ***Správa výjimek*** - otevírá dialogové okno ***Výjimky Rezidentního štítu***, v němž lze definovat adresáře 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)

8.10.3. 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. V dialogu jsou dostupná tato tlačítka:

- ***Zobrazit/Skrýt detaily*** - kliknutím na tlačítko ***Zobrazit detaily*** otevřete v dolní části dialogu novou sekci s informací o procesu, při němž došlo k detekci infekce, a s uvedeným identifikačním číslem procesu. Tlačítkem ***Skrýt detaily*** pak můžete tuto sekci dialogu opět zavřít.

Dále je třeba, abyste se rozhodli, co se má s infikovaným souborem udělat:

- ***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 detekovanou ifekci 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***

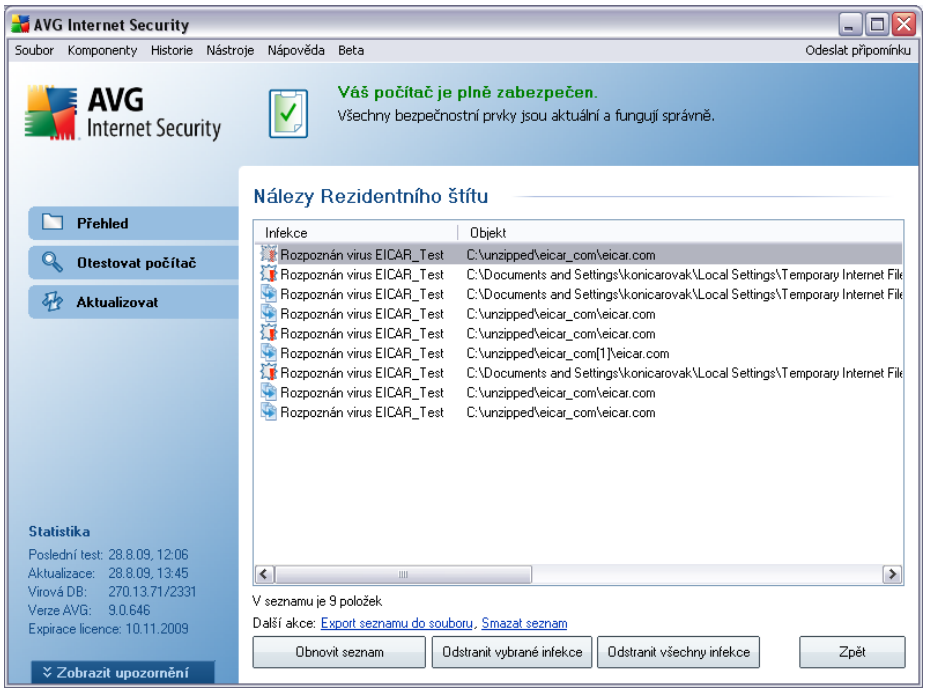
- ***Přejít k souboru*** - touto volbou zjistíte, kde je podezřelý objekt fyzicky

umístěn (*otevře se nové okno Průzkumníka Windows*)

- ***Ignorovat*** - tuto možnost rozhodně nedoporučujeme nikomu, kdo nemá skutečně dobrý důvod ji použít!

- ***Zobrazit/Skrýt detaily*** - toto tlačítko se zobrazuje střídavě v jedné nebo druhé pozici a nabízí podrobnou informaci o jménu a cestě k souboru, o názvu detekované infekce a o detailech procesu (*spuštěné aplikace*), během nějž byla infekce detekována

Celkový přehled o všech hrozbách detekovaných ***Rezidentním štítem*** najdete v dialogu ***Nálezy 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 buďto vyléčeny 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*** přejdete zpět do výchozího uživatelského rozhraní AVG (přehled komponent).

8.11. Manažer aktualizací

8.11.1. Princip Manažeru aktualizací

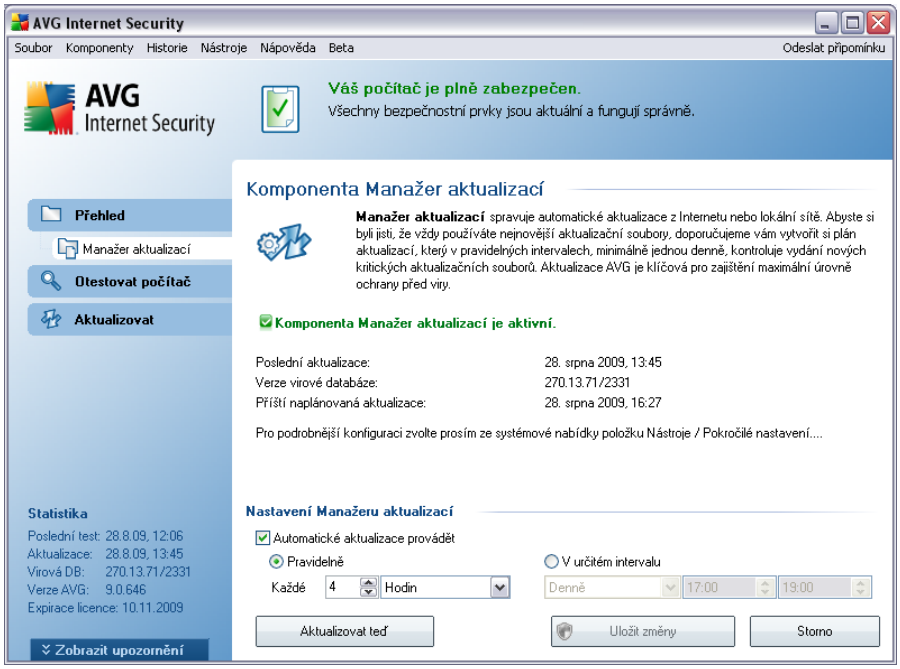
Každý bezpečnostní software může zajistit skutečnou ochranu vašeho počítače před různými typy nebezpečí pouze tehdy, je-li pravidelně aktualizován. Autoři virů stále hledají nové a nové trhliny v operačních systémech i softwarových aplikacích a snaží se jich zneužít. Denně se objevují nové viry, nový 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 aktualizačních balíků 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 čtěte prosím kapitolu Aktualizace AVG!*

8.11.2. Rozhraní komponenty Manažer aktualizací



Rozhraní komponenty ***Manažer aktualizací*** informuje o základní funkčnosti této komponenty, aktuálním stavu komponenty (*Komponenta Manažer aktualizací je aktivní*) 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

Základní nastavení komponenty

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 ověřovány a spouštěny:

- ***Pravidelně*** - určete v jakém časovém intervalu
- ***V konkrétním čase*** - 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. 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 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)

9. AVG Security Toolbar

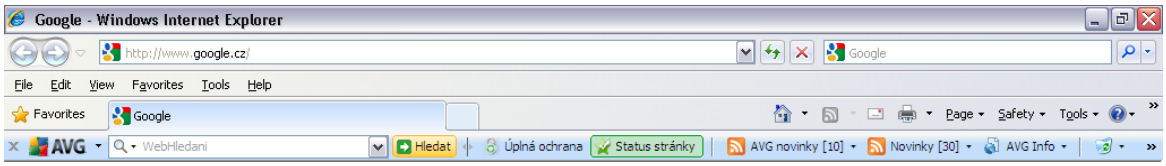
AVG Security Toolbar je nástroj, který úzce spolupracuje s komponentou ***AVG LinkScanner***. ***AVG Security Toolbar*** umožňuje úpravu nastavení komponenty **AVG 9 Anti Virus plus Firewall** přímo z prostředí internetového prohlížeče.

Pokud se rozhodnete ***AVG Security Toolbar*** nainstalovat, najdete jej v podobě nástrojové lišty ve vašem internetovém prohlížeči Internet Explorer a/nebo Mozilla Firefox. Jiné prohlížeče nejsou podporovány.

Poznámka: *Pokud používáte alternativní prohlížeč (např. Avant browser), můžete se setkat s nekorektním chováním.*

9.1. Rozhraní AVG Security Toolbaru

AVG Security Toolbar podporuje internetové prohlížeče ***MS Internet Explorer*** (*verze 6.0 a vyšší*) a ***Mozilla Firefox*** (*verze 3.0 a vyšší*). Pokud se rozhodnete nainstalovat ***AVG Security Toolbar*** (*možnost rozhodnout se, zda tuto komponentu chcete instalovat, jste měli v průběhu instalačního procesu*), bude panel s bezpečnostními prvky zobrazen ve vašem internetovém prohlížeči přímo pod řádkem pro zadání adresy v prohlížeči:



AVG Security Toolbar je tvořen těmito prvky:

9.1.1. Logo AVG

Přes rozbalovací menu pod tlačítkem s logem AVG máte přístup k obecným položkám bezpečnostního panelu. Kliknutím na logo AVG otevřete web AVG. Kliknutím na šipku po pravé straně loga AVG pak rozbalíte tuto nabídku:

- ***Informace o Toolbaru*** - tímto odkazem budete přesměrováni na domovskou stránku ***AVG Security Toolbar***, na níž najdete podrobnější informace o všech vlastnostech a možnostech bezpečnostního panelu AVG
- ***Spustit AVG 9.0*** - otevře uživatelské rozhraní ***AVG 9 Anti Virus plus Firewall***
- ***Nastavení*** - odkaz otevírá konfigurační dialog, v němž můžete editovat nastavení ***AVG Security Toolbar*** podle svých potřeb - viz následující kapitolu ***Nastavení AVG Security Toolbaru***
- ***Smazat historii*** - tlačítko umožňuje přímo v panelu ***AVG Security Toolbar*** buďto smazat celou historii, anebo jednotlivě smazat historii vyhledávání, smazat historii prohlížeče, smazat historii stahování a smazat cookies.
- ***Aktualizace*** - zkontroluje existenci aktualizační souborů pro ***AVG Security***

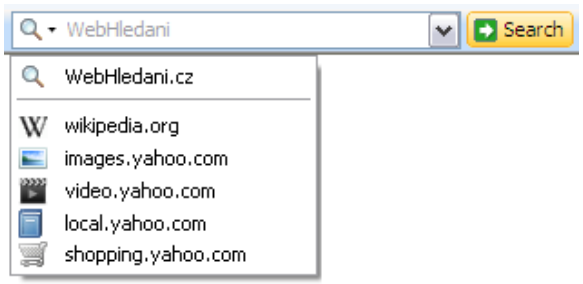
Toolbar

- ***Nápověda*** - prostřednictvím této položky můžete otevřít online nápovědu k ***AVG Security Toolbar***, kontaktovat technickou podporu, poslat nám svůj názor na tento produkt a/nebo si zobrazit informace o své verzi ***AVG Security Toolbar*** i samotné aplikaci AVG.

9.1.2. Vyhledávací pole WebHledani

Pomocí vyhledávání přes ***WebHledani*** můžete snadno prohledávat web a mít jistotu, že všechny zobrazené výsledky budou zaručeně bezpečné. Do vyhledávacího pole zadejte klíčové slovo nebo frázi a stiskněte talčítko ***Hledat*** nebo klávesu ***Enter*** - tím spustíte vyhledávání přímo na serveru WebHledani bez ohledu na to, jaká stránka je momentálně zobrazena. Vyhledávání také zaznamenává historii vašeho hledání. Všechny výsledky vyhledávání přes WebHledani jsou průběžně kontrolovány komponentou ***AVG Search-Shield***.

Alternativně můžete ve vyhledávacím poli zvolit vyhledávání ve ***Wikipedii*** nebo pomocí jiné specializovné vyhledávací služby, viz obrázek:



9.1.3. Úroveň zabezpečení

Tlačítko ***Úplná ochrana/Částečná ochrana/Žádná ochrana*** kontroluje stav komponent ***AVG Active Surf-Shield*** a ***AVG Search-Shield***. *Úplná ochrana* znamená, že jsou zapnuty obě, *Částečná ochrana* značí, že je zapnuto pouze jedno, a *Žádná ochrana*, že jsou obě vypnuty. Po stisknutí tlačítka se zobrazí dialog AVG Security Toolbar Nastavení na záložce ***Bezpečnost***.

9.1.4. Status stránky

Tlačítko zobrazuje přímo v liště toolbaru vyhodnocení aktuálně zobrazené stránky podle kriterií komponenty ***AVG Active Surf-Shield***:

- Odkazovaná stránka je bezpečná (u výsledků dodaných z vyhledávání Yahoo! v rámci služby ***AVG Security Toolbar*** se tato ikona zobrazovat nebude!).
- Stránka se jeví jako podezřelá.
- Stránka obsahuje odkazy na nebezpečné stránky.
- Stránka obsahuje aktivní hrozby. Pro vlastní bezpečnost vám nebude

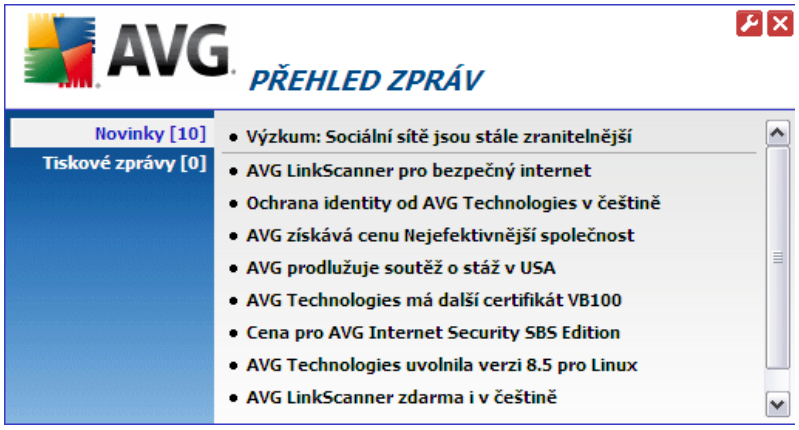
umožněno na tuto stránku vstoupit.

- Stránka je nepřístupná a nemohla být prověřena

Kliknutím na tuto položku otevřete informační panel s podrobným popisem statutu dané stránky.

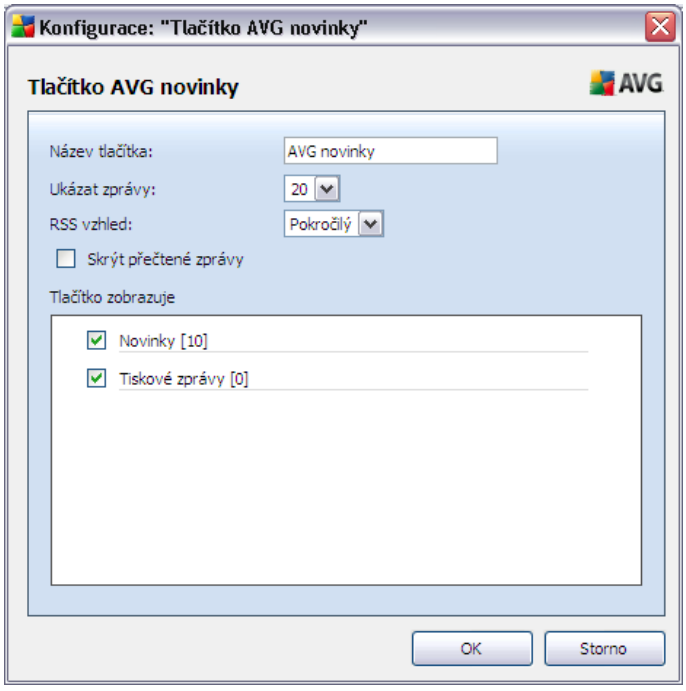
9.1.5. AVG novinky

Přímo v prostředí ***AVG Security Toolbaru*** otevřete tímto tlačítkem aktuální ***Přehled zpráv*** o AVG, ať už jde o zprávy z tisku nebo tisková prohlášení společnosti AVG:



V pravém horním rohu přehledu jsou k dispozici dvě červená ovládací tlačítka:

- - tlačítko otevírá editační dialog, v němž můžete nastavit parametry tlačítka ***AVG novinky***, zobrazeného v ***AVG Security Toolbaru***:

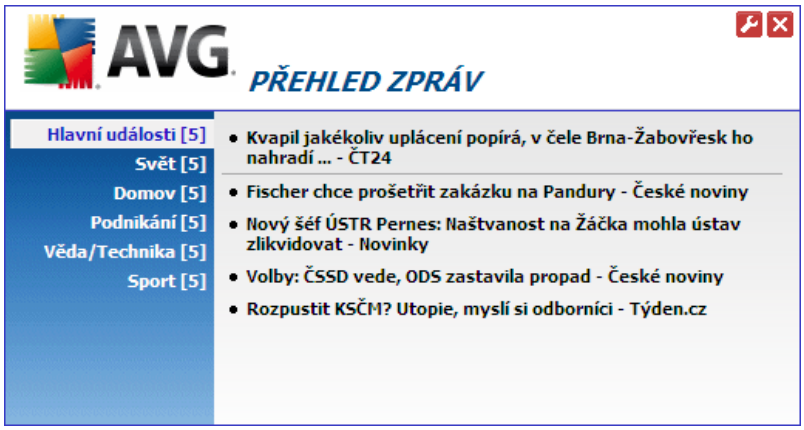


- ***Název tlačítka*** - máte možnost změnit název tlačítka, jak bude zobrazen v ***AVG Security Toolbaru***
- ***Ukázat zprávy*** - můžete si nastavit požadovaný počet zpráv, které mají být aktuálně zobrazeny
- ***RSS vzhled*** - volbou Pokročilý/Základní si můžete zvolit si vzhled aktuálního zobrazení přehledu zpráv (***výchozí je pokročilé nastavení, viz obrázek výše***)
- ***Skrýt přečtené zprávy*** - označením této položky potvrzujete, že každá již přečtená zpráva nemá být nadále zobrazována v přehledu zpráv a uvolní tak místo nové zprávě
- ***Tlačítko zobrazuje*** - v tomto poli pak můžete označit, které kategorie zpráv mají být v přehledu v prostředí ***AVG Security Toolbaru*** zobrazovány

- - kliknutím na toto tlačítko zavřete právě rozbalený přehled zpráv

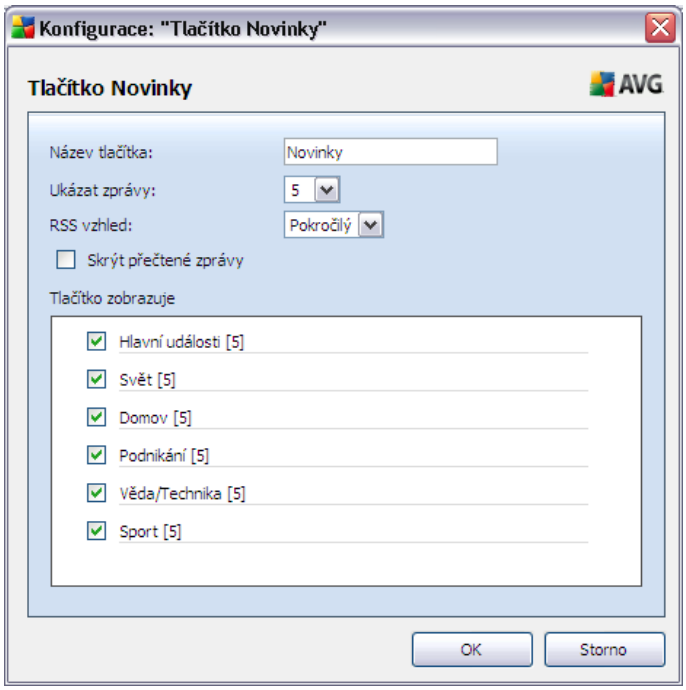
9.1.6. Novinky

Podobně, přímo v prostředí ***AVG Security Toolbaru*** otevřete tímto tlačítkem aktuální ***Přehled zpráv*** z vybraných médií rozdělený do tématických sekcí:



V pravém horním rohu přehledu jsou k dispozici dvě červená ovládací tlačítka:

-  - tlačítko otevírá editační dialog, v němž můžete nastavit parametry tlačítka ***Novinky***, zobrazeného v ***AVG Security Toolbaru***:



  - ***Název tlačítka*** - máte možnost změnit název tlačítka, jak bude zobrazen v ***AVG Security Toolbaru***
  - ***Ukázat zprávy*** - můžete si nastavit požadovaný počet zpráv, které mají být aktuálně zobrazeny

- ***RSS vzhled*** - volbou Pokročilý/Základní si můžete zvolit si vzhled aktuálního zobrazení přehledu zpráv (***výchozí je pokročilé nastavení, viz obrázek výše***)

- ***Skrýt přečtené zprávy*** - označením této položky potvrzujete, že každá již přečtená zpráva nemá být nadále zobrazována v přehledu zpráv a uvolní tak místo nové zprávě

- ***Tlačítko zobrazuje*** - v tomto poli pak můžete označit, které kategorie zpráv mají být v přehledu v prostředí ***AVG Security Toolbaru*** zobrazovány

-  - kliknutím na toto tlačítko zavřete právě rozbalený přehled zpráv

9.1.7. AVG Info

Tímto tlačítkem otevřete nabídku s odkazy na důležité obecně bezpečnostní informace a informace týkající se **AVG 9 Anti Virus plus Firewall**:

- ***Informace o Toolbaru*** - tímto odkazem budete přesměrováni na domovskou stránku ***AVG Security Toolbar***, na níž najdete podrobnější informace o všech vlastnostech a možnostech bezpečnostního panelu AVG

- ***Informace o hrozbách*** - zobrazí stránku na webu AVG, kde najdete důležitá data týkající se aktuálních hrozeb, doporučení pro odstraňování virů, informace o aktualizacích AVG, přístup do Virové encyklopedie a další relevantní informace

- ***AVG novinky*** - zobrazí webovou stránku s nejnovějšími tiskovými zprávami o AVG

- ***Aktuální úroveň nebezpečí*** - zobrazí webovou stránku virové laboratoře s grafickým znázorněním aktuálního stavu virové nákazy na webu

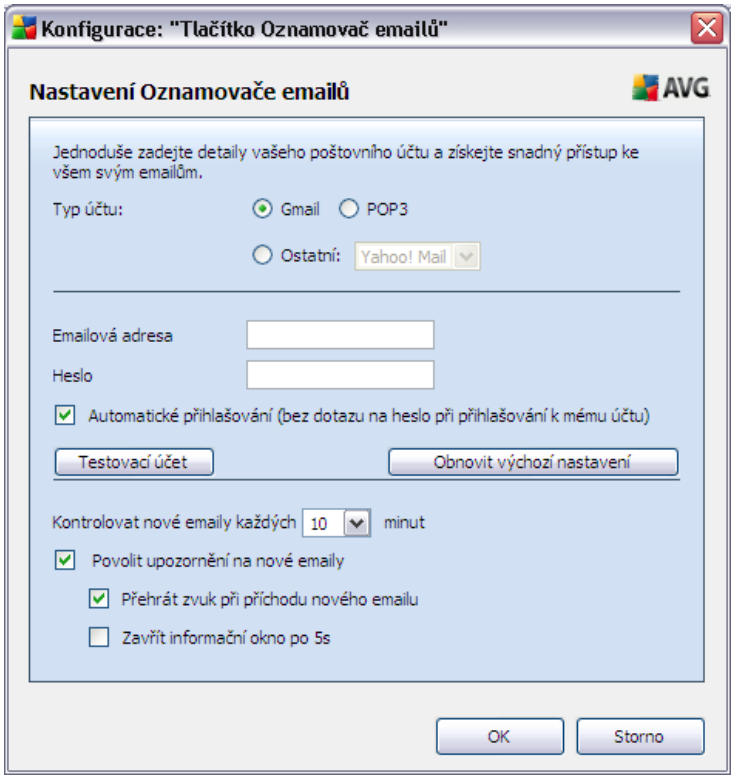
- ***Encyklopedie virů*** - zobrazí webovou stránku Virové encyklopedie s vyhledáváním, kde můžete získat detailní informace o jednotlivých typech virů

9.1.8. Smazat historii

Tímto tlačítkem můžete mazat historii vašeho prohlížeče obdobně jako prostřednictvím ***Logo AVG -> Smazat historii***.

9.1.9. Oznamovač e-mailů

Tlačítkem ***Oznamovač e-mailů*** můžete aktivovat možnost být upozorněni na doručené e-mailové zprávy přímo v prostředí ***AVG Security Toolbar***. Tlačítko otevírá následující editační dialog, v němž definujete parametry svého e-mailového účtu a pravidla pro zobrazování informací o doručených zprávách. Postupujte prosím podle instrukcí uvedených v dialogu:



9.2. Nastavení AVG Security Toolbaru

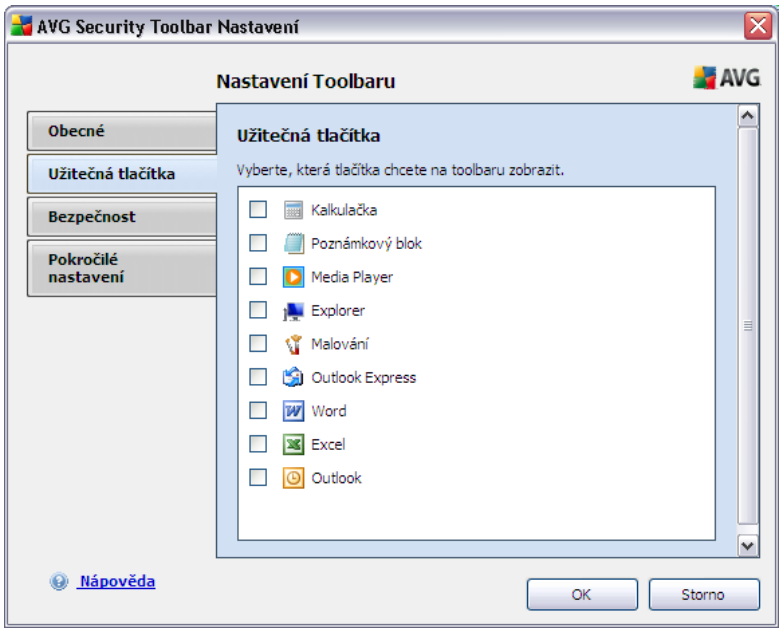
Veškeré nastavení parametrů ***AVG Security Toolbar*** probíhá na rozdíl od ostatních komponent **AVG 9 Anti Virus plus Firewall** přímo z panelu ***AVG Security Toolbar***. Editační rozhraní je dostupné volbou *AVG / Nastavení* a otevírá se v tomto samostatném dialogu nazvaném ***Nastavení Toolbaru*** rozděleném do čtyř sekcí:

9.2.1. Záložka Obecné

Na této záložce máte možnost označit, která ovládací tlačítka mají být v panelu AVG Security Toolbar zobrazena nebo naopak skryta. Označte jakoukoliv možnost, pokud chcete, aby byla formou tlačítka dostupná přímo z toolbaru. Následuje popis funkčnosti jednotlivých tlačítek:

- ***Tlačítko statusu stránky -*** tlačítko nabízí možnost zobrazení informace o statutu stránky přímo v panelu ***AVG Security Toolbaru***
- ***Tlačítko AVG novinky*** - tlačítko nabízí strukturovaný přehled s novinkami a tiskovými zprávami o AVG
- ***Tlačítko Novinky*** - tlačítko nabízí strukturovaný přehled aktuálních zpráv z denního tisku
- ***Tlačítko AVG Info*** - tlačítko poskytuje přehled informací o toolbaru, o aktuálních hrozbách na internetu, novinky o produktech AVG, informace o aktuální úrovni bezpečnosti a odkaz na encyklopedii virů
- ***Tlačítko Smazat historii*** - tlačítko umožňuje buďto smazat celou historii, anebo jednotlivě smazat historii vyhledávání, smazat historii prohlížeče, smazat historii stahování a smazat cookies
- ***Tlačítko oznamovač emailů*** - tlačítko umožňuje zobrazení doručených e-mailových zpráv přímo v prostředí ***AVG Security Toolbaru***

9.2.2. Záložka Užitečná tlačítka



Na záložce ***Užitečná tlačítka*** můžete výběrem ze seznamu označit aplikace, jejichž ikona má být zobrazena v AVG Toolbaru. Toto zobrazení pak funguje jako zkratkové tlačítko k okamžitému spuštění dané aplikace přímo z prostředí toolbaru.

9.2.3. Záložka Bezpečnost

Záložka ***Bezpečnost*** je rozdělena do dvou sekcí, ***AVG Bezpečné surfování*** a ***Hodnocení***, v nichž máte možnost označením příslušných políček zvolit, které funkce ***AVG Security Toolbar*** chcete využít:

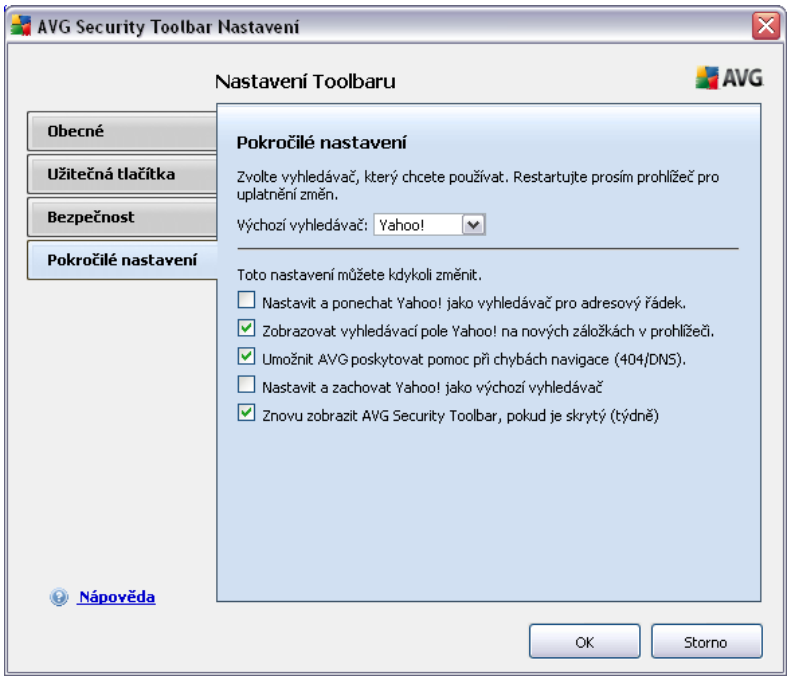
- ***AVG bezpečné surfování*** - označením položky aktivujete nebo naopak vypnete službu ***AVG Search-Shield*** a ***AVG Active Surf-Shield***

- ***Hodnocení*** - výběr položek v této sekci se týká označení výsledků vyhledávání komponentou ***AVG Search-Shield***, která vyhodnocuje jednotlivé odkazy grafickými symboly:

  - stránka je bezpečná
  - stránka se jeví jako podezřelá
  - stránka obsahuje odkazy na nebezpečné stránky
  - stránka obsahuje aktivní hrozby
  - stránka je nepřístupná a nemohla být prověřena

Volbou položek v tomto nastavení určíte, o kterých typech detekce si přejete být informování. Nemáte však možnost vypnout zobrazení červené ikony, která upozorňuje na skutečné a akutní nebezpečí. ***I zde však doporučujeme podržet nastavení definované výrobcem, pokud nemáte skutečný důvod tuto konfiguraci měnit***.

9.2.4. Záložka Pokročilé nastavení



Na záložce ***Pokročilé nastavení*** nejprve zvolte, jaký výchozí vyhledavač si přejete používat. V nabídce najdete tyto možnosti: *WebHledani, Baidu, Yahoo!, Yandex*.

Změníte-li výchozí vyhledavač, je třeba restartovat Váš internetový prohlížeč, aby změna vešla v platnost.

Dále můžete svou volbou aktivovat nebo vypnout další podrobné možnosti nastavení ***AVG Security Toolbaru***:

- ***Nastavit a ponechat WebHledani jako vyhledavač pro adresový řádek*** - Pokud je tato položka zapnuta a Vy vepíšete do adresového řádku jakékoliv klíčové slovo, bude toto slovo automaticky považováno za termín k vyhledávání a pro vyhledání relevantních stránek s tímto klíčovým slovem bude automaticky použita služba WebHledani.

- ***Zobrazovat vyhledávací pole Yahoo! na nových záložkách v prohlížeči*** - Položka je ve výchozím nastavení zapnuta a při otevření každé nové záložky ve Vašem prohlížeči zobrazí stránku s přímým vyhledáváním prostřednictvím Yahoo!

- ***Umožnit AVG poskytovat pomoc při chybách navigace (404/DNS)*** - Pokud při vyhledávání narazíte na neexistující stránku nebo stránku, jež nemůže být zobrazena (chyba 404), budete automaticky přesměrováni na stránku, která Vám umožní vyhledat alternativní tematicky příbuzné stránky pomocí nastaveného prohlížeče.

- ***Nastavit a zachovat WebHledani jako výchozí vyhledavač*** - WebHledani je výchozím vyhledávačem pro hledání v rámci ***AVG Security Toolbar***. Pokud chcete, aby se stal výchozím vyhledavačem vašeho internetového prohlížeče, označte tuto položku.

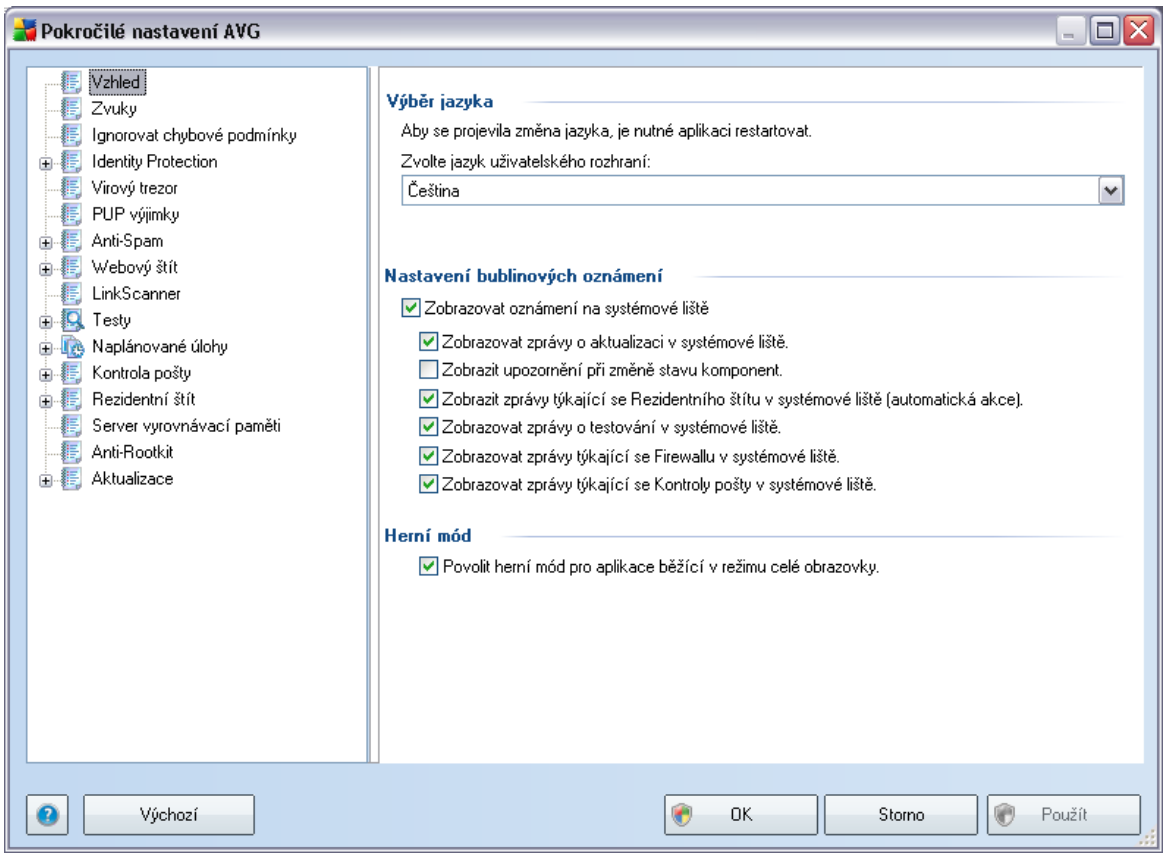
- ***Znovu zobrazit AVG Security Toolbar, pokud je skrytý (týdně)*** - Položka je ve výchozím nastavení aktivována a zajistí, že pokud dojde náhodou a nechtěně ke skrytí ***AVG Security Toolbaru***, bude jeho zobrazení po uplynutí jednoho týdne obnoveno.

10. Pokročilé nastavení AVG

Dialog pro pokročilou editaci nastaveni programu **AVG 9 Anti Virus plus Firewall** se otevírá v novém okně ***Pokročilé nastavení AVG***. Toto okno je rozděleno do dvou částí: v levé části okna najdete přehlednou stromově uspořádanou navigaci konfigurací programu. Volbou komponenty, jejíž parametry chcete editovat (*případně volbou konkrétní části této komponenty*) otevřete v pravé části okna příslušný editační dialog.

10.1. Vzhled

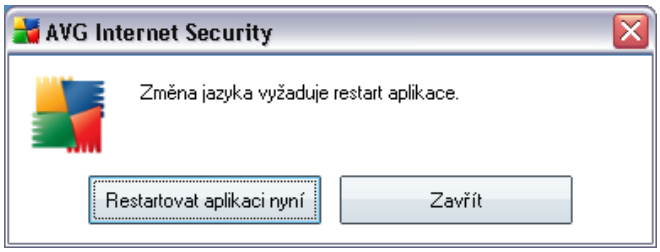
První položka navigačního seznamu, ***Vzhled***, se týká obecného nastavení uživatelského rozhraní aplikace a základních možností chování programu:



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 ***Uživatelská instalace - Zvolte komponenty***) 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*** zavřete 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 přinášejí typicky informace o změně stavu některé klíčové komponenty AVG a je vhodné věnovat 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 vztažených k určité komponentě **AVG 9 Anti Virus plus Firewall**. 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 informačních 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 aktualizačního procesu; 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*** - volbou položky rozhodnete, zda mají být zobrazena nebo naopak

potlačena informativní hlášení týkající se kontroly souborů při kopírování, otevírání nebo i ukládání (*toto nastavení se projeví 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 Firewallu v systémové liště*** - volbou položky rozhodnete, zda mají být zobrazena nebo naopak potlačena informativní hlášení o stavu a procesech týkajících se komponenty Firewall, například hlášení o aktivaci/deaktivaci komponenty, o aktuálním povolení či blokování provozu apod.; informace o ostatních procesech se budou zobrazovat normálně;

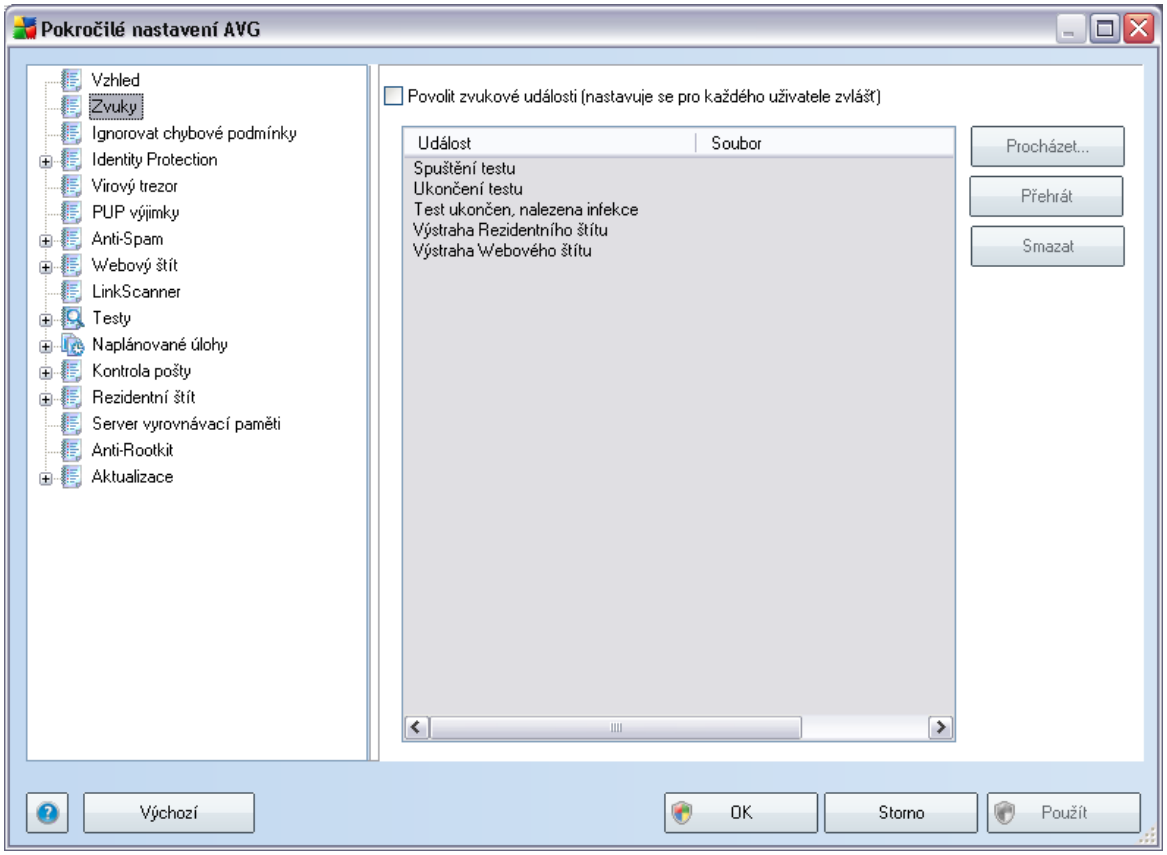
- ***Zobrazovat zprávy týkající se Kontroly pošty v systémové liště*** - volbou položky rozhodnete, zda mají být zobrazena nebo naopak potlačena informativní hlášení o průběhu testování příchozích a odchozích zpráv elektronické pošty; informace o ostatních procesech se budou zobrazovat normálně.

Herní mód

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

10.2. 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 vypnuta*) a tím aktivujete seznam akcí, k nimž je možné zvukový doprovod přiřadit:

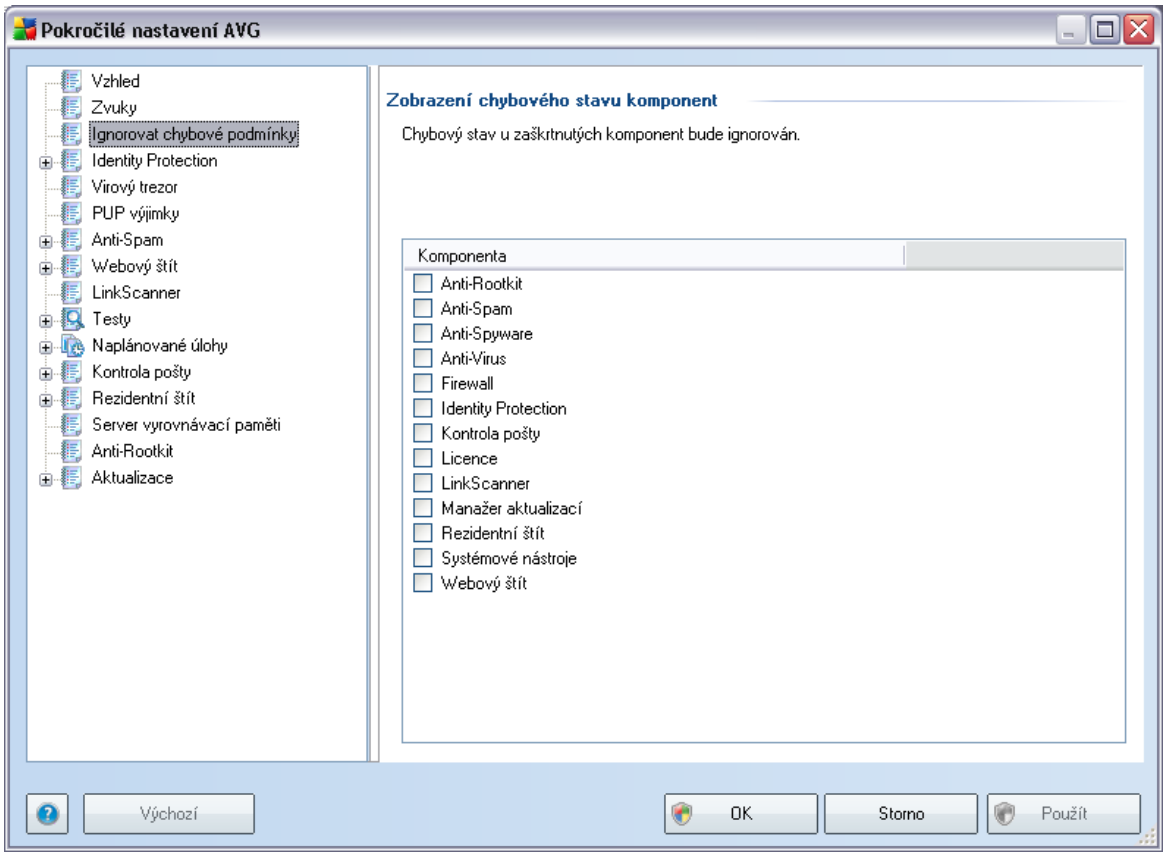


Poté vyberte ze seznamu konkrétní událost a tlačítkem ***Procházet*** zobrazte strukturu svého disku, kde vyberete příslušný zvuková soubor a zvolené akci jej přiřadíte. Chcete-li si přiřazený zvuk poslechnout, označte v seznamu příslušnou akci a stiskněte tlačítko ***Přehrát***. Tlačítkem ***Smazat***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

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

10.3. 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:

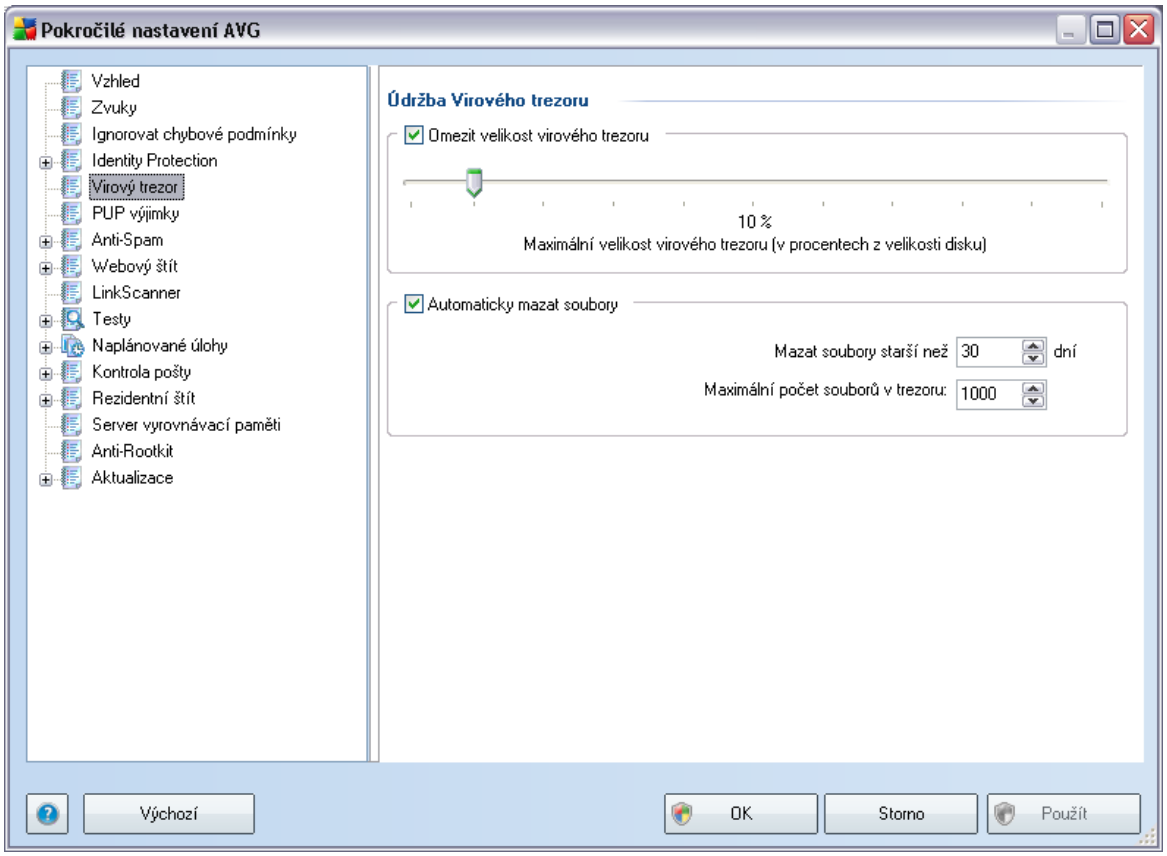
- ***ikony na systémové liště*** - pokud vše funguje jak má, je ikona zobrazena barevně; objeví-li se chyba, ikona se zobrazí se žlutým vykřičníkem
- textového popisu aktuálního problému v sekci ***Informace o stavu zabezpečení*** v hlavním okně AVG

Může se ale stát, že si z nějakého důvodu přejete dočasně 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 jej sami navodili a jste si vědomi 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 okně AVG.

10.4. Virový trezor



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

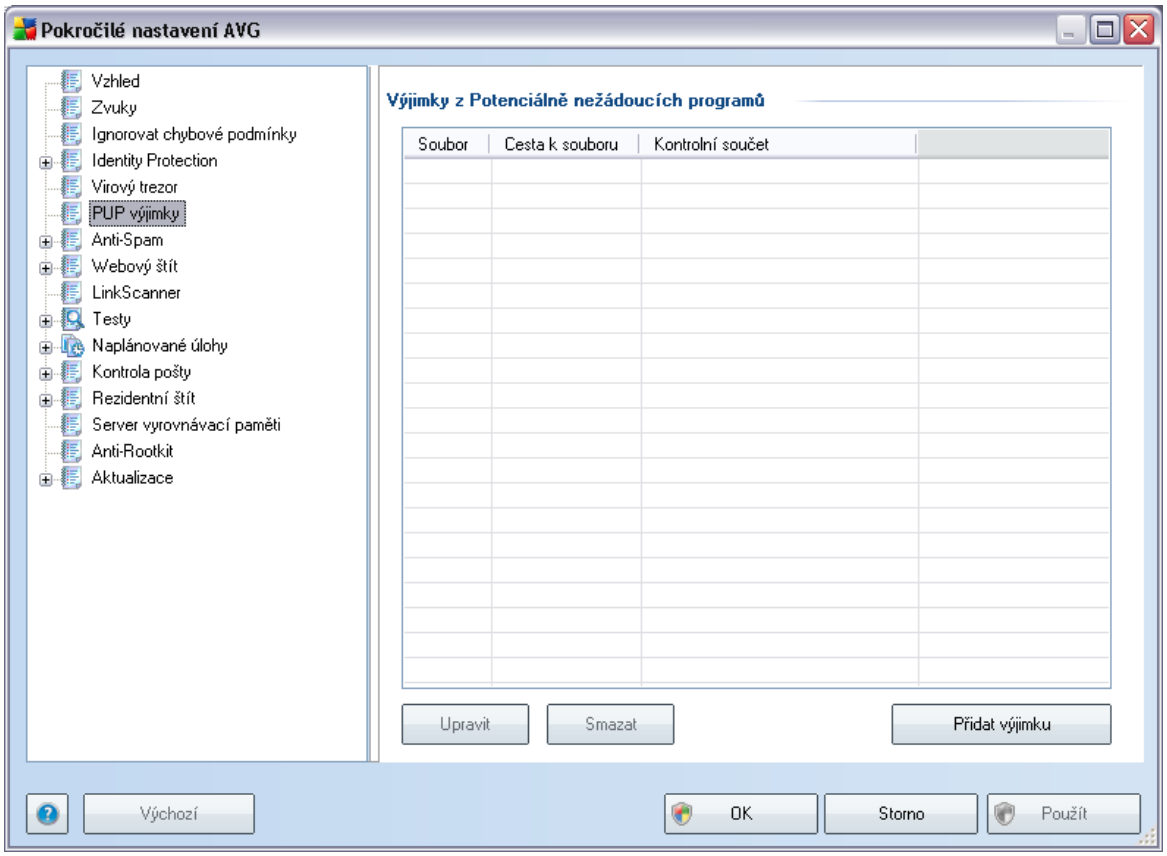
- ***Omezit velikost virového trezoru*** - na posuvníku můžete nastavit maximální povolenou velikost ***Virového trezoru***. Velikost je určena procentuálně jako poměrná část velikosti vašeho lokálního disku.

- ***Automaticky mazat soubory*** - v této sekci definujete maximální dobu, po niž 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***)

10.5. PUP výjimky

AVG 9 Anti Virus plus Firewall 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.

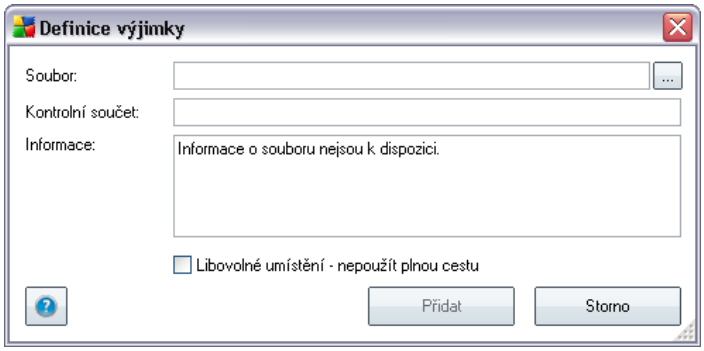


Dialog ***Výjimky z Potenciálně nežádoucích programů*** zobrazuje seznam již definovaných a aktuálně platných výjimek z potenciálně nežádoucích programů. Výjimku můžete editovat, smazat anebo nově přidat. Ke každé jednotlivé výjimce najdete v přehledu následující informace:

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

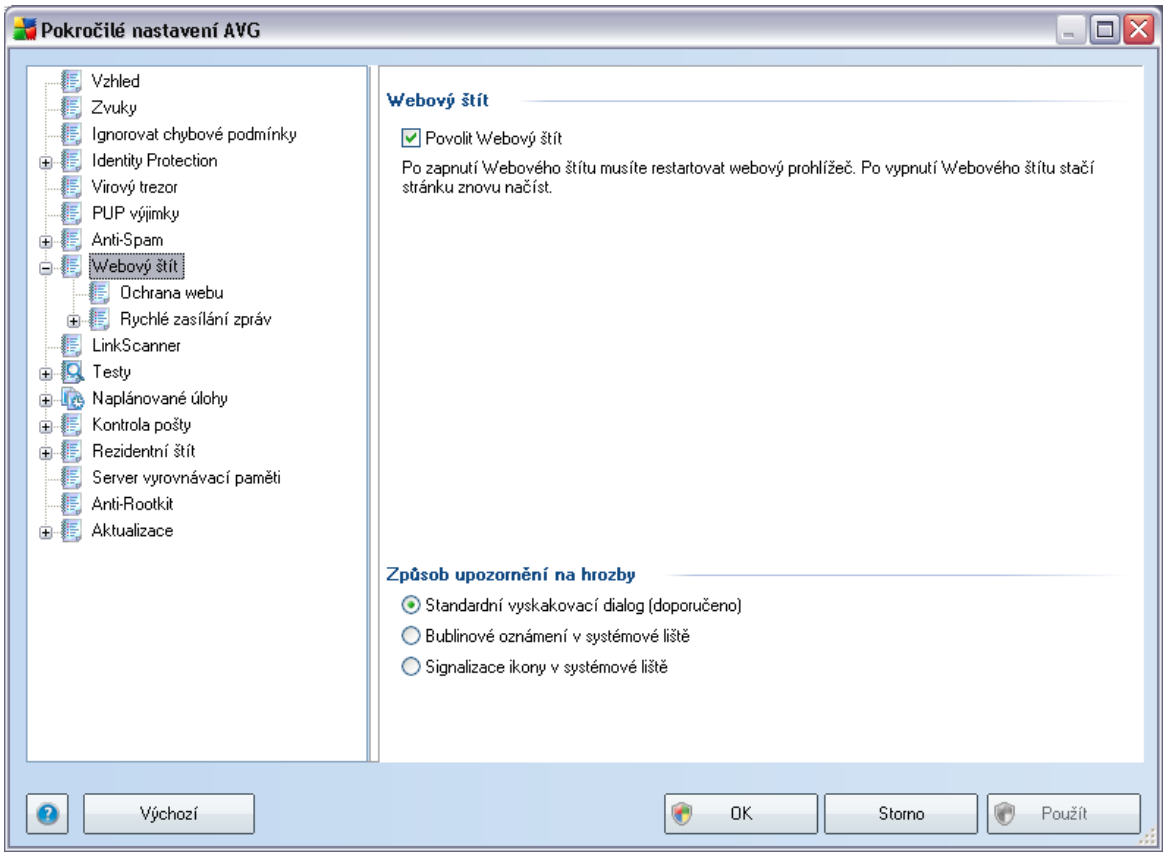
Ovládací tlačítka dialogu

- ***Upravit*** - otevře editační dialog (*totožný s dialogem pro zadání nové výjimky, viz níže*) již definované výjimky, kde můžete měnit 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. Je-li 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*).

10.6. Webový štít



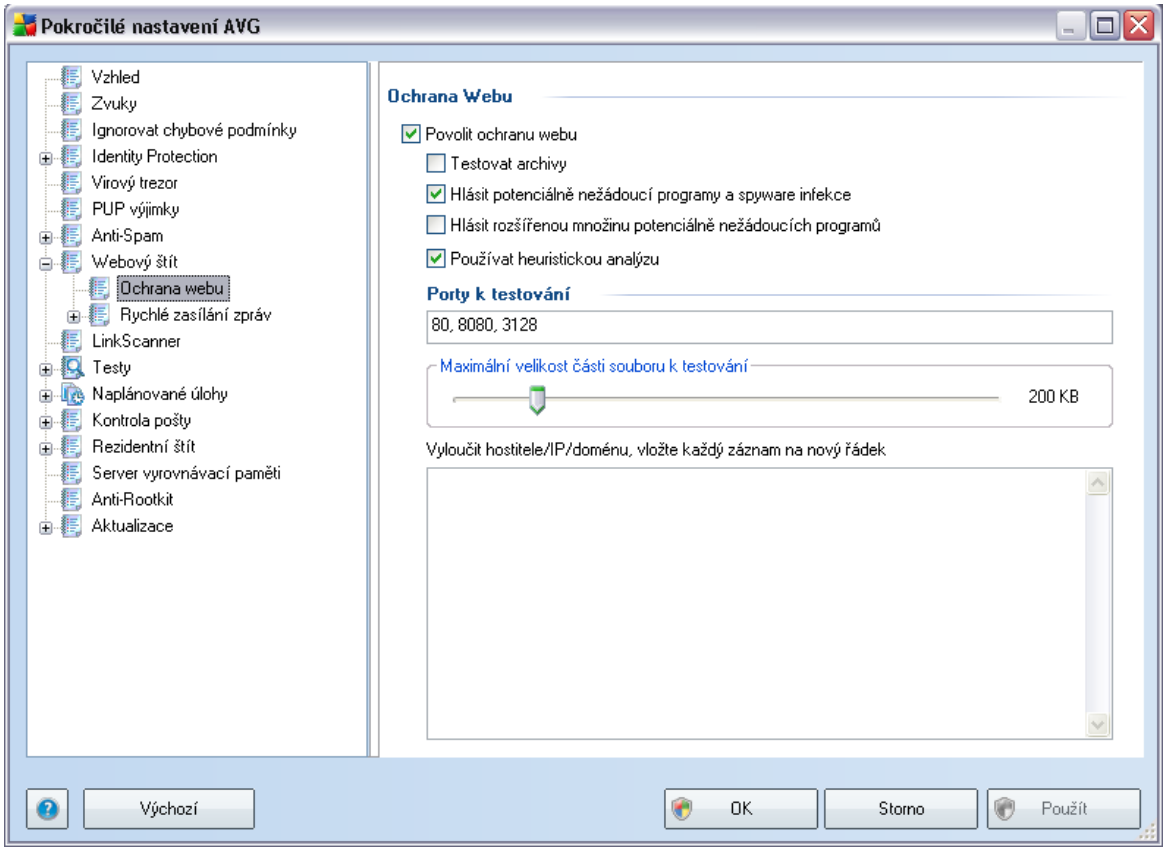
Dialog ***Webový štít*** nabízí možnost celkové aktivace/deaktivace komponenty ***Webový štít*** prostřednictvím označení položky ***Povolit Webový štít*** (*ve výchozím nastavení zapnuto*). Pokročilé nastavení této komponenty pak najdete na dalších hierarchicky řazených dialozích odkazovaných z navigace.

- ***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.

10.6.1. Ochrana webu



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

- ***Povolit ochranu webu*** - touto volbou potvrzujete, že v rámci komponenty ***Webový štít*** si přejete, aby byla prováděna kontrola obsahu navštěvovaných www stránek. Za předpokladu, že je tato volba zapnuta (*výchozí nastavení*), můžete dále povolit nebo vypnout tyto volby:
  - ***Testovat archívy*** - (*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 malware, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány vědomě a se souhlasem uživatele. Doporučujeme nicméně ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.

- ***Hlásit rozšířenou množinu potenciálně nežádoucích programů*** - zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v původní 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.

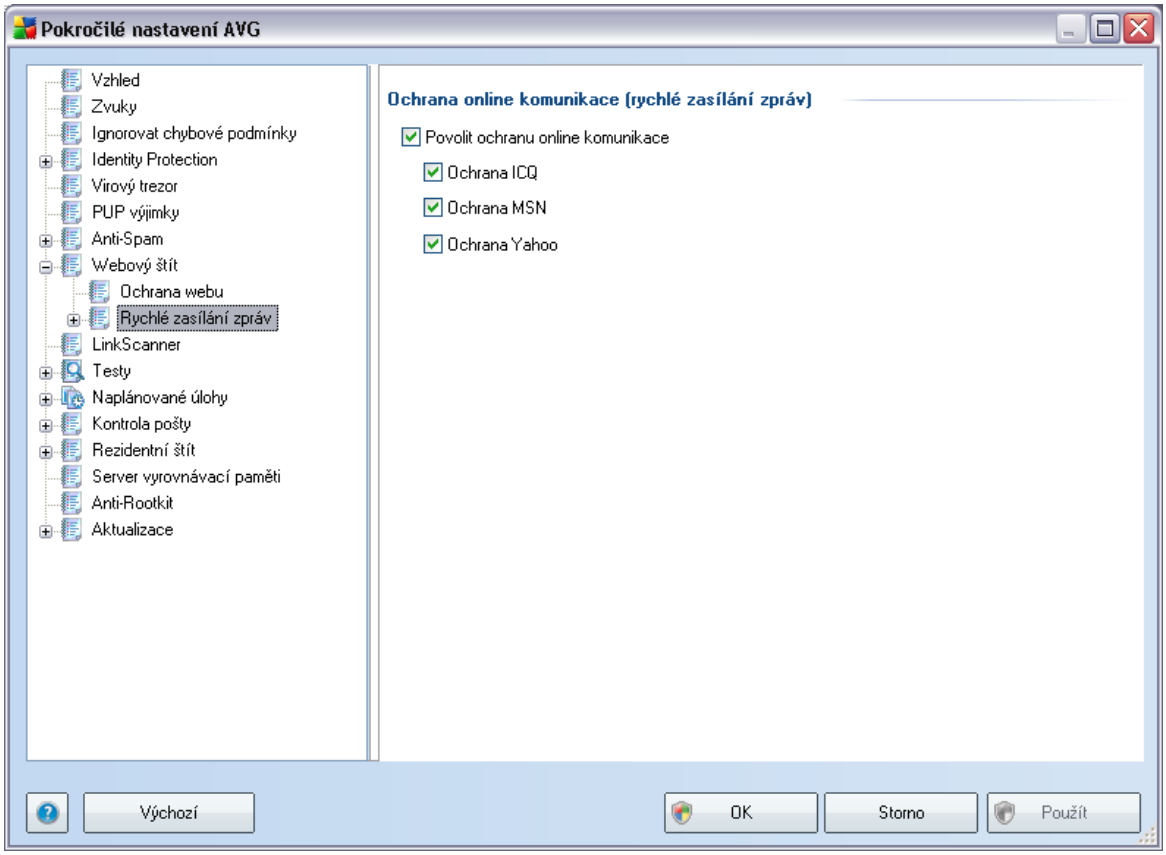
- ***Používat heuristickou analýzu*** - (*ve výchozím nastavení zapnuto*) kontrola obsahu zobrazované www stránky pomocí metody heuristické analýzy (*dynamická emulace instrukcí testovaného objektu v prostředí virtuálního počítače*).

- ***Porty k testování*** - v tomto poli jsou ve výchozím nastavení uvedena čísla portů standardně používaných pro http komunikaci. Pokud se vaše nastavení liší od běžného, můžete čísla portů změnit podle vlastní potřeby.

- ***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 časově náročná a může výrazně zpomalit načítání www stránky. Posuvníkem tedy můžete nastavit maximální velikost souboru, který si přejete 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) či domény, jež mají být z kontroly ***Webovým štítem*** vyňaty. Uvádějte tedy výhradně adresy hostitelů, u nichž si můžete být obsahem www stránek naprosto jisti.

10.6.2. Rychlé zasílání zpráv

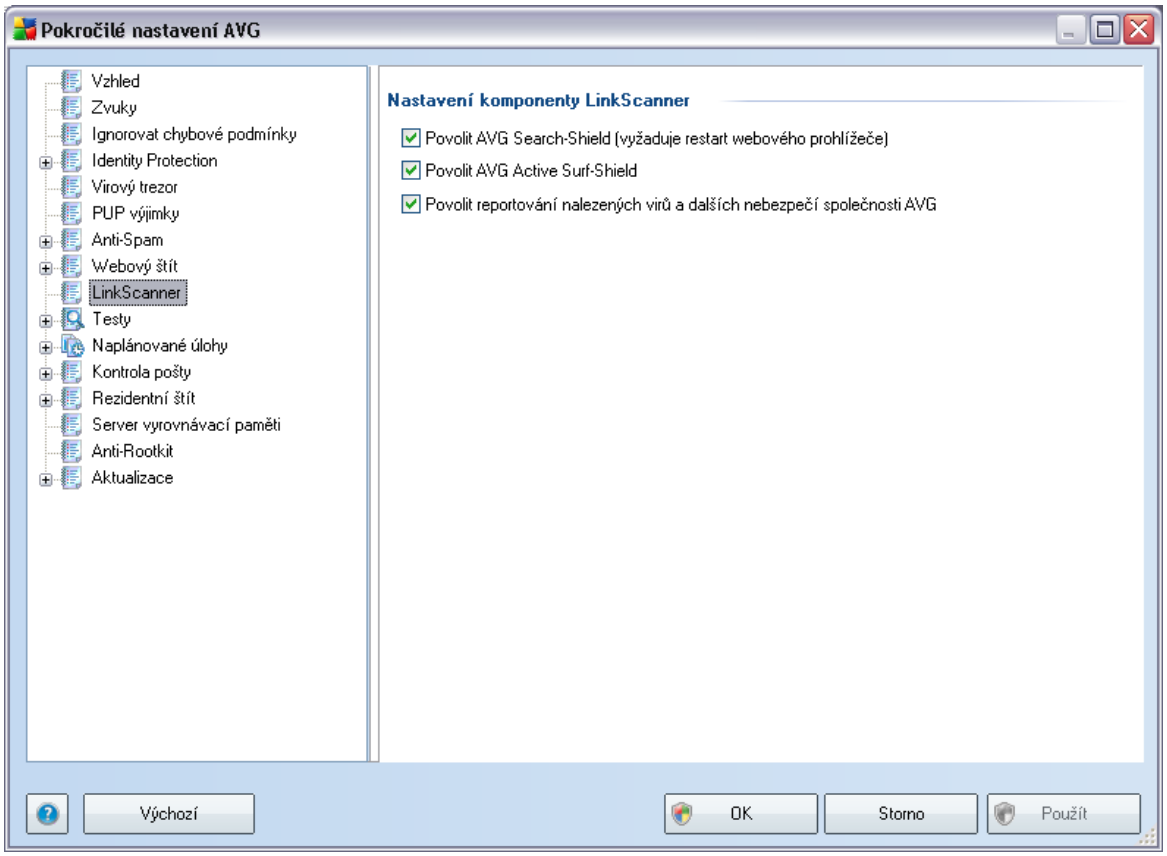


V dialogu ***Ochrana online komunikace (rychlé zasílání zpráv)*** můžete editovat parametry komponenty ***Webový štít*** vztahující se k online kontrole okamžité komunikace. V tuto chvíli jsou podporovány tyto tři programy pro rychlé zasílání zpráv: ***ICQ***, ***MSN*** a ***Yahoo*** - označte příslušnou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

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

10.7. LinkScanner

Dialog ***Nastavení komponenty LinkScanner*** umožňuje zapnout či vypnout funkčnost základních složek ***LinkScanner***:



- ***Povolit AVG Search-Shield*** - (*ve výchozím nastavení zapnuto*): služba je aktivní při vyhledávání na serverech Google, Yahoo!, 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 (*vyžaduje restart webového prohlížeče*).

- ***Povolit AVG Active 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.

- ***Povolit reportování nalezených virů a dalších nebezpečí společnosti AVG*** - (*ve výchozím nastavení zapnuto*): označte tuto položku, pokud se chcete zapojit do projektu zpětného reportování nebezpečných www stránek do databáze.

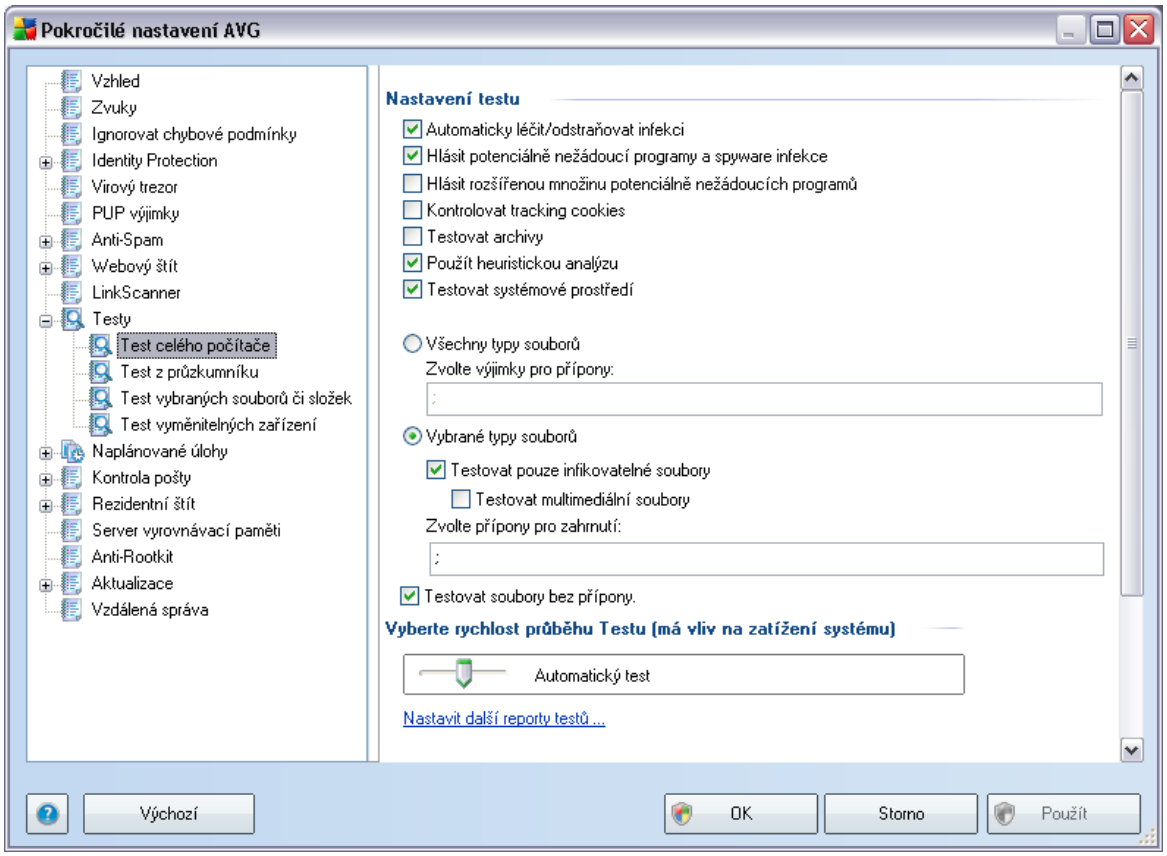
10.8. Testy

Pokročilé nastavení testů je rozděleno do čtyř kategorií, které odpovídají jednotlivým typům výrobcem 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

10.8.1. 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/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 malware, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány vědomě 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 původní 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;

Dále se můžete rozhodnout, zda si přejete testovat

- ***Všechny typy souborů*** - přičemž 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.

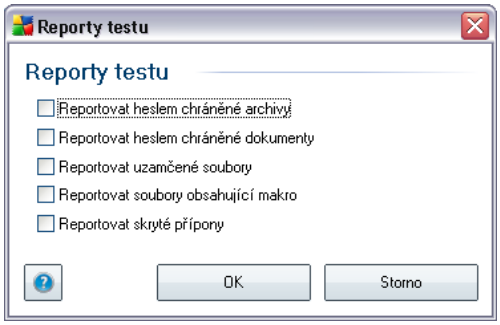
- U položky ***Testovat soubory bez přípon*** pak rozhodněte, zda se mají testovat i soubory se skrytou či neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme , abyste se tohoto nastavení podrželi, pokud nemáte skutečný důvod jej měnit. Soubory bez přípon jsou obecně vysoce podezřelé a měly by být otestovány.

Priorita testu

V sekci ***Priorita testu*** pak můžete nastavit požadovanou rychlost testování v závislosti na zátěži systémových zdrojů. Ve výchozím nastavení je tato hodnota nastavena ***Automatický test***, což odpovídá střední úrovni využití systémových prostředků.. 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 situaci, 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 testů ...

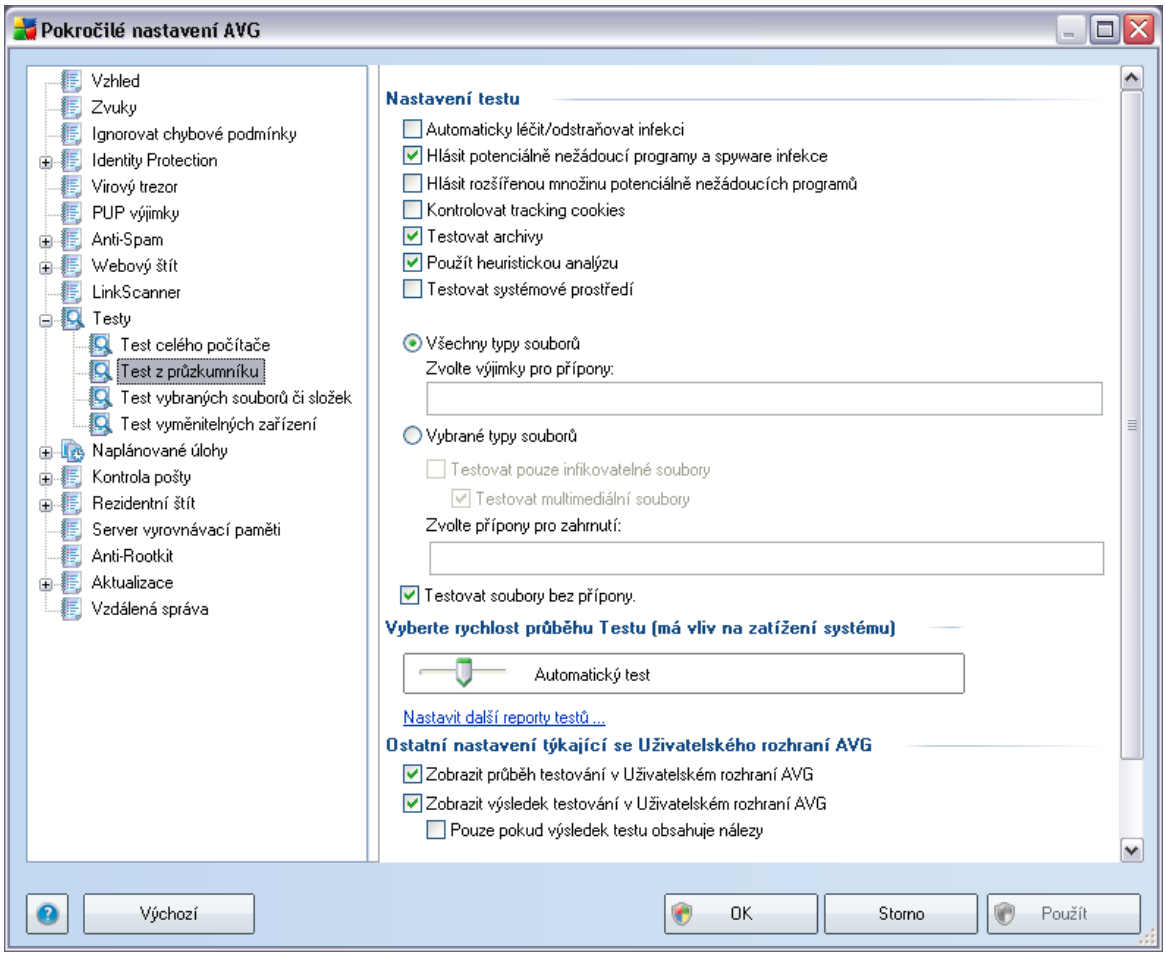
Kliknutím na odkaz ***Nastavit další reporty testů ...*** otevřete samostatné dialogové okno ***Reporty testů***, v němž můžete označením příslušných položek určit situace, jejichž výskyt během testu má být hlášen:



10.8.2. 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 testům spouštěným nad konkrétními objekty přímo z průzkumníku Windows (*Test z průzkumníku*), viz kapitola ***Testování v průzkumníku***

Windows:



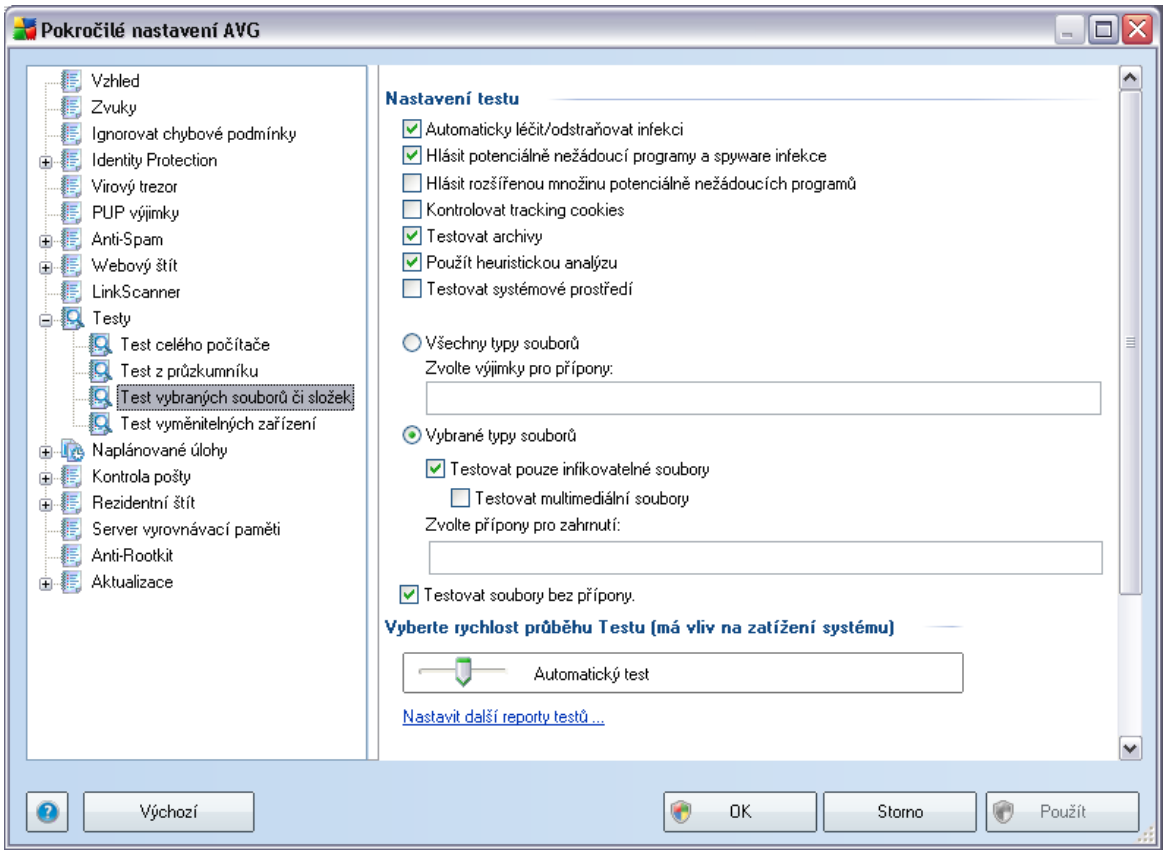
Veškeré možnosti editace parametrů testu jsou totožné s ***editací parametrů Testu celého počítače***. Odlišné je pouze výchozí nastavení těchto parametrů (*například Test celého počítače ve výchozím nastavení neprovádí kontrolu archivů, ale provádí kontrolu systémového prostředí, zatímco u Testu z průzkumníku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

10.8.3. 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:

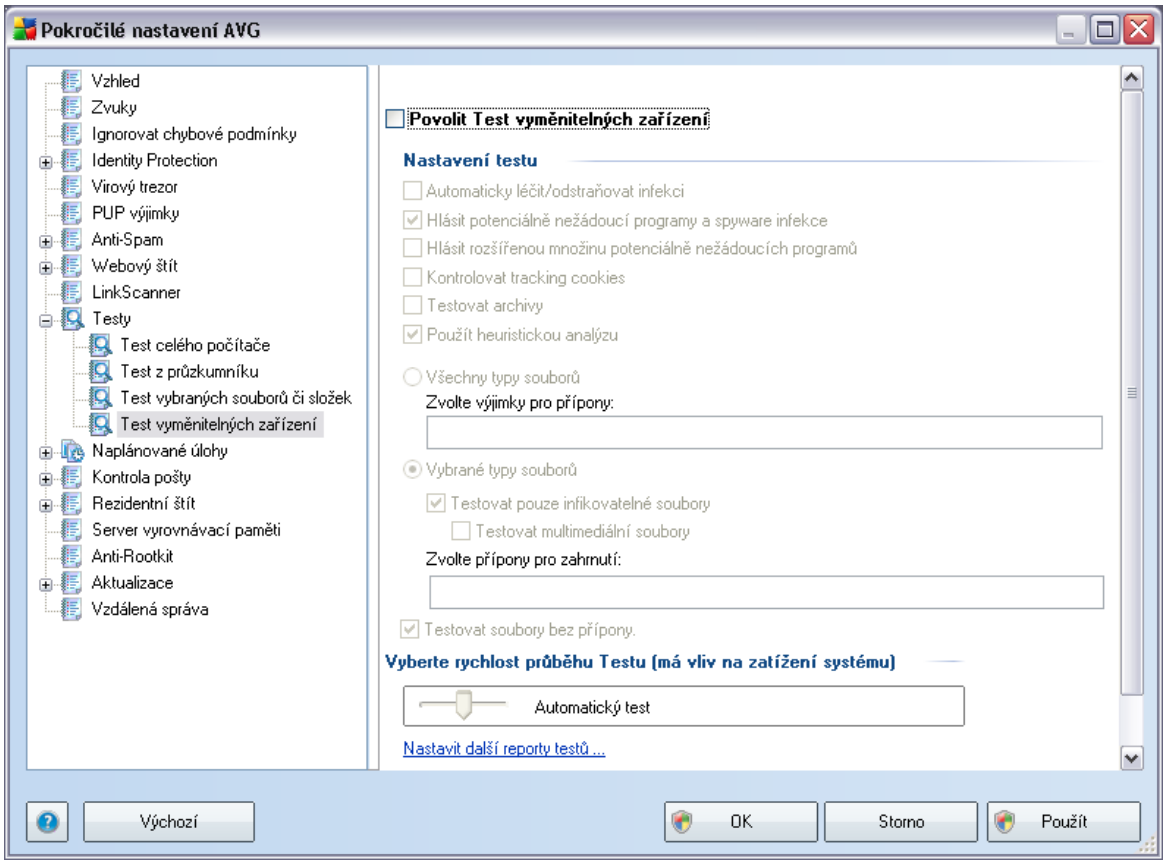


Veškeré parametry nastavené v tomto konfiguračním dialogu se vztahují pouze na ty oblasti vašeho počítače, které jste vybrali pro testování v rámci ***Testu vybraných souborů či složek***!

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

10.8.4. Test vyměnitelných zařízení

Editační rozhraní ***Testu vyměnitelných zařízení*** je také velmi podobné rozhraní ***Testu celého počítače***:



Test vyměnitelných zařízení se spouští automaticky bezprostředně při zapojení vyměnitelného zařízení k vašemu počítači. Ve výchozím nastavení je toto testování vypnuto. Testovat vyměnitelná 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***.

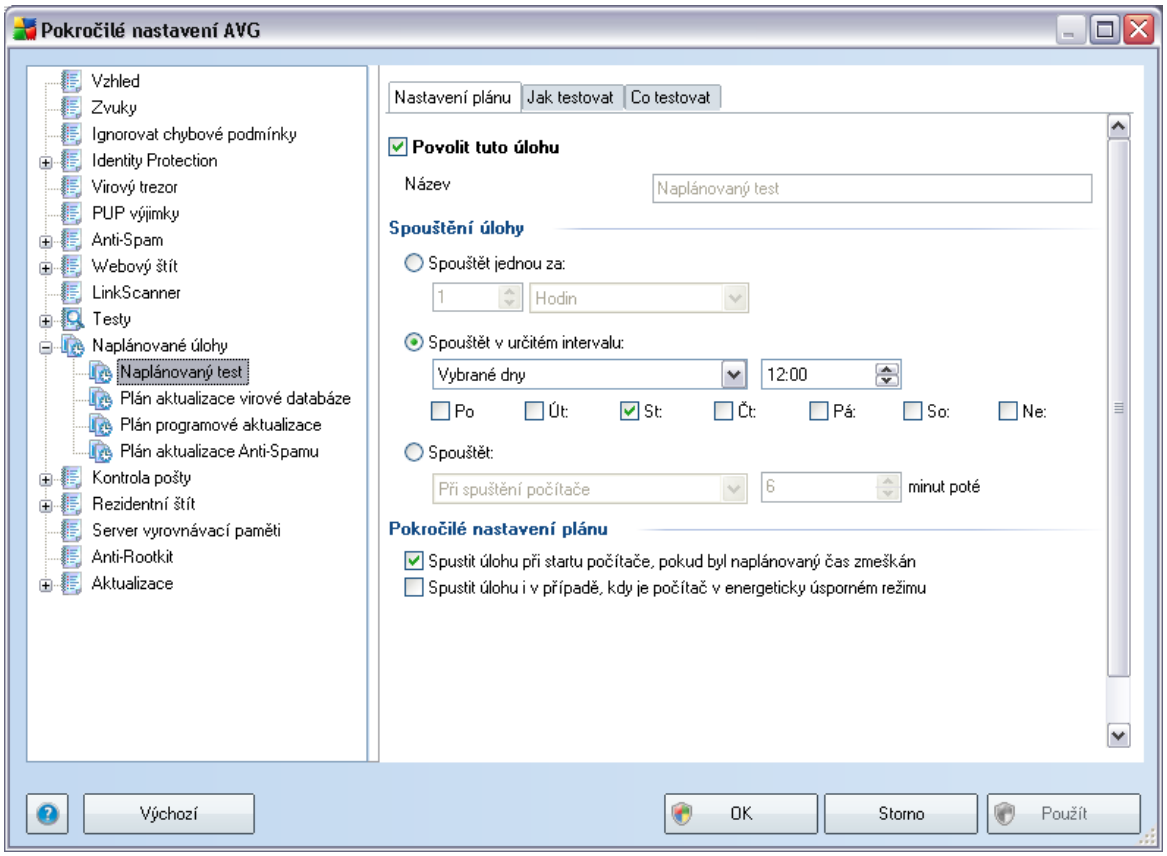
10.9. Naplánované úlohy

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

- Plánu testu celého počítače
- Plánu aktualizace virové databáze
- Plánu programové aktualizace

10.9.1. Naplánovaný test

Parametry naplánovaného testu můžete editovat (*případně nastavit plán nový*) na třech záložkách:



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

V textovém poli ***Název*** (*toto pole je u všech předem nastavených plánů deaktivováno*) je uvedeno jméno přiřazené právě nastavenému 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 případné názvy, abyste se později v naplánovaných úlohách snadněji vyznali.

Příklad: *Nevhodným názvem testu je například "Nový test" nebo "Martinův 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 - vámi nastavený test*

bude vždy specifickým nastavením testu vybraných souborů a složek.

V tomto dialogu můžete dále definovat tyto parametry testu:

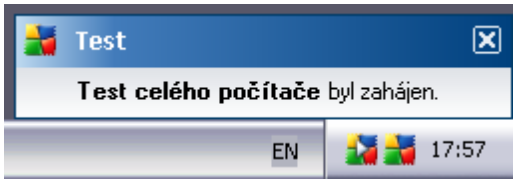
Spouštění úlohy

V této sekci dialogu určete, v jakých časových intervalech má být nově naplánovaný test spouštěn. Časové určení můžete zadat buďto opakovaným spuštěním testu po uplynutí určené doby (***Spouštět jednou za***) nebo stanovením přesného data a času (***Spouštět v určený čas***), případně určením události, na niž se spuštění testu váže (***Spouštět při spuštění počítače***).

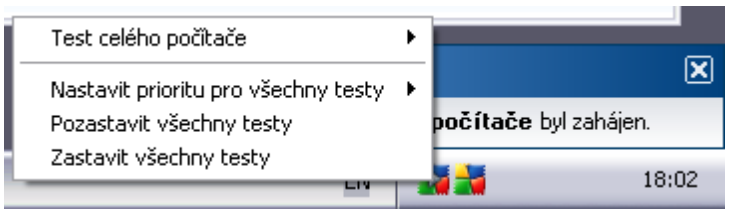
Pokročilé nastavení plánu

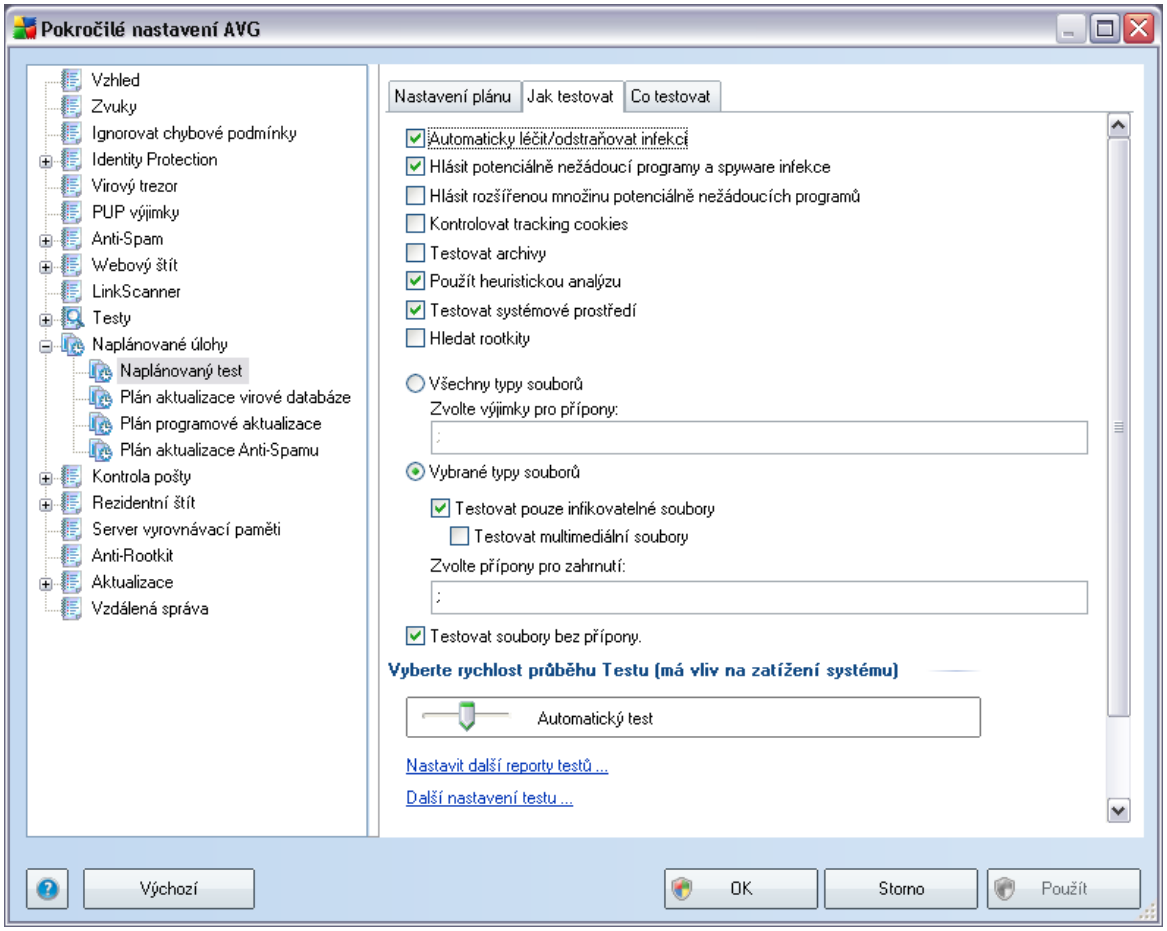
Tato sekce umožňuje definovat podmínky, kdy má či nemá být test spuštěn, jestliže je počítač v úsporném režimu nebo zcela vypnutý a naplánovaný test spuštění testu byl zmeškán.

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 bílou šipkou - viz předchozí obrázek*), 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 měnit, doporučujeme se podržet 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 vypnuto*): 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 malware, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány vědomě 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 původní 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 prověří i systémové oblasti vašeho počítače;

- ***Hledat rootkity*** - (*ve výchozím nastavení vypnuto*): označením této položky zahrnete do testu i možnost detekce rootkitů, která je jinak samostatně dostupná v rámci komponenty ***Anti-Rootkit***;

Dále se můžete rozhodnout, zda si přejete testovat

- ***Všechny typy souborů*** - přičemž máte zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou (*po uložení se čárky změní na středníky*);

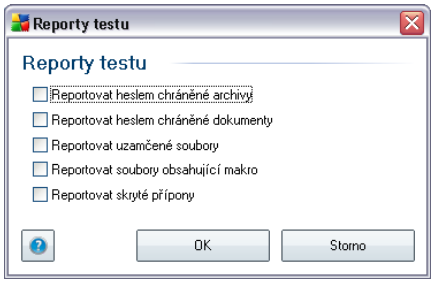
- ***Vybrané typy souborů*** - můžete se rozhodnout, že chcete, aby se testy spouštěly pouze nad soubory, které lze považovat za infikovatelné (*soubory, které nemohou být infekcí zasaženy, se testovat nebudou - například prosté textové soubory nebo některé nespustitelné soubory*), a to včetně multimediálních 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 rozhodněte, zda se mají testovat i soubory se skrytou či neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme , abyste se tohoto nastavení podrželi, pokud nemáte skutečný důvod jej měnit. Soubory bez přípon jsou obecně vysoce podezřelé a měly by být otestovány.

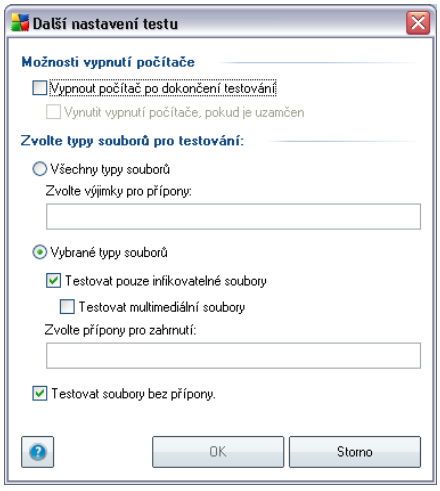
Priorita testu

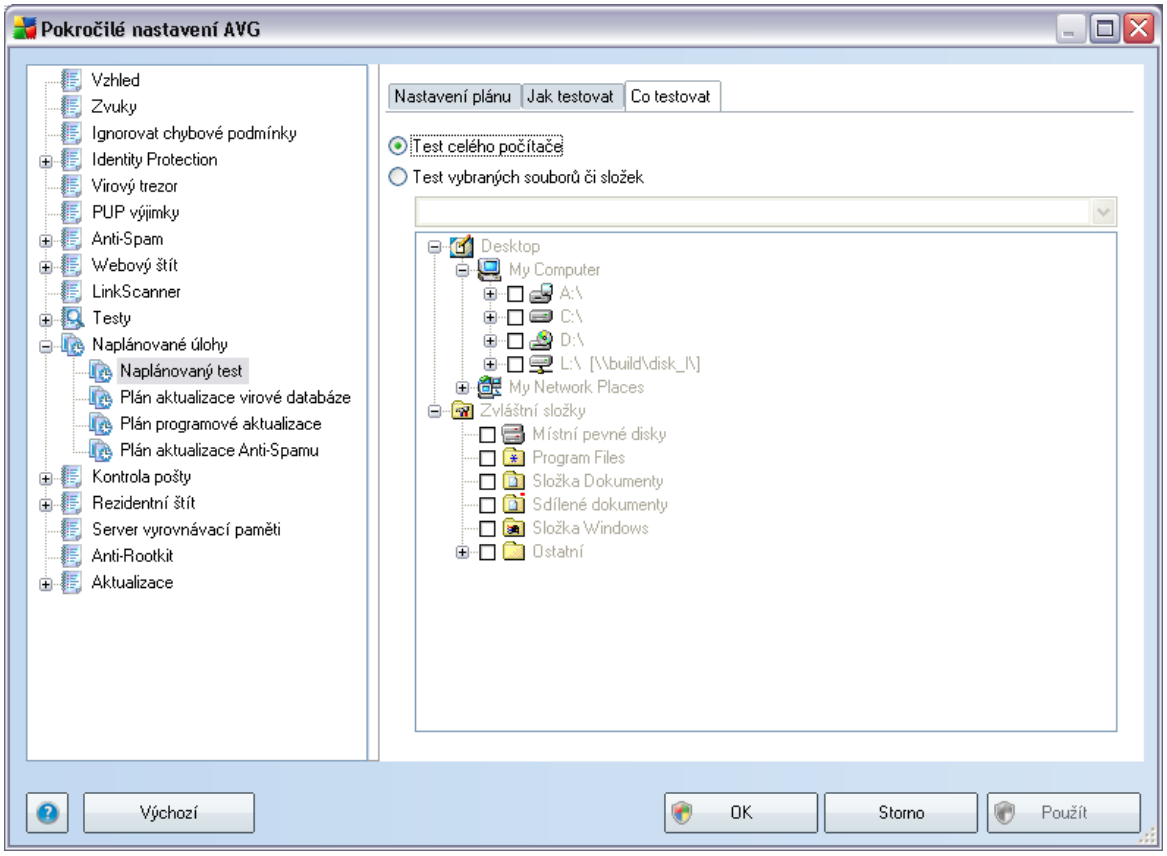
V sekci ***Priorita testu*** pak můžete nastavit požadovanou rychlost testování v závislosti na zátěži systémových zdrojů. Ve výchozím nastavení je tato hodnota nastavena střední úroveň automatického využití systémových prostředků. Pokud se rozhodnete pro spuštění rychlého testu, proběhne test v kratším čase, ale po dobu jeho běhu bude výrazně zvýšena zátěž systémových zdrojů, takže vaše práce na počítači bude obtížnější (*tato varianta je vhodná pro situaci, 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.

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:



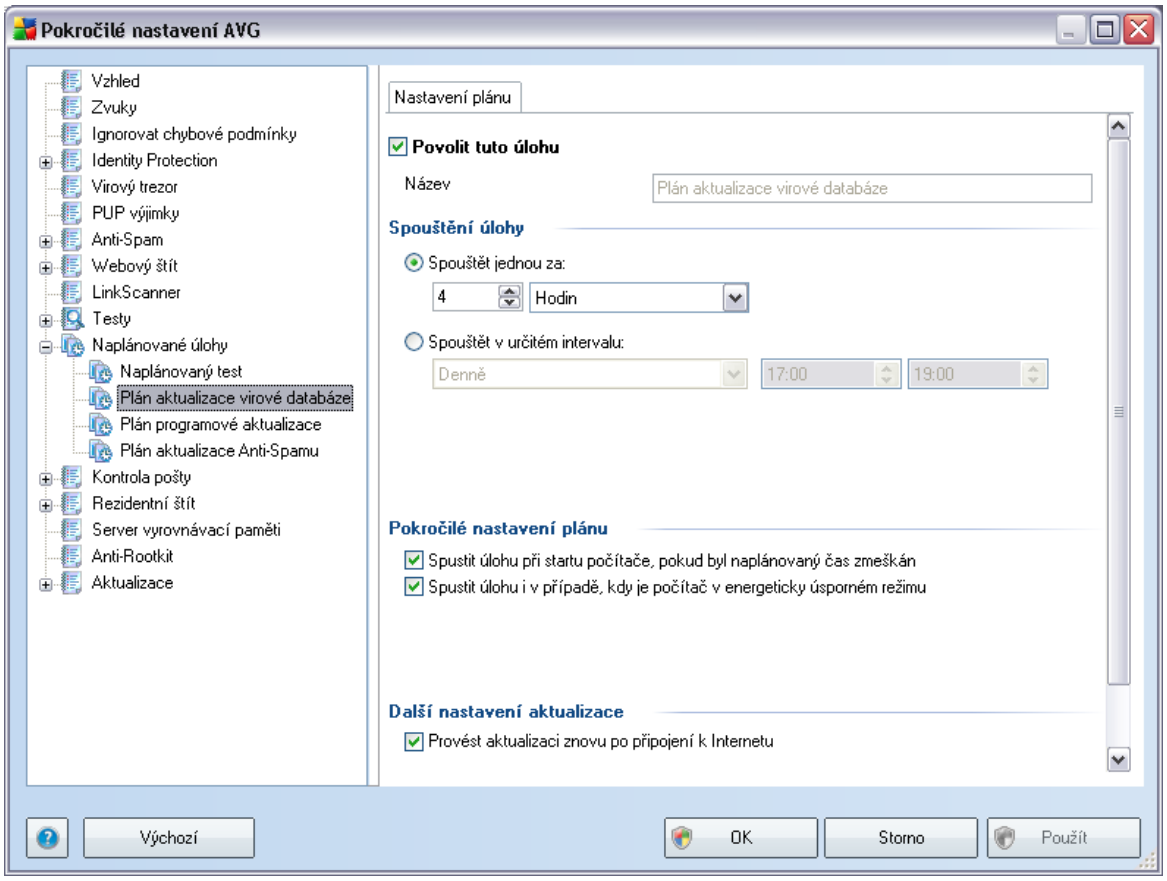
Kliknutím na odkaz ***Další nastavení testu ...*** otevřete nový dialog ***Možnosti vypnutí počítače***, v němž můžete zvolit, zda má být po dokončení spuštěného testu počítač automaticky vypnut. Pokud potvrdíte tuto volbu (***Vypnout počítač po dokončení testování***), aktivuje se současně další možnost, 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*** definujte, 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 sekci dialogu se aktivuje zobrazená stromová struktura vašeho disku a v ní můžete označit adresáře, jejichž obsah má být testován.

10.9.2. Plán aktualizace virové databáze



Na záložce ***Nastavení plánu*** máte nejprve možnost jednoduchým označením položky ***Povolit tuto úlohu*** naplánovanou aktualizaci (dočasně) deaktivovat, a později podle potřeby znovu použít. 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 přiřazené právě nastavenému 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 určené doby (***Spouštět jednou za***) nebo stanovením přesného data a času (***Spouštět v určený čas***).

Pokročilé nastavení plánu

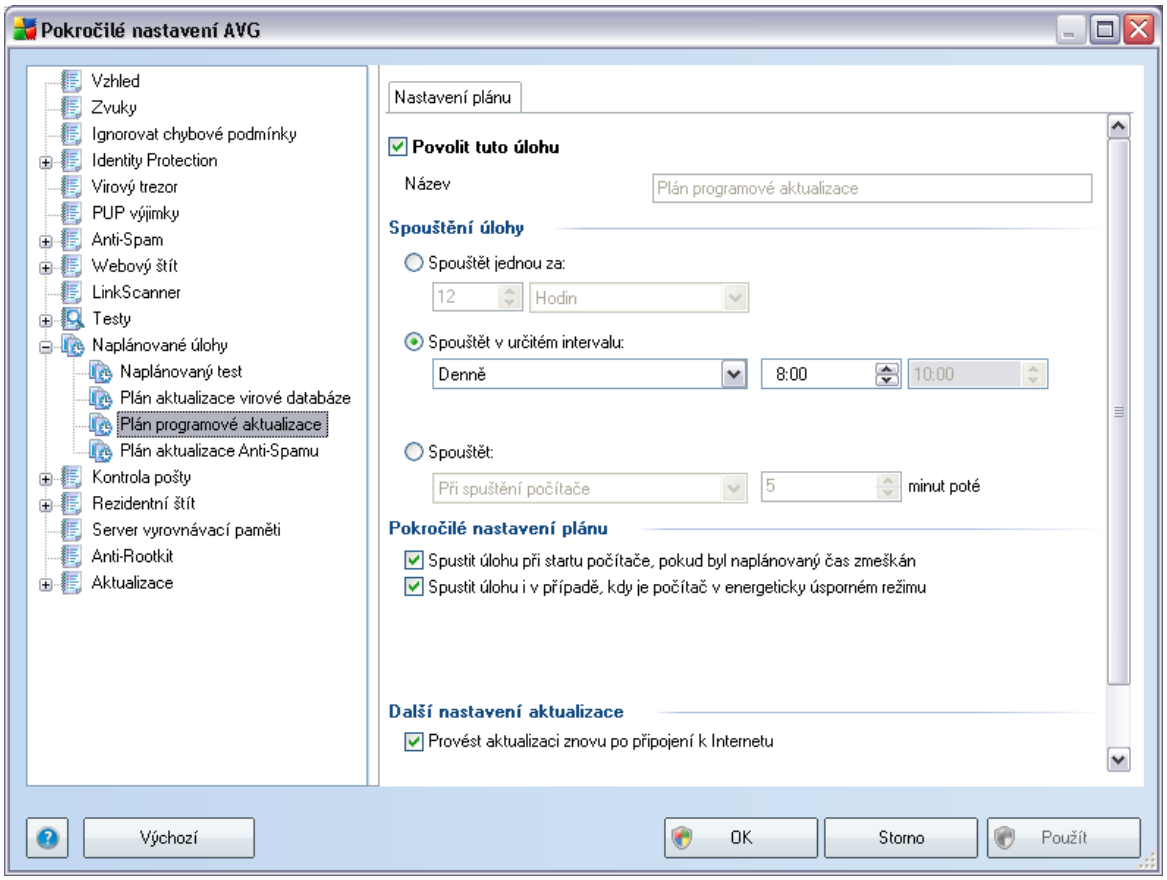
Tato sekce umožňuje definovat podmínky, kdy má či nemá být aktualizace virové databáze spuštěna, jestliže je počítač v úsporném režimu nebo zcela vypnutý a naplánovaný čas spuštění aktualizace byl zmeškán.

Další nastavení aktualizace

Volbou položky ***Provést aktualizaci znovu po připojení k Internetu*** zajistíte, že pokud dojde během aktualizace virové databáze 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***).

10.9.3. Plán programové aktualizace



Na záložce ***Nastavení plánu*** máte nejprve možnost jednoduchým označením položky ***Povolit tuto úlohu*** naplánovanou programovou aktualizaci (*dočasně*) deaktivovat, a

později podle potřeby znovu použít. V textovém poli ***Název*** (*toto pole je u všech předem nastavených plánů deaktivováno*) je uvedeno jméno přiřazené právě nastavenému plánu programové aktualizace.

Spouštění úlohy

Určete, v jakých časových intervalech má být nově naplánovaná programové aktualizace provedena. Časové určení můžete zadat buďto opakovaným spuštěním aktualizace po uplynutí určené 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.

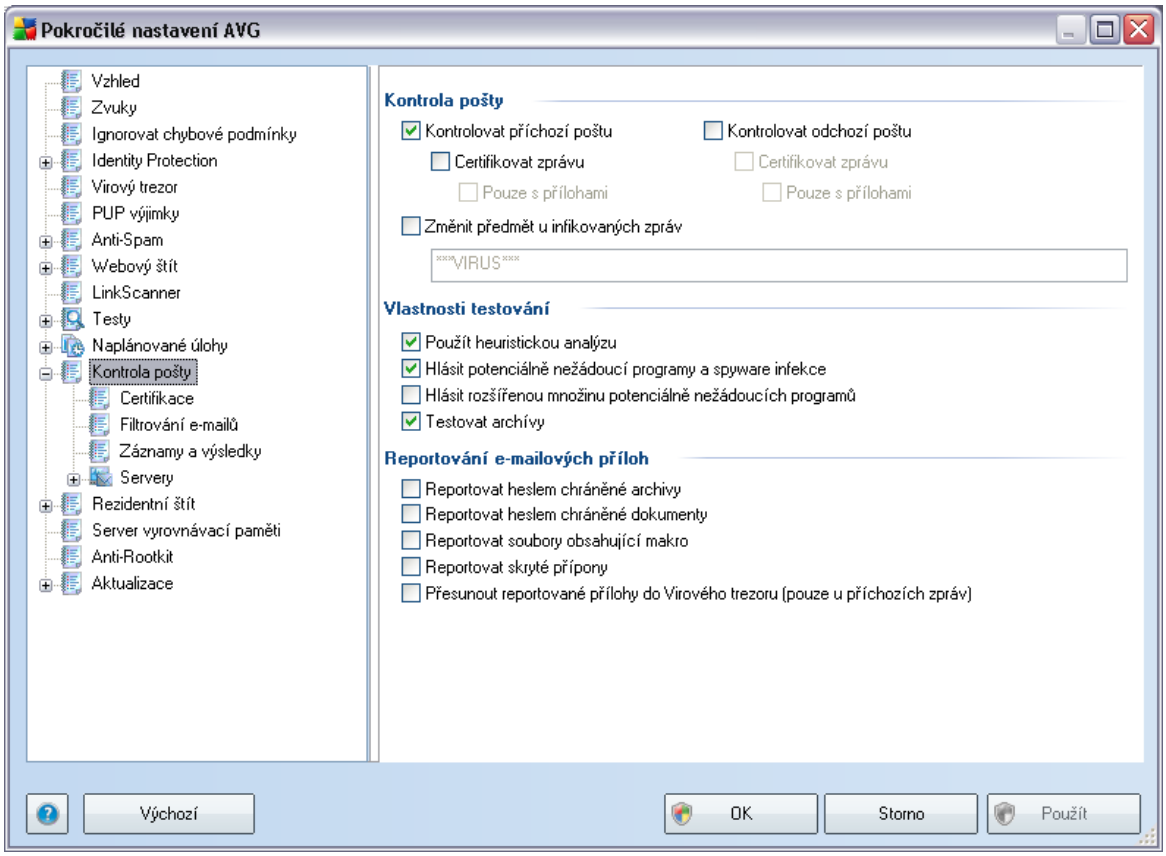
Další nastavení aktualizace

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 souběhu naplánované programové aktualizace a naplánovaného testu, proces aktualizace je považován za prioritní a test bude přerušen.*

10.10. Kontrola pošty



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

- ***Kontrola pošty*** - v této sekci jsou dostupná základní nastavení, pro příchozí a odchozí poštu zvlášť:
    - Zda má být pošta kontrolována nebo ne.
    - Zda má být na konec neinfikovaných e-mailů přidán certifikační text. Tento text lze upravit v dialogu ***Certifikace***.
    - Zda se má tento certifikační text přidávat pouze na konec zpráv s přílohou.

Chcete-li ***Změnit předmět u infikovaných zpráv***, zatrhněte políčko a do textového pole pod ním vepište požadované označení. Tento text pak bude přidán do pole "Předmět" u každé otestované a infikované 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*** – použít heuristiku při testování e-mailů. Když je tato možnost aktivována, můžete filtrovat přílohy e-mailů nejen podle přípony, ale i podle skutečného obsahu a formátu (*který příponě 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 poněkud problematickou kategorii malware, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány vědomě a se souhlasem uživatele. Doporučujeme nicméně ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.

- ***Hlásit rozšířenou množinu potenciálně nežádoucích programů*** - zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v původní 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 archivy*** – testovat obsah archivů v přílohách zpráv.

- ***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 archívy 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.

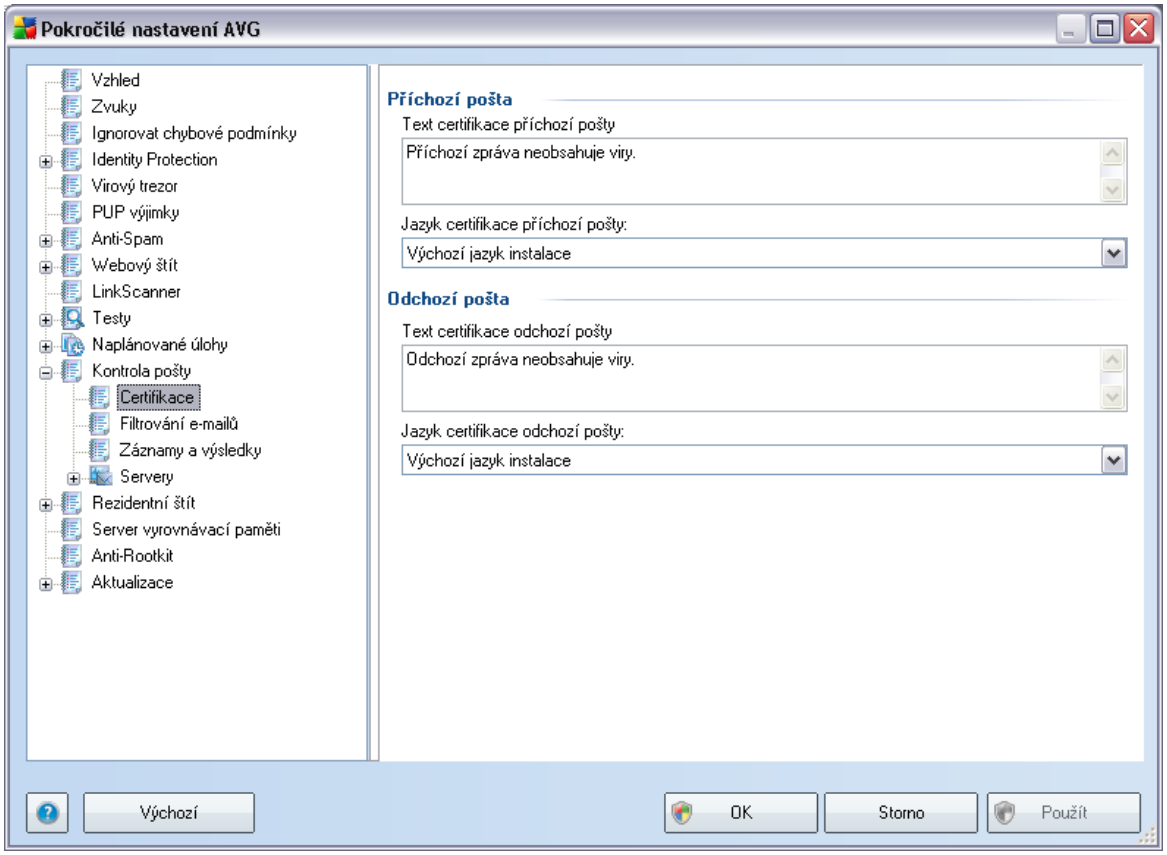
  - ***Reportovat soubory obsahující makro*** – makro je napevno určený sled kroků, který usnadňuje uživateli často opakované složitější úkoly (*makra ve Wordu jsou typickým příkladem*). Makro může obsahovat různé instrukce, a to i potenciálně nebezpečné; chcete-li reportovat všechny dokumenty s makry, označte toto políčko.

  - ***Reportovat skryté přípony*** – skryté přípony mohou podezřelý spustitelný soubor "něco.txt.exe" zamaskovat tak, aby se uživateli jevil jen jako neškodný textový soubor "něco.txt"; po zakšrtnutí tohot políčka budou soubory se skrytými příponami reportovány jako potenciálně

nebezpečné.

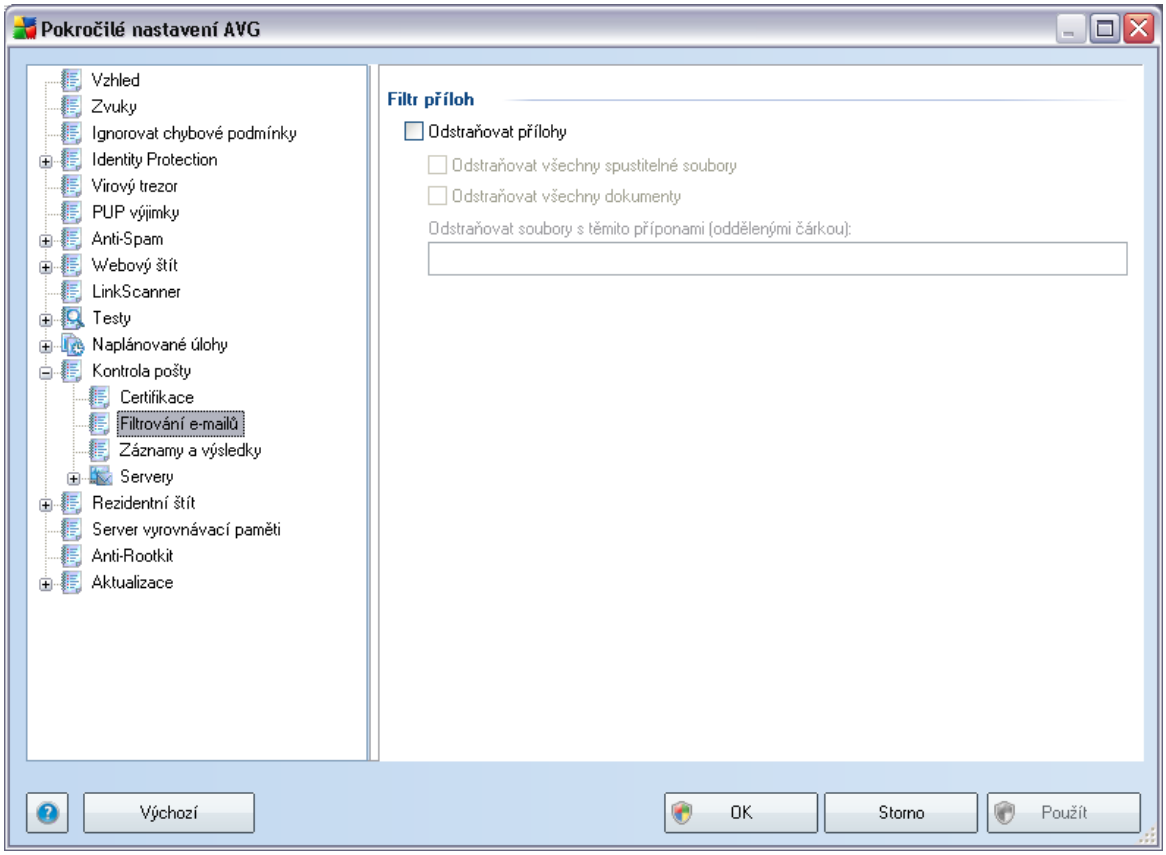
- Zaškrtnutím políčka ***Přesunout reportované přílohy do Virového trezoru*** určíte, že všechny výše vybrané soubory z příloh e-mailů se mají nejen reportovat, ale rovněž automaticky přesouvat do ***Virového trezoru***.

10.10.1. Certifikace



V dialogu ***Certifikace*** můžete nastavit text certifikace a jazyk, v němž má být certifikace zobrazena. Toto nastavení se může lišit pro ***Příchozí poštu*** a ***Odchozí poštu***.

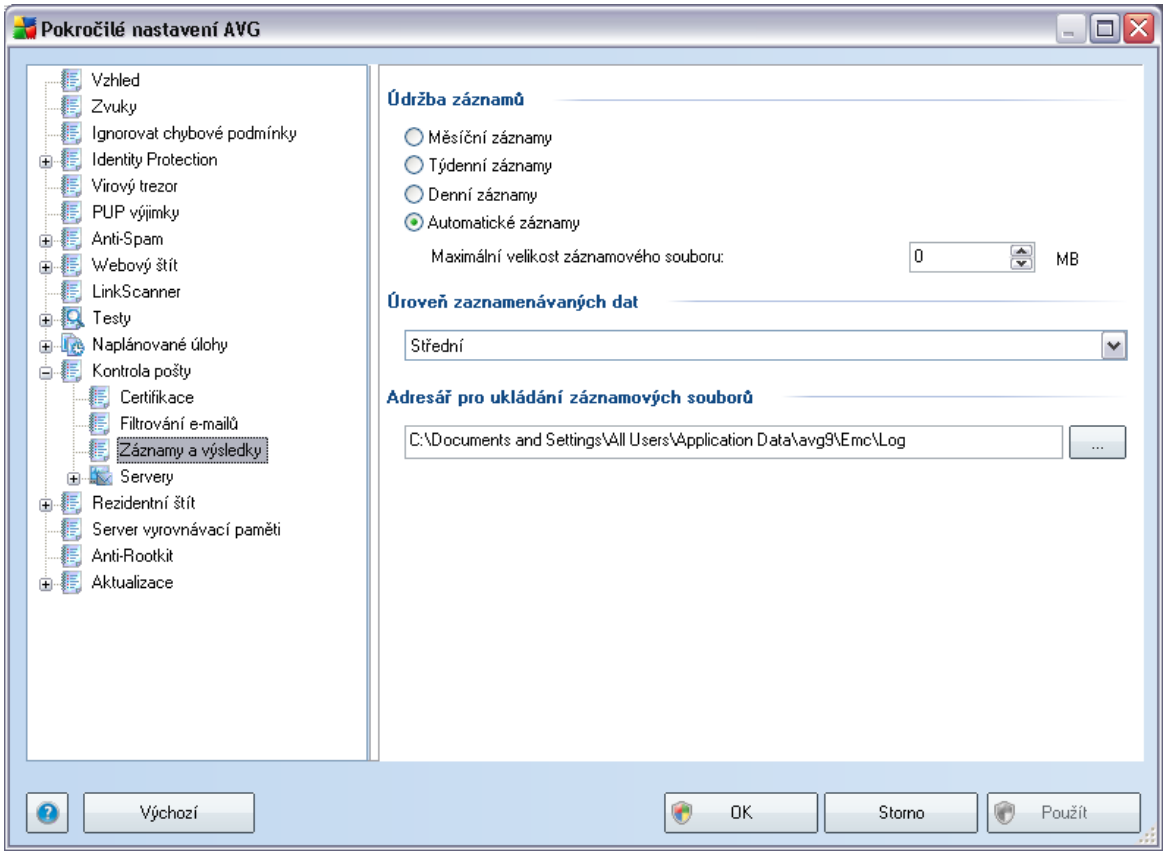
10.10.2. Filtrování e-mailů



Dialog ***Filtrování 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

10.10.3. Záznamy a výsledky

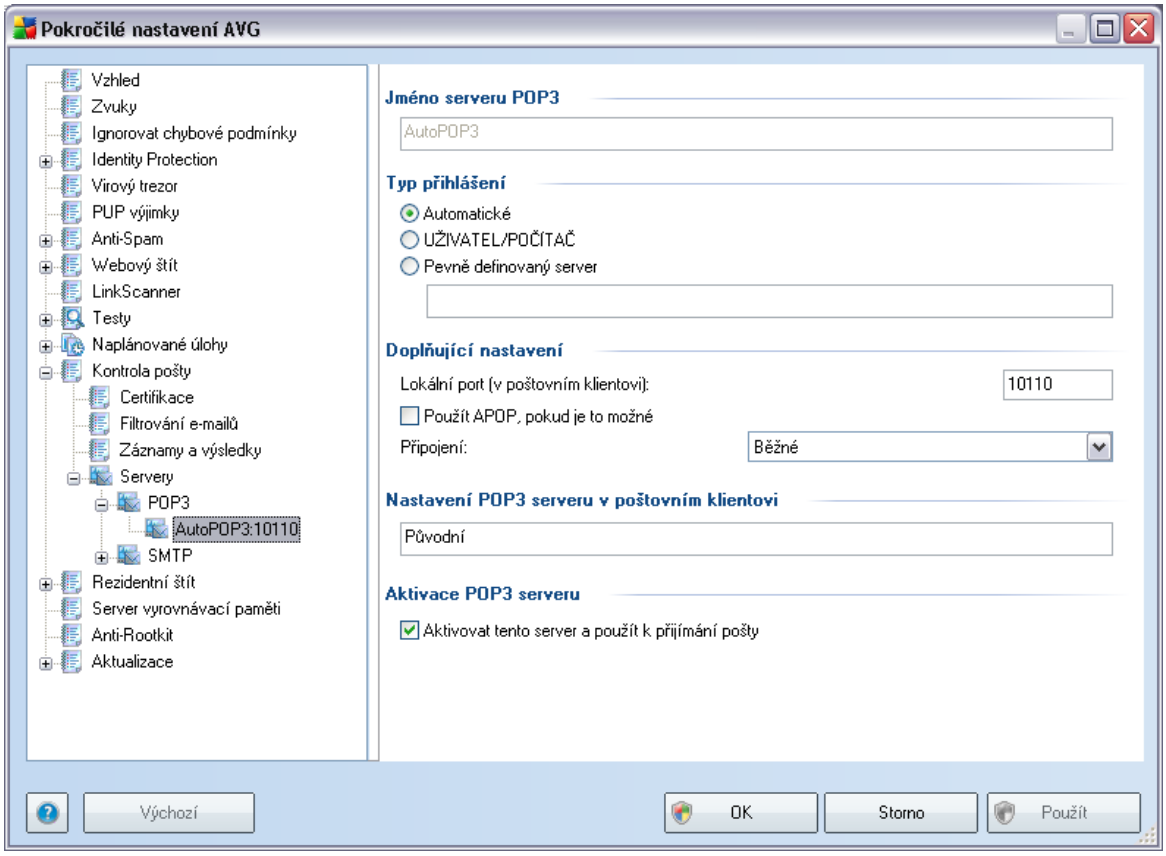


Dialog odkazovaný položkou ***Záznamy a výsledky*** umožňuje nastavení parametrů správy výsledků kontroly pošty a je rozdělen do několika sekcí:

- ***Údržba záznamů*** - zvolte frekvenci, s jakou mají být protokolovány záznamy o průběhu a výsledcích kontroly pošty (*denně, týdně, měsíčně*); a také maximální velikost protokolu (*v MB*)
- ***Úroveň zaznamenávaných dat*** - oproti výchozí nastavené střední úrovni můžete zvolit úroveň nižší (*základní informace o připojení*) nebo vyšší (*protokolování veškerého provozu, při nastavení této úrovně protokolování jsou zaznamenávány celé e-mailové zprávy včetně jejich obsahu*)
- ***Adresář pro ukládání záznamových souborů*** - určete, kam má být uložen protokolovací soubor

10.10.4. Servery

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

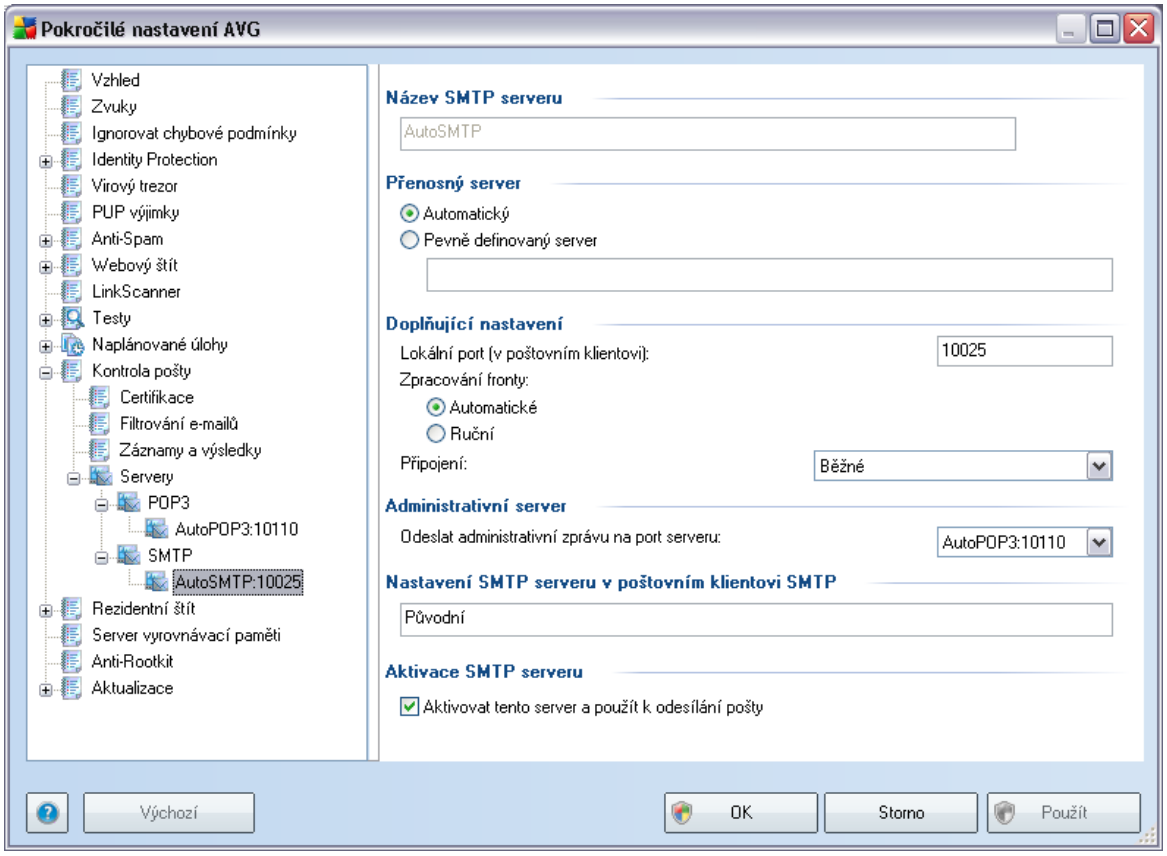


V tomto dialogu (odkaz ***Servery / POP3***) nastavujete server ***Kontroly pošty*** s protokolem POP3 pro příchozí poštu:

- ***Jméno serveru*** - v tomto poli můžete zadat jméno nově přidaných serverů (*server POP3 přidáte tak, že kliknete pravým tlačítkem myši nad položkou POP3 v levém navigačním menu*). U automaticky vytvořeného serveru "AutoPOP3" je toto pole deaktivováno.
- ***Typ přihlášení*** - definuje, jak má být určen poštovní server, ze kterého bude přijímána pošta
    - ***Automatické*** - cílový server bude určen podle nastavení ve vaší poštovní aplikaci; není třeba nic dále specifikovat
    - ***UŽIVATEL/POČÍTAČ*** - nejjednodušší a nejobecnější způsob určení cílového poštovního serveru tzv. proxy způsobem. Jméno nebo adresa (popř. i port) je zadán jako součást přihlašovacího jména uživatele pro daný poštovní server a je od něj oddělen znakem /. Například pro účet user1 na serveru pop.acme.com a port 8200 použijete přihlašovací jméno user1/pop.acme.com:8200.
    - ***Pevně definovaný server*** - v tomto případě bude vždy použit konkrétní

server. Je třeba zadat adresu nebo jméno vašeho poštovního serveru. Přihlašovací jméno pak zůstane beze změny. Jako jméno je možné použít jak doménový název (např. pop.acme.com), tak IP adresu (např. 123.45.67.89). Pokud poštovní server používá nestandardní port, lze tento port zadat za jméno serveru oddělený dvojtečkou (např. pop.acme.com:8200). Standardní port pro POP3 komunikaci je 110.

- ***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 POP3 komunikaci.
  - ***Použít APOP, pokud je to možné*** - tato volba zajišťuje bezpečnější způsob přihlašování k poštovnímu serveru. Je-li použita, bude komponenta ***Kontrola pošty*** při přihlašování používat alternativní způsob předání hesla k uživatelskému účtu, který spočívá v tom, že heslo není otevřenou formou odesláno serveru, ale je jím zašifrován proměnlivý řetězec, obdržený ze serveru. Tato funkce je samozřejmě aktivována pouze v případě, že ji cílový poštovní server podporuje.
  - ***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.
- ***Nastavení POP3 serveru v poštovním klientovi*** - uvádí informaci o tom, jak nastavit klientskou poštovní aplikaci tak, aby přijímané poštovní zprávy byly kontrolovány prostřednictvím právě upravovaného serveru ***Kontroly pošty***. Jde o pohledovou kontrolu, údaje odpovídají parametrům nastaveným v tomto dialogu a dialozích souvisejících.
- ***Aktivace POP3 serveru*** - zapnutím/vypnutím položky máte možnost aktivovat či deaktivovat právě nastavený POP3 server



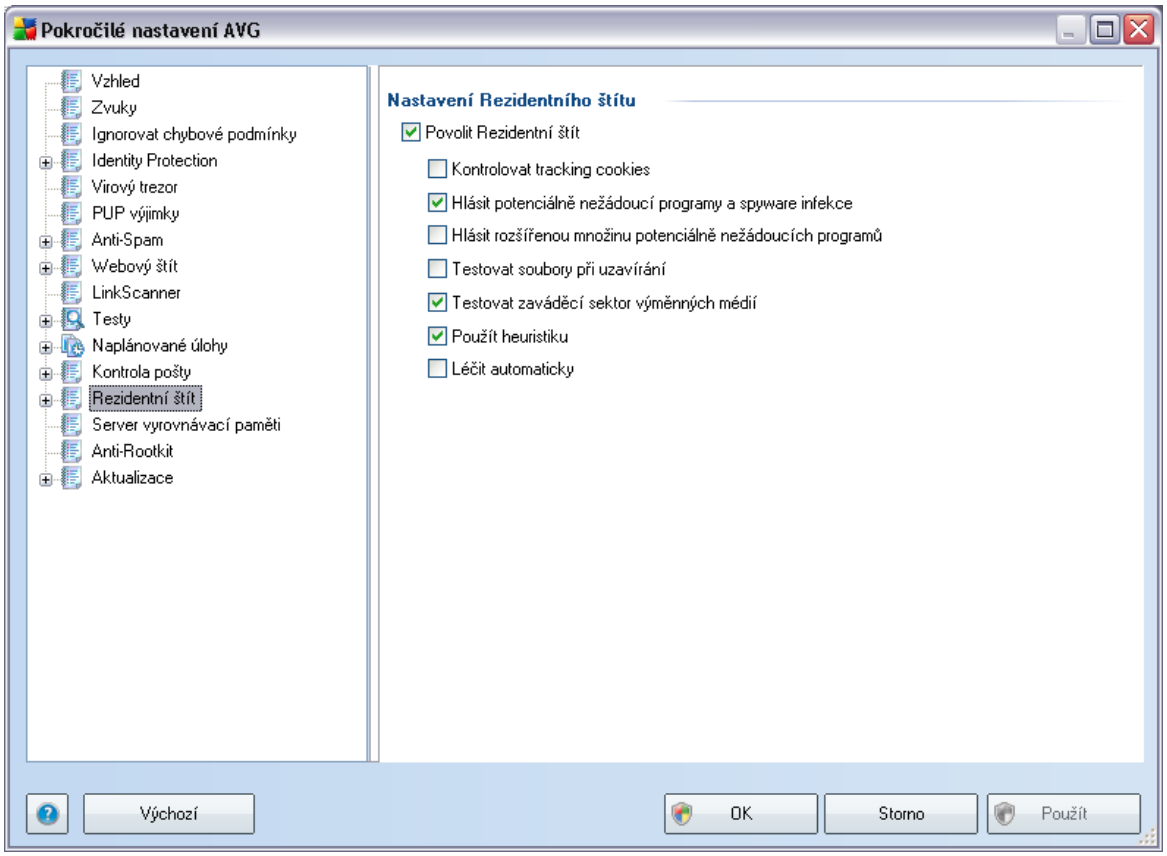
V tomto dialogu (odkaz ***Servery / SMTP***) nastavujete server ***Kontroly pošty*** s protokolem SMTP pro odchozí poštu:

- ***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.
- ***Přenosný server*** - definuje, jak má být určen poštovní server, ze kterého bude odesílána pošta:
  - ***Automatický*** - 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. smtp.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. 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.
    - ***Zpracování fronty*** - určuje, jak má komponenta ***Kontroly pošty*** postupovat při vyřizování požadavků na odeslání poštovní zprávy:
        - Automatické - odesílaná zpráva je ihned doručena (odeslána) na cílový poštovní server
        - Ruční - zpráva je zařazena do fronty odesílaných zpráv a odeslána později hromadně
    - ***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.
- ***Administrativní server*** - uvádí číslo portu serveru, který bude použit pro zpětné doručování administrativních hlášení. Tato hlášení jsou generována například v okamžiku, kdy je odesílaná zpráva cílovým poštovním serverem odmítnuta nebo tento poštovní server není dostupný.
- ***Nastavení SMTP serveru v poštovním klientovi SMTP*** - uvádí informaci o tom, jak nastavit klientskou poštovní aplikaci tak, aby odesílané zprávy byly kontrolovány prostřednictvím právě upravovaného serveru pro kontrolu odesílané pošty. Jde o pohledovou kontrolu, údaje odpovídají parametrům nastaveným v tomto dialogu a dialozích souvisejících.
- ***Aktivace SMTP serveru*** - zapnutím/vypnutím položky máte možnost aktivovat či deaktivovat právě nastavený SMTP server

10.11. 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 či deaktivovat ochranu ***Rezidentního štítu*** označením či vypnutím položky ***Povolit Rezidentní štít*** (*tato položka je ve výchozím nastavení zapnuta*). Dále můžete prostým výběrem rozhodnout, které funkce ***Rezidentního štítu*** mají být aktivovány:

- ***Kontrolovat tracking cookies*** - 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 malware, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány vědomě a se souhlasem uživatele. Doporučujeme nicméně ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.

- ***Hlásit rozšířenou množinu potenciálně nežádoucích programů*** - zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v původní 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*** - 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

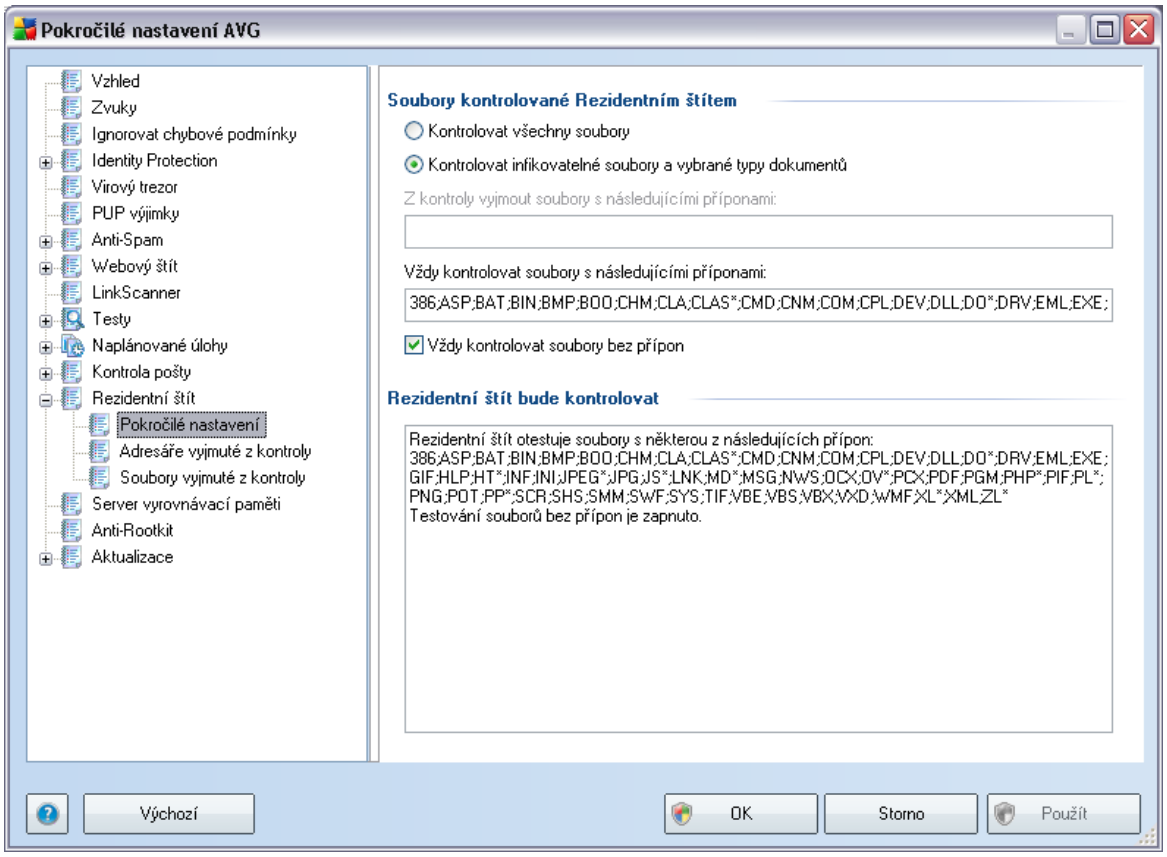
- ***Testovat zaváděcí sektor výměnných médií*** - (*ve výchozím nastavení zapnuto*)

- ***Použít heuristiku*** - (*ve výchozím nastavení zapnuto*) k detekci infekce bude použita i metoda heuristické analýzy (*dynamické emulace instrukcí testovaného objektu v prostředí virtuálního počítače*)

- ***Léčit automaticky*** - detekovaná infekce bude automaticky vyléčena, jestliže je k dispozici léčba toho konkrétního viru; a všechny infekce, jež nelze vyléčit, budou odstraněny.

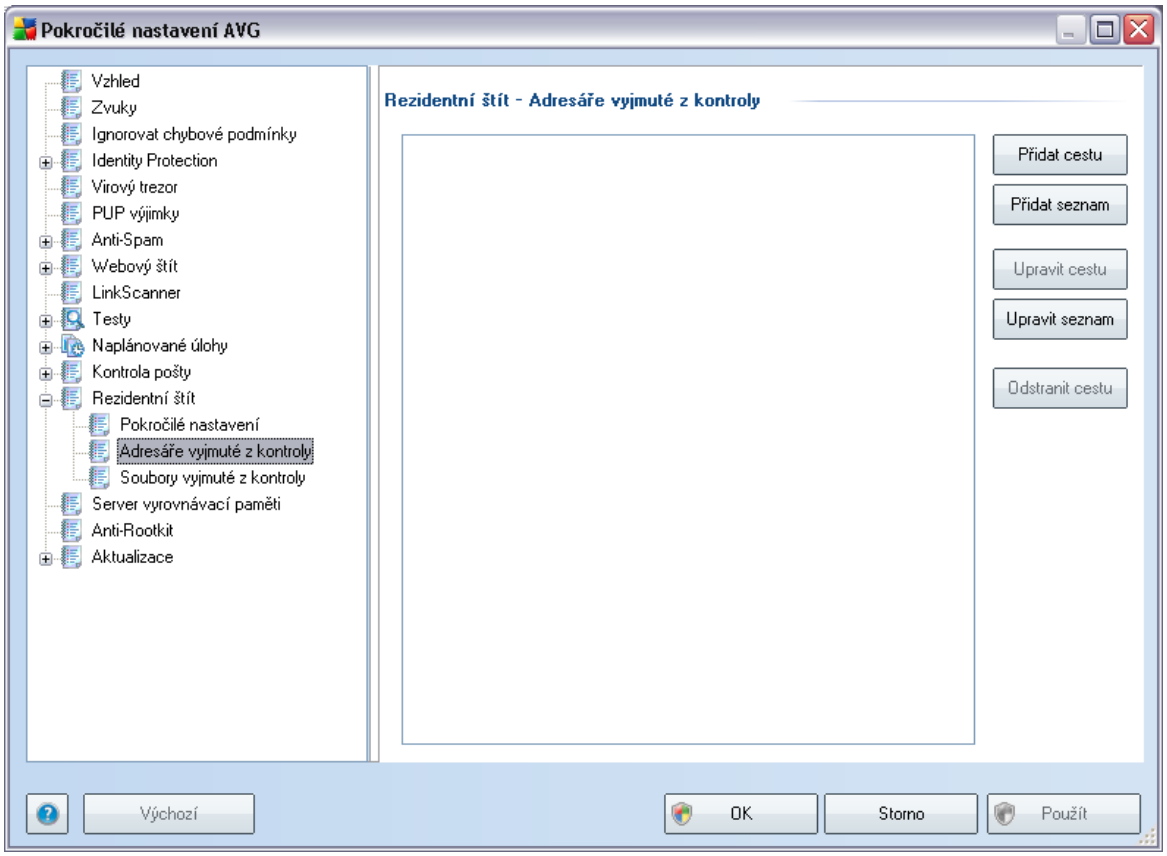
10.11.1. Pokročilé nastavení

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



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

10.11.2. Adresáře vyjmuté z kontroly



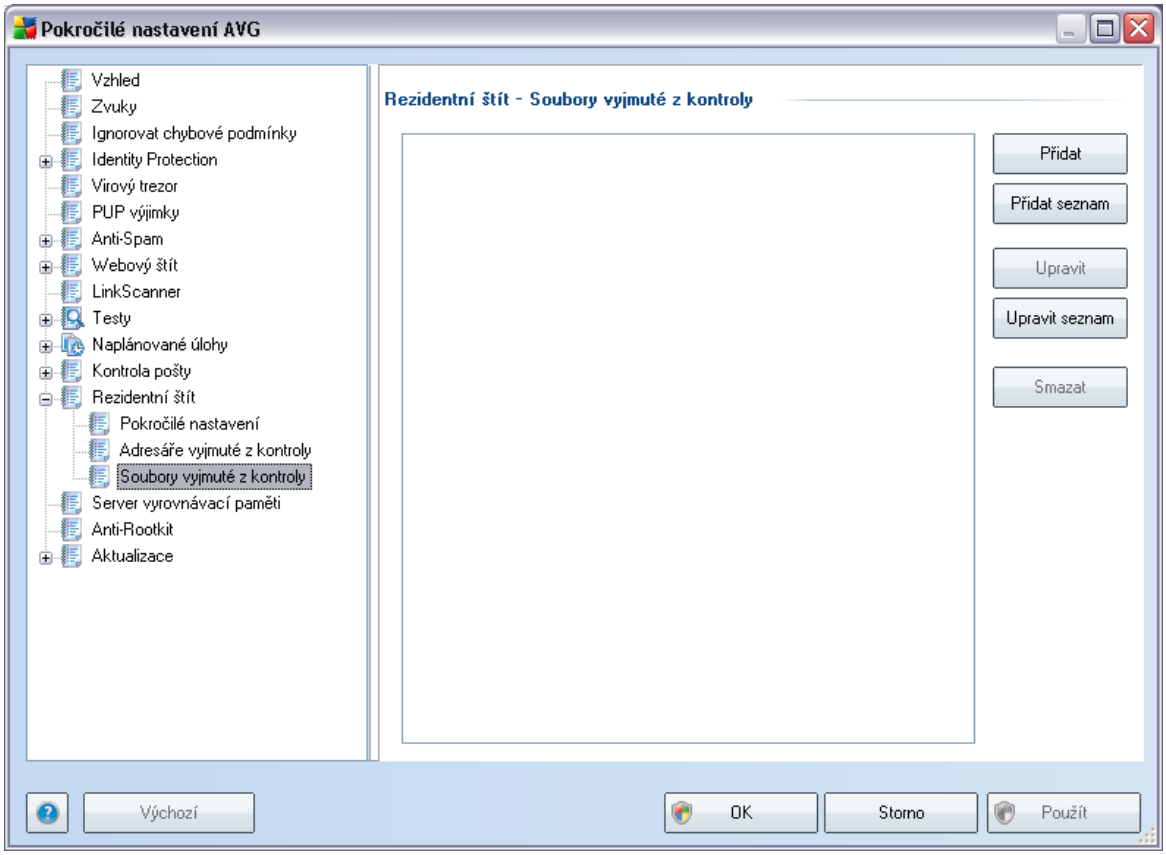
Dialog ***Rezidentní štít - adresáře vyňaté z kontroly*** nabízí možnost definovat adresáře, které mají být z testování ***Rezidentním štítem*** vypuštěny.

Pokud to není naprosto nutné, doporučujeme žádné adresáře nevyjímat!

Dialog obsahuje následující ovládací tlačítka:

- ***Přidat cestu*** – umožňuje výběrem z navigačního stromu lokálního disku vybrat další adresáře definované jako výjimky
- ***Přidat seznam*** – umožňuje přímo zadat seznam adresářů, které mají být z testování ***Rezidentního štítu*** vyňaty
- ***Upravit cestu*** – umožňuje editovat zadání cesty ke zvolenému adresáři
- ***Upravit seznam*** – umožňuje editovat zadání seznamu adresářů
- ***Odstranit cestu*** – umožňuje odstranit cestu ke zvolenému adresáři

10.11.3. Soubory vyjmuté z kontroly



Dialog ***Rezidentní štít - soubory vyňaté z kontroly*** nabízí možnost definovat samostatné soubory, které mají být z testování ***Rezidentním štítem*** vypuštěny.

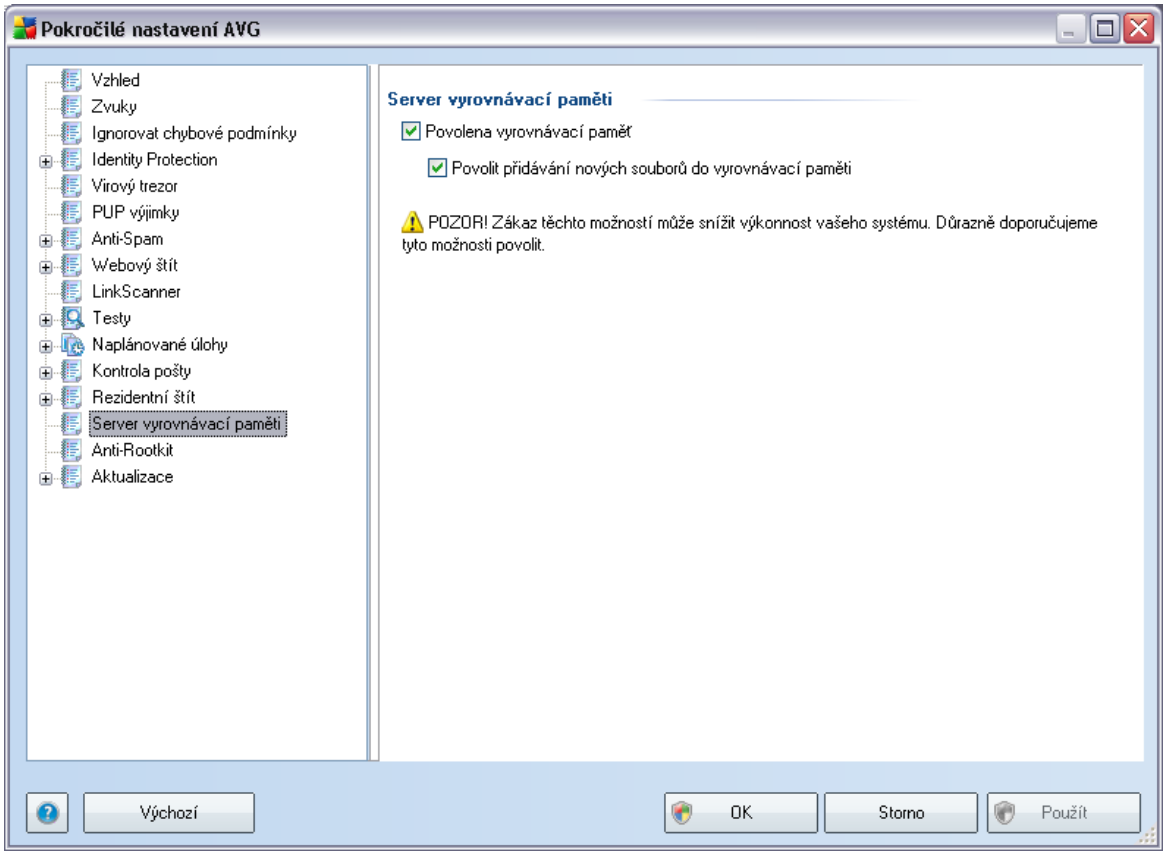
Pokud to není naprosto nutné, doporučujeme žádné soubory nevyjímat!

Dialog obsahuje následující ovládací tlačítka:

- ***Přidat*** – umožňuje výběrem z navigačního stromu lokálního disku vybrat další soubory definované jako výjimky
- ***Přidat seznam*** – umožňuje přímo zadat seznam souborů, které mají být z testování ***Rezidentního štítu*** vyňaty
- ***Upravit*** – umožňuje editovat zadání cesty ke zvolenému souboru
- ***Upravit seznam*** – umožňuje editovat zadání seznamu souborů
- ***Smazat*** – umožňuje odstranit cestu ke zvolenému souboru

10.12. Server vyrovnávací paměti

Server vyrovnávací paměti je proces k urychlení testování (*pro testy na vyžádání, naplánované testy počítače i testy Rezidentního štítu*). V rámci tohoto procesu **AVG 9 Anti Virus plus Firewall** detekuje a ukládá informace o důvěryhodných souborech (*tj. o systémových souborech s digitálním podpisem*): tyto soubory jsou pak automaticky považovány za bezpečné a není třeba je znovu testovat.

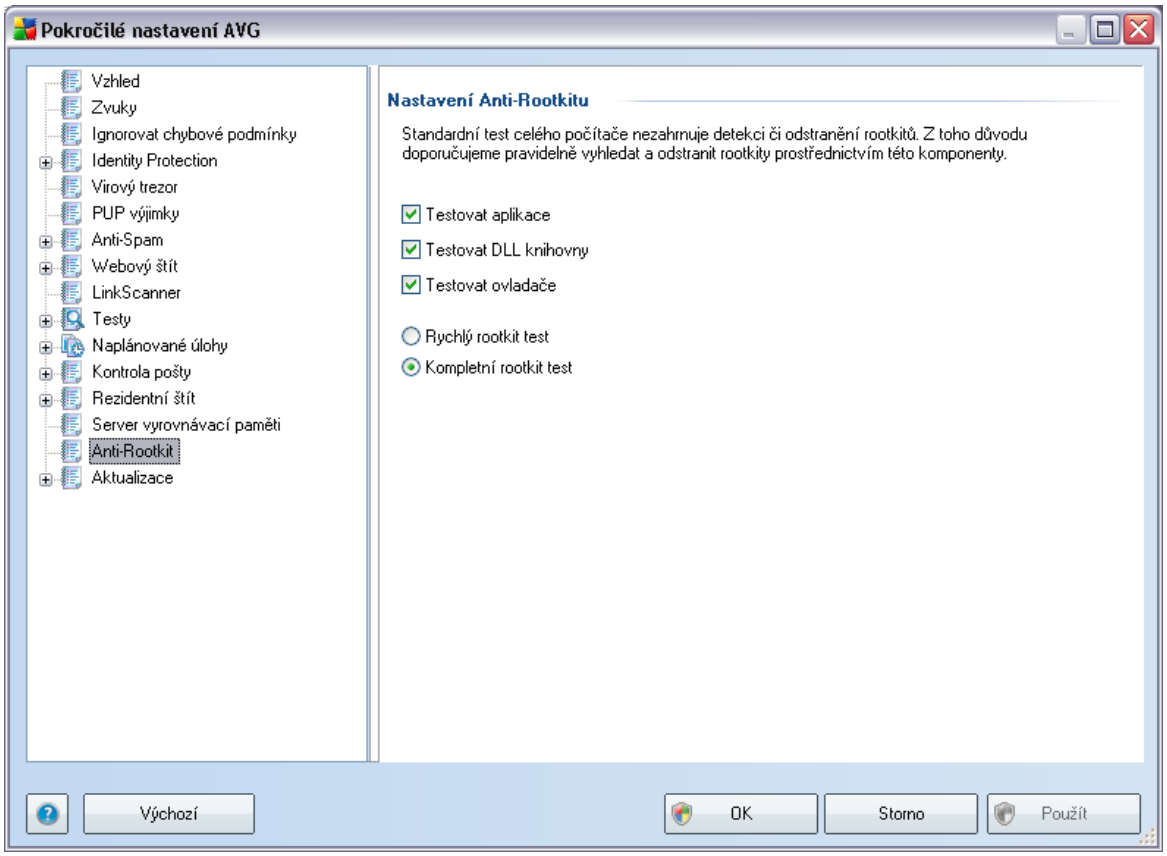


Dialog nastavení nabízí dvě možnosti:

- ***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.

10.13. 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***.

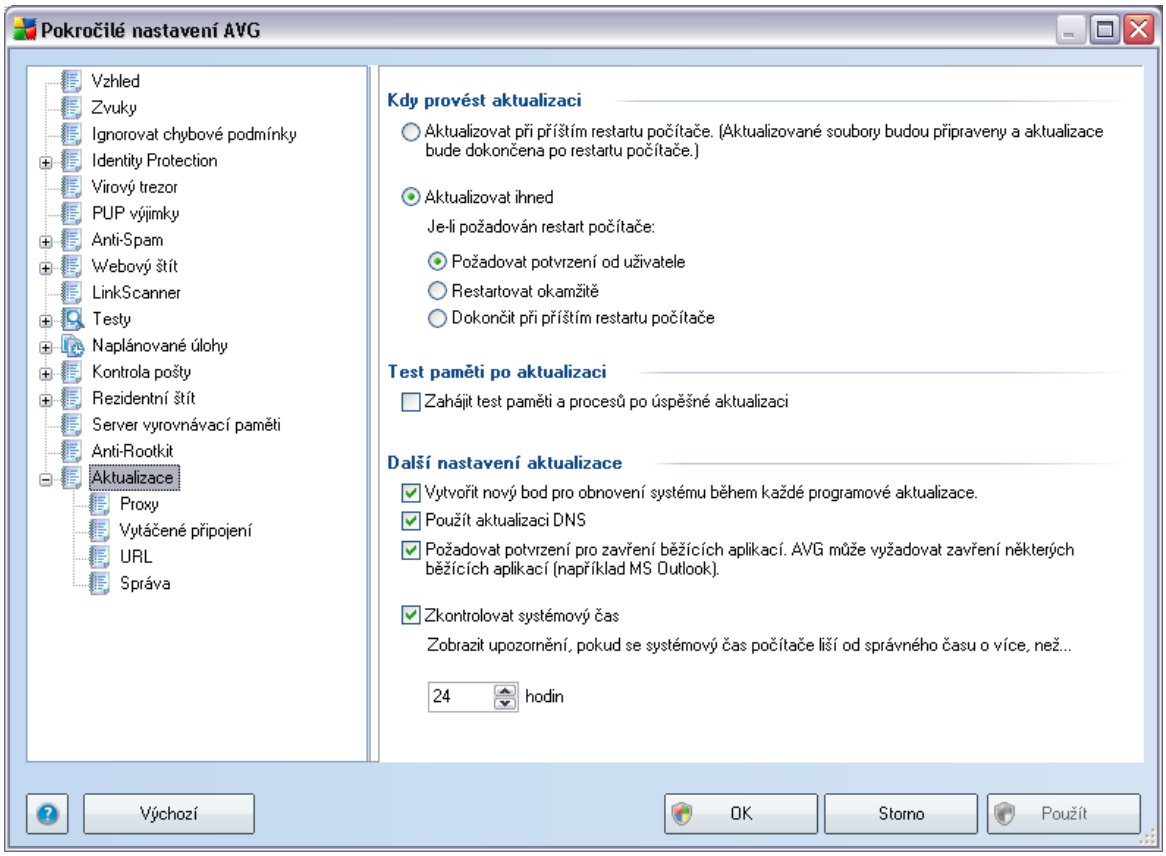
Označením příslušného políčka (*jednoho nebo více*) označte, jaké objekty mají být testovány:

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

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

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

10.14. 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: aktualizaci lze naplánovat na příští restart počítače nebo můžete provést aktualizaci okamžitě. Ve výchozím nastavení je zvolena alternativa okamžité aktualizace, protože ta zaručuje nejvyšší míru bezpečnosti. Naplánování aktualizace na příští restart lze doporučit pouze v případě, že počítač skutečně pravidelně restartujete, a to nejméně jednou denně.

Ponecháte-li nastavenu výchozí konfiguraci a aktualizační proces spustíte okamžitě, můžete pro případ vyžadovaného restartu počítače rozhodnout, jak má být restart proveden:

- ***Požadovat potvrzení od uživatele*** - 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 opět doporučujeme použít pouze tehdy, když jste si jisti, že počítač bude skutečně restartován nejpozději do 24 hodin

Test paměti po aktualizaci

Označíte-li tuto položku, bude po každé úspěšně 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:

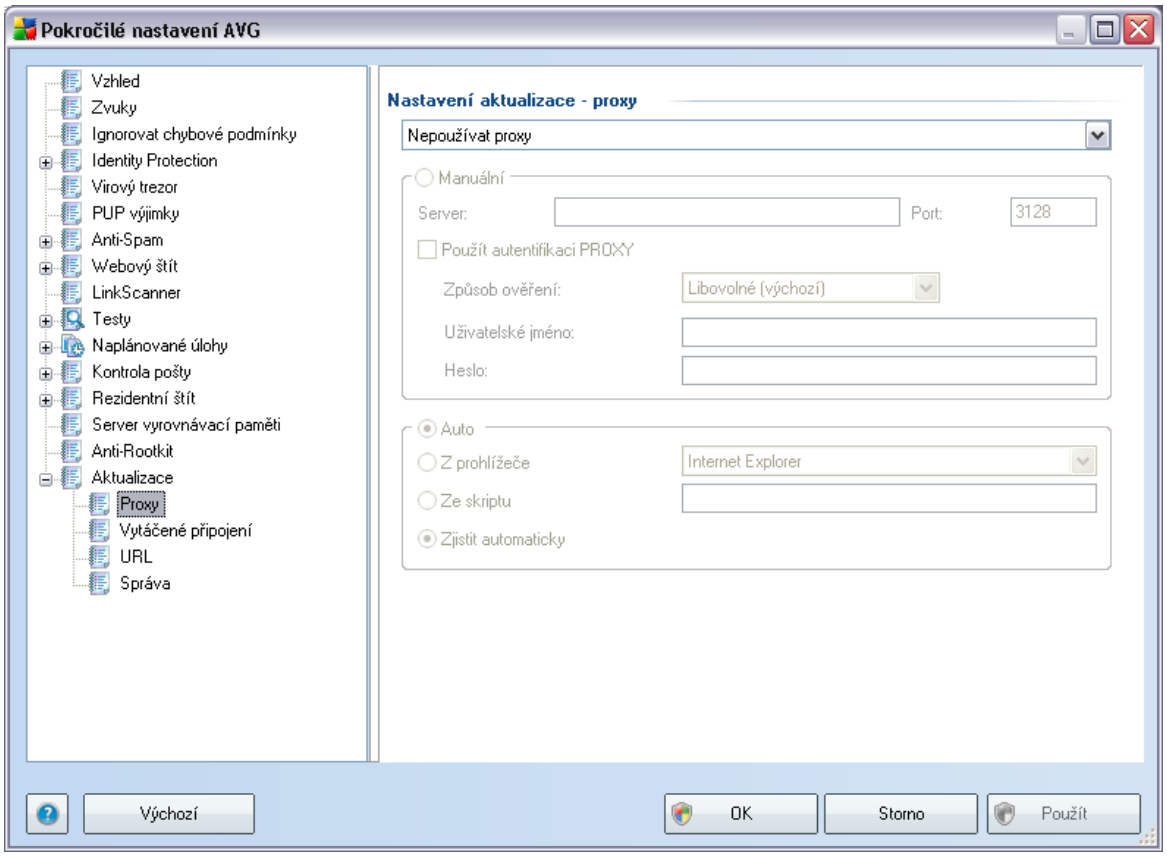
- ***Po každé programové aktualizaci vytvořit nový bod pro obnovení systému*** - před každým spuštěním programové aktualizace AVG je tak zvaný systémový bod pro obnovení systému. V případě, že aktualizační proces nebude z nějakého důvodu dokončen a váš operační systém bude ohrožen, můžete za pomoci tohoto zálohovacího bodu obnovit OS v jeho původní konfiguraci. Tato možnost je dostupná přes volbu *Start / Všechny programy / Příslušenství / Systémové nástroje / Obnova systému*, ale jakékoliv zásahy do tohoto nastavení lze doporučit výhradně pokročilým a zkušeným uživatelům! Chcete-li využít této možnosti, ponechejte políčko označené.

- ***Použít aktualizaci DNS*** - označením této položky potvrdíte, že chcete použít metodu detekce aktualizačních souborů, s jejíž pomocí lze eliminovat objem dat přenesených mezi aktualizačním serverem a AVG klientem;

- ***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 nastaveném na počítači a skutečným časem, a to v okamžiku, kdy rozdíl těchto dvou časů dosáhne stanoveného počtu hodin.

10.14.1. Proxy



Proxy server je samostatný server nebo služba běžící na libovolném počítači, která slouží k zajištění bezpečnějšího připojení k internetu. Podle nastavení pravidel sítě 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 určete, 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 sítě*)

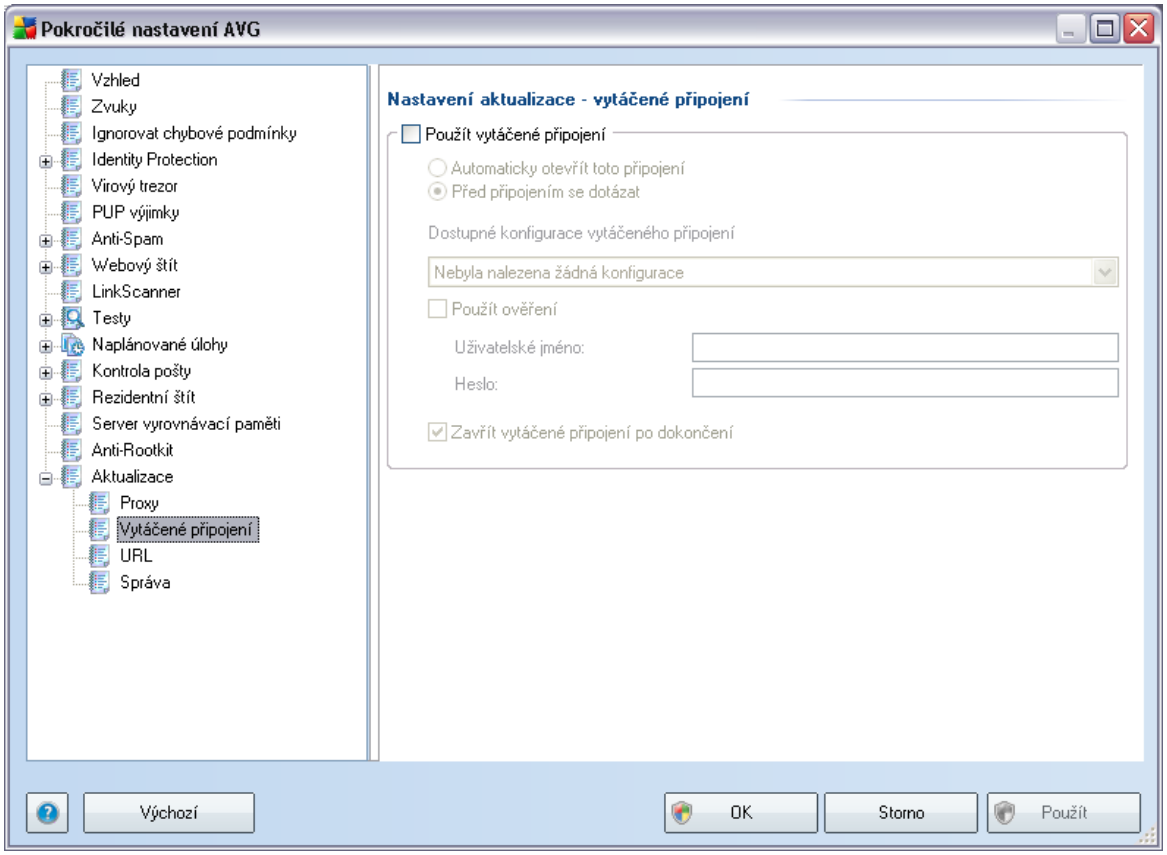
Proxy server může mít dále nastavena různá přístupová práva pro jednotlivé uživatele. Jestliže je váš proxy server takto nastaven, označte položku ***Použít autentifikaci PROXY*** a zadejte své ***Uživatelské jméno*** a ***Heslo*** pro připojení k internetu přes proxy server.

Automatické nastavení

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

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

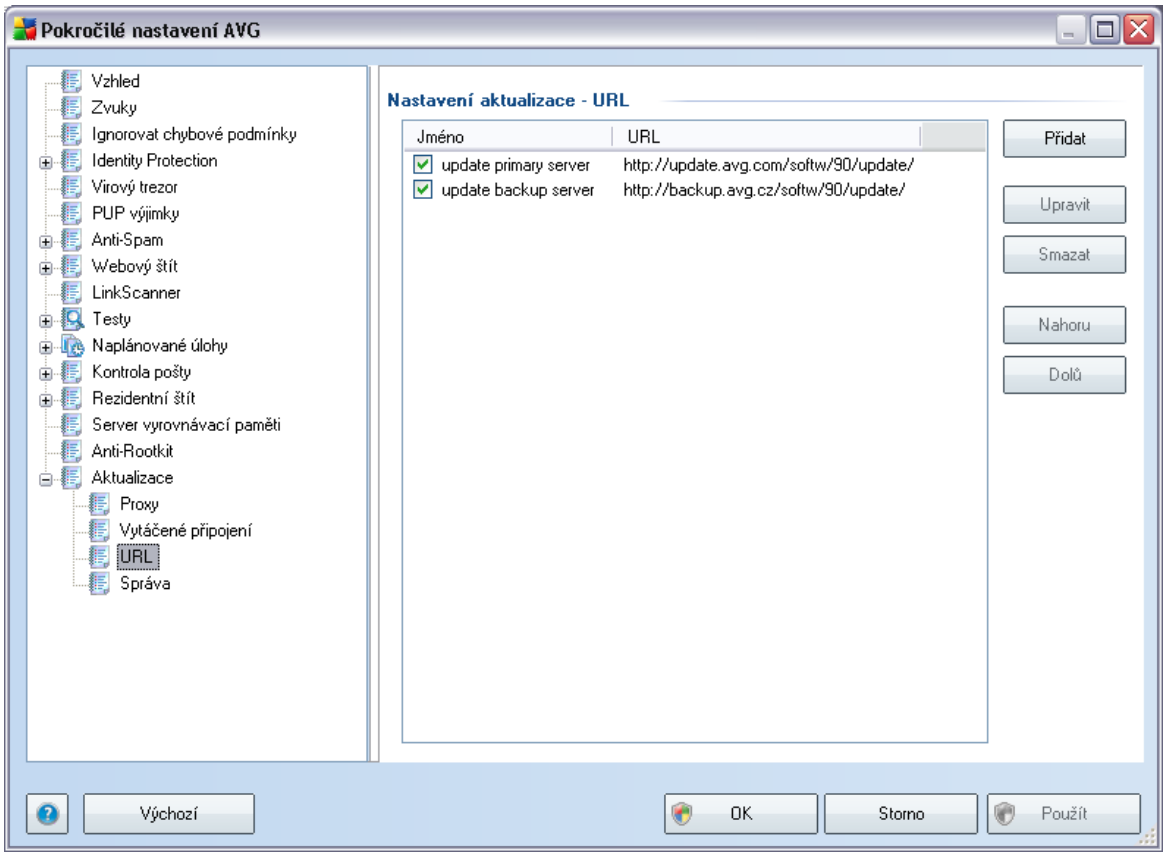
10.14.2. Vytáčené připojení



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

Určete, zda má být připojení k internetu provedeno automaticky (***Automaticky otevřít toto připojení***) anebo je třeba, aby uživatel každé připojení potvrdil (***Před připojením se dotázat***). U automatického připojení se dále můžete rozhodnout, zda má být připojení po provedení aktualizace ukončeno (***Zavřít vytáčené připojení po dokončení***).

10.14.3. URL

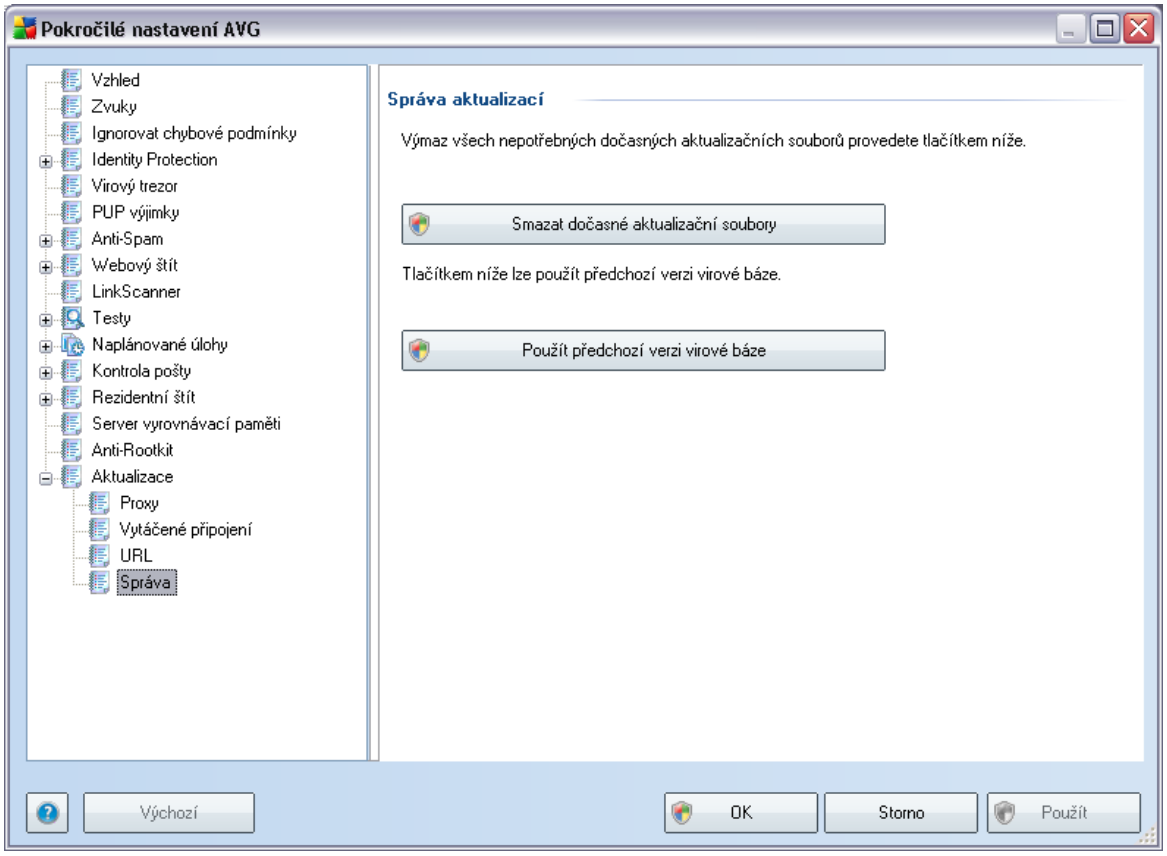


Dialog ***URL*** nabízí seznam internetových adres, odkud mohou být aktualizační souboru staženy. Seznam a jeho jednotlivé položky lze editovat pomocí následujících ovládacích tlačítek:

- ***Přidat*** – otevře dialog, kde lze specifikovat další URL k přidání do seznamu
- ***Upravit*** - otevře dialog, kde lze editovat parametry stávající URL
- ***Smazat*** – smaže zvolenou položku seznamu
- ***Nahoru*** – přemístí zvolenou URL na o jednu pozici v seznamu výš
- ***Dolů*** - přemístí zvolenou URL na o jednu pozici v seznamu níž

10.14.4. Správa

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

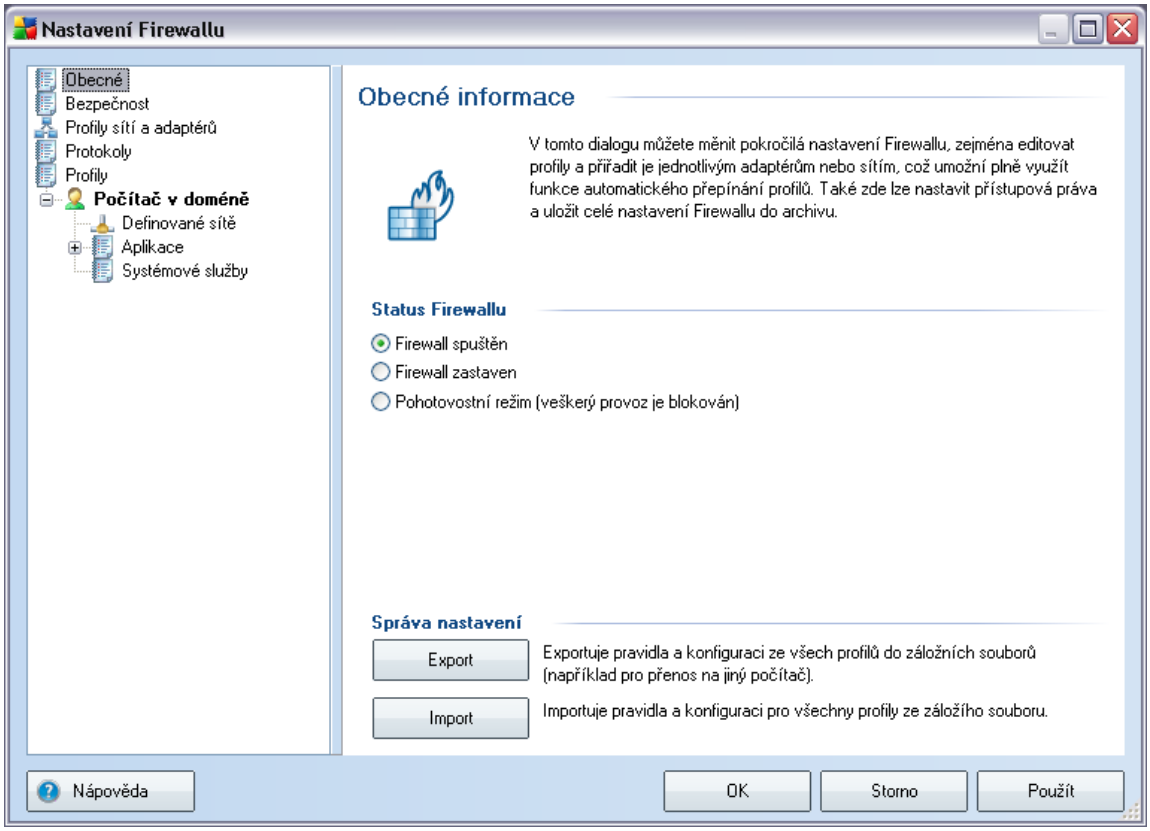


- ***Smazat dočasné aktualizační soubory*** - tímto tlačítkem odstraníte ze svého pevného disku všechny již nepotřebné soubory aktualizací (*ve výchozím nastavení správy aktualizačních souborů se tyto uchovávají po dobu po 30 dní*)
- ***Použít předchozí verzi virové báze*** – tímto tlačítkem odstraníte 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*)

11. Nastavení Firewallu

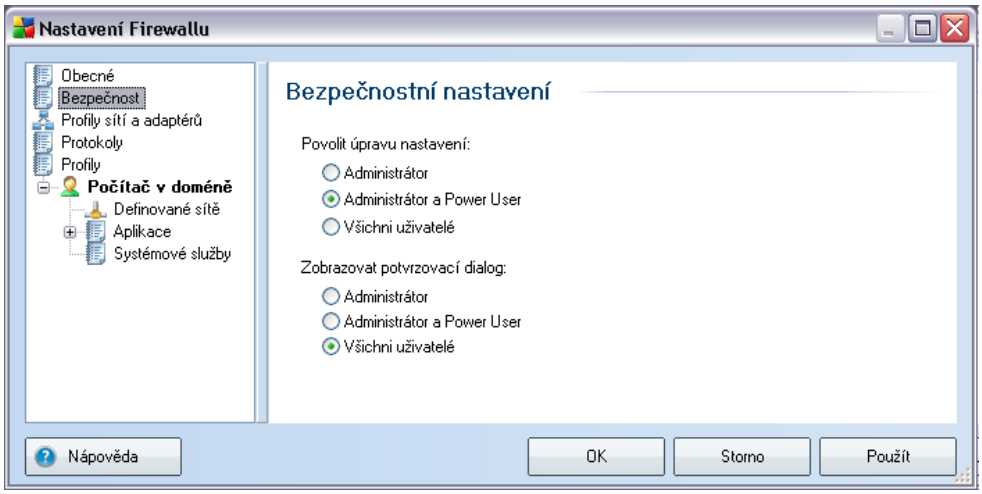
Konfigurace ***Firewallu*** se otevírá v samostatném okně, kde můžete na několika dialozích nastavit velmi pokročilé parametry komponenty. ***Editaci pokročilé konfigurace je však určena výhradně znalým a zkušeným uživatelům.***

11.1. Obecné



V dialogu ***Obecné informace*** můžete ***Exportovat*** nastavení komponenty ***Firewall*** do záložních souborů anebo naopak ***Importovat*** kompletní zálohované nastavení ***Firewallu***.

11.2. Bezpečnost



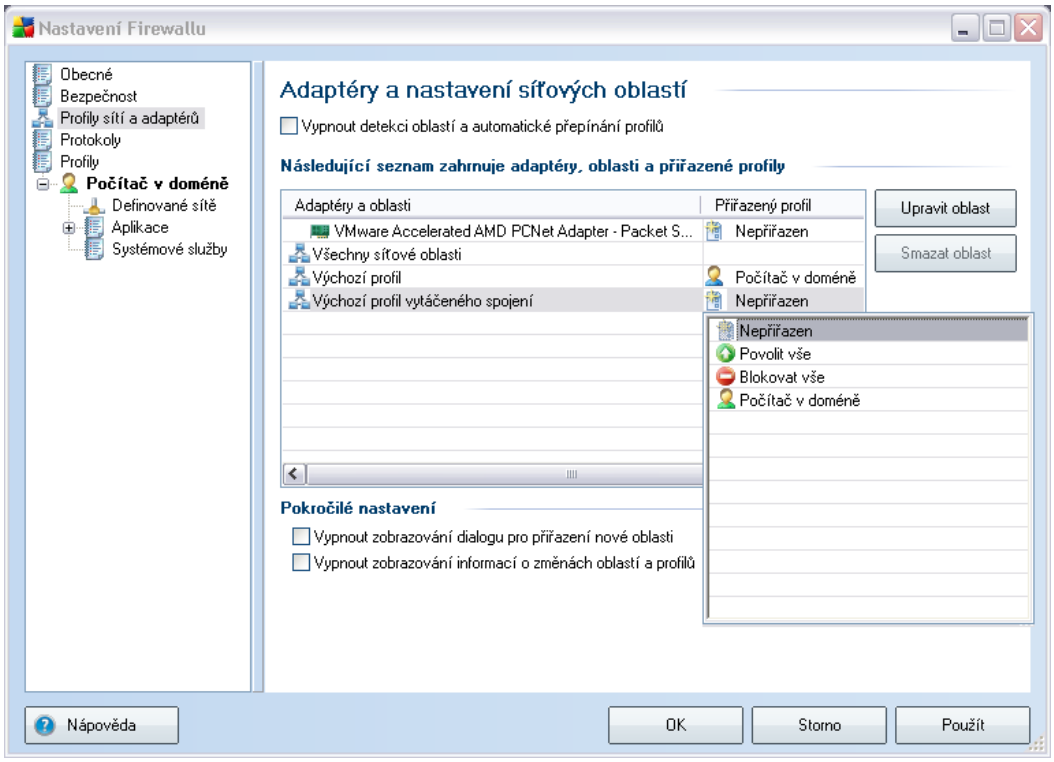
V dialogu ***Bezpečnostní nastavení*** definujte obecná pravidla pro správu komponenty ***Firewall*** bez ohledu na nastavený profil:

- ***Povolit úpravu nastavení*** - určete, kdo má právo měnit konfiguraci ***Firewallu***
- ***Zobrazovat potvrzovací dialog*** - komu se mají zobrazovat dotazovací dialogy vyžadující rozhodnutí v situaci, která není ošetřena definovaným pravidlem ***Firewallu***

V obou případech můžete přiřadit konkrétní pravomoc některé z těchto kategorií uživatelů:

- ***Administrátor*** – má kompletní kontrolu nad počítačem a právo přiřazovat jednotlivé uživatele do skupin s různou úrovní pravomocí
- ***Administrátor a Power User*** – administrátor může uživatele začlenit do specifické skupiny (*Power Users*) a sám definovat pravomoci jejích členů
- ***Všichni uživatelé*** – ostatní uživatelé nezařazení do specificky definovaných skupin

11.3. Profily sítí a adaptérů



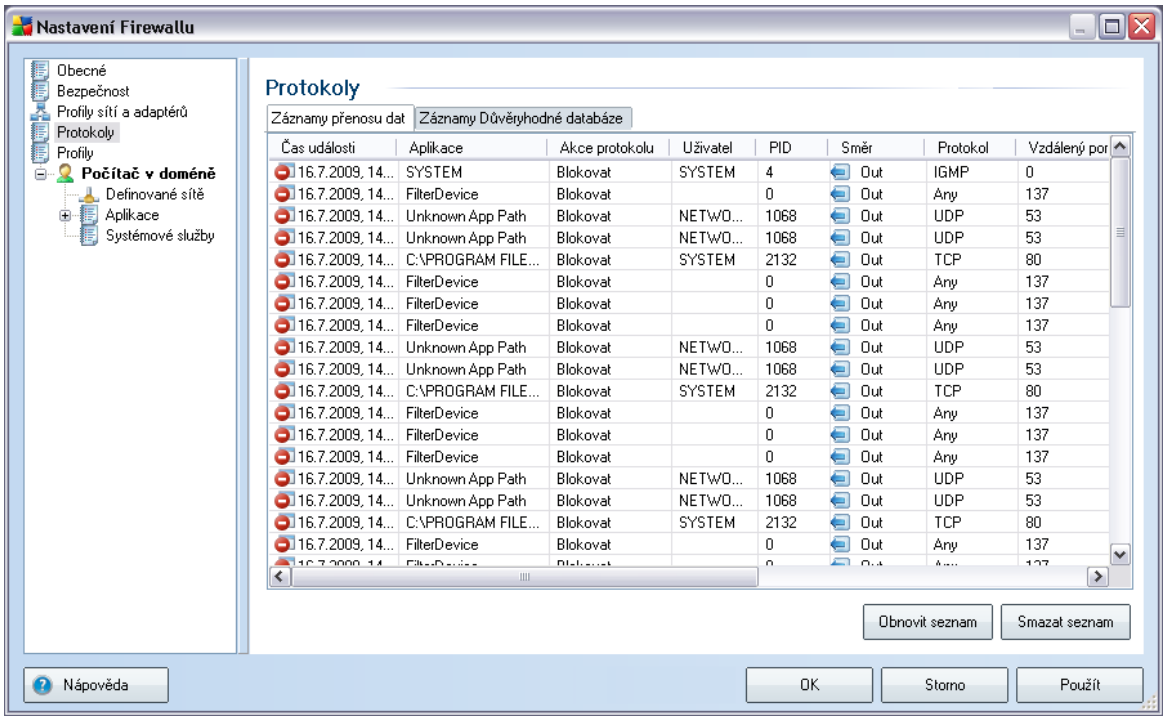
V dialogu ***Adaptéry a nastavení síťových oblastí*** můžete editovat nastavení související s přiřazením jednotlivých definovaných profilů specifickým adaptérům a jim příslušným sítím:

- ***Vypnout detekci oblastí a automatické přepínání profilů*** - každému typu síťového rozhraní, respektive oblasti, lze přiřadit jeden z předdefinovaných profilů. Pokud specifické profily definovat nechcete, bude se automaticky používat jediný společný profil nastavený na základě vaší volby způsobu použití počítače a způsobu připojení počítače k síti v průběhu ***Instalačního procesu***. Pokud se však rozhodnete profily rozlišovat a přiřadit je jednotlivě specifickým adaptérům a jim příslušným oblastem, a později toto nastavení potřebujete z nějakého důvodu dočasně deaktivovat, označte položku ***Vypnout detekci oblastí a automatické přepínání profilů***.

- ***Seznam adaptérů, oblastí a přiřazených profilů*** - v seznamu najdete přehled detekovaných adaptérů a oblastí. Každému z nich máte možnost přiřadit specifický profil z nabídky definovaných profilů. Tuto nabídku otevřete kliknutím myši na příslušnou položku seznamu adaptérů a vyberte profil.

- ***Pokročilé nastavení*** - označením příslušné volby deaktivujete zobrazování informačních hlášení.

11.4. Protokoly



Dialog ***Protokoly*** nabízí seznamy všech protokolovaných událostí ***Firewallu*** s přehledem parametrů jednotlivých událostí (*čas události, jméno aplikace, která se pokoušela navázat spojení, příslušnou akci protokolu, jméno uživatele, PID, směr připojení, typ protokolu, číslo vzdáleného a místního portu, ...*) na dvou záložkách:

- ***Záznamy přenosu dat*** - nabízí informace o veškeré aktivitě aplikací, které se jakýkoliv způsobem pokusily o navázání síťové komunikace
- ***Záznamy důvěryhodné databáze*** - *Důvěryhodná databáze* je interní databáze AVG, v níž jsou shromážděny informace o aplikacích, které mají ověřený certifikát, jsou prověřené a důvěryhodné, a komunikace jim může být povolena. Při prvním pokusu jakékoliv aplikace o navázání síťové komunikace (*tedy v situaci, kdy pro danou aplikaci ještě není nastaveno žádné pravidlo*) je třeba zjistit, zda má být této aplikaci komunikace povolena. AVG nejprve prohledá *Důvěryhodnou databázi*, a pokud je v ní daná aplikace uvedena, bude její komunikace automaticky povolena. Teprve v případě, že o aplikaci nemáme k dispozici žádné informace, budete v samostatném dialogu dotázáni, zda si přejete komunikaci povolit.

Ovládací tlačítka dialogu

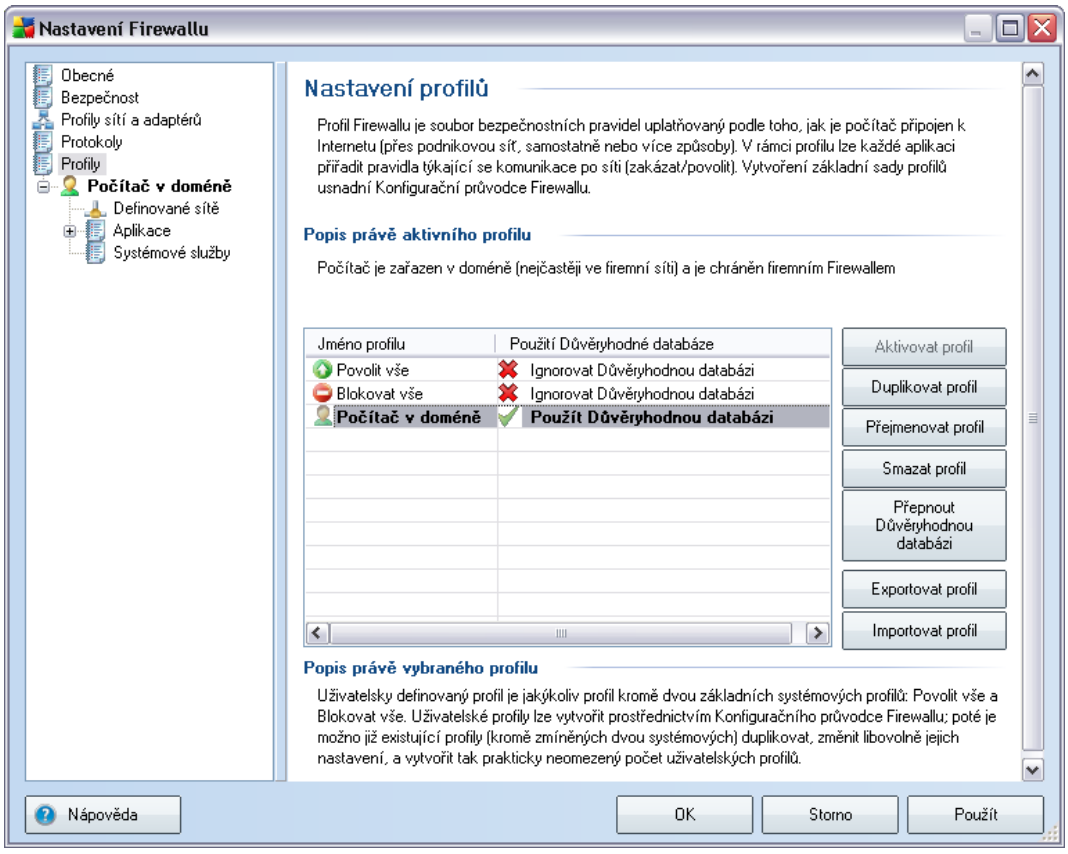
- ***Nápověda*** - otevírá kontextovou nápovědu k aktuálnímu dialogu.
- ***Obnovit seznam*** - protokolované parametry lze řadit podle zvoleného atributu: data chronologicky, ostatní sloupce abecedně (*klikněte na nadpis*

příslušného sloupce). Tímto tlačítkem pak můžete zobrazené informace aktualizovat.

- ***Smazat seznam*** - odstraní všechny záznamy z tabulky ***Protokoly***.

11.5. Profily

V dialogu ***Nastavení profilů*** najdete seznam všech dostupných profilů:



Všechny uživatelské (*nikoli systémové*) profily můžete editovat pomocí následujících ovládacích tlačítek:

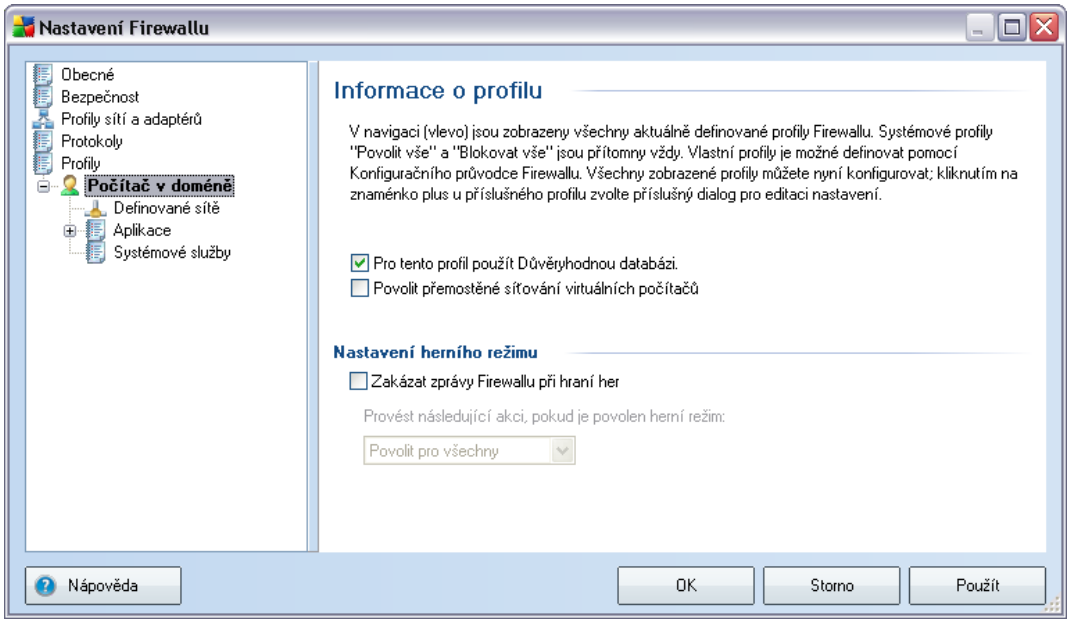
- ***Aktivovat profil*** - tlačítkem nastavíte zvolený profil jako aktivní, jeho nastavení bude použito pro řízení provozu ***Firewallem***
- ***Duplikovat profil*** - vytvoří kopii zvoleného profilu se stejným nastavením; tuto kopii pak budete moci editovat a přejmenovat, čímž bude definován nový profil

- ***Přejmenovat profil*** - umožní definovat nové jméno zvoleného profilu
- ***Smazat profil*** - smaže zvolený profil ze seznamu
- ***Přepnout Důvěryhodnou databázi*** - u konkrétního zvoleného profilu umožní využití záznamů *Důvěryhodné databáze* (*interní databáze AVG shromažďující informace o ověřených a certifikátem opatřených aplikacích, jimž může být komunikace vždy povolena.*)
- ***Exportovat profil*** - zaznamená konfiguraci zvoleného profilu do souboru, který uloží pro případné použití v budoucnosti
- ***Importovat profil*** - nastaví konfiguraci zvoleného profilu ze záložního souboru
- ***Nápověda*** - otevře kontextovou nápovědu k aktuálnímu dialogu

Ve spodní části dialogu pak najdete popis v seznamu aktuálně zvoleného profilu.

Podle počtu definovaných profilů, jež se zobrazí v seznamu tohoto dialogu, se bude generovat i další menu v levé sekci se stromovou navigací. Každý z definovaných profilů vytvoří v navigaci svou vlastní větev pod položkou ***Profily***. Jednotlivé profily lze pak samostatně editovat v následujících dialozích (*identických pro všechny profily*):

11.5.1. Informace o profilu



Dialog ***Informace o profilu*** je úvodním dialogem k sekci, v níž můžete editovat nastavení jednotlivých profilů v samostatných dialozích členěných podle jednotlivých parametrů příslušných každému profilu:

- ***Pro tento profil použít Důvěryhodnou databázi*** - (*ve výchozím nastavení zapnuto*) označením položky aktivujete možnost použití *Důvěryhodné databáze*,

tedy interní databáze AVG, v níž jsou shromážděny informace o aplikacích, které mají ověřený certifikát, jsou prověřené a důvěryhodné, a komunikace jim může být povolena. Při prvním pokusu jakékoliv aplikace o navázání síťové komunikace (*v situaci, kdy pro danou aplikaci ještě není nastaveno žádné pravidlo*) je třeba zjistit, zda má být této aplikaci komunikace povolena. AVG nejprve prohledá *Důvěryhodnou databázi*, a pokud je v ní daní aplikace uvedena, bude její komunikace automaticky povolena. Teprve v případě, že o aplikaci nemáme k dispozici žádné informace, budete v samostatném dialogu dotázáni, zda si přejete komunikaci povolit.

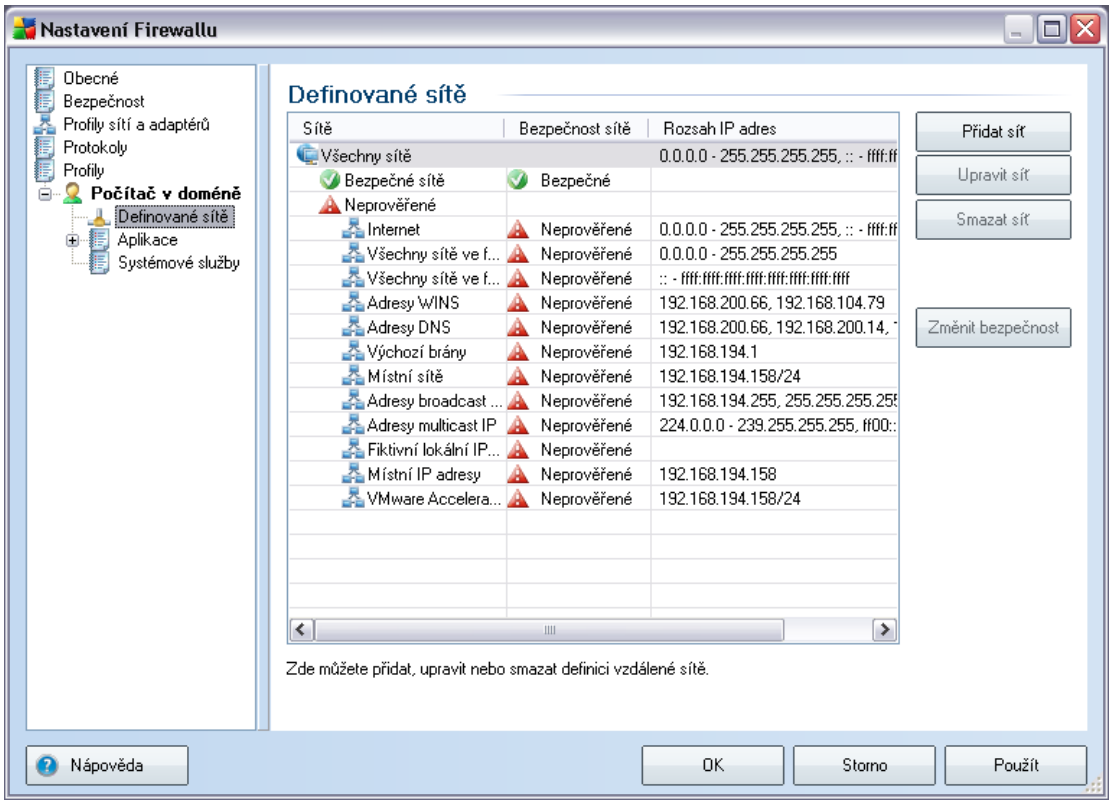
- ***Povolit přemostění síťování virtuálních počítačů*** - (*ve výchozím nastavení vypnuto*) označením této položky umožníte přímé připojení virtuálního počítače ve VMware do sítě

Nastavení herního režimu

V sekci ***Nastavení herního režimu*** se můžete rozhodnout a označením položky potvrdit, že si přejete, aby vám byly zobrazovány informační hlášení ***Firewallu*** i během práce s aplikací, která využívá celé obrazovky (*typicky hry, ale i veškeré full-screen aplikace, například PPT prezentace*). Tato oznámení mohou být při práci na celé obrazovce poněkud rušivá.

Jestliže tedy zapnete položku ***Zakázat zprávy Firewallu při hraní her***, v rozbalovací nabídce pak zvolte, jaká akce má být provedena v případě, že se o komunikaci po síti pokusí nově detekovaná aplikace, pro niž dosud nebylo nastaveno pravidlo a na jejíž chování by se za normálních okolností ***Firewall*** zeptal - všechny takovéto aplikace mohou být buďto jednotně povoleny nebo zablokovány.

11.5.2. Definované sítě

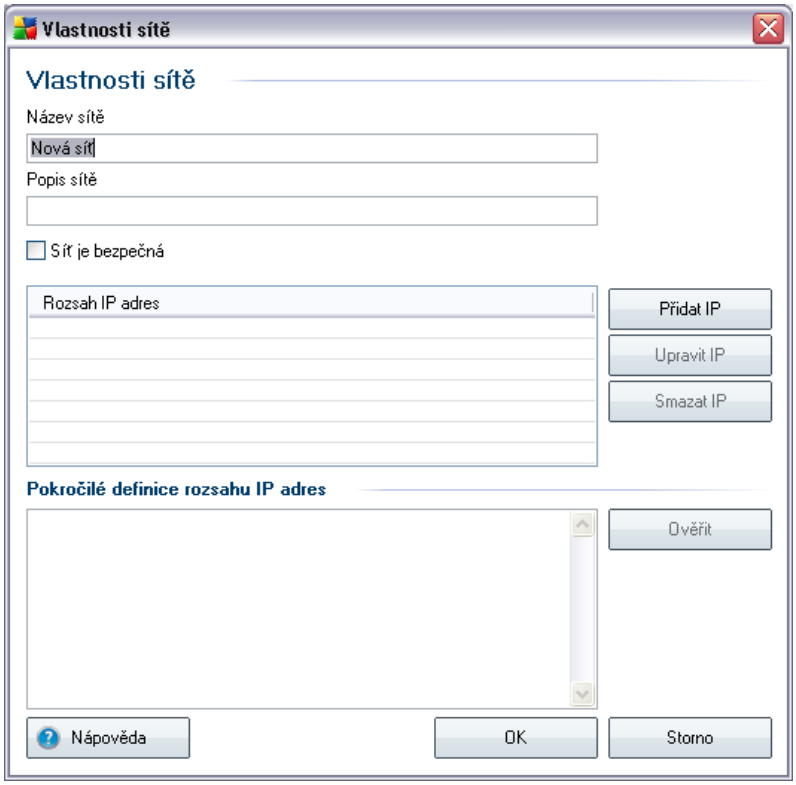


Dialog ***Definované sítě*** nabízí seznam všech sítí, k nimž je váš počítač připojen. O detekovaných sítích jsou k dispozici tyto informace:

- ***Sítě*** - seznam jmen všech detekovaných sítí, k nimž je počítač připojen
- ***Bezpečnost sítě*** - ve výchozím nastavení jsou všechny sítě označeny jako neprověřené; pokud jste si jisti jejich bezpečností, můžete konkrétní síť označit jako bezpečnou (*klikněte na položku seznamu odpovídající konkrétní síti a v kontextové nabídce zvolte Bezpečné*) - všechny bezpečné sítě pak budou zahrnuty do skupiny těch, do nichž bude aplikaci povoleno se připojit, bude-li mít nastaveno pravidlo ***Povolit pro bezpečné***
- ***Rozsah IP adres*** - rozsah každé sítě bude detekován automaticky a uveden ve tvaru rozpětí IP adres

Ovládací tlačítka

- ***Přidat síť*** - otevře dialogové okno ***Vlastnosti sítě***, v němž můžete definovat parametry nově přidávané sítě:



V dialogu lze zadat ***Název sítě***, uvést stručný ***Popis sítě*** a případně označit síť za bezpečnou. Síť můžete definovat manuálně v samostatném dialogu dostupném prostřednictvím tlačítka ***Přidat IP*** (podobně ***Upravit IP*** / ***Smazat IP***), kde zadáte rozsah nebo masku sítě.

Při velkém množství sítí, které chcete definovat jako součást přidávané sítě, můžete využít hromadného přidání v sekci ***Pokročilé definice rozsahu IP adres***: do textového pole vložte seznam sítí (*v jakémkoli známém formátu*) a tlačítkem ***Ověřit*** zjistěte, zda jsou všechny zadány v platném tvaru. Pokud ano, stiskem tlačítka ***OK*** potvrdíte jejich uložení.

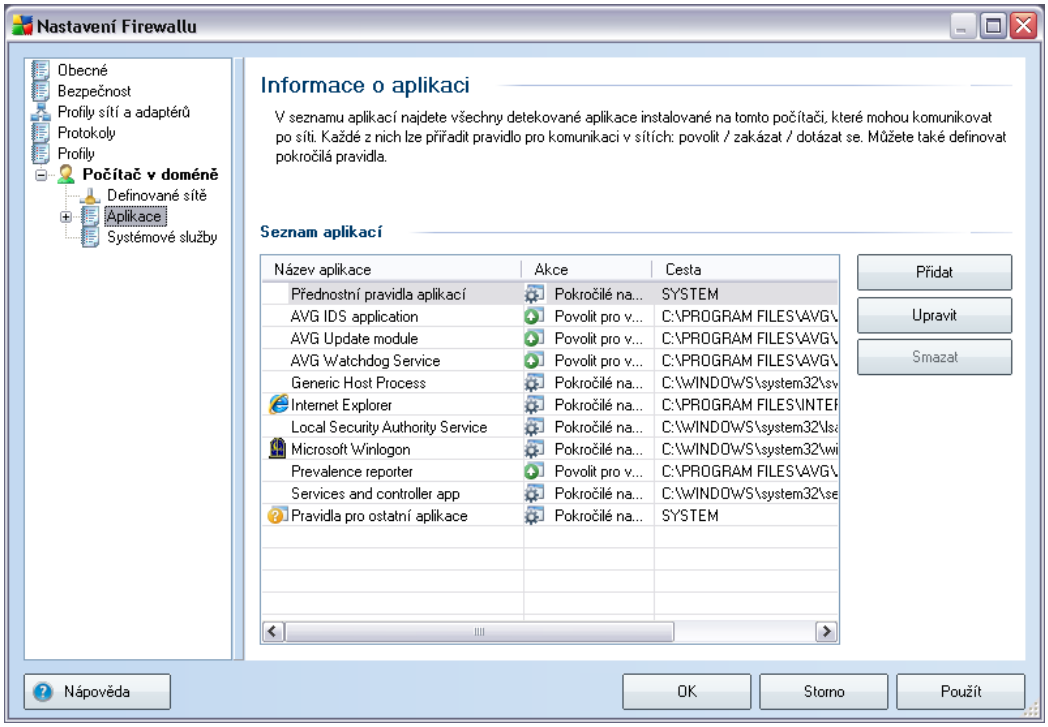
- ***Upravit síť*** - otevře dialogové okno ***Vlastnosti sítě*** (*viz výše*), v němž můžete editovat parametry již definované sítě (*okno je identické s oknem pro přidání nové sítě, popis tedy najdete v předchozím odstavci*)

- ***Smazat síť*** - odstraní záznam o zvolené síti ze seznamu

- ***Změnit bezpečnost*** - ve výchozím nastavení jsou všechny sítě označeny jako neprověřené; pokud jste si jisti jejich bezpečností, můžete konkrétní síť označit tímto tlačítkem jako bezpečnou (*a podobně, je-li síť definována jako bezpečná, tímto tlačítkem můžete změnit její status a označit ji za nebezpečnou*).

- ***Nápověda*** - otevře kontextovou nápovědu k aktuálnímu dialogu

11.5.3. Aplikace



V dialogu ***Informace o aplikaci*** najdete přehled všech instalovaných aplikací, které mohou komunikovat po síti. Zároveň je tu dostupný i přehled ikon znázorňujících jednotlivé akce:

- Povolit komunikaci pro všechny sítě
- Povolit komunikaci pro sítě zařazené do kategorie bezpečných (Povolit pro bezpečné)
- Blokovat komunikaci
- Zobrazit dotazovací dialog
- Pokročilé nastavení

Aplikace uvedené v seznamu byly detekovány na vašem počítači a byly jim přiřazeny příslušné akce.

Poznámka: Uvědomte si, prosím, že detekovány mohou být pouze ty aplikace, které byly na vašem počítači instalovány už ve chvíli spuštění Průvodce nastavením Firewallu; pokud jste nainstalovali novou aplikaci později, budete pro ni muset definovat pravidla samostatně. Ve chvíli, kdy se nová aplikace poprvé pokusí navázat síťovou komunikaci, bude buď vytvořeno pravidlo podle Důvěryhodné databáze, anebo budete vyzváni k nastavení pravidla; pak bude třeba rozhodnout, zda má být komunikace této aplikaci povolena nebo blokována. Svou volbu můžete uložit jako trvalé pravidlo (které bude následně

uvedeno v seznamu v tomto dialogu).

Samozřejmě je také možné definovat pravidla pro nové aplikace okamžitě – stiskněte tlačítko ***Přidat*** v tomto dialogu a vyplňte údaje o aplikaci.

Kromě aplikací obsahuje seznam ještě dvě speciální položky:

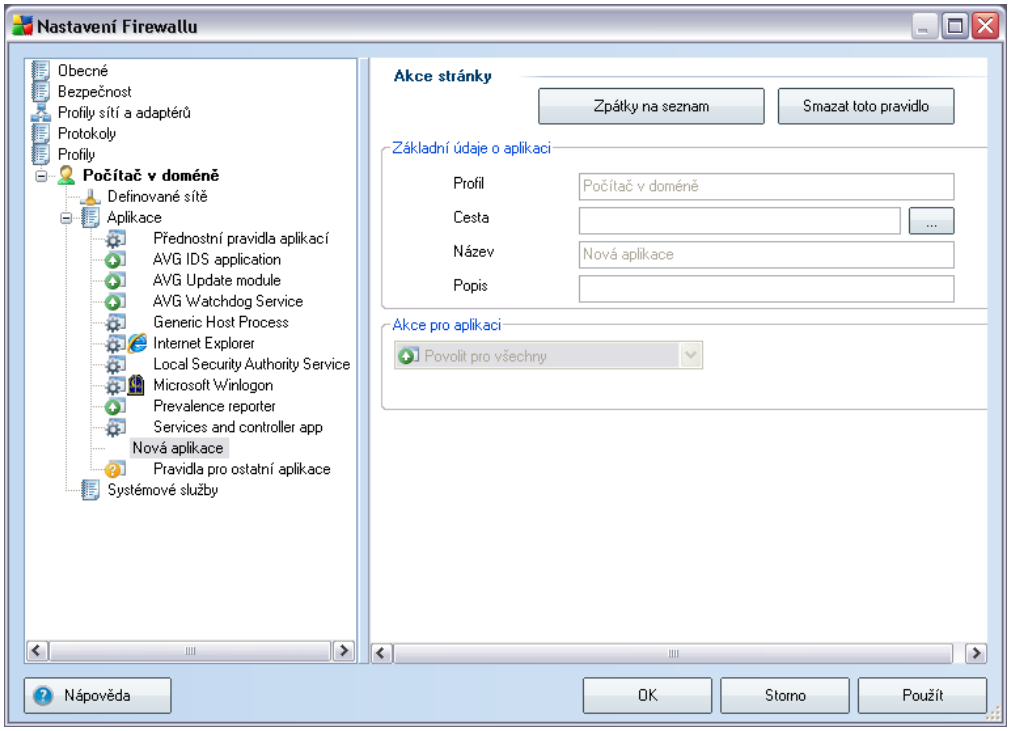
- ***Přednostní pravidla aplikací*** (*první řádek seznamu*) jsou preferenčními pravidly a jsou uplatňována přednostně před pravidly definovanými pro specifickou aplikaci.
- ***Pravidla pro ostatní aplikace*** (*poslední řádek seznamu*) se používají jako "poslední instance" v situaci, kdy nelze použít žádné specifické pravidlo pro aplikaci, například pro neznámou a nedefinovanou aplikaci.

Tyto položky se možnostmi svého nastavení liší od běžných aplikací a jsou určeny výhradně pro pokročilé uživatele.

Ovládací tlačítka

Seznam můžete editovat pomocí těchto ovládacích tlačítek:

- ***Přidat*** - otevře prázdný dialog ***Akce stránky*** pro přidání nové aplikace
- ***Upravit*** - otevře již vyplněný dialog ***Akce stránky*** pro upravení parametrů stávající aplikace
- ***Smazat*** - odstraní zvolenou aplikaci ze seznamu
- ***Nápověda*** - otevře kontextovou nápovědu k aktuálnímu dialogu



V tomto dialogu můžete definovat podrobná nastavení pro konkrétní aplikaci.

Akce stránky

- Tlačítko ***Zpátky na seznam*** zobrazí seznam všech aktuálně definovaných pravidel pro aplikace.
- Tlačítko ***Smazat toto pravidlo*** vymaže právě zobrazené pravidlo pro aplikaci. Prosím pozor, tato akce je nevratná!

Základní údaje o aplikaci

V této sekci zadejte ***Název*** aplikace a případně i ***Popis*** (*stručný komentář pro vlastní potřebu*). V poli ***Cesta*** uveďte plnou cestu k umístění aplikace (*spustitelného souboru*) na disku; nebo můžete aplikaci lokalizovat pomocí stromové struktury disku, jejíž zobrazení otevřete stiskem tlačítka "***...***".

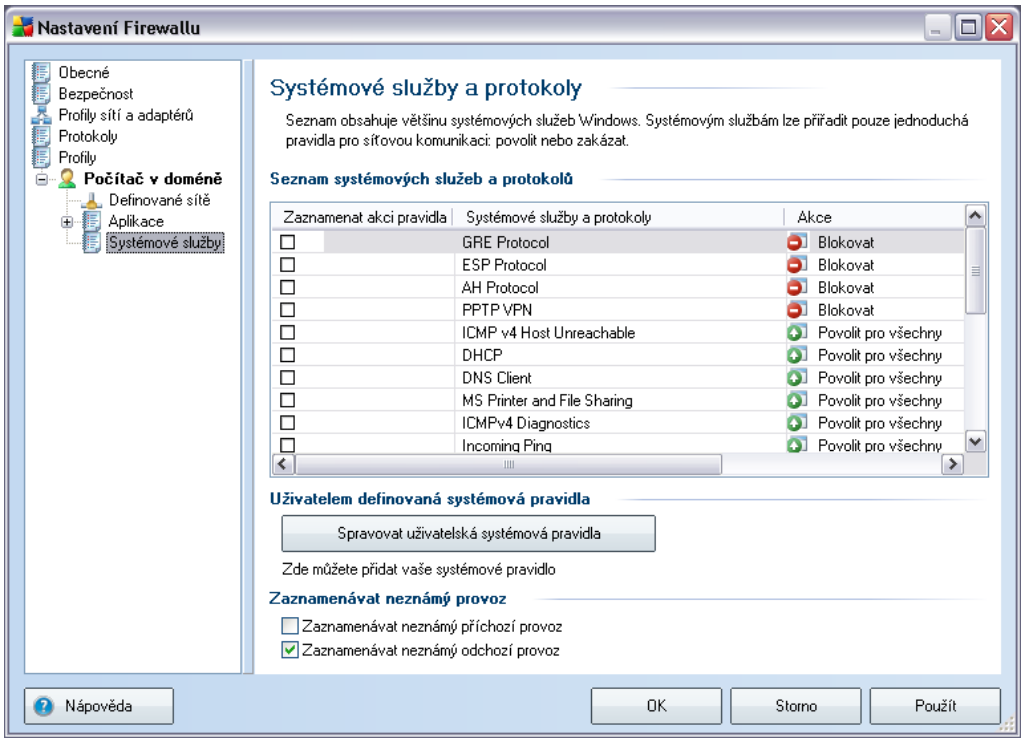
Akce pro aplikaci

V rozbalovacím menu můžete vybrat pravidlo, které chcete aplikaci přiřadit. Tímto pravidlem určujete, jak se Firewall zachová v situaci, kdy se aplikace pokusí navázat komunikaci po síti:

- ***Povolit pro všechny*** komunikace bude aplikaci povolena ve všech definovaných sítích a na všech adaptérech bez omezení.
- ***Povolit pro bezpečné*** komunikace bude aplikaci povolena pouze v sítích definovaných jako bezpečné.
- ***Blokovat*** komunikace bude automaticky zablokována; aplikaci nebude povoleno připojit se k žádné síti.
- ***Dotázat se*** při pokusu aplikace o navázání komunikace bude zobrazen dotazovací dialog o tom, zda si přejete tento pokus o komunikaci jednorázově povolit nebo zablokovat.
- ***Pokročilé nastavení*** zobrazí v dolní části dialogu sekci pro podrobné nastavení pravidla pro aplikaci. V sekci ***Podrobná pravidla pro aplikaci*** můžete definovat detailní pravidla; detaily nastavení budou uplatňovány podle pořadí v seznamu; jejich prioritu tedy můžete měnit posunem v seznamu pomocí tlačítek ***Nahoru*** nebo ***Dolů***. Označíte-li některé pravidlo v seznamu, v dolní části dialogu se zobrazí přehled detailů pravidla. Každá položka vyznačená modrým podtrženým písmem může být po kliknutí změněna v příslušném dialogu (*v každém je dostupná samostatná nápověda*). Označený detail pravidla lze vymazat stisknutím tlačítka ***Smazat***. Chcete-li definovat nový detail, použijte tlačítko ***Přidat***; tím otevřete dialog ***Upravit detail pravidla***, kde lze zadat všechna potřebná nastavení.

11.5.4. Systémové služby

Veškeré editace v dialogu Systémové služby a protokoly jsou určeny VÝHRADNĚ zkušeným uživatelům!

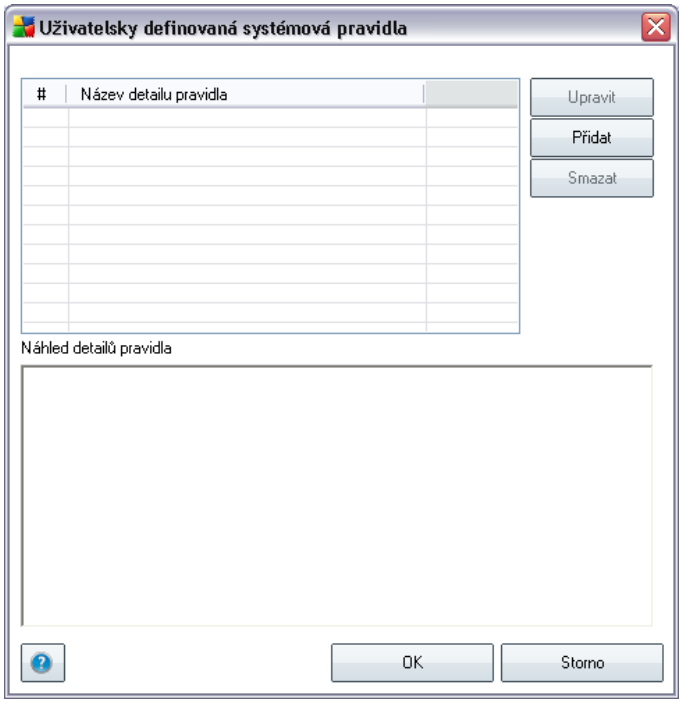


Dialog ***Systémové služby a protokoly*** uvádí přehled standardních systémových služeb Windows a protokolů, které mohou komunikovat po síti, a přehled ikon znázorňujících jednotlivé akce. Tabulka obsahuje tyto sloupce:

- ***Zaznamenat akci pravidla*** - označením políčka můžete zapnout protokolování akce příslušného pravidla.
- ***Systémové služby a protokoly*** - v tomto sloupci jsou zobrazena jména příslušných systémových služeb.
- ***Akce*** - sloupec zobrazuje ikony příslušné k určené akci:
  - Povolit komunikaci pro všechny sítě
  - Povolit komunikaci pro sítě zařazené do kategorie bezpečných (*Povolit pro bezpečné*)
  - Blokovat komunikaci
- ***Sítě*** - v tomto sloupci je uvedeno, ke které konkrétní síti se systémové pravidlo vztahuje.

Seznam (*včetně přiřazených akcí*) lze editovat pomocí těchto tlačítek:

- Tlačítko ***Upravit*** otevře dialog, v němž lze upravit pravidla existující aplikace.
- Chcete-li vytvořit vlastní systémové pravidlo, použijte tlačítko ***Spravovat uživatelská systémová pravidla***. V horní části dialogu ***Uživatelsky definovaná systémová pravidla*** vidíte přehled všech detailů právě editovaného systémového pravidla, v dolní části pak přehled vybraného detailu. S uživatelskými pravidly můžete pracovat pomocí tlačítek ***Upravit***, ***Přidat*** a ***Smazat***; systémová pravidla definovaná výrobcem pak můžete pouze ***Upravit***:



Upozornění: *Nastavení systémových pravidel je velmi pokročilé a je určeno zejména správcům sítí, kteří potřebují plnou kontrolu nad konfigurací Firewallu do nejmenších podrobností. Pokud nejste obeznámeni s typy komunikačních protokolů, čísly síťových portů, definicemi IP adres atd., prosíme, neměňte tato nastavení! Pokud nastavení skutečně měnit potřebujete, detailní popis jednotlivých dialogů najdete v příslušném souboru nápovědy.*

Zaznamenávat neznámý provoz

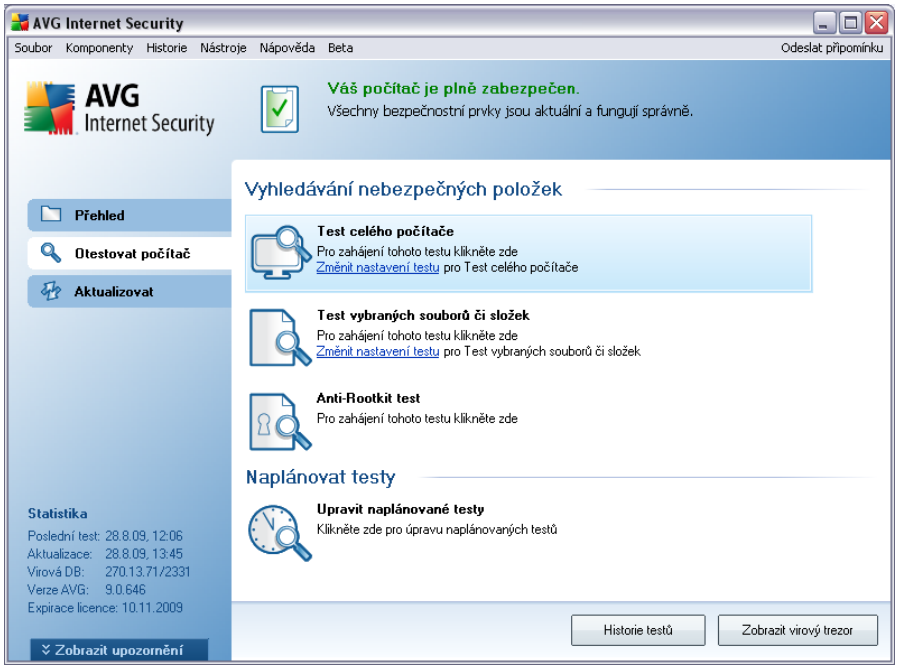
- ***Zaznamenávat neznámý příchozí provoz*** – označením této položky zajistíte, že všechny neznáme pokusy o navázání komunikace s vaším počítačem budou zaznamenány v protokolu.
- ***Zaznamenávat neznámý odchozí provoz*** *(ve výchozím nastavení zapnuto)* – označením této položky zajistíte, že všechny neznáme pokusy vašeho

počítače a komunikaci do sítě budou zaznamenány v protokolu.

12. AVG testování

Testování je elementární součástí **AVG 9 Anti Virus plus Firewall**. Testy lze spouštět na vyžádání podle okamžité situace (on-demand testy) nebo nastavit jejich pravidelné spouštění podle plánu.

12.1. Rozhraní pro testování



Testovací rozhraní AVG je dostupné prostřednictvím zkratkového tlačítka ***Otestovat počítač***. 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 testu - zde můžete definovat nové testy a nastavovat jejich spouštění 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

12.2. Přednastavené testy

Jednou z hlavních funkcí **AVG 9 Anti Virus plus Firewall** 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 viru prostý.

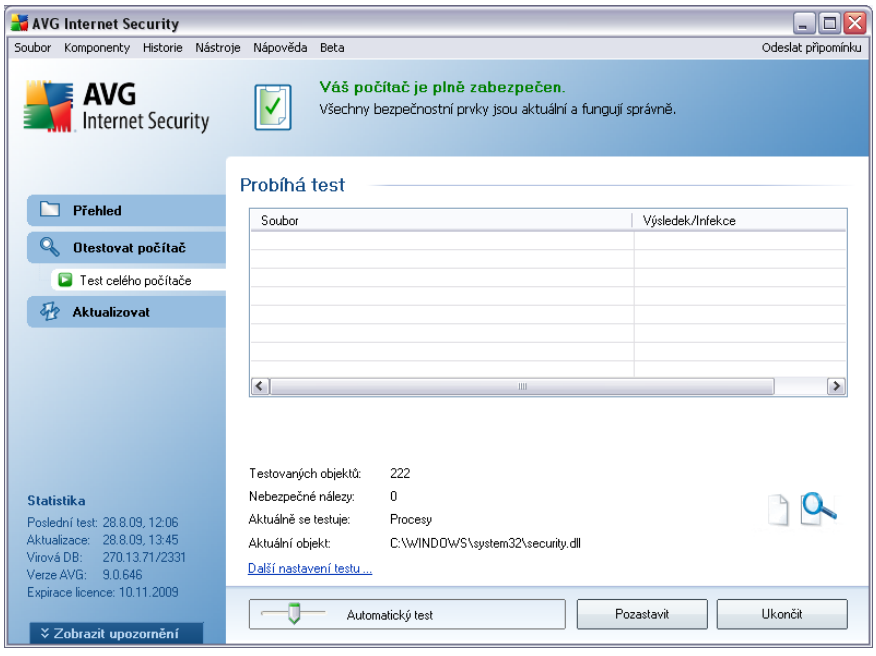
V **AVG 9 Anti Virus plus Firewall** najdete dva typy výrobcem nastavených testů:

12.2.1. 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 vyléčí či přesune do Virového trezoru. ***Test celého počítače*** by měl být na počítači naplánován minimálně jednou týdně.

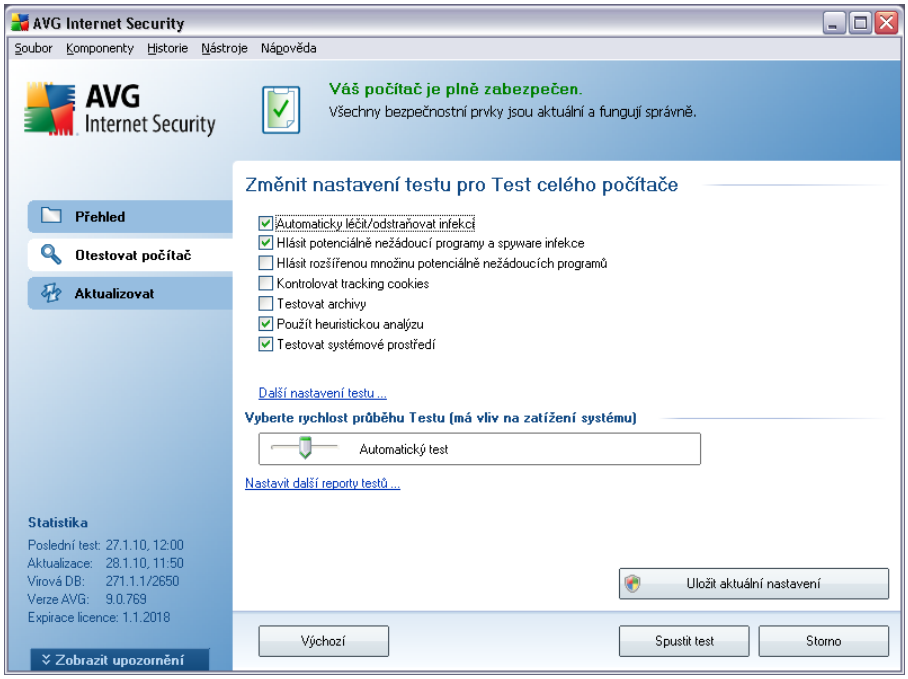
Spuštění testu

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***.



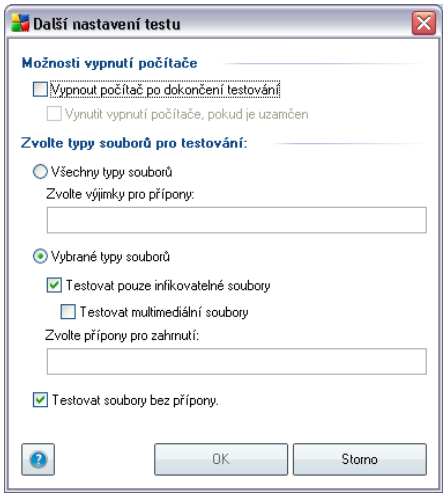
Editace nastavení testu

Předem 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 důvod konfiguraci testu měnit, doporučujeme se podržet výrobcem definovaného nastavení!***



- ***Parametry testu*** - v seznamu parametrů testu můžete jednotlivé volby podle potřeby vypínat/zapínat. Ve výchozím nastavení je většina parametrů zapnuta a budou tak během testu automaticky použity.

- ***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 souborů pro testování*** - dále se můžete rozhodnout, zda si přejete testovat

  - ***Všechny typy souborů*** - přičemž máte zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou;

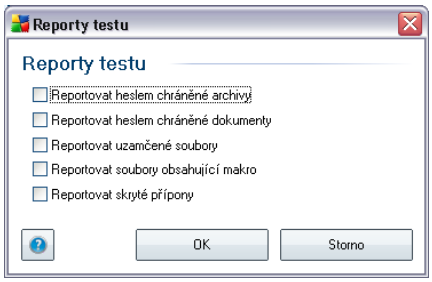
  - ***Vybrané typy souborů*** - můžete se rozhodnout, že chcete, aby se testy spouštěly pouze nad soubory, které lze považovat za infikovatelné (*soubory, které nemohou být infekcí zasaženy, se testovat nebudou - například prosté textové soubory nebo některé nespustitelné soubory*), a to včetně multimediálních souborů (*video, audio soubory - ponecháte-li tuto položku 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 rozhodněte, zda se mají testovat i soubory se skrytou či neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme , abyste se tohoto nastavení podrželi, pokud nemáte skutečný důvod jej měnit. Soubory bez přípon jsou obecně vysoce podezřelé a měly by být otestovány.

- ***Priorita testu*** - posuvníkem lze změnit prioritu testu, která je ve výchozím nastavení na střední hodnotě. Střední (automatická) hodnota nastavení optimalizuje rychlost testu počítače a vytížení 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 testů*** - odkaz otevírá nový dialog ***Reporty testů***, 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.*

12.2.2. Test vybraných souborů či složek

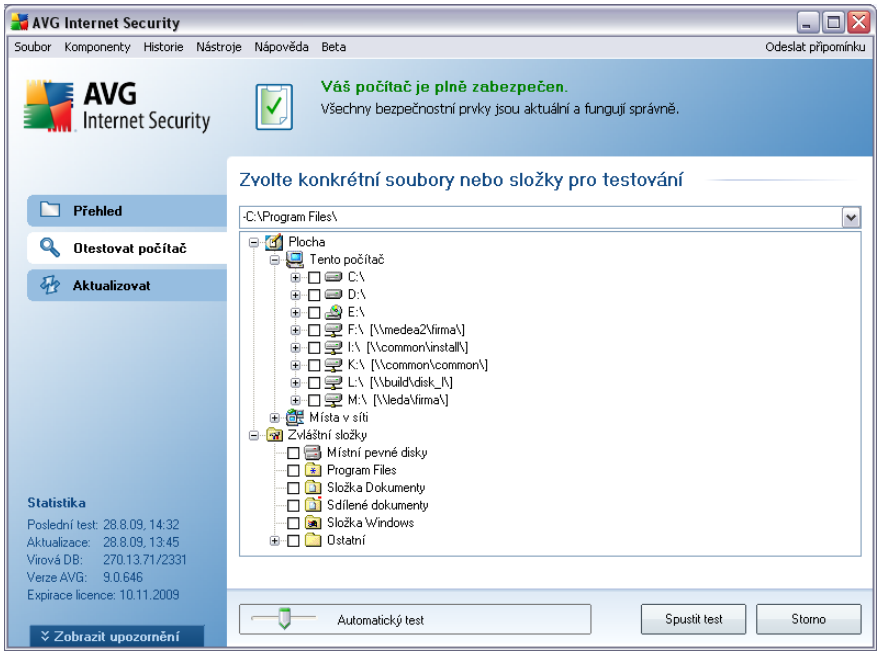
Test vybraných souborů či složek kontroluje pouze uživatelem definované oblasti počítače (zvolené složky, pevné disky, diskety, CD, optické disky, …). Postup při nálezu a léčbě/odstraňování virové nákazy je stejný jako u ***Testu celého počítače***: nalezené viry jsou vyléčeny nebo přesunuty do Virového trezoru. ***Test vybraných souborů či složek*** můžete s výhodou použít pro nastavení vlastních testů, jejichž spouštění nastavíte podle vašich potřeb.

Spuštění testu

Test vybraných souborů či složek spusťte přímo z rozhraní pro testování kliknutím na graficky znázorněnou položku ***Test vybraných souborů či 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.

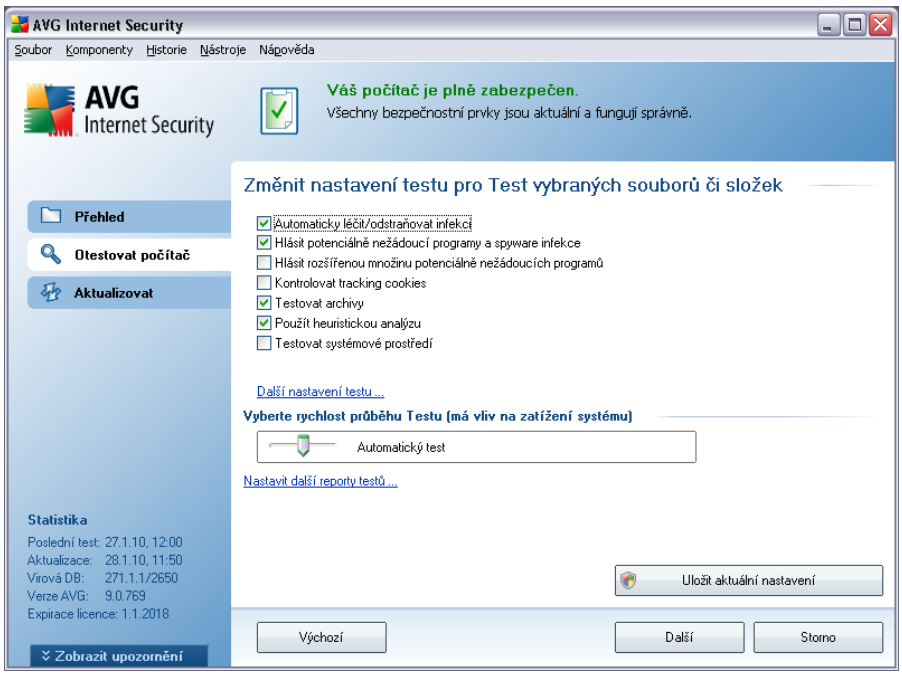
Pokud si přejete zkontrolovat určitý adresář bez kontroly všech v něm obsažených podadresářů, napište před automaticky vygenerovanou cestu k adresáři znaménko "**-**". Parametrem "!" před cestou k adresáři zase určíte, že celý adresář má být z testu vypuštěn.

Samotný test pak spustíte stiskem tlačítka ***Spustit test*** a jeho průběh je identický s průběhem testu celého počítače.



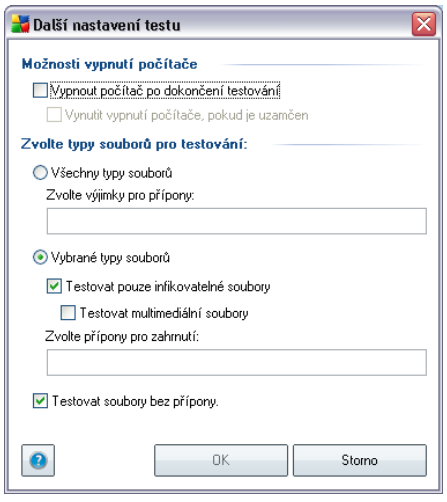
Editace nastavení testu

Předem definované výchozí nastavení ***Testu vybraných souborů či složek*** máte možnost editovat v dialogu ***Změnit nastavení testu pro Test vybraných souborů či složek*** *(dostupného z rozhraní pro testování prostřednictvím odkazu Změnit nastavení testu u Testu vybraných souborů a složek).* ***Pokud však nemáte skutečný důvod konfiguraci testu měnit, doporučujeme se podržet výrobcem definovaného nastavení!***



- ***Parametry testu*** - v seznamu parametrů testu můžete jednotlivé volby podle potřeby vypínat/zapínat (*podrobný popis tohoto nastavení najdete v kapitole Pokročilé nastavení AVG / Testy / Test vybraných souborů či složek*).

- ***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 souborů pro testování*** - dále se můžete rozhodnout, zda si přejete testovat

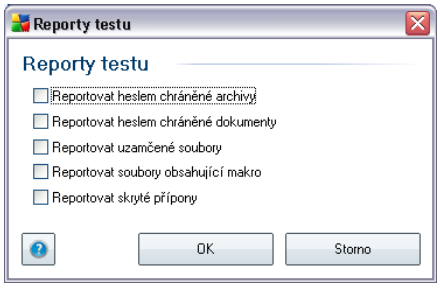
  - ***Všechny typy souborů*** - přičemž máte zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou;

  - ***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 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 rozhodněte, zda se mají testovat i soubory se skrytou či neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme , abyste se tohoto nastavení podrželi, pokud nemáte skutečný důvod jej měnit. Soubory bez přípon jsou obecně vysoce podezřelé a měly by být otestovány.

- ***Priorita testu*** - posuvníkem lze změnit prioritu testu, která je ve výchozím nastavení na střední hodnotě. Střední (*automatická*) hodnota nastavení optimalizuje rychlost testu počítače a vytížení 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 testů*** - odkaz otevírá nový dialog ***Reporty testů***, v němž můžete označit, které typy nálezů mají být hlášeny:



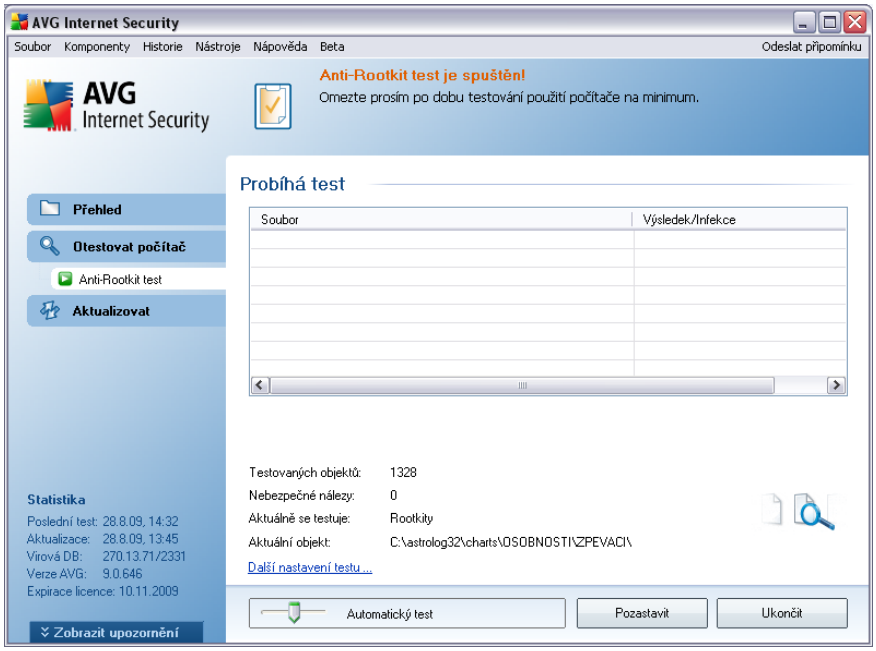
Upozornění: *Samotné možnosti nastavení testu jsou shodné s parametry nově definovaného testu, které jsou podrobně popsány v kapitole* ***AVG testování / Naplánování testu / Jak testovat****. Pokud se rozhodnete výchozí nastavení* ***Testu vybraných souborů či složek*** *změnit, můžete pak svou konfiguraci 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 či složek).*

12.2.3. Anti-Rootkit test

Anti-Rootkit test prohledává počítač na přítomnost rootkitů (*programů a technologií, které dokáží maskovat přítomnost malware v počítači*). Dojde-li k nálezu rootkitu, nemusí to nutně znamenat, že je počítač infikovaný. V některých případech mohou být rootkity použity jako ovladače nebo části korektních aplikací.

Spuštění testu

Anti-Rootkit test spusťte přímo z rozhraní pro testování kliknutím na graficky znázorněnou položku ***Anti-Rootkit test***. 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***.

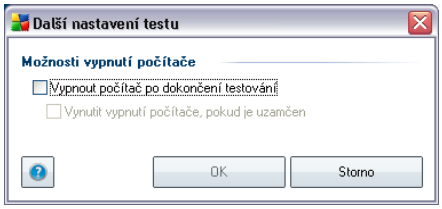


Editace nastavení testu

Anti-Rootkit test se spouští vždy ve výchozím nastavení a editace testu je dostupná pouze v ***Pokročilém nastavení AVG / Anti-Rootkit***. V rozhraní pro testování jsou dostupná jen tato nastavení, a to výhradně v průběhu testu:

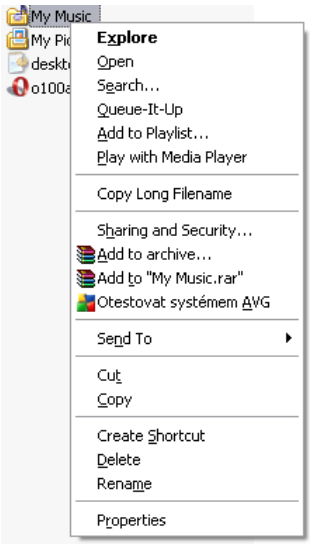
- ***Automatický test*** - posuvníkem lze změnit prioritu testu, která je ve výchozím nastavení na střední hodnotě. Střední (*automatická*) hodnota nastavení optimalizuje rychlost testu počítače a vytížení systémových zdrojů. Test můžete spustit pomaleji a tedy s nižší zátěží systémových zdrojů (*vhodné, 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*).

- ***Další nastavení testu*** - odkaz otevírá nový dialog ***Další nastavení testu***, v němž můžete definovat, má-li v souvislosti s ***Anti-Rootkit testem*** dojít k vypnutí počítače (***Vypnout počítač po dokončení testování***, *respektive* ***Vynutit vypnutí počítače, pokud je uzamčen***):



12.3. Testování v průzkumníku Windows

AVG 9 Anti Virus plus Firewall nabízí kromě přednastavených testů spouštěných 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

12.4. Testování z příkazové řádky

V rámci **AVG 9 Anti Virus plus Firewall** existuje také možnost spustit test z příkazové řádky. Tuto možnost využijete například na serverech nebo třeba při vytváření dávkových skriptů, které mají být spouštěny po startu počítače. Z příkazové řádky můžete spustit test s nastavením většiny parametrů, které jsou dostupné v grafickém rozhraní AVG.

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

- ***avgscanx*** na 32-bitových OS
- ***avgscana*** na 64-bitových OS

Syntaxe příkazu

Syntaxe příkazu pro spuštění testu z příkazové řádky je následující:

- ***avgscanx /parametr*** ... tedy například ***avgscanx /comp*** pro spuštění testu celého počítače
- ***avgscanx /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: ***avgscanx /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, příp. /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.

12.4.1. Parametry CMD testu

V následujícím přehledu nabízíme seznam dostupných parametrů testu:

- ***/SCAN*** Test vybraných souborů či 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

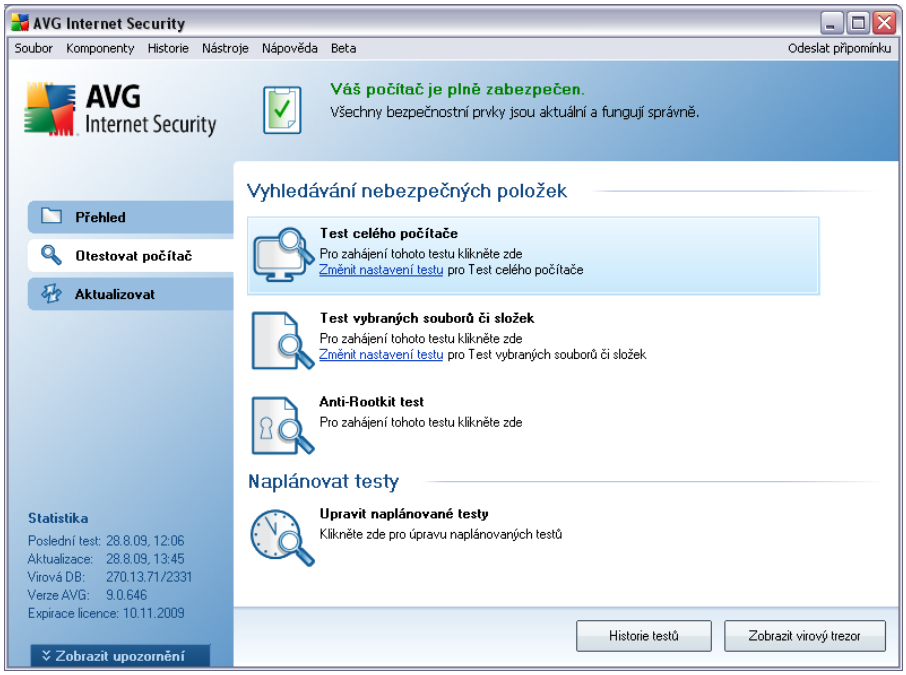
- ***/PUP*** Hlásit "Potenciálně nebezpečné programy"
- ***/REG*** Testovat registry
- ***/COO*** Testovat cookies
- ***/?*** Zobrazit nápovědu k tomuto tématu
- ***/HELP*** Zobrazit nápovědu k tomuto tématu
- ***/PRIORITY*** Nastavit prioritu testu /Low, Auto, High/ (viz ***Pokročilé nastavení / Testy***)
- ***/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

12.5. Naplánování testu

Testy v **AVG 9 Anti Virus plus Firewall** lze spouštět buďto na vyžádání (*například v situaci, kdy máte podezření na zavlečení infekce na váš počítač nebo z jiného důvodu*) anebo podle nastaveného plánu. Doporučujeme používat především spouštění testů podle plánu, protože tímto přístupem zajistíte svému počítači dostatečnou prevenci a budete moci pracovat bez starostí o to, zda a kdy test spustit.

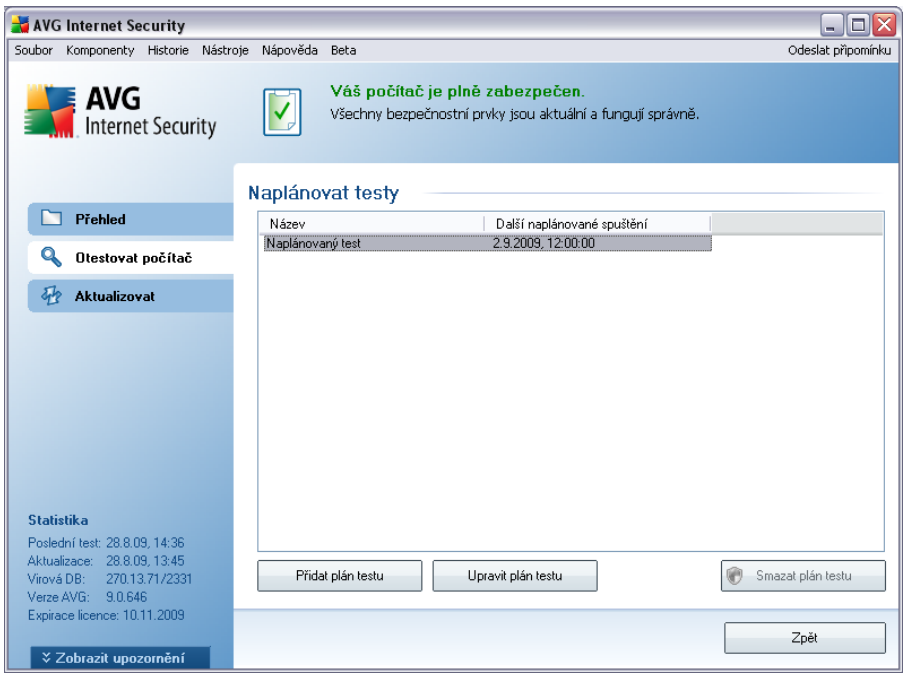
Test celého počítače by měl být spouštěn pravidelně, a to nejméně jednou týdně. Pokud vám to však provoz na vašem počítači umožňuje, doporučujeme spouštět test celého počítače jednou denně; tak je také ve výchozí konfiguraci nastaven plán testů. Jestliže je počítač trvale zapnutý, je vhodné naplánovat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

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*** otevřete nový dialog ***Naplánovat testy***, v němž najdete přehled všech aktuálně naplánovaných testů:



Pracovat můžete s těmito ovládacími tlačítky:

- ***Přidat plán testu*** - tlačítkem otevřete dialog ***Nastavení pro naplánovaný test***, na záložce ***Nastavení plánu***. V tomto dialogu máte možnost specifikovat parametry nově definovaného testu.

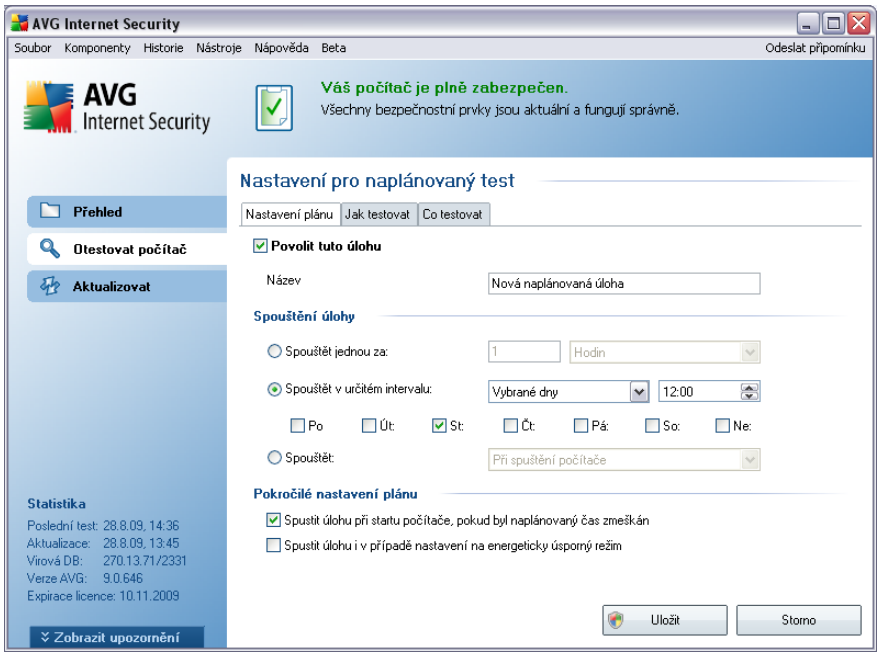
- ***Upravit plán testu*** - tlačítko může být použito pouze v případě, že jste ze seznamu naplánovaných testů vybrali již existující test. V takovém případě se tlačítko zobrazí jako aktivní a kliknutím na něj se přepnete do dialogu ***Nastavení pro naplánovaný test***, na záložku ***Nastavení plánu***. 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 může 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

12.5.1. Nastavení plánu

Chcete-li naplánovat nový test a jeho pravidelné spouštění, vstupte do dialogu ***Nastavení pro naplánovaný test*** (*kliknutím na tlačítko* ***Přidat plán testu*** *v dialogu* ***Naplánování testu***). Dialog je rozdělen do tří záložek: ***Nastavení plánu*** - *viz obrázek* (*výchozí záložka, na kterou budete automaticky přesměrováni*), ***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 současně výstižné názvy testů, abyste později snadno rozeznali, o jaký test se jedná.

Příklad: *Nevhodným názvem testu je například "Nový test" nebo "Martinův 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 - vámi nastavený test bude vždy specifickým nastavením testu vybraných souborů a složek.*

V tomto dialogu můžete dále definovat tyto parametry testu:

- ***Spouštění úlohy*** - určete, v jakých časových intervalech má být nově naplánovaný test spouštěn. Časové určení můžete zadat buďto opakovaným spuštěním testu po uplynutí určené doby (***Spouštět jednou za***) nebo stanovením přesného data a času (***Spouštět v určený čas***), případně určením události, na niž se spuštění testu váže (***Spouštět při spuštění počítače***).

- ***Pokročilé nastavení plánu*** - tato sekce umožňuje definovat podmínky, kdy má či nemá být test spuštěn, jestliže je počítač v úsporném režimu nebo zcela vypnutý a naplánovaný test spuštění testu byl zmeškán.

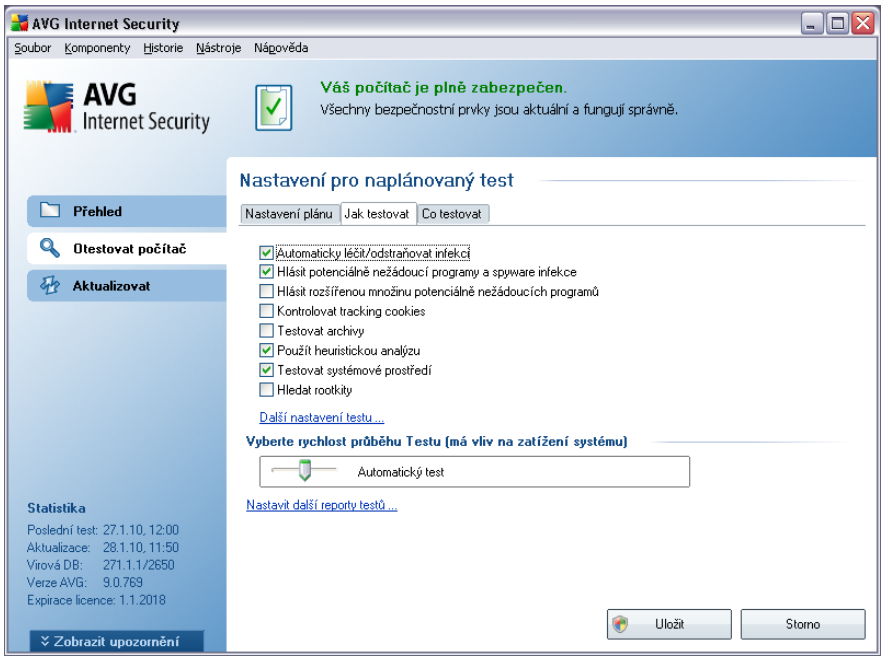
Ovládací tlačítka dialogu

Ze všech tří záložek dialogu ***Nastavení pro naplánovaný test*** (***Nastavení plánu***, ***Jak testovat*** a ***Co testovat***) jsou dostupná dvě ovládací tlačítka, jež mají stejnou funkčnost 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.

12.5.2. 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 měnit, doporučujeme se podržet 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 malware, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány vědomě 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 původní 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*);

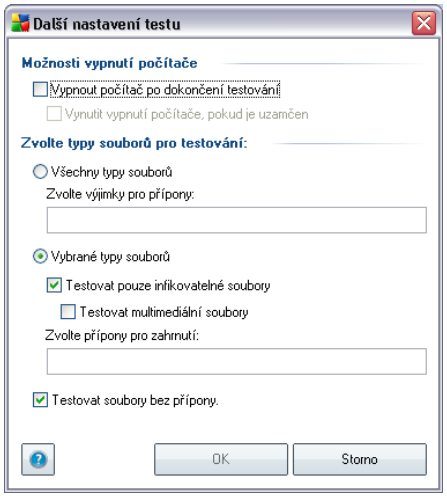
- ***Testovat archivy*** - (*ve výchozím nastavení vypnuto*): parametr definuje, že test má kontrolovat všechny soubory, a to i takové, které jsou zabaleny v některém typu archivu, například ZIP, RAR, ...

- ***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 prověří i systémové oblasti vašeho počítače;

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 souborů pro testování*** - dále se můžete rozhodnout, zda si přejete testovat

    - ***Všechny typy souborů*** - přičemž máte zároveň možnost vyjmout z

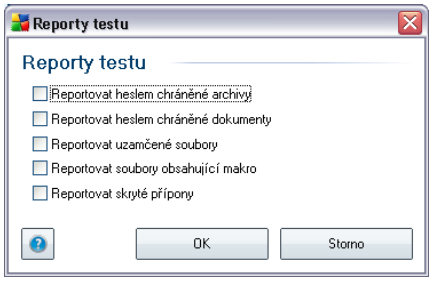
testování soubory definované seznamem přípon oddělených čárkou;

- ***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 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 rozhodněte, zda se mají testovat i soubory se skrytou či neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme , abyste se tohoto nastavení podrželi, pokud nemáte skutečný důvod jej měnit. Soubory bez přípon jsou obecně vysoce podezřelé a měly by být otestovány.

- ***Priorita testu*** - posuvníkem lze změnit prioritu testu, která je ve výchozím nastavení na střední hodnotě. Střední (automatická) hodnota nastavení optimalizuje rychlost testu počítače a vytížení 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 testů*** - odkaz otevírá nový dialog ***Reporty testů***, v němž můžete označit, které typy nálezů mají být hlášeny:



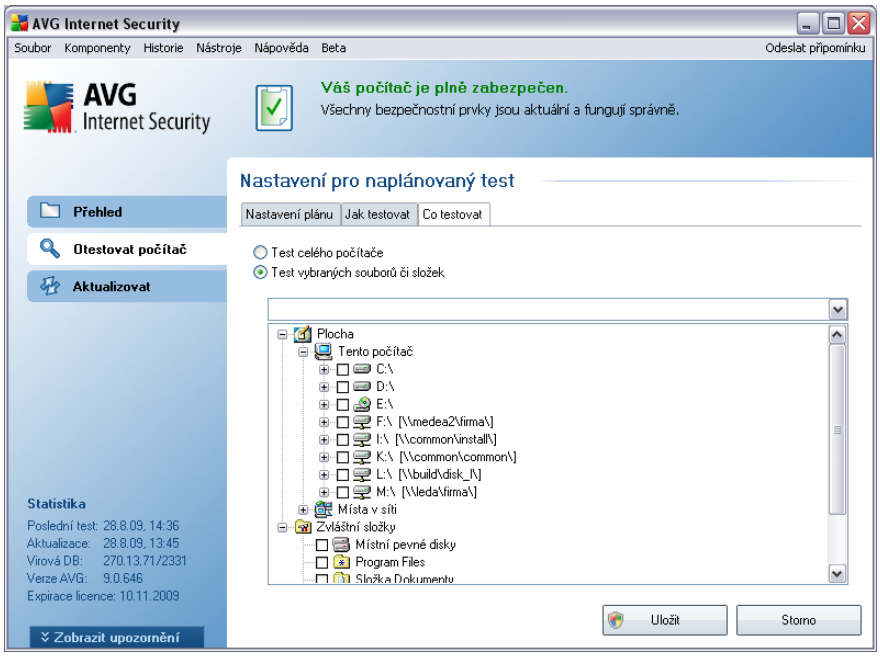
Ovládací tlačítka dialogu

Ze všech tří záložek dialogu ***Nastavení pro naplánovaný test*** (***Nastavení plánu***, ***Jak testovat*** a ***Co testovat***) jsou dostupná dvě ovládací tlačítka, jež mají stejnou funkčnost 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](#).

12.5.3. Co testovat



Na záložce ***Co testovat*** definujte, 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 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 zaškrtávacích políček. Zvolené adresáře se následně zobrazí v textovém poli v horní části dialogového okna a pomocí rozbalovací nabídky se můžete vracet k seznamu vašich předchozích výběrů. Existuje i druhá alternativa: můžete zadat cestu ke konkrétnímu adresáři přímo do textového pole ručně (*zadáte-li více cest současně, oddělte je středníkem bez mezer*).

V zobrazené stromové struktuře je zahrnuta také větev s 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*** - C:\Program Files\
- ***Složka Dokumenty***
    - *pro Win XP:* C:\Documents and Settings\Default User\My Documents\

- *pro Windows Vista/7*: C:\Users\user\Documents\

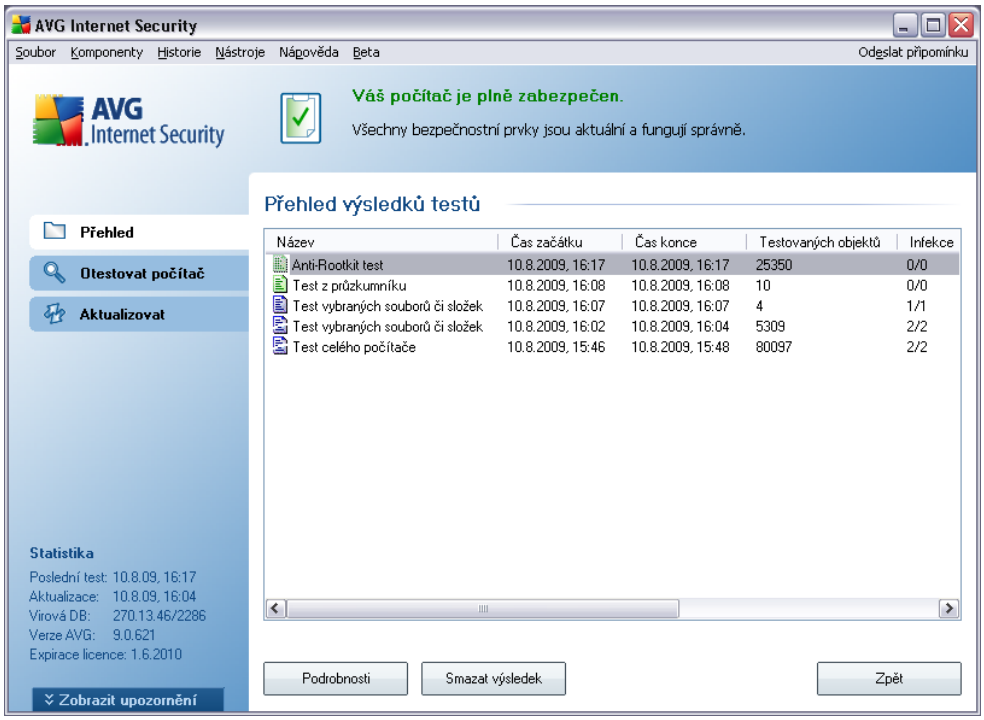
- ***Sdílené dokumenty***
  - *pro Win XP:* C:\Documents and Settings\All Users\Documents\
  - *pro Windows Vista/7*: C:\Users\Public\Documents\
- ***Složka Windows*** - C:\Windows\
- ***Ostatní***
  - *Systémový disk* - pevný disk, na němž je instalován operační systém (*obvykle C:*)
  - *Systémová složka* - Windows/System32
  - *Složka dočasných souborů* - Documents and Settings/User/Local Settings/Temp (*Windows XP*) nebo C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)
  - *Temporary Internet Files* - 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 funkčnost 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.

12.6. 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 přepůlená - celá ikona značí, že test proběhl celý a byl řádně ukončen, přepůlená ikona identifikuje nedokončený nebo přerušený test.

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

- ***Čas začátku*** - datum a přesný čas spuštění testu
- ***Čas konce*** - datum a přesný čas ukončení testu
- ***Testovaných objektů*** - 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 řádném či předčasném ukončení

Ovládací tlačítka dialogu

Ovládacími tlačítky pro dialog ***Přehled výsledků testů*** 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 y přehledu testů odstranit
- ***Zpět*** - přepíná zpět do výchozího dialogu testovacího rozhraní

12.7. Detail výsledku testu

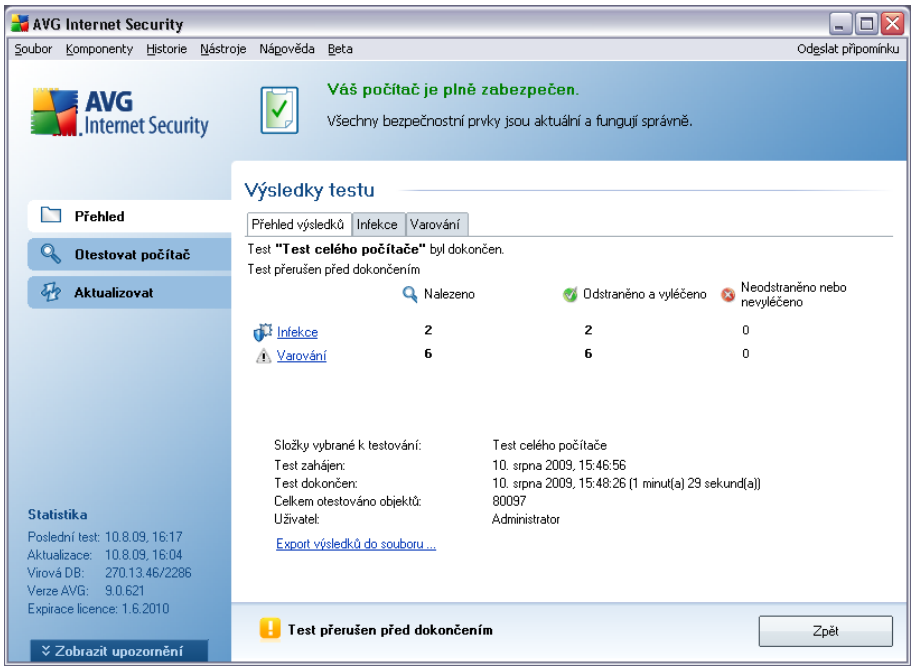
Jestliže v dialogu ***Přehled výsledků testů*** vyberete jeden test ze seznamu a označíte jej, můžete stiskem tlačítka ***Podrobnosti*** přejít do dialogu ***Výsledky testů***, v němž jsou zobrazeny detailní informace o průběhu a výsledku zvoleného testu.

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 podmínečně tehdy, když byla během testu detekována virová infekce
- ***Spyware*** - záložka se zobrazuje podmínečně tehdy, když byl během testu detekován spyware
- ***Varování*** - záložka se zobrazuje podmínečně s upozorněním na výskyt cookies
- ***Informace*** - záložka se zobrazuje podmínečně a zobrazuje informace (*typicky varovná upozornění*) o nálezech, 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).

12.7.1. Záložka Přehled výsledků



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

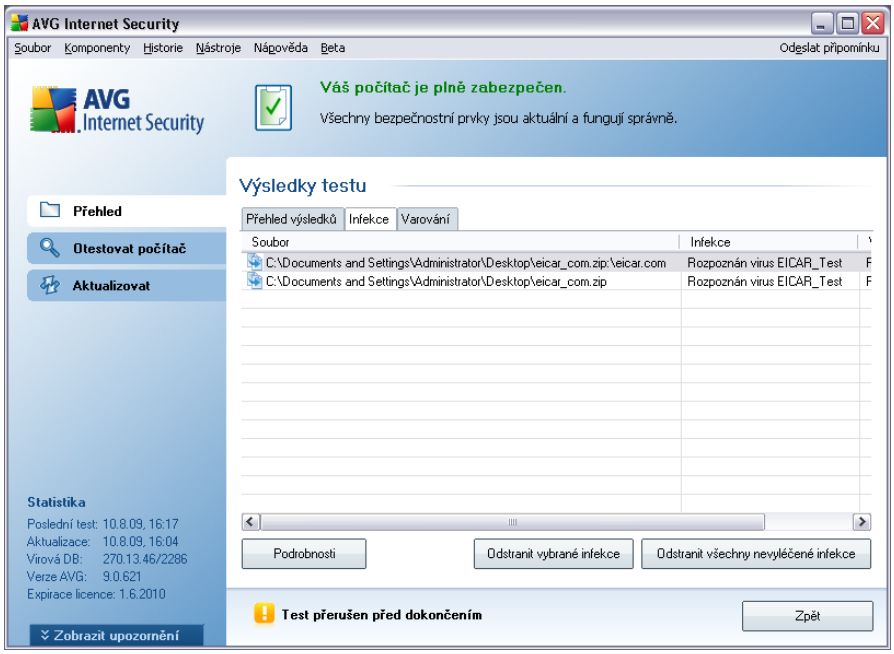
- detekovaných virových infekcích / spyware
- vyléčených virových infekcích / spyware
- počtu virových infekcích / spyware, které se nepodařilo odstranit nebo vyléčit

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

Ovládací tlačítka dialogu

V dialogu je dostupné jediné ovládací tlačítko ***Zpět***, kterým se vrátíte do dialogu ***Přehled výsledků testů***.

12.7.2. Záložka Infekce



Záložka ***Infekce*** se v dialogu ***Výsledky testu*** zobrazuje podmínečně v případě, že během testu byla detekována virová infekce. Záložka je rozdělena do tří sekcí a uvádí následující informace:

- ***Soubor*** - plná adresa původního 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 původním umístění (*například pokud máte v nastavení konkrétního testu vypnutou možnost automatického léčení*)
    - ***Vyléčeno*** - infikovaný objekt byl automaticky vyléčen a ponechán ve svém původním 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 původního umístění

- ***Přidáno k výjimkám PUP*** - nález byl vyhodnocen jako výjimka a připojen k seznamu výjimek PUP (*výjimky lze editovat v dialogu* ***PUP výjimky*** *pokročilého nastavení*)

- ***Zamčený soubor - neotestován*** - objekt je zamčený a nebylo možno jej otestovat

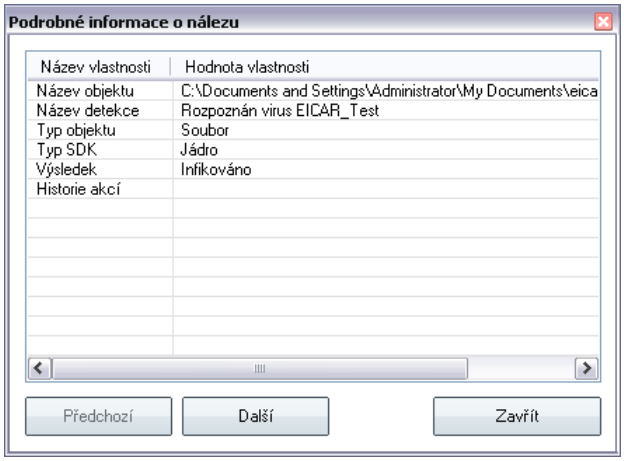
- ***Potenciálně nebezpečný objekt*** - objekt je detekován jako potenciálně nebezpečný, ale nikoli infikovaný (*může například obsahovat makra*). Informace má tedy pouze charakter upozornění.

- ***Pro dokončení akce je potřeba 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 nálezu***:



  V tomto dialogu najdete detailní informace 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.

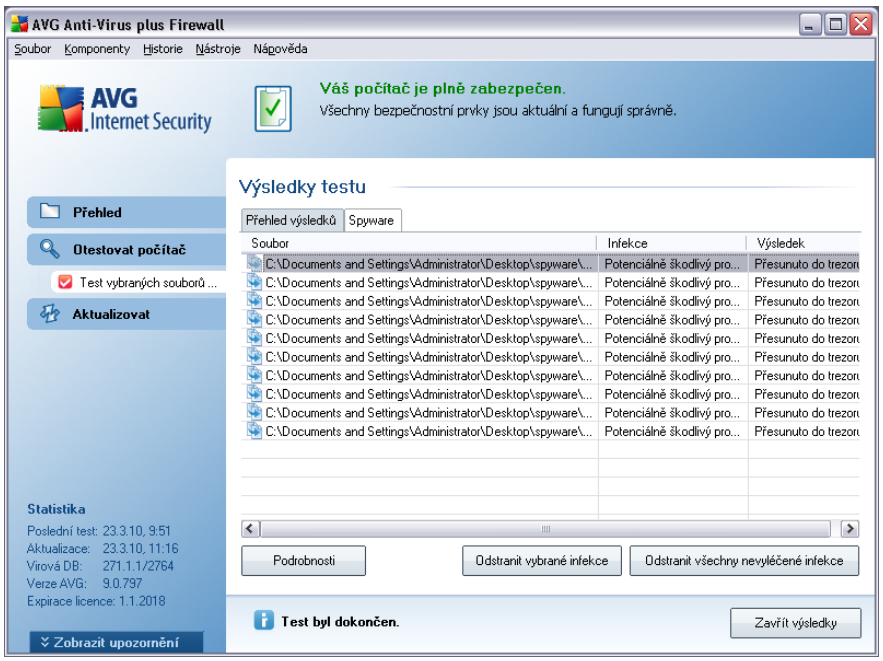
- ***Odstranit vybrané infekce*** - tlačítkem přesunete v seznamu označený nález do ***Virového trezoru***

- ***Odstranit všechny nevyléčené infekce*** - tlačítko odstraní všechny nálezy, které nelze léčit ani nemohou být přesunuty do ***Virového trezoru***

- ***Zavřít výsledky*** - zavírá detail výsledku testu a přepíná zpět do dialogu

[Přehled výsledků testů](#)

12.7.3. Záložka Spyware



Záložka ***Spyware*** se v dialogu ***Výsledky testu*** zobrazuje podmínečně v případě, že během testu byl detekován spyware. Záložka je rozdělena do tří sekcí a uvádí následující informace:

- ***Soubor*** - plná adresa původního 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 původním umístění (například pokud máte v nastavení konkrétního testu vypnutou možnost automatického léčení)
    - ***Vyléčeno*** - infikovaný objekt byl automaticky vyléčen a ponechán ve svém původním 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 původního

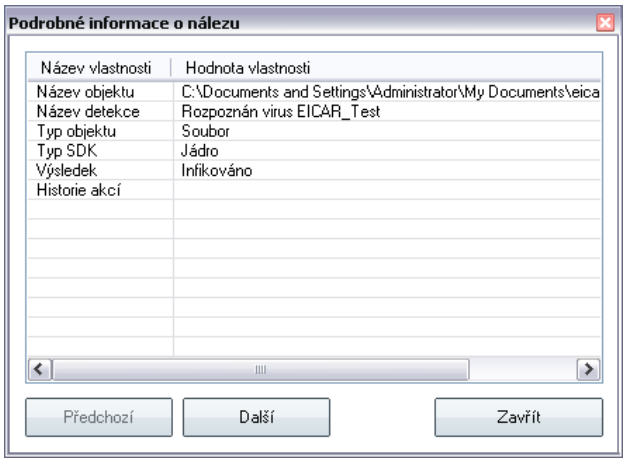
umístění

- **Přidáno k výjimkám PUP** - nález byl vyhodnocen jako výjimka a připojen k seznamu výjimek PUP (*výjimky lze editovat v dialogu* ***PUP výjimky*** *pokročilého nastavení*)
- **Zamčený soubor** - neotestován - objekt je zamčený 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 potřeba 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 nálezu***:



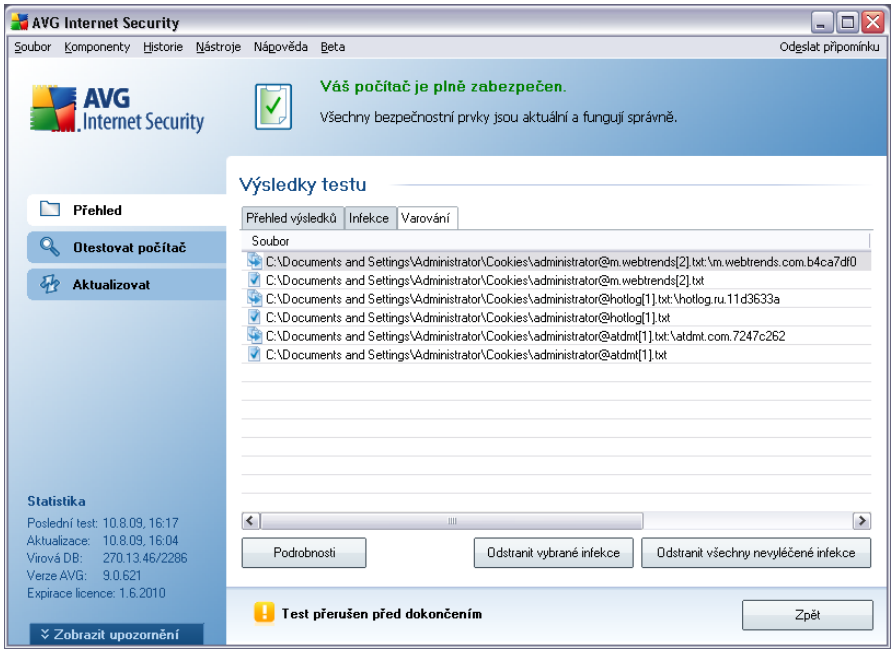
V tomto dialogu najdete informaci o infekci (*například umístění a jméno detekovaného infikovaného objektu, typ objektu, typ SDK, výsledek detekce a historii akcí provedených nad detekovaným objektem*). Pomocí tlačítek ***Předchozí*** / ***Následující*** můžete postupně zobrazovat informace o jednotlivých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

- ***Odstranit vybrané infekce*** - tlačítkem přesunete v seznamu označený nález do ***Virového trezoru***
- ***Odstranit všechny nevyléčené infekce*** - tlačítko odstraní všechny nálezy, které nelze léčit ani nemohou být přesunuty do ***Virového trezoru***

- ***Zavřít výsledky*** - zavírá detail výsledku testu a přepíná zpět do dialogu ***Přehled výsledků testů***

12.7.4. Záložka Varování

Záložka ***Varování*** zobrazuje informace o "podezřelých" objektech (*nejčastěji 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 přímou 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 nejběžnějších takto detekovaných objektů:

- ***Skryté soubory*** nejsou ve výchozím nastavení Windows viditelné. Některé viry nebo jiné hrozby se mohou vyhýbat svému odhaleni 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, předvyplnění uživatelského jména, atd.

- ***Podezřelé registrové 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.

12.7.5. Záložka Rootkity

Záložka ***Rootkity*** se objeví ve výsledcích testu pouze v případě, že jste spustili ***Anti-Rootkit test***.

Rootkit je program speciálně vytvořený tak, aby dokázal převzít kontrolu nad vaším počítačem, aniž by požádal o jakoukoliv autorizaci. Většinou se nepokouší ovládnout hardware, jejich cílem je ovládnout vás 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 světě škodlivého kódu poměrně výsadní postavení, jelikož pronikají hluboko do systému, přebírají požadavky systémových volání a správné výsledky nahrazují svými vlastními.

Struktura této záložky je identická se strukturou záložek ***Infekce*** nebo ***Spyware***.

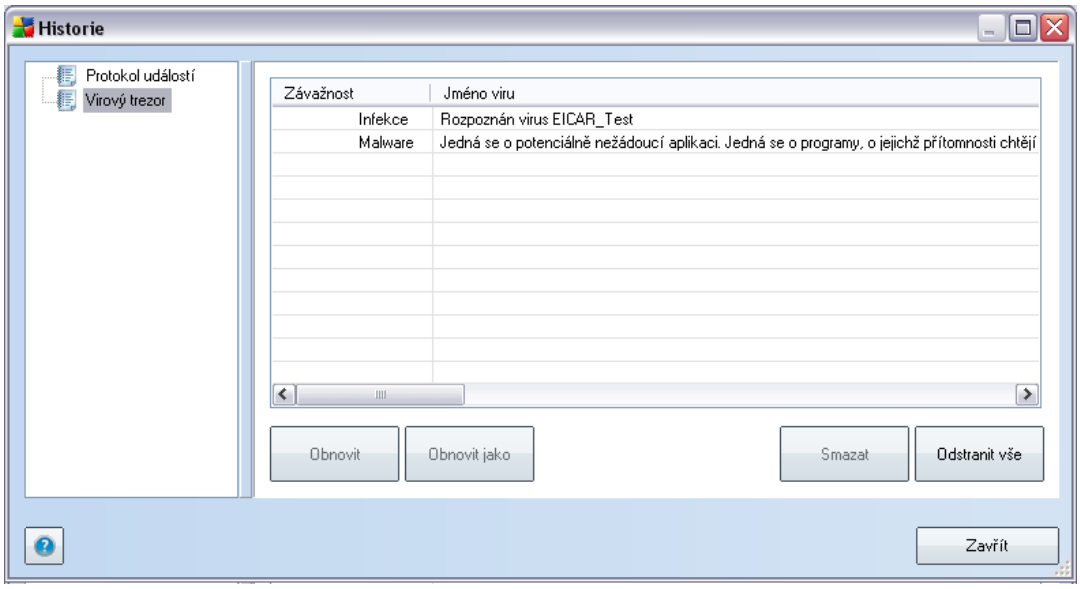
12.7.6. Záložka Informace

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 časté 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 přípona***: Soubory se skrytou příponou mohou představovat např. obrázek, ale také mohou být spustitelné (*např. obrazek.jpg.exe*). Druhá přípona 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 (*např. 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.
- ***Zamčený soubor***: Reportovaný soubor je zamčený, a tedy nemohl být otestován programem AVG. Tato informace ve výsledku testů znamená, že soubor je permanentně používán systémem (*např. stránkovací soubor*).

12.8. Virový trezor



Virový trezor je bezpečným prostředím pro správu podezřelých/infikovaných objektů nalezených během testů 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 příslušný 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*** - je zde uvedena informace o typu nálezu (*rozlišuje typy nálezů podle úrovně jejich infekčnosti - objekty mohou být pozitivně/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
- ***Původní název objektu*** - všechny detekované objekty v tabulce jsou uvedeny pod standardním jménem, kterým byly označeny během detekce při testování. Pokud měl detekovaný objekt své původní 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 původního umístění
- ***Obnovit jako*** - pokud se rozhodnete detekovanou infekci z ***Virového trezoru*** umístit do zvolené složky, použijte toto tlačítko. Podezřelý a detekovaný objekt bude uložen pod svým původním jménem, a pokud toto není známo, bude uložen pod standardním jménem, kterým byl označen při detekci.
- ***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).

13. Aktualizace AVG

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

V průběhu instalačního procesu AVG jste byli v dialogu ***Nastavení pravidelných aktualizací a testů*** dotázáni na na frekvenci kontroly nových aktualizací. Dostupnými možnostmi volby jsou ***Každé 4 hodiny*** a ***Jednou denně***. Vzhledem k tomu že aktualizace nejsou vydávány podle pevného plánu, ale v reakci na počet a závažnost nových hrozeb, dopručujeme kontrolovat aktualizace alespoň jednou denně. Kontrola každé 4 hodiny zajistí, že Váš **AVG 9 Anti Virus plus Firewall** bude aktuální během celého dne.

13.1. 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 souběhu naplánované programové aktualizace a naplánovaného testu, proces aktualizace je považován za prioritní a test bude přerušen.*

13.2. 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.

13.3. Průběh aktualizace

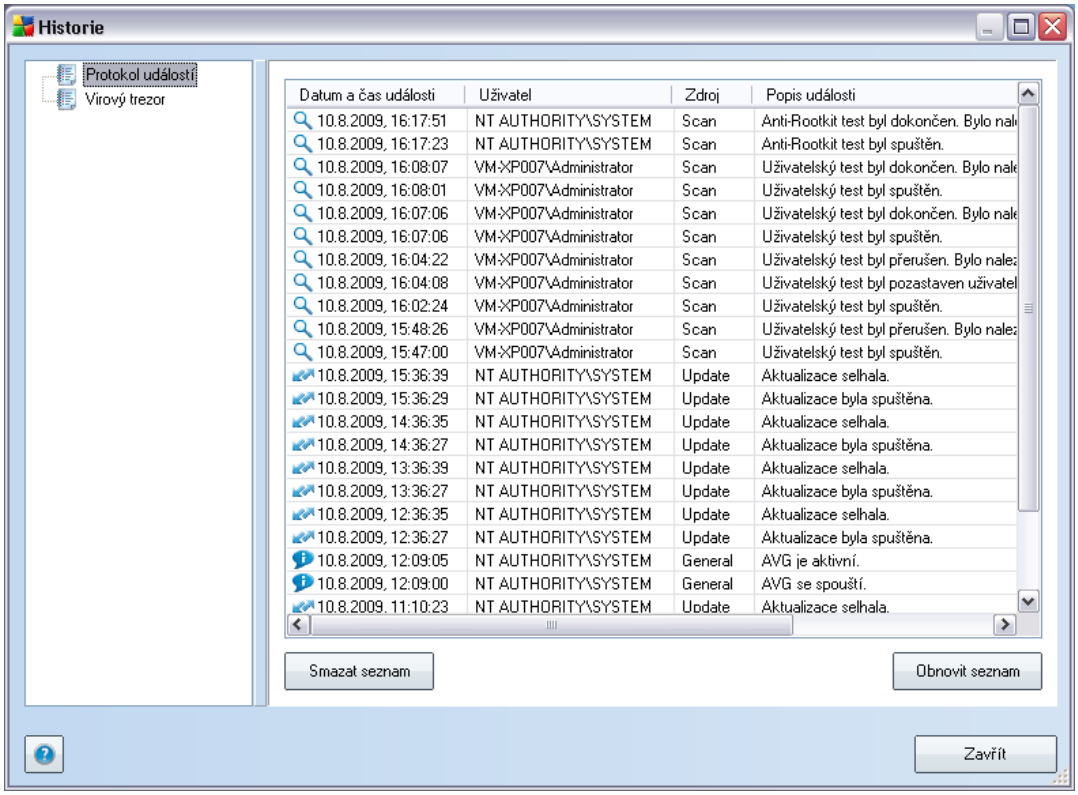
Proces aktualizace můžete spustit podle potřeby okamžitě zkratkovými tlačítkem ***Aktualizovat***. Toto tlačítko je vždy dostupné z kteréhokoliv dialogu uživatelského rozhraní AVG. V každém případě však doporučujeme provádět aktualizace i v předem určených termínech podle plánu nastaveného v Manažeru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

Po spuštění aktualizace dojde nejprve k ověření, zda existují nové aktualizační soubory, jež dosud nebyly aplikovány. Pokud ano, AVG zahájí jejich okamžité 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 aktualizačního 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 vás OS obnovit v původní konfiguraci. Tato možnost je dostupná přímo v operačním systému z menu Start / Programy / Příslušenství / Systémové nástroje / Obnova systému. Doporučujeme pouze zkušeným uživatelům!*

14. Protokol událostí



Historie událostí je dostupná volbou položky systémového menu ***Historie/Protokol událostí***. V tomto dialogu najdete přehled všech důležitých událostí, které nastaly v průběhu práce **AVG 9 Anti Virus plus Firewall**. Zaznamenávány jsou události, mezi které patří například:

- informace o aktualizacích programu
- spuštění/ukončení/přerušení testů (včetně testů spouštěných automaticky)
- události týkající se nalezení viru (testováním či Rezidentním štítem) s uvedením konkrétního místa nálezu
- ostatní důležité události

Ovládací tlačítka dialogu

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

15. FAQ a technická podpora

V případě problémů s AVG se pokuste vyhledat řešení na webu AVG (http://www.avg.cz/) v sekci ***FAQ***.

Pokud na svůj dotaz nenajdete uspokojivou odpověď, obraťte se prosím na oddělení technické podpory AVG prostřednictvím kontaktního formuláře dostupného ze systémového menu volbou položky ***Nápověda / Odborná pomoc online***.