AVG File Server 2011

Uživatelský manuál

Verze dokumentace 2011.03 (23. 2. 2011)

Obsah

1. Úvod

Tento uživatelský manuál je kompletní dokumentací programu **AVG File Server 2011**.

Gratulujeme k vaší volbě programu AVG File Server 2011!

AVG File Server 2011 je jedním z produktů nové řady oceňovaného bezpečnostního software AVG, jež byl navržen pro klid vaší duše a stoprocentní bezpečnost vašeho serveru. Stejně jako všechny produkty nové řady AVG byl i **AVG File Server 2011** 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 File Server 2011** přináší moderní grafické rozhraní v kombinaci s agresivnějším a rychlejším testováním. Pro větší pohodlí přináší více procesů v plně automatickém režimu a nabízí nové 'inteligentní' uživatelské možnosti, které se přesně přizpůsobí vašim potřebám.

Produkty AVG nabízejí

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

2. Podmínky instalace AVG

2.1. Podporované operační systémy

AVG File Server 2011 je určen k ochraně stanic s těmito operačními systémy:

- Windows 2003 Server a Windows 2003 Server x64 Edice
- Windows 2008 Server a Windows 2008 Server x64 Edice

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

2.2. Minimální / doporučené HW požadavky

Minimální hardwarové požadavky pro **AVG File Server 2011**:

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

Doporučené hardwarové požadavky pro **AVG File Server 2011**:

- Procesor Intel Pentium 1,8 GHz
- 512 MB RAM paměti
- 600 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.com).

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

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

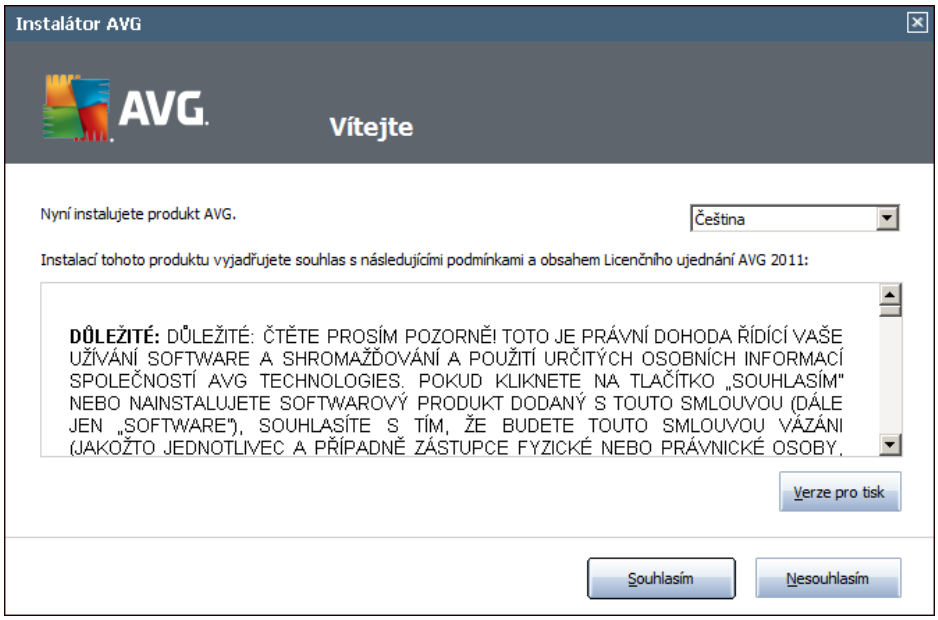
4. Instalační proces AVG

Pro instalaci **AVG File Server 2011** 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.com), sekce ***Centrum podpory / Stáhnout*** a nejnovější instalační soubor si odtud stáhnout.

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

4.1. Vítejte

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



Upozornění: *Zde volíte jazyk instalačního procesu. V tomto jazyce bude instalován program AVG, spolu s angličtinou, která se instaluje automaticky. Pokud si přejete nainstalovat další volitelné jazyky, do nichž budete moci uživatelské rozhraní programu přepínat, můžete je definovat v dialogu* ***Uživatelské volby****.*

Dialog dále obahuje plné znění závazné licenční smlouvy AVG. Text si pečlivě přečtěte a svůj souhlas s licenčním ujednáním potvrďte stiskem tlačítka ***Souhlasím***. Pokud s licenční smlouvou nesouhlasíte a stisknete tlačítko ***Nesouhlasím***, instalace bude okamžitě ukončena.

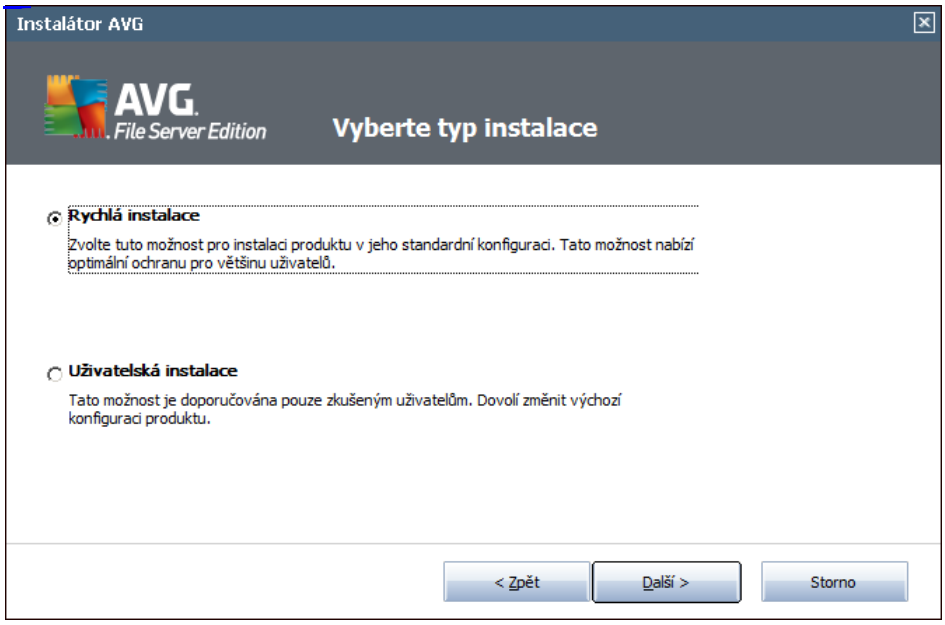
4.2. Aktivujte vaši licenci

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

Licenční číslo najdete buďto na registrační kartě v krabicovém balení **AVG File Server 2011**, anebo v potvrzovacím emailu, který jste obdrželi při zakoupení **AVG File Server 2011** 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***.

4.3. Vyberte typ instalace



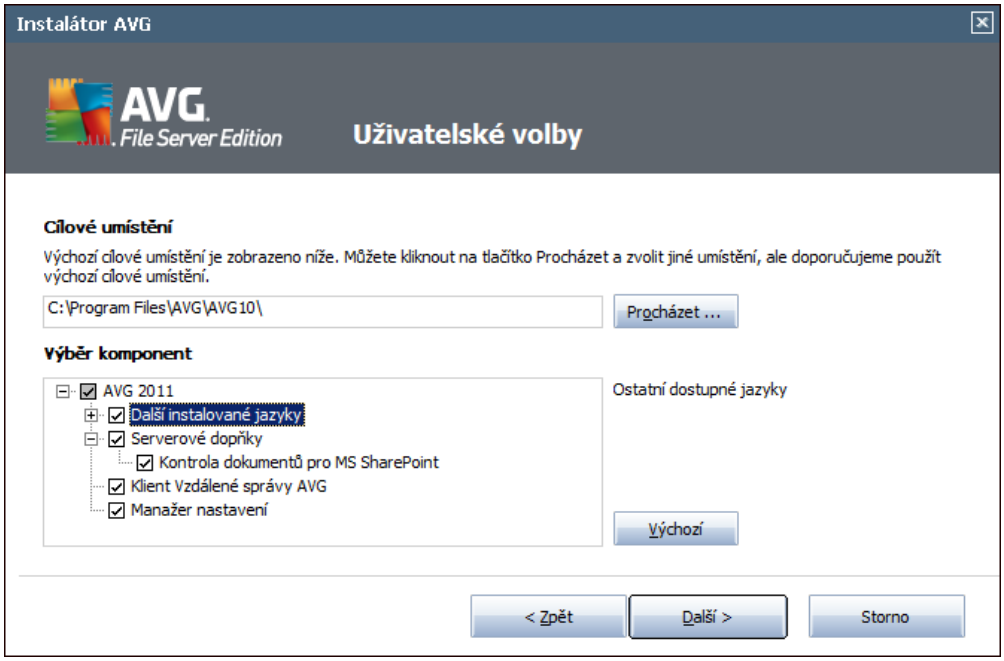
Dialog ***Vyberte typ instalace*** vám dává na výběr mezi ***rychlou*** a ***uživatelskou*** instalací.

Většině uživatelů doporučujeme použít ***rychlou instalaci***, kdy bude AVG nainstalován zcela automaticky s nastavením definovaným výrobcem. Toto nastavení zaručuje maximální úroveň bezpečnosti a optimální využití zdrojů. Pokud se v budoucnu vyskytne potřeba některé konkrétní nastavení změnit, budete mít vždy možnost editovat konfiguraci AVG přímo v aplikaci. Pokud se rozhodnete pro možnost ***rychlé instalace***, stiskem tlačítka ***Další*** postoupíte k dialogu ***Konfigurace ochrany AVG je kompletní***.

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. Jestliže zvolíte tuto možnost, po stisku tlačítka ***Další*** budete přesměrováni k dialogu ***Uživatelské volby***.

4.4. Uživatelské volby

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



Cílové umístění

V sekci ***Cílové umístění*** máte určit, kam má být program **AVG File Server 2011** 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.

Výběr komponent

Sekce ***Výběr komponent*** nabízí přehled komponent **AVG File Server 2011**, 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!

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

- ***Volba jazyka***

V přehledu instalovaných komponent máte v tuto chvíli možnost definovat, v jakém jazyce (*nebo jazycích*) má být AVG instalován. Rozbalte položku ***Další instalované jazyky*** a požadované jazyky vyberte z příslušné nabídky.

- ***Serverové doplňky - Kontrola dokumentů pro MS SharePoint***

Tato komponenta testuje dokumenty uložené v rámci MS SharePoint a chrání před možným nebezpečím. Protože se jedná o klíčovou součást **AVG File Server 2011**, její instalaci důrazně doporučujeme.

- ***Klient vzdálené správy AVG***

Pokud plánujete později zapojit počítač, na němž právě instalujete AVG, do Vzdálené správy AVG, označte prosím ve výběru i tuto položku.

- ***Manažer nastavení***

Správce nastavení AVG je malá aplikace, která vám umožní jednoduše a rychle upravovat nastavení lokálních instalací AVG (a to včetně těch, které nepracují pod Vzdálenou správou). K tomuto účelu slouží konfigurační soubory (ve formátu .pck), které lze s pomocí Správce nastavení AVG snadno vytvořit na každém počítači s nainstalovaným programem AVG. Tyto soubory pak můžete nahrát na libovolné přenosné médium a použít v kterémkoli počítači. Totéž pochopitelně platí i o samotné aplikaci Správce nastavení AVG. Pro podrobnější informace o tomto programu klikněte **zde**.

Pokračujte stiskem tlačítka ***Další***.

4.5. Postup instalace

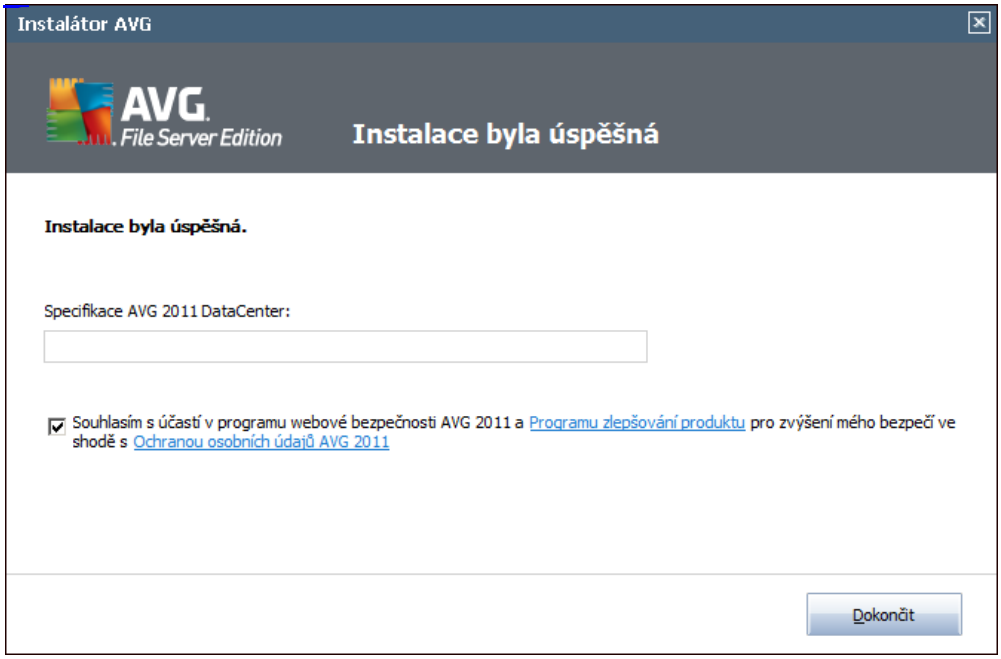
Potvrzením předchozího dialogu dojde ke spuštění samotného procesu instalace, jehož průběh můžete sledovat v dialogu ***Postup instalace***. Tento dialog je pouze informativní a nevyžaduje žádný váš zásah.

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

4.6. Konfigurace ochrany AVG je kompletní

Dialog ***Instalace byla úspěšná*** potvrzuje, že **AVG File Server 2011** byl plně nainstalován a nastaven k optimálnímu výkonu.

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



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

Souhlasím s účastí v programu webové bezpečnosti AVG 2011 a Programu zlepšování produktu ... - označením této volby dáváte najevo svůj souhlas s účastí v Programu zlepšování produktu (*podrobnosti najdete v kapitole Pokročilé nastavení AVG / Program zlepšování produktu*). V rámci tohoto programu probíhá sběr anonymních informací o detekovaných hrozbách s cílem zvýšit celkovou úroveň bezpečnosti na Internetu.

5. Po instalaci

5.1. Registrace produktu

Po dokončení instalace **AVG File Server 2011** prosím zaregistrujte svůj produkt na webu AVG (http://www.avg.com), 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.

5.2. Otevření uživatelského rozhraní

Uživatelské rozhraní AVG je dostupné několika cestami:

- dvojklikem na ***ikonu AVG na systémové liště***
- dvojklikem na ikonu AVG na ploše
- z nabídky ***Start/Všechny programy/AVG 2011/Uživatelské rozhraní AVG***

5.3. Spuštění testu celého počítače

Jelikož existuje jisté riziko, že virus byl na váš počítač zavlečen již před instalací **AVG File Server 2011**, 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***.

5.4. Výchozí konfigurace AVG

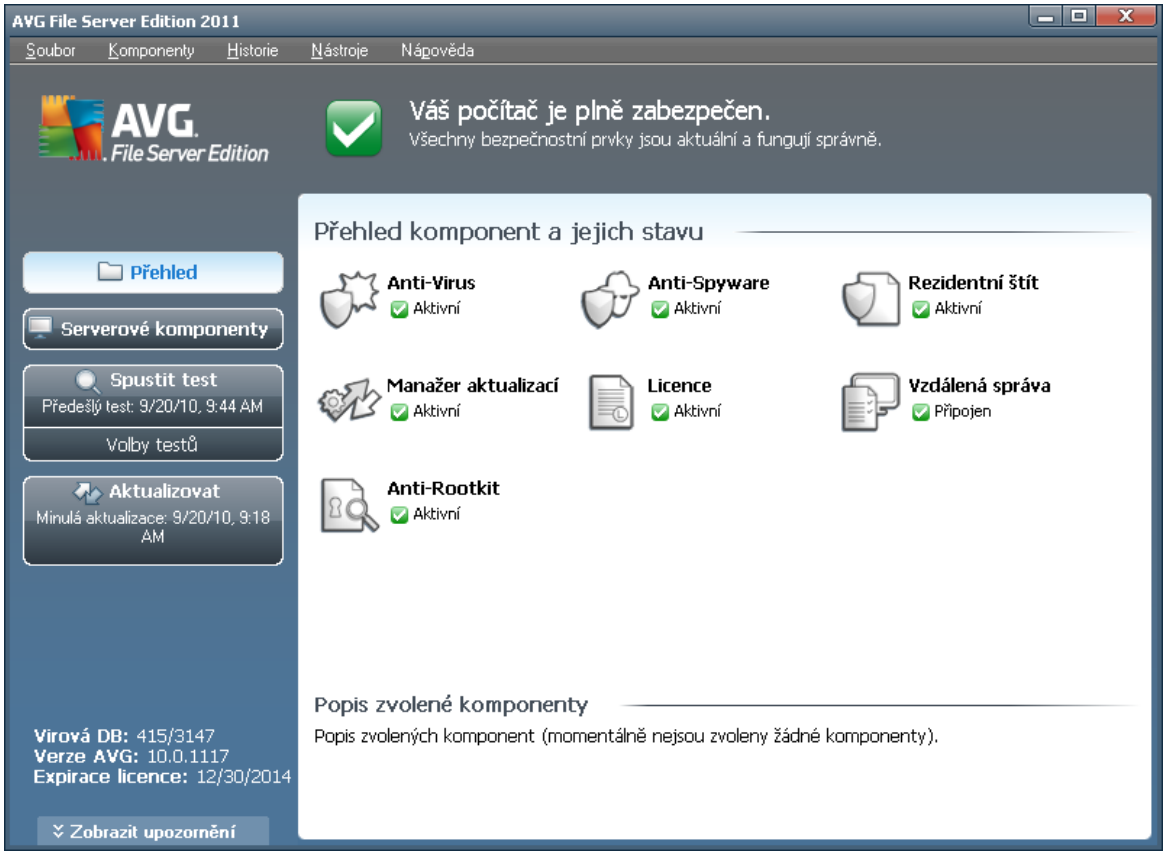
Ve výchozí konfiguraci (*bezprostředně po instalaci AVG File Server 2011*) jsou všechny komponenty a funkce **AVG File Server 2011** nastaveny výrobcem k optimálnímu výkonu bezpečnostního software.

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***.

6. Uživatelské rozhraní AVG

AVG File Server 2011 se otevře v tomto rozhraní:



Hlavní okno je rozděleno do několika sekcí:

- ***Systémové menu*** *(navigace Windows zobrazená zcela nahoře)* je standardní navigací, která umožňuje přístup ke všem komponentám, vlastnostem a službám AVG - podrobnosti >>
- ***Informace o stavu zabezpečení*** *(v horní části okna)* podává základní informaci o aktuálním stavu programu AVG - podrobnosti >>
- ***Zkratková tlačítka*** *(v levé části okna)* 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 >>

6.1. Systémové menu

Systémové menu je standardní navigací používanou ve všech oknech Windows. Je umístěno v rozhraní **AVG File Server 2011** 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:

6.1.1. Soubor

- ***Konec*** - zavírá uživatelské rozhraní **AVG File Server 2011**. Aplikace AVG však zůstává spuštěna, běží trvale na pozadí a váš počítač je stále chráněn!

6.1.2. Komponenty

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

- ***Přehled komponent*** - přepne uživatelské rozhraní na dialog ***Přehled komponent a jejich stavu***
- ***Serverové komponenty*** - zobrazí přehled serverových komponent - podrobnosti >>
- ***Anti-Virus*** chrání váš počítač proti útočícím virům - podrobnosti >>
- ***Anti-Spyware*** chrání váš počítač před spyware a adware - podrobnosti >>

6.1.3. 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***
- ***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 File Server 2011**

6.1.4. Nástroje

- ***Otestovat počítač*** - přepíná do testovacího rozhraní AVG a přímo spouští ***Test celého počítače***

- ***Otestovat zvolený adresář*** - přepíná do testovacího rozhraní AVG a nabízí ve stromové struktuře vašeho disku možnost definovat ty složky, které mají být otestovány

- ***Otestovat soubor*** - umožňuje spustit test na vyžádání nad samostatným souborem, který vyberete ve stromové struktuře na vašem disku

- ***Aktualizovat*** - automaticky spouští proces aktualizace **AVG File Server 2011**

- ***Aktualizace 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 File Server 2011**. Obecně doporučujeme podržet výchozí výrobcem definované nastavení aplikace.

6.1.5. Nápověda

- ***Obsah*** - otevírá nápovědu k programu AVG

- ***Odborná pomoc online*** - otevírá web AVG (http://www.avg.com) na stránce centra zákaznické podpory

- ***AVG na webu*** - otevírá web AVG (http://www.avg.com)

- ***Informace o virech*** - otevírá ***Virovou encyklopedii*** na webu AVG (http://www.avg.com), v níž lze dohledat podrobné informace o detekovaných nálezech

- ***Stáhnout AVG Rescue CD*** - otevře prohlížet na stránce s možností stažení AVG Resuce CD.

- ***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.com) 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 File Server 2011**, *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 File Server 2011** *s prodejním číslem, položky se zobrazí jako* ***Zaregistrovat*** *a* ***Aktivovat***. *Podrobnější informace o možnostech aktivace a registrace najdete v kapitole Licence.*

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

6.2. Informace o stavu zabezpečení

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

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

 - Oranžová ikona informuje o stavu, kdy jedna (*nebo více*) komponent není správně nastavena. Nejedná se o kritický problém, pravděpodobně jste se sami rozhodli některou komponentu deaktivovat. V každém případě jste stále chráněni. 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.

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

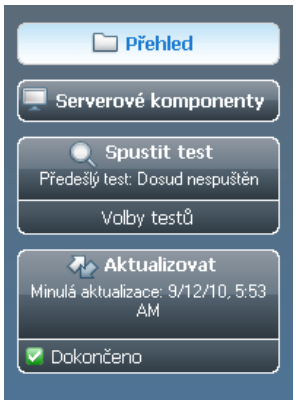
stavu a zajistíte tak nejvyšší úroveň bezpečnosti!

Důrazně doporučujeme, abyste věnovali pozornost údajům zobrazeným v sekci ***Informace o stavu zabezpečení*** a pokud AVG hlásí jakýkoliv problém, zaměřte se na jeho řešení. Pokud ignorujete chybová hlášení AVG, váš počítač je ohrožen!

Poznámka: *Informaci o stavu AVG lze v kterémkoliv okamžiku práce na počítači získat také pohledem na ikonu na systémové liště.*

6.3. Zkratková tlačítka

Zkratková tlačítka *(v levé části uživatelského rozhraní AVG)* 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 >>***
- ***Serverové komponenty*** - zobrazí přehled serverových komponent - viz kapitola ***Serverové komponenty AVG >>***
- ***Spustit test*** - ve výchozím nastavení tlačítko uvádí informaci (*typ testu a datum spuštění*) o testu, který byl spuštěn naposledy. Můžete buďto kliknout na příkaz ***Spustit test***, čímž dojde ke spuštění téhož testu, nebo na příkaz ***Otestovat počítač***, čímž otevřete testovací rozhraní AVG, kde je možné přímo spouštět testy vašeho počítače, plánovat jejich spuštění či editovat parametry testů - viz kapitola ***AVG Testování >>***
- ***Aktualizovat*** - tlačítko uvádí datum posledního spuštění procesu aktualizace. Stiskem tlačítka otevřete nové rozhraní a aktualizaci přímo spustíte - viz kapitola ***Aktualizace AVG >>***

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

6.4. Přehled komponent

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

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

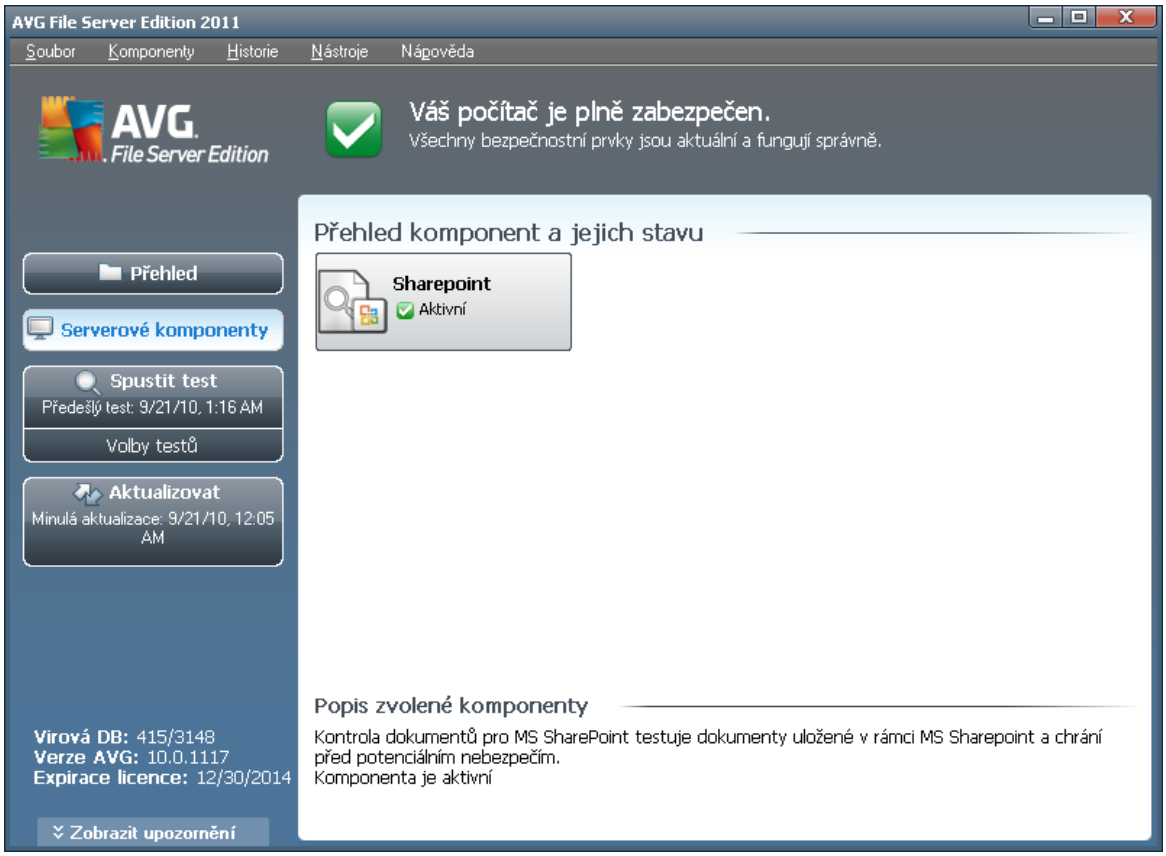
V rámci **AVG File Server 2011** najdete v sekci ***Přehled komponent*** informace o těchto komponentách:

- ***Anti-Virus*** chrání váš počítač proti útočícím virům - podrobnosti >>
- ***Anti-Spyware*** chrání váš počítač před spyware a adware - podrobnosti >>
- ***Rezidentní štít*** pracuje na pozadí a kontroluje soubory při jejich kopírování, otevírání a ukládání - podrobnosti >>
- ***Manažer aktualizací*** spravuje aktualizační procesy AVG - podrobnosti >>
- ***Licence*** zobrazuje licenční číslo, typ licence, datum expirace atd. - podrobnosti >>
- ***Vzdálená správa*** se zobrazuje pouze podmínečně v případě, že instalujete síťovou edici produktu AVG a rozhodli jste se během instalačního procesu tuto komponentu doinstalovat
- ***Anti-Rootkit*** detekuje programy a technologie, které dokáží maskovat přítomnost nebezpečného software - 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.

6.5. Serverové komponenty



Sekce ***Serverové komponenty*** 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 File Server 2011** najdete v sekci ***Serverové komponenty*** informace o těchto komponentách:

- ***SharePoint*** testuje dokumenty uložené v rámci MS SharePoint a chrání před možným nebezpečím - 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 změnou ikony na systémové liště.

6.6. Statistika

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

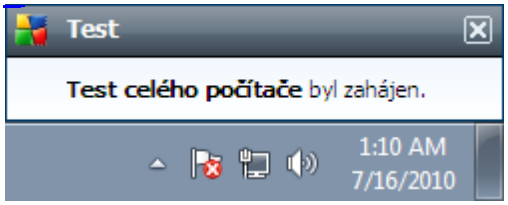
- ***Virová DB*** - informace o verzi aktuálně instalované virové databáze
- ***Verze AVG*** - informace o instalované verzi AVG *(číslo ve tvaru 10.0.xxxx, kde 10.0 zastupuje produktovou řadu AVG a xxxx označuje číslo sestavení)*
- ***Expirace licence*** - datum, kdy dojde k expiraci vaší licence AVG

6.7. Ikona na systémové liště

Ikona na systémové liště (*vpravo dole na monitoru, na panelu Windows*) ukazuje aktuální stav **AVG File Server 2011**. 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, 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
- ***Běžící testy*** - tato položka se zobrazuje pouze tehdy, je-li aktuálně spuštěn některý test. U tohoto běžícího testu pak můžete nastavit jeho prioritu, případně test pozastavit nebo ukončit. K dispozici jsou dále možnosti *Nastavit prioritu pro všechny testy*, *Pozastavit všechny testy* a *Zastavit všechny testy* .
- ***Aktualizovat*** - spustí okamžitou ***aktualizaci***
- ***Nápověda*** - otevře soubor nápovědy na úvodní stránce

7. Komponenty AVG

7.1. Anti-Virus

7.1.1. Princip Anti-Viru

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

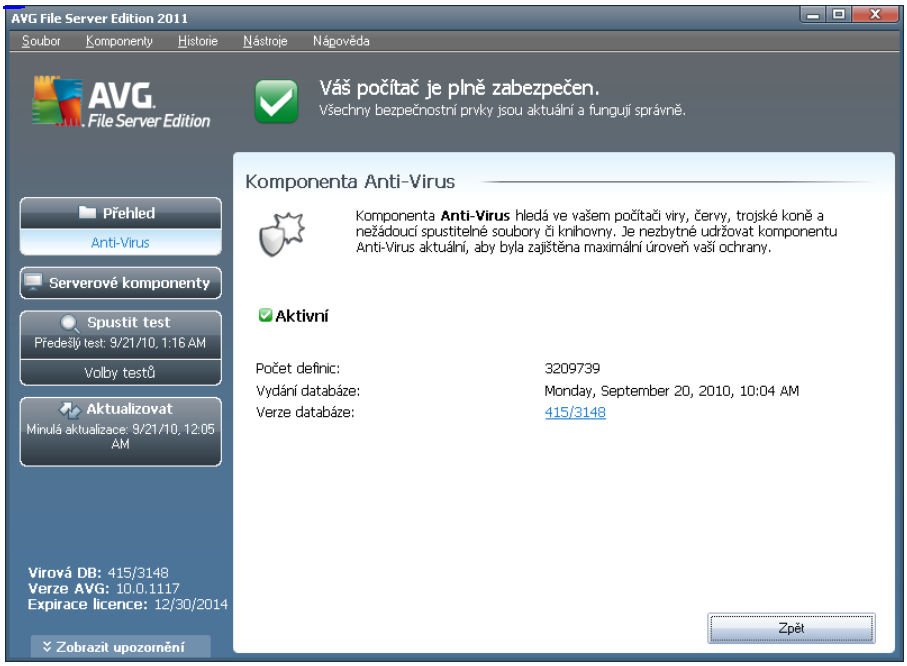
Dobrá antivirová ochrana zaručí, že na počítači nebude spuštěn žádný známý virus!

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.

7.1.2. Rozhraní komponenty Anti-Virus



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

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

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

7.2. Anti-Spyware

7.2.1. Princip Anti-Spyware

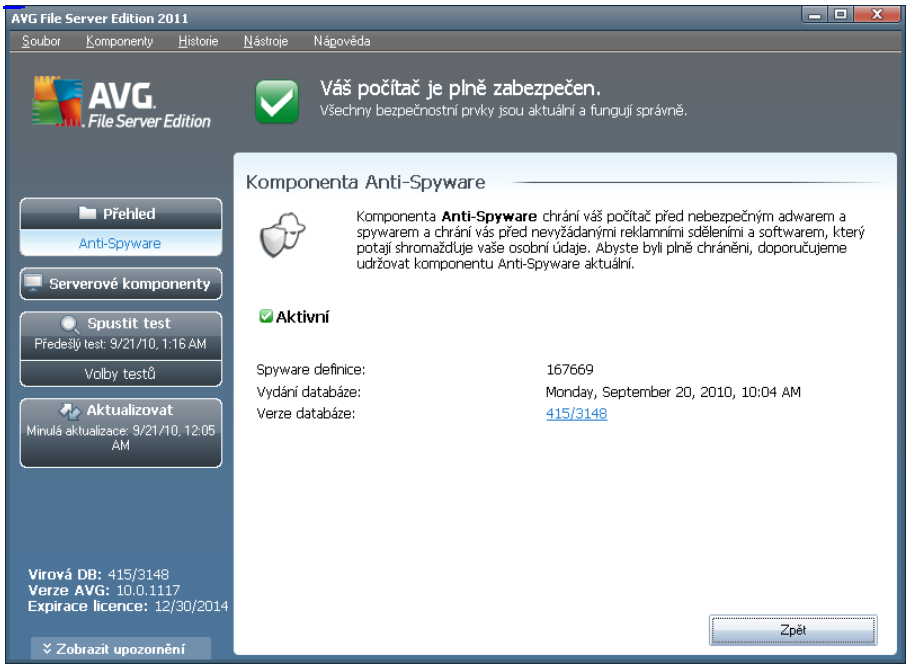
Spyware se obvykle definuje jako jeden z typů malware, to jest software, který z vašeho počítače sbírá informace bez vašeho vědomí. Některé aplikace typu spyware mohou být nainstalovány na váš počítač záměrně; častým příkladem jsou třeba reklamní upoutávky, pop-up okna nebo jiné typy obtížného software.

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 File Server 2011** 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.

7.2.2. Rozhraní komponenty Anti-Spyware



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

- ***Spyware definice*** - číslo udává počet vzorků spyware definovaných v aktuální verzi spyware databáze
- ***Vydání databáze*** - datum 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*).

7.3. Rezidentní štít

7.3.1. Princip Rezidentního štítu

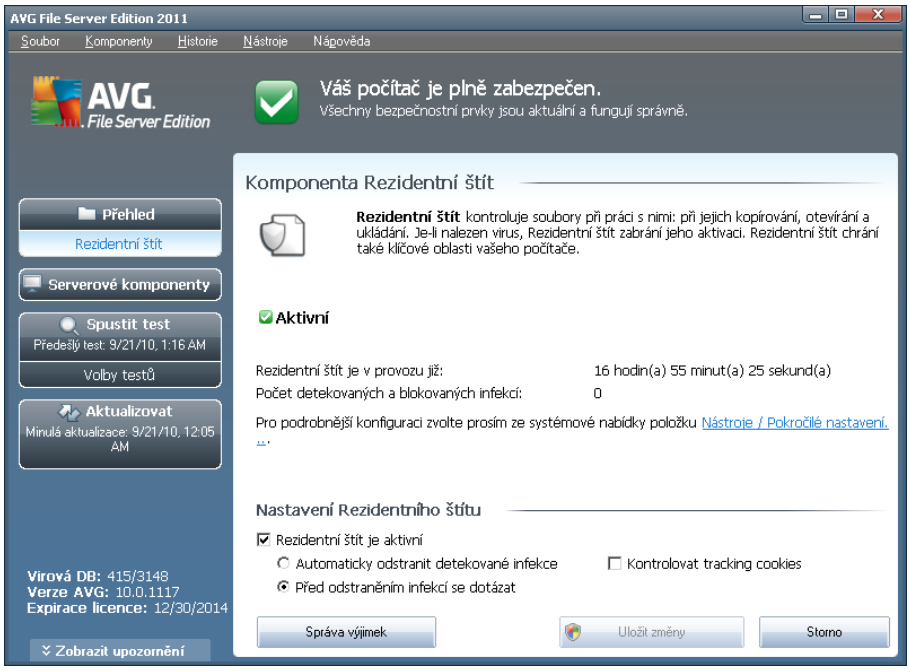
Komponenta ***Rezidentní štít*** poskytuje vašemu počítači nepřetržitou ochranu. Testuje všechny soubory, které otvíráte, kopírujete, ukládáte, a kontroluje také systémové oblasti počítače. V případě pozitivního nálezu v právě používaném souboru zastaví prováděnou operaci a zabrání aktivaci viru. Jelikož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

Rezidentní štít

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

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

7.3.2. Rozhraní komponenty Rezidentní štít



Rozhraní ***Rezidentního štítu*** nabízí kromě popisu funkce komponenty a informace o jejím aktuálním stavu 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*)

Nastavení Rezidentního štítu

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

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

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

Tato volba nijak 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***:

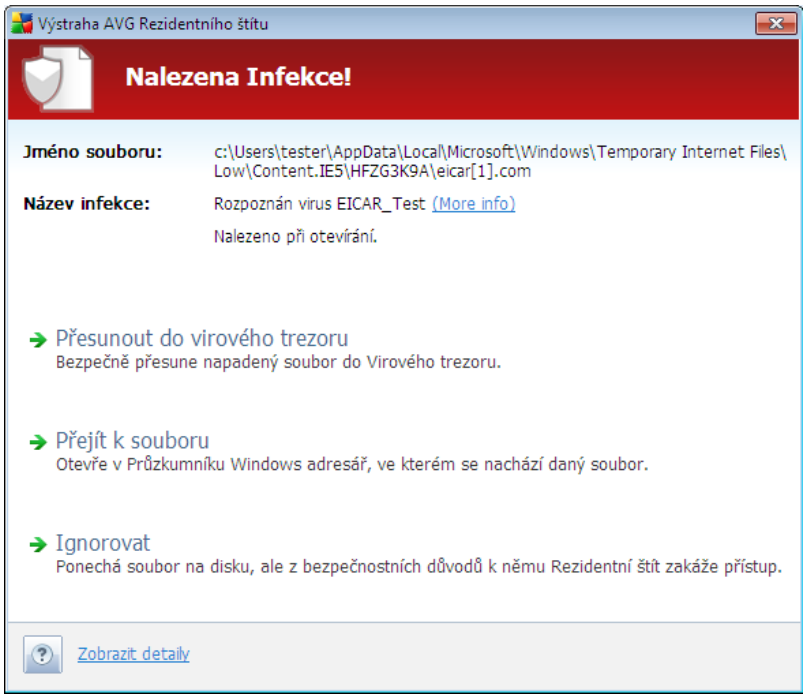
- ***Správa výjimek*** - otevírá dialogové okno ***Výjimky Rezidentního štítu***, v němž lze definovat adresáře a soubory, které mají být z kontroly ***Rezidentním***

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*)

7.3.3. Nálezy Rezidentního štítu

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



V dialogu je uvedena informace o souboru, který byl detekován jako infikovaný (*Jméno souboru*) a jméno rozpoznané infekce (*Název infekce*). Dále pak následuje odkaz do ***Virové encyklopedie***, kde najdete detailní informace o rozpoznané infekci, jsou-li tyto údaje známy (*Více informací*).

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

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

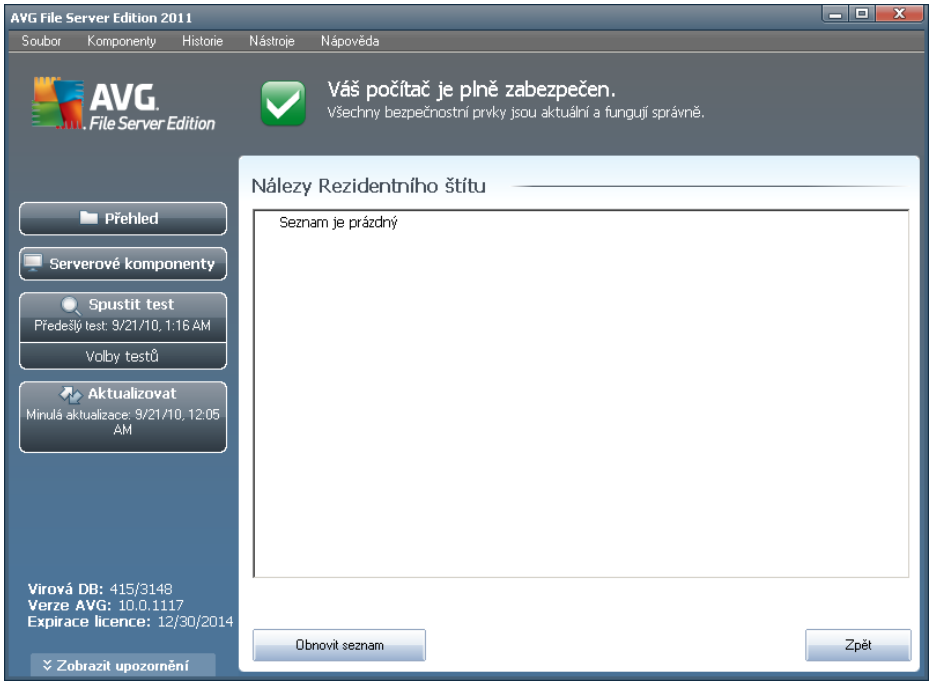
- ***Odstranit infekci jako uživatel s právy skupiny Power Users*** - označte toto políčko, pokud se domníváte, že nemáte dostatečné oprávnění k tomu odstranit infekci jako běžný uživatel. Uživatelé skupiny Power Users mají

rozšířená přístupová práva a je-li infekce detekována například v systémovém adresáři, bude nutné označit tuto volbu, aby mohla být infekce odstraněna.

- ***Léčit*** - toto tlačítko se zobrazí pouze v případě, že 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!

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

Celkový přehled o všech hrozbách detekovaných ***Rezidentním štítem*** najdete v dialogu ***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*).

7.4. Manažer aktualizací

7.4.1. Princip Manažeru aktualizací

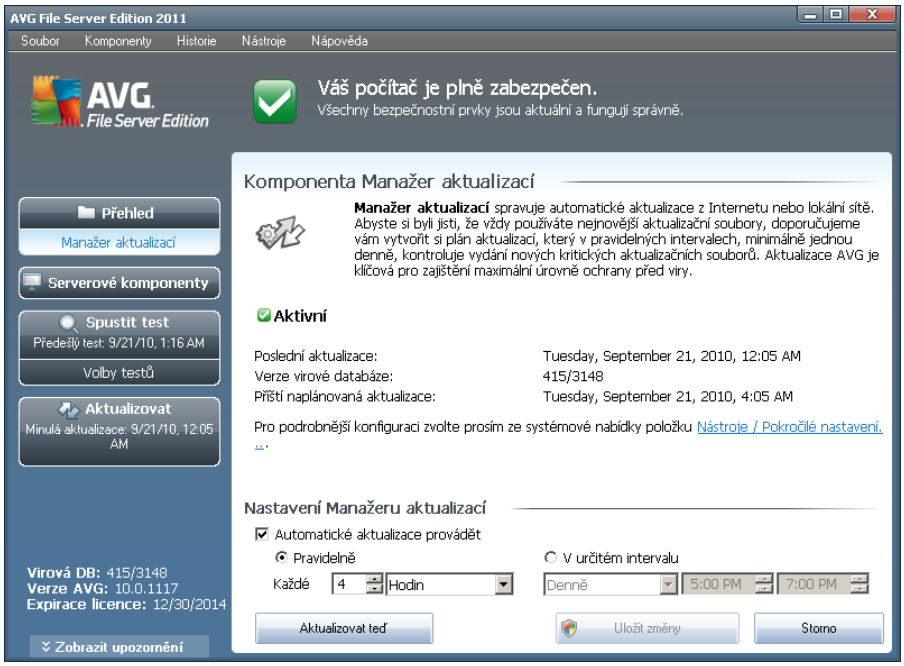
Každý bezpečnostní software může zajistit skutečnou ochranu vašeho počítače před různými typy nebezpečí pouze tehdy, je-li pravidelně aktualizován. Autoři virů stále hledají nové a nové trhliny v operačních systémech i softwarových aplikacích a snaží se jich zneužít. Denně se objevují nové viry, nový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

7.4.2. Rozhraní komponenty Manažer aktualizací



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

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

Nastavení Manažeru aktualizací

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

Dále pak můžete definovat, kdy mají být aktualizace ověřovány a spouštěny:

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

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

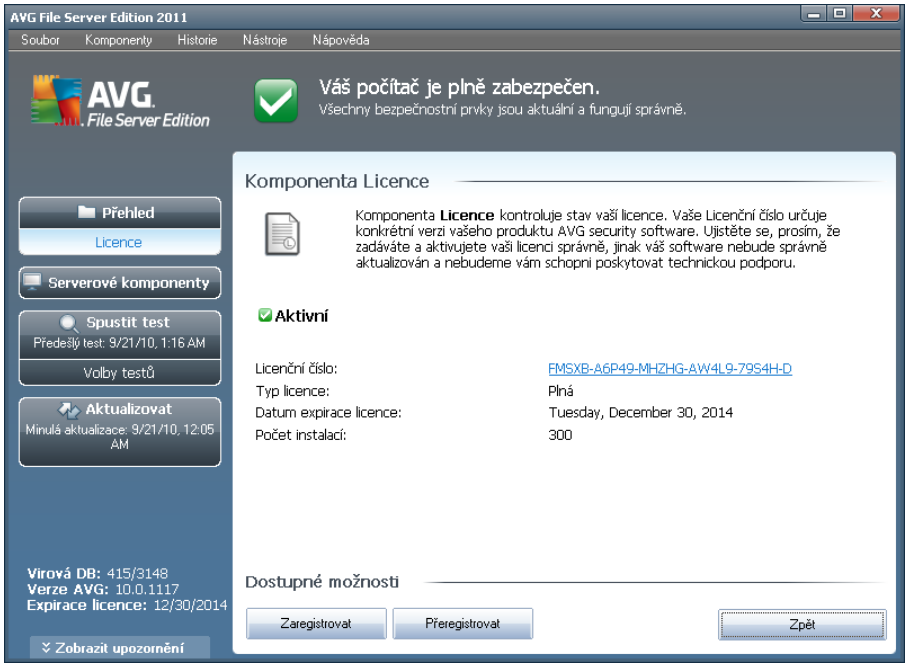
Poznámka: *Všechny komponenty AVG jsou výrobcem nastaveny k optimálnímu výkonu. Změnu konfigurace by měli provádět pouze zkušení uživatelé. Chcete-li tedy změnit nastavení programu AVG, zvolte ze systémového menu položku* ***Nástroje / Pokročilé nastavení*** *a editaci nastavení proveďte v nově otevřeném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

7.5. 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 File Server 2011**, je třeba licenci prodloužit. Prodloužení licence lze provést on-line na webu AVG.
- ***Počet instalací*** - číslo udává počet stanic, na něž můžete **AVG File Server 2011** s tímto licenčním číslem oprávněně instalovat.

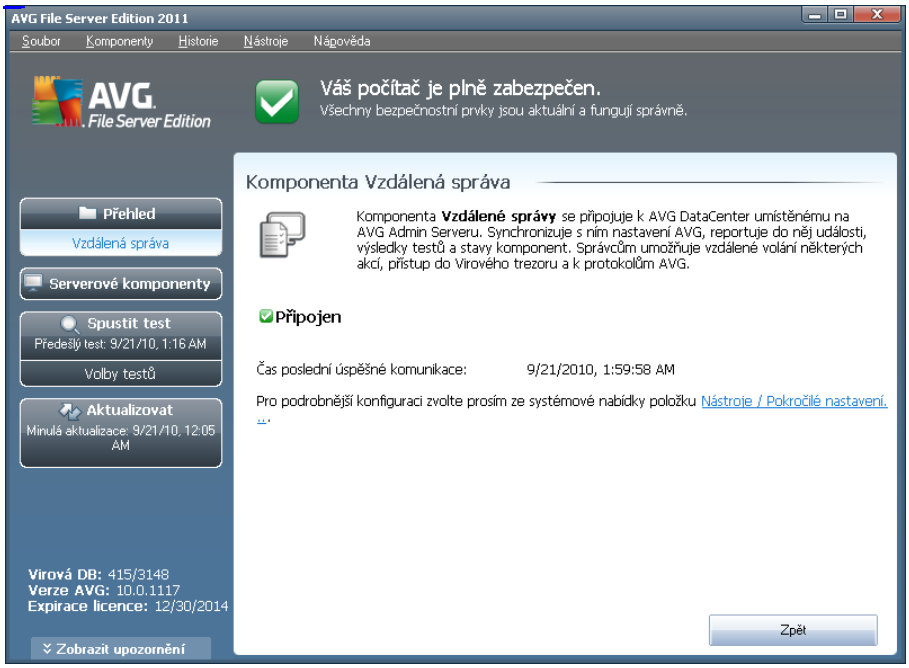
Ovládací tlačítka dialogu

- ***Zaregistrovat*** - otevírá web AVG (http://www.avg.com) 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 File Server 2011**, *tlačítka se zobrazí jako* ***Koupit online *a* ***Aktivovat*** *a odkáží Vás na web AVG, kde si můžete přímo zakoupit plnou verzi programu. Pokud máte nainstalovaný program* **AVG File Server 2011** *s prodejním číslem, tlačítka budou pojmenována* ***Zaregistrovat*** *a* ***Aktivovat***.

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

7.6. Vzdálená správa



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

Pro podrobný popis funkce a možností této komponenty a zapojení klientské stanice AVG do systému vzdálené správy vás odkazujeme na samostatnou dokumentaci 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*)

7.7. 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.

7.7.1. Princip Anti-Rootkitu

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

7.7.2. Rozhraní komponenty Anti-Rootkit

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

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.*

Nastavení Anti-Rootkitu

Ve spodní části rozhraní najdete sekci ***Nastavení Anti-Rootkitu***, v níž můžete nastavit některé základní funkce testu na přítomnost rootkitů. Nejprve označením příslušného políčka (*jednoho nebo více*) označte, jaké objekty mají být testovány:

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

Dále se 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*)

Ovládací tlačítka dialogu

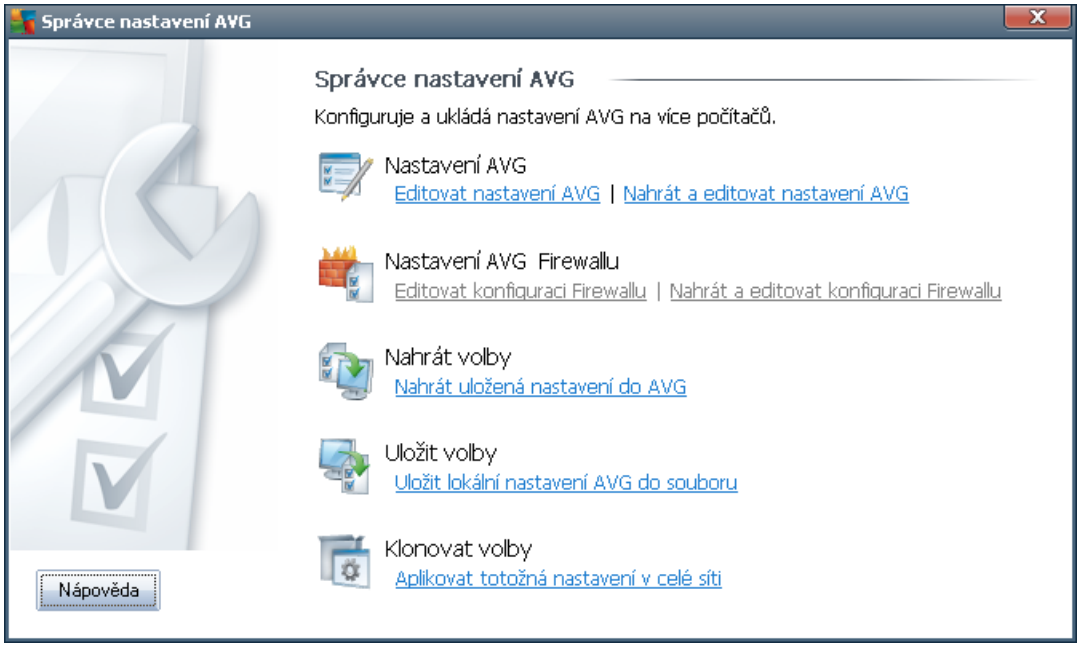
- ***Vyhledat rootkity*** - jelikož testování přítomnosti rootkitů není implicitní součástí ***Testu celého počítače***, slouží rozhraní komponenty ***Anti-Rootkit*** přímo ke spuštění samostatného testu; test spustíte stiskem tohoto tlačítka
- ***Uložit změny*** - stiskem tlačítka aplikujete veškeré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

8. Manažer nastavení AVG

Manažer nastavení AVG je nástroj určený zejména pro menší sítě. Umožňuje kopírovat, upravovat a distribuovat konfiguraci AVG, kterou lze následně uložit na přenosné médium (např. USB flash disk) a aplikovat ručně na vybrané stanice.

Tento nástroj je volitelnou součástí instalace AVG a lze jej spustit z Windows nabídky Start skrze:

Všechny programy/AVG 2011/Manažer nastavení AVG



- **Nastavení AVG**

    - ***Editovat nastavení AVG*** - otevře dialog pokročilého nastavení vaší lokální instalace AVG. Všechny změny provedené v tomto dialogu se projeví v lokální instalaci AVG.

    - ***Nahrát a editovat nastavení AVG*** - pokud již máte k dispozici dříve uložený soubor s konfigurací AVG (.pck), použijte tento odkaz pro jeho otevření a následné úpravy. Otevře se opět dialog pokročilého nastavení AVG a provedené změny budou po stisku tlačítka ***OK*** nebo ***Použít***, uloženy do původního souboru.

- **Nastavení AVG Firewallu**

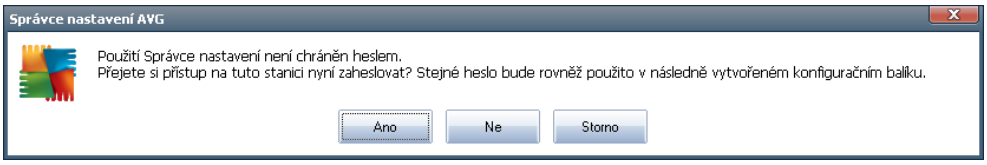
    Tato sekce by vám umožnila provádět změny v nastavení Firewallu vaší lokální instalace AVG, popřípadě upravovat nastavení Firewallu v již připraveném souboru s konfigurací AVG (.pck). Protože však váš AVG File Server 2011 nezahrnuje komponentu Firewall, jsou oba odkazy zobrazeny šedě a nejsou aktivní.

- **Nahrát volby**

  - ***Nahrát uložená nastavení do AVG*** - tímto odkazem lze otevřít soubor s konfigurací AVG (.pck) a aplikovat jej na lokální instalaci AVG.

- **Uložit volby**

  - ***Uložit lokální nastavení AVG do souboru*** - tento odkaz použijte k uložení konfigurace místní instalace AVG do souboru (.pck). Pokud jste nenastavili heslo pro Povolené akce, zobrazí se následující dialog:



  Zvolte ***Ano***, pokud si nyní přejete nastavit heslo pro přístup k Povoleným položkám. Tlačítkem ***Ne*** vytvoření hesla přeskočíte a budete moci pokračovat v uložení konfigurace do souboru.

- **Klonovat volby**

  - ***Aplikovat totožná nastavení v celé síti*** - tento odkaz umožňuje vytvořit instalační balík se stejným nastavením, jako má místní instalace AVG.

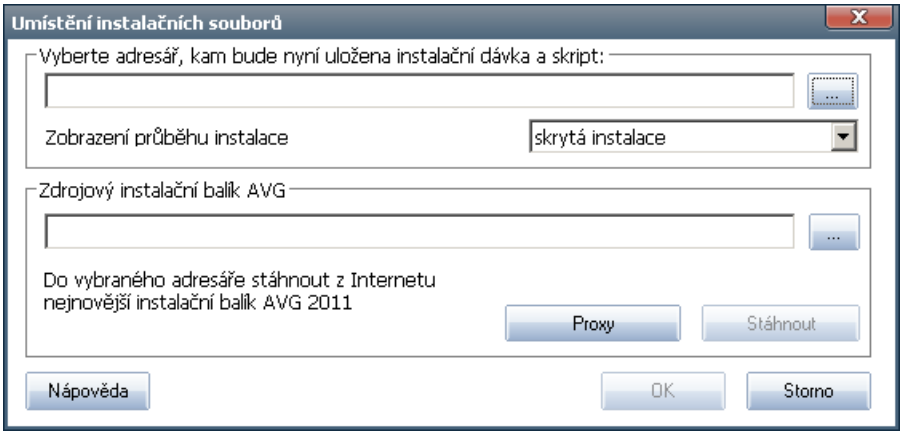
    Proces klonování zahrnuje většinu nastavení AVG s výjimkou následujících položek:

    ✓ *Nastavení jazyka*

    ✓ *Nastavení zvuků*

    ✓ *Seznam povolených položek a PUP výjimky komponenty Identity protection*

    Nejprve zvolte složku, do které si přejete instalační skript uložit:



Z rolovací nabídky zvolte jednu z možností:

- ✓ *Skrytá instalace* - na stanici nebude aktuálně přihlášenému uživateli zobrazeno žádné informační okno týkající se procesu instalace.
- ✓ *Zobrazit průběh instalace* - instalace nebude vyžadovat žádnou interakci uživatele, nicméně bude moci průběh instalace sledovat.
- ✓ *Zobrazit průvodce instalací* - instalační průvodce bude na stanici viditelný a aktuálně přihlášený uživatel bude muset potvrdit všechny kroky ručně.

Tlačítkem ***Stáhnout*** lze spustit stahování nejnovějšího instalačního balíku AVG přímo ze stránek výrobce do vybraného adresáře. Alternativně můžete do zvolené složky instalační balík nakopírovat ručně.

Pro nastavení proxy serveru pro připojení k síti zvolte tlačítko ***Proxy*** a vyplňte požadované údaje.

Kliknutím na tlačítko ***OK*** zahájíte proces klonování instalace. Před zahájením se může zobrazit opět dialog pro zadání hesla pro přístup k povoleným položkám (viz výše). Jakmile proces skončí, ve zvoleném adresáři by se měl nacházet mj. také soubor ***AvgSetup.bat***. Spuštěním tohoto souboru dojde k instalaci AVG s vybraným nastavením.

9. Serverové komponenty AVG

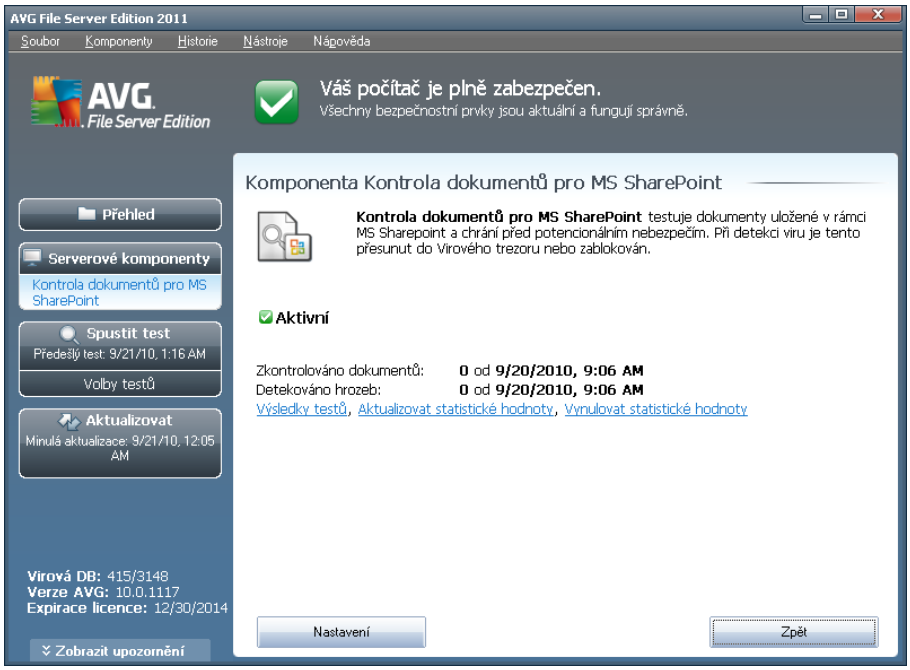
9.1. Kontrola dokumentů pro MS SharePoint

9.1.1. Princip kontroly dokumentů

Úkolem serverové komponenty ***Kontrola dokumentů pro MS SharePoint*** je kontrolovat všechny dokumenty uložené v MS SharePoint. V případě nalezení viru, je škodlivý kód přemístěn do Virového trezoru, případně zcela odstraněn.

Microsoft SharePoint je souborem produktů a softwarových prvků, které mimo jiné zahrnují moduly pro internetové sdílení dokumentů (prostřednictvím aplikace Internet Explorer), řízení procesů, vyhledávání nebo obecnou správu dokumentů. SharePoint lze používat jako platformu pro webové stránky, jež přistupují ke sdíleným datům, informačním databázím či dokumentům.

9.1.2. Rozhraní komponenty Kontrola dokumentů



Rozhraní ***Kontroly dokumentů pro MS SharePoint*** nabízí kromě popisu funkce komponenty a informace o jejím aktuálním stavu (*Rezidentní štít je spuštěn a plně funkční.*) také stručný statistický přehled:

- ***Zkontrolovano dokumentů*** - udává počet dokumentů zkontrolovaných od určitého data
- ***Detekováno hrozeb*** **-** udává počet hrozeb nalezených od určitého data

Tuto statistiku můžete kdykoli obnovit kliknutím na odkaz ***Aktualizovat statistické***

hodnoty. Nová data by se měla objevit téměř okamžitě. Jestliže chcete, aby se statistika začala vést znovu od začátku, klikněte na odkaz ***Vynulovat statistické hodnoty***. Kliknutím na odkaz ***Výsledky testů*** otevřete nový dialog, obsahující přehled výsledků testů. Údaje v tomto přehledu můžete třídit s pomocí přepínačů a/nebo záložek.

Ovládací tlačítka dialogu

Ovládací tlačítka dostupná v rozhraní komponenty ***Kontroly dokumentů pro MS SharePoint***:

- ***Nastavení*** - otevírá nový dialog, v němž můžete upravovat některé parametry testování dokumentů, prováděného serverovou komponentou ***Kontrola dokumentů pro MS SharePoint*** (více informací o tomto dialogu se dozvíte v kapitolách ***Pokročilé nastavení Kontroly dokumentů pro MS SharePoint*** a ***Akce nad nálezy***).
- ***Zpět*** - stiskem tlačítka se vrátíte do výchozího ***rozhraní serverových komponent AVG***.

10. AVG pro SharePoint Portal Server

Tato kapitola je věnována nastavení AVG na ***MS SharePoint Portal Serveru***, který považujeme za speciální případ souborového serveru.

10.1. Správa programu

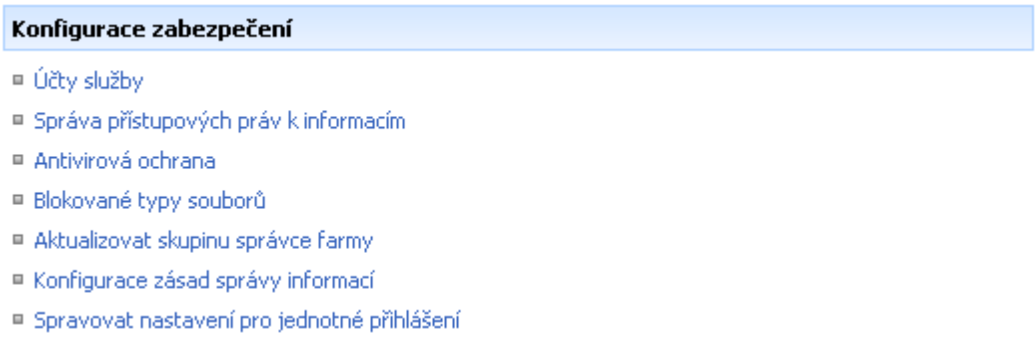
AVG pro SharePoint Portal Server používá rozhraní Microsoft SP VSAPI 1.4 pro ochranu vašeho serveru před možnou virovou infekcí. Objekty jsou testovány na potenciální přítomnost škodlivého software ve chvíli, kdy jsou nahrávány nebo stahovány ze serveru. Konfiguraci antivirové ochrany můžete nastavit pomocí rozhraní ***Centrální správy SharePoint*** vašeho serveru. V rámci ***Centrální správy SharePoint*** lze také prohlížet a spravovat log soubor **AVG pro SharePoint Portal Server**.

Rozhraní ***Centrální správy SharePoint*** (*SharePoint Central Administration*) můžete spustit, pokud jste přihlášeni na počítači, kde běží váš server. Toto rozhraní je webové (*stejně jako je tomu u uživatelských rozhraní SharePoint Portal Server*). Otevřete jej pomocí položky ***SharePoint Central Administration*** (*Centrální správa SharePoint*) ve složce ***Programs/Microsoft Office Server*** (*případně SharePoint Portal Server*) hlavní nabídky ***Start*** systému Windows:

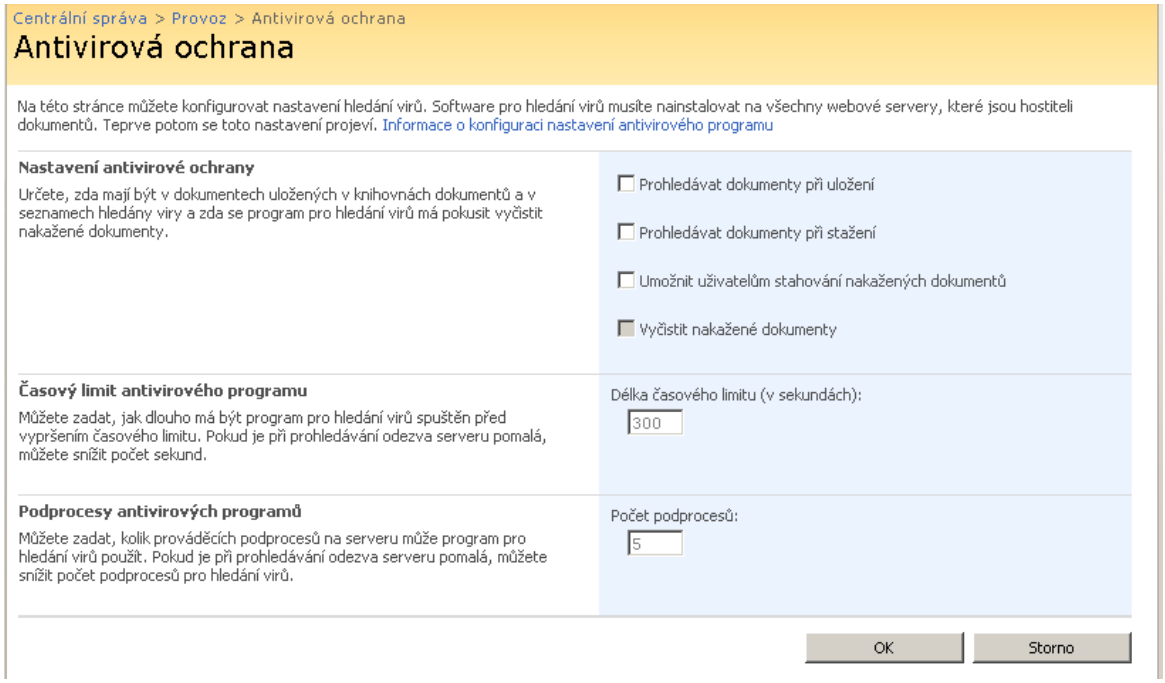
K centrální správě lze přistupovat také vzdáleně pomocí příslušných přihlašovacích práv a URL stránky ***Centrální správy SharePoint***.

10.2. Konfigurace AVG pro SPPS 2007

V rozhraní ***SharePoint 3.0 Central Administration*** můžete snadno nastavovat parametry a akce testovacího jádra **AVG pro SharePoint Portal Server**. Zvolte možnost ***Provoz*** v části ***Centrální správa***. Zobrazí se nový dialog, ze kterého vyberte volbu ***Antivirová ochrana*** v sekci ***Konfigurace zabezpečení***.



Otevřete tak následující okno:

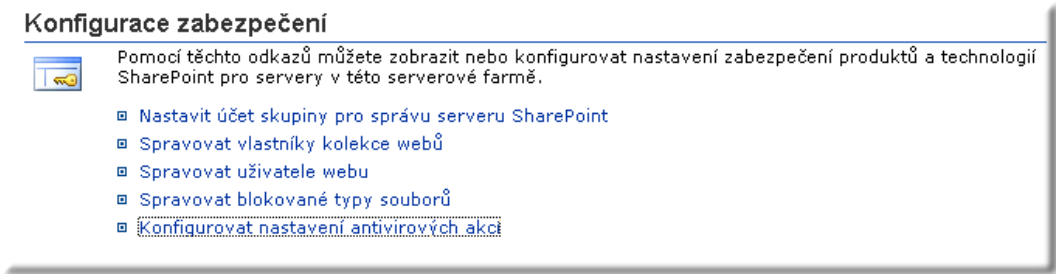


Zde můžete nastavit různé akce a parametry prvků antivirové ochrany **AVG pro SharePoint Portal Server**:

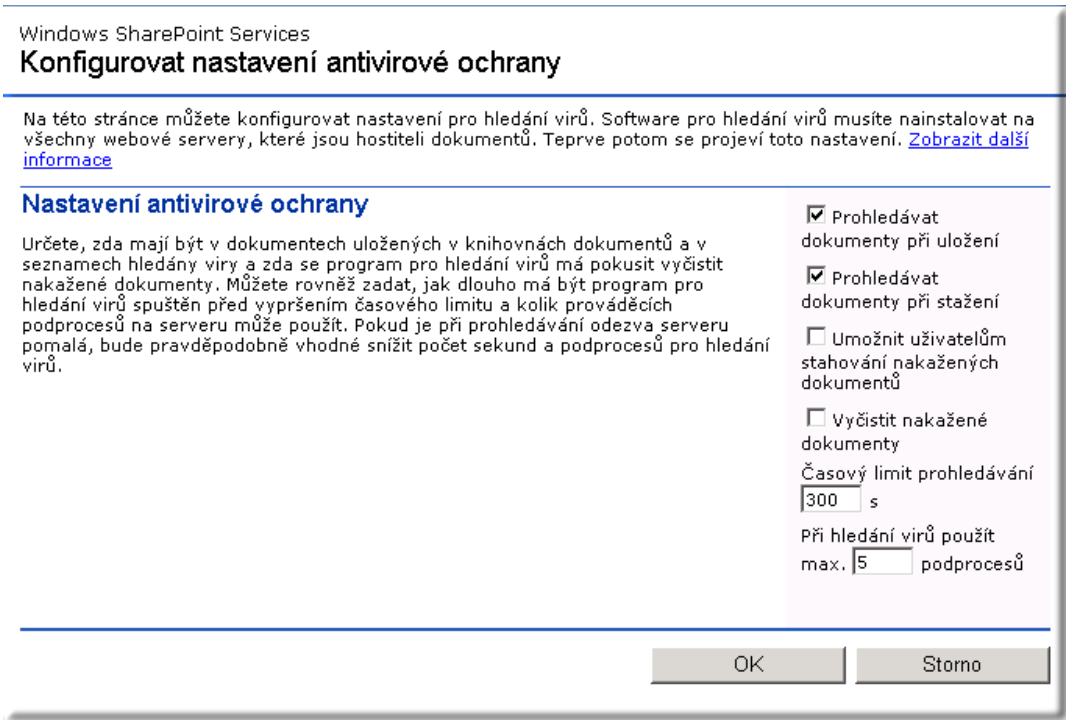
- ***Prohledávat dokumenty při uložení*** – zapne/vypne kontrolu ukládaných dokumentů
- ***Prohledávat dokumenty při stažení*** – zapne/vypne kontrolu stahovaných dokumentů
- ***Umožnit uživatelům stahování nakažených dokumentů*** – umožní/zakáže uživatelům stahovat nakažené dokumenty
- ***Vyčistit nakažené dokumenty*** – zapne/vypne automatické mazání nakažených dokumentů
- ***Délka časového limitu (v sekundách)*** – maximální doba (v sekundách), po kterou bude běžet proces antivirové kontroly v rámci jednoho spuštění (snižte tuto hodnotu, pokud se odezva serveru při kontrole dokumentů jeví jako příliš pomalá)
- ***Počet podprocesů*** – udává počet vláken antivirové kontroly, která mohou běžet najednou; zvýšením tohoto čísla lze zrychlit proces kontroly dokumentů díky vyšší úrovni paralelismu, na druhou stranu to však také může snížit rychlost odezvy serveru

10.3. Konfigurace AVG pro SPPS 2003

V rozhraní ***Centrální správa SharePoint*** můžete snadno nastavovat parametry a akce testovacího jádra **AVG pro SharePoint Portal Server**. Zvolte možnost ***Konfigurovat nastavení antivirových akcí*** v části ***Konfigurace zabezpečení***:



Otevřete tak následující okno:



Zde můžete nastavit různé akce a parametry prvků antivirové ochrany **AVG pro SharePoint Portal Server**:

- ***Prohledávat dokumenty při uložení*** – zapne/vypne kontrolu ukládaných dokumentů
- ***Prohledávat dokumenty při stažení*** – zapne/vypne kontrolu stahovaných dokumentů
- ***Umožnit uživatelům stahování nakažených dokumentů*** – umožní/zakáže

uživatelům stahovat nakažené dokumenty

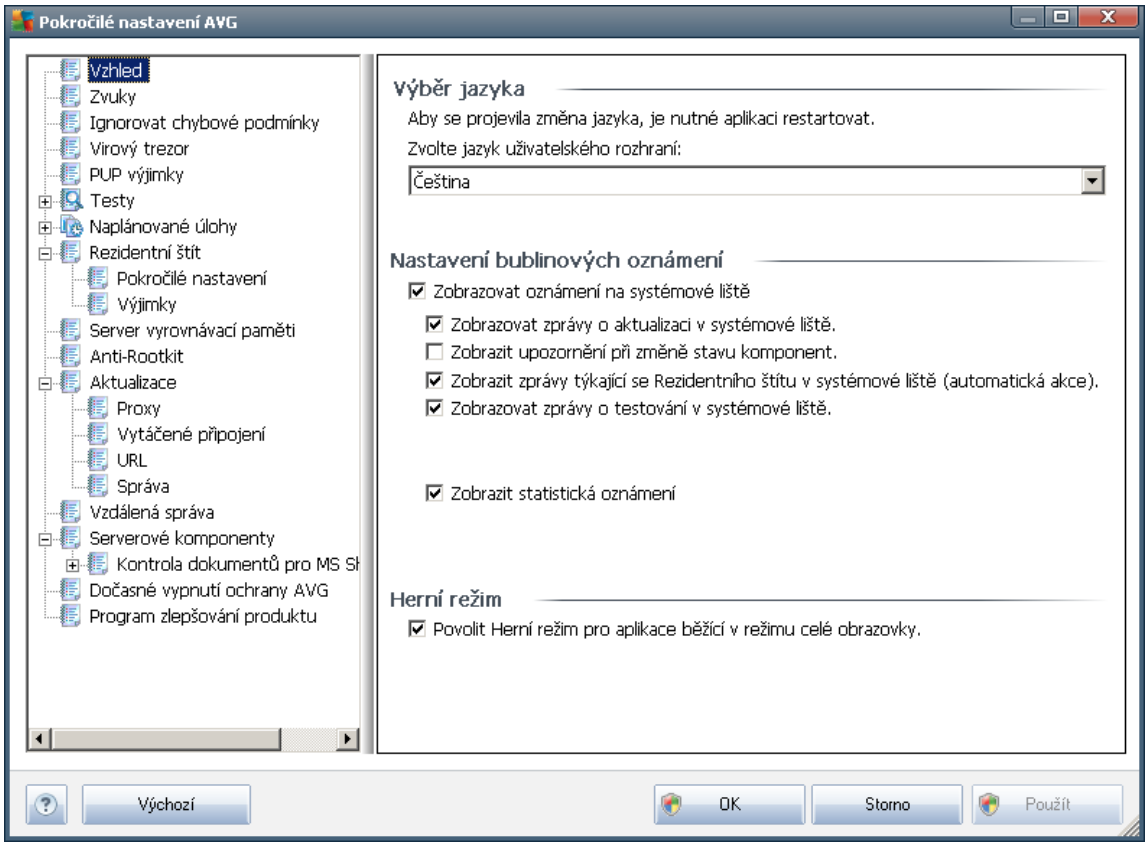
- ***Vyčistit nakažené dokumenty*** – zapne/vypne automatické léčení nakažených dokumentů (pokud to typ infekce umožní)
- ***Časový limit prohledávání*** – maximální doba (*v sekundách*), po kterou bude běžet proces antivirové kontroly v rámci jednoho spuštění (*snižte tuto hodnotu, pokud se odezva serveru při kontrole dokumentů jeví jako příliš pomalá*)
- ***Při hledání virů použít max. X podprocesů*** – X udává počet vláken antivirové kontroly, která mohou běžet najednou; zvýšením tohoto čísla lze zrychlit proces kontroly dokumentů díky vyšší úrovni paralelismu, na druhou stranu to však také může snížit rychlost odezvy serveru

11. Pokročilé nastavení AVG

Dialog pro pokročilou editaci nastaveni programu **AVG File Server 2011** 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.

11.1. Vzhled

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



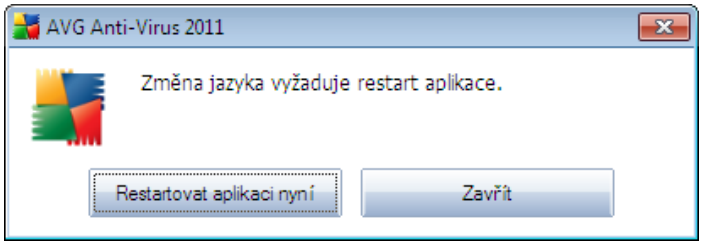
Výběr jazyka

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

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

- Stiskem tlačítka ***OK*** 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 File Server 2011**. Všechny volby provádíte označením příslušné položky v takto strukturované nabídce:

- ***Zobrazovat oznámení na systémové liště*** - položka je ve výchozím nastavení označena, informace se zobrazují. Zrušením označení položky tedy zcela vypnete zobrazování jakýchkoliv 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 (automatická akce)*** - 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*);

- o ***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;

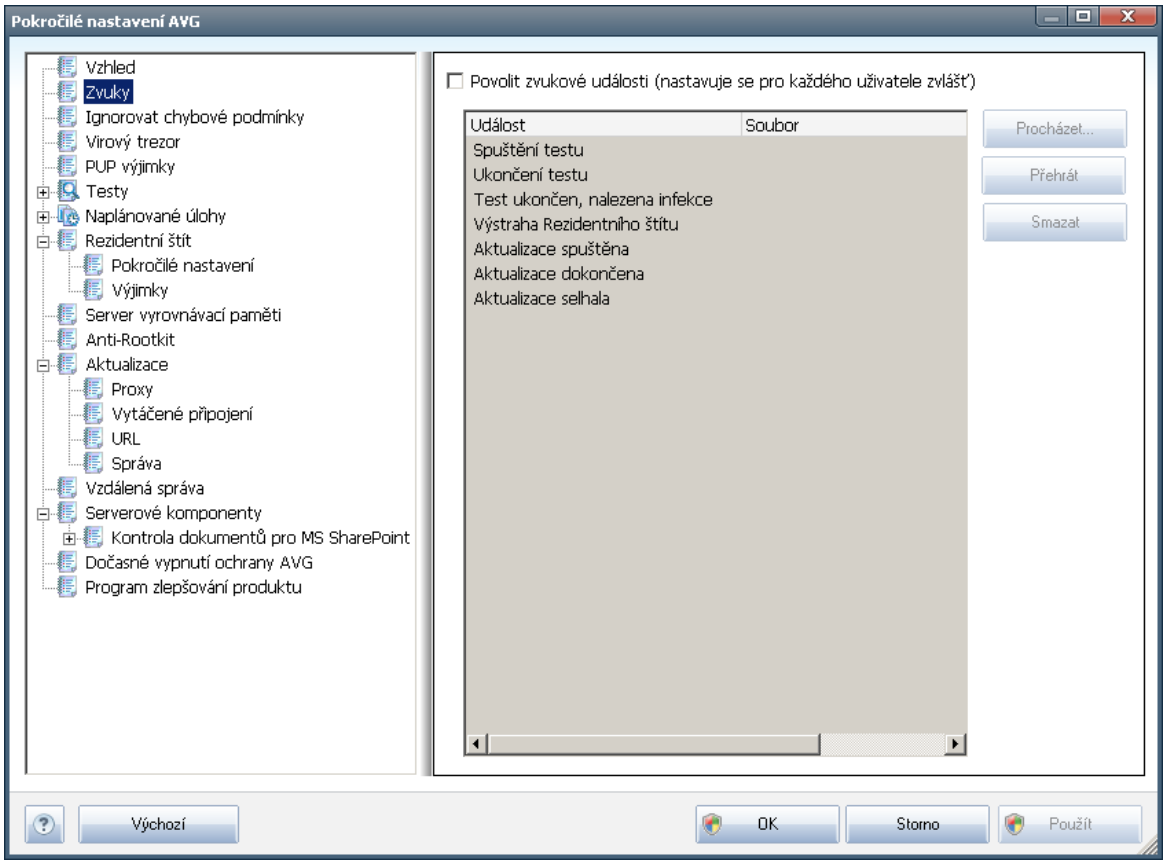
o ***Zobrazit statistická oznámení*** - volbou položky umožníte zobrazení pravidelného statistického přehledu v systémové liště.

Herní režim

Tato funkce je navržena s ohledem na aplikace, jež běží na celé obrazovce. Zobrazení oznámení AVG (*například 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*).

11.2. 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:

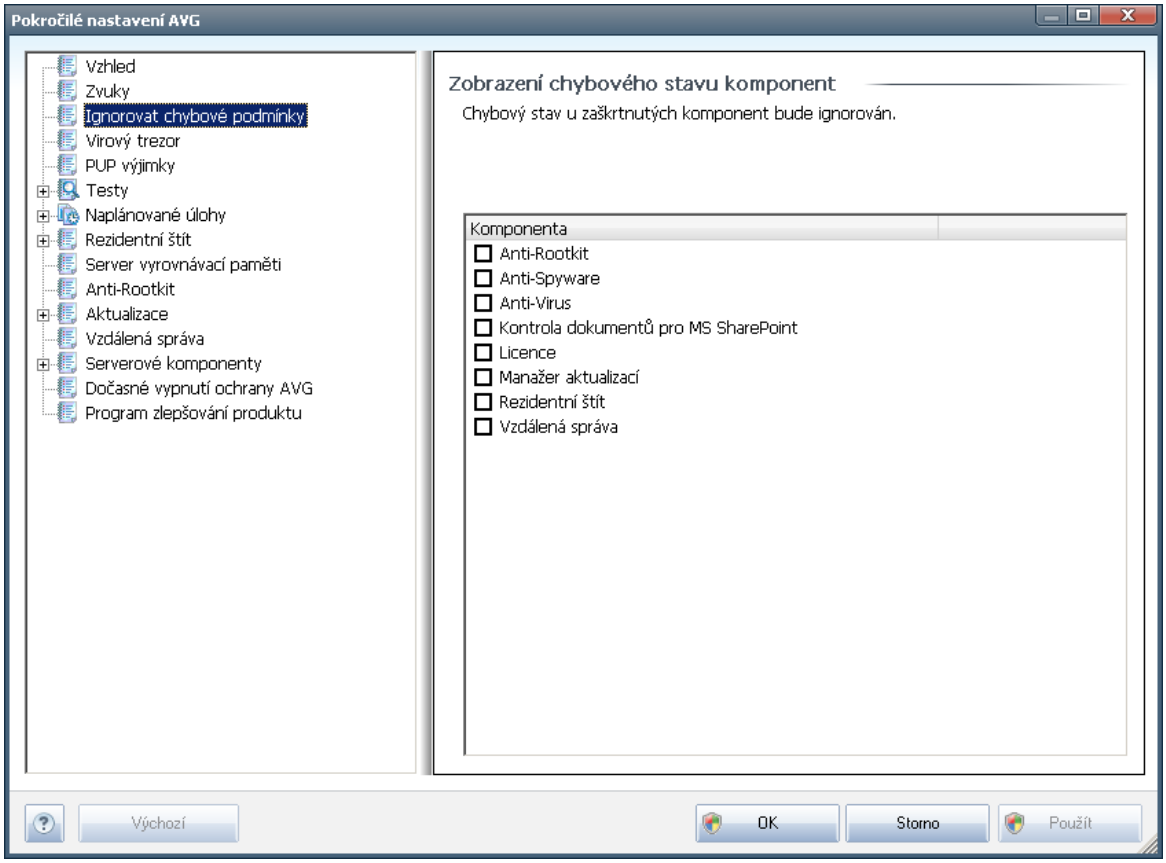


Poté vyberte ze seznamu konkrétní událost a tlačítkem ***Procházet*** zobrazte strukturu svého disku, kde vyberete příslušný zvuková soubor a zvolené akci jej přiřadíte. Chcete-li si přiřazený zvuk poslechnout, označte v seznamu příslušnou akci a stiskněte tlačítko ***Přehrát***. Tlačítkem ***Smazat***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

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

11.3. Ignorovat chybové podmínky

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



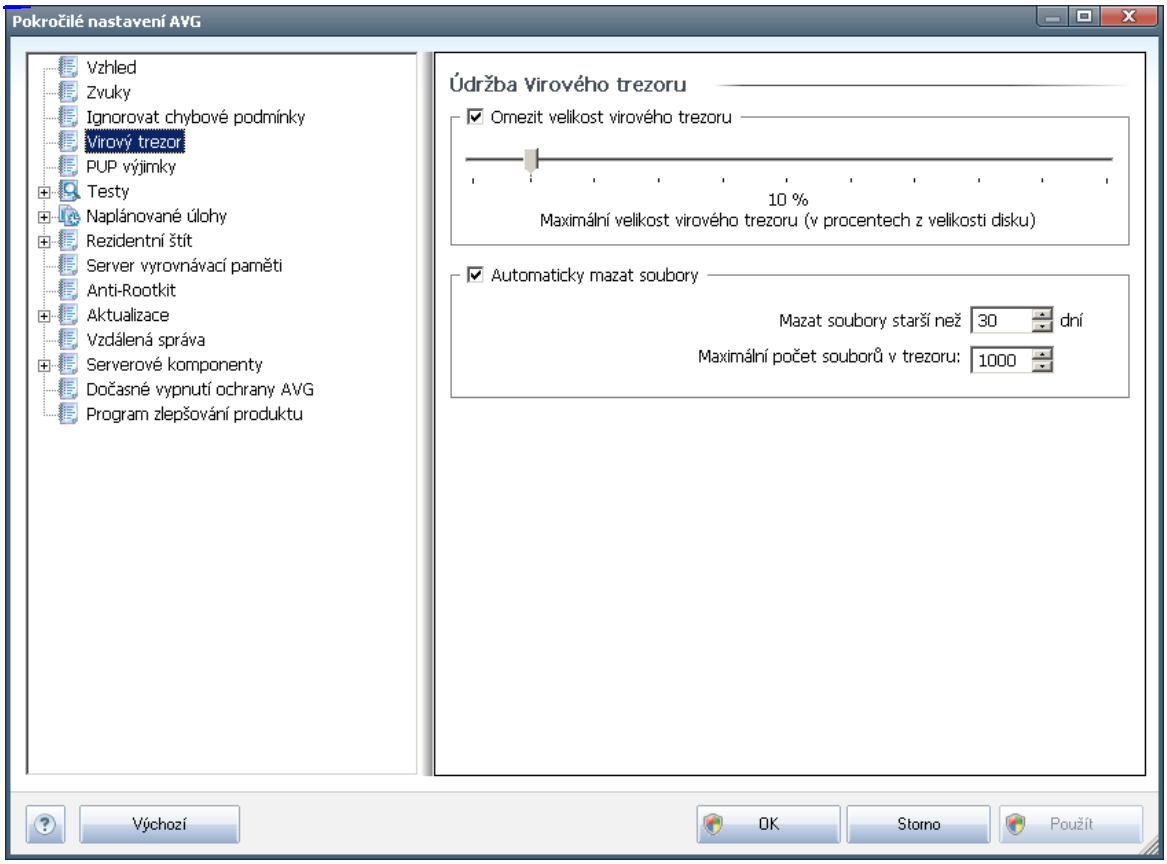
V základním nastavení programu není zvolena žádná komponenta. To znamená, že pokud dojde k jakékoliv chybě v libovolné programové komponentě, budete o tomto stavu okamžitě informováni, a to prostřednictvím:

- ***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.

11.4. Virový trezor



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

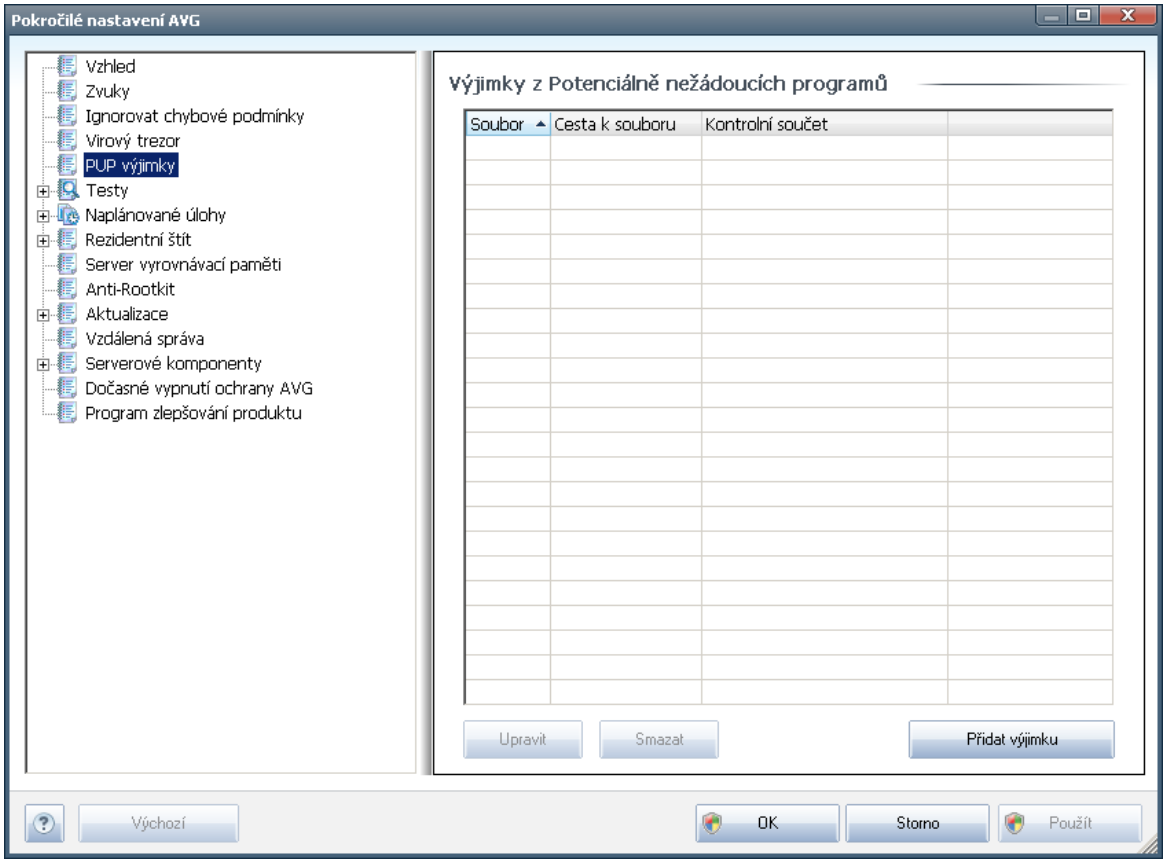
- ***Omezit velikost virového trezoru*** - na posuvníku můžete nastavit maximální povolenou velikost ***Virového trezoru***. Velikost je určena procentuálně jako poměrná část velikosti vašeho lokálního disku.

- ***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***)

11.5. PUP výjimky

AVG File Server 2011 má schopnost analyzovat spustitelné programy, případně DLL knihovny, a určit, které z nich by mohly být nežádoucí (např. spyware). Může se však stát, že některé z programů detekovaných jako nežádoucí, jsou na vašem počítači nainstalovány s vaším vědomím a přejete si je používat. Příkladem může být bezplatný program, který obsahuje adware: termínem adware obecně rozumíme software generující zobrazení reklamy, obvykle přibalený jako doplněk k programu distribuovanému zdarma. AVG může takový program při testech hlásit jako nežádoucí; pokud si však přejete jej na počítači ponechat, můžete jej definovat jako výjimku z potenciálně nežádoucích programů.



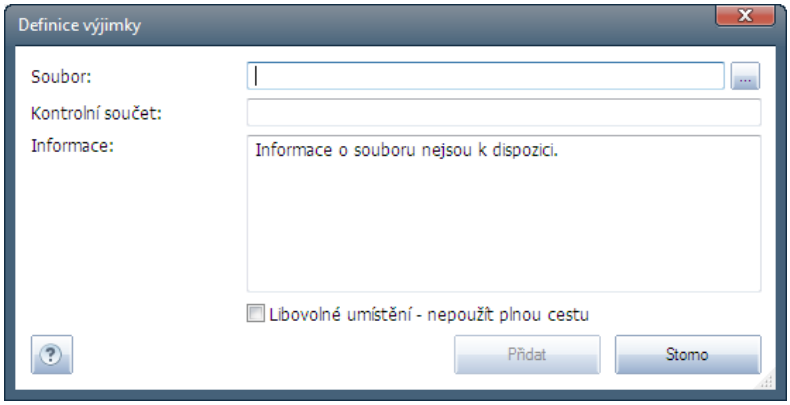
Dialog ***Výjimky z Potenciálně nežádoucích programů*** zobrazuje seznam již definovaných a aktuálně platných výjimek z potenciálně nežádoucích programů. Výjimku můžete editovat, smazat anebo nově přidat. Ke každé jednotlivé výjimce najdete v přehledu následující informace:

- ***Soubor*** - uvádí jméno konkrétní aplikace

- ***Cesta k souboru*** - ukazuje cestu k umístění aplikace na disku
- ***Kontrolní součet*** - uvádí unikátní "podpis" vybraného souboru - automaticky vygenerovaný 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*).

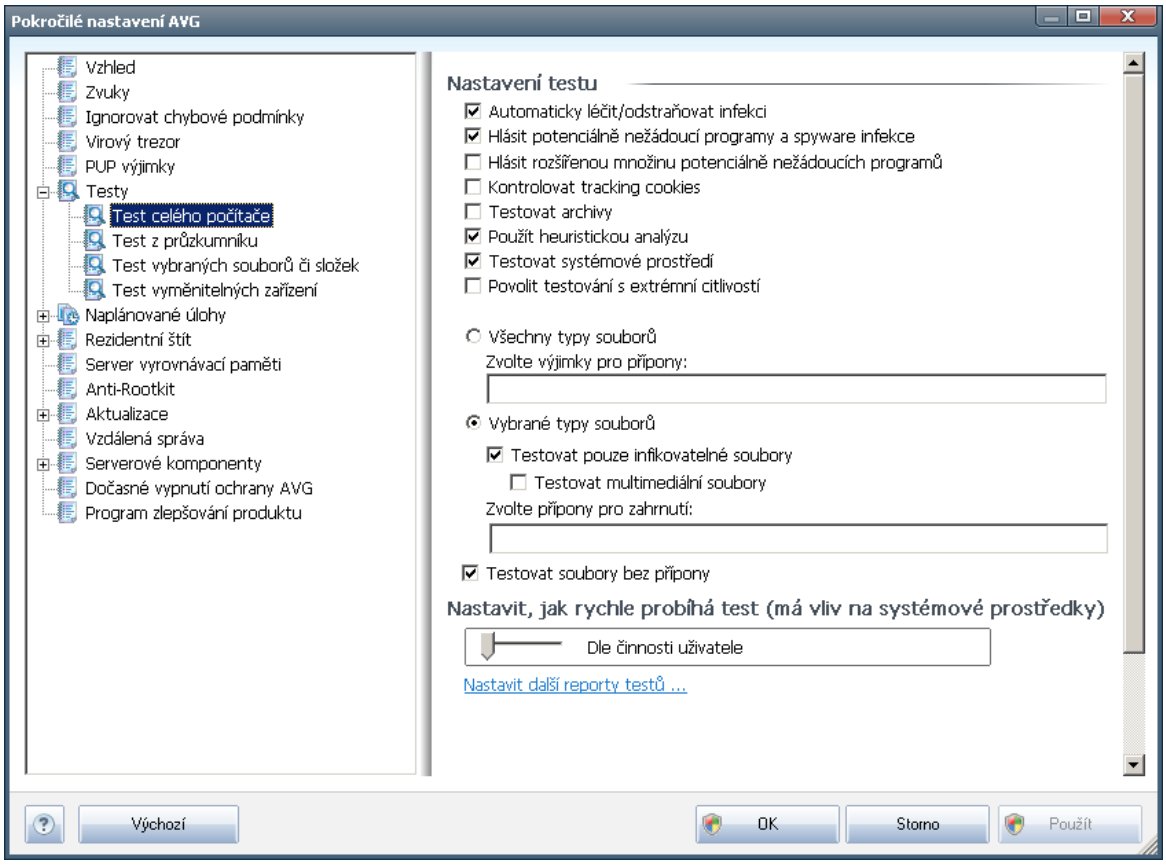
11.6. Testy

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

11.6.1. 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.

- ***Povolit testování s extrémní citlivostí*** (*ve výchozím nastavení vypnuto*) - ve specifických situacích (*při podezření na infekci ve vašem počítači*) můžete zvolit tuto metodu testování, která aktivuje nejdůkladnější testovací algoritmy a velmi podrobně prověří naprosto všechny oblasti vašeho počítače. Mějte však na paměti, že tato metoda je časově velmi náročná.

Dále se můžete rozhodnout, zda si přejete testovat

- ***Všechny typy souborů*** - 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.

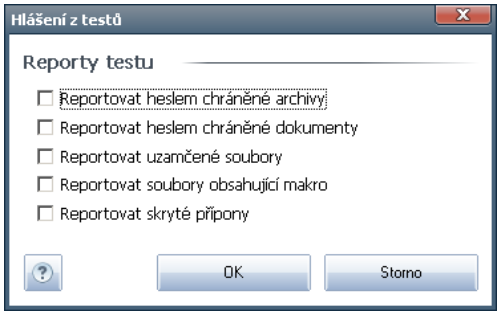
- U položky ***Testovat soubory bez přípon*** pak rozhodněte, zda se mají testovat i soubory se skrytou či neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme , abyste se tohoto nastavení podrželi, pokud nemáte skutečný důvod jej měnit. Soubory bez přípon jsou obecně vysoce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

Nastavit, jak rychle probíhá test

V této sekci pak můžete nastavit požadovanou rychlost testování v závislosti na zátěži systémových zdrojů. Ve výchozím nastavení je tato hodnota nastavena ***Dle činnosti uživatele***, 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.

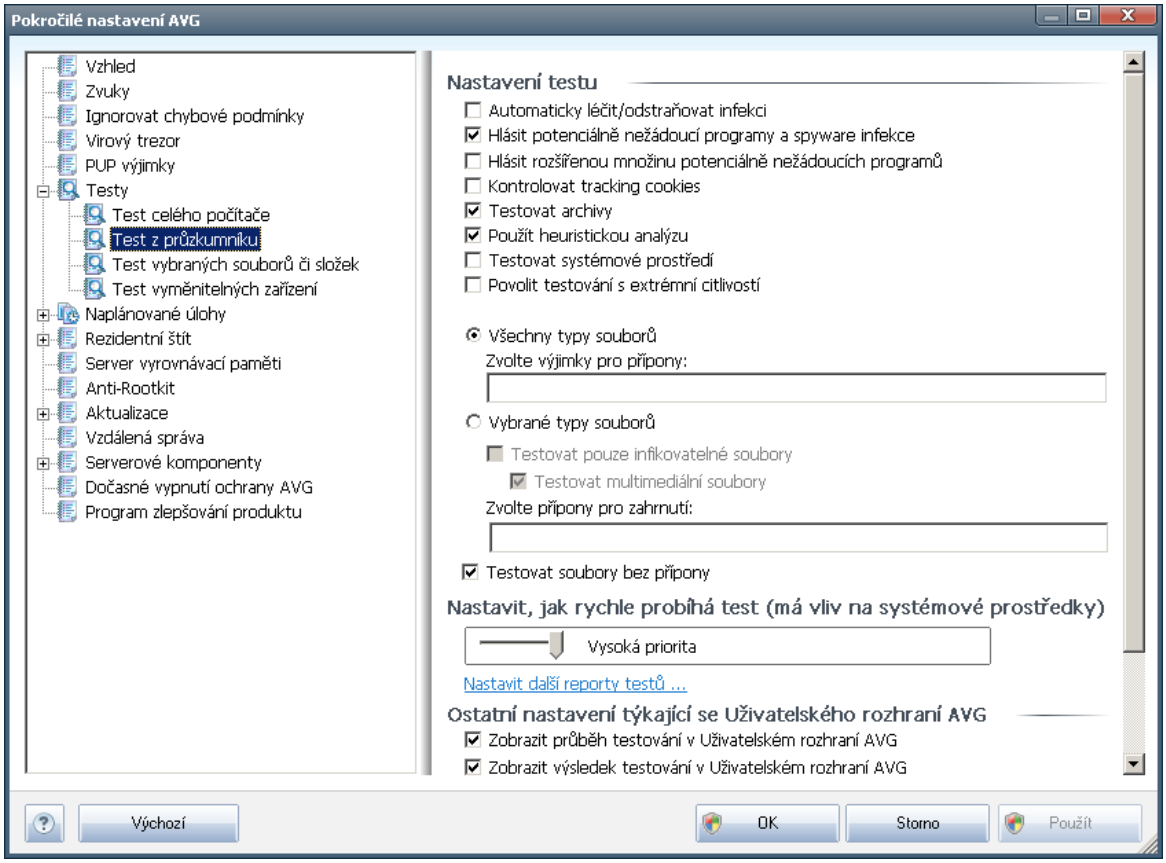
Nastavit další reporty testů ...

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:



11.6.2. 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***:



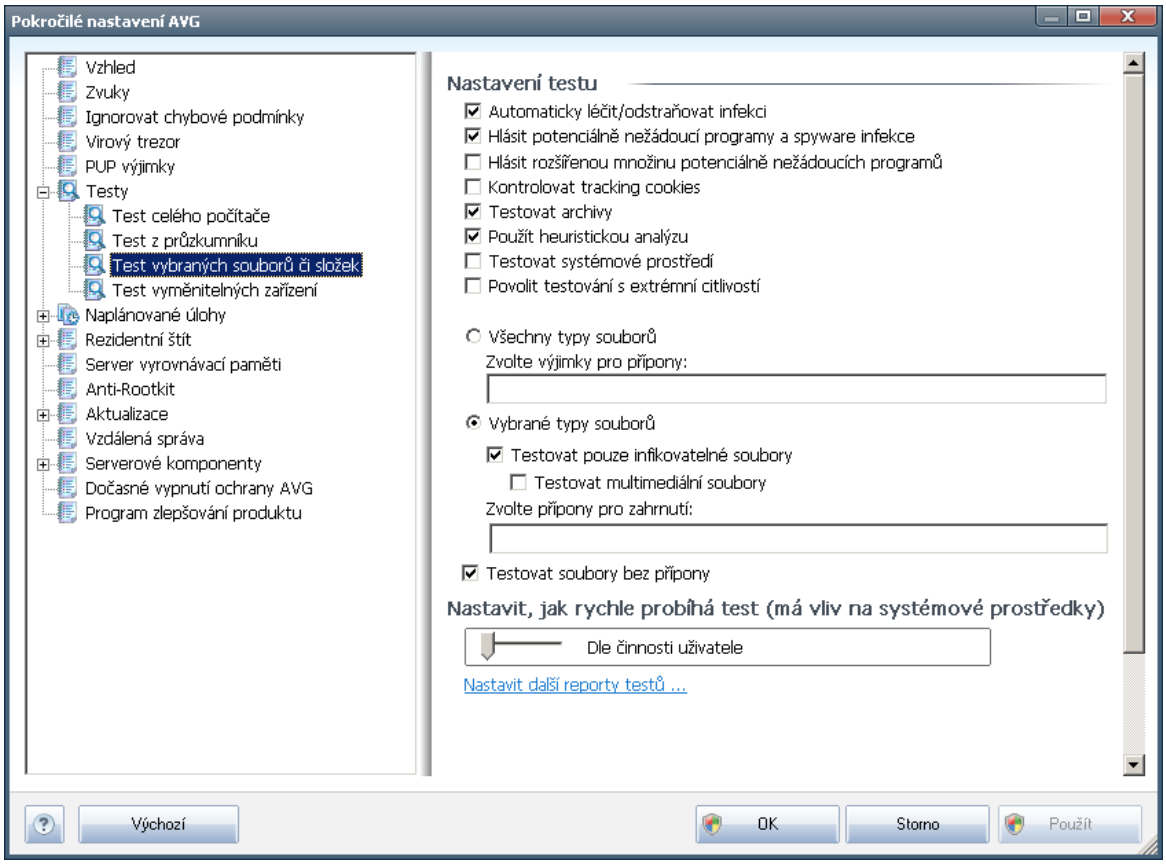
Veškeré možnosti editace parametrů testu jsou totožné s ***editací parametrů Testu celého počítače***. Odlišné je pouze výchozí nastavení těchto parametrů (*například Test celého počítače ve výchozím nastavení neprovádí kontrolu archivů, ale provádí kontrolu systémového prostředí, zatímco u Testu z průzkumníku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

11.6.3. 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:

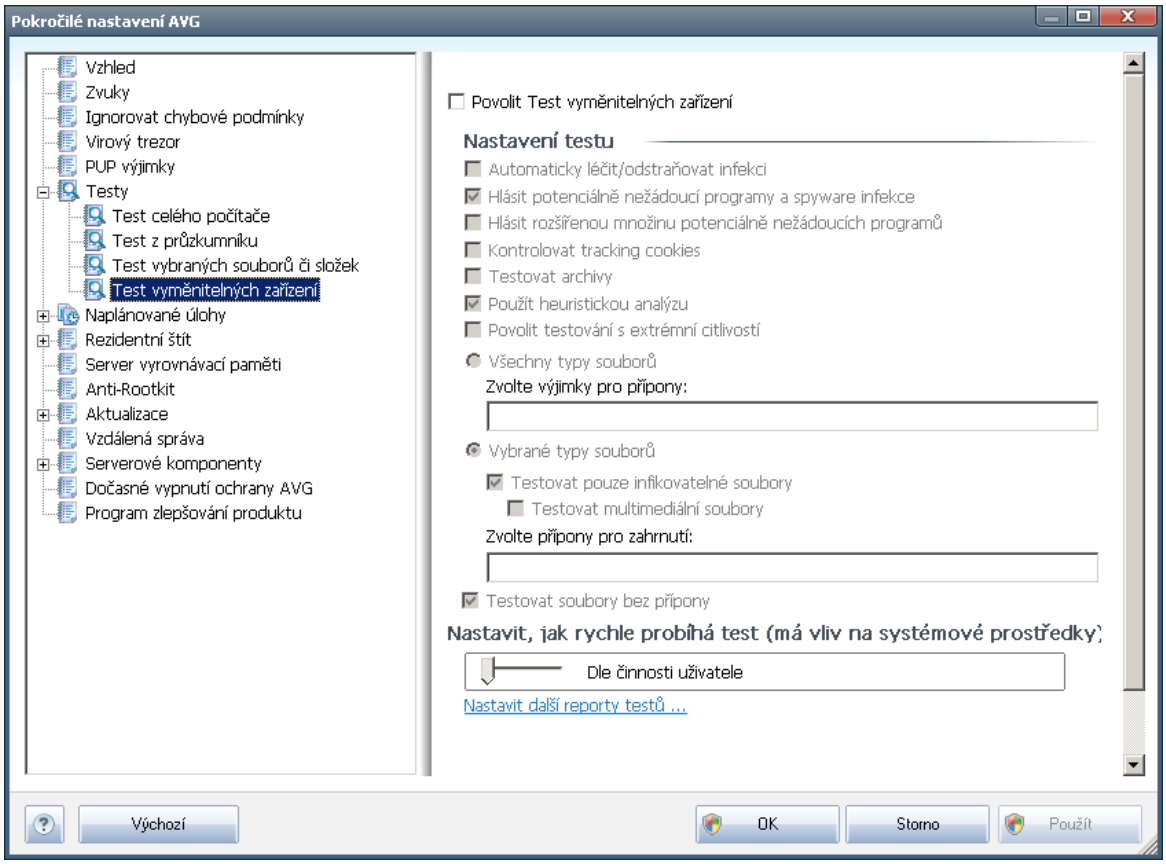


Veškeré parametry nastavené v tomto konfiguračním dialogu se vztahují pouze na ty oblasti vašeho počítače, které jste vybrali pro testování v rámci ***Testu vybraných souborů či složek***!

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

11.6.4. 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***.

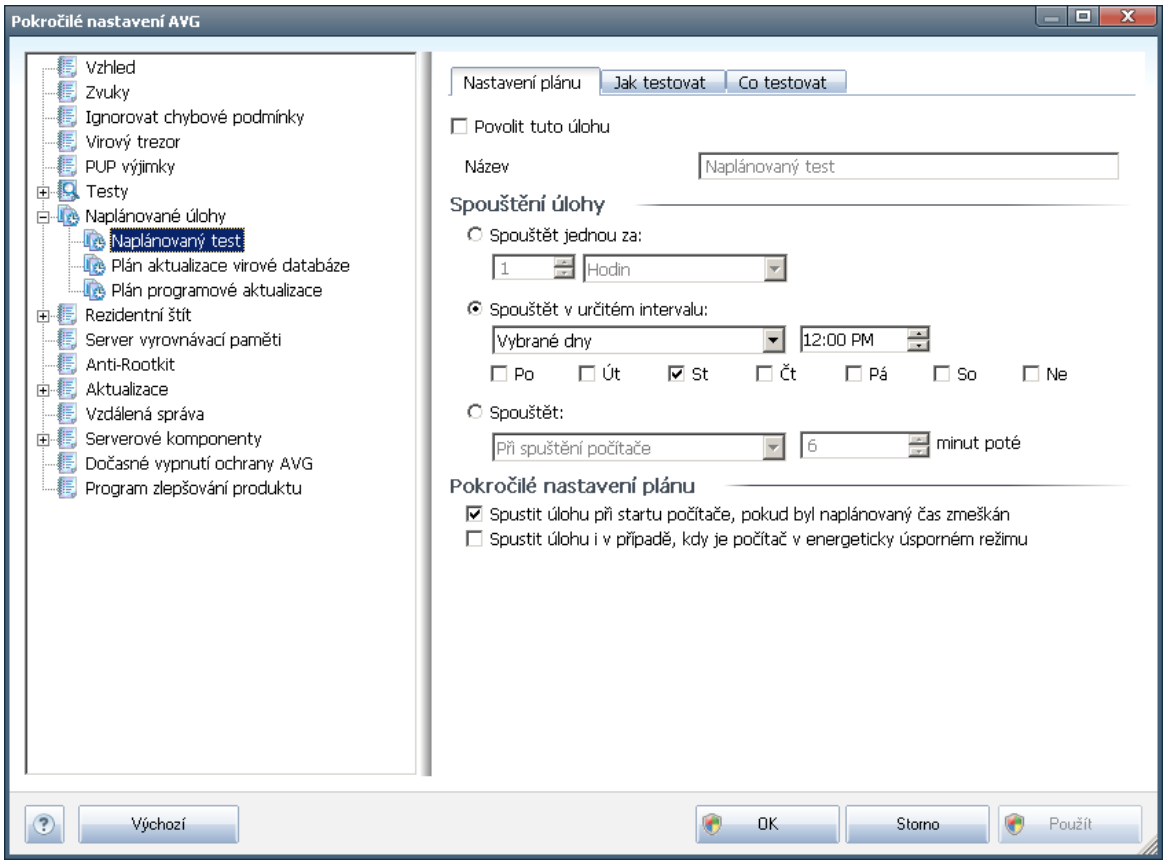
11.7. Naplánované úlohy

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

- Naplánovný test
- Plánu aktualizace virové databáze
- Plánu programové aktualizace

11.7.1. 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:

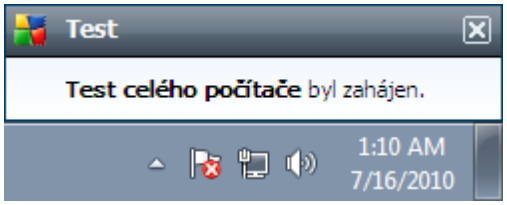
Spouštění úlohy

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***).

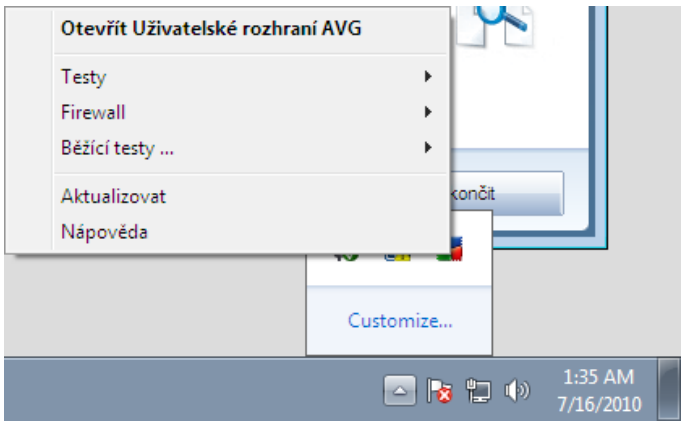
Pokročilé nastavení plánu

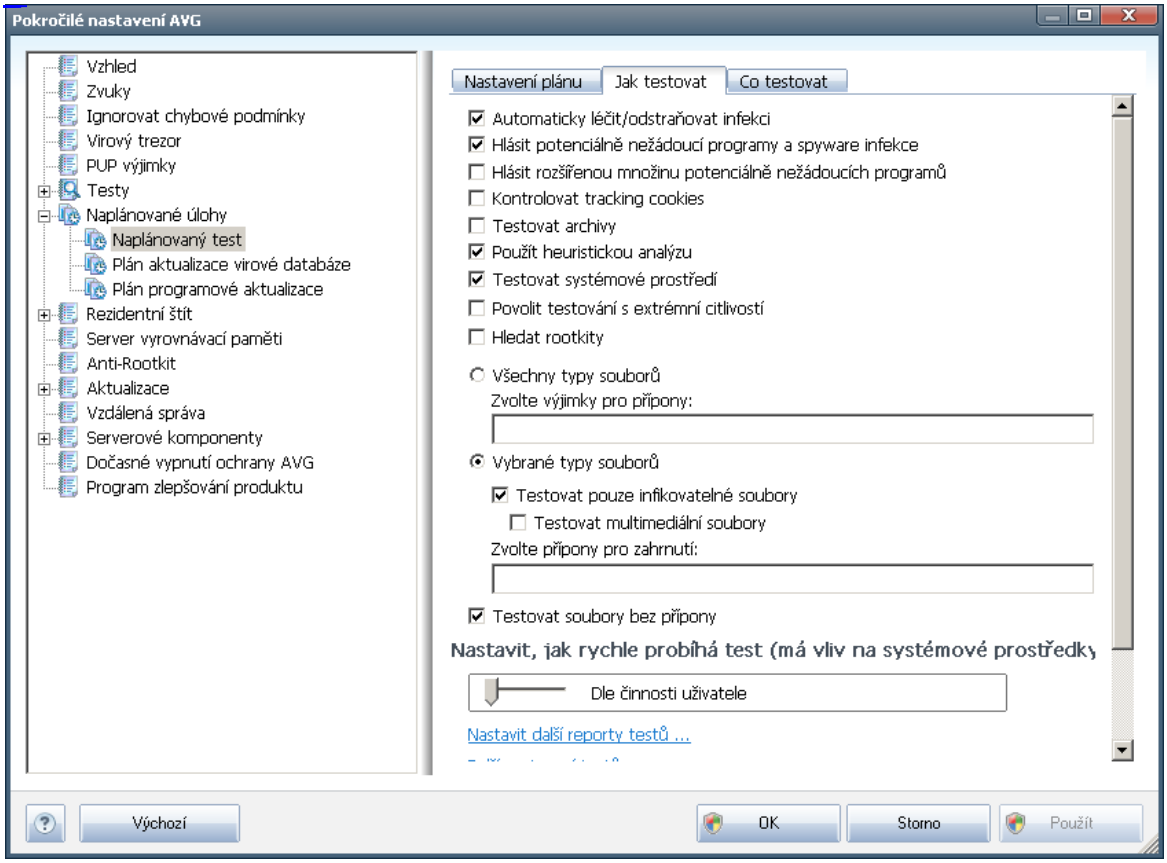
Tato sekce umožňuje definovat podmínky, kdy má či nemá být test spuštěn, jestliže je počítač v úsporném režimu nebo zcela vypnutý a naplánovaný test spuštění testu byl zmeškán.

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 problikávajícím světlem*), která vás informuje o běžícím testu. Kliknutím pravého tlačítka myši nad touto ikonou otevřete kontextové menu, z něhož můžete běžící test pozastavit nebo ukončit, a rovněž změnit prioritu právě probíhajícího testu:





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

- ***Povolit testování s extrémní citlivostí*** (*ve výchozím nastavení vypnuto*) - ve specifických situacích (například při podezření na infekci starším typem viru) můžete zvolit tuto metodu testování, která aktivuje nejdůkladnější testovací algoritmy a velmi podrobně prověří naprosto všechny oblasti vašeho počítače. Mějte však na paměti, že tato metoda je časově velmi náročná.

- ***Hledat rootkity*** (*ve výchozím nastavení vypnuto*): označením této položky zahrnete do testu i možnost detekce 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

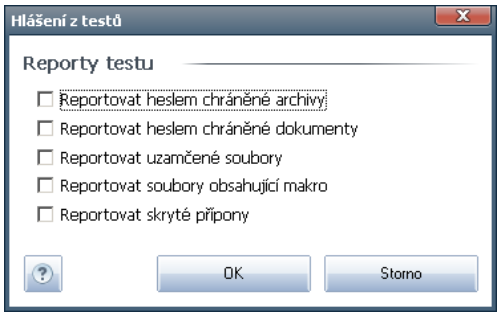
i soubory se skrytou či neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme , abyste se tohoto nastavení podrželi, pokud nemáte skutečný důvod jej měnit. Soubory bez přípon jsou obecně vysoce podezřelé a měly by být otestovány.

Nastavit, jak rychle probíhá test

V sekci ***Priorita testu*** pak můžete nastavit požadovanou rychlost testování v závislosti na zátěži systémových zdrojů. Ve výchozím nastavení je tato hodnota nastavena na úroveň ***Dle činnosti uživatele*** 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.

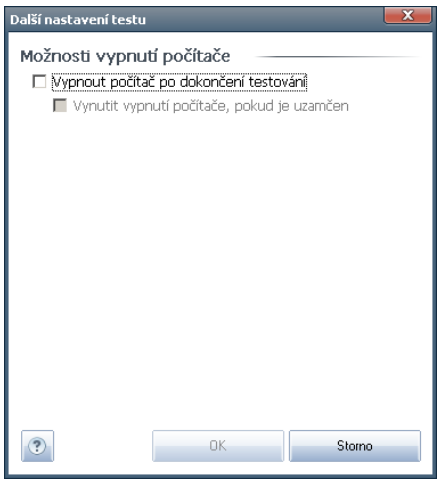
Nastavit další reporty testů

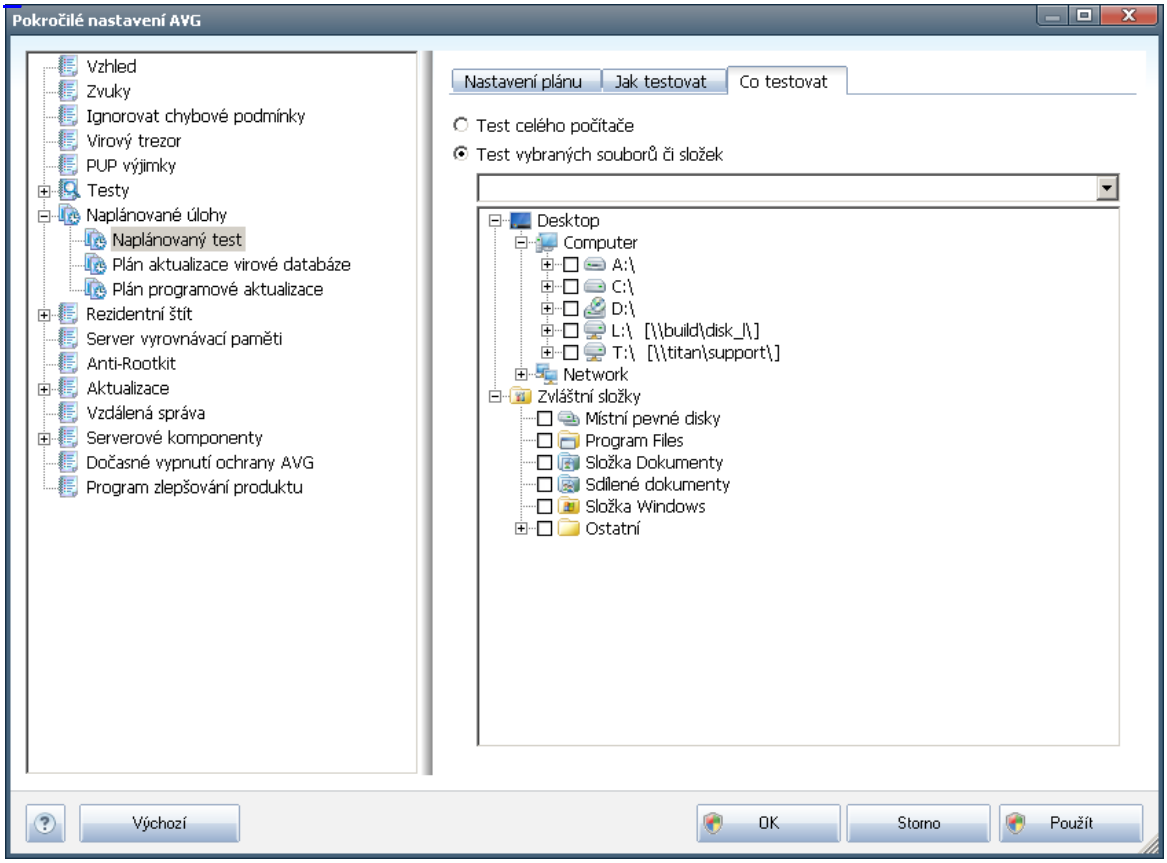
Kliknutím na odkaz ***Nastavit další reporty testů ...*** otevřete samostatné dialogové okno Reporty testů, v němž můžete označením příslušných položek určit situace, jejichž výskyt během testu má být hlášen:



Další nastavení testu

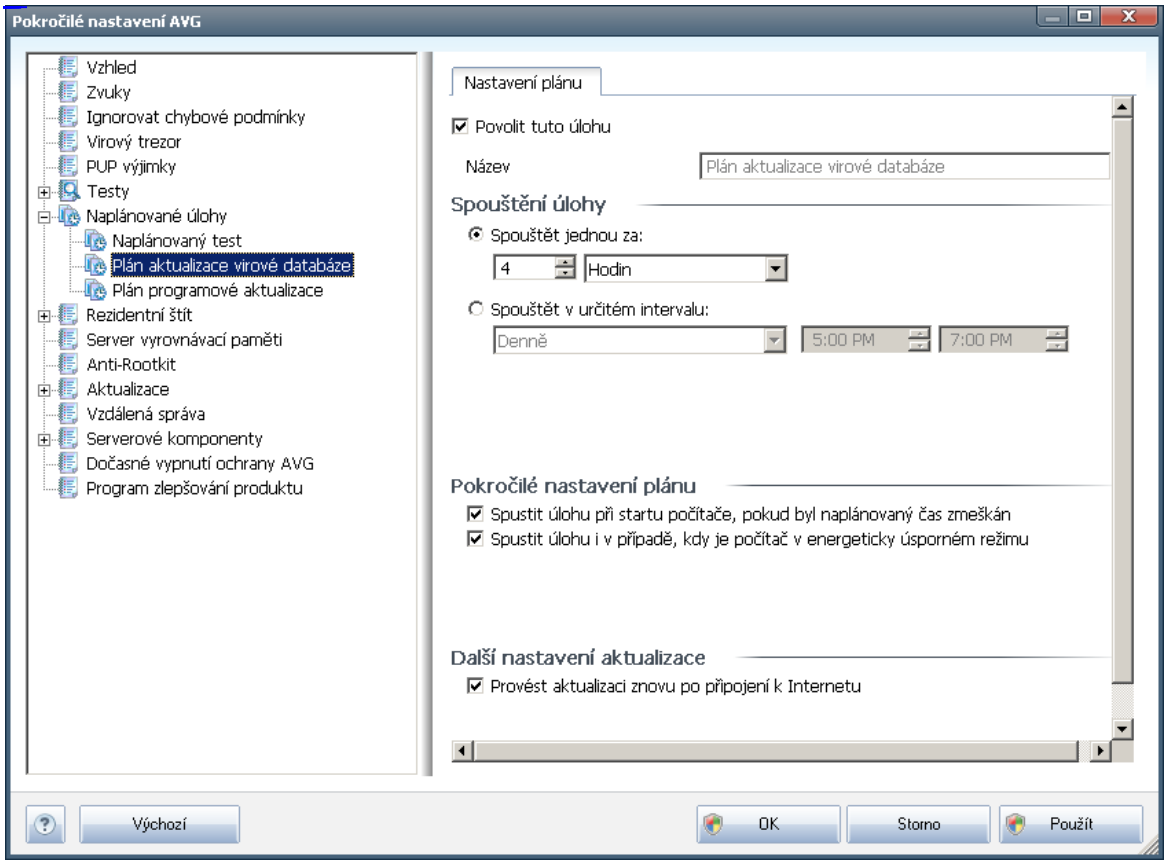
Kliknutím na odkaz ***Další nastavení testu ...*** otevřete nový dialog ***Možnosti vypnutí počítače***, v němž můžete zvolit, zda má být po dokončení spuštěného testu počítač automaticky vypnut. Pokud potvrdíte tuto volbu (***Vypnout počítač po dokončení testování***), aktivuje se současně další možnost,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





Na záložce ***Co testovat*** 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.

11.7.2. 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

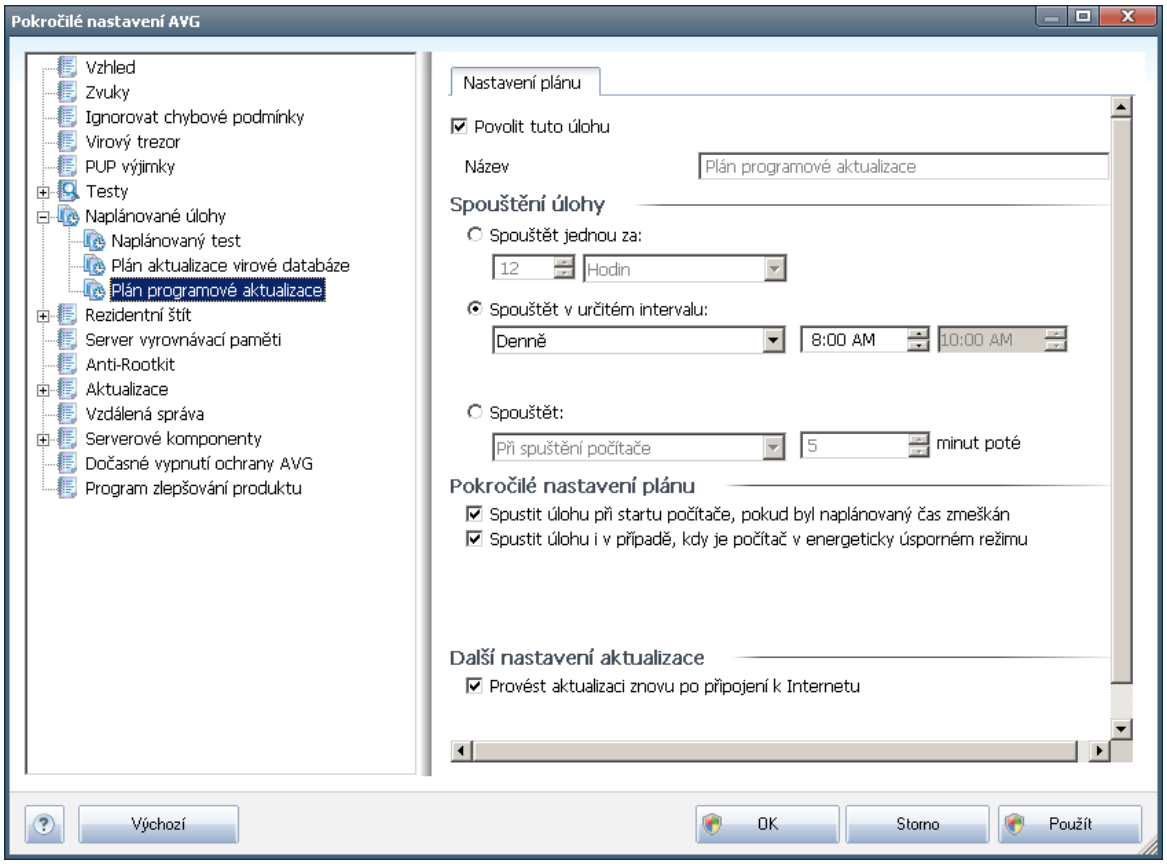
Tato sekce umožňuje definovat podmínky, kdy má či nemá být aktualizace virové databáze spuštěna, jestliže je počítač v úsporném režimu nebo zcela vypnutý a naplánovaný čas spuštění aktualizace byl zmeškán.

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***).

11.7.3. 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

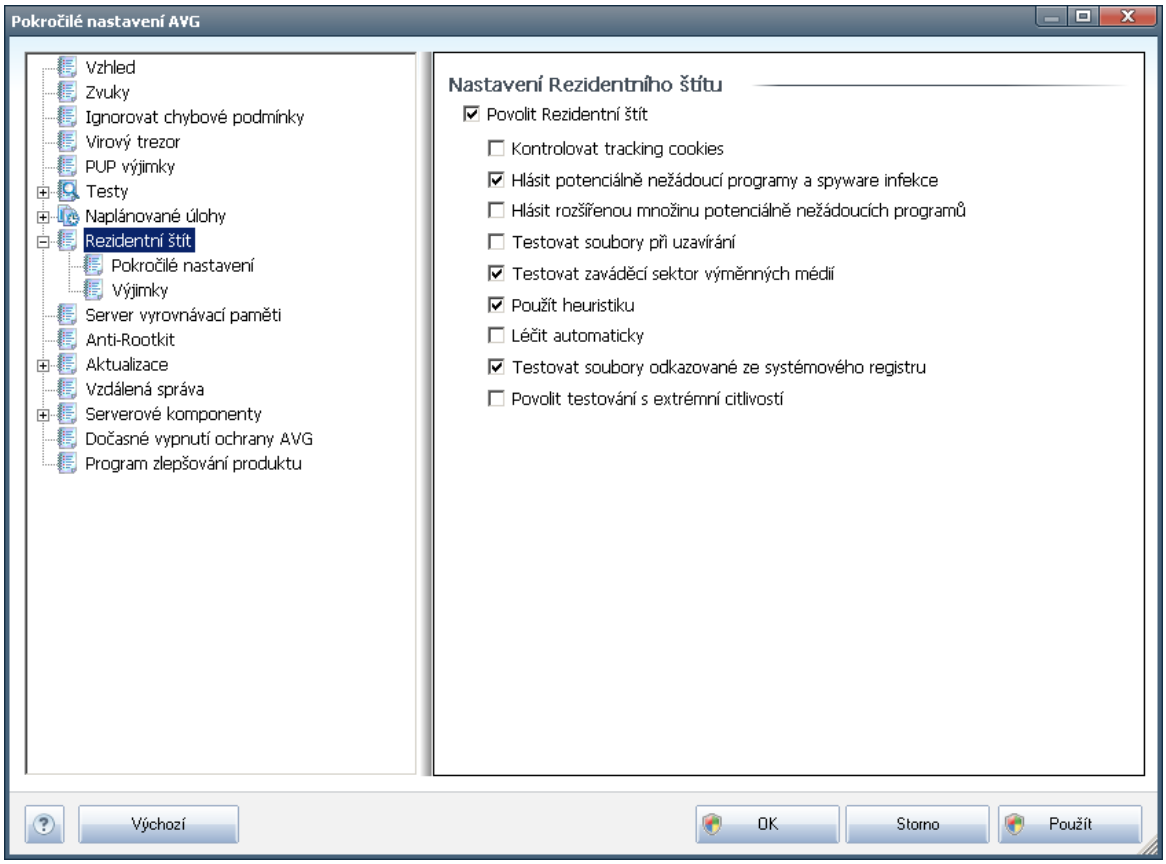
Volbou položky ***Provést aktualizaci znovu po připojení k Internetu*** zajistíte, že pokud dojde během programové aktualizace k problémům s připojením a aktualizace tedy nebude moci být dokončena, bude znovu spuštěna bezprostředně po obnovení připojení.

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.*

11.8. 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*** (*ve výchozím nastavení vypnuto*) - parametr definuje, že mají být detekovány cookies (*HTTP data zaslaná serverem prohlížeči a uložena na počítači uživatele; při každé další návštěvě téhož serveru prohlížeč posílá cookies zpět serveru, který podle nich rozlišuje jednotlivé uživatele*)

- ***Hlásit potenciálně nežádoucí programy a spyware infekce*** (*ve výchozím nastavení zapnuto*) - kontrola přítomnosti potenciálně nežádoucích programů (*spustitelné programy, které mohou fungovat jako spyware nebo adware*). Zaškrtnutím tohoto políčka aktivujete ***Anti-Spyware***, tj. bude se testovat přítomnost spyware, nejen virů. Spyware představuje poněkud problematickou kategorii 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.

- ***Testovat soubory při uzavírání*** (*ve výchozím nastavení vypnuto*) - kontrola souborů při zavírání zajišťuje, že AVG testuje aktivní objekty (např. aplikace, dokumenty, …) nejen při jejich spuštění/otevření, ale také při zavírání; tato funkce pomáhá chránit váš počítač před sofistikovanými viry

- ***Testovat 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*)

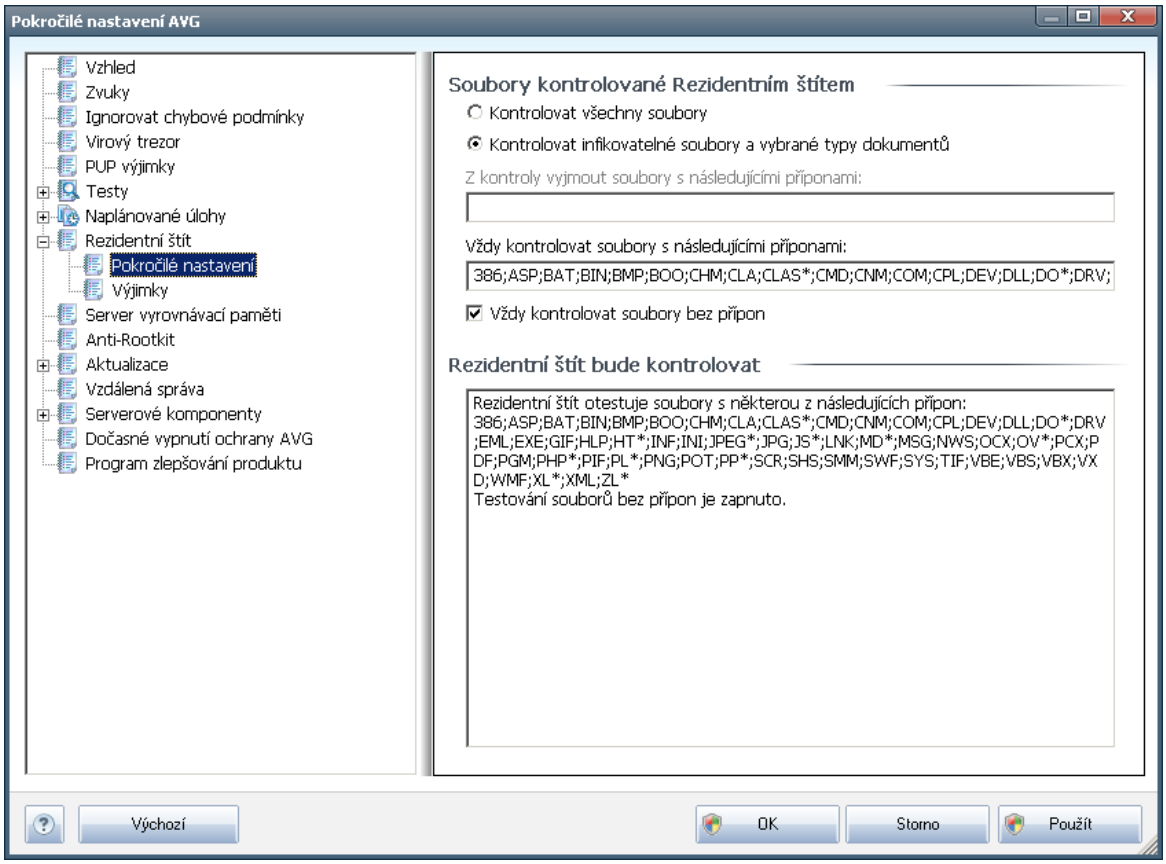
- ***Léčit automaticky*** (*ve výchozím nastavení vypnuto*) - detekovaná infekce bude automaticky vyléčena, jestliže je k dispozici léčba toho konkrétního viru; a všechny infekce, jež nelze vyléčit, budou odstraněny.

- ***Testovat soubory odkazované ze systémového registru*** (*ve výchozím nastavení zapnuto*) - AVG bude testovat všechny spustitelné soubory přidané do systémového registru, aby tak zabránil možnému spuštění již známé infekce při přístím startu počítače.

- ***Povolit testování s extrémní citlivostí*** (*ve výchozím nastavení vypnuto*) - ve specifických situacích (*mimořádný stav ohrožení počítače*) můžete zvolit tuto metodu kontroly, která aktivuje nejdůkladnější a nejpodrobnější testovací algoritmy. Mějte však na paměti, že tato metoda je časově velmi náročná.

11.8.1. Pokročilé nastavení

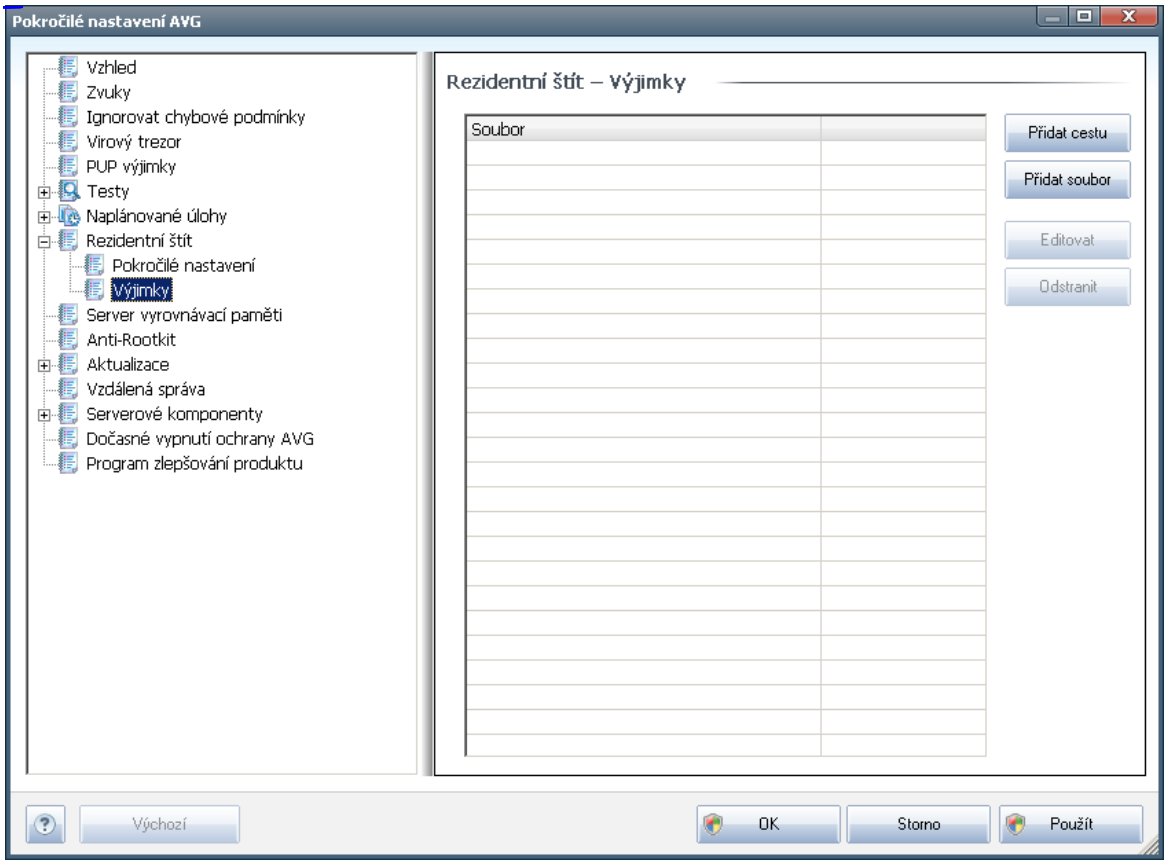
V dialogu ***Soubory kontrolované Rezidentním štítem*** máte možnost nastavení kontroly souborů a dokumentů vybraných typů (*konkrétních přípon*):



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.

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

11.8.2. Výjimky



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

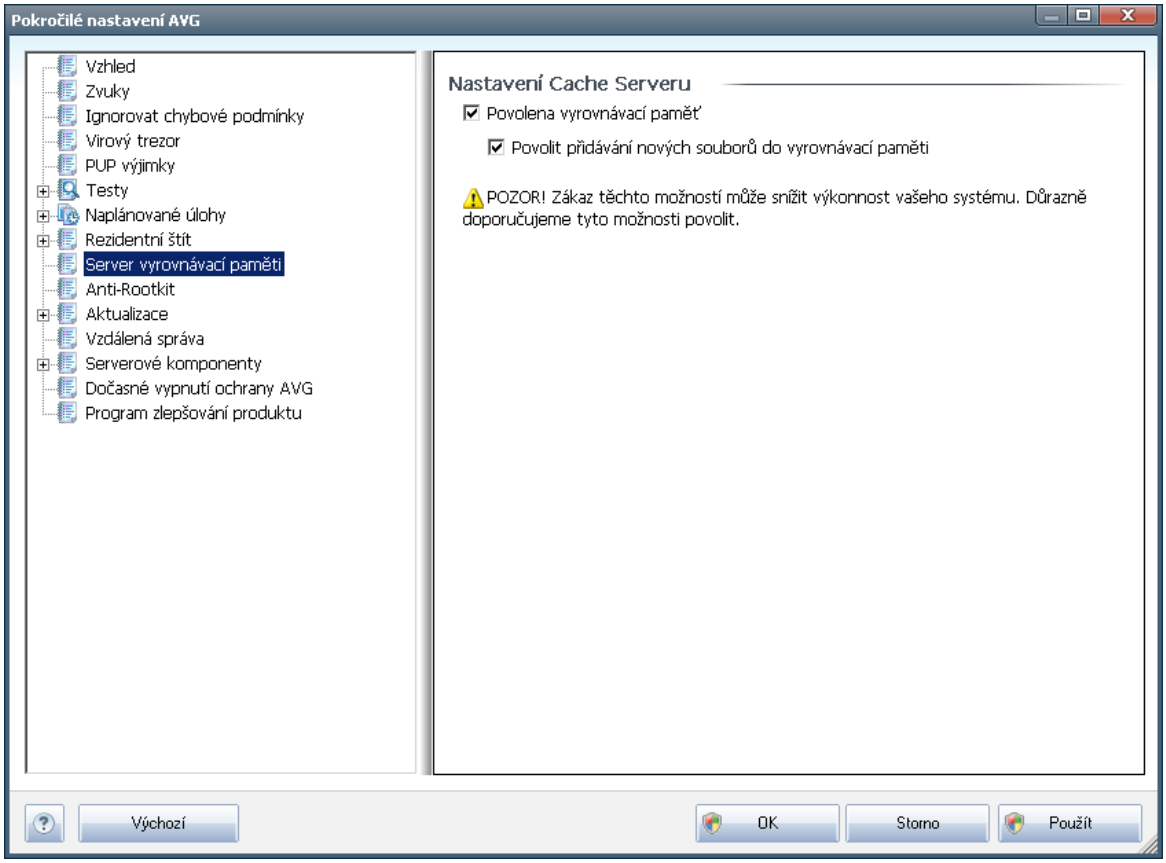
Pokud to není nezbytně nutné, důrazně doporučujeme, abyste z testování žádné položky nevyjímali!

V dialogu jsou k dispozici tato ovládací tlačítka:

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

11.9. 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 File Server 2011** 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.



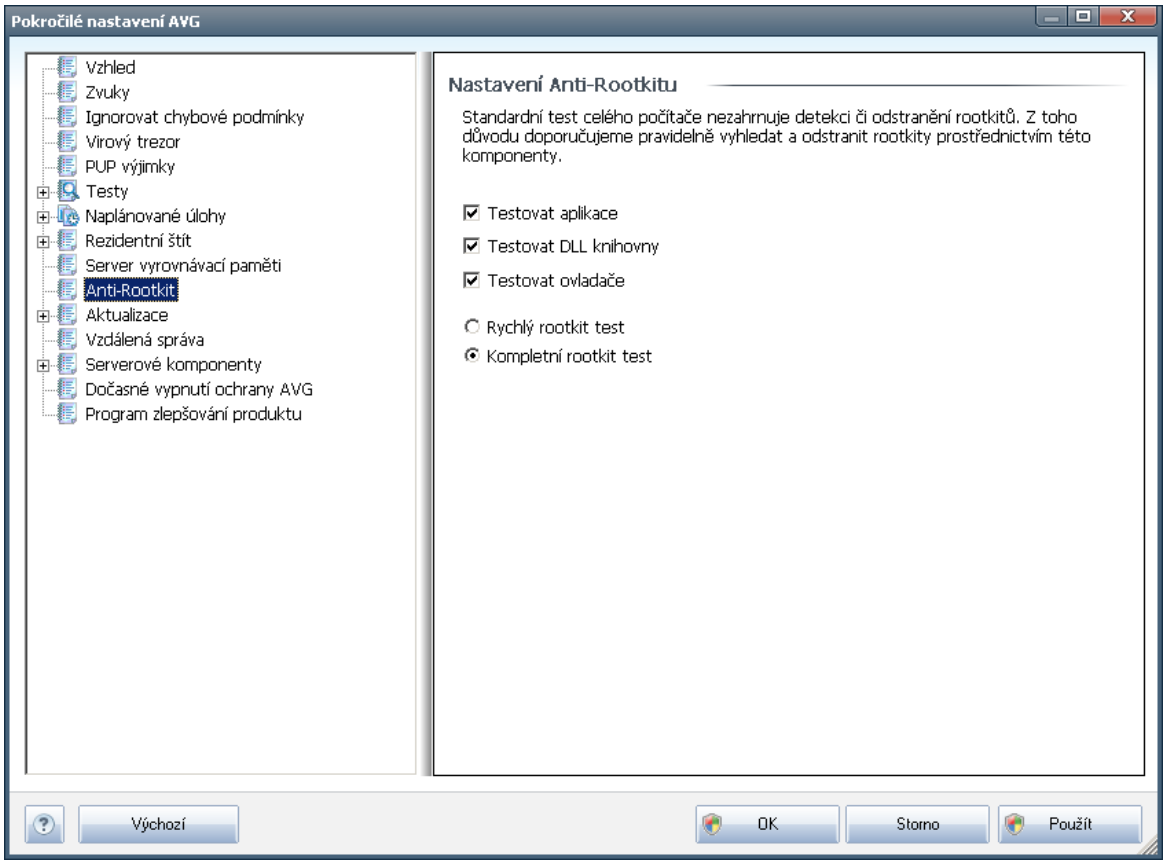
Dialog nastavení nabízí dvě možnosti:

- ***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.

11.10. 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:

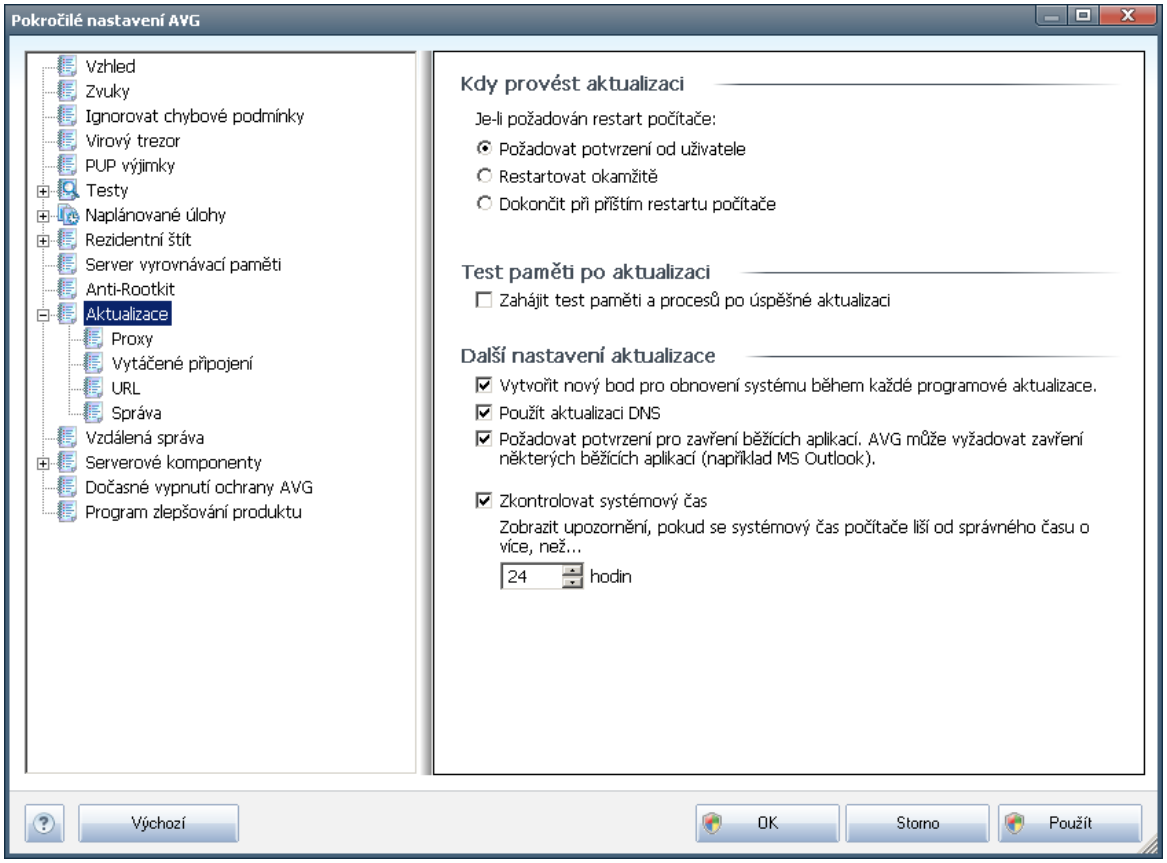
- ***Testovat aplikace***
- ***Testovat DLL knihovny***
- ***Testovat ovladače***

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*)

11.11. 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:

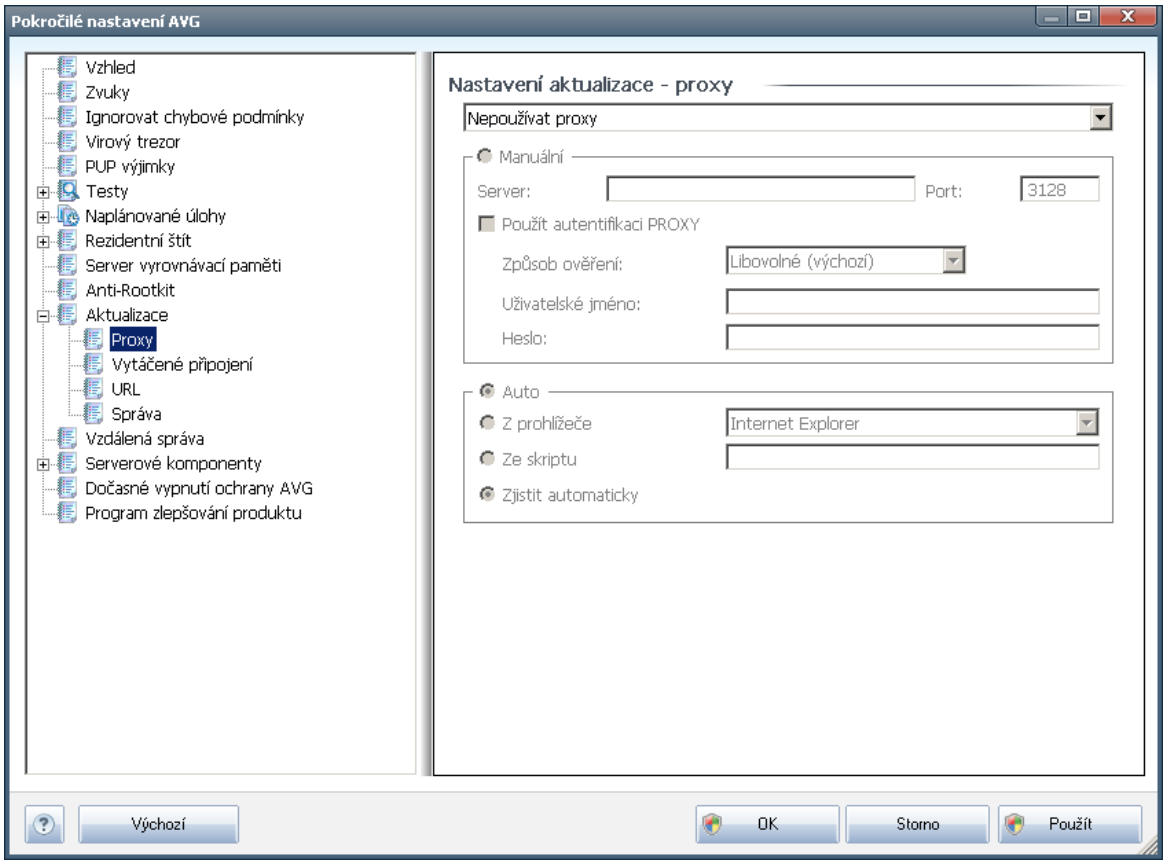
- ***Po každé programové aktualizaci vytvořit nový bod pro obnovení systému*** - před každým spuštěním programové aktualizace AVG je tak zvaný systémový bod pro obnovení systému. V případě, že aktualizační proces nebude z nějakého důvodu dokončen a váš operační systém bude ohrožen, můžete za pomoci tohoto 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.

11.11.1. 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*)

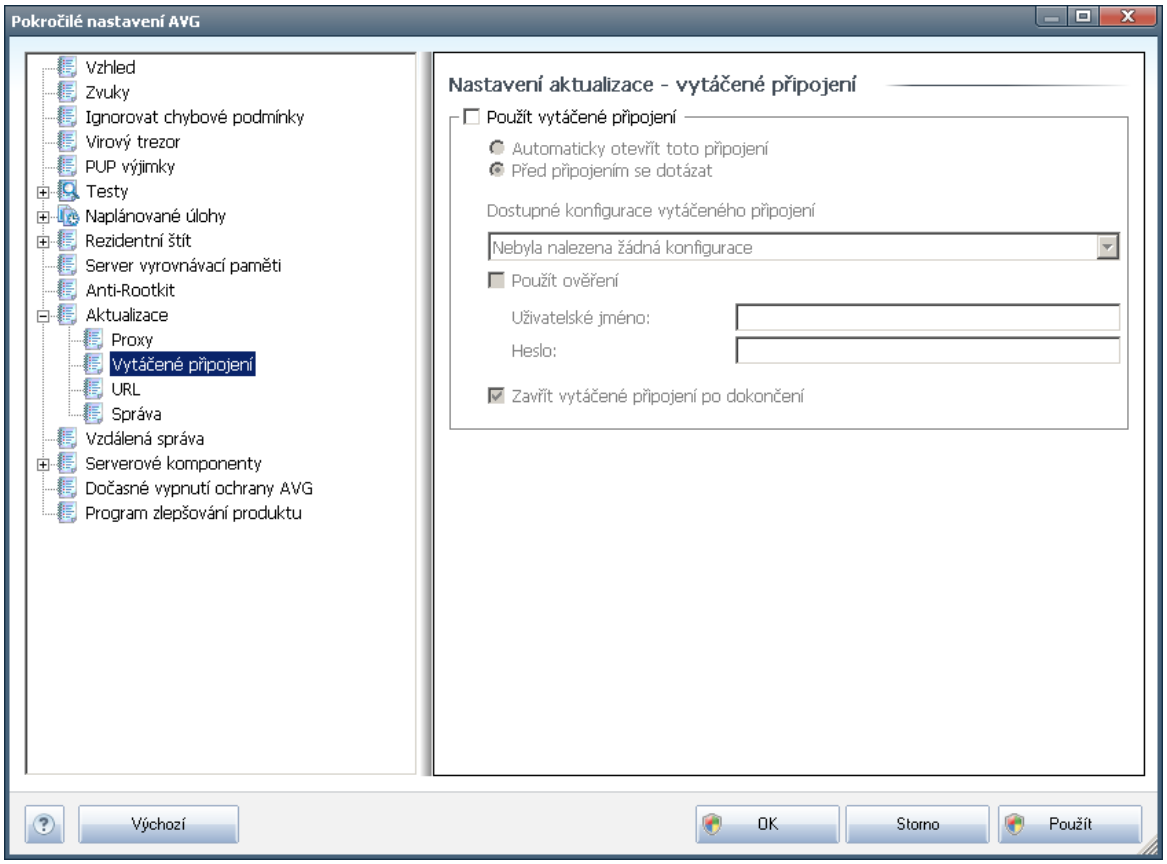
Proxy server může mít dále nastavena různá přístupová práva pro jednotlivé uživatele. Jestliže je váš proxy server takto nastaven, označte položku ***Použít autentifikaci PROXY*** a zadejte své ***Uživatelské jméno*** a ***Heslo*** pro připojení k internetu přes proxy server.

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

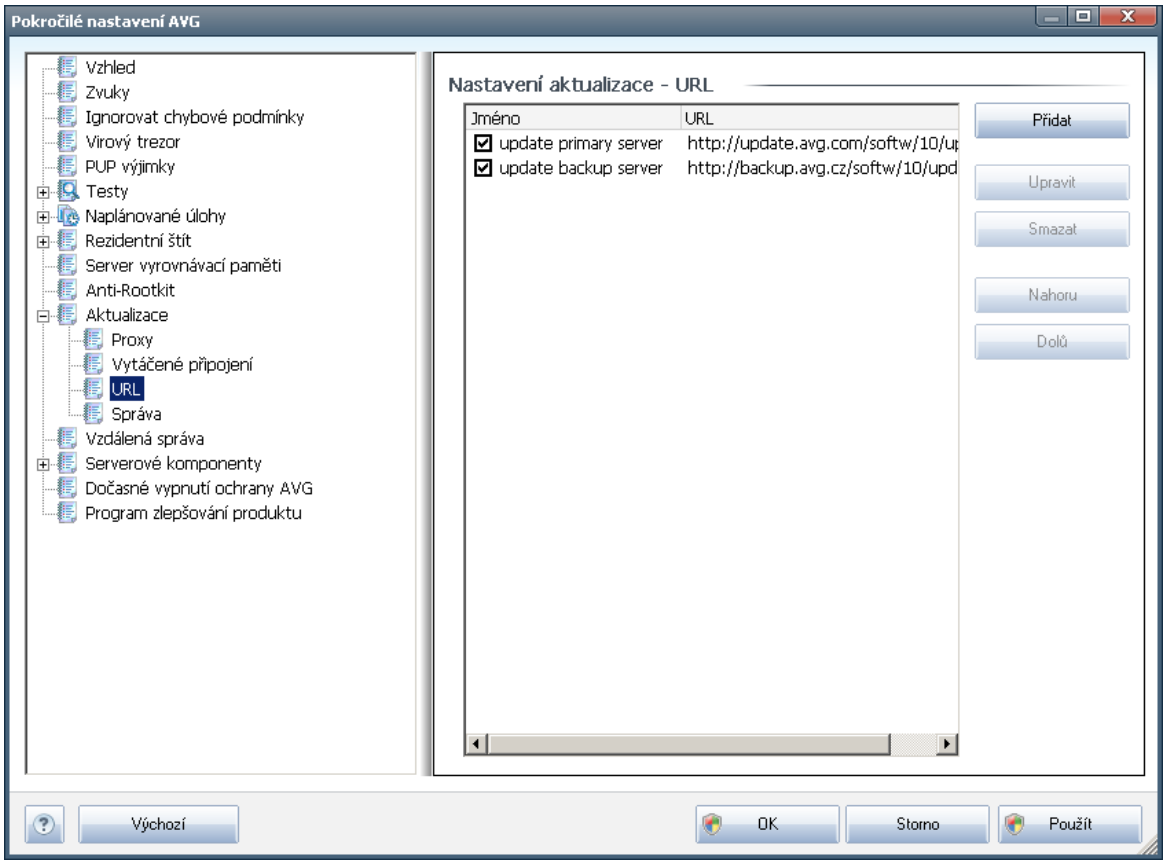
11.11.2. Vytáčené připojení



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***).

11.11.3. URL

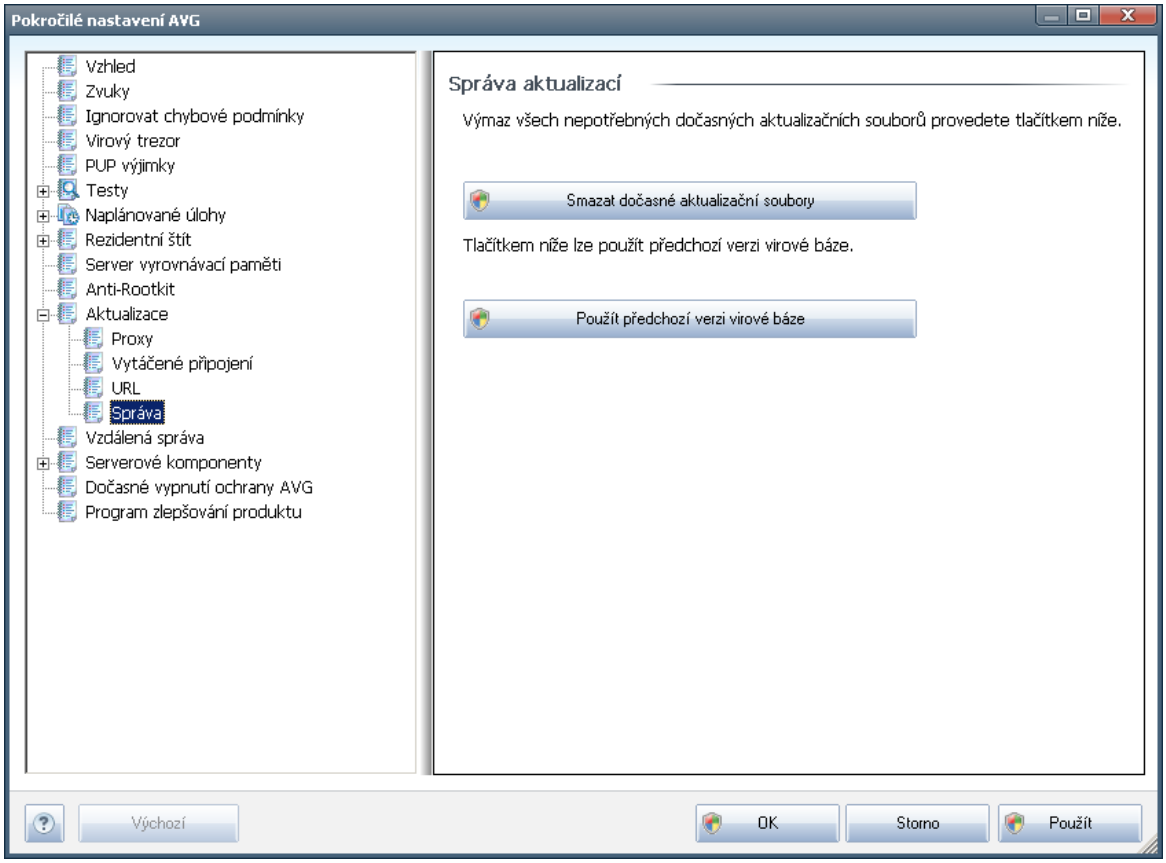


Dialog ***URL*** nabízí seznam internetových adres, odkud mohou být aktualizační souboru staženy. Seznam a jeho jednotlivé položky lze editovat pomocí následujících ovládacích tlačítek:

- ***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

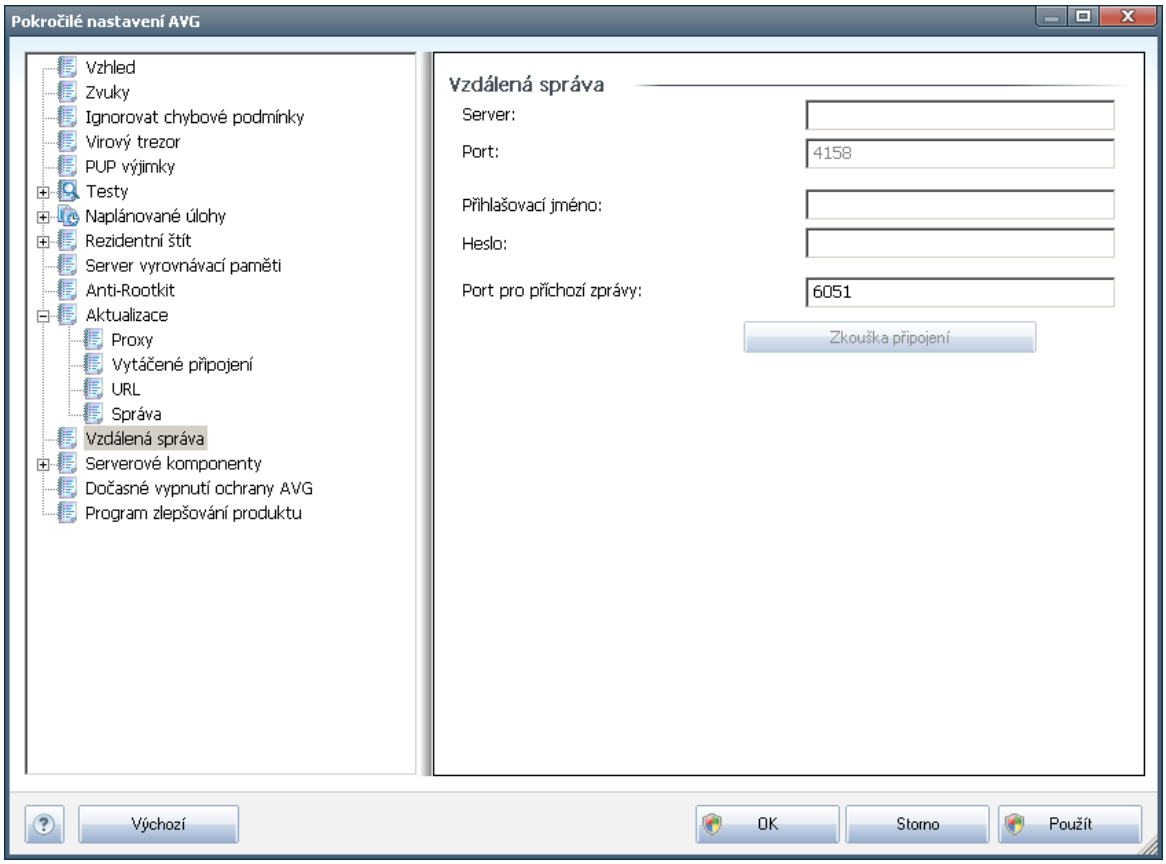
11.11.4. Správa

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*)

11.12. Vzdálená správa



Nastavení v dialogu ***Vzdálená správa*** slouží k připojení klientské stanice AVG do systému vzdálené správy. Pokud plánujete připojení ke vzdálené správě, nastavte prosím tyto parametry:

- ***Server*** - jméno (*případně IP adresa*) serveru, na němž je nainstalován AVG Admin Server
- ***Port*** - uveďte číslo portu, na němž komunikuje AVG Admin Server s AVG klientem (*za výchozí nastavení je považován port číslo 4158 - pokud používáte tento port, není třeba hodnotu specifikovat*)
- ***Přihlašovací jméno*** - pokud je komunikace mezi AVG klientem a AVG Admin Serverem definována jako zabezpečená, zadejte své přihlašovací jméno ...
- ***Heslo*** - ... a příslušné heslo
- ***Port pro příchozí zprávy*** - číslo portu, na němž AVG klient přijímá zprávy od AVG Admin Serveru

Tlačítko ***Zkouška připojení*** slouží k ověření skutečnosti, že všechny v tomto dialogu uvedené údaje jsou platné, byly nastaveny správně a je možné se jejich

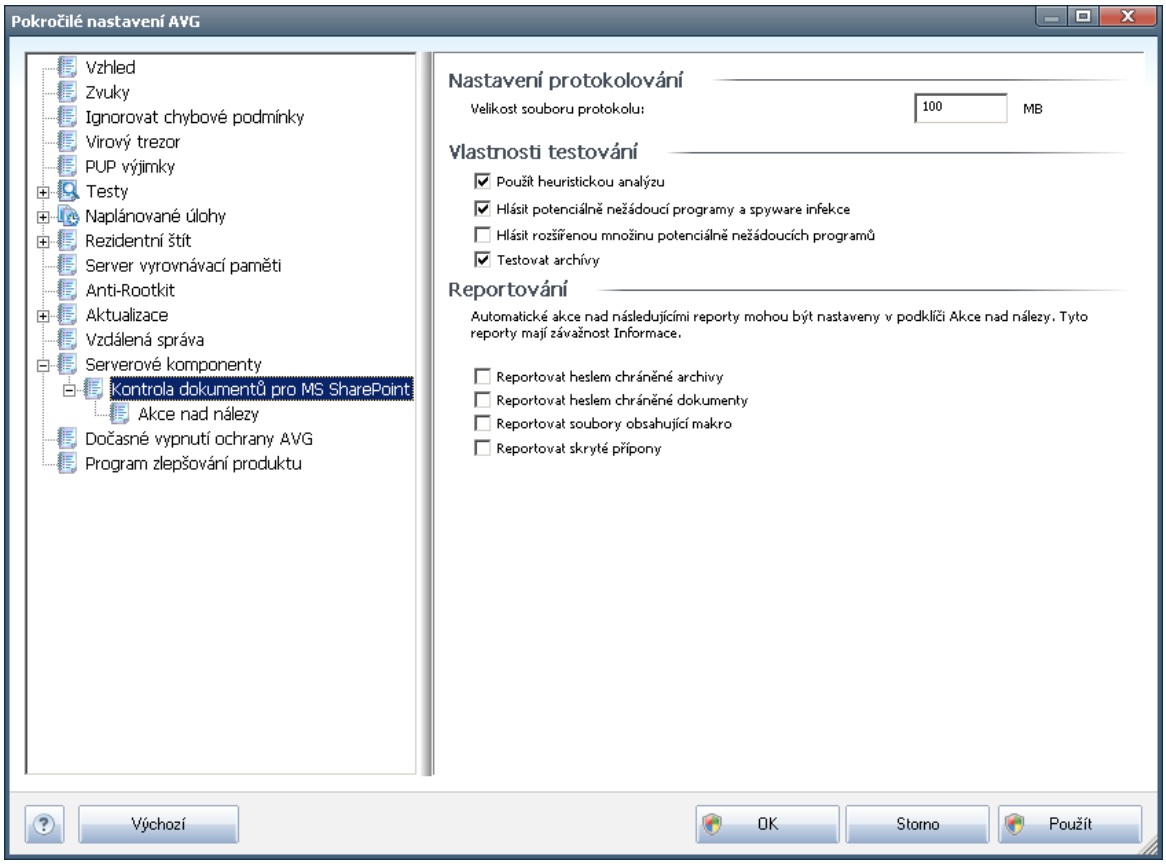
prostřednictvím připojit k DataCenter.

Poznámka: *Pro podrobné informace o vzdálené správě si prosím přečtěte dokumentaci k SMB edici AVG.*

11.13. Serverové komponenty

11.13.1. Kontrola dokumentů pro MS SharePoint

V tomto dialogu pokročilého nastavení můžete upravovat některé parametry testování dokumentů, prováděného serverovou komponentou ***Kontrola dokumentů pro MS SharePoint***. Je rozdělen na několik sekcí:



Nastavení protokolování

Textové pole **Velikost souboru protokolu** – soubor protokolu obsahuje záznamy o rozličných událostech, spojených s činností komponenty ***Kontrola dokumentů pro MS SharePoint***. Mezi tyto události patří například nahrávání knihoven, nalezení viru, zprávy a varování o možných problémech apod. S pomocí textového políčka můžete nastavit maximální velikost tohoto souboru.

Vlastnosti testování

- ***Použít heuristickou analýzu*** – použít heuristiku při testování dokumentů. Když je tato možnost aktivována, můžete filtrovat dokumenty nejen podle přípony, ale i podle skutečného obsahu a formátu (který příponě nemusí odpovídat).

- ***Hlásit potenciálně nežádoucí programy a spyware infekce*** – použít mechanismus Anti-Spyware, tj. detekovat a hlásit rovněž podezřelé a potenciálně nežádoucí programy při testování dokumentů.

- ***Hlásit rozšířenou množinu potenciálně nežádoucích programů*** - zaškrtnutím tohoto políčka aktivujete detekci rozšířené sady spyware: programů, které jsou v původní podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům, případně jde o zásadně neškodné, avšak poněkud obtěžující programy (různé doplňky do prohlížeče atd.). 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. Tato detekce je doplňkem předchozí možnosti, samostatně tedy není dostačující: pokud chcete ochranu před základními typy spyware, pak ponechte vždy označené předchozí políčko, a toto pak označte volitelně k němu.

- ***Testovat archivy*** – testovat obsah archivů.

Reportování

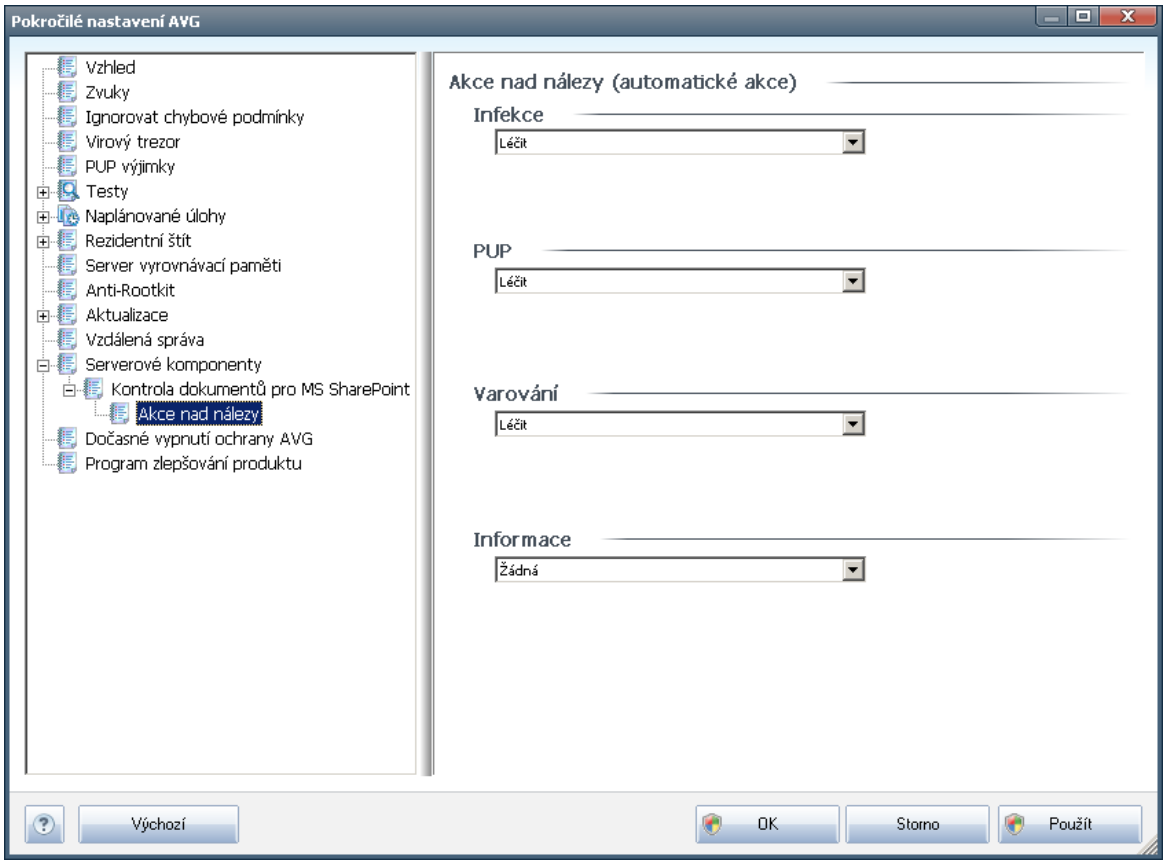
- ***Reportovat heslem chráněné archivy*** – archivy (ZIP, RAR etc.) chráněné heslem není možné otestovat na přítomnost virů; po zaškrtnutí tohoto políčka se tyto archívy budou označovat jako potenciálně nebezpečné.

- ***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.

11.13.2. Akce nad nálezy



V tomto dialogu můžete nastavit, jak se bude komponenta ***Kontrola dokumentů pro MS SharePoint*** chovat, když nalezne hrozbu. Hrozby jsou pro účely této komponenty rozděleny do několika kategorií:

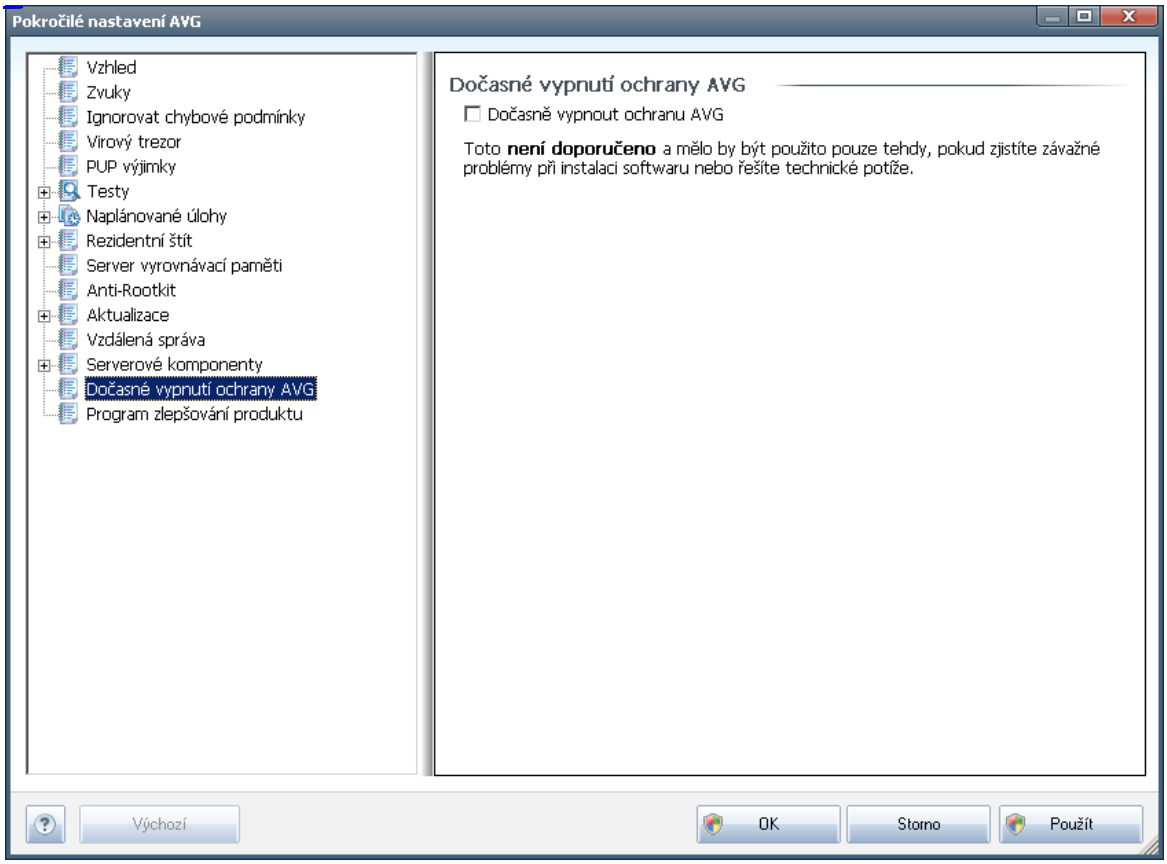
- ***Infekce*** – nebezpečné kódy, které se kopírují a šíří se, často nepozorovaně, aby napáchaly škody v systému uživatele.
- ***PUP (Potenciálně nežádoucí programy)*** – různé druhy progarmů, které mohou, ale také nemusí představovat hrozbu.
- ***Varování*** – nalezené objekty, které nebylo možno otestovat.
- ***Informace*** – zahrnuje všechny nalezené potenciální hrozby, které však nelze zařadit do žádné z výše uvedených kategorií.

S pomocí rolovacích nabídek můžete stanovit automatickou akci pro každou z těchto kategorií:

- ***Žádná*** – dokument, v němž bude nalezena tato hrozba, bude ponechán ve svém umístění.

- ***Léčit*** - AVG se pokusí nalezenou hrozbu vyléčit.
- ***Přesunout do trezoru*** – každý takto infikovaný dokument bude přesunut do karanténního prostředí Virového trezoru.
- ***Odstranit*** – každý dokument, v němž bude detekována tato hrozba, bude automaticky smazán.

11.14. Dočasné vypnutí ochrany AVG



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

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

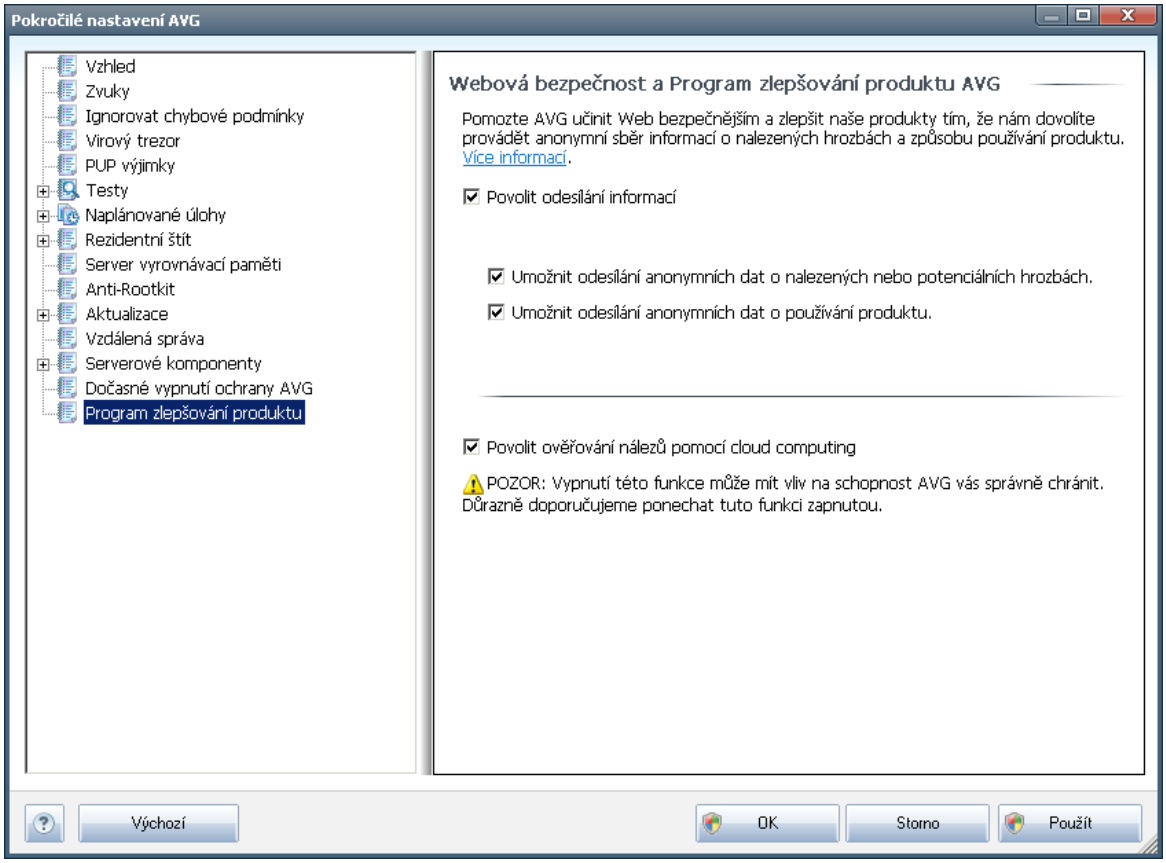
V naprosté většině případů ***není nutné*** deaktivovat AVG před instalací nového software nebo ovladačů, a to ani tehdy, pokud budete během instalace vyzváni k zavření všech spuštěných aplikací. Pokud by v takovém případě došlo ke kolizi, pravděpodobně bude stačit deaktivovat ***Rezidentní štít***.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

vysoce zranitelný.

11.15. Program zlepšování produktu

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

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



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

- ***Virus*** je kód, který dokáže sám sebe kopírovat a šířit, často zcela nepozorovaně, dokud nenadělá spoustu škody. Některé viry představují vážnou hrozbu, napadají soubory, mění je a vymazávají z disku, jiné dělají věci na první pohled celkem neškodné, například přehrávají nějakou hudbu. Nebezpečné jsou však všechny viry, a to kvůli základní vlastnosti nekontrolovatelného množení – i jednoduchý virus se dokáže během chvilky namnožit tak, že zabere veškerou paměť a způsobí pád systému.

- ***Červ*** je typ viru, který však na rozdíl od běžných virů nepotřebuje ke svému šíření jiný objekt; rozesílá sám sebe na další počítače zcela bez pomoci, nejčastěji elektronickou poštou, a tak způsobuje přetížení sítí a e-mailových serverů.

- ***Spyware*** je obvykle definován jako typ malware (*malware = anglická zkratka pro "malicious software", tj. škodlivé programy obecně*) a většinou zahrnuje především programy – nejčastěji tzv. *trojské koně* určené k odcizení osobních informací, hesel, čísel kreditních karet a podobně, případně k proniknutí do počítače za účelem poskytnutí přístupu cizí osobě; samozřejmě to vše bez vědomí vlastníka počítače.

- ***Potenciálně nežádoucí programy*** (*z anglického Potentially Unwanted Programs = PUP*) jsou typem spyware, který představuje potenciální riziko pro váš počítač. Příkladem PUP může být adware, to je program určený k distribuci reklamy. Ten se většinou projevuje tak, že zobrazuje v internetovém prohlížeči vyskakovací okna s reklamou, což je sice otravné, ale ne skutečně ohrožující.

- ***Sledovací cookies*** lze rovněž považovat za druh spyware, jelikož tyto malé soubory, uložené ve vašem internetovém prohlížeči a posílané nazpět "mateřské" webové stránce, kdykoli se na ni znovu připojíte, mohou obsahovat různé osobní informace, například seznam stránek, na které jste se v poslední době dívali, a podobně.

- ***Exploit*** je škodlivý kód, který využívá chyby nebo bezpečnostní skuliny v operačním systému, internetovém prohlížeči nebo jiném často používaném programu.

- ***Phishing*** je pokus, jak získat citlivá data vydáváním se za důvěryhodnou instituci. Potenciální oběti jsou obvykle kontaktovány hromadným e-mailem obsahujícím výzvu k aktualizaci bankovních údajů (*jinak bude konto uzavřeno...*) a následuje odkaz na webovou stránku příslušné banky, která mnohdy vypadá velmi věrně, ale je samozřejmě falešná.

- ***Hoaxy*** jsou řetězové podvodné nebo poplašné e-maily obsahující například falešné nabídky práce, případně nabídky, které pracovníky zneužijí k nelegálním aktivitám, výzvy k vybrání velké sumy peněz, podvodné loterie a podobně.

- ***Nebezpečné webové stránky*** dokáží nepozorovaně instalovat škodlivé programy do vašeho počítače, a stránky napadené hackery dělají totéž, jen se jedná o stránky původně slušné a neškodné, které se však po útoku hackerů chovají zcela nepředvídatelně.

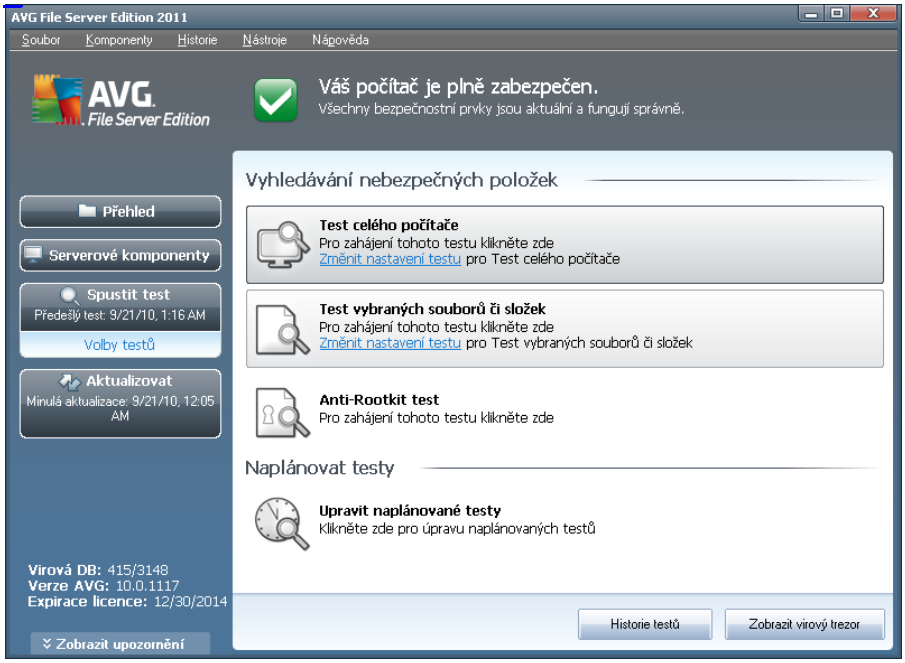
Systém AVG obsahuje ochranu proti všem zmíněným typům hrozeb a škodlivých programů:

- ***Anti-Virus*** chrání váš počítač před viry,
- ***Anti-Spyware*** chrání váš počítač před spyware.

12. AVG testování

Testování je elementární součástí **AVG File Server 2011**. 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 File Server 2011** je testování na vyžádání. Testy na vyžádání jsou navrženy tak, že mohou testovat různé části vašeho počítače, kdykoliv se objeví podezření na možnost virové infekce. V každém případě však doporučujeme provádět testy pravidelně, i když považujete váš počítač za zcela viru prostý.

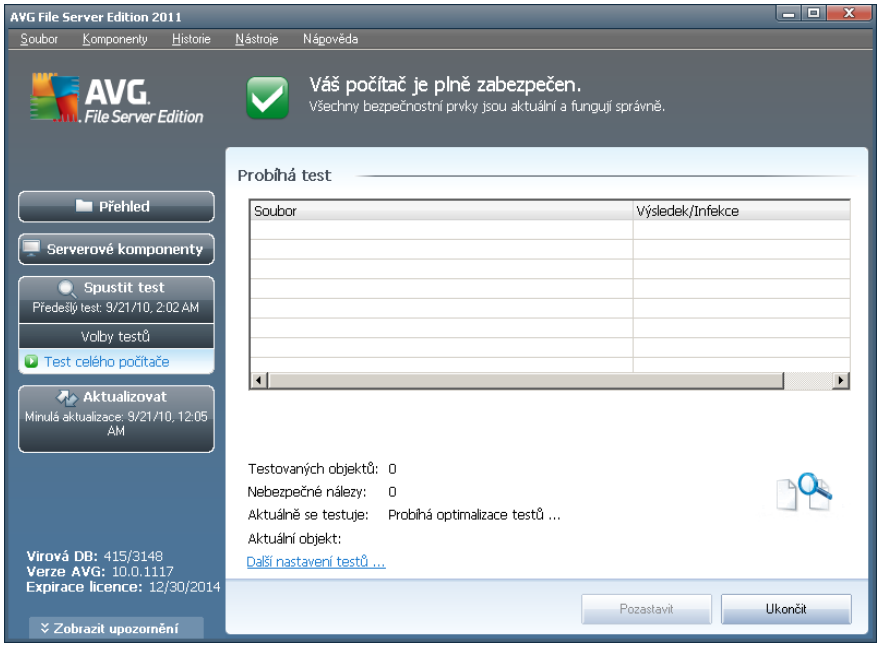
V **AVG File Server 2011** najdete tyto typy výrobcem nastavených testů:

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.

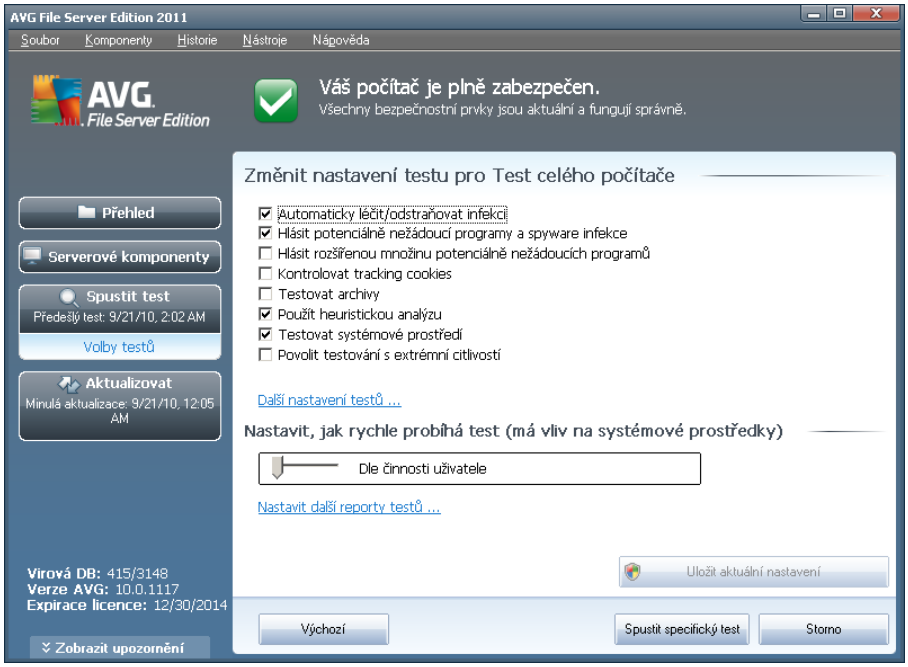
Spuštění testu

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:

    - ***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*).

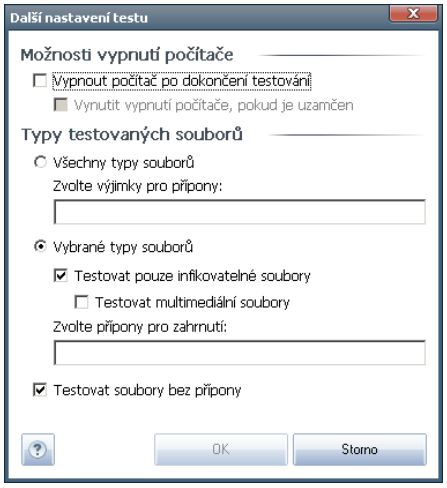
- **Testovat archivy** (*ve výchozím nastavení vypnuto*) - parametr definuje, že test má kontrolovat všechny soubory zabalené v některém typu archivu, například ZIP, RAR, ...

- **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.

- **Povolit testování s extrémní citlivostí** (*ve výchozím nastavení vypnuto*) - ve specifických situacích (*například při podezření na infekci starším typem viru*) můžete zvolit tuto metodu testování, která aktivuje nejdůkladnější testovací algoritmy a velmi podrobně prověří naprosto všechny oblasti vašeho počítače. Mějte však na paměti, že tato metoda je časově velmi náročná.

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



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

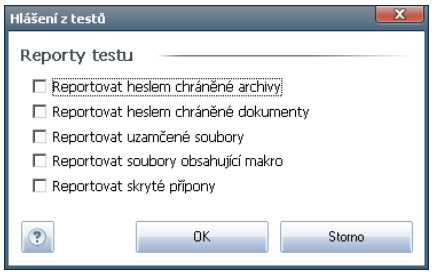
  - ***Vybrané typy souborů*** - můžete se rozhodnout, že chcete, aby se testy spouštěly pouze nad soubory, které lze považovat za infikovatelné (*soubory, které nemohou být infekcí zasaženy, se testovat nebudou - například prosté textové soubory nebo některé nespustitelné soubory*), a to včetně multimediálních 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.

- ***Nastavit, jak rychle probíhá test*** - posuvníkem lze změnit prioritu testu, která je ve výchozím nastavení na hodnotě ***Dle činnosti uživatele***. Tato 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

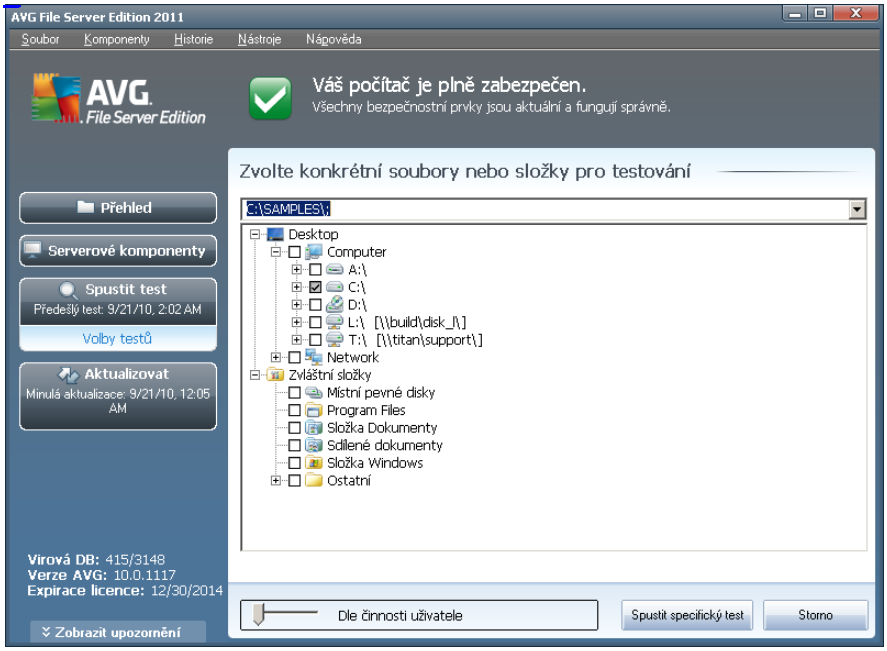
Test vybraných souborů či složek kontroluje pouze uživatelem definované oblasti počítače (*zvolené složky, pevné disky, diskety, CD, optické disky, …*). Postup při nálezu a léčbě/odstraňování virové nákazy je stejný jako u ***Testu celého počítače***: nalezené viry jsou vyléčeny nebo přesunuty do ***Virového 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.

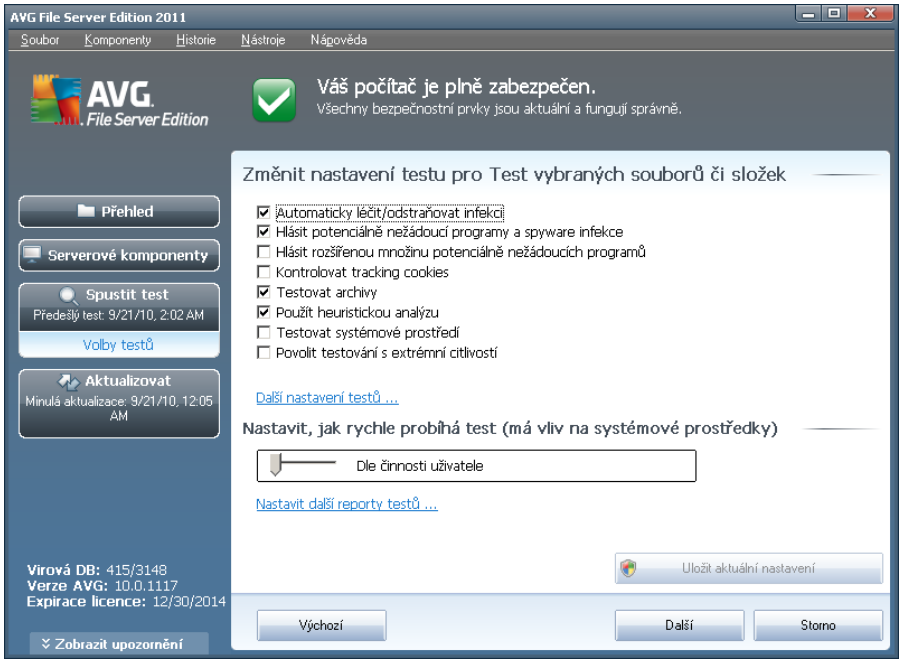
Pokud si přejete zkontrolovat určitý adresář bez kontroly všech v něm obsažených podadresářů, napište před automaticky vygenerovanou cestu k adresáři znaménko "**-**". Parametrem "!" před cestou k adresáři zase určíte, že celý adresář má být z testu vypuštěn.

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



Editace nastavení testu

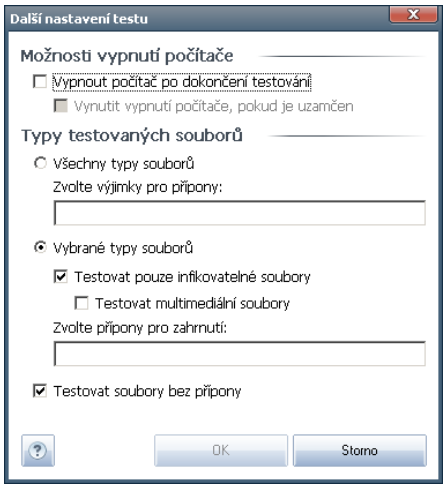
Předem definované výchozí nastavení ***Testu vybraných souborů či složek*** máte možnost editovat v dialogu ***Změnit nastavení testu pro Test vybraných souborů či složek*** *(dostupného z rozhraní pro testování prostřednictvím odkazu Změnit nastavení testu u Testu vybraných souborů a složek).* ***Pokud 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:
    - ***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 zapnuto*) - 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 vypnuto*) - test prověří i systémové oblasti vašeho počítače.
    - ***Povolit testování s extrémní citlivostí*** (*ve výchozím nastavení vypnuto*) - ve specifických situacích (*při podezření na infekci zavlečenou do vašeho počítače*) můžete zvolit tuto metodu testování, která aktivuje nejdůkladnější testovací algoritmy a velmi podrobně prověří naprosto

všechny oblasti vašeho počítače. Mějte však na paměti, že tato metoda je časově velmi náročná.

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



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

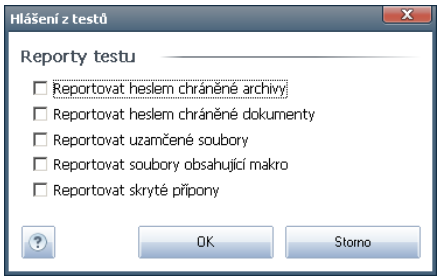
    - ***Všechny typy souborů*** - přičemž máte zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou;

    - ***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 hodnotě ***Dle činnosti uživatele***. Tato 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:



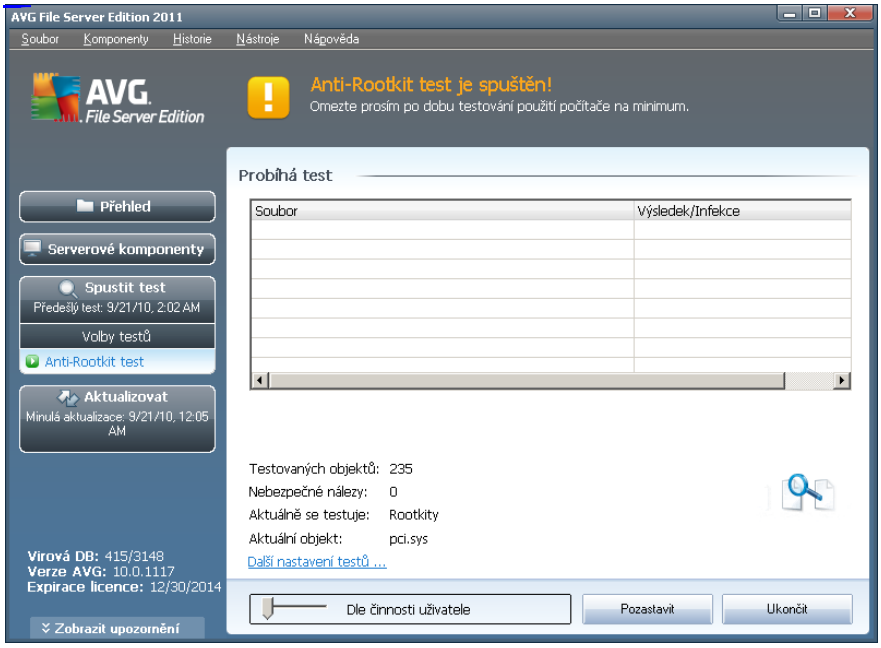
Upozornění: *Samotné možnosti nastavení testu jsou shodné s parametry nově definovaného testu, které jsou podrobně popsány v kapitole* ***AVG testování / Naplánování testu / Jak testovat****. Pokud se rozhodnete výchozí nastavení* ***Testu vybraných souborů či složek*** *změnit, můžete pak svou konfiguraci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

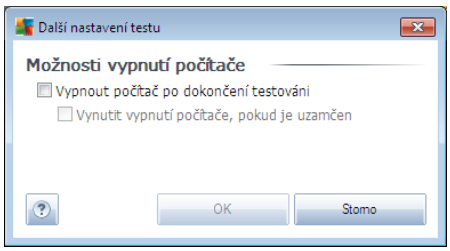


Editace nastavení testu

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:

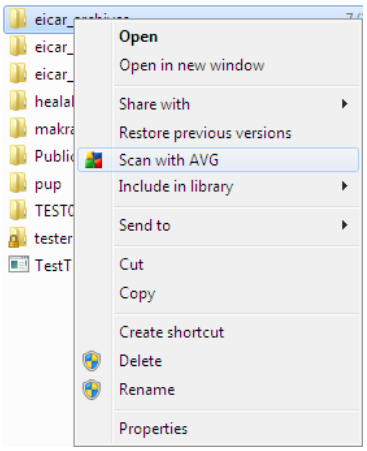
- ***Automatický test*** - posuvníkem lze změnit prioritu testu, která je ve výchozím nastavení na střední hodnotě. Střední (*automatická*) hodnota nastavení optimalizuje rychlost testu počítače a vytížení systémových zdrojů. Test můžete spustit pomaleji a tedy s nižší zátěží systémových zdrojů (*vhodné, 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 File Server 2011 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 File Server 2011** 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/

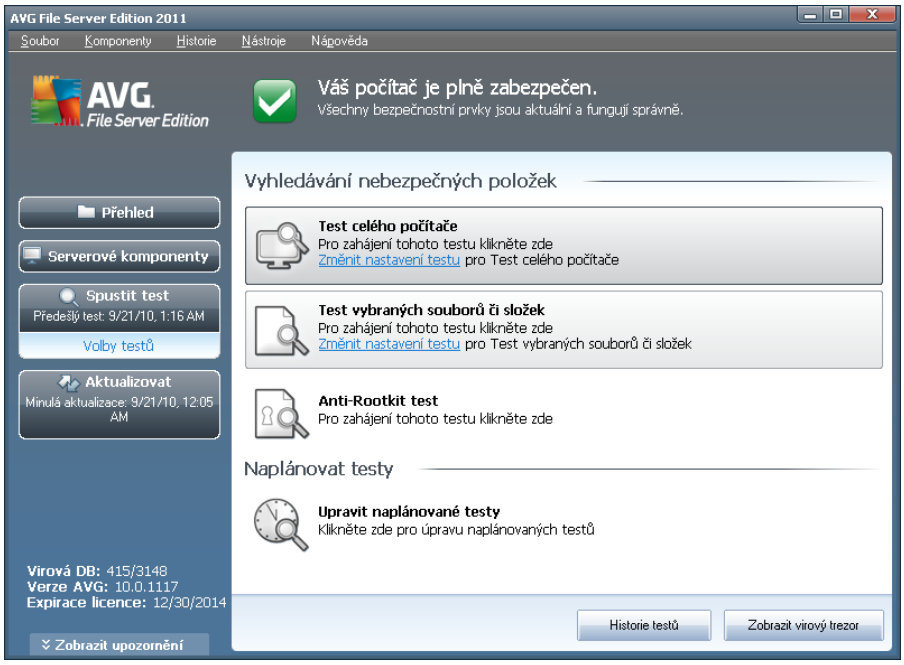
- ***/NOEXT*** Netestovat soubory s těmito příponami /například NOEXT=JPG/
- ***/ARC*** Testovat archívy
- ***/CLEAN*** Automaticky léčit
- ***/TRASH*** Přesunout infikované soubory do Virového trezoru
- ***/QT*** Rychlý test
- ***/MACROW*** Hlásit makra
- ***/PWDW*** Hlásit heslem chráněné soubory
- ***/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 File Server 2011** 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.

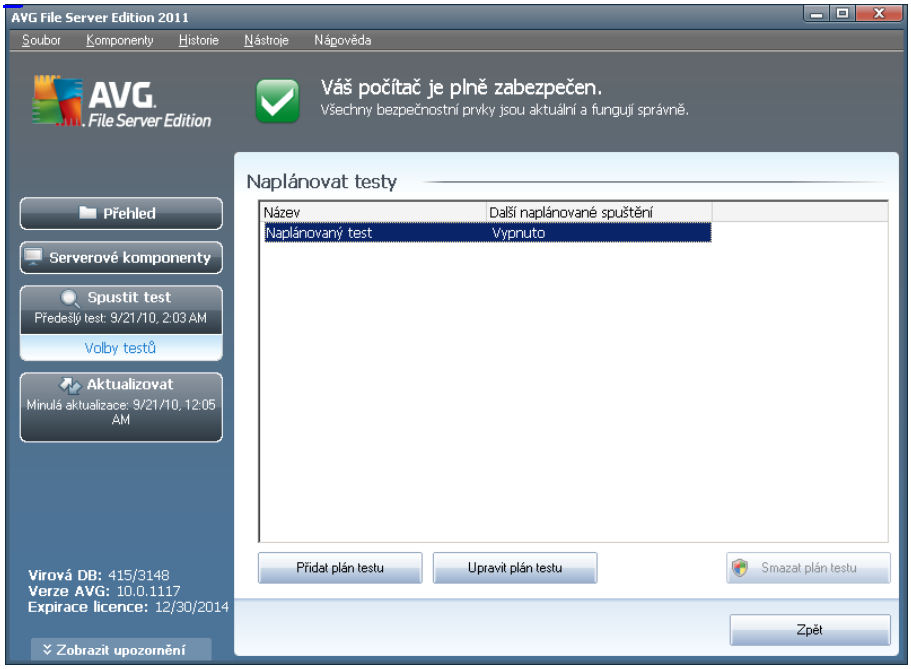
Test celého počítače by měl být spouštěn pravidelně, a to nejméně jednou týdně. Pokud vám to však provoz na vašem počítači umožňuje, doporučujeme spouštět test celého počítače jednou denně; tak je také ve výchozí konfiguraci nastaven plán testů. Jestliže je počítač trvale zapnutý, je vhodné naplánovat 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:

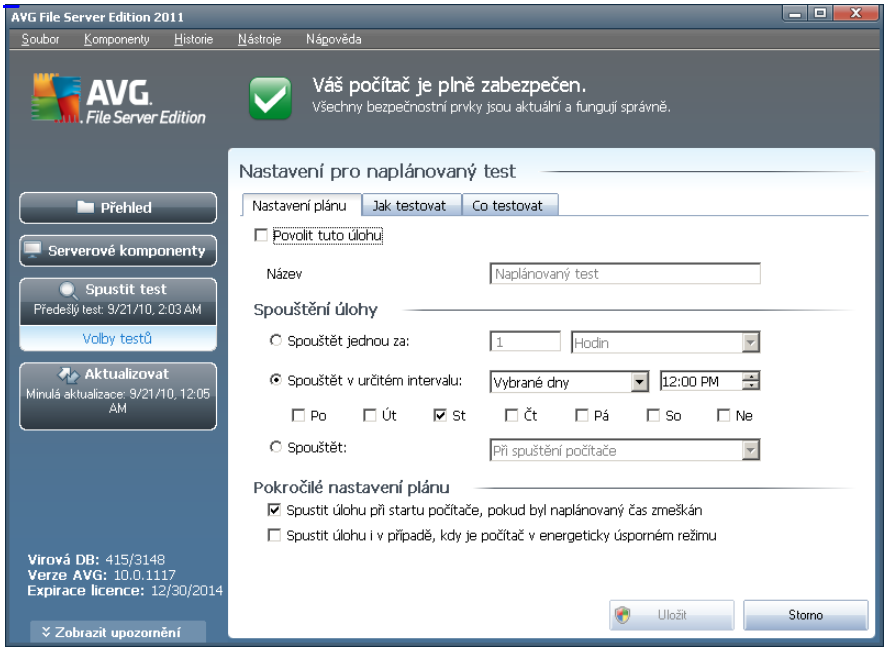


Pracovat můžete s těmito ovládacími tlačítky:

- ***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.

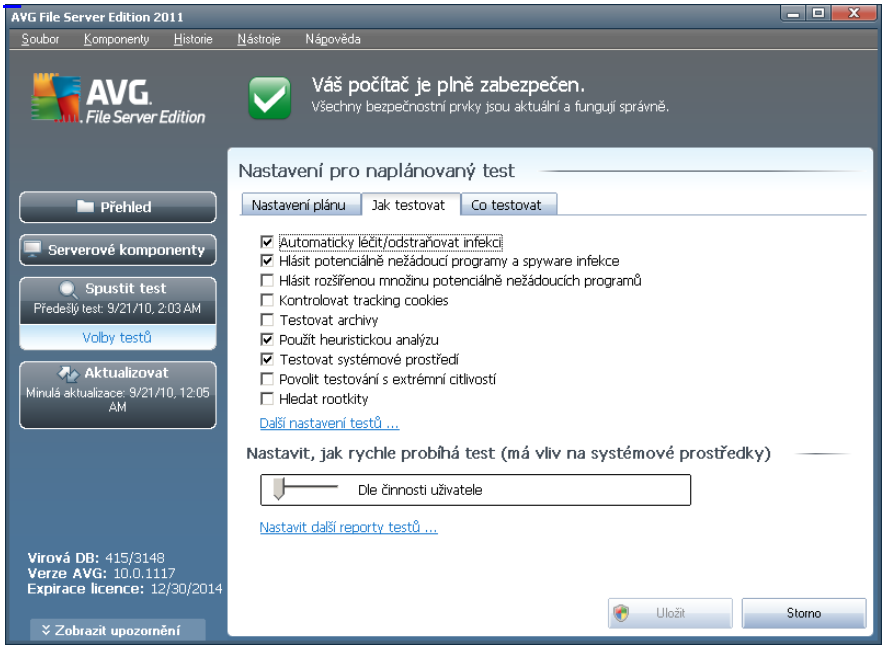
Ovládací tlačítka dialogu

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, ...

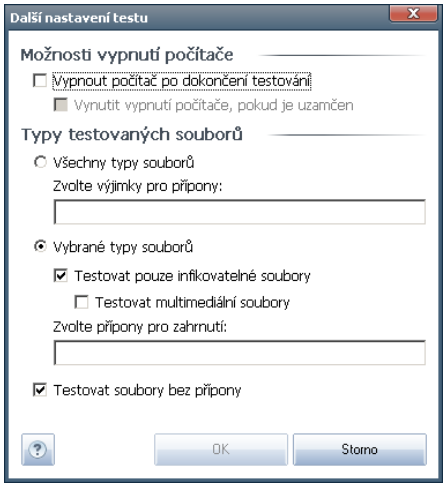
- ***Použít heuristickou analýzu*** - (*ve výchozím nastavení zapnuto*): během testu bude použita k detekci infekce i metoda heuristické analýzy (*dynamické emulace instrukcí testovaného objektu v prostředí virtuálního počítače*).

- ***Testovat systémové prostředí*** - (*ve výchozím nastavení zapnuto*): test prověří i systémové oblasti vašeho počítače.

- ***Povolit testování s extrémní citlivostí*** (*ve výchozím nastavení vypnuto*) - ve specifických situacích (*při podezření na infekci ve vašem počítači*) můžete zvolit tuto metodu testování, která aktivuje nejdůkladnější testovací algoritmy a velmi podrobně prověří naprosto všechny oblasti vašeho počítače. Mějte však na paměti, že tato metoda je časově velmi náročná.

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;

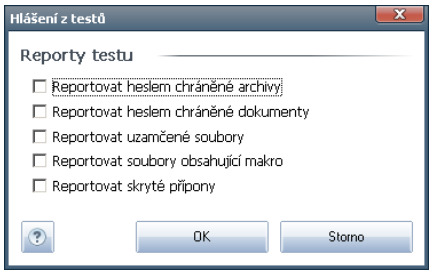
  - ***Vybrané typy souborů*** - můžete se rozhodnout, že chcete, aby se testy spouštěly pouze nad soubory, které lze považovat za infikovatelné (*soubory, které nemohou být infekcí zasaženy, se testovat nebudou - například prosté textové soubory nebo některé nespustitelné soubory*), a to včetně multimediálních 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.

- ***Nastavit, jak rychle probíhá teste*** - posuvníkem lze změnit prioritu testu. Střední 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:



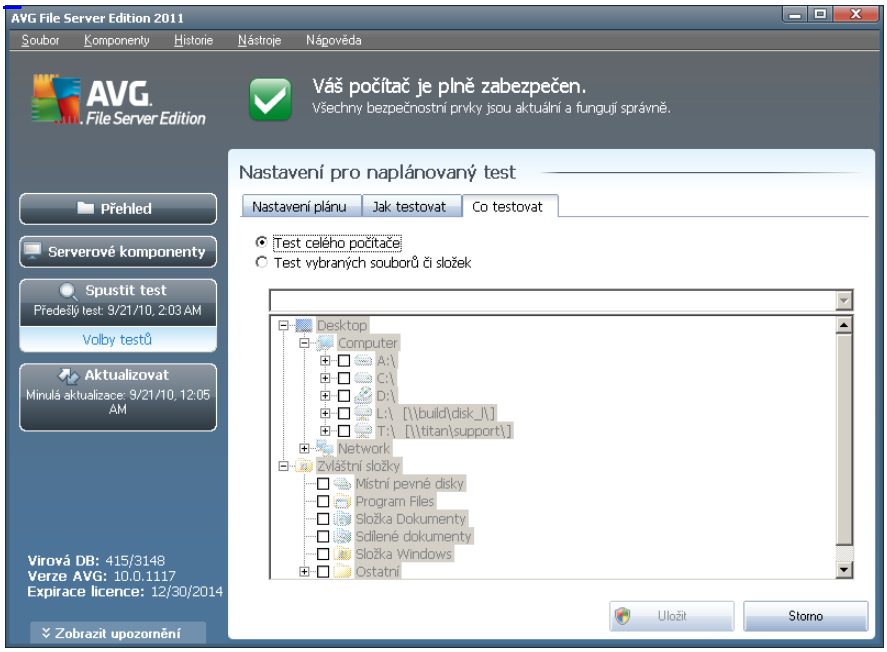
Ovládací tlačítka dialogu

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\
    - *v 64-bitové verzi* C:\Program Files (x86)
- ***Složka Dokumenty***
    - *pro Win XP:* C:\Documents and Settings\Default User\My Documents\

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

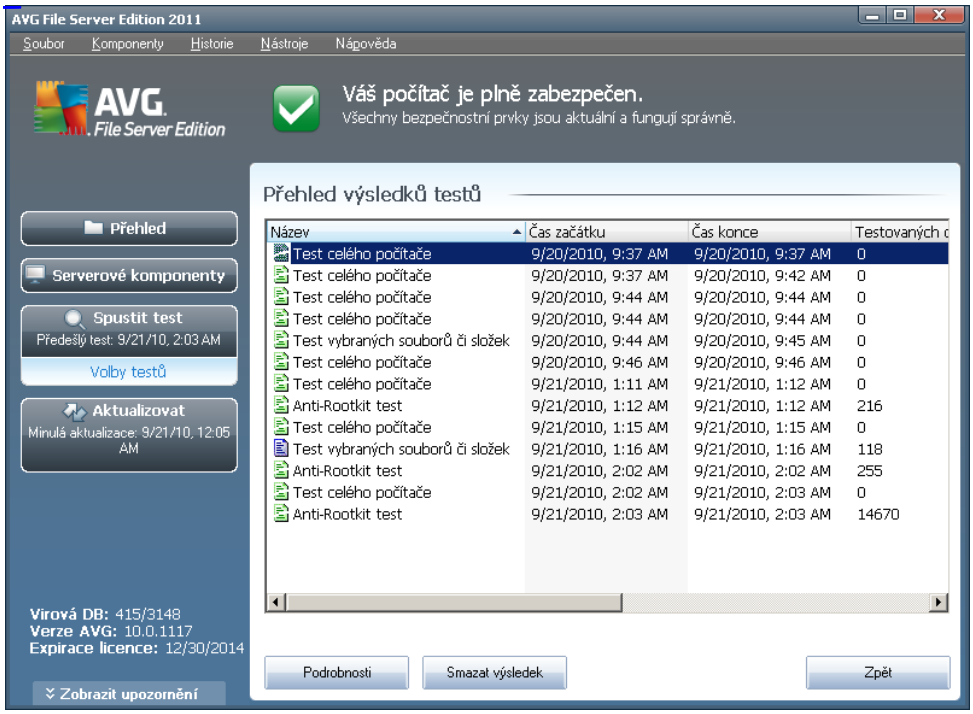
- ***Sdílené dokumenty***
  - pro *Win XP:* C:\Documents and Settings\All Users\Documents\
  - pro *Windows Vista/7*: C:\Users\Public\Documents\
- ***Složka Windows*** - C:\Windows\
- ***Ostatní***
  - *Systémový disk* - pevný disk, na němž je instalován operační systém (*obvykle C:*)
  - *Systémová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

Ovládací tlačítka dialogu

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

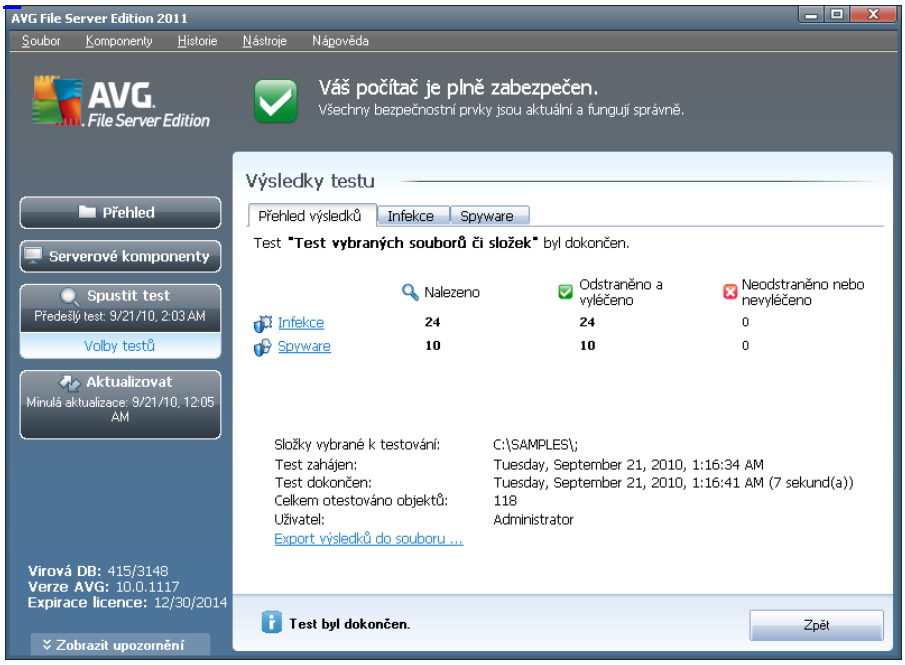
Jestliže v dialogu ***Přehled výsledků testů*** vyberete jeden test ze seznamu a označíte jej, můžete stiskem tlačítka ***Podrobnosti*** přejít do dialogu ***Výsledky testů***, v němž jsou zobrazeny detailní informace o průběhu a výsledku zvoleného testu.

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
- ***Rootkity*** - záložka se zobrazuje podmínečně tehdy, když byl během testu detekován rootkit
- ***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:

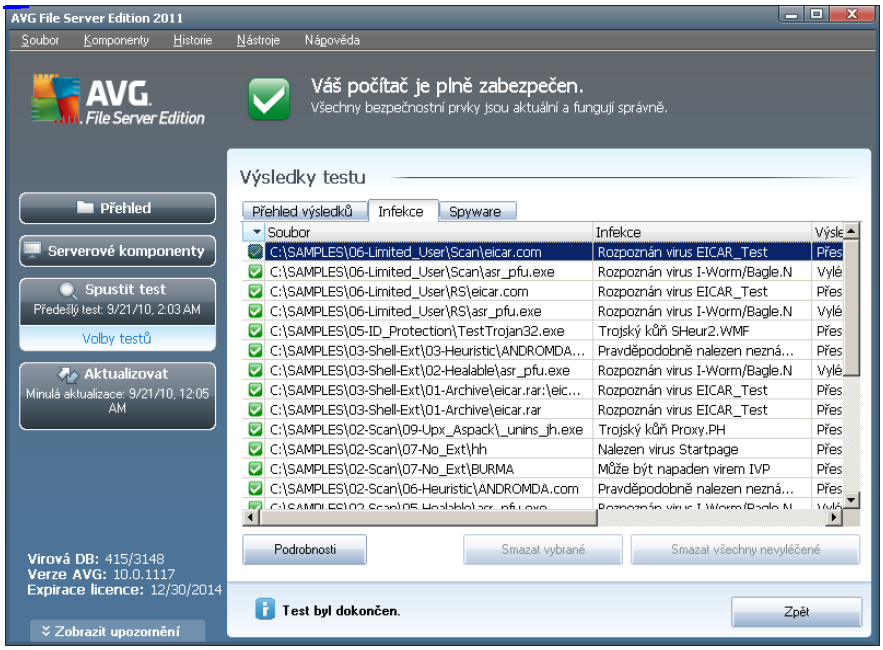
- detekovaných virových infekcích / spyware
- vyléčených virových infekcích / spyware
- počtu virových infekcích / spyware, které se nepodařilo odstranit nebo vyléčit

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

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

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

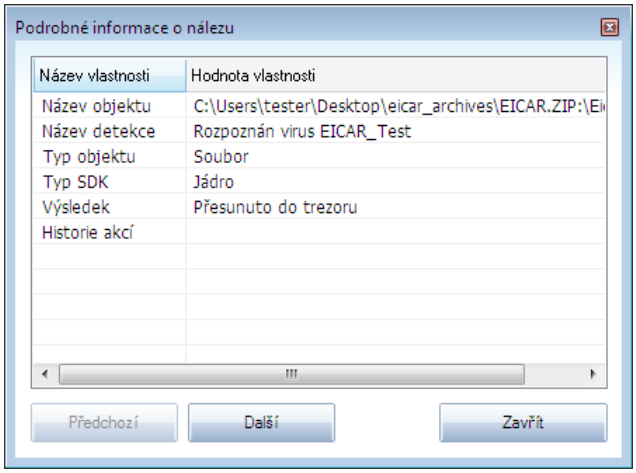
- o ***Potenciálně nebezpečný objekt*** - objekt je detekován jako potenciálně nebezpečný, ale nikoli infikovaný (*může například obsahovat makra*). Informace má tedy pouze charakter upozornění.

- o ***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***:



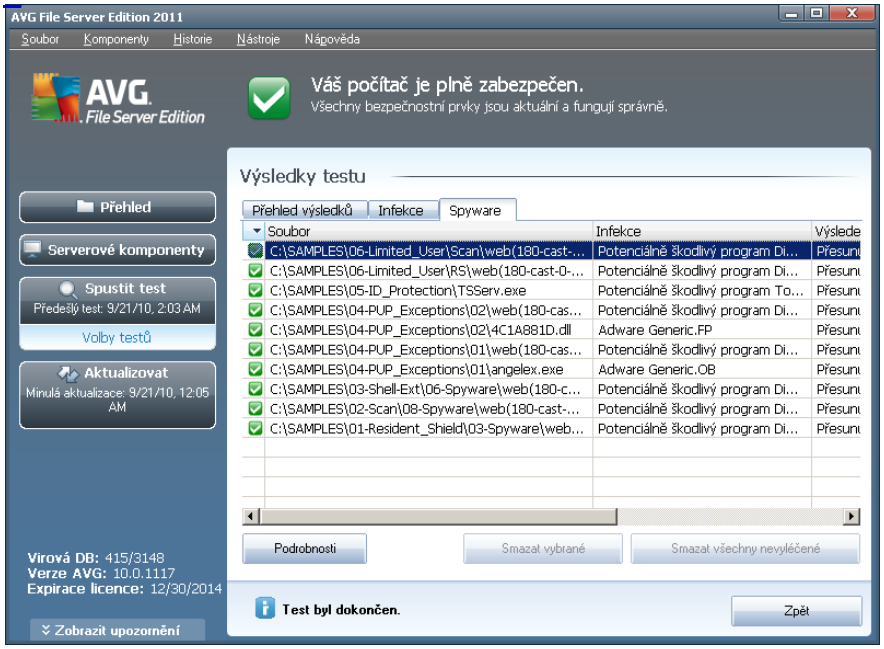
  V tomto dialogu najdete detailní informace o infekci (*například umístění a jméno detekovaného infikovaného objektu, typ objektu, typ SDK, výsledek detekce a historii akcí provedených nad detekovaným objektem*). Pomocí tlačítek ***Předchozí*** / ***Další*** můžete postupně zobrazovat informace o jednotlivých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

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

- ***Smazat všechny nevyléčené*** - 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:

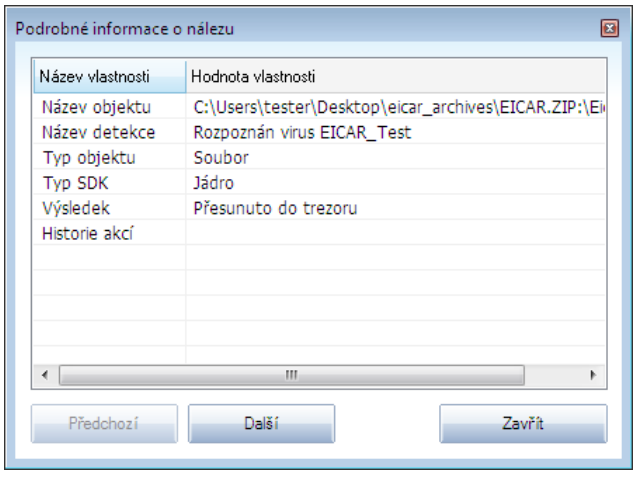
- ***Soubor*** - plná adresa původního umístění infikovaného objektu na lokálním disku
- ***Infekce*** - jméno detekovaného spyware (*podrobnosti o jednotlivých virech najdete ve* ***Virové encyklopedii*** *online*)
- ***Výsledek*** - uvádí, v jakém stavu se infikovaný a během testu detekovaný objekt 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

- o ***Obnoveno*** - objekt byl obnoven z ***Virového trezoru*** zpět do původního umístění
- o ***Přidáno k výjimkám PUP*** - nález byl vyhodnocen jako výjimka a připojen k seznamu výjimek PUP (*výjimky lze editovat v dialogu* ***PUP výjimky*** *pokročilého nastavení*)
- o ***Zamčený soubor*** - neotestován - objekt je zamčený a nebylo možno jej otestovat
- o ***Potenciálně nebezpečný objekt*** - objekt je detekován jako potenciálně nebezpečný, ale nikoli infikovaný (může například obsahovat makra). Informace má tedy pouze charakter upozornění.
- o ***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.

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

- ***Smazat všechny nevyléčené*** - 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.

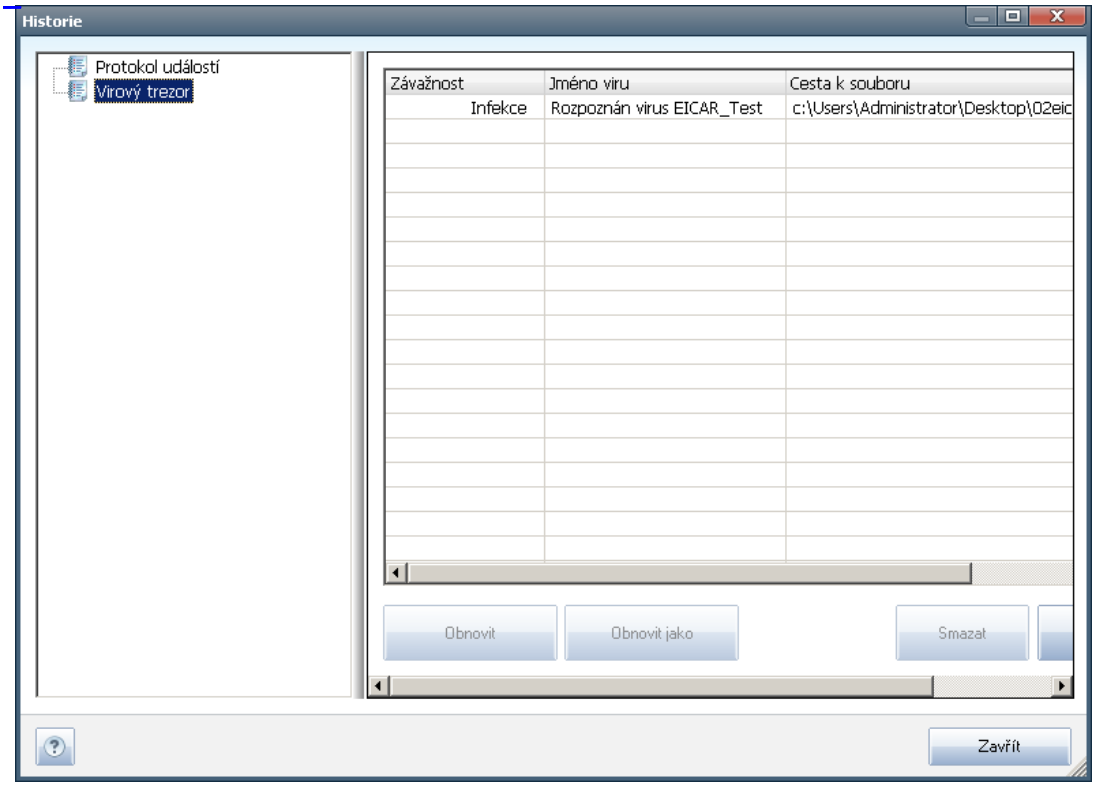
- ***Dokument s makry***: Detekovaný dokument může obsahovat škodlivé makro.

- ***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*** - zde je 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.

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 nebo častěji.Jedině tak zajistíte, že Váš **AVG File Server 2011** 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.

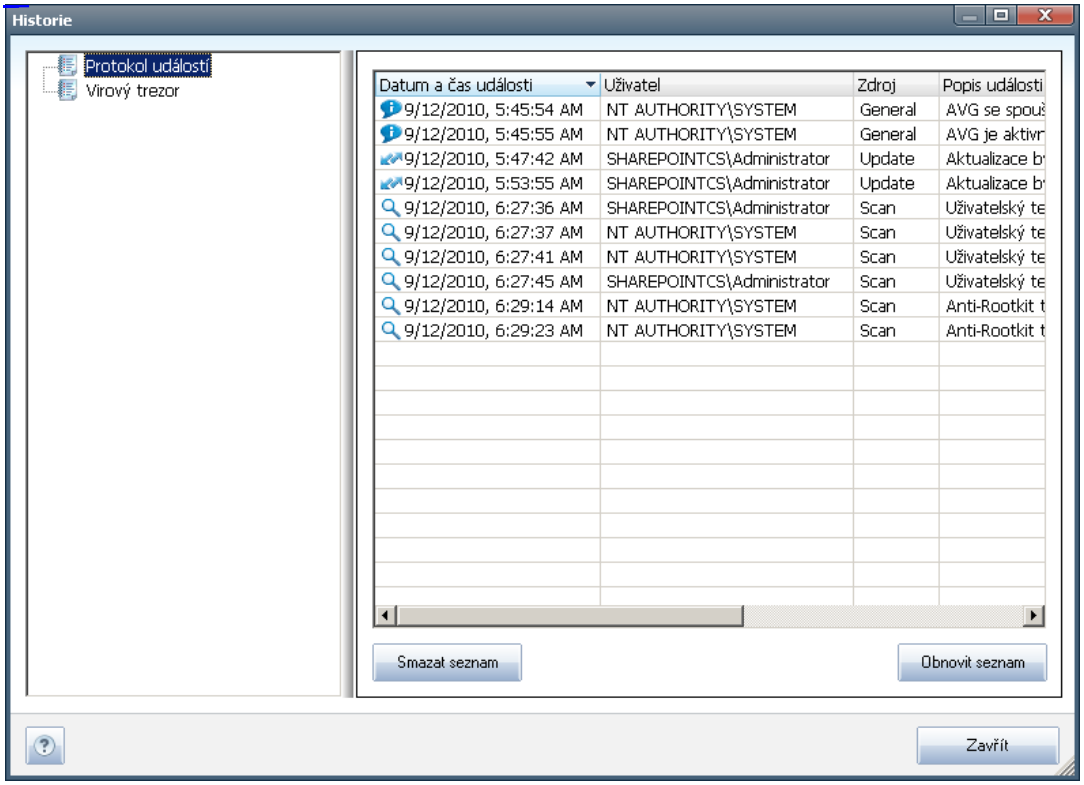
13.3. Průběh aktualizace

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



Dialog ***Historie*** je dostupný volbou položky systémového menu ***Historie/Protokol událostí***. V tomto dialogu najdete přehled všech důležitých událostí, které nastaly v průběhu práce **AVG File Server 2011**. 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

Ké každé události jsou evidovány následující údaje:

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

- ***Popis události*** obsahuje stručný popis události

Ovládací tlačítka dialogu

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

15. FAQ a technická podpora

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