AVG Anti-Virus 2012

Uživatelský manuál

Verze dokumentace 2012.24 (19.6.2012)

Obsah

1. Úvod

Tento uživatelský manuál je kompletní dokumentací programu **AVG Anti-Virus 2012.**

Aplikace **AVG Anti-Virus 2012** ochranu v reálném čase před současnými nejpokročilejšími hrozbami. Chatujte, stahujte a zasílejte soubory bez obav. Hrajte hry a sledujte videa bez starostí a přerušování:

- Bezpečně stahujte a sdílejte soubory a posílejte zprávy díky komponentě AVG Webový štít
- Buďte v bezpečí na sociálních sítíchdíky aplikaci AVG Social Networking Protection
- Procházejte Internet a vyhledávejte bez obav díky ochraně v reálném čase LinkScanner

2. Podmínky instalace AVG

2.1. Podporované operační systémy

AVG Anti-Virus 2012 je určen k ochraně pracovních stanic s těmito operačními systémy:

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

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

***Poznámka**: Komponenta ID Protection není podporována na Windows XP x64. Na tomto operačním systémm lze nainstalovat AVG Anti-Virus 2012, ale pouze bez této komponenty.*

2.2. Minimální / doporučené HW požadavky

Minimální hardwarové požadavky pro **AVG Anti-Virus 2012**:

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

Doporučené hardwarové požadavky pro **AVG Anti-Virus 2012**:

- Procesor Intel Pentium 1,8 GHz
- 512 MB RAM paměti
- 1350 MB volného místa na pevném disku (*z instalačních důvodů*)

3. Instalační proces AVG

Kde najdu instalační soubor?

Pro instalaci **AVG Anti-Virus 2012** na váš počítač potřebujete aktuální instalační soubor. Abyste zajistili, že instalujete vždy nejnovější verzi **AVG Anti-Virus 2012**, je vhodné stáhnout si instalační soubor z webu AVG (http://www.avg.cz/). V sekci ***Centrum podpory / Stáhnout*** najdete strukturovaný přehled instalačních souborů k jednotlivým edicím AVG.

Pokud si nejste jisti, které soubory budete k instalaci potřebovat, doporučujeme Vám službu ***Vyberte produkt*** ve spodní části webové stránky. Třemi jednoduchými otázkami definuje tato služba přesně ty soubory, které budete potřebovat. Po stisknutí tlačítka ***Pokračovat*** Vám pak nabídne seznam souborů ke stažení přesně na míru Vašim potřebám.

Jak probíhá proces instalace?

Pokud jste si již stáhli Instalační soubor a uložili jej k sobě na disk, můžete spustit samotný instalační proces. Instalace probíhá ve sledu jednoduchých a přehledných dialogových oken, z nichž každé vysvětluje, co je třeba v konkrétním kroku provést. Popis jednotlivých oken nyní nabízíme:

3.1. Vítejte: Volba jazyka

Instalační proces je zahájen otevřením dialogu ***Vítejte v instalátoru AVG***:

V tomto dialogu máte možnost zvolit jazyk instalačního procesu. Kliknutím na rozbalovací menu otevřete nabídku všech dostupných jazyků. Po potvrzení Vaší volby bude instalační proces nadále probíhat ve zvoleném jazyce.

Pozor: V tuto chvíli volíte pouze jazyk instalačního procesu. Aplikace AVG Anti-Virus 2012 bude tedy nainstalována ve zvoleném jazyce a také v angličtině, která se instaluje

automaticky. Je však možné nainstalovat ještě další volitelné jazyky, v nichž můžete aplikaci AVG zobrazit. Svůj výběr alternativních jazyků budete moci provést později během instalačního procesu, konkrétně v dialogu nazvaném Uživatelské volby.

3.2. Vítejte: Licenční ujednání

Dialog ***Vítejte v instalátoru AVG*** v následujícím kroku zobrazí licenční ujednání:

Přečtěte si prosím pečlivě celý text závazné licenční smlouvy AVG. Svůj souhlas s licenčním ujednáním potvrďte stiskem tlačítka ***Souhlasím***. Pokud s licenční smlouvou nesouhlasíte a stisknete tlačítko ***Nesouhlasím***, instalace bude okamžitě ukončena.

Ochrana osobních údajů AVG

Kromě licenčního ujednání se v tomto kroku instalace můžete také seznámit s politikou ***Ochrany osobních údajů AVG*** a ***Upozorněním na zpracování údajů***. Kliknutím na příslušný odkaz budete přesměrováni na webovou stránku AVG (http://www.avg.cz/), která Vás v plném rozsahu seznámí s požadovaným prohlášením.

Ovládací tlačítka dialogu

V prvním dialogu instalace jsou k dispozici pouze dvě ovládací tlačítka:

- ***Souhlasím*** - Kliknutím potvrzujete, že jste četli licenční ujednání a přijímáte jej v plném rozsahu. Instalace bude pokračovat přechodem do následujícího dialogu instalačního procesu.
- ***Nesouhlasím*** - Kliknutím odmítáte přijmout licenční ujednání. Instalační proces bude bezprostředně ukončen. **AVG Anti-Virus 2012** nebude nainstalován!

- ***Zpět*** - Kliknutím na tlačítko se vrátíte o jeden krok zpět do předchozího dialogu instalačního procesu.

3.3. Aktivujte vaši licenci

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

Kde najdu licenční číslo

Licenční číslo najdete buďto na registrační kartě v krabicovém balení **AVG Anti-Virus 2012**, anebo v potvrzovacím emailu, který jste obdrželi při zakoupení **AVG Anti-Virus 2012** 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*).

Jak použít metodu Copy & Paste

Následující přehled kroků je stručným popisem toho, jak použít metodu ***Copy & Paste*** *(kopíruj a vlož)* při vkládání licenčního čísla **AVG Anti-Virus 2012**:

- Otevřete e-mail, který obsahuje zaslané licenční číslo.
- Klikněte levým tlačítkem myši před první znak licenčního čísla. S tlačítkem stále stisknutým přejeďte myší na konec licenčního čísla a teprve nyní tlačítko pusťte. Licenční číslo je nyní označeno (vysvíceno).
- Podržte stisknutou klávesu ***Ctrl*** a současně stiskněte tlačítko ***C*** *(kopírovat)*.
- Umístěte kurzor na místo, kam chcete vložit kopírovanou informaci.

- Podržte stisknutou klávesu ***Ctrl*** a současně stiskněte tlačítko ***V*** *(vložit)*.
- Informace bude zkopírována na místo, kam jste umístili kurzor.

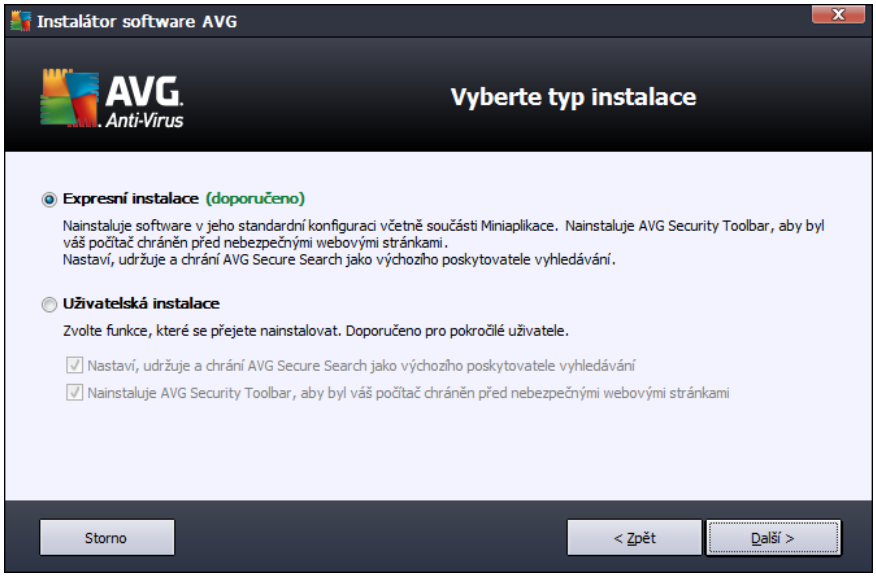
Ovládací tlačítka dialogu

Podobně jako ve většině dialogů instalace, jsou i zde dostupná tři ovládací tlačítka:

- ***Zpět*** - Kliknutím na tlačítko se vrátíte o jeden krok zpět do předchozího dialogu instalačního procesu.
- ***Další*** - Kliknutím na tlačítko pokračujete v instalačním procesu a přejdete do následujícího dialogu.
- ***Storno*** - Kliknutím na toto tlačítko bezprostředně ukončíte instalační proces; **AVG Anti-Virus 2012** nebude nainstalován!

3.4. Vyberte typ instalace

Dialog ***Vyberte typ instalace*** vám dává na výběr mezi ***Expresní instalací*** a ***Uživatelskou instalací***:



Expresní instalace

Většině uživatelů doporučujeme použít expresní instalaci. Tak bude **AVG Anti-Virus 2012** nainstalován zcela automaticky s konfigurací definovanou výrobcem, a to včetně miniaplikace AVG, doplňku pro internetové prohlížeče AVG Security Toolbar a s nastavením služby AVG Secure Search jako výchozího poskytovatele vyhledávání. Výchozí 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 Anti-Virus 2012** přímo v aplikaci.

Stiskem tlačítka ***Další*** postoupíte k následujícímu dialogu instalace.

Uživatelská instalace

Uživatelská instalace je vhodná pouze pro pokročilé a znalé uživatele. Doporučit ji lze v případě, že máte skutečný důvod instalovat **AVG Anti-Virus 2012** s nestandardním nastavením tak, aby vyhovovalo specifickým požadavkům vašeho systému. V této sekci máte možnost zvolit si, zda mají být nainstalovány následující funkce *(obě jsou ve výchozím nastavení označeny a určeny k instalaci, a pokud jejich označení nevypnete, budou automaticky nainstalovány)*:

- ***Nastaví, udržuje a chrání AVG Secure Search jako výchozího poskytovatele vyhledávání*** - ponecháte-li tuto volbu zapnutou, bude výchozím poskytovatelem vyhledávání AVG Secure Search, který úzce splupracuje s komponentou Link Scanner a společně tak zajišťují vaši maximální bezpečnost online.

- ***Nainstaluje AVG Security Toolbar, aby byl váš počítač chráněn před nebezpečnými webovými stránkami*** - ponecháte-li tuto položku označenu, bude nainstalován AVG Security Toolbar, který zajišťuje dostupnost bezpečnostních prvků AVG přímo z prostředí vašeho webového prohlížeče.

Pokud se rozhodnete pro uživatelskou instalaci, zobrazí se nová sekce ***Cílové umístění***. Zde máte možnost určit, kam má být program **AVG Anti-Virus 2012** instalován. Ve výchozím nastavení bude program instalován do adresáře programových souborů umístěném typicky na disku C:, jak je uvedeno v textovém poli v tomto dialogu. Pokud si přejete toto umístění změnit, pomocí tlačítka ***Procházet*** zobrazte strukturu vašeho disku a zvolte požadovaný adresář. Chcete-li se následně vrátit k původnímu umístění definovanému výrobcem, můžete tak učinit pomocí tlačítka ***Výchozí***.

Po stisku tlačítka ***Další*** budete přesměrováni k dialogu Uživatelské volby.

Ovládací tlačítka dialogu

Podobně jako ve většině dialogů instalace, jsou i zde dostupná tři ovládací tlačítka:

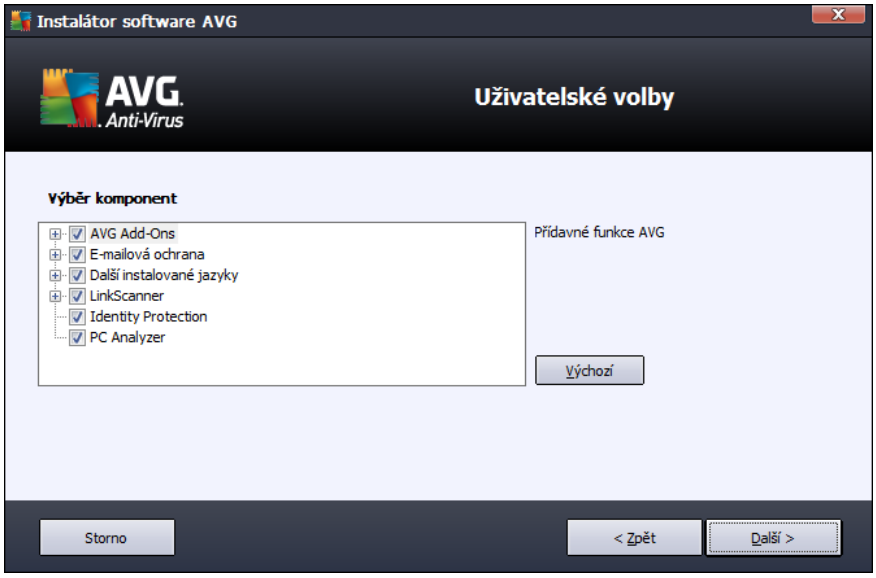
- ***Storno*** - Kliknutím na toto tlačítko bezprostředně ukončíte instalační proces; **AVG Anti-Virus 2012** nebude nainstalován!

- ***Zpět*** - Kliknutím na tlačítko se vrátíte o jeden krok zpět do předchozího dialogu instalačního procesu.

- ***Další*** - Kliknutím na tlačítko pokračujete v instalačním procesu a přejdete do následujícího dialogu.

3.5. Uživatelské volby

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



Sekce ***Výběr komponent*** nabízí přehled komponent **AVG Anti-Virus 2012**, 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 jednotlivých komponentách najdete v kapitole Přehled komponent. Chcete-li se vrátit k výchozí konfiguraci nastavené výrobcem, stiskněte tlačítko ***Výchozí***.

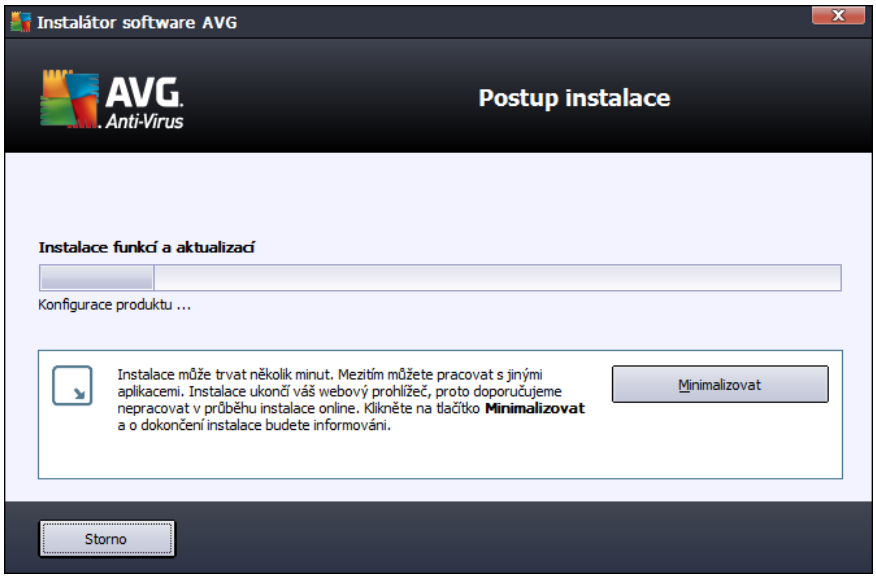
Ovládací tlačítka dialogu

Podobně jako ve většině dialogů instalace, jsou i zde dostupná tři ovládací tlačítka:

- ***Storno*** - Kliknutím na toto tlačítko bezprostředně ukončíte instalační proces; **AVG Anti-Virus 2012** nebude nainstalován!
- ***Zpět*** - Kliknutím na tlačítko se vrátíte o jeden krok zpět do předchozího dialogu instalačního procesu.
- ***Další*** - Kliknutím na tlačítko pokračujete v instalačním procesu a přejdete do následujícího dialogu.

3.6. Postup instalace

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



Počkejte prosím na dokončení instalace. Poté budete automaticky přesměrováni k následujícímu dialogu.

Ovládací tlačítka dialogu

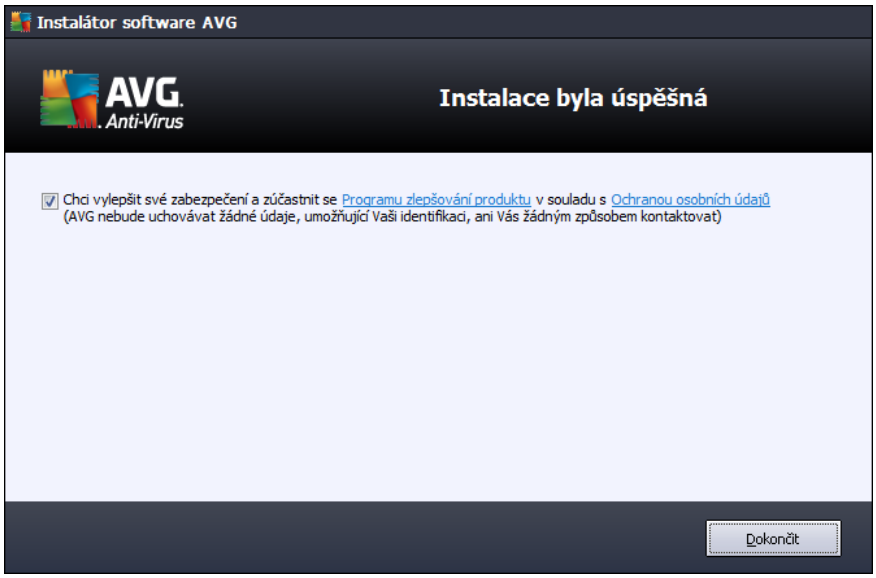
V dialogu jsou dostupná dvě ovládací tlačítka:

- ***Minimalizovat*** - Instalace může trvat několik minut. Tlačítkem zmenšíte dialogové okno instalace pouze na ikonu na systémové liště. Dialog se opět otevře v plné velikosti, jakmile bude instalace dokončena.

- ***Storno*** - Toto tlačítko použijte výhradně tehdy, přejete-li si běžící instalační proces přerušit. V takovém případě nebude **AVG Anti-Virus 2012** nainstalován!

3.7. Instalace byla úspěšná

Dialog ***Instalace byla úspěšná*** potvrzuje, že **AVG Anti-Virus 2012** byl plně nainstalován a nastaven k optimálnímu výkonu:



Program zlepšování produktu a ochrana osobních údajů

V tomto dialogu máte možnost se rozhodnout, zda se chcete zúčastnit ***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. Veškerá data jsou zpracována v souladu se zásadami ochrany osobních údajů; kliknutím na odkaz ***Ochrana osobních údajů*** budete přesměrováni na webovou stránku AVG (http://www.avg.cz/), která Vás v plném rozsahu seznámí se zásadami ochrany osobních údajů společnosti AVG Technologies. Pokud souhlasíte, ponechte prosím volbu označenou *(ve výchozím nastavení je tato možnost zapnuta)*.

Pro dokončení procesu instalace stiskněte tlačítko ***Dokončit***.

4. Po instalaci

4.1. Registrace produktu

Po dokončení instalace **AVG Anti-Virus 2012** prosím zaregistrujte svůj produkt na webu AVG (http://www.avg.cz/). Registrace vám umožní získat přístup k uživatelskému účtu AVG, dostávat informace o aktualizacích AVG, a zprostředkuje další služby poskytované registrovaným uživatelům AVG.

Nejsnazší přístup k registraci je přímo z prostředí aplikace **AVG Anti-Virus 2012**, a to volbou položky hlavního menu Nápověda/Registrovat. Následně budete přesměrováni na stránku ***Registrace*** na webu AVG (http://www.avg.cz/), kde dále postupujte podle uvedených instrukcí.

4.2. Otevření uživatelského rozhraní

Hlavní dialog AVG je dostupný několika cestami:

- dvojklikem na ikonu AVG na systémové liště
- dvojklikem na ikonu AVG na ploše
- z nabídky ***Start / Všechny programy / AVG 2012***

4.3. Spuštění testu celého počítače

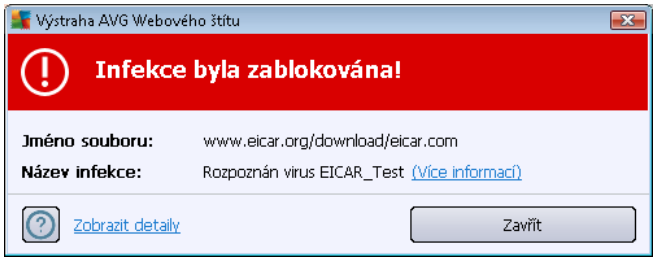
Jelikož existuje jisté riziko, že virus byl na váš počítač zavlečen již před instalací **AVG Anti-Virus 2012**, doporučujeme po instalaci spustit Test celého počítače, který zkontroluje celý počítač a ověří případnou přítomnost virů a potenciálně nežádoucích programů. První test počítače může trvat asi hodinu, ale z hlediska vaší bezpečnosti je skutečně nanejvýš důležité jej nechat proběhnout. Instrukce ke spuštění testu najdete v kapitole AVG testování.

4.4. Test virem Eicar

Chcete-li ověřit, že **AVG Anti-Virus 2012** byl správně nainstalován, proveďte test virem EICAR.

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

Stáhněte si soubor ***eicar.com*** a pokuste se jej uložit na lokální disk. Ihned poté, co potvrdíte stažení testovacího souboru, zareaguje Webový štít (*který je součástí komponenty LinkScanner*) varovným upozorněním. Toto upozornění dokazuje, že **AVG Anti-Virus 2012** na vašem počítači je správně nainstalován:



Z webu http://www.eicar.com můžete také stáhnout komprimovanou verzi testovacího 'viru' EICAR (*například ve formátu eicar_com.zip*). Při stahování tohoto souboru nedojde k detekci Webovým štítem a soubor budete moci uložit na disk. Při jeho rozbalení bude však virus detekován Rezidentním štítem v rámci komponenty Anti-Virus.

Pokud není testovací soubor EICAR identifikován jako virus, je nutné znovu prověřit konfiguraci AVG Anti-Virus 2012!

4.5. Výchozí konfigurace AVG

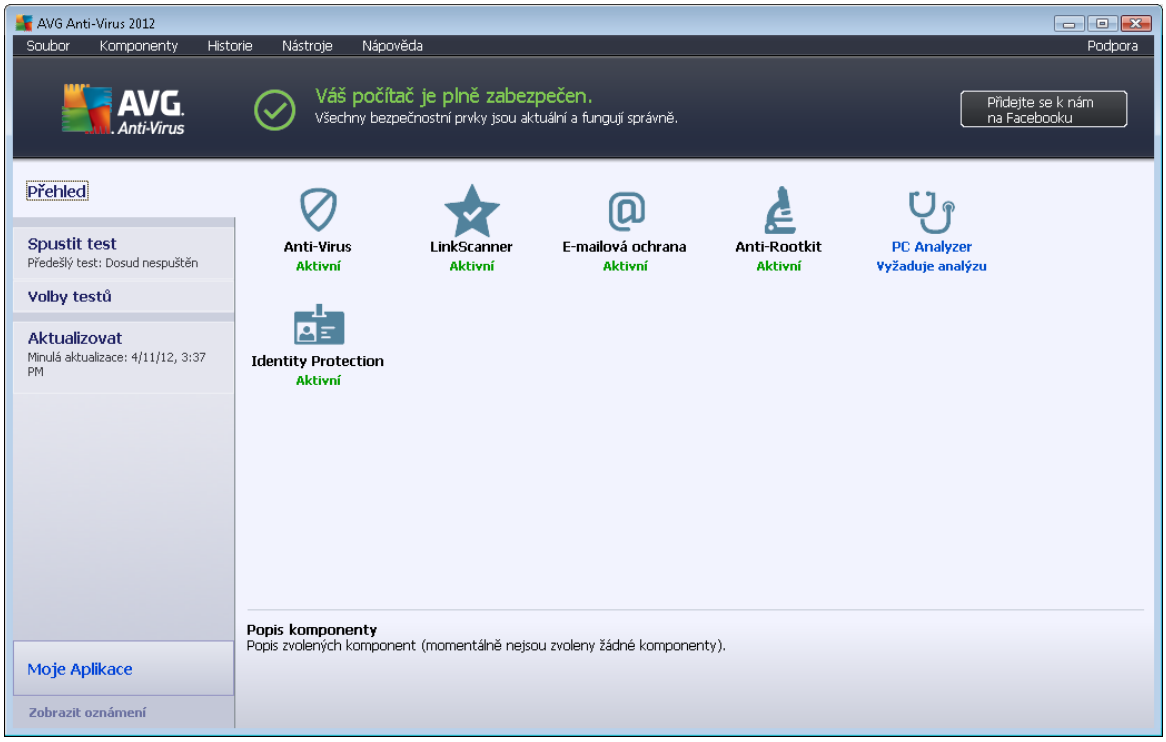
Ve výchozí konfiguraci (*bezprostředně po instalaci*) jsou všechny komponenty a funkce **AVG Anti-Virus 2012** nastaveny výrobcem k optimálnímu výkonu bezpečnostního software.

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 vždy přímo z hlavního dialogu 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.

5. Uživatelské rozhraní AVG

AVG Anti-Virus 2012 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 Anti-Virus 2012** - podrobnosti >>
- ***Informace o stavu zabezpečení*** *(v horní části okna)* podává základní informaci o aktuálním stavu **AVG Anti-Virus 2012** - podrobnosti >>
- ***Připojte se k nám na Facebooku*** *(zcela vpravo v horní části okna)* - toto tlačítko Vám jedném kliknutím umožní připojit se k AVG komunitě na Facebooku. Tlačítko se však zobrazuje pouze tehdy, jsou-li všechny komponenty AVG plně funkční a nastaveny k optimálnímu výkonu *(podrobné informace o tom, jak rozpoznat aktuální stav komponent, najdete v kapitole Informace o stavu zabezpečení)*
- ***Zkratková tlačítka*** *(v levé části okna)* umožňují rychlý přístup k nejdůležitějším a nejčastěji používaným funkcím **AVG Anti-Virus 2012** - podrobnosti >>
- ***Moje aplikace*** *(v levé spodní části okna)* otevírají přehled doplňkových aplikací **AVG Anti-Virus 2012**: LiveKive, Family Safety a PC Tuneup
- ***Přehled komponent*** *(ve střední části okna)* nabízí přehled všech instalovaných komponent **AVG Anti-Virus 2012** - podrobnosti >>

- ***Ikona na systémové liště*** *(v pravém dolním rohu monitoru, na systémové liště)* je indikátorem aktuálního stavu **AVG Anti-Virus 2012** -podrobnosti >>

- ***Miniaplikace AVG*** *(panel Windows sidebar, podporováno pouze v OS Windows Vista/7)* umožňuje rychlý přístup k testování a aktualizaci programu - podrobnosti >>

5.1. Systémové menu

Systémové menu je standardní navigací používanou ve všech oknech Windows. Je umístěno v rozhraní **AVG Anti-Virus 2012** vodorovně zcela nahoře. Prostřednictvím tohoto menu můžete přistupovat k jednotlivým komponentám, vlastnostem a službám AVG.

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

5.1.1. Soubor

- ***Konec*** - zavírá hlavní dialog **AVG Anti-Virus 2012**. Aplikace AVG však zůstává spuštěna, běží trvale na pozadí a váš počítač je stále chráněn!

5.1.2. Komponenty

Položka systémového menu Komponenty obsahuje odkazy k jednotlivým instalovaným komponentám AVG a otevírá hlavní dialog příslušné komponenty:

- ***Přehled komponent*** - přepne uživatelské rozhraní na dialog přehled komponent a jejich stavu

- ***Anti-Virus*** detekuje na vašem počítači viry, spyware, červy, trojany, nežádoucí spustitelné soubory nebo kniovny a chrání vás před nimi - podrobnosti >>

- ***LinkScanner*** vás chrání před webovými útoky v době, kdy surfujete na Internetu - podrobnosti >

- ***E-mailová Ochrana*** kontroluje všechny příchozí e-mailové zprávy a filtruje SPAM, blokuje viry, phishingové útoky a jiné hrozby - podrobnosti >>

- ***Anti-Rootkit*** testuje všechny aplikace, ovladače a knihovny na přítomnost skrytých rootkitů - podrobnosti >>

- ***PC Analyzer*** analyzuje stav vašeho počítače a nabízí přehled zjištěných údajů - podrobnosti >>

- ***Identity Protection*** nepřetržitě chrání vaše digitální data před novými a neznámými hrozbami - podrobnosti >>

- ***Vzdálená správa*** se zobrazuje pouze podmínečně v případě, že instalujete Business Edici produktu AVG a rozhodli jste se během instalačního procesu tuto komponentu doinstalovat

5.1.3. Historie

- Výsledky testů - přepíná do testovacího rozhraní AVG, konkrétně do dialogu s přehledem výsledků testů.
- Nálezy Rezidentního štítu - otevírá dialog s přehledem infekcí detekovaných Rezidentním štítem
- Nálezy Kontroly pošty - otevírá dialog s přehledem příloh detekovaných jako nebezpečné komponentou E-mailová ochrana
- Nálezy Webového štítu - otevírá dialog s přehledem infekcí detekovaných službou Webový štít v rámci komponenty LinkScanner
- Virový trezor - otevírá rozhraní karanténního prostoru (Virového trezoru), kam jsou přesouvány detekované infekční soubory, jež se nepodařilo automaticky vyléčit. V tomto prostoru jsou soubory zcela izolovány a tím je zajištěna naprostá bezpečnost vašeho počítače, a současně zde lze soubory uložit pro případnou další práci s nimi.
- Protokol událostí - otevírá rozhraní historie událostí s přehledem všech protokolovaných akcí **AVG Anti-Virus 2012**

5.1.4. Nástroje

- Otestovat počítač - 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 pouze nad jedním konkrétním souborem. Kliknutím na tuto volbu se otevře nové okno s náhledem stromové struktury vašeho disku. Zvolte požadovaný soubor a potvrďte spuštění testu.
- Aktualizovat - Automaticky spouští proces aktualizace AVG Anti-Virus 2012.
- ***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 Anti-Virus 2012**. Obecně doporučujeme dodržet výchozí výrobcem definované nastavení aplikace.

5.1.5. Nápověda

- ***Obsah*** - otevírá nápovědu k programu AVG
- ***Získat podporu*** - otevírá web AVG (http://www.avg.cz/) na stránce centra zákaznické podpory

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

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

- ***Reaktivovat*** - otevírá dialog Aktivace AVG, v němž jsou již předem vyplněna data, jež jste zadali v dialogu Registrace AVG během instalačního procesu. V dialogu ***Aktivace AVG*** můžete zadat své licenční číslo, kterým buďto nahradíte prodejní číslo, s nímž jste AVG instalovali, nebo kterým změníte dosavadní licenční číslo za jiné, např. při přechodu na jiný produkt z řady AVG.

- ***Registrovat*** - otevírá web AVG (http://www.avg.cz/) na stránce ***Registrace***. Vyplňte prosím své registrační údaje; pouze registrovaní zákazníci mají plný přístup k technické podpoře AVG.

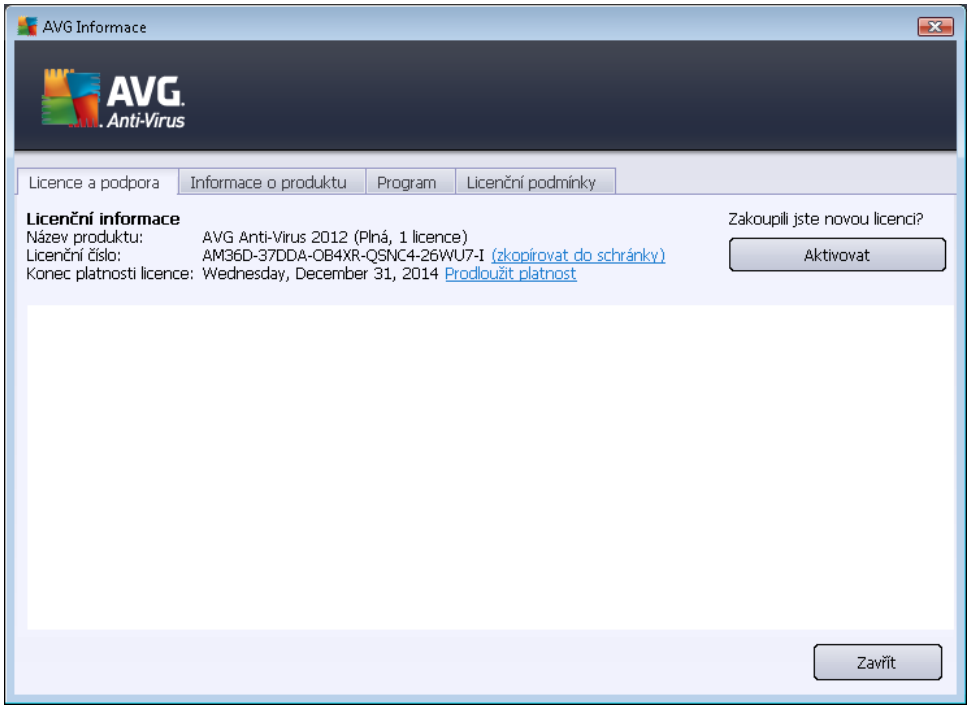
Poznámka*: Máte-li nainstalovanou zkušební verzi* **AVG Anti-Virus 2012***, dvě posledně uvedené položky se zobrazí jako* ***Zakoupit*** *a* ***Aktivovat*** *a odkáží Vás na web AVG, kde si můžete přímo zakoupit plnou verzi programu. Pokud máte nainstalovaný program* **AVG Anti-Virus 2012** *s prodejním číslem, položky se zobrazí jako* ***Zaregistrovat*** *a* ***Aktivovat****.*

- ***O AVG*** - otevírá dialog ***AVG Informace***, v němž na čtyřech záložkách najdete informace o zakoupené licenci a dostupné podpoře, o produktu, o programu a dále plné znění licenční smlouvy.

5.1.6. Podpora

Položka ***Podpora*** otevírá nový dialog ***AVG Informace*** s kompletním výčtem informací, které můžete potřebovat například při kontaktu se zákaznickou podporou. Dialog dále obsahuje základní údaje o instalovaném programu **AVG Anti-Virus 2012** (*verzi programu a databáze*), licenční údaje a seznam odkazů na zdroje podpory. Dialog ***AVG Informace*** je rozdělen do čtyř záložek, strukturovaný do logických celků:

Záložka ***Licence a podpora*** nabízí přehled licenčních informací, tedy název produktu *(typ licence a počet povolených instalací)*, licenční číslo a konec platnosti licence:



Ovládací prvky dialogu

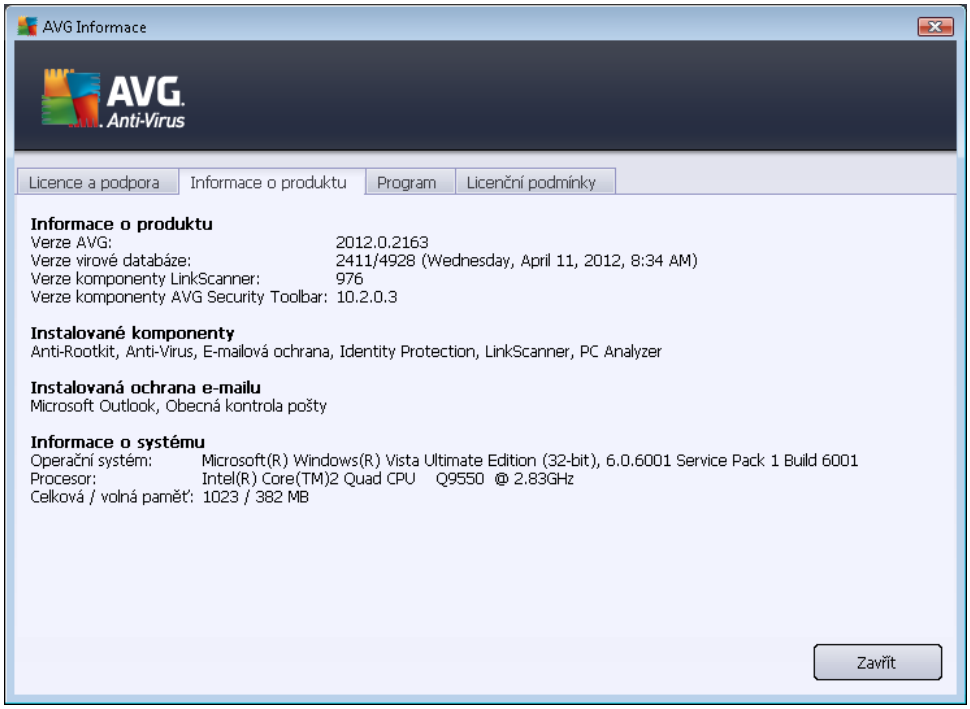
Na záložce najdete tyto odkazy a tlačítka:

- ***(Re)Aktivovat*** - Tlačítkem otevřete nový dialog ***AVG Aktivovat software***. Do tohoto dialogu zadejte své licenční číslo, kterým buďto nahradíte prodejní číslo *(s nímž jste AVG Anti-Virus 2012 instalovali)*, nebo kterým změníte dosavadní licenční číslo za jiné *(např. při přechodu na jiný produkt z řady AVG).* Můžete rovněž zadat své osobní údaje *(jméno, název firmy)*.

- ***Zkopírovat do schránky*** - Licenční číslo musí být zadáno naprosto přesně ve tvaru, jak je uvedeno. Proto je třeba věnovat mimořádnou pozornost jeho přepisu. Klinutím na odkaz *Zkopírovat do schránky* bude vaše licenční číslo uloženo do schánky a můžete jej prostým vložením použít kdekoliv potřebujete. Tím je zajištěno, že při jeho přepisu nedojde k chybě.

- ***Prodloužit platnost*** - Prodloužit platnost licence **AVG Anti-Virus 2012** je možné kdykoliv, nejlépe však aspoň jeden měsíc před datem expirace. Na blížíci se datum expitace budete upozorněni. Kliknutím na odkaz budete přesměrováni na stránku na webu AVG (http://www.avg.cz/), kde najdete podrobné informace o aktuálním stavu vaší licence, datum expirace a nabídku možností prodloužení licence.

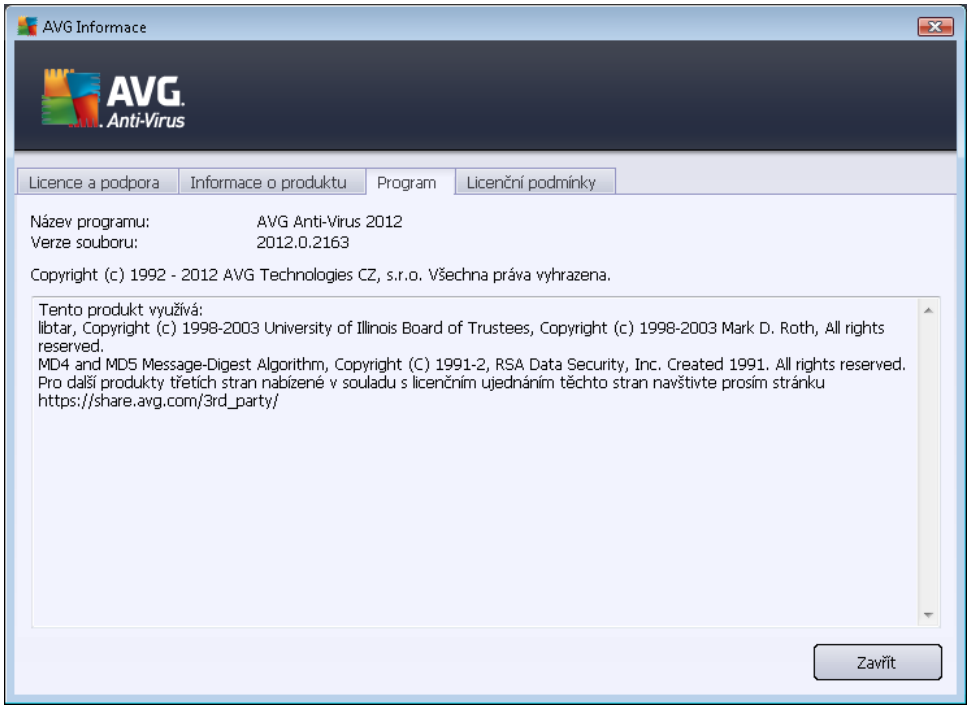
Záložka ***Informace o produktu*** podává přehled nejdůležitějších technických informací o **AVG Anti-Virus 2012**:



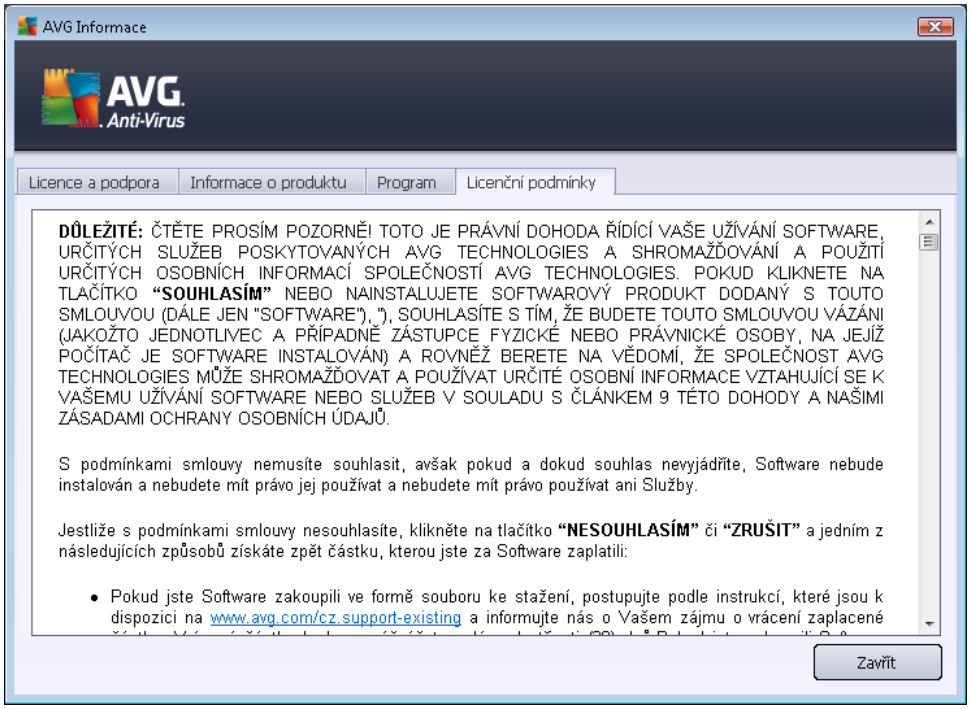
Záložka je rozčleněna do několika sekcí:

- ***Informace o produktu*** - seznam informací o verzi **AVG Anti-Virus 2012**, verzi virové databáze, verzi komponenty LinkScanner a verzi komponenty AVG Security Toolbar.
- ***Instalované komponenty*** - kompletní výčet všech aktuálně nainstalovaných komponent.
- ***Instalovaná ochrana e-mailu*** - přehled instalovaných doplňků pro kontrolu pošty; tyto informace můžete potřebovat při kontaktu s pracovníkem zákaznické podpory.
- ***Informace o systému*** - přehled parametrů vašeho operačního systému: procesor, operační systém, verze Windows, číslo sestavení, service pack a údaje o celkovém a volném objemu paměti

Záložka ***Program*** uvádí přesný název instalované edice **AVG Anti-Virus 2012** a číslo verze instalačního souboru. Dále jsou uvedeny informace o použitém kódu třetích stran:



Na záložce ***Licenční podmínky*** najdete plné znění licenčního ujednání mezi Vámi a společností AVG Technologies:



5.2. Informace o stavu zabezpečení

Sekce ***Informace o stavu zabezpečení*** je umístěna v horní části rozhraní **AVG Anti-Virus 2012**. V této sekci najdete vždy informaci o aktuálním stavu vašeho **AVG Anti-Virus 2012**. V sekci může být zobrazena jedna z následujících ikon, jejichž význam vysvětlujeme:

 - Zelená ikona informuje, že ***program AVG Anti-Virus 2012 na vašem počítači je plně funkční***, aktualizován a všechny instalované komponenty pracují správně. Jste zcela chráněni.

 - Žlutá 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.

Žlutá 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 (*kontextové menu otevřete pravám tlačítkem myši*) nad ikonou komponenty v přehledu komponent v hlavním okně **AVG Anti-Virus 2012**. Touto volbou dáváte

najevo, že jste si vědomi faktu, že se konkrétní komponenta nachází v chybovém stavu, ale z nějakého důvodu si přejete tento stav zachovat a nebýt na něj upozorňováni ikonou na systémové liště. Může nastat situace, kdy budete potřebovat využít této možnosti, ale rozhodně nedoporučujeme, abyste v tomto stavu setrvávali déle, než je nutné.

Alternativně bude žlutá ikona zobrazena také v situaci, kdy **AVG Anti-Virus 2012** vyžaduje restart počítače (***Restartovat nyní***). Věnujte prosím pozornost tomuto varování a restartujet počítač pomocí tlačítka ***Restartovat nyní***.

 - Oranžová ikona ***informuje o kritickém stavu AVG Anti-Virus 2012!*** Některá z komponent je nefunkční a **AVG Anti-Virus 2012** 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 Anti-Virus 2012 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 Anti-Virus 2012 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 Anti-Virus 2012** hlásí jakýkoliv problém, zaměřte se na jeho řešení. Pokud ignorujete chybová hlášení **AVG Anti-Virus 2012**, váš počítač je ohrožen!

Poznámka: *Informaci o stavu AVG Anti-Virus 2012 lze v kterémkoliv okamžiku práce na počítači získat také pohledem na ikonu na systémové liště.*

5.3. Zkratková tlačítka

Zkratková tlačítka najdete v levé části hlavního dialogu **AVG Anti-Virus 2012**. Tato tlačítka umožňují rychlý přístup k nejdůležitějším a nejčastěji používaným funkcím aplikace, tedy k zejména k testování a aktualizacím. Tlačítka jsou dostupná ze všech dialogů uživatelského rozhraní **AVG Anti-Virus 2012**:

Zkratková tlačítka jsou graficky rozdělena do tří sekcí:

- ***Spustit test*** - Ve výchozím nastavení tlačítko uvádí informaci o testu, který byl spuštěn naposledy (*tedy typ testu a datum jeho posledního spuštění*). Kliknutím na příkaz ***Spustit***

test dojde k opětovnému spuštění téhož testu. Pokud chcete spustit jiný test, klikněte na položku ***Volby testů***. Tím otevřete testovací rozhraní AVG Anti-Virus 2012, kde můžete přímo spustit libovolný test, naplánovat spuštění testu či editovat parametry testu. *(Podrobnosti v kapitole AVG Testování)*

- ***Volby testů*** - Tímto tlačítkem se z libovolného aktuálně otevřeného dialogu AVG vrátíte do úvodní obrazovky hlavního dialogu AVG s přehledem všech nainstalovaných komponent. *(Podrobnosti najdete v kapitole Přehled komponent)*

- ***Aktualizovat*** - Tlačítko uvádí datum a čas, kdy byl naposledy spuštěn proces aktualizace. Stiskem tlačítka aktualizaci rovnou spustíte a budete moci sledovat její průběh. *(Podrobnosti v kapitole Aktualizace AVG)*

Zkratková tlačítka jsou dostupná z uživatelského rozhraní v kterémkoli okamžiku práce s **AVG Anti-Virus 2012**. Ať už jejich pomocí spustíte libovolný proces, test nebo aktualizaci, aplikace se přepne do nového dialogu, ale zkratková tlačítka jsou stále k dispozici. Probíhající proces je navíc v navigaci graficky znázorněn, takže budete mít vždy kontrolu nad tím, které procesy v **AVG Anti-Virus 2012** jsou aktuálně spuštěny.

5.4. Přehled komponent

Rozdělení Přehledu komponent

Sekce ***Přehled komponent*** je umístěna ve střední části hlavního dialogu **AVG Anti-Virus 2012**. Tato sekce je rozdělena do dvou částí:

- ***Přehled všech instalovaných komponent*** je tvořen grafickými panely jednotlivých komponent. Každý panel je označen ikonou komponenty a nese informací o tom, zda je tato komponenta aktuálně aktivní či neaktivní.

- ***Popis komponenty*** je umístěn ve spodní části dialogu a stručně Vás seznámí se základní funkčností zvolené komponenty. Rovněž v této části najdete informaci o aktuálním stavu zvolené komponenty.

Seznam instalovaných komponent

V rámci **AVG Anti-Virus 2012** najdete v sekci ***Přehled komponent*** informace o těchto komponentách:

- ***Anti-Virus*** detekuje na vašem počítači viry, spyware, červy, trojany, nežádoucí spustitelné soubory nebo knihovny a chrání vás před nimi - podrobnosti >>

- ***LinkScanner*** vás chrání před webovými útoky v době, kdy surfujete na Internetu - podrobnosti >

- ***E-mailová Ochrana*** kontroluje všechny příchozí e-mailové zprávy a filtruje SPAM, blokuje viry, phishingové útoky a jiné hrozby - podrobnosti >>

- ***Anti-Rootkit*** testuje všechny aplikace, ovladače a knihovny na přítomnost skrytých rootkitů

- podrobnosti >>

- ***PC Analyzer*** analyzuje stav vašeho počítače a nabízí přehled zjištěných údajů - podrobnosti >>

- ***Identity Protection*** nepřetržitě chrání vaše digitální data před novými a neznámými hrozbami - podrobnosti >>

- ***Vzdálená správa*** se zobrazuje pouze podmínečně v případě, že instalujete Business Edici produktu AVG a rozhodli jste se během instalačního procesu tuto komponentu doinstalovat

Dostupné akce

- ***Přejezdem myši nad ikonou komponenty*** tuto komponentu v přehledu vysvítíte a současně se ve spodní části hlavního dialogu zobrazí stručný popis funkce této komponenty.

- ***Jednoduchým kliknutím na libovolnou ikonu komponenty*** otevřete vlastní rozhraní komponenty s přehledem základních statistických dat.

- ***Kliknutím pravého tlačítka myši nad ikonou komponenty*** pak otevřete kontextové menu, které nabízí několik možností:

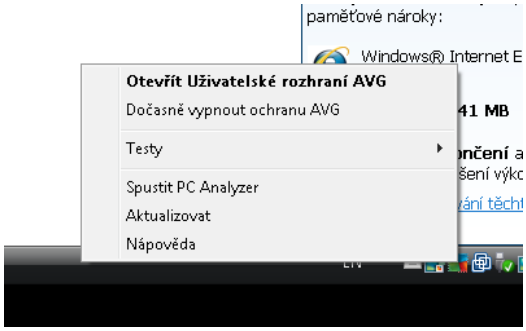
  - ***Otevřít*** - Kliknutím na tuto položku otevřete grafické rozhraní komponenty *(podobně jako jednoduchým kliknutím na vlastní ikonu komponenty)*.

  - ***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.

  - ***Otevřít v Pokročilém nastavení*** - Tato volba je dostupná pouze u těch komponent, u nichž je možnost pokročilého nastavení k dispozici.

5.5. Ikona na systémové liště

Ikona AVG na systémové liště *(zobrazena na panelu Windows vpravo dole na monitoru)* ukazuje aktuální stav **AVG Anti-Virus 2012**. Ikona je viditelná v každém okamžiku vaší práce na počítači, bez ohledu na to, zda máte či nemáte otevřeno uživatelské rozhraní aplikace:



Zobrazení systémové ikony AVG

Ikona může být zobrazena v několika variantách:

- Jestliže je ikona zobrazena barevně bez dalších prvků, jsou všechny komponenty **AVG Anti-Virus 2012** aktivní a plně funkční. Toto zobrazení ale také označuje situaci, kdy některá z komponent není v plně funkčním stavu, ale uživatel se rozhodl ignorovat stav komponenty. *(Volbou ignorovat stav komponenty 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.)*

- Pokud je ikona zobrazena s vykřičníkem, znamená to, že některá komponenta *(či více komponent)* je v chybovém stavu. Věnujte tomuto hlášení pozornost a pokuste se odstranit problém v konfiguraci komponenty, která není správně nastavena. Abyste mohli provést úpravy v nastavení komponenty, otevřete hlavní dialog aplikace dvojklikem na ikonu na systémové liště. Podrobnější informaci o tom, která komponenta je v chybovém stavu, pak najdete v sekci informace o stavu zabezpečení.

- Ikona na systémové liště může být také zobrazena barevně s probleskujícím otáčejícím se paprskem. Toto grafické znázornění signalizuje právě probíhající aktualizaci **AVG Anti-Virus 2012**.

- Alternativní zobrazení ikony s šipkou znamená, že právě běží některý z testů **AVG Anti-Virus 2012**.

Informace systémové ikony AVG

Ikona AVG na systémové liště dále poskytuje informace o aktuálním dění v programu **AVG Anti-Virus 2012**. Při změně stavu **AVG Anti-Virus 2012** (*automatické spuštění naplánované aktualizace nebo testu, změna stavu některé komponenty, přechod programu do chybového stavu, ...*) budete okamžitě informováni prostřednictvím vysunovacího okna zobrazeného nad ikonou na systémové liště:

Akce dostupné ze systémové ikony AVG

Ikonu AVG na systémové liště lze také použít pro rychlý přístup k hlavnímu dialogu **AVG Anti-Virus 2012**, to se otevře dvojklikem na ikonu. Kliknutí pravým tlačítkem myši nad ikonou otevírá kontextové menu s těmito možnostmi:

- ***Otevřít uživatelské rozhraní AVG*** - Otevře hlavní dialog **AVG Anti-Virus 2012**.

- ***Dočasně vypnout ochranu AVG*** - Položka umožňuje jednorázově deaktivovat celou ochranu zajištěnou programem **AVG Anti-Virus 2012**. 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 Anti-Virus 2012** před instalací nového software nebo ovladačů, a to ani tehdy, pokud budete během instalace vyzváni k zavření všech spuštěných aplikací. Jestliže budete opravdu nuceni deaktivovat **AVG Anti-Virus 2012**, 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.

- .

- ***Testy*** - Otevře vysunovací nabídku přednastavených testů (Test celého počítače a Test vybraných souborů či složek) 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*.

- ***Spustit PC Analyzer*** - Spustí funkci komponenty PC Analyzer.

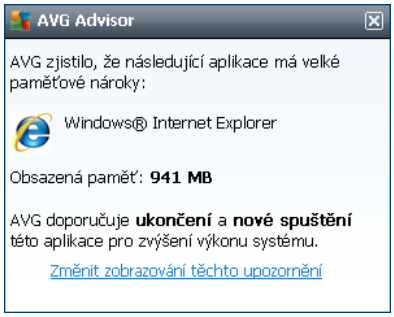
- ***Aktualizovat*** - Spustí okamžitou aktualizaci **AVG Anti-Virus 2012**.

- ***Nápověda*** - Otevře soubor nápovědy na úvodní stránce.

5.6. AVG Advisor

Hlavním úkolem ***AVG Advisoru*** je detekovat prolémy, které mohou zpomalovat nebo ohrožovat váš počítač, a navrhnout jejich řešení. Pokud se vám zdá, že se váš počítač náhle výrazně zpomalil *(ať už při prohlížení Internetu či z hlediska celkového výkonu)*, není obvykle na první pohled patrné, co je příčinou tohoto zpomalení a jak jej odstranit. Tady vstupuje do hry ***AVG Advisor***: ten sleduje výkon vašeho počítače, průběžně monitoruje všechny běžíci procesy, preventivně upozorňuje na možné problémy a nabízí návod k jejich řešení.

AVG Advisor se zobrazuje pouze v aktuální situaci v tomto dialogu na systémové liště:



AVG Advisor monitoruje tyto konkrétní situace:

- ***Stav aktuálně otevřeného webového prohlížeče***. U webového prohlížeče může poměrně snadno dojít k přetížení paměti, zejména pokud máte po delší dobu současně otevřeno prohlížení na několika záložkách. Tím se výrazně zvyšuje spotřeba systémových zdrojů a dochází ke zpomalení vašeho počítače. Řešením je v takové situaci restart webového prohlížeče.

- ***Spuštění Peer-To-Peer spojení***. Při použití P2P protokolu pro sdílení souborů jednotlivá spojení spotřebovávají značný objem přenosového pásma. Může se stát, že i po dokončení přenosu zůstane pásmo aktivní a výsledkem je zpomalení počítače.

- ***Neznámá síť se zdánlivě známým jménem***. Tento problém se týká uživatelů, kteří se připojují se svými přenosnými počítači k různým sítím. Narazíte-li na neznámou síť s obvyklým a zdánlivě známým jménem *(například Doma nebo MojeWifi)*, může dojít k omylu a náhodně se tak připojíte k neprověřené a potenciálně nebezpečné síti. ***AVG Advisor*** dokáže této situaci předejít a včas vás varovat, že se ve skutečnosti jedná o novou, neznámou síť. Pokud se rozhodnete považovat tuto síť za bezpečnou, můžete ji uložit do seznamu známých sítí a při příštím připojení k této síti se již notifikace ***AVG Advisoru*** nezobrazí.

V každé z těchto situací Vás ***AVG Advisor*** varuje před možným konfliktem a zobrazí jméno a ikonu problematického procesu či aplikace. Dále pak navrhne jednoduché řešení, kterým lze problému předejít.

Podporované webové prohlížeče

Služba ***AVG Advisor*** funguje v těchto webových prohlížečích: Internet Explorer, Chrome, Firefox, Opera, Safari.

5.7. Miniaplikace AVG

Miniaplikace AVG se zobrazuje na ploše Windows (*v sekci Windows Sidebar*). Tato funkce je podporována pouze v operačních systémech Windows Vista a Windows 7. ***Miniaplikace AVG*** vám umožní okamžitou dostupnost nejdůležitějších funkcí **AVG Anti-Virus 2012**, a to testování a aktualizace**:**

Rychlé spuštění testu nebo aktualizace

Miniaplikace AVG Vám v případě potřeby umožňuje okamžitě spustit test nebo aktualizaci:

- ***Spustit test*** - Kliknutím na volbu ***Spustit test*** spustíte přímo z prostředí miniaplikace test celého počítače. Jeho průběh můžete sledovat v pozměněném rozhraní miniaplikace v jednoduchém statistickém přehledu, kde najdete informace o počtu otestovaných objektů, detekovaných hrozeb a vyléčených hrozeb. V průběhu testu můžete proces testování kdykoliv pozastavit nebo ukončit. Podrobné informace o výsledku testu pak najdete standardně v dialogu Přehled výsledků testu, který lze z miniaplikace otevřít

kliknutím na volbu ***Zobrazit detaily*** *(test bude označen jako Test z miniaplikace)*.

- ***Aktualizovat*** - Kliknutím na volbu ***Aktualizovat*** spustíte proces aktualizace **AVG Anti-Virus 2012** přímo z prostředí minaplikace:

Přístup k sociálním sítím

Miniaplikace AVG dále nabízí zkratková tlačítka, jejichž pomocí se spojíte s AVG komunitou v nejrozšířenějších sociaálních sítích *(Twitter, Facebook a LinkedIn)*:

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

- ***Facebook*** - Otevírá internetový prohlížeč na webu sociální sítě Facebook, konkrétně na stránce ***AVG komunity***.

- ***LinkedIn*** - Tato funkce je dostupná pouze v síťové instalaci (*instalaci s licenčním číslem některé z AVG Business Edicí*) a otevírá internetový prohlížeč na stránce ***AVG***

SMB Community v rámci sociální sítě LinkedIn.

Další funkce dostupné z miniaplikace

- ***PC Analyzer***  - Otevírá hlavní dialog komponenty PC Analyzer a rovnou spouští proces anylýzy.
- ***Vyhledávání*** - Zadejte klíčové slovo a výsledky vyhledávání se zobrazí v nově otevřeném okně prohlížeče, který obvykle používáte.

6. Komponenty AVG

6.1. Anti-Virus

Komponenta ***Anti-Virus*** je základním prvkem **AVG Anti-Virus 2012** a obsahuje několik zásadních funkcí bezpečnostního programu:

- Testovací jádro
- Rezidentní ochranu
- Anti-Spyware ochranu

6.1.1. Testovací jádro

Testovací jádro, které je základem komponenty ***Anti-Virus***, testuje 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 Virového trezoru.

Profesionální antivirová ochrana AVG Anti-Virus 2012 zaručí, že na počítači nebude spuštěn žádný známý virus!

Detekční metody

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. 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 Anti-Virus 2012** kombinaci uvedených technik v rámci jednoho testu. Příkladem může být situace, kdy je virus zachycený skenováním přesně identifikován pomocí heuristické analýzy. **AVG Anti-Virus 2012** 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.

AVG Anti-Virus 2012 poskytuje vašemu počítači nepřetržitou ochranu!

6.1.2. Rezidentní ochrana

AVG Anti-Virus 2012 Vám zajistí naprosté bezpečí prostřednictvím tak zvané rezidentní ochrany. Komponenta ***Anti-Virus*** testuje všechny soubory *(s určenými příponami nebo i bez přípon)*, které otvíráte, kopírujete, ukládáte. Kontroluje také systémové oblasti počítače i vyměnitelná média (*flash disky apod.*). V případě pozitivního nálezu v právě používaném souboru zastaví prováděnou operaci a zabrání aktivaci viru. Funkce rezidentní ochrany pracuje "na pozadí", takže obvykle probíhající procesy ani nezaznamenáte. Upozornění se zobrazí pouze v případě, že dojde k nálezu škodlivého kódu a k zabránění jeho aktivaci.

Rezidentní ochrana se načte do paměti počítače automaticky, ihned po spuštění, a je nanejvýš důležité, aby byla zapnuta nepřetržitě!

6.1.3. Anti-Spyware ochrana

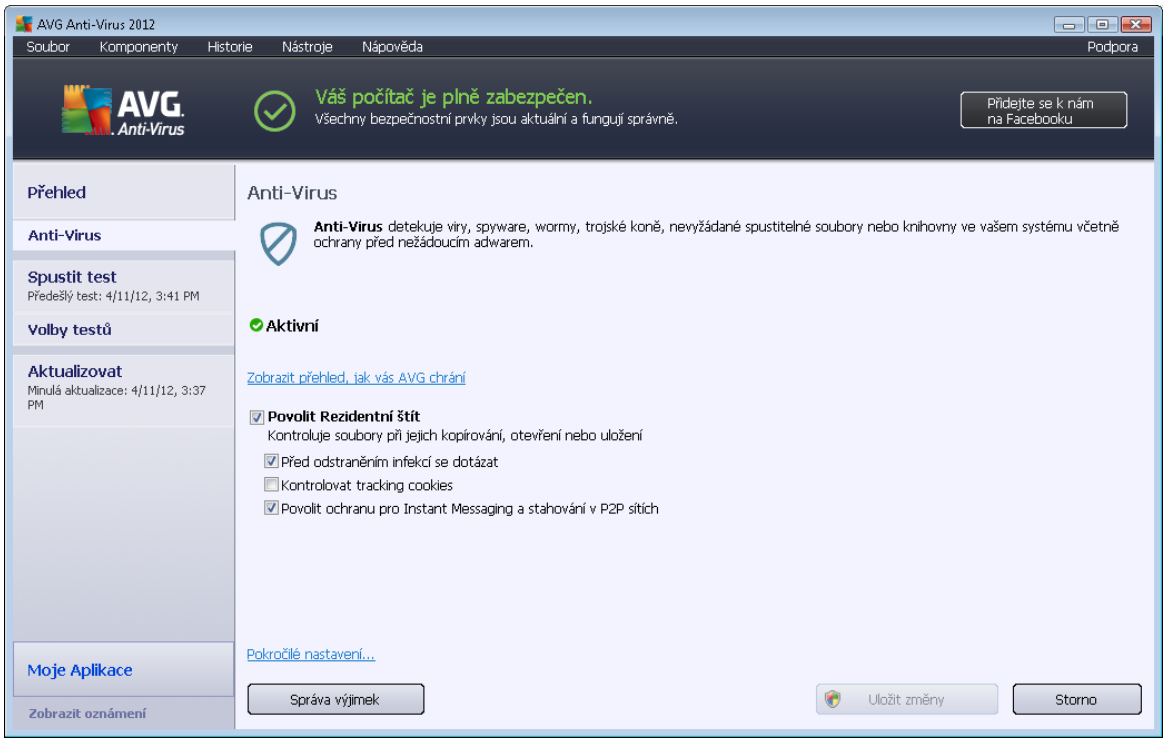
Anti-Spyware je v podstatě tvořen databází známých *(již identifikovaných)* definic spyware. Odborníci v laboratořích AVG intenzivně pracují na identifikaci a popisu nejnovějších vzorků spyware, okamžitě jakmile se nový spyware objeví. Identifikované definice pak přidávají do spyware databáze. Během aktualizačního procesu dojde ke stažení těchto nových definic na Váš počítač, čímž je zaručena Vaše nepřetržitá a spolehlivá ochrana proti nejnovějším hrozbám. ***Anti-Spyware*** umožňuje kompletní kontrolu Vašeho počítače a detekci případného malware/spyware. ***Anti-Spyware*** detekuje i tak zvaný "spící" malware, tedy malware, který byl na Váš počítač zavlečen, ale dosud nebyl aktivován.

Co je to 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***: pracuje nepřetržitě a na pozadí prověřuje veškeré aplikace, které spouštíte.

6.1.4. Rozhraní komponenty Anti-Virus

Dialog komponenty ***Anti-Virus*** nabízí stručný přehled funkcí komponenty a informace o jejím aktuálním stavu *(Aktivní).* Dále zde najdete základní možnosti konfigurace komponenty:



Možnosti konfigurace

Dialog nabízí základní možnosti konfigurace komponenty ***Anti-Virus***. Následuje stručný popis jednotlivých funkcí:

- ***Zobrazit online přehled, jak vás AVG chrání*** - Kliknutím na odkaz budete přesměrováni na speciální stránku na webu AVG (http://www.avg.cz/). Na této stránce najdete detailní statistický přehled všech aktivit **AVG Anti-Virus 2012**, které proběhly na vašem počítači za určený časový úsek i celkově od okamžiku instalace programu.

- ***Povolit Rezidentní štít*** - Označením či naopak dostraněním označení u této položky jednoduše zapnete nebo vypnete rezidentní ochranu. Rezidentní štít testuje soubory při jakékoliv činnosti s nimi prováděné, tedy při jejich kopírování, otevírání či ukládání. Pokud by při některém z těchto úkonů byl detekován virus, budete o nálezu okamžitě vyrozuměni. Ve výchozím nastavení je tato funkce zapnuta, a doporučujeme, abyste ji zapnutou ponechali! Pokud se rozhodnete ponechat rezidentní ochranu spuštěnou, máte dále možnost definovat, jak má být s případnou zachycenou infekcí naloženo:

    - ***Automaticky odstranit detekované infekce*** / ***Před odstraněním infekcí se dotázat*** - Ponechejte tuto položku označenou, pokud chcete být při detekci hrozby dotázáni na to, jaké kroky mají být dále podniknuty. V opačném případě bude hrozba

automaticky přesunuta do Virového trezoru. Tato vaše volba nemá žádný vliv na úroveň bezpečnosti a je pouze preferenční.

- ***Kontrolovat Tracking Cookies*** - Nezávisle na předchozí volbě můžete dále rozhodnout, 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.

- ***Povolit ochranu pro Instant Messaging a stahování v P2P sítích*** - Označením této položky potvrzujete, že si přejete, aby byla prováděna kontrola okamžité on-line komunikace *(to je komunikace pomocí programů pro okamžité zasílání zpráv, jakými jsou například ICQ, MSN Messenger, Yahoo Messenger ...)*.

- ***Pokročilé nastavení*** - Kliknutím na odkaz budete přesměrováni do příslušného dialogu Pokročilého nastavení **AVG Anti-Virus 2012**, kde můžete editovat konfiguraci komponenty do nejmenších podrobností. Mějte však na paměti, že výchozí konfigurace všech komponent **AVG Anti-Virus 2012** je nastavena tak, aby program podával optimální výkon a poskytoval maximální možnou úroveň bezpečí. Pokud nemáte skutečný důvod ke změně, doporučujeme ponechat výchozí nastavení!

Ovládací tlačítka dialogu

V dialogu jsou dostupné tyto ovládací prvky:

- ***Správa Výjimek*** - Otevře nový dialog nazvaný ***Rezidentní štít - Výjimky***. Editace výjimek Rezidentního štítu je rovněž dostupná prostřednictvím hlavního menu, a to touto cestou: Pokročilé nastavení / Anti-Virus / Rezidentní štít / Výjimky *(podrobný popis tohoto dialogu najdete v příslušné kapitole)*. V tomto dialogu můžete specifikovat soubory nebo adresáře, které mají být vyňaty z kontroly Rezidentním štítem. 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.

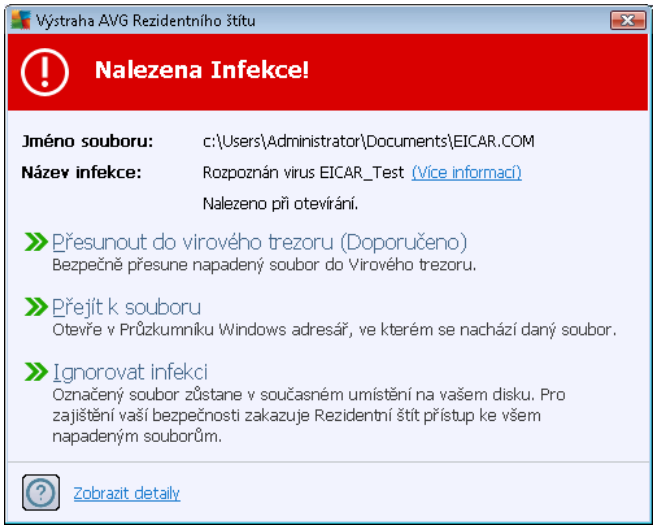
  - *Upravit seznam* - Umožňuje upravit celý seznam definovaných výjimek ručně v dialogu, který se chová jako textový editor.

- ***Použít*** - Uloží všechny změny v nastavení komponenty provedené v tomto dialogu a poté přepne aplikaci do hlavního dialogu **AVG Anti-Virus 2012** (*přehled komponent*).

- ***Storno*** - Zruší veškeré změny v nastavení komponenty provedené v tomto dialogu. Žádná z provedených změn nebude uložena. Následně bude aplikace přepnuta do hlavního dialogu **AVG Anti-Virus 2012** (*přehled komponent*).

6.1.5. 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 se nabízí několik alternativ. ***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)***:

- ***Léčit*** - toto tlačítko se zobrazí pouze v případě, že detekovanou infekci 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 (Doporučeno)*** - 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 infekci*** - tuto možnost rozhodně nedoporučujeme nikomu, kdo nemá skutečně dobrý důvod ji použít!

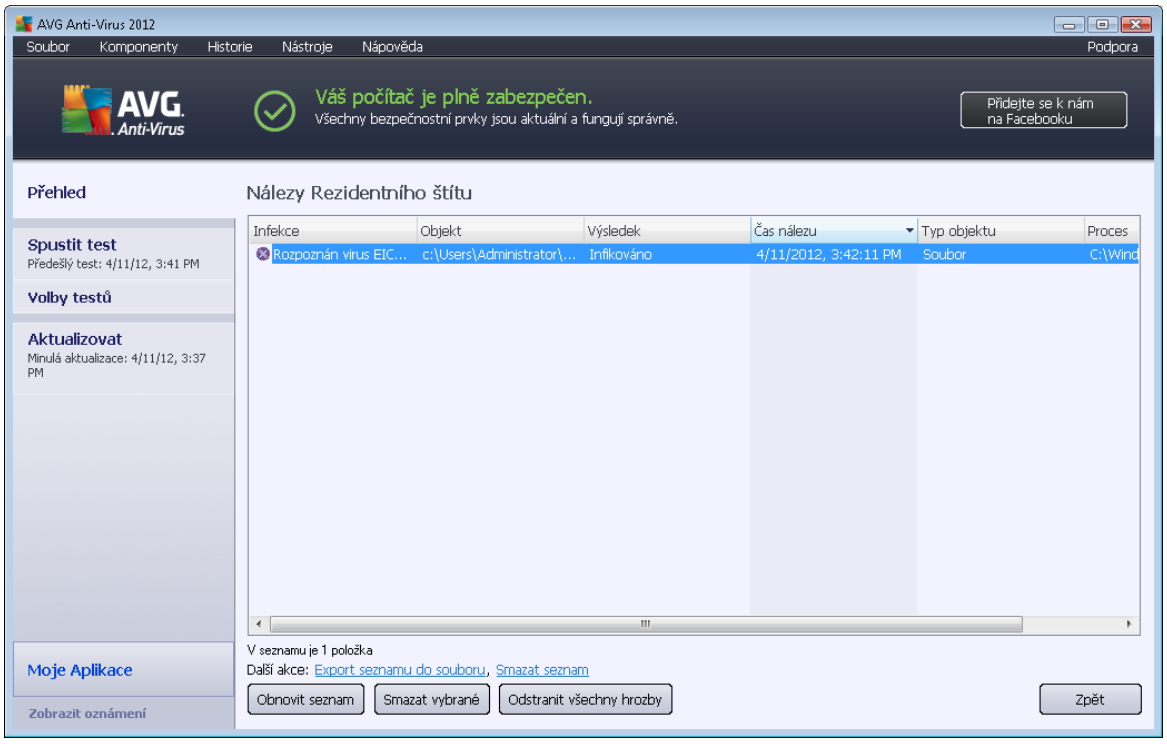
Poznámka: *Může se stát, že velikost detekovaného objektu bude větší než objem volného prostoru ve Virovém trezoru. V tom případě budete při pokusu o přesun infikovaného objektu vyrozuměni*

varovným hlášením o nedostatku místa ve Virovém trezoru. Objem Virového trezoru si však můžete sami nastavit. Velikost prostoru ve Virovém trezoru je dána percentuálně a závisí na celkové velikosti vašeho pevného disku. Nastavení velikosti Virového trezoru lze provést v dialogu Virový trezor v rámci Pokročilého nastavení AVG, položka 'Omezit velikost Virového trezoru'.

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

Přehled nálezů Rezidentního štítu

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 hlavního dialogu AVG (*přehled komponent*).

6.2. LinkScanner

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

LinkScanner podporuje tyto vyhledavače: Google Search, Yahoo Search, Bing Search.

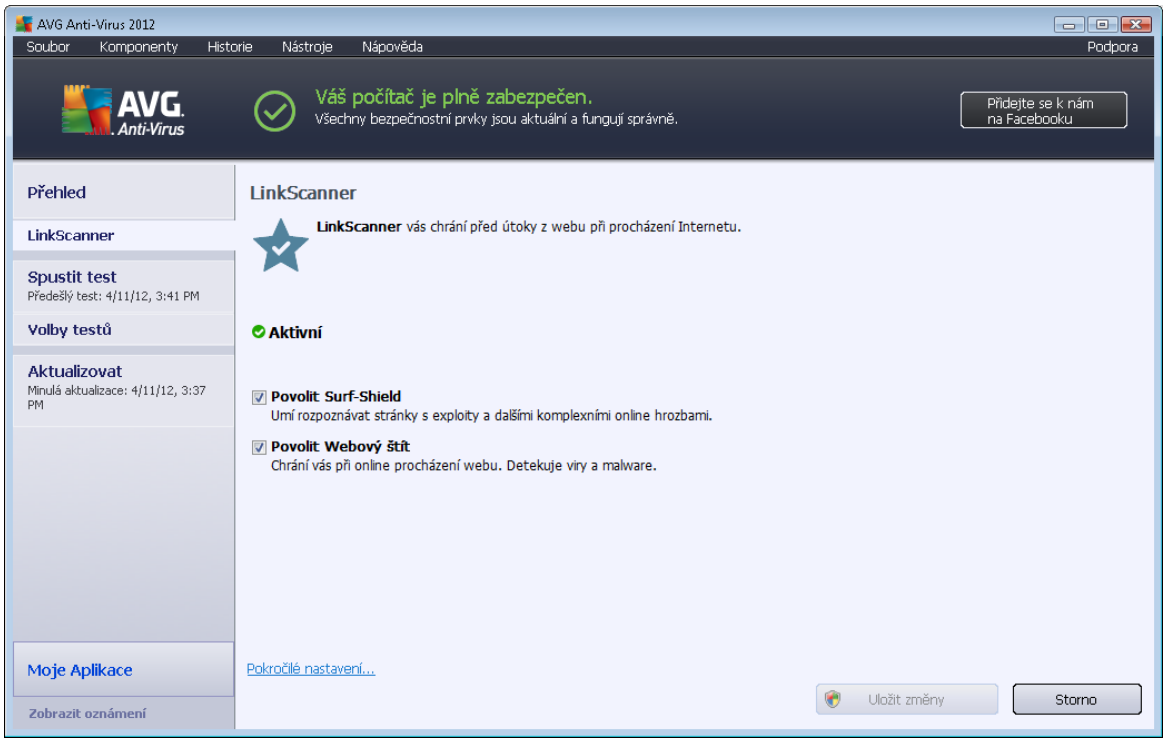
LinkScanner není určen k ochraně serverů!

Technologie ***LinkScanner*** obsahuje tyto hlavní funkce:

- Surf-Shield zabraňuje infikování počítače při nechtěném stahování nebezpečných souborů či skriptů a zároveň zajišťuje, že stránky, které navštívíte, nabízejí ve chvíli jejich otevření bezpečný obsah. Funkce testuje obsah internetových stránek, které navštěvujete, bez ohledu na internetovou adresu stránky.
- Webový štít funguje jako ochrana v reálném čase při surfování po Internetu. Tato služba testuje obsah navštívených webových stránek a souborů v nich obsažených, a to ještě před tím, než jsou zobrazeny ve vašem prohlížeči nebo staženy na váš počítač. Webový štít detekuje případné viry a spyware obsažené ve stránce, kterou se chystáte navštívit, a okamžitě zabrání jejich stažení a v případě, že při jeho načítání detekuje virus nebo spyware, okamžitě zabrání jejich stažení.

6.2.1. Rozhraní Link Scanneru

Hlavní dialog komponenty LinkScanner uvádí stručný popis funkcí této komponenty a zprávu o jejím aktuálním stavu *(Aktivní)*:



Ve spodní části dialogu lze provést základní nastavení funkcí komponenty:

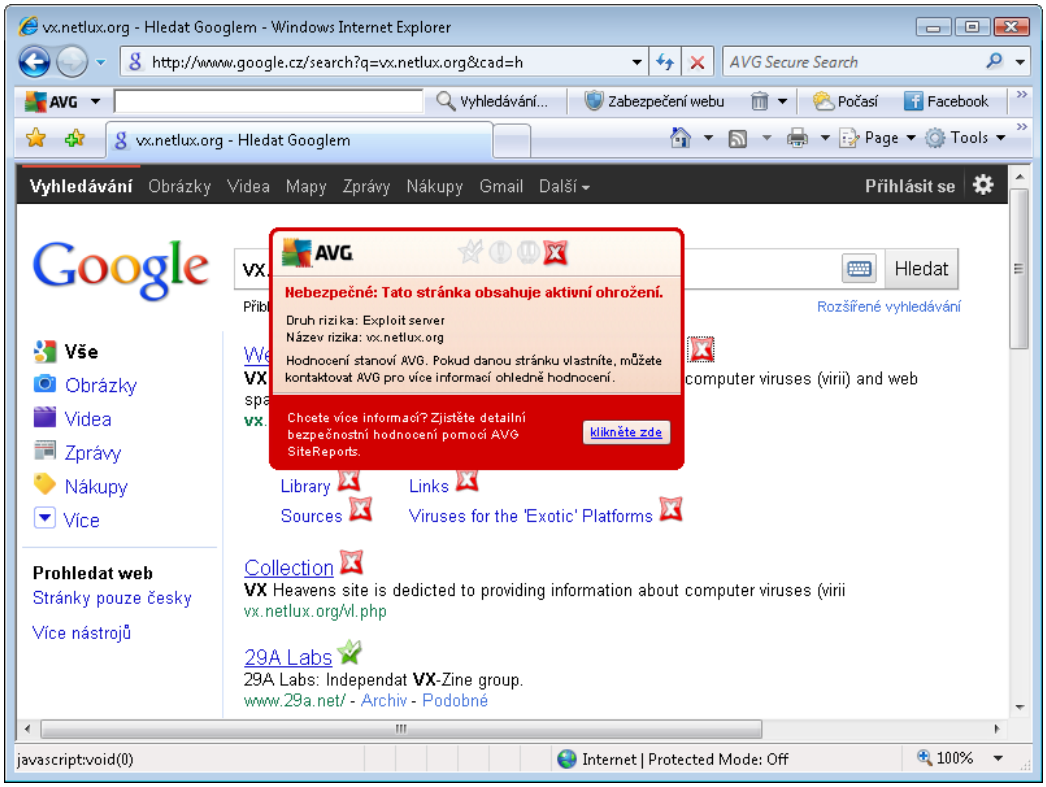
- ***Povolit Surf-Shield*** - (*ve výchozím nastavení zapnuto*): Označením či zrušením označení této položky lze službu Surf-Shield aktivovat či deaktivovat.
- ***Povolit Webový štít*** - (*ve výchozím nastavení zapnuto*): Označením či zrušením označení této položky aktivujete či vypnete službu Webový štít.

Výchozí konfigurace* AVG Anti-Virus 2012 *je nastavena k optimálnímu výkonu programu. Proto doporučujeme výchozí nastavení ponechat, pokud nemáte skutečně dobrý důvod je měnit.

6.2.2. Nálezy služby Surf-Shield

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

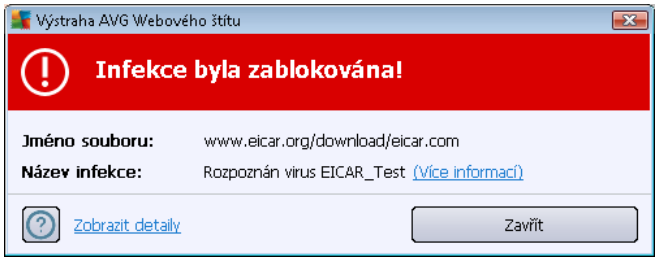
Narazíte-li na nebezpečnou webovou stránku, LinkScanner vás bude varovat tímto oznámením:



Vstup na takto označenou stránku rozhodně nedoporučujeme!

6.2.3. Nálezy Webového štítu

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

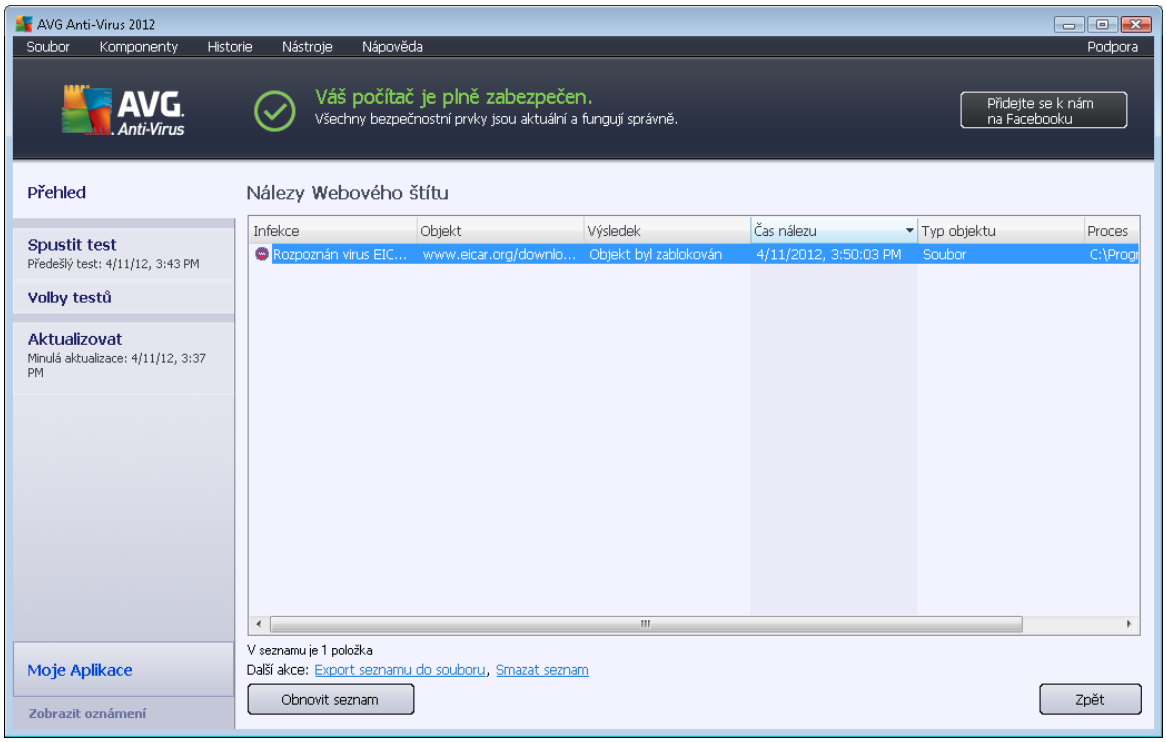


V tomto varovném dialogu najdete informaci o souboru, který byl detekován jako infikovaný (*Jméno souboru*) a jméno rozpoznané infekce (*Název infekce*), a odkaz do Virové encyklopedie, kde najdete podrobnější informace o rozpoznané infekci, jsou-li tyto údaje známy. V dialogu jsou dostupná tato tlačítka:

- ***Zobrazit detaily*** - kliknutím na tlačítko otevřete nové pop-up okno s informací o procesu, při němž došlo k detekci infekce, a s uvedeným identifikačním číslem procesu.

- ***Zavřít*** - tímto tlačítkem varovný dialog zavřete.

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



U každého z detekovaných objektů jsou k dispozici následující informace:

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

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

Ovládací tlačítka

- ***Obnovit seznam*** - aktualizujete seznam všech nálezů
- ***Zpět*** - přejdete zpět do výchozího hlavního dialogu AVG *(přehled komponent)*

6.3. E-mailová ochrana

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

Komponenta ***E-mailová ochrana*** zodpovídá za kontrolu veškeré příchozí i odchozí pošty. Pokud je v e-mailové zprávě detekován virus, je okamžitě přemístěn do Virového trezoru. Komponenta umí také odfiltrovat určité typy e-mailových příloh a označovat prověřené e-mailové zprávy certifikačním textem. ***E-mailová ochrana*** zahrnuje dvě základní funkce:

- Kontrola příchozí a odchozí pošty
- Anti-Spam kontrola

6.3.1. Kontrola pošty

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

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

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

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

Kontrola pošty není určena k ochraně poštovních serverů!

6.3.2. Anti-Spam

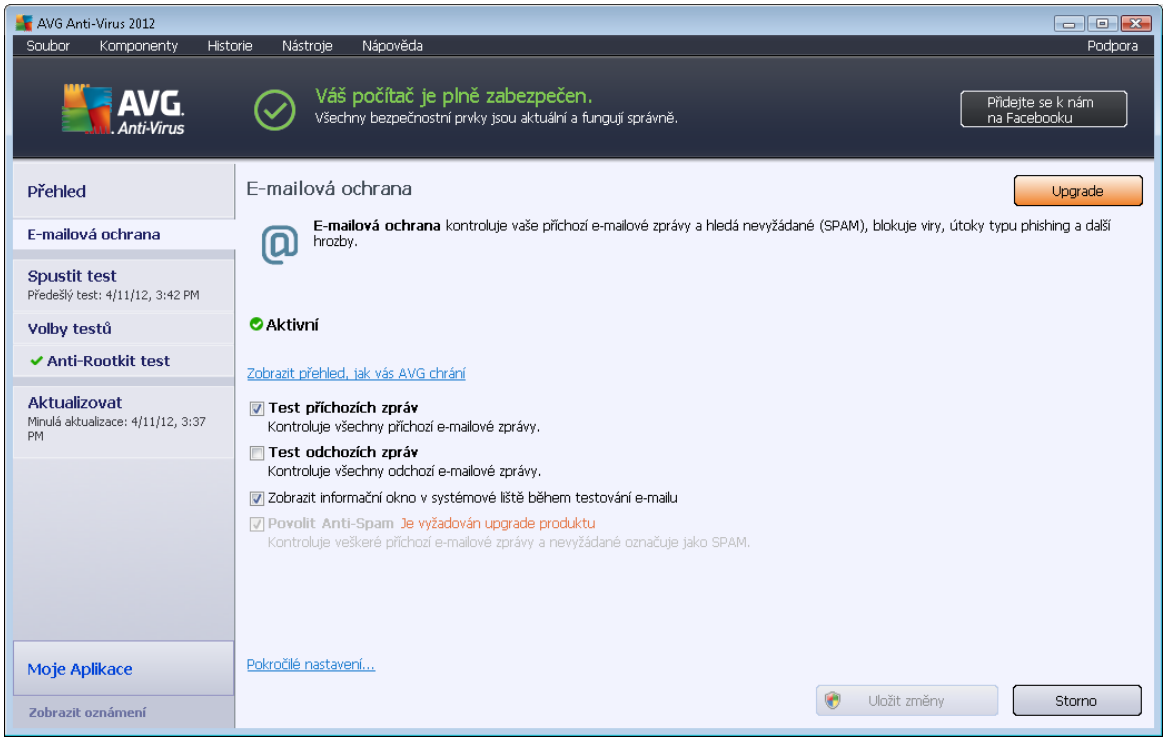
Jak funguje Anti-Spam?

Anti-Spam kontroluje veškerou příchozí poštu a nežádoucí zprávy označuje jako spam. ***Anti-Spam*** dokáže upravit předmět emailu, který je identifikován jako spam, přidáním vámi definovaného textového řetězce. Poté již můžete snadno filtrovat emaily podle definovaného označení ve vašem poštovním klientovi. K detekci spamu v jednotlivých zprávách používá ***Anti-Spam*** několika analytických metod a zaručuje tedy maximální úroveň ochrany proti nevyžádané poště. ***Anti-Spam*** pracuje s pravidelně aktualizovanou databází a lze nastavit i kontrolu pomocí RBL serverů (*veřejných seznamů "nebezpečných" e-mailových adres*) nebo ručně přidávat povolené (*Whitelist*) a zakázané (*Blacklist*) poštovní adresy.

Co je to spam?

Termínem spam označujeme nevyžádanou elektronickou poštu, převážně reklamního charakteru, jež je jednorázově hromadně rozesílána obrovskému počtu adresátů, čímž zahlcuje jejich poštovní schránky. Termín spam se nevztahuje na oprávněný e-mail komerčního charakteru, k jehož přijetí dal zákazník svůj souhlas. Spam je nejen nepříjemný a obtížný, ale je také častým zdrojem virů nebo distributorem textu urážlivého charakteru.

6.3.3. Rozhraní komponenty E-mailová ochrana



V dialogu ***E-mailová ochrana*** najdete stručný popis funkce komponenty a informaci o aktuálním stavu komponenty *(Aktivní).* Prostřednictvím odkazu ***Zobrazit online přehled, jak Vás AVG chrání*** se můžete přepnout na dedikovanou stránku na webu AVG (http://www.avg.cz/), kde najdete detailní

statistiku aktivity a detekcí **AVG Anti-Virus 2012**.

Základní nastavení E-mailové ochrany

Dále máte v dialogu ***E-mailová ochrana*** možnost editovat základní nastavení komponenty:

- ***Test příchozích zpráv*** *(ve výchozím nastavení zapnuto)* - Označením položky určíte, že má být prováděna kontrola všech doručených emailů.
- ***Test odchozích zpráv*** *(ve výchozím nastavení vypnuto)* - Označením položky definujete, že mají být testovány veškeré odesílané emaily.
- ***Zobrazit informační okno v systémové liště během testování e-mailu*** *(ve výchozím nastavení zapnuto)* - Označením položky definujete, zda si přejete zobrazit oznamovací dialog, který se objeví nad ikonou AVG na systémové liště při zahájení testování pošty.

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.

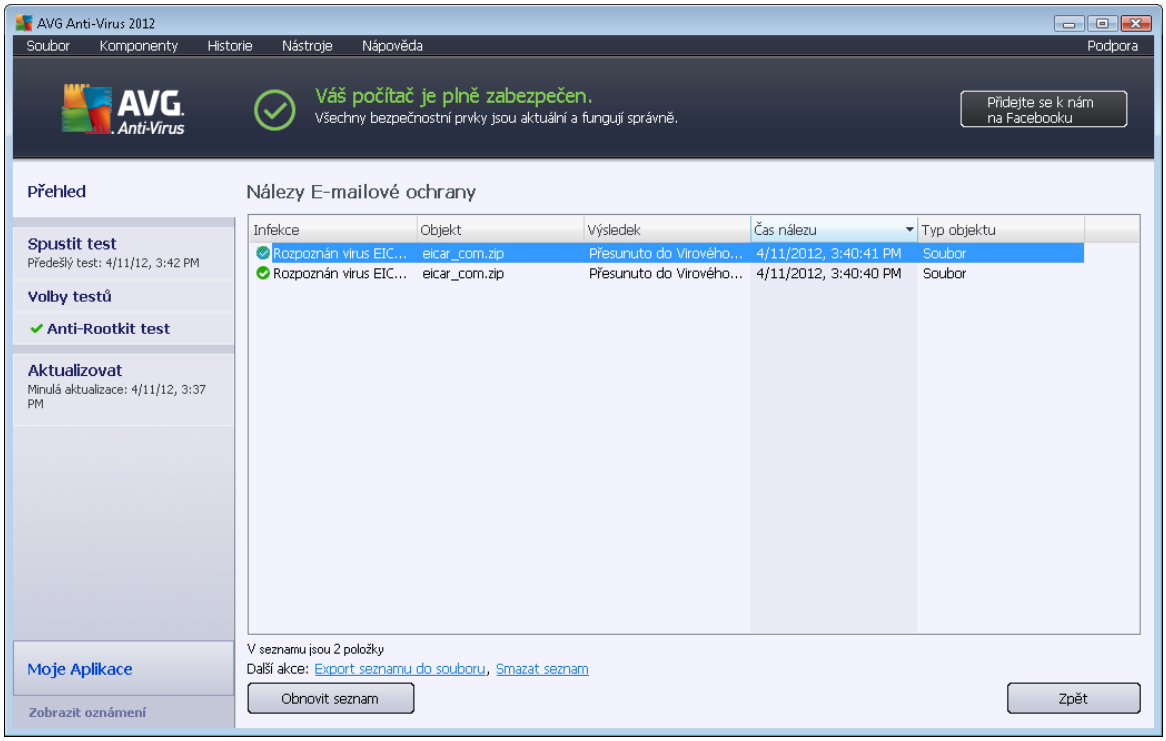
Položka ***Povolit Anti-Spam*** aktivuje filtraci nežádoucích zpráv v příchozí poště. Služba Anti-Spam však bohužel není v rámci **AVG Anti-Virus 2012** dostupná a je k dispozici pouze ve vyšších edicích AVG. ***Navštivte prosím web AVG (http://www.avg.cz/), kde najdete informace o možnostech přechodu na vyšší verzi produktu.***

Ovládací tlačítka

Ovládací tlačítka dostupná v dialogu ***E-mailová ochrana***:

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

6.3.4. Nálezy E-mailové ochrany



V dialogu ***Nálezy Kontroly pošty*** (*dostupném ze systémového menu volbou položek Historie / Nálezy Kontroly pošty*) se bude zobrazovat seznam nálezů detekovaných komponentou E-mailová ochrana. U každého z detekovaných objektů jsou k dispozici následující informace:

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

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

Ovládací tlačítka

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

- ***Obnovit seznam*** - Aktualizuje seznam nálezů podle momentálního stavu.
- ***Zpět*** - Přejdete zpět do předchozího zobrazeného dialogu.

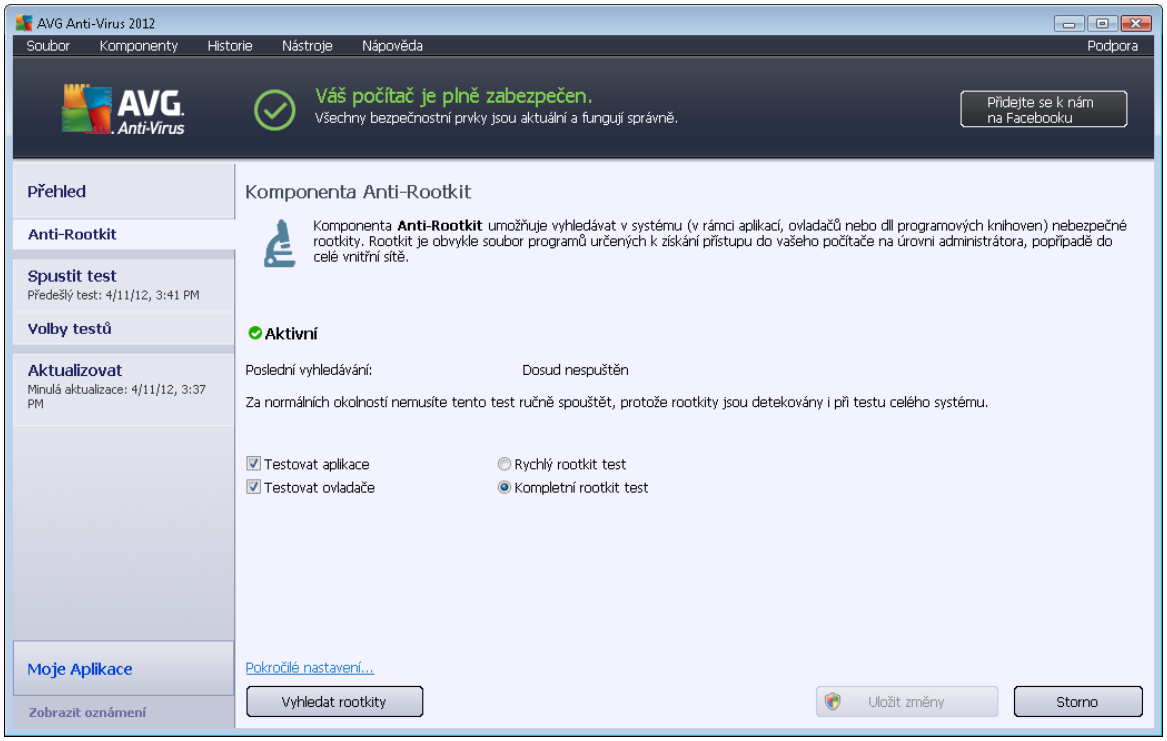
6.4. Anti-Rootkit

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 ***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.

Co je to 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.

6.4.1. Rozhraní komponenty Anti-Rootkit



Dialog komponenty ***Anti-Rootkit*** uvádí stručný popis základní funkčnosti této komponenty, informaci o stavu komponenty *(Aktivní)* a dále informaci o době a času posledního spuštění komponenty (*Poslední vyhledávání; vyhledávání rootkitů probíhá ve výchozím nastavení automaticky v rámci Testu celého počítače*). V dialogu komponenty ***Anti-Rootkit*** je dále uveden odkaz Nástroje/ Pokročilé nastavení, kterým se přepnete do prostředí editace komponenty ***Anti-Rootkit***.

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.

Základní nastavení Anti-Rootkitu

Ve spodní části dialogu 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 ovladače***

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

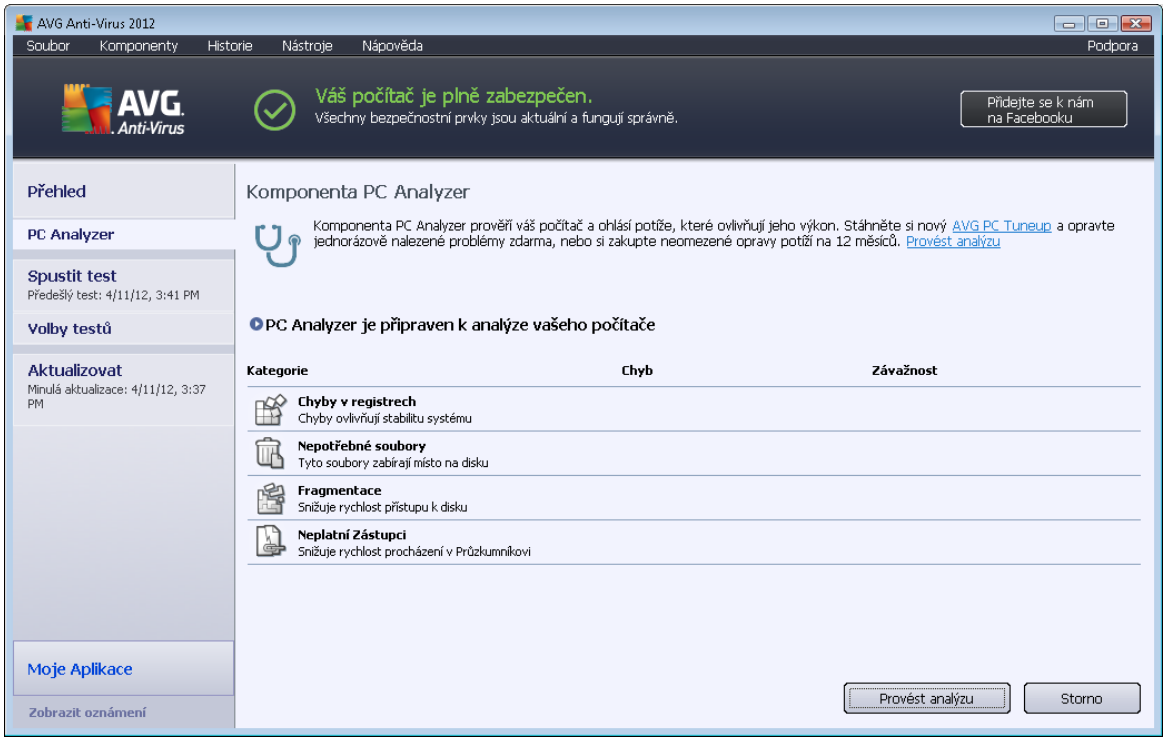
- ***Rychlý rootkit test*** - Testuje všechny běžící procesy, nahrané ovladače a systémový adresář (*většinou c:\Windows*).
- ***Kompletní rootkit test*** - Testuje všechny všechny běžící procesy, nahrané ovladače, systémový adresář (*většinou c:\Windows*) a také všechny lokální disky (*včetně flash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

Ovládací tlačítka dialogu

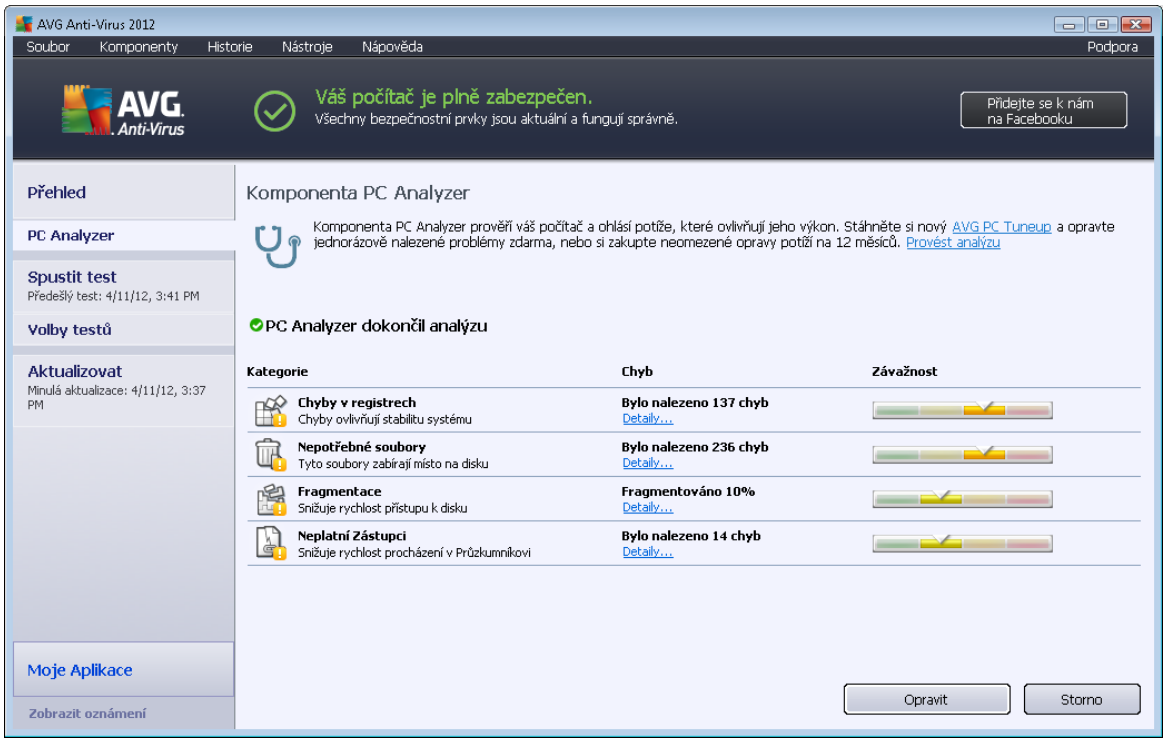
- ***Vyhledat rootkity*** - Jelikož testování přítomnosti rootkitů není implicitní součástí Testu celého počítače, slouží dialog ***Anti-Rootkit*** přímo ke spuštění samostatného testu; test spustíte stiskem tohoto tlačítka.
- ***Uložit změny*** - Stiskem tlačítka aplikujete veškeré změny v nastavení,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

6.5. PC Analyzer

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



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



- ***Chyby v registrech*** uvádí počet chyb v registrech Windows. Oprava registrů vyžaduje

poměrně pokročilé znalosti, nedoporučujeme vám tudíž pouštět se do opravy na vlastní pěst.

- ***Nepotřebné soubory*** uvádí počet souborů, bez nichž byste se pravděpodobně obešli. Typickým příkladem mohou být různé typy dočasných souborů a soubory v odpadkovém koši.

- ***Fragmentace*** spočítá, jaká procentuální část vašeho pevného disku je fragmentována. Fragmentací pevného disku rozumíme skutečnost, že pevný disk se již dlouho používán a jednotlivé na něm uložené soubory jsou tedy fyzicky roztroušeny na různých částech disku. Tento problém lze odstranit použitím libovolného nástroje pro defragmentaci.

- ***Poškozené odkazy*** spočítá existující odkazy, které již nejsou funkční, například proto, že vedou na neexistující lokace.

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

Ovládací tlačítka

- ***Provést analýzu*** *(tlačítko se zobrazí před zahájením analýzy)* - stiskem tlačítka spustíte okamžitou analýzu počítače

- ***Opravit*** *(tlačítko se zobrazí po dokončení analýzy)* - stiskem tlačítka přejdete na web AVG (http://www.avg.cz/) na stránce s podrobnými a aktuálními informacemi o komponentě PC Analyzer

- ***Storno*** - stiskem tlačítka můžete přerušit právě běžící analýzu, anebo se vrátit do výchozího hlavního dialogu AVG *(přehled komponent)* po ukončení procesu analýzy

6.6. Identity Protection

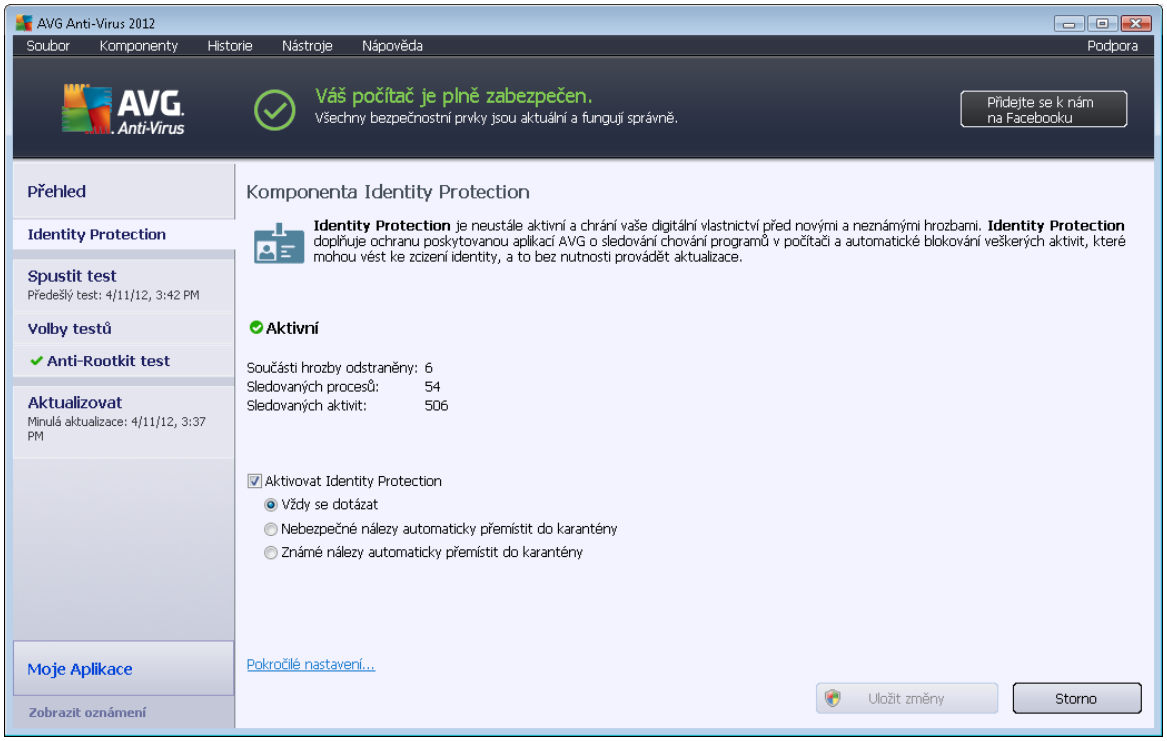
Identity Protection je komponentou, která průběžně a v reálném čase zajišťuje ochranu před různými druhy malware a virů, a to na bázi identifikace specifického chování těchto typů aplikací. ***Identity Protection*** zajišťuje bezpečnost při nákupech, bankovních operacích a jiných elektronických transakcích. Slouží k detekci malware a je zaměřena na prevenci zcizení osobních dat (*přístupová hesla, bankovní účty, čísla kreditních karet, ...*) a cenných informací prostřednictvím škodlivého software (*malware*), který útočí na váš počítač. ***Identity Protection*** zajistí, že všechny programy běžící na vašem počítači nebo ve vaší síti pracují správně. ***Identity Protection*** rozpozná jakékoliv podezřelé chování a škodlivý program zablokuje.

Identity Protection zajišťuje v reálném čase ochranu vašeho počítače proti novým a dosud neznámým hrozbám. Monitoruje všechny *(i skryté)* procesy a více než 285 různých vzorců chování, takže dokáže rozpoznat potenciálně nebezpečné chování v rámci vašeho systému. Díky této schopnosti umí ***Identity Protection*** detekovat hrozby, které ještě ani nejsou popsány ve virové databázi. Jakmile se neznámý kus kódu dostane do vašeho počítače, ***Identity Protection*** jej sleduje, pozoruje a zaznamenává případné příznaky škodlivého chování. Jestliže je soubor shledán škodlivým, ***Identity Protection*** jej přemístí do Virového trezoru a vrátí zpět do původního stavu veškeré změny systému provedené tímto kódem *(vložené kusy kódu, změny v registrech, otevřené*

porty apod.). ***Identity Protection*** vás chrání, aniž byste museli spouštět jakýkoliv test. Tato technologie je vysoce proaktivní, aktualizaci vyžaduje jen zřídka a trvale hlídá vaše bezpečí.

Identity Protection je bezpečnostní složkou komplementární ke komponentě Anti-Virus. Pro naprostou bezpečnost vašeho počítače důrazně doporučujeme, abyste si nainstalovali obě komponenty!

6.6.1. Rozhraní Identity Protection



Dialog ***Identity Protection*** uvádí stručný popis základní funkčnosti této komponenty, informaci o stavu komponenty *(Aktivní)* a dále některé další statistické údaje:

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

Základní nastavení Identity Protection

Ve spodní části rozhraní můžete nastavit některé základní funkce komponenty:

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

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

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

- ***Pokročilé nastavení*** - Kliknutím na odkaz budete přesměrováni do příslušného dialogu Pokročilého nastavení **AVG Anti-Virus 2012**, kde můžete editovat konfiguraci komponenty do nejmenších podrobností. Mějte však na paměti, že výchozí konfigurace všech komponent **AVG Anti-Virus 2012** je nastavena tak, aby program podával optimální výkon a poskytoval maximální možnou úroveň bezpečí. Pokud nemáte skutečný důvod ke změně, doporučujeme ponechat výchozí nastavení!

Ovládací tlačítka dialogu

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

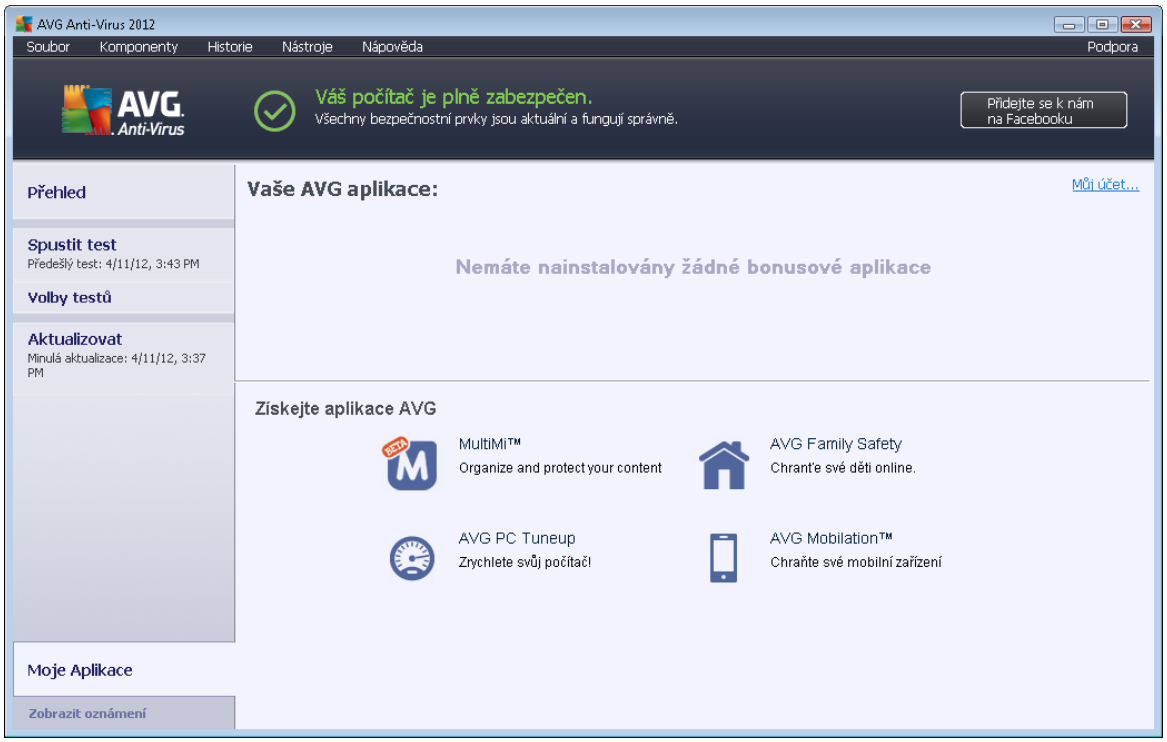
- ***Uložit změny*** - stiskem tohoto tlačítka budou uloženy všechny v tomto dialogu provedené změny
- ***Storno*** - stiskem tlačítka se vrátíte do výchozího hlavního dialogu AVG (*přehled komponent*)

6.7. Vzdálená správa

Komponenta ***Vzdálená správa*** se v hlavním dialogu **AVG Anti-Virus 2012** zobrazí pouze v případě, že jste instalovali síťovou verzi produktu *(informaci o instalované licenci najdete na záložce Verze v dialogu Informace, který lze otevřít ze systémového menu volbou položky Podpora)*. 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 webu AVG (http://www.avg.cz/) v sekci ***Centrum podpory / Stáhnout / Dokumentace***.

7. Moje Aplikace

Dialog ***Moje Aplikace*** *(dostupný kniknutím na tlačítko Moje Aplikace v hlavním dialogu AVG)* nabízí přehled samostatných AVG aplikací:



Dialog je rozdělen do dvou částí:

- ***Vaše AVG aplikace*** - sekce obsahuje přehled všech samostatných AVG aplikací, které již máte na svém počítači nainstalovány;
- ***Get AVG Apps*** - sekce nabízí přehled samostatných AVG aplikací, které na svém počítači nemáte a které by Vás mohly zajímat. Tyto aplikace jsou připraveny k okamžité instalaci. Nabídka aplikací se dynamicky mění podle Vaší licence, podle země, v níž se nacházíte, a podle dalších kritérií. Podrobné informace o aktuální nabídce najdete na webu AVG (http://www.avg.cz/).

Následující seznam uvádí všechny dostupné samostatné AVG aplikace a stručně popisuje jejich funkčnost:

7.1. AVG LiveKive

AVG LiveKive je aplikací pro online zálohování na zabezpečených serverech. ***AVG LiveKive*** automaticky zálohuje veškeré vaše dokumenty, fotografie a hudbu na bezpečném místě. V tomto záložním umístění budou vaše data dostupná odkudkoliv, z počítače i z mobilu s webovým rozhraním, a můžete je sdílet se svou rodinou či přáteli. ***AVG LiveKive*** nabízí tyto vlastnosti:

- Bezpečné zálohy v případě, že by došlo k poškození Vašeho počítače a/nebo pevného

disku

- Přístup k Vašim datům z jakéhokoliv příslušenství připojenému k Internetu
- Snadnou organizaci dat
- Sdílení dat s autorizovanými osobami

Podrobné informace o aplikaci najdete na dedikované stránce AVG, k níž se připojíte prostřednictvím odkazu AVG LiveKive v dialogu Moje aplikace.

7.2. AVG Mobilation

AVG Mobilation nabízí zabezpečení Vašeho mobilního telefonu *(smart phone)* proti virům a malware. Zároveň slouží jako ochrana proti zneužití Vašcih osobních dat, pokud telefon ztratíte nebo Vám bude odcizen. ***AVG Mobilation*** obsahuje tyto funkce:

- *Prověřování souborů* umožňuje testování souborů v jednotlivých úložištích;
- *Task Killer* dokáže ukončit libovolnou aplikaci v případě, že se telefon výrazně zpomalil nebo zasekl;
- *Uzamknutí aplikace* nabízí možnost chránit aplikace heslem proti zneužití;
- *Tuneup* shromažďuje jednotlivé systémové parametry do jednoho přehledu pro snazší správu systému;
- *Záloha aplikací* umožňuje zálohovat aplikace na paměťovou kartu a později je ze zálohy obnovit;
- *Spam a falešné stránky* označí Vámi vybrané SMS zprávy jako spam a nahlášené webové stránky jako podvodné;
- *Smazat osobní údaje* vzdáleně smaže veškerá Vaše osobní data z telefonu v případě, že Vám byl odcizen;
- *Bezpečné procházení webu* nabízí průběžnou kontrolu webových stránek, které navštívíte.

Podrobné informace o aplikaci najdete na dedikované stránce AVG, k níž se připojíte prostřednictvím odkazu AVG Mobilation v dialogu Moje aplikace.

7.3. AVG Family Safety

AVG Family Safety pomáhá ochránit vaše děti před nevhodným obsahem webových stránek, internetových médií a výsledků vyhledávání. ***AVG Family Safety*** umožňuje sledovat i aktivity Vašich dětí v sociálních sítích a diskusních skupinách. Pokud dojde k detekci slov, frází či vět, která mohou poukazovat na potenciální ohrožení Vašich dětí, budete o této skutečnosti uvědoměni zasláním SMS zprávy nebo e-mailu. Pro každé ze svých dětí navíc můžete nastavit příslušnou úroveň zabezpečení a sledovat jejich činnost prostřednictvím samostatných účtů.

Podrobné informace o aplikaci najdete na dedikované stránce AVG, k níž se připojíte

prostřednictvím odkazu AVG Family Safety v dialogu Moje aplikace.

7.4. AVG PC Tuneup

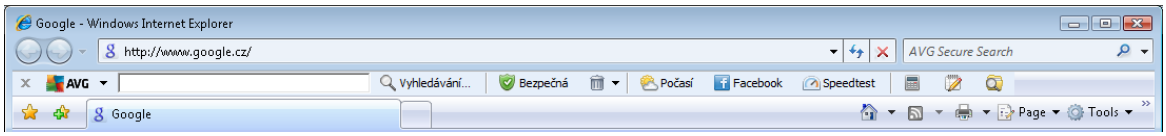
Application ***AVG PC Tuneup*** je pokročilým nástrojem pro detailní systémovou analýzu a optimalizaci, umožňující zrychlit a vylepšit výkon vašeho počítače. ***AVG PC Tuneup*** nabízí například tyto služby:

- vyčištění a defragmentace disku; oprava chybných sektorů
- oprava a defragmentace registrů
- optimalizace nastavení pro Internet, pročištění historie
- detekce a odstranění duplicitních souborů
- deaktivace zbytečných služeb, které zpomalují výkon počítače
- odinstalace nepoužívaných programů
- manuální správa programů spouštěných automaticky při startu Windows
- optimalizace systémových procesů
- přehled všech běžících procesů, služeb a uzamčených souborů
- přehled souborů, které zabírají nejvíce místa
- detailní přehled systémových informací

Podrobné informace o aplikaci najdete na dedikované stránce AVG, k níž se připojíte prostřednictvím odkazu AVG PC Tuneup v dialogu Moje aplikace.

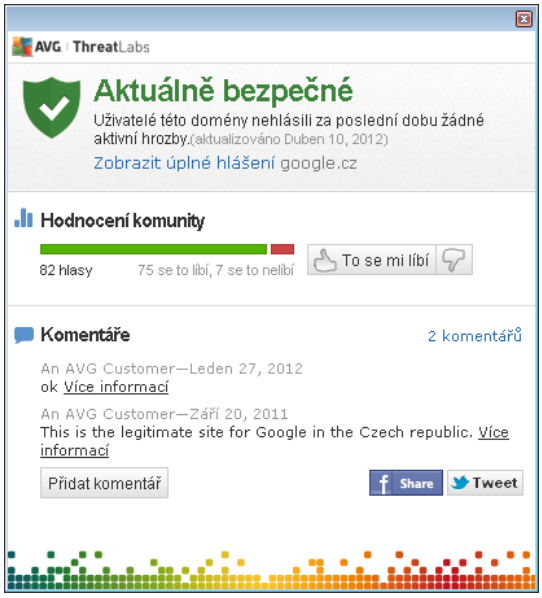
8. AVG Security Toolbar

AVG Security Toolbar je nástroj, který úzce spolupracuje s komponentou LinkScanner a zajišťuje Vaši maximální bezpečnost při veškerém pohybu online. ***AVG Security Toolbar*** se v rámci **AVG Anti-Virus 2012** instaluje volitelně; možnost rozhodnout se, zda tuto komponentu chcete instalovat, jste měli v průběhu instalačního procesu. ***AVG Security Toolbar*** je dostupný v podobě nástrojové lišty ve vašem internetovém prohlížeči. Podporovanými prohlížeči jsou Internet Explorer (*ve verzi 6.0 a vyšší*) a/nebo Mozilla Firefox (*ve verzi 3.0 a vyšší*). Jiné prohlížeče nejsou podporovány *(pokud používáte alternativní prohlížeč, např. Avant browser, můžete se setkat s nekorektním chováním)*.



AVG Security Toolbar je tvořen těmito prvky:

- ***Logo AVG*** s rozbalovací nabídkou:
  - ***Použít bezpečné vyhledávání AVG*** - Umožňuje vyhledávání prostřednictvím vyhledavače ***AVG Secure Search***, kdy jsou všechny výsledky vyhledávání jsou průběžně kontrolovány službou Search-Shield a máte tak naprostou jistotu bezpečného pohybu online.
  - ***Aktuální míra ohrožení*** - Otevře web virové laboratoře s grafickým znázorněním aktuální úrovně nebezpečí na Internetu.
  - ***AVG Threat Labs*** - Otevře stránku ***AVG Threat Lab*** *(http://www.avgthreatlabs.com)*, kde najdete informace o bezpečnosti jednotlivých webů a aktuální úrovni online ohrožení.
  - ***Nápověda k liště*** - Otevírá online nápovědu k jednotlivým funkcím ***AVG Security Toolbar***.
  - ***Odeslat zpětnou vazbu k produktu*** - Otevře stránku s online formulářem, jehož prostřednictvím nám můžete zaslat svůj názor na ***AVG Security Toolbar***.
  - ***O aplikaci*** - Otevře samostatné okno s informací o aktuální instalované verzi ***AVG Security Toolbar***.
- ***Vyhledávací pole*** - Při vyhledávání prostřednictvím ***AVG Security Toolbar*** můžete snadno prohledávat web a mít jistotu, že všechny zobrazené výsledky budou zaručeně bezpečné. Do vyhledávacího pole zadejte klíčové slovo nebo frázi a stiskněte tlačítko ***Vyhledávání*** nebo klávesu ***Enter***. Všechny výsledky vyhledávání jsou průběžně kontrolovány službou Search-Shield *(v rámci komponenty LinkScanner)*.
- ***Zabezpečení*** - Tlačítkem otevřete nový dialog s informací o úrovni bezpečnosti na webové stránce, kde se právě teď nacházíte (*Aktuálně bezpečné*). Tento přehled pak můžete otevřít přímo v okně prohlížeče se všemi detaily o bezpečnostních aktivitách vztažených k právě prohlížené stránce (*Zobrazit úplné hlášení*):



- ***Vymazat*** - Tlačítko s ikonou odpadkového koše otevírá rozbalovací menu, kde si můžete vybrat, zda chcete vymazat informace o navštívených stránkách, stahovaných souborech, informace uvedené do formulářů anebo vymazat kompletně celou historii vašeho vyhledávání na webu.

- ***Počasí*** - Tlačítkem otevřete samostatné okno s informací o aktuálním počasí v dané lokalitě a s výhledem na následující dva dny. Tato informace je aktualizována každých 3-6 hodin. V dialogu můžete ručně změnit požadovanou lokalitu a také rozhodnout, zda si přejete uvádět teplotu ve stupních Celsia nebo Fahrenheita.

- ***Facebook*** - Tlačítko umožňuje přímé připojení k sociální síti Facebook z prostředí ***AVG Security Toolbaru***.

- ***Speedtest*** - Tlačítko umožňuje přístup k on-line aplikaci, s jejíž pomocí můžete ověřit funkčnost vašeho připojení k internetu *(ping)*, rychlost stahování a nahrávání.

- Zkratková tlačítka pro rychlý přístup k aplikacím ***Kalkulačka***, ***Poznámkový blok***, ***Průzkumník Windows***.

9. AVG Do Not Track

AVG Do Not Track dokáže identifikovat webové stránky, které sbírají data o vaší činnosti online. Ikona v prohlížeči zobrazí informaci o webových stránkách či reklamních sítích, jež sbírají informace o vaší aktivitě a nabídne vám možnost sběr dat povolit nebo nepovolit.

- ***AVG Do Not Track*** vám poskytne dodatečné informace o ochraně osobních údajů každé webové stránky a také přímý odkaz na možnost odhlášení konkrétní služby, pokud je tato k dispozici.
- ***AVG Do Not Track*** také podporuje protokol W3C DNT, který automaticky vyrozumí příslušnou webovou stránku, že si nepřejete být sledováni. Tato notifikace je ve výchozím nastavení zapnuta, ale lze ji vypnout.
- ***AVG Do Not Track*** je službou poskytovanou za těchto podmínek.
- ***AVG Do Not Track*** je ve výchozím nastavení zapnutý, ale lze jej libovolně deaktivovat. Instrukce k deaktivaci služby najdete v sekci FAQ na stránce Jak vypnout funkci AVG Do Not Track.
- Další podrobné informace o službě ***AVG Do Not Track*** najdete na našem webu website.

Aktuálně je služba ***AVG Do Not Track*** podporovaná v prohlížečích Mozilla Firefox, Chrome a Internet Explorer. *(V prohlížeči Internet Explorer je ikona AVG Do Not Track umístěna zcela vpravo na panelu příkazů. Pokud ikonu ve výchozím nastavení prohlížeče nevidíte, ujistěte se prosím, že máte panel příkazů aktivován. Jestliže ikona přesto není na monitoru viditelná, potáhněte prosím panel příkazů směrem doleva, aby se zobrazily všechny dostupné ikony a tlačítka této nástrojové lišty.)*

9.1. Rozhraní služby AVG Do Not Track

Služba ***AVG Do Not Track*** dokáže rozpoznat různé typy sběru dat a o jejich případné detekci vás informuje tímto dialogem:

Veškeré detekované služby sběru dat jsou jmenovitě uvedeny v seznamu ***Sledování na této stránce*** . ***AVG Do Not Track*** rozlišuje tři typy sběru dat:

- ***Služba Web Analytics*** *(ve výchozím nastavení povoleny):* Služby poskytující lepší výkon a prohlížení příslušných webových stránek. V této kategorii najdete služby jakými jsou například Google Analytics, Omniture nebo Yahoo Analytics. Tyto služby nejsou ve výchozím nastavení blokovány a doporučujeme tuto konfiguraci ponechat. Při zablokování této kategorie služeb by mohlo dojít k chybám ve fungování samotné webové stránky.

- ***Tlačítka sociální sítě*** *(ve výchozím nastavení povoleny):* Prvky sloužící k lepší práci se sociálními sítěmi. Tato tlačítka propojují navštěvované stránky se sociálními sítěmi. Jste-li k těmto sítím přihlášeni, mohou tato tlačítka sbírat informace o vaší činnosti na Internetu. Mezi tlačítka sociálních sítí patří: modul plug-in sítě Facebook, tlačítko sítě Twitter, tlačítko Google +1 apod.

- ***Reklamní sítě*** *(některé reklamní sítě jsou ve výchozím nastavení blokovány):* Služby, které přímo či nepřímo sbírají nebo sdílejí na různých stránkách informace o vaší činnosti na Internetu s cílem nabízet individuální reklamy *(narozdíl od reklam založených na obsahu)*. Tyto služby se řídí zásadami ochrany osobních údajů příslušné reklamní sítě *(zásady ochrany osobních údajů jsou dostupné na webových stránkách dané sítě)*.

Poznámka: *V dialogu nemusí být vždy zobrazeny všechny tři sekce, pokud některá z popisovaných služeb není ve webové stránce přítomna.*

V dialogu jsou rovněž uvedeny dva hypertextové odkazy:

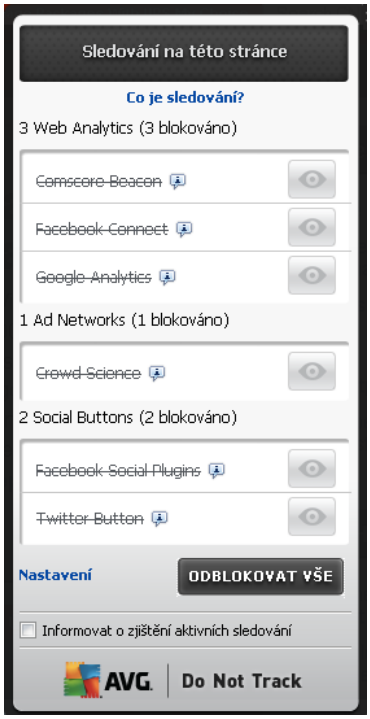
- ***Co je sledování?*** - kliknutím na tento odkaz v horní části dialogu budete přesměrováni na webovou stránku s podrobným vysvětlením principu sledování a popisem jednotlivých typů sledování.

- ***Nastavení*** - klinutím na tento odkaz ve spodní části dialogu budete přesměrováni na webovou stránku, kde máte možnost nastavit konkrétní parametry služby ***AVG Do Not Track*** *(podrobný popis nastavení najdete v kapitole Nastavení služby AVG Do Not Track)*

9.2. Informace o sledovacích procesech

V seznamu detekovaných služeb sběru dat uvádí vždy jen jméno konkrétní služby. Abyste se dokázali správně rozhodnout, zda službu zablokovat či povolit, budete potřebovat vědět více. Najeďte myší na konkrétní položku seznamu. Zobrazí se informační bublina s podrobnými údaji o službě. Dozvíte se, zda tato konkrétní služba sbírá data osobního charakteru či se soustředí na jiný druh dat, zda dochází ke sdílení dat s dalšími subjekty a zda uchovává nasbíraná data k dalšímu případnému použití.

Ve spodní části bubliny pak najdete aktivní odkaz ***Ochrana osobních údajů***, přes nějž budete přesměrování na stránku s prohlášením o ochraně osobních údajů na serveru příslušné detekované služby.

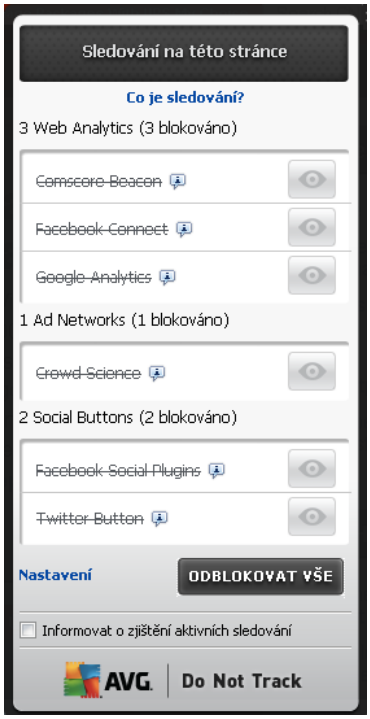


9.3. Blokování sledovacích procesů

Nad kompletním seznamem služeb Web Analytics / tlačítek sociální sítě / reklamních sítí se také snadno rozhodnete, které služby mají být blokovány. Na výběr máte ze dvou možností:

- ***Blokovat vše*** - Stiskem tohoto tlačítka, které je umístěno ve spodní části dialogu, zakážete jakýkoliv sběr dat všem detekovaným službám. *(Mějte však na paměti, že tento krok může způsobit poruchy funkčnosti webové stránky, v níž služba běží!)*

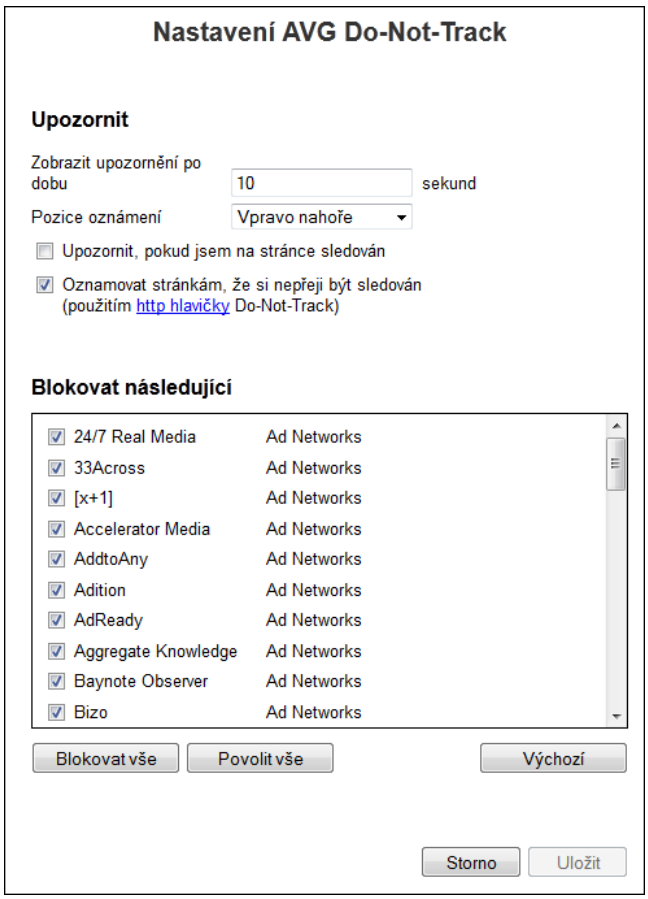
-  - Pokud nechcete jednorázově zablokovat všechny detekované služby, dá se blokování či povolení nastavit u každé z detekovaných služeb jednotlivě. Některým z detekovaných služeb například sledování povolíte*(například Web Analytics):* tyto systémy používají shromážděná data k optimalizaci své webové stránky a zlepšují tak uživatelské prostředí internetu. Současně však můžete zcela zakázat sledování všem službám zařazeným v kategorii reklamních sítí. Jednoduchým kliknutím na ikonu  u příslušného procesu tuto službu zablokujete *(v obrázku se zobrazí jako přeškrtnutý)* a nebo opět povolíte.



9.4. Nastavení služby AVG Do Not Track

Přímo v dialogu ***AVG Do Not Track*** je dostupná pouze jedna možnost konfigurace, a tou je zaškrtávací políčko nazvané ***Informovat o zjištění aktivních sledování***. Ve výchozím nastavení je tato položka vypnuta. Označením položky potvrdíte, že si přejete být vyrozuměni pokaždé, když vstoupíte na stránku, v níž bude detekován nová, dosud neblokovaná služba. Je-li položka označena a ***AVG Do Not Track*** detekuje novou službu sběru dat ve stránce, na níž se aktuálně nacházíte, objeví se na vaší obrazovce oznamovací dialog. V opačném případě, tedy pokud tuto volbu nezapnete, bude jediným indikátorem detekce nové služby změna barvy ikonky ***AVG Do Not Track*** *(umístěná na panelu příkazů vašeho prohlížeče)* ze zelené na žlutou.

Ve spodní části dialogu ***AVG Do Not Track*** najdete však také odkaz ***Nastavení***. Kliknutím na tento odkaz budete přesměrováni na samostatnou webovou stránku s možností dalšího detailního nastavení parametrů služby ***Nastavení AVG Do Not Track***:



- ***Zobrazit upozornění po dobu*** *(ve výchozím nastavení: 10)* - V tomto políčku můžete určit, po jak dlouhou dobu *(v sekundách)* si přejete ponechat notifikační dialog ***AVG Do Not Track*** zobrazený na vašem monitoru. Číslo musí spadat do rozmezí 0 až 60 sekund *(pokud nastavíte hodnotu 0, notifikační dialog se na vší obrazovce vůbec neobjeví)*.

- ***Pozice oznámení*** *(ve výchozím nastavení: Vpravo nahoře)* - Otevřete rozbalovací menu a vyberte, v jaké pozici na vašem monitoru se má notifikační dialog ***AVG Do Not Track*** zobrazovat.

- ***Upozornit, pokud jsem na stránce sledován*** *(ve výchozím nastavení vypnuto)* - Označením položky potvrdíte, že si přejete být vyrozuměni pokaždé, když vstoupíte na stránku, v níž bude detekována nová, dosud neblokovaná služba sběru dat. Je-li položka označena a ***AVG Do Not Track*** detekuje novou službu ve stránce, na níž se aktuálně nacházíte, objeví se na vaší obrazovce oznamovací dialog. V opačném případě, tedy pokud tuto volbu nezapnete, bude jediným indikátorem detekce nového sledovacího procesu změna barvy ikonky ***AVG Do Not Track*** *(umístěná na panelu příkazů vašeho prohlížeče)* ze zelené na žlutou.

- ***Oznamovat stránkám, že si nepřeji být sledován*** *(ve výchozím nastavení zapnuto)* -

Ponecháte-li položku označenou, bude ***AVG Do Not Track*** automaticky informovat provozovatele detekovaných služeb sběru dat, že si nepřejete být sledováni.

- ***Blokovat následující*** *(ve výchozím nastavení jsou všechny uvedené služby sběru dat povoleny)* - V této sekci najdete seznam všech známých služeb sběru dat, které lze klasifikovat jako reklamní sítě. Ve výchozím nastavení ***AVG Do Not Track*** blokuje některé z reklamních sítí automaticky, u jiných ponechává rozhodnutí na vaší volbě. Hromadně zablokovat všechny uvedené služby můžete kliknutím na tlačítko ***Blokovat vše***.

V konfigurační stránce ***Nastavení AVG Do Not Track*** jsou vám k dispozici tato ovládací tlačítka:

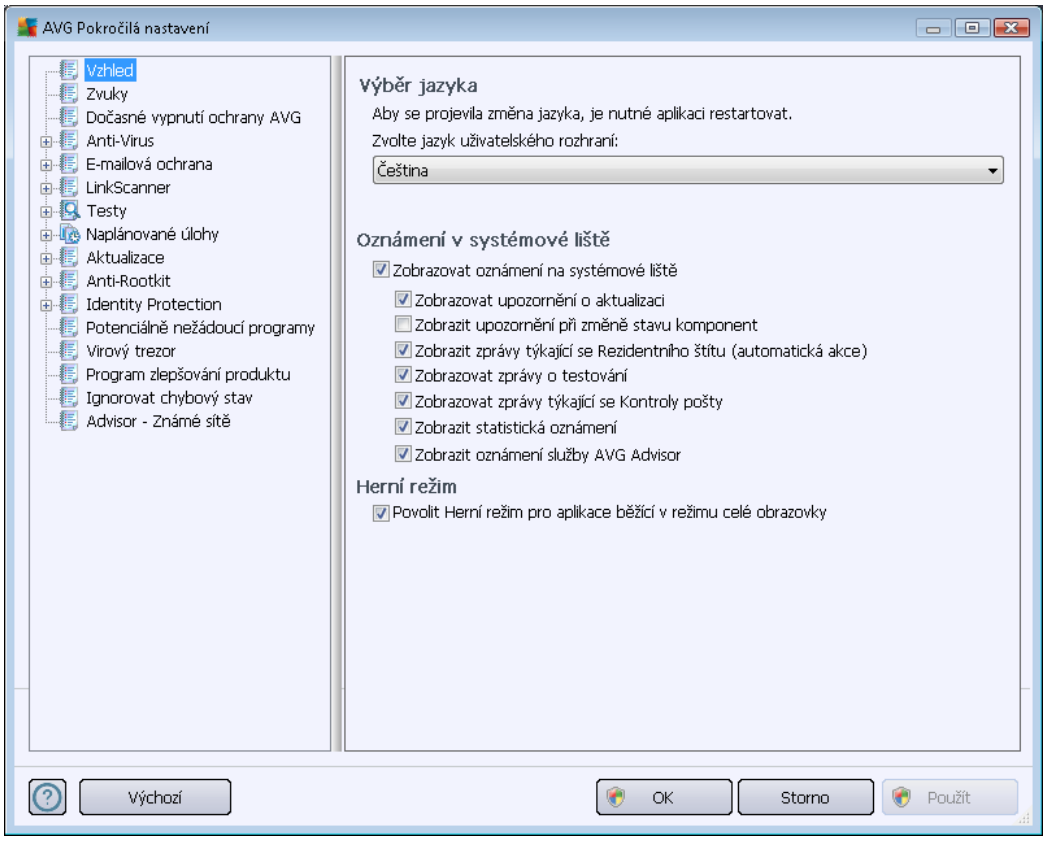
- ***Blokovat vše*** - kliknutím jednorázově zablokujete všechny výše uvedené služby v seznamu, jež jsou klasifikovány jako reklamní sítě;
- ***Povolit vše*** - kliknutím jednorázově povolíte všechny dříve zablokované služby uvedené v seznamu, jež jsou klasifikovány jako reklamní sítě;
- ***Výchozí*** - kliknutím zahodíte veškeré vlastní nastavení a vrátíte se k výchozí konfiguraci;
- ***Storno*** - kliknutím zrušíte všechna svá vlastní, dosud neuložená nastavení;
- ***Uložit*** - kliknutím použijete a uložíte veškerá vlastní provedená nastavení.

10. Pokročilé nastavení AVG

Dialog pro pokročilou editaci nastaveni programu **AVG Anti-Virus 2012** se otevírá v novém okně ***Pokročilé nastavení AVG***. Toto okno je rozděleno do dvou částí: v levé části okna najdete přehlednou stromově uspořádanou navigaci konfigurací programu. Volbou komponenty, jejíž parametry chcete editovat (*případně volbou konkrétní části této komponenty*) otevřete v pravé části okna příslušný editační dialog.

10.1. Vzhled

První položka navigačního seznamu, ***Vzhled***, se týká obecného nastavení hlavního dialogu **AVG Anti-Virus 2012** a nabízí možnost nastavení základních prvků programu:

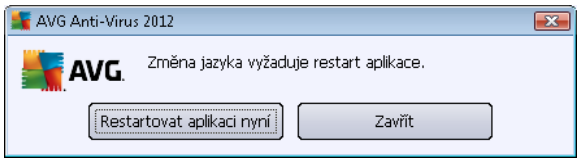


Výběr jazyka

V sekci ***Výběr jazyka*** můžete z rozbalovacího menu zvolit jazyk, v němž má být zobrazen hlavní dialog **AVG Anti-Virus 2012**. V nabídce budou dostupné jen ty jazyky, které jste zvolili během instalačního procesu (*viz kapitola Uživatelské volby*) a také angličtina (*angličtina se vždy instaluje automaticky*). Pro zobrazení **AVG Anti-Virus 2012** v požadovaném jazyce je však nutné aplikaci restartovat. Postupujte prosím následovně:

- V rozbalovacím menu zvolte požadovaný jazyk aplikace

- Svou volbu potvrďte stiskem tlačítka ***Použít*** *(vpravo ve spodním rohu dialog)*
- Stiskem tlačítka ***OK*** znovu potvrďte, že chcete změnu provést
- Objeví se nový dialog s informací o tom, že pro dokončení změny aplikace je nutné **AVG Anti-Virus 2012** restartovat
- Stiskem tlačítka ***Restartovat aplikaci nyní*** vyjádříte svůj souhlas s restartem a během sekundy se aplikace přepne do nově zvoleného jazyka:



Oznámení v systémové liště

V této sekci můžete potlačit zobrazování systémových oznámení o aktuálním stavu aplikace **AVG Anti-Virus 2012**. Ve výchozím nastavení programu jsou systémová oznámení povolena. Doporučujeme toto nastavení ponechat! Systémová oznámení přinášejí například informace o spuštění aktualizace či testu, o změně stavu některé komponenty **AVG Anti-Virus 2012** a podobně. Je rozhodně 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 Anti-Virus 2012**. Své vlastní nastavení můžete provést označením příslušné položky ve strukturované nabídce:

- ***Zobrazovat oznámení na systémové liště*** *(ve výchozím nastavení zapnuto)* - Položka je ve výchozím nastavení označena, takže se zobrazují veškerá informativní hlášení. Zrušením označení položky zcela vypnete zobrazování jakýchkoliv systémových oznámení. Jestliže je tato volba zapnuta, máte dále možnost definovat pravidla pro zobrazování jednotlivých typů informací:
  - ***Zobrazovat zprávy o aktualizaci v systémové liště*** *(ve výchozím nastavení zapnuto)* - 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*** *(ve výchozím nastavení vypnuto)* - Volbou položky rozhodnete, zda mají být zobrazena nebo naopak potlačena informativní hlášení o vypnutí/zapnutí komponenty, výskytu chyby ve funkci komponenty, apod. V případě hlášení problému odpovídá tato volba grafickým změnám ikony na systémové liště, která indikuje jakýkoliv problém v libovolné komponentě.
  - ***Zobrazit zprávy týkající se Rezidentního štítu v systémové liště (automatická akce)*** *(ve výchozím nastavení zapnuto)* - Volbou položky rozhodnete, zda mají být zobrazena nebo naopak potlačena informativní hlášení týkající se kontroly souborů

při kopírování, otevírání nebo i ukládání (*toto nastavení se projeví pouze tehdy, má-li Rezidentní štít povoleno automatické léčení detekované infekce*).

- ***Zobrazovat zprávy o testování v systémové liště*** *(ve výchozím nastavení zapnuto)* - Volbou položky rozhodnete, zda mají být zobrazena nebo naopak potlačena informativní hlášení o automatickém spuštění naplánovaného testu, jeho průběhu, ukončení a výsledcích; informace o ostatních procesech se budou zobrazovat normálně.

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

- ***Zobrazit statistická oznámení*** *(ve výchozím nastavení zapnuto)* - Volbou položky umožníte zobrazení pravidelného statistického přehledu v systémové liště.

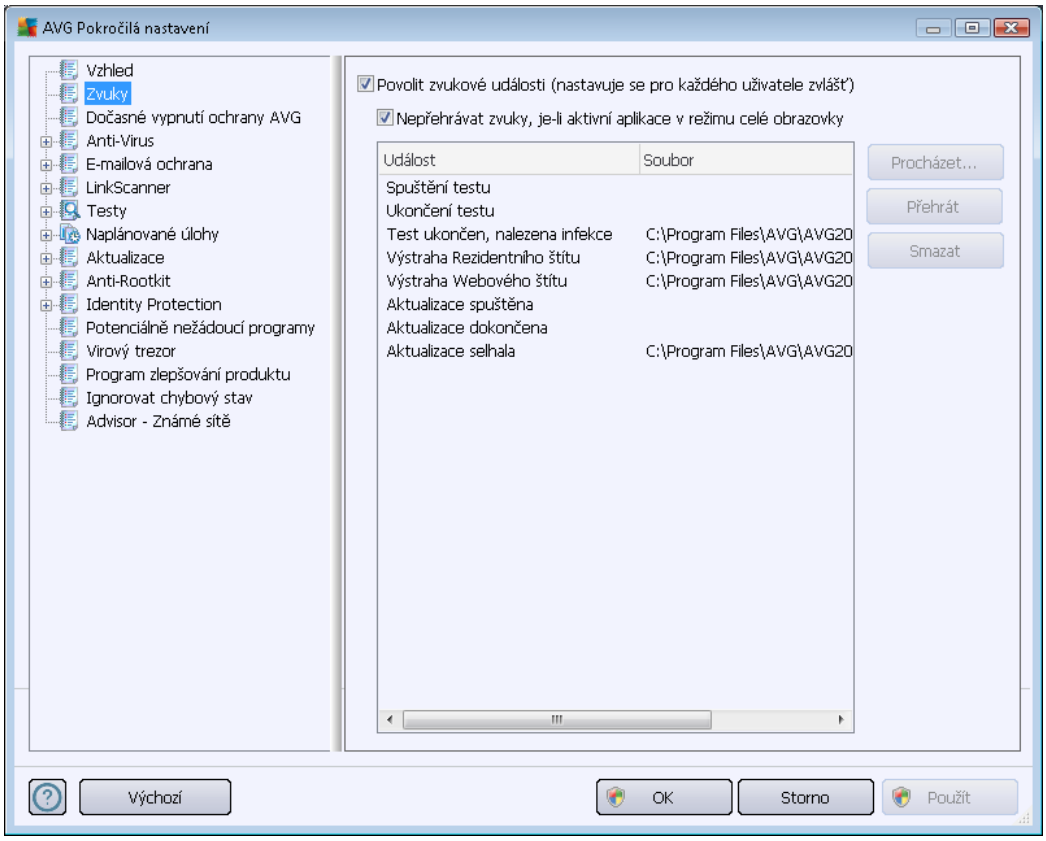
- ***Zobrazit oznámení služby AVG Advisor*** *(ve výchozím nastavení zapnuto)* - Volbou položky rozhodnete, zda chcete ponechat zapnutá veškerá oznámení služby AVG Advisor zobrazovaná ve vysouvacím panelu na systémovou lištou.

Herní režim

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

10.2. Zvuky

V dialogu ***Zvuky*** můžete rozhodnout, zda chcete být o jednotlivých akcích **AVG Anti-Virus 2012** informováni zvukovým oznámením:



Nastavení zvuků je platné pouze pro aktuálně otevřený uživatelský účet. Každý uživatel má tedy možnost individuálního nastavení. Přihlásíte-li se k počítači jako jiný uživatel, můžete si zvolit svou vlastní sadu zvuků. Pokud tedy chcete povolit zvukovou signalizaci, ponechte položku ***Povolit zvukové události*** označenou (*ve výchozím nastavení je tato volba zapnutá*). Tím se aktivuje seznam akcí, k nimž je možné zvukový doprovod přiřadit. Dále můžete označit položku ***Nepřehrávat zvuky, je-li aktivní aplikace v režimu celé obrazovky***, čímž potlačíte zvuková upozornění v situaci, kdy by zvuk mohl působit rušivě *(viz také nastavení Herního režimu, které popisujeme v kapitole Pokročilé nastavení/Vzhled tohoto dokumentu)*.

Ovládací tlačítka dialogu

- ***Procházet*** - Ze seznamu událostí si vyberte tu událost, jíž chcete přiřadit konkrétní zvuk. Pomocí tlačítka ***Procházet*** pak prohledejte svůj pevný disk a příslušný zvukový soubor lokalizujte. *(Upozorňujeme, že v tuto chvíli jsou podporovány pouze zvukové soubory ve formátu *.wav!)*

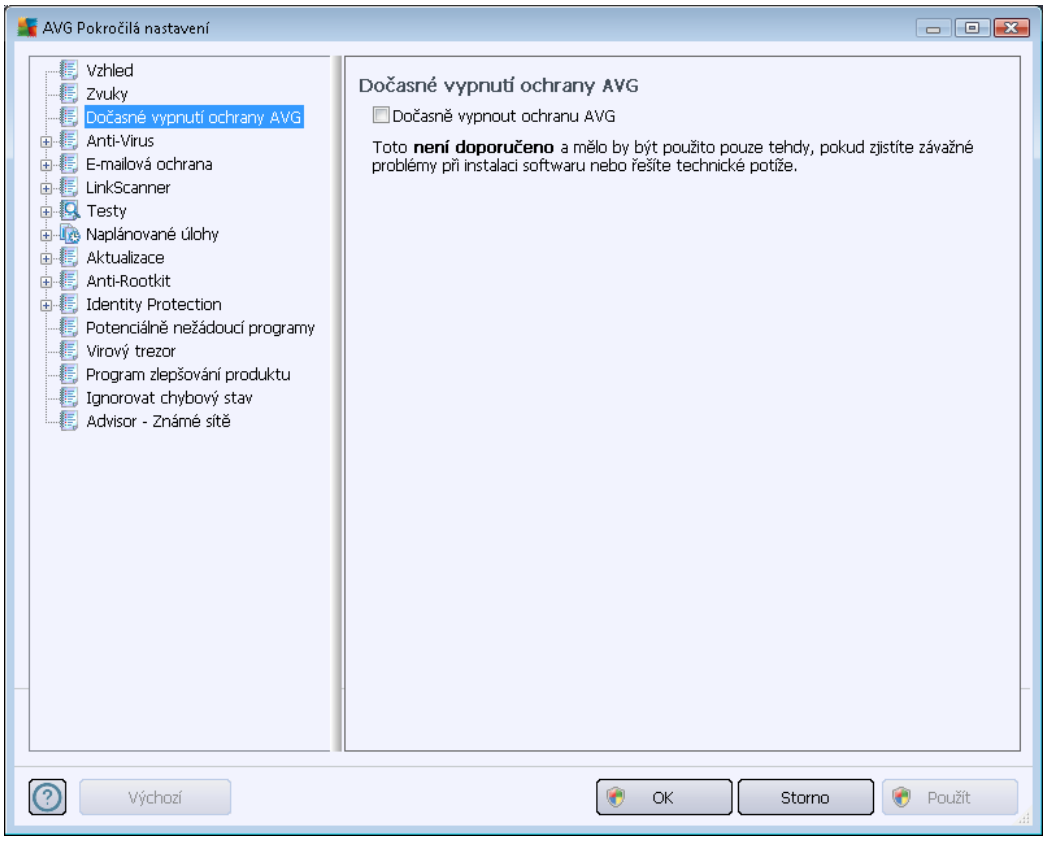
- ***Přehrát*** - Chcete-li si přiřazený zvuk poslechnout, označte v seznamu příslušnou akci a stiskněte tlačítko ***Přehrát***.

- ***Smazat*** - Tlačítkem ***Smazat*** pak můžete zvuk přiřazený konkrétní akci zase odebrat.

10.3. Dočasné vypnutí ochrany AVG

V dialogu ***Dočasné vypnutí ochrany AVG*** máte možnost označením jediné dostupné položky jednorázově deaktivovat celou ochranu zajištěnou programem **AVG Anti-Virus 2012.**

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



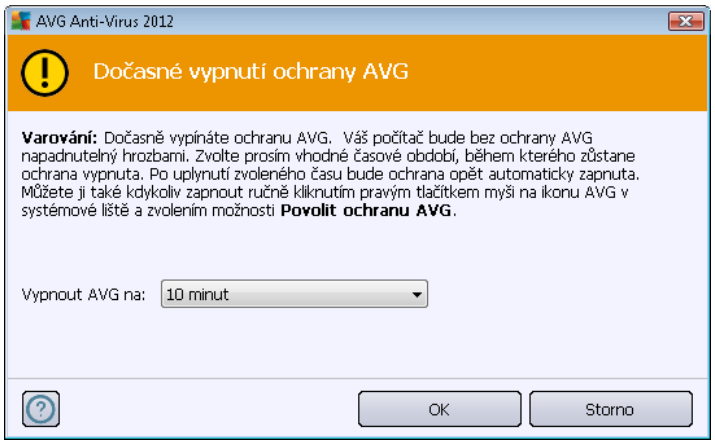
V naprosté většině případů ***není nutné*** deaktivovat **AVG Anti-Virus 2012** před instalací nového software nebo ovladačů, a to ani tehdy, pokud budete během instalace vyzváni k zavření všech spuštěných aplikací. Pokud by v takovém případě došlo ke kolizi, pravděpodobně bude stačit deaktivovat rezidentní ochranu (*Povolit Rezidentní štít*). Jestliže budete opravdu nuceni deaktivovat **AVG Anti-Virus 2012**, 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.

Jak vypnout ochranu AVG

- Označte políčko ***Dočasně vypnout ochranu AVG*** a svou volbu potvrďte stiskem tlačítka ***Použít***

- V nově otevřeném dialogu ***Dočasné vypnutí ochrany AVG*** pak nastavte požadovaný čas,

po který potřebujete **AVG Anti-Virus 2012** vypnout. Standardně bude ochrana vypnuta po dobu 10 minut, což je dostačující pro všechny běžné úkony. Můžete si však zvolit i delší časový interval, ale tuto možnost nedoporučujeme, pokud to není naprosto nezbytně nutné. Po uplynutí zvoleného časového intervalu se všechny vypnuté komponenty znovu automaticky aktivují. Maximální časová lhůta vynutí ochrany AVG je do příštího restartu vašeho počítače.

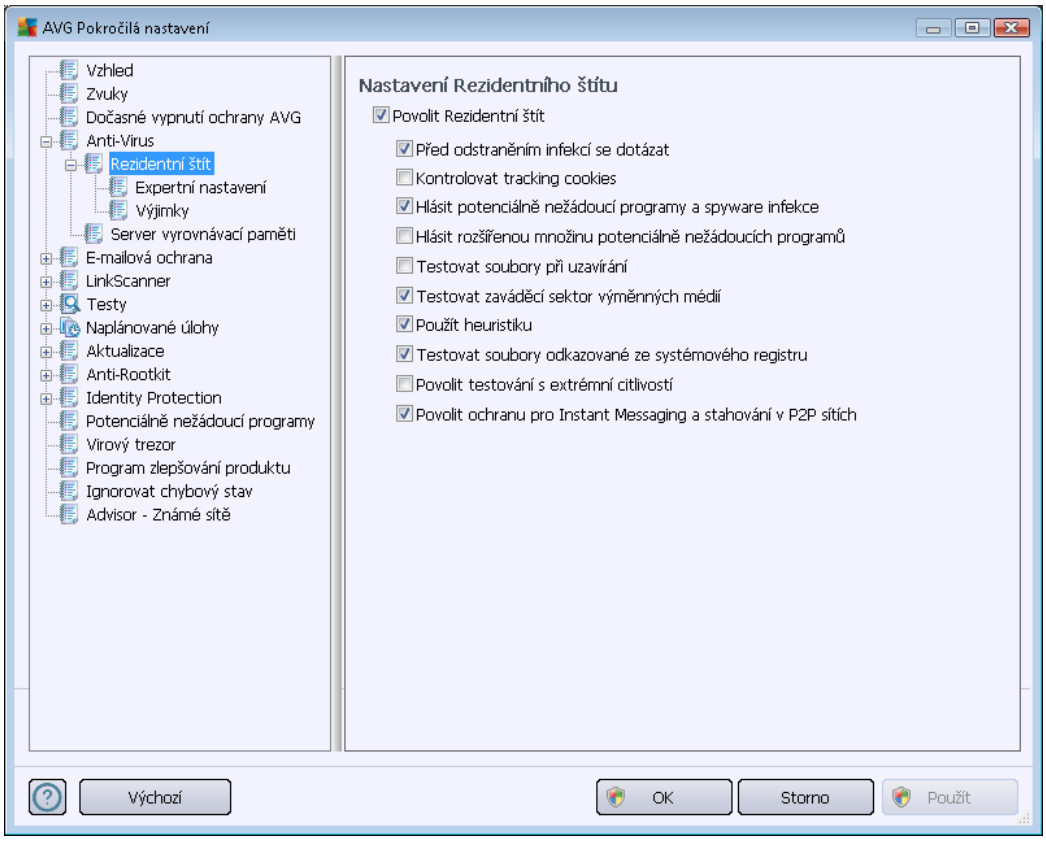


10.4. Anti-Virus

Komponenta ***Anti-Virus*** chrání váš počítač nepřetržitě před všemi známými typy virů a spyware, včetně tzv. spících, zatím neaktivních hrozeb.

10.4.1. Rezidentní štít

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

- ***Před odstraněním infekcí se dotázat*** (*ve výchozím nastavení zapnuto*) - pokud je políčko zaškrtnuté, Rezidentní štít nebude s nalezenými infekcemi nic dělat automaticky a vždy se vás zeptá, jak si přejete s nimi naložit. Pokud necháte políčko neoznačené, pak se **AVG Anti-Virus 2012** pokusí každou nalezenou infekci vyléčit, a pokud to nepůjde, přesune objekt do virového trezoru.

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

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

poněkud problematickou kategorii hrozeb, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány 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*)

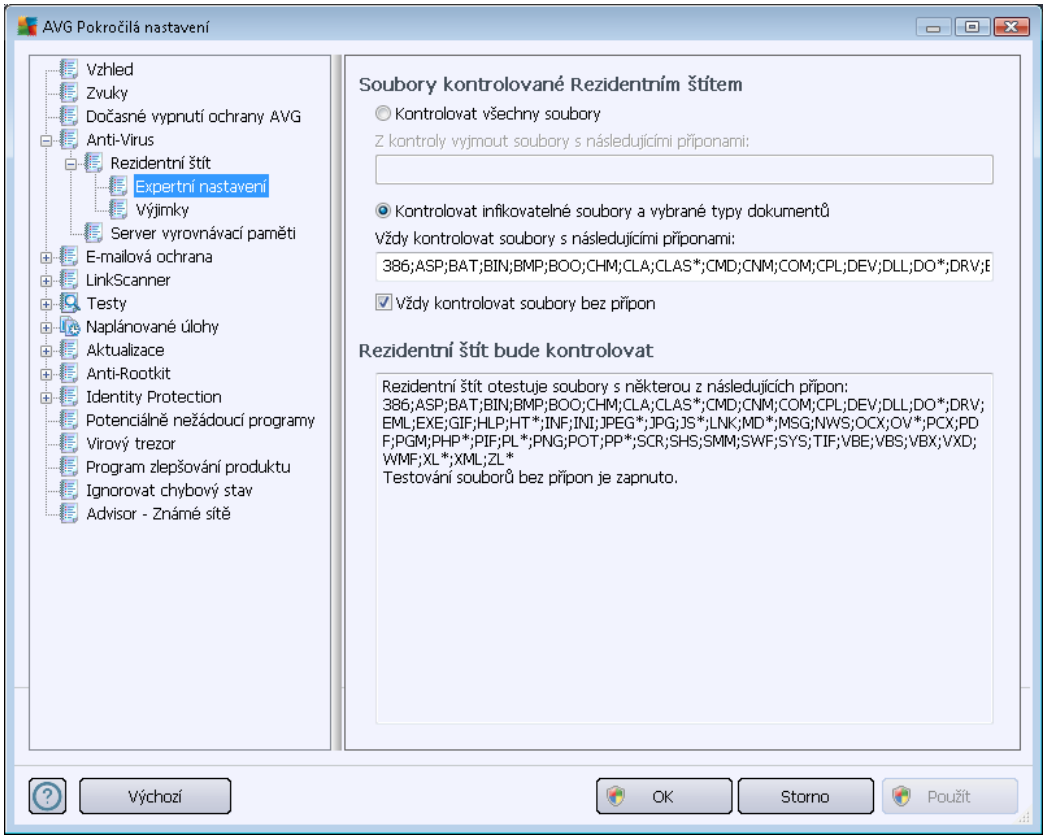
- ***Použít heuristiku*** (*ve výchozím nastavení zapnuto*) - k detekci infekce bude použita i metoda heuristické analýzy (*dynamické emulace instrukcí testovaného objektu v prostředí virtuálního počítače*)

- ***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 příštím 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.

- ***Povolit ochranu pro Instant Messaging a stahování v P2P sítích*** (*ve výchozím nastavení zapnuto*) - Označením této položky potvrzujete, že si přejete, aby byla prováděna kontrola okamžité on-line komunikace *(t.j. komunikace pomocí programů pro okamžité zasílání zpráv, jakými jsou například AIM, Yahoo!, ICQ, Skype, MSN Messenger, ...)* a dat stahovaných v rámci Peer-to-Peer sítí *(t.j. sítí, které umožňují přímé propojení mezi klienty bez serveru, které se používá například pro sdílení hudby apod.)*.

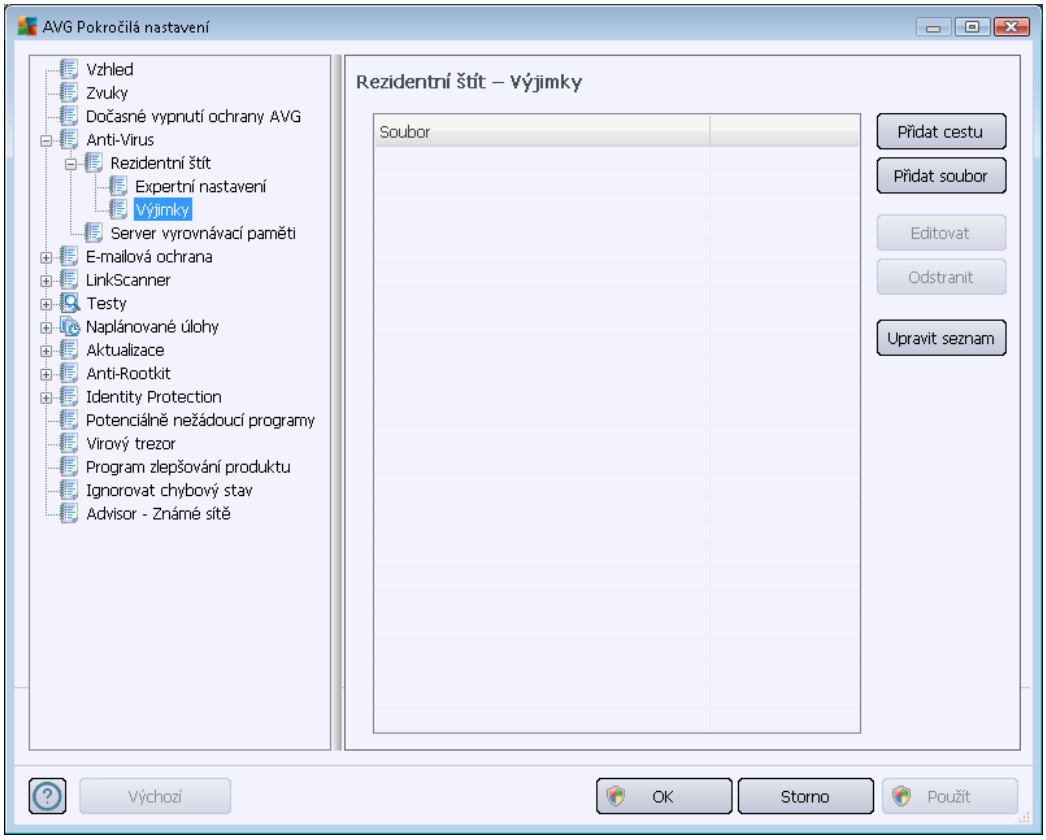
V dialogu ***Soubory kontrolované Rezidentním štítem*** máte možnost nastavení kontroly souborů a dokumentů vybraných typů (*konkrétních přípon*):



Svou volbou rozhodněte, zda chcete ***Kontrolovat všechny soubory*** nebo pouze ***Kontrolovat infikovatelné soubory a vybrané typy dokumentů*** - v tom případě pak můžete definovat seznam přípon souborů, které mají být z kontroly vyňaty a seznam přípon souborů, které se mají kontrolovat za všech okolností.

Označením políčka ***Vždy kontrolovat soubory bez přípon*** (*ve výchozím nastavení zapnuto*) zajistíte, že i soubory bez přípon v neznámém formátu budou testovány. Doporučujeme ponechat tuto volbu zapnutou, protože soubory bez přípon jsou vždy podezřelé.

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



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

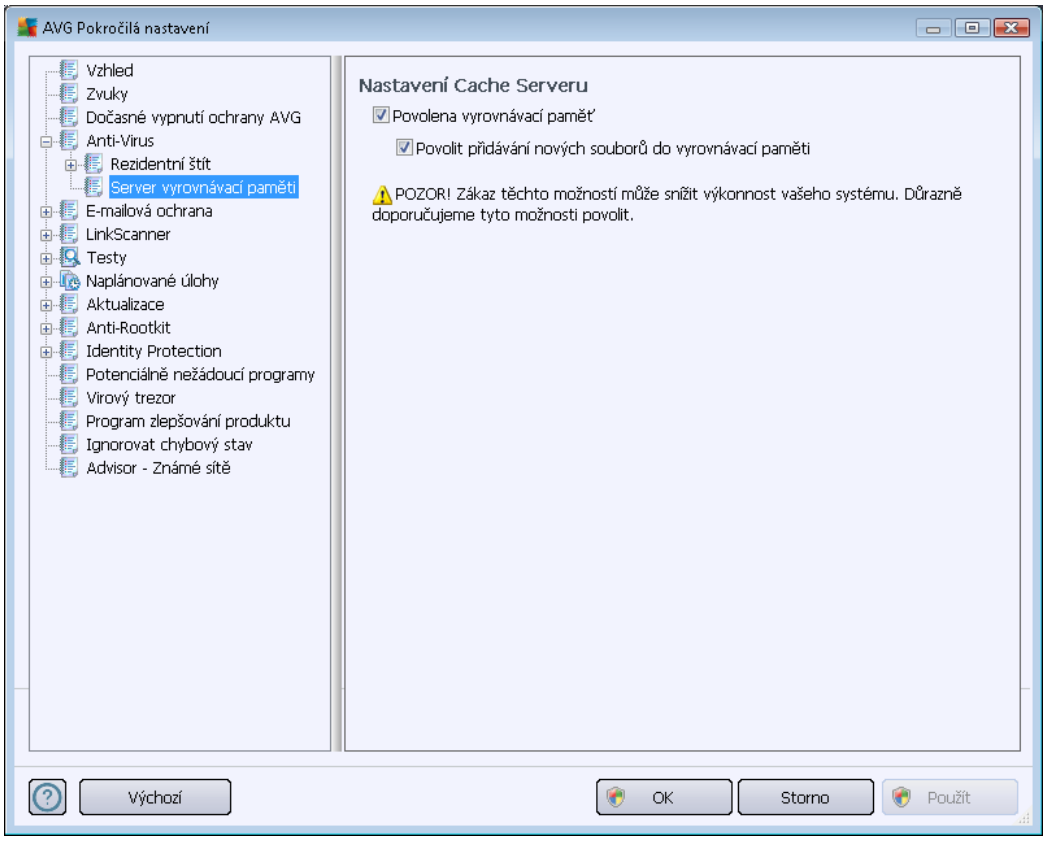
Pokud to není nezbytně nutné, důrazně doporučujeme, abyste z testování žádné položky nevyjímali!

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
- ***Upravit seznam*** - umožňuje upravit celý seznam definovaných výjimek ručně v dialogu, který se chová jako textový editor

10.4.2. Server vyrovnávací paměti

Dialog ***Nastavení Cache Serveru*** se vztahuje k procesu serveru vyrovnávací paměti, jehož úkolem je zrychlit průběh všech testů **AVG Anti-Virus 2012**:



V rámci tohoto procesu **AVG Anti-Virus 2012** detekuje důvěryhodné soubory *(za důvěryhodný lze považovat například soubory digitálně podepsány důvěryhodným zdrojem)* a indexuje je. Indexované soubory jsou pak automaticky považovány za bezpečné a nemusí již být znovu testovány, dokud v nich nedojde ke změně.

Dialog ***Nastavení Cache Serveru*** nabízí následující možnosti konfigurace:

- ***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 definic.

Pokud nemáte skutečný důvod cache server vypínat, důrazně doporučujeme, abyste se

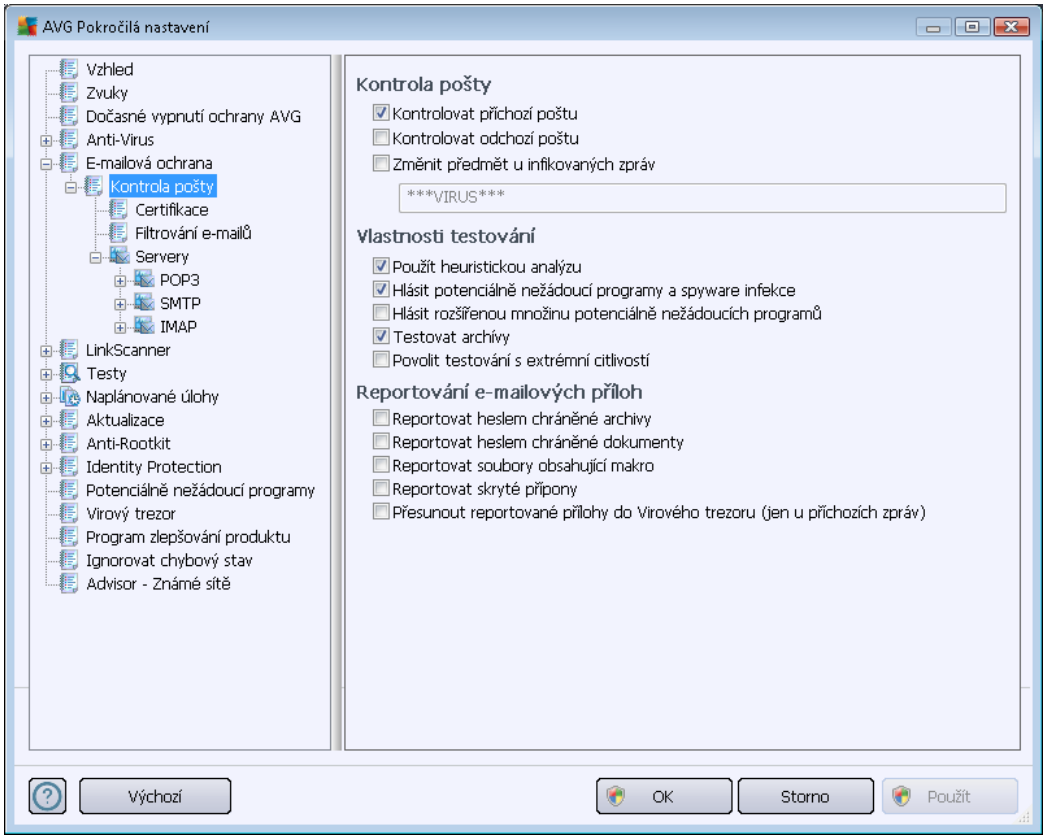
přidrželi výchozího nastavení a ponechali obě položky zapnuté! V opačném případě může dojít k výraznému snížení rychlosti a výkonnosti Vašeho systému.

10.5. E-mailová ochrana

V sekci ***E-mailová ochrana*** máte možnost editovat podrobné nastavení pro Kontrola pošty a Anti-Spam:

10.5.1. Kontrola pošty

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



Kontrola pošty

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

- ***Kontrolovat příchozí poštu*** (*ve výchozím nastavení zapnuto*) - označením zapnete/vypnete možnost testování všech příchozích e-mailů
- ***Kontrolovat odchozí poštu*** (*ve výchozím nastavení vypnuto*) - označením zapnete/vypnete možnost testování všech e-mailů odesílaných z vašeho účtu
- ***Změnit předmět u infikovaných zpráv*** (*ve výchozím nastavení vypnuto*) - pokud si přejete být upozorněni, že otestovaná zpráva byla vyhodnocena jako infikovaná, můžete aktivovat tuto položku a do textového pole vepsat požadované označení takovéto e-mailové

zprávy. Tento text pak bude přidán do pole "Předmět" u každé pozitivně detekované zprávy (*slouží ke snadnější identifikaci a filtrování*). Výchozí hodnota je ***VIRUS*** a doporučujeme ji ponechat.

Vlastnosti testování

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

- ***Použít heuristickou analýzu*** (*ve výchozím nastavení zapnuto*) - použít heuristiku při testování e-mailů. Když je tato možnost aktivována, můžete filtrovat přílohy e-mailů nejen podle přípony, ale i podle skutečného obsahu a formátu (*který příponě nemusí odpovídat*). Filtrování lze nastavit v dialogu Filtrování e-mailů.

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

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

Reportování e-mailových příloh

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

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

- ***Reportovat heslem chráněné dokumenty*** – dokumenty chráněné heslem není možné otestovat na přítomnost virů; po zaškrtnutí tohoto políčka se tyto archivy budou označovat

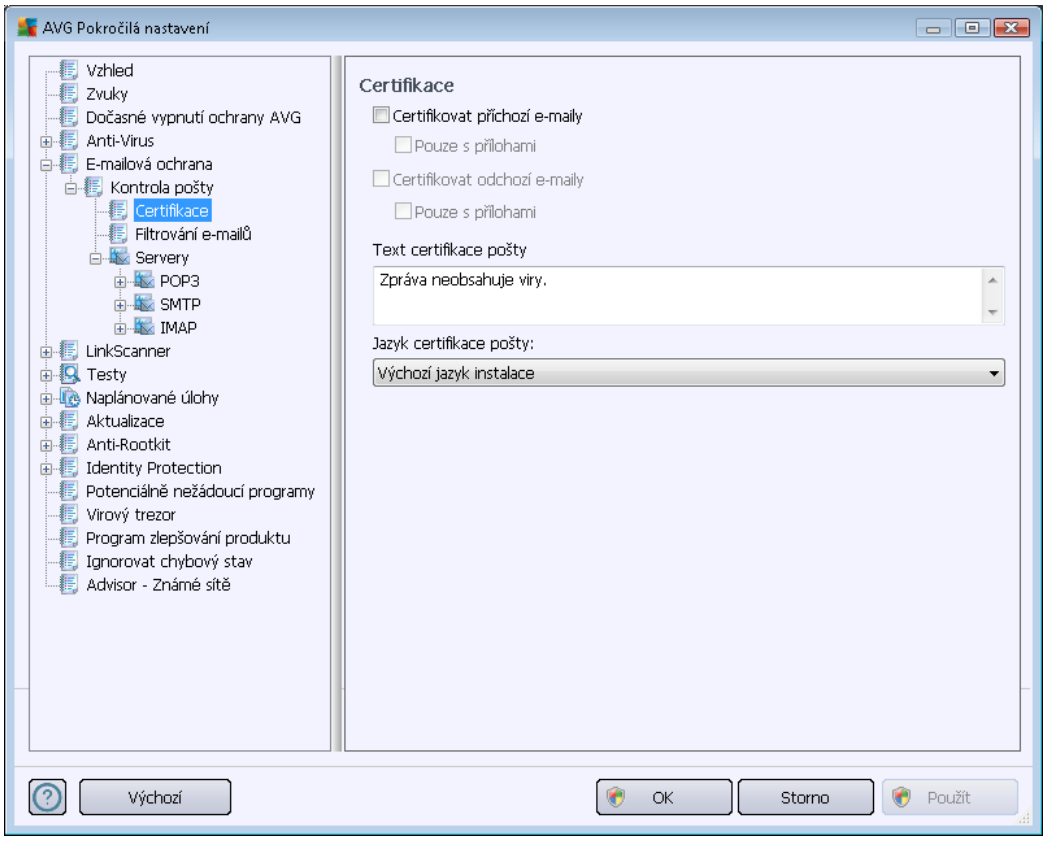
jako potenciálně nebezpečné.

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

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

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

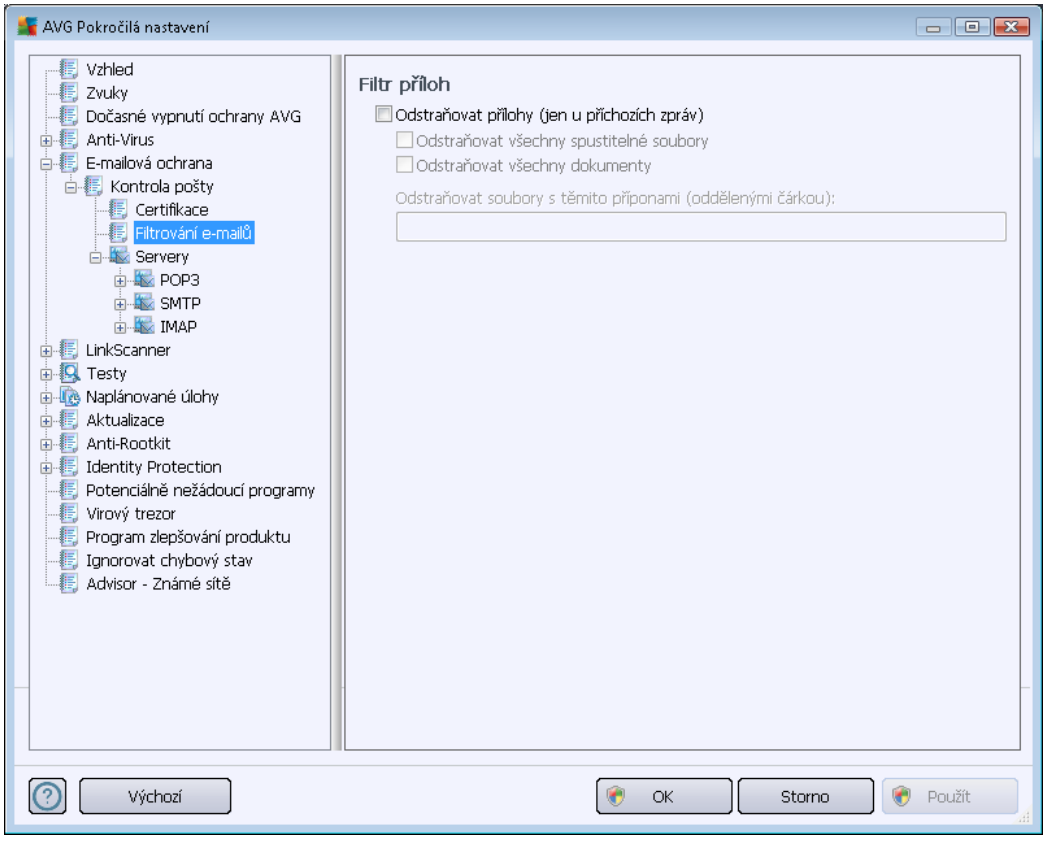
V dialogu ***Certifikace*** můžete označením příslušných políček rozhodnout, zda si přejete certifikovat příchozí poštu (***Certifikovat příchozí e-maily***) a/nebo odchozí poštu (***Certifikovat odchozí e-maily***). U každé z těchto voleb můžete dále označením možnosti ***Pouze s přílohami*** nastavit parametr, který určuje, že v rámci příchozí či odchozí pošty budou certifikačním textem označeny výhradně poštovní zprávy s přílohou:



Ve výchozím nastavení obsahuje certifikační text pouze základní informaci ve znění *Zpráva*

neobsahuje viry. Tuto informaci můžete doplnit či změnit podle vlastního uvážení. Text certifikace, který si přejete zobrazovat v poště, dopište do pole ***Text certifikace pošty***. V sekci ***Jazyk certifikace pošty*** máte pak možnost zvolit, v jakém jazyce se má zobrazovat automaticky generovaná část certifikace (*Zpráva neobsahuje viry*).

Poznámka: *Volbou požadovaného jazyka zajistíte, že se v tomto jazyce zobrazí pouze automaticky generovaná část certifikace. Váš vlastní doplněný text přeložen nebude!*



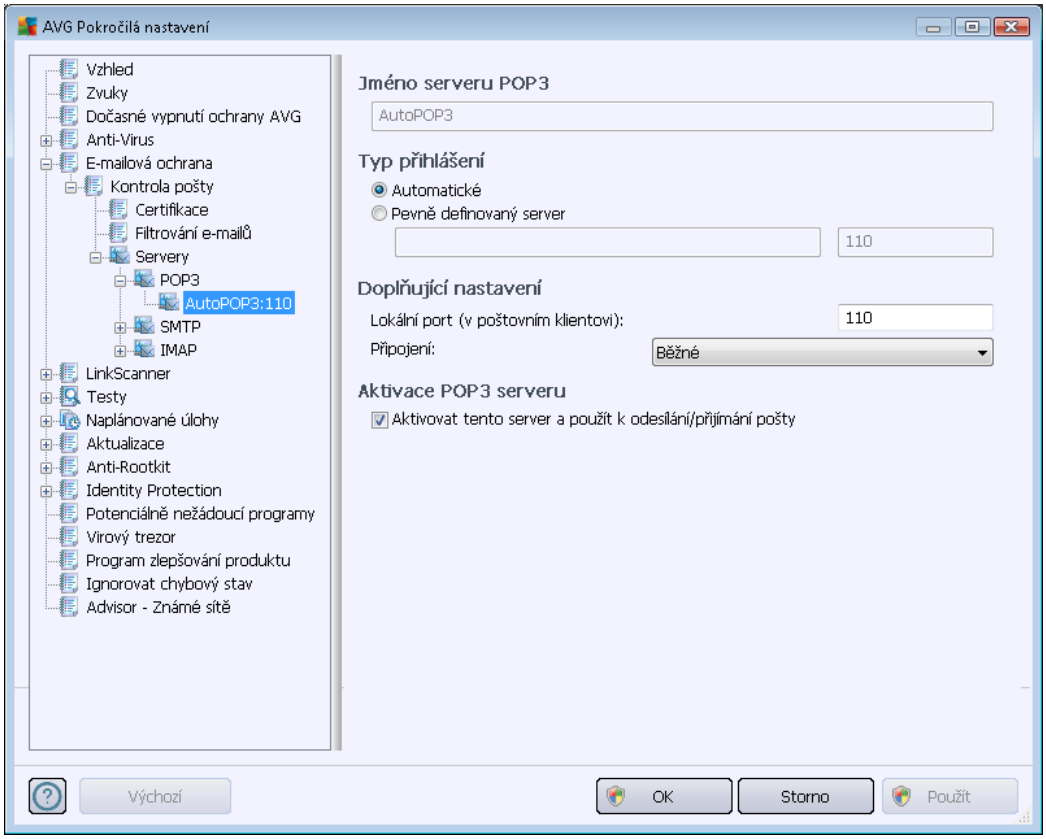
Dialog ***Filtr příloh*** umožňuje nastavení parametrů pro testování příloh e-mailových zpráv. Ve výchozím nastavení je možnost ***Odstraňovat přílohy*** vypnuta. Pokud se rozhodnete pro její aktivaci, budou automaticky odstraněny všechny přílohy zpráv, které byly detekovány jako infikované nebo potenciálně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

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

V sekci ***Servery*** máte možnost editovat parametry jednotlivých serverů Kontroly pošty:

- POP3 server
- SMTP server
- IMAP server

Rovněž můžete definovat nový server příchozí či odchozí pošty, a to pomocí tlačítka ***Přidat nový server***.



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

- ***Jméno serveru POP3*** - v tomto poli můžete zadat jméno nově přidaných serverů (*server POP3 přidáte tak, že kliknete pravým tlačítkem myši nad položkou POP3 v levém navigačním menu*). U automaticky vytvořeného serveru "AutoPOP3" je toto pole deaktivováno.
- ***Typ přihlášení*** - definuje, jak má být určen poštovní server, ze kterého bude přijímána pošta

- ***Automatické*** - cílový server bude určen podle nastavení ve vaší poštovní aplikaci; není třeba nic dále specifikovat

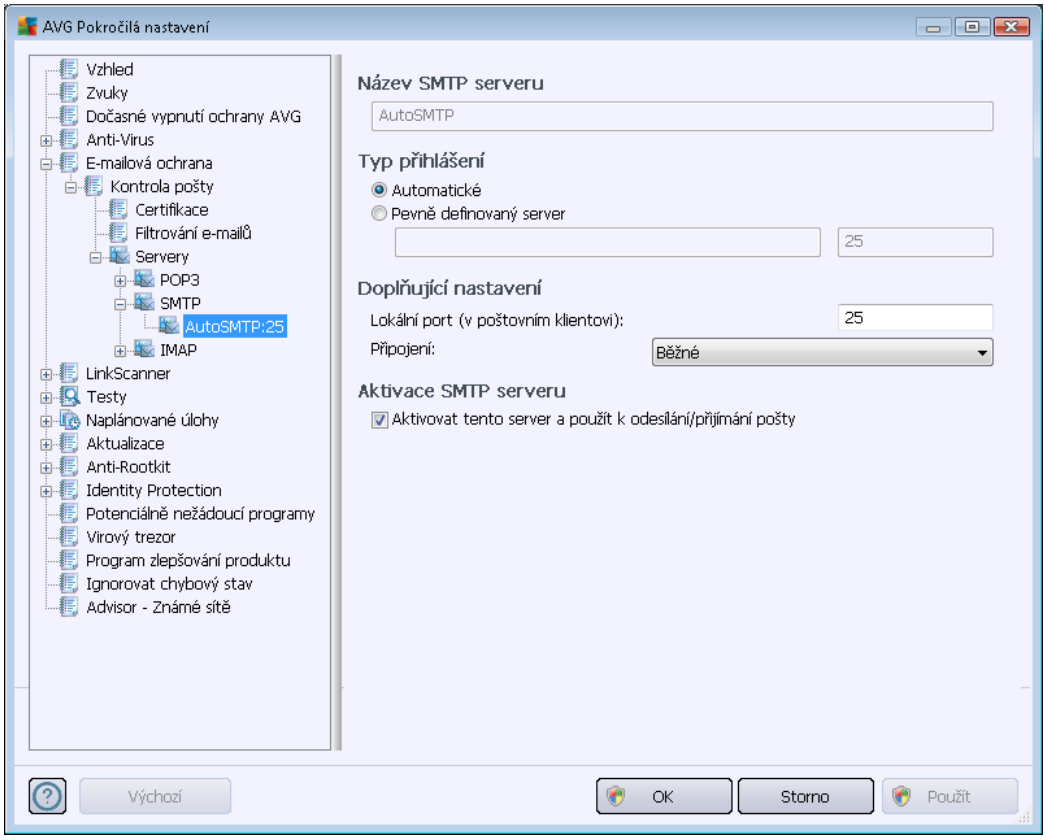
- ***Pevně definovaný server*** - v tomto případě bude vždy použit konkrétní server. Je třeba zadat adresu nebo jméno vašeho poštovního serveru. Přihlašovací jméno pak zůstane beze změny. Jako jméno je možné použít jak doménový název (*například pop.acme.com*), tak IP adresu (*například 123.45.67.89*).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

- ***Doplňující nastavení*** - specifikuje další detailní parametry:

  - ***Lokální port*** - určuje, na kterém portu lze očekávat komunikaci z poštovní aplikace. Tento port je pak také nutné v poštovní aplikaci zadat jako port pro POP3 komunikaci.

  - ***Připojení*** - v této rozbalovací nabídce můžete specifikovat typ připojení (*standardní/ zabezpečené na vyhrazeném portu/zabezpečené na běžném portu*). Pokud zvolíte zabezpečené připojení, budou posílaná data kryptována a nebude možné jejich sledování nikým jiným. I tato funkce může být aktivována pouze v případě, že ji cílový poštovní server podporuje.

- ***Aktivace POP3 serveru*** - zapnutím/vypnutím položky máte možnost aktivovat či deaktivovat právě nastavený POP3 server



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

- ***Název SMTP serveru*** - v tomto poli můžete zadat jméno nově přidaných serverů (*server SMTP přidáte tak, že kliknete pravým tlačítkem myši nad položkou SMTP v levém navigačním menu*). U automaticky vytvořeného serveru "AutoSMTP" je toto pole deaktivováno.

- ***Typ přihlášení*** - definuje, jak má být určen poštovní server, ze kterého bude odesílána pošta:

    - ***Automatické*** - cílový server bude určen podle nastavení ve vaší poštovní aplikaci; není třeba nic dále specifikovat

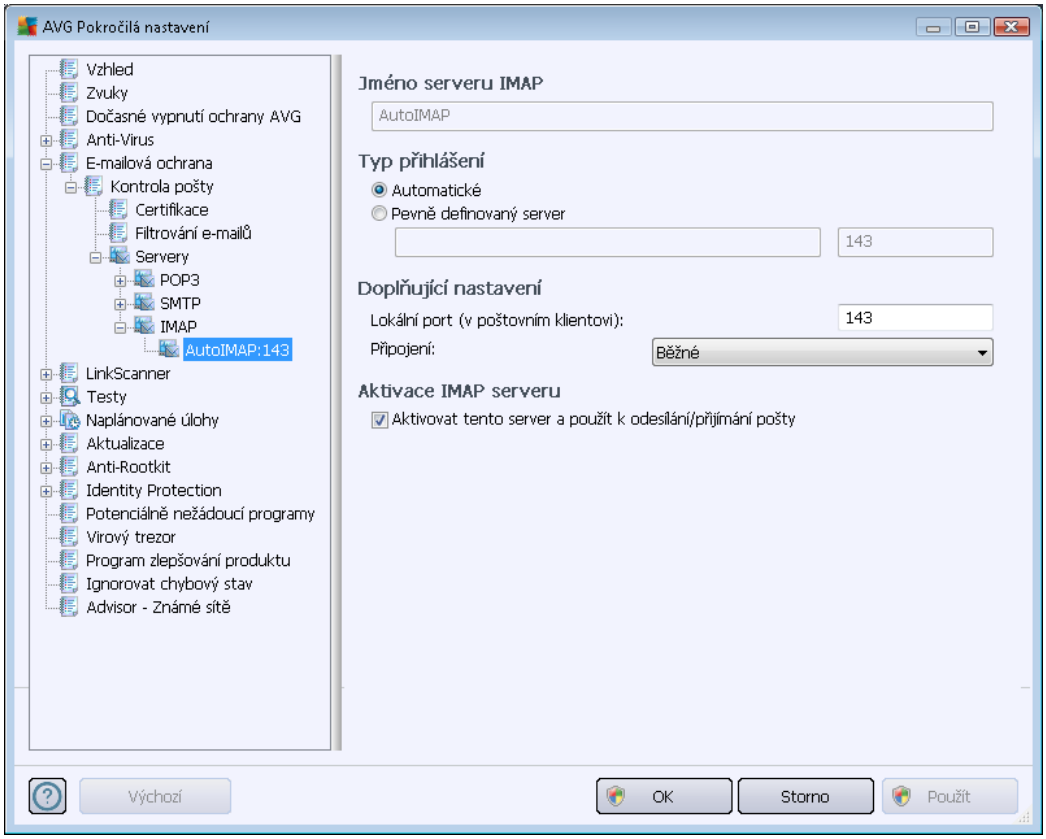
    - ***Pevně definovaný server*** - v tomto případě bude vždy použit konkrétní server. Do editačního řádku je třeba zadat adresu nebo jméno vašeho poštovního serveru. Jako jméno je možné použít jak doménový název (*např. smtp.acme.com*), tak i IP adresu (*např. 123.45.67.89*). Pokud poštovní server používá nestandardní port, lze tento port zadat za jméno serveru oddělený dvojtečkou (*např. smtp.acme.com:8200*). Standardní port pro SMTP komunikaci je 25.

- ***Doplňující nastavení*** - specifikuje další detailní parametry:

- **Lokální port** - určuje, na kterém portu lze očekávat komunikaci z poštovní aplikace. Tento port je pak také nutné v poštovní aplikaci zadat jako port pro SMTP komunikaci.

- **Připojení** - v této rozbalovací nabídce můžete specifikovat typ připojení (*standardní/ zabezpečené na vyhrazeném portu/zabezpečené na běžném portu*). Pokud zvolíte zabezpečené připojení, budou posílaná data kryptována a nebude možné jejich sledování nikým jiným. Tato funkce může být aktivována pouze v případě, že ji cílový poštovní server podporuje.

- ***Aktivace SMTP serveru*** - zapnutím/vypnutím položky máte možnost aktivovat či deaktivovat právě nastavený SMTP server



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

- ***Jméno serveru IMAP*** - v tomto poli můžete zadat jméno nově přidaných serverů (*server IMAP přidáte tak, že kliknete pravým tlačítkem myši nad položkou IMAP v levém navigačním menu*). U automaticky vytvořeného serveru "AutoIMAP" je toto pole deaktivováno.

- ***Typ přihlášení*** - definuje, jak má být určen poštovní server, ze kterého bude odesílána pošta:

- **_Automatické_** - cílový server bude určen podle nastavení ve vaší poštovní aplikaci; není třeba nic dále specifikovat

- **_Pevně definovaný server_** - v tomto případě bude vždy použit konkrétní server. Do editačního řádku je třeba zadat adresu nebo jméno vašeho poštovního serveru. Jako jméno je možné použít jak doménový název (*např. imap.acme.com*), tak i IP adresu (*např. 123.45.67.89*). Pokud poštovní server používá nestandardní port, lze tento port zadat za jméno serveru oddělený dvojtečkou (*např. imap.acme.com:8200*). Standardní port pro IMAP komunikaci je 143.

- **_Doplňující nastavení_** - specifikuje další detailní parametry:

  - **_Lokální port_** - určuje, na kterém portu lze očekávat komunikaci z poštovní aplikace. Tento port je pak také nutné v poštovní aplikaci zadat jako port pro IMAP komunikaci.

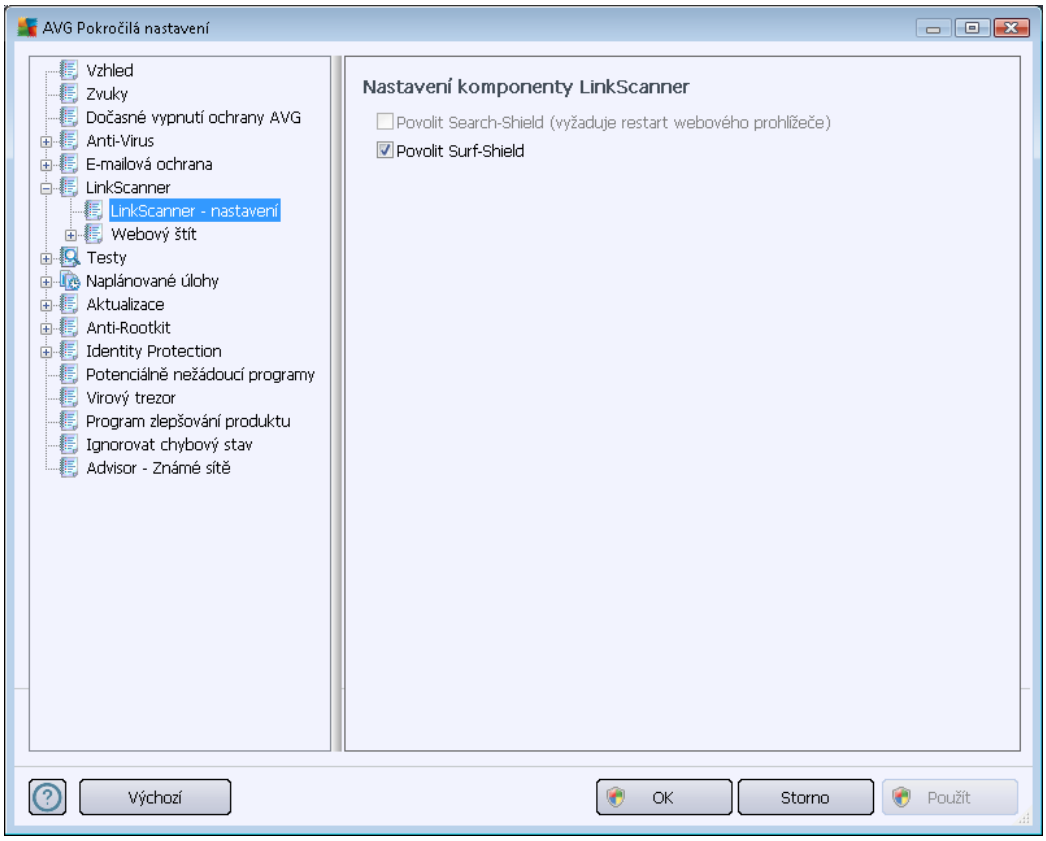
  - **_Připojení_** - v této rozbalovací nabídce můžete specifikovat typ připojení (*standardní/ zabezpečené na vyhrazeném portu/zabezpečené na běžném portu*). Pokud zvolíte zabezpečené připojení, budou posílaná data kryptována a nebude možné jejich sledování nikým jiným. Tato funkce může být aktivována pouze v případě, že ji cílový poštovní server podporuje.

- **_Aktivace IMAP serveru_** - zapnutím/vypnutím položky máte možnost aktivovat či deaktivovat právě nastavený IMAP server

10.6. LinkScanner

10.6.1. LinkScanner - nastavení

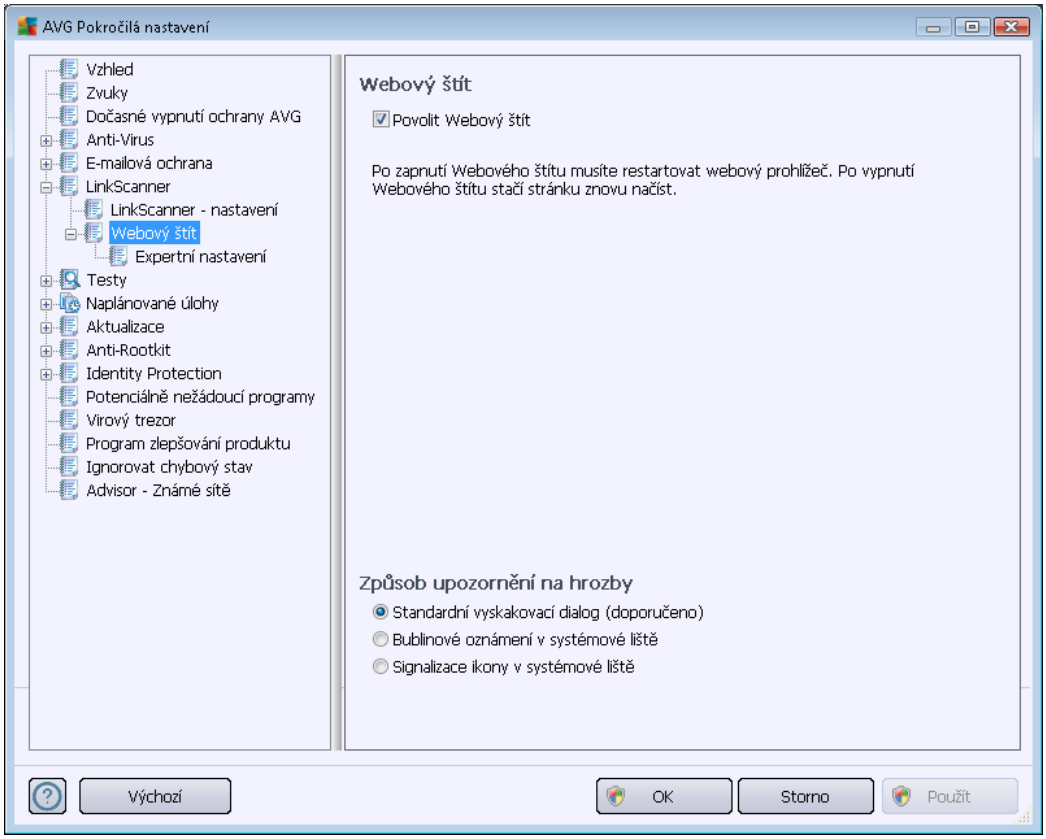
Dialog ***Nastavení komponenty LinkScanner*** umožňuje zapnout či vypnout funkčnost základních složek LinkScanner:



- *Povolit Search-Shield* - V konfiguračním dialogu je tato možnost deaktivována, protože podpora služby Search-Shield byla ve všech produktech AVG ukončena.

- ***Povolit Surf-Shield*** - (*ve výchozím nastavení zapnuto*): aktivní ochrana proti agresivním webovým stránkám. Kontrola stránek se provádí v okamžiku jejich načítání. Stránky s nebezpečným obsahem jsou v příslušném internetovém prohlížeči (nebo jiné aplikaci, která používá HTTP) rovnou zablokovány.

10.6.2. Webový štít



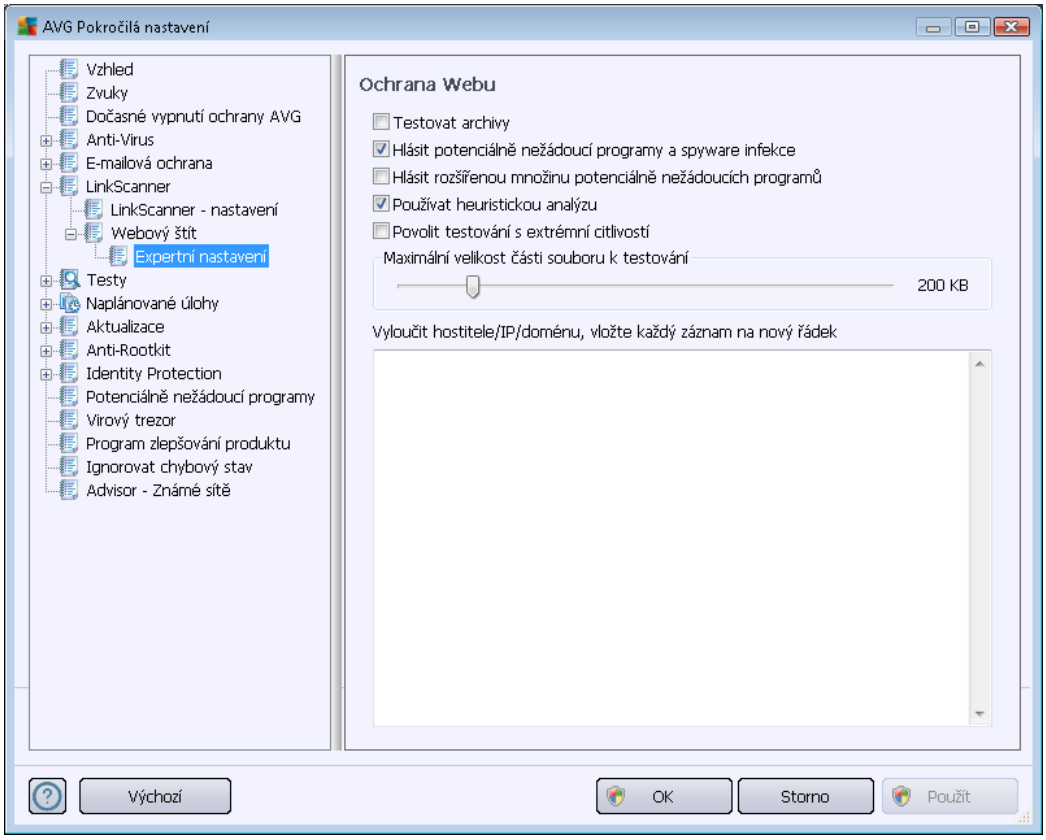
Dialog ***Webový štít*** nabízí tyto možnosti:

- ***Povolit Webový štít*** *(ve výchozím nastavení zapnuto)* - Označením položky aktivujete/deaktivujete službu ***Webový štít***. Pokročilé nastavení této komponenty pak najdete v podkategorii Ochrana webu.

- ***Povolit AVG Akcelerátor*** *(ve výchozím nastavení zapnuto)* - Označením položky aktivujete/deaktivujete službu ***AVG Akcelerátor***, která umožňuje plynulé přehrávání videa v režimu online a urychluje stahování.

Způsob upozornění na hrozby

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



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

- ***Povolit ochranu webu*** - touto volbou potvrzujete, že v rámci služby ***Webový štít*** si přejete, aby byla prováděna kontrola obsahu navštěvovaných www stránek. Za předpokladu, že je tato volba zapnuta (*výchozí nastavení*), můžete dále povolit nebo vypnout tyto volby:
    - ***Testovat archívy*** - (*ve výchozím nastavení vypnuto*) kontrola obsahu archivu, jež mohou být přítomny na zobrazované www stránce.
    - ***Hlásit potenciálně nežádoucí programy a spyware infekce*** - (*ve výchozím nastavení zapnuto*) kontrola přítomnosti potenciálně nežádoucích programů (*spustitelné programy, které mohou fungovat jako spyware nebo adware*). Zaškrtnutím tohoto políčka aktivujete Anti-Spyware, tj. bude se testovat přítomnost spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, 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.

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

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

- ***Maximální velikost částí souboru k testování*** - pokud jsou na zobrazované stránce přítomny vložené soubory, lze kontrolovat také jejich obsah ještě dříve, než budou staženy na váš počítač. Kontrola velkých souborů je však časově náročná a může výrazně zpomalit načítání www stránky. Posuvníkem tedy můžete nastavit maximální velikost souboru, který si přejete pomocí komponenty ***Webový štít*** testovat. I v případě, že soubor určený ke stažení bude větší než je nastavená povolená velikost souboru, a bude tudíž stažen bez kontroly ***Webovým štítem***, jste stále pod ochranou AVG: pokud by soubor byl infikován, bude okamžitě detekován ***Rezidentním štítem***.

- ***Vyloučit hostitele/IP/doménu*** - do textového pole můžete zadat konkrétní adresu serveru (hostitele, IP adresu, IP adresu s maskou nebo URL) či domény, jež mají být z kontroly ***Webovým štítem*** vyňaty. Uvádějte tedy výhradně adresy hostitelů, u nichž si můžete být obsahem www stránek naprosto jisti.

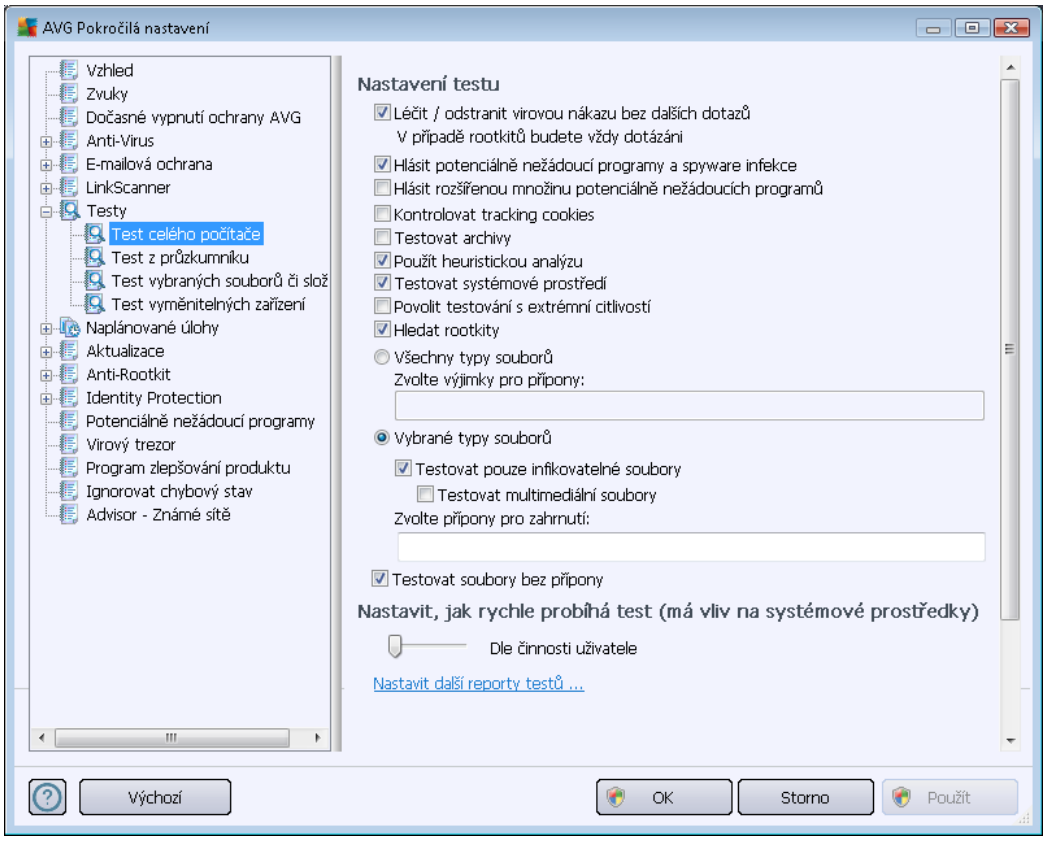
10.7. Testy

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

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

10.7.1. 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:

- ***Léčit / odstranit virovou nákazu bez dalších dotazů*** (*ve výchozím nastavení zapnuto*) - je-li během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. Pokud virus automaticky léčit nelze, bude infikovaný objekt automaticky přesunut do Virového trezoru.

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

- ***Hledat rootkity*** (*ve výchozím nastavení zapnuto*) - Parametr komponenty Anti-Rootkit prohledává počítač na přítomnost rootkitů, tedy 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.

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

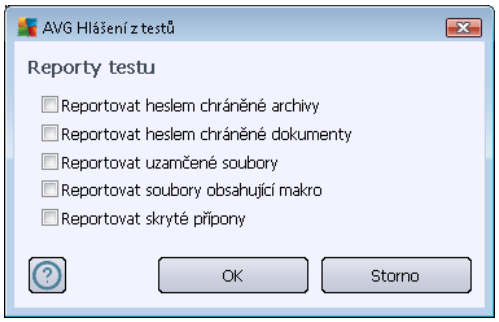
měnit. Soubory bez přípon jsou obecně vysoce podezřelé a měly by být otestovány.

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.

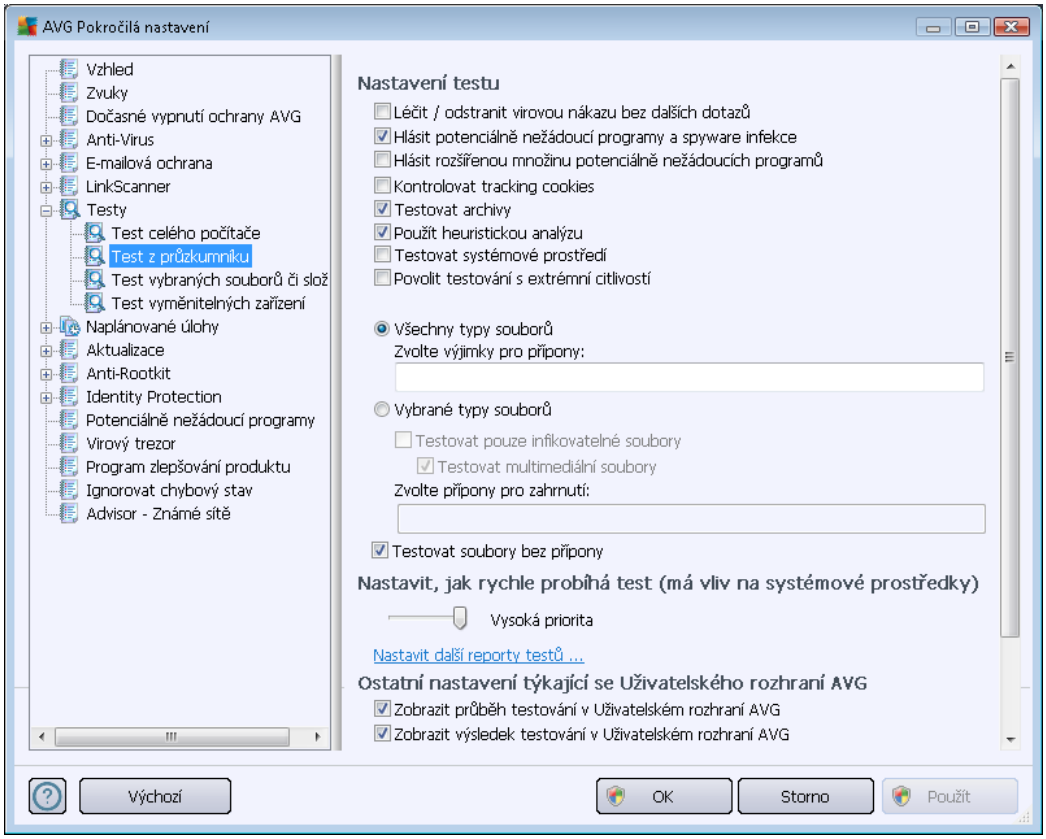
Nastavit další reporty testů ...

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



10.7.2. Test z průzkumníku

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



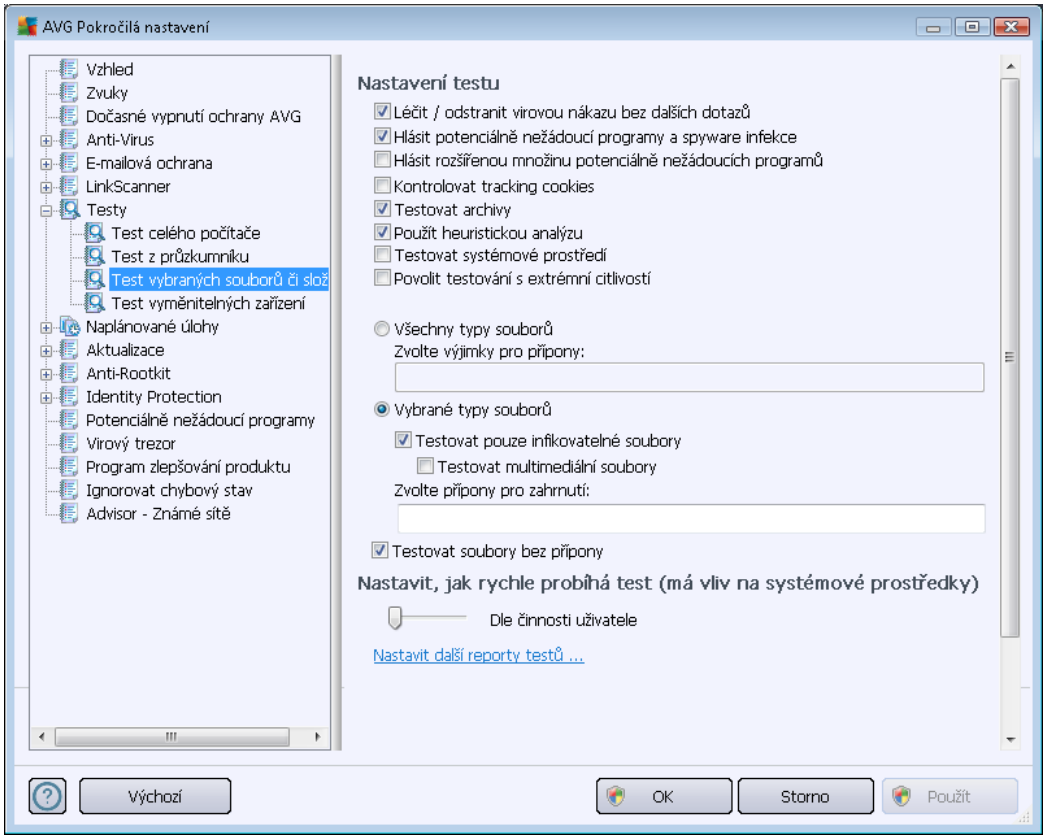
Veškeré možnosti editace parametrů testu jsou totožné s editací parametrů Testu celého počítače. Odlišné je pouze výchozí nastavení těchto parametrů (*například Test celého počítače ve výchozím nastavení neprovádí kontrolu archivů, ale provádí kontrolu systémového prostředí, zatímco u Testu z průzkumníku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

Poznámka: *Podrobný popis jednotlivých parametrů najdete v kapitole Pokročilé nastavení AVG / Testy / Test celého počítače.*

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

10.7.3. 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:

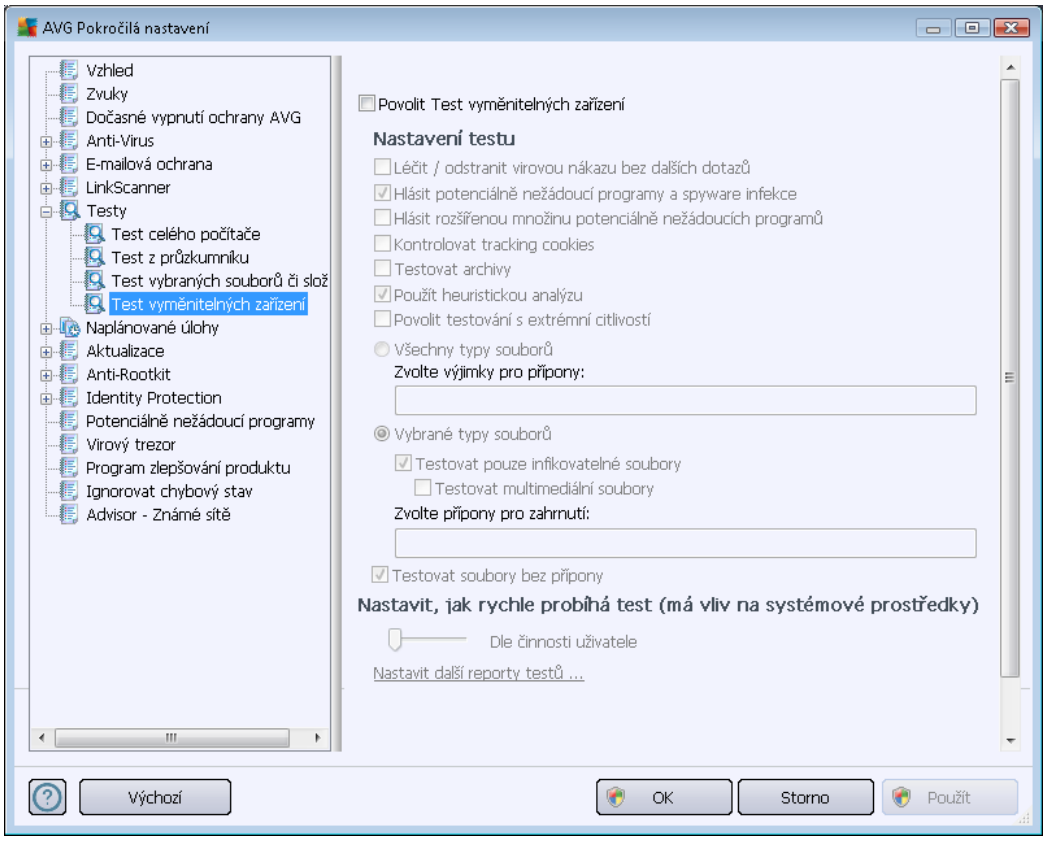


Veškeré parametry nastavené v tomto konfiguračním dialogu se vztahují pouze na ty oblasti vašeho počítače, které jste vybrali pro testování v rámci Testu wybraných souborů či složek!

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

10.7.4. Test vyměnitelných zařízení

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



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

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

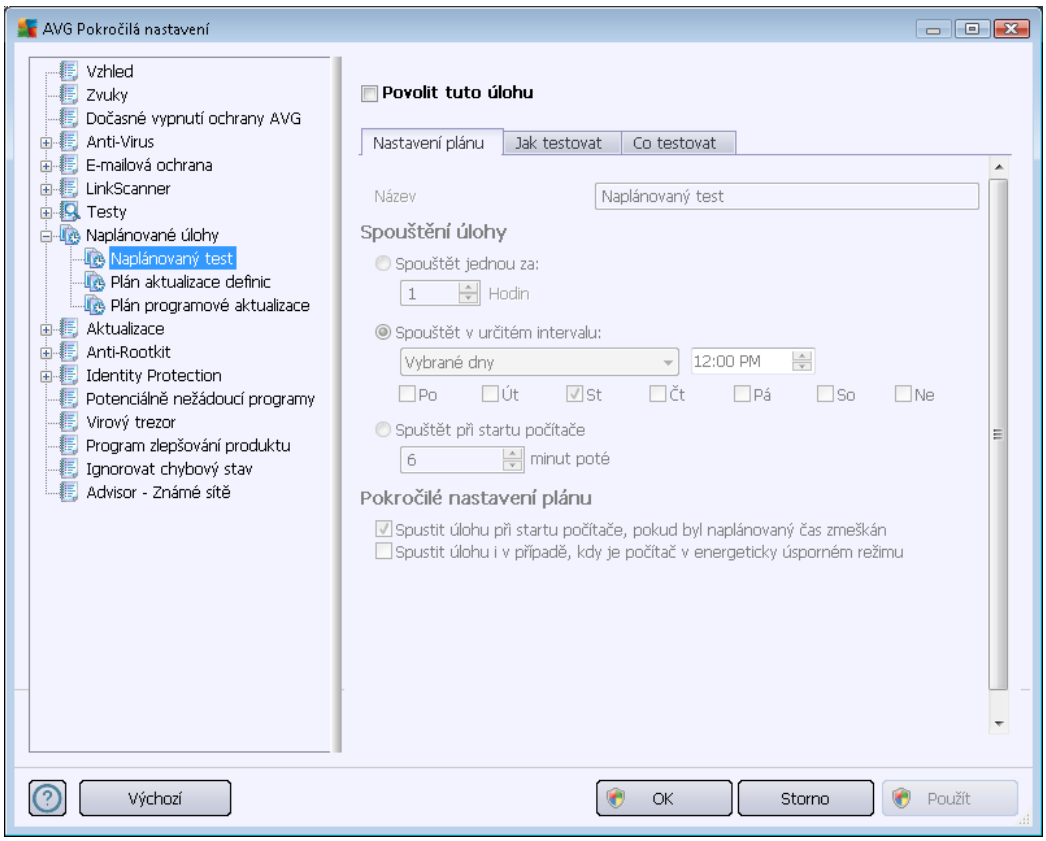
10.8. Naplánované úlohy

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

- Naplánovný test
- Plánu aktualizace definic
- Plánu programové aktualizace

10.8.1. Naplánovaný test

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

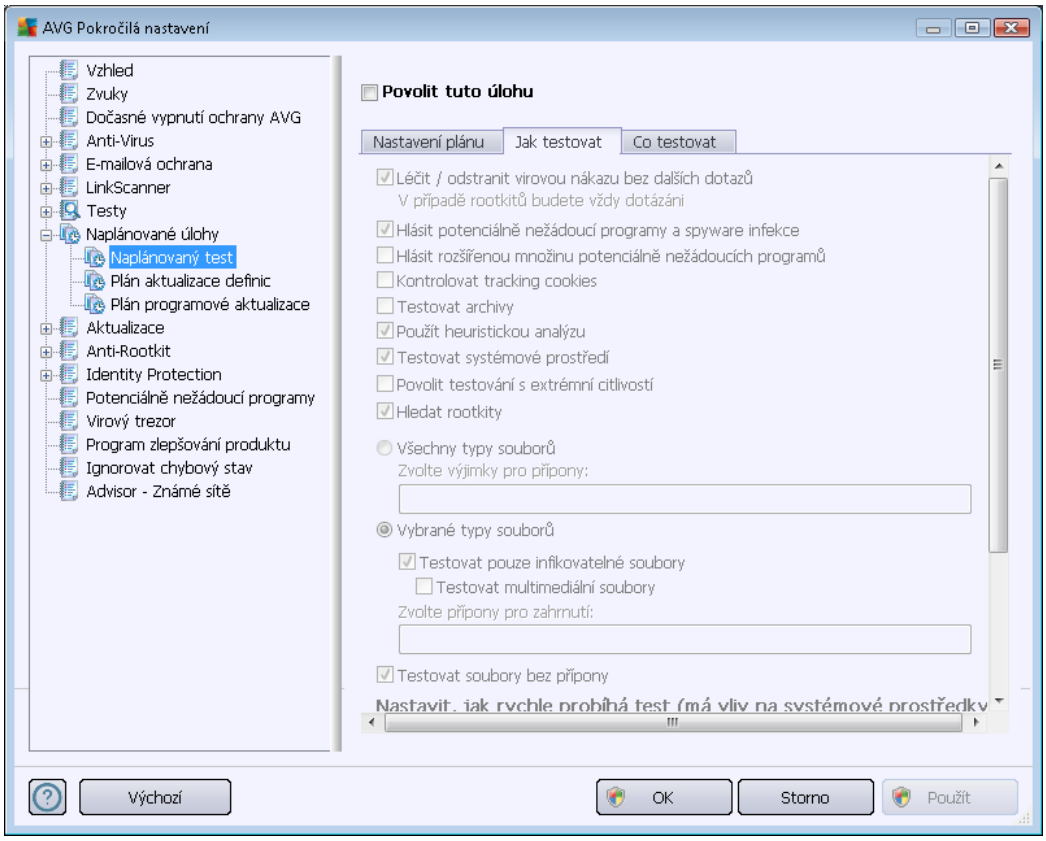
Spouštění úlohy

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 určitém intervalu***), případně určením události, na niž se spuštění testu váže (***Spouštět při startu 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***:

- ***Léčit / odstranit virovou nákazu bez dalších dotazů|*** (*ve výchozím nastavení zapnuto*): je-li během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. Pokud virus automaticky léčit nelze, bude infikovaný objekt automaticky přesunut do Virového trezoru;

- ***Hlásit potenciálně nežádoucí programy a spyware infekce*** (*ve výchozím nastavení zapnuto*): kontrola přítomnosti potenciálně nežádoucích programů (*spustitelné programy, které mohou fungovat jako spyware nebo adware*). Zaškrtnutím tohoto políčka aktivujete Anti-Spyware, tj. bude se testovat přítomnost spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány 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 zapnuto*): parametr komponenty Anti-Rootkit prohledává počítač na přítomnost rootkitů, tedy 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.

Dále se můžete rozhodnout, zda si přejete testovat

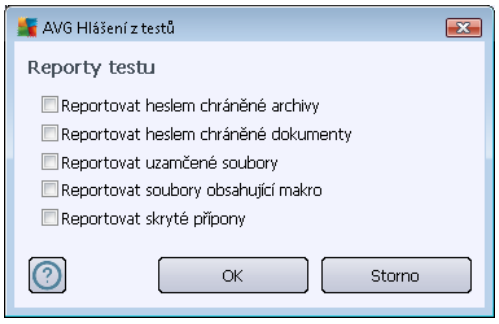
- ***Všechny typy souborů*** - přičemž máte zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou (*po uložení se čárky změní na středníky*);
- ***Vybrané typy souborů*** - můžete se rozhodnout, že chcete, aby se testy spouštěly pouze nad soubory, které lze považovat 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 *dle činnosti uživatele*. 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.

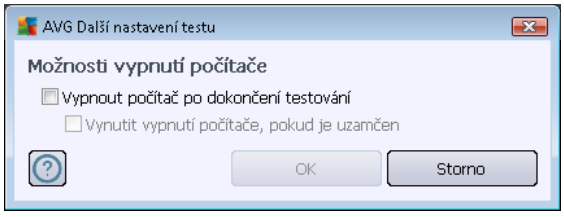
Nastavit další reporty testů

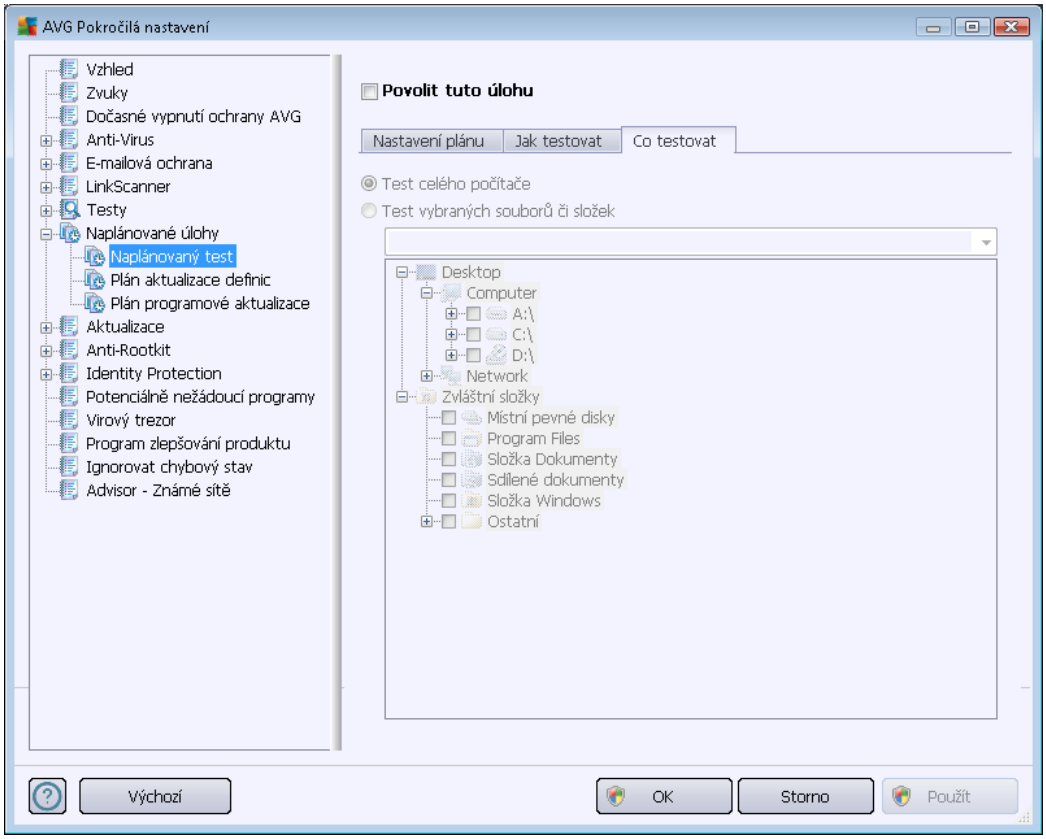
Kliknutím na odkaz ***Nastavit další reporty testů ...*** otevřete samostatné dialogové okno ***Reporty testu***, v němž můžete označením příslušných položek určit situace, jejichž výskyt během testu má být hlášen:



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***).

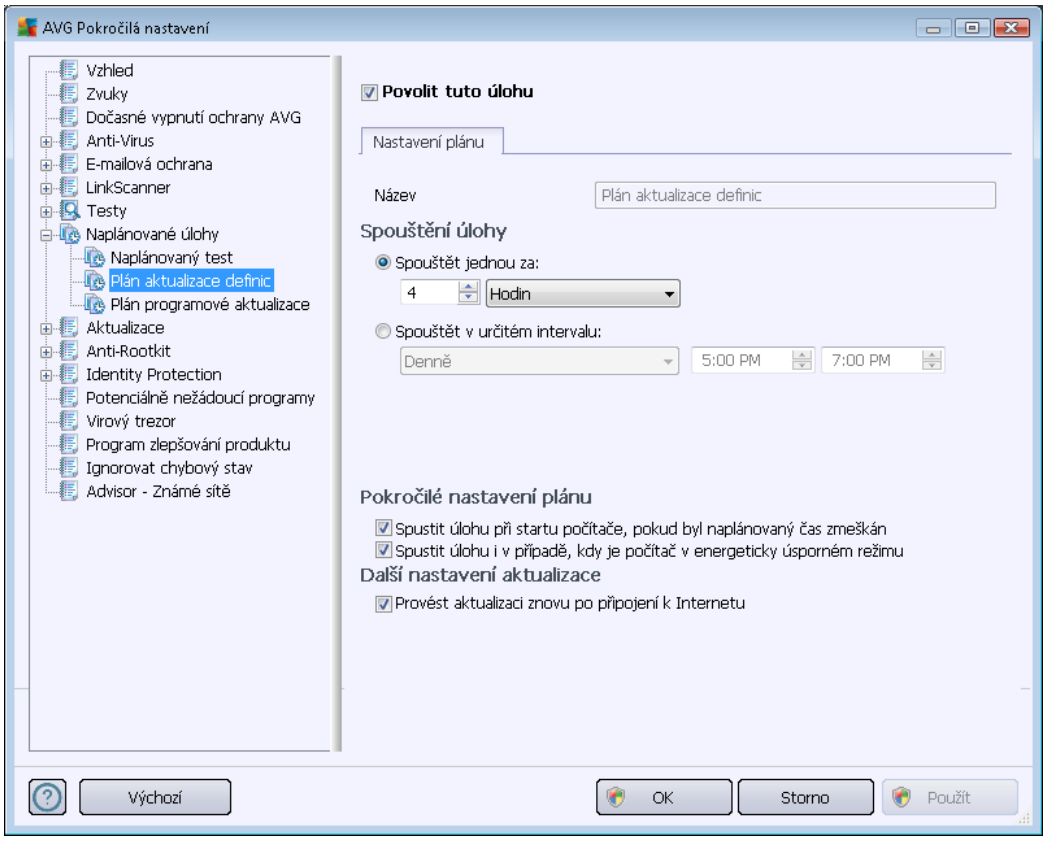




Na záložce ***Co testovat*** definujte, zda si přejete naplánovat Test celého počítače nebo Test vybraných souborů či složek. V případě, že se rozhodnete pro test vybraných souborů a složek, ve spodní sekci dialogu se aktivuje zobrazená stromová struktura vašeho disku a v ní můžete označit adresáře,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

10.8.2. Plán aktualizace definic

V případě ***skutečně nutné*** potřeby můžete prostým vypnutím položky ***Povolit tuto úlohu*** naplánovanou aktualizaci *(dočasně)* deaktivovat, a později znovu zapnout:



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 definic provedena. Časové určení můžete zadat buďto opakovaným spuštěním aktualizace po uplynutí určené doby (***Spouštět jednou za***) nebo stanovením přesného data a času (***Spouštět v určitém intervalu***).

Pokročilé nastavení plánu

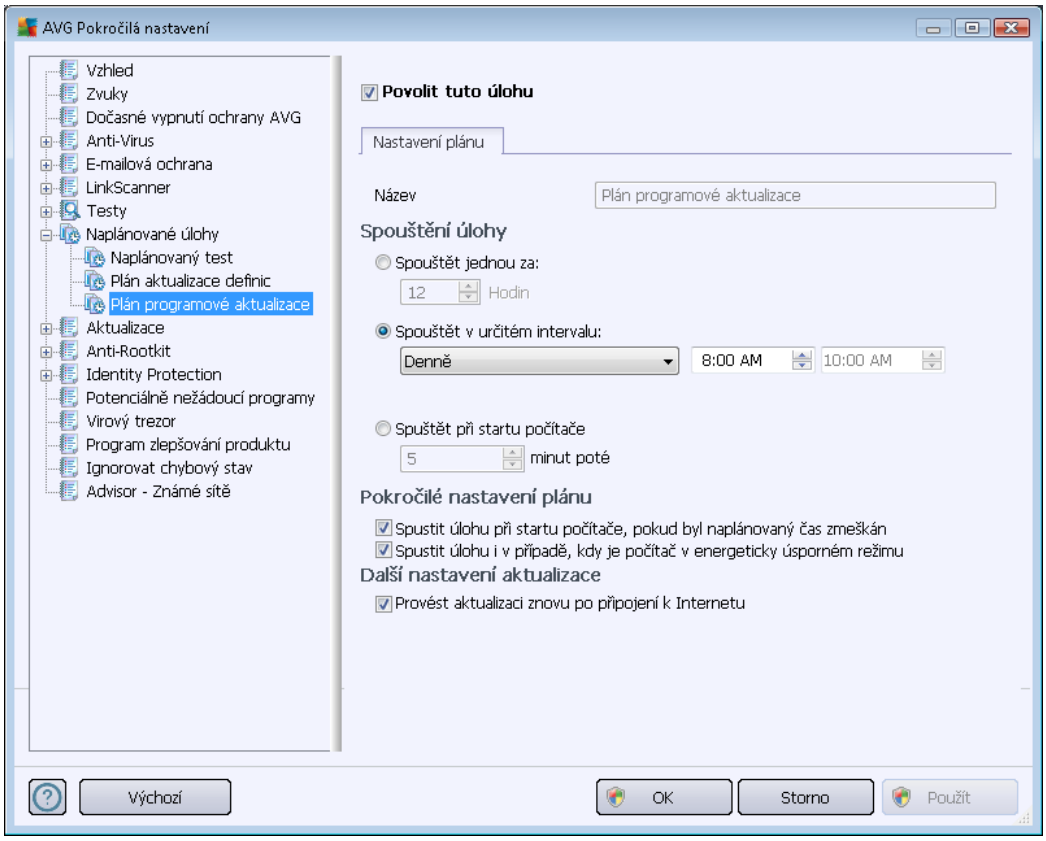
Tato sekce umožňuje definovat podmínky, kdy má či nemá být aktualizace definic spuštěna, jestliže je počítač v úsporném režimu nebo zcela vypnutý a naplánovaný čas spuštění aktualizace byl zmeškán.

Další nastavení aktualizace

Volbou položky ***Provést aktualizaci znovu po připojení k Internetu*** zajistíte, že pokud dojde během aktualizace definic k problémům s připojením a aktualizace tedy nebude moci být dokončena, bude znovu spuštěna bezprostředně po obnovení připojení. O automatickém spuštění aktualizace budete v určeném čase informováni prostřednictvím pop-up okna nad ikonou AVG na systémové liště (*za předpokladu, že ponecháte zapnutou volbu Zobrazovat oznámení na systémové liště v Pokročilém nastavení/Vzhled*).

10.8.3. Plán programové aktualizace

V případě ***skutečně nutné*** potřeby můžete prostým vypnutím položky ***Povolit tuto úlohu*** naplánovanou programovou aktualizaci (*dočasně*) deaktivovat, a později znovu zapnout:



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 určitém intervalu***),

případně určením události, na niž se spuštění aktualizace váže (***Spouštět při spuštění počítače***).

Pokročilé nastavení plánu

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

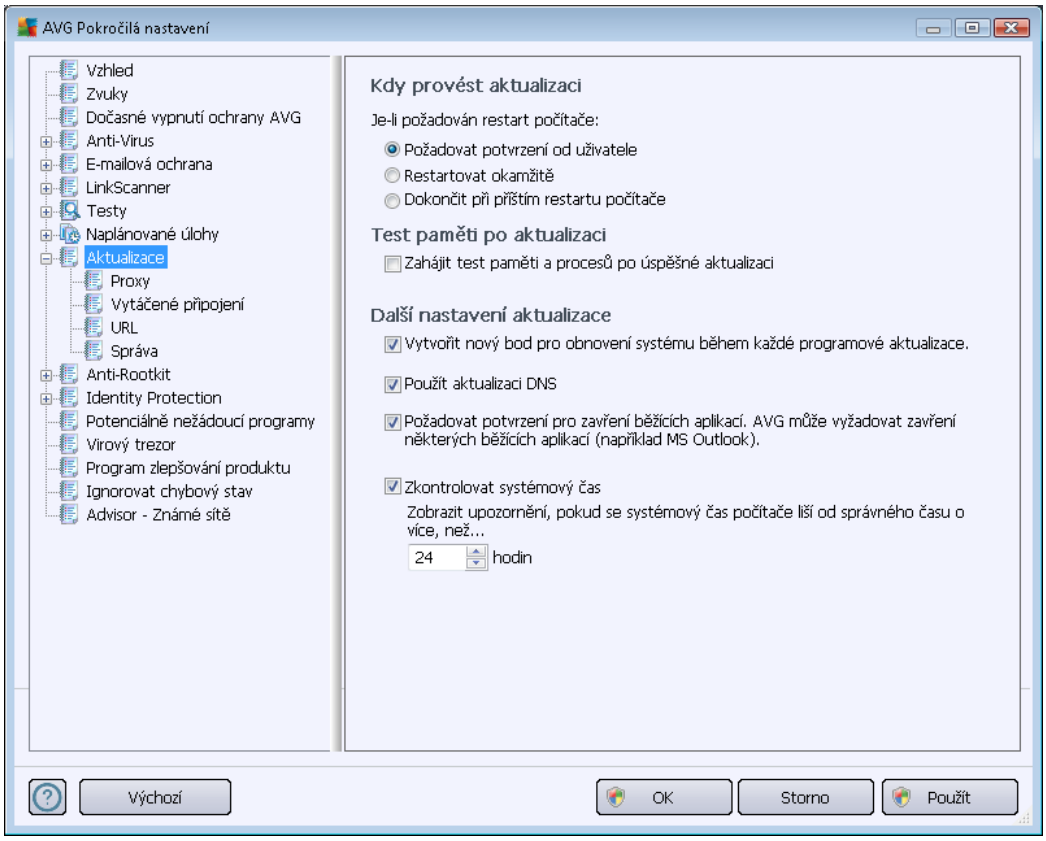
Další nastavení aktualizace

Volbou položky ***Provést aktualizaci znovu po připojení k Internetu*** zajistíte, že pokud dojde během programové aktualizace k problémům s připojením a aktualizace tedy nebude moci být dokončena, bude znovu spuštěna bezprostředně po obnovení připojení. O automatickém spuštění aktualizace budete v určeném čase informováni prostřednictvím pop-up okna nad ikonou AVG na systémové liště *(za předpokladu, že ponecháte zapnutou volbu Zobrazovat oznámení na systémové liště v Pokročilém nastavení/Vzhled)*.

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

10.9. Aktualizace

Položka navigace ***Aktualizace*** otevírá dialog, v němž můžete specifikovat obecné parametry související s aktualizací AVG:



Kdy provést aktualizaci

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

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

Test paměti po aktualizaci

Označíte-li tuto položku, bude po každé 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:

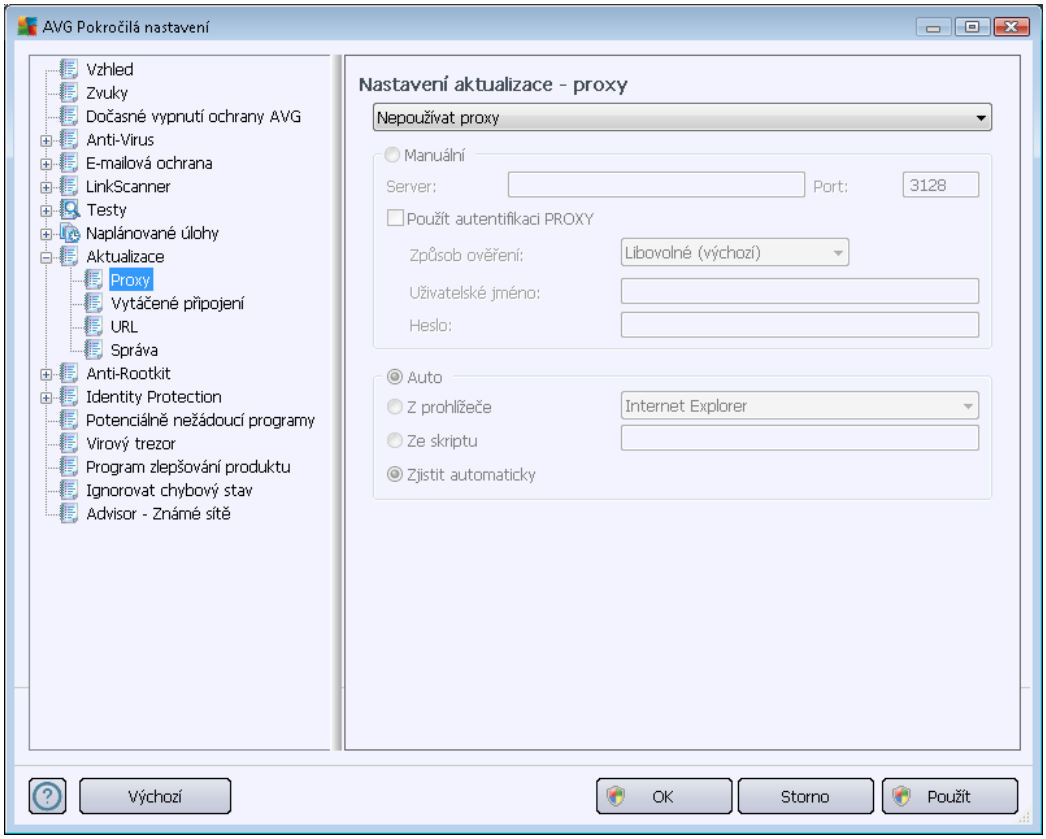
- ***Vytvořit nový bod pro obnovení systému ...*** - před každým spuštěním programové aktualizace AVG je vytvořen takzvaný systémový bod pro obnovení systému. V případě, že aktualizační proces nebude z nějakého důvodu dokončen a váš operační systém bude ohrožen, můžete za pomoci tohoto zálohovacího bodu 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*** (*ve výchozím nastavení zapnuto*) - pokud je tato položka označena, při spuštění aktualizace **AVG Anti-Virus 2012** vyhledá na DNS serveru informaci o aktuální verzi virové databáze a aktuální verzi programu a následně stáhne pouze nejmenší nezbytně nutné aktualizační soubory. Tím se sníží celkový objem stahovaných dat a urychlí proces aktualizace.

- ***Požadovat potvrzení pro zavření běžících aplikací*** (*ve výchozím nastavení zapnutou*) zajistíte, že v případě, že bude nutné zavřít některé spuštěné aplikace, aby mohla být aktualizace dokončena, budete před jejich zavřením upozorněni varovným hlášením.

- ***Zkontrolovat systémový čas*** - označením této položky určíte, že si přejete, abyste byli informováni o případném rozporu mezi časem nastaveném na počítači a skutečným časem, a to v okamžiku, kdy rozdíl těchto dvou časů dosáhne stanoveného počtu hodin.

10.9.1. Proxy



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

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

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

Manuální nastavení

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

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

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

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

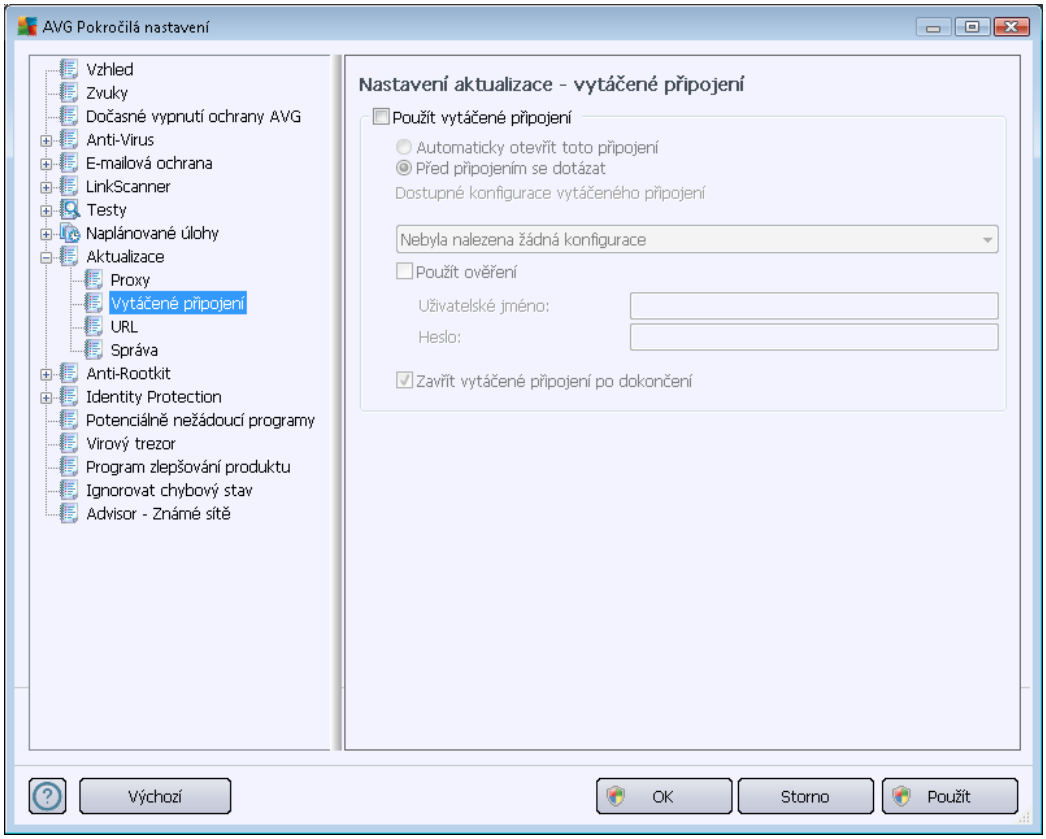
Automatické nastavení

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

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

10.9.2. Vytáčené připojení

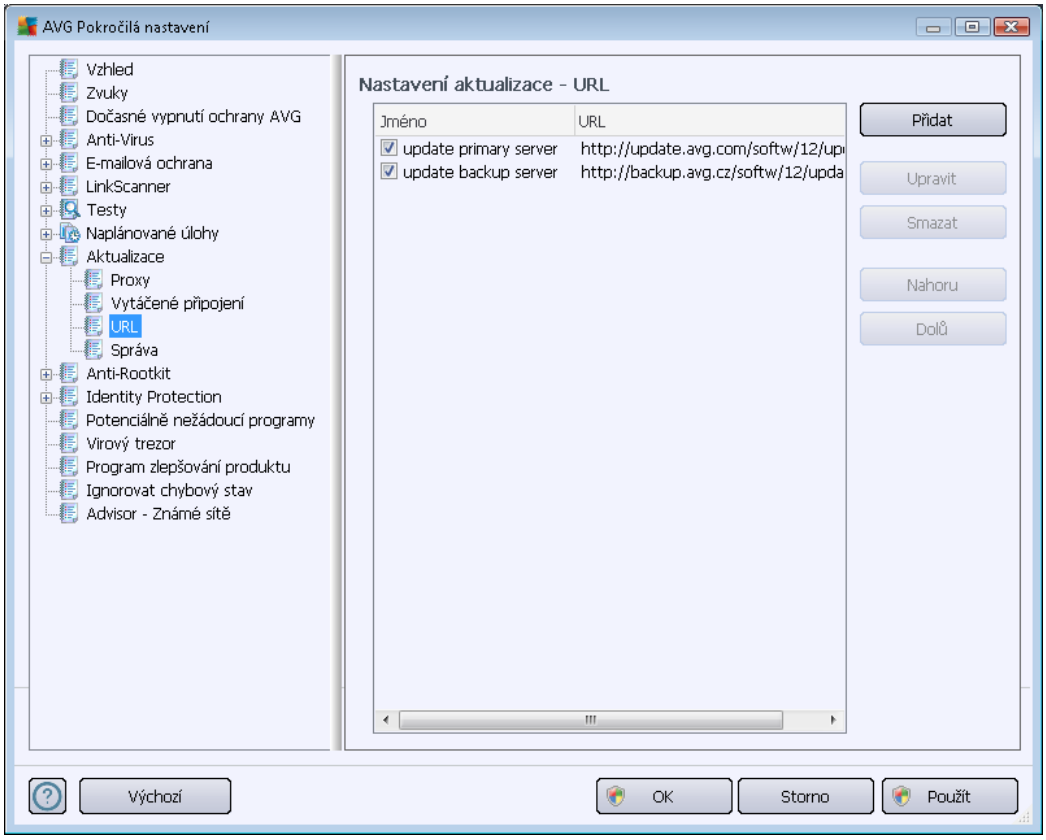
Parametry nastavované v dialogu ***Nastavení aktualizace - vytáčené připojení*** se vztahují k telefonickému připojení. Jednotlivá pole záložky jsou neaktivní, pokud neoznačíte položku ***Použít vytáčené připojení***. Touto volbou se pak aktivují ostatní pole.



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

10.9.3. URL

Dialog ***URL*** nabízí seznam internetových adres, odkud mohou být aktualizační souboru staženy:



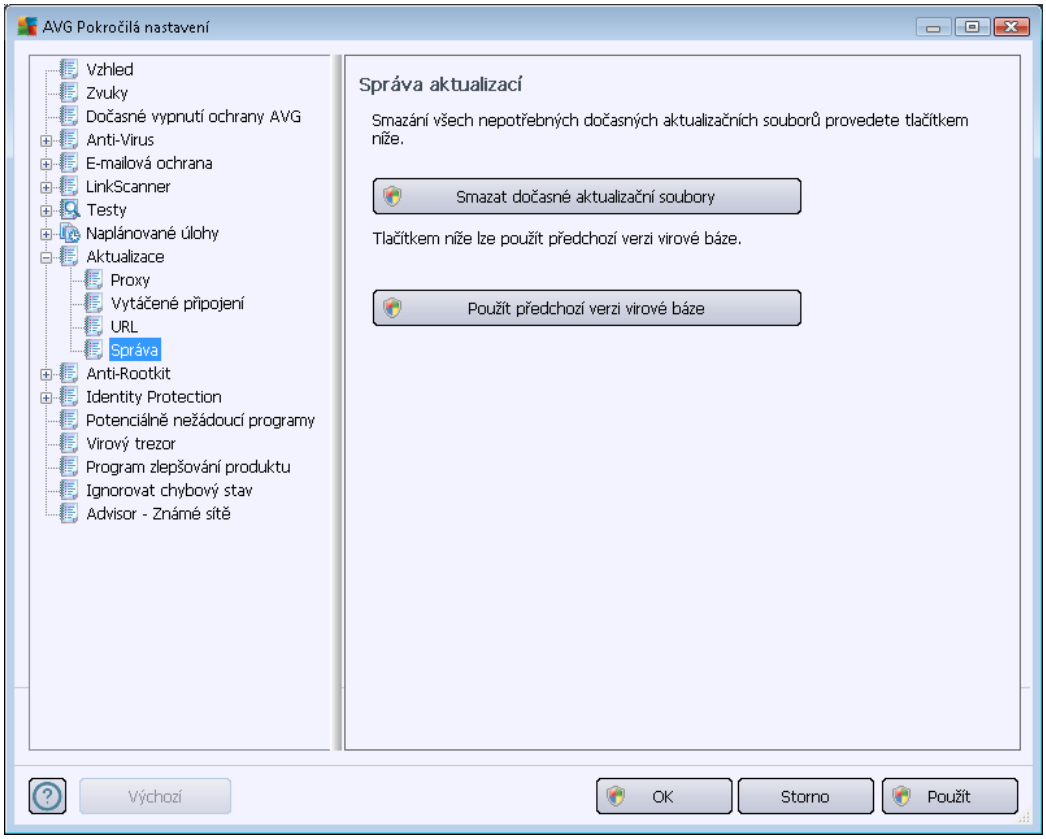
Ovládací tlačítka dialogu

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 výše
- ***Dolů*** - přemístí zvolenou URL na o jednu pozici v seznamu níže

10.9.4. Správa

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

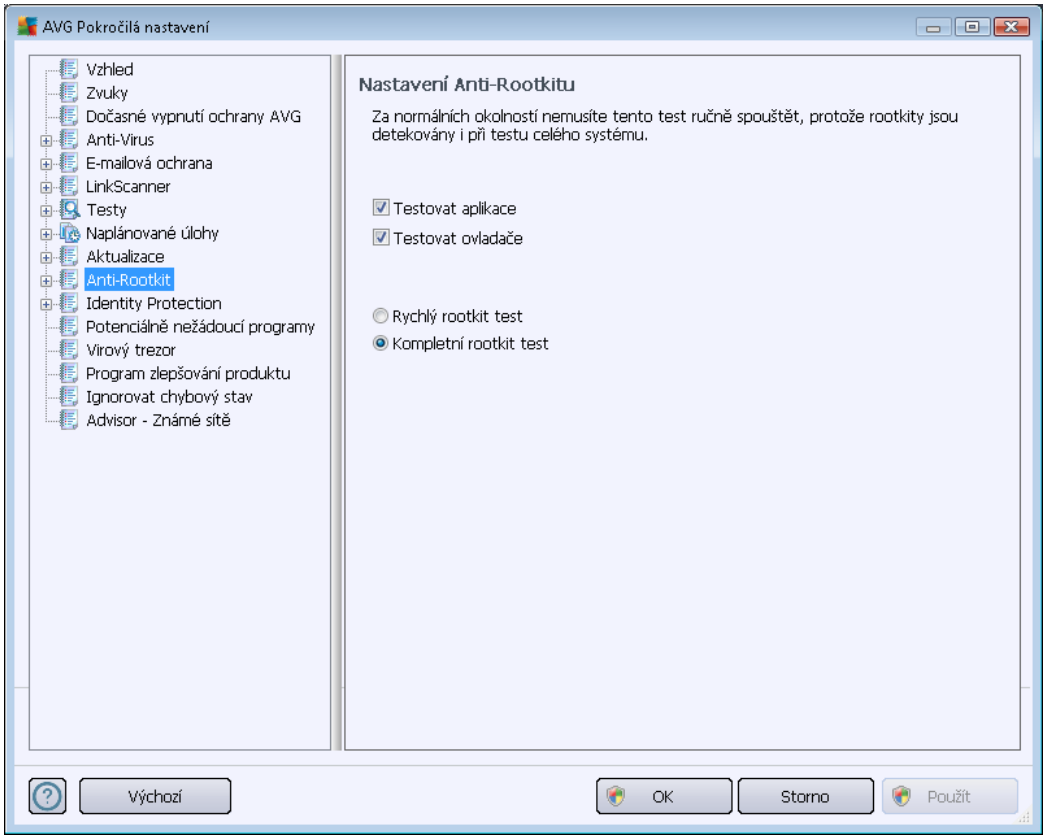


- ***Smazat dočasné aktualizační soubory*** - tímto tlačítkem odstraníte ze svého pevného disku všechny již nepotřebné soubory aktualizací (*ve výchozím nastavení správy aktualizačních souborů se tyto uchovávají po dobu po 30 dní*)

- ***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*)

10.10. Anti-Rootkit

V dialogu ***Nastavení Anti-Rootkitu*** máte možnost editovat konfiguraci komponenty Anti-Rootkit a specifické parametry vyhledávání rootkitů, které je ve výchozím nastavení zahrnuto v rámci Testu celého počítače:



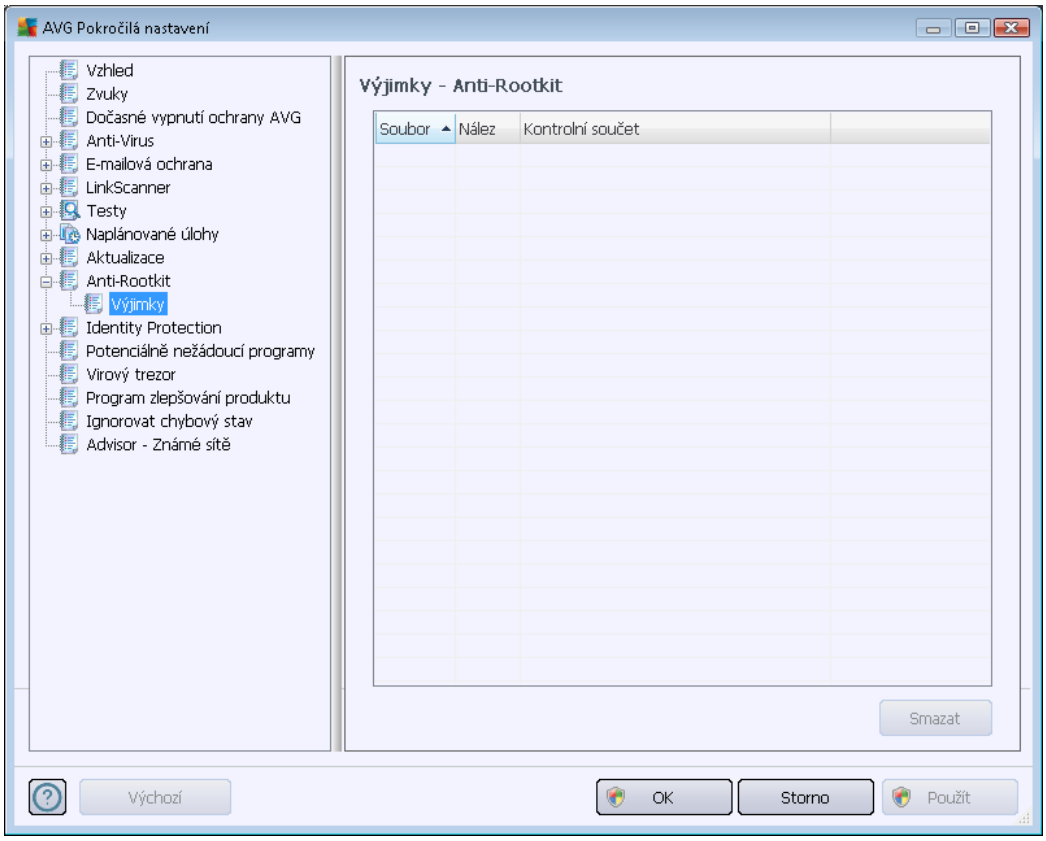
Editace všech funkcí komponenty Anti-Rootkit uvedená v tomto dialogu je dostupná i přímo z rozhraní komponenty Anti-Rootkit.

Možnosti ***Testovat aplikace*** a ***Testovat ovladače*** umožňují určit, co vše má být v testu na rootkity zahrnuto. Jiné než výchozí nastavení doporučujeme pouze zkušeným uživatelům; jinak prosím ponechte všechny možnosti zapnuté. Dále se pak můžete rozhodnout, v jakém režimu si přejete test spustit:

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

10.10.1. Výjimky

V dialogu ***Výjimky - Anti-Rootkit*** můžete definovat specifické soubory *(například ovladače, které mohou být falešně detekovány jako rootkity)*, jež mají být z testování vyňaty:

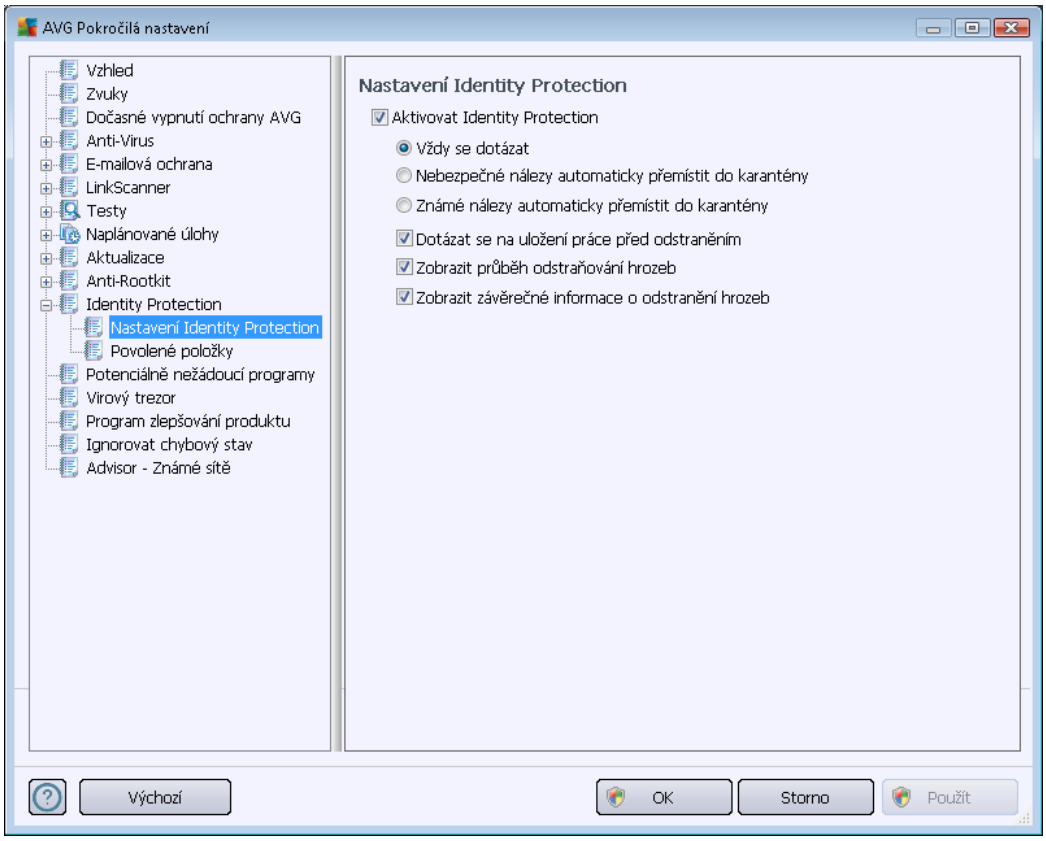


10.11. Identity Protection

Identity Protection je komponentou, která průběžně a v reálném čase zajišťuje ochranu před různými druhy malware a virů, a to na bázi identifikace specifického chování těchto typů aplikací *(podrobný popis fungování komponenty najdete v kapitole Identity Protection)*.

10.11.1. Nastavení Identity Protection

Dialog ***Nastavení Identity Protection*** umožňuje zapnout či vypnout některé základní vlastnosti komponenty Identity Protection:



Položka ***Aktivovat Identity Protection*** (*ve výchozím nastavení zapnuta*) aktivuje všechny dále nastavené funkce této komponenty.

Důrazně doporučujeme ponechat komponentu zapnutou!

Je-li položka ***Aktivovat Identity Protection*** označena a komponenta je aktivní, máte dále možnost určit, co se má stát v případě detekce hrozby:

- ***Vždy se dotázat*** (*ve výchozím nastavení zvoleno*) **-** při nálezu potenciální škodlivé aplikace budete dotázáni, zda má být tato aplikace skutečně přesunuta do karantény; tímto dotazem lze zabránit tomu, aby byly odstraněny i programy, které ve skutečnosti škodlivé nejsou a Vy je na Vašem počítači chcete.

- ***Nebezpečné nálezy automaticky přemístit do karantény*** **-** označte tuto položku, pokud si přejete, aby veškeré aplikace detekované jako možný malware byly automaticky a okamžitě přesunuty do bezpečného prostoru Virového trezoru. Pokud ponecháte výchozí nastavení, budete při nálezu potenciální škodlivé aplikace dotázáni, zda má být tato aplikace skutečně přesunuta do karantény - tímto dotazem lze zabránit tomu, aby byly odstraněny i programy, které ve skutečnosti škodlivé nejsou a Vy je na Vašem počítači chcete.

- ***Známé nálezy automaticky přemístit do karantény*** - označte tuto položku, pokud si přejete, aby veškeré aplikace detekované jako možný malware byly automaticky a okamžitě přesunuty do Virového trezoru.

Pak můžete označením příslušných políček volitelně aktivovat další vlastnosti Identity Protection:

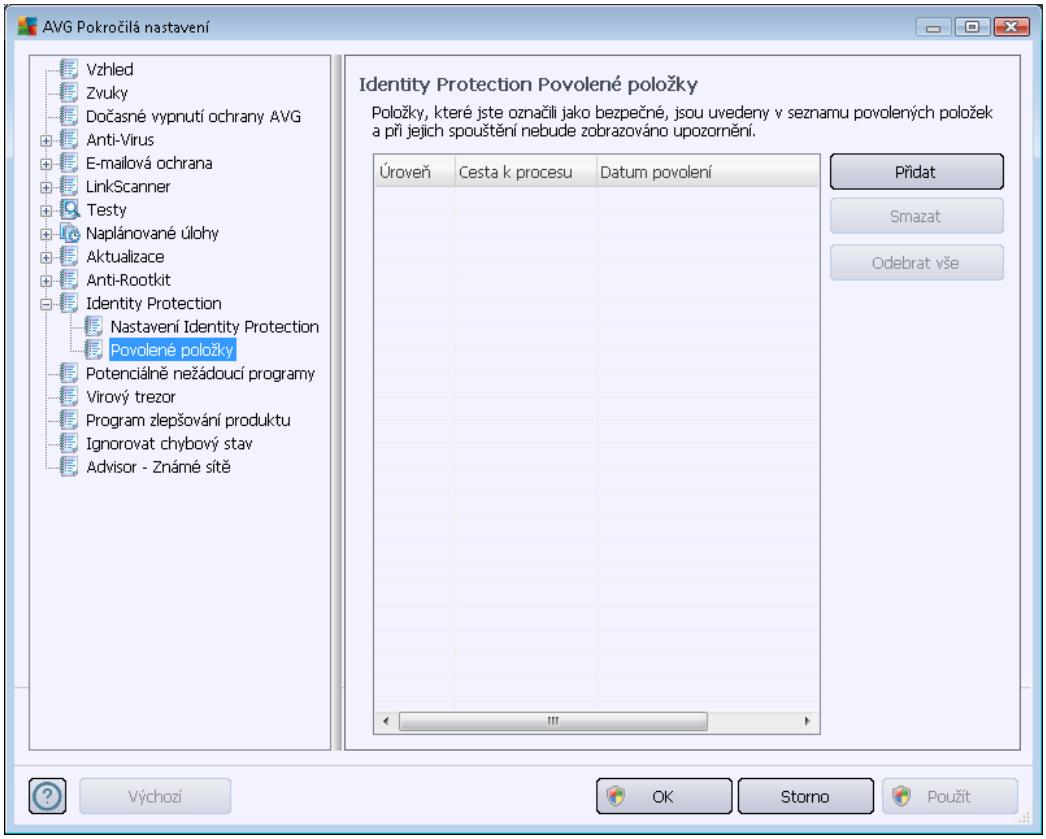
- ***Dotázat se na uložení práce před odstraněním*** - (*ve výchozím nastavení zapnuto*) - označte tuto položku, pokud si přejete, abyste byli v případě detekce škodlivého software a jeho odstranění vyzváni k uložení práce rozdělané v příslušném programu. Položka je ve výchozím nastavení zapnuta a důrazně doporučujeme toto nastavení ponechat.

- ***Zobrazit průběh odstraňování hrozeb*** - (*ve výchozím nastavení zapnuto*) - je-li položka označena, při detekci potenciálního malware bude v samostatném nově otevřeném dialogu zobrazen postup jeho přemisťování do karantény.

- ***Zobrazit závěrečné informace o odstranění hrozeb*** - (*ve výchozím nastavení zapnuto*) - je-li položka označena, zobrazí Identity Protection podrobné informace o každé položce, kterou umístí do karantény, včetně úrovně závažnosti, přesného umístění a dalších charakteristik.

10.11.2. Povolené položky

Pokud jste v dialogu Nastavení Identity Protection ponechali položku ***Nebezpečné nálezy automaticky přemístit do karantény*** neoznačenou, budete při každém nálezu potenciálně nebezpečné aplikace dotázáni, zda má být tato aplikace skutečně považována za malware a přesunuta do Virového trezoru. Jestliže se tedy rozhodnete označit spornou aplikaci (*detekovanou jako malware na základě jejího chování*) za bezpečnou a potvrdíte, že si přejete tuto aplikaci ponechat spuštěnou na svém počítači, bude aplikace přidána do seznamu ***Povolených položek*** a už nebude považována za škodlivou:



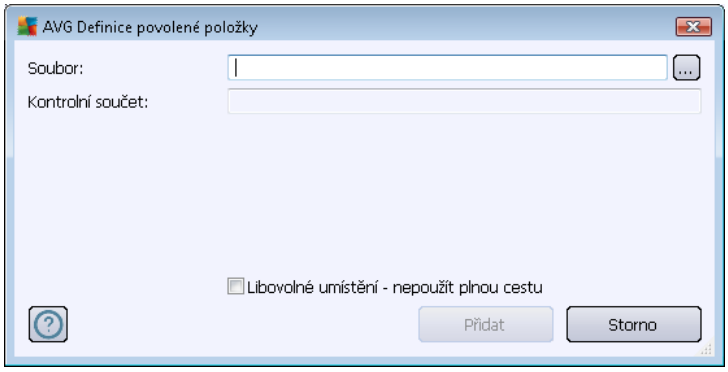
V seznamu ***Povolené položky*** najdete následující informace o každé aplikaci:

- ***Úroveň*** - grafické zobrazení závažnosti běžícího procesu na čtyřstupňové v rozpětí méně významný (■□□□) až kritický (■■■■)
- ***Cesta k procesu*** - cesta k umístění spustitelného souboru dané aplikace (*procesu*)
- ***Datum povolení*** - datum, kdy jste ručně označili danou aplikaci jako povolenou

Ovládací tlačítka dialogu

Ovládacími tlačítky dialogu ***Identity Protection Povolené položky*** jsou:

- ***Přidat*** - otevře editační dialog, v němž můžete nastavit parametry nově přidávané aplikace:

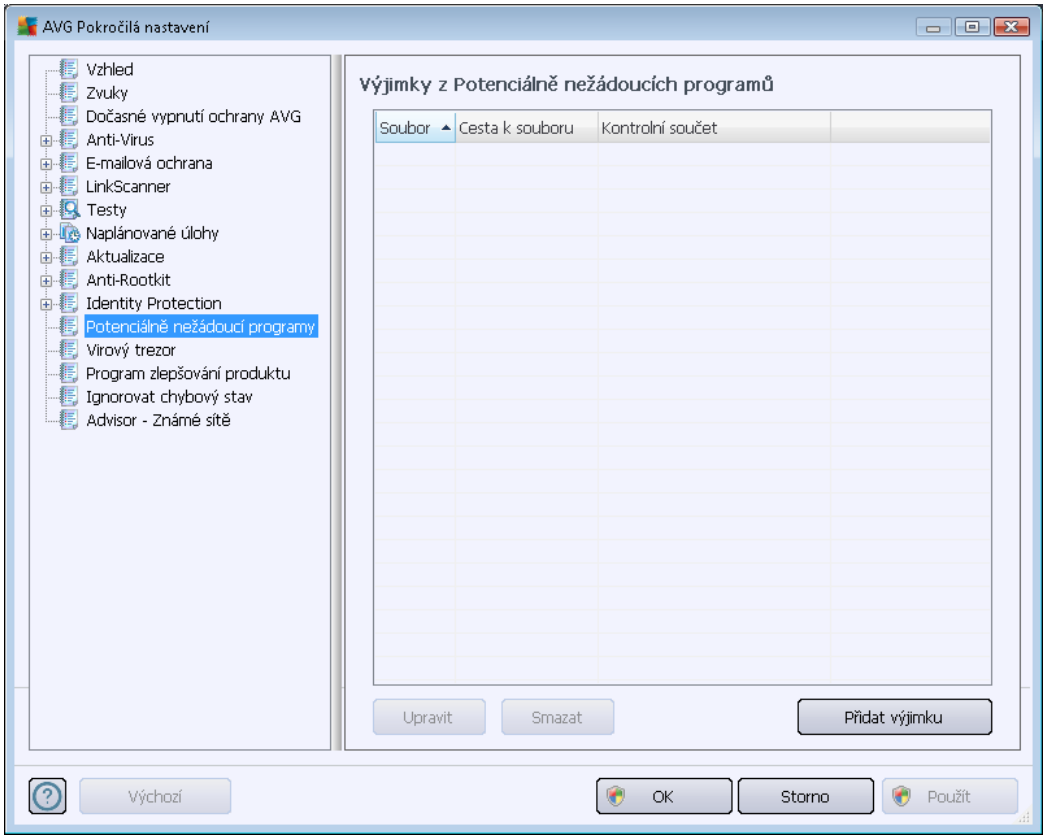


- ***Soubor*** - zadejte plnou cestu k souboru, který chcete označit jako výjimku
- ***Kontrolní součet*** - uvádí unikátní "podpis" vybraného souboru - automaticky vygenerovaný řetězec znaků, který umožní jednoznačně odlišit zvolený soubor od všech ostatních. Tento součet je vygenerován a zobrazen až po úspěšném přidání dané výjimky.
- ***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*).

- ***Smazat*** - stiskem tlačítka odstraníte vybranou položku ze seznamu povolených aplikací
- ***Odebrat vše*** - stiskem tlačítka odstraníte všechny položky ze seznamu povolených aplikací

10.12. Potenciálně nežádoucí programy

AVG Anti-Virus 2012 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 Anti-Virus 2012** 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.

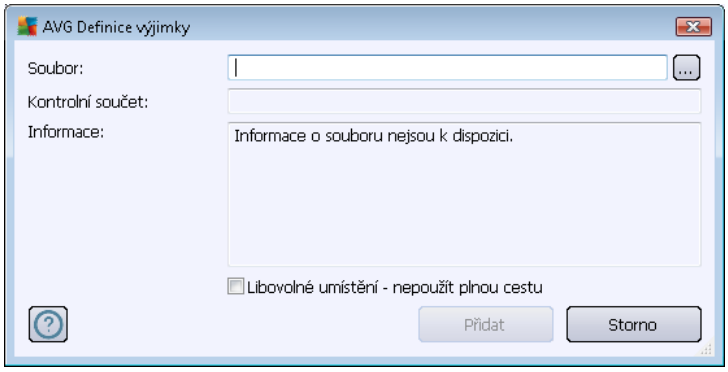


Dialog ***Výjimky z Potenciálně nežádoucích programů*** zobrazuje seznam již definovaných a aktuálně platných výjimek z potenciálně nežádoucích programů. Výjimku můžete editovat, smazat anebo nově přidat. Ke každé jednotlivé výjimce najdete v přehledu následující informace:

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

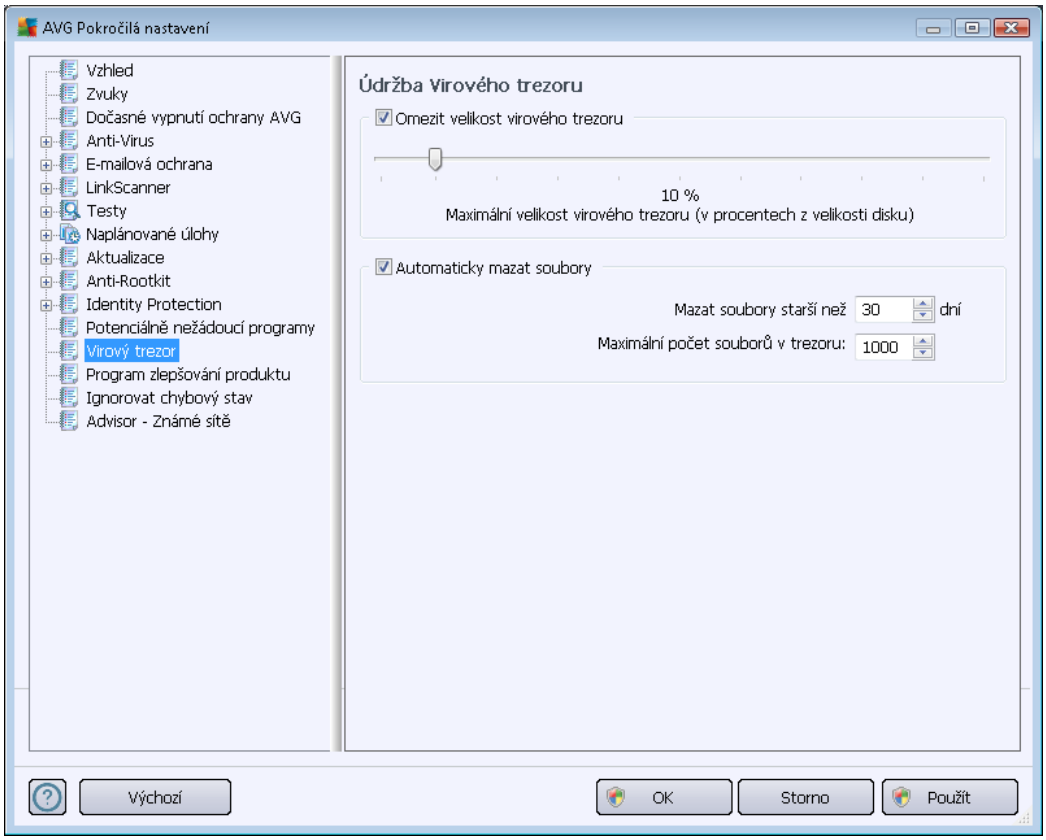
Ovládací tlačítka dialogu

- ***Upravit*** - otevře editační dialog (*totožný s dialogem pro zadání nové výjimky, viz níže*) již definované výjimky, kde můžete měnit nastavené parametry
- ***Smazat*** - odstraní označenou položku ze seznamu výjimek
- ***Přidat výjimku*** - otevře editační dialog, v němž můžete nastavit parametry nově definované výjimky:



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

10.13. Virový trezor



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

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

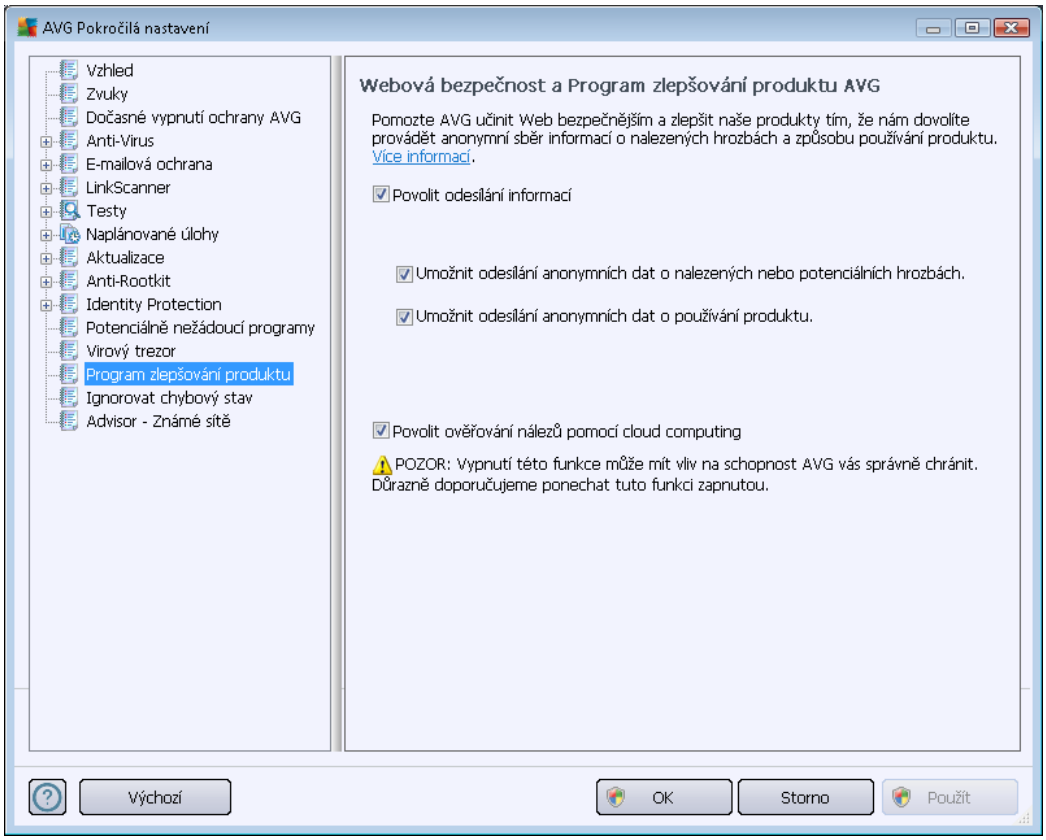
- ***Automaticky mazat soubory*** - V této sekci definujete maximální dobu, po niž se mají uchovávat soubory ve Virovém trezoru (***Mazat soubory starší než ... dní***), a maximální počet souborů uložených ve Virovém trezoru (***Maximální počet souborů v trezoru***).

10.14. 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. Ponecháte-li položku ***Povolit odesílání informací*** zapnutou, umožníte tak reportování informací o detekovaných hrozbách týmu expertů společnosti AVG Technologies. 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. Reporty nikdy neobsahují žádná vaše soukromá data. Reportování je samozřejmě dobrovolné, nicméně vás

prosíme, abyste je ponechali aktivováno. Výrazně nám tím pomůžete s vylepšováním ochrany vašeho počítače.



V dialogu najdete tyto možnosti nastavení:

- ***Povolit odesílání informací*** (*ve výchozím nastavení zapnuto*) - Chcete-li nám pomoci dále zlepšovat program AVG, ponechejte toto políčko označené. Tím povolíte odesílání informací o všech hrozbách, na které eventuelně narazíte při surfování po Internetu; tato funkce nám pomáhá shromažďovat nejnovější data od uživatelů po celém světě a neustále tak vylepšovat jejich ochranu. Reportování probíhá automaticky, takže vám nezpůsobí žádné nepohodlí, a nezahrnuje žádná osobní data.

    - ***Umožnit po potvrzení uživatelem odesílání dat o nesprávně identifikovaných e-mailech*** (*ve výchozím nastavení zapnuto*) – zasílání informací o e-mailových zprávách, které byly komponentou Anti-Spam mylně označeny za spam, nebo naopak nebyly označeny, i když o spam skutečně šlo. V případě zasílání těchto informací budete napřed požádáni o svolení.

    - ***Umožnit odesílání anonymních dat o nalezených nebo potenciálních hrozbách*** (*ve výchozím nastavení zapnuto*) – zasílání informací o jakémkoli podezřelém nebo skutečně nebezpečném kódu či vzorci chování *(může jít o virus, spyware, případně nebezpečnou webovou stránku, na kterou jste se pokusili přejít)* nalezeném ve vašem počítači.

- **Umožnit odesílání anonymních dat o používání produktu** (*ve výchozím nastavení zapnuto*) – zasílání základních statistických dat o používání systému AVG jako např. počet nalezených infekcí, proběhlých testů, úspěšných/neúspěšných aktualizací atp.

- ***Povolit ověřování nálezů pomocí cloud computing*** (*ve výchozím nastavení zapnuto*) – nalezené infekce, hrozby a podezřelé kódy budou ověřeny, zda nejde o falešné detekce *(tj. ve skutečnosti neškodné)*.

Nejčastější hrozby

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.

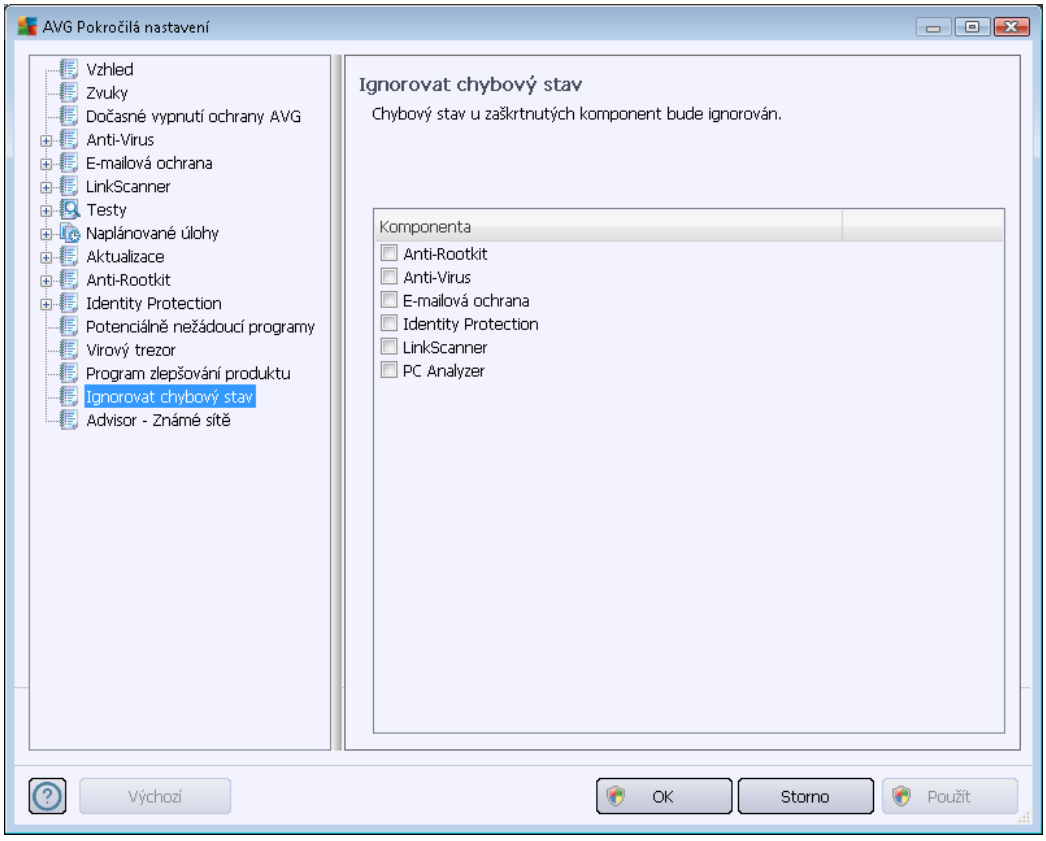
- ***Hoaxy*** jsou řetězové podvodné nebo poplašné e-maily obsahující například falešné nabídky práce, případně nabídky, které pracovníky zneužijí k nelegálním aktivitám, výzvy k vybrání velké sumy peněz, podvodné loterie a podobně.

- ***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.

AVG Anti-Virus 2012 obsahuje ochranu proti všem zmíněným typům hrozeb a škodlivých programů! Stručný přehled funkcionality jednotlivých komponent najdete v kapitole Přehled komponent.

10.15. Ignorovat chybový stav

V dialogu ***Ignorovat chybový stav*** máte možnost označit ty komponenty, jejichž případný chybový stav si přejete ignorovat:



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

- ikony na systémové liště - pokud vše funguje jak má, je ikona zobrazena barevně; objeví-li se chyba, ikona se zobrazí se žlutým vykřičníkem

- textového popisu aktuálního problému v sekci Informace o stavu zabezpečení v hlavním okně AVG

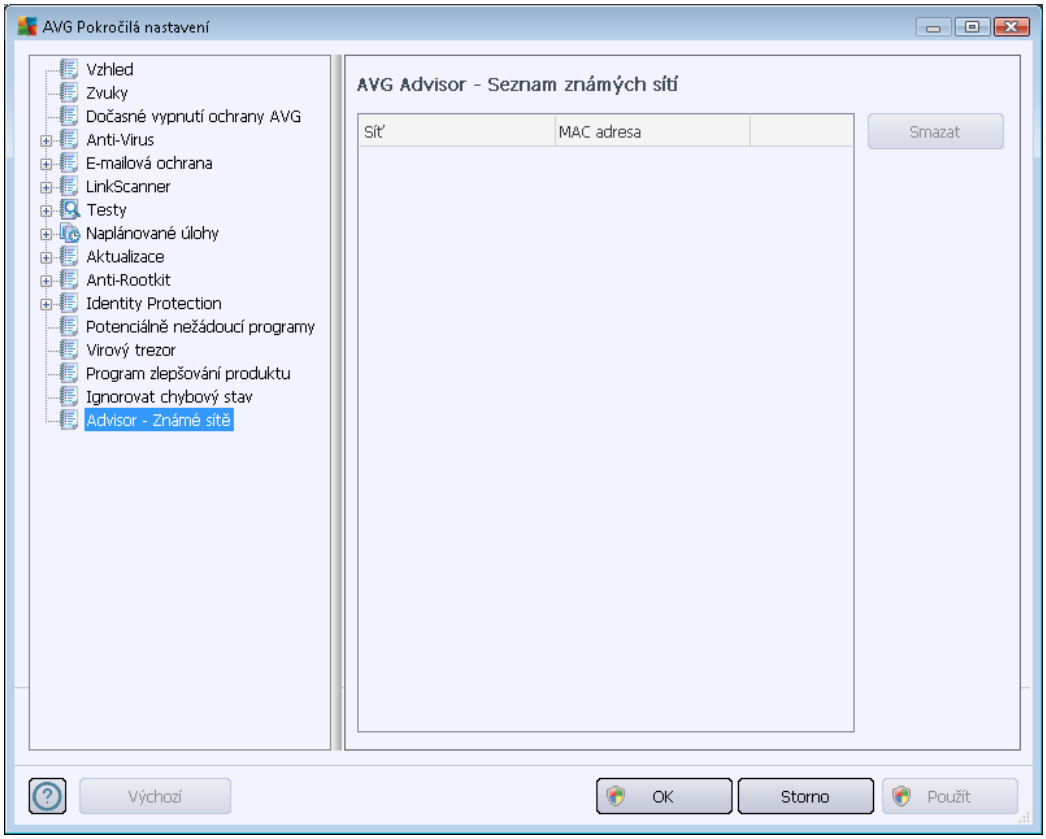
Může se ale stát, že si z nějakého důvodu přejete dočasně deaktivovat určitou komponentu (*samozřejmě doporučujeme ponechat všechny komponenty trvale zapnuté a ve výchozím nastavení, ale tato možnost existuje*). Pak by ikona na systémové liště automaticky oznamovala chybový stav, který ale de facto není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

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

10.16. Advisor - známé sítě

Služba AVG Advisor obsahuje funkci, která sleduje sítě, do nichž se připojujete. Pokud objeví síť dosud nepoužitou *(avšak s názvem, který používá některá ze známých sítí, což může být matoucí)*, upozorní vás na to a doporučí, abyste si síť prověřili. Pokud usoudíte, že síť je bezpečná, můžete ji uložit do tohoto seznamu *(prostřednictvím odkazu v informačním dialogu AVG Advisoru, který se vysune nad systémovou lištou při detekci neznámé sítě - podrobný popis najdete v kapitole AVG Advisor)*. AVG Advisor si zapamatuje jedinečné identifikační údaje sítě, zejména adresu MAC, a příště už vás nebude upozorňovat. Každá síť, k níž se připojíte, bude pro příště automaticky považována za známou, a přidána do seznamu. Libovolné položky můžete vymazat pomocí tlačítka ***Smazat***; příslušná síť pak bude znovu považována za neznámou a neprověřenou.

V tomto dialogu si tedy můžete ověřit, které sítě jsou považovány za známé:

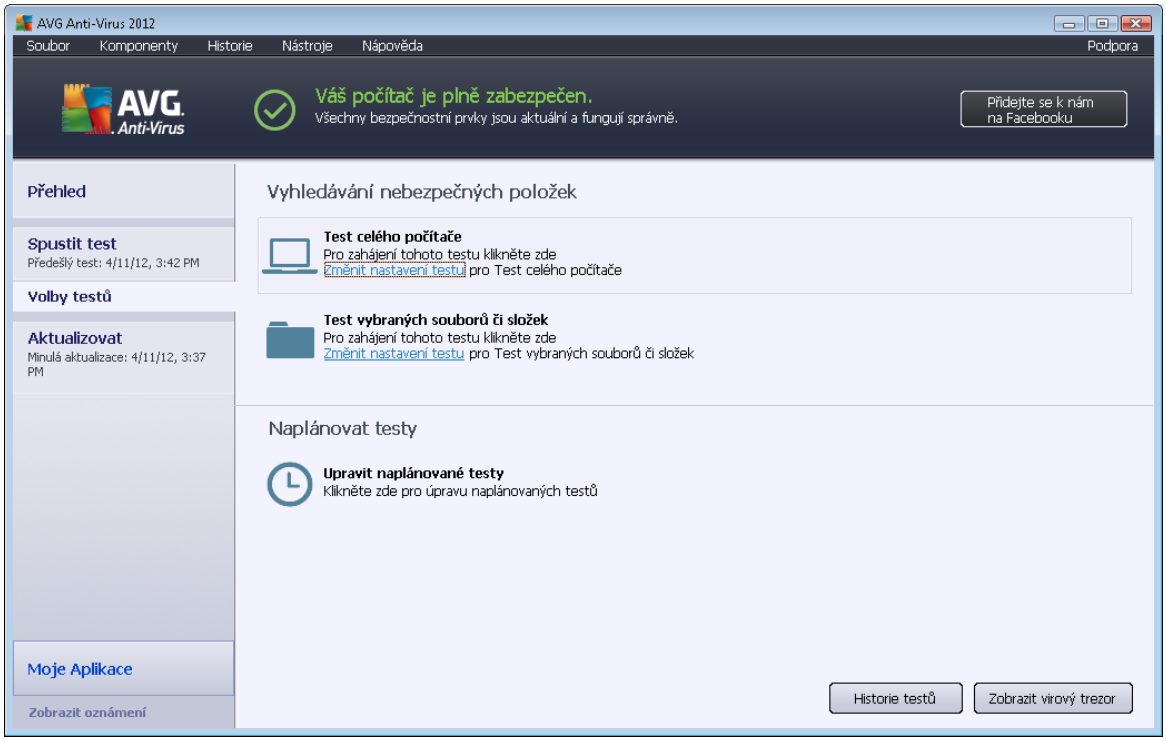


Poznámka: *Funkce známé sítě v rámci služby AVG Advisor není podporována na Windows XP 64-bit.*

11. AVG testování

Ve výchozím nastavení **AVG Anti-Virus 2012** se nespouští žádný test automaticky, protože po úvodním otestování počítače jste průběžně chráněni rezidentními komponentami **AVG Anti-Virus 2012**, které eventuelní škodlivý kód zachycují okamžitě. Samozřejmě ale můžete naplánovat test k pravidelnému spouštění v určený čas, případně kdykoli spustit ručně libovolný test podle vlastních požadavků.

11.1. Rozhraní pro testování



Testovací rozhraní AVG je dostupné prostřednictvím zkratkového tlačítka ***Volby testů***. Jeho stiskem se přepnete 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
- 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

11.2. Přednastavené testy

Jednou z hlavních funkcí **AVG Anti-Virus 2012** 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.

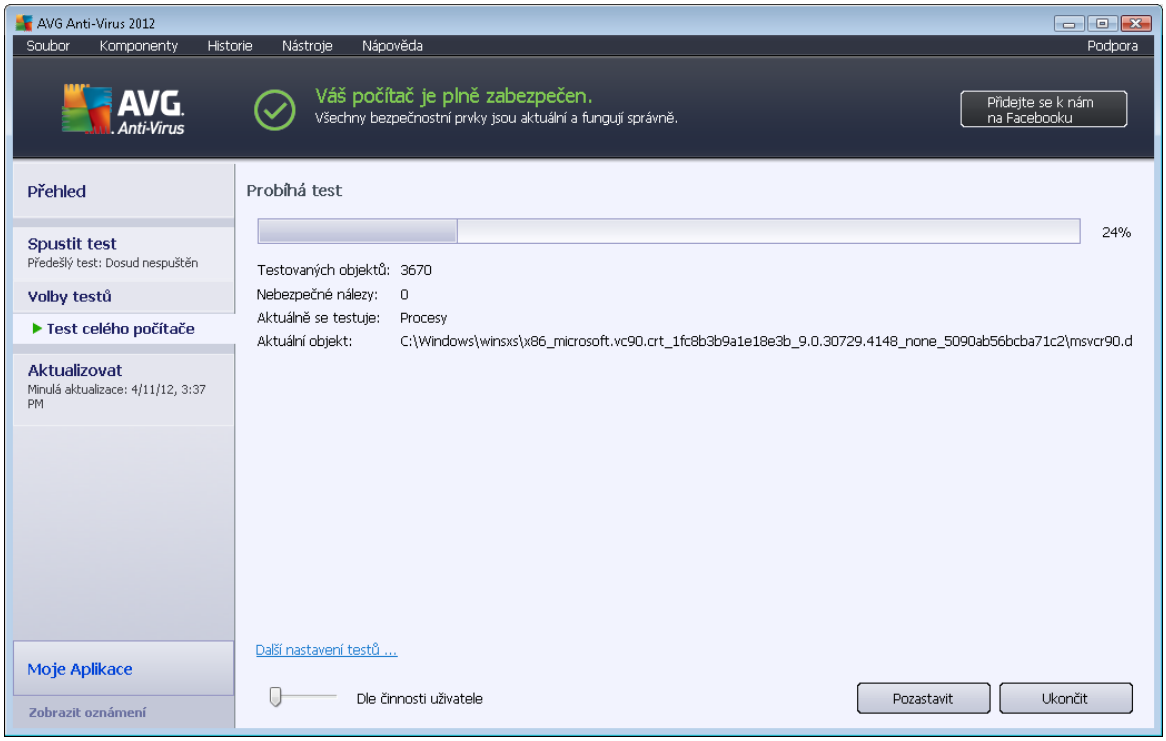
V **AVG Anti-Virus 2012** najdete tyto typy výrobcem nastavených testů:

11.2.1. 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.

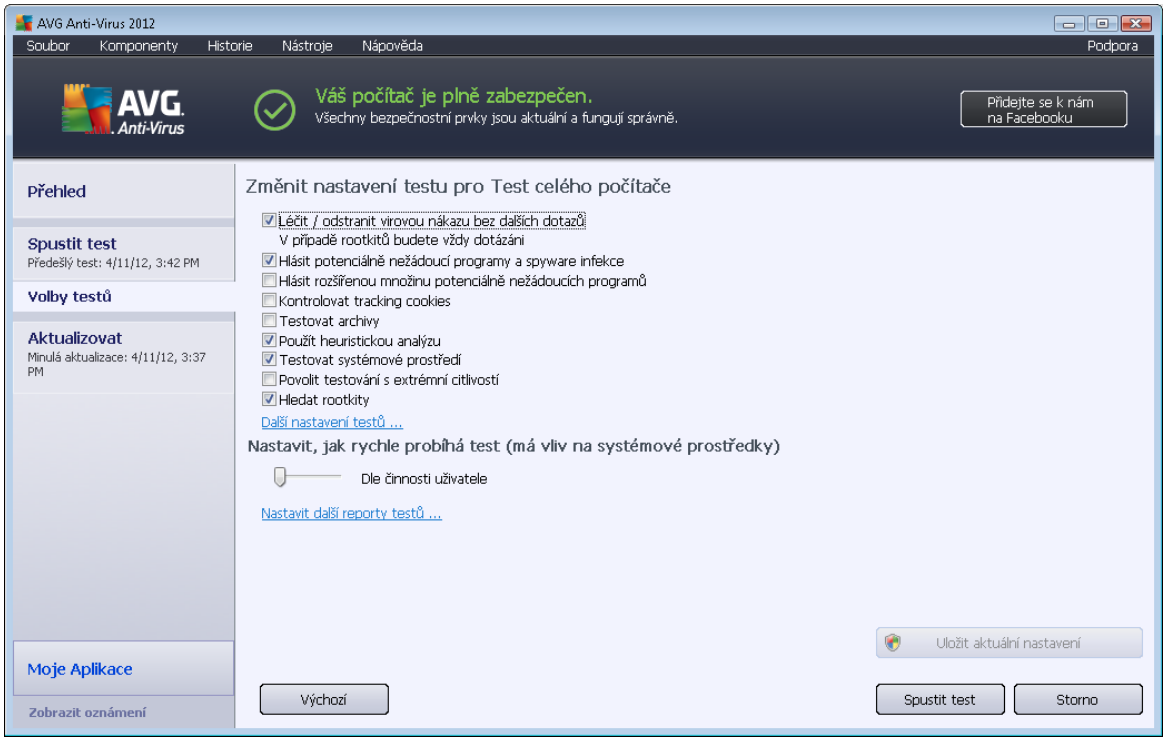
Spuštění testu

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:

    - ***Léčit / odstranit virovou nákazu bez dalších dotazů*** - (*ve výchozím nastavení zapnuto*): je-li během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. Pokud virus automaticky léčit nelze, bude infikovaný objekt automaticky přesunut do Virového trezoru.

    - ***Hlásit potenciálně nežádoucí programy a spyware infekce*** - (*ve výchozím nastavení zapnuto*): kontrola přítomnosti potenciálně nežádoucích programů (*spustitelné programy, které mohou fungovat jako spyware nebo adware*). Zaškrtnutím tohoto políčka aktivujete Anti-Spyware, tj. bude se testovat přítomnost spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány vědomě a se souhlasem uživatele. Doporučujeme nicméně ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.

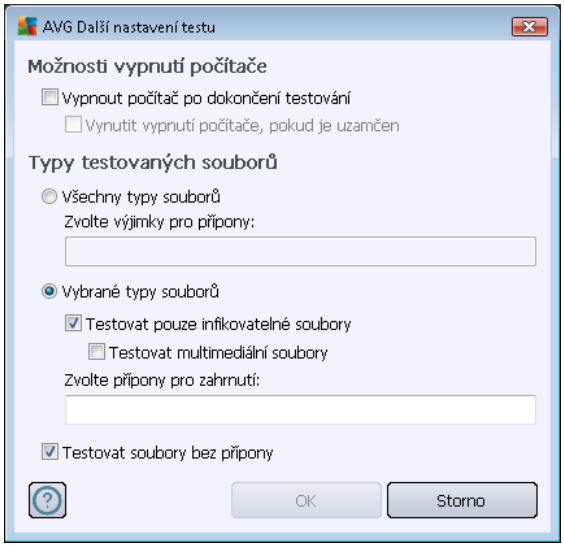
    - ***Hlásit rozšířenou množinu potenciálně nežádoucích programů*** (*ve výchozím nastavení vypnuto*) - zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v původní podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. 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.
- ***Hledat rootkity*** (*ve výchozím nastavení zapnuto*) - Parametr komponenty Anti-Rootkit prohledává počítač na přítomnost rootkitů, tedy 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.

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



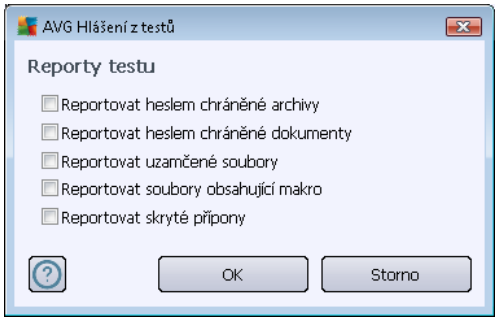
- ***Možnosti vypnutí počítače*** - určete, zda má být počítač po dokončení testu automaticky vypnut. Pokud potvrdíte tuto možnost (***Vypnout počítač po dokončení testování***), aktivuje se nová volba (***Vynutit vypnutí počítače, pokud je uzamčen***),

při jejímž potvrzení dojde po dokončení testu k vypnutí počítače i tehdy, jestliže je počítač momentálně zamknut.

- o ***Typy testovaných souborů*** - 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. Ve výchozím nastavení je tato hodnota nastavena *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 testu***, v němž můžete označit, které typy nálezů mají být hlášeny:



Upozornění: *Samotné možnosti nastavení testu jsou shodné s parametry nově definovaného testu, které jsou podrobně popsány v kapitole AVG testování / 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.*

11.2.2. Test vybraných souborů či složek

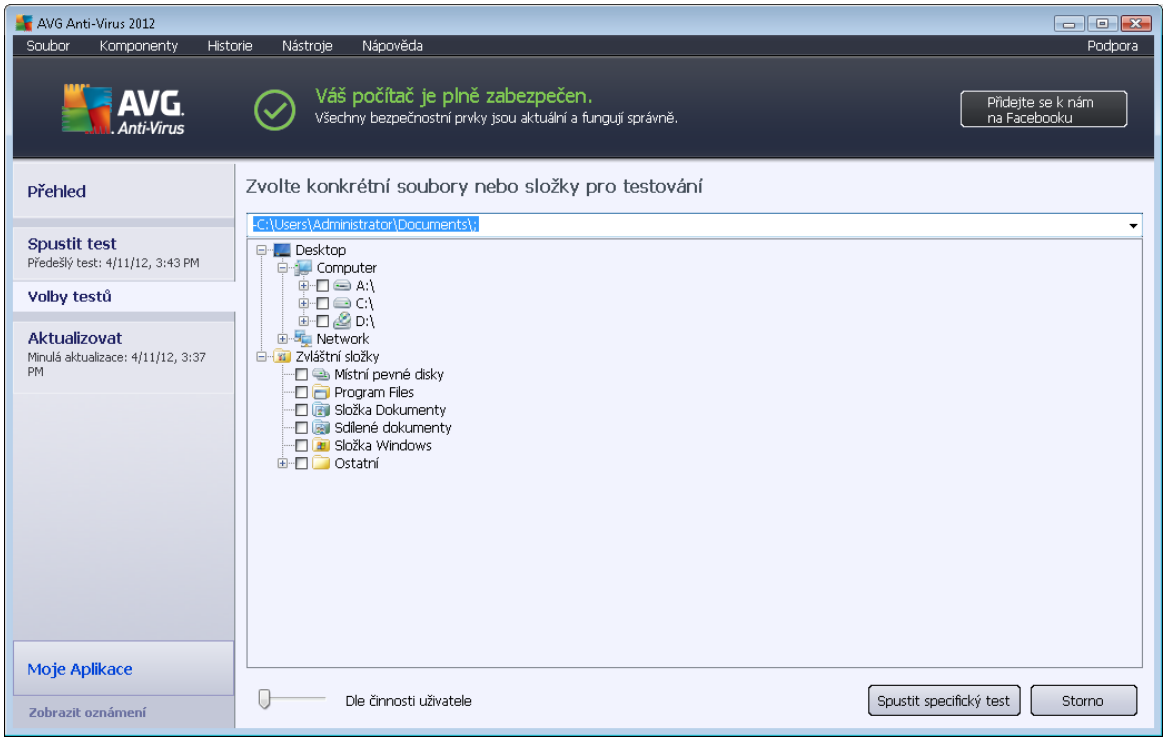
Test vybraných souborů či složek kontroluje pouze uživatelem definované oblasti počítače (*zvolené složky, pevné disky, diskety, CD, optické disky, ...*). Postup při nálezu a léčbě/ odstraňování virové nákazy je stejný jako u ***Testu celého počítače***: nalezené viry jsou vyléčeny nebo přesunuty do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

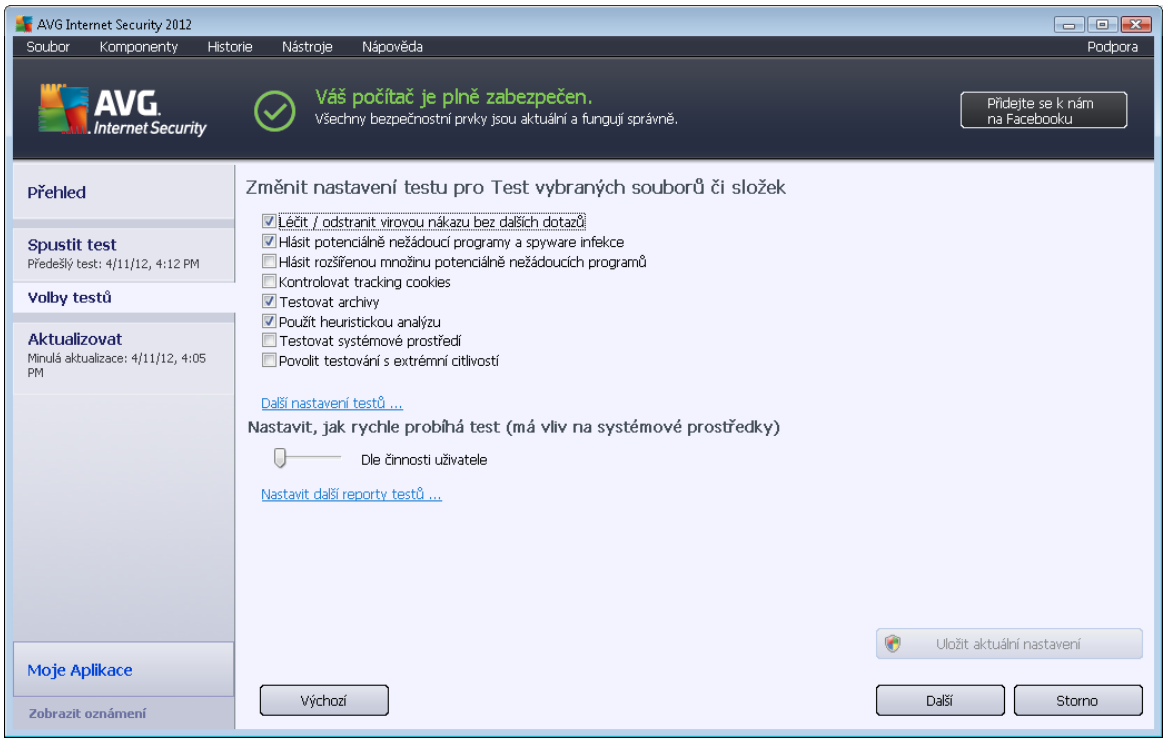
Samotný test pak spustíte stiskem tlačítka ***Spustit test*** a jeho průběh je identický s průběhem Testu celého počítače.



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:

    - ***Heal / remove virus infection without asking me*** - (*ve výchozím nastavení zapnuto*): je-li během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. Pokud virus automaticky léčit nelze, bude infikovaný objekt automaticky přesunut do Virového trezoru.

    - ***Hlásit potenciálně nežádoucí programy a spyware infekce*** - (*ve výchozím nastavení zapnuto*): kontrola přítomnosti potenciálně nežádoucích programů (*spustitelné programy, které mohou fungovat jako spyware nebo adware*). Zaškrtnutím tohoto políčka aktivujete Anti-Spyware, tj. bude se testovat přítomnost spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány 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*).

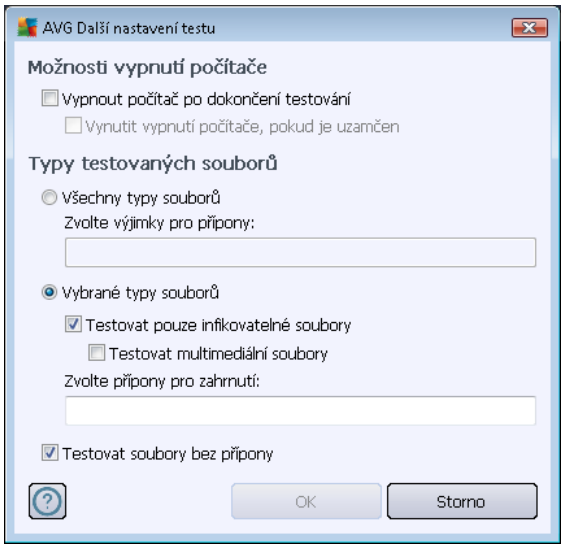
- **Testovat archivy** (*ve výchozím nastavení zapnuto*) - parametr definuje, že test má kontrolovat všechny soubory zabalené v některém typu archivu, například ZIP, RAR, ...

- **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.

- **Typy testovaných souborů** - dále se můžete rozhodnout, zda si přejete testovat

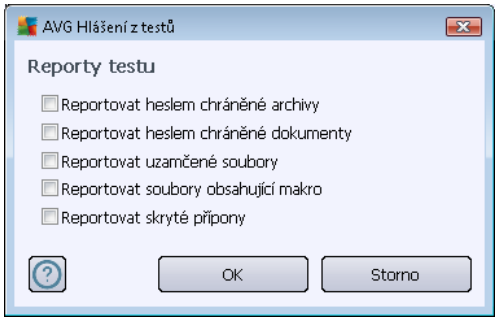
- ***Všechny typy souborů*** - přičemž máte zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou;

- ***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. Ve výchozím nastavení je tato hodnota nastavena *dle činnosti uživatele*, čímž 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*).

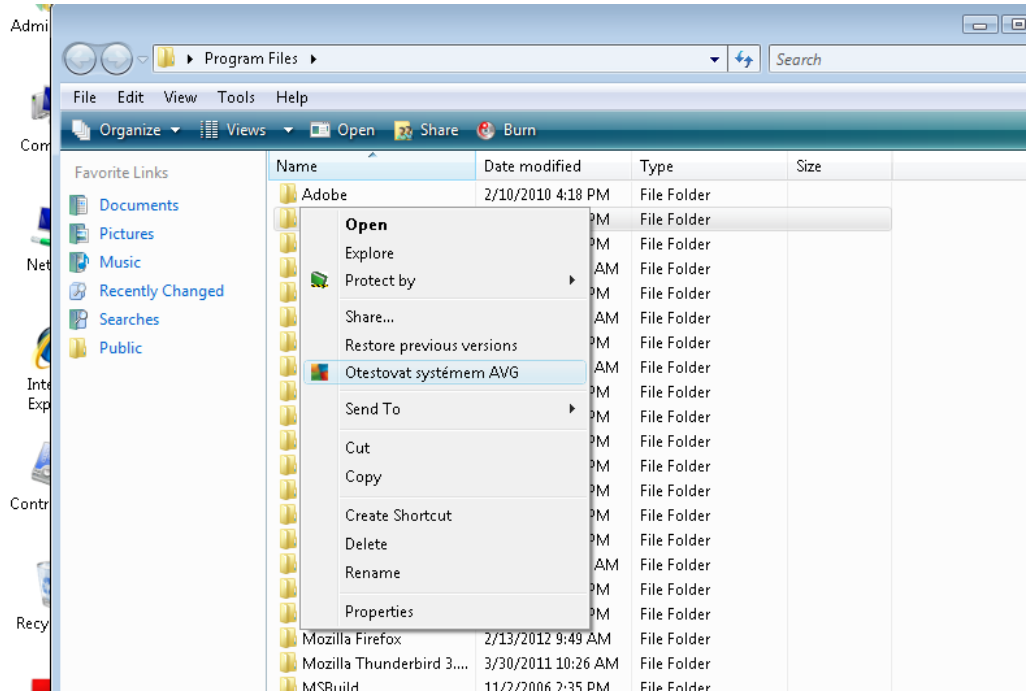
- ***Nastavit další reporty testů*** - odkaz otevírá nový dialog ***Reporty testu***, v němž můžete označit, které typy nálezů mají být hlášeny:



Upozornění: *Samotné možnosti nastavení testu jsou shodné s parametry nově definovaného testu, které jsou podrobně popsány v kapitole AVG testování / 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).*

11.3. Testování v průzkumníku Windows

AVG Anti-Virus 2012 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 Anti-Virus 2012**

11.4. Testování z příkazové řádky

V rámci **AVG Anti-Virus 2012** 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.

11.4.1. Parametry CMD testu

V následujícím přehledu nabízíme seznam dostupných parametrů testu:

- /SCAN — Test wybraných 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
- /LOG Vygenerovat soubor s výsledkem testu
- /MACROW Hlásit makra
- /PWDW Hlásit heslem chráněné soubory
- /ARCBOMBSW Reportovat archivní bomby (opakovaně komprimované archivy)
- /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
- /PUPEXT Hlásit rozšířenou množinu Potenciálně nebezpečných programů
- /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

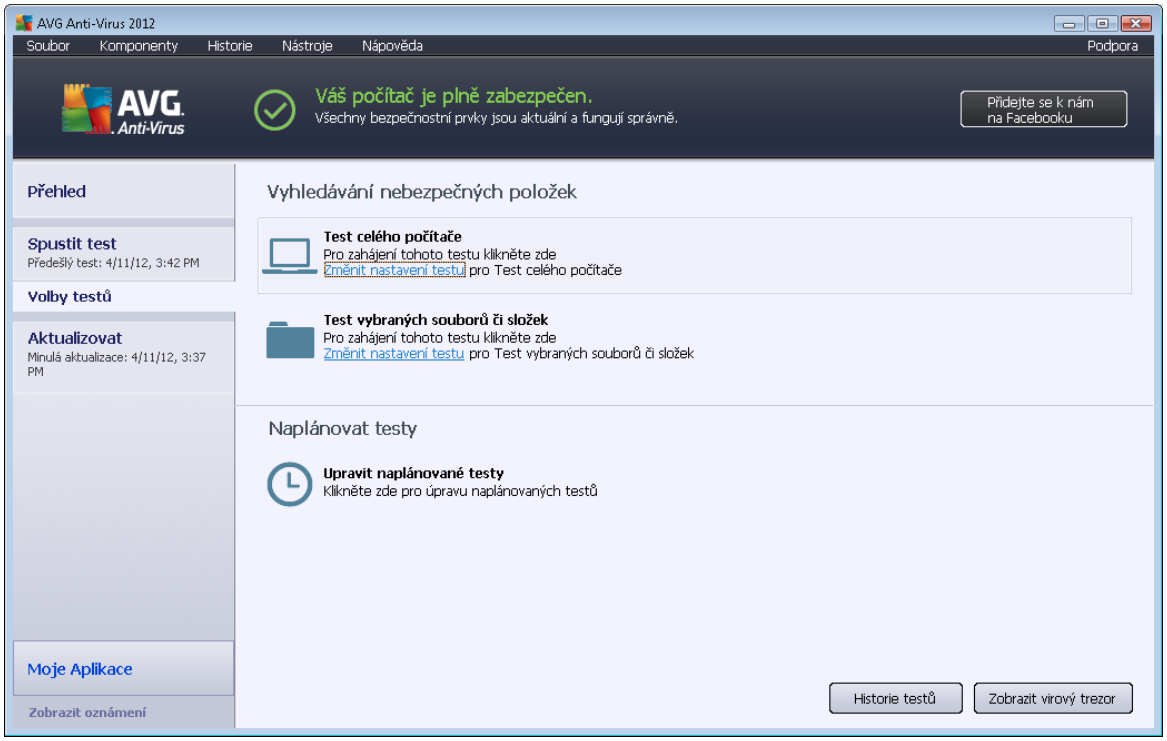
- /ADS Testovat alternativní datové proudy (pouze NTFS)
- /HIDDEN Hlásit soubory se skrytou příponou
- /INFECTABLEONLY Testovat pouze infikovatelné soubory
- /THOROUGHSCAN Povolit testování s extrémní citlivostí
- /CLOUDCHECK Ověřit falešné detekce
- /ARCBOMBSW Hlásit opakovaně komprimované archivní soubory

11.5. Naplánování testu

Testy v **AVG Anti-Virus 2012** 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.

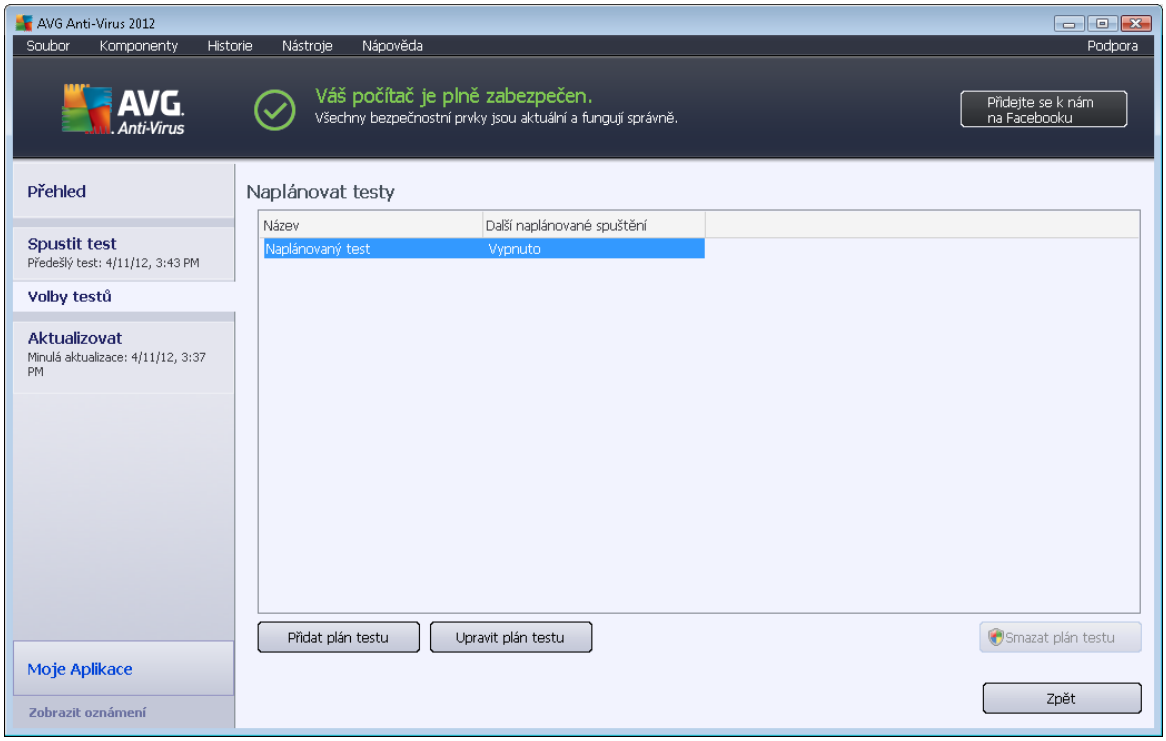
Test celého počítače by měl být spouštěn pravidelně, a to nejméně jednou týdně. Pokud vám to však provoz na vašem počítači umožňuje, doporučujeme spouštět test celého počítače jednou denně; tak je také ve výchozí konfiguraci nastaven plán testů. Jestliže je počítač trvale zapnutý, je vhodné naplánovat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

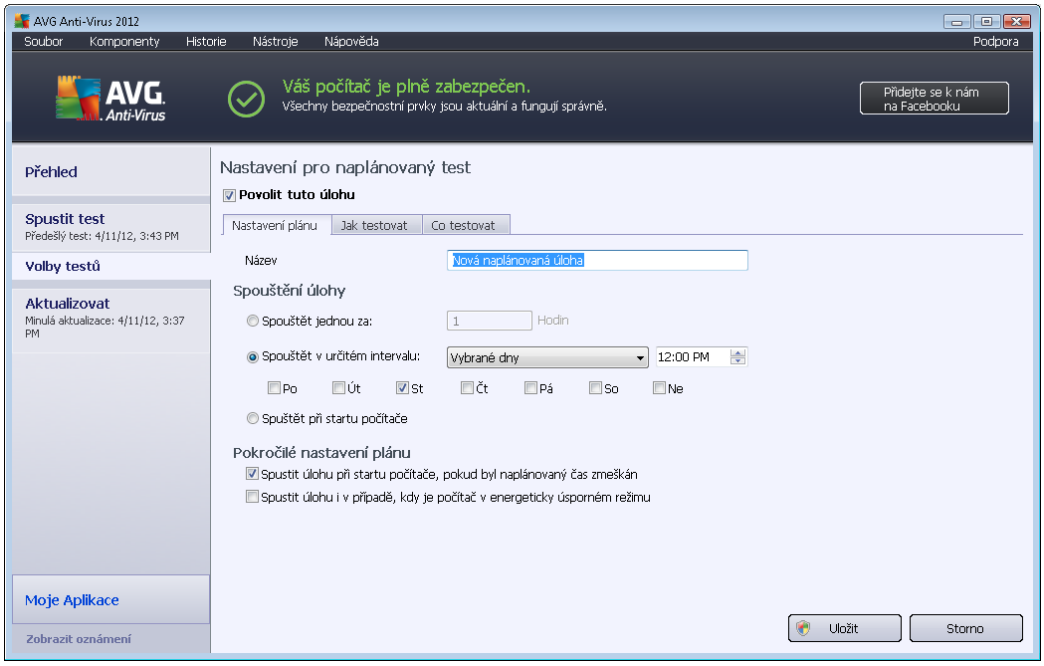


Pracovat můžete s těmito ovládacími tlačítky:

- ***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

11.5.1. 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 určitém intervalu***), 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

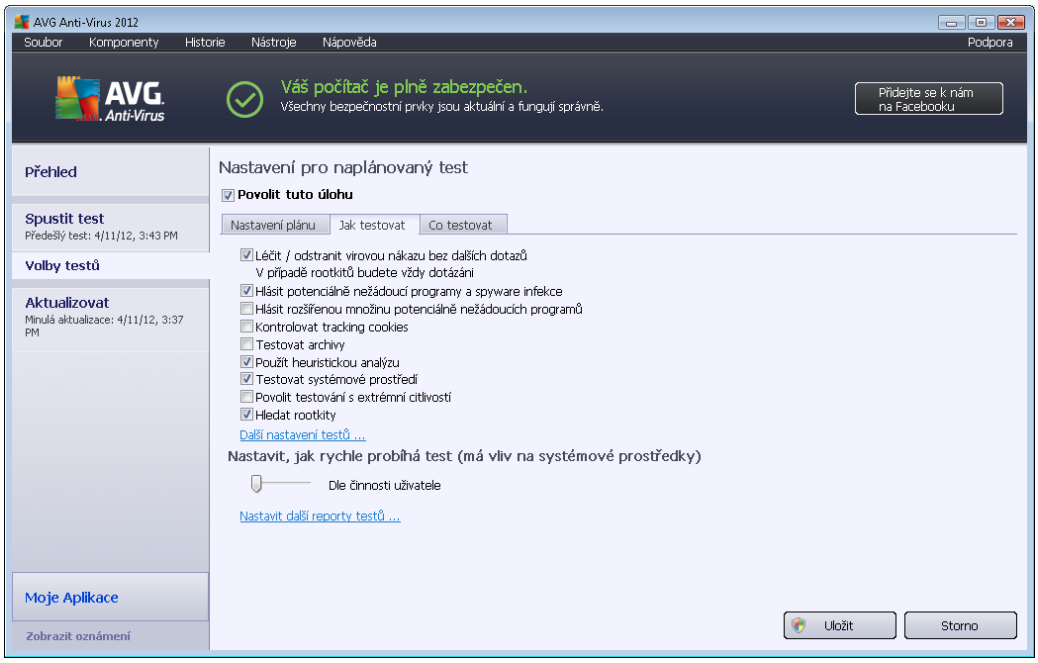
Ze všech tří záložek dialogu ***Nastavení pro naplánovaný test*** *(Nastavení plánu, Jak testovat a Co testovat)* jsou dostupná dvě ovládací tlačítka, jež mají stejnou funkčnost na kterékoli záložce

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.

11.5.2. 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:

- ***Léčit / odstranit virovou nákazu bez dalších dotazů*** - (*ve výchozím nastavení zapnuto*): je-li během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. Pokud virus automaticky léčit nelze, anebo pokud se rozhodnete tuto funkci vypnout, budete o nálezu viru vyrozuměni a můžete rozhodnout, co se má dále s infikovaným objektem provést. Doporučeným postupem je přesunutí objektu do Virového trezoru.

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

poněkud problematickou kategorii hrozeb, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány 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*).

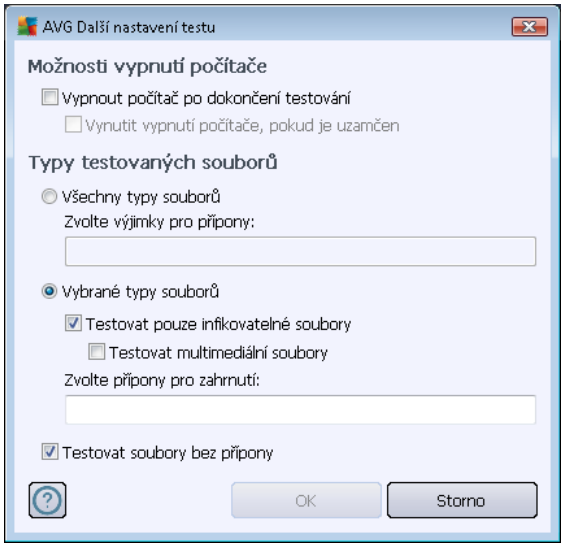
- ***Testovat systémové prostředí*** - (*ve výchozím nastavení zapnuto*): test prověří i systémové oblasti vašeho počítače.

- ***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.

- ***Hledat rootkity*** *(ve výchozím nastavení zapnuto):* parametr komponenty Anti-Rootkit prohledává počítač na přítomnost rootkitů, tedy 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.

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.

- ***Typy testovaných souborů*** - dále se můžete rozhodnout, zda si přejete testovat

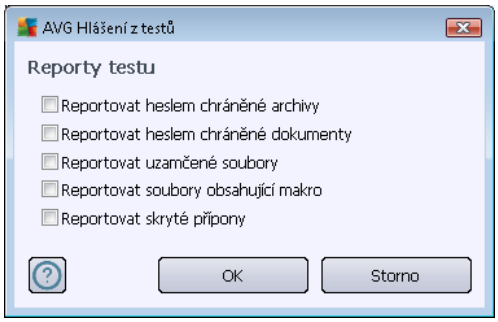
  - ***Všechny typy souborů*** - přičemž máte zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou;

  - ***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. Ve výchozím nastavení je tato hodnota nastavena *dle činnosti uživatele*, čímž 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 testu***, v němž můžete označit, které typy nálezů mají být hlášeny:



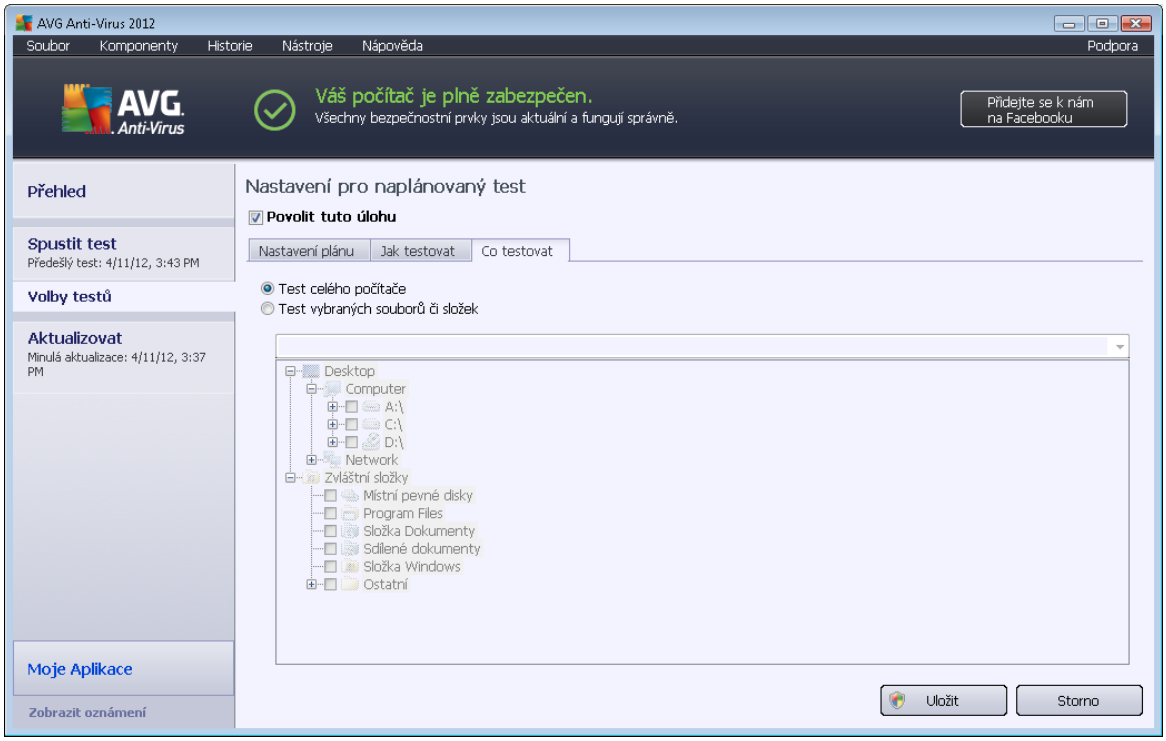
Ovládací tlačítka dialogu

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.

11.5.3. 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\

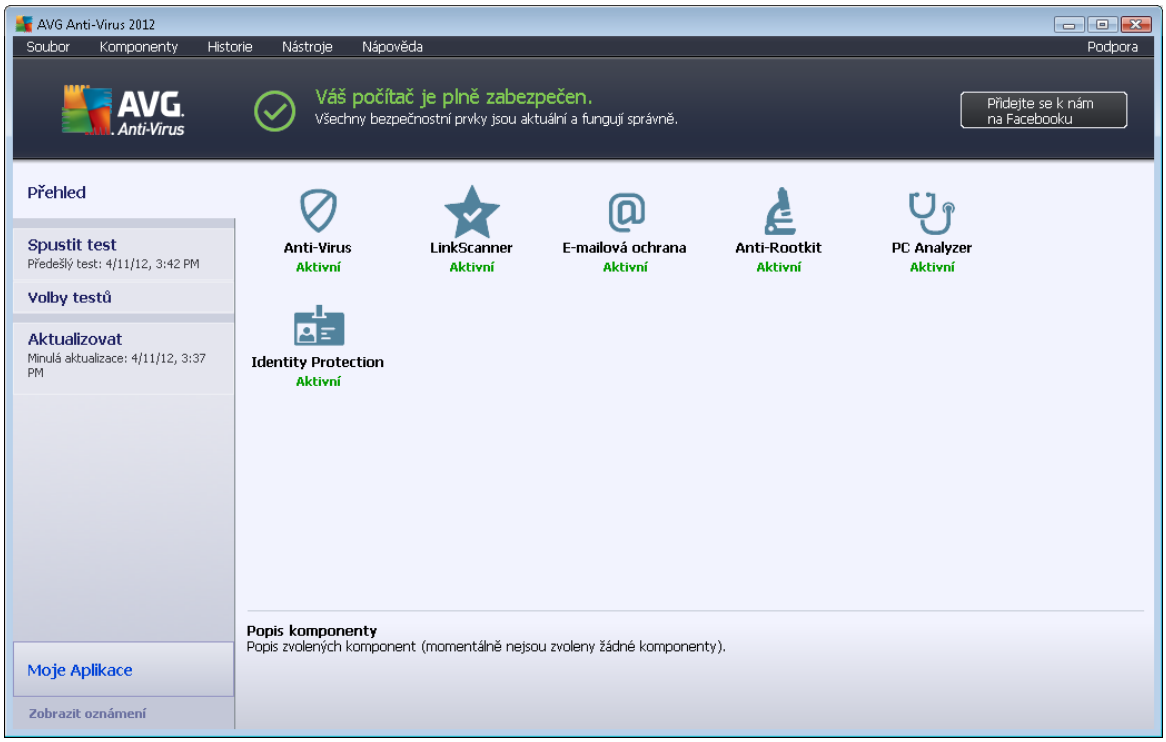
- ***Sdílené dokumenty***
  - *pro Win XP:* C:\Documents and Settings\All Users\Documents\
  - *pro Windows Vista/7*: C:\Users\Public\Documents\
- ***Složka Windows*** - C:\Windows\
- ***Ostatní***
  - *Systémový disk* - pevný disk, na němž je instalován operační systém (*obvykle C:*)
  - *Systémová 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.

11.6. 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

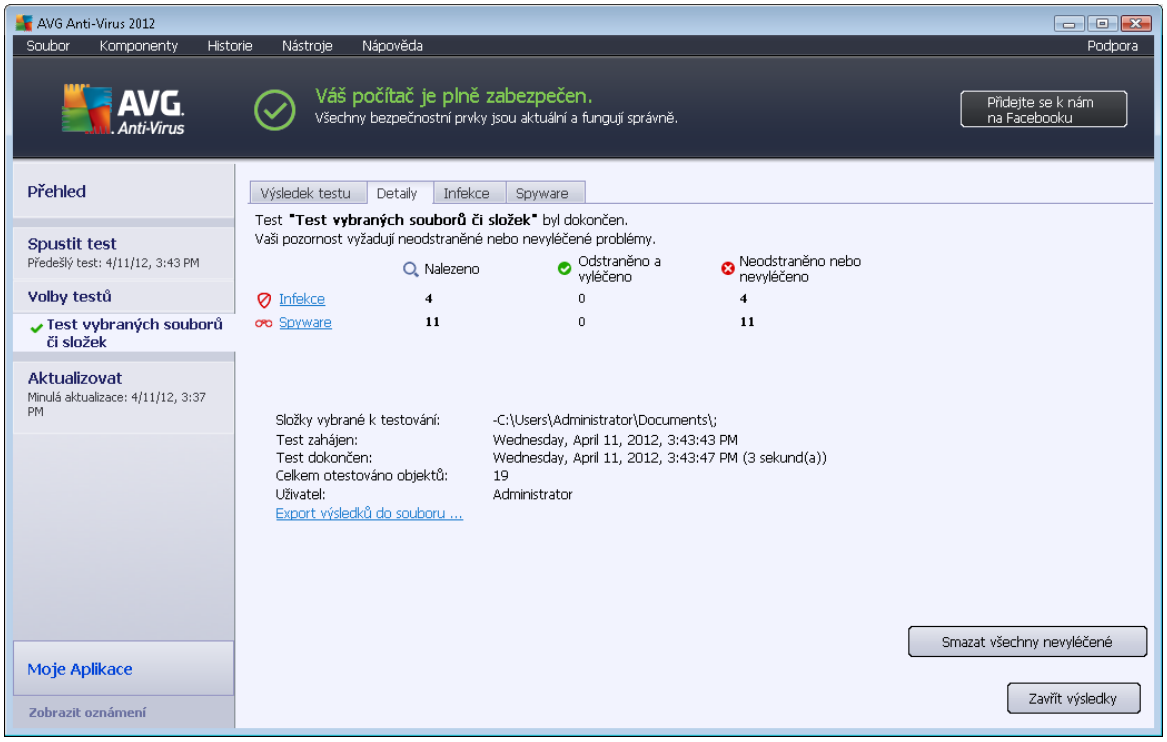
11.7. Detail výsledku testu

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*).

11.7.1. Záložka Přehled výsledků



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

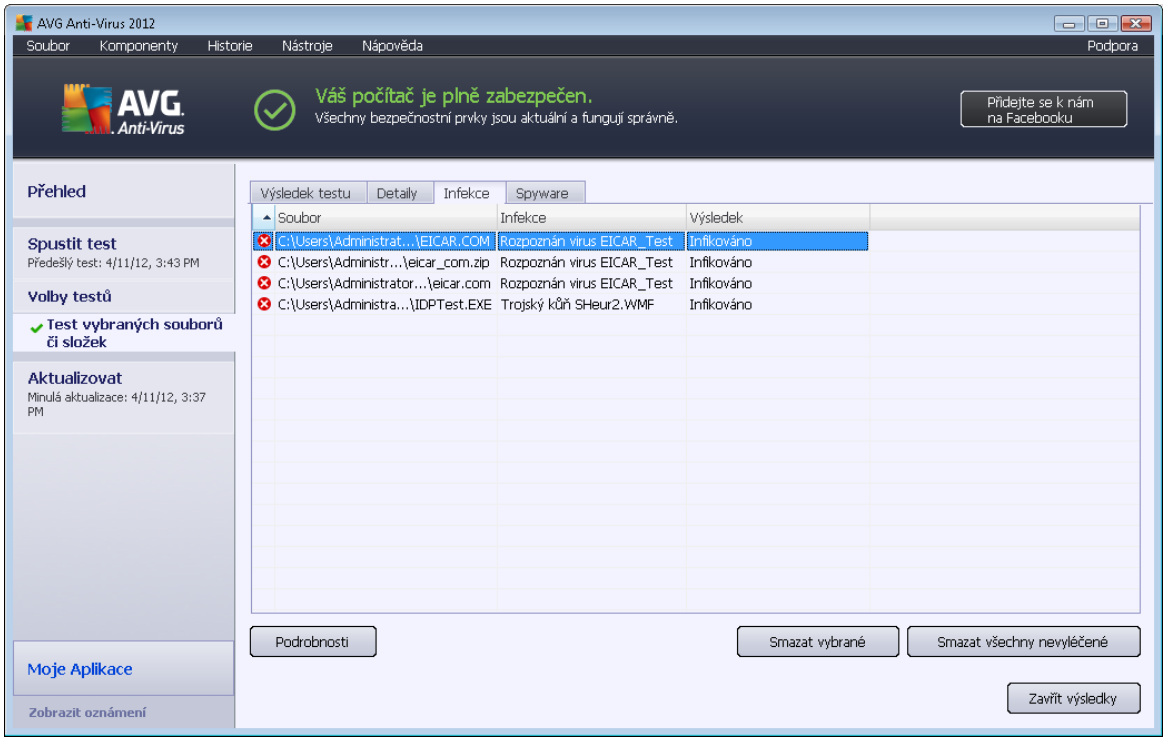
- detekovaných virových infekcích / spyware
- vyléčených virových infekcích / spyware
- počtu virových infekcích / spyware, které se nepodařilo odstranit nebo vyléčit

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.

11.7.2. 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
    - ***Přidáno k výjimkám PUP*** - nález byl vyhodnocen jako výjimka a připojen k seznamu výjimek PUP *(výjimky lze editovat v dialogu PUP výjimky pokročilého*

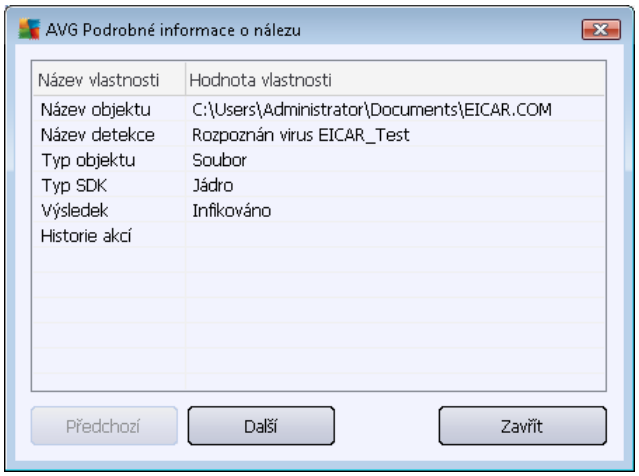
nastavení)

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

Ovládací tlačítka dialogu

V dialogu jsou dostupná tato tlačítka:

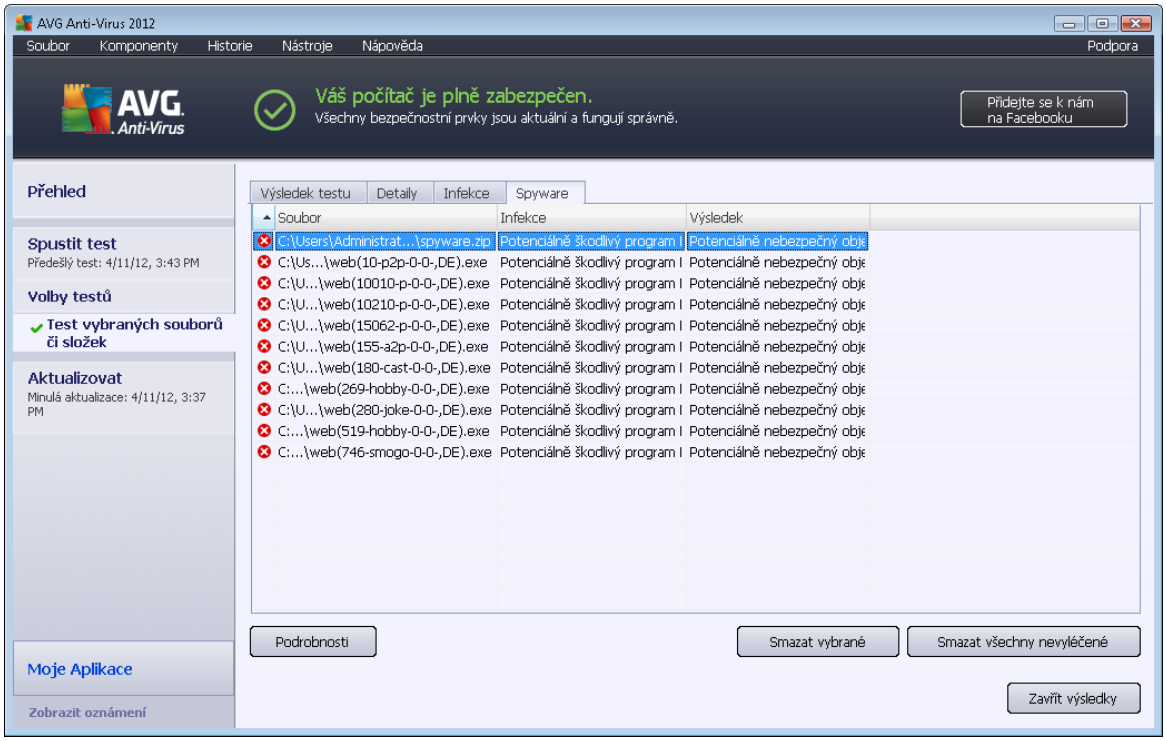
- **Podrobnosti** - tlačítko otevírá nové dialogové okno **Podrobné informace o nálezu**:



  V tomto dialogu najdete detailní informace o infekci (*například umístění a jméno detekovaného infikovaného objektu, typ objektu, typ SDK, výsledek detekce a historii akcí provedených nad detekovaným objektem*). Pomocí tlačítek **Předchozí** / **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

11.7.3. Záložka Spyware



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

- ***Soubor*** - plná adresa původního umístění infikovaného objektu na lokálním disku
- ***Infekce*** - jméno detekovaného spyware *(podrobnosti o jednotlivých virech najdete ve Virové encyklopedii online)*
- ***Výsledek*** - uvádí, v jakém stavu se infikovaný a během testu detekovaný objekt aktuálně nachází:
    - ***Infikováno*** - infikovaný objekt byl rozpoznán a zůstává ve svém původním umístění (například pokud máte v nastavení konkrétního testu vypnutou možnost automatického léčení)
    - ***Vyléčeno*** - infikovaný objekt byl automaticky vyléčen a ponechán ve svém původním umístění
    - ***Přesunuto do trezoru*** - infikovaný objekt byl přesunut do bezpečného prostoru Virového trezoru
    - ***Smazáno*** - infikovaný objekt byl smazán
    - ***Obnoveno*** - objekt byl obnoven z Virového trezoru zpět do původního umístění

- 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

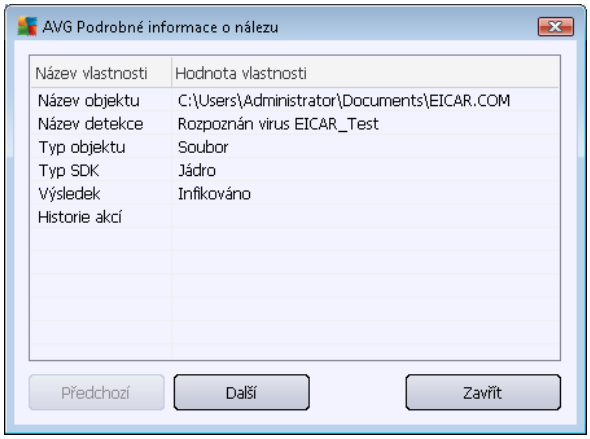
- o ***Potenciálně nebezpečný objekt*** - objekt je detekován jako potenciálně nebezpečný, ale nikoli infikovaný *(může například obsahovat makra)*. Informace má tedy pouze charakter upozornění.

- 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

11.7.4. 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 testu zobrazuje **AVG Anti-Virus 2012** 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 Anti-Virus 2012** 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.

11.7.5. Záložka Rootkity

Záložka ***Rootkity*** se objeví ve výsledcích testu pouze v případě, že byl během Testu celého počítače ve vašem počítači detekován 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.

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

11.7.6. 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 kompres***e: 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 Anti-Virus 2012** (*ani jiným bezpečnostním programem*) zkontrolovány, proto jsou označeny jako potenciálně nebezpečné.

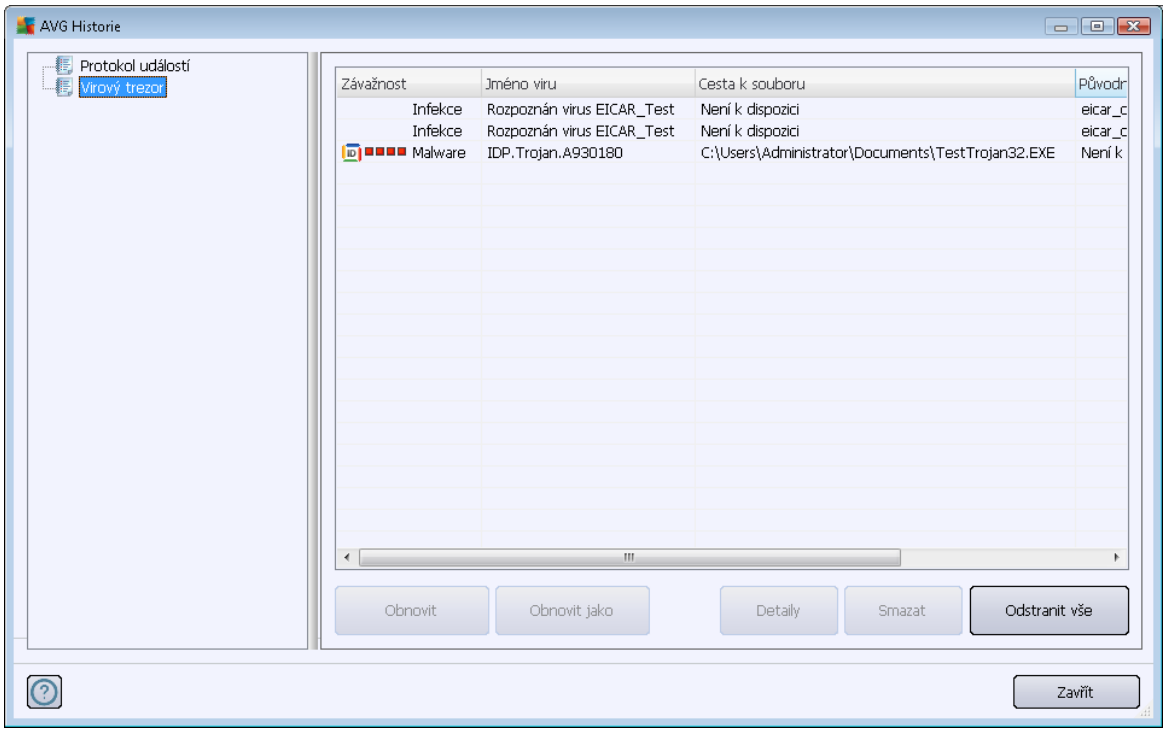
- ***Dokument s makry***: Detekovaný dokument může obsahovat škodlivé makro.

- ***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 Anti-Virus 2012** 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 Anti-Virus 2012** 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 Anti-Virus 2012**. Tato informace ve výsledku testů znamená, že soubor je permanentně používán systémem (*např. stránkovací soubor*).

11.8. 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*** - jestliže jste si v rámci instalace programu **AVG Anti-Virus 2012** nainstalovali také komponentu Identity Protection, najdete v tomto sloupci grafické znázornění závažnosti infekce přesunuté do karantény na čtyřstupňové škále v rozpětí nezávadný (□□□□) až vysoce rizikový (■■■■); zároveň je zde uvedena informace o typu nálezu (*rozlišuje typy nálezů podle úrovně jejich infekčnosti - objekty mohou být pozitivně/potenciálně infikované*)

- ***Jméno viru*** - uvádí název detekované infekce viru podle Virové encyklopedie (*on-line*)

- ***Cesta k souboru*** - plná cesta k původnímu umístění souboru, který byl detekován jako infikovaný, na lokálním disku

- ***Původní název objektu*** - všechny detekované objekty v tabulce jsou uvedeny pod standardním jménem, kterým byly označeny během detekce při testování. Pokud měl detekovaný objekt své původní specifické jméno a toto jméno je známo, bude uvedeno v tomto sloupci (*například příloha emailu může být označena jménem, které neodpovídá skutečnému detekovanému infekčnímu obsahu, pak budou uvedena obě jména*).

- ***Datum uložení*** - datum a čas detekce infikovaného souboru a jeho přesunutí do ***Virového trezoru***

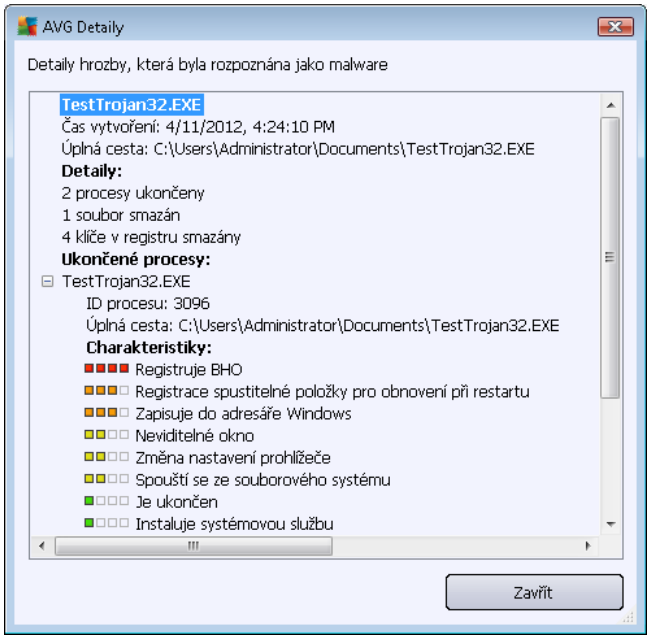
Ovládací tlačítka dialogu

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

- ***Obnovit*** - přesune infikovaný soubor z ***Virového trezoru*** zpět do původního umístění

- ***Obnovit jako*** - pokud se rozhodnete detekovanou infekci z ***Virového trezoru*** umístit do zvolené složky, použijte toto tlačítko. Podezřelý a detekovaný objekt bude uložen pod svým původním jménem, a pokud toto není známo, bude uložen pod standardním jménem, kterým byl označen při detekci.

- ***Detaily*** - toto tlačítko se týká pouze objektů nalezených komponentou Identity Protection. Po kliknutí se zobrazí přehled detailních informací o této hrozbě (*které soubory/procesy byly dotčeny a jak, charakteristika procesu atd.*). U jiných objektů než detekcí IDP je toto tlačítko neaktivní!



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

12. Aktualizace AVG

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.

Vzhledem k tomu, jak rychle se dnes šíří nově vzniklé počítačové hrozby, je nezbytně nutné Váš **AVG Anti-Virus 2012** pravidelně aktualizovat. V ideálním případě ponechte prosím program ve výchozím nastavení, kdy je zapnuta automatická aktualizace. Bez aktuální virové databáze nebude **AVG Anti-Virus 2012** schopen zachytit nejnovější viry!

Je naprosto klíčové pravidelně aktualizovat AVG! Aktualizace definic by měla být naplánována minimálně jednou denně. Méně kritické programové aktualizace mohou být naplánovány jednou týdně.

12.1. Spouštění aktualizace

Pro zajištění maximální bezpečnosti ověřuje **AVG Anti-Virus 2012** ve výchozím aktualizaci definic každé čtyři hodiny. Vzhledem k tomu že aktualizace AVG nejsou vydávány podle pevného plánu, ale v reakci na počet a závažnost nových hrozeb, je tato kontrola nezbytná a zajistí, že Váš **AVG Anti-Virus 2012** bude aktuální během celého dne.

Pokud si přejete omezit počet výskytů kontroly aktualizace, máte možnost nastavit vlastní parametry spouštění aktualizace. V každém případě však doporučujeme, abyste aktualizaci spouštěli nejméně jednou děnně! Nastavení lze editovat v sekci Pokročilé nastavení/Naplánované úlohy, konkrétně v dialozích:

- Plán aktualizace definic
- Plán programové aktualizace

V případě, že si přejete ověřit existenci nových aktualizačních souborů okamžitě, použijte tlačítko Aktualizovat dostupné v hlavním dialogu aplikace. Toto tlačítko je vždy dostupné z kteréhokoliv dialogu uživatelského rozhraní AVG.

12.2. Průběh aktualizace

Po spuštění aktualizace dojde nejprve k ověření, zda existují nové aktualizační soubory, jež dosud nebyly aplikovány. Pokud ano, **AVG Anti-Virus 2012** zahájí jejich okamžité stahování a spustí samotný proces aktualizace. V průběhu tohoto procesu budete přepnuti do dialogu ***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 zálohy systému (tzv. system restore point). V případě selhání procesu aktualizace a pádu systému lze z této zálohy obnovit váš operační systém v původní konfiguraci. Tato možnost je dostupná přímo v operačním systému, a to z nabídky Start / Programy / Příslušenství / Systémové nástroje / Obnova systému. Doporučujeme pouze zkušeným uživatelům!*

12.3. Úrovně aktualizace

AVG Anti-Virus 2012 rozlišuje dvě úrovně aktualizace:

- ***Aktualizace definic*** zajišťuje, že jste chráněni proti nejnovějším hrozbám, které by mohly poškodit Váš počítač. Zahrnuje pouze změny nezbytné pro spolehlivé fungování antivirové ochrany. 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.

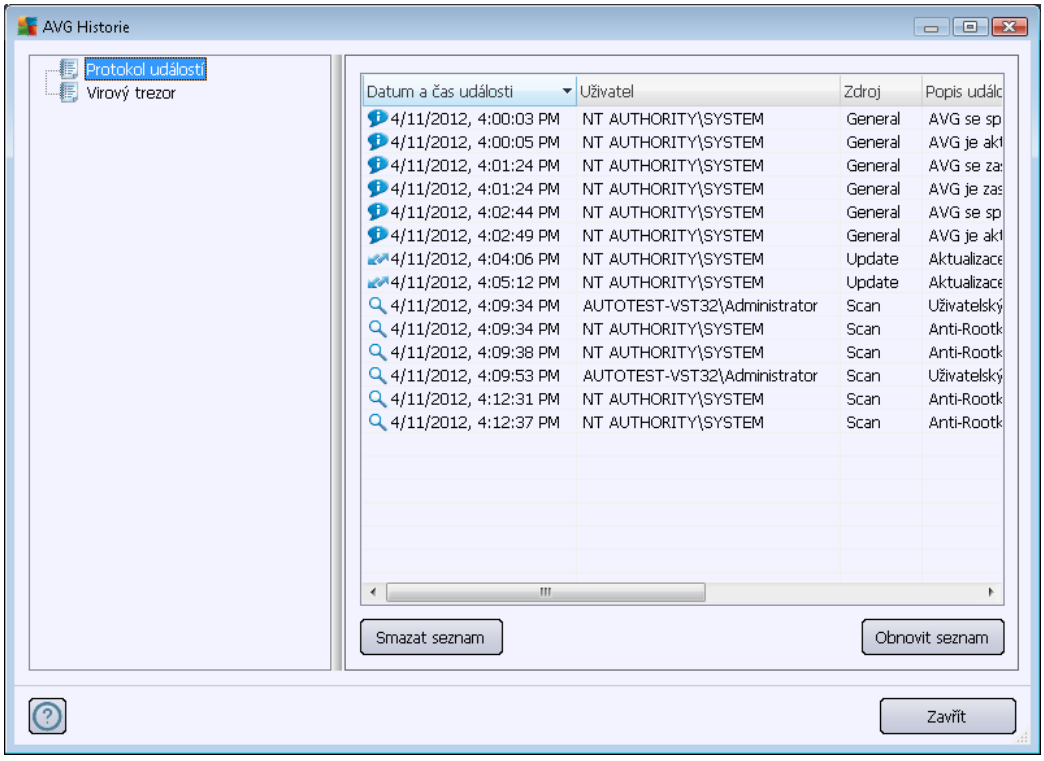
Při nastavování plánu aktualizací je možné definovat požadavky na spouštění obou úrovní aktualizace:

- Plán aktualizace definic

- Plán programové aktualizace

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

13. 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 Anti-Virus 2012**. Zaznamenávány jsou různé typy událostí, například:

- informace o aktualizacích programu
- informace o spuštění/ukončení/přerušení testů (*včetně testů spouštěných automaticky*)
- informace o událostech týkající se nalezení viru (*při testování či rezidentním štítem*) s uvedením konkrétního místa nálezu
- informace o ostatních důležitých událostech

Ké každé události jsou evidovány následující údaje:

- ***Datum a čas události*** udává přesný datum a čas, kdy se událost odehrála
- ***Uživatel*** uvádí jméno uživatele, který byl aktuálně přihlášen v době, kdy k události došlo
- ***Zdroj*** zobrazuje informaci o zdrojové komponentě či jiné části AVG, která událost spustila
- ***Popis události*** obsahuje stručný popis události

Ovládací tlačítka dialogu

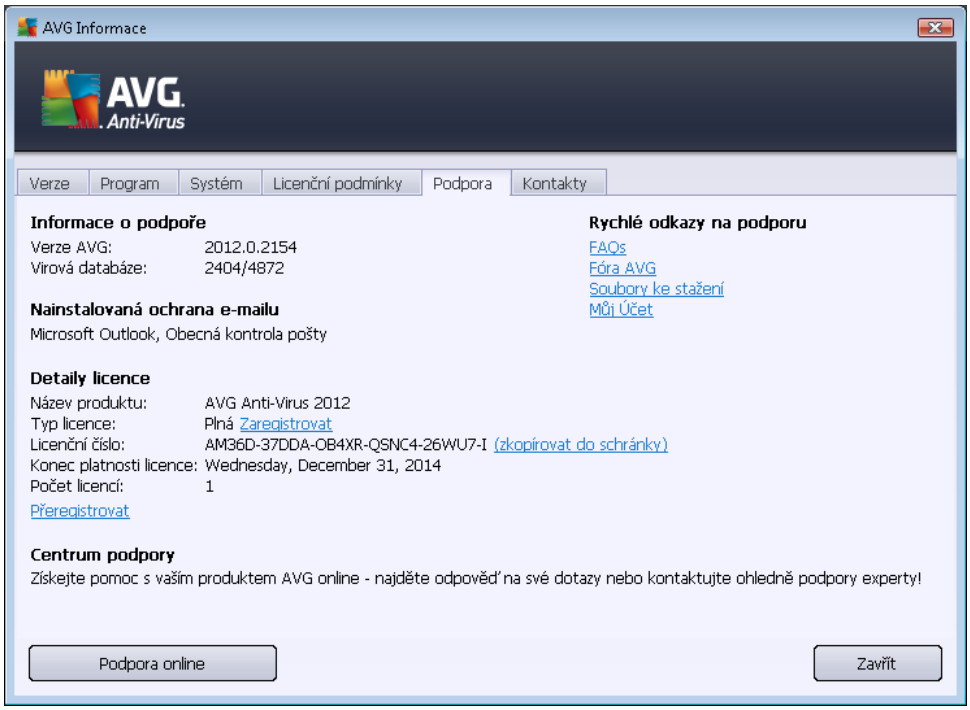
- ***Smazat seznam*** - stiskem tlačítka můžete vymazat veškeré protokolované záznamy ze seznamu událostí
- ***Obnovit seznam*** - stiskem tlačítka provedete aktualizaci záznamů v seznamu událostí

14. FAQ a technická podpora

Máte-li s Vaší aplikací **AVG Anti-Virus 2012** jakékoliv technické potíže nebo chcete-li položit obchodní dotaz, existuje několik způsobů, jak vyhledat pomoc. Zvolte si prosím některou z následujících možností:

- ***Podpora na webu***: Přímo z prostředí aplikace AVG můžete přejít do specifické sekce webu AVG (http://www.avg.cz/), která je vyhrazena zákaznické podpoře. V hlavním menu zvolte položku ***Nápověda / Získat podporu***. Budete automaticky přesměrováni na příslušnou stránku s nabídkou dostupné podpory. Dále prosím postupujte podle pokynů uvedených na webu.

- ***Podpora (v hlavním menu)***: Systémové menu aplikace AVG *(v horní liště hlavního dialogu)* obsahuje položku ***Podpora***. Ta otevírá nový dialog s kompletním výčtem informací, které můžete potřebovat při kontaktu se zákaznickou podporou. Dialog dále obsahuje základní údaje o instalovaném programu AVG (*verzi programu a databáze*), licenční údaje a seznam odkazů na zdroje podpory:



- ***Řešení potíží v nápovědě***: Přímo v nápovědě programu **AVG Anti-Virus 2012** je nově k dispozici sekce ***Řešení potíží*** *(soubor nápevědy lze otevřít z kteréhokoliv dialogu aplikace stiskem klávesy F1)*. Ta nabízí výčet nejčastějších situací technického rázu, v nichž si uživatel přeje vyhledat odbornou pomoc. Zvolte prosím položku, která nejlépe vystihuje Váš aktuální problém a po rozkliknutí se otevře návod s podobným postupem doporučovaným pro tuto situaci.

- ***Centrum podpory na webu AVG***: Alternativní možností je vyhledat řešení svého problému na webu AVG (http://www.avg.cz/). V sekci ***Centrum podpory*** najdete strukturovaný přehled tematických okruhů, které řeší problémy obchodního i technického charakteru.

- ***Často kladené otázky***: Na webu AVG (http://www.avg.cz/) najdete také samostanou a detailně členěnou sekci často kladených otázek. Tato sekce je dostupná volbou ***Centrum podpory / FAQ***. Otázky jsou opět přehledně rozděleny do kategorií obchodní, technické a virové.

- ***Informace o virech a hrozbách***: Samostatná kapitola je na webu AVG (http://www.avg.cz/) věnována virové tematice *(webová stránka je dostupná prostřednictvím volby Nápověda / Informace o virech v hlavním menu)*. Volbou ***Centrum podpory / Informace o virech a hrozbách*** vstoupíte na stránku, která poskytuje stukturovaný přehled informací souvisejících s hrozbami online. Najdete zde také rady, jak odstranit viry, spyware a jak zůstat trvale chráněni.

- ***Diskusní fórum***: Můžete také využít diskusního fóra pro uživatele AVG produktů na adrese http://forums.avg.com.