AVG AntiVirus Free Edition

Uživatelský manuál

Verze dokumentace AVG.07 (26.11.2015)

Obsah

1. Úvod

Tento uživatelský manuál nabízí přehled úloh a detekčních technologií poskytovaných **AVG AntiVirus Free Edition**.

Aplikace **AVG AntiVirus Free Edition** poskytuje v reálném čase ochranu před současnými nejpokročilejšími hrozbami. Můžete chatovat, posílat zprávy, stahovat a zasílat soubory zcela bez obav. Užívejte si při hraní her či sledování videa. Bez starostí se můžete pohybovat v sociálních sítích či procházet Internet a vyhledávat potřebné informace.

AVG AntiVirus Free Edition je dostupný zdarma a jeho funkčnost je omezená. Pokud během používání AVG AntiVirus Free Edition zjistíte, že byste dali přednost plné funkčnosti profesionální verze AVG, navštivte prosím web AVG (http://www.avg.cz/), kde najdete informace o možnostech koupě placených produktů AVG.

Kromě dokumentace můžete také využít dalších dostupných zdrojů informací o **AVG AntiVirus Free Edition**:

- ***Nápověda***: Přímo v nápovědě programu **AVG AntiVirus Free Edition** je nově k dispozici sekce ***Řešení potíží***. 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 podrobným 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 ***Podpora*** najdete přehled tematických okruhů, které řeší problémy obchodního i technického charakteru, sekci často kladených otázek i veškeré potřebné kontakty.

- ***AVG ThreatLabs***: Samostatná AVG stránka (*http://www.avg.com/about-viruses*) je věnována virové tematice a poskytuje strukturovaný přehled informací souvisejících s hrozbami online. Najdete zde také rady, jak odstranit viry, spyware a jak zůstat trvale chráněni.

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

2. Podmínky instalace AVG

2.1. Podporované operační systémy

AVG AntiVirus Free Edition 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 (všechny edice)
- Windows 7 (všechny edice)
- Windows 8 (všechny edice)
- Windows 10 (všechny edice)

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

***Poznámka**: Komponenta Identity Protection není podporována na Windows XP x64. Na tomto operačním systému lze nainstalovat AVG AntiVirus Free Edition, ale pouze bez této komponenty.*

2.2. Minimální / doporučené požadavky na hardware

Minimální hardwarové požadavky pro **AVG AntiVirus Free Edition** jsou tyto:

- Procesor Intel Pentium 1,5 GHz nebo rychlejší
- 1,2 GB volného místa na pevném disku, z instalačních důvodů
- 512 MB RAM paměti (Windows XP) / 1024 MB RAM paměti (Windows Vista, Windows 7)

Doporučené hardwarové požadavky pro **AVG AntiVirus Free Edition** jsou tyto:

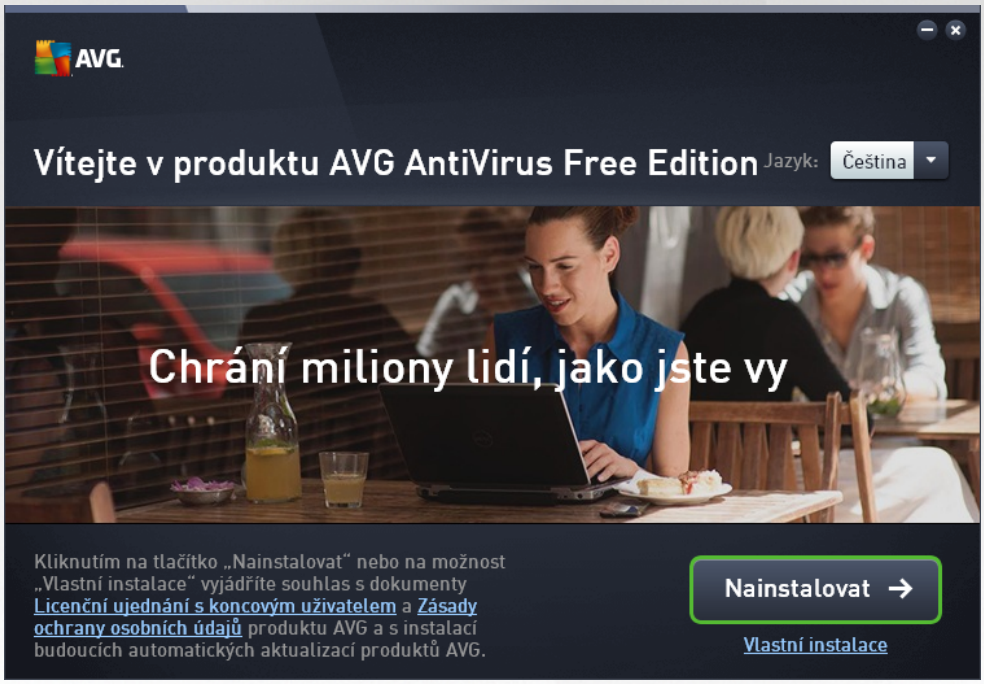
- Procesor Intel Pentium 1,8 GHz nebo rychlejší
- 1,5 GB volného místa na pevném disku, z instalačních důvodů
- 1024 MB RAM paměti

3. Instalační proces AVG

Pro instalaci **AVG AntiVirus Free Edition** na váš počítač potřebujete aktuální instalační soubor. Abyste zajistili, že instalujete vždy nejnovější verzi **AVG AntiVirus Free Edition**, je vhodné stáhnout si instalační soubor z webu AVG (http://free.avg.com/cz-cs/uvod/). 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!

Instalační proces je zahájen otevřením dialogu ***Vítejte v produktu AVG AntiVirus Free Edition***:



Volba jazyka

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. Také aplikace bude komunikovat v jazyce podle vaší volby. Budete však mít možnost kdykoliv přepnout do angličtiny, která se instaluje automaticky.

Licenční ujednání s koncovýcm uživatelem a Zásady ochrany osobních údajů

Dříve než postoupíte k dalšímu kroku instalace, doporučujeme vám seznámit se s ***Licenčním ujednáním s koncovým uživatelem*** a se ***Zásadami ochrany osobních údajů***. Oba dokumenty jsou k dipozici formou aktivního odkazu uvedeného v textu ve spodní části dialogu. Kliknutím na každý z odkazů se otevře nový dialog / nové okno prohlížeče s plným zněním smlouvy. Prosím, přečtěte si pečlivě celý text těchto právně závazných dokumentů a svůj souhlas s nimi potvrdíte stiskem tlačítka ***Nainstalovat***.

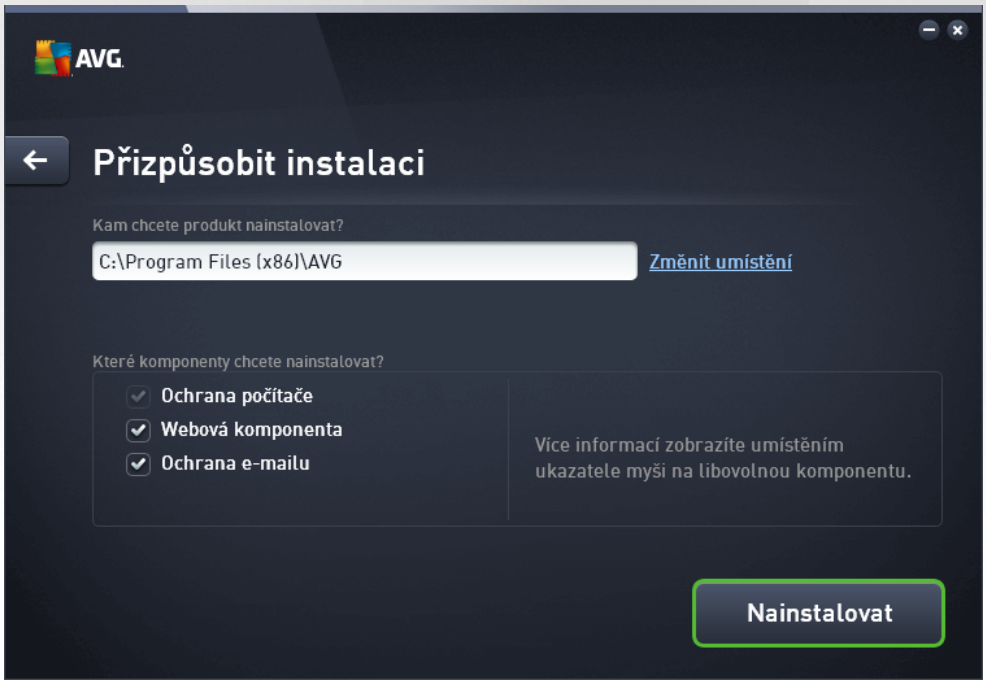
Pokračovat v instalaci

Instalační proces lze snadno spustit tlačítkem ***Nainstalovat***. Instalační proces se spustí ve zcela automatickém režimu. Tuto možnost standardní instalace **AVG AntiVirus Free Edition** doporučujeme většině uživatelů. Aplikace bude nainstalována s konfigurací definovanou výrobcem. 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 přímo v aplikaci.

Alternativou je možnost ***Vlastní instalace***, kterou můžete spustit prostřednictvím aktivního linku umístěného pod tlačítkem ***Nainstalovat***. Vlastní instalace je vhodná pouze pro pokročilé a znalé uživatele. Doporučit ji lze v případě, že máte skutečný důvod instalovat aplikaci s nestandardním nastavením tak, aby vyhovovalo specifickým požadavkům vašeho systému. Pokud se rozhodnete pro tuto možnost, budete po vyplnění licenčního čísla přesměrováni do dialogu nazvaného ***Přizpůsobit instalaci***, kde můžete specifikovat své požadavky.

3.2. Přizpůsobit instalaci

Dialog ***Přizpůsobit instalaci*** vám umožňuje nastavit podrobné parametry instalace:



Kam chcete produkt nainstalovat?

Nyní máte možnost se rozhodnout, kam má být aplikace nainstalována. Adresa v textovém poli určuje standardní výchozí umístění instalace do adresáře Program Files. Pokud si přejete vybrat jiné umístění, klikněte na odkaz ***Změnit umístění***, kterým se otevře nové okno se stromovou strukturou vašeho disku. Zvolte příslušné umístění a svou volbu potvrďte.

Které komponenty chcete nainstalovat?

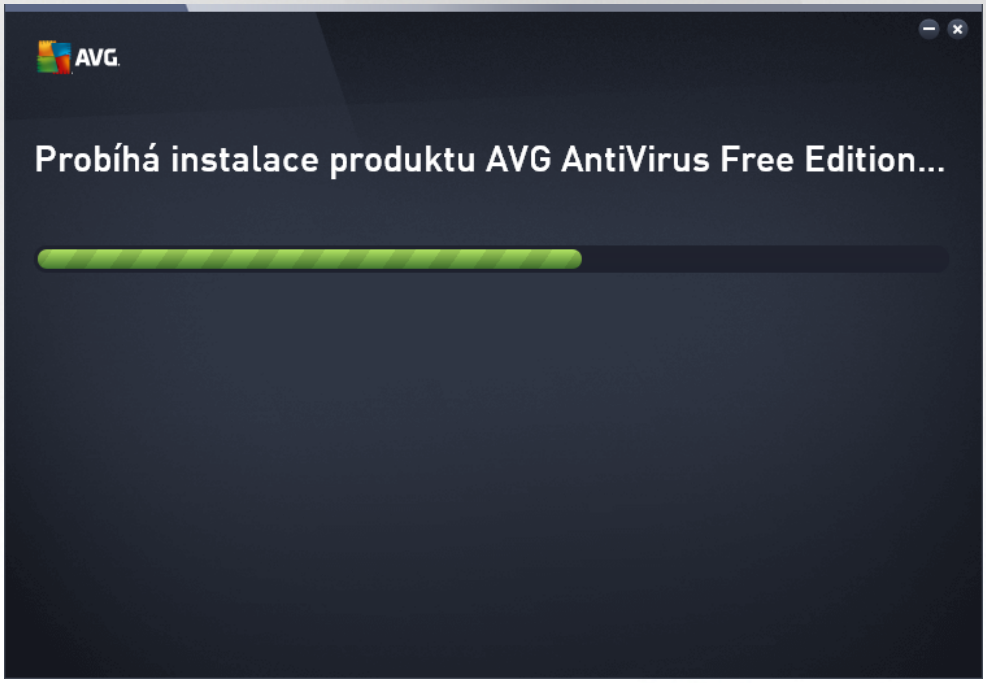
Tato sekce nabízí přehled komponent, které můžete nainstalovat. Pokud vám výchozí nastavení nevyhovuje, máte možnost jednotlivé komponenty odebrat. Volit můžete pouze z komponent, které jsou zahrnuty v AVG AntiVirus Free Edition a pouze tyto komponenty vám také budou v dialogu nabídnuty! Výjimkou je komponenta ***Ochrana počítače***, která je samotnou podstatou aplikaci a není možné ji z instalace vyjmout. Najedete-li myší nad kteroukoliv komponentu v seznamu, po pravé straně se zobrazí stručný popis funkčnosti této komponenty. Podrobné informace o jednotlivých komponentách najdete v kapitole Přehled komponent.

Pokračovat v instalaci

V instalaci lze pokračovat stiskem tlačítka ***Nainstalovat***. V případě, že se potřebujete vrátit k předchozímu dialogu s volbou jazyka instalace, použijte tlačítko s šipkou  v horní části dialogu.

3.3. Probíhá instalace AVG

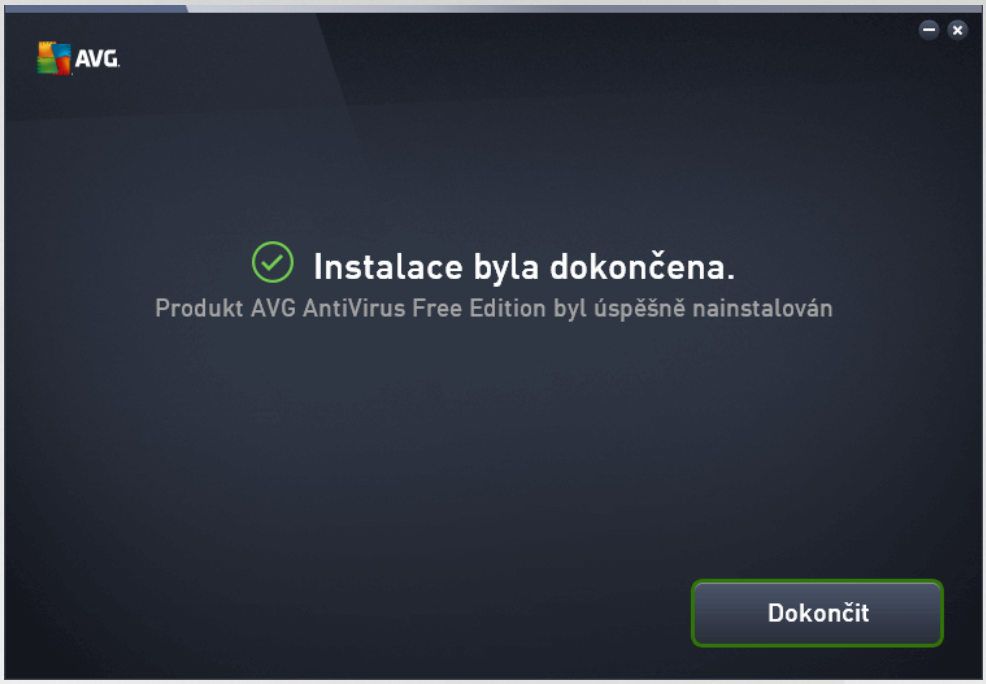
Potvrzením v předchozím dialogu jste spustili samotný proces instalace. Jeho průběh můžete nyní sledovat. Tento dialog je pouze informativní a nevyžaduje žádný váš zásah:



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

3.4. Instalace byla dokončena

Dialog ***Instalace byla dokončena*** potvrzuje, že AVG AntiVirus Free Edition byl plně nainstalován a nastaven k optimálnímu výkonu:



Stiskem tlačítka ***Dokončit*** instalační proces uzavřete.

4. Po instalaci

4.1. První aktualizace virové databáze

Bezprostředně po dokončení instalace *(a po restartu počítače, pokud je vyžadován)* **AVG AntiVirus Free Edition** automaticky aktualizuje svou virovou databázi i všechny komponenty a aktivuje je, což může pár minut trvat. O průběhu procesu aktualizace budete vyrozuměni textovým textovým hlášením v hlavním dialogu. Prosíme o chvíli strpení, než proběhne stažení aktualizačních souborů a samotný proces aktualizace **AVG AntiVirus Free Edition**, teprve poté bude aplikace plně připravena k vaší ochraně!

4.2. Registrace produktu

AVG AntiVirus Free Edition nevyžaduje nutně registraci programu. Registraci je však vhodné provést, pokud chcete využívat služeb diskusního fóra **AVG AntiVirus Free Edition**, respektive, chcete-li vznést vlastní dotaz nebo na jiný reagovat. Pro čtení je fórum dostupné i bez registrace. Nejsnazší přístup k registraci je přímo z prostředí aplikace **AVG AntiVirus Free Edition**, a to volbou položky Možnosti / Zaregistrovat AVG. Následně budete přesměrováni na registrační stránku AVG Free fóra, kde dále postupujte podle uvedených instrukcí. Po vyplnění registračního foírmuláře Vám na uvedenou adresu zašleme aktivační kód, s nímž se do fóra přihlásíte.

4.3. Otevření uživatelského rozhraní

Hlavní dialog **AVG AntiVirus Free Edition** je dostupný několika cestami:

- dvojklikem na ikonu AVG AntiVirus Free Edition na systémové liště
- dvojklikem na ikonu AVG Protection na ploše
- z nabídky *Start / Všechny programy / AVG / AVG Protection*

4.4. Spuštění testu celého počítače

Jelikož existuje jisté riziko, že virus byl na váš počítač zavlečen již před instalací **AVG AntiVirus Free Edition**, doporučujeme po instalaci spustit Test celého počítače, který zkontroluje celý počítač a ověří případnou přítomnost virů a potenciálně nežádoucích aplikací. 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.

4.5. Test virem Eicar

Chcete-li ověřit, že **AVG AntiVirus Free Edition** 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 **AVG AntiVirus Free Edition** varovným upozorněním. Toto upozornění

dokazuje, že **AVG AntiVirus Free Edition** na vašem počítači je správně nainstalován:

Pokud není testovací soubor EICAR identifikován jako virus, je nutné znovu prověřit konfiguraci **AVG AntiVirus Free Edition**!

4.6. Výchozí konfigurace AVG

Ve výchozí konfiguraci (*bezprostředně po instalaci*) jsou všechny komponenty a funkce **AVG AntiVirus Free Edition** 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.*** Pokud se domníváte, že je nutné konfiguraci AVG přenastavit podle vašich aktuálních potřeb, proveďte editaci parametrů v Pokročilém nastavení AVG: zvolte položku hlavního menu *Možnosti / Pokročilé nastavení* a editaci nastavení proveďte v nově otevřeném dialogu Pokročilém nastavení AVG.

5. Uživatelské rozhraní AVG

AVG AntiVirus Free Edition se otevře v tomto rozhraní:

Hlavní okno je rozděleno do několika sekcí:

- ***Horní navigace*** sestává ze čtyř aktivních odkazů uvedených v linii v horní části hlavního okna *(Líbí se mi AVG, Výsledky, Podpora, Možnosti)*. Podrobnosti >>
- ***Informace o stavu zabezpečení*** podává základní informaci o aktuálním stavu **AVG AntiVirus Free Edition**. Podrobnosti >>
- ***Přehled instalovaných komponent*** najdete ve vodorovném pásu ve střední části okna. Komponenty jsou znázorněny jako světle zelené bloky s ikonou příslušné komponenty a informací o jejím aktuálním stavu. Podrobnosti >>
- ***Moje aplikace*** jsou graficky znázorněny ve středním pásu hlavního okna a nabízejí přehled doplňkových aplikací **AVG AntiVirus Free Edition**, které buďto již máte nainstalovány na svém počítači, nebo jejichž instalaci vám doporučujeme. Podrobnosti >>
- ***Zkratková tlačítka pro testování, zlepšení výkonu a aktualizaci*** ve spodní řadě hlavního okna umožňují rychlý přístup k nejdůležitějším a nejčastěji používaným funkcím **AVG AntiVirus Free Edition**. Podrobnosti >>

Mimo hlavní okno **AVG AntiVirus Free Edition** můžete k aplikaci přistupovat ještě prostřednictvím následujícího prvku:

- ***Ikona na systémové liště*** se nachází v pravém dolním rohu monitoru *(na systémové liště)* a je indikátorem aktuálního stavu **AVG AntiVirus Free Edition**. Podrobnosti >>

5.1. Horní navigace

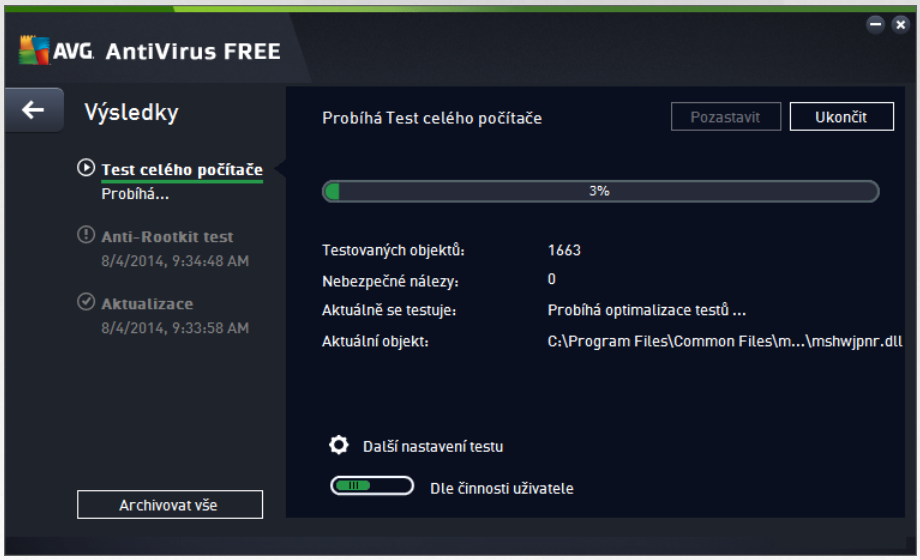
Horní navigace sestává z několika aktivních odkazů uvedených v linii v horní části hlavního okna. Obsahuje tato tlačítka:

5.1.1. Připojte se k nám v síti Facebook

Prostřednictvím odkazu se jediným kliknutím můžete připojit k AVG komunitě na Facebooku a sdílet nejnovější informace, novinky, tipy a triky pro vaši naprostou bezpečnost.

5.1.2. Výsledky

Otevírá samostatný dialog ***Výsledky***, v němž najdete přehled všech relevantních hlášení o průběhu a výsledcích spuštěných testů a aktualizací. Pokud test nebo proces aktualizace právě běží, zobrazí se v hlavním uživatelském rozhraní vedle položky ***Výsledky*** rotující kolečko. Kliknutím na něj se můžete kdykoliv přepnout do dialogu se zobrazením probíhajícího procesu.



5.1.3. Podpora

Odkaz otevírá samostaný dialog, v němž jsou na čtyřech záložkách shrnuty informace o **AVG AntiVirus Free Edition** potřebné například při kontaktu se zákaznickou podporou:

- ***Licence a podpora*** - Záložka nabízí přehled licenčních informací, tedy název produktu, licenční číslo a konec platnosti licence. Ve spodní části dialogu najdete také přehledný seznam všech dostupných kontaktů uživatelské podpory. V dialogu jsou k dispozici tyto ovládací prvky:
    - *(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 AntiVirus Free Edition instalovali)*, nebo kterým změníte dosavadní licenční číslo za jiné *(např. při přechodu na jiný produkt z řady AVG)*.
    - *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.

- *Zakoupit* - Zakoupit plnou profesionální licenci z nabídky produktů AVG můžete na webu AVG *(http://www.avg.cz/)*, kde najdete podrobné informace o jednotlivých nabízených programech.

- ***Produkt*** - Záložka podává přehled nejdůležitějších technických informací o **AVG AntiVirus Free Edition** rozdělených do sekcí informace o produktu, instalované komponenty a nainstalovaná ochrana e-mailu.

- ***Program*** - Na záložce najdete detailní technické informace o instalovaném **AVG AntiVirus Free Edition**: číslo verze produktu a seznam všech souvisejících produktů i s číslem jejich verze. V dalších dvou sekcích záložky je pak k dispozici přehled všech instalovaných komponent a rovněž seznam verzí použitých databází.

- ***Licenční ujednání*** - Na záložce najdete plné znění licenčního smlouvy mezi Vámi a společností AVG Technologies.

5.1.4. Možnosti

Ovládání vašeho **AVG AntiVirus Free Edition** je dostupné prostřednictvím jednotlivých možností sdružených v položce ***Možnosti***. Kliknutím na šipku vedle této položky otevřete rozbalovací menu s následující nabídkou:

- ***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.

- ***Aktualizace*** - Automaticky spouští proces aktualizace **AVG AntiVirus Free Edition**.

- ***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.

- ***Virový trezor*** - Otevírá rozhraní karanténního prostoru, Virového trezoru, kam jsou přesouvány detekované infekční soubory. V tomto prostoru jsou soubory zcela izolovány a tím je zajištěna naprostá bezpečnost vašeho počítače, a současně zde lze hrozby uložit pro případnou další práci s nimi.

- ***Historie*** se dělí na další specifické podkategorie:

  - *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.

  - *Nález Identity Protection* - Otevírá dialog s přehledem detekcí komponenty Identity Protection.

  - *Nálezy E-mailové ochrany* - Otevírá dialog s přehledem příloh detekovaných jako nebezpečné

komponentou Ochrana e-mailu.

- *Protokol událostí* - Otevírá dialog historie událostí s přehledem všech protokolovaných akcí **AVG AntiVirus Free Edition**.

- ***Pokročilé nastavení ...*** - Otevírá dialog pokročilého nastavení AVG, kde máte možnost editovat konfiguraci **AVG AntiVirus Free Edition**. Obecně doporučujeme podržet výchozí výrobcem definované nastavení aplikace.

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

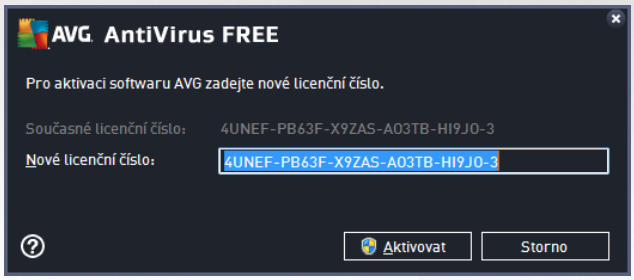
- ***Získat podporu*** - Otevírá dedikovaný dialog s přehledem všech dostupných informací a kontaktů zákaznické podpory.

- ***AVG na webu*** - Otevírá web **AVG AntiVirus Free Edition** *(http://free.avg.com/cz-cs/uvod/)*.

- ***Informace o virech*** - Otevírá web **AVG AntiVirus Free Edition** *(http://free.avg.com/cz-cs/uvod/)* na stránce věnované podrobným informacím o virech a hrozbách, kde lze dohledat podrobné informace o detekovaných nálezech.

- ***Zakoupit*** - Otevírá web AVG *(http://www.avg.cz/)* s možností online zakoupení plné verze programu AVG.

- ***Aktivovat*** - Otevírá aktivační dialog, v němž jsou již předem vyplněna data zadaná během instalačního procesu. V tomto dialogu můžete zadat své nové licenční číslo (*například při přechodu na placený produkt z řady AVG*), jímž nahradíte číslo odpovídající volné licenci AVG Free:



- ***Zaregistrovat AVG AntiVirus Free Edition*** / ***MyAccount*** - Otevírá web **AVG AntiVirus Free Edition** *(http://free.avg.com/cz-cs/uvod/)* na registračním formuláři. Vyplněním registračního formuláře získáte plný přístup k online diskusnímu fóru, které je pro **AVG AntiVirus Free Edition** jediným zdrojem technické podpory.

- ***Prémiová podpora*** - Otevírá internetovou stránku centra podpory AVG, kde si můžete zvolit svůj produkt a nechat si zobrazit dostupné možnosti podpory.

- ***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. *(Tentýž dialog je k dispozici volbou položky Podpora v navigaci přímo v hlavním okně aplikace.)*

5.2. Informace o stavu zabezpečení

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

 Zelená ikona informuje, že program ***AVG AntiVirus Free Edition 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! Tato komponenta bude v základním uživatelském rozhraní zobrazena s varovným oranžovým pruhem.

Žlutá ikona se zobrazí rovněž v případě, kdy jste se z nějakého důvodu vědomě rozhodli ignorovat chybový stav komponenty. Volba ***Ignorovat chybový stav*** je dostupná volbou větve Ignorovat chybový stav v Pokročilém nastavení. 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. 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 AntiVirus Free Edition** vyžaduje restart počítače (***Restartovat nyní***). Věnujte prosím pozornost tomuto varování a počítač restartujte!

 Oranžová ikona ***informuje o kritickém stavu AVG AntiVirus Free Edition***! Některá z komponent je nefunkční a **AVG AntiVirus Free Edition** nemůže plně chránit váš počítač. Věnujte prosím okamžitou pozornost opravě tohoto problému!

V případě, kdy AVG AntiVirus Free Edition 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 AntiVirus Free Edition 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 AntiVirus Free Edition** hlásí jakýkoliv problém, zaměřte se na jeho řešení. Pokud ignorujete chybová hlášení **AVG AntiVirus Free Edition**, váš počítač je ohrožen!

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

5.3. Přehled komponent

Přehled instalovaných komponent najdete ve vodorovném pásu ve střední části okna. Komponenty jsou znázorněny jako světle zelené bloky s ikonou komponenty. Každá komponenta uvádí informaci o aktuálním stavu ochrany. Jestliže je komponenta v pořádku a plně funkční, je tato informace uvedena zeleným textem. Pokud je komponenta pozastavena, její funkčnost je omezena či se nachází v chybovém stavu, budete na tuto skutečnost upozorněni varovným textem v oranžovém poli. ***Prosím, věnujte pozornost konfiguraci komponenty, která není nastavena k plné aktivitě!***

Při přejezdu myší přes grafické znázornění komponenty se ve spodní části hlavního okna zobrazí krátký text. Ten vás seznámí se základní funkčností zvolené komponenty. Dále podává informaci o aktuálním stavu komponenty, případně upřesňuje, která služba v rámci dané komponenty není nastavena k optimálnímu výkonu.

Seznam instalovaných komponent

V rámci **AVG AntiVirus Free Edition** najdete v sekci ***Přehled komponent*** informace o těchto komponentách:

- ***Počítač*** - Komponenta detekuje na vašem počítači viry, spyware, červy, trojany, nežádoucí spustitelné soubory nebo knihovny a chrání vás před nimi. Podrobnosti >>
- ***Web*** - Chrání vás před webovými útoky v době, kdy surfujete na Internetu. Podrobnosti >>
- ***Identita*** - Tato komponenta nepřetržitě chrání vaše digitální data před novými a neznámými hrozbami na Internetu. Podrobnosti >>
- ***E-maily*** - Kontroluje všechny příchozí e-mailové zprávy a filtruje SPAM, blokuje viry, phishingové útoky a jiné hrozby. Podrobnosti >>
- ***Firewall*** - Řídí veškerou komunikaci na všech síťových portech, a tak vás chrání před nebezpečnými útoky a pokusy o vniknutí do vašeho počítače. *Komponenta Firewall není v této edici aktivována a je dostupná pouze v plné profesionální verzi. Pokud máte zájem o využití této služby a všech dalších ochranných prvků některé z profesionálních edic, navštivte prosím web AVG (http://www.avg.cz/), kde najdete informace o možnostech koupě placených produktů AVG.*

Dostupné akce

- ***Přejezdem myši nad ikonou komponenty*** tuto komponentu v přehledu vysvítíte a současně se ve spodní části hlavního dialogu zobrazí stručný popis funkce komponenty.
- ***Jednoduchým kliknutím na ikonu komponenty*** otevřete vlastní rozhraní komponenty s informací o jejím aktuálním stavu komponenty, přístupem k nastavení a k přehledu základních statistických dat.

5.4. Moje aplikace

V sekci ***Moje aplikace*** *(řádek zelených bloků pod sadou komponent)* najdete přehled doplňkových aplikací AVG, které buďto již máte nainstalovány na svém počítači, nebo jejichž instalaci vám doporučujeme. Grafické bloky znázorněné v této sekci se zobrazují podmínečně a mohou představovat některé z těchto aplikací:

- ***Mobile protection*** nabízí zabezpečení Vašeho mobilního telefonu *(smart phone)* proti virům a malware. Zároveň slouží jako ochrana proti zneužití Vašich osobních dat, pokud telefon ztratíte nebo Vám bude odcizen.
- ***PC Tuneup*** je pokročilým nástrojem pro detailní systémovou analýzu a optimalizaci, umožňující zrychlit a vylepšit výkon vašeho počítače.

Pro podrobné informace o konkrétní aplikaci uvedené v této sekci klikněte na blok příslušný této aplikaci. Budete přesměrováni na webovou stránku vyhrazenou té které aplikaci, odkud si můžete rovnou stáhnout příslušný instalační soubor.

5.5. Zkratková tlačítka pro testování a aktualizaci

Zkratková tlačítka pro testování a aktualizaci najdete ve spodním pásu hlavního dialogu **AVG AntiVirus Free Edition**. Tato tlačítka umožňují rychlý přístup k nejdůležitějším a nejčastěji používaným funkcím aplikace, tedy k zejména k testování a aktualizacím:

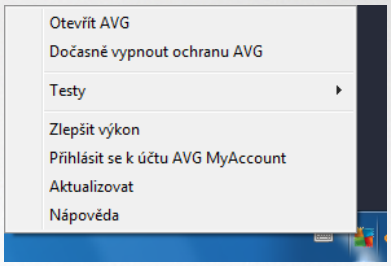
- ***Spustit test*** - Tlačítko je graficky rozděleno do dvou částí. Stiskem volby ***Spustit test*** dojde k okamžitému spuštění Testu celého počítače, o jehož průběhu a výsledku budete vyrozuměni v automaticky otevřeném okně Výsledky. Volbou položky ***Možnosti*** přejdete do dialogu ***Možnosti testu***, kde můžete spravovat naplánované testy a editovat parametry Testu celého počítače a Testu vybraných souborů či složek. *(Podrobné informace o testování najdete v kapitole AVG Testování)*

- ***Zlepšit výkon*** - Tlačítko otevírá prostředí služby ***PC Analyzer***, nástroje pro detailní systémovou analýzu a optimalizaci umožňující zrychlit a vylepšit výkon vašeho počítače.

- ***Aktualizovat*** - Stiskem tlačítka se automaticky spustí aktualizace produktu, o jejímž výsledku budete vyrozuměni v dialogu nad ikonou AVG na systémové liště. *(Podrobné informace o procesu aktualizace najdete v kapitole Aktualizace AVG)*

5.6. Ikona na systémové liště

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



Zobrazení systémové ikony AVG

- Jestliže je ikona zobrazena barevně bez dalších prvků, jsou všechny komponenty **AVG AntiVirus Free Edition** aktivní a plně funkční. Toto zobrazení ale také označuje situaci, kdy některá z komponent není v plně funkčním stavu, ale uživatel se rozhodl Ignorovat chybový stav. *(Volbou Ignorovat chybový stav 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 uživatelské rozhraní 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 AntiVirus Free**

Edition.

-  Alternativní zobrazení ikony s šipkou znamená, že právě běží některý z testů **AVG AntiVirus Free Edition**.

Informace systémové ikony AVG

Ikona AVG na systémové liště dále poskytuje informace o aktuálním dění v programu **AVG AntiVirus Free Edition**. Při změně stavu **AVG AntiVirus Free Edition** (*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

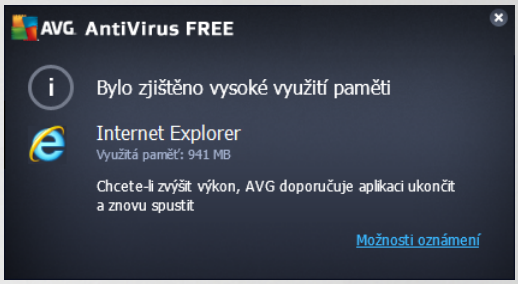
Ikonu AVG na systémové liště lze také použít pro rychlý přístup k uživatelské rozhraní aplikace **AVG AntiVirus Free Edition**, to se otevře dvojklikem na ikonu. Kliknutí pravým tlačítkem myši nad ikonou otevírá kontextové menu s těmito možnostmi:

- ***Otevřít AVG*** - Otevře uživatelské rozhraní aplikace **AVG AntiVirus Free Edition**.
- ***Dočasně vypnout ochranu AVG*** - Položka umožňuje jednorázově deaktivovat celou ochranu zajištěnou programem **AVG AntiVirus Free Edition**. 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 AntiVirus Free Edition** 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 AntiVirus Free Edition**, 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*, *Test vybraných souborů či složek* a *Anti-Rootkit test*) a následnou volbou požadovaný test přímo spustíte.
- ***Běžící testy*** - Tato položka se zobrazuje pouze tehdy, je-li aktuálně spuštěn některý test. U tohoto běžícího testu pak můžete nastavit jeho prioritu, případně test pozastavit nebo ukončit. K dispozici jsou dále možnosti *Nastavit prioritu pro všechny testy*, *Pozastavit všechny testy* a *Zastavit všechny testy*.
- ***Zlepšit výkon*** - Spustí komponentu PC Analyzer.
- ***Přihlásit se k účtu AVG MyAccount*** - Otevírá domovskou stránku Můj účet, kde můžete spravovat předplacené produkty, obnovit platnost AVG licence, zakoupit doplňující produkty, stáhnout instalační soubory, zkontrolovat uskutečněné objednávky a vystavené faktury či spravovat osobní udaje.
- ***Aktualizovat*** - Spustí okamžitou aktualizaci **AVG AntiVirus Free Edition**.
- ***Nápověda*** - Otevře soubor nápovědy na úvodní stránce.

5.7. 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 běžící 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.

6. Komponenty AVG

6.1. Ochrana počítače

Komponenta ***Ochrana počítače*** nabízí v rámci **AVG AntiVirus Free Edition** pouze službu ***AntiVirus***. Služba ***Datový sejf*** není v této edici aktivována a je dostupná pouze v plné profesionální verzi. Pokud máte zájem o využití této služby a všech dalších ochranných prvků některé z profesionálních edic, navštivte prosím web AVG *(http://www.avg.cz/)*, kde najdete informace o možnostech koupě placených produktů AVG.

- ***AntiVirus*** je tvořen jádrem, které testuje všechny soubory a jejich aktivitu, systémové oblasti počítače i vyměnitelná média *(flash disky apod.)* a prověřuje případnou přítomnost známých virů. Pokud detekuje virus, okamžitě zabrání, aby mohl být aktivován a následně jej odstraní nebo přesune do Virového trezoru. Tento proces bez ustání probíhá na pozadí a vy jej v podstatě nezaznamenáte - mluvíme o tak zvané rezidentní ochraně. AntiVirus také používá metodu heuristické analýzy, kdy 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. **AVG AntiVirus Free Edition** umí také analyzovat aplikace, 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.

- ***Datový sejf*** je službou, s jejíž pomocí můžete vytvořit bezpečné virtuální úložiště pro svá cenná a citlivá data. Obsah Datového sejfu je zašifrován a chráněn heslem, které si sami nastavíte, a vaše data jsou tedy zajištěna před neautorizovaným přístupem. *V produktu AVG AntiVirus Free Edition není služba Datový trezor bohužel automaticky zahrnuta. Pokud byste rádi využili i tohoto typu ochrany, navštivte prosím webovou stránku AVG (http://www.avg.cz/), kde najdete informace o možnostech přechodu na placené a plně profesionální produkty AVG.*

Ovládací prvky dialogu

Mezi oběma sekcemi v dialogu přecházíte pouhým kliknutím na panel příslušný té které službě; po kliknutí se panel vysvítí světlejším odstínem modré. V obou sekcích dialogu se můžete setkat s několika ovládacími prvky. Jejich funkčnost je stejná, ať přísluší jedné či druhé bezpečnostní službě *(AntiVirus či Datový sejf)*:

 ***Povoleno / Zakázáno*** - Tlačítko svým vzhledem i chováním připomíná semafor. Jednoduchým kliknutím se dá přepínat mezi dvěma polohami. Zelená barva odpovídá stavu ***Povoleno***, který znamená, že bezpečnostní služba AntiVirus je aktivní a plně funkční. Červená barva pak odpovídá stavu ***Zakázáno***, kdy je služby vypnuta. Pokud nemáte skutečný důvod službu vypínat, doporučujeme, abyste veškerou bezpečnostní konfiguraci ponechali ve výchozím stavu. Výchozí nastavení zajišťuje optimální výkon programu a vaši maximální bezpečnost. Jestliže z nějakého důvodu chcete službu dočasně vypnout, budete okamžitě upozorněni na možné nebezpečí červeným nápisem ***Varování*** a informací o skutečnosti, že v tuto chvíli nejste plně chráněni. ***Jakmile to bude možné, službu opět aktivujte!***

 ***Nastavení*** - Kliknutím na tlačítko přejdete do rozhraní pro pokročilé nastavení programu **AVG AntiVirus Free Edition**. Přesněji řečeno, budete nasměrováni do dialogu, v němž lze provést veškerou konfiguraci zvolené služby, v tomto případě služby AntiVirus. V prokročilém nastavení můžete editovat veškeré parametry jednotlivých bezpečnostních služeb **AVG AntiVirus Free Edition**, ale jakoukoliv konfiguraci doporučujeme pouze znalým uživatelům!

 ***Šipka*** - Pomocí šipky v levé horní části dialogu se vrátíte zpět do základního uživatelského rozhraní s přehledem komponent.

V produktu **AVG AntiVirus Free Edition** není služba ***Datový sejf*** bohužel automaticky zahrnuta. Pokud byste rádi využili i tohoto typu ochrany, navštivte prosím webovou stránku AVG (*http://www.avg.cz/*), kde najdete informace o možnostech přechodu na placené a plně profesionální produkty AVG.

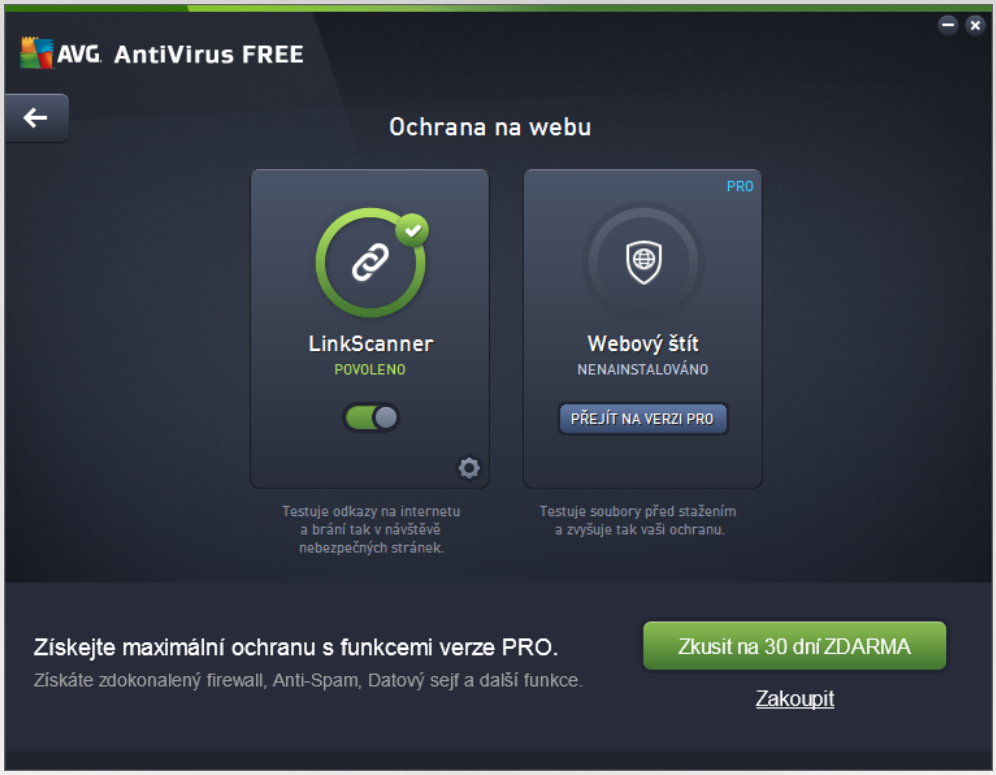
6.2. Ochrana na webu

Komponenta ***Ochrana na webu*** nabízí v rámci **AVG AntiVirus Free Edition** pouze službu ***LinkScanner***. Služba ***Webový štít*** není v této edici aktivována a je dostupná pouze v plné profesionální verzi. Pokud máte zájem o využití této služby a všech dalších ochranných prvků některé z profesionálních edic, navštivte prosím web AVG *(http://www.avg.cz/)*, kde najdete informace o možnostech koupě placených produktů AVG.

- ***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. Technologie LinkScanneru prověřuje obsah internetových stránek a zajišťuje, že jsou stránky bezpečné v okamžiku, kdy je to nejdůležitější, tedy když se chystáte otevřít adresu URL. Link Scanner 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, Link Scanner přístup k této stránce okamžitě zablokuje. Mějte na paměti, že váš počítač se může velmi snadno poškodit při pouhé návštěvě infikované webové stránky. ***LinkScanner není určen k ochraně serverů!***

- ***Webový štít*** *(v AVG AntiVirus Free Edition není služba dostupná)* je typ rezidentní ochrany, která běží na pozadí a v reálném čase kontroluje obsah webových stránek nebo souborů stahovaných z Internetu. Každá stránka je prověřena ještě předtím, než je skutečně stažena a zobrazena webovým

prohlížečem. Webový štít detekuje, že stránka, kterou se chystáte navštívit, obsahuje nebezpečný javascript, a v takovém případě nebude infikovaná stránka vůbec zobrazena. Také rozpozná, že stránka obsahuje malware, který by mohl být prohlížením stránky zavlečen na váš počítač, a zabrání jeho stažení. ***Webový štít není určen k ochraně serverů!***



Ovládací prvky dialogu

Mezi oběma sekcemi v dialogu přecházíte pouhým kliknutím na panel příslušný té které službě; po kliknutí se panel vysvítí světlejším odstínem modré. V obou sekcích dialogu se můžete setkat s několika ovládacími prvky. Jejich funkčnost je stejná, ať přísluší jedné či druhé bezpečnostní službě *(aktivní je však pouze služba Link Scanner)*:

Povoleno / Zakázáno - Tlačítko svým vzhledem i chováním připomíná semafor. Jednoduchým kliknutím se dá přepínat mezi dvěma polohami. Zelená barva odpovídá stavu ***Povoleno***, který znamená, že bezpečnostní služba je aktivní a plně funkční. Červená barva pak odpovídá stavu ***Zakázáno***, kdy je služby vypnuta. Pokud nemáte skutečný důvod službu vypínat, doporučujeme, abyste veškerou bezpečnostní konfiguraci ponechali ve výchozím stavu. Výchozí nastavení zajišťuje optimální výkon programu a vaši maximální bezpečnost. Jestliže z nějakého důvodu chcete službu dočasně vypnout, budete okamžitě upozorněni na možné nebezpečí červeným nápisem ***Varování*** a informací o skutečnosti, že v tuto chvíli nejste plně chráněni. ***Jakmile to bude možné, službu opět aktivujte!***

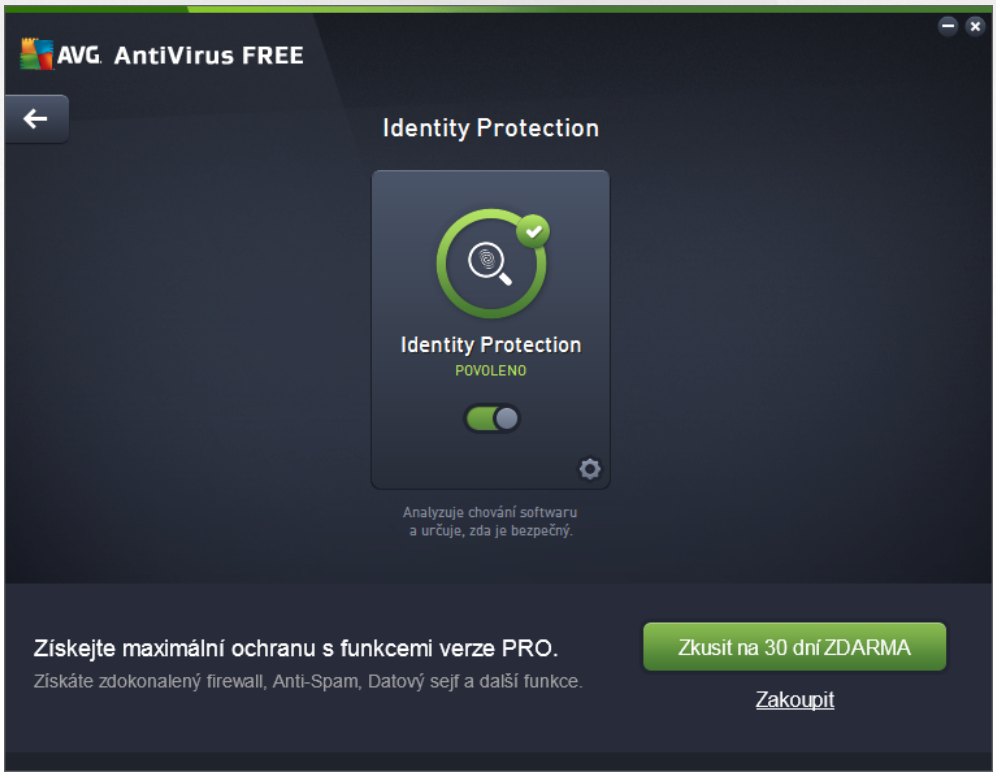
Nastavení - Kliknutím na tlačítko přejdete do rozhraní pro pokročilé nastavení programu **AVG AntiVirus Free Edition**. Přesněji řečeno, budete nasměrováni do dialogu, v němž lze provést veškerou konfiguraci zvolené služby, v tomto případě služby LinkScanner Surf-Shield. V prokročilém nastavení můžete editovat veškeré parametry jednotlivých bezpečnostních služeb **AVG AntiVirus Free Edition**, ale jakoukoliv konfiguraci doporučujeme pouze znalým uživatelům!

Šipka - Pomocí šipky v levé horní části dialogu se vrátíte zpět do základního uživatelského rozhraní s přehledem komponent.

V produktu **AVG AntiVirus Free Edition** není služba ***Webový štít*** bohužel automaticky zahrnuta. Pokud byste rádi využili i tohoto typu ochrany, stiskem tlačítka ***GO PRO*** budete přesměrováni na dedikovanou webovou stránku AVG (*http://www.avg.cz/*), kde najdete informace o možnostech koupě placených produktů AVG.

6.3. 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 nežádoucí aplikaci 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.



Ovládací prvky dialogu

 ***Povoleno / Zakázáno*** - Tlačítko svým vzhledem i chováním připomíná semafor. Jednoduchým kliknutím se dá přepínat mezi dvěma polohami. Zelená barva odpovídá stavu ***Povoleno***, který znamená, že bezpečnostní služba Identity Protection je aktivní a plně funkční. Červená barva pak odpovídá stavu ***Zakázáno***, kdy je služby vypnuta. Pokud nemáte skutečný důvod službu vypínat, doporučujeme, abyste veškerou bezpečnostní konfiguraci ponechali ve výchozím stavu. Výchozí nastavení zajišťuje optimální výkon programu a vaši maximální bezpečnost. Jestliže z nějakého důvodu chcete službu dočasně vypnout, budete okamžitě upozorněni na možné nebezpečí červeným nápisem ***Varování*** a informací o skutečnosti, že v tuto chvíli nejste plně chráněni. ***Jakmile to bude možné, službu opět aktivujte!***

 ***Nastavení*** - Kliknutím na tlačítko přejdete do rozhraní pro pokročilé nastavení programu **AVG AntiVirus Free Edition**. Přesněji řečeno, budete nasměrováni do dialogu, v němž lze provést veškerou konfiguraci zvolené služby, v tomto případě služby Identity Protection. V prokročilém nastavení můžete editovat veškeré parametry jednotlivých bezpečnostních služeb **AVG AntiVirus Free Edition**, ale jakoukoliv konfiguraci doporučujeme pouze znalým uživatelům!

 ***Šipka*** - Pomocí šipky v levé horní části dialogu se vrátíte zpět do základního uživatelského rozhraní s přehledem komponent.

6.4. E-mailová ochrana

Komponenta ***Ochrana e-mailu*** nabízí v rámci **AVG AntiVirus Free Edition** pouze službu ***Kontrola pošty***. Služba ***Anti-Spam*** není v této edici aktivována a je dostupná pouze v plné profesionální verzi. Pokud máte zájem o využití této služby a všech dalších ochranných prvků některé z profesionálních edic, navštivte prosím web AVG (*http://www.avg.cz/*), kde najdete informace o možnostech koupě placených produktů AVG.

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

- ***Anti-Spam*** *(v AVG AntiVirus Free Edition není služba dostupná)* kontroluje veškerou příchozí poštu a nežádoucí zprávy označuje jako 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.)*. Anti-Spam dokáže upravit předmět e-mailu, který je identifikován jako spam, přidáním vámi definovaného textového řetězce. Poté již můžete snadno filtrovat e-maily 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 a zakázané poštovní adresy.

Ovládací prvky dialogu

Mezi oběma sekcemi v dialogu přecházíte pouhým kliknutím na panel příslušný té které službě; po kliknutí se panel vysvítí světlejším odstínem modré. V obou sekcích dialogu se můžete setkat s několika ovládacími prvky. Jejich funkčnost je stejná, ať přísluší jedné či druhé bezpečnostní službě *(aktivní je však pouze služba Kontrola pošty)*:

Povoleno / Zakázáno - Tlačítko svým vzhledem i chováním připomíná semafor. Jednoduchým kliknutím se dá přepínat mezi dvěma polohami. Zelená barva odpovídá stavu ***Povoleno***, který znamená, že bezpečnostní služba je aktivní a plně funkční. Červená barva pak odpovídá stavu ***Zakázáno***, kdy je služby vypnuta. Pokud nemáte skutečný důvod službu vypínat, doporučujeme, abyste veškerou bezpečnostní konfiguraci ponechali ve výchozím stavu. Výchozí nastavení zajišťuje optimální výkon programu a vaši maximální bezpečnost. Jestliže z nějakého důvodu chcete službu dočasně vypnout, budete okamžitě upozorněni na možné nebezpečí červeným nápisem ***Varování*** a informací o skutečnosti, že v tuto chvíli nejste plně chráněni. ***Jakmile to bude možné, službu opět aktivujte!***

V rámci sekce Kontrola pošty najdete dva "semafory". Jejich pomocí můžete samostatně určit, zda si přejete, aby se testovaly zprávy příchozí, odchozí, nebo obojí. Ve výchozím nastavení je služba zapnuta pro testování příchozí pošty, ale pro odchozí poštu vypnuta - u odchozích zpráv je riziko zavlečení infekce minimální.

Nastavení - Kliknutím na tlačítko přejdete do rozhraní pro pokročilé nastavení programu **AVG AntiVirus Free Edition**. Přesněji řečeno, budete nasměrováni do dialogu, v němž lze provést veškerou konfiguraci zvolené služby, v tomto případě služby Kontrola pošty. V prokročilém nastavení můžete

editovat veškeré parametry jednotlivých bezpečnostních služeb **AVG AntiVirus Free Edition**, ale jakoukoliv konfiguraci doporučujeme pouze znalým uživatelům!

Šipka - Pomocí šipky v levé horní části dialogu se vrátíte zpět do základního uživatelského rozhraní s přehledem komponent.

V produktu **AVG AntiVirus Free Edition** není služba Anti-Spam bohužel automaticky zahrnuta. Pokud byste rádi využili i tohoto typu ochrany, stiskem tlačítka ***GO PRO*** budete přesměrováni na dedikovanou webovou stránku AVG (*http://www.avg.cz/*), kde najdete informace o možnostech koupě placených produktů AVG.

6.5. PC Analyzer

Komponenta PC Analyzer je nástrojem pro detailní systémovou analýzu a optimalizaci umožňující zrychlit a vylepšit výkon vašeho počítače. Otevírá se buďto přímo z hlavního uživatelského rozhraní tlačítkem ***Zlepšit výkon*** nebo toutéž volbou v kontextovém menu ikony AVG na systémové liště. Průběh kontroly budete moci sledovat přímo v tabulce, a tam budou posléze zobrazeny i výsledky analýzy:

Analyzovat lze následující:

- ***Chyby v registrech*** - případné chyby v registru Windows, které mohou zpomalovat váš počítač a zobrazovat chybové hlášky.
- ***Nepotřebné soubory*** - počet souborů, bez kterých se pravděpodobně bez potíží obejdete a zabírají tedy v počítači zbytečně místo. Typicky jde o různé typy dočasných souborů a o smazané soubory, tj. obsah koše.
- ***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.
- ***Neplatní Zástupci*** - upozorní na odkazy či zástupce aplikací, které již nefungují, odkazují na neexistující soubory či složky apod.

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

Ovládací tlačítka dialogu

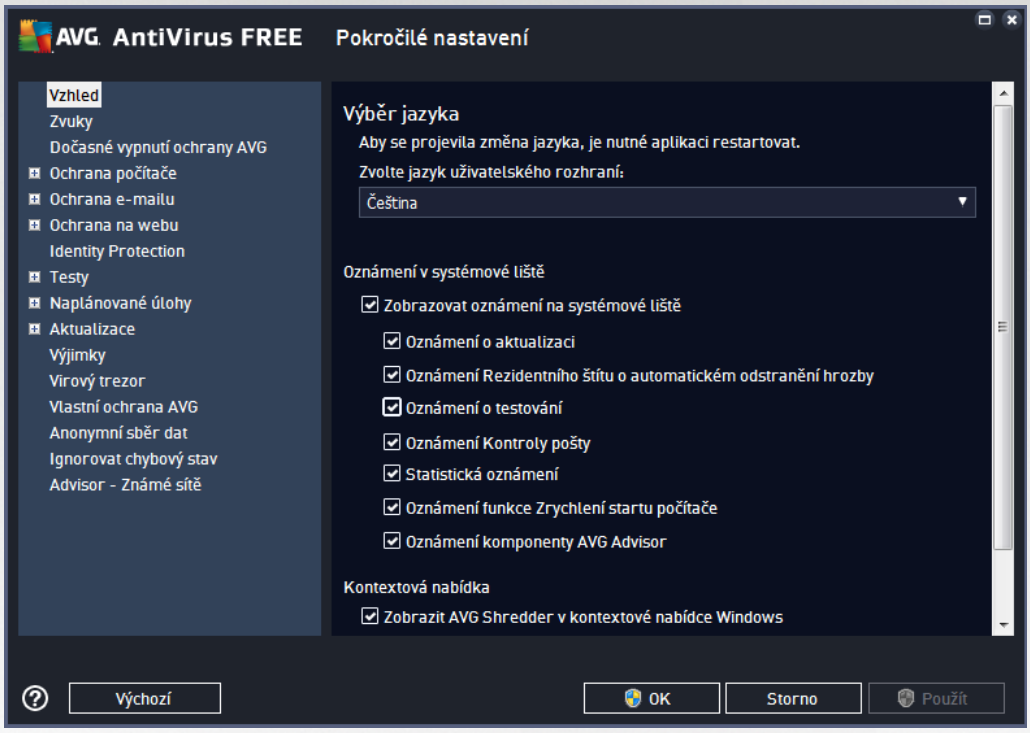
- ***Zastavit analýzu*** *(tlačítko se zobrazí v průběhu analýzy)* - Stiskem tlačítka bezprostředně zastavíte probíhající analýzu počítače

- ***Opravit*** *(tlačítko se zobrazí po dokončení analýzy)* - V rámci produktu **AVG AntiVirus Free Edition** je funkčnost komponenty PC Analyzer bohužel omezená pouze na analýzu aktuálního stavu počítače. V placených verzích však AVG nabízí možnost využít pokročilého nástroje pro detailní systémovou analýzu a úpravy vedoucí ke zlepšení výkonu a rychlosti vašeho PC. Kliknutím na tlačítko budete přesměrování na dedikovanou webovou stránku, kde najdete veškeré potřebné informace.

7. Pokročilé nastavení AVG

7.1. Vzhled

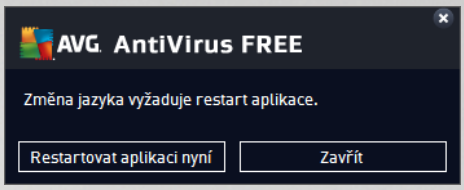
První položka navigačního seznamu, ***Vzhled***, se týká obecného nastavení uživatelského rozhraní **AVG AntiVirus Free Edition** a nabízí možnost nastavení základních prvků programu:



Výběr jazyka

V sekci ***Výběr jazyka*** můžete z rozbalovacího menu zvolit jazyk, v němž má být zobrazeno uživatelské rozhraní **AVG AntiVirus Free Edition**. V nabídce budou dostupné jen ty jazyky, které jste zvolili během instalačního procesu a také angličtina (*angličtina se vždy instaluje automaticky*). Pro zobrazení **AVG AntiVirus Free Edition** 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 AntiVirus Free Edition** restartovat
- Stiskem tlačítka ***Restartovat aplikaci nyní*** vyjádříte svůj souhlas s restartem a během sekundy se aplikace přepne do nově zvoleného jazyka:



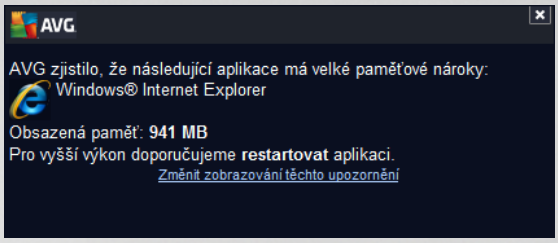
Oznámení v systémové liště

V této sekci můžete potlačit zobrazování systémových oznámení o aktuálním stavu aplikace **AVG AntiVirus Free Edition**. 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 AntiVirus Free Edition** 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 AntiVirus Free Edition**. 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:
    - ***Oznámení o aktualizaci*** *(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.
    - ***Oznámení Rezidentního štítu o automatickém odstranění hrozby*** *(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*).
    - ***Oznámení o testování*** *(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.
    - ***Oznámení Kontroly pošty*** *(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.
    - ***Statistická oznámení*** *(ve výchozím nastavení zapnuto)* - volbou položky umožníte zobrazení pravidelného statistického přehledu v systémové liště.
    - ***Oznámení funkce Zrychlení startu počítače*** *(ve výchozím nastavení zapnuto)* - Volbou položky rozhodnete, zda si přejete být vyrozuměni o zrychleném startu Vašeho počítače.

- ***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.

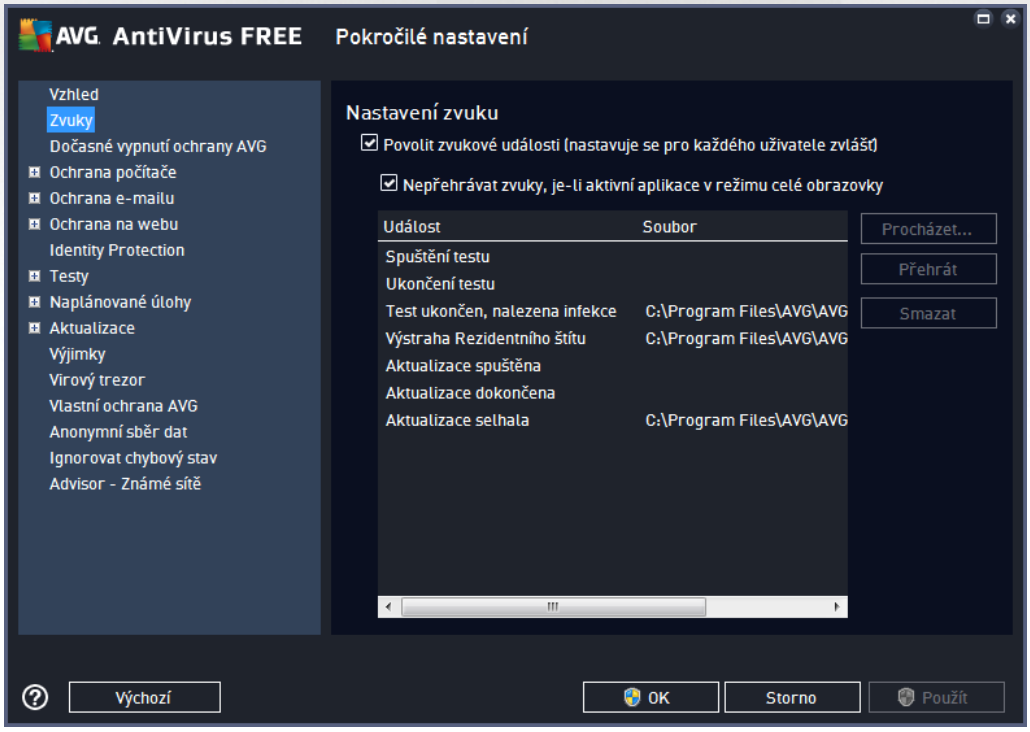


Herní režim

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

7.2. Zvuky

V dialogu ***Nastavení zvuku*** můžete rozhodnout, zda chcete být o jednotlivých akcích **AVG AntiVirus Free Edition** 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!)*

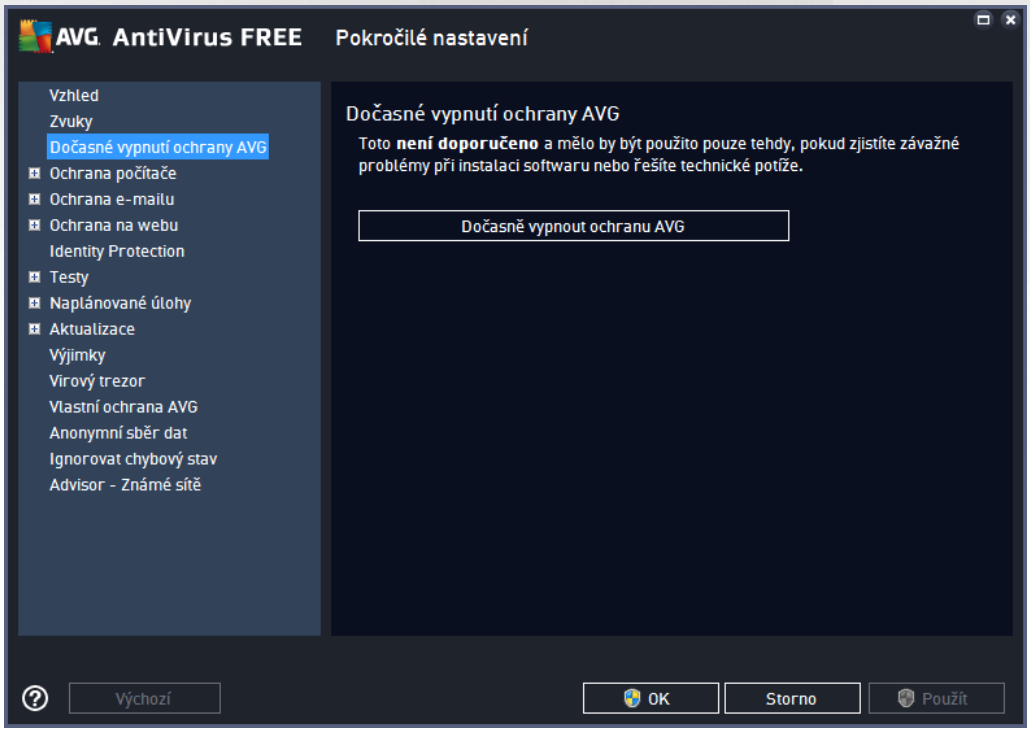
- ***Přehrát*** - Chcete-li si přiřazený zvuk poslechnout, označte v seznamu příslušnou akci a stiskněte tlačítko ***Přehrát***.

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

7.3. Dočasné vypnutí ochrany AVG

V dialogu ***Dočasné vypnutí ochrany AVG*** máte možnost označením jediné dostupné položky jednorázově deaktivovat celou ochranu zajištěnou programem **AVG AntiVirus Free Edition**.

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

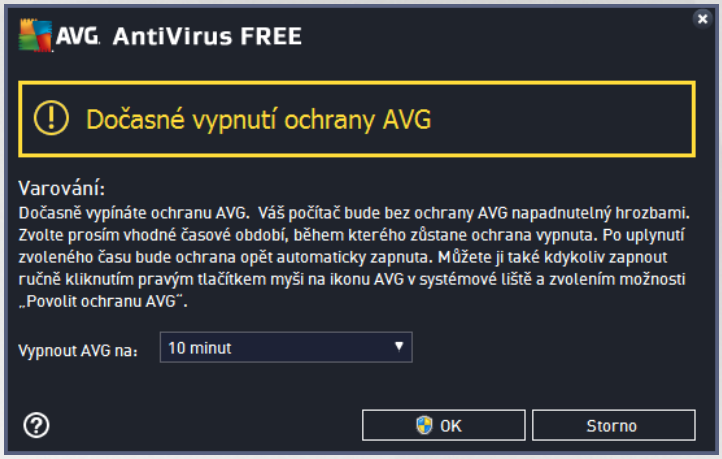


V naprosté většině případů ***není nutné*** deaktivovat **AVG AntiVirus Free Edition** před instalací nového software nebo ovladačů, a to ani tehdy, pokud budete během instalace vyzváni k zavření všech spuštěných aplikací. Pokud by v takovém případě došlo ke kolizi, pravděpodobně bude stačit deaktivovat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

- Klikněte na tlačítko ***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 AntiVirus Free Edition** 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.



7.4. Ochrana počítače

7.4.1. AntiVirus

AntiVirus za pomoci ***Rezidentního štítu*** chrání váš počítač nepřetržitě před všemi známými typy virů, spyware a malware obecně, včetně tzv. spících, zatím neaktivních hrozeb.

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*) - 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.

- ***Hlásit Potenciálně nežádoucí aplikace a spywarové hrozby*** (*ve výchozím nastavení zapnuto*) - Kontrola přítomnosti potenciálně nežádoucích aplikací (*spustitelné programy, které mohou fungovat jako spyware nebo adware*). Zaškrtnutím tohoto políčka aktivujete testování přítomnosti spyware, nejen virů. Spyware představuje poněkud problematickou kategorii malware, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány vědomě a se souhlasem uživatele. Doporučujeme ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.

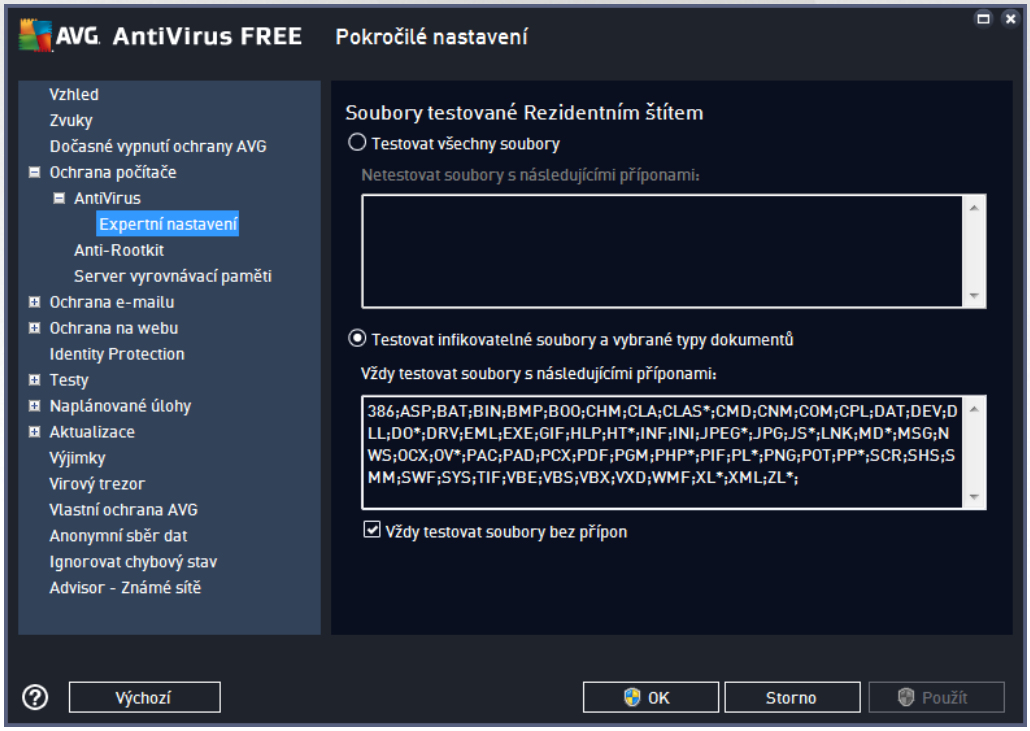
- ***Hlásit rozšířenou množinu potenciálně nežádoucích aplikací*** (*ve výchozím nastavení vypnuto*) - Zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware, tj. programů, které jsou v původní podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým 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 přístím startu počítače.
- ***Povolit testování s extrémní citlivostí*** (*ve výchozím nastavení vypnuto*) - Ve specifických situacích (*mimořádný stav ohrožení počítače*) můžete zvolit tuto metodu kontroly, která aktivuje nejdůkladnější a nejpodrobnější testovací algoritmy. Mějte však na paměti, že tato metoda je časově velmi náročná.

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

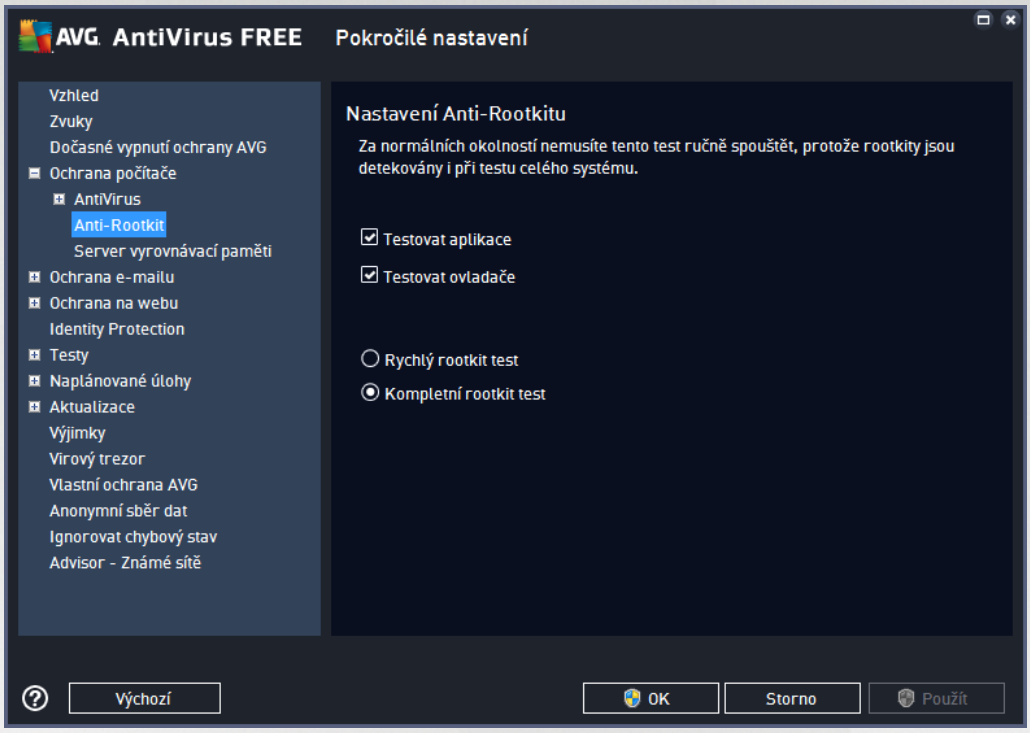


Svou volbou rozhodněte, zda chcete ***Testovat všechny soubory*** nebo pouze ***Testovat infikovatelné soubory a vybrané typy dokumentů***. Pro urychlení testování a současné dosažení maximální bezpečnosti doporučujeme ponechat výchozí nastavení. Tak budou testovány infikovatelné s příponami uvedenými v příslušné sekci dialogu. Seznam přípon můžete dále editovat podle vlastního uvážení.

Označením políčka ***Vždy testovat 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.

7.4.2. Anti-Rootkit

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

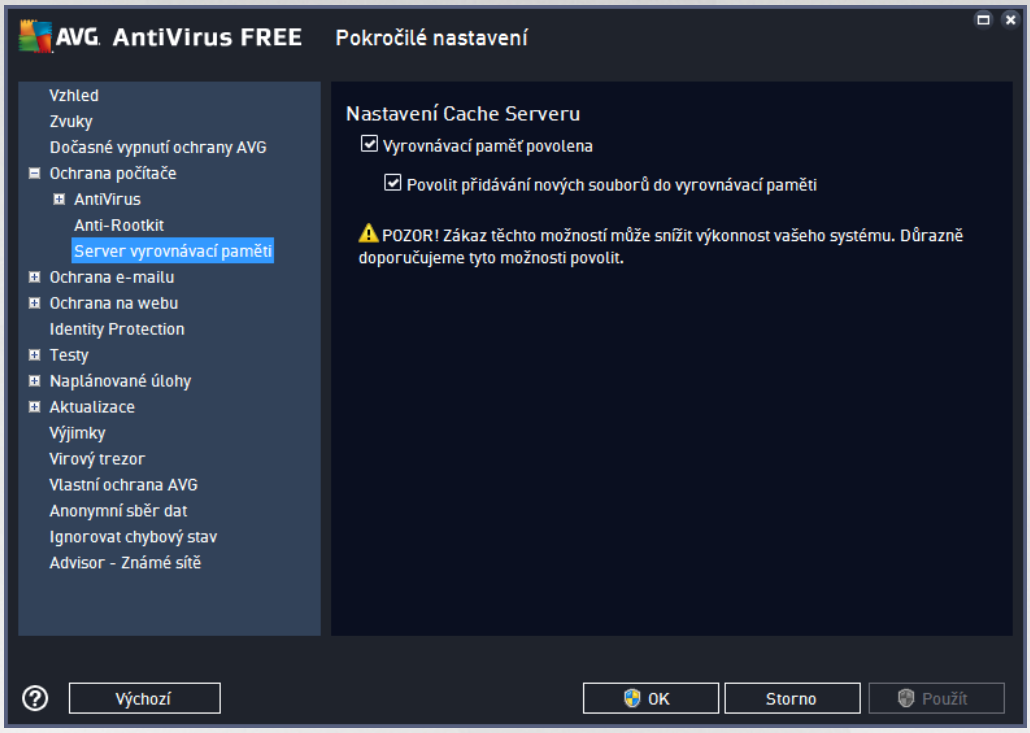


Možnosti ***Testovat aplikace*** a ***Testovat ovladače*** umožňují určit, co vše má být v testu na rootkity zahrnuto. Jiné než výchozí nastavení doporučujeme pouze zkušeným uživatelům; jinak prosím ponechte všechny možnosti zapnuté. Dále se pak můžete rozhodnout, v jakém režimu si přejete test spustit:

- ***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*)

7.4.3. Server vyrovnávací paměti

Dialog ***Nastavení Cache Serveru*** se vztahuje k procesu serveru vyrovnávací paměti, jehož úkolem je zrychlit průběh všech testů **AVG AntiVirus Free Edition**:



V rámci tohoto procesu **AVG AntiVirus Free Edition** 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.

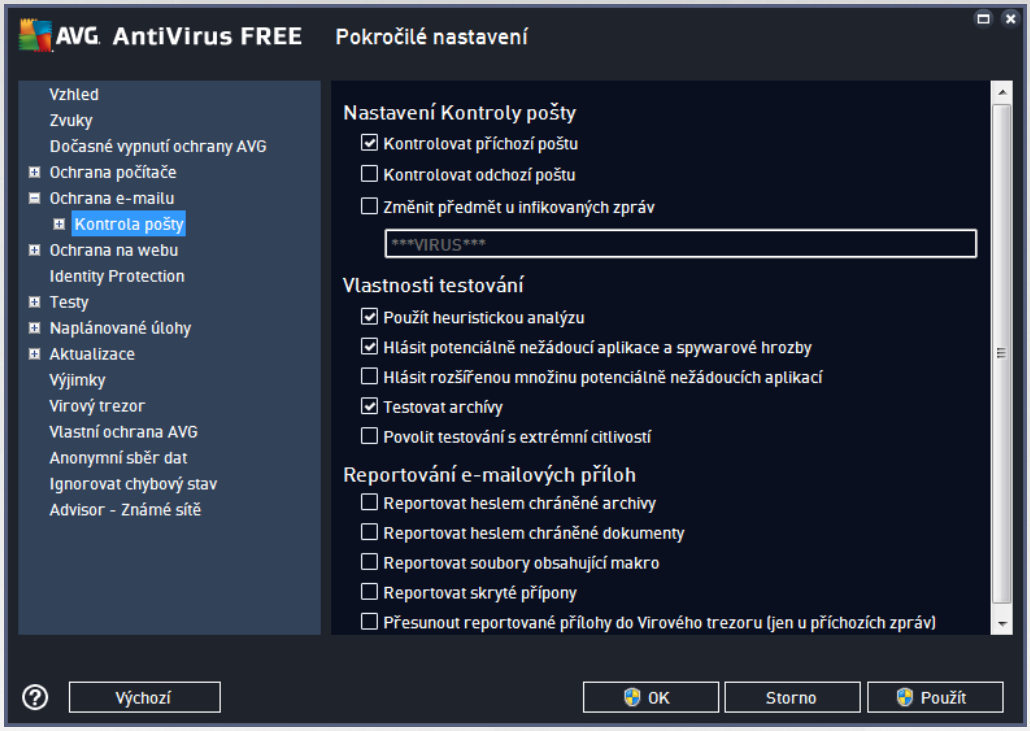
Pokud nemáte skutečný důvod cache server vypínat, důrazně doporučujeme, abyste se přidrželi výchozího nastavení a ponechali obě položky zapnuté! V opačném případě může dojít k výraznému snížení rychlosti a výkonnosti Vašeho systému.

7.5. Ochrana emailu

V této sekci máte možnost editovat podrobné nastavení pro službu Kontrola pošty:

7.5.1. 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*) - chcete-li být upozorněni na to, 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 aplikace a spywarové hrozby*** (*ve výchozím nastavení zapnuto*) - kontrola přítomnosti potenciálně nežádoucích aplikací (*spustitelné programy, které mohou fungovat jako spyware nebo adware*). Zaškrtnutím tohoto políčka aktivujete testování přítomnosti spyware, nejen virů. Spyware představuje poněkud problematickou kategorii malware, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány vědomě a se souhlasem uživatele. Doporučujeme ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.

- ***Hlásit rozšířenou množinu potenciálně nežádoucích aplikací*** (*ve výchozím nastavení vypnuto*) - zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware, tj. 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 E-mailové ochrany.

- ***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.

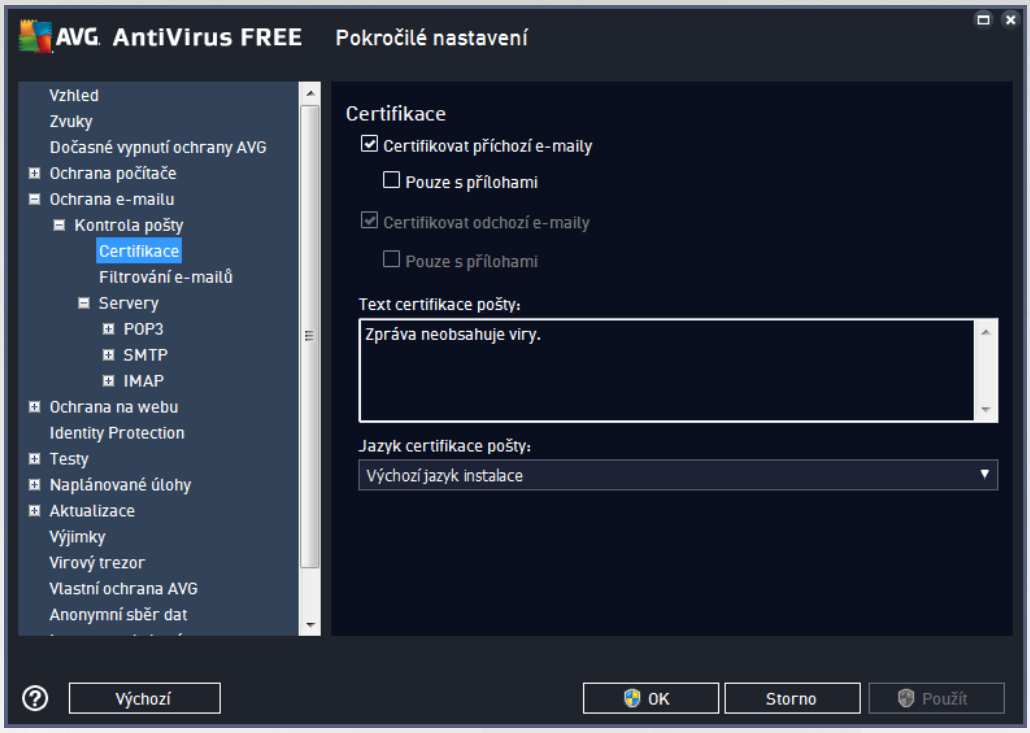
- ***Reportovat heslem chráněné dokumenty*** - dokumenty chráněné heslem není možné otestovat na přítomnost virů; po zaškrtnutí tohoto políčka se tyto archivy budou označovat jako potenciálně nebezpečné.

- ***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 tohoto políčka budou soubory se skrytými příponami reportovány jako potenciálně nebezpečné.

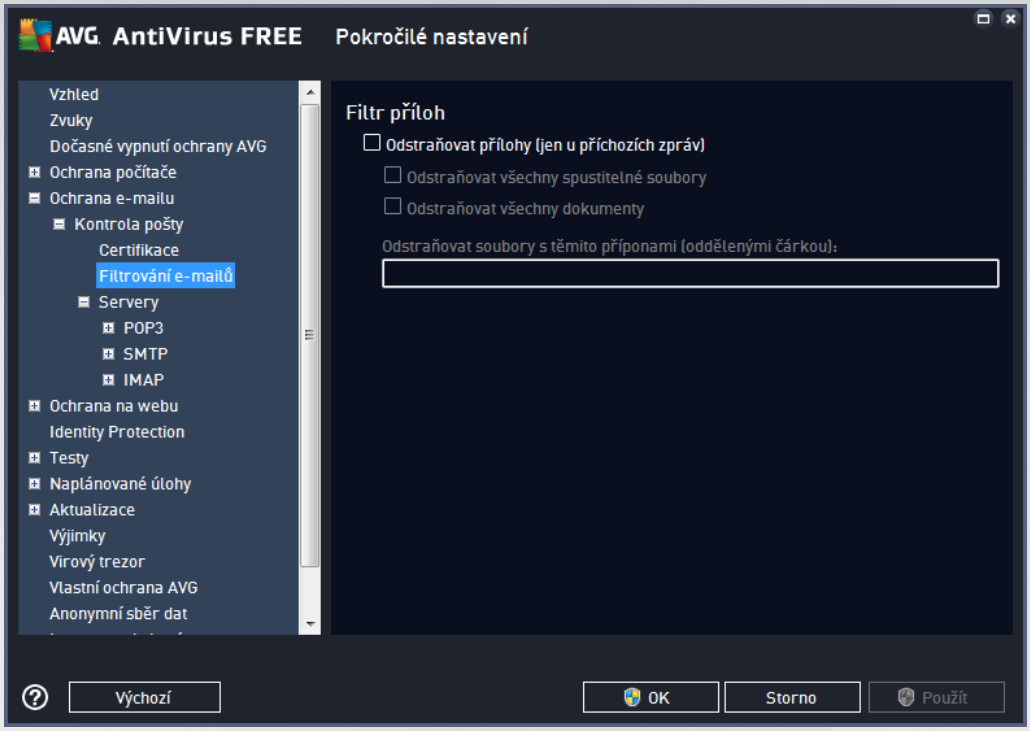
- Zaškrtnutím políčka ***Přesunout reportované přílohy do Virového trezoru*** určíte, že všechny výše vybrané soubory z příloh e-mailů se mají nejen reportovat, ale rovněž automaticky přesouvat do Virového trezoru.

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!*



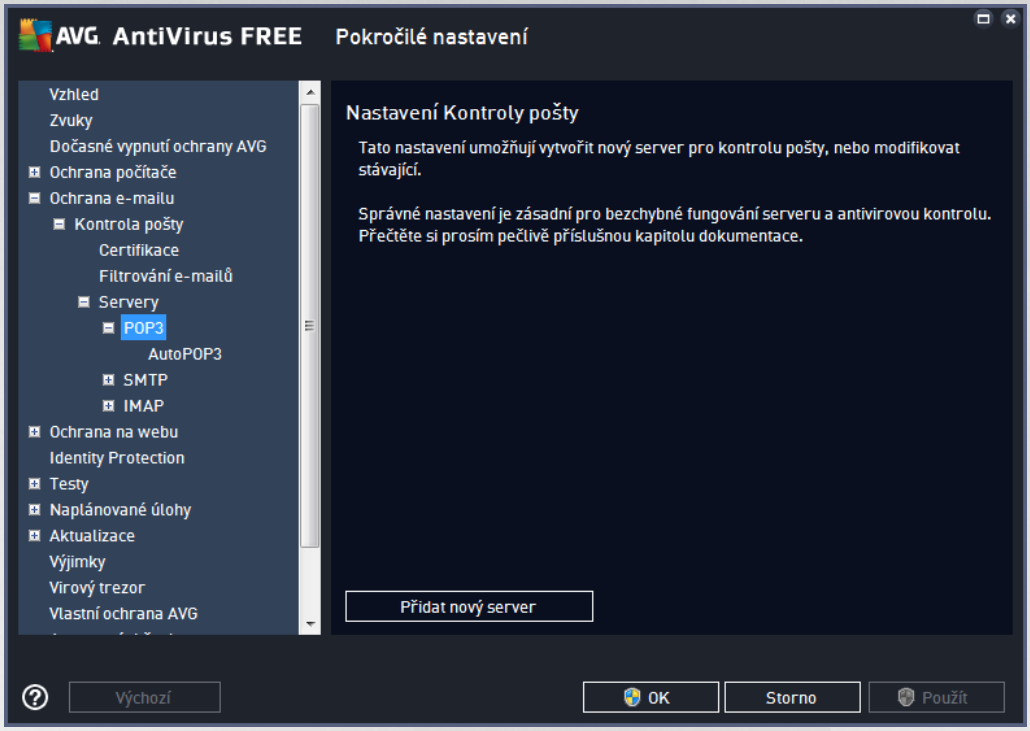
Dialog ***Filtr příloh*** umožňuje nastavení parametrů pro testování příloh e-mailových zpráv. Ve výchozím nastavení je možnost ***Odstraňovat přílohy*** vypnuta. Pokud se rozhodnete pro její aktivaci, budou automaticky odstraněny všechny přílohy zpráv, které byly detekovány jako infikované nebo potenciálně 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

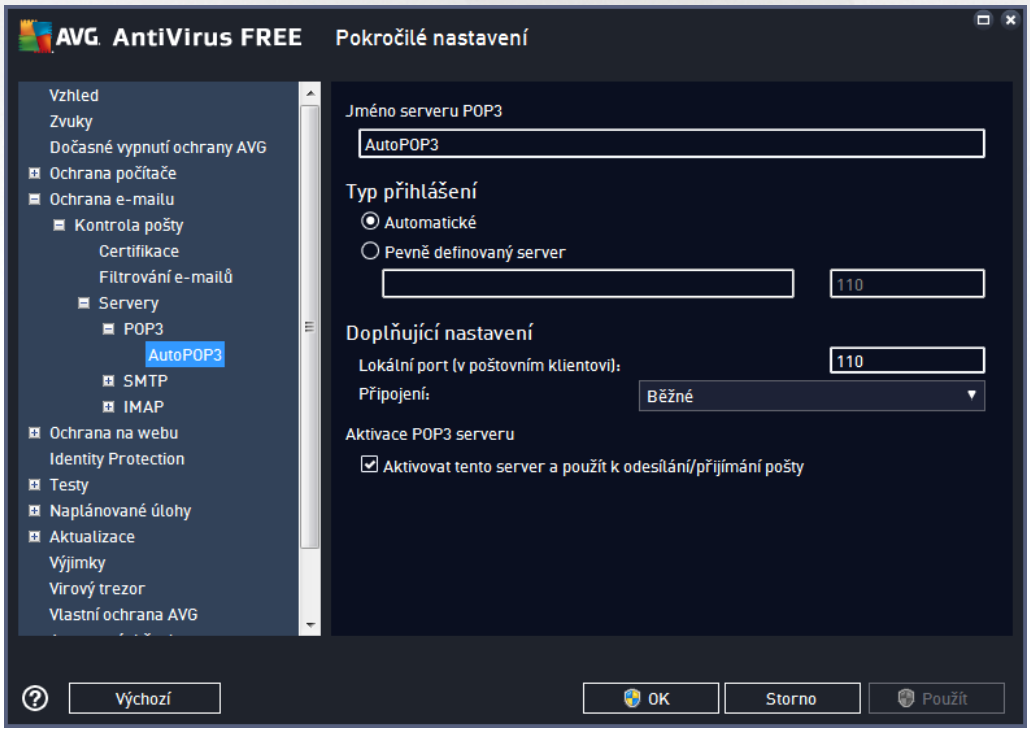
V sekci ***Servery*** máte možnost editovat parametry jednotlivých serverů Kontroly pošty:

- POP3 server
- SMTP server
- IMAP server

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



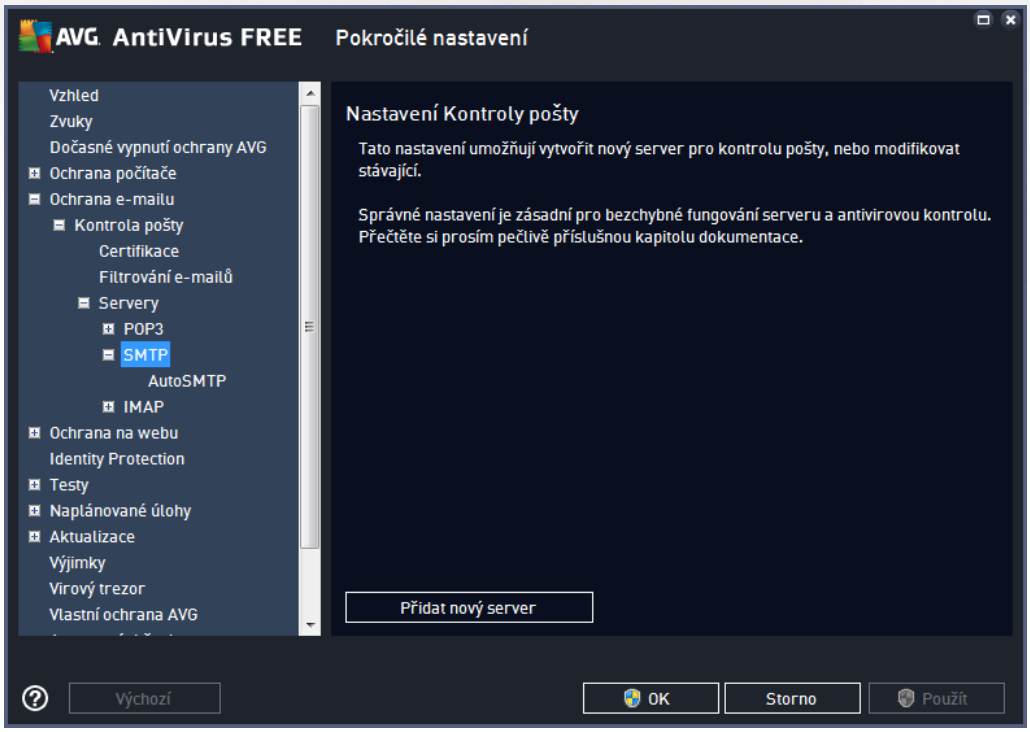
V tomto dialogu (*odkaz **Servery / POP3***) nastavujete server Kontroly pošty s protokolem POP3 pro příchozí poštu:



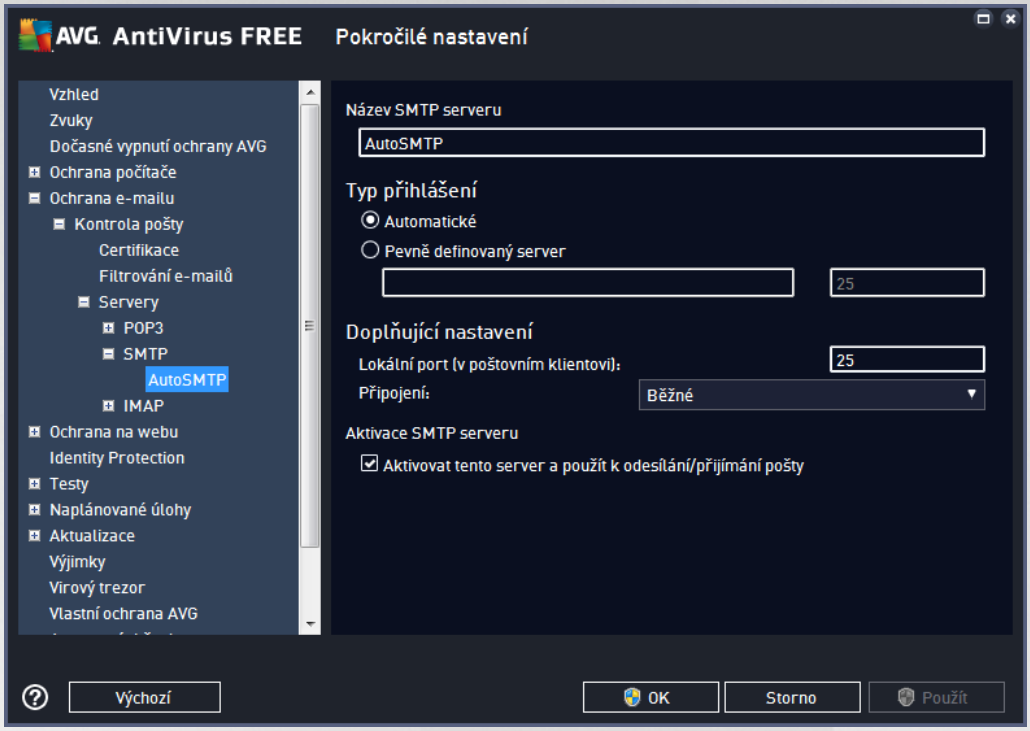
- ***Jméno serveru POP3*** - v tomto poli můžete zadat jméno nově přidaných serverů (*server POP3 přidáte*

tak, že kliknete pravým tlačítkem myši nad položkou POP3 v levém navigačním menu).

- ***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: Běžné (*standardní připojení*), SSL (*zabezpečené na vyhrazeném portu*) anebo výchozí SSL (*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 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

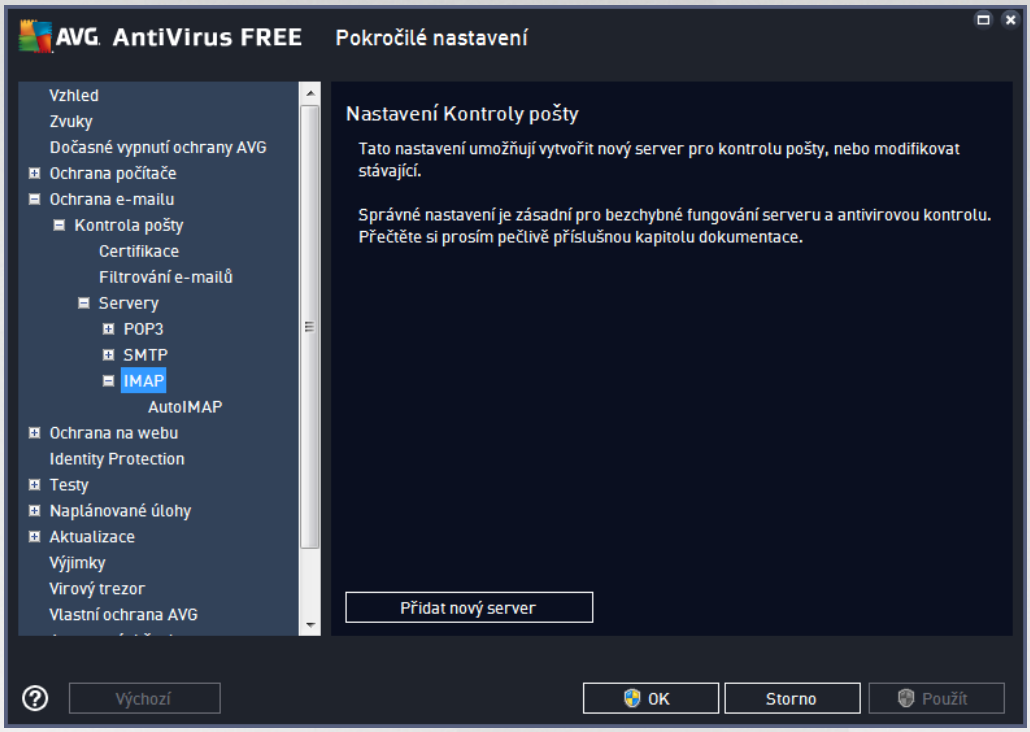
  - ***Pevně definovaný server*** - v tomto případě bude vždy použit konkrétní server. Do editačního řádku je třeba zadat adresu nebo jméno vašeho poštovního serveru. Jako jméno je možné použít jak doménový název (*např. smtp.acme.com*), tak i IP adresu (*např. 123.45.67.89*). Pokud poštovní server používá 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:

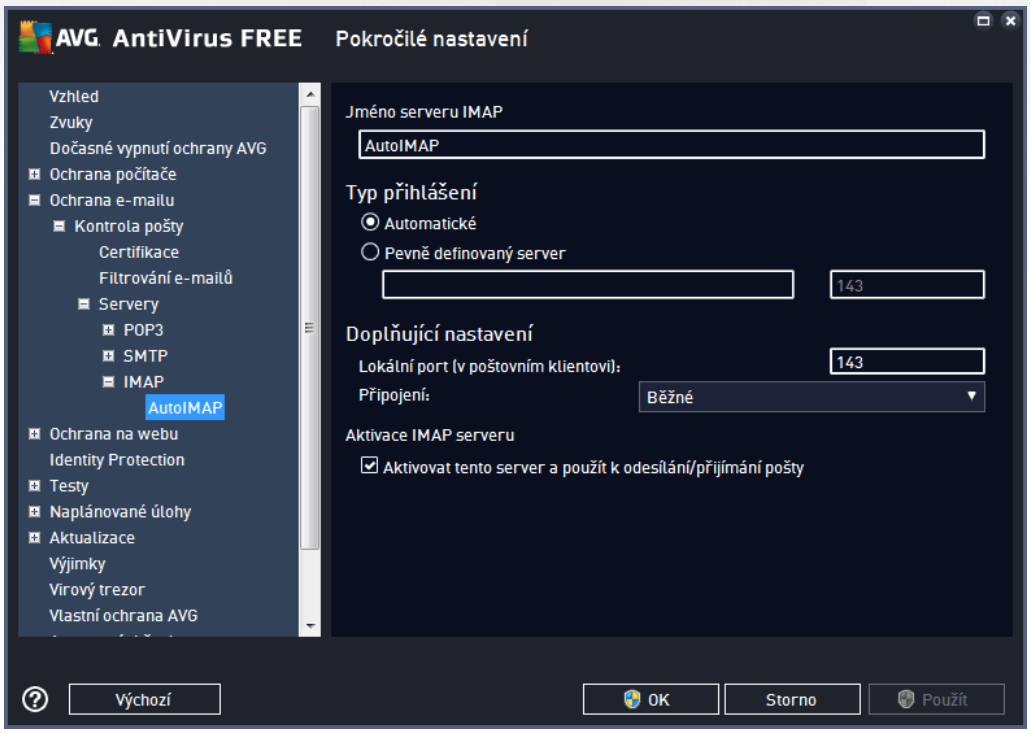
  - ***Lokální port*** - určuje, na kterém portu lze očekávat komunikaci z poštovní aplikace. Tento port je pak také nutné v poštovní aplikaci zadat jako port pro SMTP komunikaci.

  - ***Připojení*** - v této rozbalovací nabídce můžete specifikovat typ připojení: Běžné (*standardní připojení*), SSL (*zabezpečené na vyhrazeném portu*) anebo výchozí SSL (*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 SMTP serveru*** - zapnutím/vypnutím položky máte možnost aktivovat či deaktivovat právě nastavený SMTP server



V tomto dialogu nastavujete server Kontroly pošty s protokolem IMAP pro odchozí poštu:



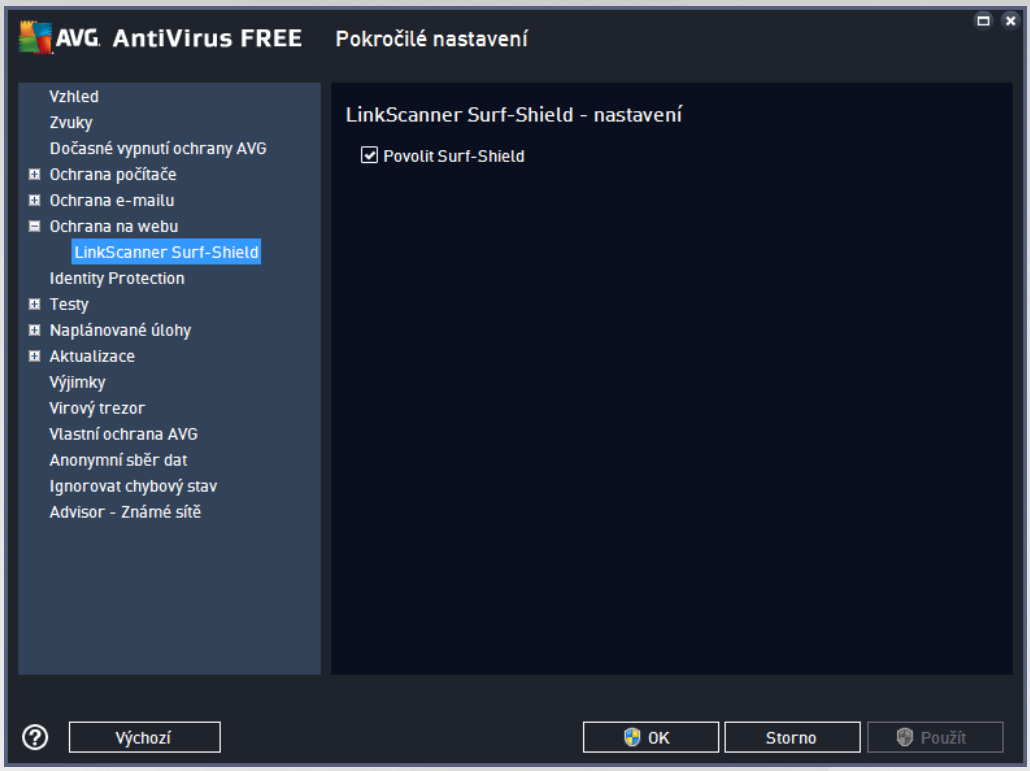
Jméno serveru IMAP - v tomto poli můžete zadat jméno nově přidaných serverů (*server IMAP přidáte tak, že kliknete pravým tlačítkem myši nad položkou IMAP v levém navigačním menu*).

- ***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: Běžné (*standardní připojení*), SSL (*zabezpečené na vyhrazeném portu*) anebo výchozí SSL (*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 IMAP serveru*** - zapnutím/vypnutím položky máte možnost aktivovat či deaktivovat právě nastavený IMAP server

7.6. Ochrana na webu

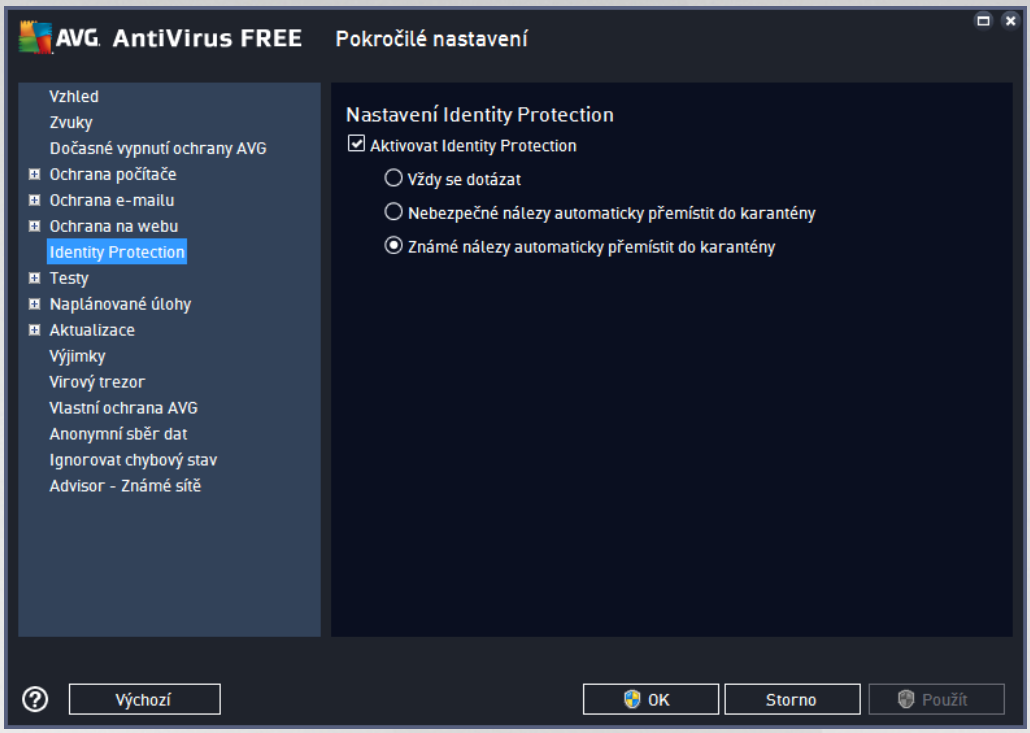
7.6.1. LinkScanner Surf-Shield

Dialog ***LinkScanner Surf-Shield - nastavení*** umožňuje zapnout či vypnout funkci ***Povolit Surf-Shield*** (*ve výchozím nastavení zapnuto*), která zajišťuje aktivní ochranu proti agresivním webovým stránkám. Kontrola stránek se provádí v okamžiku jejich načítání. Stránky s nebezpečným obsahem jsou v příslušném internetovém prohlížeči (nebo jiné aplikaci, která používá HTTP) rovnou zablokovány.



7.7. 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 Identita*). Dialog ***Nastavení Identity Protection*** umožňuje zapnout či vypnout některé základní vlastnosti komponenty *Identita*:



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*** - 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*** (*výchozí nastavení*) - označte tuto položku, pokud si přejete, aby veškeré aplikace detekované jako možný malware byly automaticky a okamžitě přesunuty do Virového trezoru.

7.8. Testy

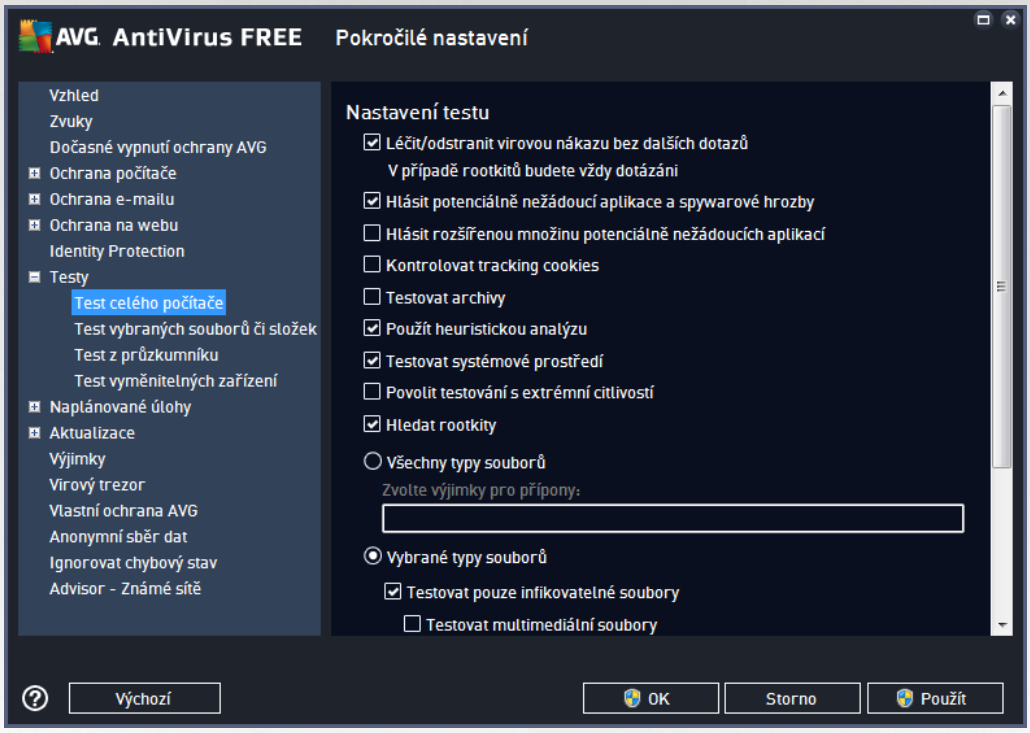
Pokročilé nastavení testů je rozděleno do čtyř kategorií, které odpovídají jednotlivým typům výrobcem definovaných testů:

- ***Test celého počítače*** - výrobcem nastavený standardní test
- ***Test vybraných souborů či složek*** - výrobcem nastavený standardní test s možností definovat oblasti testování

- ***Test z průzkumníku*** - specifický test spouštěný nad zvolenými objekty přímo v prostředí Windows
- ***Test vyměnitelných zařízení*** - specifický test vyměnitelných zařízení připojených v danou chvíli k Vašemu PC

7.8.1. Test celého počítače

Položka ***Test celého počítače*** nabízí možnost editovat parametry předem nastaveného ***Testu celého počítače***:



Nastavení testu

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

- ***Léčit/odstranit virovou nákazu bez dalších dotazů*** (*ve výchozím nastavení zapnuto*) - jestliže je během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. V případě, že virus automaticky léčit nelze, bude infikovaný objekt přesunut do Virového trezoru.
- ***Hlásit Potenciálně nežádoucí aplikace a spywarové hrozby*** (*ve výchozím nastavení zapnuto*) - kontrola přítomnosti potenciálně nežádoucích aplikací (*spustitelné programy, které mohou fungovat jako spyware nebo adware*). Zaškrtnutím tohoto políčka aktivujete testování přítomnosti spyware, nejen virů. Spyware představuje poněkud problematickou kategorii malware, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány vědomě a se souhlasem uživatele. Doporučujeme ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
- ***Hlásit rozšířenou množinu potenciálně nežádoucích aplikací*** (*ve výchozím nastavení vypnuto*) - zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware, tj. 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 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 testovat 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 služby 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

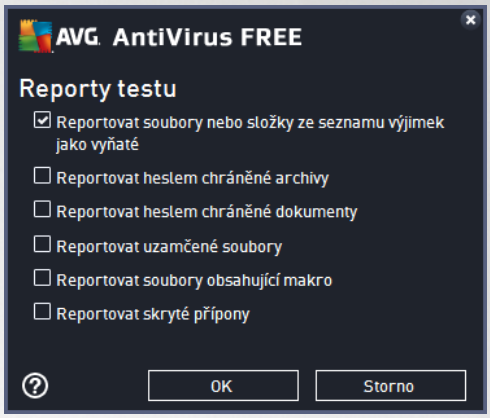
V této sekci pak můžete nastavit požadovanou rychlost testování v závislosti na zátěži systémových zdrojů.

Ve výchozím nastavení je tato hodnota nastavena na úroveň ***Dle činnosti uživatele***, což znamená, že je využito minimum systémových prostředků ve chvíli, kdy s počítačem pracujete, a naopak maximum ve chvíli, kdy s počítačem nepracujete.

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.

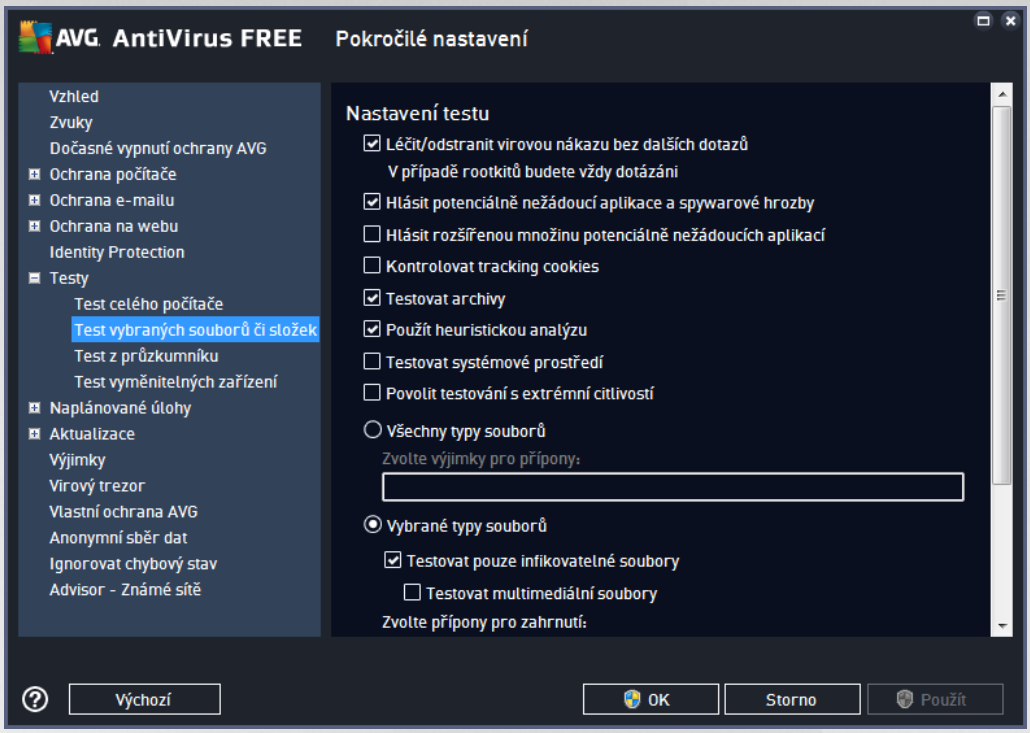
Nastavit další reporty testů ...

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:



7.8.2. Test vybraných souborů či složek

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

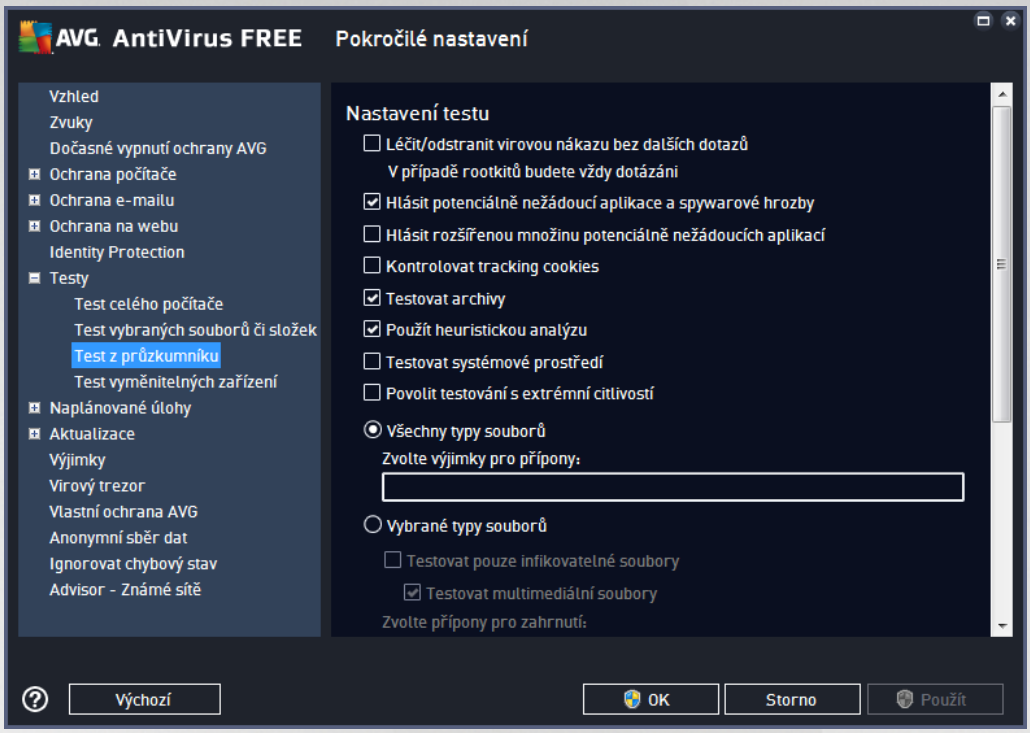


Veškeré parametry nastavené v tomto konfiguračním dialogu se vztahují pouze na ty oblasti vašeho počítače, které jste vybrali pro testování v rámci Testu vybraných souborů či složek!

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

7.8.3. 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:



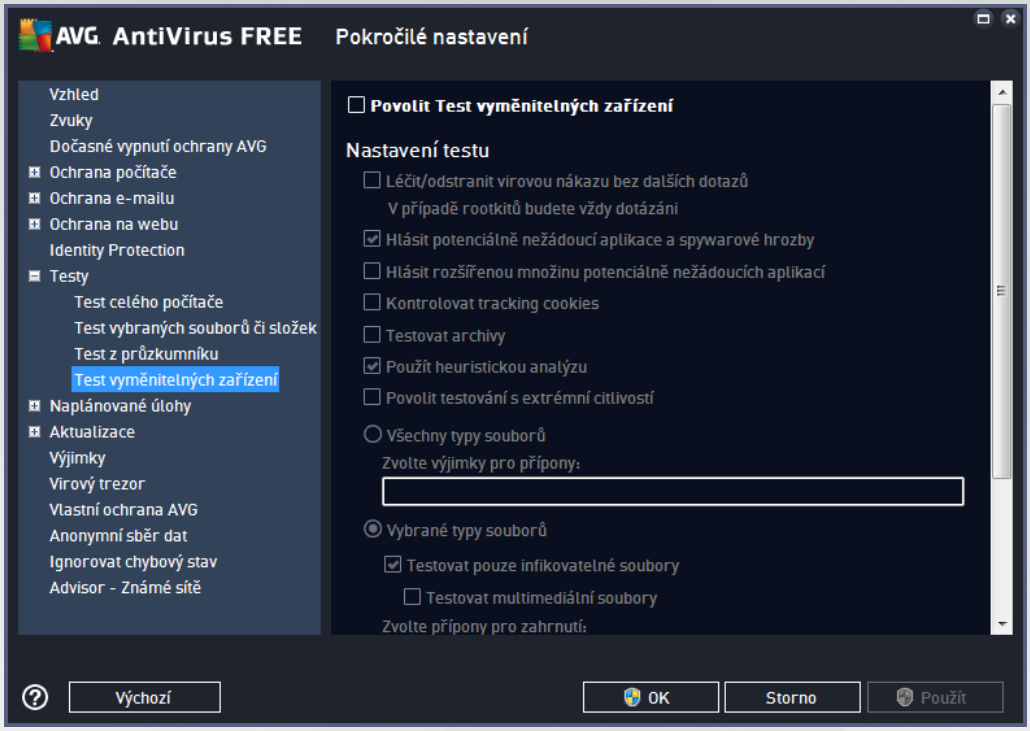
Veškeré možnosti editace parametrů testu jsou totožné s editací parametrů Testu celého počítače. Odlišné je pouze výchozí nastavení těchto parametrů (*například Test celého počítače ve výchozím nastavení neprovádí kontrolu archivů, ale provádí kontrolu systémového prostředí, zatímco u Testu z průzkumníku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

7.8.4. Test vyměnitelných zařízení

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



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

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

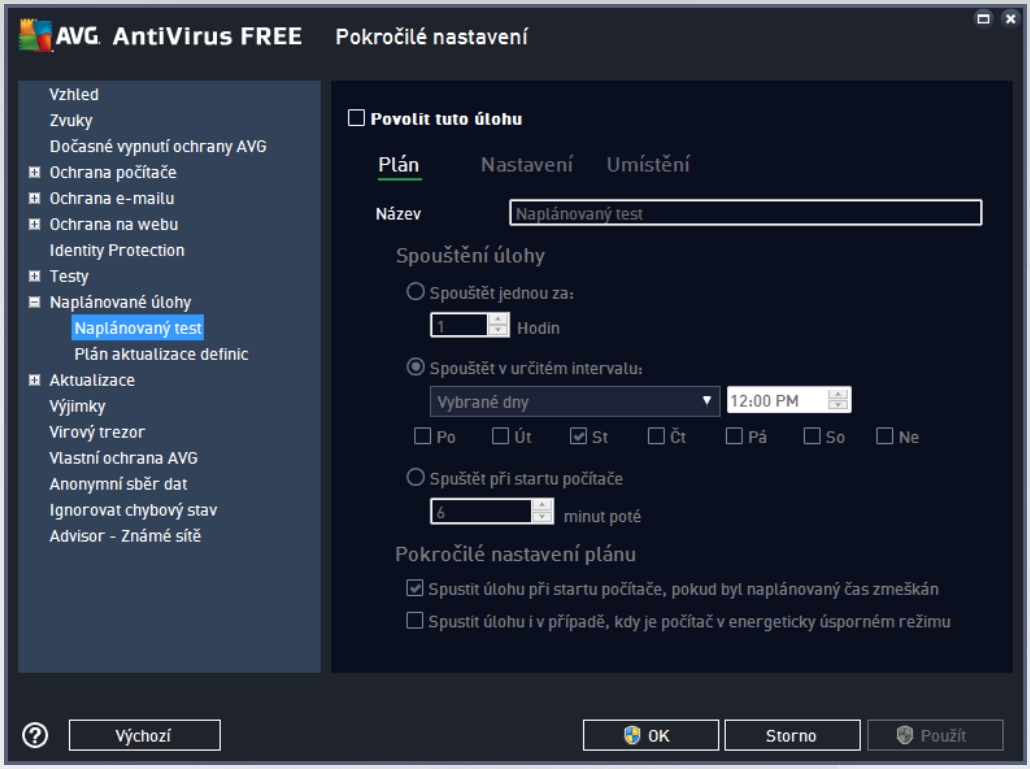
7.9. Naplánované úlohy

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

- Naplánovaného testu
- Plánu aktualizace definic

7.9.1. Naplánovaný test

V tomto dialogu máte možnost konfigurovat nastavení naplánovaného testu a určit čas jeho spuštění v pravidelných intervalech. Parametry naplánovaného testu můžete editovat 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. V rámci **AVG AntiVirus Free Edition** není bohužel možné vytvářet vlastní plány testování.

AVG AntiVirus Free Edition je dostupný zdarma a jeho funkčnost je omezená. Pokud během používání AVG AntiVirus Free Edition zjistíte, že byste dali přednost plné funkčnosti profesionální verze AVG, navštivte prosím web AVG (http://www.avg.cz/), kde najdete informace o možnostech koupě placených produktů AVG.

V tomto dialogu můžete dále definovat tyto parametry testu:

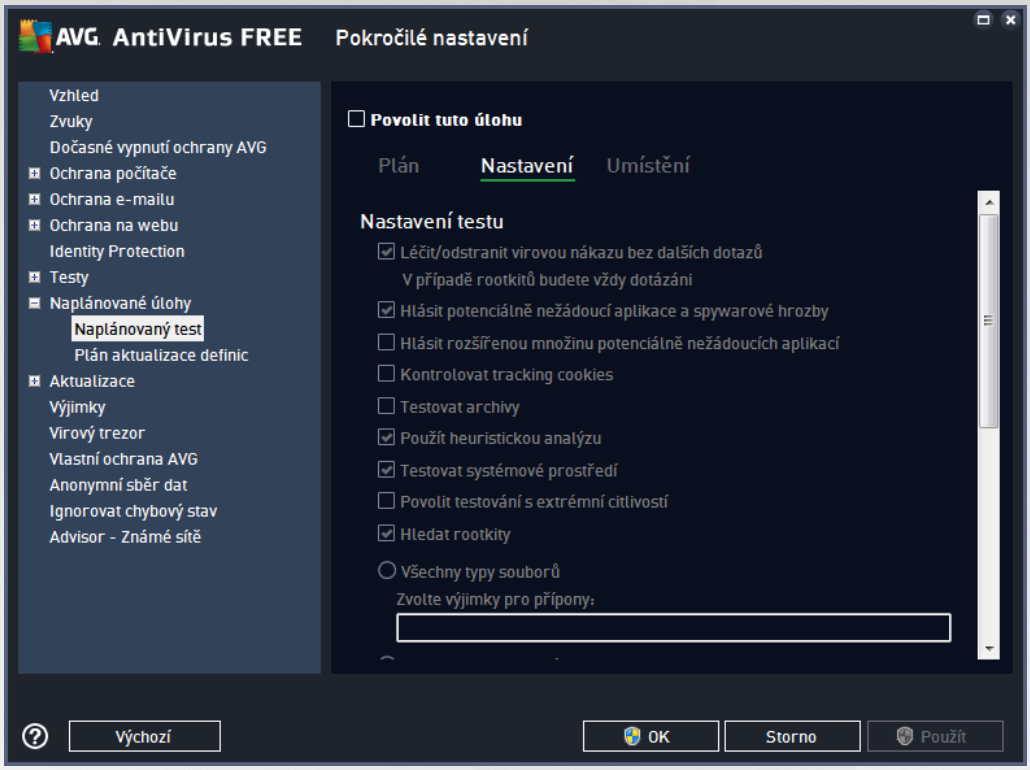
Spouštění úlohy

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

- ***Spustit úlohu při startu počítače, pokud byl naplánovaný čas zmeškán*** - jestliže je test naplánován na konkrétní čas, tato možnost *(ve výchozím nastavení označena)* zajistí, že test bude spuštěn bezprostředně po zapnutí počítače, pokud byl tento v době naplánovaného spuštění vypnutý.

- ***Spustit úlohu i v případě nastavení na energeticky úsporný režim*** - označením této položky rozhodnete, že test má být spuštěn i v případě, že počítač běží například pouze na baterii.



Záložka ***Nastavení*** 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*): jestliže je během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. V případě, že virus automaticky léčit nelze, bude infikovaný objekt přesunut do Virového trezoru.

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

- ***Hlásit rozšířenou množinu potenciálně nežádoucích aplikací*** (*ve výchozím nastavení vypnuto*): zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware, tj. 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 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 testovat 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

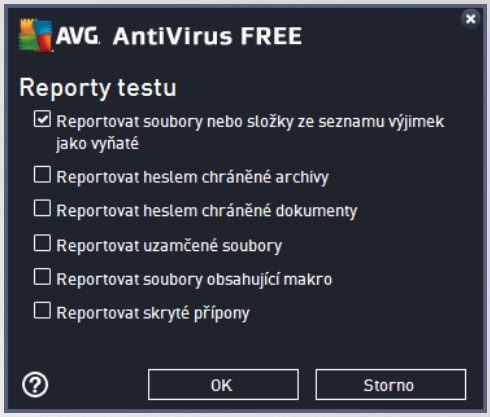
V této sekci pak můžete nastavit požadovanou rychlost testování v závislosti na zátěži systémových zdrojů. Ve výchozím nastavení je tato hodnota nastavena na úroveň ***Dle činnosti uživatele***, což znamená, že je využito minimum systémových prostředků ve chvíli, kdy s počítačem pracujete, a naopak maximum ve chvíli, kdy s počítačem nepracujete.

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.

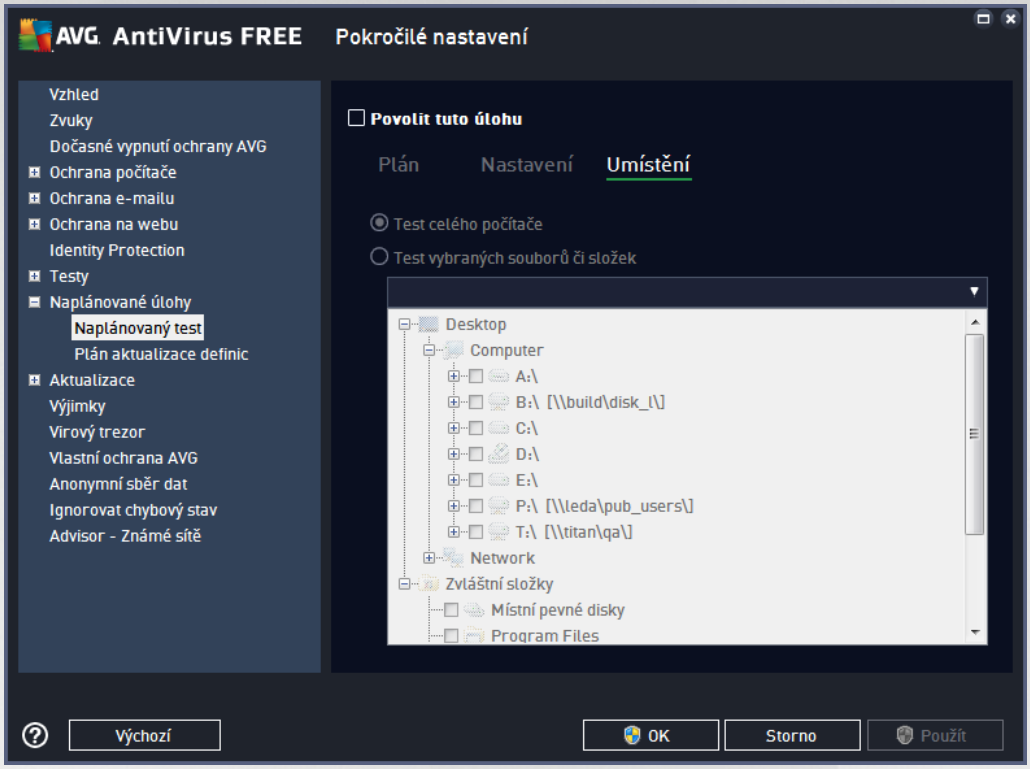
Nastavit další reporty testů

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:



Možnosti vypnutí počítače

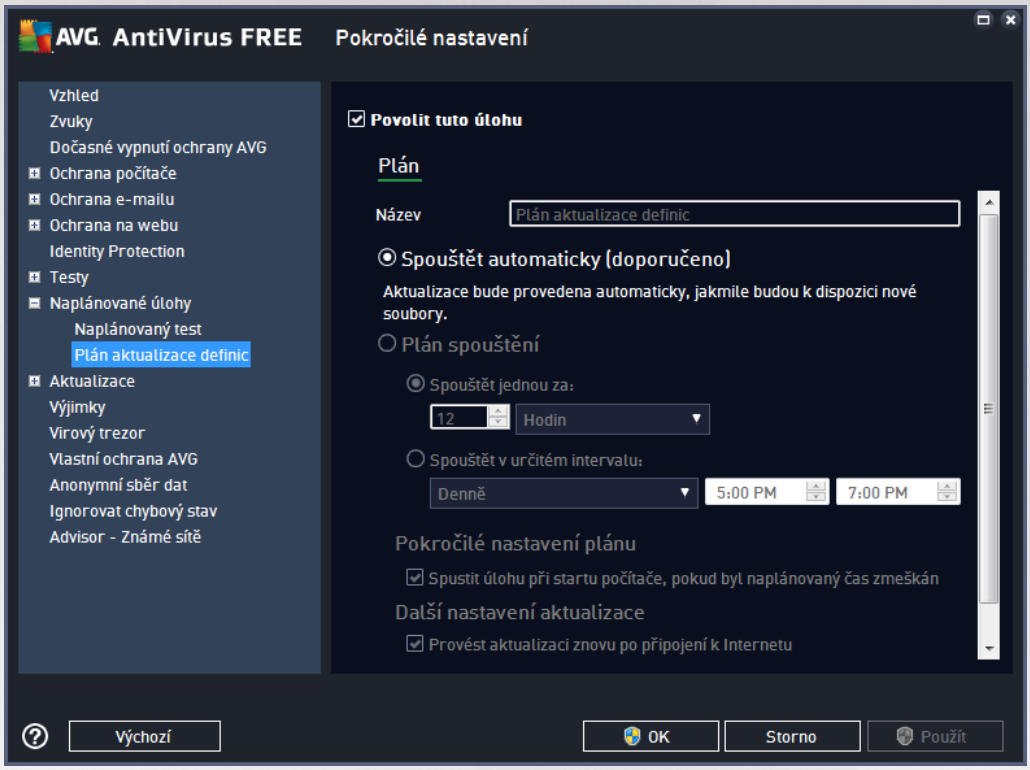
V sekci ***Možnosti vypnutí počítače*** můžete zvolit, zda má být po dokončení spuštěného testu počítač automaticky vypnut. Pokud potvrdíte tuto volbu (***Vypnout počítač po dokončení testování***), aktivuje se současně další možnost, jejímž zapnutím vynutíte vypnutí počítače i za situace, že počítač bude ve chvíli dokončení testu zamčen (***Vynutit vypnutí počítače, pokud je uzamčen***).



Na záložce ***Umístění*** 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.

7.9.2. Plán aktualizace definic

Na záložce ***Plán*** máte nejprve možnost jednoduchým označením položky ***Povolit tuto úlohu*** naplánovanou aktualizaci *(dočasně)* deaktivovat, a později podle potřeby znovu použít.



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

Ve výchozím nastavení je úloha spouštěna automaticky (***Spouštět automaticky***) vždy, jakmile je k dispozici nová aktualizace. V rámci **AVG AntiVirus Free Edition** není bohužel možnost osobního nastavení dostupná. *Pokud máte zájem o využití této možnosti a všech dalších ochranných prvků některé z profesionálních edic, navštivte prosím web AVG (http://www.avg.cz/), kde najdete informace o možnostech koupě placených produktů AVG.*

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.

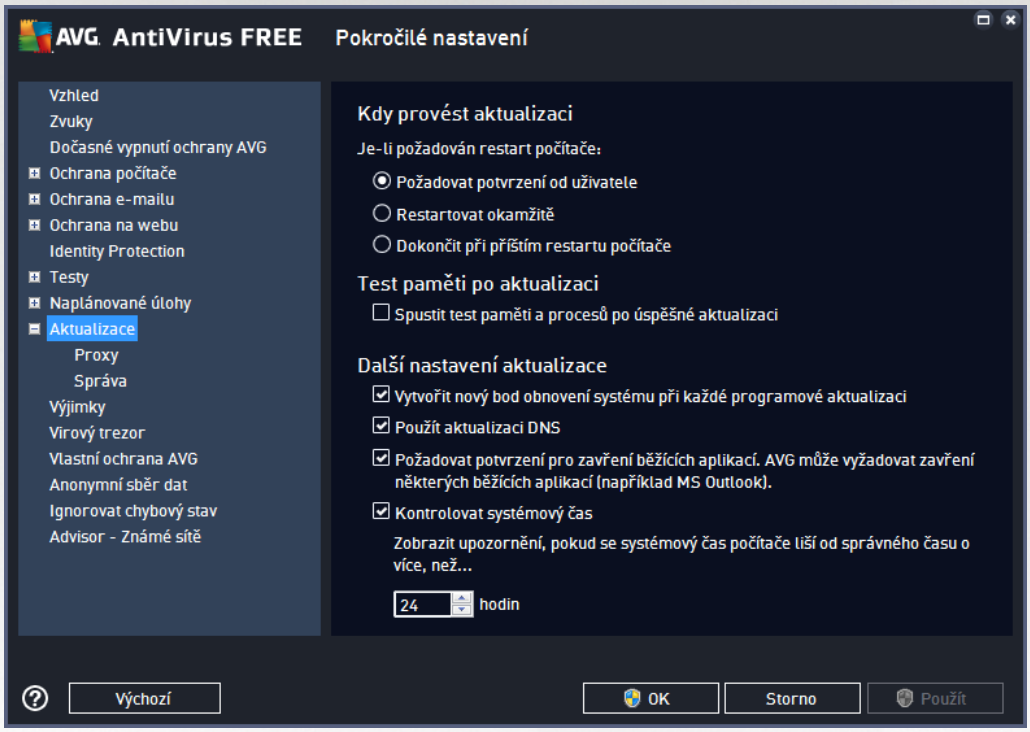
Další nastavení aktualizace

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)*.

7.10. 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:

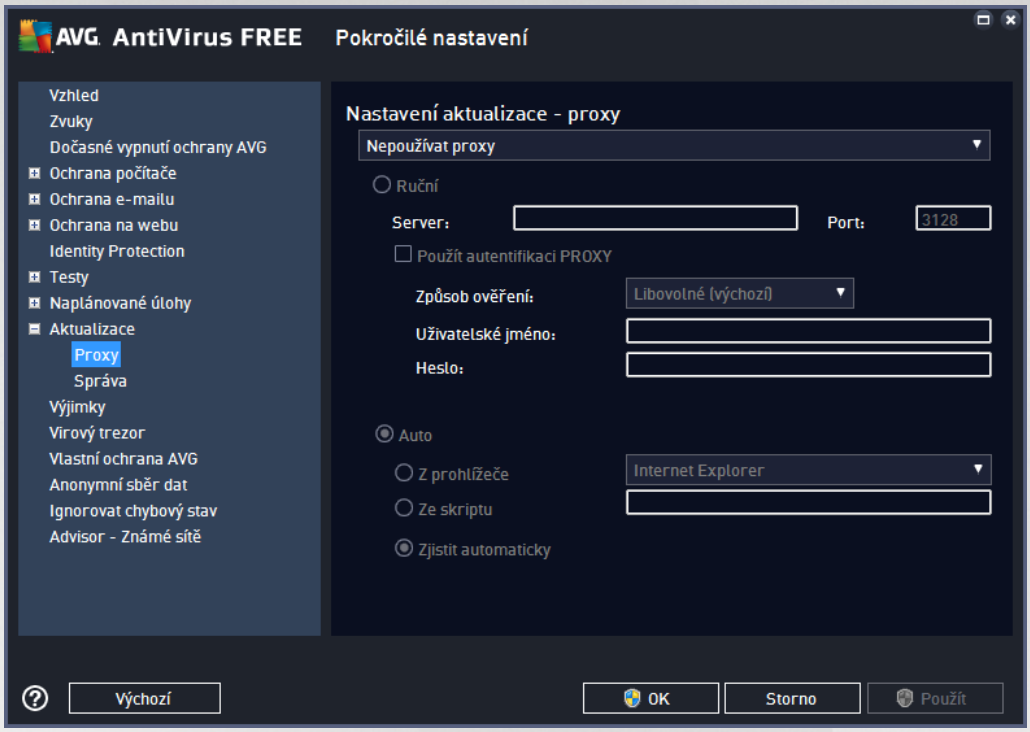
- ***Vytvořit nový bod pro obnovení systému při každé programové aktualizaci*** (*ve výchozím nastavení zapnuto*) - před každým spuštěním programové aktualizace AVG je tak zvaný systémový bod pro obnovení systému. V případě, že aktualizační proces nebude z nějakého důvodu dokončen a váš operační systém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

- ***Použít aktualizaci DNS*** (*ve výchozím nastavení zapnuto*) - pokud je tato položka označena, při spuštění aktualizace **AVG AntiVirus Free Edition** 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 zapnuto*) 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*** (*ve výchozím nastavení zapnuto*) - 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.

7.10.1. 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:

- ***Nepoužívat proxy -*** výchozí nastavení
- ***Použít proxy***
- ***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.

Ruční nastavení

Při manuálním nastavení (*volba **Ruční** 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.

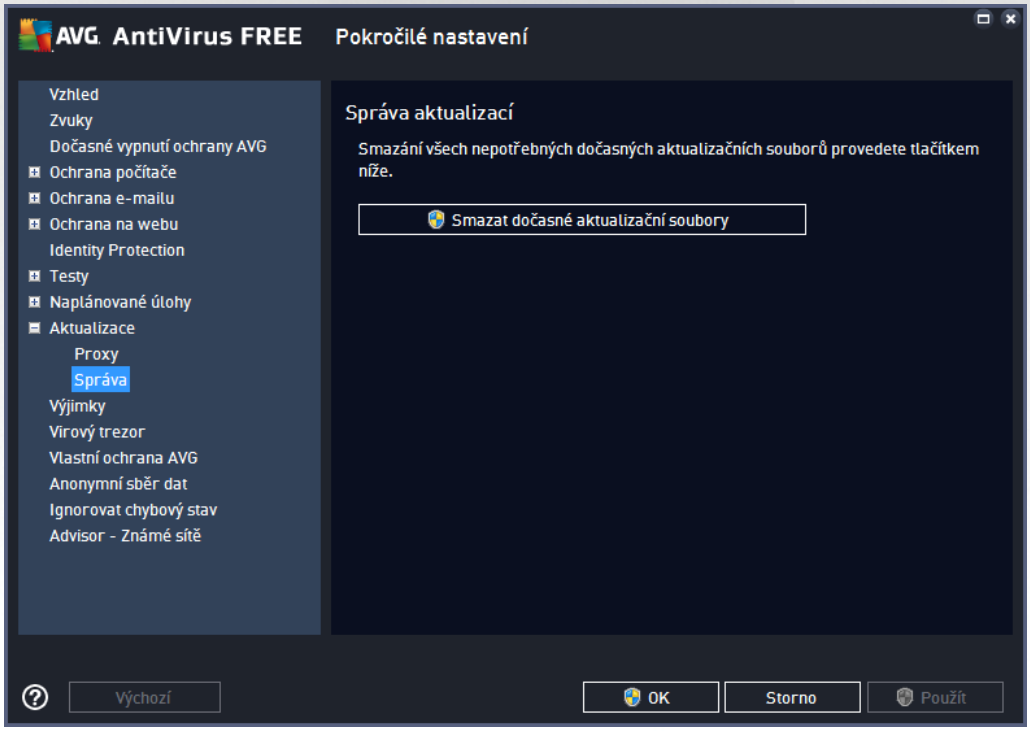
Automatické nastavení

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

- ***Z prohlížeče*** - nastavení se převezme z vašeho internetového 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

7.10.2. Správa

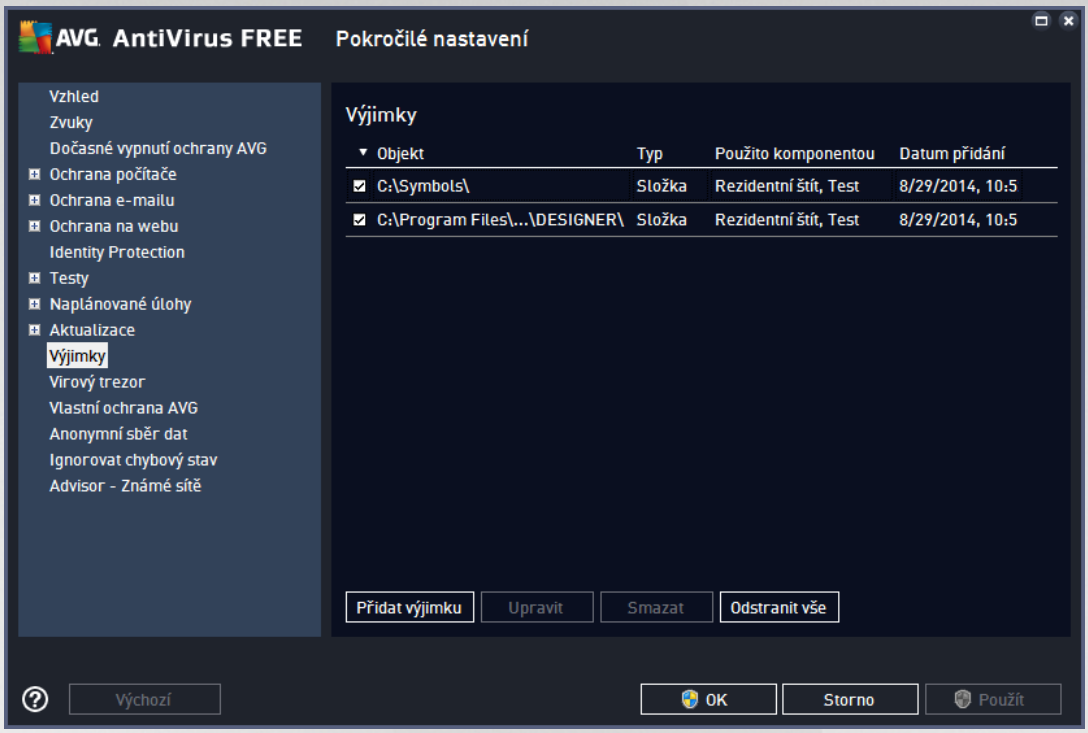
Dialog ***Správa aktualizací*** obsahuje jedinou akci v podobě tlačítka nazvaného ***Smazat dočasné aktualizační soubory*** - tímto tlačítkem odstraníte ze svého pevného disku všechny již nepotřebné soubory aktualizací (*ve výchozím nastavení správy aktualizačních souborů se tyto uchovávají po dobu 30 dní*):



7.11. Výjimky

V dialogu ***Výjimky*** můžete definovat výjimky, to jest položky, které budou z kontroly programem **AVG AntiVirus Free Edition** vyňaty. Výjimku jmůžete definovat například v situaci, kdy AVG opakovaně detekuje určitý program nebo soubor jako hrozbu nebo blokuje webovou stránku, o níž bezpečně víte, že ji lze považovat za bezpečnou. Pak přidáte dotyčný soubor nebo webovou stránku na seznam výjimek a AVG tyto objekty nadále nebude reportovat jako možný zdroj nákazy.

Na seznam výjimek přidávejte pouze ty soubory, programy či webové stránky, které lze s naprostou jistotou označit za bezpečné!



Tabulka v dialogu zobrazuje seznam již definovaných výjimek. Každá položka má vedle sebe zaškrtávací políčko. Je-li políčko označeno, je výjimka aktuálně platná a definovaný objekt tedy není předmětem kontroly. Jestliže je položka uvedena v seznamu, ale není označena, znamená to, že jste ji sice definovali jako výjimku, ale v tuto chvíli není aktivována a uvedený objekt podléhá kontrole programem AVG. Položky v seznamu můžete řadit podle jednotlivých parametrů, a to tak, že kliknete na záhlaví sloupce, jehož charakteristiku chcete použít jako kritérium řazení položek.

Ovládací prvky dialogu

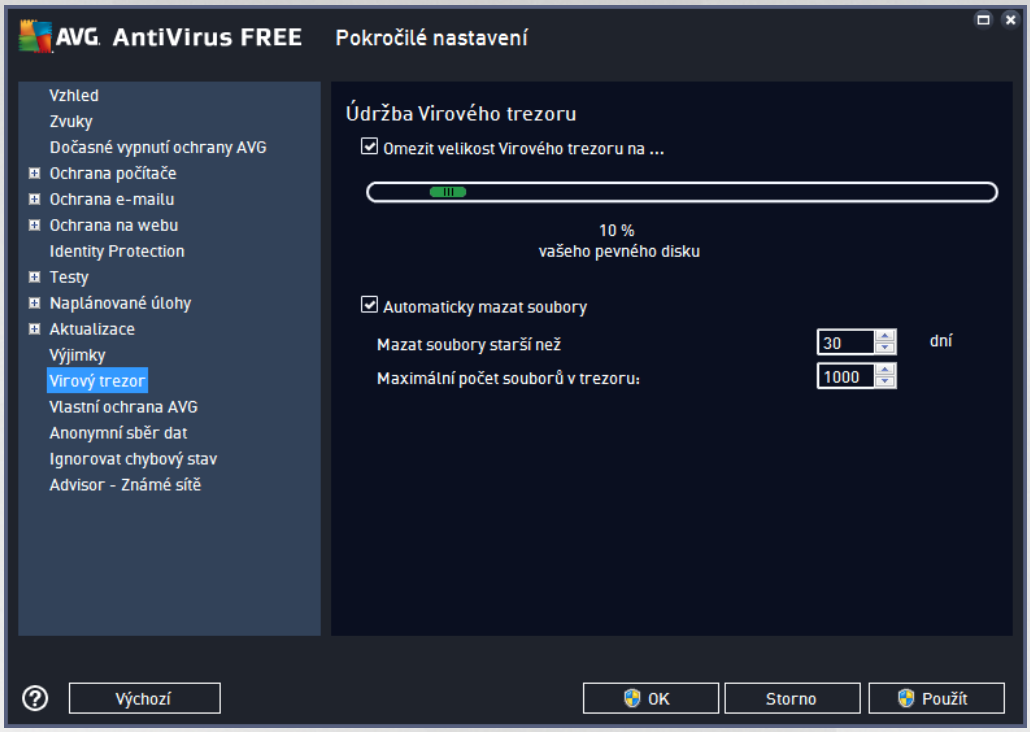
- ***Přidat výjimku*** - Kliknutím na tlačítko otevřete nový dialog, v němž lze specifikovat objekty, jež mají být vyňaty z kontroly programem AVG. Nejprve musíte určit, o jaký typ objektu se jedná: zda jde o soubor, adresář, nebo o webovou stránku. Pak prohlížením disku určíte přesnou cestu k danému objektu nebo zadáte konkrétní URL. Nakonec budete vyzváni, abyste rozhodli, které bezpečnostní služby AVG mají definovaný objekt vynechat ze své kontroly *(Rezidentní štít, Identity Protection, Test)*.

- ***Upravit*** - Tlačítko je aktivní, pouze pokud jsou již definovány a v seznamu uvedeny nějaké výjimky. Stiskem tlačítka pak otevřete editační dialog, v němž můžete upravovat nastavené parametry zvolené výjimky.

- ***Smazat*** - Tlačítkem lze smazat dříve definované výjimky ze seznamu. Výjimky můžete buďto odstranit jednu po druhé nebo označit v seznamu celý blok výjimek a smazat je jednorázově. Po smazání definované výjimky bude objekt, jehož se výjimka týkala, opět považován za předmět kontroly AVG. Odstraněním výjimky nemažete ten který soubor nebo adresář, ale pouze nastavení pravidel pro tento objekt!

- ***Odstranit vše*** - Tlačítkem odstraníte veškeré dosud definované výjimky.

7.12. Virový trezor

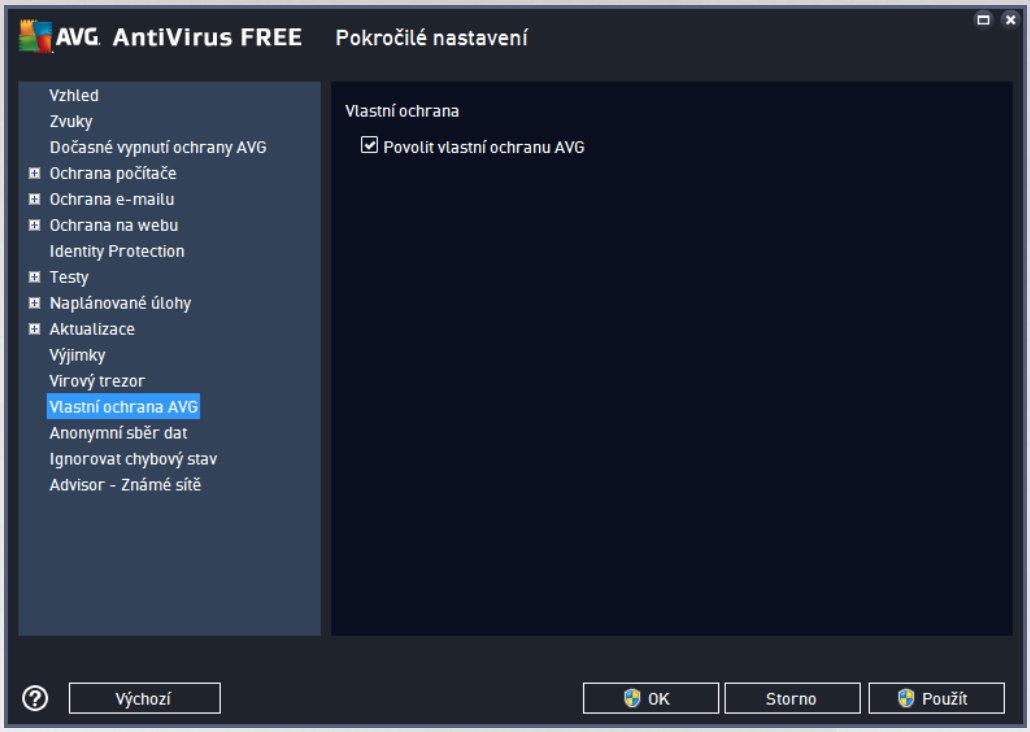


Dialog ***Údržba Virového trezoru*** umožňuje definovat několik parametrů souvisejících se správou objektů ve Virovém trezoru:

- ***Omezit velikost Virového trezoru na...*** - 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***).

7.13. Vlastní ochrana AVG

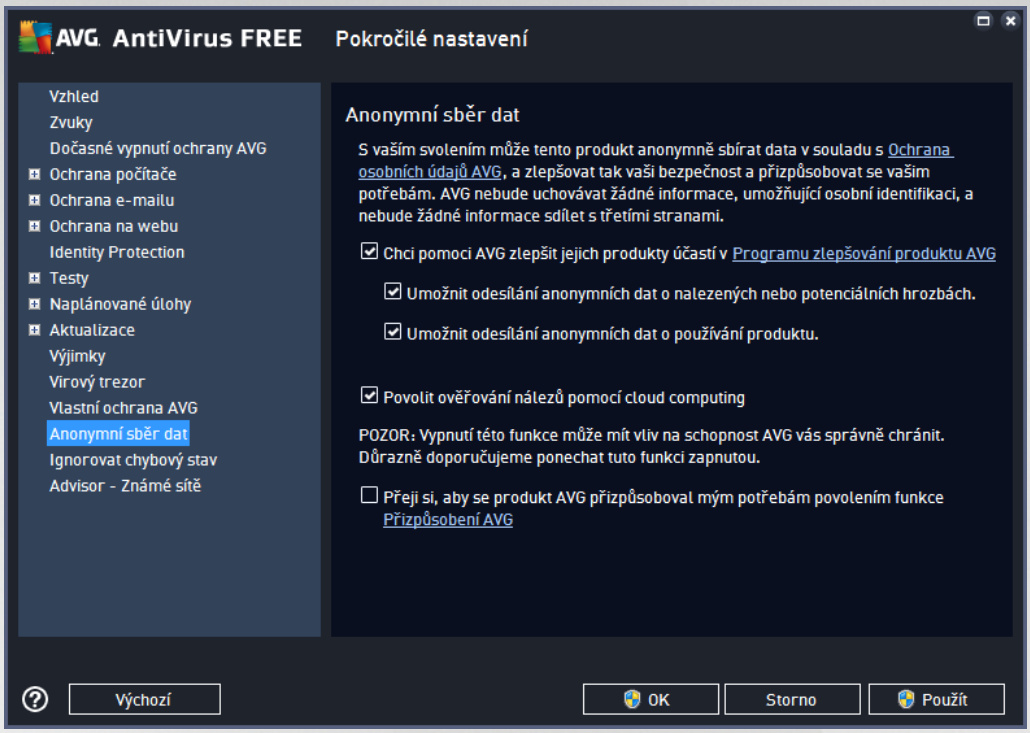


Funkce ***Vlastní ochrana*** slouží k nastavení ochrany vlastních procesů, souborů, registrových klíčů a ovladačů aplikace **AVG AntiVirus Free Edition** před jejich pozměněním či deaktivací. Důvodem implementace tohoto typu ochrany je existence sofistikovaných hrozeb, které se snaží zneškodnit antivirové programy a následně bez omezení poškodit váš počítač.

Doporučujeme, abyste tuto funkci nechali vždy zapnutou.

7.14. Anonymní sběr dat

V dialogu ***Anonymní sběr dat*** máte možnost zapojit se do spolupráce a podílet se na zlepšování produktu AVG a na celkovém zvýšení úrovně bezpečnosti na Internetu. Vaše 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.

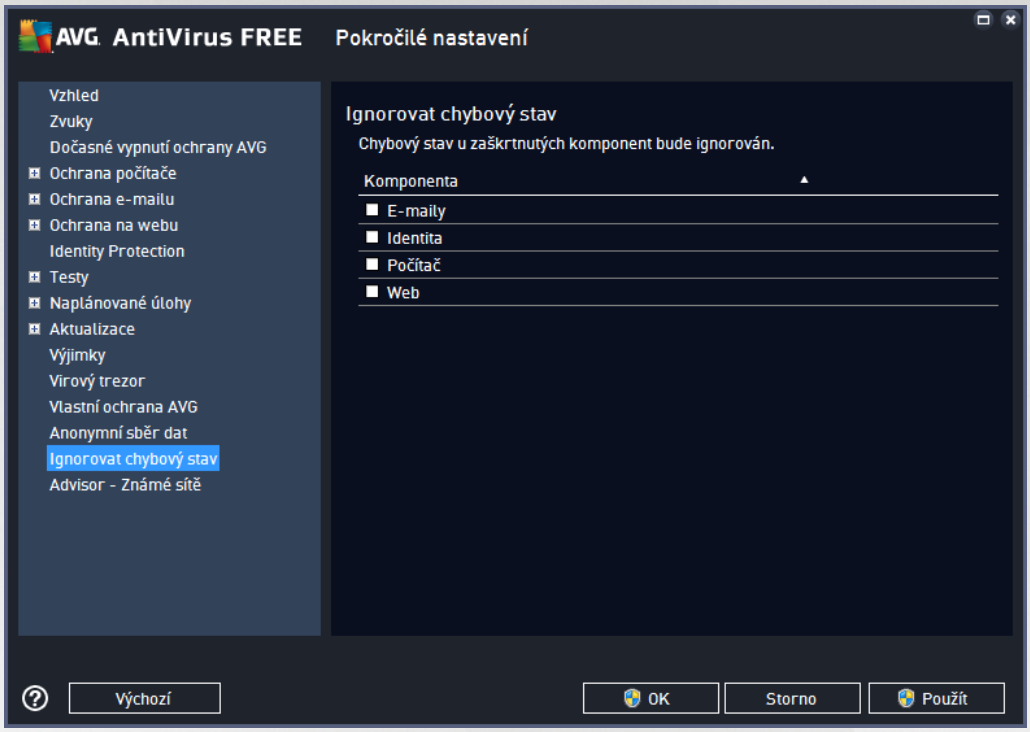


V dialogu najdete tyto možnosti nastavení:

- ***Chci pomoci AVG zlepšit jejich produkty účastí v Programu zlepšování produktu AVG*** (*ve výchozím nastavení vypnuto*) - 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 odesílání anonymních dat o nalezených nebo potenciálních hrozbách*** (*ve výchozím nastavení vypnuto*) - 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 vypnuto*) - 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)*.
- ***Přeji si, aby se produkt AVG přizpůsoboval mým potřebám povolením funkce Přizpůsobení AVG*** (*ve výchozím nastavení vypnuto*) - tato funkce anonymně analyzuje chování programů a aplikací, jež máte instalovány na svém počítači. Na základě této analýzy vám AVG dokáže nabídnout přesně zacílené služby, případně další produkty pro vaši maximální bezpečnost.

7.15. 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.

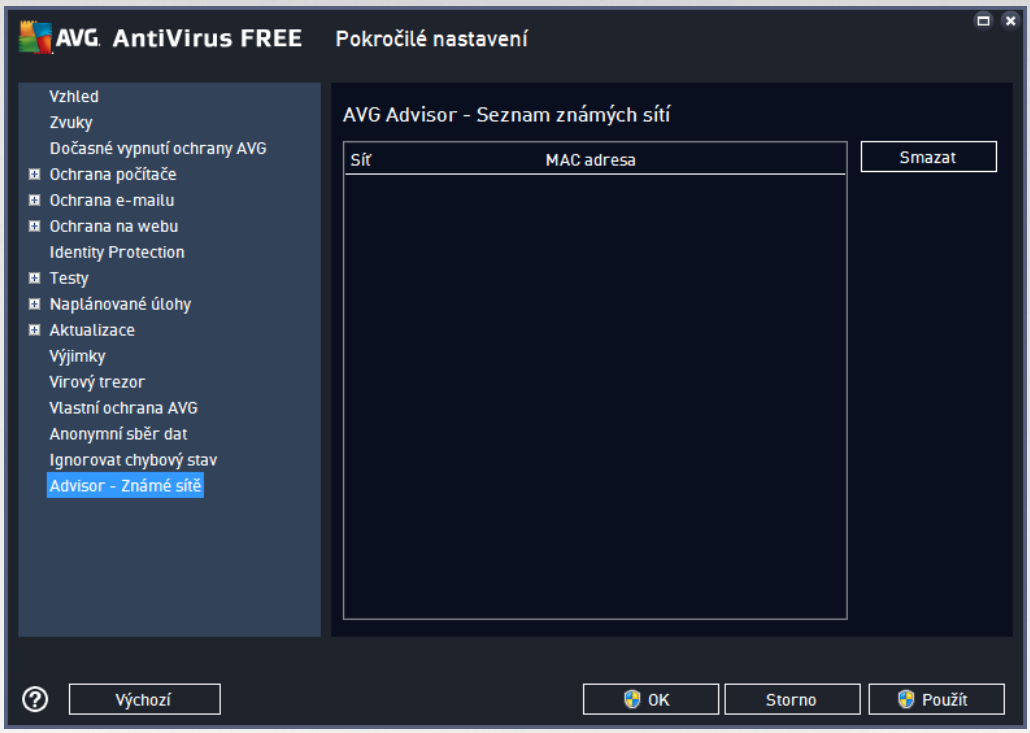
V dialogu ***Ignorovat chybový stav*** máte tedy možnost označit ty komponenty, jejichž případný chybový stav (*to znamená i jejich vypnutí*) nemá být hlášen. Můžete označit libovolnou komponentu nebo i několik komponent v seznamu. Svou volbu potvrďte stiskem tlačítka ***OK***.

7.16. 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:



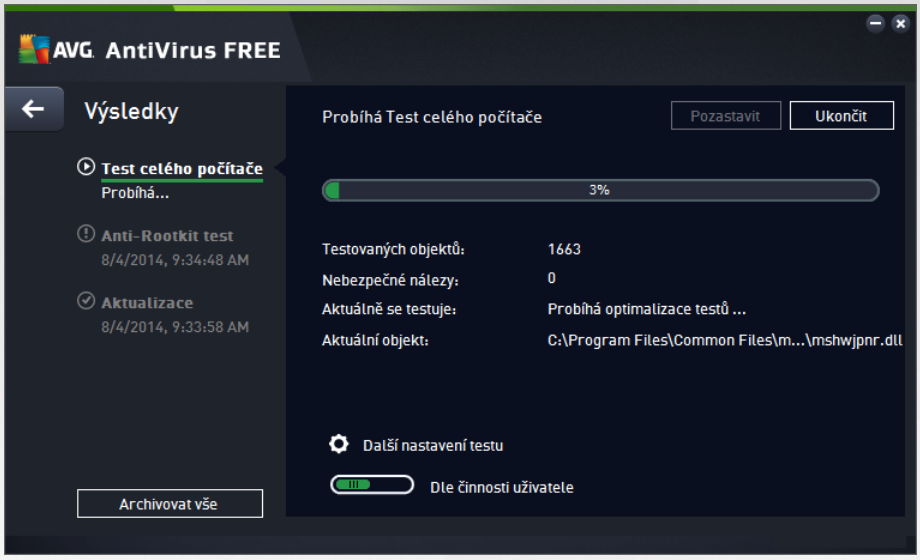
Poznámka: *Funkce známé sítě v rámci služby AVG Advisor není podporována na Windows XP 64-bit.*

8. AVG testování

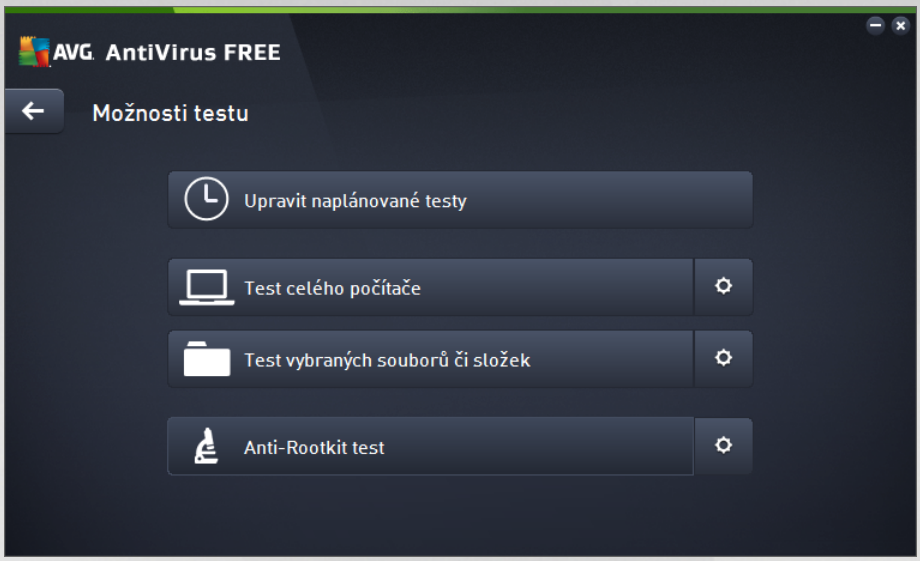
Ve výchozím nastavení **AVG AntiVirus Free Edition** se nespouští žádný test automaticky, protože po úvodním otestování počítače *(k jehož spuštění budete vyzváni)* jste průběžně chráněni rezidentními komponentami **AVG AntiVirus Free Edition**, které eventuelní škodlivý kód zachycují okamžitě. Samozřejmě ale můžete naplánovat test k pravidelnému spouštění v určený čas, případně kdykoli spustit ručně libovolný test podle vlastních požadavků.

Testovací rozhraní AVG je dostupné z hlavního uživatelského rozhraní prostřednictvím tlačítka sestávajícího ze dvou částí: 

- ***Spustit test*** - Stiskem této volby dojde k okamžitému spuštění Testu celého počítače. O průběhu a výsledku testu budete následně vyrozuměni v automaticky otevřeném okně Výsledky:



- ***Možnosti testu*** - Volbou této položky *(graficky znázorněné jako tři vodorovné čárky v zeleném poli)* přejdete do dialogu ***Možnosti testu***, kde můžete spravovat naplánované testy a editovat parametry testů:



V dialogu ***Možnosti testu*** jsou zobrazeny tři hlavní sekce pro konfiguraci testů:

- ***Upravit naplánované testy*** - Volbou této možnosti otevřete nový dialog s přehledem naplánovaných testů. V rámci **AVG AntiVirus Free Edition** není bohužel možné plánovat vlastní testy, takže v tabulkovém přehledu bude uveden jen jeden test definovaný výrobcem. Tento test je ve výchozím nastavení vypnutý. Kliknutím pravého tlačítka myši nad tímto definovaným testem rozbalíte kontextové menu a volbou položky *Povolit úlohu* test aktivujete. Jakmile je test aktivován, můžete editovat jeho konfiguraci prostřednictvím tlačítka *Upravit plán testu*.

- ***Test celého počítače / Nastavení*** - Tlačítko je rozděleno do dvou částí. Klikněte na možnost *Test celého počítače* a okamžitě spustíte kompletní testování vašeho počítače *(podrobnosti o testu celého počítače najdete v příslušné kapitole nazvané Přednastavené testy / Test celého počítače)*. Kliknutím na položku *Nastavení* přejdete do konfiguračního dialogu testu celého počítače.

- ***Test vybraných souborů či složek / Nastavení*** - I toto tlačítko je rozděleno do dvou částí. Klikněte na volbu *Test vybraných souborů či složek*, a tím okamžitě spustíte testování vybraných oblastí vašeho počítače *(podrobnosti o testu vybraných souborů a složek najdete v příslušné kapitole nazvané Přednastavené testy / Test vybraných souborů a složek)*. Kliknutím na položku *Nastavení* přejdete do konfiguračního dialogu testu vybraných souborů či složek.

- ***Prohledat počítač na přítomnost rootkitů / Nastavení*** - První část tlačítka označená textem *Prohledat počítač na přítomnost rootkitů* spouští rootkit testování *(podrobnosti o rootkit testu najdete v příslušné kapitole nazvané Přednastavené testy / Prohledat počítač na přítomnost rootkitů)*. Kliknutím na položku *Nastavení* přejdete do konfiguračního dialogu Nastavení Anti-Rootkitu.

8.1. Přednastavené testy

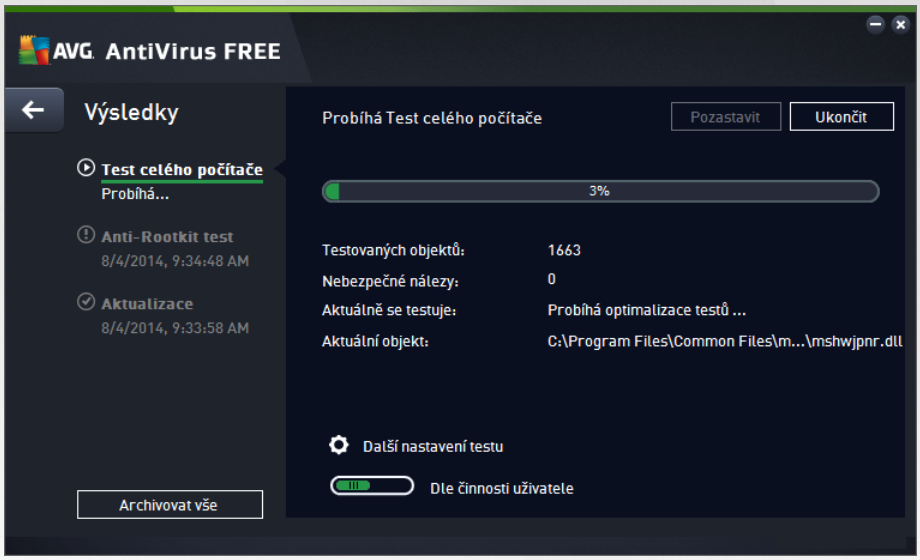
Jednou z hlavních funkcí **AVG AntiVirus Free Edition** je testování na vyžádání. Testy na vyžádání jsou navrženy tak, že mohou testovat různé části vašeho počítače, kdykoliv se objeví podezření na možnost virové infekce. V každém případě však doporučujeme provádět testy pravidelně, i když považujete váš počítač za zcela viru prostý. V **AVG AntiVirus Free Edition** najdete tyto typy výrobcem nastavených testů:

8.1.1. Test celého počítače

Test celého počítače zkontroluje celý počítač a ověří případnou přítomnost virů a potenciálně nežádoucích aplikací. 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.

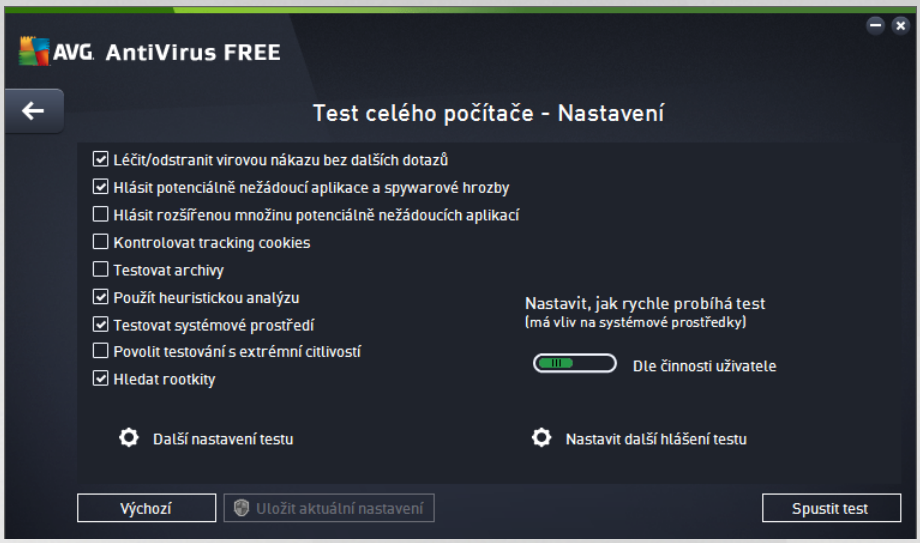
Spuštění testu

Test celého počítače spusťte přímo z hlavního uživatelského rozhraní kliknutím na graficky znázorněnou položku ***Spustit test***. U tohoto testu již není potřeba žádné další specifické nastavení, test bude tedy rovnou spuštěn a v dialogu ***Probíhá Test celého počítače*** (*viz obrázek*) můžete sledovat jeho průběh. Test můžete podle potřeby kdykoliv dočasně ***Pozastavit*** nebo ***Ukončit***.



Editace nastavení testu

Předem definované výchozí nastavení ***Testu celého počítače*** máte možnost editovat v dialogu ***Test celého počítače - Nastavení*** *(ten je dostupný prostřednictvím odkazu Nastavení u Testu celého počítače z dialogu Možnosti testu)*. ***Pokud však nemáte skutečný důvod konfiguraci testu měnit, doporučujeme se podržet výrobcem definovaného nastavení!***



V seznamu parametrů testu můžete jednotlivé volby podle potřeby vypínat/zapínat:

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

- ***Hlásit Potenciálně nežádoucí aplikace a spywarové hrozby*** *(ve výchozím nastavení zapnuto)*: kontrola přítomnosti potenciálně nežádoucích aplikací *(spustitelné programy, které mohou fungovat jako spyware nebo adware)*. Zaškrtnutím tohoto políčka aktivujete testování přítomnosti 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 ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.

- ***Hlásit rozšířenou množinu potenciálně nežádoucích aplikací*** *(ve výchozím nastavení vypnuto)*: zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware, tj. 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 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 testovat všechny soubory zabalené v některém typu archivu, například ZIP, RAR, ...

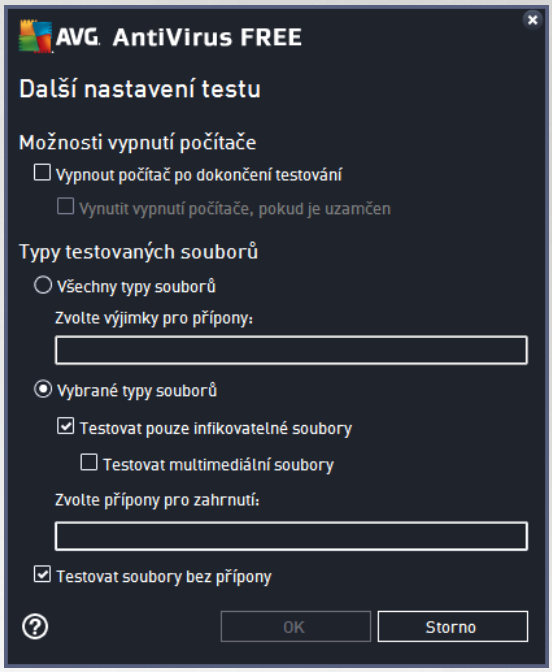
- ***Použít heuristickou analýzu*** *(ve výchozím nastavení zapnuto)*: během testu bude použita k detekci infekce i metoda heuristické analýzy *(dynamické emulace instrukcí testovaného objektu v prostředí virtuálního počítače)*.

- ***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)*: zahrne do testu celého počítače i ověření přítomnosti rootkitů, které lze spustit i jako samostatný anti-rootkit test.

- ***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.

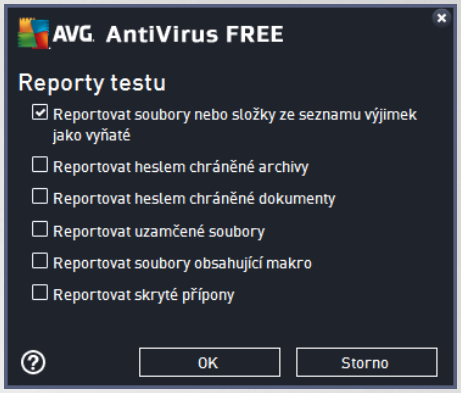
    - ***Vybrané typy souborů*** - můžete se rozhodnout, že chcete, aby se testy spouštěly pouze nad soubory, které lze považovat za infikovatelné (*soubory, které nemohou být infekcí zasaženy, se testovat nebudou - například prosté textové soubory nebo některé nespustitelné soubory*), a to včetně multimediálních 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 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 hlášení testů*** - odkaz otevírá nový dialog ***Reporty testu***, v němž můžete označit, které typy nálezů mají být hlášeny:



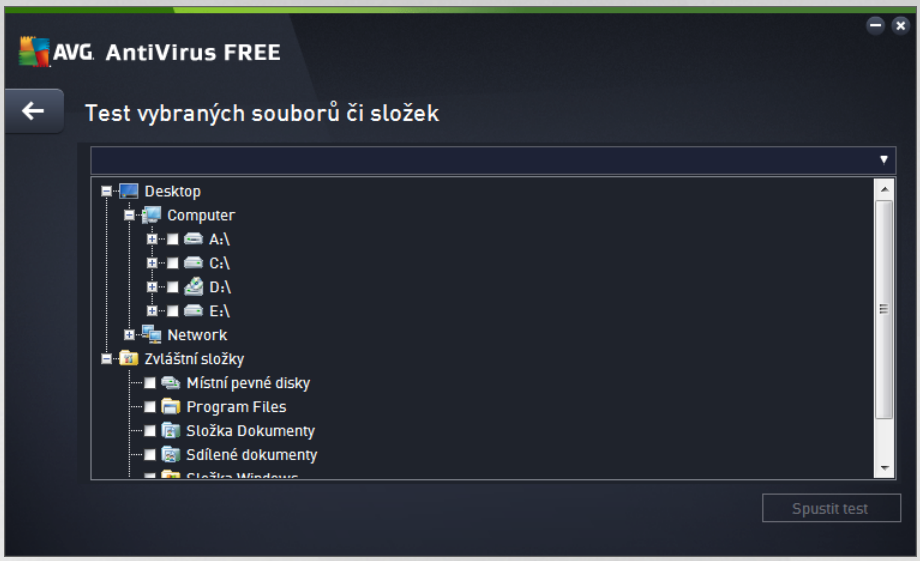
Upozornění: *Samotné možnosti nastavení testu jsou shodné s parametry nově definovaného testu, které jsou podrobně popsány v kapitole AVG testování / Naplánování testu / Jak testovat. Pokud se rozhodnete výchozí nastavení* ***Testu celého počítače*** *změnit, můžete pak svou konfiguraci uložit jako výchozí,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

8.1.2. 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.

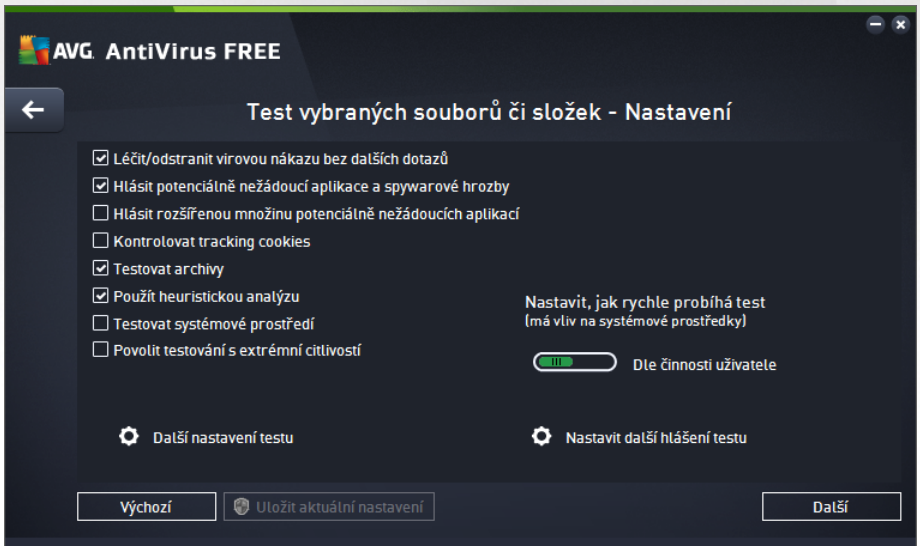
Spuštění testu

Test vybraných souborů či složek spusťte přímo z dialogu Možnosti testu kliknutím na graficky znázorněnou položku ***Test vybraných souborů či složek***. Otevře se rozhraní ***Test vybraných souborů či složek***, kde můžete v graficky znázorněné stromové struktuře vašeho počítače označit 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 ***Test vybraných souborů či složek - Nastavení*** *(ten je dostupný prostřednictvím odkazu Nastavení u Testu vybraných souborů či složek z dialogu Možnosti testu)*. ***Pokud však nemáte skutečný důvod konfiguraci testu měnit, doporučujeme se podržet výrobcem definovaného nastavení!***



V seznamu parametrů testu můžete jednotlivé volby podle potřeby vypínat/zapínat:

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

- ***Hlásit Potenciálně nežádoucí aplikace a spywarové hrozby*** *(ve výchozím nastavení zapnuto)*: Kontrola přítomnosti potenciálně nežádoucích aplikací (spustitelné programy, které mohou fungovat jako spyware nebo adware). Zaškrtnutím tohoto políčka aktivujete testování přítomnosti 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 ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.

- ***Hlásit rozšířenou množinu potenciálně nežádoucích aplikací*** *(ve výchozím nastavení vypnuto)*: Zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware, tj. 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 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)*.

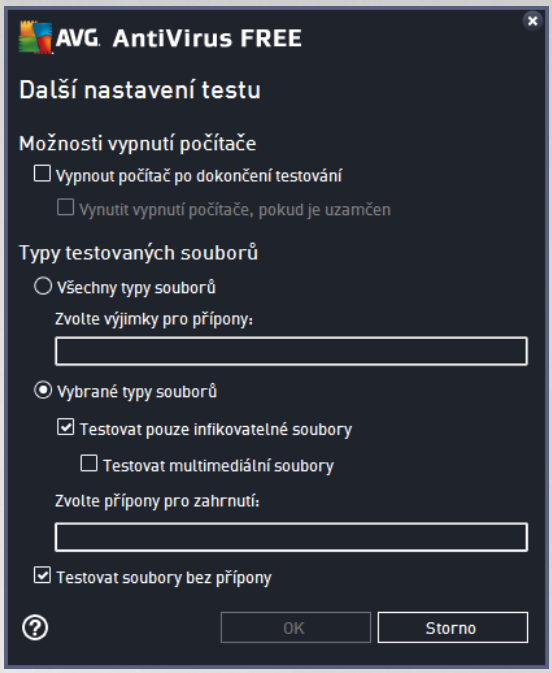
- ***Testovat archivy*** *(ve výchozím nastavení zapnuto)*: Parametr definuje, že test má testovat všechny soubory zabalené v některém typu archivu, například ZIP, RAR, ...

- ***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

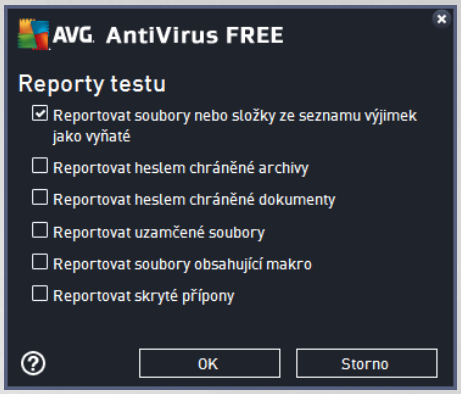
  - ***Všechny typy souborů*** - přičemž máte zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou.

  - ***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.

- ***Nastavit, jak rychle probíhá test*** - 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 hlášení testů*** - odkaz otevírá nový dialog ***Reporty testu***, v němž můžete označit, které typy nálezů mají být hlášeny:



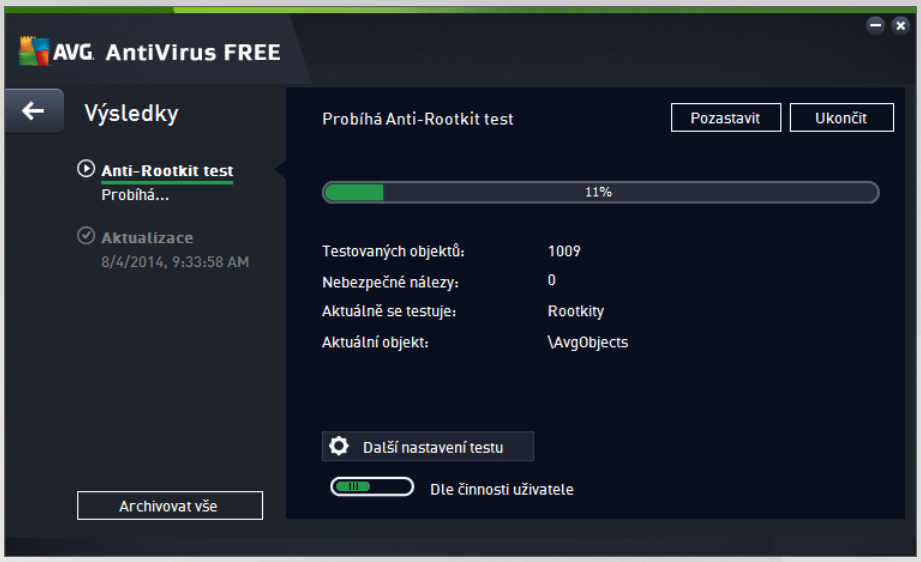
Upozornění: *Samotné možnosti nastavení testu jsou shodné s parametry nově definovaného testu, které jsou podrobně popsány v kapitole AVG testování / Naplánování testu / Jak testovat. Pokud se rozhodnete výchozí nastavení* ***Testu vybraných souborů či složek*** *změnit, můžete pak svou konfiguraci uložit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

8.1.3. Prohledat počítač na přítomnost rootkitů

Prohledat počítač na přítomnost rootkitů detekuje a účinně odstraní nebezpečné rootkity, to jest programy a technologie, které dokáží maskovat přítomnost zákeřného software v počítači. Rootkit je program speciálně vytvořený tak, aby dokázal převzít kontrolu nad vaším počítačem, aniž by požádal o jakoukoliv autorizaci. Test je schopen detekovat rootkit na základě definovaných pravidel. 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.

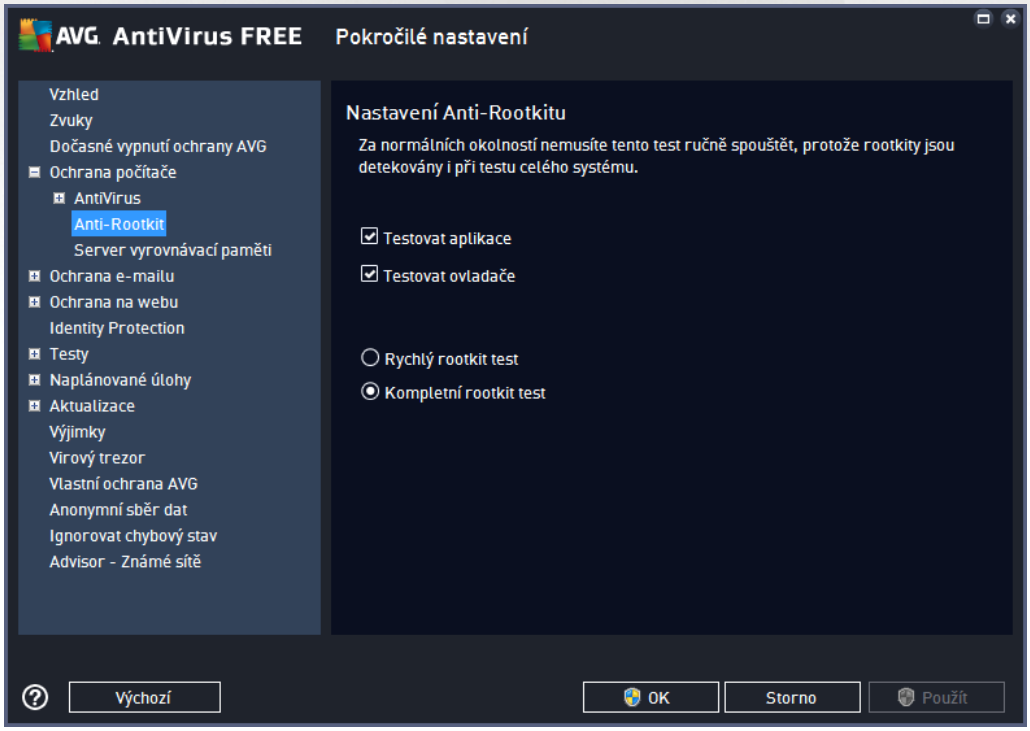
Spuštění testu

Prohledat počítač na přítomnost rootkitů spusťte přímo z dialogu Možnosti testu kliknutím na graficky znázorněnou položku ***Prohledat počítač na přítomnost rootkitů***. Otevře se rozhraní ***Probíhá Anti-Rootkit test***, v němž můžete sledovat průběh testu:



Editace nastavení testu

Předem definované výchozí nastavení ***Testu celého počítače*** máte možnost editovat v dialogu ***Test celého počítače - Nastavení*** *(ten je dostupný prostřednictvím odkazu Nastavení u Testu celého počítače z dialogu Možnosti testu)*. ***Pokud však nemáte skutečný důvod konfiguraci testu měnit, doporučujeme se podržet výrobcem definovaného nastavení!***

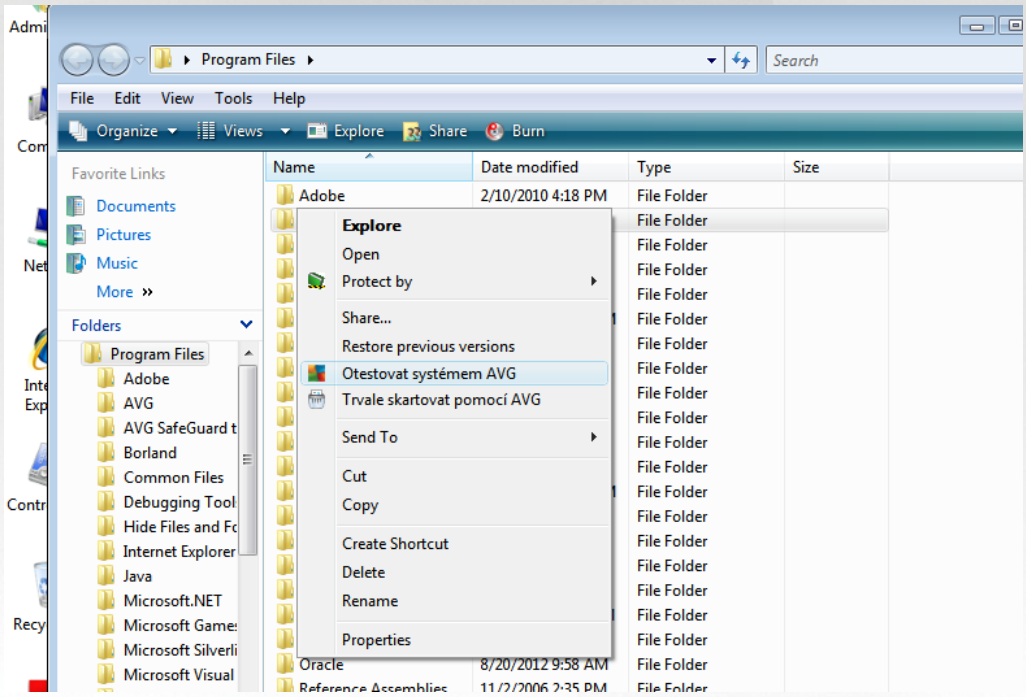


Možnosti ***Testovat aplikace*** a ***Testovat ovladače*** umožňují určit, co vše má být v testu na rootkity zahrnuto. Jiné než výchozí nastavení doporučujeme pouze zkušeným uživatelům; jinak prosím ponechte všechny možnosti zapnuté. Dále se pak můžete rozhodnout, v jakém režimu si přejete test spustit:

- ***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*)

8.2. Testování v průzkumníku Windows

AVG AntiVirus Free Edition 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*** necháte objekt otestovat programem **AVG AntiVirus Free Edition**

8.3. Testování z příkazové řádky

V rámci **AVG AntiVirus Free Edition** 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

8.3.1. 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:***

8.3.2. 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***.

8.3.3. 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:

Test samotný bude spuštěn z příkazové řádky. Uvedený dialog slouží pouze jako nástroj pro snadné nastavení parametrů testu, aniž byste je museli definovat v prostředí příkazové řádky.

8.3.4. Parametry CMD testu

V následujícím přehledu nabízíme seznam dostupných parametrů testu:

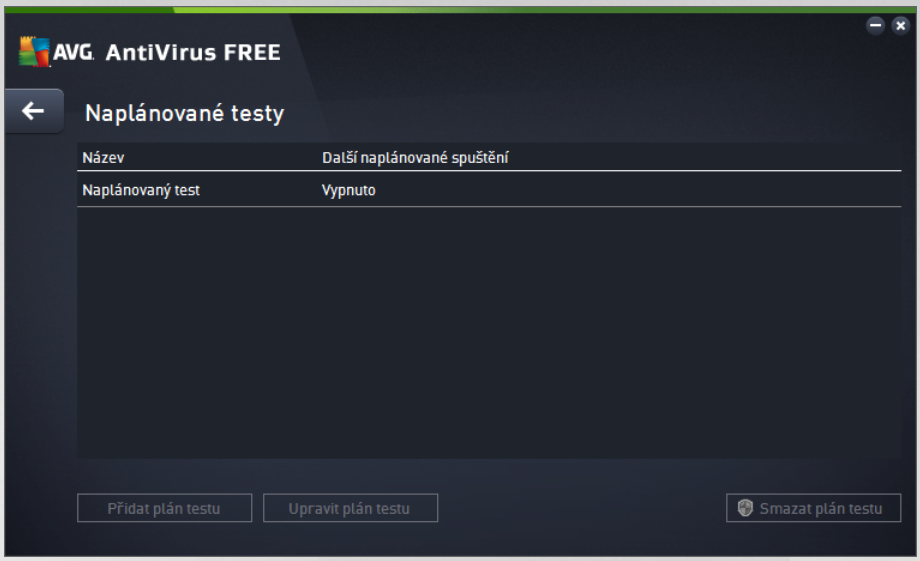
- /SCAN Test vybraných souborů či složek; /SCAN=path;path *(například /SCAN=C:\;D:\)*
- /COMP Test celého počítače
- /HEUR Použít heuristickou analýzu
- /EXCLUDE Z testu vynechat tuto cestu nebo soubory
- /@ Příkazový soubor /jméno souboru/
- /EXT Testovat pouze soubory s těmito příponami /například EXT=EXE,DLL/
- /NOEXT Netestovat soubory s těmito příponami /například NOEXT=JPG/
- /ARC Testovat archívy
- /CLEAN Automaticky léčit
- /TRASH Přesunout infikované soubory do Virového trezoru
- /QT Rychlý test
- /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 nežádoucí aplikace
- /PUPEXT Hlásit rozšířenou množinu Potenciálně nežádoucích aplikací
- /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

8.4. Naplánování testu

Testy v **AVG AntiVirus Free Edition** 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 dialogu ***Naplánované testy***, který je dostupný prostřednictvím tlačítka ***Upravit naplánované testy*** z dialogu Možnosti testu. V nově otevřeném dialogu ***Naplánované testy*** pak uvidíte kompletní přehled všech aktuálně naplánovaných testů:

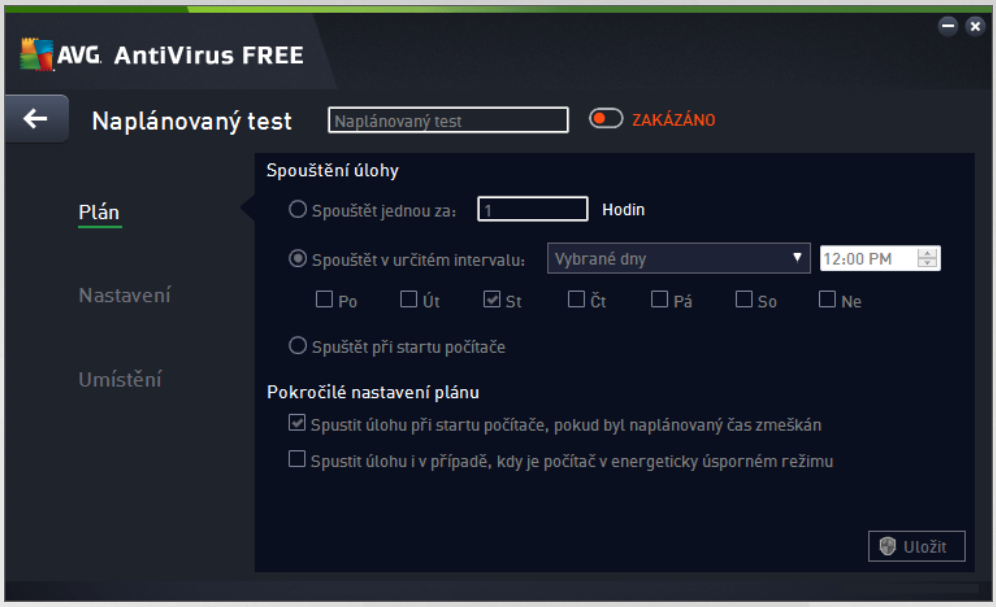


Dokud nenaplánujte vlastní testy, bude v tabulkovém přehledu uveden jen jeden test definovaný výrobcem. Tento test je ve výchozím nastavení vypnutý. Kliknutím pravého tlačítka myši nad tímto definovaným testem rozbalíte kontextové menu a volbou položky ***Povolit úlohu*** test aktivujete. Jakmile je test aktivován, můžete editovat jeho konfiguraci prostřednictvím tlačítka ***Upravit plán testu***. Pomocí tlačítka ***Přidat plán testu*** můžete také nastavit svůj vlastní naplánovaný test. Parametry naplánovaného testu můžete editovat (*případně nastavit plán nový*) na třech záložkách:

- Plán
- Nastavení
- Umístění

Na každé záložce máte nejprve možnost jednoduchým přepnutím semaforu naplánovaný test (*dočasně*) deaktivovat, a později podle potřeby znovu použít.

8.4.1. Plán



V textovém poli v horní části záložky ***Plán*** můžete zadat jméno, které si přejete přiřadit právě vytvářenému testu. Snažte se vždy používat stručné, popisné a případné názvy, abyste se později v naplánovaných úlohách snadněji vyznali. Například 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.

V 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)*.

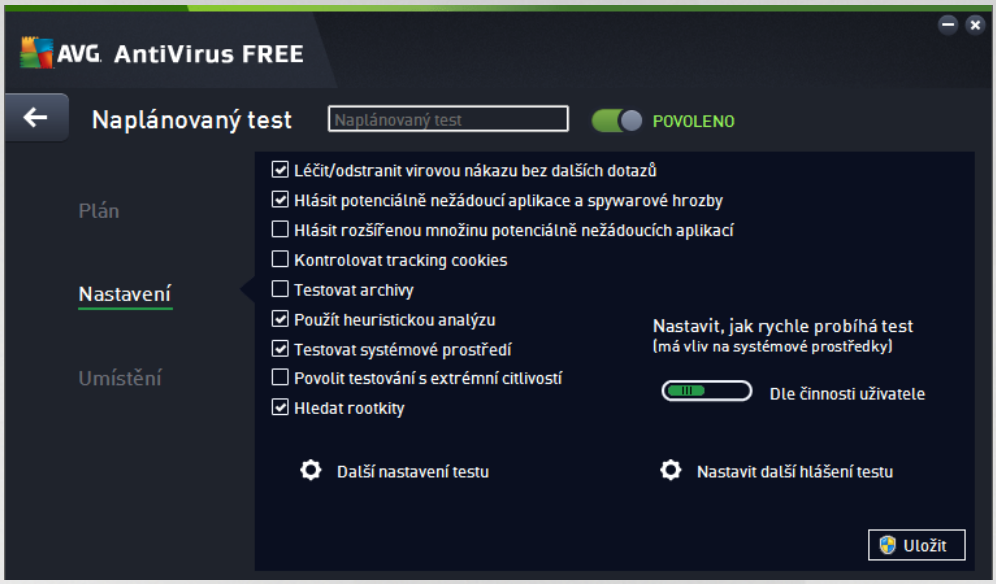
- ***Pokročilé nastavení plánu*** - Tato sekce umožňuje definovat podmínky, kdy má či nemá být test spuštěn, jestliže je počítač v úsporném režimu nebo zcela vypnutý a naplánovaný čas spuštění testu byl zmeškán. O automatickém spuštění testu budete v určeném čase informováni prostřednictvím pop-up okna nad ikonou AVG na systémové liště. Po zahájení testu se na systémové liště objeví nová ikona AVG *(barevná s probikávajícím 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.

Ovládací tlačítka 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 dialogu Naplánované testy. Chcete-li tedy nastavit parametry plánu testu na všech záložkách, uložte je stiskem tohoto tlačítka teprve poté, co jste zadali všechny své požadavky.

-  - Pomocí šipky v levé horní části dialogu se vrátíte zpět do přehledu naplánovaných testů.

8.4.2. Nastavení



V textovém poli v horní části záložky ***Nastavení*** můžete zadat jméno, které si přejete přiřadit právě vytvářenému testu. Snažte se vždy používat stručné, popisné a případné názvy, abyste se později v naplánovaných úlohách snadněji vyznali. Například 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.

Záložka ***Nastavení*** nabízí seznam parametrů testu, které můžete podle potřeby vypínat/zapínat. ***Pokud nemáte skutečný důvod konfiguraci testu měnit, doporučujeme se podržet výrobcem definovaného nastavení***:

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

- ***Hlásit potenciálně nežádoucí aplikace a spywarové hrozby*** (*ve výchozím nastavení zapnuto*): kontrola přítomnosti potenciálně nežádoucích aplikací (*spustitelné programy, které mohou fungovat jako spyware nebo adware*). Zaškrtnutím tohoto políčka aktivujete testování přítomnosti 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 ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.

- ***Hlásit rozšířenou množinu potenciálně nežádoucích aplikací*** (*ve výchozím nastavení vypnuto*): zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware, tj. 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.

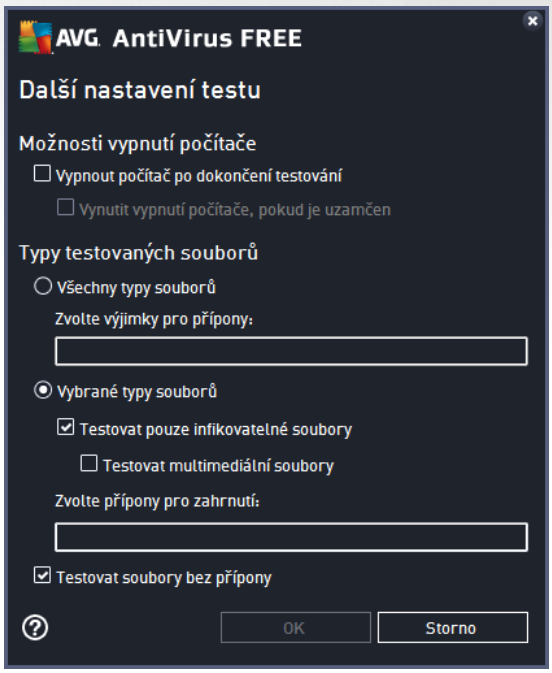
- ***Kontrolovat tracking cookies*** (*ve výchozím nastavení vypnuto*): parametr definuje, že během testu

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 testovat 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 služby 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 testů

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.

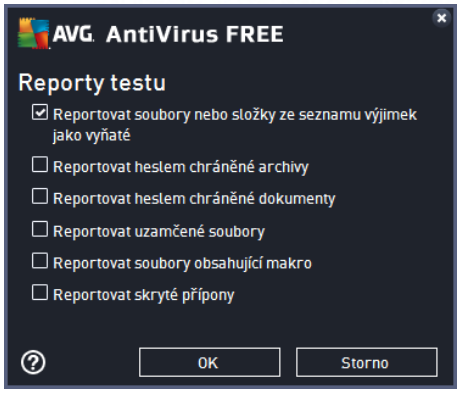
  - U položky ***Testovat soubory bez přípon*** pak rozhodněte, zda se mají testovat i soubory se skrytou či neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme, abyste se tohoto nastavení podrželi, pokud nemáte skutečný důvod jej měnit. Soubory bez přípon jsou obecně vysoce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

Nastavit, jak rychle probíhá 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*. 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 hlášení testu

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

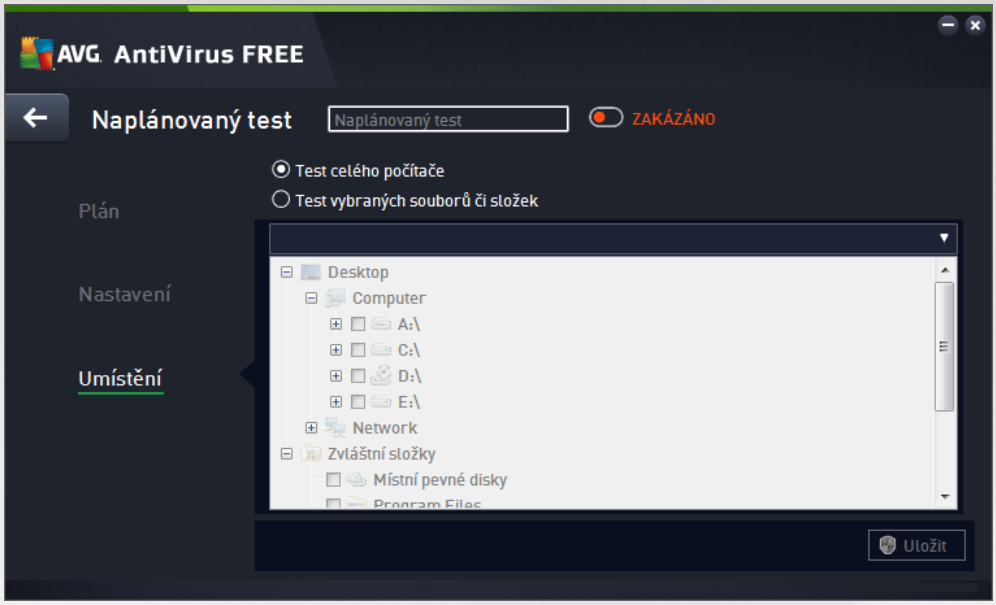


Ovládací tlačítka dialogu

- ***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 dialogu Naplánované testy. Chcete-li tedy nastavit parametry plánu testu na všech záložkách, uložte je stiskem tohoto tlačítka teprve poté, co jste zadali všechny své požadavky.

-  - Pomocí šipky v levé horní části dialogu se vrátíte zpět do přehledu naplánovaných testů.

8.4.3. Umístění



Na záložce ***Umístění*** 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\

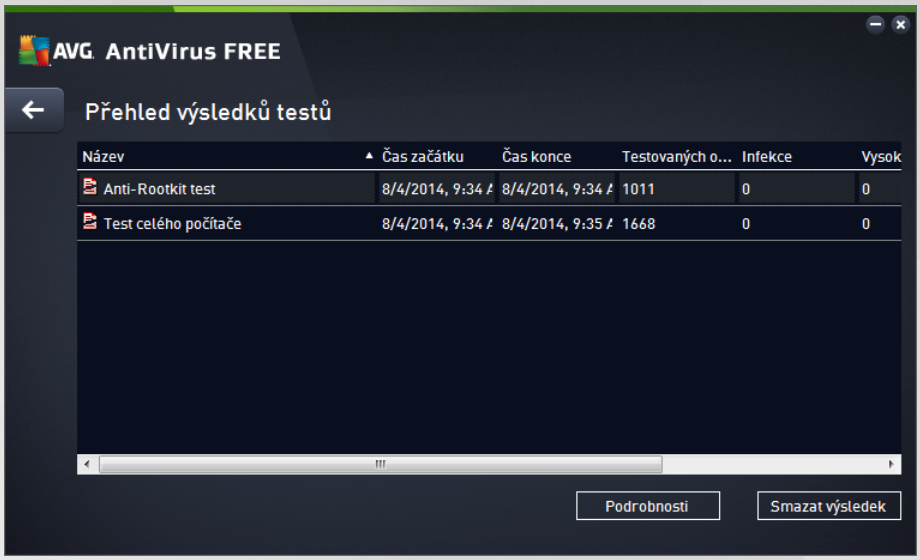
- *pro Windows Vista/7*: C:\Users\user\Documents\

- ***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

- ***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 dialogu Naplánované testy. Chcete-li tedy nastavit parametry plánu testu na všech záložkách, uložte je stiskem tohoto tlačítka teprve poté, co jste zadali všechny své požadavky.
-  - Pomocí šipky v levé horní části dialogu se vrátíte zpět do přehledu naplánovaných testů.

8.5. Výsledky testu



Dialog ***Přehled výsledků testů*** poskytuje kompletní seznam výsledků všech dosud proběhnuvších testů. V tabulce najdete ke každému z testů tyto informace:

- ***Ikona*** - První sloupec zobrazuje informativní ikonu, která vypovídá o stavu ukončení testu:
  - Test byl dokončen, žádná infekce nebyla nalezena
  - Test byl přerušen před dokončením, žádná infekce nebyla nalezena
  - Test byl dokončen, infekce byly nalezeny, ale nikoliv vyléčeny
  - Test byl přerušen před dokončením, infekce byly nalezeny, ale nikoliv vyléčeny
  - Test byl dokončen, infekce byly nalezeny a vyléčeny nebo odstraněny
  - Test byl přerušen před dokončením, infekce byly nalezeny a vyléčeny nebo odstraněny
- ***Název*** - Tento sloupec uvádí název daného testu. Buďto se jedná o jeden ze dvou možných výrobcem přednastavených testů nebo zde bude uveden název vašeho vlastního naplánovaného testu.
- ***Čas začátku*** - Uvádí přesné datum a čas spuštění testu.
- ***Čas konce*** - Uvádí přesné datum a čas ukončení, pozastavení či přerušení testu.
- ***Testovaných objektů*** - Udává celkový počet všech objektů, které byly v rámci testu prověřeny.
- ***Infekce*** - Uvádí celkový počet nalezených/odstraněných infekcí.
- ***Vysoká / Střední / Nízká*** - Následující tři sloupce pak rozdělují nalezené infekce podle jejich závažnosti na vysoce, středně či málo nebezpečné.

- ***Rootkity*** - Uvádí celkový počet rootkitů nalezených během testování.

Ovládací prvky dialogu

Podrobnosti - Kliknutím na tlačítko se zobrazí podrobný popis přehled výsledku zvoleného testu *(tj.výsledku, který jste aktuálně v tabulce označili)*.

Smazat výsledek - Kliknutím na tlačítko odstraníte zvolený záznam o výsledku testu z tabulky.

 - Pomocí šipky v levé horní části dialogu se vrátíte zpět do základního uživatelského rozhraní s přehledem komponent.

8.6. Podrobnosti výsledku testu

Přehled podrobných informací o výsledku zvoleného testu otevřete kliknutím na tlačítko ***Podrobnosti*** dostupné z dialogu Přehled výsledků testů. Tím přejdete do rozhraní téhož dialogu, kde jsou podrobně rozepsány informace o výsledku konkrétního testu. Informace jsou rozděleny na třech záložkách:

- ***Shrnutí*** - Záložka nabízí základní informace o testu: zda byl úspěšně dokončen, zda byly detekovány nějaké hrozby a jak s nimi bylo naloženo.
- ***Detaily*** - Záložka zobrazuje podrobný přehled informací o testu, včetně podrobností o jednotlivých detekovaných hroznách. Máte zde také možnost exportovat přehled do souboru a uložit jej ve formátu .csv.
- ***Nálezy*** - Tato záložka bude zobrazena pouze v případě, že v průběhu testu skutečně došlo k detekci hrozeb, a rozlišuje detekované hrozby podle jejich závažnosti:

   ***Informativní závažnost***: Nejde o skutečné hrozby, ale pouze o informace nebo varování. Typickým příkladem může být dokument obsahující makro, dokument nebo archiv chráněný heslem, uzamčený soubor a podobně.

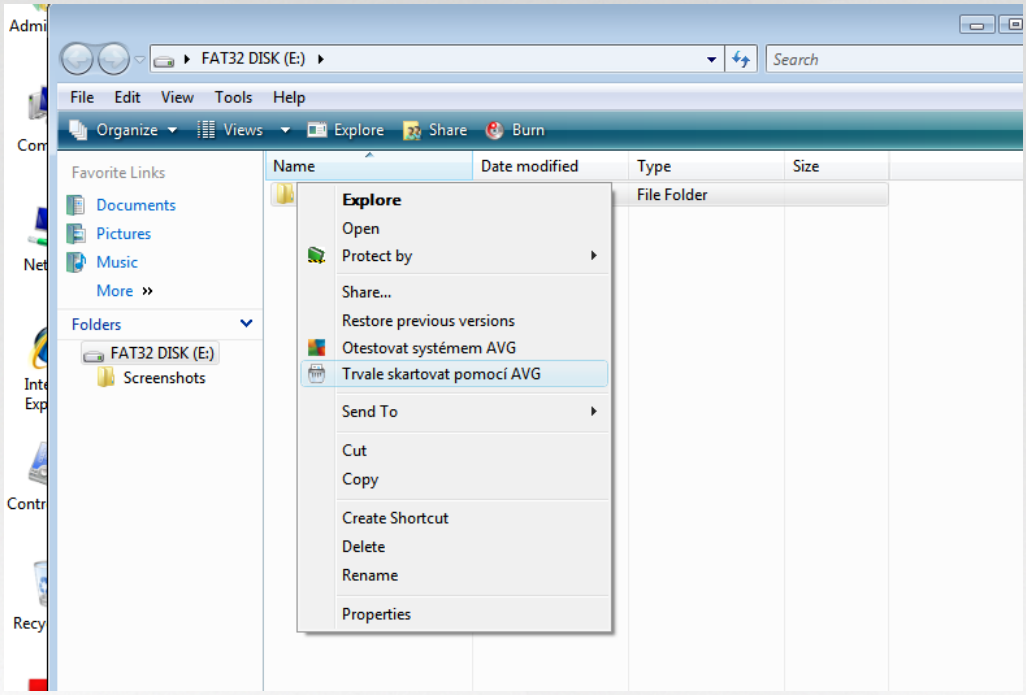
   ***Střední závažnost***: V této kategorii najdeme nejčastěji potenciálně nežádoucí aplikace, jako je například adware nebo tracking cookies.

   ***Vysoká závažnost***: Hrozbami s vysokou závažností rozumíme například viry, trojské koně, exploity apod. Řadí se sem také objekty detekované heusristickou analýzou, tedy takové hrozby, které dosud nejsou popsány ve virové databázi.

9. AVG File Shredder

AVG File Shredder je nástrojem pro absolutní vymazání (skartaci) souboru bez jakékoliv následné možnosti jeho obnovy, a to ani s použitím specializovaných nástrojů pro obnovu dat.

Chcete-li skartovat soubor či složku, vyberte zvolený objekt v aplikaci pro správu souborů *(Windows Explorer, Total Commander, ...)* a klikněte na něj pravým tlačítkem myši. Z kontextové nabídky zvolte položku ***Skartovat obsah pomocí AVG***. Tímto způsobem můžete skartovat i soubory v odpadkovém koši. Pokud vámi zvolený soubor není možné skartovat kvůli jeho specifickému umístění *(například na CD-ROM)*, budete o této skutečnosti vyrozuměni anebo možnost skartace nebude v kontextovém menu vůbec uvedena.



Mějte prosím vždy na paměti, že jednou skartovaný soubor už nelze nikdy obnovit!

10. 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:

- ***Datum uložení*** - Datum a čas detekce infikovaného souboru a jeho přesunutí do Virového trezoru.
- ***Hrozba*** - Jestliže jste si v rámci instalace programu **AVG AntiVirus Free Edition** nainstalovali také komponentu Identita, najdete v tomto sloupci grafické znázornění závažnosti infekce, od nezávadné *(tři zelené tečky)* po vysoce rizikovou *(tři červené tečky)*. Zároveň je zde uvedena informace o typu detekce a místu, kde byla zachycena. Odkaz *Více info* odkazuje na stránku s podrobnostmi o detekované infekci v on-line virové encyklopedii.
- ***Zdroj*** - Určuje, která komponenta programu **AVG AntiVirus Free Edition** uvedenou hrozbu detekovala.
- ***Oznámení*** - Sloupec je většinou prázdný, pouze ve výjimečných případech se může objevit poznámka s podrobnostmi k příslušné detekované hrozbě.

Ovládací tlačítka dialogu

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

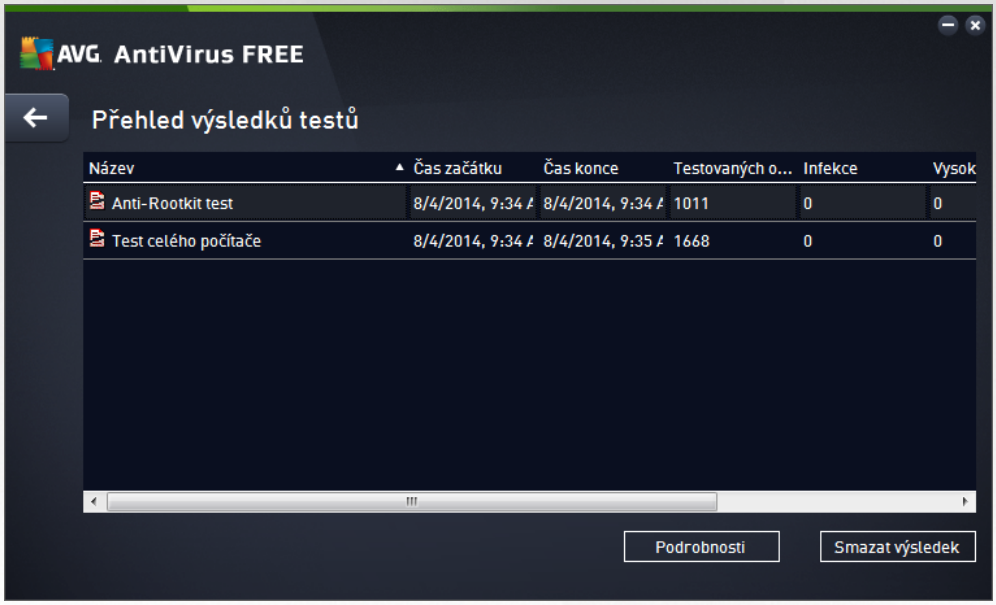
- ***Obnovit*** - přesune infikovaný soubor z ***Virového trezoru*** zpět do původního umístění
- ***Obnovit jako*** - pokud se rozhodnete detekovanou infekci z ***Virového trezoru*** umístit do zvolené složky, použijte toto tlačítko. Podezřelý a detekovaný objekt bude uložen pod svým původním jménem, a pokud toto není známo, bude uložen pod standardním jménem, kterým byl označen při detekci.
- ***Odeslat k analýze*** - toto tlačítko je aktivní pouze tehdy, pokud jste v seznamu označili jednu či více detekovaných hrozeb. K analýze by měly být odesílány pouze detekce, u nichž si nejste jisti, zda byly detekovány správně a zda se nejedná o falešný poplach (false positive, tedy vzorek označený jako potenciálně nebezpečný, o němž se domníváte, že je neškodný). Označený nález můžete v takovém případě poslat do virové laboratoře AVG k podrobné analýze.
- ***Detaily*** - chcete-li znát podrobnější informace o konkrétní hrozbě uložené ve ***Virovém trezoru***, označte zvolenou položku v seznamu a tlačítkem ***Detaily*** vyvoláte nový dialog s podrobným popisem detekované hrozby.
- ***Smazat*** - definitivně a nevratně vymaže infikovaný soubor z ***Virového trezoru***
- ***Odstranit vše*** - definitivně vymaže veškerý obsah ***Virového trezoru.*** Touto volbou jsou všechny soubory z ***Virového trezoru*** nevratně smazány z disku (*nebudou přesunuty do koše*).

11. Historie

Sekce ***Historie*** zahrnuje veškeré informace a podává podrobný přehled o všech proběhlých událostech *(např. o aktualizacích, testech, nálezech, atd.)*. Tato sekce je dostupná z hlavního uživatelského rozhraní volbou položky ***Možnosti / Historie***. Historie se dálě dělí do těchto podkategorií:

- Výsledky testů
- Nálezy Rezidentního štítu
- Nálezy E-mailové ochrany
- Protokol událostí

11.1. Výsledky testů



Dialog ***Přehled výsledků testů*** je dostupný volbou položky ***Možnosti / Historie / Výsledky testů*** v horním vodorovném menu hlavního okna **AVG AntiVirus Free Edition**. 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
- ***Vysoká / Střední*** - v těchto sloupcích je uveden počet celkově nalezených a odstraněných infekcí vysoké či střední závažnosti
- ***Informace*** - údaje o průběhu testu, zejména o jeho řádném či předčasném ukončení
- ***Rootkity*** - počet detekovaných rootkitů

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 a přehledu testů odstranit
-  - zpět do výchozího hlavního dialogu AVG *(přehled komponent)* se vrátíte prostřednictvím šipky v levém horním rohu tohoto dialogu

11.2. Nálezy Rezidentního štítu

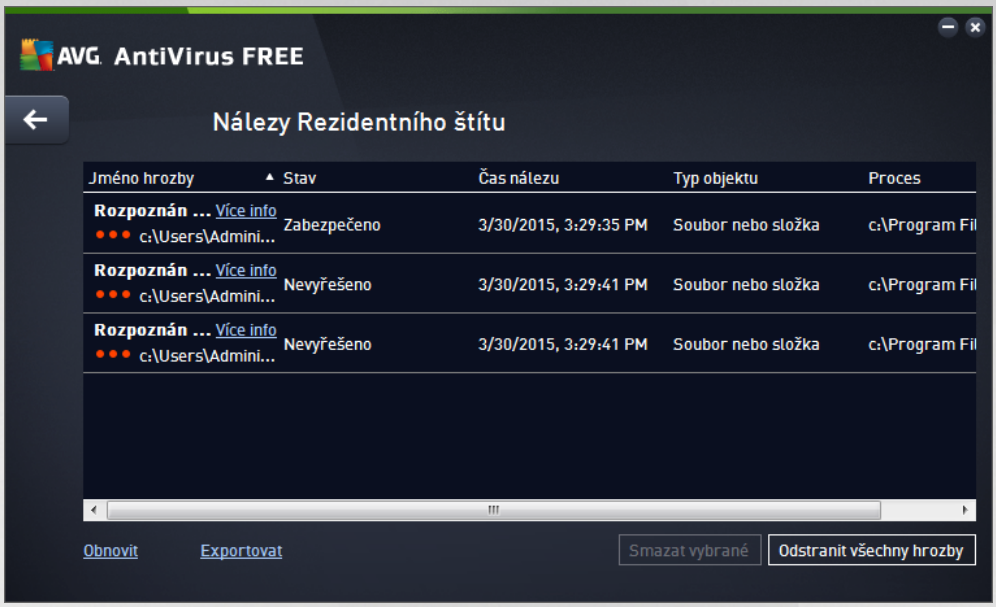
Služba ***Rezidentní štít*** je součástí komponenty ***Počítač*** a kontroluje soubory při jejich otevírání, ukládání a kopírování. Jestliže detekuje virus nebo jakýkoliv podezřelý objekt, budete okamžitě varováni tímto dialogem:

V tomto varovném dialogu najdete informaci o objektu, který byl detekován jako infikovaný (*Hrozba*) a podrobnosti o rozpoznané infekci (*Název objektu*). Odkaz Více informací vás přesměruje do online virové encyklopedie, kde najdete podrobnější údaje o detekované infekci, jsou-li tyto informace k dispozici. V dialogu dále najdete přehled možných řešení, jak naložit s detekovanou hrozbou. Jedna z alterantiv bude vždy označena jako doporučená: ***Ochránit mě (doporučeno)***. ***Pokud je to možné, zvolte vždy tuto variantu!***

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 okno s detailní informací o procesu, při němž došlo k detekci infekce, a s uvedeným identifikačním číslem procesu.

Přehled všech nálezů rezidentního štítu je dostupný v dialogu ***Nálezy Rezidentního štítu***. Tento dialog otevřete volbou položky ***Možnosti / Historie / Nálezy Rezidentního štítu*** v horním vodorovném menu hlavního okna **AVG AntiVirus Free Edition**. 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:

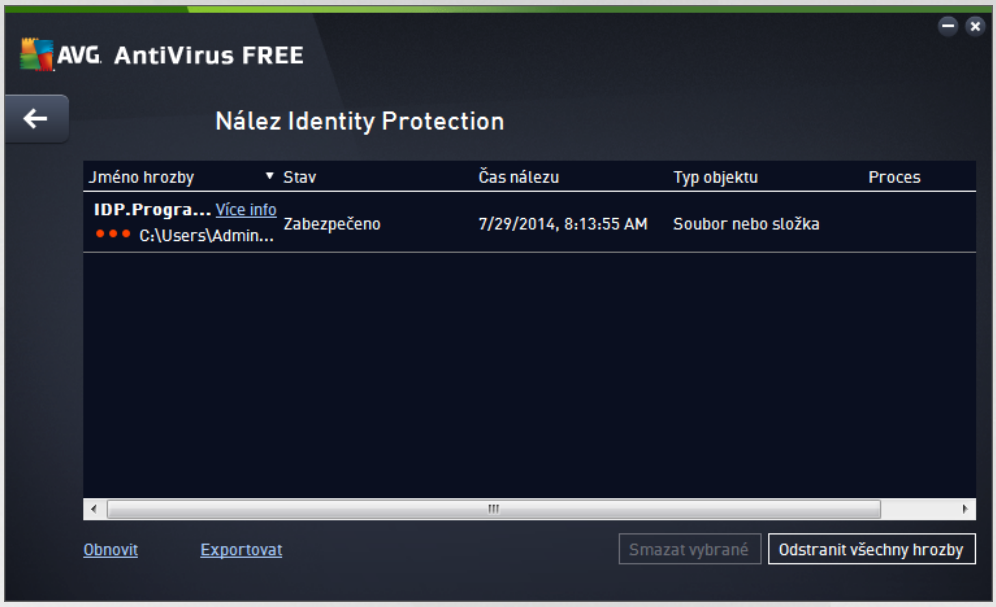
- ***Jméno hrozby*** - popis (*případně i jméno*) detekovaného objektu a jeho umístění; odkaz *Více info* směřuje na stránku s podrobnostmi o detekované infekci v on-line virové encyklopedii
- ***Stav*** - jak bylo s detekovaným objektem naloženo
- ***Čas nálezu*** - datum a čas, kdy došlo k detekci hrozby
- ***Typ objektu*** - jakého typu je detekovaný objekt
- ***Proces*** - při jaké akci byl objekt detekován

Ovládací tlačítka

- ***Obnovit*** - aktualizujete seznam všech nálezů.
- ***Exportovat*** - máte možnost celý seznam detekovaných objektů do samostatného souboru.
- ***Smazat vybrané*** - ze seznamu můžete vybrat jen některé záznamy a stiskem tlačítka pak tyto zvolené položky odstranit.
- ***Odstranit všechny hrozby*** - stiskem tlačítka vymažete všechny záznamy ze seznamu uvedeného v tomto dialogu.
-  - zpět do výchozího hlavního dialogu AVG *(přehled komponent)* se vrátíte prostřednictvím šipky v levém horním rohu tohoto dialogu.

11.3. Nález Identity Protection

Dialog ***Nález Identity Protection*** je dostupný volbou položky ***Možnosti / Historie / Nález Identity Protection*** v horním vodorovném menu hlavního okna **AVG AntiVirus Free Edition**.



V dialogu najdete seznam nálezů detekovaných komponentou Identity Protection. U každého z detekovaných objektů jsou k dispozici následující informace:

- ***Jméno hrozby*** - popis (případně i jméno) detekovaného objektu a jeho umístění; odkaz *Více info* směřuje na stránku s podrobnostmi o detekované infekci v on-line virové encyklopedii
- ***Stav*** - jak bylo s detekovaným objektem naloženo
- ***Čas nálezu*** - datum a čas detekce
- ***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

Ovládací tlačítka dostupná v dialogu ***Nález Identity Protection***:

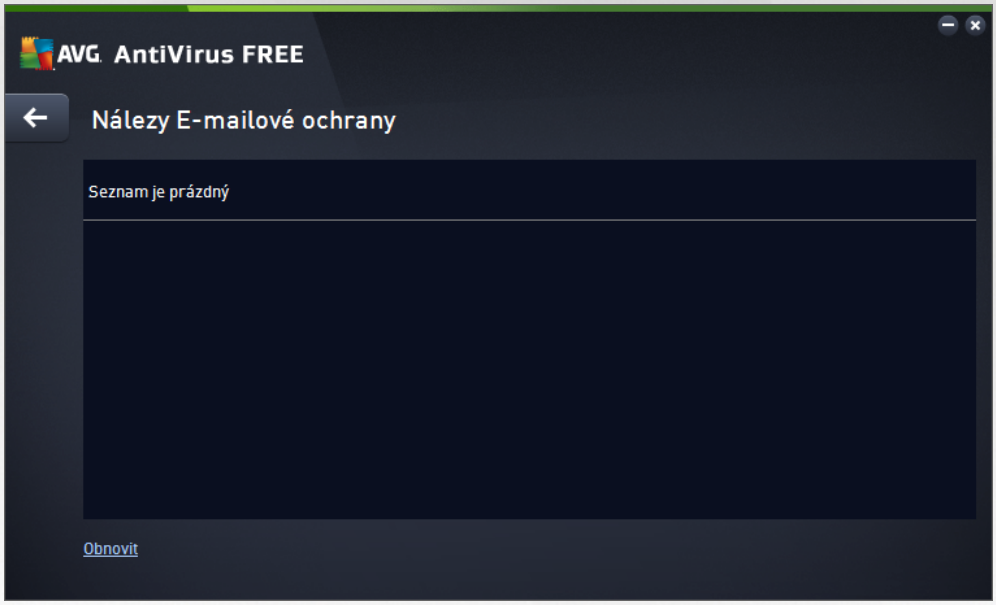
- ***Obnovit*** - Aktualizuje seznam nálezů podle momentálního stavu.
- ***Exportovat*** - máte možnost celý seznam detekovaných objektů do samostatného souboru.
- ***Smazat vybrané*** - ze seznamu můžete vybrat jen některé záznamy a stiskem tlačítka pak tyto

zvolené položky odstranit.

- ***Odstranit všechny hrozby*** - stiskem tlačítka vymažete všechny záznamy ze seznamu uvedeného v tomto dialogu.
-  - Zpět do výchozího hlavního dialogu AVG *(přehled komponent)* se vrátíte prostřednictvím šipky v levém horním rohu tohoto dialogu.

11.4. Nálezy E-mailové ochrany

Dialog ***Nálezy E-mailové ochrany*** je dostupný volbou položky ***Možnosti / Historie / Nálezy E-mailové ochrany*** v horním vodorovném menu hlavního okna **AVG AntiVirus Free Edition**.



V dialogu najdete seznam nálezů detekovaných komponentou E-maily. U každého z detekovaných objektů jsou k dispozici následující informace:

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

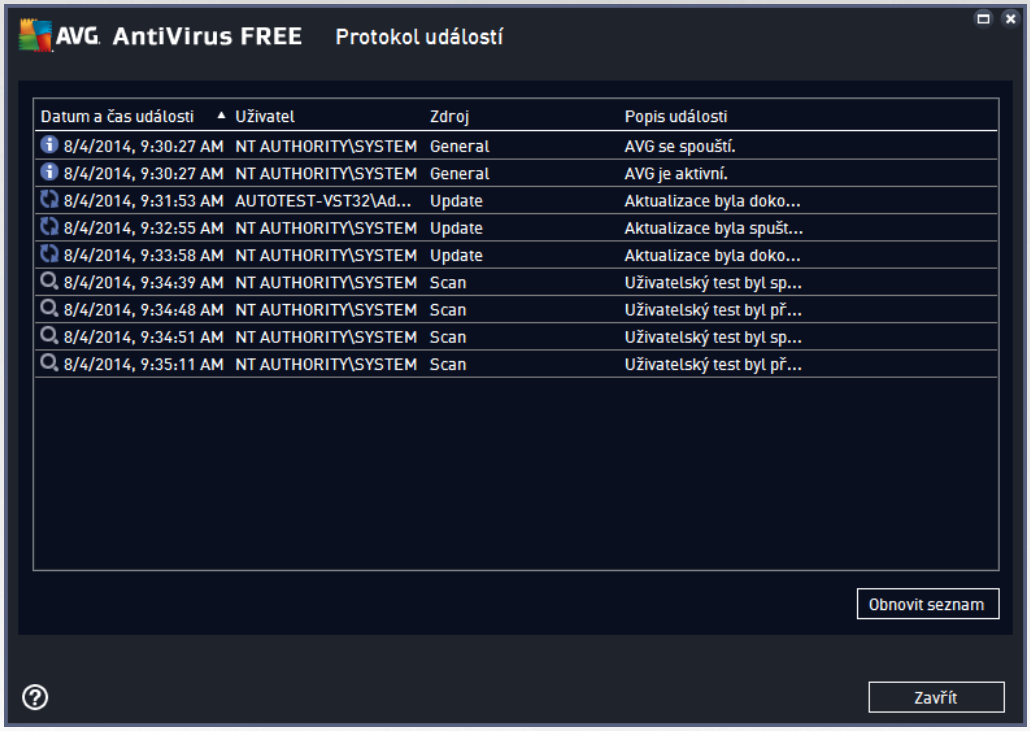
Pod seznamem pak najdete informaci o celkovém počtu detekovaných objektů. Dále máte možnost exportovat celý seznam detekovaných objektů do samostatného souboru (***Export seznamu do souboru***) a vymazat všechny záznamy o detekovaných objektech (***Smazat seznam***).

Ovládací tlačítka

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

- ***Obnovit*** - Aktualizuje seznam nálezů podle momentálního stavu.
-  - Zpět do výchozího hlavního dialogu AVG *(přehled komponent)* se vrátíte prostřednictvím šipky v levém horním rohu tohoto dialogu.

11.5. Protokol událostí



Dialog ***Protokol událostí*** je dostupný volbou položky ***Možnosti / Historie / Protokol událostí*** v horním vodorovném menu hlavního okna **AVG AntiVirus Free Edition**. V tomto dialogu najdete přehled všech důležitých událostí, které nastaly v průběhu práce **AVG AntiVirus Free Edition**. 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 a informace o ostatních důležitých událostech.

Ke 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

- ***Obnovit seznam*** - stiskem tlačítka provedete aktualizaci záznamů v seznamu událostí
- ***Zavřít*** - stiskem tlačítka se vrátíte zpět do hlavního okna **AVG AntiVirus Free Edition**

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 AntiVirus Free Edition** pravidelně aktualizovat. V ideálním případě ponechte prosím program ve výchozím nastavení, kdy je zapnuta automatická aktualizace. Bez aktuální virové databáze nebude **AVG AntiVirus Free Edition** 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.

Pro zajištění maximální bezpečnosti ověřuje **AVG AntiVirus Free Edition** ve výchozím nastavení aktualizaci virové databáze každé dvě 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 AntiVirus Free Edition** bude aktuální během celého dne. Pokud je virová databáze v **AVG AntiVirus Free Edition** starší než jeden týden, budete o tomto stavu informováni oznamovacím dialogem ***Databáze je zastaralá***; pro vyřešení chyby spusťe aktualizaci ručně kliknutím na tlačítko Aktualizovat dostupné v hlavním dialogu aplikace. Toto tlačítko je vždy dostupné z kteréhokoliv dialogu uživatelského rozhraní AVG. Tlačítko můžete použít také v případě, že si přejete okamžitě ověřit existenci nových aktualizačních souborů. Po spuštění aktualizace dojde nejprve k ověření, zda existují nové aktualizační soubory, jež dosud nebyly aplikovány. Pokud ano, **AVG AntiVirus Free Edition** zahájí jejich okamžité stahování a spustí samotný proces aktualizace. O výsledku aktualizace budete vyrozuměni v dialogu nad ikonou AVG na systémové liště.

V rámci **AVG AntiVirus Free Edition** bohužel není možné nastavovat vlastní parametry plánu aktualizace, a tak například omezit počet výskytů kontroly aktualizace. Tato editace je dostupná pouze v placených verzích programu.

13. FAQ a technická podpora

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

- ***Řešení potíží v nápovědě***: Přímo v nápovědě programu **AVG AntiVirus Free Edition** je nově k dispozici sekce ***Řešení potíží***. 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 ***Podpora*** najdete přehled tematických okruhů, které řeší problémy obchodního i technického charakteru, sekci často kladených otázek i veškeré potřebné kontakty.

- ***AVG ThreatLabs***: Samostatná AVG stránka (*http://www.avg.com/about-viruses*) je věnována virové tematice a 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 Free produktů na adrese http://forums.avg.com.

Při používání AVG AntiVirus Free Edition nemáte bohužel nárok na nepřetržitou profesionální technickou podporu poskytovanou zákazníkům AVG, kteří používají plnou verzi. Pokud uvažujete o přechodu na placenou verzi produktu, navštivte prosím web AVG (http://www.avg.cz/), kde najdete informace o možnostech koupě plné verze AVG 2013.