



AVG Anti-Virus Free Edition 2012

Uživatelský manuál

Verze dokumentace 2012.16 (16.5.2012)

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

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

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

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

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



Obsah

1. Úvod	5
2. Podmínky instalace AVG	6
2.1 Podporované operační systémy	6
2.2 Minimální / doporučené HW požadavky	6
3. Instalační proces AVG	7
3.1 Vítejte: Volba jazyka	7
3.2 Vítejte: Licenční ujednání	8
3.3 Vyberte typ instalace	9
3.4 Uživatelské volby	10
3.5 Postup instalace	11
3.6 Instalace byla úspěšná	12
4. Po instalaci	14
4.1 Registrace produktu	14
4.2 Otevření uživatelského rozhraní	14
4.3 Spuštění testu celého počítače	14
4.4 Test virem Eicar	15
4.5 Výchozí konfigurace AVG	15
5. Uživatelské rozhraní AVG	17
5.1 Systémové menu	18
5.2 Informace o stavu zabezpečení	24
5.3 Zkratková tlačítka	25
5.4 Přehled komponent	26
5.5 Ikona na systémové liště	27
5.6 AVG Advisor	29
5.7 Miniaplikace AVG	30
6. Komponenty AVG	33
6.1 Anti-Virus	33
6.2 LinkScanner	39
6.3 E-mailová ochrana	43
6.4 Anti-Rootkit	47
6.5 PC Analyzer	48



6.6 Identity Protection	50
7. Moje Aplikace	53
7.1 AVG LiveKive	53
7.2 AVG Mobilation	54
7.3 AVG Family Safety	54
7.4 AVG PC Tuneup	55
8. AVG Security Toolbar	56
9. AVG Do Not Track	58
9.1 Rozhraní služby AVG Do Not Track	59
9.2 Informace o sledovacích procesech	60
9.3 Blokování sledovacích procesů	61
9.4 Nastavení služby AVG Do Not Track	61
10. Pokročilé nastavení AVG	64
10.1 Vzhled	64
10.2 Zvuky	67
10.3 Dočasné vypnutí ochrany AVG	68
10.4 Anti-Virus	69
10.5 E-mailová ochrana	75
10.6 LinkScanner	83
10.7 Testy	84
10.8 Naplánované úlohy	90
10.9 Aktualizace	99
10.10 Anti-Rootkit	105
10.11 Identity Protection	107
10.12 Potenciálně nežádoucí programy	111
10.13 Virový trezor	114
10.14 Program zlepšování produktu	114
10.15 Ignorovat chybový stav	117
10.16 Advisor - známé sítě	118
11. AVG testování	119
11.1 Rozhraní pro testování	119
11.2 Přednastavené testy	120
11.3 Testování v průzkumníku Windows	129
11.4 Testování z příkazové řádky	129



11.5 Naplánování testu.....	132
11.6 Přehled výsledků testů.....	141
11.7 Detail výsledku testu.....	142
11.8 Virový trezor.....	149
12. Aktualizace AVG.....	152
12.1 Spouštění aktualizace.....	152
12.2 Průběh aktualizace.....	152
12.3 Úrovně aktualizace.....	153
13. Protokol událostí.....	154
14. FAQ a technická podpora.....	156



1. Úvod

Tento uživatelský manuál nabízí pohled úloh a detekčních technologií poskytovaných **AVG Anti-Virus Free Edition 2012**.

Milióny lidí po celém světě používají **AVG Anti-Virus Free Edition 2012** pro své běžné aktivity. A už je to procházení Internetu, vyhledávání nebo jen komunikování s lidmi na Facebooku, **AVG Anti-Virus Free Edition 2012** vás ochrání. Aplikace **AVG Anti-Virus Free Edition 2012** vám umožní:

- procházet Internet a vyhledávat bez obav díky ochraně v reálném čase LinkScanner
- být chráněni na sociálních sítích díky ochraně sociálních sítí AVG
- užívat si rychlost vašeho počítače – aplikace AVG Smart Scanning pracuje, když nejste u počítače, a po vašem návratu běží v režimu nízké priority
- mít stále aktuální software díky nejnovějším informacím o hrozbách, které poskytuje komunitní ochranná síť AVG a ochranná technologie Cloud

AVG Anti-Virus Free Edition 2012 je dostupný zdarma a jeho funkčnost je omezená. Pokud během používání AVG Anti-Virus Free Edition 2012 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.



2. Podmínky instalace AVG

2.1. Podporované operační systémy

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

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

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

Poznámka: Komponenta [ID Protection](#) není podporována na Windows XP x64. Na tomto operačním systému lze nainstalovat AVG Anti-Virus Free Edition 2012, ale pouze bez této komponenty.

2.2. Minimální / doporučené HW požadavky

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

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

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

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



3. Instalační proces AVG

Kde najdu instalační soubor?

Pro instalaci **AVG Anti-Virus Free Edition 2012** na váš počítač budete potřebovat aktuální instalační soubor. Abyste zajistili, že instalujete vždy nejnovější verzi **AVG Anti-Virus Free Edition 2012**, je vhodné stáhnout si instalační soubor z webu AVG (<http://free.avg.com/cz-cs/uvod/>).

Jak probíhá proces instalace?

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

3.1. Vítejte: Volba jazyka

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



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

Pozor: V tuto chvíli volíte pouze jazyk instalačního procesu. Aplikace AVG Anti-Virus Free Edition 2012 bude tedy nainstalována ve zvoleném jazyce a také v angličtině, která se instaluje automaticky. Je však možné nainstalovat ještě další volitelné jazyky, v nichž můžete aplikaci AVG zobrazit. Svůj výběr alternativních jazyků budete moci provést později během instalačního procesu, konkrétně v dialogu nazvaném [Uživatelské volby](#).



3.2. Vítejte: Licenční ujednání

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



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

Ochrana osobních údajů AVG

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

Ovládací tlačítka dialogu

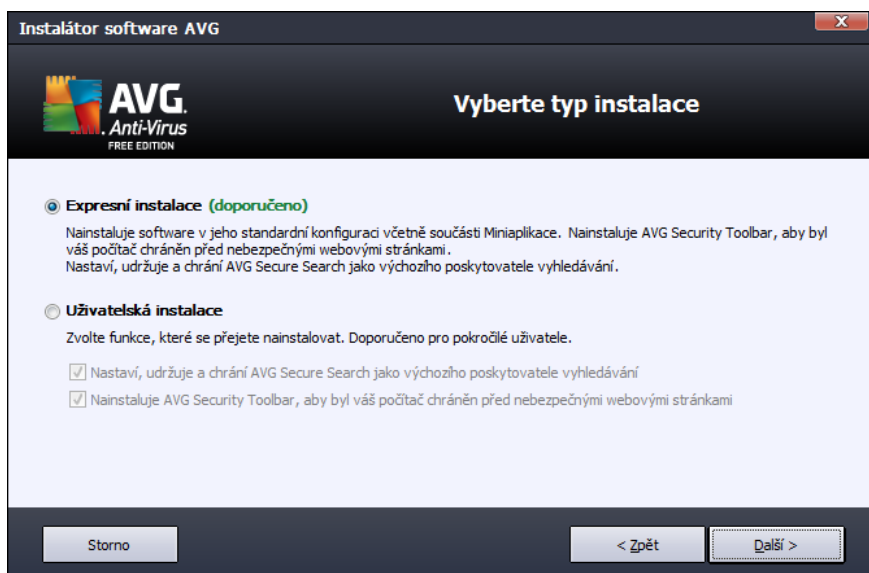
V prvním dialogu instalace jsou k dispozici tato ovládací tlačítka:

- **Verze pro tisk** - Kliknutím vytisknete licenční ujednání v plném rozsahu.
- **Nesouhlasím** - Kliknutím odmítáte přijmout licenční ujednání. Instalační proces bude bezprostředně ukončen. **AVG Anti-Virus Free Edition 2012** nebude nainstalován!
- **Zpět** - Kliknutím na tlačítko se vrátíte o jeden krok zpět do předchozího dialogu instalačního procesu.
- **Souhlasím** - Kliknutím potvrzujete, že jstečetli licenční ujednání a přijímáte jej v plném rozsahu. Instalace bude pokračovat dále do následujícího dialogu instalačního procesu.



3.3. Vyberte typ instalace

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



Expresní instalace

V této části uživatel doporučujeme použít expresní instalaci. Tak bude **AVG Anti-Virus Free Edition 2012** nainstalován zcela automaticky s konfigurací definovanou výrobcem, a to včetně [miniaplikace AVG](#), doplněk pro internetové prohlížeče a [AVG Security Toolbar](#) a s nastavením služby AVG Secure Search jako výchozího poskytovatele vyhledávání. Výchozí nastavení zaručuje maximální úroveň bezpečnosti a optimální využití zdrojů. Pokud se v budoucnu vyskytnou potřeby, které konkrétní nastavení změní, budete mít vždy možnost editovat konfiguraci **AVG Anti-Virus Free Edition 2012** přímo v aplikaci.

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

Uživatelská instalace

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

- **Nastaví, udržuje a chrání AVG Secure Search jako výchozího poskytovatele vyhledávání** - ponecháte-li tuto volbu zapnutou, bude výchozím poskytovatelem vyhledávání AVG Secure Search, který úzce spolupracuje s komponentou [Link Scanner](#) a společně tak zajišťují vaši maximální bezpečnost online.
- **Nainstaluje AVG Security Toolbar, aby byl váš počítač chráněn před nebezpečnými**



webovými stránkami - ponecháte-li tuto položku označenu, bude nainstalován [AVG Security Toolbar](#), který zajišťuje dostupnost bezpečnostních prvků AVG přímo z prostředí vašeho webového prohlížeče.

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

Po stisku tlačítka **Další** budete přesměrováni k dialogu [Uživatelské volby](#).

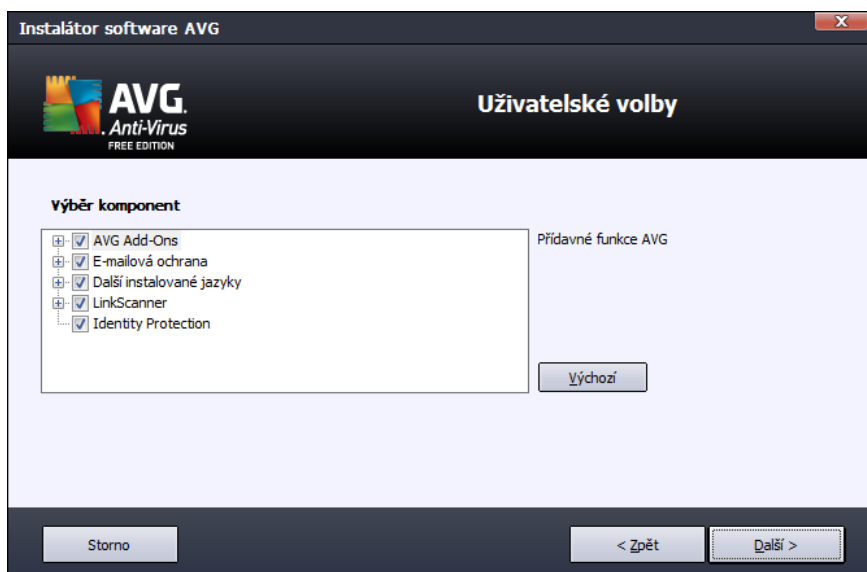
Ovládací tlačítka dialogu

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

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

3.4. Uživatelské volby

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





Sekce **Výběr komponent** nabízí pohled na komponenty **AVG Anti-Virus Free Edition 2012**, které můžete nainstalovat. Pokud vám výchozí nastavení nevyhovuje, máte možnost jednotlivé komponenty odebrat/přidat.

Volíte-li pouze z těch komponent, které jsou zahrnuty v AVG Anti-Virus Free Edition 2012. Pouze tyto komponenty vám také budou v dialogu nabídnuty!

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

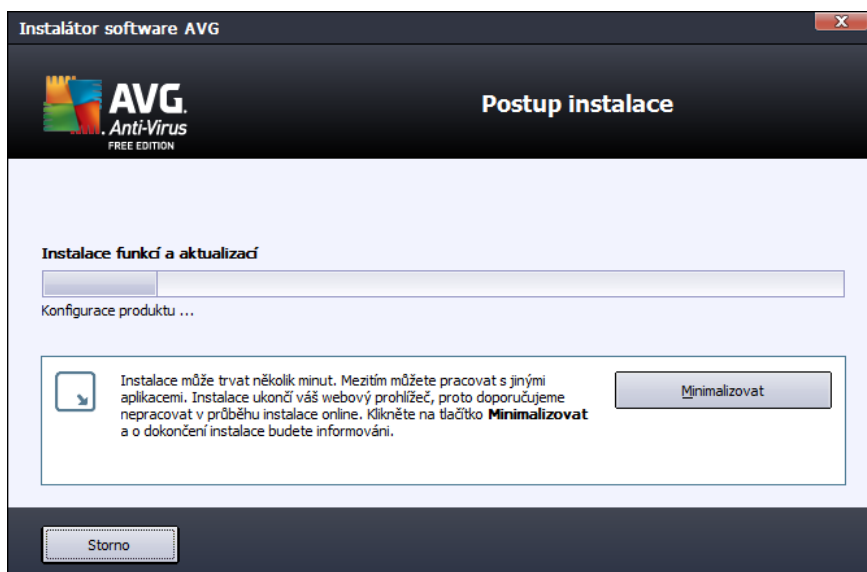
Ovládací tlačítka dialogu

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

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

3.5. Postup instalace

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





Po kejte prosím na dokonění instalace. Poté budete automaticky přesměrováni k následujícímu dialogu.

Ovládací tlačítka dialogu

V dialogu jsou dostupná dvě ovládací tlačítka:

- **Minimalizovat** - Instalace může trvat několik minut. Tlačítkem zmenšíte dialogové okno instalace pouze na ikonu na systémové liště. Dialog se opět otevře v plné velikosti, jakmile bude instalace dokončena.
- **Storno** - Toto tlačítko použijte výhradně tehdy, přejete-li si být zrušit instalační proces. V takovém případě nebude **AVG Anti-Virus Free Edition 2012** nainstalován!

3.6. Instalace byla úspěšná

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

V tomto dialogu máte možnost se rozhodnout, zda se chcete zúčastnit **Programu zlepšování produktu** (podrobnosti najdete v kapitole [Pokročilé nastavení AVG / Program zlepšování produktu](#)). V rámci tohoto programu probíhá sběr anonymních informací o detekovaných hrozbách s cílem zvýšit celkovou úroveň bezpečnosti na Internetu. Veškerá data jsou zpracována v souladu se zásadami ochrany osobních údajů; kliknutím na odkaz **Ochrana osobních údajů** budete přesměrováni na webovou stránku AVG (<http://www.avg.cz/>), která Vás v plném rozsahu seznámí se zásadami ochrany osobních údajů společnosti AVG Technologies. Pokud souhlasíte, ponechte prosím volbu označenou (ve výchozím nastavení je tato možnost zapnuta).

Chcete-li být pravidelně informováni o novinkách, označte prosím možnost **Přeji si dostávat informace o novinkách, speciálních nabídkách a bezpečnostních upozorněních**. Uveďte prosím svůj kontaktní e-mail.



V rámci zlepšování našich produktů a služeb bychom se Vás před dokončením instalačního procesu **AVG Anti-Virus Free Edition 2012** rádi zeptali, **Co je hlavním důvodem pro volbu produktu AVG?** Vyberte prosím nejpříhodnější odpověď z nabídky rozbalovacího menu. Vaše účast v tomto dotazníku je samozřejmě dobrovolná.

Ovládací tlačítka dialogu

V tomto dialogu je k dispozici pouze jediné ovládací tlačítko: **Dokonit**. Touto volbou dokoníte celý instalační proces. Váš počítač je nyní chráněn aplikací **AVG Anti-Virus Free Edition 2012**.



4. Po instalaci

4.1. Registrace produktu

AVG Anti-Virus Free Edition 2012 nevyžaduje nutnou registraci programu. Registraci je však vhodné provést, pokud chcete využívat služeb [diskusního fóra AVG Anti-Virus Free Edition 2012](#), respektive, chcete-li vznést vlastní dotaz nebo na jiný reagovat. Prostředí je fórum dostupné i bez registrace.

Nejsnazší přístup k registraci je přímo z prostředí aplikace **AVG Anti-Virus Free Edition 2012**, a to volbou položky hlavního menu [Nápověda/Zaregistrovat AVG Anti-Virus Free Edition 2012](#). Následně budete postupovat při registraci na registrační stránku [AVG Free fóra](#), kde dále postupujte podle uvedených instrukcí. Po vyplnění registračního formuláře Vám na uvedenou adresu zašleme aktivací kód, s nímž se do fóra přihlásíte.

4.2. Otevření uživatelského rozhraní

[Hlavní dialog](#) **AVG Anti-Virus Free Edition 2012** je dostupný několika cestami:

- dvojklikem na [ikonu AVG na systémové liště](#)
- dvojklikem na ikonu AVG na ploše
- z nabídky **Start / Všechny programy / AVG 2012**

4.3. Spuštění testu celého počítače

Jelikož existuje jisté riziko, že virus byl na váš počítač zavlečen již před instalací **AVG Anti-Virus Free Edition 2012**, doporučujeme po instalaci spustit [Test celého počítače](#), který zkontroluje celý počítač a ověří přítomnost virů a potenciálně nežádoucích programů. První test počítače může trvat asi hodinu, ale z hlediska vaší bezpečnosti je skutečně nanejvýš důležité jej nechat probíhat.

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

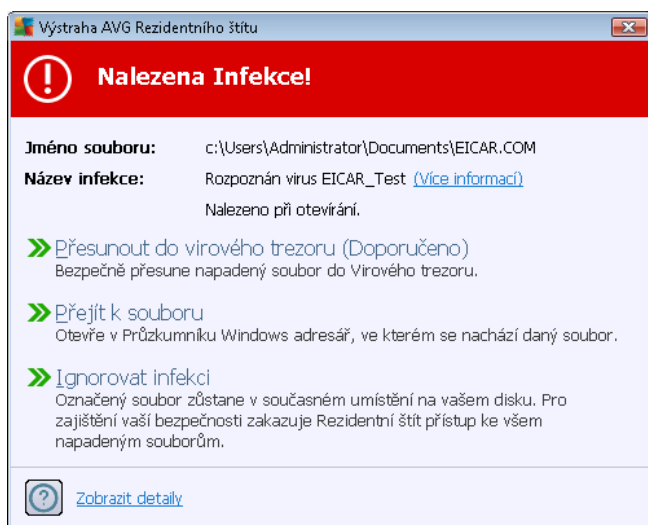


4.4. Test virem Eicar

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

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

Stáhněte si soubor [eicar.com](http://www.eicar.com). **AVG Anti-Virus Free Edition 2012** zareaguje varovným upozorněním pokaždé při pokusu uložit tento soubor na lokální disk (*pokud používáte například Internet Explorer*) anebo po uložení při pokusu otevřít právě stažený soubor (*pokud používáte například Mozilla Firefox*). Varování se objeví ve formě výstražného upozornění [Rezidentního štítu](#), který je součástí komponenty [Anti-Virus](#). Toto upozornění dokazuje, že **AVG Anti-Virus Free Edition 2012** na vašem počítači je správně nainstalován:



Pokud není testovací soubor EICAR identifikován jako virus, je nutné znovu provést konfiguraci **AVG Anti-Virus Free Edition 2012**!

4.5. Výchozí konfigurace AVG

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

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

Jednoduché, spíše preferenční změny v nastavení [komponent AVG Free](#) jsou dostupné přímo z uživatelského rozhraní pro jednotlivé komponenty. Pokud se domníváte, že je nutné konfiguraci

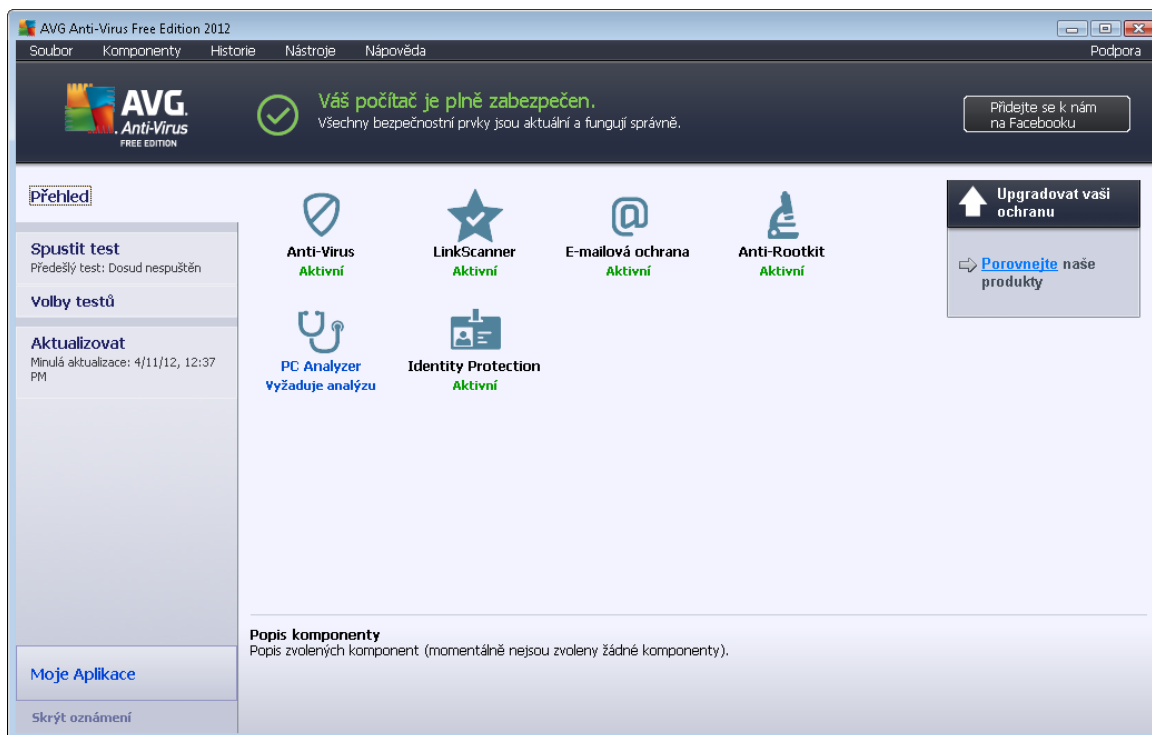


AVG Anti-Virus Free Edition 2012 p enastavit podle vašich aktuálních potřeb, proveďte editaci parametrů v [Pokročilém nastavení AVG](#): zvolte ze systémového menu položku **Nástroje/Pokročilé nastavení** a editaci nastavení proveďte v nově otevřeném dialogu [Pokročilém nastavení AVG](#).



5. Uživatelské rozhraní AVG

AVG Anti-Virus Free Edition 2012 se otevírá v tomto rozhraní:



Hlavní okno je rozděleno do několika sekcí:

- **Systémové menu** (navigace Windows zobrazená zcela nahoře) je standardní navigací, která umožňuje přístup ke všem komponentám, vlastnostem a službám **AVG Anti-Virus Free Edition 2012** - [podrobnosti >>](#)
- **Informace o stavu zabezpečení** (v horní části okna) podává základní informaci o aktuálním stavu **AVG Anti-Virus Free Edition 2012** - [podrobnosti >>](#)
- **Připojte se k nám na Facebooku** (zcela vpravo v horní části okna) - toto tlačítko Vám jedním kliknutím umožní připojit se k [AVG komunitě na Facebooku](#). Tlačítko se však zobrazuje pouze tehdy, jsou-li všechny komponenty AVG plně funkční a nastaveny k optimálnímu výkonu (podrobné informace o tom, jak rozpoznat aktuální stav komponent, najdete v kapitole [Informace o stavu zabezpečení](#))
- **Zkratková tlačítka** (v levé části okna) umožní rychlý přístup k nejdůležitějším a nejčastěji používaným funkcím **AVG Anti-Virus Free Edition 2012** - [podrobnosti >>](#)
- **Moje aplikace** (v levé spodní části okna) otevírají přehled doplňkových aplikací **AVG Anti-Virus Free Edition 2012**: [LiveKive](#), [Family Safety](#) a [PC Tuneup](#)
- **Přehled komponent** (ve střední části okna) nabízí přehled všech instalovaných komponent **AVG Anti-Virus Free Edition 2012** - [podrobnosti >>](#)



- **Ikona na systémové liště** (v pravém dolním rohu monitoru, na systémové liště) je indikátorem aktuálního stavu **AVG Anti-Virus Free Edition 2012** - [podrobnosti >>](#)
- **Miniaplikace AVG** (panel Windows sidebar, podporováno pouze v OS Windows Vista/7) umožňuje rychlý přístup k testování a aktualizaci programu - [podrobnosti >>](#)
- **Upgradovat vaši ochranu** (vpravo uprostřed) otevírá web AVG (<http://www.avg.cz/>) na stránce s porovnáním stávajícího zabezpečení vašeho počítače prostřednictvím **AVG Anti-Virus Free Edition 2012** proti možnosti plně profesionální ochrany poskytnuté některými z placených produktů AVG. Na této stránce máte rovněž možnost přejít přímo ke koupi zvoleného produktu AVG.

5.1. Systémové menu

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

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

5.1.1. Soubor

- **Konec** - zavírá uživatelské rozhraní **AVG Anti-Virus Free Edition 2012**. Aplikace AVG však zůstává spuštěna, běžící trvale na pozadí a váš počítač je stále chráněn!

5.1.2. Komponenty

Položka systémového menu [Komponenty](#) obsahuje odkazy k jednotlivým instalovaným komponentám AVG a otevírá uživatelské rozhraní vždy na jejich výchozí stránce:

- **Přehled komponent** - přepne uživatelské rozhraní na dialog [přehled komponent a jejich stavu](#)
- **Anti-Virus** detekuje na vašem počítači viry, spyware, červy, trojany, nežádoucí spustitelné soubory nebo knihovny a chrání vás před nimi - [podrobnosti >>](#)
- **Link Scanner** vás chrání před webovými útoky v době, kdy surfujete na Internetu - [podrobnosti >](#)
- **E-mailová Ochrana** kontroluje všechny přicházející e-mailové zprávy a filtruje SPAM, blokuje viry, phishingové útoky a jiné hrozby - [podrobnosti >>](#)
- **Anti-Rootkit** testuje všechny aplikace, ovladače a knihovny na přítomnost skrytých rootkitů - [podrobnosti >>](#)
- **PC Analyzer** analyzuje stav vašeho počítače a nabízí přehled zjištěných údajů - [podrobnosti >>](#)
- **Identity Protection** nepřetržitě chrání vaše digitální data před novými a neznámými hrozbami - [podrobnosti >>](#)



- **Security Toolbar** nabízí p ímý p ístup k vybraným funkcím AVG p ímo z prost edí vašeho internetového prohlíže e - [podrobnosti >>](#)

5.1.3. Historie

- [Výsledky test](#) - p epíná do testovacího rozhraní AVG, konkrétn do dialogu s p ehledem výsledk test .
- [Nálezy Rezidentního štítu](#) - otevírá dialog s p ehledem infekcí detekovaných [Rezidentním štítem](#)
- [Nálezy Kontroly pošty](#) - otevírá dialog s p ehledem p íloh detekovaných jako nebezpečné komponentou [Kontrola pošty](#)
- [Virový trezor](#) - otevírá rozhraní karanténního prostoru ([Virového trezoru](#)), kam jsou p esouvány detekované infek ní soubory, jež se nepoda ilo automaticky vylé it. V tomto prostoru jsou soubory zcela izolovány a tím je zajišt na naprostá bezpečnost vašeho počíta e, a sou asn zde lze soubory uložit pro p ípadnou další práci s nimi.
- [Protokol událostí](#) - otevírá rozhraní historie událostí s p ehledem všech protokolovaných akcí **AVG Anti-Virus Free Edition 2012**

5.1.4. Nástroje

- [Otestovat počíta e](#) - p epíná do [testovacího rozhraní AVG](#) a p ímo spouští [Test celého počíta e](#)
- [Otestovat zvolený adresá ...](#) - p epíná do [testovacího rozhraní AVG](#) a nabízí ve stromové struktu e vašeho disku možnost definovat ty složky, které mají být otestovány
- [Otestovat soubor...](#) - umož ũje spustit test na vyžádání nad samostatným souborem, který vyberete ve stromové struktu e na vašem disku
- [Aktualizovat](#) - automaticky spouští proces aktualizace **AVG Anti-Virus Free Edition 2012**
- **Aktualizace z adresá e...** - spustí proces aktualizace z aktualiza ního souboru umíst ěného v definovaném adresá i na lokálním disku. Tuto alternativu doporu ũjeme pouze jako náhradní ešení pro p ípad, že v danou chvíli nebude k dispozici p ípojení k Internetu (*nap . počíta e je zavirovaný a odpojený ze sít , počíta e je p ípojen k síti, kde není p ístup k Internetu, apod.*). V nov otev ěném okn vyberte adresá , do n íž jste p edem umístili aktualiza ní soubory, a spus te aktualizaci.
- [Pokro ilé nastavení...](#) - otevírá dialog [Pokro ilého nastavení AVG](#), kde máte možnost editovat konfiguraci **AVG Anti-Virus Free Edition 2012**. Obecn doporu ũjeme podržet výchozí výrobcem definované nastavení aplikace.

5.1.5. Nápověda

- **Obsah** - otevírá nápov du k programu AVG.
- **Získat podporu** - otevírá web **AVG Anti-Virus Free Edition 2012** (<http://free.avg.com/cz-cs/uvod/>) na [stránce centra zákaznické podpory](#).

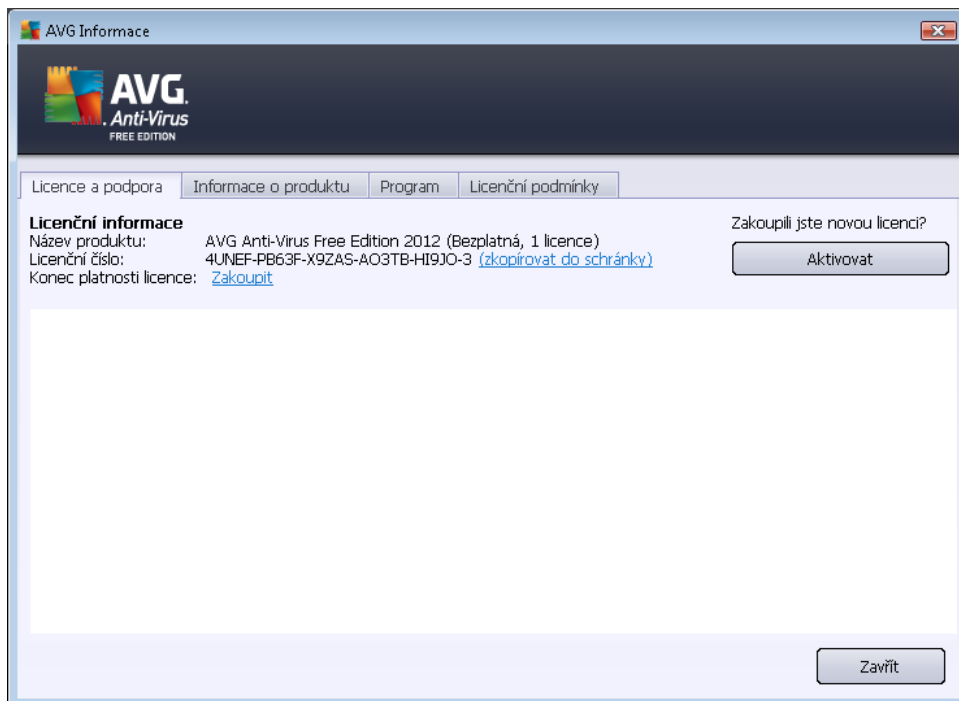


- **AVG na webu** - otevírá web **AVG Anti-Virus Free Edition 2012** (<http://free.avg.com/cz-cs/uvod/>).
- **Informace o virech** - otevírá web **AVG Anti-Virus Free Edition 2012** (<http://free.avg.com/cz-cs/uvod/>) na [stránce v nované podrobným informacím o virech a hrozbách](#), kde lze dohledat podrobné informace o detekovaných nálezech.
- **Zakoupit** - otevírá web AVG (<http://www.avg.cz/>) s možností online zakoupení plné verze programu AVG.
- **Aktivovat** - otevírá dialog **Aktivace AVG**, v němž jsou již předem vyplněna data zadaná během [instalace programu](#). V tomto dialogu můžete zadat své nové licenční číslo (například při přechodu na placený produkt z *AVG*), jímž nahradíte číslo odpovídající volné licenci AVG Free.
- **Zaregistrovat AVG Anti-Virus Free Edition 2012** - otevírá web **AVG Anti-Virus Free Edition 2012** (<http://free.avg.com/cz-cs/uvod/>) na [registračním formuláři](#). Vyplněním registračního formuláře získáte přístup k online diskusnímu fóru, které je pro **AVG Anti-Virus Free Edition 2012** jediným zdrojem technické podpory.
- **Přímiová 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.

5.1.6. Podpora

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

Záložka **Licence a podpora** nabízí přehled licenčních informací, tedy název produktu (*typ licence a počet povolených instalací*), licenční číslo a konec platnosti licence (*pro AVG Anti-Virus Free Edition 2012 není tato položka vyplněna, jelikož platnost free produktu není licenční nijak omezena*):



Ovládací prvky dialogu

Na záložce najdete tyto odkazy a tlačítka:

- **(Re)Aktivovat** - Tlačítkem otevřete nový dialog **AVG Aktivovat software**. Do tohoto dialogu zadejte své licenční číslo, kterým změníte dosavadní licenční číslo za jiné, například v případě na placený produkt z řady AVG. Můžete rovněž zadat své osobní údaje (*jméno, název firmy*).
- **Zkopírovat do schránky** - Licenční číslo musí být zadáno naprosto přesně ve tvaru, jak je uvedeno. Proto je třeba věnovat mimořádnou pozornost jeho přesnosti. Kliknutím na odkaz *Zkopírovat do schránky* bude vaše licenční číslo uloženo do schránky a můžete jej prostým vložením použít kdekoliv potřebujete. Tím je zajištěno, že při jeho přesnosti nedojde k chybě.
- **Zakoupit** - AVG Anti-Virus Free Edition 2012 je dostupný zdarma a jeho funkčnost je omezená. Pokud byste měli zájem o jeho používání zjistíte, že byste dali přednost plné funkčnosti profesionální verze AVG, klikněte na uvedený odkaz. Tím budete přesměrováni na web AVG (<http://www.avg.cz/>), kde najdete informace o možnostech koupě placených produktů AVG.



Záložka **Informace o produktu** podává p ehled nejd ležit jších technických informací o **AVG Anti-Virus Free Edition 2012**:



Záložka je roz len na do n kolika sekcí:

- **Informace o produktu** - seznam informací o verzi **AVG Anti-Virus Free Edition 2012**, verzi virové databáze, verzi komponenty [LinkScanner](#) a verzi komponenty [AVG Security Toolbar](#).
- **Instalované komponenty** - kompletní vý et všech aktuáln nainstalovaných komponent.
- **Instalovaná ochrana e-mailu** - p ehled instalovaných dopl k pro kontrolu pošty.
- **Informace o systému** - p ehled parametr vašeho opera ního systému: procesor, opera ní systém, verze Windows, íslo sestavení, service pack a údaje o celkovém a volném objemu pam ti.

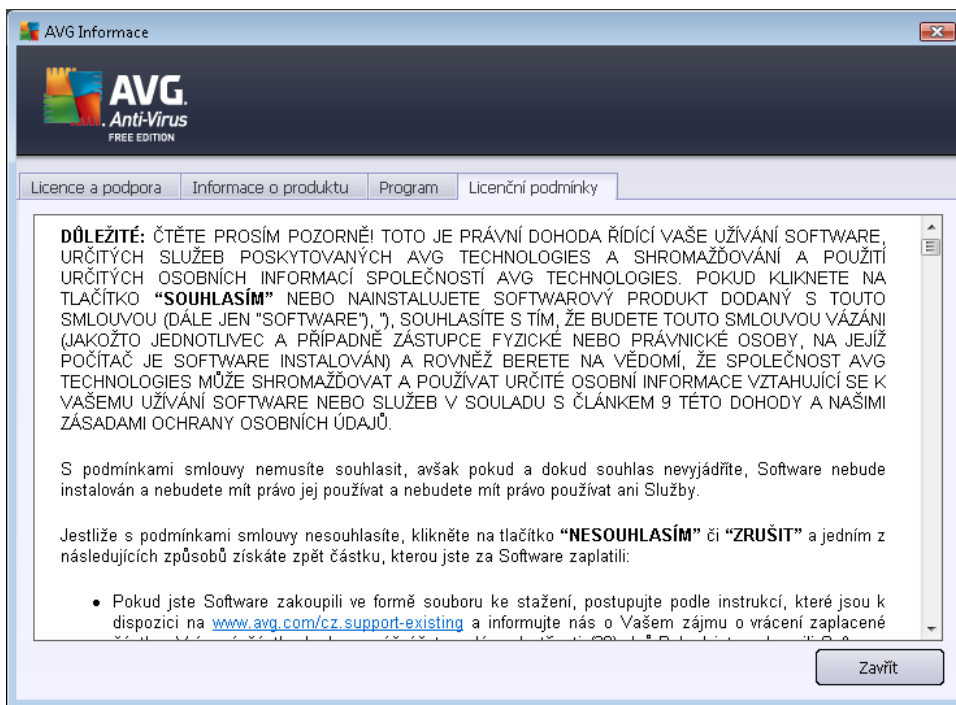


Záložka **Program** uvádí přesný název instalované edice **AVG Anti-Virus Free Edition 2012** a číslo verze instalačního souboru. Dále jsou uvedeny informace o použitých třetích stranách:





Na záložce **Licen ní podmínky** najdete plné zn ní licen ního ujednání mezi Vámi a společností AVG Technologies:



5.2. Informace o stavu zabezpečení

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



- Zelená ikona informuje, že program **AVG Anti-Virus Free Edition 2012 na vašem počítaři 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. Prosto prosím věnujte pozornost konfiguraci komponenty, která není nastavena k plné aktivitě! Jméno této komponenty bude v sekci **Informace o stavu zabezpečení** uvedeno.

Žlutá ikona se zobrazí rovněž v případě, kdy jste se z nějakého důvodu v domě rozhodli ignorovat chybový stav komponenty. Volba **Ignorovat stav komponenty** je dostupná z kontextového menu (*kontextové menu otevřete pravým tlačítkem myši*) nad ikonou komponenty v [přehledu komponent](#) v hlavním okně **AVG Anti-Virus Free Edition 2012**. Touto



volbou dáváte najevo, že jste si v domě v faktě, že se konkrétní komponenta nachází v chybovém stavu, ale z nějakého důvodu si nepřijete tento stav zachovat a nebyť na něj upozorování [ikonou na systémové liště](#). Může nastat situace, kdy budete potřebovat využít této možnosti, ale rozhodně nedoporučujeme, abyste v tomto stavu setrvali déle, než je nutné.

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



- Oranžová ikona **informuje o kritickém stavu AVG Anti-Virus Free Edition 2012!** Některá z komponent je nefunkční a **AVG Anti-Virus Free Edition 2012** nemůže plně chránit váš počítač. V tuto chvíli prosím okamžitou pozornost opravě tohoto problému.

V případě, kdy **AVG Anti-Virus Free Edition 2012** není nastaven k plnému a optimálnímu výkonu se vedle informace o stavu zabezpečení zobrazí tlačítko **Opravit** (případně **Opravit vše**, pokud se problém týká více než jediné komponenty), jehož stiskem **AVG Anti-Virus Free Edition 2012** automaticky spustí proces kontroly a přenastavení všech parametrů k optimálnímu výkonu. Tímto tlačítkem snadno uvedete program do optimálního stavu a zajistíte tak nejvyšší úroveň bezpečnosti!

Doporučujeme, abyste v nově zobrazených údajích v sekci **Informace o stavu zabezpečení** a pokud **AVG Anti-Virus Free Edition 2012** hlásí jakýkoliv problém, zaměřte se na jeho řešení. Pokud ignorujete chybová hlášení **AVG Anti-Virus Free Edition 2012**, váš počítač je ohrožen!

Poznámka: Informaci o stavu **AVG Anti-Virus Free Edition 2012** lze v kterémkoliv okamžiku práce na počítači získat také pohledem na [ikonu na systémové liště](#).

5.3. Zkratková tlačítka

Zkratková tlačítka najdete v levé části [uživatelského rozhraní](#) **AVG Anti-Virus Free Edition 2012**. Tato tlačítka umožní rychlý přístup k nejdůležitějším a nejčastěji používaným funkcím aplikace, tedy k zejména k testování a aktualizacím. Tlačítka jsou dostupná ze všech dialogů uživatelského rozhraní **AVG Anti-Virus Free Edition 2012**:



Zkratková tlačítka jsou graficky rozdělena do tří sekcí:

- **Spustit test** - Ve výchozím nastavení tlačítko uvádí informaci o testu, který byl spuštěn



naposledy (tedy typ testu a datum jeho posledního spuštění). Kliknutím na příkaz **Spustit test** dojde k opětovnému spuštění téhož testu. Pokud chcete spustit jiný test, klikněte na položku **Volby test**. Tím otevřete [testovací rozhraní AVG Anti-Virus Free Edition 2012](#), kde můžete přímo spustit libovolný test, naplánovat spuštění testu i editovat parametry testu. (Podrobnosti v kapitole [AVG Testování](#))

- **Volby test** - Tímto tlačítkem se z libovolného aktuálně otevřeného dialogu AVG vrátíte do úvodní obrazovky [hlavního dialogu AVG](#) s pohledem všech nainstalovaných komponent. (Podrobnosti najdete v kapitole [Pohled komponent](#))
- **Aktualizovat** - Tlačítko uvádí datum a čas, kdy byl naposledy spuštěn proces [aktualizace](#). Stiskem tlačítka aktualizaci rovnou spustíte a budete moci sledovat její průběh. (Podrobnosti v kapitole [Aktualizace AVG](#))

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

5.4. Přehled komponent

Rozdělení Pohledu komponent

Sekce **Pohled komponent** je umístěna ve střední části [uživatelského rozhraní AVG Anti-Virus Free Edition 2012](#). Tato sekce je rozdělena do dvou částí:

- **Pohled všech instalovaných komponent** je tvořen grafickými panely jednotlivých komponent. Každý panel je označen ikonou komponenty a nese informaci o tom, zda je tato komponenta aktuálně aktivní i neaktivní.
- **Popis komponenty** je umístěn ve spodní části dialogu a stručně Vás seznámí se základními funkcemi zvolené komponenty. Rovněž v této části najdete informaci o aktuálním stavu zvolené komponenty.

Seznam instalovaných komponent

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

- **Anti-Virus** detekuje na vašem počítači viry, spyware, červy, trojany, nežádoucí spustitelné soubory nebo knihovny a chrání vás před nimi - [podrobnosti >>](#)
- **Link Scanner** vás chrání před webovými útoky v době, kdy surfujete na Internetu - [podrobnosti >](#)
- **E-mailová Ochrana** kontroluje všechny přichozí e-mailové zprávy a filtruje SPAM, blokuje viry, phishingové útoky a jiné hrozby - [podrobnosti >>](#)



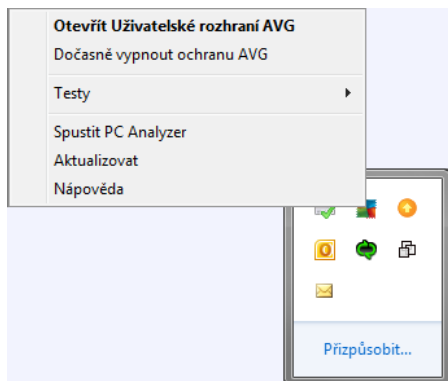
- **Anti-Rootkit** testuje všechny aplikace, ovladače a knihovny na přítomnost skrytých rootkit - [podrobnosti >>](#)
- **PC Analyzer** analyzuje stav vašeho počítače a nabízí přehled zjištěných údajů - [podrobnosti >>](#)
- **Identity Protection** nepřetržitě chrání vaše digitální data před novými a neznámými hrozbami - [podrobnosti >>](#)
- **Security Toolbar** nabízí přímý přístup k vybraným funkcím AVG přímo z prostředí vašeho internetového prohlížeče - [podrobnosti >>](#)

Dostupné akce





- **Přejezdem myši nad ikonou komponenty** tuto komponentu v přehledu vysvítíte a současně se ve spodní části [uživatelského rozhraní](#) zobrazí stručný popis funkce této komponenty.
- **Jednoduchým kliknutím na libovolnou ikonu komponenty** otevřete vlastní rozhraní komponenty s přehledem základních statistických dat.
- **Kliknutím pravého tlačítka myši nad ikonou komponenty** pak otevřete kontextové menu, které nabízí několik možností:
 - **Otevřít** - Kliknutím na tuto položku otevřete grafické rozhraní komponenty (*podobně jako jednoduchým kliknutím na vlastní ikonu komponenty*).
 - **Ignorovat stav komponenty** - Touto volbou dáváte najevo, že jste si v domě fakt, že se ta která [komponenta nachází v chybovém stavu](#), ale z nějakého důvodu si přejete tento stav zachovat a nebýt na něj upozorováni [ikonou na systémové liště](#).
 - **Otevřít v Pokročilém nastavení** - Tato volba je dostupná pouze u těch komponent, u nichž je možnost [pokročilého nastavení](#) k dispozici.

5.5. Ikona na systémové liště

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

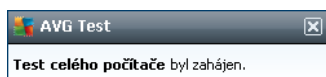


Zobrazení systémové ikony AVG

-  Jestliže je ikona zobrazena barevně bez dalších prvků, jsou všechny komponenty **AVG Anti-Virus Free Edition 2012** aktivní a plně funkční. Toto zobrazení ale také označuje situaci, kdy některá z komponent není v plně funkčním stavu, ale uživatel se rozhodl [ignorovat stav komponenty](#). (Volbou ignorovat stav komponenty dáváte najevo, že jste si v domě na vlastní odpovědnost a riziko rozhodli zachovat a nebyť na něj upozorováni.)
-  Pokud je ikona zobrazena s výkřikem, znamená to, že některá komponenta (i více komponent) je v [chybovém stavu](#). Vnujte 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 informace o tom, která komponenta je v [chybovém stavu](#), najdete v sekci [informace o stavu zabezpečení](#).
-  Ikona na systémové liště může být také zobrazena barevně s probleskujícím otáčejícím se paprskem. Toto grafické znázornění signalizuje právě probíhající aktualizaci **AVG Anti-Virus Free Edition 2012**.
-  Alternativní zobrazení ikony s šipkou znamená, že právě začíná který z testů **AVG Anti-Virus Free Edition 2012**.

Informace systémové ikony AVG

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





Akce dostupné ze systémové ikony AVG

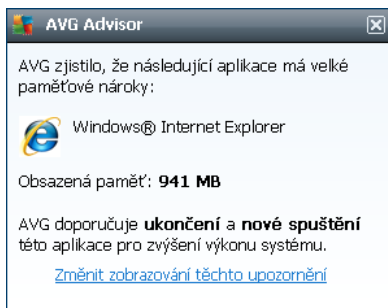
Ikonu AVG na systémové liště lze také použít pro rychlý přístup k [uživatelské rozhraní aplikace AVG Anti-Virus Free Edition 2012](#), to se otevře dvojklikem na ikonu. Kliknutí pravým tlačítkem myši nad ikonou otevírá kontextové menu s těmito možnostmi:

- **Otevřít uživatelské rozhraní AVG** - Otevře [uživatelské rozhraní aplikace AVG Anti-Virus Free Edition 2012](#).
- **Dočasně vypnout ochranu AVG** - Položka umožňuje jednorázově deaktivovat celou ochranu zajištěnou programem **AVG Anti-Virus Free Edition 2012**. Můžete prosím pamatovat, že tato volba by v žádném případě neměla být použita, pokud to není opravdu nezbytně nutné! V naprosté většině případů není nutné deaktivovat **AVG Anti-Virus Free Edition 2012** před instalací nového software nebo ovladače, a to ani tehdy, pokud budete během instalace vyzváni k zavěšení všech spuštěných aplikací. Jestliže budete opravdu nuceni deaktivovat **AVG Anti-Virus Free Edition 2012**, zapněte jej hned, jakmile to bude možné. Pamatujte, že pokud jste připojeni k Internetu nebo k jiné síti, je váš počítač bez aktivní ochrany vysoce zranitelný.
- **Testy** - Otevře vysunovací nabídku [přednastavených testů](#) ([Test celého počítače](#), [Test vybraných souborů a 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*.
- **Spustit PC Analyzer** - Spustí komponentu [PC Analyzer](#).
- **Aktualizovat** - Spustí okamžitou [aktualizaci AVG Anti-Virus Free Edition 2012](#).
- **Nápověda** - Otevře soubor nápovědy na úvodní stránce.

5.6. AVG Advisor

Hlavním úkolem **AVG Advisoru** je detekovat problémy, které mohou zpomalovat nebo ohrožovat váš počítač, a navrhnout jejich řešení. Pokud se vám zdá, že se váš počítač náhle výrazně zpomalil (*a už při prohlížení Internetu i 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, přibližně monitoruje všechny běžící procesy, preventivně upozoruje 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 aktuální otevřeného webového prohlížeče.** U webového prohlížeče můžete 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 známým sítím. Narazíte-li na neznámou síť s obvyklým a zdánlivě známým jménem (*například Doma nebo MojeWifi*), můžete dojít k omylu a náhodně se tak připojíte k neprověřené a potenciálně nebezpečné síti. **AVG Advisor** dokáže této situaci předejít a 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 připojení k této síti se již notifikace **AVG Advisoru** nezobrazí.

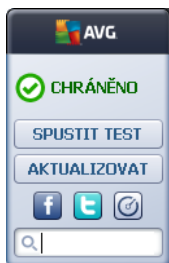
V každé z těchto situací Vás **AVG Advisor** varuje před možným konfliktem a zobrazí jméno a ikonu problematického procesu či aplikace. Dále pak navrhne jednoduché řešení, kterým lze problém předejít.

Podporované webové prohlížeče

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



5.7. Miniaplikace AVG

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



Rychlé spuštění testu nebo aktualizace

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

- **Spustit test** - kliknutím na volbu **Spustit test** spustíte přímo z prostředí miniaplikace [test celého počítače](#). Jeho průběh můžete sledovat v pozmiňném rozhraní miniaplikace v jednoduchém statistickém pohledu, kde najdete informace o počtu otestovaných objektů, detekovaných hrozbách a vyladěných hrozbách. V průběhu testu můžete proces testování kdykoliv pozastavit  nebo ukončit . Pro přístup k podrobným informacím o výsledku použijte odkaz **Zobrazit detaily**, kterým otevřete hlavní uživatelské rozhraní s pohledem dat z průběhu testu.




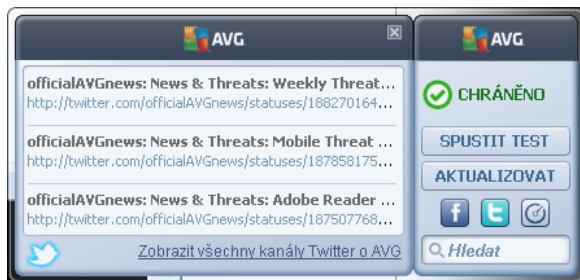
- **Aktualizovat** - kliknutím na volbu **Aktualizovat** spustíte proces aktualizace **AVG Anti-Virus Free Edition 2012** přímo z prostředí miniaplikace:




Přístup k sociálním sítím


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

- **Twitter**  - otevírá další rozhraní **Miniaplikace AVG** s p ehledem nejnov ějších záznam ō AVG uve ejn ěných na sociální síti Twitter. Stiskem odkazu **Zobrazit všechny kanály AVG Twitter** otev ete nové okno vašeho internetového prohlíže ě a budete p esm ěrování p ěmo na web Twitter, konkrétn ě na stránku s p ehledem novinek týkajících se AVG:



- **Facebook**  - otevírá internetový prohlíže ě na webu sociální síti Facebook, konkrétn ě na stránce **AVG komunity**

Další funkce dostupné z miniaplikace

- **PC Analyzer**  - otevírá uživatelské rozhraní komponenty [PC Analyzer](#)
- **Vyhledávání** - zadejte klíčové slovo a výsledky vyhledávání se zobrazí v nov ě otev ěném okn ě prohlíže ě, který obvykle používáte



6. Komponenty AVG

6.1. Anti-Virus

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

- [Testovací jádro](#)
- [Rezidentní ochranu](#)
- [Anti-Spyware ochranu](#)

6.1.1. Testovací jádro

Testovací jádro, které je základem komponenty **Anti-Virus**, testuje všechny soubory a jejich aktivitu (*otevírání/zavírání souboru atd.*) a provádí je v případě potřeby v přítomnosti známých virů. Pokud detekuje virus, okamžitě zabrání, aby mohl být aktivován a následně jej odstraní nebo přesune do [Virového trezoru](#).

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

Detekční metody

Většina antivirových programů používá metodu heuristické analýzy, při níž jsou soubory testovány na přítomnost typických virových charakteristik. To znamená, že antivirový skener dokáže rozpoznat i nový, dosud neznámý virus podle toho, že tento virus nese určité znaky typické pro již existující viry. Komponenta **Anti-Virus** používá k detekci počítačových virů následující techniky:

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

V případech, kdy použití jediné techniky nepostačí, umožňuje **AVG Anti-Virus Free Edition 2012** kombinaci uvedených technik v rámci jednoho testu. Příkladem může být situace, kdy je virus zachycený skenováním přesně identifikován pomocí heuristické analýzy. **AVG Anti-Virus Free Edition 2012** umí také analyzovat spustitelné programy, případně DLL knihovny a určité, které z nich by mohly být potenciálně nežádoucí (*jak o například spyware, adware aj.*). Na žádost uživatele umožní tyto programy odstranit i k nim zablokovat přístup.

AVG Anti-Virus Free Edition 2012 poskytuje vašemu počítači nepřetržitou ochranu!



6.1.2. Rezidentní ochrana

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

Rezidentní ochrana se na počítači automaticky, ihned po spuštění, a je nanejvýš důležitá, aby byla zapnuta nepřetržitě !

6.1.3. Anti-Spyware ochrana

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

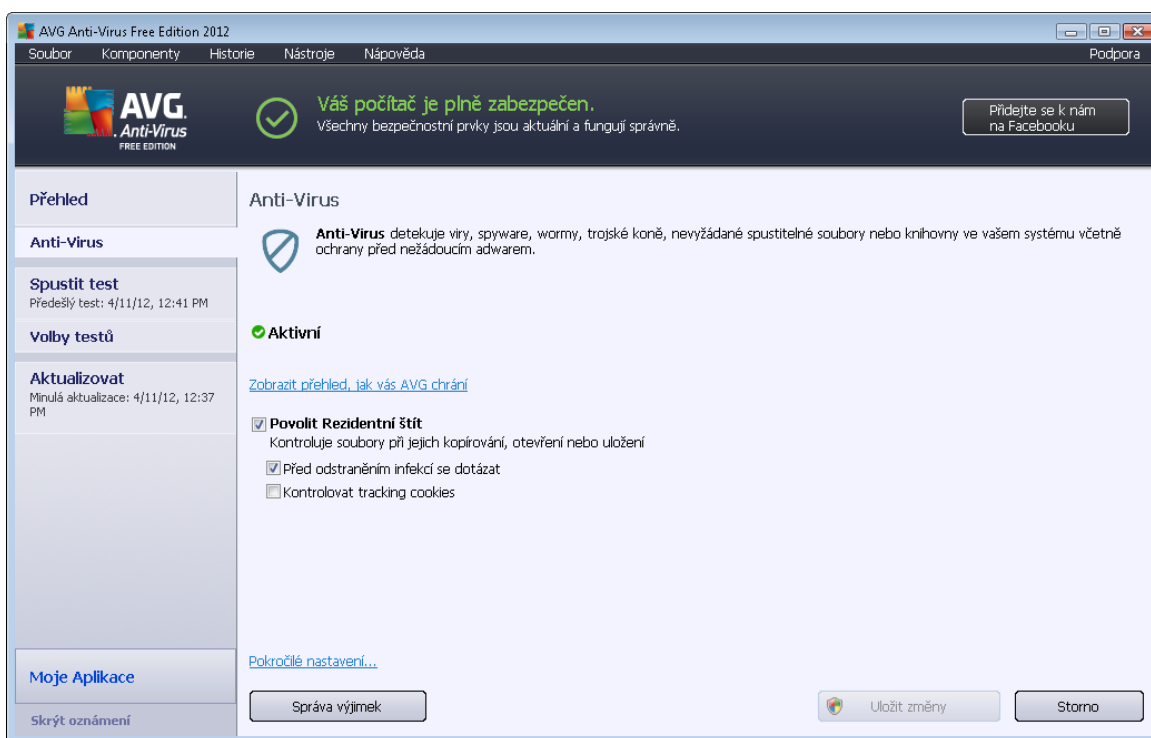
Co je to spyware?

Spyware se obvykle definuje jako jeden z typů malware, to jest software, který z vašeho počítače sbírá informace bez vašeho vědomí. Některé aplikace typu spyware mohou být nainstalovány na váš počítač záměrně; ostatním příkladem jsou třeba reklamní upoutávky, pop-up okna nebo jiné typy obtížného software. V ideálním případě byste se měli pokusit zabránit jakémukoli druhu spyware a/ nebo malware v samotném průběhu na váš počítač. Nejčastějším zdrojem nákazy jsou v současné době webové stránky s potenciálně nebezpečným obsahem. Rozšířen je i přenos pomocí e-mailu nebo prostřednictvím serverů a virů. Nejdůležitějším prvkem ochrany je tedy trvale zapnutý scanner běžící na pozadí, jakým je například **Anti-Spyware**: pracuje nepřetržitě a na pozadí provádí veškeré aplikace, které spouštíte.



6.1.4. Rozhraní komponenty Anti-Virus

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



Možnosti konfigurace

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

- **Zobrazit online přehled, jak vás AVG chrání** - Kliknutím na odkaz budete přerouváni na speciální stránku na webu AVG (<http://www.avg.cz/>). Na této stránce najdete detailní statistický přehled všech aktivit **AVG Anti-Virus Free Edition 2012**, které proběhly na vašem počítači za určený časový úsek i celkově od okamžiku instalace programu.
- **Povolit Rezidentní štít** - Označením i naopak dostraněním označení u této položky jednoduše zapnete nebo vypnete rezidentní ochranu. **Rezidentní štít** testuje soubory při jakémkoliv inzerování s nimi prováděném, tedy při jejich kopírování, otevírání i ukládání. Pokud by při něm bylo zjištěno, že byl detekován virus, budete o nález okamžitě vyrozuměni. Ve výchozím nastavení je tato funkce zapnuta, a doporučujeme, abyste ji zapnutou ponechali! Pokud se rozhodnete ponechat rezidentní ochranu spuštěnou, máte dále možnost definovat, jak má být s případnou zachycenou infekcí naloženo:
 - **Před odstraněním infekcí se dotázat** - Ponechejte tuto položku označenou, pokud chcete být při detekci hrozby dotázáni na to, jaké kroky mají být dále podniknuty. V opačném případě bude hrozba automaticky přesunuta do **Virového trezoru**. Tato vaše



volba nemá žádný vliv na úroveň bezpečnosti a je pouze preferenční.

- o **Kontrolovat Tracking Cookies** - Nezávisle na předchozí volbě můžete dále rozhodnout, zda se mají kontrolovat tracking cookies. (*Cookies = malé množství dat v protokolu HTTP, která server pošle prohlížeči, aby je uložil na počítači uživatele. Při každé další návštěvě téhož serveru pak prohlížeč tato data posílá zpět serveru, který podle nich rozlišuje jednotlivé uživatele, například při ukládání obsahu nákupního košíku, atp.*) V odvolaných případech slouží tato možnost k dosažení vyššího stupně bezpečnosti, ve výchozím nastavení je však vypnuta.
- **Pokročilé nastavení** - Kliknutím na odkaz budete přesměrováni do příslušného dialogu [Pokročilého nastavení AVG Anti-Virus Free Edition 2012](#), kde můžete editovat konfiguraci komponenty do nejmenších podrobností. Mějte však na paměti, že výchozí konfigurace všech komponent **AVG Anti-Virus Free Edition 2012** je nastavena tak, aby program podával optimální výkon a poskytoval maximální možnou úroveň bezpečnosti. Pokud nemáte skutečně důvod ke změně, doporučujeme ponechat výchozí nastavení!

Ovládací tlačítka dialogu

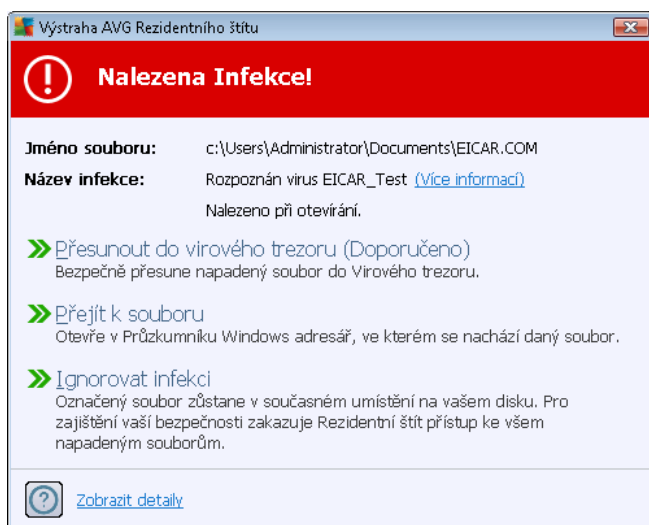
V dialogu jsou dostupné tyto ovládací prvky:

- **Správa Výjimek** - Otevře nový dialog nazvaný [Rezidentní štít - Výjimky](#). Tento dialog je rovněž dostupný prostřednictvím hlavního menu, a to touto cestou: [Pokročilé nastavení / Anti-Virus / Rezidentní štít / Výjimky](#) (*podrobný popis tohoto dialogu najdete v příslušné kapitole*). V tomto dialogu můžete specifikovat soubory nebo adresáře, které mají být vyňaty z kontroly Rezidentním štítem. Pokud to není nezbytně nutné, doporučujeme, abyste z testování žádné položky nevyjímali! V dialogu jsou k dispozici tato ovládací tlačítka:
 - o *Přidat cestu* – Umožňuje výběrem z navigačního stromu lokálního disku určit adresáře s celým obsahem, který má být vyňat z testování.
 - o *Přidat soubor* – Umožňuje výběrem z navigačního stromu lokálního disku po jednom vybrat další soubory definované jako výjimky z testování.
 - o *Editovat* – Umožňuje editovat zadání cesty ke zvolenému souboru nebo adresáři.
 - o *Odstranit* – Umožňuje odstranit cestu ke zvolenému souboru nebo adresáři.
- **Uložit změny** - Uloží všechny změny v nastavení komponenty provedené v tomto dialogu a poté přepne aplikaci do hlavního [uživatelského rozhraní AVG Anti-Virus Free Edition 2012](#) (*přehled komponent*).
- **Storno** - Zruší veškeré změny v nastavení komponenty provedené v tomto dialogu. Žádná z provedených změn nebude uložena. Následně bude aplikace přepnuta do hlavního [uživatelského rozhraní AVG Anti-Virus Free Edition 2012](#) (*přehled komponent*).

6.1.5. Nález Residentního štítu

Nalezena infekce!

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



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

Dále je třeba, abyste se rozhodli, co se má s infikovaným souborem udělat. K dispozici se nabízí několik alternativ. **Máte prosím na paměti, že nemusí být vždy dostupné všechny možnosti! Jednotlivé nabídky ešení se zobrazují na základě specifických podmínek (například jaký typ souboru je infikován, kde je umístěn a podobně):**

- **Léčit** (*toto je doporučené ešení*) - toto tlačítko se zobrazí pouze v případě, že detekovanou infekci lze léčit. V takovém případě odstraní infekci ze souboru a obnoví soubor do původního stavu. V případě, že soubor jako celek je virus, bude při aplikaci této funkce vymazán (*přesunut do [Virového trezoru](#)*)
- **Přesunout do virového trezoru** (*toto je doporučené ešení*) - infikovaný objekt bude přesunut do karanténního prostředí [Virového trezoru](#)
- **Přejít k souboru** - touto volbou zjistíte, kde je podezřelý objekt fyzicky umístěn (*otevře se nové okno Průzkumníka Windows*)
- **Ignorovat** - infikovaný objekt zůstane v původním umístění na disku, ale přístup k němu je zablokován.

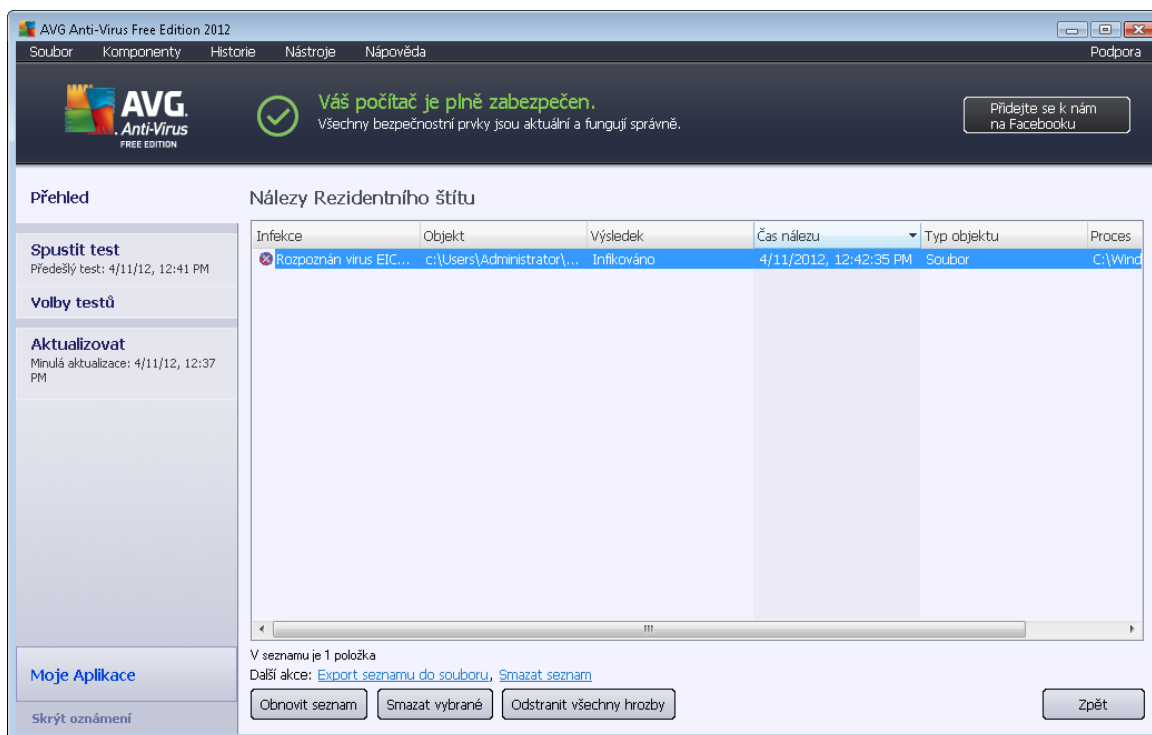
Poznámka: Máte se stát, že velikost detekovaného objektu bude větší než objem volného prostoru ve Virovém trezoru. V tom případě budete při pokusu o přesunutí infikovaného objektu vyzváni varovným hlášením o nedostatku místa ve Virovém trezoru. Objem Virového trezoru si však můžete



sami nastavit. Velikost prostoru ve Virovém trezoru je dána procentuálně a závisí na celkové velikosti vašeho pevného disku. Nastavení velikosti Virového trezoru lze provést v dialogu [Virový trezor](#) v rámci [Pokročilého nastavení AVG](#), položka 'Omezit velikost Virového trezoru'.

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

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



V dialogu najdete seznam objektů, které byly [Rezidentním štítem](#) detekovány jako nebezpečné a byly to vyloučeny nebo přesunuty do [Virového trezoru](#). U každého z detekovaných objektů jsou k dispozici následující informace:

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



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

6.2. LinkScanner

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

LinkScanner není určen k ochraně serverů!

Technologie **LinkScanner** obsahuje tři hlavní funkce:

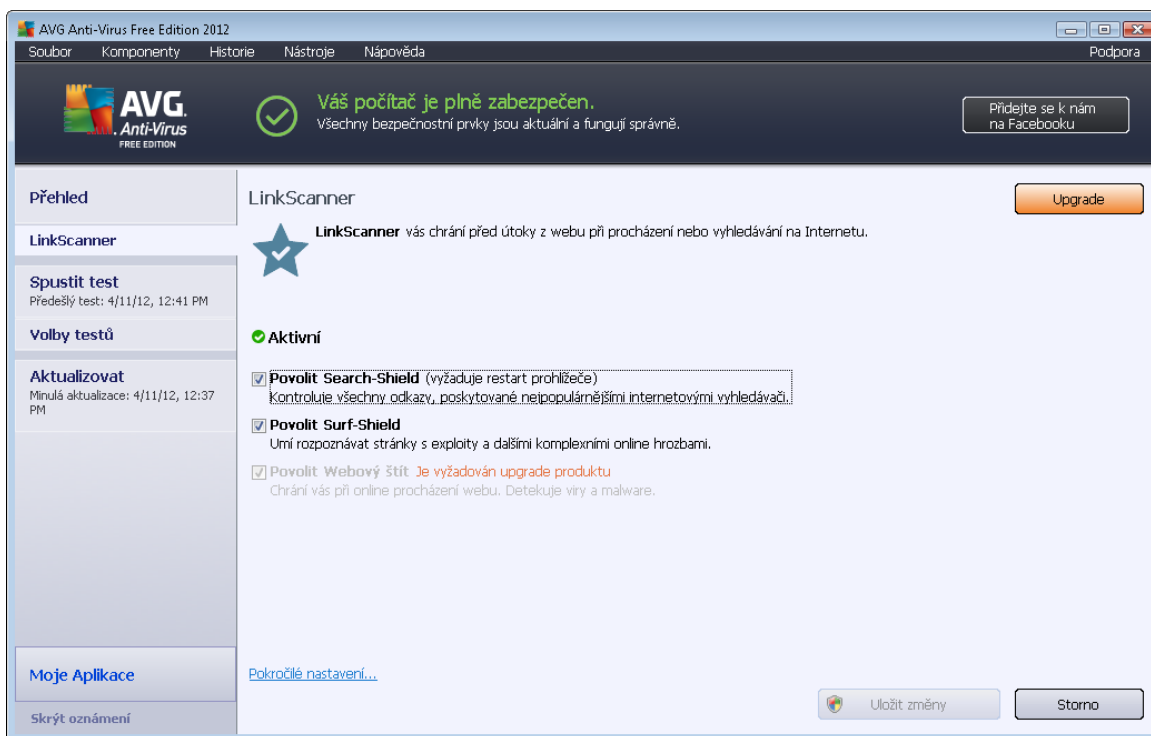
- **Search-Shield** obsahuje seznam stránek (*URL adres*), které jsou známy jako infikované. Při hledání skrze vyhledávače Google, Yahoo! JP, bezpečné vyhledávání AVG, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, Digg, a SlashDot, anebo při vyhledávání v sociálních sítích Facebook, Twitter a MySpace jsou všechny výsledky zkontrolovány na základě tohoto seznamu a ke každé položce je zobrazena verdiktová ikona.
- **Surf-Shield** zabráňuje infikování počítače při nechtěném stahování nebezpečných souborů a skriptů a zároveň zajišťuje, že stránky, které navštívíte, nabízejí ve chvíli jejich otevření bezpečný obsah. Funkce testuje obsah internetových stránek, které navštívíte, bez ohledu na internetovou adresu stránky. Pokud tedy nebyla určitá stránka detekována funkcí **Search-Shield**, může být detekována a blokována právě funkcí **Surf-Shield** při přístupu na ni.
- **Webový štít** funguje jako ochrana v reálném čase při surfování po Internetu. Tato služba testuje obsah navštívených webových stránek a souborů v nich obsažených, a to ještě předtím, než jsou zobrazeny ve vašem prohlížeči nebo staženy na váš počítač. Webový štít detekuje případné viry a spyware obsažené ve stránce, kterou se chystáte navštívit, a okamžitě zabrání jejich stažení. V rámci edice **AVG Anti-Virus Free Edition 2012** je však tato funkce deaktivována a je dostupná pouze v placených AVG produktech!

AVG Anti-Virus Free Edition 2012 je dostupný zdarma a jeho funkčnost je omezená. Pokud bychom používali AVG Anti-Virus Free Edition 2012 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.



6.2.1. Rozhraní Link Scanneru

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








Ve spodní části dialogu lze provést základní nastavení funkcí komponenty:

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

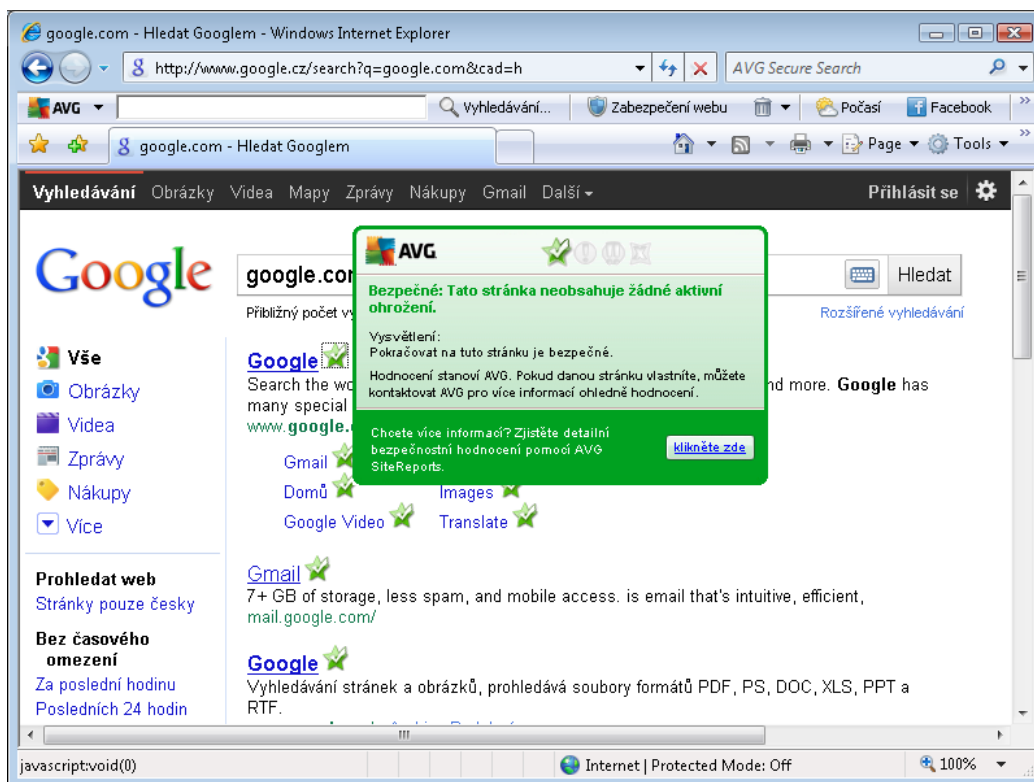
V rámci edice AVG Anti-Virus Free Edition 2012 je služba Webový štít deaktivována. Tato služba je dostupná pouze v placených verzích AVG! Jelikož je AVG Anti-Virus Free Edition 2012 poskytován zdarma, jeho funkčnost je omezená. Pokud bychom používali AVG Anti-Virus Free Edition 2012 zjistíte, že byste dali přednost plně funkční profesionální verze AVG, navštivte prosím web AVG (<http://www.avg.cz/>), kde najdete informace o možnostech koupě placených produktů AVG.

6.2.2. Nález služby Search-Shield

Při prohlížení Internetu se zapnutou kontrolou **Search-Shield** budou všechny výsledky vyhledávání pomocí nejrozšířenějších vyhledávačů (*Google, Yahoo!, bezpečné vyhledávání AVG, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Digg a SlashDot*) vyhodnoceny z hlediska bezpečnosti a rozdíleny na odkazy bezpečné a nebezpečné. Označením jednotlivých odkazů grafickými ikonami vás **Link Scanner** varuje před vstupem na nebezpečnou nebo podezřelou stránku. Během vyhodnocování jednotlivých odkazů vrácených jako výsledky vyhledávání uvidíte u každého odkazu grafický symbol označující probíhající ověření odkazu. Jakmile je kontrola dokončena, u jednotlivých odkazů budou zobrazeny následující informace:

-  Odkazovaná stránka je bezpečná.
-  Odkazovaná stránka neobsahuje žádné konkrétní hrozby, ale jeví se jako podezřelá (*je sporný její pověst, protože ji nelze doporučit například pro aktivity typu on-line nakupování a podobně*).
-  Odkazovaná stránka může být sama o sobě bezpečná, ale obsahuje odkazy na jiné nebezpečné stránky. Nebo jde o stránku s podezřelým kódem.
-  Odkazovaná stránka obsahuje aktivní hrozby! Pro vlastní bezpečnost vám nebude umožněno na tuto stránku vstoupit.
-  Odkazovaná stránka je nepřístupná a nemohla tedy být prověřena.

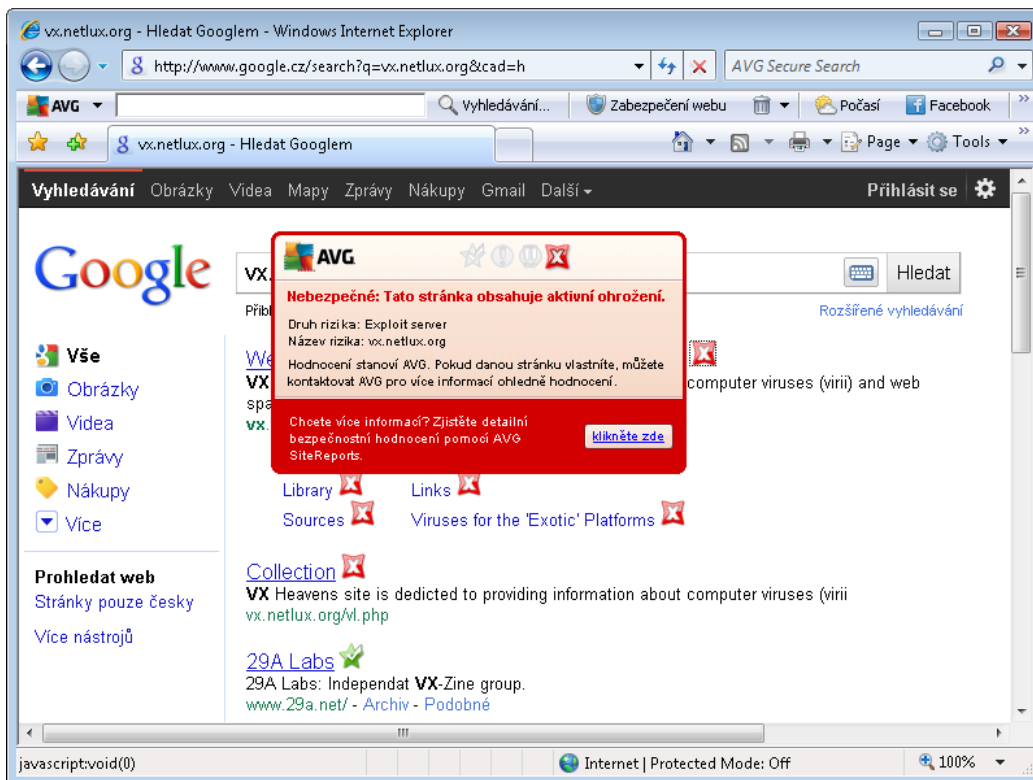
Při přejetí myší nad jednotlivými ikonami s hodnocením bezpečnosti odkazu se pak zobrazí detailní informace (*podrobnosti o hrozbě, pokud byla nalezena, IP adresa odkazu a datum kontroly odkazu službou AVG Search-Shield*) o odkazu:



6.2.3. Nálezy služby Surf-Shield

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

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



Vstup na takto označenou stránku rozhodně nedoporučujeme!

6.3. E-mailová ochrana

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

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

- [Kontrola příchozí a odchozí pošty](#)
- Anti-Spam - tato služba bohužel není v rámci **AVG Anti-Virus Free Edition 2012** dostupná a je k dispozici pouze v placených produktech AVG

AVG Anti-Virus Free Edition 2012 je dostupný zdarma a jeho funkčnost je omezená. Pokud během používání AVG Anti-Virus Free Edition 2012 zjistíte, že byste dali přednost plně funkční profesionální verzi AVG, navštivte prosím web AVG (<http://www.avg.cz/>), kde



najdete informace o možnostech koup placených produkt AVG.

6.3.1. Kontrola pošty

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

Při [instalaci](#) AVG dojde k vytvoření automatických serverů pro kontrolu příchozí i odchozí pošty, s jejichž pomocí je následně automaticky kontrolována pošta na portech 110, 25 a 143 (standardní porty pro příjem/odesílání pošty).

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

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

6.3.2. Rozhraní komponenty E-mailová ochrana

AVG Anti-Virus Free Edition 2012

Soubor Komponenty Historie Nástroje Nápověda Podpora

AVG Anti-Virus FREE EDITION

Váš počítač je plně zabezpečen.
Všechny bezpečnostní prvky jsou aktuální a fungují správně.

Přidejte se k nám na Facebooku

Přehled

E-mailová ochrana Upgrade

E-mailová ochrana kontroluje vaše příchozí e-mailové zprávy a hledá nevyžádané (SPAM), blokuje viry, útoky typu phishing a další hrozby.

Aktivní

Zobrazit přehled, jak vás AVG chrání

Test příchozích zpráv
Kontroluje všechny příchozí e-mailové zprávy.

Test odchozích zpráv
Kontroluje všechny odchozí e-mailové zprávy.

Zobrazit informační okno v systémové liště během testování e-mailu

Povolit Anti-Spam **Je vyžadován upgrade produktu**
Kontroluje veškeré příchozí e-mailové zprávy a nevyžádané označuje jako SPAM.

Moje Aplikace Pokročile nastavení...

Skrýt oznámení Uložit změny Storno



V dialogu **E-mailová ochrana** najdete stručný popis funkce komponenty a informaci o aktuálním stavu komponenty (*Aktivní*). Prostednictvím odkazu **Zobrazit online přehled, jak Vás AVG chrání** se můžete přepnout na dedikovanou stránku na webu AVG (<http://www.avg.cz/>), kde najdete detailní statistiku aktivity a detekcí **AVG Anti-Virus Free Edition 2012**.

Základní nastavení E-mailové ochrany

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

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

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

Položka **Povolit Anti-Spam** aktivuje filtraci nežádoucích zpráv v příchozí poště. Služba Anti-Spam však bohužel není v rámci **AVG Anti-Virus Free Edition 2012** dostupná a je k dispozici pouze v placených produktech AVG.

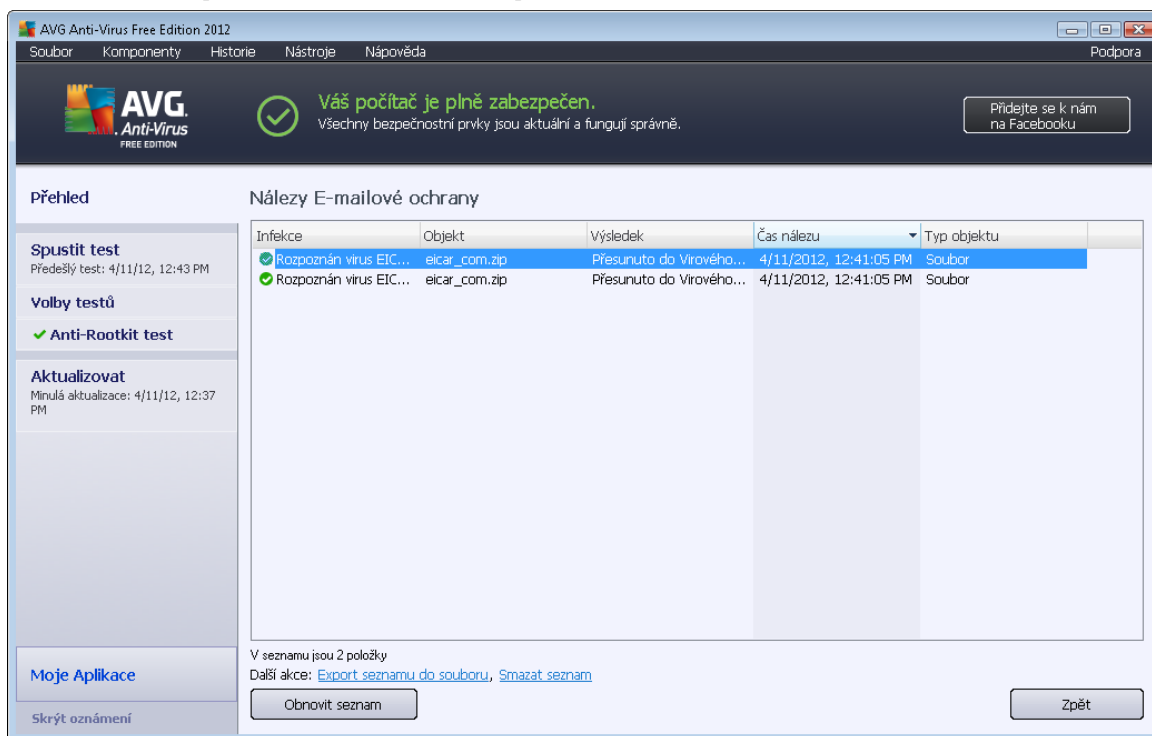
AVG Anti-Virus Free Edition 2012 je dostupný zdarma a jeho funkčnost je omezená. Pokud během používání AVG Anti-Virus Free Edition 2012 zjistíte, že byste dali přednost plně funkční profesionální verzi AVG, navštivte prosím web AVG (<http://www.avg.cz/>), kde najdete informace o možnostech koupě placených produktů AVG.

Ovládací tlačítka

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

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

6.3.3. Nález E-mailové ochrany



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

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

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

Ovládací tlačítka

Ovládací tlačítka dostupná v dialogu **Nález Kontrolы pošty**:

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

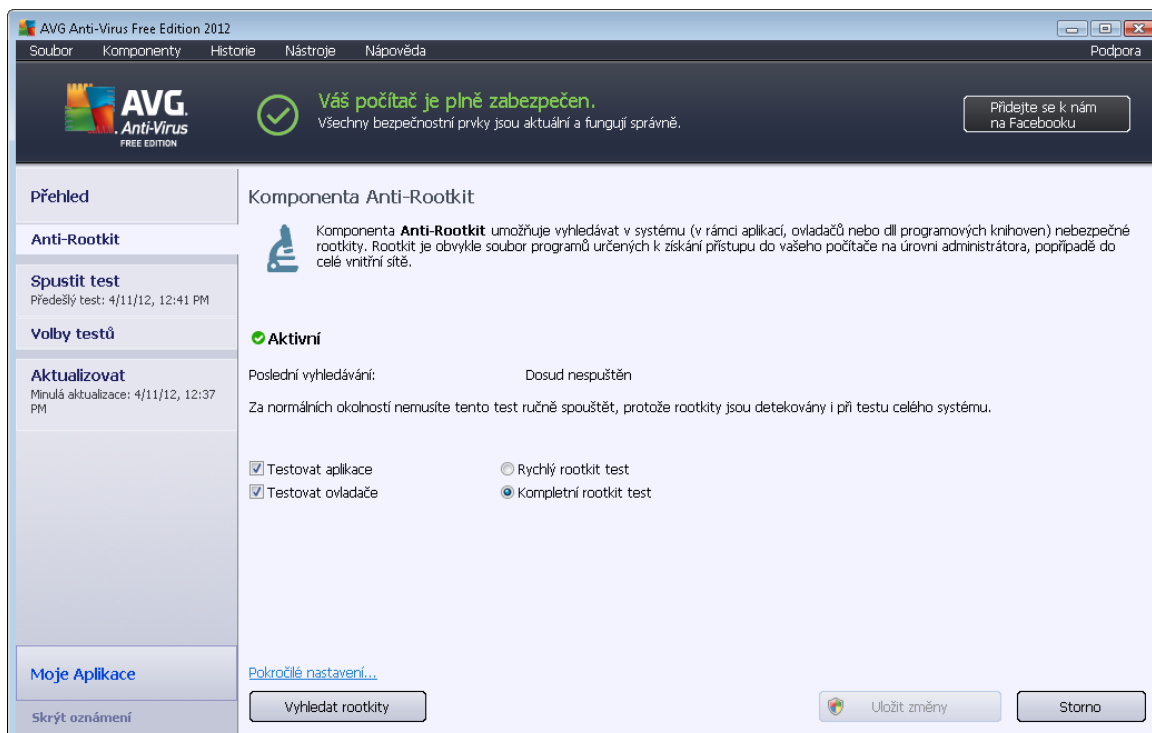
6.4. Anti-Rootkit

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

Co je to rootkit?

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

6.4.1. Rozhraní komponenty Anti-Rootkit



Dialog komponenty **Anti-Rootkit** uvádí stručný popis základní funkce této komponenty, informaci o stavu komponenty (*Aktivní*) a dále informaci o době a času posledního spuštění



komponenty (*Poslední vyhledávání; vyhledávání rootkit* probíhá ve výchozím nastavení automaticky v rámci [Testu celého počítače](#)). V dialogu komponenty **Anti-Rootkit** je dále uveden odkaz [Nástroje/Pokročilé nastavení](#), kterým se přepnete do prostředí editace komponenty **Anti-Rootkit**.

Všechny komponenty AVG jsou výrobcem nastaveny k optimálnímu výkonu. Pokud nemáte skutečný důvod jejich konfiguraci změnit, doporučujeme ponechat program ve výchozím nastavení. Změny konfigurace by měly provádět pouze zkušení uživatelé.

Základní nastavení Anti-Rootkitu

Ve spodní části dialogu můžete nastavit, které základní funkce testu na přítomnost rootkitů. Nejprve označením příslušného políčka (*jednoho nebo více*) označíte, jaké objekty mají být testovány:

- **Testovat aplikace**
- **Testovat ovladače**

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

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

Ovládací tlačítka dialogu

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

6.5. PC Analyzer

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



AVG Anti-Virus Free Edition 2012

Soubor Komponenty Historie Nástroje Nápověda Podpora

Váš počítač je plně zabezpečen.
Všechny bezpečnostní prvky jsou aktuální a fungují správně.

Přidejte se k nám na Facebooku

Přehled

PC Analyzer

Spustit test
Předěšlý test: 4/11/12, 12:41 PM

Volby testů

Aktualizovat
Minulá aktualizace: 4/11/12, 12:37 PM

Moje Aplikace

Skrýt oznámení

Komponenta PC Analyzer

Komponenta PC Analyzer prověří váš počítač a ohlásí potíže, které ovlivňují jeho výkon. Stáhněte si nový [AVG PC Tuneup](#) a opravte jednorázově nalezené problémy zdarma, nebo si zakupte neomezené opravy potíží na 12 měsíců. [Provést analýzu](#)

PC Analyzer je připraven k analýze vašeho počítače

Kategorie	Chyb	Závažnost
Chyby v registrech Chyby ovlivňují stabilitu systému		
Nepotřebné soubory Tyto soubory zabírají místo na disku		
Fragmentace Snižuje rychlost přístupu k disku		
Neplatní Zástupci Snižuje rychlost procházení v Průzkumníkovi		

Provést analýzu Storno

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

AVG Anti-Virus Free Edition 2012

Soubor Komponenty Historie Nástroje Nápověda Podpora

Váš počítač je plně zabezpečen.
Všechny bezpečnostní prvky jsou aktuální a fungují správně.

Přidejte se k nám na Facebooku

Přehled

PC Analyzer

Spustit test
Předěšlý test: 4/11/12, 12:41 PM

Volby testů

Aktualizovat
Minulá aktualizace: 4/11/12, 12:37 PM

Moje Aplikace

Skrýt oznámení

Komponenta PC Analyzer

Komponenta PC Analyzer prověří váš počítač a ohlásí potíže, které ovlivňují jeho výkon. Stáhněte si nový [AVG PC Tuneup](#) a opravte jednorázově nalezené problémy zdarma, nebo si zakupte neomezené opravy potíží na 12 měsíců. [Provést analýzu](#)

PC Analyzer dokončil analýzu

Kategorie	Chyb	Závažnost
Chyby v registrech Chyby ovlivňují stabilitu systému	Bylo nalezeno 139 chyb Detaily...	
Nepotřebné soubory Tyto soubory zabírají místo na disku	Bylo nalezeno 237 chyb Detaily...	
Fragmentace Snižuje rychlost přístupu k disku	Fragmentováno 10% Detaily...	
Neplatní Zástupci Snižuje rychlost procházení v Průzkumníkovi	Bylo nalezeno 14 chyb Detaily...	

Opravit Storno

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



pomrn pokroilé znalosti, nedoporuujeme vám tudíž pouštět se do opravy na vlastní pěst.

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

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

Ovládací tlačítka

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

6.6. Identity Protection

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

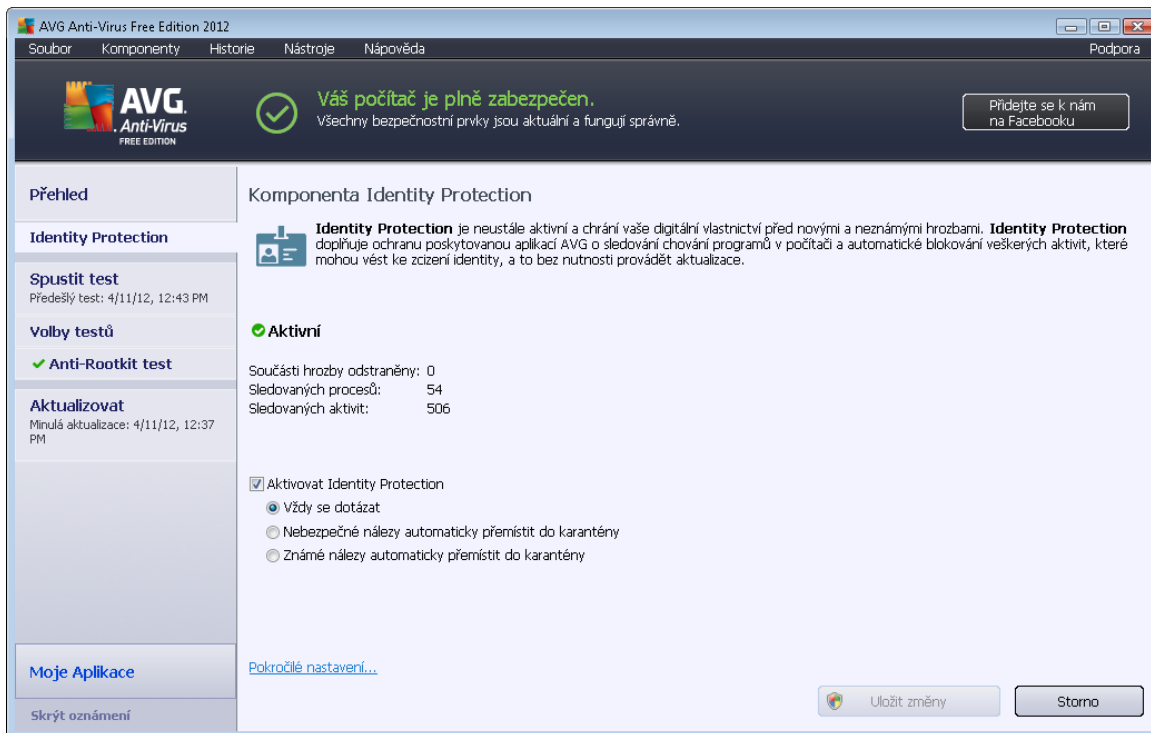
Identity Protection zajišťuje v reálném čase ochranu vašeho počítače proti novým a dosud neznámým hrozbám. Monitoruje všechny (i skryté) procesy a více než 285 různých vzorců chování, takže dokáže rozpoznat potenciálně nebezpečné chování v rámci vašeho systému. Díky této schopnosti umí **Identity Protection** detekovat hrozby, které ještě ani nejsou popsány ve virové databázi. Jakmile se neznámý kus kódu dostane do vašeho počítače, **Identity Protection** jej sleduje, pozoruje a zaznamenává případné příznaky škodlivého chování. Jestliže je soubor shledán škodlivým, **Identity Protection** jej umístí 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 vaši bezpečnost.

Identity Protection je bezpečnou součástí komplementárního ke komponentě [Anti-Virus](#). Pro naprostou bezpečnost vašeho počítače doporučujeme, abyste si nainstalovali obě komponenty!

6.6.1. Rozhraní Identity Protection



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

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

Základní nastavení Identity Protection

Ve spodní části rozhraní můžete nastavit některé základní funkce komponenty:

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



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

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

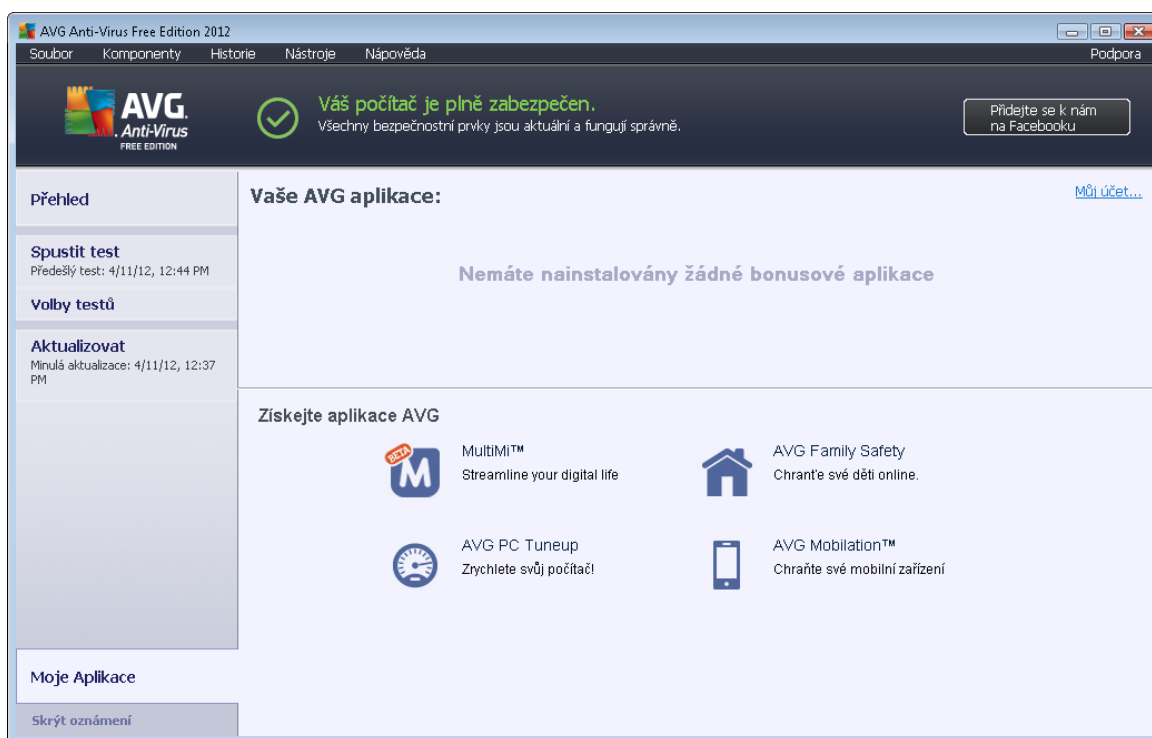
Ovládací tlačítka dialogu

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

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

7. Moje Aplikace

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



Dialog je rozdělen do dvou částí:

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

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

7.1. AVG LiveKive

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

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



disku

- Přístup k Vaším datům z jakéhokoli poskytovatele služeb připojenému k Internetu
- Snadnou organizaci dat
- Sdílení dat s autorizovanými osobami

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

7.2. AVG Mobilation

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

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

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

7.3. AVG Family Safety

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

Podrobné informace o aplikaci najdete na dedikované stránce AVG, k níž se připojíte prostřednictvím odkazu AVG Family Safety v dialogu [Moje aplikace](#).



7.4. AVG PC Tuneup

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

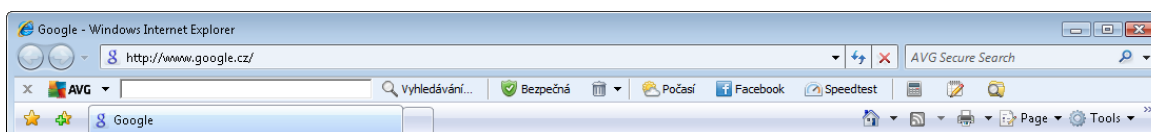
- vyhledání a defragmentace disku; oprava chybných sektorů
- oprava a defragmentace registrů
- optimalizace nastavení pro Internet, prohledání historie
- detekce a odstranění duplicitních souborů
- deaktivace zbytečných služeb, které zpomalují výkon počítače
- odinstalace nepoužívaných programů
- manuální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

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



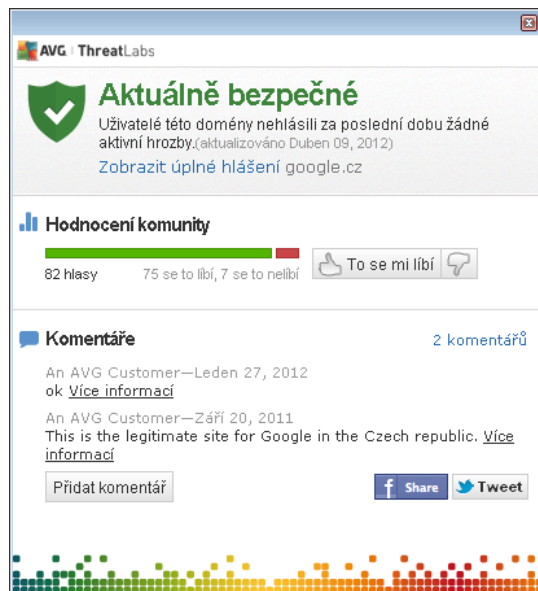
8. AVG Security Toolbar

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



AVG Security Toolbar je tvořen těmito prvky:

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



- **Vymazat** - Tlačítko s ikonou odpadkového koše otevírá rozbalovací menu, kde si můžete vybrat, zda chcete vymazat informace o navštívených stránkách, stahovaných souborech, informace uvedené do formulářů nebo vymazat kompletně celou historii vašeho vyhledávání na webu.
- **Počasí** - Tlačítkem otevřete samostatné okno s informací o aktuálním počasí v dané lokalitě a s výhledem na následující dva dny. Tato informace je aktualizována každých 3-6 hodin. V dialogu můžete ručně změnit požadovanou lokalitu a také rozhodnout, zda si přejete uvádět teplotu ve stupních Celsia nebo Fahrenheita.



- **Facebook** - Tlačítko umožňuje přímé připojení k sociální síti [Facebook](#) z prostředí **AVG Security Toolbaru**.
- **Speedtest** - Tlačítko umožňuje přístup k on-line aplikaci, s jejíž pomocí můžete ověřit funkčnost vašeho připojení k internetu (*ping*), rychlost stahování a nahrávání.
- Zkratková tlačítka pro rychlý přístup k aplikacím **Kalkulačka**, **Poznámkový blok**, **Průzkumník Windows**.



9. AVG Do Not Track

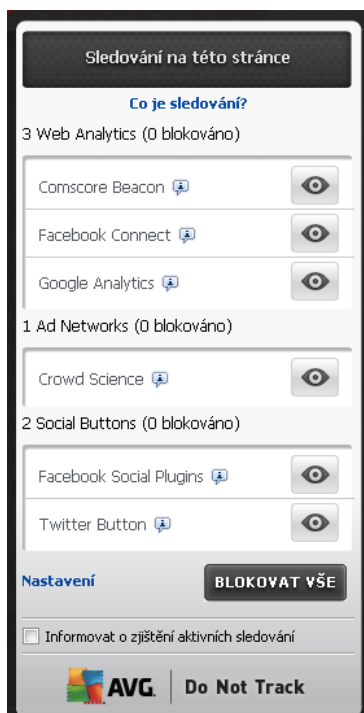
AVG Do Not Track dokáže identifikovat webové stránky, které sbírají data o vaší činnosti online. Ikona v prohlížeči zobrazí informaci o webových stránkách a reklamních sítích, jež sbírají informace o vaší aktivitě a nabídne vám možnost sběr dat povolit nebo nepovolit.

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

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

9.1. Rozhraní služby AVG Do Not Track

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



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

- **Služba Web Analytics** (ve výchozím nastavení povoleny): Služby poskytující lepší výkon a prohlížení příslušných webových stránek. V této kategorii najdete služby jakými jsou například Google Analytics, Omniture nebo Yahoo Analytics. Tyto služby nejsou ve výchozím nastavení blokovány a doporučujeme tuto konfiguraci ponechat. Při zablokování této kategorie služeb by mohlo dojít k chybám ve fungování samotné webové stránky.
- **Tlačítka sociální sítě** (ve výchozím nastavení povoleny): Prvky sloužící k lepší práci se sociálními sítěmi. Tato tlačítka propojují navštívené stránky se sociálními sítěmi. Jste-li k těmto sítím přihlášení, mohou tato tlačítka sbírat informace o vaší činnosti na Internetu. Mezi tlačítka sociálních sítí patří: modul plug-in sítě Facebook, tlačítko sítě Twitter, tlačítko Google +1 apod.
- **Reklamní síť** (některé reklamní síť jsou ve výchozím nastavení blokovány): Služby, které přímo či nepřímo sbírají nebo sdílejí na různých stránkách informace o vaší činnosti na Internetu s cílem nabízet individuální reklamy (narozdíl od reklam založených na obsahu). Tyto služby se řídí zásadami ochrany osobních údajů příslušné reklamní sítě (zásady ochrany osobních údajů jsou dostupné na webových stránkách dané sítě).

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

V dialogu jsou rovněž uvedeny dva hypertextové odkazy:

- **Co je sledování?** - kliknutím na tento odkaz v horní části dialogu budete přesměrováni na webovou stránku s podrobným vysvětlením principu sledování a popisem jednotlivých typů sledování.
- **Nastavení** - kliknutím na tento odkaz ve spodní části dialogu budete přesměrováni na webovou stránku, kde máte možnost nastavit konkrétní parametry služby **AVG Do Not Track** (podrobný popis nastavení najdete v kapitole [Nastavení služby AVG Do Not Track](#))

9.2. Informace o sledovacích procesech



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

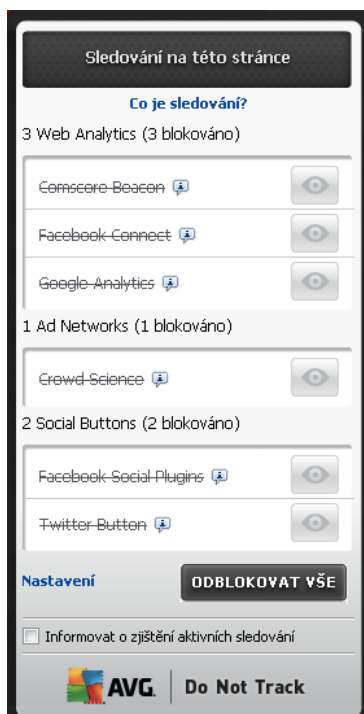
Ve spodní části bubliny pak najdete aktivní odkaz **Ochrana osobních údajů**, přes nějž budete přesměrováni na stránku s prohlášením o ochraně osobních údajů na serveru poskytlé detekované služby.



9.3. Blokování sledovacích procesů

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

- **Blokovat vše** - Stiskem tohoto tlačítka, které je umístěno ve spodní části dialogu, zakážete jakýkoliv sběr dat všem detekovaným službám. *(Máte však na paměti, že tento krok může způsobit poruchy funkčnosti webových stránek, v níž služba běží!)*
-  - Pokud nechcete jednorázově zablokovat všechny detekované služby, dá se blokování i povolení nastavit u každé z detekovaných služeb jednotlivě. Některým z detekovaných služeb například sledování povolíte (například Web Analytics): tyto systémy používají shromážděná data k optimalizaci své webové stránky a zlepšují tak uživatelské prostředí internetu. Současně však můžete zcela zakázat sledování všem službám zařazeným v kategorii reklamních sítí. Jednoduchým kliknutím na ikonu  u příslušného procesu tuto službu zablokujete (v obrázku se zobrazí jako přeškrtnutý) a nebo opět povolíte.



9.4. Nastavení služby AVG Do Not Track

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



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

Nastavení AVG Do-Not-Track

Upozornit

Zobrazit upozornění po dobu sekund

Pozice oznámení

Upozornit, pokud jsem na stránce sledován

Oznamovat stránkám, že si nepřeji být sledován (použitím [http hlavičky](#) Do-Not-Track)

Blokovat následující

<input checked="" type="checkbox"/> 24/7 Real Media	Ad Networks
<input checked="" type="checkbox"/> 33Across	Ad Networks
<input checked="" type="checkbox"/> [x+1]	Ad Networks
<input checked="" type="checkbox"/> Accelerator Media	Ad Networks
<input checked="" type="checkbox"/> AddtoAny	Ad Networks
<input checked="" type="checkbox"/> Adition	Ad Networks
<input checked="" type="checkbox"/> AdReady	Ad Networks
<input checked="" type="checkbox"/> Aggregate Knowledge	Ad Networks
<input checked="" type="checkbox"/> Baynote Observer	Ad Networks
<input checked="" type="checkbox"/> Bizo	Ad Networks

- **Zobrazit upozornění po dobu** (ve výchozím nastavení: 10) - V tomto políčku můžete určit, po jak dlouhou dobu (v sekundách) si můžete ponechat notificační dialog **AVG Do Not Track** zobrazený na vašem monitoru. Číslo musí spadat do rozmezí 0 až 60 sekund (pokud nastavíte hodnotu 0, notificační dialog se na větší obrazovce vůbec neobjeví).
- **Pozice oznámení** (ve výchozím nastavení: Vpravo nahore) - Otevřete rozbalovací menu a vyberte, v jaké pozici na vašem monitoru se má notificační dialog **AVG Do Not Track** zobrazovat.
- **Upozornit, pokud jsem na stránce sledován** (ve výchozím nastavení vypnuto) - Označením položky potvrdíte, že si můžete být vyrozuměni pokaždé, když vstoupíte na stránku, v níž bude detekována nová, dosud neblokována služba sběru dat. Je-li položka označena a **AVG Do Not Track** detekuje novou službu ve stránce, na níž se aktuálně nacházíte, objeví se na vaší obrazovce oznamovací dialog. V opačném případě, tedy pokud tuto volbu nezapnete, bude jediným indikátorem detekce nového sledovacího procesu změna barvy ikonky **AVG Do Not Track** (umístěná na panelu příkazů vašeho prohlížeče) ze zelené na žlutou.
- **Oznamovat stránkám, že si nepřeji být sledován** (ve výchozím nastavení zapnuto) -



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

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

V konfiguraci stránky **Nastavení AVG Do Not Track** jsou vám k dispozici tato ovládací tlačítka:

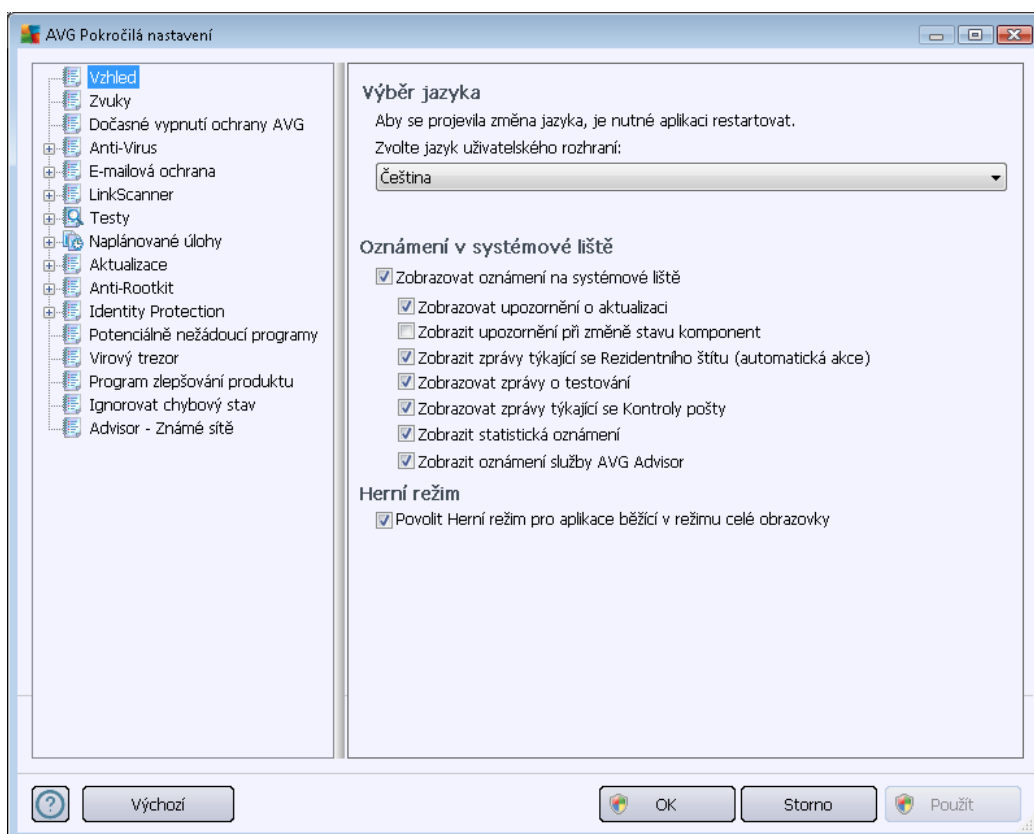
- **Blokovat vše** - kliknutím jednorázově zablokuje všechny výše uvedené služby v seznamu, jež jsou klasifikovány jako reklamní síť;
- **Povolit vše** - kliknutím jednorázově povolíte všechny dříve zablokované služby uvedené v seznamu, jež jsou klasifikovány jako reklamní síť;
- **Výchozí** - kliknutím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

10. Pokročilé nastavení AVG

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

10.1. Vzhled

První položka navigačního seznamu, **Vzhled**, se týká obecného nastavení [uživatelského rozhraní AVG Anti-Virus Free Edition 2012](#) a nabízí možnost nastavení základních prvků programu:

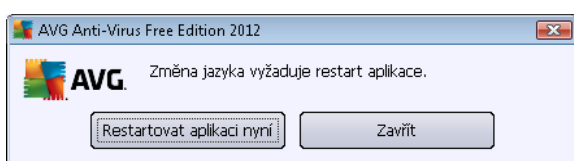


Výběr jazyka

V sekci **Výběr jazyka** můžete z rozbalovacího menu zvolit jazyk, v němž má být zobrazeno [uživatelské rozhraní AVG Anti-Virus Free Edition 2012](#). V nabídce budou dostupné jen ty jazyky, které jste zvolili během [instalace programu](#) (viz kapitola [Uživatelské volby](#)) a také angličtina (*angličtina se vždy instaluje automaticky*). Pro zobrazení **AVG Anti-Virus Free Edition 2012** v požadovaném jazyce je však nutné aplikaci restartovat. Postupujte prosím následovně:

- V rozbalovacím menu zvolte požadovaný jazyk aplikace

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



Oznámení v systémové liště

V této sekci můžete potlačit zobrazování systémových oznámení o aktuálním stavu aplikace **AVG Anti-Virus Free Edition 2012**. Ve výchozím nastavení programu jsou systémová oznámení povolena. Doporučujeme toto nastavení ponechat! Systémová oznámení přináší například informace o spuštění aktualizací nebo testů, o změně stavu některých komponent **AVG Anti-Virus Free Edition 2012** a podobně. Je rozhodně vhodné vnovat jim pozornost!

Pokud se přesto z nějakého důvodu rozhodnete, že si nepřejete být takto informováni, máte možnost kompletně potlačit zobrazování informativních oznámení, nebo zakázat pouze zobrazování informací vztahených k určité komponentě **AVG Anti-Virus Free Edition 2012**. Svě vlastní nastavení můžete provést označením příslušné položky ve strukturované nabídce:

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



Rezidentní štít povoleno [automatické léčení](#) detekované infekce).

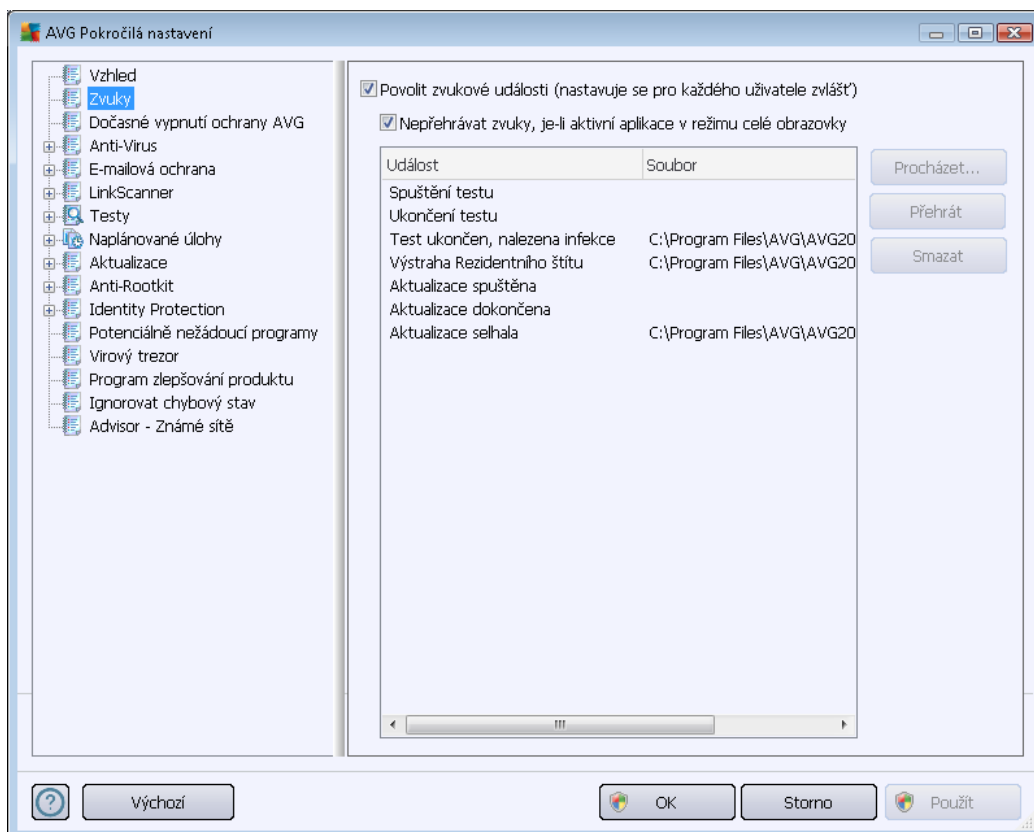
- **Zobrazovat zprávy o [testování](#) v systémové liště** (ve výchozím nastavení zapnuto) - volbou položky rozhodnete, zda mají být zobrazena nebo naopak potlačena informativní hlášení o automatickém spuštění naplánovaného testu, jeho průběhu, ukončení a výsledcích; informace o ostatních procesech se budou zobrazovat normálně.
- **Zobrazovat zprávy týkající se [Kontroly pošty](#) v systémové liště** (ve výchozím nastavení zapnuto) - volbou položky rozhodnete, zda mají být zobrazena nebo naopak potlačena informativní hlášení o průběhu testování příchozích a odchozích zpráv elektronické pošty; informace o ostatních procesech se budou zobrazovat normálně.
- **Zobrazit statistická oznámení** (ve výchozím nastavení zapnuto) - volbou položky umožníte zobrazení pravidelného statistického pohledu v systémové liště.
- **Zobrazit oznámení služby AVG Advisor** (ve výchozím nastavení zapnuto) - volbou položky rozhodnete, zda chcete ponechat zapnutá veškerá oznámení služby [AVG Advisor](#) zobrazovaná ve vysouvacím panelu na systémovou lištu.

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 i k poškození grafiky). Abychom této situaci předešli, ponechejte prosím položku **Povolit herní režim pro aplikace běžící v režimu celé obrazovky** označenou (výchozí nastavení).

10.2. Zvuky

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



Nastavení zvuk je platné pouze pro aktuálně otevřený uživatelský účet. Každý uživatel má tedy možnost individuálního nastavení. Pokud se přihlásíte-li se 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 přidat. 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 rušiv (viz také nastavení **Herního režimu**, které popisujeme v kapitole [Pokročilá nastavení/Vzhled](#) tohoto dokumentu).

Ovládací tlačítka dialogu

- **Procházet** - Ze seznamu událostí si vyberte tu událost, již chcete přidat konkrétní zvuk. Pomocí tlačítka **Procházet** pak prohledejte svůj pevný disk a příslušný zvukový soubor lokalizujte. (Upozorujeme, že v tuto chvíli jsou podporovány pouze zvukové soubory ve formátu *.wav!)
- **Přehrát** - Chcete-li si přislyšet zvuk poslechnout, označte v seznamu příslušnou akci a stiskněte tlačítko **Přehrát**.

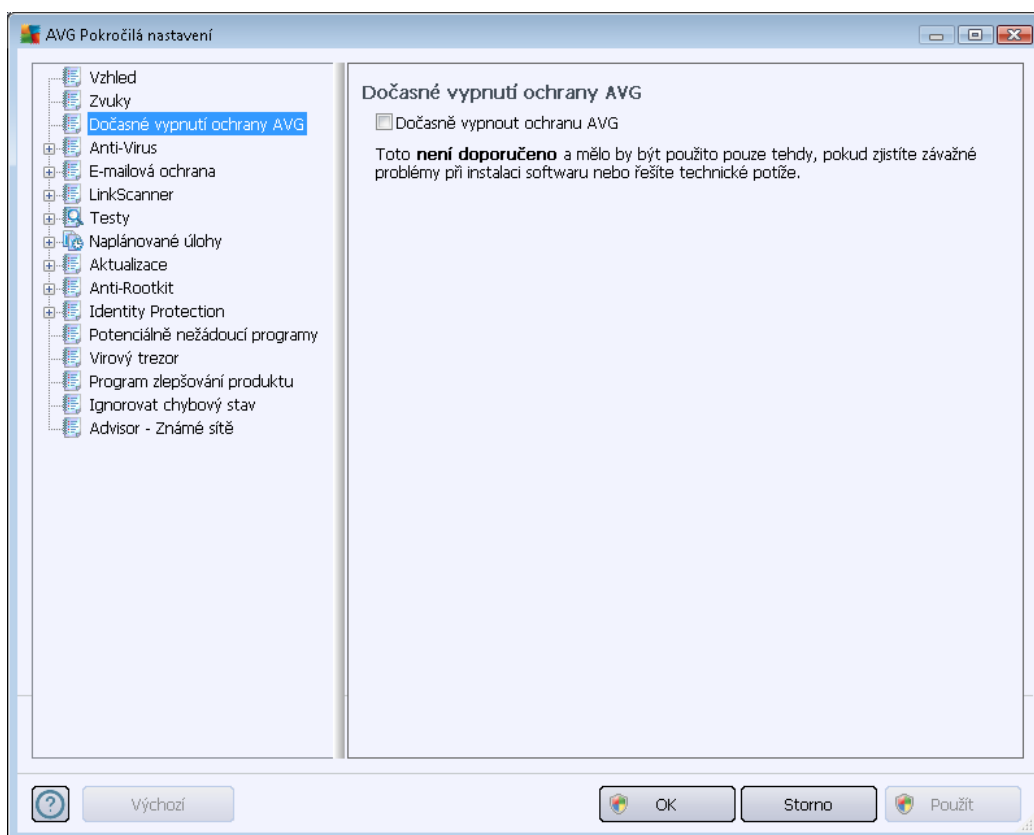


- **Smazat** - Tlačítkem **Smazat** pak můžete zvuk pí azený konkrétní akci zase odebrat.

10.3. Dočasné vypnutí ochrany AVG

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

Máte prosím na paměti, že tato volba by v žádném případě neměla být použita, pokud to není opravdu nezbytné!

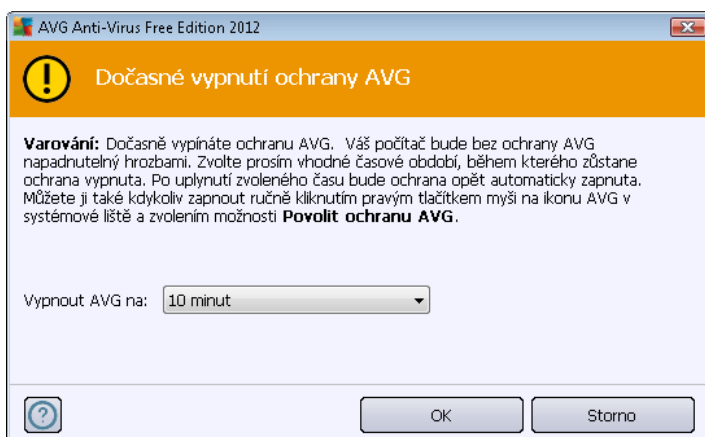


V naprosté většině případů **není nutné** deaktivovat **AVG Anti-Virus Free Edition 2012** před instalací nového softwaru nebo ovladače, a to ani tehdy, pokud budete během instalace vyzváni k zavěšení všech spuštěných aplikací. Pokud by v takovém případě došlo ke kolizi, pravděpodobně budete stačit [deaktivovat rezidentní ochranu \(Povolit Rezidentní štít\)](#). Jestliže budete opravdu nuceni deaktivovat **AVG Anti-Virus Free Edition 2012**, zapněte jej hned, jakmile to bude možné. Pamatujte, že pokud jste připojeni k Internetu nebo k jiné síti, je váš počítač bez aktivní ochrany vysoce zranitelný.

Jak vypnout ochranu AVG

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

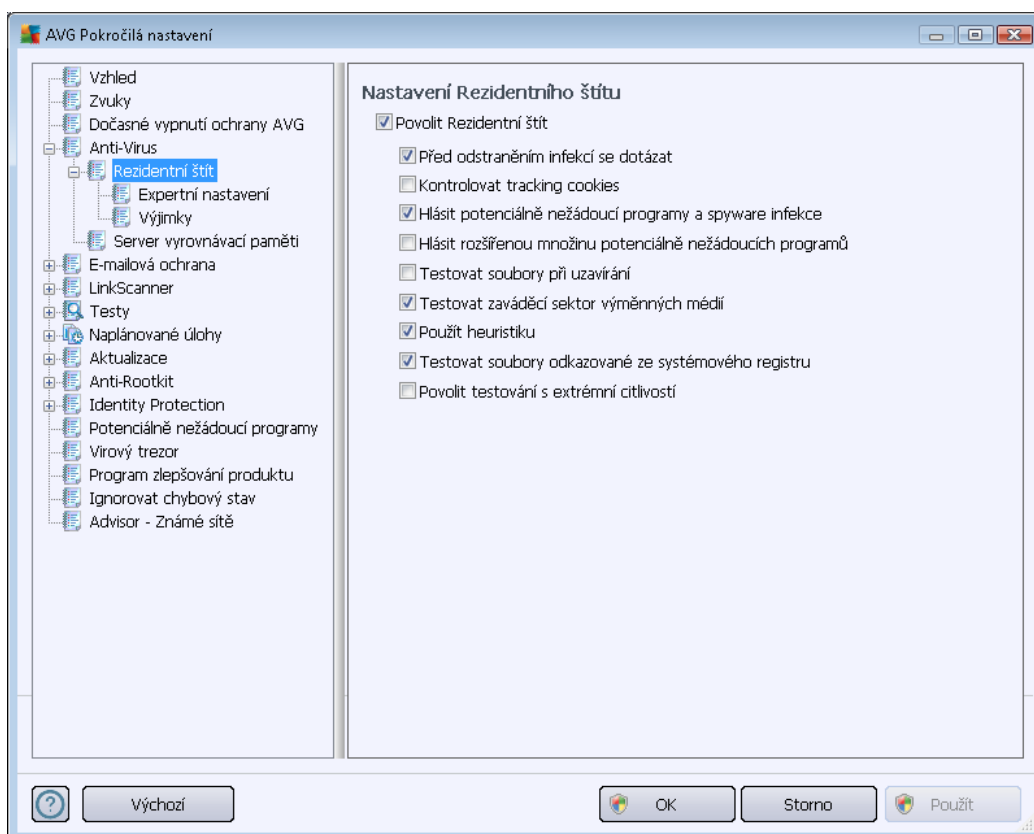
- V nov oteveném dialogu **Dočasně vypnutí ochrany AVG** pak nastavte požadovaný čas, po který pot ebuje AVG Anti-Virus Free Edition 2012 vypnout. Standardn ě bude ochrana vypnuta po dobu 10 minut, což je dosta uující pro všechny běžné úkony. M ůžete si však zvolit i delší časový interval, ale tuto možnost nedoporu ujeme, pokud to není naprosto nezbytn ě nutné. Po uplynutí zvoleného časového intervalu se všechny vypnuté komponenty znovu automaticky aktivují. Maximální časová lh ťa vynutí ochrany AVG je do p ěšího restartu vašeho počíta e.



10.4. Anti-Virus

10.4.1. Rezidentní štít

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



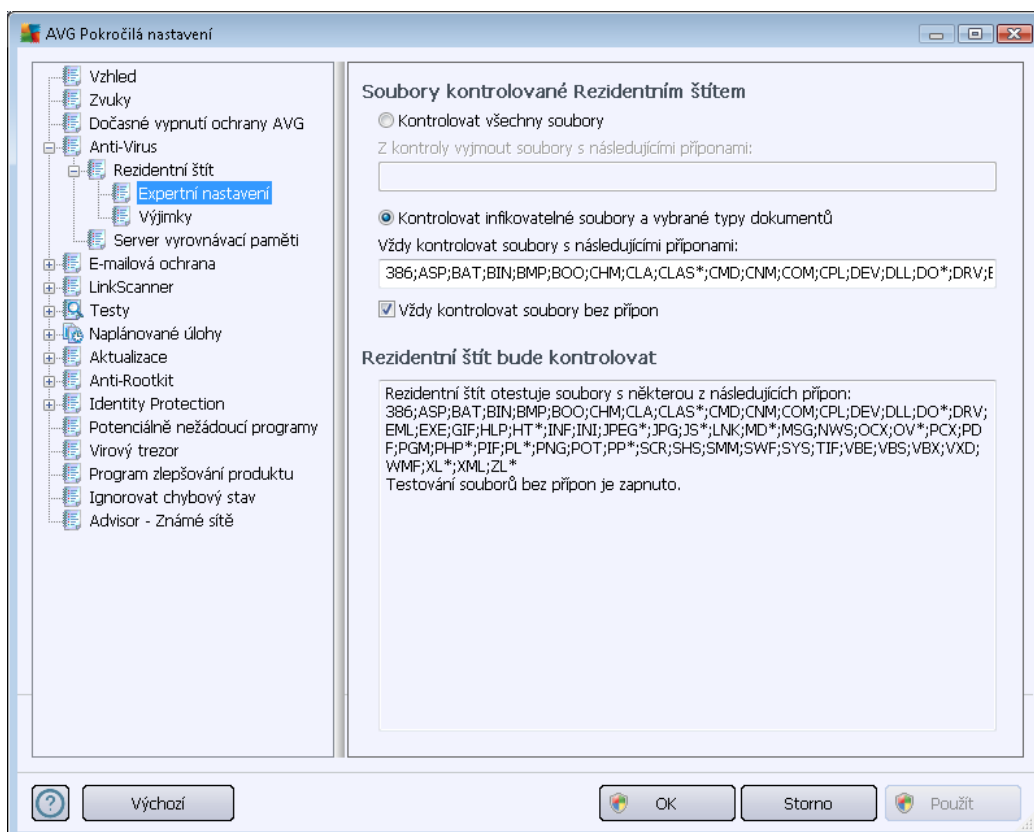
V dialogu **Nastavení Rezidentního štítu** máte možnost celkově aktivovat i deaktivovat rezidentní ochranu označením i vypnutím položky **Povolit Rezidentní štít** (tato položka je ve výchozím nastavení zapnuta). Dále můžete prostým výběrem rozhodnout, které funkce rezidentní ochrany mají být aktivovány:

- **Před odstraněním infekcí se dotázat** (ve výchozím nastavení zapnuto) - Ponechte tuto položku označenou, pokud chcete být při detekci hrozby dotázáni na to, jaké kroky mají být dále podniknuty. V opačném případě bude hrozba automaticky přesunuta do [Virového trezoru](#). Tato vaše volba nemá žádný vliv na úroveň bezpečnosti a je pouze preferenční.
- **Kontrolovat tracking cookies** (ve výchozím nastavení vypnuto) - Parametr definuje, že mají být detekovány cookies (*HTTP data zaslaná serverem prohlížeči a uložena na počítači uživatele; při každé další návštěvě téhož serveru prohlížeč posílá cookies zpět serveru, který podle nich rozlišuje jednotlivé uživatele*).
- **Hlásit potenciálně nežádoucí programy a spyware infekce** (ve výchozím nastavení zapnuto) - Kontrola přítomnosti [potenciálně nežádoucích programů](#) (spustitelné programy, které mohou fungovat jako spyware nebo adware). Zaškrtnutím tohoto políčka aktivujete [Anti-Spyware](#), tj. bude se testovat přítomnost spyware, nejen virů. Spyware představuje poněkud problematickou kategorii malware, protože i když v tichosti vytvoří program

představuje bezpečnostní riziko, jsou mnohdy instalovány v domě a se souhlasem uživatele. Doporučíme nicméně ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.

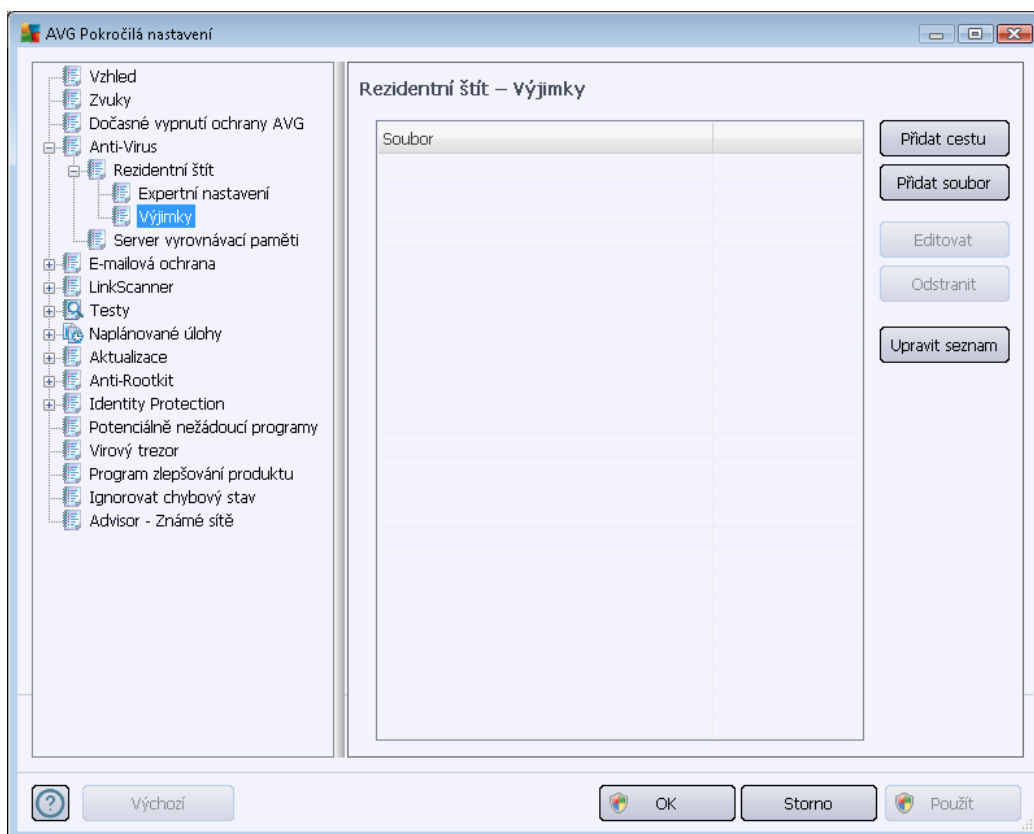
- **Hlásit rozšířenou množinu potenciálně nežádoucích programů** (ve výchozím nastavení vypnuto) - Zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně můžete 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 zavádění sektorových výměnných médií** (ve výchozím nastavení zapnuto)
- **Použít heuristiku** (ve výchozím nastavení zapnuto) - K detekci infekce bude použita i metoda [heuristické analýzy](#) (dynamické emulace instrukcí testovaného objektu v prostředí virtuálního počítače).
- **Léčit automaticky** (ve výchozím nastavení vypnuto) - Detekovaná infekce bude automaticky vyléčena, jestliže je k dispozici lékba toho konkrétního viru; a všechny infekce, jež nelze vyléčit, budou odstraněny.
- **Testovat soubory odkazované ze systémového registru** (ve výchozím nastavení zapnuto) - AVG bude testovat všechny spustitelné soubory přidané do systémového registru, aby tak zabránil možnému spuštění již známé infekce při prvním startu počítače.
- **Povolit testování s extrémní citlivostí** (ve výchozím nastavení vypnuto) - Ve specifických situacích (mimo žádný stav ohrožení počítače) můžete zvolit tuto metodu kontroly, která aktivuje nejkvalitnější a nejpodrobnější testovací algoritmy. Mějte však na paměti, že tato metoda je časově velmi náročná.

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



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

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



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

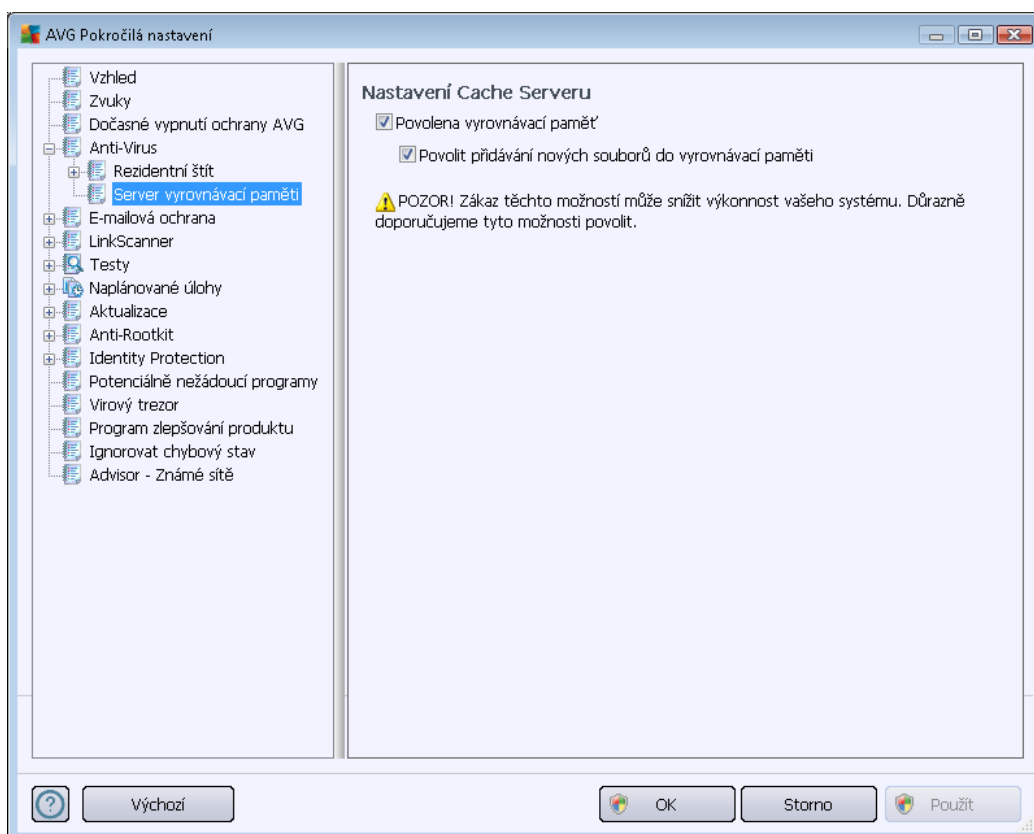
Pokud to není nezbytně nutné, dle naší doporučení nevyjímáme žádné položky z testování!

V dialogu jsou k dispozici tato ovládací tlačítka:

- **Přidat cestu** – umožňuje výběrem z navigačního stromu lokálního disku určit adresáře s celým obsahem, který má být vyat z testování
- **Přidat soubor** – umožňuje výběrem z navigačního stromu lokálního disku po jednom vybrat další soubory definované jako výjimky z testování
- **Editovat** – umožňuje editovat zadání cesty ke zvolenému souboru nebo adresáři
- **Odstranit** – umožňuje odstranit cestu ke zvolenému souboru nebo adresáři
- **Upravit seznam** - umožňuje upravit celý seznam definovaných výjimek ručně v dialogu, který se chová jako textový editor

10.4.2. Server vyrovnávací paměti

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



V rámci tohoto procesu **AVG Anti-Virus Free Edition 2012** detekuje a vyřadí nevhodné soubory (za nevhodný lze považovat například soubory digitálně podepsané z nevhodným 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.

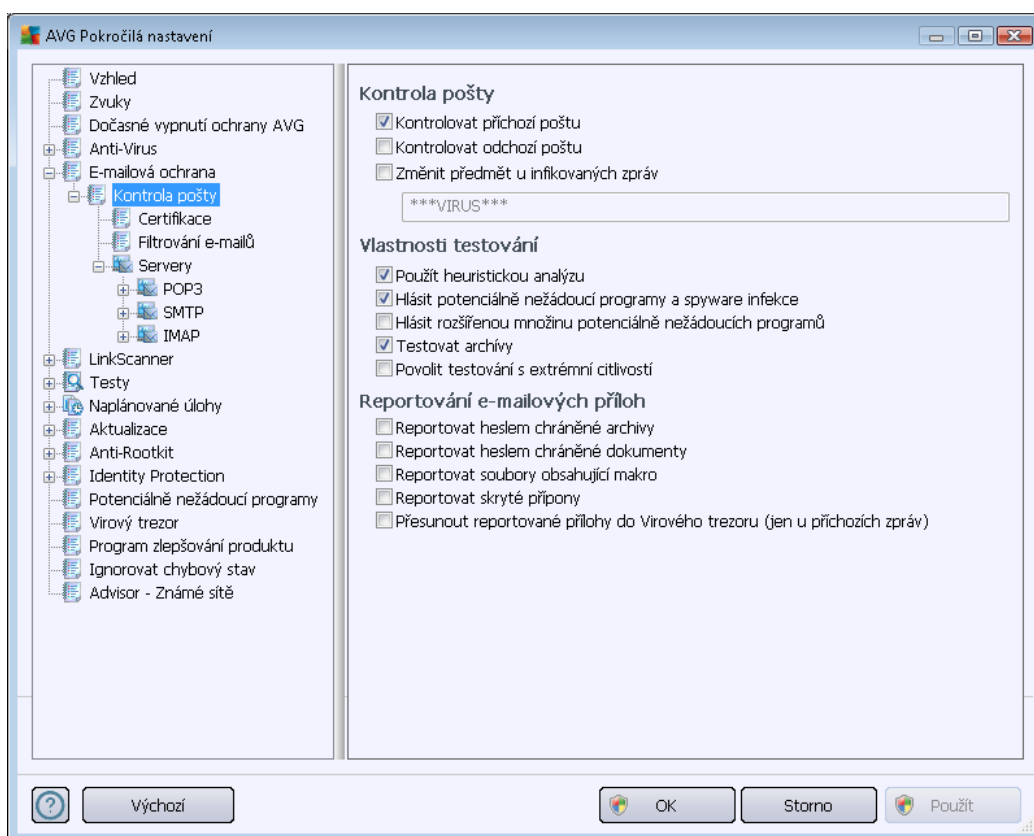
Pokud nemáte skutečný důvod cache server vypínat, důrazně doporučujeme, abyste se

p idrželi výchozího nastavení a ponechali ob položky zapnuté! V opa ném p ípad m že dojt k výraznému snížení rychlosti a výkonnosti Vašeho systému.

10.5. E-mailová ochrana

10.5.1. Kontrola pošty

Dialog **Kontrola pošty** je rozd len do t í sekcí:



Kontrola pošty

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

- **Kontrolovat p íchozí poštu** (ve výchozím nastavení zapnuto) - ozna ením zapnete/ vypnete možnost testování všech p íchozích e-mail
- **Kontrolovat odchozí poštu** (ve výchozím nastavení vypnuto) - ozna ením zapnete/vypnete možnost testování všech e-mail odesílaných z vašeho ú tu
- **Zm nit p edm t u infikovaných zpráv** (ve výchozím nastavení vypnuto) - chcete-li být upozorn ni na to, že otestovaná zpráva byla vyhodnocena jako infikovaná, m žete aktivovat



tuto položku a do textového pole vepsat požadované označení takovéto e-mailové zprávy. Tento text pak bude přidán do pole "Přidání" u každé pozitivně detekované zprávy (*slouží ke snadnější identifikaci a filtrování*). Výchozí hodnota je *****VIRUS***** a doporučení ujmeme 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 přehledy e-mailů nejen podle přehledů, ale i podle skutečného obsahu a formátu (*kteřý přehled nemusí odpovídat*). Filtrování lze nastavit v dialogu [Filtrování e-mailů](#).
- **Hlásit potenciálně nežádoucí programy a spyware infekce** (ve výchozím nastavení zapnuto) - kontrola přítomnosti [potenciálně nežádoucích programů](#) (*spustitelné programy, které mohou fungovat jako spyware nebo adware*). Zaškrtnutím tohoto políčka aktivujete [Anti-Spyware](#), tj. bude se testovat přítomnost spyware, nejen virů. Spyware představuje poněkud problematickou kategorii malware, protože i když v těsnosti s tímto programem představuje bezpečnostní riziko, jsou mnohdy instalovány v domě a se souhlasem uživatele. Doporučujeme nicméně ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
- **Hlásit rozšířenou množinu potenciálně nežádoucích programů** (ve výchozím nastavení vypnuto) - zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně můžete blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.
- **Testovat archívy** (ve výchozím nastavení zapnuto) - testovat obsah archivů v přehledech zpráv.
- **Povolit testování s extrémní citlivostí** (ve výchozím nastavení vypnuto) - ve specifických situacích (*například při podezření na infekci starším typem viru*) můžete zvolit tuto metodu testování, která aktivuje nejdokladnější testovací algoritmy a velmi podrobně prohledá naprosto všechny oblasti vašeho počítače. Můžete však na paměti, že tato metoda je časově velmi náročná.

Reportování e-mailových přehledů

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

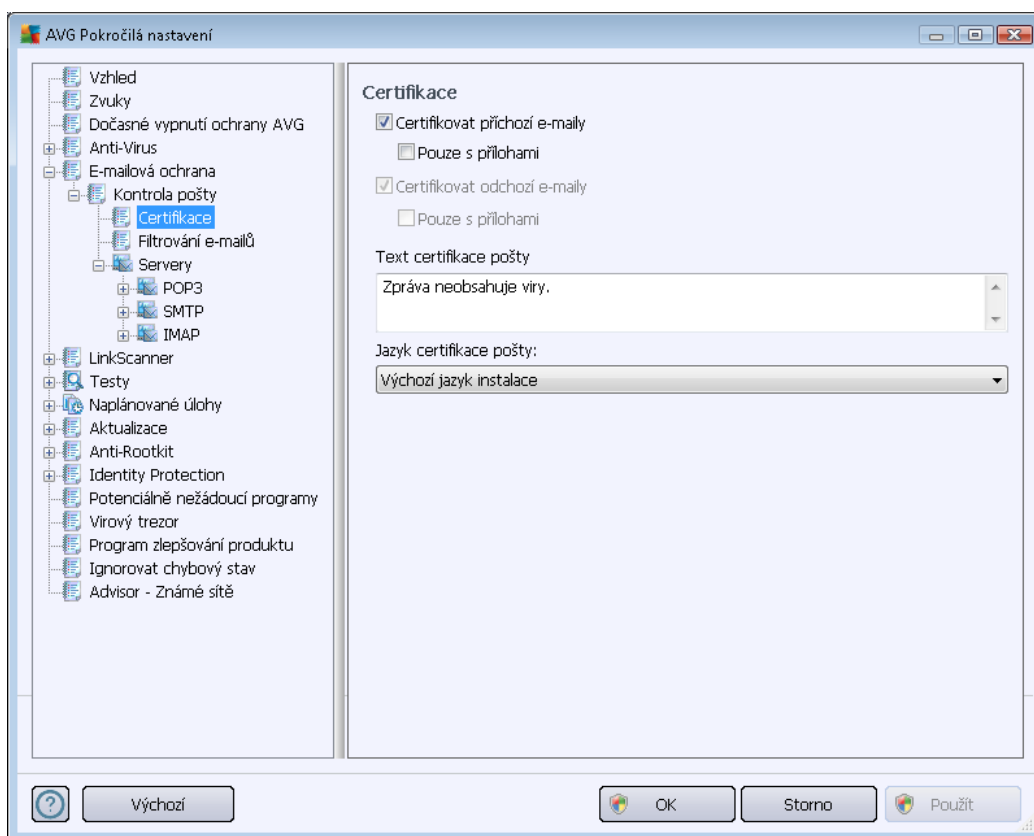
- **Reportovat heslem chráněné archívy** – archívy (ZIP, RAR atd.) chráněné heslem není možné otestovat na přítomnost virů; po zaškrtnutí tohoto políčka se tyto archívy budou označovat jako potenciálně nebezpečné.
- **Reportovat heslem chráněné dokumenty** – dokumenty chráněné heslem není možné



testovat na přítomnost virů; po zaškrtnutí tohoto políčka se tyto archivy budou označovat jako potenciálně nebezpečné.

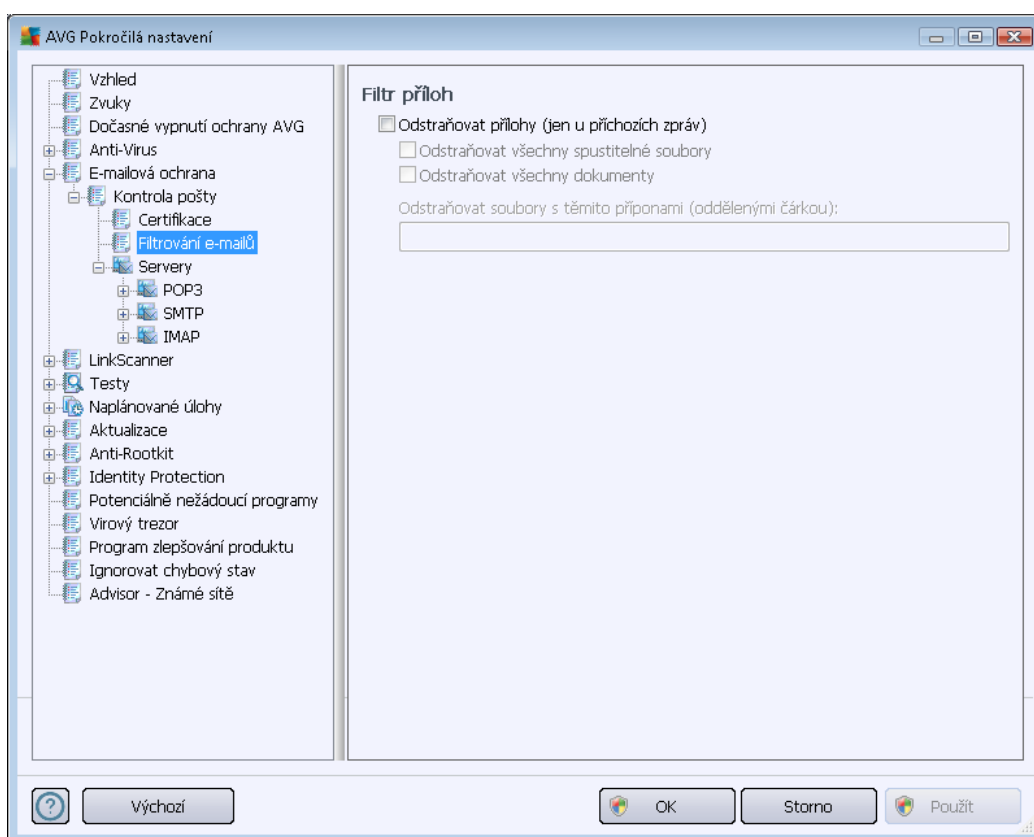
- **Reportovat soubory obsahující makro** – makro je napevněný sled kroků, který usnadňuje uživateli často opakované složitější úkoly (*makra ve Wordu jsou typickým příkladem*). Makro může obsahovat různé instrukce, a to i potenciálně nebezpečné; chcete-li reportovat všechny dokumenty s makry, označte toto políčko.
- **Reportovat skryté přípony** – skryté přípony mohou podezřelý spustitelný soubor "naco.txt.exe" zamaskovat tak, aby se uživateli jevil jen jako neškodný textový soubor "naco.txt"; po zaškrtnutí tohoto políčka budou soubory se skrytými příponami reportovány jako potenciálně nebezpečné.
- Zaškrtnutím políčka **Presunout 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-mail**) a/nebo odchozí poštu (**Certifikovat odchozí e-mail**). U každé z těchto voleb můžete dále označením možnosti **Pouze s přílohami** nastavit parametr, který určuje, že v rámci příchozí i odchozí pošty budou certifikovány pouze přílohy (textem označený výhradně poštovní zpráva s přílohou):



Ve výchozím nastavení obsahuje certifikace 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 přiložen nebude!



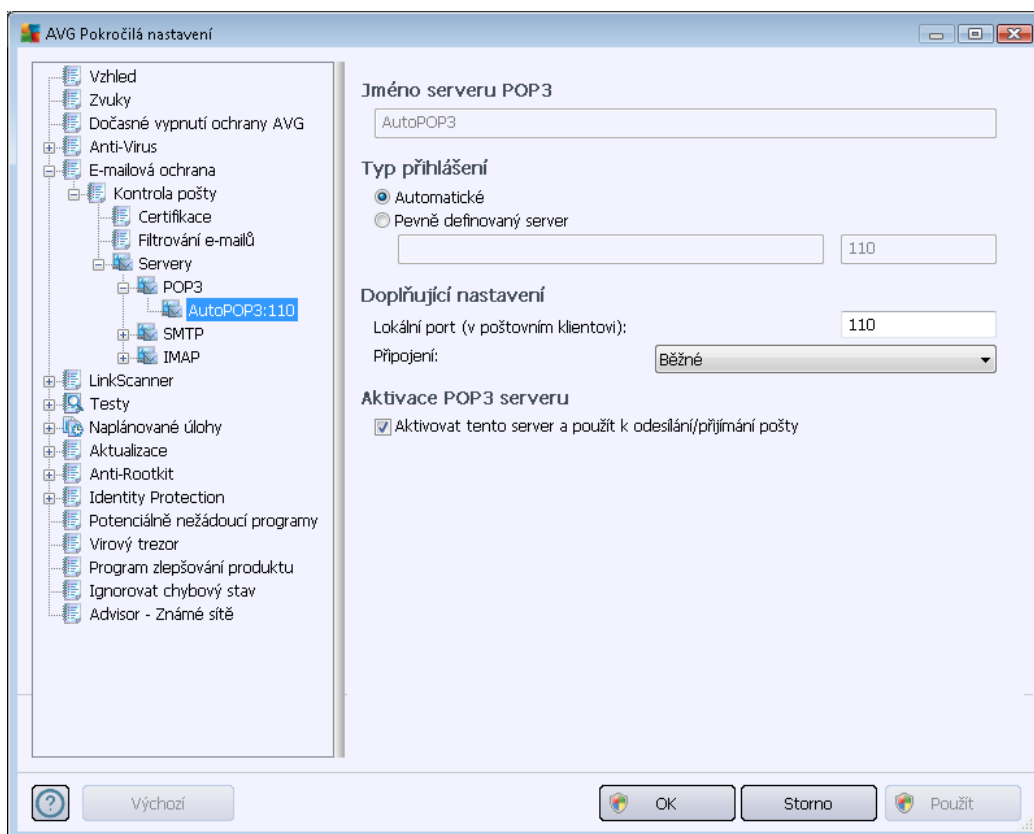
Dialog **Filtr příloh** umožňuje nastavení parametrů pro testování příloh e-mailových zpráv. Ve výchozím nastavení je možnost **Odstraňovat přílohy** vypnuta. Pokud se rozhodnete pro její aktivaci, budou automaticky odstraněny všechny přílohy zpráv, které byly detekovány jako infikované nebo potenciálně 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 pro příchozí i odchozí pošty, a to pomocí tlačítka **Přidat nový server**.

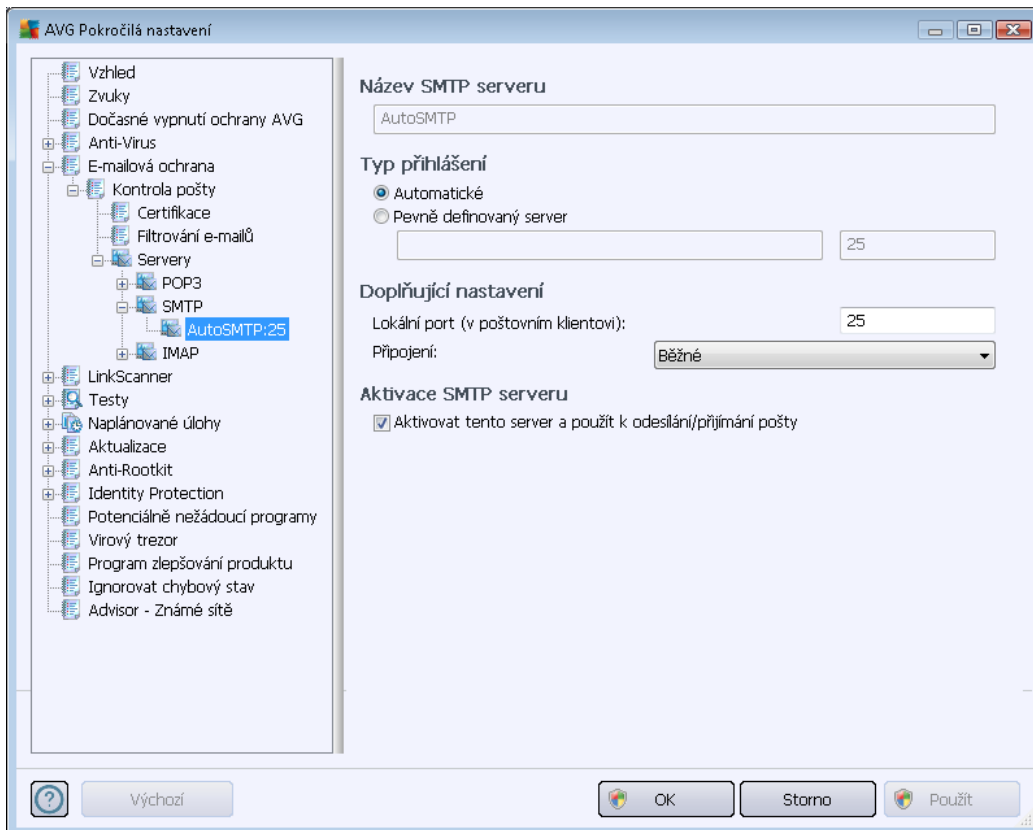


V tomto dialogu ([odkaz Servery / POP3](#)) nastavujete server [Kontroly pošty](#) s protokolem POP3 pro příchozí pošty:

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



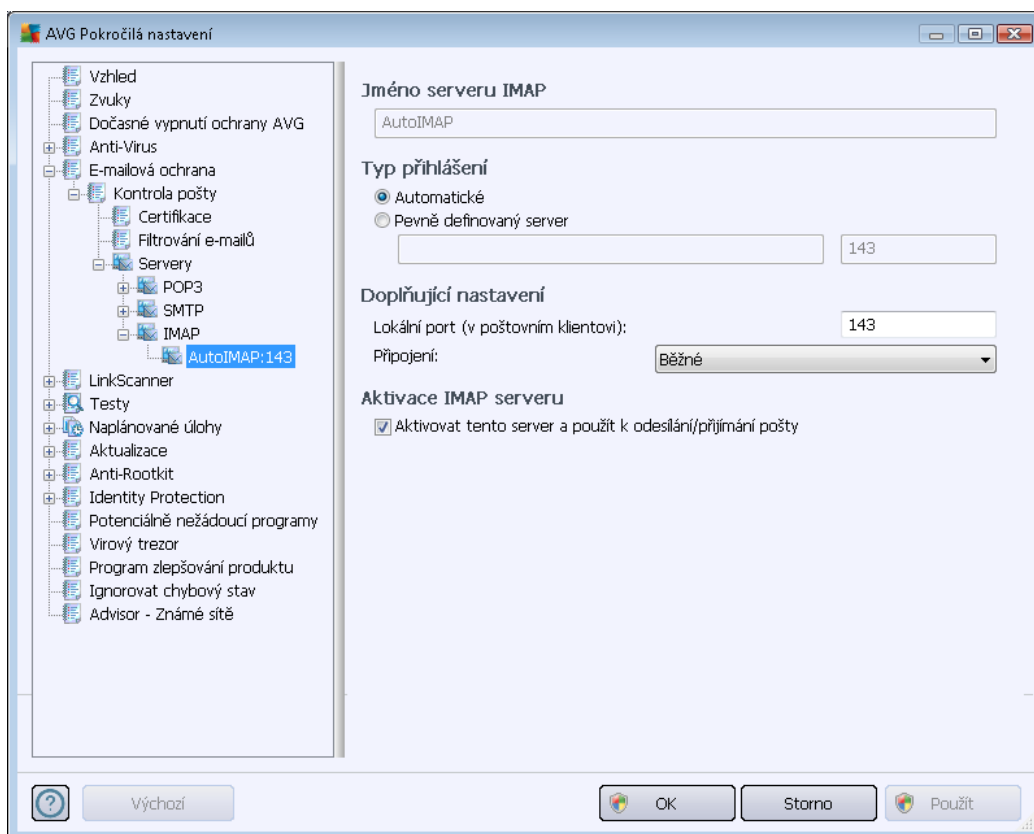
- **Automatické** - cílový server bude určen podle nastavení ve vaší poštovní aplikaci; není třeba nic dále specifikovat
- **Pevně definovaný server** - v tomto případě bude vždy použit konkrétní server. Je třeba zadat adresu nebo jméno vašeho poštovního serveru. Při přihlašovací jméno pak zůstane beze 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 (*například pop.acme.com:8200*). Standardní port pro POP3 komunikaci je 110.
- **Doplující 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: Bezpečné (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 (odkaz **Servery / SMTP**) nastavujete server **Kontroly pošty** s protokolem SMTP pro odchozí poštu:

- **Název SMTP serveru** - v tomto poli můžete zadat jméno nově přidávaných 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 (*nap. smtp.acme.com*), tak i IP adresu (*nap. 123.45.67.89*). Pokud poštovní server používá nestandardní port, lze tento port zadat za jméno serveru oddělený dvojtečkou (*nap. smtp.acme.com:8200*). Standardní port pro SMTP komunikaci je 25.
- **Doplňující nastavení** - specifikuje další detailní parametry:

- **Lokální port** - určuje, na kterém portu lze očekávat komunikaci z poštovní aplikace. Tento port je pak také nutné v poštovní aplikaci zadat jako port pro SMTP komunikaci.
- **Typ 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 cílový poštovní server podporuje.
- **Aktivace SMTP serveru** - zapnutím/vypnutím položky máte možnost aktivovat či deaktivovat právě nastavený SMTP server



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

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

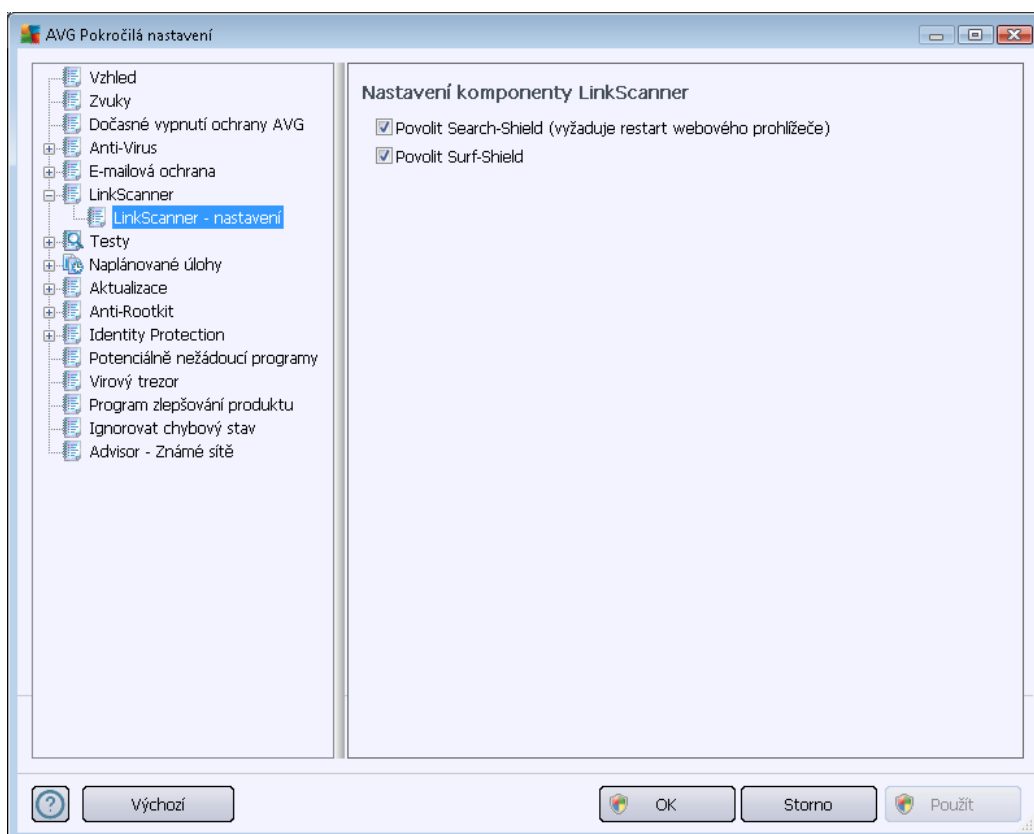


- **Automatické** - cílový server bude určen podle nastavení ve vaší poštovní aplikaci; není třeba nic dále specifikovat
- **Pevně definovaný server** - v tomto případě bude vždy použit konkrétní server. Do editačního řádku je třeba zadat adresu nebo jméno vašeho poštovního serveru. Jako jméno je možné použít jak doménový název (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.
 - **Protokol** - v této rozbalovací nabídce můžete specifikovat typ protokolu: Běžný (standardní protokol), SSL (zabezpečené na vyhrazeném portu) anebo výchozí SSL (zabezpečené na běžném portu). Pokud zvolíte zabezpečený protokol, budou posílaná data kryptována a nebude možné jejich sledování nikým jiným. I tato funkce může být aktivována pouze v případě, že cílový poštovní server podporuje.
- **Aktivace IMAP serveru** - zapnutím/vypnutím položky máte možnost aktivovat či deaktivovat právě nastavený IMAP server

10.6. LinkScanner

10.6.1. LinkScanner - nastavení

Dialog **Nastavení komponenty LinkScanner** umožňuje zapnout i vypnout funkce základních složek **LinkScanner**:



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

10.7. Testy

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

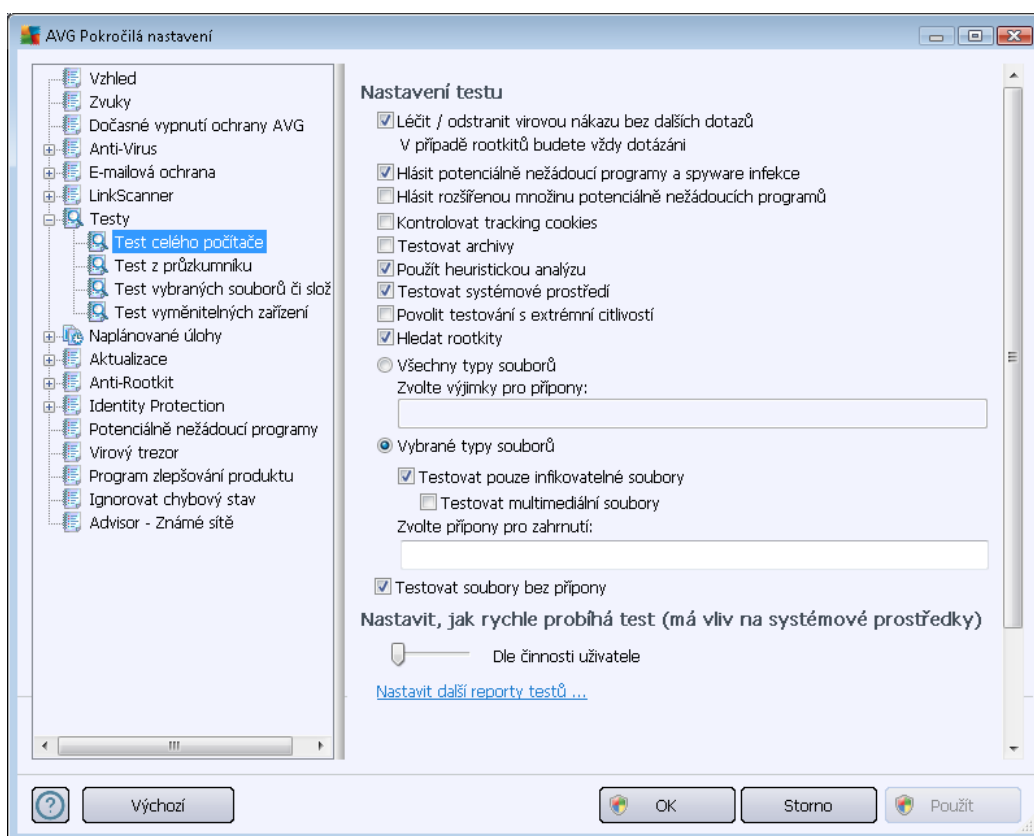
- **Test celého počítače** - výrobcem nastavený standardní test
- **Test z průzkumníku** - specifický test spouštěný nad zvolenými objekty přímo v prostředí

Windows

- **Test vybraných souborů i složek** - výrobcem nastavený standardní test s možností definovat oblasti testování
- **Test vyměnitelných zařízení** - specifický test vyměnitelných zařízení připojených v danou chvíli k Vašemu PC

10.7.1. Test celého počítače

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



Nastavení testu

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

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



- **Hlásit potenciálně nežádoucí programy a spyware infekce** (ve výchozím nastavení zapnuto) - kontrola přítomnosti [potenciálně nežádoucích programů](#) (spustitelné programy, které mohou fungovat jako spyware nebo adware). Zaškrtnutím tohoto políčka aktivujete [Anti-Spyware](#), tj. bude se testovat přítomnost spyware, nejen virů. Spyware představuje poněkud problematickou kategorii malware, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány v domě a se souhlasem uživatele. Doporučíme vám ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
- **Hlásit rozšířenou množinu potenciálně nežádoucích programů** (ve výchozím nastavení vypnuto) - zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně můžete blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.
- **Kontrolovat tracking cookies** (ve výchozím nastavení vypnuto) - parametr komponenty [Anti-Spyware](#) definuje, že během testu mají být detekovány cookies (HTTP data zaslaná serverem prohlížeči a uložena na počítači uživatele; při každé další návštěvě téhož serveru prohlížeč posílá cookies zpět serveru, který podle nich rozlišuje jednotlivé uživatele).
- **Testovat archivy** (ve výchozím nastavení vypnuto) - parametr definuje, že test má kontrolovat všechny soubory zabalené v některém typu archivu, například ZIP, RAR, ...
- **Použít heuristickou analýzu** (ve výchozím nastavení zapnuto) - během testu bude použita k detekci infekce i metoda heuristické analýzy (dynamické emulace instrukcí testovaného objektu v prostředí virtuálního počítače).
- **Testovat systémové prostředí** (ve výchozím nastavení zapnuto) - test prověří i systémové oblasti vašeho počítače.
- **Povolit testování s extrémní citlivostí** (ve výchozím nastavení vypnuto) - ve specifických situacích (při podezření na infekci ve vašem počítači) můžete zvolit tuto metodu testování, která aktivuje nejkvalitnější 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 nálezům 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** - při němž máte zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou (po uložení se čárky změní na středníky);
- **Vybrané typy souborů** - můžete se rozhodnout, že chcete, aby se testy spouštěly pouze nad soubory, které lze považovat za infikovatelné (soubory, které nemohou být infekcí zasaženy, se testovat nebudou - například prosté textové soubory nebo některé

nespustitelné soubory), a to včetně multimediálních souborů (video, audio soubory - ponecháte-li tuto položku neoznačenou, výrazně se tím zkrátí čas testování, jelikož multimediální soubory jsou obvykle poměrně velké, ale pravděpodobnost infekce je u nich velmi nízká). I zde můžete určit výjimky a pomocí seznamu přípon definovat, které soubory mají být testovány za všech okolností.

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

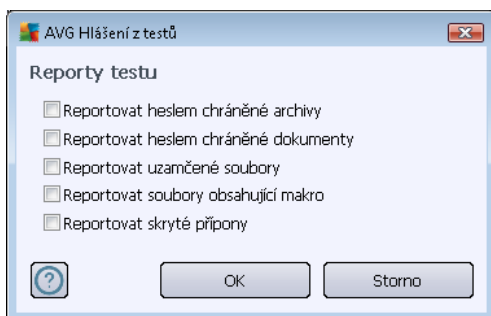
Nastavit, jak rychle probíhá test

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

Pokud se rozhodnete pro spuštění rychlého testu, proběhne test v kratším čase, ale po dobu jeho běhu bude výrazně zvýšena zatížení 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 zatížení systémových zdrojů a vaše práce na počítači nebude téměř ovlivněna, test však bude probíhat po delší dobu.

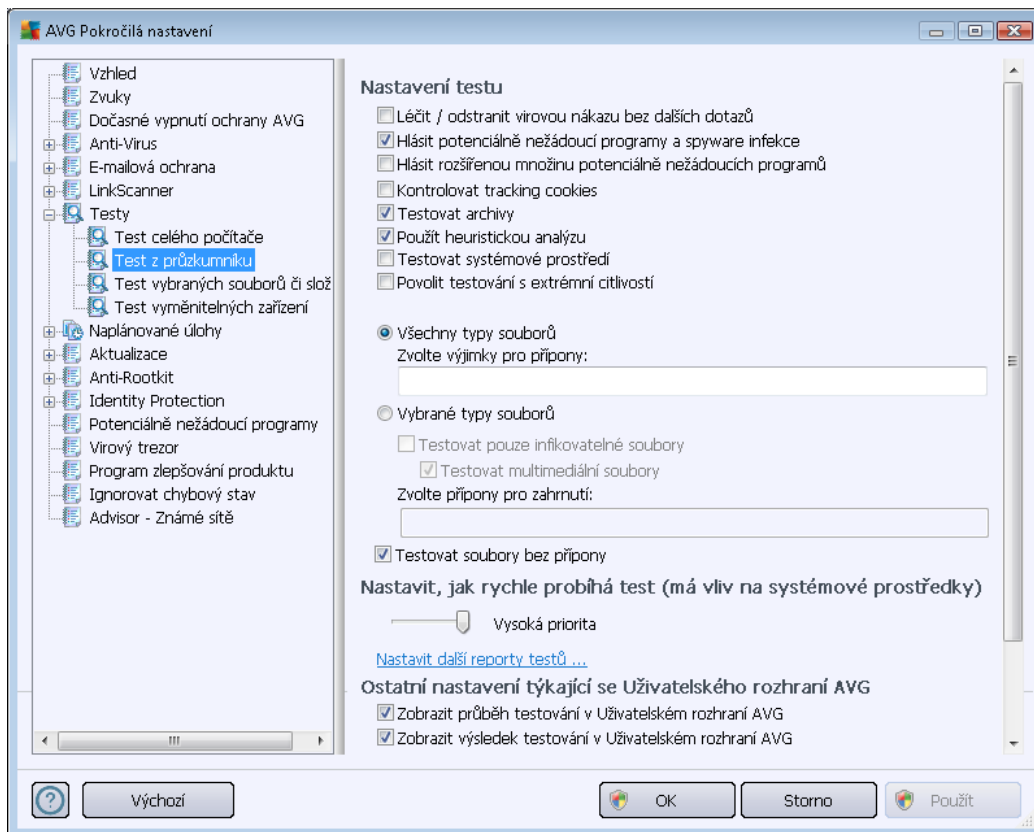
Nastavit další reporty testů ...

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



10.7.2. Test z průzkumníku

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



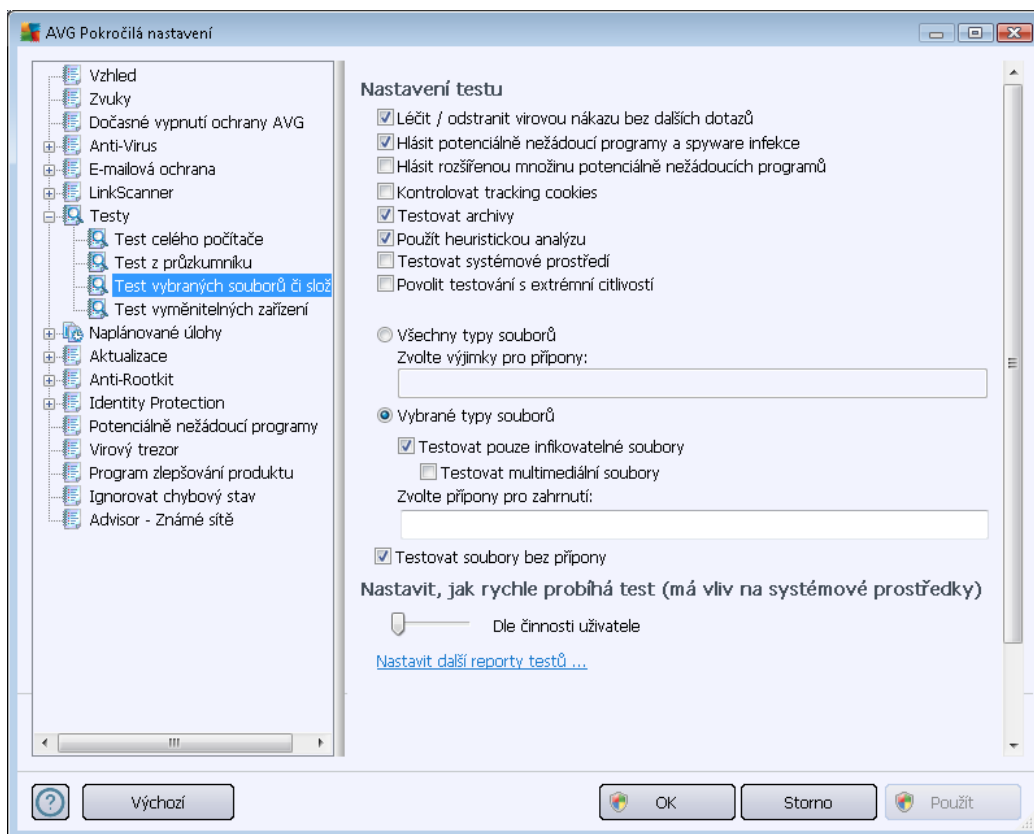
Veškeré možnosti editace parametrů testu jsou totožné s [editací parametrů Testu celého počítače](#). Odlišné je pouze výchozí nastavení těchto parametrů (například *Test celého počítače* ve výchozím nastavení neprovádí kontrolu archivů, ale provádí kontrolu systémového prostředí, zatímco u *Testu z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

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

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

10.7.3. Test vybraných souborů či složek

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

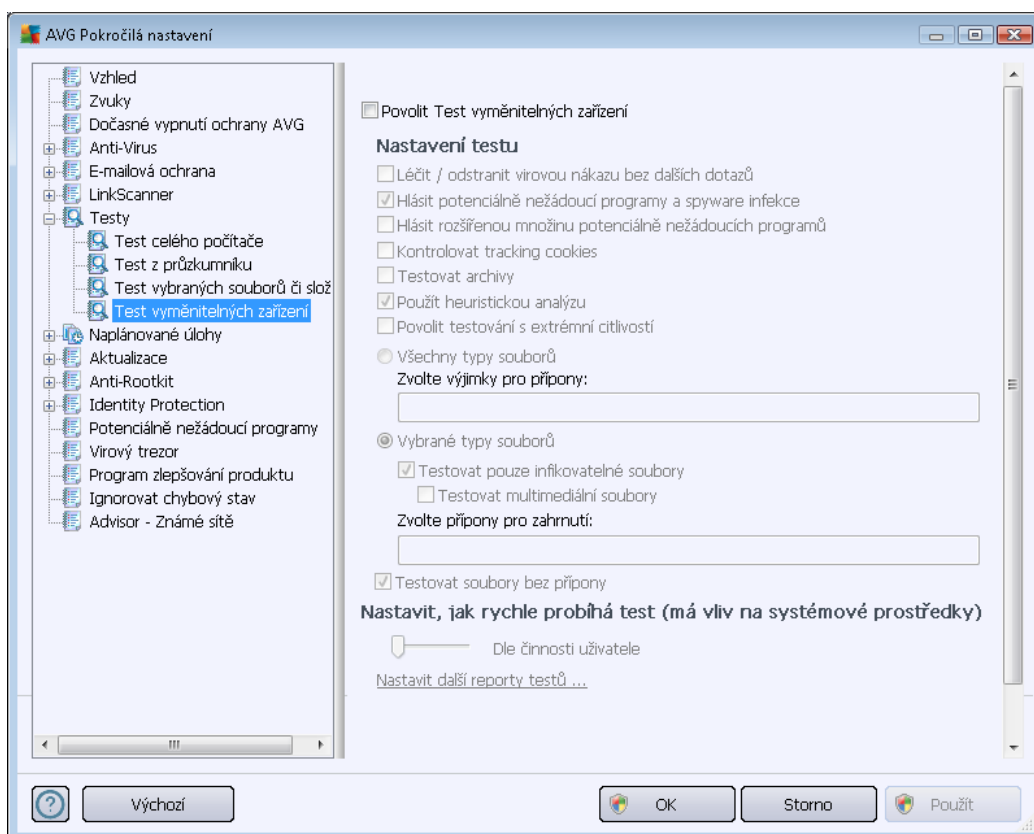


Veškeré parametry nastavené v tomto konfiguračním dialogu se vztahují pouze na ty oblasti vašeho počítače, které jste vybrali pro testování v rámci [Testu vybraných souborů či složek](#)!

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

10.7.4. Test vyměnitelných zařízení

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



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

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

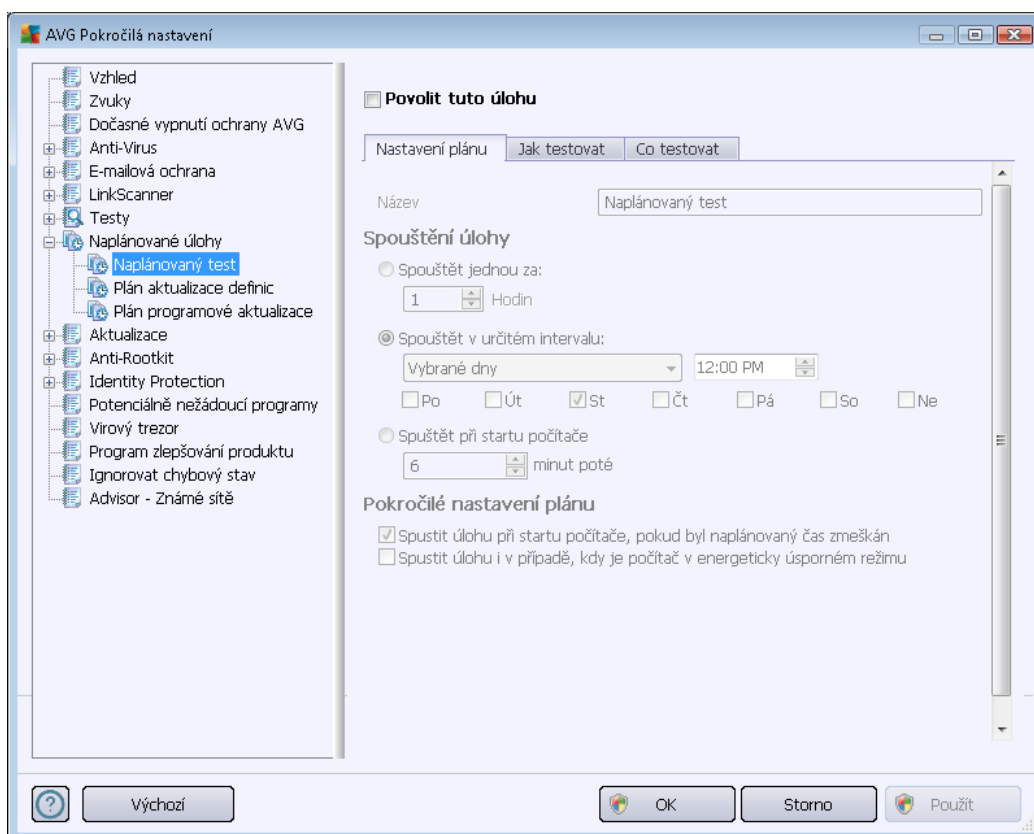
10.8. Naplánované úlohy

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

- [Naplánovaného testu](#)
- [Plánu aktualizace definic](#)
- [Plánu programové aktualizace](#)

10.8.1. Naplánovaný test

V tomto dialogu máte možnost konfigurovat nastavení naplánovaného testu a určit, jak často má být spuštěn v pravidelných intervalech. Parametry naplánovaného testu můžete editovat na všech záložkách. Na každé záložce máte nejprve možnost jednoduchým označením položky **Povolit tuto úlohu** naplánovaný test (do asn) deaktivovat, a později podle potřeby znovu použít.



V textovém poli **Název** (toto pole je u všech předem nastavených plánů deaktivováno) je uvedeno jméno pízené právě nastavenému testu. V rámci **AVG Anti-Virus Free Edition 2012** není bohužel možné vytvářet vlastní plány testování.

AVG Anti-Virus Free Edition 2012 je dostupný zdarma a jeho funkčnost je omezená. Pokud během používání AVG Anti-Virus Free Edition 2012 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

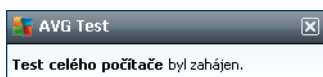
V této sekci dialogu určíte, v jakých časových intervalech má být nově naplánovaný test spuštěn.



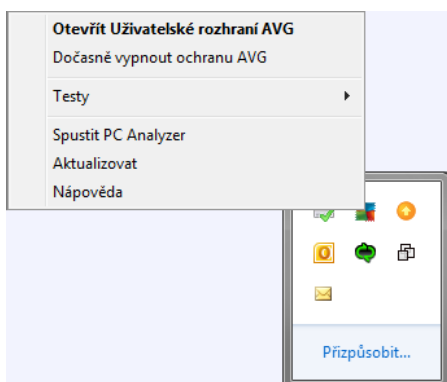
asové ur ení m žete zadat bu to opakovaným spušt ním testu po uplynutí ur ené doby (**Spoušt t jednou za**) nebo stanovením p esného data a asu (**Spoušt t v ur itém intervalu**), p ípadn ur ením události, na niž se spušt ní testu váže (**Spoušt t p i startu po íta e**).

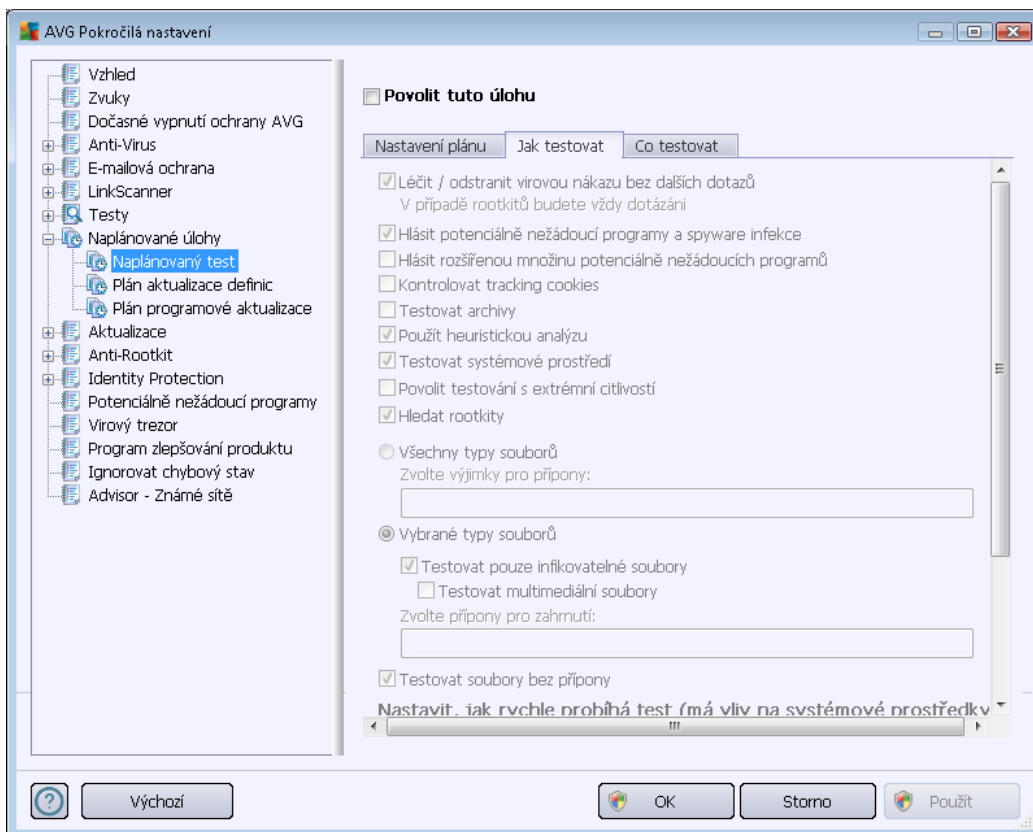
Pokro ilé nastavení plánu

Tato sekce umož ũje definovat podmínky, kdy má í nemá být test spušt n, jestliže je po íta v úsporném režimu nebo zcela vypnutý a naplánovaný as spušt ní testu byl zmeškán. O automatickém spušt ním testu budete v ur eném ase informováni prost ednictvím pop-up okna nad [ikonou AVG na systémové lišt ě](#) :



Po zahájení testu zm ní ikona na systémové lišt ě sv j vzhled (*ikona se nyní zobrazuje s otá ejícím se paprskem sv tla*), a tím vás informuje o b žícím testu. Kliknutím pravého tlačítka myši nad touto ikonou otev ete kontextové menu, z n hož m žete b žící test pozastavit nebo ukon ět, a rovn ž zm nit prioritu práv probíhajícího testu:





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

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



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

- **Kontrolovat tracking cookies** (ve výchozím nastavení vypnuto): parametr komponenty [Anti-Spyware](#) definuje, že během testu mají být detekovány cookies (*HTTP data zaslaná serverem prohlížeči a uložena na počítači uživatele; při každé další návštěvě téhož serveru prohlížeč posílá cookies zpět serveru, který podle nich rozlišuje jednotlivé uživatele*);
- **Testovat archivy** (ve výchozím nastavení vypnuto): parametr definuje, že test má kontrolovat všechny soubory, a to i takové, které jsou zabaleny v nějakém typu archivu, například ZIP, RAR, ...
- **Použít heuristickou analýzu** (ve výchozím nastavení zapnuto): během testu bude použita k detekci infekce i metoda heuristické analýzy (*dynamické emulace instrukcí testovaného objektu v prostředí virtuálního počítače*);
- **Testovat systémové prostředí** (ve výchozím nastavení zapnuto): test provádí i systémové oblasti vašeho počítače;
- **Povolit testování s extrémní citlivostí** (ve výchozím nastavení vypnuto) - ve specifických situacích (například při podezření na infekci starším typem viru) můžete zvolit tuto metodu testování, která aktivuje nejdokladnější testovací algoritmy a velmi podrobně provádí naprostě 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 nálezům 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** - pokud máte zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou (*po uložení se čárky změní na středníky*);
- **Vybrané typy souborů** - můžete se rozhodnout, že chcete, aby se testy spouštěly pouze nad soubory, které lze považovat za infikovatelné (*soubory, které nemohou být infekcí zasaženy, se testovat nebudou - například prosté textové soubory nebo některé nespustitelné soubory*), a to včetně multimediálních souborů (*video, audio soubory - ponecháte-li tuto položku neoznačenou, výrazně se tím zkrátí čas testování, jelikož multimediální soubory jsou obvykle poměrně velké, ale pravděpodobnost infekce je u nich velmi nízká*). I zde můžete určit výjimky a pomocí seznamu přípon definovat, které soubory mají být testovány za všech okolností.
- U položky **Testovat soubory bez přípon** pak rozhodnete, zda se mají testovat i soubory se skrytou nebo neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme, abyste se tohoto nastavení drželi, pokud nemáte skutečný důvod jej změnit. Soubory bez přípon jsou obecně vysoce podezřelé a měly by být otestovány.

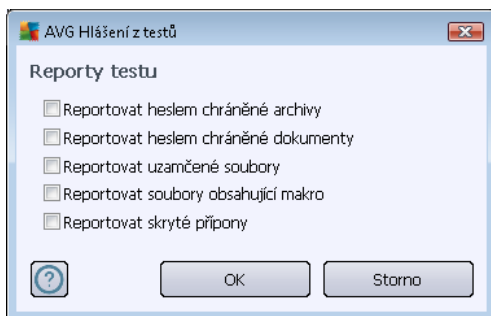
Nastavit, jak rychle probíhá test

V sekci **Priorita testu** můžete nastavit požadovanou rychlost testování v závislosti na zátěži systémových zdrojů. Ve výchozím nastavení je tato hodnota nastavena na úroveň **Dle innosti uživatele**, což znamená, že je využito minimum systémových prostředků ve chvíli, kdy se počítač nepracuje, a naopak maximum ve chvíli, kdy se počítač nepracuje.

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.

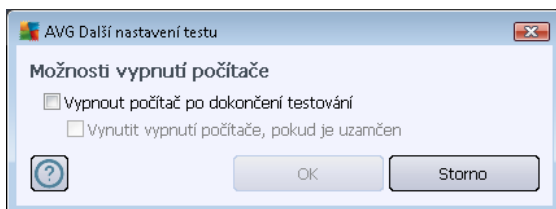
Nastavit další reporty testu

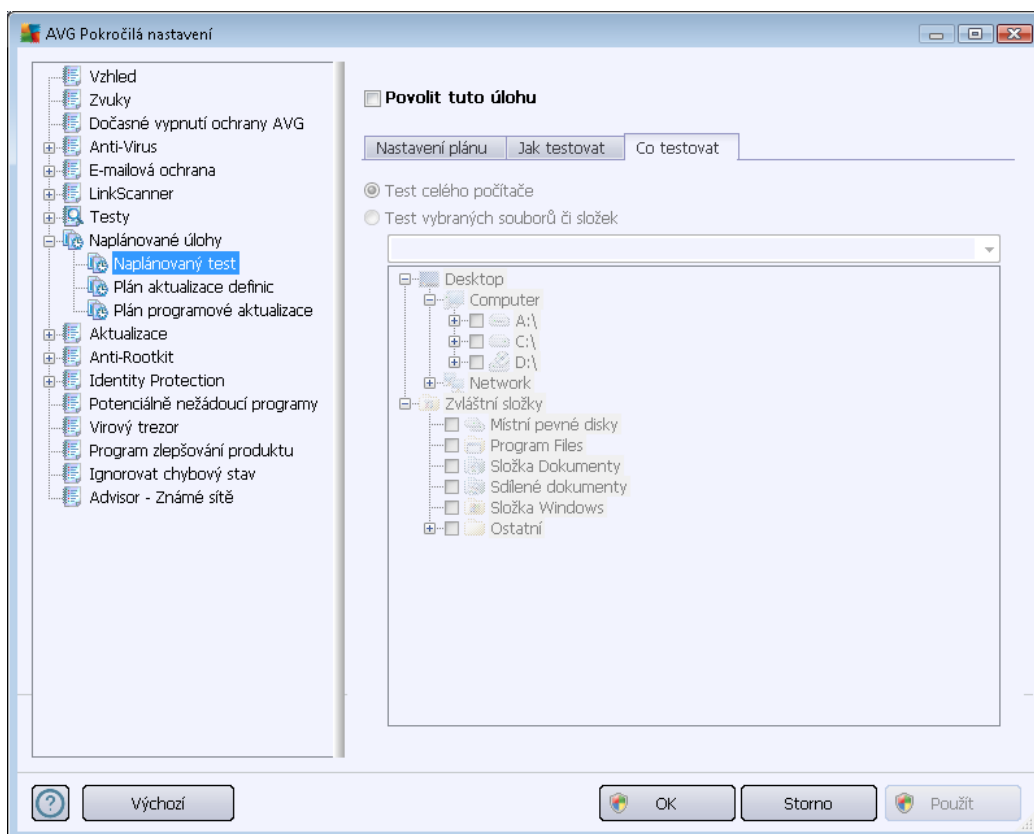
Kliknutím na odkaz **Nastavit další reporty testu ...** otevřete samostatné dialogové okno **Reporty testu**, v němž můžete označit příslušné položky určité situace, jejichž výskyt během testu má být hlášen:



Další nastavení testu

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

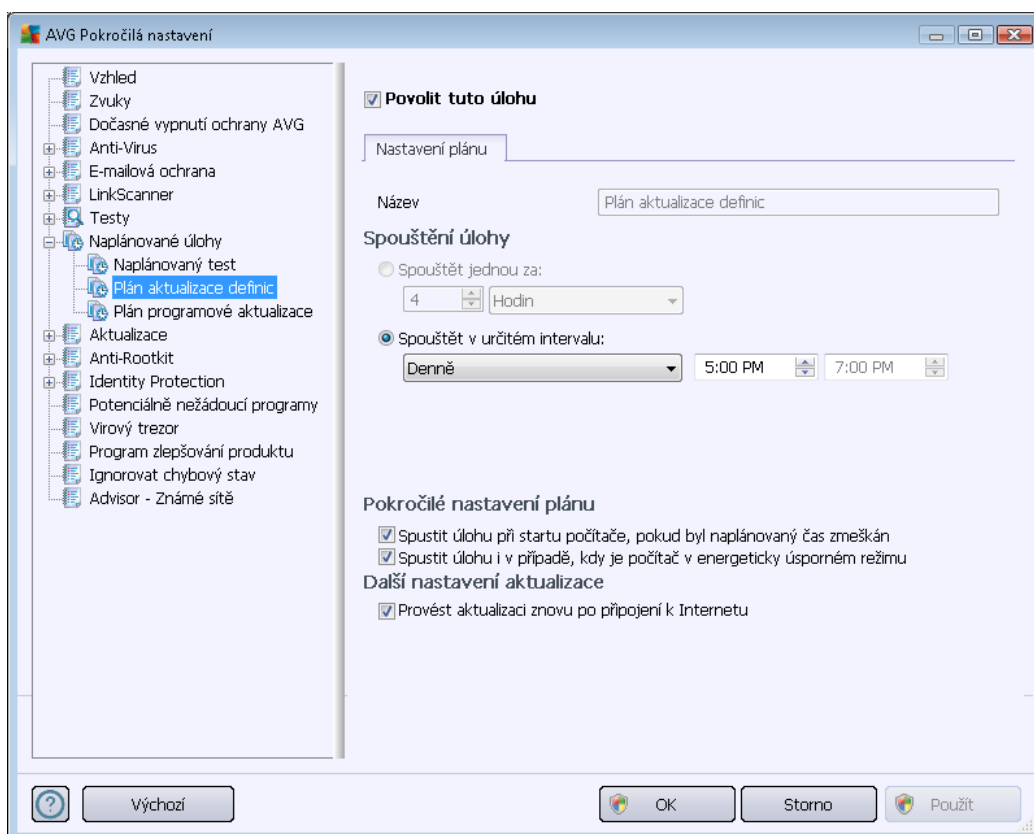




Na záložce **Co testovat** definujete, zda si přejete naplánovat [Test celého počítače](#) nebo [Test vybraných souborů či složek](#). V případě, že se rozhodnete pro test vybraných souborů a složek, ve spodní sekci dialogu se aktivuje zobrazená stromová struktura vašeho disku a v ní můžete označit adresáře,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

10.8.2. Plán aktualizace definic

Na záložce **Nastavení plánu** máte nejprve možnost jednoduchým označením položky **Povolit tuto úlohu** naplánovanou aktualizaci (dočasně) deaktivovat, a později ji 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 příslušného nastaveného plánu aktualizace.

Spouštění úloh

Určete, v jakých časových intervalech má být nově naplánovaná aktualizace definic provedena. V rámci **AVG Anti-Virus Free Edition 2012** je k dispozici pouze volba **Spouštět v určitém intervalu**. Ta je nastavena tak, aby byla aktualizace stažena nejméně jednou denně, v rozmezí dvou hodin. Můžete si však zvolit požadovaný čas intervalu, kdy má být aktualizace stažena.

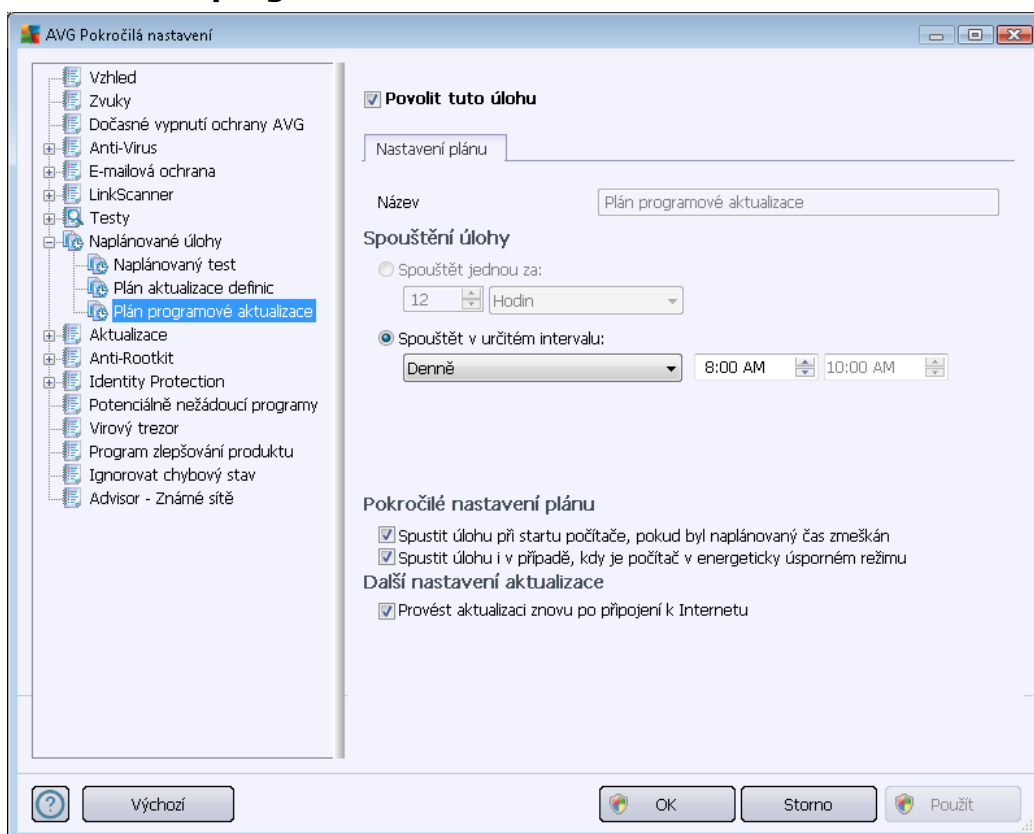
Pokročilé nastavení plánu

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 časovém intervalu informováni prostřednictvím pop-up okna nad [ikonou AVG na systémové liště](#) (za předpokladu, že ponecháte zapnutou volbu **Zobrazovat oznámení na systémové liště** v [Pokročilém nastavení/Vzhled](#)).

10.8.3. Plán programové aktualizace



Na záložce **Nastavení plánu** máte nejprve možnost jednoduchým označením položky **Povolit tuto úlohu** naplánovanou programovou aktualizaci (dočasně) deaktivovat, a později podle potřeby znovu použít. V textovém poli **Název** (toto pole je u všech předem nastavených plánů deaktivováno) je uvedeno jméno příslušného nastaveného plánu programové aktualizace.

Spouštění úloh

Určete, v jakých časových intervalech má být nově naplánovaná programová aktualizace provedena. Časové určení můžete zadat buďto opakovaným spuštěním aktualizace po uplynutí určité doby (**Spouštět jednou za**) nebo stanovením přesného data a času (**Spouštět v určitém intervalu**), případně určitým událostí, na niž se spuštění aktualizace váže (**Spouštět při spuštění počítače**).



Pokročilé nastavení plánu

Tato sekce umožňuje definovat podmínky, kdy má či nemá být programová aktualizace spuštěna, jestliže je povolena v úsporném režimu nebo zcela vypnutá a naplánovaná. Pokud byla aktualizace zmeškána.

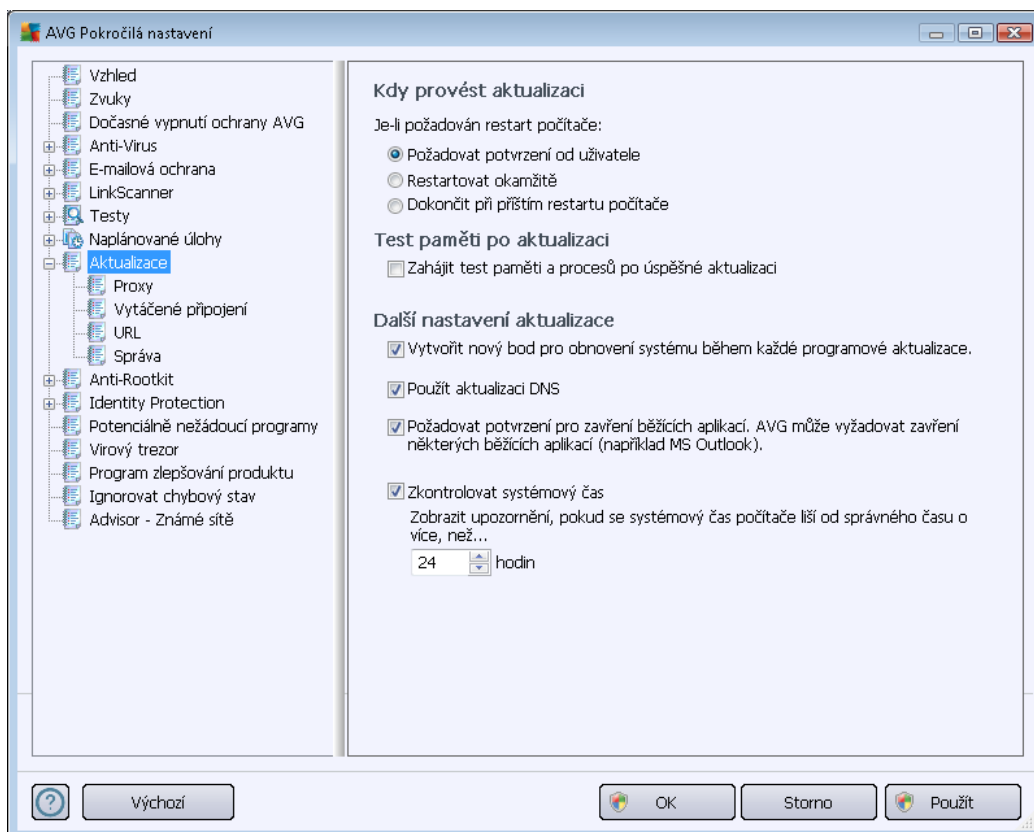
Další nastavení aktualizace

Volbou položky **Provést aktualizaci znovu po připojení k Internetu** zajistíte, že pokud dojde 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 časovém intervalu informováni prostřednictvím pop-up okna nad [ikonou AVG na systémové liště](#) (za předpokladu, že ponecháte zapnutou volbu **Zobrazovat oznámení na systémové liště** v [Pokročilém nastavení/Vzhled](#)).

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

10.9. Aktualizace

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





Kdy provést aktualizaci

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

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

Test paměti po aktualizaci

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

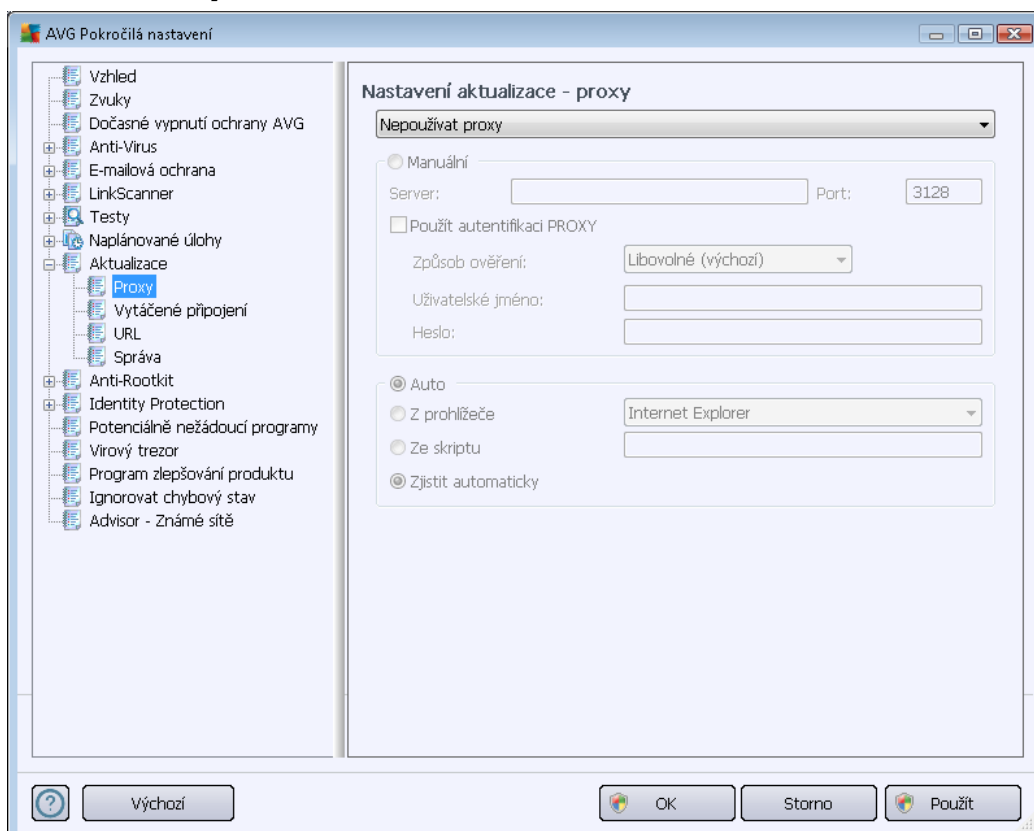
Další nastavení aktualizace

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

- **Po každé programové aktualizaci vytvořit nový bod pro obnovení systému** - před každým spuštěním programové aktualizace AVG je tak zvaný systémový bod pro obnovení systému. V případě, že aktualizací proces nebude z nějakého důvodu dokončen a váš operační systém bude ohrožen, můžete za pomoci tohoto zálohovacího bodu obnovit OS v jeho původní konfiguraci. Tato možnost je dostupná přes volbu *Start / Všechny programy / Příslušenství / Systémové nástroje / Obnova systému*, ale jakékoliv zásahy do tohoto nastavení lze doporučit výhradně pokročilým a zkušeným uživatelům! Chcete-li využít této možnosti, ponechejte políčko označené.
- **Použít aktualizaci DNS (ve výchozím nastavení zapnuto)** - pokud je tato položka označena, při spuštění aktualizace **AVG Anti-Virus Free Edition 2012** vyhledá na DNS serveru informaci o aktuální verzi virové databáze a aktuální verzi programu a následně stáhne pouze nejmenší nezbytně nutné aktualizací soubory. Tím se sníží celkový objem stahovaných dat a urychlí proces aktualizace.
- **Požadovat potvrzení pro zavěšení běžících aplikací (ve výchozím nastavení zapnuto)** zajistíte, že v případě, že bude nutné zavěsit některé spuštěné aplikace, aby mohla být aktualizace dokončena, budete před jejich zavěšením upozorněni varovným hlášením.
- **Zkontrolovat systémový čas** - označením této položky určíte, že si přejete, abyste byli

informování o případném rozporu mezi časem nastaveným na počítaři a skutečným časem, a to v okamžiku, kdy rozdíl těchto dvou časů dosáhne stanoveného počtu hodin.

10.9.1. Proxy



Proxy server je samostatný server nebo služba běžící na libovolném počítaři, 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 určíte, zda si přejete:

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

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

Manuální nastavení

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



položky:

- **Server** – zadejte IP adresu nebo jméno serveru
- **Port** – zadejte číslo portu, na němž je povolen přístup k internetu (*výchozím nastavením je číslo portu 3128, ale může být nastaveno jinak – pokud si nejste jisti, obraťte se na správce vaší 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.

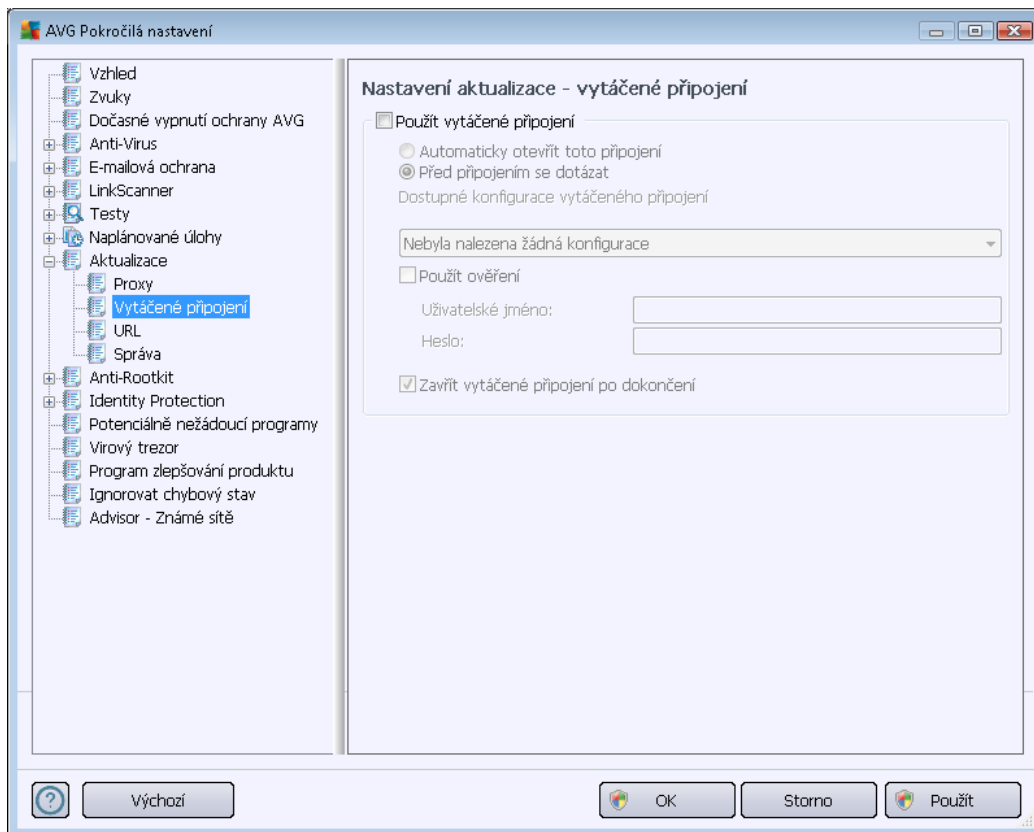
Automatické nastavení

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

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

10.9.2. Vytáčené připojení

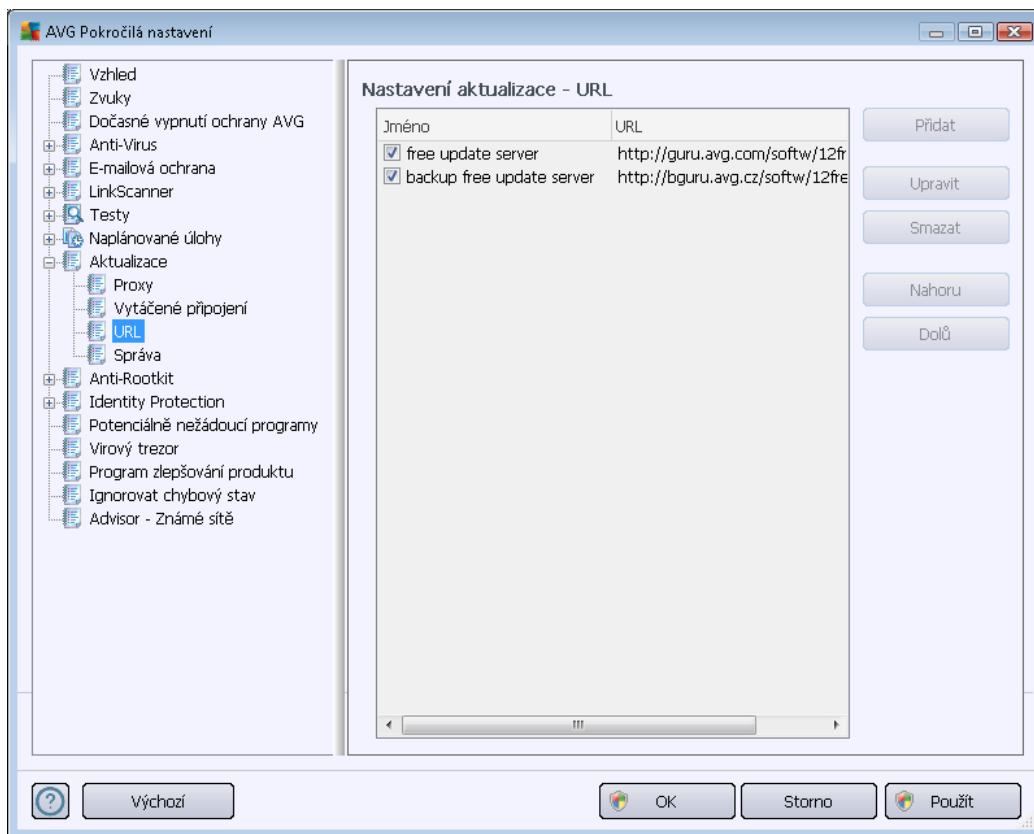
Parametry nastavované v dialogu **Nastavení aktualizace - vytáčené připojení** se vztahují k telefonickému připojení. Jednotlivá pole záložky jsou neaktivní, pokud neoznačíte položku **Použít vytáčené připojení**. Touto volbou se pak aktivují ostatní pole:



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

10.9.3. URL

Dialog **URL** nabízí seznam internetových adres, odkud mohou být aktualizací soubory staženy:



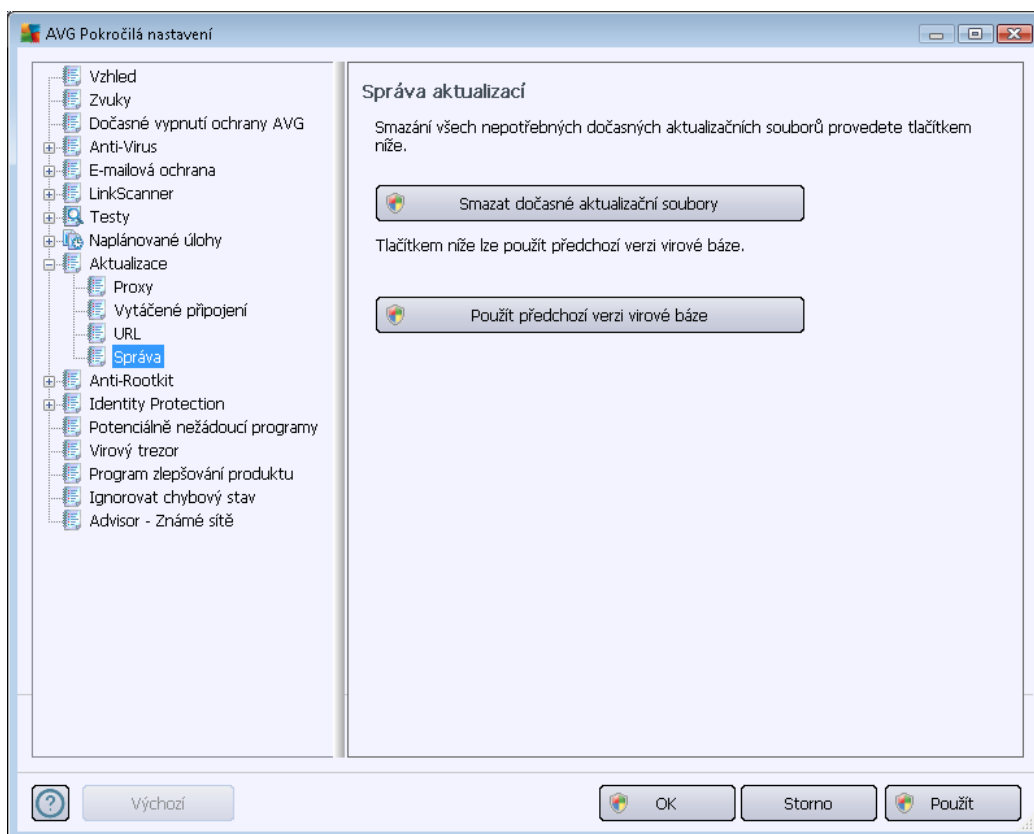
Ovládací tlačítka dialogu

Seznam a jeho jednotlivé položky nelze v rámci **AVG Anti-Virus Free Edition 2012** editovat, tato možnost je dostupná pouze u profesionálních verzí AVG. Tlačítka po pravé straně dialogu jsou tedy neaktivní.

AVG Anti-Virus Free Edition 2012 je dostupný zdarma a jeho funkce je omezená. Pokud během používání AVG Anti-Virus Free Edition 2012 zjistíte, že byste dali přednost plně funkční profesionální verzi AVG, navštivte prosím web AVG (<http://www.avg.cz/>), kde najdete informace o možnostech koupě placených produktů AVG.

10.9.4. Správa

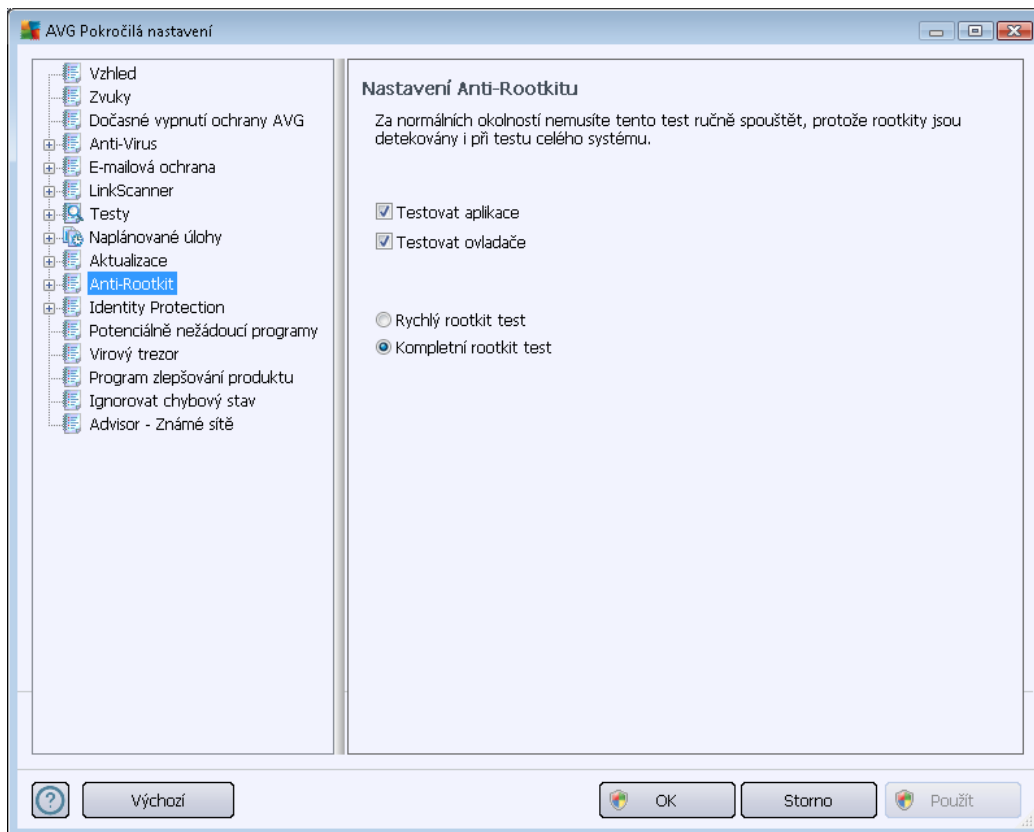
Dialog **Správa aktualizací** obsahuje dvě možnosti volby dostupné prostřednictvím dvou tlačítek:



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

10.10. Anti-Rootkit

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



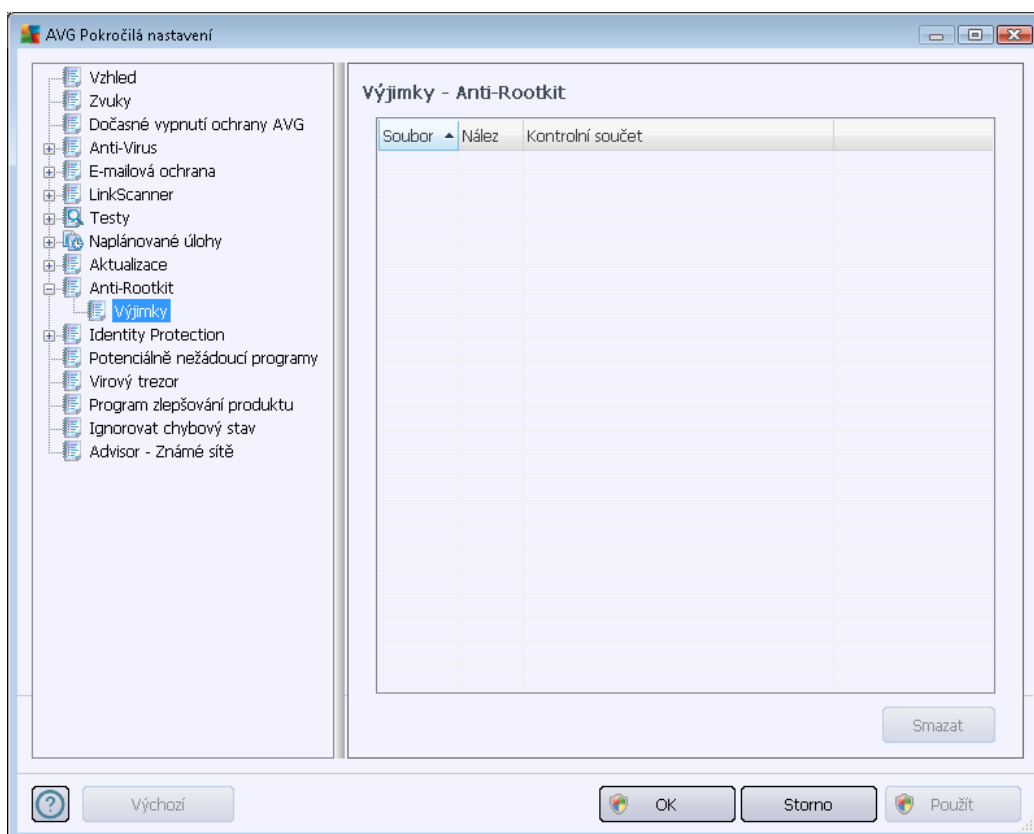
Editace všech funkcí komponenty [Anti-Rootkit](#) uvedená v tomto dialogu je dostupná i přímo z [rozhraní komponenty Anti-Rootkit](#).

Možnosti **Testovat aplikace** a **Testovat ovladače** umožní 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 můžete rozhodnout, v jakém režimu si přejete test spustit:

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

10.10.1. Výjimky

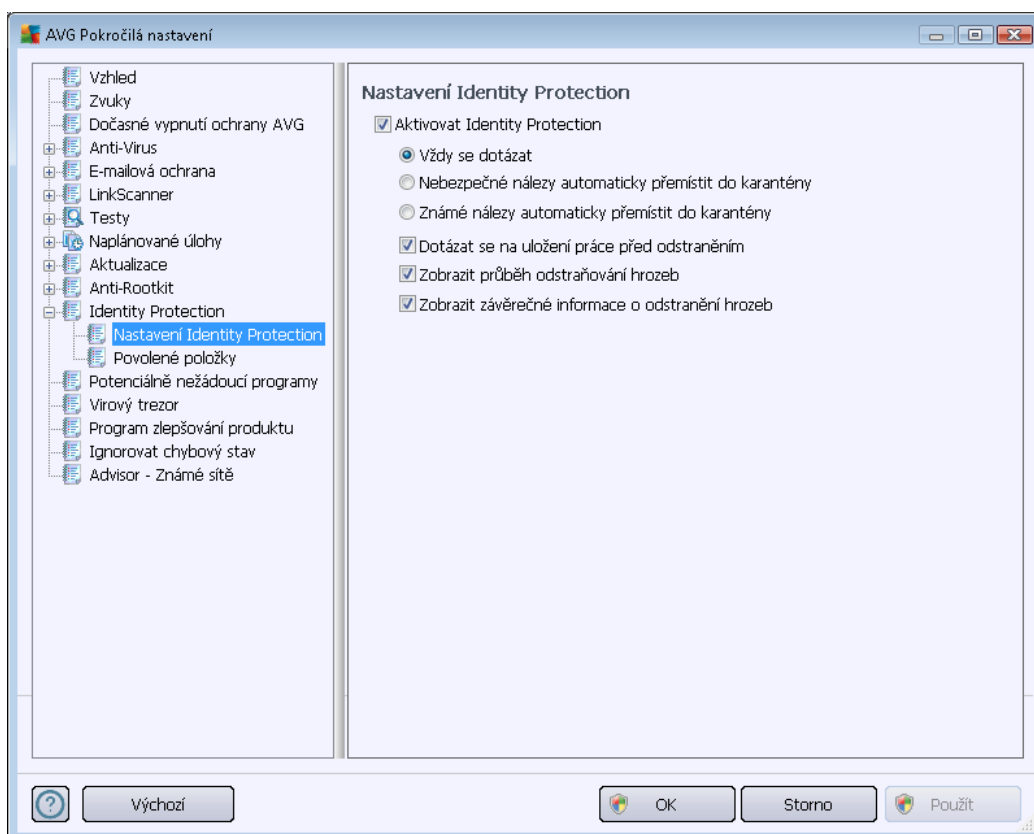
V dialogu **Výjimky - Anti-Rootkit** můžete definovat specifické soubory (například které ovládá e, jež mohou být chybně detekovány jako rootkit), které mají být z testování vyřazeny:



10.11. Identity Protection

10.11.1. Nastavení Identity Protection

Dialog **Nastavení Identity Protection** umožňuje zapnout i vypnout některé základní vlastnosti komponenty [Identity Protection](#):



Položka

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

Důležitá doporučení: ponechat komponentu zapnutou!

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

- **Vždy se dotázat** (ve výchozím nastavení zvoleno) - při nálezů potenciálně 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 počítaři 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 nálezů potenciálně 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 počítaři chcete.



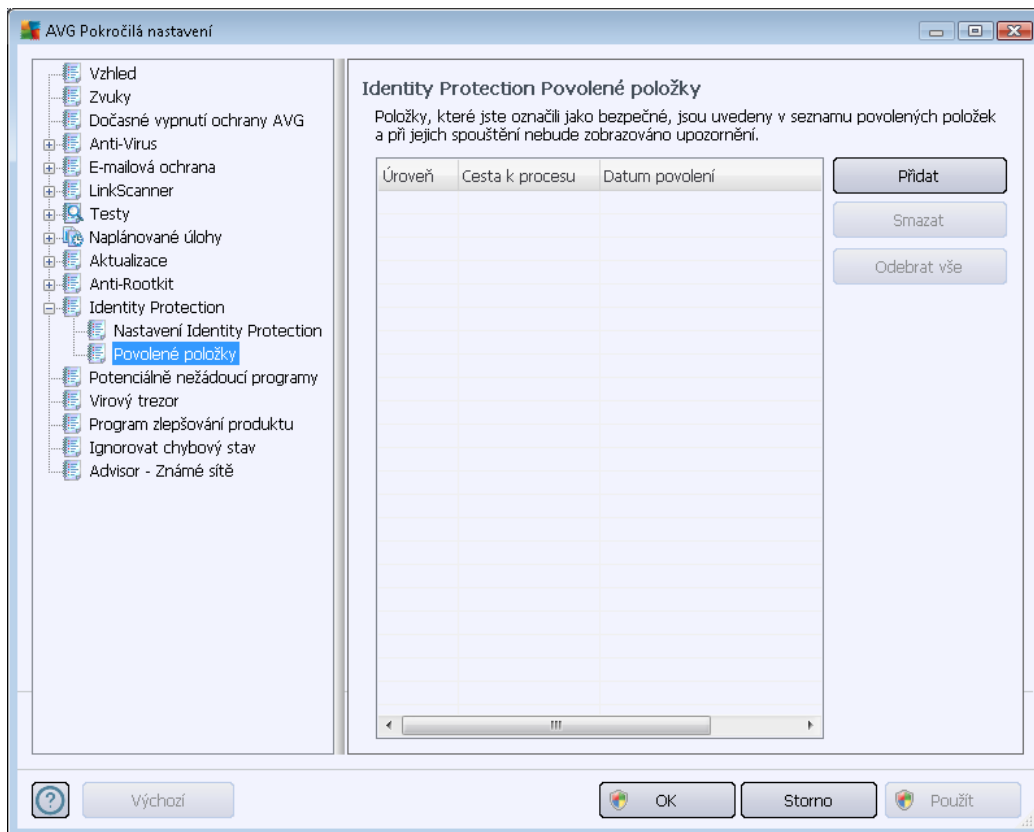
- **Známé nálezy automaticky p emístít do karantény** - ozna te tuto položku, pokud si p ejete, aby veškeré aplikace detekované jako možný malware byly automaticky a okamžit p esunuty do [Virového trezoru](#).

Pak m žete ozna ením p íslušných polí ek voliteln aktivovat další vlastnosti [Identity Protection](#):

- **Dotázat se na uložení práce p ed odstran ním** - (ve výchozím nastavení zapnuto) - ozna te tuto položku, pokud si p ejete, abyste byli v p ípad detekce škodlivého software a jeho odstran ní vyzváni k uložení práce rozd lané v p íslušném programu. Položka je ve výchozím nastavení zapnuta a d razn doporu ujeme toto nastavení ponechat.
- **Zobrazit pr b h odstra ování hrozeb** - (ve výchozím nastavení zapnuto) - je-li položka ozna ena, p í detekci potenciálního malware bude v samostatném nov otev eném dialogu zobrazen postup jeho p emis ování do karantény.
- **Zobrazit záv re né informace o odstran ní hrozeb** - (ve výchozím nastavení zapnuto) - je-li položka ozna ena, zobrazí [Identity Protection](#) podrobné informace o každé položce, kterou umístí do karantény, v etn úrovni závažnosti, p esného umíst ní a dalších charakteristik.

10.11.2. Povolené položky

Pokud jste v dialogu [Nastavení Identity Protection](#) ponechali položku **Nebezpe né nálezy automaticky p emístít do karantény** neozna enou, budete p í každém nálezu potenciáln nebezpe né aplikace dotázáni, zda má být tato aplikace skute n považována za malware a p esunuta do [Virového trezoru](#). Jestliže se tedy rozhodnete ozna it spornou aplikaci (*detekovanou jako malware na základ jejího chování*) za bezpečnou a potvrdíte, že si p ejete tuto aplikaci ponechat spušt nou na svém počíta i, bude aplikace p idána do seznamu **Povolných položek** a už nebude považována za škodlivou:



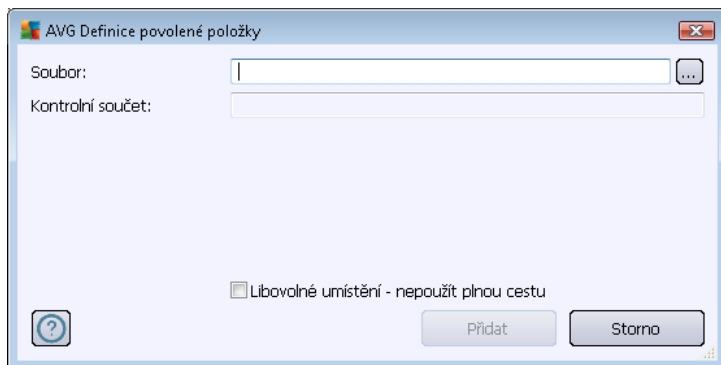
V seznamu **Povolené položky** najdete následující informace o každé aplikaci:

- **Úroveň** - grafické zobrazení závažnosti běžícího procesu na čtyřech stupních od nejnižšího až po nejvyšší (■□□□) až kritický (■□■□)
- **Cesta k procesu** - cesta k umístění spustitelného souboru dané aplikace (*procesu*)
- **Datum povolení** - datum, kdy jste ručně označili danou aplikaci jako povolenou

Ovládací tlačítka dialogu

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

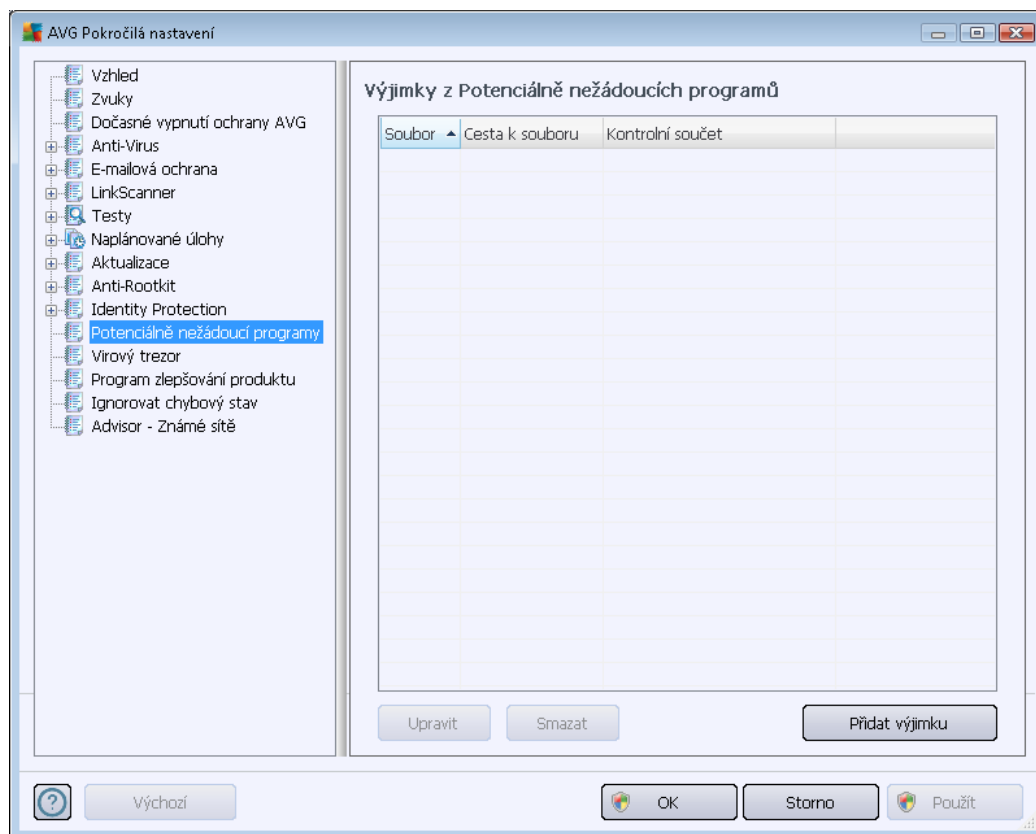
- **Přidat** - otevře editační dialog, v němž můžete nastavit parametry nově přidávané aplikace:



- **Soubor** - zadejte plnou cestu k souboru, který chcete označit jako výjimku
- **Kontrolní součet** - uvádí unikátní "podpis" vybraného souboru - automaticky vygenerovaný řetězec znaků, který umožní jednoznačně odlišit zvolený soubor od všech ostatních. Tento součet je vygenerován a zobrazen až po úspěšném přidání dané výjimky.
- **Libovolné umístění - nepoužít plnou cestu** - chcete-li uvedený soubor definovat jako výjimku pouze v tomto konkrétním umístění, ponechte položku Libovolné umístění – nepoužít úplnou cestu neoznačenou. Je-li položka označena, platí, že zadaný soubor je definován jako výjimka, a už je umístěn kdekoli (*plnou cestu ke konkrétnímu souboru však musíte vyplnit v každém případě; tento soubor bude použit jako jednoznačný vzor pro případ, že by se ve vašem systému vyskytly dva odlišné soubory stejného jména*).
- **Smazat** - stiskem tlačítka odstraní vybranou položku ze seznamu povolených aplikací
- **Odebrat vše** - stiskem tlačítka odstraní všechny položky ze seznamu povolených aplikací

10.12. Potenciálně nežádoucí programy

AVG Anti-Virus Free Edition 2012 má schopnost analyzovat spustitelné programy, například DLL knihovny, a určit, které z nich by mohly být nežádoucí (například spyware). Může se však stát, že některé z programů detekovaných jako nežádoucí, jsou na vašem počítači nainstalovány s vaším vědomím a používáte je. Příkladem může být bezplatný program, který obsahuje adware: termínem adware obecně rozumíme software generující zobrazení reklamy, obvykle přibalený jako doplněk k programu distribuovanému zdarma. **AVG Anti-Virus Free Edition 2012** může takový program při testech hlásit jako nežádoucí; pokud si však přejete jej na počítači ponechat, můžete jej definovat jako výjimku z potenciálně nežádoucích programů.

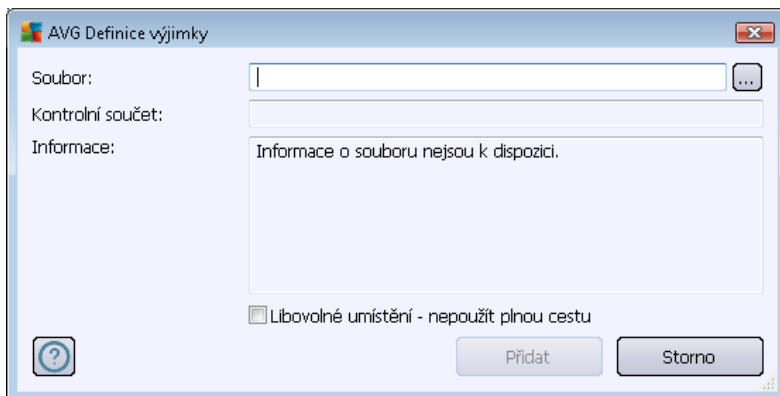


Dialog **Výjimky z Potenciálně nežádoucích programů** zobrazuje seznam již definovaných a aktuálně platných výjimek z potenciálně nežádoucích programů. Výjimku můžete editovat, smazat nebo nově přidat. Ke každé jednotlivé výjimce najdete v přehledu následující informace:

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

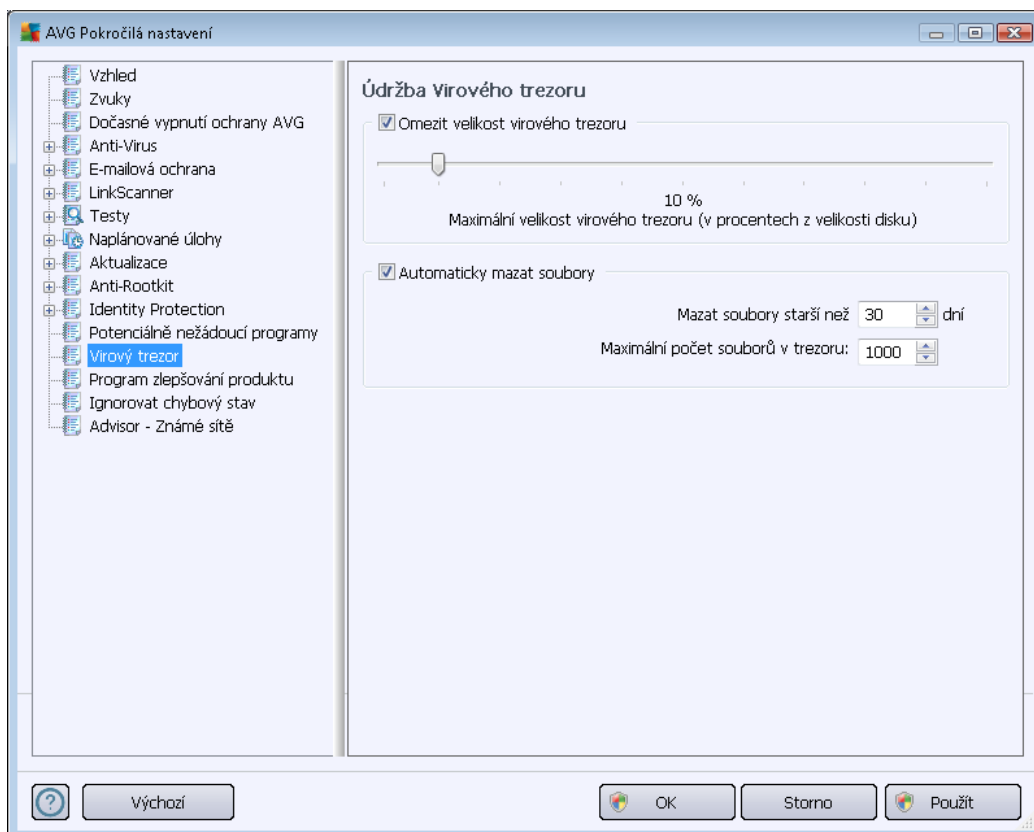
Ovládací tlačítka dialogu

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



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

10.13. Virový trezor



Dialog **Údržba Virového trezoru** umožňuje definovat několik parametrů souvisejících se správou objektů ve [Virovém trezoru](#):

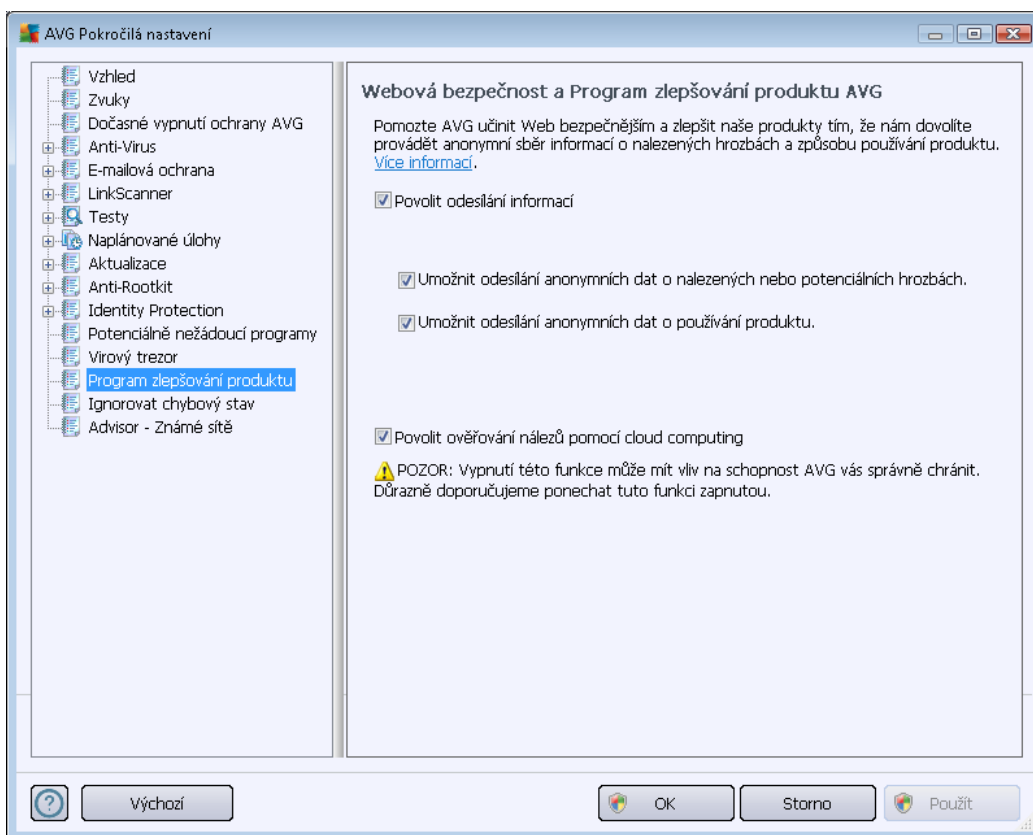
- **Omezit velikost virového trezoru** - Na posuvníku můžete nastavit maximální povolenou velikost [Virového trezoru](#). Velikost je určena procentuálně jako poměrná část velikosti vašeho lokálního disku.
- **Automaticky mazat soubory** - V této sekci definujete maximální dobu, po níž se mají uchovávat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

10.14. Program zlepšování produktu

V dialogu **Webová bezpečnost a Program zlepšování produktu AVG** máte možnost zapojit se do spolupráce a podílet se na zlepšování produktu AVG a na celkovém zvýšení úrovně bezpečnosti na Internetu. Ponecháte-li položku **Povolit odesílání informací** zapnutou (a rovněž obě z podskupin odesílaných informací), umožníte reportování informací o detekovaných hrozbách týmu expertů společnosti AVG Technologies. Tyto reporty nám pomáhají shromažďovat nejnovější informace o virech, spywaru i škodlivých webových stránkách a vylepšovat neustále ochranu pro všechny naše uživatele.

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

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



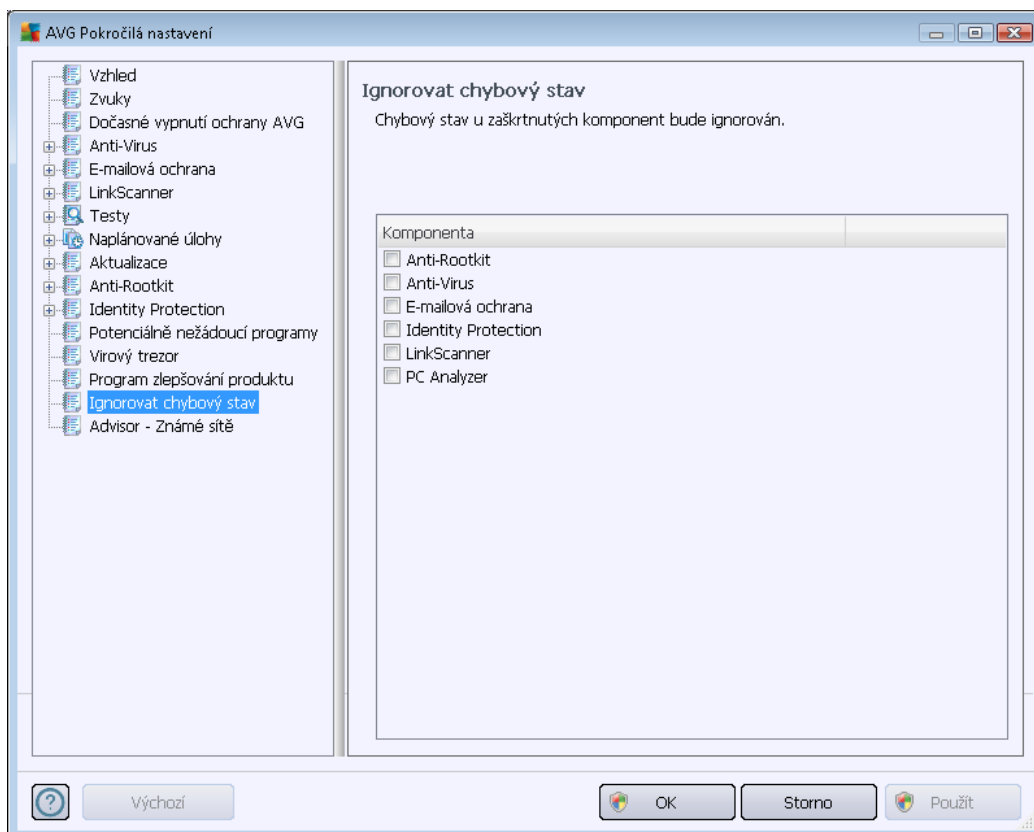
karet a podobn , p ípadn k proníknutí do počíta e za ú elem poskytnutí p ístupu cizí osob ; samoz ejm to vše bez v domí vlastníka počíta e.

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

AVG Anti-Virus Free Edition 2012 obsahuje ochranu proti všem zmín ěným typ m hrozeb a škodlivých program í ! Stru ěný p ehled funkcionality jednotlivých komponent najdete v kapitole [P ehled komponent](#).

10.15. Ignorovat chybový stav

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



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

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

Můžete se ale stát, že si z nějakého důvodu přejete 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 v domění potenciálního rizika. Zároveň by se tak zamezilo tomu, aby ikona reagovala na případnou jinou chybu v programu.

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

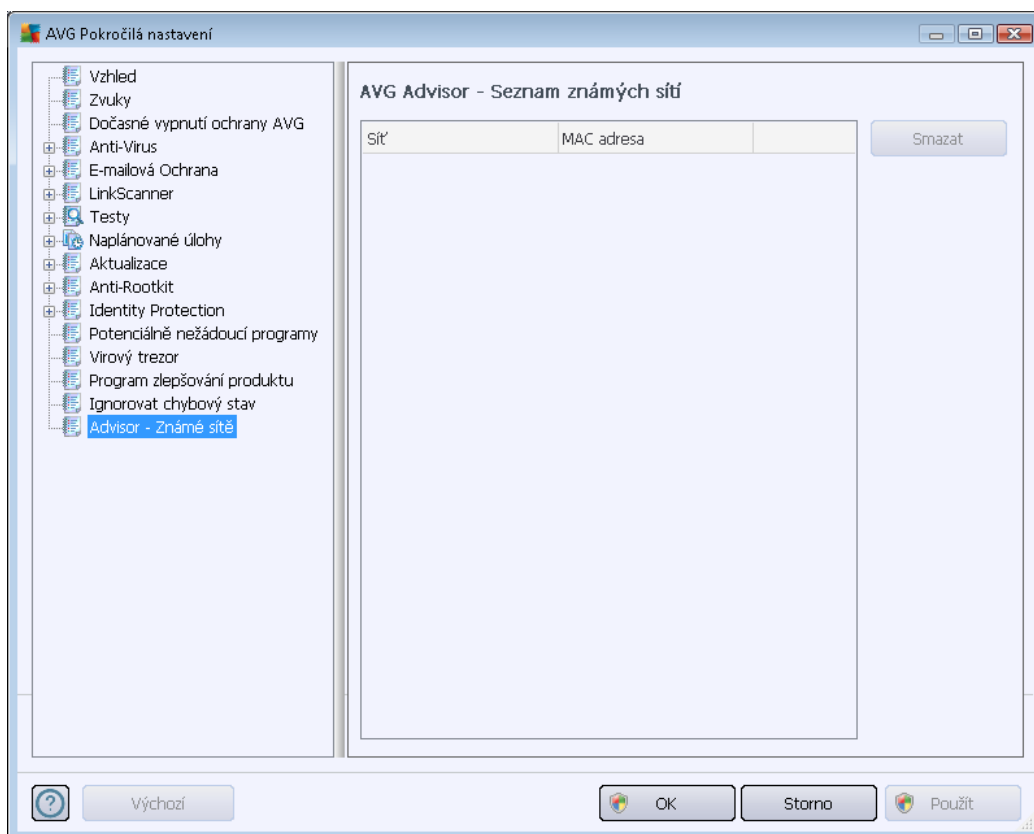


[okn_AVG](#).

10.16. Advisor - známé sítě

Služba [AVG Advisor](#) obsahuje funkci, která sleduje síť, do níž se připojíte. 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 provalidovali. 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 jediné identifikační údaje sítě, zejména adresu MAC, a přístroj už vás nebude upozorňovat. Každá síť, k níž se připojíte, bude pro přístroj automaticky považována za známou, a přidána do seznamu. Libovolné položky můžete vymazat pomocí tlačítka **Smazat**, pro síť pak bude znovu považována za neznámou a neprovalidovanou.

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

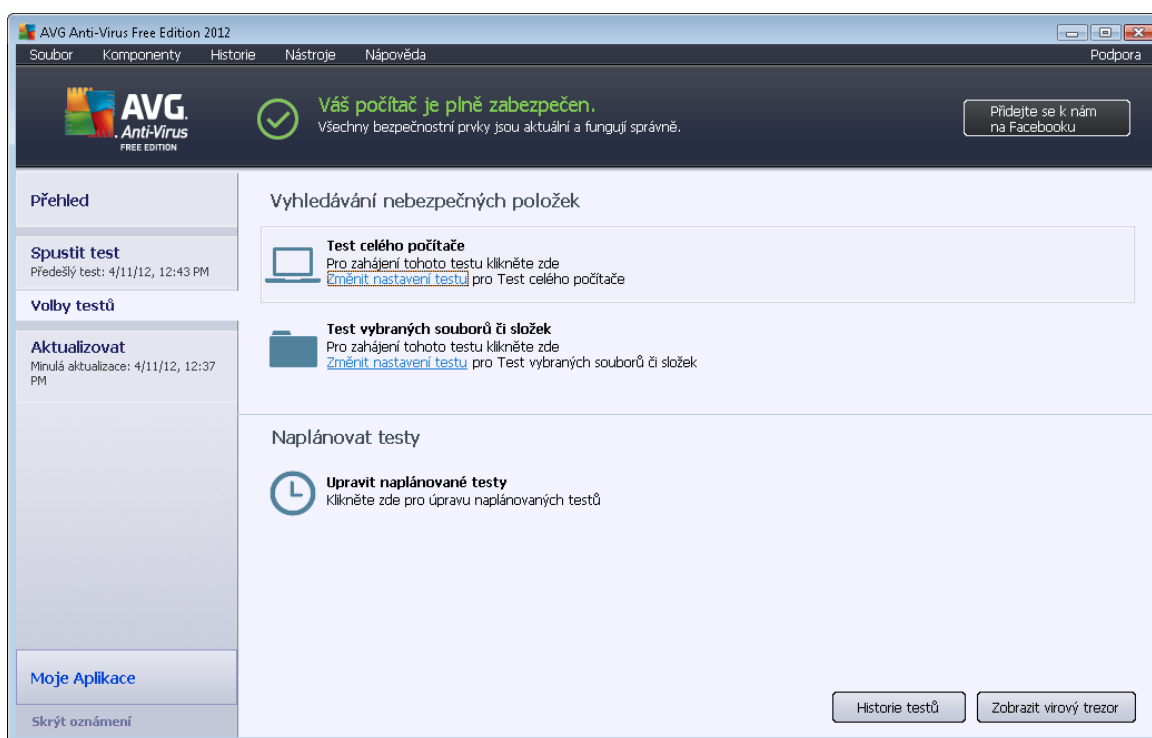


Poznámka: Funkce známé sítě v rámci služby AVG Advisor není podporována na Windows XP 64-bit.

11. AVG testování

Ve výchozím nastavení **AVG Anti-Virus Free Edition 2012** se nespouští žádný test automaticky, protože po úvodním otestování počítače jste pro bezpečnou ochranu rezidentními komponentami **AVG Anti-Virus Free Edition 2012**, které eventuelně škodlivý kód zachycují okamžitě. Samozřejmě můžete [naplánovat test](#) k pravidelnému spuštění v určený čas, případně kdykoli spustit ručně libovolný test podle vlastních požadavků.

11.1. Rozhraní pro testování



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

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

Ovládací tlačítka dialogu



Ovládací tlačítka dostupná v testovacím rozhraní jsou:

- **Historie test** - zobrazí dialog [Přehled výsledků testů](#) s kompletním seznamem historie testování
- **Zobrazit virový trezor** - v novém okně otevře [Virový trezor](#) - karanténní prostor pro uložení detekovaných infekcí

11.2. Přednastavené testy

Jednou z hlavních funkcí **AVG Anti-Virus Free Edition 2012** je testování na vyžádání. Testy na vyžádání jsou navrženy tak, že mohou testovat různé části vašeho počítače, kdykoliv se objeví podezření na možnost virové infekce. V každém případě však doporučujeme provádět testy pravidelně, i když považujete váš počítač za zcela virus-prostý.

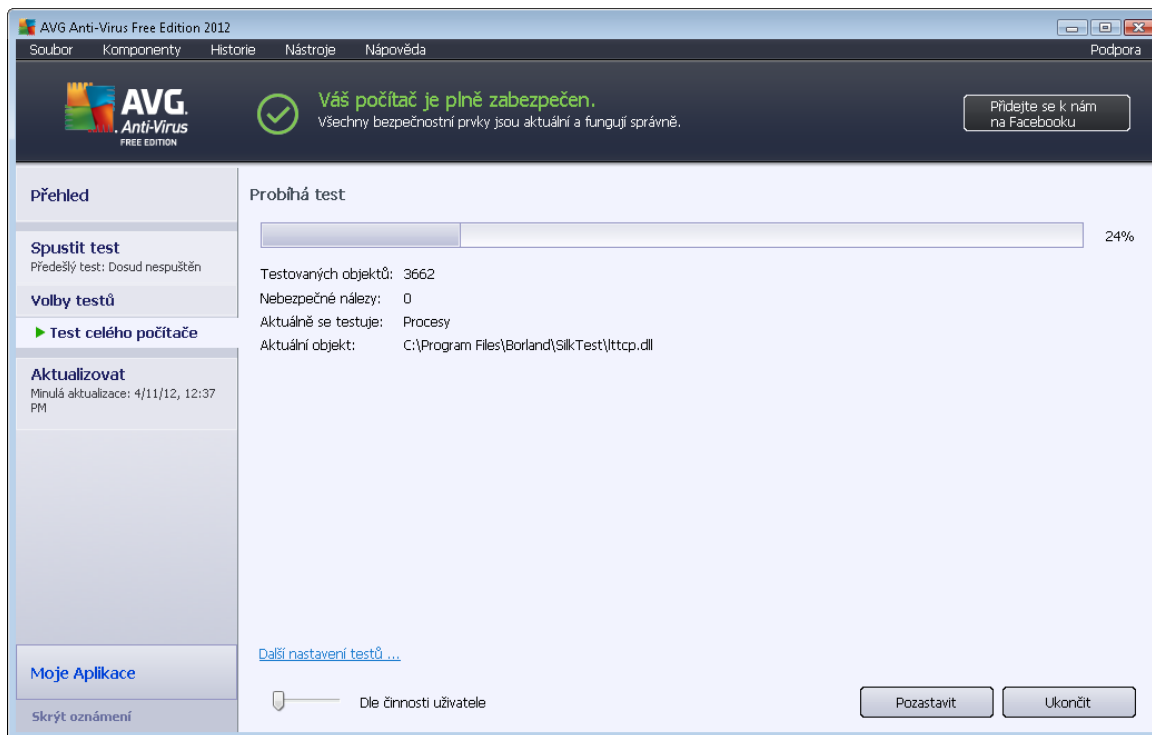
V **AVG Anti-Virus Free Edition 2012** najdete tyto typy výrobcem nastavených testů:

11.2.1. Test celého počítače

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

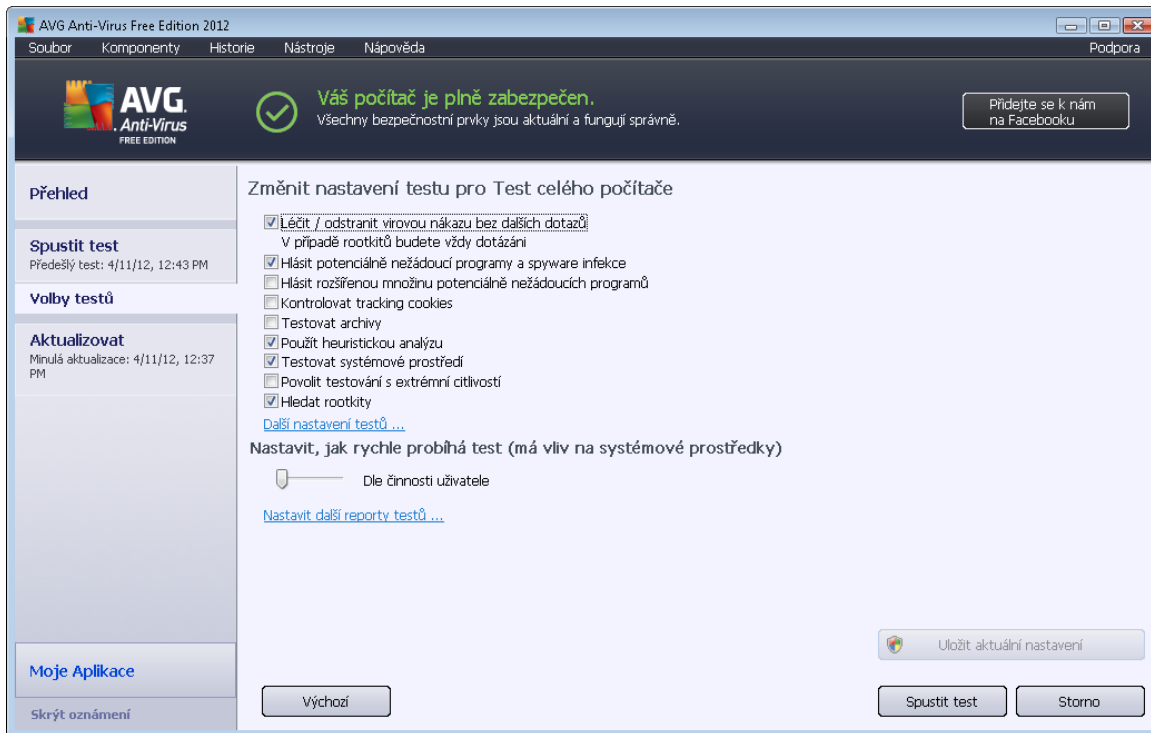
Spuštění testu

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



Editace nastavení testu

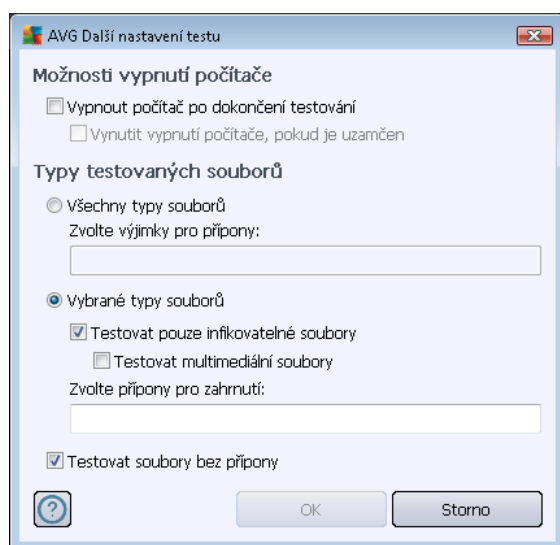
P edem definované výchozí nastavení **Testu celého počítače** máte možnost editovat v dialogu **Změnit nastavení testu pro Test celého počítače** (dostupného z [rozhraní pro testování](#) prostřednictvím odkazu **Změnit nastavení testu u Testu celého počítače**). **Pokud však nemáte skutečný důvod konfiguraci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



- **Parametry testu** - v seznamu parametrů testu můžete jednotlivé volby podle potřeby vypínat/zapínat:
 - **Léčit / odstranit virovou nákazu bez dalších dotazů** (ve výchozím nastavení zapnuto) - Je-li během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. Pokud virus automaticky léčit nelze, bude infikovaný objekt automaticky přesunut do [Virového trezoru](#).
 - **Hlásit potenciálně nežádoucí programy a spyware infekce** (ve výchozím nastavení zapnuto) - Kontrola přítomnosti [potenciálně nežádoucích programů](#) (spustitelné programy, které mohou fungovat jako spyware nebo adware). Zaškrtnutím tohoto políčka aktivujete [Anti-Spyware](#), tj. bude se testovat na přítomnost spyware, nejen virů. Spyware představuje poněkud problematickou kategorii malware, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány v domě a se souhlasem uživatele. Doporučujeme nicméně ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
 - **Hlásit rozšířenou množinu potenciálně nežádoucích programů** (ve výchozím nastavení vypnuto) - Zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v podobě od výrobce neškodné a v podobě, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.
 - **Kontrolovat tracking cookies** (ve výchozím nastavení vypnuto) - Parametr komponenty [Anti-Spyware](#) definuje, že během testu mají být detekovány cookies (

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

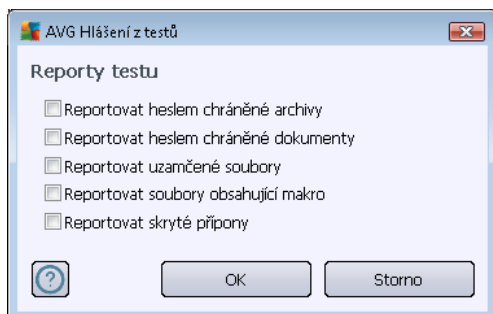
- **Testovat archivy** (ve výchozím nastavení vypnuto) - Parametr definuje, že test má kontrolovat všechny soubory zabalené v n kterém typu archivu, například ZIP, RAR, ...
 - **Použití heuristickou analýzu** (ve výchozím nastavení zapnuto) - B hem testu bude použita k detekci infekce i metoda heuristické analýzy (dynamické emulace instrukcí testovaného objektu v prostředí virtuálního počítače).
 - **Testovat systémové prostředí** (ve výchozím nastavení zapnuto) - Test provádí i systémové oblasti vašeho počítače.
 - **Povolit testování s extrémní citlivostí** (ve výchozím nastavení vypnuto) - Ve specifických situacích (například při podezření na infekci starším typem viru) můžete zvolit tuto metodu testování, která aktivuje nejdokladnější testovací algoritmy a velmi podrobně provádí naprosto všechny oblasti vašeho počítače. Můžete však na paměti, že tato metoda je časově velmi náročná.
 - **Hledat rootkity** (ve výchozím nastavení zapnuto) - Parametr komponenty [Anti-Rootkit](#) prohledává počítač na přítomnost rootkitů, tedy programů a technologií, které dokáží maskovat přítomnost malware v počítači. Dojde-li k nálezu rootkitu, nemusí to nutně znamenat, že je počítač infikovaný. V některých případech mohou být rootkity použity jako ovladače nebo části korektních aplikací.
- **Další nastavení testu** - odkaz otevírá dialog **Další nastavení testu**, kde můžete definovat následující parametry testu:



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

po jejímž potvrzení dojde po dokončení testu k vypnutí počítače a tedy, jestliže je počítač momentálně zamknut.

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



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



11.2.2. Test vybraných souborů či složek

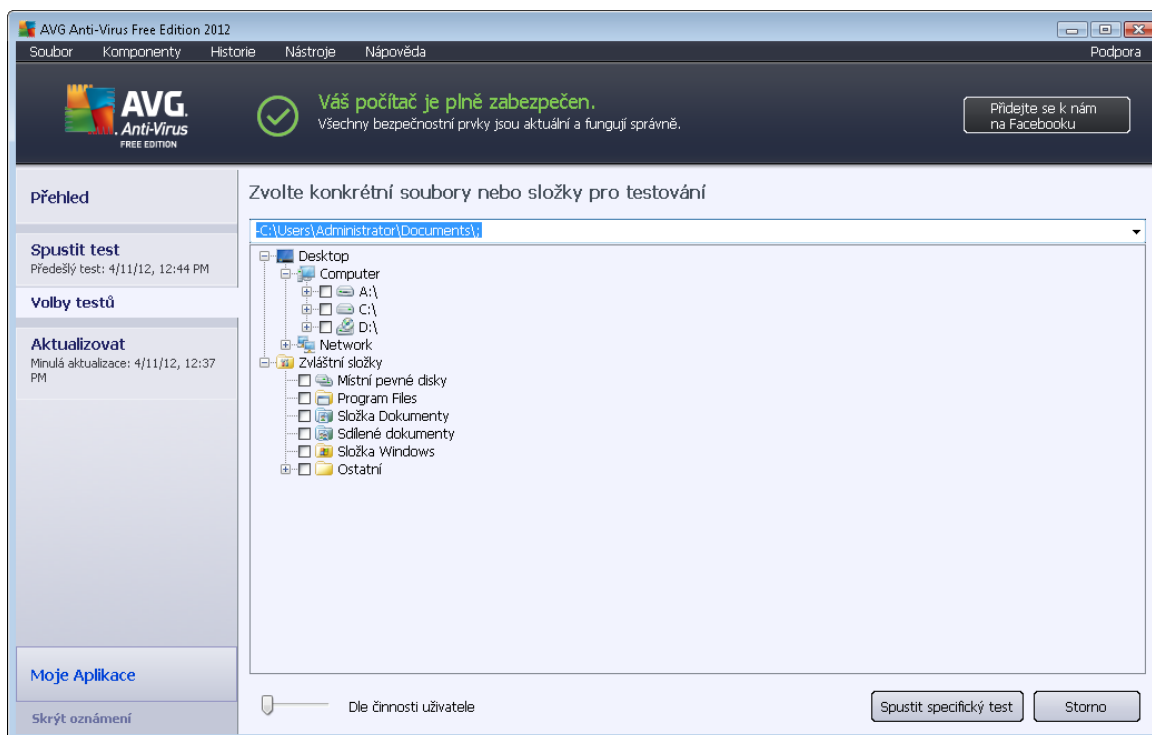
Test vybraných souborů i složek kontroluje pouze uživatelem definované oblasti počítače (zvolené složky, pevné disky, diskety, CD, optické disky, ...). Postup při nálezů a léčení / odstranění virových nákaz je stejný jako u **Testu celého počítače**: nalezené viry jsou vyléčeny nebo přesunuty do [Virového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

Spuštění testu

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

Pokud si přejete zkontrolovat určitou adresou bez kontroly všech v ní obsažených podadres, napište před automaticky vygenerovanou cestou k adresě znaménko "-". Parametrem "!" před cestou k adresě zase určíte, že celá adresa má být z testu vypuštěna.

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

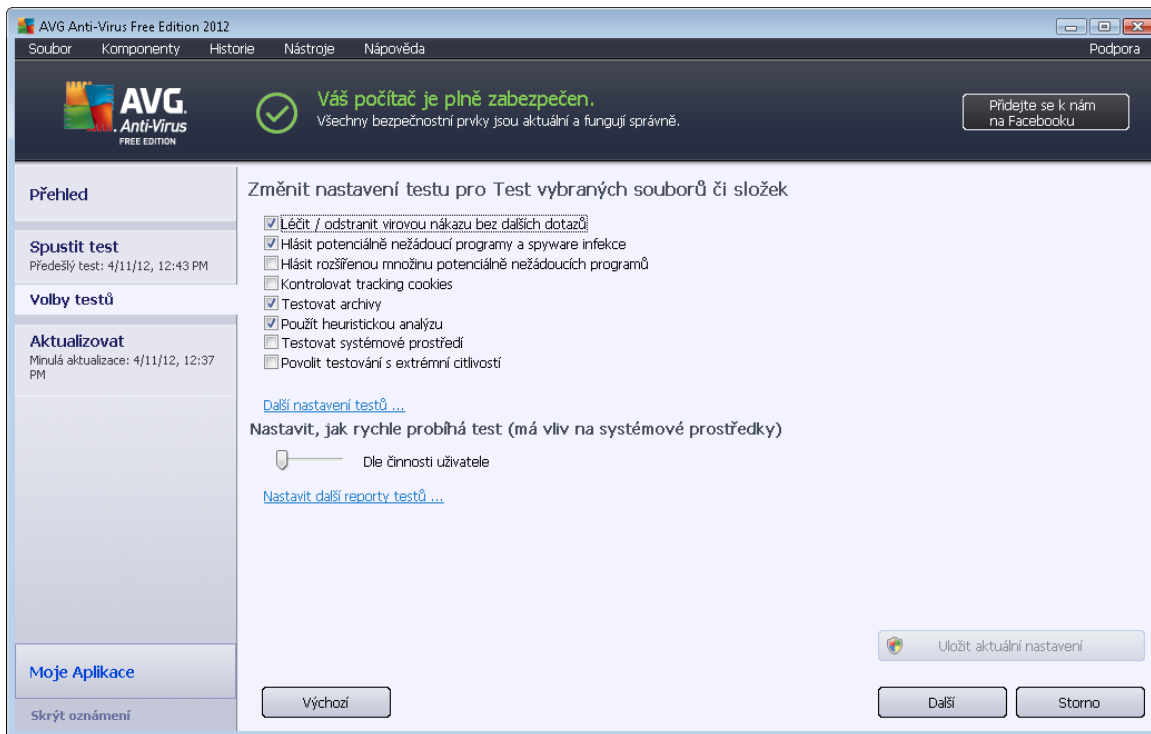


Editace nastavení testu

Předem definované výchozí nastavení **Testu vybraných souborů i složek** máte možnost editovat v



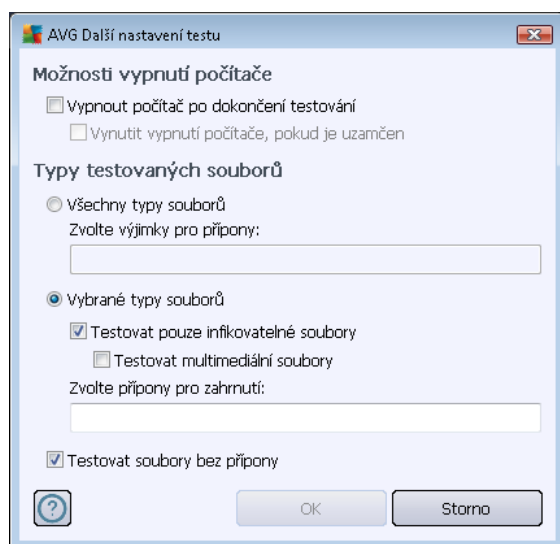
dialogu **Zm nit nastavení testu pro Test vybraných souborů i složek** (dostupného z [rozhraní pro testování](#) prost ednictvím odkazu **Zm nit nastavení testu u Testu vybraných souborů a složek**). **Pokud však nemáte skute ný d vod konfiguraci testu m nit, doporu ujeme se podržet výrobce definovaného nastavení!**



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

nícmén m že blokovat také n které legální programy, proto je ve výchozím nastavení tato možnost vypnuta.

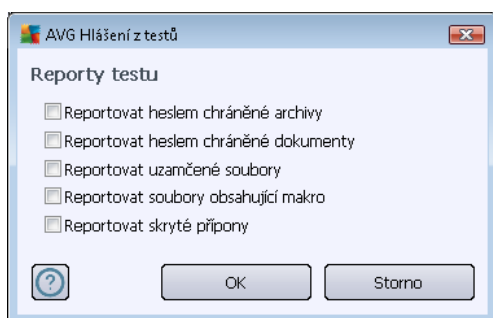
- **Kontrolovat tracking cookies** (ve výchozím nastavení vypnuto) - parametr komponenty [Anti-Spyware](#) definuje, že b hem testu mají být detekovány cookies (*HTTP data zaslaná serverem prohlíže í a uložena na po íta í uživatele; p í každé další návště v téhož serveru prohlíže posílá cookies zp t serveru, který podle nich rozlišuje jednotlivé uživatele*).
 - **Testovat archivy** (ve výchozím nastavení zapnuto) - parametr definuje, že test má kontrolovat všechny soubory zabalené v n kterém typu archivu, nap íklad ZIP, RAR, ...
 - **Použít heuristickou analýzu** (ve výchozím nastavení zapnuto) - b hem testu bude použita k detekci infekce í metoda heuristické analýzy (*dynamické emulace instrukcí testovaného objektu v prost edí virtuálního po íta e*).
 - **Testovat systémové prost edí** (ve výchozím nastavení vypnuto) - test prov í i systémové oblasti vašeho po íta e.
 - **Povolit testování s extrémní citlivostí** (ve výchozím nastavení vypnuto) - ve specifických situacích (*p í podez ení na infekci zavle enou do vašeho po íta e*) m žete zvolit tuto metodu testování, která aktivuje nejd kladn ěší testovací algoritmy a velmi podrobn ě prov í naprosto všechny oblasti vašeho po íta e. M ěte však na pam ěti, že tato metoda je asov ě velmi náro ná.
- **Další nastavení testu** - odkaz otevírá dialog **Další nastavení testu**, kde m žete definovat následující parametry testu:



- **Možnosti vypnutí po íta e** - ur ete, zda má být po íta po dokon ení testu automaticky vypnut. Pokud potvrdíte tuto možnost (**Vypnout po íta po dokon ení testování**), aktivuje se nová volba (**Vynutit vypnutí po íta e, pokud je uzam en**), p í jejímž potvrzení dojde po dokon ení testu k vypnutí po íta e í tehdy, jestliže je

pořít okamžitě zamknout.

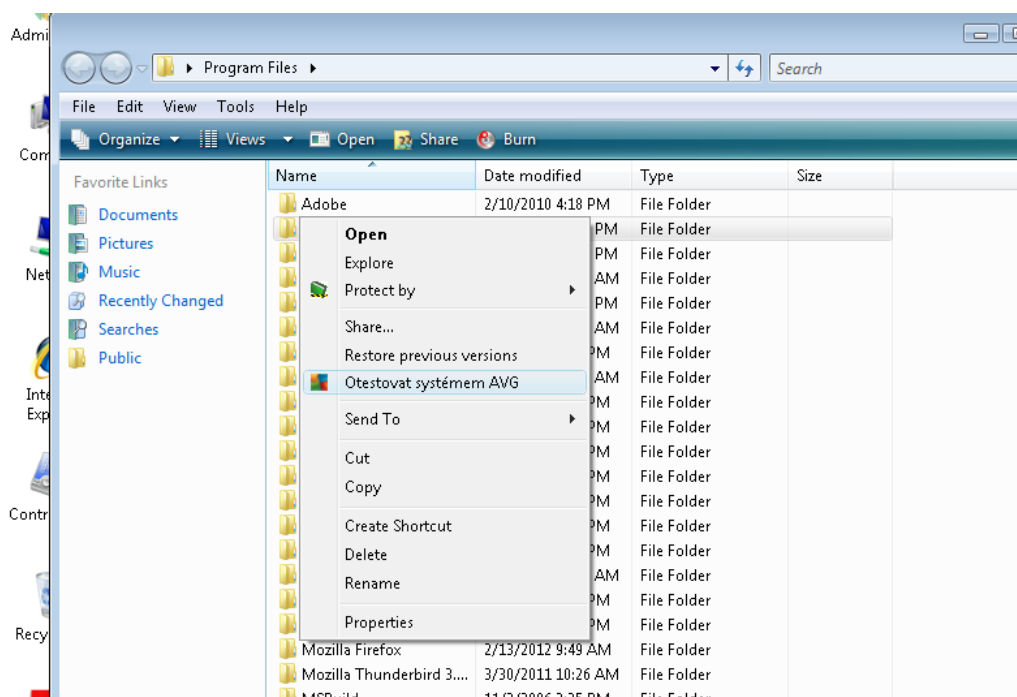
- o **Typy testovaných souborů** - dále se můžete rozhodnout, zda si přejete testovat
 - **Všechny typy souborů** - pokud vám umožňuje zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou;
 - **Vybrané typy souborů** - můžete se rozhodnout, že chcete, aby se testy 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 rozhodnete, zda se mají testovat i soubory se skrytou nebo neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme, abyste se tohoto nastavení podrželi, pokud nemáte skutečnou důvod jej změnit. Soubory bez přípon jsou obecně vysoce podezřelé a měly by být otestovány.
- **Priorita testu** - posuvníkem lze změnit prioritu testu. Ve výchozím nastavení je tato hodnota nastavena na úroveň **Dle inaktivnosti uživatele**, což znamená, že je využito minimum systémových prostředků ve chvíli, kdy se počítačem pracujete, a naopak maximum ve chvíli, kdy se počítačem nepracujete. Test můžete spustit pomaleji a tedy s nižší zátěží systémových zdrojů (*vhodné, pokud potěbuje během testu na počítači pracovat a nezáleží vám tolik na celkové době testování*) nebo naopak rychleji s vyššími nároky na systémové zdroje (*například v době, kdy na počítači nikdo nepracuje*).
- **Nastavit další reporty testů** - odkaz otevírá nový dialog **Reporty testů**, v němž můžete označit, které typy nálezů mají být hlášeny:



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

11.3. Testování v průzkumníku Windows

AVG Anti-Virus Free Edition 2012 nabízí kromě přednastavených testů spuštěných nad celým počítačem nebo jeho vybranými oblastmi i možnost rychlého otestování konkrétního objektu přímo v prostředí průzkumníka Windows. Chcete-li například otevřít neznámý soubor a nejste si jisti jeho obsahem, můžete nechat tento soubor na vyžádání otestovat. Postup je následující:



- V průzkumníku Windows označte soubor (*nebo adresář*), jehož obsah chcete prověřit
- Kliknutím pravého tlačítka myši nad objektem otevřete kontextové menu
- Volbou položky **Otestovat systémem AVG** - nechte objekt otestovat programem **AVG Anti-Virus Free Edition 2012**

11.4. Testování z příkazové řádky

V rámci AVG Anti-Virus Free Edition 2012 existuje také možnost spustit test z příkazové řádky. Tuto možnost využijete například na serverech nebo třeba při vytváření dávkových skriptů, které mají být spuštěny po startu počítače. Z příkazové řádky můžete spustit test s nastavením v řadě parametrů, které jsou dostupné v grafickém rozhraní AVG.

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

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



Syntaxe p íkazu

Syntaxe p íkazu pro spušt ní testu z p íkazové ádky je následující:

- **avgscanx /parametr** ... tedy nap íklad **avgscanx /comp** pro spušt ní testu celého po íta e
- **avgscanx /parametr /parametr** .. p í použití více parametr jsou tyto uvedeny za sebou a odd leny mezerou a lomítkem
- pokud parametr vyžaduje uvedení konkrétní hodnoty (nap íklad parametr **/scan** pro otestování vybraných oblastí po íta e, kde musíte uvést cestu k testované oblasti), jsou jednotlivé hodnoty od sebe odd leny st edníkem, nap íklad: **avgscanx /scan=C:\;D:**

Parametry p íkazu

Kompletní p ehled použitelných parametr lze zobrazit p íkazem pro p íslušný test s parametrem **/?** nebo **/HELP** (nap . **avgscanx /?**). Jediným povinným parametrem testu je **/SCAN**, p íp. **/COMP**, kterými ur íte oblasti po íta e, jež se mají testovat. Podrobný popis dostupných parametr najdete v kapitole [Parametry CMD testu](#).

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

Spušt ní CMD testu z grafického rozhraní

P í spušt ní po íta e v nouzovém režimu Windows je dostupná i možnost spušt ní testu z p íkazové ádky prost ednictvím dialogu grafického rozhraní. Samotný text bude spušt n z p íkazové ádky; dialog **Nastavení testu z p íkazové ádky** slouží pouze jako nástroj pro snadné nastavení parametr testu, aniž byste je museli definovat v prost edí p íkazové ádky.

Vzhledem k tomu, že dialog není standardn dostupný a bude zobrazen pouze v nouzovém režimu Windows, jeho podrobný popis najdete v nápov d dostupné p ímo z tohoto dialogu.

11.4.1. Parametry CMD testu

V následujícím p ehledu nabízíme seznam dostupných parametr testu:

- **/SCAN** [Test vybraných souborů i složek](#); **/SCAN=path;path** (nap íklad **/SCAN=C:\;D:**)
- **/COMP** [Test celého po íta e](#)
- **/HEUR** Použít [heuristickou analýzu](#)
- **/EXCLUDE** Z testu vynechat tuto cestu nebo soubory
- **/@** P íkazový soubor /jméno souboru/



- **/EXT**
DLL/ Testovat pouze soubory s těmito příponami /například EXT=EXE,
- **/NOEXT** Netestovat soubory s těmito příponami /například NOEXT=JPG/
- **/ARC** Testovat archívy
- **/CLEAN** Automaticky léčit
- **/TRASH** Přesunout infikované soubory do [Virového trezoru](#)
- **/QT** Rychlý test
- **/MACROW** Hlásit makra
- **/PWDW** Hlásit heslem chráněné soubory
- **/IGNLOCKED** Ignorovat zamčené soubory
- **/REPORT** Hlásit do souboru /jméno souboru/
- **/REPAPPEND** Přidat k souboru
- **/REPOK** Hlásit neinfikované soubory jako OK
- **/NOBREAK** Nepovolit přerušení testu pomocí CTRL-BREAK
- **/BOOT** Povolit kontrolu MBR/BOOT
- **/PROC** Testovat aktivní procesy
- **/PUP** Hlásit "[Potenciálně nebezpečné programy](#)"
- **/REG** Testovat registry
- **/COO** Testovat cookies
- **/?** Zobrazit nápovědu k tomuto tématu
- **/HELP** Zobrazit nápovědu k tomuto tématu
- **/PRIORITY**
[Testy](#)) Nastavit prioritu testu /Low, Auto, High/ (viz [Pokročilé nastavení /](#)
- **/SHUTDOWN** Vypnout počítač po dokončení testu
- **/FORCESHUTDOWN** Vynutit vypnutí počítače po dokončení testu
- **/ADS** Testovat alternativní datové proudy (pouze NTFS)
- **/ARCBOMBSW** Hlásit opakovaně komprimované archivní soubory

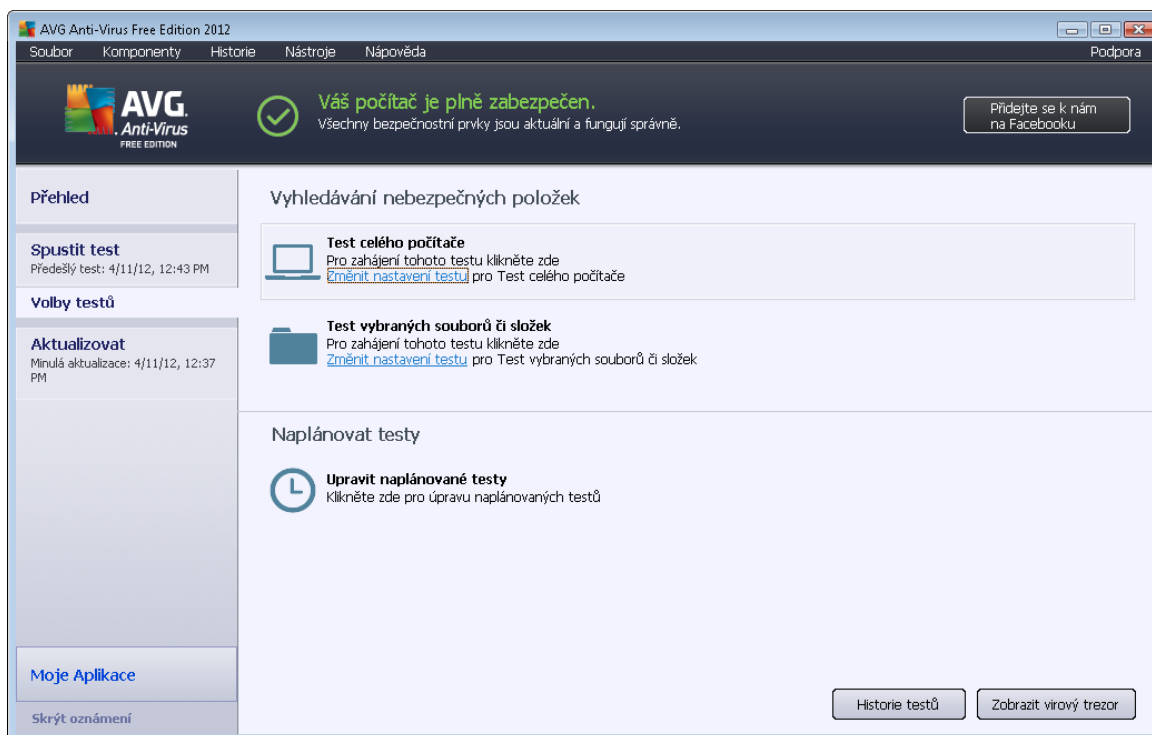


11.5. Naplánování testu

Testy v **AVG Anti-Virus Free Edition 2012** lze spouštět buďto na vyžádání (*například v situaci, kdy máte podezření na zavlečení infekce na váš počítač nebo z jiného důvodu*) anebo podle nastaveného plánu. Doporučujeme používat především spouštění testů podle plánu, protože tímto způsobem zajistíte svému počítači dostatečnou prevenci a budete moci pracovat bez starostí o to, zda a kdy test spustit.

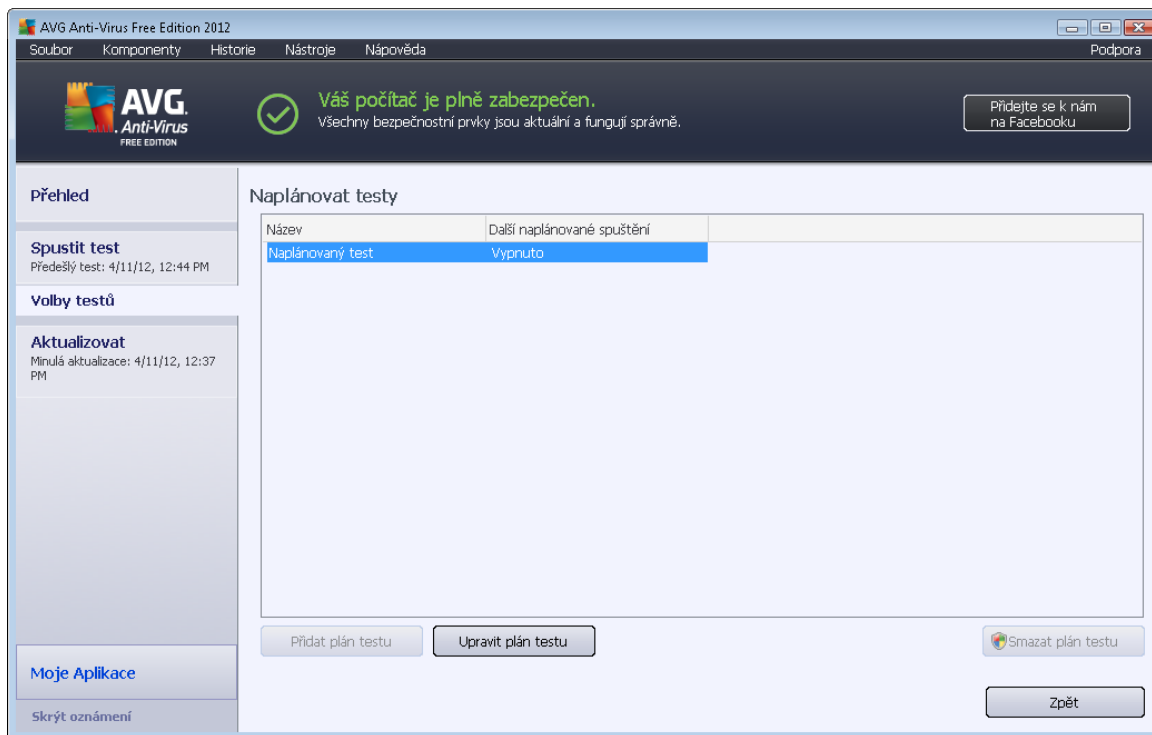
[Test celého počítače](#) by měl být spouštěn pravidelně, a to nejméně jednou týdně. Pokud vám to však provoz na vašem počítači umožní, doporučujeme spouštět test celého počítače jednou denně; tak je také ve výchozí konfiguraci nastaven plán testů. Jestliže je počítač trvale zapnutý, je vhodné naplánovat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

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



Naplánovat testy

Kliknutím na grafickou ikonu v sekci **Naplánovat testy** otevřete nový dialog **Naplánovat testy**, v němž najdete přehled všech aktuálně naplánovaných testů.

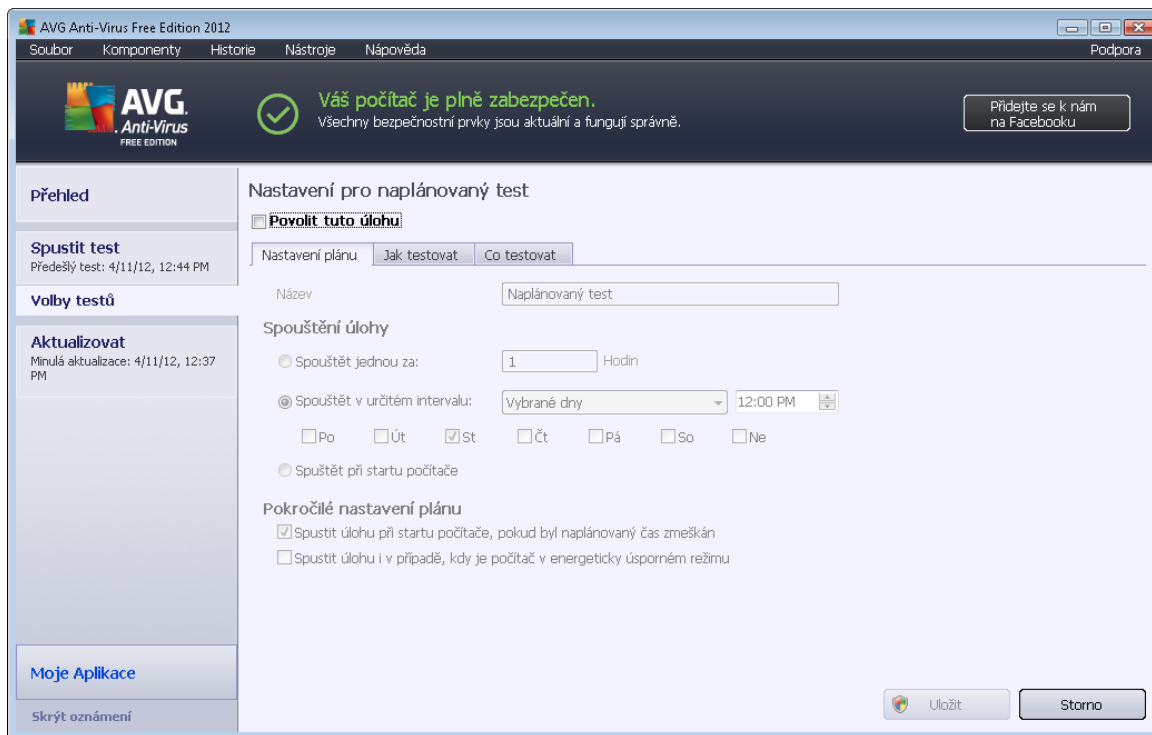


Pracovat můžete s těmito ovládacími tlačítky:

- **Přidat plán testu** - v **AVG Anti-Virus Free Edition 2012** je toto tlačítko deaktivováno. Plánování uživatelských testů je dostupné pouze v profesionálních edicích AVG!
- **Upravit plán testu** - tlačítko může být použito pouze v případě, že jste ze seznamu naplánovaných testů vybrali již existující test. V takovém případě se tlačítko zobrazí jako aktivní a kliknutím na něj se přepnete do dialogu **Nastavení pro naplánovaný test**, na záložku [Nastavení plánu](#). Zde jsou již zadány parametry stávajícího testu, které můžete editovat.
- **Smazat plán testu** - tlačítko je rovněž aktivní pouze v případě, že jste ze seznamu naplánovaných testů vybrali již existující test. ten pak můžete stiskem tlačítka zrušit. Odebírat však můžete jen své vlastní nastavené plány; **Plán testu celého počítače**, který je nastaven jako výchozí, smazat nelze.
- **Zpět** - návrat do [testovacího rozhraní AVG](#)

11.5.1. Nastavení plánu

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



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

Položka **Název** je v **AVG Anti-Virus Free Edition 2012** předem nastavena a jméno testu nelze změnit. Editace názvu testu je možná pouze u vlastních uživatelských testů, které je však dostupné výhradně v profesionálních edicích AVG.

V tomto dialogu můžete dále definovat tyto parametry testu:

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

Ovládací tlačítka dialogu

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

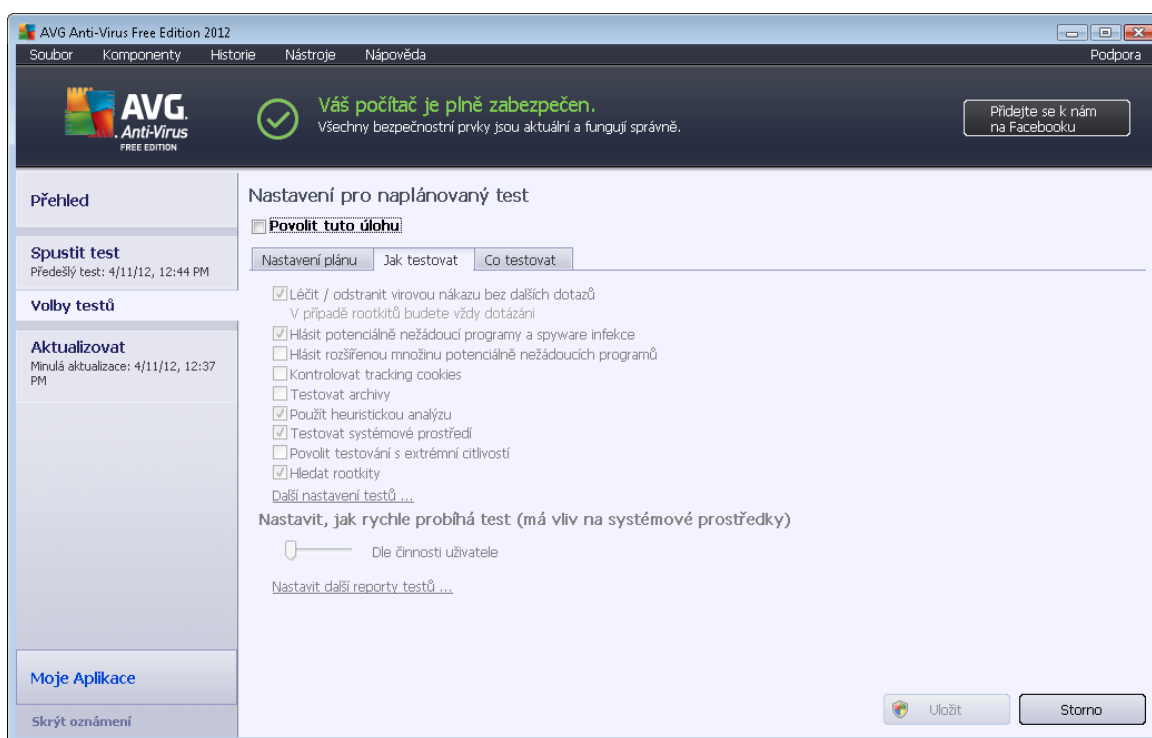
- **Uložit** - uloží všechny změny, které jste provedli na této záložce nebo na libovolné jiné



záložce dialogu pro nastavení plánu testu a p epe vás zp t do [výchozího dialogu testovacího rozhraní AVG](#). Chcete-li tedy nastavit parametry plánu testu na všech záložkách, uložte je stiskem tohoto tlačítka teprve poté, co jste zadali všechny své požadavky.

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

11.5.2. Jak testovat



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

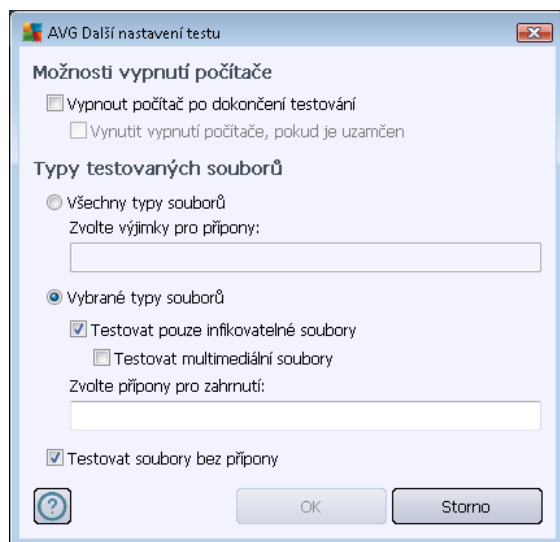
- **Léčit / odstranit virovou nákazu bez dalších dotazů** - (ve výchozím nastavení zapnuto): je-li během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. Pokud virus automaticky léčit nelze, anebo pokud se rozhodnete tuto funkci vypnout, budete o nálezů viru vyrozuměni a můžete rozhodnout, co se má dále s infikovaným objektem provést. Doporučeným postupem je přesunutí objektu do [Virového trezoru](#).
- **Hlásit potenciálně nežádoucí programy a spyware infekce** - (ve výchozím nastavení zapnuto) kontrola přítomnosti [potenciálně nežádoucích programů](#) (spustitelné programy, které mohou fungovat jako spyware nebo adware). Zaškrtnutím tohoto políčka aktivujete [Anti-Spyware](#), tj. bude se testovat přítomnost spyware, nejen virů. Spyware představuje poněkud problematickou kategorii malware, protože i když většina těchto programů

představuje bezpečnostní riziko, jsou mnohdy instalovány v domě a se souhlasem uživatele. Doporuujeme nicméně ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.

- **Hlásit rozšířenou množinu potenciálně nežádoucích programů** - (ve výchozím nastavení vypnuto): zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.
- **Kontrolovat tracking cookies** - (ve výchozím nastavení vypnuto): parametr komponenty [Anti-Spyware](#) definuje, že během testu mají být detekovány cookies (*HTTP data zaslaná serverem prohlížeči a uložena na počítači uživatele; při každé další návštěvě téhož serveru prohlížeč posílá cookies zpět serveru, který podle nich rozlišuje jednotlivé uživatele*).
- **Testovat archivy** - (ve výchozím nastavení vypnuto): parametr definuje, že test má kontrolovat všechny soubory, a to i takové, které jsou zabaleny v některém typu archivu, například ZIP, RAR, ...
- **Použít heuristickou analýzu** - (ve výchozím nastavení zapnuto): během testu bude použita k detekci infekce i metoda heuristické analýzy (*dynamické emulace instrukcí testovaného objektu v prostředí virtuálního počítače*).
- **Testovat systémové prostředí** - (ve výchozím nastavení zapnuto): test prověří i systémové oblasti vašeho počítače.
- **Povolit testování s extrémní citlivostí** (ve výchozím nastavení vypnuto) - ve specifických situacích (*při podezření na infekci ve vašem počítači*) můžete zvolit tuto metodu testování, která aktivuje nejdokladnější testovací algoritmy a velmi podrobně prověří naprosto všechny oblasti vašeho počítače. Mějte však na paměti, že tato metoda je srovnatelně 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 nálezům rootkitu, nemusí to nutně znamenat, že je počítač infikovaný. V některých případech mohou být rootkity použity jako ovladače nebo části korektních aplikací.

Dále máte možnost upravit konfiguraci testu tímto nastavením:

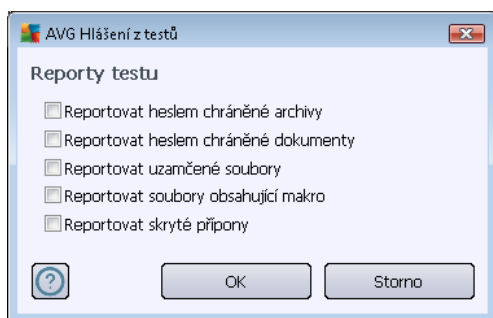
- **Další nastavení testu** - odkaz otevírá dialog **Další nastavení testu**, kde můžete definovat následující parametry testu:



- **Možnosti vypnutí počítače** - určete, zda má být počítač po dokončení testu automaticky vypnut. Pokud potvrdíte tuto možnost (**Vypnout počítač po dokončení testování**), aktivuje se nová volba (**Vynutit vypnutí počítače, pokud je uzamčen**), při jejímž potvrzení dojde po dokončení testu k vypnutí počítače a tehdy, jestliže je počítač momentálně zamknut.
- **Typy testovaných souborů** - dále se můžete rozhodnout, zda si přejete testovat
 - **Všechny typy souborů** - pokud máte zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou;
 - **Vybrané typy souborů** - můžete se rozhodnout, že chcete, aby se testy spouštěly pouze nad soubory, které lze považovat za infikovatelné (*soubory, které nemohou být infekcí zasaženy, se testovat nebudou - například prosté textové soubory nebo některé nespustitelné soubory*), a to včetně multimediálních souborů (*video, audio soubory - ponecháte-li tuto položku neoznají, výrazně se tím zkrátí čas testování, jelikož multimediální soubory jsou obvykle poměrně velké, ale pravděpodobnost infekce je u nich velmi nízká*). I zde můžete určit výjimky a pomocí seznamu přípon definovat, které soubory mají být testovány za všech okolností.
 - U položky **Testovat soubory bez přípon** pak rozhodnete, zda se mají testovat i soubory se skrytou nebo neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme, abyste se tohoto nastavení drželi, pokud nemáte skutečně důvod jej změnit. Soubory bez přípon jsou obecně vysoce podezřelé a měly by být otestovány.
- **Nastavit, jak rychle probíhá test** - posuvníkem lze změnit prioritu testu. Ve výchozím nastavení je tato hodnota nastavena na úroveň **Dle inosti uživatele**, což znamená, že je využito minimum systémových prostředků ve chvíli, kdy s počítačem pracujete, a naopak maximum ve chvíli, kdy s počítačem nepracujete. Test můžete spustit pomaleji a tedy s nižší zátěží systémových zdrojů (*vhodné, pokud potřebujete během testu na počítači pracovat a nezáleží vám tolik na celkové době testování*) nebo naopak rychleji s vyššími

nároky na systémové zdroje (*například v době, kdy na počítači nikdo nepracuje*).

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

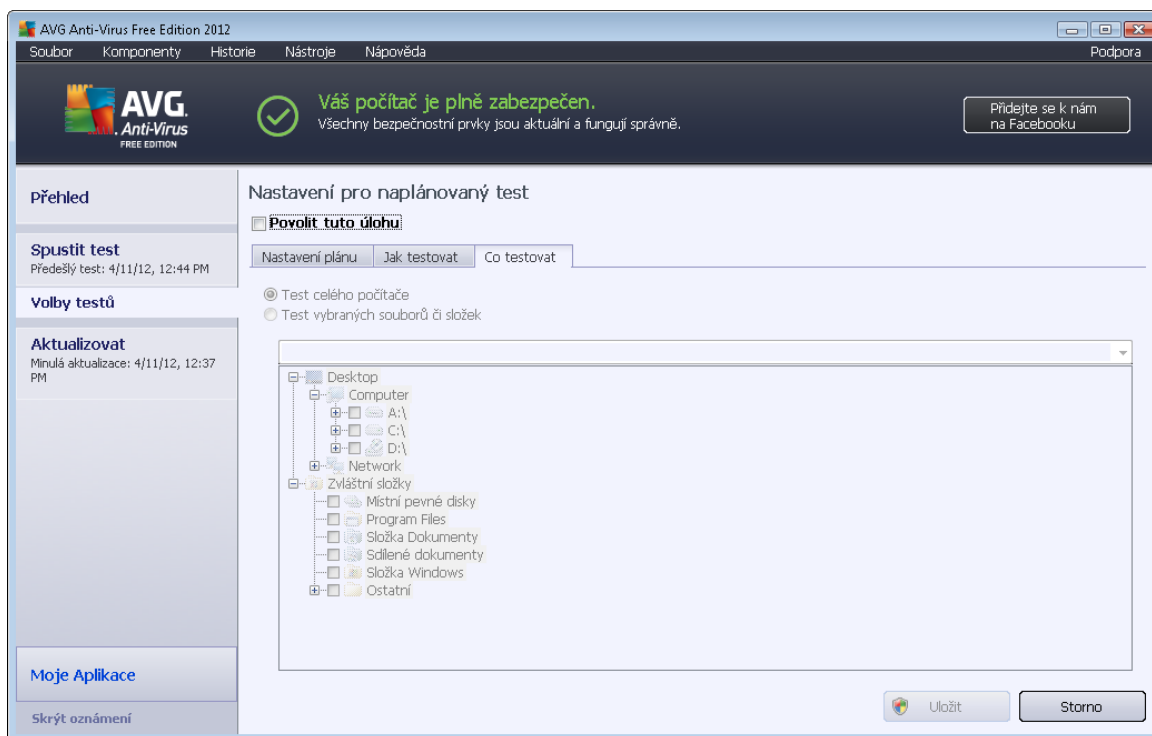


Ovládací tlačítka dialogu

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

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

11.5.3. Co testovat



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

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

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

- **Místní pevné disky** - všechny pevné disky počítače
- **Program files**
 - C:\Program Files\
 - v 64-bitové verzi C:\Program Files (x86)
- **Složka Dokumenty**



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

- **Sdílené dokumenty**

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

- **Složka Windows** - C:\Windows\

- **Ostatní**

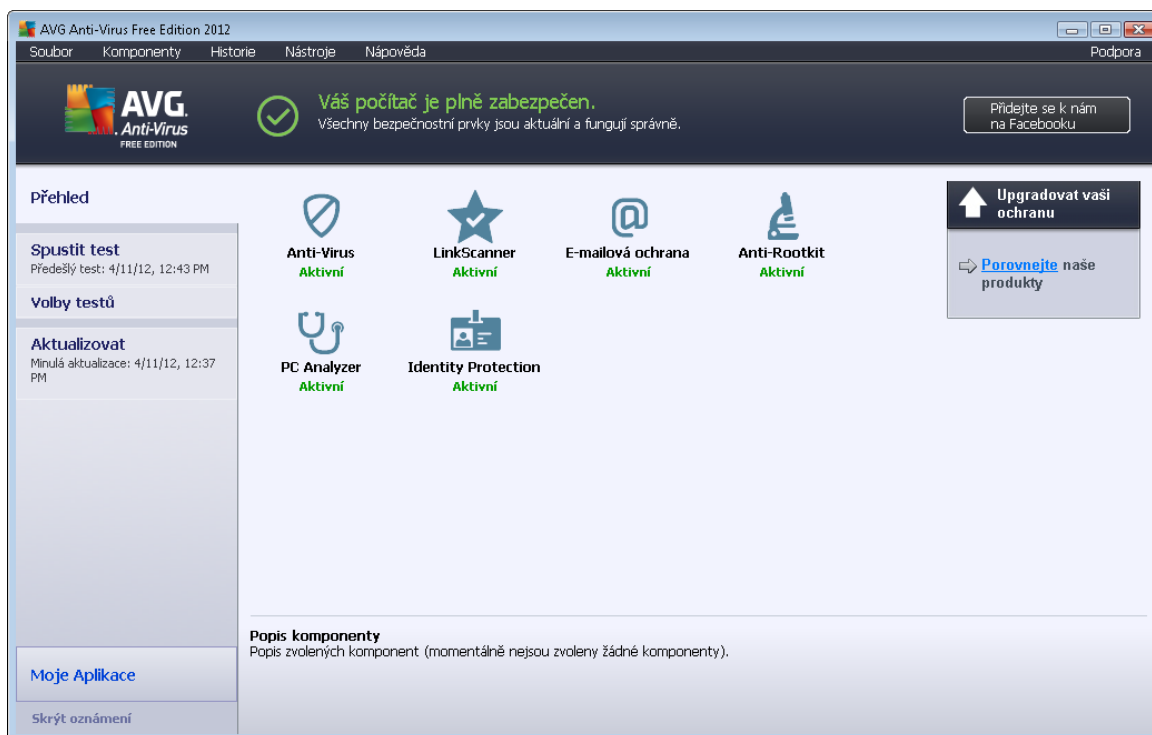
- o Systémový disk - pevný disk, na němž je instalován operační systém (*obvykle C:*)
- o Systémová složka - C:\Windows\System32\
- o Složka dočasné soubory - C:\Documents and Settings\User\Local\ (*Windows XP*) nebo C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)
- o Temporary Internet Files -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

Ovládací tlačítka dialogu

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


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


11.6. Přehled výsledků testů




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

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

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

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

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

Ve všech případech může být ikona buďto celistvá nebo poloplená - celá ikona značí, že test probíhal celý a byl úspěšně ukončen, poloplená ikona identifikuje nedokončený nebo přerušený test.

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

- **časová značka** - datum a přesný čas spuštění testu



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

Ovládací tlačítka dialogu

Ovládací tlačítka pro dialog **Přehled výsledků testu** jsou:

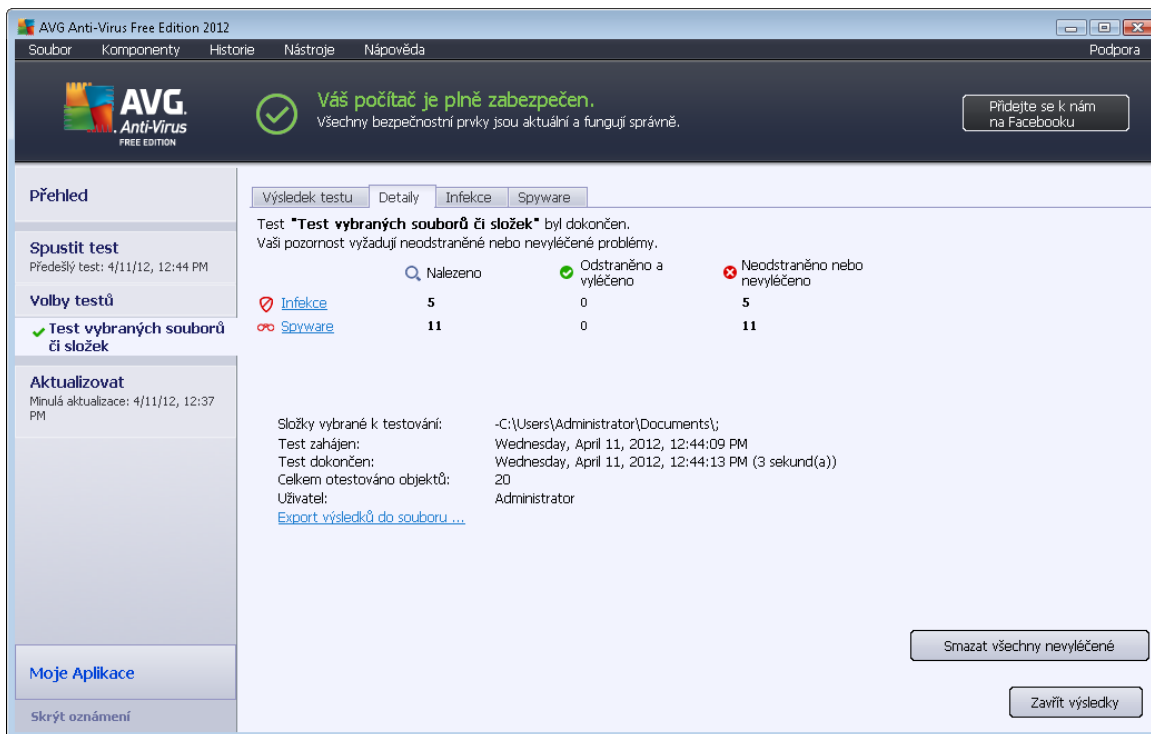
- **Podrobnosti** - stiskem tlačítka pak přejdete do dialogu [Výsledky testu](#), kde se zobrazí podrobné informace o testu zvoleném v přehledu
- **Smazat výsledek** - stiskem tlačítka můžete záznam o zvoleném testu v přehledu testů odstranit
- **Zpět** - přepíná zpět do výchozího dialogu [testovacího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

11.7. Detail výsledku testu

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

- [Detaily](#) - záložka se zobrazuje vždy a nabízí statistická data popisující průběh testu
- [Infekce](#) - záložka se zobrazuje podmíněně tehdy, když byla během testu detekována virová infekce
- [Spyware](#) - záložka se zobrazuje podmíněně tehdy, když byl během testu detekován spyware
- [Varování](#) - záložka se zobrazuje podmíněně s upozorněním na výskyt cookies
- [Rootkity](#) - záložka se zobrazuje podmíněně tehdy, když byl během testu detekován rootkit
- [Informace](#) - záložka se zobrazuje podmíněně a zobrazuje informace (typicky varovná upozornění) o nálezích, které mohou být potenciálně nebezpečné, ale nelze je klasifikovat jako konkrétní typ infekce. Rovněž se zde zobrazí případně nalezené objekty, které nemohly být otestovány (například zaheslované archivy).

11.7.1. Záložka Detaily



AVG Anti-Virus Free Edition 2012

Soubor Komponenty Historie Nástroje Nápověda Podpora

AVG Anti-Virus FREE EDITION

Váš počítač je plně zabezpečen.
Všechny bezpečnostní prvky jsou aktuální a fungují správně.

Přidejte se k nám na Facebooku

Přehled

Spustit test
Předošlý test: 4/11/12, 12:44 PM

Volby testů

Test vybraných souborů či složek

Aktualizovat
Minulá aktualizace: 4/11/12, 12:37 PM

Moje Aplikace
Skrýt oznámení

Výsledek testu **Detaily** Infekce Spyware

Test "**Test vybraných souborů či složek**" byl dokončen.
Vaši pozornost vyžadují neodstraněné nebo nevyřešené problémy.

	Nalezeno	Odstraněno a vyřešeno	Neodstraněno nebo nevyřešeno
Infekce	5	0	5
Spyware	11	0	11

Složky vybrány k testování: -C:\Users\Administrator\Documents\;
 Test zahájen: Wednesday, April 11, 2012, 12:44:09 PM
 Test dokončen: Wednesday, April 11, 2012, 12:44:13 PM (3 sekund(a))
 Celkem otestováno objektů: 20
 Uživatel: Administrator
[Export výsledků do souboru ...](#)

Smazat všechny nevyřešené

Zavřít výsledky

Na záložce **Detaily** najdete podrobnou statistiku testu s informacemi o:

- detekovaných virových infekcích / spyware
- vylé ených virových infekcích / spyware
- po tu virových infekcí / spyware, které se nepoda ilo odstranit nebo vylé it

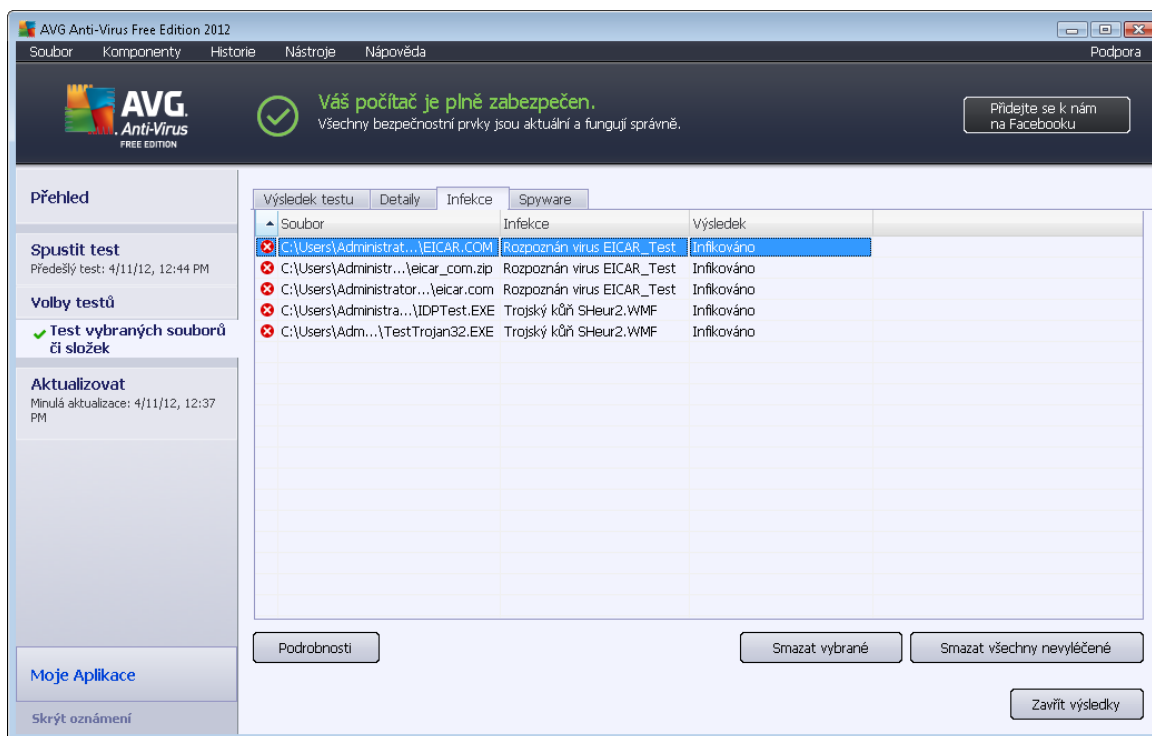
Dále jsou uvedeny informace o datu a ase spušt ní testu, celkovém po tu otestovaných objekt , o dob trvání testu a po tu chyb, k nimž b hem testu došlo.

Ovládací tla ítka dialogu

V dialogu jsou dostupná tato ovládací tla ítka:

- **Smazat všechny nevyře ené** - tímto tla ítkem m žete okamžit smazat všechny detekované infekce, jež se nepoda ilo vylé it.
- **Zav řít výsledky** - kliknutím se vrátíte do dialogu [P ehled výsledk test](#) .

11.7.2. Záložka Infekce



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

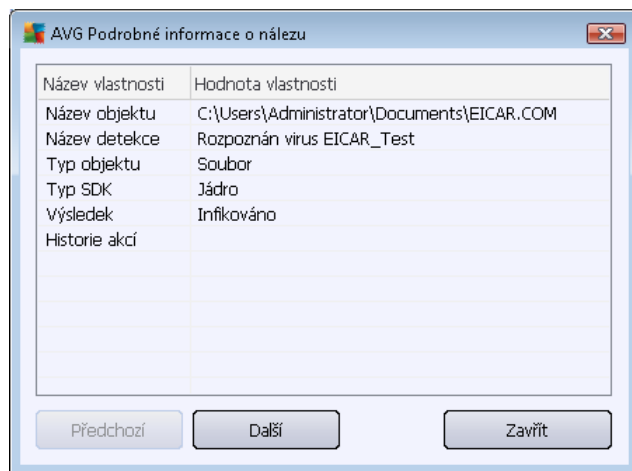
- **Soubor** - plná adresa povodního umístění infikovaného objektu na lokálním disku
- **Infekce** - jméno detekovaného viru (*podrobnosti o jednotlivých virech najdete ve [Virové encyklopedii](#)*)
- **Výsledek** - uvádí, v jakém stavu se infikovaný a z testu detekovaný objekt aktuálně nachází:
 - **Infikováno** - infikovaný objekt byl rozpoznán a zůstává ve svém povodním umístění (například pokud máte v nastavení konkrétního testu [vypnutou možnost automatického léčení](#))
 - **Vyléno** - infikovaný objekt byl automaticky vyléno a ponechán ve svém povodním umístění
 - **Pesunuto do trezoru** - infikovaný objekt byl přesunut do bezpečného prostoru [Virového trezoru](#)
 - **Smazáno** - infikovaný objekt byl smazán
 - **Obnoveno** - objekt byl obnoven z [Virového trezoru](#) zpět do povodního umístění

- **P idáno k výjimkám PUP** - nález byl vyhodnocen jako výjimka a připojen k seznamu výjimek PUP (*výjimky lze editovat v dialogu [PUP výjimky](#) pokračování nastavení*)
- **Zam ený soubor - neotestován** - objekt je zam ený a nebylo možno jej otestovat
- **Potenciálně nebezpečný objekt** - objekt je detekován jako potenciálně nebezpečný, ale nikoli infikovaný (*možná obsahuje makra*). Informace má tedy pouze charakter upozornění.
- **Pro dokončení akce je třeba provést restart** - infikovaný objekt nebylo možno odstranit, pro jeho odstranění je třeba provést restart počítače

Ovládací tlačítka dialogu

V dialogu jsou dostupná tato tlačítka:

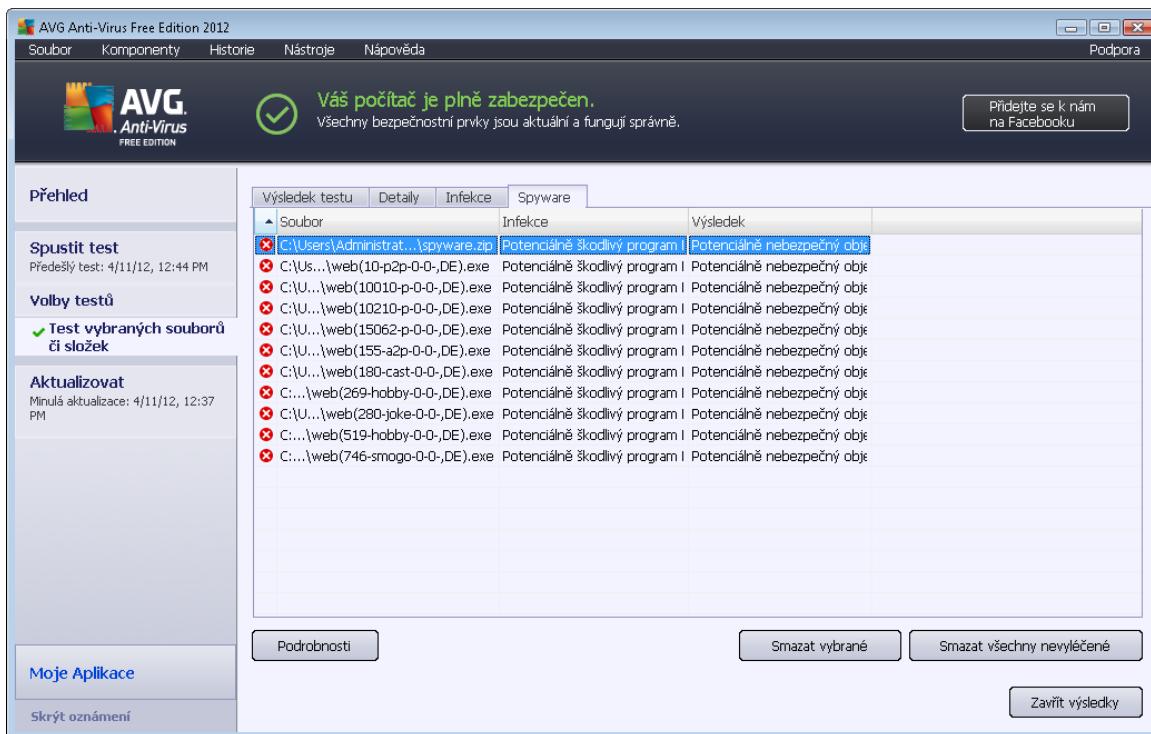
- **Podrobnosti** - tlačítko otevírá nové dialogové okno **Podrobné informace o nález:**



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

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

11.7.3. Záložka Spyware



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

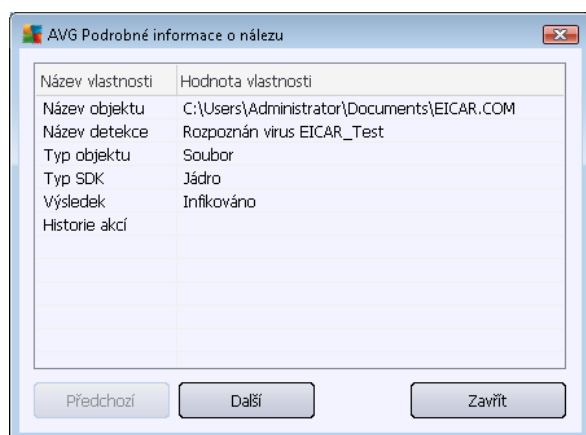
- **Soubor** - plná adresa povodního umístění infikovaného objektu na lokálním disku
- **Infekce** - jméno detekovaného spyware (*podrobnosti o jednotlivých virech najdete ve [Virové encyklopedii online](#)*)
- **Výsledek** - uvádí, v jakém stavu se infikovaný a během testu detekovaný objekt aktuálně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

- **P idáno k výjimkám PUP** - nález byl vyhodnocen jako výjimka a připojen k seznamu výjimek PUP (*výjimky lze editovat v dialogu [PUP výjimky](#) pokračování nastavení*)
- **Zam ený soubor** - neotestován - objekt je zam ený a nebylo možno jej otestovat
- **Potenciáln nebezpečný objekt** - objekt je detekován jako potenciálně nebezpečný, ale nikoli infikovaný (*m že například obsahovat makra*). Informace má tedy pouze charakter upozorn ění.
- **Pro dokon ení akce je potřeba provést restart** - infikovaný objekt nebylo možno odstranit, pro jeho odstran ění je třeba provést restart počítače

Ovládací tlačítka dialogu

V dialogu jsou dostupná tato tlačítka:

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



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

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



11.7.4. Záložka Varování

Záložka **Varování** zobrazuje informace o "podezřelých" objektech (*nejastji souborech*) detekovaných během testu. Při kontrole Rezydentním štítem je k tomuto typu objektů zakázán přístup. Příkladem mohou být skryté soubory, soubory cookies, podezřelé registrové klíče, heslem chráněné dokumenty či archivy, maskovací jména atd. Takovéto soubory nepředstavují přímou hrozbu pro Vaše počítače nebo bezpečnost, ale informace o nich mohou být užitečné například při odware nebo spyware infekce. Pokud ve výsledku testu zobrazuje **AVG Anti-Virus Free Edition 2012** pouze varování, není třeba provádět žádnou akci.

Nabízíme stručný popis nejčastějších takto detekovaných objektů:

- **Skryté soubory** nejsou ve výchozím nastavení Windows viditelné. Některé viry nebo jiné hrozby se mohou vyhýbat svému odhalení právě použitím tohoto atributu pro své soubory. Pokud **AVG Anti-Virus Free Edition 2012** reportuje skrytý soubor a vy máte podezření že je infikován, můžete jej přesunout do [Virového trezoru](#).
- **Cookies** jsou textové soubory používané internetovými stránkami k ukládání uživatelských informací. Ty mohou být využívány pro volbu vlastního vzhledu stránek, vyplnění uživatelského jména, atd.
- **Podezřelé registrové klíče** - některé škodlivé programy ukládají své informace do registru pro zajištění jejich automatického spuštění po startu počítače, nebo pro rozšíření jejich vlivu na operační systém.

11.7.5. Záložka Rootkity

Záložka **Rootkity** se objeví ve výsledcích testu pouze v případě, že byl během [Testu celého počítače](#) ve vašem počítači detekován rootkit.

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

Struktura této záložky je identická se strukturou záložek [Infekce](#) nebo [Spyware](#).

11.7.6. Záložka Informace

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

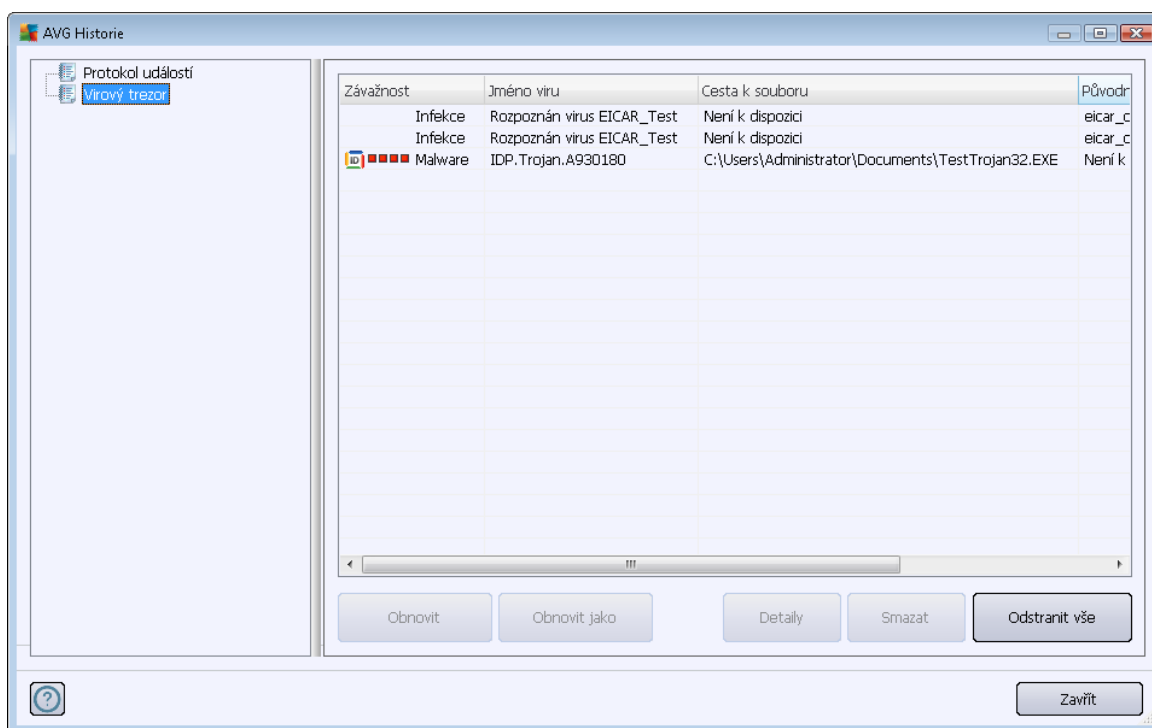
Hlášení na záložce **Informace** může být zobrazeno z jednoho z následujících důvodů:

- **Runtime komprese**: Soubor byl zkomprimován jedním z méně běžných runtime kompresorů, což může naznačovat pokus o ochranu před otestováním takového souboru, ale rozhodně nemusí být každý takto hlášený soubor infikovaný.



- **Rekurzní runtime komprese:** Podobné jako v předchozím případě, ovšem méně často při použití u běžných aplikací. Takovéto soubory jsou podezřelé a měli byste zvážit jejich odstranění.
- **Heslem chráněné dokumenty nebo archivy:** Heslem chráněné soubory nemohou být programem **AVG Anti-Virus Free Edition 2012** (ani jiným bezpečnostním programem) zkontrolovány, proto jsou označeny jako potenciálně nebezpečné.
- **Dokument s makry:** Detekovaný dokument může obsahovat škodlivé makro.
- **Skrytá přípona:** Soubory se skrytou příponou mohou představovat například obrázek, ale také mohou být spustitelné (například `obrazek.jpg.exe`). Druhá přípona je ve výchozím nastavení Windows skrytá. **AVG Anti-Virus Free Edition 2012** Vás na tyto soubory upozorní, abyste předešli jejich náhodnému spuštění.
- **Soubor spuštěný z nesprávného umístění:** Pokud je nainstalovaný systémový soubor spuštěný z jiného než výchozího umístění (například `winlogon.exe` spuštěný z jiné složky než Windows), **AVG Anti-Virus Free Edition 2012** o této nesrovnalosti informuje. Některé viry skrývají svou přítomnost v systému použitím jmen běžných systémových procesů.
- **Zaměněný soubor:** Reportovaný soubor je zaměněný, a tedy nemohl být otestován programem **AVG Anti-Virus Free Edition 2012**. Tato informace ve výsledku test znamená, že soubor je permanentně používán systémem (například stránkový soubor).

11.8. Virový trezor





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

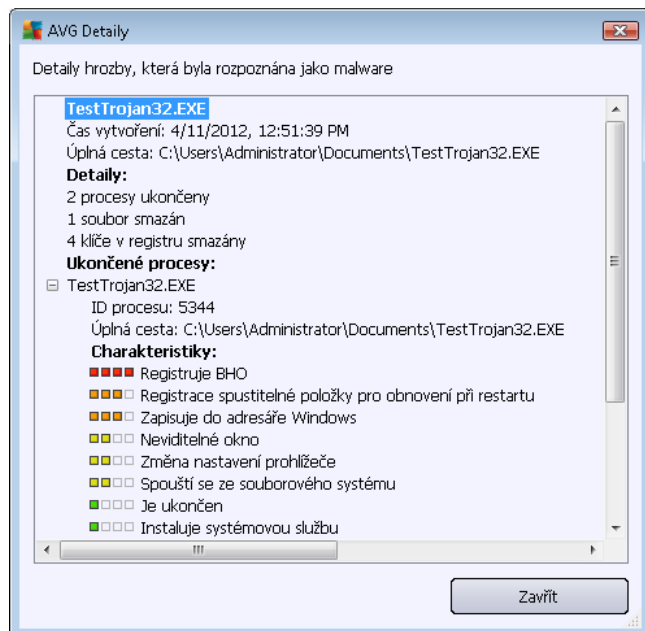
Rozhraní **Virového trezoru** se otevírá v samostatném okně a nabízí přehled informací o infikovaných objektech uložených v karanténě :

- **Závažnost** - jestliže jste si v rámci instalace programu **AVG Anti-Virus Free Edition 2012** nainstalovali také komponentu [Identity Protection](#), najdete v tomto sloupci grafické znázornění závažnosti infekce přesunutá do karantény na čtyřech stupních škály v rozptylu: nezávadný (□□□□) až vysoce rizikový (■ ■ ■ ■); zároveň je zde uvedena informace o typu nález (rozlišuje typy nález podle úrovně jejich infekčnosti - objekty mohou být pozitivní / potenciálně infikované)
- **Jméno viru** - uvádí název detekované infekce viru podle [Virové encyklopedie](#) (on-line)
- **Cesta k souboru** - plná cesta k původnímu umístění souboru, který byl detekován jako infikovaný, na lokálním disku
- **Původní název objektu** - všechny detekované objekty v tabulce jsou uvedeny pod standardním jménem, kterým byly označeny během detekce při testování. Pokud má detekovaný objekt své původní specifické jméno a toto jméno je známo, bude uvedeno v tomto sloupci (například příloha emailu může být označena jménem, které neodpovídá skutečnému detekovanému infekčnímu obsahu, pak budou uvedena obě jména).
- **Datum uložení** - datum a čas detekce infikovaného souboru a jeho přesunutí do **Virového trezoru**

Ovládací tlačítka dialogu

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

- **Obnovit** - přesune infikovaný soubor z **Virového trezoru** zpět do původního umístění
- **Obnovit jako** - pokud se rozhodnete detekovanou infekci z **Virového trezoru** umístit do zvolené složky, použijte toto tlačítko. Podezřelý a detekovaný objekt bude uložen pod svým původním jménem, a pokud toto není známo, bude uložen pod standardním jménem, kterým byl označen při detekci.
- **Detaily** - toto tlačítko se týká pouze objektů nalezených komponentou [Identity Protection](#). Po kliknutí se zobrazí přehled detailních informací o této hrozbě (které soubory/procesy byly dotčeny a jak, charakteristika procesu atd.). U jiných objektů než detekcí IDP je toto tlačítko neaktivní!



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



12. Aktualizace AVG

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

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

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

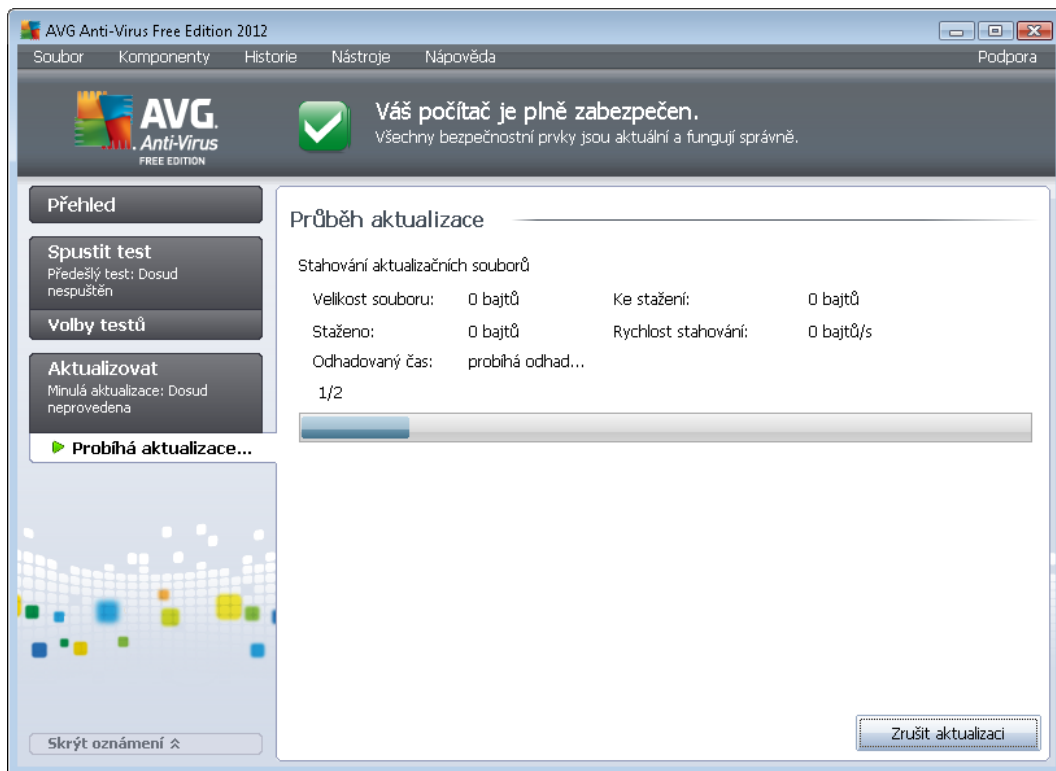
12.1. Spouštění aktualizace

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

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

12.2. Průběh aktualizace

Po spuštění aktualizace dojde nejprve k ověření, zda existují nové aktualizací soubory, jež dosud nebyly aplikovány. Pokud ano, **AVG Anti-Virus Free Edition 2012** zahájí jejich okamžité stahování a spustí samotný proces aktualizace. V průběhu tohoto procesu budete přepnuti do dialogu **Aktualizace**, kde můžete sledovat průběh aktualizace v grafickém zobrazení a současně v přehledu statistických parametrů tohoto procesu (*velikost aktualizacího souboru, objem stažených dat, rychlost stahování, doba trvání, ...*):



Poznámka: Po zahájení programové aktualizace AVG dojde k vytvoření zálohy systému (tzv. system restore point). V případě selhání procesu aktualizace a pádu systému lze z této zálohy obnovit váš operační systém v původní konfiguraci. Tato možnost je dostupná přímo v operačním systému, a to z nabídky Start / Programy / Služby / Systémové nástroje / Obnova systému. Doporučujeme pouze zkušeným uživatelům!

12.3. Úrovně aktualizace

AVG Anti-Virus Free Edition 2012 rozlišuje dvě úrovně aktualizace:

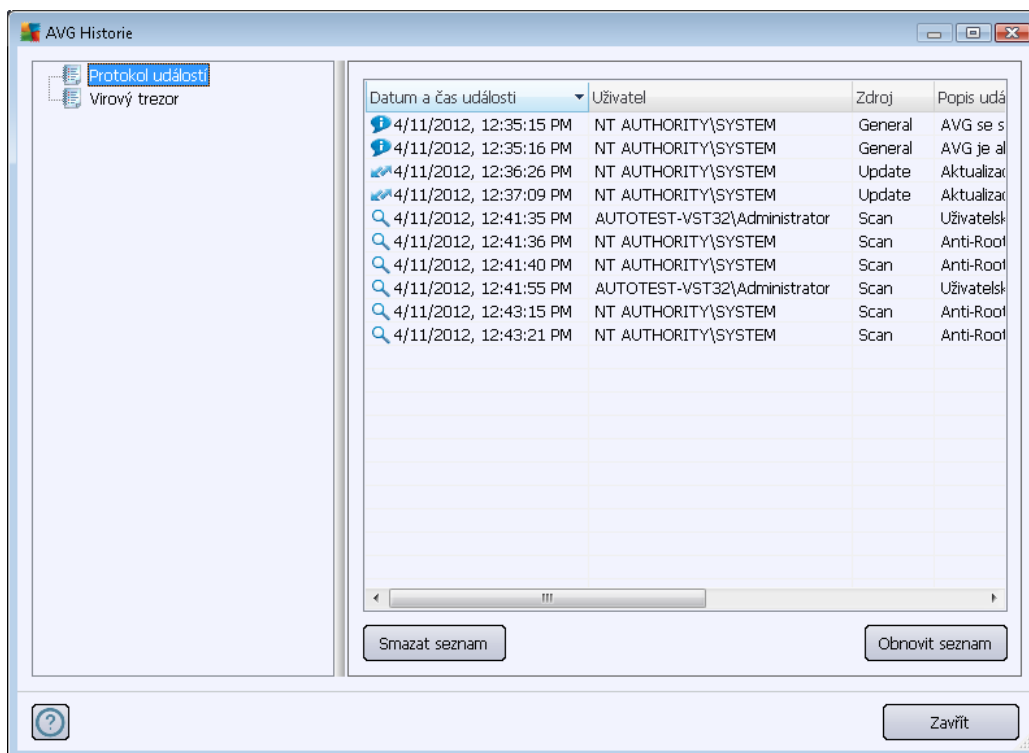
- **Aktualizace definic** zahrnuje změny nezbytné pro spolehlivé fungování antivirové ochrany. Neobsahuje změny v kódu aplikace a aktualizuje pouze virovou a spyware databázi. Aktualizaci doporučujeme spustit co nejdříve po jejím vydání.
- **Programová aktualizace** zahrnuje různé programové změny a doplňky.

Při [nastavování plánu aktualizací](#) je možné definovat požadavky na spouštění obou úrovní aktualizace:

- [Plán aktualizace definic](#)
- [Plán programové aktualizace](#)

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

13. Protokol událostí



Dialog **Historie** je dostupný volbou položky [systémového menu Historie/Protokol událostí](#). V tomto dialogu najdete přehled všech dležících událostí, které nastaly v průběhu práce **AVG Anti-Virus Free Edition 2012**. Zaznamenávají jsou různé typy událostí, například:

- informace o aktualizacích programu
- informace o spuštění/ukončení/přerušování testů (včetně testů spuštěných automaticky)
- informace o událostech týkajících se nalezení viru (komponentou [Rezidentní štít](#), [Identity Protection](#) i při [testování](#)) s uvedením konkrétního místa nálezů
- informace o ostatních dležících událostech

K každé události jsou evidovány následující údaje:

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

Ovládací tlačítka dialogu



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



14. FAQ a technická podpora

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

- **ešení potíží v nápovědě** : Přímou nápověď programu **AVG Anti-Virus Free Edition 2012** je nově k dispozici sekce **ešení potíží**. Ta nabízí výčet nejčastějších situací technického rázu, v nichž si uživatel může vyhledat odbornou pomoc. Zvolte prosím položku, která nejlépe vystihuje Váš aktuální problém a po rozkliknutí se otevře návod s podobným postupem doporučeným pro tuto situaci.
- **Centrum podpory na webu AVG**: Alternativní možností je vyhledat řešení svého problému na webu AVG (<http://www.avg.cz/>). V sekci **Centrum podpory** najdete strukturovaný přehled tematických okruhů, které řeší problémy obchodního i technického charakteru.
- **často kladené otázky**: Na webu AVG (<http://www.avg.cz/>) najdete také samostatnou a detailně členěnou sekci často kladených otázek. Tato sekce je dostupná volbou **Centrum podpory / FAQ**. Otázky jsou opět přehledně rozděleny do kategorií obchodní, technické a virové.
- **Informace o virech a hrozbách**: Samostatná kapitola je na webu AVG (<http://www.avg.cz/>) věnována virové tematice. Volbou **Centrum podpory / Informace o virech a hrozbách** vstoupíte na stránku, která poskytuje strukturovaný přehled informací souvisejících s hrozbami online. Najdete zde také rady, jak odstranit viry, spyware a jak zůstat trvale chráněni.
- **Diskusní fórum**: Můžete také využít diskusního fóra pro uživatele AVG Free produktu na adrese <http://forums.avg.com>.

Při používání AVG Anti-Virus Free Edition 2012 nemáte bohužel nárok na nepřetržitou profesionální technickou podporu poskytovanou zákazníky 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 2012.