



# AVG Internet Security 2012

## Uživatelský manuál

### **Verze dokumentace 2012.20 (28.3.2012)**

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

<b>1. Úvod</b>	<b>5</b>
<b>2. Podmínky instalace AVG</b>	<b>6</b>
2.1 Podporované operační systémy	6
2.2 Minimální / doporučené HW požadavky	6
<b>3. Instalační proces AVG</b>	<b>7</b>
3.1 Vítejte: Volba jazyka	7
3.2 Vítejte: Licenční ujednání	8
3.3 Aktivujte vaši licenci	9
3.4 Vyberte typ instalace	10
3.5 Uživatelské volby	12
3.6 Nainstalovat AVG Security Toolbar	13
3.7 Postup instalace	13
3.8 Instalace byla úspěšná	15
<b>4. Po instalaci</b>	<b>16</b>
4.1 Registrace produktu	16
4.2 Otevření uživatelského rozhraní	16
4.3 Spuštění testu celého počítače	16
4.4 Test virem Eicar	16
4.5 Výchozí konfigurace AVG	17
<b>5. Uživatelské rozhraní AVG</b>	<b>18</b>
5.1 Systémové menu	19
5.2 Informace o stavu zabezpečení	27
5.3 Zkratková tlačítka	28
5.4 Přehled komponent	29
5.5 Ikona na systémové liště	30
5.6 AVG Advisor	32
5.7 Miniaplikace AVG	33
<b>6. Komponenty AVG</b>	<b>36</b>
6.1 Anti-Virus	36
6.2 LinkScanner	42
6.3 E-mailová ochrana	47



6.4 Firewall	51
6.5 Anti-Rootkit	55
6.6 Systémové nástroje	56
6.7 PC Analyzer	62
6.8 Identity Protection	64
6.9 Vzdálená správa	66
<b>7. Moje Aplikace</b>	<b>67</b>
7.1 AVG LiveKive	67
7.2 AVG Mobilation	68
7.3 AVG Family Safety	68
7.4 AVG PC Tuneup	69
<b>8. AVG Security Toolbar</b>	<b>70</b>
<b>9. AVG Do Not Track</b>	<b>72</b>
9.1 Rozhraní služby AVG Do Not Track	73
9.2 Informace o sledovacích procesech	74
9.3 Blokování sledovacích procesů	75
9.4 Nastavení služby AVG Do Not Track	75
<b>10. Nastavení Firewallu</b>	<b>78</b>
10.1 Obecné	78
10.2 Bezpečnost	79
10.3 Profily sítí a adaptérů	80
10.4 IDS	81
10.5 Protokoly	83
10.6 Profily	84
<b>11. Pokročilé nastavení AVG</b>	<b>95</b>
11.1 Vzhled	95
11.2 Zvuky	98
11.3 Dočasné vypnutí ochrany AVG	99
11.4 Anti-Virus	101
11.5 E-mailová ochrana	106
11.6 LinkScanner	124
11.7 Testy	128
11.8 Naplánované úlohy	134



11.9 Aktualizace.....	144
11.10 Anti-Rootkit.....	150
11.11 Identity Protection.....	152
11.12 Potenciálně nežádoucí programy.....	156
11.13 Virový trezor.....	159
11.14 Program zlepšování produktu.....	159
11.15 Ignorovat chybový stav.....	162
11.16 Advisor - známé sítě.....	163
<b>12. AVG testování.....</b>	<b>165</b>
12.1 Rozhraní pro testování.....	165
12.2 Přednastavené testy.....	166
12.3 Testování v průzkumníku Windows.....	175
12.4 Testování z příkazové řádky.....	175
12.5 Naplánování testu.....	178
12.6 Přehled výsledků testů.....	188
12.7 Detail výsledku testu.....	189
12.8 Virový trezor.....	196
<b>13. Aktualizace AVG.....</b>	<b>199</b>
13.1 Spouštění aktualizace.....	199
13.2 Průběh aktualizace.....	199
13.3 Úrovně aktualizace.....	200
<b>14. Protokol událostí.....</b>	<b>202</b>
<b>15. FAQ a technická podpora.....</b>	<b>204</b>



## 1. Úvod

Tento uživatelský manuál je kompletní dokumentací programu **AVG Internet Security 2012**.

Aplikace **AVG Internet Security 2012** poskytuje vícevrstvou ochranu vždy, když jste připojeni k Internetu, takže si nemusíte dělat starosti s krádežemi identity, viry nebo přístupem na nebezpečné stránky. Obsahuje ochrannou technologii Cloud AVG a komunitní ochrannou síť AVG, což znamená, že sbíráme informace ohledně nejnovějších hrozeb a sdílíme je v komunitě, abyste obdrželi tu nejlepší ochranu:

- Nakupujte a používejte internetové bankovníctví online bezpečně díky bráně AVG Firewall a aplikacím Anti-Spam a Identity Protection
- Buďte v bezpečí na sociálních sítích díky aplikaci AVG Social Networking Protection
- Procházejte Internet a vyhledávejte informace bez obav díky technologii LinkScanner zajišťující ochranu v reálném čase



## 2. Podmínky instalace AVG

### 2.1. Podporované operační systémy

AVG Internet Security 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 Internet Security 2012, ale pouze bez této komponenty.

### 2.2. Minimální / doporučené HW požadavky

Minimální hardwarové požadavky pro **AVG Internet Security 2012**:

- Procesor Intel Pentium 1,5 GHz
- 512 MB RAM paměti
- 1000 MB volného místa na pevném disku (z instalace dříve)

Doporučené hardwarové požadavky pro **AVG Internet Security 2012**:

- Procesor Intel Pentium 1,8 GHz
- 512 MB RAM paměti
- 1550 MB volného místa na pevném disku (z instalace dříve)



### 3. Instalační proces AVG

#### Kde najdu instalační soubor?

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

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

#### Jak probíhá proces instalace?

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

#### 3.1. Vítejte: Volba jazyka

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



V tomto dialogu máte možnost zvolit jazyk instalačního procesu. V pravém horním rohu okna kliknutím rozbalíte nabídku všech dostupných jazyků. Po potvrzení Vaší volby bude instalační proces nadále probíhat ve zvoleném jazyce.

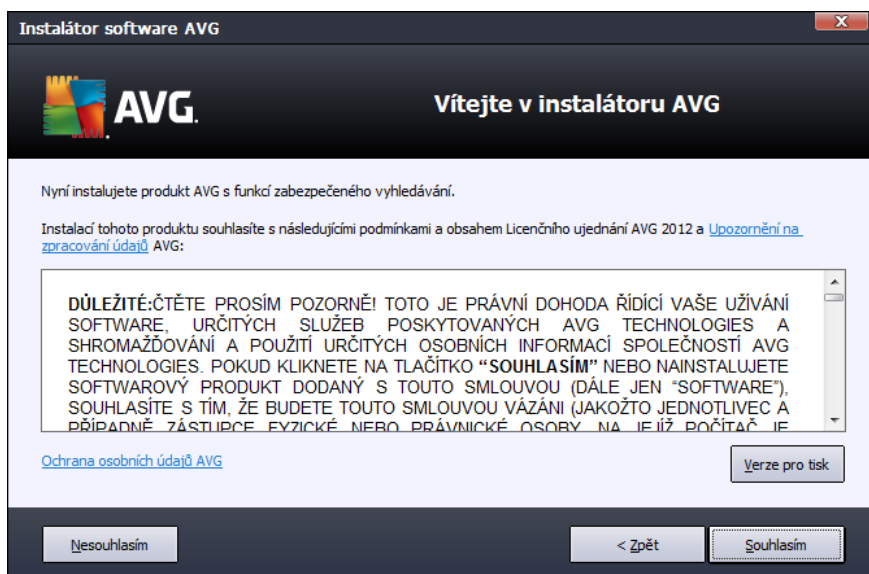
**Pozor: V tuto chvíli volíte pouze jazyk instalačního procesu. Aplikace AVG Internet Security 2012 bude tedy nainstalována ve zvoleném jazyce a také v angličtině, která se instaluje**



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:



Prohlédněte si prosím pečlivě celý text závazné licenční smlouvy AVG. Svůj souhlas s licenčním ujednáním potvrdíte 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. V levém spodním rohu dialogu najdete odkaz **Ochrana osobních údajů AVG**. Kliknutím na něj budete přesměrováni na webovou stránku AVG (<http://www.avg.cz/>), která Vás v plném rozsahu seznámí se zásadami ochrany osobních údajů společnosti AVG Technologies.

#### Ovládací tlačítka dialogu

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

- **Souhlasím** - Kliknutím potvrzujete, že jstečetli licenční ujednání a přijímáte jej v plném rozsahu. Instalace bude pokračovat p echodem do následujícího dialogu instalačního procesu.
- **Nesouhlasím** - Kliknutím odmítáte přijmout licenční ujednání. Instalační proces bude bezprostředně ukončen. **AVG Internet Security 2012** nebude nainstalován!





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

### 3.3. Aktivujte vaši licenci

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

#### Kde najdu licenční číslo

Licenční číslo najdete buďto na registrační kartě v krabicovém balení **AVG Internet Security 2012**, anebo v potvrzovacím emailu, který jste obdrželi při zakoupení **AVG Internet Security 2012** on-line. Licenční číslo musí být zadáno naprosto přesně ve tvaru, jak je uvedeno, proto prosím věnujte velkou pozornost jeho přesnosti. Pokud máte číslo k dispozici v digitální formě, doporučujeme jej do příslušného pole zkopírovat (*metodou kopírovat a vložit*).

#### Jak použít metodu Copy & Paste

Následující popis krok za krokem je stručným popisem toho, jak použít metodu **Copy & Paste** (*kopíruj a vlož*) při vkládání licenčního čísla **AVG Internet Security 2012**:

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



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

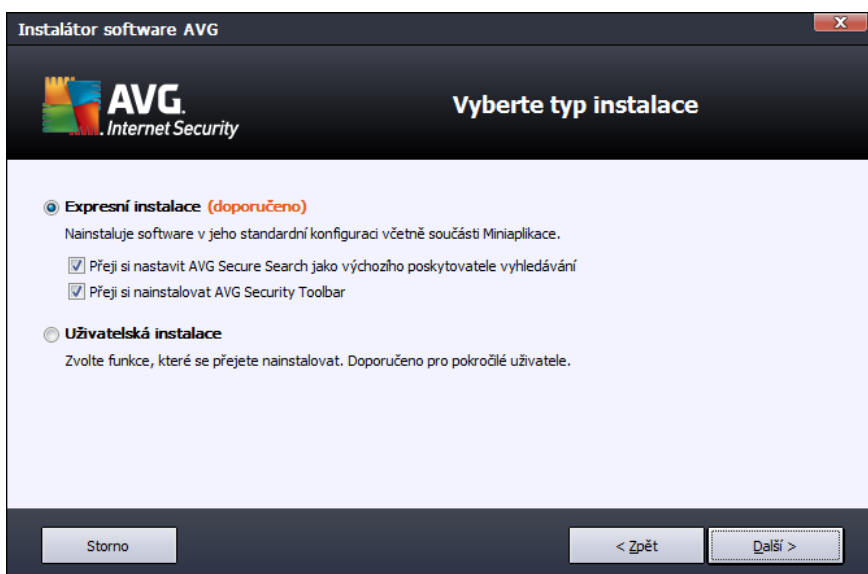
### Ovládací tlačítka dialogu

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

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

## 3.4. Vyberte typ instalace

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



### Expresní instalace

Většinu uživatelů doporučíme použít expresní instalaci, kdy bude **AVG Internet Security 2012** nainstalován zcela automaticky s nastavením definovaným výrobcem, včetně [miniaplikace AVG](#). Toto nastavení zaručuje maximální úroveň bezpečnosti a optimální využití zdrojů. Pokud se v budoucnu vyskytne potřeba některých konkrétních nastavení změnit, budete mít vždy možnost editovat konfiguraci **AVG Internet Security 2012** přímo v aplikaci.

V této sekci najdete dvě možnosti volby. Obě jsou ve výchozím nastavení zapnuty, a pokud nemáte



Od tohoto nastavení můžete doporučené je takto ponechat:

- **Přejít si nastavit AVG Secure Search jako výchozího poskytovatele vyhledávání** - ponecháte-li tuto volbu zapnutou, **AVG Internet Security 2012** bude pro vyhledávání používat službu AVG Secure Search, která úzce spolupracuje s komponentou [Link Scanner](#) a zajišťuje tak vaši maximální bezpečnost při pohybu po webu.
- **Přejít si nainstalovat AVG Security Toolbar** - ponecháte-li tuto možnost označenu, bude nainstalován [AVG Security Toolbar](#), který rovněž pomáhá zvýšit vaši bezpečnost online.

Stiskem tlačítka **Další** postoupíte k dialogu [Instalovat AVG Security Toolbar](#).

### Uživatelská instalace

Uživatelská instalace je vhodná pouze pro pokročilé a znalé uživatele. Doporučujeme ji pouze v případě, že máte skutečnou potřebu instalovat **AVG Internet Security 2012** s nestandardním nastavením tak, aby vyhovovalo specifickým požadavkům vašeho systému.

Pokud se rozhodnete pro uživatelskou instalaci, zobrazí se nová sekce **Cílové umístění**. Zde máte možnost určit, kam má být program **AVG Internet Security 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 předvolnému umístění definovanému výrobcem, můžete tak učinit pomocí tlačítka **Výchozí**.

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

### Ovládací tlačítka dialogu

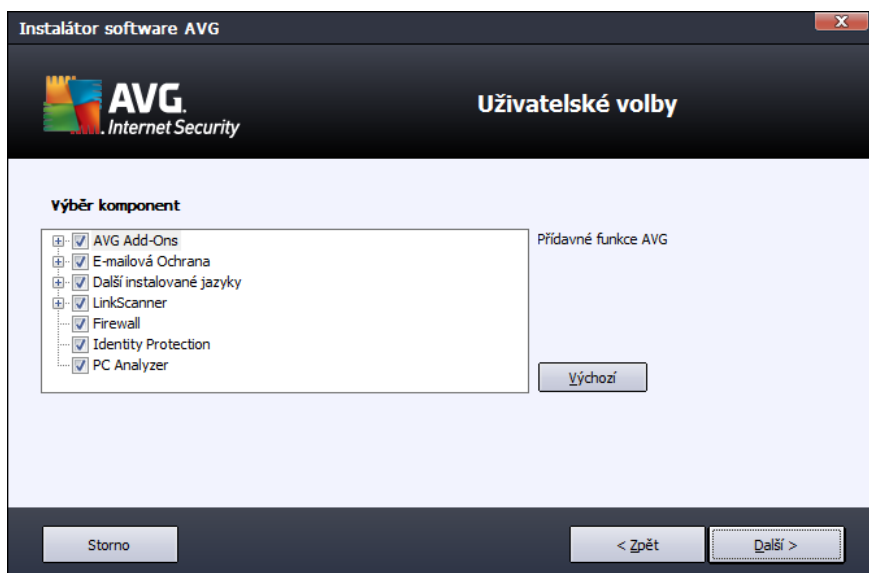
Podobně jako ve většině dialogů instalace, jsou i zde dostupná tři ovládací tlačítka:

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



### 3.5. Uživatelské volby

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



Sekce **Výběr komponent** nabízí přehled komponent **AVG Internet Security 2012**, které můžete nainstalovat. Pokud vám výchozí nastavení nevyhovuje, máte možnost jednotlivé komponenty odebrat/přidat.

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

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

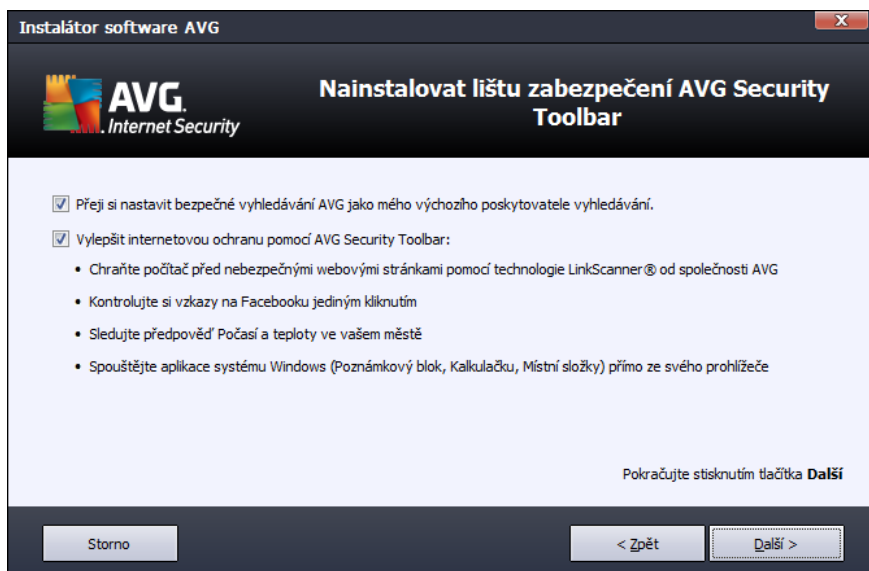
#### Ovládací tlačítka dialogu

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

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



### 3.6. Nainstalovat AVG Security Toolbar



V dialogu **AVG Security Toolbar** rozhodnete, zda si v rámci **AVG Internet Security 2012** přejete nainstalovat i službu [AVG Security Toolbar](#). Pokud nezměníte výchozí nastavení, bude tato komponenta automaticky nainstalována do vašeho internetového prohlížeče (podporované prohlížeče jsou *Microsoft Internet Explorer v. 6.0 nebo novější* a *Mozilla Firefox v. 3.0 nebo novější*) a zajistí kompletní on-line ochranu při prohlížení webu.

V tomto dialogu máte také možnost rozhodnout, zda si přejete nastavit bezpečné vyhledávání AVG jako výchozí službu vyhledávání. Pokud ano, ponechte označené příslušné políčko.

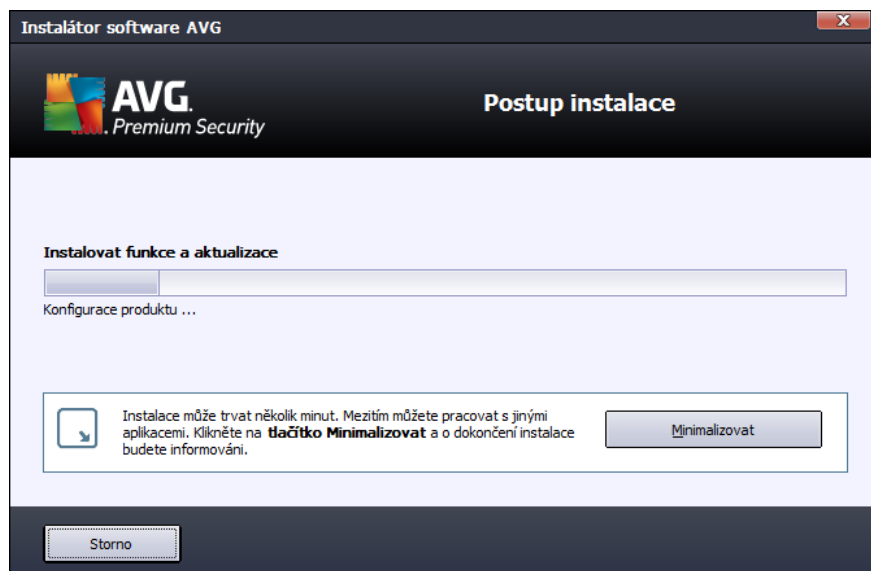
#### Ovládací tlačítka dialogu

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

- **Storno** - Kliknutím na toto tlačítko bezprostředně ukončíte instalační proces; **AVG Internet Security 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.

### 3.7. 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.

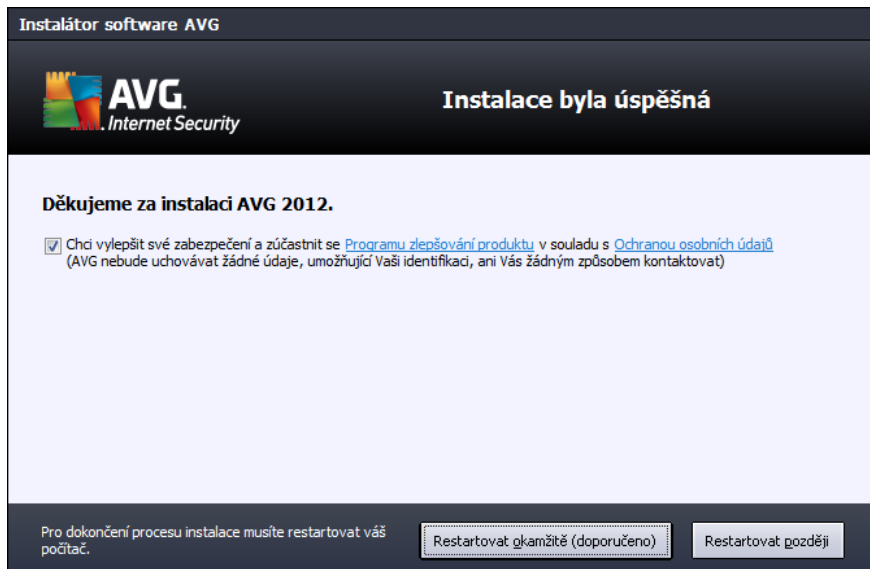
### Ovládací tlačítka dialogu

V dialogu je dostupné jediné ovládací tlačítko - **Storno**. Toto tlačítko použijte výhradně tehdy, přejete-li si přerušit instalační proces. V takovém případě nebude **AVG Internet Security 2012** nainstalován!



### 3.8. Instalace byla úspěšná

Dialog **Instalace byla úspěšná** potvrzuje, že **AVG Internet Security 2012** byl plně nainstalován a nastaven k optimálnímu výkonu:



#### Program zlepšování produktu

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. Pokud souhlasíte s tímto tvrzením, ponechte prosím volbu **Souhlasím s účastí v programu webové bezpečnosti AVG 2012 a Programu zlepšování produktu ...** označenou (ve výchozím nastavení je tato možnost zapnuta).

#### Restart počítače

Pro dokončení procesu instalace je třeba, abyste restartovali svůj počítač: rozhodněte se, zda chcete **Restartovat okamžitě** nebo tento krok odložit a **Restartovat později**.



## 4. Po instalaci

### 4.1. Registrace produktu

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

Nejsnazší přístup k registraci je přímo z prostředí aplikace **AVG Internet Security 2012**, a to volbou položky hlavního menu [Nápověda/Registrovat](#). Následně budete přeměněni na stránku **Registrace** na webu AVG (<http://www.avg.cz/>), kde dále postupujte podle uvedených instrukcí.

### 4.2. Otevření uživatelského rozhraní

[Hlavní dialog AVG](#) je dostupný několika cestami:

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

### 4.3. Spuštění testu celého počítače

Jelikož existuje jisté riziko, že virus byl na váš počítač zavlečen již před instalací **AVG Internet Security 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 dležitější jej nechat proběhnout. Instrukce ke spuštění testu najdete v kapitole [AVG testování](#).

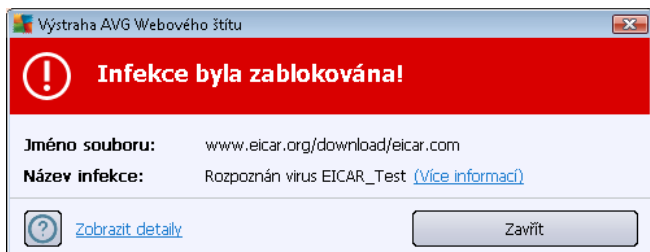
### 4.4. Test virem Eicar

Chcete-li ověřit, že **AVG Internet Security 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 (*protože jsou schopny jej rozpoznat a označit skutečným jménem; hlásí jeho přítomnost například takto "EICAR-AV-Test"*). 'Virus' EICAR si můžete stáhnout z internetu na adrese <http://www.eicar.com>, kde také najdete všechny nezbytné informace o 'viru' samotném a testování tímto 'virem'.

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





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

**Pokud není testovací soubor EICAR identifikován jako virus, je nutné znovu provést konfiguraci AVG Internet Security 2012!**

#### 4.5. Výchozí konfigurace AVG

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

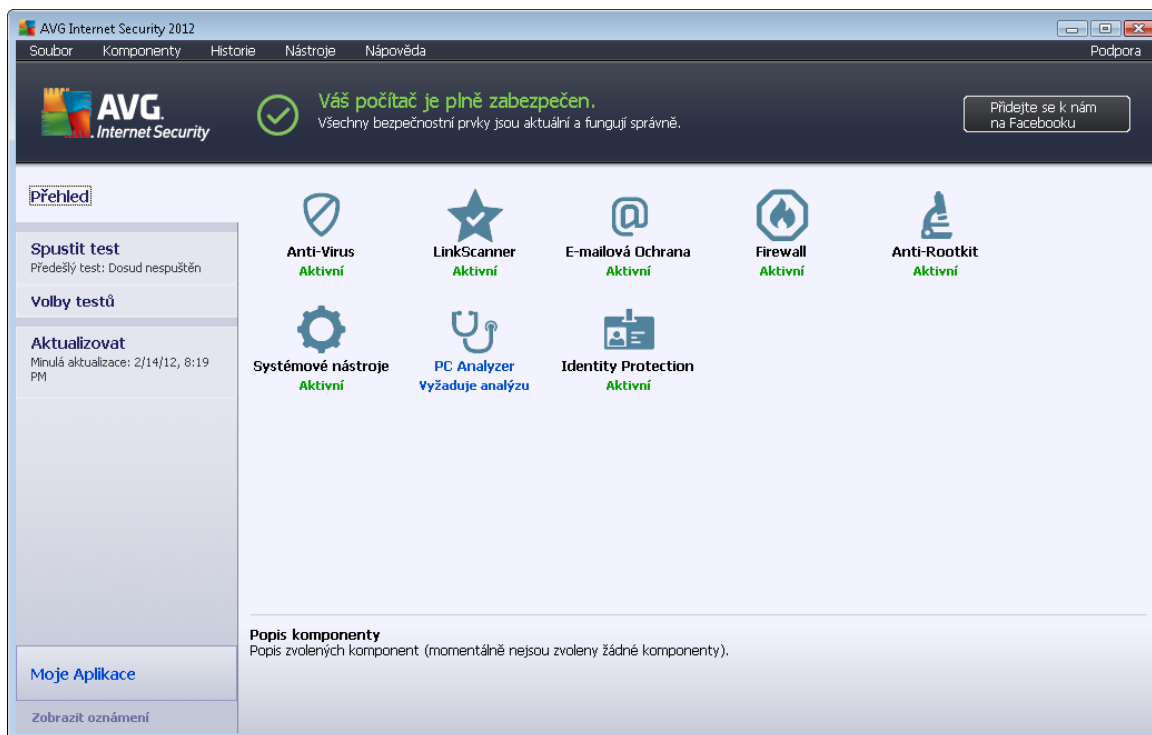
**Pokud nemáte skutečný důvod jejich konfiguraci změnit, doporučujeme ponechat program v tomto nastavení! Změnu konfigurace by měla provádět pouze zkušený uživatel.**

Jednoduché, spíše preferenční změny v nastavení [komponent AVG](#) jsou dostupné vždy přímo z hlavního dialogu pro jednotlivé komponenty. Pokud se domníváte, že je nutné konfiguraci AVG přenastavit podle vašich aktuálních potřeb, proveďte editaci parametrů v [Pokročilém nastavení AVG](#): zvolte ze systémového menu položku **Nástroje/Pokročilé nastavení** a editaci nastavení proveďte v nově otevřeném dialogu [Pokročilém nastavení AVG](#).



## 5. Uživatelské rozhraní AVG

AVG Internet Security 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 Internet Security 2012** - [podrobnosti >>](#)
- **Informace o stavu zabezpečení** (v horní části okna) podává základní informaci o aktuálním stavu **AVG Internet Security 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 Internet Security 2012** - [podrobnosti >>](#)
- **Moje aplikace** (v levé spodní části okna) otevírají přehled doplňkových aplikací **AVG Internet Security 2012**: [LiveKive](#), [Family Safety](#) a [PC Tuneup](#)
- **Přehled komponent** (ve střední části okna) nabízí přehled všech instalovaných komponent **AVG Internet Security 2012** - [podrobnosti >>](#)



- **Ikona na systémové liště** (v pravém dolním rohu monitoru, na systémové liště) je indikátorem aktuálního stavu **AVG Internet Security 2012** - [podrobnosti >>](#)
- **Miniaplikace AVG** (panel Windows sidebar, podporováno pouze v OS Windows Vista/7) umožňuje rychlý přístup k testování a aktualizaci programu - [podrobnosti >>](#)

## 5.1. Systémové menu

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

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

### 5.1.1. Soubor

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

### 5.1.2. Komponenty

Položka systémového menu [Komponenty](#) obsahuje odkazy k jednotlivým instalovaným komponentám AVG a otevírá hlavní dialog příslušné komponenty:

- **Přehled komponent** - přepne uživatelské rozhraní na dialog [přehled komponent a jejich stavu](#)
- **Anti-Virus** detekuje na vašem počítači viry, spyware, červy, trojany, nežádoucí spustitelné soubory nebo knihovny a chrání vás před nimi - [podrobnosti >>](#)
- **LinkScanner** vás chrání před webovými útoky v době, kdy surfujete na Internetu - [podrobnosti >](#)
- **E-mailová Ochrana** kontroluje všechny příchozí e-mailové zprávy a filtruje SPAM, blokuje viry, phishingové útoky a jiné hrozby - [podrobnosti >>](#)
- **Firewall** řídí veškerou komunikaci na všech síťových portech, a tak vás chrání před nebezpečnými útoky a pokusy o vniknutí do vašeho počítače - [podrobnosti >>](#)
- **Anti-Rootkit** testuje všechny aplikace, ovladače a knihovny na přítomnost skrytých rootkitů - [podrobnosti >>](#)
- **Systémové nástroje** zobrazují detailní přehled prostředí AVG a poskytují informace o operacím systému - [podrobnosti >>](#)
- **PC Analyzer** analyzuje stav vašeho počítače a nabízí přehled zjištěných údajů - [podrobnosti >>](#)
- **Identity Protection** nepřetržitě chrání vaše digitální data před novými a neznámými hrozbami - [podrobnosti >>](#)



- **Vzdálená správa** se zobrazuje pouze podmíněně v případě, že instalujete Business Edici produktu AVG a rozhodli jste se během [instalačního procesu](#) tuto komponentu doinstalovat.

### 5.1.3. Historie

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

### 5.1.4. Nástroje

- **Otestovat počítač** - Přímo spouští **Test celého počítače**.
- **Otestovat zvolený adresář...** - Přepíná do **testovacího rozhraní AVG** a nabízí ve stromové struktuře vašeho disku možnost definovat ty složky, které mají být otestovány.
- **Otestovat soubor...** - Umožňuje spustit test na vyžádání pouze nad jedním konkrétním souborem. Kliknutím na tuto volbu se otevře nové okno s náhledem stromové struktury vašeho disku. Zvolte požadovaný soubor a potvrďte spuštění testu.
- **Aktualizovat** - Automaticky spouští proces aktualizace AVG Internet Security 2012.
- **Aktualizace z adresáře...** - Spustí proces aktualizace z aktualizací souboru umístěného v definovaném adresáři na lokálním disku. Tuto alternativu doporučujeme pouze jako náhradní řešení pro případ, že v danou chvíli nebude k dispozici připojení k Internetu (*např. počítač je zavirovaný a odpojený ze sítě, počítač je připojen k síti, kde není přístup k Internetu, apod.*). V nově otevřeném okně vyberte adresář, do nějž jste předešle umístili aktualizací soubory, a spusťte aktualizaci.
- **Pokročilé nastavení...** - Otevírá dialog **Pokročilého nastavení AVG**, kde máte možnost editovat konfiguraci **AVG Internet Security 2012**. Obecně doporučujeme dodržet výchozí výrobcem definované nastavení aplikace.



- [Nastavení Firewallu...](#) - Otevírá samostatný dialog pro pokročilou konfiguraci komponenty Firewall.

### 5.1.5. Nápověda

- **Obsah** - otevírá nápovědu k programu AVG
- **Získat podporu** - otevírá web AVG (<http://www.avg.cz/>) na stránce centra zákaznické podpory
- **AVG na webu** - otevírá web AVG (<http://www.avg.cz/>)
- **Informace o virech** - otevírá [Virovou encyklopedii](#) na webu AVG (<http://www.avg.cz/>), v níž lze dohledat podrobné informace o detekovaných nálezech
- **Reaktivovat** - otevírá dialog Aktivace AVG, v němž jsou již předem vyplněna data, jež jste zadali v dialogu [Registrace AVG](#) během [instalace svého procesu](#). V dialogu **Aktivace AVG** můžete zadat své licenční číslo, kterým budete nahradit prodejní číslo, s nímž jste AVG instalovali, nebo kterým změníte dosavadní licenční číslo za jiné, například přechodem na jiný produkt z řady AVG.
- **Registrovat** - otevírá web AVG (<http://www.avg.cz/>) na stránce **Registrace**. Vyplňte prosím své registrační údaje; pouze registrovaní zákazníci mají plný přístup k technické podpoře AVG.

**Poznámka:** Máte-li nainstalovanou zkušební verzi **AVG Internet Security 2012**, dví poslední uvedené položky se zobrazí jako **Zakoupit a Aktivovat** a odkáží Vás na web AVG, kde si můžete přímou zakoupit plnou verzi programu. Pokud máte nainstalovaný program **AVG Internet Security 2012** s prodejním číslem, položky se zobrazí jako **Zaregistrovat a Aktivovat**.

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

### 5.1.6. Podpora

Položka **Podpora** otevírá nový dialog **Informace** s kompletním výčtem informací, které můžete potřebovat například při kontaktu se zákaznickou podporou. Dialog dále obsahuje základní údaje o instalovaném programu **AVG Internet Security 2012** (verzi programu a databáze), licenční údaje a seznam odkazů na zdroje podpory:

Dialog **Informace** je rozdělen do šesti záložek, strukturovaný do logických celků :



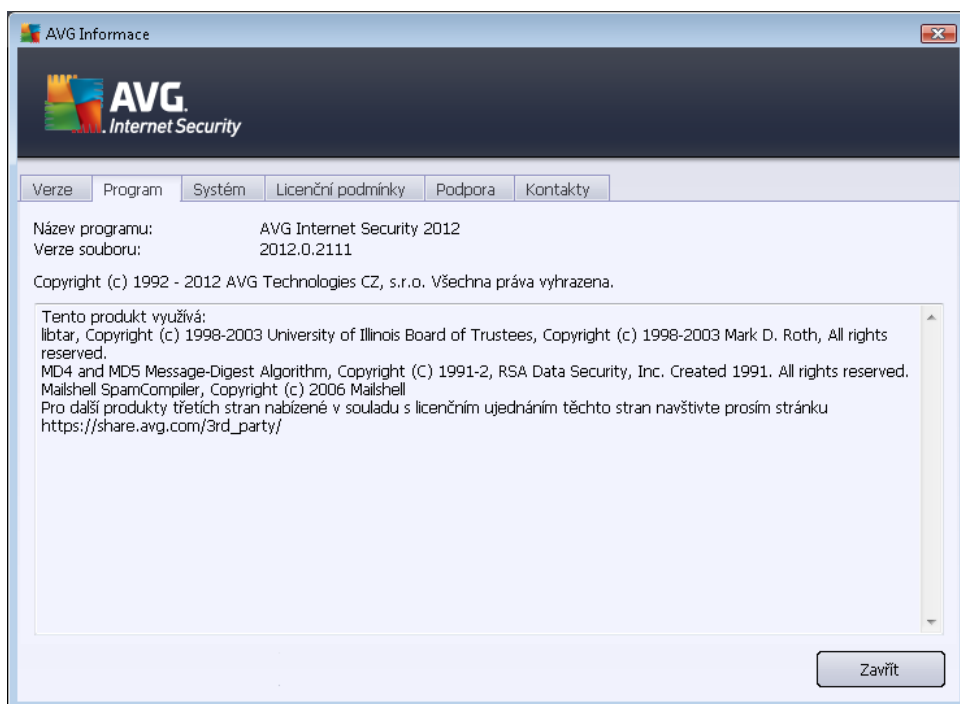
Záložka **Verze** je rozdělena do tří sekcí:



- **Informace o podpoře** - Uvádí informace o verzi **AVG Internet Security 2012**, o verzi virové databáze, verzi databáze pro [Anti-Spam](#) a verzi [LinkScanneru](#).
- **Uživatelské informace** - Uvádí informace o uživateli licence a společnosti.
- **Detaily licence** - Uvádí údaje týkající se Vaší licence (*název produktu, typ licence, licenční číslo, datum expirace licence a počet instalací*). V této sekci můžete také volbou odkazu **Zaregistrovat** provést online registraci Vašeho **AVG Internet Security 2012**, čímž získáte plný přístup k [technické podpoře AVG](#). Pomocí odkazu **Přeregistrovat** pak otevřete dialog **Aktivace AVG**; do tohoto dialogu zadejte své licenční číslo, kterým buďto nahradíte prodejní číslo (*s nímž jste AVG Internet Security 2012 instalovali*), nebo kterým změníte dosavadní licenční číslo za jiné (*například přechodu na jiný produkt z řady AVG*).



Záložka **Program** uvádí přesný název instalované edice **AVG Internet Security 2012** a číslo verze instalačního souboru. Dále jsou uvedeny informace o použitých kódech třetích stran:





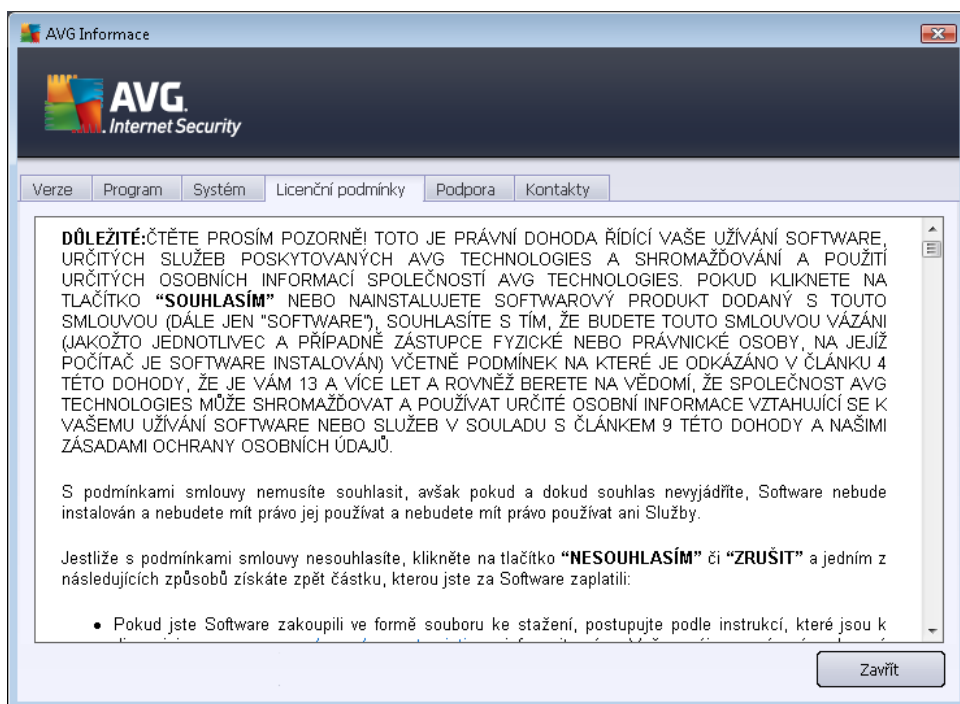
Záložka **Systém** nabízí pohled parametrů Vašeho operačního systému: procesor, operační systém, verze Windows, číslo sestavení, service pack a údaje o celkovém a volném objemu paměti:







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





Záložka **Podpora** je rozčleněna do několika sekcí:



- **Informace o podpoře** - Uvádí informace o verzi **AVG Internet Security 2012** a verzi virové databáze.
- **Rychlé odkazy na podporu** - Nabízí seznam dostupných možností zákaznické podpory a odkazy na webové stránky AVG (<http://www.avg.cz/>), fórum uživatelů, FAQ, ...
- **Nainstalovaná ochrana e-mailu** - Uvádí přehled instalovaných doplňků pro kontrolu pošty. Tyto informace můžete použít i pro kontakt s pracovníkem zákaznické podpory.
- **Detaily licence** - Uvádí údaje týkající se Vaší licence (*název produktu, typ licence, licenční číslo, datum expirace licence a počet instalací*). V této sekci můžete také volbou odkazu **Zaregistrovat** provést online registraci Vašeho AVG Internet Security 2012, čímž získáte plný přístup k [technické podpoře AVG](#). Pomocí odkazu **Přeregistrovat** pak otevřete dialog **Aktivace AVG**; do tohoto dialogu zadejte své licenční číslo, kterým budete nahradit prodejní číslo (*s nímž jste AVG Internet Security 2012 instalovali*), nebo kterým změníte dosavadní licenční číslo za jiné (*např. při přechodu na jiný produkt z řady AVG*).
- **Centrum podpory** - Pomocí tlačítka **Podpora online** budete přesměrováni na dedikovanou stránku na webu AVG (<http://www.avg.cz/>), kde najdete kompletní výčet všech dostupných možností zákaznické podpory.



Záložka **Kontakty** nabízí seznam dostupných kontaktů do společnosti AVG Technologies, i kontakty na lokální zástupce a prodejce AVG:



## 5.2. Informace o stavu zabezpečení

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



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



- Žlutá ikona informuje o stavu, kdy **jedna (nebo více) komponent není správně nastavena**. Nejedná se o kritický problém, pravděpodobně jste se sami rozhodli některou komponentu deaktivovat. V každém případě jste stále chráněni. Pro mějte prosím vnujte 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 Internet Security 2012**. Touto volbou



dáváte najevo, že jste si v domě na fakt, že se konkrétní komponenta nachází v chybovém stavu, ale z nějakého důvodu si přejete tento stav zachovat a nebyť na něj upozorování [ikonou na systémové liště](#). Můžete 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 Internet Security 2012** vyžaduje restart počítače (**Restartovat nyní**). Vždy prosím pozornost tomuto varování a restartujte počítač pomocí tlačítka **Restartovat nyní**.



- Oranžová ikona **informuje o kritickém stavu AVG Internet Security 2012!** Některá z komponent je nefunkční a **AVG Internet Security 2012** nemůže plně chránit váš počítač. Vždy prosím okamžitou pozornost opravě tohoto problému. Pokud nebudete sami schopni problém odstranit, kontaktujte oddělení [technické podpory AVG](#).

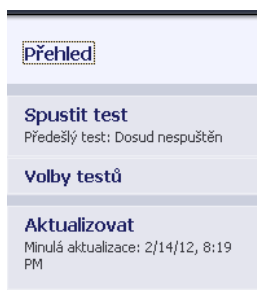
V případě, kdy **AVG Internet Security 2012** není nastaven k plnému a optimálnímu výkonu se vedle informace o stavu zabezpečení zobrazí tlačítko **Opravit** (případně **Opravit vše**, pokud se problém týká více než jediné komponenty), jehož stiskem **AVG Internet Security 2012** automaticky spustí proces 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 Internet Security 2012** hlásí jakýkoliv problém, zaměřte se na jeho řešení. Pokud ignorujete chybová hlášení **AVG Internet Security 2012**, váš počítač je ohrožen!

**Poznámka:** Informaci o stavu **AVG Internet Security 2012** lze v kterémkoliv okamžiku práce na počítači získat také pohledem na [ikonu na systémové liště](#).

### 5.3. Zkratková tlačítka

**Zkratková tlačítka** najdete v levé části [hlavního dialogu AVG Internet Security 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 Internet Security 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 oprotivnému spuštění téhož testu. Pokud chcete spustit jiný test, klikněte na položku **Volby test**. Tím otevřete [testovací rozhraní AVG Internet Security 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 Internet Security 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 Internet Security 2012** jsou aktuálně spuštěny.

## 5.4. Přehled komponent

### Rozdělení Pohledu komponent

Sekce **Pohled komponent** je umístěna ve střední části [hlavního dialogu AVG Internet Security 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 Internet Security 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 >>](#)
- **LinkScanner** 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 >>](#)
- **Firewall** řídí veškerou komunikaci na všech síťových portech, a tak vás chrání před



nebezpečnými útoky a pokusy o vniknutí do vašeho počítače - [podrobnosti >>](#)

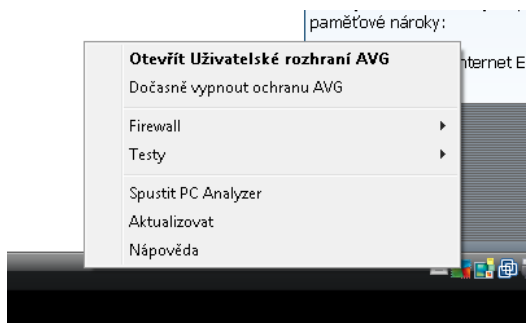
- **Anti-Rootkit** testuje všechny aplikace, ovladače a knihovny na přítomnost skrytých rootkitů - [podrobnosti >>](#)
- **Systémové nástroje** zobrazují detailní pohled prostředí AVG a poskytují informace o operačním systému - [podrobnosti >>](#)
- **PC Analyzer** analyzuje stav vašeho počítače a nabízí pohled zjištěných údajů - [podrobnosti >>](#)
- **Identity Protection** nepřetržitě chrání vaše digitální data před novými a neznámými hrozbami - [podrobnosti >>](#)
- **Vzdálená správa** se zobrazuje pouze podmíněně v případě, že instalujete Business Edici produktu AVG a rozhodli jste se během [instalačního procesu](#) tuto komponentu doinstalovat

### Dostupné akce

- **Přejezdem myši nad ikonou komponenty** tuto komponentu v pohledu vysvítíte a souasně se ve spodní části [hlavního dialogu](#) zobrazí stručný popis funkce této komponenty.
- **Jednoduchým kliknutím na libovolnou ikonu komponenty** otevřete vlastní rozhraní komponenty s pohledem 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 Internet Security 2012**. Ikona je viditelná v každém okamžiku vaší práce na počítači, bez ohledu na to, zda máte ikonu otevřenou [uživatelské rozhraní aplikace](#):



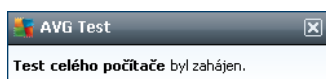
## Zobrazení systémové ikony AVG

Ikona může být zobrazena v několika variantách:

- Jestliže je ikona zobrazena barevně bez dalších prvků, jsou všechny komponenty **AVG Internet Security 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 fakturu, že se ta která [komponenta nachází v chybovém stavu](#), ale z nějakého důvodu si přejete tento stav zachovat a nebýt 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 [hlavní dialog aplikace](#) dvojklikem na ikonu na systémové liště. Podrobnější informace o tom, která komponenta je v [chybovém stavu](#), pak najdete v sekci [informace o stavu zabezpečení](#).
- Ikona na systémové liště může být také zobrazena barevně s probleskujícím otáčejícím se paprskem. Toto grafické znázornění signalizuje právě probíhající aktualizaci **AVG Internet Security 2012**.
- Alternativní zobrazení ikony s šipkou znamená, že právě běží některý z testů **AVG Internet Security 2012**.

## Informace systémové ikony AVG

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





## Akce dostupné ze systémové ikony AVG

**Ikonu AVG na systémové liště** lze také použít pro rychlý přístup k [hlavnímu dialogu AVG Internet Security 2012](#), to se otevře dvojklikem na ikonu. Kliknutí pravým tlačítkem myši nad ikonou otevírá kontextové menu s těmito možnostmi:

- **Otevřít uživatelské rozhraní AVG** - Otevře [hlavní dialog AVG Internet Security 2012](#).
- **Dočasně vypnout ochranu AVG** - Položka umožní jednorázově deaktivovat celou ochranu zajištěnou programem **AVG Internet Security 2012**. Můžete prosím na paměti, že tato volba by v žádném případě neměla být použita, pokud to není opravdu nezbytně nutné! V naprosté většině případů není nutné deaktivovat **AVG Internet Security 2012** před instalací nového software nebo ovladače, a to ani tehdy, pokud budete během instalace vyzváni k zavření všech spuštěných aplikací. Jestliže budete opravdu nuceni deaktivovat **AVG Internet Security 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.
- **Firewall** - Otevře vysunovací nabídku s možnostmi nastavení [Firewallu](#), z níž můžete přímou možnost nejdelší parametry, a to [status Firewallu](#) (*Firewall spuštěn/Firewall zastaven/Pohotovostní režim*), [přepínání herního režimu](#) a [profily Firewallu](#).
- **Testy** - Otevře vysunovací nabídku [přednastavených testů](#) ([Test celého počítače](#) a [Test vybraných souborů a složek](#)) a následnou volbou požadovaný test přímou spustíte.
- **Běžící testy ...** - Tato položka se zobrazuje pouze tehdy, je-li aktuálně spuštěn některý test. U tohoto běžícího testu můžete nastavit jeho prioritu, případně test pozastavit nebo ukončit. K dispozici jsou dále možnosti *Nastavit prioritu pro všechny testy*, *Pozastavit všechny testy* a *Zastavit všechny testy*.
- **Spustit PC Analyzer** - Spustí funkci komponenty [PC Analyzer](#).
- **Aktualizovat** - Spustí okamžitou [aktualizaci AVG Internet Security 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 neproverené 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.

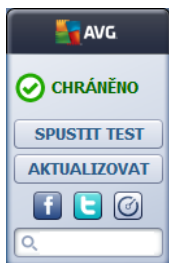
V každé z těchto situací Vás **AVG Advisor** varuje před možným konfliktem a zobrazí jméno a ikonu problematického procesu či aplikace. Dále pak navrhne jednoduché řešení, kterým lze problém předejít.

### 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 Internet Security 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 pozemním rozhraní miniaplikace v jednoduchém statistickém pohledu, kde najdete informace o počtu otestovaných objektů, detekovaných hrozbách a vyloučených hrozbách. V průběhu testu můžete proces testování kdykoliv pozastavit  nebo ukončit . Podrobné informace o výsledku testu pak najdete standardně v dialogu [Pohled výsledk testu](#), který lze z miniaplikace otevřít kliknutím na volbu **Zobrazit detaily** (test bude označen jako *Test z miniaplikace*).




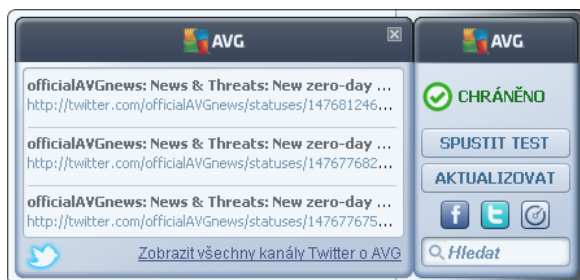
- **Aktualizovat** - Kliknutím na volbu **Aktualizovat** spustíte proces aktualizace **AVG Internet Security 2012** přímo z prostředí miniaplikace:





### Přístup k sociálním sítím


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

- **Twitter**  - Otevírá další rozhraní **Miniaplikace AVG** s p ehledem nejnov jších záznam o AVG uve ejn ných na sociální síti Twitter. Stiskem odkazu **Zobrazit všechny kanály AVG Twitter** otev ete nové okno vašeho internetového prohlíže e a budete p esm rování p ímo 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**.
- **LinkedIn**  - Tato funkce je dostupná pouze v sí ové instalaci (*instalaci s licen ním íslem n které z AVG Business Edicí*) a otevírá internetový prohlíže ě na stránce **AVG SMB Community** v rámci sociální síti LinkedIn.

### Další funkce dostupné z miniaplikace

- **PC Analyzer**  - Otevírá hlavní dialog komponenty [PC Analyzer](#) a rovnou spouští proces analýzy.
- **Vyhledávání** - Zadejte klí ové slovo a výsledky vyhledávání se zobrazí v nov ě otev ěném okn ě prohlíže e, který obvykle používáte.



## 6. Komponenty AVG

### 6.1. Anti-Virus

Komponenta **Anti-Virus** je základním prvkem **AVG Internet Security 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 izolovaném prostředí. Pokud detekuje virus, okamžitě zabrání, aby mohl být aktivován a následně jej odstraní nebo přesune do [Virového trezoru](#).

**Profesionální antivirová ochrana AVG Internet Security 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 Internet Security 2012** kombinaci uvedených technik v rámci jednoho testu. Příkladem může být situace, kdy je virus zachycený skenováním přesně identifikován pomocí heuristické analýzy. **AVG Internet Security 2012** umí také analyzovat spustitelné programy, například DLL knihovny a určí, které z nich by mohly být potenciálně nežádoucí (*jako například spyware, adware aj.*). Na žádost uživatele umožní tyto programy odstranit i k nim zablokovat přístup.

**AVG Internet Security 2012 poskytuje vašemu počítači nepřetržitou ochranu!**



### 6.1.2. Rezidentní ochrana

**AVG Internet Security 2012** Vám zajistí naprosté bezpečí prostřednictvím tak zvané rezidentní ochrany. Komponenta **Anti-Virus** testuje všechny soubory (s určitými výjimkami nebo i bez výjimek), které otvíráte, kopírujete, ukládáte. Kontroluje také systémové oblasti počítače i vyměnitelná média (flash disk 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 váš počítač, čímž je zaručena vaše nepřetržitá a spolehlivá ochrana proti nejnovějším hrozbám. **Anti-Spyware** umožňuje kompletní kontrolu vašeho počítače a detekci případného malware/spyware. **Anti-Spyware** detekuje i tak zvaný "spící" malware, tedy malware, který byl na váš počítač zavlečen, ale dosud nebyl aktivován.

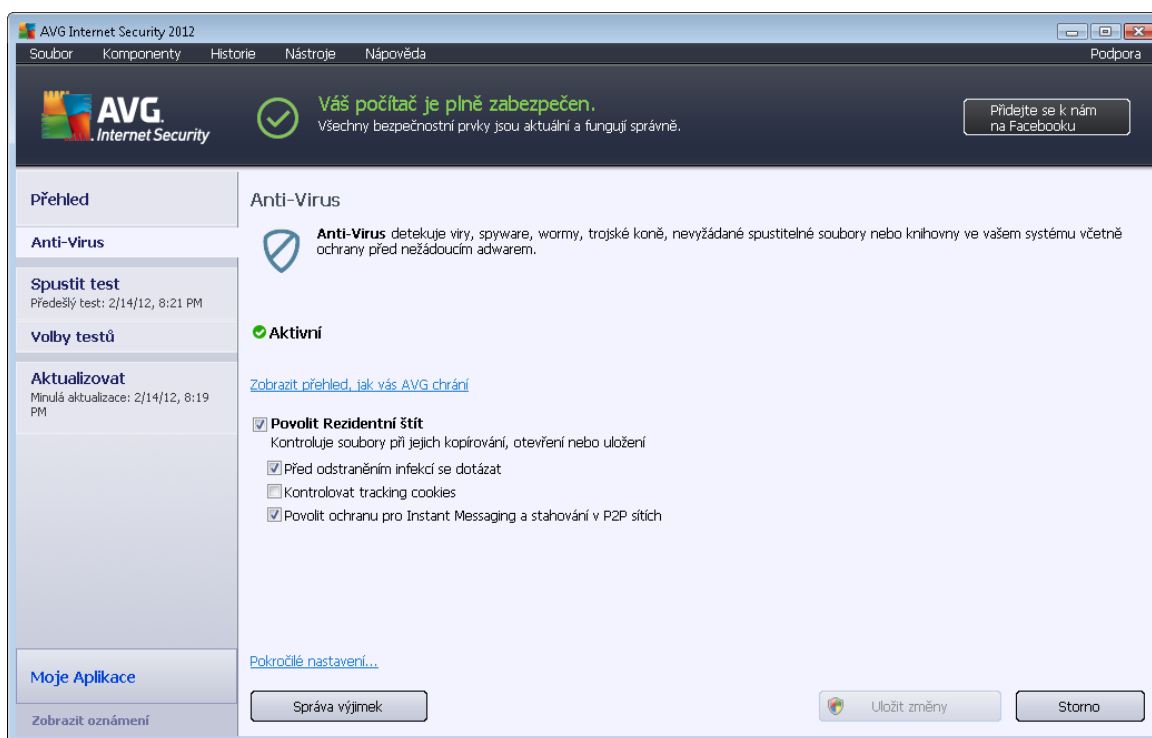
#### Co je to spyware?

Spyware se obvykle definuje jako jeden z typů malware, to jest software, který z vašeho počítače sbírá informace bez vašeho vědomí. Některé aplikace typu spyware mohou být nainstalovány na váš počítač záměrně; 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 Internet Security 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 n kterém z těchto úkonů byl detekován virus, budete o nález okamžitě vyrozuměni. Ve výchozím nastavení je tato funkce zapnutá, a doporučujeme, abyste ji zapnutou ponechali! Pokud se rozhodnete ponechat rezidentní ochranu spuštěnou, máte dále možnost definovat, jak má být s případnou zachycenou infekcí naloženo:
  - **Automaticky odstranit detekované infekce / Před odstraněním infekcí se dotázat** - Ponechejte tuto položku označenou, pokud chcete být při detekci hrozby dotázáni na to, jaké kroky mají být dále podniknuty. V opačném případě bude hrozba



automaticky přesunuta do [Virového trezoru](#). Tato vaše volba nemá žádný vliv na úroveň bezpečnosti a je pouze preferenční.

- **Kontrolovat Tracking Cookies** - Nezávisle na předchozí volbě můžete dále rozhodnout, zda se mají kontrolovat tracking cookies. (*Cookies = malé množství dat v protokolu HTTP, která server pošle prohlížeči, aby je uložil na počítači uživatele. Při každé další návštěvě téhož serveru pak prohlížeč tato data posílá zpět serveru, který podle nich rozlišuje jednotlivé uživatele, například při ukládání obsahu nákupního košíku, atp.*) V odvodněných případech slouží tato možnost k dosažení vyššího stupně bezpečnosti, ve výchozím nastavení je však vypnuta.
- **Povolit ochranu pro Instant Messaging a stahování v P2P sítích** - Označením této položky potvrzujete, že si přejete, aby byla prováděna kontrola okamžité on-line komunikace (*to je komunikace pomocí programů pro okamžité zasílání zpráv, jakými jsou například ICQ, MSN Messenger, Yahoo Messenger ...*).
- **Pokročilé nastavení** - Kliknutím na odkaz budete přesměrováni do příslušného dialogu [Pokročilé nastavení AVG Internet Security 2012](#), kde můžete editovat konfiguraci komponenty do nejmenších podrobností. Mějte však na paměti, že výchozí konfigurace všech komponent **AVG Internet Security 2012** je nastavena tak, aby program podával optimální výkon a poskytoval maximální možnou úroveň bezpečnosti. Pokud nemáte skutečné důvody ke změně, doporučujeme ponechat výchozí nastavení!

## Ovládací tlačítka dialogu

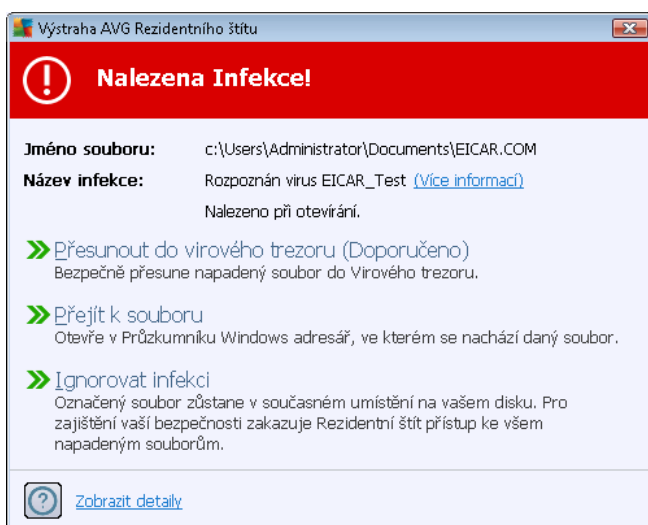
V dialogu jsou dostupné tyto ovládací prvky:

- **Správa Výjimek** - Otevře nový dialog nazvaný **Rezidentní štít - Výjimky**. Editace výjimek Rezidentního štítu je rovněž dostupná prostřednictvím hlavního menu, a to touto cestou: [Pokročilé nastavení / Anti-Virus / Rezidentní štít / Výjimky](#) (*podrobný popis tohoto dialogu najdete v příslušné kapitole*). V tomto dialogu můžete specifikovat soubory nebo adresáře, které mají být vyňaty z kontroly Rezidentním štítem. Pokud to není nezbytně nutné, doporučujeme, abyste z testování žádné položky nevyjímali! V dialogu jsou k dispozici tato ovládací tlačítka:
  - **Přidat cestu** – Umožňuje výběrem z navigačního stromu lokálního disku určit adresáře s celým obsahem, který má být vyňat z testování.
  - **Přidat soubor** – Umožňuje výběrem z navigačního stromu lokálního disku po jednom vybrat další soubory definované jako výjimky z testování.
  - **Editovat** – Umožňuje editovat zadání cesty ke zvolenému souboru nebo adresáři.
  - **Odstranit** – Umožňuje odstranit cestu ke zvolenému souboru nebo adresáři.
  - **Upravit seznam** - Umožňuje upravit celý seznam definovaných výjimek ručně v dialogu, který se chová jako textový editor.
- **Použít** - Uloží všechny změny v nastavení komponenty provedené v tomto dialogu a poté přepne aplikaci do [hlavního dialogu AVG Internet Security 2012](#) (*přehled komponent*).

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

### 6.1.5. Nálezy Rezidentního štítu

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



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

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

- **Léčit** - toto tlačítko se zobrazí pouze v případě, že detekovanou infekci lze léčit. V takovém případě odstraní infekci ze souboru a obnoví soubor do původního stavu. V případě, že soubor jako celek je virus, bude při aplikaci této funkce vymazán (přesunut do [Virového trezoru](#))
- **Přesunout do virového trezoru (Doporučeno)** - infikovaný objekt bude přesunut do karanténního prostředí [Virového trezoru](#)
- **Přejít k souboru** - touto volbou zjistíte, kde je podezřelý objekt fyzicky umístěn (otevře se nové okno Průzkumníka Windows)
- **Ignorovat infekci** - tuto možnost rozhodně nedoporučíme nikomu, kdo nemá skutečně dobrý důvod ji použít!

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





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

### Přehled nálezů Rezidentního štítu

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

Infekce	Objekt	Výsledek	Čas nálezů	Typ objektu	Proces
Rozpoznán virus EIC...	c:\Users\Administrator\...	Infikováno	2/14/2012, 8:24:06 PM	Soubor	C:\Wind

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 (popis a 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).

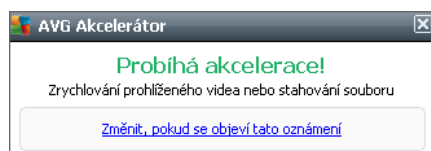
## 6.2. LinkScanner

**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 náhodou technologie **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 tyto hlavní funkce:

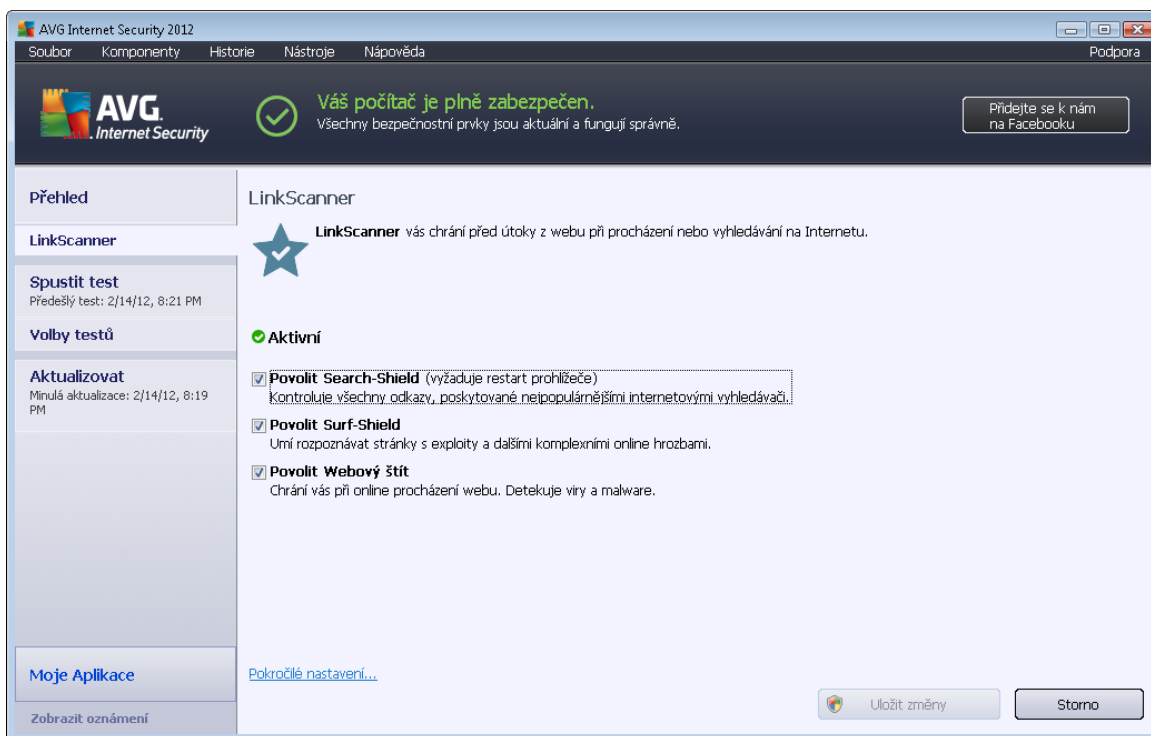
- **Search-Shield** obsahuje seznam stránek (*URL adresy*), které jsou známy jako infikované. Při hledání skrze vyhledávače Google, Yahoo! JP, eBay, Twitter, Digg, SlashDot, bezpečné vyhledávání AVG, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, a SlashDot jsou všechny výsledky zkontrolovány na základě tohoto seznamu a ke každé položce je zobrazena verdiktová ikona (*pro výsledky ve vyhledávači Yahoo! JP jsou zobrazeny tyto verdiktové ikony pouze pro infikované stránky*).
- **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 a v případě, že při jeho navštívění detekuje virus nebo spyware, okamžitě zabrání jejich stažení.
- **AVG Accelerator** umožňuje plynulé přehrávání videa v režimu online a obecně urychluje stahování. O tom, že je proces akcelerace videa při stahování momentálně aktivní, budete informováni prostřednictvím pop-up okna nad systémovou lištou:





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






**Výchozí konfigurace AVG Internet Security 2012 je nastavena k optimálnímu výkonu programu. Proto doporučujeme výchozí nastavení ponechat, pokud nemáte skutečně dobrý důvod, aby tomu bylo jinak.**

### 6.2.2. Nálezy služby Search-Shield

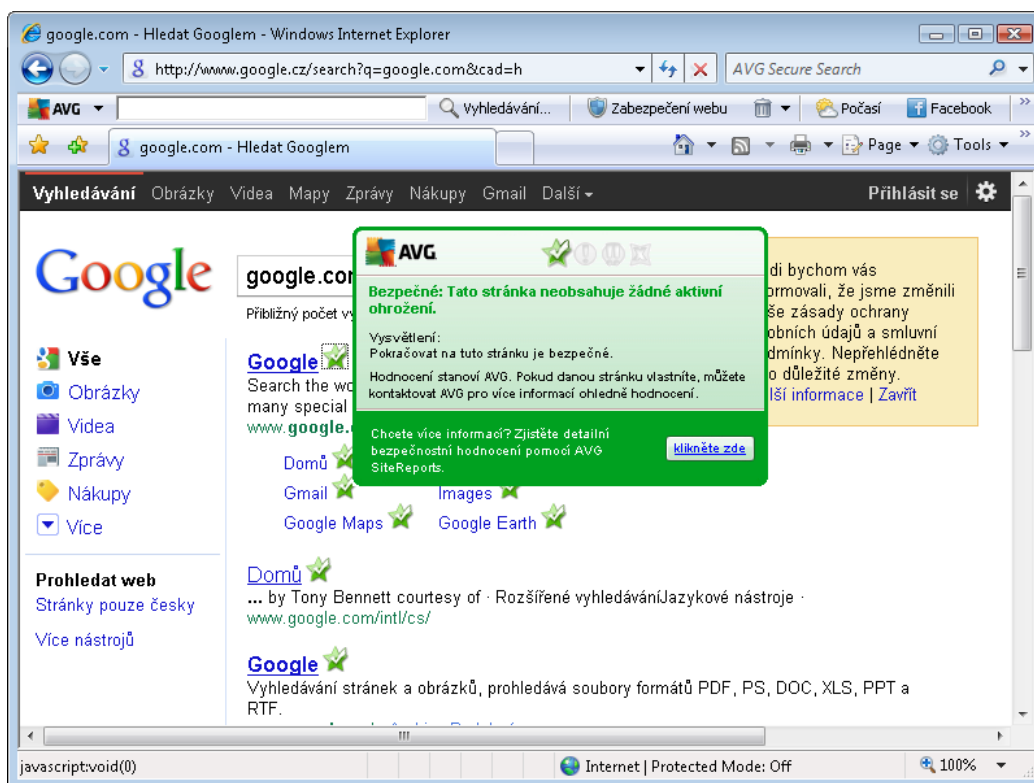
Při prohlížení Internetu se zapnutou kontrolou **Search-Shield** budou všechny výsledky vyhledávání pomocí nejrozšířenějších vyhledávačů (*Google, Yahoo!, bezpečné vyhledávání AVG, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask a Seznam*) vyhodnoceny z hlediska bezpečnosti a rozděleny na odkazy bezpečné a nebezpečné. Označením jednotlivých odkazů grafickými ikonami vás [LinkScanner](#) varuje před vstupem na nebezpečnou nebo podezřelou stránku. Během vyhodnocování jednotlivých odkazů vrácených jako výsledky vyhledávání uvidíte u každého odkazu grafický symbol



oznaující 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 provozitel, proto ji nelze doporučit například pro aktivity typu on-line nakupování a podobně).
-  Odkazovaná stránka může být sama o sobě bezpečná, ale obsahuje odkazy na jiné nebezpečné stránky. Nebo jde o stránku s podezřelým kódem.
-  Odkazovaná stránka obsahuje aktivní hrozby! Pro vlastní bezpečnost vám nebude umožněno na tuto stránku vstoupit.
-  Odkazovaná stránka je nepřístupná a nemohla tedy být prověřena.

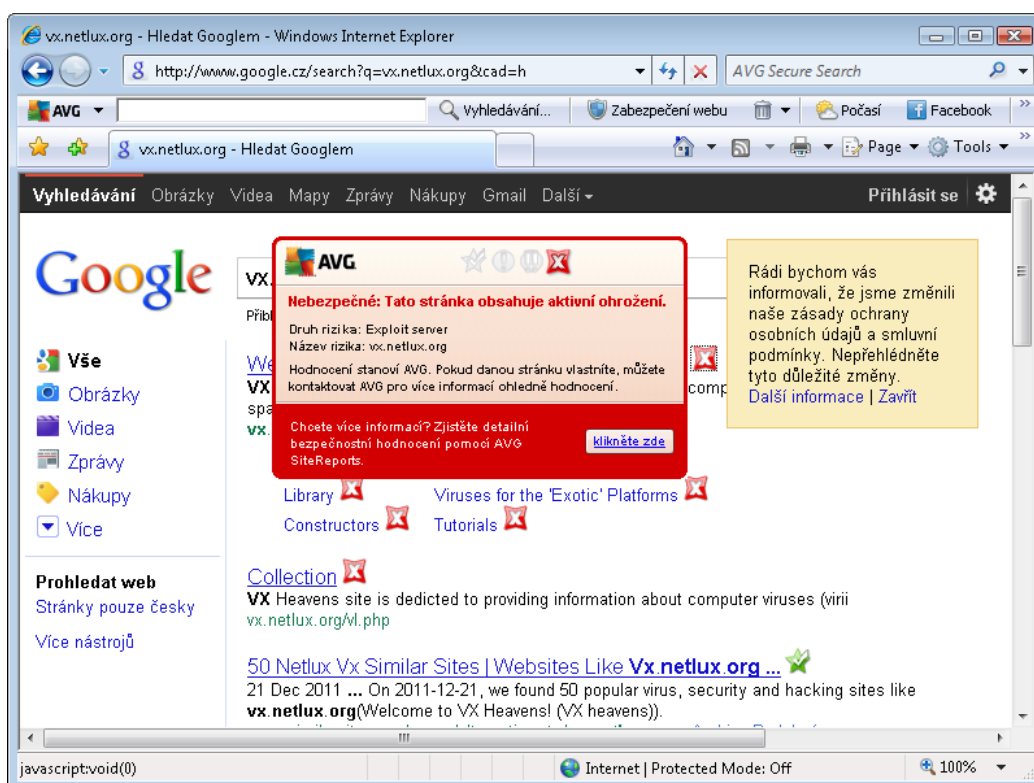
Při přejetí myší nad jednotlivými ikonami s hodnocením bezpečnosti odkazu se pak zobrazí detailní informace (podrobnosti o hrozbě, pokud byla nalezena, IP adresa odkazu a datum kontroly odkazu službou AVG Search-Shield) o odkazu:



### 6.2.3. Nález 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.

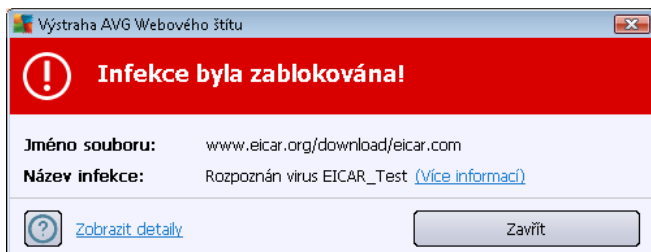
Narazíte-li na nebezpečnou webovou stránku, **LinkScanner** vás bude varovat tímto oznámením:



**Vstup na takto označenou stránku rozhodně nedoporučujeme!**

### 6.2.4. Nález Webového štítu

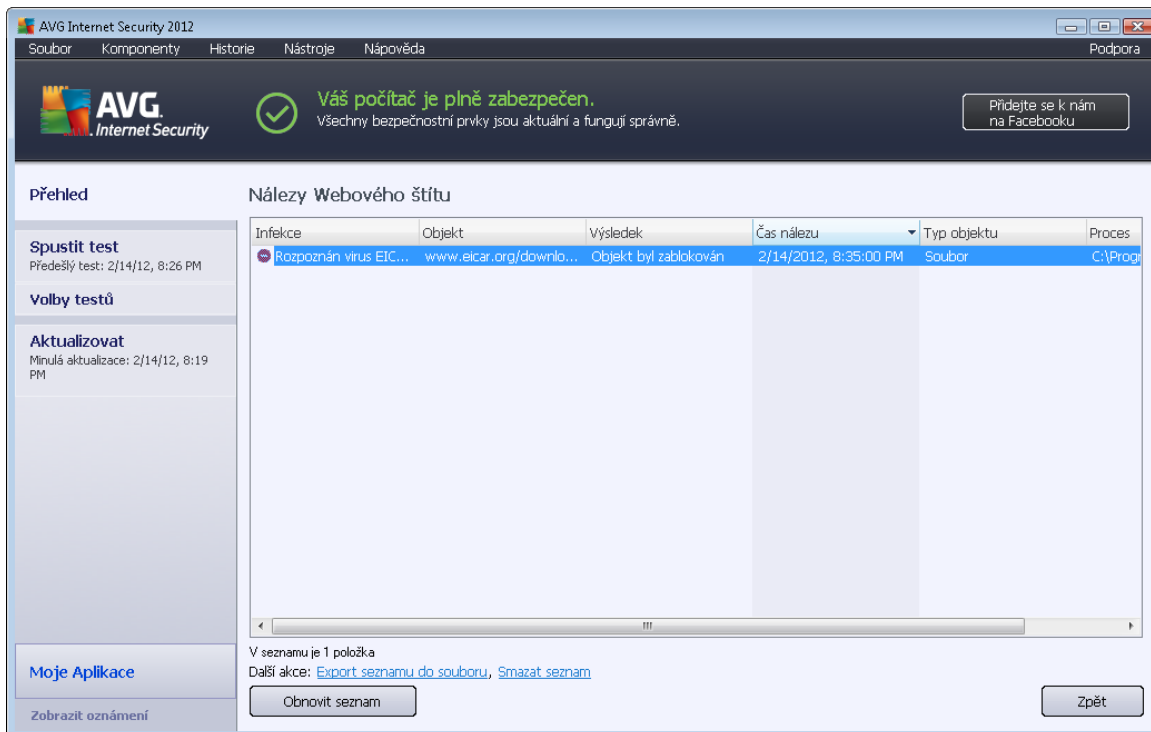
**Webový štít** kontroluje v reálném čase obsah webových stránek nebo souborů stahovaných z Internetu. Každá stránka je prověřena ještě předtím, než je skutečně stažena a zobrazena webovým prohlížečem. Jestliže detekuje virus nebo jakýkoliv podezřelý objekt, budete okamžitě varováni tímto dialogem:



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

- **Zobrazit detaily** - kliknutím na tlačítko otevře nové pop-up okno s informací o procesu, při němž došlo k detekci infekce, a s uvedeným identifikačním číslem procesu.
- **Zavřít** - tímto tlačítkem varovný dialog zavěte.

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



U každého z detekovaných objektů jsou k dispozici následující informace:

- **Infekce** - popis (případně i jméno) detekovaného objektu
- **Objekt** - umístění detekovaného objektu (*stránka, odkud byl objekt stažen*)



- **Výsledek** - jak bylo s detekovaným objektem naloženo (*blokáce*)
- **as nález** - datum a čas, kdy došlo k detekci hrozby
- **Typ objektu** - jakého typu je detekovaný objekt
- **Proces** - při jaké akci byl objekt detekován

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

### Ovládací tlačítka

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

## 6.3. E-mailová ochrana

Jedním z nejčastějších zdrojů virů a trojských koní je e-mail. A díky phishingu a spamu se e-mail stává ještě v těmto zdrojům nebezpečí. Toto nebezpečí narůstá obzvláště u zdarma dostupných poštovních účtů (*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 těmto společnostech v těsnou spolupráci používají firemní poštovní účty a snaží se riziko minimalizovat implementací anti-spamových filtrů.

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

- [Kontrola příchozí a odchozí pošty](#)
- [Anti-Spam kontrola](#)

### 6.3.1. Kontrola pošty

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

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

**Kontrola pošty není určena k ochraně poštovních serverů !**

## 6.3.2. Anti-Spam

### Jak funguje Anti-Spam?

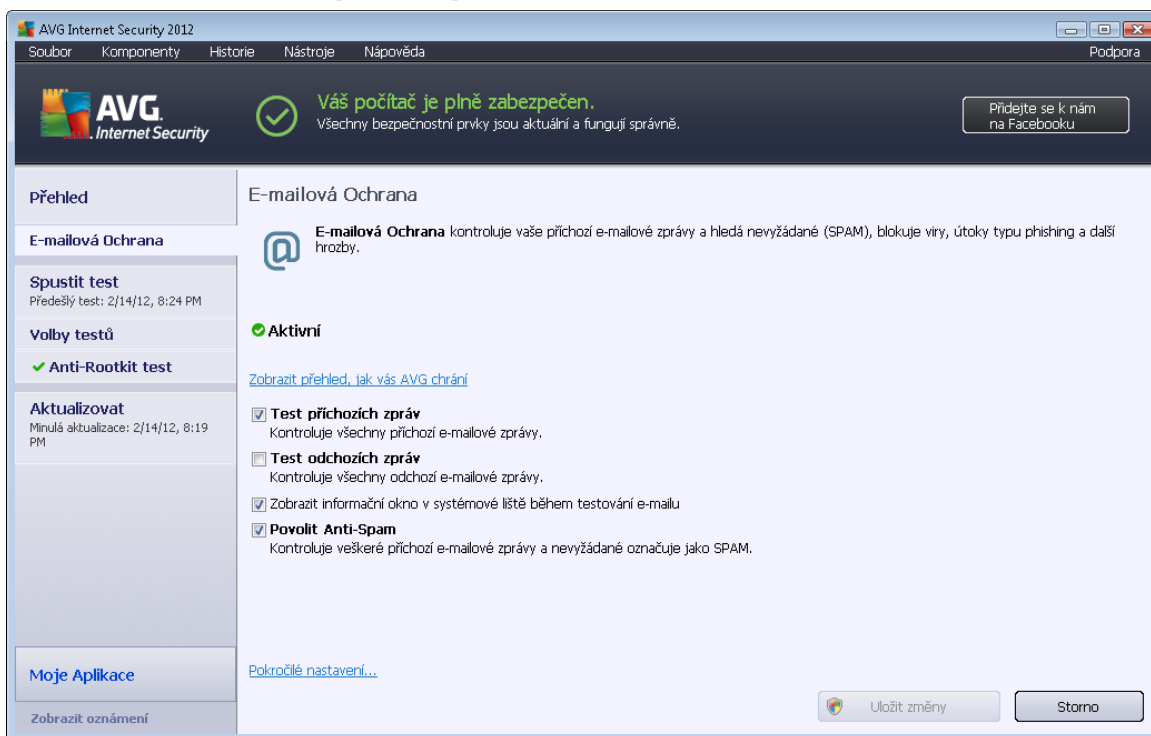
**Anti-Spam** kontroluje veškerou příchozí poštu a nežádoucí zprávy označuje jako spam. **Anti-Spam** dokáže upravit předmět emailu, který je identifikován jako spam, přidáním vámi definovaného textového přetvácení. Poté již můžete snadno filtrovat emaily podle definovaného označení ve vašem poštovním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

### Co je to spam?

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



### 6.3.3. Rozhraní komponenty E-mailová ochrana



V dialogu **E-mailová ochrana** najdete stručný popis funkce komponenty a informaci o aktuálním stavu komponenty (*Aktivní*). Prostřednictvím odkazu **Zobrazit online přehled, jak Vás AVG chrání** se můžete přepnout na dedikovanou stránku na webu AVG (<http://www.avg.cz/>), kde najdete detailní statistiku aktivity a detekcí **AVG Internet Security 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.
- **Povolit Anti-Spam** (ve výchozím nastavení zapnuto) - Označením položky určíte, zda si přejete provádět filtraci nežádoucích zpráv v příchozí poště.

**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 měli provádět pouze zkušení uživatelé. Chcete-li tedy**



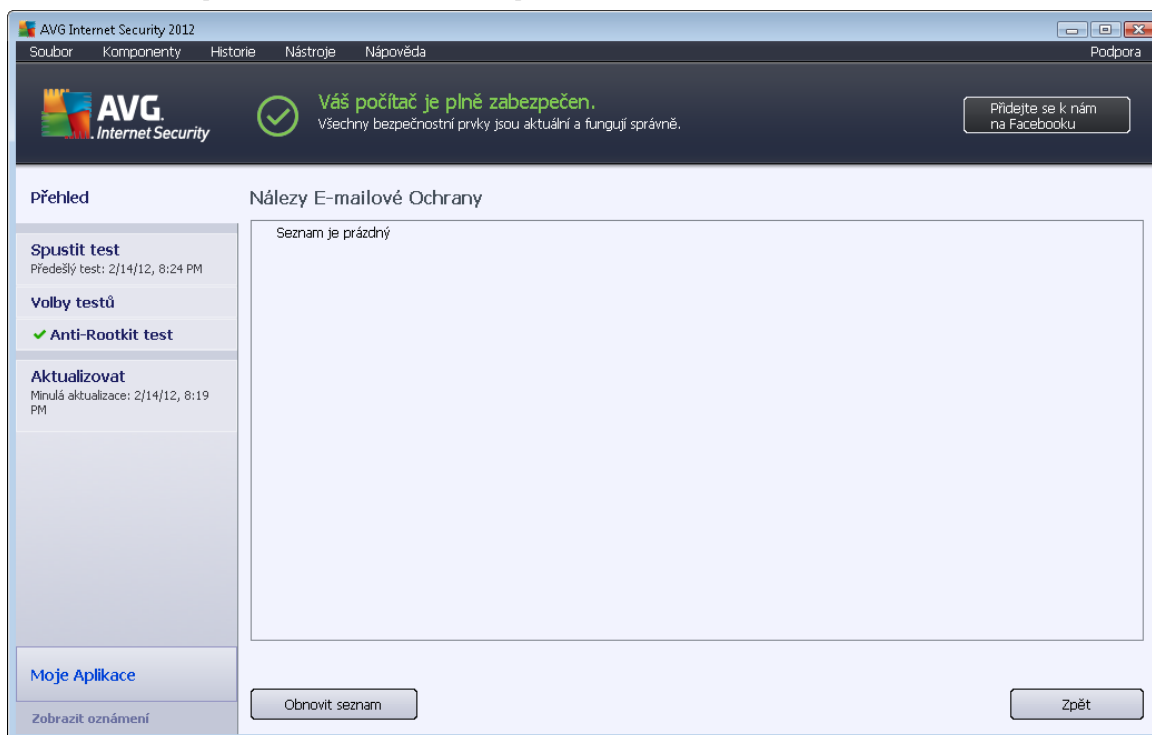
zm nit nastavení programu AVG, zvolte ze systémového menu položku **Nástroje / Pokro** ilé nastavení a editaci nastavení prove te v nov oteveném dialogu [Pokro ilé nastavení AVG](#).

### 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)

### 6.3.4. Nález E-mailové ochrany



V dialogu **Nález Kontroly pošty** (dostupném ze systémového menu volbou položek **Historie / Nález Kontroly pošty**) se bude zobrazovat seznam nález 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 **Nálezů Kontrola pošty**:

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

## 6.4. Firewall

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

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

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

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

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

### 6.4.1. Princip Firewallu

V rámci **AVG Internet Security 2012** řídí komponenta **Firewall** veškerý provoz na všech síťových portech vašeho počítače. Podle předem nastavených pravidel vyhodnocuje jednak aplikace, které běžně běží na vašem počítači (a pokoušejí se o komunikaci do sítě internetu nebo do lokální sítě), a také aplikace, které se snaží navázat komunikaci s vaším počítačem zvenčí. Každé z těchto aplikací **Firewall** komunikaci na síťových portech buďto povolí nebo zakáže. Ve výchozím nastavení platí, že pokud jde o neznámou aplikaci (tedy aplikaci, pro niž ještě nebylo v rámci Firewallu definováno pravidlo), **Firewall** se zeptá, zda si přejete tento pokus o komunikaci povolit nebo zablokovat.



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

### Co umí AVG Firewall

- Automaticky povoluje nebo blokuje pokusy o komunikaci [aplikacím](#), pro něž má definované pravidlo, nebo se dotáže a požádá o potvrzení volby
- Pracuje s [profily](#) nastavenými podle definovaných pravidel, jež reflektují vaše potřeby
- Automaticky [přepíná profily](#) podle aktuálního připojení k síti nebo podle aktuálně použitých síťových adaptérů

### 6.4.2. Profily Firewallu

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

#### Dostupné profily

- **Povolit vše** - systémový profil **Povolit vše** je přednastaveným profilem a je k dispozici za všech okolností. Jestliže je tento profil aktivován, je povolena veškerá komunikace a nejsou uplatňována žádná bezpečnostní pravidla, jako kdyby byl [Firewall](#) vypnutý (*tj. jsou povoleny všechny aplikace, ale kontrola na bázi paketů stále probíhá - chcete-li zcela zrušit jakékoliv filtrování, je nutné Firewall vypnout*). Tento systémový profil nelze duplikovat, smazat ani modifikovat.
- **Blokovat vše** - systémový profil **Blokovat vše** je přednastaveným profilem a je k dispozici za všech okolností. Jestliže je tento profil aktivován, je veškerá komunikace zakázána a počítač není dostupný z vnějších sítí ani sám nemůže žádnou komunikaci s externími servery navázat. Tento systémový profil nelze duplikovat, smazat ani modifikovat.
- **Uživatelské profily** - uživatelské profily umožní využít automatického přepínání profilů, což je obzvláště užitečné při přechodu z počítače do různých sítí (*například s notebookem*). Uživatelské profily se generují automaticky bezprostředně po dokončení instalace **AVG Internet Security 2012** a pokrývají veškeré individuální potřeby v rámci pravidel [Firewallu](#). K dispozici jsou tyto uživatelské profily:
  - **Přímé připojení k Internetu** – vhodný pro běžné domácí počítače připojené přímo k Internetu nebo notebooky používané mimo chráněnou firemní síť. Tato alternativa je rovněž vhodná pro připojení pomocí notebooku z různých neznámých a pravděpodobně naprosto nezabezpečených míst (*internetová kavárna, hotelový pokoj atd.*). Budou využita poměrně restriktivní pravidla, protože se nedá předpokládat přítomnost dalších bezpečnostních opatření a úkolem [Firewallu](#) je zajistit pokud možno co nejvyšší úroveň ochrany uživatele.
  - **Počítač v doméně** – vhodný pro počítače v lokální síti, například ve škole nebo ve



firm . Dá se p edpokládat, že taková sí je chrán na dalšími prost edky (*nap íklad softwarovým nebo hardwarovým firewallem*) a úrove její bezpe nosti je vyšší než u samostatn p ípojeného po íta e. Proto budou nastavená pravidla mén restriktivní a povolí nap íklad p ístup ke sdíleným adresám, diskovým jednotkám a podobn .

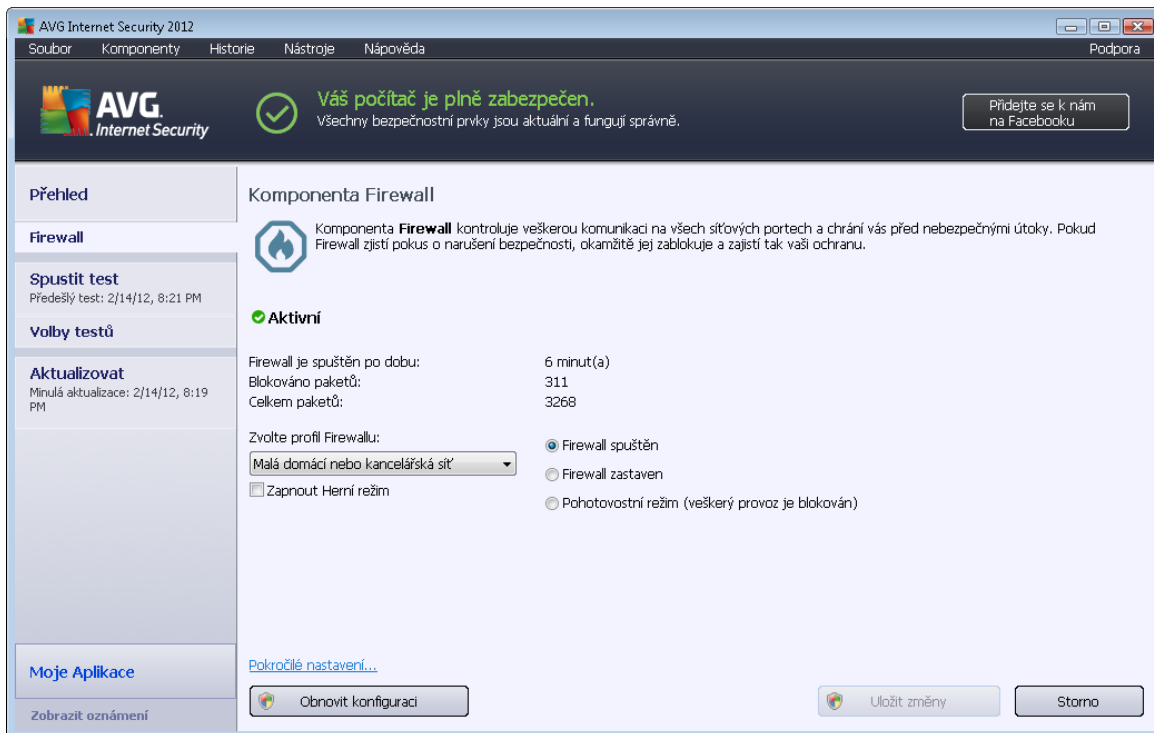
- o **Malá domácí nebo kancelá ská sí** – vhodný pro po íta e v malé síti, nap íklad doma nebo v menší firm . Typicky se jedná jen o n kolik propojených po íta bez možnosti centrální správy, které ásto sdílejí tiskárnu, scanner nebo podobné za ízení, a pravidla [Firewallu](#) musí tento stav zohlednit.

### P epínání profil

Funkce p epínání profil umož ňuje [Firewallu](#) p í použití ur ítého sí ového adaptéru nebo p í p ípojení k ur íté síti automatické p epnutí na definovaný profil. Pokud nebyl dané oblasti síti dosud žádný profil p íazen, pak bude p í p íštím p ípojení k této oblasti zobrazen dialog Firewallu, v n mž budete vyzváni k p íazení profilu. Profily m žete p íazovat všem lokálním sí ovým rozhraním nebo oblastem a podrobné nastavení pak definovat v dialogu [Profily sítí a adaptér](#) , kde lze tuto vlastnost také zcela vypnout, pokud ji nechcete používat (*pak bude pro jakékoli p ípojení použit výchozí profil*).

Dá se p edpokládat, že této vlastnosti využijí uživatelé s notebookem, kte í se p ípojují k mnoha r zným sítím. Používáte-li nep enosný stolní po íta a jste p ípojení vždy stejným typem p ípojení (*nap íklad kabelovým p ípojením k Internetu*), nemusíte se p epínáním profil v podstat v bec zabývat.

### 6.4.3. Rozhraní komponenty Firewall



Hlavní dialog nazvaný **Komponenta Firewall** nabízí krom základních informací o funkci



komponenty a jejím aktuální stavu (*Aktivní*) také stručný statistický přehled:

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

### Základní nastavení Firewallu

- **Zvolte profil Firewallu** - v rozbalovací nabídce zvolte jeden z definovaných profilů (*podrobný popis jednotlivých profilů a jejich doporučeného použití najdete v kapitole [Profily Firewallu](#)*)
- **Zapnout Herní režim** - chcete-li zajistit, aby v průběhu práce s aplikacemi, jež běží na celé obrazovce (*hry, prezentace, filmy atd.*) [Firewall](#) nezobrazoval dialogy s dotazy na povolení či zablokování komunikace u neznámých aplikací, označte tuto položku. Je-li tato volba zapnuta a dojde k situaci, kdy se neznámá aplikace pokusí navázat síťovou komunikaci, [Firewall](#) tento pokus zablokuje a povolí automaticky podle nastavení v aktuálním použitém profilu. **Upozornění:** Je-li herní režim zapnutý, bude spuštění všech naplánovaných úloh (*test, aktualizací*) pozastaveno do doby, než bude aplikace ukončena.
- Dále máte v sekci základního nastavení možnost volby ze tří alternativ určujících aktuální stav komponenty [Firewall](#):
  - **Firewall spuštěn (výchozí nastavení)** - touto volbou umožníte komunikaci těm aplikacím, pro něž je v pravidlech definovaných v rámci zvoleného profilu [Firewall](#) provoz povolen.
  - **Firewall zastaven** - touto volbou vypnete [Firewall](#), veškerý síťový provoz je povolen a není kontrolován!
  - **Pohotovostní režim (veškerý provoz je blokován)** - touto volbou můžete v případě potřeby zastavit veškerý provoz na všech síťových portech; [Firewall](#) zůstává spuštěn, ale veškerý síťový provoz je blokován.

**Poznámka:** Všechny komponenty AVG Internet Security 2012 jsou výrobcem nastaveny k optimálnímu výkonu. Pokud nemáte skutečný důvod jejich konfiguraci změnit, doporučujeme ponechat program ve výchozím nastavení. Změnu konfigurace by měli provádět pouze zkušení uživatelé. Chcete-li tedy změnit nastavení komponenty Firewall, zvolte ze systémového menu položku **Nástroje/Nastavení Firewallu** a editaci nastavení proveďte v nově otevřeném dialogu [Nastavení Firewallu](#).

### Ovládací tlačítka

- **Obnovit konfiguraci** - stiskem tlačítka přepíšete aktuální konfiguraci komponenty [Firewall](#) a vrátíte se k výchozí konfiguraci nastavené na základě automatické detekce.
- **Uložit změny** - stiskem tlačítka budou uloženy všechny v tomto dialogu provedené změny.



- **Storno** - stiskem tlačítka se vrátíte do výchozího [hlavního dialogu AVG](#) (přehled komponent).

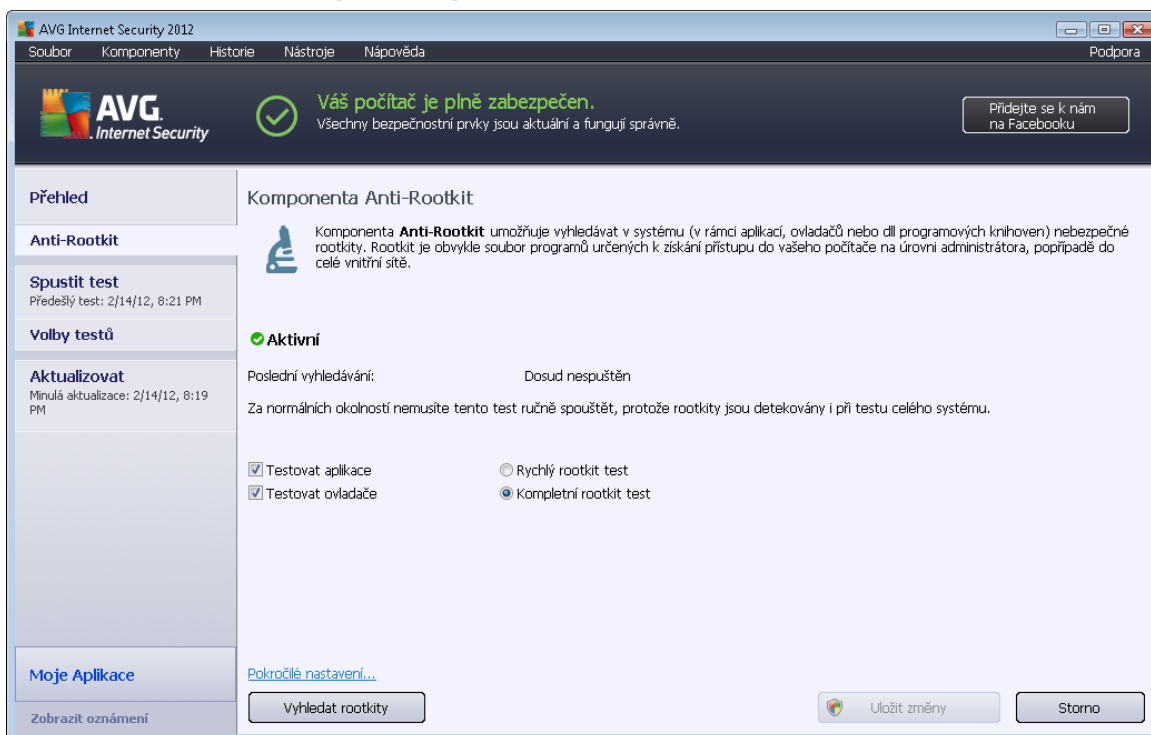
## 6.5. Anti-Rootkit

**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 nálezům 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 tichosti se nepokouší ovládnout hardware, jejich cílem je ovládnout váš operační systém. Rootkity umožňují skrývat běžící procesy, soubory a systémové údaje a upravují tedy operační systém tak, aby nebyly běžnými prostředky uživatele zjistitelné. Rootkity mají ve své škodlivého kódu poměrně výsadní postavení, jelikož pronikají hluboko do systému, přebírají požadavky systémových volání a správné výsledky nahrazují svými vlastními.

### 6.5.1. 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 označím 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).

## 6.6. Systémové nástroje

**Systémovými nástroji** jsou nyní nástroje pro detailní přehled prostředí **AVG Internet Security 2012** a operačního systému. Komponenta zobrazuje tyto informace:

- [Procesy](#) - seznam procesů (např. aplikací), které jsou momentálně aktivní na Vašem počítači
- [Síťová připojení](#) - seznam momentálně aktivních spojení
- [Pospuštění](#) - seznam všech aplikací, které jsou spuštěny během startu operačního





systému Windows

- [Rozšíření prohlíže](#) - seznam dopl k (aplikací), které jsou nainstalovány do Vašeho internetového prohlíže e
- [Prohlíže LSP](#) - seznam LSP (Layered Service Provider)

**Jednotlivé p ehledy je možné i editovat, ale tuto editaci doporu ujeme pouze opravdu zkušeným uživatel m!**

### 6.6.1. Procesy

Úroveň závažnosti	Název procesu	Cesta k procesu	Okno	PID
■□□□	SYSTEM	SYSTEM		4
■□□□	WMIPRVSE.EXE	C:\WINDOWS\SYSTEM32\WBEM\WMIPRVSE.EXE		172
■□□□	MSDTC.EXE	C:\WINDOWS\SYSTEM32\MSDTC.EXE		3644
■□□□	SMSS.EXE	C:\WINDOWS\SYSTEM32\SMSS.EXE		396
■□□□	VMWARETRAY.EXE	C:\PROGRAM FILES\VMWARE\VMWARE TOOLS\VMWARETRAY.EXE		420
■□□□	AVGRSX.EXE	C:\PROGRAM FILES\AVG\AVG2012\AVGRSX.EXE		432
■□□□	AVGCSRFX.EXE	C:\PROGRAM FILES\AVG\AVG2012\AVGCSRFX.EXE		472
■□□□	VMWAREUSER.EXE	C:\PROGRAM FILES\VMWARE\VMWARE TOOLS\VMWAREUSER.EXE		644
■□□□	AVGTRAY.EXE	C:\PROGRAM FILES\AVG\AVG2012\AVGTRAY.EXE		660
■□□□	VPROT.EXE	C:\PROGRAM FILES\AVG SECURE SEARCH\VPROT.EXE		668
■□□□	SIDEBAR.EXE	C:\PROGRAM FILES\WINDOWS\SIDEBAR\SIDEBAR.EXE		680

Dialog **Procesy** obsahuje seznam proces (tj. spušt ných aplikací), které jsou v sou asné dob na vašem počítači aktivní. Seznam obsahuje n kolik sloupc :

- **Úroveň závažnosti** – grafické zobrazení závažnosti b žícího procesu na ty stup ové v rozptí mén významný (■□□□) až kritický (■□□■)
- **Název procesu** – jméno spušt ného procesu
- **Cesta k procesu** – fyzická cesta ke spušt nému procesu
- **Okno** – pokud se vztahuje na daný proces, ukazuje název okna aplikace
- **PID** - identifika ní íslo procesu je jedine ným identifikátorem interního procesu systému Windows



## Ovládací tlačítka

Ovládací tlačítka dostupná v tabulce **Procesy**:

- **Obnovit seznam** - aktualizuje seznam procesů podle momentálního stavu
- **Ukončit proces** - v seznamu můžete vybrat jednu nebo více aplikací a následně je ukončit stisknutím tohoto tlačítka. **Doporučujeme, abyste neukončili žádné aplikace, pokud si nejste naprosto jisti, že představují skutečnou hrozbu!**
- **Zpět** - přejdete zpět do výchozího [hlavního dialogu AVG](#) (přehled komponent)

## 6.6.2. Síťová připojení

Aplikace	Protokol	Místní adresa	Vzdálená adresa	Stav
[Systémový proces]	TCP	AutoTest-VST32:139	AutoTest-VST32:0	Poslouchá
[Systémový proces]	TCP	AutoTest-VST32:445	AutoTest-VST32:0	Poslouchá
[Systémový proces]	TCP6	[0:0:0:0:0:0:0:0]:445	[0:0:0:0:0:0:0:0]:0	Neznámý
[Systémový proces]	UDP	AutoTest-VST32:138		
[Systémový proces]	UDP	AutoTest-VST32:137		
[Systémový proces]	TCP	AutoTest-VST32:49184	192.168.183.1:445	Navázáno
[Systémový proces]	TCP6	[0:0:0:0:0:0:0:0]:5357	[0:0:0:0:0:0:0:0]:0	Neznámý
[Systémový proces]	TCP	AutoTest-VST32:5357	AutoTest-VST32:0	Poslouchá
wininit.exe	TCP6	[0:0:0:0:0:0:0:0]:49152	[0:0:0:0:0:0:0:0]:0	Neznámý
wininit.exe	TCP	AutoTest-VST32:49152	AutoTest-VST32:0	Poslouchá
svchost.exe	UDP6	[0:0:0:0:0:0:0:0]:500		
svchost.exe	UDP	AutoTest-VST32:500		
svchost.exe	UDP	AutoTest-VST32:1900		
svchost.exe	UDP	AutoTest-VST32:5355		
svchost.exe	UDP6	[0:0:0:0:0:0:0:0]:5355		
svchost.exe	UDP	AutoTest-VST32:57829		
svchost.exe	UDP	AutoTest-VST32:3702		
svchost.exe	TCP6	[0:0:0:0:0:0:0:0]:49156	[0:0:0:0:0:0:0:0]:0	Neznámý

Dialog **Síťová připojení** obsahuje seznam v daném okamžiku aktivních připojení. Seznam je rozdělen do několika sloupců:

- **Aplikace** - název aplikace, ke které se vztahuje dané připojení (s výjimkou OS Windows 2000, kde se informace nezobrazuje)
- **Protokol** - typ přenosového protokolu, který je pro připojení využíván:
  - TCP – protokol používaný ve spojení s protokolem IP (*Internet Protocol*) k přenosu informací po internetu
  - UDP – alternativa protokolu TCP



- **Místní adresa** - IP adresa lokálního počítače a aktuálně používané číslo portu
- **Vzdálená adresa** - IP adresu vzdáleného počítače a číslo portu, ke kterému se připojuje. Je-li to možné, vyhledá také jméno hostitele vzdáleného počítače.
- **Stav** – nejpravděpodobnější stávající stav připojení (*Spojeno, Server by se měl odpojit, Probíhá přímá, Aktivní uzavření dokončeno, Pasivní uzavření, Aktivní uzavření*)

Chcete-li v přehledu zobrazit pouze externí připojení, označte volbu **Skrýt místní spojení** dole pod seznamem.

## Ovládací tlačítka

Ovládací tlačítka dostupná v tabulce **Síťová připojení**:

- **Ukončit spojení** – ukončí jedno (nebo více) zvolených připojení
- **Ukončit proces** – ukončí jednu (nebo více) aplikací, které se vztahují ke spojení zvolenému v seznamu připojení
- **Zpět** - přejdete zpět do výchozího [hlavního dialogu AVG](#) (přehled komponent)

**N kdy je možné ukončit pouze aplikace, které jsou aktuálně ve stavu připojení. Doporuujeme, abyste neukončili žádné spojení, pokud si nejste naprosto jisti, že připojení představuje skutečnou hrozbu!**

## 6.6.3. Po spuštění

Název	Umístění	Cesta
WindowsWelcomeCenter	\REGISTRY\USER\S-1-5-20\Software\Micro...	rundll32.exe oobefldr.dll,ShowWelcomeCen...
Sidebar	\REGISTRY\USER\S-1-5-20\Software\Micro...	%ProgramFiles%\Windows Sidebar\Sidebar...
vProt	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Program Files\AVG Secure Search\vprot...
WindowsWelcomeCenter	\REGISTRY\USER\S-1-5-19\Software\Micro...	rundll32.exe oobefldr.dll,ShowWelcomeCen...
C:\Windows\system32\mshta.exe "%1"...	\REGISTRY\MACHINE\SOFTWARE\Classes...	C:\Windows\system32\mshta.exe "%1" %*
SilkTest Agent	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Automation\startagent.bat"
AVG_TRAY	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Program Files\AVG\AVG2012\avgtray.exe"
VMware User Process	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Program Files\VMware\VMware Tools\V...
Sidebar	\REGISTRY\USER\S-1-5-21-2323238519-...	C:\Program Files\Windows Sidebar\sidebar.e...
SHELL	\INI\system.ini\BOOT\SHELL	SYSTEM32\Windows NT\CurrentVersion...
VMware Tools	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Program Files\VMware\VMware Tools\V...
hffsrsv	\REGISTRY\MACHINE\SOFTWARE\Microso...	c:\windows\hffext\hffsrsv.exe
Adobe Reader Speed Launcher	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Program Files\Adobe\Reader 8.0\Reade...
Sidebar	\REGISTRY\USER\S-1-5-19\Software\Micro...	%ProgramFiles%\Windows Sidebar\Sidebar...
AppInit_DLLs	\REGISTRY\MACHINE\SOFTWARE\Microso...	qaphooks.dll



Dialog **Po spuštění** zobrazuje seznam všech aplikací, které jsou spuštěny automaticky při spuštění systému Windows. Často se stává, že se na některé typy škodlivého software zapisují do registru práva při spuštění.

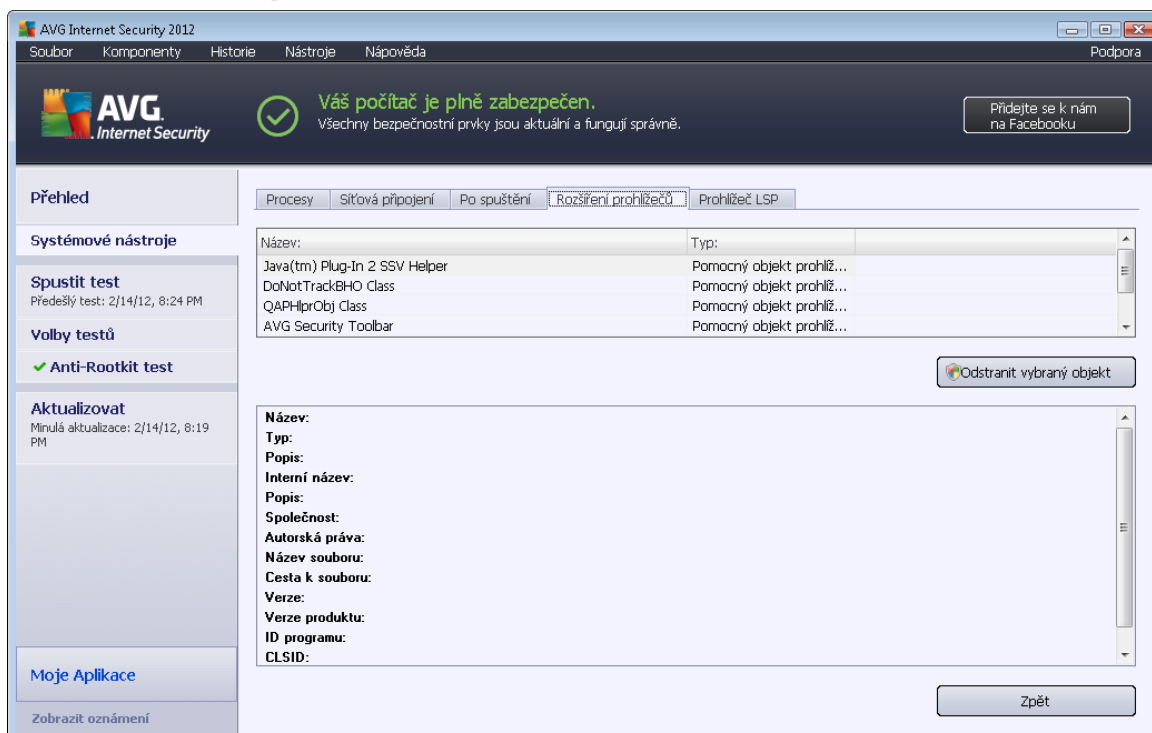
### Ovládací tlačítka

Ovládací tlačítka dostupná v tabulce **Po spuštění**:

- **Odstranit označené** - Tímto tlačítkem lze po označení vymazat jeden nebo více zápisů.
- **Zpět** - Přejdete zpět do výchozího [hlavního dialogu AVG](#) (přehled komponent).

**Doporučujeme, abyste ze seznamu neodstraňovali žádné aplikace, pokud si nejste naprosto jisti, že představují skutečnou hrozbu!**

### 6.6.4. Rozšíření prohlížečů



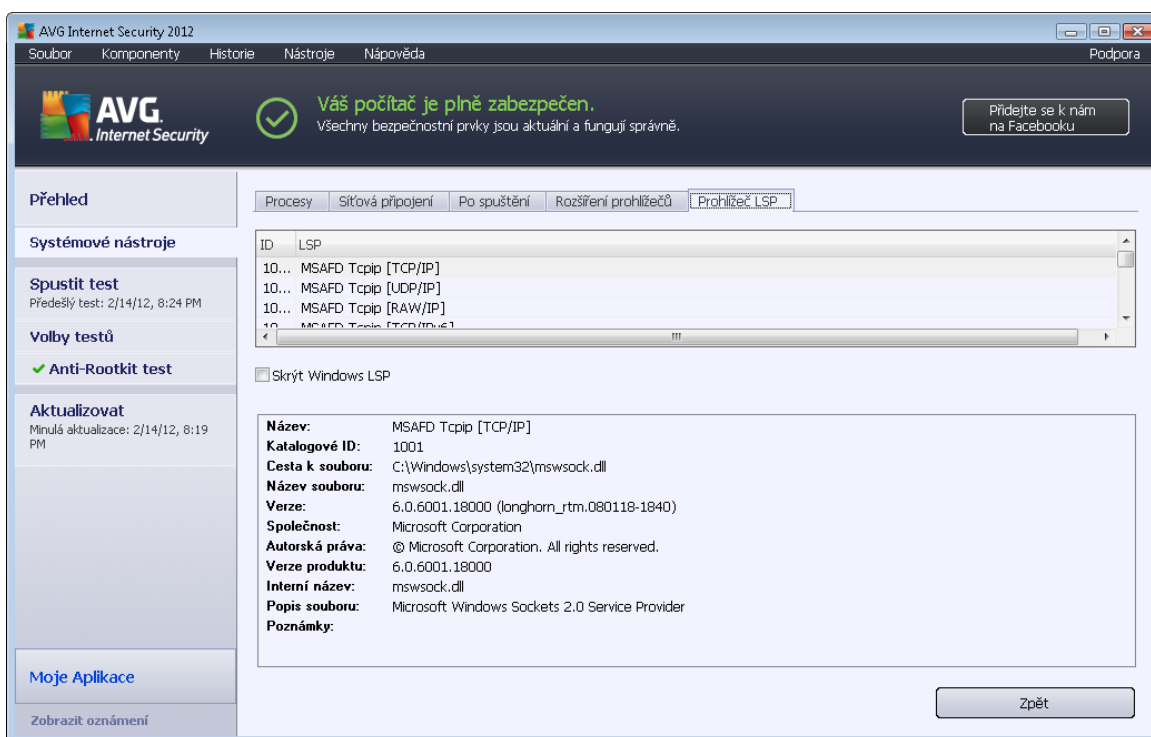
Dialog **Rozšíření prohlížečů** obsahuje seznam doplňků (tj. aplikací), které jsou nainstalovány ve vašem internetovém prohlížeči. Tento seznam může obsahovat standardní doplňky, ale také potenciálně škodlivý software. Kliknutím na konkrétní objekt v seznamu se ve spodní části dialogu zobrazí přehled detailních informací o konkrétním doplňku.

### Ovládací tlačítka dialogu

Ovládací tlačítka dostupná v záložce **Rozšíření prohlížeče** :

- **Odstranit vybraný objekt** - odstraní ze seznamu ten doplněk, který je momentálně označen. **Doporučujeme, abyste ze seznamu neodstraňovali žádné doplňky, pokud si nejste naprosto jisti, že představují skutečnou hrozbu!**
- **Zpět** - pojedete zpět do výchozího [hlavního dialogu AVG](#) (přehled komponent)

### 6.6.5. Prohlížeč LSP



Dialog **Prohlížeč LSP** zobrazuje seznam Layered Service Providers (**LSP**). **Layered Service Provider** je systémový ovladač spojený se síťovými službami operačního systému Windows. Má přístup ke všem údajům, které do počítače vstupují a které z něho odcházejí, včetně schopnosti tyto údaje modifikovat. Některé LSP jsou nezbytné k tomu, aby umožnily systému Windows spojení s ostatními počítači v Internetu. Některé typy malware se však také mohou nainstalovat jako LSP, a získat tak přístup ke všem údajům, které váš počítač přenáší. Proto vám tato kontrola může pomoci provést všechny možné hrozby ze strany LSP.

V některých případech je možné opravit poškozené LSP (např. když došlo k odstranění souboru, ale zápisy do registrace stávají nedotčené). Je-li zjištěn opravitelný LSP, zobrazí se nové tlačítko, s jehož pomocí lze LSP opravit.

#### Ovládací tlačítka dialogu

Ovládací tlačítka dostupná v záložce **Prohlížeč LSP**.



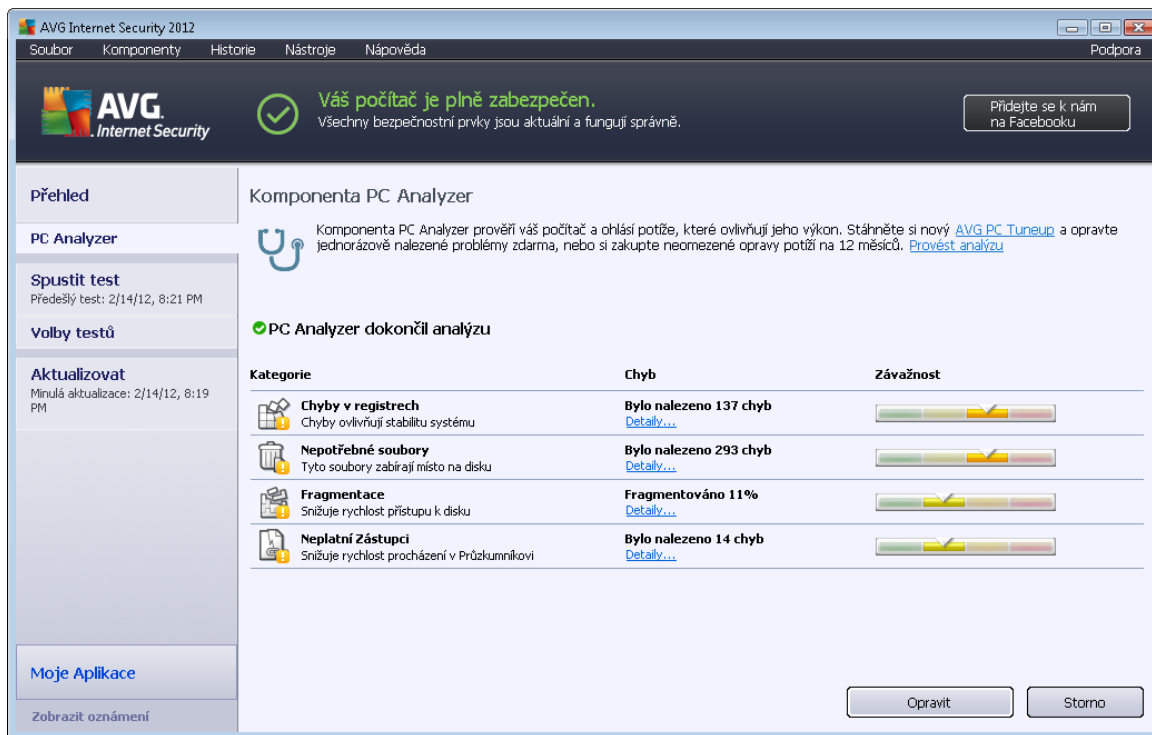
- **Skrýt Windows LSP** - pokud chcete zařadit LSP systému Windows do seznamu, zrušte volbu u této položky
- **Zpět** - přejdete zpět do výchozího [hlavního dialogu AVG](#) (přehled komponent)


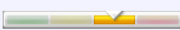


## 6.7. PC Analyzer

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

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

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



Kategorie	Chyb	Závažnost
<b>Chyby v registrech</b> Chyby ovlivňují stabilitu systému	Bylo nalezeno 137 chyb <a href="#">Detaily...</a>	
<b>Nepotřebné soubory</b> Tyto soubory zabírají místo na disku	Bylo nalezeno 293 chyb <a href="#">Detaily...</a>	
<b>Fragmentace</b> Snižuje rychlost přístupu k disku	Fragmentováno 11% <a href="#">Detaily...</a>	
<b>Neplatní Zástupci</b> Snižuje rychlost procházení v Průzkumníkovi	Bylo nalezeno 14 chyb <a href="#">Detaily...</a>	

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

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

### Ovládací tlačítka

- **Provést analýzu** (tlačítko se zobrazí před zahájením analýzy) - stiskem tlačítka spustíte okamžitou analýzu počítače
- **Opravit** (tlačítko se zobrazí po dokončení analýzy) - stiskem tlačítka přejdete na web AVG



(<http://www.avg.cz/>) na stránce s podrobnými a aktuálními informacemi o komponentě PC Analyzer

- **Storno** - stiskem tlačítka můžete přerušit průběh živé analýzy, anebo se vrátit do výchozího [hlavního dialogu AVG](#) (přehled komponent) po ukončení procesu analýzy

## 6.8. Identity Protection

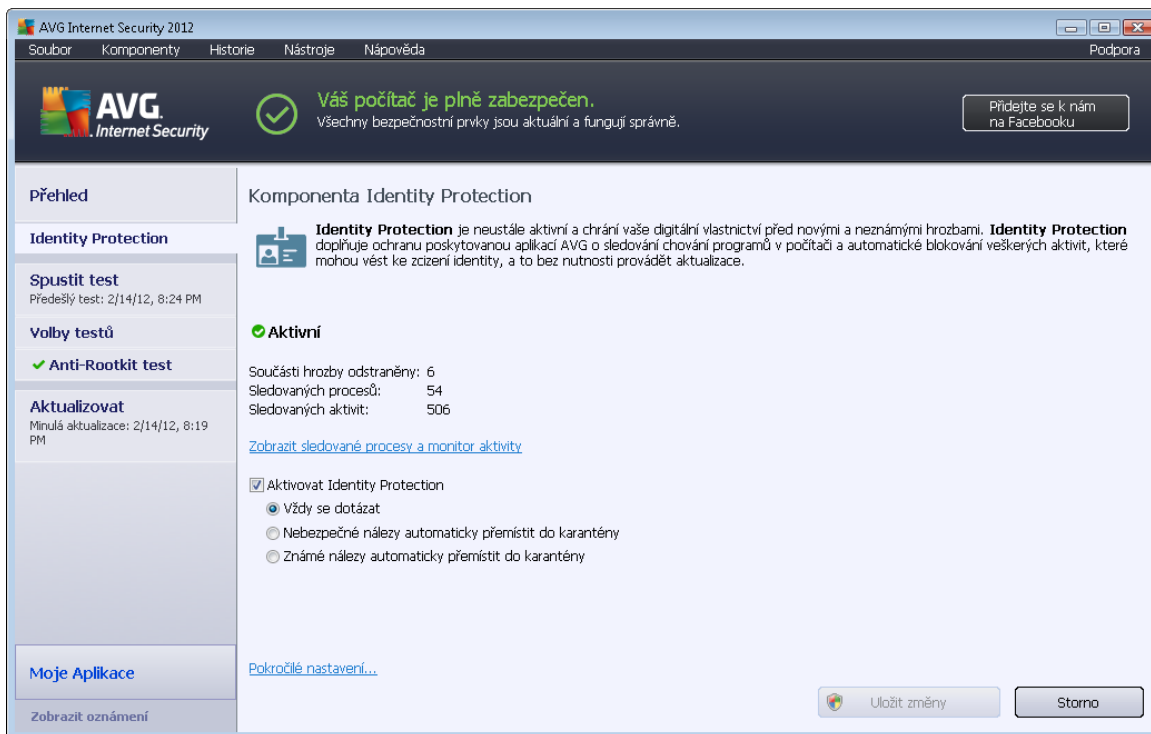
**Identity Protection** je komponentou, která pomáhá a v reálném čase zajišťuje ochranu před různými druhy malware a viry, a to na bázi identifikace specifického chování těchto typů aplikací. **Identity Protection** zajišťuje bezpečnost při nákupu, bankovních operacích a jiných elektronických transakcích. 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 přemístí do [Virového trezoru](#) a vrátí zpět do původního stavu veškeré změny systému provedené tímto kódem (*vložené kusy kódu, změny v registrech, otevřené porty apod.*). **Identity Protection** vás chrání, aniž byste museli spouštět jakýkoliv test. Tato technologie je vysoce proaktivní, aktualizaci vyžaduje jen zřídka a trvale hlídá vaše bezpečí.

**Identity Protection je bezpečnostní složkou komplementární ke komponentě [Anti-Virus](#). Pro naprostou bezpečnost vašeho počítače a dle doporučení, abyste si nainstalovali obě komponenty!**



## 6.8.1. Rozhraní Identity Protection



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

- **Součástí 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

Pod základní statistikou je uveden odkaz [Zobrazit sledované procesy a monitor aktivity](#), s jehož pomocí se můžete přepnout do dialogu komponenty [Systémové nástroje](#), kde najdete detailní přehled všech monitorovaných 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.

Můžete 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



n 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 podezřelých aktivit 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, doporučujeme tuto konfiguraci ponechat*)
- **Nebezpečné nálezy automaticky přemístit do karantény** - veškeré aplikace detekované jako malware budou automaticky zablokovány
- **Známé nálezy automaticky přemístit do karantény** - zablokovány budou jen ty aplikace, o nichž lze s naprostou jistotou říci, že se skutečně jedná o malware
- **Pokročilé nastavení** - Kliknutím na odkaz budete přemístěni do příslušného dialogu [Pokročilého nastavení AVG Internet Security 2012](#), kde můžete editovat konfiguraci komponenty do nejmenších podrobností. Mějte však na paměti, že výchozí konfigurace všech komponent **AVG Internet Security 2012** je nastavena tak, aby program podával optimální výkon a poskytoval maximální možnou úroveň bezpečí. Pokud nemáte skutečný důvod ke změně, doporučujeme ponechat výchozí nastavení!

### Ovládací tlačítka dialogu

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

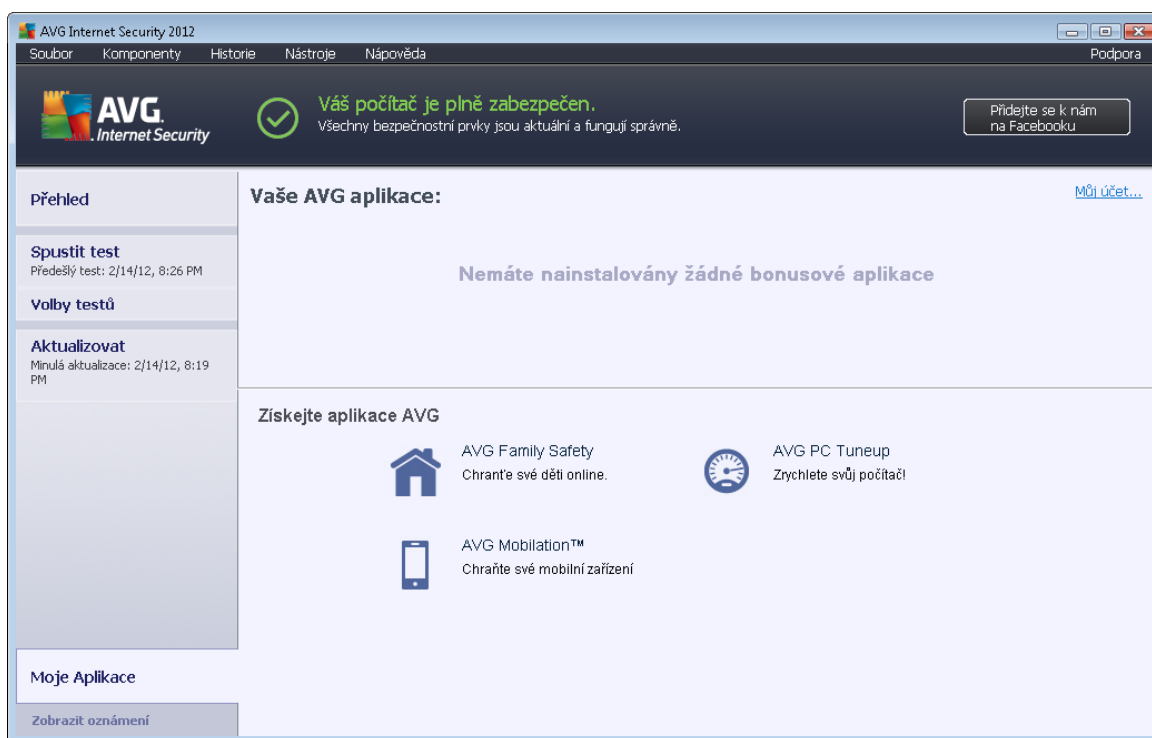
- **Uložit změny** - stiskem tohoto tlačítka budou uloženy všechny v tomto dialogu provedené změny
- **Storno** - stiskem tlačítka se vrátíte do výchozího [hlavního dialogu AVG](#) (přehled komponent)

## 6.9. Vzdálená správa

Komponenta **Vzdálená správa** se v hlavním dialogu **AVG Internet Security 2012** zobrazí pouze v případě, že jste instalovali síťovou verzi produktu (*informaci o instalované licenci najdete na záložce [Verze](#) v dialogu [Informace](#), který lze otevřít ze systémového menu volbou položky [Podpora](#)*). Pro podrobný popis funkce a možností této komponenty a zapojení klientské stanice AVG do systému vzdálené správy vás odkazujeme na samostatnou dokumentaci vztahující se tomuto tématu, která je ke stažení webu AVG (<http://www.avg.cz/>) v sekci **Centrum podpory / Stáhnout / Dokumentace**.

## 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 jakéhokoliv prostředí 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. **AVG Family Safety** umožňuje sledovat i aktivity Vašich dětí v sociálních sítích a diskusních skupinách. Pokud dojde k detekci slov, frází či vět, která mohou poukazovat na potenciální ohrožení Vašich dětí, budete o této skutečnosti uvědomeni zasláním SMS zprávy nebo e-mailu. Pro každé ze svých dětí navíc můžete nastavit příslušnou úroveň zabezpečení a sledovat jejich činnost 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:

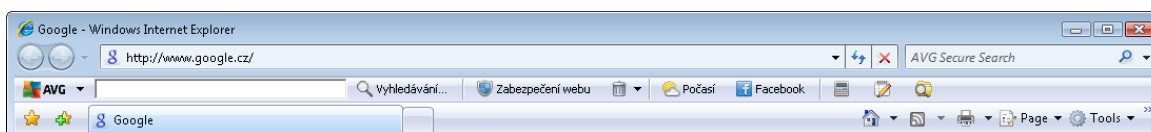
- vyhledání a defragmentace disku; oprava chybných sektorů
- oprava a defragmentace registrů
- optimalizace nastavení pro Internet, prohledání historie
- detekce a odstranění duplicitních souborů
- deaktivace zbytečných služeb, které zpomalují výkon počítače
- odinstalace nepoužívaných programů
- manuální 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](#).**



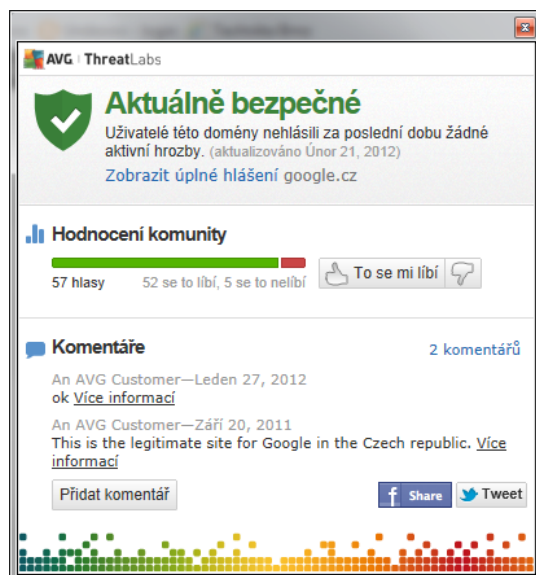
## 8. AVG Security Toolbar

**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 Internet Security 2012** instaluje volitelně; možnost rozhodnout se, zda tuto komponentu chcete instalovat, jste měli v průběhu [instalačního procesu](#). **AVG Security Toolbar** je dostupný v podobě nástrojové lišty ve vašem internetovém prohlížeči. Podporovanými prohlížeči jsou Internet Explorer (ve verzi 6.0 a vyšší) a/nebo Mozilla Firefox (ve verzi 3.0 a vyšší). Jiné prohlížeče nejsou podporovány (pokud používáte alternativní prohlížeč, 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 laboratoř 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](#)).
- **Site Safety** - 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**):



- **Delete** - 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**.
- 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.

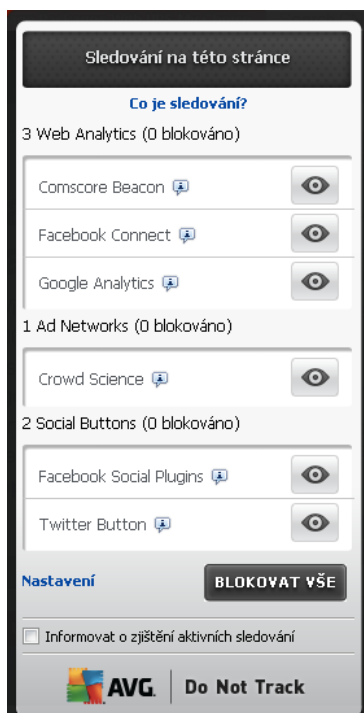
- **AVG Do Not Track** vám poskytne dodatečné informace o ochraně osobních údajů každé webové stránky a také přímý odkaz na možnost odhlášení konkrétní služby, pokud je tato k dispozici.
- **AVG Do Not Track** také podporuje [protokol W3C DNT](#), který automaticky vyzoomí příslušnou webovou stránku, že si nepřejete být sledováni. Tato notifikace je ve výchozím nastavení zapnutá, ale lze ji vypnout.
- **AVG Do Not Track** je službou poskytovanou za [tuto podmínku](#).
- **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 sítě jsou ve výchozím nastavení blokovány): Služby, které přímo či nepřímo sbírají nebo sdílejí na různých stránkách informace o vaší činnosti na Internetu s cílem nabízet individuální reklamy (narozdíl od reklam založených na obsahu). Tyto služby se řídí zásadami ochrany osobních údajů příslušné reklamní sítě (zásady ochrany osobních údajů jsou dostupné na webových stránkách dané sítě).

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

V dialogu jsou rovněž uvedeny dva hypertextové odkazy:

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

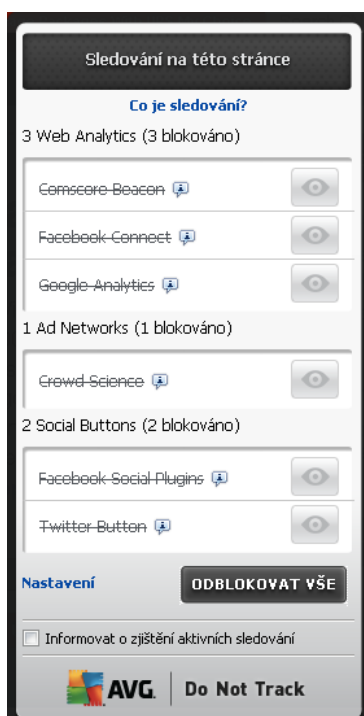
Ve spodní části bubliny pak najdete aktivní odkaz **Ochrana osobních údajů**, přes nějž budete přesměrováni na stránku s prohlášením o ochraně osobních údajů na serveru poskytlé detekované služby.



### 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 nichž 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

Přímě 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 poli můžete určit, po jak dlouhou dobu (v sekundách) si můžete ponechat notifikační dialog **AVG Do Not Track** zobrazený na vašem monitoru. Číslo musí spadat do rozmezí 0 až 60 sekund (pokud nastavíte hodnotu 0, notifikační dialog se na vaší obrazovce vůbec neobjeví).
- **Pozice oznámení** (ve výchozím nastavení: Vpravo nahore) - Otevřete rozbalovací menu a vyberte, v jaké pozici na vašem monitoru se má notifikační dialog **AVG Do Not Track** zobrazovat.
- **Upozornit, pokud jsem na stránce sledován** (ve výchozím nastavení vypnuto) - Označením položky potvrdíte, že si 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 o tom, 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 vaši volbu. 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.

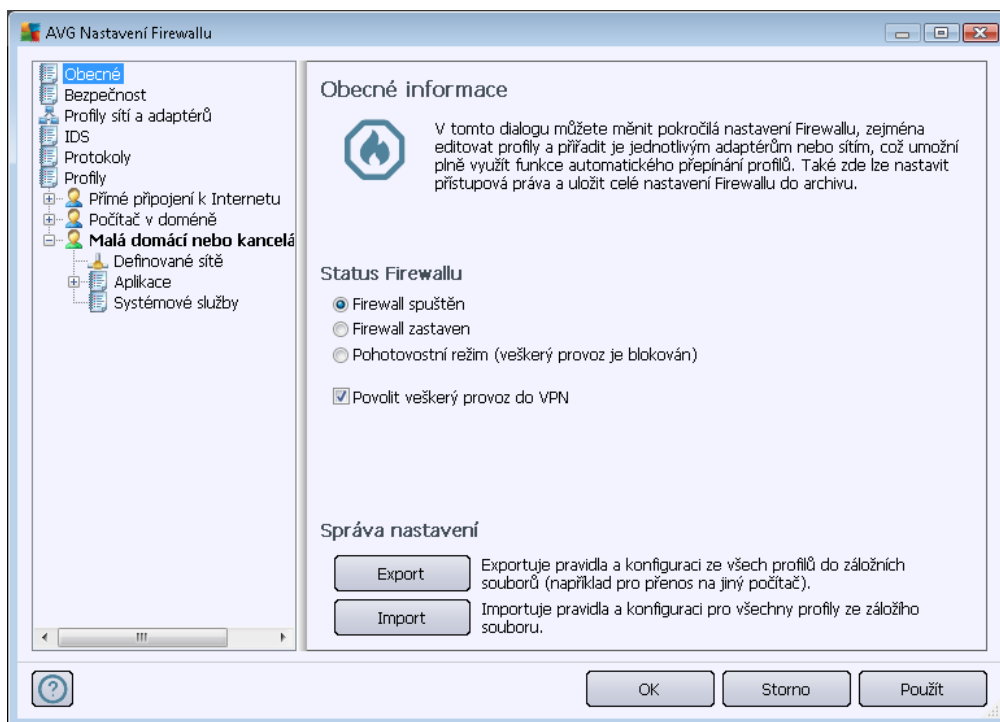
## 10. Nastavení Firewallu

Konfigurace [Firewallu](#) se otevírá v samostatném okně, kde můžete na několika dialogových nastavení velmi pokročilé parametry komponenty.

**Mjte prosím na paměti, že všechny komponenty AVG Internet Security 2012 jsou výrobcem nastaveny k optimálnímu výkonu. Pokud nemáte skutečný důvod jejich konfiguraci měnit, doporučujeme ponechat program ve výchozím nastavení. Editace pokročilé konfigurace je určena výhradně znalým a zkušeným uživatelům!**

### 10.1. Obecné

Dialog **Obecné informace** je rozdělen do dvou sekcí:



#### Status Firewallu

V sekci **Status Firewallu** máte možnost přepínat podle aktuálního potřebný stav komponenty [Firewall](#):

- **Firewall spuštěn** - touto volbou umožníte komunikaci těmto aplikacím, pro něž je v pravidlech definovaných v rámci zvoleného [profilu Firewallu](#) provoz povolen.
- **Firewall zastaven** - touto volbou vypnete [Firewall](#), veškerý síťový provoz je povolen a není kontrolován!
- **Pohotovostní režim (veškerý provoz je blokován)** - touto volbou můžete v případě potřeby zastavit veškerý provoz na všech síťových portech; [Firewall](#) zůstává spuštěn, ale veškerý síťový provoz je blokován.

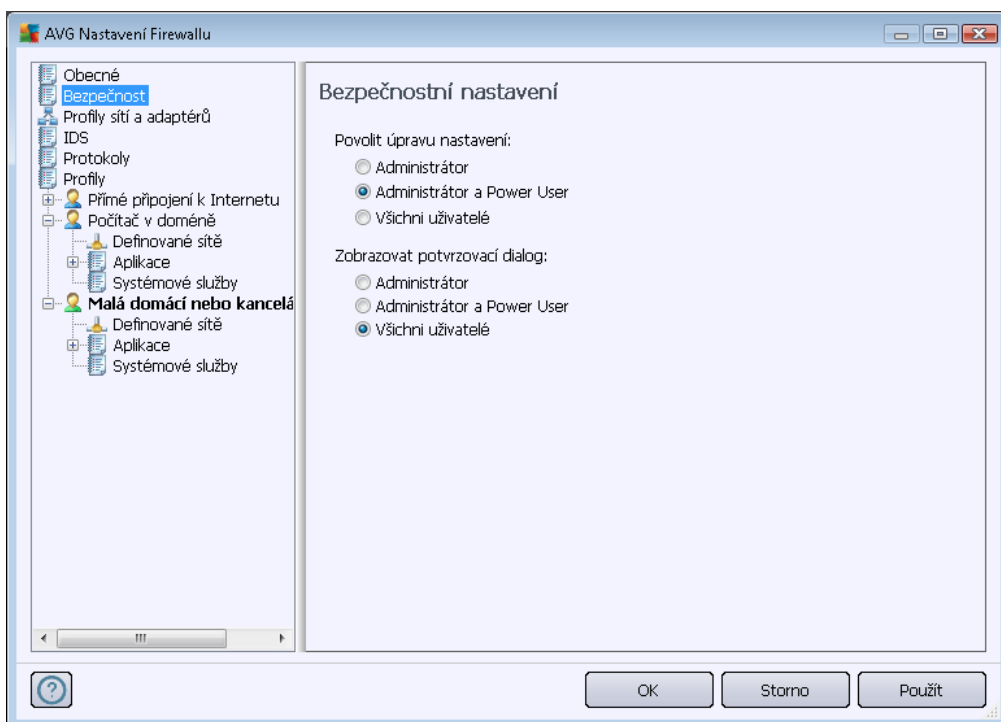
- **Povolit veškerý provoz do VPN** (ve výchozím nastavení zapnuto) - pokud používáte VPN (Virtual Private Network) přiipojení, například z domu do práce, doporuujeme ponechat možnost aktivovanou. **AVG Firewall** automaticky vyhledá adaptéry na vašem počítači, které VPN přiipojení využívá, a povolí komunikaci všech aplikací do cílové sítě (resp. aplikací, které již nemají vlastní, specifické pravidlo). Pokud váš systém používá jiné síťové adaptéry, měli byste tento jednoduchý krok uchránit nutností zadávat speciální pravidlo pro každou aplikaci, které chcete umožnit komunikaci přes VPN.

**Poznámka:** Pokud se v budoucnu nemůžete připojit přes VPN, patrně není povolena komunikace některého z potřebovaných systémových protokolů: GRE, ESP, L2TP, PPTP. Nastavení lze změnit v dialogu [Systémové služby](#).

## Správa nastavení

V sekci **Správa nastavení** lze prostřednictvím dvou tlačítek **Exportovat** nastavení komponenty [Firewall](#) do záložních souborů anebo naopak **Importovat** kompletní zálohované nastavení [Firewallu](#).

## 10.2. Bezpečnost



V dialogu **Bezpečnostní nastavení** definujete obecná pravidla pro správu komponenty [Firewall](#) bez ohledu na nastavený profil:

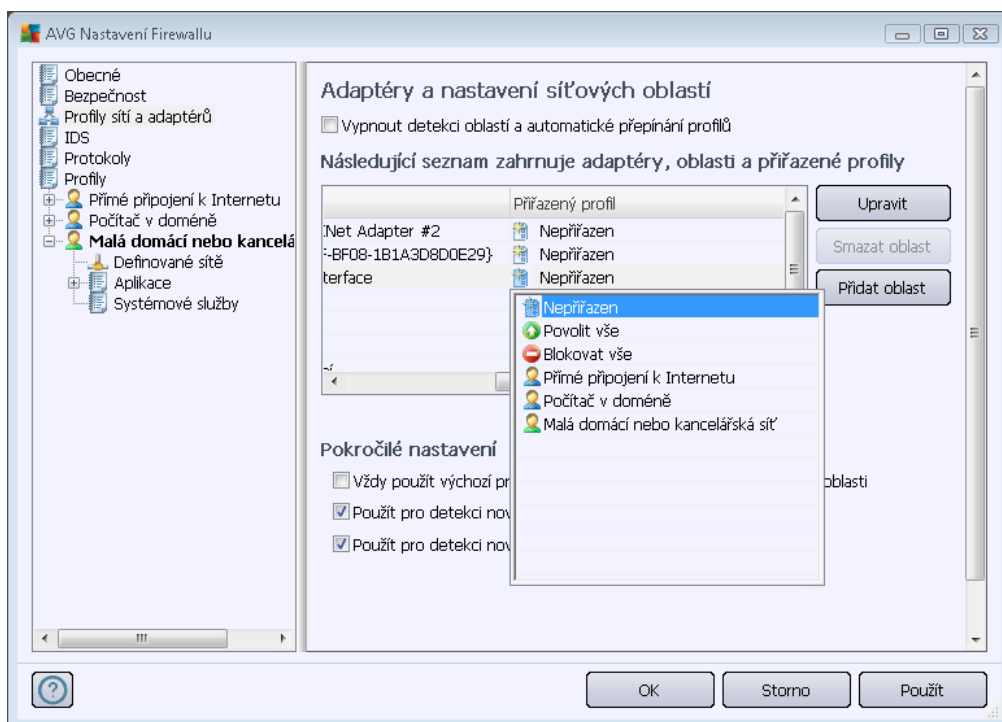
- **Povolit úpravu nastavení** - určete, kdo má právo měnit konfiguraci [Firewallu](#).
- **Zobrazovat potvrzovací dialog** - svou volbou určíte, komu se mají zobrazovat dotazovací dialogy vyžadující rozhodnutí v situaci, která není ošetřena definovaným pravidlem [Firewallu](#).

V obou případech můžete přidat konkrétní pravomoc na které z těchto kategorií uživatel :

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

### 10.3. Profily sítí a adaptérů

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



- **Vypnout detekci oblastí a automatické přepínání profilů** (ve výchozím nastavení vypnuto) - Každému typu síťového rozhraní, respektive oblasti, lze přidat jeden z předdefinovaných profilů. Pokud specifické profily definovat nechcete, bude se automaticky používat jediný společný profil. Pokud se však rozhodnete profily rozlišovat a přidat je jednotlivě specifickým adaptérům a jim příslušným oblastem, a později toto nastavení potěbujete z nějakého důvodu dočasně deaktivovat, označte položku **Vypnout detekci oblastí a automatické přepínání profilů**.
- **Seznam adaptérů, oblastí a přidělených profilů** - V seznamu najdete přehled detekovaných adaptérů a oblastí. Každému z nich máte možnost přidat specifický profil z





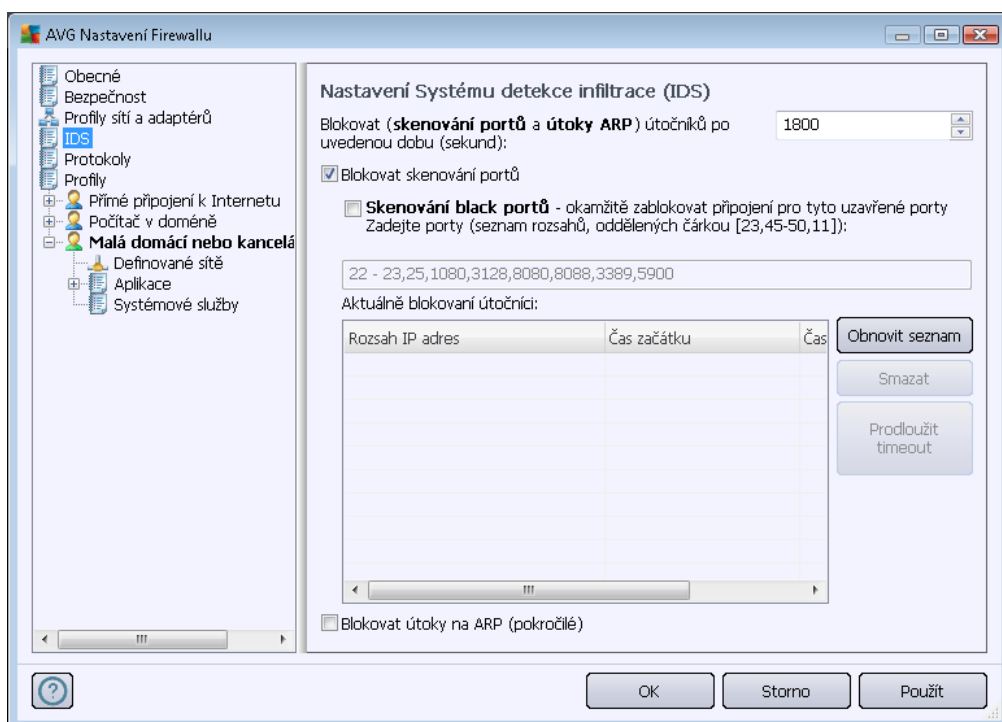
nabídky definovaných profilů. Tuto nabídku otevřete kliknutím levého tlačítka myši na příslušnou položku seznamu adaptérů (ve sloupci *Připojený profil*) a vyberte profil z kontextového menu.

## Pokročilé nastavení

- **Vždy použít defaultní profil a nezobrazovat dialog pro připojení nové oblasti** - Kdykoliv se váš počítač připojí k nové síti, [Firewall](#) vás na tuto skutečnost upozorní zobrazením dialogu, v němž budete vyzváni, abyste zvolili typ síťového připojení a přidali odpovídající [profil Firewallu](#). Pokud nechcete, aby se tento dialog zobrazoval, označte tuto položku.
- **Použít pro detekci nových sítí heuristiku AVG** - Umožňuje sběr informací o nově detekované síti prostřednictvím vlastního mechanismu AVG (*tato možnost je však k dispozici pouze na OS VISTA a vyšších operačních systémech*).
- **Použít pro detekci nových sítí heuristiku Microsoft** - Umožňuje sběr informací o nově detekované síti prostřednictvím služby Windows (*tato možnost je však dostupná pouze u OS Windows Vista a vyšších*).

## 10.4. IDS

Systém detekce infiltrace je speciální metodou analýzy chování určenou k identifikaci a zablokování podezřelých pokusů o komunikaci na specifických portech vašeho počítače. Parametry IDS můžete konfigurovat v dialogu **Nastavení Systému detekce infiltrace (IDS)**:





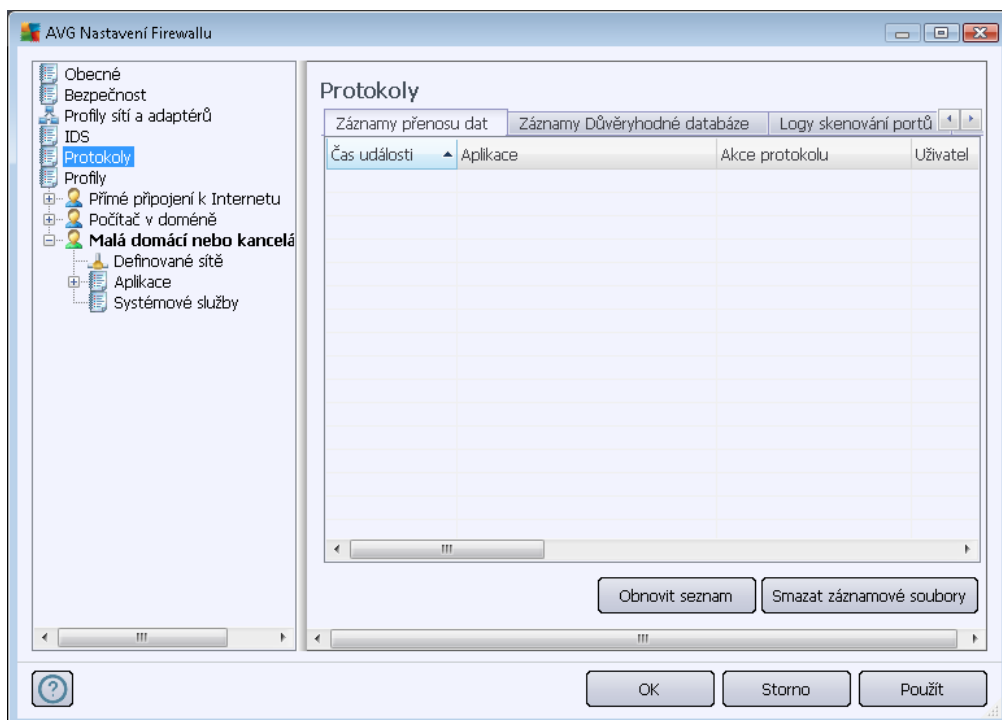
Dialog **Nastavení Systému detekce infiltrace (IDS)** nabízí tyto možnosti nastavení:

- **Blokovat (skenování port a útoky ARP) úto ník po uvedenou dobu** - Ur ete (v sekundách), jak dlouho poté, kdy na n m bude detekován pokus o podez elou komunikaci, má být port blokován. Ve výchozím nastavení je asový interval stanoven na 1800 sekund (30 minut).
- **Blokovat skenování port** (ve výchozím nastavení zapnuto) – Ozna ením této položky definujete, že si p ejete zablokovat veškeré pokusy o komunikaci zven í na všech TCP a UDP portech. U každého p ípojení bude povoleno p t pokus a šestý již bude zablokován. Položka je ve výchozím nastavení zapnuta a doporu ujeme toto nastavení ponechat. Pokud ponecháte volbu **Blokovat skenování port** povolenu, je dále k dispozici další podrobné nastavení (v opa ném p ípad je následující položka deaktivována):
  - **Skenování black port** – Ozna ením této možnosti okamžit zablokujete jakékoli pokusy o komunikaci na portech definovaných v textovém poli pod touto položkou. Jednotlivé porty nebo rozp tí port musí být odd leny árkou. Ve výchozím nastavení je textovém poli p edem definován seznam doporu ených port a máte možnost použít tuto alternativu.
  - **Aktuáln blokovaní ú astníci** - Sekce nabízí seznam všech pokus o komunikaci, jež jsou komponentou [Firewall](#) momentáln blokovány. Kompletní historii blokováných pokus o komunikaci pak najdete v dialogu [Protokoly](#) (záložka *Logy skenování port* ).
- **Blokovat útoky na ARP (pokro ilé)** (ve výchozím nastavení vypnuto) - Ozna ením této položky aktivujete blokovaní speciálních pokus o komunikaci uvnit lokální síť , které **IDS** detekuje jako potenciáln nebezpe né. K této položce se vztahuje asový interval nastavený v horn í části tohoto dialogu **Blokovat úto níky po uvedenou dobu**. Použití této možnosti blokace doporu ujeme však pouze skute n pokro ilým uživatel m, znalým typ a úrovn rizika v jejich lokální síti.

### Ovládací tlačítka dialogu

- **Obnovit seznam** - stiskem tlačítka aktualizujete seznam aktuáln blokováných úto ník ( zobrazíte nejnov jší blokované pokusy o komunikaci)
- **Smazat** - stiskem tlačítka odstraníte ze seznamu blokováných ú astník zvolenou položku
- **Prodloužit timeout** - stiskem tlačítka prodloužíte definovaný asový interval, po jehož dobu má být zvolený pokus o komunikaci blokován. P í použití této volby se zobrazí nový dialog, v n mž m žete nastavit pesný as a datum trvání blokace, anebo se rozhodnout blokovat zvolený pokus o komunikaci neomezen .

## 10.5. Protokoly



Dialog **Protokoly** nabízí seznamy všech protokolovaných událostí **Firewallu** s p ehledem parametr jednotlivých událostí ( *čas události, jméno aplikace, která se pokoušela navázat spojení, p íslušnou akci protokolu, jméno uživatele, PID, sm r p ípojení, typ protokolu, íslo vzdáleného a místního portu, ...*) na ty ech záložkách:

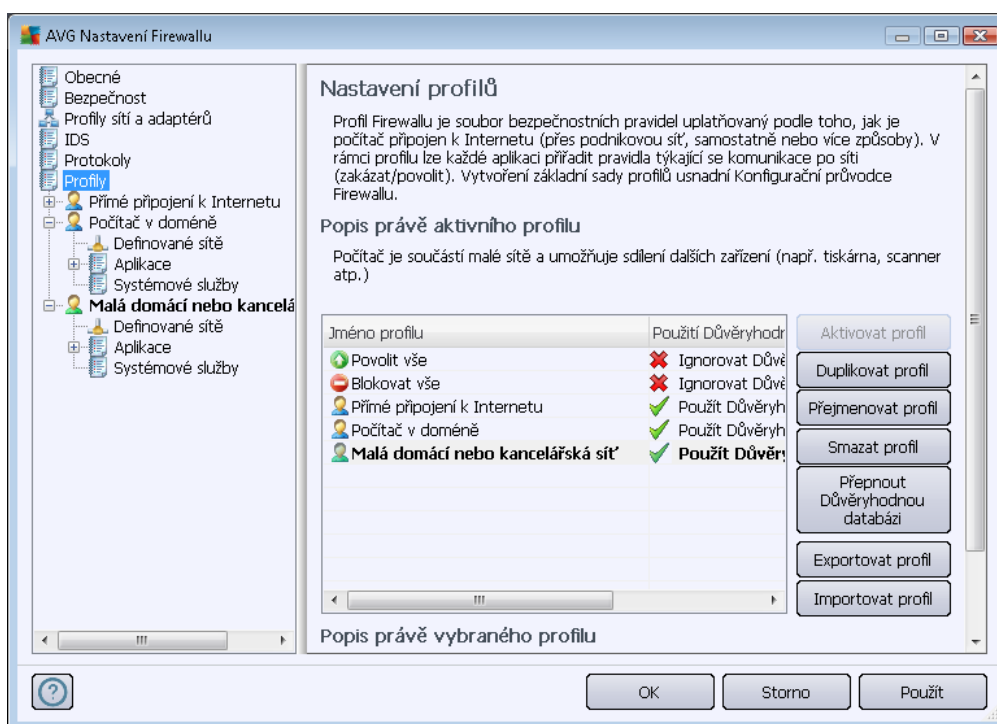
- **Záznamy p enosu dat** - nabízí informace o veškeré aktivit aplikací, které se jakýkoliv zp sobem pokusily o navázání sí ové komunikace.
- **Záznamy D v ryhodné databáze** - *D v ryhodná databáze* je interní databáze AVG, v níž jsou shromážděny informace o aplikacích, které mají ověný certifikát, jsou prověně a d v ryhodné, a komunikace jim m že být povolena. P í prvním pokusu jakékoliv aplikace o navázání sí ové komunikace (*tedy v situaci, kdy pro danou aplikaci ještě není nastaveno žádné pravidlo*) je t eba zjistit, zda má být této aplikaci komunikace povolena. AVG nejprve prohledá *D v ryhodnou databázi*, a pokud je v ní daná aplikace uvedena, bude její komunikace automaticky povolena. Teprve v p ípad , že o aplikaci nemáme k dispozici žádné informace, budete v samostatném dialogu dotázáni, zda si p ežete komunikaci povolit.
- **Logy skenování port** - zaznamenává veškeré události související s ínností **Systému detekce infiltrace**.
- **ARP logy** - zaznamenává blokování speciálních pokus ů komunikaci uvnit lokální sít ( *volba [Blokovat útoky na ARP](#)*), které **Systém detekce infiltrace** detekuje jako potenciálně nebezpečné.

## Ovládací tlačítka

- **Obnovit seznam** - Protokolované parametry lze editovat podle zvoleného atributu: data chronologicky, ostatní sloupce abecedně (klikněte na nadpis příslušného sloupce). Tlačítkem **Obnovit seznam** pak můžete zobrazené informace aktualizovat.
- **Smazat záznamové soubory** - Stiskem tlačítka odstraní všechny záznamy z tabulky.

## 10.6. Profily

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



Systémové profily (*Povolit vše*, *Blokovat vše*) editovat nelze. Všechny uživatelské profily (*Přímé připojení k Internetu*, *Počítač v doméně*, *Malá domácí nebo kancelářská síť*) však můžete spravovat za pomoci následujících ovládacích tlačítek:

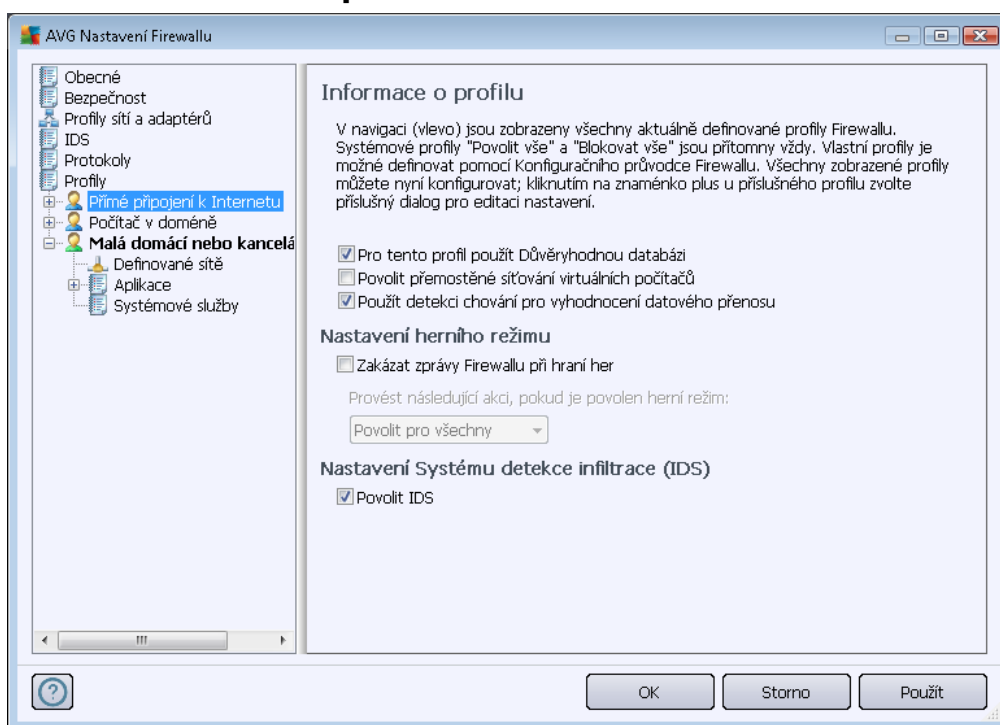
- **Aktivovat profil** - Tlačítkem nastavíte zvolený profil jako aktivní, jeho nastavení bude použito pro řízení provozu **Firewallem**.
- **Duplikovat profil** - Vytvoří kopii zvoleného profilu se stejným nastavením; tuto kopii pak budete moci editovat a přejmenovat, čímž bude definován nový profil.
- **Přejmenovat profil** - Umožní definovat nové jméno zvoleného profilu.
- **Smazat profil** - Smaže zvolený profil ze seznamu.

- **P epnout D v ryhodnou databázi** - U konkrétního zvoleného profilu umožní využití záznamů D v ryhodné databázi (interní databáze AVG shromaž ují informace o ov ených a certifikátem opat ených aplikacích, jimž m že být komunikace vždy povolena ).
- **Exportovat profil** - Zaznamená konfiguraci zvoleného profilu do souboru, který uloží pro p ípadné použití v budoucnosti.
- **Importovat profil** - Nastaví konfiguraci zvoleného profilu ze záložního souboru.

Ve spodní ásti dialogu pak najdete popis v seznamu aktuáln zvoleného profilu.

Podle po tu definovaných profil , jež se zobrazí v seznamu tohoto dialogu, se bude generovat i další menu v levé sekci se stromovou navigací. Každý z definovaných profil vytvo í v navigaci svou vlastní v tev pod položkou **Profily**. Jednotlivé profily lze pak samostatn editovat v následujících dialozích ( *identických pro všechny profily*):

### 10.6.1. Informace o profilu



Dialog **Informace o profilu** je úvodním dialogem k sekci, v níž m žete editovat nastavení jednotlivých profil v samostatných dialozích len ných podle jednotlivých parametr p íslušných každému profilu:

- **Pro tento profil použít D v ryhodnou databázi** (ve výchozím nastavení zapnuto) - Ozna ením položky aktivujete možnost použití D v ryhodné databáze, tedy interní databáze AVG, v níž jsou shromaž dny informace o aplikacích, které mají ov ený certifikát, jsou prov ené a d v ryhodné, a komunikace jim m že být povolena. P í prvním pokusu jakékoliv aplikace o navázání sí ové komunikace (v situaci, kdy pro danou aplikaci



*ještě není nastaveno žádné pravidlo*) je třeba zjistit, zda má být této aplikaci komunikace povolena. AVG nejprve prohledá *D* v *rychlostní databázi*, a pokud je v ní daná aplikace uvedena, bude její komunikace automaticky povolena. Teprve v případě, že o aplikaci nemáme k dispozici žádné informace, budete v samostatném dialogu dotázáni, zda si přejete komunikaci povolit.

- **Povolit připojení síťových virtuálních počítačů** (ve výchozím nastavení vypnuto) - Označením této položky umožníte přímé připojení virtuálního počítače ve VMware do sítě.
- **Použít detekci chování pro vyhodnocení datového proudění** (ve výchozím nastavení zapnuto) - Označením této položky umožníte [Firewallu](#), aby připojení aplikace, jež se pokouší navázat síťovou komunikaci, využil funkce komponenty [Identity Protection](#) a zjistil tak, zda daná aplikace vykazuje jakoukoliv podezřelou činnost nebo ji lze považovat za bezpečnou.

### Nastavení herního režimu

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

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

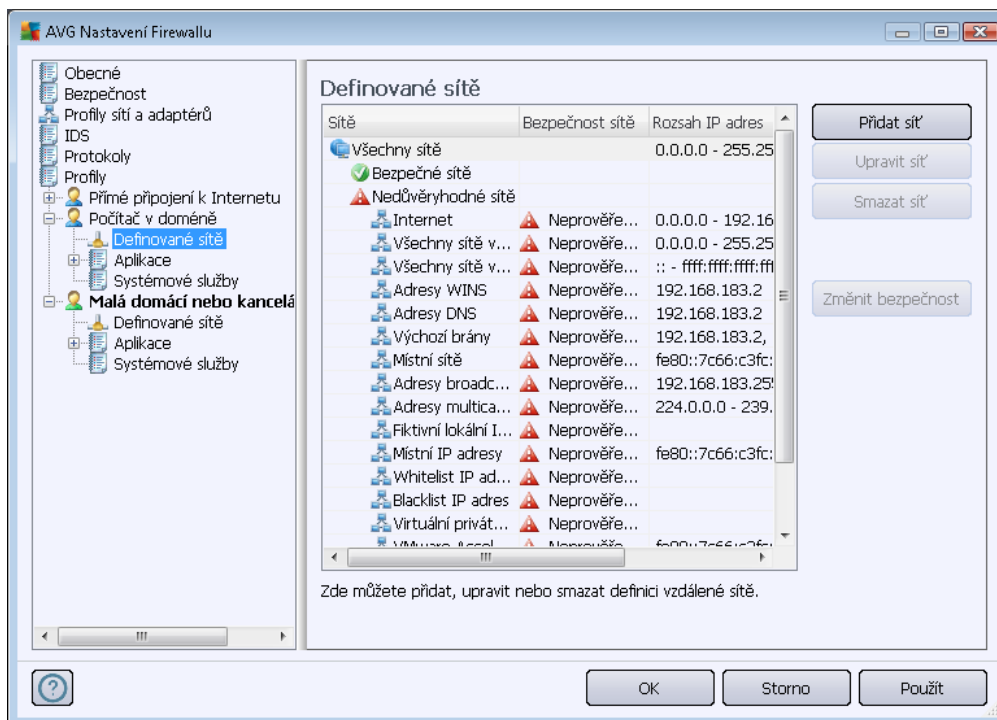
Je-li herní režim zapnutý, bude spuštěn všech naplánovaných úloh (*test, aktualizací*) pozastaveno do doby, než bude aplikace ukončena.

### Nastavení Systému detekce infiltrace (IDS)

Volbou položky **Povolit IDS** aktivujete speciální metodou analýzy chování určenou k identifikaci a zablokování podezřelých pokusů o komunikaci na specifických portech vašeho počítače (*podrobný popis možností nastavení Systému detekce infiltrace najdete v kapitole [IDS](#)*).

## 10.6.2. Definované sítě

Dialog *Definované sítě* nabízí seznam všech sítí, k nimž je váš počítač připojen.

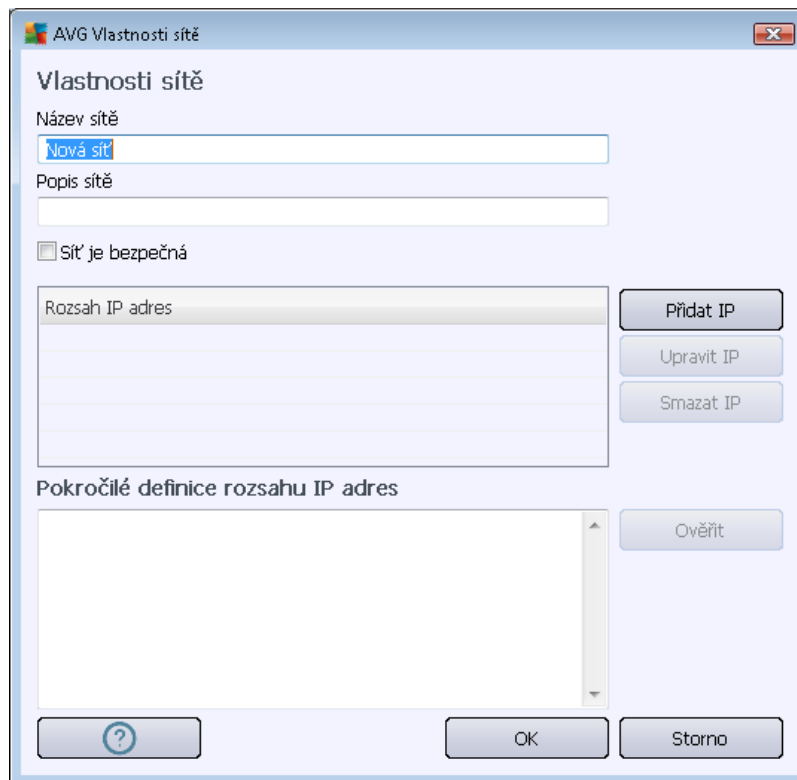


O detekovaných sítích jsou v seznamu k dispozici tyto informace:

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

### Ovládací tlačítka

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



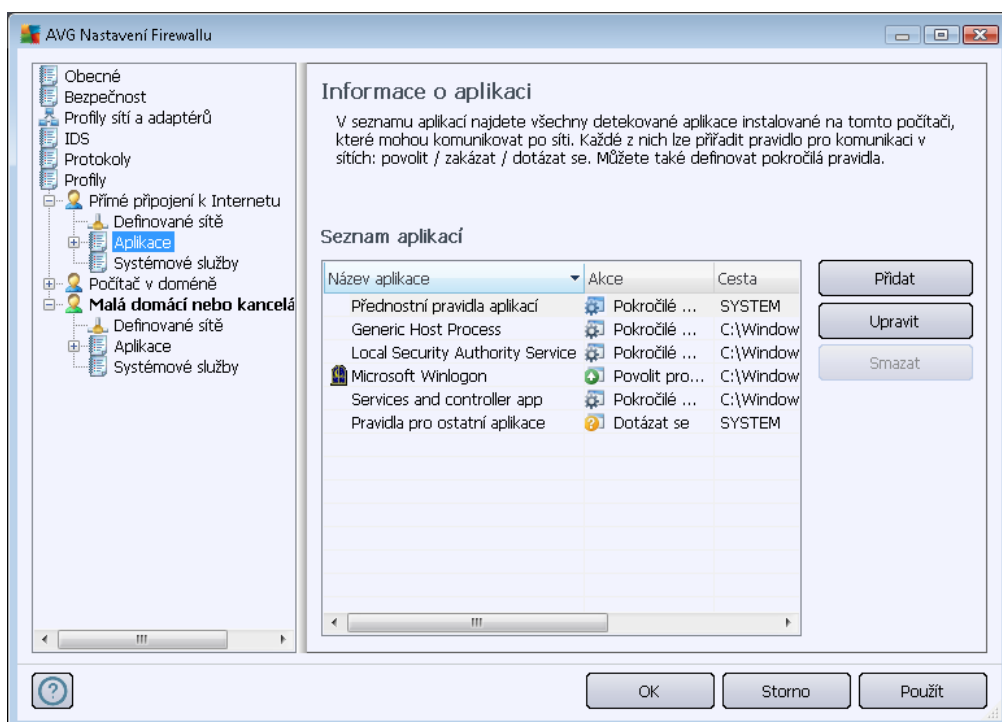
V dialogu lze zadat **Název sítě**, uvést stručný **Popis sítě** a případně označit síť za bezpečnou. Síť můžete definovat manuálně v samostatném dialogu dostupném prostřednictvím tlačítka **Přidat IP** (podobně **Upravit IP** / **Smazat IP**), kde zadáte rozsah nebo masku sítě. Při velkém množství sítí, které chcete definovat jako součást přidávané sítě, můžete využít hromadného přidání v sekci **Pokročilé definice rozsahu IP adres**: do textového pole vložte seznam sítí (v jakémkoli známém formátu) a tlačítkem **Ověřit** zjistíte, zda jsou všechny zadány v platném tvaru. Pokud ano, stiskem tlačítka **OK** potvrdíte jejich uložení.

- **Upravit síť** - Otevře dialogové okno **Vlastnosti sítě** (viz výše), v němž můžete editovat parametry již definované sítě (*okno je identické s oknem pro přidání nové sítě, popis tedy najdete v předchozím odstavci*).
- **Smazat síť** - Odstraní záznam o zvolené síti ze seznamu.
- **Zmítnit bezpečnost** - Ve výchozím nastavení jsou všechny sítě označeny jako neprovozené; pokud jste si jisti jejich bezpečností, můžete konkrétní síť označit tímto tlačítkem jako bezpečnou (*a podobně, je-li síť definována jako bezpečná, tímto tlačítkem můžete změnit její status a označit ji za nebezpečnou*).








### 10.6.3. Aplikace

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



Aplikace uvedené v **Seznamu aplikací** byly detekovány na vašem počítači (a byly jim přiřazeny příslušné akce). Rozlišujeme tyto typy akcí:

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

**Uvědomte si, prosím, že detekovány mohou být pouze ty aplikace, které byly na vašem počítači instalovány už ve chvíli instalace AVG Internet Security 2012; pokud jste nainstalovali novou aplikaci později, budete pro ni muset definovat pravidla samostatně. Ve chvíli, kdy se nová aplikace poprvé pokusí navázat síťovou komunikaci, bude buď vytvořeno pravidlo podle D v rybné databázi, anebo budete vyzváni k nastavení pravidla; pak budete muset rozhodnout, zda má být komunikace této aplikace povolena nebo blokována. Svou volbu můžete uložit jako trvalé pravidlo (které bude následně uvedeno v seznamu v tomto dialogu).**

Samořejmě je také možné definovat pravidla pro nové aplikace okamžitě – stisknete tlačítko **Přidat**



v tomto dialogu a vyplíte údaje o aplikaci.

Kromě aplikací obsahuje seznam ještě dvě speciální položky:

- **P ednostní pravidla aplikací** (*první ádek seznamu*) jsou preferenčními pravidly a jsou uplatňována před pravidly definovanými pro specifickou aplikaci.
- **Pravidla pro ostatní aplikace** (*poslední ádek seznamu*) se používají jako "poslední instance" v situaci, kdy nelze použít žádné specifické pravidlo pro aplikaci, například pro neznámou a nedefinovanou aplikaci. Vyberte akci, která se má spustit při pokusu takové aplikace o komunikaci po síti:
  - *Blokovat* - komunikace bude vždy zablokována.
  - *Povolit* - komunikace bude povolena.
  - *Dotázat se* – budete dotázáni, zda má být komunikace povolena nebo zakázána.

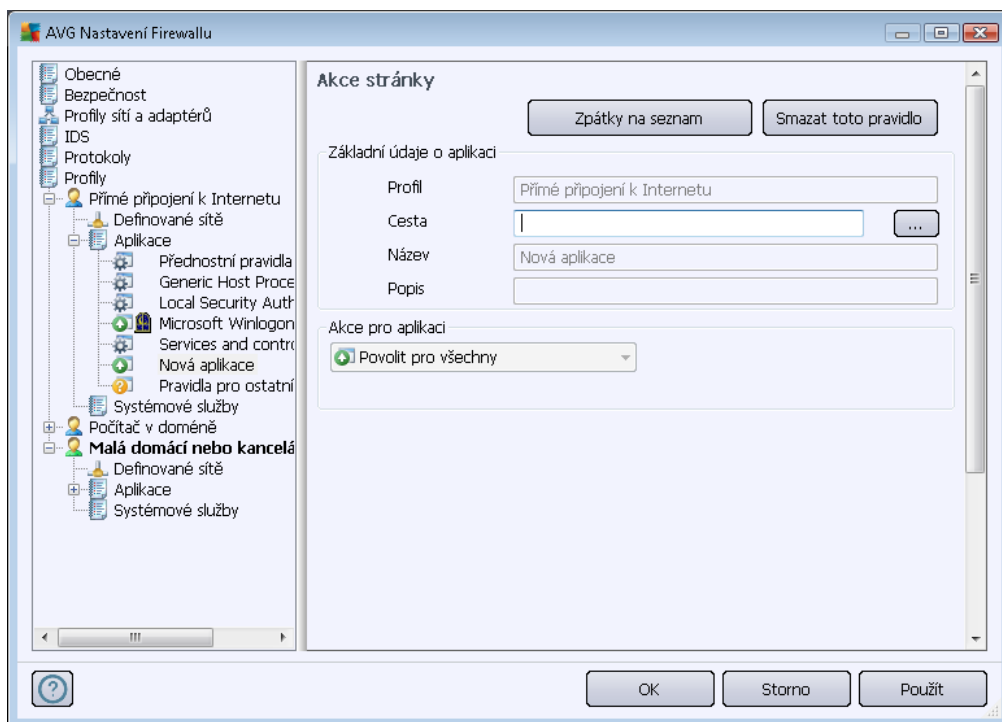
***Tyto položky se možnostmi svého nastavení liší od běžných aplikací a jsou určeny výhradně pro pokročilé uživatele! Důrazně doporučujeme, abyste nastavení těchto položek neupravovali!***

### **Ovládací tlačítka**

Seznam můžete editovat pomocí těchto ovládacích tlačítek:

- **Přidat** - Otevře prázdný dialog [Akce stránky](#) pro přidání nové aplikace.
- **Upravit** - Otevře již vyplněný dialog [Akce stránky](#) pro upravení parametrů stávající aplikace.
- **Smazat** - Odstraní zvolenou aplikaci ze seznamu.

V dialogu **Akce stránky** můžete definovat podrobná nastavení pro konkrétní aplikaci:



### Ovládací tlačítka

Dva ovládací tlačítka dialogu jsou dostupná hned v úvodu:

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

### Základní údaje o aplikaci

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

### Akce pro aplikaci

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

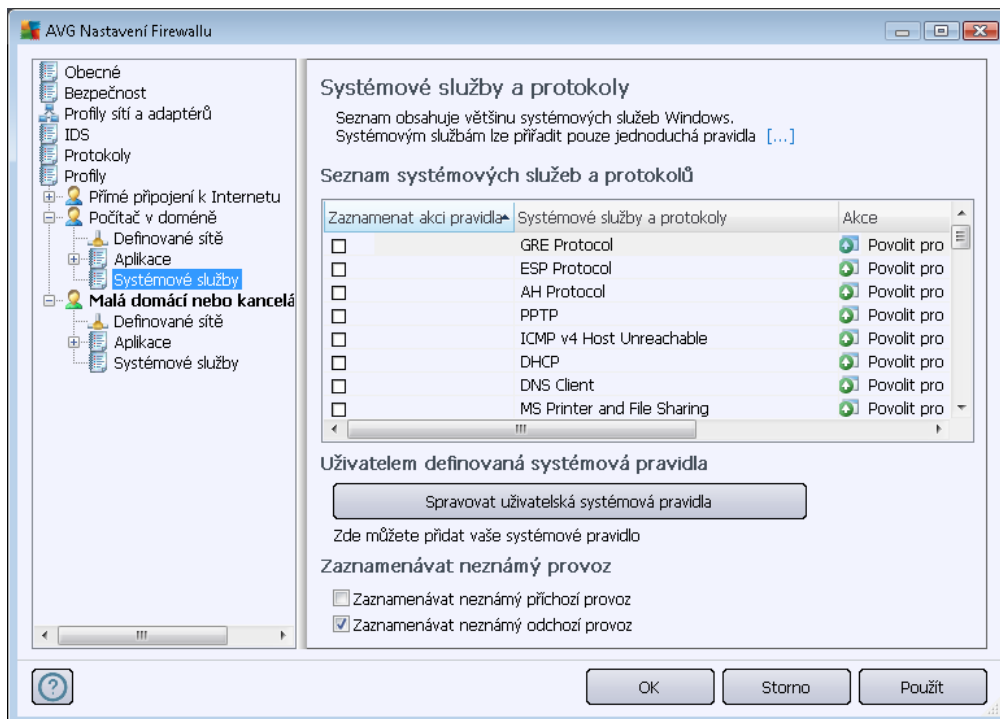


- **Povolit pro všechny** - Komunikace bude aplikaci povolena ve všech definovaných sítích a na všech adaptérech bez omezení.
- **Povolit pro bezpečné** - Komunikace bude aplikaci povolena pouze v sítích definovaných jako bezpečné.
- **Blokovat** - Komunikace bude automaticky zablokována; aplikaci nebude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

#### 10.6.4. Systémové služby

***Veškeré editace v dialogu Systémové služby a protokoly jsou určeny VÝHRADNĚ ZKUŠENÝM UŽIVATELŮM!***

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



### Seznam systémových služeb a protokolů

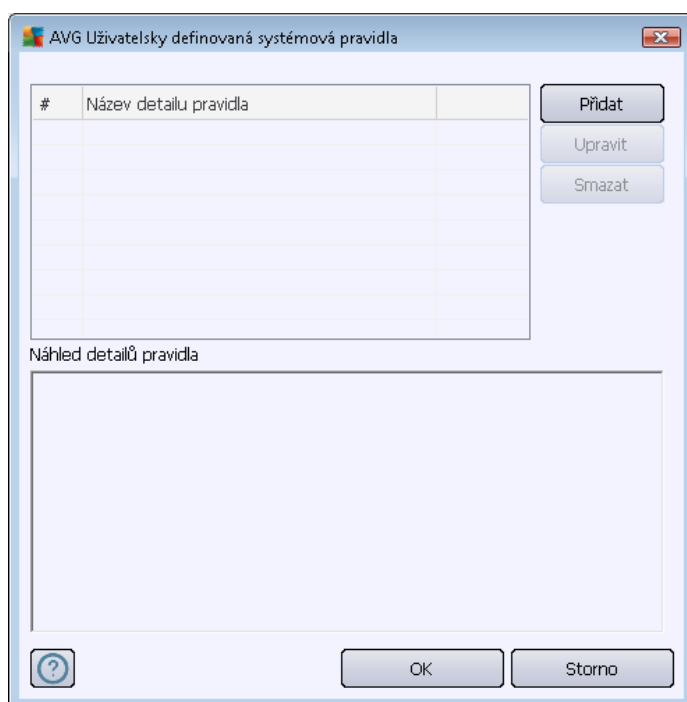
Tabulka obsahuje tyto sloupce:

- **Zaznamenat akci pravidla** - Označením polí můžete zapnout [protokolování](#) akce příslušného pravidla.
- **Systémové služby a protokoly** - V tomto sloupci jsou zobrazena jména příslušných systémových služeb.
- **Akce** - Sloupec zobrazuje ikony příslušné konkrétní akce:
  - Povolit komunikaci pro všechny sítě
  - Povolit komunikaci pro síť zařazenou do kategorie bezpečných (*Povolit pro bezpečné*)
  - Blokovat komunikaci
- **Síť** - V tomto sloupci je uvedeno, ke které konkrétní síti se systémové pravidlo vztahuje.

Chcete-li editovat nastavení libovolné položky v seznamu (včetně *přizpůsobených akcí*), klikněte na položku pravým tlačítkem myši a zvolte možnost **Upravit**. **Máte však na paměti, že editaci systémového pravidla může provádět pouze správce nebo uživatel. Důrazně doporučujeme systémová pravidla needitovat!**

## Uživatelsky definovaná systémová pravidla

Chcete-li vytvořit vlastní systémové pravidlo, použijte tlačítko **Spravovat uživatelská systémová pravidla**. V horní části dialogu **Uživatelsky definovaná systémová pravidla** vidíte přehled všech detailů prvně editovaného systémového pravidla, v dolní části pak přehled vybraného detailu. S uživatelskými pravidly můžete pracovat pomocí tlačítek **Upravit**, **Přidat** a **Smazat**, systémová pravidla definovaná výrobcem pak můžete pouze **Upravit**.



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

## Zaznamenávat neznámý provoz

- **Zaznamenávat neznámý příchozí provoz** (ve výchozím nastavení vypnuto) – Označením této položky zajistíte, že všechny neznámé pokusy o navázání komunikace s vaším počítačem budou zaznamenány v [Protokolech](#).
- **Zaznamenávat neznámý odchozí provoz** (ve výchozím nastavení zapnuto) – Označením této položky zajistíte, že všechny neznámé pokusy vašeho počítače a komunikací do sítě budou zaznamenány v [Protokolech](#).

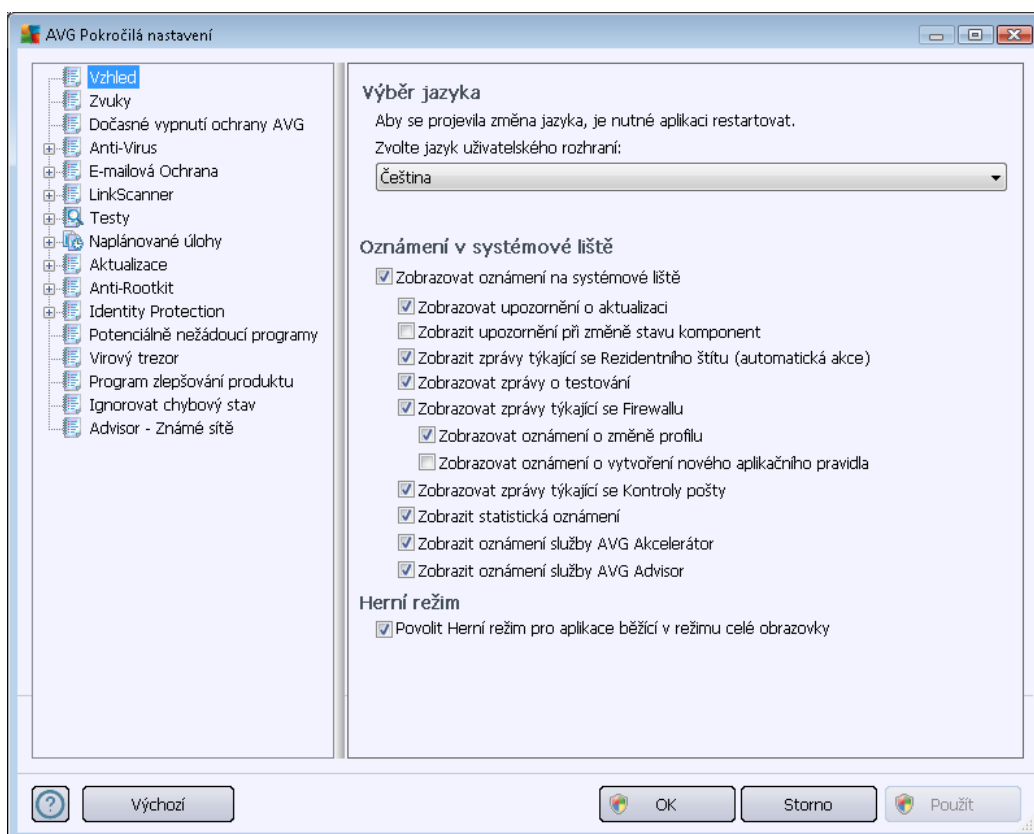


## 11. Pokročilé nastavení AVG

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

### 11.1. Vzhled

První položka navigačního seznamu, **Vzhled**, se týká obecného nastavení [hlavního dialogu AVG Internet Security 2012](#) a nabízí možnost nastavení základních prvků programu:

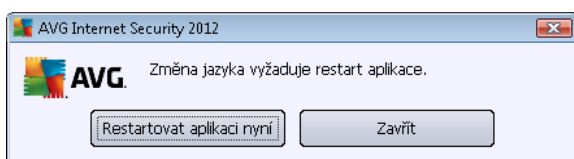


#### Výběr jazyka

V sekci **Výběr jazyka** můžete z rozbalovacího menu zvolit jazyk, v němž má být zobrazen [hlavní dialog AVG Internet Security 2012](#). V nabídce budou dostupné jen ty jazyky, které jste zvolili během [instalačního procesu](#) (viz kapitola [Uživatelské volby](#)) a také angličtina (angličtina se vždy instaluje automaticky). Pro zobrazení **AVG Internet Security 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 dialog)
- 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 Internet Security 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 Internet Security 2012**. Ve výchozím nastavení programu jsou systémová oznámení povolena. Doporučujeme toto nastavení ponechat! Systémová oznámení přináší například informace o spuštění aktualizací či testů, o změně stavu některých komponent **AVG Internet Security 2012** a podobně. Je rozhodně vhodné v novat jim pozornost!

Pokud se přesto z nějakého důvodu rozhodnete, že si nepřejete být takto informováni, máte možnost kompletně potlačit zobrazování informativních oznámení, nebo zakázat pouze zobrazování informací vztažených k určité komponentě **AVG Internet Security 2012**. Své vlastní nastavení můžete provést označením příslušné položky ve strukturované nabídce:

- **Zobrazovat oznámení na systémové liště** (ve výchozím nastavení zapnuto) - Položka je ve výchozím nastavení označena, takže se zobrazují veškerá informativní hlášení. Zrušením označení položky zcela vypnete zobrazování jakýchkoliv systémových oznámení. Jestliže je tato volba zapnuta, máte dále možnost definovat pravidla pro zobrazování jednotlivých typů informací:
  - **Zobrazovat zprávy o aktualizaci v systémové liště** (ve výchozím nastavení zapnuto) - Volbou položky rozhodnete, zda mají být zobrazena nebo naopak potlačena informativní hlášení o spuštění, průběhu a dokončení 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 projeví pouze tehdy, má-li Rezydentní 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 [Firewallu](#) v systémové liště** (*ve výchozím nastavení zapnuto*) - Volbou položky rozhodnete, zda mají být zobrazena nebo naopak potlačena informativní hlášení o stavu a procesech týkajících se komponenty [Firewall](#), například hlášení o aktivaci/deaktivaci komponenty, o aktuálním povolení i blokování provozu apod. Informace o ostatních procesech se budou zobrazovat normálně. Tato položka se dále dělí do dvou specifických možností (*podrobný popis obou najdete v kapitole [Firewall](#) této dokumentace*):
  - **Zobrazovat oznámení o změně profilu** (*ve výchozím nastavení zapnuto*) - Informuje o automatických změnách profilu [Firewallu](#).
  - **Zobrazovat oznámení o vytvoření nového aplikačního pravidla** (*ve výchozím nastavení vypnuto*) - Informuje o automatickém vytvoření pravidla pro novou aplikaci na základě seznamu bezpečných aplikací.
- **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 v nástrojové liště oznámení o komponentě [AVG Akcelerátor](#)** (*ve výchozím nastavení zapnuto*) - Volbou položky rozhodnete, zda mají být zobrazena nebo naopak potlačena informativní hlášení o aktivitě [AVG Akcelerátoru](#). [AVG Akcelerátor](#) umožňuje plynulé přehrávání videa v režimu online a urychluje stahování.
- **Zobrazit oznámení služby [AVG Advisor](#)** (*ve výchozím nastavení zapnuto*) - Volbou položky rozhodnete, zda chcete ponechat zapnutá všechna oznámení služby [AVG Advisor](#) zobrazovaná ve vysouvacím panelu na systémovou liště.

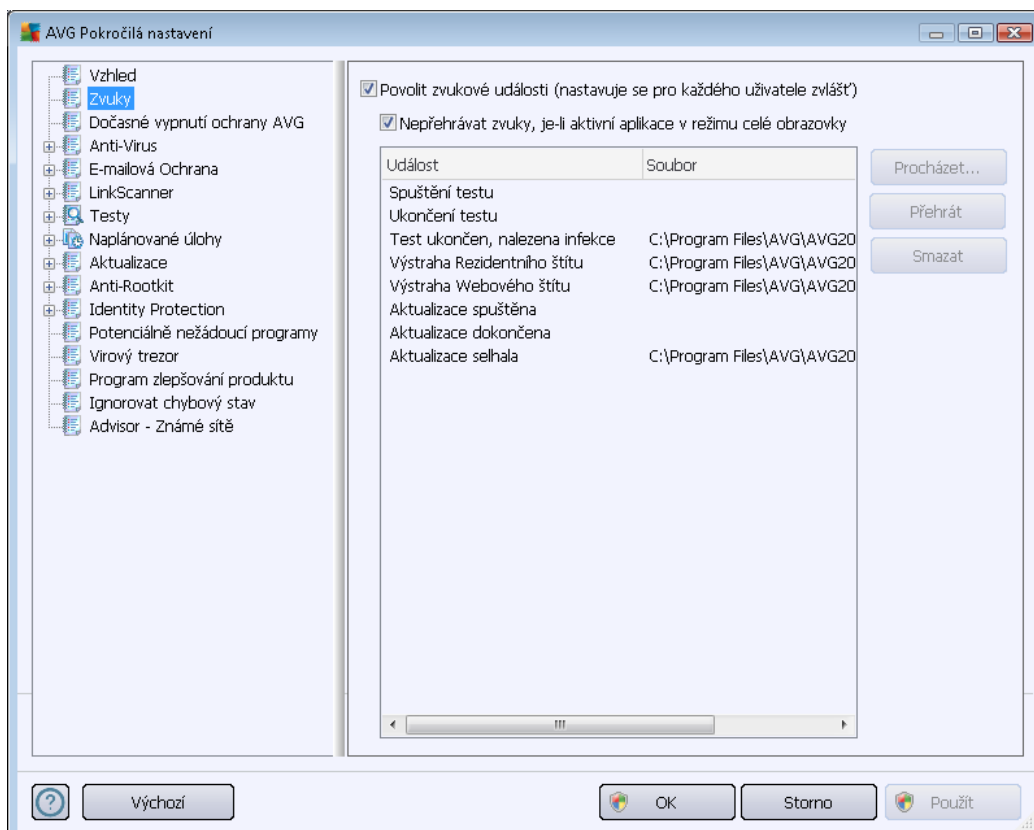


## Herní režim

Tato funkce je navržena s ohledem na aplikace, jež b ž í na celé obrazovce. Zobrazení oznámení AVG (*nap íklad informace o spušt ní testu apod.*) by v tomto p ípad p sobilo velmi rušiv (*došlo by k minimalizaci i k poškození grafiky*). Abyste této situaci p edešli, ponechejte prosím položku **Povolit herní režim pro aplikace b ž ící v režimu celé obrazovky** ozna enou (*v ýchozí nastavení*).

## 11.2. Zvuky

V dialogu **Zvuky** m ž ete rozhodnout, zda chcete být o jednotlivých akcích **AVG Internet Security 2012** informováni zvukovým oznámením:





Nastavení zvuk je platné pouze pro aktuálně otevřený uživatelský účet. Každý uživatel má tedy možnost individuálního nastavení. Přihlásíte-li se k počítači jako jiný uživatel, můžete si zvolit svou vlastní sadu zvuků. Pokud tedy chcete povolit zvukovou signalizaci, ponechte položku **Povolit zvukové události** označenou (ve výchozím nastavení je tato volba zapnutá). Tím se aktivuje seznam akcí, k nimž je možné zvukový doprovod přidat. Dále můžete označit položku **Nep e hrávat 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 [Pokročilé nastavení/Vzhled](#) tohoto dokumentu).

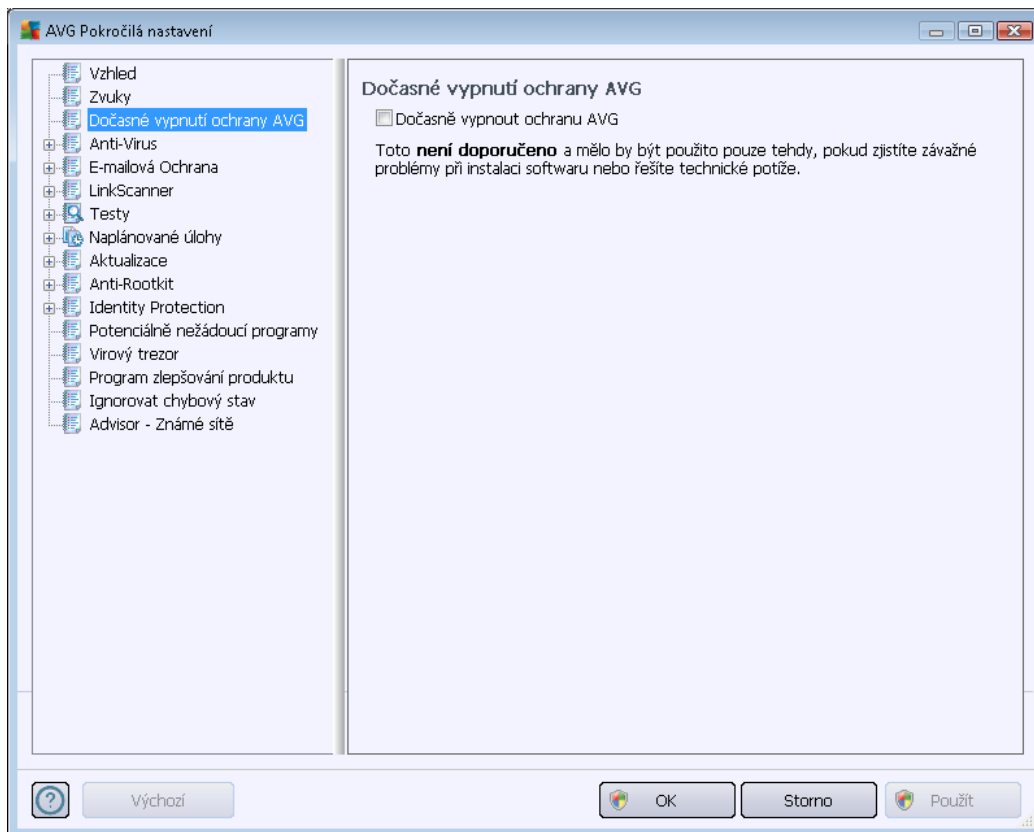
### Ovládací tlačítka dialogu

- **Procházet** - Ze seznamu událostí si vyberte tu událost, jíž 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!)
- **P e hrát** - Chcete-li si přidat zvuk poslechnout, označte v seznamu příslušnou akci a stiskněte tlačítko **P e hrát**.
- **Smazat** - Tlačítkem **Smazat** pak můžete zvuk přidat konkrétní akci zase odebrat.

### 11.3. Dočasné vypnutí ochrany AVG

V dialogu **Dočasné vypnutí ochrany AVG** máte možnost označením jediné dostupné položky jednorázově deaktivovat celou ochranu zajišťovanou programem **AVG Internet Security 2012**.

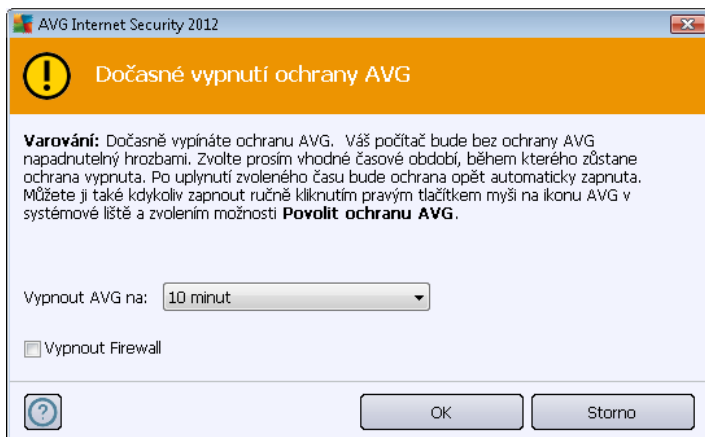
**Mjte prosím na paměti, že tato volba by v žádném případě neměla být použita, pokud to není opravdu nezbytně nutné!**



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

### Jak vypnout ochranu AVG

- Označte políčko **Dočasně vypnout ochranu AVG** a svou volbu potvrďte stiskem tlačítka **Použít**
- V nově otevřeném dialogu **Dočasné vypnutí ochrany AVG** pak nastavte požadovaný čas, po který potrubujete **AVG Internet Security 2012** vypnout. Standardně bude ochrana vypnuta po dobu 10 minut, což je dostatečné pro všechny běžné úkony. Můžete si však zvolit i delší časový interval, ale tuto možnost nedoporučujeme, pokud to není naprosto nezbytně nutné. Po uplynutí zvoleného časového intervalu se všechny vypnuté komponenty znovu automaticky aktivují. Maximální časová lhůta vynutí ochrany AVG je do přetížení restartu vašeho počítače.

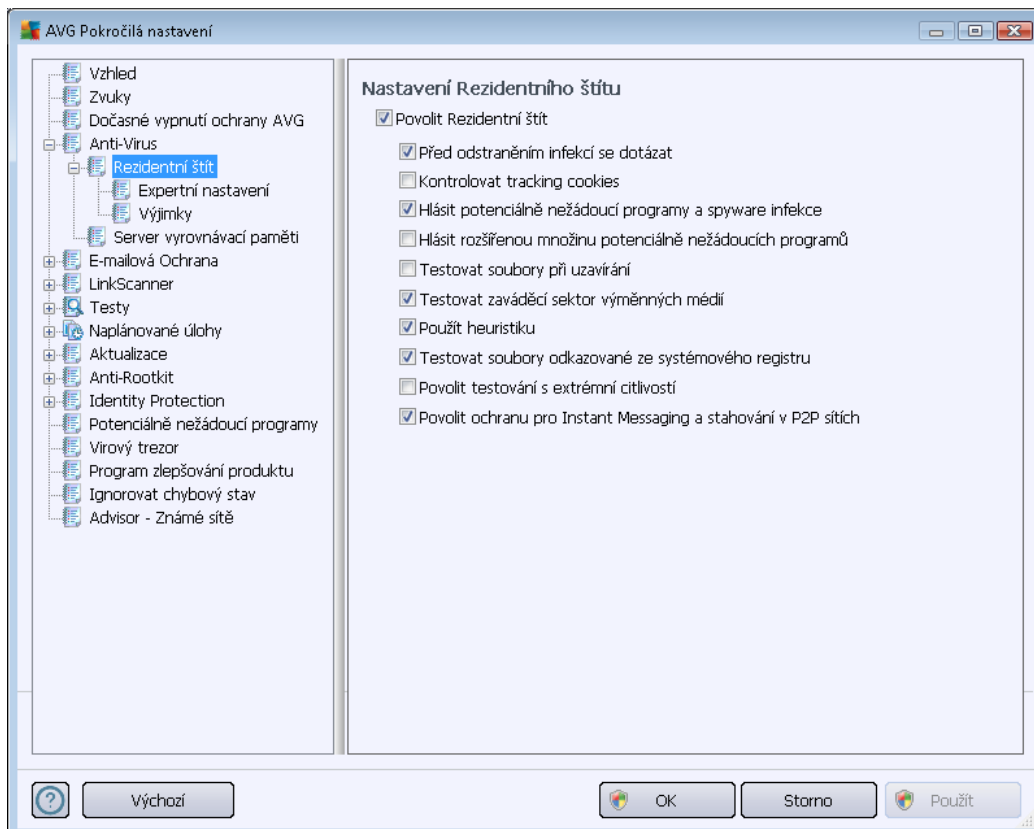


## 11.4. Anti-Virus

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

### 11.4.1. Rezidentní štít

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



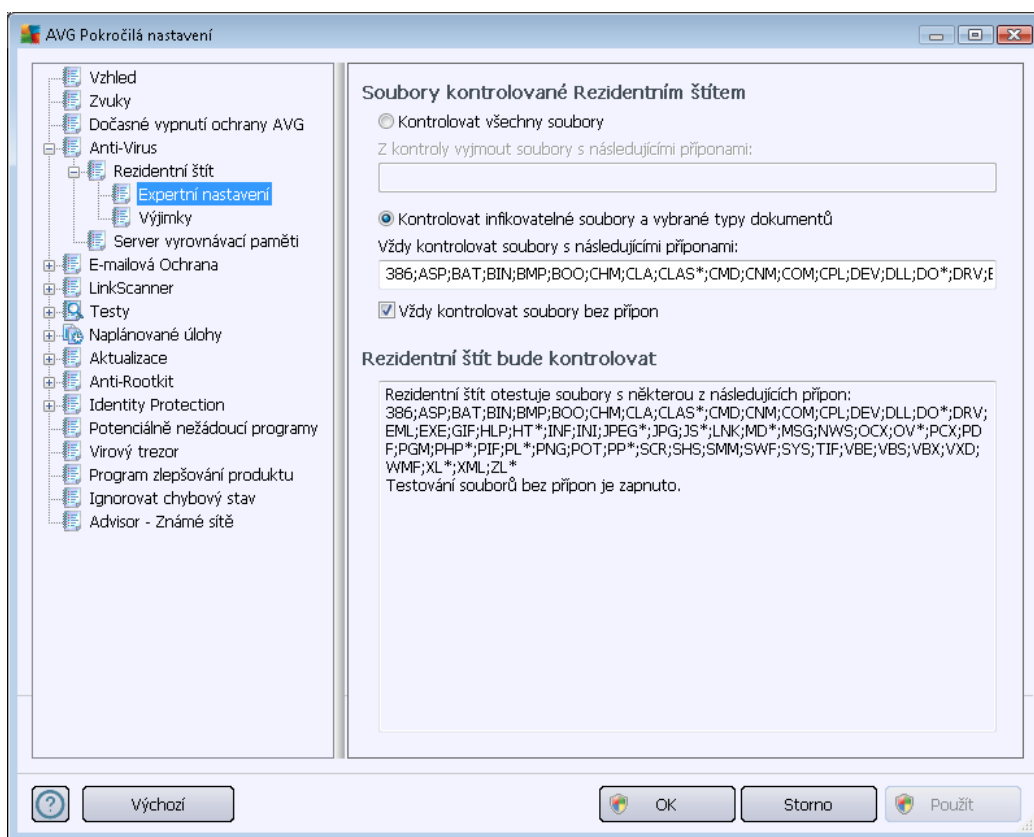


V dialogu **Nastavení Rezidentního štítu** máte možnost celkově aktivovat i deaktivovat rezidentní ochranu označením i vypnutím položky **Povolit Rezidentní štít** (*tato položka je ve výchozím nastavení zapnuta*). Dále můžete prostým výběrem rozhodnout, které funkce rezidentní ochrany mají být aktivovány:

- **Před odstraněním infekcí se dotázat** (ve výchozím nastavení zapnuto) - pokud je políčko zaškrtnuté, Rezidentní štít nebude s nalezenými infekcemi nic dříve automaticky a vždy se vás zeptá, jak si budete s nimi naložit. Pokud necháte políčko neoznačené, pak se **AVG Internet Security 2012** pokusí každou nalezenou infekci vyléčit, a pokud to nepůjde, přesune objekt do [virového trezoru](#).
- **Kontrolovat tracking cookies** (ve výchozím nastavení vypnuto) - parametr definuje, že mají být detekovány cookies (*HTTP data zaslaná serverem prohlížeči a uložena na počítači uživatele; při každé další návštěvě téhož serveru prohlížeč posílá cookies zpět serveru, který podle nich rozlišuje jednotlivé uživatele*)
- **Hlásit potenciálně nežádoucí programy a spyware infekce** (ve výchozím nastavení zapnuto) - kontrola přítomnosti [potenciálně nežádoucích programů](#) (*spustitelné programy, které mohou fungovat jako spyware nebo adware*). Zaškrtnutím tohoto políčka aktivujete [Anti-Spyware](#), tj. bude se testovat přítomnost spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány 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 může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.
- **Testovat soubory při uzavírání** (ve výchozím nastavení vypnuto) - kontrola souborů při zavírání zajišťuje, že AVG testuje aktivní objekty (např. aplikace, dokumenty, ...) nejen při jejich spuštění/otevření, ale také při zavírání; tato funkce pomáhá chránit váš počítač před sofistikovanými viry
- **Testovat zavedení cílů v médiích** (ve výchozím nastavení zapnuto)
- **Použít heuristiku** (ve výchozím nastavení zapnuto) - k detekci infekce bude použita i metoda [heuristické analýzy](#) (*dynamické emulace instrukcí testovaného objektu v prostředí virtuálního počítače*)
- **Testovat soubory odkazované ze systémového registru** (ve výchozím nastavení zapnuto) - AVG bude testovat všechny spustitelné soubory přidávané 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 nejdokladnější a nejpodrobnější testovací algoritmy. Mějte však na paměti, že tato metoda je časově velmi náročná.

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

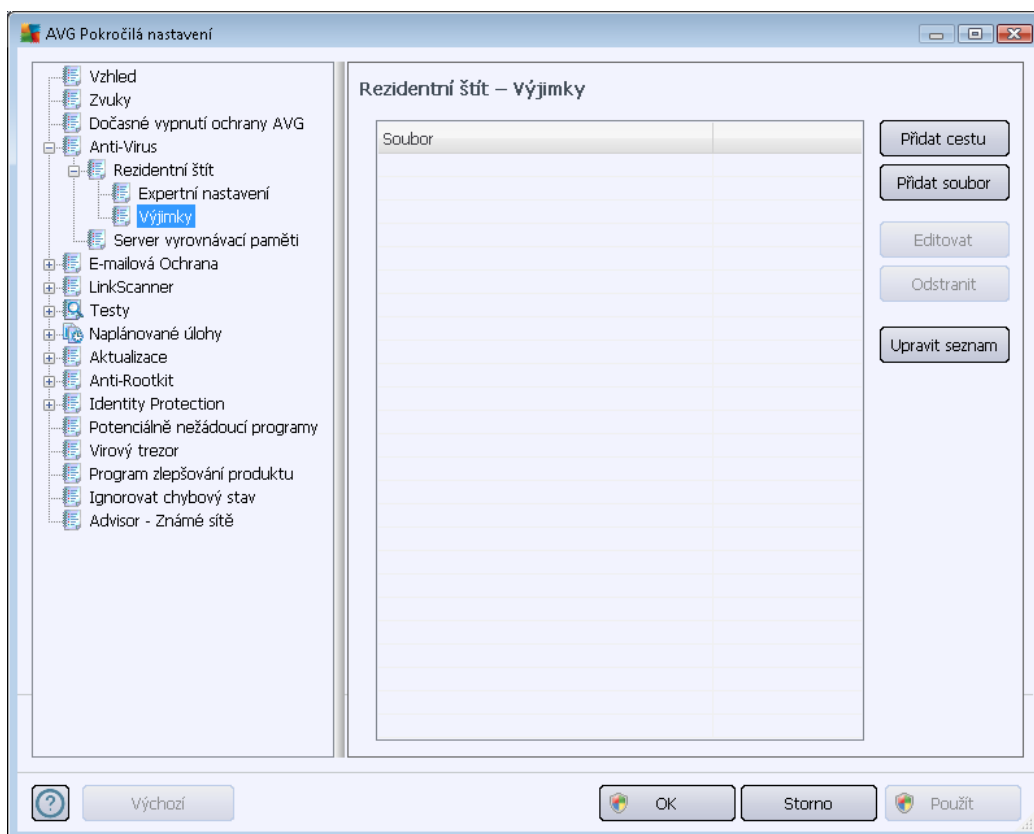
V dialogu **Soubory kontrolované Rezidentním štítem** máte možnost nastavení kontroly souborů a dokumentů vybraných typů (konkrétních přípon):



Svou volbou 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 vyňaty a seznam přípon souborů, které se mají kontrolovat za všech okolností.

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

Sekce ve spodní části dialogu nazvaná **Residentní štít bude kontrolovat** následně sumarizuje aktuální nastavení a zobrazuje detailní přehled 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!**

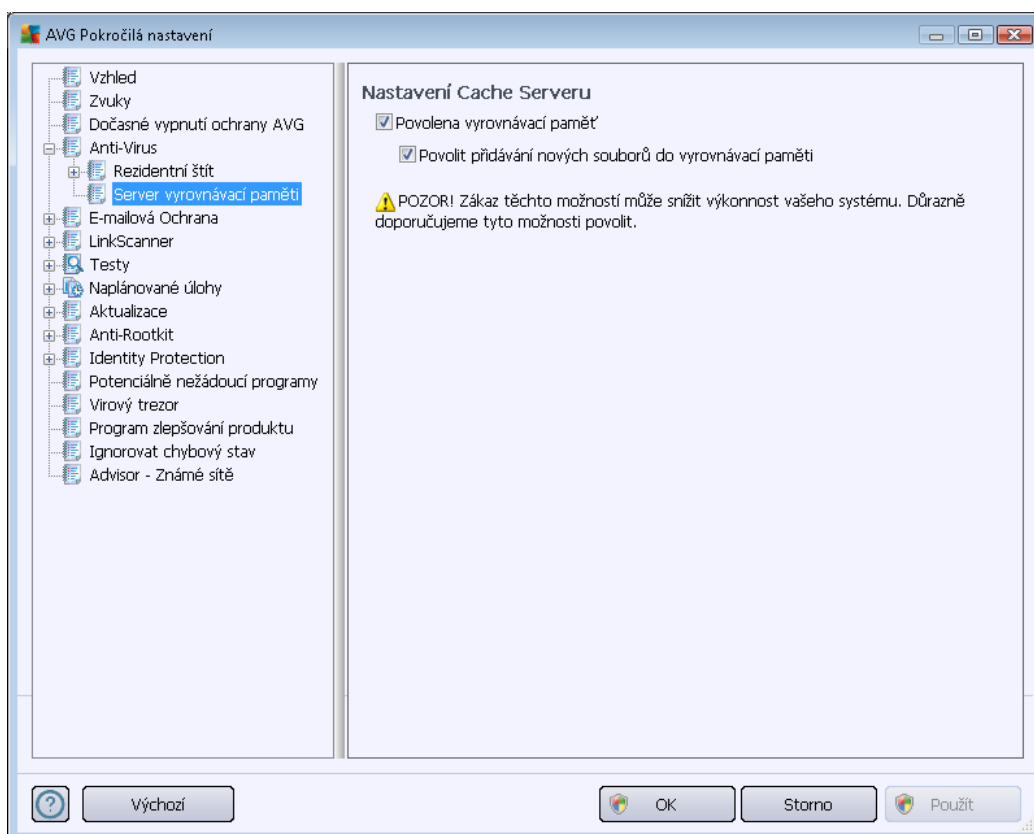
V dialogu jsou k dispozici tato ovládací tlačítka:

- **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



### 11.4.2. Server vyrovnávací paměti

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



V rámci tohoto procesu **AVG Internet Security 2012** detekuje a vyřadí nebezpečné soubory (za dříve vyřazených lze považovat například soubory digitálně podepsané z důvěryhodným zdrojem) a indexuje je. Indexované soubory jsou pak automaticky považovány za bezpečné a nemusí již být znovu testovány, dokud v nich nedojde ke změně.

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

- **Povolena vyrovnávací paměť** (ve výchozím nastavení zapnuto) - pokud tuto možnost vypnete, deaktivujete tak proces vyrovnávací paměti a vyprázdníte cache. Mějte prosím na mysli, že vypnutím tohoto procesu dojde ke zpomalení testu i celkového výkonu vašeho počítače, protože bude nutné provést test přítomnosti viru a spyware u každého jednotlivého souboru.
- **Povolit přidávání nových souborů do vyrovnávací paměti** (ve výchozím nastavení zapnuto) - pokud tuto možnost vypnete, zabráníte tak přidávání nových souborů do vyrovnávací paměti. Všechny soubory, které jsou již v paměti uloženy, budou zachovány a vynechány z testování, pokud nedojde k deaktivaci celé vyrovnávací paměti anebo do přetížení aktualizace definic.

**Pokud nemáte skutečnou potřebu od cache serveru vypínat, důrazně doporučujeme, abyste se**



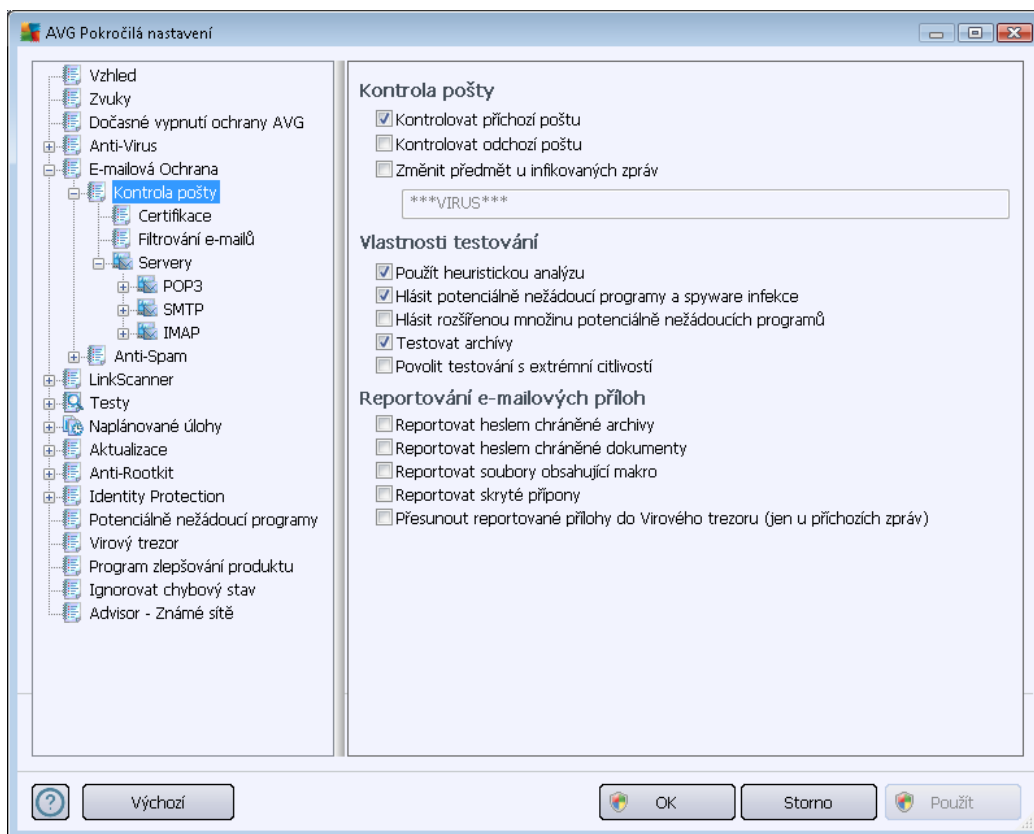
**p idrželi výchozího nastavení a ponechali ob položky zapnuté! V opa ném p ípad m že dojít k výraznému snížení rychlosti a výkonnosti Vašeho systému.**

## 11.5. E-mailová ochrana

V sekci **E-mailová ochrana** máte možnost editovat podrobné nastavení pro [Kontrola pošty](#) a [Anti-Spam](#):

### 11.5.1. 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 odeslaných z vašeho ú tu
- **Zm nit p edm t u infikovaných zpráv** (ve výchozím nastavení vypnuto) - pokud si p ežete být upozorn ni, že otestovaná zpráva byla vyhodnocena jako infikovaná, m žete aktivovat tuto položku a do textového pole vepsat požadované ozna ení takovéto e-mailové



zprávy. Tento text pak bude přidán do pole "Předmět" u každé pozitivně detekované zprávy (slouží ke snadnější identifikaci a filtrování). Výchozí hodnota je \*\*\*VIRUS\*\*\* a doporučíme 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 předměty e-mailů nejen podle předmětů, ale i podle skutečného obsahu a formátu (který předmět nemusí odpovídat). Filtrování lze nastavit v dialogu [Filtrování e-mailů](#).
- **Hlásit potenciálně nežádoucí programy a spyware infekce** (ve výchozím nastavení zapnuto) - kontrola přítomnosti [potenciálně nežádoucího programu](#) (spustitelné programy, které mohou fungovat jako spyware nebo adware). Zaškrtnutím tohoto políčka aktivujete [Anti-Spyware](#), tj. bude se testovat přítomnost spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány v domě a se souhlasem uživatele. Doporučíme ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
- **Hlásit rozšířenou množinu potenciálně nežádoucího programu** (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.
- **Testovat archívy** (ve výchozím nastavení zapnuto) - testovat obsah archivů v předmětech 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. Mějte však na paměti, že tato metoda je časově velmi náročná.

## Reportování e-mailových předmětů

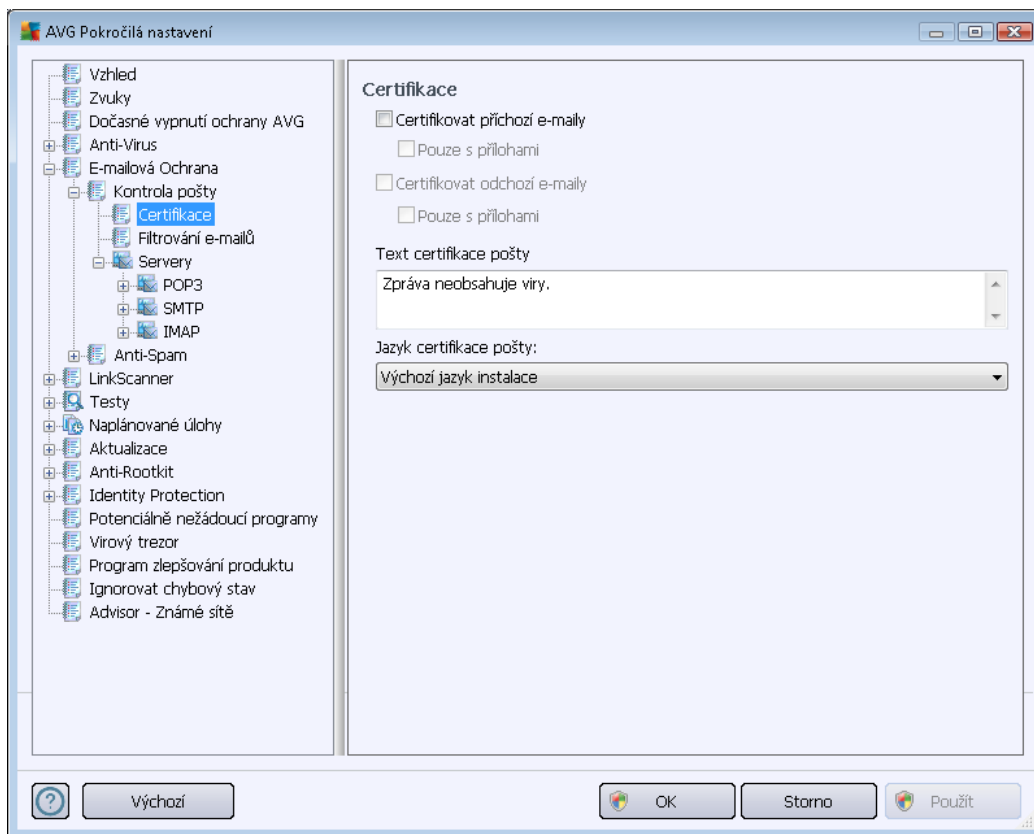
V této sekci lze nastavit reportování potenciálně nežádoucího nebo podezřelých souborů. Prosím pozor, v případě detekce takového souboru nebude zobrazen žádný dialog s varováním, e-mail bude pouze označen certifikačním textem a nález bude zaznamenán do dialogu [Nálezy Kontroly pošty](#).

- **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 otestovat na přítomnost virů; po zaškrtnutí tohoto políčka se tyto archívy budou označovat

jako potenciálně nebezpečné.

- **Reportovat soubory obsahující makro** – makro je napevno určený sled kroků, který usnadňuje uživateli často opakované složitější úkoly (*makra ve Wordu jsou typickým příkladem*). Makro může obsahovat různé instrukce, a to i potenciálně nebezpečné; chcete-li reportovat všechny dokumenty s makry, označte toto políčko.
- **Reportovat skryté přípony** – skryté přípony mohou podezřelý spustitelný soubor "naco.txt.exe" zamaskovat tak, aby se uživateli jevil jen jako neškodný textový soubor "naco.txt"; po zakštrnutí tohoto políčka budou soubory se skrytými příponami reportovány jako potenciálně nebezpečné.
- Zaškrtnutím políčka **Přesunout reportované přílohy do Virového trezoru** určíte, že všechny výše vybrané soubory z příloh e-mailů se mají nejen reportovat, ale rovněž automaticky přesouvat do [Virového trezoru](#).

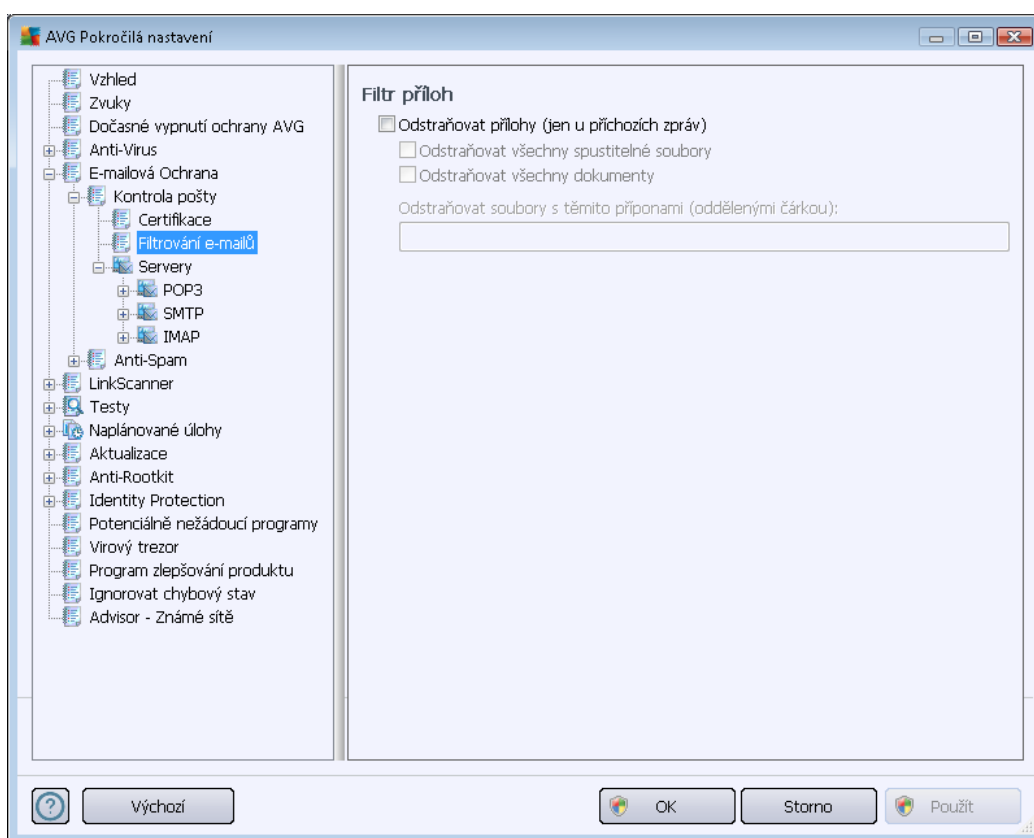
V dialogu **Certifikace** můžete označením příslušných políček rozhodnout, zda si přejete certifikovat příchozí poštu (**Certifikovat příchozí e-mail**) a/nebo odchozí poštu (**Certifikovat odchozí e-mail**). U každé z těchto voleb můžete dále označením možnosti **Pouze s přílohami** nastavit parametr, který určuje, že v rámci příchozí i odchozí pošty budou certifikovány pouze přílohy.



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

neobsahuje viry. Tuto informaci můžete doplnit i 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!



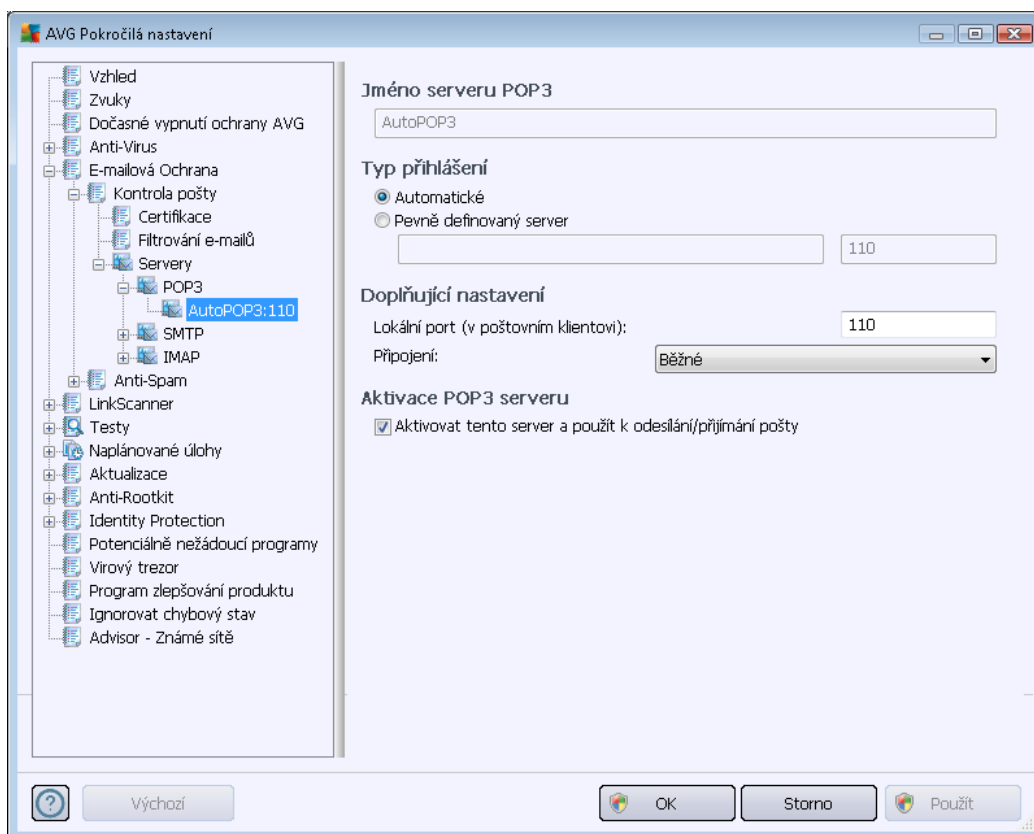
Dialog **Filtr příloh** umožňuje nastavení parametrů pro testování příloh e-mailových zpráv. Ve výchozím nastavení je možnost **Odstraňovat přílohy** vypnuta. Pokud se rozhodnete pro její aktivaci, budou automaticky odstraněny všechny přílohy zpráv, které byly detekovány jako infikované nebo potenciálně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

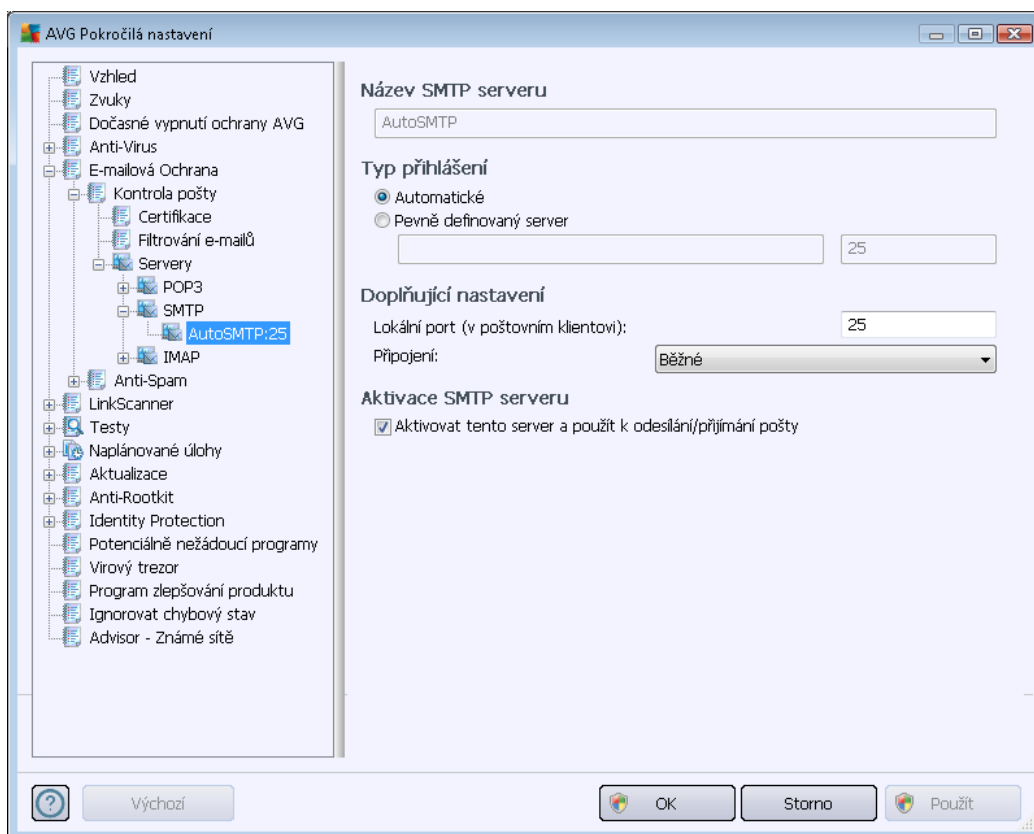


V tomto dialogu (odkaz **Servery / POP3**) nastavujete server [Kontroly pošty](#) s protokolem POP3 pro příchozí pošty:

- **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 (*standardní/zabezpečené na vyhrazeném portu/zabezpečené na běžném portu*). Pokud zvolíte zabezpečené připojení, budou posílaná data kryptována a nebude možné jejich sledování nikým jiným. I tato funkce může být aktivována pouze v případě, že ji cílový poštovní server podporuje.
- **Aktivace POP3 serveru** - zapnutím/vypnutím položky máte možnost aktivovat či deaktivovat právě nastavený POP3 server

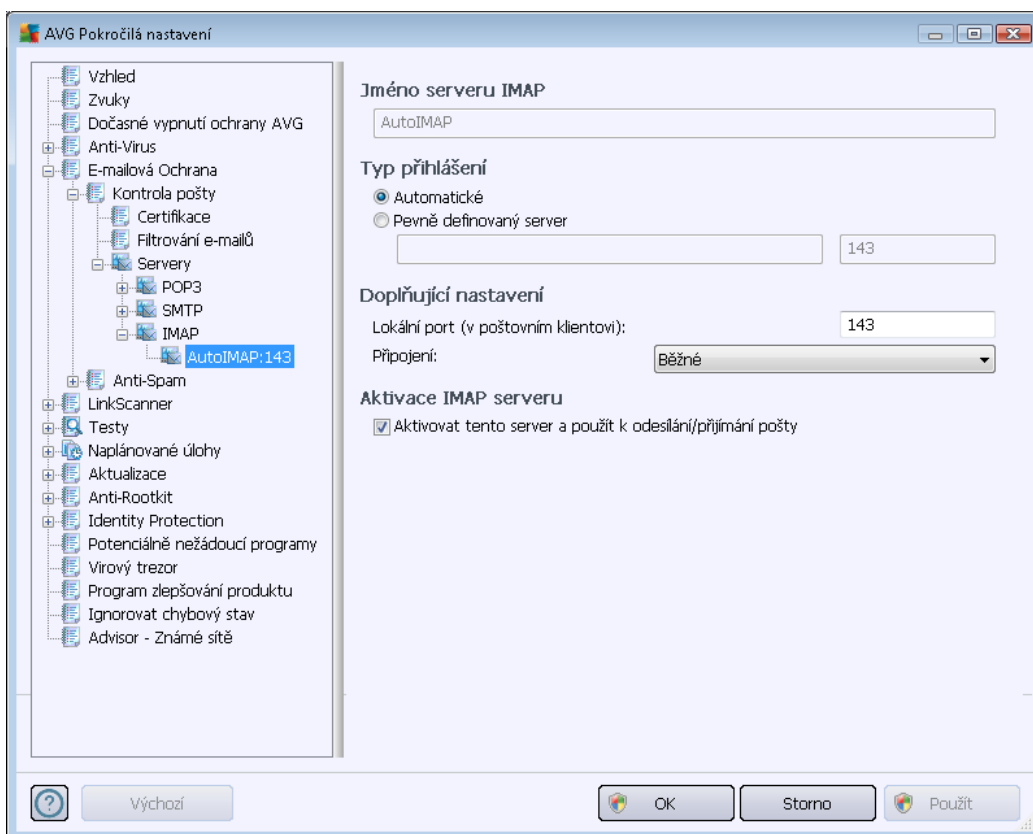


V tomto dialogu (odkaz **Servery / SMTP**) nastavujete server **Kontroly pošty** s protokolem SMTP pro odchozí poštu:

- **Název SMTP serveru** - v tomto poli můžete zadat jméno nově 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 (*standardní/zabezpečené na vyhrazeném portu/zabezpečené na běžném portu*). Pokud zvolíte zabezpečené připojení, budou posílaná data kryptována a nebude možné jejich sledování nikým jiným. Tato funkce může být aktivována pouze v případě, že cílový poštovní server podporuje.
- **Aktivace SMTP serveru** - zapnutím/vypnutím položky máte možnost aktivovat či deaktivovat právě nastavený SMTP server



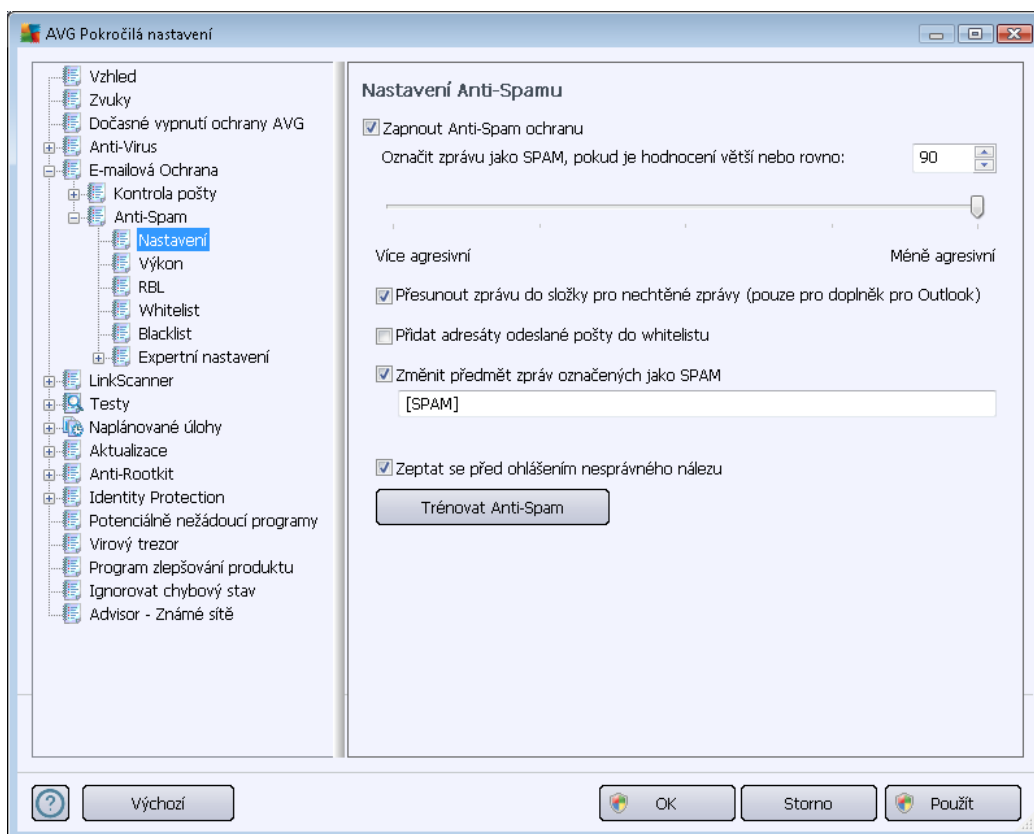
V tomto dialogu (odkaz **Servery / IMAP**) nastavujete server **Kontroly pošty** s protokolem IMAP pro odchozí poštu:

- **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.
  - **Typ spojení** - v této rozbalovací nabídce můžete specifikovat typ spojení (*standardní/zabezpečené na vyhrazeném portu/zabezpečené na běžném portu*). Pokud zvolíte zabezpečené spojení, budou posílaná data kryptována a nebude možné jejich sledování nikým jiným. 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

### 11.5.2. Anti-Spam



V dialogu **Nastavení Anti-Spamu** můžete označením položky **Zapnout Anti-Spam ochranu** celkově povolit či zakázat funkci služby **Anti-Spam**.

V tomto dialogu také můžete definovat, jak chcete nastavit úroveň ochrany proti spamu - více či méně agresivní. Na základě několika dynamických testovacích technik pak filtr komponenty **Anti-Spam** přiřadí každé zprávě určitou skóre (například podle toho, nakolik se obsah zprávy blíží textu, který lze považovat za spam). Hodnotu úrovně citlivosti pro označení spamu lze nastavit buď pomocí vepsání číselné hodnoty do příslušného pole nebo pomocí posuvníku (v rozsahu hodnot 50-90).

Obecně doporučujeme nastavit úroveň citlivosti na spam v rozmezí 50-90. Následuje přehled úrovní ochrany, jež odpovídají jednotlivým hodnotám:

- **Hodnota 80-90** - E-mailové zprávy, u nichž se dá předpokládat charakter spamu, budou odfiltrovány. Je možné, že omylem dojde k odfiltrování některých zpráv, jež nejsou spamového charakteru.
- **Hodnota 60-79** - Toto nastavení je již považováno za poměrně agresivní konfiguraci. E-mailové zprávy, které mohou být považovány za spam, budou odfiltrovány. Současně však dojde k poměrně velkému odchytu zpráv, které nejsou spamového charakteru, ale na základě určitých znaků mohou být takto vyhodnoceny.
- **Hodnota 50-59** - Velmi agresivní konfigurace. Nespamové e-mailové zprávy budou ve větší míře odfiltrovány spolu se zprávami pozitivně detekovanými jako spam. **Tato konfigurace**



*už není doporučeným nastavením pro běžné uživatele.*

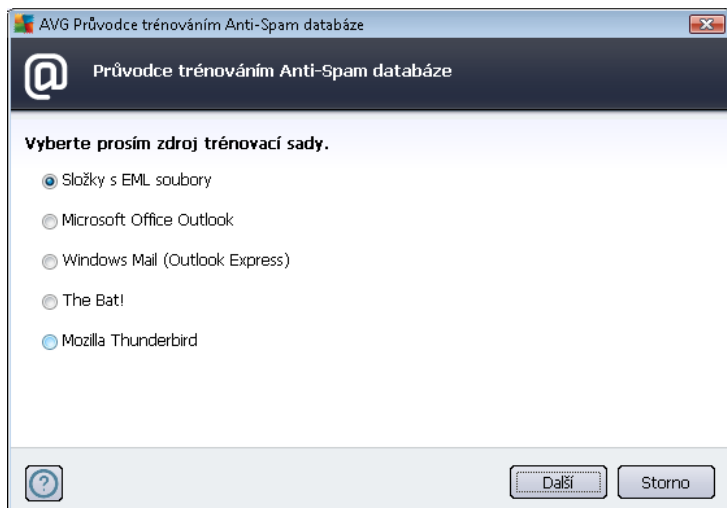
V dialogu **Nastavení Anti-Spamu** můžete dále nastavit, jak se má zacházet s e-mailovými zprávami pozitivně detekovanými jako spam:

- **Přesunout zprávu do složky pro nechtěné zprávy (pouze pro doplněk pro Outlook)** - Označením této položky zvolíte, že každá zpráva, jejíž obsah bude se zohledněním nastavené úrovně citlivosti označen jako spam, bude automaticky přesunuta do složky pro nevyžádané zprávy. Tato možnost platí pouze pro poštovní program MS Outlook.
- **Přidat adresáty odeslané pošty do [whitelistu](#)** - Označením této položky potvrdíte, že adresáti vámi odeslaných e-mailových zpráv jsou považováni za důvěryhodné a pošta odeslaná z jejich útu může být bez obav doručena.
- **Zmítnout zprávy u zpráv označených jako spam** - Označením této položky aktivujete textové pole, v němž máte možnost editovat text, kterým si přejete označovat zprávy detekované jako spam - tento text pak bude automaticky vepsán do pole u každé detekované e-mailové zprávy.
- **Zeptat se před ohlášením nesprávného dotazu** - Pokud jste během [instalace](#) potvrdili svou účast v [Programu zlepšování produktu](#), povolili jste odesílání reportů o detekovaných hrozbách do AVG. Tato hlášení jsou odesílána automaticky. Pokud si však přejete mít možnost zkontrolovat, že detekovaná zpráva má být skutečně klasifikována jako spam, označte položku **Zeptat se před ohlášením nesprávného dotazu** a před odesláním reportu vám bude zobrazen dotazovací dialog vyžadující vaše potvrzení.

### Ovládací tlačítka dialogu

Tlačítko **Trénovat Anti-Spam** otevírá [Průvodce trénováním Anti-Spam databáze](#). Popis jednotlivých kroků průvodce najdete v [samostatné kapitole](#).

V prvním dialogu **Průvodce trénováním Anti-Spam databáze** je nutno vybrat zdroj e-mailových zpráv, které chcete pro trénink použít. K trénování se obvykle používají zprávy, které byly anti-spamovou ochranou mylně označeny jako spam, nebo naopak nevyžádané zprávy, které prošly anti-spamovou ochranou bez povšimnutí.



Na výběr jsou následující možnosti:

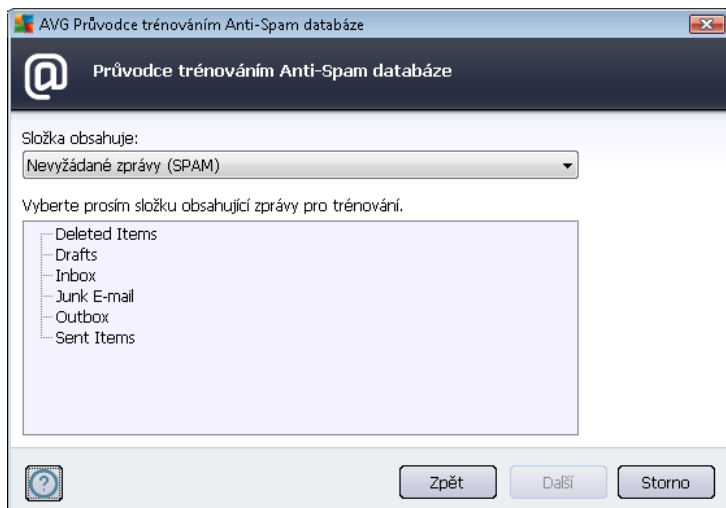
- **Konkrétní e-mailový program** - pokud používáte některý z uvedených e-mailových programů (*MS Outlook, Outlook Express, The Bat!*), jednoduše vyberte příslušnou možnost
- **Složky s EML soubory** - používáte-li jiný e-mailový program, než které jsou v dialogu uvedeny, pak je vhodné nejdříve požadované zprávy uložit do nějakého adresáře na disk (ve formátu *.eml*), nebo se ujistit, že víte, kam váš e-mailový program zprávy ukládá. Poté zvolte možnost **Složky s EML soubory**; v dalším kroku budete moci zadat umístění těchto složek.

Chcete-li průběh trénování co nejvíce urychlit a zjednodušit, doporučujeme e-mailové zprávy doporučit jít tak, aby ve zvolené složce byly umístěny pouze ty zprávy, které chcete použít pro trénink - žádané a nevyžádané zvlášť. Nicméně není to nutné, protože před zahájením samotného trénování budete mít možnost zprávy filtrovat.

Jakmile je zvolena požadovaná možnost, stiskněte tlačítko **Další** a přejděte k dalšímu kroku.

Zobrazení dialogu v tomto kroku průvodce závisí na vaší předchozí volbě.

### **Volba složky s EML soubory**



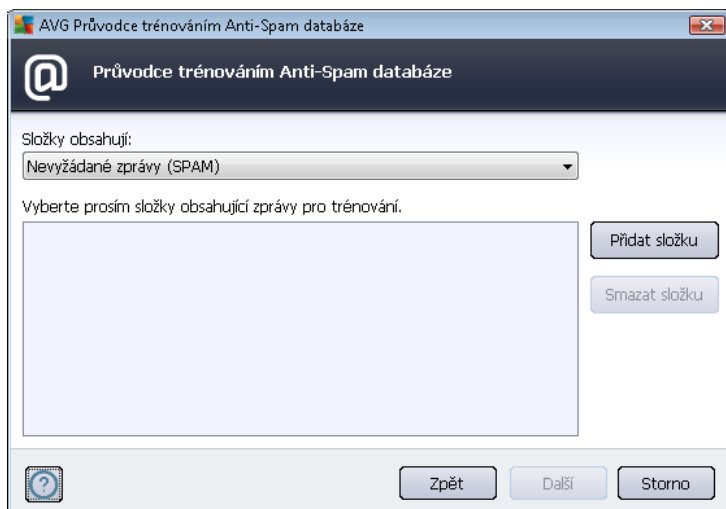
V tomto dialogu volíte složku se zprávami, které chcete pro trénování použít. Stiskn te tlačítko **Přidat složku** a ur čete umíst ění adresář e s .eml soubory (*uloženými e-maily*). Cesta k vybranému adresá ři pak bude zobrazena v dialogu. Pro odebrání složky ze seznamu použijte tlačítko **Smazat složku** po jejím ozna ění.

V rozbalovací nabídce **Složka obsahuje** zadejte, jaké zprávy se ve vybrané složce nacházejí - zda vyžádané (tzv. *HAM*), nebo nevyžádané (*SPAM*). V dalším dialogu budete moci zprávy ve složce filtrovat, takže složka nemusí obsahovat pouze e-maily ur čené k trénování.

Chcete-li pokrač ovat, stiskn te tlačítko **Následující** a pokrač ujte k část [Zp sob filtrování zpráv](#).

### Volba konkrétního e-mailového programu

Pokud jste vybrali n který e-mailový program, zobrazí se nový dialog se složkami.

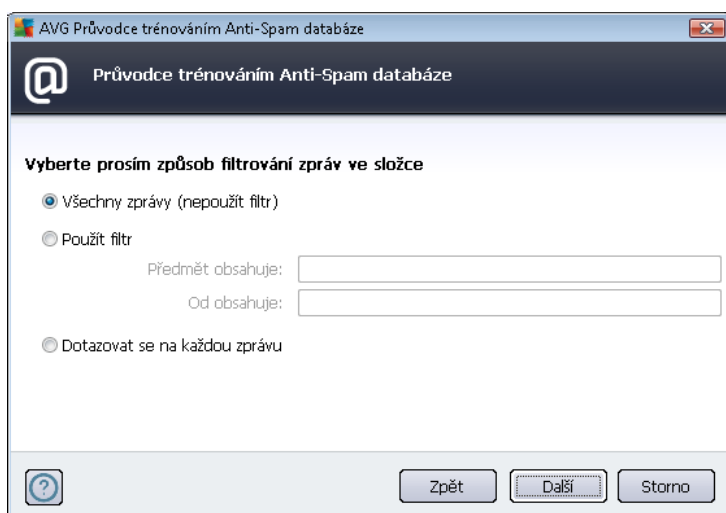


**Poznámka:** V p říp ad Microsoft Office Outlook bude nejprve pot eba zvolit MS Office Outlook

profil.

V rozbalovací nabídce **Složka obsahuje** zadejte, jaké zprávy se ve vybrané složce nacházejí - zda vyžádané (tzv. *HAM*), nebo nevyžádané (*SPAM*). V dalším dialogu budete moci zprávy ve složce filtrovat, takže složka nemusí obsahovat pouze e-maily určené k trénování. V hlavní sekci dialogu je zobrazen navigační strom příslušného e-mailového programu. Vyberte složku obsahující e-maily k trénování a označte ji.

Stiskem tlačítka **Další** pokračujte k části [Způsob filtrování zpráv](#).



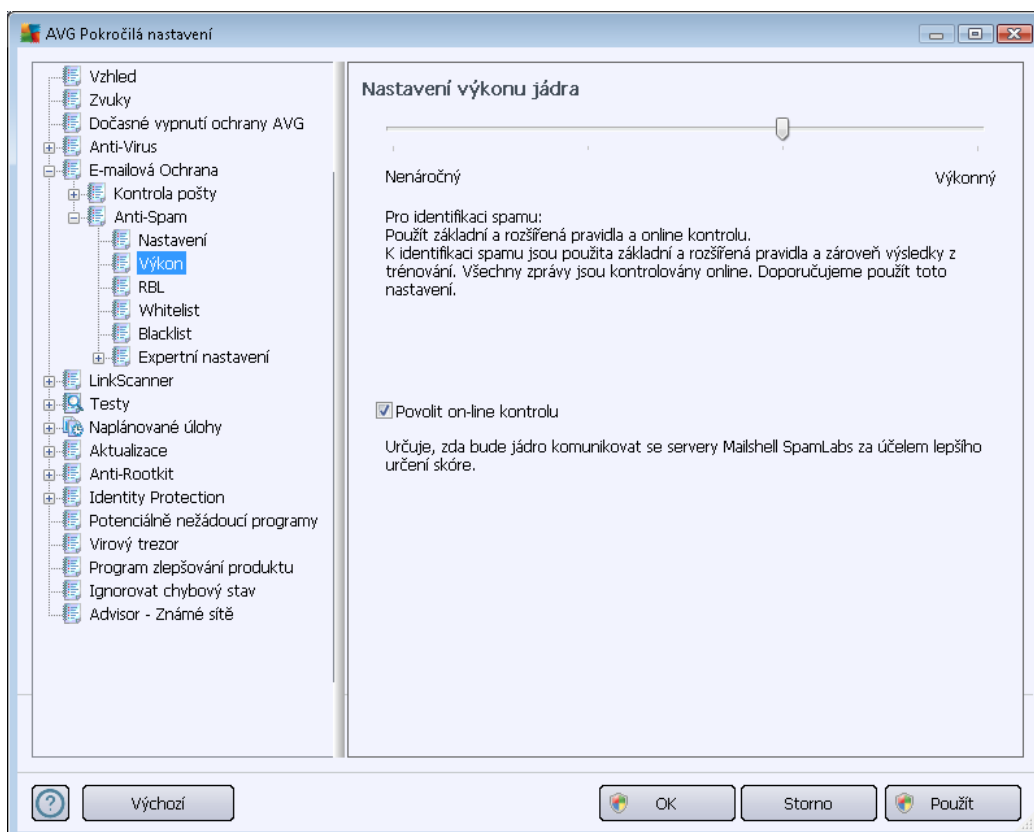
V tomto dialogu můžete zvolit možnosti filtrování zpráv ve vybrané složce:

- **Všechny zprávy (nepoužít filtr)** - Jste-li si jisti, že složka obsahuje pouze zprávy, které chcete použít k trénování, a žádné další, zvolte možnost **Všechny zprávy (nepoužít filtr)**.
- **Použít filtr** - Tuto alternativu zvolte v případě, že chcete zprávy filtrovat pokračujícím způsobem. Do textových polí můžete doplnit slovo (*jméno*), část slova nebo více slov, která se mají vyhledávat v polích "Odesílatel" a "Předmět" v hlavě zprávy. Všechny e-maily, které budou tímto kritériím přesně vyhovovat, budou bez dalších dotazů použity k trénování. Vyplníte-li oba textová pole (*Předmět obsahuje:* a *Od obsahuje:*), budou k trénování použity i zprávy, které vyhoví jen jedné z obou podmínek!
- **Dotazovat se na každou zprávu** - Pokud si nejste jisti, jaké zprávy složka obsahuje, a chcete, aby se průvodce u každé z nich zeptal, zda ji chcete nebo nechcete použít k trénování, pak zvolte možnost **Dotazovat se na každou zprávu**.

Jakmile máte vybránu příslušnou možnost filtrování, stiskněte tlačítko **Další**. V následujícím informativním dialogu potvrdíte svou volbu opět tlačítkem **Další**. Poté bude zahájeno trénování zpráv podle zvolených kritérií.



Dialog **Nastavení výkonu jádra** (odkazovaný položkou **Výkon**) nabízí možnost konfigurace parametrů výkonu komponenty **Anti-Spam**:



Položkou posuvníku určete úroveň testovacího výkonu na ose **Nenáročný / Výkonný** režim.

- **Výkonný režim** spotřebuje velký objem paměti. Během testovacího procesu budou k identifikaci spamu použity následující parametry: pravidla a spamové databáze, základní a pokročilá nastavení, IP adresy spammerů a spamové databáze.
- **Nenáročný režim** znamená, že během testovacího procesu nebudou k identifikaci spamu použita žádná pravidla. Identifikace spamu bude založena výhradně na porovnání s testovacími daty. Tento režim pro běžné používání nedoporučujeme, nastavení lze doporučit výhradně u počítačů s velmi nízkou úrovní hardwarového vybavení.

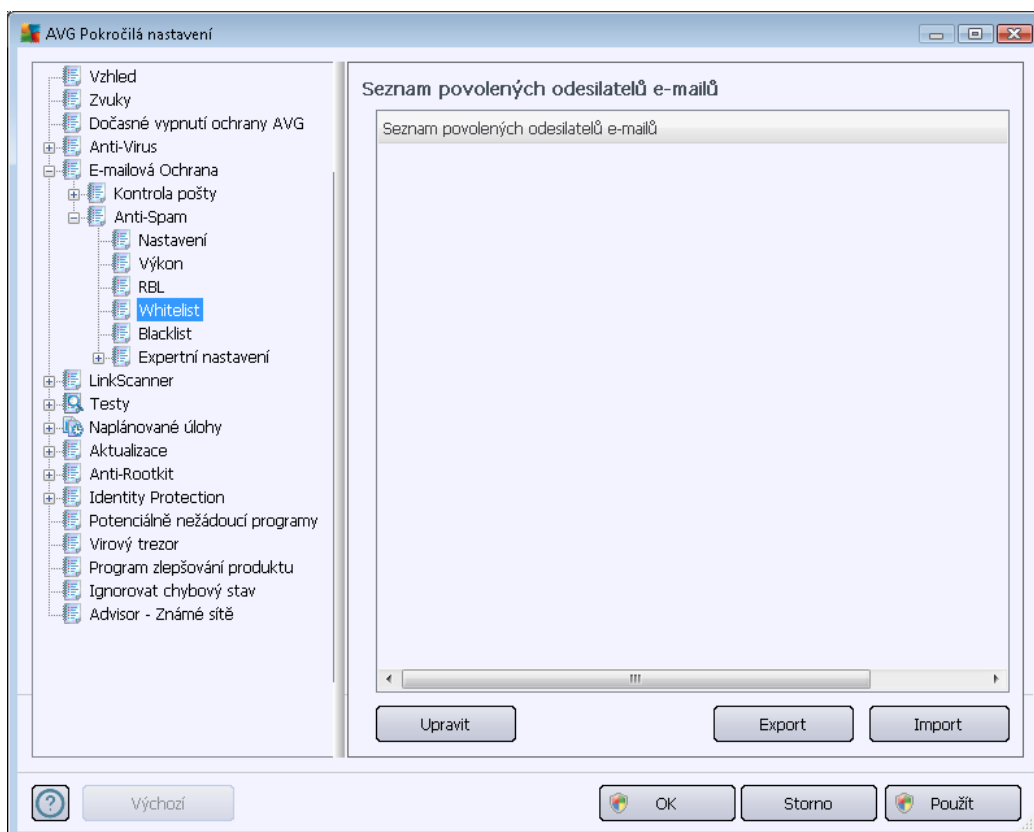
Položka **Povolit on-line kontrolu** je ve výchozím nastavení označena a určuje, že pro přesnější detekci spamu bude k testování použita i komunikace se servery společnosti [Mailshell](#), a během testování budou testovaná data porovnávána s databází této společnosti v online režimu.

**Obecně doporučujeme dodržet výchozí nastavení, pokud nemáte skutečný důvod tuto konfiguraci změnit. Změnu parametru nastavení výkonu jádra lze doporučit výhradně znalým a zkušeným uživatelům!**





Položka **RBL** otevírá editační dialog **Realtime Blackhole Lists**, v němž máte možnost povolit funkci **Dotazovat RBL servery**.

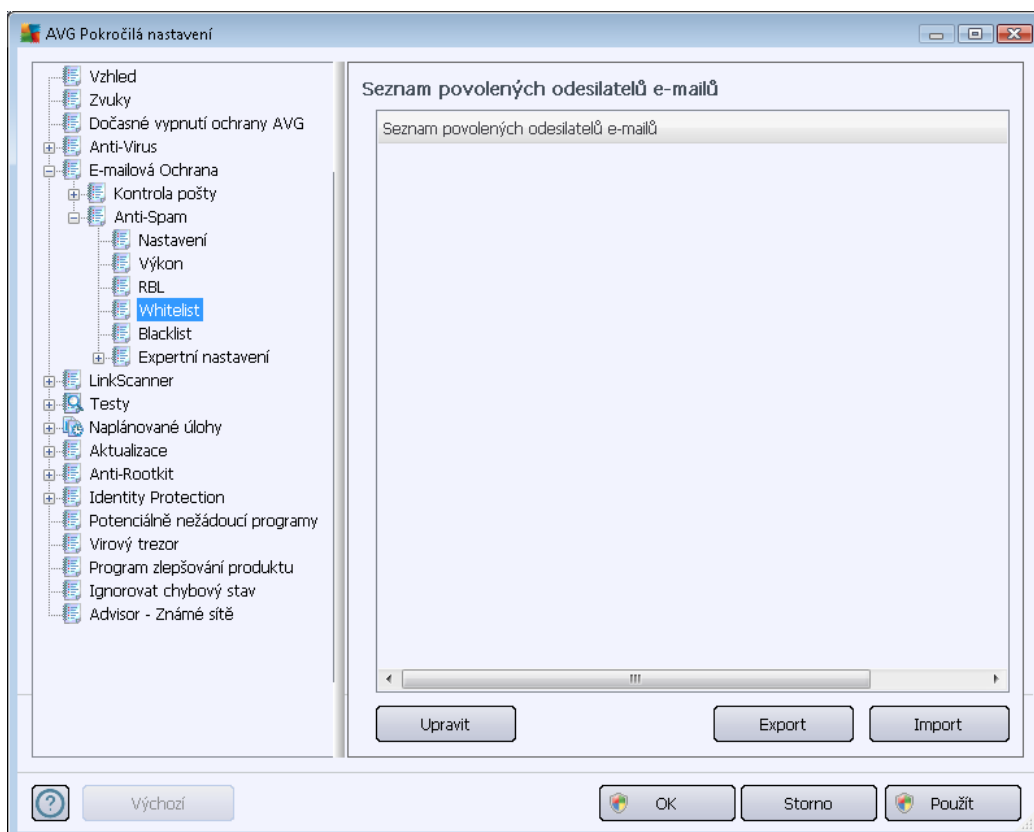


RBL (*Realtime Blackhole List*) server je DNS server s rozsáhlou databází známých odesílatelů spamu. Při zapnutí této funkce budou všechny příchozí zprávy v reálném čase porovnávány s RBL databází a při nalezení shody označeny jako spam. Databáze RBL server obsahuje skutečně nejnovější a neaktuálnější záznamy o existujících centrech spamu a díky porovnávání e-mailových zpráv proti těmto databázím lze dosáhnout maximální úrovně ochrany před nevyžádanou poštou. Tato vlastnost se hodí zejména pro uživatele, kteří dostávají velké množství spamových zpráv, jež nemohou být detekovány pouze na základě pravidel definovaných jádrem služby [Anti-Spam](#).

Položka **Seznam RBL server** vám dále umožní nastavit adresy konkrétních serverů, na nichž jsou tyto spamové databáze umístěny (*zapnutí této služby může na některých operačních systémech a konfiguracích zpomalit proces příjmu pošty, protože každá jednotlivá zpráva musí být prověřena proti databázi RBL serveru*).

**Touto službou nedochází k odesílání žádných osobních nebo citlivých dat!**

Položka **Whitelist** otevírá dialog se seznamem e-mailových adres a doménových jmen, u nichž víte, že pošta z těchto adres/domén doručena nikdy nebude mít charakter spamu:



V editačním rozhraní máte možnost sestavit seznam odesílatelů, u nichž předpokládáte, že vám nikdy nepošlou poštu, kterou lze považovat za spam (*nevyžádanou poštu*). Můžete také sestavit seznam kompletních doménových jmen (*například avg.com*), o nichž víte, že negenerují nevyžádanou poštu. Jakmile budete mít připraven tento seznam adres a domén, můžete je zadat do **Whitelistu** dvěma způsoby: pomocí vložením jednotlivých adres nebo jednorázovým importem celého seznamu.

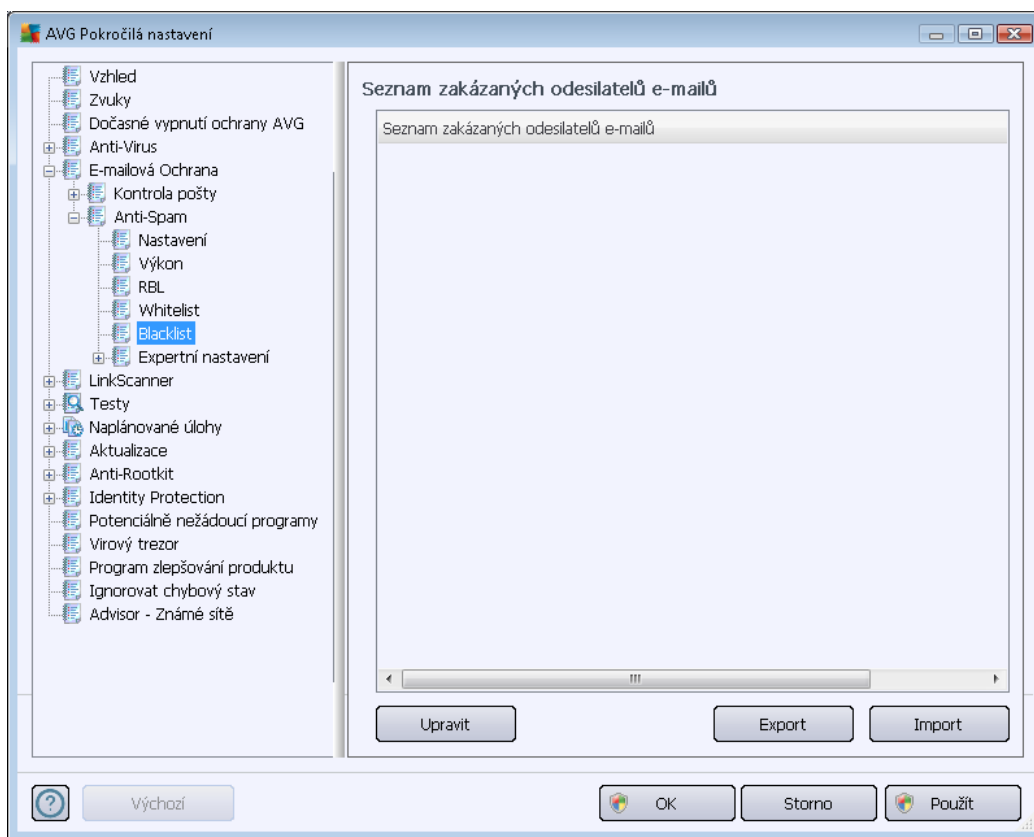
### Ovládací tlačítka dialogu

K dispozici jsou vám tato ovládací tlačítka:

- **Upravit** - stiskem tohoto tlačítka otevřete dialog, v němž můžete manuálně přidávat adresy ze seznamu (*můžete také použít jednorázovou metodu "kopírovat a vložit"*). Adresy/doménová jména vkládejte po jednom na každý řádek.
- **Export** - pokud budete z libovolného důvodu chtít seznam adres/doménových jmen exportovat, můžete export provést pomocí tohoto tlačítka. Veškeré záznamy budou uloženy ve formátu prostého textu.

- **Import** - pokud již máte seznam adres/doménových jmen uložený v textovém souboru, můžete jej snadno importovat za použití tohoto tlačítka. Obsah seznamu musí být rozdělen tak, že každý řádek obsahuje pouze jedinou položku (*adresu nebo doménové jméno*).

Položka **Blacklist** otevírá dialog se seznamem e-mailových adres a doménových jmen, která mají být zablokována pro příjem jakékoliv pošty. To znamená, že pošta odeslaná z kterékoliv uvedené adresy nebo domény bude vždy označena jako spam:



V editačním rozhraní máte možnost sestavit seznam odesílatelů, u nichž předpokládáte, že poštu, kterou vám posílají, lze považovat za spam (*nevyžádaná pošta*). Můžete také sestavit seznam kompletních doménových jmen (*například spammingcompany.com*), u nichž je předpoklad, že budou generovat nevyžádanou poštu. Pošta odeslaná z kterékoliv uvedené adresy bude pak detekována jako spam. Jakmile budete mít připraven tento seznam adres a domén, můžete je zadat do **Blacklistu** dvěma způsoby: pomocí vložením jednotlivých adres nebo jednorázovým importem celého seznamu.

### Ovládací tlačítka dialogu

K dispozici jsou vám tato ovládací tlačítka:

- **Upravit** - stiskem tohoto tlačítka otevřete dialog, v němž můžete manuálně přidávat adresy ze seznamu (*můžete také použít jednorázovou metodu "kopírovat a vložit"*). Adresy/



doménová jména vkládejte po jednom na každý řádek.

- **Export** - pokud budete z libovolného důvodu chtít seznam adres/doménových jmen exportovat, můžete export provést pomocí tohoto tlačítka. Veškeré záznamy budou uloženy ve formátu prostého textu.
- **Import** - pokud již máte seznam adres/doménových jmen uložený v textovém souboru, můžete jej snadno importovat za použití tohoto tlačítka. Soubor, z něhož import provádíte, musí být ve formátu prostého textu a obsah musí být rozdelen tak, že každý řádek obsahuje pouze jedinou položku (*adresu nebo doménové jméno*).

*V této Pokročilé nastavení obsahuje rozsáhlé možnosti nastavení komponenty Anti-Spam. Tato nastavení jsou určena výhradně pokročilým uživatelům, jako jsou správci sítí, kteří potřebují antispamovou ochranu nastavit do detailů pro co nejlepší ochranu e-mailových serverů. Z tohoto důvodu není v dialogích pokročilého nastavení dostupná běžná nápověda, pouze stručný popis příslušné funkce přímo v dialogu.*

*Doporučujeme neměnit žádná pokročilá nastavení, pokud nejste dobře obeznámeni se všemi funkcemi nástroje Spamcatcher (MailShell Inc.). Nevhodné změny nastavení by mohly vyústit v nespolehlivost až nefunkčnost celé komponenty.*

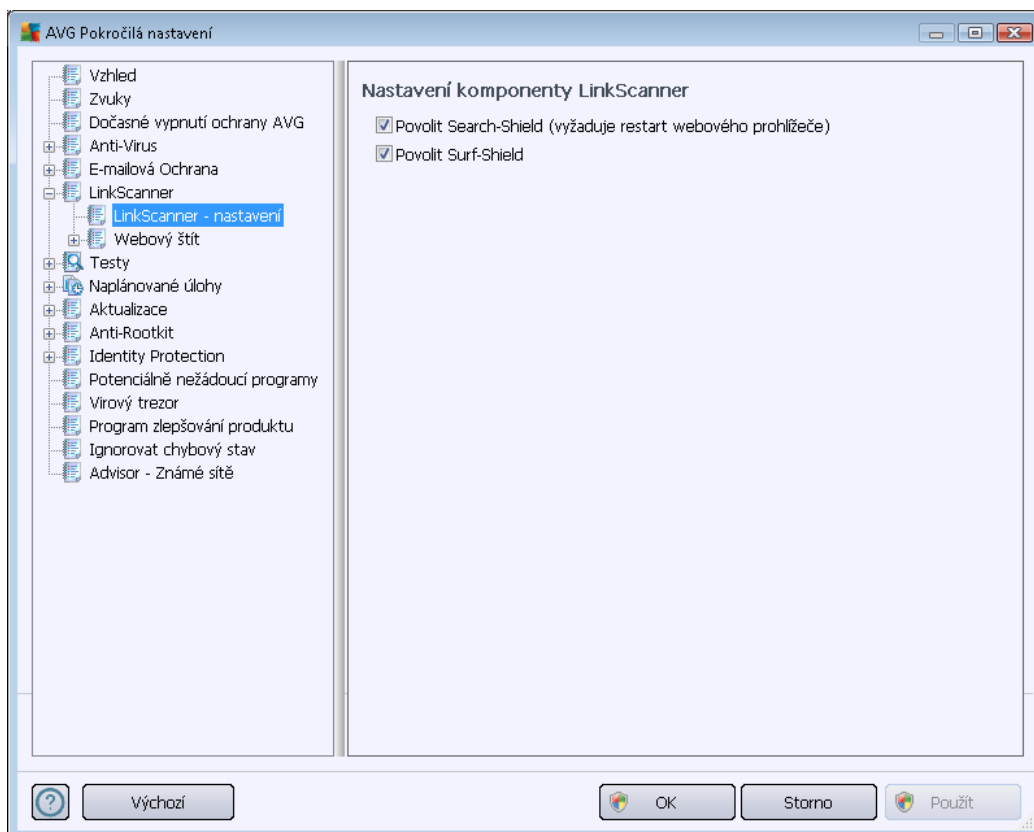
Pokud se přesto domníváte, že je nutné změnit konfiguraci služby [Anti-Spam](#) na úrovni pokročilého nastavení, pokračujte prosím podle instrukcí uvedených přímo v dialogu. Obecně platí, že v každém dialogu máte možnost zapnout jednu konkrétní funkci služby [Anti-Spam](#) a její popis je uveden přímo v dialogu:

- **Paměť** - fingerprint, reputace domén, LegitRepute
- **Trénování** - počet slovních záznamů, práh pro samotrénování, váha
- **Filtrování** - seznam jazyků, seznam zemí, povolené IP adresy, blokové IP adresy, blokové země, blokové znakové sady, falešní odesílatelé
- **RBL** - RBL servery, multidetekce, práh, časový limit, maximum IP adres
- **Internetové připojení** - časový limit, proxy server, autentifikace proxy

## 11.6. LinkScanner

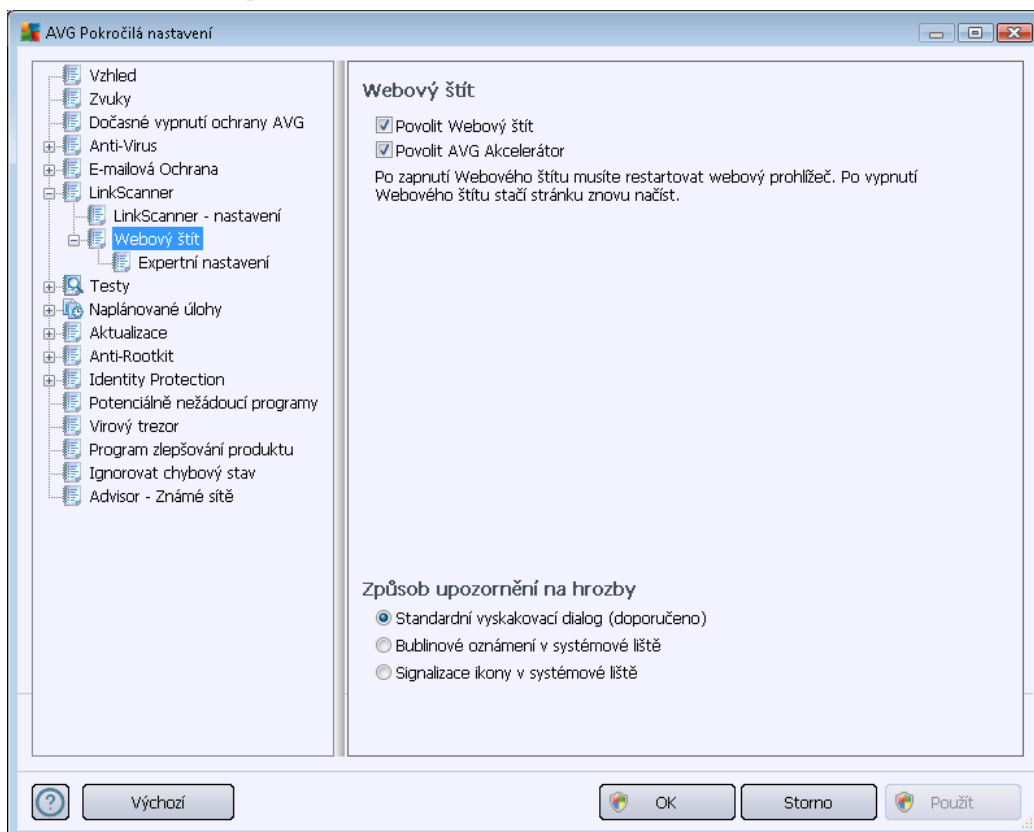
### 11.6.1. LinkScanner - nastavení

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, eBay, Twitter, 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.

## 11.6.2. Webový štít

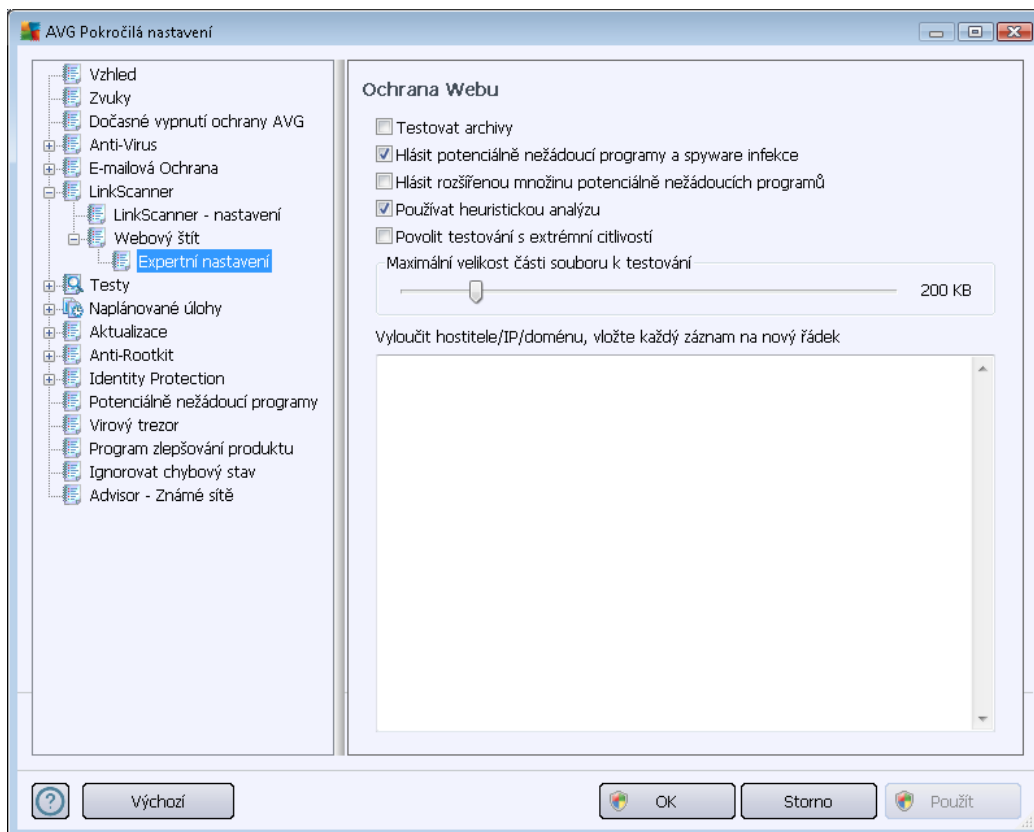


Dialog **Webový štít** nabízí tyto možnosti:

- **Povolit Webový štít** (ve výchozím nastavení zapnuto) - Označením položky aktivujete/deaktivujete službu **Webový štít**. Pokroilé nastavení této komponenty pak najdete v podkategorii [Ochrana webu](#).
- **Povolit AVG Akcelerátor** (ve výchozím nastavení zapnuto) - Označením položky aktivujete/deaktivujete službu **AVG Akcelerátor**, která umožňuje plynulé přehrávání videa v režimu online a urychluje stahování.

### Způsob upozornění na hrozby

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



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

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

dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.

- **Používat heuristickou analýzu** - (ve výchozím nastavení zapnuto) kontrola obsahu zobrazované www stránky pomocí metody [heuristické analýzy](#) (dynamická emulace instrukcí testovaného objektu v prostředí virtuálního počítače).
- **Povolit testování s extrémní citlivostí** - (ve výchozím nastavení vypnuto) ve specifických situacích (například při podezření na infekci starším typem viru) můžete zvolit tuto metodu testování, která aktivuje nejdokladnější testovací algoritmy a velmi podrobně prohledává naprosto všechny oblasti vašeho počítače. Mějte však na paměti, že tato metoda je asociována velmi náročná.
- **Maximální velikost částí souboru k testování** - pokud jsou na zobrazované stránce přítomny vložené soubory, lze kontrolovat také jejich obsah ještě dříve, než budou staženy na váš počítač. Kontrola velkých souborů je však asociována a může výrazně zpomalit načítání www stránky. Posuvníkem tedy můžete nastavit maximální velikost souboru, který si můžete pomocí komponenty **Webový štít** testovat. I v případě, že soubor určený ke stažení bude větší než je nastavená povolená velikost souboru, a bude tudíž stažen bez kontroly **Webovým štítem**, jste stále pod ochranou AVG: pokud by soubor byl infikován, bude okamžitě detekován **Rezidentním štítem**.
- **Vyloučit hostitele/IP/doménu** - do textového pole můžete zadat konkrétní adresu serveru (hostitele, IP adresu, IP adresu s maskou nebo URL) i domény, jež mají být z kontroly **Webovým štítem** vyloučeny. Uvádíte tedy výhradně adresy hostitelů, u nichž si můžete být obsahem www stránek naprosto jisti.

## 11.7. Testy

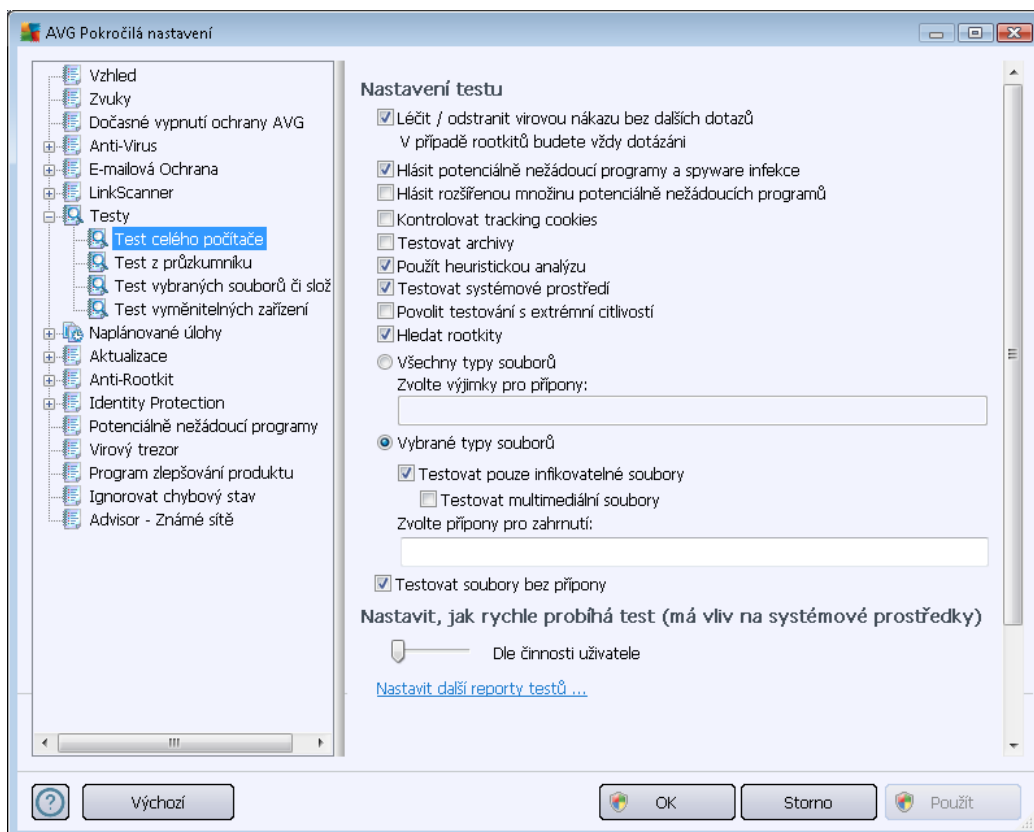
Pokročilé nastavení testů je rozděleno do čtyř kategorií, které odpovídají jednotlivým typům výrobcem definovaných testů :

- **[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 zařízeních](#)** - specifický test vyměnitelných zařízení připojených v danou chvíli k Vašemu PC



### 11.7.1. Test celého počítače

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



#### Nastavení testu

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

- **Léčit / odstranit virovou nákazu bez dalších dotazů** (ve výchozím nastavení zapnuto) - je-li během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. Pokud virus automaticky léčit nelze, bude infikovaný objekt automaticky přesunut do [Virového trezoru](#).
- **Hlásit potenciálně nežádoucí programy a spyware infekce** (ve výchozím nastavení zapnuto) - kontrola přítomnosti [potenciálně nežádoucích programů](#) (spustitelné programy, které mohou fungovat jako spyware nebo adware). Zaškrtnutím tohoto políčka aktivujete [Anti-Spyware](#), tj. bude se testovat přítomnost spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány v domě a se souhlasem uživatele. Doporučujeme 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 podstatku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.
- **Kontrolovat tracking cookies** (ve výchozím nastavení vypnuto) - parametr komponenty [Anti-Spyware](#) definuje, že během testu mají být detekovány cookies (*HTTP data zaslaná serverem prohlížeči a uložena na počítači uživatele; při každé další návštěvě téhož serveru prohlížeč posílá cookies zpět serveru, který podle nich rozlišuje jednotlivé uživatele*).
- **Testovat archivy** (ve výchozím nastavení vypnuto) - parametr definuje, že test má kontrolovat všechny soubory zabalené v některém typu archivu, například ZIP, RAR, ...
- **Použít heuristickou analýzu** (ve výchozím nastavení zapnuto) - během testu bude použita k detekci infekcí 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 (*při podezření na infekci ve vašem počítači*) můžete zvolit tuto metodu testování, která aktivuje nejkvalitnější testovací algoritmy a velmi podrobně provádí 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** - 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 či neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme, abyste se tohoto nastavení drželi, pokud nemáte skutečný důvod její

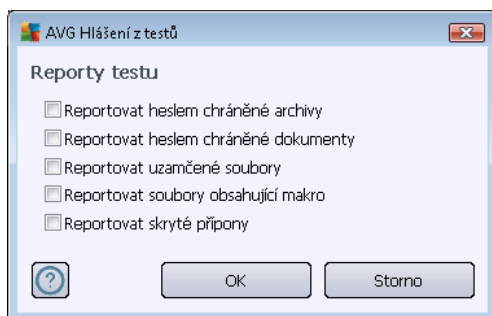
m nit. Soubory bez p ípon jsou obecn ýsoce podez elé a m ly by být otestovány.

### Nastavit, jak rychle probíhá test

V této sekci pak m žete nastavit požadovanou rychlost testování v závislosti na zát ži systémových zdroj . Ve výchozím nastavení je tato hodnota nastavena *dle innosti uživatele*, což odpovídá st ední úrovni využití systémových prost edk .. Pokud se rozhodnete pro spušt ní rychlého testu, prob hne test v kratším ase, ale po dobu jeho b hu bude výrazn zvýšena zát ž systémových zdroj , takže vaše práce na po íta i bude obtížn jší (*tato varianta je vhodná pro situaci, kdy je po íta spušt n, ale nikdo na n m aktuáln nepracuje*). Naopak, prodloužením doby testu snížíte zát ž systémových zdroj a vaše práce na po íta i nebude tém olivn na, test však bude probíhat po delší dobu.

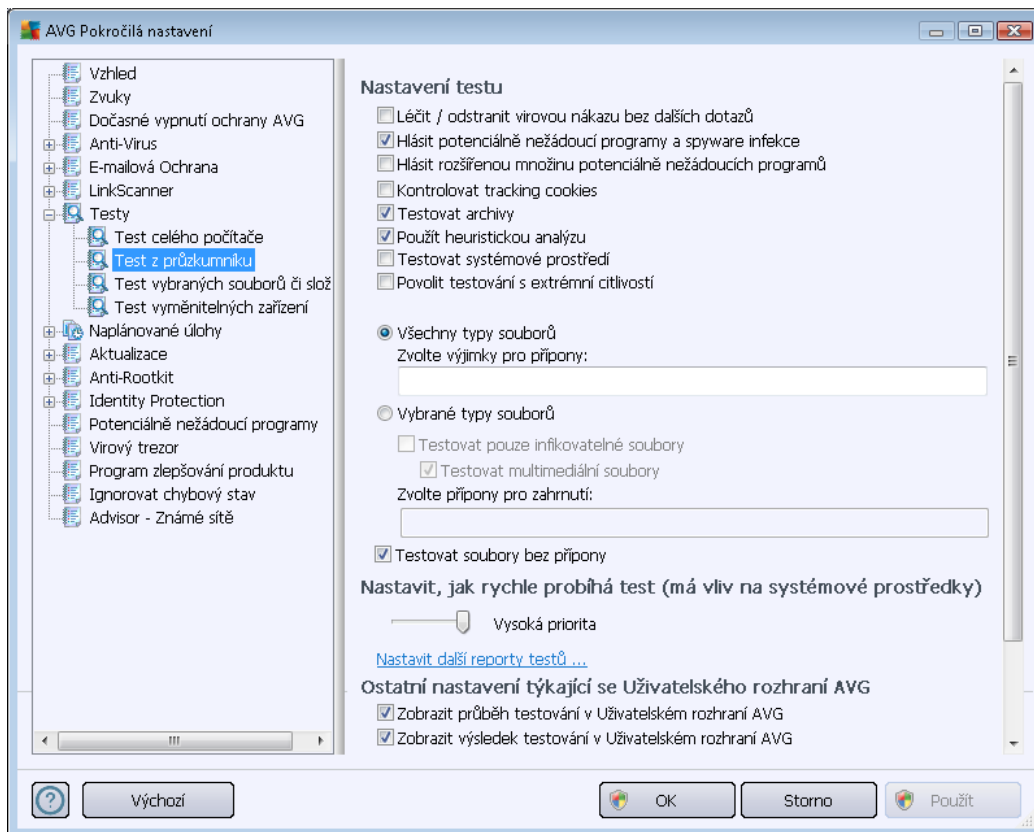
### Nastavit další reporty test ...

Kliknutím na odkaz **Nastavit další reporty test ...** otev ete samostatné dialogové okno **Reporty testu**, v n m žete ozna ením p íslušných položek ur it situace, jejichž výskyt b hem testu má být hlášen:



### 11.7.2. Test z průzkumníku

Podobn jako p edchozí položka [Test celého počíta e](#) nabízí i tato položka, **Test z průzkumníku**, možnost editovat parametry výrobcem nastaveného testu. Konfigurace se tentokrát vztahuje k [test m spušt ným nad konkrétními objekty počíta e z průzkumníku Windows](#) (*Test z průzkumníku*), viz kapitola [Testování v průzkumníku Windows](#):



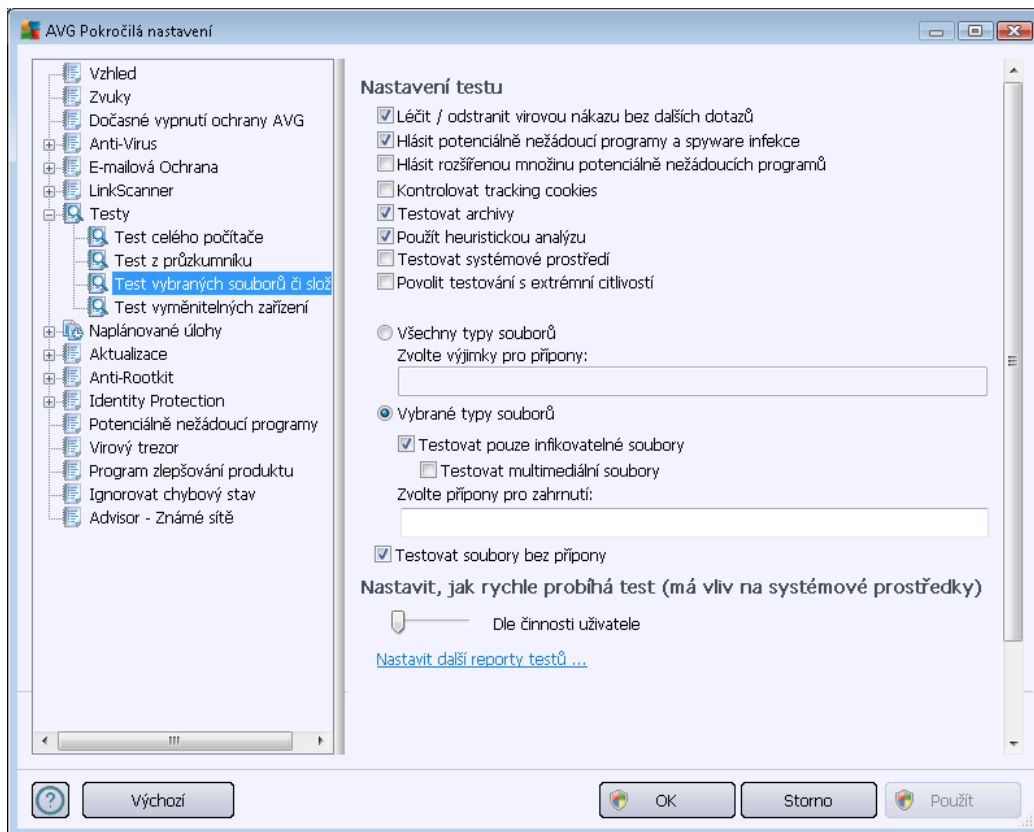
Veškeré možnosti editace parametrů testu jsou totožné s [editací parametrů Testu celého počítače](#). Odlišné je pouze výchozí nastavení těchto parametrů (například *Test celého počítače* ve výchozím nastavení neprovádí kontrolu archivů, ale provádí kontrolu systémových prostředků, zatímco u *Testu z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

### 11.7.3. 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 výchozími nastaveními, které je pro [Test celého počítače](#) nastaveno striktněji:

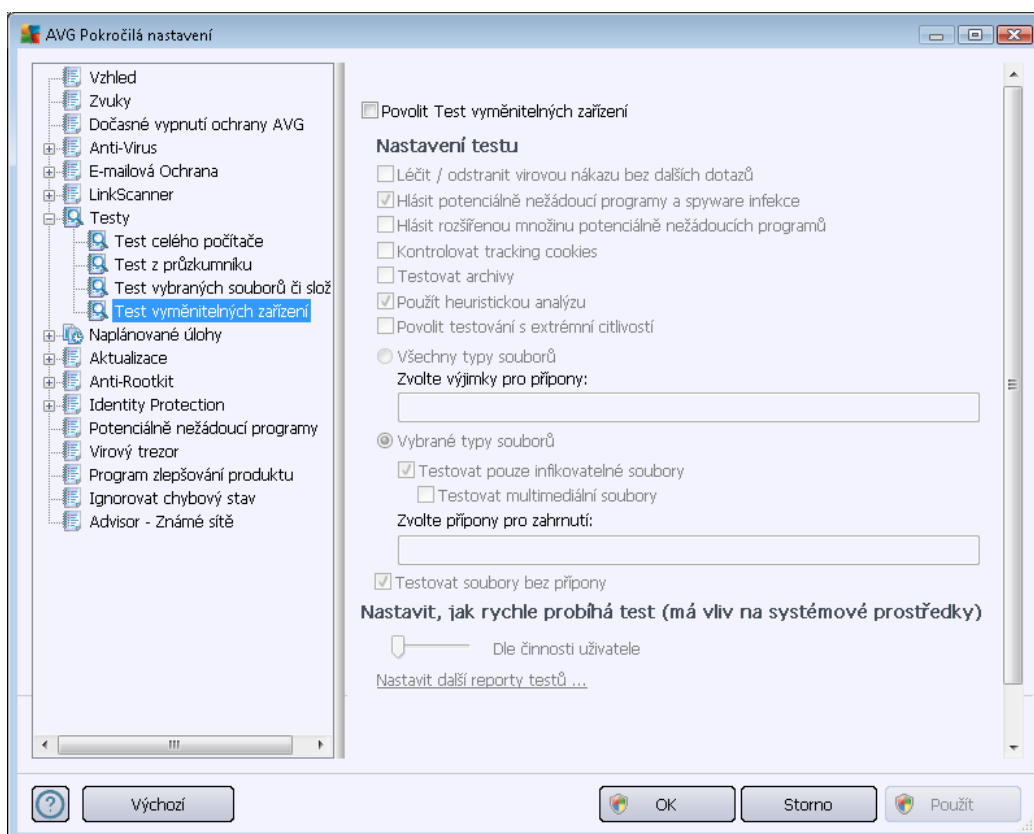


Veškeré parametry nastavené v tomto configuračním dialogu se vztahují pouze na ty oblasti vašeho počítače, které jste vybrali pro testování v rámci [Testu vybraných souborů či složek](#)!

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

### 11.7.4. 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](#).

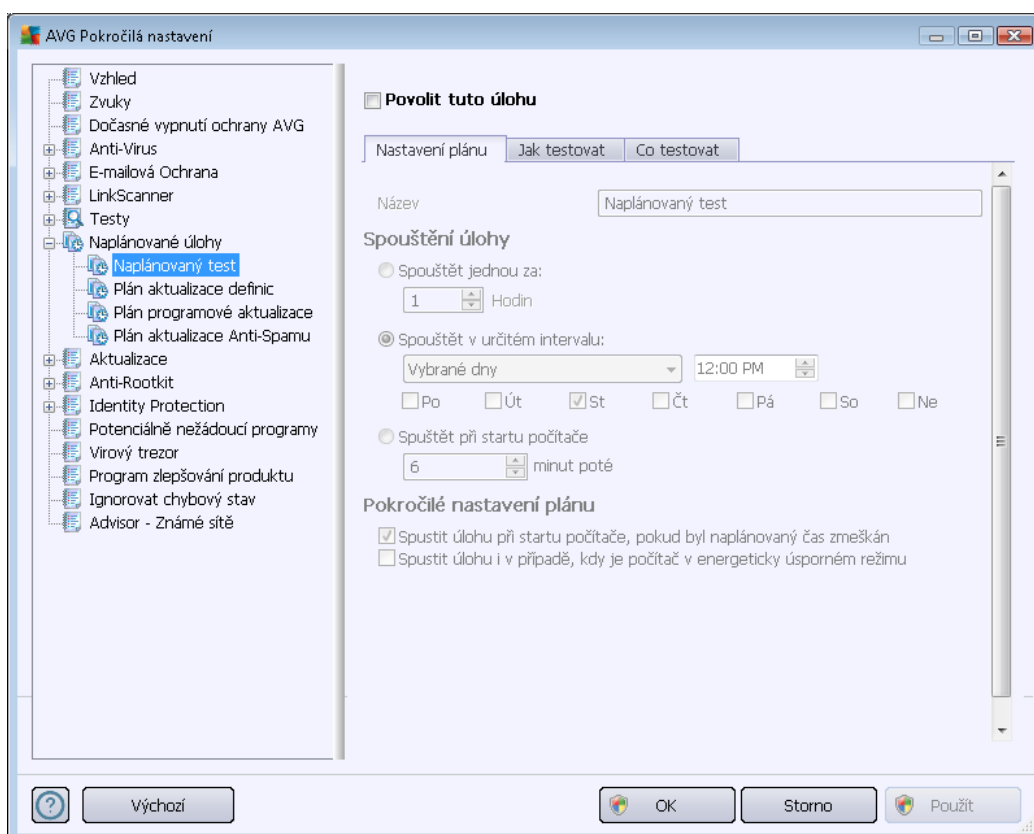
### 11.8. Naplánované úlohy

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

- [Naplánovaný test](#)
- [Plán aktualizace definic](#)
- [Plán programové aktualizace](#)
- [Plán aktualizace Anti-Spamu](#)

### 11.8.1. Naplánovaný test

Parametry naplánovaného testu můžete editovat (případně nastavit plán nový) na těchto záložkách. Na každé záložce máte nejprve možnost jednoduchým označením položky **Povolit tuto úlohu** naplánovaný test (dole) 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 testu. U nově vytvářených plánů (nový plán vytvoříte tak, že kliknete pravým tlačítkem myši nad položkou **Naplánovaný test** v levém navigačním menu) bude textové pole aktivní a dostanete možnost definovat své vlastní pojmenování plánu. Snažte se vždy používat stručné, popisné a případně názvy, abyste se později v naplánovaných úlohách snadno vyznali.

**Příklad:** Nevhodným názvem testu je například "Nový test" nebo "Martinův test", protože ani jeden název nevypovídá o tom, co test ve skutečnosti kontroluje. Naproti tomu správným popisným názvem testu může být například "Test systémových oblastí" nebo "Test disku C:" a podobně. Rovněž není nutné označovat testy termíny Test celého počítače versus Test vybraných souborů a složek - váš nastavený test bude vždy specifickým nastavením [testu vybraných souborů a složek](#).

V tomto dialogu můžete dále definovat tyto parametry testu:

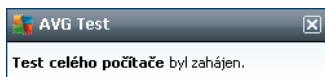
#### Spouštění úloh



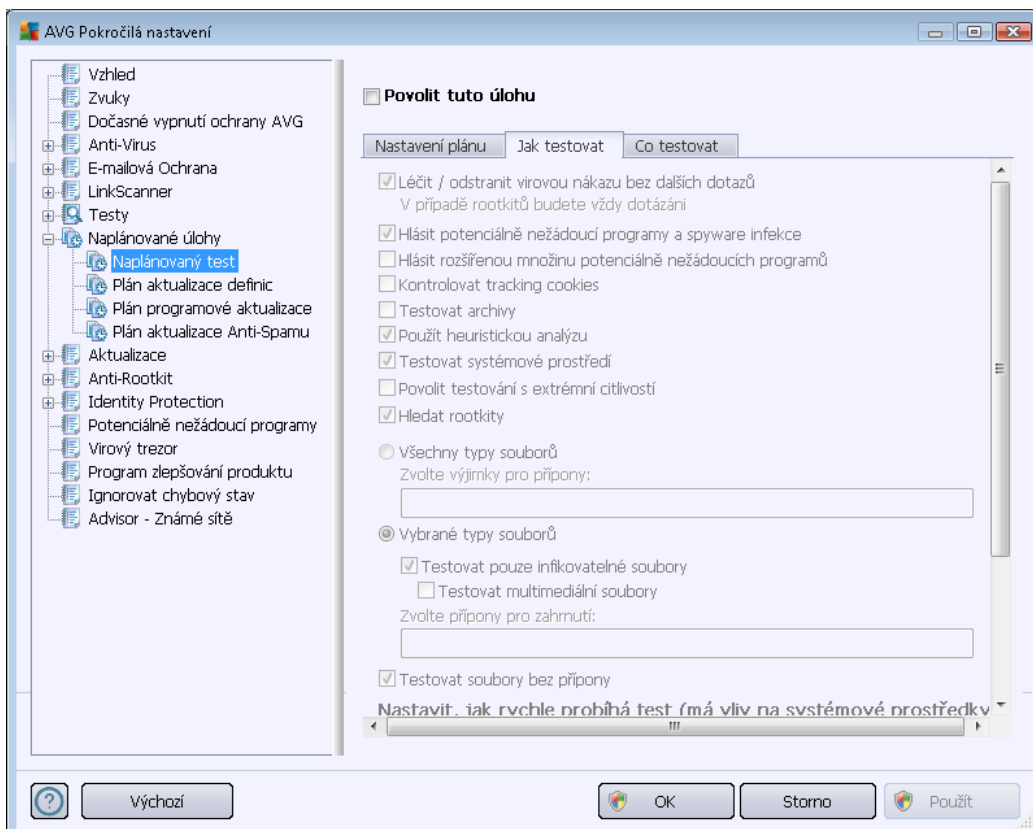
V této sekci dialogu určete, v jakých časových intervalech má být nově naplánovaný test spuštěn. Časové určení můžete zadat buďto opakovaným spuštěním testu po uplynutí určité doby (**Spouštět jednou za**) nebo stanovením přesného data a času (**Spouštět v určitém intervalu**), případně určit události,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

## Pokročilé nastavení plánu

Tato sekce umožňuje definovat podmínky, kdy má či nemá být test spuštěn, jestliže je počítač v úsporném režimu nebo zcela vypnutý a naplánovaný test spuštění testu byl zmeškán. O automatickém spuštění testu budete v určeném čase informováni prostřednictvím pop-up okna nad [ikonou AVG na systémové liště](#):



Po zahájení testu se na systémové liště objeví [nová ikona AVG](#) (barevná s problikávajícím světlem), která vás informuje o běžícím testu. Kliknutím pravého tlačítka myši nad touto ikonou otevřete kontextové menu, z něhož můžete buďtest pozastavit nebo ukončit, a rovněž změnit prioritu právě probíhajícího testu.







Záložka **Jak testovat** nabízí seznam parametrů testu, které můžete podle potřeby vypínat/zapínat. Ve výchozím nastavení je většina parametrů zapnuta a budou tak během testu automaticky použity. **Pokud nemáte skutečný důvod konfiguraci testu změnit, doporučíme 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 hrozeb, 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 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 archívy** (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 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. 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 nich kterých případech mohou být rootkity použity jako ovladače nebo části korektních aplikací.

Dále se můžete rozhodnout, zda si je chcete testovat

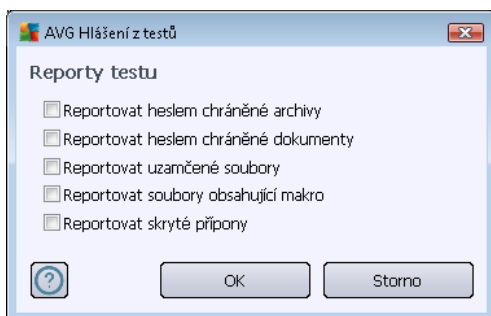
- **Všechny typy souborů** - pokud máte zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou (*po uložení se čárky změní na středníky*);
- **Vybrané typy souborů** - můžete se rozhodnout, že chcete, aby se testy spouštěly pouze nad soubory, které lze považovat za infikovatelné (*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 či neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme, abyste se tohoto nastavení drželi, pokud nemáte skutečnou důvod její 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 zatížení systémových zdrojů. Ve výchozím nastavení je tato hodnota nastavena *dle zátěže uživatele*. Pokud se rozhodnete pro spuštění rychlého testu, proběhne test v kratším čase, ale po dobu jeho běhu bude výrazně zvýšena zátěž systémových zdrojů, takže vaše práce na počítači bude obtížnější (*tato varianta je vhodná pro situaci, kdy je počítač spuštěn, ale nikdo na něm aktuálně nepracuje*). Naopak, prodloužením doby testu snížíte zátěž systémových zdrojů a vaše práce na počítači nebude téměř ovlivněna, test však bude probíhat po delší dobu.

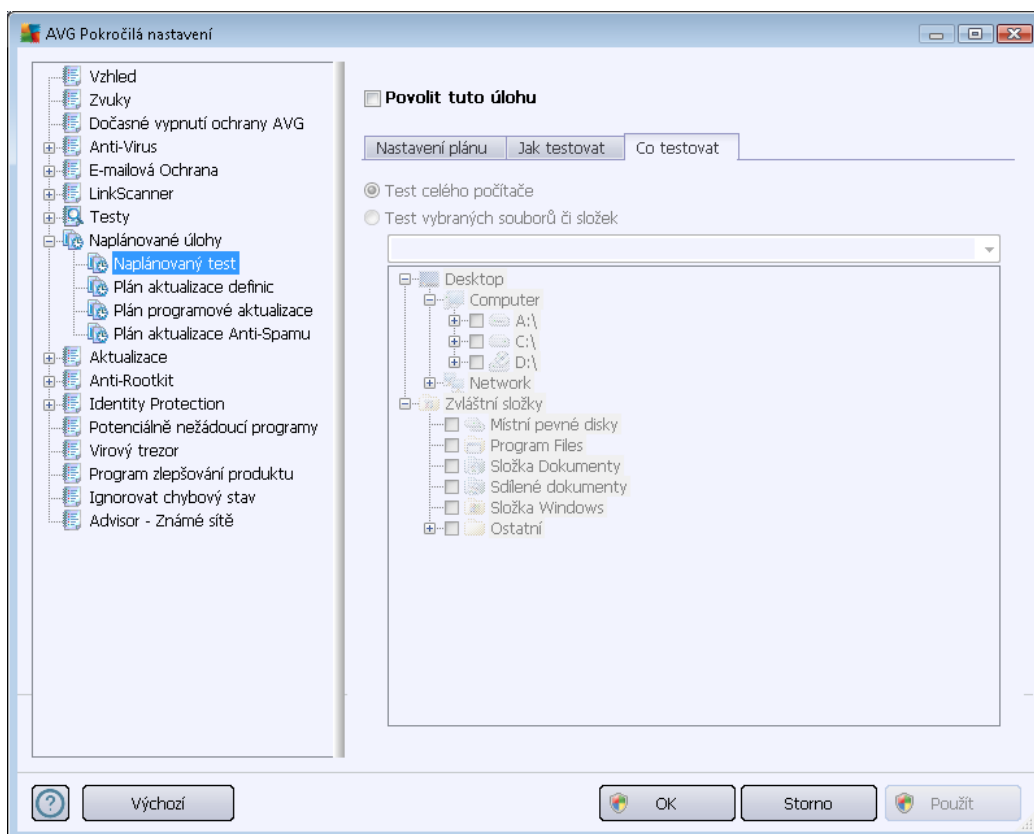
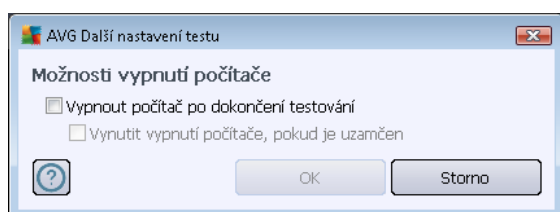
### Nastavit další reporty testu

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



## Další nastavení testu

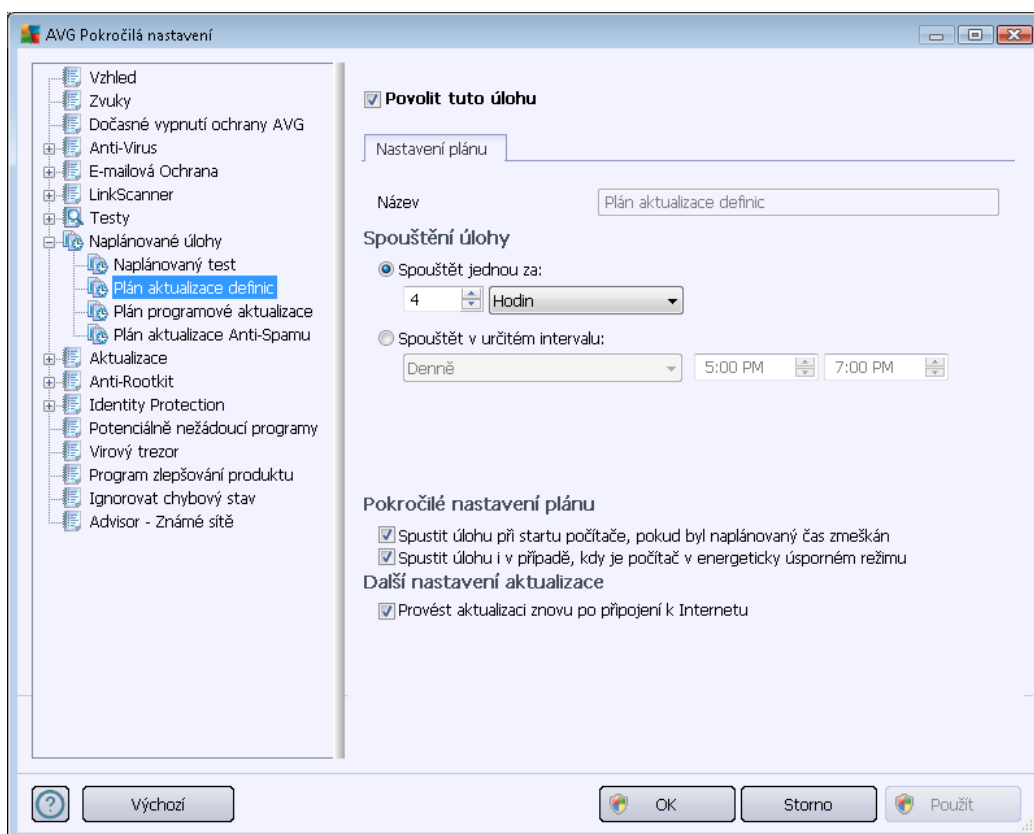
Kliknutím na odkaz **Další nastavení testu ...** otevřete nový dialog **Možnosti vypnutí počítače**, v něm můžete zvolit, zda má být po dokončení spuštění testu počítač automaticky vypnut. Pokud potvrdíte tuto volbu (**Vypnout po úspěšném dokončení testování**), aktivuje se současně další možnost, jejímž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



Na záložce **Co testovat** 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 části dialogu se aktivuje zobrazená stromová struktura vašeho disku a v ní můžete označit adresáře, jejichž obsah má být testován.

### 11.8.2. Plán aktualizace definic

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



V tomto dialogu můžete nastavit přesnější parametry plánu aktualizace. V textovém poli **Název** (toto pole je u všech předem nastavených plánů deaktivováno) je uvedeno jméno příslušného nastaveného plánu aktualizace.

#### Spouštění úloh

Určete, v jakých časových intervalech má být nově naplánovaná aktualizace definic provedena. Časové určení můžete zadat buďto opakovaným spuštěním aktualizace po uplynutí určité doby (**Spouštění jednou za**) nebo stanovením přesného data a času (**Spouštění v určitém intervalu**).

#### Pokročilé nastavení plánu

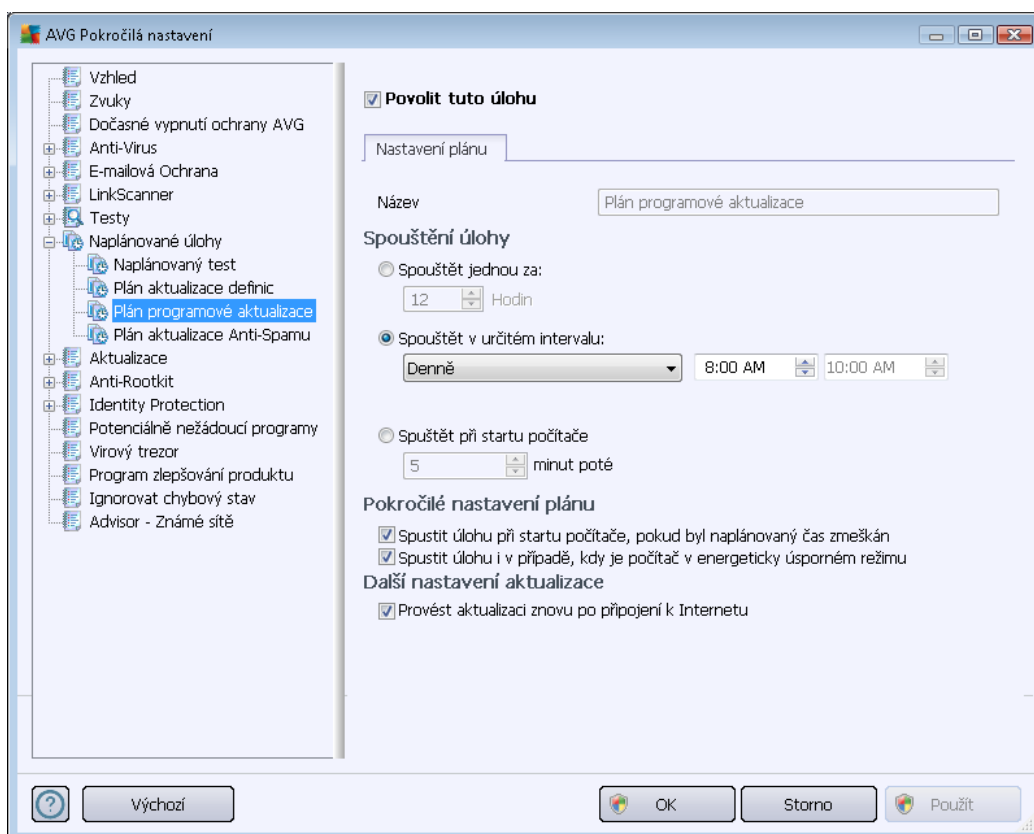
Tato sekce umožňuje definovat podmínky, kdy má či nemá být aktualizace definic spuštěna, jestliže je počítač v úsporném režimu nebo zcela vypnutý a naplánovaný čas spuštění aktualizace byl zmeškán.

## Další nastavení aktualizace

Volbou položky **Provést aktualizaci znovu po připojení k Internetu** zajistíte, že pokud dojde během aktualizace definic k problémům s připojením a aktualizace tedy nebude moci být dokončena, bude znovu spuštěna bezprostředně po obnovení připojení. O automatickém spuštění aktualizace budete v určeném 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](#)).

### 11.8.3. Plán programové aktualizace

V případě **skutečně nutného** potřeby můžete prostým vypnutím položky **Povolit tuto úlohu** naplánovanou programovou aktualizací (dočasné) deaktivovat, a později ji znovu zapnout:



V textovém poli **Název** (toto pole je u všech předešle nastavených plánů deaktivováno) je uvedeno jméno příslušného nastaveného plánu programové aktualizace.

## Spouštění úlohy

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 určením události, na niž se spustí aktualizace váže (**Spustit při spuštění počítače**).

### **Pokročilé nastavení plánu**

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

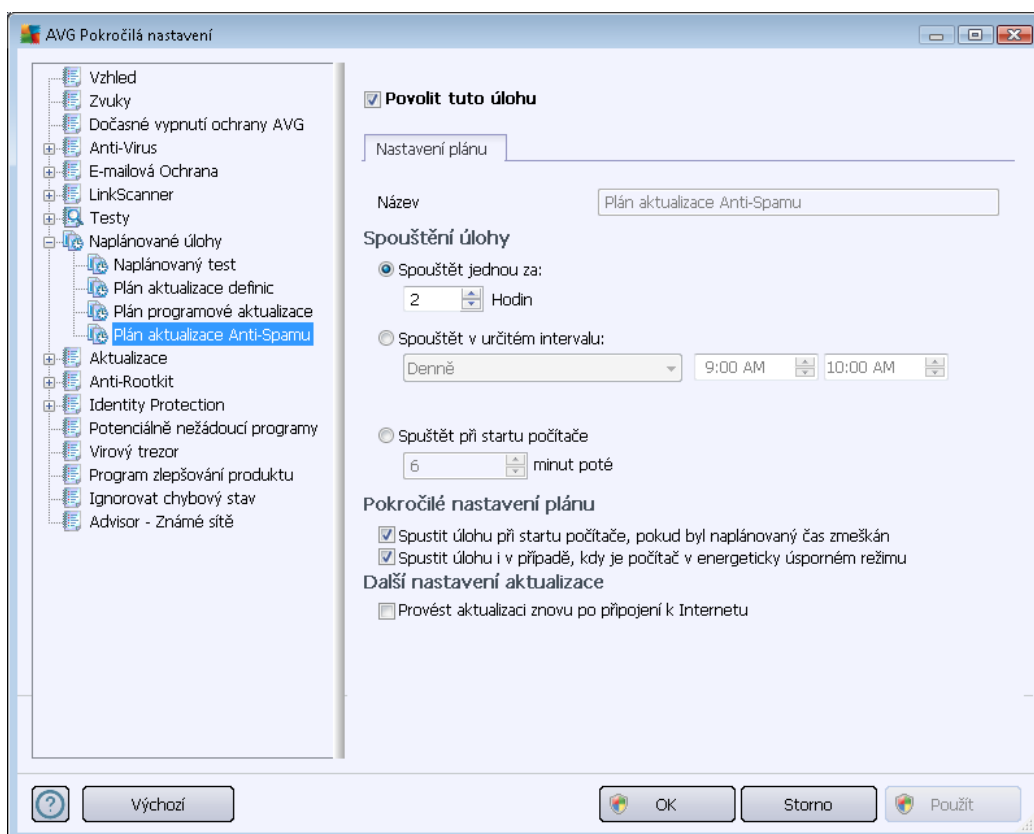
### **Další nastavení aktualizace**

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

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

#### 11.8.4. Plán aktualizace Anti-Spamu

V případě **skutečně nutné** můžete prostým vypnutím položky **Povolit tuto úlohu** deaktivovat přednastavený plán aktualizace komponenty [Anti-Spam](#), a později ji znovu aktivovat:



V tomto dialogu můžete nastavit přesnější parametry plánu aktualizace. V textovém poli **Název** (toto pole je u všech přednastavených plánů deaktivováno) je uvedeno jméno přednastavenému plánu aktualizace komponenty [Anti-Spam](#).

#### Spouštění úloh

Určete, v jakých časových intervalech má být nově naplánovaná aktualizace [Anti-Spamu](#) 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 určitím událostí, na niž se spuštění aktualizace [Anti-Spamu](#) váže (**Spouštět při spuštění počítače**).

#### Pokročilé nastavení plánu

Tato sekce umožňuje definovat podmínky, kdy má či nemá být aktualizace [Anti-Spamu](#) spuštěna,



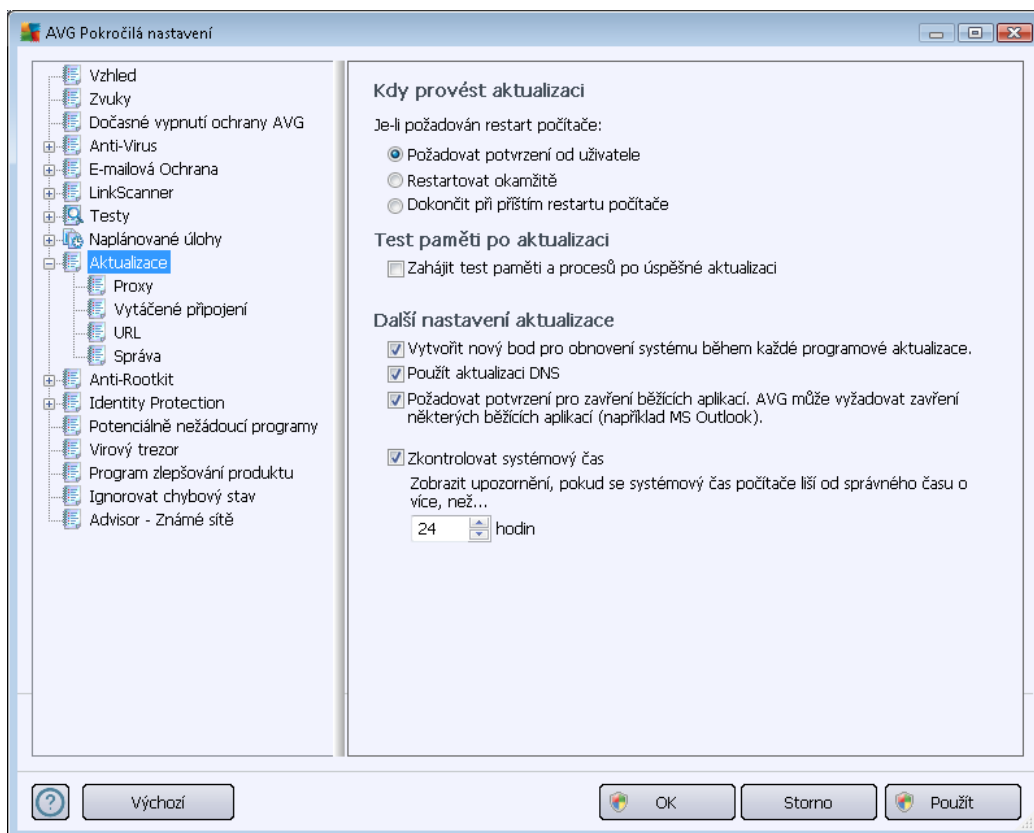
jestliže je poříta v úsporném režimu nebo zcela vypnutý a naplánovaný čas spuštění aktualizace byl zmeškán.

## Další nastavení aktualizace

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

## 11.9. 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

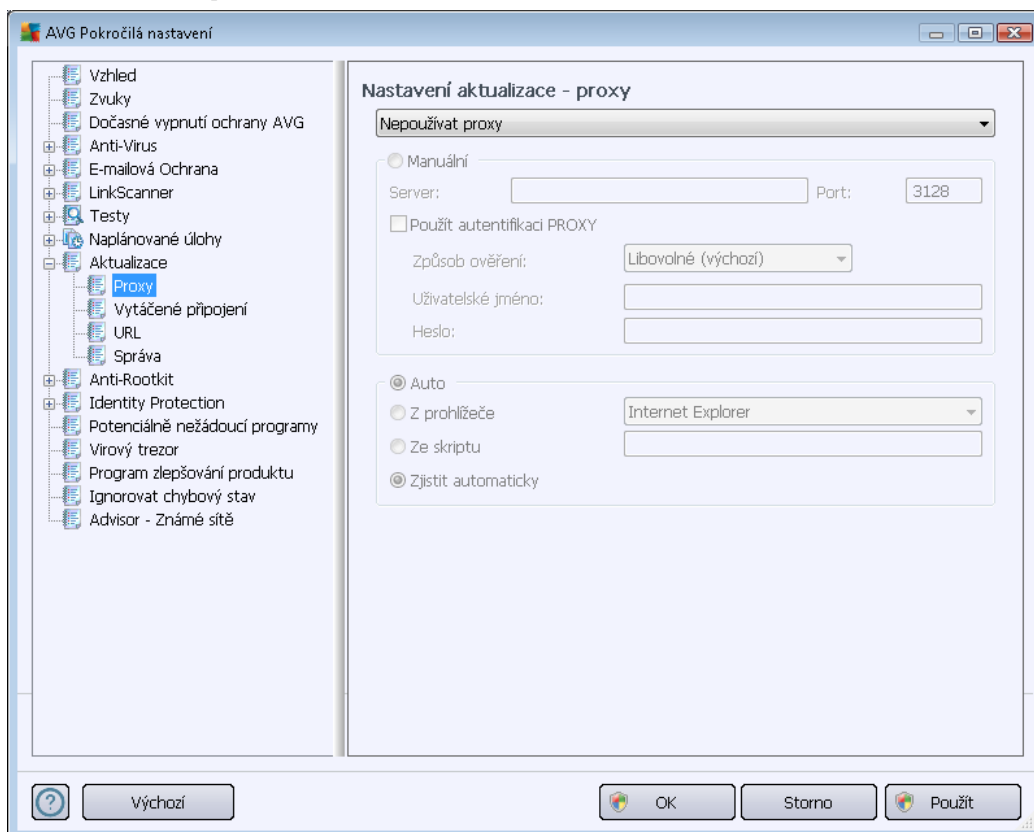
Označíte-li tuto položku, bude po každé úspěšné dokončené aktualizaci spuštěn test paměti. V případě, že by nejnovější aktualizace obsahovala nové virové definice, budou tak tyto okamžitě aplikovány během testu.

### Další nastavení aktualizace

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

- **Vytvořit nový bod pro obnovení systému ...** - před každým spuštěním programové aktualizace AVG je vytvořen takzvaný systémový bod pro obnovení systému. V případě, že aktualizací proces nebude z jakéhodůvodu 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 jakékoli 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 Internet Security 2012** vyhledá na DNS serveru informaci o aktuální verzi virové databáze a aktuální verzi programu a následně stáhne pouze nejmenší nezbytné aktualizací soubory. Tím se sníží celkový objem stahovaných dat a urychlí proces aktualizace.
- **Požadovat potvrzení pro zavěšení běžících aplikací** (*ve výchozím nastavení zapnutou*) 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 informováni o případném rozporu mezi časem nastaveným na počítači a skutečným časem, a to v okamžiku, kdy rozdíl těchto dvou časů dosáhne stanoveného počtu hodin.

### 11.9.1. Proxy



Proxy server je samostatný server nebo služba b žící na libovolném po íta i, která slouží k zajišt ní bezpečnosti p ípojení k internetu. Podle nastavení pravidel sít pak lze na Internet p istupovat bu to p ímo nebo p es proxy server; ob možnosti mohou být také povoleny sou asn . V první položce dialogu **Nastavení aktualizace - proxy** tedy volbou z rozbalovací nabídky combo boxu ur ete, zda si p ejete:

- **Použit proxy**
- **Nepoužívat proxy** - výchozí nastavení
- **Zkusit p ípojení p es proxy a v p ípad selhání se p ípojit p ímo**

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

#### Manuální nastavení

Při manuálním nastavení (volba **Manuální** aktivuje p íslušnou 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 síť* )

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.

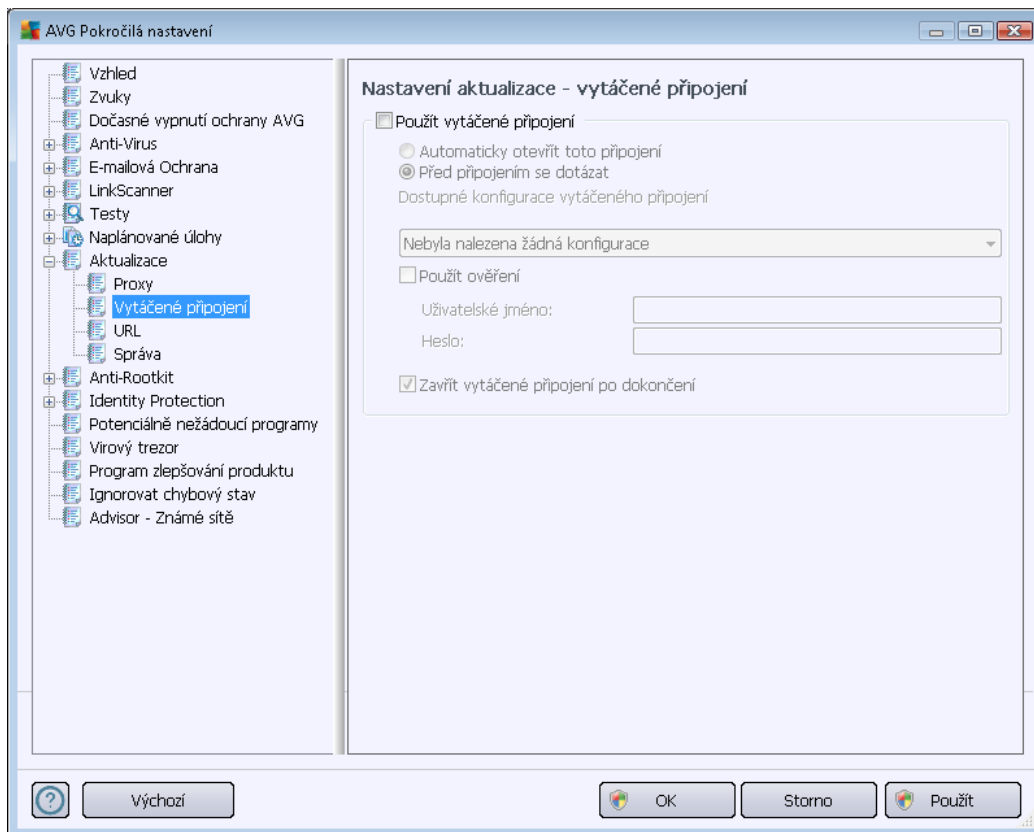
### Automatické nastavení

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 z 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

### 11.9.2. Vytáčené připojení

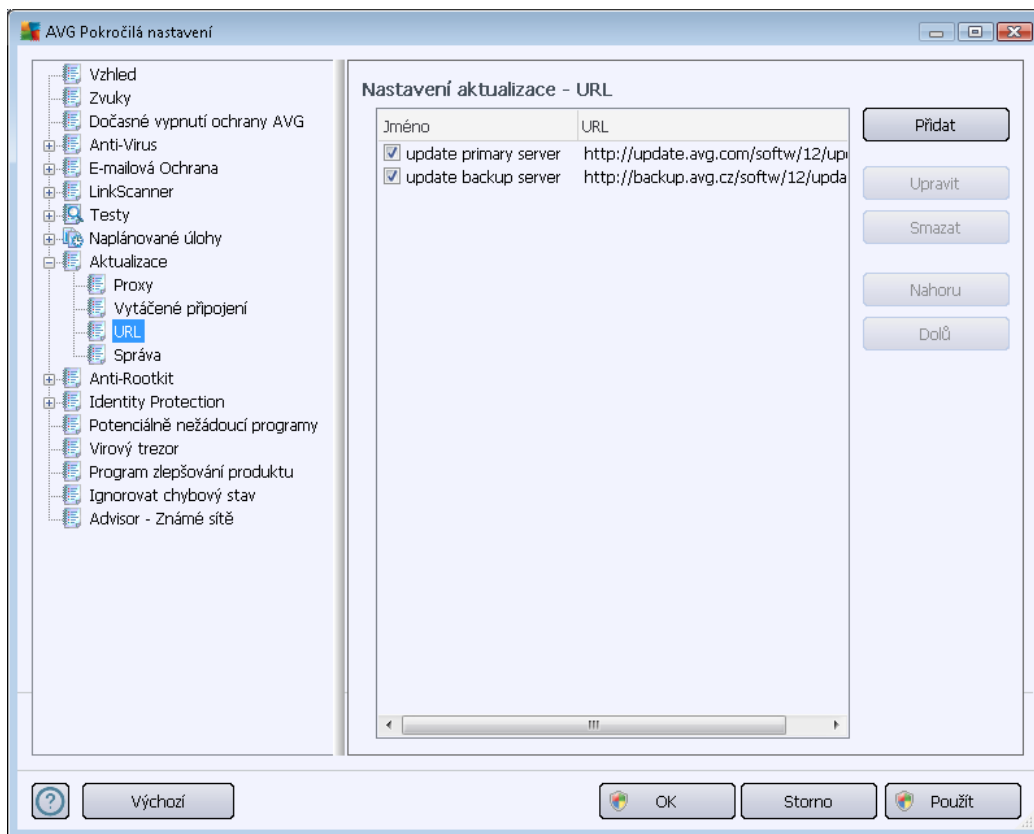
Parametry nastavované v dialogu **Nastavení aktualizace - vytáčené připojení** se vztahují k telefonickému připojení. Jednotlivá pole záložky jsou neaktivní, pokud neoznačíte položku **Použít vytáčené připojení**. Touto volbou se pak aktivují ostatní pole.



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***).

### 11.9.3. URL

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



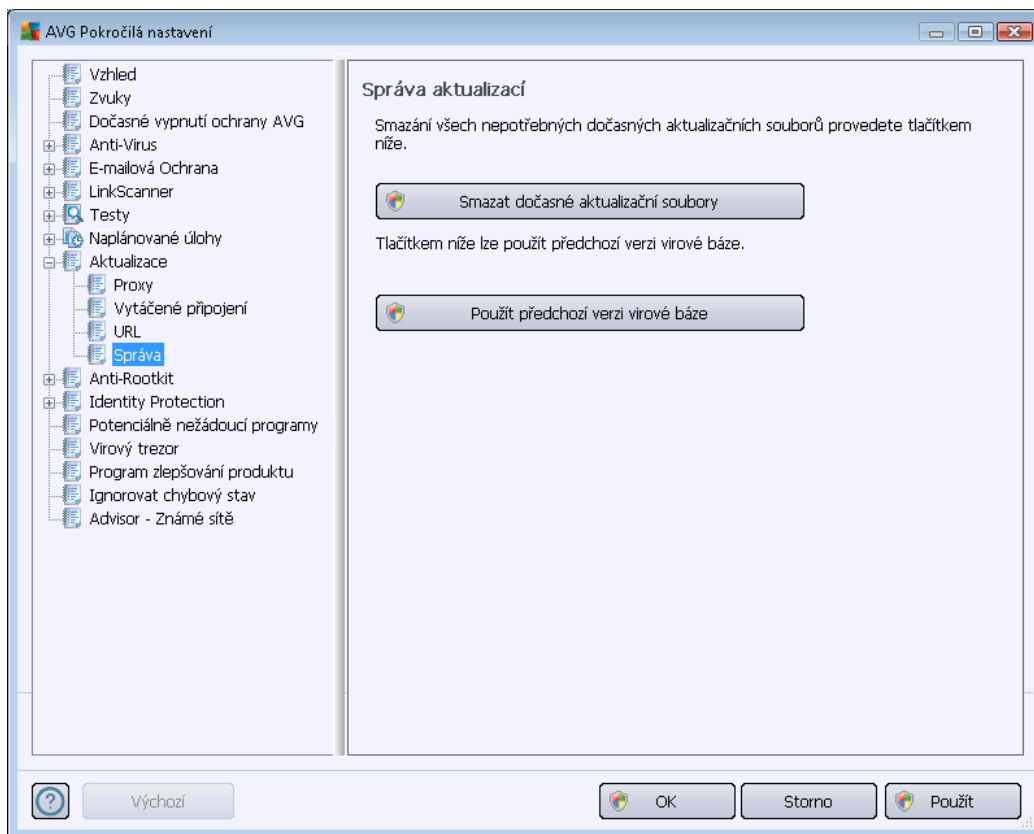
#### Ovládací tlačítka dialogu

Seznam a jeho jednotlivé položky lze editovat pomocí následujících ovládacích tlačítek:

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

### 11.9.4. Správa

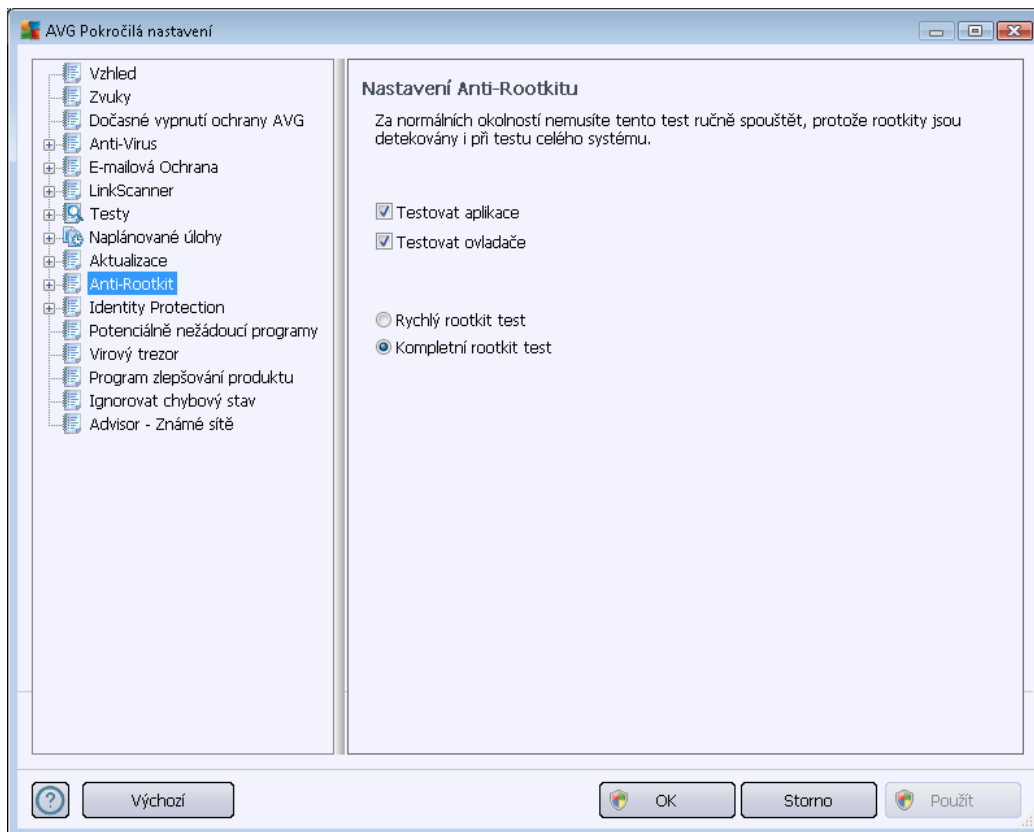
Dialog **Správa aktualizací** obsahuje dvě možnosti volby dostupné prostřednictvím dvou tlačítek:



- **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)

### 11.10. 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](#):



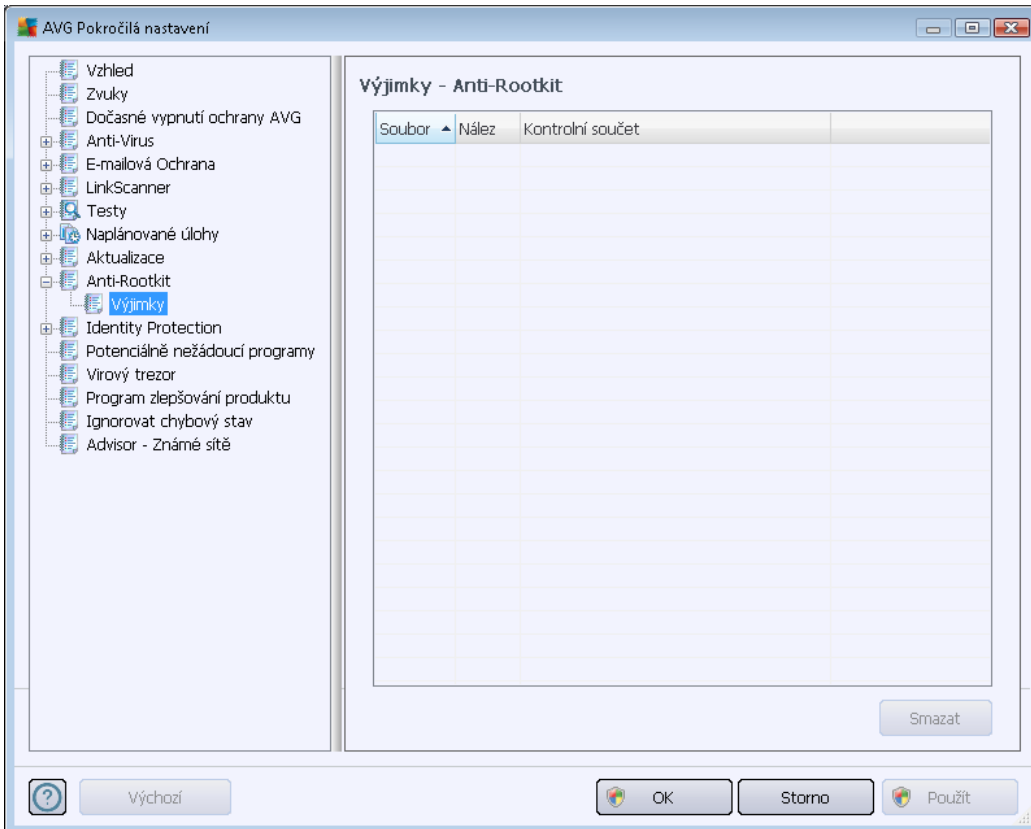
Editace všech funkcí komponenty [Anti-Rootkit](#) uvedená v tomto dialogu je dostupná i přímo z [rozhraní komponenty Anti-Rootkit](#).

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)

### 11.10.1. Výjimky

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



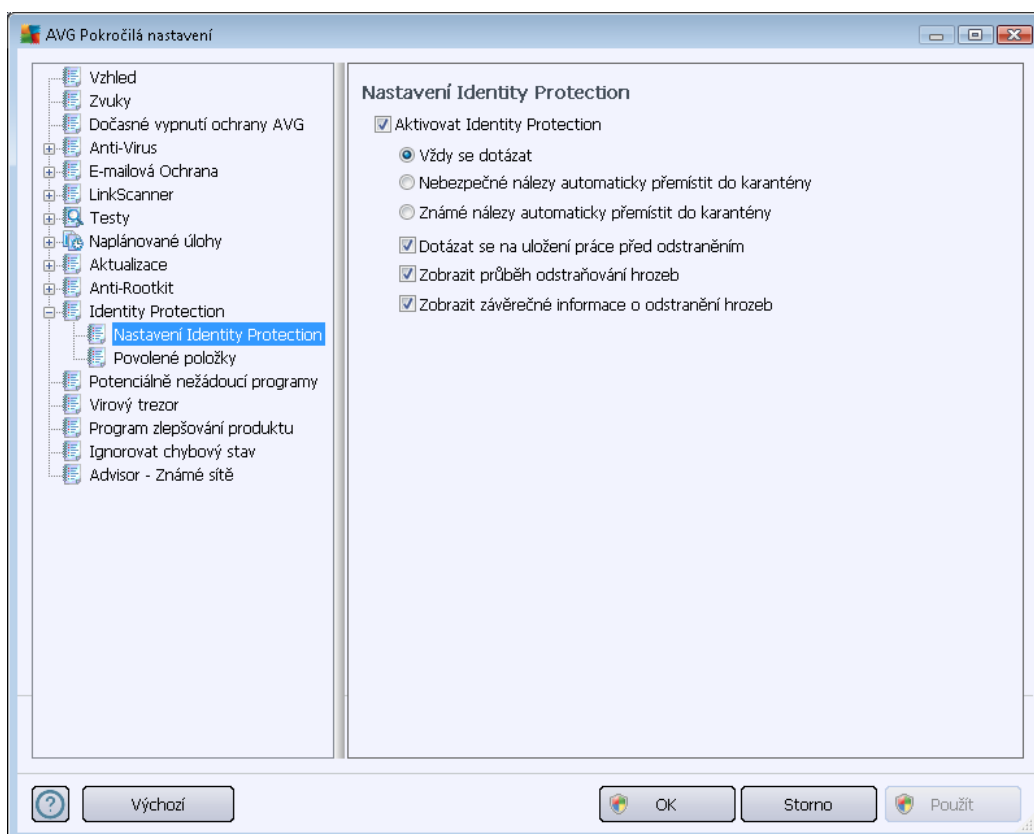
### 11.11. Identity Protection

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



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



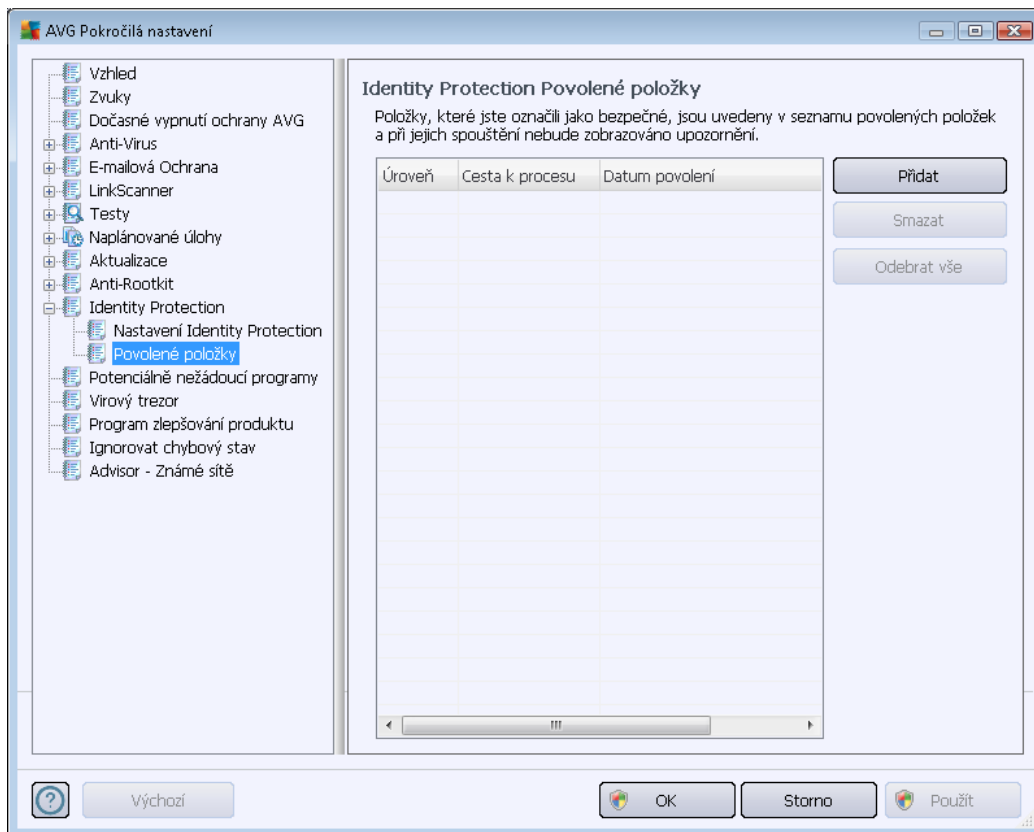
- **Známé nálezy automaticky p emístít do karantény** - ozna te tuto položku, pokud si p ejete, aby veškeré aplikace detekované jako možný malware byly automaticky a okamžit p esunuty do [Virového trezoru](#).

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.

### 11.11.2. Povolené položky

Pokud jste v dialogu [Nastavení Identity Protection](#) ponechali položku **Nebezpe né nálezy automaticky p emístít do karantény** nezna 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:



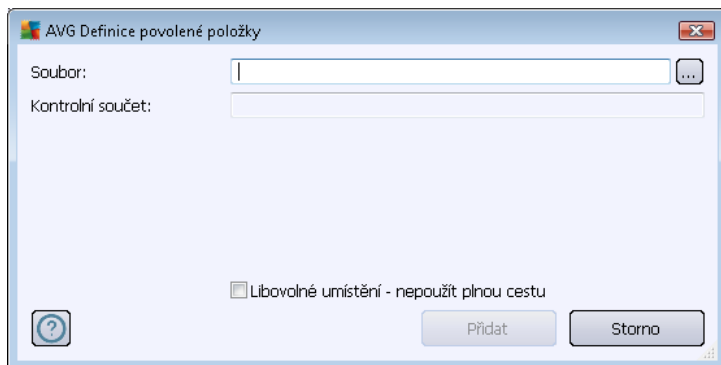
V seznamu **Povolené položky** najdete následující informace o každé aplikaci:

- **Úroveň** - grafické zobrazení závažnosti běžícího procesu na čtyřech stupních od nejnižšího až po kritický (■□□□) až (■□■□)
- **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:

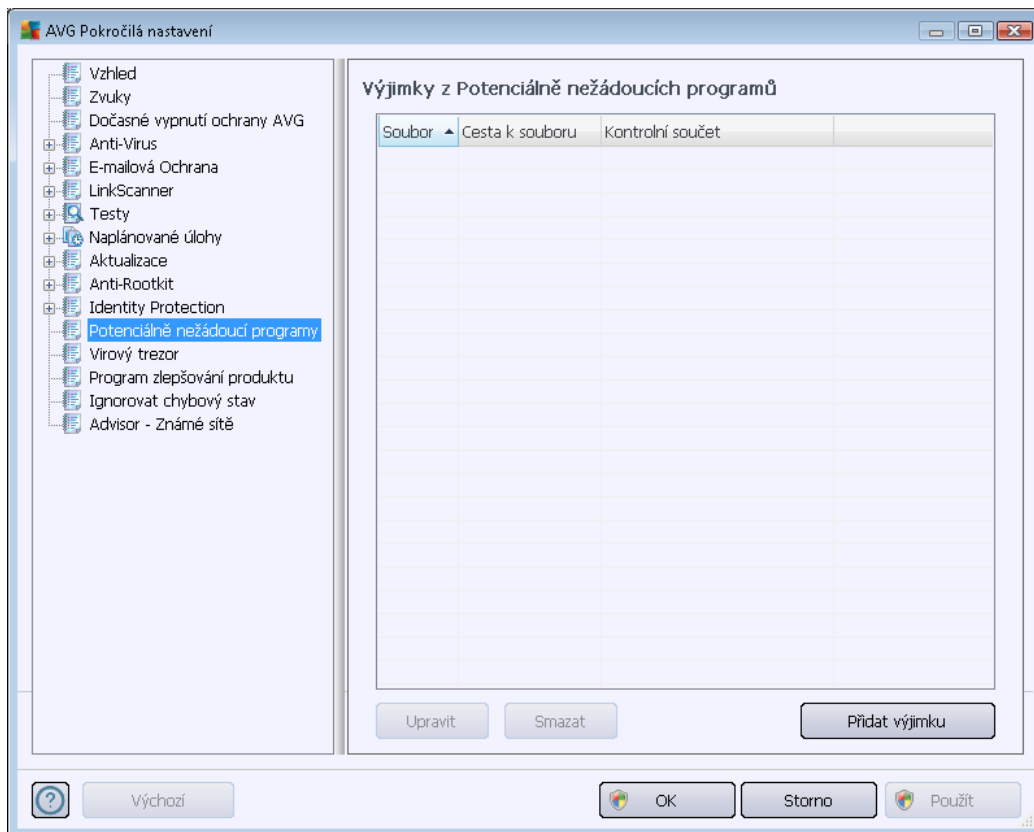
- **Přidat** - otevře editační dialog, v němž můžete nastavit parametry nově přidávané aplikace:



- **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 kdekoliv (*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

## 11.12. Potenciálně nežádoucí programy

**AVG Internet Security 2012** má schopnost analyzovat spustitelné programy, případně DLL knihovny, a určit, které z nich by mohly být nežádoucí (*např. spyware*). Může se však stát, že některé z programů detekovaných jako nežádoucí, jsou na vašem počítači nainstalovány s vaším vědomím a 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 Internet Security 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.

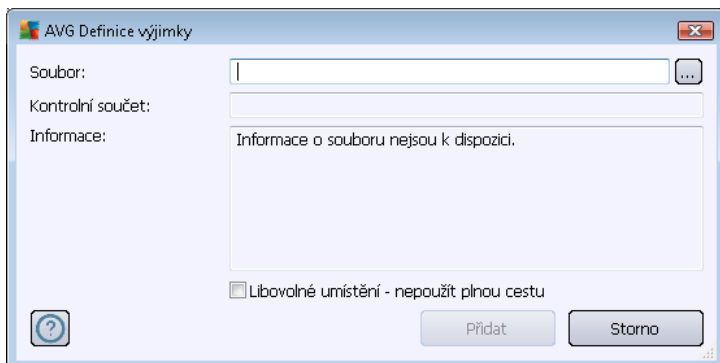


Dialog **Výjimky z Potenciálně nežádoucích programů** zobrazuje seznam již definovaných a aktuálně platných výjimek z potenciálně nežádoucích programů. Výjimku můžete editovat, smazat nebo nově přidat. Ke každé jednotlivé výjimce najdete v přehledu následující informace:

- **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.

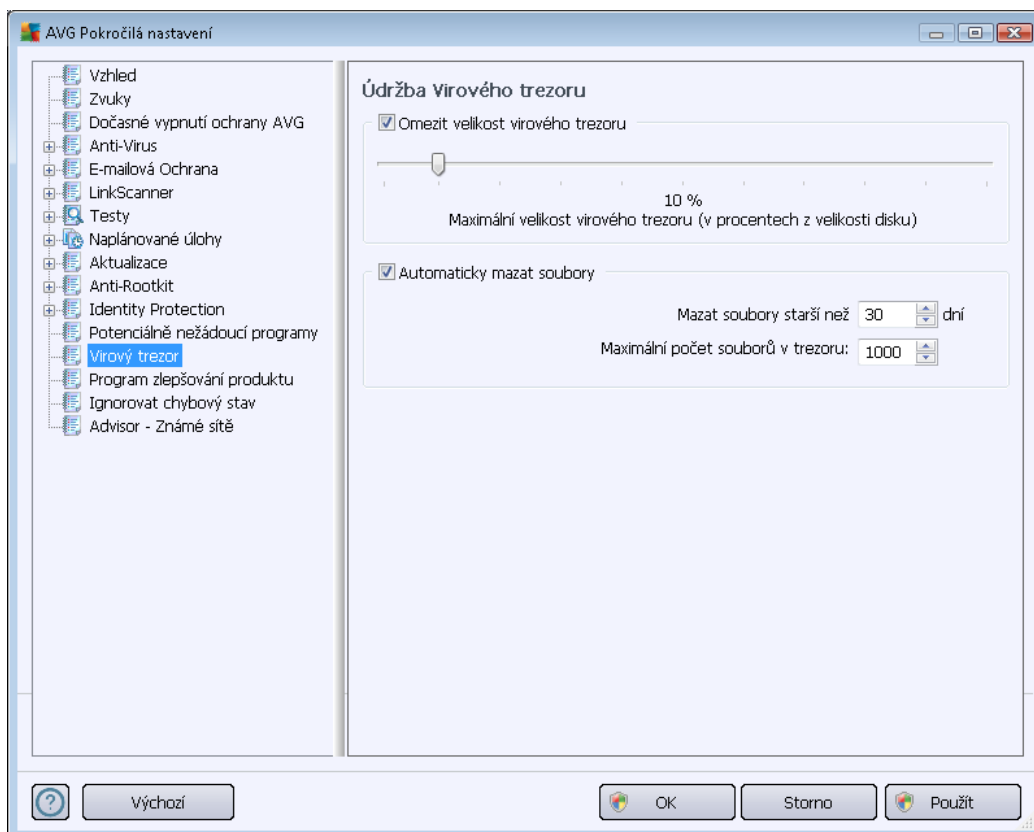
### Ovládací tlačítka dialogu

- **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*).

### 11.13. 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**).

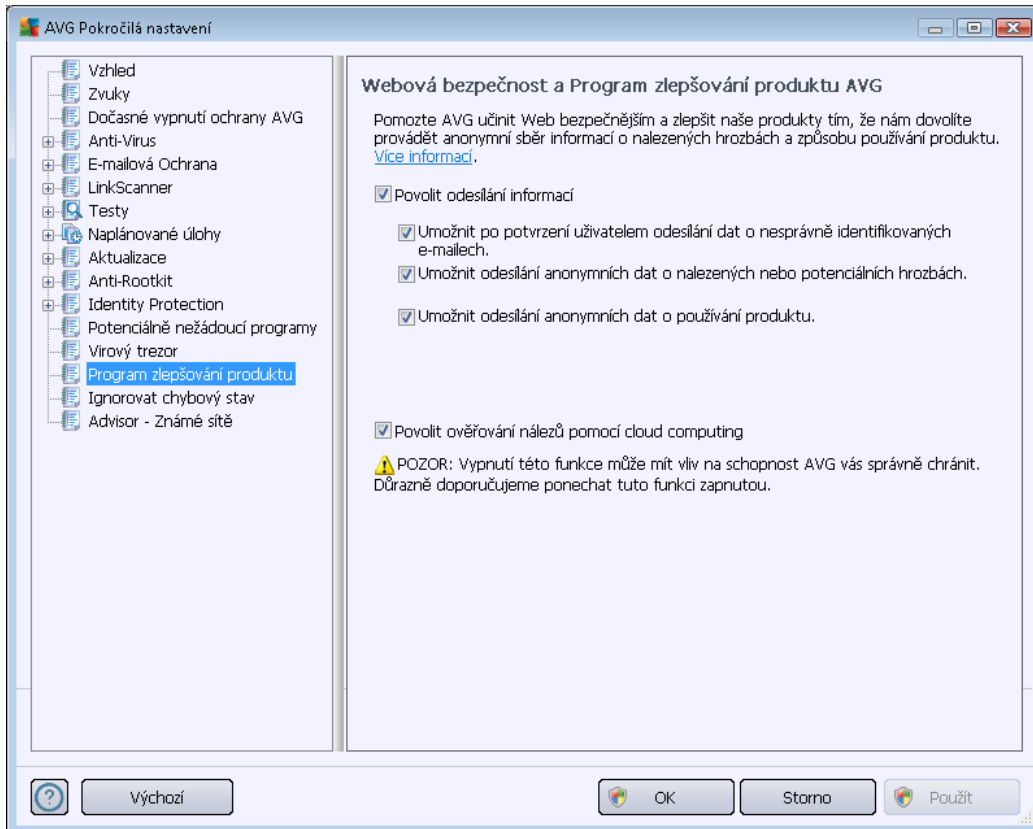
### 11.14. Program zlepšování produktu

V dialogu **Webová bezpečnost a Program zlepšování produktu AVG** máte možnost zapojit se do spolupráce a podílet se na zlepšování produktu AVG a na celkovém zvýšení úrovně bezpečnosti na Internetu. Ponecháte-li položku **Povolit odesílání informací** zapnutou, umožníte tak reportování informací o detekovaných hrozbách týmu expertů společnosti AVG Technologies. Tyto reporty nám pomáhají shromážďovat 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 aktivovány. Výrazně nám tím pomůžete s vylepšováním ochrany vašeho počítače.



V dialogu najdete tyto možnosti nastavení:

- **Povolit odeslání informací** (ve výchozím nastavení zapnuto) - Chcete-li nám pomoci dále zlepšovat program AVG, ponechejte toto políčko označené. Tím povolíte odeslání informací o všech hrozbách, na které eventuelně narazíte při surfování po Internetu; tato funkce nám pomáhá shromažďovat nejnovější data od uživatelů po celém světě a neustále tak vylepšovat jejich ochranu. Reportování probíhá automaticky, takže vám nezpůsobí žádné nepohodlí, a nezahrnuje žádná osobní data.
  - **Umožnit po potvrzení uživatelem odeslání dat o nesprávně identifikovaných e-mailech** (ve výchozím nastavení zapnuto) – zaslání informací o e-mailových zprávách, které byly komponentou **Anti-Spam** mylně označeny za spam, nebo naopak nebyly označeny, i když o spam skutečně šlo. V případě zaslání těchto informací budete napřed požádáni o svolení.
  - **Umožnit odeslání anonymních dat o nalezených nebo potenciálních hrozbách** (ve výchozím nastavení zapnuto) – zaslání informací o jakémkoli podezřelém nebo skutečně nebezpečném kódu či vzorci chování (*může jít o virus, spyware, případně nebezpečnou webovou stránku, na kterou jste se pokusili přejít*) nalezeném ve vašem počítači.





- **Umožnit odesílání anonymních dat o používání produktu** (ve výchozím nastavení zapnuto) – zasílání základních statistických dat o používání systému AVG jako například o nalezených infekcích, probíhajících testech, úspěšných/neúspěšných aktualizacích atp.
- **Povolit ověření nálezů pomocí cloud computing** (ve výchozím nastavení zapnuto) – nalezené infekce, hrozby a podezřelé kódy budou ověřeny, zda nejde o falešné detekce (tj. ve skutečnosti neškodné).

## Největší hrozby

V dnešní době už de facto nemluvíme o antivirové ochraně, ale obecně o webové bezpečnosti. Na Internetu se vyskytuje obrovské množství různých hrozeb, jejichž rozsah daleko přesahuje kategorii virů. Auto i nebezpečných kódů a webových stránek jsou stále vynalézavější, a tak se denně objevují nejen nové viry, ale i zcela nové typy hrozeb, triků a technik, jak uživatele podvést a využít. Uvědomte si ty největší, 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, mazají je a vymazávají z disku, jiné dělají v cíli na první pohled celkem neškodné, například přehrávají nějakou hudbu. Nebezpečné jsou však všechny viry, a to kvůli základní vlastnosti nekontrolovatelného množení – i jednoduchý virus se dokáže během chvilky namnožit tak, že zabere veškerou paměť a způsobí pád systému.
- **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, například elektronickou poštou, a tak způsobuje přetížení sítě a e-mailových serverů.
- **Spyware** je obvykle definován jako typ malware (*malware = anglická zkratka pro "malicious software", tj. škodlivé programy obecně*) a v tšinou zahrnuje především programy – například tzv. *trojské koně* určené k odcizení osobních informací, hesel, čísel kreditních karet a podobně, například proniknutí do počítače a za účelem poskytnutí přístupů cizím osobám; samozřejmě to vše bez vědomí vlastníka počítače.
- **Potenciálně nežádoucí programy** (z *anglického Potentially Unwanted Programs = PUP*) jsou typem spyware, který představuje potenciální riziko pro váš počítač. Příkladem PUP může být adware, to je program určený k distribuci reklamy. Ten se v tšinou projevuje tak, že zobrazuje v internetovém prohlížeči vyskakovací okna s reklamou, což je sice otravné, ale ne skutečně ohrožující.
- **Sledovací cookies** lze rovněž považovat za druh spyware, jelikož tyto malé soubory, uložené ve vašem internetovém prohlížeči a posílané nazpět "mateřské" webové stránky, kdykoli se na ni znovu připojíte, mohou obsahovat různé osobní informace, například seznam stránek, na které jste se v poslední době dívali, a podobně.
- **Exploit** je škodlivý kód, který využívá chyby nebo bezpečnostní skuliny v operačním systému, internetovém prohlížeči nebo jiném často používaném programu.
- **Phishing** je pokus, jak získat citlivá data vydáváním se za důvěryhodnou instituci. Potenciální oběti jsou obvykle kontaktovány hromadným e-mailem obsahujícím výzvu k

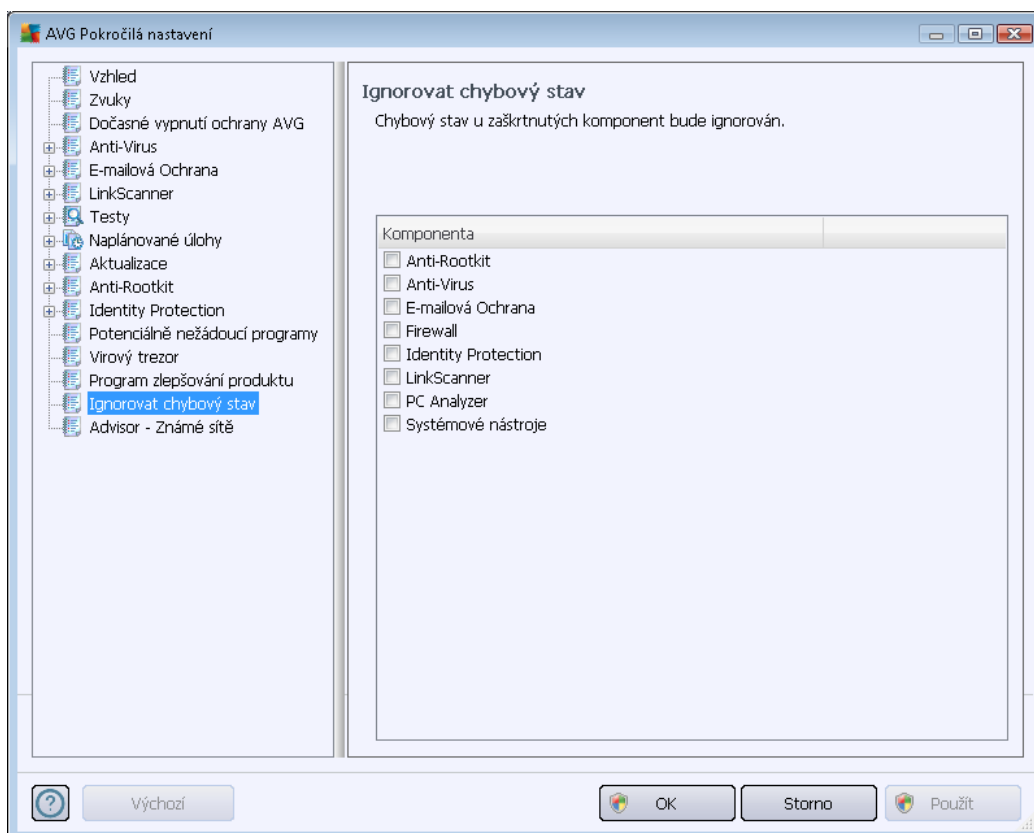
aktualizaci bankovních údaj (jinak bude konto uzavřeno...) a následuje odkaz na webovou stránku příslušné banky, která mnohdy vypadá velmi v reálném světě, ale je samozřejmě falešná.

- **Hoaxy** jsou četné zlověstné podvodné nebo poplašné e-maily obsahující například falešné nabídky práce, například nabídky, které pracovníky zneužijí k nelegálním aktivitám, výzvy k vybrání velké sumy peněz, podvodné loterie a podobně.
- **Nebezpečné webové stránky** dokáží nepozorovaně instalovat škodlivé programy do vašeho počítače, a stránky napadené hackery dělají totéž, jen se jedná o stránky příslušné a neškodné, které se však po útoku hackerů chovají zcela nepředvídatelně.

**AVG Internet Security 2012 obsahuje ochranu proti všem zmíněným typům hrozeb a škodlivých programů! Stručný přehled funkcionality jednotlivých komponent najdete v kapitole [Přehled komponent](#).**

### 11.15. Ignorovat chybový stav

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



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



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

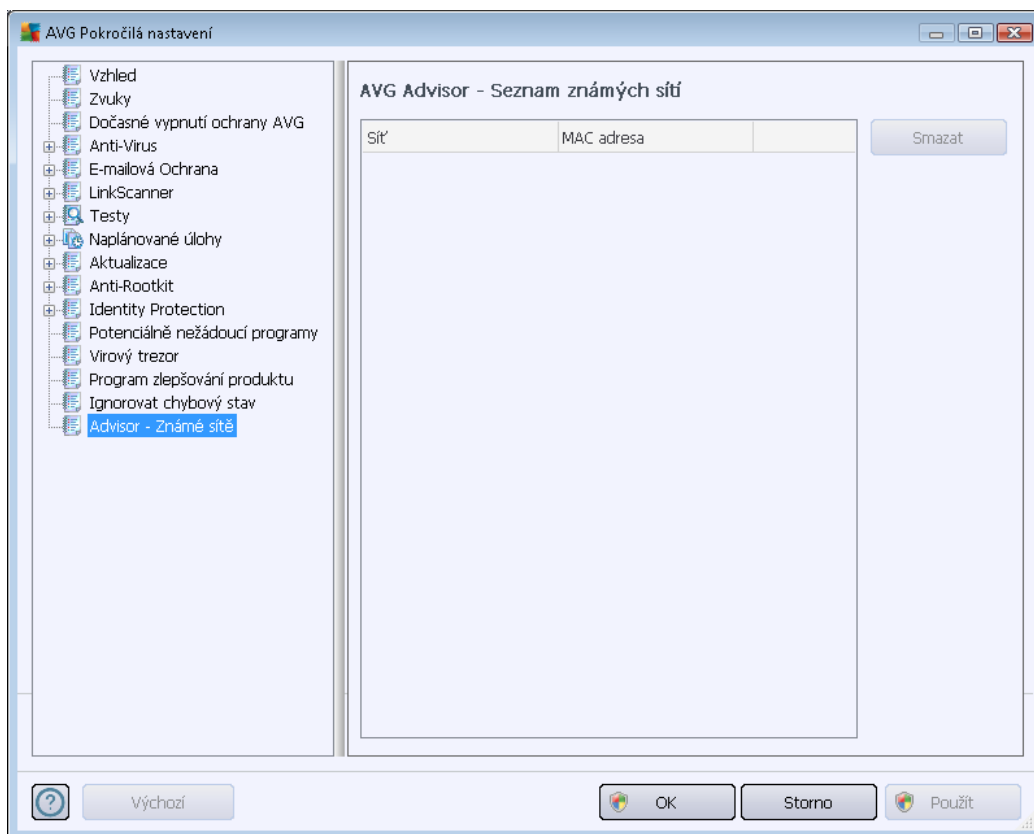
Můžete se ale stát, že si z nějakého důvodu budete chtít deaktivovat určitou komponentu (samozřejmě doporučujeme ponechat všechny komponenty trvale zapnuté a ve výchozím nastavení, ale tato možnost existuje). Pak by ikona na systémové liště automaticky oznamovala chybový stav, který ale de facto není chybovým stavem, jelikož jste jej sami navodili a jste si v domě 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 tyto komponenty, jejichž případný chybový stav (to znamená i jejich vypnutí) nemá být hlášen. Stejná možnost (Ignorovat stav komponenty) je dostupná pro jednotlivé komponenty také přímo z [přehledu komponent v hlavním okně AVG](#).

### 11.16. 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 prověřili. Pokud usoudíte, že síť je bezpečná, můžete ji uložit do tohoto seznamu (prostřednictvím odkazu v informačním dialogu AVG Advisoru, který se vysune nad systémovou lištěm při detekci neznámé sítě - podrobný popis najdete v kapitole [AVG Advisor](#)). [AVG Advisor](#) si zapamatuje jediné identifikační údaje sítě, zejména adresu MAC, a přístě už vás nebude upozorňovat. Každá síť, k níž se připojíte, bude pro přístě automaticky považována za známou, a přidána do seznamu. Libovolné položky můžete vymazat pomocí tlačítka **Smazat**; příslušná síť pak bude znovu považována za neznámou a neproverěnou.

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



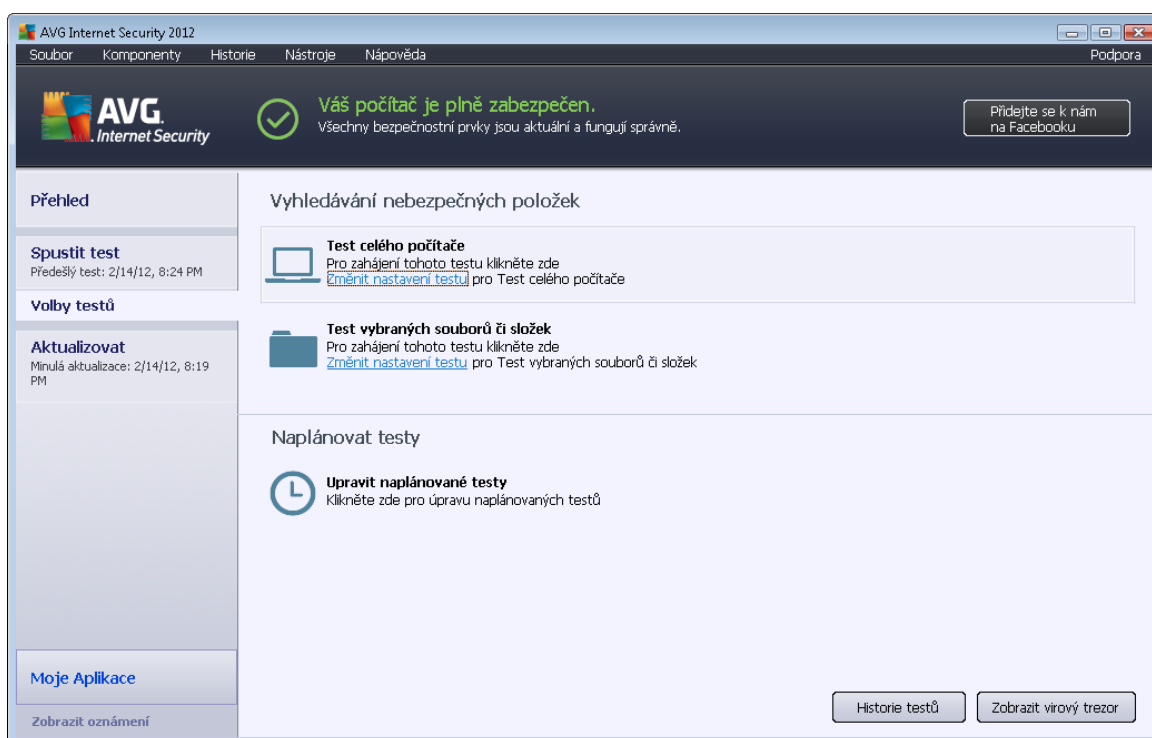
**Poznámka:** Funkce známé sítě v rámci služby AVG Advisor není podporována na Windows XP 64-bit.



## 12. AVG testování

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

### 12.1. Rozhraní pro testování



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

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

## 12.2. Přednastavené testy

Jednou z hlavních funkcí **AVG Internet Security 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.

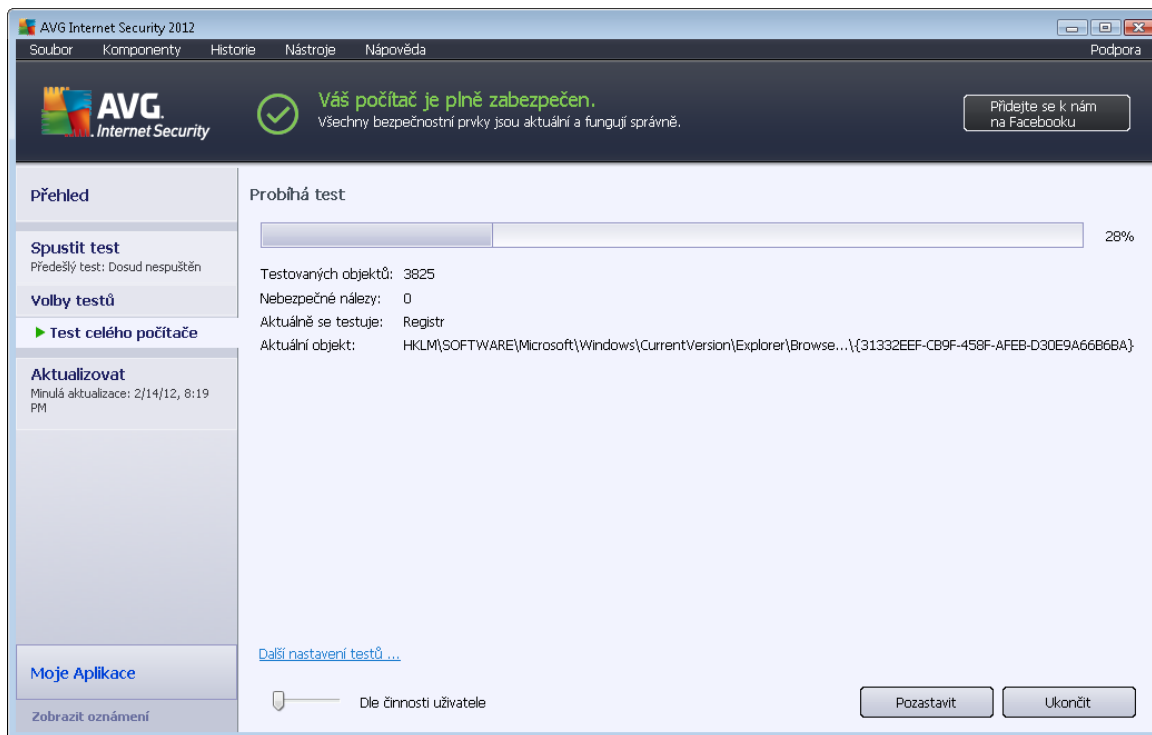
V **AVG Internet Security 2012** najdete tyto typy výrobcem nastavených testů :

### 12.2.1. Test celého počítače

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

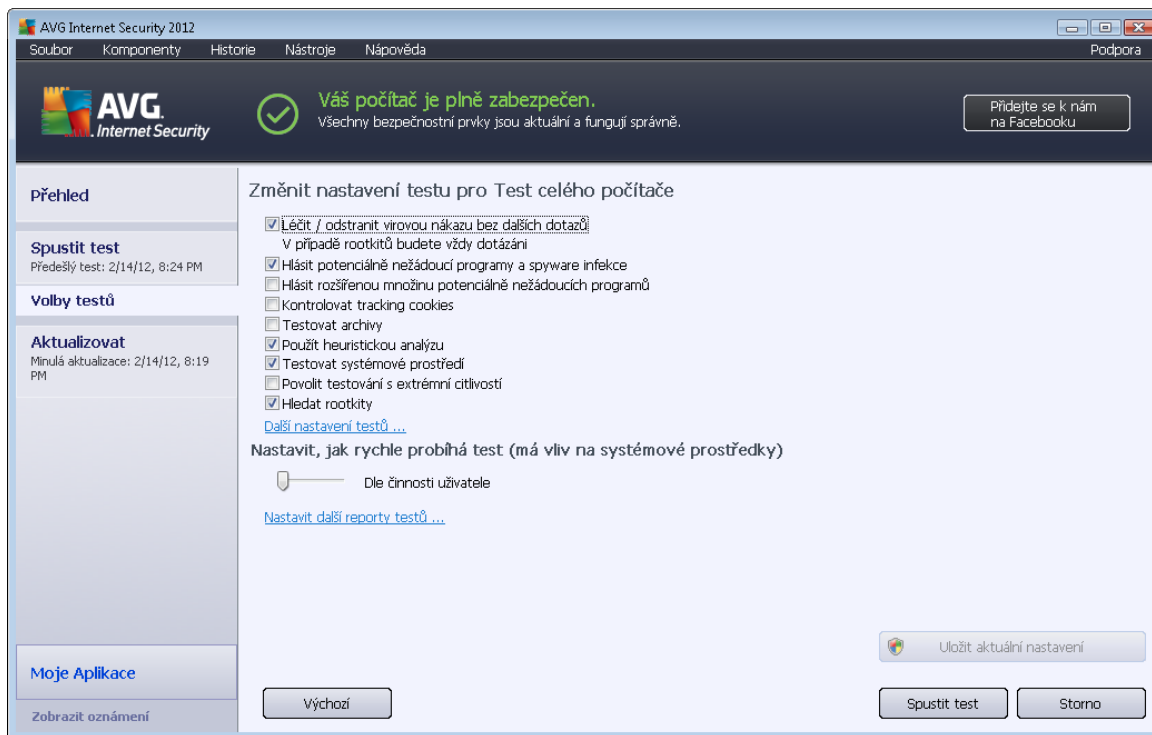
#### Spuštění testu

**Test celého počítače** spusíte 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!**

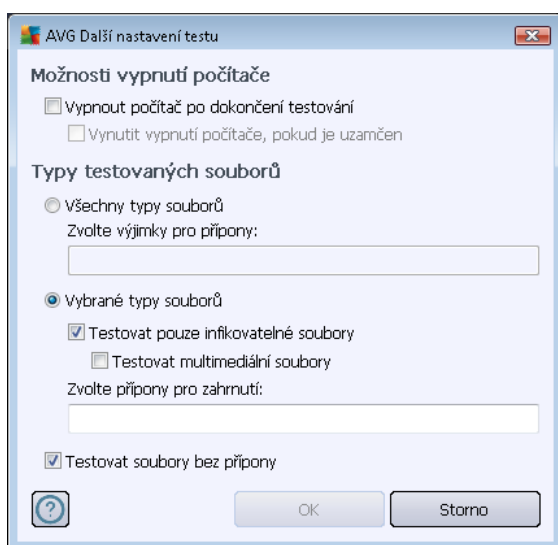


- **Parametry testu** - v seznamu parametrů testu můžete jednotlivé volby podle potřeby vypínat/zapínat:
  - **Léčit / odstranit virovou nákazu bez dalších dotazů** - (ve výchozím nastavení zapnuto): je-li během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k 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 hrozeb, 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 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).

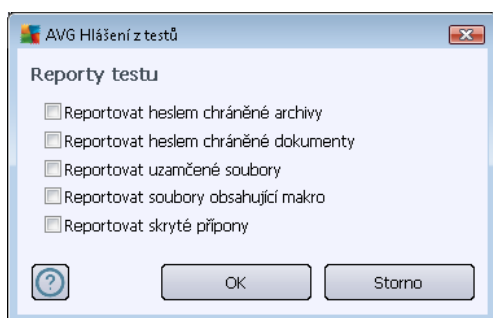
- **Testovat archivy** (ve výchozím nastavení vypnuto) - parametr definuje, že test má kontrolovat všechny soubory zabalené v n kterém typu archivu, například ZIP, RAR, ...
  - **Použití heuristickou analýzu** (ve výchozím nastavení zapnuto) - během testu bude použita k detekci infekce i metoda heuristické 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 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 rootkitů, 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 neoznacenou, 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 skutečnou 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 *dle zátěže uživatele*. Tato hodnota nastavení optimalizuje rychlost testu počítače a vytížení systémových zdrojů. Test můžete spustit pomaleji a tedy s nižší zátěží systémových zdrojů (*vhodné, pokud potěbujete 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 nikdy nepracuje*).
- **Nastavit další reporty testů** - odkaz otevírá nový dialog **Reporty testů**, v němž můžete označit, které typy nálezů mají být hlášeny:



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



## 12.2.2. Test vybraných souborů či složek

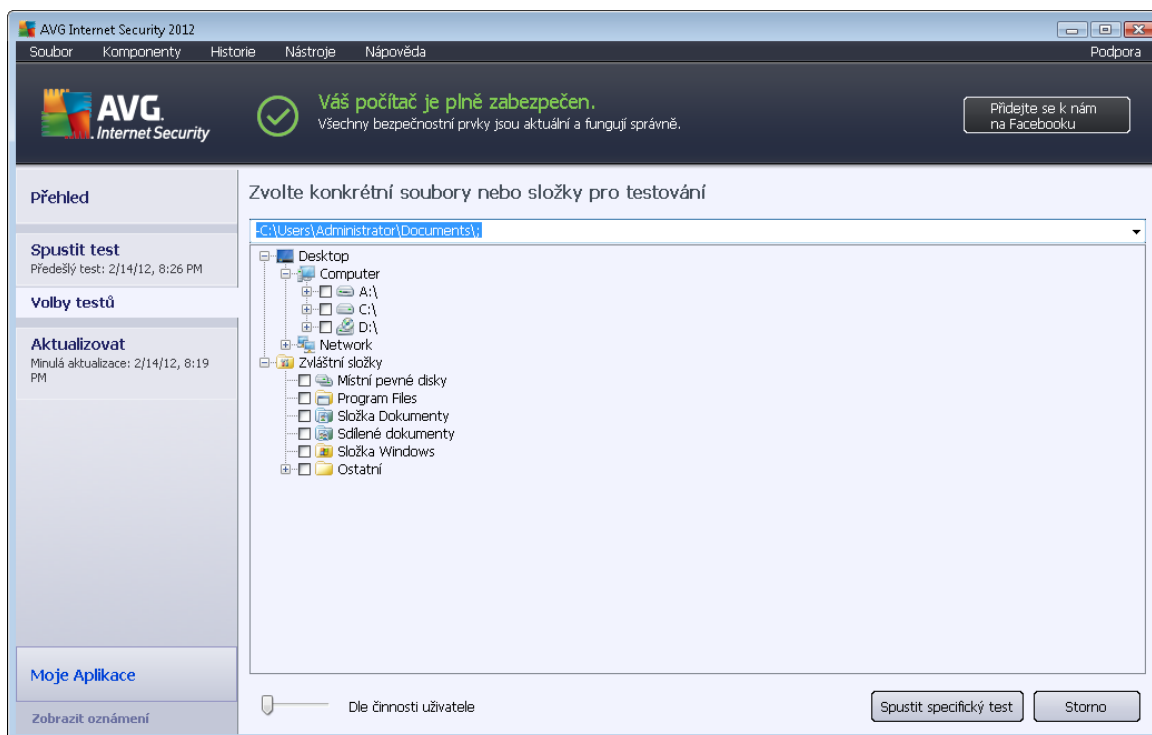
**Test vybraných souborů i složek** kontroluje pouze uživatelem definované oblasti počítače (zvolené složky, pevné disky, diskety, CD, optické disky, ...). Postup při nálezů a léčení / odstranění virových nákaz je stejný jako u **Testu celého počítače**: nalezené viry jsou vyléčeny nebo přesunuty do [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 určitý adresář bez kontroly všech v něm obsažených podadresářů, napište před automaticky vygenerovanou cestu k adresáři znaménko "-". Parametrem "!" před cestou k adresáři zase určíte, že celý adresář má být z testu vypuštěn.

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

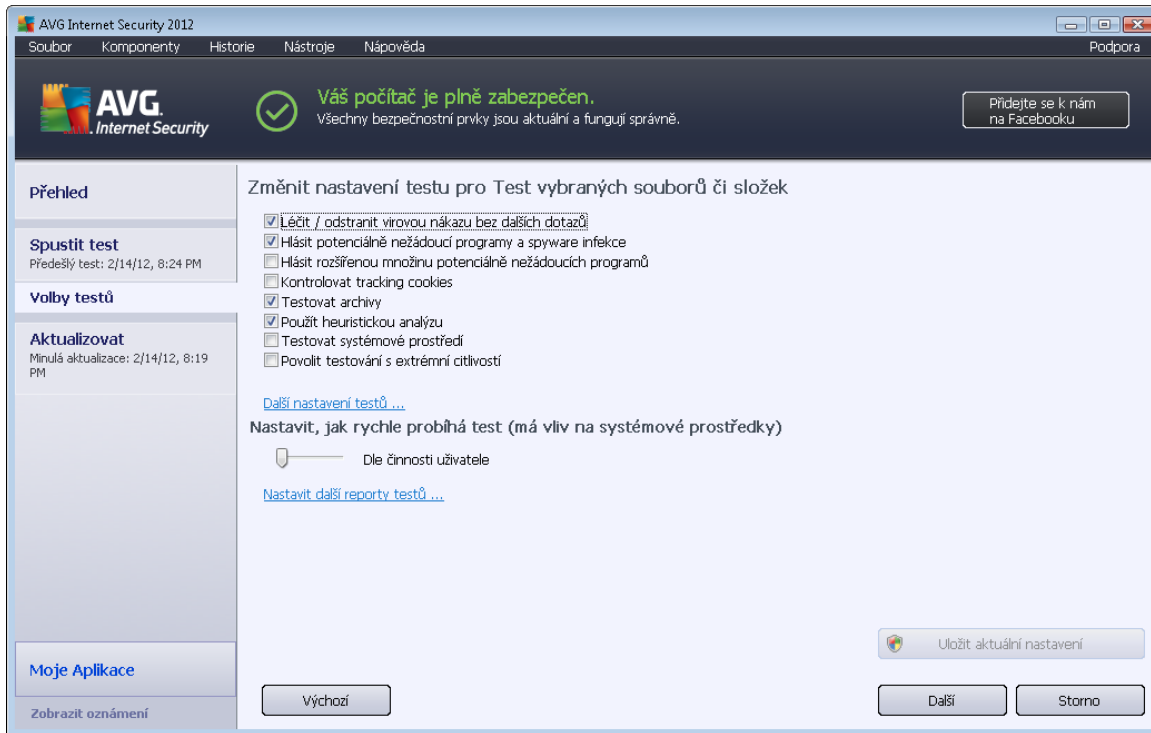


### Editace nastavení testu

Předejm definované výchozí nastavení **Testu vybraných souborů i složek** máte možnost editovat v dialogu **Změnit nastavení testu pro Test vybraných souborů i složek** (dostupného z [rozhraní pro testování](#) prostřednictvím odkazu **Změnit nastavení testu u Testu vybraných souborů a složek**).

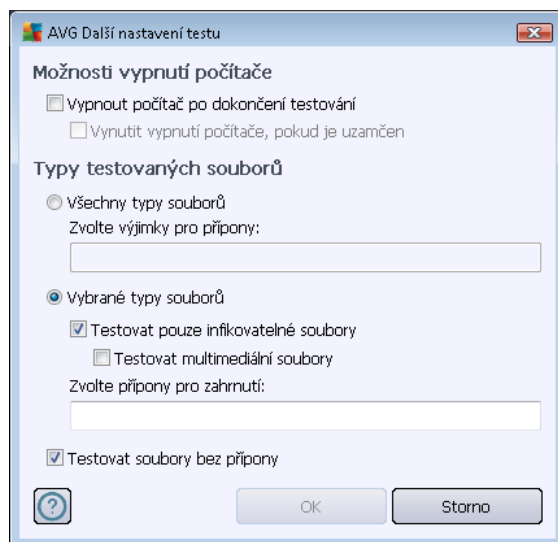


**Pokud však nemáte skutečný vod konfiguraci testu m nit, doporu ujeme se podržet výrobce definovaného nastavení!**



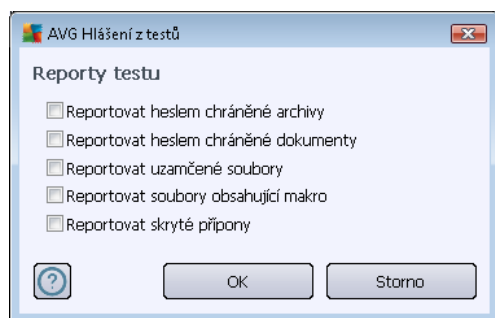
- **Parametry testu** - v seznamu parametrů testu můžete jednotlivé volby podle potřeby vypínat/zapínat:
  - **Heal / remove virus infection without asking me** - (ve výchozím nastavení zapnuto): je-li během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. Pokud virus automaticky léčit nelze, bude infikovaný objekt automaticky přesunut do [Virového trezoru](#).
  - **Hlásit potenciálně nežádoucí programy a spyware infekce** - (ve výchozím nastavení zapnuto): kontrola přítomnosti [potenciálně nežádoucích programů](#) (spustitelné programy, které mohou fungovat jako spyware nebo adware). Zaškrtnutím tohoto políčka aktivujete [Anti-Spyware](#), tj. bude se testovat přítomnost spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány 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 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 zasláná serverem prohlížeči a uložena na počítači uživatele; při každé další návštěvě téhož serveru prohlížeč posílá cookies zpět serveru, který podle nich rozlišuje jednotlivé uživatele).
  - **Testovat archivy** (ve výchozím nastavení zapnuto) - parametr definuje, že test má kontrolovat všechny soubory zabalené v n kterém typu archivu, například ZIP, RAR, ...
  - **Použít heuristickou analýzu** (ve výchozím nastavení zapnuto) - během testu bude použita k detekci infekce i metoda heuristické analýzy (dynamické emulace instrukcí testovaného objektu v prostředí virtuálního počítače).
  - **Testovat systémové prostředí** (ve výchozím nastavení vypnuto) - test provádí i systémové oblasti vašeho počítače.
  - **Povolit testování s extrémní citlivostí** (ve výchozím nastavení vypnuto) - ve specifických situacích (při podezření na infekci zavlečenou do vašeho počítače) můžete zvolit tuto metodu testování, která aktivuje nejdokladnější testovací algoritmy a velmi podrobně provádí naprosto všechny oblasti vašeho počítače. Mějte však na paměti, že tato metoda je časově velmi náročná.
- **Další nastavení testu** - odkaz otevírá dialog **Další nastavení testu**, kde můžete definovat následující parametry testu:



- **Možnosti vypnutí počítače** - určete, zda má být počítač po dokončení testu automaticky vypnut. Pokud potvrdíte tuto možnost (**Vypnout počítač po dokončení testování**), aktivuje se nová volba (**Vynutit vypnutí počítače, pokud je uzamčen**), při jejímž potvrzení dojde po dokončení testu k vypnutí počítače i tehdy, jestliže je počítač momentálně zamknut.
- **Typy testovaných souborů** - dále se můžete rozhodnout, zda si přejete testovat

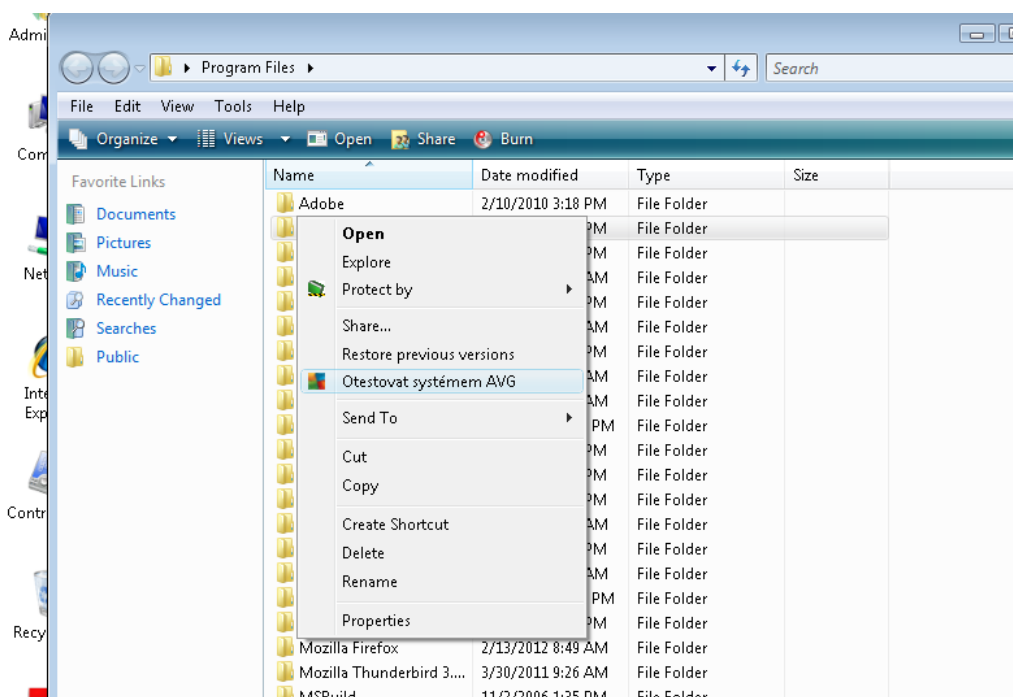
- **Všechny typy soubor** - pokud máte zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou;
- **Vybrané typy soubor** - můžete se rozhodnout, že chcete, aby se testy spouštěly pouze nad soubory, které lze považovat za infikovatelné (*soubory, které nemohou být infekcí 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 drželi, 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 *dle inosti uživatele*, čímž optimalizuje rychlost testu prioritou a vytížení systémových zdrojů. Test můžete spustit pomaleji a tedy s nižší zátěží systémových zdrojů (*vhodné, pokud potřebujete během testu na počítači pracovat a nezáleží vám tolik na celkové době testování*) nebo naopak rychleji s vyššími nároky na systémové zdroje (*například v době, kdy na počítači nikdy 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 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](#)).

### 12.3. Testování v průzkumníku Windows

AVG Internet Security 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 Internet Security 2012**

### 12.4. Testování z příkazové řádky

V rámci AVG Internet Security 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 ů jsou tyto uvedeny za sebou a odd ěleny 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 ěleny st edníkem, nap íklad: **avgscanx /scan=C:\;D:\**

## Parametry p íkazu

Kompletní p ehled použitelných parametr ů 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 ů najdete v kapitole [Parametry CMD testu](#).

Test spustíte stiskem klávesy **Enter**. V pr ůběhu 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 ěn z p íkazové ádky; dialog **Nastavení testu z p íkazové ádky** slouží pouze jako nástroj pro snadné nastavení parametr ů testu, aniž byste je museli definovat v prost edí p íkazové ádky.

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

### 12.4.1. Parametry CMD testu

V následujícím p ehledu nabízíme seznam dostupných parametr ů testu:

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



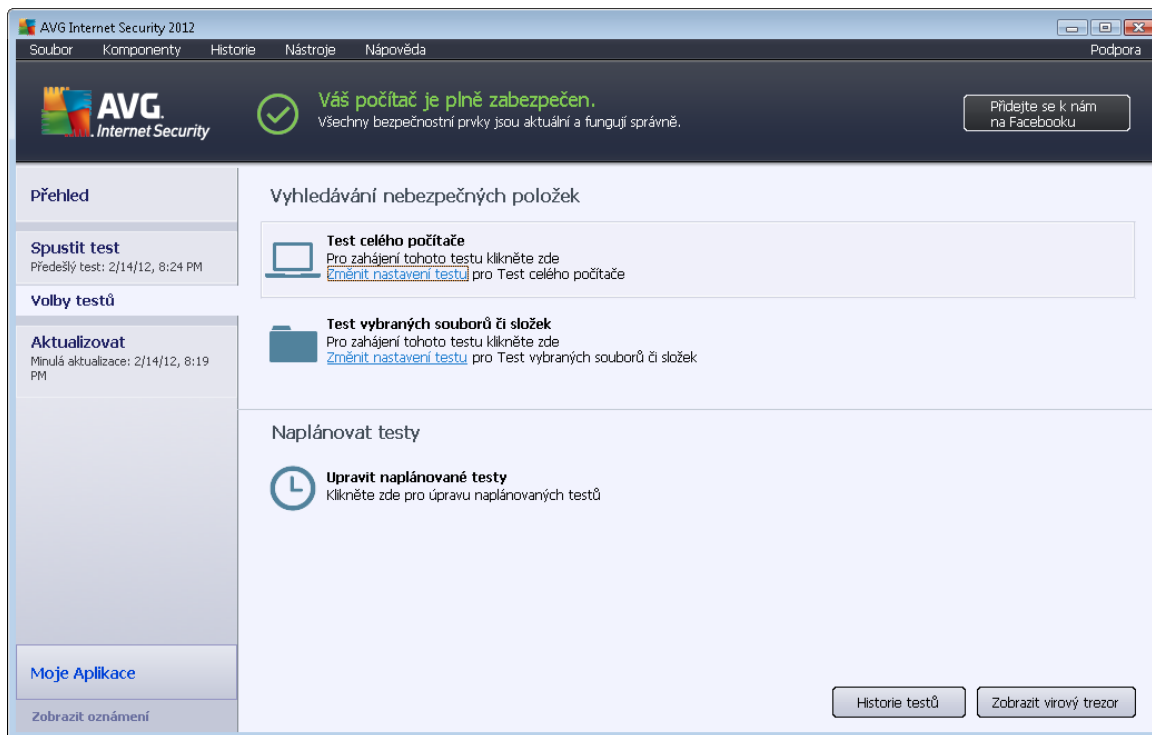
- /ADS Testovat alternativní datové proudy (pouze NTFS)
- /HIDDEN Hlásit soubory se skrytou příponou
- /INFECTABLEONLY Testovat pouze infikovatelné soubory
- /THOROUGHSCAN Povolit testování s extrémní citlivostí
- /CLOUDCHECK Ověřit falešné detekce
- /ARCBOMBSW Hlásit opakovaně komprimované archivní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

## 12.5. Naplánování testu

Testy v **AVG Internet Security 2012** lze spouštět buďto na vyžádání (*například v situaci, kdy máte podezření na zvláštní 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.

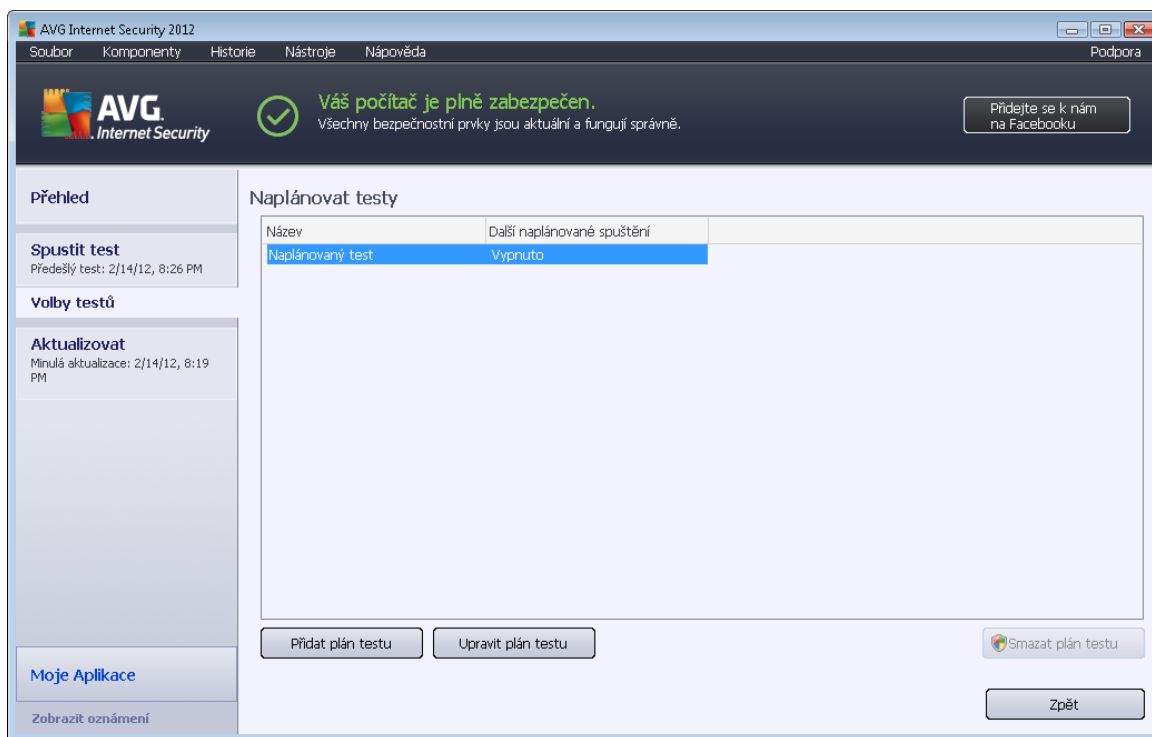
[Test celého počítače](#) by měl být spouštěn pravidelně, a to nejméně jednou týdně. Pokud vám to však provoz na vašem počítači umožní, doporučujeme spouštět test celého počítače jednou denně; tak je také ve výchozí konfiguraci nastaven plán testů. Jestliže je počítač trvale zapnutý, je vhodné naplánovat spuštění **Testu celého počítače** na dobu mimo pracovní hodiny. Pokud počítač vypínáte, nezapomejte využít možnosti [spustit test při startu počítače, pokud byl naplánovaný aš 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** otevře nový dialog **Naplánovat testy**, v něm můžete najít přehled všech aktuálně naplánovaných testů :

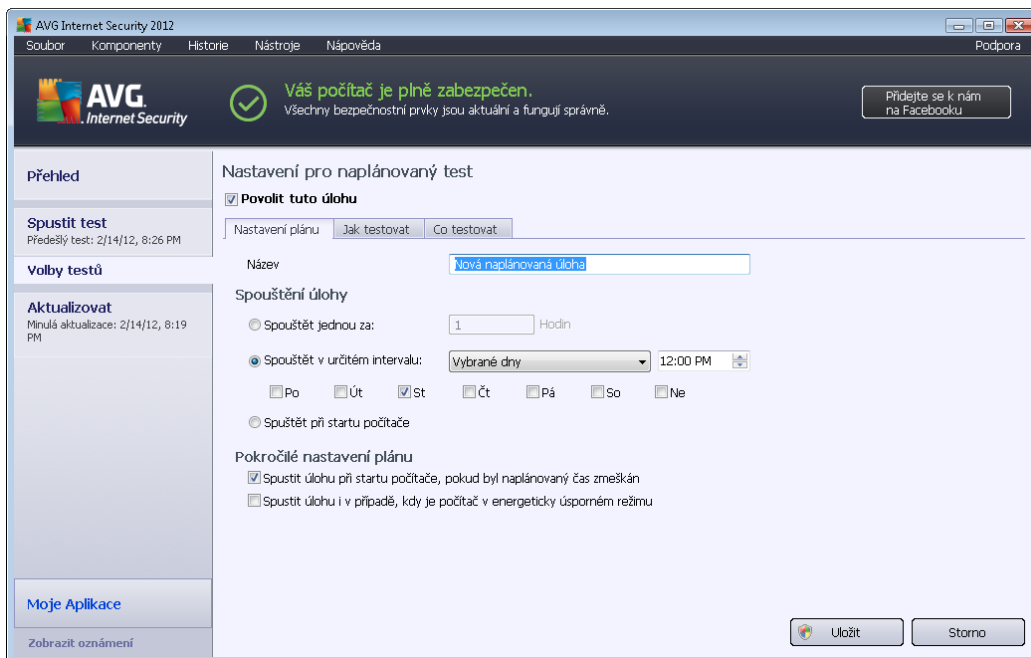


Pracovat můžete s těmito ovládacími tlačítky:

- **Přidat plán testu** - tlačítkem otevřete dialog **Nastavení pro naplánovaný test**, na záložce [Nastavení plánu](#). V tomto dialogu máte možnost specifikovat parametry nově definovaného testu.
- **Upravit plán testu** - tlačítkem můžete 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 být stiskem tlačítka zrušen. Odebírat však můžete jen své vlastní nastavené plány; **Plán testu celého počítače**, který je nastaven jako výchozí, smazat nelze.
- **Zpět** - návrat do [testovacího rozhraní AVG](#)

### 12.5.1. Nastavení plánu

Chcete-li naplánovat nový test a jeho pravidelné spuštění, vstupte do dialogu **Nastavení pro naplánovaný test** (kliknutím na tlačítko **Přidat plán testu** v dialogu **Naplánování testu**). Dialog je rozdělen do tří záložek: **Nastavení plánu** (viz obrázek; výchozí záložka, na kterou budete automaticky 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 podle potřeby znovu použít.

Dále pojmenujte test, který chcete vytvořit a naplánovat. Jméno testu zadejte do textového pole u položky **Název**. Snažte se používat stručné a souhlasné výstižné názvy testů, abyste později snadno rozeznali, o jaký test se jedná.

**Příklad:** Nevhodným názvem testu je například "Nový test" nebo "Martin v test", protože ani jeden název nevypovídá o tom, co test ve skutečnosti kontroluje. Naproti tomu správným popisným názvem testu může být například "Test systémových oblastí" nebo "Test disku C:" a podobně. Rovněž není nutné označovat testy termíny Test celého počítače versus Test vybraných souborů a složek - váš nastavený test bude vždy specifickým nastavením testu vybraných souborů a složek.

V tomto dialogu můžete dále definovat tyto parametry testu:

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

### Ovládací tlačítka dialogu

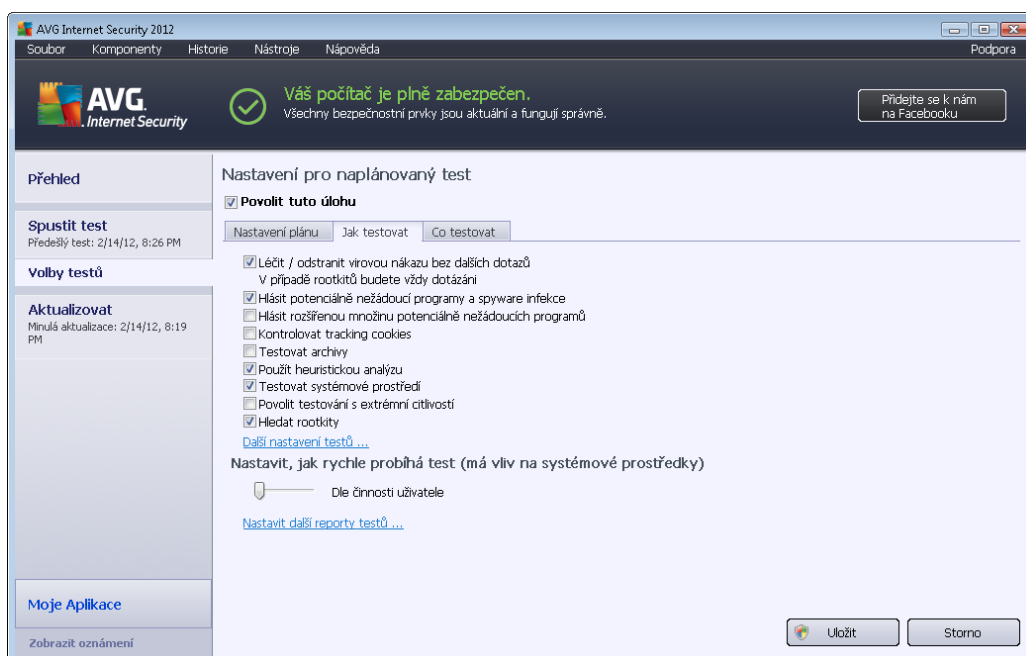
Ze všech tří záložek dialogu **Nastavení pro naplánovaný test** (*Nastavení plánu*, [Jak testovat](#) a [Co testovat](#)) jsou dostupná dvě ovládací tlačítka, jež mají stejnou funkci na kterékoli záložce



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](#).

## 12.5.2. Jak testovat



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

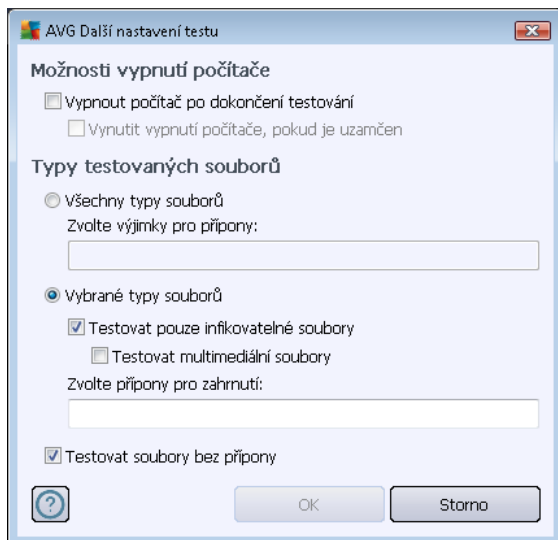
- **Léčit / odstranit virovou nákazu bez dalších dotazů** - (ve výchozím nastavení zapnuto): je-li během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. Pokud virus automaticky léčit nelze, anebo pokud se rozhodnete tuto funkci vypnout, budete o nález virusu 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

pon kud problematickou kategorií hrozeb, protože i když v tšina t chto program p edstavuje bezpečnostní riziko, jsou mnohdy instalovány v dom a se souhlasem uživatele. Doporu ujeme nicmén ponechat tuto volbu aktivní, protože výrazn zlepšuje zabezpečení vašeho počíta e.

- **Hlásit rozší enou množinu potenciáln nežádoucích program** - (ve výchozím nastavení vypnuto): zaškrtnutím tohoto polí ka m žete aktivovat navíc detekci rozší ené sady spyware: program , které jsou v p vodní podob od výrobce neškodné a v po ádku, ale mohou být snadno zneužity ke škodlivým ú el m. Jde o dodate né opat ení, které zlepšuje zabezpečení vašeho počíta e na další úrovni, nicmén 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 i a uložena na počíta i uživatele; p i každé další návště v téhož serveru prohlíže posílá cookies zp t serveru, který podle nich rozlišuje jednotlivé uživatele*).
- **Testovat archívy** - (ve výchozím nastavení vypnuto): parametr definuje, že test má kontrolovat všechny soubory, a to i takové, které jsou zabaleny v n kterém typu archívu, například ZIP, RAR, ...
- **Použít 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 počíta e*).
- **Testovat systémové prost edí** - (ve výchozím nastavení zapnuto): test prov í i systémové oblasti vašeho počíta e.
- **Povolit testování s extrémní citlivostí** (ve výchozím nastavení vypnuto): ve specifických situacích (*p i podez ení na infekci ve vašem počíta i*) m žete zvolit tuto metodu testování, která aktivuje nejd kladn jší testovací algoritmy a velmi podrobn prov í naprosto všechny oblasti vašeho počíta e. M jte však na pam ti, že tato metoda je asov velmi náro ná.
- **Hledat rootkity** (ve výchozím nastavení zapnuto): parametr komponenty [Anti-Rootkit](#) prohledává počíta na p ítomnost rootkit , tedy program a technologií, které dokáží maskovat p ítomnost malware v počíta i. Dojde-li k nálezu rootkitu, nemusí to nutn znamenat, že je počíta infikovaný. V n kterých p ípadech mohou být rootkity použity jako ovlada e nebo ásti korektních aplikací.

Dále máte možnost upravit konfiguraci testu tímto nastavením:

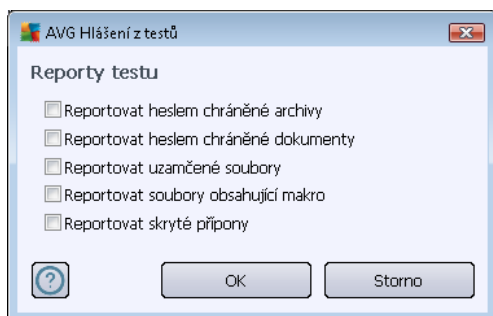
- **Další nastavení testu** - odkaz otevírá dialog **Další nastavení testu**, kde m žete definovat následující parametry testu:



- **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** - při němž 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 dle *inertnosti uživatele*, čímž optimalizuje rychlost testu počítače a vytížení systémových zdrojů. Test můžete spustit pomaleji a tedy s nižší zátěží systémových zdrojů (*vhodné, pokud potřebujete během testu na počítači pracovat a nezáleží vám tolik na celkové době testování*) nebo naopak rychleji s vyššími nároky na systémové zdroje (*například v době, kdy na počítači nikdo nepracuje*).



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

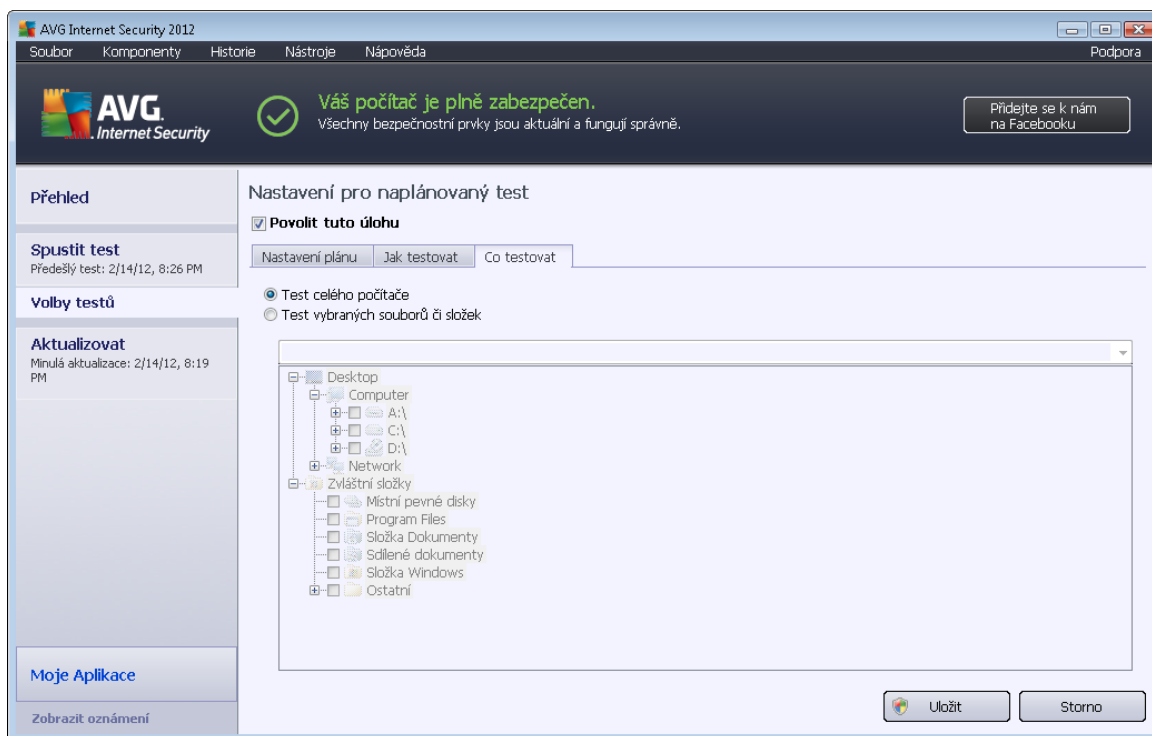


### Ovládací tlačítka dialogu

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](#).

### 12.5.3. 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 zaškrtnutých 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 (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**



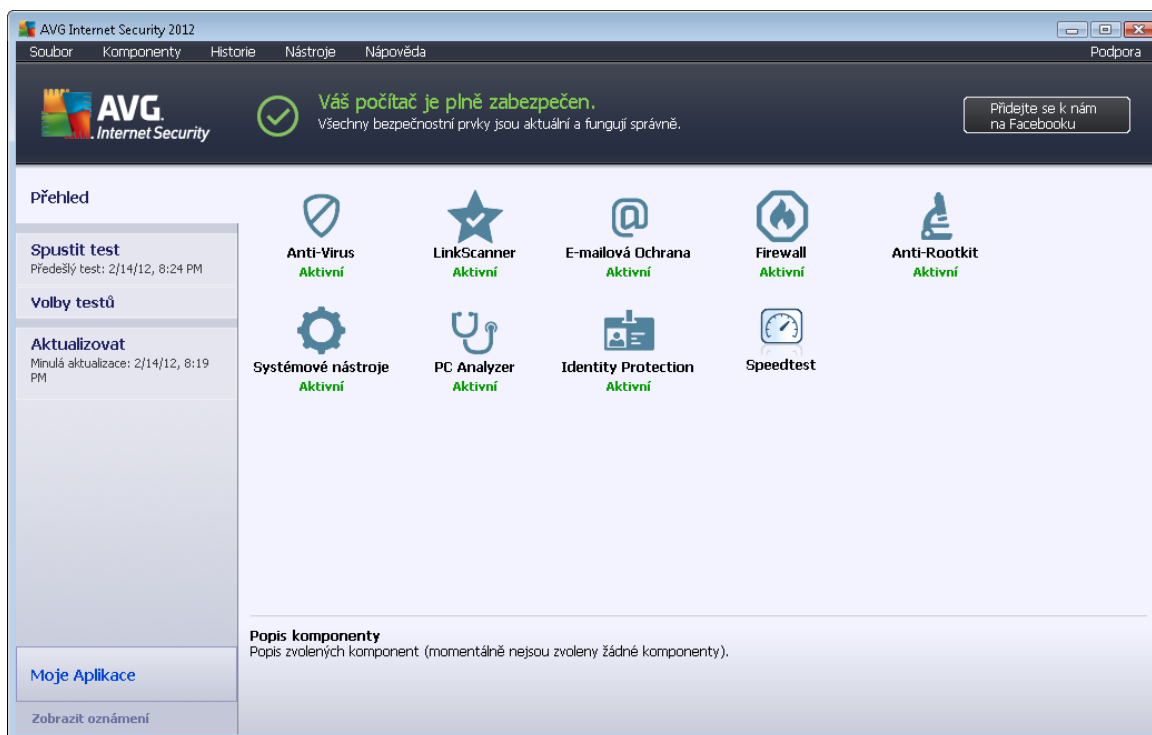
- pro Win XP: C:\Documents and Settings\Default User\My Documents\
- pro Windows Vista/7: C:\Users\user\Documents\
- **Sdílené dokumenty**
  - pro Win XP: C:\Documents and Settings\All Users\Documents\
  - pro Windows Vista/7: C:\Users\Public\Documents\
- **Složka Windows** - C:\Windows\
- **Ostatní**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

### Ovládací tlačítka dialogu

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


## 12.6. Přehled výsledků testů




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

- **Název** - označením testu může být buďto název jednoho z [přednastavených testů](#) nebo název, kterým jste sami označili [vlastní test](#). Každý název je předznačen 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 proběhl 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 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](#)

## 12.7. 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:

- [Přehled výsledků](#) - 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).

### 12.7.1. Záložka Přehled výsledků

The screenshot shows the AVG Internet Security 2012 interface. At the top, a green checkmark indicates the computer is fully protected. The main area displays the results of a test titled "Test vybraných souborů či složek". The test was completed on 2/14/12 at 8:26 PM. The results table shows 4 infections found, 0 removed, and 4 not removed. Additionally, 11 spyware items were found, 0 removed, and 11 not removed. The interface includes a sidebar with options like "Spustit test", "Volby testů", "Aktualizovat", and "Moje Aplikace".

Nalezeno	Odstraněno a vyléčeno	Neodstraněno nebo nevyléčeno
4	0	4
11	0	11

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

Složky vybrané k testování: -C:\Users\Administrator\Documents\;  
Test zahájen: Tuesday, February 14, 2012, 8:26:01 PM  
Test dokončen: Tuesday, February 14, 2012, 8:26:04 PM (3 sekund(a))  
Celkem otestováno objektů: 19  
Uživatel: Administrator

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

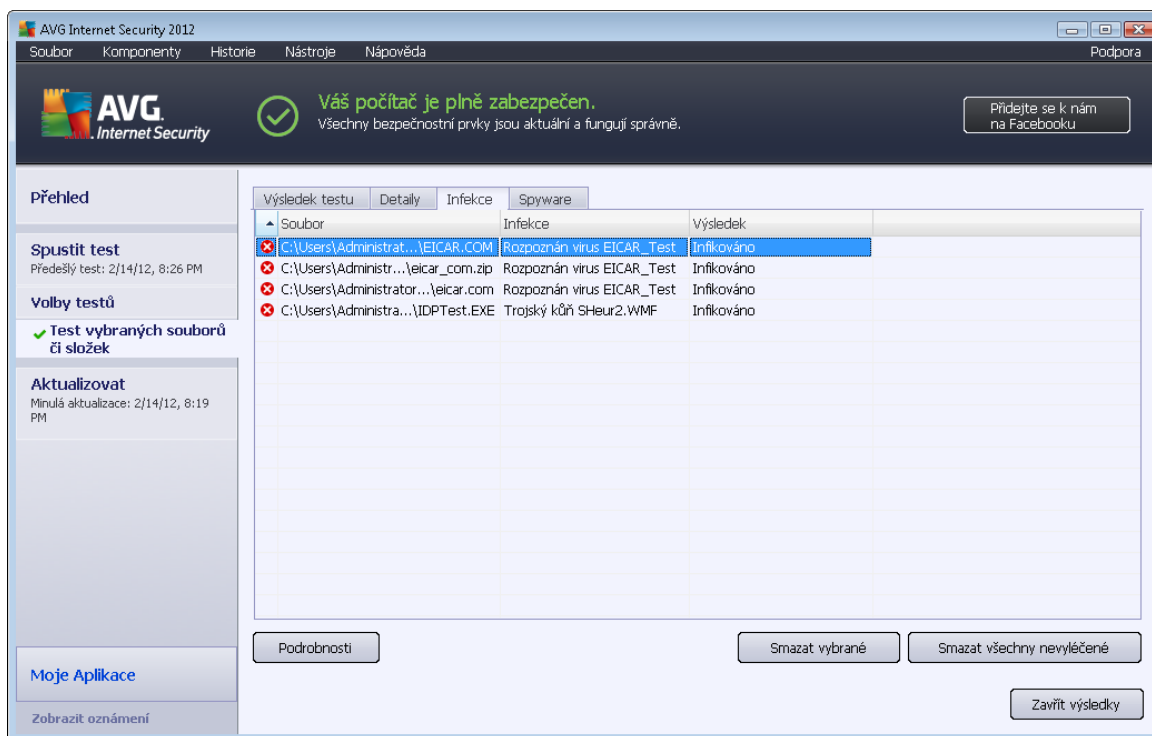
- detekovaných virových infekcích / spyware
- vyléčených virových infekcích / spyware
- počet virových infekcích / spyware, které se nepodařilo odstranit nebo vyléčit

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

#### Ovládací tlačítka dialogu

V dialogu je dostupné jediné ovládací tlačítko **Zpět**, kterým se vrátíte do dialogu [Přehled výsledků testu](#).

## 12.7.2. 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 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
  - **Přidáno k výjimkám PUP** - nález byl vyhodnocen jako výjimka a připojen k seznamu výjimek PUP (*výjimky lze editovat v dialogu [PUP výjimky](#) pomocí*

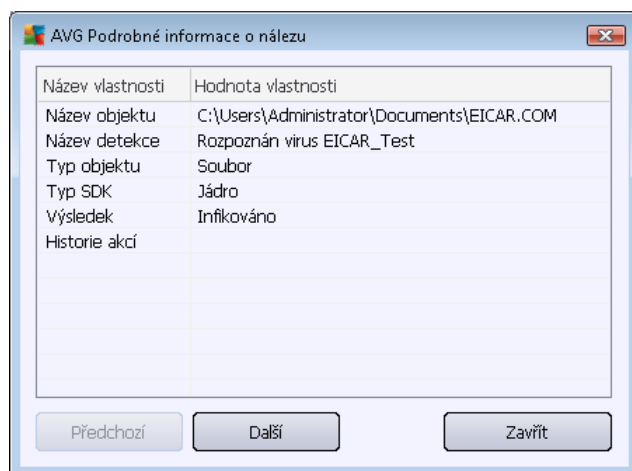
*nastavení)*

- **Zam ený soubor - neotestován** - objekt je zam ený a nebylo možno jej otestovat
- **Potenciáln nebezpe ný objekt** - objekt je detekován jako potenciáln nebezpe ný, ale nikoli infikovaný (*m že nap íklad obsahovat makra*). Informace má tedy pouze charakter upozorn ní.
- **Pro dokon ení akce je pot eba provést restart** - infikovaný objekt nebylo možno odstranit, pro jeho odstran ní je t eba provést restart počíta e

### Ovládací tlačítka dialogu

V dialogu jsou dostupná tato tlačítka:

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

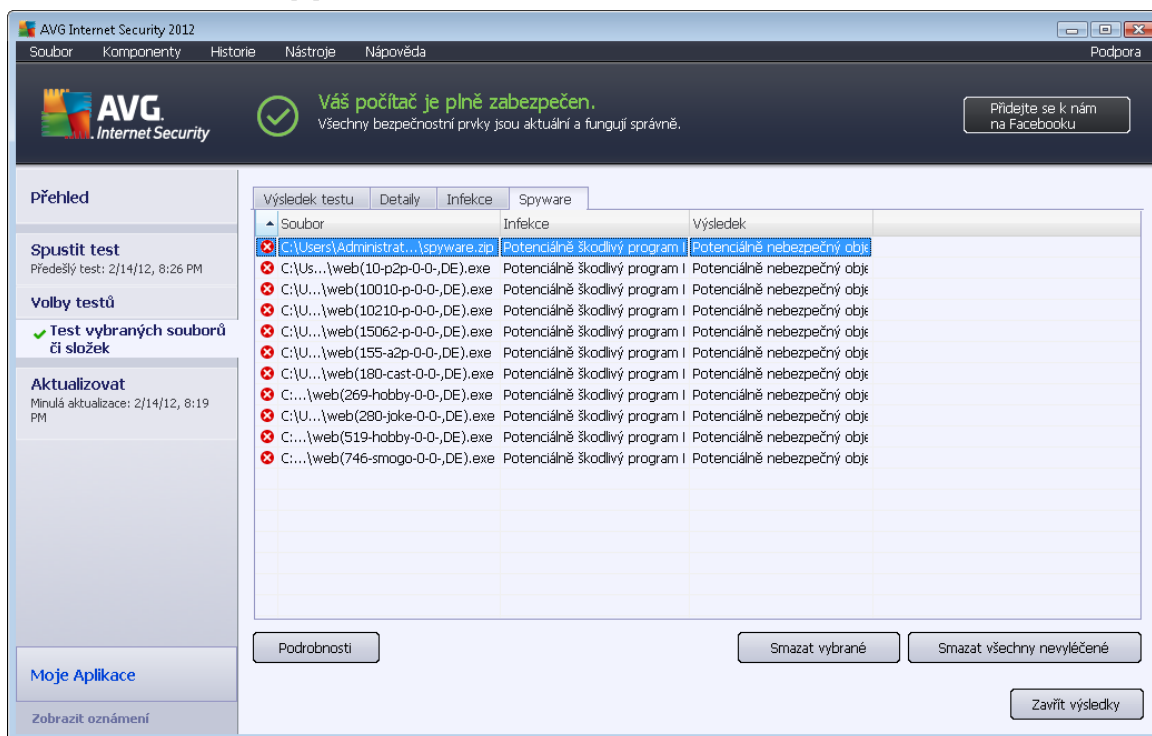


V tomto dialogu najdete detailní informace o infekci (*nap íklad umíst ní a jméno detek ovaného infik ovaného objektu, typ objektu, typ SDK, výsledek detekce a historii akcí provedených nad detek ovaným objektem*). Pomocí tlačítek **Předchozí** / **Další** můžete postupně zobrazovat informace o jednotlivých nálezů. Tlačítkem **Zavřít** dialog zavřete.

- **Smazat vybrané** - tlačítkem přesunete v seznamu ozna ený nález do [Virového trezoru](#)
- **Smazat všechny nevylé ené** - tlačítko odstraní všechny nálezy, které nelze lé it ani nemohou být přesunuty do [Virového trezoru](#)
- **Zavřít výsledky** - zavřá detail výsledku testu a přepíná zp t do dialogu [Přehled výsledk test](#)



### 12.7.3. Záložka Spyware



Soubor	Infekce	Výsledek
C:\Users\Administrat...spyware.zip	Potenciálně škodlivý program	Potenciálně nebezpečný obje
C:\Us...web(10-p2p-0-0-,DE).exe	Potenciálně škodlivý program	Potenciálně nebezpečný obje
C:\U...web(10010-p-0-0-,DE).exe	Potenciálně škodlivý program	Potenciálně nebezpečný obje
C:\U...web(10210-p-0-0-,DE).exe	Potenciálně škodlivý program	Potenciálně nebezpečný obje
C:\U...web(15062-p-0-0-,DE).exe	Potenciálně škodlivý program	Potenciálně nebezpečný obje
C:\U...web(155-a2p-0-0-,DE).exe	Potenciálně škodlivý program	Potenciálně nebezpečný obje
C:\U...web(180-cast-0-0-,DE).exe	Potenciálně škodlivý program	Potenciálně nebezpečný obje
C:...web(269-hobby-0-0-,DE).exe	Potenciálně škodlivý program	Potenciálně nebezpečný obje
C:\U...web(280-joke-0-0-,DE).exe	Potenciálně škodlivý program	Potenciálně nebezpečný obje
C:...web(519-hobby-0-0-,DE).exe	Potenciálně škodlivý program	Potenciálně nebezpečný obje
C:...web(746-smogo-0-0-,DE).exe	Potenciálně škodlivý program	Potenciálně nebezpečný obje

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:

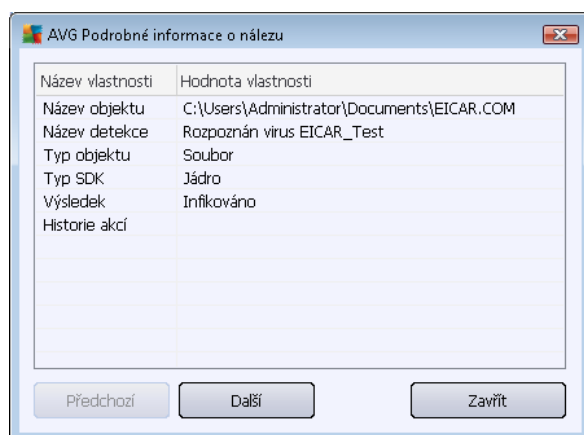
- **Soubor** - plná adresa povodního umístění infikovaného objektu na lokálním disku
- **Infekce** - jméno detekovaného spyware (*podrobnosti o jednotlivých virech najdete ve [Virové encyklopedii online](#)*)
- **Výsledek** - uvádí, v jakém stavu se infikovaný a během testu detekovaný objekt aktuálně 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
  - **Presunuto 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](#) pokročilého nastavení*)
- **Zaměněný soubor** - neotestován - objekt je zaměněný a nebylo možno jej otestovat
- **Potenciálně nebezpečný objekt** - objekt je detekován jako potenciálně nebezpečný, ale nikoli infikovaný (*může například obsahovat makra*). Informace má tedy pouze charakter upozornění.
- **Pro dokončení akce je 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 nálezů**:



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

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



#### 12.7.4. 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 v případě adware nebo spyware infekce. Pokud ve výsledku testu zobrazuje **AVG Internet Security 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 Internet Security 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.

#### 12.7.5. 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. V tichosti 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 své škodlivé kódu poměrně výsadní postavení, jelikož pronikají hluboko do systému, přebírají požadavky systémových volání a správné výsledky nahrazují svými vlastními.

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

#### 12.7.6. Záložka Informace

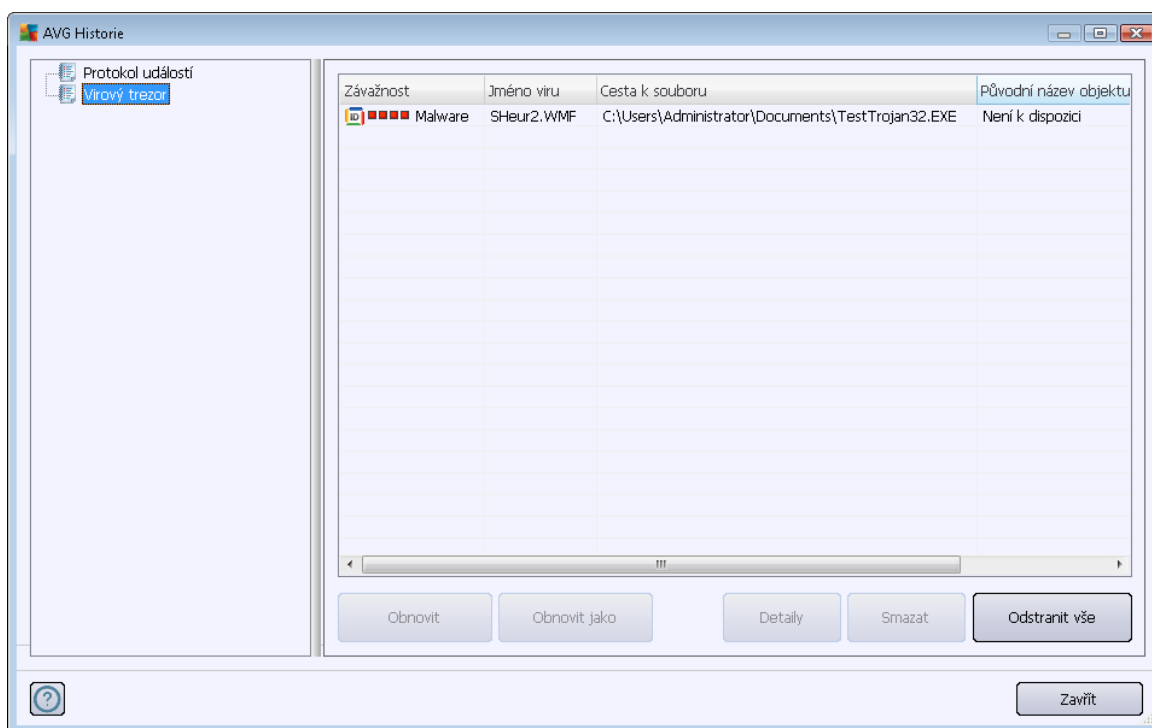
Záložka **Informace** obsahuje údaje o takových "nálezích", které nelze zařadit do kategorie infekcí, spyware, ... ani je pozitivně označit za nebezpečné, přesto zasluhují pozornost. Jsou to tedy soubory, které nejsou infikované, ale mohou být podezřelé. Takové soubory jsou hlášeny jako [Varování](#)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

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

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

- **Rekurzní runtime komprese:** Podobné jako v předchozím případě, ovšem méně 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 Internet Security 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 Internet Security 2012** vás na tyto soubory upozorní, abyste předešli jejich náhodnému spuštění.
- **Soubor spuštěný z nesprávného umístění:** Pokud je nalezen kterýkoliv systémový soubor spuštěný z jiného než výchozího umístění (například *winlogon.exe* spuštěný z jiné složky než Windows), **AVG Internet Security 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 Internet Security 2012**. Tato informace ve výsledku testů znamená, že soubor je permanentně používán systémem (například stránkový soubor).

## 12.8. 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.

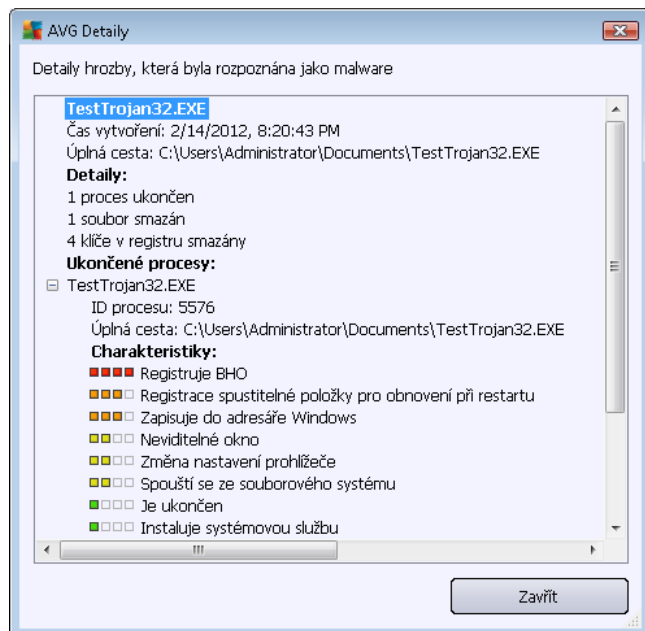
Rozhraní **Virového trezoru** se otevírá v samostatném okně a nabízí přehled informací o infikovaných objektech uložených v karanténě :

- **Závažnost** - jestliže jste si v rámci instalace programu **AVG Internet Security 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 pro přílohu emailu může být označeno 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*).



## 13. 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 šíí nově vzniklé počítačové hrozby, je nezbytně nutné Vás **AVG Internet Security 2012** pravidelně aktualizovat. V ideálním případě ponechte prosím program ve výchozím nastavení, kdy je zapnuta automatická aktualizace. Bez aktuální virové databáze nebude **AVG Internet Security 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.***

### 13.1. Spouštění aktualizace

Pro zajištění maximální bezpečnosti ověřte **AVG Internet Security 2012** ve výchozím nastavení aktualizací definic každé čtyři hodiny. Vzhledem k tomu, že aktualizace AVG nejsou vydávány podle pevného plánu, ale v reakci na počet a závažnost nových hrozeb, je tato kontrola nezbytná a zajistí, že váš **AVG Internet Security 2012** bude aktuální během celého dne.

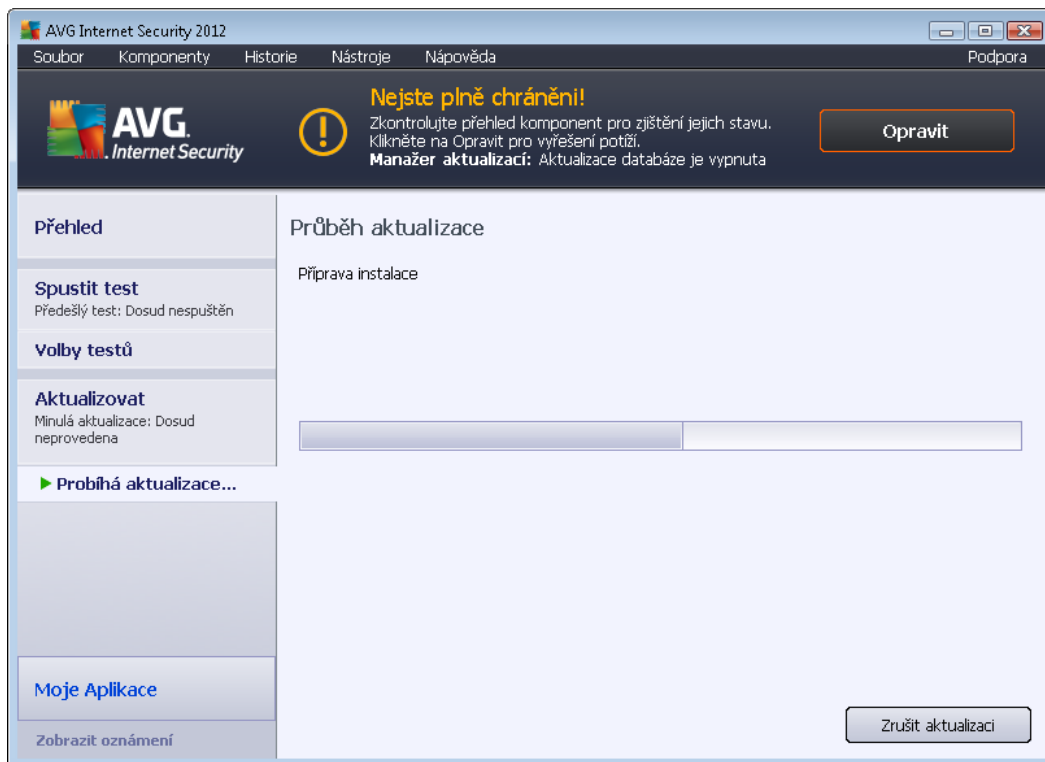
Pokud si přejete omezit počet výskytů kontroly aktualizace, máte možnost nastavit vlastní parametry spouštění aktualizace. V každém případě však doporučujeme, abyste aktualizaci spouštěli nejméně jednou denně! Nastavení lze editovat v sekci [Pokročilé nastavení/Naplánované úlohy](#), konkrétně v dialogích:

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

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](#).

### 13.2. Průběh aktualizace

Po spuštění aktualizace dojde nejprve k ověření, zda existují nové aktualizací soubory, jež dosud nebyly aplikovány. Pokud ano, **AVG Internet Security 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 / Příslušenství / Systémové nástroje / Obnova systému. Doporučujeme pouze zkušeným uživatelům!

### 13.3. Úrovně aktualizace

AVG Internet Security 2012 rozlišuje dvě úrovně aktualizace:

- **Aktualizace definic** zajišťuje, že jste chráněni proti nejnovějším hrozbám, které by mohly poškodit váš počítač. Zahrnuje pouze změny nezbytné pro spolehlivé fungování antivirové ochrany. Neobsahuje změny v kódu aplikace a aktualizuje pouze virovou, spamovou a spyware databázi.
- **Programová aktualizace** zahrnuje různé programové změny a doplňky. U klíčových systémových (souborový server) doporučujeme neprovádět aktualizaci automaticky po jejím vydání, ale nejprve ji otestovat v testovacím prostředí.

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

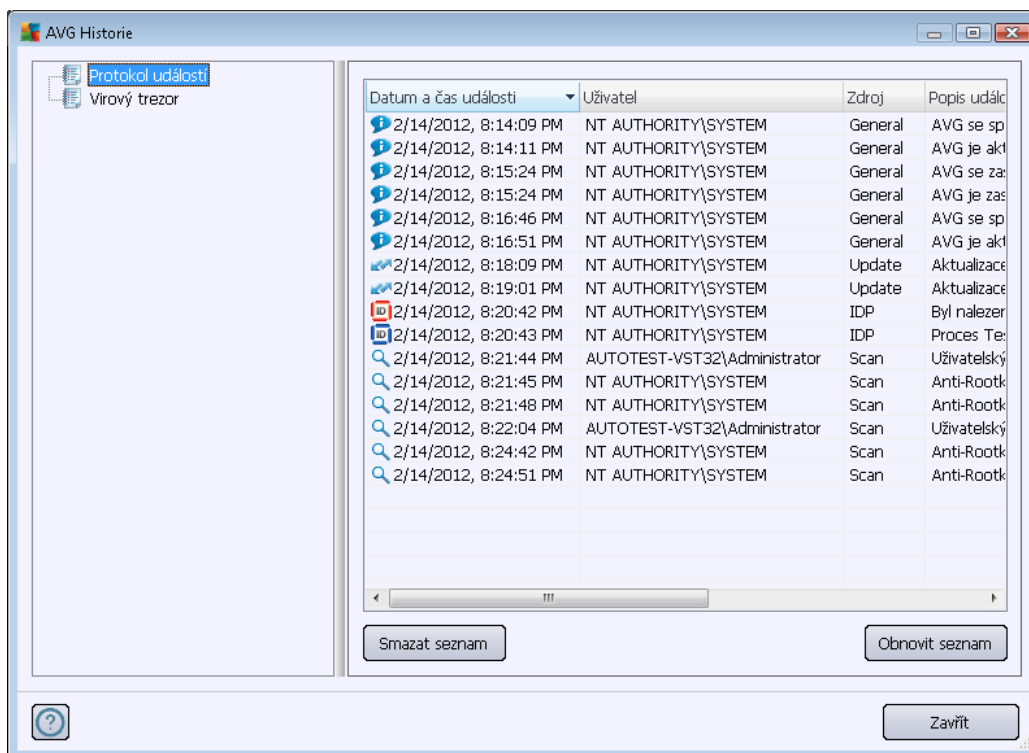
- [Plán aktualizace definic](#)
- [Plán programové aktualizace](#)





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

## 14. 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 Internet Security 2012**. Zaznamenávají se 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 (přes [testování](#) i [rezidentním štítem](#)) s uvedením konkrétního místa nálezů
- informace o ostatních dležících událostech

Ke každé události jsou evidovány následující údaje:

- **Datum a čas události** udává přesné 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

## 15. FAQ a technická podpora

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

- **Podpora na webu:** Přímo z prostředí aplikace AVG můžete přejít do specifické sekce webu AVG (<http://www.avg.cz/>), která je vyhrazena zákaznické podpoře. V hlavním menu zvolte položku **Návod** / **Získat podporu**. Budete automaticky přemístěni na příslušnou stránku s nabídkou dostupné podpory. Dále prosím postupujte podle pokynů uvedených na webu.
- **Podpora (v hlavním menu):** Systémové menu aplikace AVG (v horní liště hlavního dialogu) obsahuje položku **Podpora**. Ta otevírá nový dialog s kompletním výhledem informací, které můžete potřebovat při kontaktu se zákaznickou podporou. Dialog dále obsahuje základní údaje o instalovaném programu AVG (verzi programu a databáze), licenční údaje a seznam odkazů na zdroje podpory:



- **ešení potíží v návodu:** Přímo v návodu programu **AVG Internet Security 2012** je nově k dispozici sekce **ešení potíží** (soubor návodů lze otevřít z kteréhokoliv dialogu aplikace stiskem klávesy F1). Ta nabízí výhled 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 výhled tematických okruhů, které řeší problémy obchodního i technického charakteru.



- **asto kladené otázky:** Na webu AVG (<http://www.avg.cz/>) najdete také samostatnou a detailnějším způsobem sekci asto kladených otázek. Tato sekce je dostupná volbou **Centrum podpory / FAQ**. Otázky jsou opět přehledně rozděleny do kategorií obchodní, technické a virové.
- **Informace o virech a hrozbách:** Samostatná kapitola je na webu AVG (<http://www.avg.cz/>) věnována virové tematice (*webová stránka je dostupná prostřednictvím volby Nápověda / Informace o virech v hlavním menu*). Volbou **Centrum podpory / Informace o virech a hrozbách** vstoupíte na stránku, která poskytuje 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 produktů na adrese <http://forums.avg.com>.