AVG Internet Security 2013

Uživatelský manuál

Verze dokumentace 2013.10 (30.11.2012)

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

Tento produkt používá RSA Data Security, Inc. MD5 Message-Digest Algorithm, Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991.
Tento produkt obsahuje kód knihovny C-SaCzech, Copyright (c) 1996-2001 Jaromír Doleček (dolecek@ics.muni.cz).
Tento produkt používá kompresní knihovnu libbzip2, Copyright (c) 1996-2002 Julian R. Seward.
Tento produkt používá kompresní knihovnu zlib Copyright (C) 1995-1998 Jean-loup Gailly and Mark Adler.

Obsah

1. Úvod 5

2. Podmínky instalace AVG 6

2.1 Podporované operační systémy 6
2.2 Minimální / doporučené HW požadavky 6

3. Instalační proces AVG 7

3.1 Vítejte: Volba jazyka 7
3.2 Vítejte: Licenční ujednání 8
3.3 Aktivujte vaši licenci 9
3.4 Vyberte typ instalace 10
3.5 Uživatelské volby 12
3.6 Postup instalace 13
3.7 Instalace byla úspěšná 14

4. Po instalaci 15

4.1 Registrace produktu 15
4.2 Otevření uživatelského rozhraní 15
4.3 Spuštění testu celého počítače 15
4.4 Test virem Eicar 15
4.5 Výchozí konfigurace AVG 16

5. Uživatelské rozhraní AVG 17

5.1 Horní navigace 18
5.2 Informace o stavu zabezpečení 22
5.3 Přehled komponent 23
5.4 Moje aplikace 24
5.5 Zkratková tlačítka pro testování a aktualizaci 24
5.6 Ikona na systémové liště 25
5.7 Miniaplikace AVG 26
5.8 AVG Advisor 28
5.9 AVG Accelerator 28

6. Komponenty AVG 30

6.1 Počítač 30
6.2 Procházení webu 31
6.3 Identita 33
6.4 E-maily 34
6.5 Firewall 36

6.6 PC Analyzer 39

7. AVG Security Toolbar 41

8. AVG Do Not Track 43

8.1 Rozhraní služby AVG Do Not Track 43
8.2 Informace o sledovacích procesech 44
8.3 Blokování sledovacích procesů 45
8.4 Nastavení služby AVG Do Not Track 46

9. Nastavení Firewallu 48

9.1 Obecné 48
9.2 Aplikace 50
9.3 Sdílené souborů a tiskáren 51
9.4 Pokročilé nastavení 52
9.5 Definované sítě 53
9.6 Systémové služby 54
9.7 Protokoly 55

10. Pokročilé nastavení AVG 58

10.1 Vzhled 58
10.2 Zvuky 61
10.3 Dočasné vypnutí ochrany AVG 62
10.4 Ochrana počítače 63
10.5 Kontrola pošty 67
10.6 Ochrana procházení webu 82
10.7 Identity Protection 85
10.8 Testy 86
10.9 Naplánované úlohy 91
10.10 Aktualizace 100
10.11 Výjimky 104
10.12 Virový trezor 106
10.13 Vlastní ochrana AVG 107
10.14 Anonymní sběr dat 107
10.15 Ignorovat chybový stav 110
10.16 Advisor - známé sítě 111

11. AVG testování 112

11.1 Přednastavené testy 113
11.2 Testování v průzkumníku Windows 121
11.3 Testování z příkazové řádky 122

11.4 Naplánování testu 124
11.5 Výsledky testu 131
11.6 Podrobnosti výsledku testu 132

12. Virový trezor 134

13. Historie 136

13.1 Výsledky testů 136
13.2 Nálezy Rezidentního štítu 138
13.3 Nálezy Emailové ochrany 140
13.4 Nálezy Webového štítu 141
13.5 Protokol událostí 143
13.6 Protokol Firewallu 144

14. Aktualizace AVG 146

14.1 Spouštění aktualizace 146
14.2 Průběh aktualizace 146
14.3 Úrovně aktualizace 147

15. FAQ a technická podpora 148

1. Úvod

Tento uživatelský manuál je kompletní uživatelskou dokumentací programu **AVG Internet Security 2013**.

Aplikace **AVG Internet Security 2013** 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. Můžete bez obav nakupovat a používat internetové bankovnictví, pohybovat se v sociálních sítích, procházet Internet a vyhledávat potřebné informace.

2. Podmínky instalace AVG

2.1. Podporované operační systémy

AVG Internet Security 2013 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)
- Windows 8 (x32 a x64)

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

***Poznámka**: Komponenta Identita není podporována na Windows XP x64. Na tomto operačním systémm lze nainstalovat AVG Internet Security 2013, ale pouze bez této komponenty.*

2.2. Minimální / doporučené HW požadavky

Minimální hardwarové požadavky pro **AVG Internet Security 2013**:

- Procesor Intel Pentium 1,5 GHz nebo rychlejší
- 512 MB RAM paměti (Windows XP) / 1024 MB RAM paměti (Windows Vista, Windows 7)
- 1,3 GB volného místa na pevném disku (*z instalačních důvodů*)

Doporučené hardwarové požadavky pro **AVG Internet Security 2013**:

- Procesor Intel Pentium 1,8 GHz nebo rychlejší
- 512 MB RAM paměti (Windows XP) / 1024 MB RAM paměti (Windows Vista, Windows 7)
- 1,6 GB volného místa na pevném disku (*z instalačních důvodů)*

3. Instalační proces AVG

Pro instalaci **AVG Internet Security 2013** na váš počítač potřebujete aktuální instalační soubor. Abyste zajistili, že instalujete vždy nejnovější verzi **AVG Internet Security 2013**, je vhodné stáhnout si instalační soubor z webu AVG (http://www.avg.cz/). V sekci ***Podpora / Stažení*** najdete strukturovaný přehled instalačních souborů k jednotlivým edicím AVG.

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

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

3.1. Vítejte: Volba jazyka

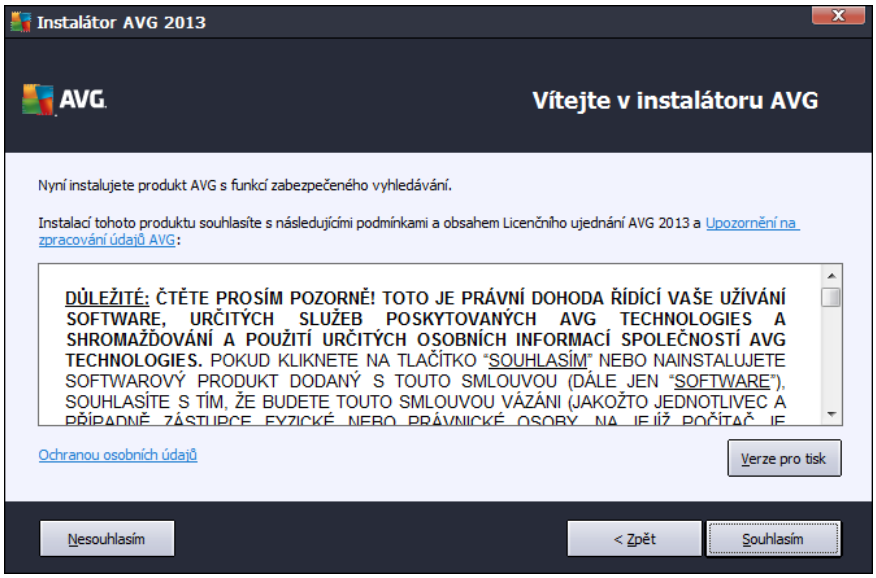
Instalační proces je zahájen otevřením dialogu ***Vítejte v instalátoru AVG***:

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

Pozor: V tuto chvíli volíte pouze jazyk instalačního procesu. Aplikace AVG Internet Security 2013 bude tedy nainstalována ve zvoleném jazyce a také v angličtině, která se instaluje automaticky. Je však možné nainstalovat ještě další volitelné jazyky, v nichž můžete aplikaci AVG zobrazit. Svůj výběr alternativních jazyků budete moci provést později během instalačního procesu, konkrétně v dialogu nazvaném *Uživatelské volby*.

3.2. Vítejte: Licenční ujednání

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



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

Ochrana osobních údajů AVG

Kromě licenčního ujednání se v tomto kroku instalace můžete také seznámit s ***Upozorněním na zpracování údajů AVG***, s funkcí ***AVG Personalizace*** a s politikou ochrany osobních údajů ***AVG Privacy Policy*** *(všechny zmiňované funkce jsou v dialogu zobrazeny formou aktivního odkazu na speciální webovou stránku, kde najdete podrobné informace)*. Kliknutím na příslušný odkaz budete přesměrováni na webovou stránku AVG (http://www.avg.cz/), která Vás v plném rozsahu seznámí s požadovaným prohlášením.

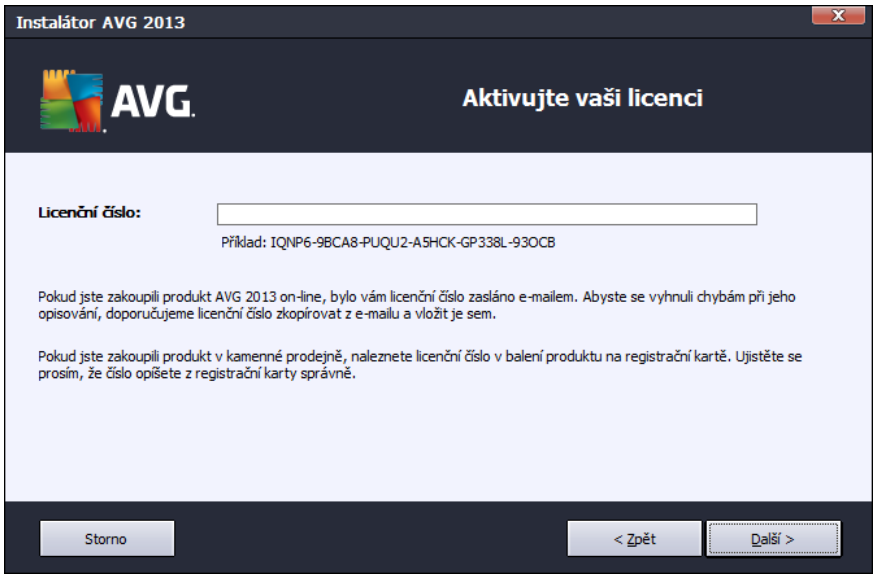
Ovládací tlačítka dialogu

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

- ***Verze pro tisk*** - Tímto tlačítkem máte možnost zobrazit plné znění licenční smlouvy ve webovém rozhraní v přehledném formátu pro tisk.
- ***Souhlasím*** - Kliknutím potvrzujete, že jste četli licenční ujednání a přijímáte jej v plném rozsahu. Instalace bude pokračovat přechodem do následujícího dialogu instalačního procesu.
- ***Nesouhlasím*** - Kliknutím odmítáte přijmout licenční ujednání. Instalační proces bude bezprostředně ukončen. **AVG Internet Security 2013** nebude nainstalován!
- ***Zpět*** - Kliknutím na tlačítko se vrátíte o jeden krok zpět do předchozího dialogu instalačního procesu.

3.3. Aktivujte vaši licenci

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



Kde najdu licenční číslo

Licenční číslo najdete buďto na registrační kartě v krabicovém balení **AVG Internet Security 2013**, anebo v potvrzovacím e-mailu, který jste obdrželi při zakoupení **AVG Internet Security 2013** on-line. Licenční číslo musí být zadáno naprosto přesně ve tvaru, jak je uvedeno, proto prosím věnujte velkou pozornost jeho přepisu. Pokud máte číslo k dispozici v digitální formě, doporučujeme jej do příslušného pole zkopírovat (*metodou kopírovat a vložit*).

Jak použít metodu Copy & Paste

Následující přehled kroků je stručným popisem toho, jak použít metodu ***Copy & Paste*** *(kopíruj a vlož)* při vkládání licenčního čísla **AVG Internet Security 2013**:

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

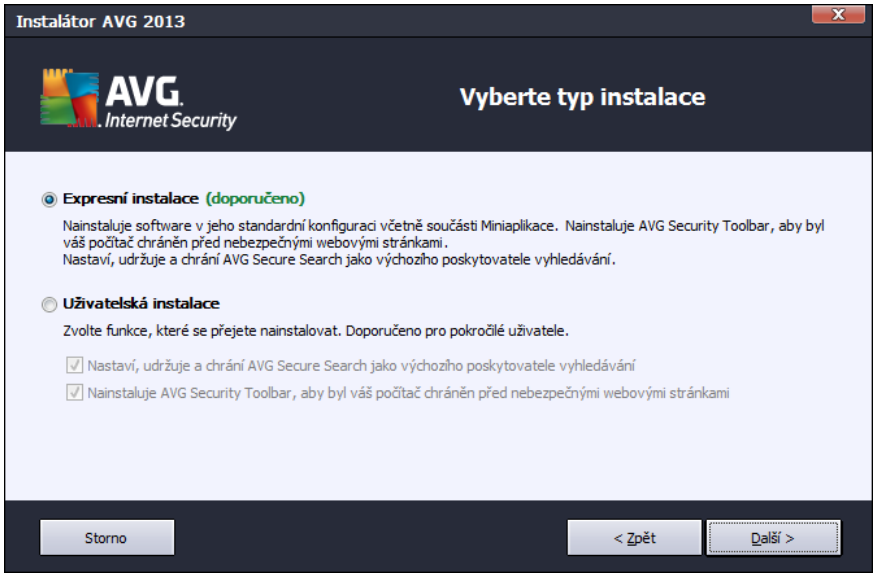
Ovládací tlačítka dialogu

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

- ***Storno*** - Kliknutím na toto tlačítko bezprostředně ukončíte instalační proces; **AVG Internet Security 2013** nebude nainstalován!
- ***Zpět*** - Kliknutím na tlačítko se vrátíte o jeden krok zpět do předchozího dialogu instalačního procesu.
- ***Další*** - Kliknutím na tlačítko pokračujete v instalačním procesu a přejdete do následujícího dialogu.

3.4. Vyberte typ instalace

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



Expresní instalace

Většině uživatelů doporučujeme použít expresní instalaci. Tak bude **AVG Internet Security 2013** nainstalován zcela automaticky s konfigurací definovanou výrobcem, a to včetně miniaplikace AVG, doplňku pro internetové prohlížeče AVG Security Toolbar a s nastavením služby AVG Secure Search jako výchozího poskytovatele vyhledávání. Výchozí nastavení zaručuje maximální úroveň bezpečnosti a optimální využití zdrojů. Pokud se v budoucnu vyskytne potřeba některé konkrétní nastavení změnit, budete mít vždy možnost editovat konfiguraci **AVG Internet Security 2013** přímo v aplikaci.

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

Uživatelská instalace

Uživatelská instalace je vhodná pouze pro pokročilé a znalé uživatele. Doporučit ji lze v případě, že máte skutečný důvod instalovat **AVG Internet Security 2013** s nestandardním nastavením tak, aby vyhovovalo specifickým požadavkům vašeho systému. V této sekci máte možnost zvolit si, zda mají být nainstalovány

následující funkce *(obě jsou ve výchozím nastavení označeny a určeny k instalaci, a pokud jejich označení nevypnete, budou automaticky nainstalovány)*:

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

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

Pokud se rozhodnete pro uživatelskou instalaci, zobrazí se nová sekce ***Cílové umístění***. Zde máte možnost určit, kam má být program **AVG Internet Security 2013** instalován. Ve výchozím nastavení bude program instalován do adresáře programových souborů umístěném typicky na disku C:, jak je uvedeno v textovém poli v tomto dialogu. Pokud si přejete toto umístění změnit, pomocí tlačítka ***Procházet*** zobrazte strukturu vašeho disku a zvolte požadovaný adresář. Chcete-li se následně vrátit k původnímu umístění definovanému výrobcem, můžete tak učinit pomocí tlačítka ***Výchozí***.

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

Ovládací tlačítka dialogu

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

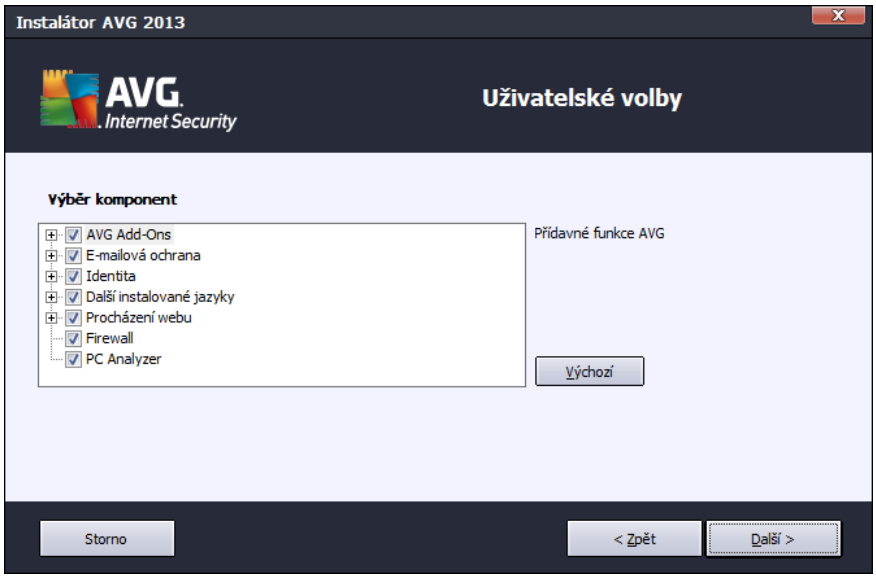
- ***Storno*** - Kliknutím na toto tlačítko bezprostředně ukončíte instalační proces; **AVG Internet Security 2013** nebude nainstalován!

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

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

3.5. Uživatelské volby

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



Sekce ***Výběr komponent*** nabízí přehled komponent **AVG Internet Security 2013**, které můžete nainstalovat. Pokud vám výchozí nastavení nevyhovuje, máte možnost jednotlivé komponenty odebrat/přidat.

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

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

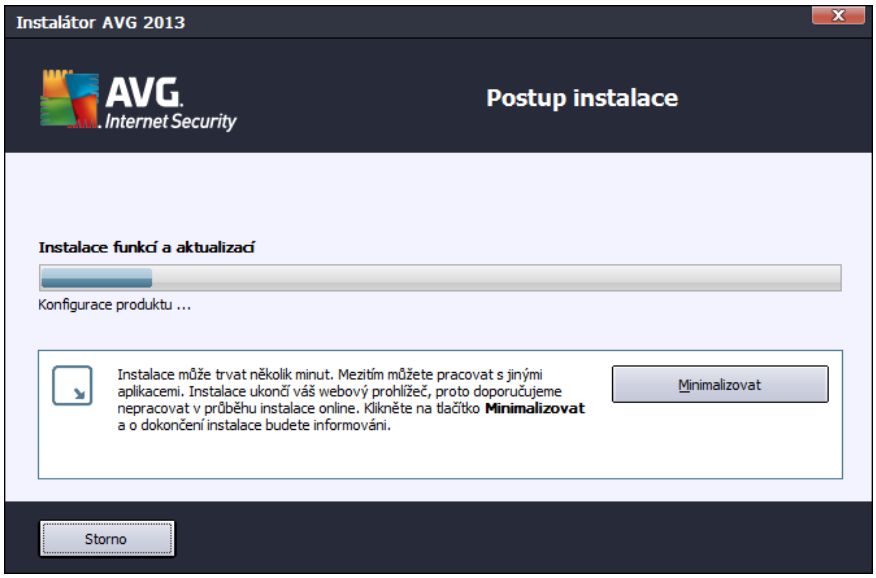
Ovládací tlačítka dialogu

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

- ***Storno*** - Kliknutím na toto tlačítko bezprostředně ukončíte instalační proces; **AVG Internet Security 2013** nebude nainstalován!
- ***Zpět*** - Kliknutím na tlačítko se vrátíte o jeden krok zpět do předchozího dialogu instalačního procesu.
- ***Další*** - Kliknutím na tlačítko pokračujete v instalačním procesu a přejdete do následujícího dialogu.

3.6. Postup instalace

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



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

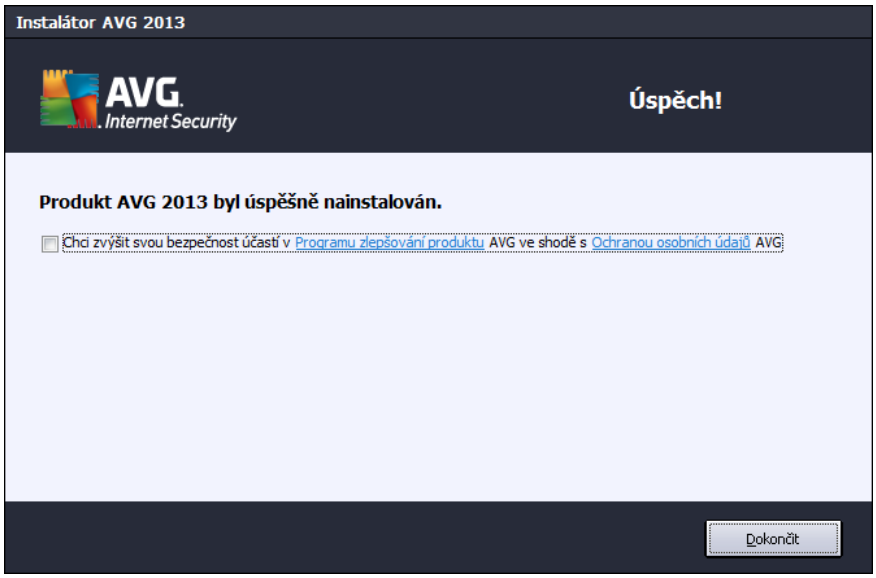
Ovládací tlačítka dialogu

V dialogu jsou dostupná dvě ovládací tlačítka:

- ***Minimalizovat*** - Instalace může trvat několik minut. Tlačítkem zmenšíte dialogové okno instalace pouze na ikonu na systémové liště. Dialog se opět otevře v plné velikosti, jakmile bude instalace dokončena.
- ***Storno*** - Toto tlačítko použijte výhradně tehdy, přejete-li si běžící instalační proces přerušit. V takovém případě nebude **AVG Internet Security 2013** nainstalován!

3.7. Instalace byla úspěšná

Dialog ***Instalace byla úspěšná*** potvrzuje, že **AVG Internet Security 2013** byl plně nainstalován a nastaven k optimálnímu výkonu:



Program zlepšování produktu a ochrana osobních údajů

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

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

4. Po instalaci

4.1. Registrace produktu

Po dokončení instalace **AVG Internet Security 2013** prosím zaregistrujte svůj produkt na webu AVG *(http://www.avg.cz/)*. Registrace vám umožní získat přístup k uživatelskému účtu AVG, dostávat informace o aktualizacích AVG, a zprostředkuje další služby poskytované registrovaným uživatelům AVG. Nejsnazší přístup k registraci je přímo z prostředí aplikace **AVG Internet Security 2013**, a to volbou položky Možnosti / Registrovat. Následně budete přesměrováni na stránku ***Registrace*** na webu AVG *(http://www.avg.cz/)*, kde dále postupujte podle uvedených instrukcí.

4.2. Otevření uživatelského rozhraní

Hlavní dialog AVG je dostupný několika cestami:

- dvojklikem na ikonu AVG na systémové liště
- dvojklikem na ikonu AVG na ploše
- z nabídky ***Start / Všechny programy / AVG / AVG 2013***

4.3. Spuštění testu celého počítače

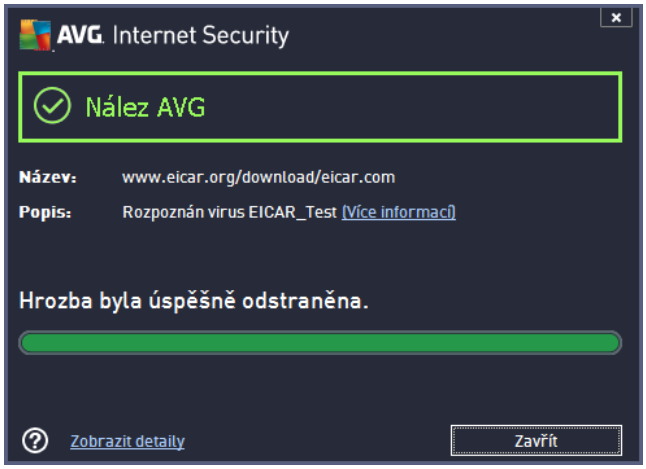
Jelikož existuje jisté riziko, že virus byl na váš počítač zavlečen již před instalací **AVG Internet Security 2013**, doporučujeme po instalaci spustit Test celého počítače, který zkontroluje celý počítač a ověří případnou přítomnost virů a potenciálně nežádoucích programů. První test počítače může trvat asi hodinu, ale z hlediska vaší bezpečnosti je skutečně nanejvýš důležité jej nechat proběhnout. Instrukce ke spuštění testu najdete v kapitole AVG testování.

4.4. Test virem Eicar

Chcete-li ověřit, že **AVG Internet Security 2013** byl správně nainstalován, proveďte test virem EICAR.

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

Stáhněte si soubor *eicar.com* a pokuste se jej uložit na lokální disk. Ihned poté, co potvrdíte stažení testovacího souboru, zareaguje **AVG Internet Security 2013** varovným upozorněním. Toto upozornění dokazuje, že **AVG Internet Security 2013** na vašem počítači je správně nainstalován:



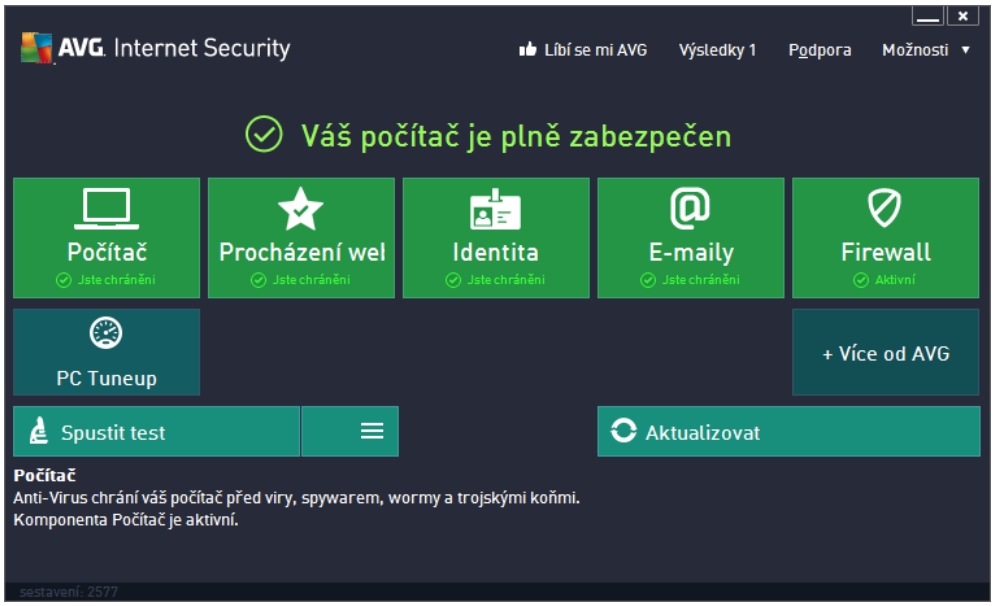
Pokud není testovací soubor EICAR identifikován jako virus, je nutné znovu prověřit konfiguraci AVG Internet Security 2013!

4.5. Výchozí konfigurace AVG

Ve výchozí konfiguraci (*bezprostředně po instalaci*) jsou všechny komponenty a funkce **AVG Internet Security 2013** nastaveny výrobcem k optimálnímu výkonu bezpečnostního software. ***Pokud nemáte skutečný důvod jejich konfiguraci měnit, doporučujeme ponechat program v tomto nastavení! Změnu konfigurace by měli provádět pouze zkušení uživatelé.*** Pokud se domníváte, že je nutné konfiguraci AVG přenastavit podle vašich aktuálních potřeb, proveďte editaci parametrů v Pokročilém nastavení AVG: zvolte položku hlavního menu *Možnosti / Pokročilé nastavení* a editaci nastavení proveďte v nově otevřeném dialogu Pokročilém nastavení AVG.

5. Uživatelské rozhraní AVG

AVG Internet Security 2013 se otevře v tomto rozhraní:



Hlavní okno je rozděleno do několika sekcí:

- ***Horní navigace*** sestává ze čtyř aktivních odkazů uvedených v linii v horní části hlavního okna *(Líbí se mi AVG, Výsledky, Podpora, Možnosti)*. Podrobnosti >>
- ***Informace o stavu zabezpečení*** podává základní informaci o aktuálním stavu **AVG Internet Security 2013**. Podrobnosti >>
- ***Přehled instalovaných komponent*** najdete ve vodorovném pásu ve střední části okna. Komponenty jsou znázorněny jako světle zelené bloky s ikonou příslušné komponenty a informací o jejím aktuálním stavu. Podrobnosti >>
- ***Moje aplikace*** jsou graficky znázorněny ve středním pásu hlavního okna a nabízejí přehled doplňkových aplikací **AVG Internet Security 2013**, které buďto již máte nainstalovány na svém počítači, nebo jejichž instalaci vám doporučujeme. Podrobnosti >>
- ***Zkratková tlačítka pro testování a aktualizaci*** ve spodní řadě hlavního okna umožňují rychlý přístup k nejdůležitějším a nejčastěji používaným funkcím **AVG Internet Security 2013**. Podrobnosti >>

Mimo hlavní okno **AVG Internet Security 2013** můžete k aplikaci přistupovat ještě prostřednictvím následujících dvou prvků:

- ***Ikona na systémové liště*** se nachází v pravém dolním rohu monitoru *(na systémové liště)* a je indikátorem aktuálního stavu **AVG Internet Security 2013**. Podrobnosti >>
- ***Miniaplikace AVG*** je dostupná volitelně z panelu Windows sidebar (*podporováno pouze v OS Windows Vista/7/8*) a umožňuje rychlý přístup k testování a aktualizaci programu. Podrobnosti >>

5.1. Horní navigace

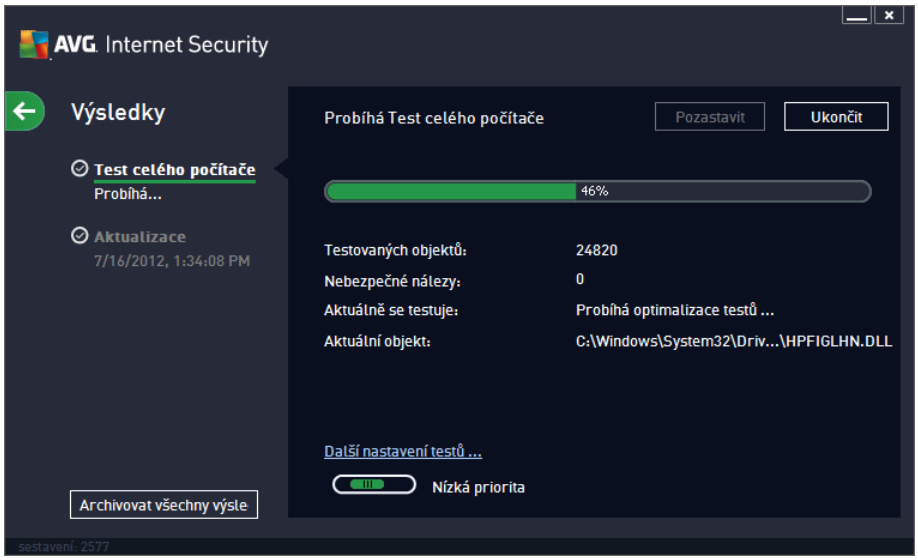
Horní navigace sestává z několika aktivních odkazů uvedených v linii v horní části hlavního okna. Obsahuje tato tlačítka:

5.1.1. Líbí se mi AVG

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

5.1.2. Výsledky

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

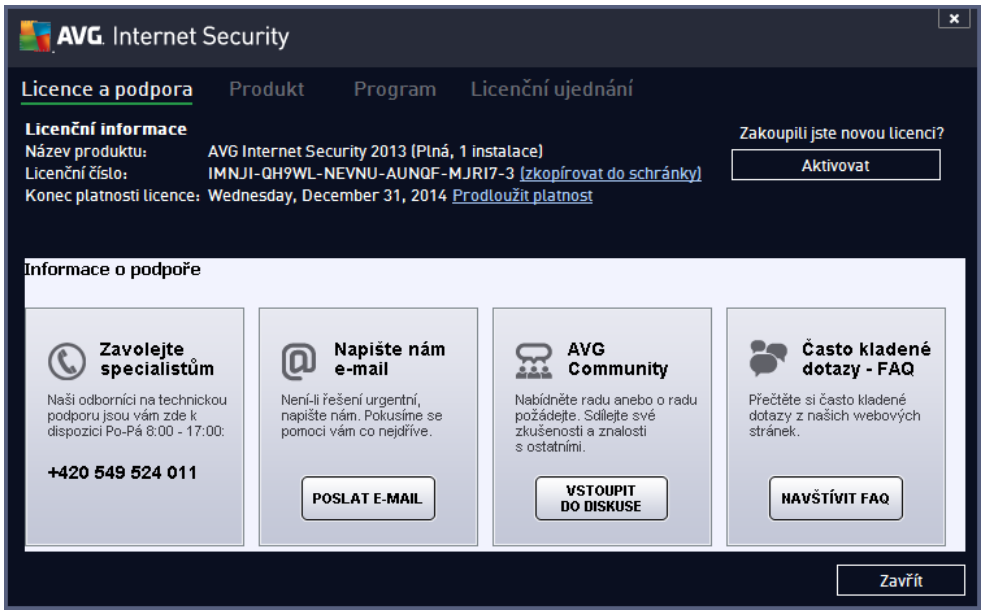


5.1.3. Podpora

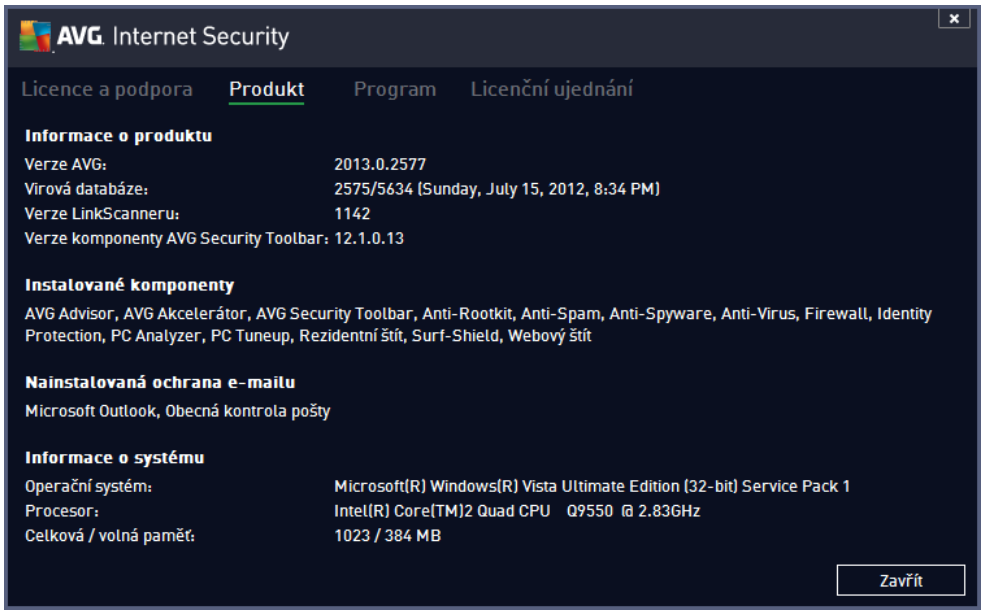
Odkaz otevírá smostaný dialog, v němž jsou na čtyřech záložkách shrnuty informace o **AVG Internet Security 2013** potřebné například při kontaktu se zákaznickou podporou:

- ***Licence a podpora*** - Záložka nabízí přehled licenčních informací, tedy název produktu, licenční číslo a konec platnosti licence. Ve spodní části dialogu je najdete také přehledný seznam všech dostupných kontaktů uživatelské podpory. V dialogu jsou k dispozici tyto ovládací prvky:
    - *(Re)Aktivovat* - Tlačítkem otevřete nový dialog ***AVG Aktivovat software***. Do tohoto dialogu zadejte své licenční číslo, kterým buďto nahradíte prodejní číslo *(s nímž jste AVG Internet Security 2013 instalovali)*, nebo kterým změníte dosavadní licenční číslo za jiné *(např. při přechodu na jiný produkt z řady AVG)*. Můžete rovněž zadat své osobní údaje *(jméno, název firmy)*.
    - *Zkopírovat do schránky* - Licenční číslo musí být zadáno naprosto přesně ve tvaru, jak je uvedeno. Proto je třeba věnovat mimořádnou pozornost jeho přepisu. Klinutím na odkaz ***Zkopírovat do schránky*** bude vaše licenční číslo uloženo do schánky a můžete jej prostým vložením použít kdekoliv potřebujete. Tím je zajištěno, že při jeho přepisu nedojde k chybě.

- *Prodloužit platnost* - Prodloužit platnost licence **AVG Internet Security 2013** je možné kdykoliv, nejlépe však aspoň jeden měsíc před datem expirace. Na blížíci se datum expitace budete upozorněni. Kliknutím na odkaz budete přesměrováni na stránku na webu AVG *(http://www.avg.cz/)*, kde najdete podrobné informace o aktuálním stavu vaší licence, datum expirace a nabídku možností prodloužení licence.

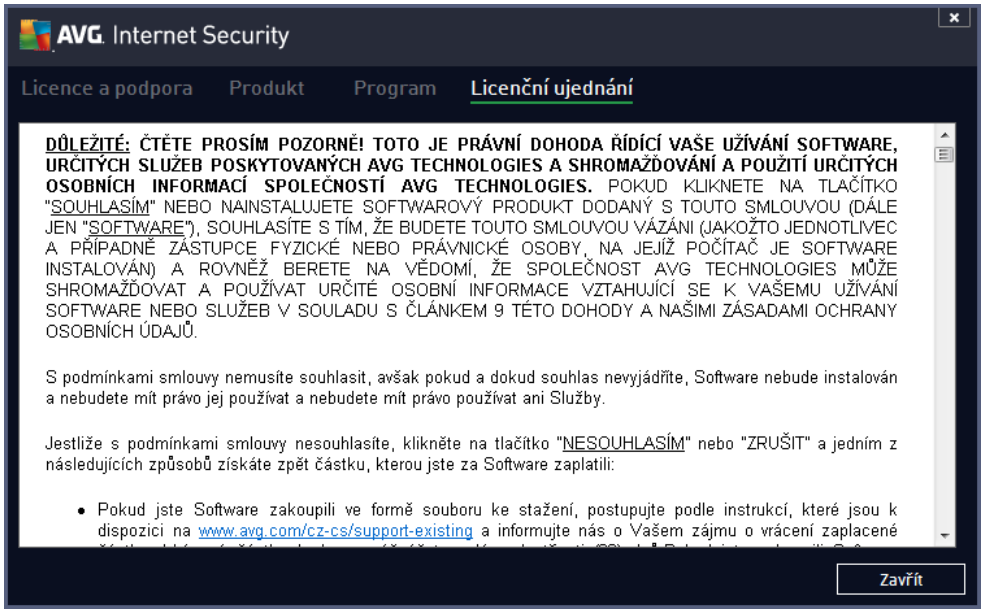


- ***Produkt*** - Záložka podává přehled nejdůležitějších technických informací o **AVG Internet Security 2013** rozdělených do sekcí informace o produktu, instalované komponenty, nainstalovaná ochrana e-mailu a informace o systému:



- ***Program*** - Záložka uvádí přesný název instalované edice **AVG Internet Security 2013** a číslo verze instalačního souboru. Dále jsou uvedeny informace o použitém kódu třetích stran:

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



5.1.4. Možnosti

Ovládání vašeho **AVG Internet Security 2013** je dostupné prostřednictvím jednotlivých možností sdružených v položce ***Možnosti***. Kliknutím na šipku vedle této položky otevřete rozbalovací menu s následující nabídkou:

- ***Otestovat počítač*** - Přímo spouští test celého počítače.
- ***Otestovat zvolený adresář...*** - Přepíná do testovacího rozhraní AVG a nabízí ve stromové struktuře vašeho disku možnost definovat ty složky, které mají být otestovány.
- ***Otestovat soubor...*** - Umožňuje spustit test na vyžádání pouze nad jedním konkrétním souborem.

Kliknutím na tuto volbu se otevře nové okno s náhledem stromové struktury vašeho disku. Zvolte požadovaný soubor a potvrďte spuštění testu.

- ***Aktualizovat*** - Automaticky spouští proces aktualizace **AVG Internet Security 2013**.
- ***Aktualizace z adresáře ...*** - Spustí proces aktualizace z aktualizačního souboru umístěného v definovaném adresáři na lokálním disku. Tuto alternativu doporučujeme pouze jako náhradní řešení pro případ, že v danou chvíli nebude k dispozici připojení k Internetu *(např. počítač je zavirovaný a odpojený ze sítě, počítač je připojen k síti, kde není přístup k Internetu, apod.)*. V nově otevřeném okně vyberte adresář, do nějž jste předem umístili aktualizační soubory, a spusťte aktualizaci.
- ***Virový trezor*** - Otevírá rozhraní karanténního prostoru, Virového trezoru, kam jsou přesouvány detekované infekční soubory, 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.
- ***Historie*** se dělí na další specifické podkategorie:
  - *Výsledky testů* - Přepíná do testovacího rozhraní AVG, konkrétně do dialogu s přehledem výsledků testů.
  - *Nálezy Rezidentního štítu* - Otevírá dialog s přehledem infekcí detekovaných Rezidentním štítem.
  - *Nálezy Emailové ochrany* - Otevírá dialog s přehledem příloh detekovaných jako nebezpečné komponentou Emailová ochrana.
  - *Nálezy Webového štítu* - Otevírá dialog s přehledem infekcí detekovaných Webovým štítem.
  - *Protokol událostí* - Otevírá dialog historie událostí s přehledem všech protokolovaných akcí **AVG Internet Security 2013**.
  - *Protokol Firewallu* - Otevírá dialog se záznamem o všech akcích Firewallu.
- ***Pokročilé nastavení ...*** - Otevírá dialog pokročilého nastavení AVG, kde máte možnost editovat konfiguraci **AVG Internet Security 2013**. Obecně doporučujeme dodržet výchozí výrobcem definované nastavení aplikace.
- ***Nastavení Firewallu ...*** - Otevírá samostatný dialog pro pokročilou konfiguraci komponenty Firewall.
- ***Obsah nápovědy*** - 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.
- ***(Re)Aktivovat*** - Otevírá dialog ***Aktivace AVG***, v němž jsou již předem vyplněna data, jež jste zadali během instalačního procesu. V dialogu ***Aktivace AVG*** můžete zadat své licenční číslo, kterým buďto nahradíte prodejní číslo, s nímž jste AVG instalovali, nebo kterým změníte dosavadní licenční číslo za jiné, např. při přechodu na jiný produkt z řady AVG. Máte-li nainstalovanou zkušební verzi **AVG**

Internet Security 2013, dvě posledně uvedené položky se zobrazí jako ***Zakoupit*** a ***Aktivovat*** a odkáží Vás na web AVG, kde si můžete přímo zakoupit plnou verzi programu. Pokud máte nainstalovaný program **AVG Internet Security 2013** s prodejním číslem, položky se zobrazí jako ***Zaregistrovat*** a ***Aktivovat***.

- ***Registrovat / Můj účet*** - 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.

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

5.2. Informace o stavu zabezpečení

Sekce ***Informace o stavu zabezpečení*** je umístěna v horní části rozhraní **AVG Internet Security 2013**. V této sekci najdete vždy informaci o aktuálním stavu vašeho **AVG Internet Security 2013**. V sekci může být zobrazena jedna z následujících ikon, jejichž význam vysvětlujeme:

- Zelená ikona informuje, že ***program AVG Internet Security 2013 na vašem počítači je plně funkční***, aktualizován a všechny instalované komponenty pracují správně. Jste zcela chráněni.

- Žlutá ikona informuje o stavu, kdy ***jedna (nebo více) komponent není správně nastavena***. Nejedná se o kritický problém, pravděpodobně jste se sami rozhodli některou komponentu deaktivovat. V každém případě jste stále chráněni. Přesto prosím věnujte pozornost konfiguraci komponenty, která není nastavena k plné aktivitě! Tato komponenta bude v základním uživatelském rozhraní zobrazena s varovným oranžovým pruhem.

Žlutá ikona se zobrazí rovněž v případě, kdy jste se z nějakého důvodu vědomě rozhodli ignorovat chybový stav komponenty. Volba ***Ignorovat chybový stav*** je dostupná volbou větve Ignorovat chybový stav v Pokročilém nastavení. Touto volbou dáváte najevo, že jste si vědomi faktu, že se konkrétní komponenta nachází v chybovém stavu, ale z nějakého důvodu si přejete tento stav zachovat a nebýt na něj upozorňováni. Může nastat situace, kdy budete potřebovat využít této možnosti, ale rozhodně nedoporučujeme, abyste v tomto stavu setrvávali déle, než je nutné!

Alternativně bude žlutá ikona zobrazena také v situaci, kdy **AVG Internet Security 2013** vyžaduje restart počítače (***Restartovat nyní***). Věnujte prosím pozornost tomuto varování a počítač restartujte!

- Oranžová ikona ***informuje o kritickém stavu AVG Internet Security 2013!*** Některá z komponent je nefunkční a **AVG Internet Security 2013** nemůže plně chránit váš počítač. Věnujte prosím okamžitou pozornost opravě tohoto problému! Pokud nebudete sami schopni problém odstranit, kontaktujte oddělení technické podpory AVG.

V případě, kdy AVG Internet Security 2013 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 2013 automaticky spustí proces kontroly a přenastavení všech parametrů k optimálnímu výkonu. Tímto tlačítkem snadno uvedete program do optimálního stavu a zajistíte tak nejvyšší úroveň bezpečnosti!

Důrazně doporučujeme, abyste věnovali pozornost údajům zobrazeným v sekci ***Informace o stavu zabezpečení*** a pokud **AVG Internet Security 2013** hlásí jakýkoliv problém, zaměřte se na jeho řešení. Pokud ignorujete chybová hlášení **AVG Internet Security 2013**, váš počítač je ohrožen!

Poznámka: *Informaci o stavu AVG Internet Security 2013 lze v kterémkoliv okamžiku práce na počítači získat také pohledem na ikonu na systémové liště.*

5.3. Přehled komponent

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

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

Seznam instalovaných komponent

V rámci **AVG Internet Security 2013** najdete v sekci ***Přehled komponent*** informace o těchto komponentách:

- ***Počítač*** - Komponenta zahrnuje dva ochranné procesy: ***AntiVirus Shield*** detekuje na vašem počítači viry, spyware, červy, trojany, nežádoucí spustitelné soubory nebo kniovny a chrání vás před nimi; ***Anti-Rootkit*** testuje všechny aplikace, ovladače a knihovny na přítomnost skrytých rootkitů. Podrobnosti >>
- ***Procházení webu*** - Chrání vás před webovými útoky v době, kdy surfujete na Internetu. Podrobnosti >>
- ***Identita*** - Tato komponenta prostřednictvím služby ***Identity Shield*** nepřetržitě chrání vaše digitální data před novými a neznámými hrozbami na Internetu. Podrobnosti >>
- ***Emaily*** - 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 >>

Dostupné akce

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

5.4. Moje aplikace

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

- ***Mobile protection*** nabízí zabezpečení Vašeho mobilního telefonu *(smart phone)* proti virům a malware. Zároveň slouží jako ochrana proti zneužití Vašich osobních dat, pokud telefon ztratíte nebo Vám bude odcizen.

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

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

- ***PC Tuneup*** je pokročilým nástrojem pro detailní systémovou analýzu a optimalizaci, umožňující zrychlit a vylepšit výkon vašeho počítače.

- ***MulitMi*** sdružuje Vaše účty a sítě, spojuje Vás s přáteli a rodinou, dovoluje prohlížet internet, sdílet obrázky, videa a soubory jednoduchým přetažením. MultiMi také obsahuje službu LinkScanner Safe Surf, který automaticky a v reálném čase ověřuje odkazy sdílené na sociálních sítích.

- ***AVG Toolbar*** je dostupný v podobě nástrojové lišty ve vašem internetovém prohlížeči a zajišťuje Vaši maximální bezpečnost při veškerém pohybu online.

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

5.5. Zkratková tlačítka pro testování a aktualizaci

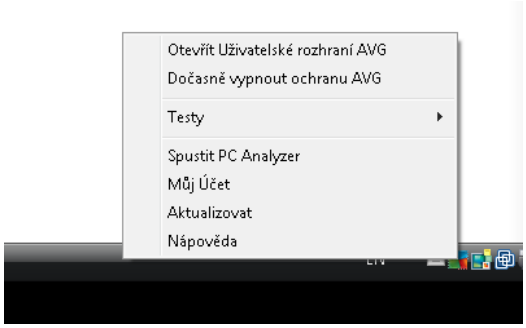
Zkratková tlačítka pro testování a aktualizaci najdete ve spodním pásu hlavního dialogu **AVG Internet Security 2013**. Tato tlačítka umožňují rychlý přístup k nejdůležitějším a nejčastěji používaným funkcím aplikace, tedy k zejména k testování a aktualizacím:

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

- ***Aktualizovat*** - Stiskem tlačítka se automaticky spustí aktualizace produktu, o jejímž průběhu a výsledku budete vyrozuměni v automaticky otevřeném okně Výsledky. *(Podrobné informace o procesu aktualizace najdete v kapitole Aktualizace AVG)*

5.6. Ikona na systémové liště

Ikona AVG na systémové liště *(zobrazena na panelu Windows vpravo dole na monitoru)* ukazuje aktuální stav **AVG Internet Security 2013**. Ikona je viditelná v každém okamžiku vaší práce na počítači, bez ohledu na to, zda máte či nemáte otevřeno uživatelské rozhraní aplikace:



Zobrazení systémové ikony AVG

Ikona může být zobrazena v několika variantách:

- Jestliže je ikona zobrazena barevně bez dalších prvků, jsou všechny komponenty **AVG Internet Security 2013** aktivní a plně funkční. Toto zobrazení ale také označuje situaci, kdy některá z komponent není v plně funkčním stavu, ale uživatel se rozhodl Ignorovat chybový stav. *(Volbou Ignorovat chybový stav dáváte najevo, že jste si vědomi faktu, že se ta která komponenta nachází v chybovém stavu, ale z nějakého důvodu si přejete tento stav zachovat a nebýt na něj upozorňováni.)*

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

- Ikona na systémové liště může být také zobrazena barevně s probleskujícím otáčejícím se paprskem. Toto grafické znázornění signalizuje právě probíhající aktualizaci **AVG Internet Security 2013**.

- Alternativní zobrazení ikony s šipkou znamená, že právě běží některý z testů **AVG Internet Security 2013**.

Informace systémové ikony AVG

Ikona AVG na systémové liště dále poskytuje informace o aktuálním dění v programu **AVG Internet Security 2013**. Při změně stavu **AVG Internet Security 2013** (*automatické spuštění naplánované aktualizace nebo testu, přepnutí 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 2013**, 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 2013**.
- ***Dočasně vypnout ochranu AVG*** - Položka umožňujě jednorázově deaktivovat celou ochranu zajištěnou programem **AVG Internet Security 2013**. Mějte prosím na paměti, že tato volba by v žádném případě neměla být použita, pokud to není opravdu nezbytně nutné! V naprosté většině případů není nutné deaktivovat **AVG Internet Security 2013** před instalací nového software nebo ovladačů, a to ani tehdy, pokud budete během instalace vyzvání k zavření všech spuštěných aplikací. Jestliže budete opravdu nuceni deaktivovat **AVG Internet Security 2013**, zapněte jej hned, jakmile to bude možné. Pamatujte, že pokud jste připojeni k Internetu nebo k jiné síti, je váš počítač bez aktivní ochrany vysoce zranitelný.
- ***Testy*** - Otevře vysunovací nabídku přednastavených testů (Test celého počítače a Test vybraných souborů či složek) a následnou volbou požadovaný test přímo spustíte.
- ***Běžící testy ...*** - Tato položka se zobrazuje pouze tehdy, je-li aktuálně spuštěn některý test. U tohoto běžícího testu pak můžete nastavit jeho prioritu, případně test pozastavit nebo ukončit. K dispozici jsou dále možnosti *Nastavit prioritu pro všechny testy*, *Pozastavit všechny testy* a *Zastavit všechny testy*.
- ***Spustit PC Analyzer*** - Spustí funkci komponenty PC Analyzer.
- ***Můj účet*** - Otevírá domovskou stránku Můj účet, kde můžete spravovat předplacené produkty, obnovit platnost AVG licence, zakoupit doplňující produkty, stáhnout instalační soubory, zkontrolovat uskutečněné objednávky a vystavené faktury či spravovat osobní udaje.
- ***Aktualizovat*** - Spustí okamžitou aktualizaci **AVG Internet Security 2013**.
- ***Nápověda*** - Otevře soubor nápovědy na úvodní stránce.

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 2013**, a to testování a aktualizace:

Ovládací prvky miniaplikace

Miniaplikace AVG Vám v případě potřeby umožňuje okamžitě spustit test nebo aktualizaci; nabízí zkratková tlačítka, jejichž pomocí se spojíte s AVG komunitou v nejrozšířenějších sociálních sítích *(Twitter, Facebook a LinkedIn)* a zprostředkuje vyhledávání ve vašem obvyklém vyhledavači:

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

- ***Aktualizovat*** - Kliknutím na volbu ***Aktualizovat*** spustíte proces aktualizace **AVG Internet Security 2013** přímo z prostředí minaplikace:

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

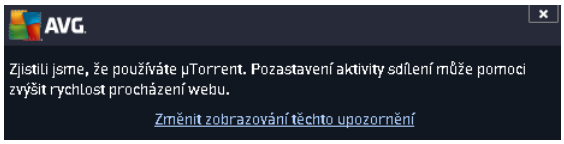
- ***Facebook*** - Otevírá internetový prohlížeč na webu sociální sítě Facebook, konkrétně na stránce ***AVG komunity***.

- ***Vyhledávání*** - Zadejte klíčové slovo a výsledky vyhledávání se zobrazí v nově otevřeném okně prohlížeče, který obvykle používáte.

5.8. AVG Advisor

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

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



AVG Advisor monitoruje tyto konkrétní situace:

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

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

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

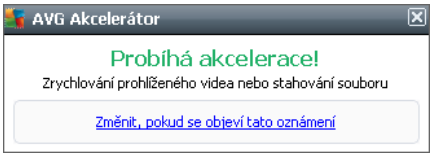
V každé z těchto situací Vás ***AVG Advisor*** varuje před možným konfliktem a zobrazí jméno a ikonu problematického procesu či aplikace. Dále pak navrhne jednoduché řešení, kterým lze problému předejít.

Podporované webové prohlížeče

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

5.9. AVG Accelerator

AVG Accelerator umožňuje plynulé přehrávání videa v režimu online a obecně urychluje stahování. O tom, že je proces akcelerace videa či stahování momentálně aktivní, budete informováni prostřednictvím pop-up okna nad systémovou lištou:


AVG Akcelerátor
Probíhá akcelerace!
Zrychlování prohlíženého videa nebo stahování souboru
Změnit, pokud se objeví tato oznámení

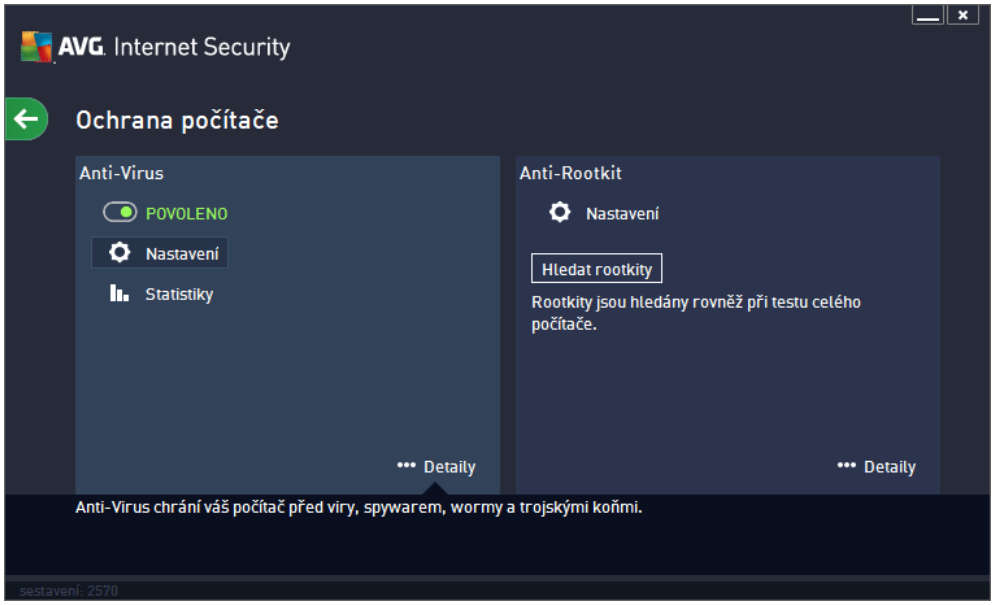
6. Komponenty AVG

6.1. Počítač

Komponenta ***Ochrana počítače*** zahrnuje dvě bezpečnostní služby: ***AntiVirus*** a ***Anti-Rootkit***.

- ***AntiVirus*** je tvořen jádrem, které testuje všechny soubory a jejich aktivitu, systémové oblasti počítače i vyměnitelná média *(flash disky apod.)* a prověřuje případnou přítomnost známých virů. Pokud detekuje virus, okamžitě zabrání, aby mohl být aktivován a následně jej odstraní nebo přesune do Virového trezoru. Tento proces bez ustání probíhá na pozadí a vy jej v podstatě nezaznamenáte - mluvíme o tak zvané rezidentní ochraně. AntiVirus také používá metodu heuristické analýzy, kdy jsou soubory testovány na přítomnost typických virových charakteristik. To znamená, že antivirový skener dokáže rozpoznat i nový, dosud neznámý virus podle toho, že tento virus nese určité znaky typické pro již existující viry. **AVG Internet Security 2013** umí také analyzovat spustitelné programy, případně DLL knihovny a určit, které z nich by mohly být potenciálně nežádoucí *(jako například spyware, adware aj.)*. Na žádost uživatele umožní tyto programy odstranit či k nim zablokovat přístup.

- ***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. Rootkit je program speciálně vytvořený tak, aby dokázal převzít kontrolu nad vaším počítačem, aniž by požádal o jakoukoliv autorizaci. Anti-Rootkit je schopen detekovat rootkit na základě definovaných pravidel. Dojde-li tedy k nálezu rootkitu, nemusí to nutně znamenat, že je počítač infikovaný. V některých případech mohou být rootkity použity jako ovladače nebo části korektních aplikací.



Ovládací prvky dialogu

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

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

Nastavení - Kliknutím na tlačítko přejdete do rozhraní pro pokročilé nastavení programu **AVG Internet Security 2013**. Přesněji řečeno, budete nasměrováni do dialogu, v němž lze provést veškerou konfiguraci zvolené služby, v tomto případě služby AntiVirus nebo Anti-Rootkit. V prokročilém nastavení můžete editovat veškeré parametry jednotlivých bezpečnostních služeb **AVG Internet Security 2013**, ale jakoukoliv konfiguraci doporučujeme pouze znalým uživatelům!

Statistiky - Kliknutím na tlačítko budete přesměrováni na speciální dedikovanou stránku na webu AVG (http://www.avg.cz/). Na této stránce najdete detailní statistický přehled všech aktivit **AVG Internet Security 2013**, které proběhly na vašem počítači za určený časový úsek i celkově od okamžiku instalace programu.

Detaily - Kliknutím na tlačítko se ve spodní části dialogu zobrazí stručný popis služby, jež je aktuálně zvolena.

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

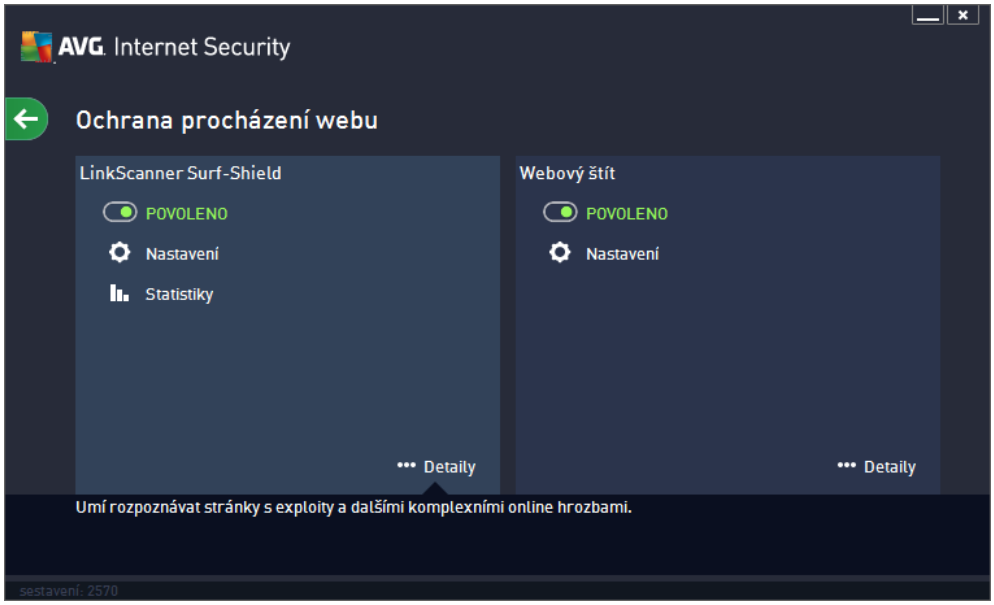
V sekci Anti-Rootkit je dále dostupné ještě tlačítko ***Hledat rootkity***, které slouží ke spuštění samostatného testu na přítomnost rootkitů *(testování přítomnosti rootkitů je však i implicitní součástí Testu celého počítače)*.

6.2. Procházení webu

Komponenta ***Ochrana procházení webu*** obsahuje dvě služby: ***LinkScanner Surf-Shield*** a ***Webový štít***.

- ***LinkScanner Surf-Shield*** zajišťuje ochranu před stále rostoucím počtem přechodných internetových hrozeb. Tyto hrozby mohou být skryty na jakékoliv webové stránce: od stránek vládních organizací až po stránky malých firem. Pouze zřídka se vyskytují déle než 24 hodin. Technologie LinkScanner Surf-Shield prověřuje obsah internetových stránek a zajišťuje, že jsou stránky bezpečné v okamžiku, kdy je to nejdůležitější, tedy když se chystáte otevřít adresu URL. Link Scanner 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, Link Scanner Surf-Shield přístup k této stránce okamžitě zablokuje. Mějte na paměti, že váš počítač se může velmi snadno poškodit při pouhé návštěvě infikované webové stránky. ***LinkScanner Surf-Shield není určen k ochraně serverů!***

- ***Webový štít*** je typ rezidentní ochrany, která běží na pozadí a v reálném čase kontroluje obsah webových stránek nebo souborů stahovaných z Internetu. Každá stránka je prověřena ještě předtím, než je skutečně stažena a zobrazena webovým prohlížečem. Webový štít detekuje, že stránka, kterou se chystáte navštívit, obsahuje nebezpečný javascript, a v takovém případě nebude infikovaná stránka vůbec zobrazena. Také rozpozná, že stránka obsahuje malware, který by mohl být prohlížením stránky zavlečen na váš počítač, a zabrání jeho stažení. ***Webový štít není určen k ochraně serverů!***



Ovládací prvky dialogu

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

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

Nastavení - Kliknutím na tlačítko přejdete do rozhraní pro pokročilé nastavení programu **AVG Internet Security 2013**. Přesněji řečeno, budete nasměrováni do dialogu, v němž lze provést veškerou konfiguraci zvolené služby, v tomto případě služby LinkScanner Surf-Shield nebo Webový štít. V prokročilém nastavení můžete editovat veškeré parametry jednotlivých bezpečnostních služeb **AVG Internet Security 2013**, ale jakoukoliv konfiguraci doporučujeme pouze znalým uživatelům!

Statistiky - Kliknutím na tlačítko budete přesměrováni na speciální dedikovanou stránku na webu AVG (http://www.avg.cz/). Na této stránce najdete detailní statistický přehled všech aktivit **AVG Internet Security 2013**, které proběhly na vašem počítači za určený časový úsek i celkově od okamžiku instalace programu.

Detaily - Kliknutím na tlačítko se ve spodní části dialogu zobrazí stručný popis služby, jež je aktuálně zvolena.

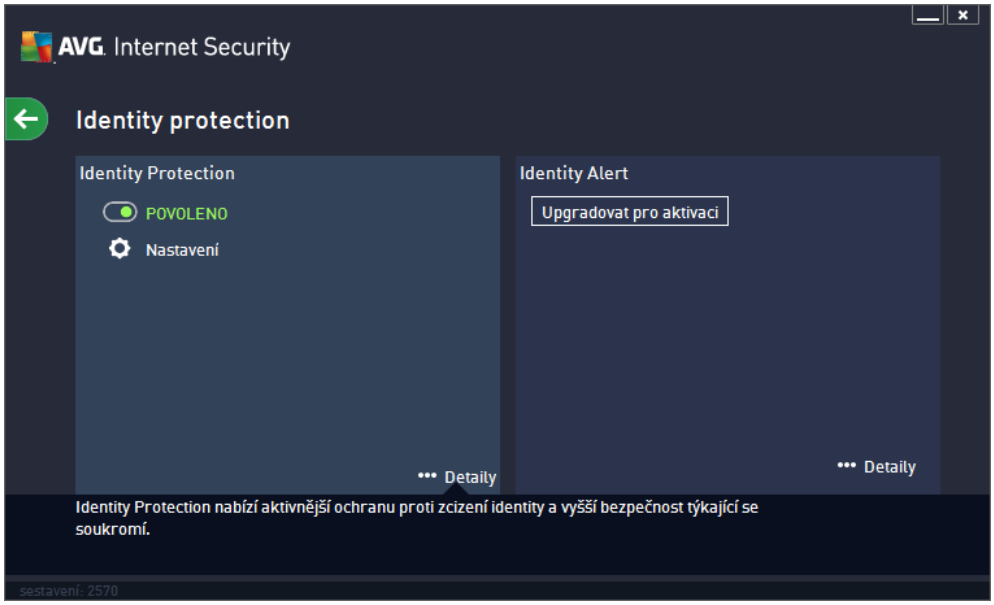
- Pomocí šipky v levé horní části dialogu se vrátíte zpět do základního uživatelského rozhraní s

přehledem komponent.

6.3. Identita

Komponenta ***Identity protection*** prostřednictvím služby ***Identity Shield*** nepřetržitě chrání vaše digitální data před novými a neznámými hrozbami na Internetu.

Identity Protection je komponentou, která průběžně a v reálném čase zajišťuje ochranu před různými druhy malware a virů, a to na bázi identifikace specifického chování těchto typů aplikací. Identity Protection zajišťuje bezpečnost při nákupech, bankovních operacích a jiných elektronických transakcích. Slouží k detekci malware a je zaměřena na prevenci zcizení osobních dat *(přístupová hesla, bankovní účty, čísla kreditních karet, ...)* a cenných informací prostřednictvím škodlivého software (malware), který útočí na váš počítač. Identity Protection zajistí, že všechny programy běžící na vašem počítači nebo ve vaší síti pracují správně. Identity Protection rozpozná jakékoliv podezřelé chování a škodlivý program zablokuje. Identity Protection zajišťuje v reálném čase ochranu vašeho počítače proti novým a dosud neznámým hrozbám. Monitoruje všechny *(i skryté)* procesy a více než 285 různých vzorců chování, takže dokáže rozpoznat potenciálně nebezpečné chování v rámci vašeho systému. Díky této schopnosti umí Identity Protection detekovat hrozby, které ještě ani nejsou popsány ve virové databázi. Jakmile se neznámý kus kódu dostane do vašeho počítače, Identity Protection jej sleduje, pozoruje a zaznamenává případné příznaky škodlivého chování. Jestliže je soubor shledán škodlivým, Identity Protection jej přemístí do Virového trezoru a vrátí zpět do původního stavu veškeré změny systému provedené tímto kódem *(vložené kusy kódu, změny v registrech, otevřené porty apod.)*. Identity Protection vás chrání, aniž byste museli spouštět jakýkoliv test. Tato technologie je vysoce proaktivní, aktualizaci vyžaduje jen zřídka a trvale hlídá vaše bezpečí.



Ovládací prvky dialogu

V dialogu se můžete setkat s několika ovládacími prvky:

Povoleno / Zakázáno - Tlačítko svým vzhledem i chováním připomíná semafor. Jednoduchým kliknutím se dá přepínat mezi dvěma polohami. Zelená barva odpovídá stavu ***Povoleno***, který znamená, že bezpečnostní služba Identity Protection je aktivní a plně funkční. Červená barva pak odpovídá stavu ***Zakázáno***, kdy je služby vypnuta. Pokud nemáte skutečný důvod službu vypínat, doporučujeme,

abyste veškerou bezpečnostní konfiguraci ponechali ve výchozím stavu. Výchozí nastavení zajišťuje optimální výkon programu a vaši maximální bezpečnost. Jestliže z nějakého důvodu chcete službu dočasně vypnout, budete okamžitě upozorněni na možné nebezpečí červeným nápisem ***Varování*** a informací o skutečnosti, že v tuto chvíli nejste plně chráněni. ***Jakmile to bude možné, službu opět aktivujte!***

Nastavení - Kliknutím na tlačítko přejdete do rozhraní pro pokročilé nastavení programu **AVG Internet Security 2013**. Přesněji řečeno, budete nasměrováni do dialogu, v němž lze provést veškerou konfiguraci zvolené služby, v tomto případě služby Identity Protection. V prokročilém nastavení můžete editovat veškeré parametry jednotlivých bezpečnostních služeb **AVG Internet Security 2013**, ale jakoukoliv konfiguraci doporučujeme pouze znalým uživatelům!

Detaily - Kliknutím na tlačítko se ve spodní části dialogu zobrazí stručný popis služby, jež je aktuálně zvolena.

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

6.4. E-maily

Komponenta ***Emailová ochrana*** zahrnuje tyto dvě bezpečnostní služby: ***Kontrola pošty*** a ***Anti-Spam***.

- ***Kontrola pošty***: Jedním z nejčastějších zdrojů virů a trojských koní je e-mail. A díky phishingu a spamu se e-mail stává ještě větším zdrojem nebezpečí. Toto nebezpečí narůstá obzvláště u zdarma dostupných poštovních účtů (*protože u těch je použití anti-spamové technologie spíše výjimkou*), které stále používá většina domácích uživatelů. Tito uživatelé také často navštěvují neznámé webové stránky a nezřídka zadávají svá osobní data (*nejčastěji svou e-mailovou adresu*) do různých formulářů na webu, čímž ještě zvyšují riziko napadení prostřednictvím elektronické pošty. Větší společnosti většinou používají firemní poštovní účty a snaží se riziko minimalizovat implementací anti-spamových filtrů. Služba Kontrola pošty zodpovídá za testování veškeré příchozí i odchozí pošty. Pokud je v e-mailové zprávě detekován virus, je okamžitě přemístěn do Virového trezoru. Komponenta umí také odfiltrovat určité typy e-mailových příloh a označovat prověřené e-mailové zprávy certifikačním textem. ***Kontrola pošty není určena k ochraně poštovních serverů!***

- ***Anti-Spam*** kontroluje veškerou příchozí poštu a nežádoucí zprávy označuje jako spam *(Termínem spam označujeme nevyžádanou elektronickou poštu, převážně reklamního charakteru, jež je jednorázově hromadně rozesílána obrovskému počtu adresátů, čímž zahlcuje jejich poštovní schránky. Termín spam se nevztahuje na oprávněný e-mail komerčního charakteru, k jehož přijetí dal zákazník svůj souhlas.)*. Anti-Spam dokáže upravit předmět e-mailu, který je identifikován jako spam, přidáním vámi definovaného textového řetězce. Poté již můžete snadno filtrovat e-maily podle definovaného označení ve vašem poštovním klientovi. K detekci spamu v jednotlivých zprávách používá Anti-Spam několika analytických metod a zaručuje tedy maximální úroveň ochrany proti nevyžádané poště. Anti-Spam pracuje s pravidelně aktualizovanou databází a lze nastavit i kontrolu pomocí RBL serverů *(veřejných seznamů "nebezpečných" e-mailových adres)* nebo ručně přidávat povolené *(Whitelist)* a zakázané *(Blacklist)* poštovní adresy.

Ovládací prvky dialogu

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

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

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

Nastavení - Kliknutím na tlačítko přejdete do rozhraní pro pokročilé nastavení programu **AVG Internet Security 2013**. Přesněji řečeno, budete nasměrováni do dialogu, v němž lze provést veškerou konfiguraci zvolené služby, v tomto případě služby Kontrola pošty nebo Anti-Spam. V prokročilém nastavení můžete editovat veškeré parametry jednotlivých bezpečnostních služeb **AVG Internet Security 2013**, ale jakoukoliv konfiguraci doporučujeme pouze znalým uživatelům!

Statistiky - Kliknutím na tlačítko budete přesměrováni na speciální dedikovanou stránku na webu AVG (http://www.avg.cz/). Na této stránce najdete detailní statistický přehled všech aktivit **AVG Internet Security 2013**, které proběhly na vašem počítači za určený časový úsek i celkově od okamžiku instalace programu.

Detaily - Kliknutím na tlačítko se ve spodní části dialogu zobrazí stručný popis služby, jež je

aktuálně zvolena.

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

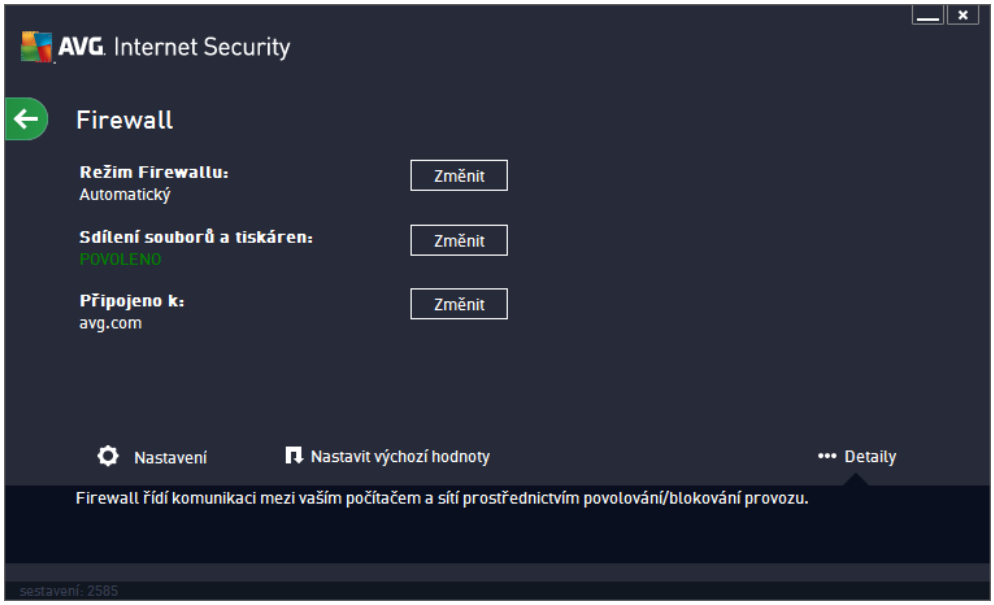
6.5. Firewall

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 nevyhovující. Pokud narazí na pokusy o proniknutí, zabrání jejich průniku dovnitř počítače. Firewall je nastaven tak, aby povolil nebo zablokoval interní či externí komunikaci *(oběma směry, dovnitř nebo ven)* na předem definovaných portech a pro vybrané softwarové aplikace. Například můžete Firewall nastavit tak, aby propouštěl 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 průběžně 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.

V rámci **AVG Internet Security 2013** řídí komponenta ***Firewall*** veškerý provoz na všech síťových portech vašeho počítače. Podle předem nastavených pravidel vyhodnocuje jednak aplikace, které 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!

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.*



Dostupné režimy Firewallu

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

- ***Automatický režim*** – V tomto režimu rozhoduje Firewall o veškerém provozu automaticky. Váš zásah nebude vyžadován za žádných okolností. Připojení známé aplikace povolí Firewall vždy a současně vytvoří pravidlo, podle něhož se tato aplikace bude nadále moci kdykoliv připojit automaticky. U ostatních aplikací rozhodne o povolení či nepovolení připojení na základě chování této aplikace, ale pravidlo vytvořeno nebude, aby ke kontrole této aplikace došlo opakovaně i při jejím příštím připojení. Firewall se v automatickém režimu chová zcela nenápadně. Volbu automatického režimu doporučujeme většině uživatelů.

- ***Interaktivní režim*** – Pro interaktivní režim se rozhodněte v případě, že chcete mít plnou kontrolu nad veškerou síťovou komunikací vašeho počítače. Firewall bude provoz monitorovat a oznámí vám každý pokus o komunikaci nebo přenos dat, přičemž budete mít možnost sami rozhodnout, zda má být tato komunikace povolena nebo zablokována. Volbu interaktivního režimu doporučujeme pouze zkušeným a znalým uživatelům!

- ***Blokovat přístup k internetu*** – V tomto režimu je veškeré připojení k Internetu v obou směrech zcela zablokováno. Toto nastavení je vhodné pro speciální situace a krátkodobé použití.

- ***Vypnout ochranu firewallem*** – Vypnutí Firewallu umožní průběh veškerému provozu ze sítě k vašemu počítači i opačným směrem. Tím se váš počítač stává vysoce zranitelným. Použití tohoto režimu lze doporučit výhradně zkušeným uživatelům, pouze krátkodobě a jedině v situaci, která toto opatření skutečně vyžaduje!

Firewall dále disponuje ještě specifickým automatickým režimem, který se aktivuje v situaci, kdy je vypnuta komponenta Počítač nebo Identita. V této situaci je riziko ohrožení vašeho počítače zvýšeno, proto bude Firewall povolovat provoz pouze pro známé a jednoznačně bezpečné aplikace. U všech ostatních aplikací bude požadovat vaše rozhodnutí. Toto řešení částečně kompenzuje sníženou ochranu vašeho počítače při vypnutí

jiné komponenty.

Ovládací prvky dialogu

Dialog nabízí přehled základních informací o stavu komponenty Firewall:

- ***Režim Firewallu*** - Uvádí, jaký režim provozu Firewallu je aktuálně zvolen. Pomocí tlačítka ***Změnit***, které najdete vedle uvedené informace, se můžete přepnout do rozhraní pro editaci nastavení Firewallu a změnit aktuálně nastavený režim za jiný *(popis a doporučené nastavení jednotlivých režimu Firewallu najdete v předchozím odstavci)*.

- ***Sdílení souborů a tiskáren*** - Uvádí, zda je v tuto chvíli povoleno sdílení souborů a tiskáren, a to v obou směrech. Sdílení souborů a tiskáren v podstatě znamená sdílení společných diskových jednotek, tiskáren, skenerů a podobných zařízení, či jakýchkoliv souborů nebo adresářů, které ve Windows označíte jako "sdílené". Sdílení těchto zdrojů je vhodné pouze v sítích, které považujete za skutečně bezpečné *(například v domácí síti, v práci nebo ve škole)*. Pokud se však připojujete k veřejné síti *(třeba na letišti nebo v internetové kavárně)*, sdílení rozhodně nedoporučujeme.

- ***Připojeno k*** - Uvádí název sítě, k níž je uživatel aktuálně připojen. U operačního systému Window XP jsou sítě uvedeny pod názvem, který si zvolil uživatel v době prvního připojení k síti. U operačních systému Windows Vista a vyšších se název sítě přebírá z Centra síťových připojení a sdílení.

V dialogu jsou dostupné tyto ovládací prvky:

Změnit - Tlačítko slouží ke změně stavu daného parametru. Podrobný popis průběhu změny je uveden v předchozím odstavci u jednotlivých parametrů.

Nastavení - Kliknutím na tlačítko přejdete do rozhraní Nastavení Firewallu, kde lze provést veškerou konfiguraci komponenty. Jakoukoliv konfiguraci lze doporučit pouze znalým a zkušeným uživatelům!

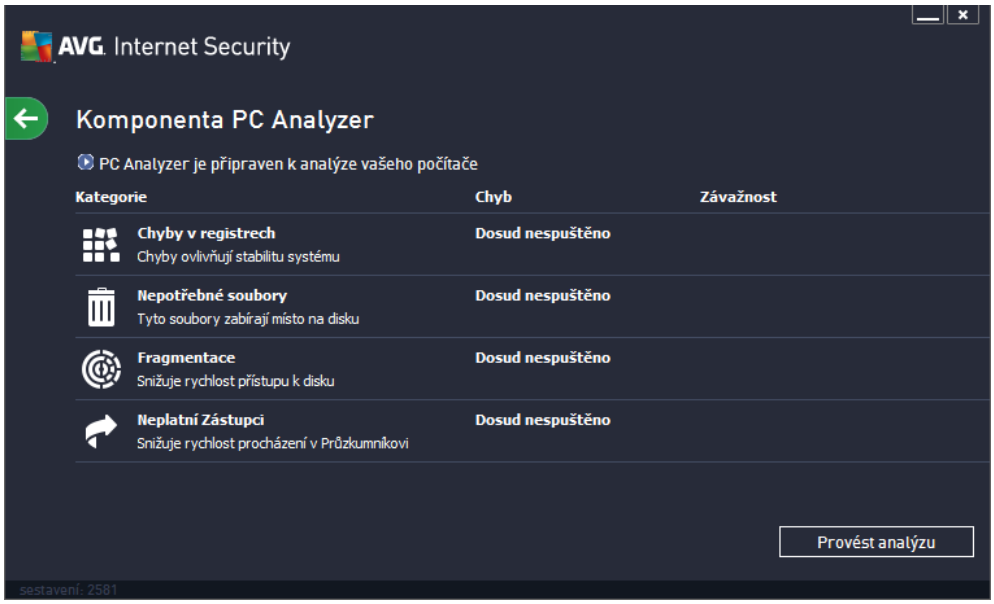
Nastavit výchozí hodnoty - Stiskem tlačítka se veškeré aktuální nastavení komponenty Firewall přepíše a bude vráceno k výchozím konfiguraci, jak byla nastavena výrobcem.

Detaily - Kliknutím na tlačítko se ve spodní části dialogu zobrazí stručný popis služby, jež je aktuálně zvolena.

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

6.6. PC Analyzer

Komponenta ***PC Analyzer*** provede celkovou kontrolu vašeho počítače a detekuje případné systémové chyby:



V základním rozhraní komponenty najdete tabulku rozdělenou do čtyř rádků, jež odpovídají jednotlivým detekovaným kategoriím problémů:

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

Samotnou analýzu pak spustíte stiskem tlačítka ***Provést analýzu***. Průběh kontroly budete moci sledovat přímo v tabulce, a tam budou posléze zobrazeny i výsledky analýzy. V přehledu výsledků bude uveden konkrétní počet chyb nalezených v systému a rozdělených podle jednotlivých kategorií (*sloupec* ***Chyb***). Výsledek analýzy bude také zobrazen graficky na ose ve sloupci ***Závažnost***.

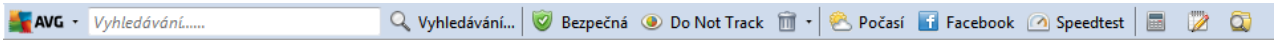
Ovládací tlačítka

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

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

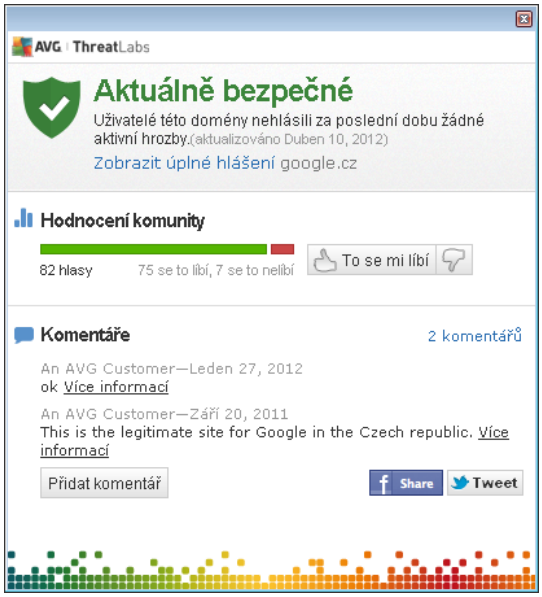
7. AVG Security Toolbar

AVG Security Toolbar je nástroj, který úzce spolupracuje se službou LinkScanner Surf-Shield a zajišťuje Vaši maximální bezpečnost při veškerém pohybu online. ***AVG Security Toolbar*** se v rámci **AVG Internet Security 2013** instaluje volitelně; možnost rozhodnout se, zda tuto komponentu chcete instalovat, jste měli v průběhu instalačního procesu. ***AVG Security Toolbar*** je dostupný v podobě nástrojové lišty ve vašem internetovém prohlížeči. Podporovanými prohlížeči jsou Internet Explorer (*ve verzi 6.0 a vyšší*) a/nebo Mozilla Firefox (*ve verzi 3.0 a vyšší*). Jiné prohlížeče nejsou podporovány *(pokud používáte alternativní prohlížeč, např. Avant browser, můžete se setkat s nekorektním chováním)*.



AVG Security Toolbar je tvořen těmito prvky:

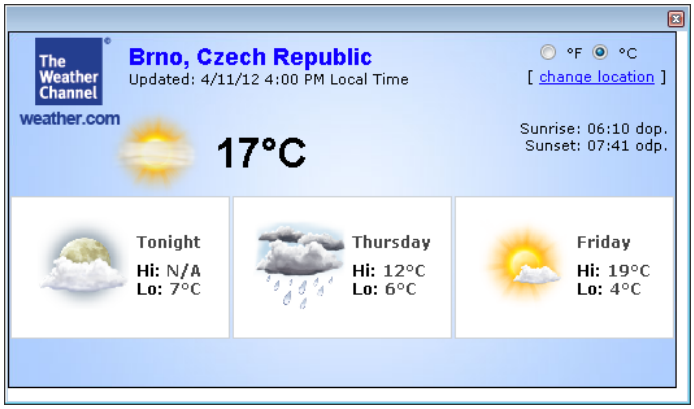
- ***Logo AVG*** s rozbalovací nabídkou:
  - ***Použít bezpečné vyhledávání AVG*** - Umožňuje vyhledávání prostřednictvím vyhledavače ***AVG Secure Search***.
  - ***Aktuální míra ohrožení*** - Otevře web virové laboratoře s grafickým znázorněním aktuální úrovně nebezpečí na Internetu.
  - ***AVG Threat Labs*** - Otevře stránku ***AVG Threat Lab*** (*http://www.avgthreatlabs.com*), kde najdete informace o bezpečnosti jednotlivých webů a aktuální úrovni online ohrožení.
  - ***Nápověda k liště*** - Otevírá online nápovědu k jednotlivým funkcím ***AVG Security Toolbar***.
  - ***Odeslat zpětnou vazbu k produktu*** - Otevře stránku s online formulářem, jehož prostřednictvím nám můžete zaslat svůj názor na ***AVG Security Toolbar***.
  - ***Odinstalovat AVG Security Toolbar*** - Otevře webovou stránku s podrobným popisem postupu při vypnutí ***AVG Security Toolbar*** v jednotlivých podporovaných prohlížečích.
  - ***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***.
- ***Zabezpečení*** - Tlačítkem otevřete nový dialog s informací o úrovni bezpečnosti na webové stránce, kde se právě teď nacházíte (*Aktuálně bezpečné*). Tento přehled pak můžete otevřít přímo v okně prohlížeče se všemi detaily o bezpečnostních aktivitách vztažených k právě prohlížené stránce (*Zobrazit úplné hlášení*):



- ***Do Not Track*** - Služba DNT dokáže identifikovat webové stránky, které sbírají data o vaší činnosti online a nabídne vám možnost sběr dat povolit nebo nepovolit. Podrobnosti >>

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

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



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

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

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

8. AVG Do Not Track

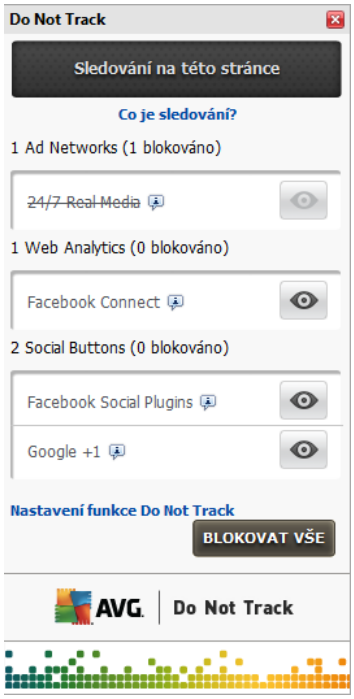
AVG Do Not Track dokáže identifikovat webové stránky, které sbírají data o vaší činnosti online. Služba ***AVG Do Not Track***, jež je součástí AVG Security Toolbaru, zobrazí informaci o webových stránkách či reklamních sítích, jež sbírají informace o vaší aktivitě a nabídne vám možnost sběr dat povolit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

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

Aktuálně je služba ***AVG Do Not Track*** podporovaná v prohlížečích Mozilla Firefox, Chrome a Internet Explorer.

8.1. Rozhraní služby AVG Do Not Track

Služba ***AVG Do Not Track*** dokáže rozpoznat různé typy sběru dat a o jejich případné detekci vás informuje změnou ikonky DNT v liště AVG Security Toolbar. Pokud jsou ve stránce rozpoznány služby, které mohou sbírat uživatelská data, u ikony DNT se objeví číslo, jež znázorňuje počet těchto detekovaných služeb: Po kliknutí na ikonu se otevře obdobný dialog:



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

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

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

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

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

Ovládací prvky dialogu

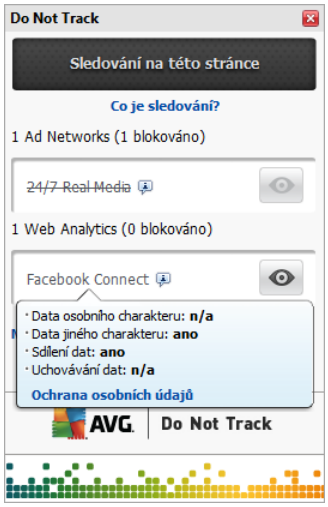
V dialogu jsou rovněž uvedeny dva hypertextové odkazy:

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

8.2. Informace o sledovacích procesech

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



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

8.3. Blokování sledovacích procesů

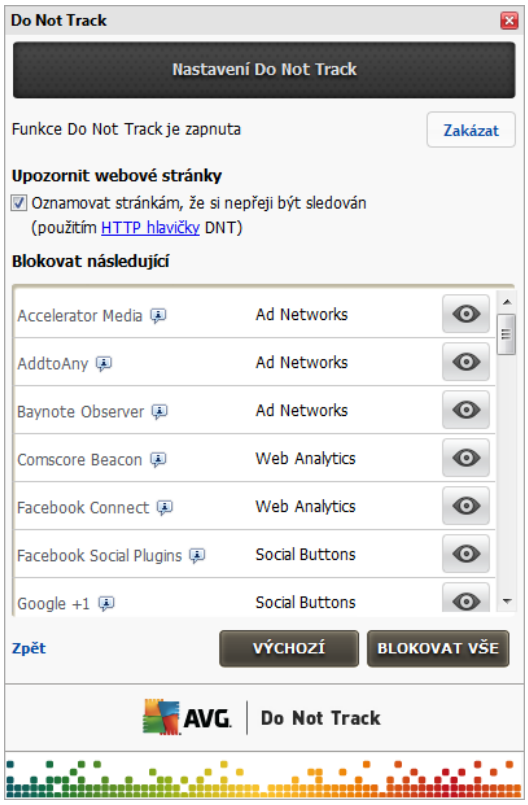
Nad kompletním seznamem služeb Web Analytics / tlačítek sociální sítě / reklamních sítí se také snadno rozhodnete, které služby mají být blokovány. Na výběr máte ze dvou možností:

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

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

8.4. Nastavení služby AVG Do Not Track

V konfiguračním dialogu ***Nastavení Do Not Track*** jsou dostupné tyto možnosti nastavení:



- ***Funkce Do Not Track je zapnuta*** - Ve výchozím nastavení je služba DNT aktivována. Stiskem tlačítka ***Zakázat*** máte možnost tuto funkci vypnout.

- ***Upozornit webové stránky*** - V této sekci máte možnost zapnout nebo vypnout volbu ***Oznamovat stránkám, že si nepřeji být sledován*** *(ve výchozím nastavení zapnuto).* Ponecháte-li položku označenou, bude ***Do Not Track*** automaticky informovat provozovatele detekovaných služeb sběru dat, že si nepřejete být sledováni.

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

Ovládací tlačítka

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

- ***Blokovat vše*** - kliknutím jednorázově zablokujete všechny výše uvedené služby v seznamu, jež jsou klasifikovány jako reklamní sítě;

- ***Odblokovat vše*** - kliknutím jednorázově povolíte všechny dříve zablokované služby uvedené v seznamu, jež jsou klasifikovány jako reklamní sítě;

- ***Výchozí*** - kliknutím zahodíte veškeré vlastní nastavení a vrátíte se k výchozí konfiguraci;
- ***Zakázat*** - ve výchozím nastavení je funkce ***Do Not Track*** zapnuta; stiskem tohoto tlačítka *(v horní části dialogu)* ji můžete deaktivovat.

9. Nastavení Firewallu

Konfigurace Firewallu se otevírá v samostatném okně, kde můžete na několika dialozích nastavit pokročilé parametry komponenty. Dialog konfigurace Firewallu lze zobrazit alternativně v základním nebo expertním nastavení. Při prvním otevření tohoto dialogu bude zobrazena základní verze, která nabízí možnost editace těchto parametrů:

- Obecné
- Aplikace
- Sdílení souborů a tiskáren

Ve spodní části dialogu najdete tlačítko ***Expertní režim***. Stiskem tohoto tlačítka se v konfiguračním dialogu objeví tyto další položky, umožňující vysoce pokročilé nastavení:

- Pokročilé nastavení
- Definované sítě
- Systémové služby
- Protokoly

Mějte prosím na paměti, že všechny komponenty AVG Internet Security 2013 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!

9.1. Obecné

Dialog ***Obecné informace*** nabízí přehled dostupných režimů komponenty Firewall. Aktuální nastavení režimu Firewallu můžete změnit prostým označením požadovaného režimu v nabídce.

Mějte prosím na paměti, že všechny komponenty AVG Internet Security 2013 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!

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

- ***Automatický režim*** – V tomto režimu rozhoduje Firewall o veškerém provozu automaticky. Váš zásah nebude vyžadován za žádných okolností. Připojení známé aplikace povolí Firewall vždy a současně vytvoří pravidlo, podle něhož se tato aplikace bude nadále moci kdykoliv připojit automaticky. U ostatních aplikací rozhodne o povolení či nepovolení připojení na základě chování této aplikace, ale pravidlo vytvořeno nebude, aby ke kontrole této aplikace došlo opakovaně i při jejím příštím připojení. Firewall se v automatickém režimu chová zcela nenápadně. ***Volbu automatického režimu doporučujeme většině uživatelů.***

- ***Interaktivní režim*** – Pro interaktivní režim se rozhodněte v případě, že chcete mít plnou kontrolu nad veškerou síťovou komunikací vašeho počítače. Firewall bude provoz monitorovat a oznámí vám každý pokus o komunikaci nebo přenos dat, přičemž budete mít možnost sami rozhodnout, zda má být tato komunikace povolena nebo zablokována. Volbu interaktivního režimu doporučujeme pouze zkušeným a znalým uživatelům!

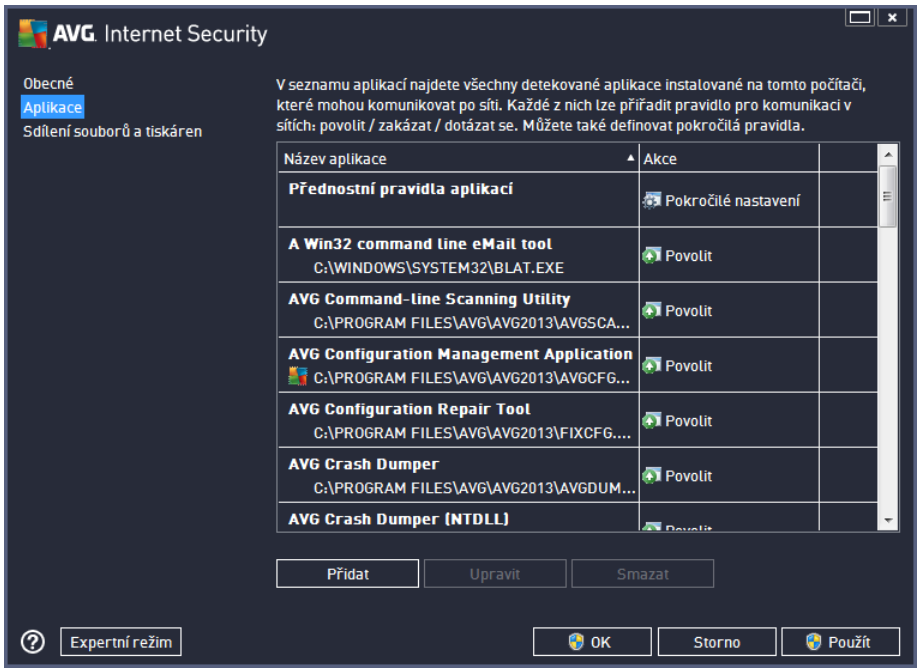
- ***Blokovat přístup k internetu*** – V tomto režimu je veškeré připojení k Internetu v obou směrech zcela zablokováno. Toto nastavení je vhodné pro speciální situace a krátkodobé použití.

- ***Vypnout ochranu firewallem*** – Vypnutí Firewallu umožní průběh veškerému provozu ze sítě k vašemu počítači i opačným směrem. Tím se váš počítač stává vysoce zranitelným. Použití tohoto režimu lze doporučit výhradně zkušeným uživatelům, pouze krátkodobě a jedině v situaci, která toto opatření skutečně vyžaduje!

Firewall dále disponuje ještě specifickým automatickým režimem, který se aktivuje v situaci, kdy je vypnuta komponenta Počítač nebo Identita. V této situaci je riziko ohrožení vašeho počítače zvýšeno, proto bude Firewall povolovat provoz pouze pro známé a jednoznačně bezpečné aplikace. U všech ostatních aplikací bude požadovat vaše rozhodnutí. Toto řešení částečně kompentuje sníženou ochranu vašeho počítače při vypnutí jiné komponenty.

9.2. Aplikace

V dialogu ***Aplikace*** najdete přehled všech aplikací, které se dosud pokusily navázat síťovou komunikaci. 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
- - Blokovat komunikaci
- - Pokročilé nastavení

Detekovány mohou být pouze ty aplikace, které byly na vašem počítači instalovány už ve chvíli instalace AVG Internet Security 2013. Ve chvíli, kdy se nová aplikace poprvé pokusí navázat síťovou komunikaci, bude buď vytvořeno pravidlo podle důvěryhodné databáze, anebo budete vyzváni k nastavení pravidla; pak bude třeba rozhodnout, zda má být komunikace této aplikaci povolena nebo blokována. Svou volbu můžete uložit jako trvalé pravidlo (které bude následně uvedeno v seznamu v tomto dialogu).

Samozřejmě je také možné definovat pravidla pro nové aplikace okamžitě – stiskněte tlačítko ***Přidat*** v tomto dialogu a vyplňte údaje o aplikaci.

Kromě aplikací obsahuje seznam ještě dvě speciální položky. ***Přednostní pravidla aplikací*** (*první řádek seznamu*) jsou preferenčními pravidly a jsou uplatňována přednostně před pravidly definovanými pro specifickou aplikaci.***Pravidla pro ostatní aplikace*** (*poslední řádek 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 pro přidání nové aplikace.
- ***Upravit*** - Otevře již vyplněný dialog pro upravení parametrů stávající aplikace.
- ***Smazat*** - Odstraní zvolenou aplikaci ze seznamu.

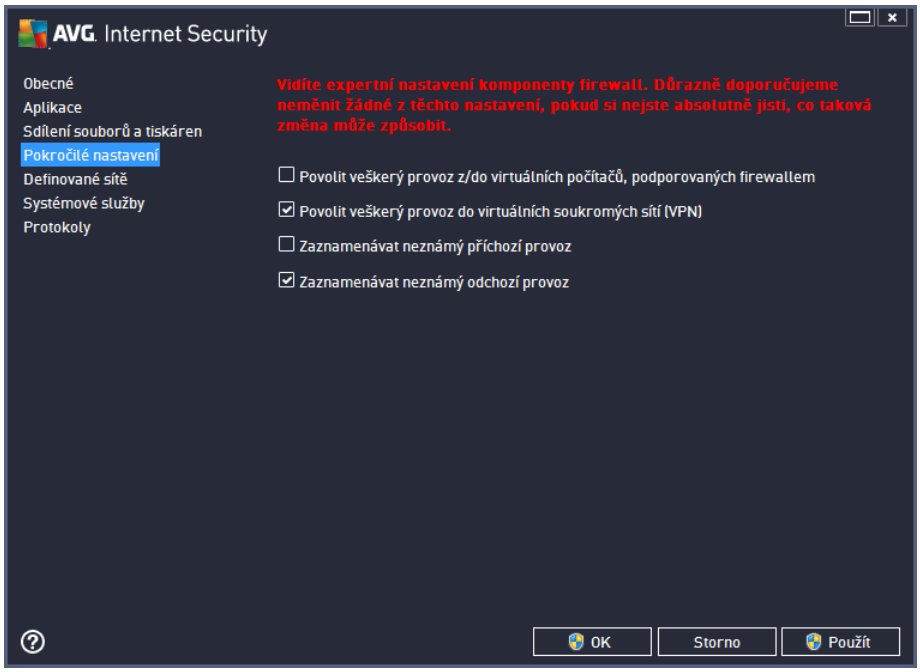
9.3. Sdílené souborů a tiskáren

Sdílení souborů a tiskáren v podstatě znamená sdílení společných diskových jednotek, tiskáren, skenerů a podobných zařízení, či jakýchkoliv souborů nebo adresářů, které ve Windows označíte jako "sdílené". Sdílení těchto zdrojů je vhodné pouze v sítích, které považujete za skutečně bezpečné *(například v domácí síti, v práci nebo ve škole)*. Pokud se však připojujete k veřejné síti *(třeba na letišti nebo v internetové kavárně)*, sdílení rozhodně nedoporučujeme.

Dialog ***Sdílení souborů a tiskáren*** umožňuje změnit nastavení sdílení souborů a tiskáren a aktuálního připojení k síti. U operačního systému Window XP jsou sítě uvedeny pod názvem, který si zvolil uživatel v době prvního připojení k síti. U operačních systému Windows Vista a vyšších se název sítě přebírá z Centra síťových připojení a sdílení.

9.4. Pokročilé nastavení

Veškeré editace v dialogu Pokročilé nastavení jsou určeny VÝHRADNĚ ZKUŠENÝM UŽIVATELŮM!

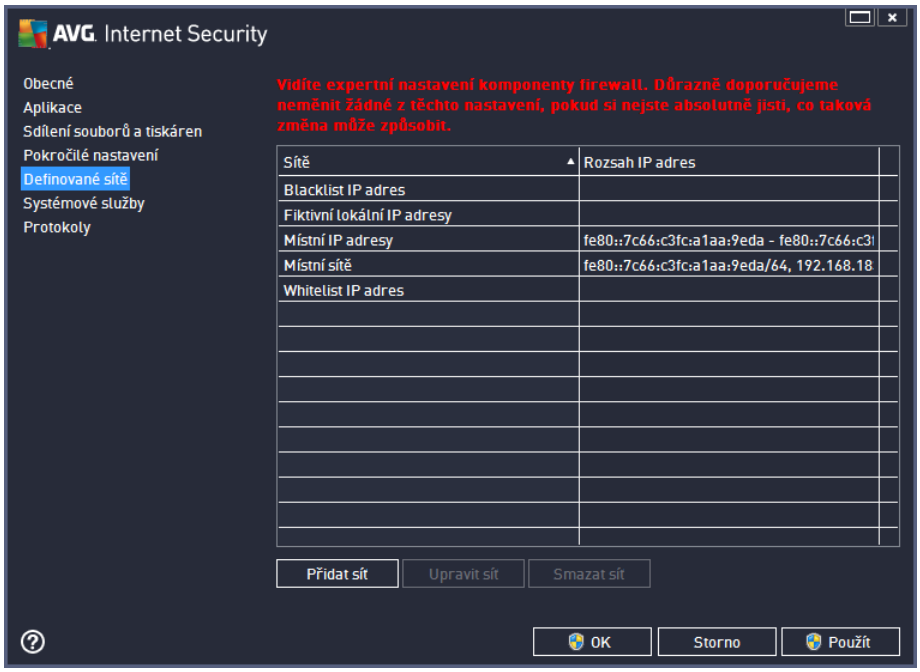


Dialog ***Pokročilé nastavení*** vám umožní zapnout či vypnout následující parametry Firewallu:

- ***Povolit veškerý provoz z/do virtuálních počítačů, podporovaných firewallem*** – podpora síťového připojení k virtuálním počítačům, například VMWare.
- ***Povolit veškerý provoz do virtuálních soukromých sítí (VPN)*** – podpora VPN připojení *(vzdálené připojení k počítači)*.
- ***Zaznamenávat neznámý příchozí/odchozí provoz*** – veškeré pokusy neznámých aplikací o komunikaci *(směrem dovnitř či ven)* budou zaznamenány v protokolu Firewallu.

9.5. Definované sítě

Veškeré editace v dialogu Definované sítě jsou určeny VÝHRADNĚ ZKUŠENÝM UŽIVATELŮM!

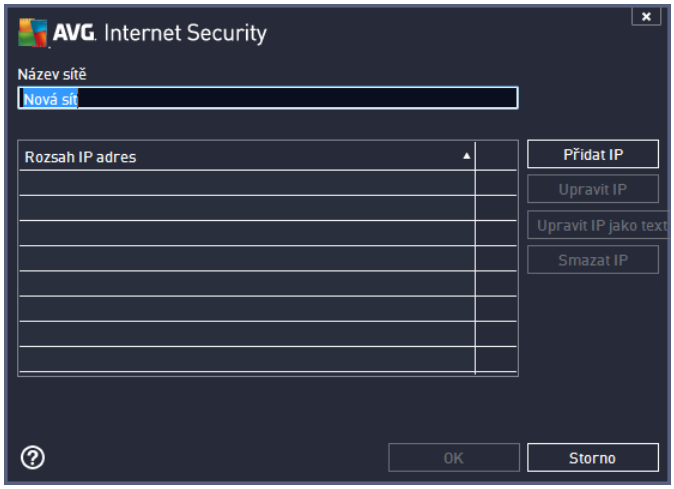


Dialog ***Definované sítě*** nabízí seznam všech sítí, k nimž je váš počítač připojen. O detekovaných sítích jsou v seznamu k dispozici tyto informace:

- ***Sítě*** - Uvádí seznam jmen všech detekovaných sítí, k nimž je počítač připojen.
- ***Rozsah IP adres*** - Rozsah každé sítě bude detekován automaticky a uveden ve tvaru rozpětí IP adres.

Ovládací tlačítka

- ***Přidat síť*** - Otevře nové dialogové okno, v němž můžete definovat parametry nově přidávané sítě, a to ***Název sítě*** a ***Rozsah IP adres***:

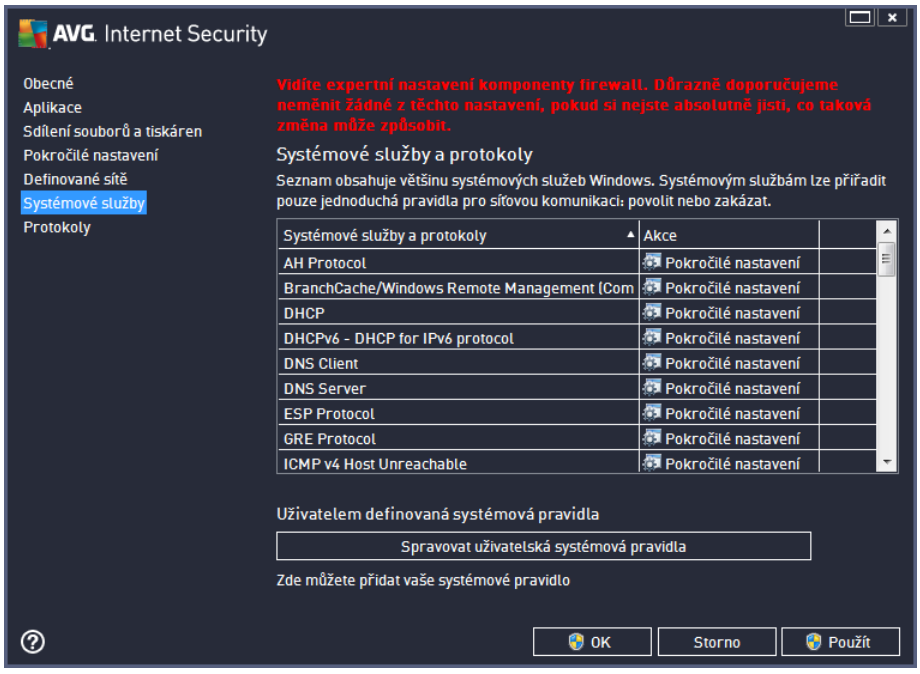


- ***Upravit síť*** - Otevře dialogové okno ***Vlastnosti sítě*** (*viz výše*), v němž můžete editovat parametry již definované sítě (*okno je identické s oknem pro přidání nové sítě, popis tedy najdete v předchozím odstavci*).

- ***Smazat síť*** - Odstraní záznam o zvolené síti ze seznamu.

9.6. 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. Tabulka obsahuje tyto sloupce:

- ***Systémové služby a protokoly*** - V tomto sloupci jsou zobrazena jména příslušných systémových

služeb.

- ***Akce*** - Sloupec zobrazuje ikony příslušné k určené akci:
  - Povolit komunikaci pro všechny sítě
  - Blokovat komunikaci

Chcete-li editovat nastavení libovolné položky v seznamu (*včetně přiřazených akcí*), klikněte na položku pravým tlačítkem myši a zvolte možnost ***Upravit***. ***Mějte však na paměti, že editaci systémového pravidla by měl provádět pouze pokročilý uživatel. Důrazně tedy doporučujeme systémová pravidla needitovat!***

Uživatelem definovaná systémová pravidla

Chcete-li vytvořit vlastní systémové pravidlo, použijte tlačítko ***Spravovat uživatelská systémová pravidla***. Tentýž dialog se také otevře, pokud se rozhodnete editovat nastavení již existujících položek seznamu systémových služeb a protokolů. V horní části dialogu vidíte přehled všech detailů právě editovaného systémového pravidla, v dolní části pak přehled vybraného detailu. S pravidly můžete pracovat pomocí tlačítek ***Upravit***, ***Přidat*** a ***Smazat***:

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, neměňte tato nastavení! Pokud nastavení skutečně měnit potřebujete, detailní popis jednotlivých dialogů najdete v příslušném souboru nápovědy.

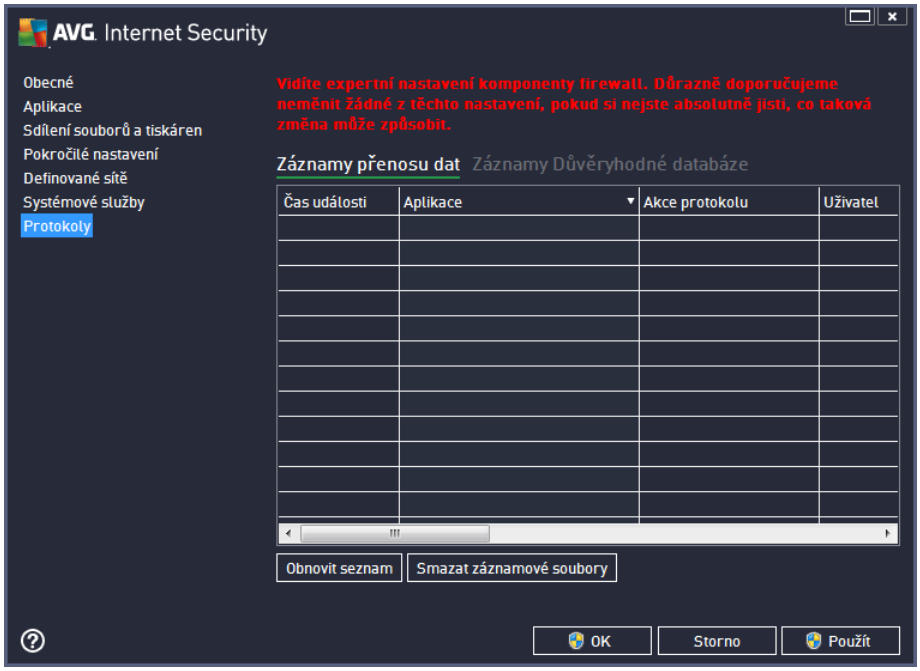
9.7. Protokoly

Veškeré editace v dialogu Protokoly jsou určeny VÝHRADNĚ ZKUŠENÝM UŽIVATELŮM!

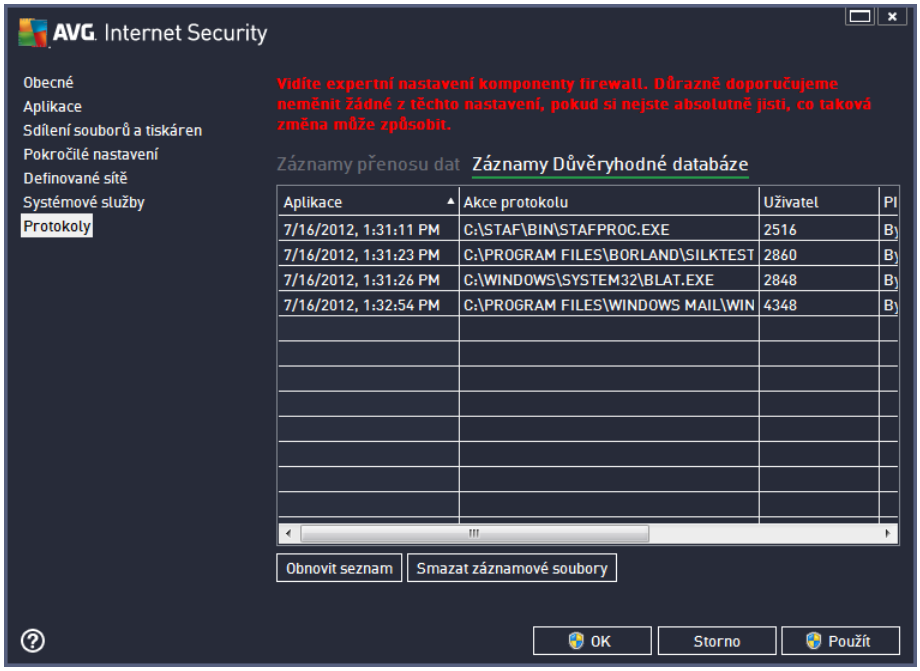
Dialog ***Protokoly*** nabízí seznamy všech protokolovaných událostí Firewallu s přehledem parametrů jednotlivých událostí, a to na dvou záložkách:

- ***Záznamy přenosu dat*** - Záložka nabízí informace o veškeré aktivitě aplikací, které se jakýkoliv

způsobem pokusily o navázání síťové komunikace. U každého záznamu najdete údaje o čase události, jméno aplikace, která se pokoušela navázat spojení, příslušnou akci protokolu, jméno uživatele, PID, směr připojení, typ protokolu, číslo vzdáleného a místního portu a informaci o vzdálené i lokální IP adrese.



- ***Záznamy Důvěryhodné databáze*** - Důvěryhodná databáze je interní databází AVG, v níž jsou shromážděny informace o aplikacích, které mají ověřený certifikát, jsou prověřené a důvěryhodné, a komunikace jim může být povolena. Při prvním pokusu jakékoliv aplikace o navázání síťové komunikace (*tedy v situaci, kdy pro danou aplikaci ještě není nastaveno žádné pravidlo*) je třeba zjistit, zda má být této aplikaci komunikace povolena. AVG nejprve prohledá *Důvěryhodnou 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.



Ovládací tlačítka

- ***Obnovit seznam*** - Protokolované parametry lze řadit podle zvoleného atributu: data chronologicky, ostatní sloupce abecedně *(klikněte na nadpis příslušného sloupce).* Tlačítkem ***Obnovit seznam*** pak můžete zobrazené informace aktualizovat.

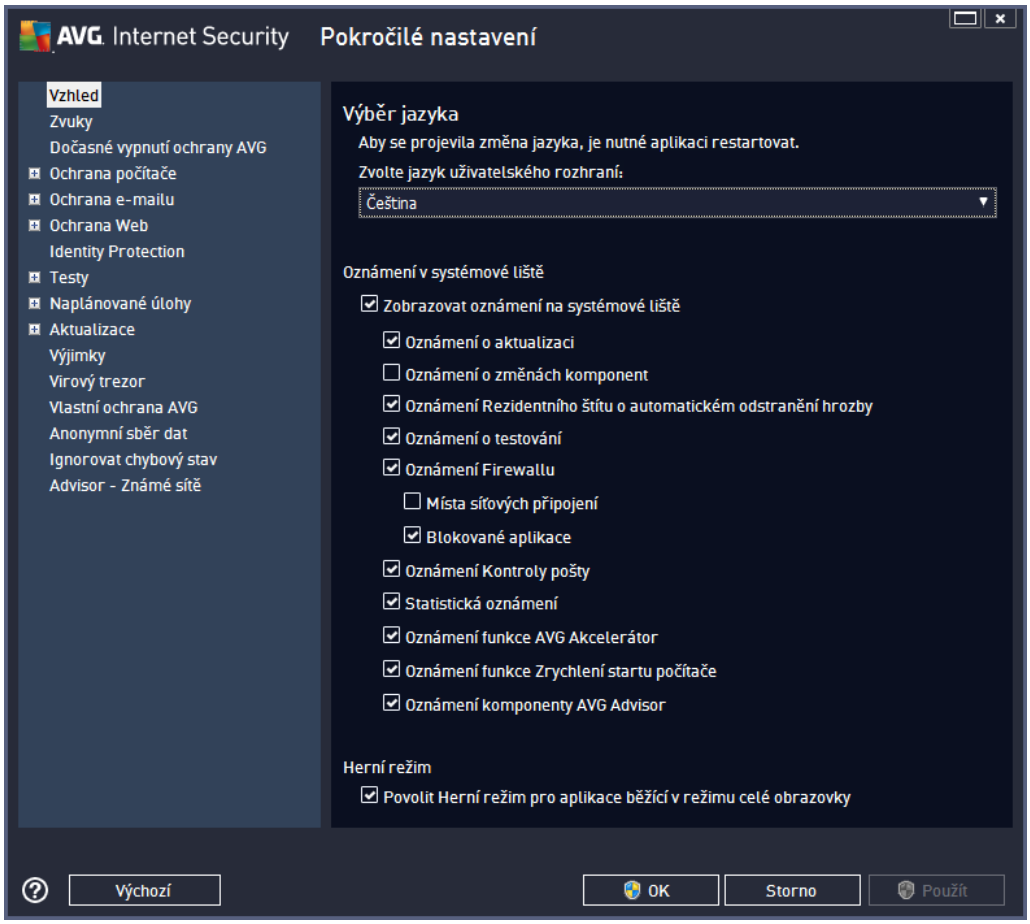
- ***Smazat záznamové soubory*** - Stiskem tlačítka odstraníte všechny záznamy z tabulky.

10. Pokročilé nastavení AVG

Dialog pro pokročilou editaci nastaveni programu **AVG Internet Security 2013** se otevírá v novém okně ***Pokročilé nastavení AVG***. Toto okno je rozděleno do dvou částí: v levé části okna najdete přehlednou stromově uspořádanou navigaci konfigurací programu. Volbou komponenty, jejíž parametry chcete editovat (*případně volbou konkrétní části této komponenty*) otevřete v pravé části okna příslušný editační dialog.

10.1. Vzhled

První položka navigačního seznamu, ***Vzhled***, se týká obecného nastavení hlavního dialogu **AVG Internet Security 2013** a nabízí možnost nastavení základních prvků programu:

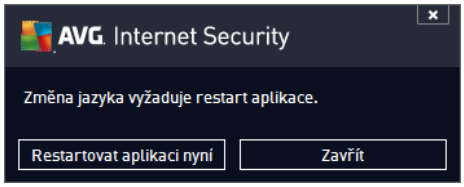


Výběr jazyka

V sekci ***Výběr jazyka*** můžete z rozbalovacího menu zvolit jazyk, v němž má být zobrazen hlavní dialog **AVG Internet Security 2013**. V nabídce budou dostupné jen ty jazyky, které jste zvolili během instalačního procesu a také angličtina (*angličtina se vždy instaluje automaticky*). Pro zobrazení **AVG Internet Security 2013** v požadovaném jazyce je však nutné aplikaci restartovat. Postupujte prosím následovně:

- V rozbalovacím menu zvolte požadovaný jazyk aplikace.
- Svou volbu potvrďte stiskem tlačítka ***Použít*** *(vpravo ve spodním rohu dialog).*

- Stiskem tlačítka ***OK*** znovu potvrďte, že chcete změnu provést.
- Objeví se nový dialog s informací o tom, že pro dokončení změny aplikace je nutné **AVG Internet Security 2013** restartovat.
- Stiskem tlačítka ***Restartovat aplikaci nyní*** vyjádříte svůj souhlas s restartem a během sekundy se aplikace přepne do nově zvoleného jazyka:



Oznámení v systémové liště

V této sekci můžete potlačit zobrazování systémových oznámení o aktuálním stavu aplikace **AVG Internet Security 2013**. Ve výchozím nastavení programu jsou systémová oznámení povolena. Doporučujeme toto nastavení ponechat! Systémová oznámení přinášejí například informace o spuštění aktualizace či testu, o změně stavu některé komponenty **AVG Internet Security 2013** a podobně. Je rozhodně vhodné věnovat jim pozornost!

Pokud se přesto z nějakého důvodu rozhodnete, že si nepřejete být takto informováni, máte možnost kompletně potlačit zobrazování informativních oznámení, nebo zakázat pouze zobrazování informací vztažených k určité komponentě **AVG Internet Security 2013**. Své vlastní nastavení můžete provést označením příslušné položky ve strukturované nabídce:

- ***Zobrazovat oznámení na systémové liště*** *(ve výchozím nastavení zapnuto)* - Položka je ve výchozím nastavení označena, takže se zobrazují veškerá informativní hlášení. Zrušením označení položky zcela vypnete zobrazování jakýchkoliv systémových oznámení. Jestliže je tato volba zapnuta, máte dále možnost definovat pravidla pro zobrazování jednotlivých typů informací:
    - ***Oznámení o aktualizaci*** *(ve výchozím nastavení zapnuto)* - Volbou položky rozhodnete, zda mají být zobrazena nebo naopak potlačena informativní hlášení o spuštění, průběhu a dokončení aktualizačního procesu; informace o ostatních procesech se budou zobrazovat normálně.
    - ***Oznámení o změnách komponent*** *(ve výchozím nastavení vypnuto)* - Volbou položky rozhodnete, zda mají být zobrazena nebo naopak potlačena informativní hlášení o vypnutí/ zapnutí komponenty, výskytu chyby ve funkci komponenty, apod. V případě hlášení problému odpovídá tato volba grafickým změnám ikony na systémové liště, která indikuje jakýkoliv problém v libovolné komponentě.
    - ***Oznámení Rezidentního štítu o automatickém odstranění hrozby*** *(ve výchozím nastavení zapnuto)* - Volbou položky rozhodnete, zda mají být zobrazena nebo naopak potlačena informativní hlášení týkající se kontroly souborů při kopírování, otevírání nebo i ukládání (*toto nastavení se projeví pouze tehdy, má-li Rezidentní štít povoleno automatické léčení detekované infekce*).
    - ***Oznámení o testování*** *(ve výchozím nastavení zapnuto)* - Volbou položky rozhodnete, zda mají být zobrazena nebo naopak potlačena informativní hlášení o automatickém spuštění naplánovaného testu, jeho průběhu, ukončení a výsledcích; informace o ostatních procesech

se budou zobrazovat normálně.

- ***Oznámení Firewallu*** *(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 či 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)*:

  - ***Místa síťových připojení*** *(ve výchozím nastavení vypnuto)* - při připojení k síti budete informováni, zda Firewall tuto síť zná a jak bude nastaveno sdílení souborů a tiskáren.

  - ***Blokované aplikace*** *(ve výchozím nastavení zapnuto)* - pokud se o připojení k síti pokouší neznámá či jakkoliv podezřelá aplikace, Firewall tento pokus zablokuje a vyrozumí vás o této skutečnosti oznámením na systémové liště. Doporučujeme ponechat tuto funkci vždy zapnutou!

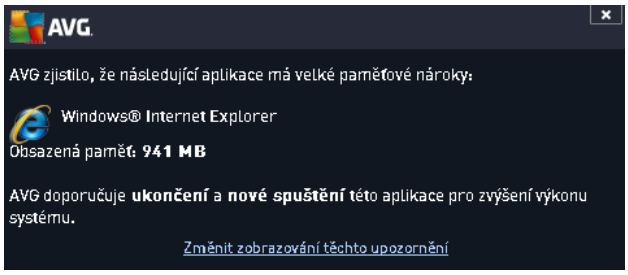
- ***Oznámení Kontroly pošty*** *(ve výchozím nastavení zapnuto)* - Volbou položky rozhodnete, zda mají být zobrazena nebo naopak potlačena informativní hlášení o průběhu testování příchozích a odchozích zpráv elektronické pošty; informace o ostatních procesech se budou zobrazovat normálně.

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

- ***Oznámení funkce 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.

- ***Oznámení funkce zrychlení startu počítače*** *(ve výchozím nastavení vypnuto)* - Volbou položky rozhodnete, zda si přejete být vyrozuměni o zrychleném startu Vašeho počítače.

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

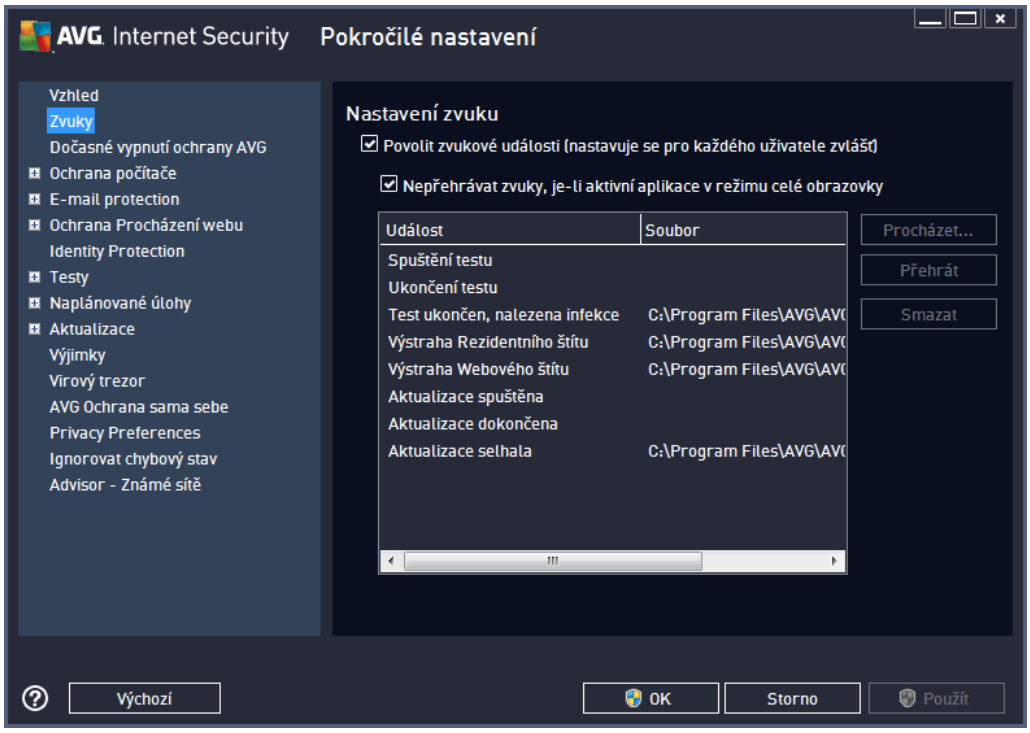


Herní režim

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

10.2. Zvuky

V dialogu ***Zvuky*** můžete rozhodnout, zda chcete být o jednotlivých akcích **AVG Internet Security 2013** informováni zvukovým oznámením:



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

Ovládací tlačítka dialogu

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

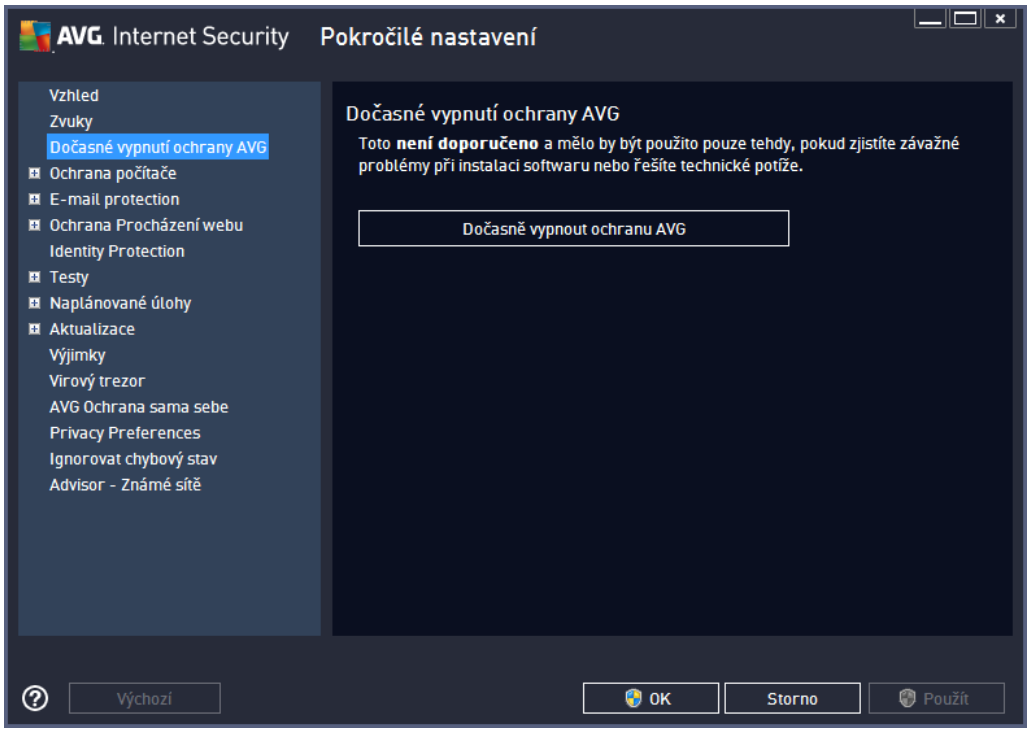
- ***Přehrát*** - Chcete-li si přiřazený zvuk poslechnout, označte v seznamu příslušnou akci a stiskněte tlačítko ***Přehrát***.

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

10.3. Dočasné vypnutí ochrany AVG

V dialogu ***Dočasné vypnutí ochrany AVG*** máte možnost označením jediné dostupné položky jednorázově deaktivovat celou ochranu zajištěnou programem **AVG Internet Security 2013**.

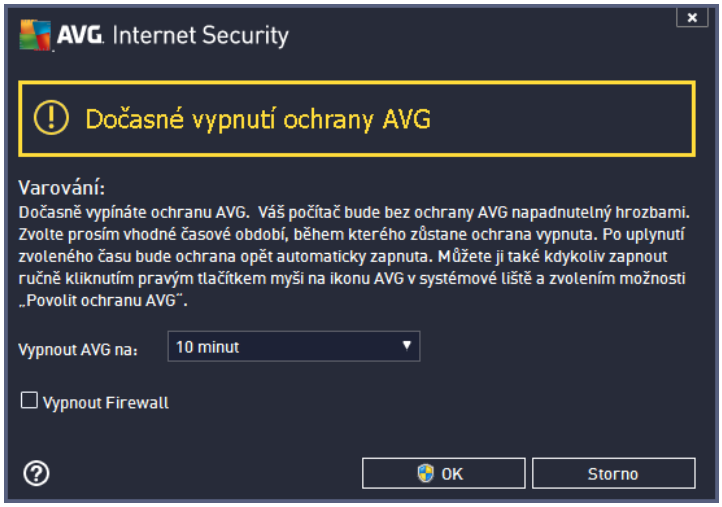
Mějte prosím na paměti, že tato volba by v žádném případě neměla být použita, pokud to není opravdu nezbytně nutné!



V naprosté většině případů ***není nutné*** deaktivovat **AVG Internet Security 2013** před instalací nového software nebo ovladačů, a to ani tehdy, pokud budete během instalace vyzváni k zavření všech spuštěných aplikací. Pokud by v takovém případě došlo ke kolizi, pravděpodobně bude stačit deaktivovat rezidentní ochranu (*Povolit Rezidentní štít*). Jestliže budete opravdu nuceni deaktivovat **AVG Internet Security 2013**, zapněte jej hned, jakmile to bude možné. Pamatujte, že pokud jste připojeni k Internetu nebo k jiné síti, je váš počítač bez aktivní ochrany vysoce zranitelný.

Jak vypnout ochranu AVG

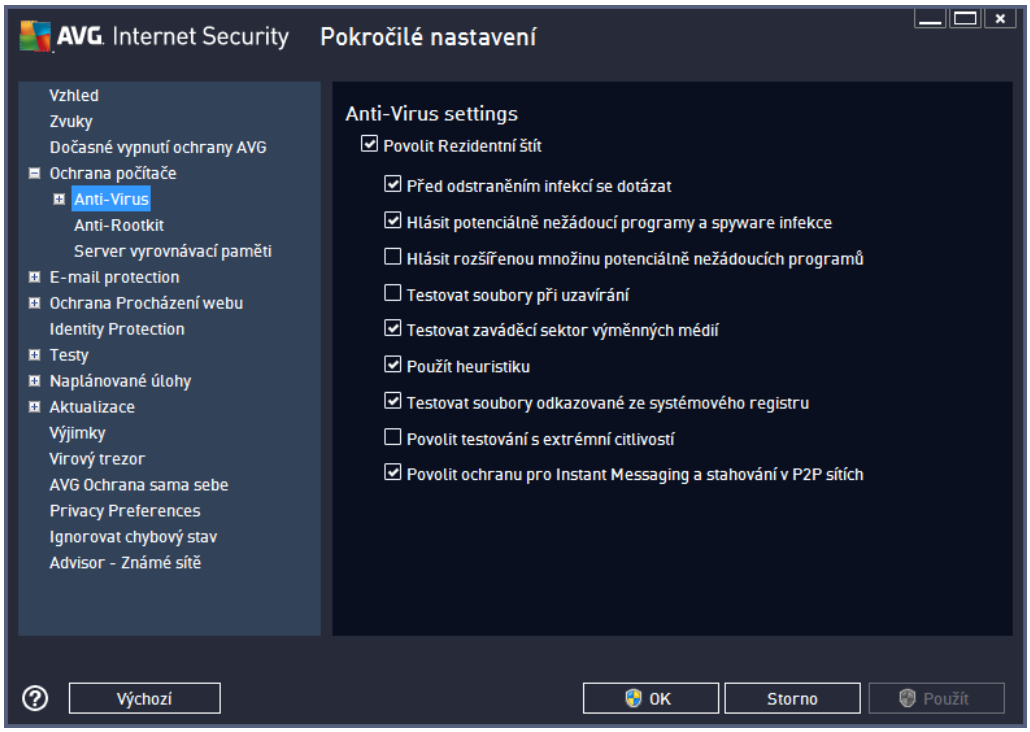
Označte políčko ***Dočasně vypnout ochranu AVG*** a svou volbu potvrďte stiskem tlačítka ***Použít***. V nově otevřeném dialogu ***Dočasné vypnutí ochrany AVG*** pak nastavte požadovaný čas, po který potřebujete **AVG Internet Security 2013** vypnout. Standardně bude ochrana vypnuta po dobu 10 minut, což je dostačující pro všechny běžné úkony. Můžete si však zvolit i delší časový interval, ale tuto možnost nedoporučujeme, pokud to není naprosto nezbytně nutné. Po uplynutí zvoleného časového intervalu se všechny vypnuté komponenty znovu automaticky aktivují. Maximální časová lhůta vynutí ochrany AVG je do příštího restartu vašeho počítače. Samostatnou volbou můžete v dialogu ***Dočasné vypnutí ochrany AVG*** vypnout i komponentu ***Firewall***, a to označením položky ***Vypnout Firewall***.



10.4. Ochrana počítače

10.4.1. AntiVirus

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



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

- ***Před odstraněním infekcí se dotázat*** (*ve výchozím nastavení zapnuto*) - pokud je políčko zaškrtnuté, Rezidentní štít nebude s nalezenými infekcemi nic dělat automaticky a vždy se vás zeptá, jak si přejete s nimi naložit. Pokud necháte políčko neoznačené, pak se **AVG Internet Security 2013** pokusí každou nalezenou infekci vyléčit, a pokud to nepůjde, přesune obejtk 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*) a spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány vědomě a se souhlasem uživatele. Doporučujeme nicméně ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.

- ***Hlásit rozšířenou množinu potenciálně nežádoucích programů*** (*ve výchozím nastavení vypnuto*) - zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v původní podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.

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

- ***Testovat zaváděcí sektor výměnných médií*** (*ve výchozím nastavení zapnuto*)

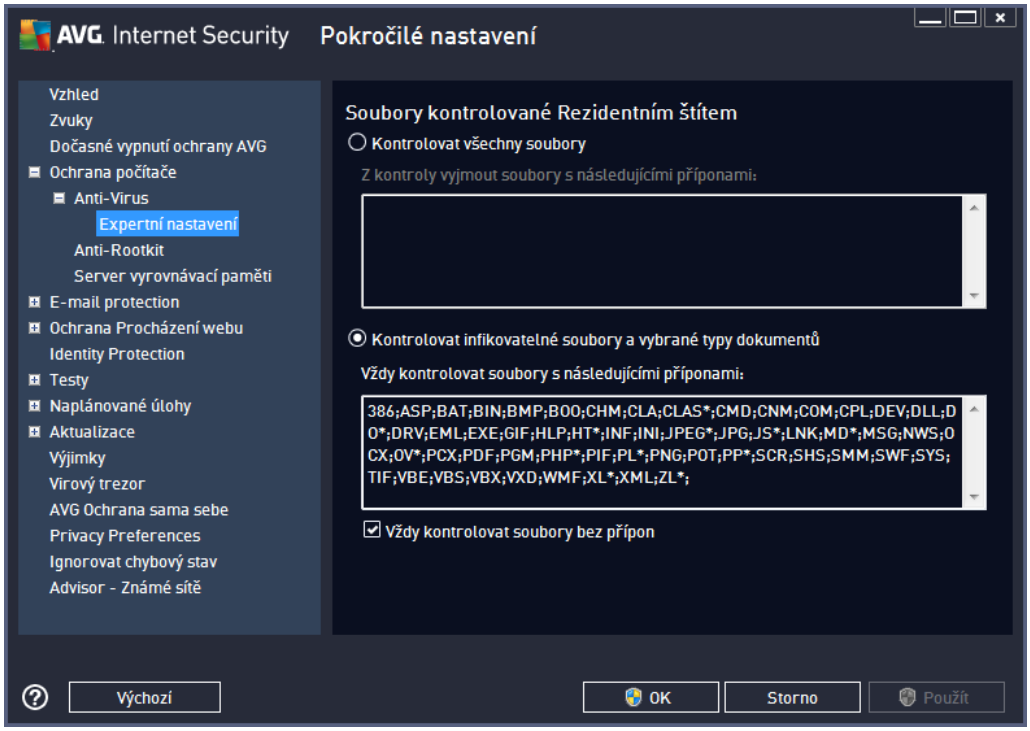
- ***Použít heuristiku*** (*ve výchozím nastavení zapnuto*) - k detekci infekce bude použita i metoda heuristické analýzy (*dynamické emulace instrukcí testovaného objektu v prostředí virtuálního počítače*)

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

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

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

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

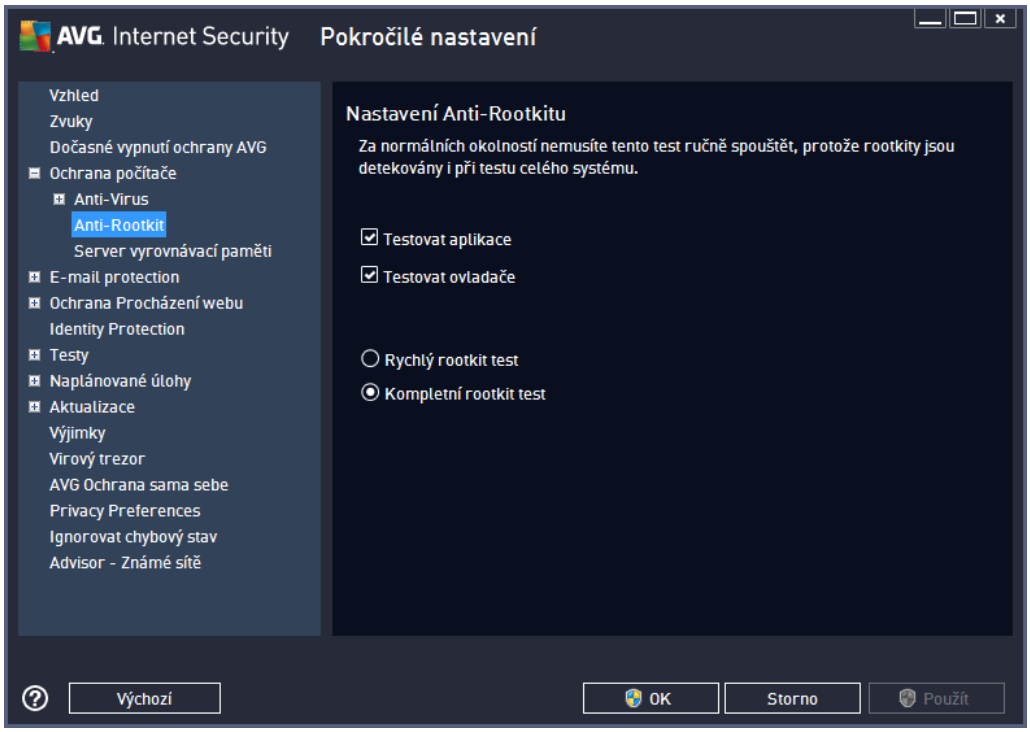


Svou volbou rozhodněte, zda chcete ***Kontrolovat všechny soubory*** nebo pouze ***Kontrolovat infikovatelné soubory a vybrané typy dokumentů***. Pro urychlení testování a současné dosažení maximální bezpečnosti doporučujeme ponechat výchozí nastavení. Tak budou testovány infikovatelné soubory s příponami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

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

10.4.2. Anti-Rootkit

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

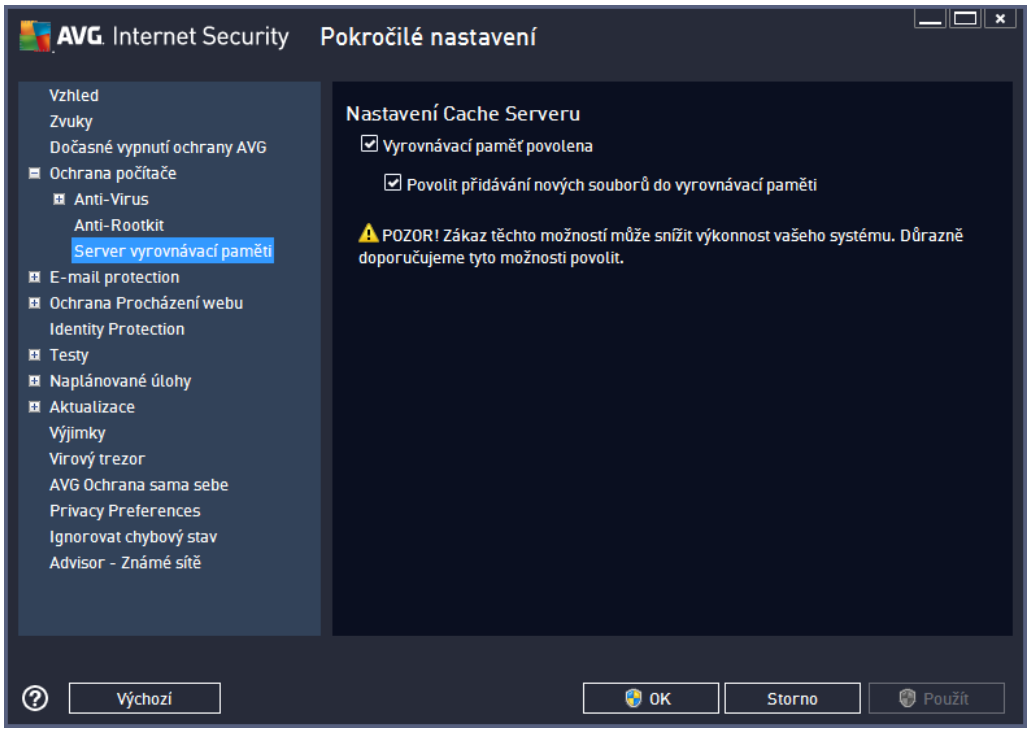


Možnosti ***Testovat aplikace*** a ***Testovat ovladače*** umožňují určit, co vše má být v testu na rootkity zahrnuto. Jiné než výchozí nastavení doporučujeme pouze zkušeným uživatelům; jinak prosím ponechte všechny možnosti zapnuté. Dále se pak můžete rozhodnout, v jakém režimu si přejete test spustit:

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

10.4.3. Server vyrovnávací paměti

Dialog ***Nastavení Cache Serveru*** se vztahuje k procesu serveru vyrovnávací paměti, jehož úkolem je zrychlit průběh všech testů **AVG Internet Security 2013**:



V rámci tohoto procesu **AVG Internet Security 2013** detekuje důvěryhodné soubory *(za důvěryhodný lze považovat například soubory digitálně podepsány důvěryhodným zdrojem)* a indexuje je. Indexované soubory jsou pak automaticky považovány za bezpečné a nemusí již být znovu testovány, dokud v nich nedojde ke změně.

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

- ***Povolena vyrovnávací paměť'*** (*ve výchozím nastavení zapnuto*) - pokud tuto možnost vypnete, deaktivujete tak proces vyrovnávací paměti a vyprázdníte cache. Mějte prosím na mysli, že vypnutím tohoto procesu dojde ke zpomalení testu i celkového výkonu vašeho počítače, protože bude nutné provést test přítomnosti viru a spyware u každého jednotlivého souboru.

- ***Povolit přidávání nových souborů do vyrovnávací paměti*** (*ve výchozím nastavení zapnuto*) - pokud tuto možnost vypnete, zabráníte tak přidávání nových souborů do vyrovnávací paměti. Všechny soubory, které jsou již v paměti uloženy, budou zachovány a vynechány z testování, pokud nedojde k deaktivaci celé vyrovnávací paměti anebo do příští aktualizace definic.

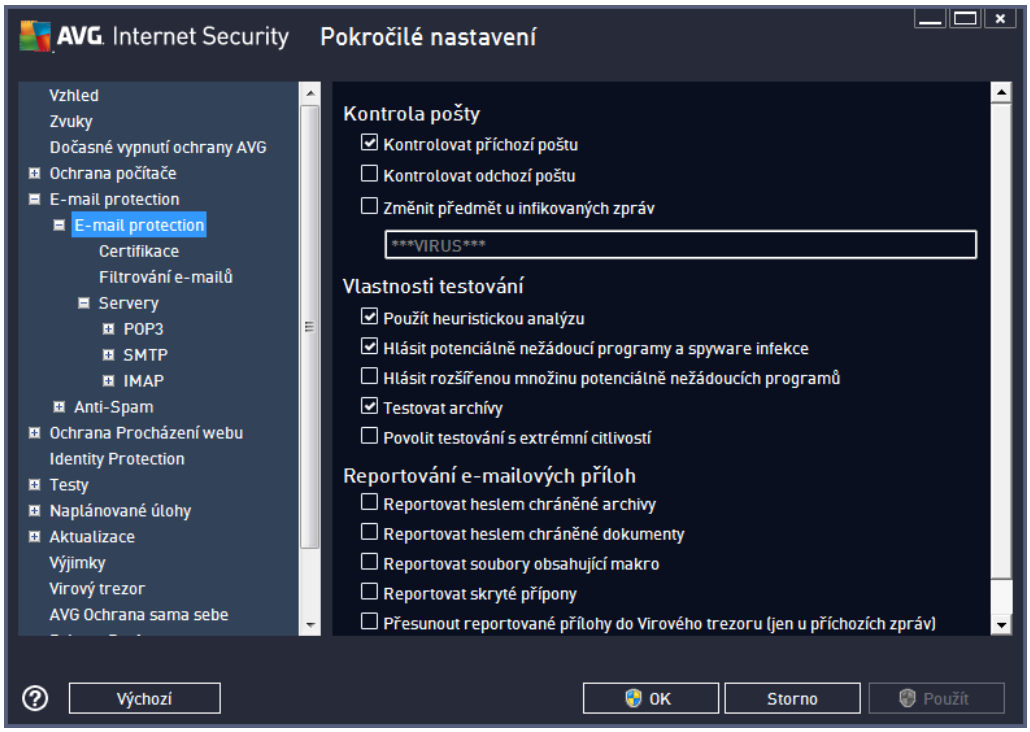
Pokud nemáte skutečný důvod cache server vypínat, důrazně doporučujeme, abyste se přidrželi výchozího nastavení a ponechali obě položky zapnuté! V opačném případě může dojít k výraznému snížení rychlosti a výkonnosti Vašeho systému.

10.5. Kontrola pošty

V této sekci máte možnost editovat podrobné nastavení pro službu Kontrola pošty a Anti-Spam:

10.5.1. Kontrola pošty

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



Kontrola pošty

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

- ***Kontrolovat příchozí poštu*** (*ve výchozím nastavení zapnuto*) - označením zapnete/vypnete možnost testování všech příchozích e-mailů
- ***Kontrolovat odchozí poštu*** (*ve výchozím nastavení vypnuto*) - označením zapnete/vypnete možnost testování všech e-mailů odesílaných z vašeho účtu
- ***Změnit předmět u infikovaných zpráv*** (*ve výchozím nastavení vypnuto*) - pokud si přejete být upozorněni, že otestovaná zpráva byla vyhodnocena jako infikovaná, můžete aktivovat tuto položku a do textového pole vepsat požadované označení takovéto e-mailové zprávy. Tento text pak bude přidán do pole "Předmět" u každé pozitivně detekované zprávy (*slouží ke snadnější identifikaci a filtrování*). Výchozí hodnota je ***VIRUS*** a doporučujeme ji ponechat.

Vlastnosti testování

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

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

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

- ***Hlásit rozšířenou množinu potenciálně nežádoucích programů*** (*ve výchozím nastavení vypnuto*) - zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v původní podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.

- ***Testovat archivy*** (*ve výchozím nastavení zapnuto*) - testovat obsah archivů v přílohách zpráv.

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

Reportování e-mailových příloh

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

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

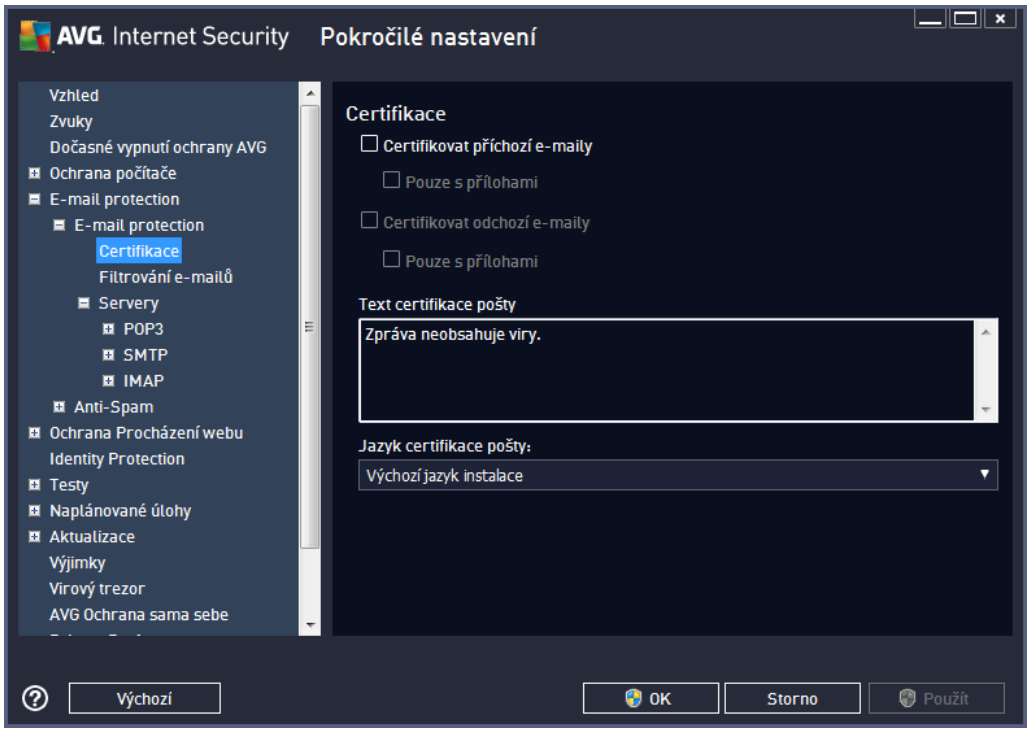
- ***Reportovat heslem chráněné dokumenty*** – dokumenty chráněné heslem není možné otestovat na přítomnost virů; po zaškrtnutí tohoto políčka se tyto archivy budou označovat jako potenciálně nebezpečné.

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

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

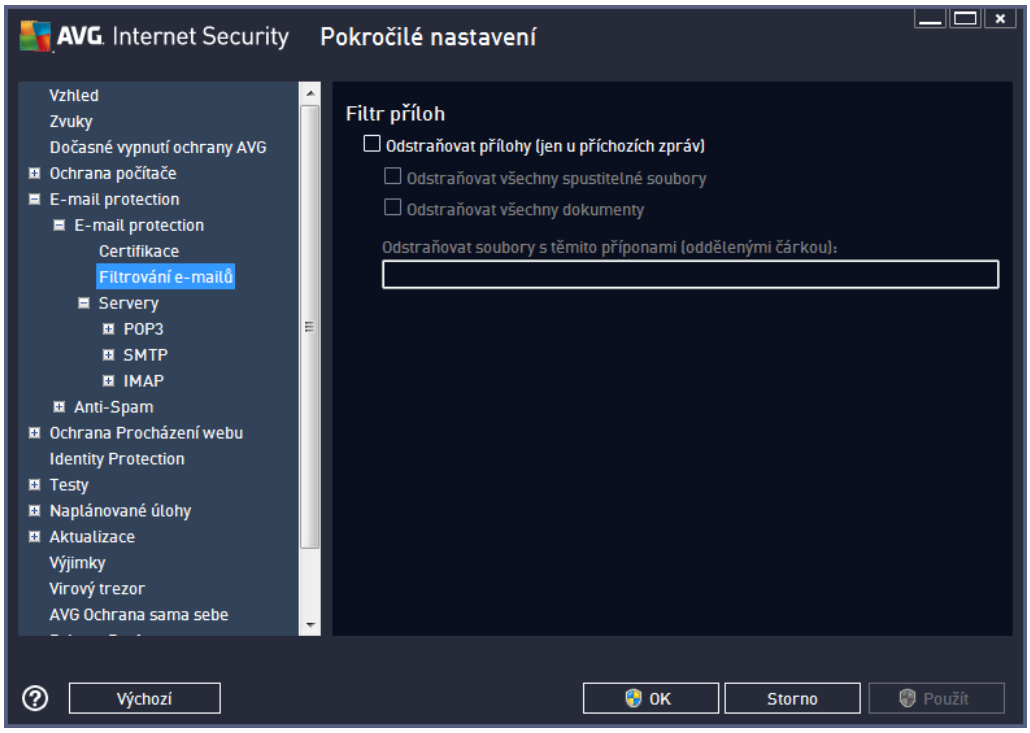
- Zaškrtnutím políčka ***Přesunout reportované přílohy do Virového trezoru*** určíte, že všechny výše vybrané soubory z příloh e-mailů se mají nejen reportovat, ale rovněž automaticky přesouvat do Virového trezoru.

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



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

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



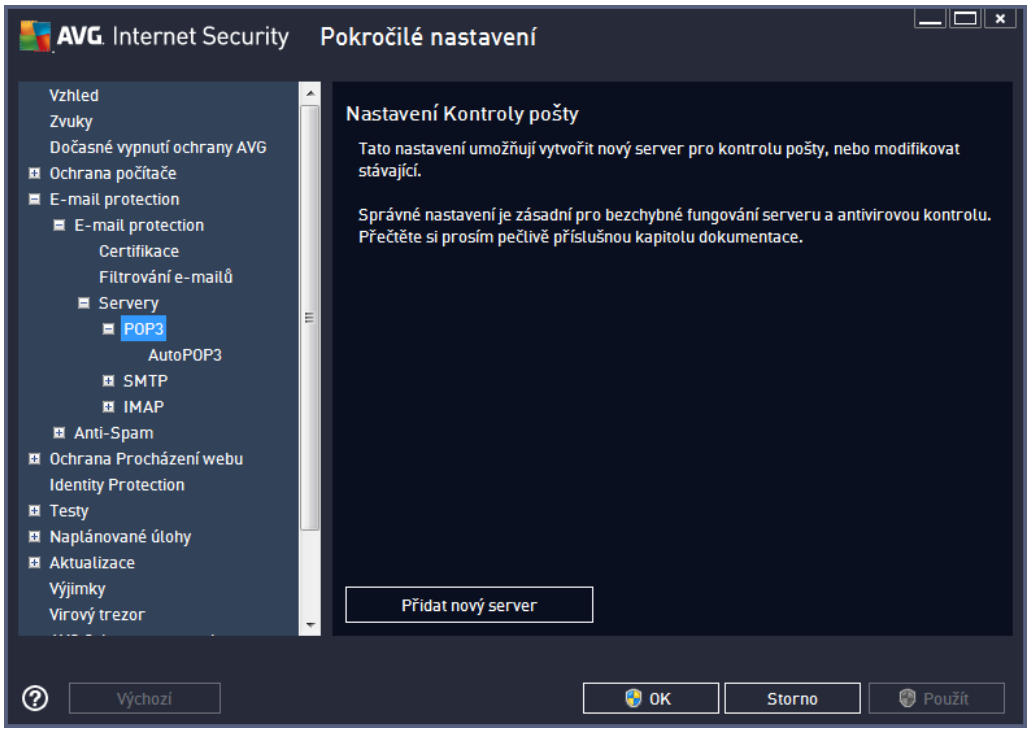
Dialog ***Filtr příloh*** umožňuje nastavení parametrů pro testování příloh e-mailových zpráv. Ve výchozím nastavení je možnost ***Odstraňovat přílohy*** vypnuta. Pokud se rozhodnete pro její aktivaci, budou automaticky odstraněny všechny přílohy zpráv, které byly detekovány jako infikované nebo potenciálně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

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

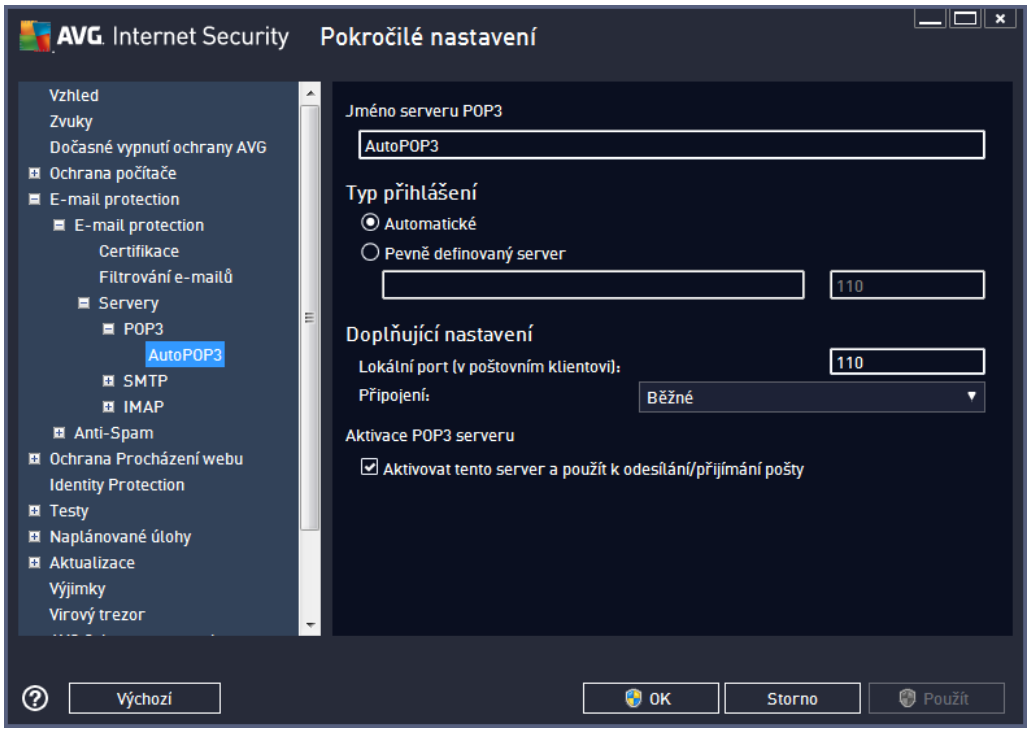
V sekci ***Servery*** máte možnost editovat parametry jednotlivých serverů Kontroly pošty:

- POP3 server
- SMTP server
- IMAP server

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



V tomto dialogu nastavujete server Kontroly pošty s protokolem POP3 pro příchozí poštu:



- ***Jméno serveru POP3*** - v tomto poli můžete zadat jméno nově přidaných serverů (*server POP3 přidáte tak, že kliknete pravým tlačítkem myši nad položkou POP3 v levém navigačním menu*). U automaticky vytvořeného serveru "AutoPOP3" je toto pole deaktivováno.

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

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

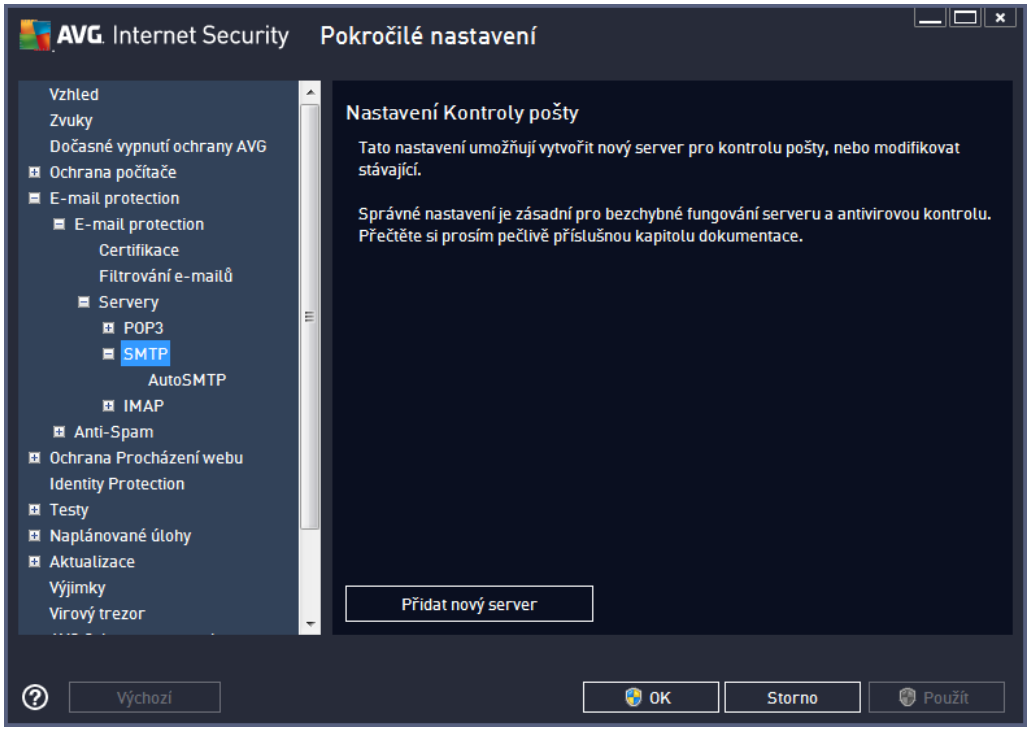
    - ***Pevně definovaný server*** - v tomto případě bude vždy použit konkrétní server. Je třeba zadat adresu nebo jméno vašeho poštovního serveru. Přihlašovací jméno pak zůstane beze změny. Jako jméno je možné použít jak doménový název (*například pop.acme.com*), tak IP adresu (*například 123.45.67.89*).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

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

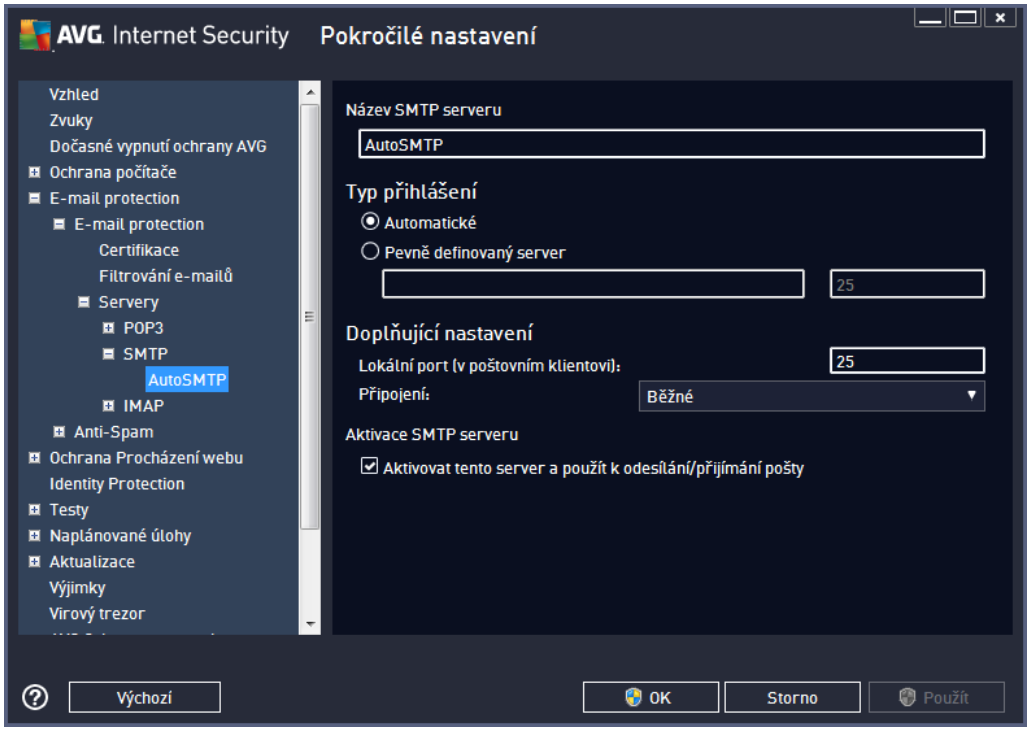
    - ***Lokální port*** - určuje, na kterém portu lze očekávat komunikaci z poštovní aplikace. Tento port je pak také nutné v poštovní aplikaci zadat jako port pro POP3 komunikaci.

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

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



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



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

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

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

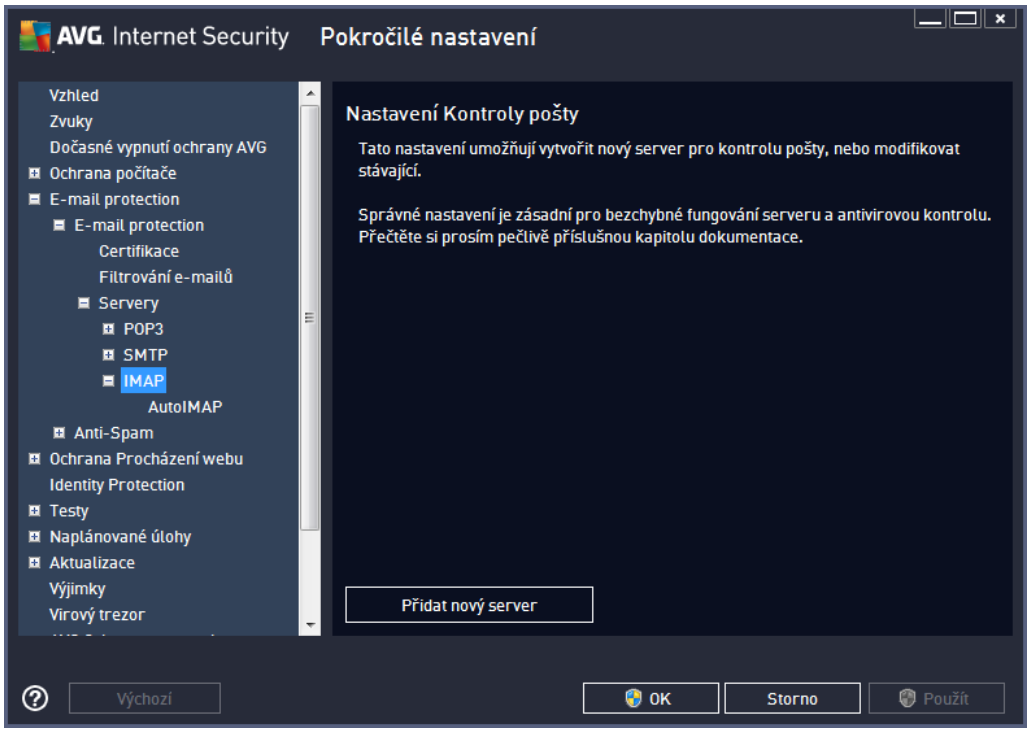
    - ***Pevně definovaný server*** - v tomto případě bude vždy použit konkrétní server. Do editačního řádku je třeba zadat adresu nebo jméno vašeho poštovního serveru. Jako jméno je možné použít jak doménový název (*např. smtp.acme.com*), tak i IP adresu (*např. 123.45.67.89*). Pokud poštovní server používá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

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

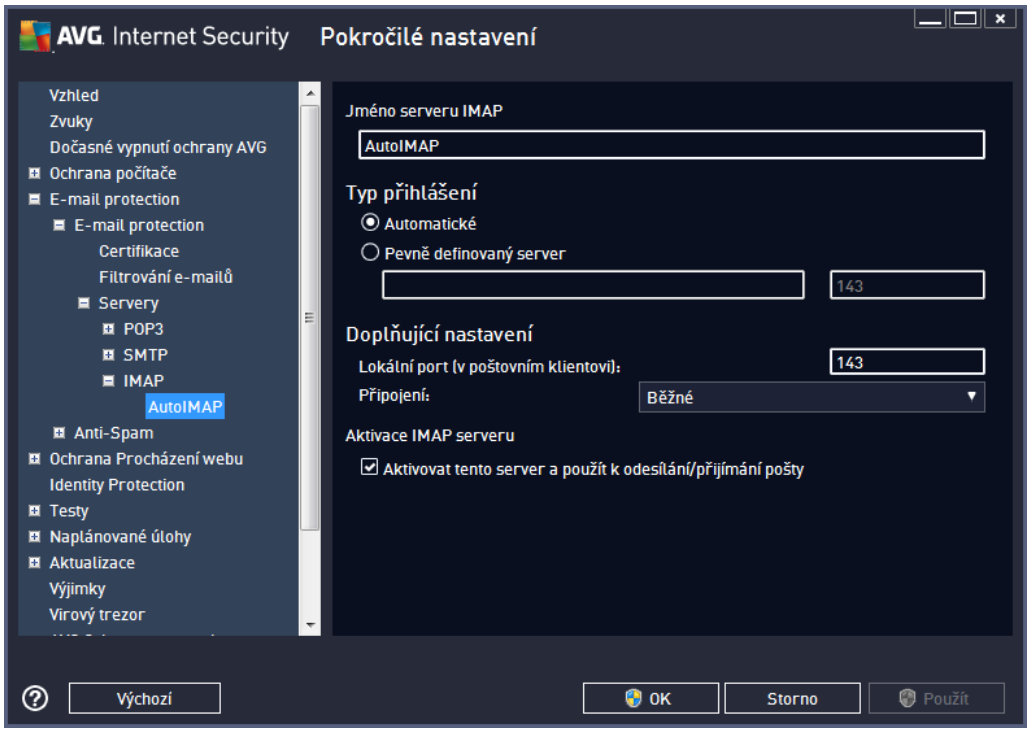
    - ***Lokální port*** - určuje, na kterém portu lze očekávat komunikaci z poštovní aplikace. Tento port je pak také nutné v poštovní aplikaci zadat jako port pro SMTP komunikaci.

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

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



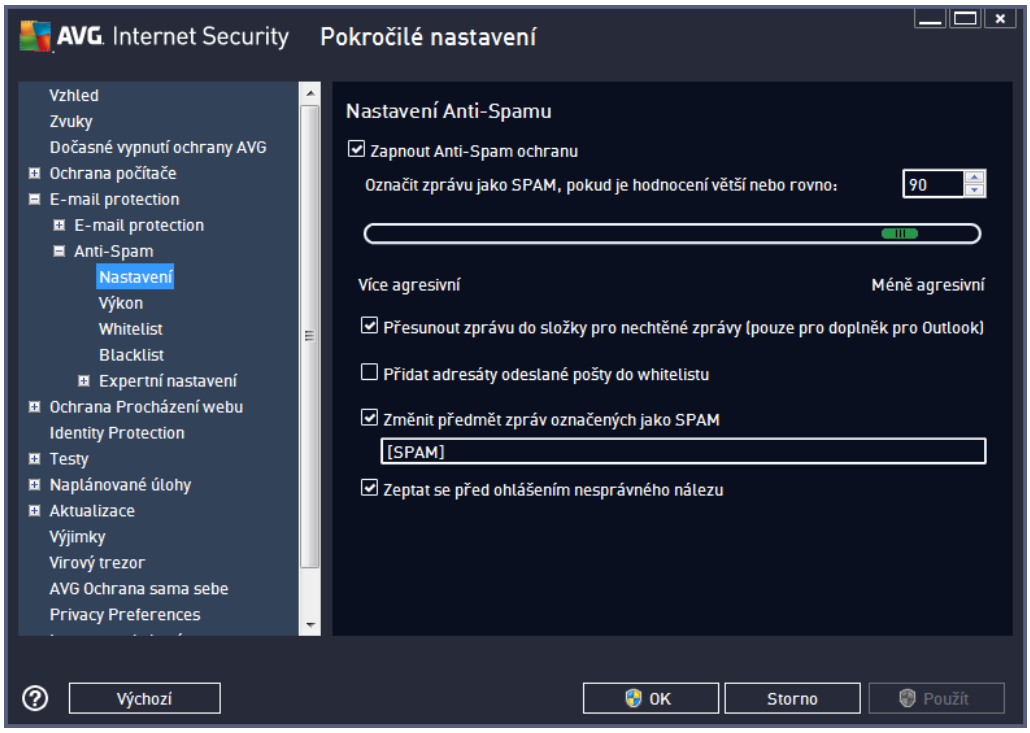
V tomto dialogu nastavujete server Kontroly pošty s protokolem IMAP pro odchozí poštu:



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

- ***Typ přihlášení*** - definuje, jak má být určen poštovní server, ze kterého bude odesílána pošta:
    - ***Automatické*** - cílový server bude určen podle nastavení ve vaší poštovní aplikaci; není třeba nic dále specifikovat
    - ***Pevně definovaný server*** - v tomto případě bude vždy použit konkrétní server. Do editačního řádku je třeba zadat adresu nebo jméno vašeho poštovního serveru. Jako jméno je možné použít jak doménový název (*např. imap.acme.com*), tak i IP adresu (*např. 123.45.67.89*). Pokud poštovní server používá nestandardní port, lze tento port zadat za jméno serveru oddělený dvojtečkou (*např. imap.acme.com:8200*). Standardní port pro IMAP komunikaci je 143.
- ***Doplňující nastavení*** - specifikuje další detailní parametry:
    - ***Lokální port*** - určuje, na kterém portu lze očekávat komunikaci z poštovní aplikace. Tento port je pak také nutné v poštovní aplikaci zadat jako port pro IMAP komunikaci.
    - ***Připojení*** - v této rozbalovací nabídce můžete specifikovat typ připojení (*standardní/ zabezpečené na vyhrazeném portu/zabezpečené na běžném portu*). Pokud zvolíte zabezpečené připojení, budou posílaná data kryptována a nebude možné jejich sledování nikým jiným. Tato funkce může být aktivována pouze v případě, že ji cílový poštovní server podporuje.
- ***Aktivace IMAP serveru*** - zapnutím/vypnutím položky máte možnost aktivovat či deaktivovat právě nastavený IMAP server

10.5.2. 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 určité skóre (*například podle toho, nakolik se obsah zprávy blíží textu, který lze považovat za spam*). Hodnotu úrovně citlivosti pro označení spamu lze nastavit buď přímo vepsáním 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*** - Emailové zprávy, u nichž se dá předpokládat charakter spamu, budou odfiltrovány. Je možné, že omylem dojde i k odfiltrování některých zpráv, jež nejsou spamového charakteru.

- ***Hodnota 60-79*** - Toto nastavení je již považováno za poměrně agresivní konfiguraci. Emailové 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

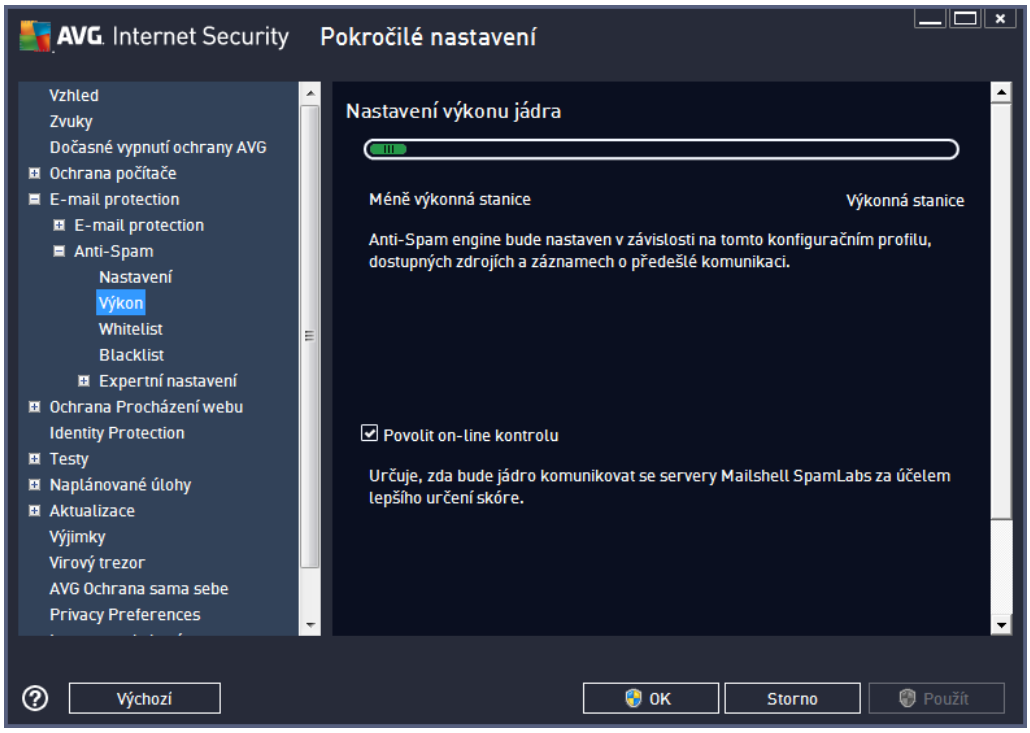
označen jako spam, bude automaticky přesunuta do složky pro nevyžádané zprávy. Tato možnost platí pouze pro poštovní program MS Outlook.

- ***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 účtu může být bez obav doručena.

- ***Změnit předmět 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 předmětu každé detekované e-mailové zprávy.

- ***Zeptat se před ohlášením nesprávného dotazu*** - Pokud jste během instalace potvrdili svou účast v projektu Anonymní sběr dat, 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 vyžadujícií vaše potvrzení.

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



Polohou posuvníku určete úroveň testovacího výkonu na ose ***Méně výkonná stanice*** / ***Výkonná stanice***.

- ***Méně výkonná stanice*** 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.

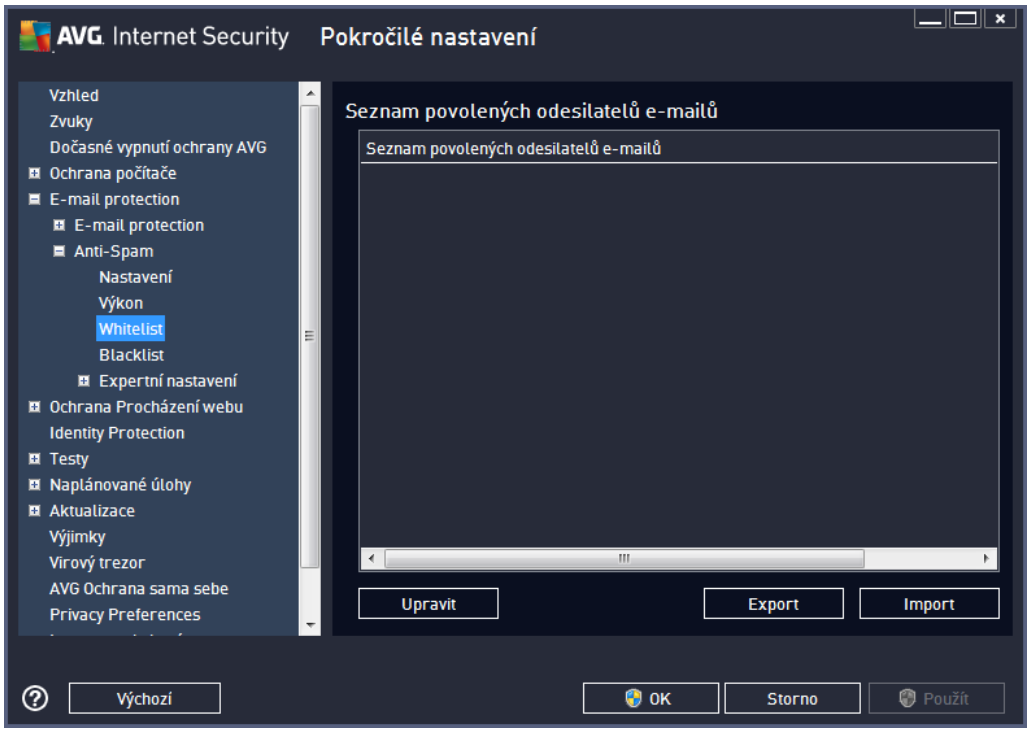
- ***Výkonná stanice*** spotřebuje velký objem paměti. Během testovacího procesu budou k identifikaci

spamu použity následující parametry: pravidla a spamové databáze, základní a pokročilé nastavení, IP adresy spammerů a spamové databáze.

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 měnit. Změnu parametrů nastavení výkonu jádra lze doporučit výhradně znalým a zkušeným uživatelům!

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



V editačním rozhraní máte možnost sestavit seznam odesilatelů, 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: přímým vložením jednotlivých adres nebo jednorázovým importem celého seznam.

Ovládací tlačítka dialogu

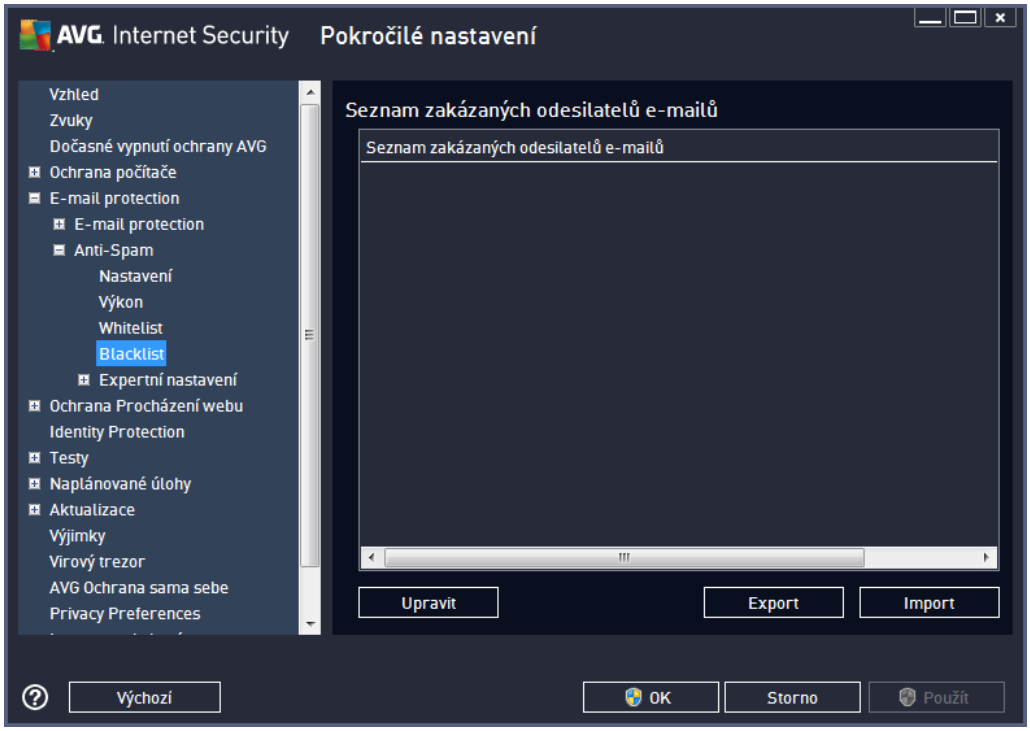
K dispozici jsou vám tato ovládací tlačítka:

- ***Upravit*** - stiskem tohoto tlačítka otevřete dialog, v němž můžete manuálně přidávat adresy ze seznamu (*můžete také použít jednorázově 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 odesilatelů, 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: přímým vložením jednotlivých adres nebo jednorázovým importem celého seznam.

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 jednorázově 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 nějž import provádíte, musí být ve formátu prostého textu a obsah musí být rozdělen tak, že každý řádek obsahuje pouze jedinou položku (*adresu nebo doménové jméno*).

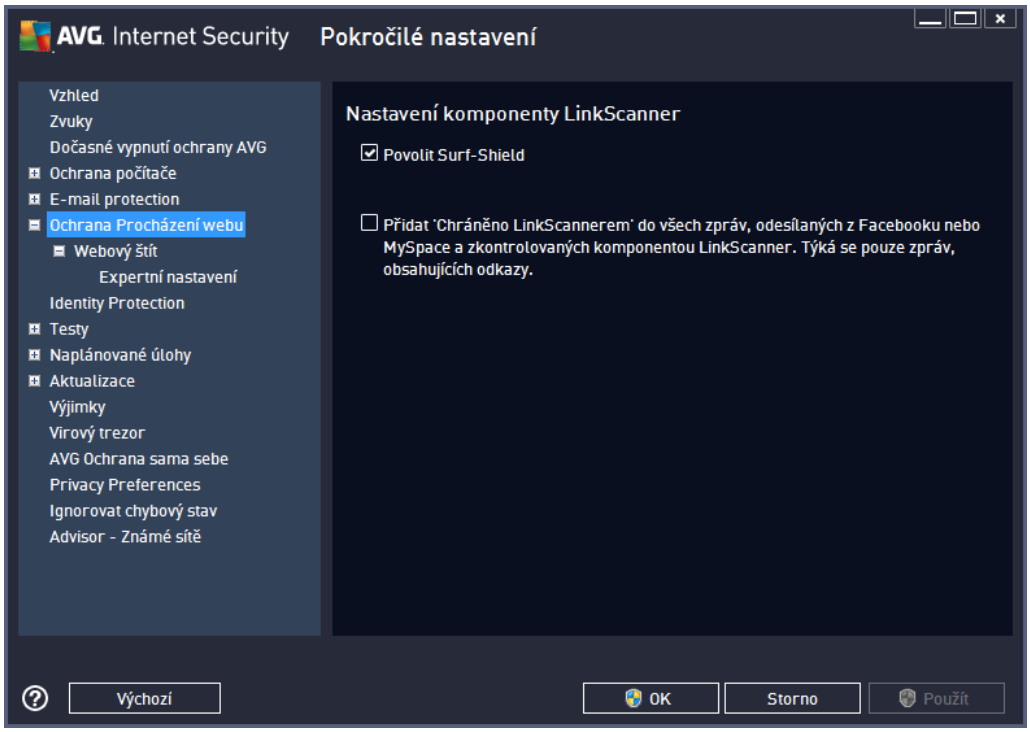
Větev Expertní nastavení obsahuje rozsáhlé možnosti nastavení komponenty Anti-Spam. Tato nastavení jsou určena výhradně pokročilým uživatelům, jako jsou správci sítí, kteří potřebují antispamovou ochranu nastavit do detailů pro co nejlepší ochranu e-mailových serverů. Z tohoto důvodu není v dialozích 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 měnit konfiguraci služby Anti-Spam na úrovni vysoce 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. Nastavit můžete tyto parametry:

- ***Filtrování*** - seznam jazyků, seznam zemí, povolené IP adresy, blokované IP adresy, blokované země, blokované znakové sady, falešní odesilatelé
- ***RBL*** - RBL servery, práh, časový limit, maximum IP adres, ignorované IP adresy
- ***Internetové připojení*** - časový limit, proxy server, autentifikace proxy

10.6. Ochrana procházení webu

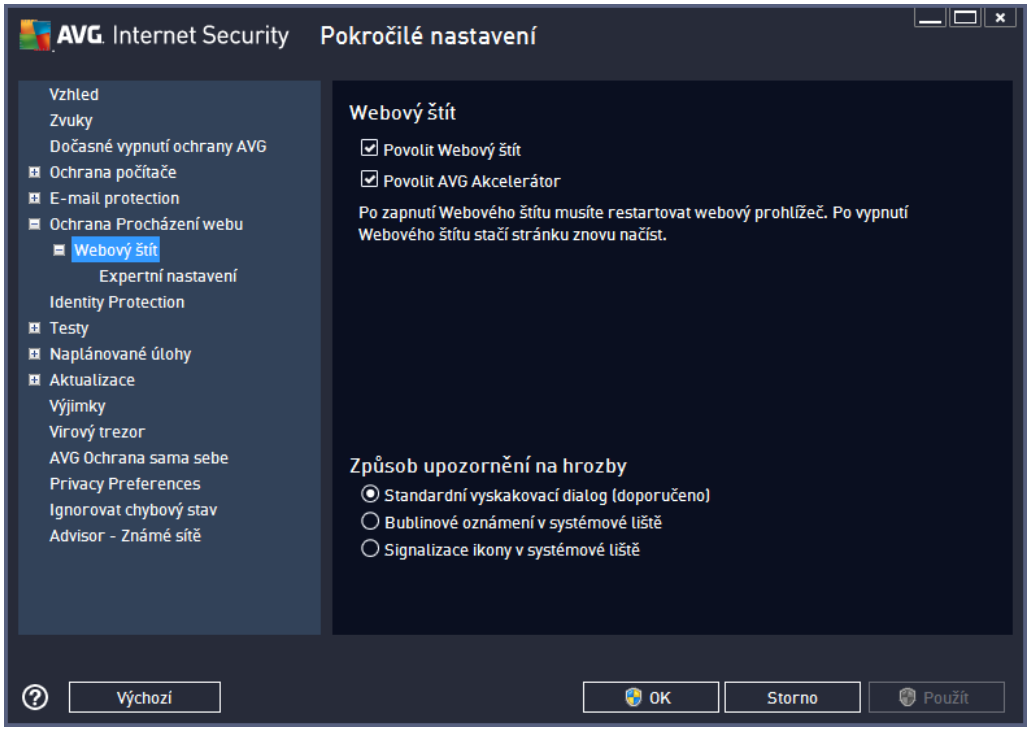
Dialog ***Nastavení komponenty LinkScanner*** umožňuje zapnout či vypnout následující funkce:



- ***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.

- ***Přidat 'Chráněno LinkScannerem'...*** - (*ve výchozím nastavení vypnuto*): potvrzením této volby zajistíte, že veškeré zprávy odesílané ze sociálních sítí Facebook či MySpace, jež obsahují aktivní odkazy do webu, budou po zkontrolování bezpečnosti těchto odkazů označeny za zkontrolované službou LinkScanner.

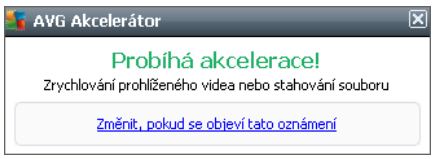
10.6.1. Webový štít



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

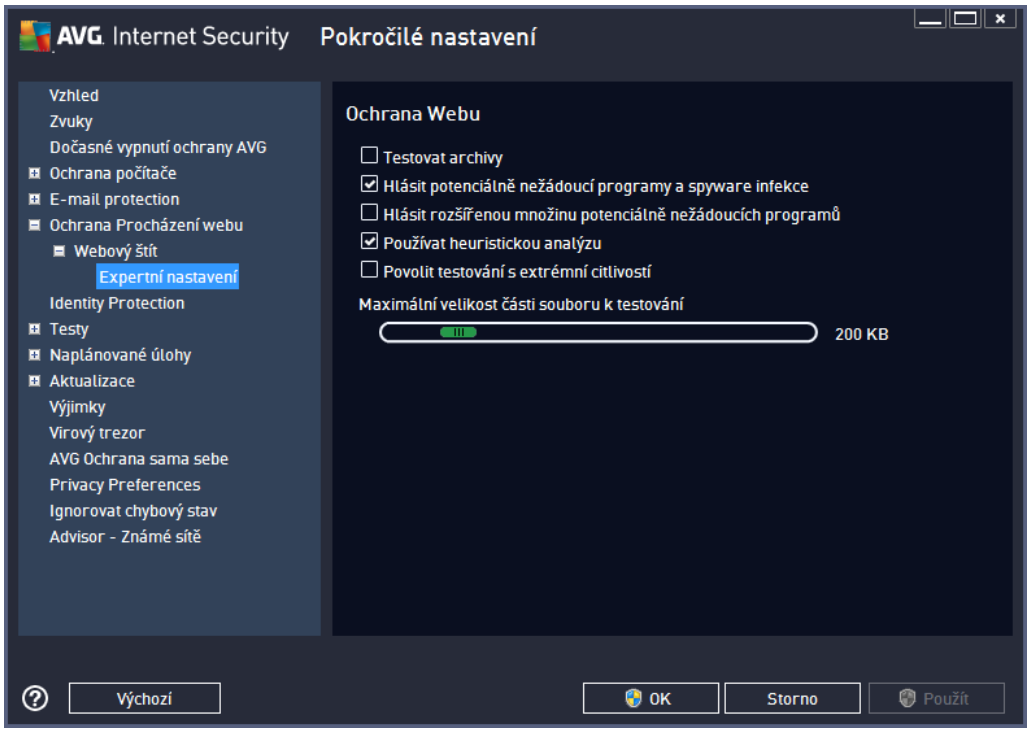
- ***Povolit Webový štít*** *(ve výchozím nastavení zapnuto)* - Označením položky aktivujete/deaktivujete službu ***Webový štít***. Pokročilé nastavení této komponenty pak najdete v podkategorii Ochrana webu.

- ***Povolit AVG Akcelerátor*** *(ve výchozím nastavení zapnuto)* - Označením položky aktivujete/deaktivujete službu AVG Akcelerátor. AVG Accelerator umožňuje plynulé přehrávání videa v režimu online a obecně urychluje stahování. O tom, že je proces akcelerace videa či stahování momentálně aktivní, budete informováni prostřednictvím pop-up okna nad systémovou lištou:



Způsob upozornění na hrozby

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



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

- ***Povolit ochranu webu*** - touto volbou potvrzujete, že v rámci služby ***Webový štít*** si přejete, aby byla prováděna kontrola obsahu navštěvovaných www stránek. Za předpokladu, že je tato volba zapnuta (*výchozí nastavení*), můžete dále povolit nebo vypnout tyto volby:
    - ***Testovat archívy*** - (*ve výchozím nastavení vypnuto*) kontrola obsahu archivu, jež mohou být přítomny na zobrazované www stránce.
    - ***Hlásit potenciálně nežádoucí programy a spyware infekce*** - (*ve výchozím nastavení zapnuto*) kontrola přítomnosti potenciálně nežádoucích programů (*spustitelné programy, které mohou fungovat jako spyware nebo adware*). Zaškrtnutím tohoto políčka aktivujete testování přítomnosti spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány vědomě a se souhlasem uživatele. Doporučujeme nicméně ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
    - ***Hlásit rozšířenou množinu potenciálně nežádoucích programů*** - (*ve výchozím nastavení vypnuto*) zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v původní podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.
    - ***Používat heuristickou analýzu*** - (*ve výchozím nastavení zapnuto*) kontrola obsahu zobrazované www stránky pomocí metody heuristické analýzy (*dynamická emulace instrukcí testovaného objektu v prostředí virtuálního počítače*).

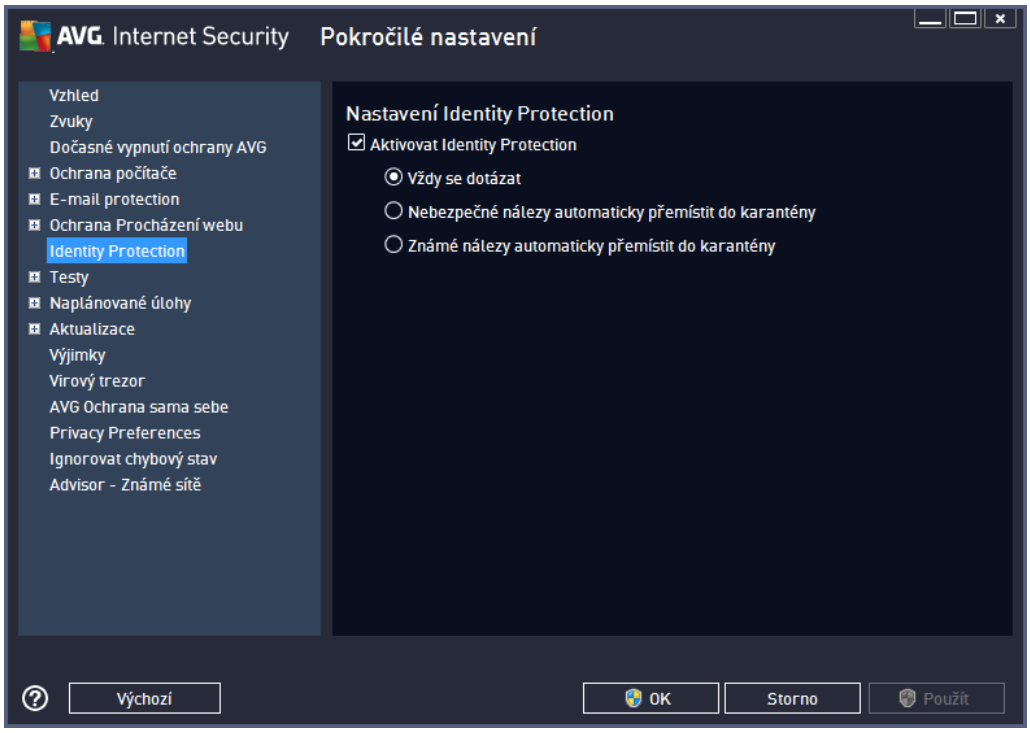
- **Povolit testování s extrémní citlivostí** - (*ve výchozím nastavení vypnuto*) ve specifických situacích (*například při podezření na infekci starším typem viru*) můžete zvolit tuto metodu testování, která aktivuje nejdůkladnější testovací algoritmy a velmi podrobně prověří naprosto všechny oblasti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

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

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

10.7. Identity Protection

Identity Protection je komponentou, která průběžně a v reálném čase zajišťuje ochranu před různými druhy malware a virů, a to na bázi identifikace specifického chování těchto typů aplikací *(podrobný popis fungování komponenty najdete v kapitole Identita)*. Dialog **Nastavení Identity Protection** umožňuje zapnout či vypnout některé základní vlastnosti komponenty *Identita*:



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

Důrazně doporučujeme ponechat komponentu zapnutou!

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

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

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

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

10.8. Testy

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

- ***Test celého počítače*** - výrobcem nastavený standardní test

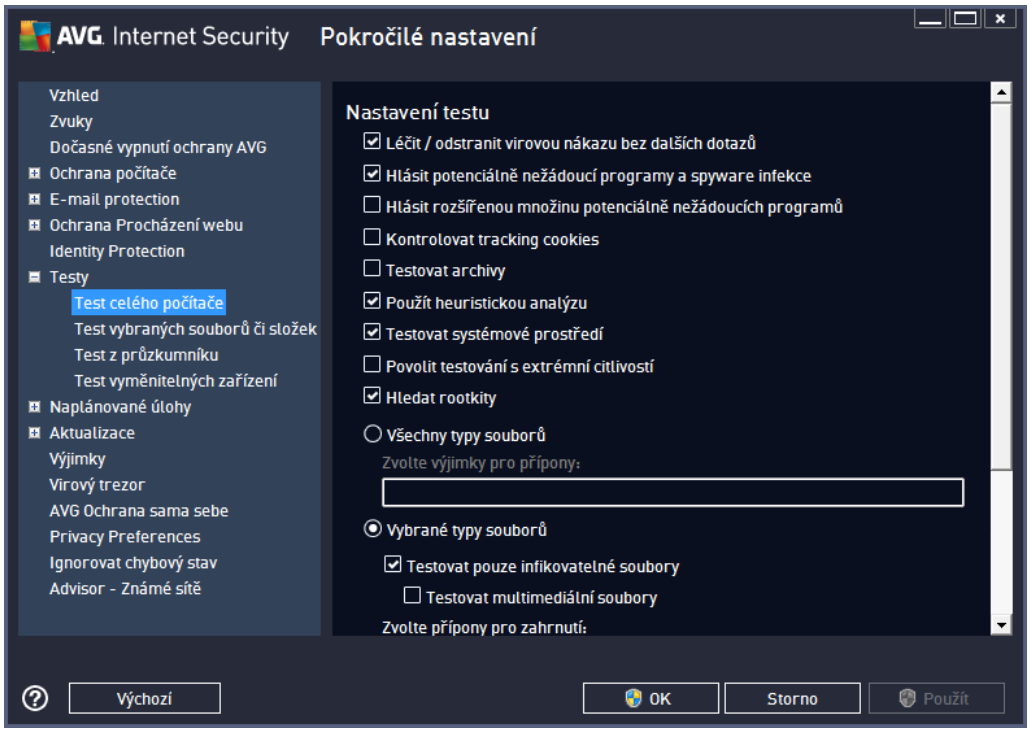
- ***Test vybraných souborů či složek*** - výrobcem nastavený standardní test s možností definovat oblasti testování

- ***Test z průzkumníku*** - specifický test spouštěný nad zvolenými objekty přímo v prostředí Windows

- ***Test vyměnitelných zařízení*** - specifický test vyměnitelných zařízení připojených v danou chvíli k Vašemu PC

10.8.1. Test celého počítače

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



Nastavení testu

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

- ***Léčit / odstranit virovou nákazu bez dalších dotazů*** (*ve výchozím nastavení zapnuto*) - 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 testování přítomnosti spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány vědomě a se souhlasem uživatele. Doporučujeme nicméně ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.

- ***Hlásit rozšířenou množinu potenciálně nežádoucích programů*** (*ve výchozím nastavení vypnuto*) - zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v původní podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.

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

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

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

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

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

- ***Hledat rootkity*** (*ve výchozím nastavení zapnuto*) - Parametr služby Anti-Rootkit prohledává počítač na přítomnost rootkitů, tedy programů a technologií, které dokáží maskovat přítomnost malware v počítači. Dojde-li k nálezu rootkitu, nemusí to nutně znamenat, že je počítač infikovaný. V některých případech mohou být rootkity použity jako ovladače nebo části korektních aplikací.

Dále se můžete rozhodnout, zda si přejete testovat

- ***Všechny typy souborů*** - přičemž máte zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou (*po uložení se čárky změní na středníky*);

- ***Vybrané typy souborů*** - můžete se rozhodnout, že chcete, aby se testy spouštěly pouze nad soubory, které lze považovat za infikovatelné (*soubory, které nemohou být infekcí zasaženy, se testovat nebudou - například prosté textové soubory nebo některé nespustitelné soubory*), a to včetně multimediálních souborů (*video, audio soubory - ponecháte-li tuto položku neoznačenou, výrazně se tím zkrátí čas testování, jelikož multimediální soubory jsou obvykle poměrně velké, ale pravděpodobnost infekce je u nich velmi nízká*). I zde můžete určit výjimky a pomocí seznamu přípon definovat, které soubory mají být testovány za všech okolností.

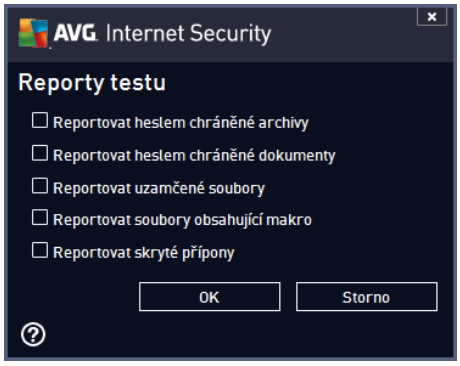
- U položky ***Testovat soubory bez přípon*** pak rozhodněte, zda se mají testovat i soubory se skrytou či neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme , abyste se tohoto nastavení podrželi, pokud nemáte skutečný důvod jej měnit. Soubory bez přípon jsou obecně vysoce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

Nastavit, jak rychle probíhá test

V této sekci pak můžete nastavit požadovanou rychlost testování v závislosti na zátěži systémových zdrojů. Ve výchozím nastavení je tato hodnota nastavena *dle činnosti uživatele*, což odpovídá střední úrovni využití systémových prostředků.. Pokud se rozhodnete pro spuštění rychlého testu, proběhne test v kratším čase, ale po dobu jeho běhu bude výrazně zvýšena zátěž systémových zdrojů, takže vaše práce na počítači bude obtížnější (*tato varianta je vhodná pro situaci, kdy je počítač spuštěn, ale nikdo na něm aktuálně nepracuje*). Naopak, prodloužením doby testu snížíte zátěž systémových zdrojů a vaše práce na počítači nebude téměř ovlivněna, test však bude probíhat po delší dobu.

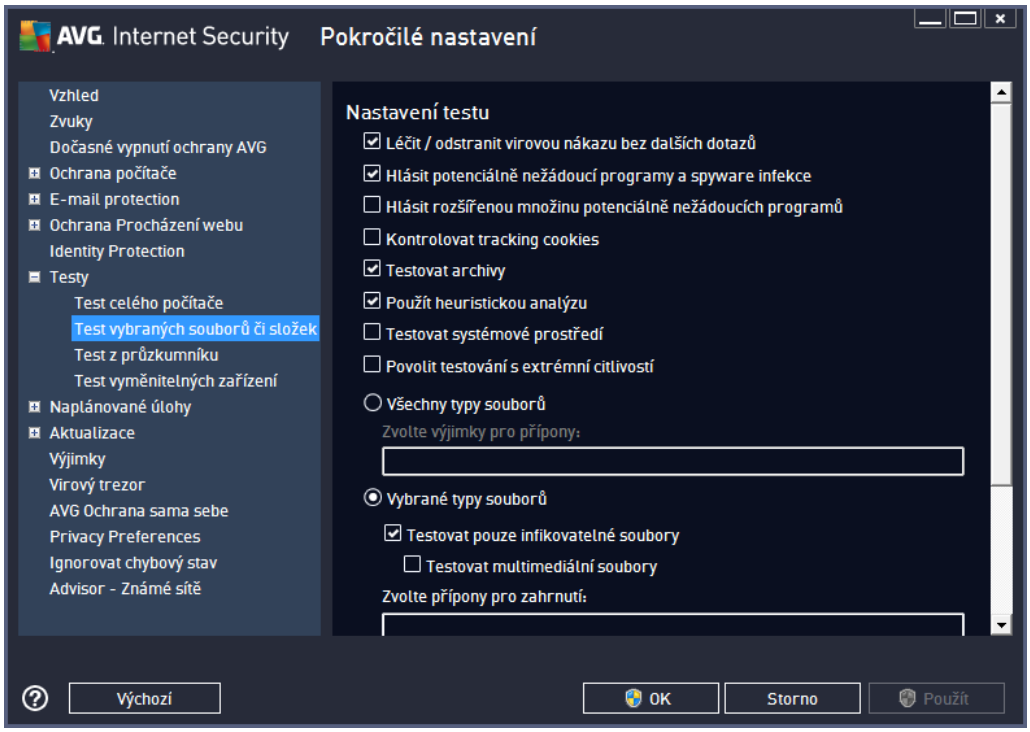
Nastavit další reporty testů ...

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



10.8.2. Test vybraných souborů či složek

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

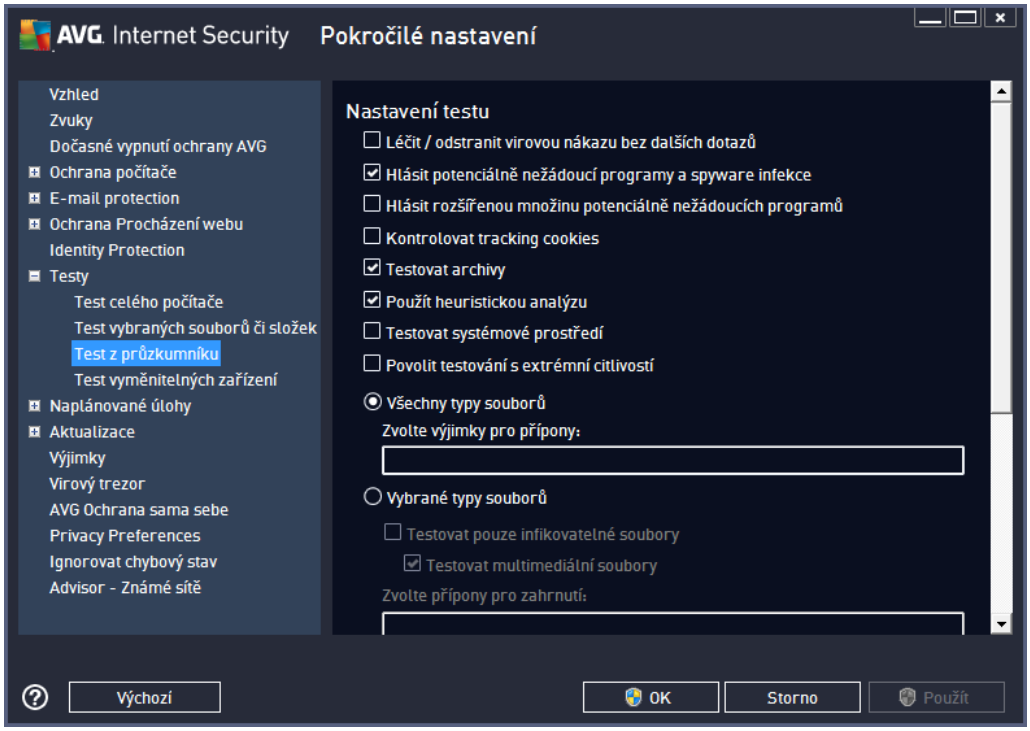


Veškeré parametry nastavené v tomto konfiguračním dialogu se vztahují pouze na ty oblasti vašeho počítače, které jste vybrali pro testování v rámci Testu vybraných souborů či složek!

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

10.8.3. Test z průzkumníku

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



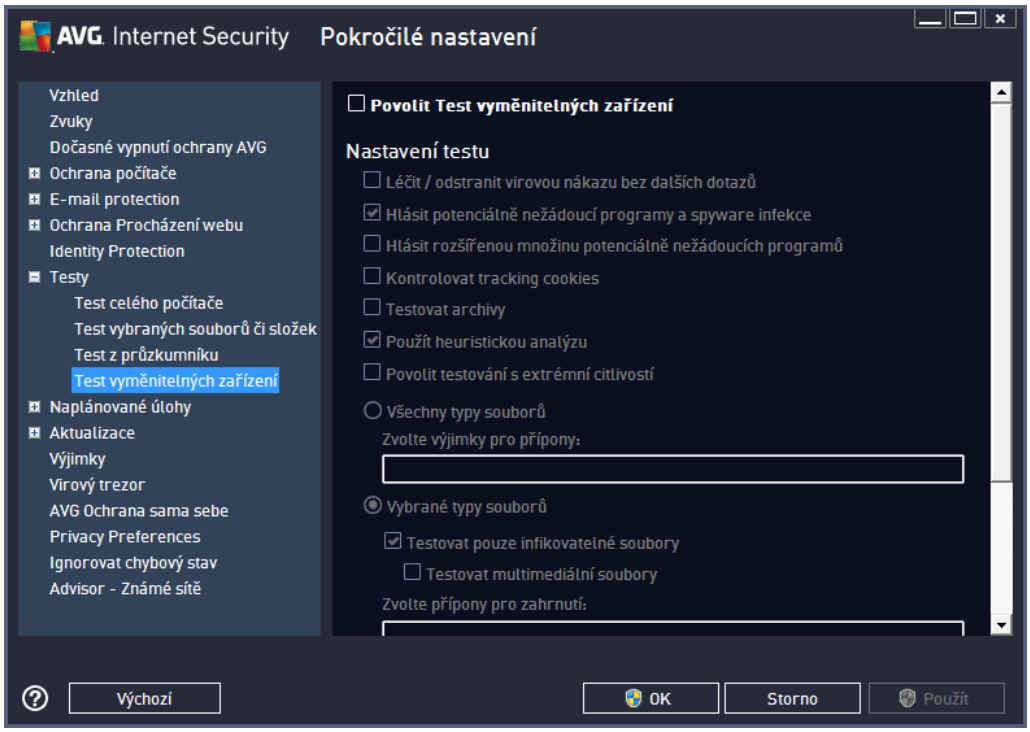
Veškeré možnosti editace parametrů testu jsou totožné s editací parametrů Testu celého počítače. Odlišné je pouze výchozí nastavení těchto parametrů (*například Test celého počítače ve výchozím nastavení neprovádí kontrolu archivů, ale provádí kontrolu systémového prostředí, zatímco u Testu z průzkumníku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

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

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

10.8.4. Test vyměnitelných zařízení

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



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

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

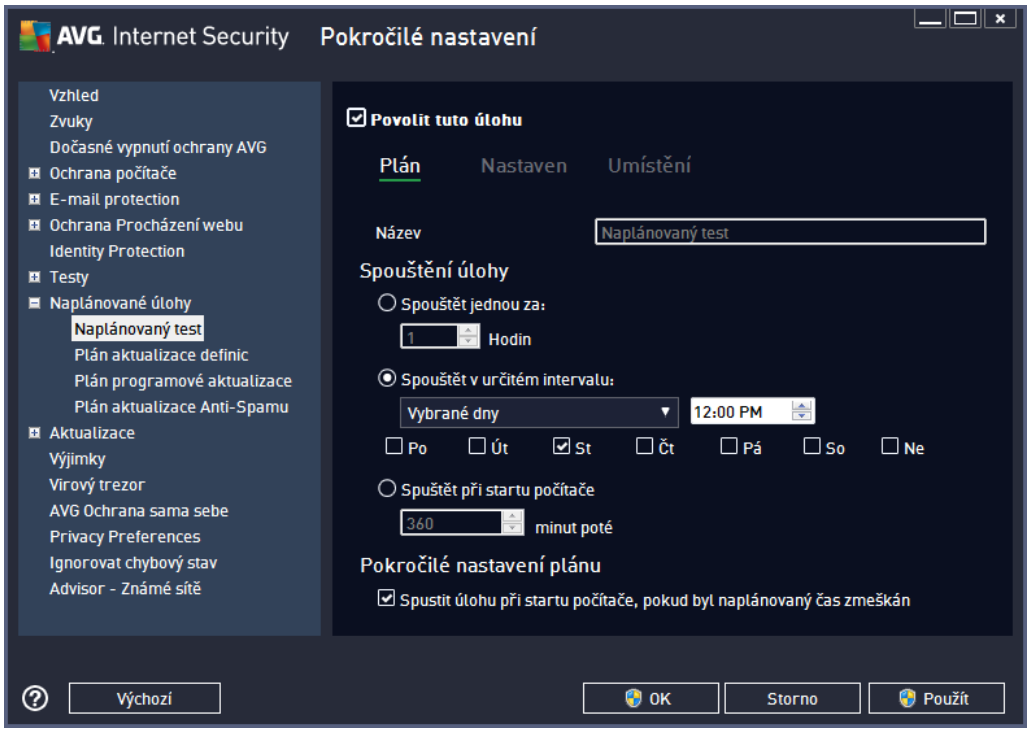
10.9. Naplánované úlohy

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

- Naplánovný test
- Plánu aktualizace definic
- Plánu programové aktualizace
- Plánu aktualizace Anti-Spamu

10.9.1. Naplánovaný test

Parametry naplánovaného testu můžete editovat (*případně nastavit plán nový*) na třech záložkách. Na každé záložce máte nejprve možnost jednoduchým označením položky ***Povolit tuto úlohu*** naplánovaný test (*dočasně*) deaktivovat, a později podle potřeby znovu použít.



V textovém poli ***Název*** (*toto pole je u všech předem nastavených plánů deaktivováno*) je uvedeno jméno přiřazené právě nastavenému testu. U nově vytvářených plánů (*nový plán vytvoříte tak, že kliknete pravým tlačítkem myši nad položkou* ***Naplánovaný test*** *v levém navigačním menu*) bude textové pole aktivní a dostanete možnost definovat své vlastní pojmenování plánu. Snažte se vždy používat stručné, popisné a případné názvy, abyste se později v naplánovaných úlohách snadněji vyznali.

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

V tomto dialogu můžete dále definovat tyto parametry testu:

Spouštění úlohy

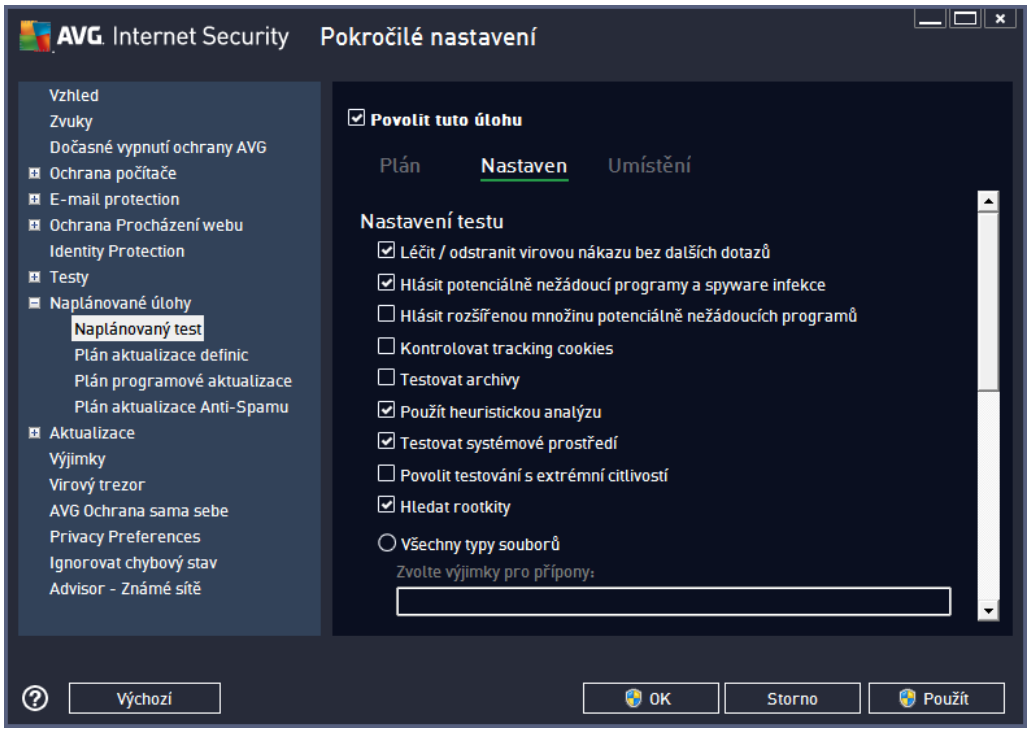
V této sekci dialogu určete, v jakých časových intervalech má být nově naplánovaný test spouštěn. Časové určení můžete zadat buďto opakovaným spuštěním testu po uplynutí určené doby (***Spouštět jednou za***) nebo stanovením přesného data a času (***Spouštět v určitém intervalu***), případně určením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

Pokročilé nastavení plánu

Tato sekce umožňuje definovat podmínky, kdy má či nemá být test spuštěn, jestliže je počítač v úsporném

režimu nebo zcela vypnutý a naplánovaný test spuštění testu byl zmeškán. O automatickém spuštění testu budete v určeném čase informováni prostřednictvím pop-up okna nad ikonou AVG na systémové liště:

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



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

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

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

- ***Hlásit rozšířenou množinu potenciálně nežádoucích programů*** (*ve výchozím nastavení vypnuto*): zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v původní podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.

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

- ***Testovat archivy*** (*ve výchozím nastavení vypnuto*): parametr definuje, že test má kontrolovat všechny soubory, a to i takové, které jsou zabaleny v některém typu archivu, například ZIP, RAR, ...

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

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

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

- ***Hledat rootkity*** (*ve výchozím nastavení zapnuto*): parametr služby Anti-Rootkit prohledává počítač na přítomnost rootkitů, tedy programů a technologií, které dokáží maskovat přítomnost malware v počítači. Dojde-li k nálezu rootkitu, nemusí to nutně znamenat, že je počítač infikovaný. V některých případech mohou být rootkity použity jako ovladače nebo části korektních aplikací.

Dále se můžete rozhodnout, zda si přejete testovat

- ***Všechny typy souborů*** - přičemž máte zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou (*po uložení se čárky změní na středníky*);

- ***Vybrané typy souborů*** - můžete se rozhodnout, že chcete, aby se testy spouštěly pouze nad soubory, které lze považovat za infikovatelné (*soubory, které nemohou být infekcí zasaženy, se testovat nebudou - například prosté textové soubory nebo některé nespustitelné soubory*), a to včetně multimediálních souborů (*video, audio soubory - ponecháte-li tuto položku neoznačenou, výrazně se tím zkrátí čas testování, jelikož multimediální soubory jsou obvykle poměrně velké, ale pravděpodobnost infekce je u nich velmi nízká*). I zde můžete určit výjimky a pomocí seznamu přípon definovat, které soubory mají být testovány za všech okolností.

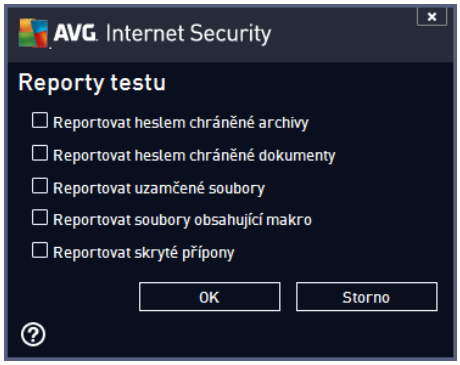
- U položky ***Testovat soubory bez přípon*** pak rozhodněte, zda se mají testovat i soubory se skrytou či neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme , abyste se tohoto nastavení podrželi, pokud nemáte skutečný důvod jej měnit. Soubory bez přípon jsou obecně vysoce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

Nastavit, jak rychle probíhá test

V této sekci pak můžete nastavit požadovanou rychlost testování v závislosti na zátěži systémových zdrojů. Ve výchozím nastavení je tato hodnota nastavena *dle činnosti uživatele*. Pokud se rozhodnete pro spuštění rychlého testu, proběhne test v kratším čase, ale po dobu jeho běhu bude výrazně zvýšena zátěž systémových zdrojů, takže vaše práce na počítači bude obtížnější (*tato varianta je vhodná pro situaci, kdy je počítač spuštěn, ale nikdo na něm aktuálně nepracuje*). Naopak, prodloužením doby testu snížíte zátěž systémových zdrojů a vaše práce na počítači nebude téměř ovlivněna, test však bude probíhat po delší dobu.

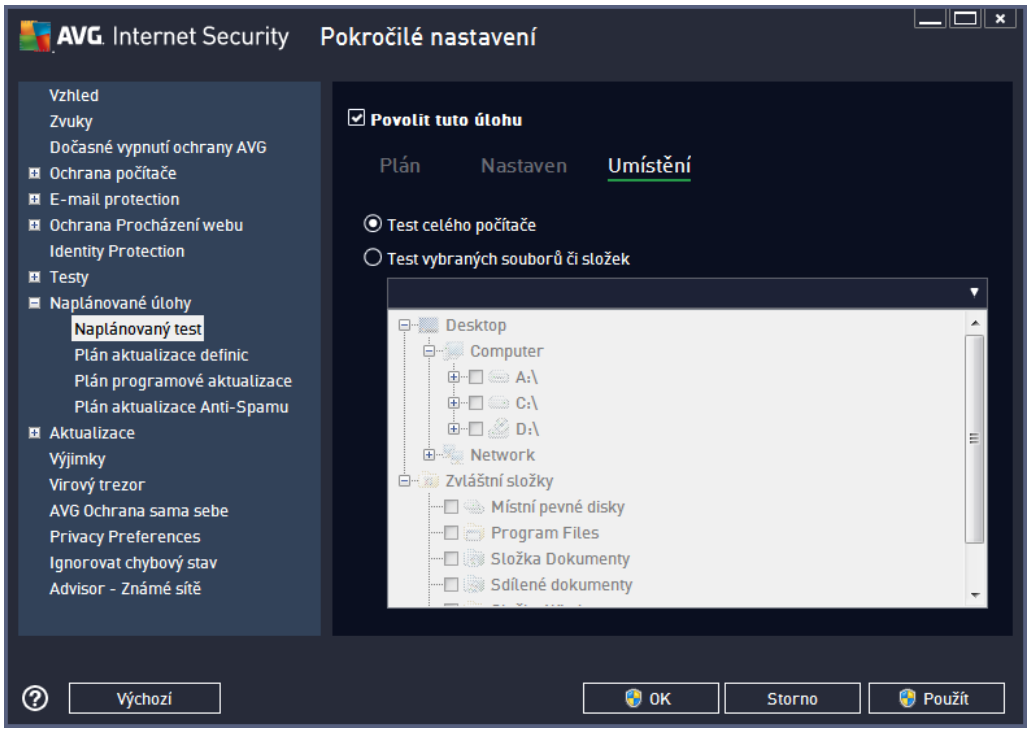
Nastavit další reporty testů

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



Možnosti vypnutí počítače

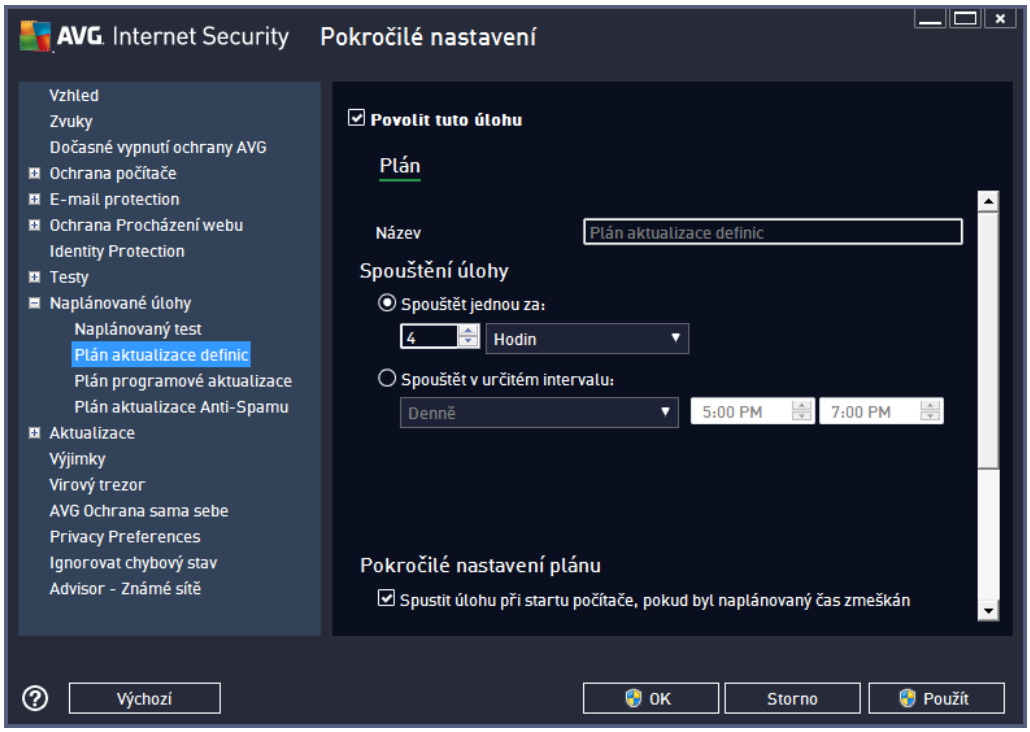
V sekci ***Možnosti vypnutí počítače*** můžete zvolit, zda má být po dokončení spuštěného testu počítač automaticky vypnut. Pokud potvrdíte tuto volbu (***Vypnout počítač po dokončení testování***), aktivuje se současně další možnost, jejímž zapnutím vynutíte vypnutí počítače i za situace, že počítač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



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

10.9.2. Plán aktualizace definic

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



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

Spouštění úlohy

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

Pokročilé nastavení plánu

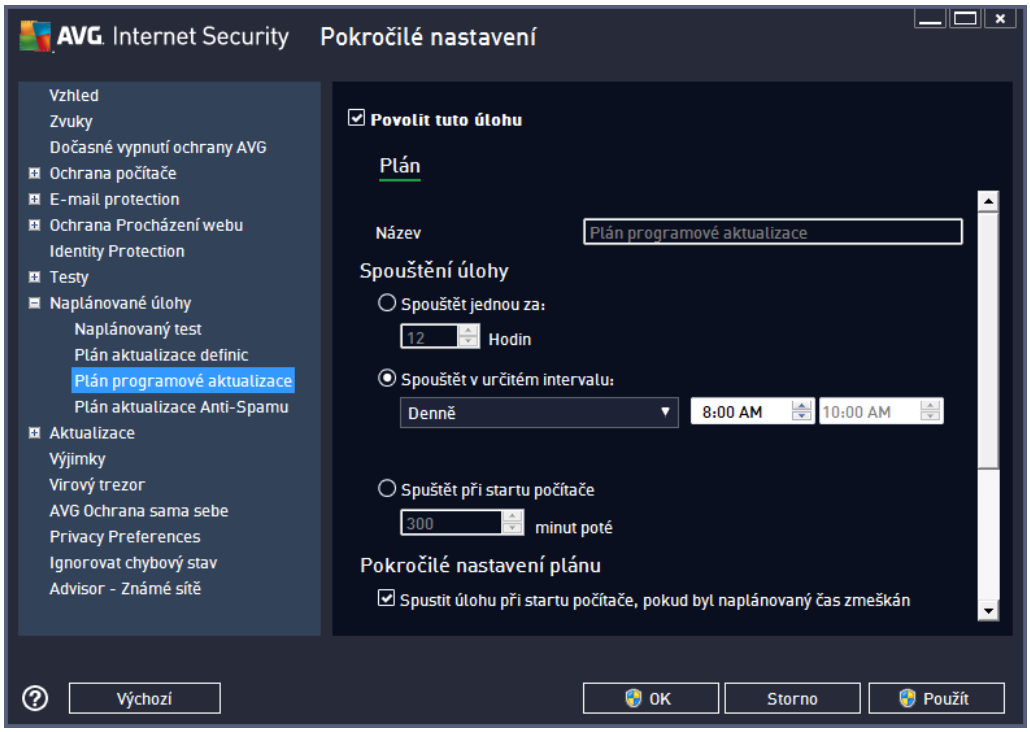
Tato sekce umožňuje definovat podmínky, kdy má či nemá být aktualizace definic spuštěna, jestliže je počítač v úsporném režimu nebo zcela vypnutý a naplánovaný čas spuštění aktualizace byl zmeškán.

Další nastavení aktualizace

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

10.9.3. Plán programové aktualizace

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



V textovém poli ***Název*** (*toto pole je u všech předem nastavených plánů deaktivováno*) je uvedeno jméno přiřazené právě nastavenému plánu programové aktualizace.

Spouštění úlohy

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

Pokročilé nastavení plánu

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

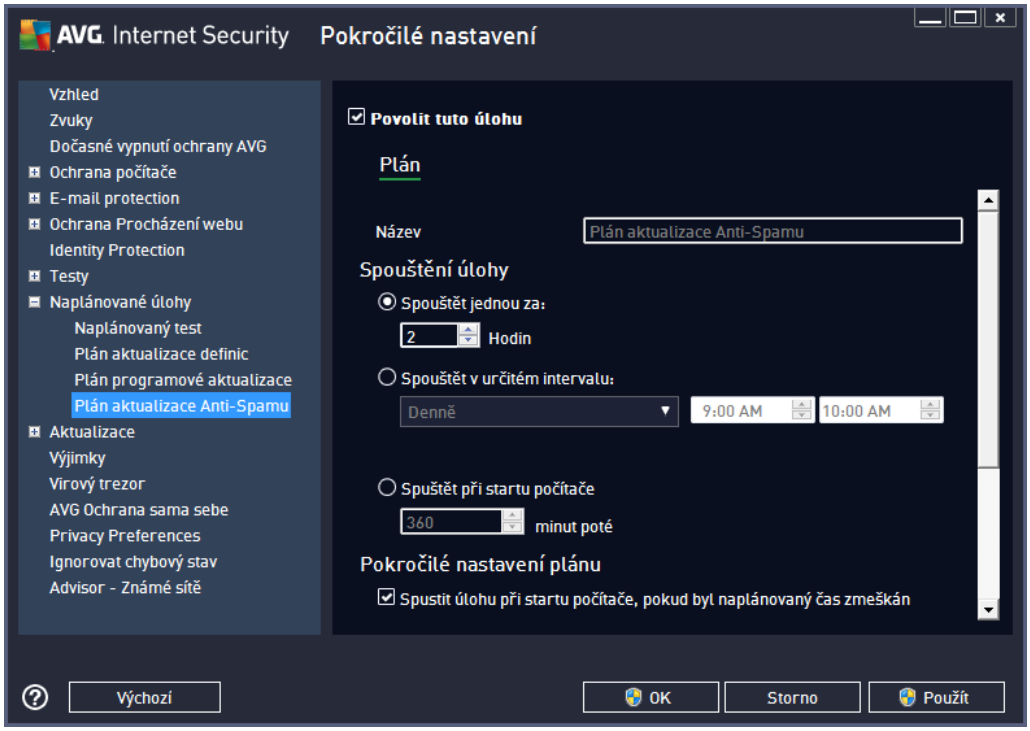
Další nastavení aktualizace

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

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

10.9.4. Plán aktualizace Anti-Spamu

V případě ***skutečně nutné*** potřeby můžete prostým vypnutím položky ***Povolit tuto úlohu*** deaktivovat přednastavený plán aktualizace služby Anti-Spam, a později jej znovu aktivovat:



V tomto dialogu můžete nastavit přesnější parametry plánu aktualizace. V textovém poli ***Název*** (*toto pole je u všech předem nastavených plánů deaktivováno*) je uvedeno jméno přiřazené právě nastavenému plánu aktualizace služby Anti-Spam.

Spouštění úlohy

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

Pokročilé nastavení plánu

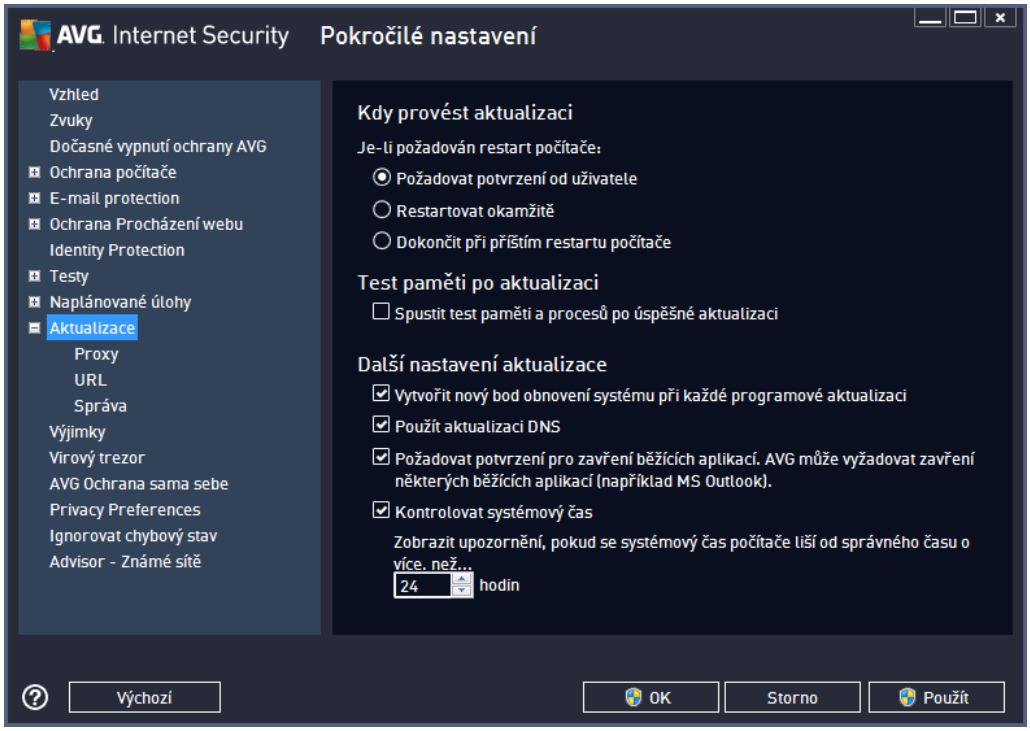
Tato sekce umožňuje definovat podmínky, kdy má či nemá být aktualizace Anti-Spamu spuštěna, jestliže je počítač v úsporném režimu nebo zcela vypnutý a naplánovaný čas spuštění aktualizace byl zmeškán.

Další nastavení aktualizace

Volbou položky ***Provést aktualizaci znovu po připojení k Internetu*** zajistíte, že pokud dojde během aktualizace 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)*.

10.10. Aktualizace

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



Kdy provést aktualizaci

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

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

Test paměti po aktualizaci

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

Další nastavení aktualizace

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

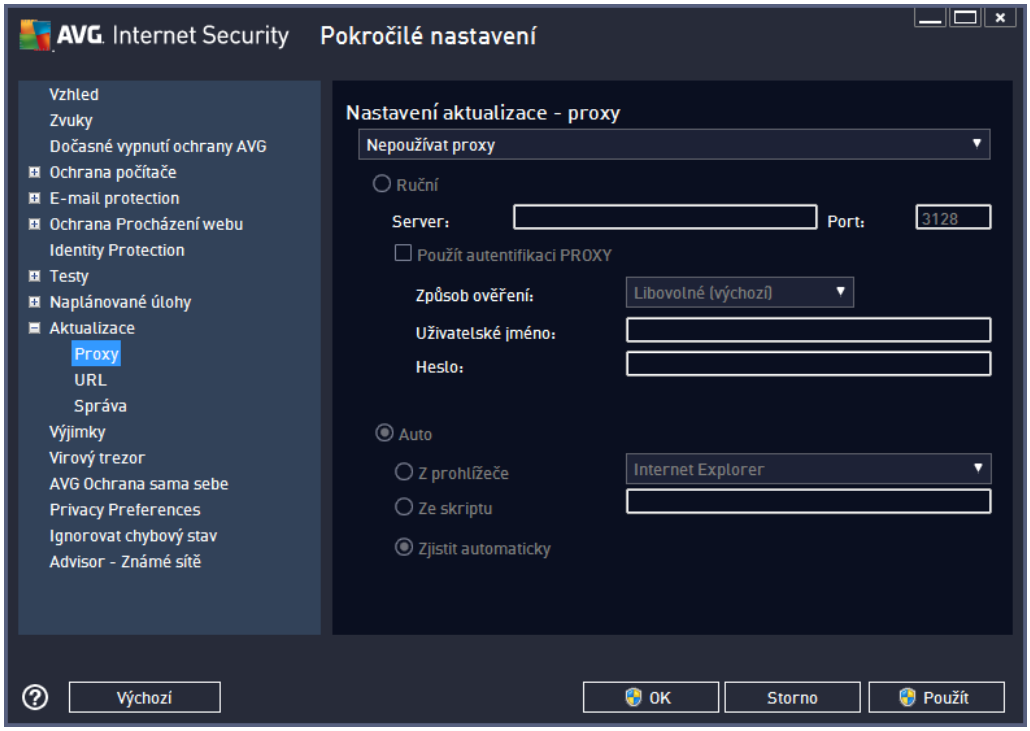
- ***Vytvořit nový bod pro obnovení systému ...*** - před každým spuštěním programové aktualizace AVG je vytvořen takzvaný systémový bod pro obnovení systému. V případě, že aktualizační proces nebude z nějakého důvodu dokončen a váš operační systém bude ohrožen, můžete za pomoci tohoto zálohovacího bodu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

- ***Použít aktualizaci DNS*** (*ve výchozím nastavení zapnuto*) - pokud je tato položka označena, při spuštění aktualizace **AVG Internet Security 2013** vyhledá na DNS serveru informaci o aktuální verzi virové databáze a aktuální verzi programu a následně stáhne pouze nejmenší nezbytně nutné aktualizační soubory. Tím se sníží celkový objem stahovaných dat a urychlí proces aktualizace.

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

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

10.10.1. Proxy



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

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

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

Manuální nastavení

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

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

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

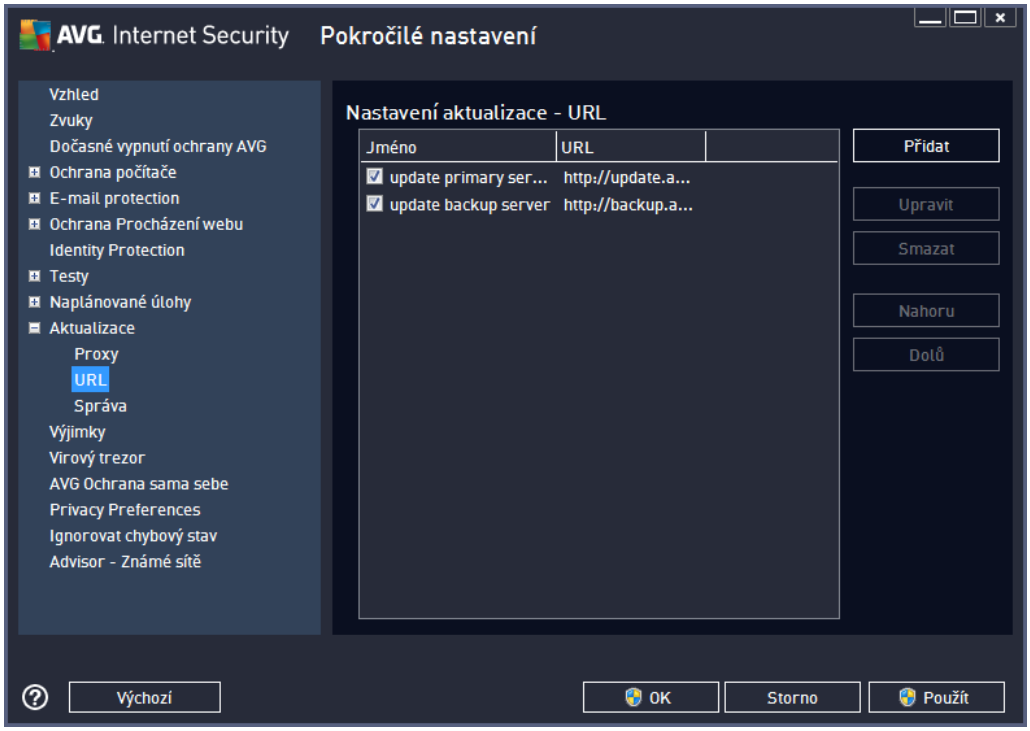
Automatické nastavení

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

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

10.10.2. URL

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



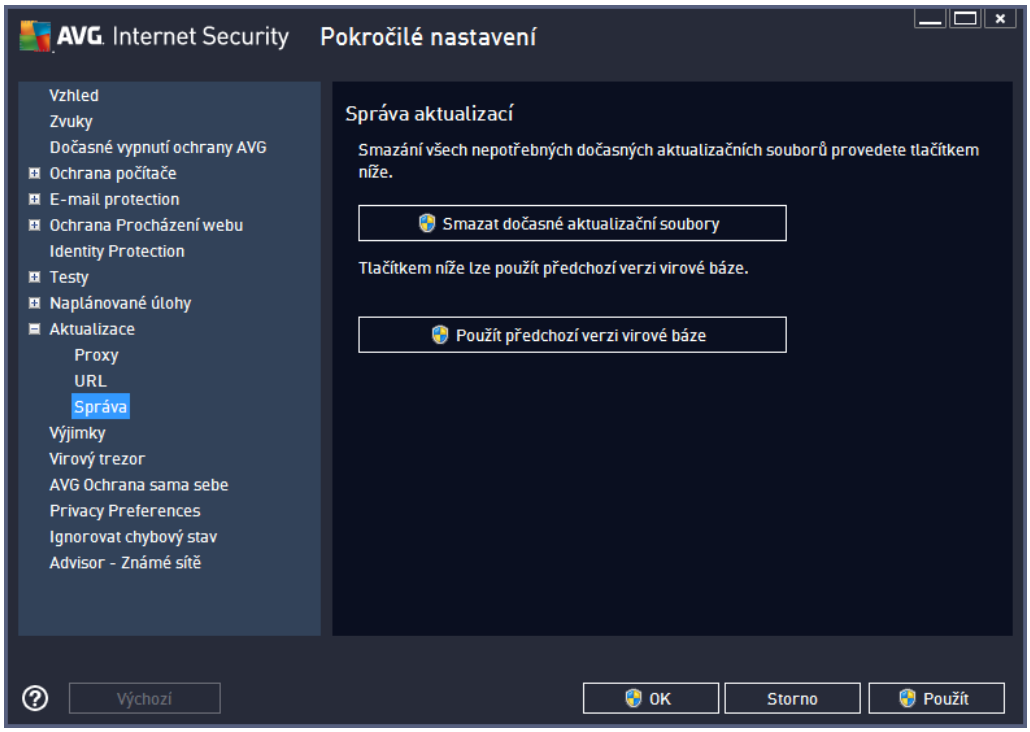
Ovládací tlačítka dialogu

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

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

10.10.3. Správa

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



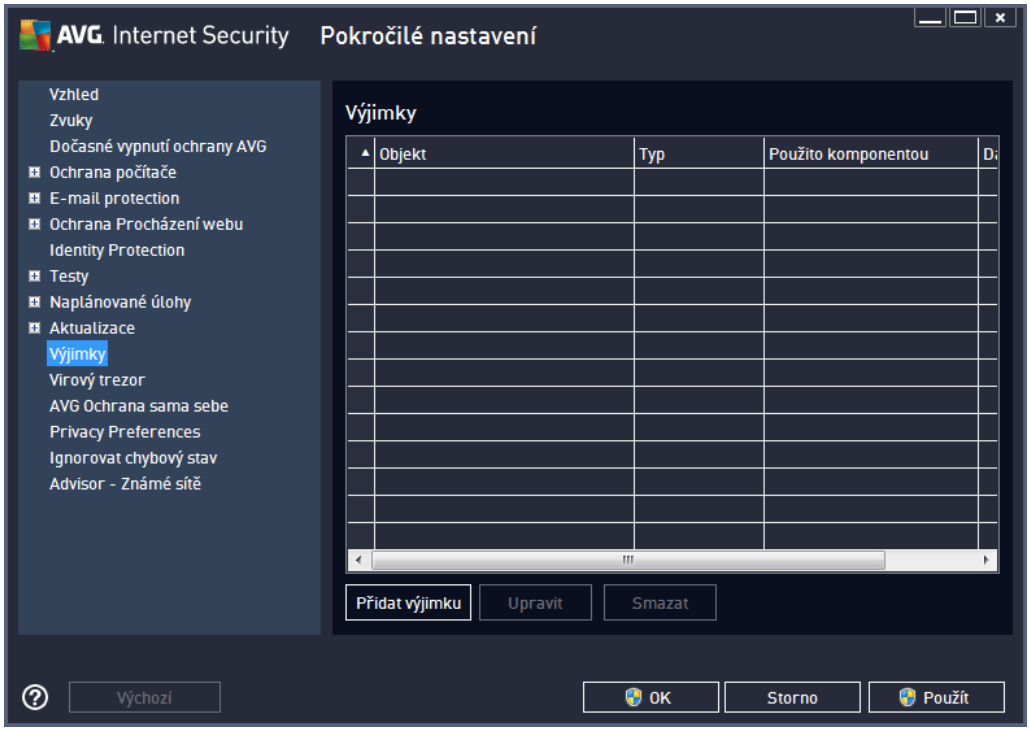
- ***Smazat dočasné aktualizační soubory*** - tímto tlačítkem odstraníte ze svého pevného disku všechny již nepotřebné soubory aktualizací (*ve výchozím nastavení správy aktualizačních souborů se tyto uchovávají po dobu po 30 dní*)

- ***Použít předchozí verzi virové báze*** – tímto tlačítkem odstraníte ze svého pevného disku poslední verzi virové databáze a vrátíte se tak k předchozí uložené verzi (*nová verze virové báze bude pochopitelně součástí další aktualizace*)

10.11. Výjimky

V dialogu ***Výjimky*** můžete definovat výjimky, to jest položky, které budou z kontroly programem **AVG Internet Security 2013** vyňaty. Výjimku jmůžete definovat například v situaci, kdy AVG opakovaně detekuje určitý program nebo soubor jako hrozbu nebo blokuje webovou stránku, o níž bezpečně víte, že ji lze považovat za bezpečnou. Pak přidáte dotyčný soubor nebo webovou stránku na seznam výjimek a AVG tyto objekty nadále nebude reportovat jako možný zdroj nákazy.

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



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

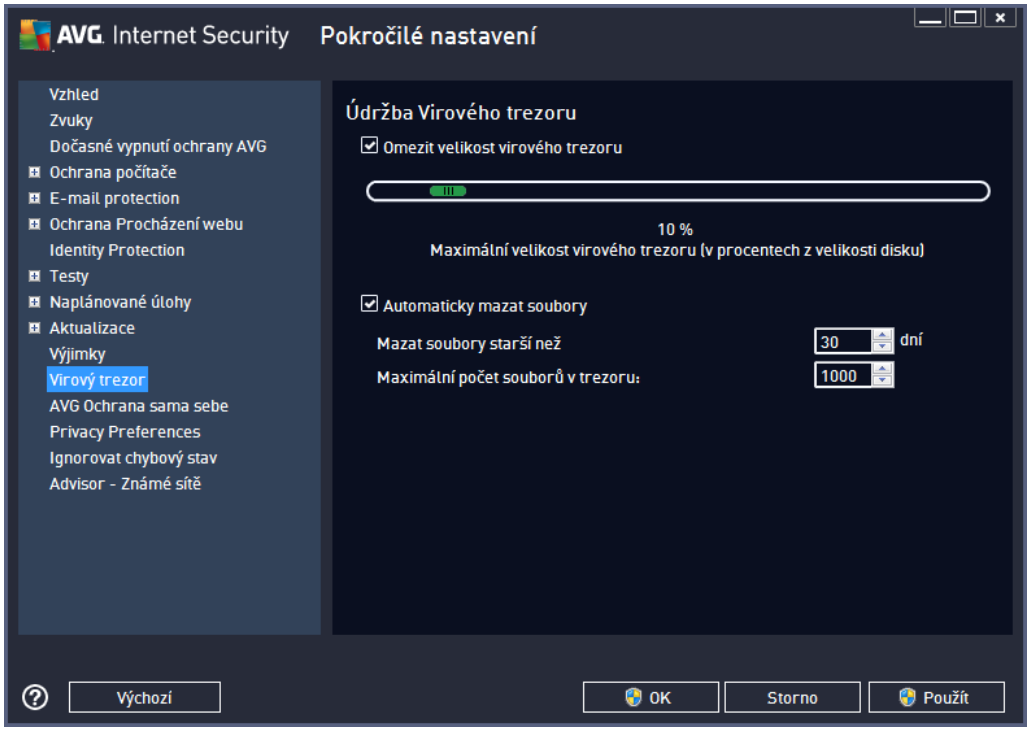
Ovládací prvky dialogu

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

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

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

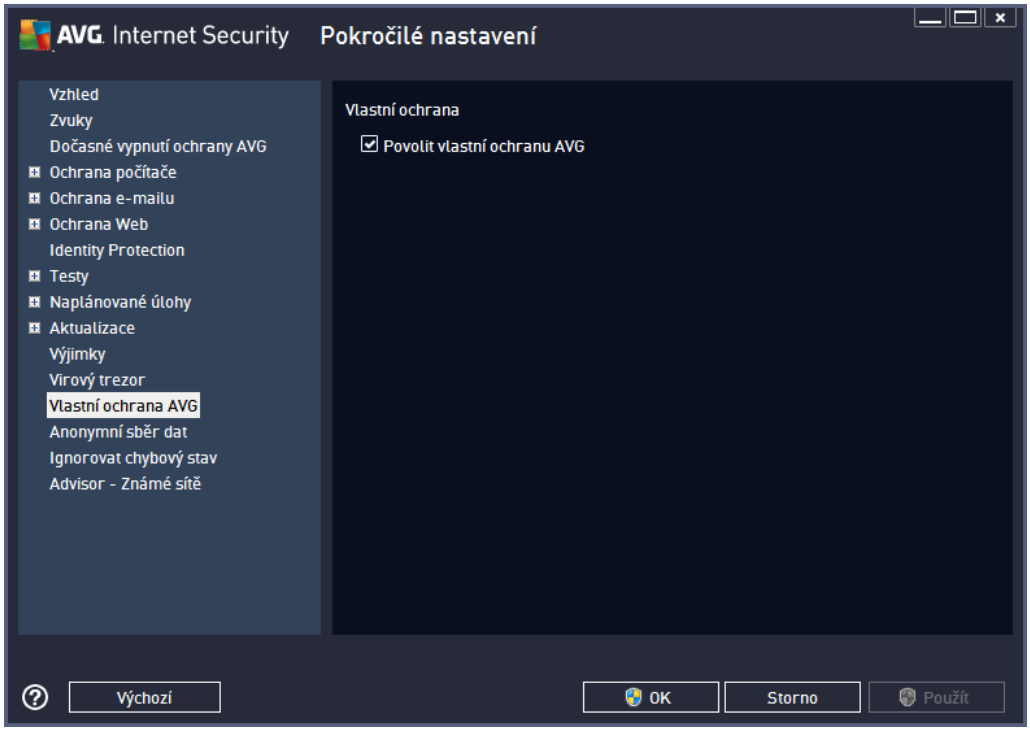
10.12. Virový trezor



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

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

10.13. Vlastní ochrana AVG

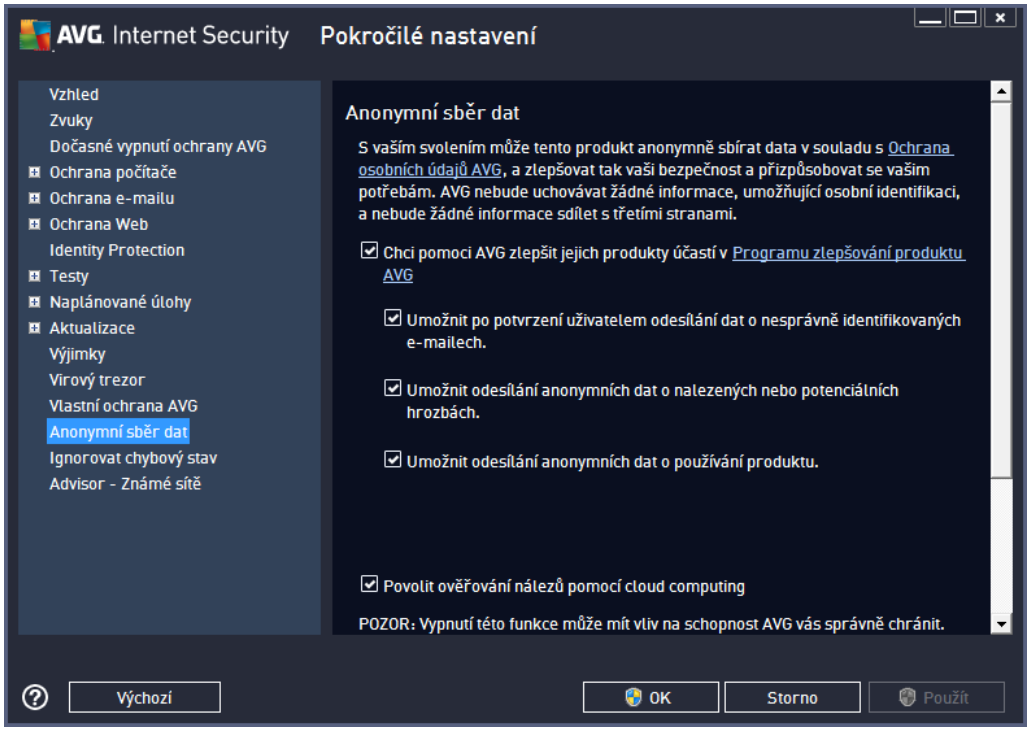


Funkce ***Vlastní ochrana AVG*** slouží k nastavení ochrany vlastních procesů, souborů, registrových klíčů a ovladačů aplikace **AVG Internet Security 2013** před jejich pozměněním či deaktivací. Důvodem implementace tohoto typu ochrany je existence sofistikovaných hrozeb, které se snaží zneškodnit antivirové programy a následně bez omezení poškodit váš počítač.

Doporučujeme, abyste tuto funkci nechali vždy zapnutou.

10.14. Anonymní sběr dat

V dialogu ***Anonymní sběr dat*** máte možnost zapojit se do spolupráce a podílet se na zlepšování produktu AVG a na celkovém zvýšení úrovně bezpečnosti na Internetu. Vaše reporty nám pomáhají shromažďovat nejčerstvější informace o virech, spywaru i škodlivých webových stránkách a vylepšovat neustále ochranu pro všechny naše uživatele. Reportování probíhá automaticky, takže vám nezpůsobí žádné nepohodlí. Reporty nikdy neobsahují žádná vaše soukromá data. Reportování je samozřejmě dobrovolné, nicméně vás prosíme, abyste je ponechali aktivováno. Výrazně nám tím pomůžete s vylepšováním ochrany vašeho počítače.



V dialogu najdete tyto možnosti nastavení:

- ***Chci pomoci AVG zlepšit jejich produkty účastí v Programu zlepšování produktu AVG*** (*ve výchozím nastavení zapnuto*) - Chcete-li nám pomoci dále zlepšovat program AVG, ponechejte toto políčko označené. Tím povolíte odesílání informací o všech hrozbách, na které eventuelně narazíte při surfování po Internetu; tato funkce nám pomáhá shromažďovat nejnovější data od uživatelů po celém světě a neustále tak vylepšovat jejich ochranu. Reportování probíhá automaticky, takže vám nezpůsobí žádné nepohodlí, a nezahrnuje žádná osobní data.
    - ***Umožnit po potvrzení uživatelem odesílání dat o nesprávně identifikovaných e-mailech*** (*ve výchozím nastavení zapnuto*) – zasílání informací o e-mailových zprávách, které byly službou Anti-Spam mylně označeny za spam, nebo naopak nebyly označeny, i když o spam skutečně šlo. V případě zasílání těchto informací budete napřed požádáni o svolení.
    - ***Umožnit odesílání anonymních dat o nalezených nebo potenciálních hrozbách*** (*ve výchozím nastavení zapnuto*) – zasílání informací o jakémkoli podezřelém nebo skutečně nebezpečném kódu či vzorci chování *(může jít o virus, spyware, případně nebezpečnou webovou stránku, na kterou jste se pokusili přejít)* nalezeném ve vašem počítači.
    - ***Umožnit odesílání anonymních dat o používání produktu*** (*ve výchozím nastavení zapnuto*) – zasílání základních statistických dat o používání systému AVG jako např. počet nalezených infekcí, proběhlých testů, úspěšných/neúspěšných aktualizací atp.
- ***Povolit ověřování nálezů pomocí cloud computing*** (*ve výchozím nastavení zapnuto*) – nalezené infekce, hrozby a podezřelé kódy budou ověřeny, zda nejde o falešné detekce *(tj. ve skutečnosti neškodné)*.

- ***Přeji si, aby se produkt AVG přizpůsoboval mým potřebám povolením funkce Přizpůsobení AVG*** - tato funkce anonymně analyzuje chování programů a aplikací, jež máte instalovány na svém počítači. Na základě této analýzy vám AVG dokáže nabídnout přesně zacílené služby, případně další produkty pro vaši maximální bezpečnost.

Nejčastější hrozby

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

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

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

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

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

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

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

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

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

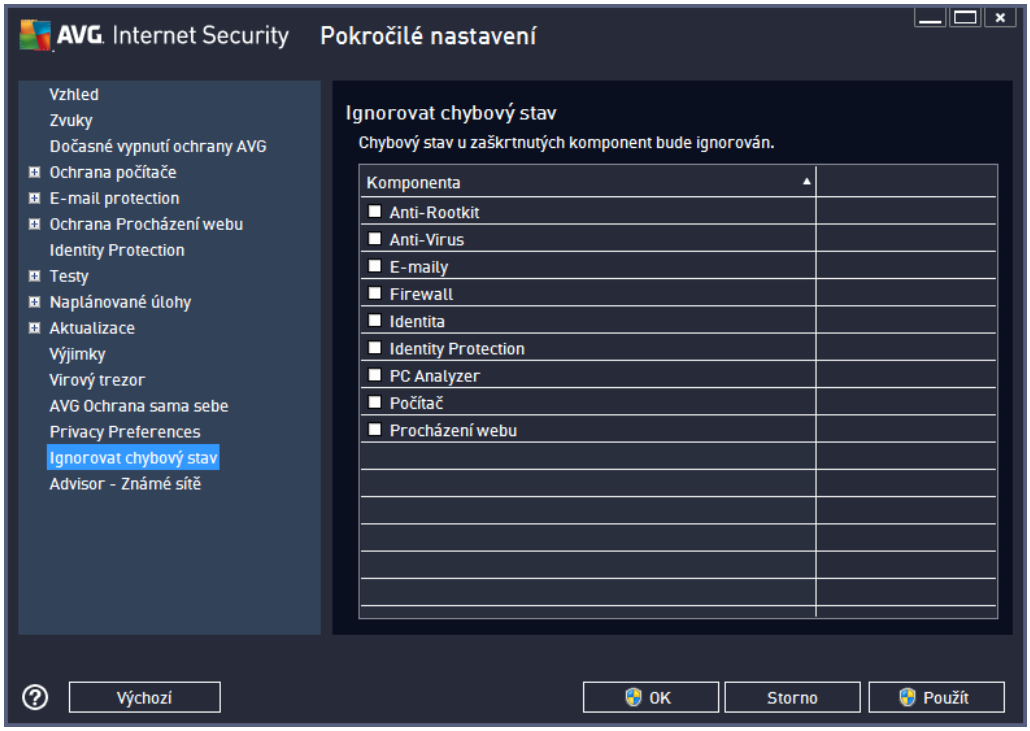
- ***Nebezpečné webové stránky*** dokáží nepozorovaně instalovat škodlivé programy do vašeho počítače, a stránky napadené hackery dělají totéž, jen se jedná o stránky původně slušné a neškodné, které se však po útoku hackerů chovají zcela nepředvídatelně.

AVG Internet Security 2013 obsahuje ochranu proti všem zmíněným typům hrozeb a škodlivých programů! Stručný přehled funkcionality jednotlivých komponent najdete v kapitole Přehled

***komponent*.**

10.15. Ignorovat chybový stav

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



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

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

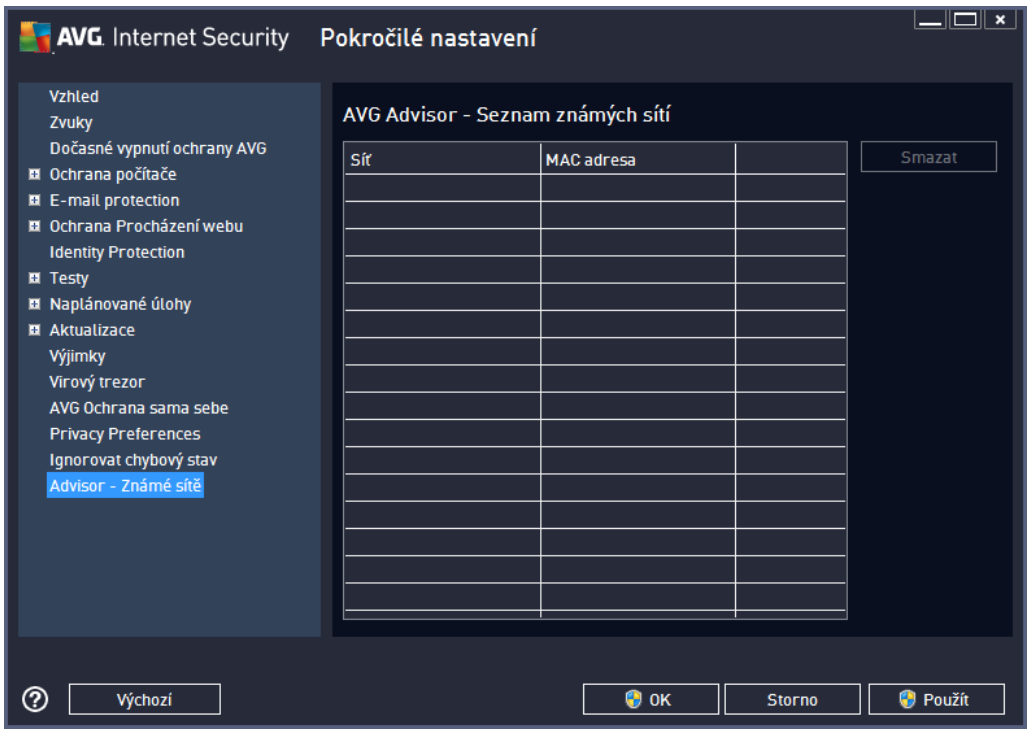
Může se ale stát, že si z nějakého důvodu přejete dočasně deaktivovat určitou komponentu. ***Samozřejmě doporučujeme ponechat všechny komponenty trvale zapnuté a ve výchozím nastavení***, ale tato možnost existuje. Pak by ikona na systémové liště automaticky oznamovala chybový stav, který ale de facto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

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

10.16. Advisor - známé sítě

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

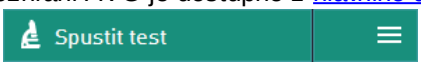
V tomto dialogu si tedy můžete ověřit, které sítě jsou považovány za známé:



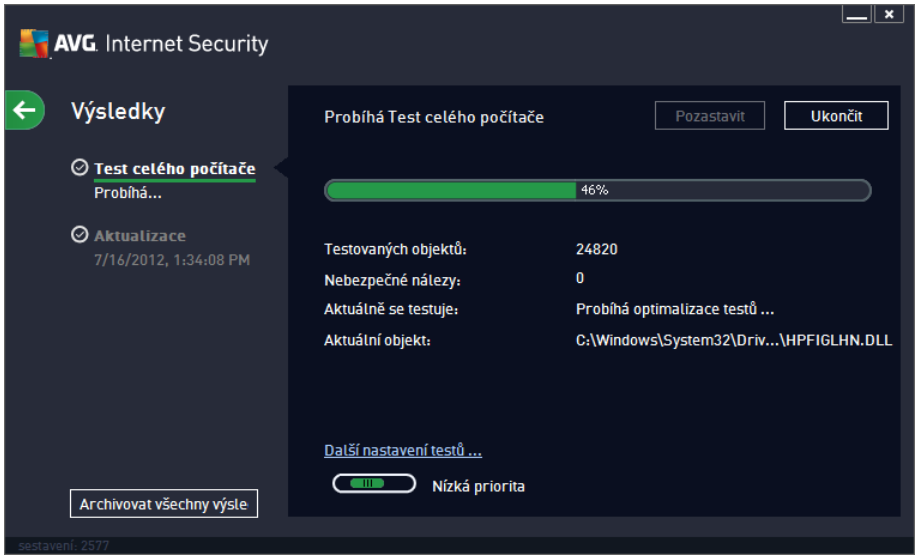
Poznámka: *Funkce známé sítě v rámci služby AVG Advisor není podporována na Windows XP 64-bit.*

11. AVG testování

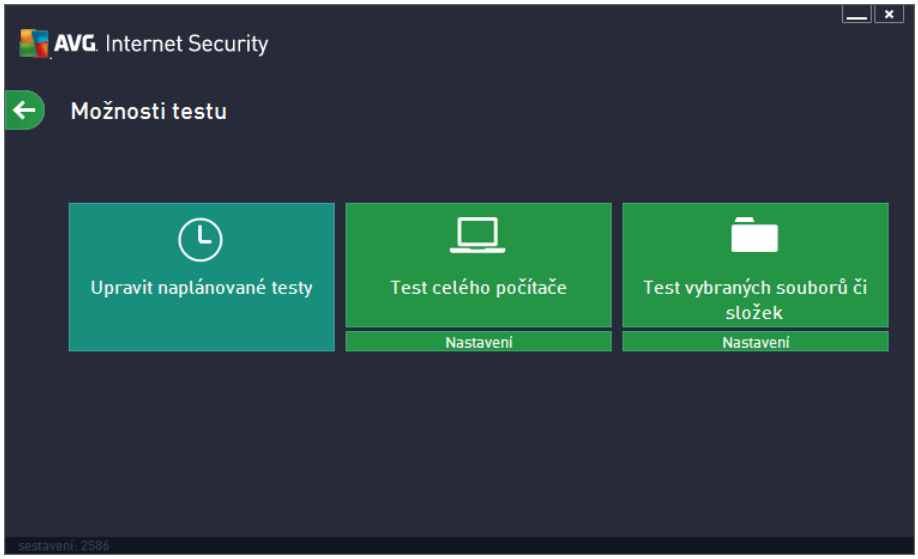
Ve výchozím nastavení **AVG Internet Security 2013** se nespouští žádný test automaticky, protože po úvodním otestování počítače *(k jehož spuštění budete vyzváni)* jste průběžně chráněni rezidentními komponentami **AVG Internet Security 2013**, které eventuelní škodlivý kód zachycují okamžitě. Samozřejmě ale můžete naplánovat test k pravidelnému spouštění v určený čas, případně kdykoli spustit ručně libovolný test podle vlastních požadavků.

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

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



- ***Možnosti testu*** - Volbou této položky *(graficky znázorněné jako tři vodorovné čárky v zeleném poli)* přejdete do dialogu ***Možnosti testu***, kde můžete spravovat naplánované testy a editovat parametry Testu celého počítače a Testu vybraných souborů či složek:



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

- ***Upravit naplánované testy*** - Volbou této možnosti otevřete nový dialog s přehledem všech naplánovaných testů. Dokud nenaplánujte vlastní testy, bude v tabulkovém přehledu uveden jen jeden test definovaný výrobcem. Tento test je ve výchozím nastavení vypnutý. Kliknutím pravého tlačítka myši nad tímto definovaným testem rozbalíte kontextové menu a volbou položky *Povolit úlohu* test aktivujete. Jakmile je test aktivován, můžete editovat jeho konfiguraci prostřednictvím tlačítka *Upravit plán testu*. Pomocí tlačítka *Přidat plán testu* můžete také nastavit svůj vlastní naplánovaný test.

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

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

11.1. Přednastavené testy

Jednou z hlavních funkcí **AVG Internet Security 2013** je testování na vyžádání. Testy na vyžádání jsou navrženy tak, že mohou testovat různé části vašeho počítače, kdykoliv se objeví podezření na možnost virové infekce. V každém případě však doporučujeme provádět testy pravidelně, i když považujete váš počítač za zcela viru prostý.

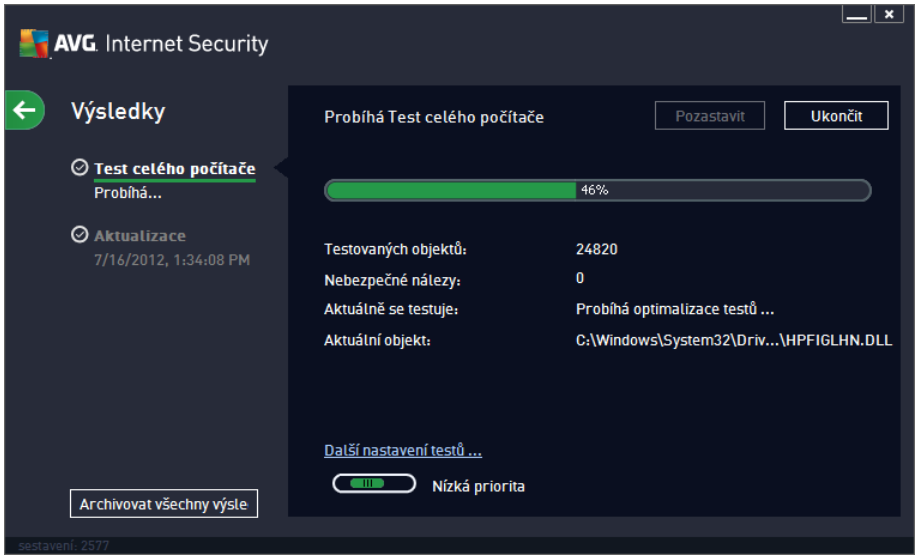
V **AVG Internet Security 2013** najdete tyto typy výrobcem nastavených testů:

11.1.1. Test celého počítače

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

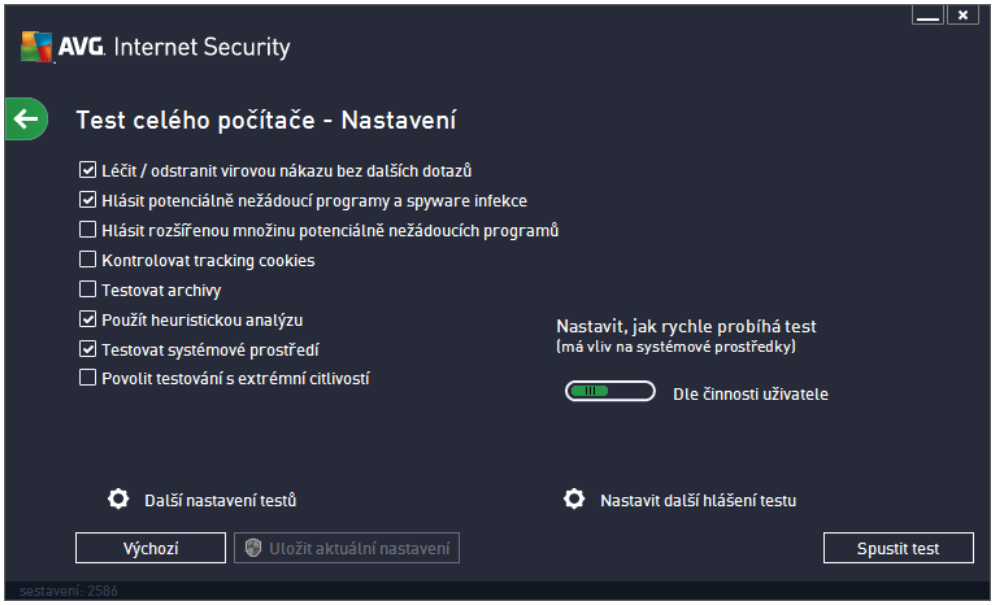
Spuštění testu

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



Editace nastavení testu

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



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

- ***Léčit / odstranit virovou nákazu bez dalších dotazů*** *(ve výchozím nastavení zapnuto)*: 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 testování přítomnosti spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány vědomě a se souhlasem uživatele. Doporučujeme nicméně ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.

- ***Hlásit rozšířenou množinu potenciálně nežádoucích programů*** *(ve výchozím nastavení vypnuto)*: zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v původní podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.

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

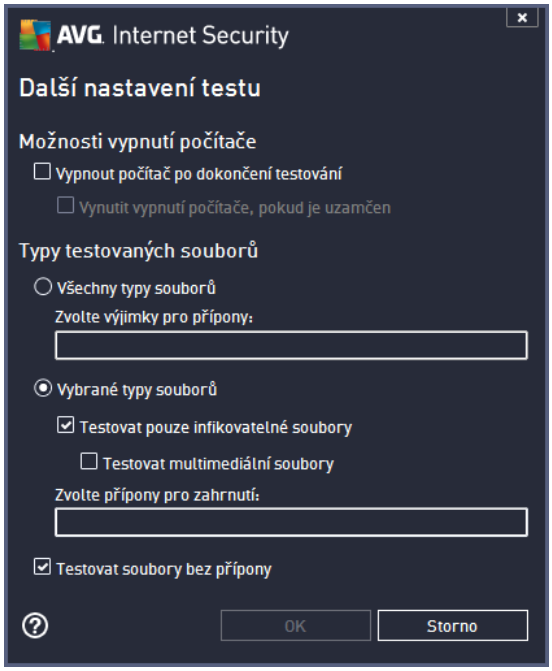
- ***Testovat archivy*** *(ve výchozím nastavení vypnuto)*: parametr definuje, že test má kontrolovat všechny soubory zabalené v některém typu archivu, například ZIP, RAR, ...

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

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

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

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



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

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

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

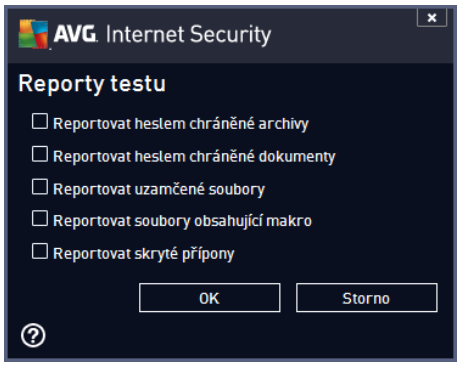
  - ***Vybrané typy souborů*** - můžete se rozhodnout, že chcete, aby se testy spouštěly pouze nad soubory, které lze považovat za infikovatelné (*soubory, které nemohou být infekcí zasaženy, se testovat nebudou - například prosté textové soubory nebo některé nespustitelné soubory*), a to včetně multimediálních souborů (*video, audio soubory - ponecháte-li tuto položku neoznačenou, výrazně se tím zkrátí čas testování, jelikož multimediální soubory jsou obvykle poměrně velké, ale pravděpodobnost infekce je u nich velmi nízká*). I zde můžete určit výjimky a pomocí seznamu přípon definovat, které soubory mají být testovány za všech okolností.

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

- ***Nastavit, jak rychle probíhá test*** - posuvníkem lze změnit prioritu testu. Ve výchozím nastavení je tato hodnota nastavena *dle činnosti uživatele.* Tato hodnota nastavení optimalizuje rychlost testu počítače a vytížení systémových zdrojů. Test můžete spustit pomaleji a tedy s nižší zátěží systémových zdrojů (*vhodné, pokud potřebujete během testu na počítači pracovat a nezáleží vám tolik na celkové době testování*) nebo naopak rychleji s vyššími nároky na systémové zdroje (*například v době, kdy na počítači nikdo nepracuje*).

- ***Nastavit další hlášení testů*** - odkaz otevírá nový dialog ***Reporty testu***, v němž můžete označit, které

typy nálezů mají být hlášeny:



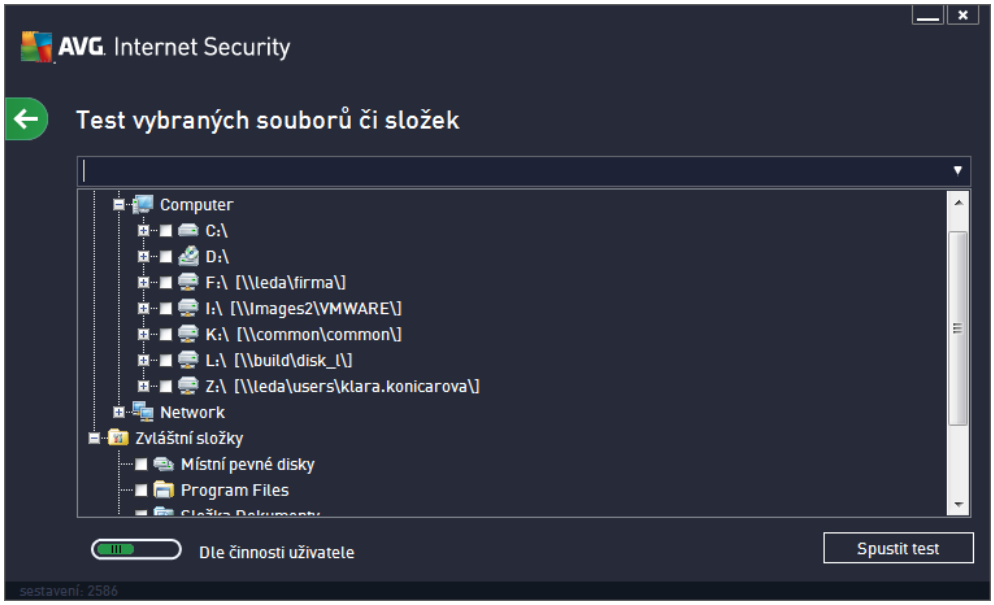
Upozornění: *Samotné možnosti nastavení testu jsou shodné s parametry nově definovaného testu, které jsou podrobně popsány v kapitole AVG testování / Naplánování testu / Jak testovat. Pokud se rozhodnete výchozí nastavení* ***Testu celého počítače*** *změnit, můžete pak svou konfiguraci uložit jako výchozí,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

11.1.2. Test vybraných souborů či složek

Test vybraných souborů či složek kontroluje pouze uživatelem definované oblasti počítače (*zvolené složky, pevné disky, diskety, CD, optické disky, ...*). Postup při nálezu a léčbě/odstraňování virové nákazy je stejný jako u ***Testu celého počítače***: nalezené viry jsou vyléčeny nebo přesunuty do Virového trezoru. ***Test vybraných souborů či složek*** můžete s výhodou použít pro nastavení vlastních testů, jejichž spouštění nastavíte podle vašich potřeb.

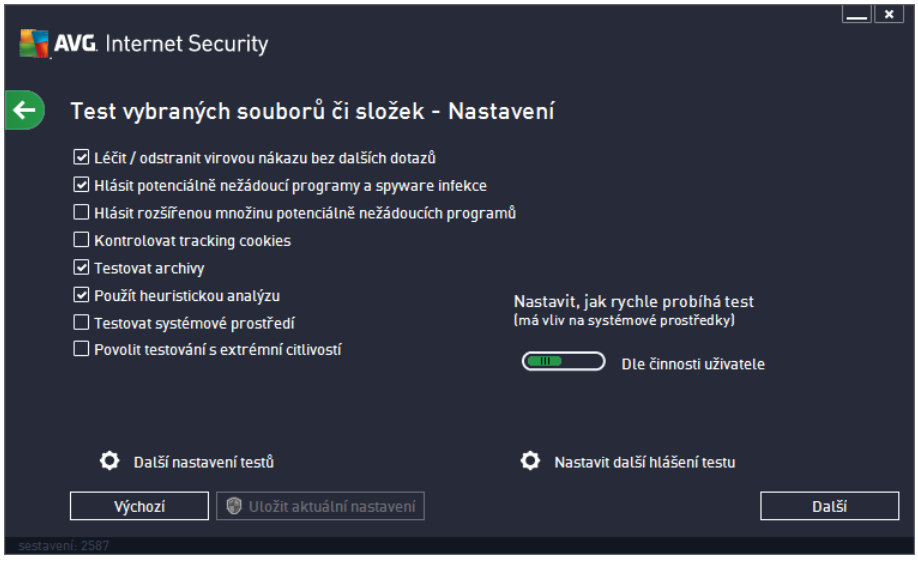
Spuštění testu

Test vybraných souborů či složek spusťte přímo z dialogu Možnosti testu kliknutím na graficky znázorněnou položku ***Test vybraných souborů či složek***. Otevře se rozhraní ***Test vybraných souborů či složek***, kde můžete v graficky znázorněné stromové struktuře vašeho počítače označit ty složky, jejichž obsah chcete nechat zkontrolovat. Cesta ke každé zvolené složce se automaticky vygeneruje v horním textovém poli dialogu. Pokud si přejete zkontrolovat určitý adresář bez kontroly všech v něm obsažených podadresářů, napište před automaticky vygenerovanou cestu k adresáři znaménko "-". Parametrem "!" před cestou k adresáři zase určíte, že celý adresář má být z testu vypuštěn. Samotný test pak spustíte stiskem tlačítka ***Spustit test*** a jeho průběh je identický s průběhem Testu celého počítače.



Editace nastavení testu

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



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

- ***Léčit / odstranit virovou nákazu bez dalších dotazů*** *(ve výchozím nastavení zapnuto)*: 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 testování přítomnosti spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány vědomě a se souhlasem uživatele. Doporučujeme nicméně ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.

- ***Hlásit rozšířenou množinu potenciálně nežádoucích programů*** *(ve výchozím nastavení vypnuto)*: Zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v původní podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.

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

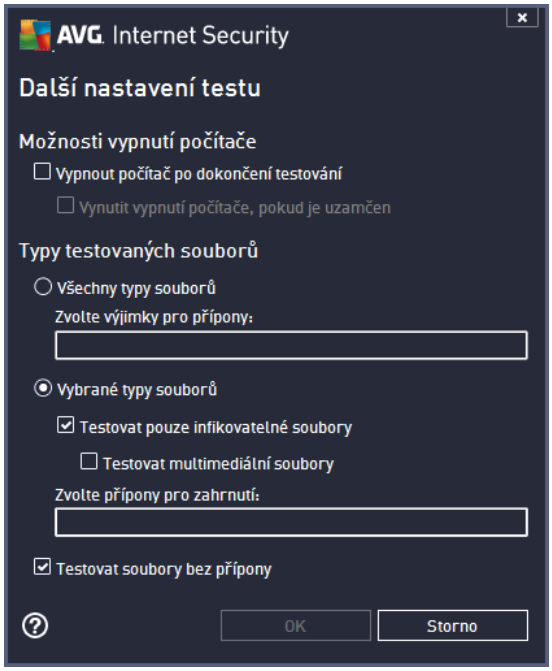
- ***Testovat archivy*** *(ve výchozím nastavení zapnuto)*: Parametr definuje, že test má kontrolovat všechny soubory zabalené v některém typu archivu, například ZIP, RAR, ...

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

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

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

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



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

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

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

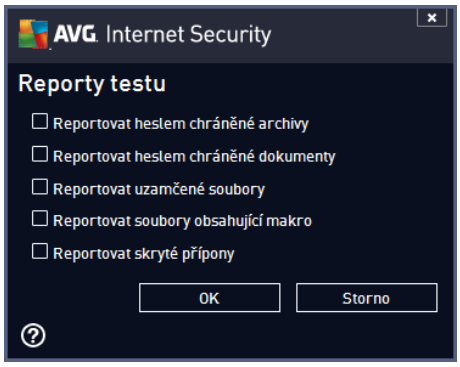
  - ***Vybrané typy souborů*** - můžete se rozhodnout, že chcete, aby se testy spouštěly pouze nad soubory, které lze považovat za infikovatelné (*soubory, které nemohou být infekcí zasaženy, se testovat nebudou - například prosté textové soubory nebo některé nespustitelné soubory*), a to včetně multimediálních souborů (*video, audio soubory - ponecháte-li tuto položku neoznačenou, výrazně se tím zkrátí čas testování, jelikož multimediální soubory jsou obvykle poměrně velké, ale pravděpodobnost infekce je u nich velmi nízká*). I zde můžete určit výjimky a pomocí seznamu přípon definovat, které soubory mají být testovány za všech okolností.

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

- ***Nastavit, jak rychle probíhá test*** - posuvníkem lze změnit prioritu testu. Ve výchozím nastavení je tato hodnota nastavena *dle činnosti uživatele*, čímž optimalizuje rychlost testu počítače a vytížení systémových zdrojů. Test můžete spustit pomaleji a tedy s nižší zátěží systémových zdrojů (*vhodné, pokud potřebujete během testu na počítači pracovat a nezáleží vám tolik na celkové době testování*) nebo naopak rychleji s vyššími nároky na systémové zdroje (*například v době, kdy na počítači nikdo nepracuje*).

- ***Nastavit další hlášení testů*** - odkaz otevírá nový dialog ***Reporty testu***, v němž můžete označit, které

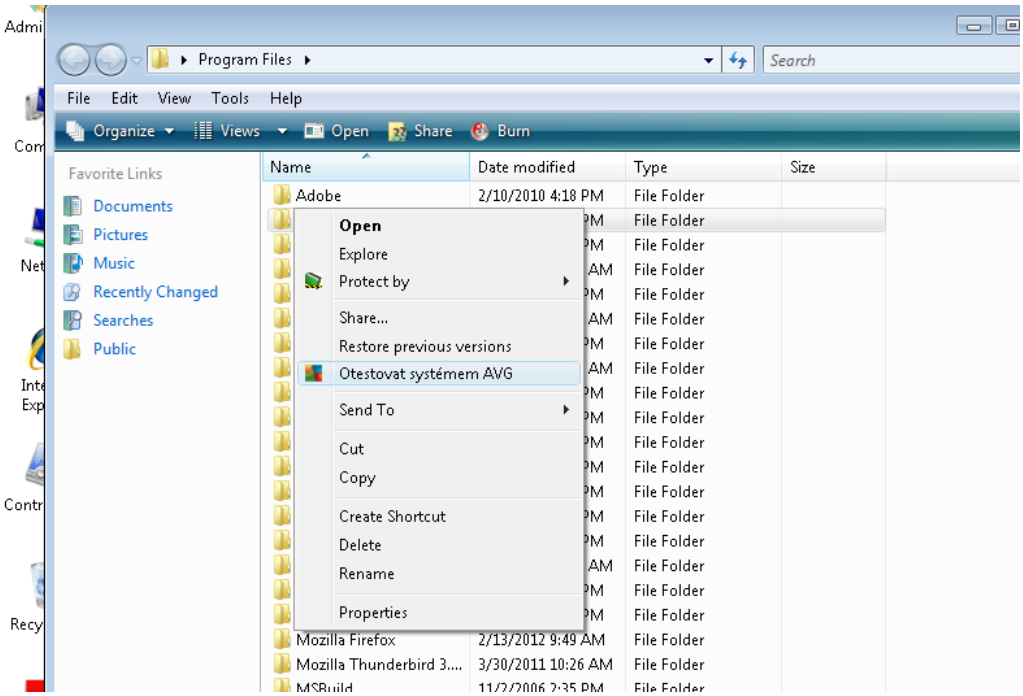
typy nálezů mají být hlášeny:



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

11.2. Testování v průzkumníku Windows

AVG Internet Security 2013 nabízí kromě přednastavených testů spouštěných nad celým počítačem nebo jeho vybranými oblastmi i možnost rychlého otestování konkrétního objektu přímo v prostředí průzkumníka Windows. Chcete-li například otevřít neznámý soubor a nejste si jisti jeho obsahem, můžete nechat tento soubor na vyžádání otestovat. Postup je následující:



- V průzkumníku Windows označte soubor (*nebo adresář*), jehož obsah chcete prověřit
- Kliknutím pravého tlačítka myši nad objektem otevřete kontextové menu

- Volbou položky ***Otestovat systémem AVG*** necháte objekt otestovat programem **AVG Internet Security 2013**

11.3. Testování z příkazové řádky

V rámci **AVG Internet Security 2013** existuje také možnost spustit test z příkazové řádky. Tuto možnost využijete například na serverech nebo třeba při vytváření dávkových skriptů, které mají být spouštěny po startu počítače. Z příkazové řádky můžete spustit test s nastavením většiny parametrů, které jsou dostupné v grafickém rozhraní AVG.

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

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

Syntaxe příkazu

Syntaxe příkazu pro spuštění testu z příkazové řádky je následující:

- ***avgscanx /parametr*** ... tedy například ***avgscanx /comp*** pro spuštění testu celého počítače
- ***avgscanx /parametr /parametr*** .. při použití více parametrů jsou tyto uvedeny za sebou a odděleny mezerou a lomítkem
- pokud parametr vyžaduje uvedení konkrétní hodnoty (například parametr ***/scan*** pro otestování vybraných oblastí počítače, kde musíte uvést cestu k testované oblasti), jsou jednotlivé hodnoty od sebe odděleny středníkem, například: ***avgscanx /scan=C:\;D:***

Parametry příkazu

Kompletní přehled použitelných parametrů lze zobrazit příkazem pro příslušný test s parametrem /? nebo /HELP (např. ***avgscanx /?***). Jediným povinným parametrem testu je /SCAN, příp. /COMP, kterými určíte oblasti počítače, jež se mají testovat. Podrobný popis dostupných parametrů najdete v kapitole Parametry CMD testu.

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

Spuštění CMD testu z grafického rozhraní

Při spuštění počítače v nouzovém režimu Windows je dostupná i možnost spuštění testu z příkazové řádky prostřednictvím dialogu grafického rozhraní. Samotný text bude spuštěn z příkazové řádky; dialog ***Nastavení testu z příkazové řádky*** slouží pouze jako nástroj pro snadné nastavení parametrů testu, aniž byste je museli definovat v prostředí příkazové řádky.

Vzhledem k tomu, že dialog není standardně dostupný a bude zobrazen pouze v nouzovém režimu Windows, jeho podrobný popis najdete v nápovědě dostupné přímo z tohoto dialogu.

11.3.1. Parametry CMD testu

V následujícím přehledu nabízíme seznam dostupných parametrů testu:

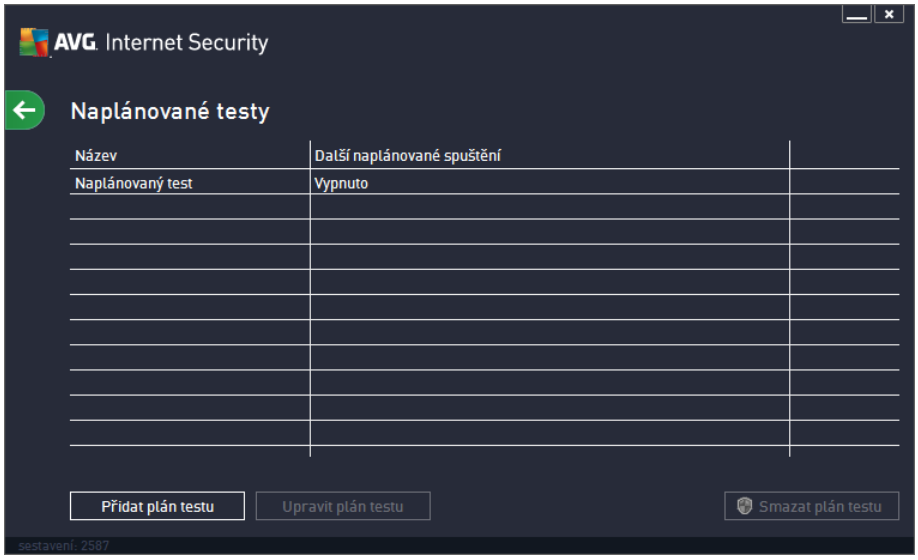
- /SCAN Test vybraných souborů či složek; /SCAN=path;path *(například /SCAN=C:\;D:\)*
- /COMP Test celého počítače
- /HEUR Použít heuristickou analýzu
- /EXCLUDE Z testu vynechat tuto cestu nebo soubory
- /@ Příkazový soubor /jméno souboru/
- /EXT Testovat pouze soubory s těmito příponami /například EXT=EXE,DLL/
- /NOEXT Netestovat soubory s těmito příponami /například NOEXT=JPG/
- /ARC Testovat archívy
- /CLEAN Automaticky léčit
- /TRASH Přesunout infikované soubory do Virového trezoru
- /QT Rychlý test
- /LOG Vygenerovat soubor s výsledkem testu
- /MACROW Hlásit makra
- /PWDW Hlásit heslem chráněné soubory
- /ARCBOMBSW Reportovat archivní bomby *(opakovaně komprimované archivy)*
- /IGNLOCKED Ignorovat zamčené soubory
- /REPORT Hlásit do souboru /jméno souboru/
- /REPAPPEND Přidat k souboru
- /REPOK Hlásit neinfikované soubory jako OK
- /NOBREAK Nepovolit přerušení testu pomocí CTRL-BREAK
- /BOOT Povolit kontrolu MBR/BOOT
- /PROC Testovat aktivní procesy
- /PUP Hlásit Potenciálně nebezpečné programy
- /PUPEXT Hlásit rozšířenou množinu Potenciálně nebezpečných programů
- /REG Testovat registry

- /COO Testovat cookies
- /? Zobrazit nápovědu k tomuto tématu
- /HELP Zobrazit nápovědu k tomuto tématu
- /PRIORITY Nastavit prioritu testu /Low, Auto, High/ *(viz Pokročilé nastavení / Testy)*
- /SHUTDOWN Vypnout počítač po dokončení testu
- /FORCESHUTDOWN Vynutit vypnutí počítače po dokončení testu
- /ADS Testovat alternativní datové proudy (pouze NTFS)
- /HIDDEN Hlásit soubory se skrytou příponou
- /INFECTABLEONLY Testovat pouze infikovatelné soubory
- /THOROUGHSCAN Povolit testování s extrémní citlivostí
- /CLOUDCHECK Ověřit falešné detekce
- /ARCBOMBSW Hlásit opakovaně komprimované archivní soubory

11.4. Naplánování testu

Testy v **AVG Internet Security 2013** lze spouštět buďto na vyžádání (*například v situaci, kdy máte podezření na zavlečení infekce na váš počítač nebo z jiného důvodu*) anebo podle nastaveného plánu. Doporučujeme používat především spouštění testů podle plánu, protože tímto přístupem zajistíte svému počítači dostatečnou prevenci a budete moci pracovat bez starostí o to, zda a kdy test spustit. Test celého počítače by měl být spouštěn pravidelně, a to nejméně jednou týdně. Pokud vám to však provoz na vašem počítači umožňuje, doporučujeme spouštět test celého počítače jednou denně; tak je také ve výchozí konfiguraci nastaven plán testů. Jestliže je počítač trvale zapnutý, je vhodné naplánovat spuštění ***Testu celého počítače*** na dobu mimo pracovní hodiny. Pokud počítač vypínáte, nezapomeňte využít možnosti spustit test při startu počítače, pokud byl naplánovaný čas zmeškán.

Plán testů lze vytvářet v dialogu ***Naplánované testy***, který je dostupný prostřednictvím tlačítka ***Upravit naplánované testy*** z dialogu Možnosti testu. V nově otevřeném dialogu ***Naplánované testy*** pak uvidíte kompletní přehled všech aktuálně naplánovaných testů:

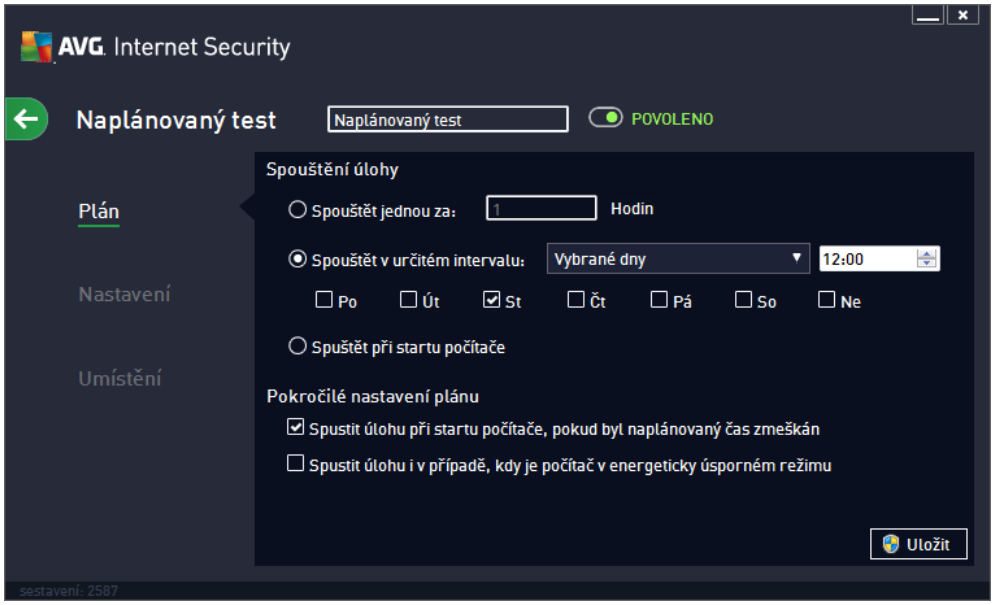


Dokud nenaplánujte vlastní testy, bude v tabulkovém přehledu uveden jen jeden test definovaný výrobcem. Tento test je ve výchozím nastavení vypnutý. Kliknutím pravého tlačítka myši nad tímto definovaným testem rozbalíte kontextové menu a volbou položky ***Povolit úlohu*** test aktivujete. Jakmile je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

- Plán
- Nastavení
- Umístění

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

11.4.1. Plán



V textovém poli v horní části záložky ***Plán*** můžete zadat jméno, které si přejete přiřadit právě vytvářenému testu. Snažte se vždy používat stručné, popisné a případné názvy, abyste se později v naplánovaných úlohách snadněji vyznali. Například nevhodným názvem testu je například "Nový test" nebo "Martinův test", protože ani jeden název nevypovídá o tom, co test ve skutečnosti kontroluje. Naproti tomu správným popisným názvem testu může být například "Test systémových oblastí" nebo "Test disku C:" a podobně.

V dialogu můžete dále definovat tyto parametry testu:

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

- ***Pokročilé nastavení plánu*** - Tato sekce umožňuje definovat podmínky, kdy má či nemá být test spuštěn, jestliže je počítač v úsporném režimu nebo zcela vypnutý a naplánovaný 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 probikávajícím světlem)*, která vás informuje o běžícím testu. Kliknutím pravého tlačítka myši nad touto ikonou otevřete kontextové menu, z něhož můžete běžící test pozastavit nebo ukončit, a rovněž změnit prioritu právě probíhajícího testu.

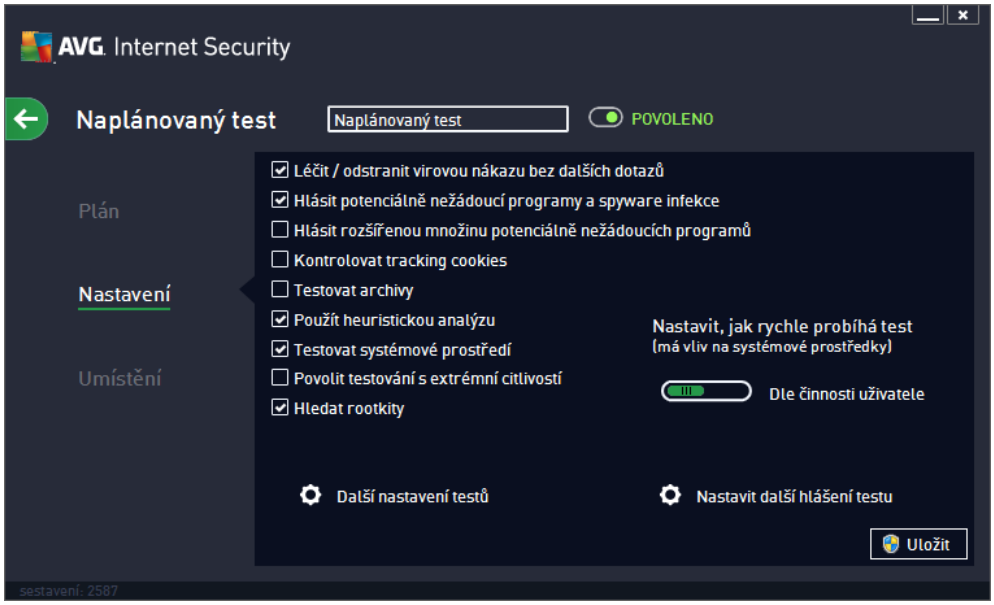
Ovládací tlačítka dialogu

- ***Uložit*** - uloží všechny změny, které jste provedli na této záložce nebo na libovolné jiné záložce dialogu pro nastavení plánu testu a přepne vás zpět do dialogu Naplánované testy. Chcete-li tedy nastavit parametry plánu testu na všech záložkách, uložte je stiskem tohoto tlačítka teprve poté, co

jste zadali všechny své požadavky.

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

11.4.2. Nastavení



V textovém poli v horní části záložky ***Nastavení*** můžete zadat jméno, které si přejete přiřadit právě vytvářenému testu. Snažte se vždy používat stručné, popisné a případné názvy, abyste se později v naplánovaných úlohách snadněji vyznali. Například nevhodným názvem testu je například "Nový test" nebo "Martinův test", protože ani jeden název nevypovídá o tom, co test ve skutečnosti kontroluje. Naproti tomu správným popisným názvem testu může být například "Test systémových oblastí" nebo "Test disku C:" a podobně.

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

- ***Léčit / odstranit virovou nákazu bez dalších dotazů|*** (*ve výchozím nastavení zapnuto*): 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 testování přítomnosti spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány vědomě a se souhlasem uživatele. Doporučujeme nicméně ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.

- ***Hlásit rozšířenou množinu potenciálně nežádoucích programů*** (*ve výchozím nastavení vypnuto*): zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware: programů, které jsou v původní podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další

úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.

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

- ***Testovat archivy*** (*ve výchozím nastavení vypnuto*): parametr definuje, že test má kontrolovat všechny soubory, a to i takové, které jsou zabaleny v některém typu archivu, například ZIP, RAR, ...

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

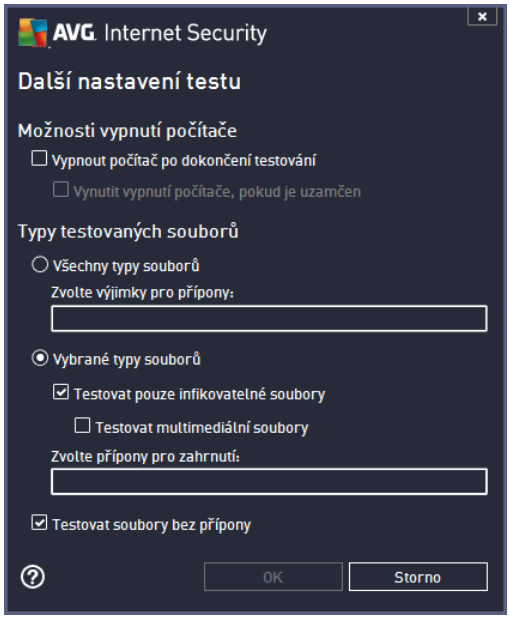
- ***Testovat systémové prostředí*** (*ve výchozím nastavení zapnuto*): test prověří i systémové oblasti vašeho počítače;

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

- ***Hledat rootkity*** (*ve výchozím nastavení zapnuto*): parametr služby Anti-Rootkit prohledává počítač na přítomnost rootkitů, tedy programů a technologií, které dokáží maskovat přítomnost malware v počítači. Dojde-li k nálezu rootkitu, nemusí to nutně znamenat, že je počítač infikovaný. V některých případech mohou být rootkity použity jako ovladače nebo části korektních aplikací.

Další nastavení testů

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



- ***Možnosti vypnutí počítače*** - určete, zda má být počítač po dokončení testu automaticky vypnut.

Pokud potvrdíte tuto možnost *(Vypnout počítač po dokončení testování)*, aktivuje se nová volba *(Vynutit vypnutí počítače, pokud je uzamčen)*, při jejímž potvrzení dojde po dokončení testu k vypnutí počítače i tehdy, jestliže je počítač momentálně zamknut.

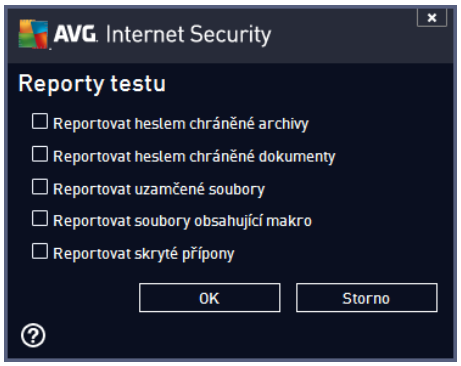
- ***Typy testovaných souborů*** - dále se můžete rozhodnout, zda si přejete testovat
  - ***Všechny typy souborů*** - přičemž máte zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou;
  - ***Vybrané typy souborů*** - můžete se rozhodnout, že chcete, aby se testy spouštěly pouze nad soubory, které lze považovat za infikovatelné *(soubory, které nemohou být infekcí zasaženy, se testovat nebudou - například prosté textové soubory nebo některé nespustitelné soubory)*, a to včetně multimediálních souborů *(video, audio soubory - ponecháte-li tuto položku neoznačenou, výrazně se tím zkrátí čas testování, jelikož multimediální soubory jsou obvykle poměrně velké, ale pravděpodobnost infekce je u nich velmi nízká)*. I zde můžete určit výjimky a pomocí seznamu přípon definovat, které soubory mají být testovány za všech okolností.
  - U položky ***Testovat soubory bez přípon*** pak rozhodněte, zda se mají testovat i soubory se skrytou či neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme , abyste se tohoto nastavení podrželi, pokud nemáte skutečný důvod jej měnit. Soubory bez přípon jsou obecně vysoce podezřelé a měly by být otestovány.

Nastavit, jak rychle probíhá test

V této sekci pak můžete nastavit požadovanou rychlost testování v závislosti na zátěži systémových zdrojů. Ve výchozím nastavení je tato hodnota nastavena *dle činnosti uživatele*. Pokud se rozhodnete pro spuštění rychlého testu, proběhne test v kratším čase, ale po dobu jeho běhu bude výrazně zvýšena zátěž systémových zdrojů, takže vaše práce na počítači bude obtížnější (*tato varianta je vhodná pro situaci, kdy je počítač spuštěn, ale nikdo na něm aktuálně nepracuje*). Naopak, prodloužením doby testu snížíte zátěž systémových zdrojů a vaše práce na počítači nebude téměř ovlivněna, test však bude probíhat po delší dobu.

Nastavit další hlášení testu

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

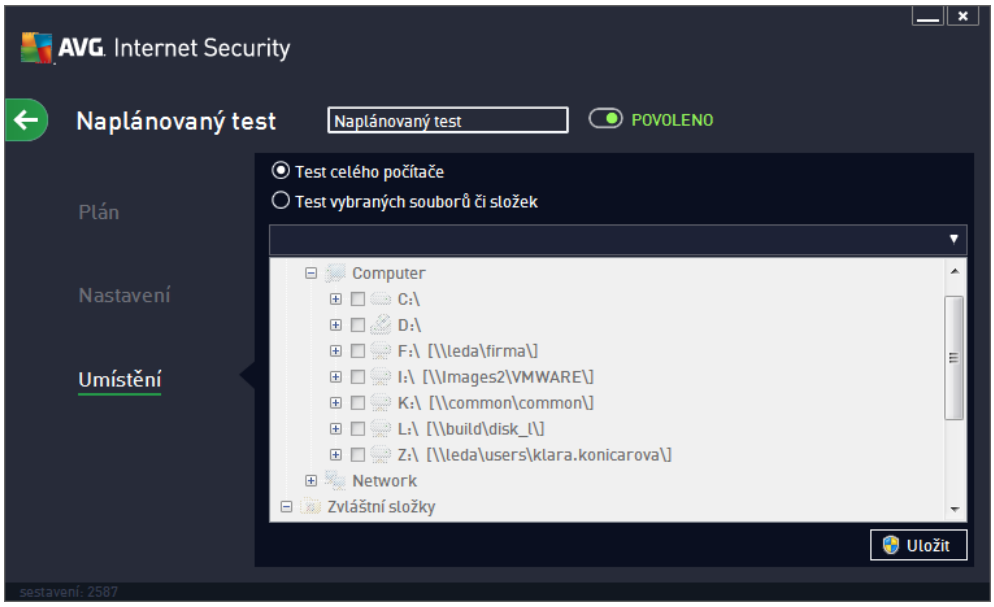


Ovládací tlačítka dialogu

- ***Uložit*** - uloží všechny změny, které jste provedli na této záložce nebo na libovolné jiné záložce dialogu pro nastavení plánu testu a přepne vás zpět do dialogu Naplánované testy. Chcete-li tedy nastavit parametry plánu testu na všech záložkách, uložte je stiskem tohoto tlačítka teprve poté, co jste zadali všechny své požadavky.

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

11.4.3. Umístění



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

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

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

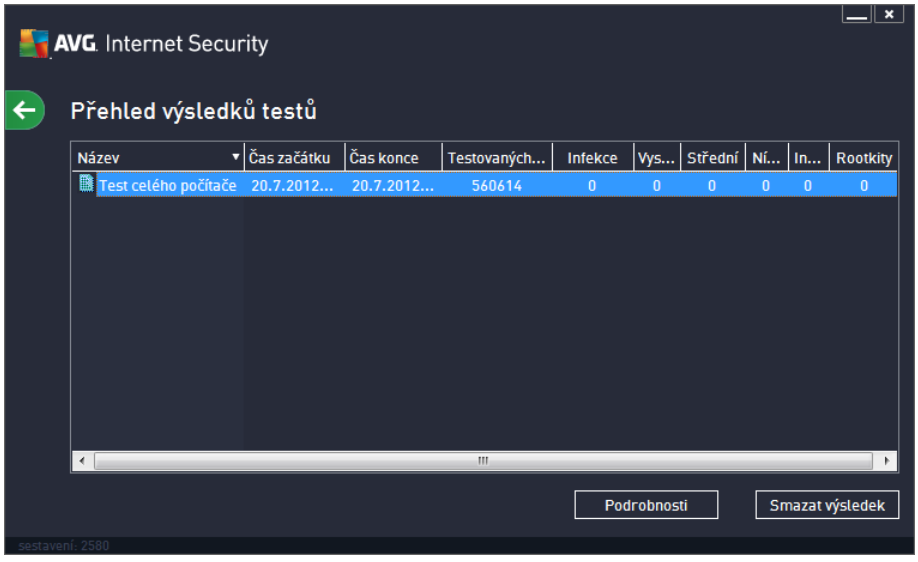
- *pro Windows Vista/7*: C:\Users\user\Documents\

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

Ovládací tlačítka dialogu

- ***Uložit*** - uloží všechny změny, které jste provedli na této záložce nebo na libovolné jiné záložce dialogu pro nastavení plánu testu a přepne vás zpět do dialogu Naplánované testy. Chcete-li tedy nastavit parametry plánu testu na všech záložkách, uložte je stiskem tohoto tlačítka teprve poté, co jste zadali všechny své požadavky.
- - Pomocí šipky v levé horní části dialogu se vrátíte zpět do přehledu naplánovaných testů.

11.5. Výsledky testu



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

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

Ovládací prvky dialogu

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

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

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

11.6. Podrobnosti výsledku testu

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

- ***Shrnutí*** - Záložka nabízí základní informace o testu: zda byl úspěšně dokončen, zda byly detekovány nějaké hrozby a jak s nimi bylo naloženo.

- ***Detaily*** - Záložka zobrazuje podrobný přehled informací o testu, včetně podrobností o jednotlivých detekovaných hroznách. Máte zde také možnost exportovat přehled do souboru a uložit jej ve formátu .csv.

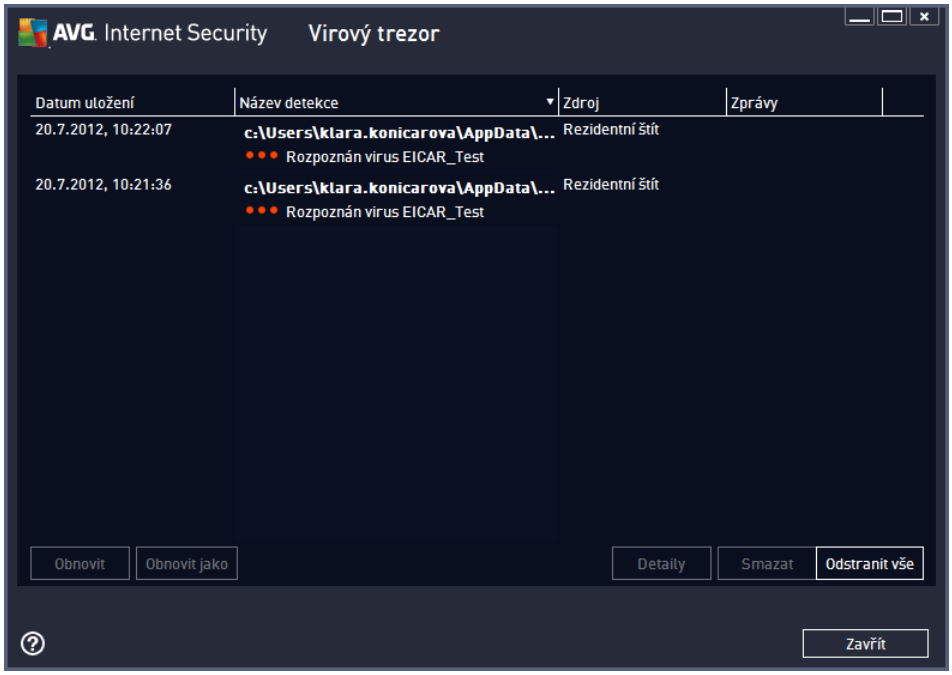
- ***Nálezy*** - Tato záložka bude zobrazena pouze v případě, že v průběhu testu skutečně došlo k detekci hrozeb, a rozlišuje detekované hrozby podle jejich závažnosti:

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

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

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

12. Virový trezor



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

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

- ***Datum uložení*** - Datum a čas detekce infikovaného souboru a jeho přesunutí do ***Virového trezoru***.
- ***Závažnost*** - Jestliže jste si v rámci instalace programu **AVG Internet Security 2013** nainstalovali také komponentu Identita, najdete v tomto sloupci grafické znázornění závažnosti infekce přesunuté do karantény na čtyřstupňové škále v rozpětí nezávadný *(tři zelené tečky)* až vysoce rizikový *(tři červené tečky)*. Zároveň je zde uvedena informace o typu nálezu (*rozlišuje typy nálezů podle úrovně jejich infekčnosti - objekty mohou být pozitivně/potenciálně infikované*).
- ***Název detekce*** - Uvádí název detekované infekce viru podle on-line virové encyklopedie.
- ***Zdroj*** - Určuje, která komponenta programu **AVG Internet Security 2013** uvedenou hrozbu detekovala.
- ***Zprávy*** - Sloupec je většinou prázdný, pouze ve výjimečných případech se může objevit poznámka s podrobnostmi k příslušné detekované hrozbě.

Ovládací tlačítka dialogu

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

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

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

- ***Detaily*** - chcete-li znát podrobnější informace o konkrétní hrozbě uložené ve ***Virovém trezoru***, označte zvolenou položku v seznamu a tlačítkem ***Detaily*** vyvoláte nový dialog s podrobným popisem detekované hrozby.

- ***Smazat*** - definitivně a nevratně vymaže infikovaný soubor z ***Virového trezoru***

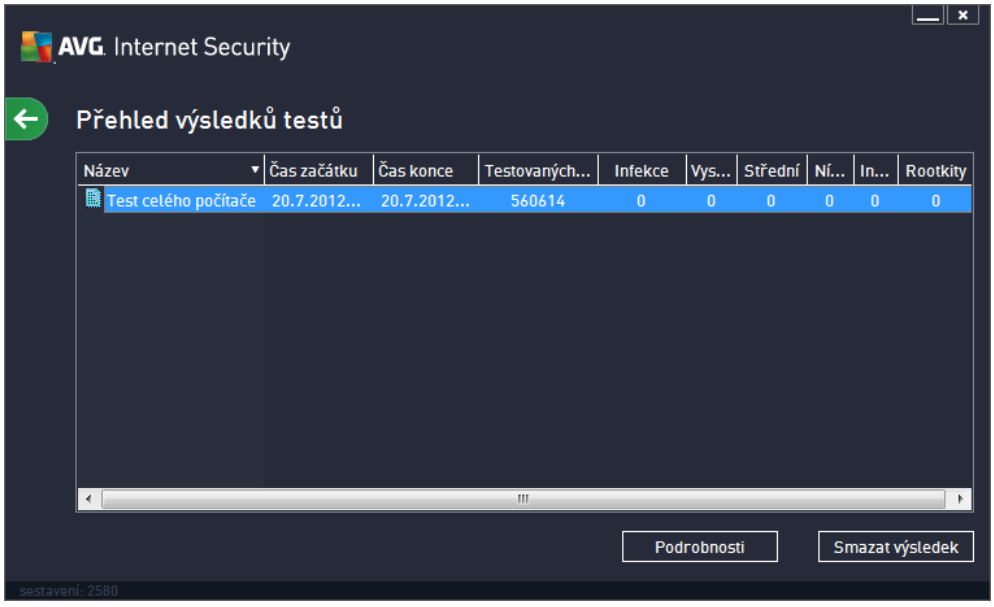
- ***Odstranit vše*** - definitivně vymaže veškerý obsah ***Virového trezoru.*** Touto volbou jsou všechny soubory z ***Virového trezoru*** nevratně smazány z disku (*nebudou přesunuty do koše*).

13. Historie

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

- Výsledky testů
- Nález rezidentního štítu
- Nálezy Emailové ochrany
- Nálezy Webového štítu
- Protokol událostí
- Protokol Firewallu

13.1. Výsledky testů



Dialog ***Přehled výsledků testů*** je dostupný volbou položky ***Možnosti / Historie / Přehled výsledků testů*** v horním vodorovném menu hlavního okna **AVG Internet Security 2013**. V tomto dialogu je zobrazen seznam všech dříve spuštěných testů společně s informacemi o jejich průběhu a výsledku:

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

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

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

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

Ve všech případech může být ikona buďto celistvá nebo přepůlená - celá ikona značí, že test proběhl celý a byl řádně ukončen, přepůlená ikona identifikuje nedokončený nebo přerušený test.

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

- ***Čas začátku*** - datum a přesný čas spuštění testu
- ***Čas konce*** - datum a přesný čas ukončení testu
- ***Testovaných objektů*** - počet objektů, které byly během testu zkontrolovány
- ***Infekce*** - číslo udává počet nalezených / odstraněných virových infekcí
- ***High / Medium / Low*** - v těchto sloupcích je uveden počet celkově nalezených a odstraněných infekcí vysoké, sdtřední či nízké závažnosti
- ***Info*** - údaje o průběhu testu, zejména o jeho řádném či předčasném ukončení
- ***Rootkity*** - počet detekovaných rootkitů

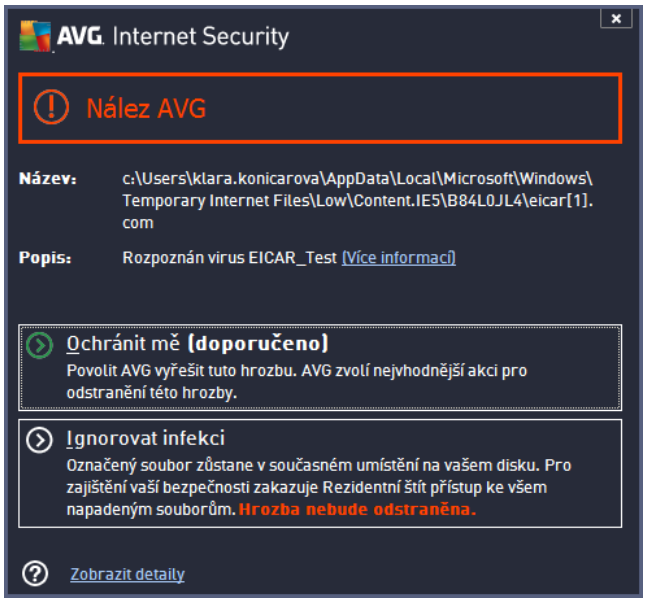
Ovládací tlačítka dialogu

Ovládacími tlačítky pro dialog ***Přehled výsledků testů*** jsou:

- ***Podrobnosti*** - stiskem tlačítka pak přejdete do dialogu Výsledky testu, kde se zobrazí podrobné informace o testu zvoleném v přehledu
- ***Smazat výsledek*** - stiskem tlačítka můžete záznam o zvoleném testu y přehledu testů odstranit
- - zpět do výchozího hlavního dialogu AVG *(přehled komponent)* se vrátíte prostřednictvím šipky v levém horním rohu tohoto dialogu

13.2. Nálezy Rezidentního štítu

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

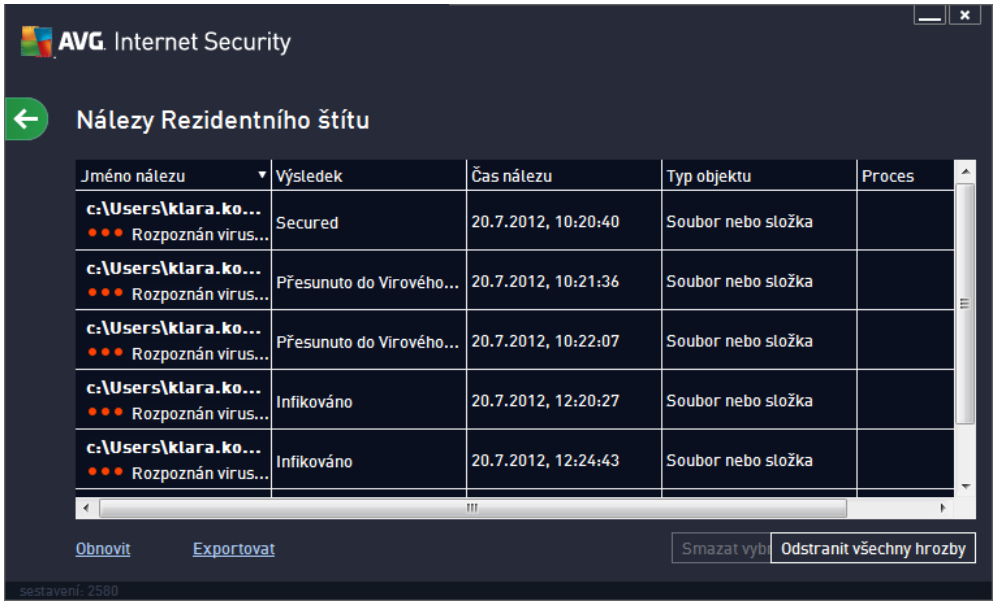


V tomto varovném dialogu najdete informaci o objektu, který byl detekován jako infikovaný (*Název*) a podrobnosti o rozpoznané infekci (*Popis*). Odkaz Více informací vás přesměruje do online virové encyklopedie, kde najdete podrobnější údaje o detekované infekci, jsou-li tyto informace k dispozici.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

Poznámka: *Může se stát, že velikost detekovaného objektu bude větší než objem volného prostoru ve Virovém trezoru. V tom případě budete při pokusu o přesun infikovaného objektu vyrozuměni varovným hlášením o nedostatku místa ve Virovém trezoru. Objem Virového trezoru si však můžete sami nastavit. Velikost prostoru ve Virovém trezoru je dána percentuálně a závisí na celkové velikosti vašeho pevného disku. Nastavení velikosti Virového trezoru lze provést v dialogu Virový trezor v rámci Pokročilého nastavení AVG, položka 'Omezit velikost Virového trezoru'.*

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

Přehled všech nálezů rezidentního štítu je dostupný v dialogu ***Nálezy Rezidentního štítu***. Tento dialog otevřete volbou položky ***Možnosti / Historie / Nálezy Rezidentního štítu*** v horním vodorovném menu hlavního okna **AVG Internet Security 2013**. V dialogu najdete seznam objektů, které byly rezidentním štítem detekovány jako nebezpečné a buďto vyléčeny nebo přesunuty do Virového trezoru.



U každého z detekovaných objektů jsou k dispozici následující informace:

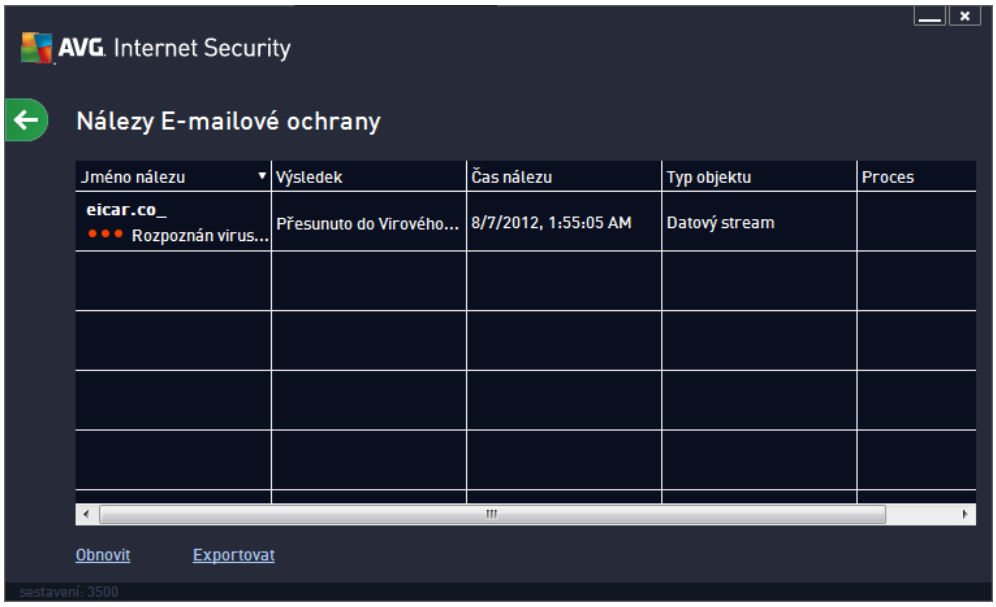
- ***Jméno nálezu*** - popis (*případně i jméno*) detekovaného objektu a jeho umístění
- ***Výsledek*** - jak bylo s detekovaným objektem naloženo (*blokace*)
- ***Čas nálezu*** - datum a čas, kdy došlo k detekci hrozby
- ***Typ objektu*** - jakého typu je detekovaný objekt
- ***Proces*** - při jaké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

Ovládací tlačítka

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

13.3. Nálezy Emailové ochrany

Dialog ***Nálezy Emailové ochrany*** je dostupný volbou položky ***Možnosti / Historie / Nálezy Emailové ochrany*** v horním vodorovném menu hlavního okna **AVG Internet Security 2013**.



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

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

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

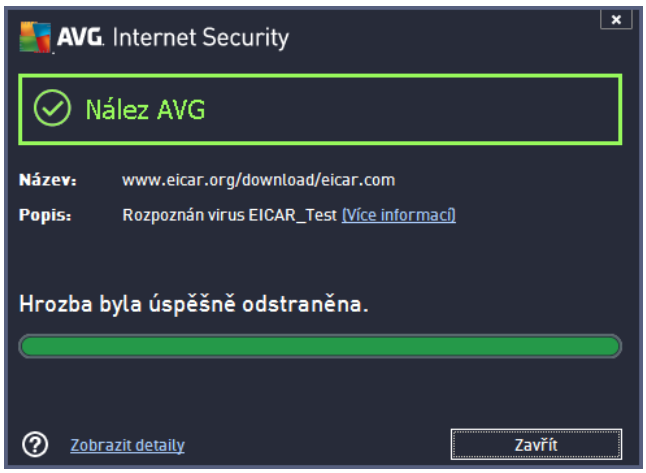
Ovládací tlačítka

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

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

13.4. Nálezy Webového štítu

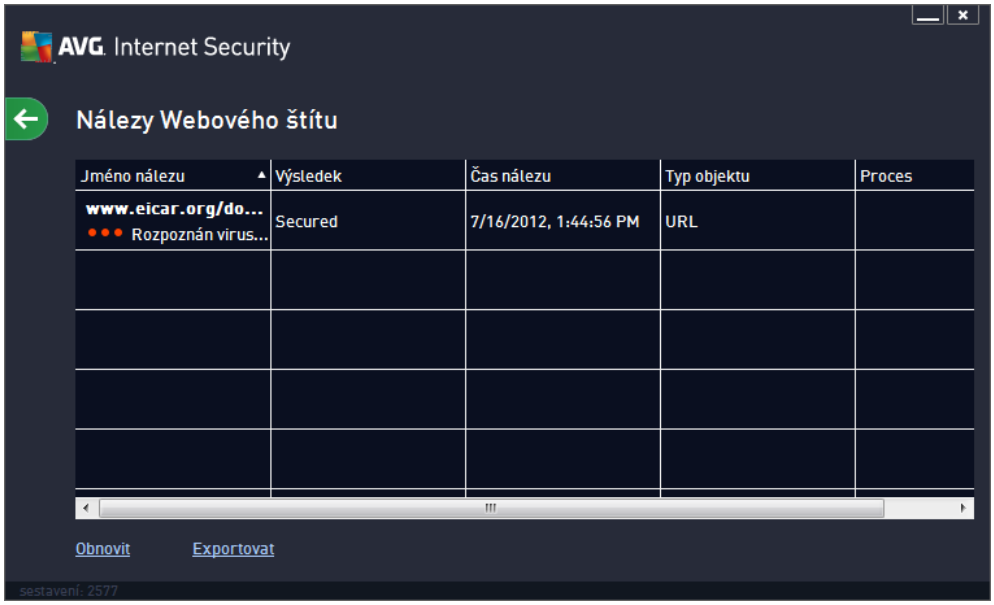
Webový štít kontroluje v reálném čase obsah webových stránek nebo souborů stahovaných z Internetu. Každá stránka je prověřena ještě předtím, než je skutečně stažena a zobrazena webovým prohlížečem. Jestliže detekuje virus nebo jakýkoliv podezřelý objekt, budete okamžitě varováni tímto dialogem:



V tomto varovném dialogu najdete informaci o objektu, který byl detekován jako infikovaný (*Název*) a podrobnosti o rozpoznané infekci (*Popis*). Odkaz Více informací vás přesměruje do online virové encyklopedie, kde najdete podrobnější údaje o detekované infekci, jsou-li tyto informace k dispozici. V dialogu jsou dostupná tato ovládací prvky:

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

Webová stránka s podezřelým souborem nebude otevřena a záznam o detekované infekci bude zaznamenán v přehledu ***Nálezy Webového štítu***. Tento přehled detekovaných nálezů je dostupný volbou položky ***Možnosti / Historie / Nálezy webového štítu*** v horním vodorovném menu hlavního okna **AVG Internet Security 2013**:



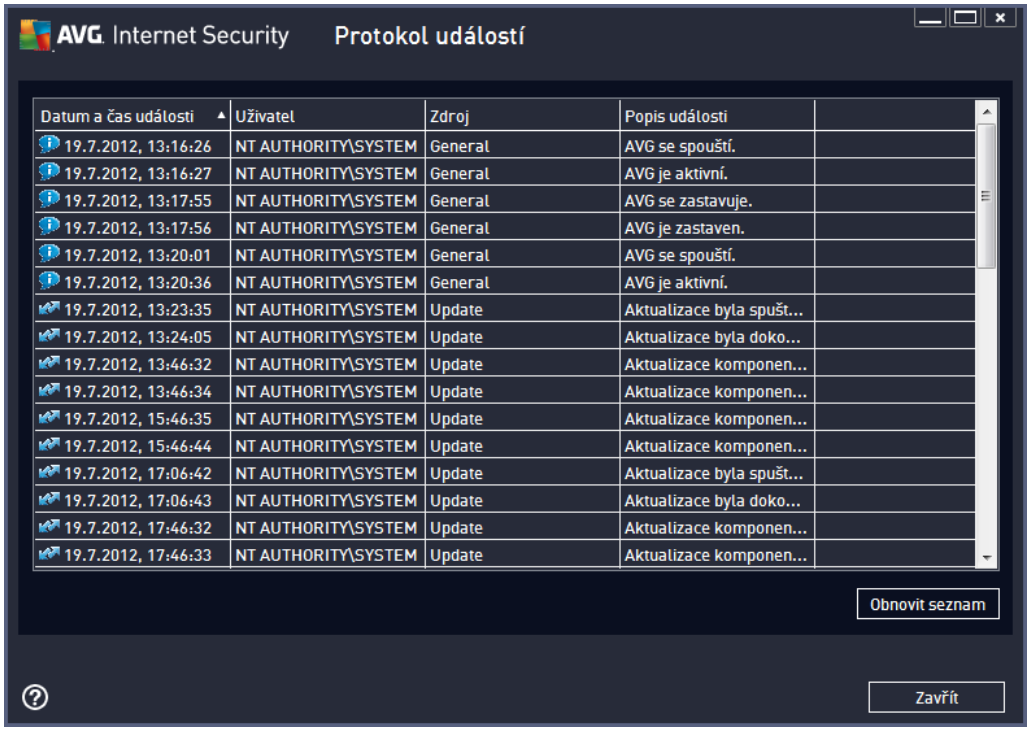
U každého z detekovaných objektů jsou k dispozici následující informace:

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

Ovládací tlačítka

- ***Obnovit*** - aktualizujete seznam všech nálezů
- ***Exportovat*** - máte možnost celý seznam detekovaných objektů do samostatného souboru
- - zpět do výchozího hlavního dialogu AVG *(přehled komponent)* se vrátíte prostřednictvím šipky v levém horním rohu tohoto dialogu

13.5. Protokol událostí



Dialog ***Protokol událostí*** je dostupný volbou položky ***Možnosti / Historie / Protokol událostí*** v horním vodorovném menu hlavního okna **AVG Internet Security 2013**. V tomto dialogu najdete přehled všech důležitých událostí, které nastaly v průběhu práce **AVG Internet Security 2013**. Zaznamenávány jsou různé typy událostí, například informace o aktualizacích programu, informace o spuštění/ukončení/přerušení testů (*včetně testů spouštěných automaticky*), informace o událostech týkající se nalezení viru (*při testování či Rezidentním štítem*) s uvedením konkrétního místa nálezu a informace o ostatních důležitých událostech.

Ké každé události jsou evidovány následující údaje:

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

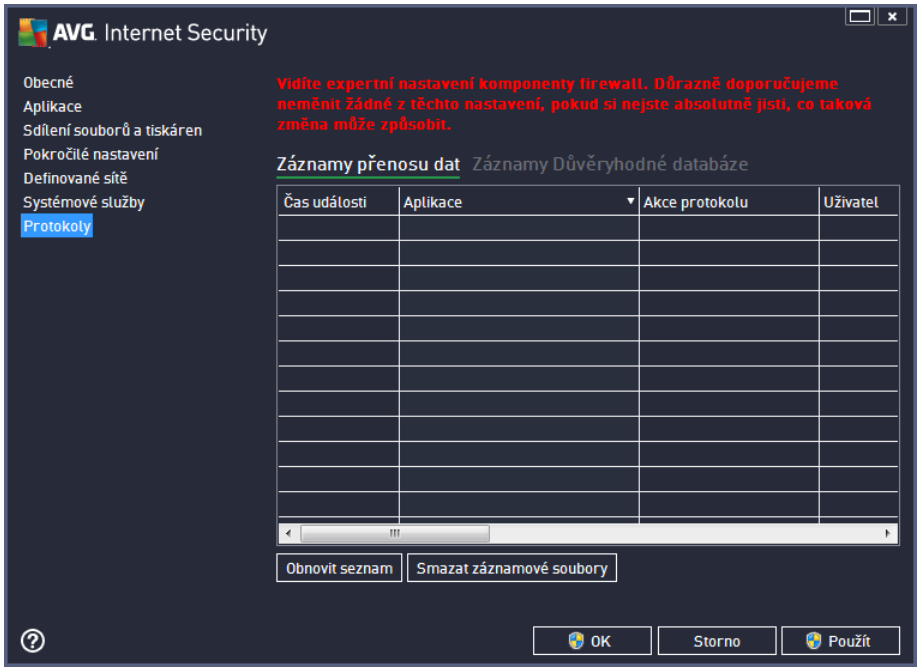
Ovládací tlačítka dialogu

- ***Obnovit seznam*** - stiskem tlačítka provedete aktualizaci záznamů v seznamu událostí
- ***Zavřít*** - stiskem tlačítka se vrátíte zpět do hlavního okna **AVG Internet Security 2013**

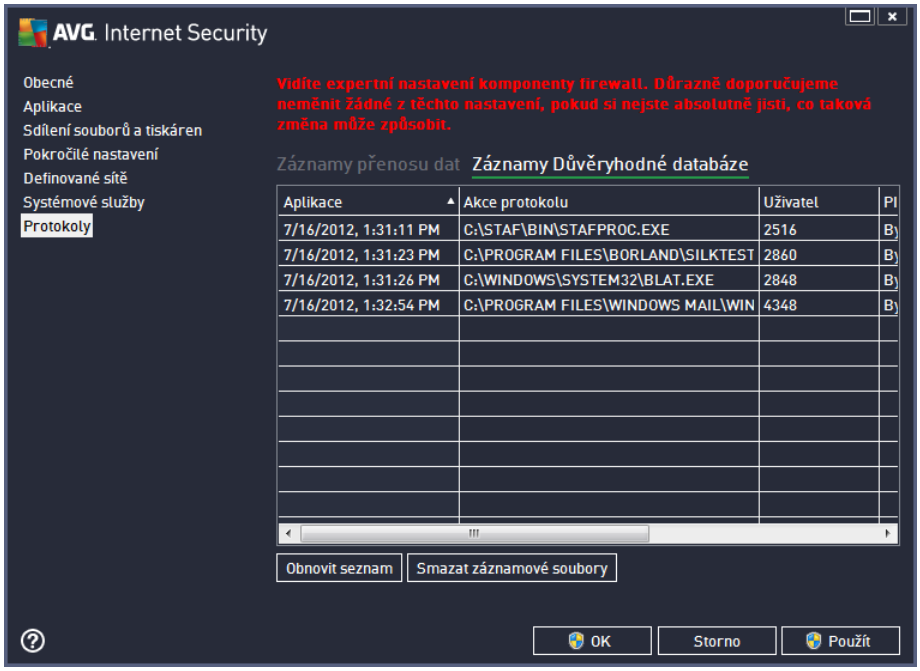
13.6. Protokol Firewallu

Dialog ***Protokoly*** nabízí seznamy všech protokolovaných událostí Firewallu s přehledem parametrů jednotlivých událostí, a to na dvou záložkách:

- ***Záznamy přenosu dat*** - Záložka nabízí informace o veškeré aktivitě aplikací, které se jakýkoliv způsobem pokusily o navázání síťové komunikace. U každého záznamu najdete údaje o čase události, jméno aplikace, která se pokoušela navázat spojení, příslušnou akci protokolu, jméno uživatele, PID, směr připojení, typ protokolu, číslo vzdáleného a místního portu a informaci o vzdálené i lokální IP adrese.



- ***Záznamy Důvěryhodné databáze*** - Důvěryhodná databáze je interní databází AVG, v níž jsou shromážděny informace o aplikacích, které mají ověřený certifikát, jsou prověřené a důvěryhodné, a komunikace jim může být povolena. Při prvním pokusu jakékoliv aplikace o navázání síťové komunikace (*tedy v situaci, kdy pro danou aplikaci ještě není nastaveno žádné pravidlo*) je třeba zjistit, zda má být této aplikaci komunikace povolena. AVG nejprve prohledá *Důvěryhodnou 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.



Ovládací tlačítka

- ***Obnovit seznam*** - Protokolované parametry lze řadit 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 odstraníte všechny záznamy z tabulky.

14. Aktualizace AVG

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

Vzhledem k tomu, jak rychle se dnes šíří nově vzniklé počítačové hrozby, je nezbytně nutné Váš **AVG Internet Security 2013** pravidelně aktualizovat. V ideálním případě ponechte prosím program ve výchozím nastavení, kdy je zapnuta automatická aktualizace. Bez aktuální virové databáze nebude **AVG Internet Security 2013** 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.

14.1. Spouštění aktualizace

Pro zajištění maximální bezpečnosti ověřuje **AVG Internet Security 2013** ve výchozím nastavení aktualizaci virové databáze 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 2013** bude aktuální během celého dne.

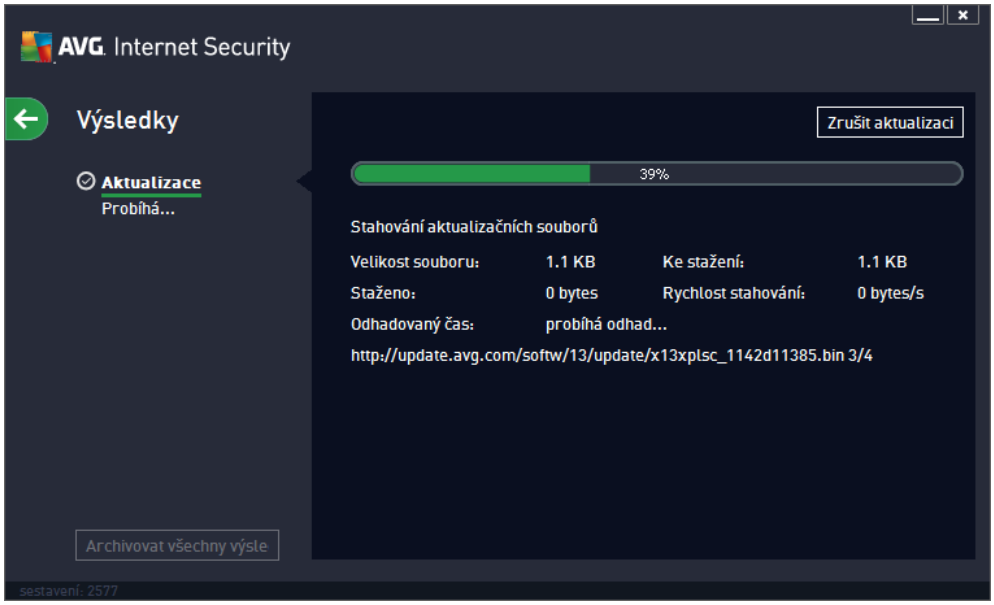
Pokud je virová databáze v **AVG Internet Security 2013** starší než jeden týden, budete o tomto stavu informováni oznamovacím dialogem ***Databáze je zastaralá***; pro vyřešení chyby spusťe aktualizaci ručně kliknutím na tlačítko Aktualizovat dostupné v hlavním dialogu aplikace. Toto tlačítko je vždy dostupné z kteréhokoliv dialogu uživatelského rozhraní AVG. Tlačítko můžete použít také v případě, že si přejete okamžitě ověřit existenci nových aktualizačních souborů.

Pokud chcete 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 dialozích:

- Plán aktualizace definic
- Plán programové aktualizace
- Plán aktualizace Anti-Spamu

14.2. Průběh aktualizace

Po spuštění aktualizace dojde nejprve k ověření, zda existují nové aktualizační soubory, jež dosud nebyly aplikovány. Pokud ano, **AVG Internet Security 2013** zahájí jejich okamžité stahování a spustí samotný proces aktualizace. V průběhu tohoto procesu budete přepnuti do samostatného dialogu ***Výsledky***, kde můžete sledovat průběh aktualizace v grafickém zobrazení a současně v přehledu statistických parametrů tohoto procesu (*velikost aktualizačního souboru, objem stažených dat, rychlost stahování, doba trvání, ...*):



14.3. Úrovně aktualizace

AVG Internet Security 2013 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 systémů (*souborový server*) doporučujeme neprovádět aktualizaci automaticky po jejím vydání, ale nejprve ji otestovat v testovacím prostředí.

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

- Plán aktualizace definic

- Plán programové aktualizace

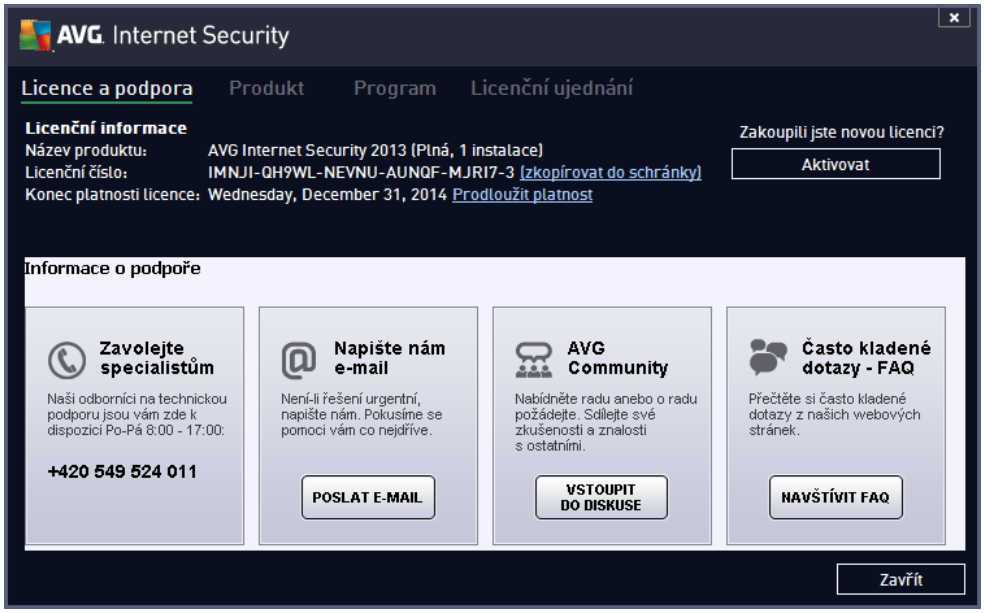
Poznámka: *Dojde-li k časovému souběhu naplánované programové aktualizace a naplánovaného testu, proces aktualizace je považován za prioritní a test bude přerušen.*

15. FAQ a technická podpora

Máte-li s Vaší aplikací **AVG Internet Security 2013** jakékoliv technické potíže nebo chcete-li položit obchodní dotaz, existuje několik způsobů, jak vyhledat pomoc. Zvolte si prosím některou z následujících možností:

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

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



- ***Řešení potíží v nápovědě***: Přímo v nápovědě programu **AVG Internet Security 2013** je nově k dispozici sekce ***Řešení potíží*** *(soubor nápevědy lze otevřít z kteréhokoliv dialogu aplikace stiskem klávesy F1)*. Ta nabízí výčet nejčastějších situací technického rázu, v nichž si uživatel přeje vyhledat odbornou pomoc. Zvolte prosím položku, která nejlépe vystihuje Váš aktuální problém a po rozkliknutí se otevře návod s podobným postupem doporučovaným pro tuto situaci.

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

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

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

také rady, jak odstranit viry, spyware a jak zůstat trvale chráněni.

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