



AVG Internet Security 2014

Uživatelský manuál

Verze dokumentace 2014.29 (29.7.2015)

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 libzip2, Copyright (c) 1996-2002 Julian R. Seward.

Tento produkt používá kompresní knihovnu zlib, Copyright (C) 1995-2002 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 požadavky na hardware	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 Dokončeno!	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	17
5.2 Informace o stavu zabezpečení	21
5.3 Přehled komponent	22
5.4 Moje aplikace	22
5.5 Zkratková tlačítka pro testování a aktualizaci	23
5.6 Ikona na systémové liště	23
5.7 AVG Advisor	25
5.8 AVG Accelerator	26
6. Komponenty AVG	27
6.1 Ochrana počítače	27
6.2 Ochrana na webu	31
6.3 Identity Protection	32
6.4 Ochrana e-mailu	33
6.5 Firewall	35



6.6 Komponenta Quick Tune	38
7. AVG Security Toolbar	40
8. AVG Do Not Track	43
8.1 Rozhraní služby AVG Do Not Track	43
8.2 Informace o sledovacích procesech	45
8.3 Blokování sledovacích procesů	45
8.4 Nastavení služby AVG Do Not Track	46
9. Pokročilé nastavení AVG	47
9.1 Vzhled	47
9.2 Zvuky	50
9.3 Dočasné vypnutí ochrany AVG	51
9.4 Ochrana počítače	52
9.5 Kontrola pošty	57
9.6 Ochrana na webu	71
9.7 Identity Protection	74
9.8 Testy	75
9.9 Naplánované úlohy	81
9.10 Aktualizace	89
9.11 Výjimky	92
9.12 Virový trezor	94
9.13 Vlastní ochrana AVG	95
9.14 Anonymní sběr dat	95
9.15 Ignorovat chybový stav	97
9.16 Advisor - známé sítě	98
10. Nastavení Firewallu	99
10.1 Obecné	99
10.2 Aplikace	101
10.3 Sdílené souborů a tiskáren	102
10.4 Pokročilé nastavení	103
10.5 Definované sítě	104
10.6 Systémové služby	105
10.7 Protokoly	106
11. AVG testování	109
11.1 Přednastavené testy	110
11.2 Testování v průzkumníku Windows	120



11.3 Testování z příkazové řádky.....	120
11.4 Naplánování testu.....	123
11.5 Výsledky testu.....	130
11.6 Podrobnosti výsledku testu.....	131
12. AVG File Shredder.....	132
13. Virový trezor.....	133
14. Historie	135
14.1 Výsledky testů.....	135
14.2 Nálezy Rezidentního štítu.....	137
14.3 Nález Identity Protection.....	139
14.4 Nálezy E-mailové ochrany.....	140
14.5 Nálezy Webového štítu.....	141
14.6 Protokol událostí.....	143
14.7 Protokol Firewallu.....	144
15. Aktualizace AVG.....	145
15.1 Spouštění aktualizace.....	145
15.2 Úrovně aktualizace.....	145
16. FAQ a technická podpora.....	147



1. Úvod

Tento uživatelský manuál je kompletní uživatelskou dokumentací programu **AVG Internet Security 2014**.

Aplikace **AVG Internet Security 2014** 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 bankovníctví, pohybovat se v sociálních sítích, procházet Internet a vyhledávat potřebné informace.

Kromě dokumentace můžete také využít dalších dostupných zdrojů informací o **AVG Internet Security 2014**:

- **Nápověda:** Přímo v nápovědě programu **AVG Internet Security 2014** je k dispozici sekce *Řešení problémů (soubor nápovědy lze otevřít z kteréhokoliv dialogu aplikace stiskem klávesy F1)*. Ta nabízí výčet nejčastějších situací technického rázu, v nichž si uživatel může vyhledat odbornou pomoc. Zvolte prosím položku, která nejlépe vystihuje Váš aktuální problém a po rozkliknutí se otevře návod s podrobným postupem doporučeným pro tuto situaci.
- **Centrum podpory na webu AVG:** Alternativní možností je vyhledat řešení svého problému na webu AVG (<http://www.avg.com/cz-cs/homepage>). V sekci **Centrum podpory** najdete strukturovaný přehled tematických okruhů, které řeší problémy obchodního i technického charakteru.
- **Časté dotazy:** Na webu AVG (<http://www.avg.com/cz-cs/homepage>) najdete také samostatnou a detailnějším způsobem nastavených otázek. Tato sekce je dostupná přes **Centrum podpory / Časté dotazy a návody**. Otázky jsou opět přehledně rozděleny do kategorií obchodní, technické a virové.
- **AVG ThreatLabs:** Samostatná AVG stránka (<http://www.avg.com/about-viruses>) je věnována virové tematice a poskytuje strukturovaný přehled informací souvisejících s hrozbami online. Najdete zde také rady, jak odstranit viry, spyware a jak zůstat trvale chráněni.
- **Diskusní fórum:** Můžete také využít diskusního fóra pro uživatele AVG produktů na adrese <http://forums.avg.com>.



2. Podmínky instalace AVG

2.1. Podporované operační systémy

AVG Internet Security 2014 je určen k ochraně pracovních stanic s těmito operačními systémy:

- Windows XP Home Edice SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edice SP1
- Windows Vista (všechny edice)
- Windows 7 (všechny edice)
- Windows 8 (všechny edice)
- Windows 10 (všechny edice)

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

Poznámka: Komponenta [Identita](#) není podporována na Windows XP x64. Na tomto operačním systému lze nainstalovat AVG Internet Security 2014, ale pouze bez této komponenty.

2.2. Minimální / doporučené požadavky na hardware

Minimální hardwarové požadavky pro **AVG Internet Security 2014**:

- 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 instalace odvodeno)

Doporučené hardwarové požadavky pro **AVG Internet Security 2014**:

- 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 instalace odvodeno)

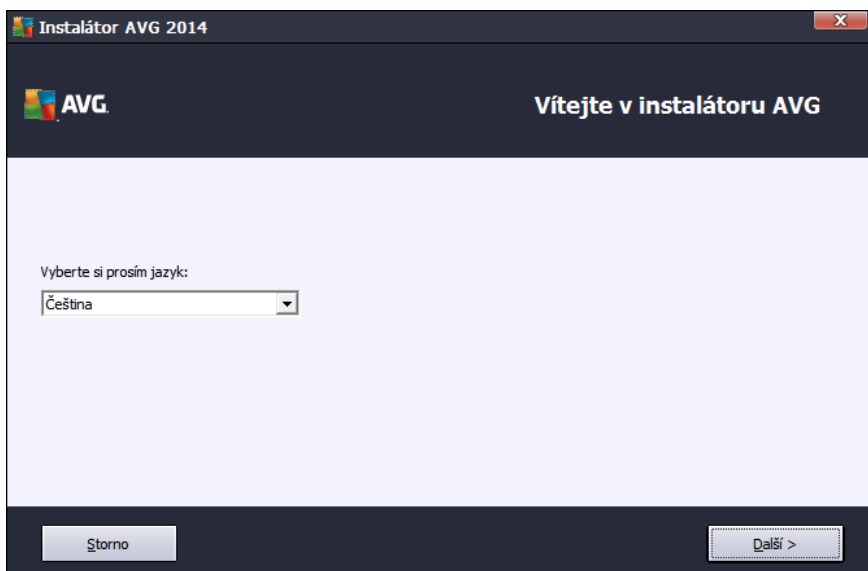


3. Instalační proces AVG

Pro instalaci **AVG Internet Security 2014** na váš počítač budete potřebovat aktuální instalační soubor. Abyste zajistili, že instalujete vždy nejnovější verzi **AVG Internet Security 2014**, je vhodné stáhnout si instalační soubor z webu AVG (<http://www.avg.com/cz-cs/homepage>). V sekci **Podpora** najdete strukturovaný přehled instalačních souborů k jednotlivým edicím AVG. 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**:



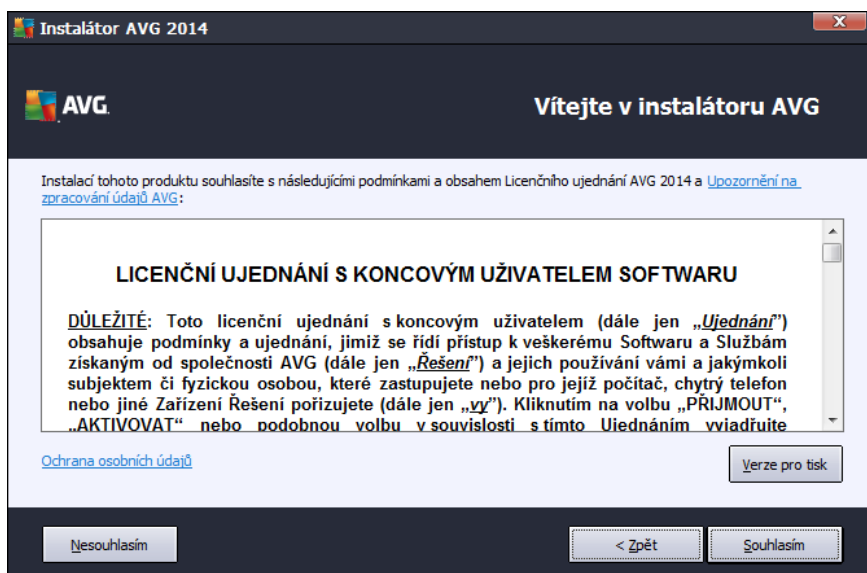
V tomto dialogu máte možnost zvolit jazyk instalačního procesu. Kliknutím na rozbalovací menu otevřete nabídku všech dostupných jazyků. Po potvrzení Vaší volby bude instalační proces nadále probíhat ve zvoleném jazyce.

Pozor: V tuto chvíli volíte pouze jazyk instalačního procesu. Aplikace AVG Internet Security 2014 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:



P e t te si prosím pe liv celý text závazné licenční smlouvy AVG. Sv j souhlas s licenčním ujednáním potvr te stiskem tlačítka **Souhlasím**. Pokud s licenční smlouvou nesouhlasíte a stisknete tlačítko **Nesouhlasím**, instalace bude okamžit ukon ena.

Upozornění na zpracování údajů AVG a Ochrana osobních údajů

Krom licenčního ujednání se v tomto kroku instalace m žete také seznámit s **Upozorněním na zpracování údajů AVG** a s **Ochranou osobních údajů**. Ob funkce jsou v dialogu zobrazeny formou aktivního odkazu na speciální webovou stránku, kde najdete podrobné informace. Kliknutím na příslušný odkaz budete př esm rováni na webovou stránku AVG (<http://www.avg.com/cz-cs/homepage>), která Vás v plném rozsahu seznámí s požadovaným prohlášením.

Ovládací tlačítka dialogu

V prvním dialogu instalace jsou k dispozici tato ovládací tlačítka:

- **Verze pro tisk** - Tímto tlačítkem máte možnost zobrazit plné znění licenční smlouvy ve webovém rozhraní v př ehledném formátu pro tisk.
- **Souhlasím** - Kliknutím potvrzujete, že jste etli licenční ujednání a přijímáte jej v plném rozsahu. Instalace bude pokračovat př echodem do následujícího dialogu instalačního procesu.
- **Nesouhlasím** - Kliknutím odmítáte přijmout licenční ujednání. Instalační proces bude bezprost edn ukon en. **AVG Internet Security 2014** 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:

Instalátor AVG 2014

AVG **Aktivujte vaši licenci**

Licenční číslo:

Příklad: IQNP6-9BCA8-PUQU2-ASHCK-GP338L-93OCB

Pokud jste zakoupili software AVG online, licenční číslo vám bylo zasláno e-mailem. Abyste předešli chybám při opisu, doporučujeme zkopírovat číslo z e-mailu a vložit je přes schránku do tohoto dialogu.

Pokud jste software zakoupili v kamenném obchodě, najdete licenční číslo na registrační kartě produktu v jeho balení. Ověřte prosím, že jste číslo zkopírovali správně.

Storno < Zpět Další >

Kde najdu licenční číslo

Licenční číslo najdete buďto na registrační kartě v krabicovém balení **AVG Internet Security 2014**, anebo v potvrzovacím e-mailu, který jste obdrželi při zakoupení **AVG Internet Security 2014** on-line. Licenční číslo musí být zadáno naprosto přesně ve tvaru, jak je uvedeno, proto prosím věnujte velkou pozornost jeho přesnému opisu. Pokud máte číslo k dispozici v digitální formě, doporučujeme jej do příslušného pole zkopírovat (*metodou kopírovat a vložit*).

Jak použít metodu Copy & Paste

Následující popis kroků je stručným popisem toho, jak použít metodu **Copy & Paste** (*kopíruj a vlož*) při vkládání licenčního čísla **AVG Internet Security 2014**:

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



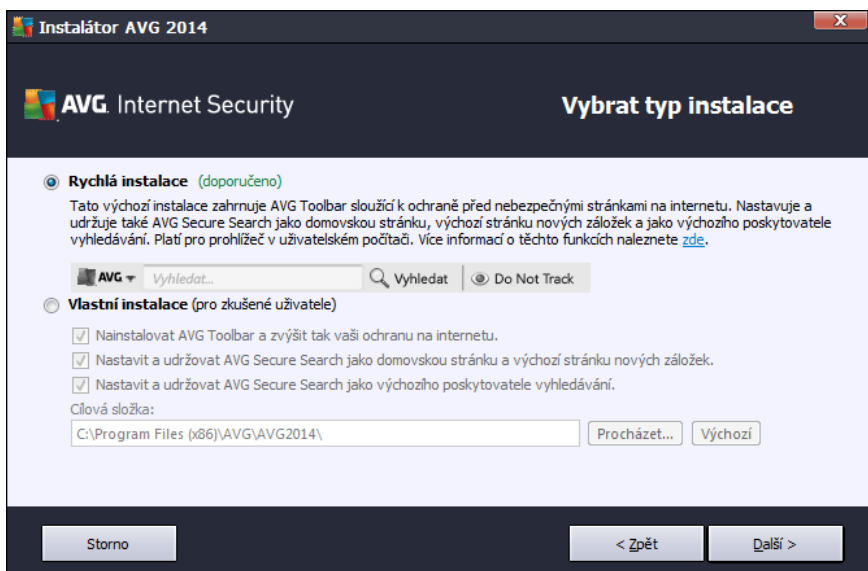
Ovládací tlačítka dialogu

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 2014** 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 **Rychlou instalací** a **Vlastní instalací**:



Rychlá instalace

Většinou uživatel doporučí použít rychlou instalaci. Tak bude **AVG Internet Security 2014** nainstalován zcela automaticky s konfigurací definovanou výrobcem, včetně [AVG Security Toolbaru](#). Výchozí nastavení zaručuje maximální úroveň bezpečnosti a optimální využití zdrojů. Pokud se v budoucnu vyskytne potřeba, které konkrétní nastavení změnit, budete mít vždy možnost editovat konfiguraci **AVG Internet Security 2014** přímo v aplikaci.

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

Vlastní instalace

Vlastní instalace je vhodná pouze pro pokročilé a znalé uživatele. Doporučit ji lze v případě, že máte skutečně specifické požadavky vašeho systému. Pokud se rozhodnete pro uživatelskou instalaci, aktivuje se v dialogu několik dalších možností volby:



- **Nainstalovat AVG Toolbar a zvýšit tak vaši ochranu na internetu** - Pokud nezmníte výchozí nastavení, bude tato komponenta automaticky nainstalována do vašeho výchozího internetového prohlížeče a zajistí kompletní on-line ochranu při prohlížení webu. Podporovanými prohlížeči jsou Internet Explorer (ve verzi 6.0 a vyšší) a/nebo Mozilla Firefox (ve verzi 3.0 a vyšší). Jiné prohlížeče nejsou podporovány; pokud používáte alternativní prohlížeč, například Avant browser, můžete se setkat s nekorektním chováním.
- **Nastavit a udržovat AVG Secure Search jako domovskou stránku a výchozí stránku nových záložek** - Pokud ponecháte tuto volbu zapnutou, AVG Secure Search bude ve vašem výchozím prohlížeči automaticky nastaven jako domovská stránka a každé nově otevřené okno se bude otevírat s tímto nastavením.
- **Nastavit a udržovat AVG Secure Search jako výchozího poskytovatele vyhledávání** - Pokud ponecháte 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.
- **Cílová složka** - Zde máte možnost určit, kam má být program **AVG Internet Security 2014** instalován. Ve výchozím nastavení bude program instalován do adresáře programových souborů umístěném typicky na disku C:, jak je uvedeno v textovém poli v tomto dialogu. Pokud si přejete toto umístění změnit, pomocí tlačítka **Procházet** zobrazíte strukturu vašeho disku a zvolíte požadovaný adresář. Chcete-li se následně vrátit k předchozímu umístění definovanému výrobcem, můžete tak učinit pomocí tlačítka **Výchozí**.

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

Ovládací tlačítka dialogu

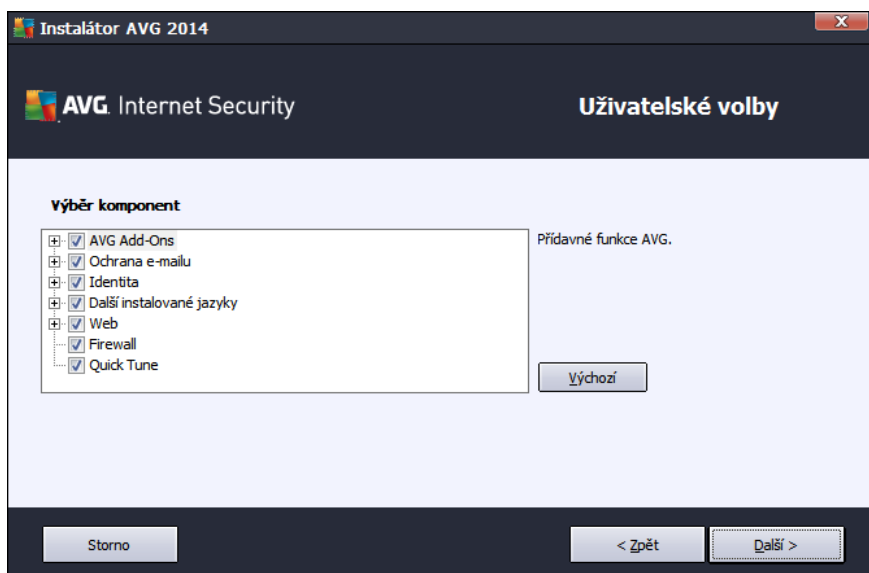
Podobně jako ve většině dialogů instalace, jsou i zde dostupná tři ovládací tlačítka:

- **Storno** - Kliknutím na toto tlačítko bezprostředně ukončíte instalační proces; **AVG Internet Security 2014** nebude nainstalován!
- **Zpět** - Kliknutím na tlačítko se vrátíte o jeden krok zpět do předchozího dialogu instalačního procesu.
- **Další** - Kliknutím na tlačítko pokračujete v instalačním procesu a přejdete do následujícího dialogu.



3.5. Uživatelské volby

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



Sekce *Výběr komponent* nabízí přehled komponent **AVG Internet Security 2014**, které můžete nainstalovat. Pokud vám výchozí nastavení nevyhovuje, máte možnost jednotlivé komponenty odebrat/přidat. **Volit můžete pouze z těch komponent, které jsou zahrnuté ve vaší zakoupené licenci AVG. Pouze tyto komponenty vám také budou v dialogu nabídnuty!** Označte kteroukoliv komponentu v seznamu *Výběr komponent* a po pravé straně se zobrazí stručný popis funkcí této komponenty. Podrobné informace o jednotlivých komponentách najdete v kapitole [Přehled komponent](#). Chcete-li se vrátit k výchozí konfiguraci nastavené výrobcem, stisknete tlačítko **Výchozí**.

Ovládací tlačítka dialogu

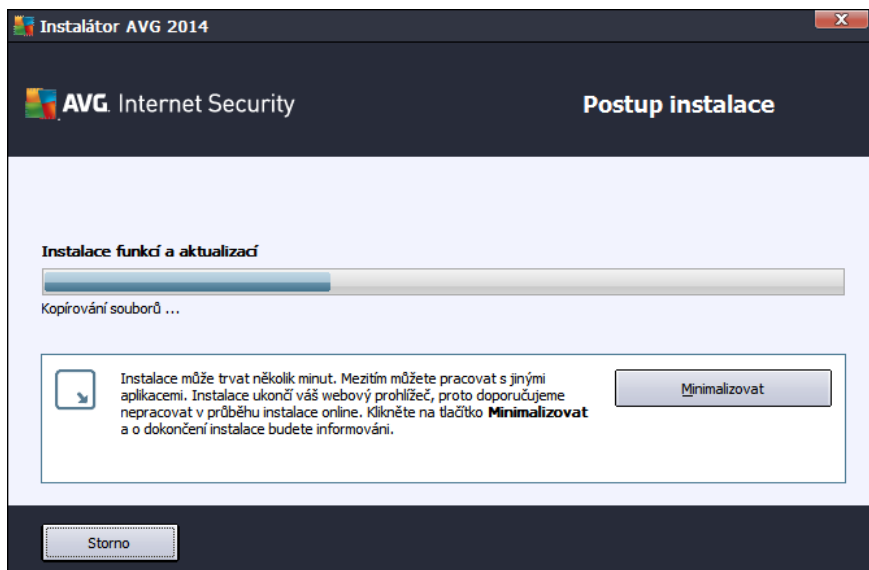
Podobně jako ve většině dialogů instalace, jsou i zde dostupná tři ovládací tlačítka:

- **Storno** - Kliknutím na toto tlačítko bezprostředně ukončíte instalační proces; **AVG Internet Security 2014** 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:



Poklejte prosím na dokončení instalace. Poté budete automaticky přemístěni k následujícímu dialogu.

Ovládací tlačítka dialogu

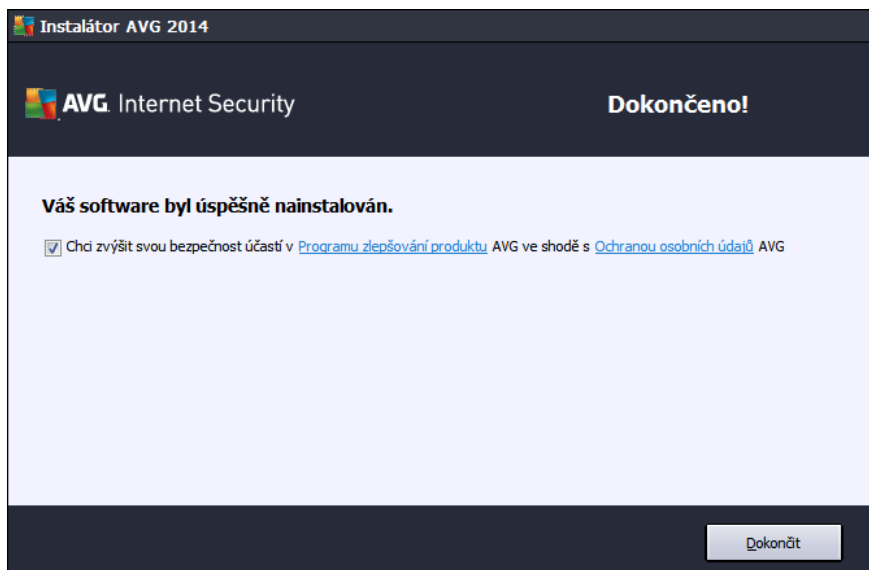
V dialogu jsou dostupná dvě ovládací tlačítka:

- **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, pokud byste si běžící instalační proces přerušit. V takovém případě nebude **AVG Internet Security 2014** nainstalován!



3.7. Dokončeno!

Dialog **Dokončeno!** potvrzuje, že **AVG Internet Security 2014** byl plně nainstalován a nastaven k optimálnímu výkonu:



Program zlepšování produktu a ochrana osobních údaj

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 údaj; kliknutím na odkaz **Ochrana osobních údaj** budete přesměrováni na webovou stránku AVG (<http://www.avg.com/cz-cs/homepage>), která Vás v plném rozsahu seznámí se zásadami ochrany osobních údaj 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 2014** prosím zaregistrujte svůj produkt na webu AVG (<http://www.avg.com/cz-cs/homepage>). Registrace vám umožní získat přístup k uživatelskému účtu AVG, dostávat informace o aktualizacích AVG, a zprostředkuje další služby poskytované registrovaným uživateli AVG. Nejsnazší přístup k registraci je přímo z prostředí aplikace **AVG Internet Security 2014**, a to volbou položky [Možnosti / Registrovat](#). Následně budete přesměrováni na stránku **Registrace** na webu AVG (<http://www.avg.com/cz-cs/homepage>), 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 2014**

4.3. Spuštění testu celého počítače

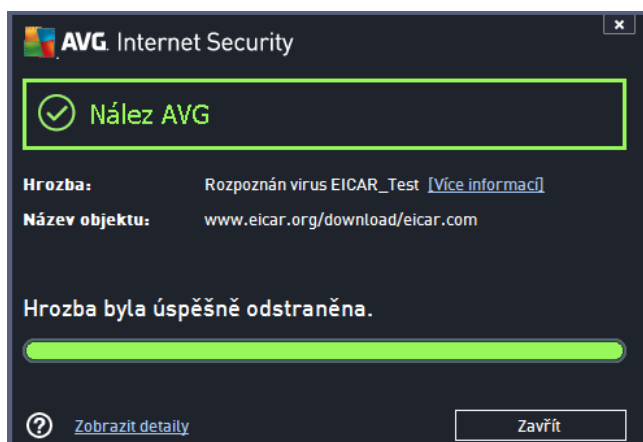
Jelikož existuje jisté riziko, že virus byl na váš počítač zavlečen již před instalací **AVG Internet Security 2014**, doporučujeme po instalaci spustit [Test celého počítače](#), který zkontroluje celý počítač a ověří přítomnost virů a potenciálně nežádoucích programů. První test počítače může trvat asi hodinu, ale z hlediska vaší bezpečnosti je skutečně nanejvýš dležitější jej nechat probíhat. Instrukce ke spuštění testu najdete v kapitole [AVG testování](#).

4.4. Test virem Eicar

Chcete-li ověřit, že **AVG Internet Security 2014** 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. Váš produkt na něj reaguje, jako by virem byl (*protože jsou schopny jej rozpoznat a označit skutečným jménem; hlásí jeho přítomnost například takto "EICAR-AV-Test"*). 'Virus' EICAR si můžete stáhnout z internetu na adrese <http://www.eicar.com>, kde také najdete všechny nezbytné informace o 'viru' samotném a testování tímto 'virem'.

Stáhněte si soubor *eicar.com* a pokuste se jej uložit na lokální disk. Ihned poté, co potvrdíte stažení testovacího souboru, zareaguje **AVG Internet Security 2014** varovným upozorněním. Toto upozornění dokazuje, že **AVG Internet Security 2014** na vašem počítači je správně nainstalován:



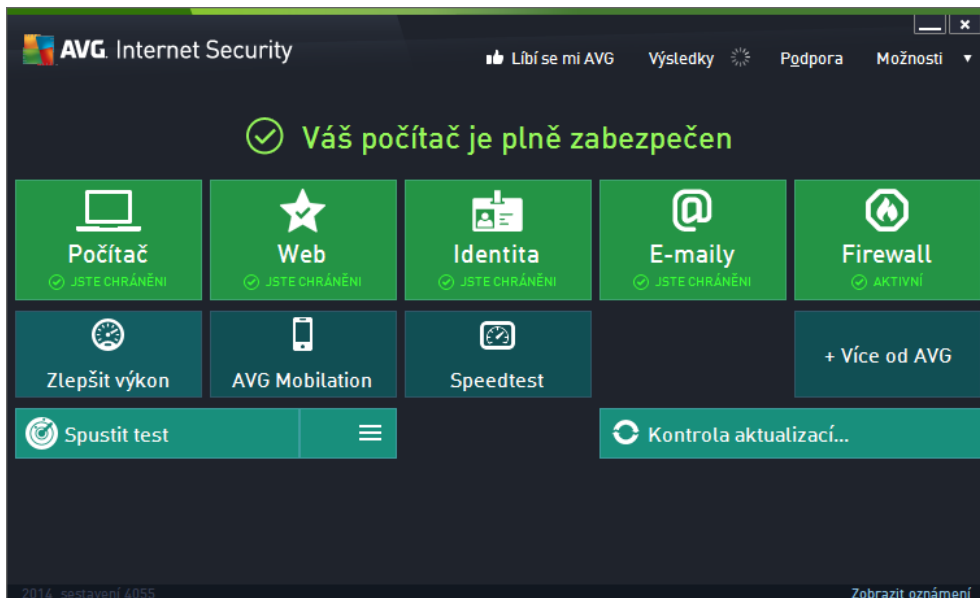
Pokud není testovací soubor EICAR identifikován jako virus, je nutné znovu provést konfiguraci AVG Internet Security 2014!

4.5. Výchozí konfigurace AVG

Ve výchozí konfiguraci (*bezprostředně po instalaci*) jsou všechny komponenty a funkce **AVG Internet Security 2014** nastaveny výrobcem k optimálnímu výkonu bezpevnostního software. ***Pokud nemáte skutečný důvod jejich konfiguraci změnit, doporučujeme ponechat program v tomto nastavení! Změnu konfigurace by měl provádět pouze zkušený 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 2014 se otevírá 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 (*Libí se mi AVG, Výsledky, Podpora, Možnosti*). [Podrobnosti >>](#)
- **Informace o stavu zabezpečení** podává základní informaci o aktuálním stavu **AVG Internet Security 2014**. [Podrobnosti >>](#)
- **Přehled instalovaných komponent** najdete ve vodorovném pásmu 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 pásmu hlavního okna a nabízejí přehled doplňkových aplikací **AVG Internet Security 2014**, které buďto již máte nainstalovány na svém počítači, nebo jejichž instalaci vám doporučujeme. [Podrobnosti >>](#)
- **Zkratková tlačítka pro testování a aktualizaci** ve spodní části hlavního okna umožní rychlý přístup k nejdůležitějším a nejčastěji používaným funkcím **AVG Internet Security 2014**. [Podrobnosti >>](#)

Mimo hlavní okno **AVG Internet Security 2014** můžete k aplikaci přistupovat ještě prostřednictvím následujícího prvku:

- **Ikona na systémové liště** se nachází v pravém dolním rohu monitoru (*na systémové liště*) a je indikátorem aktuálního stavu **AVG Internet Security 2014**. [Podrobnosti >>](#)

5.1. Horní navigace

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

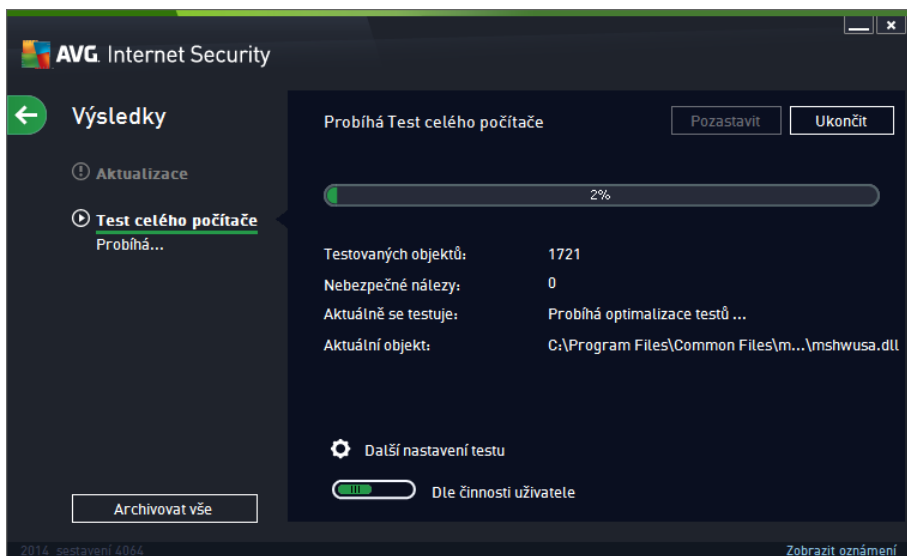


5.1.1. Líbí se mi AVG

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

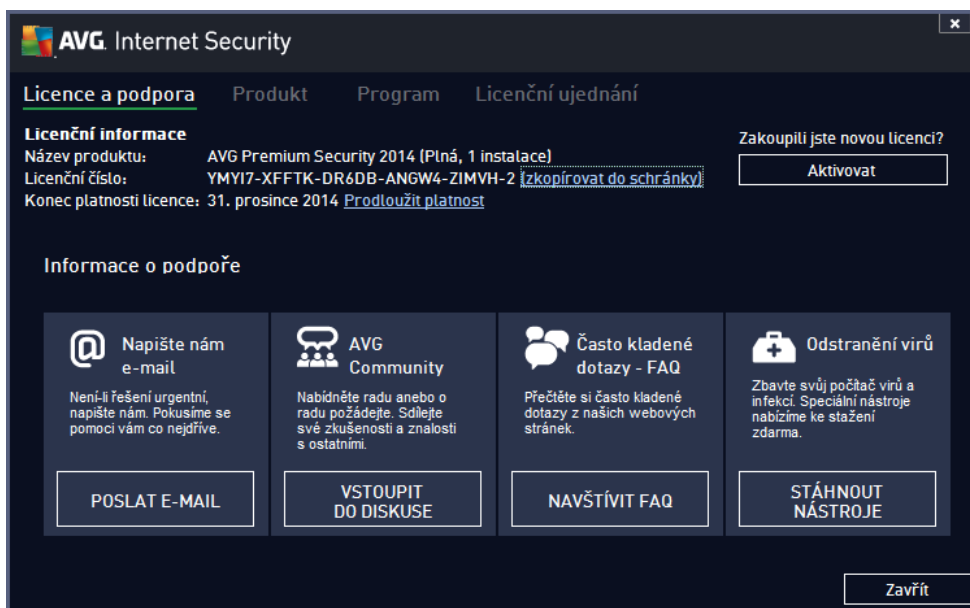
5.1.2. Výsledky

Otevírá samostatný dialog **Výsledky**, v němž najdete přehled všech relevantních hlášení o problému a výsledcích spuštěných testů a aktualizací. Pokud test nebo proces aktualizace právě probíhá, 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 samostatný dialog, v němž jsou na čtyřech záložkách shrnuty informace o **AVG Internet Security 2014** podobně například v kontaktu se zákaznickou podporou:





- **Licence a podpora** - Záložka nabízí pohled licenčních informací, tedy název produktu, licenční číslo a konec platnosti licence. Ve spodní části dialogu najdete také pohledný 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 2014 instalovali), nebo kterým změníte dosavadní licenční číslo za jiné (např. při přechodu na jiný produkt z řady AVG).
 - **Zkopírovat do schránky** - Kliknutím na odkaz **Zkopírovat do schránky** bude vaše licenční číslo uloženo do schránky a můžete jej prostým vložením použít kdekoliv potřebujete. Tím je zajištěno, že při jeho přepisování nedojde k chybám.
 - **Prodloužit platnost** - Prodloužit platnost licence **AVG Internet Security 2014** je možné kdykoliv, nejlépe však aspoň jeden měsíc před datem expirace. Na blížící se datum expirace budete upozorněni. Kliknutím na odkaz budete přesměrováni na stránku na webu AVG (<http://www.avg.com/cz-cs/homepage>), kde najdete podrobné informace o aktuálním stavu vaší licence, datum expirace a nabídku možností prodloužení licence.
- **Produkt** - Záložka podává pohled nejdůležitějších technických informací o **AVG Internet Security 2014** rozdělených do sekcí informace o produktu, instalované komponenty a nainstalovaná ochrana e-mailů.
- **Program** - Záložka uvádí přesný název instalované edice **AVG Internet Security 2014** a číslo verze instalačního souboru. Dále jsou uvedeny informace o použitém kódu těchto stran.
- **Licenční ujednání** - Na záložce najdete plné znění licenčního ujednání mezi Vámi a společností AVG Technologies.

5.1.4. Možnosti

Ovládání vašeho **AVG Internet Security 2014** je dostupné prostřednictvím jednotlivých možností sdružených v položce **Možnosti**. Kliknutím na šipku vedle této položky otevřete rozbalovací menu s následující nabídkou:

- **Otestovat počítač** - Přímo spouští test celého počítače.
- **Otestovat zvolený adresář ...** - Přepíná do testovacího rozhraní AVG a nabízí ve stromové struktuře vašeho disku možnost definovat ty složky, které mají být otestovány.
- **Otestovat soubor...** - Umožňuje spustit test na vyžádání pouze nad jedním konkrétním souborem. Kliknutím na tuto volbu se otevře nové okno s náhledem stromové struktury vašeho disku. Zvolte požadovaný soubor a potvrďte spuštění testu.
- **Aktualizace** - Automaticky spouští proces aktualizace **AVG Internet Security 2014**.
- **Aktualizace z adresáře ...** - Spustí proces aktualizace z aktualizací souboru umístěného v definovaném adresáři na lokálním disku. Tuto alternativu doporučujeme pouze jako náhradní řešení pro případ, že v danou chvíli nebude k dispozici připojení k Internetu (např. počítač je zavazován a odpojen ze sítě, počítač je připojen k síti, kde není přístup k Internetu, apod.). V nově otevřeném okně vyberte adresář, do nějž jste předem umístili aktualizací soubory, a spusťte aktualizaci.
- **Virový trezor** - Otevírá rozhraní karanténního prostoru, Virového trezoru, kam jsou přesouvány všechny detekované infekční soubory. V tomto prostoru jsou soubory zcela izolovány a tím je



zajištění na nejspolehlivější úrovni, a současně zde lze hrozby uložit pro případnou další práci s nimi.

- **Historie** se dělí na další specifické podkategorie:
 - [Výsledky test](#) - Přepíná do testovacího rozhraní AVG, konkrétně do dialogu s pohledem na výsledek testu.
 - [Nálezy Rezidentního štítu](#) - Otevírá dialog s pohledem na infekce detekované Rezidentním štítem.
 - [Nález Identity Protection](#) - Otevírá dialog s pohledem na detekce komponenty [Identita](#).
 - [Nálezy E-mailové ochrany](#) - Otevírá dialog s pohledem na přílohy detekované jako nebezpečné komponentou Ochrana e-mailu.
 - [Nálezy Webového štítu](#) - Otevírá dialog s pohledem na infekce detekované Webovým štítem.
 - [Protokol událostí](#) - Otevírá dialog historie událostí s pohledem na všechny protokolované akce **AVG Internet Security 2014**.
 - [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 2014**. 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 [dedikovaný dialog](#) s pohledem na všechny dostupné informace a kontakt zákaznické podpory.
- **AVG na webu** - Otevírá web AVG (<http://www.avg.com/cz-cs/homepage>).
- **Informace o viřech** - Otevírá viřovou encyklopedii na webu AVG (<http://www.avg.com/cz-cs/homepage>), v níž lze dohledat podrobné informace o detekovaných nálezech.
- **(Re)Aktivovat** - Otevírá aktivační dialog, v němž je třeba vyplnit licenční číslo, které jste zadali během instalačního procesu. Licenční číslo lze v dialogu editovat. Buďte si vědomi, že můžete nahradit prodejní číslo, s nímž jste AVG instalovali, číslem licenčním, anebo změnit dosavadní licenční číslo za jiné, například v případě přechodu na jiný produkt značky AVG. Máte-li nainstalovanou zkušební verzi **AVG Internet Security 2014**, dvě poslední uvedené položky se zobrazí jako **Zakoupit** a **Aktivovat** a odkáží Vás na web AVG, kde si můžete přímě zakoupit plnou verzi programu. Pokud máte nainstalovaný program **AVG Internet Security 2014** s prodejním číslem, položky se zobrazí jako **Zaregistrovat** a **Aktivovat**.
- **Registrovat / MyAccount** - Otevírá web AVG (<http://www.avg.com/cz-cs/homepage>) 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. (Tentýž dialog je k dispozici volbou položky [Podpora](#) v navigaci přímo v hlavním okně aplikace.)

5.2. Informace o stavu zabezpečení

Sekce **Informace o stavu zabezpečení** je umístěna v horní části rozhraní **AVG Internet Security 2014**. V této sekci najdete vždy informaci o aktuálním stavu vašeho **AVG Internet Security 2014**. V sekci můžete být zobrazena jedna z následujících ikon, jejichž význam vysvětlujeme:



- Zelená ikona informuje, že **program AVG Internet Security 2014 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. Prosím vnujte 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 v domě rozhodli ignorovat chybový stav komponenty. Volba **Ignorovat chybový stav** je dostupná volbou v tve [Ignorovat chybový stav](#) v [Pokročilém nastavení](#). Touto volbou dáváte najevo, že jste si v domě fakt, že se konkrétní komponenta nachází v chybovém stavu, ale z nějakého důvodu si přejete tento stav zachovat a nebyť na něj upozorování. Může nastat situace, kdy budete potřebovat využít této možnosti, ale rozhodně nedoporučujeme, abyste v tomto stavu setrvali déle, než je nutné!

Alternativně bude žlutá ikona zobrazena také v situaci, kdy **AVG Internet Security 2014** vyžaduje restart počítače (**Restartovat nyní**). Vnujte prosím pozornost tomuto varování a počítač restartujte!



- Oranžová ikona **informuje o kritickém stavu AVG Internet Security 2014!** Některá z komponent je nefunkční a **AVG Internet Security 2014** nemůže plně chránit váš počítač. Vnujte prosím okamžitou pozornost opravě tohoto problému! Pokud nebudete sami schopni problém odstranit, kontaktujte oddělení [technické podpory AVG](#).

V případě, kdy **AVG Internet Security 2014** není nastaven k plnému a optimálnímu výkonu se vedle **informace o stavu zabezpečení** zobrazí tlačítko **Opravit** (v případě **Opravit vše**, pokud se problém týká více než jediné komponenty), jehož stiskem **AVG Internet Security 2014** automaticky spustí proces kontroly a přenastavení všech parametrů k optimálnímu výkonu. Tímto tlačítkem snadno uvedete program do optimálního stavu a zajistíte tak nejvyšší úroveň bezpečnosti!

Doporučujeme, abyste vnovi pozornost údajům zobrazeným v sekci **Informace o stavu zabezpečení** a pokud **AVG Internet Security 2014** hlásí jakýkoliv problém, zaměřte se na jeho řešení. Pokud ignorujete chybová hlášení **AVG Internet Security 2014**, váš počítač je ohrožen!

Poznámka: Informaci o stavu **AVG Internet Security 2014** 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 [hlavního 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, vnujte pozornost konfiguraci komponenty, která není nastavena k plné aktivitě!**

Připejzdou myši přes grafické znázornění komponenty se ve spodní části [hlavního okna](#) zobrazí krátký text. Ten vás seznámí se základní funkcí zvolené komponenty. Dále podává informaci o aktuálním stavu komponenty, případně upozorní, která služba v rámci dané komponenty není nastavena k optimálnímu výkonu.

Seznam instalovaných komponent

V rámci **AVG Internet Security 2014** najdete v sekci **Přehled komponent** informace o těchto komponentách:

- **Pořítač** - Komponenta zahrnuje dva ochranné procesy: **AntiVirus Shield** detekuje na vašem počítači viry, spyware, červy, trojany, nežádoucí spustitelné soubory nebo knihovny a chrání vás před nimi; **Anti-Rootkit** testuje všechny aplikace, ovladače a knihovny na přítomnost skrytých rootkitů. [Podrobnosti >>](#)
- **Web** - 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 >>](#)
- **E-mail** - 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

- **Připejzdou 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** (záhlaví zelených bloků pod sadou komponent) najdete přehled doplnkových aplikací AVG, které buďto již máte nainstalovány na svém počítači, nebo jejichž instalaci vám doporučíme. Grafické bloky znázorněné v této sekci se zobrazují podmíněně 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 se sdílet se svou rodinou i přáteli.
- **Family Safety** pomáhá ochránit vaše děti před nevhodným obsahem webových stránek, internetových médií a výsledkům vyhledávání. AVG Family Safety umožňuje sledovat i aktivity Vašich dětí v sociálních sítích a diskusních skupinách. Pokud dojde k detekci slov, frází i v t, která mohou poukazovat na potenciální ohrožení Vašich dětí, budete o této skutečnosti uvdomněni zasláním SMS zprávy nebo e-mailu. Pro každé ze svých dětí navíc můžete nastavit příslušnou úroveň zabezpečení a sledovat jejich činnost prostřednictvím samostatných út.
- **PC Tuneup** je pokročilým nástrojem pro detailní systémovou analýzu a optimalizaci, umožní zrychlit a vylepšit výkon vašeho počítače.
- **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.

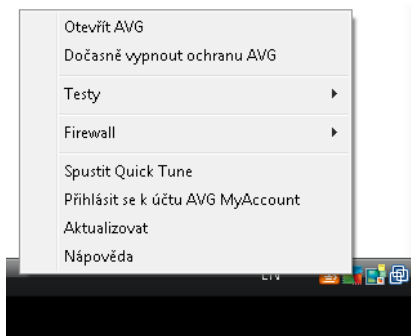
5.5. Zkratková tlačítka pro testování a aktualizaci

Zkratková tlačítka pro testování a aktualizaci najdete ve spodním pásu [hlavního dialogu AVG Internet Security 2014](#). Tato tlačítka umožní 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 i složek](#). (Podrobné informace o testování najdete v kapitole [AVG Testování](#))
- **Aktualizovat** - Stiskem tlačítka se automaticky spustí aktualizace produktu, o jejímž výsledku budete vyrozuměni v dialogu nad ikonou AVG na systémové liště. (Podrobné informace o procesu aktualizace najdete v kapitole [Aktualizace AVG](#))

5.6. Ikona na systémové liště

Ikona AVG na systémové liště (zobrazena na panelu Windows vpravo dole na monitoru) ukazuje aktuální stav **AVG Internet Security 2014**. Ikona je viditelná v každém okamžiku vaší práce na počítači, bez ohledu na to, zda máte i nemáte otevřenou [uživatelské rozhraní aplikace](#):



Zobrazení systémové ikony AVG

Ikona může být zobrazena v několika variantách:

- Jestliže je ikona zobrazena barevně bez dalších prvků, jsou všechny komponenty **AVG Internet Security 2014** 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 v domě fakturu, že se ta která [komponenta nachází v chybovém stavu](#), ale z nějakého důvodu si přejete tento stav zachovat a nebýt na něj upozorováni.)
- Pokud je ikona zobrazena s výkřikem, znamená to, že některá komponenta (i více komponent) je v [chybovém stavu](#). Vůjte tomuto hlášení pozornost a pokuste se odstranit problém v konfiguraci komponenty, která není správně nastavena. Abyste mohli provést úpravy v nastavení komponenty, otevřete [hlavní dialog aplikace](#) dvojklikem na ikonu na systémové liště. Podrobnější informace o tom, která komponenta je v [chybovém stavu](#), pak najdete v sekci [informace o stavu zabezpečení](#).
- Ikona na systémové liště může být také zobrazena barevně s probleskujícím otáčejícím se paprskem. Toto grafické znázornění signalizuje právě probíhající aktualizaci **AVG Internet Security 2014**.
- Alternativní zobrazení ikony s šipkou znamená, že právě žijete který z testů **AVG Internet Security 2014**.

Informace systémové ikony AVG

Ikona AVG na systémové liště dále poskytuje informace o aktuálním dění v programu **AVG Internet Security 2014**. Při změně stavu **AVG Internet Security 2014** (automatické spuštění naplánované aktualizace nebo testu, vypnutí profilu Firewallu, změna stavu některé komponenty, přechod programu do chybového stavu, ...) budete okamžitě informováni prostřednictvím vysunovacího okna zobrazeného nad ikonou na systémové liště.

Akce dostupné ze systémové ikony AVG

Ikona AVG na systémové liště lze také použít pro rychlý přístup k [hlavnímu dialogu](#) **AVG Internet Security 2014**, to se otevře dvojklikem na ikonu. Kliknutí pravým tlačítkem myši nad ikonou otevírá kontextové menu s těmito možnostmi:

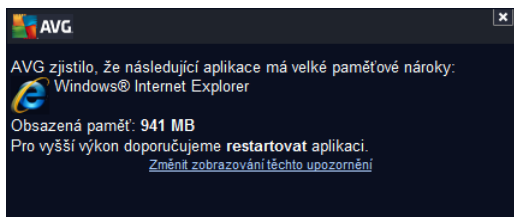


- **Otevít AVG** - Otevře [hlavní dialog AVG Internet Security 2014](#).
- **Do asn vypnout ochranu AVG** - Položka umožní jednorázově deaktivovat celou ochranu zajištěnou programem **AVG Internet Security 2014**. Můžete prosím na paměti, že tato volba by v žádném případě neměla být použita, pokud to není opravdu nezbytně nutné! V naprosté většině případů není nutné deaktivovat **AVG Internet Security 2014** před instalací nového software nebo ovladače, a to ani tehdy, pokud budete během instalace vyzváni k zavěšení všech spuštěných aplikací. Jestliže budete opravdu nuceni deaktivovat **AVG Internet Security 2014**, 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 a složek](#)) a následnou volbou požadovaný test můžete spustit.
- **Firewall** - Otevře vysunovací nabídku s možností rychlého přístupu k [dostupným režimům Firewallu](#). Volbou z nabídky okamžitě přepnete komponentu Firewall do zvoleného režimu.
- **Běžící testy ...** - Tato položka se zobrazuje pouze tehdy, je-li aktuálně spuštěn nějaký test. U tohoto běžícího testu můžete nastavit jeho prioritu, případně test pozastavit nebo ukončit. K dispozici jsou dále možnosti *Nastavit prioritu pro všechny testy*, *Pozastavit všechny testy* a *Zastavit všechny testy*.
- **Spustit Quick Tune** - Spustí funkci komponenty [Quick Tune](#).
- **Přihlásit se k účtu AVG MyAccount** - Otevírá domovskou stránku Můj účet, kde můžete spravovat předplacené produkty, obnovit platnost AVG licence, zakoupit doplňující produkty, stáhnout instalační soubory, zkontrolovat uskutečněné objednávky a vystavené faktury či spravovat osobní údaje.
- **Aktualizovat** - Spustí okamžitou [aktualizaci AVG Internet Security 2014](#).
- **Nápověda** - Otevře soubor nápovědy na úvodní stránce.

5.7. AVG Advisor

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

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



AVG Advisor monitoruje tyto konkrétní situace:



- **Stav aktuální otevřeného webového prohlížeče.** U webového prohlížeče můžete poměrně snadno dojít k přetížení paměti, zejména pokud máte po delší dobu současně otevřeno prohlížení na několika záložkách. Tím se výrazně zvyšuje spotřeba systémových zdrojů a dochází ke zpomalení vašeho počítače. Řešením je v takové situaci restart webového prohlížeče.
- **Spuštění Peer-To-Peer spojení.** Při použití P2P protokolu pro sdílení souborů jednotlivá spojení spotřebují značný objem přenosového pásma. Můžete 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 rozličným sítím. Narazíte-li na neznámou síť s obvyklým a zdánlivě známým jménem (*například Doma nebo MojeWifi*), můžete dojít k omylu a náhodně se tak připojíte k neprovozené a potenciálně nebezpečné síti. **AVG Advisor** dokáže této situaci předejít a vás varovat, že se ve skutečnosti jedná o novou, neznámou síť. Pokud se rozhodnete považovat tuto síť za bezpečnou, můžete ji uložit do seznamu známých sítí a při příchodu připojení k této síti se již notifikace **AVG Advisoru** nezobrazí.

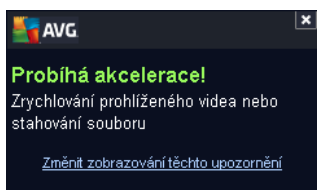
V každé z těchto situací Vás **AVG Advisor** varuje před možným konfliktem a zobrazí jméno a ikonu problematického procesu či aplikace. Dále pak navrhuje jednoduché řešení, kterým lze problém předejít.

Podporované webové prohlížeče

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

5.8. 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:



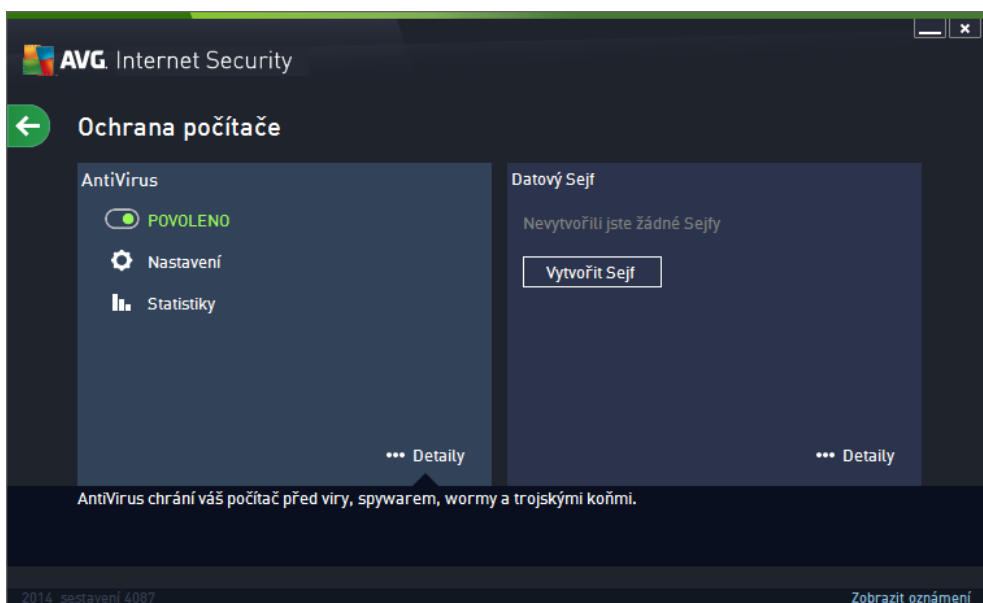


6. Komponenty AVG

6.1. Ochrana počítače

Komponenta **Ochrana počítače** zahrnuje dvě bezpečnostní služby: **AntiVirus** a **Datový sejf**.

- **AntiVirus** je tvořen jádrem, které testuje všechny soubory a jejich aktivitu, systémové oblasti počítače i vyměnitelná média (*flash disky apod.*) a provádí 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 nezaznamenate - 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 2014** umí také analyzovat spustitelné programy, případně DLL knihovny a určité, které z nich by mohly být potenciálně nežádoucí (*jako například spyware, adware aj.*). Na žádost uživatele umožní tyto programy odstranit i k nim zablokovat přístup.
- **Datový sejf** je službou, s jejíž pomocí můžete vytvořit bezpečné virtuální úložiště pro svá cenná a citlivá data. Obsah Datového Sejfu je zašifrován a chráněn heslem, které si sami nastavíte, a vaše data jsou tedy zajištěna před neautorizovaným přístupem.



Společné ovládací prvky dialogu


Mezi oběma sekcemi v dialogu přecházíte pouhým kliknutím na panel příslušné té které služby; po kliknutí se panel vysvětlí světlejším odstínem modré. V obou sekcích dialogu se můžete setkat s několika ovládacími prvky. Jejich funkčnost je stejná, a přísluší jedné i druhé bezpečnostní službě (*AntiVirus* i *File Vaults*):





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 služba vypnuta. Pokud nemáte skutečný důvod službu vypínat, doporučíme, 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 2014**. Přes něj lze provést veškerou konfiguraci zvolené služby, v tomto případě služby [AntiVirus](#). V pokročilém nastavení můžete editovat veškeré parametry jednotlivých bezpečnostních služeb **AVG Internet Security 2014**, ale jakoukoliv konfiguraci doporučíme pouze znalým uživatelům!

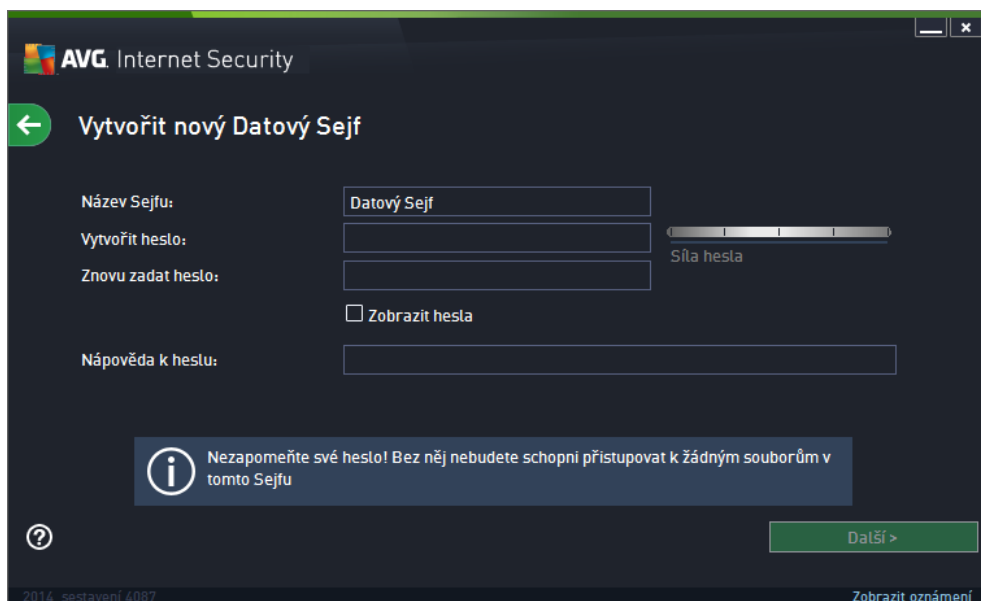
 **Statistiky** - Kliknutím na tlačítko budete přesměrováni na speciální dedikovanou stránku na webu AVG (<http://www.avg.com/cz-cs/homepage>). Na této stránce najdete detailní statistický přehled všech aktivit **AVG Internet Security 2014**, které proběhly na vašem počítači za určený časový úsek i celkově 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.

Vytvoření nového Datového Sejfu

V sekci **Datový sejf** je dostupné tlačítko **Vytvořit Sejf**. Stiskem tlačítka otevře nový dialog, v němž můžete nastavit parametry svého zamýšleného sejfu:

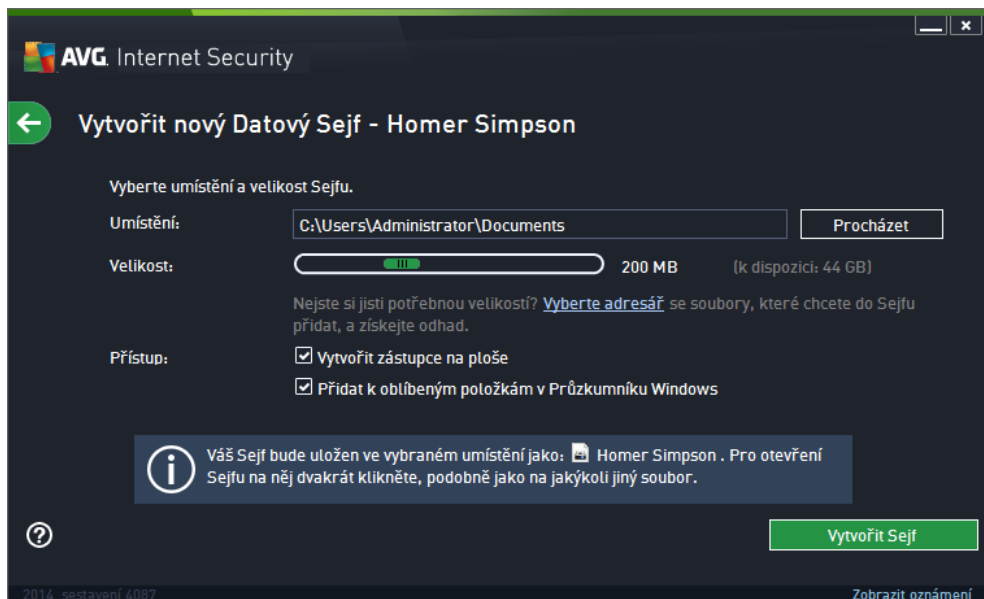


Nejprve prosím zvolte název svého sejfu a vyberte silné heslo:



- **Název Sejfu** - Chcete-li vytvořit nový sejf, nejprve pro něj musíte zvolit vhodné jméno. Pokud svůj název sdělíte s někým dalším, třeba se členy vaší rodiny, je vhodné v názvu uvést své jméno a/nebo indikaci zamýšleného obsahu sejfu, například *Honzovy e-maily*.
- **Vytvořit heslo / Znovu zadat heslo** - Vytvořte heslo pro ochranu svého sejfu a zadejte je do příslušného pole (*dvakrát, pro potvrzení*). Grafický indikátor umístěný vpravo od textového pole pro zadání hesla vám ukáže, nakolik je vaše heslo silné či slabé (*tedy relativně snadno prolomitelné za pomoci speciálních softwarových nástrojů*). Doporučujeme vám, abyste si nastavili heslo, které dosáhne alespoň střední úrovně. Heslo bude silnější, pokud v něm budou zahrnuta velká i malá písmena, číslice, speciální znaky, pomlčky a podobné znaky. Abyste si byli jisti, že jste své heslo skutečně napsali správně, můžete volbou položky **Zobrazit hesla** odkrýt text v obou textových polích (*samozejmě za předpokladu, že se vám nikdo nedívá přes rameno*).
- **Nápověda k heslu** - Dle našich doporučení můžete využít také možnosti uložit si nápovědu k heslu. Pamatujte, že **Datový sejf** je navržen s ohledem na naprostou ochranu soukromí vašich dat, k nimž lze přistoupit výhradně s použitím hesla. Pokud heslo zapomenete, ke svým datům už se nedostanete!

Jestliže jste uvedli všechny požadované informace, klikněte na tlačítko **Další** a přejděte k následujícímu kroku:



Dialog nabízí tyto možnosti konfigurace:

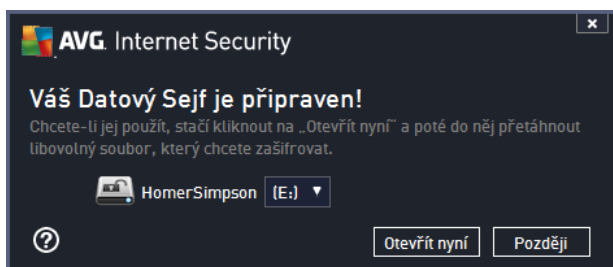
- **Umístění** - Určuje, kde bude váš datový sejf fyzicky umístěn. Pomocí tlačítka **Procházet** najdete vhodnou lokaci na svém pevném disku anebo můžete ponechat výchozí nastavení, tedy adresu *Dokumenty*. Prosím, myslíte na to, že jakmile jednu datový sejf vytvoříte, nebudete již jeho umístění moci změnit.
- **Velikost** - Můžete nastavit požadovanou velikost datového sejfu a alokovat tak potřebné místo na disku. Nastavená hodnota by měla být dobře zvážena - příliš nízká hodnota vytvoří prostor, který nebude stačit vašim potřebám, příliš vysoká hodnota zabere spoustu místa zbytečně. Pokud již máte představu o tom, která data chcete do sejfu umístit, můžete všechny dotčené soubory shromáždit v jednom adresáři a pak za pomoci odkazu **Vyberte adresář** automaticky spočítat potřebnou velikost sejfu. V každém případě, velikost sejfu lze později kdykoliv změnit.



- **Přístup** - Zaškrťovací políčka v této sekci vám umožní vytvořit si pohodlně dostupné zástupce pro přístup k vašemu datovému sejfů.

Použití vašeho Datového Sejfu

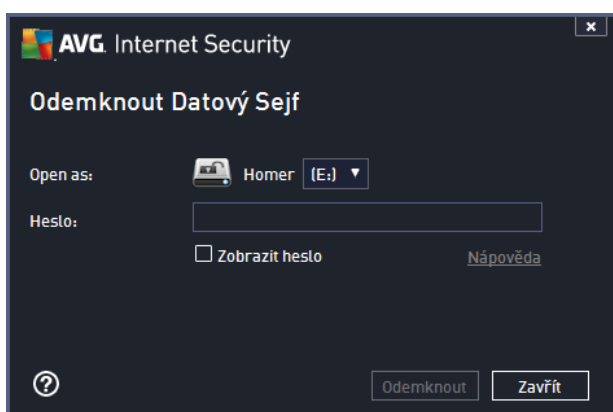
Jakmile máte nastaveny všechny potřebné údaje, stisknete tlačítko **Vytvořit sejf**. Objeví se nový dialog **Váš Datový sejf je připraven!** a můžete jej začít využívat pro ukládání vašich cenných dat. Bezprostředně po vytvoření je sejf odemčen a stačí jej otevřít. Při každém následujícím pokusu o otevření sejfu však již budete vyzváni k odemčení sejfu pomocí hesla, které jste si zvolili:



Abyste mohli datový sejf začít používat, je potřeba jej otevřít stiskem tlačítka **Otevřít nyní**. Po otevření se datový sejf zobrazí ve vašem počítači jako nový virtuální disk. Při aktivaci mu označení písmenem podle vlastního výběru volbou z rozbalovacího menu (*v nabídce se zobrazí jen aktuálně neobsazené disky*). Při standardním nastavení nebudete moci zvolit označení písmenem C (*to je určeno k označení pevného disku*), A (*disketa*) ani D (*DVD mechanika*). Pro každý nově založený datový sejf můžete z nabídky zvolit jiné písmeno pro označení virtuálního disku.

Odemčení vašeho Datového Sejfu

Při dalším pokusu o otevření sejfu budete vyzváni k odemčení sejfu pomocí hesla, které jste si zvolili:

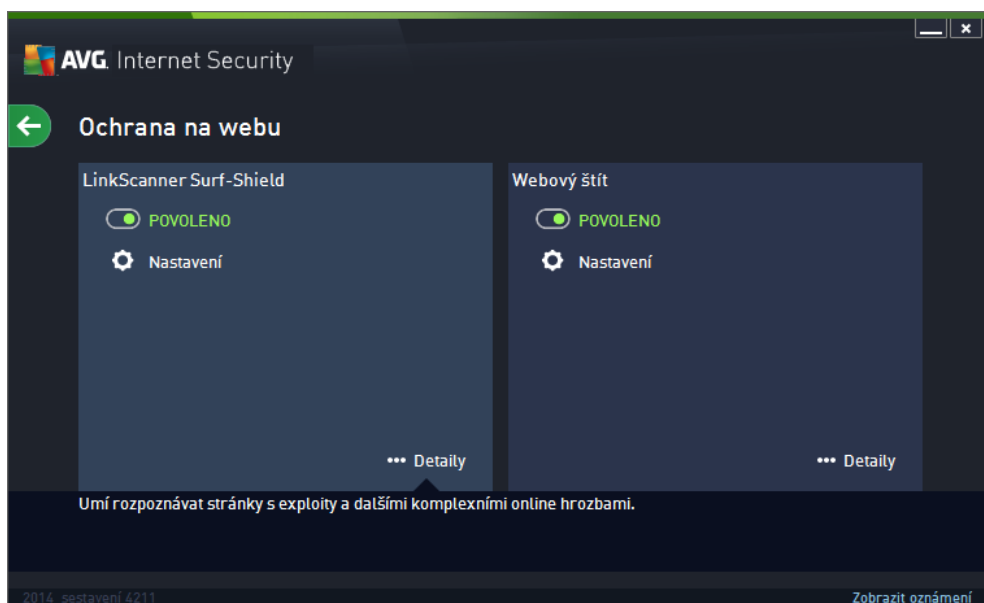


Do textového pole napište heslo, které jste si vytvořili a kliknete na tlačítko **Odemknout**. Pokud si na heslo nemůžete vzpomenout, můžete použít svou vlastní nápovědu, kterou jste definovali při vytváření datového sejfu - kliknutím na odkaz **Nápověda**. Datový sejf se poté objeví v přehledu vašich datových sejfů jako **ODEMČENÝ** a můžete do něj vkládat soubory nebo je z něj vybírat podle potřeby.

6.2. Ochrana na webu


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

- **LinkScanner Surf-Shield** zajišťuje ochranu před stále rostoucími počtem nebezpečných 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 nejdelší, tedy když se chystáte otevřít adresu URL. LinkScanner 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 nebezpečnou stránku, LinkScanner Surf-Shield před vstupem 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 zabráni jeho stažení. **Webový štít není určen k ochraně serverů!**




Ovládací prvky dialogu


Mezi oběma sekcemi v dialogu přecházíte pouhým kliknutím na panel příslušné té které služby; po kliknutí se panel vysvětlí světlejším odstínem modré. V obou sekcích dialogu se můžete setkat s několika ovládacími prvky. Jejich funkce je stejná, a patří k jedné i druhé bezpečnostní službě (*LinkScanner Surf-Shield* i *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 služba 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 2014**. Přes něj můžete nastavení do dialogu, v němž lze provést veškerou konfiguraci zvolené služby, v tomto případě služby [LinkScanner Surf-Shield](#) nebo [Webový štít](#). V pokročilém nastavení můžete editovat veškeré parametry jednotlivých bezpečnostních služeb **AVG Internet Security 2014**, ale jakoukoliv konfiguraci doporučujeme pouze znalým uživatelům!

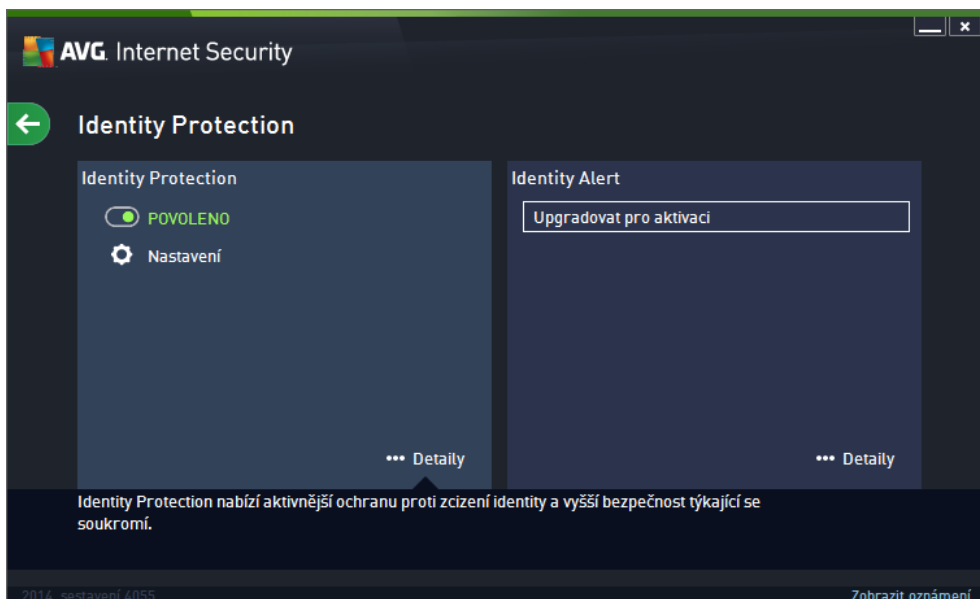
 **Detaily** - Kliknutím na tlačítko se ve spodní části dialogu zobrazí stručný popis služby, jež je aktuálně zvolena.

 - Pomocí šipky v levé horní části dialogu se vrátíte zpět do [základního uživatelského rozhraní](#) s přehledem komponent.

6.3. Identity Protection


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


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





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 služba vypnuta. Pokud nemáte skutečnou 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 2014**. Přes něj můžete nastavení do dialogu, v němž lze provést veškerou konfiguraci zvolené služby, v tomto případě služby [Identity Protection](#). V pokročilém nastavení můžete editovat veškeré parametry jednotlivých bezpečnostních služeb **AVG Internet Security 2014**, 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. Ochrana e-mailu

Komponenta **Ochrana e-mailu** 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 v tším zdrojem nebezpečí. Toto nebezpečí narůstá obzvláště u zdarma dostupných poštovních úst (protože u těchto je použití anti-spamové technologie spíše výjimkou), které stále používá většina domácích uživatelů. Tito uživatelé také často navštěvují neznámé webové stránky a nevědomky zadávají svá osobní data (nejčastěji svou e-mailovou adresu) do různých formulářů na webu, čímž ještě zvyšují riziko napadení prostřednictvím elektronické pošty. V tší společnosti v tšinou používají firemní poštovní úst a snaží se riziko minimalizovat implementací anti-spamových filtrů. Služba Kontrola pošty zodpovídá za testování veškeré přichází 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 určená k ochraně poštovních serverů!**

- **Anti-Spam** kontroluje veškerou přichází 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 zahrnuje jejich poštovní schránky. Termín spam se nevztahuje na oprávněnou e-mail komerčního charakteru, k jehož přijetí dává zákazník svůj souhlas.). Anti-Spam dokáže upravit předem e-mailu, který je identifikován jako spam, přidáním vámi definovaného textového štítku. Poté již můžete snadno filtrovat e-maily podle definovaného označení ve vašem poštovním klientovi. K detekci spamu v jednotlivých zprávách používá Anti-Spam několik analytických metod a zaručuje tedy maximální úroveň ochrany proti nevyžádané poště. Anti-Spam pracuje s pravidelně aktualizovanou databází a lze nastavit i kontrolu pomocí [RBL serveru](#) (ve svých seznamech "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 příslušné té které služby; po kliknutí se panel vysvětlí světlejším odstínem modré. V obou sekcích dialogu se můžete setkat s několika ovládacími prvky. Jejich funkce je stejná, a přísluší jedné i druhé bezpečenostní službě (*Kontrola pošty* i *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 "semafore". Jejich pomocí můžete samostatně určit, zda si přejete, aby se testovaly příchozí, odchozí, nebo obojí. Ve výchozím nastavení je služba zapnuta pro testování příchozí pošty, ale pro odchozí poštu vypnuta - u odchozích zpráv je riziko zavezení infekce minimální.

 **Nastavení** - Kliknutím na tlačítko přejdete do rozhraní pro [pokročilé nastavení](#) programu **AVG Internet Security 2014**. Přes něj můžete, budete nasměrováni do dialogu, v němž lze provést veškerou konfiguraci zvolené služby, v tomto případě služby [Kontrola pošty](#) nebo [Anti-Spam](#). V pokročilém nastavení můžete editovat veškeré parametry jednotlivých bezpečnostních služeb **AVG Internet Security 2014**, ale jakoukoliv konfiguraci doporučujeme pouze znalým uživatelům!

 **Statistiky** - Kliknutím na tlačítko budete přesměrováni na speciální dedikovanou stránku na webu AVG (<http://www.avg.com/cz-cs/homepage>). Na této stránce najdete detailní statistický přehled všech aktivit **AVG Internet Security 2014**, 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

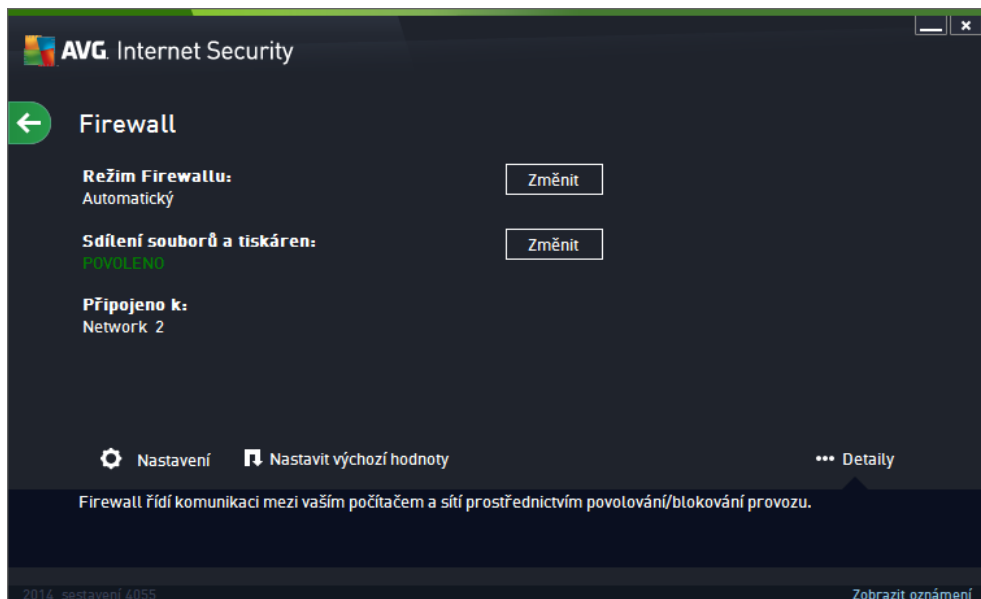
Firewall lze obecně definovat jako systém, který pomocí blokování/povolování přístupu řídí provoz mezi dvěma nebo více sítěmi. Firewall obsahuje pravidla, jež chrání vnitřní síť před útokem zvenčí (*nejde o internet*) a řídí veškerou komunikaci probíhající na jednotlivých síťových portech. Tu vyhodnocuje podle pravidel, jež má nastaveny, a rozhoduje, zda je komunikace vyhovující či nevhovující. Pokud narazí na pokusy o proniknutí, zabrání jejich pokračování. Firewall je nastaven tak, aby povolil nebo zablokoval interní i externí komunikaci (*obě směry, dovnitř nebo ven*) na předem definovaných portech a pro vybrané softwarové aplikace. Například můžete Firewall nastavit tak, aby propouštěla data stahovaná z Internetu pouze za použití prohlížeče MS Internet Explorer. Jakýkoliv jiný pokus o stažení dat pomocí jiného prohlížeče bude zablokován. Firewall vám pomůže udržet si své soukromí a zaručí, že vaše osobní informace nebudou, byť náhodně, odeslány z vašeho počítače bez vašeho svolení. Firewall přiblíženě 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 2014** 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.



Poznámka: Při instalaci AVG Internet Security 2014 může komponenta Firewall vyžadovat restart počítače. V takovém případě se dialog komponenty zobrazí s informací o nutnosti restartu. Přímo v dialogu je pak k dispozici tlačítko **Restartovat ihned**, kterým restart PC spustíte. Dokud restart neproběhne, Firewall není plně aktivní. Rovněž všechny možnosti editace v tomto dialogu budou vypnuty. Vždy prosím pozornost tomuto upozornění a proveďte restart počítače.

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 případem definovaných konfigurací.

- **Automatický režim** - V tomto režimu rozhoduje Firewall o veškerém provozu automaticky. Váš zásah nebude vyžadován za žádných okolností. Přiipojení 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 přiipojení na základě chování této aplikace, ale pravidlo vytvořeno nebude, aby ke kontrole této aplikace došlo opakovaně při jejím připojení. Firewall se v automatickém režimu chová zcela nenápadně. Volbu automatického režimu doporučujeme v tšin uživatel.
- **Interaktivní režim** - Pro interaktivní režim se rozhodnete v případě, že chcete mít plnou kontrolu nad veškerou sítíovou komunikací vašeho počítače. Firewall bude provoz monitorovat a oznámí vám každý pokus o komunikaci nebo přenos dat, při němž budete mít možnost sami rozhodnout, zda má být tato komunikace povolena nebo zablokována. Volbu interaktivního režimu doporučujeme pouze zkušeným



a znalým uživateli!

- **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 (nedoporučeno)** - Vypnutí Firewallu umožní přiblížit 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 omezení 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 režimů 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, i 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 (*těba na letišti nebo v internetové kavárně*), sdílení rozhodně nedoporučujeme.
- **Připojeno k** - Uvádí název sítě, k níž je uživatel aktuálně připojen. U operačního systému Windows XP jsou sítě uvedeny pod názvem, který si zvolil uživatel v době prvního připojení k síti. U operačních systémů 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 příslušné 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.

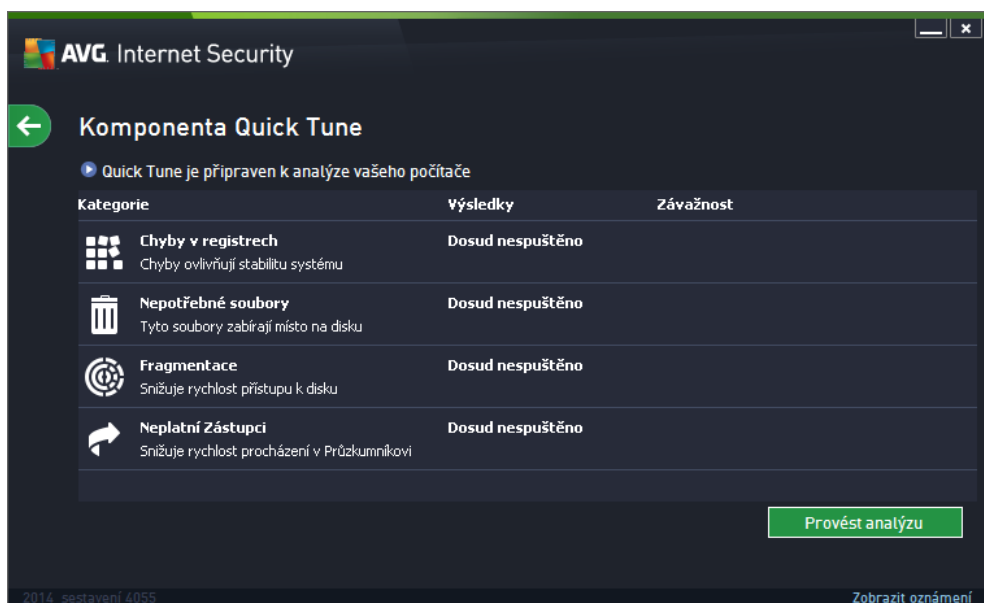
 **Detaily** - Kliknutím na tlačítko se ve spodní části dialogu zobrazí stručný popis služby, jež je aktuálně zvolena.



← - Pomocí šipky v levé horní části dialogu se vrátíte zpět do [základního uživatelského rozhraní](#) s pohledem komponent.

6.6. Komponenta Quick Tune

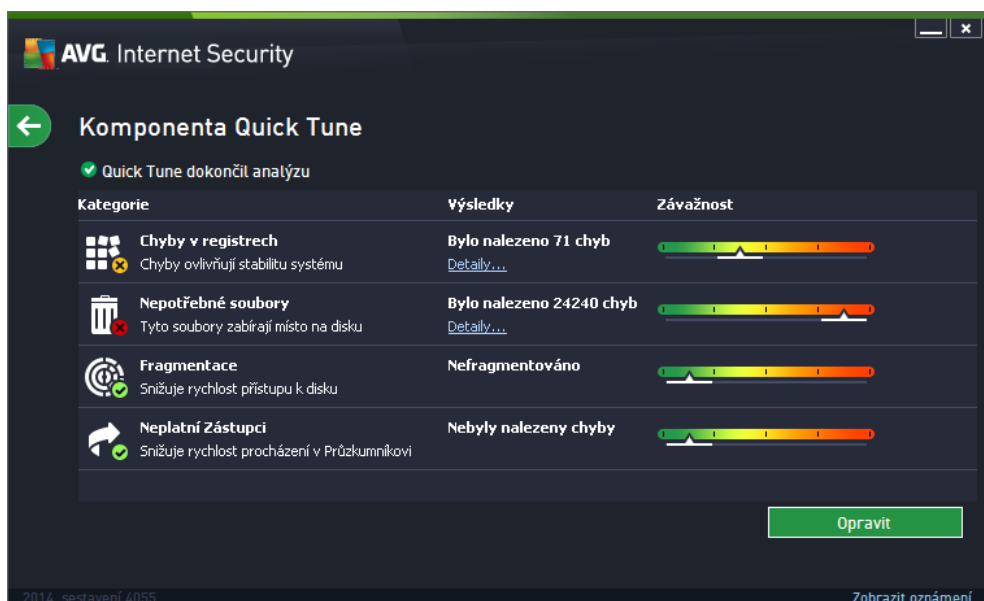
Komponenta Quick Tune je nástrojem pro detailní systémovou analýzu a optimalizaci umožňující zrychlit a vylepšit výkon vašeho počítače. Otevírá se z [hlavního uživatelského rozhraní](#) volbou položky **Zlepšit výkon**:



Analyzovat a opravit lze následující:

- **Chyby v registrech** - případné chyby v registru Windows, které mohou zpomalovat váš počítač a zobrazovat chybové hlášky.
- **Nepotřebné soubory** - počet souborů, bez kterých se pravděpodobně bez potíží obejdete a zabírají tedy v počítači zbytečné místo. Typicky jde o různé typy dočasných souborů a o smazané soubory, tj. obsah koše.
- **Fragmentace** - spočítá, jaká procentuální část vašeho pevného disku je fragmentována. Fragmentací pevného disku rozumíme skutečnost, že pevný disk se již dlouho používán a jednotlivé na něm uložené soubory jsou tedy fyzicky roztroušeny na různých částech disku.
- **Neplatní Zástupci** - upozorní na odkazy a zástupce aplikací, které již nefungují, odkazují na neexistující soubory a složky apod.

Samotnou analýzu spustíte stiskem tlačítka **Provést analýzu**. Při běhu 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 rozdelených podle jednotlivých kategorií. Výsledek analýzy bude také zobrazen graficky na ose ve sloupci **Závažnost**.

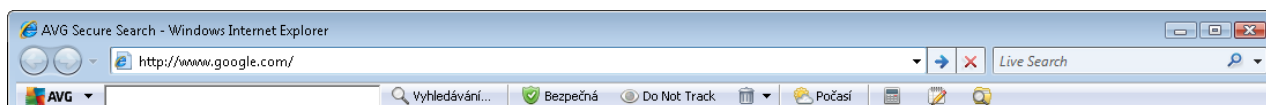
Ovládací tlačítka dialogu

- **Provést analýzu** (tlačítko se zobrazí před zahájením analýzy) - stiskem tlačítka spustíte okamžitou analýzu počítače
- **Opravit** (tlačítko se zobrazí po dokončení analýzy) - zahájí opravu nalezených chyb. Výsledek bude přehledně zobrazen ihned po ukončení oprav
- **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 2014** instaluje volitelně; možnost rozhodnout se, zda tuto komponentu chcete instalovat, jste mohli vidět při instalaci tohoto produktu. **AVG Security Toolbar** je dostupný v podobě nástrojové lišty ve vašem internetovém prohlížeči. Podporovanými prohlížeči jsou Internet Explorer (ve verzi 6.0 a vyšší) a/nebo Mozilla Firefox (ve verzi 3.0 a vyšší). Jiné prohlížeče nejsou podporovány (pokud používáte alternativní prohlížeč, například Avant browser, můžete se setkat s nekorektním chováním).



AVG Security Toolbar je tvořen těmito prvky:

- **Logo AVG** s rozbalovací nabídkou:
 - **Aktuální míra ohrožení** - Otevře webovou laboratoř s grafickým znázorněním aktuální úrovně bezpečnosti na Internetu.
 - **AVG Threat Labs** - Otevře stránku **AVG Threat Lab** (<http://www.avgthreatlabs.com>), kde najdete informace o bezpečnosti jednotlivých webových stránek a aktuální úrovni online ohrožení.
 - **Nápověda k liště** - Otevírá online nápovědu k jednotlivým funkcím **AVG Security Toolbar**.
 - **Odeslat zpětnou vazbu o produktu** - Otevře stránku s online formulářem, jehož prostřednictvím nám můžete zaslat svůj názor na **AVG Security Toolbar**.
 - **Licenční ujednání s koncovým uživatelem** - Otevírá stránku na webu AVG s plným zněním licenční smlouvy vázané k užívání **AVG Internet Security 2014**.
 - **Zásady ochrany osobních údajů** - Otevírá webovou stránku AVG, která Vás v plném rozsahu seznámí se zásadami ochrany osobních údajů společnosti AVG Technologies.
 - **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 nacházíte (**Bezpečná**). Tento pohled pak můžete otevřít přímo v okně prohlížeče se všemi detaily o bezpečnostních aktivitách vztažených k právě prohlížené stránce (**Kompletní zpráva o stránce**):



AVG Site Safety

Bezpečná Kompletní zpráva o stránce
 Nejnovější aktualizace: 17.7.2013

Adresa URL stránky http://www.google.cz/?gws_rd=cr
 Název stránky Google

Bezpečná
 Na této stránce se nenachází žádné aktivní hrozby. Můžete ji s klidem otevřít.

Riziková
 Pozor – tato stránka může obsahovat hrozby. Doporučujeme ji neotevřít.

Nebezpečná
 Tato stránka obsahuje aktivní hrozby. Doporučujeme ji neotevřít.

30denní aktivita hrozeb pro <http://www.google.cz>...

Internetová stránka	google.cz
Poslední aktualizace ...	Jul 17, 2013
IP adresa	173.194.40.55
Rychlost	Fast
Velikost	56.15 KB
Soubory cookie	Yes
Oblíbenost stránky	Top Site
Umístění serveru	US
Zabezpečení SSL	Disabled

Podobné internetové ...

- <http://seznam.cz/>
- <http://centrum.cz/>
- <http://www.atlas.cz/>
- <http://zive.cz/>

- **Do Not Track** - Služba DNT dokáže identifikovat webové stránky, které sbírají data o vaší inności online a nabídne vám možnost sbírat data 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 formuláře nebo vymazat kompletně celou historii vašeho vyhledávání na webu.
- **Počasí** - Tlačítkem otevřete samostatné okno s informací o aktuálním počasí v dané lokalitě a s výhledem na následující dva dny. Tato informace je aktualizována každých 3-6 hodin. V dialogu můžete změnit požadovanou lokalitu a také rozhodnout, zda si přejete uvádět teplotu ve stupních Celsia nebo Fahrenheita.



The Weather Channel
 weather.com

Brno, Czech Republic
 Updated: 7/17/13 10:30 AM Local Time [change location]

24°C
 Sunrise: 05:07 dop.
 Sunset: 08:52 odp.

Today Hi: 27°C Lo: 17°C	Thursday Hi: 28°C Lo: 18°C	Friday Hi: 28°C Lo: 16°C
-------------------------------	----------------------------------	--------------------------------

- **Facebook** - Tlačítko umožňuje přímé připojení k sociální síti [Facebook](#) z prostředí **AVG Security**



Toolbaru.

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




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 i 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 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 [tuto podmínku](#).
- **AVG Do Not Track** je ve výchozím nastavení zapnutý, ale lze jej libovolně deaktivovat. Instrukce k deaktivaci služby najdete v sekci FAQ na stránce [Jak vypnout funkci AVG Do Not Track](#).
- Další podrobné informace o službě **AVG Do Not Track** najdete na našem [webu](#).

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 sběrů dat a o jejich případné detekci vás informuje zmnou 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 sbírají data jsou uvedeny v seznamu **Sledování na této stránce**. **AVG Do Not Track** rozlišuje tři typy sbírají data:

- **Služba Web Analytics** (ve výchozím nastavení povoleny): Služby poskytující lepší výkon a prohlížení p íslušných 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.
- **Reklamní síť** (některé reklamní sítě jsou ve výchozím nastavení blokovány): Služby, které přímo nebo 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 (základy ochrany osobních údajů jsou dostupné na webových stránkách dané sítě).
- **Tlačítka sociální sítě** (ve výchozím nastavení povoleny): Prvky sloužící k lepší práci se sociálními sítěmi. Tato tlačítka propojují navštívené stránky se sociálními sítěmi. Jste-li k této síti přihlášení, mohou tato tlačítka sbírat informace o vaší činnosti na Internetu. Mezi tlačítka sociálních sítí patří: plug-in síť Facebook, tlačítko síť Twitter, tlačítko Google +1 apod.

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

Ovládací prvky dialogu

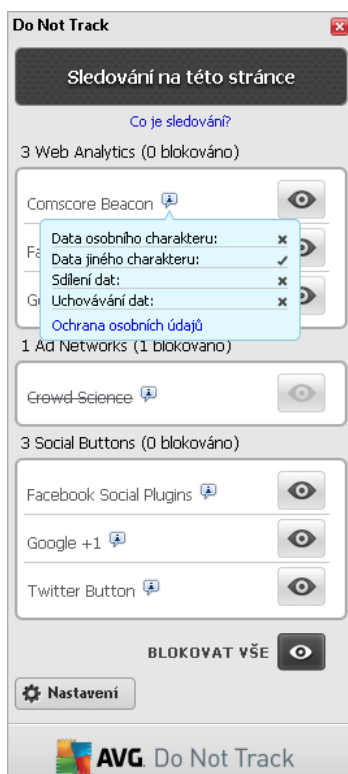
- **Co je sledování?** - Kliknutím na tento odkaz v horní části dialogu budete přesměrováni na webovou stránku s podrobným vysvětlením principu sledování a popisem jednotlivých typů sledování.



- **Blokovat vše** - Stiskem tohoto tlačítka, které je umístěno ve spodní části dialogu, zakážete veškerý sběr dat všem detekovaným službám (*podrobnosti najdete v kapitole [Blokování sledovacích procesů](#)*).
- **Nastavení** - Kliknutím na toto tlačítko 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 vidět více. Najdete myši 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 přesměrováni na stránku s prohlášením o ochraně osobních údajů na serveru poskytlé detekované služby.

8.3. Blokování sledovacích procesů

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

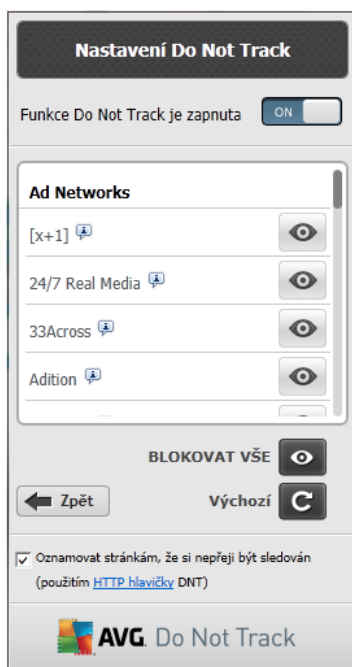
- **Blokovat vše** - Stiskem tohoto tlačítka, které je umístěno ve spodní části dialogu, zakážete jakýkoliv sběr dat všem detekovaným službám. (*Mjte však na paměti, že tento krok může způsobit poruchy funkčnosti webových stránek, v nichž služba běží!*)



-  - Pokud nechcete jednorázově zablokovat všechny detekované služby, dá se blokování i povolení nastavit u každé z detekovaných služeb jednotlivě. Na kterém z detekovaných služeb sledování povolíte (například Web Analytics): tyto systémy používají shromažďovaná data k optimalizaci své webové stránky a zlepšují tak uživatelské prostředí internetu. Součástí 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 ji povolíte.

8.4. Nastavení služby AVG Do Not Track

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



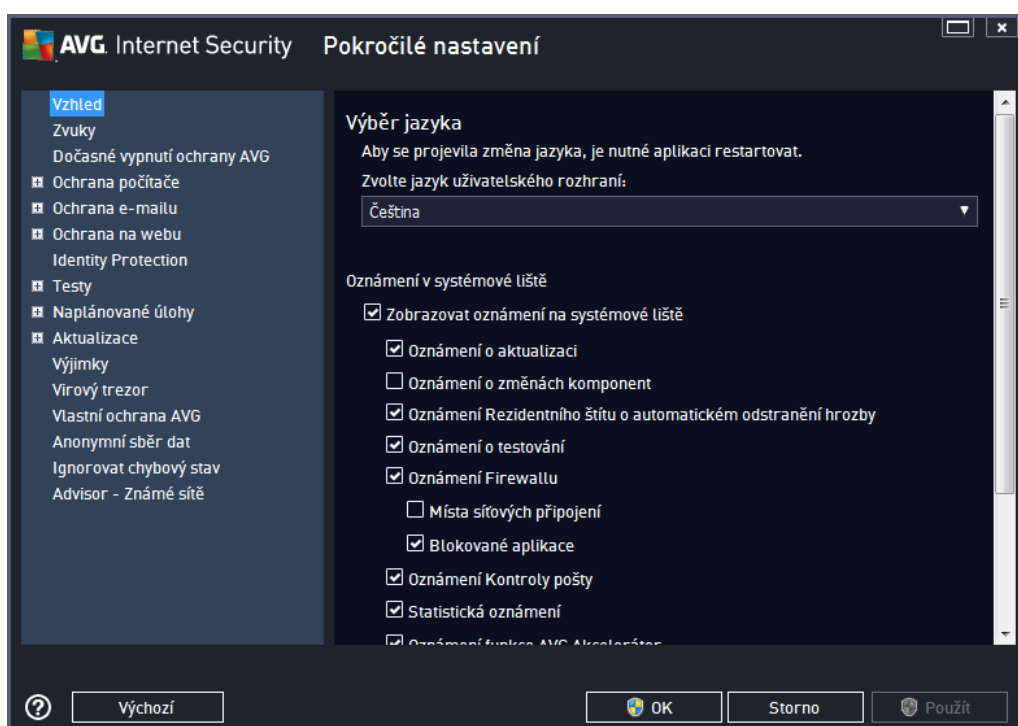
- **Funkce Do Not Track je zapnuta** - Ve výchozím nastavení je služba DNT aktivována (spínač v pozici ON). Funkci můžete vypnout přepnutím spínače do pozice OFF.
- V centrální sekci dialogu najdete seznam všech známých služeb sdružených do reklamních sítí, které lze klasifikovat jako reklamní síť. Ve výchozím nastavení **Do Not Track** blokuje některé z reklamních sítí automaticky, u jiných ponechává rozhodnutí na vaší volbu. Hromadně zablokovat všechny uvedené služby můžete kliknutím na tlačítko **Blokovat vše**. Stiskem tlačítka **Výchozí** zrušíte veškeré provedené úpravy nastavení a vrátíte se do původní konfigurace.
- **Oznamovat stránkám, že si nepřejí být sledován** - V této sekci máte možnost zapnout nebo vypnout volbu **Oznamovat stránkám, že si nepřejí být sledován** (ve výchozím nastavení zapnuto). Ponecháte-li položku označenou, bude **Do Not Track** automaticky informovat provozovatele detekovaných služeb sdružených do reklamních sítí, že si nepřejete být sledováni.

9. Pokročilé nastavení AVG

Dialog pro pokročilou editaci nastavení programu **AVG Internet Security 2014** se otevírá v novém okně **Pokročilé nastavení AVG**. Toto okno je rozděleno do dvou částí: v levé části okna najdete přehlednou stromovou strukturu konfigurací programu. Volbou komponenty, jejíž parametry chcete editovat (připadnou volbou konkrétní části této komponenty) otevřete v pravé části okna příslušný editační dialog.

9.1. Vzhled

První položka navigačního seznamu, **Vzhled**, se týká obecného nastavení [hlavního dialogu](#) **AVG Internet Security 2014** a nabízí možnost nastavení základních prvků programu:



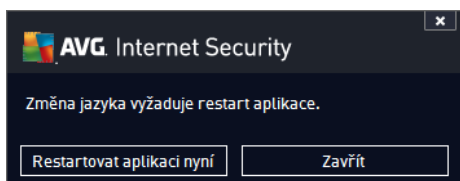
Výběr jazyka

V sekci **Výběr jazyka** můžete z rozbalovacího menu zvolit jazyk, v němž má být zobrazen [hlavní dialog](#) **AVG Internet Security 2014**. 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 2014** v požadovaném jazyce je však nutné aplikaci restartovat. Postupujte prosím následovně:

- V rozbalovacím menu zvolte požadovaný jazyk aplikace.
- Svou volbu potvrdíte stiskem tlačítka **Použít** (vpravo ve spodním rohu dialogu).
- Stiskem tlačítka **OK** znovu potvrdíte, že chcete změnu provést.
- Objeví se nový dialog s informací o tom, že pro dokončení změny aplikace je nutné **AVG Internet Security 2014** 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 2014**. Ve výchozím nastavení programu jsou systémová oznámení povolena. Doporučujeme toto nastavení ponechat! Systémová oznámení přináší například informace o spuštění aktualizace či testu, o změně stavu některých komponent **AVG Internet Security 2014** a podobně. Je rozhodně vhodné v novat jim pozornost!

Pokud se přesto z nějakého důvodu rozhodnete, že si nepřejete být takto informováni, máte možnost kompletně potlačit zobrazování informativních oznámení, nebo zakázat pouze zobrazování informací vztahených k určité komponentě **AVG Internet Security 2014**. 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 aktualizací; 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 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 i blokování provozu apod. Informace o ostatních procesech se budou zobrazovat normálně. Tato položka se dále dělí do dvou specifických možností (*podrobný popis obou najdete v kapitole [Firewall](#) této dokumentace*):

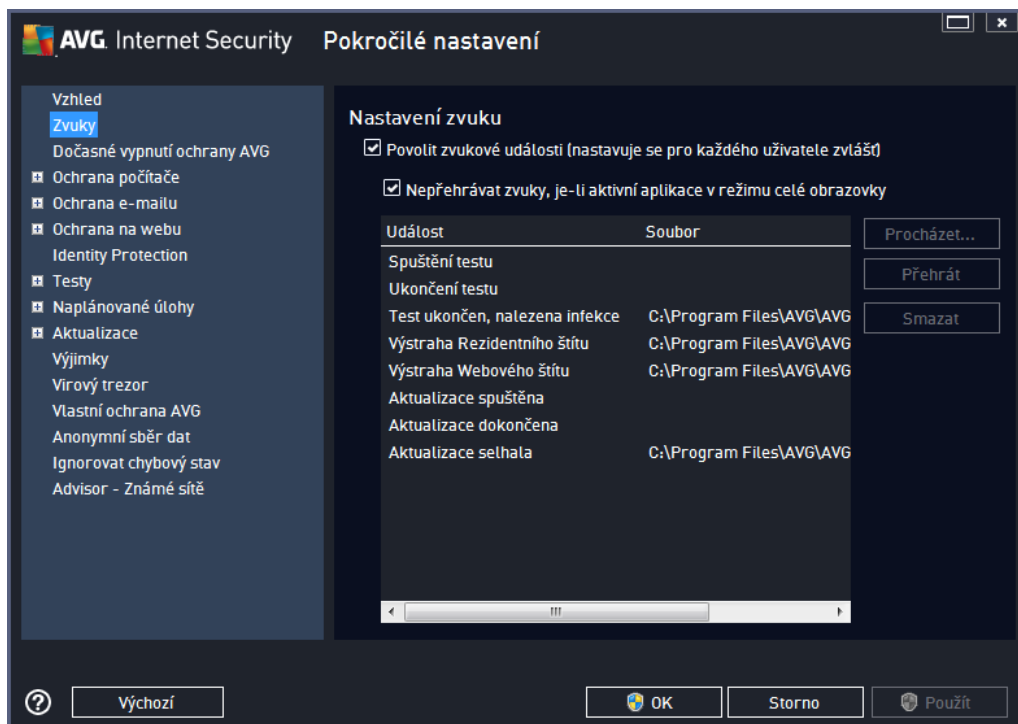
- **Místa síťových připojení** (ve výchozím nastavení vypnuto) - při připojení k síti budete informováni, zda Firewall tuto síť zná a jak bude nastaveno sdílení souborů a tiskáren.
- **Blokované aplikace** (ve výchozím nastavení zapnuto) - pokud se o připojení k síti pokouší neznámá či jakkoliv podezřelá aplikace, Firewall tento pokus zablokuje a vyrozumí vás o této skutečnosti oznámením na systémové liště. Doporučujeme ponechat tuto funkci vždy zapnutou!
- o **Oznámení [Kontroly pošty](#)** (ve výchozím nastavení zapnuto) - Volbou položky rozhodnete, zda mají být zobrazena nebo naopak potlačena informativní hlášení o příchozích a odchozích zprávách elektronické pošty; informace o ostatních procesech se budou zobrazovat normálně.
- o **Statistická oznámení** (ve výchozím nastavení zapnuto) - Volbou položky umožníte zobrazení pravidelného statistického přehledu v systémové liště.
- o **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.
- o **Oznámení komponenty AVG Advisor** (ve výchozím nastavení zapnuto) - Volbou položky rozhodnete, zda chcete ponechat zapnutá všechna oznámení služby [AVG Advisor](#) zobrazená ve vysouvacím panelu na systémové liště.

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).

9.2. Zvuky

V dialogu **Nastavení zvuku** můžete rozhodnout, zda chcete být o jednotlivých akcích **AVG Internet Security 2014** informováni zvukovým oznámením:



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

Ovládací tlačítka dialogu

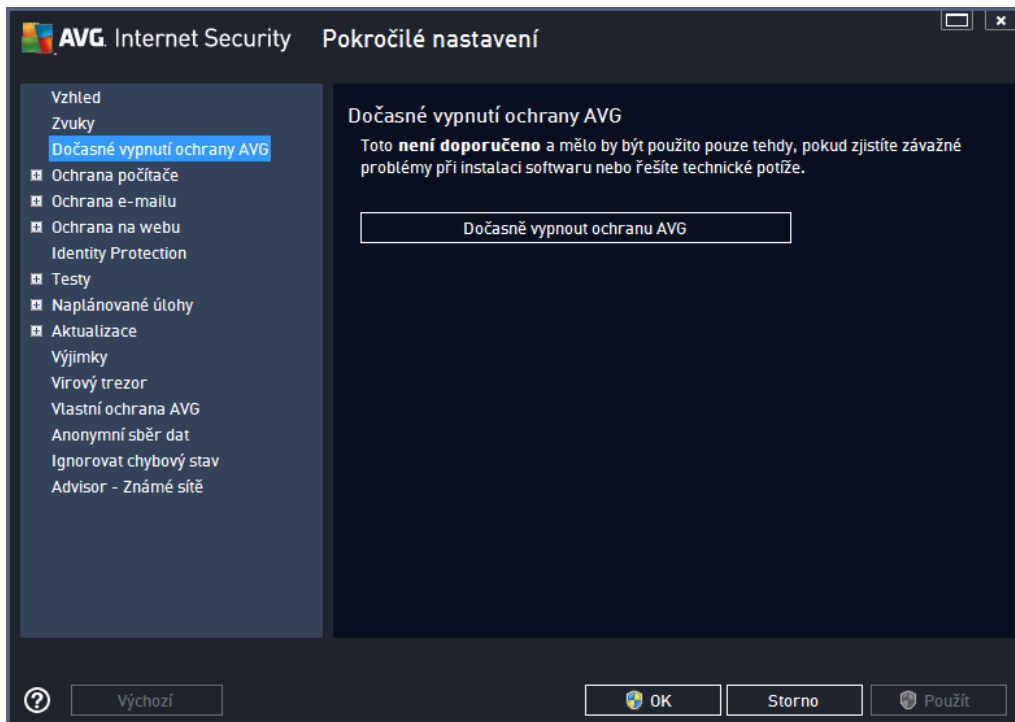
- **Procházet...** - Ze seznamu událostí si vyberte tu událost, již chcete přidat konkrétní zvuk. Pomocí tlačítka **Procházet** pak prohledejte svůj pevný disk a příslušný zvukový soubor lokalizujte. (Upozorujeme, že v tuto chvíli jsou podporovány pouze zvukové soubory ve formátu *.wav!)
- **Přehrát**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



9.3. 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 2014**.

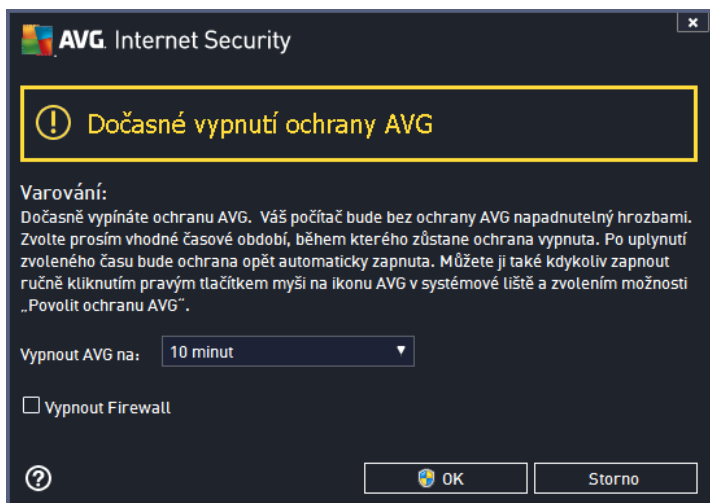
Máte prosím na paměti, že tato volba by v žádném případě neměla být použita, pokud to není opravdu nezbytně nutné!



V naprosté většině případů **není nutné** deaktivovat **AVG Internet Security 2014** před instalací nového software nebo ovladače, a to ani tehdy, pokud budete během instalace vyzváni k zavěšení všech spuštěných aplikací. Pokud by v takovém případě došlo ke kolizi, pravděpodobně bude stačit [deaktivovat rezidentní ochranu](#) (v odkazovaném dialogu zrušíte označení u položky **Povolit Rezidentní štít**). Jestliže budete opravdu nuceni deaktivovat **AVG Internet Security 2014**, zapněte jej hned, jakmile to bude možné. Pamatujte, že pokud jste připojeni k Internetu nebo k jiné síti, je váš počítač bez aktivní ochrany vysoce zranitelný.

Jak vypnout ochranu AVG

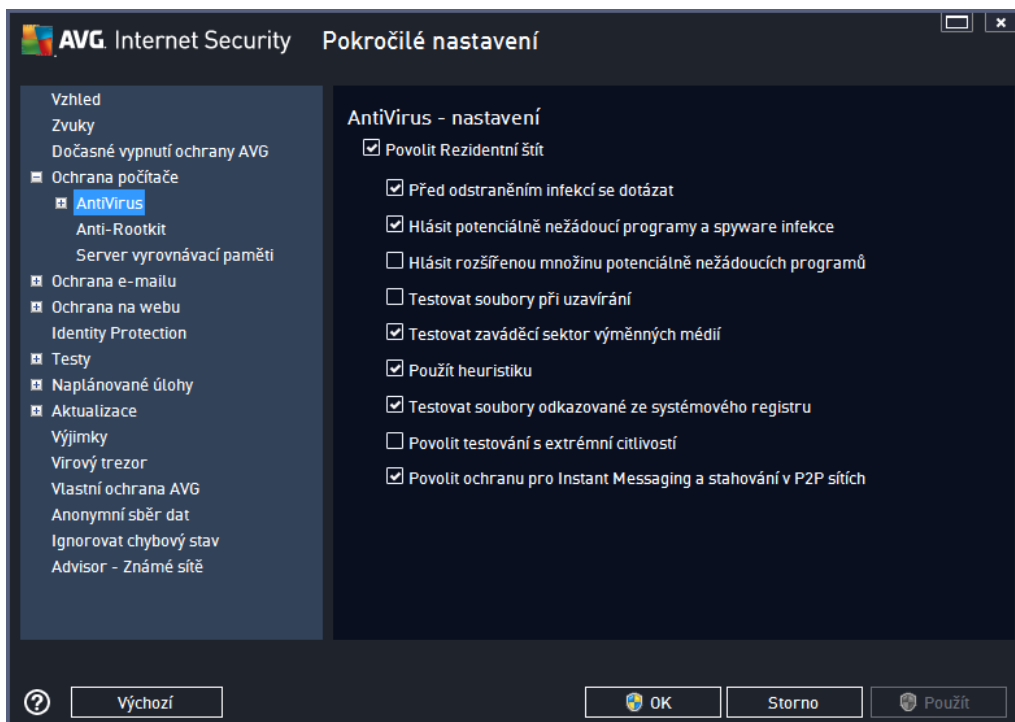
Klikněte na tlačítko **Dočasné vypnout ochranu AVG** a svou volbu potvrďte stiskem tlačítka **Použít**. V nově otevřeném dialogu **Dočasné vypnutí ochrany AVG** pak nastavte požadovaný čas, po který potebujete **AVG Internet Security 2014** vypnout. Standardně bude ochrana vypnuta po dobu 10 minut, což je dostatečné pro všechny běžné úkony. Můžete si však zvolit i delší časový interval, ale tuto možnost nedoporučujeme, pokud to není naprosto nezbytně nutné. Po uplynutí zvoleného časového intervalu se všechny vypnuté komponenty znovu automaticky aktivují. Maximální doba 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**.



9.4. Ochrana počítače

9.4.1. AntiVirus

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



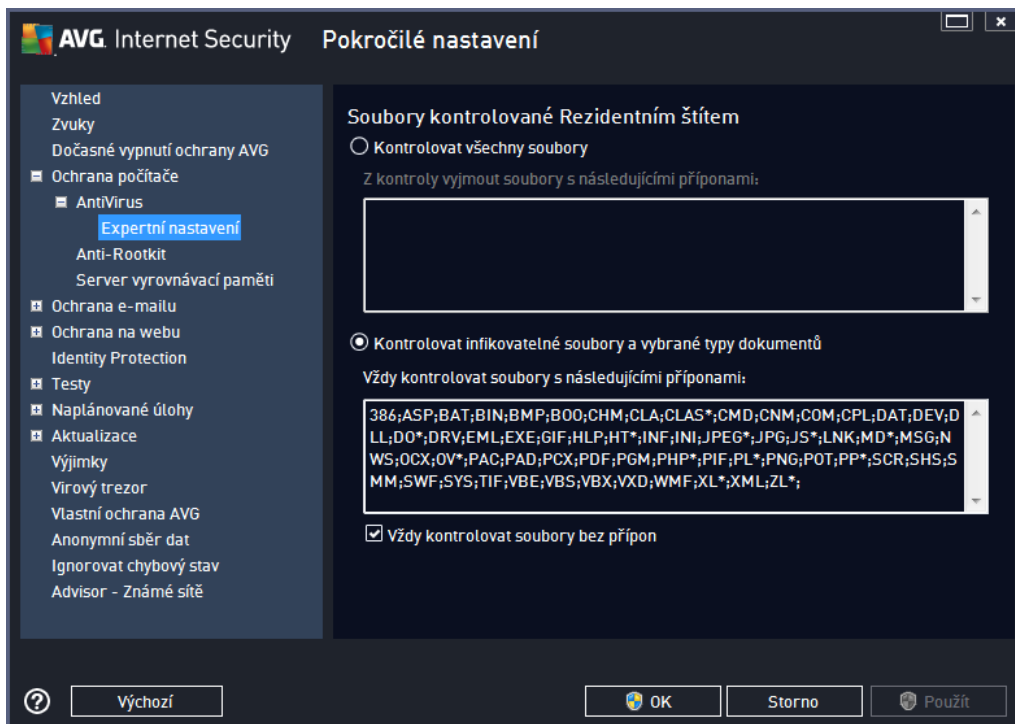
V dialogu **Nastavení Rezidentního štítu** máte možnost celkově aktivovat i deaktivovat rezidentní ochranu označením i vypnutím položky **Povolit Rezidentní štít** (tato položka je ve výchozím nastavení zapnuta). Dále můžete prostým výběrem rozhodnout, které funkce rezidentní ochrany mají být aktivovány:



- **Před odstraněním infekcí se dotázat** (ve výchozím nastavení zapnuto) - pokud je políčko zaškrtnuté, Rezidentní štít nebude s nalezenými infekcemi nic dlelat automaticky a vždy se vás zeptá, jak si přejete s nimi naložit. Pokud necháte políčko neoznačené, pak se **AVG Internet Security 2014** pokusí každou nalezenou infekci vyléčit, a pokud to nepůjde, přesune objekt do [vírového 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 v tšině něco program představuje bezpečnostní riziko, jsou mnohdy instalovány v domě a se souhlasem uživatele. Doporučujeme ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
- **Hlásit rozšířenou množinu potenciálně nežádoucích programů** (ve výchozím nastavení vypnuto) - zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware, tj. programů, které jsou v povodní podobě od výrobce neškodné a v podstatě, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.
- **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 přidávané do systémového registru, aby tak zabránil možnému spuštění již známé infekce při prvním startu počítače.
- **Povolit testování s extrémní citlivostí** (ve výchozím nastavení vypnuto) - ve specifických situacích (mimo žádný stav ohrožení počítače) můžete zvolit tuto metodu kontroly, která aktivuje nejkvalitnější a nejpodrobnější testovací algoritmy. Mějte však na paměti, že tato metoda je srovnatelně 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):

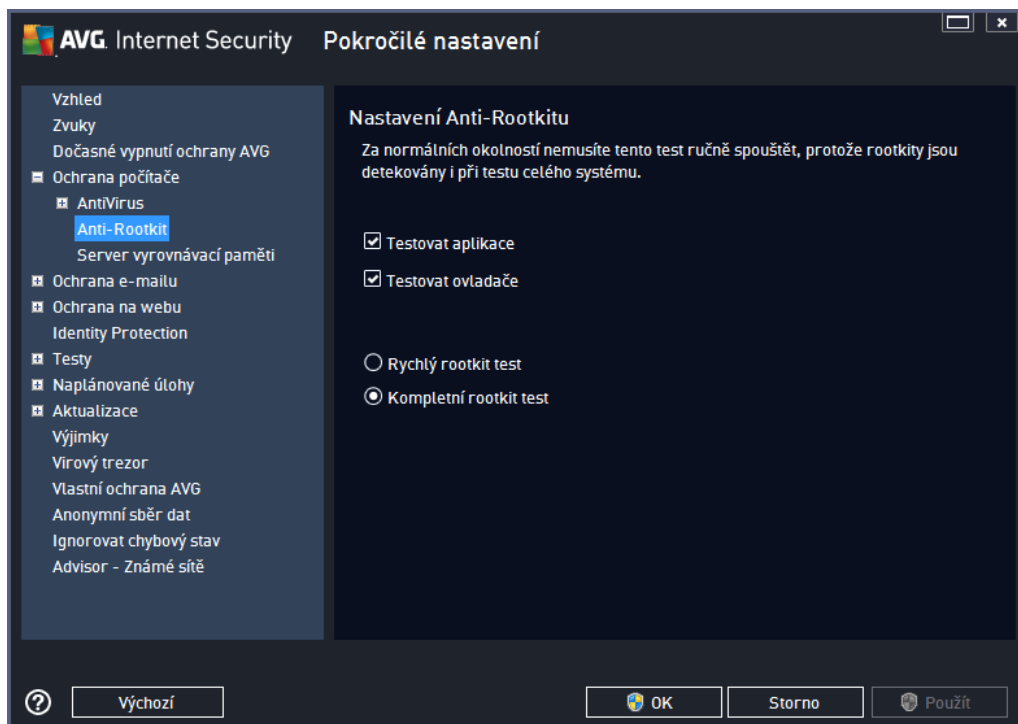


Svou volbou rozhodnete, zda chcete **Testovat všechny soubory** nebo pouze **Testovat infikovatelné soubory a vybrané typy dokumentů**. Pro urychlení testování a současně dosažení maximální bezpečnosti doporučujeme ponechat výchozí nastavení. Tak budou testovány infikovatelné soubory s příponami uvedenými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

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

9.4.2. Anti-Rootkit

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

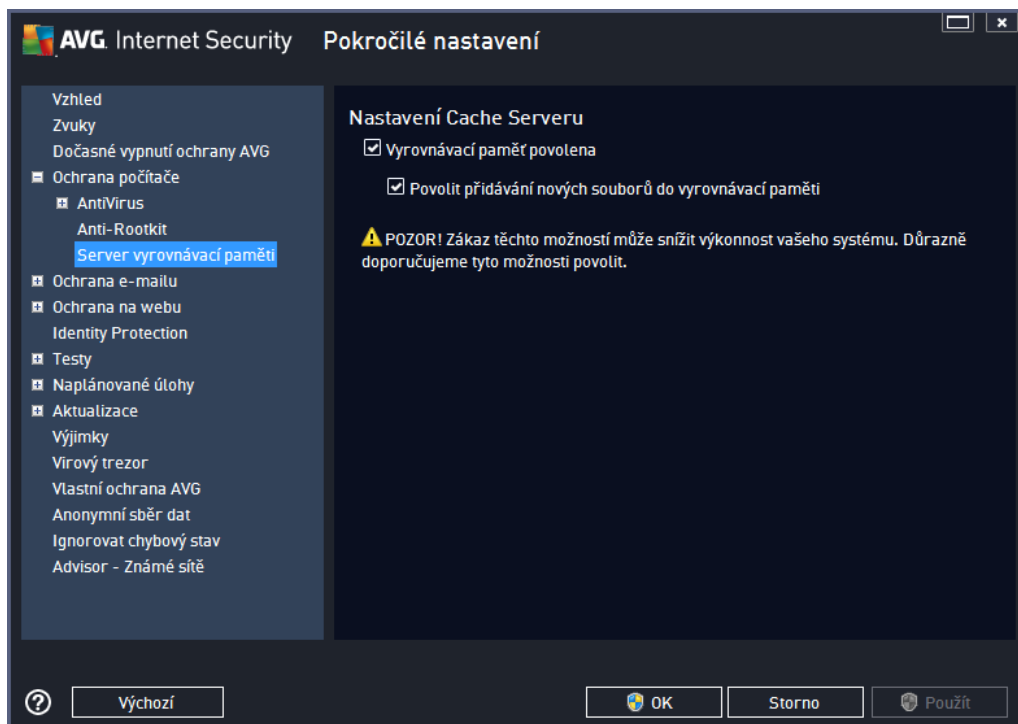


Možnosti **Testovat aplikace** a **Testovat ovladače** umožní určit, co vše má být v testu na rootkity zahrnuto. Jiné než výchozí nastavení doporučíme pouze zkušeným uživatelům; jinak prosím ponechte všechny možnosti zapnuté. Dále se pak můžete rozhodnout, v jakém režimu si přejete test spustit:

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

9.4.3. Server vyrovnávací paměti

Dialog **Nastavení Cache Serveru** se vztahuje k procesu serveru vyrovnávací paměti, jehož úkolem je zrychlit přístup ke všem testům **AVG Internet Security 2014**:



V rámci tohoto procesu **AVG Internet Security 2014** detekuje a vyřadí soubory (za daných podmínek lze považovat například soubory digitálně podepsané z důvěryhodného zdroje) 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.

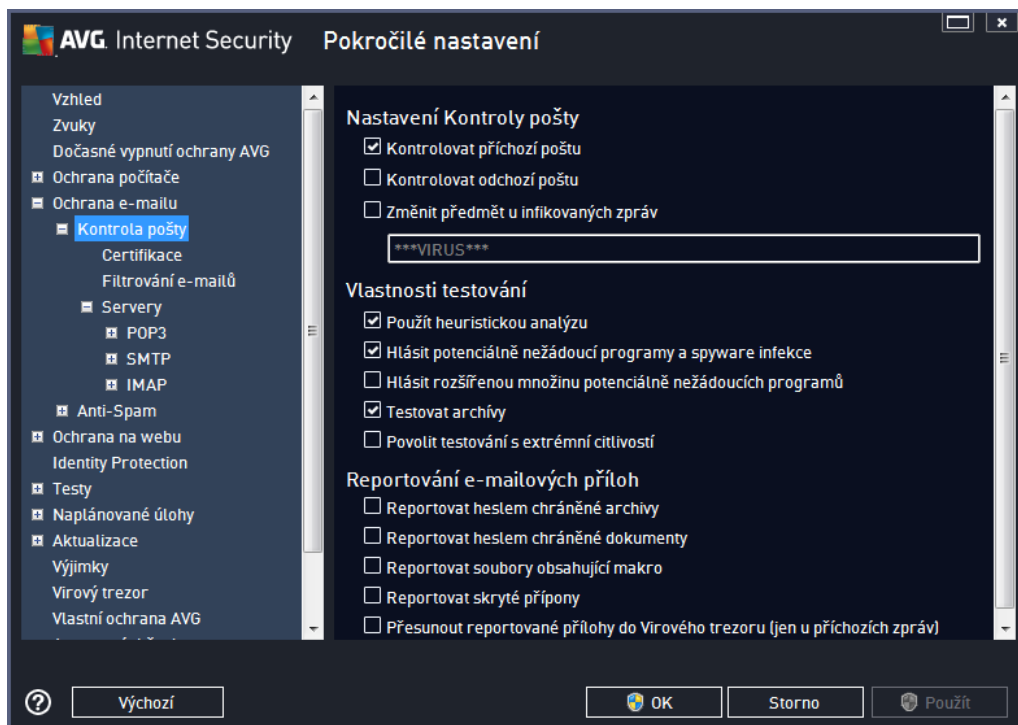
Pokud nemáte skutečnou důvod cache server vypínat, důrazně doporučujeme, abyste se přidrželi výchozího nastavení a ponechali obě položky zapnuté! V opačném případě dojde k výraznému snížení rychlosti a výkonosti Vašeho systému.

9.5. Kontrola pošty

V této sekci máte možnost editovat podrobné nastavení pro službu [Kontrola pošty](#) a [Anti-Spam](#):

9.5.1. 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 útu
- **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 doporuujeme 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-



mail . Když je tato možnost aktivována, můžete filtrovat přiložky e-mail nejen podle přípony, ale i podle skutečného obsahu a formátu (*který přípona nemusí odpovídat*). Filtrování lze nastavit v dialogu [Filtrování e-mail](#) .

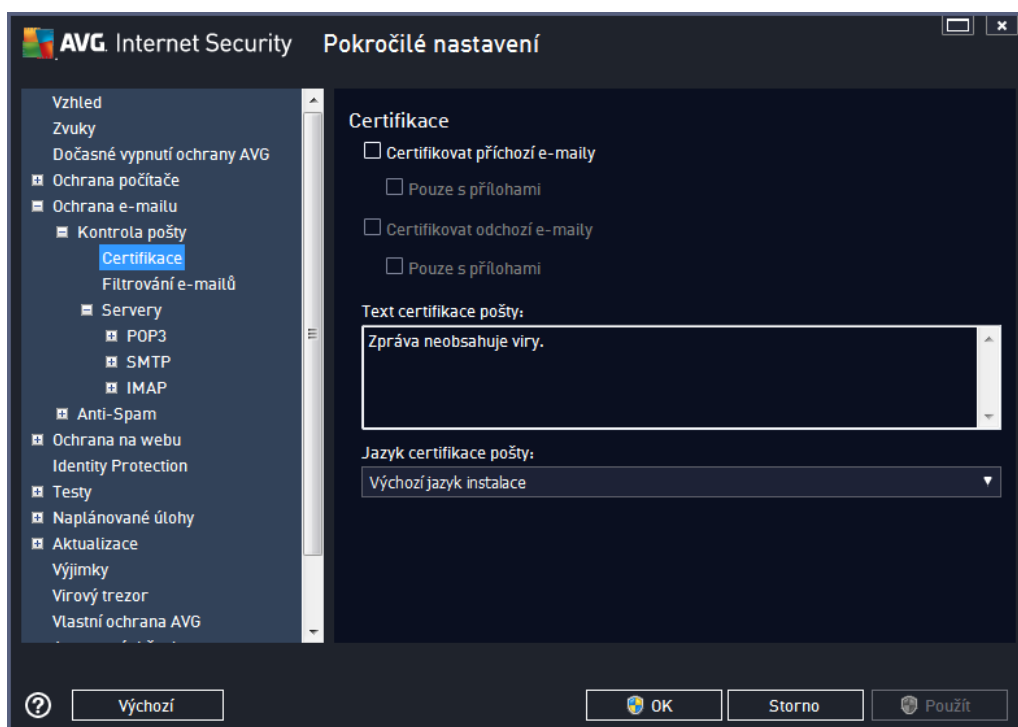
- **Hlásit potenciálně nežádoucí programy a spyware infekce** (ve výchozím nastavení zapnuto) - kontrola přítomnosti potenciálně nežádoucích programů (*spustitelné programy, které mohou fungovat jako spyware nebo adware*). Zaškrtnutím tohoto políčka aktivujete testování přítomnosti spyware, nejen virů. Spyware představuje poněkud problematickou kategorii hrozeb, protože i když většina těchto programů představuje bezpečnostní riziko, jsou mnohdy instalovány v domě a se souhlasem uživatele. Doporučujeme ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
- **Hlásit rozšířenou množinu potenciálně nežádoucích programů** (ve výchozím nastavení vypnuto) - zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware, tj. programů, které jsou v podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.
- **Testovat 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 nejkvalitnější testovací algoritmy a velmi podrobně prohledá naprosto všechny oblasti vašeho počítače. Mějte však na paměti, že tato metoda je srovnatelně 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](#).

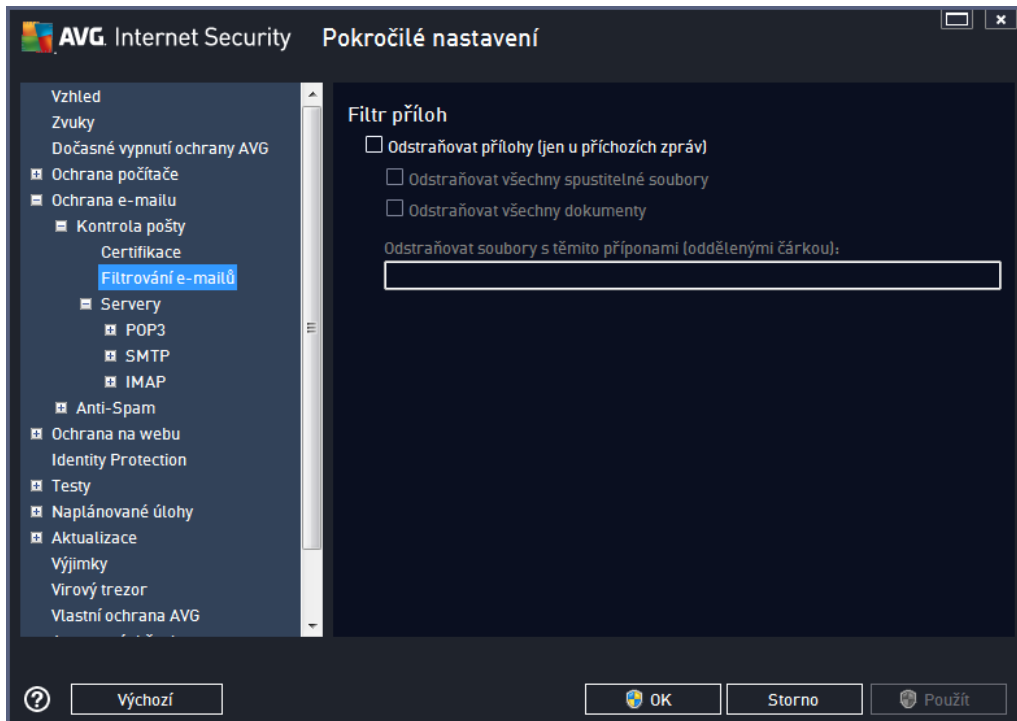
- **Reportovat heslem chráněné archivy** - archivy (ZIP, RAR atd.) chráněné heslem není možné otestovat na přítomnost virů; po zaškrtnutí tohoto políčka se tyto archivy budou označovat jako potenciálně nebezpečné.
- **Reportovat heslem chráněné dokumenty** - dokumenty chráněné heslem není možné otestovat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

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



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

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



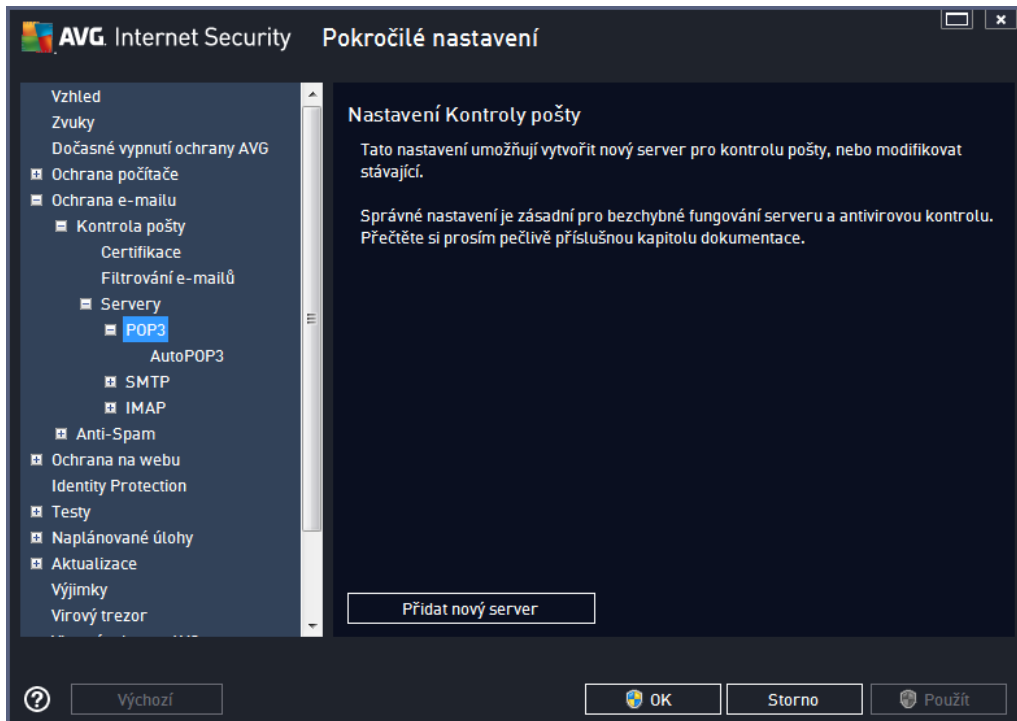
Dialog **Filtr příloh** umožňuje nastavení parametrů pro testování příloh e-mailových zpráv. Ve výchozím nastavení je možnost **Odstraňovat přílohy** vypnuta. Pokud se rozhodnete pro její aktivaci, budou automaticky odstraněny všechny přílohy zpráv, které byly detekovány jako infikované nebo potenciálně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

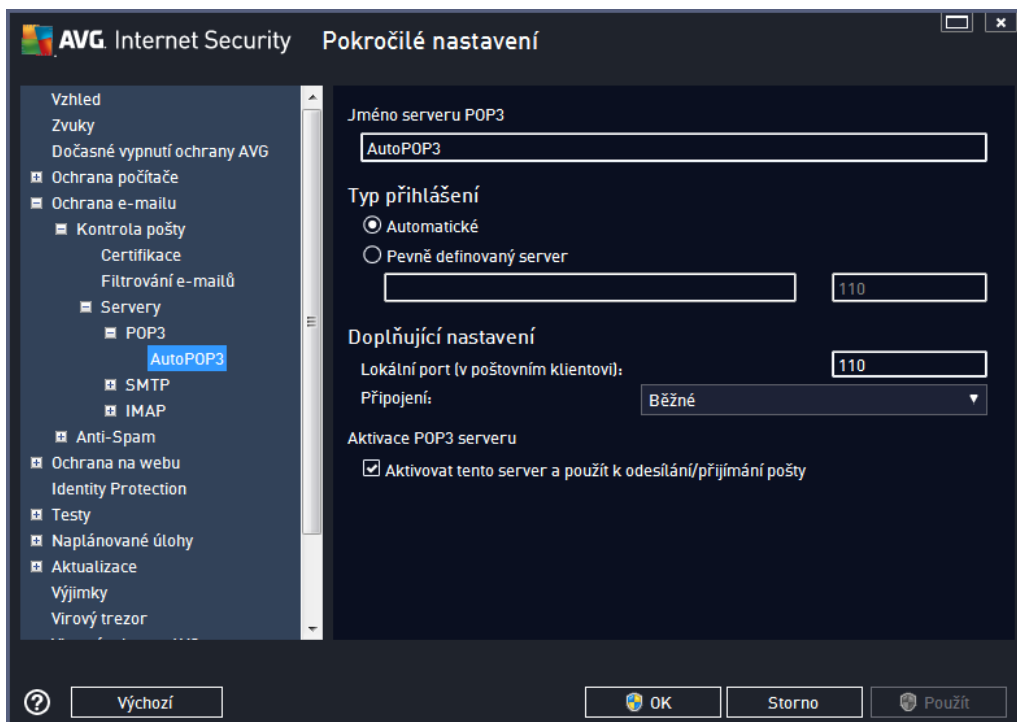
V sekci **Servery** máte možnost editovat parametry jednotlivých serverů [Kontroly pošty](#):

- [POP3 server](#)
- [SMTP server](#)
- [IMAP server](#)

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



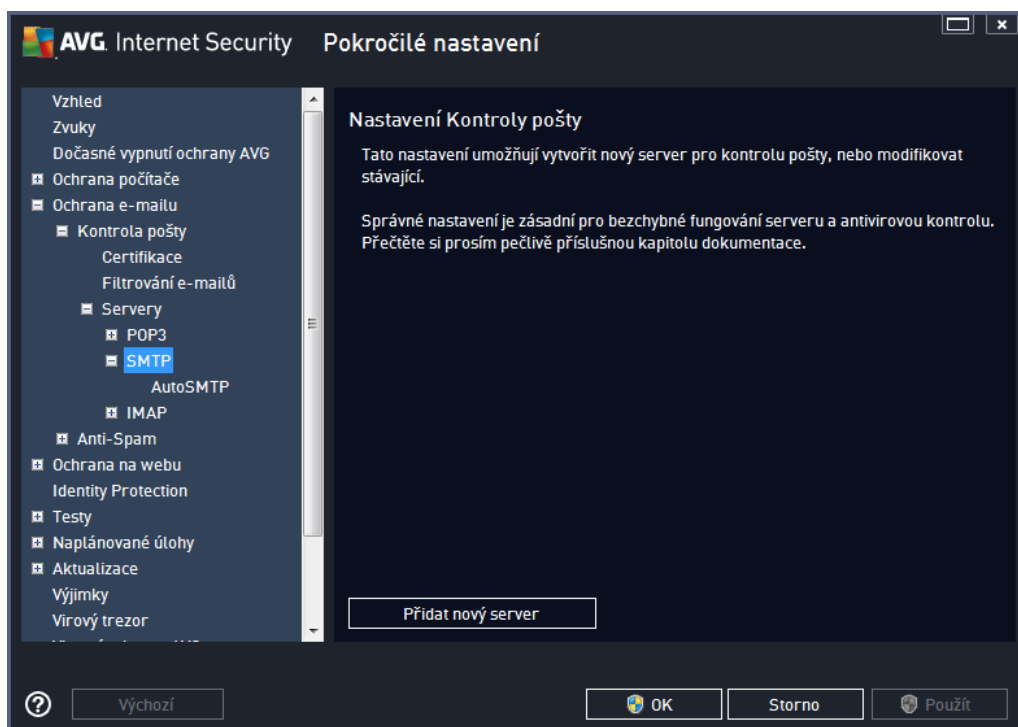
V tomto dialogu nastavujete server [Kontroly pošty](#) s protokolem POP3 pro p íchozí poštu:



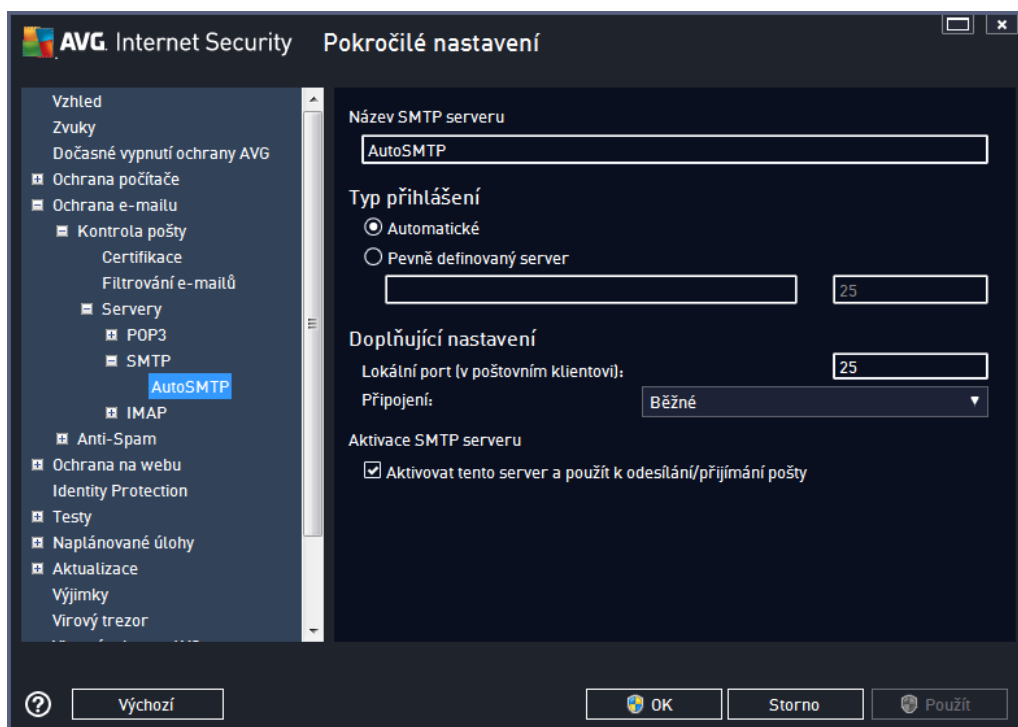
- **Jméno serveru POP3** - v tomto poli m žete zadat jméno nov p idaných server (server POP3 p idáte tak, že kliknete pravým tla ítkem myši nad položkou POP3 v levém naviga ním menu).



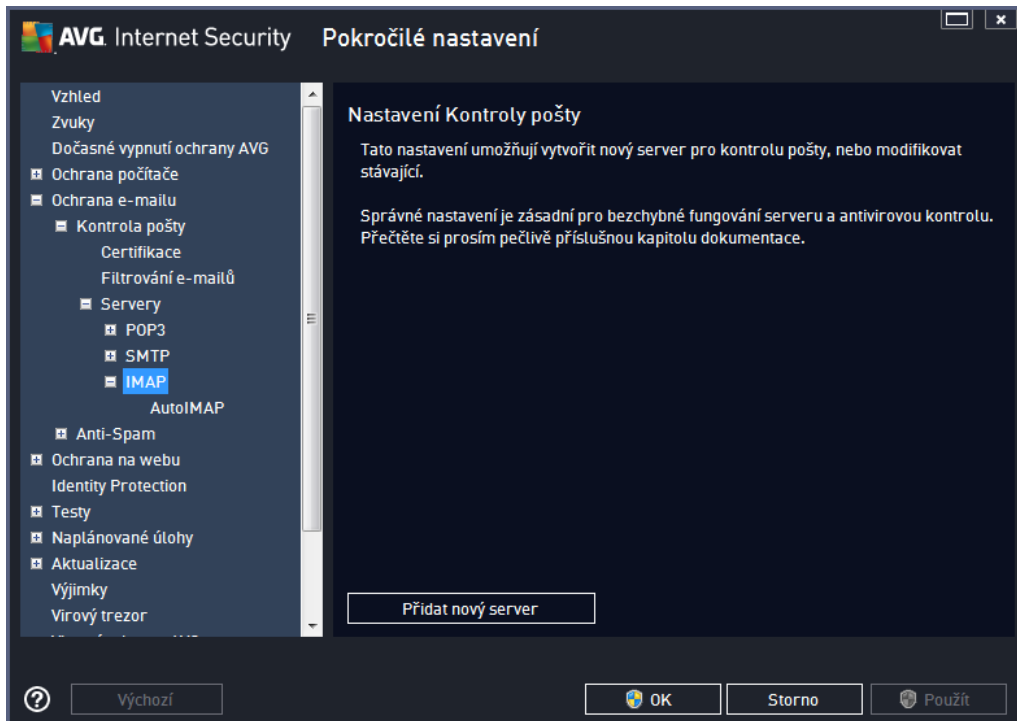
- **Typ p íhlášení** - definuje, jak má být určen poštovní server, ze kterého bude přijímána pošta
 - **Automatické** - cílový server bude určen podle nastavení ve vaší poštovní aplikaci; není třeba nic dále specifikovat.
 - **Pevně definovaný server** - v tomto případě bude vždy použit konkrétní server. Je třeba zadat adresu nebo jméno vašeho poštovního serveru. Při ihlášovacím jménu pak lze stanovit bezpečnostní jméno. Jako jméno je možné použít jak doménový název (*například pop.acme.com*), tak IP adresu (*například 123.45.67.89*). Pokud poštovní server používá nestandardní port, lze tento port zadat za jméno serveru oddělený dvojtečkou (*například pop.acme.com:8200*). Standardní port pro POP3 komunikaci je 110.
- **Doplňující nastavení** - specifikuje další detailní parametry:
 - **Lokální port** - určuje, na kterém portu lze očekávat komunikaci z poštovní aplikace. Tento port je 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 je cílový poštovní server podporuje.
- **Aktivace POP3 serveru** - zapnutím/vypnutím položky máte možnost aktivovat i deaktivovat právě nastavený POP3 server



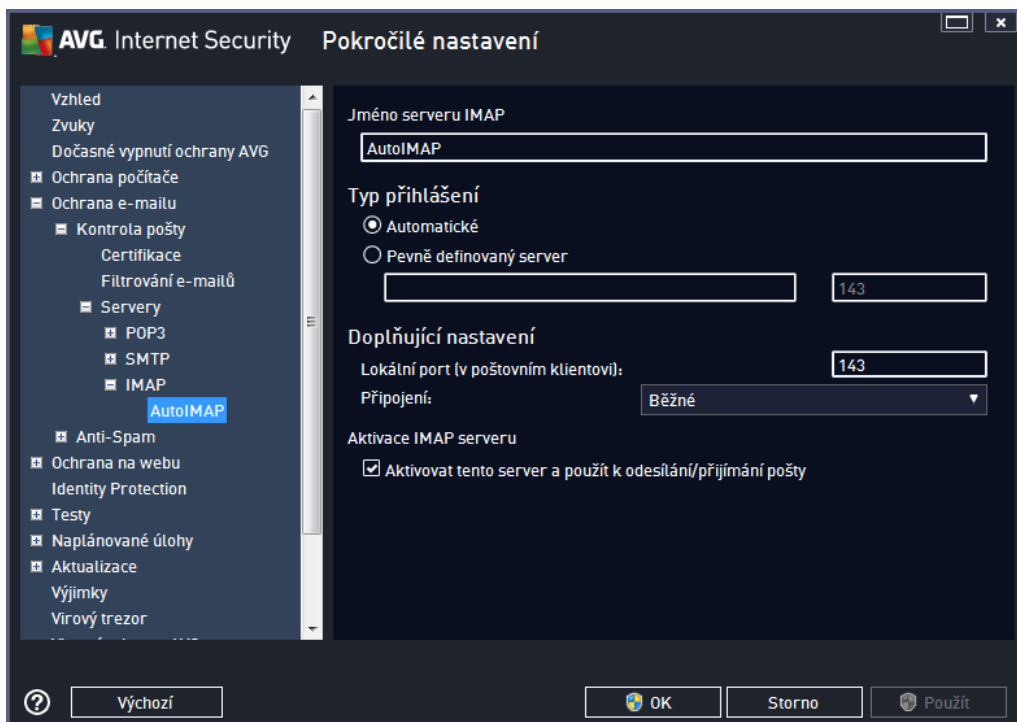
V tomto dialogu nastavujete server [Kontroly pošty](#) s protokolem SMTP pro odchozí poštu:



- **Název SMTP serveru** - v tomto poli můžete zadat jméno nově určených serverů (server SMTP používáte tak, že kliknete pravým tlačítkem myši nad položkou SMTP v levém navigačním menu). U automaticky vytvořeného serveru "AutoSMTP" je toto pole deaktivováno.
- **Typ přihlášení** - definuje, jak má být určen poštovní server, ze kterého bude odesílána pošta:
 - **Automatické** - cílový server bude určen podle nastavení ve vaší poštovní aplikaci; není třeba nic dále specifikovat
 - **Pevně definovaný server** - v tomto případě bude vždy použit konkrétní server. Do editačního řádku je třeba zadat adresu nebo jméno vašeho poštovního serveru. Jako jméno je možné použít jak doménový název (*nap. smtp.acme.com*), tak i IP adresu (*nap. 123.45.67.89*). Pokud poštovní server používá nestandardní port, lze tento port zadat za jméno serveru oddělený dvojtečkou (*nap. smtp.acme.com:8200*). Standardní port pro SMTP komunikaci je 25.
- **Doplňující nastavení** - specifikuje další detailní parametry:
 - **Lokální port** - určuje, na kterém portu lze očekávat komunikaci z poštovní aplikace. Tento port je pak také nutné v poštovní aplikaci zadat jako port pro SMTP komunikaci.
 - **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 je cílový poštovní server podporuje.
- **Aktivace SMTP serveru** - zapnutím/vypnutím položky máte možnost aktivovat i deaktivovat právě nastavený SMTP server



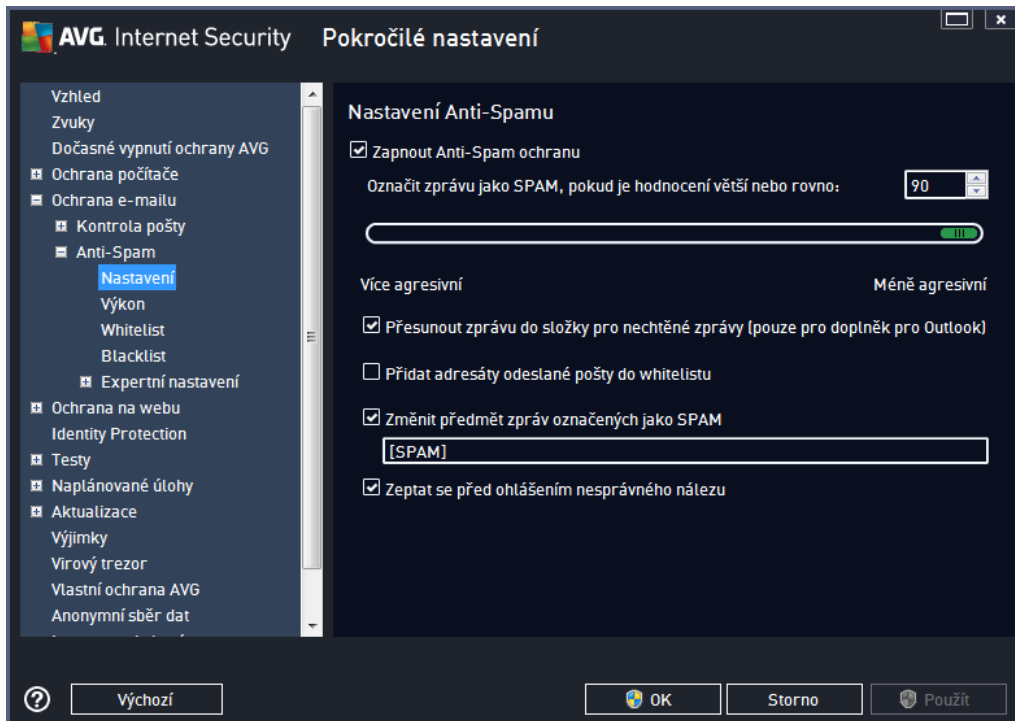
V tomto dialogu nastavujete server [Kontroly pošty](#) s protokolem IMAP pro odchozí poštu:



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

- **Typ p íhlášení** - 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 (*imap.acme.com*), tak i IP adresu (*123.45.67.89*). Pokud poštovní server používá nestandardní port, lze tento port zadat za jméno serveru oddělený dvojtečkou (*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 cílový poštovní server podporuje.
- **Aktivace IMAP serveru** - zapnutím/vypnutím položky máte možnost aktivovat i deaktivovat právě nastavený IMAP server

9.5.2. Anti-Spam



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

V tomto dialogu také můžete definovat, jak chcete nastavit úroveň ochrany proti spamu - více i méně agresivní. Na základě několika dynamických testovacích technik pak filtr komponenty **Anti-Spam** přidělí každé zprávě určitou skóre (například podle toho, nakolik se obsah zprávy blíží textu, který lze považovat za spam). Hodnotu úrovně citlivosti pro označení spamu lze nastavit buď přímo vepsáním číselné hodnoty do příslušného pole nebo pomocí posuvníku u položky **Označit zprávu jako SPAM, pokud je hodnocení větší nebo rovno**.

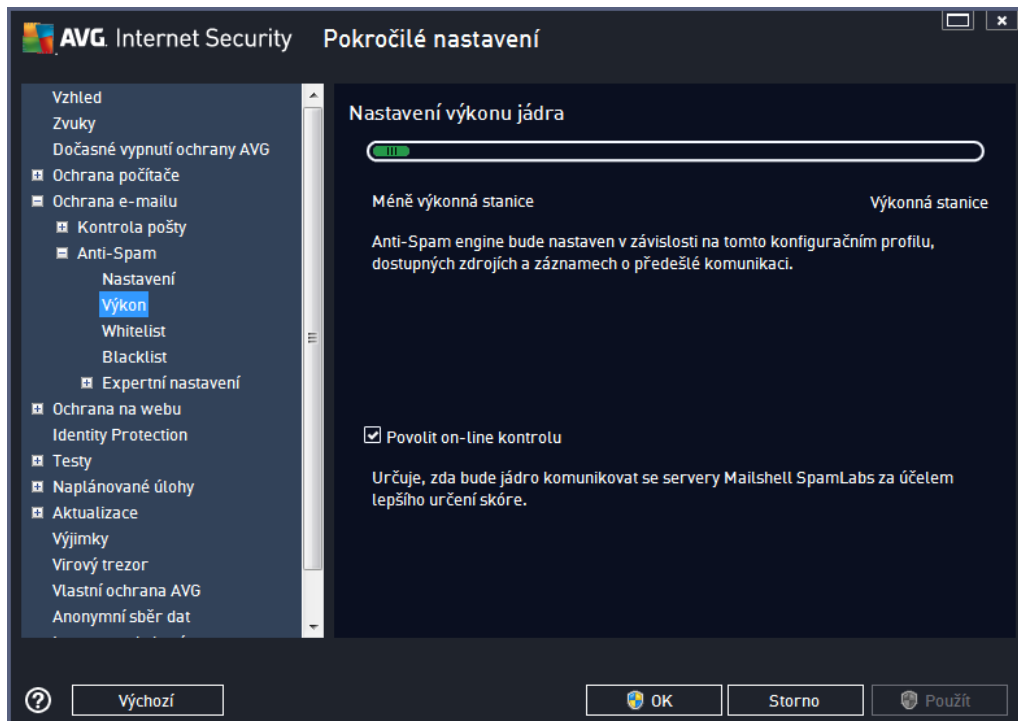
Úroveň citlivosti na spam lze nastavit v rozmezí 50-90. Následuje přehled úrovní ochrany, jež odpovídají jednotlivým hodnotám:

- **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 doporučena žádným nastavením pro běžné uživatele.**

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

- **P esunout zprávu do složky pro necht ěné zprávy (pouze pro dopln ěk pro Outlook)** - Ozna ěním této položky zvolíte, že každá zpráva, jejíž obsah bude se zohledn ěním nastavené úrovn ě citlivosti ozna ěn jako spam, bude automaticky p esunuta do složky pro nevyžadán ě zprávy. Tato možnost platí pouze pro poštovní program MS Outlook.
- **P idat adresáty odeslan ě pošty na seznam povolen ěch odesílatel ě** - Ozna ěním této položky potvrdíte, že adresáti vámi odeslan ěch e-mailov ěch zpráv jsou považováni za d ě v ryhodn ě a pošta odeslan ě z jejich ú tu m ě že být bez obav doru ěna.
- **Zm ěnit p edm ět zprávy u zpráv ozna ěných jako spam** - Ozna ěním této položky aktivujete textové pole, v n ěmž máte možnost editovat text, kter ěm si p ežete ozna ěvat zprávy detekovan ě jako spam - tento text pak bude automaticky vepsán do p edm ětu každ ě detekovan ě e-mailov ě zprávy.
- **Zeptat se p ed ohlášen ěm nesprávn ěho dotazu** - Pokud jste b ěhem instalace potvrdili svou ú ast v projektu [Anonymn ě sb ěr dat](#), povolili jste odesílání report ů o detekovan ěch hrozbách do AVG. Tato hlášen ě jsou odesílána automaticky. Pokud si vřak p ežete mít možnost zkontrolovat, že detekovan ě zpráva má být skute ěn klasifikována jako spam, ozna ěte položku **Zeptat se p ed ohlášen ěm nesprávn ěho dotazu** a p ed odeslán ěm reportu vám bude zobrazen dotazovac ě dialog vyžaduj ěcí vaře potvrzen ě.

Dialog **Nastaven ě výkonu jádra** (odkazovan ě položkou **V ěkon**) nabízí možnost konfigurace parametr ů výkonu komponenty **Anti-Spam**:



Polohou posuvn ěku ur ěete úrove Ň testovac ěho výkonu na ose **M ěn ě v ěkonn ě stanice / V ěkonn ě stanice**.

- **M ěn ě v ěkonn ě stanice** znamená, že b ěhem testovac ěho procesu nebudou k identifikaci spamu použ ěta žádn ě pravidla. Identifikace spamu bude založena v ěhradn ě na porovn ěn ě s testovac ěmi daty. Tento reŇim pro b ěžn ě pouŇívání nedoporu ěujeme, nastaven ě lze doporu ěit v ěhradn ě u po ěta ě s



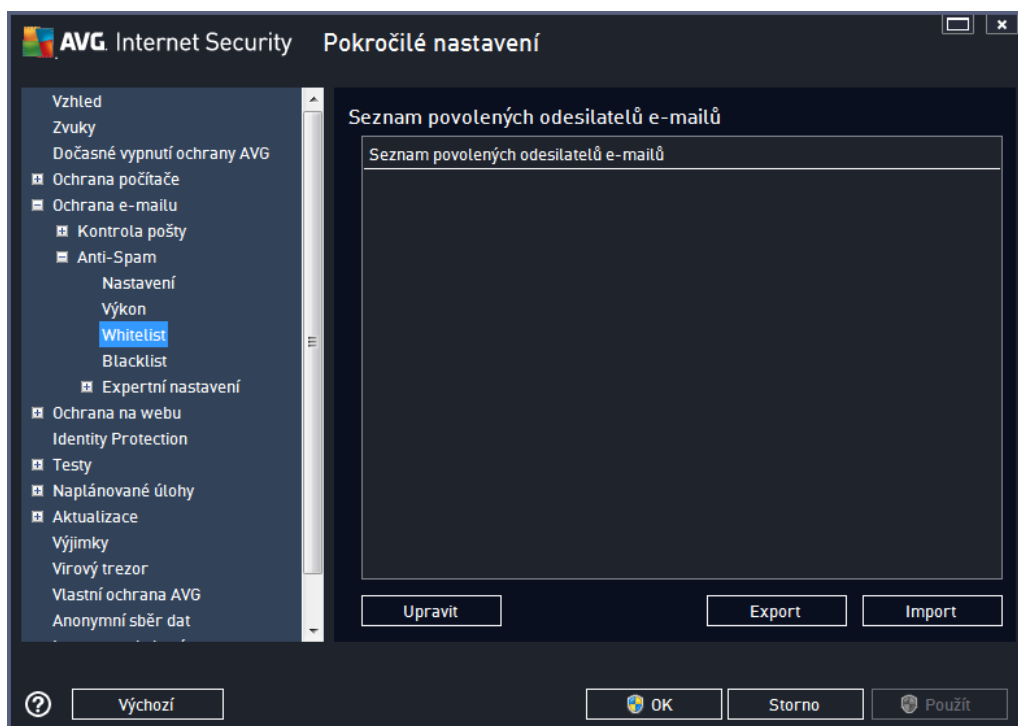
velmi nízkou úrovní hardwarového vybavení.

- **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.

Obecná doporučení: ujmeme dodržet výchozí nastavení, pokud nemáte skutečný důvod tuto konfiguraci změnit. Změna 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 doručena nikdy nebude mít charakter spamu:



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

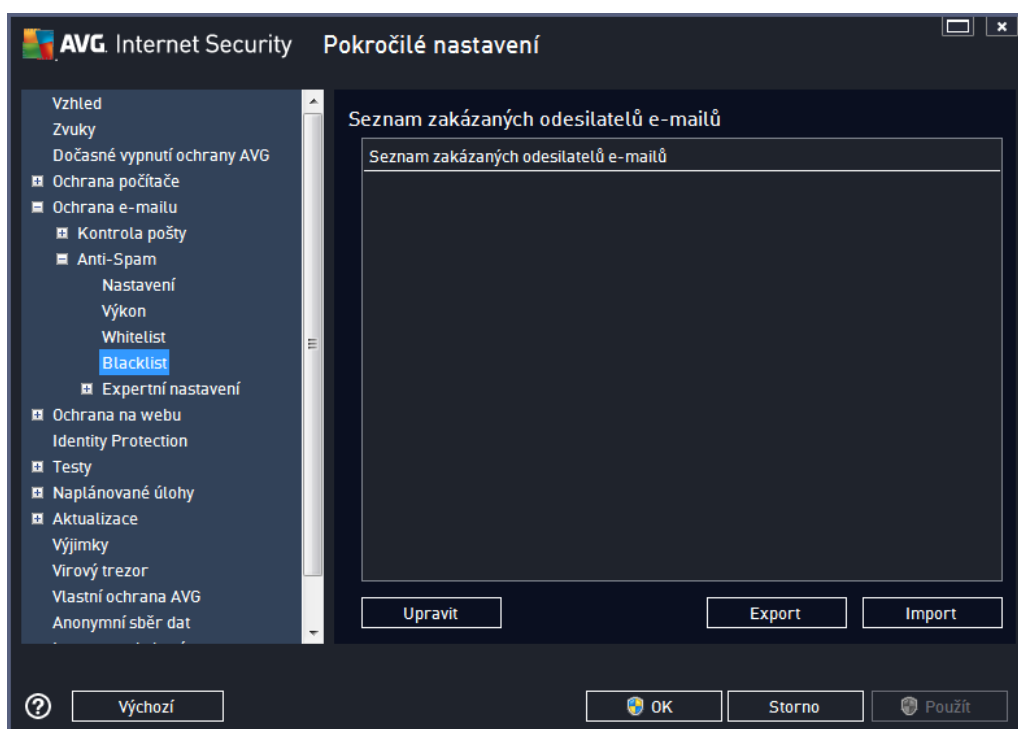
Ovládací tlačítka dialogu

K dispozici jsou vám tato ovládací tlačítka:



- **Upravit** - stiskem tohoto tlačítka otevřete dialog, v něm můžete manuálně přidávat adresy ze seznamu (můžete také použít jednorázovou metodu "kopírovat a vložit"). Adresy/doménová jména vkládáte 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 jednu položku (adresu nebo doménové jméno).

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



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

Ovládací tlačítka dialogu

K dispozici jsou vám tato ovládací tlačítka:



- **Upravit** - stiskem tohoto tlačítka otevřete dialog, v němž můžete manuálně přidávat adresy ze seznamu (můžete také použít jednorázovou metodu "kopírovat a vložit"). Adresy/doménová jména vkládejte po jednom na každý řádek.
- **Export** - pokud budete z libovolného důvodu chtít seznam adres/doménových jmen exportovat, můžete export provést pomocí tohoto tlačítka. Veškeré záznamy budou uloženy ve formátu prostého textu.
- **Import** - pokud již máte seznam adres/doménových jmen uložený v textovém souboru, můžete jej snadno importovat za použití tohoto tlačítka. Soubor, z něž import provádíte, musí být ve formátu prostého textu a obsah musí být rozdělen tak, že každý řádek obsahuje pouze jednu položku (adresu nebo doménové jméno).

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

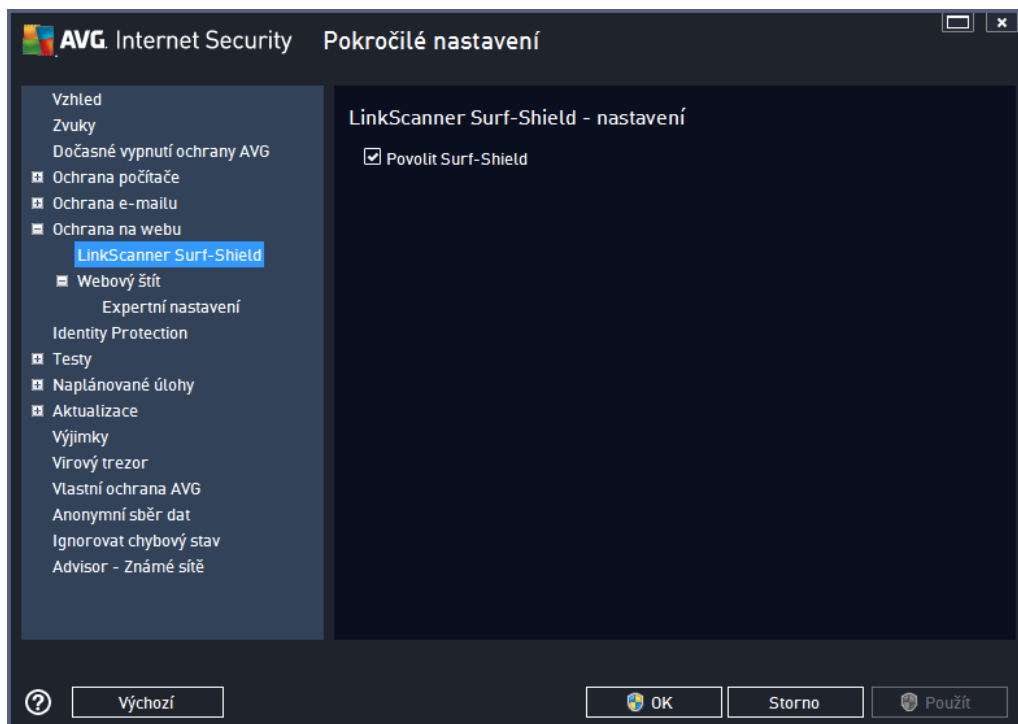
Pokud se přesto domníváte, že je nutné mít konfiguraci služby Anti-Spam na úrovni vysoce pokročilého nastavení, pokračujte prosím podle instrukcí uvedených přímo v dialogu. Obecně platí, že v každém dialogu máte možnost zapnout jednu konkrétní funkci služby Anti-Spam a její popis je uveden přímo v dialogu. Nastavit můžete tyto parametry:

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



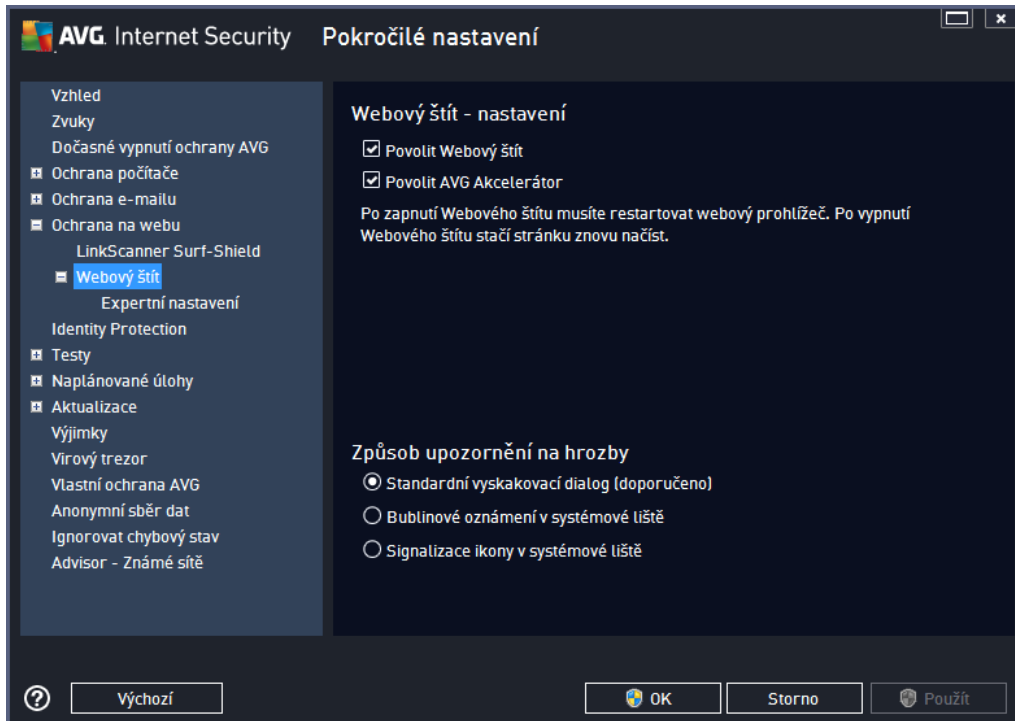
9.6. Ochrana na webu

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



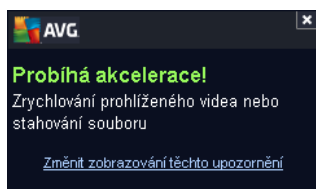
- **Povolit Surf-Shield** - (ve výchozím nastavení zapnuto): aktivní ochrana proti agresivním webovým stránkám. Kontrola stránek se provádí v okamžiku jejich načítání. Stránky s nebezpečným obsahem jsou v příslušném internetovém prohlížeči (nebo jiné aplikaci, která používá HTTP) rovnou zablokovány.

9.6.1. Webový štít



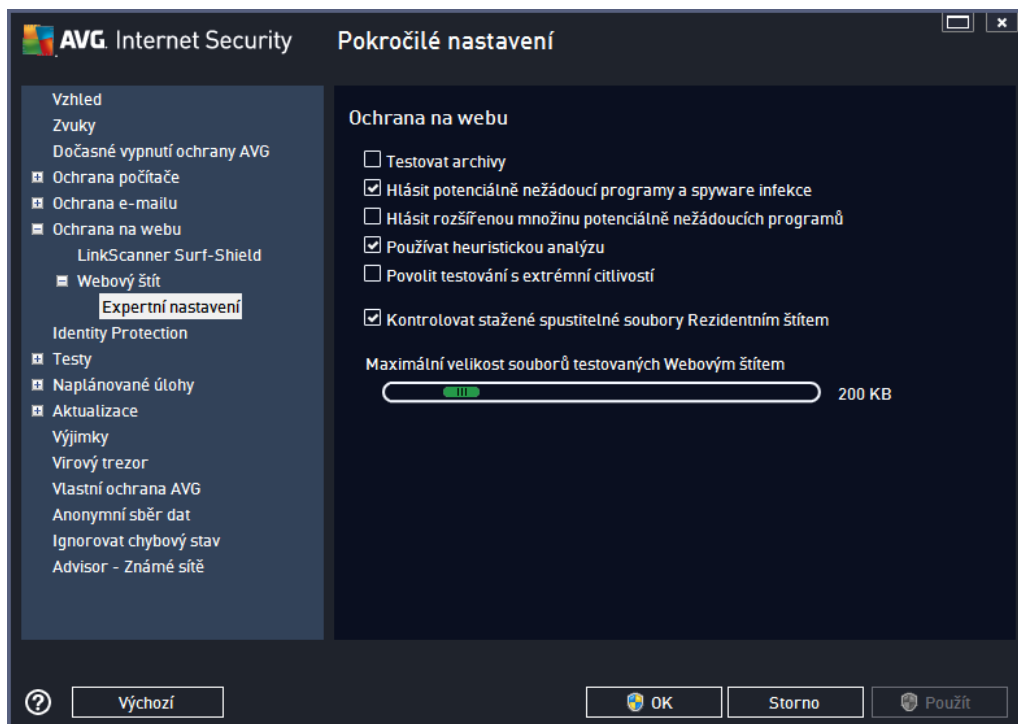
Dialog **Webový štít - nastavení** nabízí tyto možnosti:

- **Povolit Webový štít** (ve výchozím nastavení zapnuto) - Označením položky aktivujete/deaktivujete službu **Webový štít**. Pokročilé nastavení této komponenty pak najdete v podkategorii [Ochrana na 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 při 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 signalizační ikonou v systémové liště.



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

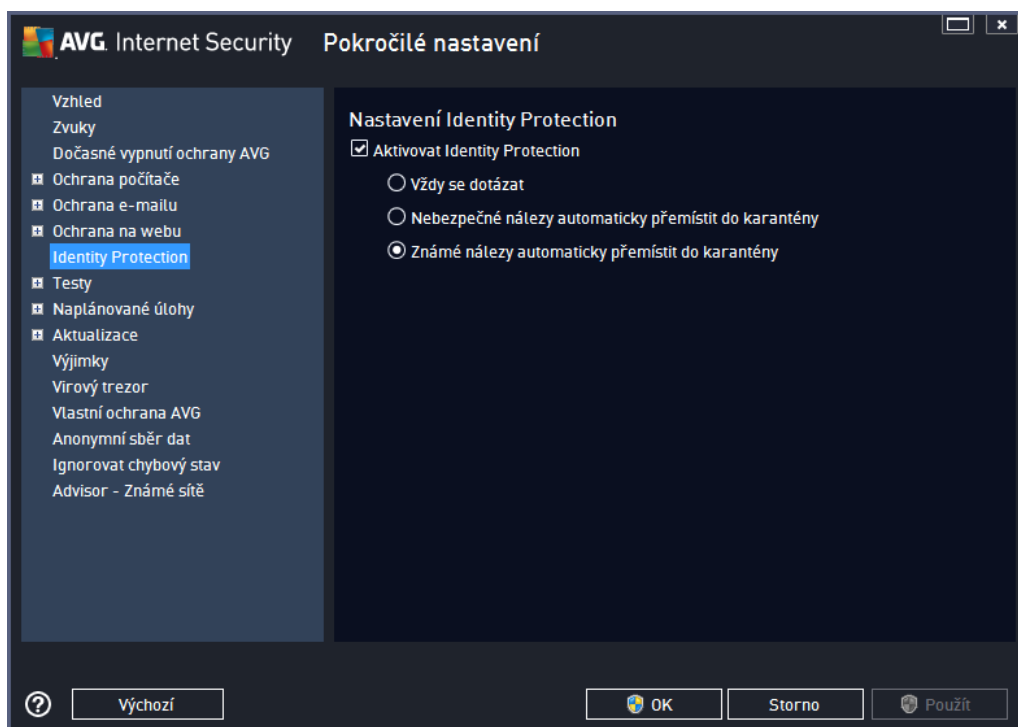
- **Povolit ochranu webu** - touto volbou potvrzujete, že v rámci služby **Webový štít** si přejete, aby byla prováděna kontrola obsahu navštívených www stránek. Zapravidopokladu, že je tato volba zapnuta (*výchozí nastavení*), můžete dále povolit nebo vypnout tyto volby:
 - **Testovat archívy** - (ve *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 v domě a se souhlasem uživatele. Doporučujeme ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
 - **Hlásit rozšířenou množinu potenciálně nežádoucích programů** - (ve *výchozím nastavení vypnuto*) zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware, tj. programů, které jsou v podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně můžete blokovat také některé legální programy, proto je ve *výchozím nastavení* tato možnost vypnuta.
 - **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 nejkvalitnější testovací algoritmy a velmi podrobně prohledá naprosto všechny oblasti vašeho počítače. Mějte však na paměti, že tato metoda je aspoň velmi náročná.
- **Kontrolovat stažené spustitelné soubory Rezidentním štítem** - (ve výchozím nastavení zapnuto) testování spustitelných souborů (tj. souborů s příponami exe, bat, com) poté, co byly kompletně staženy do počítače. Za normálních okolností testuje rezidentní štít soubory z internetu ještě před vlastním stažením. Velikost takto testovaných souborů je však omezena a dá se nastavit, viz následující položka **Maximální velikost částí souboru k testování**. Větší soubory, mezi něž spustitelné soubory obvykle patří, se tedy testují po částech. Spustitelný soubor může v počítači provádět různé činnosti a změny, ověření jeho naprosté bezpečnosti je tedy klíčové. Proto doporučujeme ponechat tuto volbu zapnutou a otestovat nejen jednotlivé části kódu před stažením, ale také celý spustitelný soubor po stažení. Pokud tuto možnost vypnete, neznamená to, že spustitelné soubory stažené z internetu budou otestovány nedostatečně; AVG pouze nebude schopno posoudit kód jako celek, a proto může dojít k většímu výskytu falešných detekcí.

Posuvník dole v dialogu umožní definovat **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 aspoň 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.

9.7. Identity Protection

Identity Protection je komponentou, která pomáhá a v reálném světě 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** umožní zapnout či vypnout n, které základní vlastnosti komponenty [Identita](#):



Položka **Aktivovat Identity Protection** (ve výchozím nastavení zapnuta) aktivuje všechny dále nastavené funkce komponenty [Identity Protection](#). **D razn doporu ujeme ponechat komponentu zapnutou!** Je-li položka **Aktivovat Identity Protection** označena a komponenta je aktivní, máte dále možnost určit, co se má stát v případě detekce hrozby:

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

9.8. Testy

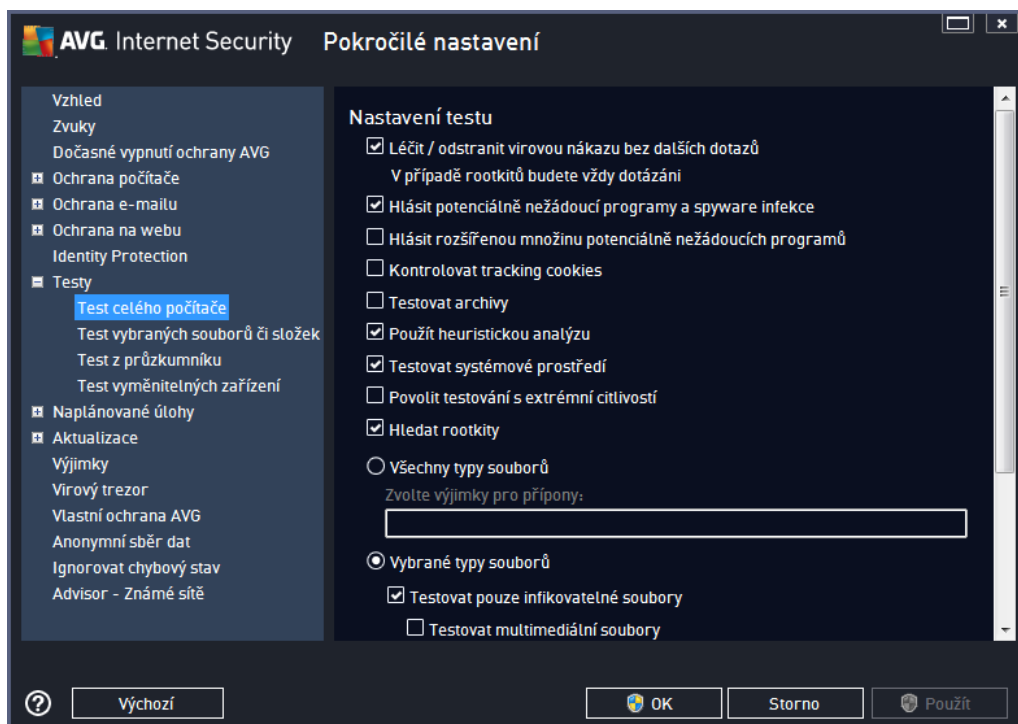
Pokročilé nastavení testů je rozděleno do čtyř kategorií, které odpovídají jednotlivým typům výrobem definovaných testů:

- **Test celého počítače** - výrobcem nastavený standardní test
- **Test vybraných souborů a 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

9.8.1. Test celého počítače

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



Nastavení testu

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

- **Léčit/odstranit virovou nákazu bez dalších dotazů** (ve výchozím nastavení zapnuto) - jestliže je během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. V případě, že virus automaticky léčit nelze, bude infikovaný objekt přesunut do [Virového trezoru](#).
- **Hlásit potenciálně nežádoucí 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 v domě a se souhlasem uživatele. Doporučujeme ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
- **Hlásit rozšířenou množinu potenciálně nežádoucích programů** (ve výchozím nastavení vypnuto) - zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware, tj. programů,



kteře jsou v p v odn podob od vobce neškodn a v p o adku, ale mohou bt snadno zneužit ke škodlivm u el m. Jde o dodate n opat en, kter zlepšuje zabezpe en vašeho po řta e na dalš úrovni, nicmn m že blokovat tak n kter legln programy, proto je ve vchozm nastaven tato mořnost vypnuta.

- **Kontrolovat tracking cookies** (ve vchozm nastaven vypnuto) - parametr definuje, že b hem testu mají bt detekovny cookies (*HTTP data zaslan serverem prohlže i a uložena na po řta i uřivatele; p i kařd dalš nvšt v thoř serveru prohlže posl cookies zp t serveru, kter podle nich rozlišuje jednotliv uřivatele*).
- **Testovat archivy** (ve vchozm nastaven vypnuto) - parametr definuje, že test m testovat vřechny soubory zabalen v n kterm typu archivu, nap řklad ZIP, RAR, ...
- **Pouřt heuristickou analzu** (ve vchozm nastaven zapnuto) - b hem testu bude pouřita k detekci infekce i metoda heuristické analzy (*dynamické emulace instrukcí testovanho objektu v prost ed virtulnho po řta e*).
- **Testovat systmov prost ed** (ve vchozm nastaven zapnuto) - test prov ř i systmov oblasti vašeho po řta e.
- **Povolit testovn s extrémn citlivost** (ve vchozm nastaven vypnuto) - ve specifickch situacch (*p i podez en na infekci ve vašem po řta i*) m řete zvolit tuto metodu testovn, kter aktivuje nejd kladn řš testovac algoritmy a velmi podrobn prov ř naprosto vřechny oblasti vašeho po řta e. M řte vřak na pam ti, že tato metoda je asov velmi nro n.
- **Hledat rootkity** (ve vchozm nastaven zapnuto) - Parametr sluřby [Anti-Rootkit](#) prohledv po řta na p řtomnost rootkit , tedy program a technologi, kter dokř maskovat p řtomnost malware v po řta i. Dojde-li k nlezu rootkitu, nemus to nutn znamenat, že je po řta infikovn. V n kterch p řpadech mohou bt rootkity pouřity jako ovlada e nebo řsti korektnch aplikac.

Dle se m řete rozhodnout, zda si p ežete testovat:

- **Vřechny typy soubor** - p i emř mte zrove mořnost vyjmout z testovn soubory definovan seznamem p řpon odd lench řrkou (*po uložení se řrky zm n na st ednky*).
- **Vybran typy soubor** - m řete se rozhodnout, že chcete, aby se testy spouřt ly pouze nad soubory, kter lze považovat za infikovateln (*soubory, kter nemohou bt infekc zasřeny, se testovat nebudou - nap řklad prost textov soubory nebo n kter nespustiteln soubory*), a to v etn multimedlnch soubor (*video, audio soubory - ponechte-li tuto polořku neozna enou, vrazn se tm zkrt as testovn, jelikoř multimedln soubory jsou obvykle pom řn velké, ale pravd podobnost infekce je u nich velmi nzk*). I zde m řete ur řit vjimky a pomoc seznamu p řpon definovat, kter soubory mají bt testovny za vřech okolnost.
- U polořky **Testovat soubory bez p řpon** pak rozhodn te, zda se mají testovat i soubory se skrytou ř i neznmou p řponou. Tato polořka je ve vchozm nastaven zapnuta a doporu ujeme, abyste se tohoto nastaven podrřeli, pokud nemte skute n d vod jej m nit. Soubory bez p řpon jsou obecn vysoce podez el a m ly by bt otestovny.

Nastavit, jak rychle probh test

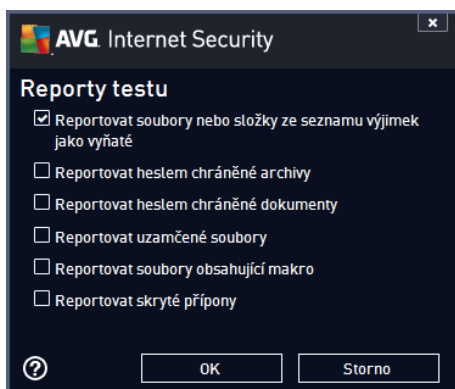
V tto sekci pak m řete nastavit pořadovanou rychlost testovn v zvislosti na zt ři systmovch zdroj .



Ve výchozím nastavení je tato hodnota nastavena *dle innosti 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.

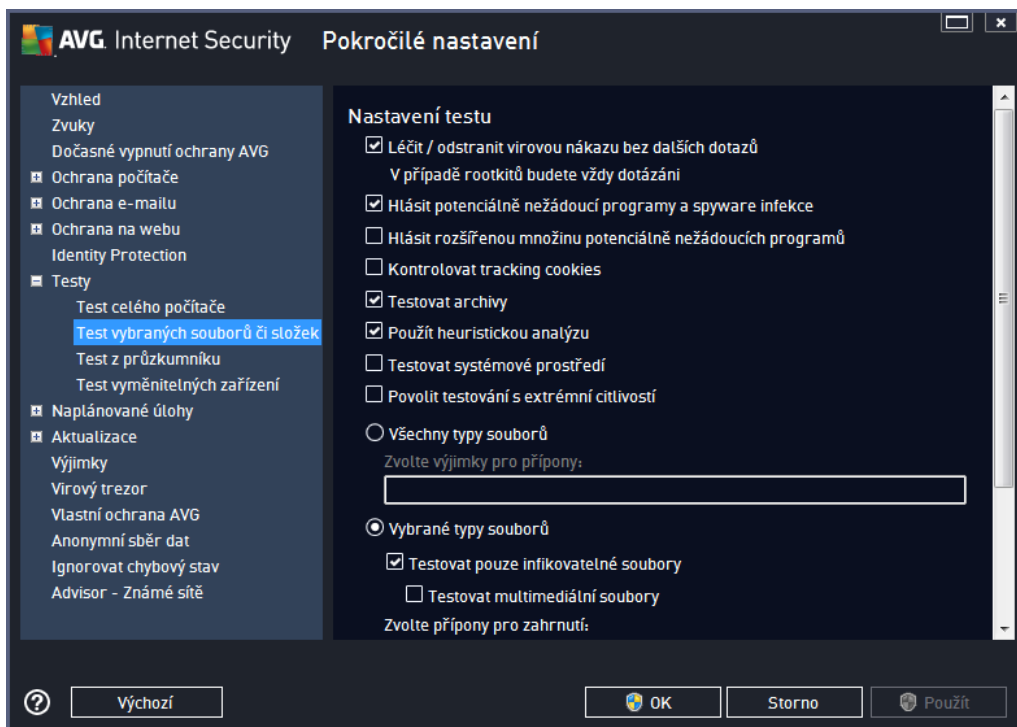
Nastavit další reporty test ...

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



9.8.2. 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:

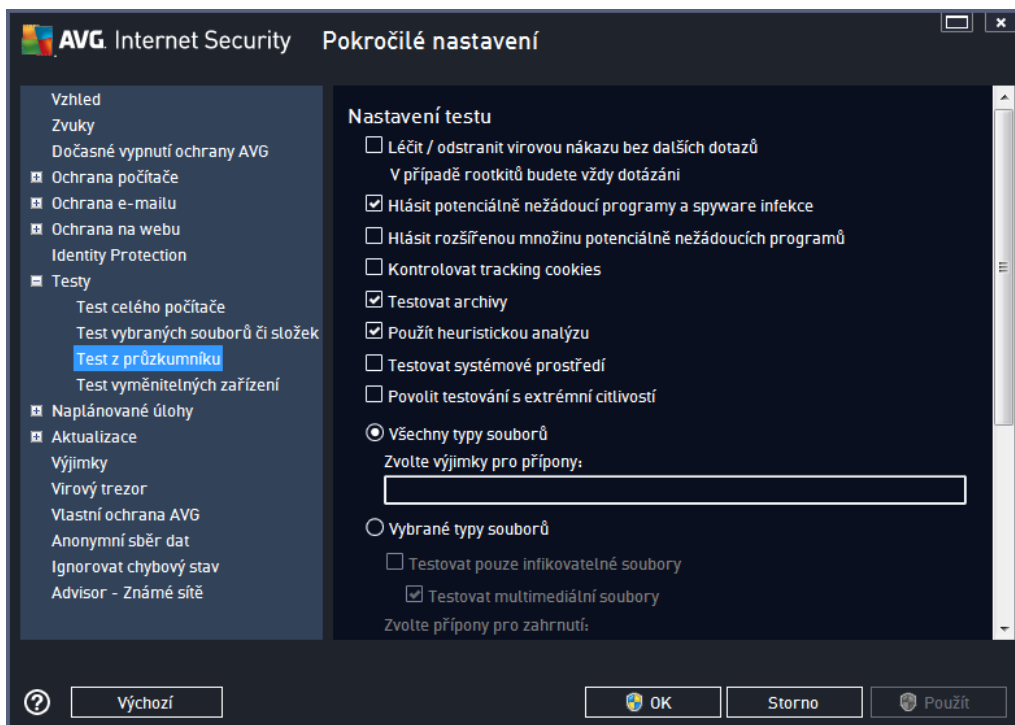


Veškeré parametry nastavené v tomto konfiguračním dialogu se vztahují pouze na ty oblasti vašeho počítače, které jste vybrali pro testování v rámci [Testu vybraných souborů či složek](#)!

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

9.8.3. 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 spuštěným nad konkrétními objekty přímo z průzkumníku Windows](#) (*Test z průzkumníku*), viz kapitola [Testování v průzkumníku Windows](#):



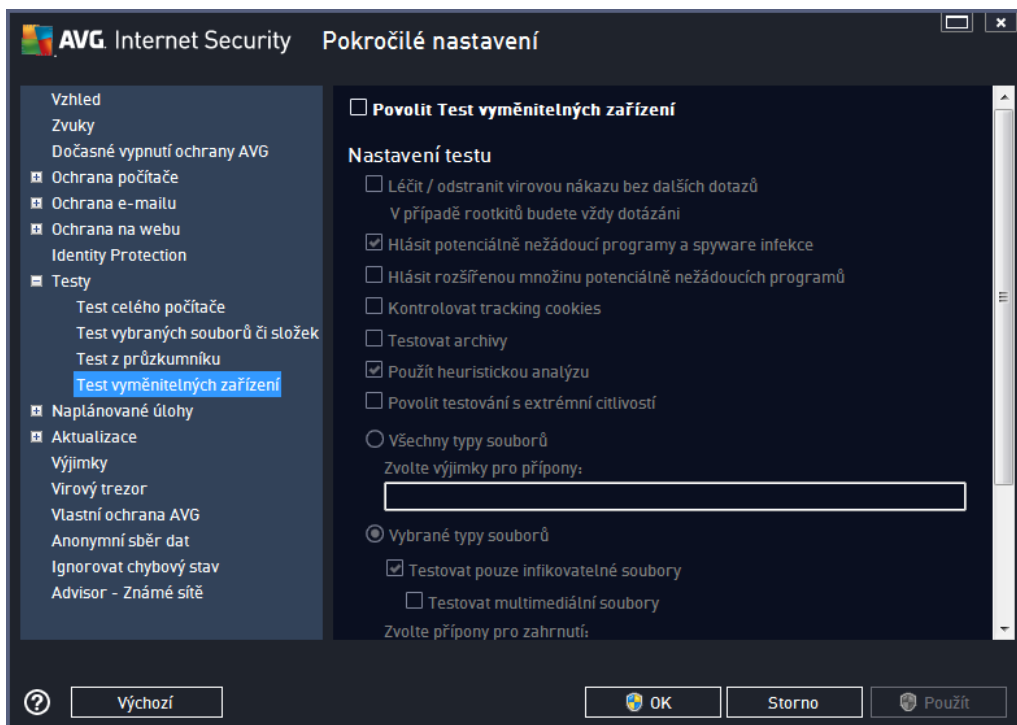
Veškeré možnosti editace parametrů testu jsou totožné s [editací parametrů Testu celého počítače](#). Odlišné je pouze výchozí nastavení těchto parametrů (například [Test celého počítače](#) ve výchozím nastavení neprovádí kontrolu archivů, ale provádí kontrolu systémového prostředí, zatímco u [Testu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

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

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

9.8.4. Test vyměnitelných zařízení

Editace 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](#).

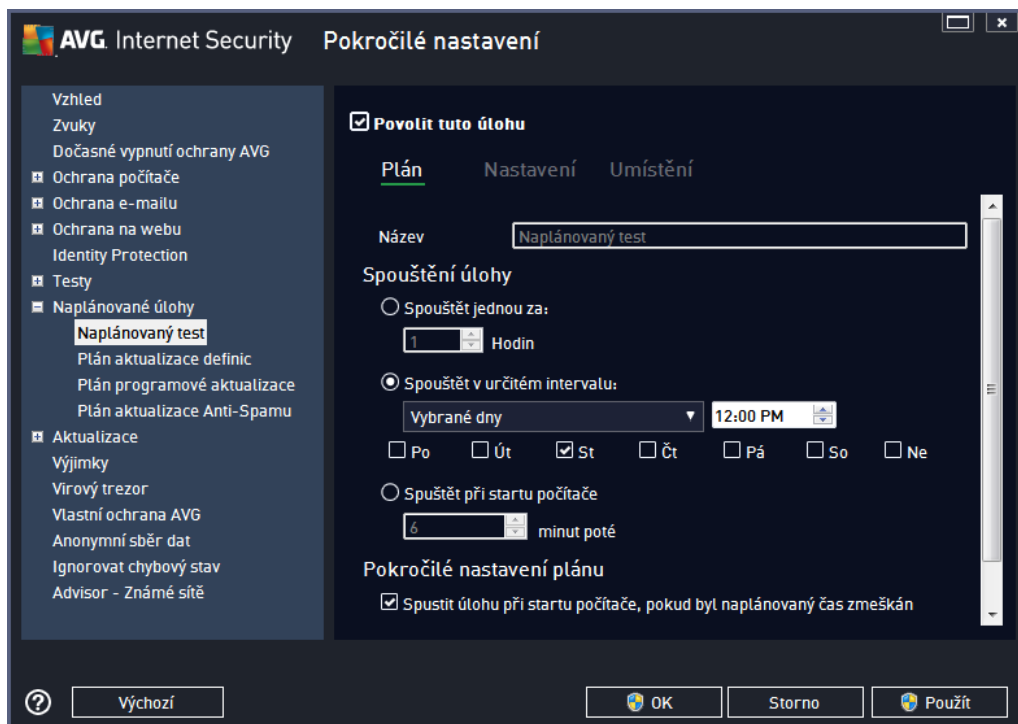
9.9. Naplánované úlohy

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

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

9.9.1. Naplánovaný test

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



V textovém poli **Název** (toto pole je u všech předem nastavených plánů deaktivováno) je uvedeno jméno příslušného nastaveného testu. U nově vytvářených plánů (nový plán vytvoříte tak, že kliknete pravým tlačítkem myši nad položkou **Naplánovaný test** v levém navigačním menu) bude textové pole aktivní a dostanete možnost definovat své vlastní pojmenování plánu. Snažte se vždy používat stručné, popisné a případně názvy, abyste se později v naplánovaných úlohách 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" - váš nastavený test bude vždy specifickým nastavením testu vybraných souborů a složek.

V tomto dialogovém okně dále definovat tyto parametry testu:

Spouštění úloh

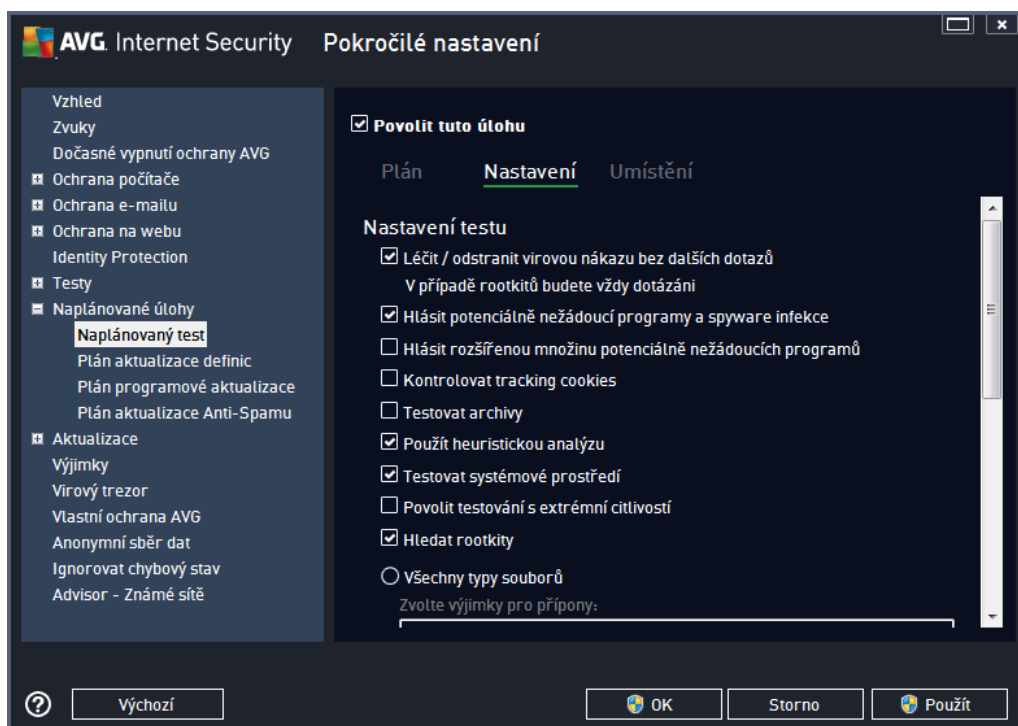
V této sekci dialogu určíte, v jakých časových intervalech má být nově naplánovaný test spuštěn. Určení můžete zadat buďto opakovaným spuštěním testu po uplynutí určité doby (**Spouštět jednou za**) nebo stanovením přesného data a času (**Spouštět v určitém intervalu**), případně určením události, na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

Pokročilé nastavení plánu

- **Spustit úlohu při startu počítače, pokud byl naplánovaný čas zmeškán** - jestliže je test naplánován na konkrétní čas, tato možnost (ve výchozím nastavení označena) zajistí, že test bude

spuštění bezprostředně po zapnutí počítače, pokud byl tento v době naplánovaného spuštění vypnutý.

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



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

- **Léčit/odstranit virovou nákazu bez dalších dotazů** (ve výchozím nastavení zapnuto): jestliže je během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. V případě, že virus automaticky léčit nelze, bude infikovaný objekt přesunut do [Virového trezoru](#).
- **Hlásit potenciálně nežádoucí 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 v domě a se souhlasem uživatele. Doporučujeme ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
- **Hlásit rozšířenou množinu potenciálně nežádoucích programů** (ve výchozím nastavení vypnuto): zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware, tj. programů, které jsou v podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.



- **Kontrolovat tracking cookies** (ve výchozím nastavení vypnuto): parametr definuje, že během testu mají být detekovány cookies (*HTTP data zaslaná serverem prohlížeči a uložena na počítači uživatele; při každé další návštěvě téhož serveru prohlížeč posílá cookies zpět serveru, který podle nich rozlišuje jednotlivé uživatele*).
- **Testovat archivy** (ve výchozím nastavení vypnuto): parametr definuje, že test má testovat všechny soubory, a to i takové, které jsou zabaleny v n kterém typu archivu, například ZIP, RAR, ...
- **Použít heuristickou analýzu** (ve výchozím nastavení zapnuto): během testu bude použita k detekci infekce i metoda heuristické analýzy (*dynamické emulace instrukcí testovaného objektu v prostředí virtuálního počítače*).
- **Testovat systémové prostředí** (ve výchozím nastavení zapnuto): test proví i systémové oblasti vašeho počítače.
- **Povolit testování s extrémní citlivostí** (ve výchozím nastavení vypnuto): ve specifických situacích (například při podezření na infekci starším typem viru) můžete zvolit tuto metodu testování, která aktivuje nejdokladnější testovací algoritmy a velmi podrobně proví naprosto všechny oblasti vašeho počítače. Můžete však na paměti, že tato metoda je asov 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 n kterých případech mohou být rootkity použity jako ovladače nebo části korektních aplikací.

Dále se můžete rozhodnout, zda si přejete testovat:

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

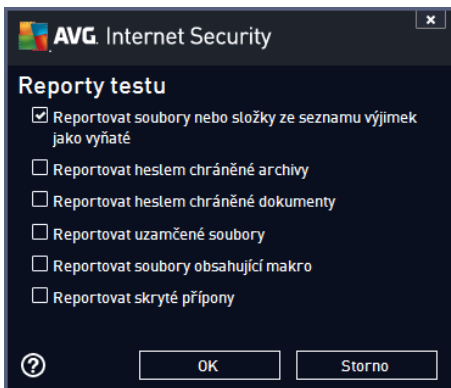
Nastavit, jak rychle probíhá test

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



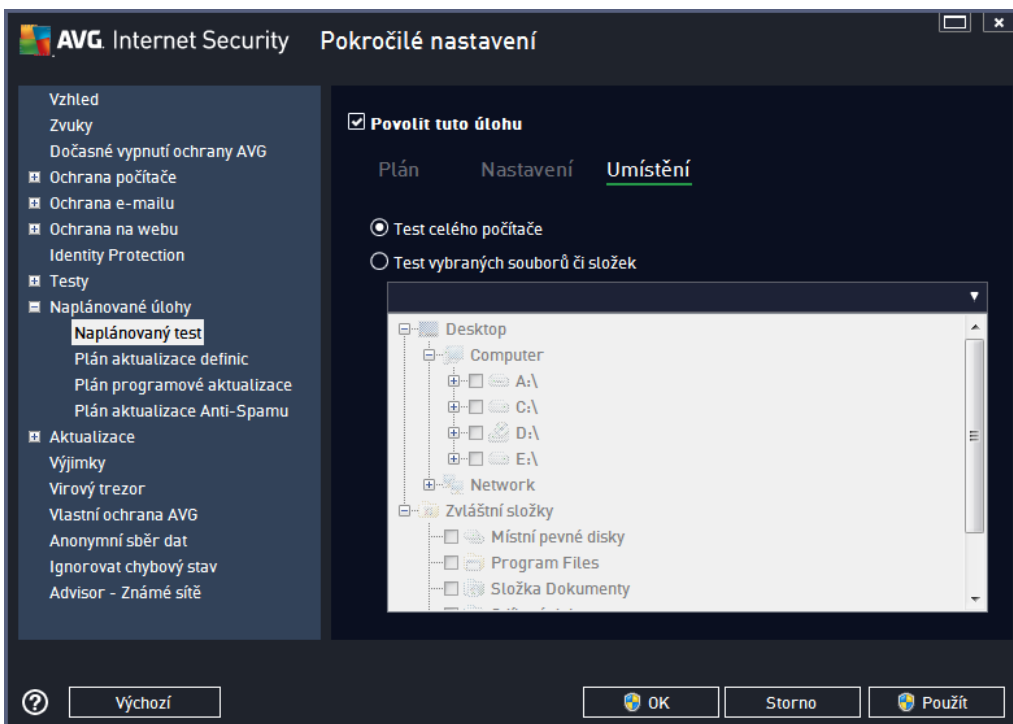
Nastavit další reporty test

Kliknutím na odkaz **Nastavit další reporty test ...** otevřete samostatné dialogové okno **Reporty testu**, v němž můžete označím 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 spuštění testu počítač automaticky vypnut. Pokud potvrdíte tuto volbu (**Vypnout počítač po dokončení testování**), aktivuje se související další možnost, jejímž zapnutím vynutíte vypnutí počítače i za situace, že počítač bude ve chvíli dokončení testu zamčen (**Vynutit vypnutí počítače, pokud je uzamčen**).



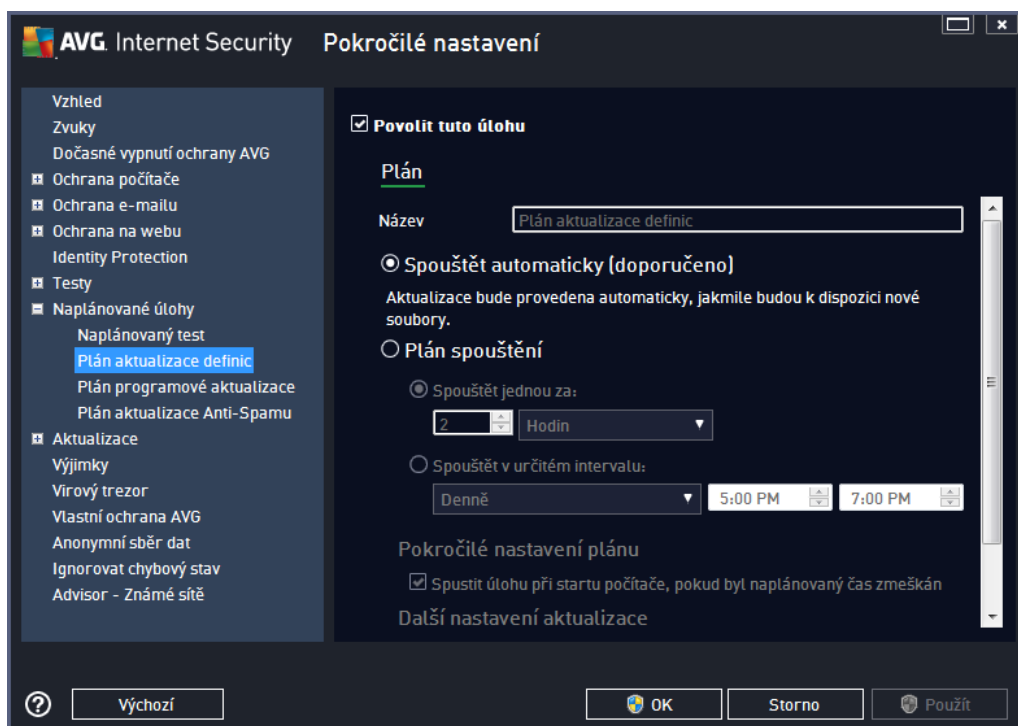
Na záložce **Umístění** definujete, zda si plánujete naplánovat [Test celého počítače](#) nebo [Test vybraných souborů](#)



[i 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.

9.9.2. Plán aktualizace definic

V případě **skutečně nutné** 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 úloh

Ve výchozím nastavení je úloha spouštěna automaticky (**Spouštět automaticky**) vždy, jakmile je k dispozici nová aktualizace. Doporučujeme toto nastavení aplikace ponechat. Pouze máte-li skutečně důvod nastavit kontrolu aktualizací definic virové databáze jinak, můžete tak učinit v osobním nastavení. Určete, v jakých časových intervalech má být nově naplánovaná aktualizace definic provedena. Časové určení můžete zadat buďto opakovaným spuštěním aktualizace po uplynutí určité doby (**Spouštět jednou za**) nebo stanovením přesného data a času (**Spouštět v určitém intervalu**).

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.

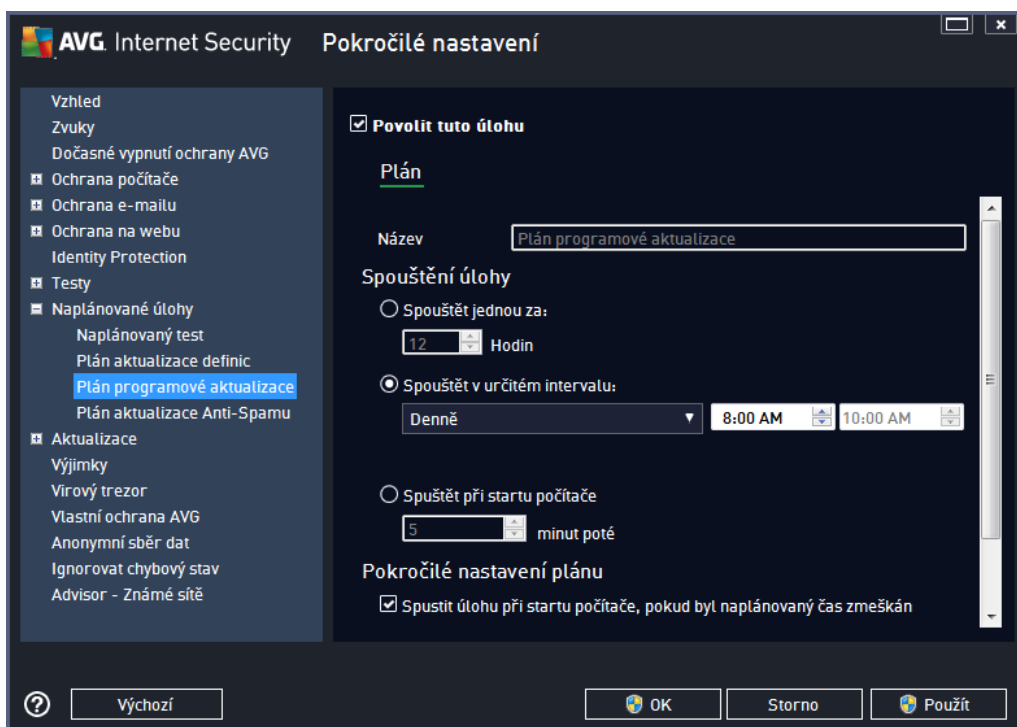


Další nastavení aktualizace

Volbou položky **Provést aktualizaci znovu po p ipojení k Internetu** zajistíte, že pokud dojde b hem aktualizace definic k problém m s p ipojením a aktualizace tedy nebude moci být dokon ena, bude znovu spušt na bezprost edn po obnovení p ipojení. O automatickém spušt ní aktualizace budete v ur eném ase informováni prost ednictvím pop-up okna nad [ikonou AVG na systémové lišt](#) (za p edpokladu, že ponecháte zapnutou volbu **Zobrazovat oznámení na systémové lišt** v [Pokro ilém nastavení/Vzhled](#)).

9.9.3. Plán programové aktualizace

V p ípad **skute n nutné** pot eby m žete prostým vypnutím položky **Povolit tuto úlohu** naplánovanou programovou aktualizaci (do asn) deaktivovat, a pozd ji znovu zapnout:



V textovém poli **Název** (toto pole je u všech p edem nastavených plán deaktivováno) je uvedeno jméno p íazené práv nastavenému plánu programové aktualizace.

Spoušt ní úlohy

Ur ete, v jakých asových intervalech má být nov naplánovaná programové aktualizace provedena. asové ur ení m žete zadat bu to opakovaným spušt ní m aktualizace po uplynutí ur ené doby (**Spoušt t jednou za**) nebo stanovením p esného data a asu (**Spoušt t v ur itém intervalu**), p ípadn ur ením události, na niž se spušt ní aktualizace váže (**Spoušt t p i startu po íta e**).

Pokro ilé nastavení plánu

Tato sekce umož ũje definovat podmínky, kdy má í nemá být programové aktualizace spušt na, jestliže je



pořít v úsporném režimu nebo zcela vypnutý a naplánovaný čas spuštění aktualizace byl zmeškán.

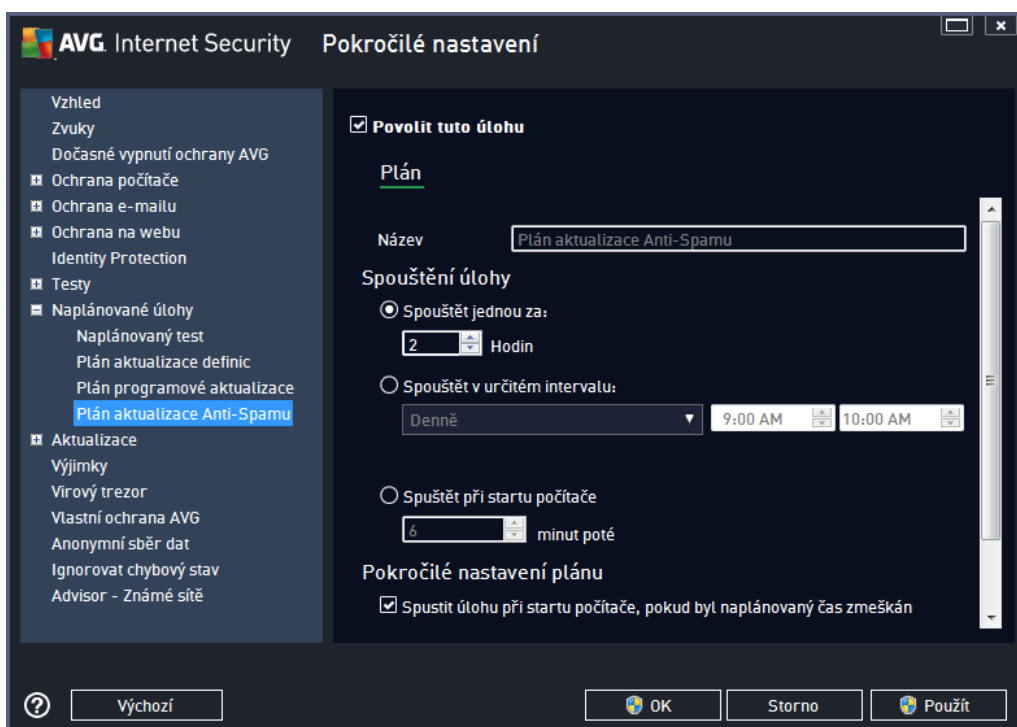
Další nastavení aktualizace

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 soubohu naplánované programové aktualizace a naplánovaného testu, proces aktualizace je považován za prioritní a test bude přerušeno. O případné kolizi budete informováni.

9.9.4. Plán aktualizace Anti-Spamu

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



V tomto dialogu můžete nastavit přesnější parametry plánu aktualizace. V textovém poli **Název** (toto pole je u všech přednastavených plánů deaktivováno) je uvedeno jméno přednastavenému plánu aktualizace 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 určité doby (**Spouštět jednou**



za) nebo stanovením přesného data a času (**Spouštět v určeném intervalu**), případně určením události, na niž se spustí aktualizace Anti-Spamu váže (**Spouštět po i startu počítače**).

Pokročilé nastavení plánu

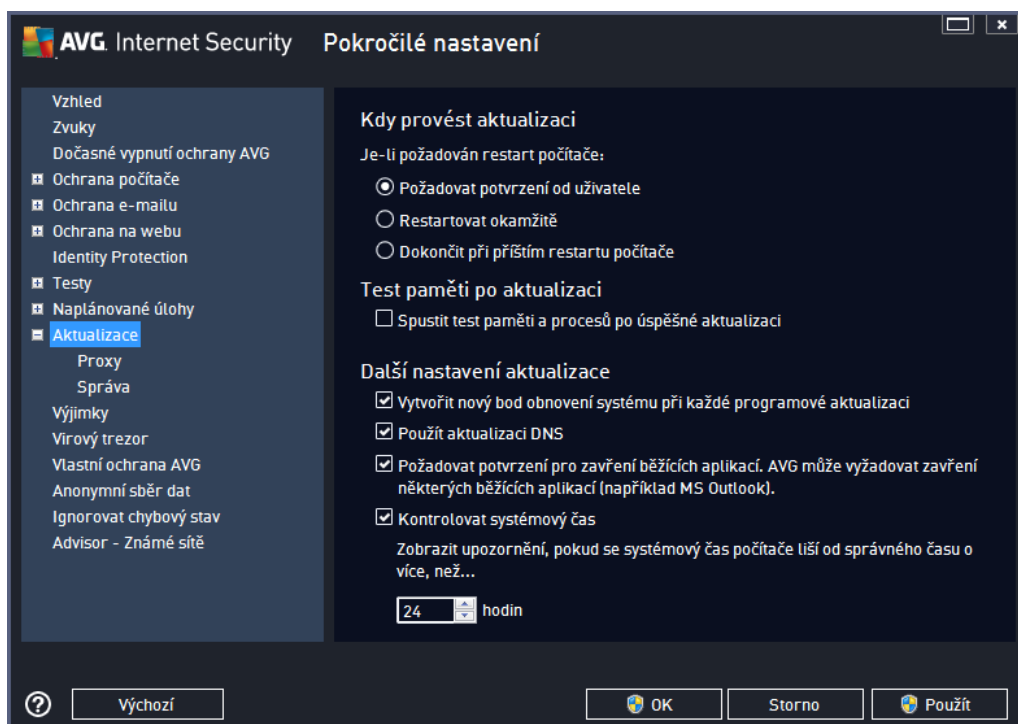
Tato sekce umožňuje definovat podmínky, kdy má či nemá být aktualizace Anti-Spamu spuštěna, jestliže je počítač v úsporném režimu nebo zcela vypnutý a naplánovaný čas spuštění aktualizace byl zmeškán.

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](#)).

9.10. 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

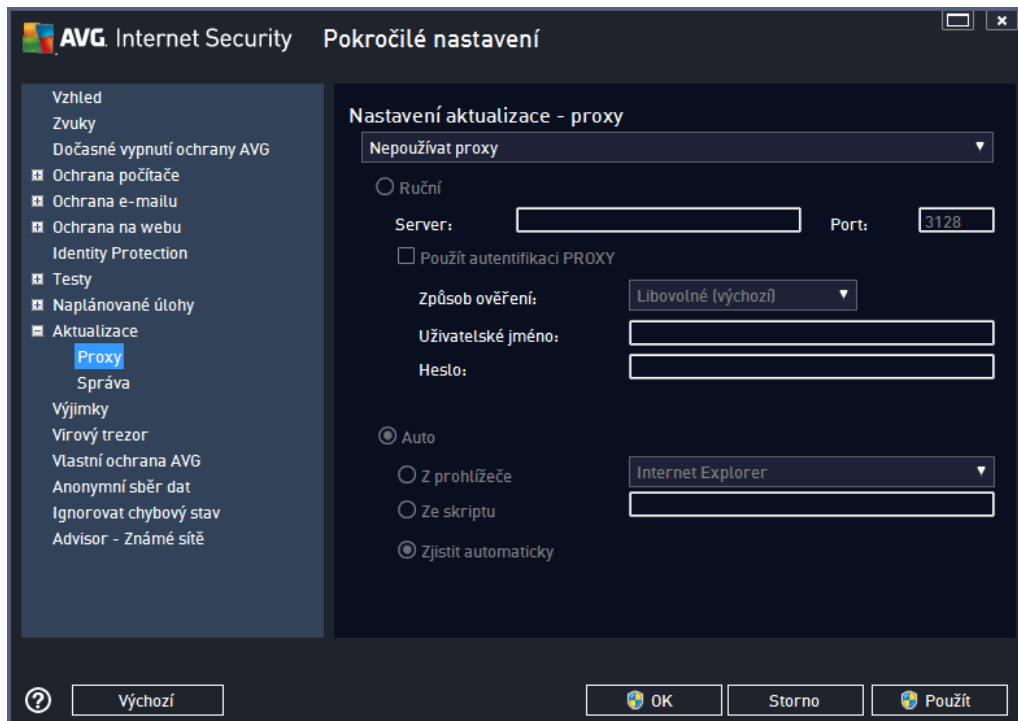
Označíte-li tuto položku, bude po každé úspěšné dokončené aktualizaci spuštěn test paměti. V případě, že by nejnovější aktualizace obsahovala nové virové definice, budou tak tyto okamžitě aplikovány během testu.

Další nastavení aktualizace

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

- **Vytvořit nový bod pro obnovení systému při každé programové aktualizaci (ve výchozím nastavení zapnuto)** - před každým spuštěním programové aktualizace AVG je vytvořen takzvaný systémový bod pro obnovení systému. V případě, že aktualizací proces nebude z nějakého důvodu dokončen a váš operační systém bude ohrožen, můžete za pomoci tohoto zálohovacího bodu obnovit OS v jeho původní konfiguraci. Tato možnost je dostupná přes volbu *Start / Všechny programy / Podpora / Systémové nástroje / Obnova systému*, ale jakékoliv zásahy do tohoto nastavení lze doporučit výhradně pokročilým a zkušeným uživatelům! Chcete-li využít této možnosti, ponechte políčko označené.
- **Použít aktualizaci DNS (ve výchozím nastavení zapnuto)** - pokud je tato položka označena, při spuštění aktualizace **AVG Internet Security 2014** vyhledá na DNS serveru informaci o aktuální verzi virové databáze a aktuální verzi programu a následně stáhne pouze nejmenší nezbytně nutné aktualizací soubory. Tím se sníží celkový objem stahovaných dat a urychlí proces aktualizace.
- **Požadovat potvrzení pro zavření běžících aplikací (ve výchozím nastavení zapnuto)** zajistíte, že v případě, že bude nutné zavřít některé spuštěné aplikace, aby mohla být aktualizace dokončena, budete před jejich zavřením upozorněni varovným hlášením.
- **Zkontrolovat systémový čas (ve výchozím nastavení zapnuto)** - označením této položky určíte, že si přejete, abyste byli informováni o případném rozporu mezi časem nastaveným na počítači a skutečným časem, a to v okamžiku, kdy rozdíl těchto dvou časů dosáhne stanoveného počtu hodin.

9.10.1. Proxy



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

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

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

Ruční nastavení

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

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

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

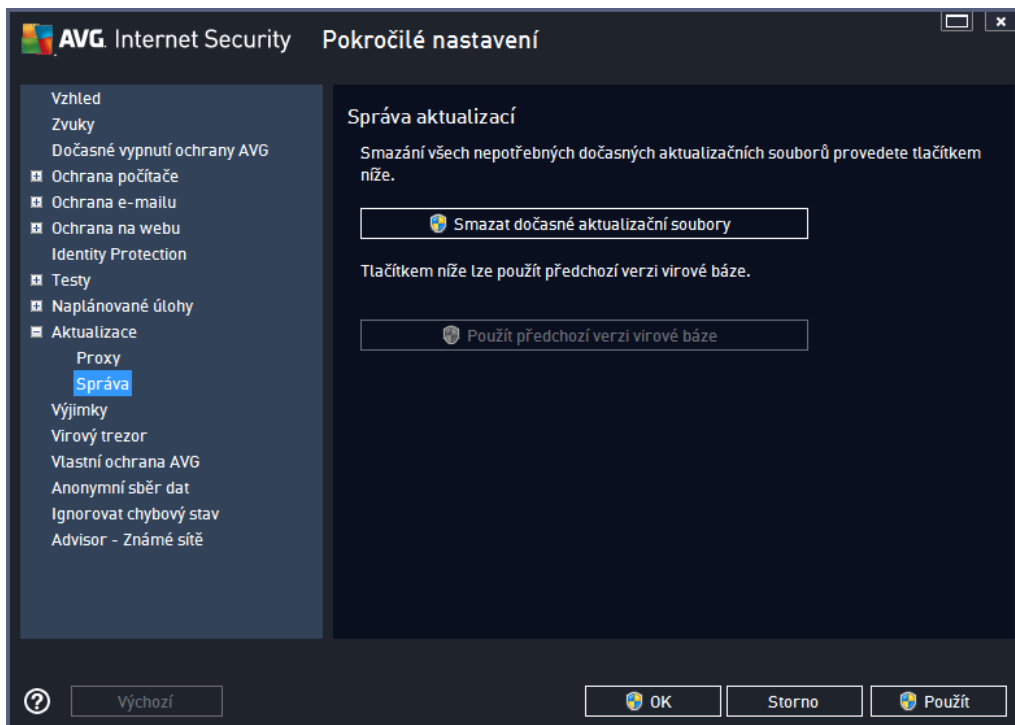
Automatické nastavení

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

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

9.10.2. Správa

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



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

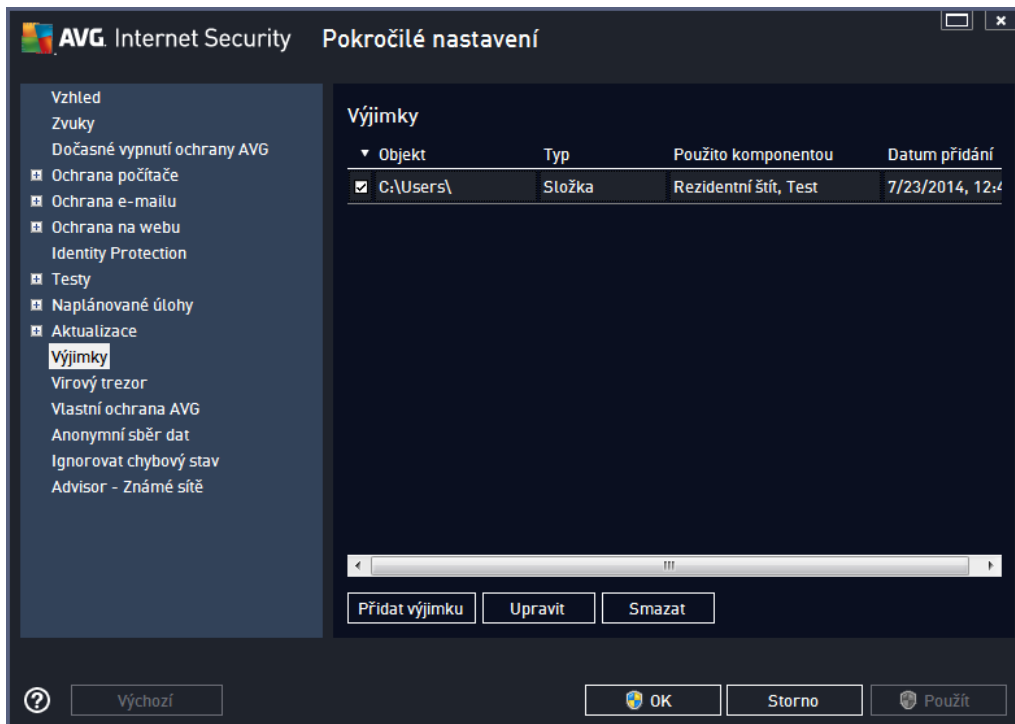
9.11. Výjimky

V dialogu **Výjimky** můžete definovat výjimky, to jest položky, které budou z kontroly programem **AVG Internet Security 2014** vyjaty. Výjimku můžete definovat například v situaci, kdy AVG opakovaně detekuje určitý program nebo soubor jako hrozbu nebo blokuje webovou stránku, o níž bezpochybně 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 a webové stránky, které lze s naprostou jistotou označit za bezpečné!



Tabulka v dialogu zobrazuje seznam již definovaných výjimek. Každá položka má vedle sebe zaškrtačací 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 editovat podle jednotlivých parametrů, a to tak, že kliknete na záhlaví sloupce, jehož charakteristiku chcete použít jako kritérium zařazení položek.

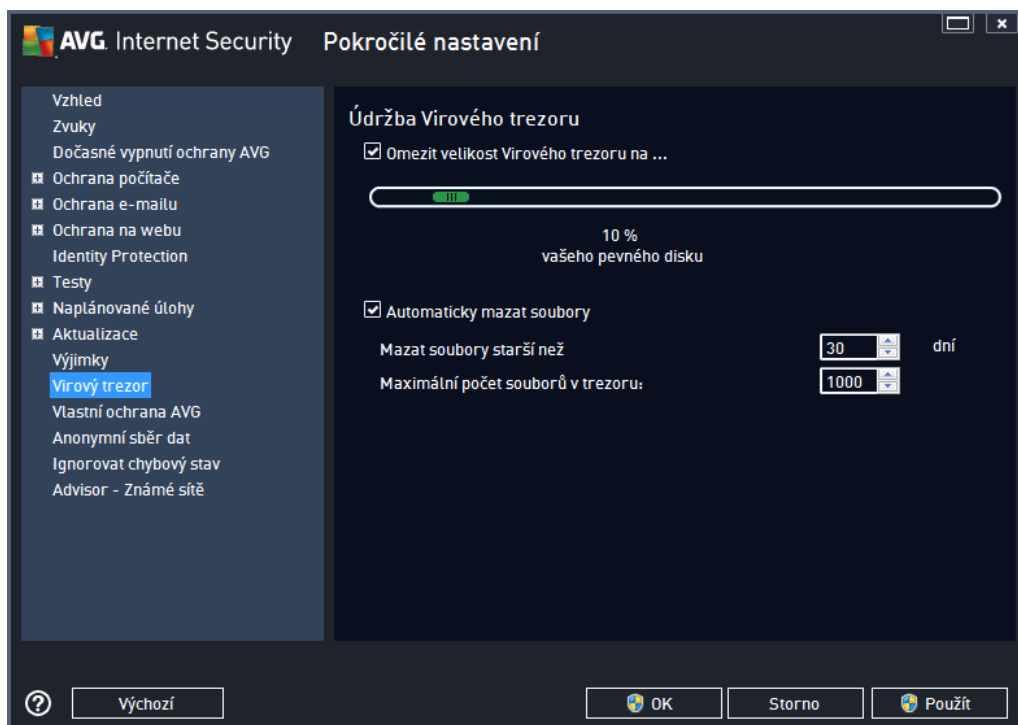
Ovládací prvky dialogu

- **Přidat výjimku** - Kliknutím na tlačítko otevřete nový dialog, v němž lze specifikovat objekty, jež mají být vyňaty z kontroly programem AVG. Nejprve musíte určit, o jaký typ objektu se jedná: zda jde o soubor, adresář, nebo o webovou stránku. Pak prohlížením disku určíte přesnou cestu k danému objektu nebo zadáte konkrétní URL. Nakonec budete vyzváni, abyste rozhodli, které bezpečnostní služby AVG mají definovaný objekt vynechat ze své kontroly (*Rezidentní štít, Identity Protection, Test*).
- **Upravit** - Tlačítko je aktivní, pouze pokud jsou již definovány a v seznamu uvedeny nějaké výjimky. Stiskem tlačítka pak otevřete editační dialog, v němž můžete upravovat nastavené parametry zvolené výjimky.
- **Smazat** - Tlačítkem lze smazat dříve definované výjimky ze seznamu. Výjimky můžete buďto odstranit jednu po druhé nebo označit v seznamu celý blok výjimek a smazat je jednorázově. Po



smazání definované výjimky bude objekt, jehož se výjimka týkala, opět považován za předmět kontroly AVG. Odstraněním výjimky nemažete ten který soubor nebo adresář, ale pouze nastavení pravidel pro tento objekt!

9.12. Virový trezor

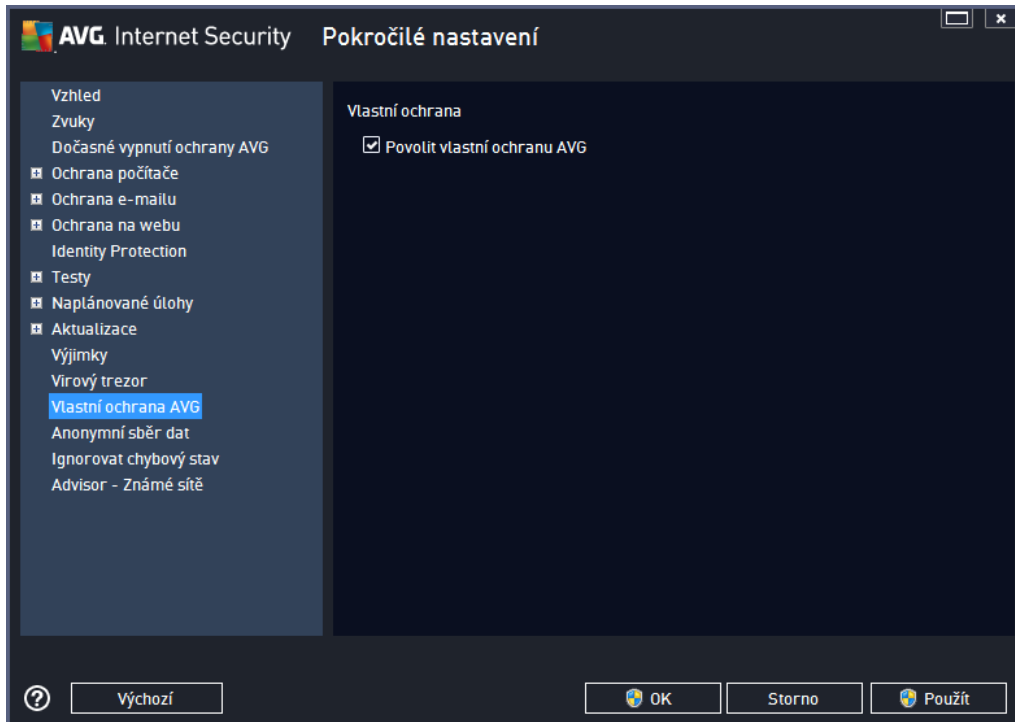


Dialog **Údržba Virového trezoru** umožňuje definovat několik parametrů souvisejících se správou objektů ve [Virovém trezoru](#):

- **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 níž se mají uchovávat soubory ve [Virovém trezoru](#) (**Mazat soubory starší než ... dní**), a maximální počet souborů uložených ve [Virovém trezoru](#) (**Maximální počet souborů v trezoru**).



9.13. Vlastní ochrana AVG

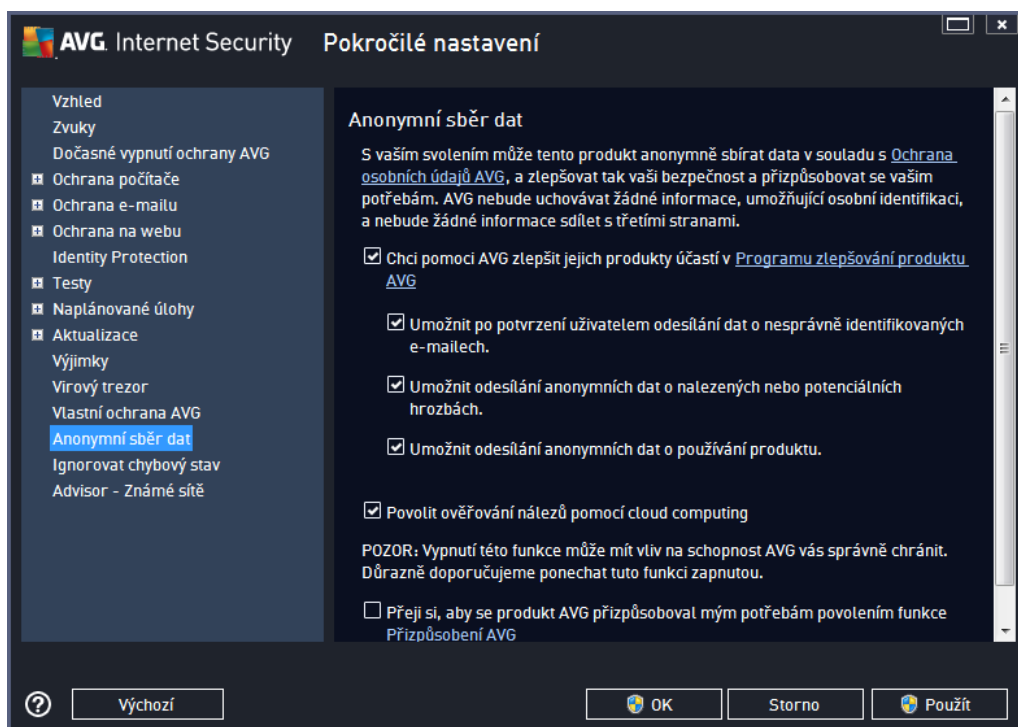


Funkce **Vlastní ochrana AVG** slouží k nastavení ochrany vlastních procesů, souborů, registrových klíčů a ovladačů aplikace **AVG Internet Security 2014** před jejich pozmeněním i deaktivací. Důvodem implementace tohoto typu ochrany je existence sofistikovaných hrozeb, které se snaží zneškodnit antivirové programy a následně bez omezení poškodit váš počítač.

Doporuujeme, abyste tuto funkci nechali vždy zapnutou.

9.14. 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 nejnovější 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:

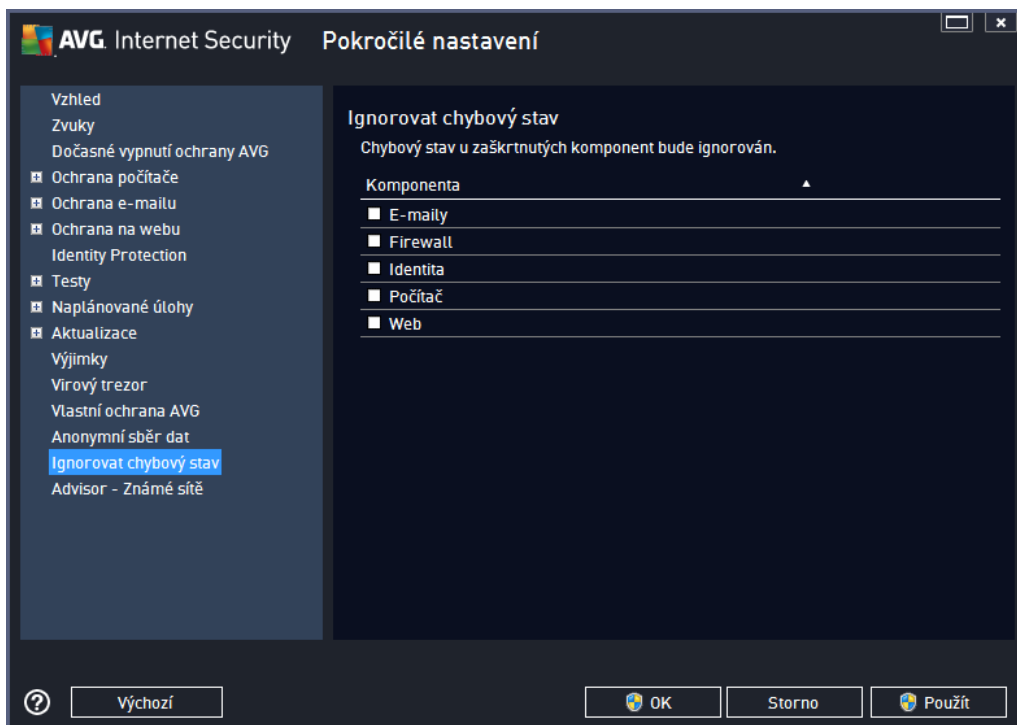
- **Chci pomoci AVG zlepšit jejich produkty účastí v Programu zlepšování produktu AVG** (ve výchozím nastavení zapnuto) - Chcete-li nám pomoci dále zlepšovat program AVG, ponechte toto políčko označené. Tím povolíte odesílání informací o všech hrozbách, na které eventuálně narazíte při surfování po Internetu; 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 například počet nalezených infekcí, probíhání 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).
- **Přejí si, aby se produkt AVG přizpůsoboval mým potřebám povolením funkce Přizpůsobení AVG** (ve výchozím nastavení vypnuto) - tato funkce anonymně analyzuje chování programu 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.

9.15. Ignorovat chybový stav

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



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

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

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

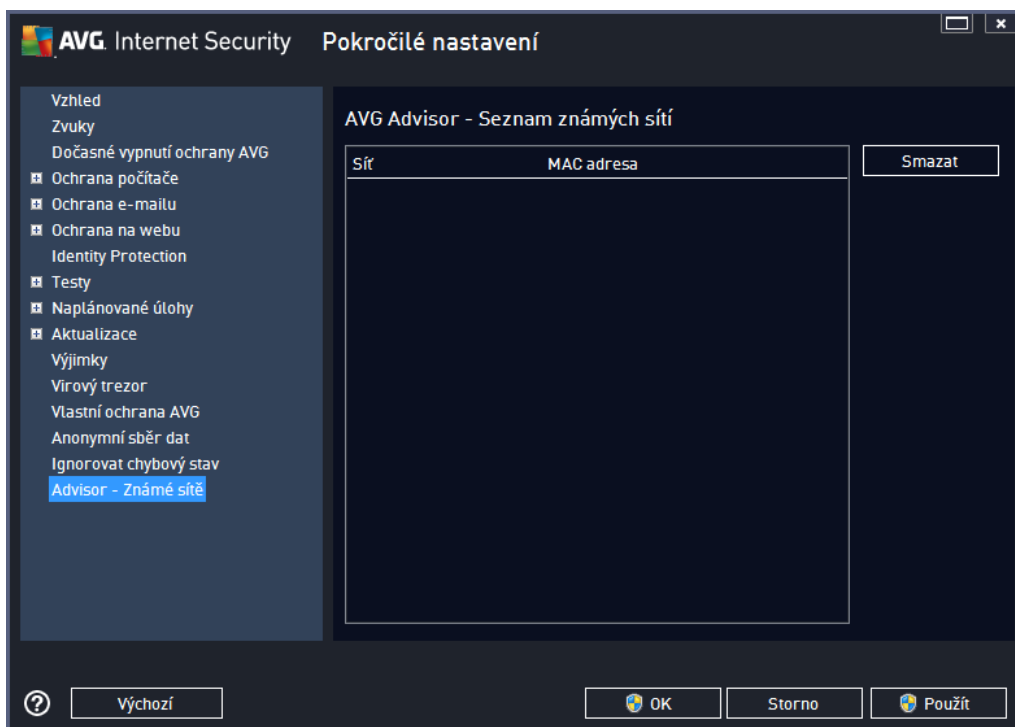
V dialogu **Ignorovat chybový stav** máte tedy možnost označit ty komponenty, jejichž případný chybový stav (to znamená i jejich vypnutí) nemá být hlášen. Můžete označit libovolnou komponentu nebo i několik komponent v seznamu. Svou volbu potvrdíte stiskem tlačítka **OK**.



9.16. Advisor - známé sítě

Služba [AVG Advisor](#) obsahuje funkci, která sleduje síť, do níž se připojíte. Pokud objeví síť dosud nepoužitou (avšak s názvem, který používá některá ze známých sítí, což může být matoucí), upozorní vás na to a doporučí, abyste si síť prověřili. Pokud usoudíte, že síť je bezpečná, můžete ji uložit do tohoto seznamu (prostřednictvím odkazu v informačním dialogu AVG Advisoru, který se vysune nad systémovou lištou při detekci neznámé sítě - podrobný popis najdete v kapitole [AVG Advisor](#)). [AVG Advisor](#) si zapamatuje jediné identifikační údaje sítě, zejména adresu MAC, a přístupu už vás nebude upozorňovat. Každá síť, k níž se připojíte, bude pro přístupu 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.



10. Nastavení Firewallu

Konfigurace [Firewallu](#) se otevírá v samostatném okně, kde můžete na několika dialogových nastavitelných parametrech 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](#)

10.1. Obecné

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

Máte prosím na paměti, že všechny komponenty AVG Internet Security 2014 jsou výrobcem nastaveny k optimálnímu výkonu. Pokud nemáte skutečný důvod jejich konfiguraci změnit, 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, například 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. Při 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 při jejím připojení. Firewall se v automatickém režimu chová zcela nenápadně. **Volbu automatického režimu doporučujeme v tšim uživatel.**
- **Interaktivní režim** - Pro interaktivní režim se rozhodnete 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, při němž 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 přebít 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 omezení částečně kompenzuje sníženou ochranu vašeho počítače při vypnutí



jiné komponenty.

10.2. 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 2014. Ve chvíli, kdy se nová aplikace poprvé pokusí navázat síťovou komunikaci, bude buď vytvořeno pravidlo podle dříve v rozhodné databázi, anebo budete vyzváni k nastavení pravidla; pak bude třeba rozhodnout, zda má být komunikace této aplikace povolena nebo blokována. Svou volbu můžete uložit jako trvalé pravidlo (které bude následně uvedeno v seznamu v tomto dialogu).

Samozřejmě je také možné definovat pravidla pro nové aplikace okamžitě - stisknete tlačítko **Přidat** v tomto dialogu a vyplíte údaje o aplikaci.

Kromě aplikací obsahuje seznam ještě dvě speciální položky. **Přednostní pravidla aplikací** (první řádek seznamu) jsou preferenční pravidla a jsou uplatňována 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.

10.3. Sdílené soubory a tiskárny

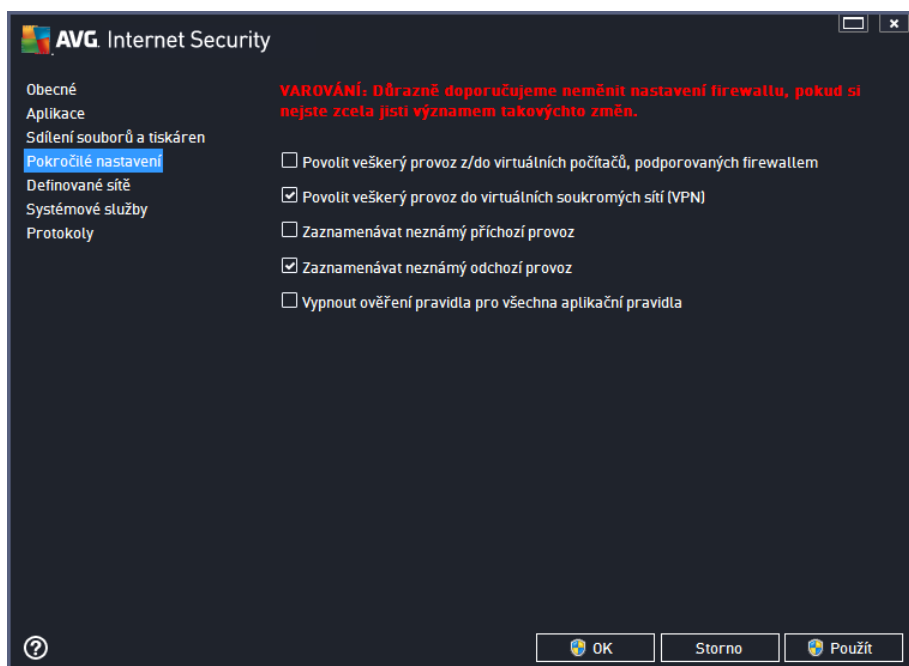
Sdílení souborů a tiskáren v podstatě znamená sdílení společných diskových jednotek, tiskáren, skenerů a podobných zařízení, i jakýchkoliv souborů nebo adresářů, které ve Windows označíte jako "sdílené". Sdílení těchto zdrojů je vhodné pouze v sítích, které považujete za skutečně bezpečné (například 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 Windows XP jsou sítě uvedeny pod názvem, který si zvolil uživatel v době prvního připojení k síti. U operačních systémů Windows Vista a vyšších se název sítě vybírá z Centra síťových připojení a sdílení.

10.4. Pokročilé nastavení

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



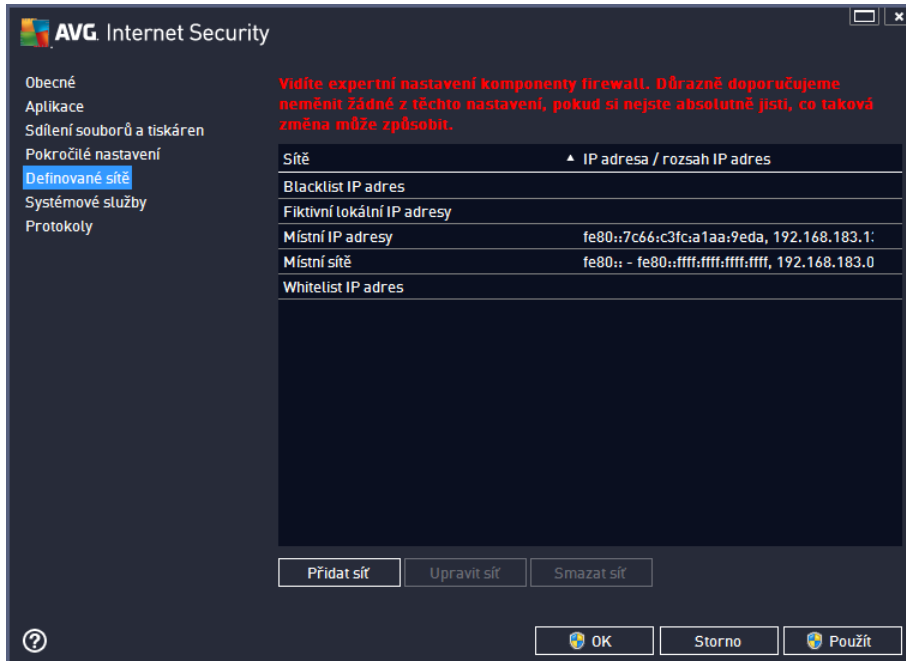
Dialog **Pokročilé nastavení** vám umožní zapnout i vypnout následující parametry Firewallu:

- **Povolit veškerý provoz z/do virtuálních počítačů, podporovaných firewallem** - podpora síťového spojení k virtuálním počítačům, například VMware.
- **Povolit veškerý provoz do virtuálních soukromých sítí (VPN)** - podpora VPN při spojení (vzdálené spojení k počítači).
- **Zaznamenávat neznámý příchozí/odchozí provoz** - veškeré pokusy neznámých aplikací o komunikaci (smeřovat dolů / ven) budou zaznamenány v [protokolu Firewallu](#).
- **Vypnout ověření pravidla pro všechna aplikační pravidla** - Firewall pravidelně kontroluje všechny soubory, k nimž byla vytvořena aplikační pravidla. Pokud zaznamená změnu v binárním souboru, Firewall se pokusí znovu potvrdit důvěryhodnost aplikace standardním způsobem, tedy například ověřením certifikátu aplikace, vyhledáním aplikace v [důvěryhodné databázi](#) apod. Jestliže aplikaci nelze ani poté považovat za zcela bezpečnou, Firewall dále postupuje podle toho, v jakém [režimu](#) běží:
 - je-li Firewall spuštěn v [Automatickém režimu](#), bude aplikace ve výchozím nastavení povolena;
 - je-li Firewall spuštěn v [Interaktivním režimu](#), bude aplikace zablokována a uživatel prostřednictvím dotazovacího dialogu vyzván, aby rozhodl, zda aplikaci nadále povolit i blokovat.

Pro jednotlivá aplikační pravidla lze samozřejmě nastavit postup i jednotlivě, a to v dialogu [Aplikace](#).

10.5. Definované sítě

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

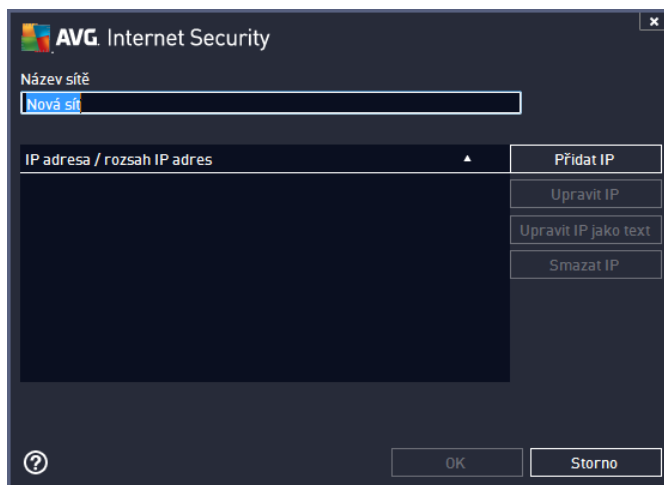


Dialog **Definované sítě** nabízí seznam všech sítí, k nimž je váš počítač připojen. O detekovaných sítích jsou v seznamu k dispozici tyto informace:

- **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 rozptí 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 něm 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.

10.6. Systémové služby

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



Dialog **Systémové služby a protokoly** uvádí pohled standardních systémových služeb Windows a protokolů, které mohou komunikovat po síti, a pohled ikon z názorů jednotlivých akcí. Tabulka obsahuje tyto sloupce:



- **Systémové služby a protokoly** - V tomto sloupci jsou zobrazena jména příslušných systémových služeb.
- **Akce** - Sloupec zobrazuje ikony příslušné konkrétní akci:
 - Povolit komunikaci pro všechny sítě
 - Blokovat komunikaci

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

Uživatelsky definovaná systémová pravidla

Chcete-li vytvořit vlastní systémové pravidlo, použijte tlačítko **Spravit 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**.



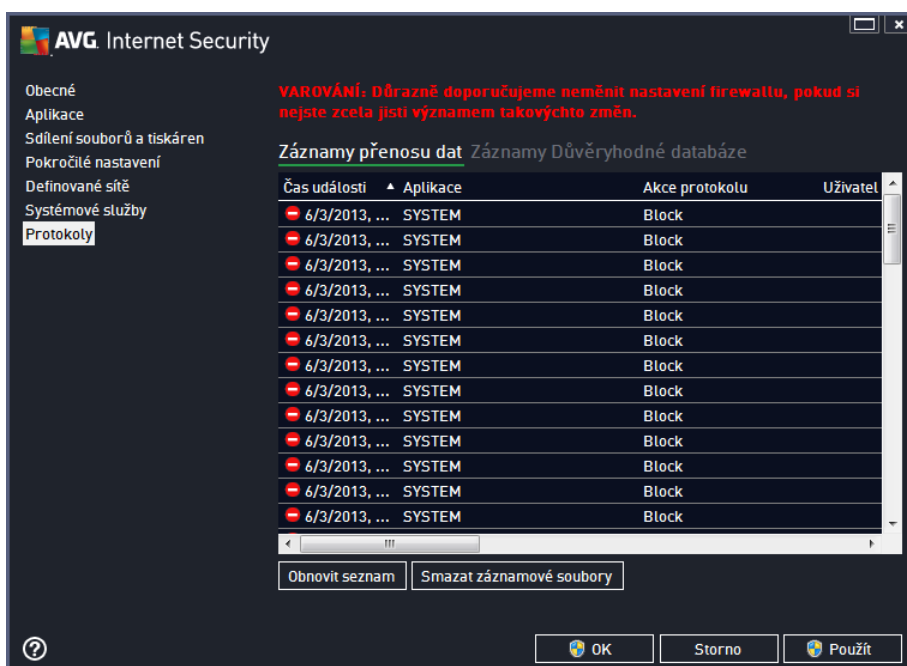
Nastavení systémových pravidel je velmi pokročilé a je určeno zejména správcům sítí, kteří potřebují plnou kontrolu nad konfigurací Firewallu do nejmenších podrobností. Pokud nejste obeznámeni s typy komunikací, protokoly, čísly síťových portů, definicemi IP adres atd., prosíme, nemějte toto nastavení!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

10.7. Protokoly

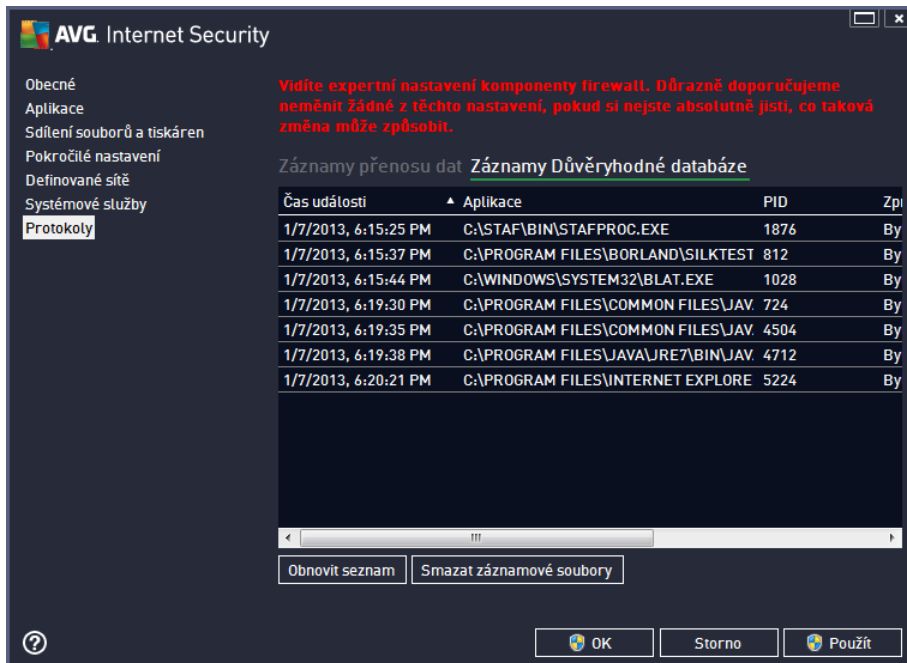
Veškeré editace v dialogu Protokoly jsou určeny VÝHRADNĚ ZKUŠENÝM UŽIVATELŮM!

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

- **Záznamy p enosu dat** - Záložka nabízí informace o veškeré aktivit aplikací, které se jakýkoliv zp sobem pokusily o navázání sí ové komunikace. U každého záznamu najdete údaje o ase události, jméno aplikace, která se pokoušela navázat spojení, p íslušnou akci protokolu, jméno uživatele, PID, sm r p ipojení, typ protokolu, íslo vzdáleného a místního portu a informaci o vzdálené i lokální IP adrese.



- **Záznamy D v ryhodné databáze** - D v ryhodná databáze je interní databází AVG, v níž jsou shromážděny informace o aplikacích, které mají ověný certifikát, jsou prověněné a d v ryhodné, a komunikace jim může být povolena. Při prvním pokusu jakékoliv aplikace o navázání sí ové 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 D v ryhodnou 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 můžete komunikaci povolit.




Ovládací tlačítka

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

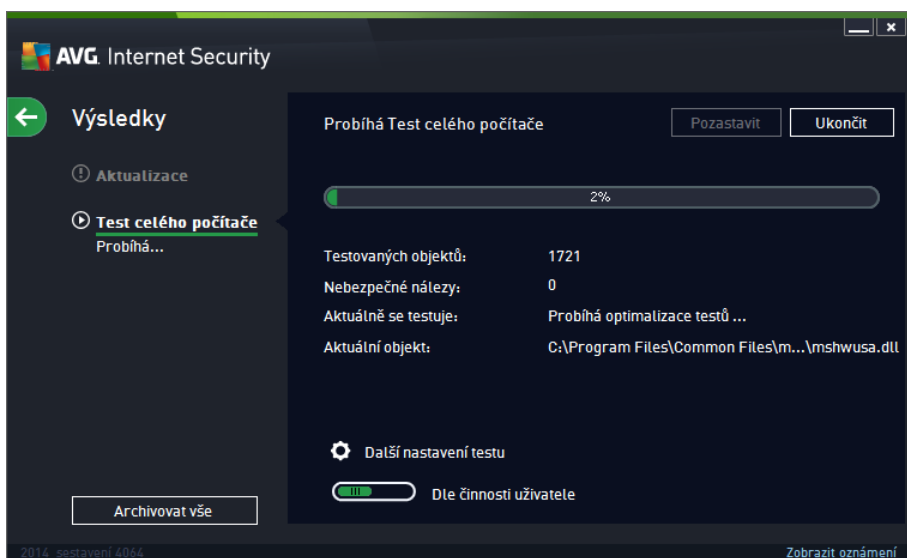
11. AVG testování

Ve výchozím nastavení **AVG Internet Security 2014** se nespouští žádný test automaticky, protože po úvodním otestování počítače (*k jehož spuštění budete vyzváni*) jste pro běžnou ochranu rezidentními komponentami **AVG Internet Security 2014**, které eventuální škodlivý kód zachycují okamžitě. Samozřejmě můžete [naplánovat test](#) k pravidelnému spuštění v určených čas, případně kdykoli spustit ručně libovolný test podle vlastních požadavků.

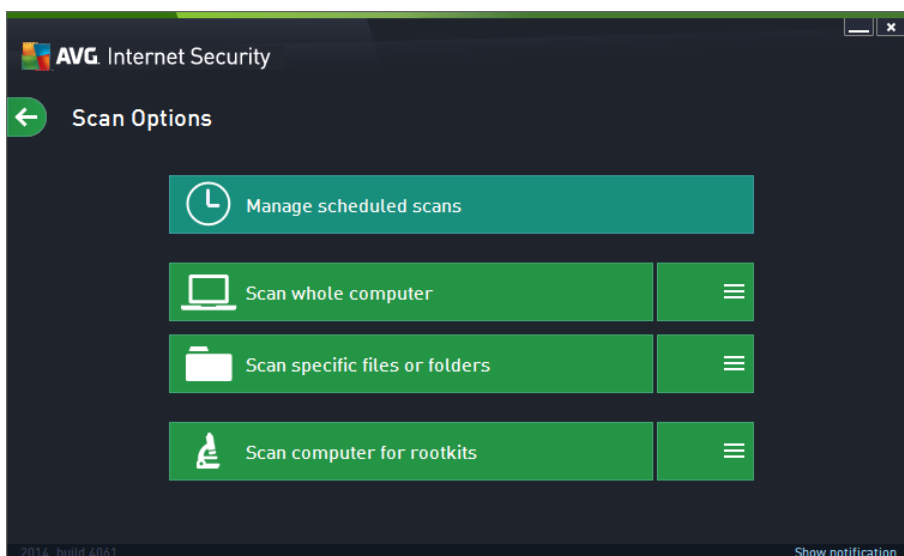
Testovací rozhraní AVG je dostupné z [hlavního uživatelského rozhraní](#) prostřednictvím tlačítka sestávajícího ze

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 znázorněná 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 i složek](#):



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

- **Upravit naplánované testy** - Volbou této možnosti otevřete nový [dialog s pohledem všech naplánovaných testů](#). Dokud nenaplánujete vlastní testy, bude v tabulkovém pohledu 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. Kliknutí 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 a složek / Nastavení** - Toto tlačítko je rozděleno do dvou částí. Kliknutí na volbu *Test vybraných souborů a 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 a složek](#).
- **Prohledat počítač na přítomnost rootkitů / Nastavení** - První část tlačítka označená textem *Prohledat počítač na přítomnost rootkitů* spustí rootkit testování (*podrobnosti o rootkit testu najdete v příslušné kapitole nazvané [Přednastavené testy / Prohledat počítač na přítomnost rootkitů](#)*). Kliknutím na položku *Nastavení* přejdete do [konfiguračního dialogu Nastavení Anti-Rootkitu](#).

11.1. Přednastavené testy

Jednou z hlavních funkcí **AVG Internet Security 2014** je testování na vyžádání. Testy na vyžádání jsou navrženy tak, že mohou testovat různé části vašeho počítače, kdykoliv se objeví podezření na možnost virové infekce. V každém případě však doporučujeme provádět testy pravidelně, i když považujete váš počítač za zcela virus prostý.



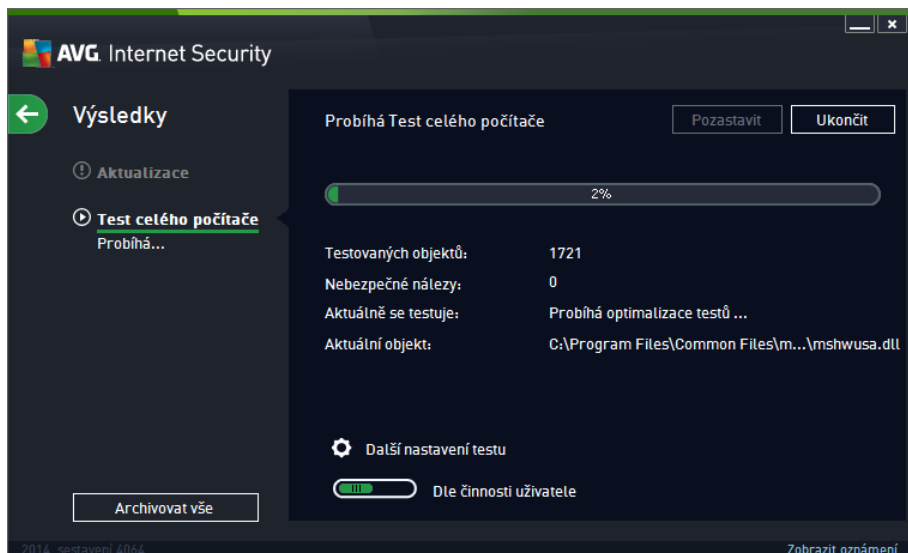
V **AVG Internet Security 2014** najdete tyto typy výrobcem nastavených testů :

11.1.1.1. Test celého počítače

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

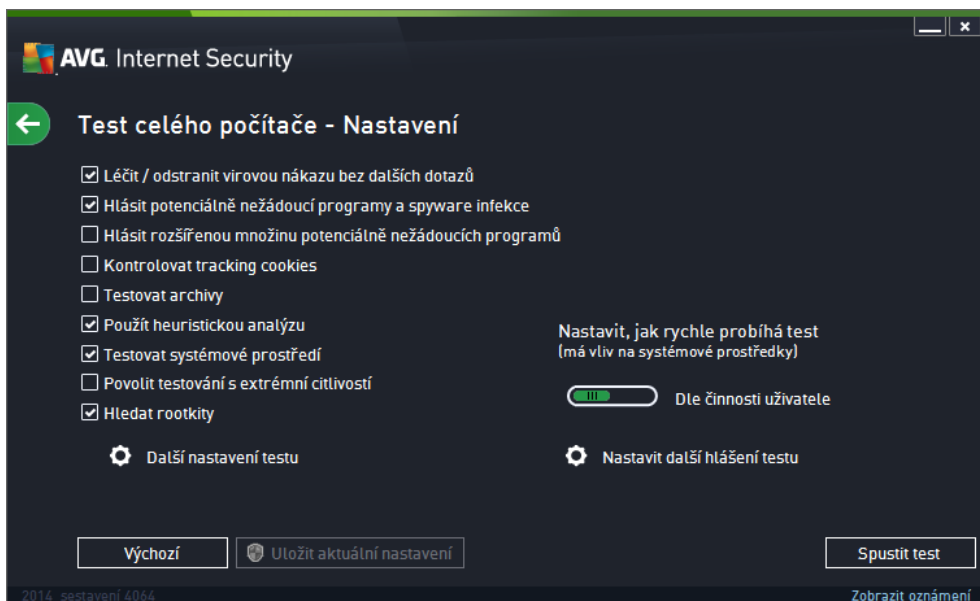
Spuštění testu

Test celého počítače spusťte přímo z [hlavního uživatelského rozhraní](#) kliknutím na graficky zobrazenou 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** můžete sledovat jeho průběh. Test můžete podle potřeby kdykoliv dočasně **Pozastavit** nebo **Ukončit**.



Editace nastavení testu

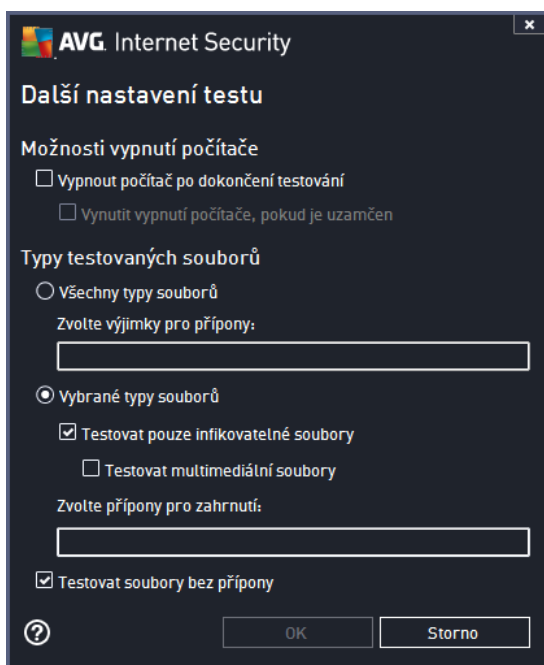
Pokud definované výchozí nastavení **Testu celého počítače** máte možnost editovat v dialogu **Test celého počítače - Nastavení** (ten je dostupný prostřednictvím odkazu **Nastavení** u **Testu celého počítače** z dialogu [Možnosti testu](#)). **Pokud však nemáte skutečný přístup k konfiguraci testu, doporučujeme se držet výrobcem definovaného nastavení!**



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

- **Léčit/odstranit virovou nákazu bez dalších dotazů** (ve výchozím nastavení zapnuto): jestliže je během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. V případě, že virus automaticky léčit nelze, bude infikovaný objekt přesunut do [Virového trezoru](#).
- **Hlásit potenciálně nežádoucí 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 v domě a se souhlasem uživatele. Doporučujeme ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
- **Hlásit rozšířenou množinu potenciálně nežádoucích programů** (ve výchozím nastavení vypnuto): zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware, tj. programů, které jsou v podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.
- **Kontrolovat tracking cookies** (ve výchozím nastavení vypnuto): parametr definuje, že během testu mají být detekovány cookies (HTTP data zaslaná serverem prohlížeči a uložena na počítači uživatele; při každé další návštěvě téhož serveru prohlížeč posílá cookies zpět serveru, který podle nich rozlišuje jednotlivé uživatele).
- **Testovat archivy** (ve výchozím nastavení vypnuto): parametr definuje, že test má testovat všechny soubory zabalené v některém typu archivu, například ZIP, RAR, ...
- **Použít heuristickou analýzu** (ve výchozím nastavení zapnuto): během testu bude použita k detekci infekce i metoda heuristické analýzy (dynamické emulace instrukcí testovaného objektu v prostředí virtuálního počítače).

- **Testovat systémové prostředí** (ve výchozím nastavení zapnuto): test prov í i systémové oblasti vašeho počíta e.
- **Povolit testování s extrémní citlivostí** (ve výchozím nastavení vypnuto): ve specifických situacích (nap íklad p i podez ení na infekci starším typem viru) m žete zvolit tuto metodu testování, která aktivuje nejd kladn ější testovací algoritmy a velmi podrobn ě prov í naprosto všechny oblasti vašeho počíta e. M ějte však na pam ěti, že tato metoda je asov ě velmi náro ná.
- **Hledat rootkity** (ve výchozím nastavení zapnuto): zahrne do testu celého počíta e i ov ení p ítomnosti rootkit ů, které lze spustit i jako [samostatný anti-rootkit test](#).
- **Další nastavení testu** - odkaz otevírá dialog **Další nastavení testu**, kde m žete definovat následující parametry testu:

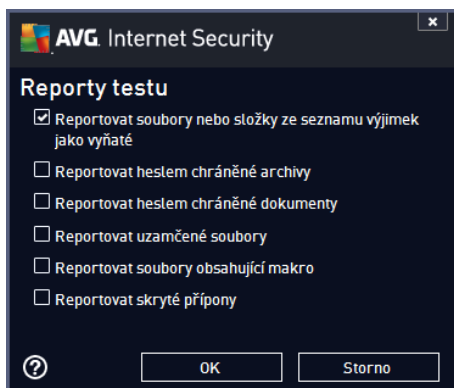


- **Možnosti vypnutí počíta e** - ur ete, zda má být počíta e po dokon ení testu automaticky vypnut. Pokud potvrdíte tuto možnost (**Vypnout počíta e po dokon ení testování**), aktivuje se nová volba (**Vynutit vypnutí počíta e, pokud je uzam en**), p i jejímž potvrzení dojde po dokon ení testu k vypnutí počíta e i tehdy, jestliže je počíta e momentáln ě zamknut.
- **Typy testovaných soubor** - dále se m žete rozhodnout, zda si p ejete testovat:
 - **Všechny typy soubor** - p i emž máte zároveň možnost vyjmout z testování soubory definované seznamem p ípon odd elených árkou.
 - **Vybrané typy soubor** - m žete se rozhodnout, že chcete, aby se testy spoušt ěly pouze nad soubory, které lze považovat za infikovatelné (*soubory, které nemohou být infekcí zasaženy, se testovat nebudou - nap íklad prosté textové soubory nebo n které nespustitelné soubory*), a to v etn ě multimediálních soubor (*video, audio soubory - ponecháte-li tuto položku nezna enou, výrazn ě se tím zkrátí as testování, jelikož multimediální soubory jsou obvykle pom ě velké, ale pravd ě podobnost infekce je u nich velmi nízká*). I zde m žete ur ět výjimky a pomocí seznamu p ípon definovat, které soubory

mají být testovány za všech okolností.

- U položky **Testovat soubory bez přípon** pak rozhodnete, zda se mají testovat i soubory se skrytou či neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme, abyste se tohoto nastavení drželi, pokud nemáte skutečnou důvod její změny. 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 *innosti uživatele*. Tato hodnota nastavení optimalizuje rychlost testu počítače a vytížení systémových zdrojů. Test můžete spustit pomaleji a tedy s nižší zátěží systémových zdrojů (*vhodné, pokud potěbujete během testu na počítači pracovat a nezáleží vám tolik na celkové době testování*) nebo naopak rychleji s vyššími nároky na systémové zdroje (*například v době, kdy na počítači nikdo nepracuje*).
- **Nastavit další hlášení testu** - odkaz otevírá nový dialog **Reporty testu**, v němž můžete označit, které typy nálezů mají být hlášeny:



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

11.1.2. Test vybraných souborů či složek

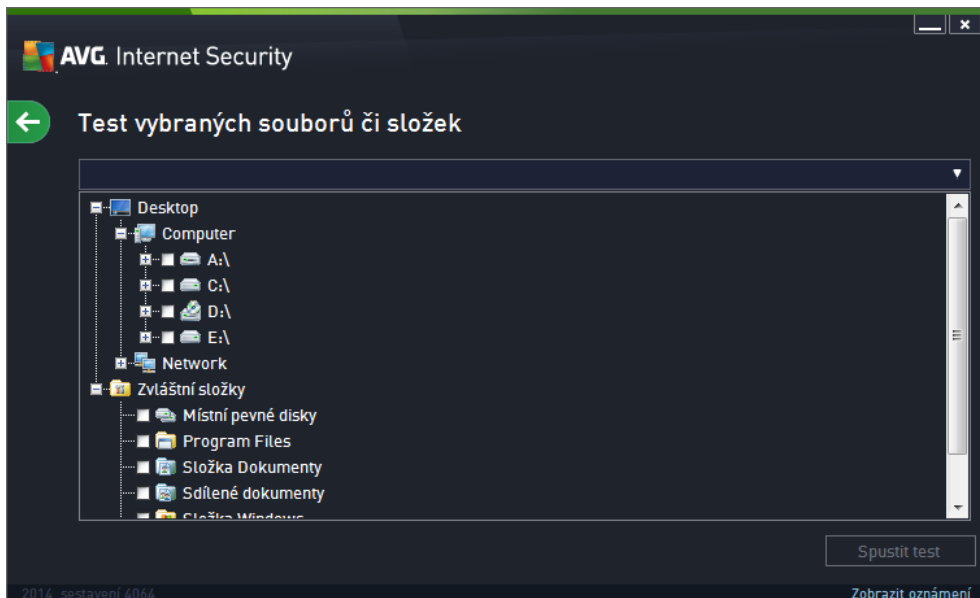
Test vybraných souborů i složek kontroluje pouze uživatelem definované oblasti počítače (zvolené složky, pevné disky, diskety, CD, optické disky, ...). Postup při nálezů a léb /odstranění virové nákazy je stejný jako u **Testu celého počítače**: nalezené viry jsou vyléeny nebo přesunuty do [Virového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

Spuštění testu

Test vybraných souborů i složek spustíte přímo z dialogu [Možnosti testu](#) kliknutím na graficky znázorněnou položku **Test vybraných souborů i složek**. Otevře se rozhraní **Test vybraných souborů i 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

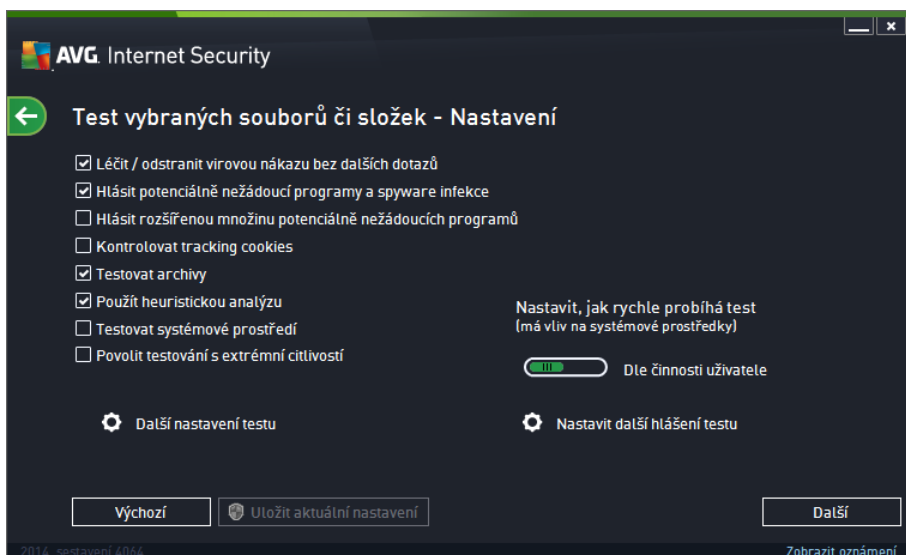


tlačítka **Spustit test** a jeho obsah je identický s obsahem [Testu celého počítače](#).



Editace nastavení testu

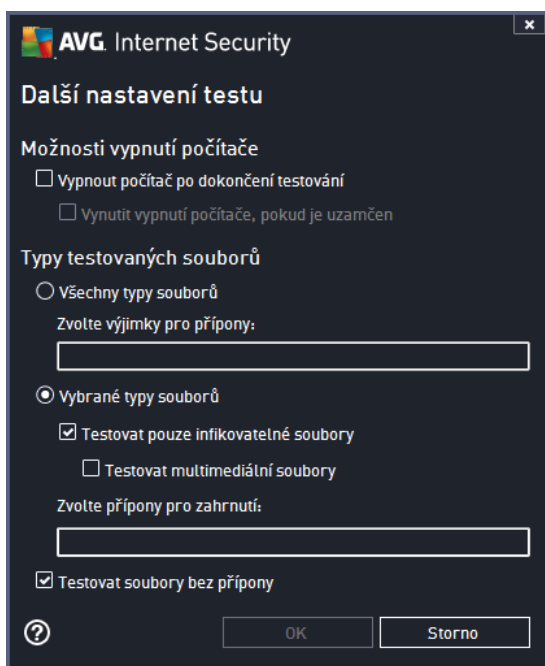
Pokud definované výchozí nastavení **Testu vybraných souborů či složek** máte možnost editovat v dialogu **Test vybraných souborů či složek - Nastavení** (ten je dostupný prostřednictvím odkazu **Nastavení** u **Testu vybraných souborů či složek** z dialogu **Možnosti testu**). **Pokud však nemáte skutečný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



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

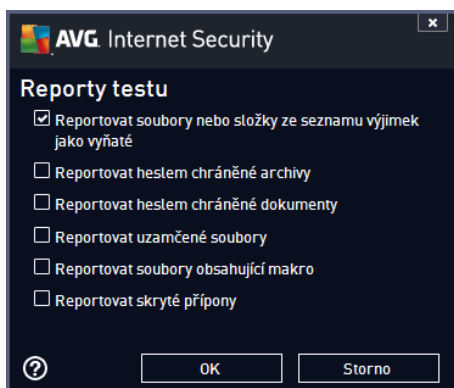
- **Léčit/odstranit virovou nákazu bez dalších dotazů** (ve výchozím nastavení zapnuto): jestliže je během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. V případě, že virus automaticky léčit nelze, bude infikovaný objekt přesunut do [Virového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

- **Hlásit potenciálně nežádoucí 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 v domě a se souhlasem uživatele. Doporučujeme ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
- **Hlásit rozšířenou množinu potenciálně nežádoucích programů** (ve výchozím nastavení vypnuto): Zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware, tj. programů, které jsou v podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům. Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta.
- **Kontrolovat tracking cookies** (ve výchozím nastavení vypnuto): Parametr definuje, že během testu mají být detekovány cookies (*HTTP data zaslaná serverem prohlížeči a uložena na počítači uživatele; při každé další návštěvě téhož serveru prohlížeč posílá cookies zpět serveru, který podle nich rozlišuje jednotlivé uživatele*).
- **Testovat archivy** (ve výchozím nastavení zapnuto): Parametr definuje, že test má testovat všechny soubory zabalené v některém typu archivu, například ZIP, RAR, ...
- **Použít heuristickou analýzu** (ve výchozím nastavení zapnuto): Během testu bude použita k detekci infekce i metoda heuristické analýzy (*dynamické emulace instrukcí testovaného objektu v prostředí virtuálního počítače*).
- **Testovat systémové prostředí** (ve výchozím nastavení vypnuto): Test prověří i systémové oblasti vašeho počítače.
- **Povolit testování s extrémní citlivostí** (ve výchozím nastavení vypnuto): Ve specifických situacích (při podezření na infekci zavlečenou do vašeho počítače) můžete zvolit tuto metodu testování, která aktivuje nejkritičtější testovací algoritmy a velmi podrobně prověří naprosto všechny oblasti vašeho počítače. Mějte však na paměti, že tato metoda je srovnatelně 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** - při němž máte zároveň možnost vyjmout z testování soubory definované seznamem přípon oddělených čárkou.
 - **Vybrané typy souborů** - můžete se rozhodnout, že chcete, aby se testy spouštěly pouze nad soubory, které lze považovat za infikovatelné (*soubory, které nemohou být infekcí zasaženy, se testovat nebudou - například prosté textové soubory nebo některé nespustitelné soubory*), a to včetně multimediálních souborů (*video, audio soubory - ponecháte-li tuto položku neoznáměnou, výrazně se tím zkrátí čas testování, jelikož multimediální soubory jsou obvykle poměrně velké, ale pravděpodobnost infekce je u nich velmi nízká*). I zde můžete určit výjimky a pomocí seznamu přípon definovat, které soubory mají být testovány za všech okolností.
 - U položky **Testovat soubory bez přípon** pak rozhodnete, zda se mají testovat i soubory se skrytou nebo neznámou příponou. Tato položka je ve výchozím nastavení zapnuta a doporučujeme, abyste se tohoto nastavení drželi, pokud nemáte skutečný důvod je změnit. Soubory bez přípon jsou obecně vysoce podezřelé a měly by být otestovány.
- **Nastavit, jak rychle probíhá test** - posuvníkem lze změnit prioritu testu. Ve výchozím nastavení je tato hodnota nastavena *dle přání 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 test** - odkaz otevírá nový dialog **Reporty testu**, v něm můžete označit, které typy nálezů mají být hlášeny:



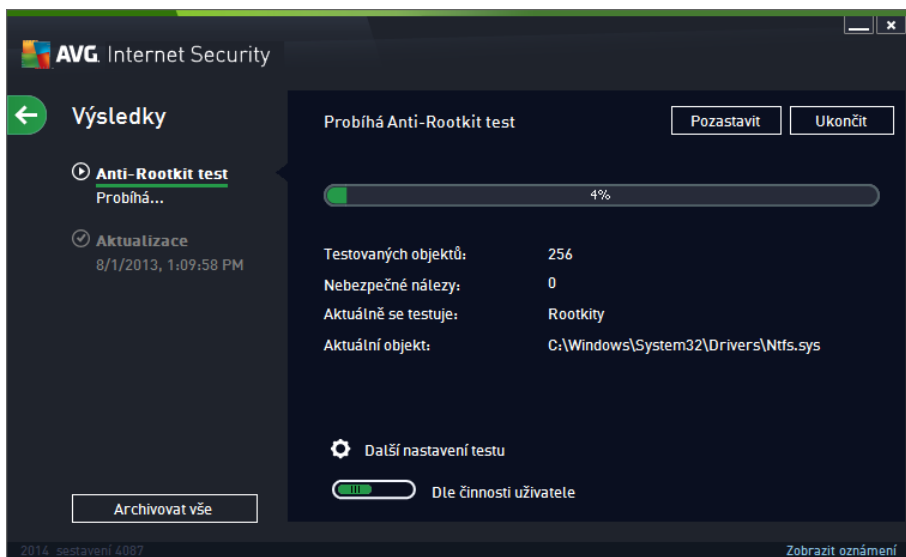
Upozornění: Samotné možnosti nastavení testu jsou shodné s parametry nově definovaného testu, které jsou podrobně popsány v kapitole [AVG testování / Naplánování testu / Jak testovat](#). Pokud se rozhodnete výchozí nastavení **Testu vybraných souborů i složek** změnit, můžete pak svou konfiguraci uložit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

11.1.3. Prohledat počítač na přítomnost rootkitů

Prohledat počítač na přítomnost rootkitů detekuje a umožňuje odstranění nebezpečné rootkity, to jsou programy a technologie, které dokážou maskovat přítomnost zákeřného software v počítači. Rootkit je program speciálně vytvořený tak, aby dokázal převzít kontrolu nad vaším počítačem, aniž by požádal o jakoukoliv autorizaci. Test je schopen detekovat rootkit na základě definovaných pravidel. Dojde-li tedy k nálezům rootkitu, nemusí to nutně znamenat, že je počítač infikovaný. V některých případech mohou být rootkity použity jako ovládací nebo části korektních aplikací.

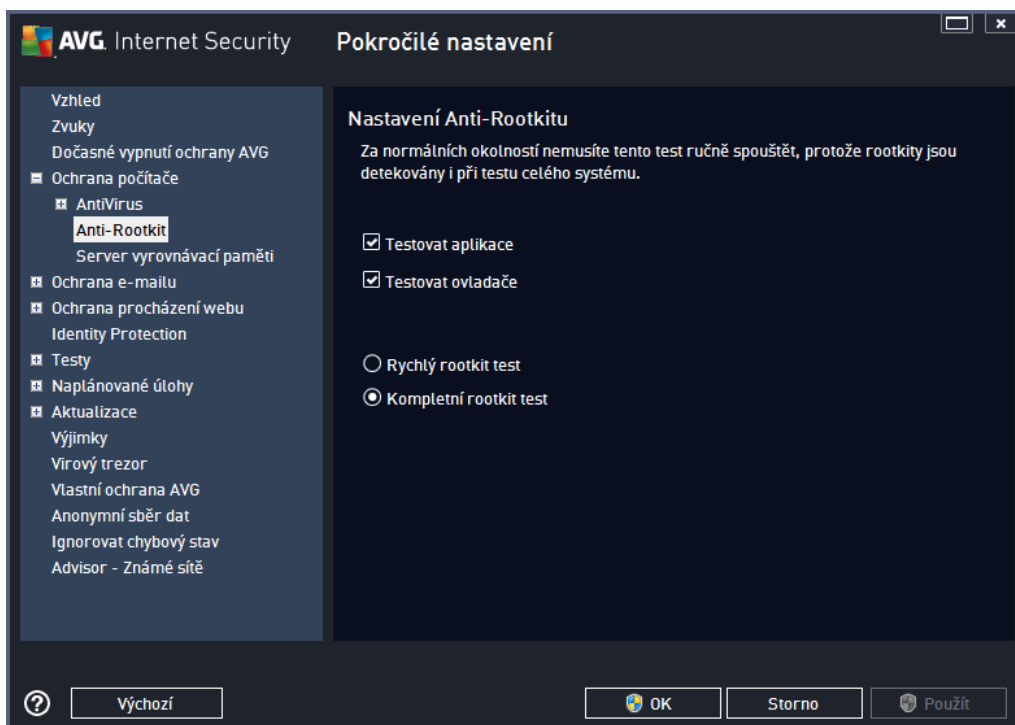
Spuštění testu

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



Editace nastavení testu

P edem 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** a z dialogu **Možnosti testu**). **Pokud však nemáte skutečný přístup k konfiguraci testu, doporučujeme se držet výrobcem definovaného nastavení!**



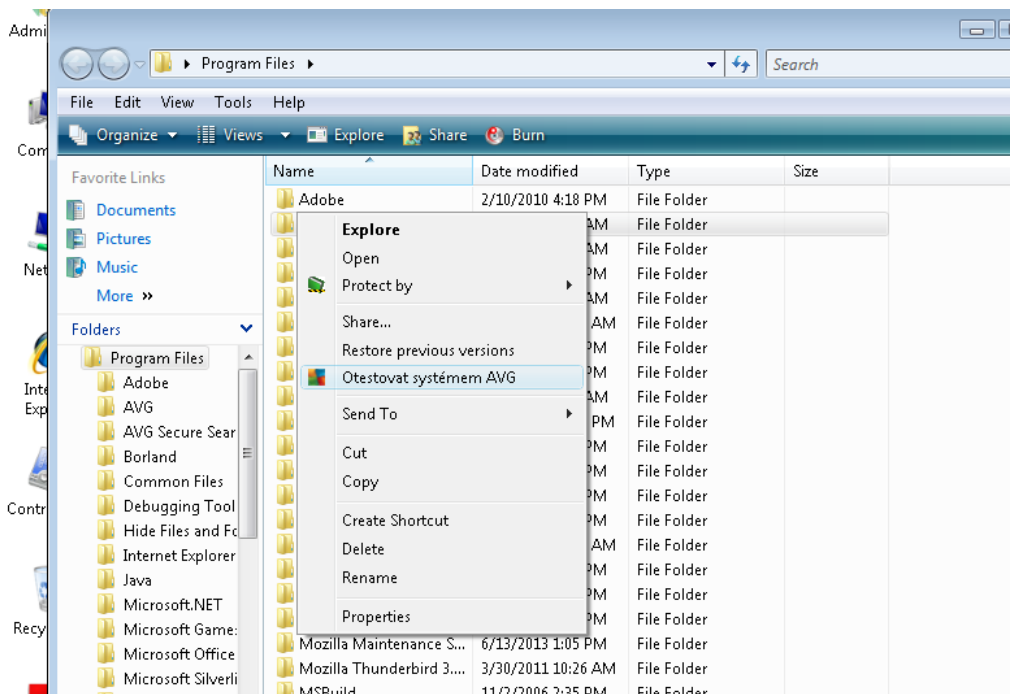
Možnosti **Testovat aplikace** a **Testovat ovladače** umožňují určit, co vše má být v testu na rootkity zahrnuto. Jiné než výchozí nastavení doporučujeme pouze zkušeným uživatelům; jinak prosím ponechte všechny možnosti zapnuté. Dále se můžete rozhodnout, v jakém režimu si přejete test spustit:



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

11.2. Testování v průzkumníku Windows

AVG Internet Security 2014 nabízí kromě přednastavených testů spuštění 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 označíte 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 2014**

11.3. Testování z příkazové řádky

V rámci **AVG Internet Security 2014** existuje také možnost spustit test z příkazové řádky. Tuto možnost využijete například na serverech nebo třeba při vytváření dávkových skriptů, které mají být spuštěny po startu počítače. Z příkazové řádky můžete spustit test s nastavením v šifrovaném parametru, 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** (například **avgscanx /?**). Jediným povinným parametrem testu je **/SCAN**, například **/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 i 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 tímto příponami /například EXT=EXE,DLL/
- /NOEXT Netestovat soubory s tímto příponami /například NOEXT=JPG/
- /ARC Testovat archívy
- /CLEAN Automaticky léčit
- /TRASH Přesunout infikované soubory do [Virového trezoru](#)
- /QT Rychlý test
- /LOG Vygenerovat soubor s výsledkem testu
- /MACROW Hlásit makra
- /PWDW Hlásit heslem chráněné soubory
- /ARCBOMBSW Reportovat archivní bomby (*opakovaně komprimované archivy*)
- /IGNLOCKED Ignorovat zamčené soubory
- /REPORT Hlásit do souboru /jméno souboru/
- /REPAPPEND Přidat k souboru
- /REPOK Hlásit neinfikované soubory jako OK
- /NOBREAK Nepovolit přerušení testu pomocí CTRL-BREAK
- /BOOT Povolit kontrolu MBR/BOOT
- /PROC Testovat aktivní procesy
- /PUP Hlásit Potenciálně nebezpečné programy
- /PUPEXT Hlásit rozšířenou množinu Potenciálně nebezpečných programů
- /REG Testovat registry
- /COO Testovat cookies
- /? Zobrazit nápovědu k tomuto tématu
- /HELP Zobrazit nápovědu k tomuto tématu
- /PRIORITY Nastavit prioritu testu /Low, Auto, High/ (viz [Pokročilá nastavení / Testy](#))
- /SHUTDOWN Vypnout počítač po dokončení testu
- /FORCESHUTDOWN Vynutit vypnutí počítače po dokončení testu
- /ADS Testovat alternativní datové proudy (pouze NTFS)

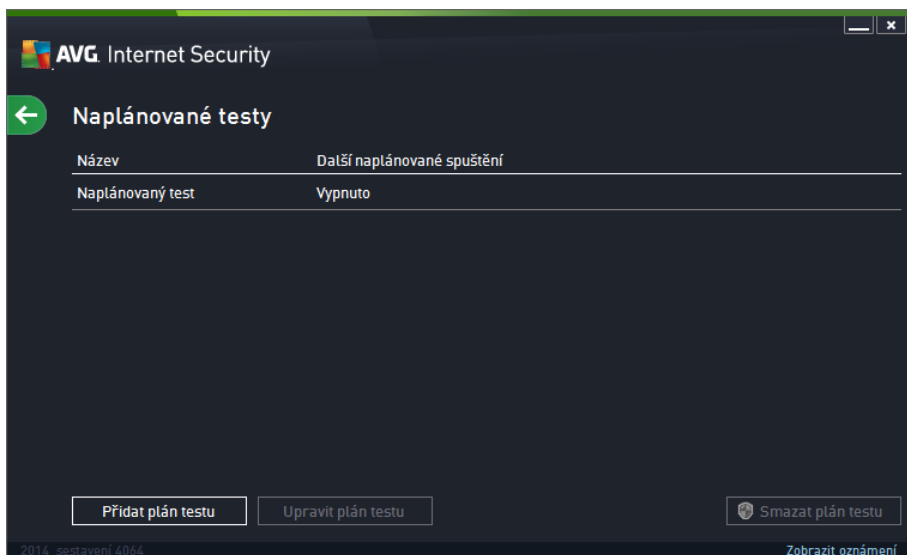


- /HIDDEN Hlásit soubory se skrytou příponou
- /INFECTABLEONLY Testovat pouze infikovatelné soubory
- /THOROUGHSCAN Povolit testování s extrémní citlivostí
- /CLOUDCHECK Ověřit falešné detekce
- /ARCBOMBSW Hlásit opakovaně komprimované archivní soubory

11.4. Naplánování testu


Testy v **AVG Internet Security 2014** lze spouštět buďto na vyžádání (*například v situaci, kdy máte podezření na zavlečení infekce na váš počítač nebo z jiného zdroje*) anebo podle nastaveného plánu. Doporučujeme používat především spouštění testů podle plánu, protože tímto postupem zajistíte svému počítači dostatečnou prevenci a budete moci pracovat bez starostí o to, zda a kdy test spustit. [Test celého počítače](#) by měl být spouštěn pravidelně, a to nejméně jednou týdně. Pokud vám to však provoz na vašem počítači umožní, doporučujeme spouštět test celého počítače jednou denně; tak je také ve výchozí konfiguraci nastaven plán testů. Jestliže je počítač trvale zapnutý, je vhodné naplánovat spuštění **Testu celého počítače** na dobu mimo pracovní hodiny. Pokud počítač vypínáte, nezapomeňte využít možnosti [spustit test při startu počítače, pokud byl naplánovaný](#) a zmeškán.

Plán testů lze vytvářet v 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:

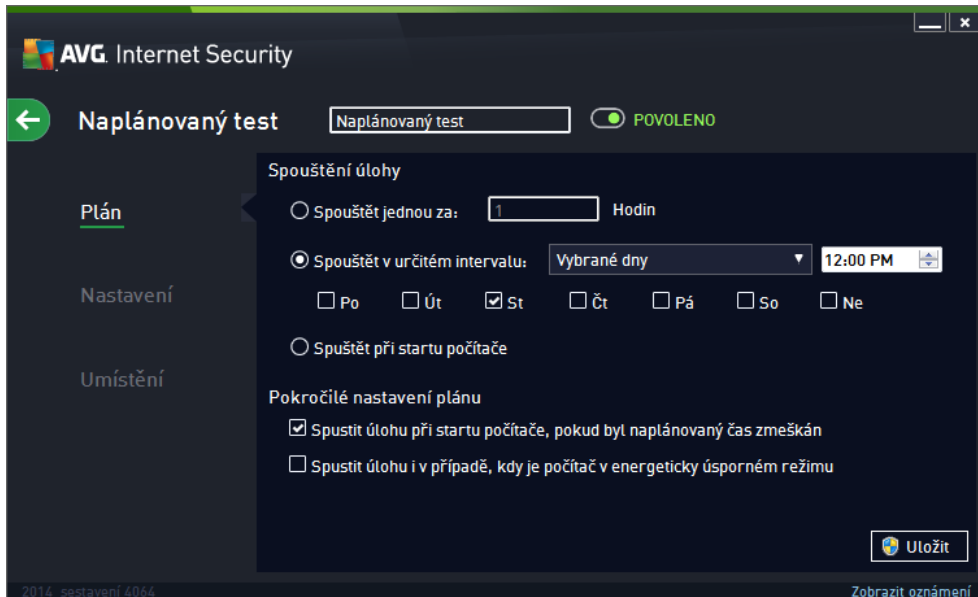


V tomto dialogu máte možnost naplánovat své vlastní testy, a to pomocí tlačítka **Přidat plán testu**. Parametry naplánovaného testu můžete editovat (*přidat, nastavit plán nový*) na těchto záložkách:

- [Plán](#)
- [Nastavení](#)
- [Umístění](#)

Na každé záložce máte nejprve možnost jednoduchým p eputím semaforu  naplánovaný test (do asn) deaktivovat, a pozd ji podle pot eby znovu použít.

11.4.1. Plán



V textovém poli v horní ásti záložky **Plán** m žete zadat jméno, které si p ežete p i adit práv vytvá enému testu. Snažte se vždy používat stru né, popisné a p ípadné názvy, abyste se pozd ji v naplánovaných úlohách snadn ji vyznali. Nap íklad nevhodným názvem testu je nap íklad "Nový test" nebo "Martin v test", protože ani jeden název nelypovídá o tom, co test ve skute nosti kontroluje. Naproti tomu správným popisným názvem testu m že být nap íklad "Test systémových oblastí" nebo "Test disku C:" a podobn .


V dialogu m žete dále definovat tyto parametry testu:

- **Spouštění úlohy** - V této sekci dialogu ur ete, v jakých asových intervalech má být nov naplánovaný test spušt n. asové ur ení m žete zadat bu to opakovaným spušt ním testu po uplynutí ur ené doby (*Spoušt t jednou za*) nebo stanovením pesného data a asu (*Spoušt t v ur itém intervalu*), p ípadn ur ením události, na niž se spušt ní testu váže (*Spoušt t p i startu počíta e*).
- **Pokro ilé nastavení plánu** - Tato sekce umož uje definovat podmínky, kdy má i nemá být test spušt n, jestliže je po íta v úsporném režimu nebo zcela vypnutý a naplánovaný as spušt ní testu byl zmeškán. O automatickém spušt ním testu budete v ur eném ase informováni prost ednictvím pop-up okna nad [ikonou AVG na systémové lišt](#) . Po zahájení testu se na systémové lišt objeví [nová ikona AVG](#) (barevná s problikávajícím sv tlem), která vás informuje o b žícím testu. Kliknutím pravého tlačítka myši nad touto ikonou otev ete kontextové menu, z n hož m žete b žící test pozastavit nebo ukon it, a rovn ž zm nit prioritu práv probíhajícího testu.

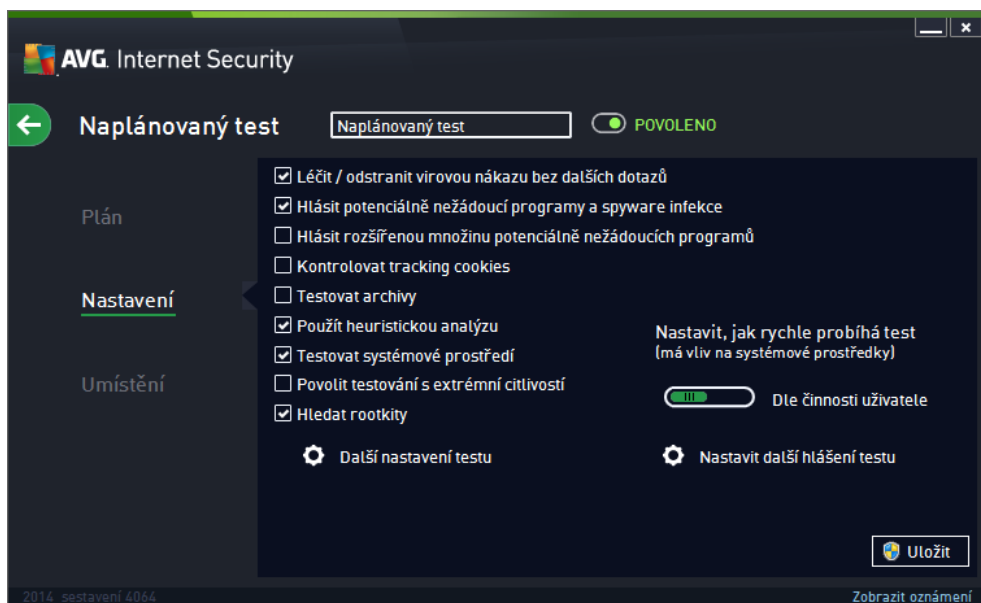
Ovládací tlačítka dialogu

- **Uložit** - uloží všechny zm ny, které jste provedli na této záložce nebo na libovolné jiné záložce dialogu pro nastavení plánu testu a p epne vás zp t 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 přidat právě vytvářenému testu. Snažte se vždy používat stručné, popisné a případně názvy, abyste se později v naplánovaných úlohách snadněji vyznali. Například nevhodným názvem testu je například "Nový test" nebo "Martin v test", protože ani jeden název nevyovídá 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 vodotěsný konfiguraci testu, doporučujeme se držet výrobcem definovaného nastavení:**

- **Léčit/odstranit virovou nákazu bez dalších dotazů** (ve výchozím nastavení zapnuto): jestliže je během testu identifikován virus, je možné jej automaticky léčit, pokud je k dispozici metoda k jeho vyléčení. V případě, že virus automaticky léčit nelze, bude infikovaný objekt přesunut do [Virového trezoru](#).
- **Hlásit potenciálně nežádoucí 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 v tšinu určitý program představuje bezpečnostní riziko, jsou mnohdy instalovány v domě a se souhlasem uživatele. Doporučujeme ponechat tuto volbu aktivní, protože výrazně zlepšuje zabezpečení vašeho počítače.
- **Hlásit rozšířenou množinu potenciálně nežádoucích programů** (ve výchozím nastavení vypnuto): zaškrtnutím tohoto políčka můžete aktivovat navíc detekci rozšířené sady spyware, tj. programů, které jsou v povodní podobě od výrobce neškodné a v případě, ale mohou být snadno zneužity ke

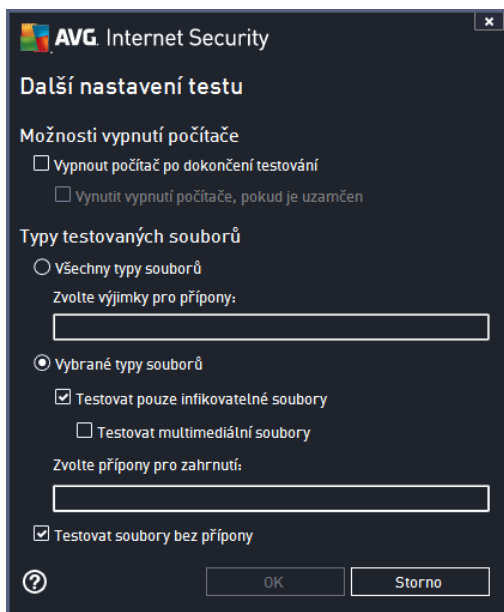


škodlivým ú el m. Jde o dodate né opat ení, které zlepšuje zabezpe ení vašeho počíta e na další úrovni, nicmén m že blokovat také n které legální programy, proto je ve výchozím nastavení tato možnost vypnuta.

- **Kontrolovat tracking cookies** (ve výchozím nastavení vypnuto): parametr definuje, že b hem testu mají být detekovány cookies (*HTTP data zaslaná serverem prohlíže i a uložena na počíta i uživatele; p i každé další návště v téhož serveru prohlíže posílá cookies zp t serveru, který podle nich rozlišuje jednotlivé uživatele*);
- **Testovat archivy** (ve výchozím nastavení vypnuto): parametr definuje, že test má testovat všechny soubory, a to i takové, které jsou zabaleny v n kterém typu archivu, například ZIP, RAR, ...
- **Použít heuristickou analýzu** (ve výchozím nastavení zapnuto): b hem testu bude použita k detekci infekce i metoda heuristické analýzy (*dynamické emulace instrukcí testovaného objektu v prost edí virtuálního počíta e*);
- **Testovat systémové prost edí** (ve výchozím nastavení zapnuto): test prov í i systémové oblasti vašeho počíta e;
- **Povolit testování s extrémní citlivostí** (ve výchozím nastavení vypnuto): ve specifických situacích (nap íklad p i podez ení na infekci starším typem viru) m žete zvolit tuto metodu testování, která aktivuje nejd kladn jší testovací algoritmy a velmi podrobn prov í naprosto všechny oblasti vašeho počíta e. M jte však na pam ti, že tato metoda je asov velmi náro ná.
- **Hledat rootkity** (ve výchozím nastavení zapnuto): parametr služby Anti-Rootkit prohledává počíta na p ítomnost rootkit , tedy program a technologií, které dokáží maskovat p ítomnost malware v počíta i. Dojde-li k nálezu rootkitu, nemusí to nutn znamenat, že je počíta infikovaný. V n kterých p ípadech mohou být rootkity použity jako ovlada e nebo ásti korektních aplikací.

Další nastavení test

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



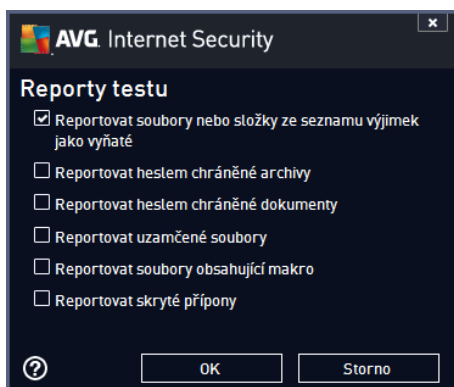
- **Možnosti vypnutí po íta e** - ur ete, zda má být po íta po dokon ení testu automaticky vypnut. Pokud potvrdíte tuto možnost (*Vypnout po íta po dokon ení testování*), aktivuje se nová volba (*Vynutit vypnutí po íta e, pokud je uzam en*), p í jejímž potvrzení dojde po dokon ení testu k vypnutí po íta e i tehdy, jestliže je po íta momentáln zamknut.
- **Typy testovaných soubor** - dále se m žete rozhodnout, zda si p ežete testovat:
 - **Všchny typy soubor** - p í emž máte zároveň možnost vyjmout z testování soubory definované seznamem p ípon odd lených árkou.
 - **Vybrané typy soubor** - m žete se rozhodnout, že chcete, aby se testy spoušt ly pouze nad soubory, které lze považovat za infikovatelné (*soubory, které nemohou být infekcí zasaženy, se testovat nebudou - například prosté textové soubory nebo n které nespustitelné soubory*), a to v etn multimediálních soubor (*video, audio soubory - ponecháte-li tuto položku neozna enou, výrazn se tím zkrátí as testování, jelikož multimediální soubory jsou obvykle pom m velké, ale pravd podobnost infekce je u nich velmi nízká*). I zde m žete ur it výjimky a pomocí seznamu p ípon definovat, které soubory mají být testovány za všech okolností.
 - U položky **Testovat soubory bez p ípon** pak rozhodn te, zda se mají testovat i soubory se skrytou í neznámou p íponou. Tato položka je ve výchozím nastavení zapnuta a doporu ujeme, abyste se tohoto nastavení podrželi, pokud nemáte skute ný d vod jej m nit. Soubory bez p ípon jsou obecn ysoce podez elé a m ly by být otestovány.

Nastavit, jak rychle probíhá test


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

Nastavit další hlášení testu

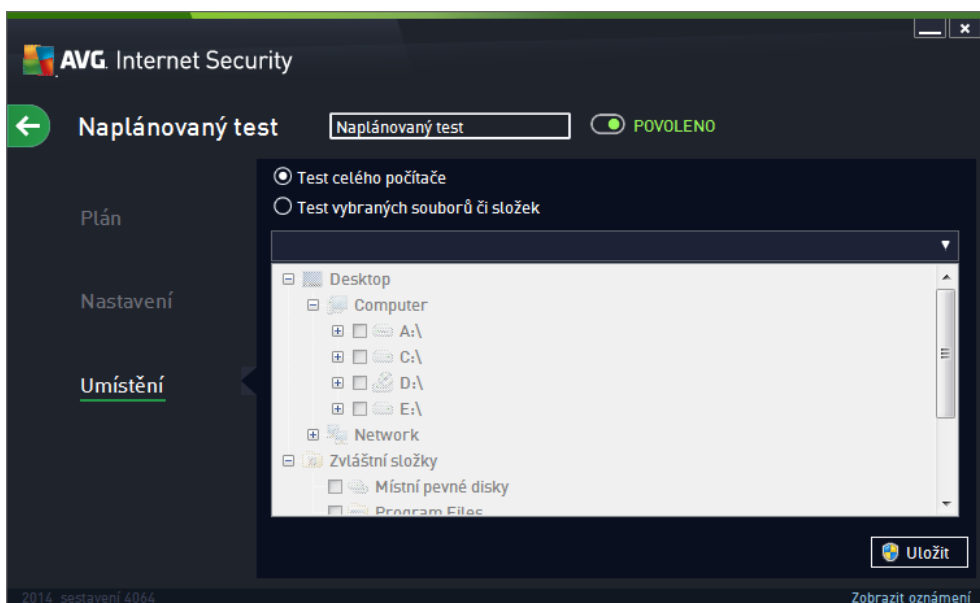
Kliknutím na odkaz **Nastavit další hlášení testu** otev ete samostatné dialogové okno **Reporty testu**, v n mž m žete ozna ením p íslušných položek ur it situace, jejichž výskyt b hem testu má být hlášen:



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


V zobrazené stromové struktuře je zahrnuta také v textovém označení **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**

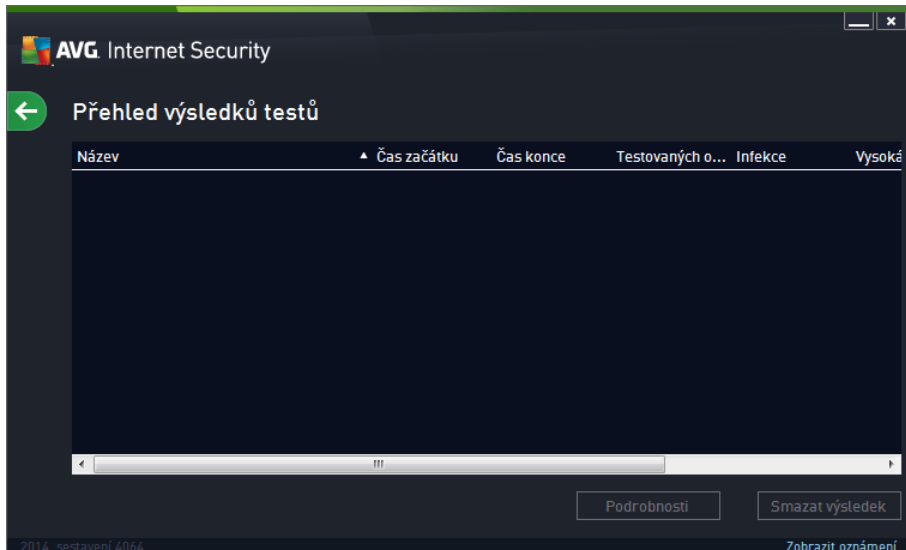


- *pro Win XP*: C:\Documents and Settings\Default User\My Documents\
- *pro Windows Vista/7*: C:\Users\user\Documents\
 - **Sdílené dokumenty**
 - *pro Win XP*: C:\Documents and Settings\All Users\Documents\
 - *pro Windows Vista/7*: C:\Users\Public\Documents\
 - **Složka Windows** - C:\Windows\
 - **Ostatní**
 - *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 proběhnutých 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 vyléeny
 -  Test byl přerušen před dokončením, infekce byly nalezeny, ale nikoliv vyléeny
 -  Test byl dokončen, infekce byly nalezeny a vyléeny nebo odstraněny
 -  Test byl přerušen před dokončením, infekce byly nalezeny a vyléeny 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 vysoké, střední a málo nebezpečné.



- **Rootkity** - Uvádí celkový počet [rootkit](#) nalezených během testování.

Ovládací prvky dialogu

Podrobnosti - Kliknutím na tlačítko se zobrazí [podrobný popis pohled výsledku zvoleného testu](#) (tj. výsledku, který jste aktuálně v tabulce označili).

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



- Pomocí šipky v levé horní části dialogu se vrátíte zpět do [základního uživatelského rozhraní](#) s pohledem komponent.

11.6. Podrobnosti výsledku testu

Pohled podrobných informací o výsledku zvoleného testu otevřete kliknutím na tlačítko **Podrobnosti** dostupné z dialogu [Pohled výsledku testu](#). Tím přejdete do rozhraní téhož dialogu, kde jsou podrobně rozepsány informace o výsledku konkrétního testu. Informace jsou rozděleny na těchto 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 pohled informací o testu, včetně podrobností o jednotlivých detekovaných hroznách. Máte zde také možnost exportovat pohled 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.

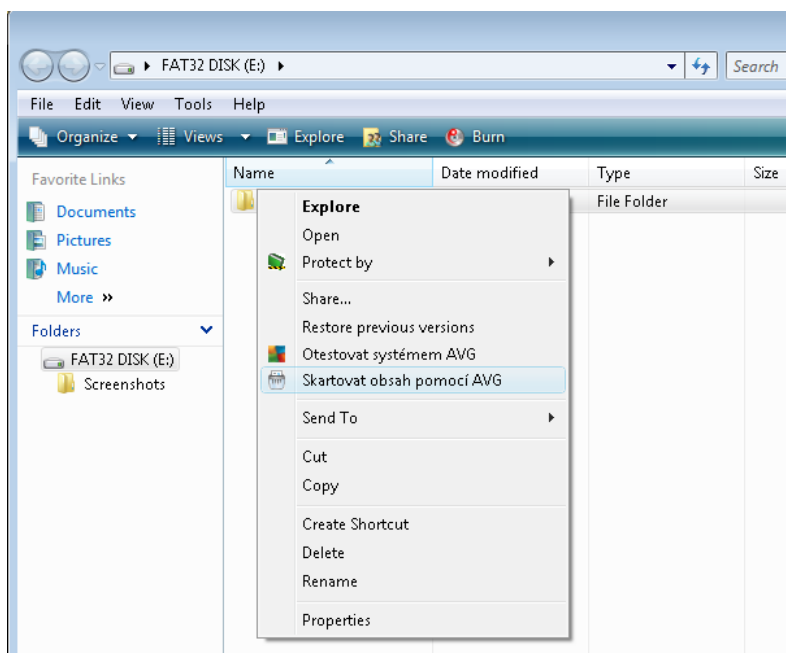
• **Vysoká závažnost**: Hrozbami s vysokou závažností rozumíme například viry, trojské koně, exploity apod. Včetně se sem také objevují objekty detekované heuristickou analýzou, tedy takové hrozby, které dosud nejsou popsány ve virové databázi.



12. AVG File Shredder

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

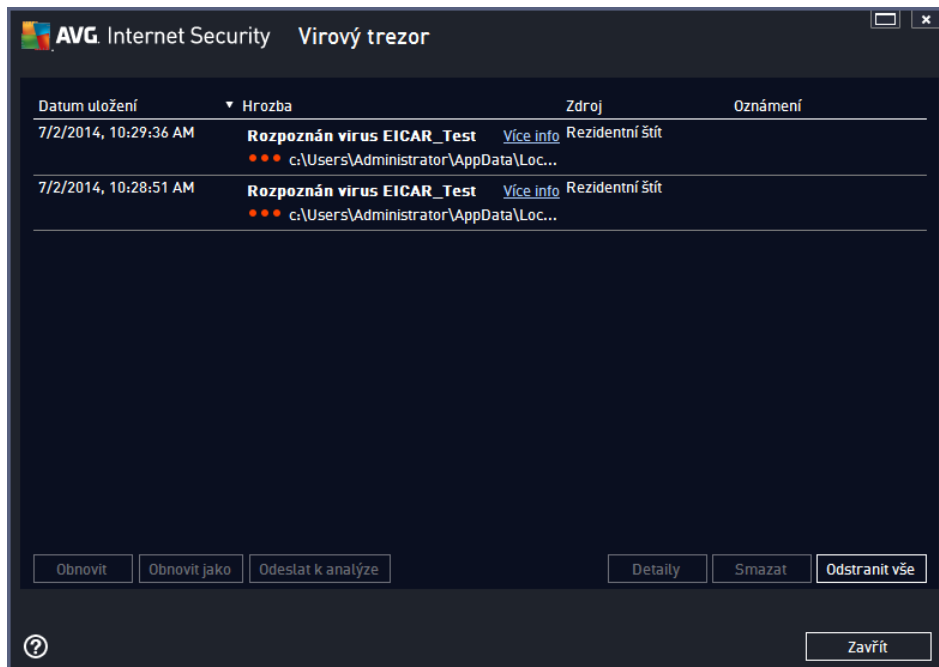
Chcete-li skartovat soubor i složku, vyberte zvolený objekt v aplikaci pro správu souborů (*Windows Explorer, Total Commander, ...*) a klikněte na něj pravým tlačítkem myši. Z kontextové nabídky zvolte položku **Skartovat obsah pomocí AVG**. Tímto způsobem můžete skartovat i soubory v odpadkovém koši.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



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



13. Virový trezor



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

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

- **Datum uložení** - Datum a čas detekce infikovaného souboru a jeho přesunutí do **Virového trezoru**.
- **Hrozba** - Jestliže jste si v rámci instalace programu **AVG Internet Security 2014** nainstalovali také komponentu [Identita](#), najdete v tomto sloupci grafické znázornění závažnosti infekce, od nezávadné (*ti zelené tečky*) po vysoce rizikovou (*ti červené tečky*). Zároveň je zde uvedena informace o typu detekce a místě, kde byla zachycena. Odkaz [Více info](#) odkazuje na stránku s podrobnostmi o detekované infekci v on-line [virové encyklopedii](#).
- **Zdroj** - Určuje, která komponenta programu **AVG Internet Security 2014** uvedenou hrozbu detekovala.
- **Oznámení** - Sloupec je většinou prázdný, pouze ve výjimečných případech se může objevit poznámka s podrobnostmi k přeslušné detekované hrozbě.

Ovládací tlačítka dialogu

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



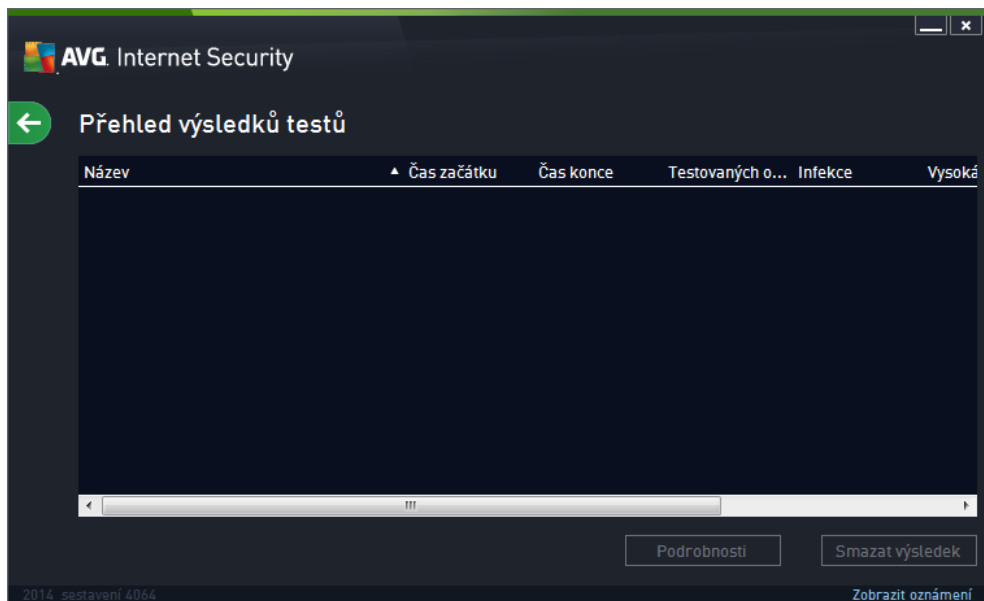
- **Obnovit** - přesune infikovaný soubor z **Virového trezoru** zpět do původního umístění.
- **Obnovit jako** - pokud se rozhodnete detekovanou infekci z **Virového trezoru** umístit do zvolené složky, použijte toto tlačítko. Podezřelý a detekovaný objekt bude uložen pod svým původním jménem, a pokud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

14. Historie

Sekce **Historie** zahrnuje veškeré informace a podává podrobný pohled o všech probíhajících událostech (např. o aktualizacích, testech, nálezích, 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](#)


14.1. Výsledky testů



Dialog **Přehled výsledků testů** je dostupný volbou položky **Možnosti / Historie / Výsledky testů** v horním vodorovném menu hlavního okna **AVG Internet Security 2014**. 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 nepřipravená - celá ikona znamená, že test probíhal celý a byl úspěšně ukončen, nepřipravená ikona identifikuje nedokončený nebo přerušovaný test.

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

- **čas začátku** - datum a přesný čas spuštění testu
- **čas konce** - datum a přesný čas ukončení testu
- **Testovaných objektů** - počet objektů, které byly během testu zkontrolovány
- **Infekce** - číslo udává počet nalezených / odstraněných virových infekcí
- **Vysoká / Střední** - v těchto sloupcích je uveden počet celkově nalezených a odstraněných infekcí vysoké i střední závažnosti
- **Informace** - údaje o průběhu testu, zejména o jeho úspěšném i nepřesném ukončení
- **Rootkity** - počet detekovaných [rootkitů](#)

Ovládací tlačítka dialogu

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

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



14.2. Nálezy Rezidentního štítu

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

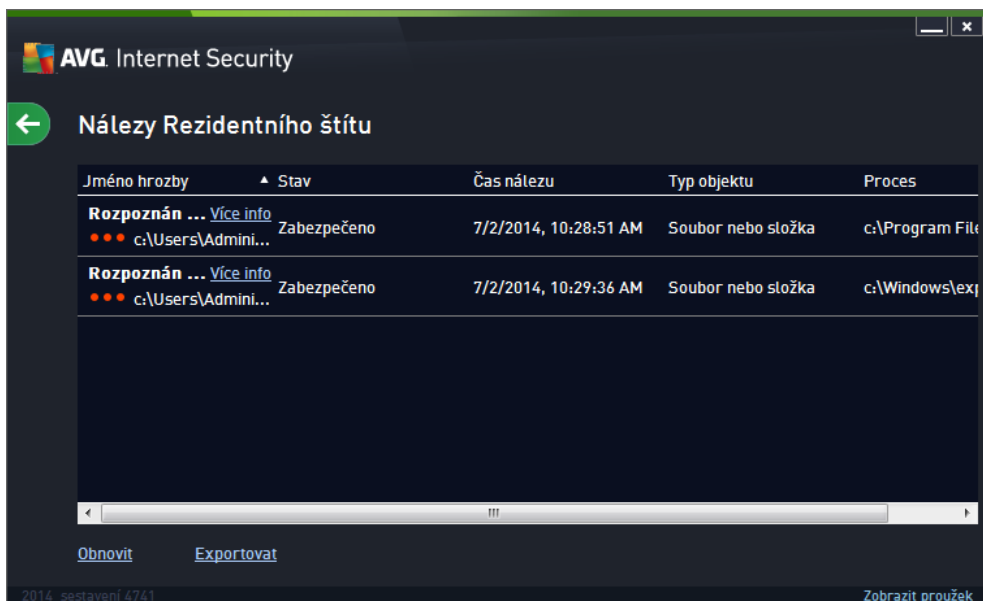


V tomto varovacím dialogu najdete informaci o objektu, který byl detekován jako infikovaný (*Hrozba*) a podrobnosti o rozpoznané infekci (*Popis*). Odkaz *Více informací* odkazuje na stránku s podrobnostmi o detekované infekci v on-line [virové encyklopedii](#), jsou-li tyto informace k dispozici. V dialogu dále najdete přehled možných řešení, jak naložit s detekovanou hrozbou. Jedna z alternativ 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 přesunutí infikovaného objektu vyzváni varovacím hlášením o nedostatku místa ve Virovém trezoru. Objem Virového trezoru si však můžete sami nastavit. Velikost prostoru ve Virovém trezoru je dána procentuálně a závisí na celkové velikosti vašeho pevného disku. Nastavení velikosti Virového trezoru lze provést v dialogu [Virový trezor](#) v rámci [Pokročilého nastavení AVG](#), položka 'Omezit velikost Virového trezoru'.

Ve spodní části dialogu najdete pak odkaz **Zobrazit detaily**. Kliknutím na tento odkaz otevřete nové 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 2014**. V dialogu najdete seznam objektů, které byly rezidentním štítem detekovány jako nebezpečné a buďto byly odstraněny nebo přesunuty do [Virového trezoru](#).



U každého z detekovaných objektů jsou k dispozici následující informace:

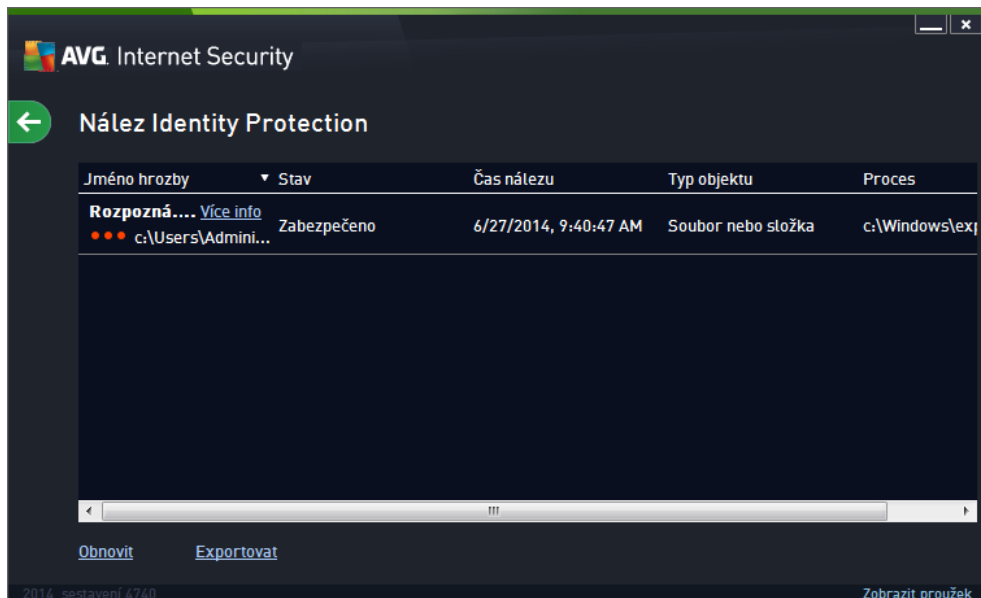
- **Jméno hrozby** - popis (případně jméno) detekovaného objektu a jeho umístění. Odkaz *Více info* odkazuje na stránku s podrobnostmi o detekované infekci v on-line [virové encyklopedii](#).
- **Stav** - jak bylo s detekovaným objektem naloženo (*blokáce*)
- **čas nálezu** - datum a čas, kdy došlo k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

Ovládací tlačítka

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

14.3. Nález Identity Protection

Dialog **Nález Identity Protection** je dostupný volbou položky **Možnosti / Historie / Nález Identity Protection** v horním vodorovném menu hlavního okna **AVG Internet Security 2014**.




V dialogu najdete seznam nález detekovaných komponentou [Identity Protection](#). U každého z detekovaných objektů jsou k dispozici následující informace:

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

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

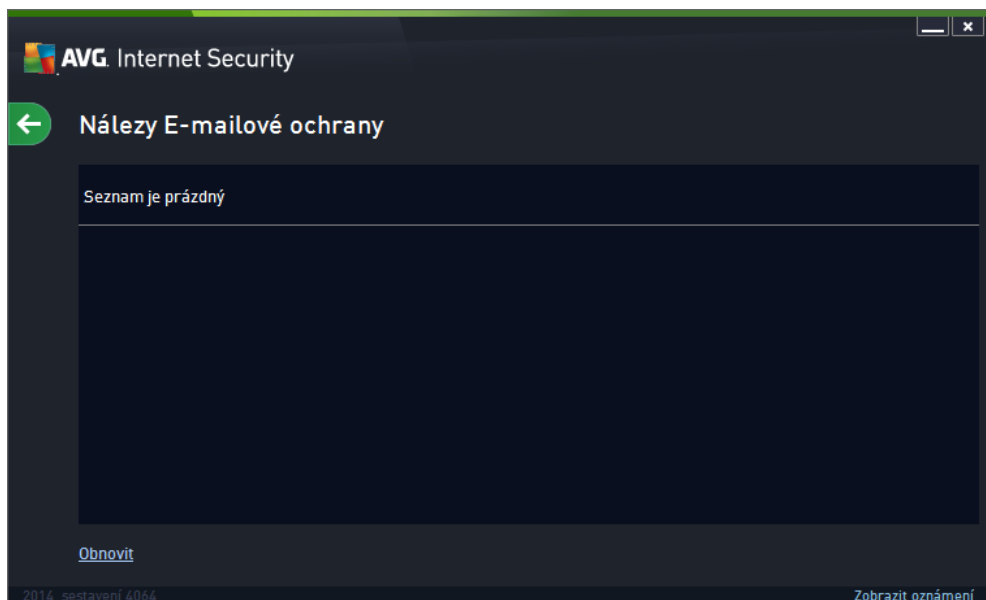
Ovládací tlačítka

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

- **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.

14.4. Nálezy E-mailové ochrany

Dialog **Nálezy E-mailové ochrany** je dostupný volbou položky **Možnosti / Historie / Nálezy E-mailové ochrany** v horním vodorovném menu hlavního okna **AVG Internet Security 2014**.




V dialogu najdete seznam nálezů detekovaných komponentou [Kontrola pošty](#). U každého z detekovaných objektů jsou k dispozici následující informace:

- **Jméno nálezů** - popis (případně i jméno) detekovaného objektu a jeho umístění
- **Výsledek** - jak bylo s detekovaným objektem naloženo
- **čas nálezů** - 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**).

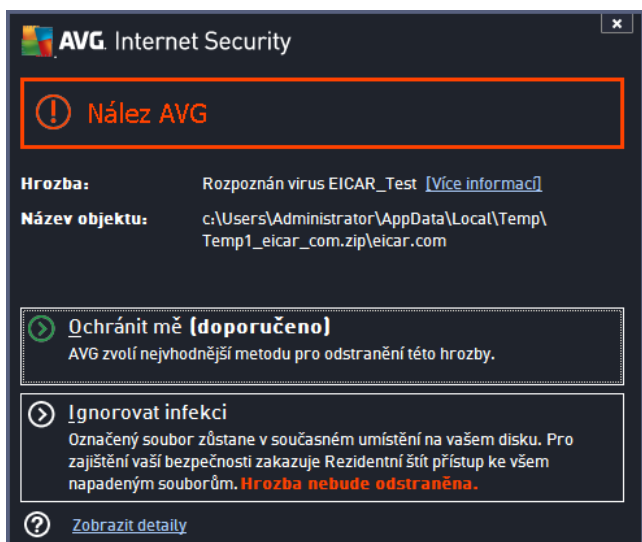
Ovládací tlačítka

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.

14.5. Nález Webového štítu

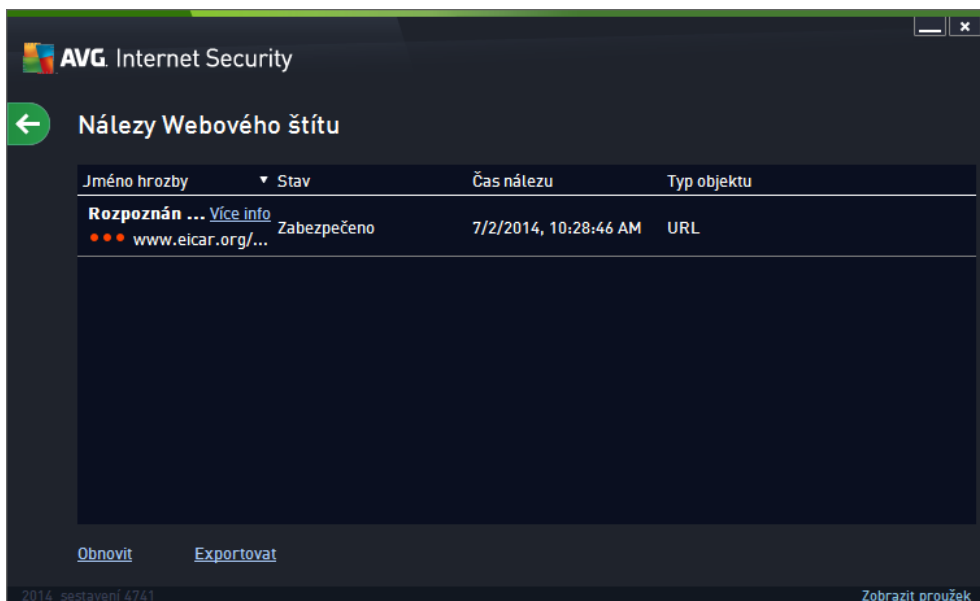
Webový štít kontroluje v reálném čase obsah webových stránek nebo souborů stahovaných z Internetu. Každá stránka je prověřena ještě předtím, než je skutečně stažena a zobrazena webovým prohlížečem. Jestliže detekuje virus nebo jakýkoliv podezřelý objekt, budete okamžitě varováni tímto dialogem:



V tomto varovném dialogu najdete informaci o objektu, který byl detekován jako infikovaný (*Hrozba*) a podrobnosti o rozpoznané infekci (*Název objektu*). Odkaz *Více informací* odkazuje na stránku s podrobnostmi o detekované infekci v on-line [vírové encyklopedii](#), jsou-li tyto informace k dispozici. V dialogu jsou dostupná tato ovládací prvky:

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


Webová stránka s podezřelým souborem nebude otevřena a záznam o detekované infekci bude zaznamenán v pohledu **Nález Webového štítu**. Tento pohled detekovaných nálezů je dostupný volbou položky **Možnosti / Historie / Nález webového štítu** v horním vodorovném menu hlavního okna **AVG Internet Security 2014**:



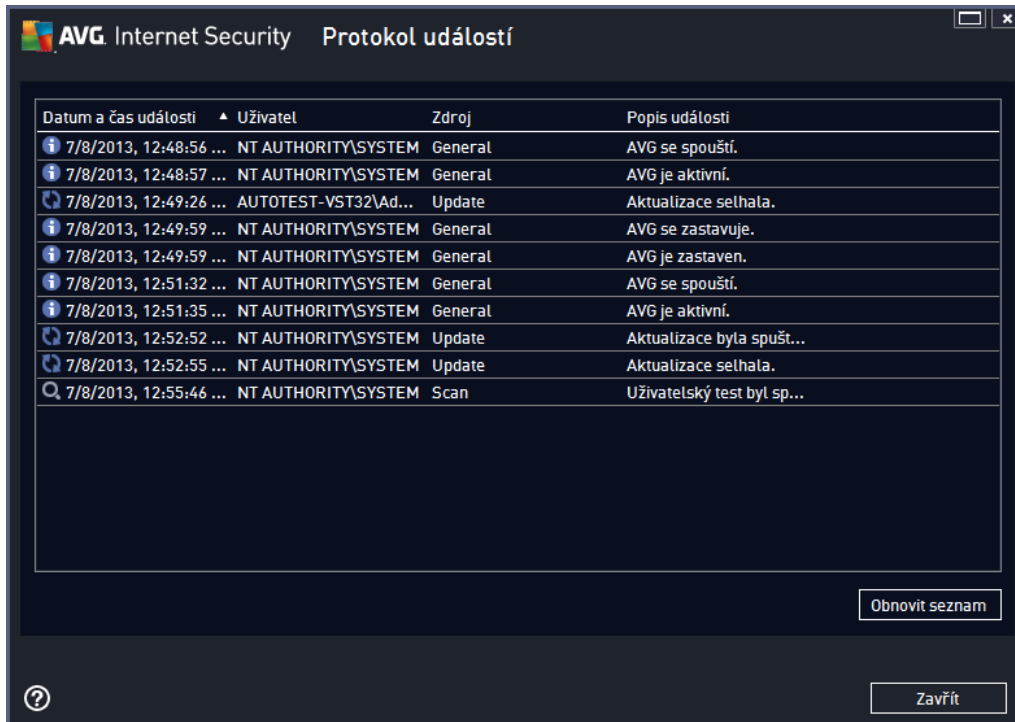
U každého z detekovaných objektů jsou k dispozici následující informace:

- **Jméno hrozby** - popis (případně jméno) detekovaného objektu a jeho umístění (stránka, odkud byl objekt stažen); odkaz [Více info](#) odkazuje na stránku s podrobnostmi o detekované infekci v on-line [vírové encyklopedii](#).
- **Stav** - jak bylo s detekovaným objektem naloženo (blokace)
- **čas nálezu** - datum a čas, kdy došlo k detekci hrozby
- **Typ objektu** - jakého typu je detekovaný objekt

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

14.6. Protokol událostí



Dialog **Protokol událostí** je dostupný volbou položky **Možnosti / Historie / Protokol událostí** v horním vodorovném menu hlavního okna **AVG Internet Security 2014**. V tomto dialogu najdete přehled všech důležitých událostí, které nastaly v průběhu práce **AVG Internet Security 2014**. Zaznamenávají se různé typy událostí, například informace o aktualizacích programu, informace o spuštění/ukončení/přerušení testů (včetně testů spuštěných automaticky), informace o událostech týkajících se nalezení virů (přes [testování](#) i *Residentním štítem*) s uvedením konkrétního místa nálezů a informace o ostatních důležitých událostech.

Ke každé události jsou evidovány následující údaje:

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

Ovládací tlačítka dialogu

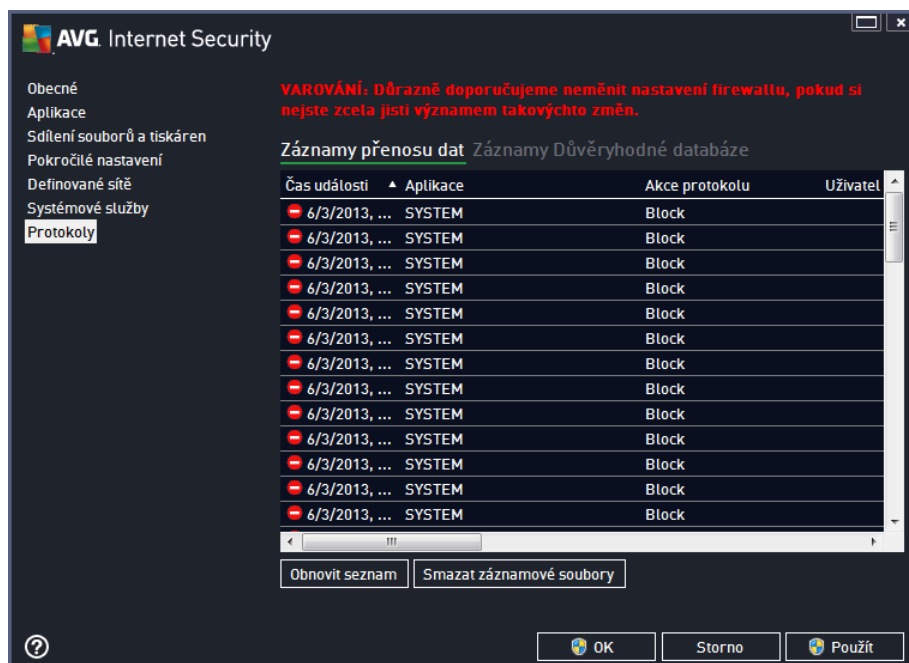
- **Obnovit seznam** - stiskem tlačítka provedete aktualizaci záznamů v seznamu událostí
- **Zavřít** - stiskem tlačítka se vrátíte zpět do [hlavního okna](#) **AVG Internet Security 2014**

14.7. Protokol Firewallu

Tento dialog je určen výhradně pro expertní konfiguraci. Doporuujeme, abyste neměnili žádné nastavení, pokud si nejste absolutně jisti dopadem případných změn!

Dialog **Protokoly** nabízí seznamy všech protokolovaných událostí Firewallu s pohledem 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 době události, jméno aplikace, která se pokoušela navázat spojení, příslušnou akci protokolu, jméno uživatele, PID, směr spojení, typ protokolu, číslo vzdáleného a místního portu a informaci o vzdálené i lokální IP adrese.



- **Záznamy Důvěryhodné databáze** - Důvěryhodná databáze je interní databáze 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 jakékoli 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 editovat podle zvoleného atributu: data chronologicky, ostatní sloupce abecedně (klikněte na nadpis příslušného sloupce). Tlačítkem **Obnovit seznam** pak můžete zobrazené informace aktualizovat.
- **Smazat záznamové soubory** - Stiskem tlačítka odstraní všechny záznamy z tabulky.



15. Aktualizace AVG

Každý bezpečnostní software má za úkol 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 nezbytné Váš **AVG Internet Security 2014** pravidelně aktualizovat. V ideálním případě ponechte prosím program ve výchozím nastavení, kdy je zapnuta automatická aktualizace. Bez aktuální virové databáze nebude **AVG Internet Security 2014** 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.

15.1. Spouštění aktualizace

Pro zajištění maximální bezpečnosti ověřte **AVG Internet Security 2014** ve výchozím nastavení aktualizací 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 2014** bude aktuální během celého dne.

Pokud je virová databáze v **AVG Internet Security 2014** starší než jeden týden, budete o tomto stavu informováni oznamovacím dialogem **Databáze je zastaralá**; pro vyřešení chyby spusíte 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 aktualizací souborů. Po spuštění aktualizace dojde nejprve k ověření, zda existují nové aktualizací soubory, jež dosud nebyly aplikovány. Pokud ano, **AVG Internet Security 2014** zahájí jejich okamžité stahování a spustí samotný proces aktualizace. O výsledku aktualizace budete vyrozuměni v dialogu nad ikonou AVG na systémové liště.

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 dialogích:

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

15.2. Úrovně aktualizace

AVG Internet Security 2014 rozlišuje dvě úrovně aktualizace:

- **Aktualizace definic** zajišťuje, že jste chráněni proti nejnovějším hrozbám, které by mohly poškodit váš počítač. Zahnuje 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 systém



(souborový server) doporučíme 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 soubihu naplánované programové aktualizace a naplánovaného testu, proces aktualizace je považován za prioritní a test bude přerušeno. O případné kolizi budete informováni.



16. FAQ a technická podpora

Máte-li s Vaší aplikací **AVG Internet Security 2014** 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:** Pokud máte z prostředí aplikace AVG nějaké potíže, můžete přejít do specifické sekce webu AVG (<http://www.avg.com/cz-cs/homepage>), která je vyhrazena zákaznické podpoře. V hlavním menu zvolte položku **Nápověda / Získat podporu**. Budete automaticky přemístěni na příslušnou stránku s nabídkou dostupné podpory. Dále prosím postupujte podle pokynů uvedených na webu.
- **Podpora (v hlavním menu):** Systémové menu aplikace AVG (v horní liště hlavního dialogu) obsahuje položku **Podpora**. Ta otevírá nový dialog s kompletním výběrem informací, které můžete potřebovat při kontaktu se zákaznickou podporou. Dialog dále obsahuje základní údaje o instalovaném programu AVG (verze programu a databáze), licenční údaje a seznam odkazů na zdroje podpory.
- **Řešení potíží v nápovědě:** Pokud v nápovědě programu **AVG Internet Security 2014** je nově k dispozici sekce **Řešení potíží** (soubor nápovědy lze otevřít z kteréhokoliv dialogu aplikace stiskem klávesy F1). Ta nabízí výběr nejčastějších situací technického rázu, v nichž si uživatel může vyhledat odbornou pomoc. Zvolte prosím položku, která nejlépe vystihuje Váš aktuální problém a po rozkliknutí se otevře návod s podobným postupem doporučeným pro tuto situaci.
- **Centrum podpory na webu AVG:** Alternativní možností je vyhledat řešení svého problému na webu AVG (<http://www.avg.com/cz-cs/homepage>). V sekci **Centrum podpory** najdete strukturovaný přehled tematických okruhů, které řeší problémy obchodního i technického charakteru.
- **Časté dotazy:** Na webu AVG (<http://www.avg.com/cz-cs/homepage>) najdete také samostatnou a detailnějším způsobem nastavených otázek. Tato sekce je dostupná přes **Centrum podpory / Časté dotazy a návody**. Otázky jsou opět přehledně rozděleny do kategorií obchodní, technické a virové.
- **AVG ThreatLabs:** Samostatná AVG stránka (<http://www.avg.com/about-viruses>) je věnována virové tematice a poskytuje strukturovaný přehled informací souvisejících s hrozbami online. Najdete zde také rady, jak odstranit viry, spyware a jak zůstat trvale chráněni.
- **Diskusní fórum:** Můžete také využít diskusního fóra pro uživatele AVG produktů na adrese <http://forums.avg.com>.