AVG AntiVirus 2013

Používateľská príručka

Revízia dokumentu 2013.11 (13.2.2013.)

Copyright AVG Technologies CZ, s.r.o. Všetky práva vyhradené.
Všetky ostatné ochranné známky sú vlastníctvom príslušných vlastníkov.

Tento produkt používa algoritmus MD5 Message-Digest spoločnosti RSA Data Security, Inc., Copyright (C) 1991 – 1992, RSA Data Security, Inc. spoločnosť bola založená v roku 1991.
Tento produkt používa kód z knižnice C-SaCzech, Copyright (c) 1996 – 2001 Jaromir Dolecek (dolecek@ics.muni.cz).
Tento produkt používa knižnicu kompresie zlib, Copyright (c) 1995 – 2002 Jean-loup Gailly a Mark Adler.
Tento produkt používa knižnicu kompresie libbzip2, Copyright (c) 1996 – 2002 Julian R Seward.

Obsah

1. Úvod 5

2. Požiadavky na inštaláciu produktu AVG 6

2.1 Podporované operačné systémy 6
2.2 Minimálne a odporúčané hardvérové požiadavky 6

3. Proces inštalácie produktu AVG 7

3.1 Vitajte! Výber jazyka 7
3.2 Vitajte! Licenčná zmluva 8
3.3 Aktivujte si licenciu 9
3.4 Výber typu inštalácie 10
3.5 Vlastné možnosti 11
3.6 Nainštalovať AVG Security Toolbar 12
3.7 Priebeh inštalácie 13
3.8 Inštalácia prebehla úspešne 14

4. Po inštalácii 15

4.1 Registrácia produktu 15
4.2 Otvorenie používateľského rozhrania 15
4.3 Kontrola celého počítača 15
4.4 Test EICAR 15
4.5 Predvolená konfigurácia AVG 16

5. Používateľské rozhranie AVG 17

5.1 Horný navigačný rad 18
5.2 Informácie o stave zabezpečenia 22
5.3 Prehľad súčastí 23
5.4 Moje aplikácie 24
5.5 Kontrola/Aktualizovať rýchle odkazy 25
5.6 Ikona v paneli úloh 25
5.7 Miniaplikácia AVG 27
5.8 AVG Advisor 28
5.9 AVG Akcelerátor 29

6. Súčasti AVG 30

6.1 Počítač 30
6.2 Web 31
6.3 Identita 33

6.4 E-maily 35
6.5 Quick Tune 37

7. AVG Security Toolbar 39

8. AVG Do Not Track 41

8.1 Rozhranie aplikácie AVG Do Not Track 41
8.2 Informácie o sledovacích procesoch 43
8.3 Blokovanie sledovacích procesov 44
8.4 Nastavenia aplikácie AVG Do Not Track 44

9. Rozšírené nastavenia programu AVG 46

9.1 Vzhľad 46
9.2 Zvuky 49
9.3 Dočasne vypnúť ochranu AVG 50
9.4 Ochrana počítača 51
9.5 Kontrola pošty 56
9.6 Ochrana prezerania webu 66
9.7 Identity Protection 69
9.8 Kontroly 70
9.9 Plány 75
9.10 Aktualizácia 83
9.11 Výnimky 87
9.12 Vírusový trezor 89
9.13 AVG Sebaochrana 90
9.14 Preferencie ochrany osobných údajov 90
9.15 Ignorovať chybný stav 93
9.16 Aplikácia Advisor – známe siete 94

10. Kontrola programom AVG 95

10.1 Vopred definované kontroly 96
10.2 Kontrola z prieskumníka 104
10.3 Kontrola z príkazového riadka 105
10.4 Plánovanie kontroly 107
10.5 Výsledky kontrol 115
10.6 Podrobnosti výsledkov kontrol 117

11. Vírusový trezor 118

12. História 120

12.1 Výsledky kontrol 120
12.2 Nálezy súčasti Rezidentný štít 121
12.3 Nálezy súčasti Ochrana e-mailu 124
12.4 Nálezy súčasti Webový štít 125
12.5 Protokol histórie udalostí 127

13. Aktualizácie AVG 128

13.1 Spustenie aktualizácie 128
13.2 Úrovne aktualizácie 128

14. FAQ a technická podpora 130

1. Úvod

Táto príručka podrobne dokumentuje produkt **AVG AntiVirus 2013**.

Produkt

Produkt **AVG AntiVirus 2013** ponúka ochranu pred najdômyselnejšími súčasnými hrozbami v reálnom čase. Môžete v bezpečí chatovať, preberať a vymieňať si súbory, hrať hry a sledovať videá bez akéhokoľvek prerušenia. Môžete preberať a zdieľať súbory a bezpečne odosielať správy, používať sociálne siete a surfovať či vyhľadávať informácie s ochranou v reálnom čase.

2. Požiadavky na inštaláciu produktu AVG

2.1. Podporované operačné systémy

AVG AntiVirus 2013 sa používa na ochranu počítačov s týmito operačnými systémami:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (32-bitová a 64-bitová verzia, všetky edície)
- Windows 7 (32-bitová a 64-bitová verzia, všetky edície)
- Windows 8 (32- a 64-bitový

(a prípadne s novšími balíkmi Service Pack – platí pre určité operačné systémy)

***Poznámka**: Súčasť Identita nepodporuje 64-bitové operačné systémy Windows XP. Produkt AVG AntiVirus 2013 sa môže inštalovať pod týmto operačným systémom, ale bez súčasti IDP.*

2.2. Minimálne a odporúčané hardvérové požiadavky

Minimálne hardvérové požiadavky pre produkt **AVG AntiVirus 2013**:

- Procesor Intel Pentium 1,5 GHz alebo rýchlejší
- 512 MB (Windows XP)/1 024 MB (Windows Vista, Windows 7) pamäte RAM
- 1,3 GB voľného miesta na pevnom disku *(na účely inštalácie)*

Odporúčané hardvérové požiadavky pre produkt **AVG AntiVirus 2013**:

- Procesor Intel Pentium 1,8 GHz alebo rýchlejší
- 512 MB (Windows XP)/1 024 MB (Windows Vista, Windows 7) pamäte RAM
- 1,6 GB voľného miesta na pevnom disku *(na účely inštalácie)*

3. Proces inštalácie produktu AVG

Na nainštalovanie programu **AVG AntiVirus 2013** do počítača sa musí použiť najnovší inštalačný súbor. Aby ste sa uistili, že inštalujete najnovšiu verziu aplikácie **AVG AntiVirus 2013**, odporúčame vám prevziať inštalačný súbor priamo z webovej lokality spoločnosti AVG (http://www.avg.com/). V časti ***Centrum podpory/Na prevzatie*** sa nachádza štruktúrovaný prehľad inštalačných súborov pre každú z edícií AVG.

Ak neviete, ktoré súbory treba nainštalovať, môžete využiť službu ***Vybrať produkt*** v spodnej časti webovej lokality. Odpoviete na tri jednoduché otázky a služba vyberie súbory presne podľa vašich potrieb. Stlačením tlačidla ***Pokračovať*** budete presmerovaní na úplný zoznam súborov na prevzatie prispôsobených podľa vašich požiadaviek.

Po prevzatí a uložení inštalačného súboru na pevný disk môžete spustiť proces inštalácie. Postup inštalácie predstavuje rad následných jednoduchých a prehľadných dialógových okien. Každé dialógové okno obsahuje stručné informácie o jednotlivých krokoch procesu inštalácie. Ďalej ponúkame podrobné vysvetlenia každého z dialógových okien:

3.1. Vitajte! Výber jazyka

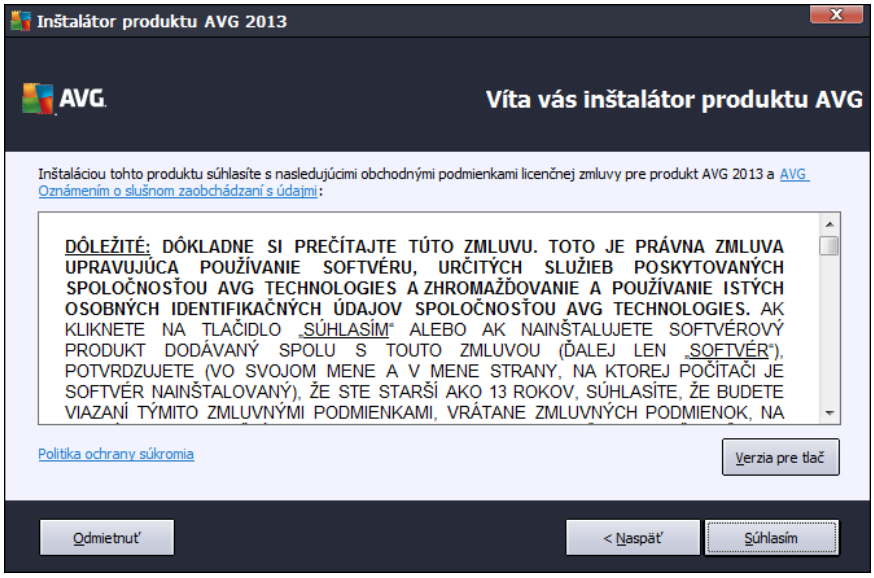
Proces inštalácie začína dialógovým oknom ***Víta vás sprievodca inštaláciou AVG***:

V tomto dialógovom okne zvolíte jazyk, ktorý sa použije pri procese inštalácie. Kliknutím na rozbaľovacie pole zobrazíte ponuku jazykov. Vyberte požadovaný jazyk a proces inštalácie sa posunie k výberu jazyka.

Pozor: Teraz vyberáte iba jazyk procesu inštalácie. Aplikácia AVG AntiVirus 2013 sa nainštaluje vo zvolenom jazyku a v angličtine, v ktorej sa vždy inštaluje automaticky. Vždy je však možné nainštalovať viac jazykov a pracovať s aplikáciou AVG AntiVirus 2013 v ktoromkoľvek z nich. V jednom z nasledujúcich dialógových okien Vlastné možnosti dostanete možnosť potvrdiť výber alternatívnych jazykov.

3.2. Vitajte! Licenčná zmluva

Dialógové okno ***Víta vás sprievodca inštaláciou AVG*** ponúka úplné znenie licenčnej zmluvy AVG:



Pozorne si celý text prečítajte. Na potvrdenie, že ste si prečítali a pochopili zmluvu a súhlasíte s jej znením stlačte tlačidlo ***Súhlasím***. Ak nesúhlasíte s licenčnou zmluvou, stlačte tlačidlo ***Nesúhlasím*** a proces inštalácie sa ihneď ukončí.

Ochrana osobných údajov v spoločnosti AVG

Okrem licenčnej zmluvy ponúka toto inštalačné okno aj možnosť zistiť viac o ***Zásadách slušnosti pri spracovaní údajov v spoločnosti AVG*** , ***personalizácii AVG*** a ***Ochrane osobných údajov v spoločnosti AVG*** *(všetky uvedené funkcie sú zobrazené v dialógovom okne v podobe aktívneho hypertextového odkazu, ktorý vás presmeruje na príslušnú webovú lokalitu s podrobnejšími informáciami)*. Kliknutím na príslušný odkaz budete presmerovaní na webovú lokalitu AVG (http://www.avg.com/, kde nájdete plné znenie týchto vyjadrení.

Ovládacie tlačidlá

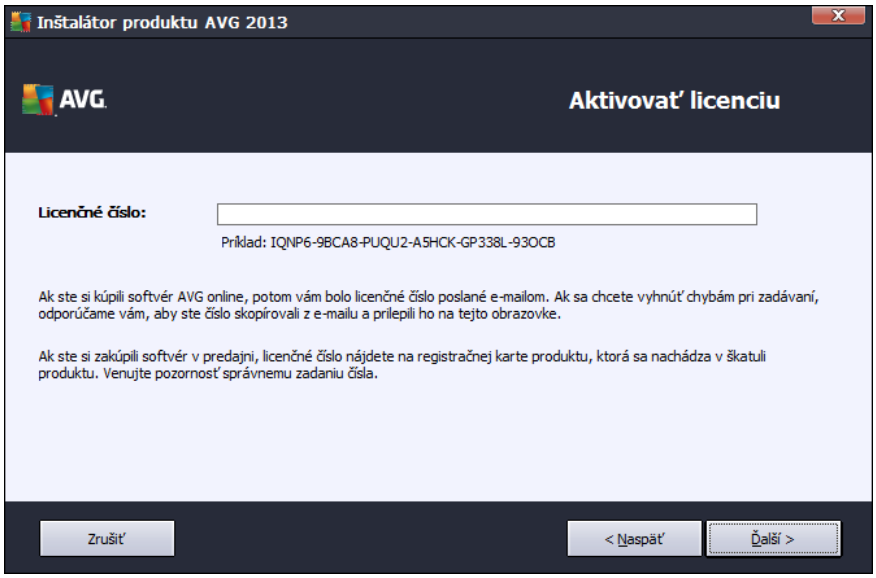
V prvom dialógovom okne inštalácie sa nachádzajú iba dve ovládacie tlačidlá:

- ***Verzia pre tlač*** – Kliknutím na toto tlačidlo zobrazíte plné znenie licenčnej zmluvy AVG určené tak pre zobrazenie na webe, ako aj upravené pre tlač.
- ***Zamietnuť*** – Kliknutím na toto tlačidlo odmietnete podmienky licenčnej zmluvy. Inštalačný postup sa okamžite ukončí. Aplikácia **AVG AntiVirus 2013** sa nenainštaluje!
- ***Naspäť*** – Kliknutím sa vrátite o jeden krok k predchádzajúcemu dialógovému oknu inštalácie.
- ***Prijať*** – Kliknutím na toto tlačidlo potvrdíte, že ste prečítali, pochopili a prijali podmienky

licenčnej zmluvy. Inštalácia bude pokračovať a zobrazí sa ďalšie inštalačné dialógové okno.

3.3. Aktivujte si licenciu

V dialógovom okne ***Aktivujte si licenciu*** zadajte licenčné číslo do príslušného textového poľa:



Kde nájsť licenčné číslo

Predajné číslo sa nachádza na obale disku CD v škatuli produktu **AVG AntiVirus 2013**. Licenčné číslo sa nachádza v e-mailovej správe s potvrdením, ktorú ste dostali po zakúpení produktu **AVG AntiVirus 2013** on-line. Číslo sa musí zadať presne tak, ako je uvedené. Ak máte k dispozícii licenčné číslo v digitálnej podobe (*v e-mailovej správe*), na jeho vloženie vám odporúčame použiť funkciu kopírovať a prilepiť.

Ako používať metódu Kopírovať a Prilepiť

Pomocou metódy ***Kopírovať a Prilepiť*** vložte licenčné číslo produktu **AVG AntiVirus 2013** do programu. Tak zabezpečíte zadanie správneho čísla. Postupujte podľa nasledujúcich pokynov:

- Otvorte e-mail s licenčným číslom
- Kliknite ľavým tlačidlom myši na začiatok licenčného čísla, podržte tlačidlo stlačené a presuňte kurzor myši na koniec čísla. Potom tlačidlo uvoľnite. Číslo by sa malo zvýrazniť.
- Stlačte a podržte kláves ***Ctrl*** a stlačte kláves ***C***. Tým číslo skopírujete.
- Nasmerujte kurzor a kliknite na miesto, kam chcete skopírované číslo vložiť.
- Stlačte a podržte kláves ***Ctrl*** a stlačte kláves ***V***. Tým prilepíte číslo na vybrané miesto.

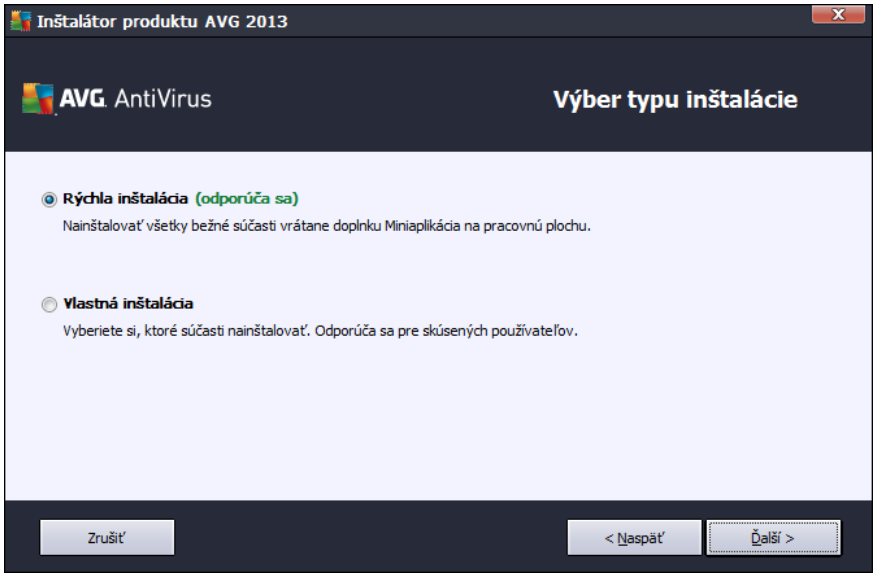
Ovládacie tlačidlá

Ako väčšina dialógových okien, aj toto má k dispozícii tri ovládacie tlačidlá:

- ***Zrušiť*** – Kliknutím okamžite ukončíte priebeh inštalácie. Aplikácia **AVG AntiVirus 2013** sa nenainštaluje!
- ***Naspäť*** – Kliknutím sa vrátite o jeden krok k predchádzajúcemu dialógovému oknu inštalácie.
- ***Ďalej*** – Kliknutím posuniete priebeh inštalácie o krok ďalej.

3.4. Výber typu inštalácie

Dialógové okno ***Vyberte typ inštalácie*** ponúka dve možnosti inštalácie: ***Expresnú*** a ***Vlastnú inštaláciu***:



Expresná inštalácia

Väčšine používateľov odporúčame ponechať štandardnú ***expresnú*** inštaláciu. Takto nainštalujete program **AVG AntiVirus 2013** v plne automatickom režime s nastaveniami vopred definovanými dodávateľom programu, vrátane Miniaplikácie AVG, súčasti AVG Security Toolbara nastavením súčasti AVG Secure Search ako predvoleného poskytovateľa vyhľadávania. Táto konfigurácia poskytuje maximálne zabezpečenie s optimálnym využitím zdrojov. Ak v budúcnosti budete chcieť zmeniť konfiguráciu, vždy to bude možné priamo v aplikácii **AVG AntiVirus 2013**.

Stlačením tlačidla ***Ďalej*** pokračujte k ďalšiemu dialógovému oknu procesu inštalácie.

Vlastná inštalácia

Vlastnú inštaláciu by mali používať len skúsení používatelia, ktorí majú skutočný dôvod inštalovať produkt **AVG AntiVirus 2013** s neštandardnými nastaveniami, napr. na účely prispôsobenia konkrétnym systémovým potrebám. Ak sa rozhodnete pre túto možnosť, v dialógovom okne sa zobrazí nová časť s názvom ***Cieľový priečinok***. Tu môžete zadať umiestnenie, kam sa produkt **AVG AntiVirus 2013** má nainštalovať. Produkt **AVG AntiVirus 2013** sa štandardne inštaluje do priečinka Program Files na disku C:, ako je to uvedené v textovom poli dialógového okna. Ak si želáte zmeniť toto miesto, tlačidlom ***Prehľadávať*** otvorte prehľad diskových jednotiek a vyberte príslušný priečinok. Na obnovenie predvoleného umiestnenia nastaveného dodávateľom softvéru použite tlačidlo ***Predvolené***.

Potom stlačte tlačidlo ***Ďalej***. Otvorí sa dialógové okno Vlastné možnosti.

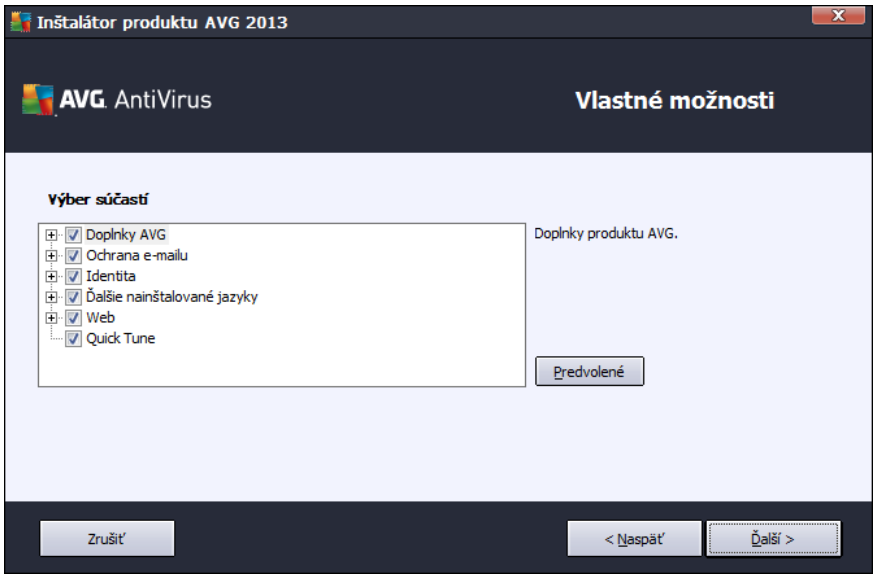
Ovládacie tlačidlá

Ako väčšina dialógových okien, aj toto má k dispozícii tri ovládacie tlačidlá:

- ***Zrušiť*** – Kliknutím okamžite ukončíte priebeh inštalácie. Aplikácia **AVG AntiVirus 2013** sa nenainštaluje!
- ***Naspäť*** – Kliknutím sa vrátite o jeden krok k predchádzajúcemu dialógovému oknu inštalácie.
- ***Ďalej*** – Kliknutím posuniete priebeh inštalácie o krok ďalej.

3.5. Vlastné možnosti

Dialógové okno ***Vlastné možnosti*** umožňuje nastaviť podrobné parametre inštalácie:



V časti ***Výber súčastí*** sa nachádza prehľad všetkých súčastí programu **AVG AntiVirus 2013**, ktoré

je možné inštalovať. Ak vám predvolené nastavenia nevyhovujú, môžete odstrániť/pridať špecifické komponenty. ***Môžete však vybrať len tie súčasti, ktoré sú súčasťou edície AVG, ktorú ste si zakúpili!*** Zvýraznite položku v zozname ***Výber súčastí*** a na pravej strane v tejto časti sa zobrazia stručné informácie o príslušnej súčasti. Ďalšie informácie o funkcionalite jednotlivých súčastí sa nachádzajú v kapitole Prehľad súčastí v tejto dokumentácii. Na obnovenie predvolenej konfigurácie nastavenej dodávateľom softvéru použite tlačidlo ***Predvolené***.

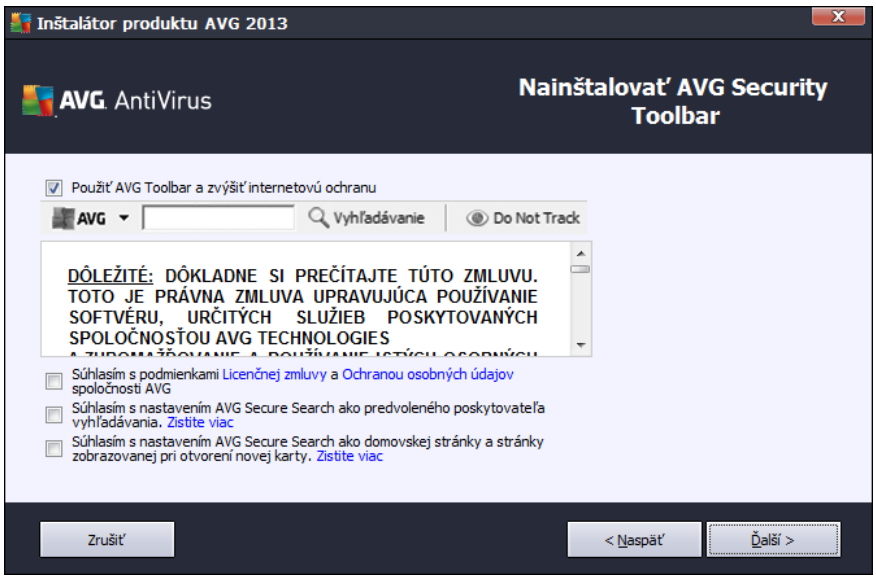
Ovládacie tlačidlá

Ako väčšina dialógových okien, aj toto má k dispozícii tri ovládacie tlačidlá:

- ***Zrušiť*** – Kliknutím okamžite ukončíte priebeh inštalácie. Aplikácia **AVG AntiVirus 2013** sa nenainštaluje!
- ***Naspäť*** – Kliknutím sa vrátite o jeden krok k predchádzajúcemu dialógovému oknu inštalácie.
- ***Ďalej*** – Kliknutím posuniete priebeh inštalácie o krok ďalej.

3.6. Nainštalovať AVG Security Toolbar

V dialógovom okne ***Inštalácia súčasti AVG Security Toolbar*** nastavte, či sa má nainštalovať súčasť ***AVG Security Toolbar***. Ak nezmeníte predvolené nastavenia, potom sa táto súčasť nainštaluje automaticky do internetového prehliadača (*v súčasnosti sú podporované prehliadače Microsoft Internet Explorer vo verzii 6.0 a vyššej a Mozilla Firefox vo verzii 3.0 a vyššej*) a bude sa starať o komplexnú ochranu počas surfovania na internete. V súčasnosti medzi podporované prehľadávače patrí Internet Explorer (*verzia 6.0 a novšia*) alebo Mozilla Firefox (*verzia 3.0 a novšia*). Iné prehliadače nie sú podporované *(ak používate alternatívny internetový prehliadač (napr. Avant Browser), môžete sa stretnúť s neočakávaným správaním).*



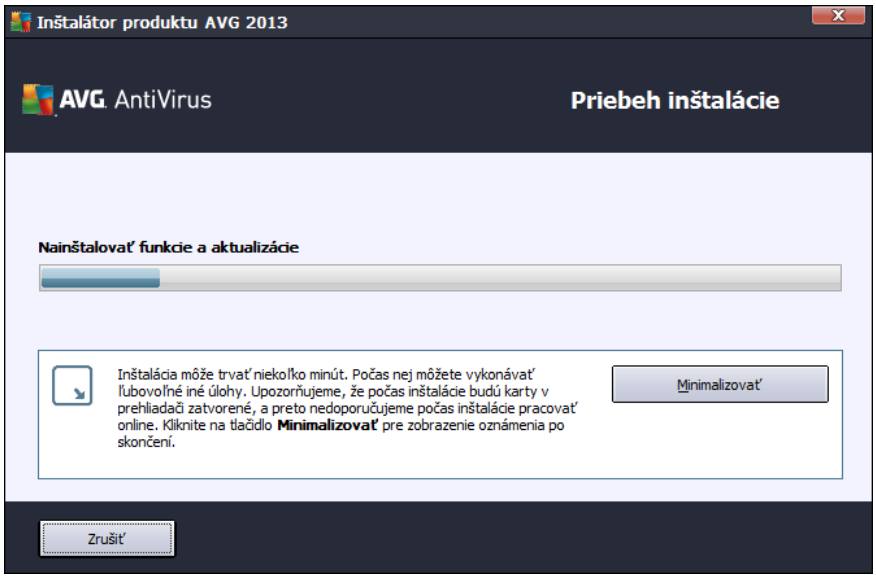
V dialógovom okne sa môžete rozhodnúť ohľadne tejto konfigurácie:

- ***Nastaviť službu AVG Secure Search ako predvoleného poskytovateľa vyhľadávania a zachovať toto nastavenie*** – nechajte políčko zaškrtnuté, čím potvrdíte, že chcete používať ako poskytovateľa vyhľadávania vyhľadávací nástroj AVG Secure Search, ktorý úzko spolupracuje s komponentom Link Scanner Surf Shield na zabezpečení vašej najvyššej bezpečnosti on-line.

- ***Nainštalovať panel nástrojov AVG Security Toolbar na zvýšenie internetovej ochrany*** – nechajte políčko zaškrtnuté, aby sa nainštaloval panel nástrojov AVG Security Toolbar, ktorý zabezpečí vašu maximálnu bezpečnosti pri prehliadaní internetu.

3.7. Priebeh inštalácie

Dialógové okno ***Priebeh inštalácie*** informuje o priebehu procesu inštalácie a používateľ v ňom nemusí nič robiť:



Po dokončení procesu inštalácie sa automaticky otvorí ďalšie dialógové okno.

Ovládacie tlačidlá

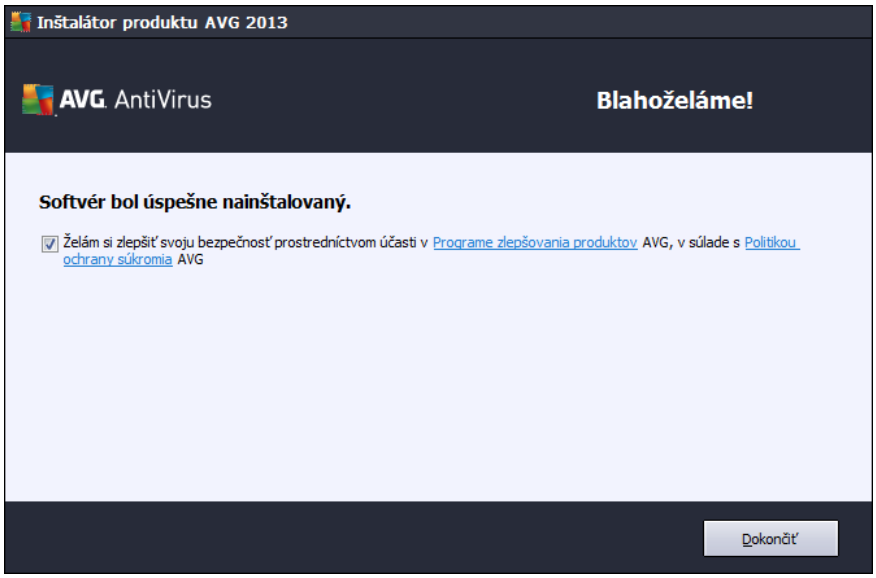
V tomto dialógovom okne sa nachádzajú dve ovládacie tlačidlá:

- ***Minimalizovať*** – Proces inštalácie môže trvať niekoľko minút. Kliknutím na toto tlačidlo minimalizujete dialógové okno na ikonu na systémovej lište. Toto okno sa otvorí po dokončení inštalácie.

- ***Zrušiť*** – Toto tlačidlo použite iba vtedy, keď chcete zastaviť proces inštalácie. Nezabudnite, že v takom prípade sa aplikácia **AVG AntiVirus 2013** nenainštaluje!

3.8. Inštalácia prebehla úspešne

Dialógové okno ***Inštalácia prebehla úspešne*** potvrdí, že sa program **AVG AntiVirus 2013** celý nainštaloval a nastavil:



Program zlepšovania produktov a Ochrana osobných údajov

Tu sa môžete rozhodnúť, či sa chcete podieľať na ***programe zlepšovania produktov*** (*podrobnosti nájdete v kapitole Rozšírené nastavenia programu AVG/Program zlepšovania produktov*), ktorý zhromažďuje anonymné informácie o zistených hrozbách s cieľom zvýšiť celkovú úroveň zabezpečenia na internete. So všetkými údajmi spoločnosť AVG narába ako s dôvernými a v zhode so zásadami Ochrany osobných údajov v spoločnosti AVG. Kliknutím na odkaz ***Ochrana osobných údajov*** budete presmerovaní na webovú lokalitu AVG http://www.avg.com/, kde nájdete plné znenie zásad ochrany osobných údajov v spoločnosti AVG. Ak súhlasíte, nechajte túto možnosť začiarknutú *(možnosť je štandardne začiarknutá)*.

Inštaláciu dokončite stlačením tlačidla ***Dokončiť***.

4. Po inštalácii

4.1. Registrácia produktu

Po nainštalovaní produktu **AVG AntiVirus 2013** zaregistrujte produkt on-line na webovej lokalite AVG (*http://www.avg.com/*). Registráciou získate úplný prístup k používateľskému účtu AVG, informáciám o aktualizáciách AVG a ďalším službám poskytovaným výhradne registrovaným používateľom. Najjednoduchší spôsob registrácie je priamo z používateľského rozhrania aplikácie **AVG AntiVirus 2013**. Označte položku v hornom navigačnom pruhu Možnosti/Zaregistrovať teraz. Budete presmerovaní na stránku ***Registrácia*** na webovej lokalite AVG *(http://www.avg.com/)*. Postupujte podľa pokynov na tejto stránke.

4.2. Otvorenie používateľského rozhrania

Hlavné dialógové okno AVG sa otvára niekoľkými spôsobmi:

- Dvakrát kliknite na ikonu AVG v paneli úloh
- Dvakrát kliknite na ikonu AVG na pracovnej ploche
- v ponuke ***Štart/Všetky programy/AVG/AVG 2013***

4.3. Kontrola celého počítača

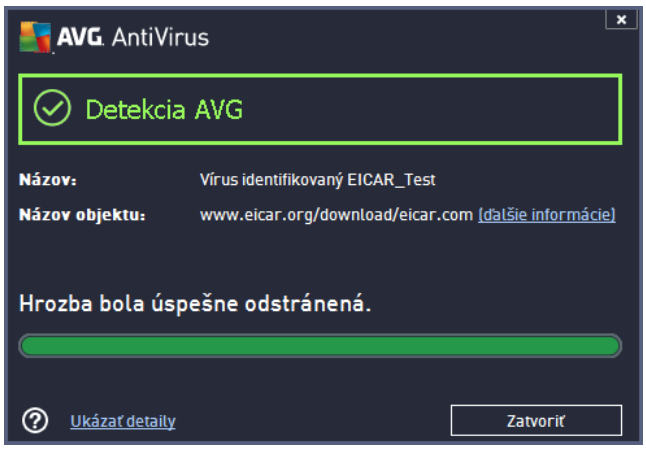
Existuje potenciálne riziko, že sa do vášho počítača dostal počítačový vírus ešte pred nainštalovaním produktu **AVG AntiVirus 2013**. Z tohto dôvodu by ste mali spustiť Kontrolu celého počítača, aby sa vylúčila možnosť existencie infekcie v počítači. Prvá kontrola môže istý čas trvať *(približne hodinu)*, no odporúča sa ju nechať dokončiť, aby ste sa uistili, že váš počítač nie je v ohrození. Pokyny na spustenie Kontroly celého počítača sa nachádzajú v kapitole Kontrola programom AVG.

4.4. Test EICAR

Na kontrolu, či sa program **AVG AntiVirus 2013** nainštaloval správne, môžete použiť test EICAR.

Test EICAR je štandardná a absolútne bezpečná metóda, ktorá sa používa na testovanie funkcie antivírusového systému. Je bezpečná, pretože v skutočnosti nejde o vírus a neobsahuje žiadne fragmenty vírusového kódu. Väčšina produktov naň reaguje ako na vírus (*aj keď ho obyčajne označí jednoznačným názvom, ako napríklad „EICAR-AV-Test“*). Vírus EICAR si môžete prevziať na internetových stránkach EICAR na adrese www.eicar.com, kde nájdete aj všetky potrebné informácie o teste EICAR.

Prevezmite si súbor *eicar.com* a uložte ho na pevný disk počítača. Hneď po potvrdení prevzatia testovacieho súboru program **AVG AntiVirus 2013** naň zareaguje varovaním. Zobrazenie tohto oznámenia znamená, že je program AVG správne nainštalovaný v počítači.



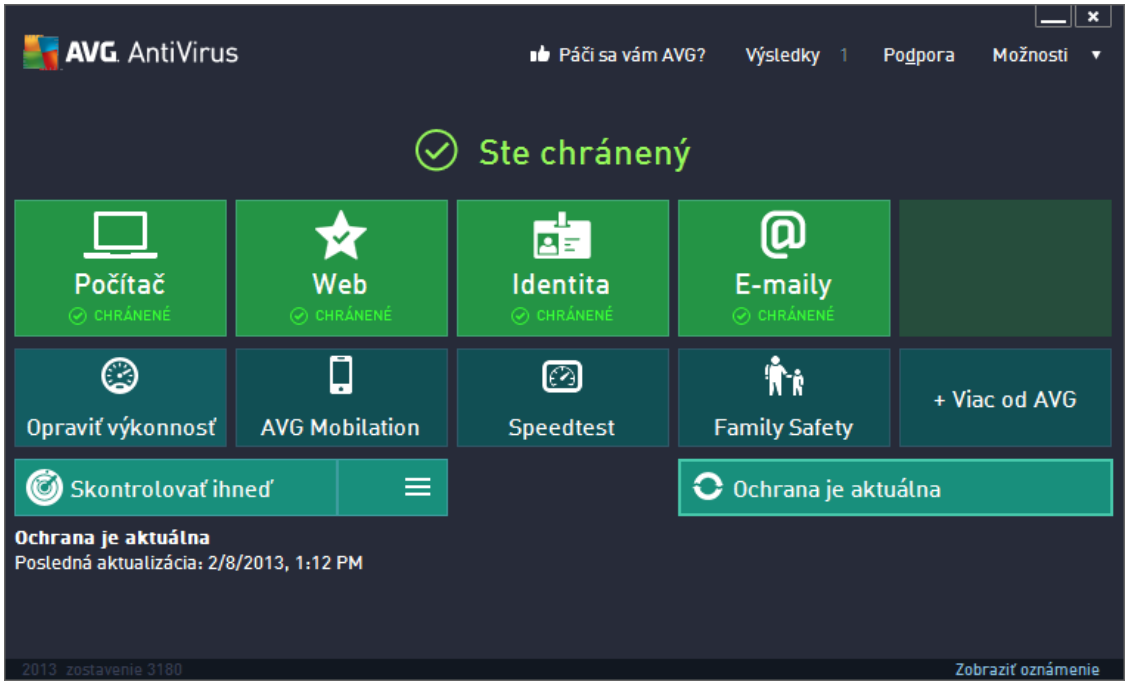
Ak sa programu AVG nepodarí identifikovať testovací súbor EICAR ako vírus, skontrolujte ešte raz konfiguráciu programu!

4.5. Predvolená konfigurácia AVG

Predvolenú konfiguráciu, (*t. j. nastavenie aplikácie bezprostredne po inštalácii*) produktu **AVG AntiVirus 2013,** nastavil dodávateľ softvéru tak, aby všetky súčasti a funkcie fungovali optimálnym spôsobom. ***Nemeňte konfiguráciu AVG, ak na to nemáte vážny dôvod! Zmeny nastavení by mali vykonávať len skúsení používatelia.*** Ak chcete upraviť konfiguráciu programu AVG podľa svojich potrieb, prejdite do časti Rozšírené nastavenia programu AVG: vyberte položku Hlavnej ponuky *Možnosti/Rozšírené nastavenia* a upravte konfiguráciu programu AVG v novootvorenom dialógovom okne Rozšírené nastavenia programu AVG.

5. Používateľské rozhranie AVG

AVG AntiVirus 2013 sa otvára v hlavnom okne:



Hlavné okno je rozdelené na niekoľko častí:

- ***Navigácia v hornom riadku*** obsahuje štyri aktívne odkazy zoradené v hornej časti hlavného okna *(Páči sa mi AVG, Výsledky, Podpora, Možnosti)*. Detaily >>
- ***Informácie o stave zabezpečenia*** je časť so základnými informáciami o aktuálnom stave vášho **AVG AntiVirus 2013**. Detaily >>
- ***Prehľad nainštalovaných súčastí*** nájdete vo vodorovnom pruhu blokov v strednej časti hlavného okna. Súčasti sú zobrazené ako zelené obdĺžniky s ikonou príslušnej súčasti. Poskytujú informácie o jej stave. Detaily >>
- ***Moje aplikácie*** sú graficky znázornené v dolnom pruhu hlavného okna a obsahujú prehľad aplikácií doplňujúcich **AVG AntiVirus 2013**, ktoré sú na počítači buď už nainštalované, alebo sa ich inštalácia odporúča. Detaily >>
- ***Rýchle odkazy Kontrola/Aktualizácia*** sa nachádzajú v dolnom pruhu hlavného okna. Tieto tlačidlá umožňujú okamžitý prístup k väčšine najdôležitejších a najčastejšie používaných funkcií programu AVG. Detaily >>

Okrem hlavného okna produktu **AVG AntiVirus 2013** existujú ešte dve ďalšie kontrolné súčasti, cez ktoré máte prístup k aplikácii:

- ***Ikona v paneli úloh*** sa nachádza v pravom dolnom rohu monitora *(v paneli úloh)* a zobrazuje aktuálny stav produktu **AVG AntiVirus 2013**. Detaily >>

- ***Miniaplikácia AVG*** je prístupná na bočnom paneli systému Windows (*podporovanom iba vo verziách systému Windows Vista/7/8*). Umožňuje rýchly prístup ku kontrole a aktualizácii produktu **AVG AntiVirus 2013**. Detaily >>

5.1. Horný navigačný rad

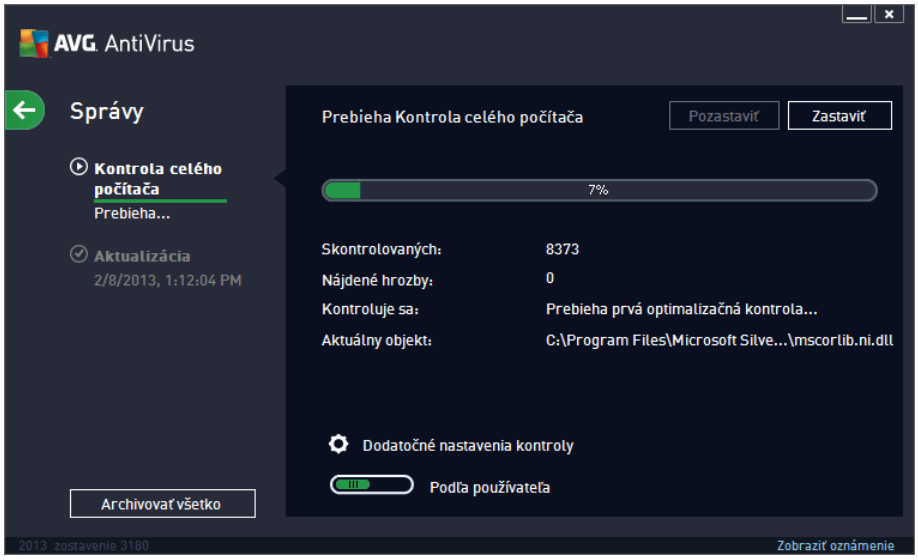
Horný navigačný rad sa skladá z radu viacerých aktívnych odkazov v hornej časti hlavného okna. Navigácia obsahuje tieto tlačidlá:

5.1.1. Páči sa mi AVG

Jedným kliknutím na odkaz sa pripojíte ku komunite AVG na sieti Facebook, kde môžete zdieľať najnovšie informácie, novinky, tipy a triky o produkte AVG pre maximálnu on-line ochranu.

5.1.2. Správy

Otvorí sa nové dialógové okno ***Správy*** s prehľadom všetkých dôležitých správ o predchádzajúcich kontrolách a aktualizáciách. Ak práve prebieha kontrola alebo aktualizácia, vedľa textu ***Správy*** v hornom navigačnom pruhu hlavného používateľského rozhrania sa zobrazí otáčajúci sa krúžok. Kliknutím na tento krúžok sa zobrazí dialógové okno s informáciami o stave prebiehajúceho procesu:



5.1.3. Podpora

Otvorí sa nové dialógové okno rozdelené na štyri záložky, v ktorých sa nachádzajú všetky dôležité informácie o aplikácii **AVG AntiVirus 2013**:

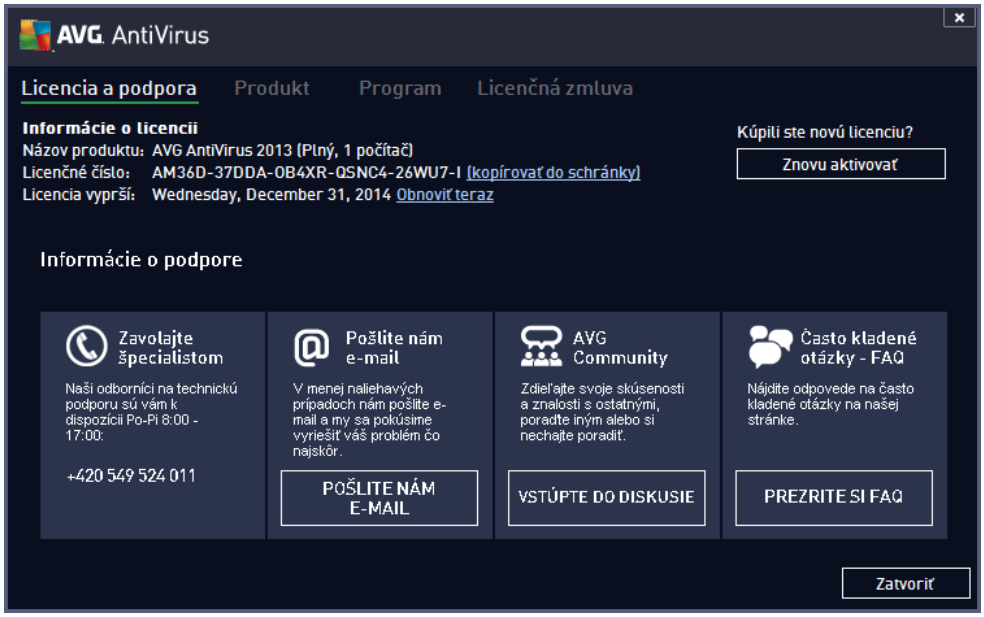
- ***Licencia a podpora*** – Táto záložka obsahuje informácie o názve produktu, licenčnom čísle a dátume exspirácie. V dolnej časti dialógového okna nájdete tiež zrozumiteľne zostavený prehľad všetkých dostupných kontaktov na zákaznícku podporu. V tejto záložke sa nachádzajú tieto aktívne odkazy a tlačidlá:

  - *Znovu aktivovať* – Kliknutím otvoríte nové dialógové okno ***Aktivovať softvér AVG***. Vyplňte licenčné číslo do príslušného poľa a nahraďte tak predajné číslo *(ktoré ste používali počas AVG AntiVirus 2013 inštalácie)* alebo zmeňte aktuálne číslo licencie

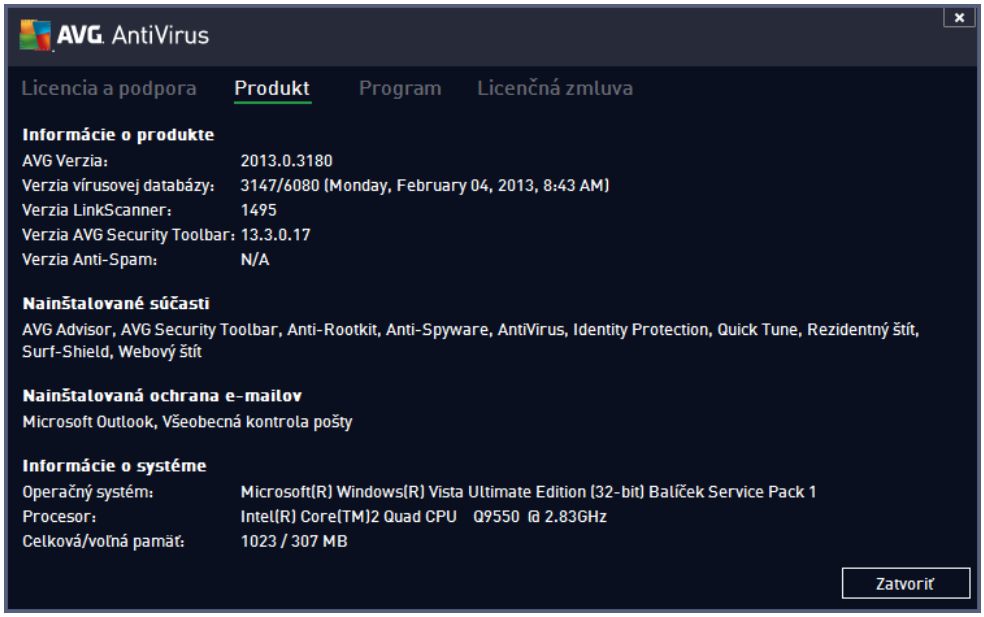
na iné *(napr. pri aktualizácii na vyšší produkt AVG)*.

- *Kopírovať do schránky* – Týmto odkazom skopírujete licenčné číslo do schránky, aby ste ho potom mohli prilepiť na miesto, kam potrebujete. Takto zaistíte, že licenčné číslo zadáte správne.

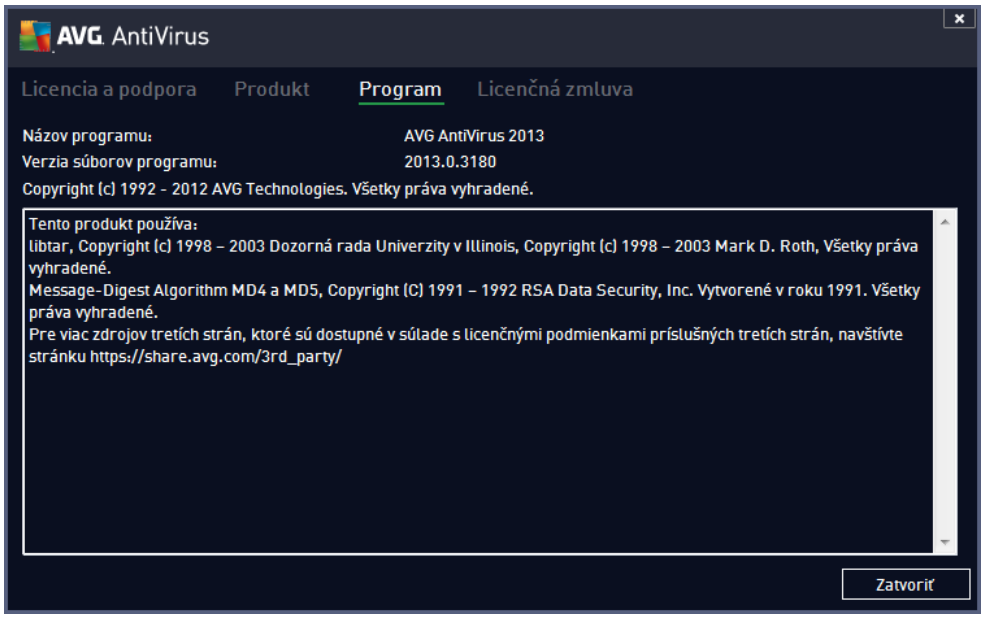
- *Obnoviť teraz* – Odporúčame, aby ste si kúpili **AVG AntiVirus 2013** obnovenie licencie v správnom čase, aspoň jeden mesiac pred vypršaním platnosti aktuálnej licencie. O blížiacom sa vypršaní platnosti budete informovaní. Týmto odkazom budete presmerovaní na webovú lokalitu AVG *(http://www.avg.com/)*, kde nájdete podrobné informácie o stave vašej licencie, jej dátume exspirácie a ponuku na obnovenie/aktualizáciu.



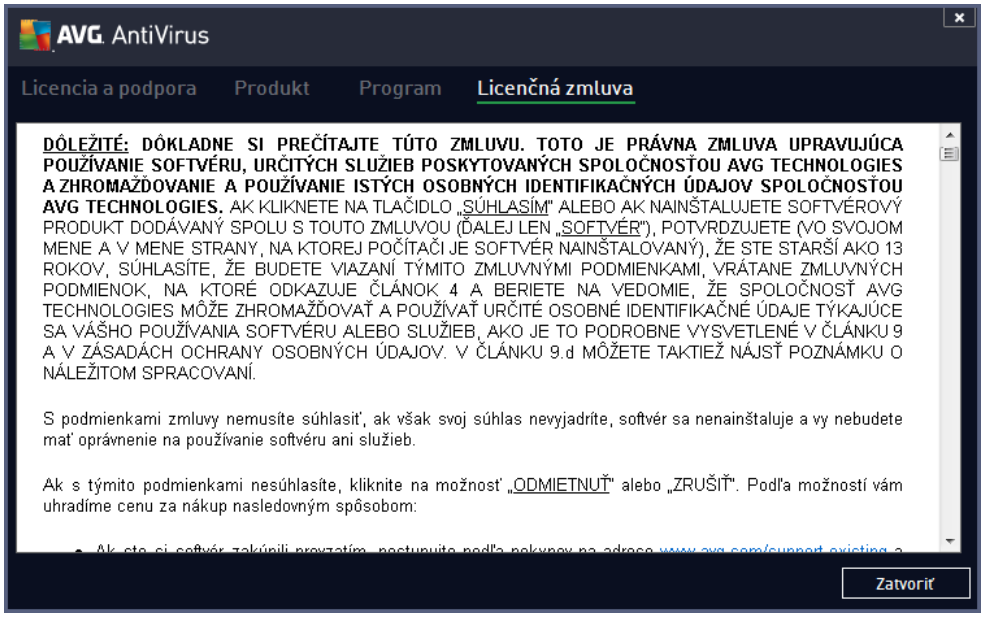
- ***Produkt*** – na tejto záložke sa nachádza prehľad **AVG AntiVirus 2013** najdôležitejších technických údajov týkajúcich sa informácií o produkte, nainštalovaných súčastiach, nainštalovanej ochrane e-mailu a informácie o systéme:



- ***Program*** – Tu sa nachádzajú údaje o verzii súboru programu a o kóde tretích strán, ktorý bol použitý pri tvorbe tohto produktu:



- ***Licenčná zmluva*** – Na tejto záložke sa nachádza plné znenie licenčnej zmluvy medzi vami a AVG Technologies:



5.1.4. Možnosti

Údržba produktu **AVG AntiVirus 2013** je dostupná prostredníctvom položky ***Možnosti***. Kliknutím na šípku otvoríte rozbaľovaciu ponuku:

- ***Skontrolovať celý počítač*** – Spustí kontrolu celého počítača.
- ***Skontrolovať vybraný priečinok...*** – Otvorí rozhranie kontroly programom AVG a pomocou stromovej štruktúry počítača umožní definovať, ktoré súbory a priečinky sa majú kontrolovať.
- ***Skontrolovať súbor...*** – Umožní vám spustiť na požiadanie test konkrétneho súboru. Kliknutím na túto možnosť sa otvorí nové okno so stromovou štruktúrou disku. Vyberte požadovaný súbor a potvrďte spustenie kontroly.
- ***Aktualizácia*** – Automaticky spustí aktualizácie produktu **AVG AntiVirus 2013**.
- ***Aktualizácia z adresára...*** – Spustí aktualizáciu z aktualizačných súborov, ktoré sa nachádzajú v nastavenom priečinku na disku počítača. Túto možnosť vám však odporúčame použiť len ako núdzové riešenie, napr. v situáciách, keď nie je vytvorené pripojenie na internet (napríklad počítač je infikovaný a odpojený od internetu; počítač je pripojený k sieti bez prístupu na internet a pod.). V novootvorenom okne vyberte priečinok, do ktorého ste predtým uložili aktualizačný súbor a spustite proces aktualizácie.
- ***Vírusový trezor*** – Otvorí rozhranie úložiska karantény (Vírusový trezor), do ktorého AVG odstraňuje všetky zistené infekcie, ktoré sa z rôznych dôvodov nedajú automaticky vyliečiť. V tejto karanténe sú infikované súbory izolované a je zaručená bezpečnosť vášho počítača a zároveň sú infikované súbory uložené pre ich budúcu možnú opravu.
- ***História*** – Ponúka ďalšie podponuky:
    - *Výsledky kontrol* – Otvorí dialógové okno s prehľadom výsledkov kontrol.

- Nálezy súčasti Rezidentný štít – Otvorí dialógové okno s prehľadom hrozieb detegovaných Rezidentným štítom.
- *Ochrana identity Identity Protection* – Otvorí dialógové okno s prehľadom hrozieb detegovaných súčasťou Identity Protection.
- Nálezy súčasti Ochrana e-mailu – Otvorí dialógové okno s prehľadom príloh e-mailových správ označených súčasťou Ochrana e-mailu ako nebezpečné.
- Nálezy súčasti Webový štít – Otvorí dialógové okno s prehľadom hrozieb zistených súčasťou Webový štít.
- Protokol histórie udalostí – Otvorí rozhranie protokolu histórie s prehľadom všetkých zaznamenaných činností aplikácie **AVG AntiVirus 2013**.

- ***Rozšírené nastavenia...*** – Otvorí dialógové okno s pokročilými nastaveniami programu AVG, kde môžete upraviť **AVG AntiVirus 2013** konfiguráciu. Odporúčame vám nemeniť predvolené nastavenia aplikácie definované výrobcom softvéru.
- ***Obsah pomocníka*** – Otvorí súbory pomocníka AVG.
- ***Získajte podporu*** – Otvorí webovú lokalitu AVG *(http://www.avg.com/)* na stránke strediska podpory zákazníkov.
- ***Vaša AVG webová stránka*** – Otvorí webovú lokalitu AVG *(http://www.avg.com/).*
- ***O vírusoch a hrozbách*** – Otvorí on-line vírusovú encyklopédiu, v ktorej si môžete vyhľadať podrobné informácie o identifikovanom víruse.
- ***Znova aktivovať*** – Otvorí sa dialógové okno ***Aktivovať AVG*** s údajmi, ktoré ste zadali pri procese inštalácie. Toto dialógové okno sa používa na vloženie licenčného čísla, buď pri nahradení predajného čísla (*čísla, s ktorým ste nainštalovali produkt AVG*), alebo pri nahradení starého licenčného čísla (*napr. pri upgradovaní na nový produkt AVG*).
- ***Zaregistrovať teraz/Môj účet*** – spojí vás s registračnou stránkou na webovej lokalite AVG http://www.avg.com/. Vyplňte vaše registračné údaje; nárok na bezplatnú technickú podporu získajú len tí zákazníci, ktorí si produkt AVG zaregistrujú. Ak používate skúšobnú verziu produktu **AVG AntiVirus 2013**, uvedené dve položky sa zobrazia v podobe ***Kúpiť teraz*** a ***Aktivovať*** a umožnia vám zakúpiť úplnú verziu programu. Ak je produkt **AVG AntiVirus 2013**nainštalovaný pomocou predajného čísla, položky sa zobrazia v podobe ***Registrovať*** a ***Aktivovať***.
- ***O AVG*** – Otvorí nové dialógové okno s tromi záložkami s údajmi o zakúpenej licencii a dostupnej podpore, produkte a s informáciami o programe. Uvedené je tu tiež plné znenie licenčnej zmluvy.

5.2. Informácie o stave zabezpečenia

Časť ***Informácie o stave zabezpečenia*** sa nachádza v hornej časti hlavného okna produktu **AVG AntiVirus 2013**. V tejto časti sa vždy nachádzajú informácie o momentálnom stave zabezpečenia programom **AVG AntiVirus 2013**. Pozrite si prehľad ikon, ktoré sa môžu nachádzať v tejto časti, a ich význam:

– Zelená ikona informuje, že produkt ***AVG AntiVirus 2013 je úplne funkčný***. Váš počítač je plne chránený, aktuálny a všetky nainštalované súčasti fungujú správne.

– Žltá ikona upozorňuje, že ***jedna súčasť alebo niekoľko súčastí je nesprávne nakonfigurovaných*** a treba venovať pozornosť ich vlastnostiam alebo nastaveniam. Nevyskytuje sa žiaden vážny problém s produktom **AVG AntiVirus 2013** a pravdepodobne ste z nejakého dôvodu vypli niektorú súčasť. Stále ste chránení. Venujte však pozornosť nastaveniam problémovej súčasti! Nesprávne nastavená súčasť sa zobrazí s varovným oranžovým pruhom v hlavnom používateľskom rozhraní.

Žltá ikona sa zobrazí aj vtedy, keď ste sa z nejakého dôvodu rozhodli ignorovať chybový stav súčasti. Voľba ***Ignorovať chybný stav*** je dostupná vo vetve Rozšírené nastavenia/Ignorovať chybný stav. Tam máte možnosť potvrdiť, že ste si vedomí chybového stavu súčasti, ale z nejakého dôvodu chcete nechať program **AVG AntiVirus 2013** v tomto stave a nechcete byť informovaní prostredníctvom ikony na paneli úloh. Môže sa vyskytnúť situácia, keď bude potrebné použiť túto možnosť; dôrazne vám však odporúčame, aby ste funkciu ***Ignorovať chybný stav*** čo najskôr znova vypli!

Žltá ikona sa zobrazí aj vtedy, ak produkt **AVG AntiVirus 2013** vyžaduje reštart počítača (***Je potrebný reštart***). Tomuto varovaniu by ste mali venovať pozornosť a reštartovať počítač.

– Oranžová ikona upozorňuje, že sa vyskytol vážny stav produktu ***AVG AntiVirus 2013***! Jedna alebo viac súčastí nefunguje správne a produkt **AVG AntiVirus 2013** nedokáže chrániť váš počítač. Venujte okamžitú pozornosť odstráneniu uvedeného problému! Ak nedokážete opraviť chybu sami, kontaktujte tím technickej podpory AVG.

Ak nie je program AVG AntiVirus 2013 nastavený tak, aby poskytoval optimálny výkon, vedľa informácie o stave zabezpečenia sa zobrazí nové tlačidlo s názvom Kliknutím opraviť (alebo Kliknutím opraviť všetko, ak sa problém týka viacerých súčastí). Stlačením tlačidla spustíte automatický proces kontroly a konfigurácie programu. Je to jednoduchý spôsob nastavenia optimálneho výkonu programu AVG AntiVirus 2013 a dosiahnutia maximálnej úrovne zabezpečenia.

Odporúčame vám, aby ste venovali pozornosť ***Informáciám o stave zabezpečenia*** a v prípade, že správa upozorňuje na problém, pokúsili sa ho ihneď odstrániť. V opačnom prípade počítač nebude dokonale chránený!

Poznámka: *Informáciu o stave produktu AVG AntiVirus 2013 vám vždy poskytuje aj ikona v paneli úloh.*

5.3. Prehľad súčastí

Prehľad nainštalovaných súčastí nájdete vo vodorovnom pruhu blokov v strednej časti hlavného okna. Súčasti sú zobrazené ako zelené obdĺžniky označené ikonou príslušnej súčasti. Každý obdĺžnik obsahuje informácie o aktuálnom stave ochrany. Ak je súčasť správne nakonfigurovaná a plne funkčná, informácie sú uvedené zelenými písmenami. Ak je súčasť pozastavená, má obmedzenú funkčnosť alebo má poruchu, zobrazí sa varovný text v oranžovom textovom poli. ***Dôrazne sa odporúča, aby ste venovali pozornosť príslušným nastaveniam súčasti.***

Presuňte kurzor myši nad súčasť. V dolnej časti hlavného okna sa zobrazí krátky text. Text uvádza základný popis funkcie súčasti. Obsahuje tiež informácie o aktuálnom stave súčasti a uvádza, ktorá

zo služieb súčasti nie je správne nakonfigurovaná.

Zoznam nainštalovaných súčastí

V programe **AVG AntiVirus 2013** sa v časti ***Prehľad súčastí*** nachádzajú informácie o týchto súčastiach:

- ***Počítač*** – tieto súčasti sa týkajú dvoch služieb: ***súčasť Rezidentný štít*** deteguje vírusy, spyware, červy, trójske kone, neželané spustiteľné súbory či knižnice v systéme a chráni vás pred škodlivým adware. Druhou súčasťou je ***Anti-Rootkit***, ktorá kontroluje nebezpečné rootkity ukryté vnútri aplikácií, ovládačov alebo knižníc. Detaily >>
- ***Prezeranie webu*** – chráni pred útokmi na webe pri vyhľadávaní a surfovaní na internete. Detaily >>
- ***Identita*** – táto súčasť spúšťa službu ***Identity Shield***, ktorá neustále chráni vaše digitálne aktíva pred novými a neznámymi hrozbami na internete. Detaily >>
- ***E-maily*** – Kontroluje prichádzajúce e-mailové správy z hľadiska prítomnosti SPAMU a blokuje vírusy, phishingové útoky či iné hrozby. Detaily >>

Dostupné činnosti

- ***Presunutím kurzora myši nad ktorúkoľvek ikonu súčasti*** sa príslušná ikona zvýrazní v prehľade súčasti. V spodnej časti používateľského rozhrania sa zároveň zobrazí opis základných funkcií súčasti.
- ***Jedným kliknutím na ikonu súčasti*** otvoríte jej rozhranie s údajmi o aktuálnom stave. Súčasne tu máte prístup ku konfigurácii a štatistickým údajom.

5.4. Moje aplikácie

V oblasti ***Moje aplikácie*** *(v rade zelených obdĺžnikov pod súpravou súčastí)* nájdete prehľad ďalších aplikácií AVG, ktoré sú buď na vašom počítači nainštalované, alebo sa ich inštalácia odporúča. Obdĺžniky sa zobrazujú podmienene a môžu predstavovať niektoré z týchto aplikácií:

- ***Mobilná ochrana*** je aplikácia, ktorá chráni mobilný telefón proti vírusom a softvéru malware. Poskytuje tiež možnosť diaľkového sledovania telefónu smartphone, pokiaľ by ste s ním stratili kontakt.
- ***Súčasť LiveKive*** sa používa výlučne na on-line zálohovanie dát na zabezpečených serveroch. LiveKive automaticky zálohuje všetky vaše súbory, fotografie a hudbu na jednom bezpečnom mieste a umožňuje vám zdieľať tieto dáta s rodinou a priateľmi a získať k nim prístup z akéhokoľvek zariadenia s pripojením na internet, vrátane telefónov iPhone a zariadení s operačným systémom Android.
- ***Funkcia Family Safety*** pomáha chrániť vaše deti pred nevhodnými webovými lokalitami, multimédiami a výsledkami vyhľadávania on-line a hlási vám ich on-line aktivitu. Aplikácia AVG Family Safety obsahuje technológiu sledujúcu stláčanie tlačidiel pri aktivitách vašich detí v chatovacích miestnostiach alebo v sociálnych sieťach. Ak zaregistruje slová, frázy

alebo jazyk, ktoré sú typické pre šikanovanie detí online, okamžite vás upozorní pomocou správy SMS alebo e-mailom. V aplikácii môžete nastaviť vhodnú úroveň ochrany pre každé dieťa a sledovať deti individuálne pomocou jedinečných prihlasovacích údajov.

- ***Súčasť PC Tuneup*** je vyspelý nástroj na podrobnú analýzu a opravu systému, ktorý sa používa na hľadanie možností, ako zvýšiť rýchlosť počítača a zlepšiť jeho celkový výkon.

- ***MultiMi*** sústreďuje všetky e-maily a účty na sociálnych sieťach na jednom mieste, čo uľahčuje kontakt s rodinou a priateľmi, prehľadávanie internetu, zdieľanie fotografií, videí a súborov. Aplikácia MultiMi obsahuje službu LinkScanner, ktorá vás chráni pred narastajúcim množstvom hrozieb na webe. Funguje tak, že analyzuje webové stránky za všetkými odkazmi na práve zobrazenej webovej stránke a uistí sa, či sú bezpečné.

- ***AVG Toolbar*** je k dispozícii priamo v internetovom prehliadači a zabezpečuje maximálnu bezpečnosť pri prezeraní internetu.

Podrobnosti o niektorej aplikácii z radu ***Moje aplikácie*** zobrazíte po kliknutí na príslušný obdĺžnik. Budete presmerovaní na príslušnú webovú stránku AVG, kde si môžete súčasť priamo prevziať.

5.5. Kontrola/Aktualizovať rýchle odkazy

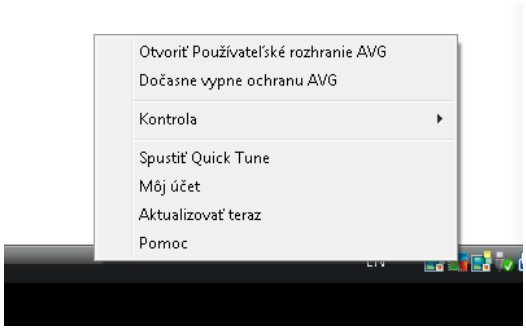
Rýchle odkazy sa nachádzajú v spodnom riadku tlačidiel v používateľskom rozhraní **AVG AntiVirus 2013**. Tieto odkazy poskytujú okamžitý prístup k najdôležitejším a najčastejšie používaným funkciám aplikácie, teda kontrole a aktualizácii. Rýchle odkazy sú dostupné zo všetkých dialógových okien používateľského rozhrania:

- ***Skontrolovať teraz*** – Tlačidlo je graficky rozdelené na dve časti. Odkazom ***Skontrolovať ihneď*** okamžite spustíte kontrolu celého počítača, môžete sledovať jej priebeh a výsledky v automaticky otvorenom okne Správy. Tlačidlo ***Možnosti*** otvorí dialógové okno ***Možnosti kontroly***, kde môžete upraviť naplánované kontroly a upraviť parametre Kontroly celého počítača/Kontroly súborov/priečinkov. *(Podrobnosti nájdete v kapitole Kontrola aplikáciou AVG)*

- ***Aktualizovať ihneď*** – Stlačením tohto tlačidla okamžite spustíte aktualizáciu. O výsledkoch aktualizácie budete informovaní v oznámení nad ikonou AVG v paneli úloh. *(Podrobnosti nájdete v kapitole Aktualizácie aplikácie AVG)*

5.6. Ikona v paneli úloh

Ikona AVG v paneli úloh *(v paneli úloh systému Windows v pravom dolnom rohu monitora)* zobrazuje aktuálny stav produktu **AVG AntiVirus 2013**. Vždy sa nachádza v paneli úloh bez ohľadu na to, či je používateľské rozhranie produktu **AVG AntiVirus 2013** otvorené alebo zatvorené:



Zobrazenie ikony AVG v systémovom paneli úloh

- Úplne vyfarbená ikona bez ďalších prvkov znamená, že všetky súčasti aplikácie **AVG AntiVirus 2013** sú aktívne a úplne funkčné. Takáto ikona sa však môže zobraziť aj vtedy, keď niektorá zo súčasti nie je úplne funkčná, ale používateľ sa rozhodol ignorovať jej stav. *(Ak ste potvrdili možnosť ignorovania stavu súčasti, potvrdzujete tým, že ste si vedomí chybového stavu súčasti, ale z nejakého dôvodu ju tak chcete ponechať a nechcete zobrazovať varovania týkajúce sa tejto situácie.)*

- Ikona s výkričníkom znamená, že súčasť *(alebo viac súčastí)* je v chybovom stave. Takýmto výstrahám vždy venujte pozornosť a snažte sa odstrániť problém konfigurácie súčasti, ktorá nie je nastavená správne. Ak chcete zmeniť konfiguráciu súčasti, dvakrát kliknite na ikonu v paneli úloh. Otvorí sa používateľské rozhranie aplikácie. Podrobné informácie o chybovom stave jednotlivých súčasti nájdete v časti Informácie o stave zabezpečenia.

- Ikona v paneli úloh sa môže ďalej zobraziť plnofarebne s blikajúcim a otáčajúcim sa majákom. Táto grafická verzia signalizuje, že prebieha aktualizácia.

- Plnofarebné zobrazenie ikony so šípkou znamená, že **AVG AntiVirus 2013** práve prebieha kontrola.

Informácie ikony AVG v systémovom paneli úloh

Ikona AVG v systémovom paneli úloh uvádza aj údaje o aktuálnych aktivitách v programe **AVG AntiVirus 2013** a možných zmenách stavu programu (*napr. automatickom spustení plánu kontroly alebo aktualizácie, zmene stavu súčasti, výskyte chybového stavu, ...*) pomocou kontextového okna, ktoré sa otvorí kliknutím na ikonu v paneli úloh.

Činnosti prístupné prostredníctvom ikony AVG v systémovom paneli úloh

Ikonu AVG v systémovom paneli úloh môžete použiť aj na rýchle zobrazenie používateľského rozhrania produktu **AVG AntiVirus 2013**. Stačí dvakrát kliknúť na ikonu. Kliknutím pravým tlačidlom myši na ikonu sa otvorí krátka kontextová ponuka s týmito možnosťami:

- ***Otvoriť používateľské rozhranie AVG*** – Kliknutím na túto položku sa otvorí používateľské rozhranie aplikácie **AVG AntiVirus 2013**.

- ***Dočasne vypnúť ochranu AVG*** – Táto možnosť umožňuje vypnúť celú ochranu produktom **AVG AntiVirus 2013** naraz. Nepoužívajte túto možnosť, ak to nie je naozaj nevyhnutné! Vo väčšine prípadov nie je potrebné vypnúť produkt **AVG AntiVirus 2013** pred inštaláciou nového softvéru alebo ovládačov, a to ani v prípade, keď inštalačný program alebo sprievodca inštaláciou softvéru odporúča, aby sa najskôr zatvorili spustené programy a aplikácie z dôvodu možného nežiaduceho prerušenia procesu inštalácie. Ak musíte dočasne vypnúť ochranu **AVG AntiVirus 2013**, znova ju zapnite bezprostredne po dokončení úloh, pre ktoré ste ju vypli. Ak ste pripojení na internet alebo k sieti v čase, keď je antivírusový softvér vypnutý, počítač nie je chránený pred útokmi.

- ***Kontrola*** – Kliknutím na túto možnosť otvoríte kontextovú ponuku vopred definovaných kontrol (*Kontrola celého počítača* a *Kontrola súborov/priečinkov*) a vyberte požadovanú kontrolu. Kontrola sa ihneď spustí.

- ***Kontroluje sa...*** – Táto položka sa zobrazí len v prípade, keď v počítači práve beží kontrola. Tejto kontrole môžete potom nastaviť prioritu, alebo ju môžete zastaviť alebo pozastaviť. Ďalej sa tu nachádzajú tieto funkcie: *Nastaviť prioritu pre všetky kontroly, Pozastaviť všetky kontroly* a *Zastaviť všetky kontroly*.

- ***Spustiť PC Analyzer*** – Kliknutím na túto možnosť sa spustí súčasť PC Analyzer.

- ***Môj účet*** – Otvorí domovskú stránku MyAccount, na ktorej môžete spravovať predplatné produktov, zaplatiť dodatočnú ochranu, prevziať inštalačné súbory, skontrolovať minulé objednávky a faktúry a spravovať osobné informácie.

- ***Aktualizovať teraz*** – Spustí okamžitú aktualizáciu.

- ***Pomocník*** – Otvorí súbor pomocníka na úvodnej strane.

5.7. Miniaplikácia AVG

Miniaplikácia AVG sa nachádza na pracovnej ploche operačného systému Windows (*bočný panel systému Windows*). Túto aplikáciu podporujú len operačné systémy Windows Vista a Windows 7/8. ***Miniaplikácia AVG*** umožňuje okamžitý prístup k najdôležitejším funkciám programu **AVG AntiVirus 2013**, t. j. kontrole a aktualizácii:

Ovládacie prvky miniaplikácie AVG

Miniaplikácia AVG vám v prípade potreby umožní okamžite spustiť kontrolu alebo aktualizáciu. Poskytuje tiež rýchly odkaz na hlavné sociálne siete a možnosť rýchleho vyhľadávania:

- ***Skontrolovať teraz*** – Kliknutím na odkaz ***Skontrolovať teraz*** sa priamo spustí kontrola

celého počítača. Priebeh kontroly môžete pozorovať v alternatívnom používateľskom rozhraní miniaplikácie. Stručný štatistický prehľad informuje o počte skontrolovaných objektov a detegovaných a vyliečených hrozieb. Počas kontroly môžete vždy pozastaviť alebo zastaviť proces. Podrobné informácie súvisiace s výsledkami kontroly sa nachádzajú v štandardnom dialógovom okne Prehľad výsledkov kontroly, ktoré sa otvára priamo v miniaplikácii výberom možnosti ***Zobraziť podrobnosti*** *(príslušné výsledky kontroly budú uvedené pod položkou Kontrola z miniaplikácie na bočnom paneli)*.

- ***Aktualizovať teraz*** – Kliknutím na odkaz ***Aktualizovať teraz*** sa **AVG AntiVirus 2013** aktualizuje priamo v mini aplikácii:

- ***Odkaz na Twitter*** – Otvorí nové rozhranie ***miniaplikácie AVG*** s prehľadom najnovších informačných kanálov AVG zverejnených na stránkach Twitter. Kliknutím na odkaz ***Zobraziť všetky informačné kanály služby Twitter súvisiace s AVG*** otvorte nové okno internetového prehliadača s internetovými stránkami Twitter, konkrétne stránkou so správami týkajúcimi sa produktu AVG.

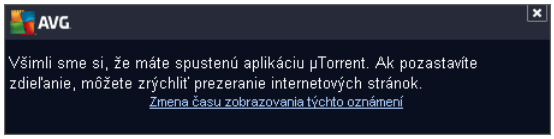
- ***Odkaz na Facebook*** – Otvorí internetový prehliadač s internetovými stránkami Facebook, konkrétne na stránke ***komunity AVG***.

- ***Vyhľadávacie políčko*** – Zadajte kľúčové slovo na okamžité zobrazenie výsledkov vyhľadávania v novom otvorenom okne v predvolenom internetovom prehliadači.

5.8. AVG Advisor

Súčasť ***AVG Advisor*** bola navrhnutá tak, aby detegovala problémy, ktoré môžu spomaľovať váš počítač alebo ho ohrozovať a na odporúčanie akcií na riešenie daných situácií. Ak sa váš počítač náhle spomalí *(počas prezerania internetu alebo sa zníži celkový výkon)*, obvykle nie je jasná presná príčina a teda ani to, ako daný problém riešiť. Preto prichádza aplikácia ***AVG Advisor***: Zobrazí oznámenie na paneli úloh, ktoré vás informuje o tom, čo môže byť daným problémom, a navrhuje spôsob opravy. ***AVG Advisor*** je služba, ktorá sleduje všetky procesy spustené na počítači, či v nich nedochádza k problémom, a ponúka tipy na ich predchádzanie.

AVG Advisor vidíte v podobe vysúvacieho kontextového okna na paneli úloh:



Súčasť ***AVG Advisor*** sleduje nasledujúce:

- ***Stav akéhokoľvek práve otvoreného internetového prehliadača***. Internetové prehliadače môžu zahlcovať pamäť, predovšetkým v prípade, ak po určitý čas zostane otvorených viacero kariet alebo okien, a môžu spotrebovávať mnoho systémových prostriedkov, t. j. spomaľovať váš počítač. V takomto prípade obvykle pomôže reštartovanie internetového prehliadača.

- ***Prebiehajúce pripojenia typu Peer-To-Peer***. Po použití protokolu P2P na zdieľanie súborov môže občas zostať pripojenie aktívne a konzumovať určitú časť rýchlosti vášho pripojenia. Výsledkom toho môže byť spomalenie prezerania internetu.

- ***Neznáma sieť so známym názvom***. To sa obvykle týka len používateľov, ktorí sa pripájajú k rôznym sieťam, typicky pomocou prenosných počítačov: V prípade, že nová neznáma sieť má rovnaký názov ako dobre známa a často používaná sieť *(napríklad Doma alebo MojeWifi)*, môže nastať omyl a nechtiac sa môžete pripojiť do úplne neznámej a potenciálne nebezpečnej siete. Súčasť ***AVG Advisor*** tomu môže predísť tak, že vás varuje, že známy názov v skutočnosti označuje novú sieť. Samozrejme, ak sa rozhodnete, že neznáma sieť je bezpečná, môžete ju uložiť do zoznamu známych sietí súčasti ***AVG Advisor***, aby v budúcnosti nebola znovu nahlasovaná.

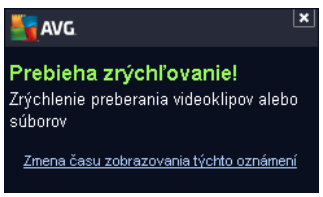
V každej z týchto situácií vás nástroj ***AVG Advisor*** upozorní na možný problém, ktorý by mohol nastať, a zobrazí názov a ikonu problémového procesu či aplikácie. Funkcia ***AVG Advisor*** tiež ponúkne návrh krokov, ktorými by ste sa mohli vyhnúť možnému problému.

Podporované webové prehliadače

Táto funkcia funguje v týchto webových prehliadačoch: Internet Explorer, Chrome, Firefox, Opera, Safari.

5.9. AVG Akcelerátor

Služba AVG Accelerator umožňuje stabilnejšie prehrávanie on-line videa a uľahčuje ďalšie preberania. Ak prebieha akcelerácia videa, v paneli úloh vás upozorní kontextové okno.



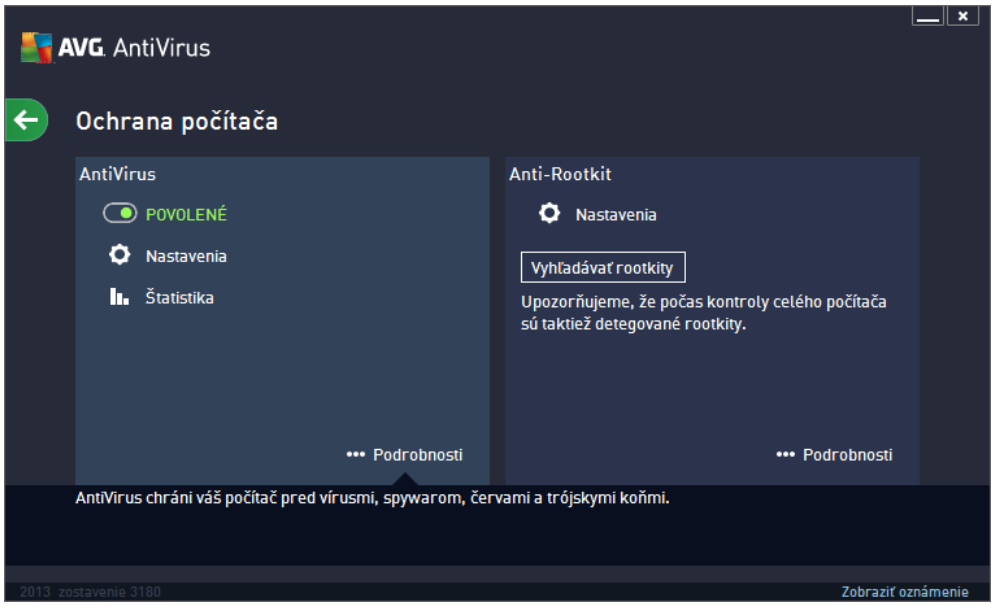
6. Súčasti AVG

6.1. Počítač

Súčasť ***Počítač*** sa týka dvoch hlavných bezpečnostných služieb: ***AntiVirus*** a ***Anti-Rootkit***:

- ***AntiVirus*** sa skladá z kontrolného jadra, ktoré stráži všetky súbory, systémové oblasti počítača a vymeniteľné médiá *(disk flash a pod.)* a kontroluje prítomnosť známych vírusov. Každý zistený vírus sa zablokuje, aby nemohol vykonávať žiadnu činnosť, a potom sa vymaže alebo sa premiestni do Vírusového trezora. Normálne tento proces ani nezbadáte, pretože rezidentná ochrana je „spustená na pozadí“. Súčasť AntiVirus používa tiež heuristickú kontrolu, pri ktorej sa v súboroch kontrolujú charakteristiky typické pre vírusy. To znamená, že program AntiVirus dokáže zistiť nový, neznámy vírus vtedy, keď obsahuje isté typické vlastnosti existujúcich vírusov. **AVG AntiVirus 2013** vie tiež analyzovať a detegovať spustiteľné aplikácie alebo knižnice DLL, ktoré by sa v systéme nemali nachádzať *(rôzne typy spyware, adware apod.)*. AntiVirus ďalej kontroluje podozrivé záznamy v databáze Registry, dočasné internetové súbory a spracuje všetky potenciálne škodlivé položky rovnakým spôsobom ako každú inú infekciu

- ***Anti-Rootkit*** je špeciálny nástroj, ktorý zisťuje a efektívne odstraňuje nebezpečné programy rootkit, teda programy a technológie, ktoré môžu zakrývať prítomnosť škodlivého softvéru v počítači. Rootkit je program určený na to, aby sa zmocnil základnej kontroly nad počítačovým systémom bez povolenia vlastníka systému a jeho právoplatných správcov. Súčasť Anti-Rootkit dokáže zistiť prítomnosť programov rootkit pomocou vopred definovanej skupiny pravidiel. Ak súčasť Anti-Rootkit nájde program rootkit, nemusí to nevyhnutne znamenať, že je tento program infikovaný. Programy rootkit sa niekedy používajú ako ovládače, príp. tvoria súčasť správnych aplikácií.



Ovládacie prvky dialógového okna

Ak chcete prepínať medzi obomi časťami dialógového okna, stačí kliknúť kdekoľvek na príslušný servisný panel. Panel sa zvýrazní v svetlejšom odtieni modrej. V oboch častiach dialógového okna nájdete tieto ovládacie prvky. Ich funkcia je rovnaká bez ohľadu na to, do ktorej bezpečnostnej služby patria *(AntiVirus alebo Anti-Rootkit*):

Zakázané/povolené – Tlačidlo môže pripomínať semafor vzhľadom aj funkciou. Kliknutím môžete prepínať medzi jeho dvomi polohami. Zelená farba symbolizuje stav ***Povolené***, čo znamená, že bezpečnostná služba AntiVirus je aktívna a plne funkčná. Červená farba predstavuje stav ***Zakázané***, t. j. služba je vypnutá. Ak nemáte dobrý dôvod na vypnutie služby, výrazne odporúčame, aby ste ponechali predvolené nastavenia pre všetky konfigurácie zabezpečenia. Predvolené nastavenia zaručujú optimálny výkon aplikácie a maximálnu bezpečnosť. Ak z nejakého dôvodu chcete vypnúť službu, budete upozornení na možné riziká červeným ***varovným*** nápisom a oznámením faktu, že momentálne nie ste úplne chránení. ***Nezabudnite, že by ste službu mali znovu aktivovať čo najskôr.***

Nastavenia – Kliknutím na tlačidlo budete presmerovaní na rozhranie rozšírených nastavení. Otvorí sa príslušné dialógové okno a budete môcť nakonfigurovať vybranú službu, t. j. AntiVirus alebo Anti-Rootkit. V rozšírených nastaveniach môžete upravovať všetky konfigurácie každej bezpečnostnej služby programu **AVG AntiVirus 2013**, no akékoľvek nastavenie odporúčame iba skúseným používateľom!

Štatistika – Kliknutím na tlačidlo budete presmerovaní na príslušnú stránku na webovej lokalite AVG (http://www.avg.com/). Na tejto lokalite sa nachádza štatistický prehľad o všetkých činnostiach aplikácie **AVG AntiVirus 2013** vykonaných v počítači v stanovenom vymedzenom intervale za celý čas.

Podrobnosti – Kliknutím na tlačidlo sa v dolnej časti dialógového okna zobrazí stručný popis označenej služby.

– Pomocou zelenej šípky v ľavej hornej časti dialógového okna sa vrátite naspäť do hlavného používateľského rozhrania s prehľadom súčastí.

V časti Anti-Rootkit nájdete tiež konkrétne tlačidlo ***Kontrolovať rootkity***, ktorým môžete priamo spustiť nezávislú kontrolu rootkitov *(kontrola rootkitov je však implicitná súčasť kontroly celého počítača)*.

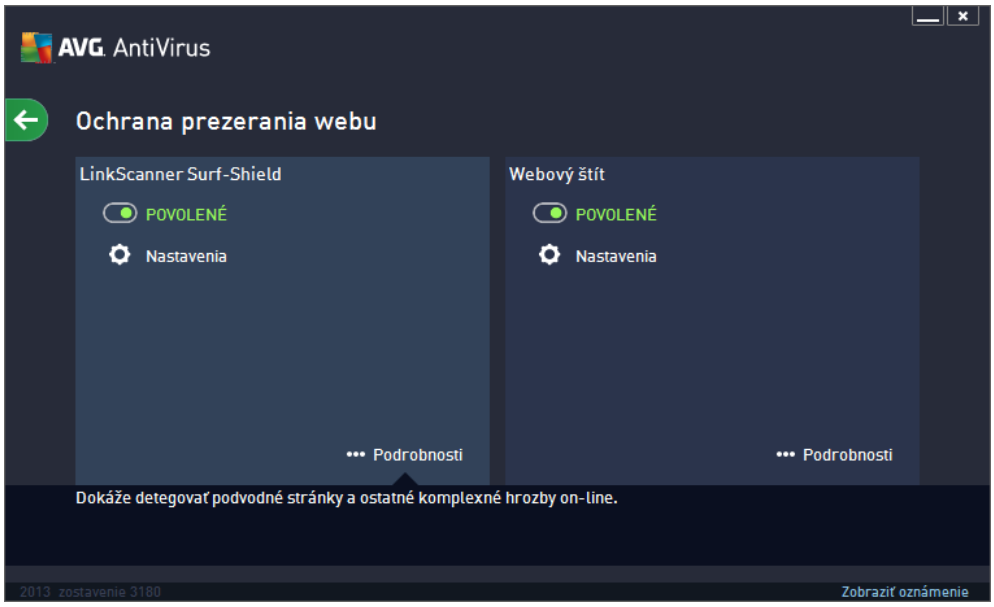
6.2. Web

Ochrana pri prezeraní webu sa skladá z dvoch služieb: ***LinkScanner Surf-Shield*** a ***Webový štít***:

- ***LinkScanner Surf-Shield*** vás chráni pred narastajúcim počtom hrozieb typu „dnes je tu, zajtra je preč“ na internete. Tieto hrozby sa môžu ukrývať na internetových stránkach akéhokoľvek typu, od vládnych až po veľké, od známych značiek až po malé podniky, a len málokedy sa na týchto stránkach udržia viac ako 24 hodín. LinkScanner vás chráni tak, že analyzuje internetové stránky za všetkými odkazmi na internetovej stránke, ktorú prezeráte, a stará sa o to, aby boli bezpečné práve v momente, keď je to najviac dôležité – v momente, keď sa chystáte kliknúť na odkaz. ***Súčasť LinkScanner Surf-Shield nie je určená na ochranu serverových platforiem!***

- ***Webový štít*** je druh rezidentnej ochrany, ktorá pracuje v reálnom čase; prehľadáva obsah navštívených internetových stránok (a súborov, ktoré sa na nich môžu nachádzať) ešte

predtým, než sa zobrazia v internetovom prehliadači alebo prevezmú do počítača. Webový štít zistí prítomnosť nebezpečného kódu JavaScript na stránke, ktorú sa práve chystáte navštíviť, a neumožní stránku zobraziť. Takisto rozpoznáva malware, ktorý sa nachádza na danej stránke, a ihneď zastaví jeho sťahovanie, aby sa nikdy nedostal do vášho počítača. Táto účinná ochrana zablokuje škodlivý kód každej webovej stránky, ktorú sa pokúšate otvoriť, a zabráni jeho prevzatiu do počítača. Ak je táto funkcia zapnutá a kliknete na odkaz alebo zadáte adresu URL nebezpečných stránok, funkcia automaticky zablokuje otvorenie týchto webových stránok, aby vás chránila pred náhodným infikovaním. Je dôležite pamätať na to, že zneužité stránky môžu infikovať váš počítač už len tým, že ich navštívite. ***Súčasť Webový štít nie je určená na ochranu na serverových platformiem!***



Ovládacie prvky dialógového okna

Ak chcete prepínať medzi obomi časťami dialógového okna, stačí kliknúť kdekoľvek na príslušný servisný panel. Panel sa zvýrazní v svetlejšom odtieni modrej. V oboch častiach dialógového okna nájdete tieto ovládacie prvky. Ich funkcia je rovnaká bez ohľadu na to, do ktorej bezpečnostnej služby patria *(LinkScanner Surf-Shield alebo Webový štít)*:

Zakázané/povolené – Tlačidlo môže pripomínať semafor vzhľadom aj funkciou. Kliknutím môžete prepínať medzi jeho dvomi polohami. Zelená farba symbolizuje stav ***Povolené***, čo znamená, že bezpečnostná služba LinkScanner Surf-Shield/Webový štít je aktívna a plne funkčná. Červená farba predstavuje stav ***Zakázané***, t. j. služba je vypnutá. Ak nemáte dobrý dôvod na vypnutie služby, výrazne odporúčame, aby ste ponechali predvolené nastavenia pre všetky konfigurácie zabezpečenia. Predvolené nastavenia zaručujú optimálny výkon aplikácie a maximálnu bezpečnosť. Ak z nejakého dôvodu chcete vypnúť službu, budete upozornení na možné riziká červeným ***varovným*** nápisom a oznámením faktu, že momentálne nie ste úplne chránení. ***Nezabudnite, že by ste službu mali znovu aktivovať čo najskôr.***

Nastavenia – Kliknutím na tlačidlo budete presmerovaní na rozhranie rozšírených nastavení. Otvorí sa príslušné dialógové okno a budete môcť nakonfigurovať vybranú službu, t.

j. LinkScanner Surf-Shield alebo Webový štít. V rozšírených nastaveniach môžete upravovať všetky konfigurácie každej bezpečnostnej služby programu **AVG AntiVirus 2013**, no akékoľvek nastavenie odporúčame iba skúseným používateľom!

Štatistika – Kliknutím na tlačidlo budete presmerovaní na príslušnú stránku na webovej lokalite AVG (http://www.avg.com/). Na tejto lokalite sa nachádza štatistický prehľad o všetkých činnostiach aplikácie **AVG AntiVirus 2013** vykonaných v počítači v stanovenom vymedzenom intervale za celý čas.

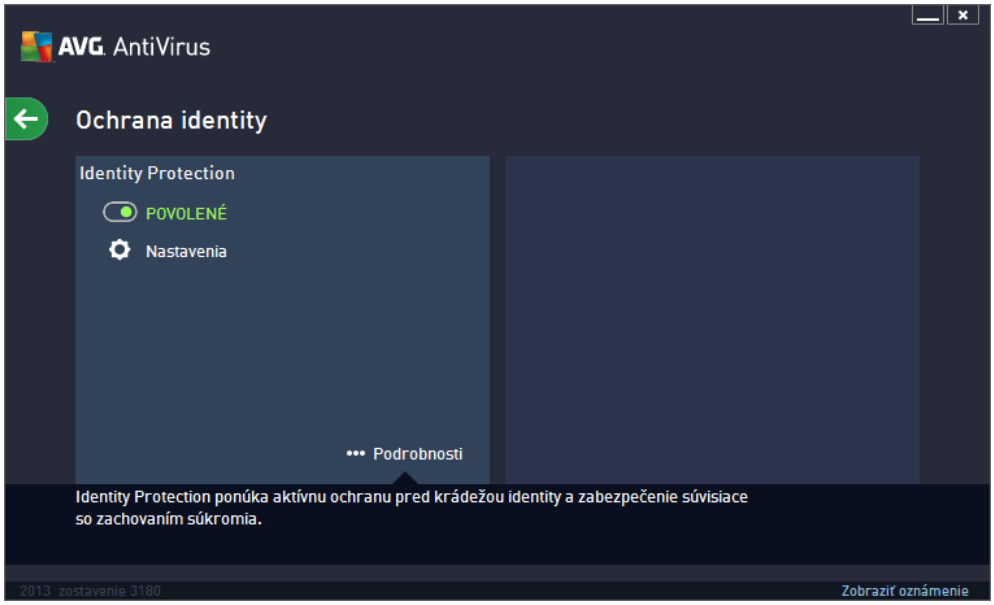
Podrobnosti – Kliknutím na tlačidlo sa v dolnej časti dialógového okna zobrazí stručný popis označenej služby.

– Pomocou zelenej šípky v ľavej hornej časti dialógového okna sa vrátite naspäť do hlavného používateľského rozhrania s prehľadom súčastí.

6.3. Identita

Súčasť ***Identity protection*** spúšťa službu ***Identity Shield***, ktorá neustále chráni vaše digitálne aktíva pred novými a neznámymi hrozbami na internete:

- ***Identity Protection*** je služba na ochranu pred škodlivým softvérom, ktorá chráni pred všetkými druhmi škodlivého softvéru (*spyware, softvérové roboty, krádež identity...*) s použitím technológií monitorovania správania a poskytuje okamžitú ochranu pred novými vírusmi. Identity Protection zabraňuje páchateľom počítačovej trestnej činnosti v oblasti odcudzenia identity, aby odcudzili vaše heslá, informácie o bankových účtoch, čísla kreditných kariet a iné cenné osobné digitálne údaje zo všetkých druhov škodlivého softvéru (*malware*), ktorý útočí na váš počítač. Zabezpečuje správne fungovanie všetkých spustených programov na počítači alebo zdieľanej sieti. Identity Protection zaznamenáva a blokuje podozrivé správanie a chráni počítač pred každým novým malware. Súčasť Identity Protection chráni počítač pred novými a dokonca aj neznámymi hrozbami v reálnom čase. Monitoruje všetky procesy *(vrátane skrytých)* a viac ako 285 rôznych modelov správania a dokáže zistiť, či sa v systéme nevyskytuje niečo škodlivé. Preto dokáže odhaliť hrozby, ktoré ešte nie sú opísané vo vírusovej databáze. Keď sa do počítača dostane neznámy kód, program ho ihneď začne sledovať z hľadiska škodlivého správania. Ak sa súbor označí ako škodlivý, súčasť Identity Protection presunie kód do Vírusového trezora a vráti späť všetky zmeny vykonané v systéme*(vloženie kódu, zmeny v databáze Registry, otvorenie portov a pod.)*. Na dosiahnutie ochrany nemusíte spúšťať kontrolu. Technológia má veľmi aktívny prístup, len zriedka sa musí aktualizovať a vždy je v strehu.



Ovládacie prvky dialógového okna

V dialógovom okne nájdete tieto ovládacie prvky:

Zakázané/povolené – Tlačidlo môže pripomínať semafor vzhľadom aj funkciou. Kliknutím môžete prepínať medzi jeho dvomi polohami. Zelená farba symbolizuje stav ***Povolené***, čo znamená, že bezpečnostná služba Identity Protection je aktívna a plne funkčná. Červená farba predstavuje stav ***Zakázané***, t. j. služba je vypnutá. Ak nemáte dobrý dôvod na vypnutie služby, výrazne odporúčame, aby ste ponechali predvolené nastavenia pre všetky konfigurácie zabezpečenia. Predvolené nastavenia zaručujú optimálny výkon aplikácie a maximálnu bezpečnosť. Ak z nejakého dôvodu chcete vypnúť službu, budete upozornení na možné riziká červeným ***varovným*** nápisom a oznámením faktu, že momentálne nie ste úplne chránení. ***Nezabudnite, že by ste službu mali znovu aktivovať čo najskôr.***

Nastavenia – Kliknutím na tlačidlo budete presmerovaní na rozhranie rozšírených nastavení. Otvorí sa príslušné dialógové okno a budete môcť nakonfigurovať vybranú službu, t. j. Identity Protection. V rozšírených nastaveniach môžete upravovať všetky konfigurácie každej bezpečnostnej služby programu **AVG AntiVirus 2013**, no akékoľvek nastavenie odporúčame iba skúseným používateľom!

Podrobnosti – Kliknutím na tlačidlo sa v dolnej časti dialógového okna zobrazí stručný popis označenej služby.

– Pomocou zelenej šípky v ľavej hornej časti dialógového okna sa vrátite naspäť do hlavného používateľského rozhrania s prehľadom súčastí.

V produkte **AVG AntiVirus 2013** služba Identity Alert žiaľ nie je štandardne zahrnutá. Ak chcete používať tento typ ochrany, stlačte tlačidlo ***Pre aktiváciu upgradujte***, ktoré vás presmeruje na príslušnú webovú stránku, kde si môžete zakúpiť licenciu Identity Alert.

Uvedomte si, že aj v aplikácii AVG Premium Security je služba Identity Alert momentálne dostupná

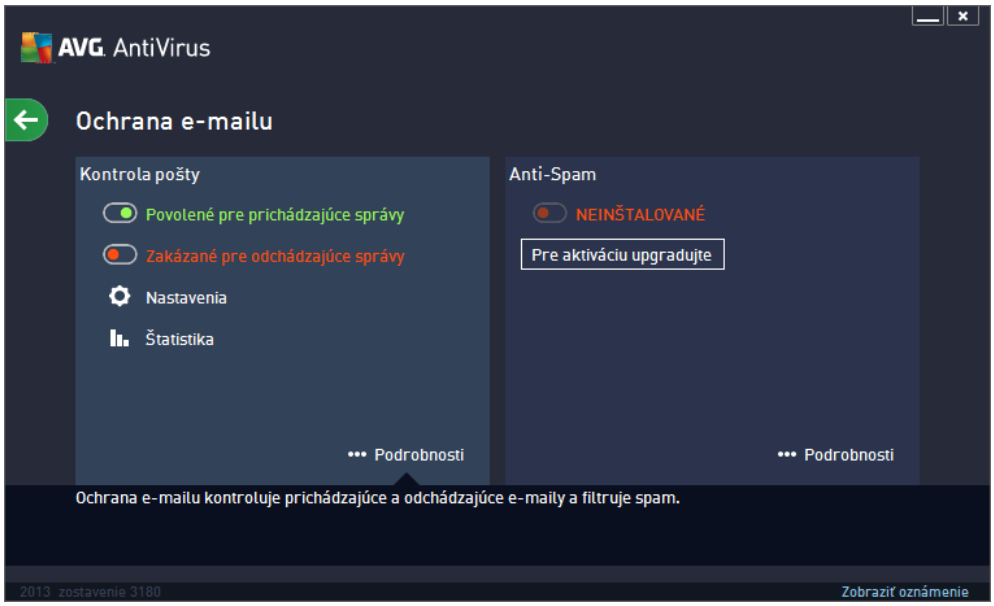
iba vo vybraných oblastiach: USA, Spojené kráľovstvo, Kanada a Írsko.

6.4. E-maily

Súčasť ***Ochrana e-mailu*** obsahuje dve služby zabezpečenia: ***Kontrola pošty*** a ***Anti-Spam***:

- ***Kontrola pošty***: Jeden z najbežnejších zdrojov vírusov a trójskych koňov je e-mail. Ohrozenia typu phishing a spam ďalej zvyšujú riziko e-mailu. Bezplatné e-mailové účty sú náchylnejšie na prijímanie takýchto škodlivých e-mailov *(pretože málokedy využívajú technológiu na ochranu pred spamom)* a domáci používatelia sa v pomerne veľkej miere spoliehajú na tieto e-mailové schránky. Domáci používatelia, ktorí surfujú po neznámych stránkach a do online formulárov vypĺňajú osobné údaje *(napr. e-mailové adresy)*, sú vo zvýšenej miere vystavení útokom prostredníctvom e-mailu. Spoločnosti obyčajne využívajú podnikové e-mailové účty a používajú antispamové filtre, a pod., aby toto riziko znížili. Súčasť Ochrana e-mailu sa stará o kontrolu jednotlivých doručených alebo odoslaných e-mailových správ a vždy, keď zistí prítomnosť vírusu, ihneď presunie správu do Vírusového trezora. Súčasť dokáže zároveň filtrovať niektoré typy e-mailových príloh a priložiť text certifikácie k správam bez infekcie. ***Súčasť Kontrola pošty nie je určená pre serverové platformy***

- Súčasť ***Anti-Spam*** kontroluje všetku prichádzajúcu poštu a nechcené správy označí ako spam *(Spam sa týka nevyžiadanej pošty, ktorá väčšinou propaguje produkty či služby a ktorá je masovo zasielaná na množstvo e-mailových adries súčasne. Podobné správy plnia poštové schránky príjemcov. Spam sa nevzťahuje na legitímne komerčné e-maily, s ktorými zákazníci súhlasia.)*. Súčasť Anti-Spam dokáže zmeniť predmet e-mailovej správy (*ktorá bola označená ako spam*) pridaním špeciálneho textového reťazca. Môžete filtrovať e-mailové správy v poštovej aplikácii. Súčasť Anti-Spam používa niekoľko metód analýzy na spracovanie jednotlivých e-mailových správ a prináša najvyššiu možnú úroveň ochrany pred nevyžiadanými e-mailovými správami. Súčasť Anti-Spam používa pravidelne aktualizovanú databázu na detekciu nevyžiadanej pošty. Rovnako môžete použiť servery RBL *(verejné databázy e-mailových adries „známych odosielateľov spamu“)* a ručne pridať e-mailové adresy do vlastného zoznamu povolených odosielateľov *(nikdy neoznačiť ako spam)* a zoznamu zakázaných odosielateľov *(vždy označiť ako spam)*.



Ovládacie prvky dialógového okna

Ak chcete prepínať medzi obomi časťami dialógového okna, stačí kliknúť kdekoľvek na príslušný servisný panel. Panel sa zvýrazní v svetlejšom odtieni modrej. V oboch častiach dialógového okna nájdete tieto ovládacie prvky. Ich funkcia je rovnaká bez ohľadu na to, do ktorej bezpečnostnej služby patria *(Kontrola pošty alebo Anti-Spam)*:

Zakázané/povolené – Tlačidlo môže pripomínať semafor vzhľadom aj funkciou. Kliknutím môžete prepínať medzi jeho dvomi polohami. Zelená farba symbolizuje stav ***Povolené***, čo znamená, že bezpečnostná služba je aktívna a plne funkčná. Červená farba predstavuje stav ***Zakázané***, t. j. služba je vypnutá. Ak nemáte dobrý dôvod na vypnutie služby, výrazne odporúčame, aby ste ponechali predvolené nastavenia pre všetky konfigurácie zabezpečenia. Predvolené nastavenia zaručujú optimálny výkon aplikácie a maximálnu bezpečnosť. Ak z nejakého dôvodu chcete vypnúť službu, budete upozornení na možné riziká červeným ***varovným*** nápisom a oznámením faktu, že momentálne nie ste úplne chránení. ***Nezabudnite, že by ste službu mali znovu aktivovať čo najskôr.***

V súčasti Kontrola pošty sa nachádzajú dve tlačidlá v podobe semaforov. Takto môžete samostatne určiť, či chcete, aby súčasť Kontrola pošty kontrolovala prichádzajúcu alebo odchádzajúcu poštu alebo oboje. Štandardne je zapnutá kontrola prichádzajúcich správ. Odchádzajúce správy sa štandardne nekontrolujú, pretože riziko ich infekcie je pomerne nízke.

Nastavenia – Kliknutím na tlačidlo budete presmerovaní na rozhranie rozšírených nastavení. Otvorí sa príslušné dialógové okno a budete môcť nakonfigurovať vybranú službu, t. j. Kontrola pošty alebo Anti-Spam. V rozšírených nastaveniach môžete upravovať všetky konfigurácie každej bezpečnostnej služby programu **AVG AntiVirus 2013**, no akékoľvek nastavenie odporúčame iba skúseným používateľom!

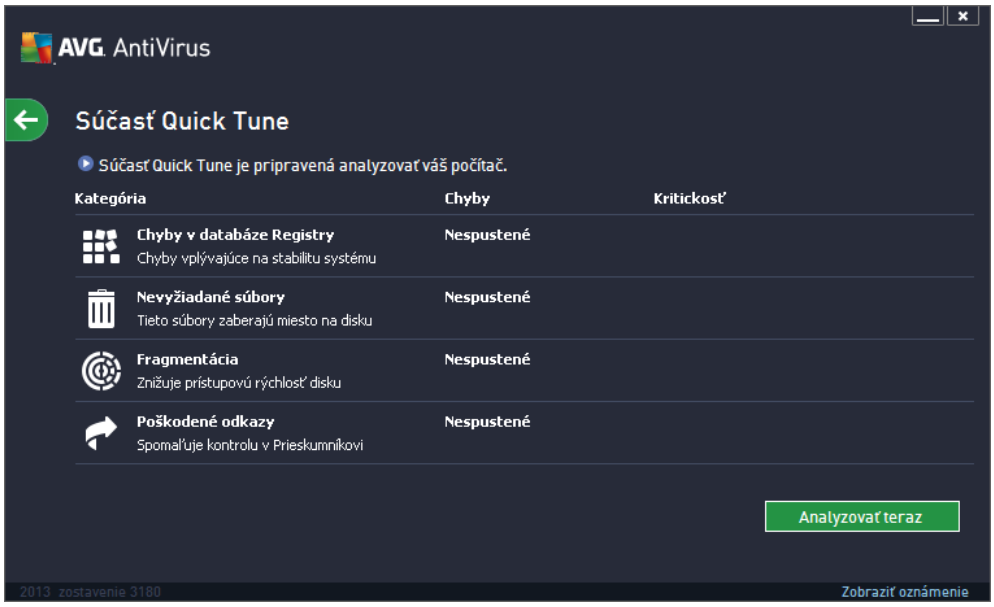
Štatistika – Kliknutím na tlačidlo budete presmerovaní na príslušnú stránku na webovej lokalite AVG (http://www.avg.com/). Na tejto lokalite sa nachádza štatistický prehľad o všetkých činnostiach aplikácie **AVG AntiVirus 2013** vykonaných v počítači v stanovenom vymedzenom intervale za celý čas.

Podrobnosti – Kliknutím na tlačidlo sa v dolnej časti dialógového okna zobrazí stručný popis označenej služby.

– Pomocou zelenej šípky v ľavej hornej časti dialógového okna sa vrátite naspäť do hlavného používateľského rozhrania s prehľadom súčastí.

6.5. Quick Tune

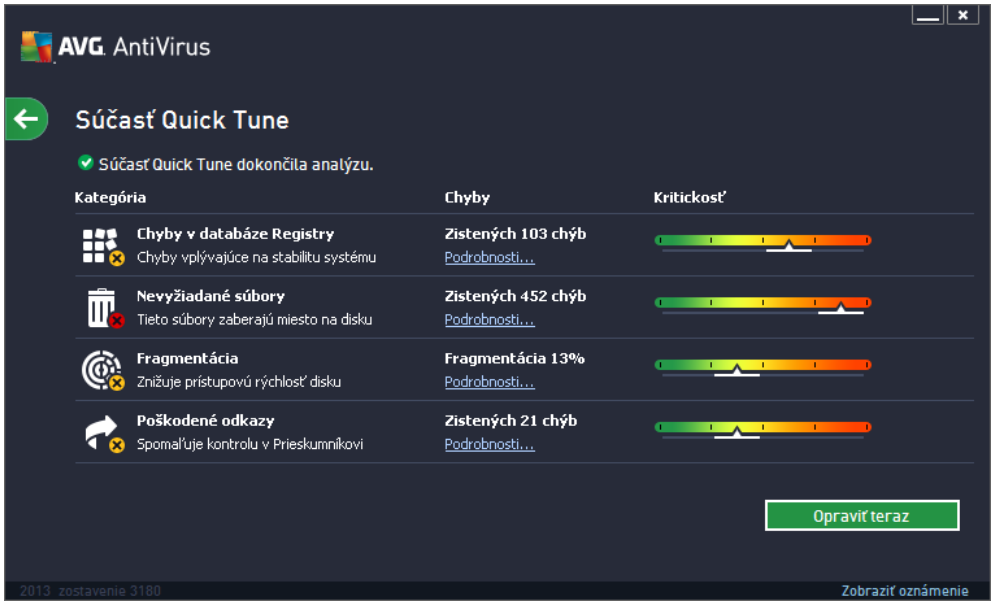
Súčasť ***Quick Tune*** je vyspelý nástroj na podrobnú analýzu a opravu systému, ktorý sa používa na hľadanie možností, ako zvýšiť rýchlosť počítača a zlepšiť jeho celkový výkon:



Umožňuje analyzovať a opraviť tieto oblasti: chyby v databáze Registry, nevyžiadané súbory, fragmentácia a poškodené odkazy:

- ***Chyby v databáze Registry*** informuje o počte chýb v databáze Registry operačného systému Windows, ktoré môžu spomaľovať váš počítač alebo spôsobovať zobrazenie chybových hlásení.
- ***Nevyžiadané súbory*** informuje o počte súborov, ktoré zaberajú miesto na pevnom disku, a ktoré sa pravdepodobne môžu vymazať. Zvyčajne ide o mnohé typy dočasných súborov a súbory v Koši.
- ***Fragmentácia*** vypočíta podiel pevného disku, ktorý je fragmentovaný, t. j. používal sa dlhý čas a väčšina súborov je umiestnená na rôznych miestach fyzického disku.
- ***Poškodené odkazy*** vyhľadá odkazy, ktoré už nie sú funkčné, vedú na neexistujúce miesta atď.

Na spustenie analýzy počítača stlačte tlačidlo ***Analyzovať teraz***. Potom si budete môcť pozrieť priebeh analýzy a výsledky priamo v tabuľke:



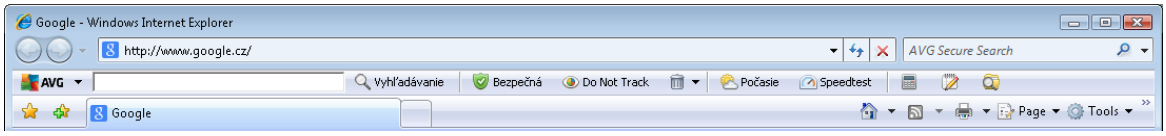
Prehľad výsledkov informuje o počte detegovaných systémových problémov (***Chyby***), ktoré sú klasifikované podľa príslušnej testovanej kategórie. Výsledky analýzy sa zobrazia aj v grafickej podobe na osi v stĺpci ***Závažnosť***.

Ovládacie tlačidlá

- ***Analyzovať teraz*** (*zobrazí sa pred spustením analýzy*) – stlačením tohto tlačidla sa ihneď spustí analýza počítača.
- ***Opraviť teraz*** (*zobrazí sa po dokončení analýzy*) – stlačením tlačidla sa odstránia všetky zistené chyby. Bezprostredne po dokončení procesu opravy sa zobrazí prehľad výsledku.
- ***Zrušiť*** – Stlačením tohto tlačidla sa zastaví spustená analýza, resp. po dokončení analýzy sa otvorí implicitné hlavné dialógové okno aplikácie AVG (*prehľad súčastí*).

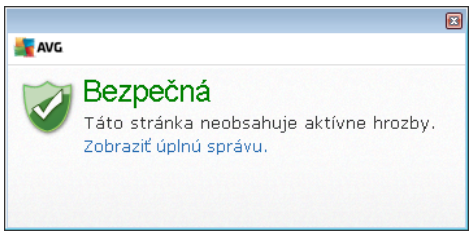
7. AVG Security Toolbar

AVG Security Toolbar je nástroj, ktorý úzko spolupracuje so súčasťou LinkScanner Surf-Shield a zabezpečuje maximálnu ochranu pri prezeraní internetu. V produkte **AVG AntiVirus 2013** je inštalácia súčasti ***AVG Security Toolbar*** voliteľná. Počas procesu inštalácie sa môžete rozhodnúť, či chcete túto súčasť nainštalovať. K súčasti ***AVG Security Toolbar*** máte prístup priamo v internetovom prehliadači. V súčasnosti medzi podporované prehľadávače patrí Internet Explorer (*verzia 6.0 a novšia*) alebo Mozilla Firefox (*verzia 3.0 a novšia*). Iné prehliadače nie sú podporované *(ak používate alternatívny internetový prehliadač (napr. Avant Browser), môžete sa stretnúť s neočakávaným správaním).*



Nástroj AVG Security Toolbar pozostáva z nasledujúcich častí:

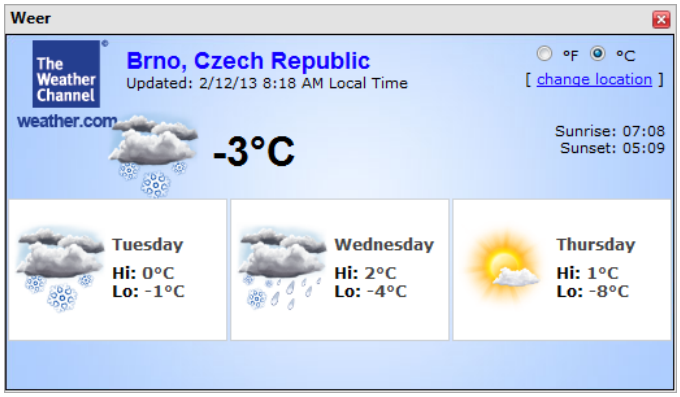
- ***Logo AVG*** s rozbaľovacou ponukou:
  - ***Aktuálna úroveň hrozieb*** – Otvorí webovú lokalitu vírusového laboratória s grafickým zobrazením momentálnej úrovne hrozieb na internete.
  - ***AVG Threat Labs*** – Otvorte konkrétnu webovú lokalitu ***AVG Threat Lab*** *(na adrese http://www.avgthreatlabs.com)*, kde nájdete informácie o bezpečnosti rôznych webových lokalít a aktuálnej úrovni on-line hrozieb.
  - ***Toolbar Help*** – Otvorí sa on-line pomocník s informáciami o funkciách nástroja ***AVG Security Toolbar***.
  - ***Submit Product feedback*** – Otvorí sa webová lokalita s formulárom, do ktorého môžete napísať svoje pocity a skúsenosti s nástrojom ***AVG Security Toolbar***.
  - ***Odinštalovať súčasť AVG Security Toolbar*** – Otvorí sa webová stránka s podrobnosťami o postupe vypnutia súčasti ***AVG Security Toolbar*** pre každý z podporovaných webových prehliadačov.
  - ***About...*** – Otvorí sa nové okno s informáciami o verzii aktuálne nainštalovanej súčasti ***AVG Security Toolbar***.
- ***Pole vyhľadávania*** – Pri surfovaní s nástrojom ***AVG Security Toolbar*** ste absolútne chránení, pretože všetky zobrazené výsledky vyhľadávania sú stopercentne bezpečné. Do poľa vyhľadávania napíšte kľúčové slovo alebo frázu a stlačte tlačidlo ***Vyhľadať*** *(alebo Enter)*.
- ***Bezpečnosť stránky*** – Toto tlačidlo otvára nové dialógové okno obsahujúce informácie o aktuálnej úrovni hrozby (*Aktuálne bezpečné*) internetovej stránky, na ktorej sa práve nachádzate. Tento krátky prehľad môžete rozbaliť a zobraziť všetky podrobnosti o všetkých bezpečnostných činnostiach týkajúcich sa internetovej stránky priamo v okne prehliadača (*Zobraziť úplnú správu*):



- ***Do Not Track*** – služba DNT vám pomáha identifikovať webové lokality, ktoré zbierajú údaje o vašich online aktivitách a umožňuje vám povoliť alebo nepovoliť ich zhromažďovanie. Detaily >>

- ***Vymazať*** – Tlačidlo „Odpadkový kôš“ ponúka rozbaľovaciu ponuku, v ktorej si môžete vybrať, či si želáte vymazať údaje o prezeraní stránok, preberaniach a on-line formulároch alebo chcete vymazať celú históriu vyhľadávania.

- ***Počasie*** – Toto tlačidlo otvorí nové dialógové okno s informáciami o počasí vo vašej oblasti a predpoveďou na najbližšie dva dni. Uvedené informácie sa pravidelne aktualizujú každé 3 hodiny až každých 6 hodín. V tomto okne môžete ručne zmeniť požadovanú oblasť a rozhodnúť sa, či chcete teplotu zobrazovať v stupňoch Celzia alebo Fahrenheita.



- ***Facebook*** – Pomocou týchto tlačidiel sa pripojíte k sociálnej sieti Facebook priamo z nástroja ***AVG Security Toolbar***.

- ***Speedtest*** – Toto tlačidlo vás presmeruje na on-line aplikáciu, ktorá vám pomôže overiť kvalitu internetového pripojenia *(ping)* a rýchlosť preberania a nahrávania.

- Tlačidlá skratiek rýchleho prístupu k týmto aplikáciám: ***Kalkulačka***, ***Poznámkový blok***, ***Prieskumník Windows***.

8. AVG Do Not Track

Aplikácia ***AVG Do Not Track*** pomáha identifikovať webové lokality, ktoré zhromažďujú údaje o vašej činnosti on-line. Funkcia ***AVG Do Not Track***, ktorá je súčasťou panelu nástrojov AVG Security Toolbar zobrazuje webové lokality alebo inzerentov zhromažďujúcich údaje o vašej aktivite a umožňuje vám to povoliť alebo zakázať.

- Aplikácia ***AVG Do Not Track*** poskytuje doplnkové informácie o zásadách ochrany osobných údajov jednotlivých služieb a tiež priame prepojenia na vyjadrenie explicitného nesúhlasu so službou, ak je takéto prepojenie k dispozícii.
- Okrem toho aplikácia ***AVG Do Not Track*** podporuje protokol W3C DNT, ktorý automaticky upozorní príslušné lokality, že si neželáte sledovanie svojej činnosti. Toto upozornenie je v predvolenom nastavení povolené, ale možno to kedykoľvek zmeniť.
- Aplikácia ***AVG Do Not Track*** sa poskytuje za týchto zmluvných podmienok.
- Aplikácia ***AVG Do Not Track*** je štandardne zapnutá, ale možno ju kedykoľvek bez problémov vypnúť. Príslušné pokyny nájdete v Častých otázkach v článku Vypnutie funkcie AVG Do Not Track.
- Ďalšie informácie o aplikácii ***AVG Do Not Track*** nájdete na našej webovej stránke.

V súčasnosti je fungovanie aplikácie ***AVG Do Not Track*** podporované len v prehľadávačoch Mozilla Firefox, Chrome a Internet Explorer.

8.1. Rozhranie aplikácie AVG Do Not Track

Keď ste on-line, aplikácia ***AVG Do Not Track*** vás upozorní ihneď, ako zistí akúkoľvek činnosť zhromažďovania údajov. V takom prípade ikona aplikácie ***AVG Do Not Track*** umiestnená na paneli nástrojov AVG Security Toolbar zmení svoj vzhľad – pri ikone sa zobrazí malé číslo informujúce o pošte služieb zhromažďujúcich údaje: Po kliknutí na ikonu sa zobrazí takéto dialógové okno:

Všetky zistené služby zhromažďujúce údaje sú uvedené v prehľade ***Sledovačov na tejto stránke***. Aplikácia ***AVG Do Not Track*** rozoznáva tieto tri druhy zhromažďovania údajov:

- ***Webová analýza*** *(v predvolenom nastavení povolená):* Služby využívané na zlepšovanie výkonnosti a využívania príslušnej webovej lokality. V tejto kategórii sú služby ako Google Analytics, Omniture alebo Yahoo Analytics. Služby webovej analýzy odporúčame neblokovať, príslušná webová stránka by nemusela správne fungovať.

- ***Reklamné siete*** *(niektoré sú v predvolenom nastavení blokované):* Služby, ktoré môžu zhromažďovať alebo poskytovať údaje o vašej činnosti on-line na viacerých lokalitách, a to priamo aj nepriamo, s cieľom ponúkať vám personalizované reklamy namiesto reklám vychádzajúcich z obsahu lokality. Tieto služby sa riadia zásadami Ochrany osobných údajov danej reklamnej siete, ktoré sú uvedené na príslušnej webovej stránke. Niektoré reklamné siete sú v predvolenom nastavení blokované.

- ***Tlačidlá sociálnych sietí*** *(v predvolenom nastavení povolené):* Prvky vyvinuté na zlepšenie používateľskej skúsenosti so sociálnymi sieťami. Tlačidlá sociálnych sietí sú poskytované sociálnymi sieťami priamo na lokalitu, ktorú navštevujete. Môžu zhromažďovať údaje o vašej činnosti, keď ste prihlásení. Medzi tlačidlá sociálnych sietí patria napríklad doplnky sociálnych sietí Facebook, Twitter alebo Google +1.

Poznámka: *Podľa toho, ktoré služby sú spustené na pozadí internetovej stránky, sa niektoré z troch uvedených častí nemusia v dialógovom okne aplikácie AVG Do Not Track zobraziť.*

Ovládacie prvky dialógového okna

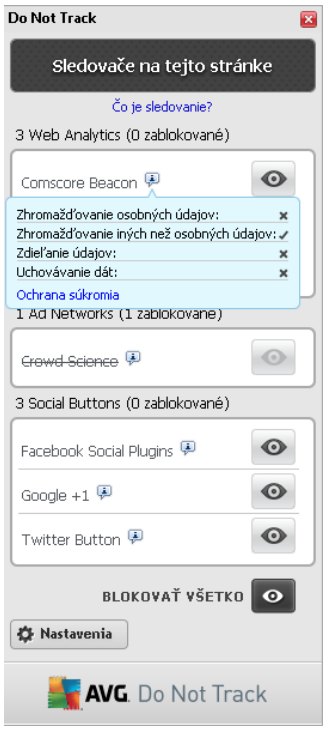
- ***Čo je sledovanie?*** – po kliknutí na toto prepojenie v hornej časti dialógového okna budete presmerovaní na špeciálnu webovú stránku s podrobným vysvetlením princípov sledovania a s popisom konkrétnych druhov sledovania.

- ***Blokovať všetky*** – Kliknite na toto tlačidlo umiestnené v spodnej časti dialógového okna, ak si neželáte vôbec žiadne zhromažďovanie údajov *(podrobnosti nájdete v kapitole Blokovanie sledovacích procesov).*

- ***Nastavenia aplikácie Do Not Track*** – po kliknutí na toto tlačidlo v dolnej časti dialógového okna budete presmerovaní na špeciálnu webovú stránku, na ktorej možno nastaviť konkrétnu konfiguráciu rôznych parametrov aplikácie ***AVG Do Not Track*** *(podrobné informácie nájdete v kapitole o nastavení aplikácie AVG Do Not Track)*

8.2. Informácie o sledovacích procesoch

V zozname detegovaných služieb zhromažďujúcich údaje sa uvádza len názov danej služby. Ak sa chcete kvalifikovane rozhodnúť, či danú službu zablokujete, alebo povolíte, budete zrejme potrebovať viac informácií. Posuňte myš nad príslušnú položku v zozname. Zobrazí sa informačná bublina, ktorá uvádza podrobné údaje o danej službe. Dozviete sa, či daná služba zhromažďuje vaše osobné údaje alebo niektoré iné dostupné údaje, či sú dané údaje zdieľané s inými subjektmi z tretích strán a či sa zhromaždené údaje ukladajú na prípadné ďalšie použitie:



V spodnej časti informačnej bubliny môžete vidieť odkaz ***Zásady ochrany osobných údajov***, ktorý vás presmeruje na internetovú stránku venovanú zásadám ochrany osobných údajov príslušnej detegovanej služby.

8.3. Blokovanie sledovacích procesov

Po rozbalení zoznamov všetkých reklamných sietí / tlačidiel sociálnych sietí / služieb webovej analýzy si môžete vybrať, ktoré sledovacie služby budú blokované. Môžete postupovať dvoma spôsobmi:

- ***Blokovať všetky*** – Kliknite na toto tlačidlo umiestnené v spodnej časti dialógového okna, ak si neželáte vôbec žiadne zhromažďovanie údajov. *(Pamätajte však, že tento krok môže narušiť funkcie príslušnej webovej stránky, na ktorej je služba spustená!)*

- – Ak si neželáte blokovať všetky detegované systémy naraz, môžete jednotlivo konkretizovať, či by daná služba mal byť povolená, alebo blokovaná. Môžete povoliť fungovanie niektorých detegovaných systémov *(napr. služba Web Analytics):* tieto systémy používajú zhromaždené údaje na optimalizáciu vlastných internetových stránok a pomáhajú tak zlepšovať spoločné internetové prostredie pre všetkých používateľov. Zároveň však môžete zablokovať činnosti zhromažďovania údajov všetkých procesov označených ako reklamné siete. Aby ste zablokovali zhromažďovanie údajov *(názov procesu sa zobrazí prešk rtnutý)* alebo ho znovu povolili, stačí, ak kliknete na ikonu umiestnenú vedľa danej služby.

8.4. Nastavenia aplikácie AVG Do Not Track

Dialógové okno ***Do Not Track Možnosti*** poskytuje nasledujúce možnosti nastavenia:

- ***Funkcia Do Not Track je zapnutá*** – funkcia je predvolene aktívna *(zapnutá)*. Funkciu vypnete posunutím spínača do polohy vypnutia.

- V strednej časti dialógového okna uvidíte pole so zoznamom známych služieb zhromažďovania údajov, ktoré možno klasifikovať ako reklamné siete. V predvolenom

nastavení služba ***Do Not Track blokuje niektoré reklamné siete automaticky a od vás závisí, či budú blokované aj ostatné siete, alebo ich necháte povolené.*** Stačí, keď kliknete na tlačidlo ***Blokovať všetko*** pod zoznamom. Alebo môžete kliknutím na tlačidlo ***Predvolené*** zrušiť všetky zmeny v nastaveniach a vrátiť sa k pôvodnému nastaveniu.

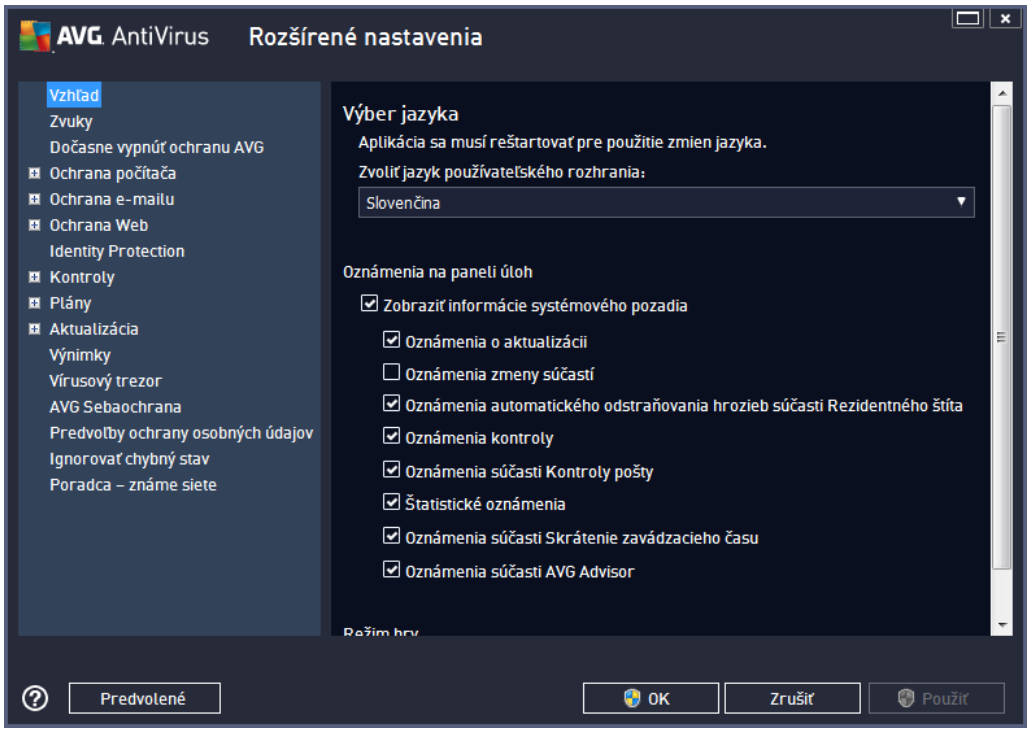
- ***Upozorniť webové lokality...*** – v tejto časti môžete prepnúť možnosť ***Upozorniť webové lokality, že nechcem byť sledovaný*** *(predvolene zapnuté).* Túto možnosť nechajte začiarknutú, aby ste potvrdili, že chcete, aby aplikácia ***Do Not Track*** informovala poskytovateľov služieb zhromažďujúcich údaje, že nechcete byť sledovaní.

9. Rozšírené nastavenia programu AVG

Dialógové okno s rozšírenou konfiguráciou produktu **AVG AntiVirus 2013** otvorí nové okno s názvom ***Rozšírené nastavenia programu AVG***. Toto okno je rozdelené na dve časti: v ľavej časti sa nachádza stromová štruktúra, ktorá sa používa na navigovanie k možnostiam konfigurácie programu. Zvolením súčasti, ktorej konfiguráciu chcete zmeniť (*alebo jej konkrétnej časti*), otvorte dialógové okno editovania v pravej časti okna.

9.1. Vzhľad

Prvá položka v navigačnej štruktúre, ***Vzhľad***, sa týka všeobecných nastavení používateľského rozhrania produktu **AVG AntiVirus 2013** a niektorých základných možností správania sa aplikácie:



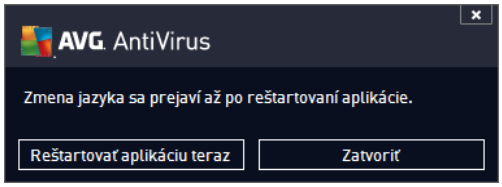
Výber jazyka

V časti ***Výber jazyka*** môžete v rozbaľovacej ponuke vybrať požadovaný jazyk. Vybraný jazyk sa potom použije pre celé používateľské rozhranie produktu **AVG AntiVirus 2013**. V rozbaľovacej ponuke sa nachádzajú len tie jazyky, ktoré ste už nainštalovali počas procesu inštalácie, plus angličtina (*tá sa inštaluje štandardne*). Zmenu jazyka produktu **AVG AntiVirus 2013** dokončíte reštartovaním aplikácie. Postupujte podľa nasledujúcich pokynov:

- V rozbaľovacej ponuke vyberte požadovaný jazyk aplikácie.
- Potvrďte výber stlačením tlačidla ***Použiť*** *(v pravom hornom rohu dialógového okna).*
- Potvrďte stlačením tlačidla ***OK.***
- Zobrazí sa nové dialógové okno s informáciami o zmene jazyka aplikácie a potrebe

reštartovať **AVG AntiVirus 2013**

- Stlačením tlačidla ***Reštartovať aplikáciu*** potvrďte súhlas s reštartovaním programu. Počkajte chvíľu, kým sa zmena jazyka prejaví:

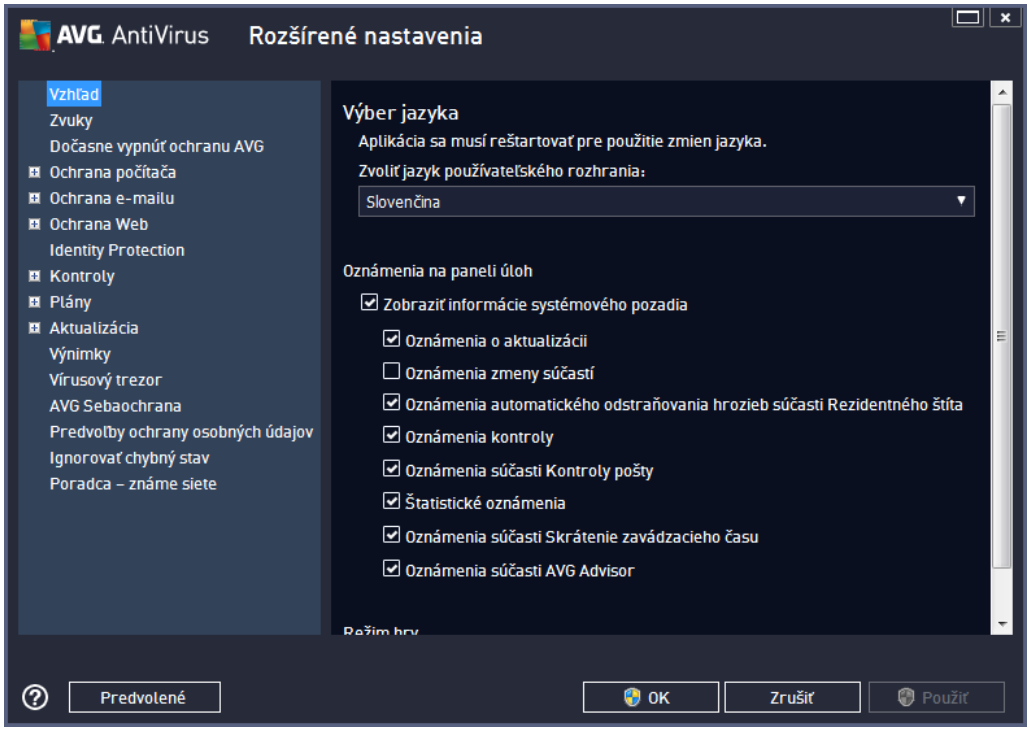


Oznámenia v paneli úloh

V tejto časti môžete zrušiť zobrazovanie oznámení v paneli úloh o stave aplikácie **AVG AntiVirus 2013**. V predvolenom nastavení je zobrazovanie oznámení v paneli úloh povolené. Dôrazne odporúčame toto nastavenie nemeniť! Systémové oznámenia informujú napríklad o spustení kontroly, spustení aktualizácie alebo o zmene súčasti **AVG AntiVirus 2013**. Týmto oznámeniam by ste rozhodne mali venovať pozornosť.

Ak sa však z nejakého dôvodu rozhodnete tieto informácie nezobrazovať alebo ak chcete zobraziť iba niektoré oznámenia *(týkajúce sa konkrétnej súčasti AVG AntiVirus 2013)*, môžete definovať a určiť vlastné predvoľby označením/zrušením označenia príslušných možností:

- ***Zobrazovať oznámenia v paneli úloh*** *(štandardne zapnuté)* – Štandardne sa zobrazujú všetky oznámenia. Ak chcete úplne vypnúť zobrazovanie všetkých oznámení, zrušte začiarknutie tejto položky. Po zapnutí môžete ďalej vybrať konkrétne oznámenia, ktoré sa majú zobrazovať:



- ***Oznámenia o aktualizáciách*** *(predvolene zapnuté)* – rozhodnite sa, či sa majú zobrazovať informácie týkajúce sa spustenia aktualizácie **AVG AntiVirus 2013**, postupu a dokončenia

- ***Oznámenia o zmene stavu súčastí*** *(predvolene vypnuté)* – rozhodnite sa, či sa majú zobrazovať informácie týkajúce sa činnosti alebo nečinnosti súčasti, prípadne či sa majú zobrazovať informácie o možnom probléme. Táto možnosť má pri oznámení chybného stavu súčasti informačnú funkciu ikony v paneli úloh, ktorá informuje o probléme týkajúcom sa súčasti produktu **AVG AntiVirus 2013**.

- ***Oznámenia automatického odstraňovania hrozieb Rezidentným štítom*** *(predvolene zapnuté)* – rozhodnite sa, či sa majú alebo nemajú zobrazovať informácie súvisiace s procesmi ukladania, kopírovania a otvárania súborov (*táto funkcia sa dá nastaviť, len keď je v súčasti Rezidentný štít zapnutá možnosť Liečiť automaticky*

- ***Oznámenia o kontrole*** *(predvolene zapnuté)* – rozhodnite sa, či sa majú zobrazovať informácie pri automatickom spustení plánu kontroly, jeho priebehu a výsledkoch

- ***Oznámenia súvisiace so súčasťou Kontrola pošty*** *(predvolene zapnuté)* – rozhodnite sa, či sa majú zobrazovať informácie po každej kontrole prichádzajúcich a odchádzajúcich e-mailových správ

- ***Štatistické oznámenia*** *(predvolene zapnuté)* – nechajte políčko začiarknuté, ak sa majú zobrazovať pravidelné štatistické prehľadové oznámenia na paneli úloh

- ***Oznámenia o skrátení zavádzacieho času*** *(predvolene vypnuté)* – rozhodnite sa, či chcete byť informovaní o skrátení zavádzacieho času systému.

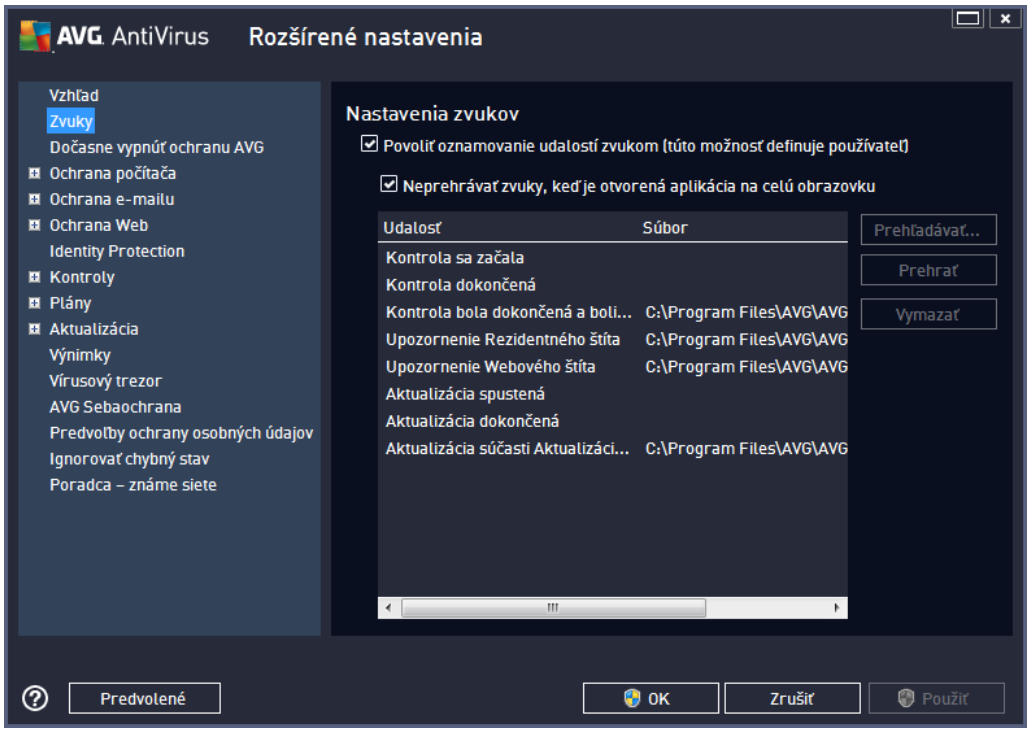
- ***Oznámenia súčasti AVG Advisor*** *(predvolene zapnuté)* – rozhodnite sa, či sa informácie o aktivite súčasti AVG Advisor majú zobrazovať v paneli úloh

Režim hrania

Táto funkcia programu AVG sa používa v súvislosti s aplikáciami spustenými na celú obrazovku, ktorých spustenie by sa mohlo narušiť (*aplikácia by sa minimalizovala alebo by sa porušila grafika*) zobrazením informačnej bubliny programu AVG (*ktorá sa zobrazí napr. pri spustení plánu kontroly*). Ak sa chcete vyhnúť podobným situáciám, nechajte začiarkavacie políčko možnosti ***Povoliť režim hrania, ak beží aplikácia v režime na celú obrazovku*** označené (*predvolené nastavenie*).

9.2. Zvuky

Dialógové okno ***Zvuky*** sa používa na zapnutie zvukových upozornení informujúcich o konkrétnych činnostiach programu **AVG AntiVirus 2013**:



Nastavenia sú platné iba pre aktuálny používateľský účet. To znamená, že používateľ na každom počítači bude mať vlastné zvukové nastavenia. Ak chcete povoliť zvukové oznamy, nechajte označenú možnosť ***Povoliť oznamovanie udalostí zvukom*** (*táto možnosť je štandardne zapnutá*), aby ste aktivovali zoznam všetkých dôležitých činností. Ďalej môžete označiť možnosť ***Neprehrávať zvuky, keď je aktívna aplikácia na celú obrazovku***, ak chcete potlačiť zvukové oznamy v situáciách, keby mohli vyrušovať *(pozrite si tiež časť Režim hry v kapitole Rozšírené nastavenia/Vzhľad v tomto dokumente)*.

Ovládacie tlačidlá

- ***Prehľadávať*** – Po označení príslušnej udalosti zo zoznamu pomocou tlačidla ***Prehľadávať*** nájdete na disku požadovaný zvukový súbor, ktorý chcete činnosti priradiť. *(V súčasnosti sú podporované iba zvukové formáty *.wav!)*

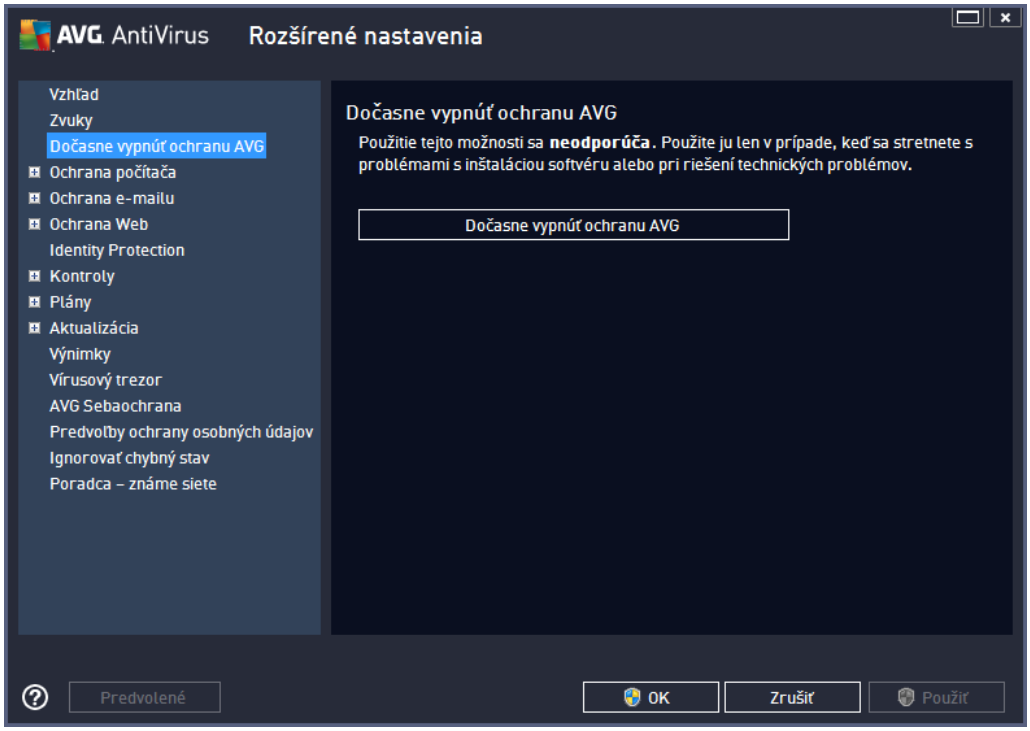
- ***Prehrať*** – Ak si chcete vypočuť zvolený zvuk, zvýraznite udalosť v zozname a stlačte tlačidlo ***Prehrať***.

- ***Vymazať*** – Na odstránenie zvuku prideleného konkrétnej udalosti použite tlačidlo ***Vymazať***
  .

9.3. Dočasne vypnúť ochranu AVG

Dialógové okno ***Dočasne vypnúť ochranu AVG*** umožňuje naraz vypnúť celú ochranu zabezpečovanú programom **AVG AntiVirus 2013**.

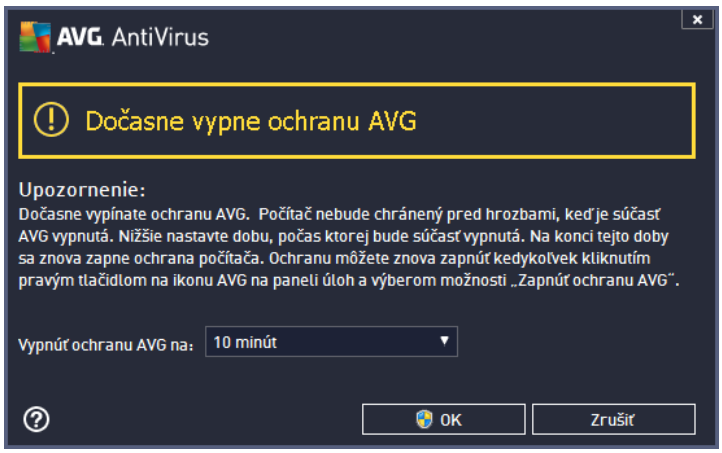
Nepoužívajte túto možnosť, ak to nie je naozaj nevyhnutné!



Vo väčšine prípadov ***nie je potrebné*** vypínať program **AVG AntiVirus 2013** pred inštaláciou nového softvéru alebo ovládačov, a to ani v prípade, ak inštalačný program alebo sprievodca inštaláciou softvéru odporúča, aby sa najskôr zatvorili otvorené programy a aplikácie z dôvodu možného nežiaduceho prerušenia procesu inštalácie. Ak sa počas inštalácie vyskytne problém, skúste najprv vypnúť rezidentnú ochranu (*Povoliť súčasť Rezidentný štít*). Ak musíte dočasne vypnúť ochranu **AVG AntiVirus 2013**, znova ju zapnite bezprostredne po dokončení úloh, pre ktoré ste ju vypli. Ak ste pripojení na internet alebo k sieti v čase, keď je antivírusový softvér vypnutý, vás počítač nie je chránený pred útokmi.

Ako vypnúť ochranu AVG

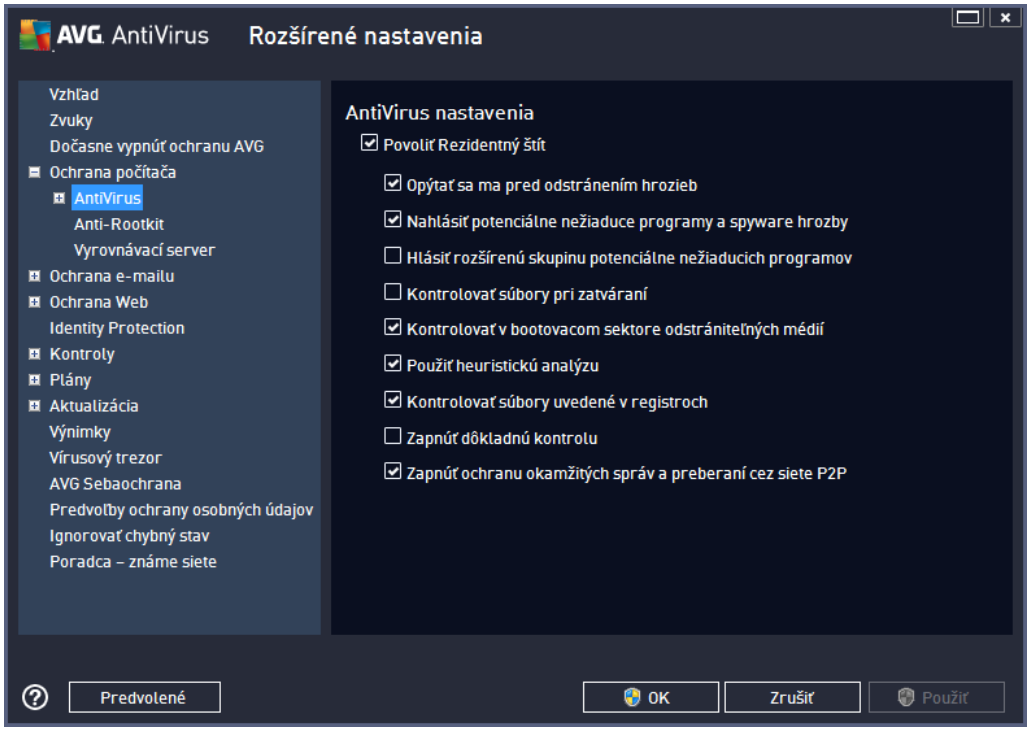
Označte začiarkavacie políčko ***Dočasne vypnúť ochranu AVG*** a potvrďte voľbu stlačením tlačidla ***Použiť***. V novootvorenom dialógovom okne ***Dočasne vypnúť ochranu AVG*** zadajte čas, na aký chcete vypnúť aplikáciu **AVG AntiVirus 2013**. V predvolenom nastavení sa ochrana vypne na 10 minút, čo by malo stačiť na dokončenie bežných úloh, ako je inštalácia nového softvéru a pod. Môžete sa rozhodnúť pre dlhší čas, no neodporúčame to, pokiaľ to nie je absolútne nutné. Potom sa všetky vypnuté súčasti automaticky znovu aktivujú. Nanajvýš môžete vypnúť ochranu AVG až do najbližšieho reštartovania počítača.



9.4. Ochrana počítača

9.4.1. AntiVirus

AntiVirus spolu s ***Rezidentným štítom*** nepretržite chránia váš počítač pred všetkými známymi druhmi vírusov, spyware a malware *(vrátane takzvaného spiaceho alebo neaktívneho malware, čo je malware, ktorý bol prevzatý, ale nebol ešte aktivovaný)*.



Dialógové okno ***Nastavenia súčasti Rezidentný štít*** umožňuje úplne aktivovať alebo vypnúť rezidentnú ochranu začiarknutím/zrušením začiarknutia položky ***Povoliť Rezidentný štít*** (*táto funkcia je štandardne zapnutá*). Okrem toho môžete určiť, ktoré funkcie rezidentnej ochrany chcete aktivovať:

- ***Opýtať sa pred odstránením hrozieb*** (*predvolene zapnuté*) – začiarknite pre zabezpečenie, že Rezidentný štít nebude vykonávať žiadne akcie automaticky a namiesto toho zobrazí dialógové okno popisujúce detegovanú hrozbu a umožní vám tak rozhodnúť sa, aká akcia by mala byť vykonaná. Ak ponecháte políčko nezačiarknuté, **AVG AntiVirus 2013** bude automaticky liečiť infekcie, a ak to nebude možné, bude objekt premiestnený do Vírusového trezora.

- ***Nahlásiť potenciálne nežiaduce programy a spyware hrozby*** (*štandardne zapnuté*) – Začiarknite toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu škodlivého softvéru: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.

- ***Hlásiť rozšírenú skupinu potenciálne nežiaducich programov*** (*štandardne vypnuté*) – začiarknite toto políčko, ak sa má detegovať rozšírená skupina spywaru: programov, ktoré sú úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpečenia počítača, ale môže blokovať dobré programy, a preto je táto funkcia štandardne vypnutá.

- ***Kontrolovať súbory pri zatváraní*** (*štandardne vypnuté*) – kontrola pri zatvorení zabezpečí, že AVG skontroluje aktívne objekty (napr. aplikácie, dokumenty…), keď sa otvárajú alebo zatvárajú; táto funkcia pomáha chrániť počítač pred niektorými druhmi dômyselných vírusov.

- ***Kontrolovať v bootovacom sektore odstrániteľných médií*** (*štandardne zapnuté*)

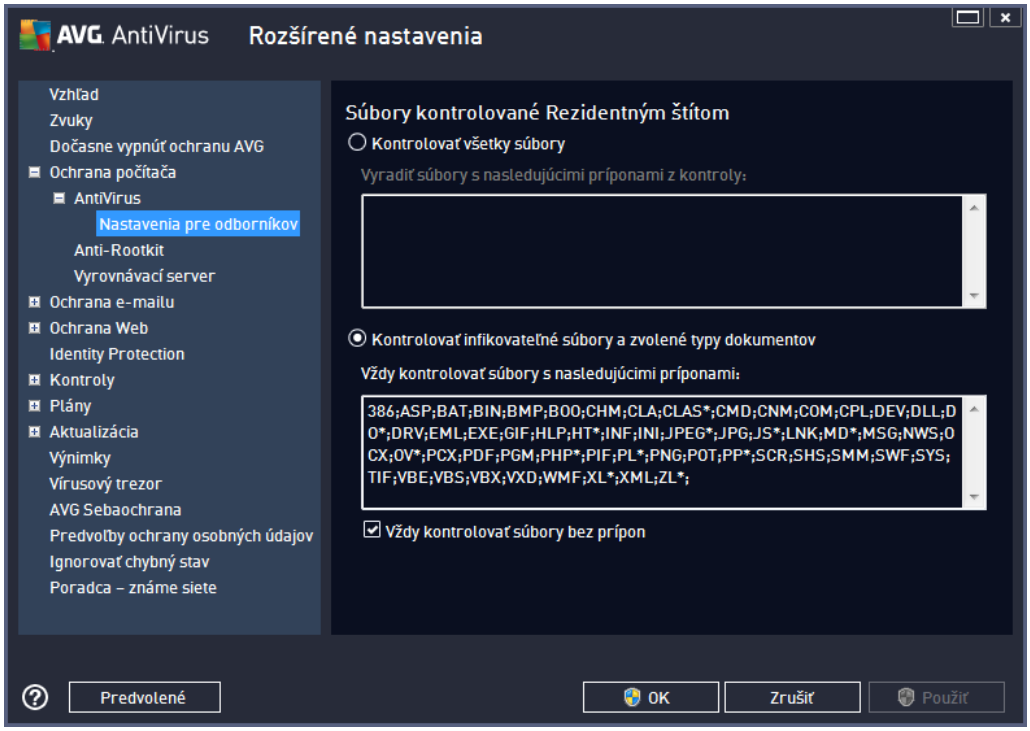
- ***Použiť heuristickú analýzu*** (*štandardne zapnuté*) – Na detekciu sa použije heuristická analýza (*dynamická emulácia inštrukcií kontrolovaného objektu v prostredí virtuálneho počítača*).

- ***Kontrolovať súbory uvedené v registroch*** (*štandardne zapnuté*) – tento parameter určuje, že AVG bude kontrolovať všetky spustiteľné súbory pridané do databázy Registry na spúšťanie pri štarte počítača, aby sa známa infekcia nemohla spustiť pri ďalšom spustení počítača.

- ***Zapnúť dôkladnú kontrolu*** (*štandardne vypnuté*) – V určitých situáciách (*napr. v stave mimoriadnej núdze*) môžete začiarknutím tohto políčka aktivovať algoritmus najdôkladnejšej kontroly, ktorý skontroluje všetky možné nebezpečné objekty do hĺbky. Upozorňujeme však, že tento spôsob je náročný na čas.

- ***Zapnúť ochranu okamžitých správ a preberaní cez siete P2P*** (*štandardne zapnuté*) – Začiarknite toto políčko, ak chcete overovať, že komunikácie cezokamžité správy (*t. j. AIM, Yahoo!, ICQ, Skype, MSN Messenger, ...*) a dáta prevzaté sieťami typu peer-to-peer *(Siete umožňujúce priame pripojenie medzi klientmi bez serverov, ktoré môžu byť nebezpečné. Obyčajne sa používajú na zdieľanie hudobných súborov.)* neobsahujú vírusy.

V dialógovom okne ***Súbory kontrolované Rezidentným štítom*** môžete nastaviť, ktoré súbory sa budú kontrolovať (*podľa konkrétnych prípon*):

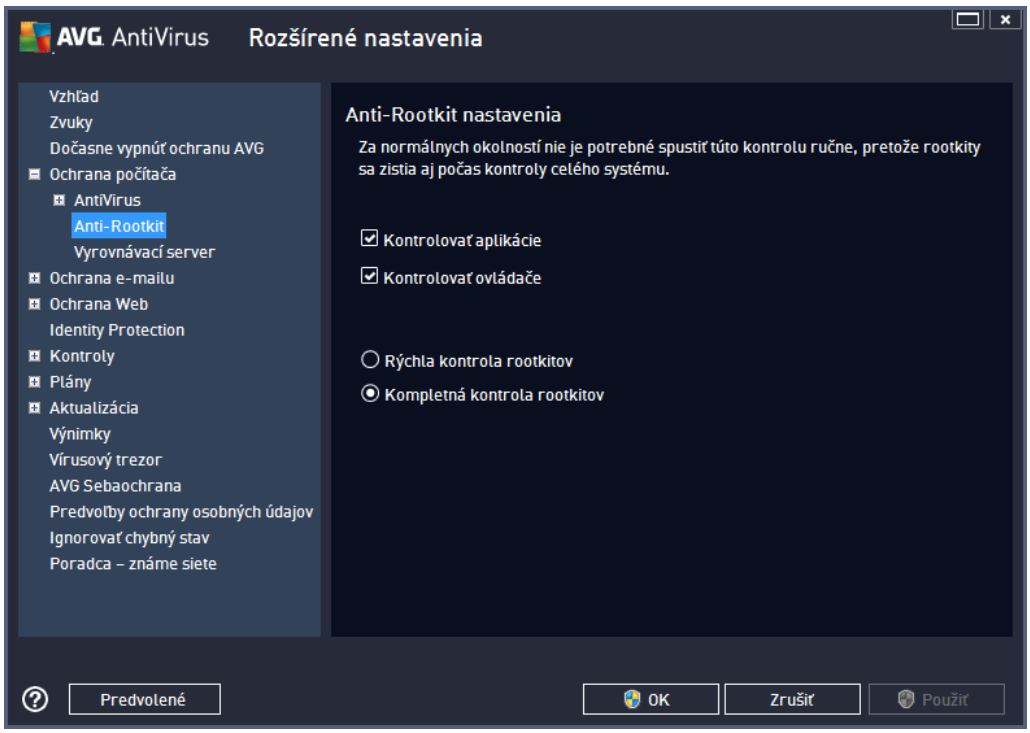


Označte príslušné začiarkavacie políčko podľa toho, či chcete použiť možnosť ***Kontrolovať všetky súbory*** alebo ***Kontrolovať infikovateľné súbory a zvolené typy dokumentov***. Ak chcete urýchliť kontrolu a súčasne zabezpečiť maximálnu úroveň ochrany, odporúčame zachovať predvolené nastavenia. Takto sa budú kontrolovať iba infikovateľné súbory. V príslušnej časti dialógového okna nájdete aj upraviteľný zoznam prípon súborov, ktoré sa majú začleniť do kontroly.

Začiarknite možnosť ***Vždy kontrolovať súbory bez prípon*** (*štandardne zapnutá*) , ak má Rezidentný štít kontrolovať aj súbory bez prípony a súbory neznámeho formátu. Odporúčame mať túto možnosť zapnutú, pretože súbory bez prípon sú podozrivé.

9.4.2. Anti-Rootkit

V dialógovom okne ***Nastavenia nástroja Anti-Rootkit*** môžete upraviť konfiguráciu služby ***Anti-Rootkit*** a konkrétne parametre kontroly. Kontrola nástrojom Anti-Rootkit je predvolený proces spustený pri Kontrole celého počítača:

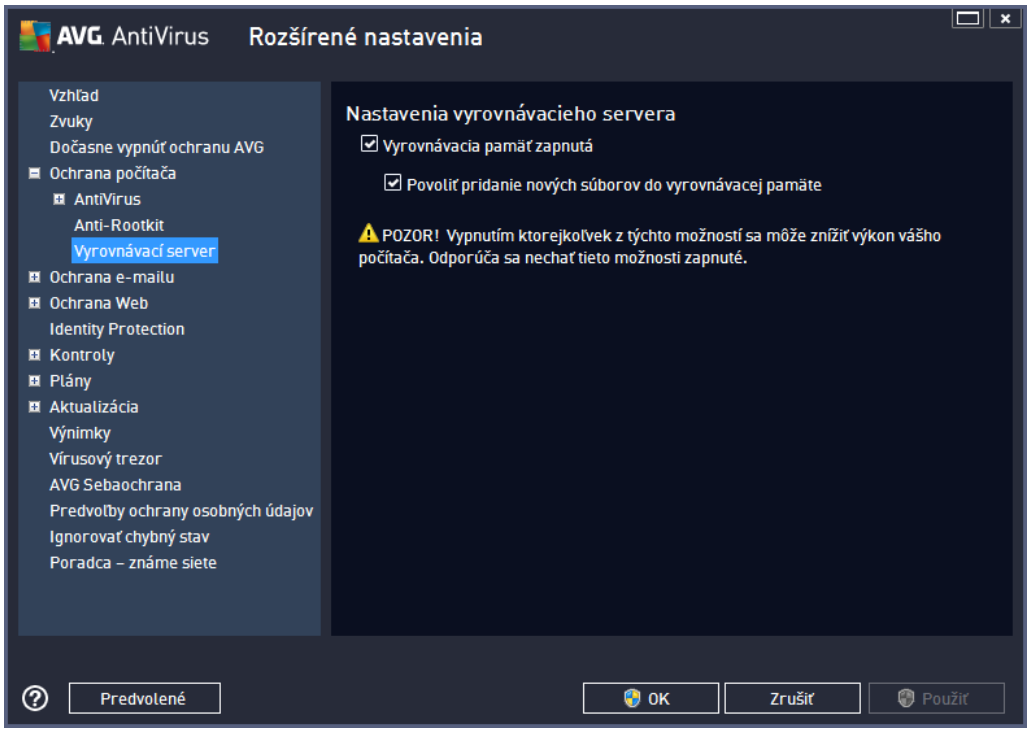


Možnosti ***Kontrolovať aplikácie*** a ***Kontrolovať ovládače*** vám umožňujú podrobne zadať, čo by malo byť súčasťou kontroly Anti-Rootkit. Tieto nastavenia sú určené pre skúsených používateľov; odporúčame vám, aby ste nechali všetky možnosti zapnuté. Môžete tiež vybrať režim kontroly rootkitov:

- ***Rýchla kontrola rootkitov*** – kontroluje všetky spustené procesy, zavedené ovládače a systémový priečinok (*zvyčajne c:\Windows*).
- ***Úplná kontrola rootkitov*** – kontroluje všetky spustené procesy, zavedené ovládače, systémový priečinok (*obyčajne c:\Windows*), plus všetky miestne disky (*vrátane pamäťových médií, nie však disketové jednotky/jednotky CD–ROM*).

9.4.3. Vyrovnávací server

Dialógové okno ***Nastavenie vyrovnávacieho servera*** sa týka procesu vyrovnávacieho servera určeného na zrýchlenie všetkých typov kontrol aplikácie **AVG AntiVirus 2013**:



Ukladá údaje zozbierané serverom a uchováva informácie o dôveryhodných súboroch (*súbor sa pokladá za dôveryhodný, ak je podpísaný digitálnym podpisom z dôveryhodného zdroja*). Tieto súbory sa potom automaticky pokladajú za bezpečné a netreba ich kontrolovať. Preto sa počas kontroly vynechávajú.

Dialógové okno ***Nastavenie vyrovnávacieho servera*** ponúka tieto možnosti konfigurácie:

- ***Vyrovnávacia pamäť zapnutá*** (*štandardne zapnuté*): Zrušením označenia tohto políčka sa vypne ***vyrovnávací server*** a vyprázdni sa vyrovnávacia pamäť. Upozorňujeme, že týmto sa môže spomaliť kontrola a znížiť celkový výkon počítača, pretože každý jeden používaný súbor sa najskôr skontroluje z hľadiska prítomnosti vírusov a spywaru.

- ***Povoliť pridanie nových súborov do vyrovnávacej pamäte*** (*štandardne zapnuté*): Zrušením označenia tohto políčka sa vypne pridávanie ďalších súborov do vyrovnávacej pamäte. Všetky súbory vo vyrovnávacej pamäti sa zachovajú a budú sa používať do úplného vypnutia funkcie vyrovnávacej pamäte, resp. do ďalšieho aktualizovania vírusovej databázy.

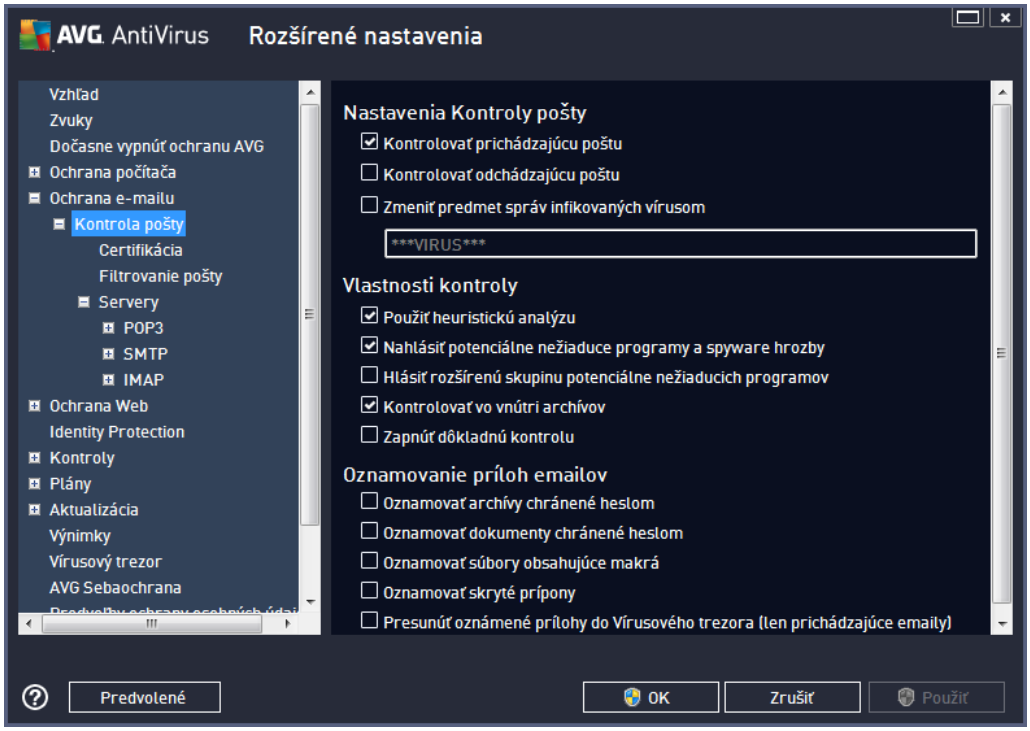
Ak nemáte oprávnený dôvod na vypnutie vyrovnávacieho servera, dôrazne odporúčame zachovať predvolené nastavenia a nechať obe možnosti zapnuté. Inak môžete zaznamenať výrazné spomalenie rýchlosti a výkonu systému.

9.5. Kontrola pošty

V tejto časti môžete upraviť podrobnosti konfigurácie nástroja Kontrola pošty a Anti-Spam:

9.5.1. Kontrola pošty

Dialógové okno ***Kontrola pošty*** je rozdelené na tri časti:



Nastavenia kontroly pošty

Táto časť umožňuje definovať tieto základné nastavenia pre prichádzajúcu alebo odchádzajúcu poštu:

- ***Kontrolovať prichádzajúcu poštu*** (*predvolene zapnuté*) – začiarknutím zapnite resp. vypnite funkciu na kontrolu všetkých e-mailov doručených do vašej poštovej aplikácie
- ***Kontrolovať odchádzajúcu poštu*** (*predvolene vypnuté*) – začiarknutím zapnite resp. vypnite funkciu na kontrolu všetkých e-mailov poslaných z vašej poštovej aplikácie
- ***Zmeniť predmet správ infikovaných vírusom*** (*predvolene vypnuté*) – ak chcete byť informovaní o detegovaní infekcie v prehľadanej e-mailovej správe, začiarknite túto položku a do textového poľa zadajte požadovaný text. Tento text sa potom pridá do poľa „Predmet“ každej detegovanej e-mailovej správy na účely jednoduchšej identifikácie a filtrovania. Predvolená hodnota je ***VIRUS*** a odporúčame vám, aby ste ju nemenili.

Vlastnosti kontroly

Táto časť sa používa na nastavenie spôsobu, akým sa budú e-mailové správy prehľadávať:

- ***Použiť heuristickú analýzu*** (*predvolene zapnuté*) – začiarknite túto možnosť, ak chcete používať metódu heuristickej detekcie pri kontrole e-mailových správ. Keď je táto možnosť zapnutá, môžete filtrovať prílohy e-mailov nielen podľa prípony, ale aj podľa samotného obsahu prílohy. Filtrovanie sa nastavuje v dialógovom okne Filtrovanie pošty.

- ***Nahlásiť potenciálne nežiaduce programy a spyware hrozby*** (*štandardne zapnuté*) – Začiarknite toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu škodlivého softvéru: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.

- ***Hlásiť rozšírenú skupinu potenciálne nežiaducich programov*** (*štandardne vypnuté*) – Začiarknite toto políčko, ak sa má detegovať rozšírená skupina spywaru: programov, ktoré sú úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpečenia počítača, ale môže blokovať dobré programy, a preto je táto funkcia štandardne vypnutá.

- ***Kontrolovať vo vnútri archívov*** (*predvolene zapnuté*) – začiarknite toto políčko, ak sa má prehľadávať obsah archívov priložených k e-mailovým správam

- ***Zapnúť dôkladnú kontrolu*** (*štandardne vypnuté*) – v určitých situáciách (*napr. pri podozrení na infikovanie počítača vírusom alebo zneužitím*) môžete začiarknutím tohto políčka aktivovať algoritmus najdôkladnejšej kontroly, ktorá skontroluje aj tie oblasti počítača, ktoré bývajú infikované len vo výnimočných prípadoch – len pre istotu. Upozorňujeme však, že tento spôsob je náročný na čas.

Oznamovanie príloh e-mailov

Táto časť umožňuje nastaviť ďalšie správy o súboroch, ktoré môžu byť potenciálne nebezpečné alebo podozrivé. Nezobrazí sa žiadne dialógové okno, na koniec e-mailovej správy sa len pridá text certifikácie a všetky takéto správy budú uvedené v dialógovom okne Nálezy súčasti Ochrana e-mailu:

- ***Oznamovať archívy chránené heslom*** – Archivačné súbory (*ZIP, RAR atď.*), ktoré sú chránené heslom, sa nedajú skontrolovať z hľadiska prítomnosti vírusov. Začiarknite toto políčko, ak sa majú oznamovať tieto archívy ako potenciálne nebezpečné.

- ***Oznamovať dokumenty chránené heslom*** – Dokumenty chránené heslom sa nedajú skontrolovať na prítomnosť vírusov; začiarknite toto políčko, ak sa majú oznamovať tieto dokumenty ako potenciálne nebezpečné.

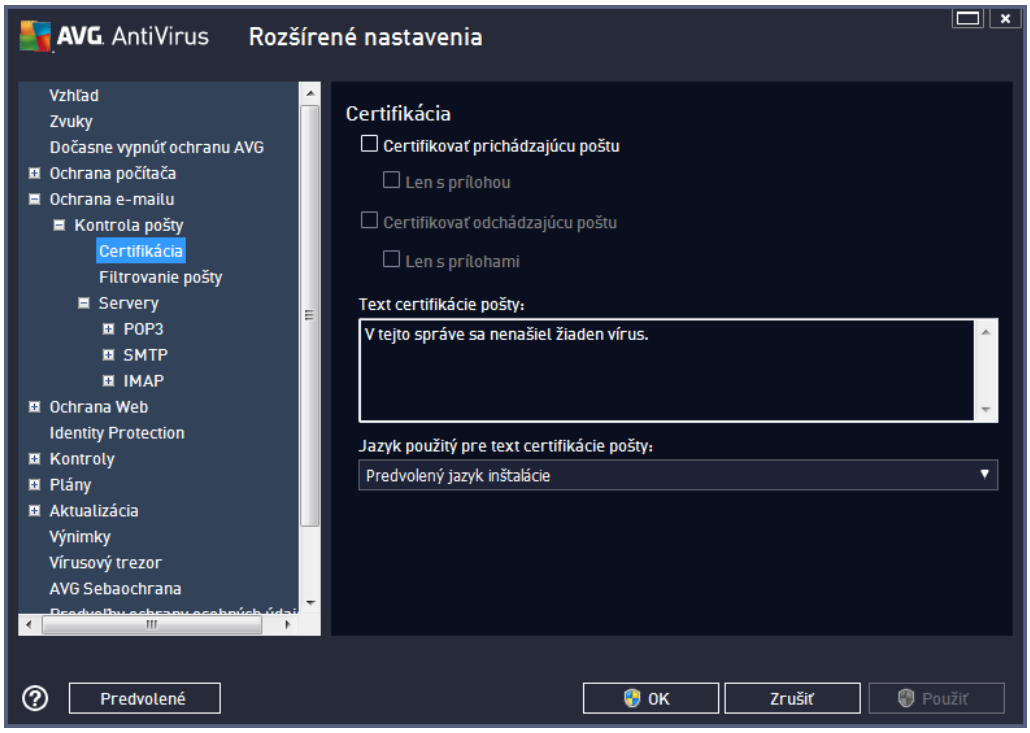
- ***Oznamovať súbory obsahujúce makrá*** – makro je vopred definovaný sled krokov, ktoré zjednodušujú konkrétne úlohy používateľovi (*makrá sa bežne používajú v programe MS Word*). Makro ako také môže obsahovať potenciálne nebezpečné inštrukcie, a preto je vhodné začiarknuť toto políčko, aby sa súbory s makrami oznamovali ako podozrivé.

- ***Oznamovať skryté prípony*** – Skrytá prípona môže spôsobiť, že sa bude podozrivý spustiteľný súbor „niečo.txt.exe“ javiť ako neškodný jednoduchý textový súbor „niečo.txt“; začiarknite toto políčko, ak sa majú tieto súbory oznamovať ako potenciálne nebezpečné.

- ***Premiestniť hlásené prílohy do Vírusového trezora*** – nastavte, či si želáte byť

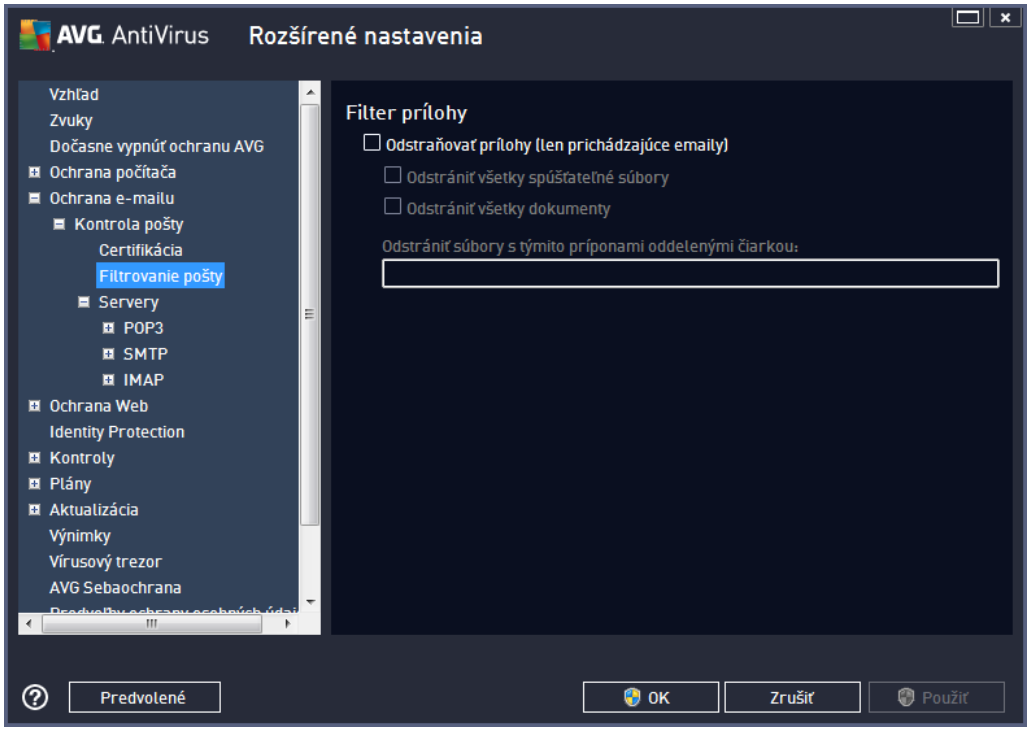
informovaní e-mailom o archívoch chránených heslom, dokumentoch chránených heslom, súboroch s makrami alebo súboroch so skrytou príponou, ktoré boli detegované ako príloha kontrolovanej e-mailovej správy. Ak sa má táto správa zobraziť počas kontroly, potom nastavte, či sa má detegovaný infikovaný objekt premiestniť do Vírusového trezora.

V dialógovom okne ***Certifikácia*** môžete označiť konkrétne začiarkavacie políčka a určiť, či chcete certifikovať prichádzajúcu poštu (***Certifikovať prichádzajúcu poštu***) alebo odchádzajúcu poštu (***Certifikovať odchádzajúcu poštu***). Pri každej možnosti môžete ďalej určiť parameter ***Len s prílohami***. Vtedy sa certifikácia bude týkať iba e-mailových správ s prílohami:



Štandardne text certifikácie obsahuje iba základné informácie: *V tejto správe sa nenašiel žiadny vírus.* Tieto informácie však podľa potreby môžete rozšíriť alebo zmeniť: do poľa ***Text e-mailovej certifikácie*** napíšte požadovaný text certifikácie. V časti ***Jazyk použitý pre text certifikácie pošty*** môžete ďalej definovať, v akom jazyku sa má automaticky vytváraná časť certifikácie (*V tejto správe sa nenašiel žiadny vírus*) zobraziť.

Poznámka: *Nezabudnite, že v požadovanom jazyku sa zobrazí iba predvolený text. Váš vlastný text sa automaticky nepreloží!*



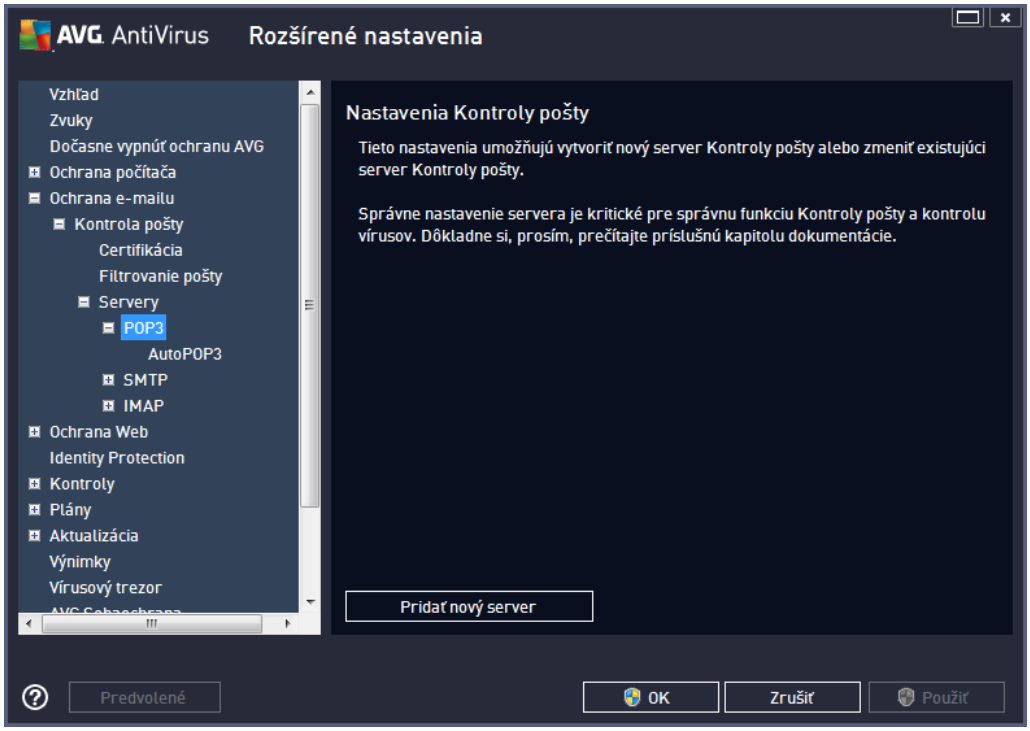
Dialógové okno ***Filter príloh*** umožňuje nastaviť parametre pre prehľadávanie príloh e-mailových správ. Štandardne je možnosť ***Odstrániť prílohy*** vypnutá. Ak sa rozhodnete funkciu aktivovať, všetky prílohy e-mailových správ detegované ako infekcie alebo potenciálne nebezpečné programy sa automaticky odstránia. Ak chcete definovať konkrétne typy príloh, ktoré sa majú odstrániť, vyberte príslušnú možnosť:

- ***Odstrániť všetky spustiteľné súbory*** – vymažú sa všetky súbory s príponou exe.
- ***Odstrániť všetky dokumenty*** – vymažú sa všetky súbory s príponami doc, docx, xls a xlsx.
- ***Odstrániť súbory s týmito príponami oddelenými čiarkou*** – odstránia sa všetky súbory s uvedenými príponami.

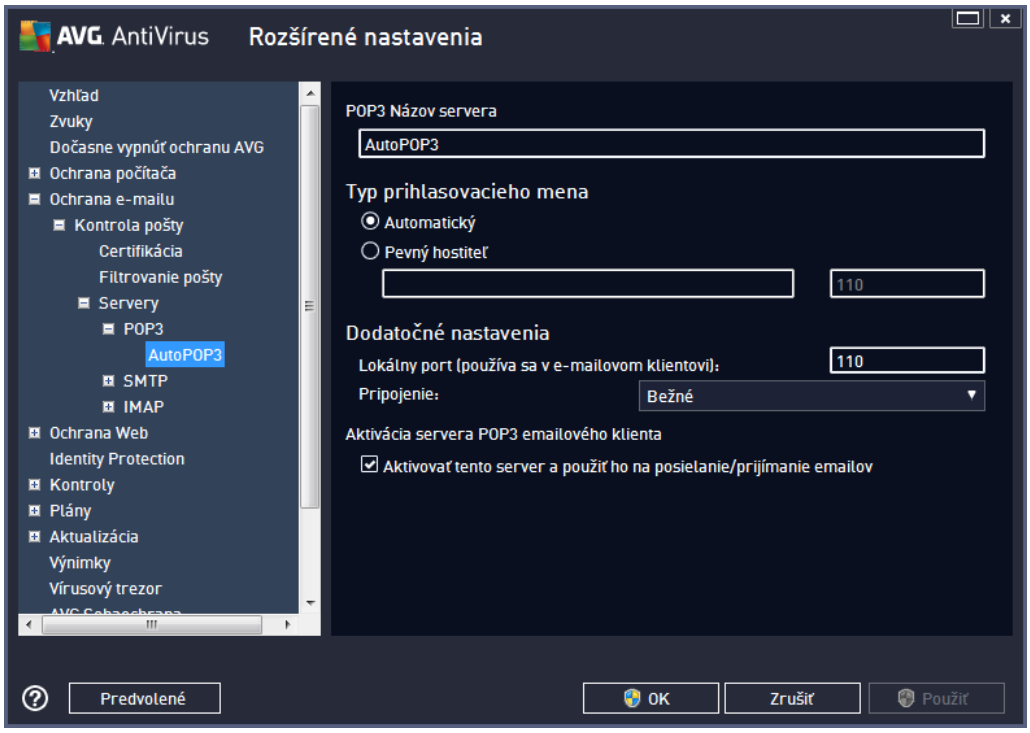
V časti ***Servery*** môžete upraviť parametre serverov súčasti Kontrola pošty:

- Server POP3
- Server SMTP
- Server IMAP

Pomocou tlačidla ***Pridať nový server*** môžete definovať nové servery pre prichádzajúcu alebo odchádzajúcu poštu.



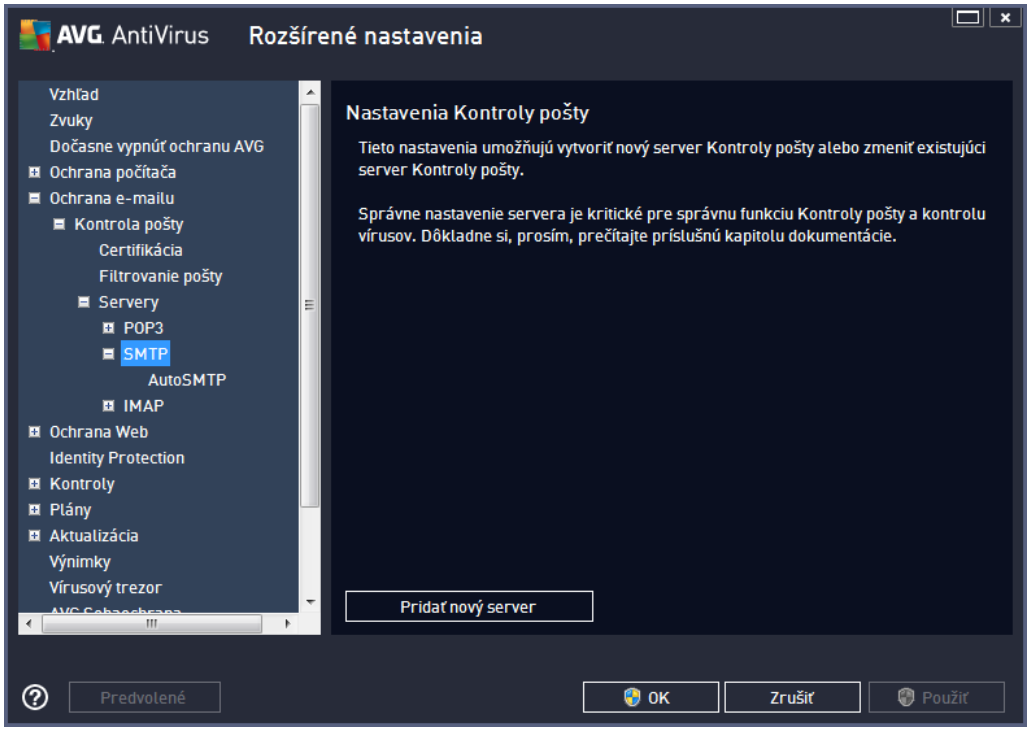
Toto dialógové okno umožňuje nastaviť pre súčasť Kontrola pošty nový server pomocou protokolu POP3 pre prichádzajúcu poštu:



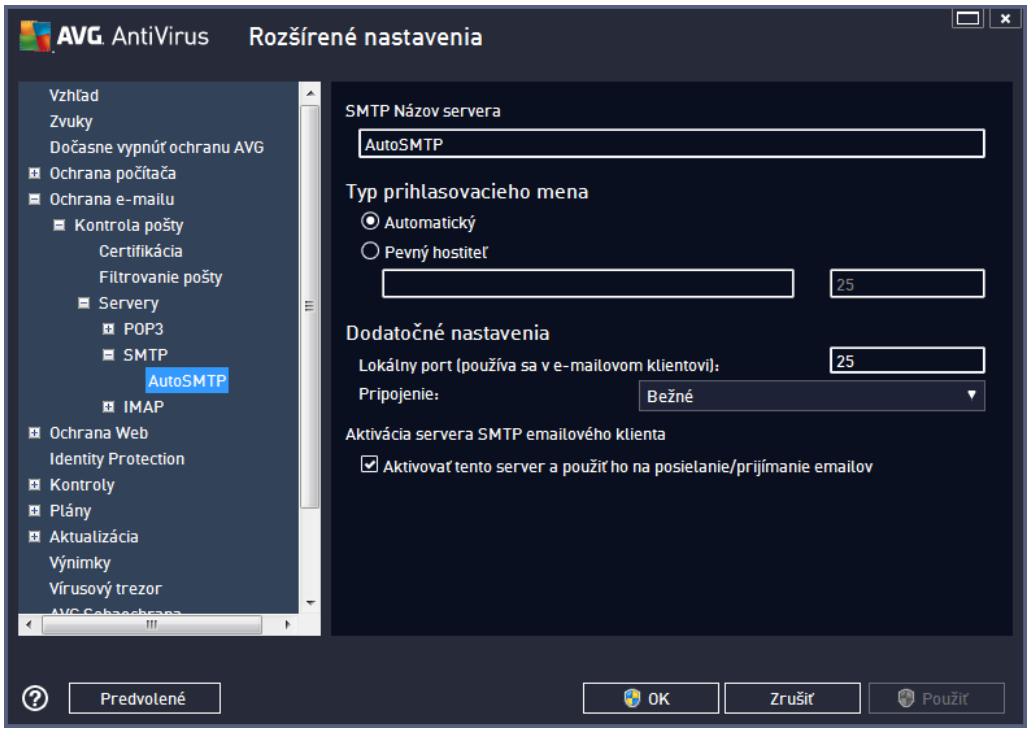
- ***Názov servera POP3*** – do tohto poľa zadajte názov novopridaných serverov (*na pridanie*

servera POP3 kliknite pravým tlačidlom myši na položku POP3 v ľavej navigačnej ponuke). Pre automaticky vytvorené servery „AutoPOP3“ je toto pole vypnuté.

- ***Typ prihlasovacieho mena*** – Určuje spôsob stanovenia poštového servera pre prichádzajúcu poštu:
    - ***Automaticky*** –
    - ***Pevný hostiteľ*** – V tomto prípade program vždy použije server, ktorý je tu uvedený. Zadajte adresu alebo názov vášho poštového servera. Prihlasovacie meno zostane nezmenené. Ako názov môžete použiť názov domény (*napríklad pop.acme.com*) alebo adresu IP (*napríklad 123.45.67.89*). Ak poštový server používa neštandardný port, môžete zadať tento port za názvom servera a použite dvojbodku ako oddeľovací znak (*napríklad pop.acme.com:8200*). Štandardný port pre komunikáciu POP3 je 110.
- ***Ďalšie nastavenia*** – používa sa na definovanie podrobnejších parametrov:
    - ***Lokálny port*** – určuje port, na ktorom sa očakáva komunikácia prichádzajúca z vašej poštovej aplikácie. Potom musíte v poštovej aplikácii nastaviť tento port ako port pre komunikáciu POP3.
    - ***Pripojenie*** – táto rozbaľovacia ponuka sa používa na nastavenie typu pripojenia, ktoré sa má použiť (*bežné/SSL/SSL predvolené*). Ak nastavíte pripojenie SSL, potom sa budú posielané dáta šifrovať a žiadna tretia strana ich nebude môcť vystopovať ani monitorovať. Táto funkcia je dostupná len vtedy, keď ju podporuje cieľový poštový server.
- ***Aktivovanie servera POP3 v poštovej aplikácii*** – začiarknutím alebo zrušením začiarknutia tejto položky sa aktivuje resp. deaktivuje uvedený server POP3



Toto dialógové okno umožňuje nastaviť pre súčasť Kontrola pošty nový server pomocou protokolu SMTP pre odchádzajúcu poštu:



- ***Názov servera SMTP*** – do tohto poľa zadajte názov novopridaných serverov (*na pridanie*

servera SMTP kliknite pravým tlačidlom myši na položku SMTP v ľavej navigačnej ponuke). Pre automaticky vytvorené servery „AutoSMTP“ je toto pole vypnuté.

- ***Typ prihlásenia*** – určuje spôsob zistenia poštového servera, ktorý sa používa pre prichádzajúcu poštu:

    - ***Automaticky*** – prihlásenie sa uskutoční automaticky podľa nastavení poštovej aplikácie

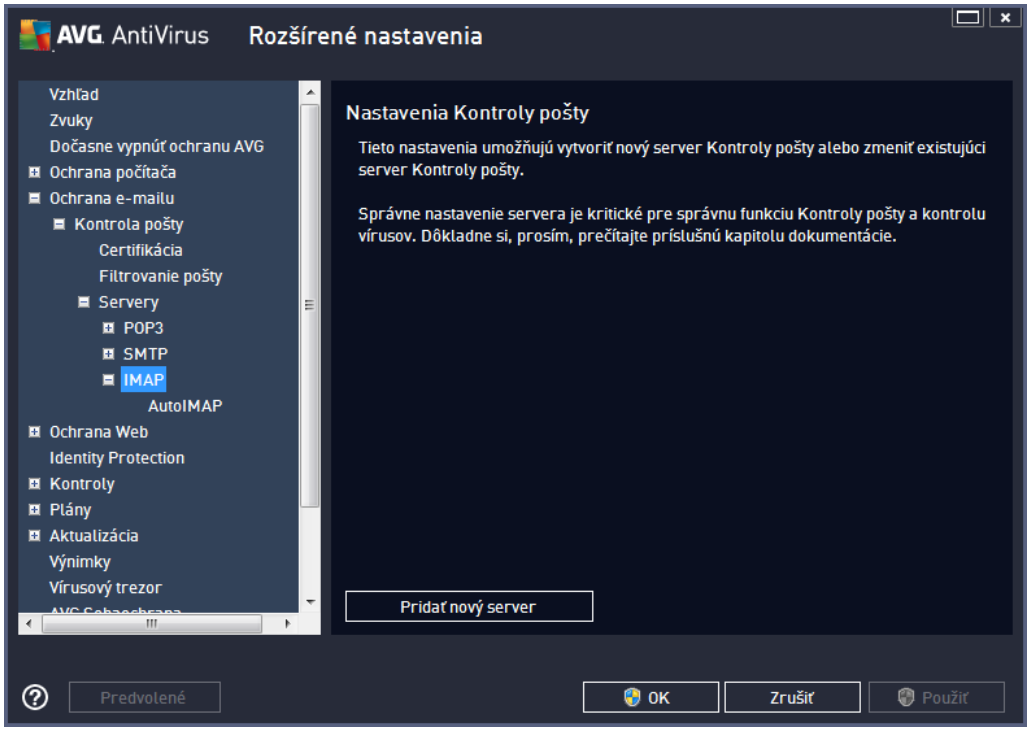
    - ***Pevný hostiteľ*** – V tomto prípade program vždy použije server, ktorý je tu uvedený. Zadajte adresu alebo názov vášho poštového servera. Ako názov môžete použiť názov domény (*napríklad smtp.acme.com*) alebo adresu IP (*napríklad 123.45.67.89*). Ak poštový server používa neštandardný port, môžete zadať tento port za názvom servera. Ako oddeľovací znak použite dvojbodku (*napríklad smtp.acme.com:8200*). Štandardný port komunikácie SMTP je 25.

- ***Ďalšie nastavenia*** – používa sa na definovanie podrobnejších parametrov:

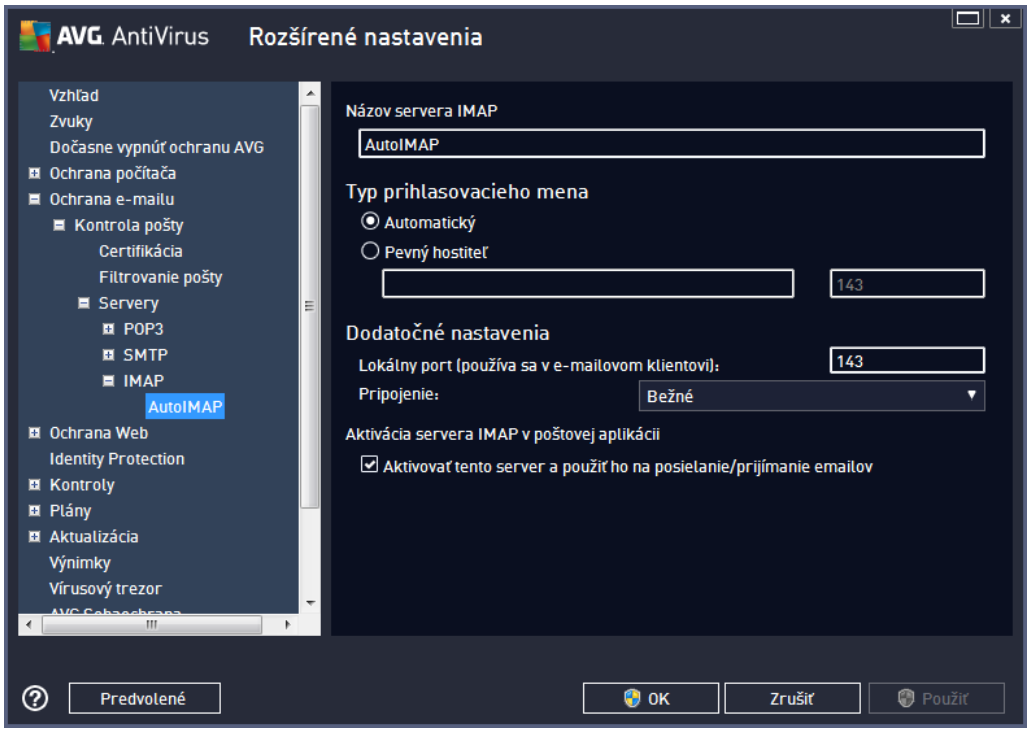
    - ***Lokálny port*** – určuje port, na ktorom sa očakáva komunikácia prichádzajúca z vašej poštovej aplikácie. Potom musíte v poštovej aplikácii nastaviť tento port ako port pre komunikáciu SMTP.

    - ***Pripojenie*** – táto rozbaľovacia ponuka sa používa na nastavenie typu pripojenia, ktoré sa má použiť (*bežné/SSL/SSL predvolené*). Ak nastavíte pripojenie SSL, potom sa budú posielané dáta šifrovať a žiadna tretia strana ich nebude môcť vystopovať ani monitorovať. Táto funkcia je dostupná len vtedy, keď ju podporuje cieľový poštový server.

- ***Aktivovanie servera SMTP v poštovej aplikácii*** – začiarknutím alebo zrušením začiarknutia tohto políčka sa aktivuje, resp. deaktivuje uvedený server SMTP



Toto dialógové okno umožňuje nastaviť pre súčasť Kontrola pošty nový server pomocou protokolu IMAP pre odchádzajúcu poštu:



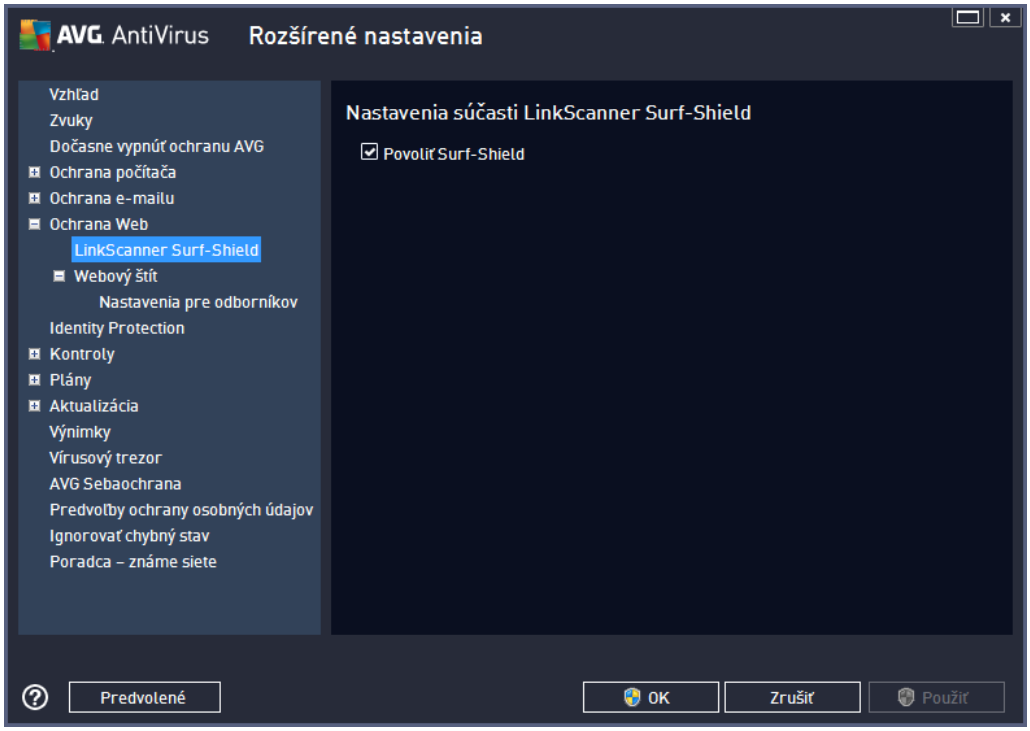
- ***Názov servera IMAP*** – do tohto poľa zadajte názov novopridaných serverov (*na pridanie*

servera IMAP kliknite pravým tlačidlom myši na položku IMAP v ľavej navigačnej ponuke). Pre automaticky vytvorené servery „AutoIMAP“ je toto pole vypnuté.

- ***Typ prihlásenia*** – určuje spôsob zistenia poštového servera, ktorý sa používa pre prichádzajúcu poštu:
    - ***Automaticky*** – prihlásenie sa uskutoční automaticky podľa nastavení poštovej aplikácie
    - ***Pevný hostiteľ*** – V tomto prípade program vždy použije server, ktorý je tu uvedený. Zadajte adresu alebo názov vášho poštového servera. Ako názov môžete použiť názov domény (*napríklad smtp.acme.com*) alebo adresu IP (*napríklad 123.45.67.89*). Ak poštový server používa neštandardný port, môžete zadať tento port za názvom servera použitím dvojbodky ako oddeľovací znak (*napríklad smtp.acme.com:8200*). Štandardný port pre komunikáciu IMAP je 143.
- ***Ďalšie nastavenia*** – používa sa na definovanie podrobnejších parametrov:
    - ***Lokálny port*** – určuje port, na ktorom sa očakáva komunikácia prichádzajúca z vašej poštovej aplikácie. Potom musíte nastaviť tento port v poštovej aplikácii ako port komunikácie IMAP.
    - ***Pripojenie*** – táto rozbaľovacia ponuka sa používa na nastavenie typu pripojenia, ktoré sa má použiť (*bežné/SSL/SSL predvolené*). Ak si zvolíte pripojenie SSL, zaslané údaje budú zakódované bez rizika vystopovania alebo monitorovania treťou stranou. Táto funkcia je dostupná len vtedy, keď ju podporuje cieľový poštový server.
- ***Aktivovanie servera IMAP v poštovej aplikácii*** – začiarknutím alebo zrušením začiarknutia tohto políčka sa aktivuje, resp. deaktivuje uvedený server IMAP

9.6. Ochrana prezerania webu

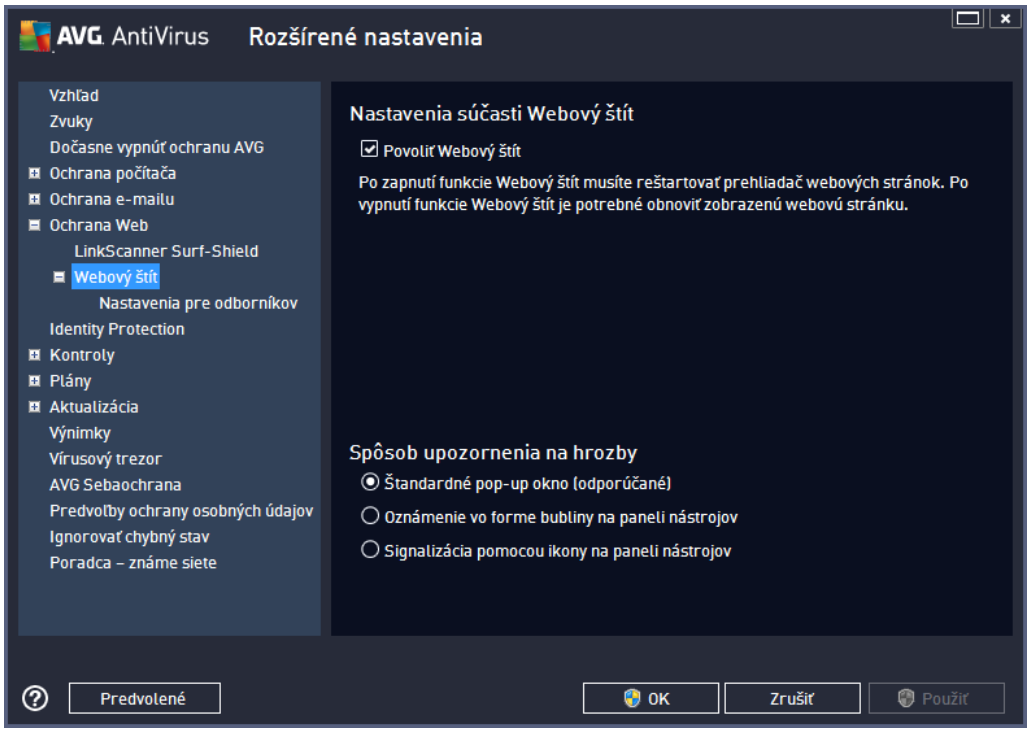
Dialógové okno s nastaveniami súčasti ***LinkScanner*** vám umožňuje zapnúť/vypnúť tieto funkcie:



- ***Povoliť Surf-Shield*** – (*štandardne zapnuté*): aktívna ochrana (*v reálnom čase*) pred webovými stránkami s nebezpečným obsahom pri ich otvorení. Pripojenie k známym škodlivým stránkam a ich nebezpečnému obsahu sa zablokuje pri otváraní v internetovom prehliadači (*alebo inej aplikácii, ktorá používa protokol HTTP*).

- ***Pridať 'Zabezpečené súčasťou LinkScanner'...*** – (*štandardne vypnuté*): potvrdením tejto možnosti zaistíte, že všetky správy odoslané zo sociálnych sietí Facebook/MySpace obsahujúce aktívne hypertextové odkazy budú obsahovať potvrdenie, že boli skontrolované súčasťou LinkScanner.

9.6.1. Webový štít

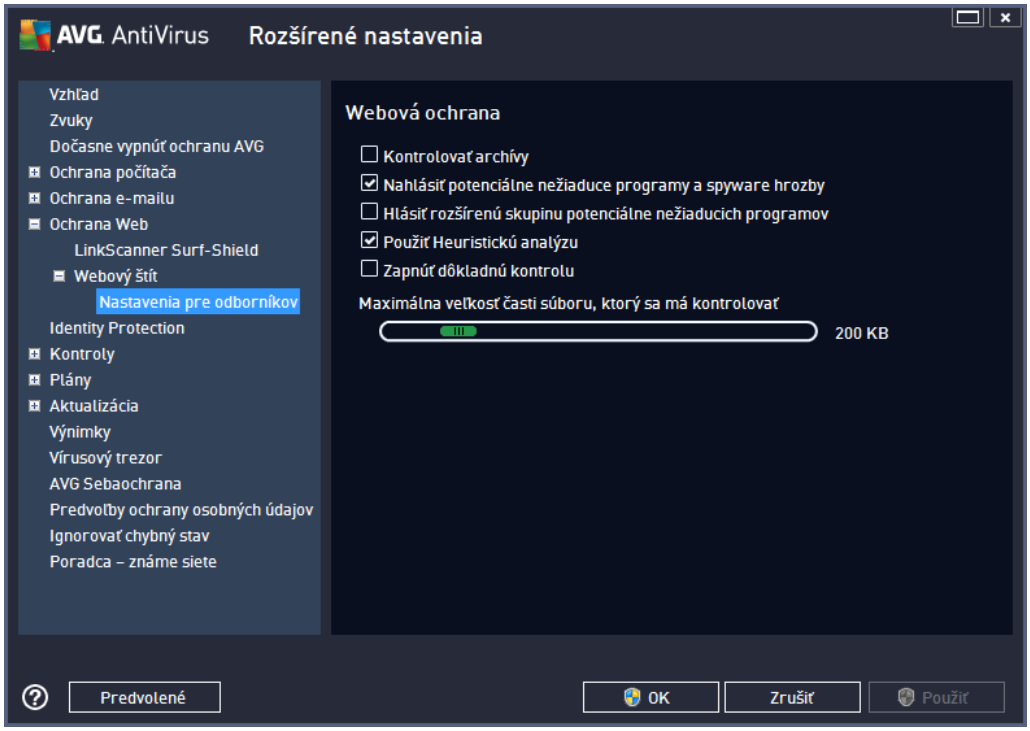


Dialógové okno ***Webový štít*** ponúka tieto možnosti:

- ***Povoliť Webový štít*** *(štandardne zapnuté)* – Aktivuje/deaktivuje celú službu ***Webový štít***. Ďalšie rozšírené nastavenia súčasti ***Webový štít*** nájdete v nasledujúcom dialógovom okne s názvom Webová ochrana.

Spôsob upozornenia na hrozby

V spodnej časti dialógového okna nastavte, akým spôsobom vás má program informovať o potenciálnej detegovanej hrozbe: pomocou štandardného kontextového okna, oznámenia v bubline na paneli úloh alebo informačnej ikony v paneli úloh.



Dialógové okno ***Webová ochrana*** umožňuje upraviť konfiguráciu súčasti z hľadiska kontroly obsahu internetových stránok. Rozhranie editácie umožňuje nastaviť tieto základné možnosti:

- ***Zapnúť webovú ochranu*** – Keď je táto funkcia zapnutá, potom bude súčasť ***Webový štít*** kontrolovať obsah internetových stránok. Za predpokladu, že je táto súčasť zapnutá (*štandardne je*), môžete aj tieto položky zapnúť/vypnúť:

    - ***Kontrolovať archívy*** – (*štandardne vypnuté*): kontrolovať obsah archívov, ktoré sa môžu nachádzať na otvorenej internetovej stránke.

    - ***Nahlásiť potenciálne nežiaduce programy a spyware hrozby*** *(predvolene zapnuté)* – začiarknite toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu škodlivého softvéru: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.

    - ***Hlásiť rozšírenú skupinu potenciálne nežiaducich programov*** – (*štandardne vypnuté*): Začiarknite toto políčko, ak sa má detegovať rozšírená skupina spywaru: programov, ktoré sú úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpečenia počítača, ale môže blokovať dobré programy, a preto je táto funkcia štandardne vypnutá.

    - ***Použiť heuristickú analýzu*** (*štandardne zapnuté*): kontrolovať obsah zobrazenej stránky pomocou metódy heuristickej analýzy (*dynamickej emulácie inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí*).

- ***Zapnúť dôkladnú kontrolu*** (*štandardne vypnuté*) – V určitých situáciách (*podozrenie na infikovanie počítača*) môžete touto možnosťou aktivovať najdôkladnejšie kontrolné algoritmy, ktoré pre istotu skontrolujú aj tie oblasti počítača, ktoré sa obyčajne vôbec neinfikujú. Upozorňujeme však, že tento spôsob je náročný na čas.

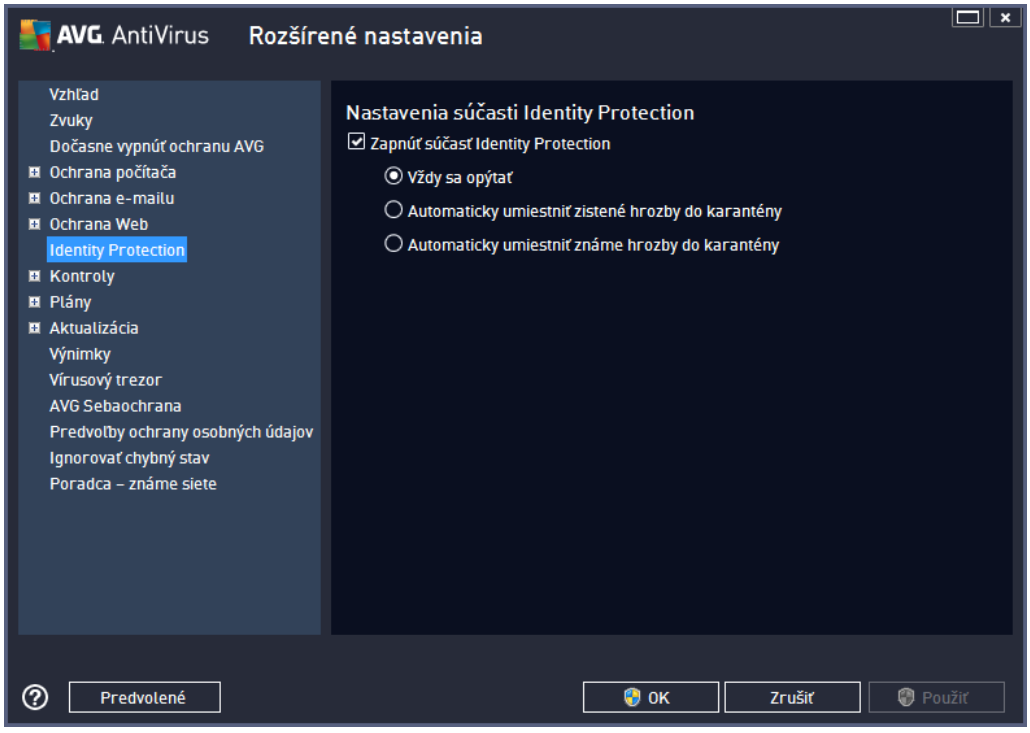
- ***Maximálna čiastková veľkosť kontrolovaného súboru*** – ak sa priložené súbory nachádzajú na otvorenej stránke, potom sa ich obsah môže zároveň skontrolovať ešte predtým, než sa súbory prevezmú do počítača. Kontrola veľkých súborov však chvíľu trvá a preberanie z internetovej stránky sa môže výrazne spomaliť. Pomocou posúvača môžete nastaviť maximálnu veľkosť súboru, ktorá sa má kontrolovať súčasťou ***Webový štít***. Aj keď je prevzatý súbor väčší než nastavená hodnota a z tohto dôvodu ho súčasť Webový štít neskontroluje, váš počítač je stále chránený: ak je súbor infikovaný, súčasť ***Rezidentný štít*** ho ihneď deteguje.

- ***Vylúčiť hostiteľa/adresu IP/domény*** – Do textového poľa zadajte presný názov servera (*hostiteľa, adresu IP, adresu IP s maskou alebo adresu URL*) alebo doménu, ktorú nemá súčasť ***Webový štít*** kontrolovať. Preto vylúčte len hostiteľa, o ktorom ste si absolútne istí, že by nikdy neposlal nebezpečné dáta.

9.7. Identity Protection

Funkcia ***Identity Protection*** je komponent na ochranu pred programami malware všetkých typov (*spyware, softvérové roboty, krádeže identity...*). Používa behaviorálne technológie a poskytuje okamžitú ochranu pred novými vírusmi *(podrobný popis funkcií komponentov nájdete v kapitole Identity*).

Dialógové okno ***Nastavenia súčasti Identity Protection*** vám umožňuje zapnúť alebo vypnúť základné funkcie súčasti Identity Protection:



Zapnúť súčasť Identity Protection(*predvolene zapnutá*) – zrušením začiarknutia sa vypne súčasť Identity Protection.

Odporúčame, aby ste tak urobili iba v prípade, ak to je naozaj nevyhnutné!

Keď je súčasť Identity Protection zapnutá, môžete nastaviť, čo sa má urobiť pri detegovaní hrozby:

- ***Vždy sa opýtať*** (*predvolene zapnuté*) – pri detegovaní hrozby sa vás program opýta, či sa má hrozba premiestniť do karantény, aby nedošlo k neželanému odstráneniu aplikácií, ktoré chcete používať.
- ***Automaticky umiestniť zistené hrozby do karantény*** – Označte toto začiarkavacie políčko, ak sa majú všetky potenciálne zistené hrozby ihneď premiestniť na bezpečné miesto vo Vírusovom trezore. Keď zachováte predvolené nastavenia, potom sa vás program opýta pri detegovaní hrozby, či sa má táto hrozba premiestniť do karantény, aby nedošlo k odstráneniu aplikácií, ktoré chcete používať.
- ***Automaticky umiestniť známe hrozby do karantény*** – Nechajte toto začiarkavacie políčko označené, ak sa majú všetky aplikácie označené ako potenciálne škodlivé automaticky a ihneď premiestniť do Vírusového trezora.

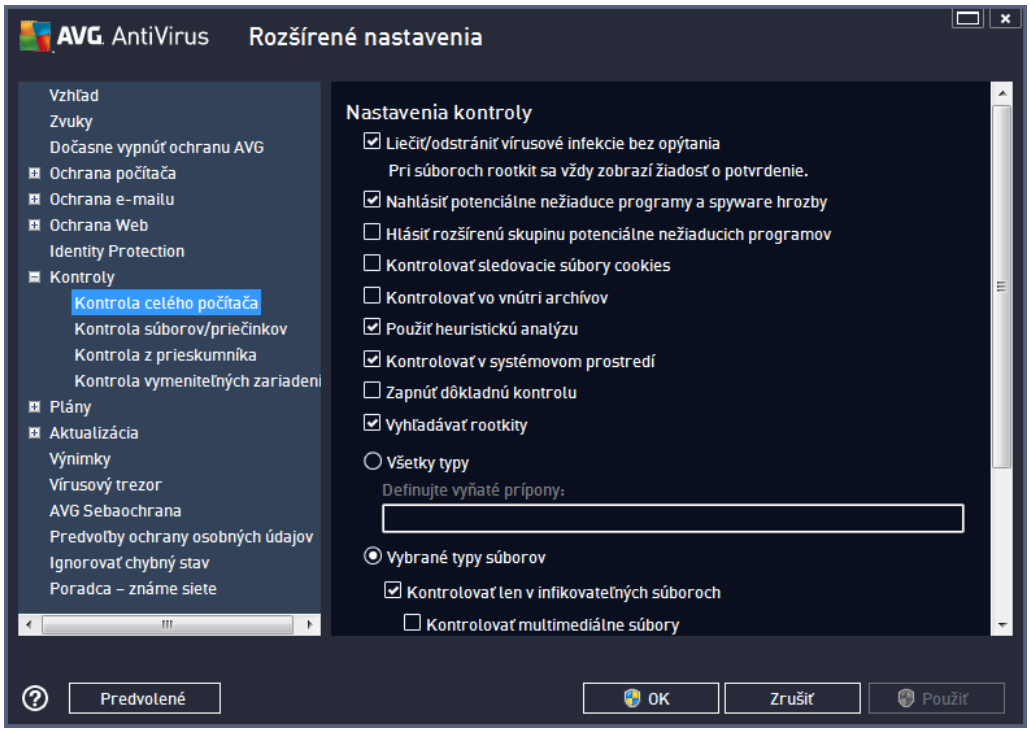
9.8. Kontroly

Rozšírené nastavenia kontroly sú rozdelené na štyri kategórie podľa konkrétnych typov kontroly definovaných dodávateľom softvéru:

- ***Kontrola celého počítača*** – štandardná vopred definovaná kontrola celého počítača.
- ***Kontrola z prieskumníka*** – špeciálna kontrola vybraného objektu priamo v prostredí programu Windows Explorer.
- ***Kontrola súborov/priečinkov*** – štandardná vopred definovaná kontrola vybraných oblastí počítača.
- ***Kontrola vymeniteľných zariadení*** – špeciálna kontrola vymeniteľných zariadení zapojených do počítača.

9.8.1. Kontrola celého počítača

Funkcia ***Kontrola celého počítača*** umožňuje upraviť parametre jednej z kontrol vopred definovaných výrobcom softvéru, Kontrola celého počítača:



Nastavenia kontroly

V časti ***Nastavenia kontroly*** sa nachádza zoznam parametrov prehľadávania, ktoré sa dajú voliteľne zapnúť resp. vypnúť:

- ***Liečiť/odstrániť infekciu bez opýtania*** (*štandardne zapnuté*) – Ak sa počas kontroly zistí prítomnosť vírusu, môže sa automaticky vyliečiť, ak je k dispozícii liečba. Ak nie je možné infikovaný súbor vyliečiť automaticky, premiestni sa do Vírusového trezora.

- ***Nahlásiť potenciálne nežiaduce programy a spyware hrozby*** (*štandardne zapnuté*) – Začiarknite toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu škodlivého softvéru: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.

- ***Hlásiť rozšírenú skupinu potenciálne nežiaducich programov*** (*štandardne vypnuté*) – Začiarknite toto políčko, ak sa má detegovať rozšírená skupina spywaru: programov, ktoré sú úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpečenia počítača, ale môže blokovať dobré programy, a preto je táto funkcia štandardne vypnutá.

- ***Kontrolovať sledovacie súbory cookies*** *(štandardne vypnuté)* – Tento parameter súčasti zapína detekciu súborov cookies (*HTTP cookies sa používajú na overenie totožnosti, sledovanie a správu konkrétnych informácií o používateľoch, akými sú napr. preferencie stránok alebo obsah elektronických nákupných košíkov*).

- ***Kontrolovať vo vnútri archívov*** (*štandardne vypnuté*) – Tento parameter určuje, že sa majú počas kontroly preverovať všetky súbory uložené vnútri archívov, napr. ZIP, RAR, ...

- ***Použiť heuristickú analýzu*** (*štandardne zapnuté*) – heuristická analýza (*dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí*) bude jednou z metód, ktoré sa použijú na detekciu vírusov počas kontroly.

- ***Kontrolovať v systémovom prostredí*** (*štandardne zapnuté*) – počas kontroly sa overujú systémové oblasti počítača.

- ***Zapnúť dôkladnú kontrolu*** (*štandardne vypnuté*) – V určitých situáciách (*podozrenie na infikovanie počítača*) môžete touto možnosťou aktivovať najdôkladnejšie kontrolné algoritmy, ktoré pre istotu skontrolujú aj tie oblasti počítača, ktoré sa obyčajne vôbec neinfikujú. Upozorňujeme však, že tento spôsob je náročný na čas.

- ***Kontrolovať rootkity*** (*štandardne zapnuté*) – Anti-Rootkit skontroluje počítač a zisťuje prítomnosť potenciálnych rootkitov, t. j. programov a technológií, ktoré dokážu zakryť činnosť škodlivého programu v počítači. Keď program deteguje rootkit, nemusí to nevyhnutne znamenať, že je počítač infikovaný. V niektorých prípadoch sa môžu určité ovládače alebo časti bežných aplikácií nesprávne označiť ako rootkity.

Mali by ste tiež určiť, čo chcete kontrolovať

- ***Všetky typy súborov*** s možnosťou definovať výnimky z prehľadávania vytvorením zoznamu čiarkou oddelených (*uložením sa čiarky zmenia na bodkočiarky*) prípon súborov, ktoré sa nemajú prehľadávať.

- ***Vybrané typy súborov*** – Môžete nastaviť, aby sa kontrolovali len súbory, pri ktorých existuje pravdepodobnosť infikovania (*(súbory, ktoré nemôžu byť napadnuté infekciou, napríklad niektoré jednoduché textové súbory alebo niektoré nespustiteľné súbory, sa nebudú kontrolovať)*, vrátane mediálnych súborov *(video, audio súborov – ak necháte toto políčko nezačiarknuté, potom sa čas prehľadávania skráti ešte viac, pretože tieto súbory sú často veľmi veľké, pričom pravdepodobnosť napadnutia vírusom je veľmi malá*). Znova môžete definovať, podľa prípony, ktoré súbory sa majú kontrolovať vždy.

- Alternatívne môžete rozhodnúť, že chcete ***kontrolovať súbory bez prípony***. Táto možnosť je štandardne zapnutá a odporúčame vám, aby ste toto nastavenie nikdy nemenili, ak na to nemáte skutočný dôvod. Súbory bez prípony sú skôr podozrivé a mali by sa vždy kontrolovať.

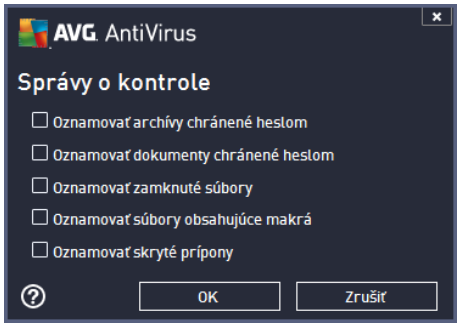
Nastaviť rýchlosť dokončenia kontroly

V časti ***Nastaviť rýchlosť dokončenia kontroly*** môžete ďalej nastaviť požadovanú rýchlosť kontroly v závislosti od využívania systémových zdrojov. Štandardne má tento parameter nastavenú úroveň automatického využívania zdrojov „*podľa používateľa*“. Ak chcete, aby prehľadávanie prebiehalo rýchlejšie, potom bude trvať kratšie, ale výrazne sa zvýši využívanie systémových zdrojov

a spomalia sa ostatné činnosti v počítači (*táto funkcia sa používa, keď je počítač zapnutý, ale nikto na ňom v danom momente nepracuje*). Na druhej strane môžete znížiť využívanie systémových zdrojov predĺžením doby trvania kontroly.

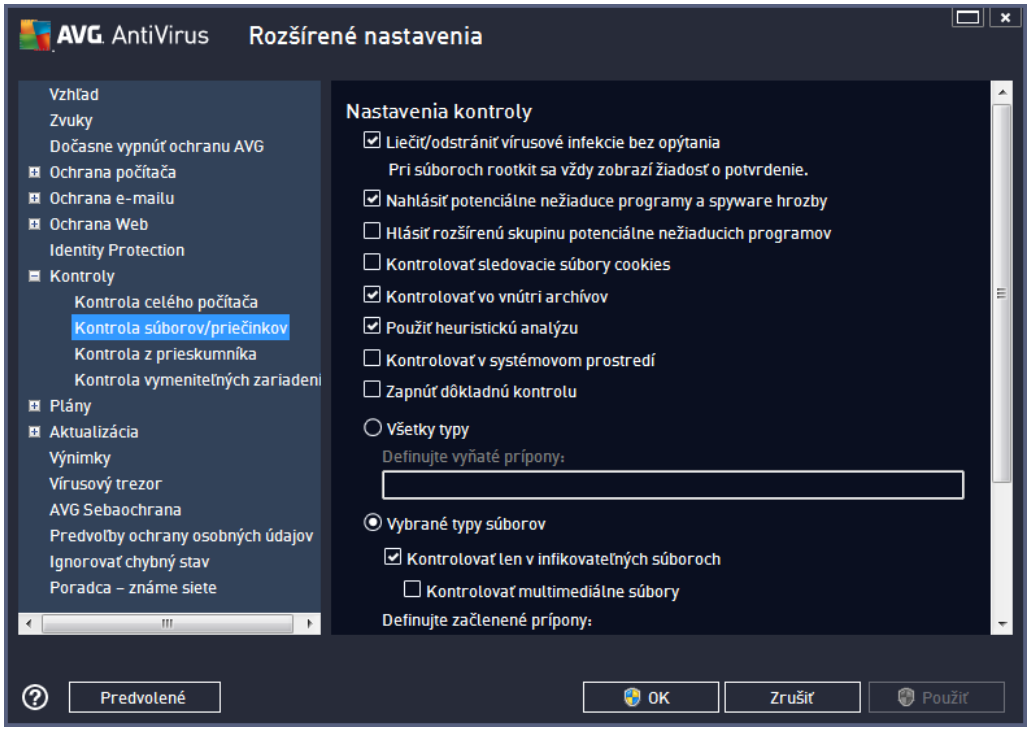
Vytvoriť ďalšie správy o kontrole...

Kliknutím na odkaz ***Vytvoriť ďalšie správy o kontrole...*** otvorte samostatné dialógové okno s názvom ***Správy o kontrole***, v ktorom môžete začiarknutím konkrétnych položiek definovať, ktoré nálezy sa majú hlásiť:



9.8.2. Kontrola súborov/priečinkov

Rozhranie editácie na ***Kontrola súborov/priečinkov*** je rovnaké ako dialógové okno editácie s názvom Kontrola celého počítača. Všetky možnosti konfigurácie sú rovnaké, predvolené nastavenia sú však prísnejšie pri Kontrola celého počítača:



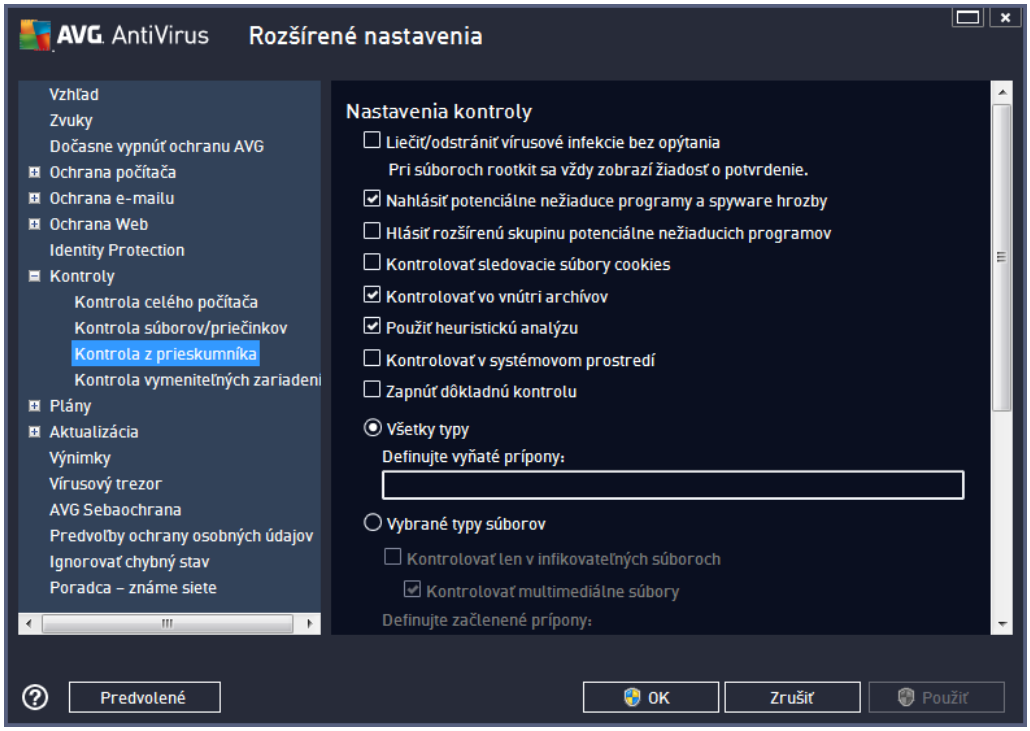
Všetky parametre nastavené v tomto dialógovom okne konfigurácie sa vzťahujú len na oblasti

vybrané na kontrolu v dialógovom okne Kontrola súborov/priečinkov!

Poznámka: *Informácie o konkrétnych parametroch sa nachádzajú v kapitole Rozšírené nastavenia AVG/Kontroly/Kontrola celého počítača.*

9.8.3. Kontrola z prieskumníka

Rovnako ako predchádzajúca funkcia Kontrola celého počítača, aj táto funkcia s názvom ***Kontrola z prieskumníka*** ponúka niekoľko možností na úpravu kontroly vopred definovanej dodávateľom softvéru. V tomto prípade súvisí konfigurácia s kontrolou konkrétnych objektov spustených v prostredí programu Windows Explorer (*prieskumník*), pozri kapitolu Kontrola z prieskumníka:



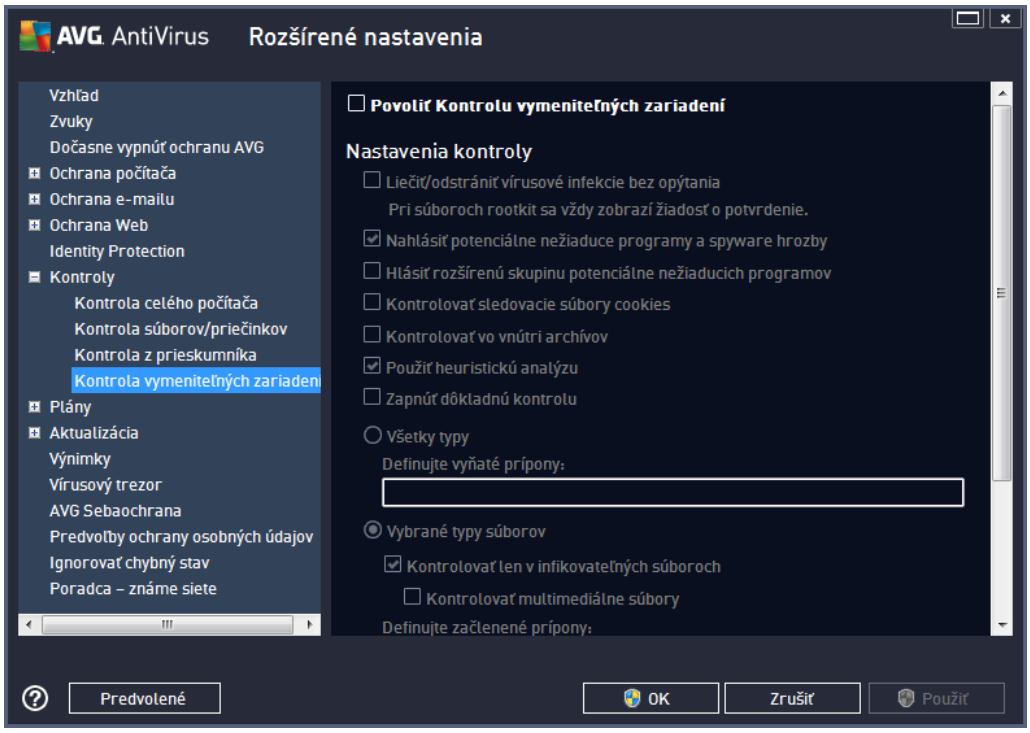
Zoznam parametrov je identický s parametrami použiteľnými pre kontrolu celého počítača. Predvolené nastavenia sa však líšia (*napríklad Kontrola celého počítača štandardne nekontroluje archívy, ale kontroluje systémové prostredie, zatiaľ čo Kontrola z prieskumníka má presne opačné nastavenia*).

Poznámka: *Informácie o konkrétnych parametroch sa nachádzajú v kapitole Rozšírené nastavenia AVG/Kontroly/Kontrola celého počítača.*

V porovnaní s dialógovým oknom Kontrola celého počítača sa v dialógovom okne ***Kontrola z prieskumníka*** nachádza aj časť s názvom ***Ďalšie nastavenia súvisiace s používateľským rozhraním AVG***, ktorá umožňuje nastaviť, či majú byť výsledky a priebeh kontroly prístupné v používateľskom rozhraní AVG. Zároveň umožňuje nastaviť, aby sa výsledky kontroly zobrazili len v prípade, keď sa počas kontrolovania deteguje infekcia.

9.8.4. Kontrola vymeniteľných zariadení

Rozhranie editácie ***Kontrola vymeniteľných zariadení*** sa veľmi podobá dialógovému oknu editácie Kontrola celého počítača:



Kontrola vymeniteľných zariadení sa spustí automaticky po pripojení vymeniteľného zariadenia k počítaču. Táto kontrola je štandardne vypnutá. Kontrola vymeniteľných zariadení je však veľmi dôležitá z hľadiska potenciálnych hrozieb, pretože tieto predstavujú zdroj infekcie. Ak chcete, aby táto kontrola bola pripravená a spustila sa automaticky v prípade potreby, označte možnosť ***Povoliť kontrolu vymeniteľných zariadení***.

Poznámka: *Informácie o konkrétnych parametroch sa nachádzajú v kapitole Rozšírené nastavenia AVG/Kontroly/Kontrola celého počítača.*

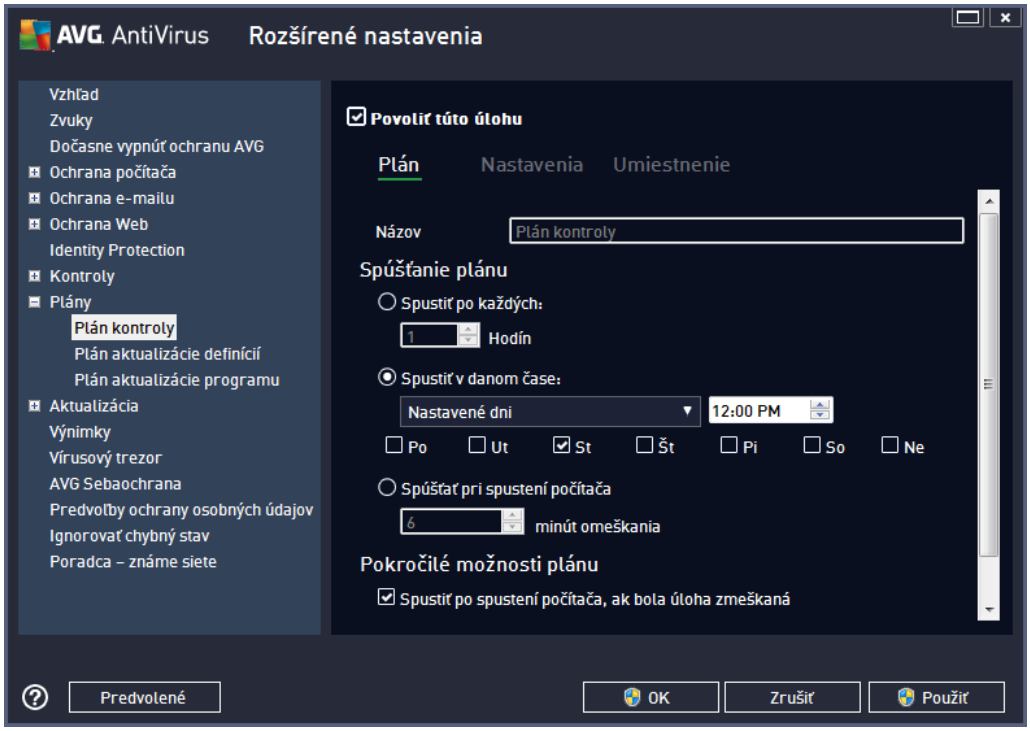
9.9. Plány

V časti ***Plány*** môžete upraviť predvolené nastavenia pre:

- Plán kontroly
- Plán aktualizácie definícií
- Plán aktualizácie programu

9.9.1. Plán kontroly

Parametre plánu kontroly sa dajú upraviť (*alebo sa dá nastaviť nový plán*) v troch kartách. Na každej karte najskôr začiarknutím, resp. zrušením začiarknutia položky ***Povoliť túto úlohu*** dočasne vypnite naplánovaný test a znova ho zapnite, keď je potrebný:



Vo vedľajšom textovom poli ***Názov*** (*neaktívne pre všetky predvolené plány*) sa nachádza názov, ktorý tomuto konkrétnemu plánu pridelil dodávateľ programu. Pre novopridané plány (*nový plán sa pridá kliknutím pravým tlačidlom myši nad položkou* ***Plán kontroly*** *v ľavej navigačnej štruktúre*) môžete definovať vlastný názov a v tom prípade bude textové pole editovateľné a budete môcť zmeniť jeho obsah. Pokúste sa použiť stručné, opisné a výstižné názvy pre kontroly, aby sa dali neskôr ľahšie navzájom odlíšiť.

Príklad: *Nie je vhodné nazvať kontrolu „Nová kontrola“ alebo „Moja kontrola“, pretože tieto názvy nesúvisia s tým, čo kontrola vlastne preveruje. Na druhej strane, príkladom dobrého opisného názvu je „Kontrola systémových oblastí“ a pod. Takisto nie je potrebné zadať do názvu kontroly, či ide o kontrolu celého počítača alebo vybraných súborov alebo priečinkov, pretože vaše vlastné kontroly budú vždy predstavovať špeciálnu verziu kontroly vybraných súborov alebo priečinkov.*

Toto dialógové okno umožňuje ďalej definovať tieto parametre kontroly:

Spúšťanie naplánovaných úloh

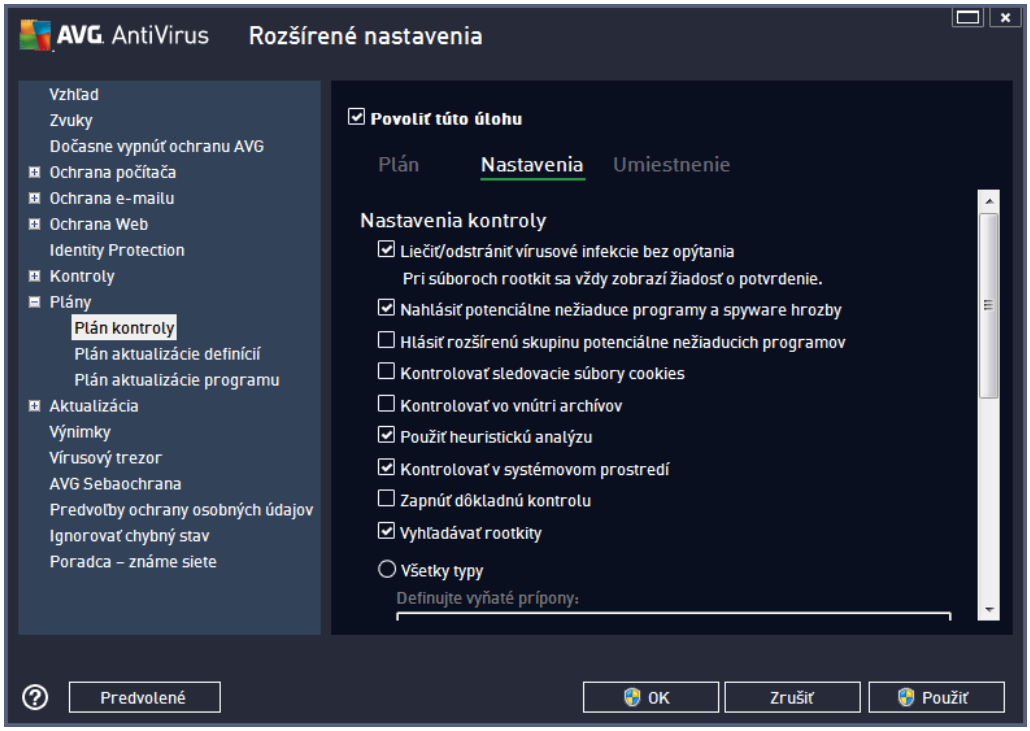
Tu môžete nastaviť časové intervaly pre novonaplánované spustenie kontroly. Čas spúšťania sa definuje ako opakované spúšťanie kontroly po uplynutí určitého času (***Spustiť po každých ...***), definovaním presného dátumu a času (***Spúšťať v konkrétnom časovom intervale ...***), prípadne definovaním udalosti, s ktorou sa bude spájať spustenie kontroly (***Spustiť pri spustení počítača***).

Rozšírené možnosti plánu

Táto časť sa používa na definovanie podmienok, pri ktorých sa má resp. nemá spustiť kontrola, keď

je počítač v úspornom režime alebo úplne vypnutý. Keď sa spustí naplánovaná kontrola v nastavenom čase, bude vás o tom informovať automaticky otvárané okno, ktoré sa otvorí nad ikonou AVG v paneli úloh.

Potom sa zobrazí nová ikona AVG v paneli úloh (*farebná s blikajúcim svetlom*), ktorá informuje o tom, že prebieha naplánovaná kontrola. Kliknutím pravým tlačidlom myši na ikonu AVG prebiehajúcej kontroly otvorte kontextovú ponuku, ktorá vám umožní pozastaviť alebo dokonca úplne zastaviť prebiehajúcu kontrolu a zároveň zmeniť prioritu práve spustenej kontroly.



V karte ***Nastavenia*** nájdete zoznam parametrov kontrolovania, ktoré sa dajú voliteľne zapnúť/vypnúť. Štandardne je väčšina parametrov zapnutá a príslušná funkcia sa použije počas kontroly. ***Ak nemáte závažný dôvod meniť tieto nastavenia, odporúčame vám ponechať vopred definovanú konfiguráciu***:

- ***Liečiť/odstrániť vírusovú infekciu bez opýtania*** *(štandardne zapnuté):* ak sa počas kontroly nájde vírus, môže byť automaticky vyliečený, pokiaľ je liek k dispozícii. Ak nie je možné infikovaný súbor vyliečiť automaticky, premiestni sa do Vírusového trezora.

- ***Nahlásiť potenciálne nežiaduce programy a spyware hrozby*** *(štandardne zapnuté):* Začiarknite toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu škodlivého softvéru: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.

- ***Hlásiť rozšírenú skupinu potenciálne nežiaducich programov*** (*štandardne vypnuté*): Začiarknite toto políčko, ak sa má detegovať rozšírená skupina spywaru: programov, ktoré sú úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu, ale neskôr sa dajú

zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpečenia počítača, ale môže blokovať dobré programy, a preto je táto funkcia štandardne vypnutá.

- ***Kontrolovať sledovacie súbory cookies*** (*štandardne vypnuté*): Tento parameter súčasti zapína funkciu na detekciu súborov cookies počas prehľadávania; (*HTTP cookies sa používajú na overenie totožnosti, sledovanie a správu konkrétnych informácií o používateľoch, akými sú napr. preferencie stránok alebo obsah elektronických nákupných košíkov*).

- ***Kontrolovať vo vnútri archívov*** (*štandardne vypnuté*): tento parameter určuje, že sa majú počas kontroly preverovať všetky súbory, aj keď sú uložené vo vnútri archívu, napr. ZIP, RAR, ...

- ***Použiť heuristickú analýzu*** (*štandardne zapnuté*): heuristická analýza (*dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí*) bude jedna z metód, ktoré sa použijú na detekciu vírusov počas kontroly.

- ***Kontrolovať v systémovom prostredí*** (*štandardne zapnuté*): počas kontroly sa budú overovať aj systémové oblasti počítača.

- ***Zapnúť dôkladnú kontrolu*** (*štandardne vypnuté):* v určitých situáciách (*podozrenie na infikovanie počítača*) môžete touto možnosťou aktivovať najdôkladnejšie kontrolné algoritmy, ktoré pre istotu skontrolujú aj tie oblasti počítača, ktoré sa obyčajne vôbec neinfikujú. Upozorňujeme však, že tento spôsob je náročný na čas.

- ***Kontrolovať rootkity*** *(štandardne zapnuté):* Kontrola súčasťou Anti-Rootkit skontroluje počítač a zisťuje prítomnosť potenciálnych rootkitov, t. j. programov a technológií, ktoré dokážu zakryť činnosť škodlivého programu v počítači. Keď program deteguje rootkit, nemusí to nevyhnutne znamenať, že je počítač infikovaný. V niektorých prípadoch sa môžu určité ovládače alebo časti bežných aplikácií nesprávne označiť ako rootkity.

Mali by ste tiež určiť, čo chcete kontrolovať

- ***Všetky typy súborov*** s možnosťou definovať výnimky z prehľadávania vytvorením zoznamu čiarkou oddelených (*uložením sa čiarky zmenia na bodkočiarky*) prípon súborov, ktoré sa nemajú prehľadávať.

- ***Vybrané typy súborov*** – Môžete nastaviť, aby sa kontrolovali len súbory, pri ktorých existuje pravdepodobnosť infikovania (*(súbory, ktoré nemôžu byť napadnuté infekciou, napríklad niektoré jednoduché textové súbory alebo niektoré nespustiteľné súbory, sa nebudú kontrolovať)*, vrátane mediálnych súborov *(video, audio súborov – ak necháte toto políčko nezačiarknuté, potom sa čas prehľadávania skráti ešte viac, pretože tieto súbory sú často veľmi veľké, pričom pravdepodobnosť napadnutia vírusom je veľmi malá)*. Znova môžete definovať, podľa prípony, ktoré súbory sa majú kontrolovať vždy.

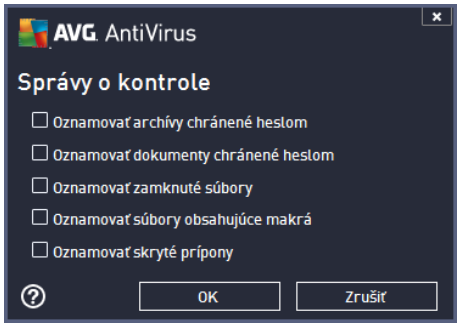
- Alternatívne môžete rozhodnúť, že chcete ***kontrolovať súbory bez prípony***. Táto možnosť je štandardne zapnutá a odporúčame vám, aby ste toto nastavenie nikdy nemenili, ak na to nemáte skutočný dôvod. Súbory bez prípony sú skôr podozrivé a mali by sa vždy kontrolovať.

Nastaviť rýchlosť dokončenia kontroly

V tejto časti môžete ďalej špecifikovať želanú rýchlosť kontroly v závislosti od využívania systémových zdrojov. V predvolenom nastavení je úroveň automatického využívania zdrojov nastavená *Podľa používateľa*. Ak chcete, aby kontrola prebiehala rýchlejšie, potom bude trvať kratšie, ale výrazne sa zvýši využívanie systémových zdrojov a spomalia sa ostatné činnosti v počítači (*táto funkcia sa používa, keď je počítač zapnutý, ale nikto na ňom v danom momente nepracuje*). Na druhej strane môžete znížiť využívanie systémových zdrojov predĺžením doby trvania kontroly.

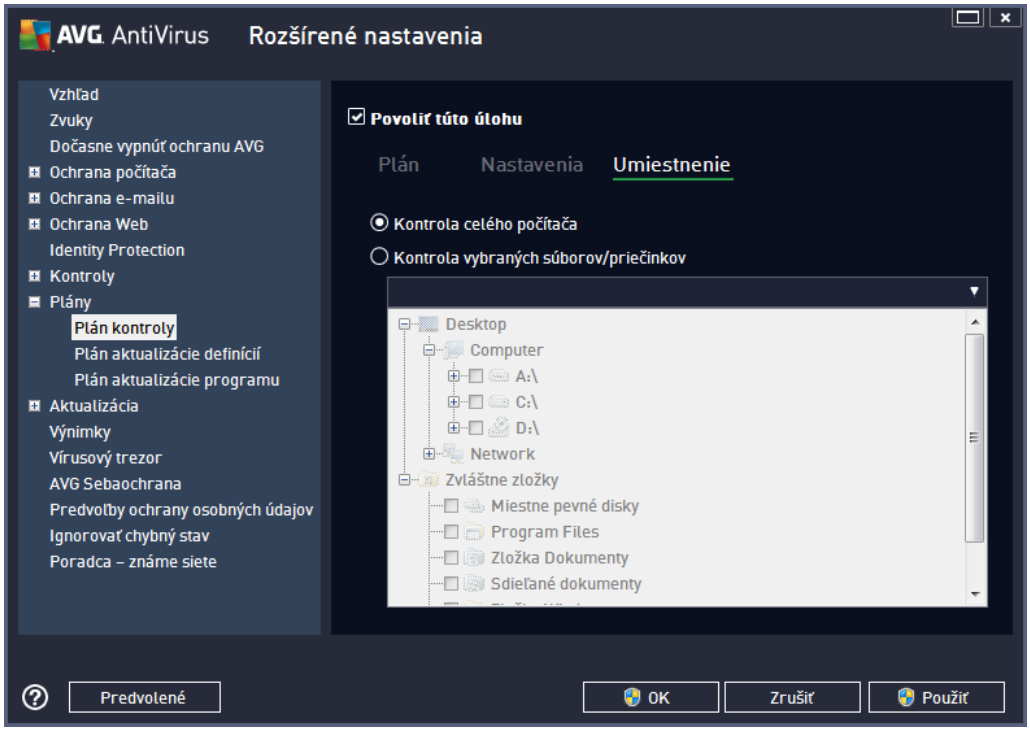
Vytvoriť ďalšie správy o kontrole

Kliknutím na odkaz ***Vytvoriť ďalšie správy o kontrole...*** otvorte samostatné dialógové okno s názvom ***Správy o kontrole***, v ktorom môžete začiarknutím konkrétnych položiek definovať, ktoré nálezy sa majú hlásiť:



Možnosti vypnutia počítača

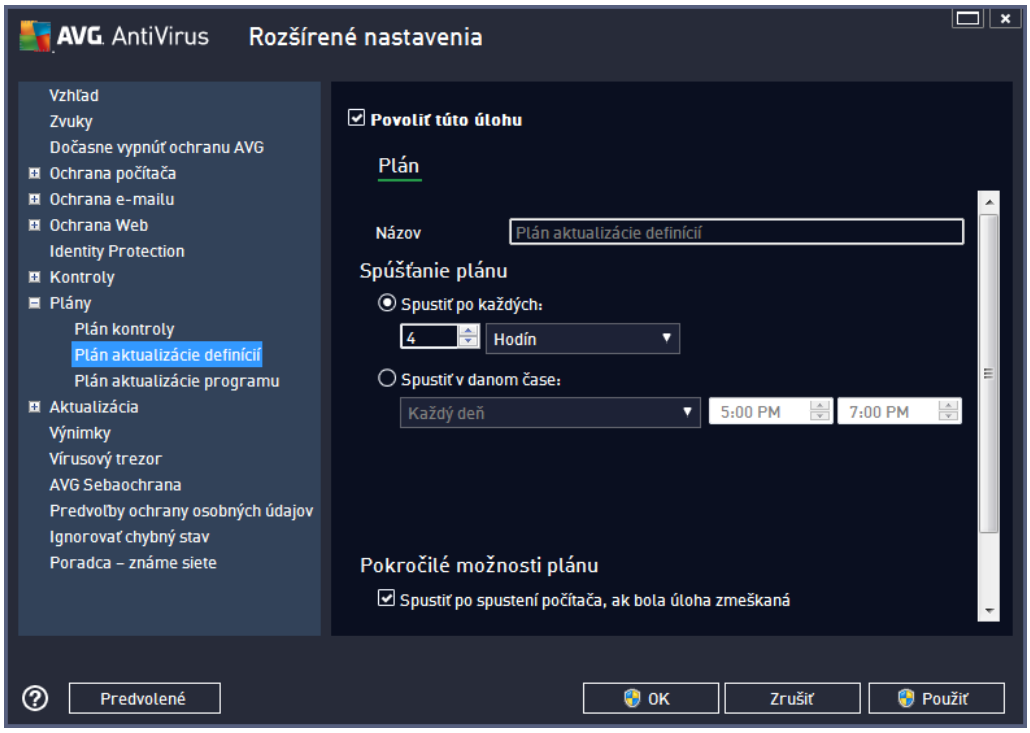
V časti ***Možnosti vypnutia počítača***môžete rozhodnúť, či sa má počítač vypnúť automaticky po dokončení procesu kontroly. Po potvrdení tejto možnosti (***Vypnúť počítač po dokončení kontroly***) sa aktivuje nová možnosť, ktorá umožní vypnúť počítač, aj keď je momentálne zablokovaný (***Vynútené vypnutie, ak je počítač zablokovaný***).



Na karte ***Umiestnenie*** môžete nastaviť, či chcete naplánovať kontrolu celého počítača alebo kontrolu súborov/priečinkov. V prípade, že zvolíte kontrolu súborov/priečinkov, v spodnej časti tohto dialógového okna sa aktivuje zobrazená stromová štruktúra a môžete určiť priečinky, ktoré sa majú kontrolovať.

9.9.2. Plán aktualizácie definícií

Ak je to ***naozaj potrebné***, zrušením začiarknutia políčka ***Povoliť túto úlohu*** môžete dočasne vypnúť naplánovanú aktualizáciu a neskôr ju znova zapnúť:



Toto dialógové okno sa používa na nastavenie niektorých podrobných parametrov plánu aktualizácie. V textovom poli ***Názov*** (*neaktívne pre všetky predvolené plány*) sa nachádza názov, ktorý tomuto konkrétnemu plánu pridelil dodávateľ programu.

Spúšťanie naplánovaných úloh

V tejto časti nastavte časové intervaly pre spúšťanie nových naplánovaných definícií aktualizácie. Časovanie sa definuje ako opakované spúšťanie aktualizácie po uplynutí určitého času (***Spustiť po každých...***) alebo nastavením presného dátumu a času (***Spúšťať v konkrétnom čase...***).

Rozšírené možnosti plánu

Táto časť sa používa na definovanie podmienok, za akých sa má/nemá spustiť aktualizácia programu, ak je počítač v úspornom režime alebo úplne vypnutý.

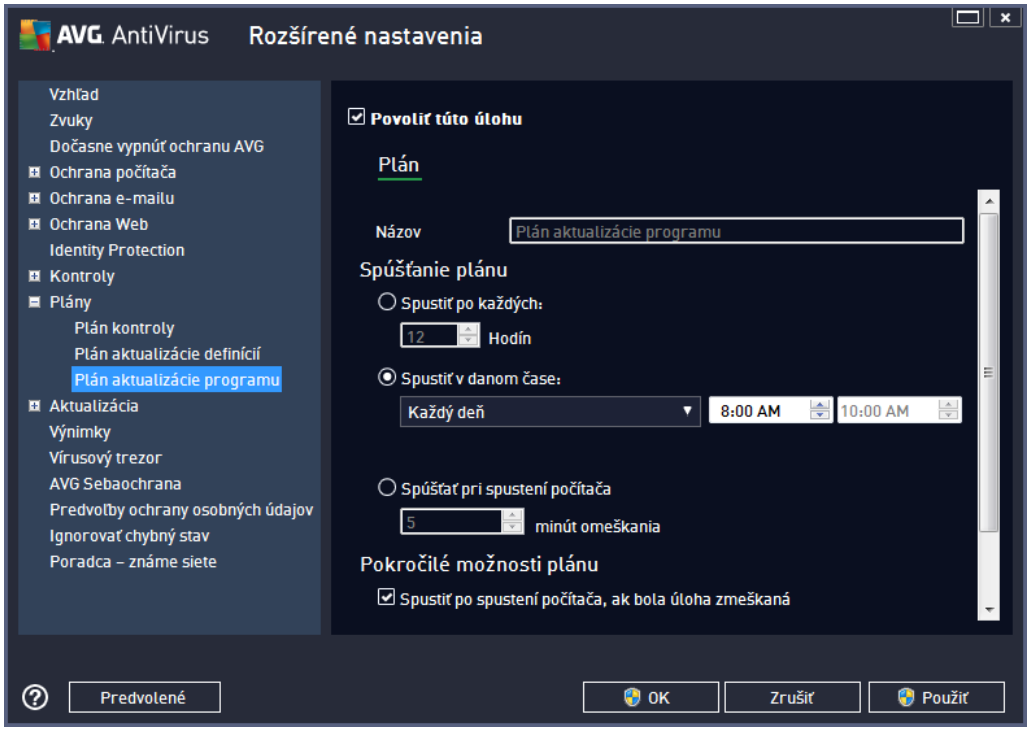
Ďalšie nastavenia aktualizácie

Nakoniec označte možnosť ***Spustiť aktualizáciu znova hneď po obnovení internetového pripojenia***, ak sa má v prípade výpadku internetového pripojenia a neúspechu procesu aktualizácie ihneď po obnovení pripojenia okamžite spustiť. Po spustení naplánovanej aktualizácie vo vami nastavenom čase sa zobrazí informácia o tejto skutočnosti v automaticky otváranom okne nad

ikonou AVG v paneli úloh (*pod podmienkou, že sa nezmenila predvolená konfigurácia v dialógom okne Rozšírené nastavenia/Vzhľad*).

9.9.3. Plán aktualizácie programu

Ak je to ***naozaj potrebné***, zrušením začiarknutia políčka ***Povoliť túto úlohu*** môžete dočasne vypnúť naplánovanú aktualizáciu programu a neskôr ju znova zapnúť:



V textovom poli ***Názov*** (*neaktívne pre všetky predvolené plány*) sa nachádza názov, ktorý tomuto konkrétnemu plánu pridelil dodávateľ programu.

Spúšťanie naplánovaných úloh

Tu zadajte časové intervaly pre spustenie novonaplánovanej aktualizácie programu. Načasovanie sa definuje ako opakované spúšťanie aktualizácie po uplynutí určitého času (***Spustiť po každých...***), definovaním presného dátumu a času (***Spúšťať v konkrétnom čase...***), prípadne definovaním udalosti, s ktorou sa bude spájať spustenie aktualizácie (***Činnosť pri spustení počítača***).

Rozšírené možnosti plánu

Táto časť sa používa na definovanie podmienok, za akých sa má/nemá spustiť aktualizácia programu, ak je počítač v úspornom režime alebo úplne vypnutý.

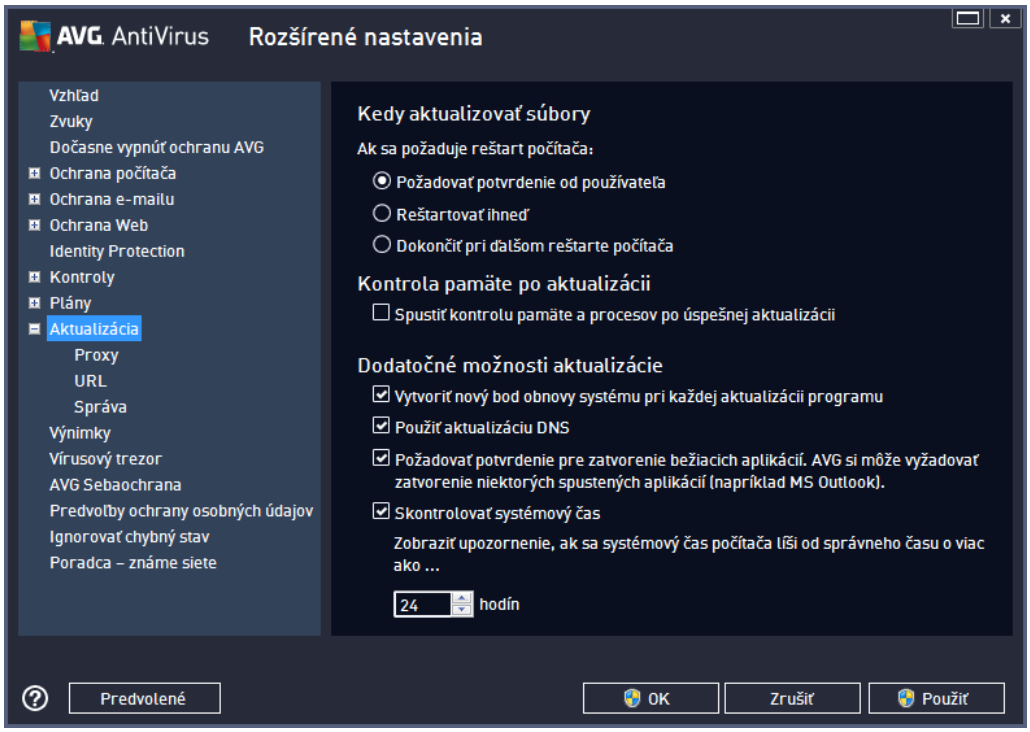
Ďalšie nastavenia aktualizácie

Označte možnosť ***Znova spustiť aktualizáciu ihneď po obnovení internetového pripojenia***, ak sa má v prípade výpadku internetového pripojenia a neúspechu procesu aktualizácie ihneď po obnovení pripojenia okamžite spustiť. Po spustení naplánovanej aktualizácie vo vami nastavenom čase sa zobrazí informácia o tejto skutočnosti v automaticky otváranom okne nad ikonou AVG v paneli úloh (*pod podmienkou, že sa nezmenila predvolená konfigurácia v dialógom okne Rozšírené nastavenia/Vzhľad*).

Poznámka: *Ak sa čas naplánovanej aktualizácie programu náhodou prekrýva s plánom kontroly, aktualizácia má vyššiu prioritu a kontrola sa preruší.*

9.10. Aktualizácia

Položka ***Aktualizácia*** v navigačnej štruktúre otvorí nové dialógové okno, ktoré umožňuje nastaviť všeobecné parametre súvisiace s aktualizáciou produktu AVG:



Kedy aktualizovať súbory

V tejto časti môžete vybrať jednu z troch možností, ktorá bude použitá v prípade, ak si proces aktualizácie vyžiada reštartovanie počítača. Dokončenie aktualizácie môžete naplánovať na ďalšie reštartovanie počítača alebo môžete ihneď reštartovať počítač:

- ***Požadovať potvrdenie od používateľa*** *(predvolené)* – zobrazí sa žiadosť, aby ste potvrdili reštartovanie počítača, ktoré je potrebné na dokončenie aktualizácie
- ***Reštartovať ihneď*** – Počítač sa automaticky reštartuje ihneď po dokončení aktualizácie a nepožiada vás o udelenie súhlasu.
- ***Dokončiť pri ďalšom reštarte počítača*** – Dokončenie aktualizácie bude odložené na

ďalšie reštartovanie počítača. Odporúčame vám, aby ste túto možnosť zapli len v prípade, ak sa počítač reštartuje pravidelne, najmenej raz za deň!

Kontrola pamäte po aktualizácii

Označte toto začiarkavacie políčko, ak sa má nová kontrola pamäte spustiť po každej úspešnej aktualizácii. Najnovšia prevzatá aktualizácia môže obsahovať nové definície vírusov, ktoré sa môžu ihneď použiť pri kontrole.

Ďalšie možnosti aktualizácie

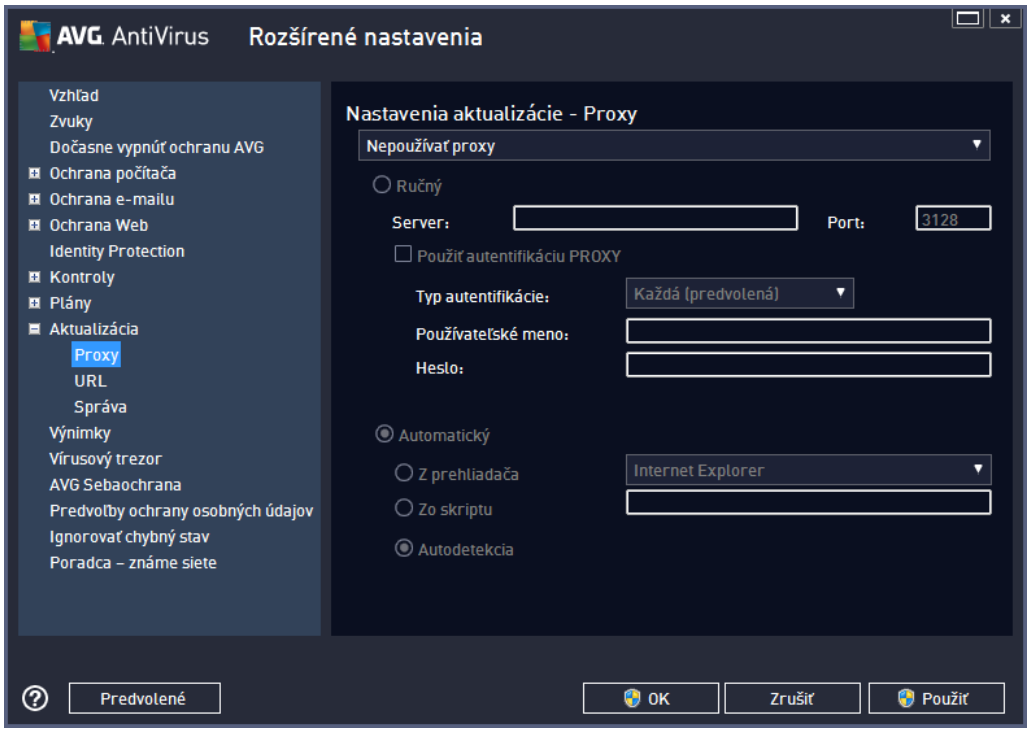
- ***Vytvoriť nový bod obnovenia systému počas každej aktualizácie programu*** – pred každým spustením aktualizácie programu AVG sa vytvorí bod obnovenia systému. Ak proces aktualizácie zlyhá a operačný systém spadne, potom vám tento bod obnovenia umožní obnoviť stav operačného systému s pôvodnou konfiguráciou. Prístup k tejto možnosti je cez ponuku Štart/Všetky programy/Príslušenstvo/Systémové nástroje/ Obnovenie systému, ale vykonať zmeny týchto nastavení sa odporúča len skúseným používateľom! Nechajte toto začiarkavacie políčko označené, ak chcete používať túto funkcionalitu.

- ***Použiť aktualizáciu DNS*** (*štandardne zapnuté*) – Ak je toto začiarkavacie políčko označené, po spustení aktualizácie program **AVG AntiVirus 2013** vyhľadá informácie o najnovšej verzii vírusovej databázy a najnovšej verzii programu na serveri DNS. Až potom sa prevezmú a nainštalujú najmenšie nevyhnutne potrebné aktualizačné súbory. Týmto spôsobom sa minimalizuje celkový objem prevzatých dát a zrýchli proces aktualizácie.

- ***Funkcia Požadovať súhlas so zatvorením spustených aplikácií*** (*štandardne zapnuté*) – Postará sa o to, aby sa žiadna spustená aplikácia nezatvorila bez vášho súhlasu, ak to je potrebné na dokončenie procesu aktualizácie.

- ***Skontrolovať systémový čas*** – Začiarknite toto políčko, ak chcete byť informovaní v prípade, keď sa systémový čas líši od skutočného času o viac, ako je nastavený počet hodín.

9.10.1. Proxy



Server proxy je samostatný server alebo služba spustená na počítači, ktorá zaručuje bezpečnejšie pripojenie do internetu. Podľa definovaných pravidiel siete potom môžete pristupovať na internet buď priamo alebo cez server proxy, pričom súčasne môžete použiť aj obidve možnosti. Potom v prvej položke dialógového okna ***Nastavenia aktualizácie – Proxy*** musíte nastaviť v ponuke, či chcete:

- ***Nepoužívať proxy*** – predvolené nastavenie
- ***Použiť proxy***
- ***Pokúsiť sa pripojiť pomocou servera proxy a ak sa to nepodarí, pripojiť priamo***

Ak si zvolíte niektorú možnosť pomocou proxy servera, budete musieť zadať ďalšie údaje. Nastavenia servera sa nastavujú buď ručne alebo automaticky.

Ručná konfigurácia

Ak sa rozhodnete pre ručnú konfiguráciu (začiarknite možnosť ***Ručná*** *na aktivovanie príslušnej časti dialógového okna*), musíte nastaviť nasledujúce parametre:

- ***Server***: Zadajte adresu IP servera alebo názov servera.
- ***Port***: Zadajte číslo portu, ktorý umožňuje prístup na internet (*štandardne je toto číslo nastavené na hodnotu 3128, ale môžete nastaviť inú hodnotu; ak máte pochybnosti, kontaktujte správcu siete*).

Proxy server môže mať tiež nakonfigurované špecifické pravidlá pre každého používateľa. Ak je

server proxy nastavený týmto spôsobom, začiarknite možnosť ***Použiť autentifikáciu PROXY*** na overenie, či sú vaše používateľské meno a heslo platné na vytvorenie pripojenia na internet cez server proxy.

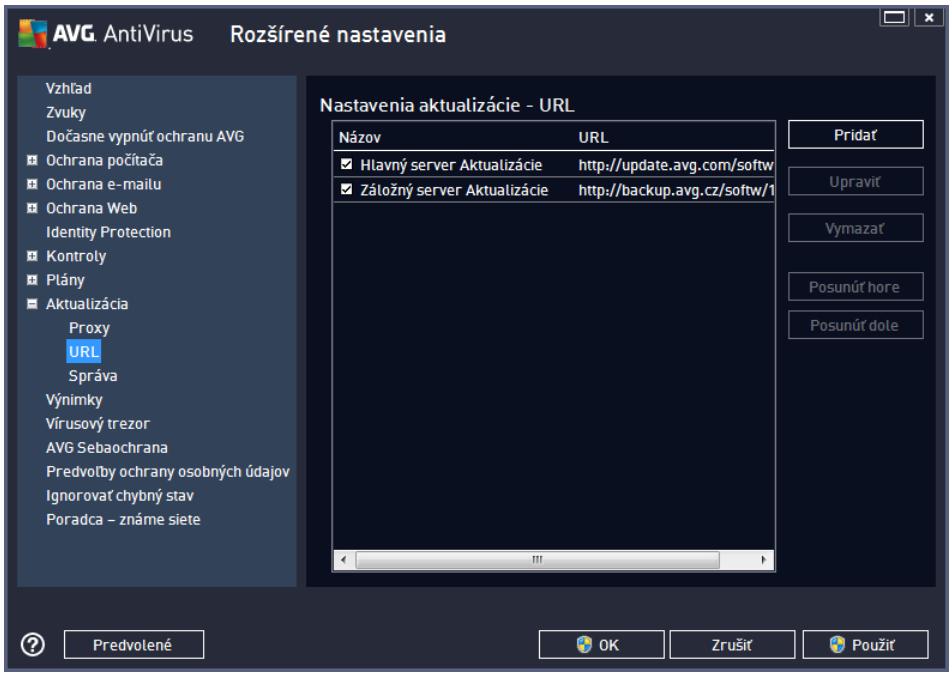
Automatická konfigurácia

Ak sa rozhodnete pre automatickú konfiguráciu (*začiarknite možnosť **Automatická** na aktivovanie príslušnej časti dialógového okna*), nastavte, odkiaľ sa má prevziať konfigurácia servera proxy:

- ***Z prehliadača*** – Konfigurácia sa načíta z predvoleného internetového prehliadača.
- ***Zo skriptu***: Konfigurácia sa načíta z prevzatého skriptu pomocou funkcie, ktorá vráti adresu servera proxy.
- ***Automatické zistenie***: Konfigurácia sa zistí automaticky priamo zo servera proxy.

9.10.2. Adresa URL

Dialógové okno ***URL*** uvádza zoznam internetových adries, z ktorých môžete prevziať aktualizačné súbory:



Ovládacie tlačidlá

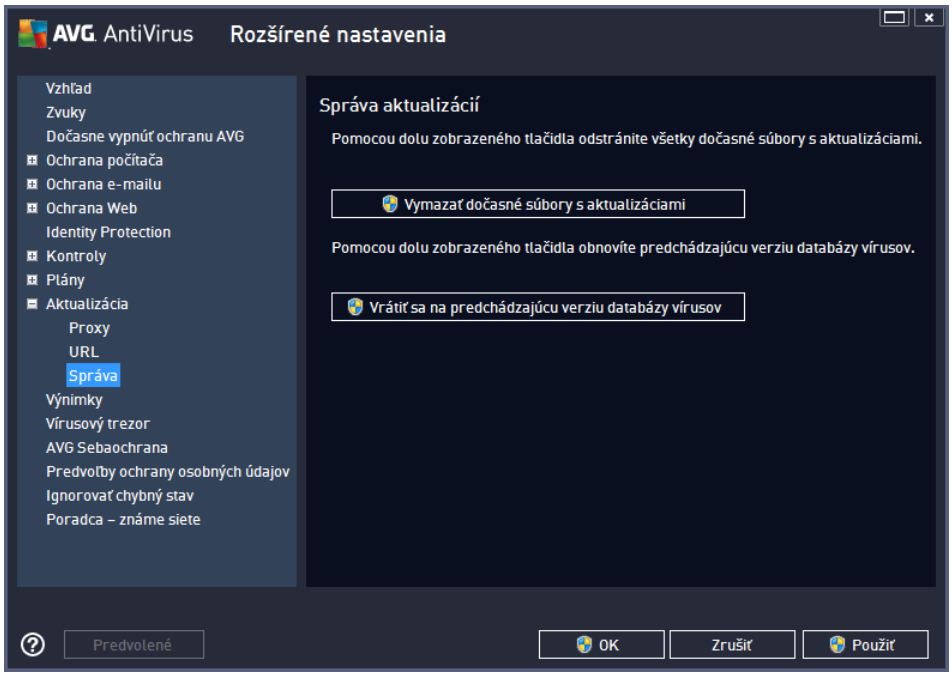
Zoznam a jeho položky môžete zmeniť pomocou nasledujúcich ovládacích tlačidiel:

- ***Pridať*** – otvorí sa dialógové okno, kde môžete zadať novú URL adresu, ktorú chcete pridať do zoznamu
- ***Upraviť*** – otvorí sa dialógové okno, kde môžete upraviť parametre zvolenej URL adresy

- ***Vymazať*** – vymaže sa zvolená URL adresa zo zoznamu
- ***Posunúť hore*** – posunie zvolenú URL adresu o jednu pozíciu v zozname hore
- ***Posunúť dole*** – posunie zvolenú URL adresu o jednu pozíciu v zozname dole

9.10.3. Správa

Dialógové okno ***Správa aktualizácií*** ponúka dve možnosti, ktoré sa sprístupnia pomocou dvoch tlačidiel:

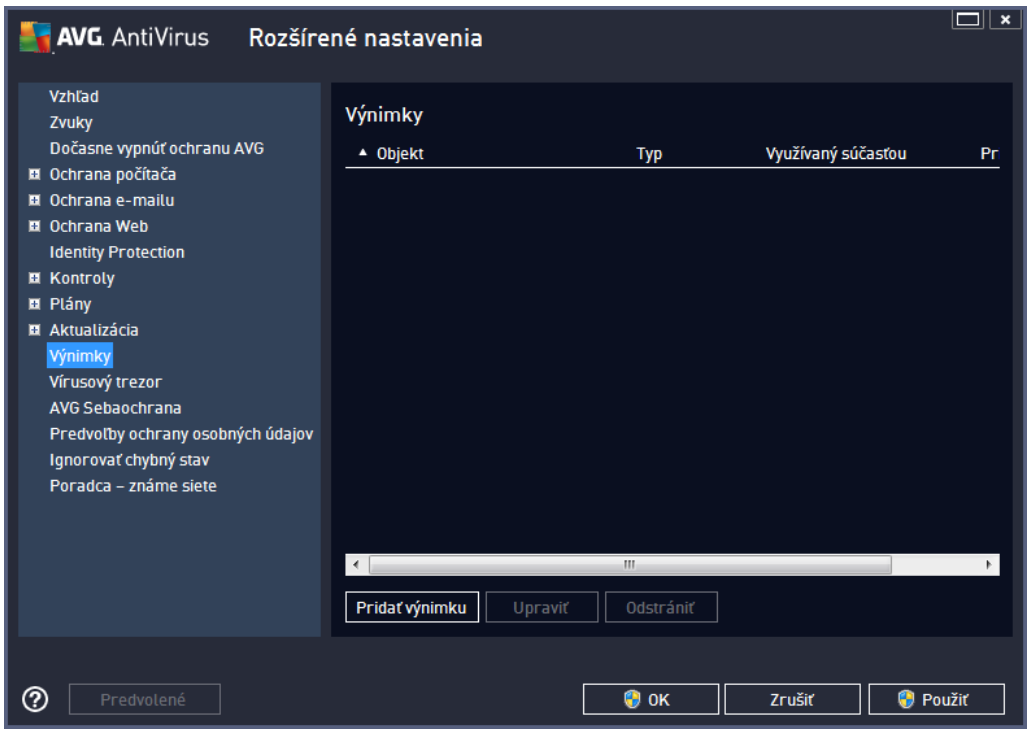


- ***Vymazať dočasné súbory s aktualizáciami*** – Stlačením tohto tlačidla sa vymažú všetky nepotrebné súbory aktualizácie z pevného disku (*v predvolenom nastavení zostanú tieto súbory uložené 30 dní*).
- ***Vrátiť sa na predchádzajúcu verziu databázy vírusov*** – Stlačením tohto tlačidla sa vymaže najnovšia verzia databázy vírusov z pevného disku a obnoví sa predchádzajúca uložená verzia (*nová verzia databázy vírusov bude tvoriť súčasť nasledujúcej aktualizácie*).

9.11. Výnimky

V dialógovom okne ***Výnimky*** môžete definovať výnimky, čiže položky, ktoré program **AVG AntiVirus 2013** bude ignorovať. Obvykle budete musieť výnimku definovať, ak program AVG neustále deteguje program alebo súbor ako hrozbu alebo blokuje bezpečnú stránku ako nebezpečnú. Pridajte takýto súbor alebo stránku do tohto zoznamu výnimiek a program AVG ho už nebude označovať ani blokovať.

Vždy sa uistite, že daný súbor, program alebo stránka sú úplne bezpečné!



Hlavná časť stránky zobrazuje zoznam výnimiek, ak už boli nejaké definované. Vedľa každej položky sa nachádza začiarkavacie políčko. Keď je začiarkavacie políčko označené, potom sa výnimka používa; keď nie je, potom je výnimka len definovaná, ale momentálne sa nepoužíva. Kliknite na hlavičku stĺpca, aby sa položky zoradili podľa príslušného kritéria.

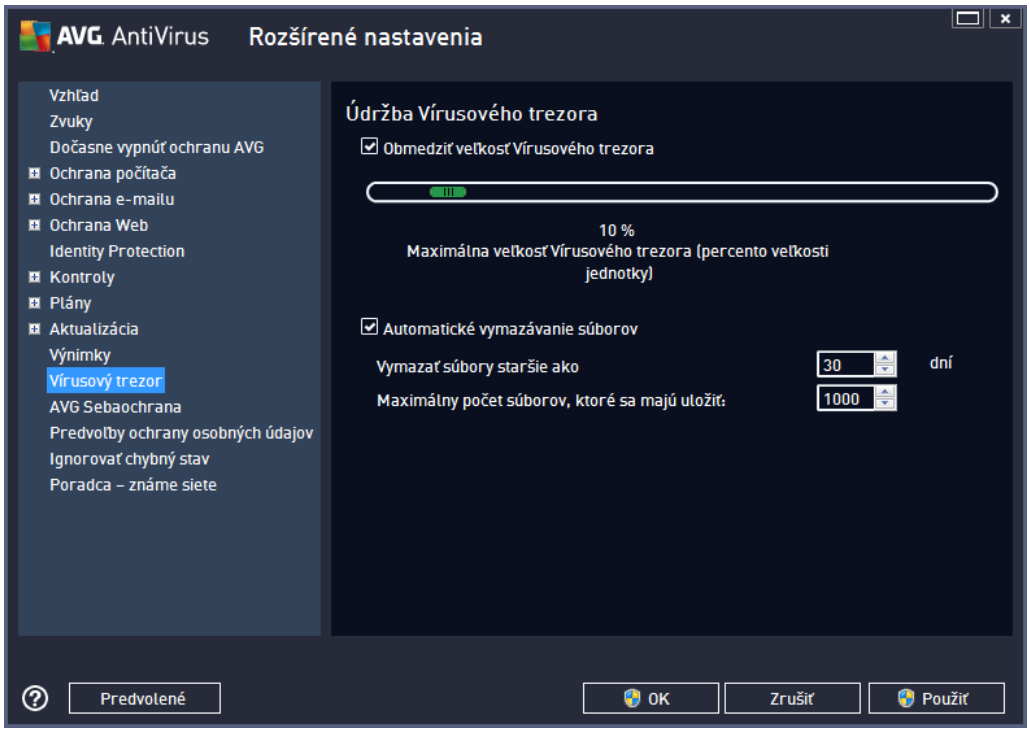
Ovládacie tlačidlá

- ***Pridať výnimku*** – Kliknutím otvoríte nové dialógové okno, kde môžete zadať položku, ktorá sa má vylúčiť z kontroly programu AVG. Najprv budete vyzvaní na zadanie typu objektu, t. j. či ide o súbor, priečinok alebo adresu URL. Potom na disku nájdite cestu k príslušnému objektu alebo napíšte URL. Nakoniec môžete zvoliť, ktoré funkcie AVG by mali vybraný objekt ignorovať *(Rezidentný štít, Identita, Kontrola, Anti-Rootkit)*.

- ***Upraviť*** – Toto tlačidlo je aktívne iba vtedy, ak už sú definované nejaké výnimky. Tie sú uvedené v tabuľke. Potom môžete týmto tlačidlom otvoriť dialógové okno úpravy vybranej výnimky a nastaviť jej parametre.

- ***Odstrániť*** – Týmto tlačidlom zrušíte zadefinovanú výnimku. Výnimky môžete odstrániť buď po jednej, alebo zvýrazniť niekoľko výnimiek v zozname a zrušiť ich naraz. Po zrušení výnimky bude program AVG príslušný súbor, priečinok či adresu URL opäť kontrolovať. Upozorňujeme, že bude odstránená len výnimka, nie súbor alebo priečinok samotný!

9.12. Vírusový trezor

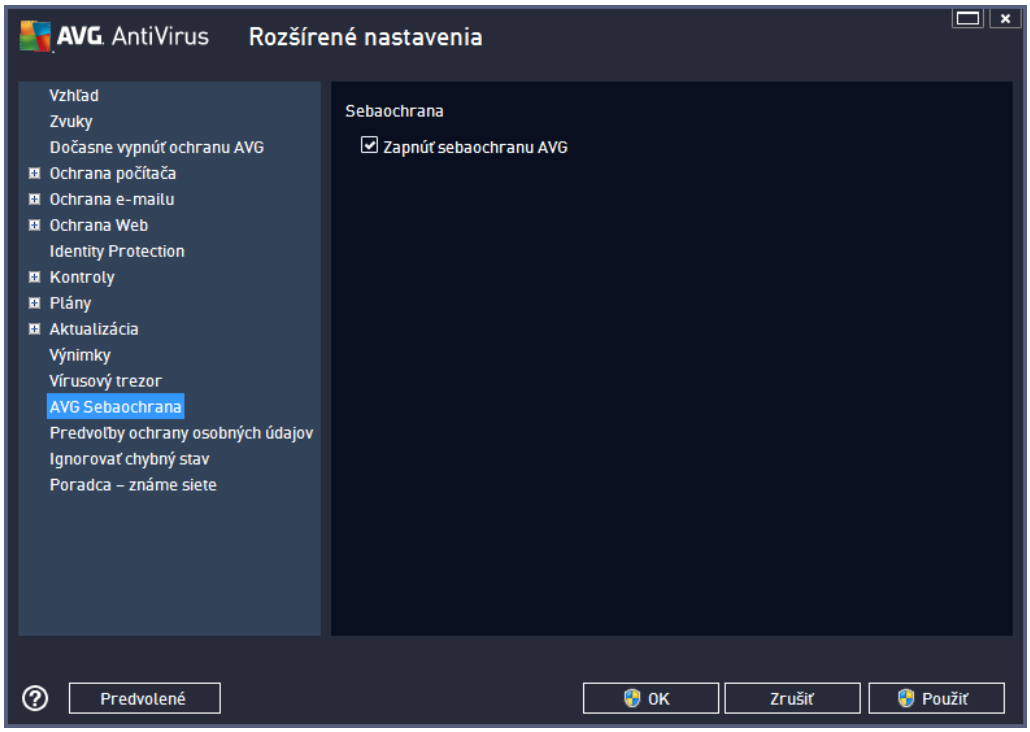


Dialógové okno ***Zachovanie Vírusového trezora*** vám umožňuje zadefinovať niekoľko parametrov ohľadom administrácie objektov uložených vo Vírusovom trezore:

- ***Obmedziť veľkosť vírusového trezora*** – použite posúvač na nastavenie maximálnej veľkosti vírusového trezora. Táto veľkosť sa uvádza úmerne v porovnaní s veľkosťou vášho lokálneho disku.

- ***Automatické vymazávanie súborov*** – v tejto časti môžete zadefinovať maximálnu dĺžku času, počas ktorého by mali byť objekty uložené vo Vírusovom trezore (***Vymazať súbory staršie ako ... dní***) a maximálny počet súborov, ktoré budú uložené vo Vírusovom trezore (***Maximálny počet uložených súborov***).

9.13. AVG Sebaochrana

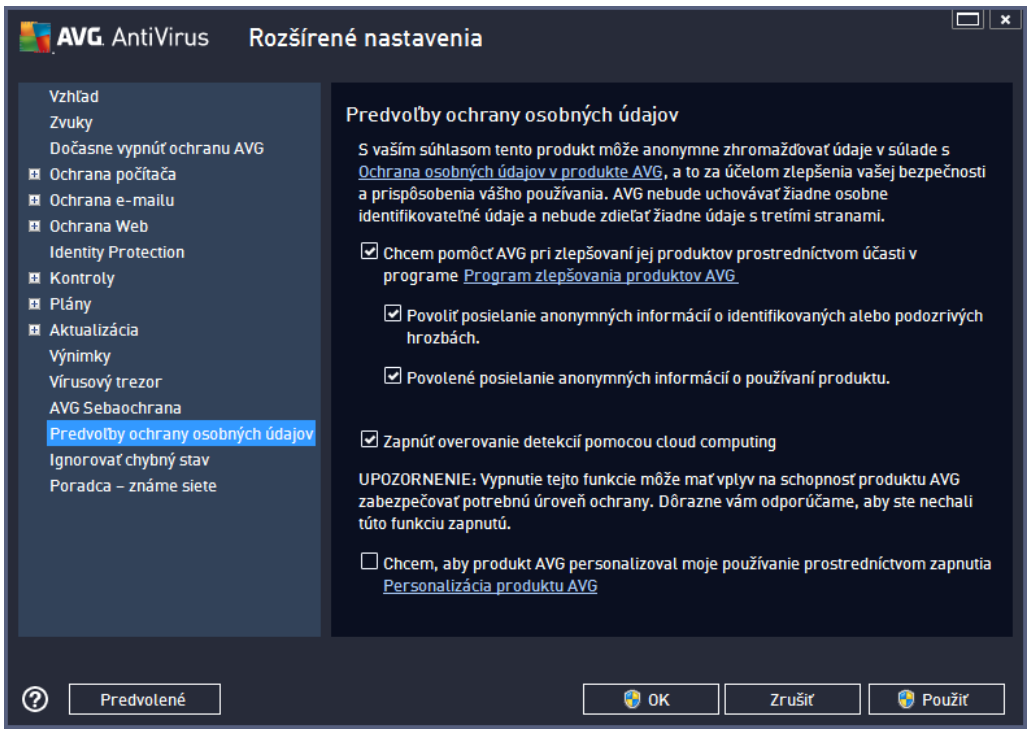


Funkcia ***AVG Sebaochrana*** umožňuje programu **AVG AntiVirus 2013** chrániť svoje vlastné procesy, súbory, záznamy v registri a ovládače pred zmenou alebo deaktiváciou. Hlavným dôvodom pre tento druh ochrany je, že niektoré sofistikované hrozby sa snažia vypnúť antivírusovú ochranu a potom nerušene poškodzujú váš počítač.

Odporúčame vám túto funkciu ponechať zapnutú!

9.14. Preferencie ochrany osobných údajov

Dialógové okno ***Preferencie ochrany osobných údajov*** vám ponúkne možnosť účasti na programe zlepšovania služieb AVG, aby ste nám pomohli zlepšiť celkovú úroveň zabezpečenia na internete. Vaše hlásenia nám pomáhajú zhromažďovať aktuálne informácie o najnovších hrozbách od účastníkov z celého sveta a umožňuje nám to zlepšovať ochranu pre každého jednotlivca. Hlásenia sa vykonávajú automaticky a preto vám nespôsobia žiadne nepohodlie. Hlásenia neobsahujú žiadne osobné údaje. Hlásenie zistených hrozieb je voliteľné, radi by sme vás ale požiadali o jeho zapnutie. Pomáha zlepšiť nielen vašu ochranu, ale aj ochranu ostatných používateľov aplikácie AVG.



V dialógovom okne sú k dispozícii tieto možnosti nastavenia:

- ***Rád by som pomohol spoločnosti AVG zlepšovať ich produkty a chcem sa zúčastniť Programu zlepšovania produktov AVG*** *(štandardne zapnuté)* – Ak nám chcete pomáhať v ďalšom zlepšovaní **AVG AntiVirus 2013**, nechajte toto políčko začiarknuté. Táto funkcia zapne oznamovanie všetkých zaznamenaných hrozieb do spoločnosti AVG a umožní nám zhromažďovať najnovšie informácie o hrozbách od všetkých účastníkov z celého sveta a zlepšovať ochranu pre každého jednotlivca. Nahlasovanie prebieha automaticky, preto vás nijako nezaťažuje, a v správach nie sú uvedené žiadne osobné údaje.
    - ***Povoliť posielanie informácií o nesprávne identifikovaných e-mailoch po potvrdení používateľom*** *(predvolene zapnuté)* – posielať informácie o e-mailových správach, ktoré boli nesprávne označené ako spam, alebo spamových správach, ktoré súčasť Anti-Spam nedetegovala. Pred poslaním tohto druhu informácií vás program požiada o potvrdenie.
    - ***Povoliť posielanie anonymných informácií o identifikovaných alebo podozrivých hrozbách*** *(predvolene zapnuté)* – posielať informácie o podozrivom alebo pozitívne nebezpečnom kóde alebo priebehu správania *(môže ísť o vírus, spyware alebo škodlivé internetové stránky, ktoré sa pokúšate otvoriť)* detegovanom na počítači.
    - ***Umožnite zasielať nám anonymné údaje o používaní produktu*** *(štandardne zapnuté)* – odosielanie základných štatistík o používaní aplikácie, ako je počet nájdených hrozieb, spustených kontrol, úspešné či neúspešné kontroly a pod.
- ***Zapnúť overovanie detekcií pomocou cloud computingu*** *(predvolene zapnuté)* – detegované hrozby sa budú overovať, či sú naozaj infikované, aby sa vylúčili nesprávne detekcie.

- ***Želám si, aby sa produkty AVG prispôsobili mojej práci zapnutím funkcie AVG Personalizácia*** – táto funkcia anonymne analyzuje správanie programov a aplikácií vo vašom počítači. Na základe tejto analýzy vám môže spoločnosť AVG ponúkať služby na mieru vašich potrieb, aby vám zabezpečila maximálnu bezpečnosť.

Najbežnejšie hrozby

V dnešnej dobe existuje oveľa viac hrozieb ako sú len jednoduché vírusy. Autori škodlivého kódu a nebezpečných internetových stránok sú však veľmi inovatívni a pomerne často sa objavujú nové typy hrozieb, pričom absolútna väčšina z nich sa vyskytuje na internete. Toto sú niektoré z najčastejšie sa vyskytujúcich hrozieb:

- ***Vírus*** je škodlivý kód, ktorý sa kopíruje a šíri často bez povšimnutia, kým nenapácha škody. Niektoré vírusy predstavujú vážnu hrozbu, ktorá dokáže vymazať alebo zámerne zmeniť súbory, zatiaľ čo iné vírusy sú zdanlivo neškodné, napríklad zahrajú melódiu. Všetky vírusy sú však nebezpečné, pretože sa dokážu množiť. Jeden jediný vírus dokáže v okamihu zaplniť celú pamäť počítača a spôsobiť jeho zlyhanie.

- ***Červ*** je podkategória vírusu, ktorý (na rozdiel od vírusu) nepotrebuje „nosič“, ku ktorému by sa pripojil; sám sa rozosiela do ostatných počítačov, zvyčajne cez e-mail, a následne často preťažuje poštové servery a sieťové systémy

- ***Spyware*** sú zvyčajne sprievodné programy kategórie malware (*malware = každý škodlivý softvér, vrátane vírusov*), zvyčajne trójske kone, ktoré sa používajú na odcudzenie osobných informácií, hesiel, čísel kreditných kariet alebo na preniknutie do počítača a umožnenie útočníkovi ovládať počítač na diaľku; všetko samozrejme bez vedomia a súhlasu vlastníka počítača.

- ***Potenciálne nežiaduce programy*** je taký typ spywaru, ktorý môže, ale nemusí byť nevyhnutne nebezpečný pre počítač. Špecifickým príkladom PNP je adware, t. j. softvér určený na šírenie reklám, zvyčajne zobrazovaním reklamných prekrývacích okien, ktoré obťažujú, ale ktoré nie sú priamo škodlivé.

- ***Sledovacie súbory cookies*** sa môžu považovať za druh spywaru, pretože tieto malé súbory, uložené v internetovom prehliadači a automaticky posielané na „hlavnú“ internetovú stránku pri jej opätovnej návšteve, môžu obsahovať údaje ako je vaša história surfovania na internete a ďalšie podobné informácie.

- ***Zneužitie*** je škodlivý kód, ktorý využíva trhlinu alebo zraniteľnosť operačného systému, internetového prehliadača alebo iného základného programu.

- ***Phishing*** je pokus o získanie citlivých osobných údajov predstieraným zastupovaním dôveryhodnej a všeobecne známej organizácie. Potenciálne obete sú často kontaktované prostredníctvom hromadných e-mailov, v ktorých sa od nich požaduje napr. aby si aktualizovali informácie o bankových účtoch. Na tento účel majú kliknúť na uvedený odkaz, ktorý potom vedie na falošnú internetovú stránku banky.

- ***Hoax*** je hromadný e-mail, ktorý obsahuje nebezpečné, alarmujúce alebo jednoducho len otravné a neužitočné informácie. Na šírenie väčšiny vyššie uvedených hrozieb sa používajú podvodné e-mailové správy typu hoax

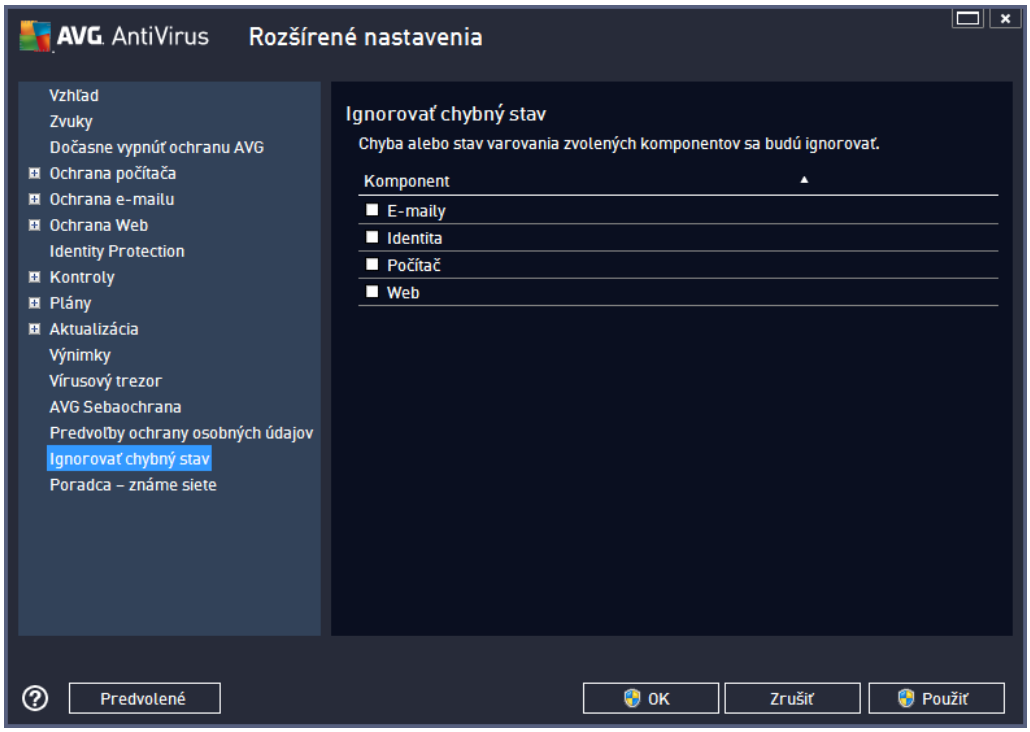
- ***Škodlivé internetové stránky*** sú napokon tie, ktoré úmyselne inštalujú škodlivý softvér do počítača a napadnuté stránky robia to isté, ibaže ide o legitímne internetové stránky, ktoré

boli zneužité na infikovanie počítača návštevníkov.

V záujme ochrany pred všetkými druhmi hrozieb produkt AVG AntiVirus 2013 obsahuje špecializované súčasti. Ich stručný opis nájdete v kapitole Prehľad súčastí.

9.15. Ignorovať chybný stav

V dialógovom okne ***Ignorovať chybný stav*** môžete označiť tie súčasti, o ktorých nechcete byť informovaní:



V predvolenom nastavení sa v tomto zozname nenachádza žiadna súčasť. To znamená, že ak sa niektorá súčasť dostane do chybového stavu, budete o tom ihneď informovaní pomocou:

- Ikony na paneli úloh – keď všetky časti aplikácie AVG fungujú správne, potom má ikona štyri farby; keď sa však vyskytne chyba, ikona bude mať žltý výkričník.
- Textového opisu existujúceho problému v časti Informácie o stave zabezpečenia v hlavnom okne programu AVG.

Môže nastať situácia, keď z nejakého dôvodu bude potrebné dočasne túto súčasť vypnúť. ***To sa neodporúča, snažte sa mať neustále všetky súčasti zapnuté a v predvolenej konfigurácii***. Avšak niekedy sa takej situácii nemožno vyhnúť. V tom prípade ikona v paneli úloh automaticky oznámi chybový stav komponentu. V tomto konkrétnom prípade však nemôžeme hovoriť o skutočnej chybe, pretože ste ju vyvolali úmyselne a ste si vedomý potenciálneho rizika. Zároveň, keď je ikona zobrazená sivou farbou, nemôže vlastne oznámiť žiadne ďalšie prípadné chyby, ktoré by sa mohli vyskytnúť.

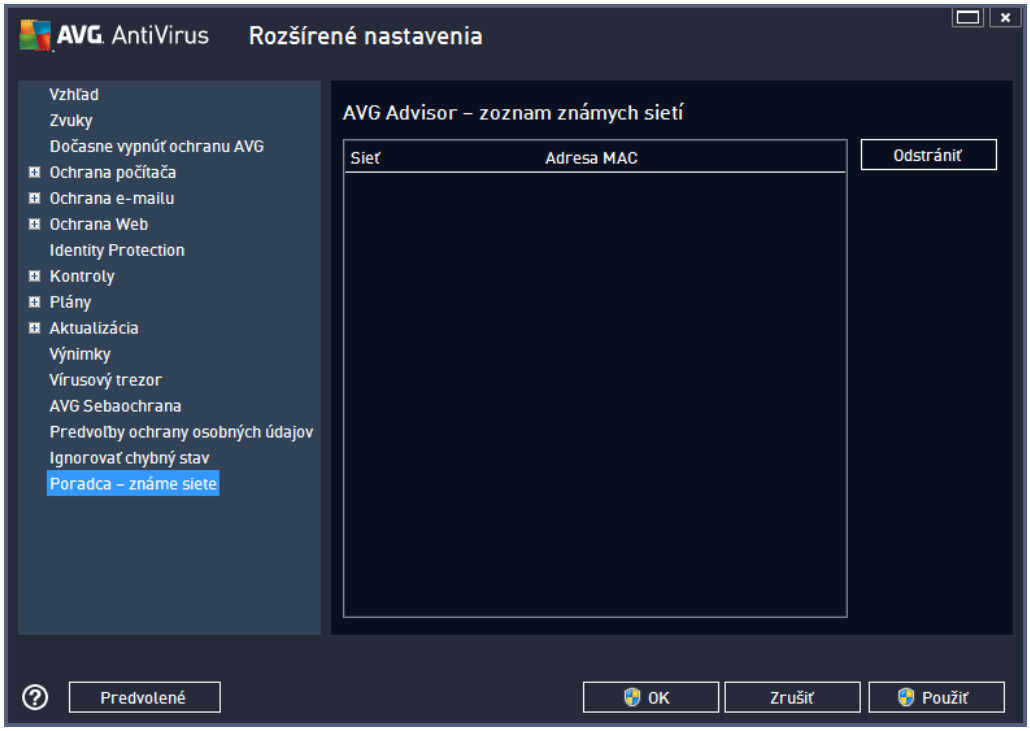
V tejto situácii môžete v dialógovom okne ***Ignorovať chybný stav*** vybrať súčasti, o ktorých prípadnom chybnom stave (*alebo vypnutí*) si neželáte byť informovaní. Kliknutím na tlačidlo ***OK***

potvrďte zmeny.

9.16. Aplikácia Advisor – známe siete

Aplikácia AVG Advisor obsahuje funkciu sledovania sietí, ku ktorým sa pripájate. Ak nájde novú sieť *(s už použitým názvom siete, čo môže viesť k omylu),* upozorní vás a odporučí vám, aby ste skontrolovali zabezpečenie danej siete. Ak sa rozhodnete, že je bezpečné pripojiť sa k novej sieti, môžete ju tiež uložiť do tohto zoznamu. *(Prostredníctvom odkazu v oblasti oznámení na paneli úloh AVG Advisor, ktoré sa vysunie nad panelom úloh pri rozpoznaní neznámej siete. Podrobnosti nájdete v kapitole AVG Advisor).* AVG Advisor si zapamätá jedinečné atribúty siete *(predovšetkým adresu MAC)* a najbližšie už oznámenie nezobrazí. Každá sieť, ku ktorej sa pripojíte, sa bude automaticky považovať za známu a pridá sa do zoznamu. Jednotlivé záznamy môžete vymazať stlačením tlačidla ***Odstrániť***; daná sieť bude následne opäť považovaná za neznámu a potenciálne nebezpečnú.

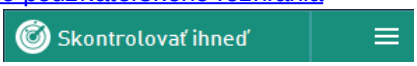
V tomto dialógovom okne môžete skontrolovať, ktoré siete sa považujú za známe:



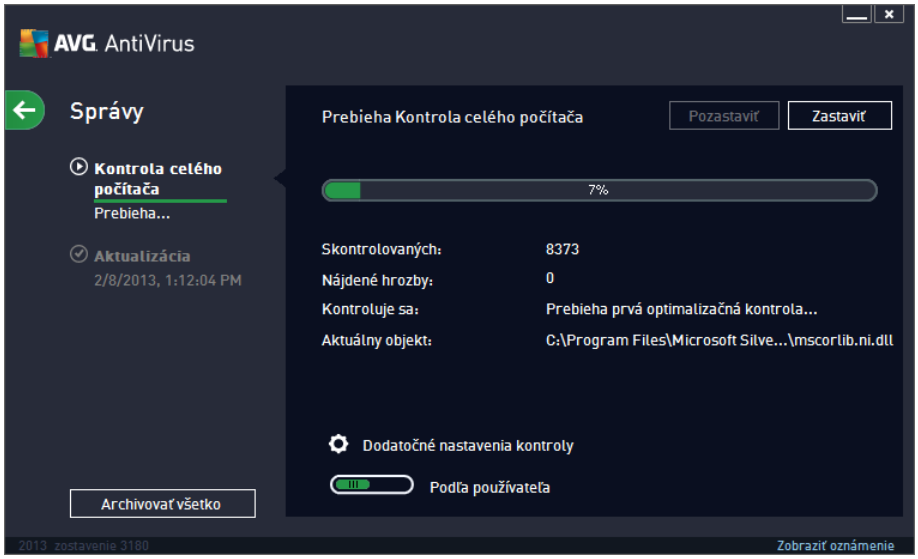
Poznámka: *Funkcia známych sietí v súčasti AVG Advisor nie je podporovaná v 64-bitových systémoch Windows XP.*

10. Kontrola programom AVG

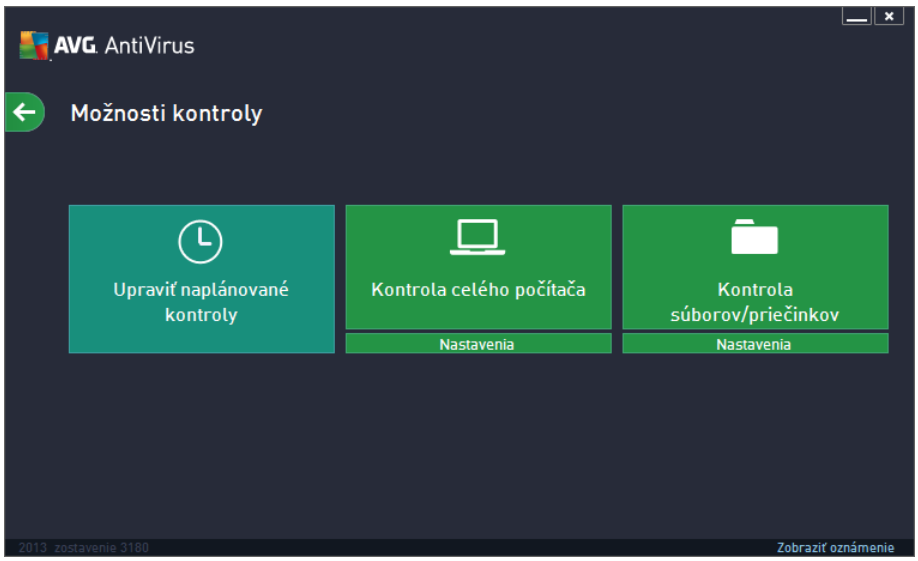
V predvolenom nastavení aplikácia **AVG AntiVirus 2013** nespúšťa žiadnu kontrolu, pretože po úvodnej kontrole *(zobrazí sa vám návrh na jej spustenie)* by ste mali byť dokonale chránení rezidentnými súčasťami produktu **AVG AntiVirus 2013**, ktoré sú vždy na stráži a nedovolia žiadnemu škodlivému kódu preniknúť do počítača. Samozrejme, že môžete naplánovať kontrolu, ktorá sa bude spúšťať v pravidelných intervaloch, alebo manuálne kedykoľvek spustiť kontrolu podľa vlastných potrieb.

K rozhraniu kontroly programu AVG máte prístup z hlavného používateľského rozhrania prostredníctvom tlačidla graficky rozdeleného na dve časti: 

- ***Skontrolovať ihneď*** – Stlačte toto tlačidlo pre okamžité spustenie Kontroly celého počítača a sledujte jej priebeh a výsledky v automaticky otvorenom okne Výsledky:



- ***Možnosti*** – Vyberte toto tlačidlo *(graficky zobrazené ako tri vodorovné čiary v zelenom poli)*, ktorým otvoríte dialógové okno ***Možnosti kontroly***, kde môžete upraviť naplánované kontroly a upraviť parametre kontroly celého počítača/kontroly súborov/priečinkov:



V dialógovom okne ***Možnosti kontroly*** sa nachádzajú tri hlavné časti konfigurácie kontroly:

- ***Upraviť naplánované kontroly*** – Kliknutím na túto možnosť sa otvorí nové dialógové okno s prehľadom všetkých naplánovaných kontrol. Než zadefinujete vlastné kontroly, zobrazí sa v tabuľke iba jeden plán kontroly, ktorý vopred definoval dodávateľ softvéru. Táto kontrola je štandardne vypnutá. Ak ju chcete zapnúť, kliknite na ňu pravým tlačidlom a v kontextovej ponuke vyberte možnosť *Povoliť úlohu*. Po povolení plánu kontroly môžete upraviť jej konfiguráciu tlačidlom *Upraviť plán kontroly* . Taktiež môžete kliknúť na možnosť *Pridať plán kontroly*, aby ste vytvorili nový plán.

- ***Kontrola celého počítača/Nastavenia*** – Tlačidlo je rozdelené na dve časti. Kliknutím na položku *Kontrola celého počítača* okamžite spustíte kontrolu celého počítača *(podrobnosti o kontrole celého počítača nájdete v príslušnej kapitole s názvom Vopred definované kontroly/Kontrola celého počítača)*. Kliknutím na spodnú časť*Nastavenia* sa zobrazí konfiguračné okno, kde môžete nastaviť parametre kontroly celého počítača.

- ***Kontrola súborov/priečinkov/Nastavenia*** – Tlačidlo je opäť rozdelené na dve časti. Kliknutím na možnosť *Kontrola súborov/priečinkov* okamžite spustíte kontrolu vybraných oblastí počítača *(podrobnosti o kontrole súborov a priečinkov nájdete v príslušnej kapitole s názvom Vopred definované kontroly/Kontrola súborov/priečinkov)*. Kliknutím na spodnú časť *Nastavenia* sa zobrazí konfiguračné okno, kde môžete nastaviť parametre kontroly súborov/priečinkov.

10.1. Vopred definované kontroly

Jednou z hlavných funkcií produktu **AVG AntiVirus 2013** je kontrola na požiadanie. Testy na požiadanie sú určené na kontrolu rôznych častí počítača pri každom podozrení možného výskytu vírusovej infekcie. Odporúča sa vykonávať takéto testy pravidelne, aj keď si myslíte, že sa vo vašom počítači nenájde žiadny vírus.

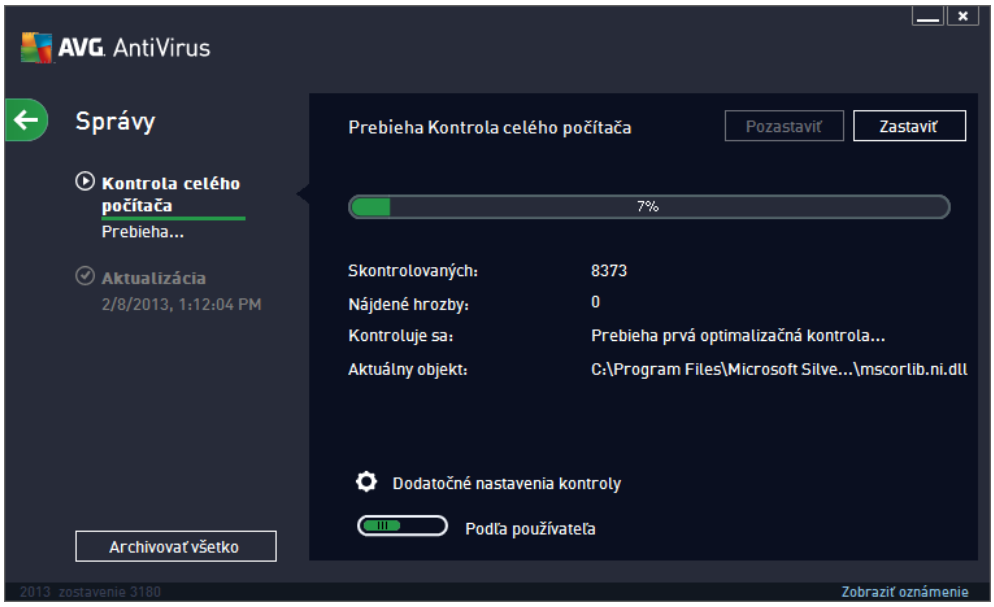
V produkte **AVG AntiVirus 2013** sa nachádzajú tieto typy kontrol vopred definované dodávateľom softvéru:

10.1.1. Kontrola celého počítača

Kontrola celého počítača – Skontroluje možné infekcie alebo potenciálne nežiaduce programy v celom počítači. Tento test bude kontrolovať všetky pevné disky vášho počítača, bude detegovať a liečiť všetky nájdené vírusy a odstráni detegovanú infekciu do Vírusového trezora. Kontrola celého počítača by mala byť naplánovaná na pracovnej stanici aspoň raz do týždňa.

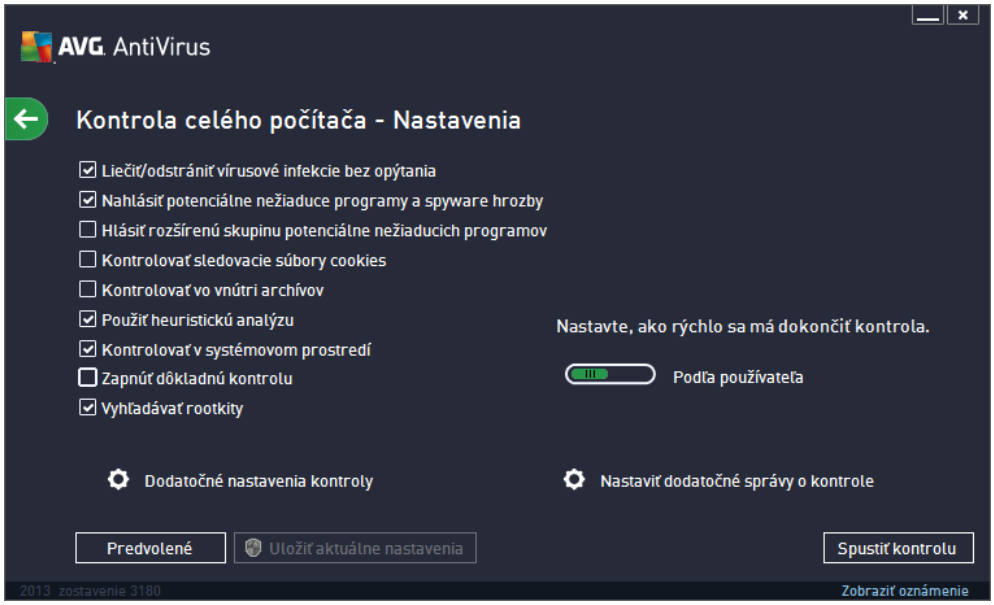
Spustenie kontroly

Kontrolu celého počítača môžete spustiť priamo z hlavného používateľského rozhrania kliknutím na tlačidlo ***Skontrolovať teraz***. Pre tento typ kontroly netreba žiadne ďalšie nastavenia, kontrola sa spustí okamžite. V dialógovom okne ***Prebieha kontrola celého počítača*** (*pozri snímku obrazovky*) môžete sledovať priebeh a výsledky. V prípade potreby môžete kontrolu dočasne prerušiť (tlačidlo ***Pozastaviť***) alebo zrušiť (tlačidlo ***Zastaviť***).



Zmena konfigurácie kontroly

Konfiguráciu ***kontroly celého počítača*** môžete upraviť v dialógovom okne ***Kontrola celého počítača – Nastavenia*** *(okno je prístupné cez odkaz Nastavenia pre Kontrolu celého počítača v rámci okna Možnosti kontroly)*. ***Odporúča sa ponechať predvolené nastavenia, ak nemáte závažný dôvod ich meniť!***



V zozname parametrov kontroly môžete zapnúť/vypnúť špecifické parametre podľa potreby:

- ***Liečiť/odstrániť vírusovú infekciu bez opýtania*** *(štandardne zapnuté)* – Ak sa počas kontroly nájde vírus, môže byť automaticky vyliečený, pokiaľ je liek k dispozícii. Ak nie je možné infikovaný súbor vyliečiť automaticky, premiestni sa do Vírusového trezora.

- ***Nahlásiť potenciálne nežiaduce programy a spyware hrozby*** *(štandardne zapnuté)* – Začiarknite toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu škodlivého softvéru: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.

- ***Hlásiť rozšírenú skupinu potenciálne nežiaducich programov*** *(štandardne vypnuté)* – Začiarknite toto políčko, ak sa má detegovať rozšírená skupina spywaru: programov, ktoré sú úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpečenia počítača, ale môže blokovať dobré programy, a preto je táto funkcia štandardne vypnutá.

- ***Kontrolovať sledovacie súbory cookies*** *(štandardne vypnuté)* – Tento parameter súčasti zapína funkciu na detekciu súborov cookies; *(HTTP cookies sa používajú na overenie totožnosti, sledovanie a správu konkrétnych informácií o používateľoch, akými sú napr. preferencie stránok alebo obsah elektronických nákupných košíkov)*.

- ***Kontrolovať vo vnútri archívov*** *(štandardne vypnuté)* – Tento parameter určuje, že sa majú počas kontroly preverovať všetky súbory uložené vnútri archívov, napr. ZIP, RAR, ...

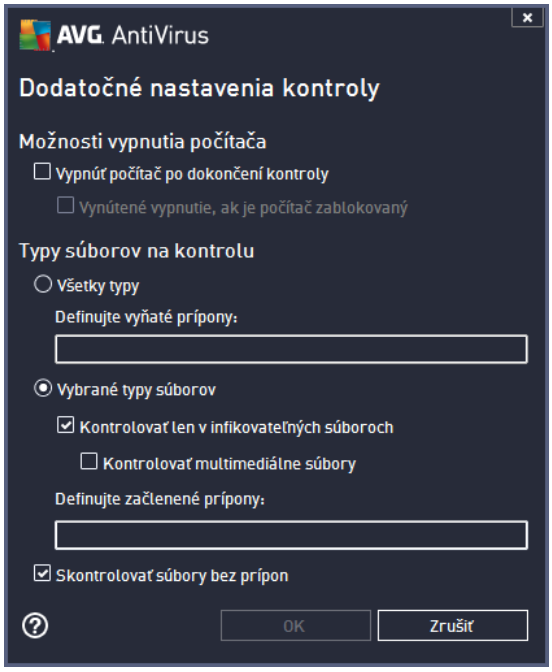
- ***Použiť heuristickú analýzu*** *(štandardne zapnuté)* – Heuristická analýza *(dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí)* bude jedna z metód, ktoré sa použijú na detekciu vírusov počas kontroly.

- ***Kontrolovať v systémovom prostredí*** *(štandardne zapnuté)* – Počas kontroly sa budú

kontrolovať aj systémové oblasti počítača.

- ***Zapnúť dôkladnú kontrolu*** *(štandardne vypnuté)* – V určitých situáciách *(podozrenie na infikovanie počítača)* môžete touto možnosťou aktivovať najdôkladnejšie kontrolné algoritmy, ktoré pre istotu skontrolujú aj tie oblasti počítača, ktoré sa obyčajne vôbec neinfikujú. Upozorňujeme však, že tento spôsob je náročný na čas.

- ***Dodatočné nastavenia kontroly***: Tento odkaz otvorí nové dialógové okno Dodatočné nastavenia kontroly, ktoré sa používa na nastavenie nasledujúcich parametrov:



  - ***Možnosti vypnutia počítača*** – Rozhodnite, či sa má počítač vypnúť automaticky po dokončení procesu kontroly. Po potvrdení tejto možnosti (***Vypnúť počítač po dokončení kontroly***) sa aktivuje nová možnosť, ktorá umožní vypnúť počítač, aj keď je momentálne zablokovaný (***Vynútené vypnutie, ak je počítač zablokovaný***).

  - ***Typy súborov na kontrolu*** – Mali by ste tiež určiť, čo chcete kontrolovať:

    - ***Všetky typy súborov*** s možnosťou definovať výnimky z kontroly vytvorením zoznamu čiarkou oddelených prípon súborov, ktoré sa nemajú kontrolovať.

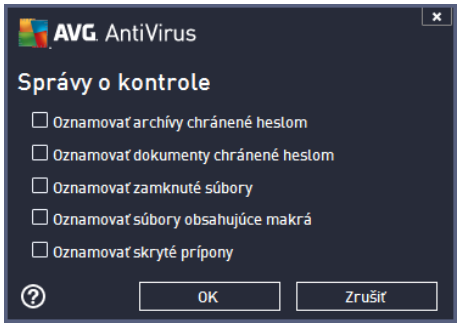
    - ***Vybrané typy súborov*** – Môžete nastaviť, aby sa kontrolovali len súbory, pri ktorých existuje pravdepodobnosť infikovania (*(súbory, ktoré nemôžu byť napadnuté infekciou, napríklad niektoré jednoduché textové súbory alebo niektoré nespustiteľné súbory, sa nebudú kontrolovať)*, vrátane mediálnych súborov *(video, audio súborov – ak necháte toto políčko nezačiarknuté, potom sa čas prehľadávania skráti ešte viac, pretože tieto súbory sú často veľmi veľké, pričom pravdepodobnosť napadnutia vírusom je veľmi malá*). Znova môžete definovať, podľa prípony, ktoré súbory sa majú kontrolovať vždy.

    - Alternatívne môžete rozhodnúť, že chcete ***kontrolovať súbory bez prípony***. Táto možnosť je štandardne zapnutá a odporúčame vám, aby ste toto nastavenie

nikdy nemenili, ak na to nemáte skutočný dôvod. Súbory bez prípony sú skôr podozrivé a mali by sa vždy kontrolovať.

- ***Nastaviť rýchlosť dokončenia kontroly*** – Pomocou posúvača zmeňte prioritu procesu kontroly. V predvolenom nastavení je úroveň automatického využívania zdrojov nastavená *Podľa používateľa*. Prípadne môžete spustiť procesy prehľadávania pomalšie, čím sa minimalizuje využívanie systémových zdrojov (*toto nastavenie je užitočné vtedy, ak potrebujete pracovať na počítači, ale nezaujíma vás, ako dlho bude prehľadávanie trvať*) alebo rýchlejšie s vyššími nárokmi na využívanie systémových zdrojov (*napr. keď sa počítač dočasne nepoužíva*).

- ***Vytvoriť ďalšie správy o kontrole*** – Odkaz otvorí nové dialógové okno ***Správy o kontrole***, v ktorom môžete určiť, aké typy možných nálezov sa majú uviesť v správach:



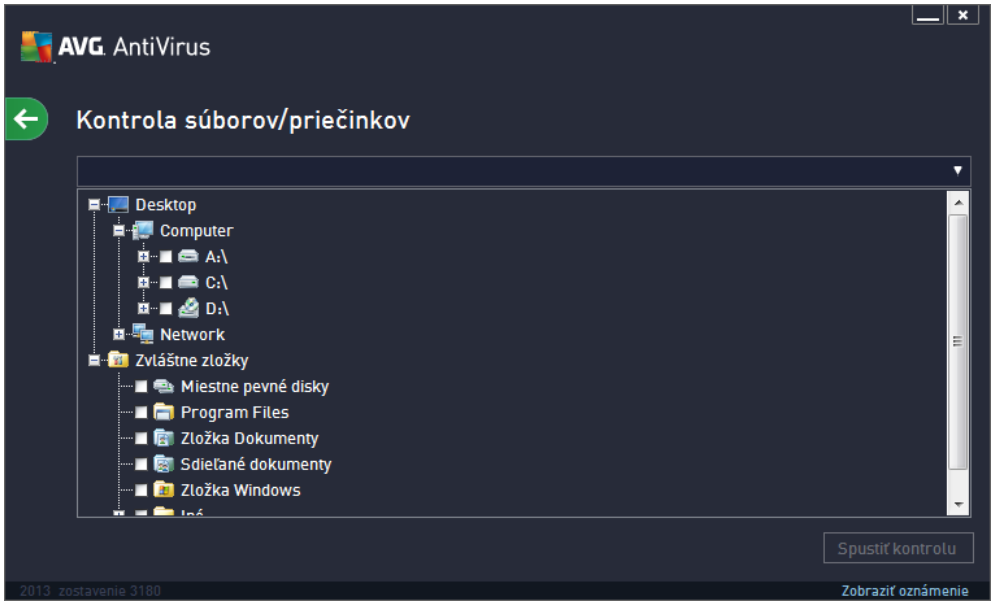
Upozornenie: *Tieto nastavenia kontroly sa zhodujú s parametrami novodefinovanej kontroly; pozri informácie v kapitole Kontrola programom AVG/Plánovanie kontroly/Ako kontrolovať. Ak sa rozhodnete zmeniť predvolenú konfiguráciu funkcie* ***Kontrola celého počítača****, svoje nové nastavenie môžete uložiť ako predvolenú konfiguráciu, ktorá sa použije pre všetky ďalšie kontroly celého počítača.*

10.1.2. Kontrola súborov/priečinkov

Kontrola súborov/priečinkov – prehľadávať sa budú len vami vybrané oblasti počítača (*vybrané priečinky, pevné disky, diskety, disky CD a pod.*). Priebeh kontroly pri detekcii vírusu a jeho liečba sú rovnaké ako pri kontrole celého počítača: všetky nájdené vírusy sa vyliečia alebo odstránia do Vírusového trezora. Kontrolu vybraných súborov alebo priečinkov môžete použiť na nastavenie vlastných testov a ich plánov v závislosti od konkrétnych potrieb.

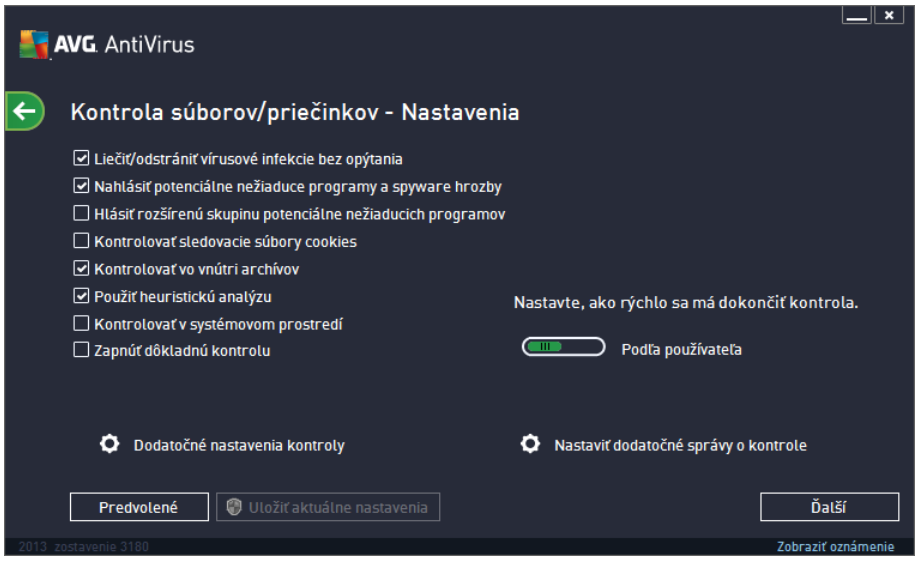
Spustenie kontroly

Funkciu ***Kontrola súborov/priečinkov*** môžete spustiť priamo z okna Možnosti kontroly kliknutím na tlačidlo **Kontrola súborov/priečinkov**. Otvorí sa nové dialógové okno s názvom ***Výber konkrétnych súborov alebo priečinkov na kontrolu***. V stromovej štruktúre počítača vyberte tie priečinky, ktoré chcete kontrolovať. Cesta ku každému zvolenému priečinku sa vygeneruje automaticky a objaví sa v textovom okne vo vrchnej časti tohto dialógového okna. Rovnako môžete nastaviť prehľadávanie konkrétneho priečinka, ktorého vnorené priečinky sa vylúčia z tohto prehľadávania; v tom prípade vložte znak mínus „**-**“ pred automaticky vygenerovanú cestu (*pozri snímku obrazovky*). Na vylúčenie celého priečinka z kontroly použite parameter „**!**“ . Napokon, ak chcete spustiť kontrolu, stlačte tlačidlo ***Spustiť kontrolu***; samotný proces kontrolovania sa v podstate zhoduje s kontrolou celého počítača.



Zmena konfigurácie kontroly

Konfiguráciu ***Kontroly súborov/priečinkov*** môžete upraviť v dialógovom okne ***Kontrola súborov/priečinkov – Nastavenia*** *(okno zobrazíte odkazom Nastavenia v časti Kontrola súborov/priečinkov v okne Možnosti kontroly)*. ***Odporúča sa ponechať predvolené nastavenia, ak nemáte závažný dôvod ich meniť!***



V tomto zozname parametrov kontroly môžete podľa potreby vypnúť alebo zapnúť konkrétne parametre:

- ***Liečiť/odstrániť vírusovú infekciu bez opýtania*** *(štandardne zapnuté)*: Ak sa počas kontroly zistí prítomnosť vírusu, môže sa automaticky vyliečiť, ak je k dispozícii liečba. Ak nie je možné infikovaný súbor vyliečiť automaticky, premiestni sa do Vírusového trezora.

- ***Nahlásiť potenciálne nežiaduce programy a spyware hrozby*** *(štandardne zapnuté)*: Začiarknite toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu škodlivého softvéru: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.

- ***Hlásiť rozšírenú skupinu potenciálne nežiaducich programov*** *(štandardne vypnuté)*: Začiarknite toto políčko, ak sa má detegovať rozšírená skupina spywaru: programov, ktoré sú úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpečenia počítača, ale môže blokovať dobré programy, a preto je táto funkcia štandardne vypnutá.

- ***Kontrolovať sledovacie súbory cookies*** *(štandardne vypnuté)*: Tento parameter súčasti zapína detekciu súborov cookies *(HTTP cookies sa používajú na overenie totožnosti, sledovanie a správu konkrétnych informácií o používateľoch, akými sú napr. preferencie stránok alebo obsah elektronických nákupných košíkov)*.

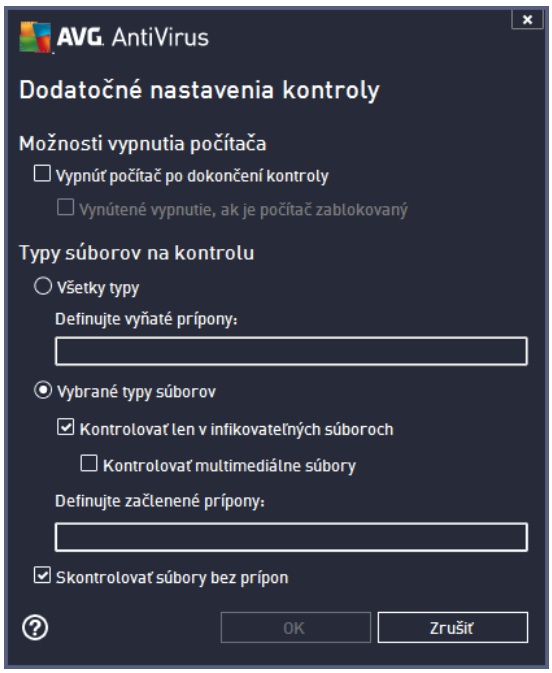
- ***Kontrolovať vo vnútri archívov*** *(štandardne zapnuté)*: Tento parameter určuje, že sa majú počas kontroly preverovať všetky súbory uložené vnútri archívov, napr. ZIP, RAR, ...

- ***Použiť heuristickú analýzu*** *(štandardne zapnuté)*: Heuristická analýza *(dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí)* bude jedna z metód, ktoré sa použijú na detekciu vírusov počas kontroly.

- ***Kontrolovať v systémovom prostredí*** *(štandardne vypnuté)*: Počas kontroly sa budú overovať aj systémové oblasti počítača.

- ***Zapnúť dôkladnú kontrolu*** *(štandardne vypnuté)*: V určitých situáciách *(podozrenie na infikovanie počítača)* môžete touto možnosťou aktivovať najdôkladnejšie kontrolné algoritmy, ktoré pre istotu skontrolujú aj tie oblasti počítača, ktoré sa obyčajne vôbec neinfikujú. Upozorňujeme však, že tento spôsob je náročný na čas.

- ***Dodatočné nastavenia kontroly*** – Tento odkaz otvorí nové dialógové okno ***Dodatočné nastavenia kontroly***, ktoré sa používa na nastavenie nasledujúcich parametrov:



- ***Možnosti vypnutia počítača*** – Rozhodnite, či sa má počítač vypnúť automaticky po dokončení procesu kontroly. Po potvrdení tejto možnosti (***Vypnúť počítač po dokončení kontroly***) sa aktivuje nová možnosť, ktorá umožní vypnúť počítač, aj keď je momentálne zablokovaný (***Vynútené vypnutie, ak je počítač zablokovaný***).

- ***Typy súborov na kontrolu*** – Mali by ste tiež určiť, čo chcete kontrolovať:

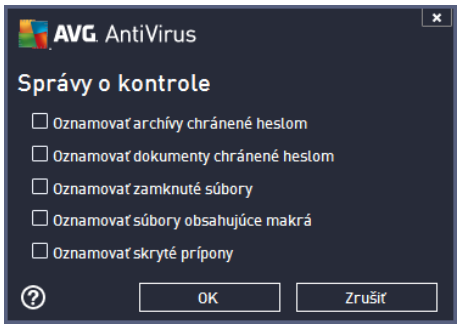
  - ***Všetky typy súborov*** s možnosťou definovať výnimky z kontroly vytvorením zoznamu čiarkou oddelených prípon súborov, ktoré sa nemajú kontrolovať.

  - ***Vybrané typy súborov*** – Môžete nastaviť, aby sa kontrolovali len súbory, pri ktorých existuje pravdepodobnosť infikovania (*(súbory, ktoré nemôžu byť napadnuté infekciou, napríklad niektoré jednoduché textové súbory alebo niektoré nespustiteľné súbory, sa nebudú kontrolovať)*, vrátane mediálnych súborov *(video, audio súborov – ak necháte toto políčko nezačiarknuté, potom sa čas prehľadávania skráti ešte viac, pretože tieto súbory sú často veľmi veľké, pričom pravdepodobnosť napadnutia vírusom je veľmi malá*). Znova môžete definovať, podľa prípony, ktoré súbory sa majú kontrolovať vždy.

  - Alternatívne môžete rozhodnúť, že chcete ***kontrolovať súbory bez prípony***. Táto možnosť je štandardne zapnutá a odporúčame vám, aby ste toto nastavenie nikdy nemenili, ak na to nemáte skutočný dôvod. Súbory bez prípony sú skôr podozrivé a mali by sa vždy kontrolovať.

- ***Nastaviť rýchlosť dokončenia kontroly*** – Pomocou posúvača zmeňte prioritu procesu kontroly. V predvolenom nastavení je úroveň automatického využívania zdrojov nastavená *Podľa používateľa*. Prípadne môžete spustiť procesy prehľadávania pomalšie, čím sa minimalizuje využívanie systémových zdrojov (*toto nastavenie je užitočné vtedy, ak potrebujete pracovať na počítači, ale nezaujíma vás, ako dlho bude prehľadávanie trvať*), alebo rýchlejšie s vyššími nárokmi na využívanie systémových zdrojov (*napr. keď sa počítač dočasne nepoužíva*).

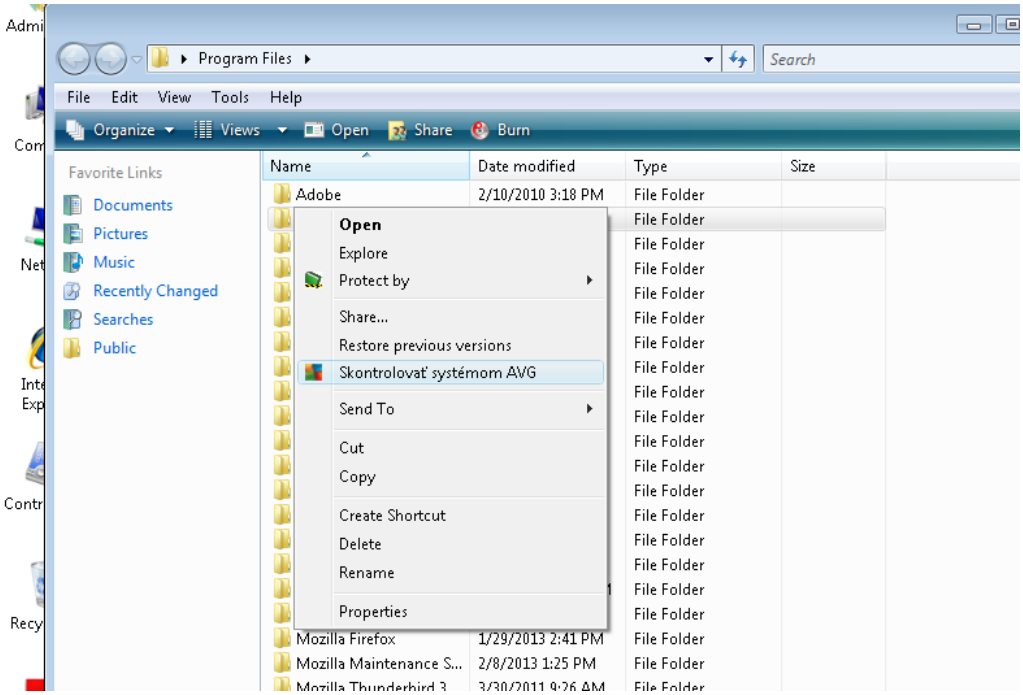
- ***Vytvoriť ďalšie správy o prehľadávaní*** – Odkaz otvorí nové dialógové okno ***Správy o prehľadávaní***, ktoré vám umožní nastaviť, ktoré typy možných nálezov sa majú hlásiť:



Upozornenie: *Tieto nastavenia kontroly sa zhodujú s parametrami novodefinovanej kontroly; pozri informácie v kapitole Kontrola programom AVG/Plánovanie kontroly/Ako kontrolovať. Ak sa rozhodnete zmeniť predvolenú konfiguráciu funkcie* ***kontrola súborov/priečinkov****, svoje nové nastavenie môžete potom uložiť ako predvolenú konfiguráciu, ktorá sa použije pre všetky ďalšie prehľadávania konkrétnych súborov alebo priečinkov. Táto konfigurácia sa zároveň použije ako šablóna pre všetky vami novonaplánované kontroly (všetky nastavené kontroly vychádzajú zo súčasnej konfigurácie kontroly vybraných súborov alebo priečinkov).*

10.2. Kontrola z prieskumníka

Okrem vopred definovaných kontrol spustených pre celý počítač alebo jeho vybrané oblasti, **AVG AntiVirus 2013** zároveň umožňuje rýchlo kontrolovať konkrétny objekt priamo v prostredí programu Prieskumník. Ak chcete otvoriť neznámy súbor a nie ste si istý jeho obsahom, môžete ho skontrolovať na požiadanie. Postupujte podľa týchto pokynov:



- V aplikácii Windows Explorer označte súbor *(alebo priečinok)*, ktorý chcete skontrolovať.

- Kliknutím pravým tlačidlom myši na objekt otvorte kontextovú ponuku.
- Výberom možnosti ***Skontrolovať programom AVG*** skontrolujte súbor programom **AVG AntiVirus 2013**

10.3. Kontrola z príkazového riadka

Program **AVG AntiVirus 2013** ponúka možnosť spustiť kontrolu z príkazového riadka. Túto funkciu môžete použiť napríklad na serveroch, alebo keď vytvárate dávkový skript, ktorý sa bude spúšťať automaticky po zavedení operačného systému. Príkazový riadok umožňuje spustiť kontrolu s väčšinou parametrov, ktoré sa nachádzajú aj v grafickom používateľskom rozhraní AVG.

Pre spustenie kontroly AVG z príkazového riadka spustite nasledovný príkaz v priečinku, kde je nainštalovaný program AVG:

- ***avgscanx*** pre 32-bitové operačné systémy
- ***avgscana*** pre 64-bitové operačné systémy

Syntax príkazu

Toto je syntax príkazového riadka:

- ***avgscanx /parameter*** ... napr. ***avgscanx /comp*** pre kontrolu celého počítača
- ***avgscanx /parameter /parameter*** ... Ak použijete niekoľko parametrov, zoraďte ich za sebou a oddeľte ich medzerou a lomkou.
- Ak sa musí uviesť konkrétna hodnota pre parameter (napr. parameter ***/scan***, ktorý si vyžaduje informáciu o tom, ktoré oblasti počítača sa majú kontrolovať, a je potrebné uviesť presnú cestu k vybranej časti), potom sa hodnoty oddelia bodkočiarkou, napríklad: ***avgscanx /scan=C:\;D:***

Parametre kontroly

Ak chcete zobraziť úplný prehľad použiteľných parametrov, zadajte príslušný príkaz spolu s parametrom /? alebo /HELP (napr. ***avgscanx /?***). Jediný povinný parameter je /SCAN, ktorý definuje oblasti počítača, ktoré sa majú kontrolovať. Podrobnejšie informácie o možnostiach sa nachádzajú v prehľade parametrov príkazového riadka.

Na spustenie kontroly stlačte kláves ***Enter***. Počas kontrolovania môžete zastaviť tento proces pomocou kombinácie tlačidiel ***Ctrl+C*** alebo ***Ctrl+Pause***.

Kontrola z príkazového riadka spustená z grafického rozhrania

Keď je systém Windows spustený v núdzovom režime, máte možnosť spustiť kontrolu pomocou príkazového riadka z grafického používateľského rozhrania. Samotná kontrola sa spustí z príkazového riadka, dialógové okno ***Command Line Composer*** umožňuje zadať väčšinu parametrov

kontroly len pomocou praktického grafického rozhrania.

Keďže toto dialógové okno je dostupné len v Núdzovom režime systému Windows, podrobnejší popis tohto dialógového okna nájdete v súbore pomocníka, ktorý otvoríte priamo z dialógového okna.

10.3.1. Parametre kontroly z príkazového riadka

Nasleduje zoznam všetkých dostupných parametrov pre kontrolu z príkazového riadka:

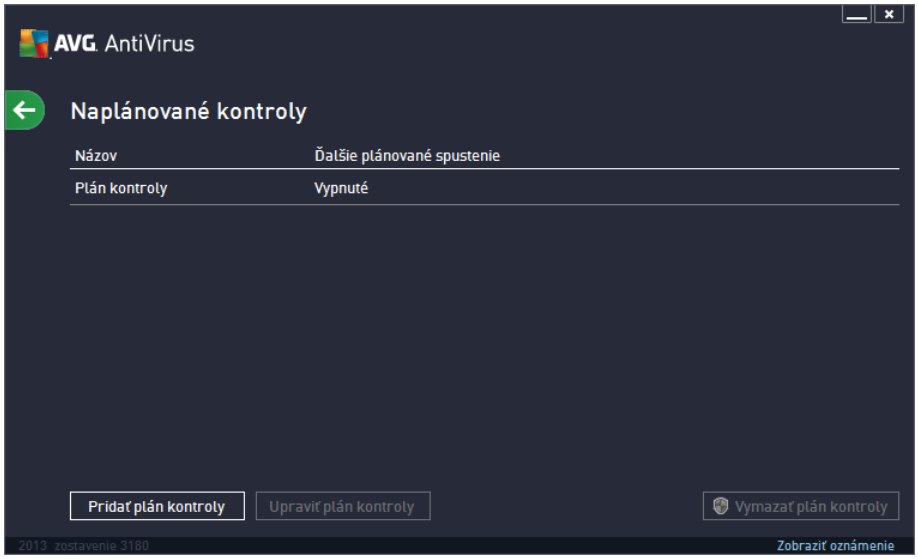
- /SCAN Kontrola súborov/priečinkov /SCAN=path;path *(napr. /SCAN=C:\;D:\)*
- /COMP Kontrola celého počítača
- /HEUR Použiť heuristickú analýzu
- /EXCLUDE Cesty alebo súbory, ktoré sa majú vyňať z kontroly
- /@ Súbor s príkazmi /názov súboru/
- /EXT Kontrolovať tieto prípony /napríklad EXT=EXE,DLL/
- /NOEXT Nekontrolovať tieto prípony /napríklad NOEXT=JPG/
- /ARC Kontrolovať archívy
- /CLEAN Automaticky vyčistiť
- /TRASH Presunúť infikované súbory do Vírusového trezora
- /QT Rýchly test
- /LOG Generovať súbor s výsledkami kontroly
- /MACROW Hlásiť makrá
- /PWDW Hlásiť súbory chránené heslom
- /ARCBOMBSW Hlásiť opakovane komprimované archívne súbory
- /IGNLOCKED Ignorovať zamknuté súbory
- /REPORT Hlásiť do súboru /názov súboru/
- /REPAPPEND Pripojiť k súboru s hlásením
- /REPOK Hlásiť neinfikované súbory so značkou OK
- /NOBREAK Nepovoliť prerušenie klávesmi CTRL-BREAK
- /BOOT Povoliť kontrolu MBR/BOOT
- /PROC Kontrolovať aktívne procesy

- /PUP Hlásiť potenciálne nežiaduce programy
- /PUPEXT Hlásiť rozšírenú skupinu potenciálne nežiaducich programov
- /REG Kontrolovať v registroch
- /COO Kontrolovať súbory cookies
- /? Zobraziť pomocníka pre túto tému
- /HELP Zobraziť pomocníka pre túto tému
- /PRIORITY Nastaviť prioritu kontroly /nízka, automatická, vysoká/ *(pozri časť Rozšírené nastavenia/Kontroly)*
- /SHUTDOWN Vypnúť počítač po dokončení kontroly
- /FORCESHUTDOWN Vynútené vypnutie počítača po dokončení kontroly
- /ADS Kontrolovať alternatívne dátové prúdy *(len pre NTFS)*
- /HIDDEN Hlásiť súbory so skrytými príponami
- /INFECTABLEONLY Kontrolovať len súbory s infikovateľnými príponami
- /THOROUGHSCAN Zapnúť dôkladnú kontrolu
- /CLOUDCHECK Kontrola nesprávnych pozitívnych detekcií
- /ARCBOMBSW Hlásiť opakovane komprimované archivačné súbory

10.4. Plánovanie kontroly

S aplikáciou **AVG AntiVirus 2013** môžete spustiť kontrolu na požiadanie *(napríklad keď máte podozrenie, že sa do počítača dostala infekcia)* alebo na základe vytvoreného plánu. Odporúča sa spúšťať kontroly na základe plánov: týmto spôsobom môžete zabezpečiť, že je váš počítač chránený pred možnosťou infekcie a nebudete si musieť robiť starosti s tým, kedy a či vôbec máte spustiť kontrolu. Odporúčame vám, aby ste pravidelne, najmenej raz za týždeň, spustili kontrolu celého počítača. Podľa možností však spúšťajte kontrolu celého počítača každý deň – tak, ako je to nastavené v predvolenej konfigurácii plánu kontroly. Ak je počítač „stále zapnutý“, potom môžete naplánovať kontrolu na čas, keď sa počítač nepoužíva. Ak je počítač v tomto čase vypnutý, potom sa zmeškané naplánované kontroly spustia pri spustení počítača.

Plán kontroly môžete vytvoriť/upraviť v dialógovom okne ***Plán kontroly***, ktoré zobrazíte tlačidlom ***Správa plánu kontroly*** v okne Možnosti kontroly. V dialógovom okne ***Plán kontroly*** môžete zobraziť prehľad všetkých naplánovaných kontrol:

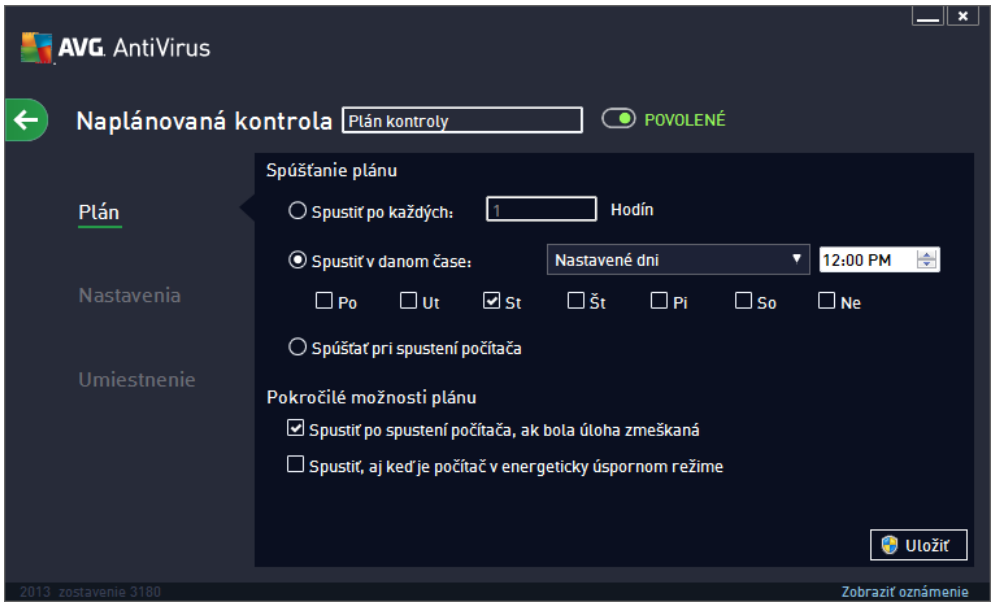


Než zadefinujete vlastné kontroly, zobrazí sa v tabuľke iba jeden plán kontroly, ktorý vopred definoval dodávateľ softvéru. Táto kontrola je štandardne vypnutá. Ak ju chcete zapnúť, kliknite na ňu pravým tlačidlom a v kontextovej ponuke vyberte možnosť ***Povoliť úlohu***. Po povolení plánu kontroly môžete upraviť jej konfiguráciu tlačidlom ***Upraviť plán kontroly***. Taktiež môžete kliknúť na tlačidlo ***Pridať plán kontroly***, aby ste vytvorili nový plán. Parametre plánu kontroly sa dajú upraviť (*alebo sa dá nastaviť nový plán*) v troch kartách:

- Plán
- Nastavenia
- Umiestnenie

Na každej záložke stačí prepnúť tlačidlo „semaforu“ , čím dočasne vypnete plánované kontroly a v prípade potreby ich znovu zapnete:

10.4.1. Plán



V hornej časti záložky ***Plán*** sa nachádza textové pole, do ktorého môžete zadať názov modulu kontroly, ktorý sa aktuálne definuje. Pokúste sa použiť stručné, opisné a výstižné názvy pre kontroly, aby sa dali neskôr ľahšie navzájom odlíšiť. Príklad: Nie je vhodné nazývať kontrolu "Nová kontrola" alebo "Moja kontrola", pretože tieto názvy sa nevzťahujú na to, čo kontrola vlastne preveruje. Na druhej strane, príkladom dobrého opisného názvu je „Kontrola systémových oblastí“ a pod.

Toto dialógové okno umožňuje ďalej definovať tieto parametre kontroly:

- ***Spustená kontrola*** – Tu môžete nastaviť časové intervaly pre novonaplánované spustenie kontroly. Čas spúšťania sa definuje ako opakované spúšťanie kontroly po uplynutí určitého času (*Spustiť po každých ...*), definovaním presného dátumu a času (*Spúšťať v konkrétnom časovom intervale ...*), prípadne definovaním udalosti, s ktorou sa bude spájať spustenie kontroly (*Spustiť pri spustení počítača)*.

- ***Možnosti pokročilého plánu*** – Táto časť vám umožňuje zadefinovať, za akých podmienok by sa kontrola mala/nemala spustiť, ak je počítač v úspornom režime alebo celkom vypnutý. Keď sa spustí plán kontroly v zadanom čase, o tejto skutočnosti budete informovaní pomocou kontextového okna, ktoré sa otvorí nad ikonou AVG v paneli úloh. Potom sa zobrazí nová ikona AVG v paneli úloh (farebná s blikajúcim svetlom), ktorá informuje o tom, že prebieha naplánovaná kontrola. Kliknutím pravým tlačidlom myši na ikonu AVG prebiehajúcej kontroly otvorte kontextovú ponuku, ktorá vám umožní pozastaviť alebo dokonca úplne zastaviť prebiehajúcu kontrolu a zároveň zmeniť prioritu práve spustenej kontroly.

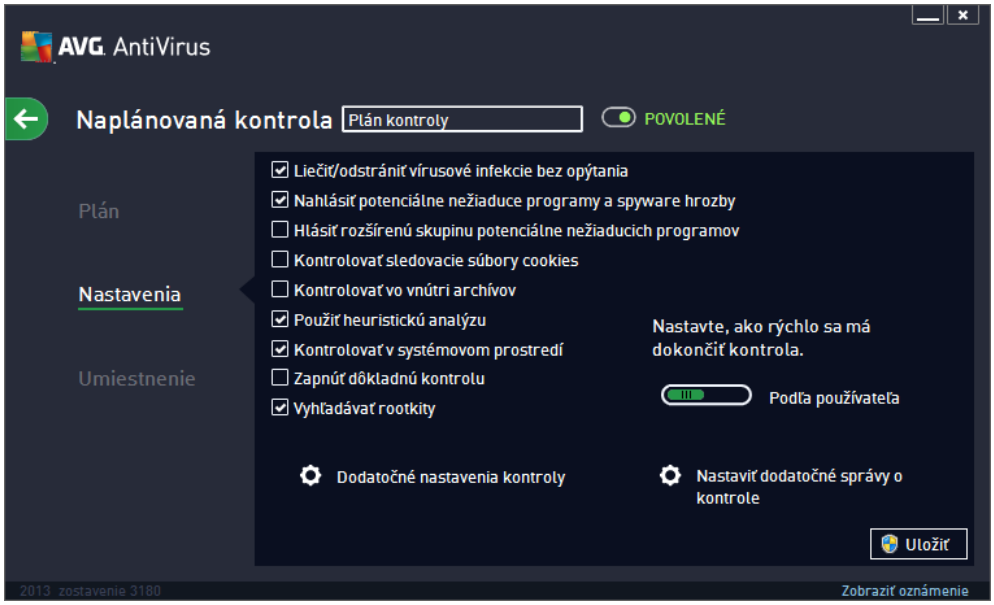
Ovládacie prvky dialógového okna

- ***Uložiť*** – Uloží všetky zmeny, ktoré ste vykonali v tejto karte alebo v inej karte tohto dialógového okna a prepne naspäť do prehľadu Naplánovaných kontrol. Preto, ak chcete konfigurovať parametre testu vo všetkých kartách, stlačte toto tlačidlo pre uloženie

parametrov až po zadaní všetkých svojich požiadaviek.

- – Zelenou šípkou v ľavej hornej časti okna sa dostanete naspäť do prehľadu Naplánovaných kontrol.

10.4.2. Nastavenia



V hornej časti záložky ***Nastavenia*** sa nachádza textové pole, do ktorého môžete zadať názov modulu kontroly, ktorý sa aktuálne definuje. Pokúste sa použiť stručné, opisné a výstižné názvy pre kontroly, aby sa dali neskôr ľahšie navzájom odlíšiť. Príklad: Nie je vhodné nazývať kontrolu "Nová kontrola" alebo "Moja kontrola", pretože tieto názvy sa nevzťahujú na to, čo kontrola vlastne preveruje. Na druhej strane, príkladom dobrého opisného názvu je „Kontrola systémových oblastí“ a pod.

V karte ***Nastavenia*** nájdete zoznam parametrov kontrolovania, ktoré sa dajú voliteľne zapnúť/ vypnúť. ***Ak nemáte závažný dôvod meniť tieto nastavenia, odporúčame vám ponechať vopred definovanú konfiguráciu***:

- ***Liečiť/odstrániť vírusovú infekciu bez opýtania*** *(štandardne zapnuté):* ak sa počas kontroly nájde vírus, môže byť automaticky vyliečený, pokiaľ je liek k dispozícii. Ak nie je možné infikovaný súbor vyliečiť automaticky, premiestni sa do Vírusového trezora.

- ***Nahlásiť potenciálne nežiaduce programy a spyware hrozby*** *(štandardne zapnuté):* Začiarknite toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu škodlivého softvéru: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.

- ***Hlásiť rozšírenú skupinu potenciálne nežiaducich programov*** (*štandardne vypnuté*): Začiarknite toto políčko, ak sa má detegovať rozšírená skupina spywaru: programov, ktoré sú úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň

zabezpečenia počítača, ale môže blokovať dobré programy, a preto je táto funkcia štandardne vypnutá.

- ***Kontrolovať sledovacie súbory cookies*** (*štandardne vypnuté*): Tento parameter súčasti zapína funkciu na detekciu súborov cookies počas prehľadávania; (*HTTP cookies sa používajú na overenie totožnosti, sledovanie a správu konkrétnych informácií o používateľoch, akými sú napr. preferencie stránok alebo obsah elektronických nákupných košíkov*).

- ***Kontrolovať vo vnútri archívov*** (*štandardne vypnuté*): tento parameter určuje, že sa majú počas kontroly preverovať všetky súbory, aj keď sú uložené vo vnútri archívu, napr. ZIP, RAR, ...

- ***Použiť heuristickú analýzu*** (*štandardne zapnuté*): heuristická analýza (*dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí*) bude jedna z metód, ktoré sa použijú na detekciu vírusov počas kontroly.

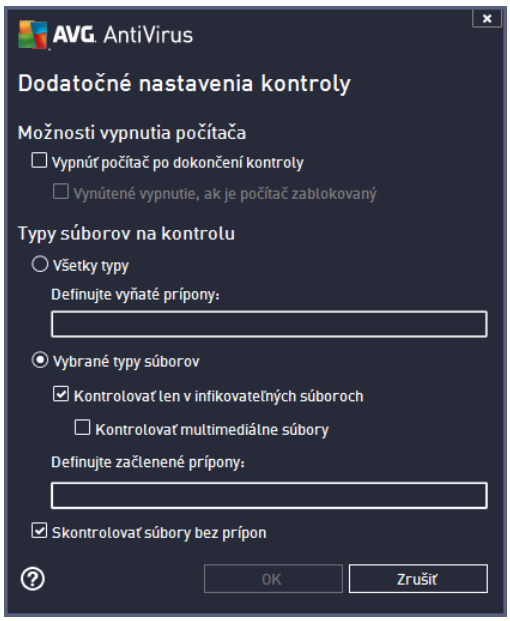
- ***Kontrolovať v systémovom prostredí*** (*štandardne zapnuté*): počas kontroly sa budú overovať aj systémové oblasti počítača.

- ***Zapnúť dôkladnú kontrolu*** (*štandardne vypnuté):* v určitých situáciách (*podozrenie na infikovanie počítača*) môžete touto možnosťou aktivovať najdôkladnejšie kontrolné algoritmy, ktoré pre istotu skontrolujú aj tie oblasti počítača, ktoré sa obyčajne vôbec neinfikujú. Upozorňujeme však, že tento spôsob je náročný na čas.

- ***Kontrolovať rootkity*** *(štandardne zapnuté):* Kontrola súčasťou Anti-Rootkit skontroluje počítač a zisťuje prítomnosť potenciálnych rootkitov, t. j. programov a technológií, ktoré dokážu zakryť činnosť škodlivého programu v počítači. Keď program deteguje rootkit, nemusí to nevyhnutne znamenať, že je počítač infikovaný. V niektorých prípadoch sa môžu určité ovládače alebo časti bežných aplikácií nesprávne označiť ako rootkity.

Ďalšie nastavenia kontroly

Odkaz otvorí nové dialógové okno ***Dodatočné nastavenia kontroly***, ktoré sa používa na nastavenie nasledujúcich parametrov:



- ***Možnosti vypnutia počítača*** – Rozhodnite, či sa má počítač vypnúť automaticky po dokončení procesu kontroly. Po potvrdení tejto možnosti *(Vypnúť počítač po dokončení kontroly)* sa aktivuje nová možnosť, ktorá umožní vypnúť počítač, aj keď je momentálne zablokovaný (*Vynútené vypnutie, ak je počítač zablokovaný)*.

- ***Typy súborov na kontrolu*** – Mali by ste tiež určiť, čo chcete kontrolovať:

    - ***Všetky typy súborov*** s možnosťou definovať výnimky z kontroly vytvorením zoznamu čiarkou oddelených prípon súborov, ktoré sa nemajú kontrolovať.

    - ***Vybrané typy súborov*** – Môžete nastaviť, aby sa kontrolovali len súbory, pri ktorých existuje pravdepodobnosť infikovania *(súbory, ktoré nemôžu byť napadnuté infekciou, napríklad niektoré jednoduché textové súbory alebo niektoré nespustiteľné súbory)* vrátane mediálnych súborov *(video, audio súborov – ak necháte toto políčko nezačiarknuté, potom sa čas kontroly skráti ešte viac, pretože tieto súbory sú často veľmi veľké, pričom pravdepodobnosť napadnutia vírusom je veľmi malá)*. Znova môžete definovať, podľa prípony, ktoré súbory sa majú kontrolovať vždy.

    - Alternatívne môžete rozhodnúť, že chcete ***kontrolovať súbory bez prípony***. Táto možnosť je štandardne zapnutá a odporúčame vám, aby ste toto nastavenie nikdy nemenili, ak na to nemáte skutočný dôvod. Súbory bez prípony sú skôr podozrivé a mali by sa vždy kontrolovať.

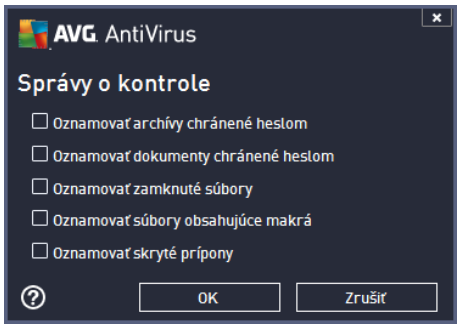
Nastaviť rýchlosť dokončenia kontroly

V tejto časti môžete ďalej špecifikovať želanú rýchlosť kontroly v závislosti od využívania systémových zdrojov. V predvolenom nastavení je úroveň automatického využívania zdrojov nastavená *Podľa používateľa*. Ak chcete, aby kontrola prebiehala rýchlejšie, potom bude trvať kratšie, ale výrazne sa zvýši využívanie systémových zdrojov a spomalia sa ostatné činnosti v počítači (*táto funkcia sa používa, keď je počítač zapnutý, ale nikto na ňom v danom momente*

nepracuje). Na druhej strane môžete znížiť využívanie systémových zdrojov predĺžením doby trvania kontroly.

Vytvoriť ďalšie správy o kontrole

Kliknutím na odkaz ***Vytvoriť ďalšie správy o kontrole...*** otvorte samostatné dialógové okno s názvom ***Správy o kontrole***, v ktorom môžete začiarknutím konkrétnych položiek definovať, ktoré nálezy sa majú hlásiť:

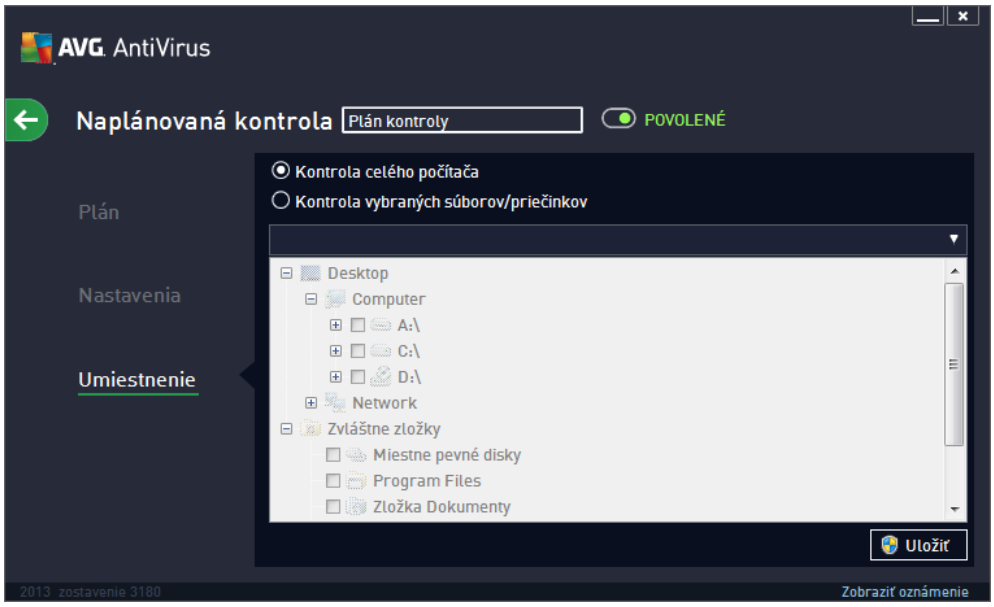


Ovládacie prvky dialógového okna

- ***Uložiť*** – Uloží všetky zmeny, ktoré ste vykonali v tejto karte alebo v inej karte tohto dialógového okna a prepne naspäť do prehľadu Naplánovaných kontrol. Preto, ak chcete konfigurovať parametre testu vo všetkých kartách, stlačte toto tlačidlo pre uloženie parametrov až po zadaní všetkých svojich požiadaviek.

- – Zelenou šípkou v ľavej hornej časti okna sa dostanete naspäť do prehľadu Naplánovaných kontrol.

10.4.3. Umiestnenie



Na karte ***Umiestnenie*** môžete nastaviť, či chcete naplánovať kontrolu celého počítača alebo kontrolu súborov/priečinkov. Keď vyberiete kontrolu súborov/priečinkov, potom sa v spodnej časti tohto dialógového okna aktivuje zobrazená stromová štruktúra, v ktorej môžete nastaviť priečinky, ktoré sa majú kontrolovať (*rozbaľte položky kliknutím na uzol so znakom plus a vyhľadajte priečinok, ktorý chcete kontrolovať*). Začiarknutím príslušných políčok môžete vybrať naraz niekoľko priečinkov. Vybrané priečinky sa zobrazia v textovom poli v hornej časti dialógového okna a do kontextovej ponuky sa uloží história vami vybraných kontrol na neskoršie účely. Úplnú cestu k požadovanému priečinku môžete zadať aj ručne (*ak zadáte viac ciest, musíte ich oddeliť bodkočiarkou bez medzier*).

V stromovej štruktúre môžete zároveň vyhľadať vetvu s názvom ***Špeciálne umiestnenia***. Nasleduje zoznam umiestnení, ktoré sa skontrolujú po označení príslušného začiarkavacieho políčka:

- ***Pevné disky počítača*** – všetky pevné disky počítača
- ***Programové súbory***
    - C:\Program Files\
    - *v 64-bitovej verzii* C:\Program Files (x86)
- ***Priečinok Moje dokumenty***
    - *vo Win XP:* C:\Documents and Settings\Default User\Moje dokumenty\
    - *vo Windows Vista/7*: C:\Users\používateľ\Dokumenty\
- ***Zdieľané dokumenty***
    - *vo Win XP*: C:\Documents and Settings\All Users\Dokumenty\

- *vo Windows Vista/7*: C:\Users\Public\Dokumenty\

- ***Adresár Windows*** – C:\Windows\

- ***Iné***

  - *Systémový disk* – pevný disk, na ktorom je nainštalovaný operačný systém (zvyčajne C:).

  - *Systémový priečinok* – C:\Windows\System32\

  - *Priečinok Temporary Files* – C:\Documents and Settings\User\Local\ (*Windows XP*) alebo C:\Users\používateľ\AppData\Local\Temp\ (*Windows Vista/7*)

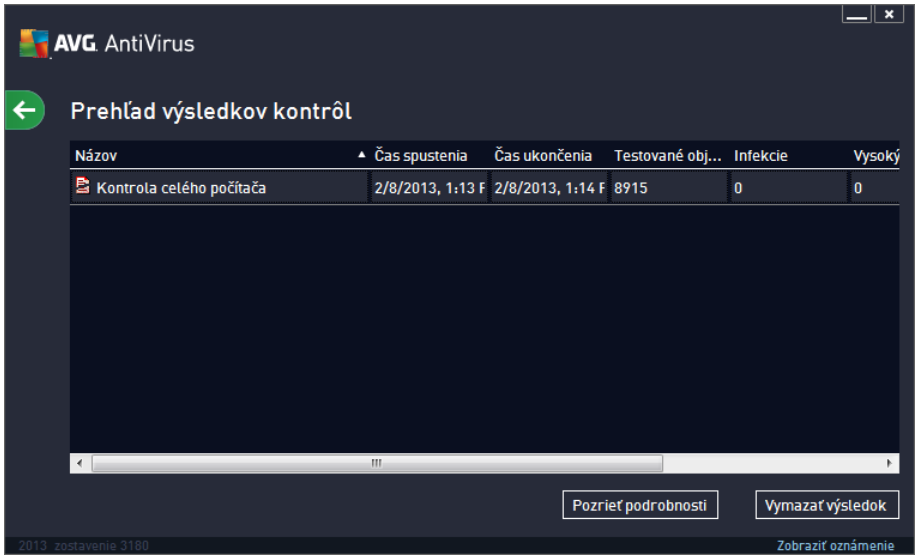
  - *Temporary Internet Files* – C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (*Windows XP*) alebo C: \Users\používateľ\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

Ovládacie prvky dialógového okna

- ***Uložiť*** – Uloží všetky zmeny, ktoré ste vykonali v tejto karte alebo v inej karte tohto dialógového okna a prepne naspäť do prehľadu Naplánovaných kontrol. Preto, ak chcete konfigurovať parametre testu vo všetkých kartách, stlačte toto tlačidlo pre uloženie parametrov až po zadaní všetkých svojich požiadaviek.

- – Zelenou šípkou v ľavej hornej časti okna sa dostanete naspäť do prehľadu Naplánovaných kontrol.

10.5. Výsledky kontrol



Dialógové okno ***Prehľad výsledkov kontrol*** obsahuje zoznam výsledkov všetkých doterajších

kontrol. Tabuľka obsahuje pre každý výsledok kontroly tieto údaje:

- ***Ikona*** – V prvom riadku je ikona popisujúca stav kontroly:
  - Nenašla sa žiadna infekcia, kontrola sa dokončila.
  - Nenašla sa žiadna infekcia, kontrola sa prerušila pred dokončením.
  - Našli sa infekcie, ktoré sa nevyliečili, kontrola sa dokončila.
  - Boli nájdené infekcie, ktoré neboli vyliečené, kontrola sa prerušila pred dokončením.
  - Našli sa infekcie a všetky sa vyliečili alebo odstránili, kontrola sa dokončila.
  - Boli nájdené infekcie a všetky boli vyliečené alebo odstránené, kontrola sa prerušila pred dokončením.
- ***Názov*** – V stĺpci sa nachádza názov príslušnej kontroly. Buď je to jedna z dvoch vopred definovaných kontrol alebo váš vlastný plán kontroly.
- ***Čas spustenia*** – Presný dátum a čas, kedy bola kontrola spustená.
- ***Čas ukončenia*** – Uvádza presný dátum a čas ukončenia, pozastavenia alebo prerušenia kontroly.
- ***Testované objekty*** – Uvádza celkový počet skontrolovaných objektov.
- ***Infekcie*** – Uvádza počet odstránených/celkových nájdených infekcií.
- ***Vysoká/Stredná/Nízka*** – V troch ďalších stĺpcoch je uvedený počet infekcií s vysokou, strednou a nízkou závažnosťou.
- ***Rootkity*** – Uvádza celkový počet rootkitov nájdených počas kontroly.

Ovládacie prvky dialógového okna

Pozrieť podrobnosti – Kliknutím na tlačidlo zobrazíte podrobné informácie o vybranej kontrole *(označenej v tabuľke vyššie)*.

Vymazať výsledky – Kliknutím na tlačidlo odstránite údaje o vybranom výsledku kontroly z tabuľky.

– Pomocou zelenej šípky v ľavej hornej časti dialógového okna sa vrátite naspäť do hlavného používateľského rozhrania s prehľadom súčastí.

10.6. Podrobnosti výsledkov kontrol

Ak chcete otvoriť prehľad s podrobnosťami o vybranom výsledku kontroly, kliknite na tlačidlo ***Pozrieť podrobnosti*** v dialógovom okne Prehľad výsledkov kontrol. Budete presmerovaní na rovnaké rozhranie dialógového okna s podrobnými informáciami o príslušných výsledkoch kontroly. Informácie sú rozdelené na tri záložky:

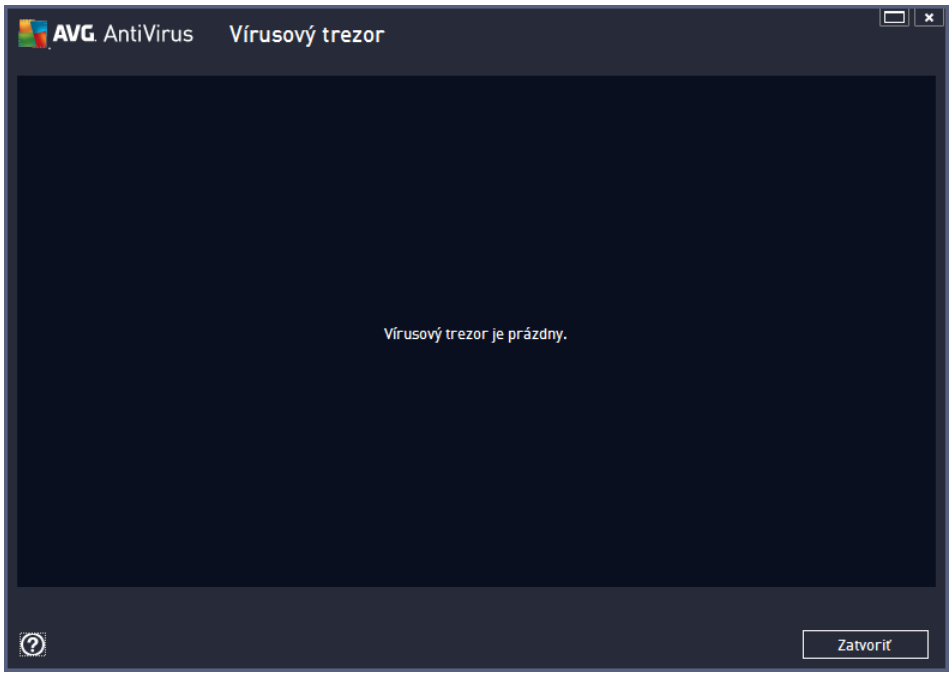
- ***Súhrn*** – Táto záložka obsahuje základné informácie o kontrole: či bola úspešne dokončená, aké hrozby sa našli a čo sa s nimi spravilo.
- ***Podrobnosti*** – táto záložka zobrazuje všetky údaje o kontrole vrátane podrobností o akýchkoľvek detegovaných hrozbách. Exportovať prehľad do súboru umožňuje uložiť výsledky kontroly do súboru s príponou .csv.
- ***Detekcie*** – táto stránka je zobrazená len v prípade, že boli počas kontroly detegované nejaké hrozby, a uvádza podrobné informácie o týchto hrozbách:

  Nízka závažnosť: informácie alebo varovania, nie skutočné hrozby. Obvykle dokumenty obsahujúce makrá, dokumenty alebo archívy chránené heslom, uzamknuté súbory, atď.

  Stredná závažnosť: obvykle PNP *(potenciálne nežiaduce programy, ako napríklad adware*) alebo sledujúce súbory cookie.

  Vysoká závažnosť: závažné hrozby, ako napríklad vírusy, trójske kone, exploity, atď. Taktiež objekty detegované heuristickou metódou detekcie, teda hrozby, ktoré ešte nie sú popísané vo vírusovej databáze.

11. Vírusový trezor



Vírusový trezor je bezpečné prostredie na správu podozrivých a infikovaných objektov detegovaných počas testov vykonaných programom AVG. Ak sa počas kontroly deteguje podozrivý objekt a aplikácia AVG ho nedokáže automaticky vyliečiť, program sa vás opýta, čo sa má s podozrivým objektom urobiť. Odporúčame vám, aby ste premiestnili objekt do ***Vírusového trezora*** pre prípad, ak by ste ho chceli použiť v budúcnosti. Hlavným účelom ***Vírusového trezora*** je uchovať všetky vymazané súbory počas určitej doby, aby ste mali čas uistiť sa, že súbor naozaj nepotrebujete. Ak zistíte, že odstránenie súboru spôsobuje problémy, môžete ho poslať na analýzu alebo obnoviť do pôvodného umiestnenia.

Rozhranie ***Vírusový trezor*** sa otvorí v samostatnom okne a poskytuje prehľad informácií o infikovaných objektoch v karanténe:

- ***Dátum uloženia*** – dátum a čas, kedy bol podozrivý súbor detegovaný a presunutý do Vírusového trezora.
- ***Úroveň závažnosti*** – ak sa rozhodnete nainštalovať súčasť Identita do programu **AVG AntiVirus 2013**, potom sa v tejto časti bude nachádzať grafické znázornenie úrovne závažnosti zisteného nálezu na stupnici so štyrmi úrovňami, od vyhovujúcej *(tri zelené bodky)* až po veľmi nebezpečnú *(tri červené bodky)*; a informácie o type infekcie (*na základe úrovne infikovateľnosti – všetky uvedené objekty môžu byť pozitívne alebo potenciálne infikované*).
- ***Názov detekcie*** – uvádza názov detegovanej infekcie podľa online vírusovej encyklopédie.
- ***Zdroj*** – uvádza, ktorá súčasť **AVG AntiVirus 2013** zistila príslušnú hrozbu.
- ***Správy*** – veľmi výnimočne môžu byť v tomto stĺpci uvedené podrobné komentáre týkajúce sa príslušnej zistenej hrozby.

Ovládacie tlačidlá

V rozhraní ***Vírusového trezora*** sa nachádzajú tieto ovládacie tlačidlá:

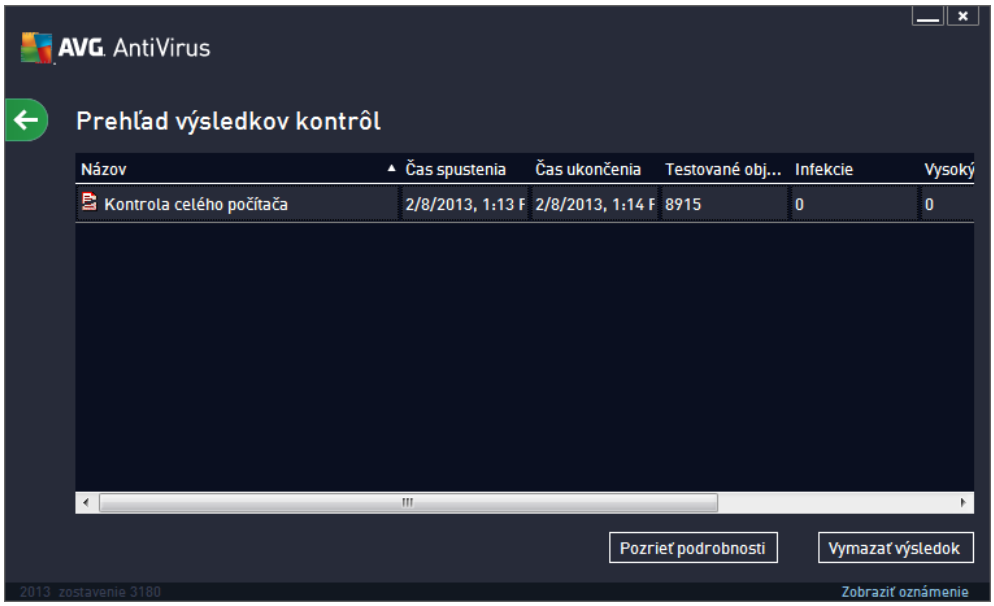
- ***Obnoviť*** – premiestni infikovaný súbor naspäť na jeho pôvodné umiestnenie na vašom disku.
- ***Obnoviť ako*** – premiestni infikovaný súbor do vybraného priečinka.
- ***Podrobnosti*** – Ak chcete zobraziť podrobné informácie o konkrétnej hrozbe vloženej do karantény ***Vírusového trezora*** , označte vybranú položku v zozname a kliknutím na tlačidlo ***Podrobnosti*** otvoríte nové dialógové okno s popisom zistenej hrozby.
- ***Vymazať*** – dokonale a nenávratne odstráni infikovaný súbor z ***Vírusového trezora***.
- ***Vyprázdniť trezor*** – dokonale vymaže celý obsah ***Vírusového trezora***. Odstránením z ***Vírusového trezora*** sa súbory úplne a nenávratne odstránia z disku (*nepremiestnia sa do Koša*).

12. História

Časť ***História*** obsahuje údaje o všetkých udalostiach v minulosti *(ako sú aktualizácie, kontroly, detekcie a pod.)* a hlásenia o týchto udalostiach. K tejto časti sa dostanete z používateľského rozhrania hlavnej obrazovky cez položku ***Možnosti/História***. Všetky udalosti zaznamenané v časti História sú rozdelené do týchto častí:

- Výsledky kontrol
- Nálezy súčasti Rezidentný štít
- Nálezy súčasti Ochrana e-mailu
- Nálezy súčasti Webový štít
- Protokol histórie udalostí

12.1. Výsledky kontrol



Dialógové okno ***Prehľad výsledkov kontrol*** sa nachádza v ponuke ***Možnosti/História/Výsledky kontrol*** v hornom navigačnom pruhu hlavného okna programu **AVG AntiVirus 2013**. V dialógovom okne sa nachádza zoznam všetkých doposiaľ spustených kontrol a informácie o ich výsledkoch:

- ***Názov***: Označenie kontroly; buď môže ísť o názov niektorého z vopred definovaných kontrol alebo o názov, ktorý ste priradili vlastnej naplánovanej kontrole. Každý názov obsahuje ikonu označujúcu výsledok kontroly:

  – zelená ikona informuje, že počas kontroly nebola detegovaná žiadna infekcia.

  – modrá ikona informuje, že počas kontroly bola detegovaná infekcia, ale infikovaný objekt bol automaticky odstránený.

– červená ikona upozorňuje, že počas kontroly bola detegovaná infekcia, ktorá sa nedala vymazať!

Každá ikona môže byť buď celá alebo rozdelená na polovicu; celá ikona predstavuje dokončené a správne ukončené kontroly; ikona rozdelená na polovicu predstavuje zrušené alebo prerušené kontroly.

Poznámka: *Podrobné informácie o každej kontrole sa nachádzajú v dialógovom okne Výsledky kontroly, ktoré sa otvára pomocou tlačidla Pozrieť podrobnosti (v spodnej časti tohto dialógového okna).*

- ***Čas spustenia***: Dátum a čas, kedy bola kontrola spustená.
- ***Čas skončenia***: Dátum a čas, kedy sa kontrola skončila.
- ***Testované objekty***: Počet objektov, ktoré sa skontrolovali počas kontroly.
- ***Infekcie***: počet detegovaných/odstránených vírusových infekcií
- ***Vysoká/Stredná/Nízka*** – V týchto stĺpcoch sa uvádza číslo odstránených/celkových infekcií nájdených pre každú z úrovní závažnosti (vysokú, strednú a nízku).
- ***Info*** – Informácie súvisiace s priebehom a výsledkami kontrolovania *(obyčajne s jeho dokončením alebo prerušením).*
- ***Rootkity*** – počet detegovaných rootkitov

Ovládacie tlačidlá

Ovládacie tlačidlá pre dialógové okno ***Prehľad výsledkov kontrol*** sú nasledovné:

- ***Pozrieť podrobnosti***: Stlačením tohto tlačidla sa otvorí dialógové okno Výsledky kontroly s podrobnými informáciami o zvolenej kontrole.
- ***Vymazať výsledky***: Stlačením tohto tlačidla sa zvolená položka odstráni z prehľadu výsledkov kontroly.
- – Ak chcete prepnúť naspäť na predvolené hlavné dialógové okno AVG *(prehľad súčastí),* použite šípku v ľavom hornom rohu tohto dialógového okna

12.2. Nálezy súčasti Rezidentný štít

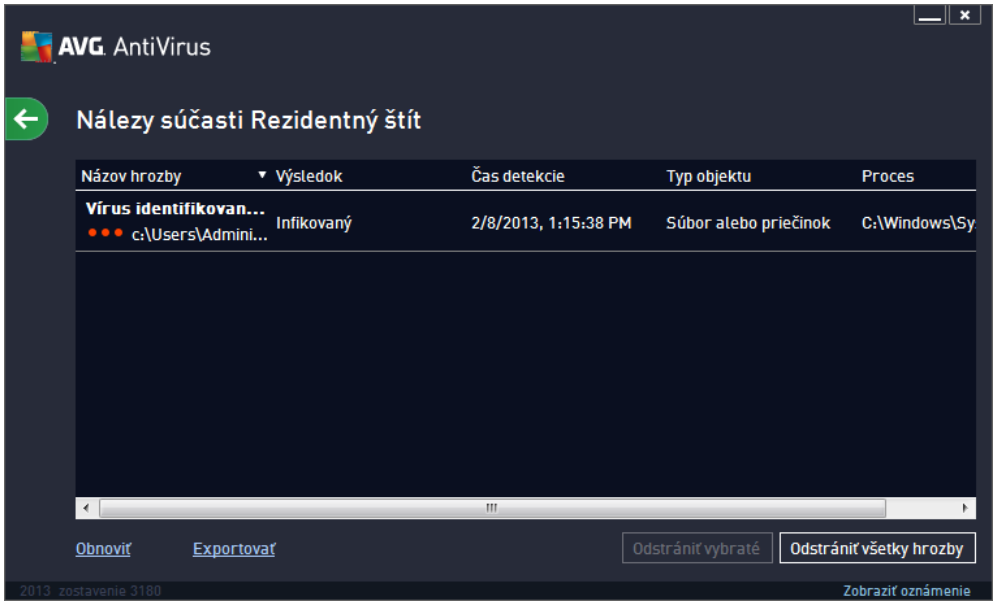
Služba ***Rezidentný štít*** je časťou súčasti ***Počítač*** a kontroluje súbory, ktoré sa práve kopírujú, otvárajú alebo ukladajú. Pri detegovaní vírusu alebo akéhokoľvek druhu hrozby vás program ihneď upozorní zobrazením tohto dialógového okna:

V tomto dialógovom okne s upozornením sa nachádzajú informácie o zistenom objekte, ktorý sa považuje za infikovaný (*Názov*), a kratší popis rozpoznanej infekcie (*Popis*). Odkaz Zobraziť podrobnosti vás presmeruje na on-line vírusovú encyklopédiu, kde nájdete podrobné informácie o zistenej infekcii, pokiaľ sú známe. V tomto okne sa nachádza aj prehľad dostupných riešení zistenej hrozby. Jedna z možností bude označená ako odporúčaná: ***Chrániť ma (odporúča sa). Ak je to možné, vždy by ste mali ponechať túto možnosť.***

Poznámka: *Môže sa stať, že veľkosť detegovaného objektu prekročí veľkosť voľného miesta vo Vírusovom trezore. V tom prípade sa zobrazí upozornenie informujúce o probléme v súvislosti s premiestňovaním infikovaného objektu do Vírusového trezora. Veľkosť Vírusového trezora však môžete zmeniť. Je definovaná ako nastaviteľné percento skutočnej veľkosti vášho pevného disku. Na zväčšenie veľkosti Vírusového trezora otvorte dialógové okno Vírusový trezor v časti Rozšírené nastavenia programu AVG kliknutím na možnosť „Obmedziť veľkosť Vírusového trezora“.*

V dolnej časti dialógového okna sa nachádza odkaz ***Zobraziť podrobnosti***. Kliknutím naň otvoríte nové okno s podrobnosťami o procese, ktorý bol spustený pri zaznamenaní infekcie, a o identifikácii procesu.

Zoznam všetkých nálezov súčasti Rezidentný štít si môžete pozrieť v dialógovom okne ***Nálezy súčasti Rezidentný štít***. Toto dialógové okno sa nachádza pod položkou ponuky ***Možnosti/História/ Nálezy súčasti Rezidentný štít*** v hornom navigačnom pruhu hlavného okna aplikácie **AVG AntiVirus 2013. Toto okno obsahuje prehľad objektov detegovaných súčasťou Rezidentný štít vyhodnotených ako nebezpečné, ktoré boli buď vyliečené alebo premiestnené do** Vírusového trezora.



Pre každý detegovaný objekt sa zobrazia tieto informácie:

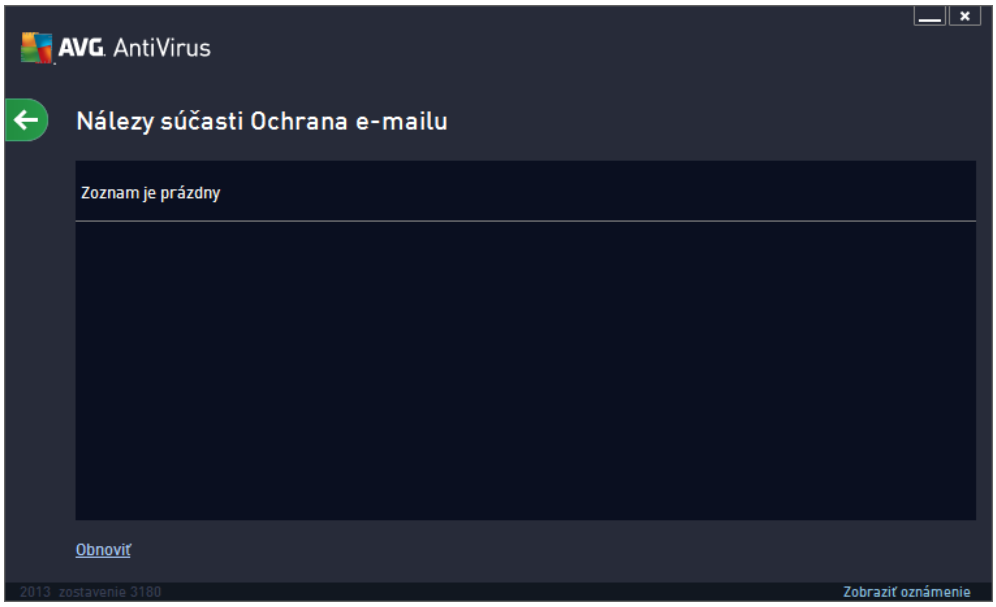
- ***Názov detekcie*** – popis (*prípadne aj názov*) zisteného objektu a jeho poloha
- ***Výsledok*** – akcia urobená na detegovanom objekte
- ***Čas detekcie*** – dátum a čas detegovania a zablokovania hrozby
- ***Typ objektu*** – typ detegovaného objektu
- ***Proces*** – Aká akcia sa vykonala na zavolanie potenciálne nebezpečného objektu, aby sa dal detegovať

Ovládacie tlačidlá

- ***Obnoviť*** – Aktualizuje sa zoznam nálezov zistených súčasťou ***Rezidentný štít***
- ***Exportovať*** – Exportuje celý zoznam zistených objektov do súboru
- ***Odstrániť vybrané*** – V zozname môžete označiť iba vybrané záznamy a týmto tlačidlom ich vymažete
- ***Odstrániť všetky hrozby*** – Týmto tlačidlom vymažete všetky záznamy v dialógovom okne.
- – Ak chcete prepnúť naspäť na predvolené hlavné dialógové okno AVG *(prehľad súčastí),* použite šípku v ľavom hornom rohu tohto dialógového okna

12.3. Nálezy súčasti Ochrana e-mailu

Dialógové okno ***Nálezy súčasti Ochrana e-mailu*** je dostupné prostredníctvom ponuky ***Možnosti/ História/Nálezy súčasti Ochrana e-mailu*** v hornom navigačnom pruhu hlavného okna programu **AVG AntiVirus 2013**.



Toto okno obsahuje zoznam všetkých detekcií súčasťou Ochrana e-mailu. Pre každý detegovaný objekt sa zobrazia tieto informácie:

- ***Názov detekcie*** – popis (*prípadne aj názov*) zisteného objektu a jeho zdroj
- ***Výsledok*** – akcia urobená na detegovanom objekte.
- ***Čas detekcie*** – dátum a čas detekcie podozrivého objektu.
- ***Typ objektu*** – typ detegovaného objektu.
- ***Proces*** – aká akcia sa vykonala na zavolanie potenciálne nebezpečného objektu, aby sa dal detegovať

V spodnej časti dialógového okna pod zoznamom nájdete informácie o celkovom počte detegovaných objektov. Môžete tiež exportovať celý zoznam detegovaných objektov do súboru (***Exportovať zoznam do súboru***) a vymazať všetky záznamy o detegovaných objektoch (***Vyprázdniť zoznam***).

Ovládacie tlačidlá

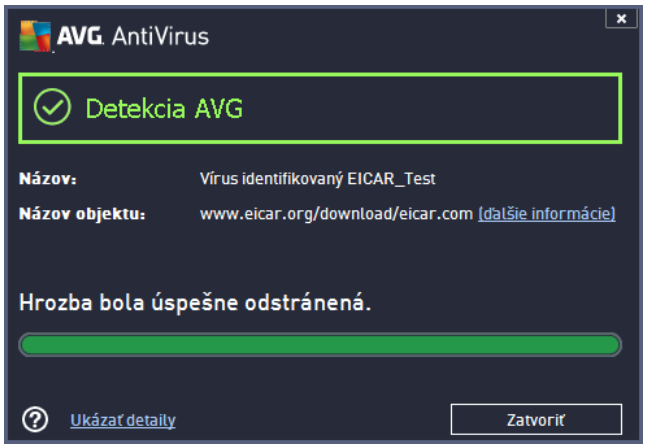
V rozhraní ***Nálezy súčasti Kontrola pošty*** sa nachádzajú nasledujúce tlačidlá:

- ***Obnoviť*** – Aktualizuje zoznam zistených hrozieb.

- – Ak chcete prepnúť naspäť na predvolené hlavné dialógové okno AVG *(prehľad súčastí),* použite šípku v ľavom hornom rohu tohto dialógového okna

12.4. Nálezy súčasti Webový štít

Webový štít kontroluje obsah navštívených internetových stránok a súborov, ktoré sa na nich môžu nachádzať, ešte predtým, než sa zobrazia v internetovom prehliadači alebo prevezmú do počítača. Pri detegovaní hrozby vás program ihneď upozorní otvorením tohto dialógového okna:

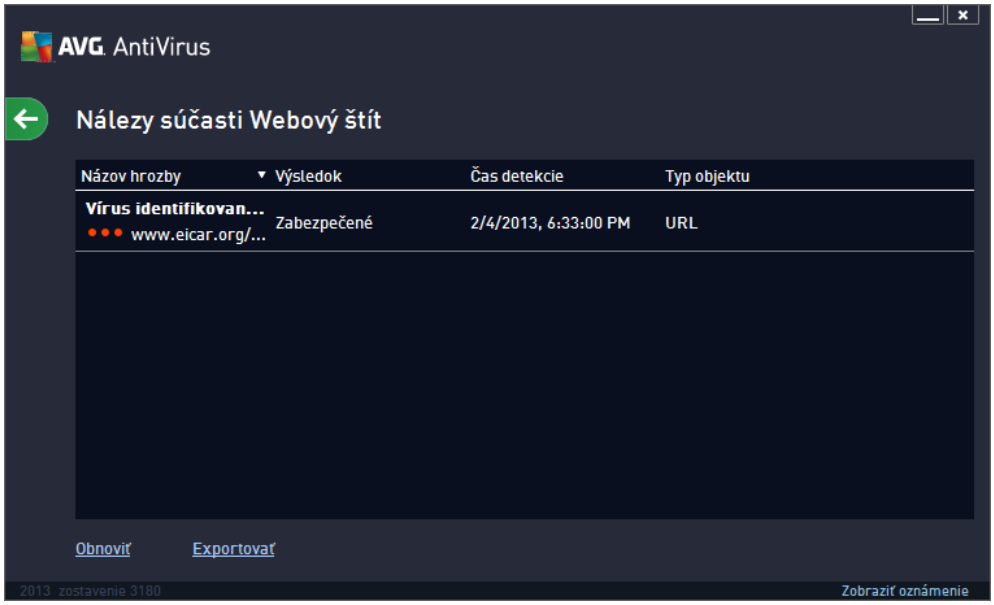


V tomto dialógovom okne s upozornením sa nachádzajú informácie o zistenom objekte, ktorý sa považuje za infikovaný (*Názov*), a kratší popis rozpoznanej infekcie (*Popis*). Odkaz Zobraziť podrobnosti vás presmeruje na on-line vírusovú encyklopédiu, kde nájdete podrobné informácie o zistenej infekcii, pokiaľ sú známe. V tomto dialógovom okne sa nachádzajú nasledujúce ovládacie prvky:

- ***Zobraziť podrobnosti*** – Kliknutím na odkaz otvoríte nové kontextové okno s informáciami o procese, ktorý bol spustený v čase detegovania infekcie, a o identifikácii procesu.

- ***Zatvoriť*** – Kliknutím na toto tlačidlo zatvorte dialógové okno s upozornením.

Podozrivá webová stránka sa neotvorí a detekcia hrozieb sa zapíše do zoznamu súčasti ***Nálezy súčasti Webový štít***. Tento prehľad zistených hrozieb sa nachádza pod položkou ponuky ***Možnosti/História/Nálezy súčasti Webový štít*** v hornom navigačnom pruhu hlavného okna aplikácie **AVG AntiVirus 2013**.



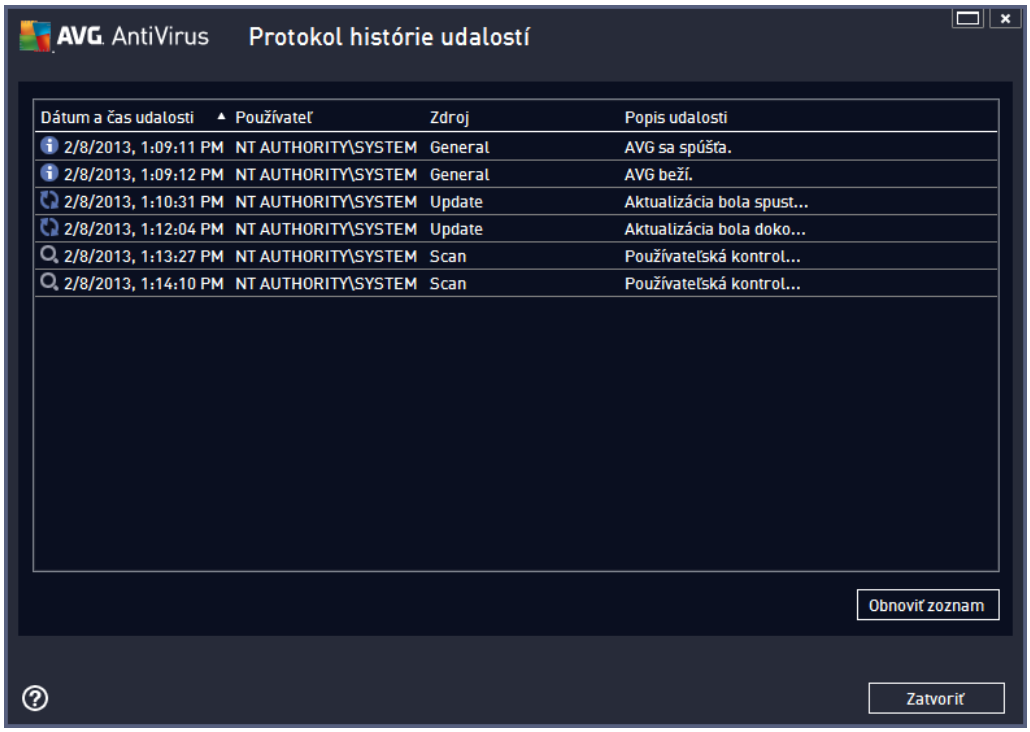
Pre každý detegovaný objekt sa zobrazia tieto informácie:

- ***Názov detekcie*** – popis (*prípadne aj názov*) zisteného objektu a jeho zdroja (*webovej stránky*)
- ***Výsledok*** – akcia urobená na detegovanom objekte
- ***Čas detekcie*** – dátum a čas detegovania a zablokovania hrozby
- ***Typ objektu*** – typ detegovaného objektu
- ***Proces*** – Aká akcia sa vykonala na zavolanie potenciálne nebezpečného objektu, aby sa dal detegovať

Ovládacie tlačidlá

- ***Obnoviť*** – Aktualizuje sa zoznam nálezov zistených súčasťou ***Rezidentný štít***
- ***Exportovať*** – Exportuje celý zoznam zistených objektov do súboru.
- – Ak chcete prepnúť naspäť na predvolené hlavné dialógové okno AVG *(prehľad súčastí),* použite šípku v ľavom hornom rohu tohto dialógového okna

12.5. Protokol histórie udalostí



Dialógové okno ***Protokol histórie udalostí*** sa nachádza v ponuke ***Možnosti/História/Protokol histórie udalostí*** v hornom navigačnom pruhu hlavného okna programu **AVG AntiVirus 2013**. V tomto dialógovom okne sa nachádza prehľad významných udalostí, ktoré sa vyskytli v čase, keď bol program **AVG AntiVirus 2013** spustený. Toto okno obsahuje záznamy týchto typov udalostí: i nformácie o aktualizáciách aplikácie AVG; informácie o spustení, ukončení alebo zastavení kontroly (*vrátane automaticky vykonávaných testov*); informácie o udalostiach týkajúcich sa detekcie vírusov (*či už Rezidentným štítom alebo kontrolou*) vrátane miesta výskytu; a ďalšie dôležité udalosti.

Každá udalosť má uvedené tieto informácie:

- ***Dátum a čas udalosti*** informuje o presnom dátume a čase výskytu udalosti.
- ***Používateľ*** určí názov aktuálne prihláseného používateľa v čase výskytu udalosti.
- ***Zdroj*** poskytne informácie o zdrojovej súčasti alebo inej časti systému AVG, ktorá pôvodne spustila udalosť.
- ***Popis udalosti*** obsahuje stručný prehľad o tom, čo sa v skutočnosti udialo.

Ovládacie tlačidlá

- ***Obnoviť zoznam*** – Stlačením tohto tlačidla aktualizujete všetky položky v zozname udalostí
- ***Zatvoriť*** – Stlačením tohto tlačidla sa vrátite do **AVG AntiVirus 2013** hlavného okna

13. Aktualizácie AVG

Žiadny bezpečnostný softvér nedokáže zaručiť skutočnú ochranu pred rôznymi typmi hrozieb, ak sa pravidelne neaktualizuje! Autori vírusov stále hľadajú nové trhliny, ktoré by mohli využiť, či už v softvéri alebo v operačných systémoch. Nové vírusy, nový malware a nové útoky hakerov sa objavujú denne. Z tohto dôvodu dodávatelia softvéru neustále vydávajú aktualizácie a bezpečnostné záplaty na opravu všetkých odhalených bezpečnostných dier.

Vzhľadom na všetky nové počítačové hrozby a rýchlosť, akou sa šíria, je mimoriadne dôležité pravidelne aktualizovať produkt **AVG AntiVirus 2013**. Najlepším riešením je ponechať predvolené nastavenia programu, v ktorých sú nastavené automatické aktualizácie. Nezabudnite, že bez aktuálnej vírusovej databázy programu **AVG AntiVirus 2013** nemôže program zistiť najnovšie hrozby!

Pravidelná aktualizácia programu AVG je nevyhnutná! Dôležité aktualizácie vírusových definícií by sa mali uskutočniť denne, ak to je možné. Menej naliehavé programové aktualizácie sa môžu uskutočniť raz za týždeň.

13.1. Spustenie aktualizácie

V záujme maximálneho využitia dostupného zabezpečenia je aplikácia **AVG AntiVirus 2013** predvolene nastavená tak, aby hľadala nové aktualizácie vírusovej databázy každé štyri hodiny. Keďže spoločnosť AVG nezverejňuje aktualizácie podľa pevného harmonogramu, ale podľa počtu a závažnosti nových hrozieb, je veľmi dôležité dbať na aktuálnosť vírusovej databázy AVG.

Ak chcete skontrolovať novú aktualizáciu okamžite, môžete tak urobiť pomocou rýchleho prepojenia Aktualizovať teraz v hlavnom používateľskom rozhraní. Toto prepojenie sa nachádza v každom dialógovom okne používateľského rozhrania. Keď spustíte aktualizáciu, AVG najskôr overí, či sú dostupné nové aktualizačné súbory. Ak program **AVG AntiVirus 2013** zistí prítomnosť nových aktualizačných súborov, začne ich preberať a spustí samotný proces aktualizácie. O výsledkoch aktualizácie budete informovaní v oznámení nad ikonou AVG v paneli úloh.

Ak chcete znížiť počet spustení aktualizácie, môžete tak urobiť pomocou vlastných parametrov spúšťania aktualizácie. ***Dôrazne sa však odporúča aktualizovať aspoň raz denne!*** Konfiguráciu môžete upraviť v časti Rozšírené nastavenia/plánovania, konkrétne v týchto dialógových oknách:

- Plán aktualizácie definícií
- Plán aktualizácie programu

13.2. Úrovne aktualizácie

Aplikácia **AVG AntiVirus 2013** ponúka na výber dve úrovne aktualizácie:

- ***Aktualizácia definícií*** obsahuje zmeny potrebné na dosiahnutie spoľahlivej ochrany pred vírusmi. Zvyčajne neobsahuje žiadne zmeny kódu a aktualizuje len databázu definícií. Táto aktualizácia by sa mala použiť čo možno najskôr.
- ***Aktualizácia programu*** – Obsahuje rôzne zmeny programu, doplnky a vylepšenia.

Pri plánovaní aktualizácie, si môžete určiť konkrétne parametre pre každú z úrovní aktualizácií:

- Plán aktualizácie definícií
- Plán aktualizácie programu

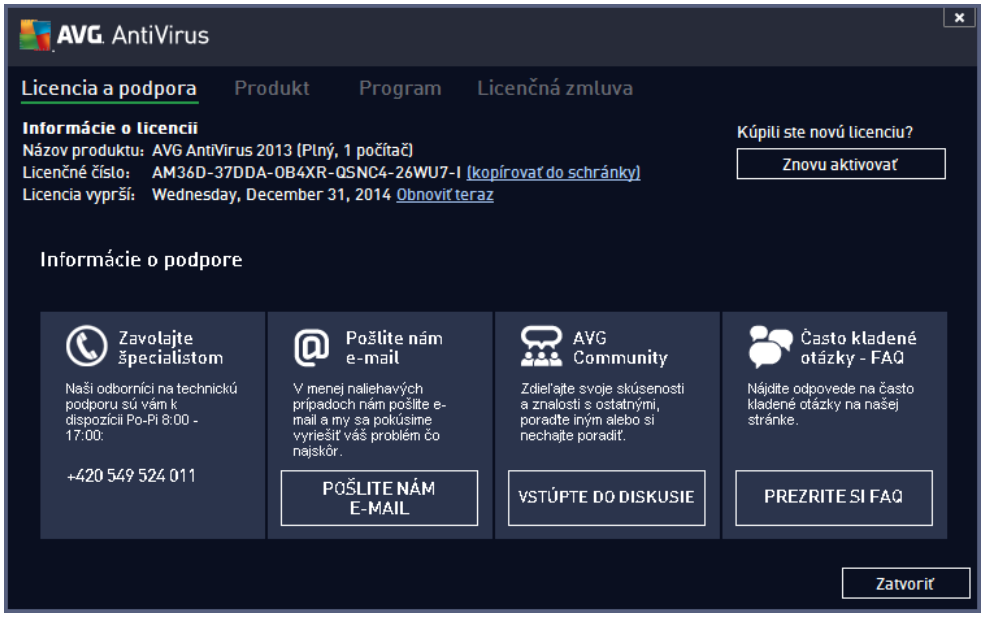
Poznámka: *Ak sa čas naplánovanej aktualizácie programu náhodou prekrýva s plánom kontroly, aktualizácia má vyššiu prioritu a kontrola sa preruší.*

14. FAQ a technická podpora

V prípade nákupných alebo technických problémov s aplikáciou **AVG AntiVirus 2013** existuje niekoľko spôsobov, ako nájsť pomoc. Vyberte si z týchto možností:

- ***Získajte podporu***: Priamo v aplikácii AVG sa môžete dostať na špeciálnu webovú lokalitu zákazníckej podpory AVG (http://www.avg.com/). V hlavnej ponuke vyberte možnosť ***Pomocník/Získajte podporu*** a ocitnete sa na webovej lokalite AVG s miestami podpory. Ak chcete pokračovať, postupujte podľa pokynov na webovej lokalite.

- ***Podpora*** *(odkaz v hlavnej ponuke)*: Ponuka aplikácie AVG (*v hornej časti hlavného používateľského rozhrania*) obsahuje prepojenie ***Podpora***, pomocou ktorého otvoríte nové dialógové okno so všetkými typmi údajov, ktoré môžete pri hľadaní pomoci potrebovať. Dialógové okno obsahuje základné údaje o nainštalovanom programe AVG (*verzia programu/databázy*), podrobnosti o licencii a zoznam rýchlych prepojení podpory:



- ***Riešenie problémov v súbore pomocníka***: Nová časť ***Riešenie problémov*** je k dispozícii priamo v súbore pomocníka v produkte **AVG AntiVirus 2013** *(súbor pomocníka otvoríte stlačením klávesu F1 v niektorom z dialógových okien aplikácie)*. V tejto časti nájdete zoznam najčastejších situácií, v ktorých používateľ potrebuje vyhľadať profesionálnu pomoc pre technický problém. Vyberte situáciu, ktorá najviac zodpovedá vášmu problému, a kliknutím zobrazte podrobné pokyny vedúce k riešeniu daného problému.

- ***Webové stredisko podpory AVG***: Riešenie problému môžete vyhľadať aj na webovej lokalite AVG (http://www.avg.com/). V časti ***Centrum pomoci*** nájdete štruktúrovaný prehľad tematických skupín týkajúcich sa nákupných a technických problémov.

- ***Časté otázky***: Na webovej lokalite AVG (http://www.avg.com/) môžete nájsť aj jednotlivé dôkladne rozčlenené časté otázky. K tejto časti sa dostanete prostredníctvom ponuky ***Centrum podpory/FAQ***. Všetky otázky sú opäť prehľadne rozdelené do kategórií podľa toho, či sa problém týka nákupu, vírusov alebo ide o technickú otázku.

- ***O vírusoch a hrozbách***: Vírusom je venovaná celá kapitola na webovej lokalite AVG (http://

www.avg.com/) *(na webovú stránku sa dostanete z hlavnej ponuky cez položky Pomocník/ O vírusoch a hrozbách)*. Výberom položky ***Centrum pomoci/O vírusoch a hrozbách*** v ponuke otvoríte stránku so štruktúrovaným prehľadom informácií o on-line hrozbách. Môžete tiež nájsť pokyny na odstraňovanie vírusov spyware a tipov na zachovanie ochrany.

- ***Diskusné fórum***: Môžete využiť aj diskusné fórum používateľov produktov AVG na adrese http://forums.avg.com.