



AVG AntiVirus 2014

Používateľská príručka

Revízia dokumentu 2014.21 (6/11/2014)

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 libzip2, 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	12
3.6 Priebeh inštalácie	13
3.7 Blahoželáme!	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	21
5.3 Prehľad súčastí	22
5.4 Moje aplikácie	23
5.5 Kontrola/Aktualizovať rýchle odkazy	24
5.6 Ikona v paneli úloh	24
5.7 AVG Advisor	26
5.8 AVG Akcelerátor	27
6. Súčasti AVG	28
6.1 Ochrana počítača	28
6.2 Ochrana prezerania webu	33
6.3 Identity Protection	34
6.4 Ochrana e-mailu	36
6.5 Súčasť Quick Tune	37

7. AVG Security Toolbar	40
8. AVG Do Not Track	43
8.1 Rozhranie aplikácie AVG Do Not Track.....	43
8.2 Informácie o sledovacích procesoch.....	45
8.3 Blokovanie sledovacích procesov.....	45
8.4 Nastavenia aplikácie AVG Do Not Track.....	46
9. Rozšírené nastavenia programu AVG	48
9.1 Vzhľad	48
9.2 Zvuky	50
9.3 Dočasne vypnúť ochranu AVG.....	51
9.4 Ochrana počítača.....	52
9.5 Kontrola pošty.....	57
9.6 Ochrana prezerania webu.....	67
9.7 Identity Protection.....	70
9.8 Kontroly.....	71
9.9 Plány	77
9.10 Aktualizácia.....	85
9.11 Výnimky.....	89
9.12 Vírusový trezor.....	91
9.13 AVG Sebaochrana.....	92
9.14 Preferencie ochrany osobných údajov.....	92
9.15 Ignorovať chybový stav.....	95
9.16 Aplikácia Advisor – známe siete.....	96
10. Kontrola programom AVG	97
10.1 Vopred definované kontroly.....	99
10.2 Kontrola z prieskumníka.....	108
10.3 Kontrola z príkazového riadka.....	108
10.4 Plánovanie kontroly.....	111
10.5 Výsledky kontrol.....	118
10.6 Podrobnosti výsledkov kontrol.....	120
11. AVG File Shredder	121
12. Vírusový trezor	122
13. História	124
13.1 Výsledky kontrol.....	124



13.2 Nálezy súčasti Rezidentný štít.....	125
13.3 Nálezy súčasti Identity Protection.....	128
13.4 Nálezy súčasti Ochrana e-mailu.....	129
13.5 Nálezy súčasti Webový štít.....	130
13.6 Protokol histórie udalostí.....	132
14. Aktualizácie AVG.....	133
14.1 Spustenie aktualizácie.....	133
14.2 Úrovne aktualizácie.....	133
15. FAQ a technická podpora.....	135



1. Úvod

Táto príručka podrobne dokumentuje produkt **AVG AntiVirus 2014**.

Produkt

Produkt **AVG AntiVirus 2014** 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, pričom vyhľadáva informácie s ochranou v reálnom čase.

Môžete využiť aj ďalšie zdroje informácií:

- **Súbor pomocníka** – časť *Riešenie problémov* je k dispozícii priamo v súbore pomocníka v produkte **AVG AntiVirus 2014** (súbor pomocníka otvoríte stlačením klávesu **F1** v akomkoľvek dialógovom okne aplikácie). V tejto časti nájdete zoznam najčastejších situácií, v ktorých používate potrebuje vyhľadať profesionálnu pomoc pre technický problém. Vyberte situáciu, ktorá najviac zodpovedá vášmu problému, a kliknutím zobrazíte podrobné pokyny vedúce k riešeniu daného problému.
- **Webové stredisko podpory AVG** – riešenie problému môžete vyhľadať 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 a návody**. Všetky otázky sú opäť prehľadne rozdelené do kategórií podľa toho, či sa problém týka nákupu, vírusov alebo ide o technickú otázku.
- **AVG ThreatLabs** – osobitná webová stránka spojená s programom AVG (<http://www.avgthreatlabs.com/website-safety-reports/>) venovaná problémom s vírusmi, ktorá poskytuje štruktúrovaný prehľad informácií súvisiacich s hrozbami on-line. Môžete tiež nájsť pokyny na odstránenie vírusov spyware a tipov na zachovanie ochrany.
- **Diskusné fórum** – môžete využiť aj diskusné fórum používateľov produktov AVG na adrese <http://forums.avg.com>.



2. Požiadavky na inštaláciu produktu AVG

2.1. Podporované operačné systémy

AVG AntiVirus 2014 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: Súčasťou [Identita](#) nepodporuje 64-bitové operačné systémy Windows XP. Produkt AVG AntiVirus 2014 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 2014**:

- 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 (*pre úspešnú inštaláciu*)

Odporované hardvérové požiadavky pre produkt **AVG AntiVirus 2014**:

- 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 (*pre úspešnú inštaláciu*)

3. Proces inštalácie produktu AVG

Na nainštalovanie programu **AVG AntiVirus 2014** do počítača sa musí použiť najnovší inštalovaný súbor. Aby ste sa uistili, že inštalujete najnovšiu verziu aplikácie **AVG AntiVirus 2014**, odporúčame vám prevziať inštalovaný súbor priamo z webovej lokality spoločnosti AVG (<http://www.avg.com/>). V sekcii **Centrum podpory/Na prevzatie** sa nachádza štruktúrovaný prehľad inštalovaných 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 prispôbených podľa vašich požiadaviek.

Po prevzatí a uložení inštalovateľného 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. Alebo ponúkame podrobné vysvetlenia každého z dialógových okien:

3.1. Vitajte! Výber jazyka

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

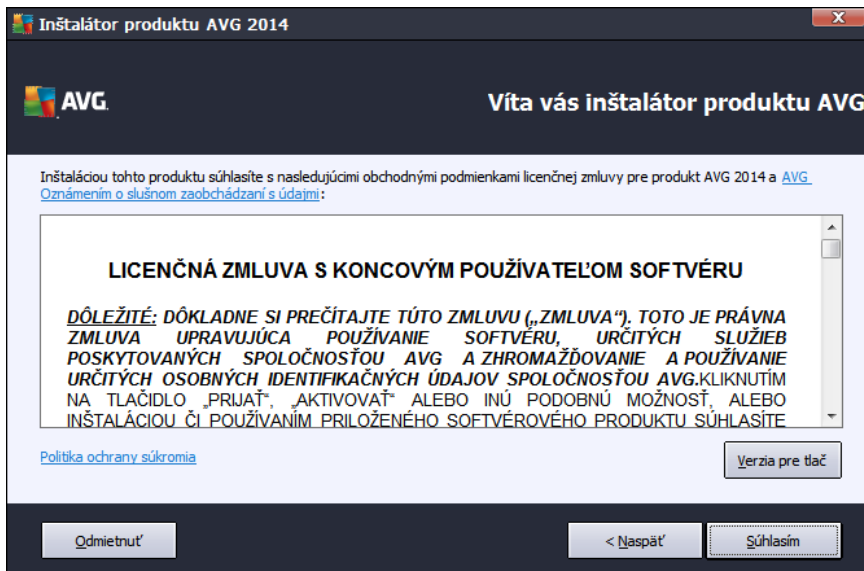


V tomto dialógovom okne zvolíte jazyk, ktorý sa použije pri procese inštalácie. Kliknutím na rozbaľovacie pole zobrazíte ponuku jazykov. Vyberte požadovaný jazyk a proces inštalácie sa posunie k výberu jazyka.

Pozor: Teraz vyberáte iba jazyk procesu inštalácie. Aplikácia AVG AntiVirus 2014 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 2014 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 licen nej zmluvy AVG:



Pozorne si celý text pre ítajte. Na potvrdenie, že ste si pre ítali a pochopili zmluvu a súhlasíte s jej znením stla te tla idlo **Súhlasím**. Ak nesúhlasíte s licen nou zmluvou, stla te tla idlo **Nesúhlasím** a proces inštalácie sa ihne ukon í.

Poznámka o férovom spracovaní a Ochrana osobných údajov v spoĽnosti AVG

Okrem licen nej zmluvy môžete v tomto dialógovom okne zisti í viac o **Poznámke o férovom spracovaní** a **Ochrane osobných údajov** v spoĽnosti AVG. Uvedené funkcie sú zobrazené v dialógovom okne ako aktívne hypertextové odkazy, ktoré vás presmerujú na webovú lokalitu, na ktorej sú uvedené podrobné informácie. Kliknutím na príslušný odkaz budete presmerovaní na webovú lokalitu AVG (<http://www.avg.com/>) kde nájdete plné znenie týchto vyjadrení.

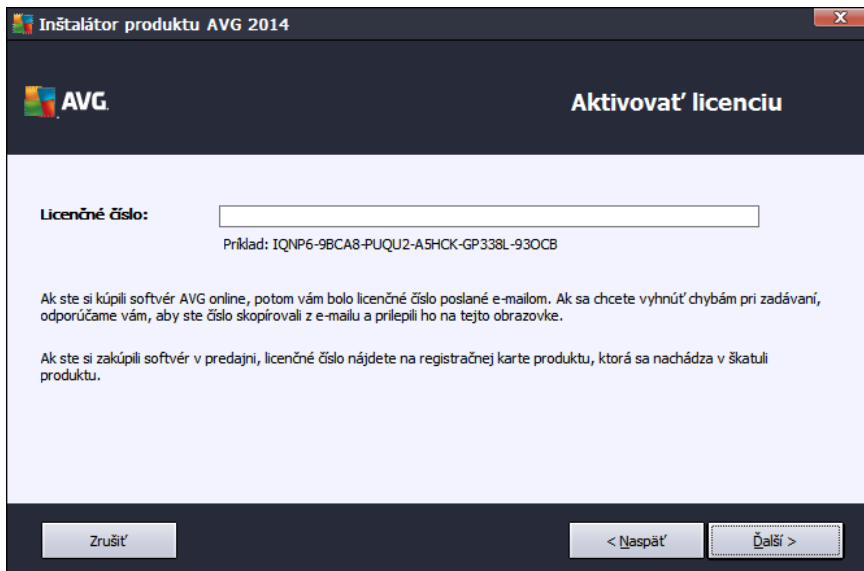
Ovládacie tla idlá

V prvom dialógovom okne inštalácie sa nachádzajú iba dve ovládacie tla idlá:

- **Verzia pre tlač** – kliknutím na toto tla idlo zobrazíte plné znenie licen nej zmluvy AVG ur ené tak pre zobrazenie na webe, ako aj upravené pre tlač .
- **Zamietnu** – kliknutím na toto tla idlo odmietnete podmienky licen nej zmluvy. Inštalácia ný postup sa okamžite ukon í. Aplikácia **AVG AntiVirus 2014** sa nenainštaluje!
- **Naspä** – kliknutím sa vrátite o jeden krok k predchádzajúcemu dialógovému oknu inštalácie.
- **Prija** – kliknutím na toto tla idlo potvrdíte, že ste pre ítali, pochopili a prijali podmienky licen nej zmluvy. Inštalácia bude pokrač ova a zobrazí sa alšie inštalácia né dialógové okno.

3.3. Aktivujte si licenciu

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



Inštalátor produktu AVG 2014

AVG. Aktivovať licenciu

Licenčné číslo:

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

Ak ste si kúpili softvér AVG online, potom vám bolo licenčné číslo poslané e-mailom. Ak sa chcete vyhnúť chybám pri zadávaní, odporúčame vám, aby ste číslo skopírovali z e-mailu a prilepili ho na tejto obrazovke.

Ak ste si zakúpili softvér v predajni, licenčné číslo nájdete na registračnej karte produktu, ktorá sa nachádza v škatuli produktu.

Zrušiť < Naspäť Ďalší >

Kde nájs licenčné číslo

Predajné číslo sa nachádza na obale disku CD v škatuli produktu **AVG AntiVirus 2014**. Licenčné číslo sa nachádza v e-mailovej správe s potvrdením, ktorú ste dostali po zakúpení produktu **AVG AntiVirus 2014** 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 kopírovania a prilepiť.

Ako používa metódu Kopírovať a Prilepiť

Pomocou metódy **Kopírovať a Prilepiť** vložte licenčné číslo produktu **AVG AntiVirus 2014** 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.

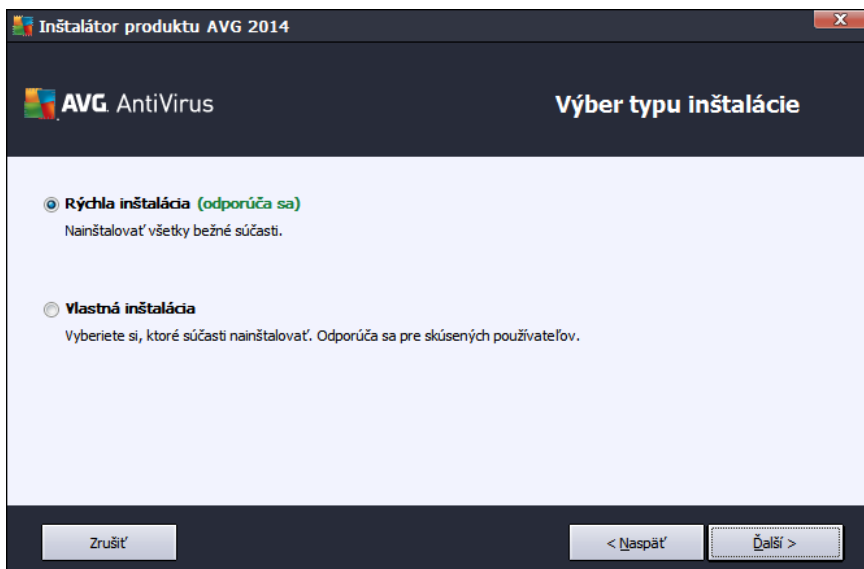
Ovládacie tlačidlá

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

- **Zruši** – kliknutím okamžite ukončíte priebeh inštalácie. Aplikácia **AVG AntiVirus 2014** 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

Váš šine používate, čo odporúčame ponechať štandardnú **expresnú** inštaláciu. Týmto spôsobom nainštalujete program **AVG AntiVirus 2014** v plne automatickom režime s nastaveniami vopred definovanými dodávateľom programu vrátane nástroja [AVG Security Toolbar](#). 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 2014**.

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

Vlastná inštalácia

Vlastnú inštaláciu by mali používať len skúsení používatelia, ktorí majú skutočný dôvod inštalovať produkt **AVG AntiVirus 2014** s neštandardnými nastaveniami, napríklad na účely prispôbenia konkrétnym systémovým potrebám. Ak sa rozhodnete pre túto možnosť, v dialógovom okne sa

aktivuje viacero nových možností:

- **Nainštalova AVG Toolbar pre zlepšenie ochrany na internete** – ak nezmeníte predvolené nastavenia, táto súasť sa nainštaluje automaticky do predvoleného internetového prehliadača (v súasnosti 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. Iné prehliadače nie sú podporované – ak používate alternatívny internetový prehliadač (napr. Avant Browser), môžete sa stretnúť s neočakávaným správaním.
- **Nastavi nástroj AVG Secure Search ako predvolenú domovskú stránku a stránku pre nové karty a zachovať toto nastavenie** – nechajte políčko zaškrtnuté pre potvrdenie, že si želáte otvárať váš predvolený internetový prehliadač a všetky jeho karty s nástrojom AVG Secure Search nastaveným ako domovskou stránkou.
- **Nastavi nástroj AVG Secure Search ako predvoleného poskytovateľa vyhľadávania a zachovať toto nastavenie** – nechajte políčko zaškrtnuté pre potvrdenie, že chcete používať ako poskytovateľa vyhľadávania vyhľadávací nástroj AVG Secure Search, ktorý úzko spolupracuje s nástrojom Link Scanner Surf Shield, na zabezpečenie vašej najvyššej bezpečnosti on-line.
- **Cieľový priečinok** – tu by ste mali určiť umiestnenie, kam by sa mal **AVG AntiVirus 2014** nainštalovať. **AVG AntiVirus 2014** sa predvolene inštaluje do priečinka programových súborov na disku C:, ako je to uvedené v textovom poli dialógového okna. Ak chcete toto umiestnenie zmeniť, použijete tlačidlo **Prehľadávať** na zobrazenie štruktúry jednotky a zvolíte príslušný priečinok. Na obnovenie predvoleného umiestnenia nastaveného dodávateľom softvéru použijete tlačidlo **Predvolené**.

Potom stlačte tlačidlo **alej**. Otvorí sa dialógové okno [Vlastné možnosti](#).

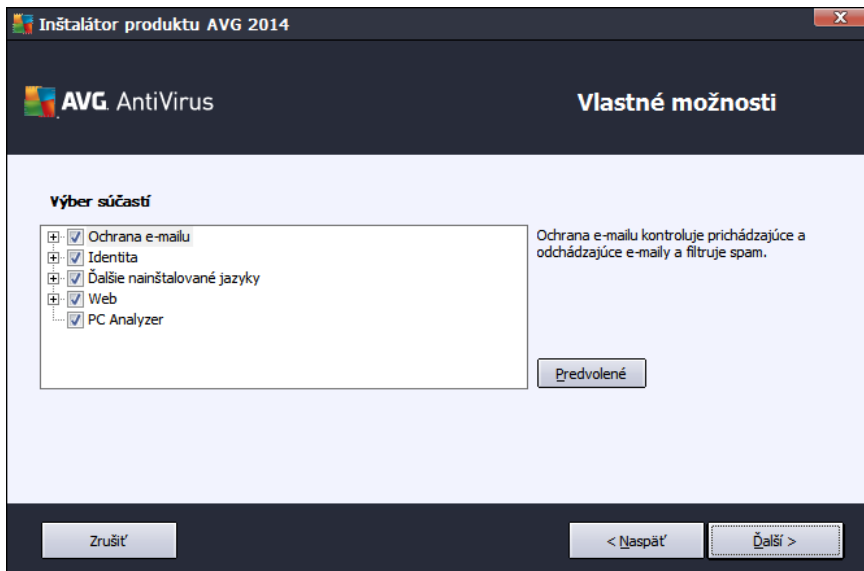
Ovládacie tlačidlá

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

- **Zrušiť** – kliknutím okamžite ukončíte priebeh inštalácie. Aplikácia **AVG AntiVirus 2014** sa nenainštaluje!
- **Naspäť** – kliknutím sa vrátíte o jeden krok k predchádzajúcemu dialógovému oknu inštalácie.
- **alej** – kliknutím posuniete priebeh inštalácie o krok **alej**.

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 2014**, 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**.

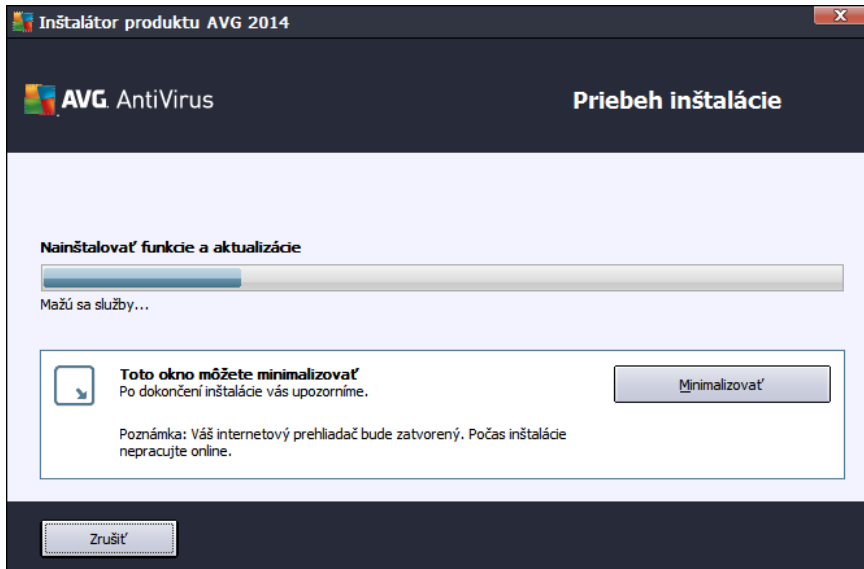
Ovládacie tlačidlá

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

- **Zrušiť** – kliknutím okamžite ukončíte priebeh inštalácie. Aplikácia **AVG AntiVirus 2014** sa nenainštaluje!
- **Naspäť** – kliknutím sa vrátite o jeden krok k predchádzajúcemu dialógovému oknu inštalácie.
- **Ďalej** – kliknutím posuniete priebeh inštalácie o krok ďalej.

3.6. 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 použijete iba vtedy, keď chcete zastaviť proces inštalácie. Nezabudnite, že v takom prípade sa aplikácia **AVG AntiVirus 2014** nenainštaluje!

3.7. Blahoželáme!

Dialógové okno **Blahoželáme!** potvrdí, že je program **AVG AntiVirus 2014** plne nainštalovaný a nastavený:



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 dokončíte stlačením tlačidla **Dokončiť**.



4. Po inštalácii

4.1. Registrácia produktu

Po nainštalovaní produktu **AVG AntiVirus 2014** 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 2014**. Označte položku [v hornom navigačnom pruhu Možnosti/Zaregistruvať 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 2014**

4.3. Kontrola celého počítača

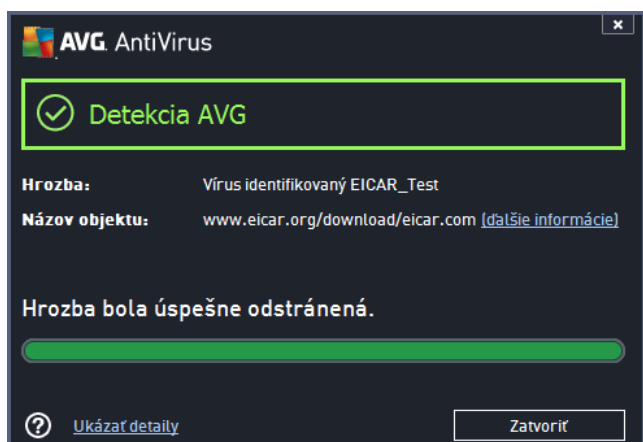
Existuje potenciálne riziko, že sa do vášho počítača dostal počítačový vírus ešte pred nainštalovaním produktu **AVG AntiVirus 2014**. Z tohto dôvodu by ste mali spustiť [Kontrolu celého počítača](#), aby sa vylúčila možnosť existencie infekcie v počítači. Prvá kontrola môže ísť a trvať (približne hodinu), no odporúčame 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 2014** 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 neexistuje vírus a neobsahuje žiadne fragmenty vírusového kódu. Väčšina produktov na ň reaguje ako na vírus (aj keď ho obyčajne označí jedným z názvov, 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. Hne po potvrdení prevzatia testovacieho súboru program **AVG AntiVirus 2014** na ň zareaguje varovaním. Zobrazenie tohto oznámenia znamená, že je program AVG správne nainštalovaný v počítači.



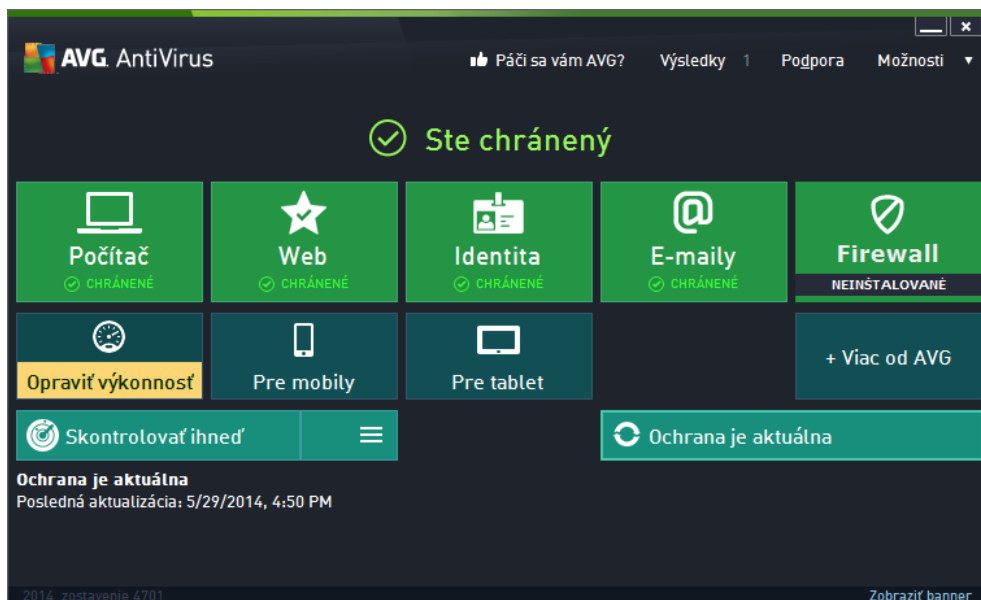
Ak sa programu AVG nepodarí identifikovať testovací súbor EICAR ako vírus, skontrolujte ešte raz konfiguráciu programu!

4.5. Predvolená konfigurácia AVG

Predvolenú konfiguráciu, (t. j. nastavenie aplikácie bezprostredne po inštalácii) produktu **AVG AntiVirus 2014**, nastavil dodávateľ softvéru tak, aby všetky služby a funkcie fungovali optimálnym spôsobom. **Nemejte 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 služby [Rozšírené nastavenia programu AVG](#): vyberte položku Hlavné ponuky Možnosti/Rozšírené nastavenia a upravte konfiguráciu programu AVG v novootvorenom dialógovom okne [Rozšírené nastavenia programu AVG](#).

5. Používateľské rozhranie AVG

AVG AntiVirus 2014 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 vám AVG*, *Výsledky*, *Podpora*, *Možnosti*). [Podrobnosti >>](#)
- **Informácie o stave zabezpečenia** je časť so základnými informáciami o aktuálnom stave vášho **AVG AntiVirus 2014**. [Podrobnosti >>](#)
- **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. [Podrobnosti >>](#)
- **Moje aplikácie** sú graficky znázornené v dolnom pruhu hlavného okna a obsahujú prehľad aplikácií doplnujúcich **AVG AntiVirus 2014**, 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 umožnia okamžitý prístup k vašim najdôležitejším a najčastejšie používaným funkciám programu AVG. [Podrobnosti >>](#)

Okrem hlavného okna produktu **AVG AntiVirus 2014** existuje ešte jedna kontrolná súprava, cez ktorú 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 2014**. [Podrobnosti >>](#)

5.1. Horný navigačný rad

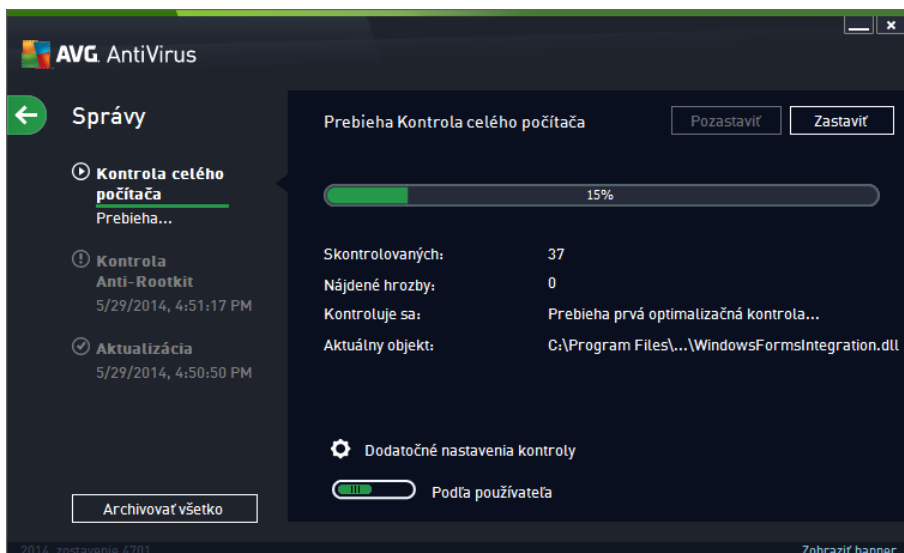
Horný navigačný rad sa skladá z radu viacerých aktívnych odkazov v hornej časti hlavného okna. Navigácia obsahuje tieto tlačidlá:

5.1.1. Pridajte sa k nám na sieti Facebook

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

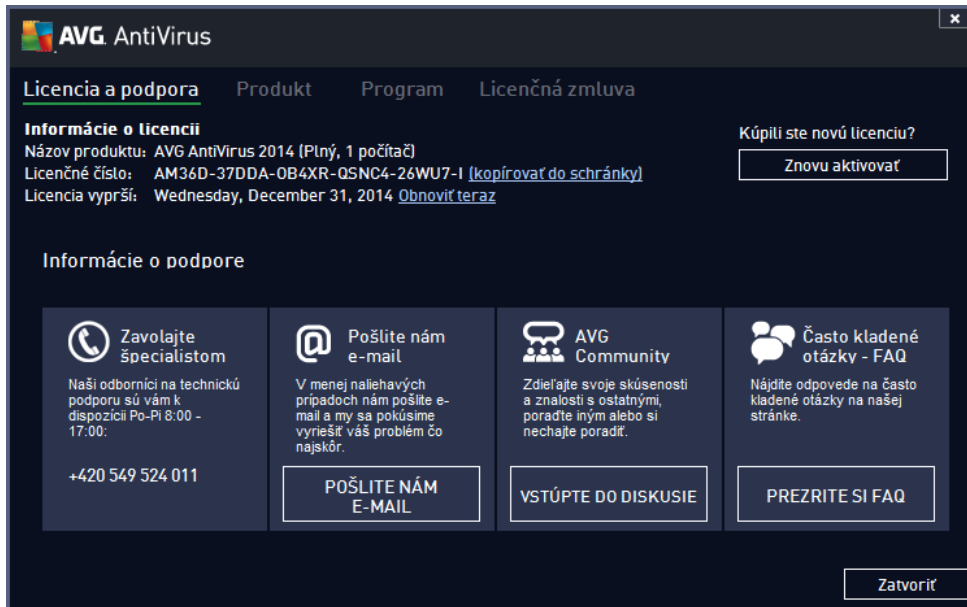
5.1.2. Správy

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 2014**:



- **Licencia a podpora** – táto záložka obsahuje informácie o názve produktu, licenčnom čísle a dátume expirácie. V dolnej časti dialógového okna nájdete tiež zoznam adres 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 2014 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 2014** 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 expirácie a ponuku na obnovenie/aktualizáciu.
- **Produkt** – na tejto záložke sa nachádza prehľad **AVG AntiVirus 2014** najdôležitejších technických údajov týkajúcich sa informácií o produkte, nainštalovaných súčiastkach, 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.

- **Licen ná zmluva** – na tejto záložke sa nachádza plné znenie licen nej zmluvy medzi vami a AVG Technologies.

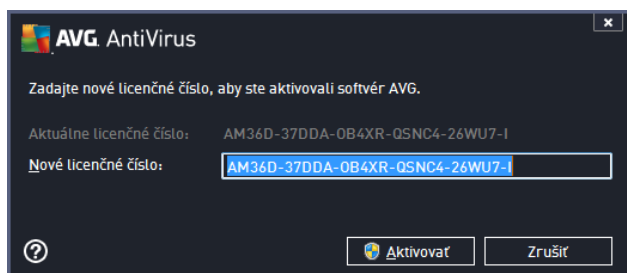
5.1.4. Možnosti

Údržba produktu **AVG AntiVirus 2014** je dostupná prostredníctvom položky **Možnosti**. Kliknutím na šípku otvoríte rozba ováciu ponuku:

- **Skontrolova celý počítač** – spustí kontrolu celého počítača.
- **Skontrolova vybraný prie inok...** – otvorí rozhranie kontroly programom AVG a pomocou stromovej štruktúry počítača umožní definovať, ktoré súbory a prie inky sa majú skontrolovať.
- **Skontrolova 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 potvrdíte spustenie kontroly.
- **Aktualizácia** – automaticky spustí aktualizácie produktu **AVG AntiVirus 2014**.
- **Aktualizácia z adresára...** – spustí aktualizáciu z aktualizovaných súborov, ktoré sa nachádzajú v nastavenom prie inku 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 novo otvorenom okne zvolíte prie inok, do ktorého ste predtým uložili aktualizovaný súbor a spustíte proces aktualizácie.
- **Vírusový trezor** – otvorí rozhranie úložiska karantény (Vírusový trezor), do ktorého AVG odstráni všetky zistené infekcie, ktoré sa z rôznych dôvodov nedajú automaticky vylíčiť. 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.
 - **Nálezy súčasti Identity Protection** – otvorí dialógové okno s prehľadom hrozieb detegovaných súčastou Identita.
 - **Nálezy súčasti Ochrana e-mailu** – otvorí dialógové okno s prehľadom príloh e-mailových správ označených súčastou Ochrana e-mailu ako nebezpečné.
 - **Nálezy súčasti Webový štít** – otvorí dialógové okno s prehľadom hrozieb zistených súčastou Webový štít.
 - **Protokol histórie udalostí** – otvorí rozhranie protokolu histórie s prehľadom všetkých zaznamenaných činností aplikácie **AVG AntiVirus 2014**.
- **Rozšírené nastavenia...** – otvorí dialógové okno s pokročilými nastaveniami programu AVG, kde môžete upraviť **AVG AntiVirus 2014** konfiguráciu. Odporúčame vám nemeň

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 na webovej lokalite AVG (<http://www.avg.com/>), v ktorej si môžete vyhľadať podrobné informácie o identifikovanom víruse.
- **(Znova) aktivovať** – otvorí sa dialógové okno aktivácie s licenčným kľúčom, ktoré ste zadali v procese inštalácie. Toto dialógové okno sa používa na úpravu licenčného kľúča buď pri nahradení predajného kľúča (s ktorým ste nainštalovali produkt AVG), alebo pri nahradení starého licenčného kľúča (napr. pri inovácii na nový produkt AVG). Ak používate skúšobnú verziu produktu **AVG AntiVirus 2014**, uvedené dve položky sa zobrazia v podobe **Kúpi teraz** a **Aktivovať** a umožnia vám zakúpiť úplnú verziu programu. Ak je produkt **AVG AntiVirus 2014** nainštalovaný pomocou predajného kľúča, položky sa zobrazia v podobe **Registrovať** a **Aktivovať** :



- **Zaregistrovať teraz / MyAccount** – 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.
- **O AVG** – otvorí nové dialógové okno s tromi záložkami s údajmi o zakúpenej licencií a dostupnej podpore, produkte a s informáciami o programe. Uvedené je tu tiež plné znenie licenčnej zmluvy. (Rovnaké dialógové okno môžete otvoriť pomocou odkazu [Podpora](#) v hlavnom navigačnom prvku.)

5.2. Informácie o stave zabezpečenia

Ikony **Informácie o stave zabezpečenia** sa nachádzajú v hornej časti hlavného okna produktu **AVG AntiVirus 2014**. V tejto časti sa vždy nachádzajú informácie o momentálnom stave zabezpečenia programom **AVG AntiVirus 2014**. Pozrite si prehľad ikon, ktoré sa môžu nachádzať v tejto časti, a ich význam:



– Zelená ikona informuje, že produkt **AVG AntiVirus 2014** je úplne funkčný. Váš počítač je plne chránený, aktuálny a všetky nainštalované súčasti fungujú správne.



– Žltá ikona upozorňuje, že **jedna súčasta alebo niektoré súčasti** je nesprávne

nakonfigurovaných a treba venovať pozornosť ich vlastnostiam alebo nastaveniam. Nevyskytuje sa žiaden vážny problém s produktom **AVG AntiVirus 2014** a pravdepodobne ste z nejakého dôvodu vypli niektorú súasť. Stále ste chránení. Venujte však pozornosť nastaveniam problémovej súasti! Nesprávne nastavená súasť 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 súasti. Vo **ba Ignorovať chybný stav** je dostupná vo vetve [Rozšírené nastavenia/Ignorovať chybný stav](#). Tam máte možnosť potvrdiť, že ste si vedomí chybového stavu súasti, ale z nejakého dôvodu chcete nechať program **AVG AntiVirus 2014** 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 2014** 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 2014!** Jedna alebo viac súastí nefunguje správne a produkt **AVG AntiVirus 2014** 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 2014 nastavený tak, aby poskytoval optimálny výkon, ved a informácie o stave zabezpečenia sa zobrazí nové tlačidlo s názvom Kliknutím opraviť (alebo Kliknutím opraviť všetko, ak sa problém týka viacerých súastí). Stlačením tlačidla spustíte automatický proces kontroly a konfigurácie programu. Je to jednoduchý spôsob nastavenia optimálneho výkonu programu AVG AntiVirus 2014 a dosiahnutia maximálnej úrovne zabezpečenia.

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

Poznámka: Informáciu o stave produktu AVG AntiVirus 2014 vám vždy poskytuje aj [ikona v paneli úloh](#).

5.3. Prehľad súčastí

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

Presuňte kurzor myši nad súasť. V dolnej časti [hlavného okna](#) sa zobrazí krátky text. Text uvádza základný popis funkcie súasti. Obsahuje tiež informácie o aktuálnom stave súasti a uvádza, ktorá zo služieb súasti nie je správne nakonfigurovaná.

Zoznam nainštalovaných súastí

V programe **AVG AntiVirus 2014** sa v **asti Prehľad sú astí** nachádzajú informácie o týchto sú astiach:

- **Poíta** – Tieto sú asti sa týkajú dvoch služieb: **sú as Rezidentný štít** deteguje vírusy, spyware, červy, trójske kone, neželané spustené súbory a knižnice v systéme a chráni vás pred škodlivým adware. Druhou sú asou je **Anti-Rootkit**, ktorá kontroluje nebezpečné rootkity ukryté vnútri aplikácií, ovláda ov alebo knižníc. [Detaily >>](#)
- **Prezeranie webu** – chráni pred útokmi na webe pri vyhľadávaní a surfovaní na internete. [Detaily >>](#)
- **Identita** – táto sú as spúšťa službu **Identity Shield**, ktorá neustále chráni vaše digitálne aktíva pred novými a neznámymi hrozbami na internete. [Podrobnosti >>](#)
- **E-maily** – kontroluje prichádzajúce e-mailové správy z hľadiska prítomnosti SPAMU a blokuje vírusy, phishingové útoky a iné hrozby. [Detaily >>](#)

Dostupné možnosti

- **Presunutím kurzora myši nad ktorúkoľvek ikonu sú astí** sa príslušná ikona zvýrazní v prehľade sú astí. V spodnej **asti používate ského rozhrania** sa zároveň zobrazí opis základných funkcií sú astí.
- **Jedným kliknutím na ikonu sú astí** 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 sú astí**) 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.
- **Sú as 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 stlačenie 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.
- **Sú as PC Tuneup** je vyspelý nástroj na podrobnú analýzu a opravu systému, ktorý sa

používa na hľadanie možností, ako zvýši rýchlosť počítača a zlepši jeho celkový výkon.

- **MultiMi** sústreďuje všetky e-maily a úlohy 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 súhrn priamo prečítať.

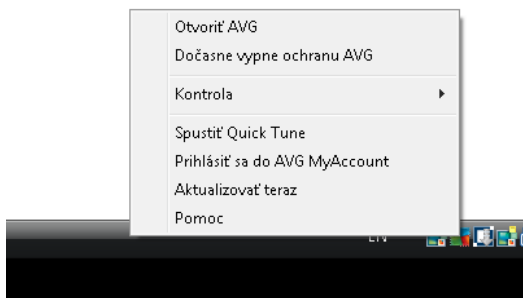
5.5. Kontrola/Aktualizovať rýchle odkazy

Rýchle odkazy sa nachádzajú v spodnom riadku tlačidiel v [používateľskom rozhraní AVG AntiVirus 2014](#). 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/priebehov](#). (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 2014**. Vždy sa nachádza v paneli úloh bez ohľadu na to, či je [používateľské rozhranie](#) produktu **AVG AntiVirus 2014** otvorené alebo zatvorené:



Zobrazenie ikony AVG v systémovom paneli úloh

-  Úplne vyfarbená ikona bez ďalších prvkov znamená, že všetky sú asť aplikácie **AVG AntiVirus 2014** sú aktívne a úplne funkčné. Takáto ikona sa však môže zobrazovať vtedy, keď niektorá zo sú asť nie je úplne funkčná, ale používateľ sa rozhodol [ignorovať jej stav](#). (Ak ste potvrdili možnosť ignorovania stavu sú asť, potvrdzujete tým, že ste si vedomí [chybového stavu sú asť](#), ale z nejakého dôvodu ju tak chcete nechať a nechcete zobrazovať varovania týkajúce sa tejto situácie.)
-  Ikona s výkričníkom znamená, že sú asť (alebo viac sú asť) je v [chybovom stave](#). Takýmto výstrahám vždy venujte pozornosť a snažte sa odstrániť problém konfigurácie sú asť, ktorá nie je nastavená správne. Ak chcete zmeniť konfiguráciu sú asť, dvakrát kliknite na ikonu v paneli úloh. Otvorí sa [používateľské rozhranie aplikácie](#). Podrobné informácie o [chybovom stave](#) jednotlivých sú asť nájdete v sú asť [Informácie o stave zabezpečenia](#).
-  Ikona v paneli úloh sa môže tiež zobrazovať plnofarebne s blikajúcim a otáčajúcim sa majákom. Táto grafická verzia signalizuje, že prebieha aktualizácia.
-  Plnofarebné zobrazenie ikony so šípkou znamená, že **AVG AntiVirus 2014** 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 2014** a možných zmenách stavu programu (napr. automatickom spustení naplánovanej kontroly alebo aktualizácie, prepnutí profilu bezpečnostnej brány Firewall, zmene stavu sú asť, výskyte chybového stavu, ...) pomocou kontextového okna, ktoré sa otvorí kliknutím na ikonu v paneli úloh.

Možnosti 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 2014**. Stačí dvakrát kliknúť na ikonu. Kliknutím pravým tlačidlom myši na ikonu sa otvorí krátko kontextová ponuka s týmito možnosťami:

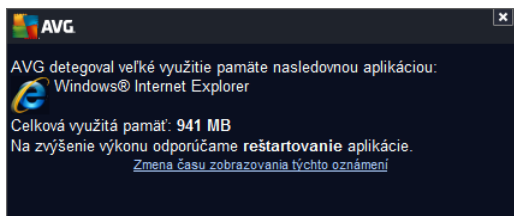
- **Otvorí program AVG** – kliknutím na túto možnosť sa otvorí [používateľské rozhranie](#) programu **AVG AntiVirus 2014**.
- **Dočasne vypnú ochranu AVG** – táto možnosť umožňuje vypnúť celú ochranu produktom **AVG AntiVirus 2014** naraz. Nepoužívajte túto možnosť, ak to nie je naozaj nevyhnutné! Vo väčšine prípadov nie je potrebné vypnúť produkt **AVG AntiVirus 2014** pred inštaláciou nového softvéru alebo ovládačov, a to ani v prípade, keď inštalovaný 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 2014**, znova ju zapnite bezprostredne po dokončení úloh, pre ktoré ste ju vypli. Ak ste pripojení na internet alebo k sieti v momente, 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 sa práve beží kontrola. Tejto kontrole môžete potom nastaviť prioritu, alebo ju môžete zastaviť alebo pozastaviť. alej sa tu nachádzajú tieto funkcie: *Nastaviť prioritu pre všetky kontroly*, *Pozastaviť všetky kontroly* a *Zastaviť všetky kontroly*.
- **Spustí Quick Tune** – kliknutím na túto možnosť sa spustí súhrn [Quick Tune](#).
- **Prihlási sa na stránku AVG MyAccount** – otvorí domovskú stránku MyAccount, na ktorej môžete spravovať predplatné produktov, zaplatiť dodatočnú ochranu, prevziať inštalované súbory, skontrolovať minulé objednávky a faktúry a spravovať osobné informácie.
- **Aktualizovať teraz** – spustí okamžitú [aktualizáciu](#).
- **Pomocník** – otvorí súbor pomocníka na úvodnej strane.

5.7. AVG Advisor

Súhrn **AVG Advisor** bola navrhnutá tak, aby detegovala problémy, ktoré môžu spomalovať váš počítač alebo ho ohrozovala 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, a v nich nedochádza k problémom, a ponúka tipy na ich predchádzanie.

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



Súhrn **AVG Advisor** sleduje nasledujúce:

- **Stav akéhokoľvek práve otvoreného internetového prehliadača.** Internetové prehliadače môžu zahlcovať pamäť, predovšetkým v prípade, ak počítač zostane otvorených viacero kariet alebo okien, a môžu spotrebúvať mnoho systémových prostriedkov, t. j. spomalovať 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 účasť 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. Súhrn **AVG Advisor** tomu môže predísť tak, že vás varuje, že známy názov v skutočnosti označuje novú sieť. Samozrejme, ak sa rozhodnete,



že neznáma sie je bezpečná, môžete ju uložiť do zoznamu známych sietí súčasti **AVG Advisor**, aby v budúcnosti nebola znovu nahlásovaná.

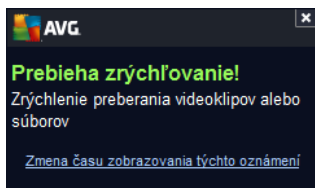
V každej z týchto situácií vás nástroj **AVG Advisor** upozorní na možný problém, ktorý by mohol nastať, a zobrazí názov a ikonu problémového procesu či aplikácie. Funkcia **AVG Advisor** tiež ponúkne návrh krokov, ktorými by ste sa mohli vyhnúť možnému problému.

Podporované webové prehliadače

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

5.8. AVG Akcelerátor

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

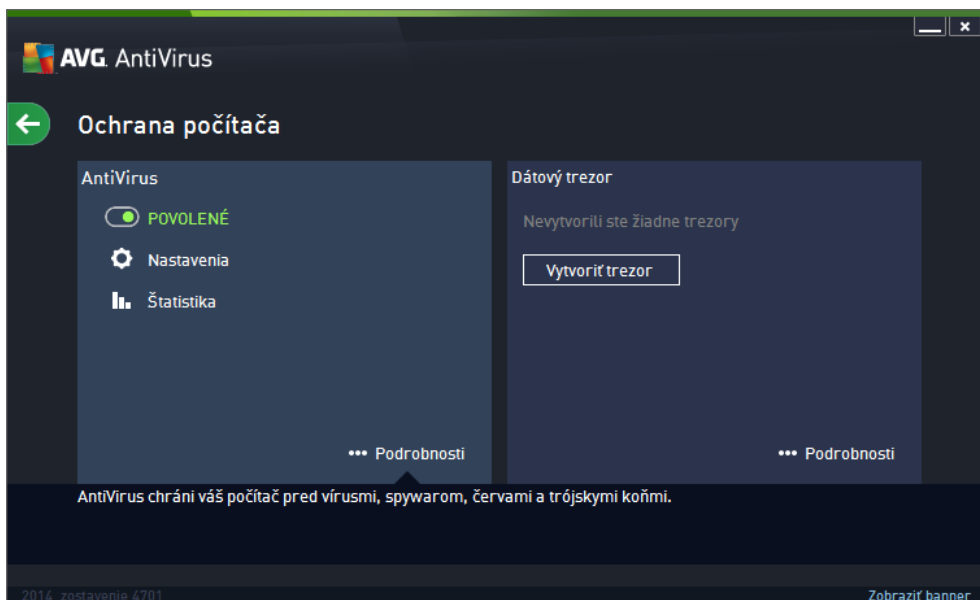


6. Súčasti AVG

6.1. Ochrana počítača


Súčasť **Počítač** sa týka dvoch hlavných bezpečnostných služieb: **AntiVirus** a **Dátový trezor**.


- **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 vykonať 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 súčasť AntiVirus dokáže detegovať nový, neznámy vírus, ak tento nový vírus obsahuje isté typické vlastnosti existujúcich vírusov. **AVG AntiVirus 2014** vie tiež analyzovať a detegovať spustené aplikácie alebo knižnice DLL, ktoré by sa v systéme nemali nachádzať (*rôzne typy spyware, adware a pod.*). AntiVirus alej kontroluje podozrivé záznamy v databáze Registry, dočasné internetové súbory a spracuje všetky potenciálne škodlivé položky rovnakým spôsobom ako každú inú infekciu.
- **Služba Dátový trezor** vám umožňuje vytvárať bezpečné virtuálne trezory, do ktorých môžete ukladať cenné alebo citlivé údaje. Obsah dátového trezora je šifrovaný a chránený heslom, ktoré si vyberiete, aby k údajom nikto nemal prístup bez povolenia.





Ovládacie prvky dialógového okna


Ak chcete prepínať medzi oboma časťami dialógového okna, stačí kliknúť kdekoko 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 File Vault*):

 **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 zaručia 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 o najskeôr.

 **Nastavenia** – kliknutím na tlačidlo budete presmerovaní na rozhranie [rozšírených nastavení](#). Otvorí sa príslušné dialógové okno a budete môcť nakonfigurovať vybranú službu, t. j. [AntiVirus](#). V rozšírených nastaveniach môžete upraviť všetky konfigurácie každej bezpečnostnej služby programu **AVG AntiVirus 2014**, 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 2014** 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.

Ako vytvorí dátový trezor

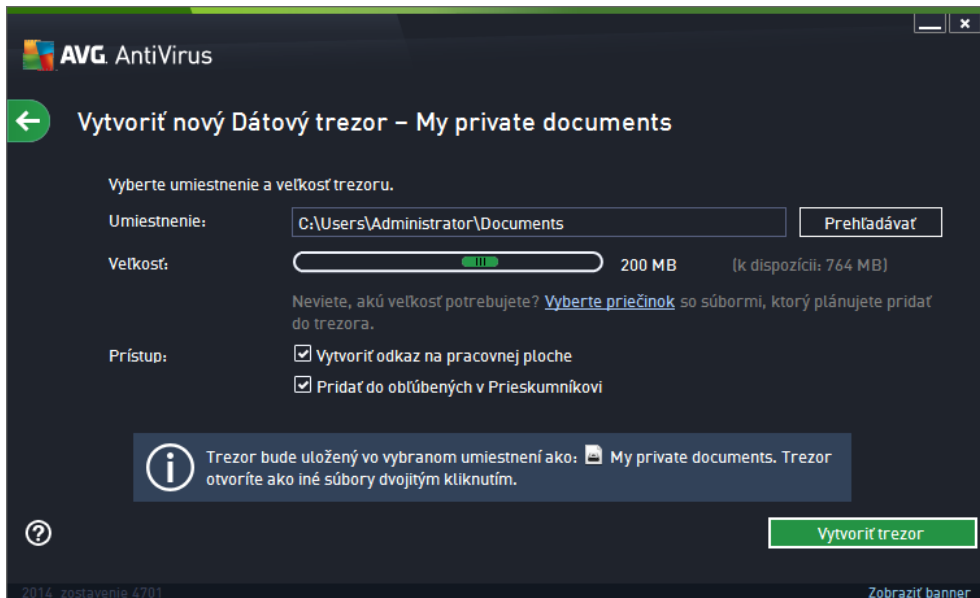
V časti **Dátový trezor** dialógového okna **Ochrana počítača** nájdete tlačidlo **Vytvorí trezor**. Kliknutím na tlačidlo otvoríte nové dialógové okno s rovnakým názvom, do ktorého môžete zadať parametre plánovaného trezora. Vyplňte všetky potrebné informácie a postupujte podľa pokynov v aplikácii:



Najprv je potrebné zadať názov trezora a vytvoriť silné heslo:

- **Názov trezora** – ak chcete vytvoriť nový dátový trezor, najprv je potrebné vybrať vhodný názov. Ak sa delíte o počítač s ostatnými členmi rodiny, môžete do názvu zahrnúť svoje meno a slovo označujúce jeho obsah, napríklad *Ockove e-maily*.
- **Vytvoriť heslo/Znovu zadať heslo** – vytvorte heslo pre dátový trezor a napíšte ho do príslušných textových polí. Grafický indikátor vpravo vám oznámi, či je heslo slabé (*pomerne jednoducho prelomite ním pomocou špeciálnych softvérových nástrojov*) alebo silné. Odporúčame zvoliť si heslo s minimálne strednou silou. Heslo môžete urobiť silnejším, ak bude obsahovať veľké písmená, čísla a iné znaky, ako napríklad bodky, pomlčky, atď. Ak sa chcete uistiť, že heslo zadávate správne, môžete zaškrtnúť políčko **Zobrazit heslo** (*samozrejme, nikto iný sa nesmie pozerať na vašu obrazovku*).
- **Pomôcka pre heslo** – dôrazne odporúčame, aby ste si vytvorili aj pomôcku pre heslo, ktorá vám pomôže spomenúť si naň v prípade, že by ste ho zabudli. Pamätajte, že dátový trezor je určený na zabezpečenie súborov a umožňuje prístup k nim len so zadaním hesla. Túto ochranu nemožno nijako obísť a ak zabudnete heslo, nebudete mať prístup do dátového trezora!

Po zadaní všetkých požadovaných údajov do textových polí kliknite na tlačidlo **alej** a pokračujte ďalším krokom:

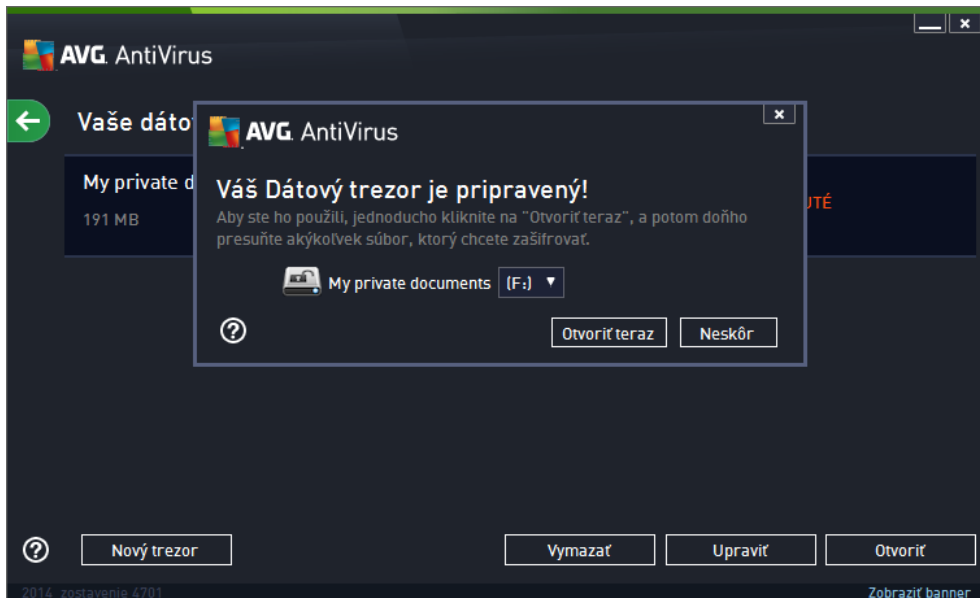


Toto dialógové okno poskytuje nasledovné možnosti konfigurácie:

- **Umiestnenie** ur uje, kde bude dátový trezor fyzicky umiestnený. Nájdite vhodné miesto na pevnom disku alebo ponechajte preddefinované umiestnenie v prie inku *Dokumenty*. Pozor, ke dátový trezor vytvoríte, jeho umiestnenie viac nemožno zmeni .
- **Ve kos** – môžete prednastavi ve kos dátového trezoru, ím sa vyhradí potrebné miesto na disku. Nastavená hodnota by nemala by príliš malá (*nedostato ná pre vaše potreby*) ani príliš ve ká (*aby trezor nezaberal zbyto ne prive a miesta na disku*). Ak už viete, o chcete do dátového trezora umiestni , môžete da všetky príslušné súbory do jedného prie inka a potom pomocou odkazu **Vybra prie inok** automaticky vypo íta celkovú ve kos . Ve kos však môžete neskôr zmeni pod a svojich potrieb.
- **Prístup** – za iarkavacie polí ka v tejto asti umož ťujú vytvori pohodlné skratky k dátovému trezoru.

Ako používa dátový trezor

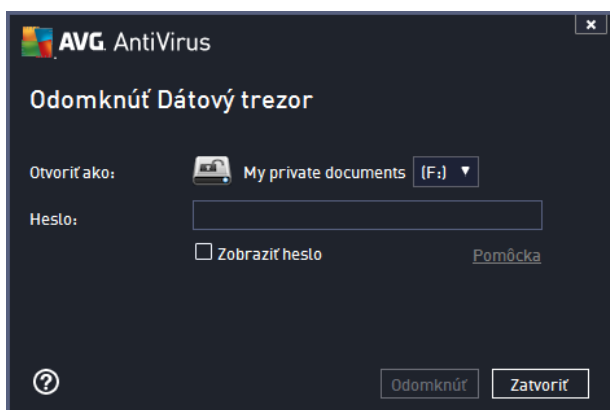
Ke budete s nastaveniami spokojní, kliknite na tlačidlo **Vytvori trezor**. Otvorí sa nové dialógové okno **Váš dátový trezor je teraz pripravený** a oznámi vám, že daný trezor je pripravený na ukladanie súborov. Práve teraz je trezor otvorený a môžete k nemu ihne pristupova . Pri každom ďalšom pokuse o prístup do trezora budete vyzvaní na odomknutie trezora pomocou hesla, ktoré ste ur ili:



Pred použitím nového dátového trezora ho musíte najskôr otvoriť – kliknite na tlačidlo **Otvoríť teraz**. Po otvorení sa dátový trezor objaví vo vašom počítači ako nový virtuálny disk. V rozbaľovacej ponuke mu priradíte písmeno podľa vášho výberu (*budete môc vybrať spomedzi aktuálne dostupných diskov*). Obvykle si nebudete môc vybrať písmeno C (zvyčajne priradené pevnému disku), A (disketová mechanika) alebo D (jednotka diskov DVD). Pri každom odomknutí dátového trezora si môžete vybrať iné dostupné písmeno.

Ako odomknúť dátový trezor

Pri ďalšom pokuse o prístup do dátového trezora budete vyzvaní na odomknutie trezora pomocou hesla, ktoré ste si určili:

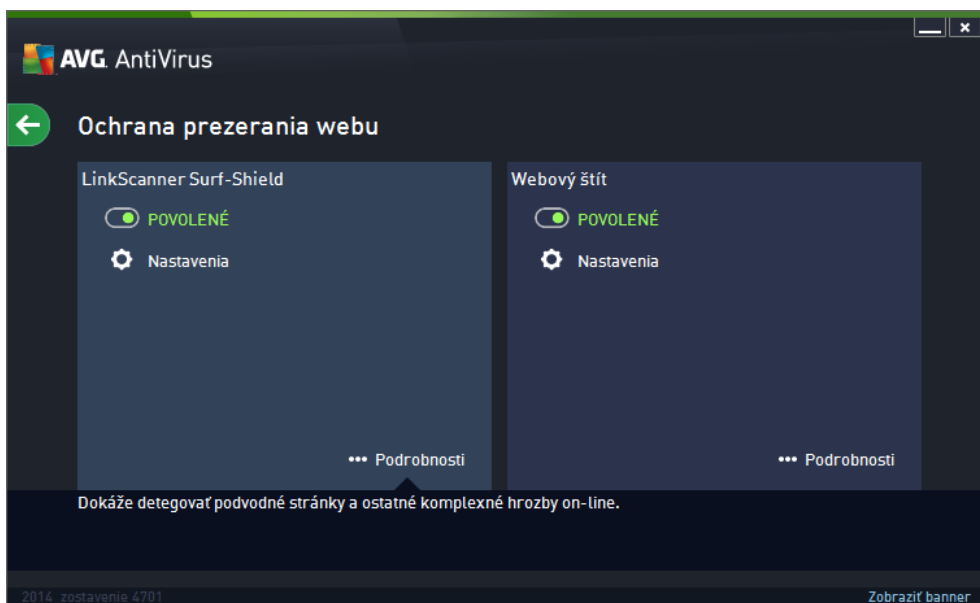


Do textového poľa sa musíte overiť napísaním vašej osoby hesla a kliknutím na tlačidlo **Odomknúť**. Ak potrebujete pripomenúť heslo, kliknite na položku **Pomôcka**, čím zobrazíte pomôcku k heslu, ktorú ste si určili pri vytváraní dátového trezora. Nový dátový trezor sa zobrazí v prehľade vašich dátových trezorov ako ODOMKNUTÝ a budete môc podľa potreby pridávať a odstraňovať súbory.

6.2. Ochrana prezerania webu


Ochrana prezerania 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 pre“ 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. **Súčasťou 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 zobrazíť. Takisto rozpoznáva malware, ktorý sa nachádza na danej stránke, a ihneď zastaví jeho sťahovanie, aby sa nikdy nedostal do vášho počítača. Táto unikátna ochrana zablokuje škodlivý kód každej webovej stránky, ktorú sa pokúšate otvoriť, a zabráni jeho prevzatíu 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 dôležité pamätať na to, že zneužitie stránky môžu infikovať váš počítač už len tým, že ich navštívite. **Súčasťou Webový štít nie je určená na ochranu serverových platforiem!**





Ovládacie prvky dialógového okna

Ak chcete prepínať medzi oboma časťami dialógového okna, stačí kliknúť kdekokoľvek 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 odporujeme, aby ste ponechali predvolené nastavenia pre všetky konfigurácie zabezpečenia. Predvolené nastavenia zaručia optimálny výkon aplikácie a maximálnu bezpečnosť. Ak z nejakého dôvodu chcete vypnúť službu, budete upozomení na možné riziká červeným **varovným** nápisom a oznámením faktu, že momentálne nie ste úplne chránení. **Nezabudnite, že by ste službu mali znovu aktivovať o najskeôr.**

 **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 upraviť všetky konfigurácie každej bezpečnostnej služby programu **AVG AntiVirus 2014**, no akékoľvek nastavenie odporujeme iba skúseným používateľom!

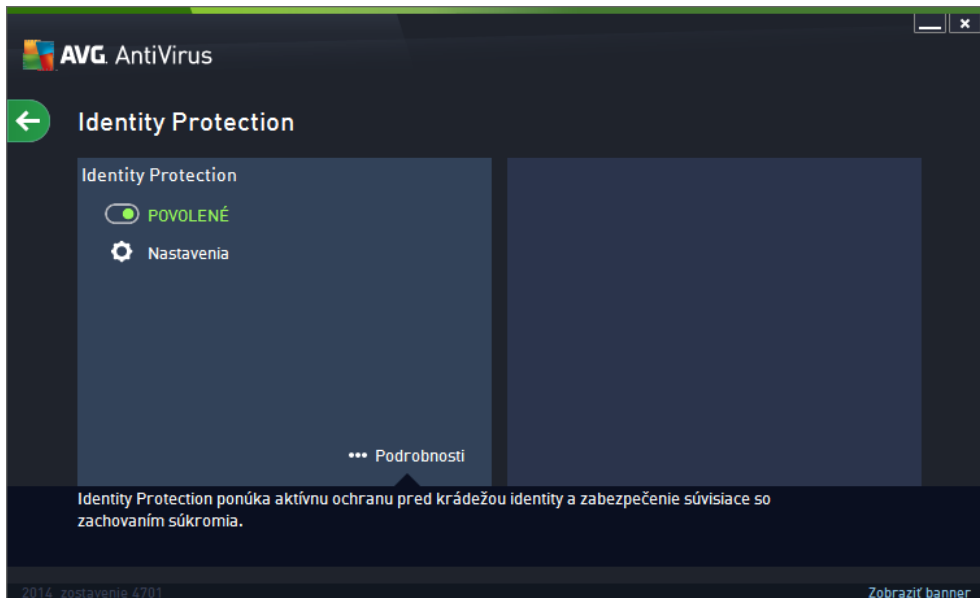
 **Podrobnosti** – kliknutím na tlačidlo sa v dolnej časti dialógového okna zobrazí stručný popis označenej služby.

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

6.3. Identity Protection


Súčasťou **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 malwarom, ktorá chráni pred všetkými druhmi malwaru (*spyware, softvérové roboty, krádež identity...*) s použitím technológií monitorovania správania a poskytuje okamžitú ochranu pred novými vírusmi. Identity Protection zabráni páchatelom po čítačovej trestnej činnosti v oblasti odcudzenia identity, aby odcudzili vaše heslá, podrobnosti 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. Súčasťou 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 nič 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 hardiskového škodlivého správania. Ak sa súbor označí ako škodlivý, súčasťou 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 veľa 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 zaručia 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 o 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 upraviť všetky konfigurácie každej bezpečnostnej služby programu **AVG AntiVirus 2014**, 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 ktorým súvisí.

V produkte **AVG AntiVirus 2014** služba Identity Alert zatiaľ 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 služby 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. Ochrana e-mailu


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

- **Kontrola pošty**: Jeden z najbežnejších zdrojov vírusov a škodlivých kódov je e-mail. Ohrozenia typu phishing a spam alej zvyšujú riziko e-mailu. Bezplatné e-mailové služby sú náchyľnejšie 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 útoku prostredníctvom e-mailu. Spoločnosť obyčajne využíva podnikové e-mailové služby 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 textové 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 vám šíri propagáciu produktov a služieb a ktorá je masovo zasielaná na množstvo e-mailových adries súčasnane. Podobné správy plnia poštové schránky príjemcov. Spam sa nevzťahuje na legítimne 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 neoznačené ako spam) a zoznamu zakázaných odosielateľov (vždy označené ako spam).





Ovládacie prvky dialógového okna


Ak chcete prepínať medzi oboma časťami dialógového okna, stačí kliknúť kdekoko 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 dvoma 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 zaručia 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 o najskôr.**

V súčasti Kontrola pošty sa nachádzajú dve tlačidlá v podobe semaforov. Takto môžete samostatne určiť, či chcete, aby súčasti 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 upraviť všetky konfigurácie každej bezpečnostnej služby programu **AVG AntiVirus 2014**, no akékoľvek nastavenie odporúčame iba skúseným používateľom!

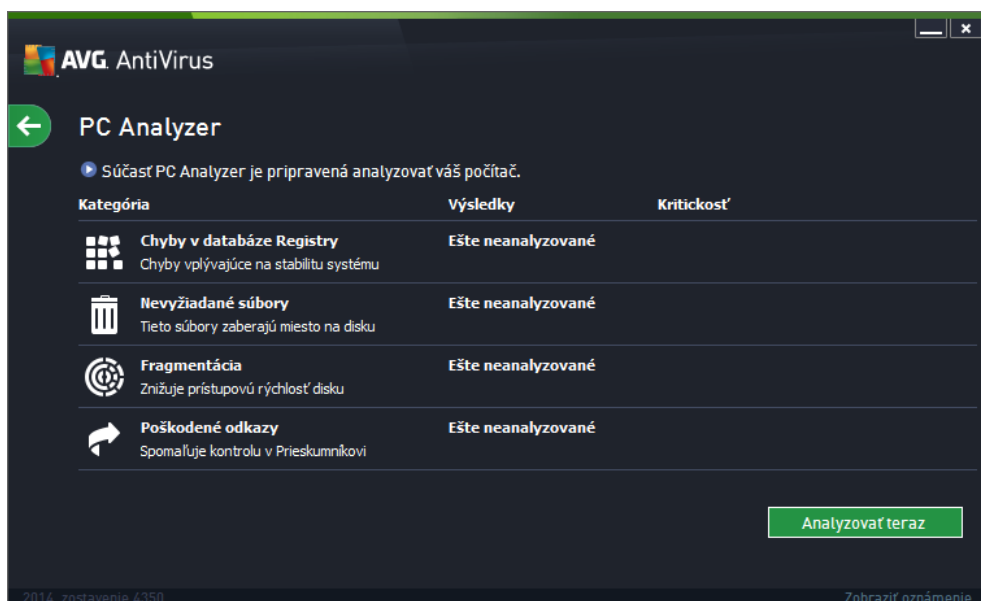
 **Štatistika** – kliknutím na tlačidlo budete presmerovaní na príslušnú stránku na webovej lokalite AVG (<http://www.avg.com/>). Na tejto lokalite sa nachádza štatistický prehľad o všetkých činnostiach aplikácie **AVG AntiVirus 2014** vykonaných v požadovanom vymedzenom intervale za celý čas.

 **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. Súčasť Quick Tune

Súčasťou **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. Otvára sa z [hlavného používateľského rozhrania](#) cez položku **Opraviť výkonnosť** :



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

- **Chyby v databáze Registry** informuje o početných chýb v databáze Registry operačného systému Windows, ktoré môžu spomalovať váš počítač alebo spôsobovať zobrazenie chybových hlásení.
- **Nevyžiadané súbory** informuje o početných 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** vypovedá podiel pevného disku, ktorý je fragmentovaný, t. j. používal sa dlhý čas a väčšina súborov je umiestnená na rôznych miestach fyzického disku.
- **Poškodené odkazy** vyhľadáva 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:



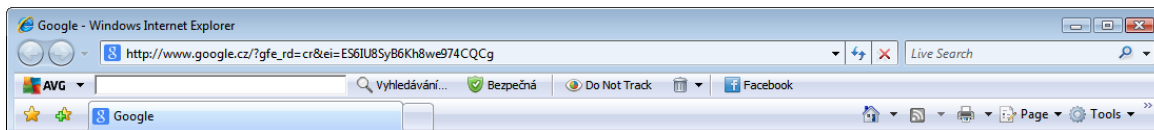
Prehľad výsledkov informuje o počte detegovaných systémových problémov, ktoré sú klasifikované podľa príslušnej testovanej kategórie. Výsledky analýzy sa zobrazia aj v grafickej podobe na osi v stupnici **Závažnosť**.

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

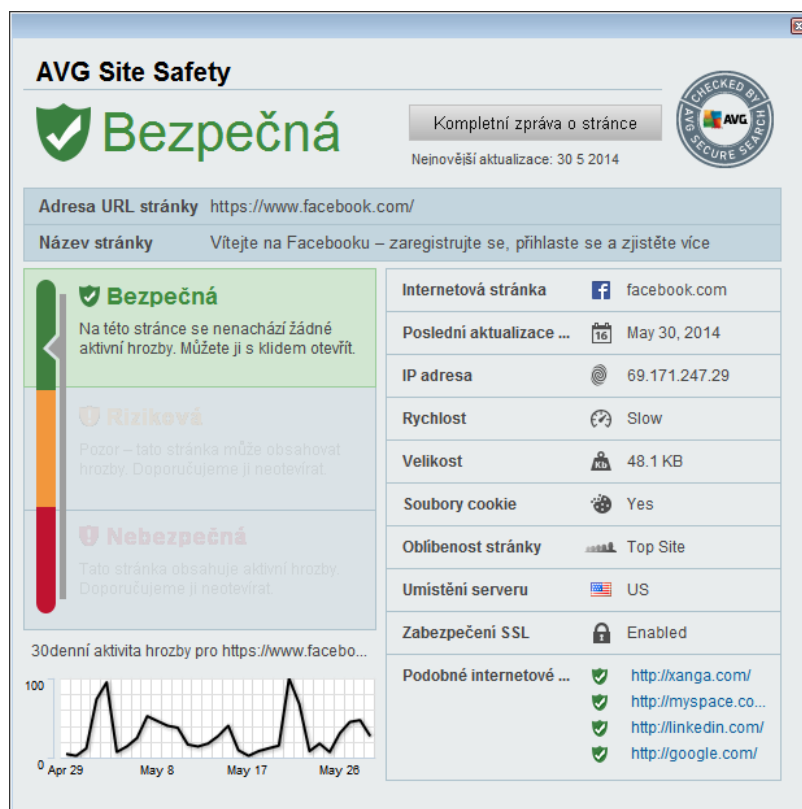
AVG Security Toolbar je nástroj, ktorý úzko spolupracuje so súasťou LinkScanner Surf-Shield a zabezpečuje maximálnu ochranu pri prezeraní internetu. V produkte **AVG AntiVirus 2014** je inštalácia súasťou **AVG Security Toolbar** voliteľná. Počas [procesu inštalácie](#) sa môžete rozhodnúť, či chcete túto súasť nainštalovať. Keď súasťou **AVG Security Toolbar** máte prístup priamo v internetovom prehliadači. V súasnosti medzi podporované prehliadače 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 neobvyklým správaním).



Nástroj **AVG Security Toolbar** pozostáva z nasledujúcich súasí:

- **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**.
 - **Licencijná zmluva koncového používateľa** – otvorí webovú lokalitu spoločnosti AVG na stránke s plným znením licencijnej zmluvy na používanie **AVG AntiVirus 2014**.
 - **Ochrana osobných údajov** – otvorí webovú lokalitu spoločnosti AVG na stránke s plným znením zásad spoločnosti AVG na ochranu osobných údajov.
 - **Odnášalova súasť AVG Security Toolbar** – otvorí sa webová stránka s podrobnosťami o postupe vypnutia súasí **AVG Security Toolbar** pre každý z podporovaných webových prehliadačov.
 - **About...** – otvorí sa nové okno s informáciami o verzii aktuálne nainštalovanej súasí **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 napíšete kľúčové slovo alebo frázu a stlačením tlačidla **Vyhľadaj** (alebo Enter).
- **Bezpečnosť stránky** – toto tlačidlo otvorí nové dialógové okno obsahujúce informácie

o aktuálnej úrovni hrozby (*Bezpečnosť*) webovej lokality, na ktorej sa práve nachádzate. Tento krátky prehľad môžete rozbaľať a zobraziť všetky podrobnosti o všetkých bezpečnostných inostiach týkajúcich sa webovej lokality priamo v okne prehliadača a (*Zobraziť úplnú správu*):



AVG Site Safety

Bezpečná Kompletní zpráva o stránce

Nejnovější aktualizace: 30.5.2014

Adresa URL stránky: <https://www.facebook.com/>

Název stránky: Vítejte na Facebooku – zaregistrujte se, přihlaste se a zjistěte více

Bezpečná

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

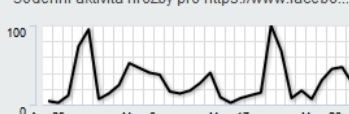
Riziková

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

Nebezpečná

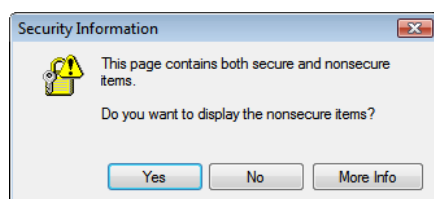
Tato stránka obsahuje aktivní hrozby. Doporučujeme ji neotevřít.

30denní aktivita hrozby pro <https://www.facebook.com/>



Internetová stránka	facebook.com
Poslední aktualizace ...	May 30, 2014
IP adresa	69.171.247.29
Rychlost	Slow
Velikost	48.1 KB
Soubory cookie	Yes
Oblíbenost stránky	Top Site
Umístění serveru	US
Zabezpečení SSL	Enabled
Podobné internetové ...	http://xanga.com/ http://myspace.co... http://linkedin.com/ http://google.com/

- **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. [Podrobnosti >>](#)
- **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 predpovečou 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**.



- Tlačítká skrátiek 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 ďalších 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 prehliadačoch 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 počte služieb zhromažďujúcich údaje:  Po kliknutí na ikonu sa zobrazí takéto dialógové okno:



Všetky zistené služby zhromažďujúce údaje sú uvedené v prehľade **Sledovanie 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 ponúknuť 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 oblastí nemusia v dialógovom okne aplikácie AVG Do Not Track zobraziť.

Ovládacie prvky dialógového okna

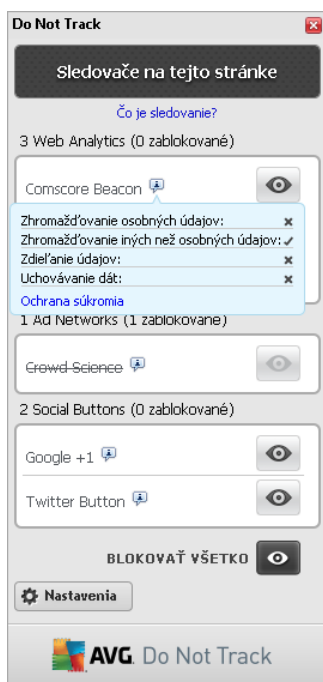
- **o je sledovanie?** – po kliknutí na toto prepojenie v hornej časti dialógového okna budete presmerovaní na špeciálnu webovú stránku s podrobným vysvetlením princípov sledovania a

s popisom konkrétnych druhov sledovania.

- **Blokova 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 blokovanie. Môžete postupovať dvoma spôsobmi:

- **Blokova 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 jednotlivu konkretizovať, či by daná služba mala byť povolená, alebo blokovávaná. 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 zablockovať činnosti zhromažďovania údajov všetkých procesov označených ako reklamné siete. Aby ste zablockovali zhromažďovanie údajov (názov procesu sa zobrazí preškrtnutý) 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 **Blokova 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**



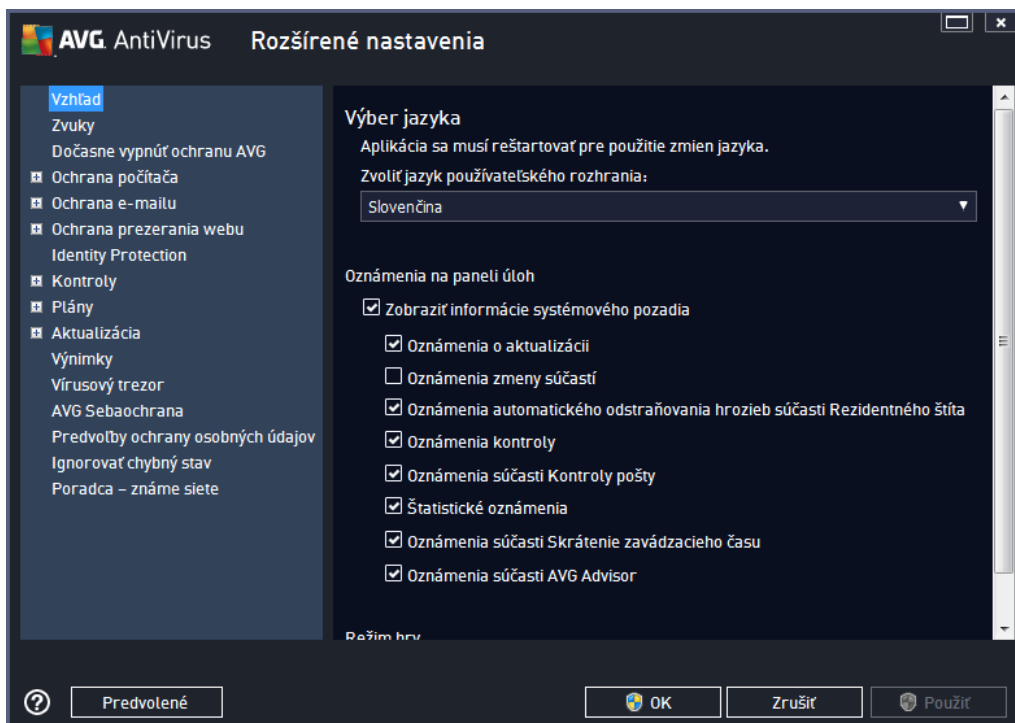
lokality, že nechcem by sledovaný (predvolene zapnuté). Túto možnosť nechajte zaškrtnutú, aby ste potvrdili, že chcete, aby aplikácia **Do Not Track** informovala poskytovateľa služieb zhromažďujúcich údaje, že nechcete byť sledovaní.

9. Rozšírené nastavenia programu AVG

Dialógové okno s rozšírenou konfiguráciou produktu **AVG AntiVirus 2014** 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 súčastí, ktorej konfiguráciu chcete zmeniť (alebo jej konkrétnej súčasti), 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 2014** a niektorých základných možností správanie sa aplikácie:



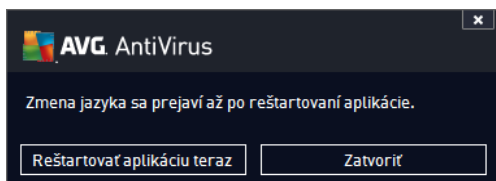
Výber jazyka

V časti **Výber jazyka** môžete v rozbaľovacej ponuke vybrať požadovaný jazyk. Vybraný jazyk sa potom použije pre celé [používateľské rozhranie](#) produktu **AVG AntiVirus 2014**. 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 2014** 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

reštartova **AVG AntiVirus 2014**

- Stla ením tlačidla **Reštartova AVG** potv rte súhlas s reštartovaním programu. Po kajete chví u, kým sa zmena jazyka prejaví:



Oznámenia na paneli úloh

V tejto asti môžete zruši zobrazovanie oznámení v paneli úloh o stave aplikácie **AVG AntiVirus 2014**. V predvolenom nastavení je zobrazovanie oznámení v paneli úloh povolené. Dôrazne odporú ame toto nastavenie nemeni ! Systémové oznámenia informujú napríklad o spustení kontroly, spustení aktualizácie alebo o zmene sú asti **AVG AntiVirus 2014**. Týmto oznámeniam by ste rozhodne mali venova pozornos .

Ak sa však z nejakého dôvodu rozhodnete tieto informácie nezobrazova alebo ak chcete zobrazi iba niektoré oznámenia (*týkajúce sa konkrétnej sú asti AVG AntiVirus 2014*), môžete definova a ur i vlastné predvo by ozna ením/zrušením ozna enia príslušných možností:

- **Zobrazova oznámenia v paneli úloh (štandardne zapnuté)** – štandardne sa zobrazujú všetky oznámenia. Ak chcete úplne vypnú zobrazovanie všetkých oznámení, zrušte za iarknutie tejto položky. Po zapnutí môžete alej vybra konkrétne oznámenia, ktoré sa majú zobrazova :
 - Oznámenia o **aktualizáciách** (*predvolene zapnuté*) – rozhodnite sa, i sa majú zobrazova informácie týkajúce sa spustenia aktualizácie **AVG AntiVirus 2014**, postupu a dokon enia
 - **Oznámenia o zmene stavu sú astí** (*predvolene vypnuté*) – rozhodnite sa, i sa majú zobrazova informácie týkajúce sa innosti alebo ne innosti sú asti, prípadne i sa majú zobrazova informácie o možnom probléme. Táto možnos má pri oznámení chybného stavu sú asti informa nú funkciu [ikony v paneli úloh](#), ktorá informuje o probléme týkajúcom sa sú asti produktu **AVG AntiVirus 2014**.
 - **Oznámenia automatického odstra ovania hrozieb Rezidentným štítom** (*predvolene zapnuté*) – rozhodnite sa, i sa majú alebo nemajú zobrazova informácie súvisiace s procesmi ukladania, kopírovania a otvárania súborov (*táto funkcia sa dá nastavi , len ke je v sú asti Rezidentný štít zapnutá možnos Lie i automaticky*).
 - **Oznámenia o kontrole** (*predvolene zapnuté*) – rozhodnite sa, i sa majú zobrazova informácie pri automatickom spustení plánu kontroly, jeho priebehu a výsledkoch
 - **Oznámenia súvisiace so sú as ou Kontrola pošty** (*predvolene zapnuté*) – rozhodnite sa, i sa majú zobrazova informácie po každej kontrole prichádzajúcich a odchádzajúcich e-mailových správ.

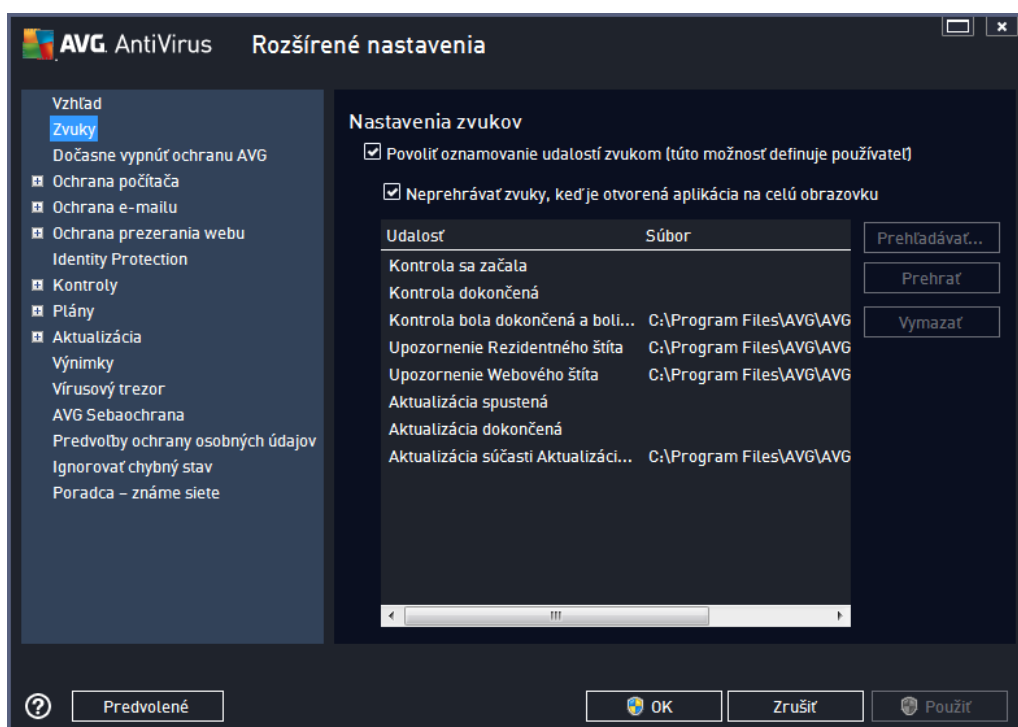
- **Štatistické oznámenia** (predvolene zapnuté) – nechajte políčko začiarknuté, ak sa majú zobrazovať pravidelné štatistické prehľadové oznámenia na paneli úloh.
- **Oznámenia o skrátení zavádzacieho času** (predvolene vypnuté) – rozhodnite sa, či chcete byť informovaní o skrátení zavádzacieho času systému.
- **Oznámenia súčasti AVG Advisor** (predvolene zapnuté) – rozhodnite sa, či sa informácie o aktivitách 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 **Povoli režim hrania, ak beží aplikácia v režime na celú obrazovku** označené (predvolené nastavenie).

9.2. Zvuky

Dialógové okno **Nastavenia zvukov** sa používa na zapnutie zvukových upozornení informujúcich o konkrétnych činnostiach programu **AVG AntiVirus 2014**:



Nastavenia sú platné iba pre aktuálny používateľský účet. To znamená, že používateľ na každom počítači bude mať vlastné zvukové nastavenia. Ak chcete povoliť zvukové oznámenia, nechajte označenú možnosť **Povoliť oznamovanie udalostí zvukom** (táto možnosť je štandardne zapnutá), aby ste aktivovali zoznam všetkých dôležitých činností, ale môžete označiť možnosť **Neprehrávať zvuky, keď je aktívna aplikácia na celú obrazovku**, ak chcete potlačiť zvukové

upozornenia v situáciách, keď by mohli vyrušovať (pozrite si tiež časť *Režim hry v kapitole [Rozšírené nastavenia/Vzhľad](#) v tomto dokumente).*

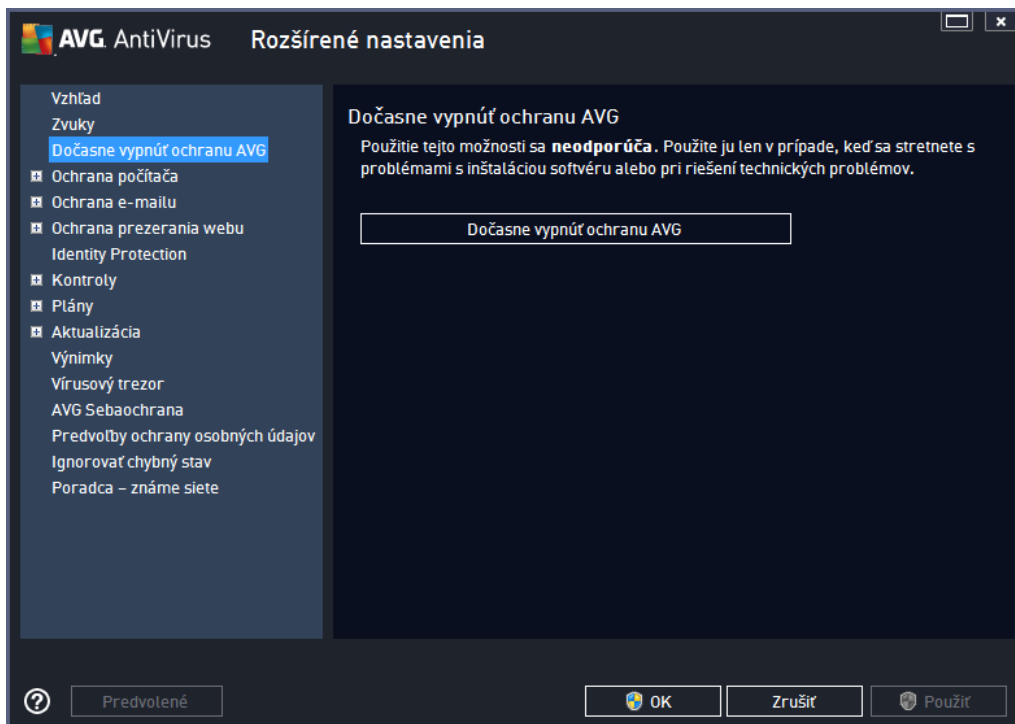
Ovládacie tlačidlá

- **Prehľadáva** ... – po označení príslušnej udalosti zo zoznamu pomocou tlačidla **Prehľadáva** nájdete na disku požadovaný zvukový súbor, ktorý chcete udalosti priradiť. (Všetky možnosti sú podporované iba zvukové formáty *.wav!)
- **Prehra** – ak si chcete vypnúť zvolený zvuk, zvýraznite udalosť v zozname a stlačte tlačidlo **Prehra**.
- **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 zabezpečenú programom **AVG AntiVirus 2014**.

Nepoužívajte túto možnosť, ak to nie je naozaj nevyhnutné!

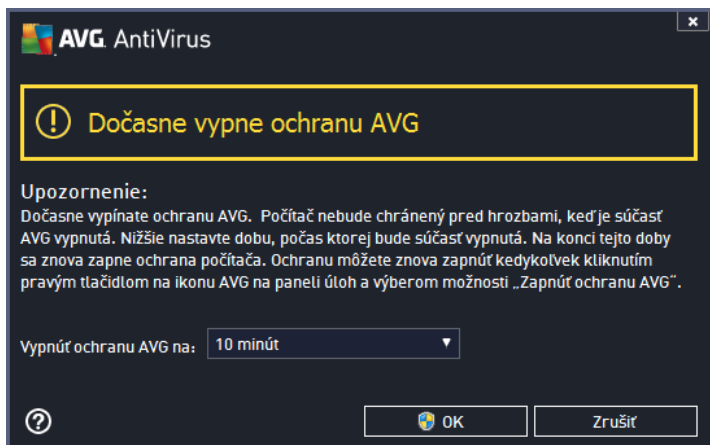


Vo väčšine prípadov **nie je potrebné** vypínať program **AVG AntiVirus 2014** pred inštaláciou nového softvéru alebo ovládačov, a to ani v prípade, ak inštalovaný program alebo sprievodca inštaláciou softvéru odporúča, aby sa najskôr zatvorili otvorené programy a aplikácie z dôvodu možného nežiaduceho prerušenia procesu inštalácie. Ak sa počas inštalácie vyskytne problém, skúste najprv vypnúť rezidentnú ochranu (*Povolíte sú časť **Rezidentný štít***). Ak musíte dočasne vypnúť ochranu **AVG AntiVirus 2014**, znova ju zapnete bezprostredne po dokončení úloh, pre ktoré ste ju vypli. Ak ste pripojení na internet alebo k sieti v momente, keď je antivírusový softvér vypnutý, váš počítač nie je

chránený pred útokmi.

Ako vypnú ochranu AVG

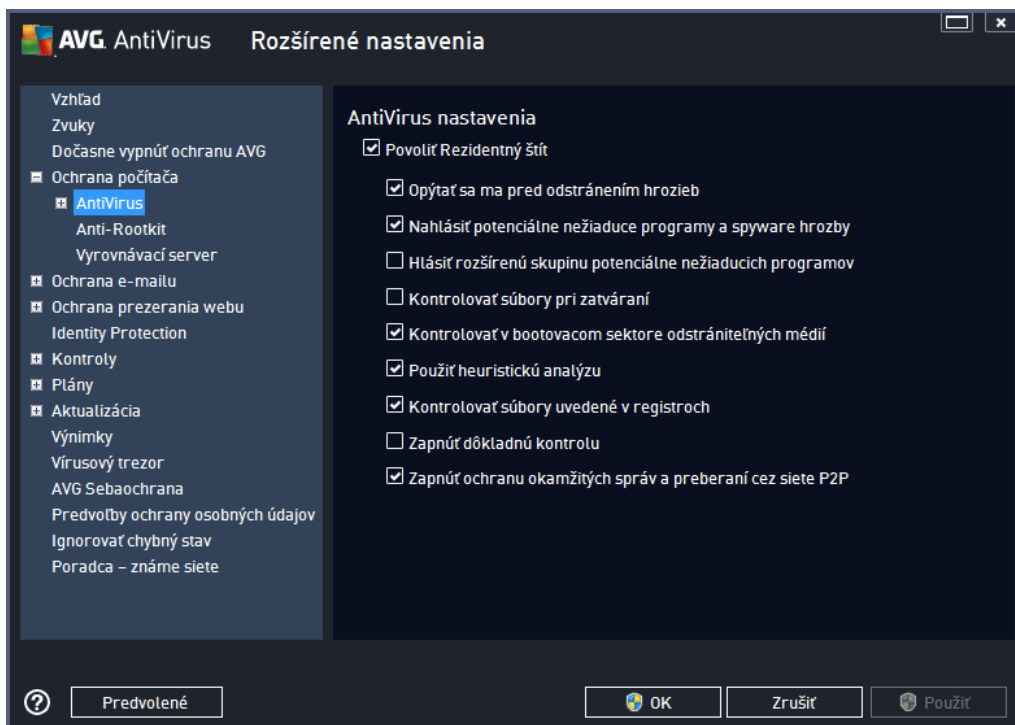
Označte začiarkavacie políčko **Dočasne vypnú ochranu AVG** a potvrdte vo bu stlačením tlačidla **Použiť**. V novootvorenom dialógovom okne **Dočasne vypnú ochranu AVG** zadajte čas, na aký chcete vypnúť aplikáciu **AVG AntiVirus 2014**. V predvolenom nastavení sa ochrana vypne na 10 minút, čo by malo 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).

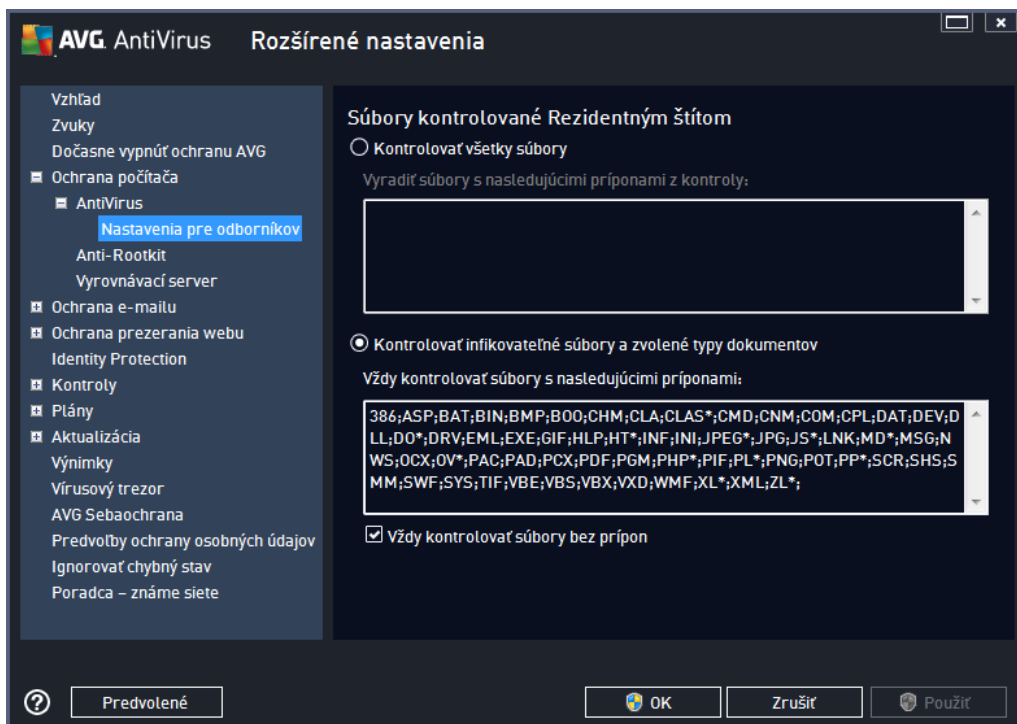


Dialógové okno **Nastavenia sú asti Rezidentný štít** umožňuje úplne aktívovať alebo vypnúť rezidentnú ochranu za iarknutím/zrušením za iarknutia položky **Povolí Rezidentný štít** (táto funkcia je štandardne zapnutá). Okrem toho môžete určiť, ktoré funkcie rezidentnej ochrany chcete aktívovať :

- **Opýtať sa pred odstránením hrozieb** (predvolene zapnuté) – za iarknite 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 neza iarknuté, **AVG AntiVirus 2014** bude automaticky liečiť infekcie, a ak to nebude možné, bude objekt premiestnený do [Vírusového trezora](#).
- **Nahlásiť potenciálne nežiaduce programy a spyware hrozby** (predvolene zapnuté) – za iarknite toto políčko, ak chcete aktívovať 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) – za iarknite 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 blokovать 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.

- **Kontrolova v bootovacom sektore odstránite ných médií** (predvolene zapnuté)
- **Použi heuristickú analýzu** (štandardne zapnuté) – na detekciu sa použije heuristická analýza (dynamická emulácia inštrukcií kontrolovaného objektu v prostredí virtuálneho počítača).
- **Kontrolova súbory uvedené v registroch** (štandardne zapnuté) – tento parameter určuje, že AVG bude kontrolovať všetky spustené súbory pridané do databázy Registry na spustenie pri štarte počítača, aby sa známa infekcia nemohla spustiť pri ďalšom spustení počítača.
- **Zapnú dôkladnú kontrolu** (štandardne vypnuté) – v určitých situáciách (napr. v stave mimoriadnej núdze) môžete za účelom zvýšenia bezpečnosti tohto políčka aktivovať algoritmus najdôkladnejšej kontroly, ktorý skontroluje všetky možné nebezpečné objekty do hĺbky. Upozorujeme však, že tento spôsob je náročný na procesor.
- **Zapnú ochranu okamžitých správ a preberaní cez sieť P2P** (predvolene zapnuté) – za účelom zvýšenia bezpečnosti môžete túto možnosť aktivovať, ak chcete overiť, že komunikácie cez okamžité správy (t. j. AIM, Yahoo!, ICQ, Skype, MSN Messenger, ...) a dáta prevzaté sieťami typu peer-to-peer (Sieť umožňuje priame pripojenie medzi klientmi bez serverov, ktoré môžu byť nebezpečné. Obyčajne sa používajú na zdieľanie hudobných súborov.) neobsahujú vírusy.

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



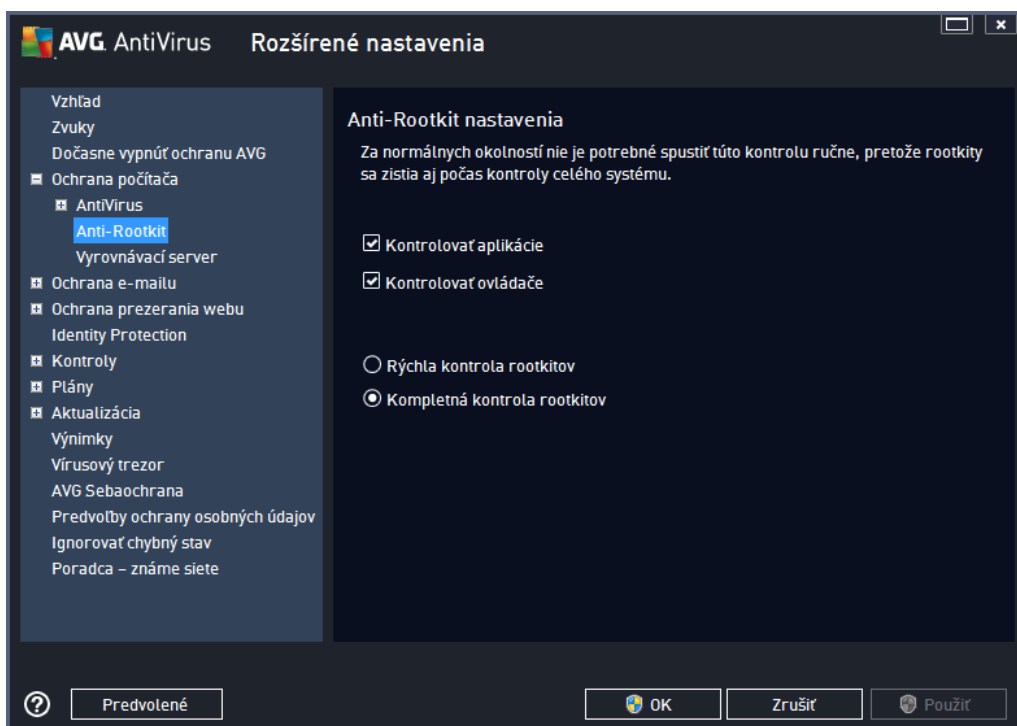
Označte príslušné začiarkavacie políčka podľa toho, či chcete použiť možnosť **Kontrolovať všetky súbory** alebo **Kontrolovať infikovateľné súbory a zvolené typy dokumentov**. Ak chcete urýchliť

kontrolu a sú asne zabezpe i maximálnu úrove ochrany, odporú ame zachova predvolené nastavenia. Takto sa budú kontrolova iba infikované súbory. V príslušnej asti dialógového okna nájdete aj upravený zoznam prípon súborov, ktoré sa majú za leni do kontroly.

Za iarknite možnos **Vždy kontrolova súbory bez prípon** (štandardne zapnutá) , ak má Rezidentný štít kontrolova aj súbory bez prípony a súbory neznámeho formátu. Odporú ame ma túto možnos zapnutú, pretože súbory bez prípon sú podozrivé.

9.4.2. Anti-Rootkit

V dialógovom okne **Nastavenia nástroja Anti-Rootkit** môžete upravi konfiguráciu služby **Anti-Rootkit** a konkrétne parametre kontroly. Kontrola nástrojom Anti-Rootkit je predvolený proces spustený pri [Kontrola celého počítača](#):

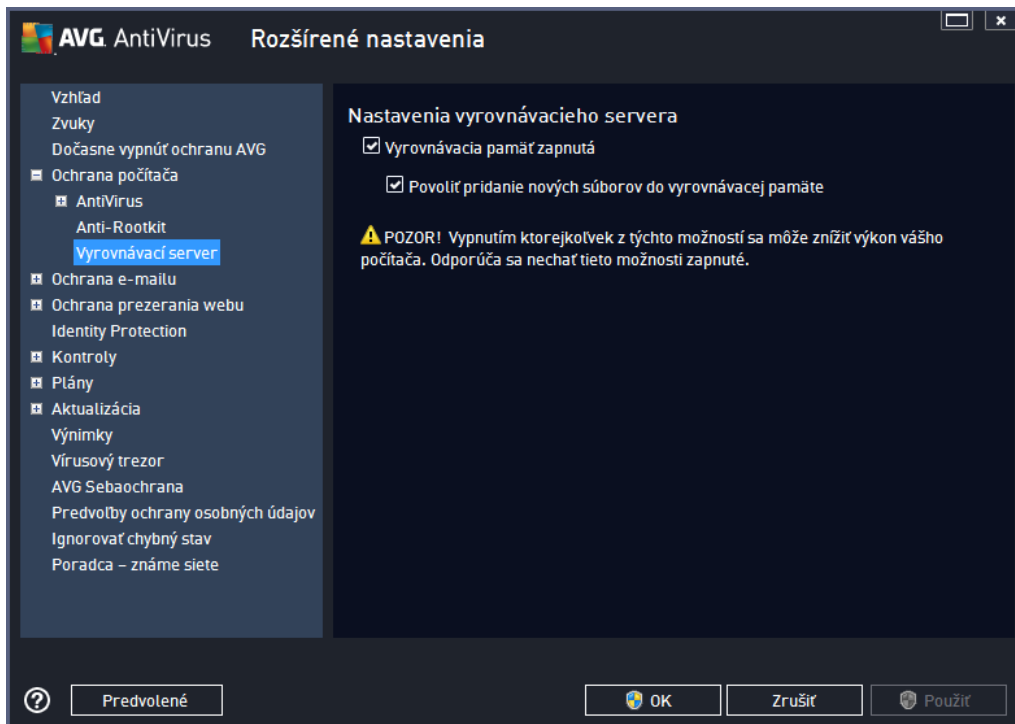


Možnosti **Kontrolova aplikácie** a **Kontrolova ovládače** vám umož ňujú podrobne zada ňovať, o by malo by sú asou kontroly Anti-Rootkit. Tieto nastavenia sú ur ené pre skúsených používateľov, odporú ame vám, aby ste nechali všetky možnosti zapnuté. Môžete tiež vybra režim kontroly rootkitov:

- **Rýchla kontrola rootkitov** – kontroluje všetky spustené procesy, zavedené ovládače a systémový prie inok (zvy ajne *c:\Windows*).
- **Úplná kontrola rootkitov** – kontroluje všetky spustené procesy, zavedené ovládače, systémový prie inok (oby ajne *c:\Windows*), plus všetky miestne disky (vrátane pamä ových 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 2014**:



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 po ich kontrole 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. Upozorujeme, 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 prídanie 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 zachovávajú a budú sa používať do úplného vypnutia funkcie vyrovnávacej pamäte, resp. do ďalšieho aktualizovania vírusovej databázy.

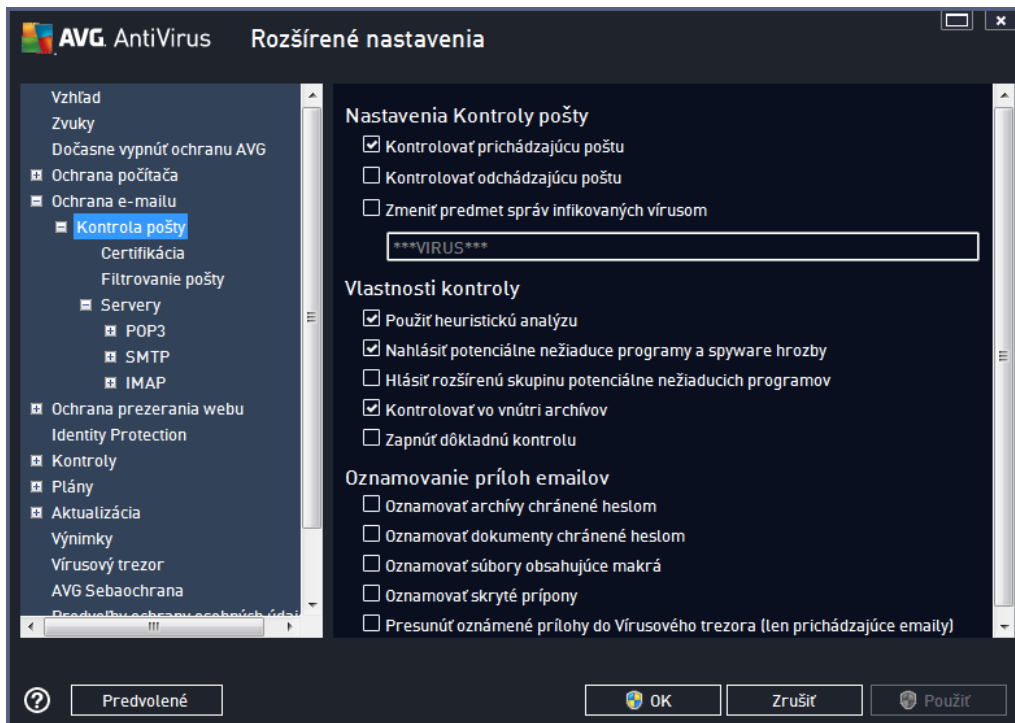
Ak nemáte oprávnený dôvod na vypnutie vyrovnávacieho servera, dôrazne odporúčame zachovať predvolené nastavenia a nechať obe možnosti zapnuté. Inak môžete zaznamenať výrazné spomalenie rýchlosti a výkonu systému.

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 zapnete resp. vypnete funkciu na kontrolu všetkých e-mailov doručených do vašej poštovej aplikácie
- **Kontrolovať odchádzajúcu poštu** (predvolene vypnuté) – začiarknutím zapnete resp. vypnete 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 prehradanej 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 prehradávať :

- **Použi 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](#).
- **Nahlási 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.
- **Hlási 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 blokovать dobré programy, a preto je táto funkcia štandardne vypnutá.
- **Kontrolova obsah vnútri archívov (štandardne zapnuté)** – začiarknite toto políčko, ak sa má kontrolovať obsah archívov priložených k e-mailovým správam.
- **Zapnú 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. Upozorujeme však, že tento spôsob je náročný na čas.

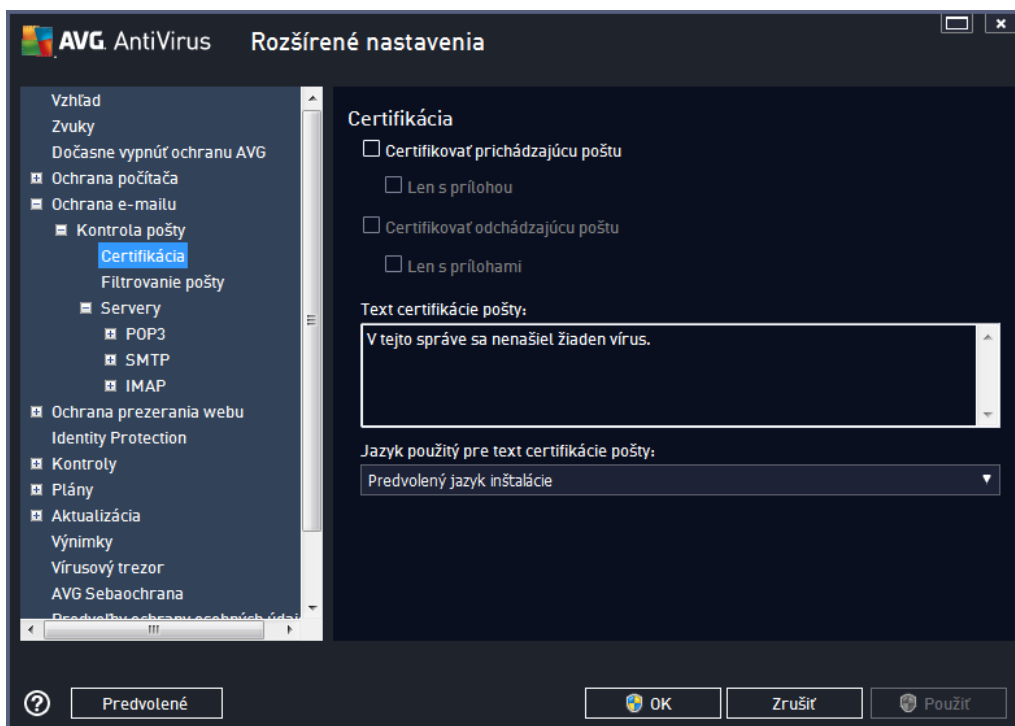
Oznamovanie príloh e-mailov

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](#):

- **Oznamova archívy chránené heslom** – archívy (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.
- **Oznamova dokumenty chránené heslom** – dokumenty chránené heslom sa nedajú skontrolovať na prítomnosť vírusov, začiarknite toto políčko, ak sa majú oznamovať tieto dokumenty ako potenciálne nebezpečné.
- **Oznamova 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.
- **Oznamova skryté prípony** – skrytá prípona môže spôsobiť, že sa bude podozrivý spustiteľný súbor „nie o.txt.exe“ javiť ako neškodný jednoduchý textový súbor „nie o.txt“; začiarknite toto políčko, ak sa majú tieto súbory oznamovať ako potenciálne nebezpečné.
- **Premiestni hlásené prílohy do Vírusového trezora** – nastavte, či si želáte by

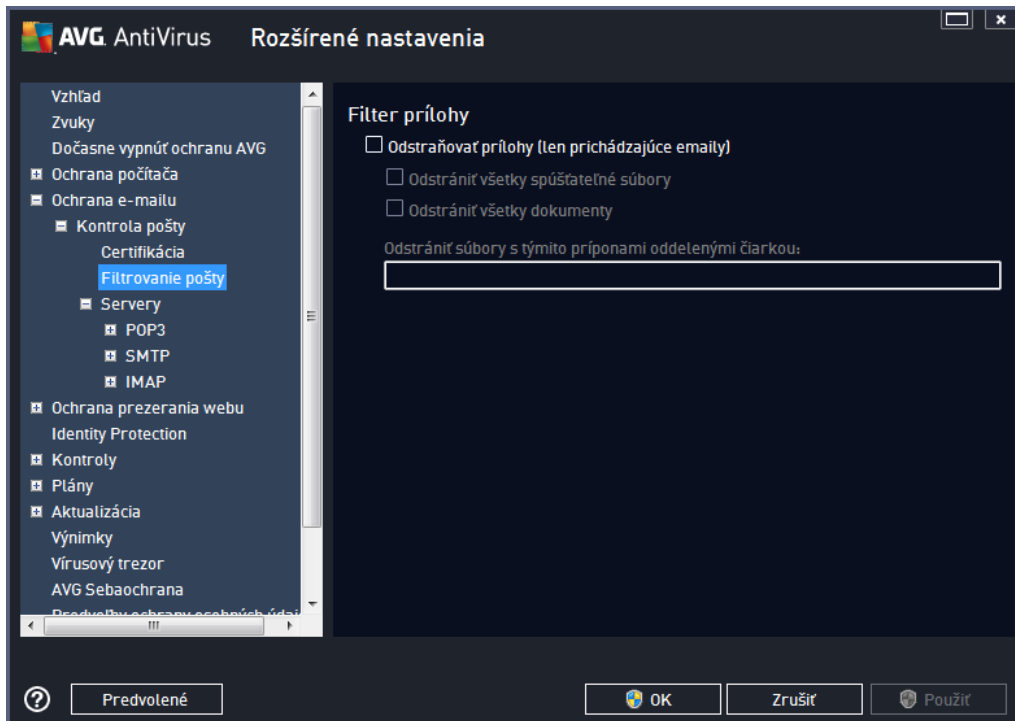
informovaní e-mailom o archívoch chránených heslom, dokumentoch chránených heslom, súboroch s makrami alebo súboroch so skrytou príponou, ktoré boli detegované ako príloha kontrolovanej e-mailovej správy. Ak sa má táto správa zobrazíť po as kontroly, potom nastavte, či sa má detegovaný infikovaný objekt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

V dialógovom okne **Certifikácia** môžete označiť konkrétne za iarkavacie políčka a určiť, či chcete certifikovať prichádzajúcu poštu (**Certifikovať prichádzajúcu poštu**) alebo odchádzajúcu poštu (**Certifikovať odchádzajúcu poštu**). Pri každej možnosti môžete tiež 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 políčka **Text e-mailovej certifikácie** napíšete požadovaný text certifikácie. V políčku **Jazyk použitý pre text certifikácie pošty** môžete tiež definovať, v akom jazyku sa má automaticky vytváraná správa certifikácie (*V tejto správe sa nenašiel žiadny vírus*) zobrazovať.

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



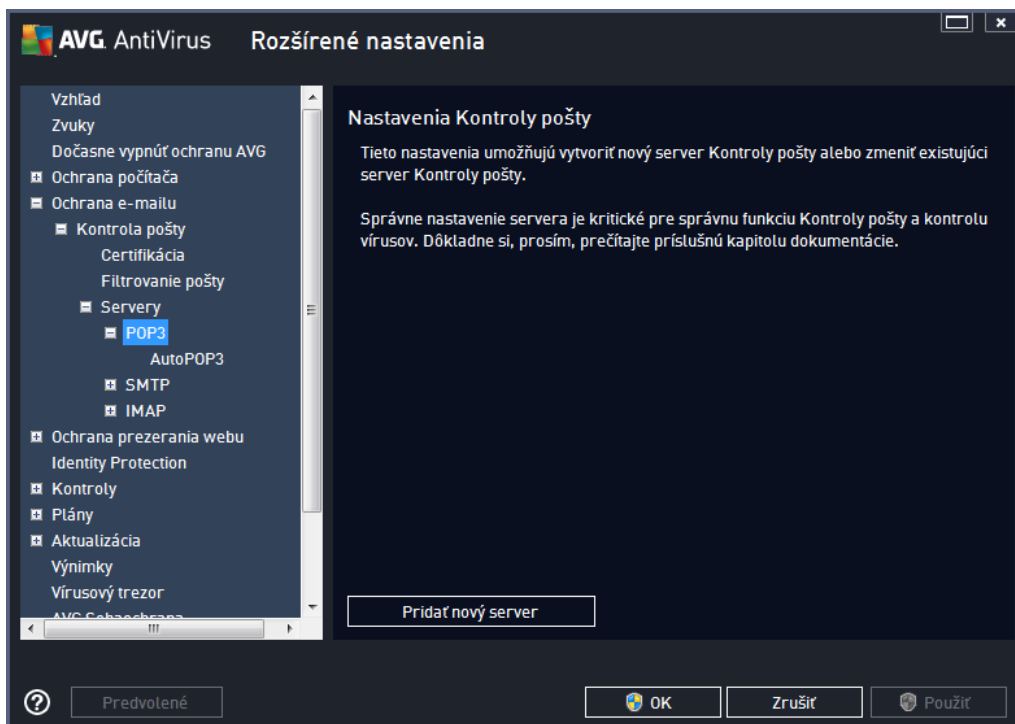
Dialógové okno **Filter príloh** umožňuje nastaviť parametre pre prehadzovanie príloh e-mailových správ. Štandardne je možnosť **Odstráni prílohy** vypnutá. Ak sa rozhodnete ju aktívovať, všetky prílohy emailových správ detegované ako infekcie alebo potenciálne nebezpečné programy sa automaticky odstránia.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

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

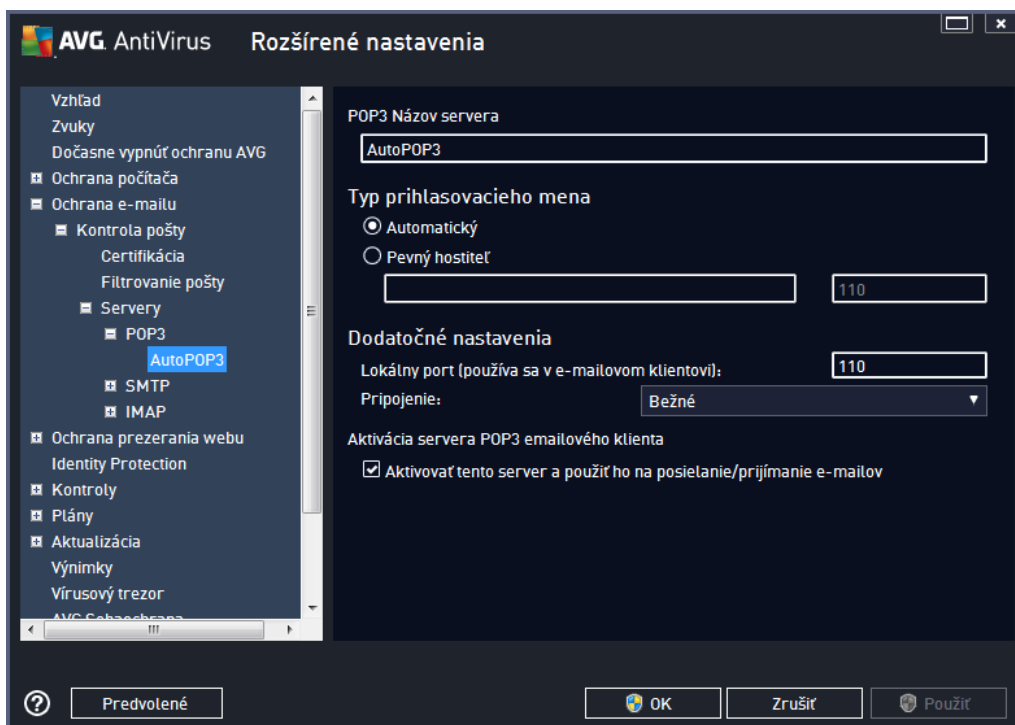
V nastavení **Servery** môžete upraviť parametre serverov súvisiaci s [Kontrolou pošty](#):

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

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



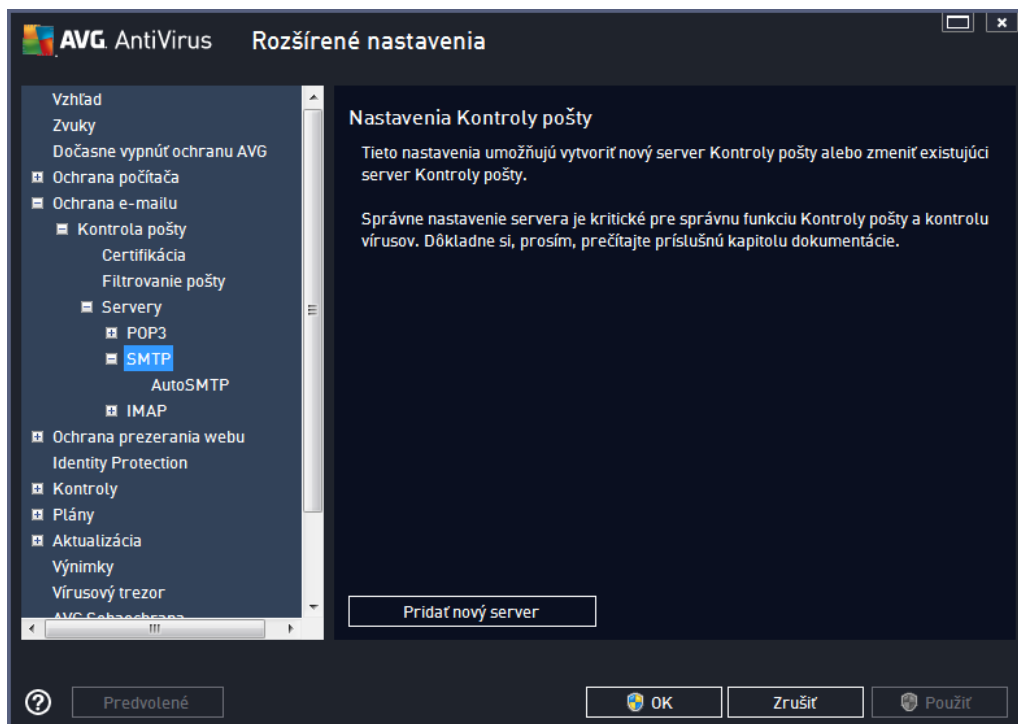
Toto dialógové okno umožní nastaviť pre súčasnú [Kontrolu pošty](#) nový server pomocou protokolu POP3 pre prichádzajúcu poštu:



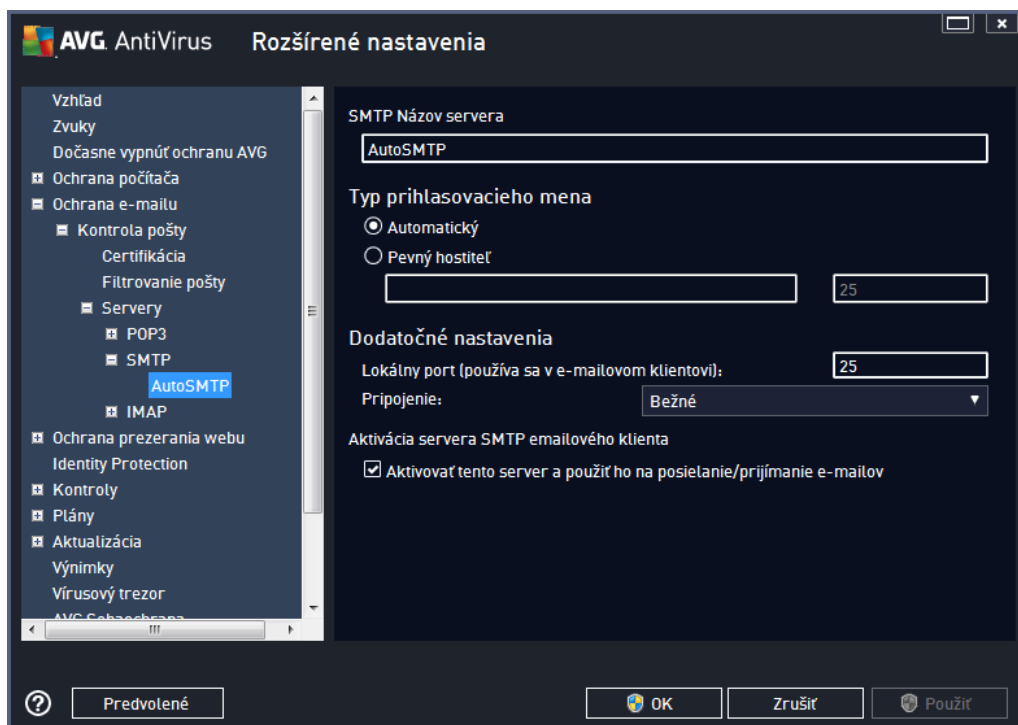
- **Názov servera POP3** – do tohto poľa zadajte názov novo pridaných serverov (na pridanie

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

- **Typ prihlásenia** – určuje spôsob zistenia poštového servera pre prichádzajúcu poštu:
 - **Automaticky** – prihlásenie sa uskutočňuje automaticky podľa nastavení poštovej aplikácie.
 - **Pevný hostiteľ** – v tomto prípade program vždy použije server, ktorý je tu uvedený. Zadáte 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 použijete dvojbodku ako oddeľovací znak (napríklad *pop.acme.com:8200*). Štandardný port pre komunikáciu POP3 je 110.
- **Dodatkové nastavenia** – uvádza podrobnejšie parametre:
 - **Lokálny port** – určuje port, na ktorom sa uskutočňuje 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 posielať dáta šifrované a žiadna tretia strana ich nebude môcť vypočítať ani monitorovať. Táto funkcia je dostupná len vtedy, keď ju podporuje cieľový poštový server.
- **Aktivácia servera POP3 v poštovej aplikácii** – označením/zrušením označenia tejto položky sa aktivuje, resp. deaktivuje uvedený server POP3



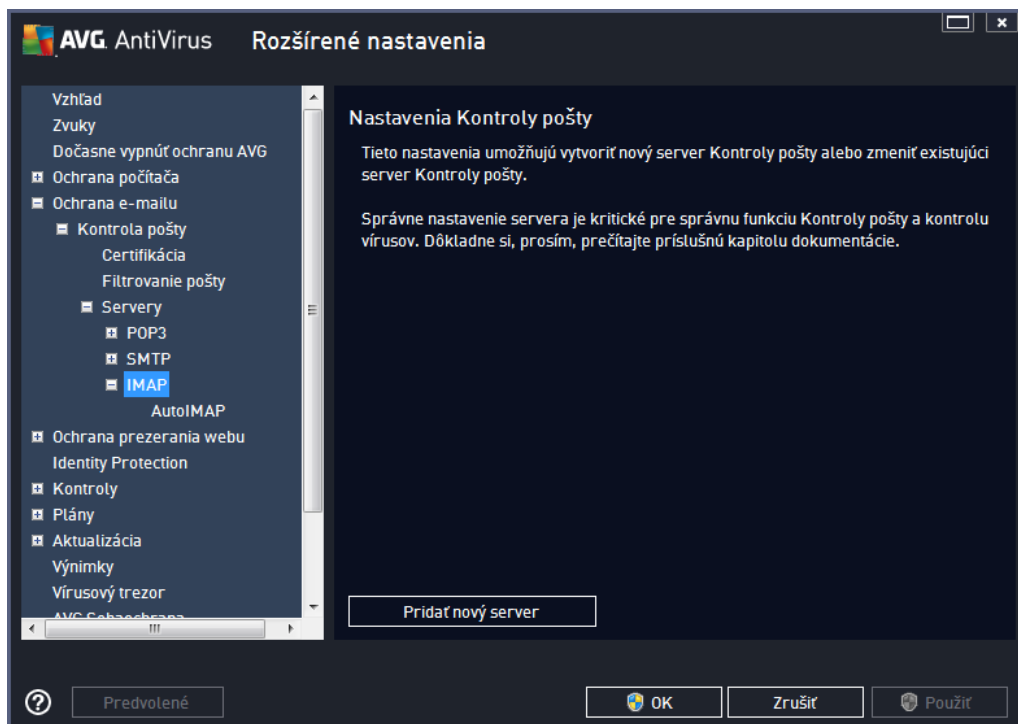
Toto dialógové okno umožní nastaviť pre súčasnú [Kontrolu pošty](#) nový server pomocou protokolu SMTP pre odchádzajúcu poštu:



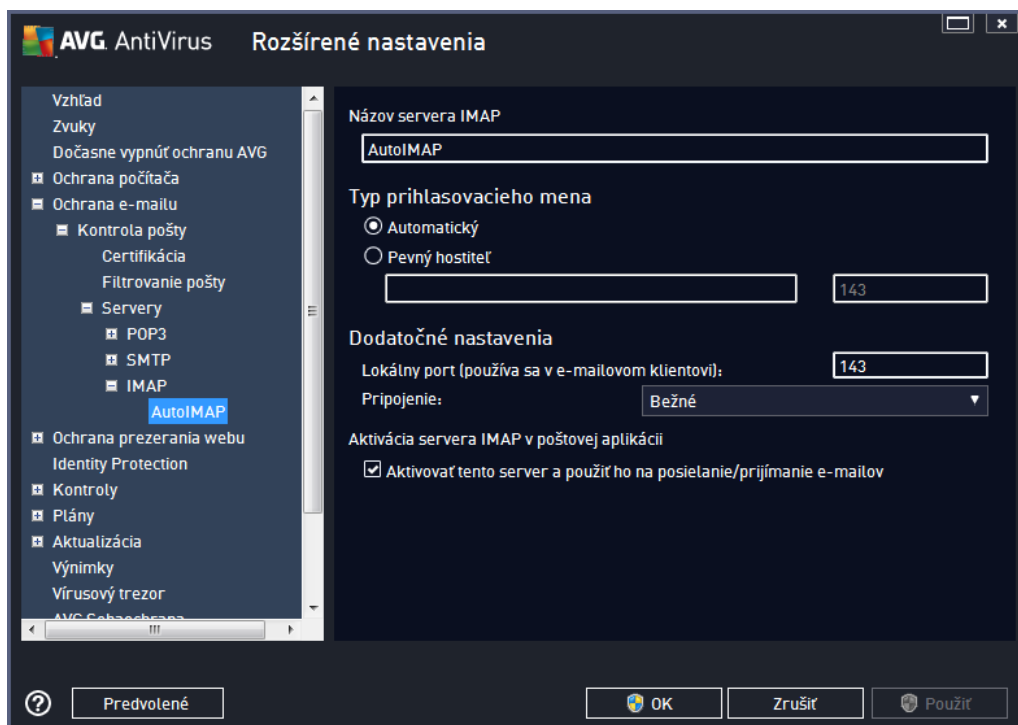
- **Názov servera SMTP** – do tohto poľa zadajte názov novo pridaných serverov (na pridanie

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

- **Typ prihlásenia** – určuje spôsob zistenia poštového servera, ktorý sa používa pre odchádzajúcu poštu:
 - **Automaticky** – prihlásenie sa uskutočňuje automaticky podľa nastavení poštovej aplikácie.
 - **Pevný hosť** – v tomto prípade program vždy použije server, ktorý je tu uvedený. Zadáte 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 použijete dvojbodku (napríklad *smtp.acme.com:8200*). Štandardný port komunikácie SMTP je 25.
- **Dodatkové nastavenia** – uvádza podrobnejšie parametre:
 - **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 posielať dáta šifrované a žiadna tretia strana ich nebude môcť vypočítať ani monitorovať. Táto funkcia je dostupná len vtedy, keď ju podporuje cieľový poštový server.
- **Aktivácia servera SMTP v poštovej aplikácii** – začiarknutím alebo zrušením začiarknutia tohto políčka sa aktivuje, resp. deaktivuje uvedený server SMTP



Toto dialógové okno umožní nastaviť pre súčasnú [Kontrolu pošty](#) nový server pomocou protokolu IMAP pre odchádzajúcu poštu:



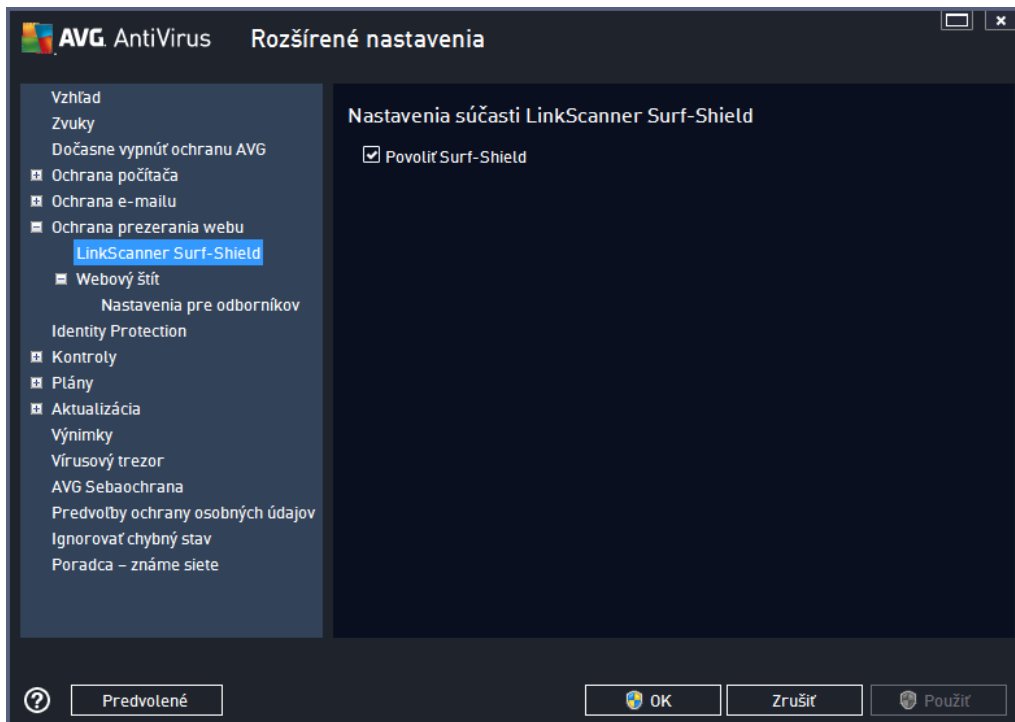
- **Názov servera IMAP** – do tohto poľa zadajte názov novo pridaných serverov (na pridanie

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

- **Typ prihlásenia** – určuje spôsob zistenia poštového servera, ktorý sa používa pre odchádzajúcu poštu:
 - **Automaticky** – prihlásenie sa uskutočňuje automaticky podľa nastavení poštovej aplikácie.
 - **Pevný hosť** – v tomto prípade program vždy použije server, ktorý je tu uvedený. Zadáte 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 oddeľovacieho znaku (napríklad *imap.acme.com:8200*). Štandardný port pre komunikáciu IMAP je 143.
- **Dodatkové nastavenia** – uvádza podrobnejšie parametre:
 - **Lokálny port používaný v** – určuje port, na ktorom sa uskutočňuje 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.
- **Aktivácia servera IMAP v poštovej aplikácii** – začiarknutím alebo zrušením začiarknutia tohto políčka sa aktivuje, resp. deaktivuje uvedený server IMAP.

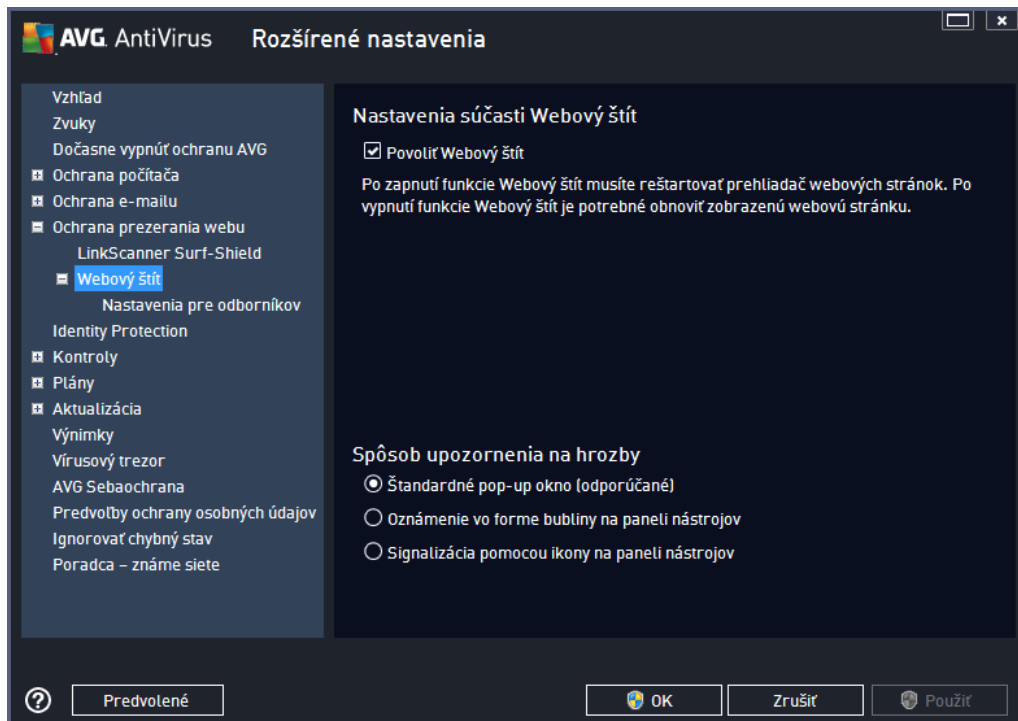
9.6. Ochrana prezerania webu

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



- **Povoliť Surf-Shield** – (predvolené 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 otvorení v internetovom prehliadači (alebo inej aplikácii, ktorá používa protokol HTTP).
- **Pridať „Zabezpečené sú správy od LinkScanner“...** – (predvolené vypnuté): potvrdením tejto možnosti zaistíte, že všetky správy odoslané zo sociálnych sietí Facebook/MySpace obsahujúce aktívne hypertextové odkazy budú obsahovať potvrdenie, že boli skontrolované súčasti LinkScanner.

9.6.1. Webový štít

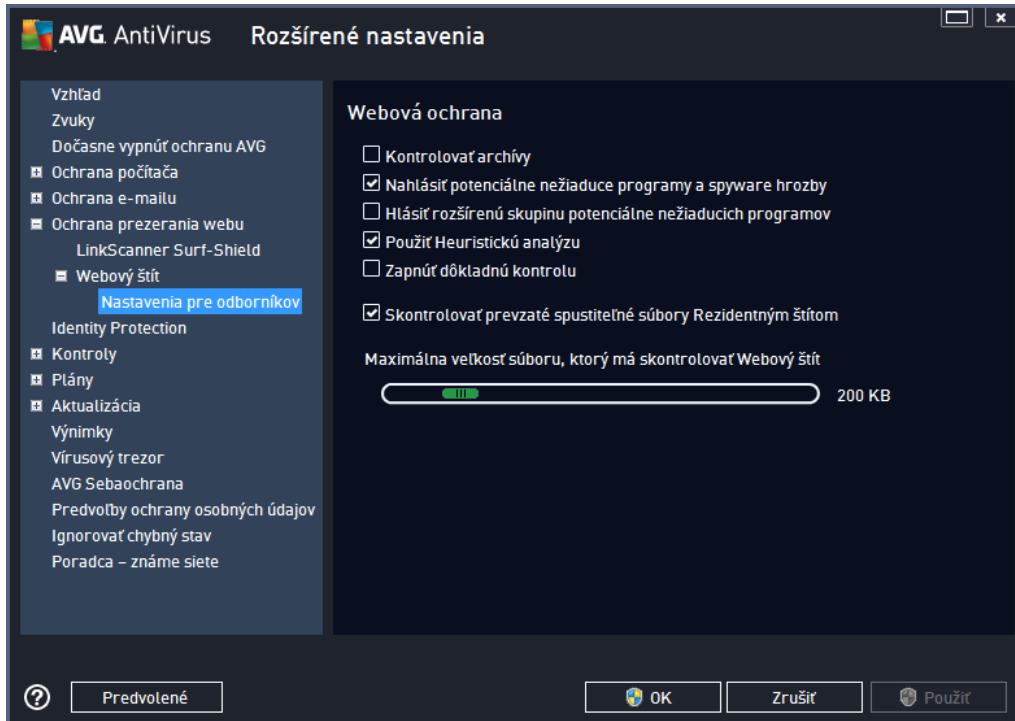


Dialógové okno **Webový štít** ponúka tieto možnosti:

- **Povoli Webový štít** (štandardne zapnuté) – aktivuje/deaktivuje celú službu **Webový štít**.
alšie rozšírené nastavenia sú v časti **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 informáciou o hrozbe pomocou 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:

- **Kontrolovať archívy** – (predvolené vypnuté): kontrolovať obsah archívov, ktoré sa môžu nachádzať na otvorenej internetovej stránke.
- **Nahlásiť potenciálne nežiaduce programy a spyware hrozby** – (predvolené zapnuté): zaškrtnite toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu malware: 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** – (predvolené vypnuté): zaškrtnite, 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 blokovать dobré programy, a preto je táto funkcia predvolené vypnutá.
- **Použiť heuristickú analýzu** – (predvolené zapnuté): kontrolovať obsah zobrazenej stránky pomocou metódy heuristickej analýzy (*dynamickéj emulácie inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí*).
- **Zapnúť dôkladnú kontrolu** – (predvolené 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. Upozorujeme však, že tento spôsob je

náro ný na as.

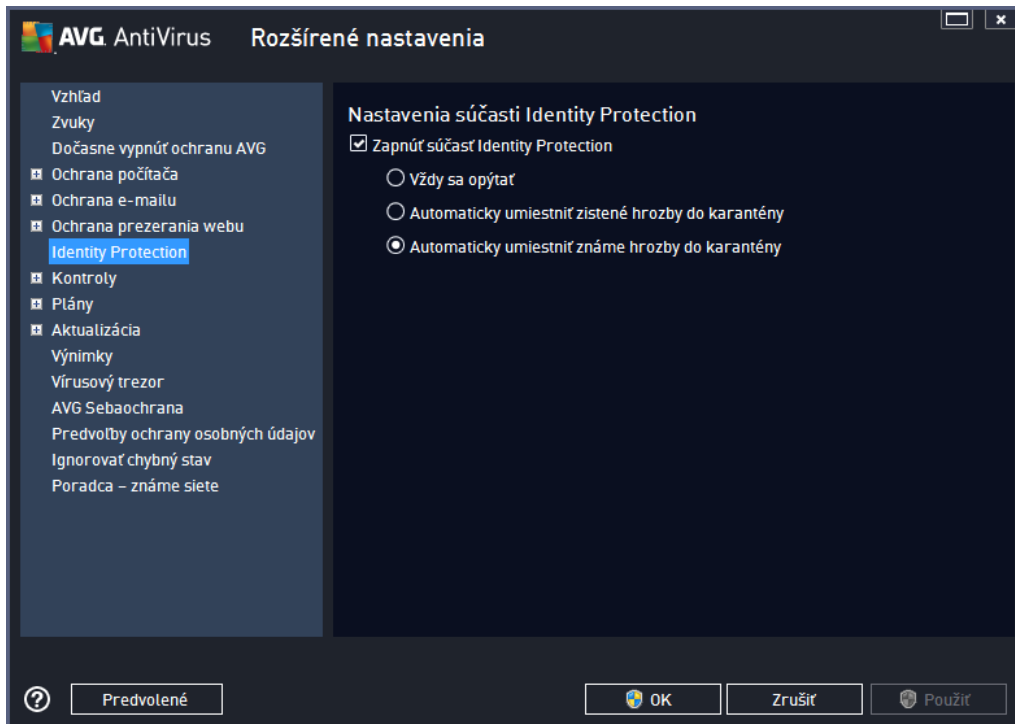
- o **Kontrolova prevzaté spustite né súbory Rezidentným štítom** – (predvolene zapnuté): kontrolova spustite né súbory (obvykle súbory s príponami exe, bat, com) po ich prevzatí. Rezidentný štít kontroluje súbory pred prevzatím, aby zabezpečil, že sa žiadny škodlivý kód nedostane do vášho počítača. Táto kontrola je však obmedzená **Maximálnou iastkovou ve kos ou kontrolovaného súboru** – pozrite si nasledujúcu položku v tomto dialógovom okne. Preto sú všetky súbory kontrolované po nastavení, a to isté platí aj pre vašu šínu spustiteľných súborov. Spustiteľné súbory môžu vo vašom počítači vykonávať rôzne úlohy, a preto je nevyhnutne nutné, aby boli na 100 % bezpečné. To je možné zabezpečiť kontrolou súboru pred jeho prevzatím a taktiež kontrolou ihne po dokončení prevzatia súboru. Odporúčame vám ponechať túto možnosť zaškrtnutú. Ak túto možnosť deaktivujete, stále môžete byť pokojní, že AVG nájde akýkoľvek potenciálne škodlivý kód. Len obvykle nebude schopný posúdiť spustiteľný súbor ako celok, takže môže ohlasovať niekedy nesprávnych detekcií.

Posúva v dolnej časti dialógového okna vám umožňuje určiť **Maximálnu iastkovú ve kos 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 prevzatie z internetovej stránky sa môže výrazne spomaliť. Pomocou posúvača môžete nastaviť maximálnu veľkosť súboru, ktorá sa má kontrolovať súčasne s **Webovým štítom**. Aj keď je prevzatý súbor väčší než nastavená hodnota a z tohto dôvodu ho súčasne Webový štít neskontroluje, váš počítač je stále chránený: ak je súbor infikovaný, súčasne **Rezidentný štít** ho ihne deteguje.

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 (predvolené 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** (predvolené 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 pod a konkrétnych typov kontroly definovaných dodávateľom softvéru:

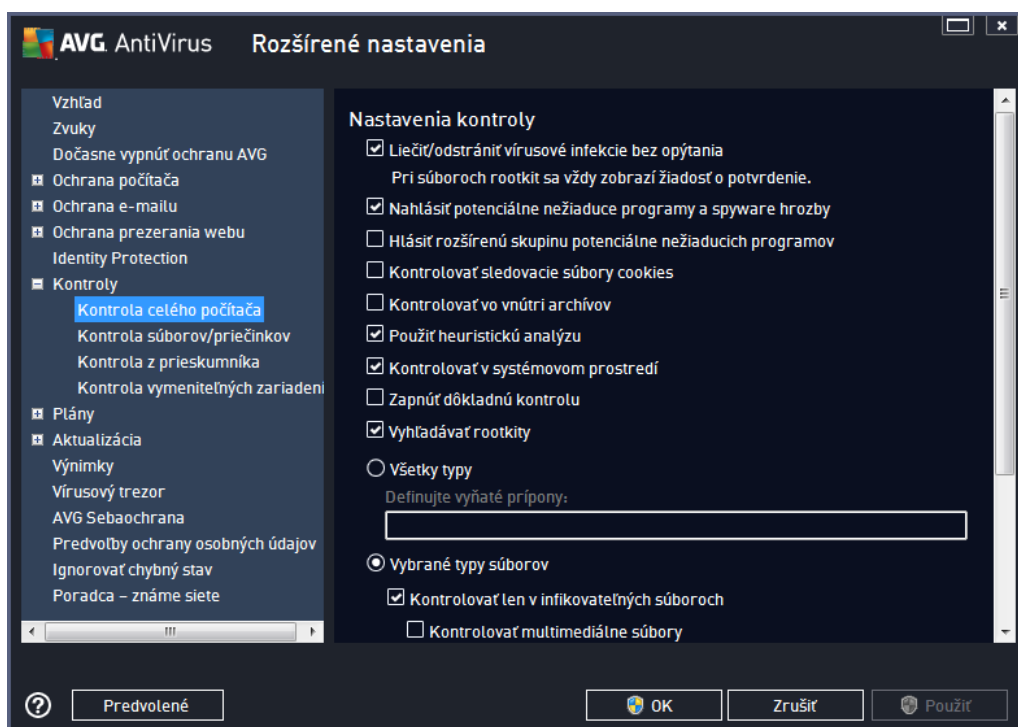
- [Kontrola celého počítača](#) – štandardná vopred definovaná kontrola celého počítača.
- [Kontrola súborov/priečinkov](#) – štandardná vopred definovaná kontrola vybraných oblastí

po íta a.

- [Kontrola z prieskumníka](#) – špeciálna kontrola vybraného objektu priamo v prostredí programu Windows Explorer.
- [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 výrobcami softvéru, [Kontrola celého počítača](#):



Nastavenia kontroly

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

- **Liečiť/odstrániť infekciu bez opýtania** (štandardne zapnuté) – ak sa počas kontroly zistí prítomnosť vírusu, môže sa automaticky vylíčiť, ak je k dispozícii liečba. Ak nie je možné infikovaný súbor vylíčiť automaticky, premiestni sa do [Vírusového trezora](#).
- **Nahlásiť potenciálne nežiaduce programy a spyware hrozby** (štandardne zapnuté) – zašiarke toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu malwaru: 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.

- **Hlási rozšírenú skupinu potenciálne nežiaducich programov** (štandardne vypnuté) – za iarknite toto polí ko, ak sa má detegova rozšírená skupina spywaru: programov, ktoré sú úplne v poriadku a neškodné, ke sa získajú priamo od výrobcu, ale neskôr sa dajú zneuži na škodlivé ú ely. Toto je alšie opatrenie, ktoré ešte viac zvyšuje úrove zabezpe enia po íta a, ale môže blokovat dobré programy, a preto je táto funkcia štandardne vypnutá.
- **Kontrolova sledovacie súbory cookies** (štandardne vypnuté) – tento parameter sú asti zapína detekciu súborov cookies (*HTTP cookies sa používajú na overenie totožnosti, sledovanie a správu konkrétnych informácií o používate och, akými sú napr. preferencie stránok alebo obsah elektronických nákupných košíkov*).
- **Kontrolova vo vnútri archívov** (štandardne vypnuté) – tento parameter ur uje, že sa majú po as kontroly preverova všetky súbory uložené vnútri archívov, napr. ZIP, RAR, ...
- **Použi heuristickú analýzu** (štandardne zapnuté) – heuristická analýza (*dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom po íta ovom prostredí*) bude jednou z metód, ktoré sa použijú na detegovanie vírusov po as kontroly.
- **Kontrolova v systémovom prostredí** (štandardne zapnuté) – po as kontroly sa overujú systémové oblasti po íta a.
- **Zapnú dôkladnú kontrolu** (štandardne vypnuté) – v ur itých situáciách (*podozrenie na infikovanie po íta a*) môžete touto možnos ou aktivova najdôkladnejšie kontrolné algoritmy, ktoré pre istotu skontrolujú aj tie oblasti po íta a, ktoré sa oby ajne vôbec neinfikujú. Upozor ujeme však, že tento spôsob je náro ný na as.
- **Kontrolova rootkity** (štandardne zapnuté) – [Anti-Rootkit](#) skontroluje po íta a zis uje prítomnos potenciálnych rootkitov, t. j. programov a technológií, ktoré dokážu zakry innos malwaru v po íta i. Ke program deteguje rootkit, nemusí to nevyhnutne znamena , že je po íta infikovaný. V niektorých prípadoch sa môžu ur ité ovláda e alebo asti bežných aplikácií nesprávne ozna i ako rootkity.

Mali by ste tiež ur i , o chcete kontrolova

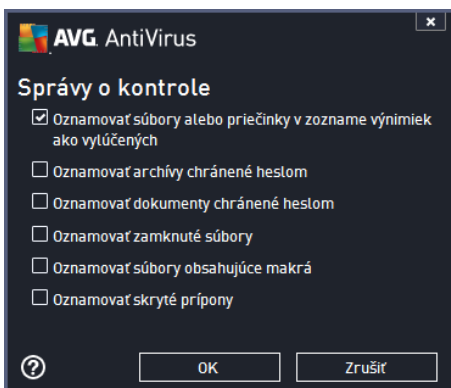
- **Všetky typy súborov** s možnos ou definova výnimky z preh adávania vytvorením zoznamu iarkou oddelených (*uložením sa iarky zmenia na bodko iarky*) prípon súborov, ktoré sa nemajú preh adáva .
- **Vybrané typy súborov** – môžete nastavi , aby sa kontrolovali len súbory, pri ktorých existuje pravdepodobnos infikovania (*súbory, ktoré nemôžu by napadnuté infekciou, napríklad niektoré jednoduché textové súbory alebo niektoré nespustite né súbory, sa nebudú kontrolova*), vrátane mediálnych súborov (*video, audio súborov – ak necháte toto polí ko neza iarknuté, potom sa as preh adávania skrátí ešte viac, pretože tieto súbory sú asto ve mi ve ké, pri om pravdepodobnos napadnutia vírusom je ve mi malá*). Znova môžete definova , pod a prípony, ktoré súbory sa majú kontrolova vždy.
- Alternatívne môžete rozhodnú , že chcete **kontrolova súbory bez prípony**. Táto možnos je štandardne zapnutá a odporú ame vám, aby ste toto nastavenie nikdy nemenili, ak na to nemáte skuto ný dôvod. Súbory bez prípony sú skôr podozrivé a mali by sa vždy kontrolova .

Nastavi rýchlos dokon enia kontroly

V asti **Nastavi rýchlos dokon enia kontroly** môžete alej nastavi požadovanú rýchlos kontroly v závislosti od využívania systémových zdrojov. Štandardne má tento parameter nastavenú úroveň automatického využívania zdrojov „*pod a používate a*“. Ak chcete, aby prehadávanie prebiehalo rýchlejšie, potom bude trvať kratšie, ale výrazne sa zvýši využívanie systémových zdrojov a spomalí 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 predžením doby trvania kontroly.

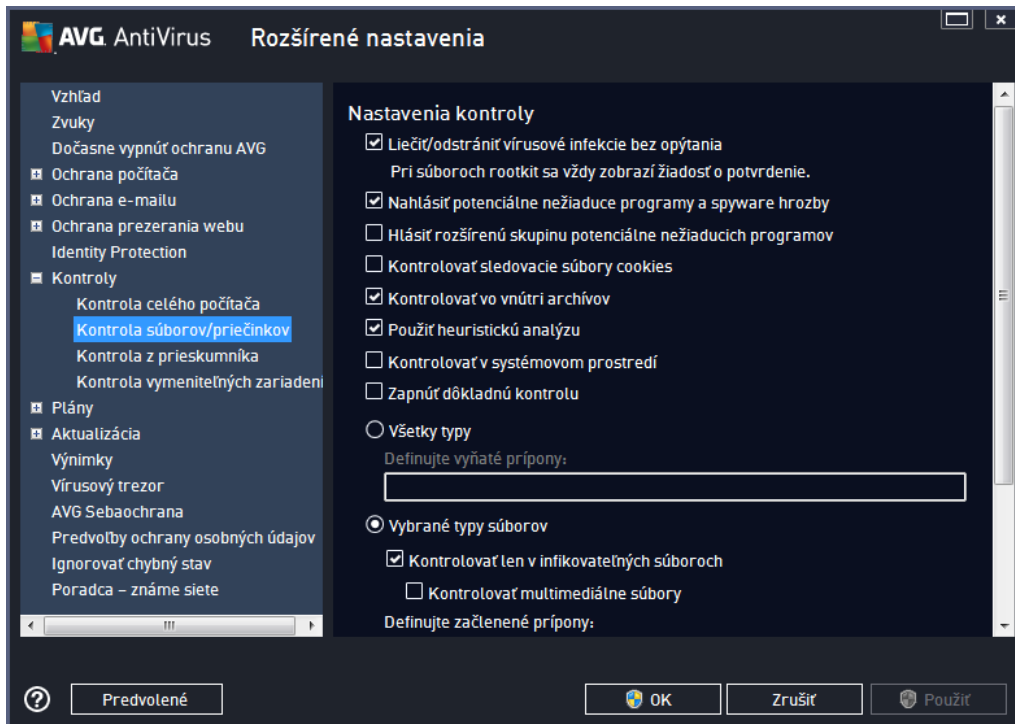
Vytvorí ďalšie správy o kontrole...

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



9.8.2. Kontrola súborov/priečinkov

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

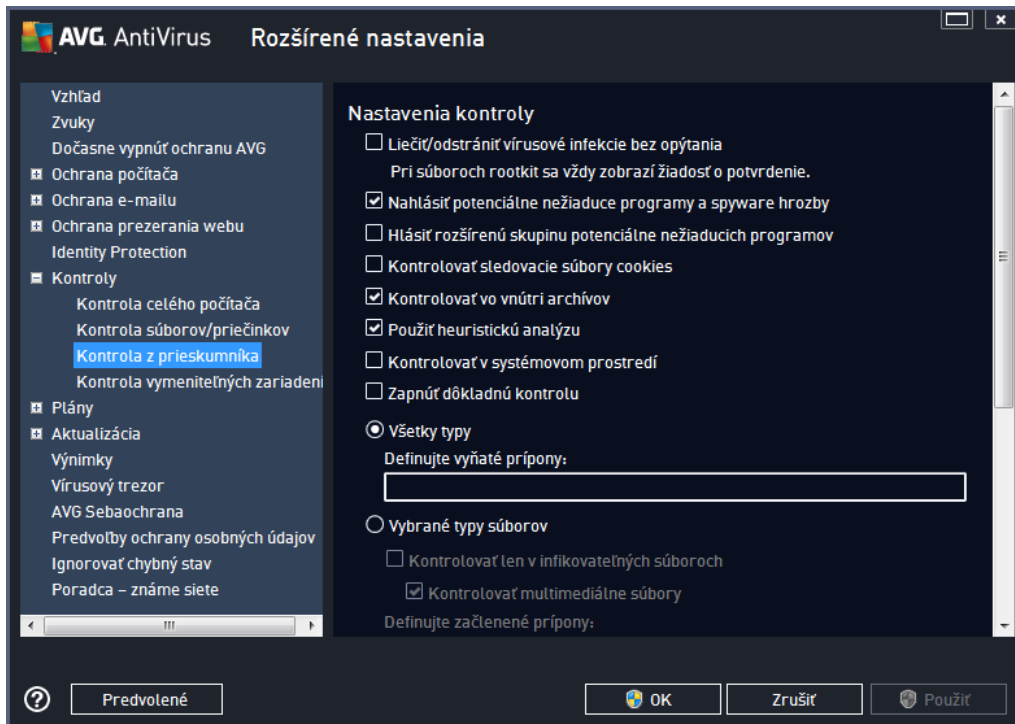


Všetky parametre nastavené v tomto dialógovom okne konfigurácie sa vzťahujú len na oblasti vybrané na kontrolu v dialógovom okne [Kontrola súborov/priečinkov](#)!

Poznámka: Informácie o konkrétnych parametroch nájdete v kapitole [Rozšírené nastavenia AVG / 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 domény softvéru. V tomto prípade súvisí konfigurácia s [kontrolou konkrétnych objektov spustených v prostredí programu Windows Explorer \(prieskumník\)](#), pozri kapitolu [Kontrola z prieskumníka](#):



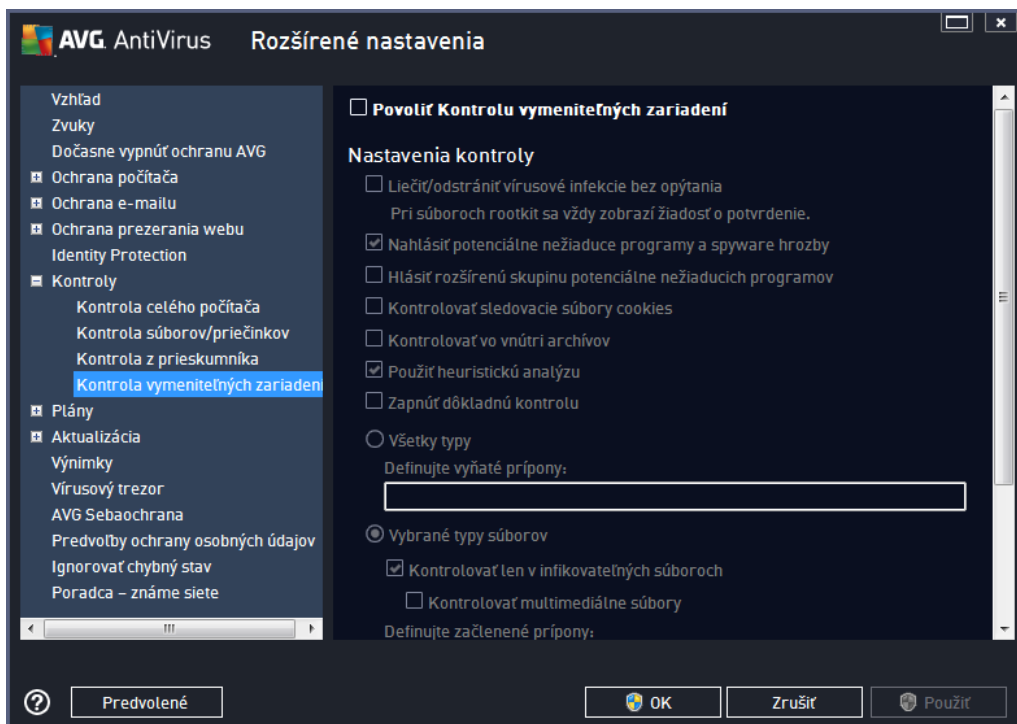
Zoznam parametrov je identický s parametrami dostupnými pre [Kontrolu celého počítača](#). Predvolené nastavenia sa však líšia (napríklad *Kontrola celého počítača* a štandardne nekontroluje archívy, ale kontroluje systémové prostredie, zatiaľ čo *Kontrola z prieskumníka* má presne opačné nastavenia).

Poznámka: Informácie o konkrétnych parametroch nájdete 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 **alšie 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** je tiež veľmi podobné 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 nájdete v kapitole [Rozšírené nastavenia AVG / Kontroly / Kontrola celého počítača](#).

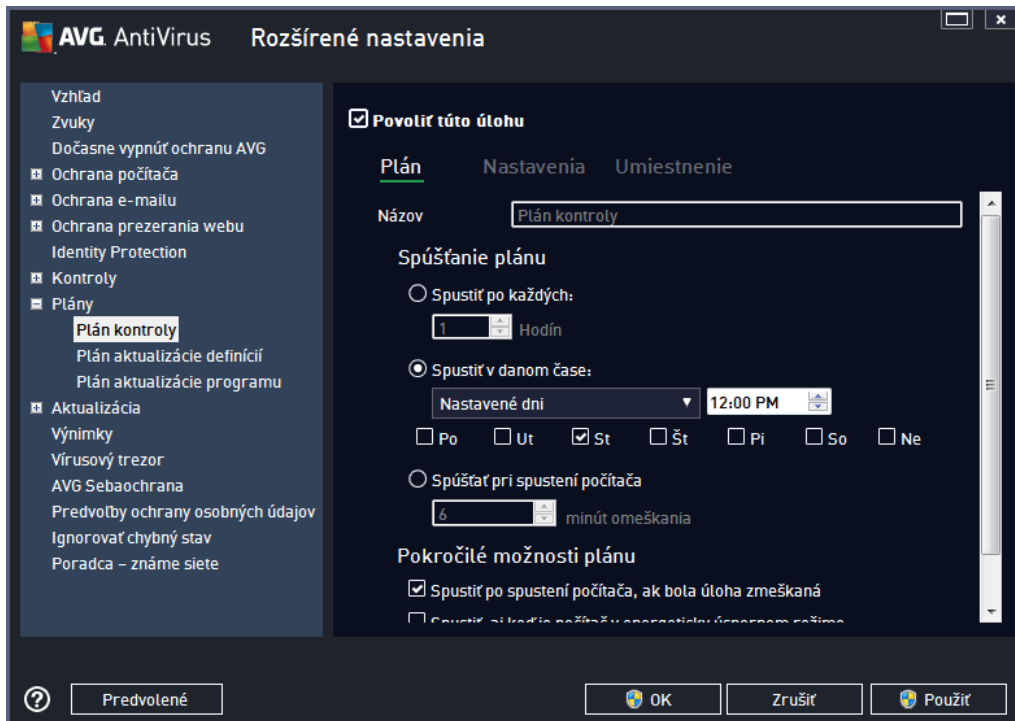
9.9. Plány

V sekcii **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 začíname kliknutím, resp. zrušením začíname kliknutia položky **Povoliť túto úlohu dočasne vypnúť naplánovaný test a znova ho zapnúť, keď je potrebný**:



Vo vedľajšom textovom poli **Názov** (neaktívne pre všetky predvolené plány) sa nachádza názov, ktorý tomuto konkrétnemu plánu prideliť dodávateľ programu. Pre novopridané plány (nový plán sa pridá kliknutím pravým tlačidlom myši nad položkou **Plán kontroly** v akejkoľvek 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 odlišiť.

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 definovať tieto parametre kontroly:

Spúšťanie naplánovaných úloh

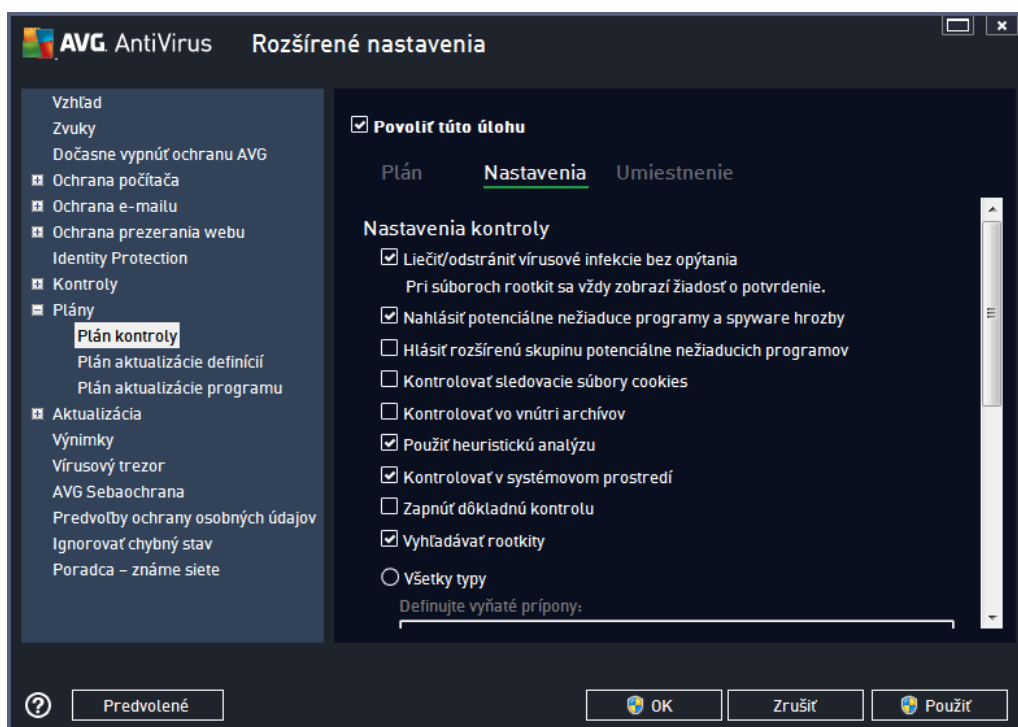
Tu môžete nastaviť časové intervaly pre novonaplánované spustenie kontroly. Každé spúšťanie sa definuje ako opakované spúšťanie kontroly po uplynutí určitého času (**Spustiť po každých ...**), definovaním presného dátumu a času (**Spúšťať v konkrétnom časovom intervale ...**), prípadne definovaním udalosti, 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 po ťa v úspornom režime alebo úplne vypnutý. Ke sa spustí naplánovaná kontrola v nastavenom ase, bude vás o tom informova 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 pozastavi alebo dokonca úplne zastavi prebiehajúcu kontrolu a zároveň zmení prioritu práve spustenej kontroly.



V karte **Nastavenia** nájdete zoznam parametrov kontrolovania, ktoré sa dajú volite ne zapnú /vypnú . Štandardne je väčšina parametrov zapnutá a príslušná funkcia sa použije počas kontroly. **Ak nemáte závažný dôvod meniť tieto nastavenia, odporujeme 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 malwaru: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporujeme vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
- **Hlásť 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

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

- **Kontrolova 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*).
- **Kontrolova 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 používajú na detekciu vírusov počas kontroly.
- **Kontrolova v systémovom prostredí** (štandardne zapnuté) – počas kontroly sa budú overovať aj systémové oblasti počítača.
- **Zapnú 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. Upozorujeme však, že tento spôsob je náročný na procesor.
- **Kontrolova rootkity** (štandardne zapnuté) – kontrola súčasti Anti-Rootkit skontroluje počítača a zisťuje prítomnosť potenciálnych rootkitov, t. j. programov a technológií, ktoré dokážu zakryť malwaru v počítači. Keď program deteguje rootkit, nemusí to nevyhnutne znamenať, že je počítač infikovaný. V niektorých prípadoch sa môžu určitým spôsobom ovládať alebo súčasti bežných aplikácií nesprávne označovať ako rootkity.

Mali by ste tiež určiť, čo chcete kontrolovať

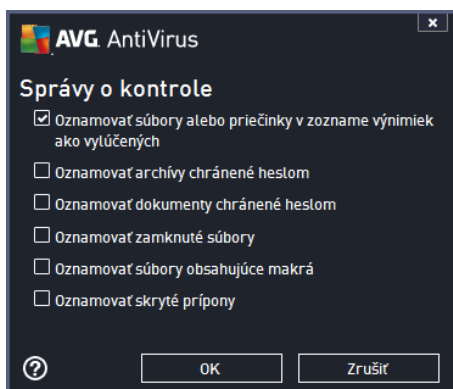
- **Všetky typy súborov** s možnosťou definovať výnimky z prehľadávania vytvorením zoznamu súborov oddelených (uložením súborov zmenia na bodkočiarku) prípon súborov, ktoré sa nemajú prehľadávať.
- **Vybrané typy súborov** – môžete nastaviť, aby sa kontrolovali len súbory, pri ktorých existuje pravdepodobnosť 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 nezaujaté, potom sa počas prehľadávania skrátí ešte viac, pretože tieto súbory sú často veľmi veľké, pričom pravdepodobnosť napadnutia vírusom je veľmi malá*). Znova môžete definovať, pod aké 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.

Nastavenie rýchlosti dokončenia kontroly

V tejto časti môžete alej 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 pred začatím doby trvania kontroly.

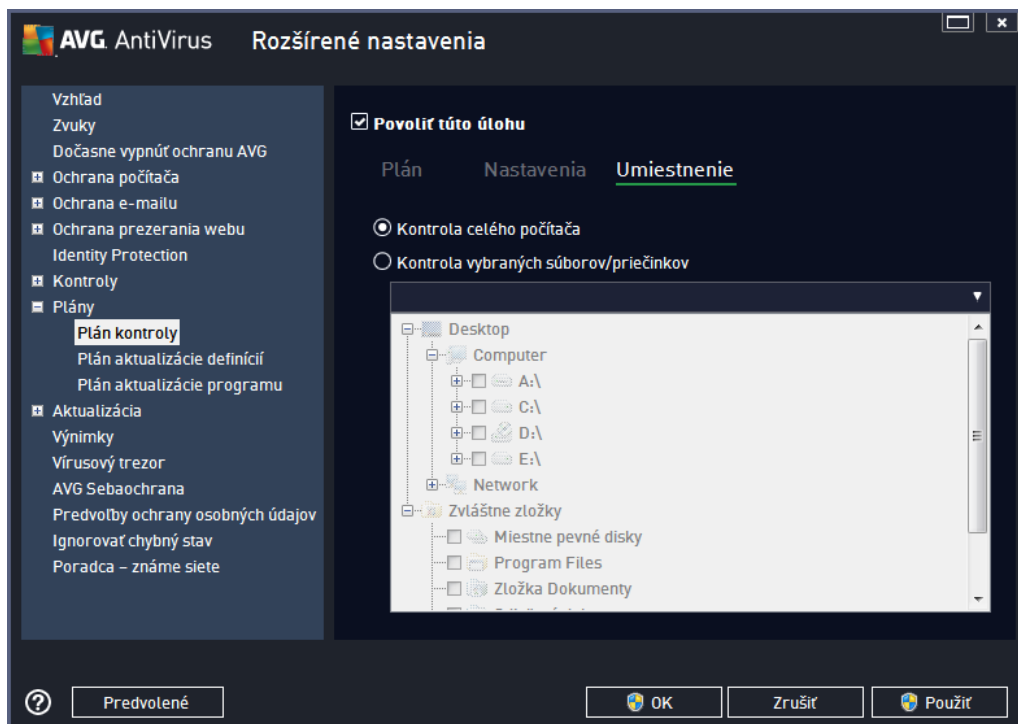
Vytvoriť ďalšie správy o kontrole

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



Možnosti vypnutia počítača

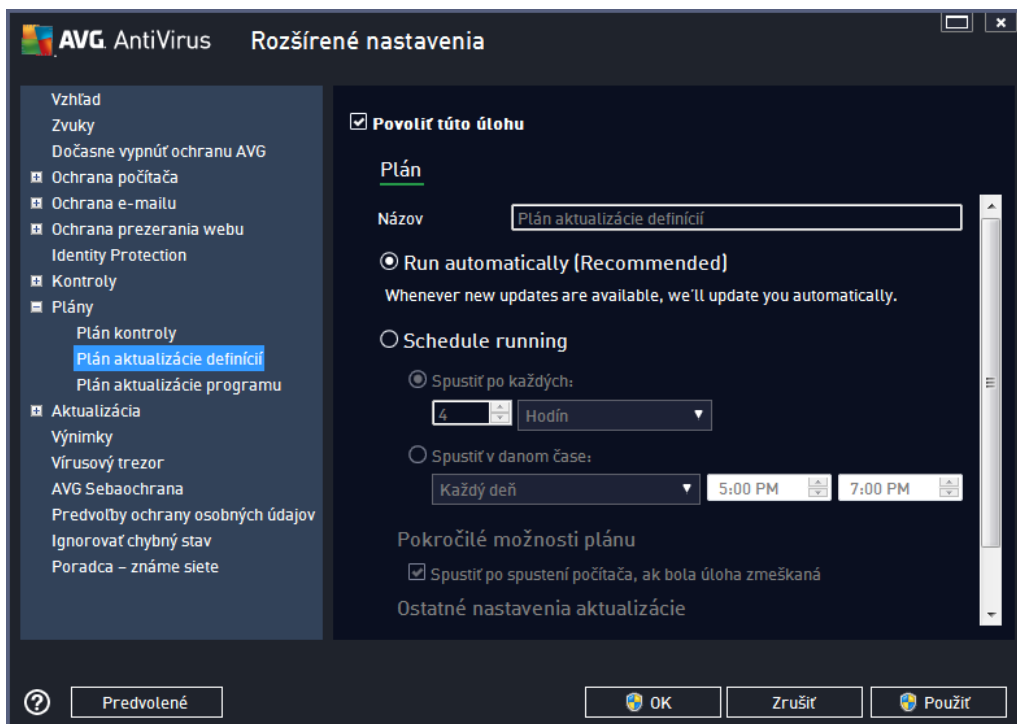
V časti **Možnosti vypnutia počítača** môžete rozhodnúť, či sa má počítač vypnúť automaticky po dokončení procesu kontroly. Po potvrdení tejto možnosti (**Vypnúť počítač po dokončení kontroly**) sa aktivuje nová možnosť, ktorá umožní vypnúť počítač, aj keď je momentálne zablokovaný (**Vynútené vypnutie,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

Spúšanie naplánovaných úloh

Predvolene sa úloha spustí automaticky (**Spustí automaticky**) hne po tom, ako je k dispozícii nová aktualizácia definícií vírusov. Odporúčame vám nemeňte toto nastavenie, ak nemáte pádný dôvod na jeho zmenu. Potom môžete nastaviť úlohu na ručné spustenie a určiť časové intervaly, v ktorých sa bude spúšťať aktualizácia nových definícií. Spúšanie sa definuje ako opakované spúšanie aktualizácie po uplynutí určitého času (**Spustí po každých...**) alebo nastavením presného dátumu a času (**Spúšťa sa 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.

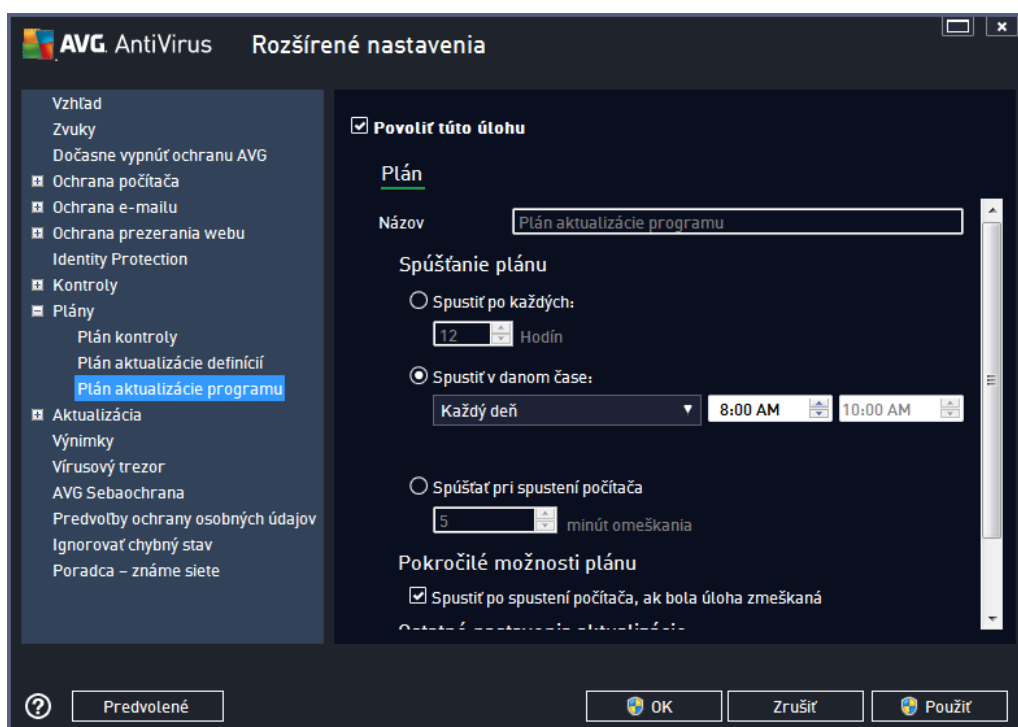
Ďalšie nastavenia aktualizácie

Nakoniec označte možnosť **Spustí aktualizáciu znova hne po obnovení internetového**

pripojenia, ak sa má v prípade výpadku internetového pripojenia a neúspechu procesu aktualizácie ihne po obnovení pripojenia okamžite spustiť. Po spustení naplánovanej aktualizácie vo vami nastavenom asse sa zobrazí informácia o tejto skutočnosti v automaticky otváranom okne nad [ikonou AVG v paneli úloh](#) (pod podmienkou, že sa nezmenila predvolená konfigurácia v dialógovom okne [Rozšírené nastavenia/Vzhľad](#)).

9.9.3. Plán aktualizácie programu

Ak je to **naozaj potrebné**, zrušením začiarknutia políčka **Povolí túto úlohu** môžete do asne 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 novo naplánovanej aktualizácie programu. Načasovanie sa definuje ako opakované spúšťanie aktualizácie po uplynutí určitého času (**Spustiť po každých...**), definovaním presného dátumu a času (**Spustiť a v konkrétnom asse...**), prípadne definovaním udalosti, s ktorou sa bude spájať spustenie aktualizácie (**Spustiť pri spustení počítača**).

Rozšírené možnosti plánu

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

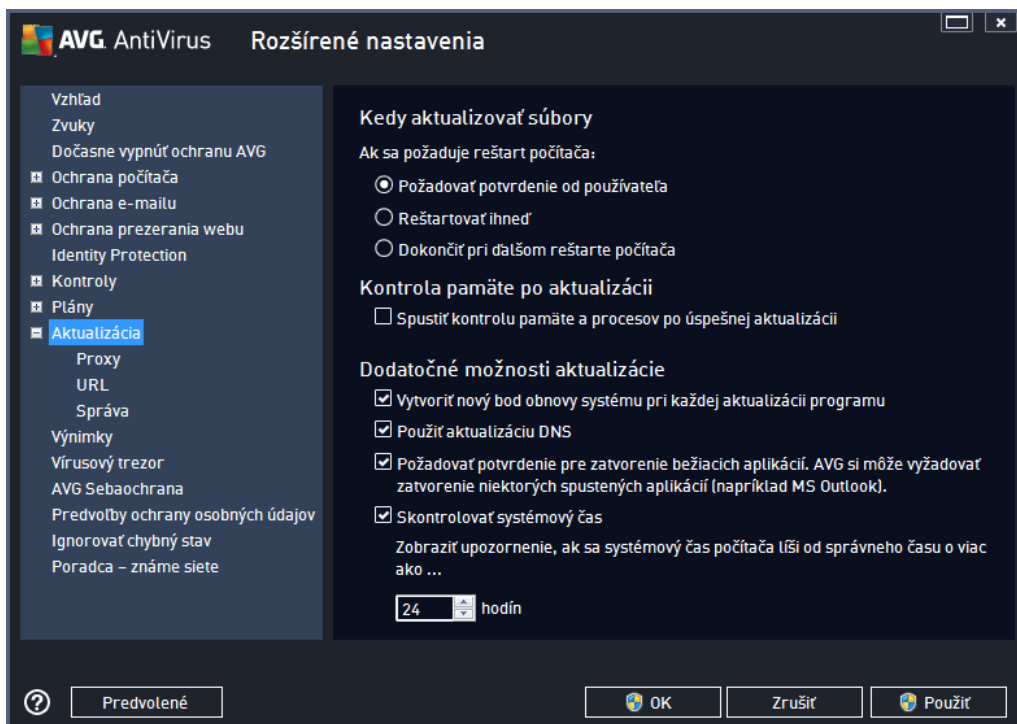
alšie nastavenia aktualizácie

Ozna te možnos **Znova spusti aktualizáciu ihne po obnovení internetového pripojenia**, ak sa má v prípade výpadku internetového pripojenia a neúspechu procesu aktualizácie ihne po obnovení pripojenia okamžite spusti . Po spustení naplánovanej aktualizácie vo vami nastavenom ase sa zobrazí informácia o tejto skuto nosti v automaticky otváranom okne nad [ikonou AVG v paneli úloh](#) (pod podmienkou, že sa nezmenila predvolená konfigurácia v dialógom okne [Rozšírené nastavenia/Vzh ad](#)).

Poznámka: Ak sa as naplánovanej aktualizácie programu náhodou prekryva s plánom kontroly, aktualizácia má vyššiu prioritu a kontrola sa preruší. V tak om prípade budete informovaní o tomto konflikte.

9.10. Aktualizácia

Položka **Aktualizácia** v naviga nej štruktúre otvorí nové dialógové okno, ktoré umož ťuje nastavi všeobecné parametre súvisiace s [aktualizáciou produktu AVG](#):



Kedy aktualizova súbory

V tejto asti môžete vybra jednu z troch možností, ktorá bude použitá v prípade, ak si proces aktualizácie vyžiada reštartovanie po íta a. Dokon enie aktualizácie môžete naplánova na alšie reštartovanie po íta a alebo môžete ihne reštartova po íta :

- **Požadova potvrdenie od používate a (predvolené)** – zobrazí sa žiados , aby ste potvrdili reštartovanie po íta a, ktoré je potrebné na dokon enie [aktualizácie](#)

- **Reštartova ihne** – po ťa sa automaticky reštartuje ihne po dokon ení [aktualizácie](#) a nepožiada vás o udelenie súhlasu.
- **Dokon i pri alšom reštarte po ťa a** – dokon enie [aktualizácie](#) bude odložené na alšie reštartovanie po ťa a. Odporú ame vám, aby ste túto možnos zapli len v prípade, ak sa po ťa reštartuje pravidelne, najmenej raz za de !

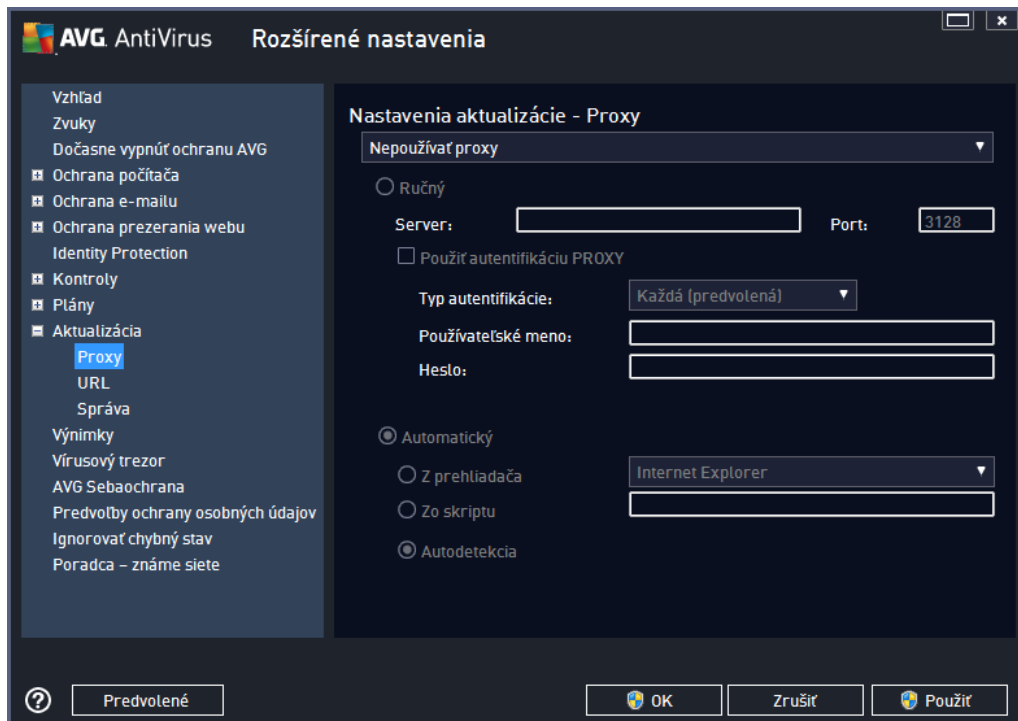
Kontrola pamäte po aktualizácii

Ozna te toto za iarkavacie polí ko, ak sa má nová kontrola pamäte spusti po každej úspešnej aktualizácii. Najnovšia prevzatá aktualizácia môže obsahova nové definície vírusov, ktoré sa môžu ihne použi pri kontrole.

alšie možnosti aktualizácie

- **Vytvori nový bod obnovy systému pri každej aktualizácii programu** (štandardne zapnuté) – pred každým spustením aktualizácie programu AVG sa vytvorí bod obnovy systému. Ak proces aktualizácie zlyhá a opera ný systém spadne, potom vám tento bod obnovenia umožní obnoví stav opera ného systému s pôvodnou konfiguráciou. Prístup k tejto možnosti je cez ponuku Štart/Všetky programy/Príslušenstvo/Systémové nástroje/Obnovenie systému, ale vykona zmeny týchto nastavení sa odporú a len skúseným používateľom! Nechajte toto za iarkavacie polí ko ozna ené, ak chcete používa túto funkcionálnosť.
- **Použi aktualizáciu DNS** (štandardne zapnuté) – ak je toto za iarkavacie polí ko ozna ené, po spustení aktualizácie program **AVG AntiVirus 2014** vyh dá informácie o najnovšej verzii vírusovej databázy a najnovšej verzii programu na serveri DNS. Až potom sa prevezmú a nainštalujú najmenšie nevyhnutne potrebné aktualizácia né súbory. Týmto spôsobom sa minimalizuje celkový objem prevzatých dát a zrýchli proces aktualizácie.
- **Funkcia Požadova 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 dokon enie procesu aktualizácie.
- **Skontrolova systémový as** (štandardne zapnuté) – za iarknite toto polí ko, ak chcete by informovaní v prípade, ke sa systémový as líši od skuto ného asu o viac, ako je nastavený po et hodín.

9.10.1. Proxy



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

- **Nepoužíva proxy** – predvolené nastavenie
- **Použije proxy**
- **Pokúsi sa pripojiť pomocou servera proxy a ak sa to nepodarí, pripojí 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 (zakliknite možnosť **Ručná na aktivovanie príslušnej časti dialógového okna**), musíte nastaviť nasledujúce parametre:

- **Server** – zadajte IP adresu servera alebo názov servera
- **Port** – zadajte číslo portu, ktorý umožní prístup na internet (predvolené 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, za iarknite možnos **Použi autentifikáciu PROXY** na overenie, i sú vaše používateľské meno a heslo platné na vytvorenie pripojenia na internet cez server proxy.

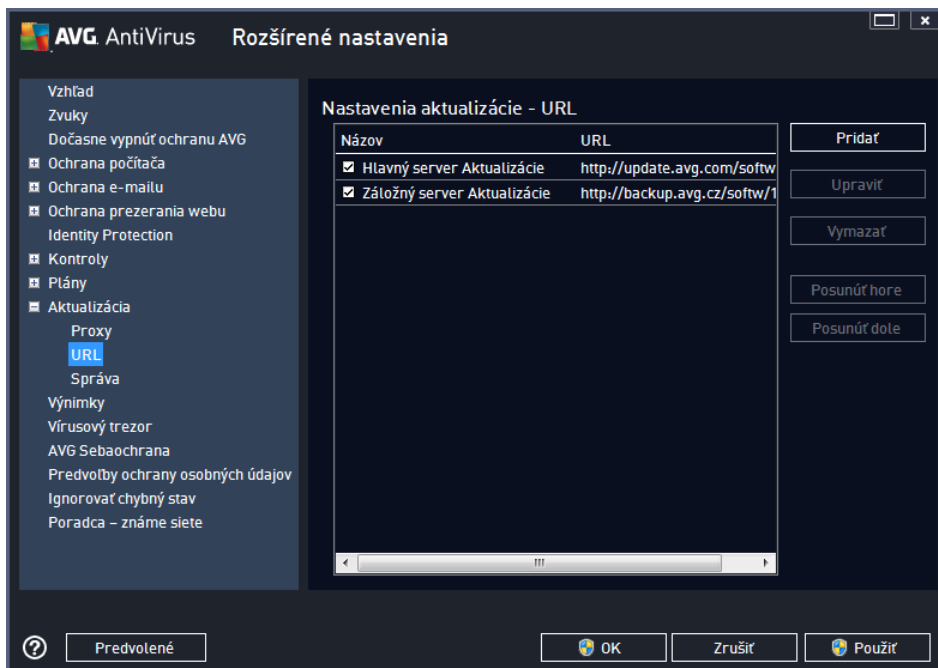
Automatická konfigurácia

Ak sa rozhodnete pre automatickú konfiguráciu (za iarknite možnos **Automatická** na aktivovanie príslušnej asti dialógového okna), nastavte, odkia sa má prevzia konfigurácia servera proxy:

- **Z prehliadača** – konfigurácia sa na íta z predvoleného internetového prehliadača.
- **Zo skriptu** – konfigurácia sa na íta z prevzatého skriptu pomocou funkcie, ktorá vráti adresu servera proxy.
- **Autodetekcia** – konfigurácia sa zistí automaticky priamo zo servera proxy.

9.10.2. Adresa URL

Dialógové okno **URL** uvádza zoznam internetových adries, z ktorých môžete prevzia aktualizácie súbory:



Ovládacie tlačidlá

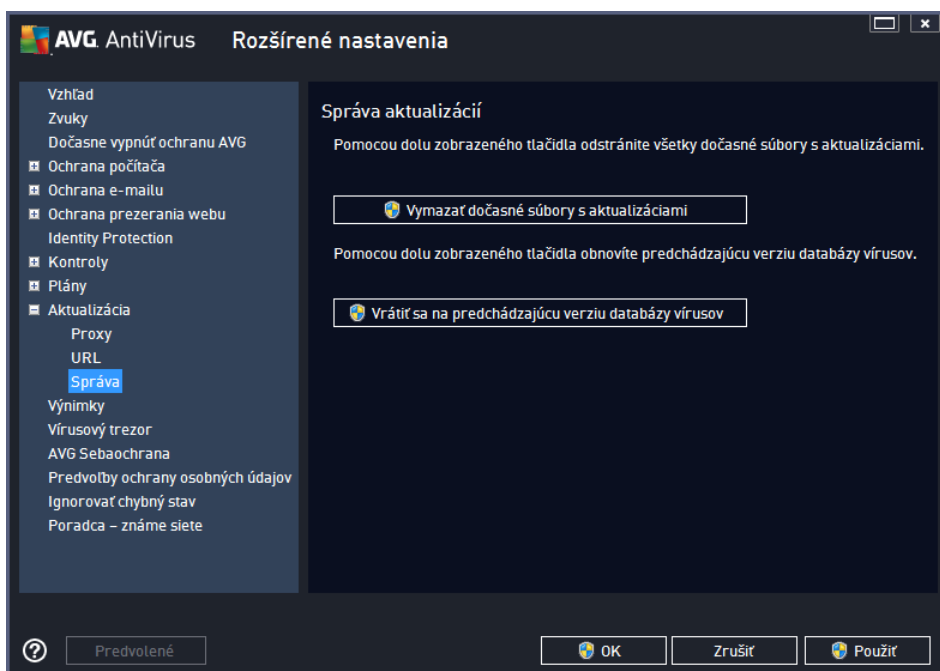
Zoznam a jeho položky môžete zmeniť pomocou nasledujúcich ovládacích tlačidiel:

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

- **Vymaza** – zo zoznamu sa vymaže zvolená adresa URL
- **Posunú hore** – posunie zvolenú adresu URL o jednu pozíciu v zozname nahor
- **Posunú dole** – posunie zvolenú adresu URL o jednu pozíciu v zozname nadol

9.10.3. Správa

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

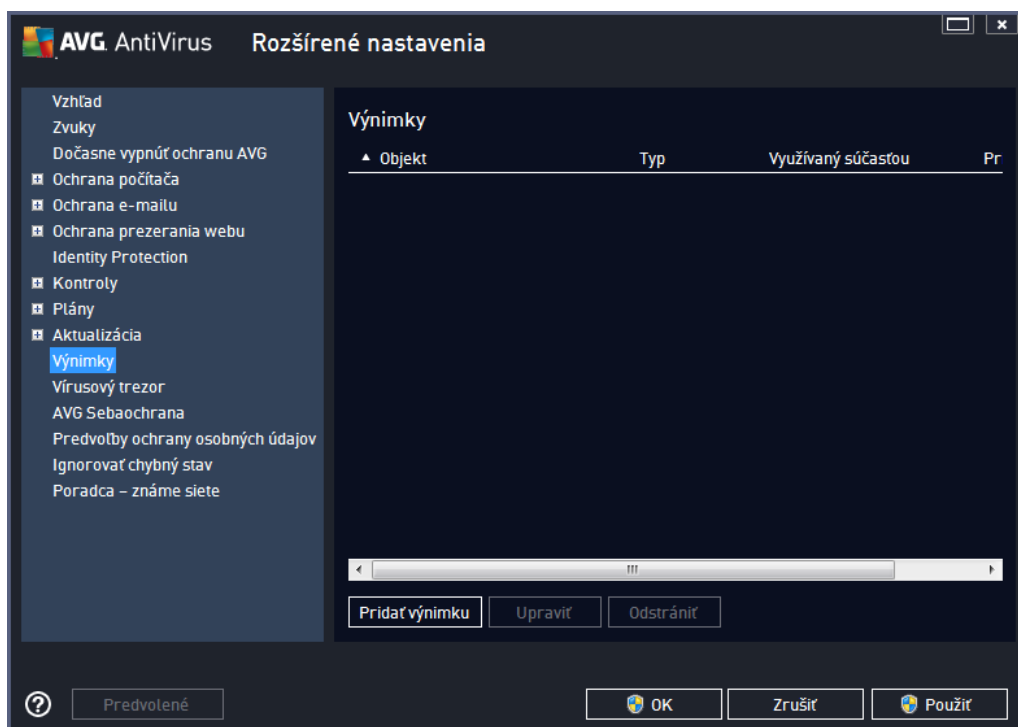


- **Vymaza dočasné súbory s aktualizáciami** – stlačením tohto tlačidla sa vymažú všetky nepotrebné súbory aktualizácie z pevného disku (v predvolenom nastavení zostanú tieto súbory uložené 30 dní).
- **Vrátiť sa na predchádzajúcu verziu databázy vírusov** – stlačením tohto tlačidla sa vymaže najnovšia 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 2014** 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!

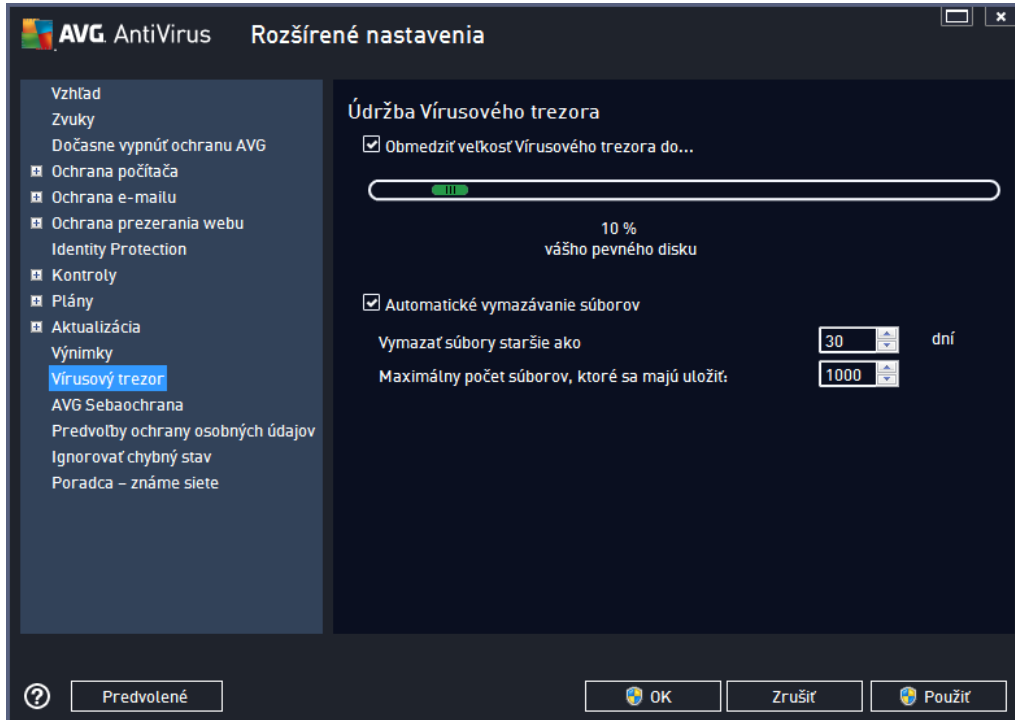


Hlavná stránka zobrazuje zoznam výnimiek, ak už boli nejaké definované. Vedľa každej položky sa nachádza začiarkavacie políčko. Keď je začiarkavacie políčko označené, potom sa výnimka používa; keď nie je, potom je výnimka len definovaná, ale momentálne sa nepoužíva. Kliknite na hlavičku stĺpca, aby sa 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 zadanú výnimku. Výnimky môžete odstrániť buď po jednej, alebo zvýrazníte niekoľko výnimiek v zozname a zrušíte ich naraz. Po zrušení výnimky bude program AVG príslušný súbor, priečinok i adresu URL opäť kontrolovať. Upozorujeme, že bude odstránená len výnimka, nie súbor alebo priečinok samotný!

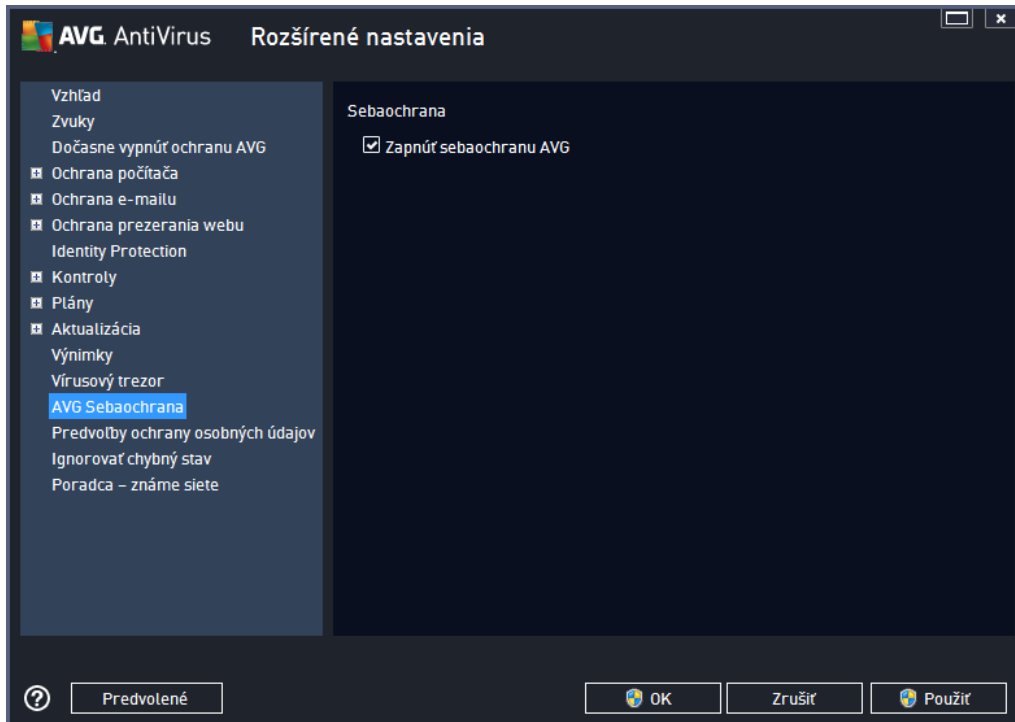
9.12. Vírusový trezor



Dialógové okno **Správa Vírusového trezora** vám umožní zadať niekoľko parametrov ohľadom administrácie objektov uložených vo [Vírusovom trezore](#):

- **Obmedziť veľkosť Vírusového trezora** – použijete posúvač na nastavenie maximálnej veľkosti [Vírusového trezora](#). Táto veľkosť sa uvádza úmerne k veľkosti lokálneho disku.
- **Automatické vymazávanie súborov** – v tejto časti môžete zadať maximálnu dĺžku času, po 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

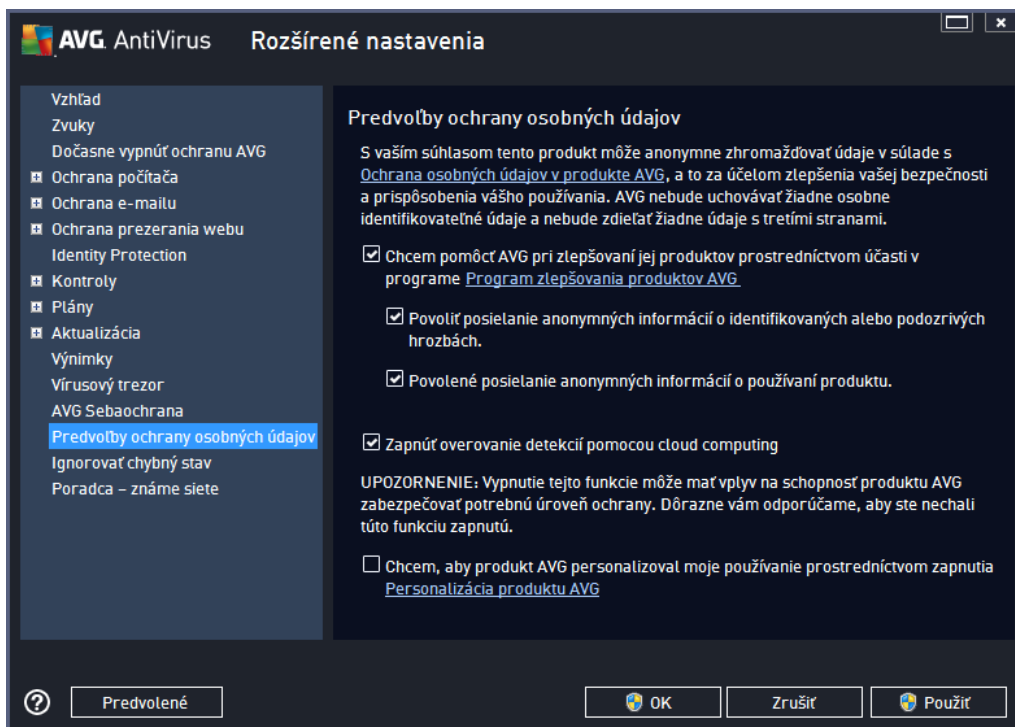


Funkcia **AVG Sebaochrana** umožní program **AVG AntiVirus 2014** chrániť svoje vlastné procesy, súbory, záznamy v registri a ovládať ich pred zmenou alebo deaktiváciou. Hlavným dôvodom pre tento druh ochrany je, že niektoré sofistikované hrozby sa snažia vypnúť antivírusovú ochranu a potom nerušené poškodzujú váš počítač.

Odporúčame vám túto funkciu ponechať zapnutú!

9.14. Preferencie ochrany osobných údajov

Dialógové okno **Preferencie ochrany osobných údajov** vám ponúkne možnosť nastaviť 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 ústníkov z celého sveta a umožní 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 (predvolené zapnuté)** – ak nám chcete pomôcť v ďalšom zlepšovaní AVG AntiVirus 2014, nechajte toto políčko zaškrtnuté. Táto funkcia zapne oznamovanie všetkých zaznamenaných hrozieb do spoločnosti AVG a umožní nám zhromažďovať najnovšie informácie o malware od všetkých užívateľov 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.
 - **Povolí posielanie informácií o nesprávne identifikovaných e-mailoch po potvrdení používateľa** (predvolené zapnuté) – posiela informácie o e-mailových správach, ktoré boli nesprávne označené ako spam, alebo spamových správach, ktoré sú našou Anti-Spam nedetegovala. Pred poslaním tohto druhu informácií vás program požiada o potvrdenie.
 - **Povolí posielanie anonymných informácií o identifikovaných alebo podozrivých hrozbách** (predvolené zapnuté) – posiela informácie o podozrivom alebo pozitívne nebezpečnom kóde alebo vzore správania (môže ísť o vírus, spyware alebo škodlivé internetové stránky, ktoré sa pokúšate otvoriť) detegovanom na počítači.
 - **Umožníte nám zasielať anonymné údaje o používaní produktu** (predvolené zapnuté) – odosielanie základných štatistík o používaní aplikácie, ako je počet nájdených hrozieb, spustených kontrol, úspešné a neúspešné kontroly a pod.
- **Zapnúť overovanie detekcií pomocou cloud computingu** (predvolené zapnuté) – detegované hrozby sa budú overovať, ak sú naozaj infikované, aby sa vylúčili nesprávne detekcie.

- **Želám si, aby sa produkty AVG prispôbili mojej práci zapnutím funkcie AVG Personalizácia (štandardne vypnutá)** – 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:

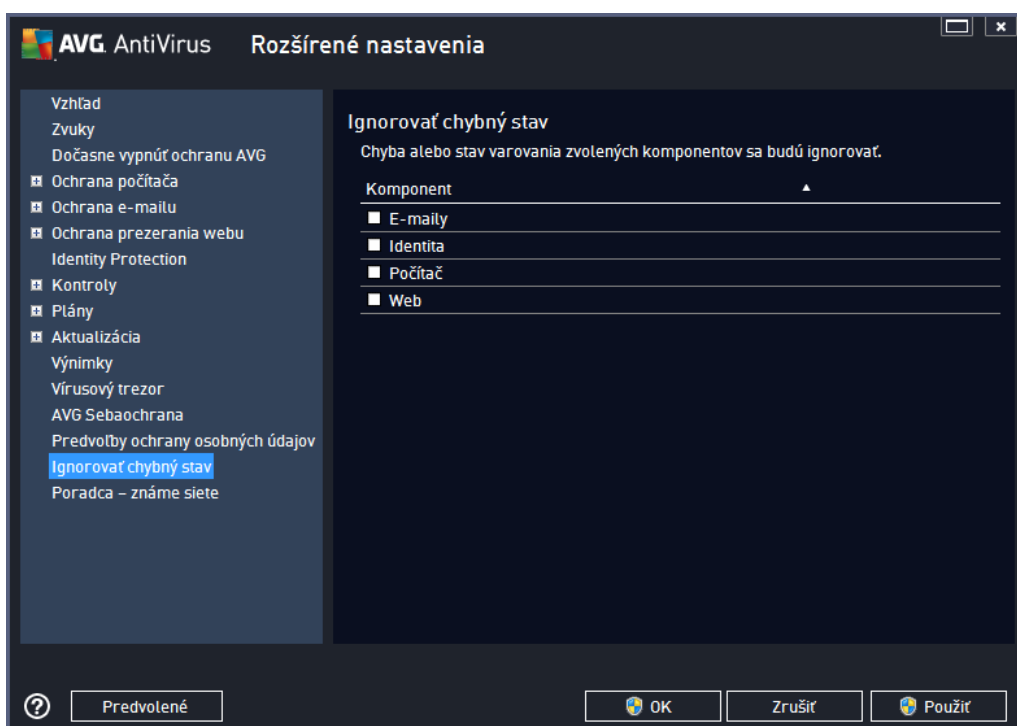
- **Vírus** je škodlivý kód, ktorý sa kopíruje a šíri často bez povšimnutia, kým nenapácha škody. Niektoré vírusy predstavujú vážnu hrozbu, ktorá dokáže vymazať alebo zámerne zmeniť súbory, zatiaľ čo iné vírusy sú zdanlivo neškodné, napríklad zahrajú melódiu. Všetky vírusy sú však nebezpečné, pretože sa dokážu množiť. Jeden jediný vírus dokáže v okamihu zaplniť celú pamäť počítača a spôsobiť jeho zlyhanie.
- **Podkategóriou vírusu je trojica**, ktorý (na rozdiel od vírusu) nepotrebuje „nosiča“, ku ktorému by sa pripojil; sám sa rozosiela do ostatných počítačov, zvyčajne cez e-mail, a následne často prechádza poštovými servermi a sieťovými systémami.
- **Spyware** sú zvyčajne sprievodné programy kategórie malware (*malware = každý škodlivý softvér vrátane vírusov*), zvyčajne trojske kone, ktoré sa používajú na odcudzenie osobných informácií, hesiel, čísel kreditných kariet alebo na preniknutie do počítača a umožnenie útoku ním ovládaného počítača; 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 prekryvacích 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 posielené na „hlavnú“ internetovú stránku pri jej opätovnej návšteve, môžu obsahovať údaje ako je vaša história surfovania na internete a ďalšie podobné informácie.
- **Exploit** 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 obeť sú často kontaktované prostredníctvom hromadných e-mailov, v ktorých sa od nich požaduje napríklad aby si aktualizovali podrobnosti 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 neuzitočné 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 legítimne internetové stránky, ktoré boli zneužitú na infikovanie počítača a návštevníkov.

V záujme ochrany pred všetkými druhmi hrozieb produkt **AVG AntiVirus 2014** obsahuje špecializované súčasti. Ich stručný opis nájdete v kapitole [Prehľad súčastí](#).

9.15. Ignorovať chybový 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 súčasti. To znamená, že ak sa niektorá súčasti dostane do chybového stavu, budete o tom ihne informovaní pomocou:

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

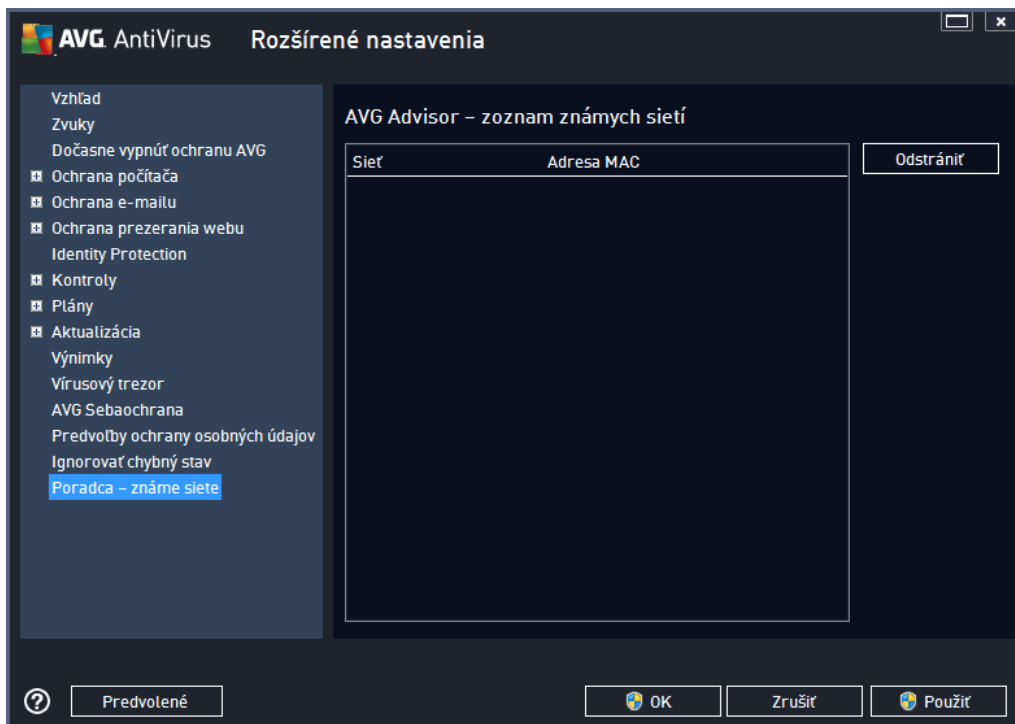
Môže nastať situácia, keď z nejakého dôvodu bude potrebné dočasne túto súčasti vypnúť. **To sa neodporúča, snažte sa mať neustále všetky súčasti zapnuté a v predvolenej konfigurácii.** Avšak niekedy sa takej situácii nemožno vyhnúť. V tom prípade ikona v paneli úloh automaticky oznámi chybový stav komponentu. 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 **Ignorova chybný stav** vybrať súčasti, o ktorých prípadnom chybnom stave (*alebo vypnutí*) si neželáte byť informovaní. Kliknutím na tlačidlo **OK** potvrdíte 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 jediné 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:

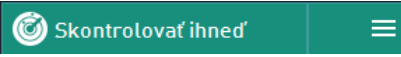


Poznámka: Funkcia známych sietí v súčasti AVG Advisor nie je podporovaná v 64-bitových systémoch Windows XP.

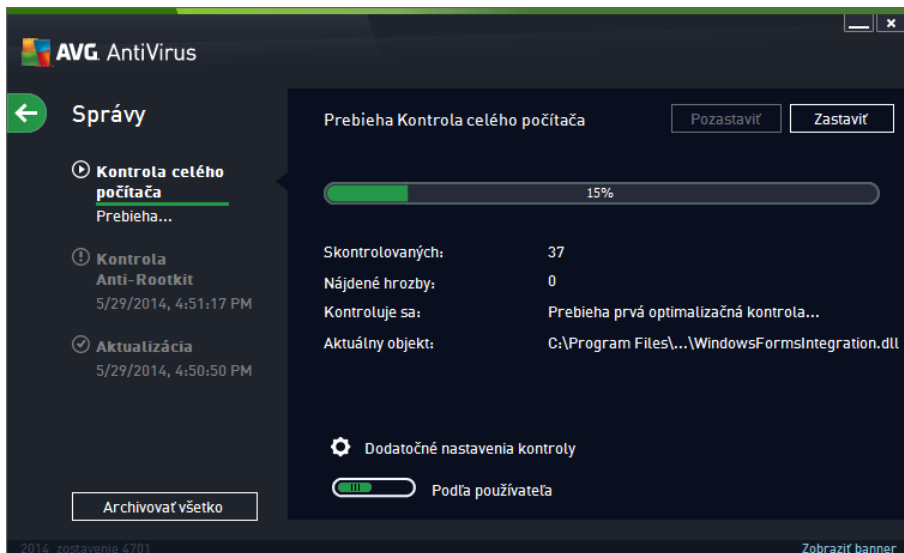
10. Kontrola programom AVG

V predvolenom nastavení aplikácia **AVG AntiVirus 2014** nespúšťa a žiadnu kontrolu, pretože po úvodnej kontrole (*zobrazí sa vám návrh na jej spustenie*) by ste mali byť dokonale chránení rezidentnými súasťami produktu **AVG AntiVirus 2014**, 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 spustíte kontrolu podľa vlastných potrieb.

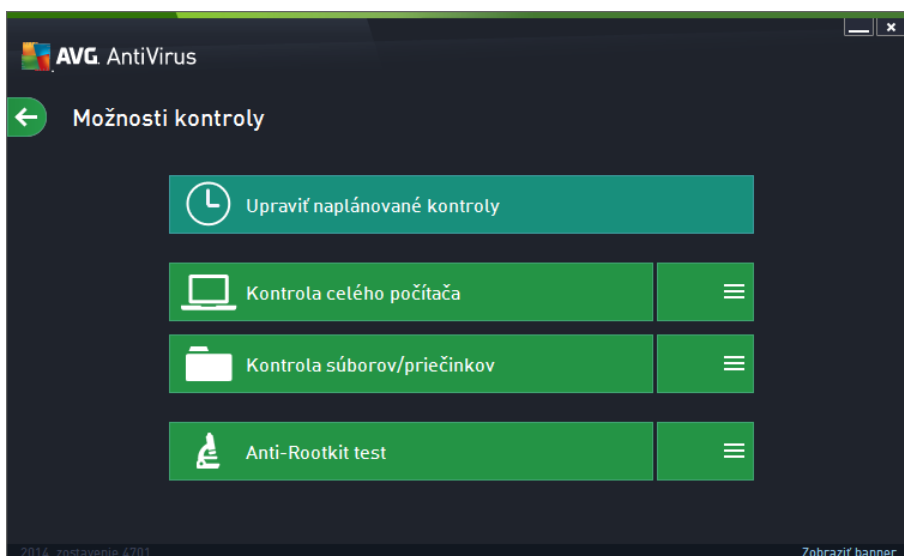
K rozhraniu kontroly programu AVG máte prístup [z hlavného používateľského rozhrania](#)

prostredníctvom tlačidla graficky rozdeleného na dve časti: 

- **Skontrolovať ihneď** – stlačíte toto tlačidlo pre okamžité spustenie [Kontroly celého počítača](#) a sledujete 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/priebehov](#).



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 tabu len jeden plán kontroly, ktorý vopred definoval dodávateľ softvéru. Táto kontrola je štandardne vypnutá. Ak ju chcete zapnúť, kliknite na tlačidlo na pravom tlačiteli a v kontextovej ponuke vyberte možnosť *Povolí 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* a okamžite spustíte kontrolu celého počítača (*podrobnosti o kontrole celého počítača nájdete v príslušnej kapitole s názvom [Vopred definované kontroly/Kontrola celého počítača](#)*). Kliknutím na 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 časť *Nastavenia* sa zobrazí konfiguračné okno, kde môžete [nastaviť parametre kontroly súborov a priečinkov](#).
- **kontrola celého počítača a na prítomnosť rootkitov / nastavenia** – avšak oboje tlačidlá označujú kontrolu celého počítača a na prítomnosť rootkitov sa spustí okamžitá kontrola anti-rootkit (*podrobnosti o kontrole rootkitov nájdete v príslušnej kapitole pod názvom [preddefinované kontroly / skontrolovanie rootkitov v počítači](#)*). Kliknutím na časť *Nastavenia* sa zobrazí konfiguračné okno, kde môžete [nastaviť parametre kontroly rootkitov](#).

10.1. Vopred definované kontroly

Jednou z hlavných funkcií produktu **AVG AntiVirus 2014** je kontrola na požiadanie. Testy na požiadanie sú určené na kontrolu rôznych častí počítača a pri každom podozrení možného výskytu vírusovej infekcie. Odporúčajú sa a sa vykonávajú takéto testy pravidelne, aj keď si myslíte, že sa vo vašom počítači nenájdú žiadny vírus.

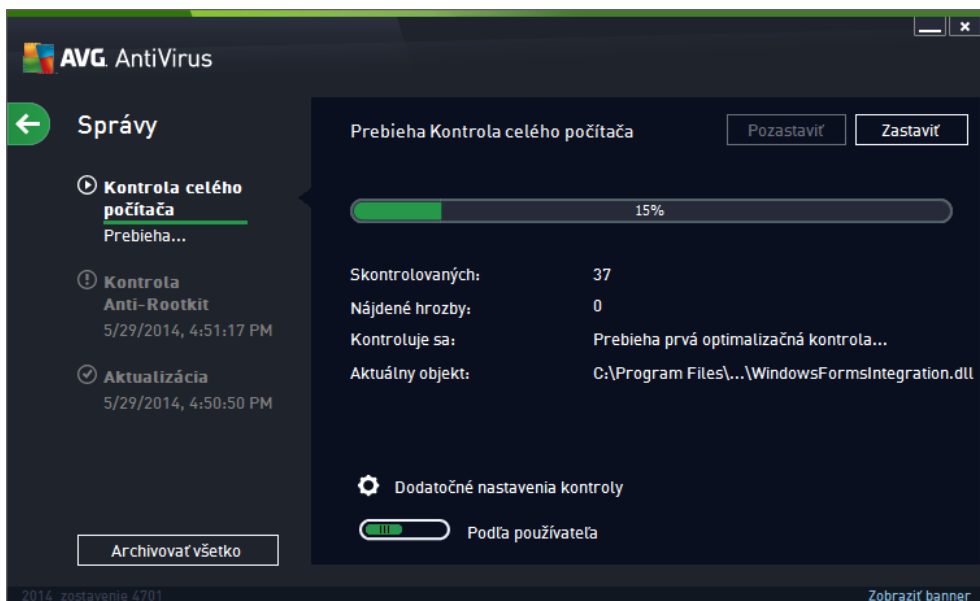
V produkte **AVG AntiVirus 2014** sa nachádzajú tieto typy kontrol vopred definované dodávateľom softvéru:

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.

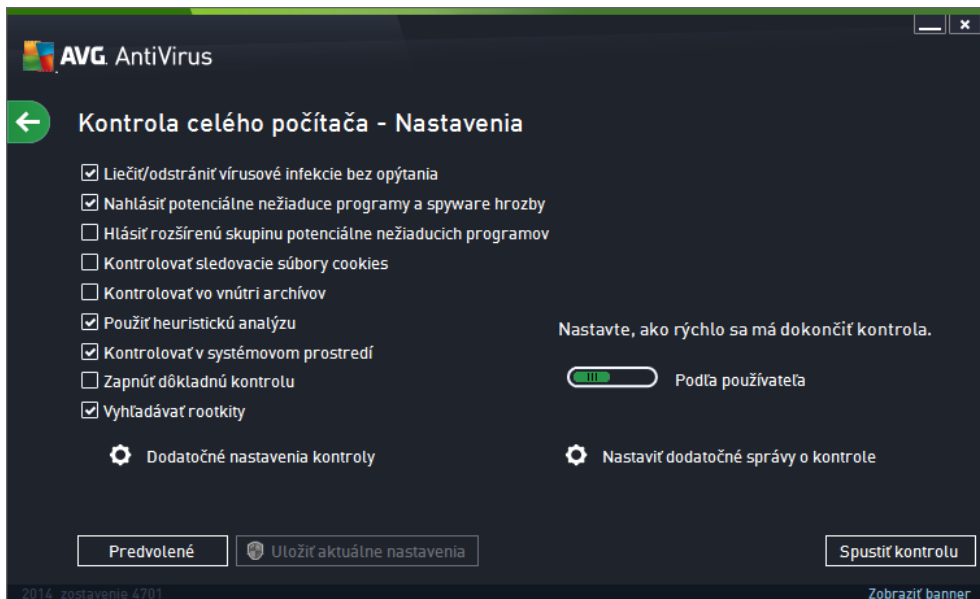
Spustenie kontroly

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

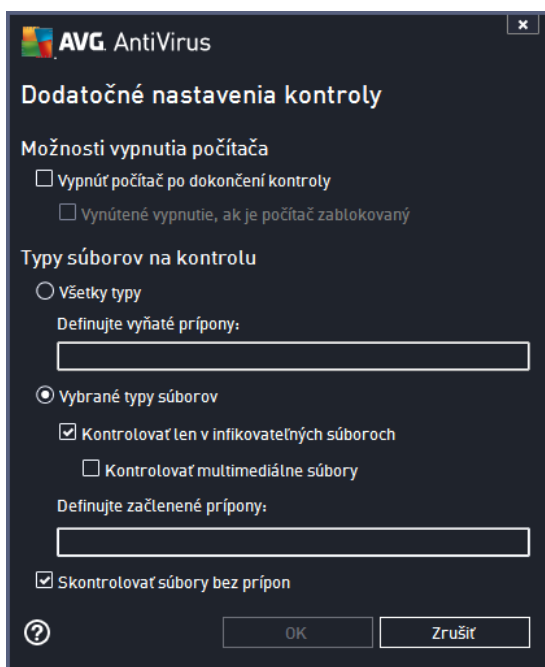
Konfiguráciu **kontroly celého počítača** môžete upraviť v dialógovom okne **Kontrola celého počítača – Nastavenia** (okno je prístupné cez odkaz **Nastavenia pre Kontrolu celého počítača** a v rámci okna **Možnosti kontroly**). **Odporúčajú sa ponechať predvolené nastavenia, ak nemáte závažný dôvod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



V zozname parametrov kontroly môžete zapnú /vypnú špecifické parametre podľa potreby:

- **Lieč i /odstráni 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, presunie sa do [Vírusového trezora](#).
- **Nahlási potenciálne nežiaduce programy a spyware hrozby** (štandardne zapnuté) – začiarknite toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu malwaru: 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.
- **Hlásí 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 blokovать dobré programy, a preto je táto funkcia štandardne vypnutá.
- **Kontrola sledovacích súborov cookies** (štandardne vypnuté) – tento parameter súvisí s funkciou 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*).
- **Kontrola vo vnútri archívov** (štandardne vypnuté) – tento parameter určuje, že sa počas kontroly preveria 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.

- **Kontrolova v systémovom prostredí (štandardne zapnuté)** – počas kontroly sa budú kontrolovať aj systémové oblasti počítača.
- **Zapnú 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. Upozorujeme však, že tento spôsob je náročný na čas.
- **Kontrolova rootkity (štandardne zapnuté)** – zahrnie kontrolu prítomnosti rootkitov do kontroly celého počítača. [Kontrolu rootkitov](#) možno spustiť aj samostatne.
- **Dodatkové nastavenia kontroly** – tento odkaz otvorí nové dialógové okno Dodatkové nastavenia kontroly, ktoré sa používa na nastavenie nasledujúcich parametrov:

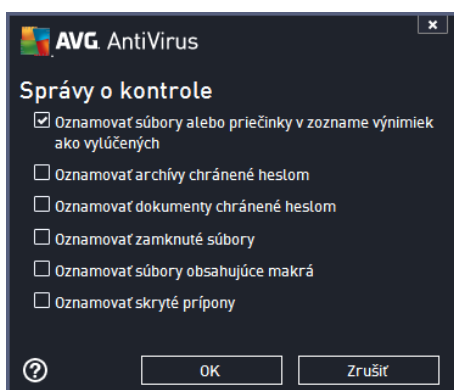


- **Možnosti vypnutia počítača** – rozhodnite, či sa má počítač vypnúť automaticky po dokončení procesu kontroly. Po potvrdení tejto možnosti (**Vypnúť po dokončení kontroly**) sa aktivuje nová možnosť, ktorá umožní vypnúť počítač, aj keď je momentálne zablokovaný (**Vynútené vypnutie, ak je počítač zablokovaný**).
- **Typy súborov na kontrolu** – mali by ste tiež určiť, čo chcete kontrolovať:
 - **Všetky typy súborov** s možnosťou definovať výnimky z kontroly vytvorením zoznamu špeciálnou 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 súbory – ak necháte toto políčko nezaškrtnuté, potom sa čas prehadzovanie skrátí ešte viac, pretože tieto súbory sú často veľa väčšie, pričom pravdepodobnosť napadnutia vírusom je veľmi malá). Znova môžete

definovať, pod a 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 zmeníte prioritu procesu kontroly. V predvolenom nastavení je úroveň automatického využívania zdrojov nastavená *Podľa používateľa*. Prípadne môžete spustiť procesy prehadzovania pomalšie, čím sa minimalizuje využívanie systémových zdrojov (*toto nastavenie je užitočné vtedy, ak potrebujete pracovať po ťažko, ale nezaujíma vás, ako dlho bude prehadzovanie trvať*) alebo rýchlejšie s vyššími nárokmi na využívanie systémových zdrojov (*napríklad keď sa po ťažko 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 novo definovanej 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.

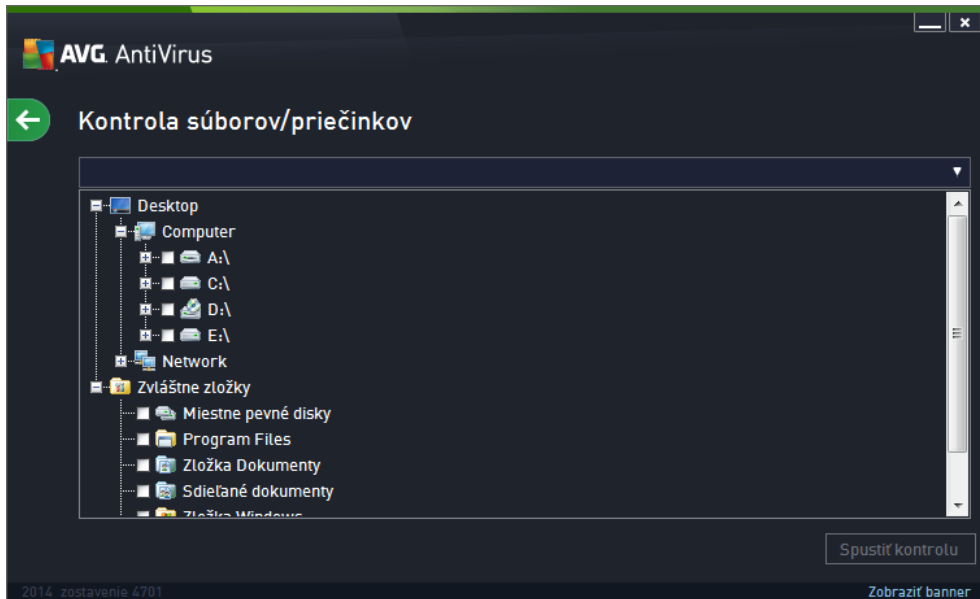
10.1.2. Kontrola súborov/priečinkov

Kontrola súborov/priečinkov – prehadzovať 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 vylúčia 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

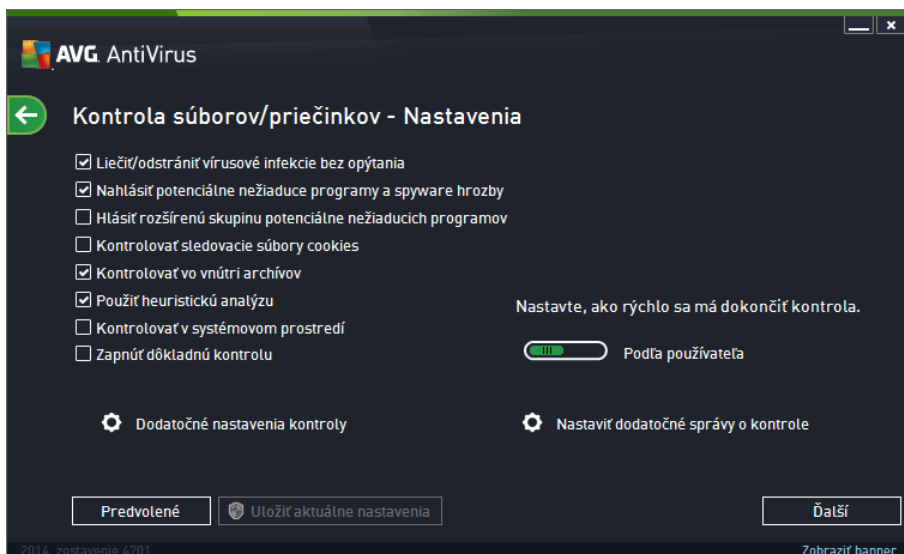
Funkciu **Kontrola súborov/priečinkov** môžete spustiť priamo z okna [Možnosti kontroly](#) kliknutím na tlačidlo **Kontrola súborov/priečinkov**. Otvorí sa nové dialógové okno s názvom **Výber konkrétnych súborov alebo priečinkov na kontrolu**. V stromovej štruktúre počítača vyberte tie priečinky, ktoré 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 použijete parameter „!“. Napokon, ak chcete spustiť kontrolu, stlačte tlačidlo **Spustiť kontrolu**; samotný proces kontrolovania sa v podstate zhoduje s [kontrolou celého počítača](#).



Zmena konfigurácie kontroly

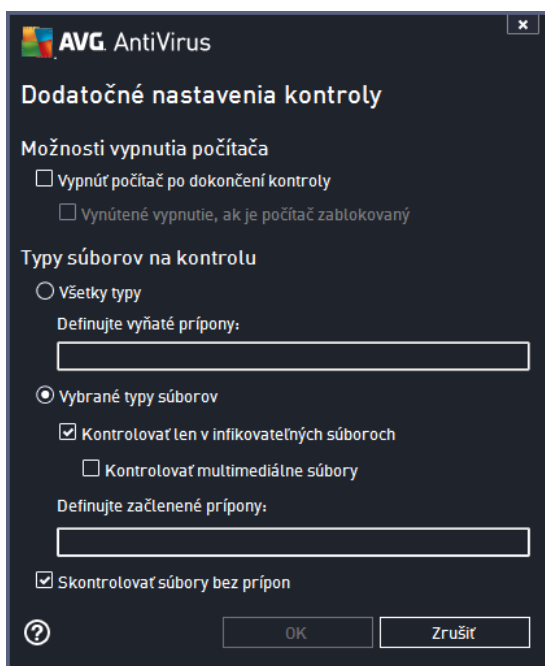
Konfiguráciu **Kontroly súborov/priečinkov** môžete upraviť v dialógovom okne **Kontrola súborov/priečinkov – Nastavenia** (okno je prístupné cez odkaz *Nastavenia pre Kontrolu súborov/priečinkov* v rámci okna [Možnosti kontroly](#)). **Odporúčame ponechať predvolené nastavenia, ak nemáte závažný dôvod ich meniť!**



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

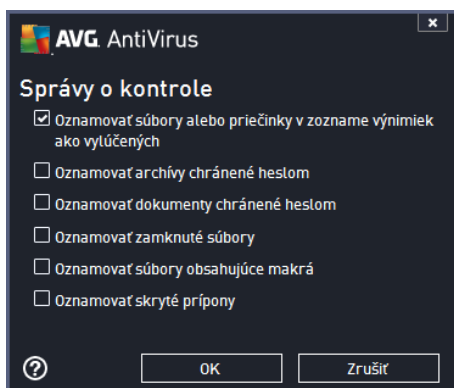
parametre:

- **Lie i /odstráni vírusovú infekciu bez opýtania** (štandardne zapnuté) – ak sa po as kontroly zistí prítomnosť vírusu, môže sa automaticky vylie i , ak je k dispozícii lie ba. Ak nie je možné infikovaný súbor vylie i automaticky, premiestni sa do [Vírusového trezora](#).
- **Nahlási potenciálne nežiaduce programy a spyware hrozby** (štandardne zapnuté) – za iarknite toto polí ko, ak chcete aktívova kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu malwaru: aj ke v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu by nainštalované úmyselne. Odporú ame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počíta a.
- **Hlási rozšírenú skupinu potenciálne nežiaducich programov** (štandardne vypnuté) – za iarknite toto polí ko, ak sa má detegova rozšírená skupina spywaru: programov, ktoré sú úplne v poriadku a neškodné, ke sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpečenia počíta a, ale môže blokova dobré programy, a preto je táto funkcia štandardne vypnutá.
- **Kontrolova sledovacie súbory cookies** (štandardne vypnuté) – tento parameter sú asti zapína detekciu súborov cookies (*HTTP cookies sa používajú na overenie totožnosti, sledovanie a správu konkrétnych informácií o používate och, akými sú napr. preferencie stránok alebo obsah elektronických nákupných košíkov*).
- **Kontrolova vo vnútri archívov** (štandardne zapnuté) – tento parameter ur uje, že sa majú po as kontroly preverova všetky súbory uložené vnútri archívov, napr. ZIP, RAR, ...
- **Použi heuristickú analýzu** (štandardne zapnuté) – heuristická analýza (*dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počíta ovom prostredí*) bude jedna z metód, ktoré sa použijú na detekciu vírusov po as kontroly.
- **Kontrolova v systémovom prostredí** (štandardne vypnuté) – po as kontroly sa budú overova aj systémove oblasti počíta a.
- **Zapnú dôkladnú kontrolu** (štandardne vypnuté) – v ur itých situáciách (*podozrenie na infikovanie počíta a*) môžete touto možnosťou aktívova najdôkladnejšie kontrolné algoritmy, ktoré pre istotu skontrolujú aj tie oblasti počíta a, ktoré sa oby ajne vôbec neinfikujú. Upozor ujeme však, že tento spôsob je náročný na as.
- **Dodatové nastavenia kontroly** – tento odkaz otvorí nové dialógové okno **Dodatové nastavenia kontroly**, ktoré sa používa na nastavenie nasledujúcich parametrov.



- **Možnosti vypnutia počítača** – rozhodnite, či sa má po skončení kontroly vypnúť počítač 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 sčiarou 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 súbory – ak necháte toto políčko nezačiarknuté, potom sa prehrávanie skrátí ešte viac, pretože tieto súbory sú často veľmi veľké, pričom pravdepodobnosť napadnutia vírusom je veľmi malá*). Znova môžete definovať, pod aké 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 zmeníte prioritu procesu kontroly. V predvolenom nastavení je úroveň automatického využívania zdrojov nastavená *Podľa používateľa*. Prípadne môžete spustiť procesy prehrávania pomalšie, čím sa minimalizuje využívanie systémových zdrojov (*toto nastavenie je užitočné vtedy, ak potrebujete pracovať na počítači, ale nezaujíma vás, ako dlho bude prehrávanie trvať*), alebo rýchlejšie s vyššími nárokmi na využívanie systémových zdrojov (*napríklad keď sa počítač dočasne nepoužíva*).

- **Vytvorí ďalšie správy o prehľadovaní** – odkaz otvorí nové dialógové okno **Správy o prehľadovaní**, ktoré vám umožní nastaviť, ktoré typy možných nálezov sa majú hlásiť:



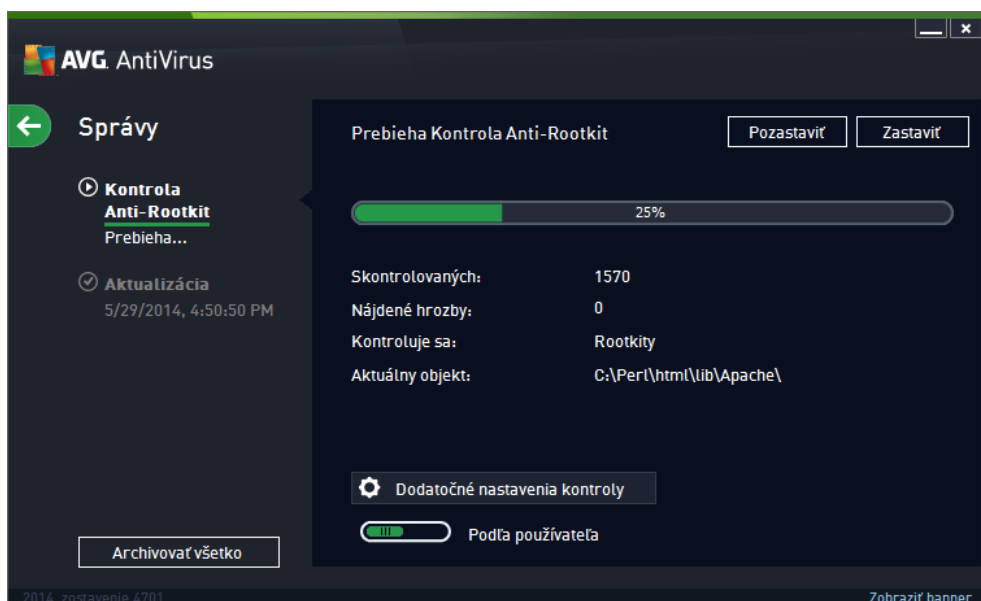
Upozornenie: Tieto nastavenia kontroly sa zhodujú s parametrami novo definovanej kontroly; pozrite informácie v kapitole [Kontrola programom AVG/Plánovanie kontroly/Ako kontrolovať](#). Ak sa rozhodnete zmeniť predvolenú konfiguráciu funkcie **kontrola súborov/priečinkov**, svoje nové nastavenie môžete potom uložiť ako predvolenú konfiguráciu, ktorá sa použije pre všetky ďalšie prehľadovania konkrétnych súborov alebo priečinkov. Táto konfigurácia sa zároveň použije ako šablóna pre všetky vami novo naplánované kontroly ([všetky nastavené kontroly vychádzajú zo súčasných nastavení kontroly vybraných súborov alebo priečinkov](#)).

10.1.3. Kontrola počítača na prítomnosť rootkitov

Kontrola počítača na prítomnosť rootkitov deteguje a následne odstráni nebezpečné rootkity, t. j. programy a technológie, ktoré dokážu zamaskovať prítomnosť škodlivého softvéru vo vašom počítači. Rootkit je program určený na to, aby sa zmocnil základnej kontroly nad počítačovým systémom bez povolenia vlastníka systému a jeho právoplatných správcov. Kontrola dokáže zistiť prítomnosť rootkitov pomocou vopred definovanej skupiny pravidiel. Ak sa nájde rootkit, nemusí to nevyhnutne znamenať, že je infikovaný. Programy rootkit sa niekedy používajú ako ovládacie, prípadne tvoria súčasť správnych aplikácií.

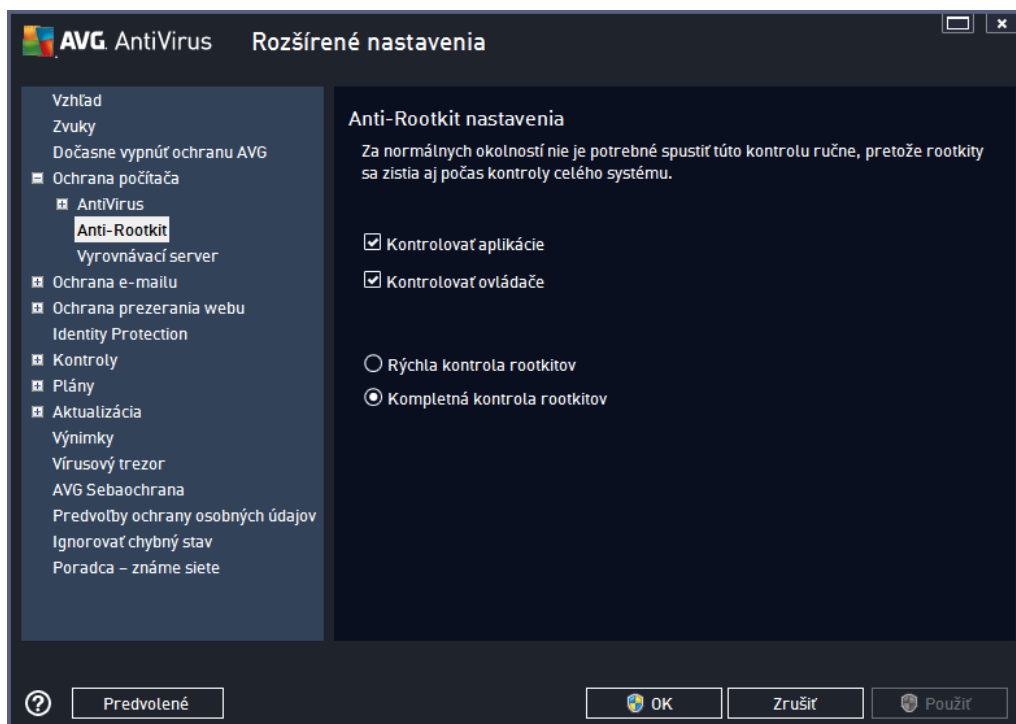
Spustenie kontroly

Kontrolu počítača na prítomnosť rootkitov možno spustiť priamo z dialógového okna [Možnosti kontroly](#) kliknutím na tlačidlo **Kontrola počítača na prítomnosť rootkitov**. Otvorí sa nové dialógové okno s názvom **Prebieha kontrola Anti-Rootkit**, v ktorom sa zobrazuje priebeh spustenej kontroly:



Zmena konfigurácie kontroly

Konfiguráciu kontroly Anti-Rootkit môžete upraviť v dialógovom okne **Kontrola Anti-Rootkit – Nastavenia** (okno je prístupné cez odkaz *Nastavenia pre Kontrolu po íta* a na prítomnosť rootkitov v rámci okna *Možnosti kontroly*). **Odporúča sa ponechať predvolené nastavenia, ak nemáte závažný dôvod ich meniť!**



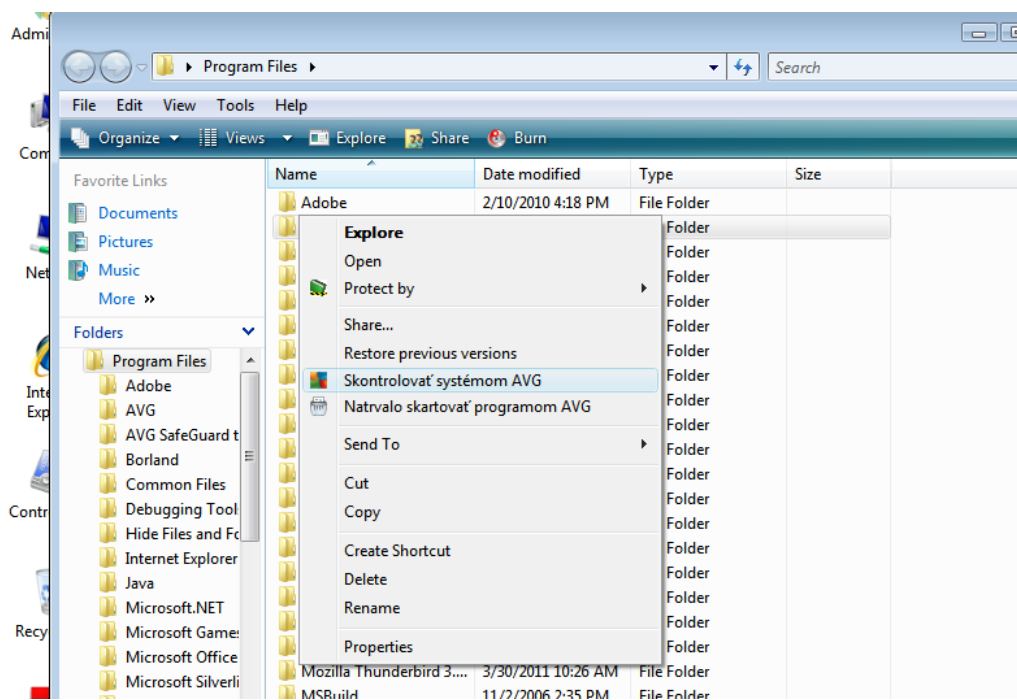
Možnosti **Kontrolovať aplikácie** a **Kontrolovať ovládače** vám umožnia podrobne zadať, čo by

malo by sú 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 ovládacie a systémové priečiny (zvyčajne c:\Windows).
- **Úplná kontrola rootkitov** – kontroluje všetky spustené procesy, zavedené ovládacie, systémové priečiny (obvyčajne c:\Windows), plus všetky miestne disky (vrátane pamäťových médií, nie však disketové jednotky/jednotky CD-ROM).

10.2. Kontrola z prieskumníka

Okrem vopred definovaných kontrol spustených pre celý počítač alebo jeho vybrané oblasti, **AVG AntiVirus 2014** zároveň umožňuje rýchlo skontrolovať konkrétny objekt priamo v prostredí programu Prieskumník. Ak chcete otvoriť neznámy súbor a nie ste si istí 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** skontrolujete súbor programom **AVG AntiVirus 2014**.

10.3. Kontrola z príkazového riadka

Program **AVG AntiVirus 2014** 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



vä šinou parametrov, ktoré sa nachádzajú aj v grafickom používateľskom rozhraní AVG.

Pre spustenie kontroly AVG z príkazového riadka spustíte nasledovný príkaz v priežinku, 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, zoradíte ich za sebou a oddelite 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 oblasti), potom sa hodnoty oddelia bodkou a čiarkou, napríklad:
avgscanx /scan=C:\;D:

Parametre kontroly

Ak chcete zobraziť úplný prehľad použitých 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 stlačíte 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** umožní zadať väšinu 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/priežinkov](#) /SCAN=path;path (napr. /SCAN=C:\;D:\)

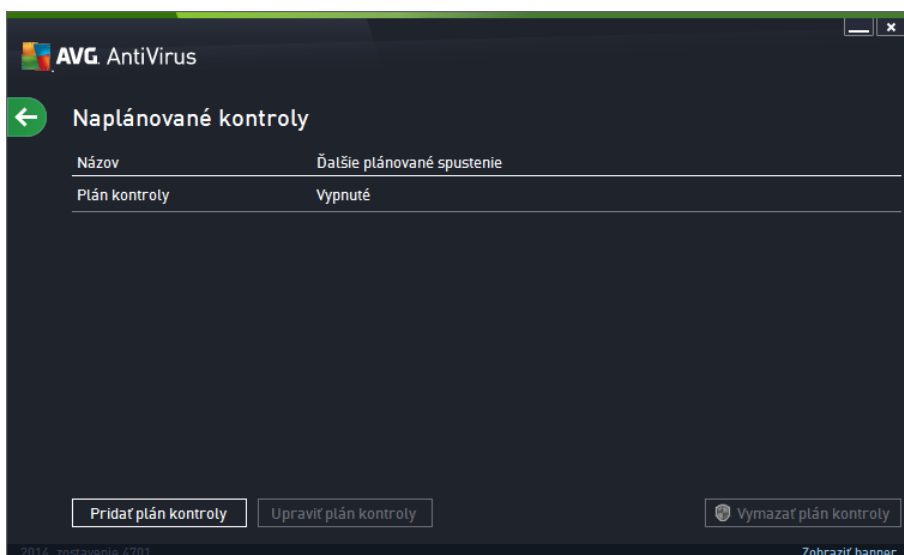
- /COMP [Kontrola celého počítača](#)
- /HEUR Použije heuristickú analýzu
- /EXCLUDE Cesty alebo súbory, ktoré sa majú vyňať z kontroly
- /@ Súbor s príkazmi /názov súboru/
- /EXT Kontrolovať tieto prípony /napríklad EXT=EXE, DLL/
- /NOEXT Nekontrolovať tieto prípony /napríklad NOEXT=JPG/
- /ARC Kontrolovať archívy
- /CLEAN Automaticky vyčistiť
- /TRASH Presunúť infikované súbory do [Vírusového trezora](#)
- /QT Rýchly test
- /LOG Generovať súbor s výsledkami kontroly
- /MACROW Hlásenie makrá
- /PWDW Hlásenie súborov chránených heslom
- /ARCBOMBSW Hlásenie opakovane komprimovaných archívnych súborov
- /IGNLOCKED Ignorovať zamknuté súbory
- /REPORT Hlásenie do súboru /názov súboru/
- /REPAPPEND Pripojiť k súboru s hlásením
- /REPOK Hlásenie neinfikovaných súborov so značkou OK
- /NOBREAK Nepovolí prerušenie klávesmi CTRL-BREAK
- /BOOT Povolí kontrolu MBR/BOOT
- /PROC Kontrolovať aktívne procesy
- /PUP Hlásenie potenciálne nežiaduce programy
- /PUPEXT Hlásenie rozšírenú skupinu potenciálne nežiaducich programov
- /REG Kontrolovať v registroch
- /COO Kontrolovať súbory cookies
- /? Zobrazí pomocníka pre túto tému
- /HELP Zobrazí pomocníka pre túto tému

- /PRIORITY Nastavi prioritu kontroly /nízka, automatická, vysoká/ ([pozri as Rozšírené nastavenia/Kontroly](#))
- /SHUTDOWN Vypnú počítač po dokončení kontroly
- /FORCESHUTDOWN Vynútené vypnutie počítača a po dokončení kontroly
- /ADS Kontrolovať alternatívne dátové prúdy (*len pre NTFS*)
- /HIDDEN Hlásia súbory so skrytými príponami
- /INFECTABLEONLY Kontrolovať len súbory s infikovanými príponami
- /THOROUGHSCAN Zapnú dôkladnú kontrolu
- /CLOUDCHECK Kontrola nesprávnych pozitívnych detekcií
- /ARCBOMBSW Hlásia opakovane komprimované archívne súbory

10.4. Plánovanie kontroly

S aplikáciou **AVG AntiVirus 2014** môžete spustiť kontrolu na požiadanie (*napríklad keď máte podozrenie, že sa do počítača dostala infekcia*) alebo na základe vytvoreného plánu. Odporúčame spustiť kontroly na základe plánov. Týmto spôsobom môžete zabezpečiť, že je váš počítač chránený pred možnou infekciou 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 možnosti však spustíte kontrolu celého počítača a 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 stave 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:

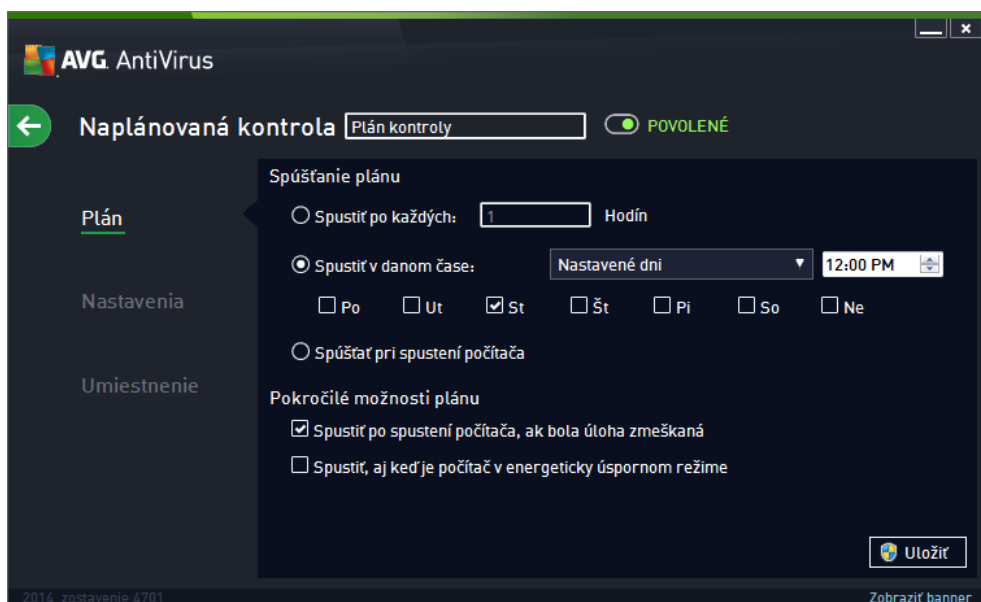


V dialógovom okne môžete zadať svoje vlastné kontroly. Pomocou tlačidla **Prida plán kontroly** si môžete vytvoriť nový plán kontroly. Parametre plánu kontroly sa dajú upraviť (alebo sa dá nastaviť nový plán) v troch kartách:

- [Plán](#)
- [Nastavenia](#)
- [Umiestnenie](#)

Na každej záložke stojí 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 používať stručné, opisné a výstižné názvy pre kontroly, aby sa dali neskôr ľahšie navzájom odlišiť. Príklad: Nie je vhodné nazývať kontrolu "Nová kontrola" alebo "Moja kontrola", pretože tieto názvy sa nevyzývajú na to, aby kontrola vlastne preveruje. Na druhej strane, príkladom dobrého opisného názvu je „Kontrola systémových oblastí“ a pod.

Toto dialógové okno umožňuje alej definovať tieto parametre kontroly:

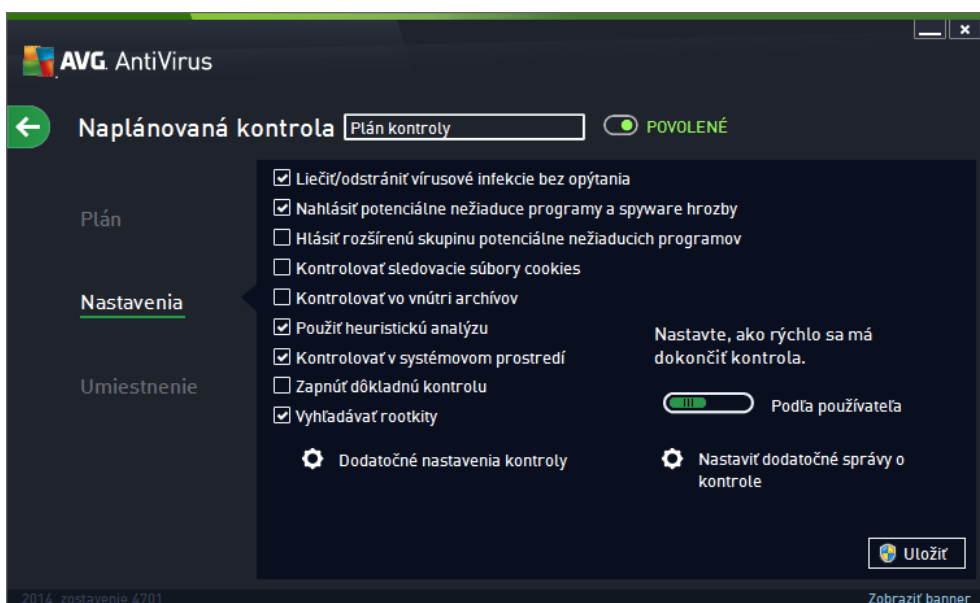
- **Spustená kontrola** – tu môžete nastaviť časové intervaly pre novonaplánované spustenie kontroly. Čas spúšťania sa definuje ako opakované spúšťanie kontroly po uplynutí určitého času (*Spustiť po každých ...*), definovaním presného dátumu a času (*Spúšťať v konkrétnom časovom intervale ...*), prípadne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

- **Uloží** – 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 šípku v ľavej hornej časti okna sa dostanete naspäť do prehľadu [Naplánovaných kontrol](#).

10.4.2. Nastavenia



V ľavej 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 odlišiť. Príklad: Nie je vhodné nazývať kontrolu "Nová kontrola" alebo "Moja kontrola", pretože tieto názvy sa nevyzývajú 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 voľne zapnúť / vypnúť. **Ak nemáte závažný dôvod meniť tieto nastavenia, odporujeme vám ponechať vopred definovanú konfiguráciu.**

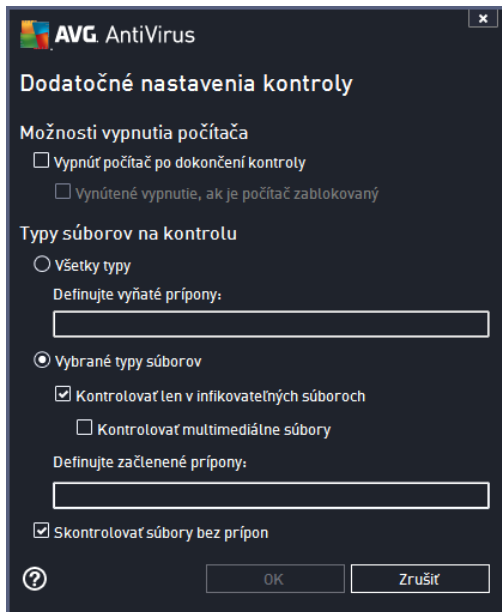
- **Liečiť / odstrániť vírusovú infekciu bez opýtania** (štandardne zapnuté) – ak sa počas kontroly nájde vírus, môže byť automaticky vyliečený, pokiaľ je liek k dispozícii. Ak nie je

možné infikovaný súbor vylíči automaticky, premiestni sa do [Vírusového trezora](#).

- **Nahlási potenciálne nežiaduce programy a spyware hrozby** (štandardne zapnuté) – začiarknite toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu malwaru: 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.
- **Hlási 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 blokovать dobré programy, a preto je táto funkcia štandardne vypnutá.
- **Kontrolova sledovacie súbory cookies** (štandardne vypnuté) – tento parameter súčasti zapína funkciu na detekciu súborov cookies počas prehadávania; (*HTTP cookies sa používajú na overenie totožnosti, sledovanie a správu konkrétnych informácií o používateľovi, akými sú napr. preferencie stránok alebo obsah elektronických nákupných košíkov*).
- **Kontrolova 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, ...
- **Použi 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.
- **Kontrolova systémové prostredie** (štandardne zapnuté) – počas kontroly sa budú overovať aj systémové oblasti počítača.
- **Zapnú dôkladnú kontrolu** (štandardne vypnuté) – v určitých situáciách (*podозrenie na infikovanie počítača*) môžete touto možnosťou aktivovať najdôkladnejšie kontrolné algoritmy, ktoré pre istotu skontrolujú aj tie oblasti počítača, ktoré sa obyčajne vôbec neinfikujú. Upozorujeme však, že tento spôsob je náročný na čas.
- **Kontrolova rootkity** (štandardne zapnuté) – kontrola súčasti Anti-Rootkit skontroluje počítača zisťuje prítomnosť potenciálnych rootkitov, t. j. programov a technológií, ktoré dokážu zakryť existenciu malwaru v počítači. Keď program deteguje rootkit, nemusí to nevyhnutne znamenať, že je počítač infikovaný. V niektorých prípadoch sa môžu určitým spôsobom ovládať alebo súčasti bežných aplikácií nesprávne označovať ako rootkity.

Ďalšie nastavenia kontroly

Odkaz otvorí nové dialógové okno **Dodatné 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 špeciálnou 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 súbory* – ak necháte toto políčko nezaškrtnuté, potom sa čas kontroly skráti ešte viac, pretože tieto súbory sú často veľmi veľké, pričom pravdepodobnosť napadnutia vírusom je veľmi malá). Znova môžete definovať, pod aké 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.

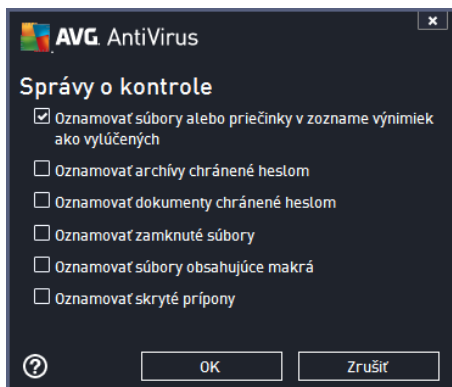
Nastaviť rýchlosť dokončenia kontroly

V tejto časti môžete alej 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 využitie systémových zdrojov a spomalí 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 pred žením doby trvania kontroly.

Vytvoriť ďalšie správy o kontrole

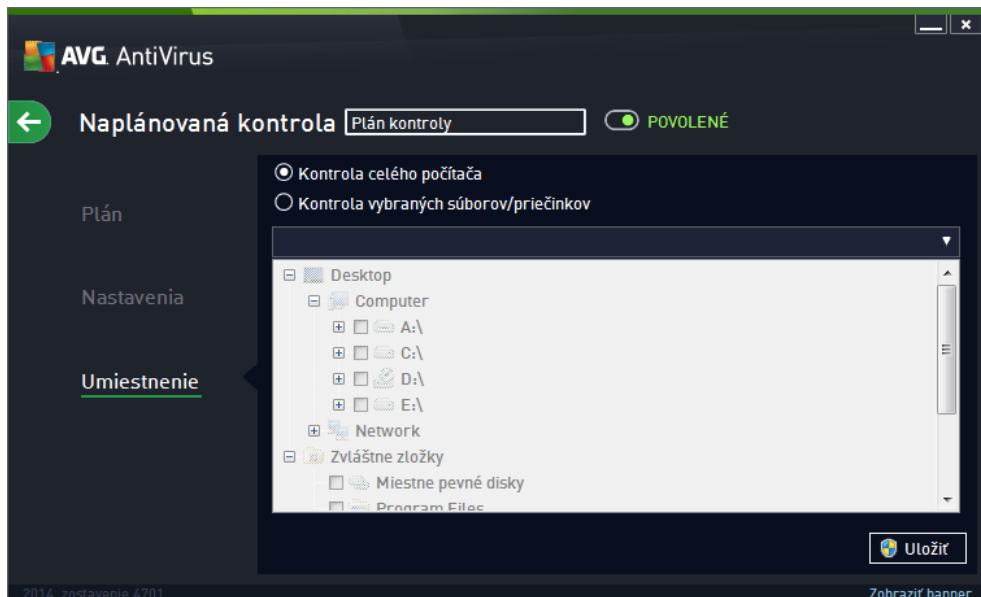
Kliknutím na odkaz **Vytvoriť ďalšie správy o kontrole...** otvorte samostatné dialógové okno s názvom **Správy o kontrole**, v ktorom môžete za kliknutím konkrétnych položiek definovať, ktoré nálezy sa majú hlásiť:



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 (rozbaťte položky kliknutím na uzol so znakom plus a vybrať priečinky, ktoré chcete kontrolovať). Začiarknutím príslušných polí ok 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 bodkou a čiarkou bez medzier).

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

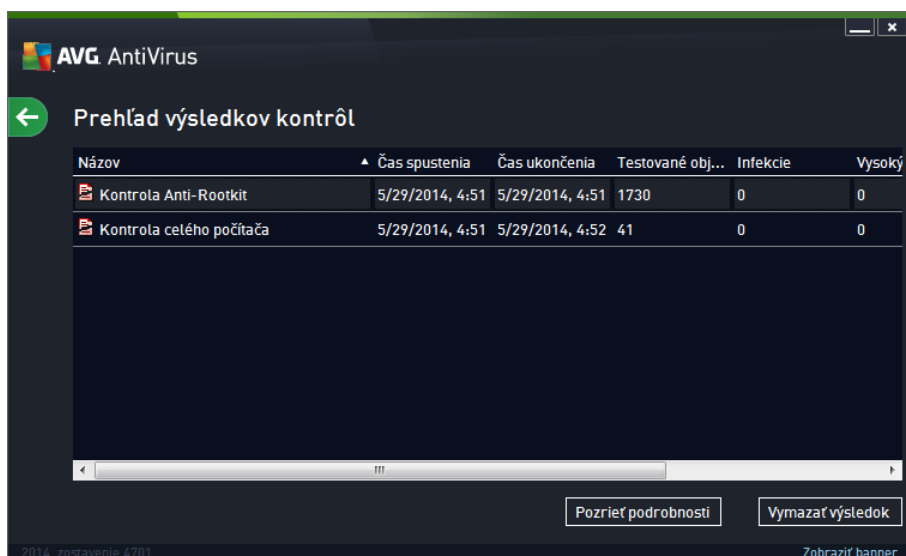
- **Pevné disky počítača** – všetky pevné disky počítača
- **Programové súbory**
 - C:\Program Files\
 - v 64-bitovej verzii C:\Program Files (x86)
- **Priečinko Moje dokumenty**
 - vo Win XP: C:\Documents and Settings\Default User\Moje dokumenty\
 - vo Windows Vista/7: C:\Users\používateľ\Dokumenty\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

- **Uloží** – 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









Názov	Čas spustenia	Čas ukončenia	Testované obj...	Infekcie	Vysoký
Kontrola Anti-Rootkit	5/29/2014, 4:51	5/29/2014, 4:51	1730	0	0
Kontrola celého počítača	5/29/2014, 4:51	5/29/2014, 4:52	41	0	0

2014, zostavenie 4701 Zobrazíť banner

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

kontrol. Tabu ka 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 nevyčistili, kontrola sa dokončila.
 -  Boli nájdené infekcie, ktoré neboli vyčistené, kontrola sa prerušila pred dokončením.
 -  Našli sa infekcie a všetky sa vyčistili alebo odstránili, kontrola sa dokončila.
 -  Boli nájdené infekcie a všetky boli vyčistené 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

Pozrite podrobnosti – kliknutím na tlačidlo zobrazíte [podrobné informácie o vybranej kontrole](#) (označené v tabu ke 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:

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

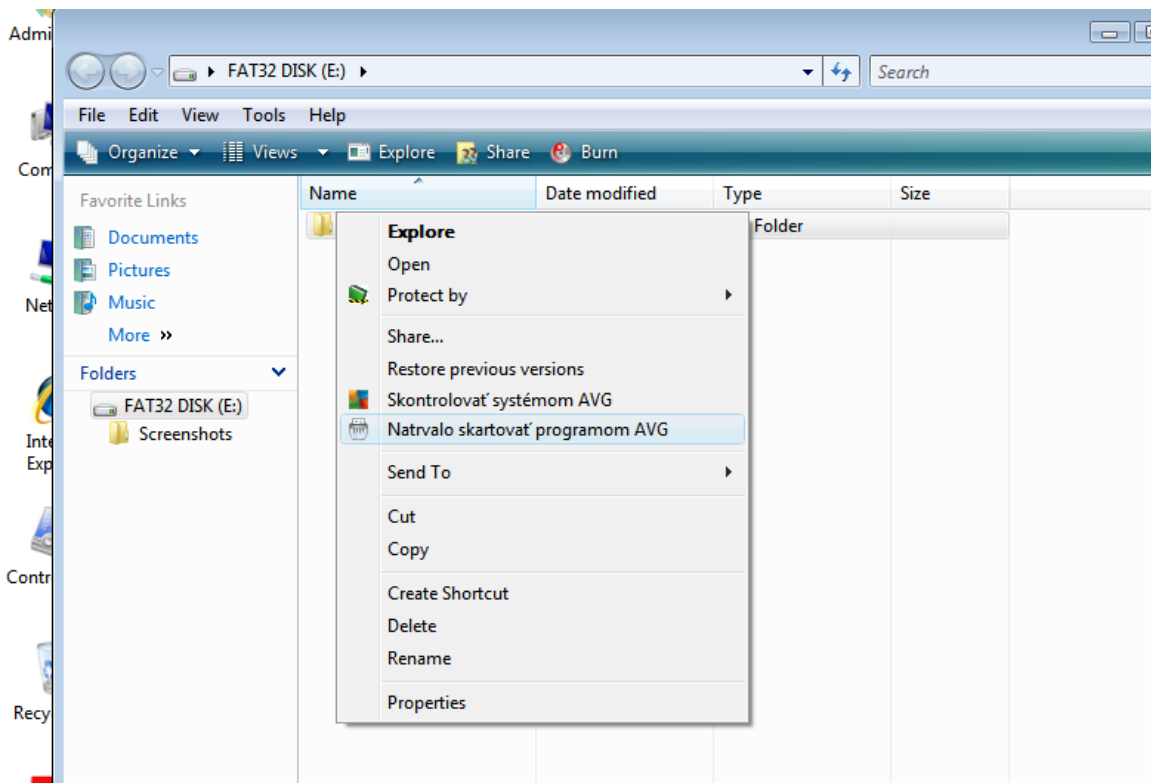
•• **Stredná závažnosť** : obvykle PNP (*potenciálne nežiaduce programy, ako napríklad adware*) alebo sledujúce súbory cookie.

••• **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. AVG File Shredder

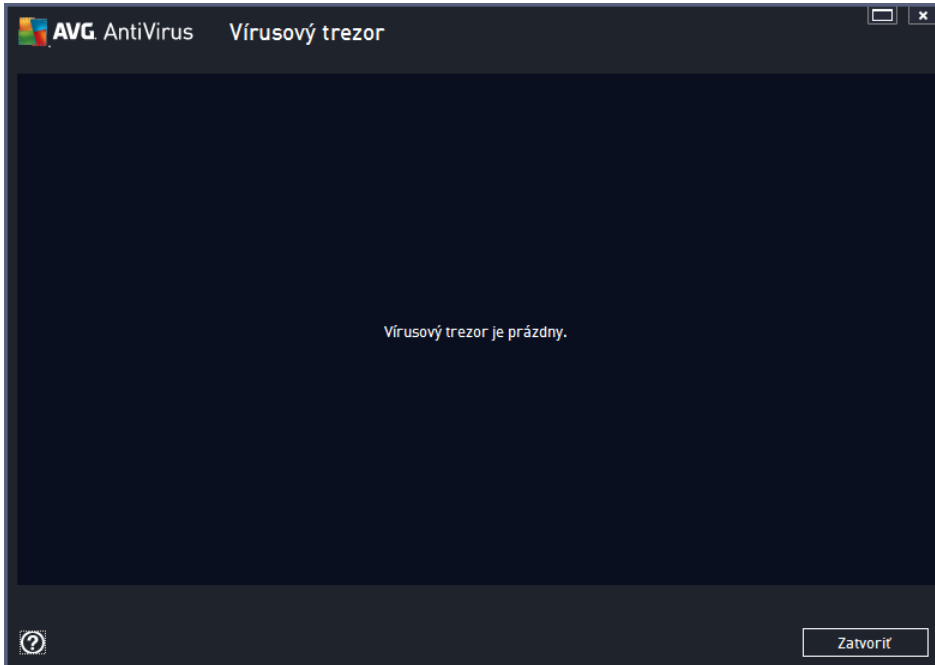
Súčasť **AVG File Shredder** bola navrhnutá na úplne bezpečné vymazávanie súborov, teda bez akejkoľvek možnosti ich obnovenia, dokonca ani s pokročilým softvérom na to určeným.

Ak chcete skartovať súbor alebo priečinok, kliknite na pravým tlačidlom myši v správcovi súborov (*Prieskumník Windows, Total Commander, ...*) a z kontextovej ponuky vyberte možnosť **Natvrvalo skartovať programom AVG**. Súbory v koši môžete takisto skartovať. Ak nebude možné určitý súbor v určitom umiestnení (napr. CD-ROM) skartovať, zobrazí sa oznámenie alebo možnosť v kontextovej ponuke nebude vôbec dostupná.



Vždy pamätajte: Hne ako súbor skartujete, je navždy stratený.

12. 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 vylíčiť, 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 uchovávať 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:

- **Pridaný dátum** – dátum a čas, kedy bol podozrivý súbor detegovaný a presunutý do Vírusového trezora.
- **Úroveň závažnosti** – ak sa rozhodnete nainštalovať súčasnú [Identita](#) do programu **AVG AntiVirus 2014**, 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 infikovanosti – všetky uvedené objekty môžu byť pozitívne alebo potenciálne infikované*).
- **Názov hrozby** – uvádza názov detegovanej infekcie podľa on-line [vírusovej encyklopédie](#).
- **Zdroj** – uvádza, ktorá súčasná **AVG AntiVirus 2014** zistila príslušnú hrozbu.
- **Správa** – 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:

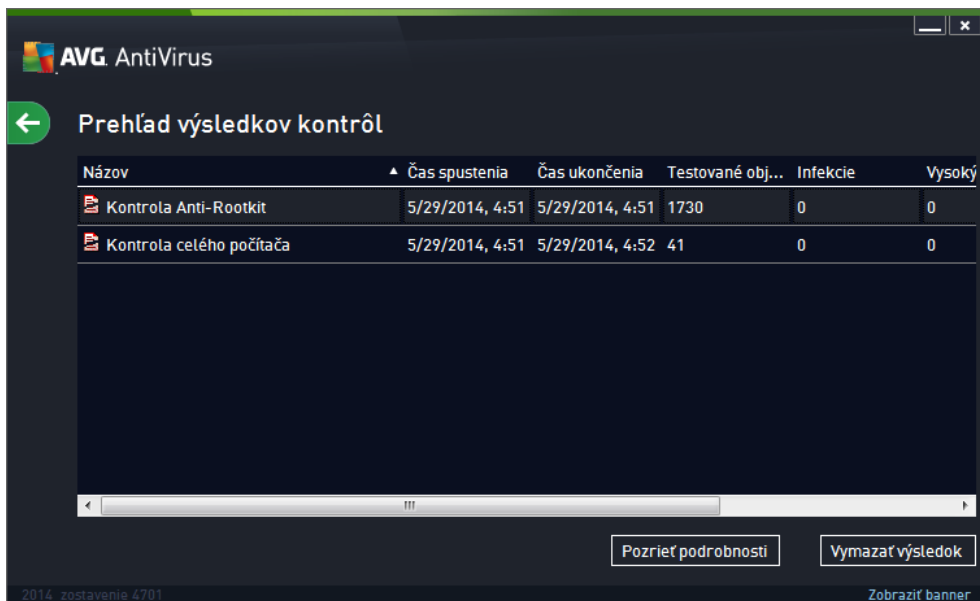
- **Obnoví** – premiestni infikovaný súbor naspäť na jeho pôvodné umiestnenie na vašom disku.
- **Obnoví ako** – premiestni infikovaný súbor do vybraného priečinka.
- **Podrobnosti** – ak chcete zobraziť podrobné informácie o konkrétnej hrozbe vloženú do karantény **Vírusového trezora**, označte vybranú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

13. História

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

- [Výsledky kontrol](#)
- [Nálezy sú stránici Rezidentný štít](#)
- [Nálezy sú stránici Ochrana e-mailu](#)
- [Nálezy sú stránici Webový štít](#)
- [Protokol histórie udalostí](#)


13.1. Výsledky kontrol




Dialógové okno **Prehľad výsledkov kontrol** sa nachádza v ponuke **Možnosti/História/Výsledky kontrol** v hornom navigačnom pruhu hlavného okna programu **AVG AntiVirus 2014**. 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 [Miestnej 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 upozoruje, 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 *Pozrite 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** – v týchto stupňoch sa uvádza číslo odstránených/celkových infekcií nájdených pre každú z úrovní závažnosti (vysokú a strednú).
- **Info** – informácie súvisiace s priebehom a výsledkami kontrolovania (*obvyčajne s jeho dokončením alebo prerušením*).
- **Rootkity** – počet detegovaných [rootkitov](#)

Ovládacie tlačidlá

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

- **Pozrite 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 späť na predvolené [hlavné dialógové okno AVG](#) (*prehľad súčasti*), použite šípku v ľavom hornom rohu tohto dialógového okna

13.2. 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 ihne upozorní zobrazením tohto dialógového okna:

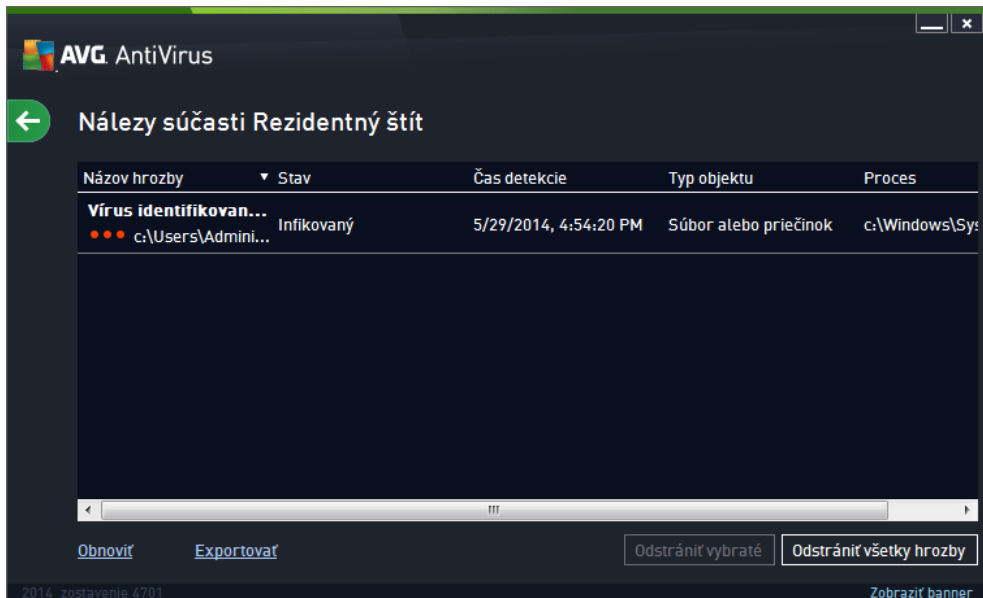


V tomto dialógovom okne s upozomením sa nachádzajú informácie o zistenom objekte, ktorý sa považuje za infikovaný (*Hrozba*), a kratší popis rozpoznanej infekcie (*Popis*). Odkaz [Zobrazí podrobnosti](#) vás presmeruje na on-line vírusovú encyklopédiu, kde nájdete podrobné informácie o zistenej infekcii,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

Poznámka: Môže sa stať, že keď sa vírus objaví v počítači, ktorý je pripojený k sieťovej zdieľanej jednotke, vírus sa môže šíriť do ostatných počítačov v sieti. V tomto prípade sa zobrazí upozornenie informujúce o probléme v súvislosti s sieťovou zdieľanou jednotkou infikovaného objektu do Vírusového trezora. Veľkosť Vírusového trezora však môžete zmeniť. Je definovaná ako nastavené percento skutočnej veľkosti vášho pevného disku. Na zväčšenie veľkosti Vírusového trezora otvorte dialógové okno [Vírusový trezor](#) v nastaveniach [Rozšírené nastavenia programu AVG](#) kliknutím na možnosť „Obmedziť veľkosť Vírusového trezora“.

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


Zoznam všetkých nálezov súčasti Rezydentný štít si môžete pozrieť v dialógovom okne **Nálezy súčasti Rezydentný štít**. Toto dialógové okno sa nachádza pod položkou ponuky **Možnosti/História/Nálezy súčasti Rezydentný štít** v hornom navigačnom pruhu [hlavného okna](#) aplikácie **AVG AntiVirus 2014**. Toto okno obsahuje prehľad objektov detegovaných súčastou Rezydentný štít vyhodnotených ako nebezpečné, ktoré boli buď vyčistené alebo premiestnené do [Vírusového trezora](#).



Pre každý detegovaný objekt sa zobrazia tieto informácie:

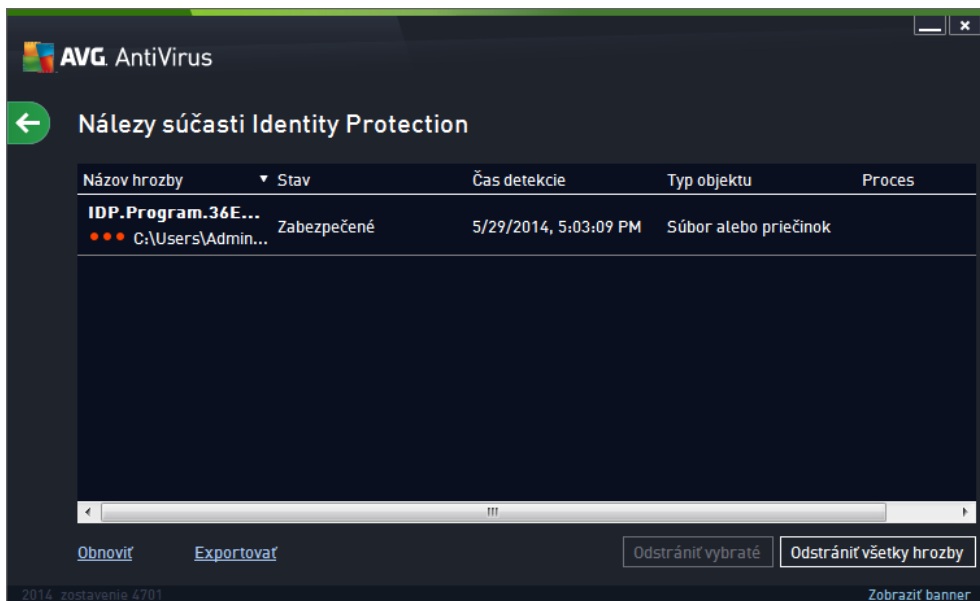
- **Názov hrozby** – popis (prípadne aj názov) zisteného objektu a jeho umiestnenie.
- **Výsledok** – akcia urobená na detegovanom objekte.
- **as detekcie** – dátum a čas detegovania a zablokovania hrozby.
- **Typ objektu** – typ detegovaného objektu.
- **Proces** – aká akcia sa vykonala na zavolaní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

Ovládacie tlačidlá

- **Obnovi** – aktualizuje sa zoznam nálezov zistených súčastiou **Webový štít**.
- **Exportova** – exportuje celý zoznam zistených objektov do súboru.
- **Odstráni vybrané** – v zozname môžete označiť iba vybrané záznamy a týmto tlačidlom ich vymažete.
- **Odstráni všetky hrozby** – týmto tlačidlom vymažete všetky záznamy v dialógovom okne.
-  – Ak chcete prepnúť späť na predvolené [hlavné dialógové okno AVG](#) (prehľad súčasti), použijete šípku v ľavom hornom rohu tohto dialógového okna.

13.3. Nálezy súčasti Identity Protection

Dialógové okno **Nálezy súčasti Identity Protection** je dostupné prostredníctvom ponuky **Možnosti / História / Nálezy súčasti Identity Protection** v hornom navigačnom pruhu hlavného okna programu AVG AntiVirus 2014.



Toto okno obsahuje zoznam všetkých detekcií súčasti [Identity Protection](#). Pre každý detegovaný objekt sa zobrazia tieto informácie:


- **Názov hrozby** – popis (prípadne aj názov) detegovaného 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 zavolaní 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 (**Vyprázdni zoznam**).

Ovládacie tlačidlá

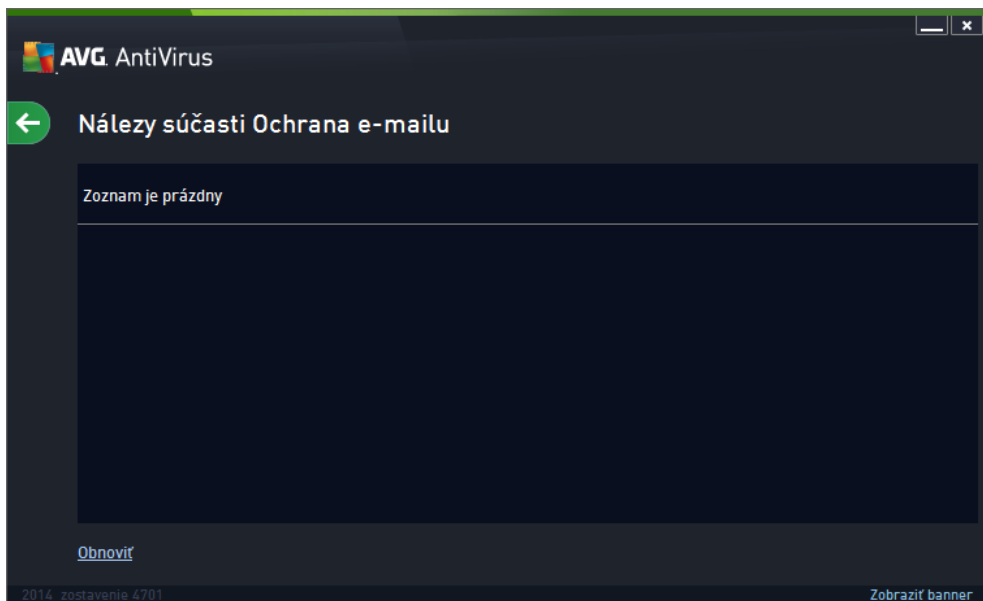
V rozhraní **výsledkov kontroly Identity Protection** sa nachádzajú tieto ovládacie tlačidlá:

- **Obnoviť zoznam** – aktualizuje zoznam detegovaných hrozieb.

-  – Ak chcete prepnúť späť na predvolené [hlavné dialógové okno AVG](#) (prehľad súasť), použite šípku v ľavom hornom rohu tohto dialógového okna.

13.4. Nálezy súasť Ochrana e-mailu

Dialógové okno **Nálezy súasť Ochrana e-mailu** je dostupné prostredníctvom ponuky **Možnosti / História / Nálezy súasť Ochrana e-mailu** v hornom navigačnom pruhu hlavného okna programu **AVG AntiVirus 2014**.




Toto okno obsahuje zoznam všetkých detekcií súasť alebo [Kontrola pošty](#). 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 **Detekovanie súasť alebo E-mail Scanner** sa nachádzajú nasledujúce tlačidlá:

- **Obnovi zoznam** – aktualizuje zoznam detekovaných hrozieb.
-  – Ak chcete prepnúť späť na predvolené [hlavné dialógové okno AVG](#) (prehľad súčasti), použijete šípku v ľavom hornom rohu tohto dialógového okna.

13.5. Nálezy súčasti Webový štít

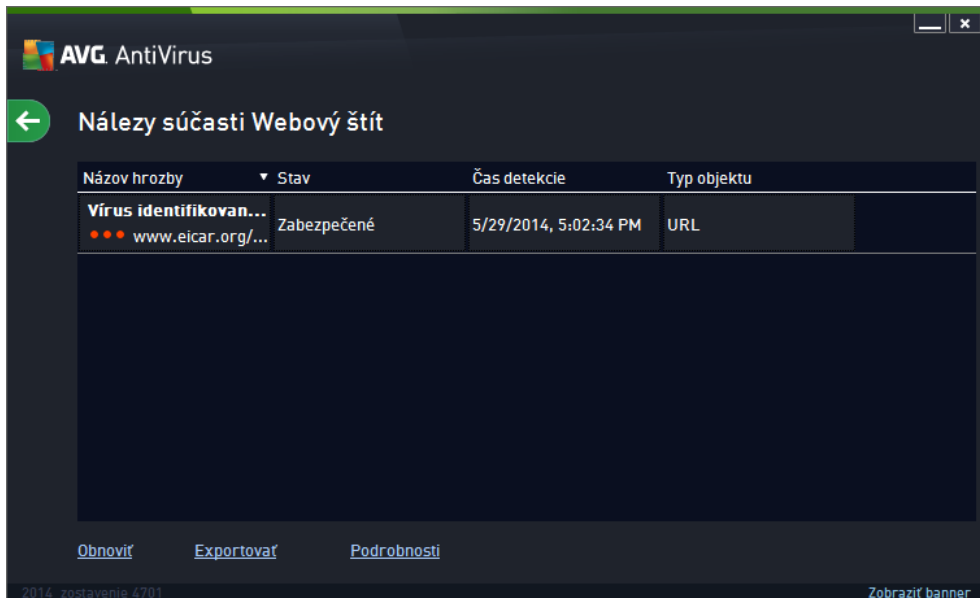
Webový štít kontroluje obsah navštívených internetových stránok a súborov, ktoré sa na nich môžu nachádzať, ešte predtým, než sa zobrazia v internetovom prehliadači alebo prevezmú do počítača. Pri detegovaní hrozby vás program ihneď upozorní otvorením tohto dialógového okna:



V tomto dialógovom okne s upozornením sa nachádzajú informácie o zistenom objekte, ktorý sa považuje za infikovaný (*Hrozba*), a kratší popis rozpoznanej infekcie (*Názov objektu*). Odkaz [Viac informácií](#) 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:

- **Zobrazí 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 2014**.



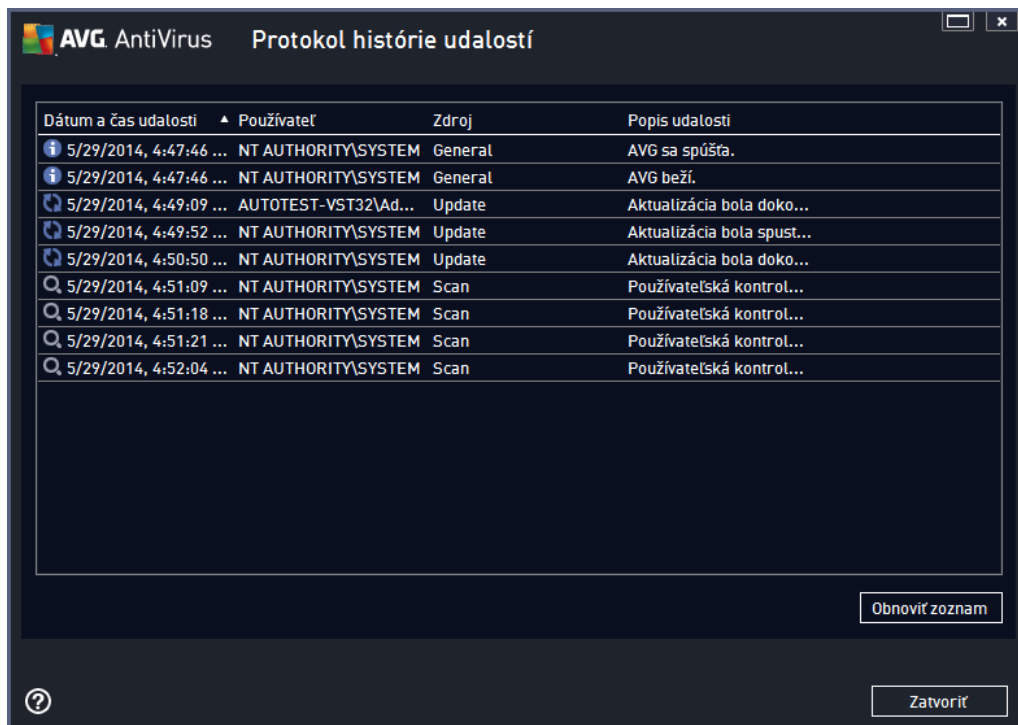
Pre každý detegovaný objekt sa zobrazia tieto informácie:

- **Názov hrozby** – popis (prípadne aj názov) zisteného objektu a jeho zdroja (webovej lokality).
- **Výsledok** – akcia urobená na detegovanom objekte.
- **as detekcie** – dátum a as detegovania a zablokovania hrozby.
- **Typ objektu** – typ detegovaného objektu.
- **Proces** – aká akcia sa vykonala na zavolaní potenciálne nebezpečného objektu, aby sa dal detegovať.

Ovládacie tlačidlá

- **Obnovi** – aktualizuje sa zoznam nálezov zistených súčasti **Webový štít**.
- **Exportova** – exportuje celý zoznam zistených objektov do súboru.
-  – Ak chcete prepnúť späť na predvolené [hlavné dialógové okno AVG](#) (prehľad súčasti), použijete šípku v ľavom hornom rohu tohto dialógového okna.

13.6. 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 2014**. V tomto dialógovom okne sa nachádza prehľad významných udalostí, ktoré sa vyskytli v čase, keď bol program **AVG AntiVirus 2014** spustený. Toto okno obsahuje záznamy týchto typov udalostí: informácie o aktualizáciách aplikácie AVG; informácie o spustení, ukončení alebo zastavení kontroly (vrátane automaticky vykonávaných testov); informácie o udalostiach týkajúcich sa detekcie vírusov (v 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 2014** hlavného okna.

14. 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 hackerov sa objavujú denne. Z tohto dôvodu dodávateľia 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 2014**. Najlepším riešením je ponechať predvolené nastavenia programu, v ktorých sú nastavené automatické aktualizácie. Nezabudnite, že bez aktuálnej vírusovej databázy programu **AVG AntiVirus 2014** 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.

14.1. Spustenie aktualizácie

V záujme maximálneho využitia dostupného zabezpečenia je aplikácia **AVG AntiVirus 2014** predvolene nastavená tak, aby hľadala nové aktualizácie vírusovej databázy každé štyri hodiny. Keďže spoločnosť AVG nezverejňuje aktualizácie pod a pevného harmonogramu, ale podľa potreby 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 aktualizované súbory. Ak program **AVG AntiVirus 2014** zistí prítomnosť nových aktualizovaných 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 spúšania aktualizácie. **Dôrazne sa však odporúča aktualizovať aspoň raz denne!** Konfiguráciu môžete upraviť v nastavení [Rozšírené nastavenia/plánovania](#), konkrétne v týchto dialógových oknách:

- [Plán aktualizácie definícií](#)
- [Plán aktualizácie programu](#)

14.2. Úrovně aktualizácie

Aplikácia **AVG AntiVirus 2014** ponúka na výber dve úrovne aktualizácie:

- **Aktualizácia definícií** obsahuje zmeny potrebné na posilnenie ochrany pred vírusmi. Zvyčajne neobsahuje žiadne zmeny kódu a aktualizuje len databázu definícií. Táto aktualizácia by sa mala používať čo 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 as naplánovanej aktualizácie programu prekrýva s plánom kontroly, aktualizácia má vyššiu prioritu a kontrola sa preruší. V takom prípade budete informovaní o tomto konflikte.

15. FAQ a technická podpora

V prípade nákupných alebo technických problémov s aplikáciou **AVG AntiVirus 2014** 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 hľadani pomoci potrebovať. Dialógové okno obsahuje základné údaje o nainštalovanom programe AVG (verzia programu/databázy), podrobnosti o licencií 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 2014** (súbor pomocníka otvoríte stlačením klávesu F1 v niektorom z dialógových okien aplikácie). V tejto časti nájdete zoznam najčastejších situácií, v ktorých používate potrebuje vyhľadať profesionálnu pomoc pre technický problém. Vyberte situáciu, ktorá najviac zodpovedá vášmu problému, a kliknutím zobrazíte podrobné pokyny vedúce k riešeniu daného problému.
- **Webové stredisko podpory AVG** – riešenie problému môžete vyhľadať 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 rozpracované časté otázky. K tejto časti sa dostanete prostredníctvom ponuky **Centrum podpory / FAQ a návody**. Všetky otázky sú opäť prehľadne rozdelené do kategórií podľa toho, či sa problém týka nákupu, vírusov alebo ide o technickú otázku.
- **AVG ThreatLabs** – osobitná webová stránka spojená s programom AVG (<http://www.avgthreatlabs.com/website-safety-reports/>) venovaná problémom s vírusmi, ktorá poskytuje štruktúrovaný prehľad informácií súvisiacich s hrozbami on-line. Môžete tiež nájsť pokyny na odstránenie vírusov spyware a tipov na zachovanie ochrany.
- **Diskusné fórum** – môžete využiť aj diskusné fórum používateľov produktov AVG na adrese <http://forums.avg.com>.