



AVG Internet Security 2013

Používateľská príručka

Revízia dokumentu 2013.12 (03/12/2013)

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

Tento produkt používa algoritmus MD5 Message-Digest spoločnosti RSA Data Security, Inc., Copyright (C) 1991 – 1992, RSA Data Security, Inc. spoločnosť bola založená v roku 1991.

Tento produkt používa kód z knižnice C-SaCzech, Copyright (c) 1996 – 2001 Jaromir Dolecek (dolecek@ics.muni.cz).

Tento produkt používa knižnicu kompresie zlib, Copyright (c) 1995 – 2002 Jean-loup Gailly a Mark Adler.
Tento produkt používa knižnicu kompresie 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	11
3.6 Nainštalovať AVG Security Toolbar	12
3.7 Priebeh inštalácie	13
3.8 Inštalácia prebehla úspešne	14
4. Po inštalácii	15
4.1 Registrácia produktu	15
4.2 Otvorenie používateľského rozhrania	15
4.3 Kontrola celého počítača	15
4.4 Test EICAR	15
4.5 Predvolená konfigurácia AVG	16
5. Používateľské rozhranie AVG	17
5.1 Horný navigačný rad	18
5.2 Informácie o stave zabezpečenia	23
5.3 Prehľad súčastí	24
5.4 Moje aplikácie	24
5.5 Kontrola/Aktualizovať rýchle odkazy	25
5.6 Ikona v paneli úloh	26
5.7 Miniaplikácia AVG	27
5.8 AVG Advisor	29
5.9 AVG Akcelerátor	30
6. Súčasti AVG	31
6.1 Počítač	31
6.2 Web	32
6.3 Identita	34



6.4 E-mailly	36
6.5 Firewall	37
6.6 Quick Tune	40
7. AVG Security Toolbar	42
8. AVG Do Not Track	44
8.1 Rozhranie aplikácie AVG Do Not Track	44
8.2 Informácie o sledovacích procesoch	46
8.3 Blokovanie sledovacích procesov	47
8.4 Nastavenia aplikácie AVG Do Not Track	47
9. Rozšírené nastavenia programu AVG	49
9.1 Vzhľad	49
9.2 Zvuky	53
9.3 Dočasne vypnúť ochranu AVG	54
9.4 Ochrana počítača	55
9.5 Kontrola pošty	60
9.6 Ochrana prezerania webu	75
9.7 Identity Protection	78
9.8 Kontroly	79
9.9 Plány	84
9.10 Aktualizácia	93
9.11 Výnimky	97
9.12 Vírusový trezor	99
9.13 AVG Sebaochrana	100
9.14 Preferencie ochrany osobných údajov	100
9.15 Ignorovať chybný stav	103
9.16 Aplikácia Advisor – známe siete	104
10. Nastavenia súčasti Firewall	105
10.1 Všeobecné	105
10.2 Aplikácie	107
10.3 Zdieľanie súborov a tlačiarňí	108
10.4 Rozšírené nastavenia	109
10.5 Zadeinované siete	110
10.6 Systémové služby	111
10.7 Protokoly	113
11. Kontrola programom AVG	115



11.1 Vopred definované kontroly.....	116
11.2 Kontrola z prieskumníka.....	124
11.3 Kontrola z príkazového riadka.....	125
11.4 Plánovanie kontroly.....	127
11.5 Výsledky kontrol.....	135
11.6 Podrobnosti výsledkov kontrol.....	137
12. Vírusový trezor.....	138
13. História.....	140
13.1 Výsledky kontrol.....	140
13.2 Nálezy súčasti Rezidentný štít.....	141
13.3 Nálezy súčasti Ochrana e-mailu.....	144
13.4 Nálezy súčasti Webový štít.....	145
13.5 Protokol histórie udalostí.....	147
13.6 Protokol súčasti Firewall.....	148
14. Aktualizácie AVG.....	150
14.1 Spustenie aktualizácie.....	150
14.2 Úrovne aktualizácie.....	150
15. FAQ a technická podpora.....	152



1. Úvod

Táto príručka podrobne dokumentuje produkt **AVG Internet Security 2013**.

Produkt **AVG Internet Security 2013** ponúka niekoľko vrstiev ochrany pre celú on-line činnosť, takže sa nemusíte obávať odcudzenia identity, vírusov ani otvorenia škodlivých lokalít. AVG Protective Cloud Technology a AVG Community Protection Network sú súčasťou balíka, čo znamená, že zhromažďujeme informácie o najnovších hrozbách a zdieľame ich v rámci našej komunity, aby sa vám dostala najlepšia možná ochrana. Môžete bezpečne nakupovať a spravovať on-line bankové účty, používať sociálne siete alebo surfovať a vyhľadávať informácie – môžete sa spoľahnúť na ochranu v reálnom čase.



2. Požiadavky na inštaláciu produktu AVG

2.1. Podporované operačné systémy

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

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

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

Poznámka: Súčasťou [Identita](#) nepodporuje 64-bitové operačné systémy Windows XP. Produkt AVG Internet Security 2013 sa môže inštalovať pod týmto operačným systémom, ale bez súčasti IDP.

2.2. Minimálne a odporúčané hardvérové požiadavky

Minimálne hardvérové požiadavky pre produkt **AVG Internet Security 2013**:

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

Odporúčané hardvérové požiadavky pre produkt **AVG Internet Security 2013**:

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

3. Proces inštalácie produktu AVG

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

Ak nevíete, 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. alej ponúkame podrobné vysvetlenia každého z dialógových okien:

3.1. Vitajte! Výber jazyka

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

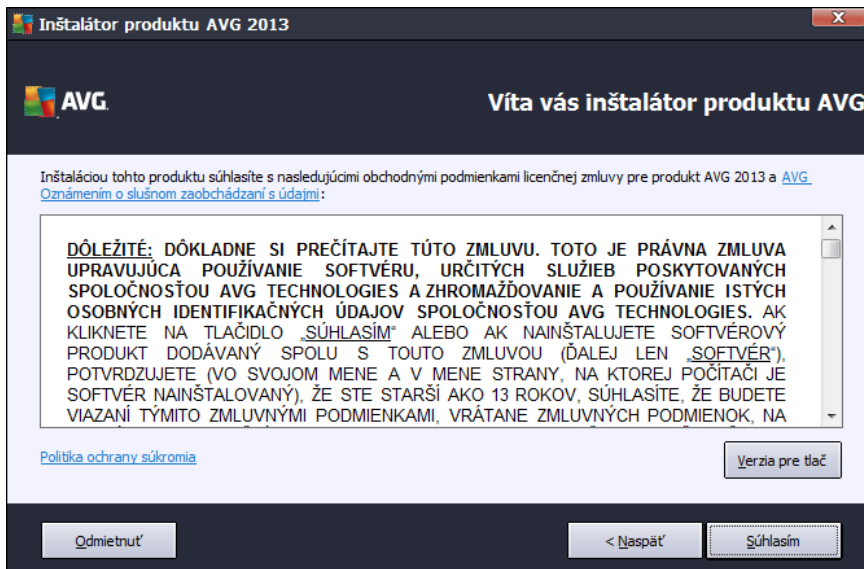


V tomto dialógovom okne zvolíte jazyk, ktorý sa použije pri procese inštalácie. Kliknutím na rozbaňovací pole zobrazíte ponuku jazykov. Vyberte požadovaný jazyk a proces inštalácie sa posunie k výberu jazyka.

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

3.2. Vitajte! Licenčná zmluva

Dialógové okno *Víta vás sprievodca inštaláciou AVG* ponúka úplné znenie 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.

Ochrana osobných údajov v spo lo nosti AVG

Okrem licen nej zmluvy ponúka toto inštalá né okno aj možnos zisti viac o **Zásadách slušnosti pri spracovaní údajov v spo lo nosti AVG**, **personalizácii AVG** a **Ochrane osobných údajov v spo lo nosti AVG** (všetky uvedené funkcie sú zobrazené v dialógovom okne v podobe aktívneho hypertextového odkazu, ktorý vás presmeruje na príslušnú webovú lokalitu s podrobnejšími informáciami). Kliknutím na príslušný odkaz budete presmerovaní na webovú lokalitu AVG (<http://www.avg.com/>), kde nájdete plné znenie týchto vyjadrení.

Ovládacie tla idlá

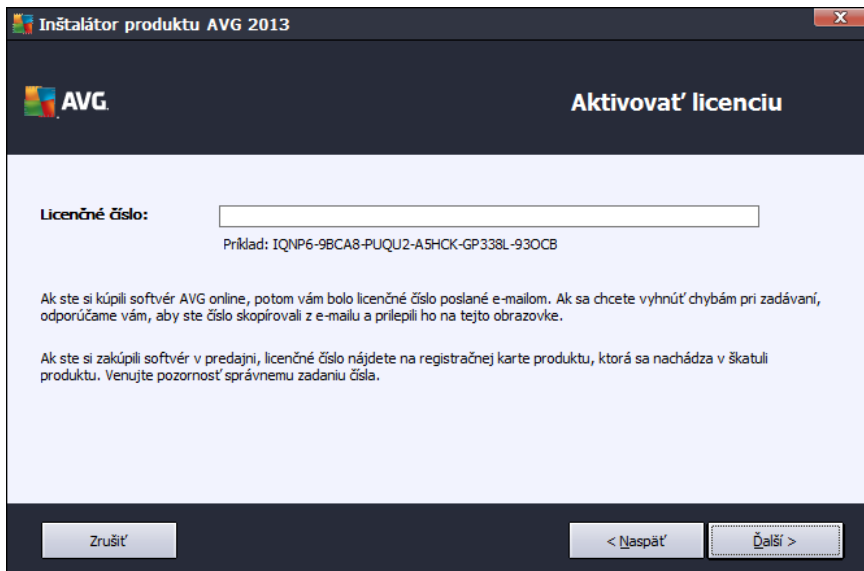
V prvom dialógovom okne inštalácie sa nachádzajú iba dve ovládacie tla idlá:

- **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. Inštalá ný postup sa okamžite ukon í. Aplikácia **AVG Internet Security 2013** 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 pokračovať a zobrazí sa ďalšie inštaláčn é dialógové okno.

3.3. Aktivujte si licenciu

V dialógovom okne **Aktivujte si licenciu** zadajte licen né íslo do príslušného textového po a:



Kde nájs licen né íslo

Predajné íslo sa nachádza na obale disku CD v škatuli produktu **AVG Internet Security 2013**. Licen né íslo sa nachádza v e-mailovej správe s potvrdením, ktorú ste dostali po zakúpení produktu **AVG Internet Security 2013** on-line. íslo sa musí zadať presne tak, ako je uvedené. Ak máte k dispozícii licen né íslo v digitálnej podobe (v e-mailovej správe), na jeho vloženie vám odporúame použiť funkciu kopírovania a prilepiť.

Ako používa metódu Kopírovania a Prilepi

Pomocou metódy **Kopírovania a Prilepi** môžete licen né íslo produktu **AVG Internet Security 2013** do programu. Tak zabezpečíte zadanie správneho ísla. Postupujte podľa nasledujúcich pokynov:

- Otvorte e-mail s licen ným íslom
- Kliknite ľavým tlačidlom myši na začiatok licen ného ísla, podržte tlačidlo stlačené a presuňte kurzor myši na koniec ísla. Potom tlačidlo uvoľnite. íslo by sa malo zvýrazniť.
- Stlaďte a podržte kláves **Ctrl** a stlaďte kláves **C**. Tým íslo skopírujete.
- Nasmerujte kurzor a kliknite na miesto, kam chcete skopírované íslo vložiť.
- Stlaďte a podržte kláves **Ctrl** a stlaďte kláves **V**. Tým prilepíte íslo na vybrané miesto.

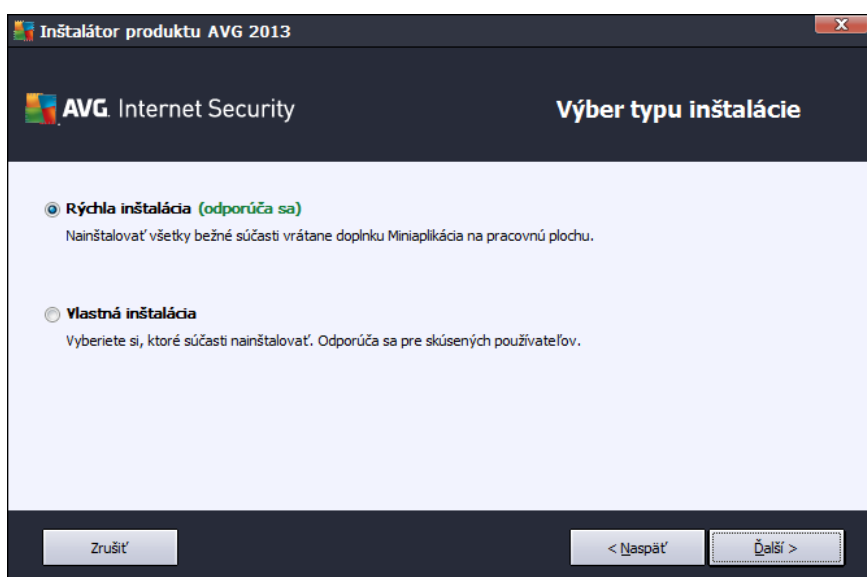
Ovládacie tlačidlá

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

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

3.4. Výber typu inštalácie

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



Expresná inštalácia

Vášine použivate ov odporúame ponecha štandardnú **expresnú** inštaláciu. Takto nainštalujete program **AVG Internet Security 2013** v plne automatickom režime s nastaveniami vopred definovanými dodávateľom programu, vrátane [Miniaplikácie AVG](#), súasti [AVG Security Toolbar](#) nastavením súasti AVG Secure Search ako predvoleného poskytovate a vyhľadávania. Táto konfigurácia poskytuje maximálne zabezpečenie s optimálnym využitím zdrojov. Ak v budúcnosti budete chcieť zmeniť konfiguráciu, vždy to bude možné priamo v aplikácii **AVG Internet Security 2013**.

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

Vlastná inštalácia

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

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

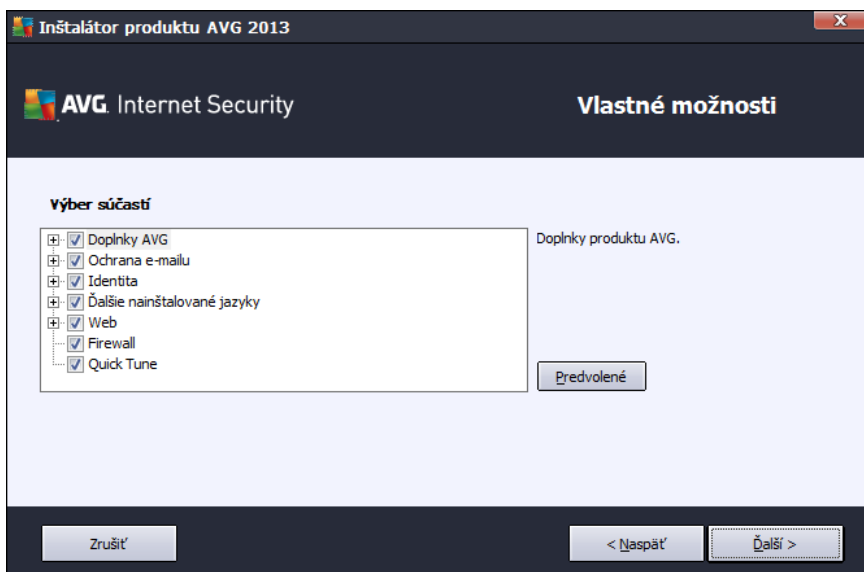
Ovládacie tlačidlá

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

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

3.5. Vlastné možnosti

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



V časti **Výber súčastí** sa nachádza prehľad všetkých súčastí programu **AVG Internet Security**

2013, ktoré je možné inštalovať. Ak vám predvolené nastavenia nevyhovujú, môžete odstrániť/pridať špecifické komponenty. **Môžete však vybrať len tie súčasti, ktoré sú súčasťou edície AVG, ktorú ste si zakúpili!** Zvýraznite položku v zozname **Výber súčastí** a na pravej strane v tejto súčasti 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 použijete tlačidlo **Predvolené**.

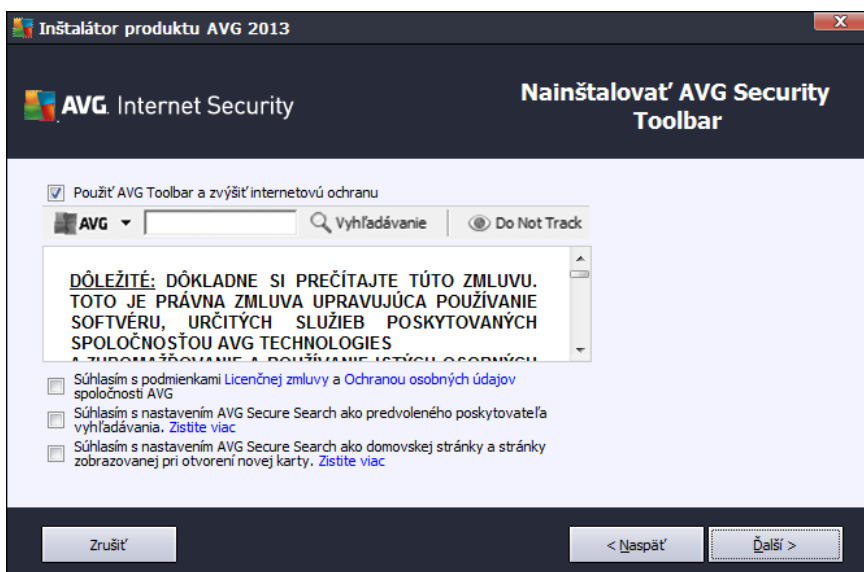
Ovládacie tlačidlá

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

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

3.6. Nainštalovať AVG Security Toolbar

V dialógovom okne **Inštalácia súčastí AVG Security Toolbar** nastavíte, či sa má nainštalovať súčnosť **AVG Security Toolbar**. Ak nezmeníte predvolené nastavenia, potom sa táto súčnosť nainštaluje automaticky do internetového prehliadača (v súčnosť sú podporované prehliadače *Microsoft Internet Explorer vo verzii 6.0 a vyššej* a *Mozilla Firefox vo verzii 3.0 a vyššej*) a bude sa starať o komplexnú ochranu počas surfovania na internete. V súčnosť 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 neokávaným správaním*).

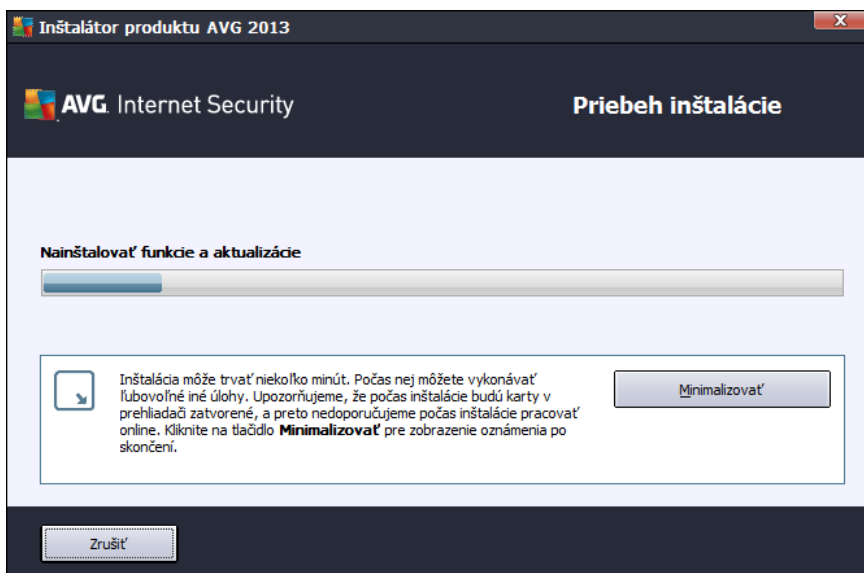


V dialógovom okne sa môžete rozhodnúť ohľadom tejto konfigurácie:

- **Nastavi službu AVG Secure Search ako predvoleného poskytovateľa a vyhľadávania a zachová toto nastavenie** – nechajte políčko zaškrtnuté, čím potvrdíte, že chcete používať ako poskytovateľa a vyhľadávacieho nástroja AVG Secure Search, ktorý úzko spolupracuje s komponentom Link Scanner Surf Shield na zabezpečenie vašej najvyššej bezpečnosti on-line.
- **Nainštalovať panel nástrojov AVG Security Toolbar na zvýšenie internetovej ochrany** – nechajte políčko zaškrtnuté, aby sa nainštaloval panel nástrojov AVG Security Toolbar, ktorý zabezpečí vašu maximálnu bezpečnosť pri prehliadaní internetu.

3.7. Priebeh inštalácie

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



Po dokončení procesu inštalácie sa automaticky otvorí ďalšie dialógové okno.

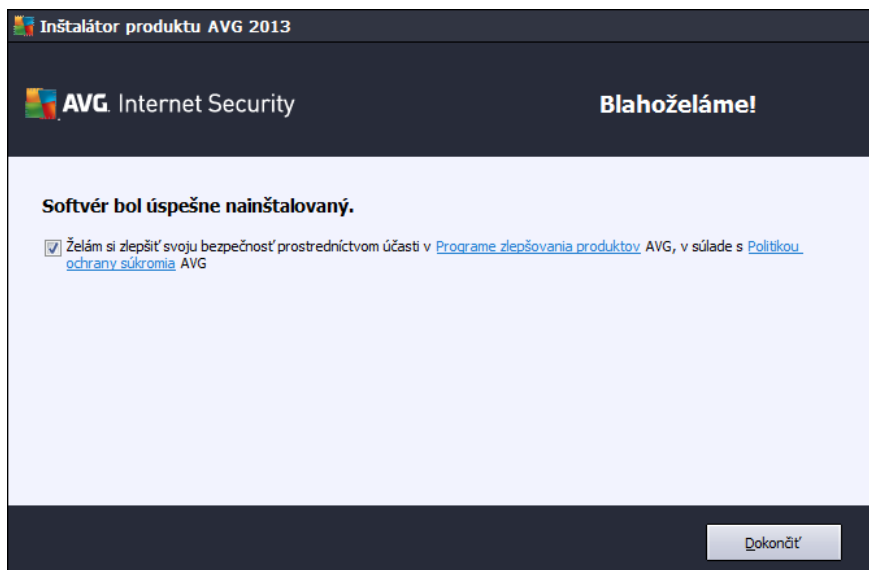
Ovládacie tlačidlá

V tomto dialógovom okne sa nachádzajú dve ovládacie tlačidlá:

- **Minimalizovať** – Proces inštalácie môže trvať niekoľko minút. Kliknutím na toto tlačidlo minimalizujete dialógové okno na ikonu na systémovej lište. Toto okno sa otvorí po dokončení inštalácie.
- **Zrušiť** – Toto tlačidlo použijete iba vtedy, keď chcete zastaviť proces inštalácie. Nezabudnite, že v takom prípade sa aplikácia **AVG Internet Security 2013** nenainštaluje!

3.8. Inštalácia prebehla úspešne

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



Program zlepšovania produktov a Ochrana osobných údajov

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

Inštaláciu dokončíte stlačením tlačidla **Dokončiť**.



4. Po inštalácii

4.1. Registrácia produktu

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

4.2. Otvorenie používateľského rozhrania

[Hlavné dialógové okno AVG](#) sa otvára niekoľkými spôsobmi:

- Dvakrát kliknite na [ikonu AVG v paneli úloh](#)
- Dvakrát kliknite na ikonu AVG na pracovnej ploche
- v ponuke **Štart/Všetky programy/AVG/AVG 2013**

4.3. Kontrola celého počítača

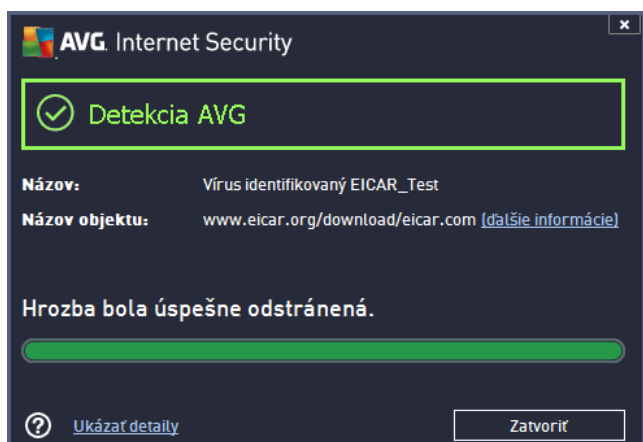
Existuje potenciálne riziko, že sa do vášho počítača dostal počítačový vírus ešte pred nainštalovaním produktu **AVG Internet Security 2013**. Z tohto dôvodu by ste mali spustiť [Kontrolu celého počítača](#), aby sa vylúčila možnosť existencie infekcie v počítači. Prvá kontrola môže trvať asi hodinu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

4.4. Test EICAR

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

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

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



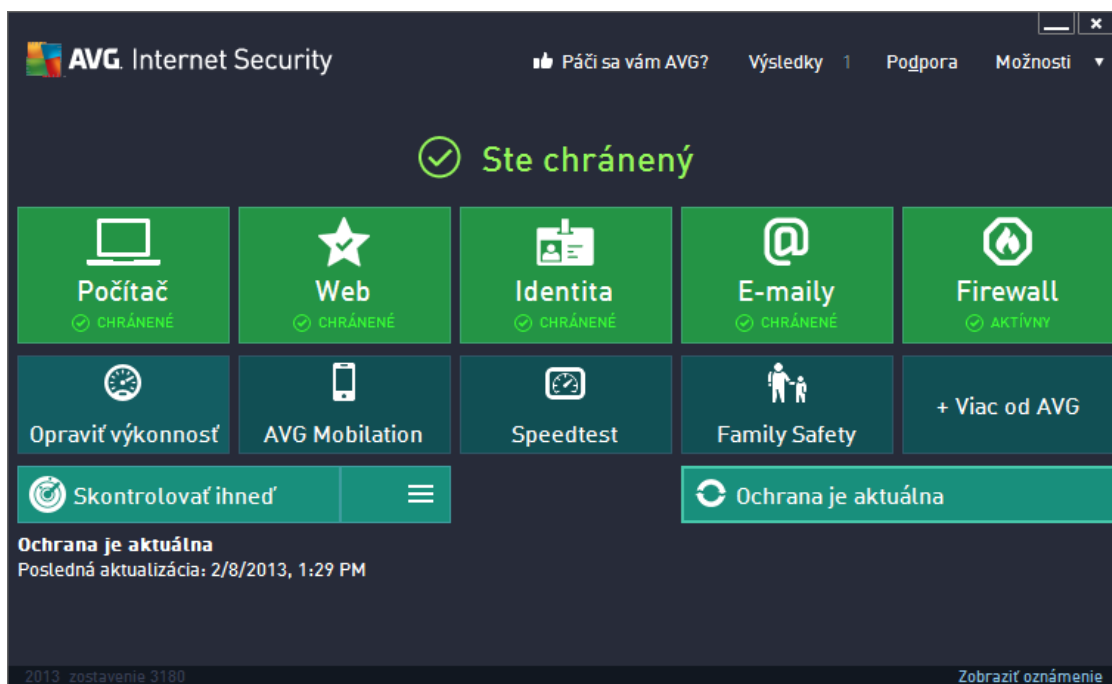
Ak sa programu AVG nepodarí identifikovať testovací súbor EICAR ako vírus, skontrolujte ešte raz konfiguráciu programu!

4.5. Predvolená konfigurácia AVG

Predvolenú konfiguráciu, (t. j. nastavenie aplikácie bezprostredne po inštalácii) produktu **AVG Internet Security 2013**, nastavil dodávateľ softvéru tak, aby všetky súčasti a funkcie fungovali optimálnym spôsobom. **Nemete 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 súčasti [Rozšírené nastavenia programu AVG](#): vyberte položku Hlavnej ponuky *Možnosti/Rozšírené nastavenia* a upravte konfiguráciu programu AVG v novootvorenom dialógovom okne [Rozšírené nastavenia programu AVG](#).

5. Používateľské rozhranie AVG

AVG Internet Security 2013 sa otvára v hlavnom okne:



Hlavné okno je rozdelené na niekoľko častí:

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

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

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

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

5.1. Horný navigačný rad

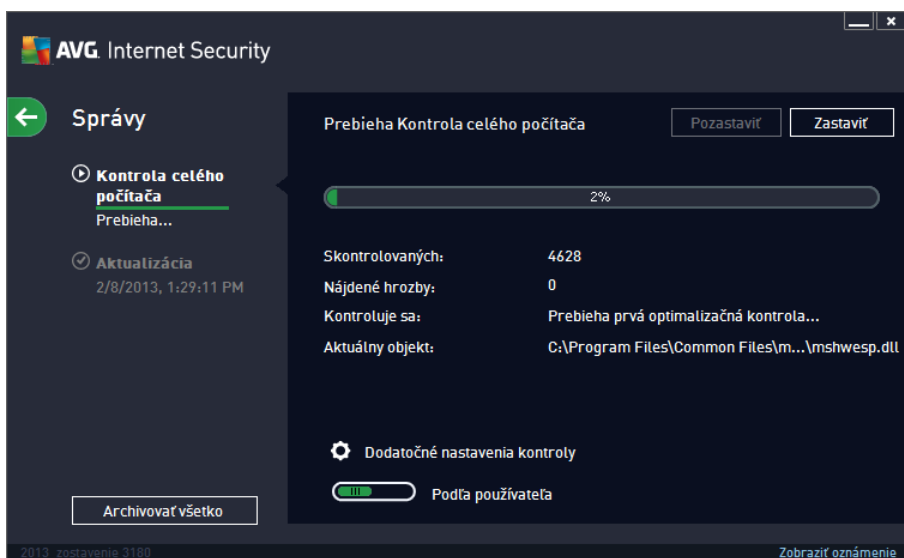
Horný navigačný rad sa skladá z radu viacerých aktívnych odkazov v hornej časti hlavného okna. Navigácia obsahuje tieto tlačidlá:

5.1.1. Páči sa mi AVG

Jedným kliknutím na odkaz sa pripojíte ku [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:



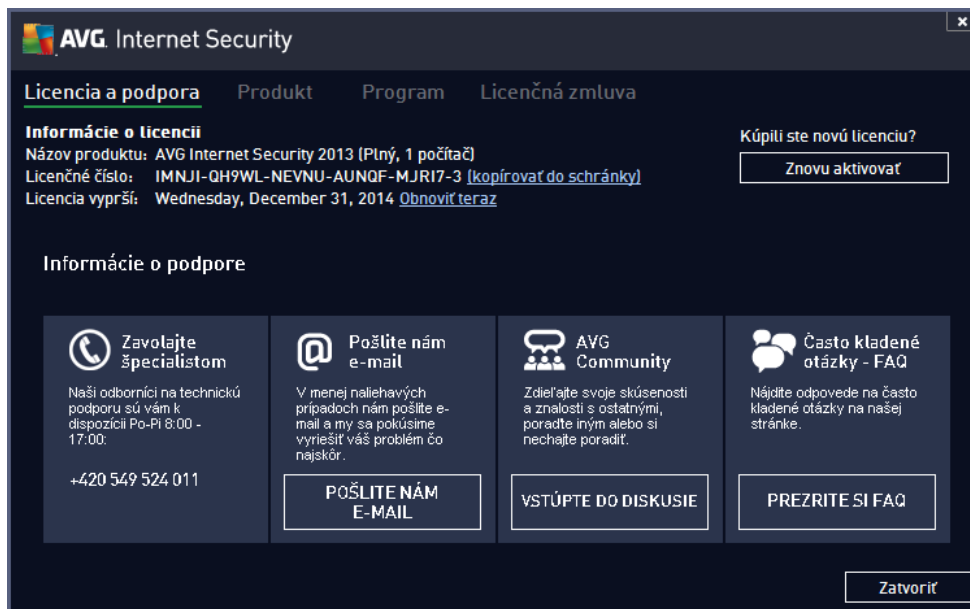
5.1.3. Podpora

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

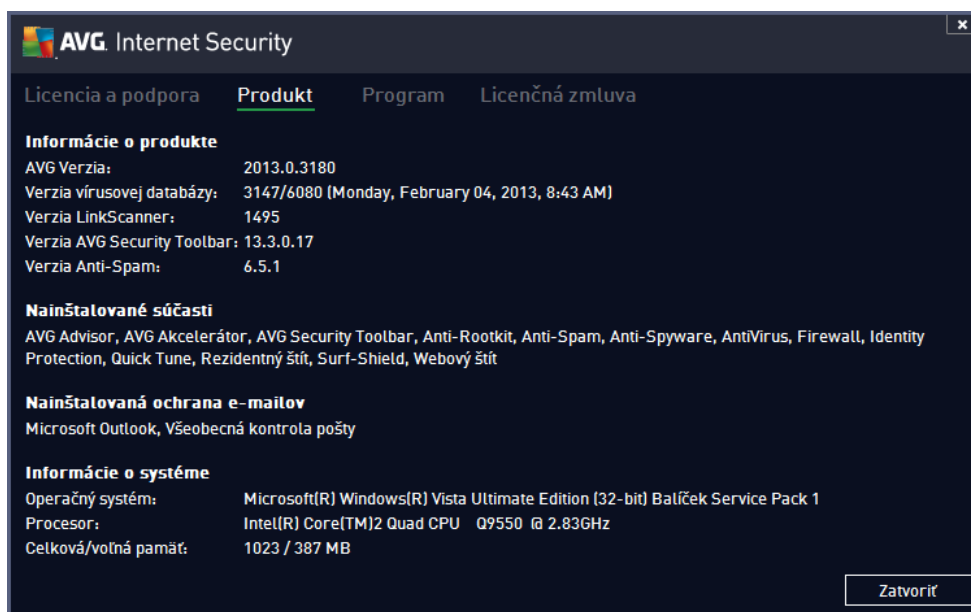
- **Licencia a podpora** – Táto záložka obsahuje informácie o názve produktu, licenčnom čísle a dátume expirácie. V dolnej časti dialógového okna nájdete tiež zoznam dostupných kontaktov na zákaznícku podporu. V tejto záložke sa nachádzajú tieto aktívne odkazy a tlačidlá:
 - **Znovu aktivovať** – Kliknutím otvoríte nové dialógové okno **Aktivovať softvér AVG**. Vyplňte licenčné číslo do príslušného poľa a nahraďte tak predajné číslo (ktoré ste používali počas AVG Internet Security 2013 inštalácie) alebo zmeňte aktuálne číslo

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

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



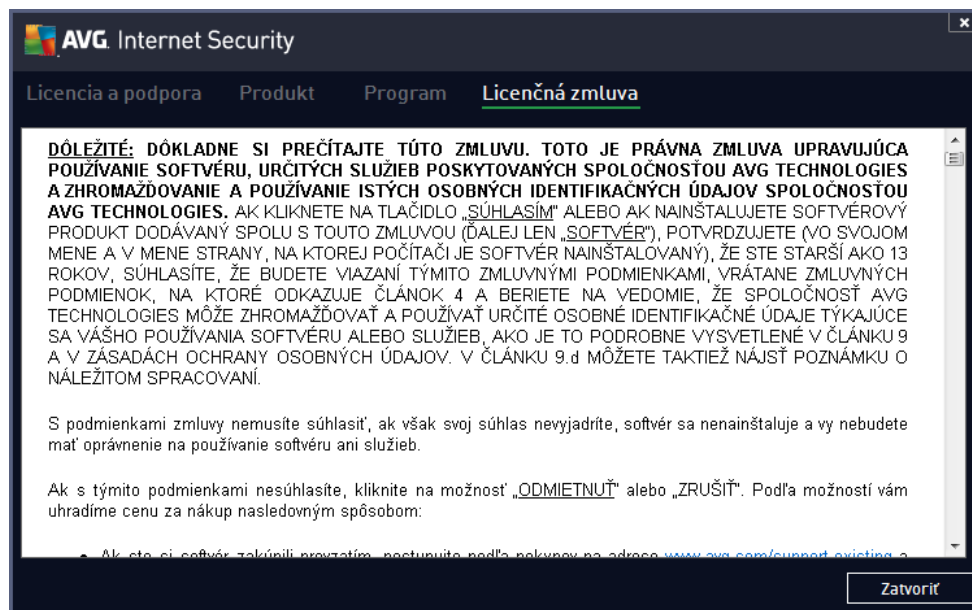
- **Produkt** – na tejto záložke sa nachádza prehľad **AVG Internet Security 2013** najdôležitejších technických údajov týkajúcich sa informácií o produkte, nainštalovaných súčiastkach, nainštalovanej ochrane e-mailu a informácie o systéme:



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



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



5.1.4. Možnosti

Údržba produktu **AVG Internet Security 2013** je dostupná prostredníctvom položky **Možnosti**. Kliknutím na šípku otvoríte rozba ováciu ponuku:

- [Skontrolova celý po íta](#) – Spustí kontrolu celého po íta a.
- [Skontrolova vybraný prie inok...](#) – Otvorí rozhranie kontroly programom AVG a pomocou stromovej štruktúry po íta a umožní definova , ktoré súbory a prie inky sa majú skontrolova .
- [Skontrolova súbor...](#) – Umožní vám spusti na požiadanie test konkrétneho súboru. Kliknutím na túto možnos sa otvorí nové okno so stromovou štruktúrou disku. Vyberte požadovaný súbor a potvr te spustenie kontroly.
- [Aktualizácia](#) – Automaticky spustí aktualizácie produktu **AVG Internet Security 2013**.
- [Aktualizácia z adresára...](#) – Spustí aktualizáciu z aktualiza ných súborov, ktoré sa nachádzajú v nastavenom prie inku na disku po íta a. Túto možnos vám však odporú ame použi len ako núdzové riešenie, napr. v situáciách, ke nie je vytvorené pripojenie na internet (napríklad po íta je infikovaný a odpojený od internetu; po íta je pripojený k sieti bez prístupu na internet a pod.). V novootvorenom okne vyberte prie inok, do ktorého ste predtým uložili aktualiza ný súbor a spustíte proces aktualizácie.
- [Vírusový trezor](#) – Otvorí rozhranie úložiska karantény (Vírusový trezor), do ktorého AVG odstra uje všetky zistené infekcie, ktoré sa z rôznych dôvodov nedajú automaticky vylie i . V tejto karanténe sú infikované súbory izolované a je zaru ená bezpe nos vášho po íta a a zároveň sú infikované súbory uložené pre ich budúcu možnú opravu.
- [História](#) – Ponúka alšie podponuky:
 - [Výsledky kontrol](#) – Otvorí dialógové okno s preh adom výsledkov kontrol.

- [Nálezy sú asti Rezidentný štít](#) – Otvorí dialógové okno s prehľadom hrozieb detegovaných Rezidentným štítom.
- *Ochrana identity Identity Protection* – Otvorí dialógové okno s prehľadom hrozieb detegovaných súčasťou Identity Protection.
- [Nálezy sú asti Ochrana e-mailu](#) – Otvorí dialógové okno s prehľadom príloh e-mailových správ označených súčasťou Ochrana e-mailu ako nebezpečné.
- [Nálezy sú asti Webový štít](#) – Otvorí dialógové okno s prehľadom hrozieb zistených súčasťou Webový štít.
- [Protokol histórie udalostí](#) – Otvorí rozhranie protokolu histórie s prehľadom všetkých zaznamenaných činností aplikácie **AVG Internet Security 2013**.
- [Protokol súčasťou Firewall](#) – Otvorí dialógové okno s podrobným prehľadom o činnosti súčasťou Firewall.
- [Rozšírené nastavenia...](#) – Otvorí dialógové okno s pokročilými nastaveniami programu AVG, kde môžete upraviť **AVG Internet Security 2013** konfiguráciu. Odporúčame vám nemeňte predvolené nastavenia aplikácie definované výrobcou softvéru.
- [Nastavenia súčasťou Firewall...](#) – Otvorí samostatné dialógové okno s rozšírenou konfiguráciou súčasťou Firewall.
- **Obsah pomocníka** – Otvorí súbory pomocníka AVG.
- **Získajte podporu** – Otvorí webovú lokalitu AVG (<http://www.avg.com/>) na stránke strediska podpory zákazníkov.
- **Vaša AVG webová stránka** – Otvorí webovú lokalitu AVG (<http://www.avg.com/>).
- **O vírusoch a hrozbách** – Otvorí on-line vírusovú encyklopédiu, v ktorej si môžete vyhľadať podrobné informácie o identifikovanom víruse.
- **Znova aktivovať** – Otvorí sa dialógové okno **Aktivovať AVG** s údajmi, ktoré ste zadali pri procese inštalácie. Toto dialógové okno sa používa na vloženie licenčného kľúča, buď pri nahradení predajného kľúča (*kľúča, s ktorým ste nainštalovali produkt AVG*), alebo pri nahradení starého licenčného kľúča (*napr. pri upgradovaní na nový produkt AVG*).
- **Zaregistrujte teraz/Môj účet** – spojí vás s registračnou stránkou na webovej lokalite AVG <http://www.avg.com/>. Vyplňte vaše registračné údaje; nárok na bezplatnú technickú podporu získajú len tí zákazníci, ktorí si produkt AVG zaregistrujú. Ak používate skúšobnú verziu produktu **AVG Internet Security 2013**, uvedené dve položky sa zobrazia v podobe **Kúpi teraz** a **Aktivovať** a umožnia vám zakúpiť úplnú verziu programu. Ak je produkt **AVG Internet Security 2013** nainštalovaný pomocou predajného kľúča, položky sa zobrazia v podobe **Registrovať** a **Aktivovať**.
- **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.

5.2. Informácie o stave zabezpečenia

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



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



– Žltá ikona upozorňuje, že **jedna súčasta alebo niekto ko súčasti je nesprávne nakonfigurovaných** a treba venovať pozornosť ich vlastnostiam alebo nastaveniam. Nevyskytuje sa žiaden vážny problém s produktom **AVG Internet Security 2013** a pravdepodobne ste z nejakého dôvodu vypli niektorú súčast. Stále ste chránení. Venujte však pozornosť nastaveniam problémovej súčasti! Nesprávne nastavená súčast sa zobrazí s varovným oranžovým pruhom v [hlavnom používateľskom rozhraní](#).

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

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



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

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

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

Poznámka: Informáciu o stave produktu **AVG Internet Security 2013** vám vždy poskytuje aj [ikona v paneli úloh](#).

5.3. Prehľad súčastí

Prehľad nainštalovaných súčastí nájdete vo vodorovnom pruhu blokov v strednej časti [hlavného okna](#). Súčasti sú zobrazené ako zelené obdĺžniky označené ikonou príslušnej súčasti. Každý obdĺžnik obsahuje informácie o aktuálnom stave ochrany. Ak je súčasná správne nakonfigurovaná a plne funkčná, informácie sú uvedené zelenými písmenami. Ak je súčasná pozastavená, má obmedzenú funkčnosť alebo má poruchu, zobrazí sa varovný text v oranžovom textovom poli.

Dôrazne sa odporúča, aby ste venovali pozornosť príslušným nastaveniam súčastí.

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

Zoznam nainštalovaných súčastí

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

- **Poíta** – tieto súčasti sa týkajú dvoch služieb: **súčasť Rezidentný štít** deteguje vírusy, spyware, červy, trójske kone, neželané spustiteľné súbory a knižnice v systéme a chráni vás pred škodlivým adware. Druhou súčasťou je **Anti-Rootkit**, ktorá kontroluje nebezpečné rootkity ukryté vnútri aplikácií, ovládačov alebo knižníc. [Detaily >>](#)
- **Prezeranie webu** – chráni pred útokmi na webe pri vyhľadávaní a surfovaní na internete. [Detaily >>](#)
- **Identita** – táto súčasť spúša službu **Identity Shield**, ktorá neustále chráni vaše digitálne aktivity pred novými a neznámymi hrozbami na internete. [Detaily >>](#)
- **E-mailly** – Kontroluje prichádzajúce e-mailové správy z hľadiska prítomnosti SPAMU a blokuje vírusy, phishingové útoky a iné hrozby. [Detaily >>](#)
- **Firewall** – Kontroluje komunikáciu na všetkých sieťových portoch, chráni pred útokmi a blokuje každý pokus o prienik. [Detaily >>](#)

Dostupné možnosti

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

5.4. Moje aplikácie

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

- **Mobilná ochrana** je aplikácia, ktorá chráni mobilný telefón proti vírusom a softvéru malware. Poskytuje tiež možnosť diaľkového sledovania telefónu smartphone, pokiaľ by ste s ním stratili kontakt.
- **Súčasť LiveKive** sa používa výlučne na on-line zálohovanie dát na zabezpečených serveroch. LiveKive automaticky zálohuje všetky vaše súbory, fotografie a hudbu na jednom bezpečnom mieste a umožňuje vám zdieľať tieto dáta s rodinou a priateľmi a získať k nim prístup z akéhokoľvek zariadenia s pripojením na internet, vrátane telefónov iPhone a zariadení s operačným systémom Android.
- **Funkcia Family Safety** pomáha chrániť vaše deti pred nevhodnými webovými lokalitami, multimédiami a výsledkami vyhľadávania on-line a hlási vám ich on-line aktivitu. Aplikácia AVG Family Safety obsahuje technológiu sledujúcu 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.
- **Súčasť PC Tuneup** je vyspelý nástroj na podrobnú analýzu a opravu systému, ktorý sa používa na vyhľadanie možností, ako zvýšiť rýchlosť počítača a zlepšiť jeho celkový výkon.
- **MultiMi** sústreďuje všetky e-maily a úlohy na sociálnych sieťach na jednom mieste, čo uľahčuje kontakt s rodinou a priateľmi, vyhľadanie internetu, zdieľanie fotografií, videí a súborov. Aplikácia MultiMi obsahuje službu LinkScanner, ktorá vás chráni pred narastajúcim množstvom hrozieb na webe. Funguje tak, že analyzuje webové stránky za všetkými odkazmi na práve zobrazenej webovej stránke a uistí sa, či sú bezpečné.
- **AVG Toolbar** je k dispozícii priamo v internetovom prehliadači a zabezpečuje maximálnu bezpečnosť pri prezeraní internetu.

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

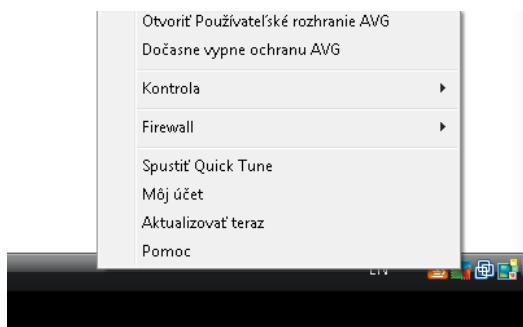
5.5. Kontrola/Aktualizovať rýchle odkazy

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





- **Skontrolovať teraz** – Tlačidlo je graficky rozdelené na dve časti. Odkazom **Skontrolovať ihneď** okamžite spustíte [kontrolu celého počítača](#), môžete sledovať jej priebeh a výsledky v automaticky otvorenom okne [Správy](#). Tlačidlo **Možnosti** otvorí dialógové okno **Možnosti kontroly**, kde môžete [upraviť naplánované kontroly](#) a upraviť parametre [Kontroly celého počítača/Kontroly súborov/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 Internet Security 2013**. Vždy sa nachádza v paneli úloh bez ohľadu na to, či je [používateľské rozhranie](#) produktu **AVG Internet Security 2013** otvorené alebo zatvorené:



Zobrazenie ikony AVG v systémovom paneli úloh

-  Úplne vyfarbená ikona bez ďalších prvkov znamená, že všetky súčasti aplikácie **AVG Internet Security 2013** sú aktívne a úplne funkčné. Takáto ikona sa však môže zobraziť aj vtedy, keď niektorá zo súčastí nie je úplne funkčná, ale používateľ sa rozhodol [ignorovať jej stav](#). (Ak ste potvrdili možnosť ignorovania stavu súčastí, potvrdzujete tým, že ste si vedomí [chybového stavu súčastí](#), ale z nejakého dôvodu ju tak chcete ponechať a nechcete zobrazovať varovania týkajúce sa tejto situácie.)
-  Ikona s výkričníkom znamená, že súčasti (alebo viac súčastí) je v [chybovom stave](#). Takýmto výstrahám vždy venujte pozornosť a snažte sa odstrániť problém konfigurácie súčastí, ktorá nie je nastavená správne. Ak chcete zmeniť konfiguráciu súčastí, dvakrát kliknite na ikonu v paneli úloh. Otvorí sa [používateľské rozhranie aplikácie](#). Podrobné informácie o [chybovom stave](#) jednotlivých súčastí nájdete v súčasti [Informácie o stave zabezpečenia](#).
-  Ikona v paneli úloh sa môže ďalej zobraziť plnofarebne s blikajúcim a otáčajúcim sa majákom. Táto grafická verzia signalizuje, že prebieha aktualizácia.
-  Plnofarebné zobrazenie ikony so šípkou znamená, že **AVG Internet Security 2013** práve prebieha kontrola.

Informácie ikony AVG v systémovom paneli úloh

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



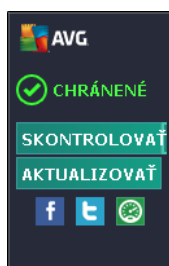
innosti prístupné prostredníctvom ikony AVG v systémovom paneli úloh

Ikonu AVG v systémovom paneli úloh môžete použiť na rýchle zobrazenie [používateľského rozhrania](#) produktu **AVG Internet Security 2013**. Stačí dvakrát kliknúť na ikonu. Kliknutím pravým tlačidlom myši na ikonu sa otvorí krátka kontextová ponuka s týmito možnosťami:

- **Otvorí používateľské rozhranie AVG** – Kliknutím na túto položku sa otvorí [používateľské rozhranie](#) aplikácie **AVG Internet Security 2013**.
- **Dočasne vypnú ochranu AVG** – Táto možnosť umožňuje vypnúť celú ochranu produktom **AVG Internet Security 2013** naraz. Nepoužívajte túto možnosť, ak to nie je naozaj nevyhnutné! Vo väčšine prípadov nie je potrebné vypnúť produkt **AVG Internet Security 2013** 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 Internet Security 2013**, 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, počítač nie je chránený pred útokmi.
- **Kontrola** – Kliknutím na túto možnosť otvoríte kontextovú ponuku [vopred definovaných kontrol](#) ([Kontrola celého počítača](#) a [Kontrola súborov/priečinkov](#)) a vyberte požadovanú kontrolu. Kontrola sa ihneď spustí.
- **Kontroluje sa...** – Táto položka sa zobrazí len v prípade, keď v počítači práve beží kontrola. Tejto kontrole môžete potom nastaviť prioritu, alebo ju môžete zastaviť alebo pozastaviť. Okrem toho sa tu nachádzajú tieto funkcie: *Nastaviť prioritu pre všetky kontroly*, *Pozastaviť všetky kontroly* a *Zastaviť všetky kontroly*.
- **Spustí PC Analyzer** – Kliknutím na túto možnosť sa spustí súhrn PC Analyzer.
- **Môj účet** – 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. Miniaplikácia AVG

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



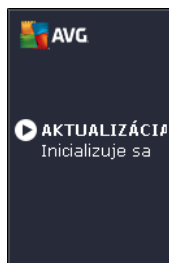
Ovládacie prvky miniaplikácie AVG


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


- **Skontrolova teraz** – Kliknutím na odkaz **Skontrolova teraz** sa priamo spustí [kontrola celého počítača](#). Priebeh kontroly môžete pozorovať v alternatívnom používateľskom rozhraní miniaplikácie. Stručný štatistický prehľad informuje o počte skontrolovaných objektov a detegovaných a vyladených hrozieb. Počas kontroly môžete vždy pozastaviť alebo zastaviť proces. Podrobné informácie súvisiace s výsledkami kontroly sa nachádzajú v štandardnom dialógovom okne [Prehľad výsledkov kontroly](#), ktoré sa otvára priamo v miniaplikácii výberom možnosti **Zobrazí podrobnosti** (príslušné výsledky kontroly budú uvedené pod položkou *Kontrola z miniaplikácie na domovnej paneli*).



- **Aktualizova teraz** – Kliknutím na odkaz **Aktualizova teraz** sa **AVG Internet Security 2013** aktualizuje priamo v miniaplikácii:



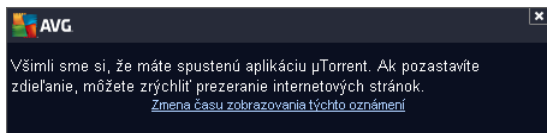
- **Odkaz na Twitter**  – Otvorí nové rozhranie **miniaplikácie AVG** s prehľadom najnovších informácií z kanálov AVG zverejnených na stránkach Twitter. Kliknutím na odkaz **Zobrazí všetky informačné kanály služby Twitter súvisiace s AVG** otvorte nové okno internetového prehliadača a s internetovými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

- **Odkaz na Facebook**  – Otvorí internetový prehliadač s internetovými stránkami Facebook, konkrétne na stránke **komunity AVG**.
- **Vyhľadávacie políčko** – Zadáte kľúčové slovo na okamžité zobrazenie výsledkov vyhľadávania v novom otvorenom okne v predvolenom internetovom prehliadači.

5.8. AVG Advisor

Súčasťou **AVG Advisor** bola navrhnutá tak, aby detegovala problémy, ktoré môžu spomahať vašu prácu 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:



Súčasťou **AVG Advisor** sleduje nasledujúce:

- **Stav akéhokoľvek práve otvoreného internetového prehliadača**. Internetové prehliadače môžu zahŕňať pamäť, predovšetkým v prípade, ak počítač zostane otvorených viacero kariet alebo okien, a môžu spotrebávať mnoho systémových prostriedkov, t. j. spomahať vašu prácu. 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. Súčasťou **AVG Advisor** tomu môže predísť tak, že vás varuje, že známy názov v skutočnosti označuje novú sieť. Samozrejme, ak sa rozhodnete, že neznáma sieť je bezpečná, môžete ju uložiť do zoznamu známych sietí súčasti **AVG Advisor**, aby v budúcnosti nebola znovu nahlasovaná.

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

Podporované webové prehliadače

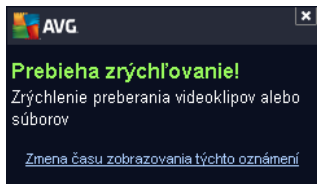
Táto funkcia funguje v týchto webových prehliadačoch: Internet Explorer, Chrome, Firefox, Opera,



Safari.

5.9. AVG Akcelerátor

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

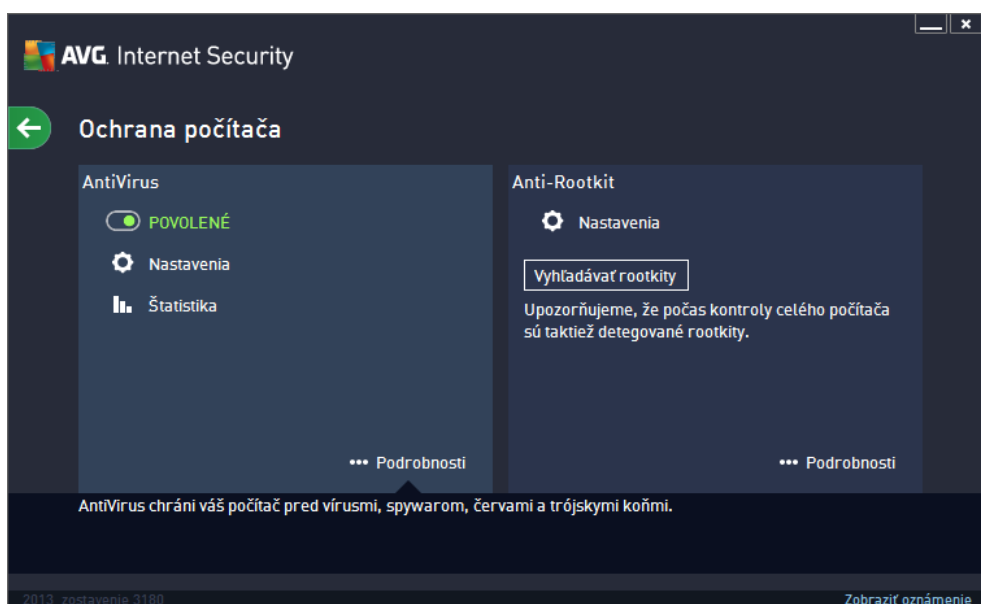


6. Súčasti AVG

6.1. Počítač


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


- **AntiVirus** sa skladá z kontrolného jadra, ktoré stráži všetky súbory, systémové oblasti počítača a vymeniteľné médiá (*disk flash a pod.*) a kontroluje prítomnosť známych vírusov. Každý zistený vírus sa zablokuje, aby nemohol vykonávať žiadnu škodu, a potom sa vymaže alebo sa premiestni do [Vírusového trezora](#). Normálne tento proces ani nezbadáte, pretože rezidentná ochrana je „spustená na pozadí“. Súčasť AntiVirus používa tiež heuristickú kontrolu, pri ktorej sa v súboroch kontrolujú charakteristiky typické pre vírusy. To znamená, že program AntiVirus dokáže zistiť nový, neznámy vírus vtedy, keď obsahuje isté typické vlastnosti existujúcich vírusov. **AVG Internet Security 2013** 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.
- **Anti-Rootkit** je špeciálny nástroj, ktorý zisťuje a efektívne odstraňuje nebezpečné programy rootkit, teda programy a technológie, ktoré môžu zakrývať prítomnosť škodlivého softvéru v počítači. Rootkit je program určený na to, aby sa zmocnil základnej kontroly nad počítačovým systémom bez povolenia vlastníka systému a jeho právoplatných správcov. Súčasť Anti-Rootkit dokáže zistiť prítomnosť programov rootkit pomocou vopred definovanej skupiny pravidiel. Ak súčasť Anti-Rootkit nájde program rootkit, nemusí to nevyhnutne znamenať, že je tento program infikovaný. Programy rootkit sa niekedy používajú ako ovládacie, príp. tvoria súčasť správnych aplikácií.





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 Anti-Rootkit*):

 **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 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 aktívovať čo najskôr.**

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

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

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

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

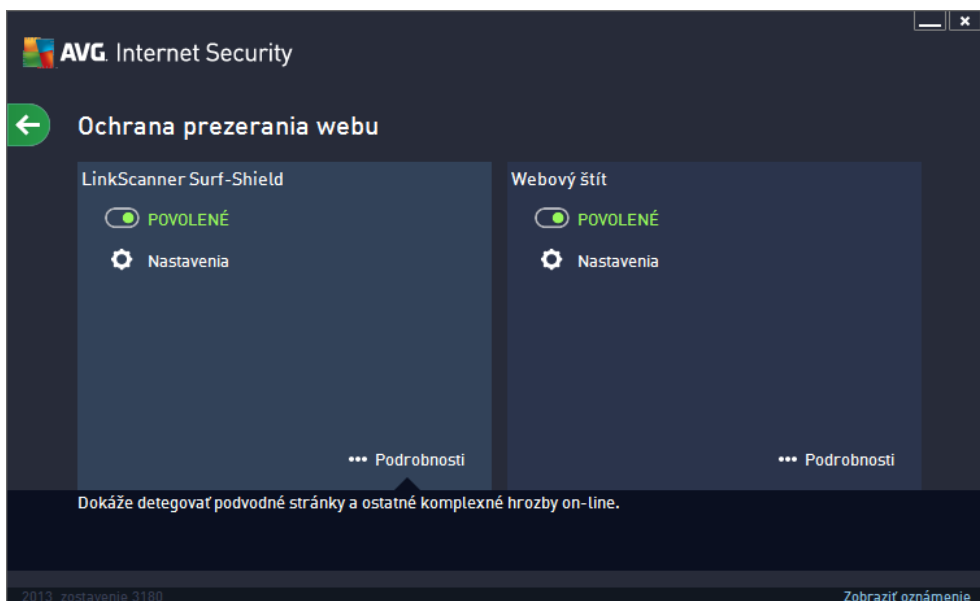
V časti Anti-Rootkit nájdete tiež konkrétne tlačidlo **Kontrola rootkity**, ktorým môžete priamo spustiť nezávislú kontrolu rootkitov (*kontrola rootkitov je však implicitná súčasť [kontroly celého počítača](#)*).

6.2. Web

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


- **LinkScanner Surf-Shield** vás chráni pred narastajúcim počtom hrozieb typu „dnes je tu, zajtra je pre“ na internete. Tieto hrozby sa môžu ukrývať na internetových stránkach akéhokoľvek typu, od vládných až po veľké, od známych značiek až po malé podniky, a len málokedy sa na týchto stránkach udržia viac ako 24 hodín. LinkScanner vás chráni tak, že analyzuje internetové stránky za všetkými odkazmi na internetovej stránke, ktorú prezeráte, a stará sa o to, aby boli bezpečné práve v momente, keď je to najviac dôležité – v momente, keď sa chystáte kliknúť na odkaz. **Súčasť LinkScanner Surf-Shield nie je určená na ochranu serverových platforiem!**
- **Webový štít** je druh rezidentnej ochrany, ktorá pracuje v reálnom čase; prehľadáva obsah navštívených internetových stránok (a súborov, ktoré sa na nich môžu nachádzať) ešte


predtým, než sa zobrazia v internetovom prehliadači alebo prevezmú do počítača. Webový štít zistí prítomnosť nebezpečného kódu JavaScript na stránke, ktorú sa práve chystáte navštíviť, a neumožní stránku zobrazí. Takisto rozpoznáva malware, ktorý sa nachádza na danej stránke, a ihneď zastaví jeho sťahovanie, aby sa nikdy nedostal do vášho počítača. Táto úpravená 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 Webového štítu nie je určená na ochranu na serverových platformách!**




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 (*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 najskejš.**

 **Nastavenia** – Kliknutím na tlačidlo budete presmerovaní na rozhranie [rozšírených nastavení](#). Otvorí sa príslušné dialógové okno a budete môcť nakonfigurovať vybranú službu, t.

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

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

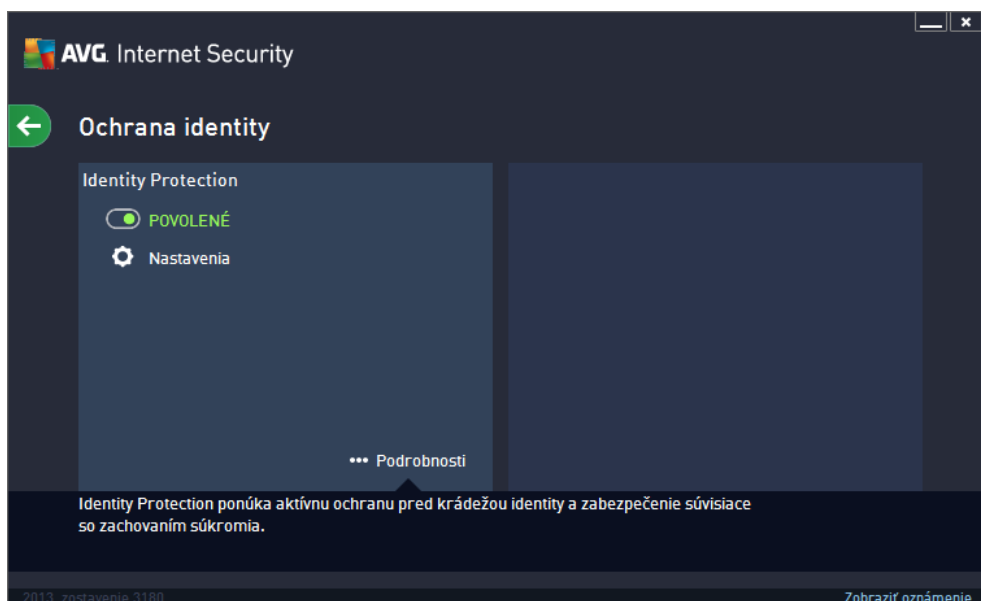
 **Podrobnosti** – Kliknutím na tlačidlo sa v dolnej časti dialógového okna zobrazí stručný popis označenej služby.

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

6.3. Identita


Súčasťou **Identity protection** sú služba **Identity Shield**, ktorá neustále chráni vaše digitálne aktíva pred novými a neznámymi hrozbami na internete:


- **Identity Protection** je služba na ochranu pred škodlivým softvérom, ktorá chráni pred všetkými druhmi škodlivého softvéru (*spyware, softvérové roboty, krádež identity...*) s použitím technológií monitorovania správania a poskytuje okamžitú ochranu pred novými vírusmi. Identity Protection zabráni páchatelom počítačovej trestnej činnosti v oblasti odcudzenia identity, aby odcudzili vaše heslá, informácie o bankových účtoch, čísla kreditných kariet a iné cenné osobné digitálne údaje zo všetkých druhov škodlivého softvéru (*malware*), ktorý útočí na váš počítač. Zabezpečuje správne fungovanie všetkých spustených programov na počítači alebo zdieľanej sieti. Identity Protection zaznamenáva a blokuje podozrivé správanie a chráni počítač pred každým novým malware. Súčasťou Identity Protection je 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 hľadiska 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 aktivít, 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 funkcii. 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 upozorení na možné riziká červeným **varovným** nápisom a oznámením faktu, že momentálne nie ste úplne chránení. **Nezabudnite, že by ste službu mali znovu aktivovať o najskejšor.**

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

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

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

V produkte **AVG Internet Security 2013** 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 Identity Alert.

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

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

6.4. E-mailly


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

- **Kontrola pošty**: Jeden z najbežnejších zdrojov vírusov a trójskych košov je e-mail. Ohrozenia typu phishing a spam alej zvyšujú riziko e-mailu. Bezplatné e-mailové služby sú náchylnejšie na prijímanie takýchto škodlivých e-mailov (*pretože málokedy využívajú technológiu na ochranu pred spamom*) a domáci používatelia sa v pomerne veľkej miere spoliehajú na tieto e-mailové schránky. Domáci používatelia, ktorí surfujú po neznámych stránkach a do online formulárov vypĺňajú osobné údaje (*napr. e-mailové adresy*), sú vo zvýšenej miere vystavení útokom prostredníctvom e-mailu. 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 označuje ako spam (*Spam sa týka nevyžiadanej pošty, ktorá vám šíri propagujúce produkty a služby 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 neoznačíte ako spam*) a [zoznamu zakázaných odosielateľov](#) (*vždy označíte 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 dvomi polohami. Zelená farba symbolizuje stav **Povolené**, čo znamená, že bezpečnostná služba je aktívna a plne funkčná. Červená farba predstavuje stav **Zakázané**, t. j. služba je vypnutá. Ak nemáte dobrý dôvod na vypnutie služby, výrazne odporúčame, aby ste ponechali predvolené nastavenia pre všetky konfigurácie zabezpečenia. Predvolené nastavenia 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 upravovať všetky konfigurácie každej bezpečnostnej služby programu **AVG Internet Security 2013**, no akékoľvek nastavenie odporúčame iba skúseným používateľom!

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

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

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

6.5. Firewall

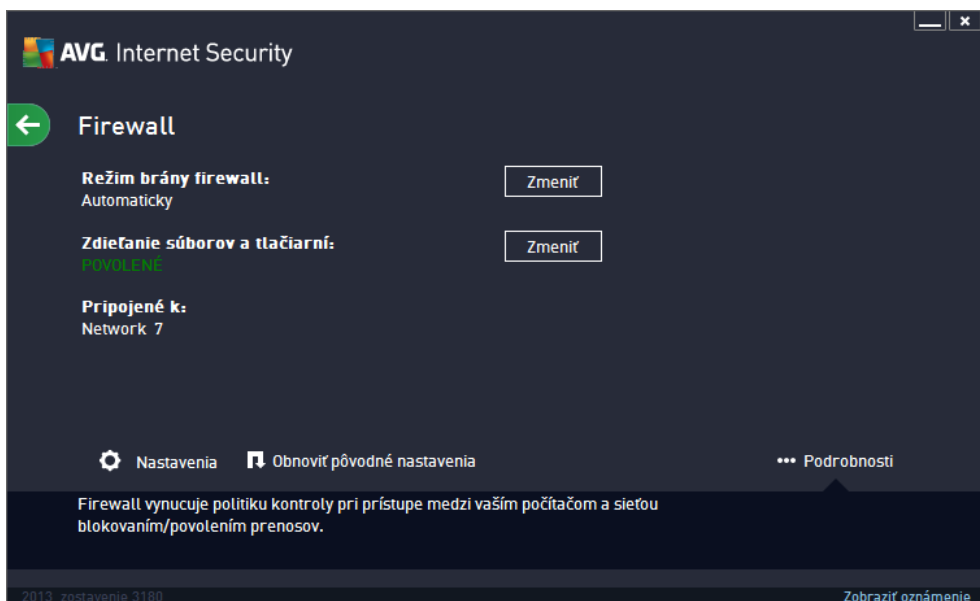
Firewall je systém, ktorý presadzuje zásady riadenia prístupu medzi dvoma alebo viacerými sieťami blokovaním, resp. povolením prenosov. Súčasť Firewall má skupinu pravidiel, ktoré chránia internú sieť pred útokmi *zvonka* (zvyčajne z internetu) a riadi komunikáciu na každom jednom sieťovom porte. Komunikácia sa vyhodnotí podľa definovaných pravidiel a potom sa buď povolí, alebo zakáže. Keď súčasť Firewall zistí pokus o preniknutie do systému, zablokuje ho a nedovolí narušiť ovi vstúpiť do počítača. Súčasť Firewall je nastavená tak, aby umožňovala alebo blokovala internú alebo externú komunikáciu (*oboma smermi, dnu aj von*) na definovaných portoch a pre definované softvérové aplikácie. Súčasť Firewall sa môže nastaviť napríklad tak, aby umožňovala tok webových

dát smerom dnu a von, len keď sa používa program Microsoft Explorer. Každý pokus o prenos webových dát iným prehliadačom sa zablokuje. chráni vaše osobne identifikovateľné informácie, aby sa neposielali z vášho počítača a bez vášho povolenia. Kontroluje spôsob, akým si počítač vymieňa a dáta s ostatnými počítačmi na internete alebo v miestnej sieti. V rámci organizácie brána Firewall chráni samostatné počítače pred útokmi interných používateľov na ostatné počítače v sieti.

V aplikácii **AVG Internet Security 2013** ovláda súhlas **Firewall** celú aktivitu na každom sieťovom porte počítača. Súhlas Firewall na základe vymedzených pravidiel vyhodnocuje aplikácie, ktoré sa buď spúšťajú v počítači (a chcú sa pripojiť k internetu/lokálnej sieti), alebo ktoré sa približujú k počítaču zvonku a snažia sa k nemu pripojiť. Pre každú z týchto aplikácií potom súhlas Firewall buď povolí, alebo zakáže komunikáciu na sieťových portoch. Ak je aplikácia neznáma (teda nemá žiadne zadané pravidlá Firewallu), súhlas Firewall sa vás predvolene spýta, či chcete blokovanie alebo povoliť tento pokus o komunikáciu.

Súhlas AVG Firewall nie je určená na ochranu serverových platforiem!

Odporúčanie: Vo všeobecnosti sa neodporúča používať viac ako jednu bránu firewall na tom istom počítači. Nainštalovaním viacerých brán firewall sa nezvýši úroveň zabezpečenia počítača. Vzniká však vyššia pravdepodobnosť, že medzi týmito dvomi aplikáciami nastane konflikt. Preto vám odporúčame, aby ste používali len jednu bránu firewall na počítači a vypli všetky ostatné, aby sa eliminovalo riziko vzniku konfliktu a súvisiacich problémov.



Dostupné režimy súhlasu Firewall

Súhlas Firewall vám umožňuje zdefinovať špecifické pravidlá zabezpečenia na základe toho, či sa váš počítač nachádza v doméne alebo ide o samostatný počítač alebo dokonca notebook. Každá z týchto možností si vyžaduje inú úroveň ochrany a jednotlivé úrovne patria do príslušných režimov. V krátkosti je režim súhlasu Firewall špecifickou konfiguráciou komponentu Firewall a môžete použiť niekedy takýchto vopred definovaných konfigurácií.

- **Automatický** – V tomto režime súhlas Firewall automaticky spracúva celú prevádzku v sieti. Z vašej strany nebudú požadované žiadne rozhodnutia. Súhlas Firewall umožní

pripojenie všetkých známych aplikácií a súčasne s tým sa vytvorí pre aplikáciu pravidlo, ktoré určí, či sa aplikácia môže v budúcnosti kedykoľvek pripojiť. Pre iné aplikácie sú nastavenia Firewall pod správania aplikácie rozhodné, či sa má pripojenie povoliť alebo zablokovávať. V takej situácii sa však pravidlo nevytvorí a aplikácia sa bude kontrolovať pri každom opätovnom pokuse o pripojenie. Automatický režim celkovo neruší a odporúča sa pre väčšinu používateľov.

- **Interaktívny** – Tento režim je praktický, ak si želáte kontrolovať všetky sieťové prenosy z a do vášho počítača. Súčasťou Firewall ich bude sledovať a upozorní vás na každý pokus o komunikáciu alebo prenos dát, čím vám umožní povoliť alebo zablokovávať daný pokus, ak to uznáte za vhodné. Odporúča sa len pokročilým používateľom.
- **Blokovať prístup na internet** – Internetové pripojenie bude úplne zablokované, nebudete mať prístup na internet a nikto zvonku nebude mať prístup do vášho počítača. Len pre zvláštne a krátkodobé použitie.
- **Vypnúť ochranu súčasti Firewall** – Vypnutím povolíte všetky sieťové prenosy z a do vášho počítača. Uvoľníte ho tak zraniteľným voči útokom hackerov. Voľbu tejto možnosti vždy starostlivo zvážte.

Všimnite si ešte špecifický automatický režim, ktorý je tiež súčasťou brány Firewall. Tento režim sa v tichosti aktivuje vtedy, ak sa súčasťou [Počítač](#) alebo [Identity Protection](#) vypnú a počítač bude preto zraniteľnejší. V takých prípadoch sú súčasťou Firewall automaticky povolené pripojenie iba známym a úplne bezpečným aplikáciám. Pri všetkých ostatných bude od vás vyžadované rozhodnutie. Cieľom je nahraďovať deaktivované súčasti ochrany a udržať počítač v bezpečí.


Ovládacie prvky dialógového okna


Dialógové okno obsahuje prehľad základných údajov o stave súčasti Firewall:


- **Režim súčasti Firewall** – Poskytuje informácie o aktuálne zvolenom režime súčasti Firewall. Tlačidlom **Zmeniť** vedľa uvedených údajov prepnete na rozhranie [nastavení súčasti Firewall](#), pokiaľ chcete zmeniť aktuálny režim na ďalší (*popis a odporúčanie týkajúce sa profilov brány Firewall nájdete v predchádzajúcom odseku*).
- **Zdieľanie súborov a tlačiarňí** – Obsahuje údaje o tom, či je aktuálne povolené zdieľanie súborov a tlačiarňí (*v oboch smeroch*). Zdieľanie súborov a tlačiarňí v podstate znamená zdieľanie akýchkoľvek súborov alebo priečinkov, ktoré ste označili v systéme Windows ako „Zdieľané“, spoločných diskových jednotiek, tlačiarňí, skenerov a všetkých podobných zariadení. Zdieľanie takýchto položiek je želané len v rámci sietí, ktoré môžu byť považované za bezpečné (*napríklad v domácnosti, v práci či v škole*). Keď ste však pripojení vo verejnej sieti (*ako napríklad Wi-Fi sieť na letisku alebo v internetovej kaviarni*), nemusíte si želať zdieľania.
- **Pripojené k** – Poskytuje údaje o názve siete, ku ktorej ste práve pripojení. V systéme Windows XP názov siete zodpovedá označeniu, ktoré ste predtým vybrali pri prvom pripojení k nej. V systéme Windows Vista a vyššie sa názov siete berie automaticky z centra sietí.


Toto dialógové okno pozostáva z nasledujúcich ovládacích prvkov:

Zmeniť – Týmto tlačidlom môžete zmeniť stav príslušného parametra. Podrobnosti o zmene parametrov nájdete v popise daného parametra v odseku vyššie.

 **Nastavenia** – Kliknutím na tlačidlo budete presmerovaní na rozhranie [Nastavenia súčasti Firewall](#), kde môžete upraviť celú konfiguráciu súčasti Firewall. Konfiguráciu by mali vykonať len skúsení používatelia.

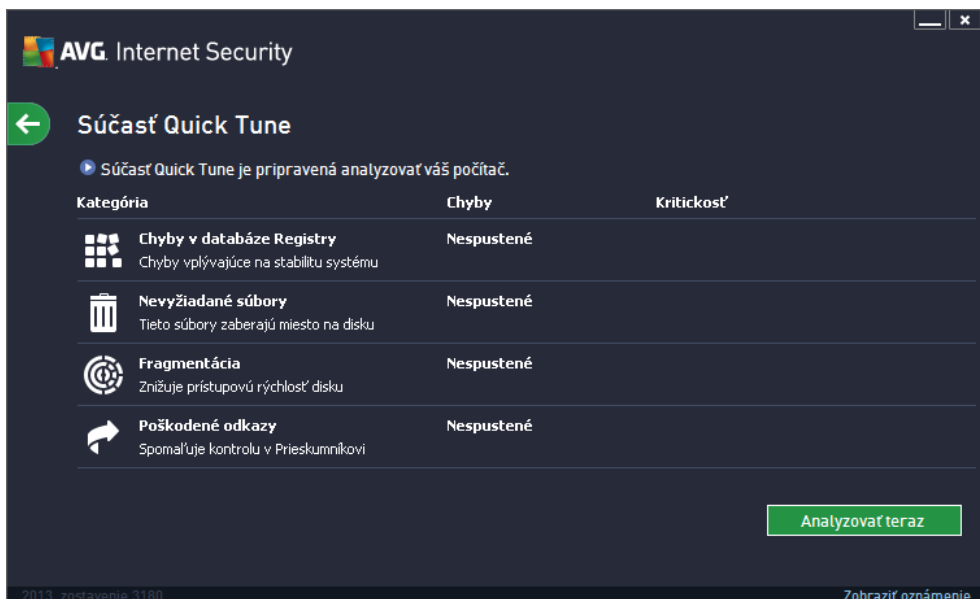
 **Obnovi konfiguráciu** – Stlačením tohto tlačidla sa prepíše používaná konfigurácia súčasti Firewall a obnoví sa predvolená konfigurácia na základe automatickej detekcie.

 **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.

6.6. Quick Tune

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

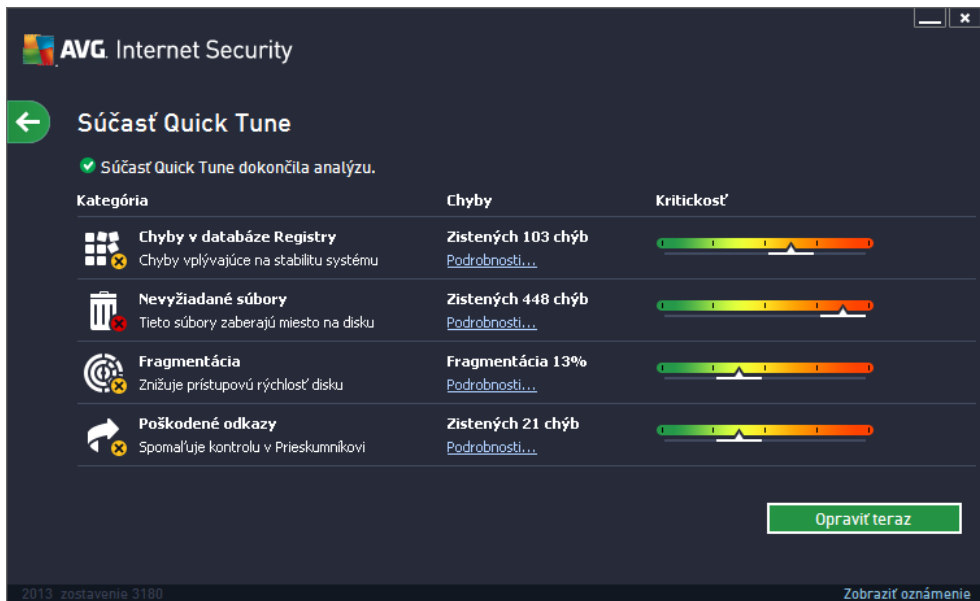


Umožňuje analyzovať a opraviť tieto oblasti: chyby v databáze Registry, nevyžiadané súbory, fragmentácia a poškodené odkazy:

- **Chyby v databáze Registry** informuje o porušení chýb v databáze Registry operačného systému Windows, ktoré môžu spomaliť váš počítač alebo spôsobovať zobrazenie chybových hlásení.
- **Nevyžiadané súbory** informuje o porušení súborov, ktoré zaberajú miesto na pevnom disku, a ktoré sa pravdepodobne môžu vymazať. Zvyčajne ide o mnohé typy dočasných súborov a súbory v Koši.
- **Fragmentácia** vypočíta podiel pevného disku, ktorý je fragmentovaný, t. j. používal sa dlhý čas a väčšina súborov je umiestnená na rôznych miestach fyzického disku.

- **Poškodené odkazy** vyhľadávajú odkazy, ktoré už nie sú funkčné, vedú na neexistujúce miesta atď.

Na spustenie analýzy po kliknutí a stlačení tlačidla **Analyzovať teraz**. Potom si budete môcť pozrieť priebeh analýzy a výsledky priamo v tabuľke:



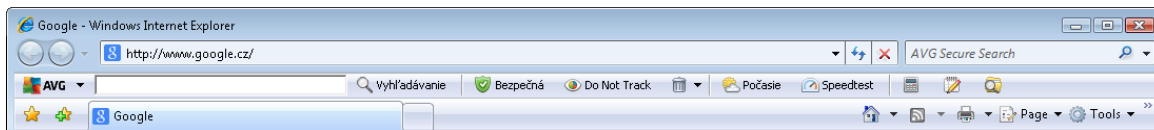
Prehľad výsledkov informuje o počte detegovaných systémových problémov (**Chyby**), ktoré sú klasifikované podľa príslušnej testovanej kategórie. Výsledky analýzy sa zobrazia aj v grafickej podobe na osi v stupni **Závažnosť**.

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).

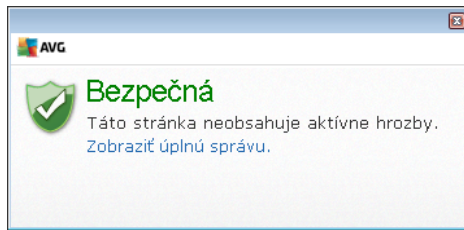
7. AVG Security Toolbar

AVG Security Toolbar je nástroj, ktorý úzko spolupracuje so sú as ou LinkScanner Surf-Shield a zabezpečuje maximálnu ochranu pri prezeraní internetu. V produkte **AVG Internet Security 2013** je inštalácia sú asti **AVG Security Toolbar** voliteľná. Po as [procesu inštalácie](#) sa môžete rozhodnúť, či chcete túto sú as nainštalovať. K sú asti **AVG Security Toolbar** máte prístup priamo v internetovom prehliadači. V sú asnosti 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 sú astí:

- **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**.
 - **Odnášalova sú as AVG Security Toolbar** – Otvorí sa webová stránka s podrobnosťami o postupe vypnutia sú asti **AVG Security Toolbar** pre každý z podporovaných webových prehliadačov.
 - **About...** – Otvorí sa nové okno s informáciami o verzii aktuálne nainštalovanej sú asti **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 otvára nové dialógové okno obsahujúce informácie o aktuálnej úrovni hrozby (**Aktuálne bezpečné**) internetovej stránky, na ktorej sa práve nachádzate. Tento krátky prehľad môžete rozbaľovať a zobrazí všetky podrobnosti o všetkých bezpečnostných problémoch týkajúcich sa internetovej stránky priamo v okne prehliadača (Zobrazí úplnú správu):



- **[Do Not Track](#)** – služba DNT vám pomáha identifikovať webové lokality, ktoré zbierajú údaje o vašich online aktivitách a umožňuje vám povoliť alebo nepovoliť ich zhromažďovanie. [Detaily >>](#)
- **Vymazať** – Tlačidlo „Odpadkový kôš“ ponúka rozbaľovaciu ponuku, v ktorej si môžete vybrať, či si želáte vymazať údaje o prezeraní stránok, preberaniach a on-line formulároch alebo chcete vymazať celú históriu vyhľadávania.
- **Počasie** – Toto tlačidlo otvorí nové dialógové okno s informáciami o počasí vo vašej oblasti a predpoveďou na najbližšie dva dni. Uvedené informácie sa pravidelne aktualizujú každé 3 hodiny až každých 6 hodín. V tomto okne môžete ručne zmeniť požadovanú oblasť a rozhodnúť sa, či chcete teplotu zobrazovať v stupňoch Celzia alebo Fahrenheita.



- **Facebook** – Pomocou týchto tlačidiel sa pripojíte k sociálnej sieti [Facebook](#) priamo z nástroja **AVG Security Toolbar**.
- **Speedtest** – Toto tlačidlo vás presmeruje na on-line aplikáciu, ktorá vám pomôže overiť kvalitu internetového pripojenia (*ping*) a rýchlosť preberania a nahrávania.
- Tlačidlá skratiek rýchleho prístupu k týmto aplikáciám: **Kalkulátka**, **Poznámkový blok**, **Prieskumník Windows**.


8. AVG Do Not Track

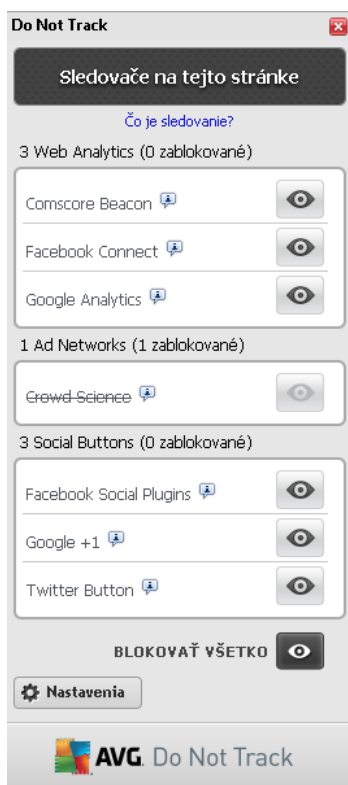
Aplikácia **AVG Do Not Track** pomáha identifikovať webové lokality, ktoré zhromažďujú údaje o vašej činnosti on-line. Funkcia **AVG Do Not Track**, ktorá je súčasťou panelu nástrojov [AVG Security Toolbar](#) zobrazuje webové lokality alebo inzerentov zhromažďujúcich údaje o vašej aktivite a umožňuje 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 súvisiacich 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 blokové): 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 blokové.
- **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.

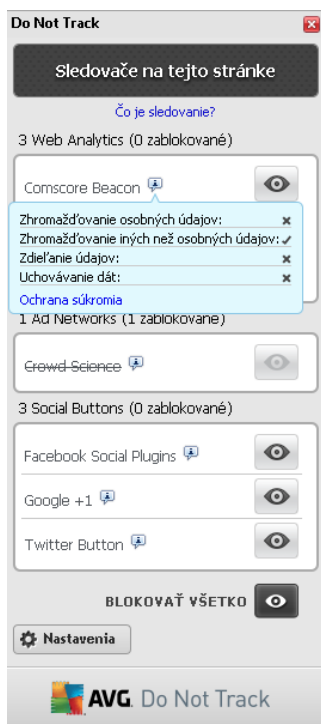
Poznámka: Podľa toho, ktoré služby sú spustené na pozadí internetovej stránky, sa niektoré z týchto uvedených prvkov nemusia v dialógovom okne aplikácie AVG Do Not Track zobraziť.

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 blokované. Môžete postupovať dvoma spôsobmi:

- **Blokovať všetky** – Kliknite na toto tlačidlo umiestnené v spodnej časti dialógového okna, ak si neželáte vôbec žiadne zhromažďovanie údajov. *(Pamätajte však, že tento krok môže narušiť funkcie príslušnej webovej stránky, na ktorej je služba spustená!)*
-  – Ak si neželáte blokovať všetky detegované systémy naraz, môžete jednotlivé 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 a 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, i budú blokované aj ostatné siete, alebo ich necháte povolené.** Stačí, keď kliknete na tlačidlo **Blokovať všetko** pod zoznamom. Alebo môžete kliknutím na tlačidlo **Predvolené** zrušiť všetky zmeny v nastaveniach a vrátiť sa k pôvodnému nastaveniu.

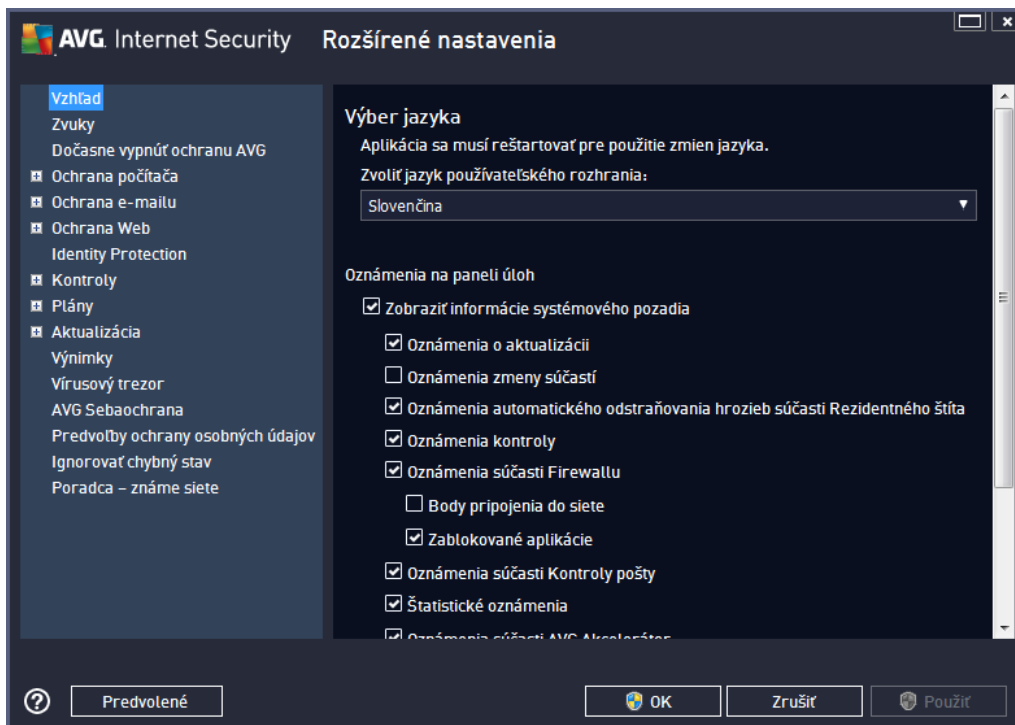
- **Upozorni webové lokality...** – v tejto časti môžete prepnúť možnosť **Upozorni webové lokality, že nechcem byť sledovaný (predvolene zapnuté)**. Túto možnosť nechajte zaškrtnutú, aby ste potvrdili, že chcete, aby aplikácia **Do Not Track** informovala poskytovateľov služieb zhromažďujúcich údaje,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

9. Rozšírené nastavenia programu AVG

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

9.1. Vzhľad

Prvá položka v navigačnej štruktúre, **Vzhľad**, sa týka všeobecných nastavení [používateľského rozhrania](#) produktu **AVG Internet Security 2013** a niektorých základných možností správy aplikácie:

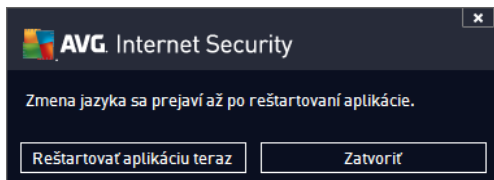


Výber jazyka

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

- V rozbaľovacej ponuke vyberte požadovaný jazyk aplikácie.
- Potvrďte výber stlačením tlačidla **Použiť** (v pravom hornom rohu dialógového okna).
- Potvrďte stlačením tlačidla **OK**.

- Zobrazí sa nové dialógové okno s informáciami o zmene jazyka aplikácie a potrebe reštartovať **AVG Internet Security 2013**
- Stlačením tlačidla **Reštartovať aplikáciu** potvrdíte súhlas s reštartovaním programu. Po každej chvíli, kým sa zmena jazyka prejaví:

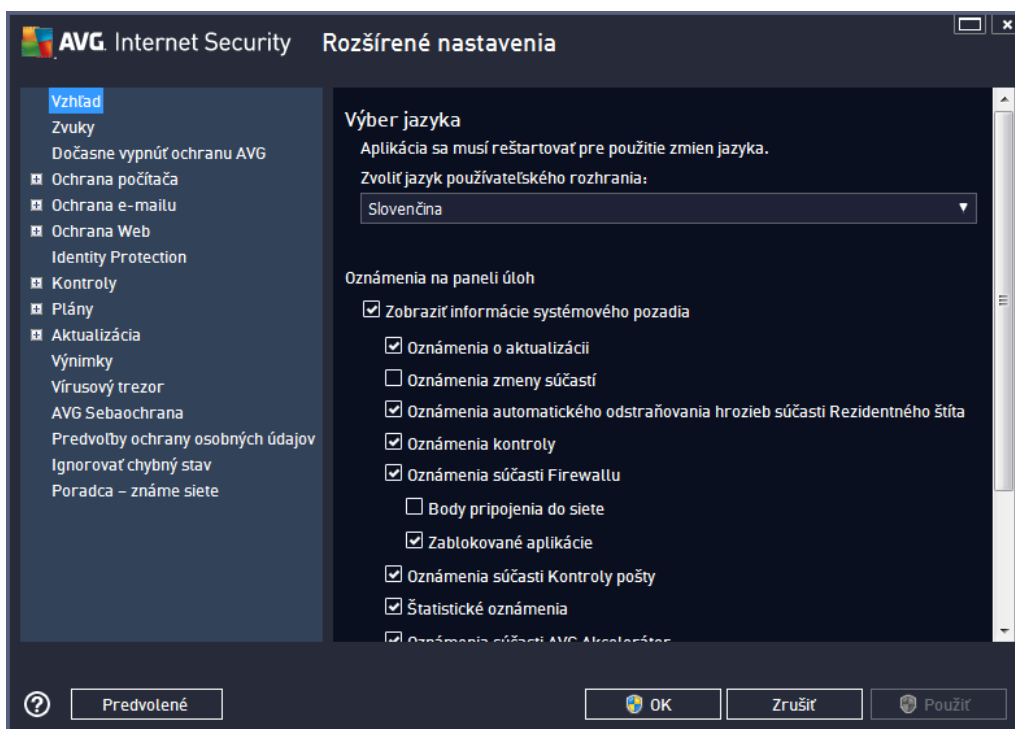


Oznámenia v paneli úloh

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

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

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



- **Oznámenia o aktualizáciách** (predvolene zapnuté) – rozhodnite sa, či sa majú zobrazovať informácie týkajúce sa spustenia aktualizácie **AVG Internet Security 2013**, postupu a dokončenia
- **Oznámenia o zmene stavu súčastí** (predvolene vypnuté) – rozhodnite sa, či sa majú zobrazovať informácie týkajúce sa činnosti alebo nečinnosti súčastí, prípadne či sa majú zobrazovať informácie o možnom probléme. Táto možnosť má pri oznámení chybného stavu súčastí informáciu funkciu [ikony v paneli úloh](#), ktorá informuje o probléme týkajúcom sa súčastí produktu **AVG Internet Security 2013**.
- **Oznámenia automatického odstraňovania hrozieb Rezidentným štítom** (predvolene zapnuté) – rozhodnite sa, či sa majú alebo nemajú zobrazovať informácie súvisiace s procesmi ukladania, kopírovania a otvárania súborov (táto funkcia sa dá nastaviť, len keď je v súčasti Rezidentný štít zapnutá možnosť *Liečiť automaticky*)
- **Oznámenia o kontrole** (predvolene zapnuté) – rozhodnite sa, či sa majú zobrazovať informácie pri automatickom spustení plánu kontroly, jeho priebehu a výsledkoch
- **Oznámenia súvisiace so súčastou Firewall** (predvolene zapnuté) – rozhodnite sa, či sa majú zobrazovať informácie súvisiace so stavom a procesmi súčasti Firewall, ako sú upozornenia o zapnutí alebo vypnutí súčasti, prípadne blokovanie prenosov atď. Na tomto mieste môžete určiť dve ďalšie možnosti (*podrobnejšie vysvetlenie každej z nich nájdete v kapitole [Firewall](#) v tomto dokumente*):
 - **Body pripojenia do siete** (predvolene vypnuté) – pri pripájaní do siete vás súčasti Firewall informuje o tom, či ide o známu sieť, a aké budú nastavenia zdieľania súborov a tlačiarň.

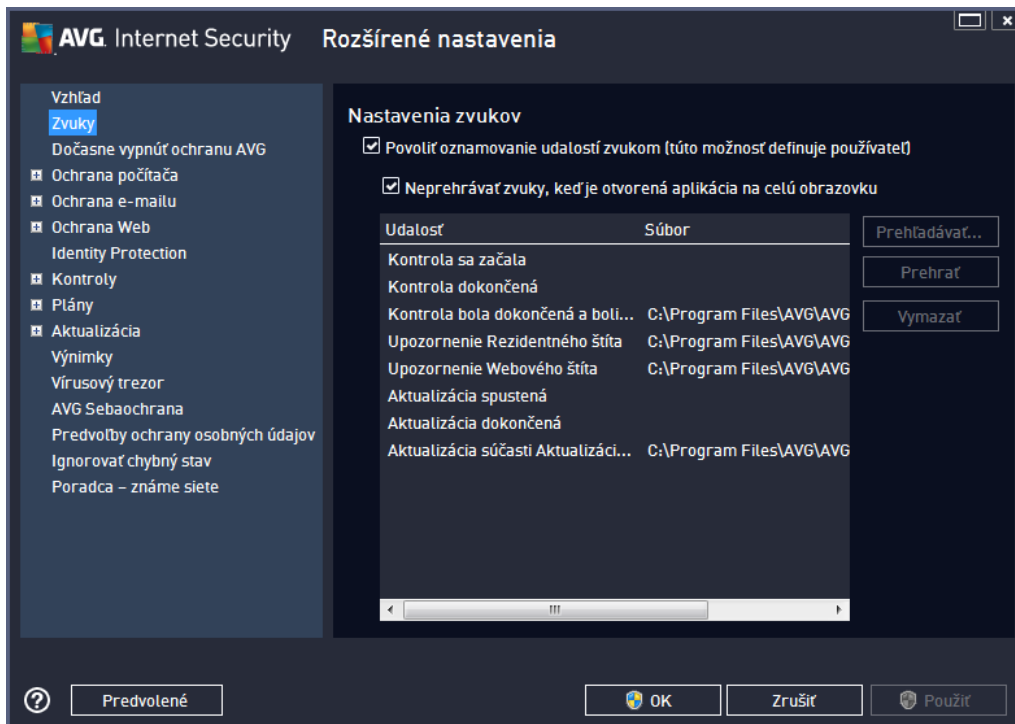
- **Blokované aplikácie** (predvolene zapnuté) – ak sa do siete pokúša pripoji neznáma alebo podozrivá aplikácia, sú as Firewall zablokuje tento pokus a zobrazí oznámenie. To je užito né, ak chcete by informovaný, preto odporú ame necha túto funkciu vždy zapnutú.
- **Oznámenia súvisiace so sú as ou Kontrola pošty** (predvolene zapnuté) – rozhodnite sa, i sa majú zobrazova informácie po každej kontrole prichádzajúcich a odchádzajúcich e-mailových správ
- **Štatistické oznámenia** (predvolene zapnuté) – nechajte polí ko za iarknuté, ak sa majú zobrazova pravidelné štatistické preh adové oznámenia na paneli úloh
- **Oznámenia sú asti AVG Akcelerátor** (predvolene zapnuté) – rozhodnite sa, i sa majú zobrazova informácie týkajúce sa inností sú asti **AVG Akcelerátor**. **Služba AVG Akcelerátor** umož ũje stabilnejšie prehrávanie on-line videa a u ah ũje alšie preberania.
- **Oznámenia o skrátení zavádzacieho asu** (predvolene vypnuté) – rozhodnite sa, i chcete by informovaní o skrátení zavádzacieho asu systému.
- **Oznámenia sú asti AVG Advisor** (predvolene zapnuté) – rozhodnite sa, i sa informácie o aktivite sú asti **AVG Advisor** majú zobrazova v paneli úloh

Režim hrania

Táto funkcia programu AVG sa používa v súvislosti s aplikáciami spustenými na celú obrazovku, ktorých spustenie by sa mohlo naruši (*aplikácia by sa minimalizovala alebo by sa porušila grafika*) zobrazením informa nej bubliny programu AVG (*ktorá sa zobrazí napr. pri spustení plánu kontroly*). Ak sa chcete vyhnú podobným situáciám, nechajte za iarkavacie polí ko možnosti **Povolí režim hrania, ak beží aplikácia v režime na celú obrazovku** ozna ené (predvolené nastavenie).

9.2. Zvuky

Dialógové okno **Zvuky** sa používa na zapnutie zvukových upozornení informujúcich o konkrétnych innoostiach programu **AVG Internet Security 2013**:



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

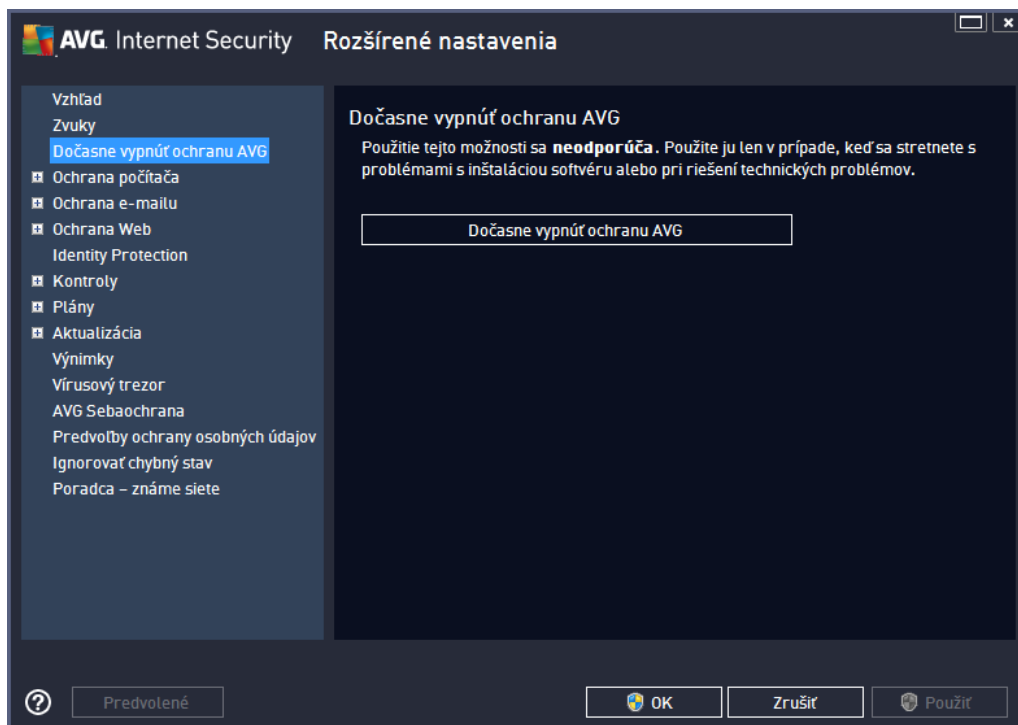
Ovládacie tlačidlá

- **Prehľadávať** – Po označení príslušnej udalosti zo zoznamu pomocou tlačidla **Prehľadávať** nájdete na disku požadovaný zvukový súbor, ktorý chcete innoosti priradiť. (V súčasnosti sú podporované iba zvukové formáty *.wav!)
- **Prehrať** – Ak si chcete vypočuť zvolený zvuk, zvýraznite udalosť v zozname a stlačte tlačidlo **Prehrať**.
- **Vymazať** – Na odstránenie zvuku prideleného konkrétnej udalosti použite tlačidlo **Vymazať**.

9.3. Dočasne vypnúť ochranu AVG

Dialógové okno **Do asne vypnúť ochranu AVG** umožňuje naraz vypnúť celú ochranu zabezpečenú programom **AVG Internet Security 2013**.

Nepoužívajte túto možnosť, ak to nie je naozaj nevyhnutné!

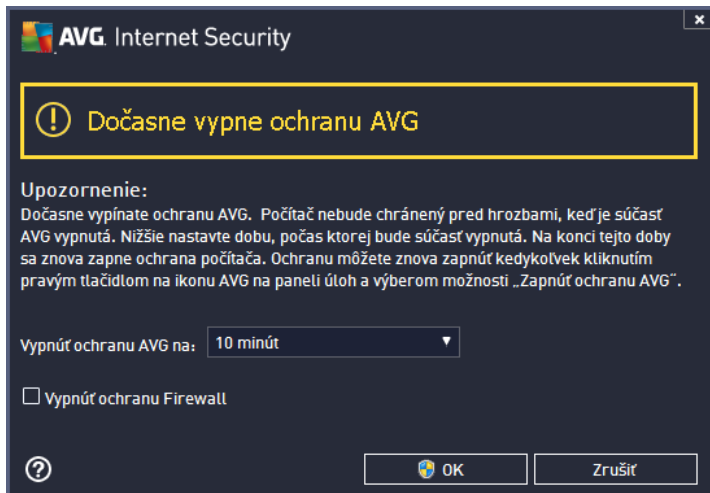


Vo väčšine prípadov **nie je potrebné** vypínať program **AVG Internet Security 2013** pred inštaláciou nového softvéru alebo ovládačov, a to ani v prípade, ak inštalovaný program alebo sprievodca inštaláciou softvéru odporúča, aby sa najskôr zatvorili otvorené programy a aplikácie z dôvodu možného nežiaduceho prerušenia procesu inštalácie. Ak sa počas inštalácie vyskytne problém, skúste najprv vypnúť rezidentnú ochranu (*Povolí súčasne Rezidentný štít*). Ak musíte dočasne vypnúť ochranu **AVG Internet Security 2013**, 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 vypnúť ochranu AVG

Označte za iarkavacie políčko **Do asne vypnúť ochranu AVG** a potvrdte voľbu stlačením tlačidla **Použiť**. V novootvorenom dialógovom okne **Do asne vypnúť ochranu AVG** zadajte čas, na aký chcete vypnúť aplikáciu **AVG Internet Security 2013**. V predvolenom nastavení sa ochrana vypne na 10 minút, čo by malo stačiť na dokončenie bežných úloh, ako je inštalácia nového softvéru a pod. Môžete sa rozhodnúť pre dlhší čas, no neodporúčame to, pokiaľ to nie je absolútne nutné. Potom sa všetky vypnuté súčasti automaticky znovu aktivujú. Nanajvýš môžete vypnúť ochranu AVG až do najbližšieho reštartovania počítača. Samostatnú možnosť vypnutia súčasti **Firewall** nájdete v dialógovom okne **Do asne vypnúť ochranu AVG**. Ak tak chcete urobiť, označte políčko **Vypnúť**

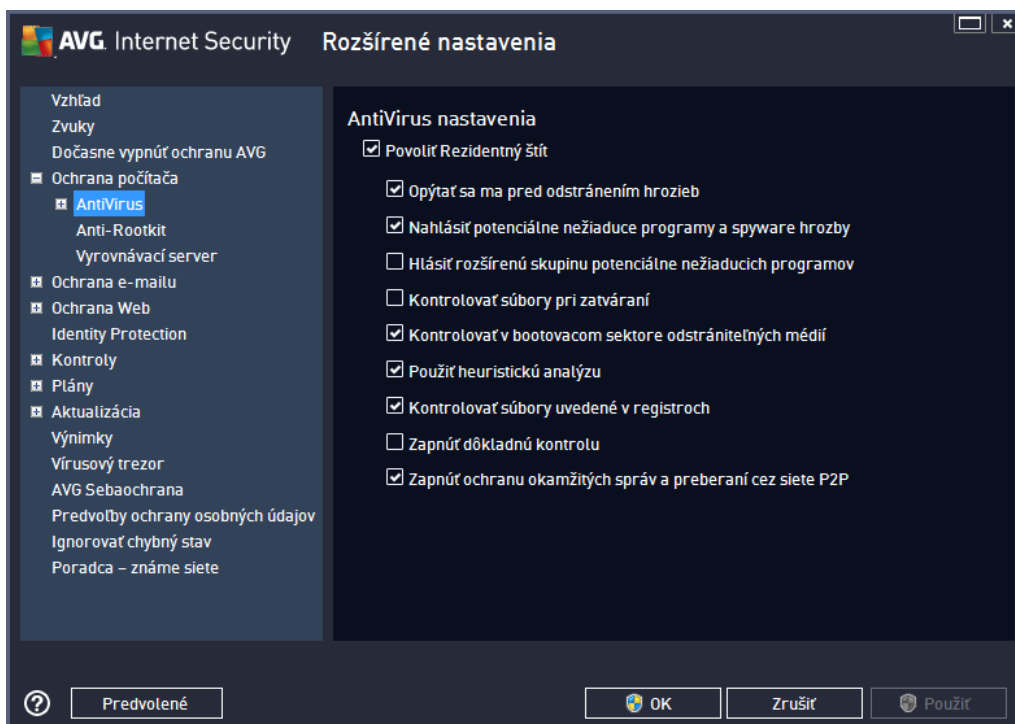
ochranu Firewall.



9.4. Ochrana počítača

9.4.1. AntiVirus

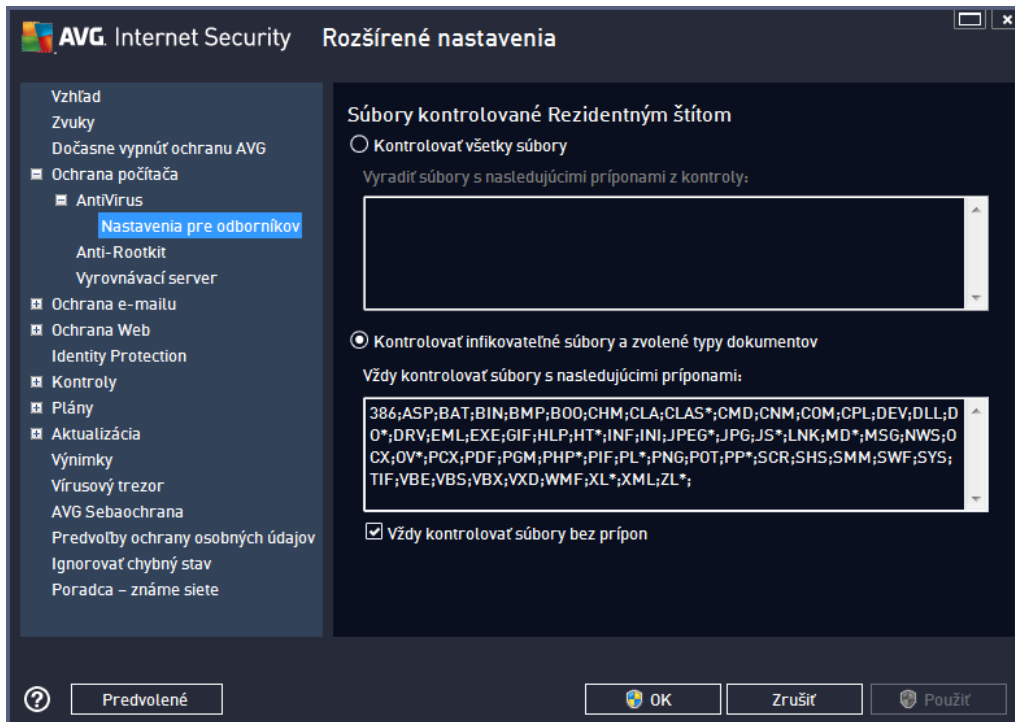
AntiVirus spolu s **Rezidentným štítom** nepretržite chránia váš počítač pred všetkými známymi druhmi vírusov, spyware a malware (vrátane takzvaného spiacneho alebo neaktívneho malware, o je malware, ktorý bol prevzatý, ale nebol ešte aktivovaný).



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

- **Opýta 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 Internet Security 2013** bude automaticky liečiť infekcie, a ak to nebude možné, bude objekt premiestnený do [Vírusového trezora](#).
- **Nahlási potenciálne nežiaduce programy a spyware hrozby** (štandardne zapnuté) – Za iarknite 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.
- **Hlásí 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.
- **Kontrolova 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** (štandardne zapnuté)
- **Použije 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 umožňuje, 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 iarknutím tohto políčka aktivovať algoritmus najdôkladnejšej kontroly, ktorý skontroluje všetky možné nebezpečné objekty do hĺbky. Upozorujeme však, že tento spôsob je náročný na čas.
- **Zapnú ochranu okamžitých správ a preberaní cez sieť P2P** (štandardne zapnuté) – Za iarknite toto políčko, 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 Rezidentným štítom** môžete nastaviť, ktoré súbory sa budú kontrolovať (podľa a konkrétnych prípon):

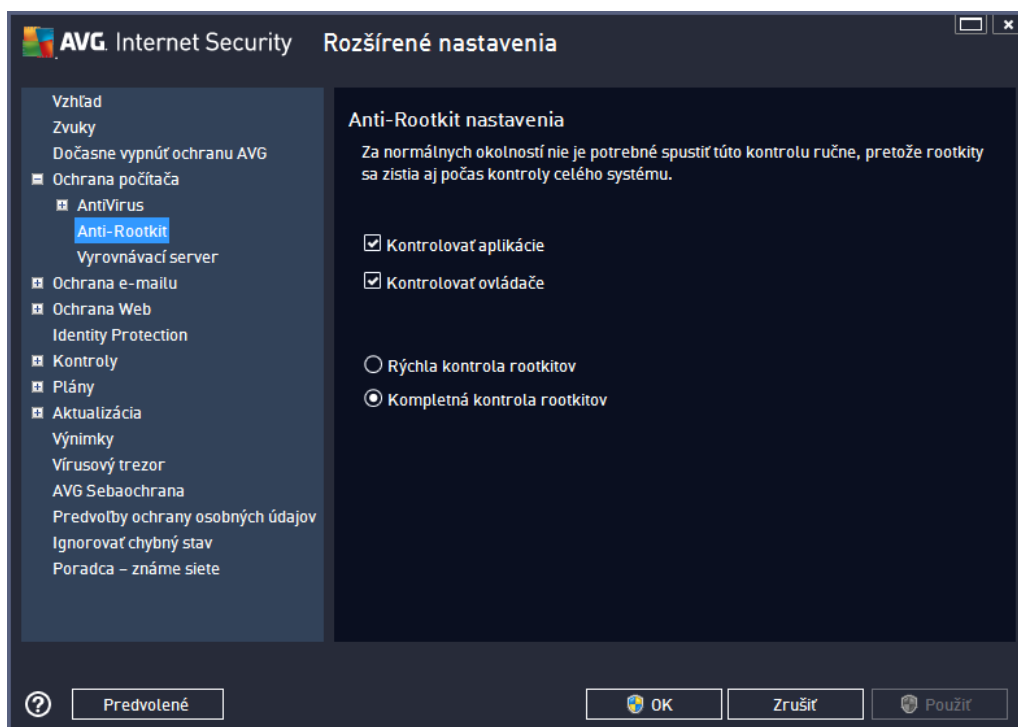


Označte príslušné začiarkavacie polia podľa toho, či chcete použiť možnosť **Kontrolovať všetky súbory** alebo **Kontrolovať infikovateľné súbory a zvolené typy dokumentov**. Ak chcete urýchliť kontrolu a súčasne zabezpečiť maximálnu úroveň ochrany, odporúčame zachovať predvolené nastavenia. Takto sa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

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

9.4.2. Anti-Rootkit

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

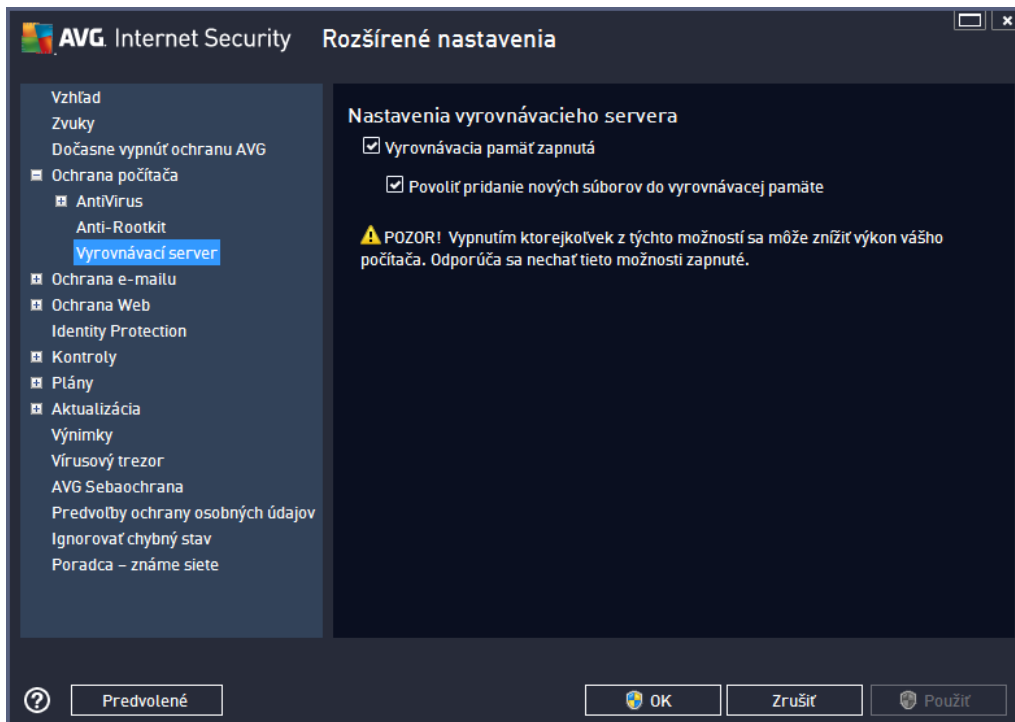


Možnosti **Kontrolova aplikácie** a **Kontrolova ovládače** vám umožňujú podrobne zadať, čo by malo byť súčasťou kontroly Anti-Rootkit. Tieto nastavenia sú určené pre skúsených používateľov; odporúčame vám, aby ste nechali všetky možnosti zapnuté. Môžete tiež vybrať režim kontroly rootkitov:

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

9.4.3. Vyrovňavací server

Dialógové okno **Nastavenie vyrovňavacieho servera** sa týka procesu vyrovňavacieho servera určeného na zrýchlenie všetkých typov kontrol aplikácie **AVG Internet Security 2013**:



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

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

- **Vyrovňavacia pamäť zapnutá (štandardne zapnuté):** Zrušením označenia tohto políčka sa vypne **vyrovňavací server** a vyprázdni sa vyrovňavacia pamäť. Upozorujeme, že týmto sa môže spomaliť kontrola a zníži celkový výkon počítača, pretože každý jeden používaný súbor sa najskôr skontroluje z hľadiska prítomnosti vírusov a spywaru.
- **Povoliť prídanie nových súborov do vyrovňavacej pamäte (štandardne zapnuté):** Zrušením označenia tohto políčka sa vypne pridávanie ďalších súborov do vyrovňavacej pamäte. Všetky súbory vo vyrovňavacej pamäti sa zachovávajú a budú sa používať do úplného vypnutia funkcie vyrovňavacej pamäte, resp. do ďalšieho aktualizovania vírusovej databázy.

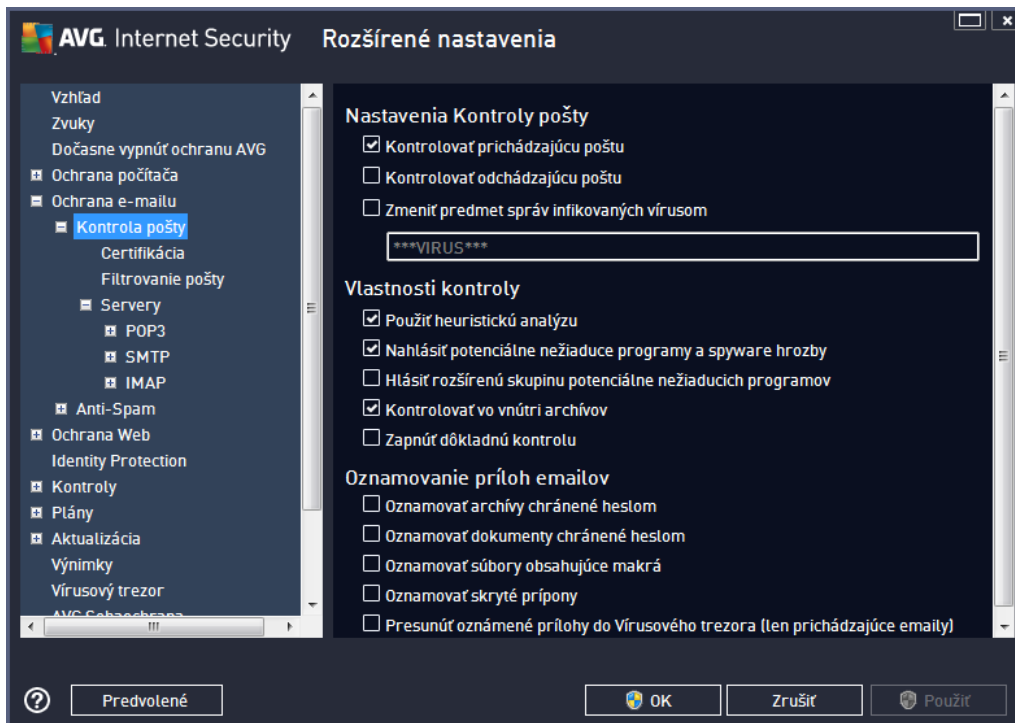
Ak nemáte oprávnený dôvod na vypnutie vyrovňavacieho servera, dôrazne odporúčame zachovať predvolené nastavenia a nechať obe možnosti zapnuté. Inak môžete zaznamenať výrazné spomalenie rýchlosti a výkonu systému.

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.
- **Kontrolovať vo vnútri archívov (predvolene zapnuté)** – začiarknite toto políčko, ak sa má prehľadávať 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.

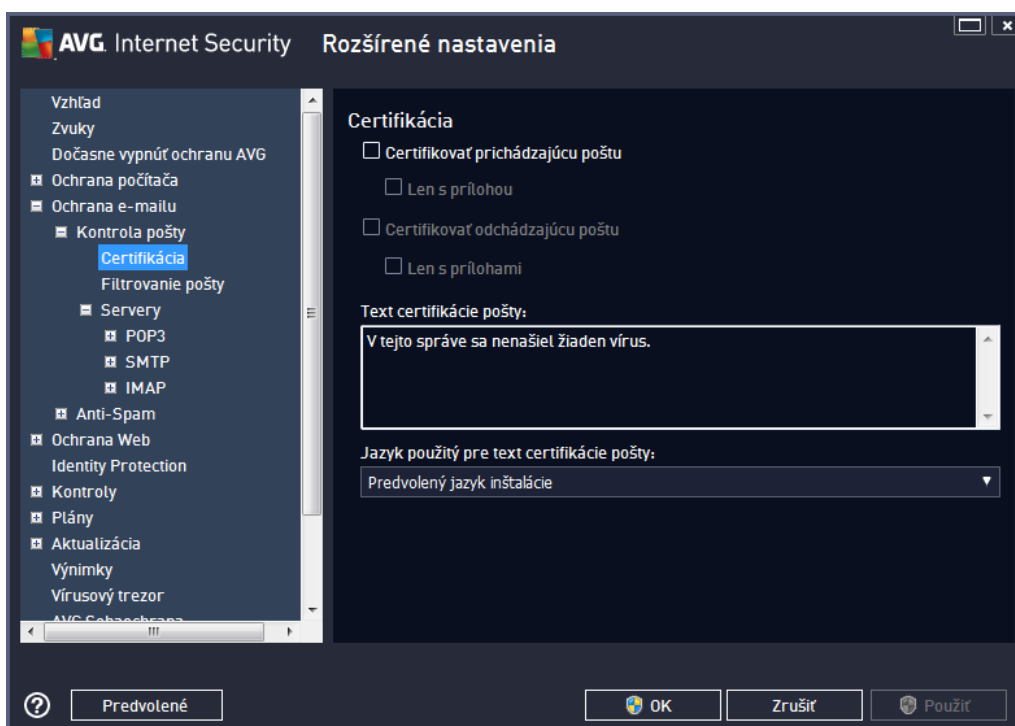
Oznamovanie príloh e-mailov

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](#):

- **Oznamovať archívy chránené heslom** – Archívované súbory (ZIP, RAR atď.), ktoré sú chránené heslom, sa nedajú skontrolovať z hľadiska prítomnosti vírusov. Začiarknite toto políčko, ak sa majú oznamovať tieto archívy ako potenciálne nebezpečné.
- **Oznamovať dokumenty chránené heslom** – Dokumenty chránené heslom sa nedajú skontrolovať na prítomnosť vírusov; začiarknite toto políčko, ak sa majú oznamovať tieto dokumenty ako potenciálne nebezpečné.
- **Oznamovať súbory obsahujúce makrá** – makro je vopred definovaný sled krokov, ktoré zjednodušujú konkrétne úlohy používateľovi (makrá sa bežne používajú v programe MS Word). Makro ako také môže obsahovať potenciálne nebezpečné inštrukcie, a preto je vhodné začiarknuť toto políčko, aby sa súbory s makrami oznamovali ako podozrivé.
- **Oznamovať skryté prípony** – Skrytá prípona môže spôsobiť, že sa bude podozrivý spustiteľný súbor „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

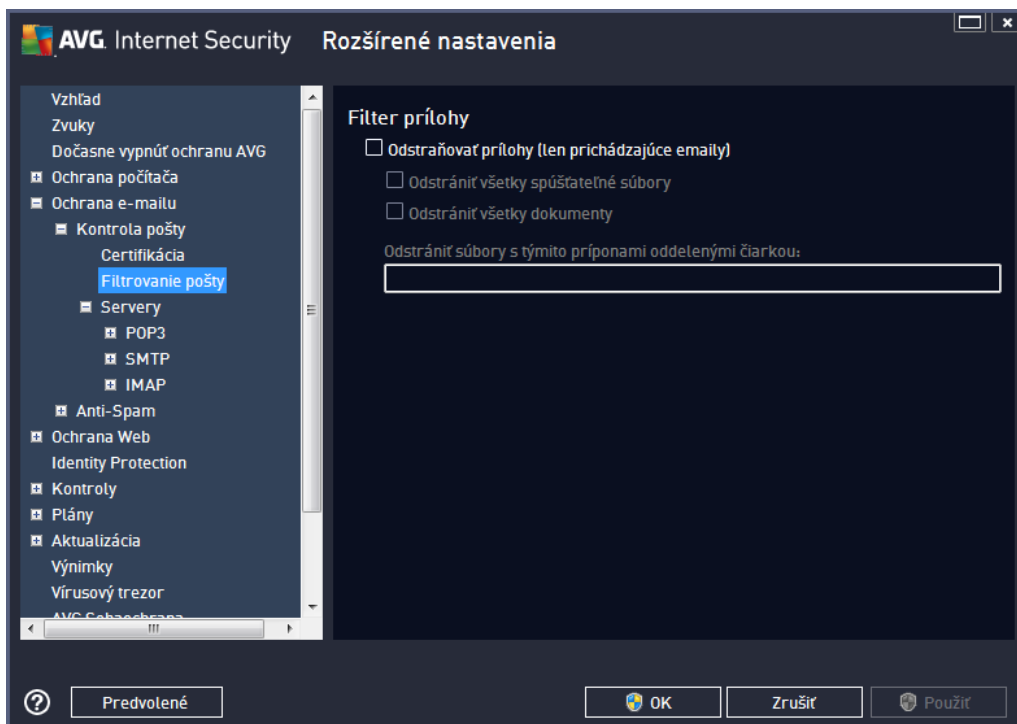
informovaní e-mailom o archívoch chránených heslom, dokumentoch chránených heslom, súboroch s makrami alebo súboroch so skrytou príponou, ktoré boli detegované ako príloha kontrolovanej e-mailovej správy. Ak sa má táto správa zobrazí po as kontroly, potom nastavte, i sa má detegovaný infikovaný objekt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

V dialógovom okne **Certifikácia** môžete ozna i konkrétne za iarkavacie polí ka a ur i, i chcete certifikova prichádzajúcu poštu (**Certifikova prichádzajúcu poštu**) alebo odchádzajúcu poшту (**Certifikova odchádzajúcu poшту**). Pri každej možnosti môžete alej ur i parameter **Len s prílohami**. Vtedy sa certifikácia bude týka 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 rozšíri alebo zmeni : do po a **Text e-mailovej certifikácie** napíšte požadovaný text certifikácie. V asti **Jazyk použitý pre text certifikácie pošty** môžete alej definova , v akom jazyku sa má automaticky vytváraná as certifikácie (*V tejto správe sa nenašiel žiadny vírus*) zobrazí .

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



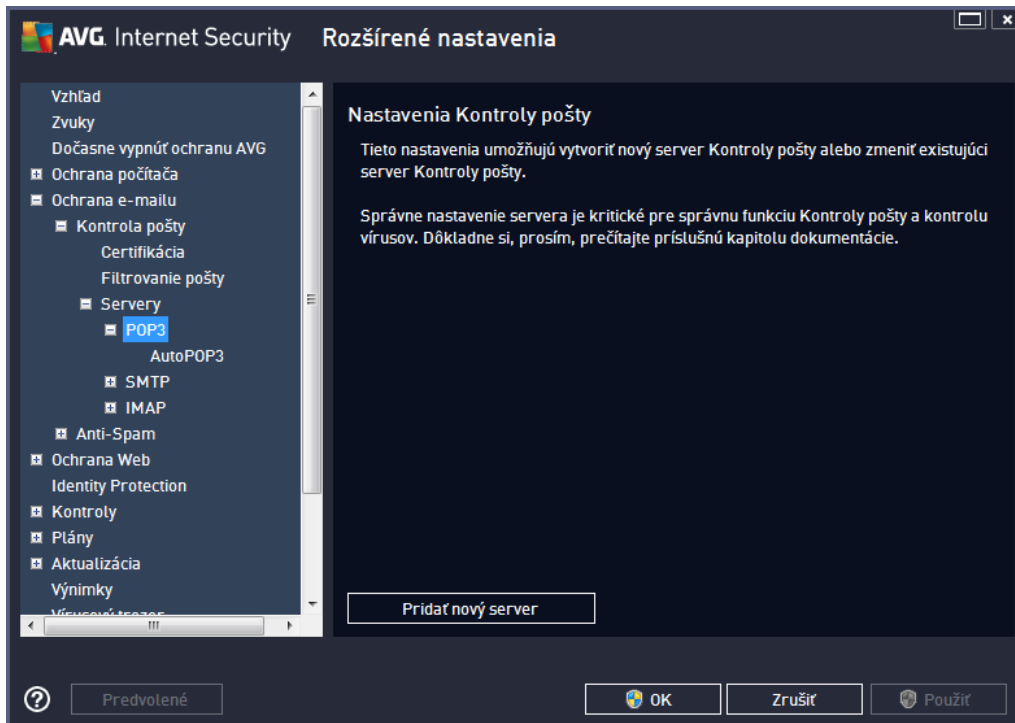
Dialógové okno **Filter príloh** umožňuje nastaviť parametre pre prehadzovanie príloh e-mailových správ. Štandardne je možnosť **Odstráni prílohy** vypnutá. Ak sa rozhodnete funkciu aktívovať, všetky prílohy e-mailových správ detegované ako infekcie alebo potenciálne nebezpečné programy sa automaticky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

- **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.

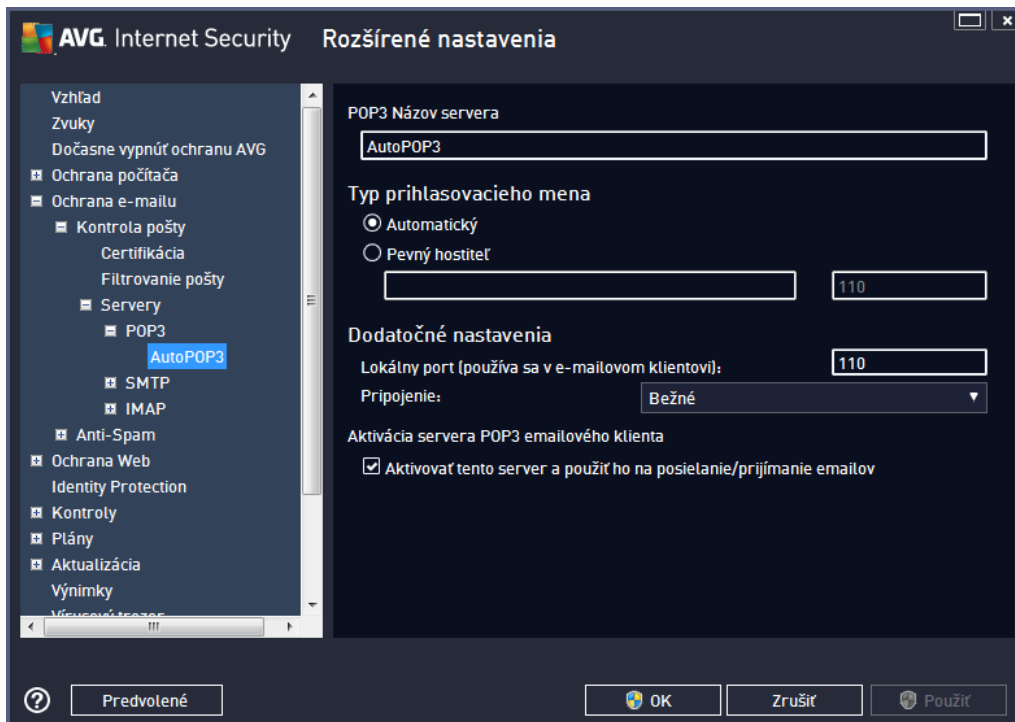
V nastavení **Servery** môžete upraviť parametre serverov sú v nastavení [Kontrola pošty](#):

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

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



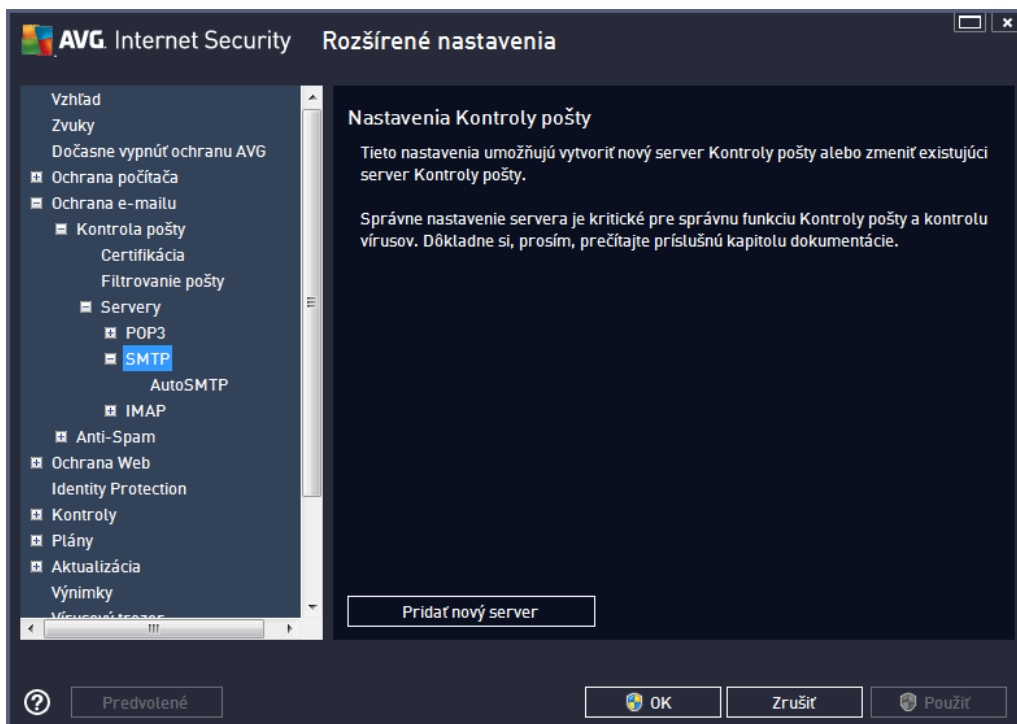
Toto dialógové okno umožní nastaviť pre súčasnú [Kontrolu pošty](#) nový server pomocou protokolu POP3 pre prichádzajúcu poštu:



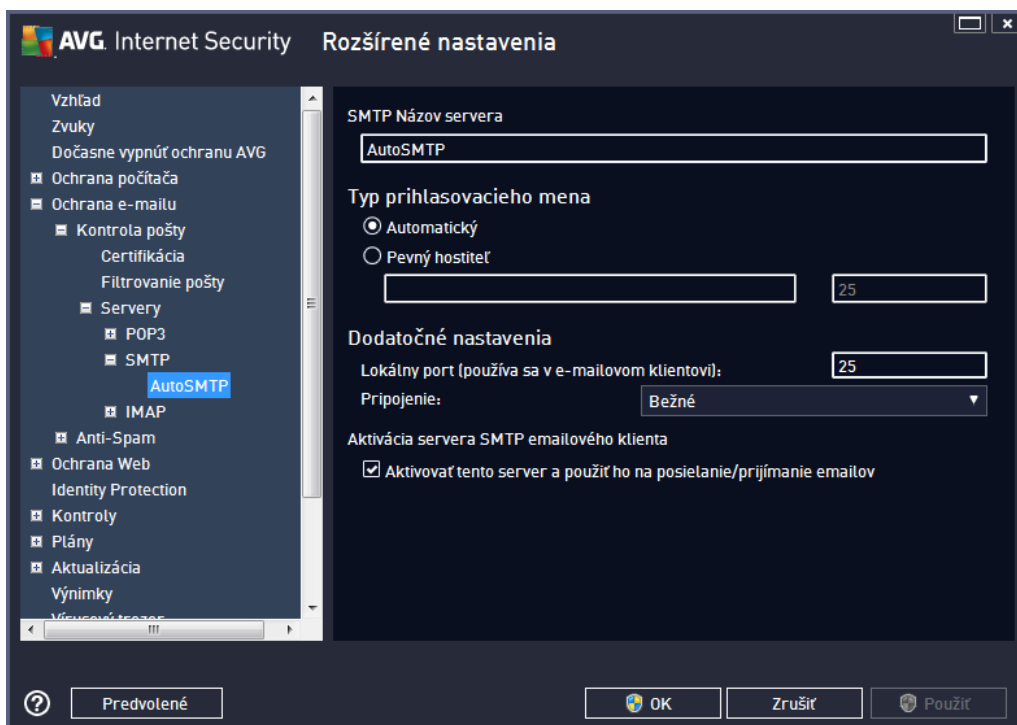
- **Názov servera POP3** – do tohto poľa zadajte názov novopridaných serverov (na pridanie

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

- **Typ prihlasovacieho mena** – Určuje spôsob stanovenia poštového servera pre prichádzajúcu poštu:
 - **Automaticky** –
 - **Pevný hosť** – V tomto prípade program vždy použije server, ktorý je tu uvedený. Zadať 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 použítie dvojbodku ako oddeľovací znak (napríklad *pop.acme.com:8200*). Štandardný port pre komunikáciu POP3 je 110.
- **Ďalšie nastavenia** – používa sa na definovanie podrobnejších parametrov:
 - **Lokálny port** – určuje port, na ktorom sa 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.
- **Aktivovanie servera POP3 v poštovej aplikácii** – za kliknutím alebo zrušením kliknutia tejto položky sa aktivuje resp. deaktivuje uvedený server POP3



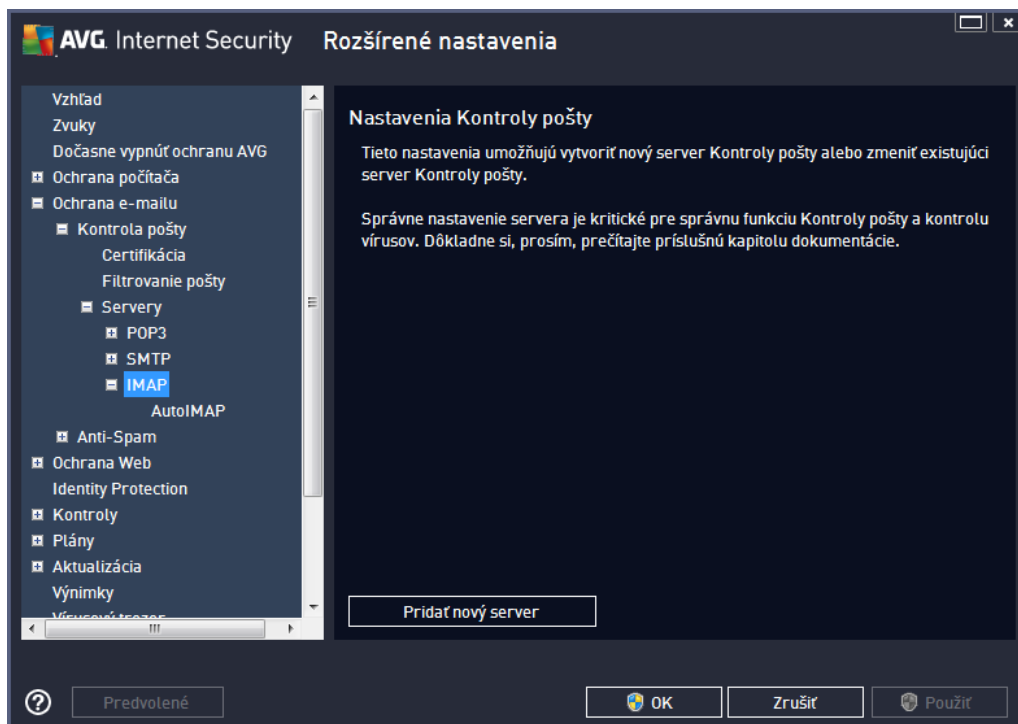
Toto dialógové okno umožní nastaviť pre súčasnú [Kontrolu pošty](#) nový server pomocou protokolu SMTP pre odchádzajúcu poštu:



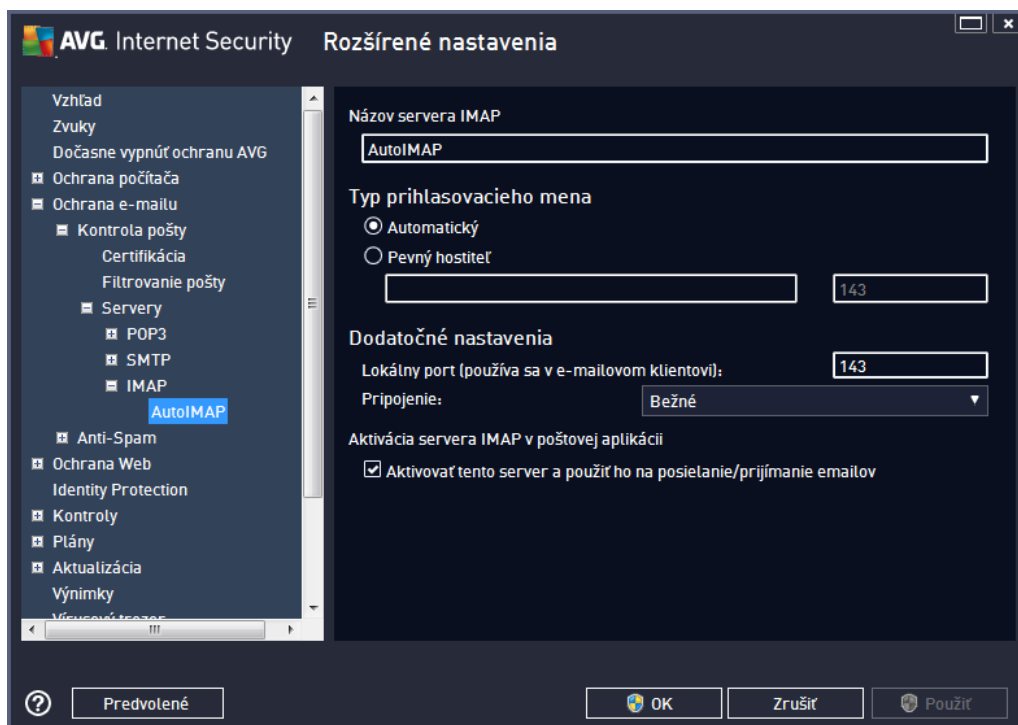
- **Názov servera SMTP** – do tohto poľa zadajte názov novopridaných serverov (na prídanie

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

- **Typ prihlásenia** – určuje spôsob zistenia poštového servera, ktorý sa používa pre prichádzajúcu poštu:
 - **Automaticky** – prihlásenie sa 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.
- **Ďalšie nastavenia** – používa sa na definovanie podrobnejších parametrov:
 - **Lokálny port** – určuje port, na ktorom sa odohráva 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.
- **Aktivovanie 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:

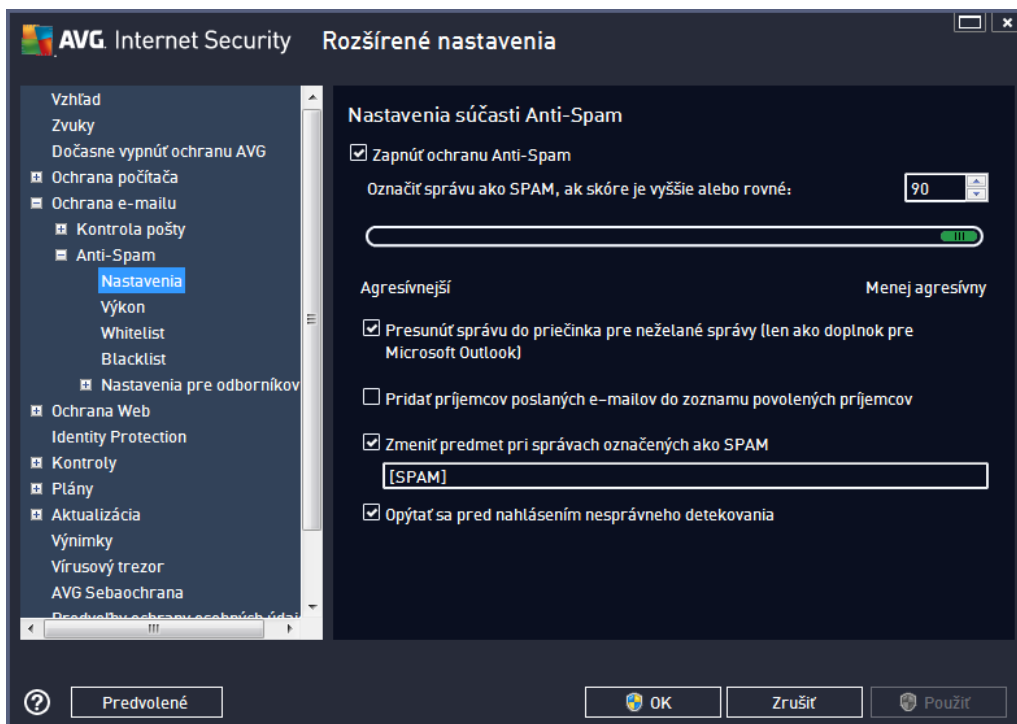


- **Názov servera IMAP** – do tohto poľa zadajte názov novopridaných serverov (na pridanie

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

- **Typ prihlásenia** – určuje spôsob zistenia poštového servera, ktorý sa používa pre prichádzajúcu poštu:
 - **Automaticky** – prihlásenie sa 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 oddeľovací znak (napríklad *smtp.acme.com:8200*). Štandardný port pre komunikáciu IMAP je 143.
- **Ďalšie nastavenia** – používa sa na definovanie podrobnejších parametrov:
 - **Lokálny port** – určuje port, na ktorom sa 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.
- **Aktivovanie servera IMAP v poštovej aplikácii** – začiarknutím alebo zrušením začiarknutia tohto políčka sa aktivuje, resp. deaktivuje uvedený server IMAP

9.5.2. Anti-Spam



V dialógovom okne **Nastavenia sú asti Anti-Spam** môžete za iarknutím alebo zrušením za iarknutia polí ka **Zapnú ochranu Anti-Spam** zapnú , resp. vypnú kontrolu e-mailovej komunikácie sú as ou Anti-Spam. Táto možnos je štandardne zapnutá a odporú ame vám, aby ste toto nastavenie nikdy nemenili, ak na to nemáte skuto ný dôvod.

alej môžete nastavi viac alebo menej agresívne hodnotenie skóre. Filter sú asti **Anti-Spam** pridelí každej správe skóre (*t. j. v akej miere sa obsah správy podobá SPAMU*) na základe nieko kých dynamických metód kontroly. Hodnotu funkcie **Ozna i správu ako spam, ke je skóre vyššie ako** môžete nastavi bu zadaním hodnoty, alebo posunutím posúva a smerom do ava alebo doprava (*nastavené hodnoty môžu by v rozsahu 50 – 90*).

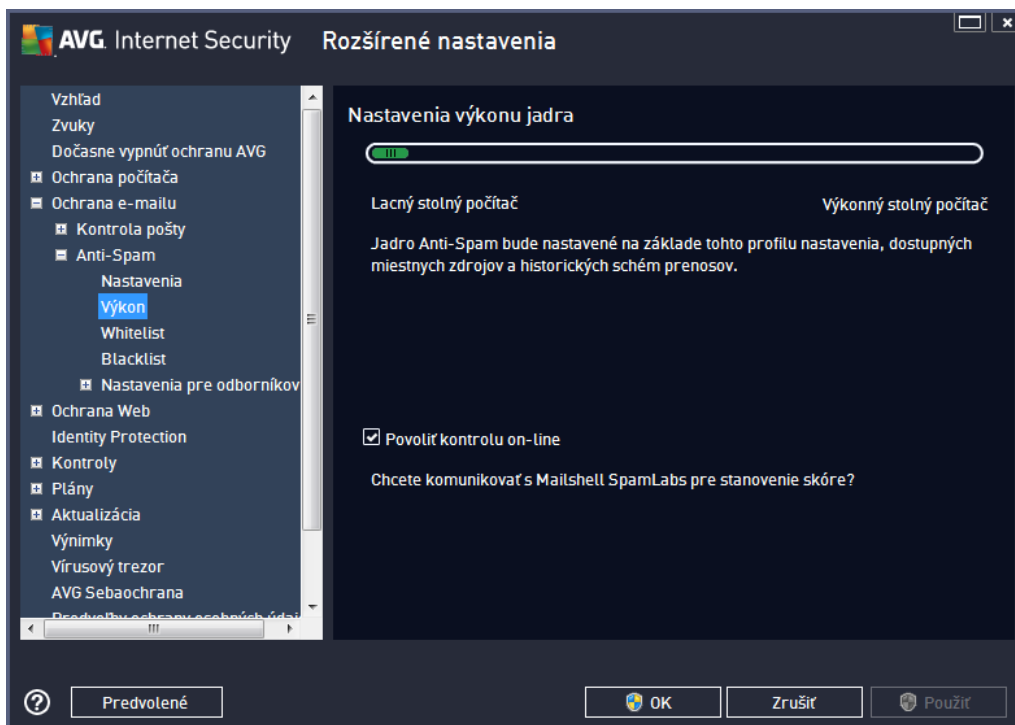
Odporú ame vám, aby ste nastavili prahovú hodnotu v pásme 50 – 90, prípade ak máte naozaj pochybnosti oh adne nastavenia, potom nastavte hodnotu 90. Toto je základný preh ad prahovej hodnoty skóre:

- **Hodnota 80 – 90** – e-mailové správy, ktoré sú s ve kou pravdepodobnos ou spam, sa budú filtrova . Niektoré správy, ktoré nie sú spam, sa môžu filtrova nesprávne.
- **Hodnota 60 – 79** – Považuje sa za celkom agresívnu konfiguráciu. E-mailové správy, ktoré sú možnými spamovými správami, budú filtrované a správy, ktoré nie sú spamové, budú pravdepodobne tiež zachytené
- **Hodnota 50 – 59** – ve mi agresívne nastavenie. E-mailové správy, ktoré nie sú spam, sa pravdepodobne zachytia ako spamové správy. Neodporú ame vám používa toto nastavenie na normálne ú ely.

V dialógovom okne **Nastavenia sú asti Anti-Spam** môžete alej definova , ako sa bude zaobchádza s nájdeným spamom:

- **Premiestni správu do prie inka pre neželané správy** (len ako doplnok pre Microsoft Outlook) – za iarknite toto polí ko, ak sa má každý detegovaný spam automaticky premiestni do konkrétneho prie inka pre spam v poštovej aplikácii MS Outlook. V sú asnosti túto službu iné poštové aplikácie nepodporujú.
- **Prida príjemcov poslaných e-mailov do zoznamu povolených** – za iarknite toto polí ko, ak sa majú všetci príjemcovia poslaných e-mailov považova za dôveryhodných a aby bolo možné doru ova všetky e-mailové správy prichádzajúce z ich e-mailových schránok
- **Zmeni predmet pri správach ozna ených ako SPAM** – ozna te toto za iarkavacie polí ko, ak chcete, aby sa všetky správy ozna ené ako spam ozna ili špecifickým slovom alebo znakom v poli s predmetom e-mailu; požadovaný text sa vkladá do aktivovaného textového po a
- **Opýta sa pred nahlásením nesprávnej detekcie** – Pod podmienkou, že ste po as procese inštalácie súhlasili s ú as ou v projekte [preferencií ochrany osobných údajov](#). V tom prípade ste povolili hlásenie zistených hrozieb spoločnosti AVG. Tieto hlásenia sa vytvárajú automaticky. Ke však za iarknete toto polí ko, potom sa vás pred nahlásením detegovaného spamu do AVG program opýta, i sa má správa naozaj klasifikova ako spam.

V dialógovom okne **Nastavenia výkonu jadrového modulu** (otvára sa pomocou položky **Výkon** v ponuke na *avej strane*) sa nachádzajú výkonové nastavenia sú asti **Anti-Spam**:



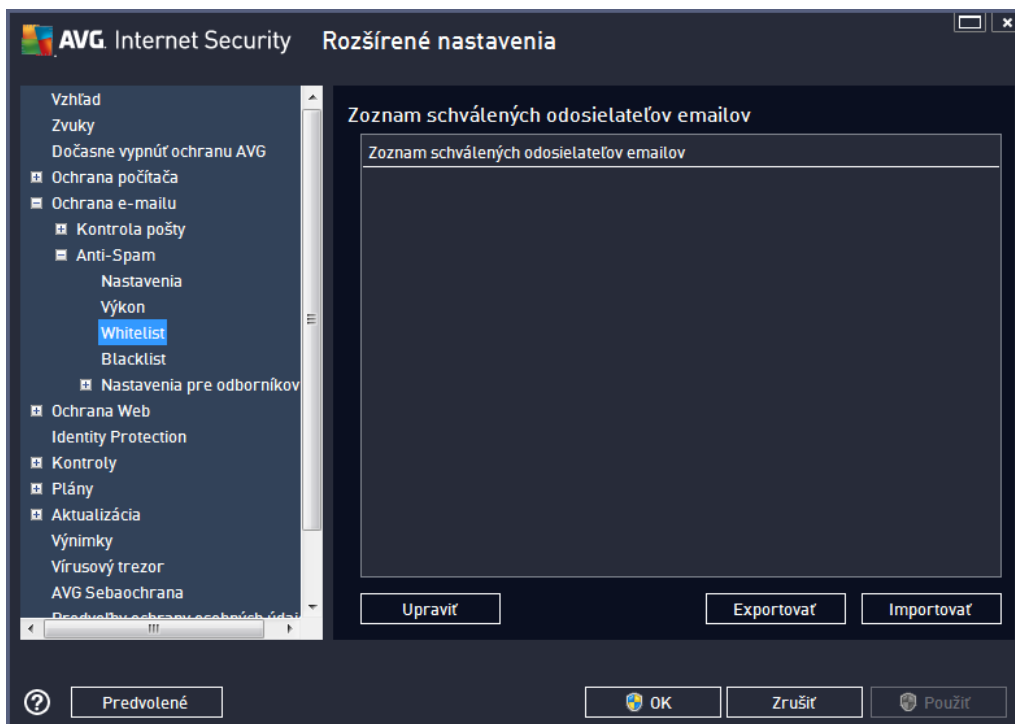
Posunutím jazdca smerom do *ava* alebo *doprava* nastavte úroveň výkonu kontroly, od režimu **Lacnejší desktop** po režim **Drahší desktop**.

- **Lacnejší desktop** – Pri kontrole sa nepoužijú žiadne pravidlá na identifikovanie spamu. Na identifikáciu sa použijú len tréningové údaje. Tento režim vám neodporujeme používať na bežné účely. Používajte ho len vtedy, keď máte poškodený alebo veľmi slabý hardvér.
- **Drahší desktop** – V tomto režime sa bude využívať väčšie množstvo pamäte. Počas procesu prehadzovania na zistenie prítomnosti spamu sa použijú nasledovné funkcie: pravidlá a vyrovnávací pamäť databázy spamu, základné a rozšírené pravidlá, adresy IP rozosielateľov spamu a databázy rozosielateľov spamu.

Položka **Povolí kontrolu on-line** je štandardne zapnutá. Používa sa na presnejšiu detekciu spamu pomocou komunikácie so servermi [Mailshell](#), t. j. kontrolované dáta sa porovnávajú s on-line databázami [Mailshell](#).

Obyčajne sa odporúča ponechať predvolené nastavenia a zmeniť ich len vtedy, ak k tomu máte závažný dôvod. Zmeny konfigurácie odporúčame robiť len skúseným používateľom!

Položka **Whitelist** otvorí dialógové okno s názvom **Zoznam schválených odosielateľov** s globálnym zoznamom povolených e-mailových adries odosielateľov a názvov domén, ktorých správy nebudú nikdy označené ako spam.



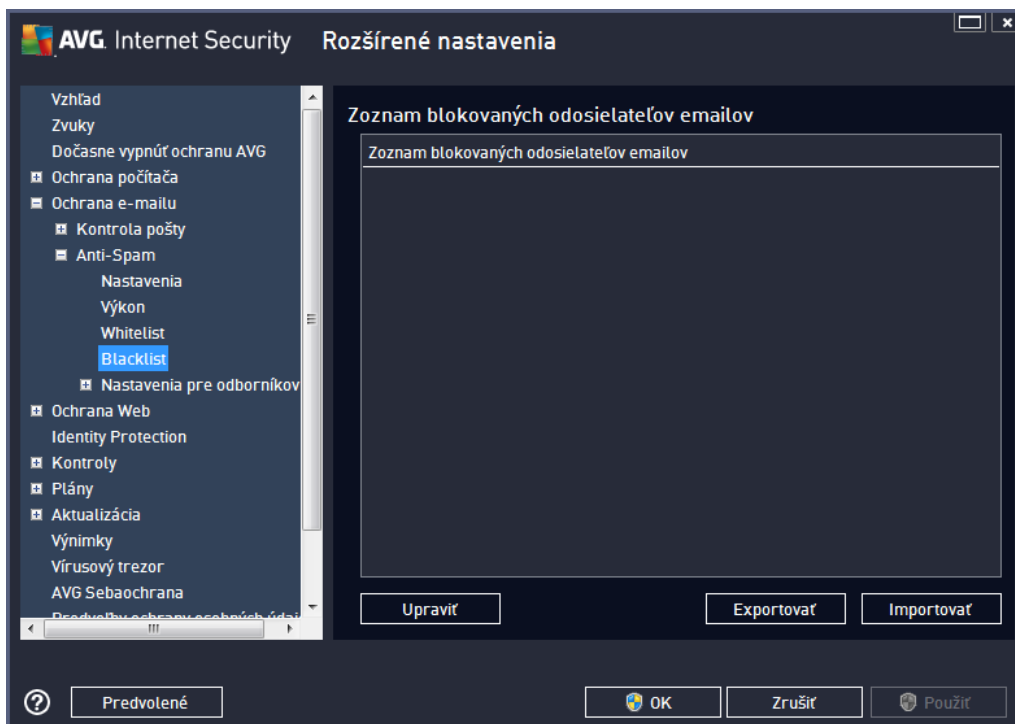
Editované rozhranie umožňuje zostaviť zoznam odosielateľov, o ktorých ste presvedčení, že vám nikdy nepošlú nevyžiadané správy (spam). Zároveň môžete vytvoriť zoznam úplných názvov domén (napríklad *avg.com*), o ktorých viete, že nevytvárajú spamové správy. Keď máte zostavený takýto zoznam odosielateľov a/alebo názvov domén, môžete ich zadať niektorou z nasledujúcich metód: priamym zadáním každej e-mailovej adresy alebo importovaním celého zoznamu adries naraz.

Ovládacie tlačidlá

Sú dostupné nasledovné ovládacie tlačidlá:

- **Upraviť** – po stlačení tohto tlačidla sa otvorí dialógové okno, do ktorého môžete ručne zadať zoznam adries (môžete použiť aj metódu kopírovania a prilepiť). Do každého riadka môžete vždy jednu položku (odosielateľ a názov domény).
- **Exportovať** – ak sa z nejakého dôvodu rozhodnete exportovať záznamy, môžete tak urobiť stlačení tohto tlačidla. Všetky súbory sa uložia do jednoduchého textového súboru.
- **Importovať** – ak už máte pripravený textový súbor s e-mailovými adresami / názvami domén, môžete ho len importovať pomocou tohto tlačidla. Súbor môže obsahovať len jednu položku (adresu, názov domény) v každom riadku.

Položka **Blacklist** otvorí dialógové okno s celkovým zoznamom blokových e-mailových adries odosielateľov a názvov domén, ktorých správy sa vždy označia ako spam.



V rozhraní úprav môžete zostaviť zoznam odosielateľov, od ktorých odakáivate nevyžiadané správy (spam). Zároveň môžete vytvoriť zoznam úplných názvov domén (napr. *spamingovaspolocnost.sk*), od ktorých odakáivate alebo ste dostali nevyžiadajúcu poštu. Všetky e-maily z uvedených adries/domén budú identifikované ako SPAM. Keď máte zostavený takýto zoznam odosielateľov a/alebo názvov domén, môžete ich zadať niektorou z nasledujúcich metód: priamym zadaním každej e-mailovej adresy alebo importovaním celého zoznamu adries naraz.

Ovládacie tlačidlá

Sú dostupné nasledovné ovládacie tlačidlá:

- **Upravi** – po stlačení tohto tlačidla sa otvorí dialógové okno, do ktorého môžete ručne zadať zoznam adries (môžete použiť aj metódu kopírovania a prilepiť). Do každého riadka môžete vždy vložiť jednu položku (odosielateľ a názov domény).
- **Exportovať** – ak sa z nejakého dôvodu rozhodnete exportovať záznamy, môžete tak urobiť stlačení tohto tlačidla. Všetky súbory sa uložia do jednoduchého textového súboru.
- **Importovať** – ak už máte pripravený textový súbor s e-mailovými adresami / názvami domén, môžete ho len importovať pomocou tohto tlačidla.

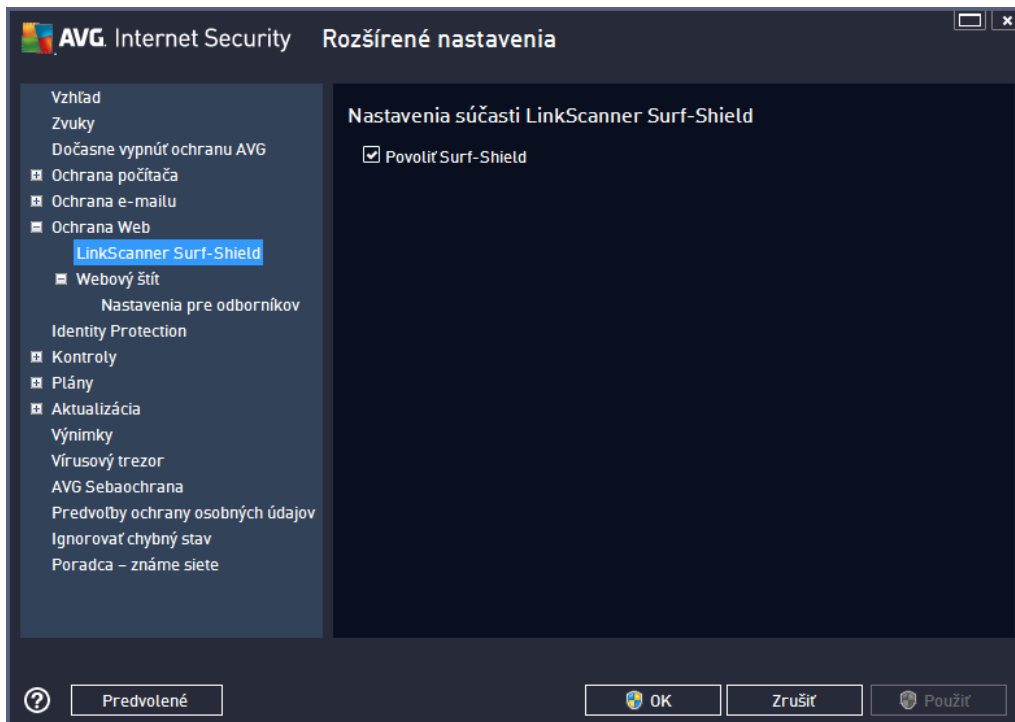
Vetva Nastavenia pre odborníkov obsahuje rozšírené možnosti nastavenia pre funkciu Anti-Spam. Tieto nastavenia sú určené výhradne pre skúsených používateľov, zvyčajne ajne správcov siete, ktorí potrebujú veľa podrobne nastaviť konfiguráciu ochrany pred nevyžiadanou poštou na dosiahnutie najlepšej možnej ochrany poštových serverov. Z tohto dôvodu nie je dostupná žiadna ďalšia pomoc pre jednotlivé dialógové okná, ale v používateľskom rozhraní sa nachádza stručný opis každej príslušnej možnosti. Dôrazne odporúčame nenechať žiadne nastavenia, ak nie ste dokonale oboznámení s rozšírenými nastaveniami programu Spamcatcher (MailShell Inc.). Každá nevhodná zmena môže mať za následok zníženie výkonu alebo nesprávne fungovanie súčastí.

Ak sa aj napriek tomu rozhodnete zmeniť konfiguráciu súčastí Anti-Spam na veľa podrobnej úrovni, postupujte podľa pokynov uvedených priamo v používateľskom rozhraní. V každom dialógovom okne nájdete jednu konkrétnu funkciu, ktorú môžete upraviť. V danom dialógovom okne je vždy uvedený jej popis. Upraviť môžete tieto parametre:

- **Filtrovanie** – zoznam jazykov, zoznam krajín, povolené adresy IP, blokované adresy IP, blokované krajiny, blokované súbory znakov, nežiaduci odosielatelia.
- **RBL** – servery RBL, viacnásobné detegovanie, prahová hodnota, časový limit, maximálny počet adries IP.
- **Internetové pripojenie** – časový limit, server proxy, autentifikácia servera proxy.

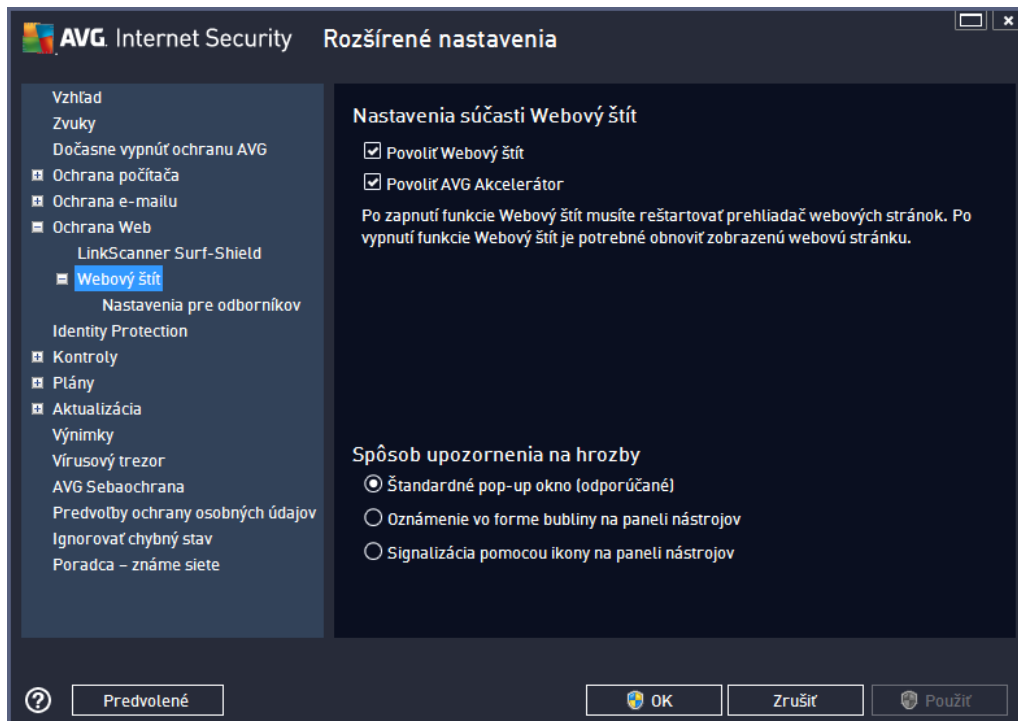
9.6. Ochrana prezerania webu

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



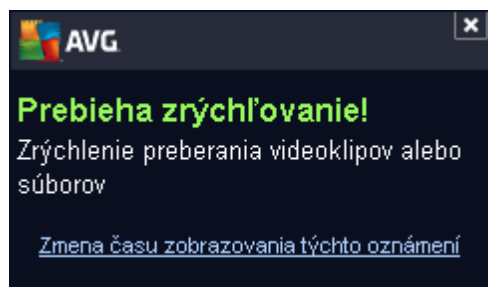
- **Povoliť Surf-Shield** – (štandardne zapnuté): aktívna ochrana (v reálnom čase) pred webovými stránkami s nebezpečným obsahom pri ich otvorení. Pripojenie k známym škodlivým stránkam a ich nebezpečnému obsahu sa zablokuje pri otvorení v internetovom prehliadači (alebo inej aplikácii, ktorá používa protokol HTTP).
- **Pridať 'Zabezpečené sú správy od spoločnosti LinkScanner'...** – (štandardne vypnuté): potvrdením tejto možnosti zaistíte, že všetky správy odoslané zo sociálnych sietí Facebook/MySpace obsahujúce aktívne hypertextové odkazy budú obsahovať potvrdenie, že boli skontrolované spoločnosťou LinkScanner.

9.6.1. Webový štít



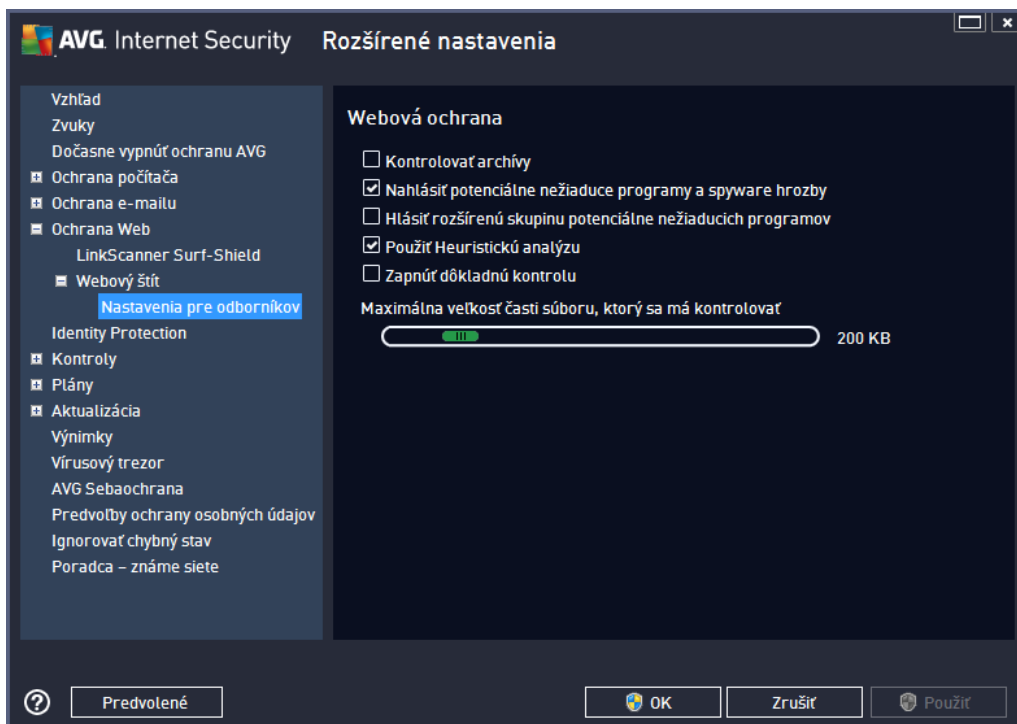
Dialógové okno **Webový štít** ponúka tieto možnosti:

- **Povoli Webový štít (štandardne zapnuté)** – Aktivuje/deaktivuje celú službu **Webový štít**. Inšie rozšírené nastavenia sú, ak **Webový štít** nájdete v nasledujúcom dialógovom okne s názvom [Webová ochrana](#).
- **Povoli AVG Accelerator (štandardne zapnuté)** – Aktivuje/vypne sa služba AVG Akcelerátor. Služba AVG Akcelerátor umožňuje stabilnejšie prehrávanie on-line videa a uľahčuje inšie preberania. Ak prebieha akcelerácia videa, v paneli úloh vás upozorní kontextové okno:



Spôsob upozornenia na hrozby

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



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

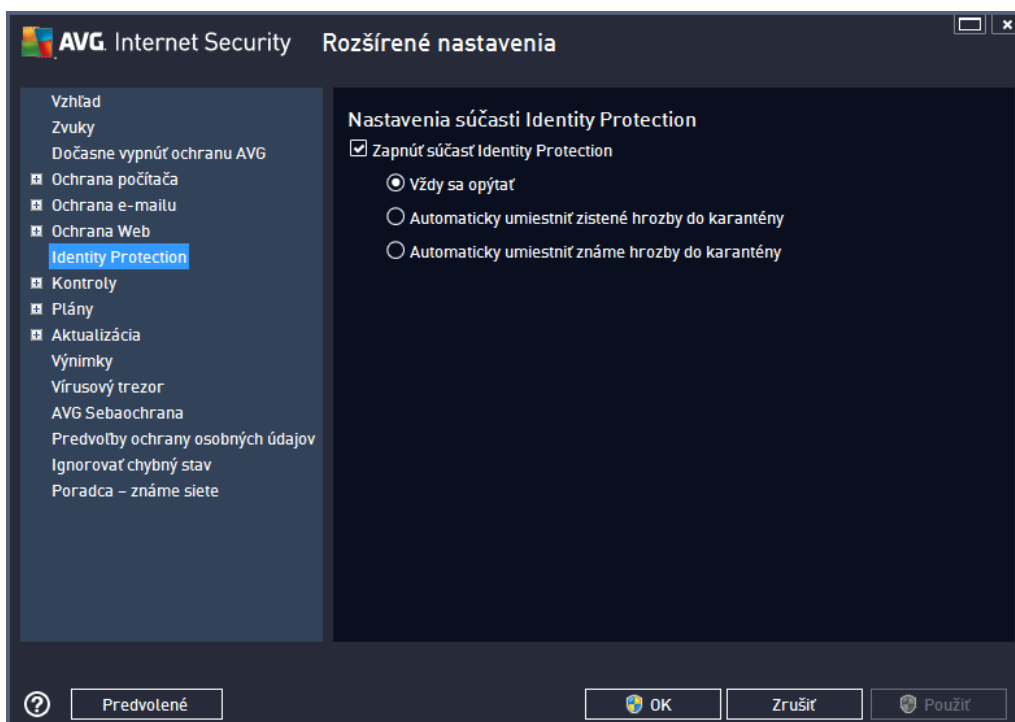
- **Zapnúť webovú ochranu** – Keď je táto funkcia zapnutá, potom bude súčasná **Webový štít** kontrolovať obsah internetových stránok. Za predpokladu, že je táto súčasná zapnutá (štandardne je), môžete aj tieto položky zapnúť/vypnúť:
 - **Kontrolovať archívy** – (štandardne vypnuté): kontrolovať obsah archívov, ktoré sa môžu nachádzať na otvorenej internetovej stránke.
 - **Nahlásiť potenciálne nežiaduce programy a spyware hrozby** (predvolene zapnuté) – začiarknite toto políčko, ak chcete 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.
 - **Hlásiti 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.
 - **Použiť heuristickú analýzu** (štandardne zapnuté): kontrolovať obsah zobrazenej stránky pomocou metódy heuristickej analýzy (dynamickkej emulácie inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí).

- o **Zapnú dôkladnú kontrolu** (štandardne vypnuté) – V určitých situáciách (podozrenie na infikovanie počítača) môžete touto možnosťou aktívovať najdôkladnejšie kontrolné algoritmy, ktoré pre istotu skontrolujú aj tie oblasti počítača, ktoré sa obyčajne vôbec neinfikujú. Upozorujeme však, že tento spôsob je náročný na zas.
- o **Maximálna veľkosť veľkosť kontrolovaného súboru** – ak sa priložené súbory nachádzajú na otvorenej stránke, potom sa ich obsah môže zároveň skontrolovať ešte predtým, než sa súbory prevezmú do počítača. Kontrola veľkosti súborov však chvíľu trvá a preberanie z internetovej stránky sa môže výrazne spomaliť. Pomocou posúvača môžete nastaviť maximálnu veľkosť súboru, ktorá sa má kontrolovať súčasne s **Webový štít**. 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 ihneď deteguje.
- o **Vylúčiť hostiteľa/adresu IP/doménu** – Do textového poľa zadajte presný názov servera (hostiteľa, adresu IP, adresu IP s maskou alebo adresu URL) alebo doménu, ktorú nemá súčasne **Webový štít** kontrolovať. Preto vylúčíte len hostiteľa, o ktorom ste si absolútne istí, že by nikdy neposlal nebezpečné dáta.

9.7. Identity Protection

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

Dialógové okno **Nastavenia súčasti Identity Protection** vám umožní zapnúť alebo vypnúť základné funkcie súčasti [Identity Protection](#):





Zapnú sú as Identity Protection(predvolene zapnutá) – zrušením za iarknutia sa vypne sú as [Identity Protection](#).

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

Ke je sú as Identity Protection zapnutá, môžete nastavi , o sa má urobi pri detegovaní hrozby:

- **Vždy sa opýta** (predvolene zapnuté) – pri detegovaní hrozby sa vás program opýta, i sa má hrozba premiestni do karantény, aby nedošlo k neželanému odstráneniu aplikácií, ktoré chcete používa .
- **Automaticky umiestni zistené hrozby do karantény** – Ozna te toto za iarkavacie polí ko, ak sa majú všetky potenciálne zistené hrozby ihne premiestni na bezpečné miesto vo [Vírusovom trezore](#). Ke zachováte predvolené nastavenia, potom sa vás program opýta pri detegovaní hrozby, i sa má táto hrozba premiestni do karantény, aby nedošlo k odstráneniu aplikácií, ktoré chcete používa .
- **Automaticky umiestni známe hrozby do karantény** – Nechajte toto za iarkavacie polí ko ozna ené, ak sa majú všetky aplikácie ozna ené ako potenciálne škodlivé automaticky a ihne premiestni do [Vírusového trezora](#).

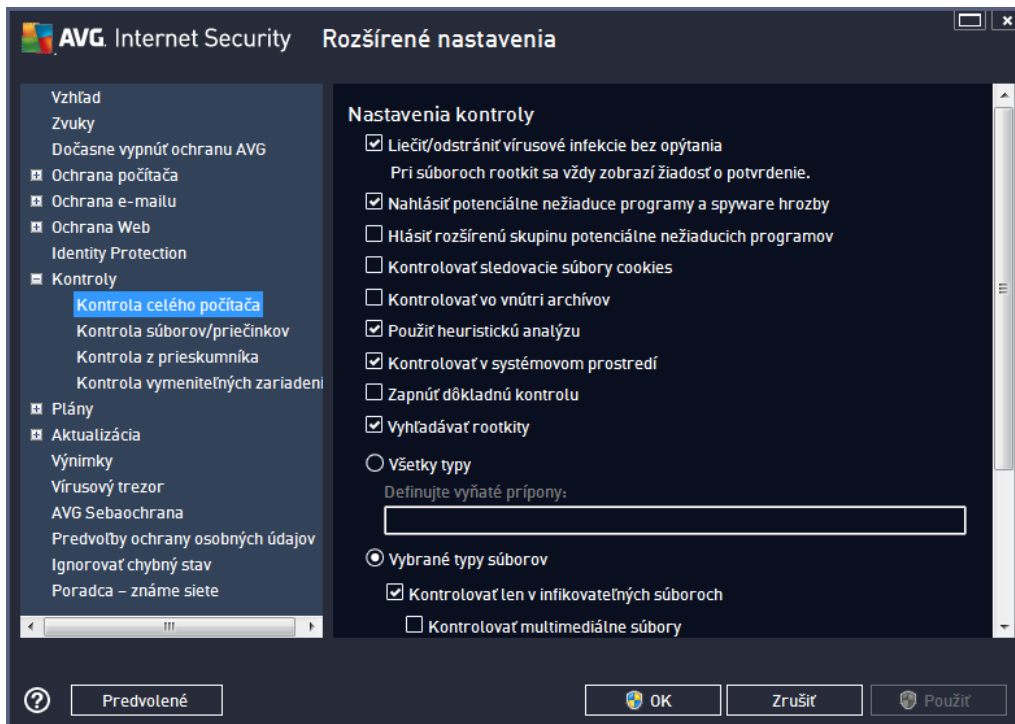
9.8. Kontroly

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 z prieskumníka](#)** – špeciálna kontrola vybraného objektu priamo v prostredí programu Windows Explorer.
- **[Kontrola súborov/prie inkov](#)** – štandardná vopred definovaná kontrola vybraných oblastí počítača.
- **[Kontrola vymeniteľných zariadení](#)** – špeciálna kontrola vymeniteľných zariadení zapojených do počítača.

9.8.1. Kontrola celého počítača

Funkcia **Kontrola celého počítača** umožňuje upraviť parametre jednej z kontrol vopred definovaných výrobcou softvéru, [Kontrola celého počítača](#):



Nastavenia kontroly

Vasti **Nastavenia kontroly** sa nachádza zoznam parametrov prehadávania, ktoré sa dajú voliť alebo zapnúť alebo vypnúť:

- **Liečiť/odstrániť vírusové infekcie bez opýtania** (štandardne zapnuté) – Ak sa počas kontroly zistí prítomnosť vírusu, môže sa automaticky vyliečiť, ak je k dispozícii liečba. Ak nie je možné infikovaný súbor vyliečiť automaticky, premiestni sa do [Vírusového trezora](#).
- **Nahlásiť potenciálne nežiaduce programy a spyware hrozby** (štandardne zapnuté) – Zaujímať 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.
- **Hlásit rozšírenú skupinu potenciálne nežiaducich programov** (štandardne vypnuté) – Zaujímať 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 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 detekciu 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 škodlivého programu 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 nespustíte 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 .

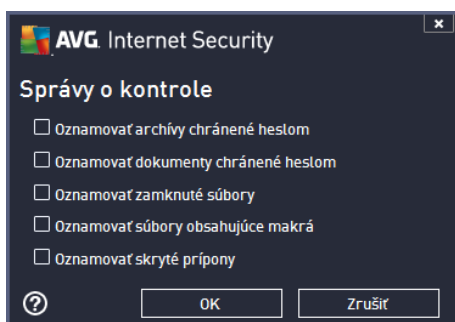
Nastavi rýchlos dokon enia kontroly

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

a spomalia sa ostatné inosti v po íta i (*táto funkcia sa používa, ke je po íta zapnutý, ale nikto na om v danom momente nepracuje*). Na druhej strane môžete zníži využívanie systémových zdrojov pred žením doby trvania kontroly.

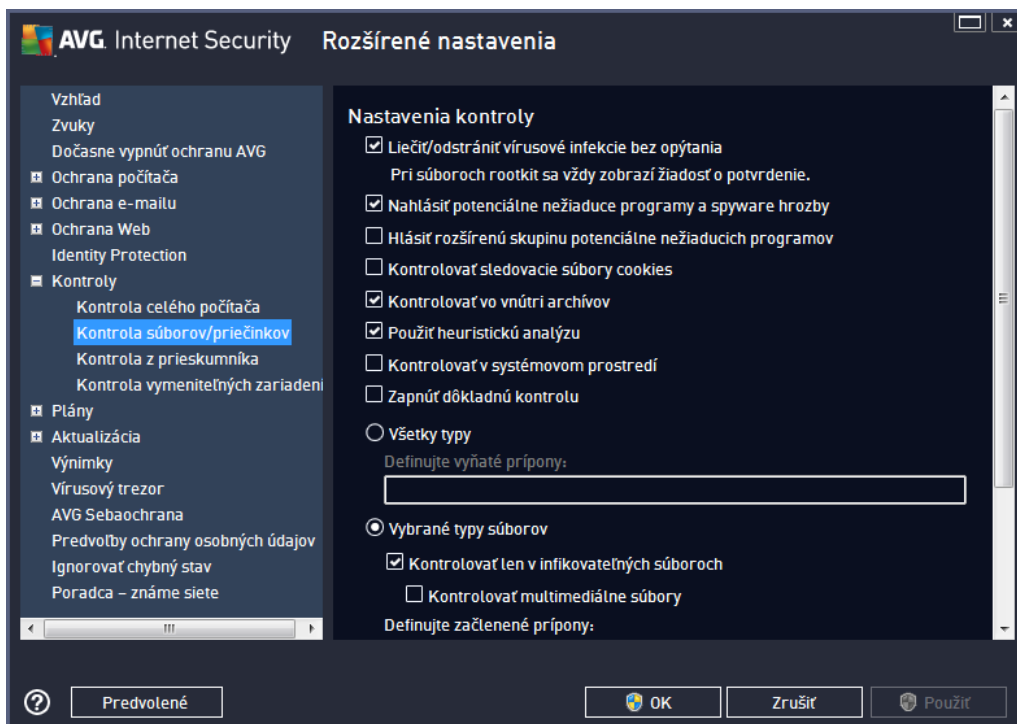
Vytvori alšie správy o kontrole...

Kliknutím na odkaz **Vytvori alšie správy o kontrole...** otvorte samostatné dialógové okno s názvom **Správy o kontrole**, v ktorom môžete za iarknutím konkrétnych položiek definova , ktoré nálezy sa majú hlási :



9.8.2. Kontrola súborov / priečinkov

Rozhranie editácie na **Kontrola súborov/prie inkov** je rovnaké ako dialógové okno editácie s názvom [Kontrola celého po íta a](#). Všetky možnosti konfigurácie sú rovnaké, predvolené nastavenia sú však prísnejšie pri [Kontrola celého po íta a](#):



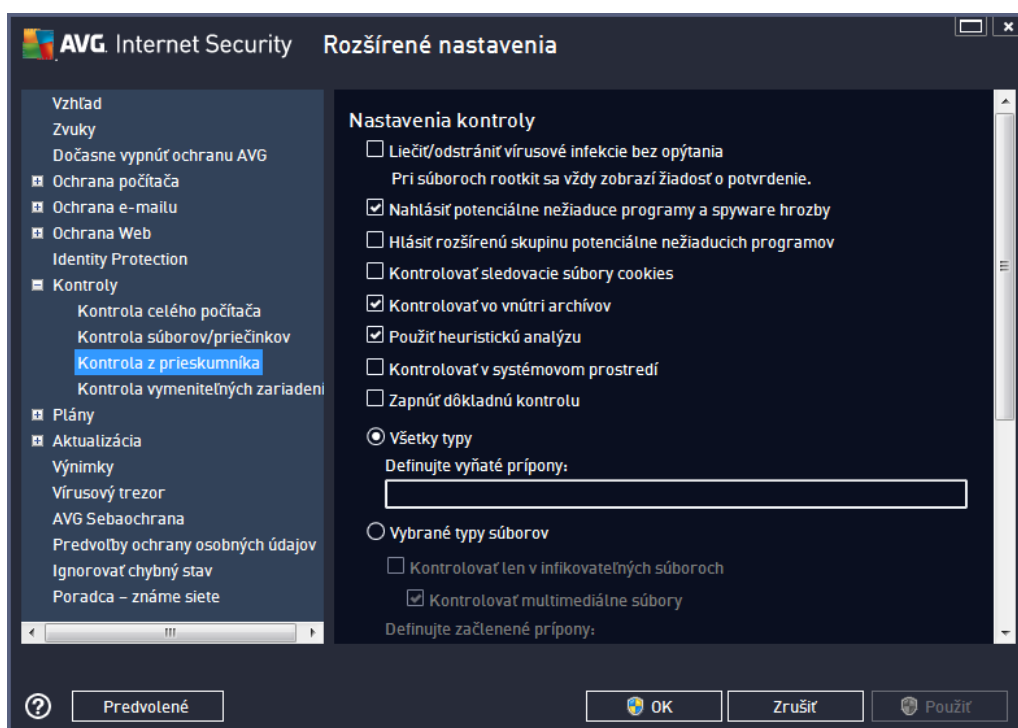
Všetky parametre nastavené v tomto dialógovom okne konfigurácie sa vz ahujú len na oblasti

vybrané na kontrolu v dialógovom okne [Kontrola súborov/priečinkov](#)!

Poznámka: Informácie o konkrétnych parametroch sa nachádzajú v kapitole [Rozšírené nastavenia AVG/Kontroly/Kontrola celého počítača](#).

9.8.3. Kontrola z prieskumníka

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



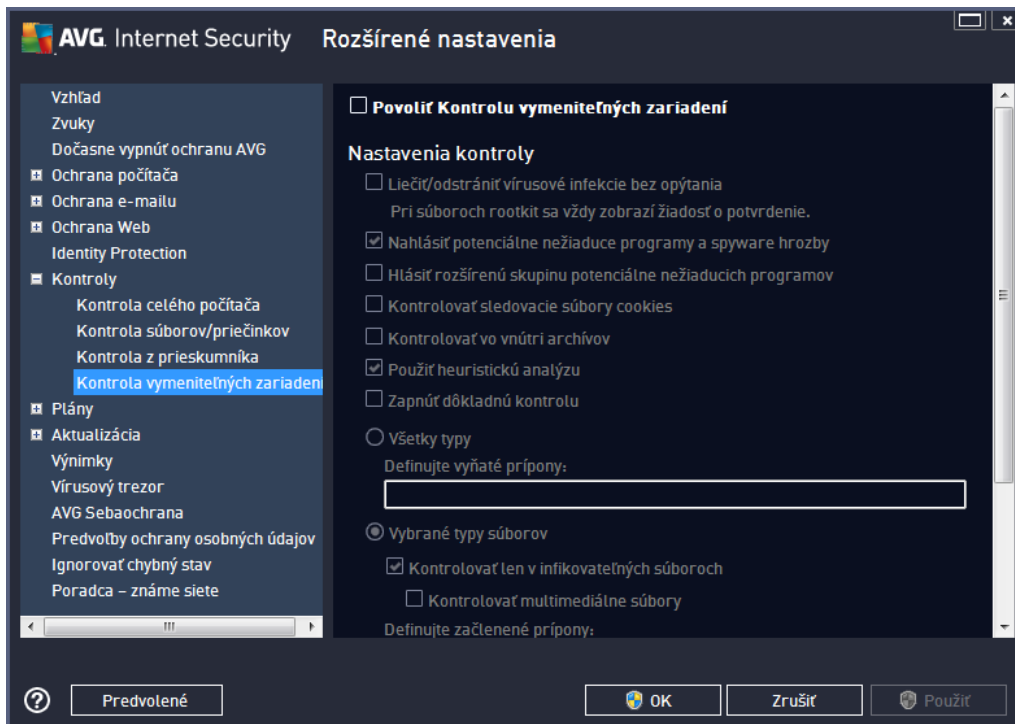
Zoznam parametrov je identický s parametrami používanými pre [kontrolu celého počítača](#). Predvolené nastavenia sa však líšia (napríklad *Kontrola celého počítača* štandardne nekontroluje archívy, ale kontroluje systémové prostredie, zatiaľ čo *Kontrola z prieskumníka* má presne opačné nastavenia).

Poznámka: Informácie o konkrétnych parametroch sa nachádzajú v kapitole [Rozšírené nastavenia AVG/Kontroly/Kontrola celého počítača](#).

V porovnaní s dialógovým oknom [Kontrola celého počítača](#) sa v dialógovom okne **Kontrola z prieskumníka** nachádza aj časť s názvom **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 po kontrolovaní deteguje infekcia.

9.8.4. Kontrola vymeniteľných zariadení

Rozhranie editácie **Kontrola vymeniteľných zariadení** sa ve mi podobá dialógovému oknu editácie [Kontrola celého počítača](#):



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

Poznámka: Informácie o konkrétnych parametroch sa nachádzajú v kapitole [Rozšírené nastavenia AVG/Kontroly/Kontrola celého počítača](#).

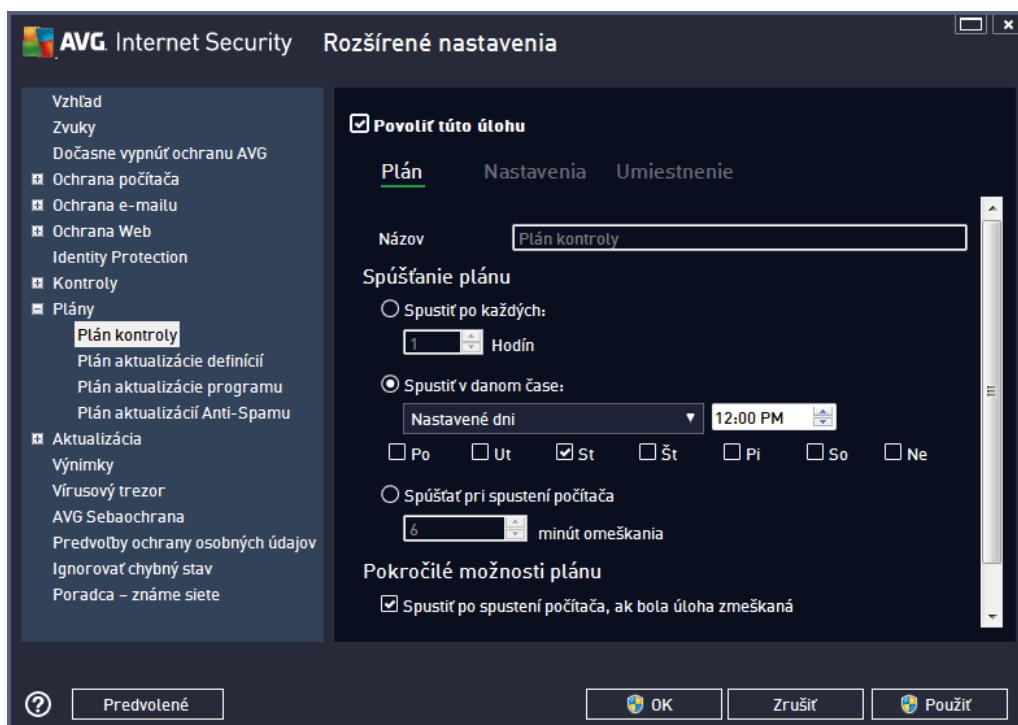
9.9. Plány

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

- [Plán kontroly](#)
- [Plán aktualizácie definícií](#)
- [Plán aktualizácie programu](#)
- [Plán aktualizácie sústav Anti-Spam](#)

9.9.1. Plán kontroly

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



Vo vedľajšom textovom poli **Názov** (neaktívne pre všetky predvolené plány) sa nachádza názov, ktorý tomuto konkrétnemu plánu 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 alej definovať tieto parametre kontroly:

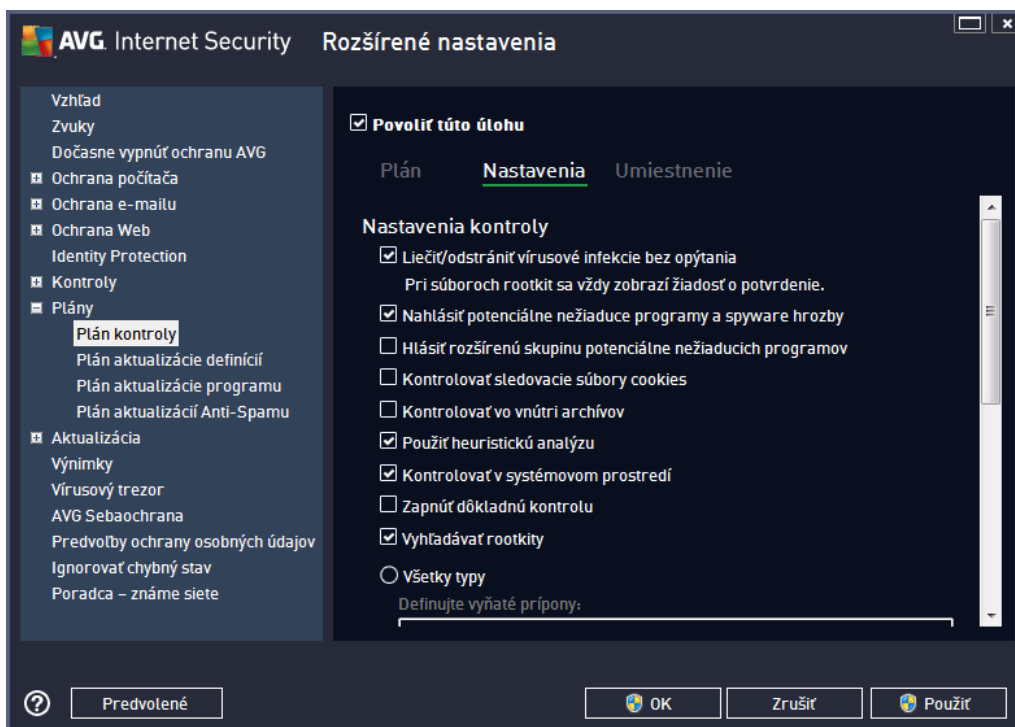
Spúšťanie naplánovaných úloh

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

Rozšírené možnosti plánu

Táto časť sa používa na definovanie podmienok, pri ktorých sa má resp. nemá spustiť kontrola, keď je počítač v úspornom režime alebo úplne vypnutý. Keď sa spustí naplánovaná kontrola v nastavenom režime, bude vás o tom informovať automaticky otvorené okno, ktoré sa otvorí nad [ikonou AVG v paneli úloh](#).

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



V karte **Nastavenia** nájdete zoznam parametrov kontrolovania, ktoré sa dajú voliť nezapnúť /vypnúť. 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 vyladený, pokiaľ je liek k dispozícii. Ak nie je možné infikovaný súbor vyladiť automaticky, presunú sa do [Vírusového trezora](#).
- **Nahlásiť potenciálne nežiaduce programy a spyware hrozby (štandardne zapnuté):** Zaujímať 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. Odporujeme vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň

zabezpečenia podľa a.

- **Hlási rozšírenú skupinu potenciálne nežiaducich programov** (štandardne vypnuté): Zaškrtnite 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 podľa a, ale môže blokovать dobré programy, a preto je táto funkcia štandardne vypnutá.
- **Kontrolova sledovacie súbory cookies** (štandardne vypnuté): Tento parameter súvisí s nastavením funkcie 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 prostredí podľa a*) bude jedna z metód, ktoré sa použijú na detekciu vírusov počas kontroly.
- **Kontrolova v systémovom prostredí** (štandardne zapnuté): počas kontroly sa budú overovať aj systémové oblasti podľa a.
- **Zapnú dôkladnú kontrolu** (štandardne vypnuté): v určitých situáciách (*podозrenie na infikovanie podľa a*) môžete touto možnosťou aktivovať najdôkladnejšie kontrolné algoritmy, ktoré pre istotu skontrolujú aj tie oblasti podľa a, ktoré sa obyčajne vôbec neinfikujú. Upozorujeme však, že tento spôsob je náročný na zas.
- **Kontrolova rootkity** (štandardne zapnuté): Kontrola súvisí s Anti-Rootkit skontroluje podľa a zisťuje prítomnosť potenciálnych rootkitov, t. j. programov a technológií, ktoré dokážu zakryť škodlivý program v počítači. Keď program deteguje rootkit, nemusí to nevyhnutne znamenať, že je počítač infikovaný. V niektorých prípadoch sa môžu určitým spôsobom ovládať alebo súvisieť s bežnými aplikáciami nesprávne označované ako rootkity.

Mali by ste tiež určiť, čo chcete kontrolovať

- **Všetky typy súborov** s možnosťou definovať výnimky z prehľadávania vytvorením zoznamu súborkou oddelených (*uložením sa súborky zmenia na bodkočiarkový 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 súbory – ak necháte toto políčko nezashkrtnuté, 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,

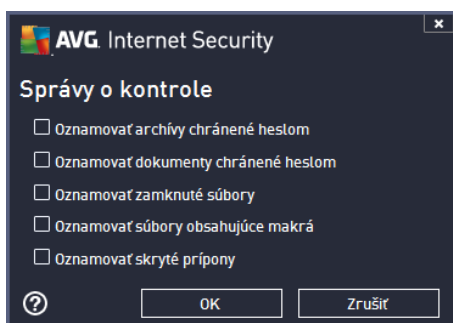
ak na to nemáte skutočný dôvod. Súbor bez prípony sú skôr podozrivé a mali by sa vždy kontrolovať.

Nastaviť rýchlosť dokončenia kontroly

V tejto časti môžete ale 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 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 využitie systémových zdrojov predĺžením doby trvania kontroly.

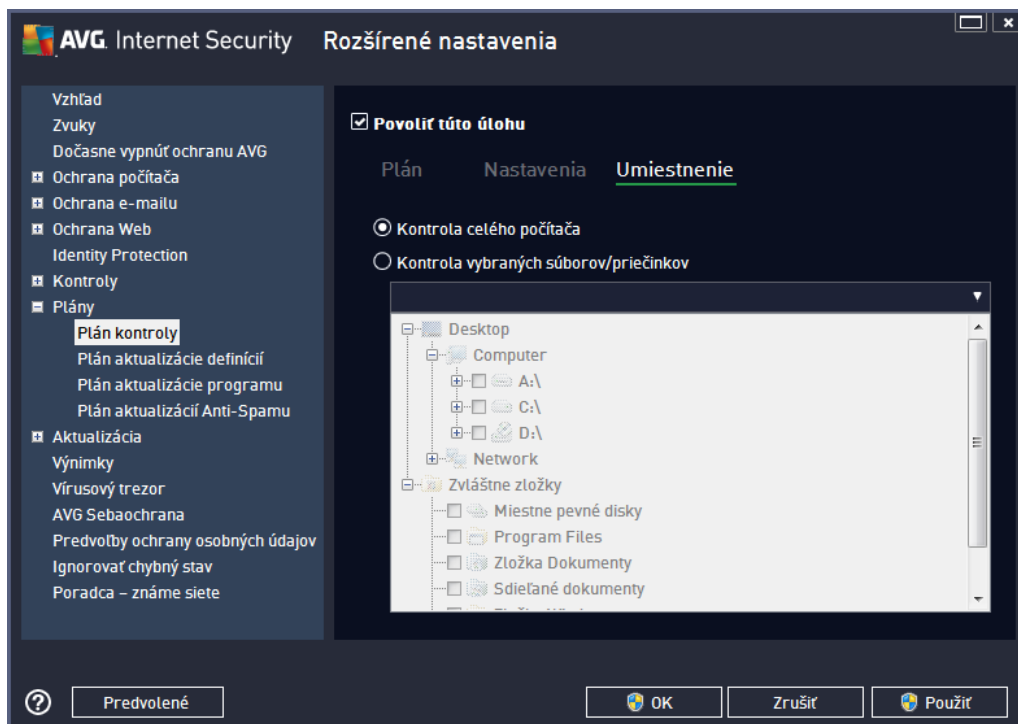
Vytvoriť ďalšie správy o kontrole

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



Možnosti vypnutia počítača

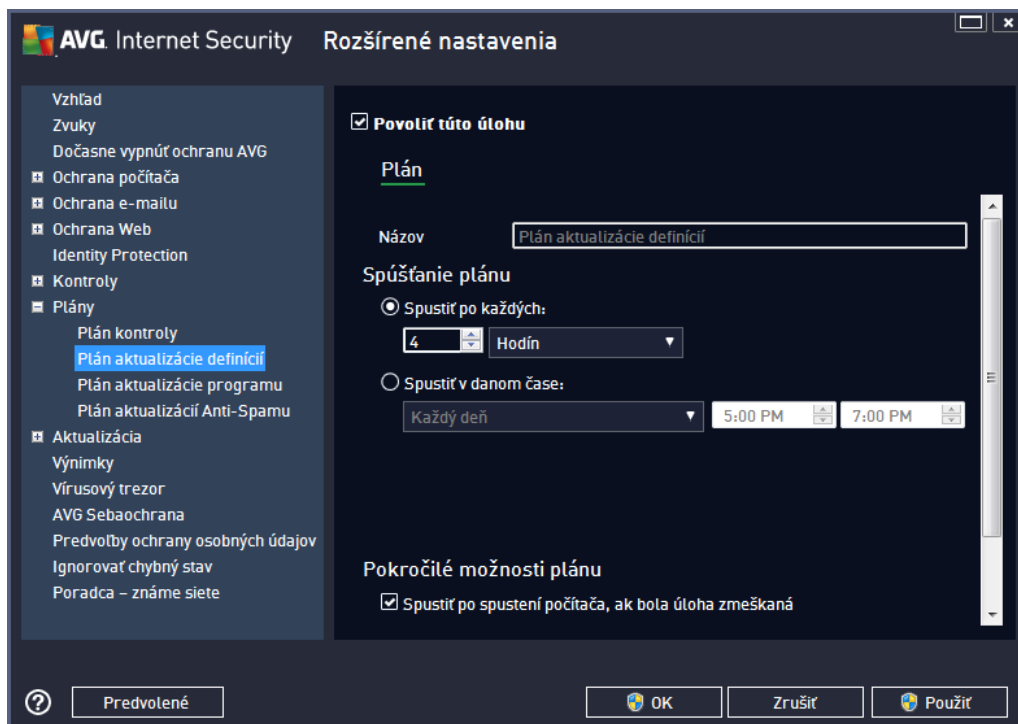
V časti **Možnosti vypnutia počítača** môžete rozhodnúť, či sa má počítač vypnúť automaticky po dokončení procesu kontroly. Po potvrdení tejto možnosti (**Vypnúť počítač po dokončení kontroly**) sa aktivuje nová možnosť, ktorá umožní vypnúť počítač, aj keď je momentálne zablokovaný (**Vynútené vypnutie,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



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

9.9.2. Plán aktualizácie definícií

Ak je to **naozaj potrebné**, zrušením začiarknutia políčka **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.

Spúšťanie naplánovaných úloh

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

Rozšírené možnosti plánu

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

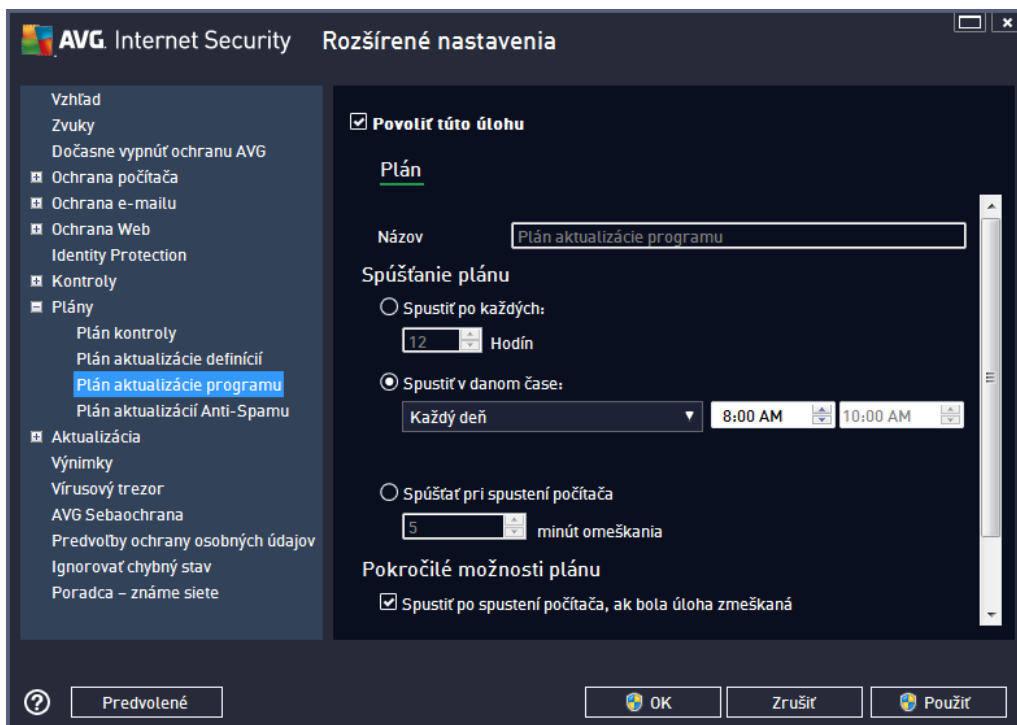
Ďalšie nastavenia aktualizácie

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

ikonou **AVG** v paneli úloh (pod podmienkou, že sa nezmenila predvolená konfigurácia v dialógom okne [Rozšírené nastavenia/Vzh ad](#)).

9.9.3. Plán aktualizácie programu

Ak je to **naozaj potrebné**, zrušením za iarknutia polí ka **Povolí túto úlohu** môžete do asne vypnú naplánovanú aktualizáciu programu a neskôr ju znova zapnú :



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

Spúš anie naplánovaných úloh

Tu zadajte asové intervaly pre spustenie novonaplánovanej aktualizácie programu. Na asovanie sa definuje ako opakované spúš anie aktualizácie po uplynutí určitého času (**Spusti po každých...**), definovaním presného dátumu a času (**Spúš a v konkrétnom ase...**), prípadne definovaním udalosti, s ktorou sa bude spája spustenie aktualizácie (**innos pri spustení po íta a**).

Rozšírené možnosti plánu

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

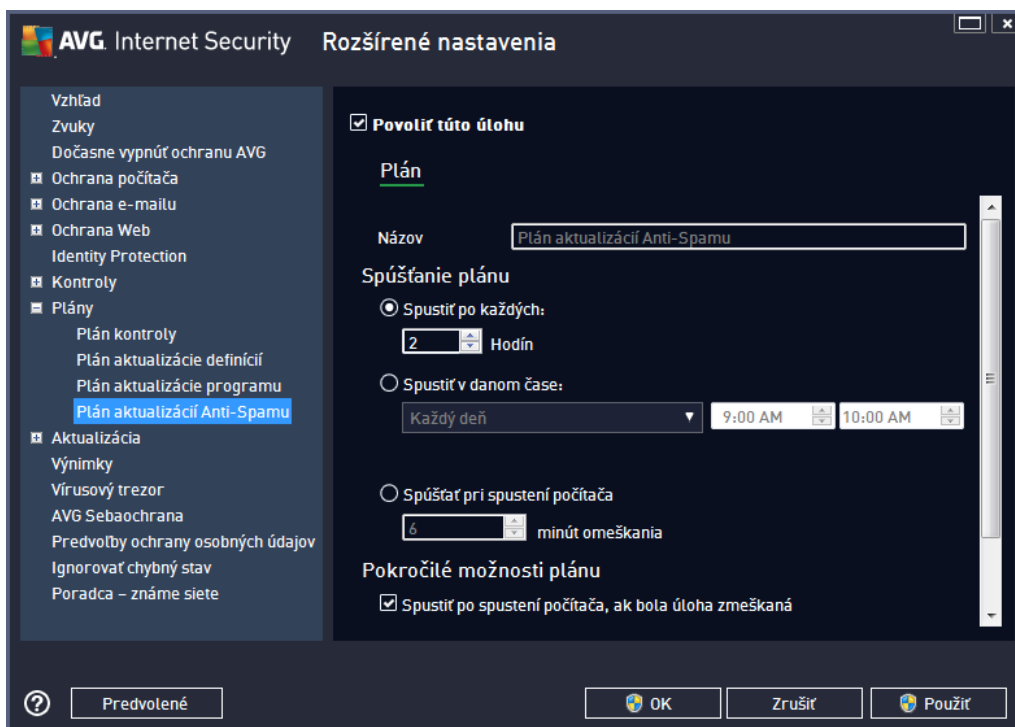
alšie nastavenia aktualizácie

Ozna te možnosť **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 spustiť. Po spustení naplánovanej aktualizácie vo vami nastavenom okne 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](#)).

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

9.9.4. Plán aktualizácie súčasti Anti-Spam

Ak je to naozaj potrebné, zrušením začiarknutia možnosti **Povolí túto úlohu** môžete dočasne vypnúť naplánovanú aktualizáciu súčasti [Anti-Spam](#) a neskôr ju znova zapnúť :



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

Spúšťanie naplánovaných úloh

Vom definujte časové intervaly pre nové naplánované spúšťanie aktualizácie súčasti Anti-Spam. Nastavenie sa nastavuje buď ako opakované spúšťanie aktualizácie súčasti Anti-Spam po uplynutí určitého času (**Spustiť po každých...**), nastavením presného dátumu a času (**Spustiť v konkrétnom časovom intervale**) alebo definovaním udalosti, s ktorou sa bude spájať spustenie aktualizácie (**Spustiť pri spustení počítača**).

Rozšírené možnosti plánu

Táto časť sa používa na definovanie podmienok, pri ktorých sa má/nemá spustiť aktualizácia súčasti Anti-Spam, keď je poškodená v úspornom režime alebo úplne vypnutý.

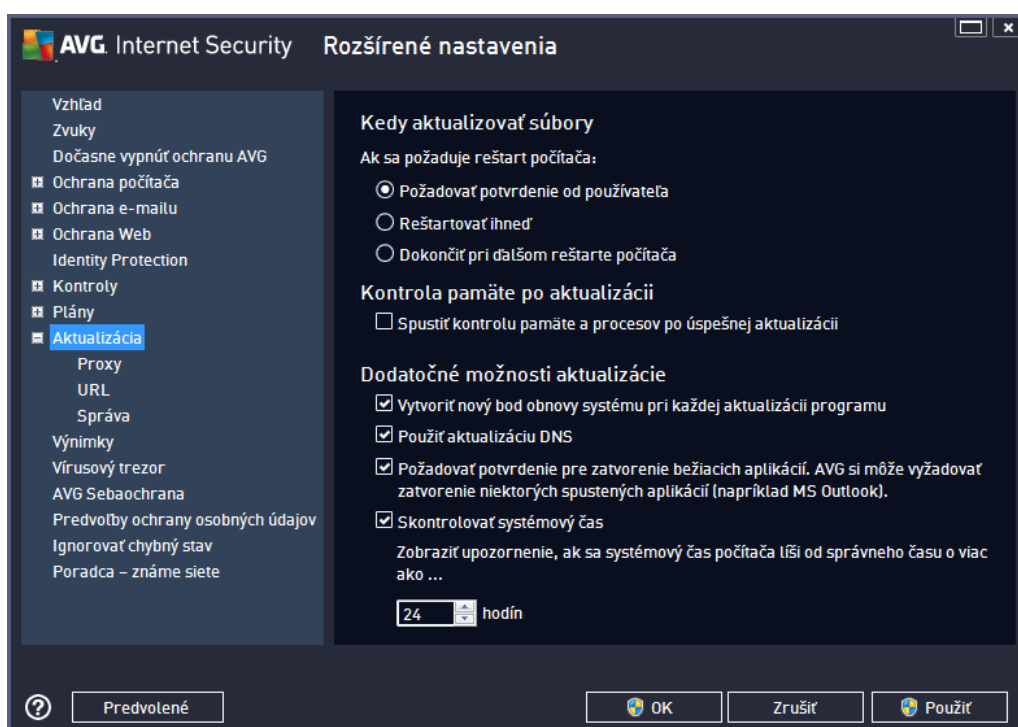
Ďalšie nastavenia aktualizácie

Označte možnosť **Spustiť aktualizáciu znova po obnovení pripojenia k internetu**, ak sa má v prípade výpadku internetového pripojenia obnoviť postup aktualizácie súčasti Anti-Spam ihneď po obnovení pripojenia.

Po spustení plánu kontroly v nastavenom okne sa zobrazí informácia v kontextovom okne nad [ikonou AVG v paneli úloh](#) (pod podmienkou, že sa nezmenila predvolená konfigurácia v dialógovom okne [Rozšírené nastavenia/Vzhľad](#)).

9.10. Aktualizácia

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



Kedy aktualizovať súbory

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

- **Požadova potvrdenie od používateľa (predvolené)** – zobrazí sa žiadosť, aby ste potvrdili reštartovanie počítača, ktoré je potrebné na dokončenie [aktualizácie](#)
- **Reštartovať ihneď** – Po dokončení počítač sa automaticky reštartuje ihneď po dokončení [aktualizácie](#) a nepožiadava vás o udelenie súhlasu.
- **Dokončiť pri ďalšom reštarte počítača** – Dokončenie [aktualizácie](#) bude odložené na ďalšie reštartovanie počítača. Odporúčame vám, aby ste túto možnosť zapli len v prípade, ak sa počítač reštartuje pravidelne, najmenej raz za deň!

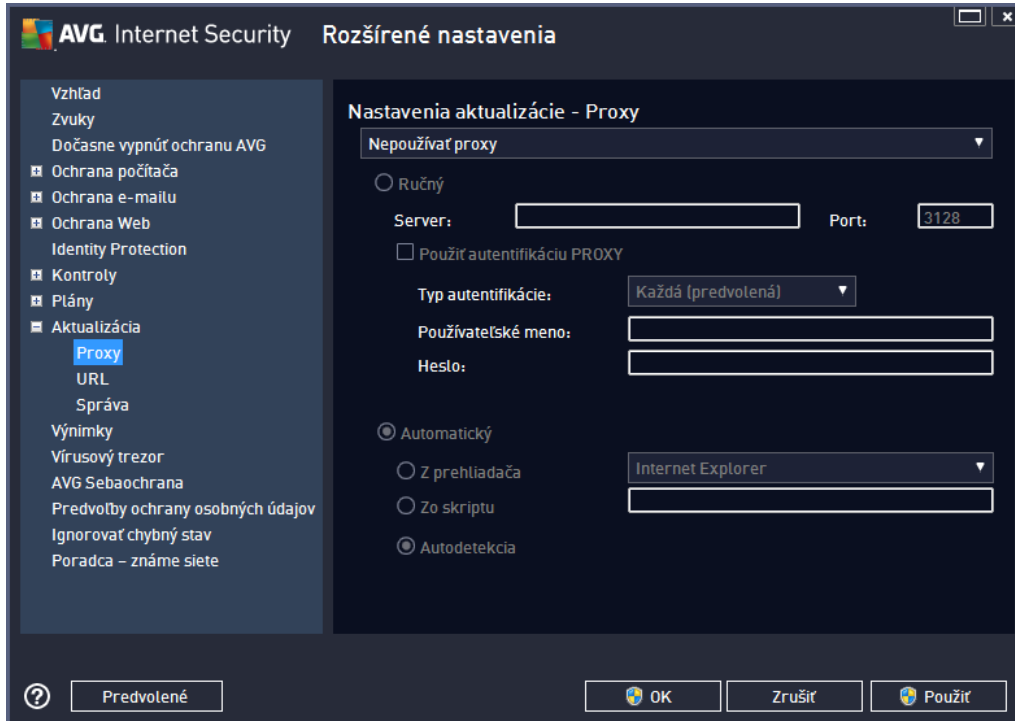
Kontrola pamäte po aktualizácii

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

Ďalšie možnosti aktualizácie

- **Vytvorí nový bod obnovenia systému po každej aktualizácii programu** – pred každým spustením aktualizácie programu AVG sa vytvorí bod obnovenia systému. Ak proces aktualizácie zlyhá a operačný systém spadne, potom vám tento bod obnovenia umožní obnoviť stav operačného systému s pôvodnou konfiguráciou. Prístup k tejto možnosti je cez ponuku Štart/Všetky programy/Príslušenstvo/Systémové nástroje/Obnovenie systému, ale vykoná zmeny týchto nastavení sa odporúča len skúseným používateľom! Nechajte toto za iarkavacie políčko označené, ak chcete používať túto funkcionálnosť.
- **Použiť aktualizáciu DNS (štandardne zapnuté)** – Ak je toto za iarkavacie políčko označené, po spustení aktualizácie programu **AVG Internet Security 2013** vyžaduje informácie o najnovšej verzii vírusovej databázy a najnovšej verzii programu na serveri DNS. Až potom sa prevzmu a nainštalujú najmenšie nevyhnutne potrebné aktualizované 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 dokončenie procesu aktualizácie.
- **Skontrolovať systémový čas** – Za iarknite toto políčko, ak chcete byť informovaní v prípade, keď sa systémový čas líši od skutočného času o viac, ako je nastavený počet hodín.

9.10.1. Proxy



Server proxy je samostatný server alebo služba spustená na počítači, ktorá 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 výponuku, ak ju chcete:

- **Nepoužíva proxy** – predvolené nastavenie
- **Použí proxy**
- **Pokúsi sa pripoji pomocou servera proxy a ak sa to nepodarí, pripoji 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.** Zadáajte adresu IP servera alebo názov servera.
- **Port.** Zadáajte číslo portu, ktorý umožní prístup na internet (štandardne je toto číslo nastavené na hodnotu 3128, ale môžete nastaviť inú hodnotu; ak máte pochybnosti, kontaktujte správcu siete).

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

server proxy nastavený týmto spôsobom, za iarknite možnos **Použi autentifikáciu PROXY** na overenie, i sú vaše používateľské meno a heslo platné na vytvorenie pripojenia na internet cez server proxy.

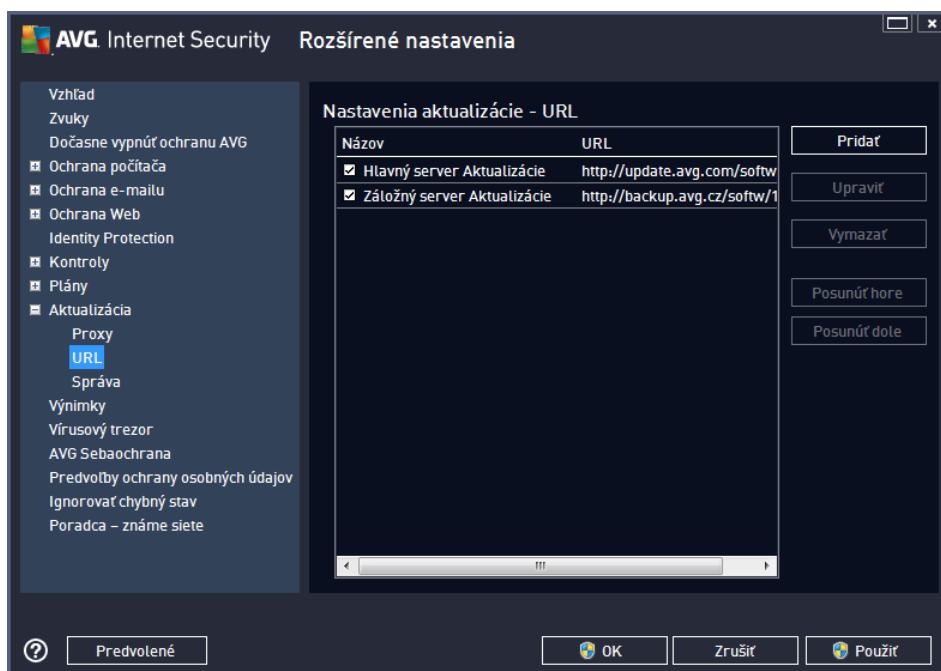
Automatická konfigurácia

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.
- **Automatické zistenie**: Konfigurácia sa zistí automaticky priamo zo servera proxy.

9.10.2. Adresa URL

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



Ovládacie tlačidlá

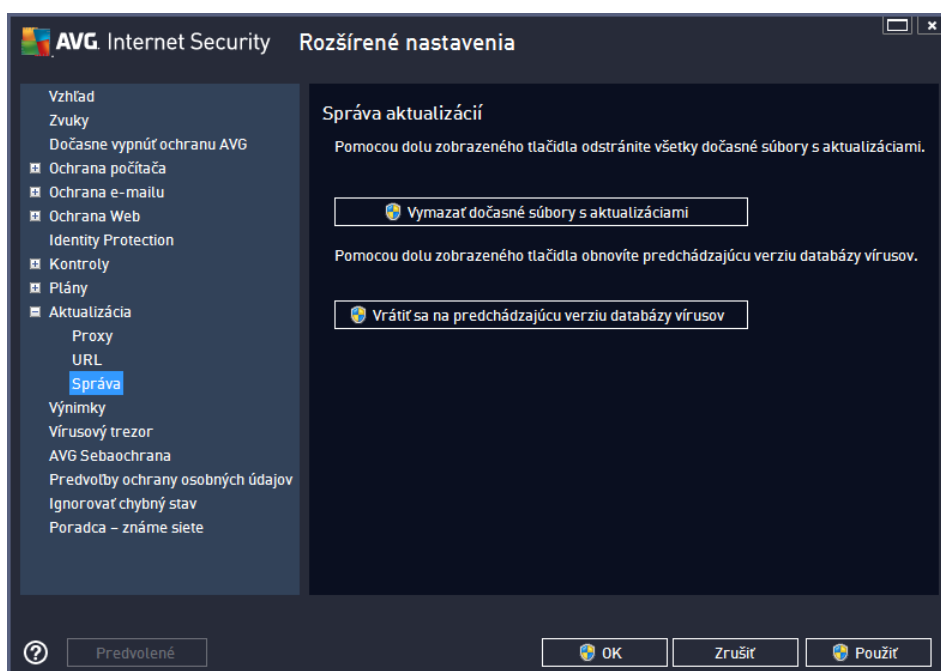
Zoznam a jeho položky môžete zmeniť pomocou nasledujúcich ovládacích tlačidiel:

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

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

9.10.3. Správa

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

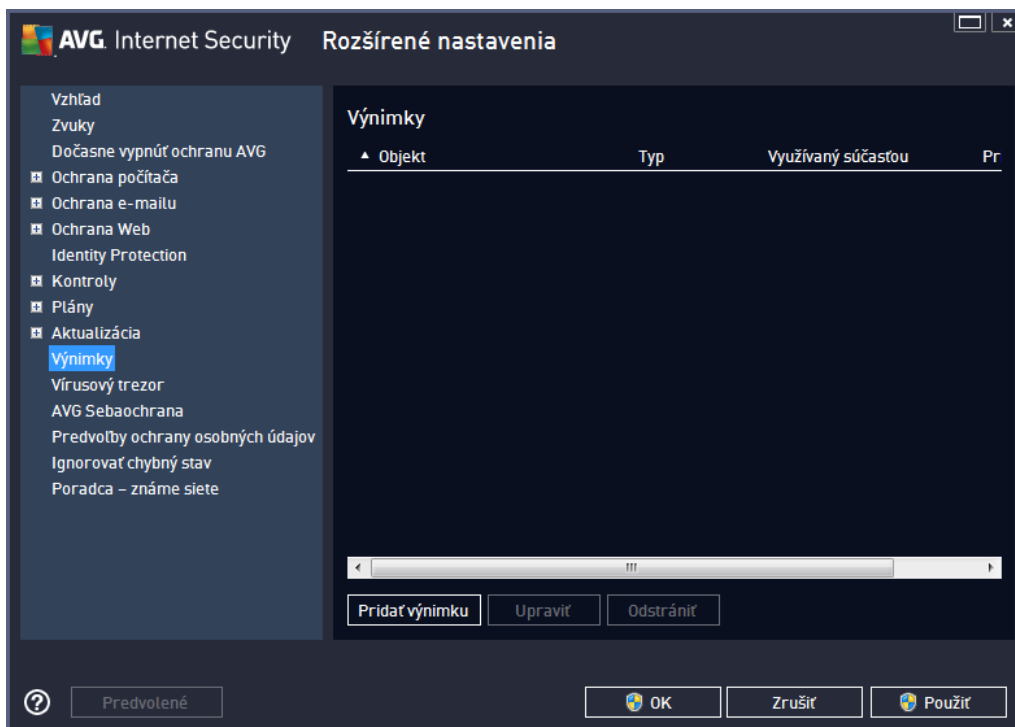


- **Vymaza dočasné súbory s aktualizáciami** – Stlačením tohto tlačidla sa vymažú všetky nepotrebné súbory aktualizácie z pevného disku (v predvolenom nastavení zostanú tieto súbory uložené 30 dní).
- **Vrátiť sa na predchádzajúcu verziu databázy vírusov** – Stlačením tohto tlačidla sa vymaže najnovšia 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 Internet Security 2013** bude ignorovať. Obvykle budete musieť výnimku definovať, ak program AVG neustále deteguje program alebo súbor ako hrozbu alebo blokuje bezpečnú stránku ako nebezpečnú. Pridajte takýto súbor alebo stránku do tohto zoznamu výnimiek a program AVG ho už nebude označovať ani blokovat.

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

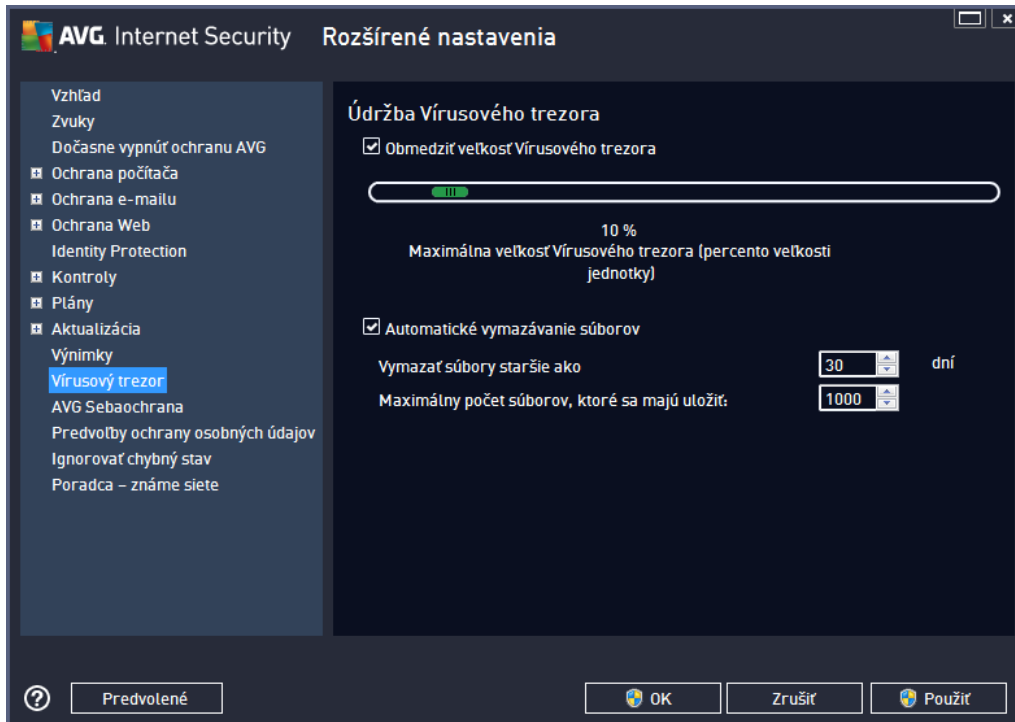


Hlavná stránka zobrazuje zoznam výnimiek, ak už boli nejaké definované. Vedľa každej položky sa nachádza začiarkavacie políčko. Keď je začiarkavacie políčko označené, potom sa výnimka používa; keď nie je, potom je výnimka len definovaná, ale momentálne sa nepoužíva. Kliknite na hlavičku stĺpca, aby sa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

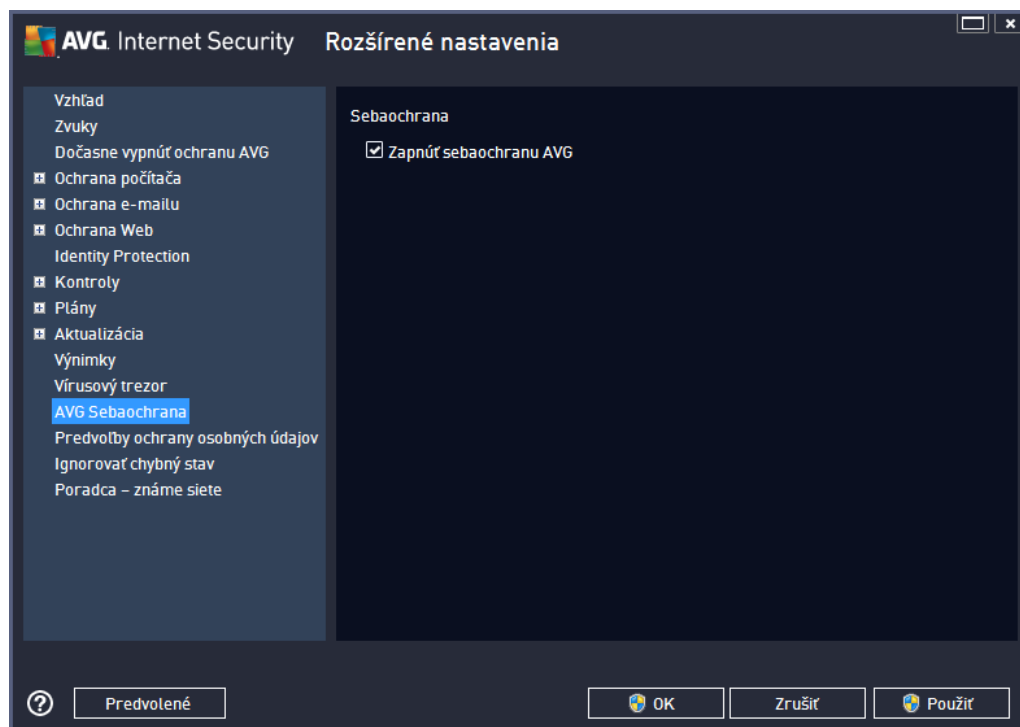
9.12. Vírusový trezor



Dialógové okno **Zachovanie Vírusového trezora** vám umožní zdefinovať niektoré parametre ochrany administrácie objektov uložených vo [Vírusovom trezore](#):

- **Obmedziť veľkosť vírusového trezora** – použijete posúvač na nastavenie maximálnej veľkosti [vírusového trezora](#). Táto veľkosť sa uvádza úmerne v porovnaní s veľkosťou vášho lokálneho disku.
- **Automatické vymazávanie súborov** – v tejto časti môžete zdefinovať 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

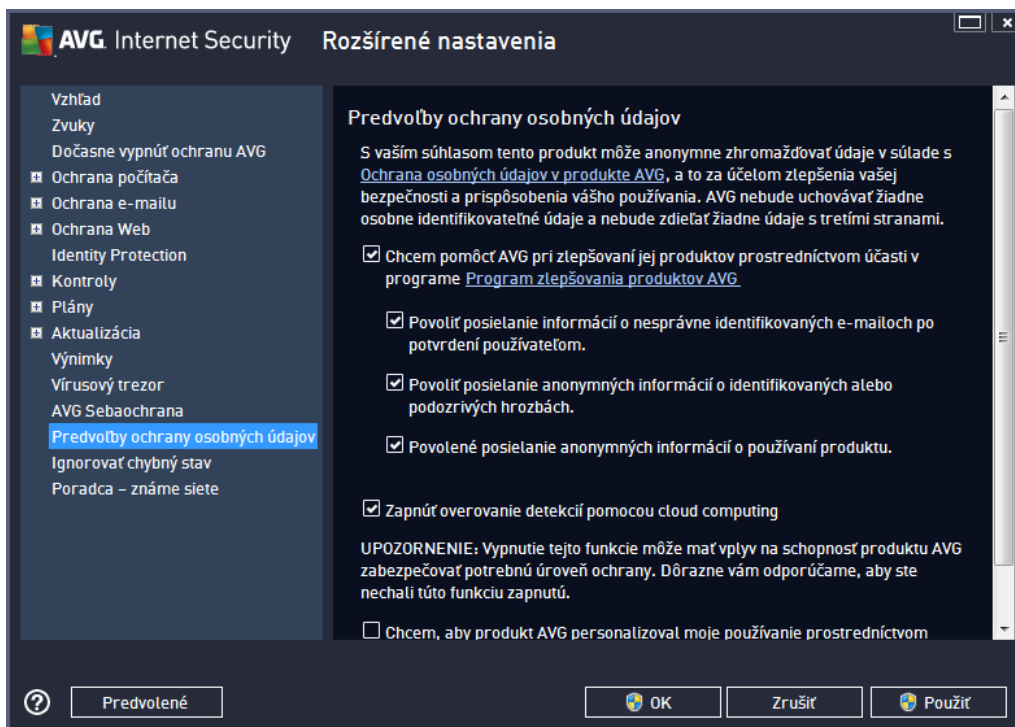


Funkcia **AVG Sebaochrana** umožňuje programu **AVG Internet Security 2013** chrániť svoje vlastné procesy, súbory, záznamy v registri a ovládať ich pred zmenou alebo deaktiváciou. Hlavným dôvodom pre tento druh ochrany je, že niektoré sofistikované hrozby sa snažia vypnúť antivírusovú ochranu a potom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

Odporujeme vám túto funkciu ponechať zapnutú!

9.14. Preferencie ochrany osobných údajov

Dialógové okno **Preferencie ochrany osobných údajov** vám ponúkne možnosť úasti 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 ústastníkov z celého sveta a umožňuje nám to zlepšovať ochranu pre každého jednotlivca. Hlásenia sa vykonávajú automaticky a preto vám nespôsobia žiadne nepohodlie. Hlásenia neobsahujú žiadne osobné údaje. Hlásenie zistených hrozieb je voliteľné, radi by sme vás ale požiadali o jeho zapnutie. Pomáha zlepšiť nielen vašu ochranu, ale aj ochranu ostatných používateľov aplikácie AVG.



V dialógovom okne sú k dispozícii tieto možnosti nastavenia:

- **Rád by som pomohol spoločnosti AVG zlepšovať ich produkty a chcem sa zúčastniť Programu zlepšovania produktov AVG (štandardne zapnuté)** – Ak nám chcete pomáhať v ďalšom zlepšovaní AVG Internet Security 2013, nechajte toto políčko zaškrtnuté. Táto funkcia zapne oznamovanie všetkých zaznamenaných hrozieb do spoločnosti AVG a umožní nám zhromažďovať najnovšie informácie o hrozbách od všetkých používateľov 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 používateľom (predvolene zapnuté)** – posiela informácie o e-mailových správach, ktoré boli nesprávne označené ako spam, alebo spamových správach, ktoré sú súčasťou Anti-Spam nedetegovala. Pred poslaním tohto druhu informácií vás program požiada o potvrdenie.
 - **Povolí posielanie anonymných informácií o identifikovaných alebo podozrivých hrozbách (predvolene zapnuté)** – posiela informácie o podozrivom alebo pozitívne nebezpečnom kóde alebo priebehu správania (môže ísť o vírus, spyware alebo škodlivé internetové stránky, ktoré sa pokúšate otvoriť) detegovanom na počítači.
 - **Umožníte zasielať nám anonymné údaje o používaní produktu (štandardne 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 computing (predvolene zapnuté)** – detegované hrozby sa budú overovať, či sú naozaj infikované, aby sa vylúčili nesprávne

detekcie.

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

Najbežnejšie hrozby

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

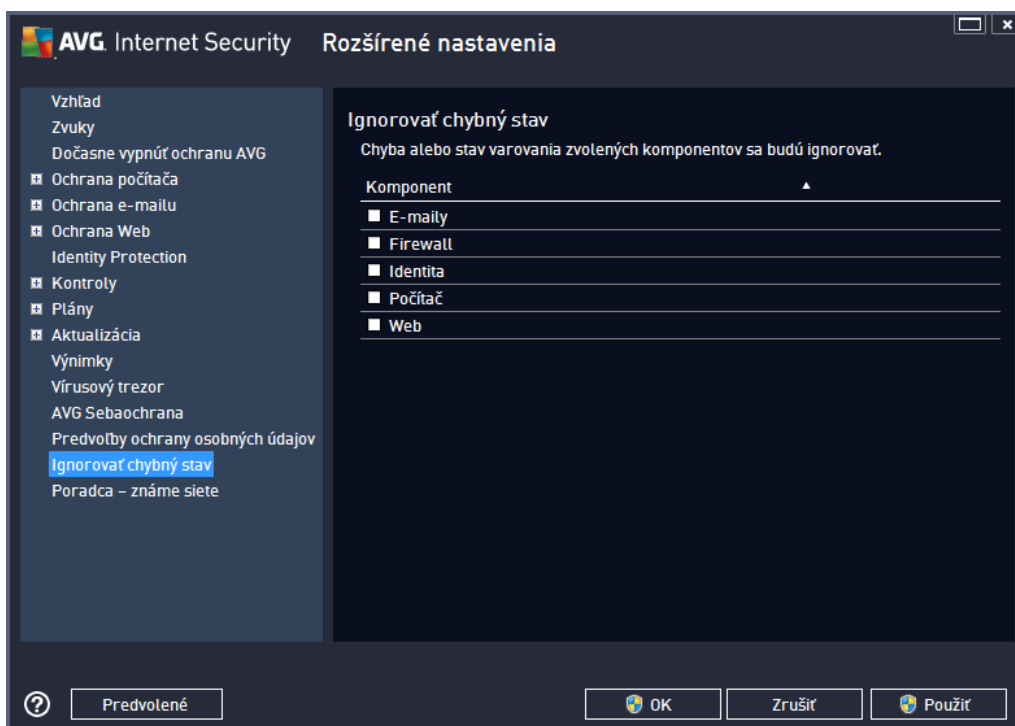
- **Vírus** je škodlivý kód, ktorý sa kopíruje a šíri často bez povšimnutia, kým nenapácha škody. Niektoré vírusy predstavujú vážnu hrozbu, ktorá dokáže vymazať alebo zámerne zmeniť súbory, zatiaľ čo iné vírusy sú zdanlivo neškodné, napríklad zahrajú melódiu. Všetky vírusy sú však nebezpečné, pretože sa dokážu množiť. Jeden jediný vírus dokáže v okamihu zaplniť celú pamäť počítača a spôsobiť jeho zlyhanie.
- **Worm** je podkategória vírusu, 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 preťažuje poštové servery a sieťové systémy
- **Spyware** sú zvyčajne sprievodné programy kategórie malware (*malware = každý škodlivý softvér, vrátane vírusov*), zvyčajne trójske kone, ktoré sa používajú na odcudzenie osobných informácií, hesiel, čísel kreditných kariet alebo na preniknutie do počítača a umožnenie útoku. Niekedy ovláda počítača na diaľku; všetko samozrejme bez vedomia a súhlasu vlastníka počítača.
- **Potenciálne nežiaduce programy** je taký typ spywaru, ktorý môže, ale nemusí byť nevyhnutne nebezpečný pre počítač. Špecifickým príkladom PNP je adware, t. j. softvér určený na šírenie reklám, zvyčajne zobrazovaním reklamných 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.
- **Zneužitie** je škodlivý kód, ktorý využíva trhlinu alebo zraniteľnosť operačného systému, internetového prehliadača alebo iného základného programu.
- **Phishing** je pokus o získanie citlivých osobných údajov predstieraným zastupovaním dôveryhodnej a všeobecne známej organizácie. Potenciálne obeť sú často kontaktované prostredníctvom hromadných e-mailov, v ktorých sa od nich požaduje napr. aby si aktualizovali informácie o bankových účtoch. Na tento účel majú kliknúť na uvedený odkaz, ktorý potom vedie na falošnú internetovú stránku banky.
- **Hoax** je hromadný e-mail, ktorý obsahuje nebezpečné, alarmujúce alebo jednoducho len otravné a 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 zneužitá na infikovanie počítača a návštevníkov.

V záujme ochrany pred všetkými druhmi hrozieb produkt AVG Internet Security 2013 obsahuje špecializované súčasti. Ich stručný opis nájdete v kapitole [Prehľad súčastí](#).

9.15. Ignorovať chybný stav

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



V predvolenom nastavení sa v tomto zozname nenachádza žiadna 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.

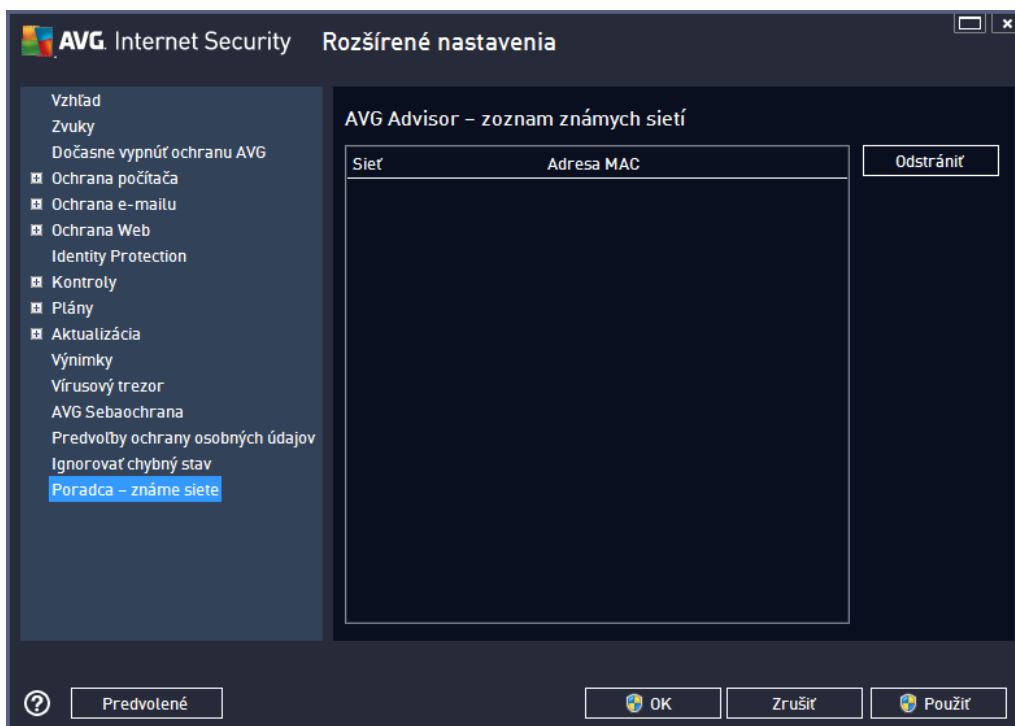
Môže nastať situácia, keď z nejakého dôvodu bude potrebné dočasne túto súčasti vypnúť. **To sa neodporúča, snažte sa mať neustále všetky súčasti zapnuté a v predvolenej konfigurácii.** Avšak niekedy sa takej situácii nemožno vyhnúť. V tom prípade ikona v paneli úloh automaticky oznámi chybový stav komponentu. 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. Nastavenia súčasti Firewall

Konfigurácia súčasti [Firewall](#) sa otvorí v novom okne, kde môžete vo viacerých dialógových oknách nastaviť všetky potrebné parametre komponentu. Konfigurácia súčasti Firewall sa otvorí v novom okne, kde môžete upraviť rozšírené parametre v niektorých konfiguračných dialógových oknách. Konfiguráciu možno zobraziť v základnom alebo v expertnom režime. Pri prvom otvorení konfiguračného okna sa otvorí základná verzia, ktorá ponúka úpravy týchto parametrov:

- [Všeobecné](#)
- [Aplikácie](#)
- [Zdieľanie súborov a tlačiarňí](#)

V dolnej časti okna sa nachádza tlačidlo **Expertný režim**. Stlačením tlačidla sa zobrazia v navigácii dialógového okna ďalšie položky, ktoré slúžia pre všetky potrebné konfigurácie súčasti Firewall:

- [Rozšírené nastavenia](#)
- [Zadefinované siete](#)
- [Systémové služby](#)
- [Protokoly](#)

Výrobca softvéru nastavil všetky súčasti produktu AVG Internet Security 2013 tak, aby dosahovali optimálny výkon. Nemajte predvolenú konfiguráciu, ak na to nemáte oprávnený dôvod. Vykonávanie zmien nastavení sa odporúča len skúseným používateľom.

10.1. Všeobecné

Dialógové okno **Všeobecné informácie** obsahuje prehľad všetkých dostupných režimov súčasti Firewall. Aktuálny výber režimu brány Firewall môžete zmeniť výberom iného režimu z ponuky.

Výrobca softvéru nastavil všetky súčasti produktu AVG Internet Security 2013 tak, aby dosahovali optimálny výkon. Nemajte predvolenú konfiguráciu, ak na to nemáte oprávnený dôvod. Vykonávanie zmien nastavení sa odporúča len skúseným používateľom.



Sú as Firewall vám umož uje zdefinova špecifické pravidlá zabezpe enia na základe toho, i sa váš po íta nachádza v doméne alebo i ide o samostatný po íta alebo dokonca notebook. Každá z týchto možností si vyžaduje inú úrove ochrany a jednotlivé úrovne patria do príslušných režimov. V krátkosti je režim sú asti Firewall špecifickou konfiguráciou komponentu Firewall a môžete použi nieko ko takýchto vopred definovaných konfigurácií:

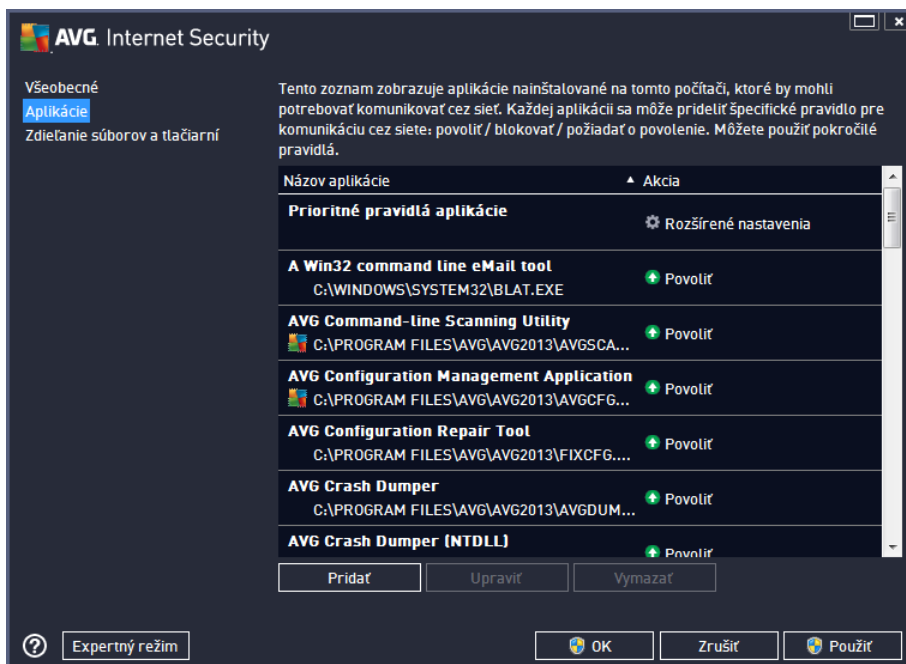
- **Automatický** – V tomto režime sú as Firewall automaticky spracúva celú prevádzku v sieti. Z vašej strany nebudú požadované žiadne rozhodnutia. Sú as Firewall umožní pripojenie všetkých známych aplikácií a sú asne s tým sa vytvorí pre aplikáciu pravidlo, ktoré ur í, i sa aplikácia môže v budúcnosti kedyko vek pripoji . Pre iné aplikácie sú as Firewall pod a správania aplikácie rozhodne, i sa má pripojenie povoli alebo zablokova . V takej situácii sa však pravidlo nevytvorí a aplikácia sa bude kontrolova pri každom opätovnom pokuse o pripojenie. **Automatický režim celkovo neruší a odporú a sa pre vā šinu používate ov.**
- **Interaktívny** – Tento režim je praktický, ak si želáte kontrolova všetky sie ové prenosy z a do vášho po íta a. Sú as Firewall ich bude sledova a upozorní vás na každý pokus o komunikáciu alebo prenos dát, ím vám umožní povoli alebo zablokova daný pokus, ako to uznáte za vhodné. Odporú a sa len pokro ílym používate om.
- **Blokova prístup na internet** – Internetové pripojenie bude úplne zablokované, nebudete ma prístup na internet a nikto zvonku nebude ma prístup do vášho po íta a. Len pre zvláštne a krátkodobé použitie.
- **Vypnú ochranu sú asti Firewall** – Vypnutím povolíte všetky sie ové prenosy z a do vášho po íta a. U iníte ho tak zranite ným vo í útokom hackerov. Vo bu tejto možnosti vždy starostlivo zväzte.

Všimnite si ešte špecifický automatický režim, ktorý je tiež sú as ou brány Firewall. Tento režim sa v tichosti aktivuje vtedy, ak sa sú asti [Po íta](#) alebo [Identity Protection](#) vypnú a po íta bude preto zranite nejší. V takých prípadoch sú as Firewall automaticky povolí pripojenie iba známym a úplne




bezpečným aplikáciám. Pri všetkých ostatných bude od vás vyžadované rozhodnutie. Cieľom je nahraď deaktivované služby ochrany a udržať počítač v bezpečí.

10.2. Aplikácie

Dialógové okno **Aplikácie** obsahuje zoznam všetkých aplikácií, ktoré sa dosiaľ pokúsili komunikovať cez sieť, a ikony pre priradenú akciu:



V **zozname aplikácií** sú uvedené aplikácie, ktoré sa v počítači našli (a ktorým boli priradené príslušné akcie). Môžete použiť tieto typy akcií:

-  – povolí komunikáciu vo všetkých sieťach
-  – zabráni komunikáciu
-  – rozšírené nastavenia definované

Všimnite si, že detegované môžu byť iba nainštalované aplikácie. V predvolenom nastavení, ak sa nová aplikácia pokúsi prvýkrát pripojiť v sieti, bezpečnostná brána firewall buď pre ňu automaticky vytvorí pravidlo pod dôveryhodnej databázy, alebo sa vás opýta, či chcete povoliť alebo blokovat komunikáciu. V druhom prípade budete môcť uložiť odpoveď ako trvalé pravidlo (ktoré sa potom zobrazí v tomto dialógovom okne).

Samozrejme, že pravidlá pre novú aplikáciu môžete definovať aj hneď: v tomto dialógovom okne stlačením tlačidla **Pridať** a vyplnením podrobností o aplikácii.

Okrem aplikácií sa v zozname nachádzajú aj dve špeciálne položky. **Prioritné pravidlá pre aplikácie** (v hornej časti zoznamu) majú prednosť a vždy sa použijú pred pravidlami jednotlivých aplikácií. **Ostatné pravidlá pre aplikácie** (v spodnej časti zoznamu) sa použijú ako „posledná možnosť“ v prípade, keď sa nepoužijú konkrétne pravidlá pre aplikácie, ako sú neznáme a nedefinované aplikácie. Vyberte akciu, ktorá sa má spustiť v prípade pokusu takejto aplikácie o

komunikáciu cez sieť : **Blokova** (komunikácia sa vždy zablokuje), **Povoli** (komunikácia sa povolí cez akúkoľvek sieť), **Spýta sa** (budete požiadaní o rozhodnutie, či danú komunikáciu povoliť alebo blokovať). **Tieto položky majú iné možnosti nastavenia než bežné aplikácie a sú určené len pre skúsených používateľov. Odporúčame vám, aby ste nemenili tieto nastavenia!**

Ovládacie tlačidlá

Na vykonanie zmien v zozname sa používajú tieto ovládacie tlačidlá:

- **Prida** – Otvorí prázdne dialógové okno na definovanie nových pravidiel pre aplikácie.
- **Upravi** – Otvorí to isté dialógové okno, ktoré sa používa na zmenu existujúcej skupiny pravidiel pre aplikácie.
- **Vymaza** – Odstráni zvolenú aplikáciu zo zoznamu.

10.3. Zdieľanie súborov a tlačiarňí

Zdieľanie súborov a tlačiarňí v podstate znamená zdieľanie akýchkoľvek súborov alebo priežinkov, ktoré ste označili v systéme Windows ako „Zdieľané“, spoločných diskových jednotiek, tlačiarňí, skenerov a všetkých podobných zariadení. Zdieľanie takýchto položiek je želané len v rámci sietí, ktoré môžu byť považované za bezpečné (napríklad v domácnosti, v práci a v škole). Keď ste však pripojení vo verejnej sieti (ako napríklad Wi-Fi sieť na letisku alebo v internetovej kaviarni), nemusíte si želať zdieľania. Súčasťou AVG Firewall môže jednoducho blokovať alebo povoliť zdieľanie a umožní vám uložiť si svoju voľbu pre už navštívené siete.

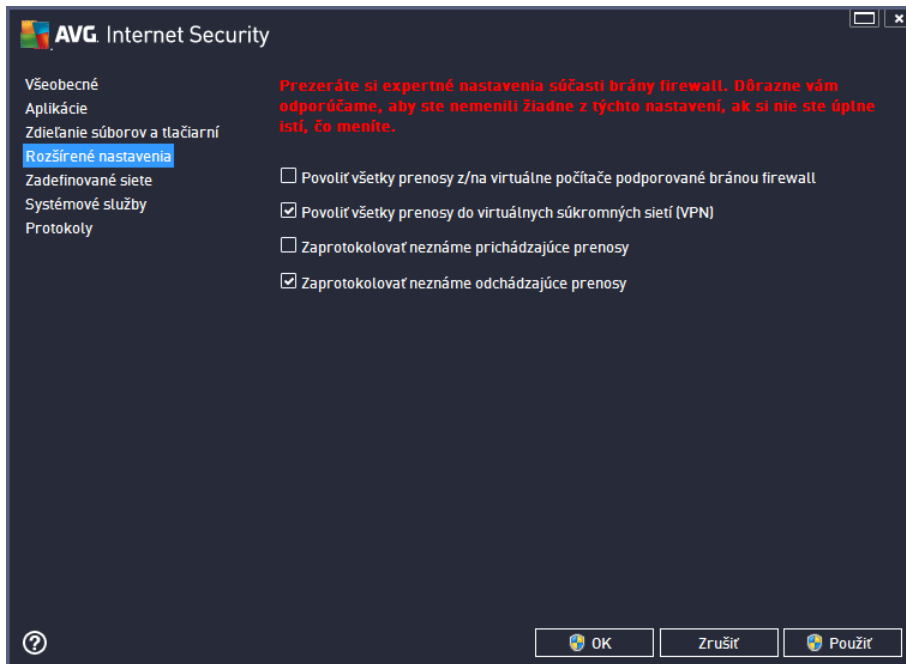


V dialógovom okne **Zdieľanie súborov a tlačiarňí** môžete upraviť konfiguráciu zdieľania súborov a tlačiarňí a aktuálne pripojených sietí. V systéme Windows XP názov siete zodpovedá označeniu, ktoré ste predtým vybrali pri prvom pripojení k nej. V systéme Windows Vista a vyššie sa názov siete

berie automaticky z centra sietí.

10.4. Rozšírené nastavenia

Akékoľvek úpravy v dialógovom okne Rozšírené nastavenia sú určené IBA PRE SKÚSENÝCH POUŽÍVATEĽOV!

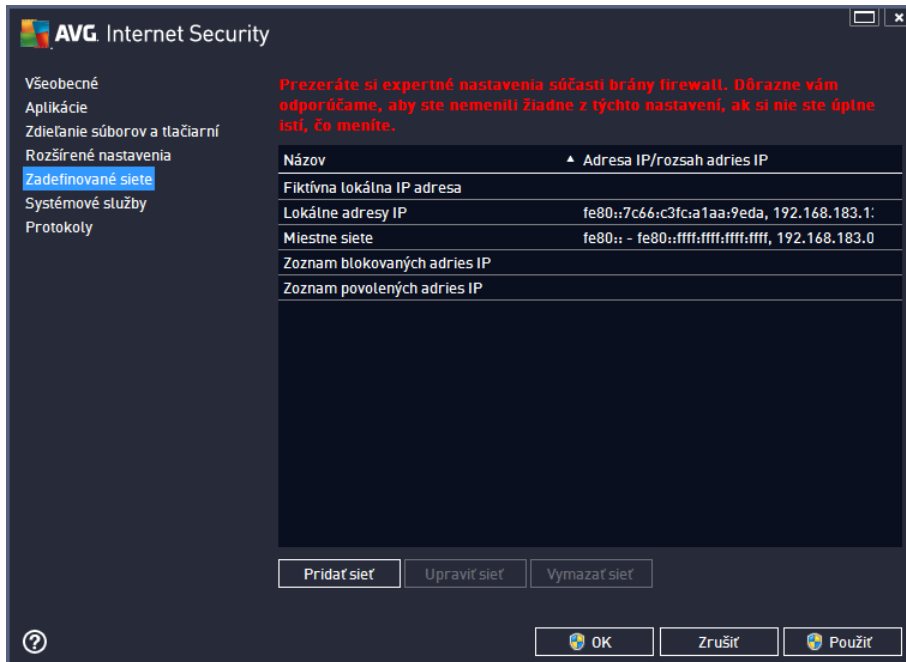


Dialógové okno **Rozšírené nastavenia** vám umožní zapnúť /vypnúť nasledovné parametre brány Firewall:

- **Povoliť všetky prenosy z/na virtuálne počítače podporované bránou firewall** – podpora sieťových pripojení na virtuálnych počítačoch, ako napríklad VMWare.
- **Povoliť všetky prenosy do virtuálnych súkromných sietí** – podpora pripojení VPN (používa sa na pripájanie k vzdialeným počítačom).
- **Zaprotokolovať neznáme prichádzajúce/odchádzajúce prenosy** – všetky pokusy o komunikáciu (prichádzajúce/odchádzajúce) od neznámych aplikácií budú zaznamenané v [Protokole súčasti Firewall](#).

10.5. Zadefinované siete

Akékoľvek úpravy v dialógovom okne Zadefinované siete sú určené IBA PRE SKÚSENÝCH POUŽÍVATEĽOV!

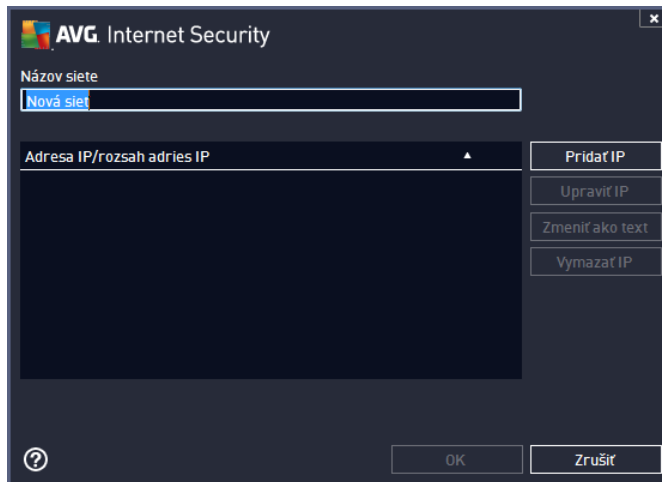


V dialógovom okne **Zadefinované siete** sa nachádza zoznam všetkých sietí, ku ktorým je váš počítač pripojený. V zozname sú uvedené nasledujúce informácie o každej zistenej sieti:

- **Siete** – Obsahuje zoznam názvov všetkých sietí, ku ktorým je počítač pripojený.
- **Rozsah IP adresy** – Každá sieť sa automaticky deteguje a uvedie sa vo forme rozsahu IP adresy.

Ovládacie tlačidlá

- **Pridať sieť** – Otvorí nové dialógové okno, kde môžete upraviť parametre novodefinovanej siete, t. j. zadať **názov siete** a **rozsah adresy IP**:





- **Upravi sie** – Otvorí dialógové okno **Vlastnosti siete** (pozrite sa vyššie), kde môžete upravi parametre zadefinovanej siete (toto dialógové okno je rovnaké ako dialógové okno pre pridanie novej siete, pozrite si popis v predchádzajúcom odseku).
- **Vymaza sie** – Odstráni odkaz na zvolenú sieť zo zoznamu sietí.

10.6. Systémové služby

Zmeny v dialógovom okne Systémové služby a protokoly odporúame LEN SKÚSENÝM POUŽÍVATEĽOM!



V dialógovom okne **Systémové služby a protokoly** sa nachádza zoznam štandardných systémových služieb a protokolov operačného systému Windows, ktoré sa môžu pokúšať komunikovať v sieti. Tabuľka má nasledujúce stĺpce:

- **Systemová služba a protokoly** – V tomto stpci je uvedený názov príslušnej systémovej služby.
- **Akcia** – V tomto stpci sa nachádza ikona pridelenej akcie:
 -  Umožni komunikáciu pre všetky siete
 -  Uzamknú komunikáciu

Ak chcete upravi nastavenia položky v zozname (*vrátane pridelených akcií*), kliknite pravým tlačidlom myši na položku a vyberte možnosť **Upravi**. **Úpravu systémových pravidiel by však mali robi len skúsení používatelia; odporú ame vám, aby ste nemenili systémové pravidlá!**

Používate om definované systémové pravidlá

Ak chcete otvori nové dialógové okno na definovanie vlastného pravidla pre systémovú službu (*pozri obrázok nižšie*), stla te tlačidlo **Správa používateľských systémových pravidiel**. Rovnaké dialógové okno sa otvorí aj vtedy, ak sa rozhodnete upravi konfiguráciu niektorej z existujúcich položiek v zozname systémových služieb a protokolov. V hornej ásti tohto dialógového okna sa nachádza prehľad všetkých podrobností o práve editovanom systémovej pravidle, v dolnej ásti sa nachádzajú zvolené informácie. Príslušným tlačidlom môžete podrobnosti o pravidle upravi , prida alebo vymaza :



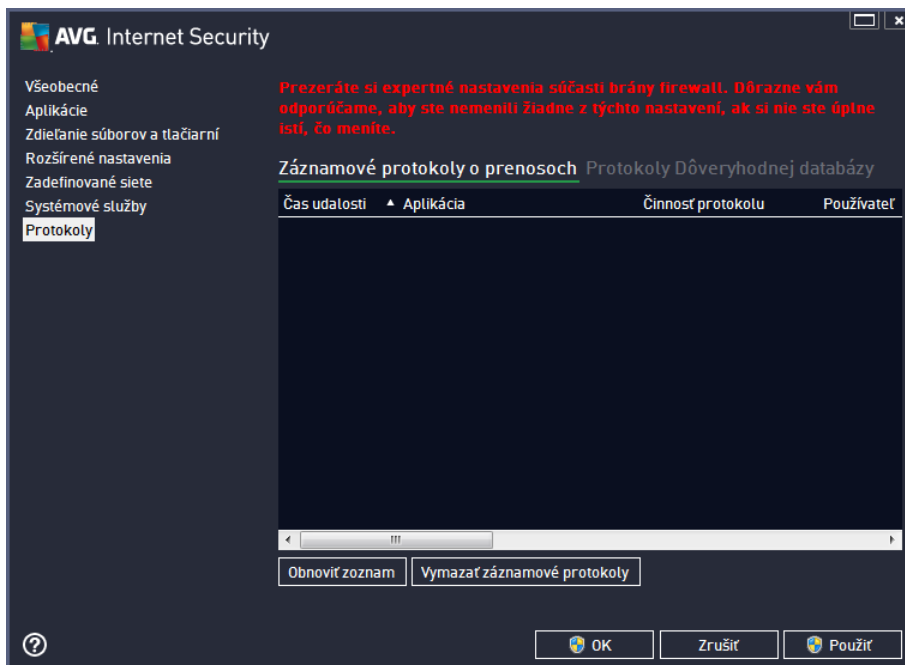
Nezabudnite, že podrobné nastavenie pravidiel je pokročilá funkcia určená najmä pre správcov siete, ktorí potrebujú mať úplnú kontrolu nad konfiguráciou súčasti Firewall. Ak nie ste oboznámení s typmi komunikačných protokolov, súčasti sieťových portov, definíciami adres IP a pod., neme te tieto nastavenia! Ak naozaj potrebujete zmeniť konfiguráciu, postupujte pod a pokynov v príslušných súboroch pomocníka.

10.7. Protokoly

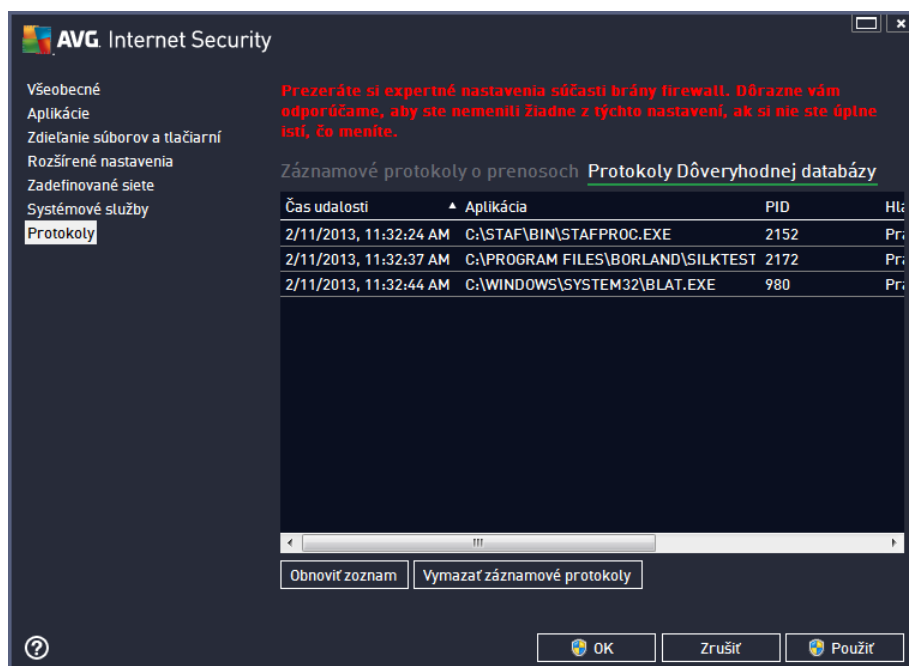
Akékoľvek úpravy v dialógovom okne Protokoly sú určené IBA PRE SKÚSENÝCH POUŽÍVATEĽOV!

Dialógové okno **Protokoly** vám umožňuje skontrolovať zoznam všetkých zaprotokolovaných činností a udalostí súčasti Firewall s podrobným popisom príslušných parametrov zobrazenom na dvoch kartách:

- **Záznamové protokoly o prenosoch** – Na tejto záložke nájdete informácie o aktivitách všetkých aplikácií, ktoré sa pokúsili pripojiť do siete. Pre každú položku tu sú uvedené údaje o čase udalosti, názve aplikácie, príslušnej protokolovanej činnosti, používateľskom názve, PID, smere prenosu, type protokolu, portoch vzdialených a miestnych a miestnych a vzdialených adresách IP.



- **Protokoly Dôveryhodnej databázy** – Dôveryhodná databáza je interná databáza spoločnosti AVG, ktorá zhromažďuje informácie o certifikovaných a dôveryhodných aplikáciách, ktorým sa môže vždy povoliť komunikácia on-line. Pri prvom pokuse novej aplikácie o pripojenie do siete (t. j. ak doposiaľ nebolo vytvorené pravidlo pre bezpečnostnú bránu firewall súvisiace s touto aplikáciou) je potrebné zistiť, či sa má povoliť sieťová komunikácia príslušnej aplikácie. AVG najskôr nahliadne do Dôveryhodnej databázy a ak je v nej aplikácia uvedená, potom sa jej automaticky povolí prístup k sieti. Až potom, a pod podmienkou, že sa v databáze nenachádzajú informácie o tejto aplikácii, sa zobrazí dialógové okno, v ktorom sa vás program opýta, či chcete povoliť aplikácii prístup k sieti.



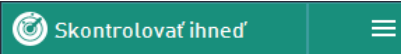
Ovládacie tlačidlá

- **Obnovi zoznam** – všetky zaznamenané parametre sa dajú usporiadať podľa vybraného atribútu: chronologicky (*dátumy*) alebo abecedne (*ostatné stĺpce*) – stačí kliknúť na hlavičku príslušného stĺpca. Použijete tlačidlo **Obnovi zoznam** na aktualizovanie práve zobrazených informácií.
- **Vymazať záznamové protokoly** – Stlačením odstránite všetky položky v tabuľke.

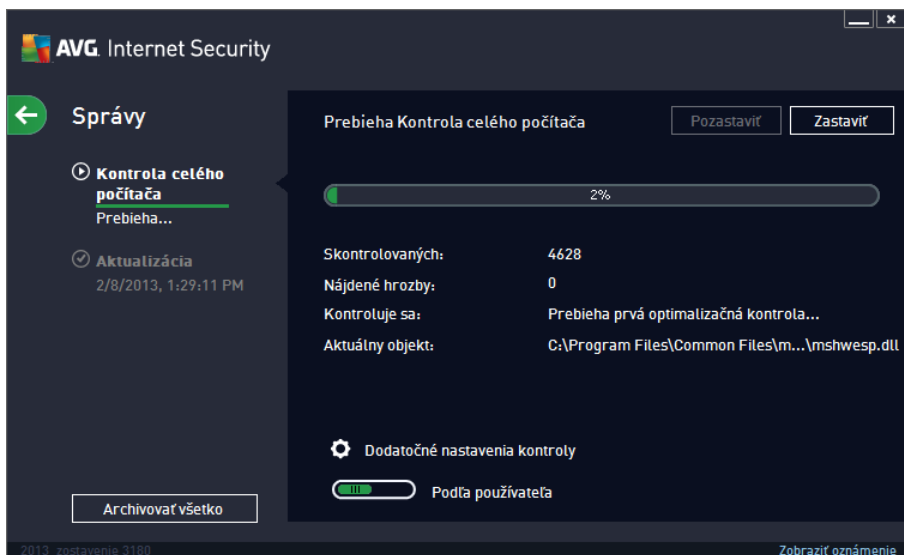
11. Kontrola programom AVG

V predvolenom nastavení aplikácia **AVG Internet Security 2013** 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 Internet Security 2013**, ktoré sú vždy na stráži a nedovolia žiadnemu škodlivému kódu preniknúť do počítača. Samozrejme, že môžete [naplánovať kontrolu](#), ktorá sa bude spúšťať v pravidelných intervaloch, alebo manuálne kedykoľvek spustíte kontrolu podľa vlastných potrieb.

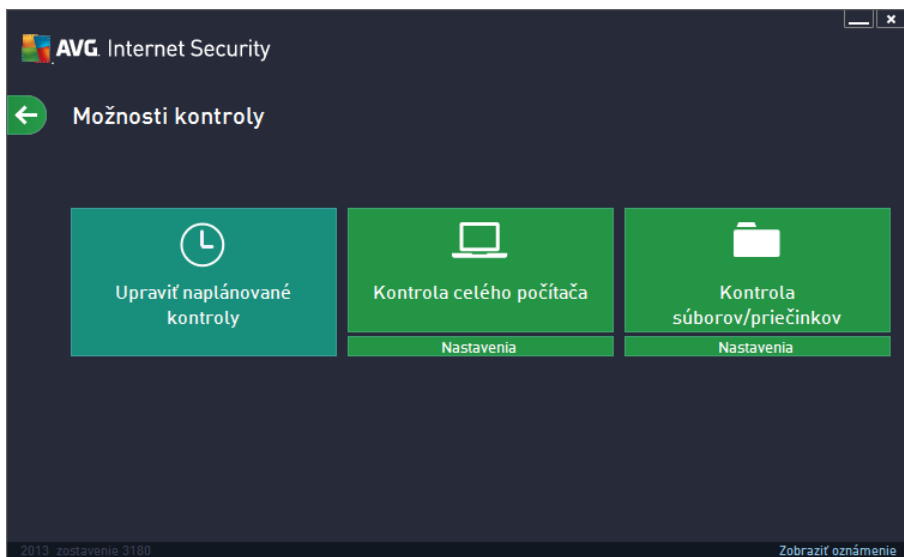
K rozhraniu kontroly programu AVG máte prístup [z hlavného používateľského rozhrania](#)

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 tabuľke iba jeden plán kontroly, ktorý vopred definoval dodávateľ softvéru. Táto kontrola je štandardne vypnutá. Ak ju chcete zapnúť, kliknite na tlačidlo na pravom okraji a v kontextovej ponuke vyberte možnosť *Povoliť úlohu*. Po povolení plánu kontroly môžete [upraviť jej konfiguráciu](#) tlačidlom *Upraviť plán kontroly*. Taktiež môžete kliknúť na možnosť *Pridať plán kontroly*, aby ste vytvorili nový plán.
- **Kontrola celého počítača/Nastavenia** – Tlačidlo je rozdelené na dve časti. Kliknutím na položku *Kontrola celého počítača* okamžite spustíte kontrolu celého počítača (*podrobnosti o kontrole celého počítača nájdete v príslušnej kapitole s názvom [Vopred definované kontroly/Kontrola celého počítača](#)*). Kliknutím na spodnú časť *Nastavenia* sa zobrazí konfiguračné okno, kde môžete [nastaviť parametre kontroly celého počítača](#).
- **Kontrola súborov/priečinkov/Nastavenia** – Tlačidlo je opäť rozdelené na dve časti. Kliknutím na možnosť *Kontrola súborov/priečinkov* okamžite spustíte kontrolu vybraných oblastí počítača (*podrobnosti o kontrole súborov a priečinkov nájdete v príslušnej kapitole s názvom [Vopred definované kontroly/Kontrola súborov/priečinkov](#)*). Kliknutím na spodnú časť *Nastavenia* sa zobrazí konfiguračné okno, kde môžete [nastaviť parametre kontroly súborov/priečinkov](#).

11.1. Vopred definované kontroly

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

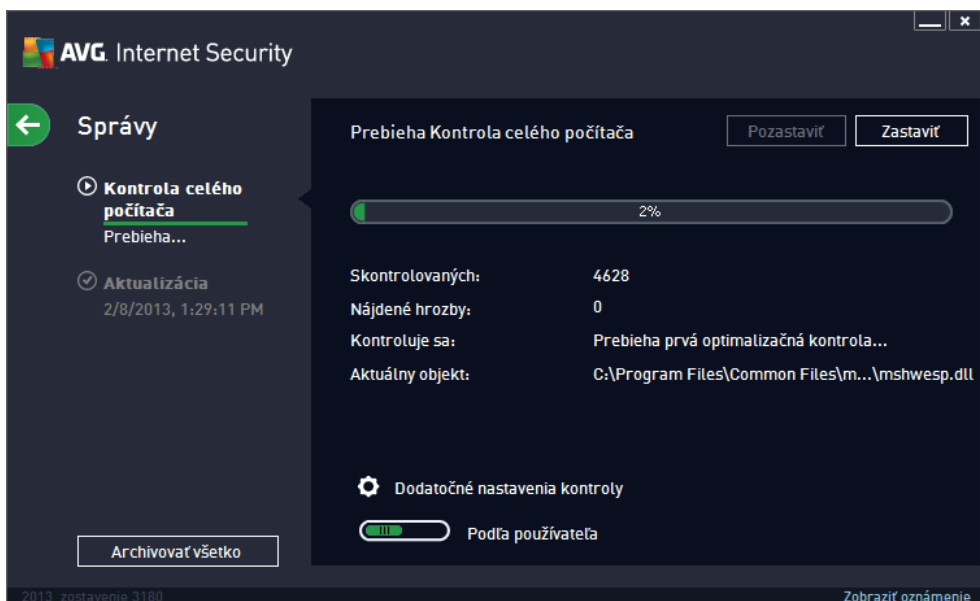
V produkte **AVG Internet Security 2013** sa nachádzajú tieto typy kontrol vopred definované dodávateľom softvéru:

11.1.1. Kontrola celého počítača

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

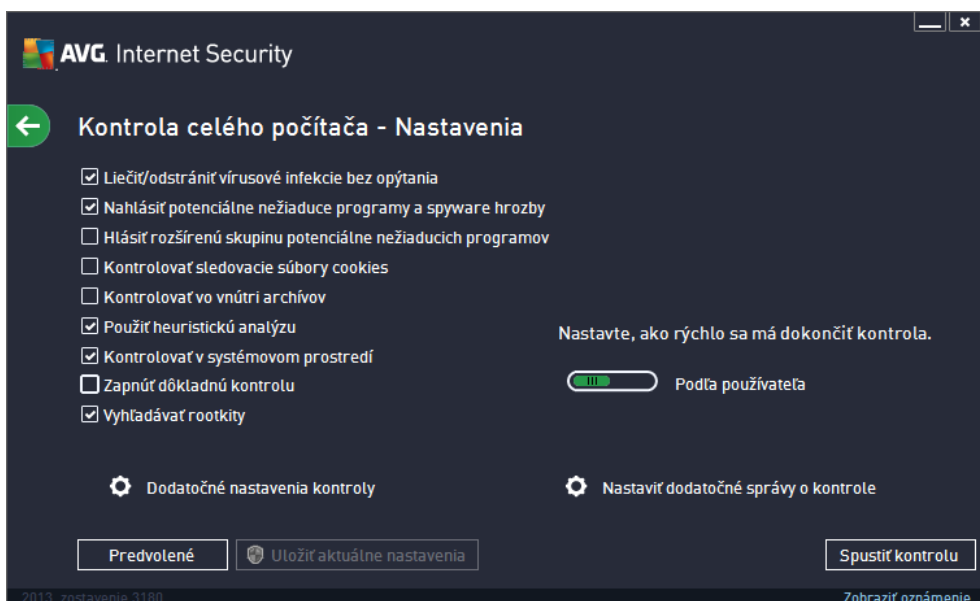
Spustenie kontroly

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



Zmena konfigurácie kontroly

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

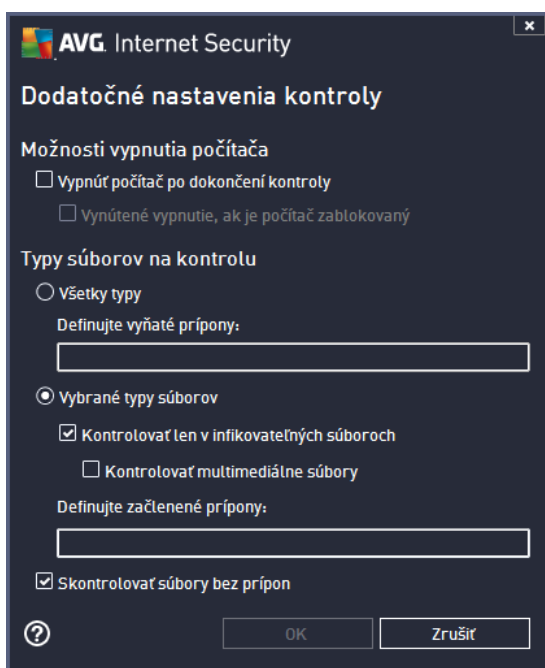


V zozname parametrov kontroly môžete zapnúť /vypnúť špecifické parametre podľa potreby:

- **Liečiť /odstrániť vírusovú infekciu bez opýtania** (štandardne zapnuté) – Ak sa počas kontroly nájde vírus, môže byť automaticky vyladený, pokiaľ je liek k dispozícii. Ak nie je možné infikovaný súbor vyladiť automaticky, presunie sa do [Vírusového trezora](#).
- **Nahlásiť potenciálne nežiaduce programy a spyware hrozby** (štandardne zapnuté) – Začiarknite toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu škodlivého softvéru: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
- **Hlásiť rozšírenú skupinu potenciálne nežiaducich programov** (štandardne vypnuté) – Začiarknite toto políčko, ak sa má detegovať rozšírená skupina spywaru: programov, ktoré sú úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpečenia počítača, ale môže 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.
- **Kontrola v systémovom prostredí** (štandardne zapnuté) – Počas kontroly sa budú

kontrolovať aj systémové oblasti počítača.

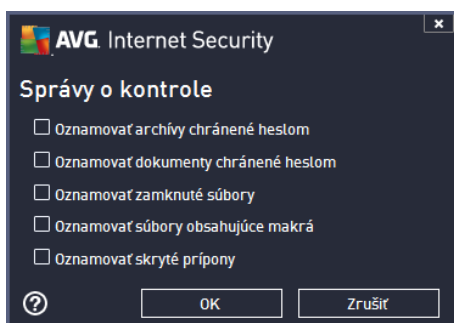
- **Zapnúť dôkladnú kontrolu (štandardne vypnuté)** – V určitých situáciách (podozrenie na infikovanie počítača) môžete touto možnosťou aktivovať najdôkladnejšie kontrolné algoritmy, ktoré pre istotu skontrolujú aj tie oblasti počítača, ktoré sa obyčajne vôbec neinfikujú. Upozorujeme však, že tento spôsob je náročný na čas.
- **Dodatkové nastavenia kontroly:** Tento odkaz otvorí nové dialógové okno Dodatkové nastavenia kontroly, ktoré sa používa na nastavenie nasledujúcich parametrov:



- **Možnosť 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 iarkou 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 časť prehľadovania skrátí ešte viac, pretože tieto súbory sú často veľa väčšie, pričom pravdepodobnosť napadnutia vírusom je oveľa nižšia*). 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. Súborý 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 pomalšie, ale nezaujíma vás, ako dlho bude prehadzovanie trvať*) alebo rýchlejšie s vyššími nárokmi na využívanie systémových zdrojov (*napríklad keď sa pracuje s veľkým množstvom dát*).
- **Vytvoriť ďalšie správy o kontrole** – Odkaz otvorí nové dialógové okno **Správy o kontrole**, v ktorom môžete určiť, aké typy možných nálezov sa majú uviesť v správach:



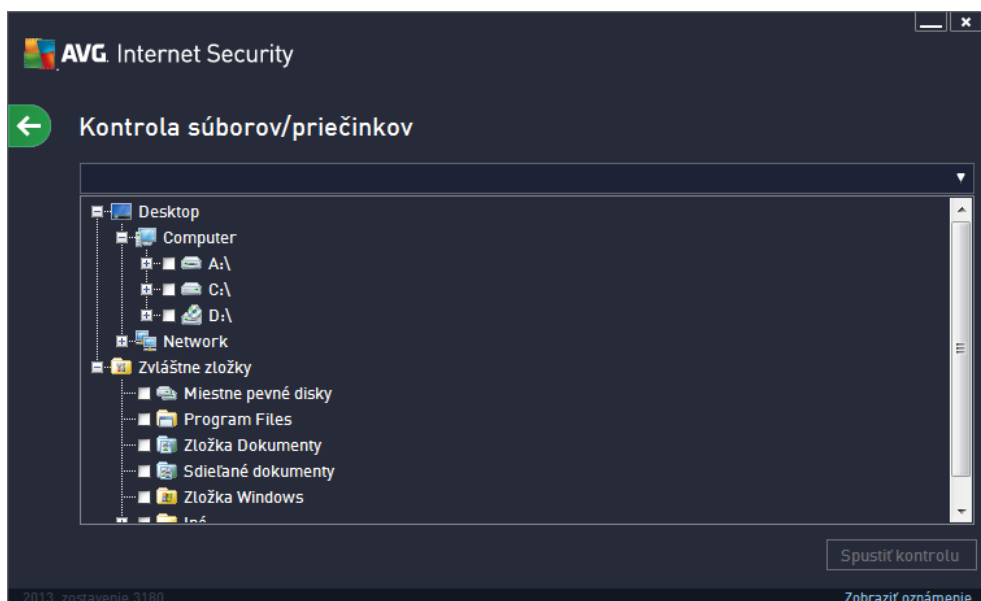
Upozornenie: Tieto nastavenia kontroly sa zhodujú s parametrami novodefinovanej kontroly; pozrite informácie v kapitole [Kontrola programom AVG/Plánovanie kontroly/Ako kontrolovať](#). Ak sa rozhodnete zmeniť predvolenú konfiguráciu funkcie **Kontrola celého počítača**, svoje nové nastavenie môžete uložiť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

11.1.2. 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.

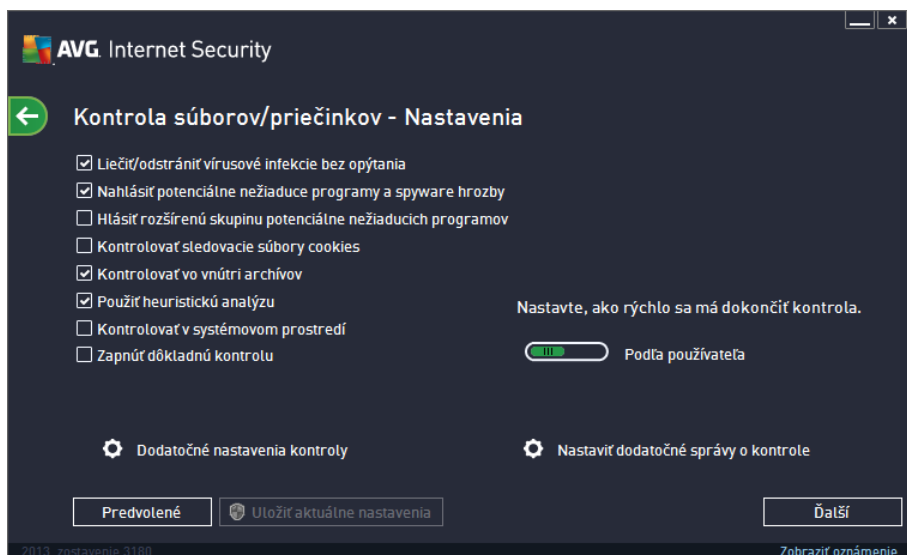
Spustenie kontroly

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 prehadzovanie konkrétneho priečinka, ktorého vnorené priečinky sa vylúčia z tohto prehadzovania; v tom prípade vložte znak mínus „-“ pred automaticky vygenerovanú cestu (*pozrite snímku obrazovky*). Na vylúčenie celého priečinka z kontroly použijete parameter „!“. Nakoniec, ak chcete spustiť kontrolu, stlačte tlačidlo **Spustiť kontrolu**; samotný proces kontrolovania sa v podstate zhoduje s [kontrolou celého počítača](#).



Zmena konfigurácie kontroly

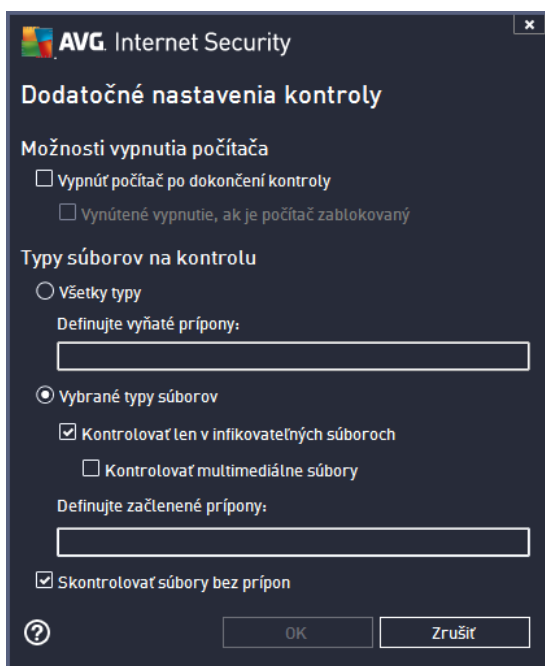
Konfiguráciu **Kontroly súborov/priečinkov** môžete upraviť v dialógovom okne **Kontrola súborov/priečinkov – Nastavenia** (okno zobrazíte odkazom **Nastavenia** v časti **Kontrola súborov/priečinkov** v okne **Možnosti kontroly**). **Odporúčame ponechať predvolené nastavenia, ak nemáte závažný dôvod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



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

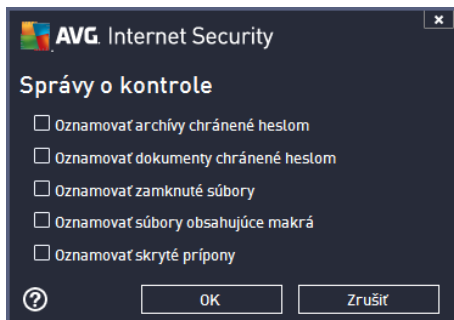
- **Liečenie/odstránenie vírusovej infekcie bez opýtania (štandardne zapnuté):** Ak sa počas kontroly zistí prítomnosť vírusu, môže sa automaticky vylíčiť, ak je k dispozícii liečba. Ak nie je možné infikovaný súbor vylíčiť automaticky, premiestni sa do [Vírusového trezora](#).

- **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 škodlivého softvéru: 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 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 zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpečenia počítača, 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 používateľoch, akými sú napr. preferencie stránok alebo obsah elektronických nákupných košíkov*).
- **Kontrolova vo vnútri archívov** (štandardne zapnuté): Tento parameter určuje, 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 počítačovom prostredí*) bude jedna z metód, ktoré sa použijú na detekciu vírusov počas kontroly.
- **Kontrolova v systémovej oblasti** (štandardne vypnuté): Počas kontroly sa budú overova aj systémovej oblasti počítača.
- **Zapnú dôkladnú kontrolu** (štandardne vypnuté): V určitých situáciách (*podозrenie na infikovanie počítača*) môžete touto možnosťou aktivova najdôkladnejšie kontrolné algoritmy, ktoré pre istotu skontrolujú aj tie oblasti počítača, ktoré sa oby ajne vôbec neinfikujú. Upozorujeme však, že tento spôsob je náročný na čas.
- **Dodatné nastavenia kontroly** – Tento 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 s iarkou 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 veľa väčšie, pričom pravdepodobnosť napadnutia vírusom je veľmi malá*). Znova môžete definovať prípony, pod ktorými sa majú kontrolovať súbory.
 - 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*).

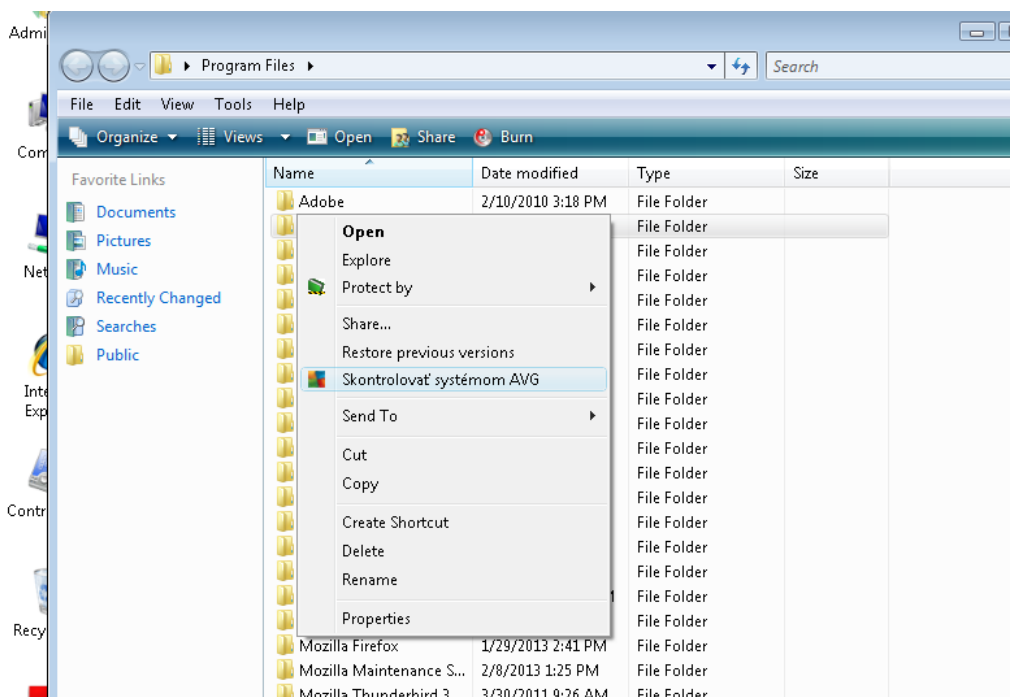
- **Vytvoriť ďalšie správy o prehľadovaní** – Odkaz otvorí nové dialógové okno **Správy o prehľadovaní**, ktoré vám umožní nastaviť, ktoré typy možných nálezov sa majú hlásiť:



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

11.2. Kontrola z prieskumníka

Okrem vopred definovaných kontrol spustených pre celý počítač alebo jeho vybrané oblasti, **AVG Internet Security 2013** zároveň umožňuje rýchlo kontrolovať 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 označíte súbor (alebo prieinok), ktorý chcete skontrolovať.



- Kliknutím pravým tlačidlom myši na objekt otvorte kontextovú ponuku.
- Výberom možnosti **Skontrolovať programom AVG** skontrolujete súbor programom **AVG Internet Security 2013**

11.3. Kontrola z príkazového riadka

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

Pre spustenie kontroly AVG z príkazového riadka spustíte nasledovný príkaz v priežinke, 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 lomkou, napríklad:
avgscanx /scan=C:\;D:

Parametre kontroly

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

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

Kontrola z príkazového riadka spustená z grafického rozhrania

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

kontroly len pomocou praktického grafického rozhrania.

Ke že 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.

11.3.1. Parametre kontroly z príkazového riadka

Nasleduje zoznam všetkých dostupných parametrov pre kontrolu z príkazového riadka:

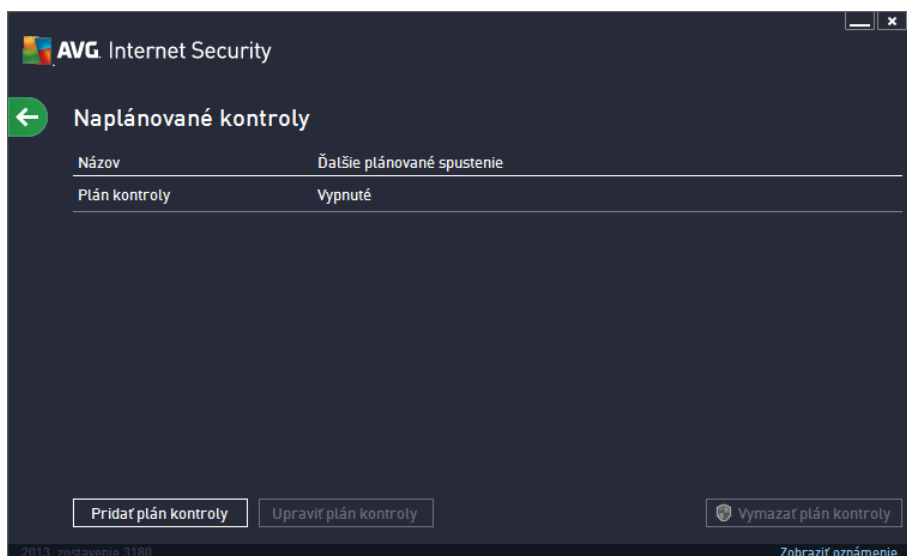
- /SCAN [Kontrola súborov/prie inkov](#) /SCAN=path;path (napr. /SCAN=C:\;D:\)
- /COMP [Kontrola celého po íta a](#)
- /HEUR Použi heuristickú analýzu
- /EXCLUDE Cesty alebo súbory, ktoré sa majú vy a z kontroly
- /@ Súbor s príkazmi /názov súboru/
- /EXT Kontrolova tieto prípony /napríklad EXT=EXE, DLL/
- /NOEXT Nekontrolova tieto prípony /napríklad NOEXT=JPG/
- /ARC Kontrolova archívy
- /CLEAN Automaticky vy isti
- /TRASH Presunú infikované súbory do [Vírusového trezora](#)
- /QT Rýchly test
- /LOG Generova súbor s výsledkami kontroly
- /MACROW Hlási makrá
- /PWDW Hlási súbory chránené heslom
- /ARCBOMBSW Hlási opakovane komprimované archívne súbory
- /IGNLOCKED Ignorova zamknuté súbory
- /REPORT Hlási do súboru /názov súboru/
- /REPAPPEND Pripoji k súboru s hlásením
- /REPOK Hlási neinfikované súbory so zna kou OK
- /NOBREAK Nepovoli prerušenie klávesmi CTRL-BREAK
- /BOOT Povolí kontrolu MBR/BOOT
- /PROC Kontrolova aktívne procesy

- /PUP Hlásí potenciálne nežiaduce programy
- /PUPEXT Hlásí rozšírenú skupinu potenciálne nežiaducich programov
- /REG Kontrolova v registroch
- /COO Kontrolova súbory cookies
- /? Zobrazí pomocníka pre túto tému
- /HELP Zobrazí pomocníka pre túto tému
- /PRIORITY Nastaví 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 Kontrolova alternatívne dátové prúdy (*len pre NTFS*)
- /HIDDEN Hlásí súbory so skrytými príponami
- /INFECTABLEONLY Kontrolova len súbory s infikovanými príponami
- /THOROUGHSCAN Zapnú dôkladnú kontrolu
- /CLOUDCHECK Kontrola nesprávnych pozitívnych detekcií
- /ARCBOMBSW Hlásí opakovane komprimované archívne súbory

11.4. Plánovanie kontroly

S aplikáciou **AVG Internet Security 2013** môžete spustiť kontrolu na požiadanie (*napríklad ke 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 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 zobrazíť prehľad všetkých naplánovaných kontrol:

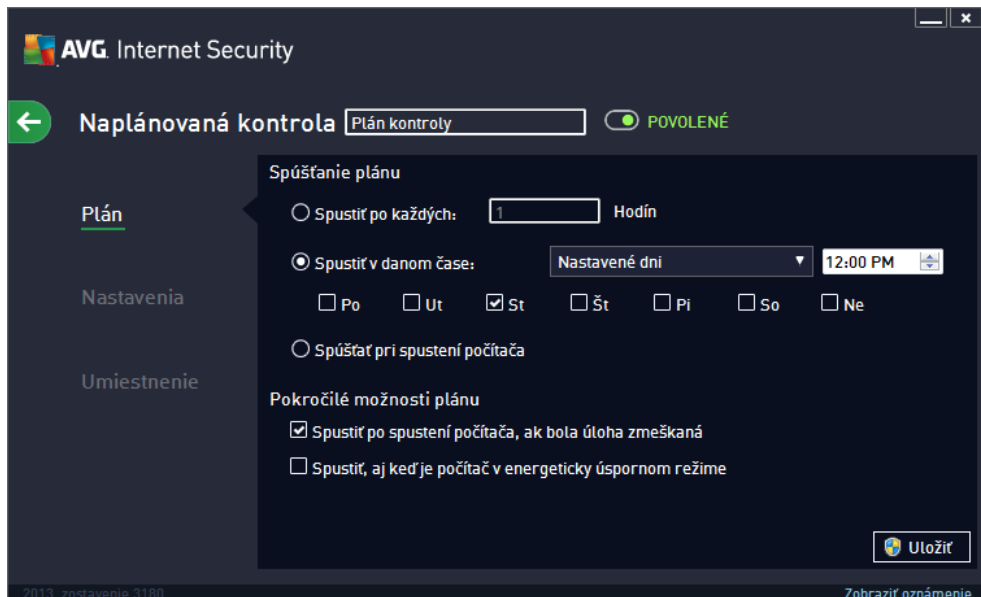


Než zadefinujete vlastné kontroly, zobrazí sa v tabu ke iba jeden plán kontroly, ktorý vopred definoval dodávateľ softvéru. Táto kontrola je štandardne vypnutá. Ak ju chcete zapnúť, kliknite na tlačidlo u pravom tlačídlom a v kontextovej ponuke vyberte možnosť **Povoliť úlohu**. Po povolení plánu kontroly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

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

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

11.4.1. Plán



V hornej časti záložky **Plán** sa nachádza textové pole, do ktorého môžete zadať názov modulu kontroly, ktorý sa aktuálne definuje. Pokúste sa použiť stručné, opisné a výstižné názvy pre kontroly, aby sa dali neskôr ľahšie navzájom 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.


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

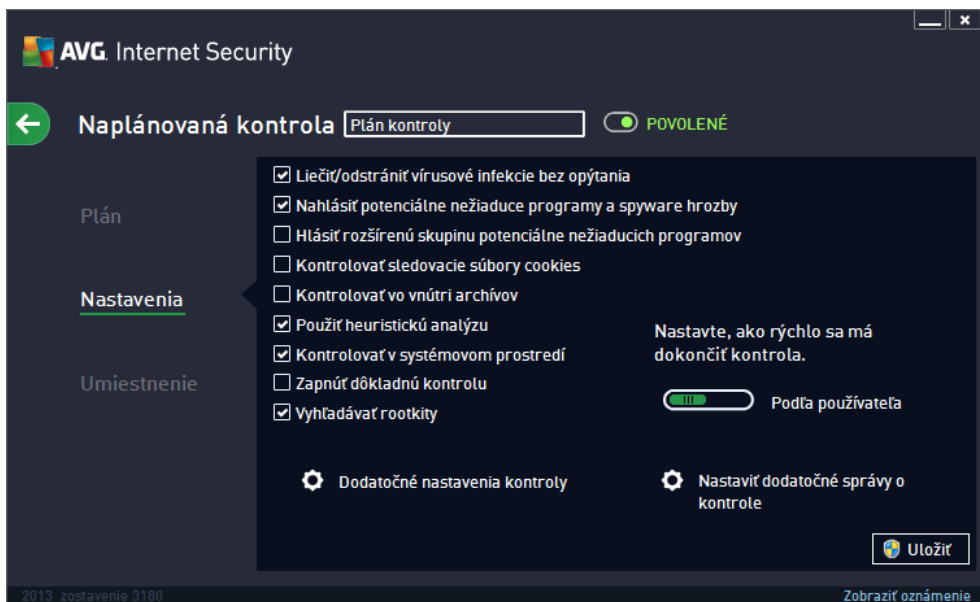
Ovládacie prvky dialógového okna

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

parametrov až po zadaní všetkých svojich požiadaviek.

-  – Zelenou šípkou v avej hornej časti okna sa dostanete naspäť do prehľadu [Naplánovaných kontrol](#).

11.4.2. Nastavenia



V hornej časti záložky **Nastavenia** sa nachádza textové pole, do ktorého môžete zadať názov modulu kontroly, ktorý sa aktuálne definuje. Pokúste sa použiť stručné, opisné a výstižné názvy pre kontroly, aby sa dali neskôr ľahšie navzájom 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.**

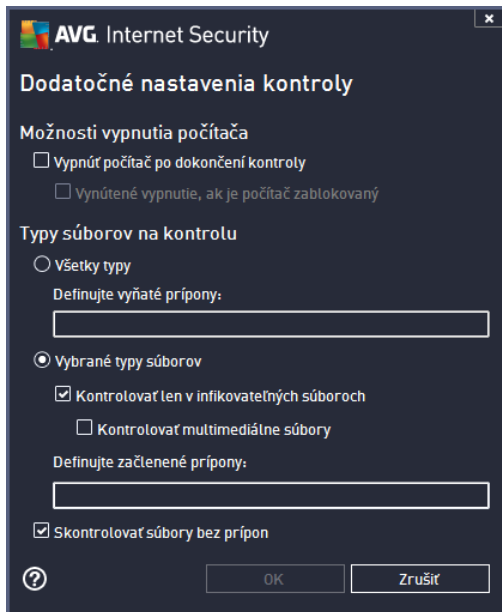
- **Liečiť / odstrániť vírusovú infekciu bez opýtania (štandardne zapnuté):** ak sa počas kontroly nájde vírus, môže byť automaticky vyladený, pokiaľ je liek k dispozícii. Ak nie je možné infikovaný súbor vyladiť automaticky, premiestni sa do [Vírusového trezora](#).
- **Nahlásiť potenciálne nežiaduce programy a spyware hrozby (štandardne zapnuté):** Začiarknite toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu škodlivého softvéru: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporujeme vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
- **Hlásiť rozšírenú skupinu potenciálne nežiaducich programov (štandardne vypnuté):** Začiarknite toto políčko, ak sa má detegovať rozšírená skupina spywaru: programov, ktoré sú úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň

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

- **Kontrola sledovacích súborov cookies** (štandardne vypnuté): Tento parameter súčasti zapína funkciu na detekciu súborov cookies počas prechádzania; (*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 vnútri archívov** (štandardne vypnuté): tento parameter určuje, že sa majú počas kontroly preverovať všetky súbory, aj keď sú uložené vo vnútri archívu, napr. ZIP, RAR, ...
- **Použiť heuristickú analýzu** (štandardne zapnuté): heuristická analýza (*dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí*) bude jedna z metód, ktoré sa použijú na detekciu vírusov počas kontroly.
- **Kontrola v systémovom prostredí** (štandardne zapnuté): počas kontroly sa budú overovať aj systémové oblasti počítača.
- **Zapnúť 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.
- **Kontrola rootkitov** (štandardne zapnuté): Kontrola súčasti Anti-Rootkit skontroluje počítača zistí prítomnosť potenciálnych rootkitov, t. j. programov a technológií, ktoré dokážu zakryť škodlivého programu 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 označiť ako rootkity.

Ďalšie nastavenia kontroly

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



- **Možnosti vypnutia počítača** – Rozhodnite, či sa má počítač vypnúť automaticky po dokončení procesu kontroly. Po potvrdení tejto možnosti (*Vypnúť počítač po dokončení kontroly*) sa aktivuje nová možnosť, ktorá umožní vypnúť počítač, aj keď je momentálne zablokovaný (*Vynútené vypnutie, ak je počítač zablokovaný*).
- **Typy súborov na kontrolu** – Mali by ste tiež určiť, čo chcete kontrolovať:
 - **Všetky typy súborov** s možnosťou definovať výnimky z kontroly vytvorením zoznamu 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.

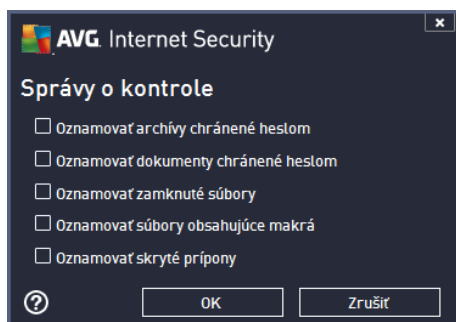
Nastaviť rýchlosť dokončenia kontroly

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 žiením doby trvania kontroly.

Vytvoriť ďalšie správy o kontrole

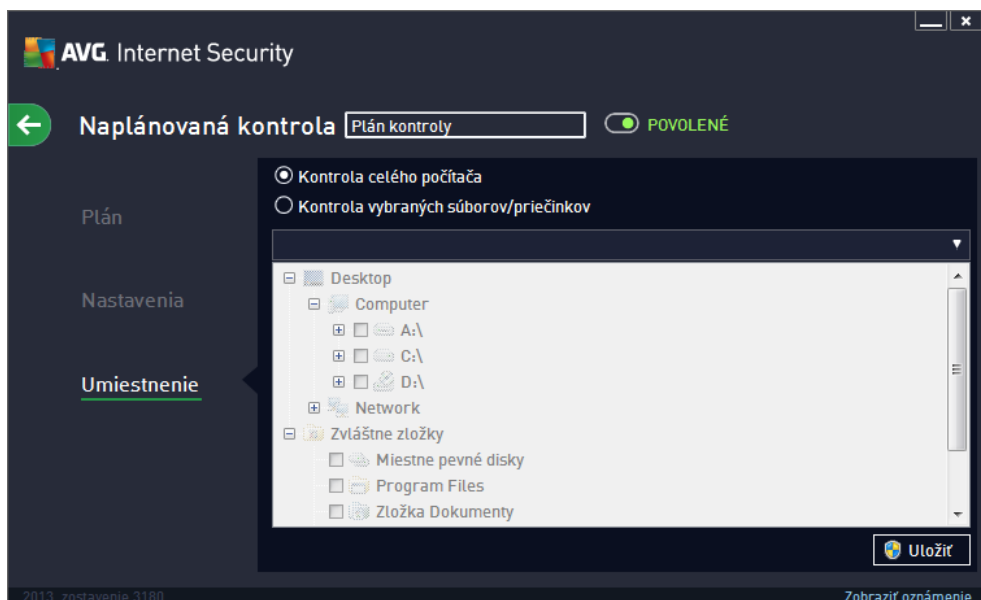
Kliknutím na odkaz **Vytvoriť ďalšie správy o kontrole...** otvorte samostatné dialógové okno s názvom **Správy o kontrole**, v ktorom môžete za kliknutím konkrétnych položiek definovať, ktoré nálezy sa majú hlásiť:



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](#).

11.4.3. 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 (rozbať položky kliknutím na uzol so znakom plus a vybrať priečinky, ktoré chcete kontrolovať). Zaškrtnutím 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 iarkou bez medzier).

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

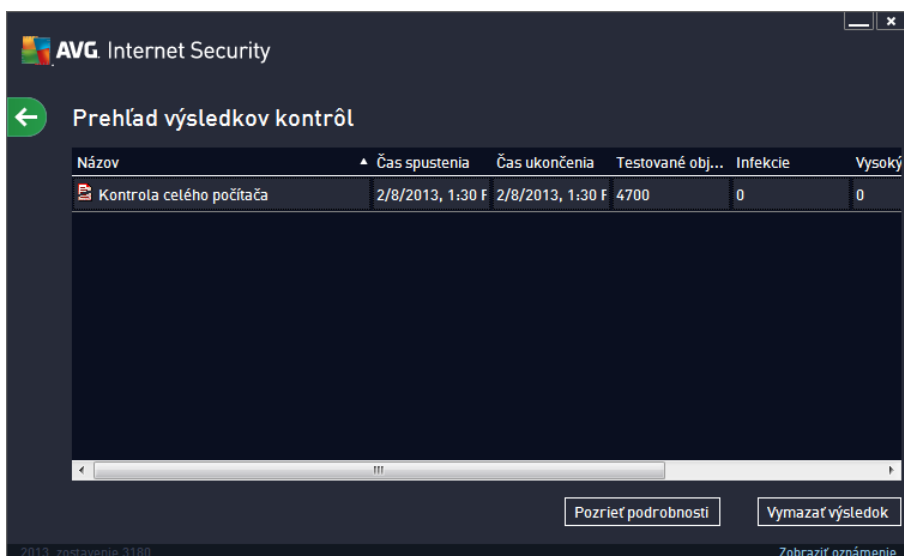
- **Pevné disky počítača** – všetky pevné disky počítača
- **Programové súbory**
 - C:\Program Files\
 - v 64-bitovej verzii C:\Program Files (x86)
- **Priečinko Moje dokumenty**
 - vo Win XP: C:\Documents and Settings\Default User\Moje dokumenty\
 - vo Windows Vista/7: C:\Users\používateľ\Dokumenty\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

11.5. Výsledky kontrol



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.

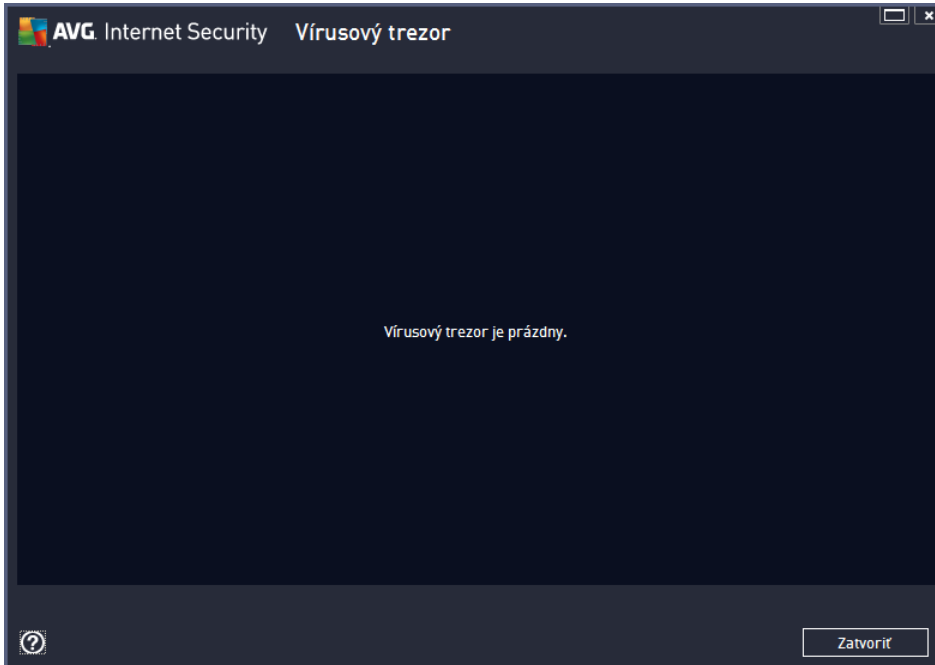
 – Pomocou zelenej šípky v ľavej hornej časti dialógového okna sa vrátite naspäť do [hlavného používateľského rozhrania](#) s prehľadom súčastí.

11.6. Podrobnosti výsledkov kontrol

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

- **Súhrn** – Táto záložka obsahuje základné informácie o kontrole: či bola úspešne dokončená, aké hrozby sa našli a čo sa s nimi spravilo.
- **Podrobnosti** – táto záložka zobrazuje všetky údaje o kontrole vrátane podrobností o akýchkoľvek detegovaných hrozbách. Exportovať prehľad do súboru umožňuje uložiť výsledky kontroly do súboru s príponou .csv.
- **Detekcie** – táto stránka je zobrazená len v prípade, že boli počas kontroly detegované nejaké hrozby, a uvádza podrobné informácie o týchto hrozbách:
 - **Nízka závažnosť** : informácie alebo varovania, nie skutočné hrozby. Obvykle dokumenty obsahujúce makrá, dokumenty alebo archívy chránené heslom, uzamknuté súbory, atď.
 - **Stredná závažnosť** : obvykle PNP (*potenciálne nežiaduce programy, ako napríklad adware*) alebo sledujúce súbory cookie.
 - **Vysoká závažnosť** : závažné hrozby, ako napríklad vírusy, trójske kone, exploity, atď. Taktiež objekty detegované heuristickou metódou detekcie, teda hrozby, ktoré ešte nie sú popísané vo vírusovej databáze.

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 istotu, že súbor naozaj nepotrebujete. Ak zistíte, že odstránenie súboru spôsobuje problémy, môžete ho poslať na analýzu alebo obnoviť do pôvodného umiestnenia.

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

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



Ovládacie tlačidlá

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

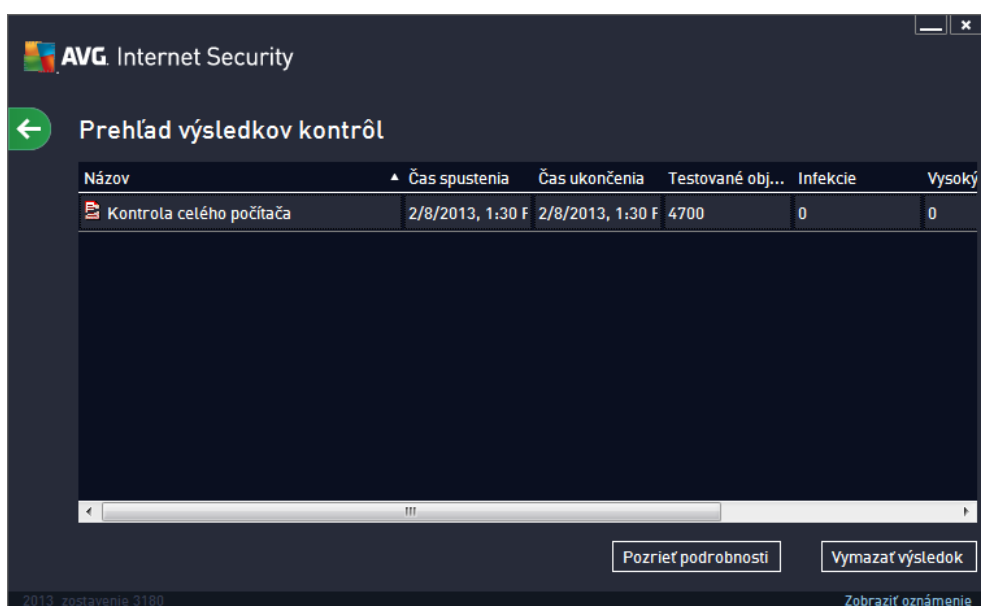
- **Obnoví** – premiestni infikovaný súbor naspäť na jeho pôvodné umiestnenie na vašom disku.
- **Obnoví ako** – premiestni infikovaný súbor do vybraného priečinka.
- **Podrobnosti** – Ak chcete zobraziť podrobné informácie o konkrétnej hrozbe vloženú do karantény **Vírusového trezora**, označte vybranú 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 asti sa dostanete z [používateľského rozhrania hlavnej obrazovky](#) cez položku **Možnosti/História**. Všetky udalosti zaznamenané v asti História sú rozdelené do týchto astí:

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


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 Internet Security 2013**. V dialógovom okne sa nachádza zoznam všetkých doposiaľ spustených kontrol a informácie o ich výsledkoch:

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

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

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

 – červená ikona 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 *Pozrieť podrobnosti* (v spodnej časti tohto dialógového okna).

- **čas spustenia:** Dátum a čas, kedy bola kontrola spustená.
- **čas skončenia:** Dátum a čas, kedy sa kontrola skončila.
- **Testované objekty:** Počet objektov, ktoré sa skontrolovali počas kontroly.
- **Infekcie:** počet detegovaných/odstránených vírusových infekcií
- **Vysoká/Stredná/Nízka** – V týchto stupňoch sa uvádza číslo odstránených/celkových infekcií nájdených pre každú z úrovní závažnosti (vysokú, strednú a nízku).
- **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:

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

13.2. Nálezy súčasti Rezidentný štít

Služba **Rezidentný štít** je časťou súčastí [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:

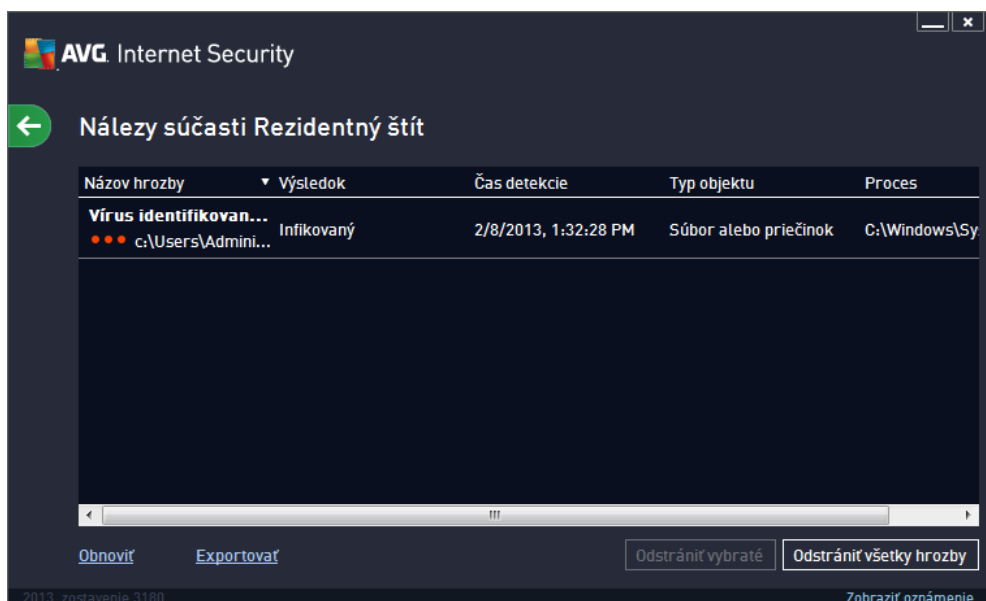


V tomto dialógovom okne s upozomením sa nachádzajú informácie o zistenom objekte, ktorý sa považuje za infikovaný (Názov), a kratší popis rozpoznanej infekcie (Popis). Odkaz [Zobrazí podrobnosti](#) vás presmeruje na on-line vírusovú encyklopédiu, kde nájdete podrobné informácie o zistenej infekcii, 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 detegovaný objekt prekráča do vášho počítača, vírus sa môže dostať do vírusového trezora. V tom prípade sa zobrazí upozornenie informujúce o probléme v súvislosti s premiestňovaním infikovaného objektu do vírusového trezora. Veľkosť vírusového trezora však môžete zmeniť. Je definovaná ako 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 Rezidentný štít si môžete pozrieť v dialógovom okne **Nálezy súčasti Rezidentný štít**. Toto dialógové okno sa nachádza pod položkou ponuky **Možnosti/História/Nálezy súčasti Rezidentný štít** v hornom navigačnom pruhu [hlavného okna](#) aplikácie **AVG Internet Security 2013**. Toto okno obsahuje prehľad objektov detegovaných súčastou Rezidentný štít vyhodnotených ako nebezpečné, ktoré boli buď vylíčené alebo premiestnené do [Vírusového trezora](#).



Pre každý detegovaný objekt sa zobrazia tieto informácie:

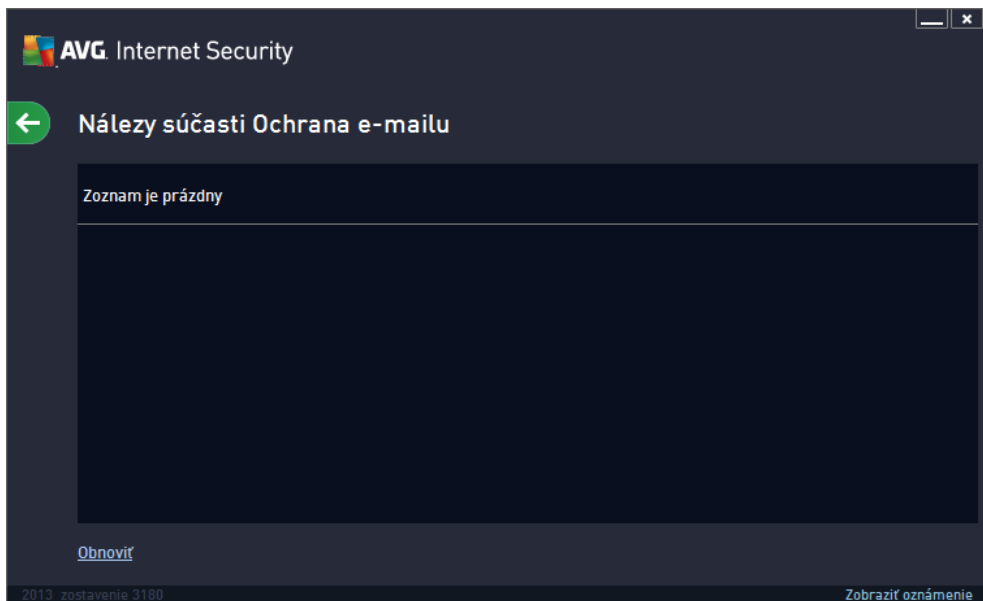
- **Názov detekcie** – popis (prípadne aj názov) zisteného objektu a jeho poloha
- **Výsledok** – akcia urobená na detegovanom objekte
- **as detekcie** – dátum a as detegovania a zablokovania hrozby
- **Typ objektu** – typ detegovaného objektu
- **Proces** – Aká akcia sa vykonala na zavolaní potenciálne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

Ovládacie tlačidlá

- **Obnovi** – Aktualizuje sa zoznam nálezov zistených súčasti **Rezidentný štít**
- **Exportovať** – 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 Ochrana e-mailu

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



Toto okno obsahuje zoznam všetkých detekcií súčasti [Ochrana e-mailu](#). Pre každý detegovaný objekt sa zobrazia tieto informácie:


- **Názov detekcie** – popis (prípadne aj názov) zisteného objektu a jeho zdroj
- **Výsledok** – akcia urobená na detegovanom objekte.
- **čas detekcie** – dátum a čas detekcie podozrivého objektu.
- **Typ objektu** – typ detegovaného objektu.
- **Proces** – aká akcia sa vykonala na 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 (**Vyprázdniť zoznam**).

Ovládacie tlačidlá

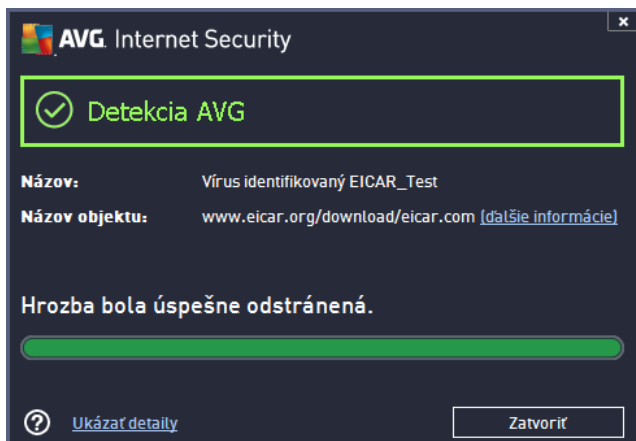
V rozhraní **Nálezy súčasti Kontrola pošty** sa nachádzajú nasledujúce tlačidlá:

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

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

13.4. Nálezy súčasti Webový štít

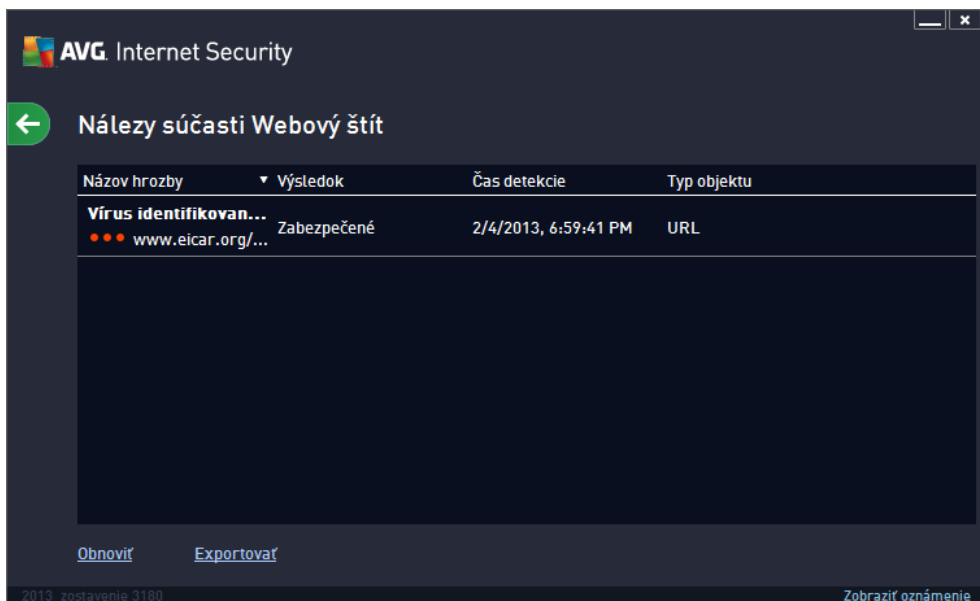
Webový štít kontroluje obsah navštívených internetových stránok a súborov, ktoré sa na nich môžu nachádzať, ešte predtým, než sa zobrazia v internetovom prehliadači alebo prevezmú do počítača. Pri detegovaní hrozby vás program ihneď upozorní otvorením tohto dialógového okna:



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

- **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 súčastí **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 Internet Security 2013**.



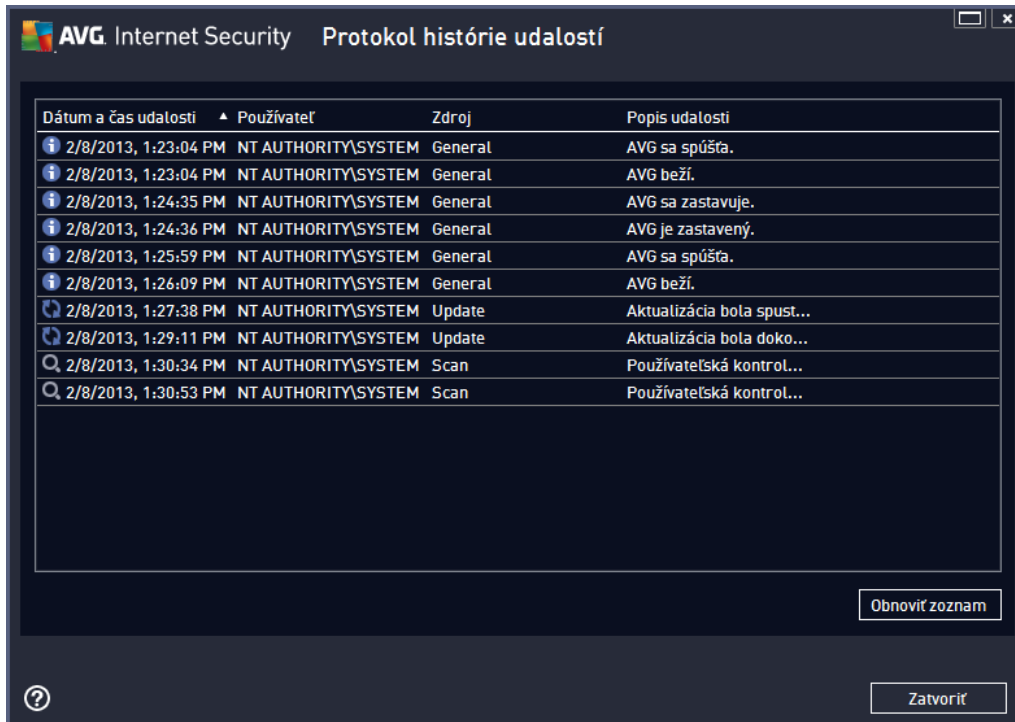
Pre každý detegovaný objekt sa zobrazia tieto informácie:

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

Ovládacie tlačidlá

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

13.5. Protokol histórie udalostí



Dialógové okno **Protokol histórie udalostí** sa nachádza v ponuke **Možnosti/História/Protokol histórie udalostí** v hornom navigačnom pruhu hlavného okna programu **AVG Internet Security 2013**. V tomto dialógovom okne sa nachádza prehľad významných udalostí, ktoré sa vyskytli v čase, keď bol program **AVG Internet Security 2013** 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 Internet Security 2013** hlavného

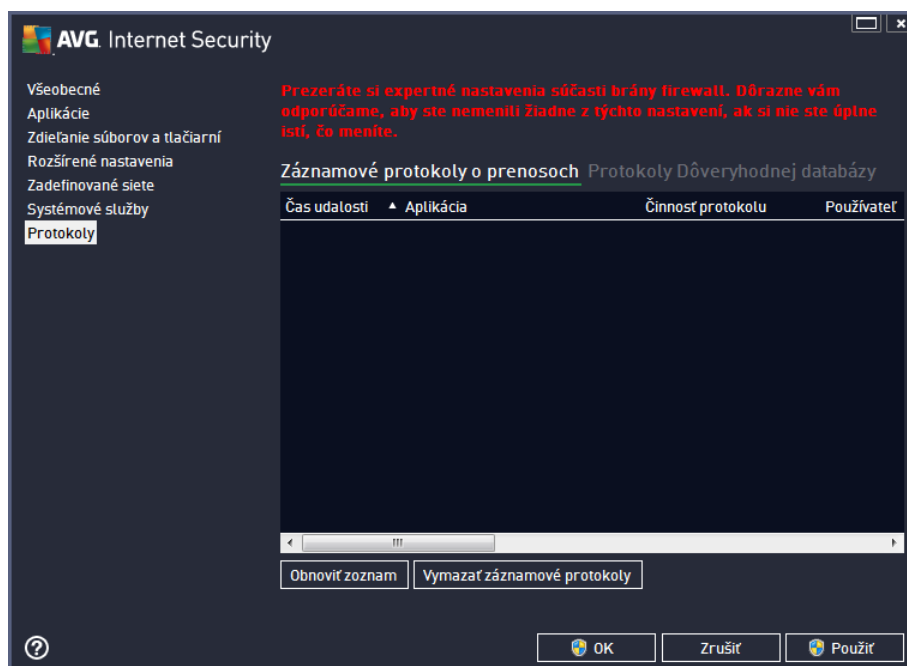
okna

13.6. Protokol súčasti Firewall

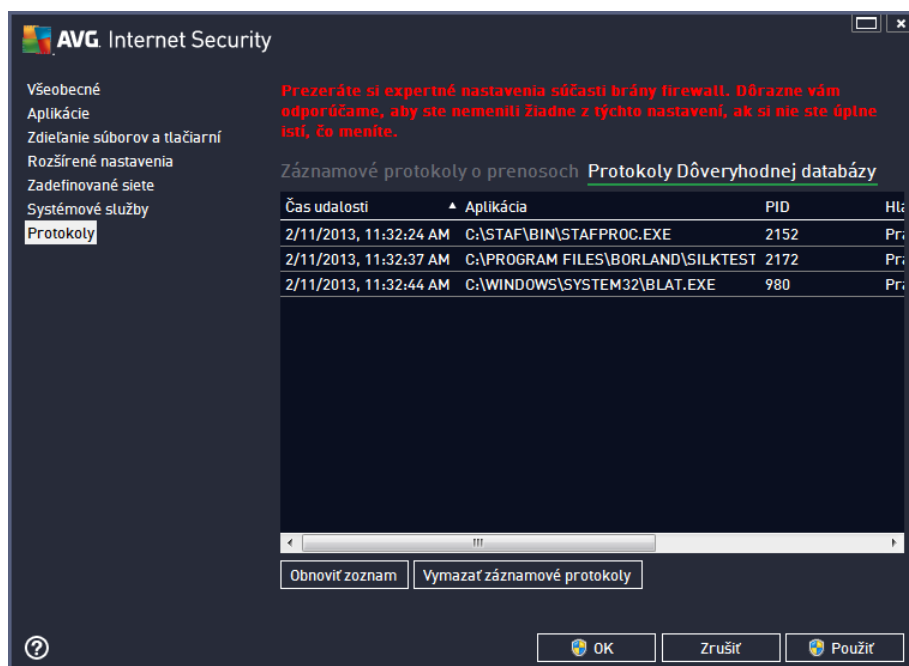
Toto dialógové okno je sú as ou expertných nastavení a odporú ame vám nemeni žiadne nastavenia, ak si zmenou nie ste úplne istí!

Dialógové okno **Protokoly** vám umož ňuje skontrolova zoznam všetkých zaprotokolovaných inností a udalostí sú asti Firewall s podrobným popisom príslušných parametrov zobrazenom na dvoch kartách:

- **Záznamové protokoly o prenosoch** – Na tejto záložke nájdete informácie o aktivitách všetkých aplikácií, ktoré sa pokúsili pripoji do siete. Pre každú položku tu sú uvedené údaje o ase udalosti, názve aplikácie, príslušnej protokolovanej innosti, používate skom názve, PID, smere prenosu, type protokolu, po te vzdialených a miestnych portov a o miestnych a vzdialených adresách IP.



- **Protokoly Dôveryhodnej databázy** – *Dôveryhodná databáza* je interná databáza spoločnosti AVG, ktorá zhromaž ňuje informácie o certifikovaných a dôveryhodných aplikáciách, ktorým sa môže vždy povoli komunikácia on-line. Pri prvom pokuse novej aplikácie o pripojenie do siete (*t. j. ak doposiaľ nebolo vytvorené pravidlo pre bezpečnostnú bránu firewall súvisiace s touto aplikáciou*) je potrebné zisti , i sa má povoli sie ová komunikácia príslušnej aplikácie. AVG najskôr nahliadne do *Dôveryhodnej databázy* a ak je v nej aplikácia uvedená, potom sa jej automaticky povolí prístup k sieti. Až potom, a pod podmienkou, že sa v databáze nenachádzajú informácie o tejto aplikácii, sa zobrazí dialógové okno, v ktorom sa vás program opýta, i chcete povoli aplikácii prístup k sieti.



Ovládacie tlačidlá

- **Obnovi zoznam** – všetky zaznamenané parametre sa dajú usporiadať podľa a vybraného atribútu: chronologicky (*dátumy*) alebo abecedne (*ostatné stĺpce*) – stačí kliknúť na hlavičku príslušného stĺpca. Použijete tlačidlo **Obnovi zoznam** na aktualizovanie práve zobrazených informácií.
- **Vymazať záznamové protokoly** – Stlačením odstránite všetky položky v tabuľke.

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 Internet Security 2013**. Najlepším riešením je ponechať predvolené nastavenia programu, v ktorých sú nastavené automatické aktualizácie. Nezabudnite, že bez aktuálnej vírusovej databázy programu **AVG Internet Security 2013** nemôže program zistiť najnovšie hrozby!

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

14.1. Spustenie aktualizácie

V záujme maximálneho využitia dostupného zabezpečenia je aplikácia **AVG Internet Security 2013** predvolene nastavená tak, aby hľadala nové aktualizácie vírusovej databázy každé štyri hodiny. Keďže spoločnosť AVG nezverejňuje aktualizácie podľa 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 Internet Security 2013** 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 spúšťania 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](#)
- [Plán aktualizácie súčasti Anti-Spam](#)

14.2. Úrovně aktualizácie

Aplikácia **AVG Internet Security 2013** ponúka na výber dve úrovne aktualizácie:

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



Pri [plánovaní aktualizácie](#), si môžete určiť konkrétne parametre pre každú z úrovní aktualizácií:

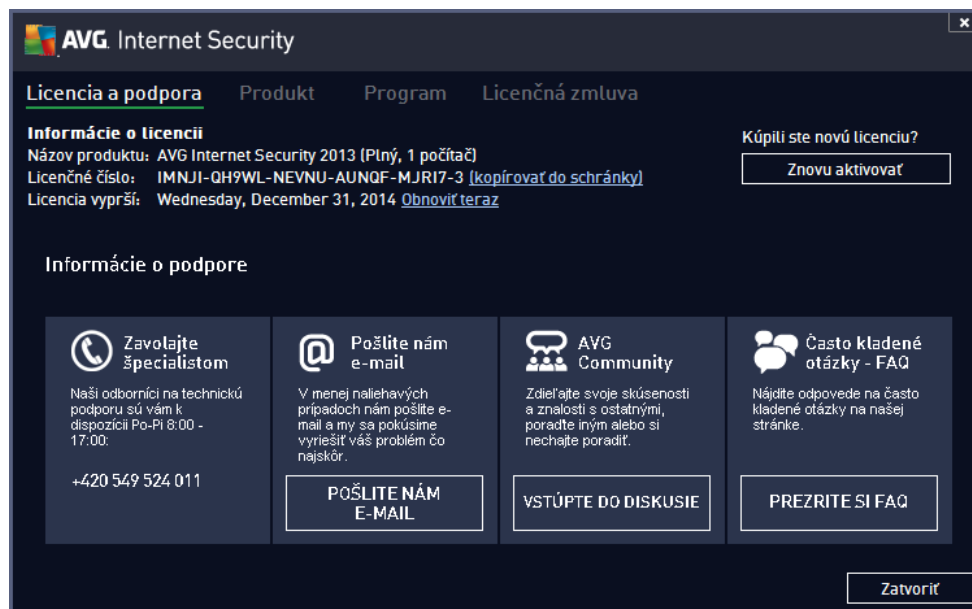
- [Plán aktualizácie definícií](#)
- [Plán aktualizácie programu](#)

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

15. FAQ a technická podpora

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

- **Získajte podporu:** Priamo v aplikácii AVG sa môžete dostať na špeciálnu webovú lokalitu zákazníckej podpory AVG (<http://www.avg.com/>). V hlavnej ponuke vyberte možnosť **Pomocník/Získajte podporu** a ocitnete sa na webovej lokalite AVG s miestami podpory. Ak chcete pokračovať, postupujte podľa pokynov na webovej lokalite.
- **Podpora (odkaz v hlavnej ponuke):** Ponuka aplikácie AVG (v hornej časti hlavného používateľského rozhrania) obsahuje prepojenie **Podpora**, pomocou ktorého otvoríte nové dialógové okno so všetkými typmi údajov, ktoré môžete pri 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 Internet Security 2013** (súbor pomocníka otvoríte stlačením klávesu **F1** v niektorom z dialógových okien aplikácie). V tejto časti nájdete zoznam najčastejších situácií, v ktorých používateľ potrebuje vyhľadať profesionálnu pomoc pre technický problém. Vyberte situáciu, ktorá najviac zodpovedá vášmu problému, a kliknutím 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.
- **Často kladené otázky.** Na webovej lokalite AVG (<http://www.avg.com/>) môžete nájsť aj jednotlivé dôkladne rozpracované často kladené otázky. K tejto časti sa dostanete prostredníctvom ponuky **Centrum podpory/FAQ**. Všetky otázky sú opäť rozdelené do kategórií podľa toho, či sa problém týka nákupu, vírusov alebo ide o technickú otázku.



- **O vírusoch a hrozbách:** Vírusom je venovaná celá kapitola na webovej lokalite AVG (<http://www.avg.com/>) (na webovú stránku sa dostanete z hlavnej ponuky cez položky *Pomocník/O vírusoch a hrozbách*). Výberom položky **Centrum pomoci/O vírusoch a hrozbách** v ponuke otvoríte stránku so štruktúrovaným prehľadom informácií o on-line hrozbách. Môžete tiež nájsť pokyny na odstránenie vírusov spyware a tipov na zachovanie ochrany.
- **Diskusné fórum:** Môžete využiť aj diskusné fórum používateľov produktov AVG na adrese <http://forums.avg.com>.