



AVG Internet Security – bez obmedzenia

Používateľská príručka

Revízia dokumentu AVG.07 (25/11/2016)

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



Obsah

1. Úvod	4
1.1 Hardvérové požiadavky	4
1.2 Softvérové požiadavky	5
2. AVG Zen	6
2.1 Proces inštalácie Zen	7
2.2 Používateľské rozhranie Zen	8
2.2.1 <i>Dlaždice kategórií</i>	8
2.2.2 <i>Pás nástrojov Zariadenia</i>	8
2.2.3 <i>Tlačidlo Správy</i>	8
2.2.4 <i>Stavové tlačidlo</i>	8
2.2.5 <i>Tlačidlo Upgradovať/Predĺžiť</i>	8
2.2.6 <i>Tlačidlo Obnoviť</i>	8
2.2.7 <i>Tlačidlo Nastavenia</i>	8
2.2.8 <i>Ikona v paneli úloh</i>	8
2.3 Sprievodcovia krok za krokom	20
2.3.1 <i>Ako prijať pozvánky?</i>	20
2.3.2 <i>Ako pridať zariadenia do svojej siete?</i>	20
2.3.3 <i>Ako zmeniť názov alebo typ zariadenia?</i>	20
2.3.4 <i>Ako sa pripojiť k existujúcej sieti Zen?</i>	20
2.3.5 <i>Ako vytvoriť novú sieť Zen?</i>	20
2.3.6 <i>Ako nainštalovať produkty AVG?</i>	20
2.3.7 <i>Ako opustiť sieť?</i>	20
2.3.8 <i>Ako odstrániť zariadenia zo svojej siete?</i>	20
2.3.9 <i>Ako zobraziť a/alebo spravovať produkty AVG?</i>	20
2.4 FAQ a podpora	34
3. AVG Internet Security	35
3.1 Proces inštalácie AVG	36
3.1.1 <i>Vitajte!</i>	36
3.1.2 <i>Inštalácia AVG</i>	36
3.2 Po inštalácii	37
3.2.1 <i>Aktualizácia vírusovej databázy</i>	37
3.2.2 <i>Registrácia produktu</i>	37
3.2.3 <i>Otvorenie používateľského rozhrania</i>	37
3.2.4 <i>Kontrola celého počítača</i>	37
3.2.5 <i>Test EICAR</i>	37
3.2.6 <i>Predvolená konfigurácia AVG</i>	37
3.3 Používateľské rozhranie AVG	39
3.3.1 <i>Horný navigačný rad</i>	39
3.3.2 <i>Informácie o stave zabezpečenia</i>	39
3.3.3 <i>Prehľad súčastí</i>	39



3.3.4	<i>Kontrola/Aktualizovať rýchle odkazy</i>	39
3.3.5	<i>AVG Advisor</i>	39
3.3.6	<i>AVG Akcelerátor</i>	39
3.4	<i>Súčasti AVG</i>	46
3.4.1	<i>Ochrana počítača</i>	46
3.4.2	<i>Ochrana prezerania webu</i>	46
3.4.3	<i>Software Analyzer</i>	46
3.4.4	<i>Ochrana e-mailu</i>	46
3.4.5	<i>Firewall</i>	46
3.4.6	<i>PC Analyzer</i>	46
3.5	<i>Rozšírené nastavenia AVG</i>	57
3.5.1	<i>Vzhľad</i>	57
3.5.2	<i>Zvuky</i>	57
3.5.3	<i>Dočasne vypnúť ochranu AVG</i>	57
3.5.4	<i>Ochrana počítača</i>	57
3.5.5	<i>Kontrola pošty</i>	57
3.5.6	<i>Ochrana prezerania webu</i>	57
3.5.7	<i>Software Analyzer</i>	57
3.5.8	<i>Kontroly</i>	57
3.5.9	<i>Plány</i>	57
3.5.10	<i>Aktualizácia</i>	57
3.5.11	<i>Výnimky</i>	57
3.5.12	<i>Vírusový trezor</i>	57
3.5.13	<i>AVG Sebaochrana</i>	57
3.5.14	<i>Preferencie ochrany osobných údajov</i>	57
3.5.15	<i>Ignorovať chybový stav</i>	57
3.5.16	<i>Advisor – známe siete</i>	57
3.6	<i>Nastavenia súčasti Firewall</i>	104
3.6.1	<i>Všeobecné</i>	104
3.6.2	<i>Aplikácie</i>	104
3.6.3	<i>Zdieľanie súborov a tlačiarňí</i>	104
3.6.4	<i>Rozšírené nastavenia</i>	104
3.6.5	<i>Zadefinované siete</i>	104
3.6.6	<i>Systémové služby</i>	104
3.6.7	<i>Protokoly</i>	104
3.7	<i>Kontrola AVG</i>	114
3.7.1	<i>Vopred definované kontroly</i>	114
3.7.2	<i>Kontrola z prieskumníka</i>	114
3.7.3	<i>Kontrola z príkazového riadka</i>	114
3.7.4	<i>Plánovanie kontrol</i>	114
3.7.5	<i>Výsledky kontrol</i>	114
3.7.6	<i>Podrobnosti výsledkov kontrol</i>	114
3.8	<i>AVG File Shredder</i>	138



3.9 Vírusový trezor	139
3.10 História	140
3.10.1 Výsledky kontrol	140
3.10.2 Nálezy súčasti Rezidentný štít	140
3.10.3 Nálezy súčasti Identity Protection	140
3.10.4 Nálezy súčasti Ochrana e-mailu	140
3.10.5 Nálezy súčasti Webový štít	140
3.10.6 Protokol histórie udalostí	140
3.10.7 Protokol súčasti Firewall	140
3.11 Aktualizácie AVG	150
3.12 Najčastejšie otázky a technická podpora	150



1. Úvod

Gratulujeme vám k nákupu balíka **AVG Internet Security – bez obmedzenia!** Tento balík vám prináša všetky výhody produktu **AVG Internet Security** rozšíreného o funkcie aplikácie **AVG Zen**.

AVG Zen

Tento neoceniteľný nástroj na správu dohľadne nielen na vaše zariadenia, ale dokonca na zariadenia celej vašej rodiny. Všetky vaše zariadenia sú prehľadne zoskupené na jednom mieste, takže si ľahko udržíte prehľad o stave ochrany, výkone a ochrane súkromia na každom zariadení. S **AVG Zen** sú dni kontrolovania každého zariadenia po jednom preč. Dokonca môžete spustiť úlohy kontroly a údržby a opraviť najnaliehavejšie problémy zabezpečenia na diaľku. Aplikácia **AVG Zen** je priamo zahrnutá do balíka **AVG Protection**, takže funguje hneď od začiatku.

[Kliknutím sem sa dozviete viac o aplikácii AVG Zen](#)

AVG Internet Security

Táto oceňovaná bezpečnostná aplikácia vytvára niekoľko vrstiev ochrany pre všetko, čo robíte on-line, takže sa nemusíte obávať odcudzenia identity, vírusov ani otvorenia škodlivých stránok. **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 ste dostali najlepšiu možnú ochranu. Môžete v bezpečí nakupovať a spravovať on-line bankové účty, používať sociálne siete alebo surfovať, pričom vyhadzujete informácie – môžete sa spoľahnúť na ochranu v reálnom čase.

[Kliknutím sem sa dozviete viac o aplikácii AVG Internet Security](#)

1.1. Hardvérové požiadavky

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

- Procesor Intel Pentium 1,5 GHz alebo rýchlejší
- 512 MB (Windows XP)/1 024 MB (Windows Vista, Windows 7 a 8) pamäte RAM
- 1,3 GB voľného miesta na pevnom disku (*na účely inštalácie*)

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

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



1.2. Softvérové požiadavky

AVG Internet Security je určený na ochranu pracovných staníc s nasledujúcimi operačnými systémami:

- Windows XP Home Edition SP3
- Windows XP Professional SP3
- Windows Vista (32-bitová a 64-bitová verzia, všetky edície)
- Windows 7 (32-bitová a 64-bitová verzia, všetky edície)
- Windows 8 (32-bitová a 64-bitová verzia)
- Windows 10 (32-bitová a 64-bitová verzia)

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



2. AVG Zen

Táto čas príručky podrobne dokumentuje produkt AVG Zen. Upozorujeme, že sa táto príručka týka iba verzie počítača tohto produktu.

Spoločnosť AVG, svetoznámy výrobca ochranného softvéru, vykonal ďalší krok v ústrety svojim zákazníkom a úplnému uspokojeniu ich potrieb týkajúcich sa zabezpečenia. Nový produkt AVG Zen efektívne spája zariadenia od stolových počítačov po prenosné zariadenia, údaje a ľudí ktorí ich používajú do jedného balíka, aby zjednodušila niektoré komplikácie digitálneho veku. Pomocou jednej aplikácie AVG Zen získajú používatelia na jednom mieste prehľad o nastaveniach zabezpečenia a súkromia všetkých svojich zariadení.

Myšlienka produktu AVG Zen je navrátiť jednotlivcom vlastniacim viacero zariadení kontrolu nad ich údajmi a zabezpečením, pretože sme presvedčení, že s kontrolou prichádza možnosť voľby. Spoločnosť AVG sa nesnaží diktovať, že je zdieľanie alebo sledovanie samo o sebe nesprávne. Chce ale svojim zákazníkom poskytnúť informácie, ktoré im umožnia mať pod kontrolou to, čo zdieľajú a či sú sledovaní, aby sa mohli sami rozhodnúť. Rozhodnúť sa, aby mohli slobodne žiť svoje životy a vychovávať svoju rodinu tak, ako chcú, uchádzať sa o zamestnanie bez strachu, že bude narušené ich súkromie.

Ďalšia výborná vlastnosť produktu AVG Zen je, že prináša zákazníkom konzistentné rozhranie na všetkých zariadeniach, takže sa aj neskúsení používatelia rýchlo naučia jednoducho spravovať a zabezpečiť všetky svoje zariadenia. Je to aspoň jedna vec, ktorá sa zjednodušuje vo svete, ktorý sa stáva zložitým a naďalej zložitejším. Ale najdôležitejšie je, že produkt AVG Zen je navrhnutý tak, aby bežným ľuďom prinášal pokoj do každodenného života. Ako sa Internet stáva stredom nášho sveta, produkt AVG Zen je tu, aby nám pomohol sa v ňom orientovať.

Táto čas dokumentácie obsahuje popis niektorých funkcií produktu AVG Zen. Ak by ste potrebovali informácie o iných produktoch spoločnosti AVG, pozrite si ďalšiu časť tejto dokumentácie alebo aj samostatných používateľských sprievodcov. Týchto sprievodcov si môžete stiahnuť na internetových stránkach spoločnosti [AVG](http://AVG.com).



2.1. Proces inštalácie Zen


Na nákup a stiahnutie vášho balíka **AVG Internet Security – bez obmedzenia** použijete nasledujúcu [webovú stránku](#). Spustíte proces inštalácie AVG Internet Security. Pozostáva len z niekoľkých krokov a jeho dokončenie by malo byť jednoduché (kliknutím sem si o ňom prečítate viac). V rámci procesu sa taktiež nainštaluje AVG Zen. Ihneď po inštalácii sa zobrazí [používateľské rozhranie Zen](#). Bude vám tiež ponúknutá možnosť vytvoriť si novú sieť Zen alebo sa pripojiť do existujúcej. To však nie je povinné – túto ponuku môžete preskočiť a využiť pripojenie do siete Zen kedykoľvek v budúcnosti.

Tiež by vás mohli zaujímať tieto súvisiace témy:

- [Ktoré tri používateľské režimy má AVG Zen?](#)
- [Ako prijať pozvánky?](#)
- [Ako sa pripojiť k existujúcej sieti Zen?](#)
- [Ako vytvoriť novú sieť Zen?](#)

2.2. Používateľské rozhranie Zen



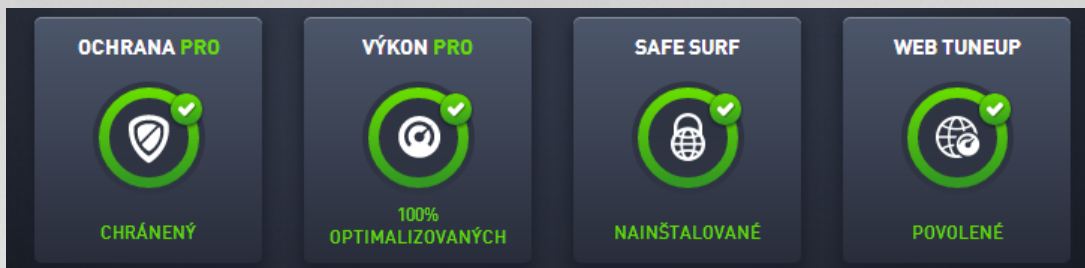
Toto je hlavné dialógové okno používateľského rozhrania AVG Zen. V každom inom dialógovom okne sa v ľavom hornom rohu vždy nachádza tlačidlo  – kliknutím na ňu sa vrátite naspäť na hlavnú obrazovku (v niektorých nasledujúcich dialógových oknách vás toto tlačidlo vráti o jeden krok naspäť, t. j. na predchádzajúce dialógové okno).

Toto dialógové okno sa skladá z niekoľkých oddelených častí:

- [Dlaždice kategórií](#)
- [Pás nástrojov Zariadenia](#)
- [Tlačidlo Správ](#)
- [Stavové tlačidlo](#)
- [Tlačidlo Upgradova /Pred ži](#)
- [Tlačidlo Obnovi](#)
- [Tlačidlo Nastavenia](#)
- [Ikona v paneli úloh](#)



2.2.1. Dlaždice kategórií



Dlaždice kategórií vám umožňujú inštalovanie softvérových produktov AVG, zobrazovanie ich stavu a jednoduché otvorenie ich používateľského rozhrania. [Administrátor](#) siete Zen ich môže jednoducho používať na zobrazenie a správu produktov AVG nainštalovaných na vzdialených zariadeniach. Pomocou [páru nástrojov Zariadenia](#) môžete prepínať medzi vzdialenými zariadeniami pripojenými do vašej siete Zen.

V každej dlaždici je kruh, ktorého farba závisí od stavu produktov v danej kategórii (mali by ste sa snažiť, aby mal zelenú farbu). V prípade niektorých kategórií môže byť kruh neúplný, čo znamená, že už máte nainštalovaný produkt z tejto kategórie, ale ešte existuje nejaký produkt, ktorý nainštalovaný nemáte.

Bez ohľadu na to, na aký typ zariadenia sa dívate, vždy uvidíte tie isté dlaždice. Ich obsah ale bude rôzny v závislosti na type sledovaného zariadenia (zariadenie s [Windowsom](#), [Androidom](#) alebo [Macom](#)).

2.2.1.1. Zariadenia s Windowsom

INTERNET SECURITY/ANTIVIRUS FREE

AVG Internet Security – tento bezpečnostný softvér vytvára niekoľko vrstiev ochrany pre všetko, čo robíte online, takže sa nemusíte obávať odcudzenia identity, vírusov ani otvorenia škodlivých stránok. 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 online bankové účty, používať sociálne siete alebo surfovať a vyhľadávať informácie – môžete sa spoľahnúť na ochranu v reálnom čase.

AVG AntiVirus Free – prípadne môžete použiť len základnú ochranu počítača, ktorá je zdarma. AVG AntiVirus Free vás bude spoľahlivo chrániť pred vírusmi, spyware a iným malware, škodlivými odkazmi na internete a krádežou identity, ale neobsahuje doplnkové funkcie, ako napríklad Firewall, Anti-Spam, Dátový trezor, prioritné aktualizácie a prémiovú podporu.

Prehľad stavov

- Ak nie je nainštalované AVG Internet Security ani AVG AntiVirus Free, táto dlaždica zostane sivá a pod ňou bude nápis „Nechránené“. Kliknutím na ňu ale môžete jednoducho [nainštalovať túto aplikáciu AVG](#).
- Ak je problémov vyžadujúcich vašu pozornosť príliš mnoho (napríklad keď je celá ochrana deaktivovaná), bude kruh vnútri dlaždice červený a pod ním bude nápis „Nechránené“. V prípade, že je problémov málo a nie sú kritické, bude dlaždica zelená a pod ňou bude nápis „Čiastočne chránené“. V oboch prípadoch uvidíte vo farebnom kruhu číslo (v pravom hornom rohu dlaždice) uvádzajúce počet problémov, ktoré by vás mohli zaujímať. Stlačením tlačidla [Správy](#) zobrazíte zoznam problémov a môžete ich vyriešiť.
- Ak neexistujú žiadne problémy, bude kruh v dlaždici zelený a pod ním bude nápis „Chránené“.

čo sa stane, keď kliknete na túto dlaždicu:

- Ak ešte nie je nainštalovaná žiadna ochrana počítača – otvorí sa nové dialógové okno, v ktorom



budete môc spusti jej inštaláciu. [Pre ítajte si viac o inštalácii produktov AVG.](#)

- Ak zobrazujete svoje vlastné zariadenia, na ktorých je nainštalované AVG Internet Security alebo AVG AntiVirus Free – otvorí sa ich používateľské rozhranie.
- Ak zobrazujete vzdialené zariadenie, na ktorom je nainštalované AVG Internet Security alebo AVG AntiVirus Free (a ste prihlásení ako [administrátor](#)), otvorí sa dialógové okno so stručným prehľadom stavu aplikácie na vzdialenom zariadení. Toto dialógové okno vám taktiež umožní vykonať viacero činností na diaľku, ako napríklad spustiť kontrolu (tlačidlo **Skontrolovať teraz**) alebo vykonať aktualizáciu (tlačidlo **Aktualizácia**). Ostatné činnosti vykonávané na diaľku, ako napríklad zapnutie predtým deaktivovaných súčastí ochrany, sú prístupné prostredníctvom kliknutia na tlačidlo **Zobrazí podrobnosti**, ktorým otvoríte [dialógové okno Správy](#) aktuálne vybraného zariadenia. [Pre ítajte si viac o zobrazovaní a správe vzdialených zariadení.](#)

PC TUNEUP

Aplikácia **AVG PC TuneUp** umožňuje obnovenie úplného výkonu operačného systému, hier a programov. Aplikácia AVG PC TuneUp môže automaticky spúšťať a dôležité úlohy údržby, ako je čistenie pevného disku a registrov, alebo ich môžete spúšťať manuálne. Aplikácia AVG PC TuneUp rozpozná, či sú v systéme nejaké problémy a navrhne jednoduché riešenia. Aplikáciu AVG PC TuneUp môžete tiež použiť na úpravu vzhľadu systému Windows podľa vašich požiadaviek.

Prehľad stavov

- Ak nie je aplikácia AVG PC TuneUp nainštalovaná, táto dlaždica bude sivá a pod ňou bude nápis „Neoptimalizované“. Kliknutím jednoducho [nainštalujete túto aplikáciu AVG.](#)
- Ak je problémov vyžadujúcich vašu pozornosť príliš mnoho (napríklad keď je celé AVG PC TuneUp deaktivované), bude kruh vnútri dlaždice červený a pod ním bude nápis „Neoptimalizované“. V prípade, že je problémov málo a nie sú kritické, bude dlaždica zelená a pod ňou bude nápis „Čiastočne optimalizované“. V oboch prípadoch uvidíte v oranžovom kruhu číslo (v pravom hornom rohu dlaždice) uvádzajúce počet problémov, ktoré by vás mohli zaujímať. Stlačením tlačidla [Správy](#) zobrazíte zoznam problémov a môžete ich vyriešiť.
- Ak neexistujú žiadne problémy s aplikáciou AVG PC TuneUp, bude kruh v dlaždici zelený a pod ním bude nápis „Optimalizované“.

čo sa stane, keď kliknete na túto dlaždicu:

- Ak ešte nie je nainštalované AVG PC TuneUp – otvorí sa nové dialógové okno, v ktorom budete môc spustiť inštaláciu AVG PC TuneUp. [Pre ítajte si viac o inštalácii produktov AVG.](#)
- Ak zobrazujete svoje vlastné zariadenia, ktoré majú nainštalované AVG PC TuneUp – otvorí sa používateľské rozhranie AVG PC TuneUp.
- Ak zobrazujete (ako [administrátor](#)) vzdialené zariadenie s nainštalovanou aplikáciou AVG PC TuneUp – otvorí sa dialógové okno so stručným prehľadom stavu AVG PC TuneUp na vzdialenom zariadení. Toto dialógové okno vám taktiež umožní vykonať viacero činností na diaľku, ako napríklad spustiť údržbu (tlačidlo **Spustiť údržbu**) alebo vykonať aktualizáciu (tlačidlo **Aktualizácia**). Ostatné činnosti vykonávané na diaľku sú prístupné prostredníctvom kliknutia na tlačidlo **Zobrazí podrobnosti**, ktorým otvoríte [dialógové okno Správy](#) aktuálne vybraného zariadenia. [Pre ítajte si viac o prezeraní a spravovaní stavu vzdialených zariadení.](#)

HMA! PRO VPN

Hide My Ass! Pro VPN – táto platená aplikácia vám umožní pripájať sa na internet bezpečne a v súkromí, takže môžete chrániť svoje osobné údaje a pripájať sa odkiaľkoľvek na stránky, ktoré máte radi – dokonca aj na verejnej Wi-Fi a v nebezpečných sieťach.



Prehľad stavov

- Ak nie je aplikácia HMA! Pro VPN nainštalovaná, táto dlaždica ostane sivá a pod ňou bude nápis „Nenainštalované“. Kliknutím na ňu alebo môžete jednoducho [nainštalovať tento produkt AVG](#).
- Ak je celá aplikácia HMA! Pro VPN deaktivovaná, bude kruh v tejto dlaždici žltý a pod ním bude nápis „Deaktivované“.
- Ak je aplikácia HMA! Pro VPN aktívna a funguje bez problémov, bude kruh v tejto dlaždici zelený a pod ním bude nápis „Aktivované“.

čo sa stane, keď kliknete na túto dlaždicu:

- Ak ešte nie je aplikácia HMA! Pro VPN nainštalovaná – otvorí sa nové dialógové okno, v ktorom budete môcť spustiť jej inštaláciu. Po kliknutí na tlačidlo **Zistite viac** budete presmerovaní na internetovú stránku AVG, kde si budete môcť kúpiť tento softvér.
- Ak zobrazujete svoje vlastné zariadenie, na ktorom je nainštalovaná aplikácia HMA! Pro VPN – otvorí sa používateľské rozhranie HMA! Pro VPN.
- Ak zobrazujete (ako [administrátor](#)) vzdialené zariadenie, na ktorom je nainštalovaná táto aplikácia – otvorí sa dialógové okno so stručným prehľadom stavu tejto aplikácie na vzdialenom zariadení. Toto dialógové okno však obsahuje iba informácie a neumožňuje vykonanie žiadnej zmeny. [Prečítajte si viac o zobrazovaní a správe vzdialených zariadení.](#)

WEB TUNEUP

AVG Web TuneUp – výkonný prídavok prehliadača a je úplne zdarma a funguje v rozhraniach prehliadačov Chrome, Firefox a Internet Explorer. Upozorní vás na nebezpečné stránky a umožní vám zablokovať dotieravé sledovacie programy (zobrazením toho, ktoré internetové stránky zbierajú údaje o vašich on-line aktivitách). Umožňuje tiež rýchle a jednoduché odstránenie vašich stôp po on-line aktivitách, vrátane histórie prehliadania, sťahovania a súborov cookie.

Prehľad stavov

- Ak nie je AVG Web TuneUp nainštalovaný, táto dlaždica bude sivá a pod ňou bude nápis „Nenainštalované“. Kliknutím však jednoducho [tento doplnok prehliadača a AVG nainštalujete](#). *Niektoré prehliadače je potrebné reštartovať na dokončenie inštalácie neho procesu. Niekedy budete musieť povoliť inštaláciu priamo v prehliadači.*
- Ak je celý AVG Web TuneUp deaktivovaný, bude kruh v tejto dlaždici žltý a pod ním bude nápis „Deaktivované“. V takomto prípade môžete kliknúť na dlaždicu a prejsť na odkaz **Otvoriť v prehliadači** (prípadne použiť [tlačidlo Správy](#)). Otvorí sa váš prehliadač a zobrazia sa podrobné pokyny o aktivácii AVG Web TuneUp vo vašom prehliadači.
- Ak je doplnok prehliadača a AVG Web TuneUp aktívny a funguje bez problémov, bude kruh v tejto dlaždici zelený a pod ním bude nápis „Aktivované“.

čo sa stane, keď kliknete na túto dlaždicu:

- Ak AVG Web TuneUp ešte nie je nainštalovaný – otvorí sa nové dialógové okno, prostredníctvom ktorého si AVG Web TuneUp budete môcť nainštalovať. [Prečítajte si viac o inštalácii produktov AVG.](#)
- Ak si prezerať svoje vlastné zariadenia s nainštalovaným doplnkom AVG Web TuneUp – otvorí sa prehľad AVG Web TuneUp, ktorý vám umožní prezerať si zoznam jednotlivých funkcií ochrany súkromia (**Site Safety, Do Not Track, odstránenie prehliadača** a **AVG Secure Search**), kde uvidíte, ktoré sú aktívne a spustené. Prepojenie **Otvoriť v prehliadači** môžete použiť na otvorenie rozhrania AVG Web TuneUp vo vašom predvolenom webovom prehliadači.
- Ak zobrazujete (ako [administrátor](#)) vzdialené zariadenie s nainštalovaným doplnkom AVG Web TuneUp – otvorí sa dialógové okno so stručným prehľadom stavu AVG Web TuneUp na vzdialenom



zariadení. Toto dialógové okno je iba informatívne a neumožňuje vykonanie žiadnej zmeny. Ak sa vyskytnú problémy vyžadujúce si vašu pozornosť, prístupné sa tlačidlo **Zobrazí podrobnosti**. Kliknutím na ňu otvoríte [dialógové okno Správy](#) aktuálne vybratého zariadenia. [Prečítajte si viac o prezeraní a spravovaní stavu vzdialených zariadení.](#)

Tiež by vás mohli zaujímať tieto súvisiace témy:

- [Ako nainštalovať produkty AVG?](#)
- [Ako zobraziť a/alebo spraviť produkty AVG?](#)

2.2.1.2. Zariadenia s Androidom

Táto príručka sa venuje iba používaniu aplikácie AVG Zen na počítačoch; ako [administrátor](#) budete mať s veľkou pravdepodobnosťou v sieti aj zariadenia so systémom Android™. V takom prípade nebudete prekvapení, ak na dlaždiciach [kategórií](#) týchto zariadení uvidíte iný obsah.

Aktuálne dostupné aplikácie AVG pre mobilné zariadenia:

- **AVG AntiVirus** (zadarmo alebo platený) – táto aplikácia chráni pred nebezpečnými vírusmi, malware, spyware a textovými správami a pomáha chrániť vaše osobné údaje. Táto aplikácia prináša efektívnu a jednoducho použiteľnú ochranu pred vírusmi a malware spolu s kontrolou aplikácií v reálnom čase, lokátorom telefónu, nástrojom na ukončenie úloh, zámkom aplikácií a vymazaním miestneho zariadenia na ochranu pred hrozbami pre ochranu súkromia a on-line identity. Ochrana v reálnom čase vás chráni pred rizikami v stiahnutých aplikáciách a hrách.
- **AVG Cleaner** (zadarmo) – táto aplikácia umožňuje rýchle vymazanie a vyčistenie prehliadača, histórie telefonátov a textových správ, a tiež identifikuje a odstraňuje nežiaduce dočasné údaje aplikácií z internej pamäte zariadenia a karty SD. Výrazne optimalizuje využitie miesta na úložisku, aby vaše zariadenie so systémom Android™ fungovalo lepšie a pracovalo plynulejšie.
- **AVG PrivacyFix** (zadarmo) – táto aplikácia prináša jednoduchý spôsob, ako chrániť svoje súkromie on-line prostredníctvom prenosného zariadenia. Umožňuje prístup ku hlavnému panelu, ktorý rýchlo a jednoducho zobrazí, aké údaje zdieľate v sieťach Facebook, Google a LinkedIn a s kým ich zdieľate. Ak chcete niečo zmeniť, stačí jedno kliknutie, ktoré vás preniesie presne tam, kde môžete zmeniť svoje nastavenia. Nová ochrana proti sledovaniu Wi-Fi umožňuje nastavenie sietí Wi-Fi, ktoré poznáte a schvaľujete, čím zabráni sledovaniu vášho zariadenia prostredníctvom ostatných sietí.

Jednotlivé kategórie sú takéto:

OCHRANA

Kliknutím na túto dlaždicu zobrazíte informácie týkajúce sa aplikácie **AVG AntiVirus** – informácie o kontrole a jej výsledkoch, a tiež o aktualizáciách definícií vírusov. Ako [administrátor](#) siete taktiež môžete spustiť kontrolu (tlačidlo **Skontrolovať teraz**) alebo vykonať aktualizáciu (tlačidlo **Aktualizácia**) vzdialeného zariadenia so systémom Android.

VÝKON

Kliknutím na túto dlaždicu zobrazíte údaje týkajúce sa výkonu, teda ktoré funkcie zlepšenia výkonu aplikácie **AVG AntiVirus** sú aktívne (**Nástroj na ukončenie úloh**, **Stav batérie**, **Dátový balík** (iba v platenej verzii) a **Využitie úložiska**), a či je aplikácia **AVG Cleaner** nainštalovaná a spustená (spolu so štatistikou).



SÚKROMIE

Kliknutím na túto dlaždicu zobrazíte údaje týkajúce sa vášho súkromia, teda ktoré funkcie ochrany súkromia aplikácie **AVG AntiVirus** sú aktívne (**Zámok aplikácií**, **Záloha aplikácií** a **Blokovanie hovorov a správ**), a či je aplikácia **AVG PrivacyFix** nainštalovaná a spustená.

OCHRANA PROTI UKRADNUTIU

Kliknutím na túto dlaždicu zobrazíte informácie o funkcii **Ochrana proti ukradnutiu** aplikácie **AVG AntiVirus**, ktorá umožňuje lokalizáciu strateného prenosného zariadenia na mapách Google Maps. Ak je na pripojenom zariadení nainštalovaná platená verzia (**Pro**) aplikácie **AVG AntiVirus**, tiež uvidíte stav funkcie **Fotopasca** (tajné snímanie osôb snažiacich sa prekona uzamknutie prenosného zariadenia) a funkcie **Zámok zariadenia** (umožňuje uzamknutie zariadenia v prípade, že došlo k výmene karty SIM).

Tiež by vás mohli zaujímať tieto súvisiace témy:

- [Ako pripojiť prenosné zariadenie so systémom Android k existujúcej sieti Zen?](#)
- [Ako zobrazíť a/alebo spravovať produkty AVG?](#)

2.2.1.3. Zariadenia Mac

Táto príručka sa venuje iba používaniu aplikácie AVG Zen na počítačoch; ako [administrátor](#) však budete mať možnosť kontrolovať pravdepodobnosťou v sieti aj zariadenia Mac. V takom prípade nebudete prekvapení, ak na dlaždiciach [kategórií](#) týchto zariadení uvidíte iný obsah.

V súhrnnej zoznami sú dostupné aplikácie AVG pre zariadenia Mac (len v angličtine):

- **AVG AntiVirus** (bezplatný) – táto výkonná aplikácia vám umožňuje kontrolovať konkrétne súbory a priežinky, či neobsahujú vírusy a iné hrozby, alebo dokonca jediným kliknutím spustiť dôkladnú kontrolu celého vášho zariadenia Mac. Taktiež je k dispozícii ochrana v reálnom čase ticho spustená na pozadí. Každý súbor, ktorý otvoríte alebo uložíte, sa automaticky skontroluje bez toho, aby sa vaše zariadenie Mac spomalilo.
- **AVG Cleaner** (bezplatný) – táto aplikácia vám umožňuje vyčistiť všetok nepotrebný neporiadok, ako napríklad súbory z vyrovnávacej pamäte a nevyžiadané súbory, históriu stiahnutých súborov, obsah odpadkového koša, atď., aby ste uvoľnili priestor. Taktiež dokáže nájsť na pevnom disku duplicitné súbory a rýchlo odstrániť nepotrebné kópie.

Jednotlivé kategórie sú takéto:

OCHRANA

Kliknutím na túto dlaždicu zobrazíte informácie týkajúce sa aplikácie **AVG AntiVirus** – informácie o kontrole a jej výsledkoch, a tiež o aktualizáciách definícií vírusov. Taktiež môžete vidieť, či je ochrana v reálnom čase aktívna alebo vypnutá. Ako [administrátor](#) siete máte taktiež možnosť aktualizovať nástroj AVG AntiVirus na vzdialenom zariadení (tlačidlo **Aktualizácia**), alebo zapnúť predtým deaktivovanú ochranu v reálnom čase (prostredníctvom [dialógového okna Správy](#), ku ktorému získate prístup kliknutím na tlačidlo **Zobrazíť podrobnosti**). [Prečítajte si viac o zobrazovaní a správe vzdialených zariadení.](#)



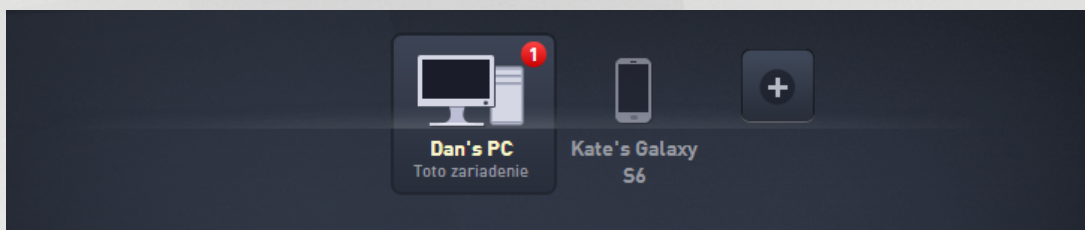
VÝKON

Kliknutím na túto dlaždicu zobrazíte údaje týkajúce sa výkonu, teda údaje o dvoch súčiastkach nástroja **AVG Cleaner** – **Disk Cleaner** a **Duplicate Finder**. Vidíte, kedy naposledy prebehlo testovanie pomocou týchto dvoch nástrojov pre zvýšenie výkonu, a aké boli výsledky.

Tiež by vás mohli zaujímať tieto súvisiace témy:


- [Ako pripojiť zariadenie Mac k existujúcej sieti Zen?](#)
- [Ako zobrazíť a/alebo spravovať produkty AVG?](#)

2.2.2. Pás nástrojov Zariadenia



Táto časť AVG Zen používateľského rozhrania zobrazuje všetky zariadenia dostupné vo vašej Zen sieti. Ak ste [samostatný používateľ](#) alebo ste [pripojení](#) do siete Zen, uvidíte len jedno zariadenie – to, ktoré práve používate. Ako [administrátor](#) siete môžete mať k dispozícii toko zariadení, že budete musieť použiť tlačidlá so šípkami, aby ste si ich mohli všetky zobráť.

Vyberte zariadenie, ktoré chcete zobráť, kliknutím na jeho dlaždicu. Zobrázi sa [oddiel Kategórie](#), ktorý sa príslušne mení a zobrazuje stav produktov AVG na vybranom zariadení. Tiež si môžete všimnúť číslo v oranžovom krúžku zobrazené v pravom hornom rohu niektorých dlaždíc. Toto znamená, že niektoré produkty AVG na tomto zariadení hlásia problémy, ktoré by vás mohli zaujímať. V takom prípade kliknite na [tlačidlo Správy](#), kde nájdete viac informácií.

V roli administrátora siete Zen môžete tiež pridať nové zariadenia do svojej siete. Toto vykonáte tak, že kliknete na tlačidlo  na pravej strane pásu nástrojov. Pozvané zariadenia sa okamžite objavia v pásu nástrojov Zariadenia. Ostanú však neaktívne (v stave "čaká sa") a budú čakať, kým ich používatelia nepřijmú pozvanie.

Taktiež môžete kliknutím pravým tlačidlom myši na akúkoľvek z dlaždíc otvoriť malú kontextovú ponuku, umožňujúcu vám vykonať niektoré činnosti pre vybrané zariadenie:

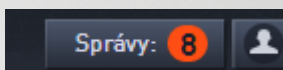
- **Premenova** – názov zariadenia v spodnej časti dlaždice sa stane textovým poľom, aby ste ho mohli upraviť alebo úplne zmeniť.
- **Zmeniť ikonu** – otvorí sa dialógové okno [Nastavenia zariadenia](#), čo vám umožní vybrať si novú ikonu pre zvolené zariadenie (aby ste [zmenili jeho typ](#)).
- **Odstrániť zo siete** – vybrané zariadenie sa odstráni z vašej siete Zen (budete požiadaní o potvrdenie). *Upozorujeme, že nemôžete odstrániť vaše aktuálne zariadenie (to, ktoré práve teraz používate).*



Tiež by vás mohli zaujímať tieto súvisiace témy:

- [Ako pridať zariadenia do svojej siete?](#)
- [Ako odstrániť zariadenia zo svojej siete?](#)
- [Ako prijať pozvánky do siete Zen?](#)

2.2.3. Tlačidlo Správy



Toto tlačidlo sa nachádza nad [pásom nástrojov Zariadenia](#) a na ňavôd od [stavového tlačidla](#). Zobrazuje sa iba v prípade, ak niektorý z produktov AVG na aktuálnom zariadení hlási problém. Číslo vo farebnom kruhu uvádza počet problémov, ktoré by vás mohli zaujímať.

Ako [administrátor siete](#) máte taktiež možnosť prístupu k **dialógovému oknu Správy** vzdialených zariadení tým, že kliknete na tlačidlo **Zobrazí podrobnosti** (v zobrazení dlaždice kategórií). Upozorujeme, že toto tlačidlo je k dispozícii, len ak existujú naliehavé problémy vyžadujúce si vašu pozornosť. [Kliknite sem, aby ste si prečítali o tejto a ďalších možnostiach vzdialenej správy.](#)

Po kliknutí na toto tlačidlo sa zobrazí nové dialógové okno:



Toto dialógové okno zobrazuje zoznam problémov zoradený podľa kategórie produktov. Problémy sú zobrazené rôznymi farbami (červenou, žltou alebo modrou), vďaka čomu rozpoznáte urgentné problémy od tých menej urgentných.

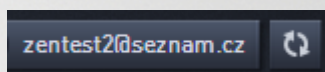


Ak ste [administrátor](#) s viac ako jedným zariadením v sieti, toto dialógové okno bude vyzerá trochu inak. Na ľavej strane nájdete prehľad zariadení, takže môžete zobraziť len problémy týkajúce sa daného zariadenia. Ak chcete vidieť všetky správy od všetkých zariadení v zoradenom zozname, použijete možnosť **VŠETKY ZARIADENIA** (je úplne navrchu v prehľade).

Niektoré problémy je taktiež možné vyriešiť priamo z tohto dialógového okna – vedľa nich sa zobrazuje zvláštny tlačidlo (najčastejšie nazvané **Opraviť teraz**). Ako [administrátor](#) siete môžete opraviť tieto problémy na diaľku, priamo z vášho AVG Zen. Ako [jediný](#) alebo [pripojený používateľ](#) môžete spravovať produkty AVG len na vašom vlastnom zariadení, ale stále je omnoho pohodlnejšie zobrazenie všetkých problémov bez nutnosti otvárať rozhrania jednotlivých aplikácií.

Napríklad, ak vidíte text „**FIREWALL SA MUSÍ REŠTARTOVAŤ – Ak chcete aktivovať Firewall, reštartujte počítač**“, môžete kliknúť na tlačidlo **Reštartovať teraz**. Hneď na to sa počítač reštartuje, aby aktivoval súčasne Firewall.

2.2.4. Stavové tlačidlo



Toto tlačidlo zobrazuje aktuálny [režim používateľa](#). Ako [administrátor](#) siete Zen obvykle uvidíte svoj e-mail zaregistrovaný v úste MyAccount, ktorý ste použili na pripojenie k sieti.

Po kliknutí na toto tlačidlo sa zobrazí zoznam ďalších akcií. Dostupné akcie závisia na [režime používateľa](#), ktorý práve používate:

Ako samostatný používateľ :

- **Pripojiť** – vám umožní [pripojenie k existujúcej sieti Zen](#) (alebo umožní [vytvoriť novú](#)).
- **Zistiť viac** – otvorí novú obrazovku obsahujúcu krátke informácie o AVG Zen a vytvorení siete Zen (taktiež ho môžete použiť na prístup k podrobnejšiemu prehľadu online).
- **Prejsť na úste AVG MyAccount** – spustí prehľad a otvorí webovú lokalitu <https://myaccount.avg.com/>, na ktorej sa môžete prihlásiť ku svojmu účtu AVG MyAccount.

Ako pripojený používateľ :

- **Prihlásiť sa ako administrátor** – prihlásením získate oprávnenia [administrátora](#), ktoré vám umožnia zobrazovať a spravovať túto sieť Zen (vyžaduje sa prihlásenie).
- **Opustiť túto sieť** – kliknutím [opustíte túto sieť Zen](#) (vyžaduje sa potvrdenie).
- **Povedzte mi viac** – zobrazí dialógové okno s informáciami o sieti Zen, ku ktorej ste aktuálne pripojení a ste jej administrátorom.
- **Prejsť na úste AVG MyAccount** – spustí prehľad a otvorí webovú lokalitu <https://myaccount.avg.com/>, na ktorej sa môžete prihlásiť ku svojmu účtu AVG MyAccount.

Ako administrátor:

- **Odhlásiť sa ako administrátor** – kliknutím odhlásite administrátorské práva a prepnete sa do režimu [pripojeného používateľa](#) v rovnakej sieti Zen.
- **Prejsť na úste AVG MyAccount** – spustí prehľad a otvorí webovú lokalitu <https://myaccount.avg.com/>, na ktorej sa môžete prihlásiť ku svojmu účtu AVG MyAccount.



o je ú et AVG MyAccount?

AVG MyAccount je bezplatná internetová (cloudová) služba AVG, ktorá umož ňuje:

- zobrazí informácie o registrovaných produktoch a licenciách
- jednoducho obnoví predplatné a stiahnu produkty
- skontrolova vystavené objednávky a faktúry
- spravova osobné informácie a heslo
- použi AVG Zen

Ú et AVG MyAccount je prístupný priamo na webovej stránke <https://myaccount.avg.com/>.

2.2.4.1. Tri používateľské režimy

V aplikácii AVG Zen sú k dispozícii tri používateľské režimy. Text zobrazený na **stavovom tla idle** závisí na tom, ktorý používateľský režim používate:

- **Samostatný používateľ** (na stavovom tla idle je nápis **Pripoji**) – práve ste nainštalovali nástroj AVG Zen. Váš ú et AVG MyAccount nemá oprávnenia administrátora, nie ste ani pripojení ku žiadnej sieti, takže môžete len zobrazova a spravova produkty AVG nainštalované v tomto zariadení.
- **Pripojený používateľ** (na stavovom tla idle je nápis **Pripoji**) –) – použili ste párovací kód, iže [prijali pozvánku](#) do nie ej siete. Všetky produkty AVG vo vašom zariadení môže zobrazova (a spravova) administrátor siete. Vy sami môžete stále zobrazova a spravova produkty AVG nainštalované v tomto zariadení (ako keby ste boli samostatný používateľ). Ak si už neželáte by pripojení k sieti, môžete [ju jednoducho opusti](#).
- **Administrátor** (na stavovom tla idle je nápis zobrazujúci **názov prihláseného ú tu AVG MyAccount**) – prihlásili [ste sa prostredníctvom ú tu MyAccount](#) (možno ste predtým [vytvorili nový](#)). To znamená, že máte prístup ku všetkým funkciám aplikácie AVG Zen . Môžete [pridáva do svojej siete zariadenia](#), vzdialene zobrazova stav produktov AVG, ktoré sú na nich nainštalované, a v prípade potreby [ich odstráni](#) zo svojej siete. Môžete dokonca vykona rôzne [innosti vykonávané na dia ku](#) na pripojených zariadeniach.

Tiež by vás mohli zaujíma tieto súvisiace témy:

- [Ako prija pozvánky?](#)
- [Ako sa pripoji k existujúcej sieti Zen?](#)
- [Ako vytvorí novú sie Zen?](#)
- [Ako opusti sie ?](#)
- [Ako zobrazí a/alebo spravova produkty AVG?](#)



2.2.5. Tlačidlo Upgradovať/Predĺžiť



Kliknutím na toto malé tlačidlo (napravo od [Stavového tlačidla](#)) otvoríte v prehliadači on-line obchod AVG:

- Ak v súčasnosti používate bezplatný softvér AVG, no chcete vyskúšať prvky a možnosti, ktoré prinášajú iba platené verzie, môžete si prostredníctvom obchodu kúpiť 1 alebo 2-ročné predplatné.
- Ak využívate platený softvér AVG, no platnosť vášho predplatného skoro vyprší (alebo už vypršala), môžete ju obnoviť prostredníctvom obchodu.

Na aktiváciu nového zakúpeného (alebo predĺženého) predplatného je potrebné, aby ste sa prihlásili k svojmu účtu tu [AVG MyAccount](#).

2.2.6. Tlačidlo Obnoviť



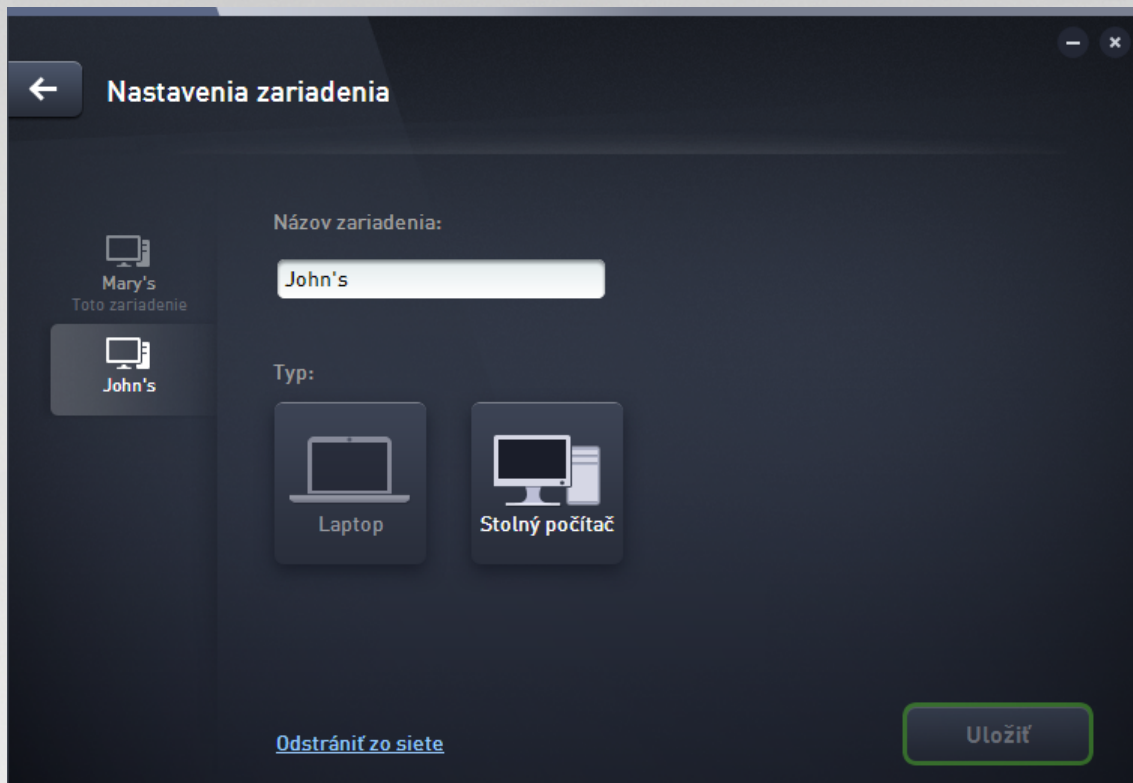
Kliknutím na toto malé tlačidlo (napravo od [tlačidla Upgradovať/Predĺžiť](#)) okamžite obnovíte všetky údaje všetkých [zariadení](#) a [kategórií](#). Toto sa môže hodiť napríklad v prípade, že zariadenie, ktoré ste práve pridali, nie je ešte zobrazené v [páse nástrojov Zariadenia](#), ale vy viete, že je pripojené, a chcete vidieť podrobnosti o tomto zariadení.

2.2.7. Tlačidlo Nastavenia



Kliknutím na toto malé tlačidlo (napravo od tlačidla [Obnoviť](#)) otvoríte malé dialógové okno:

- môžete kliknúť na možnosť **Nastavenia zariadenia**, čím sa otvorí dialógové okno Nastavenia zariadenia, kde môžete [zmeniť názov a typ](#) vášho zariadenia (a tiež ostatných zariadení vo vašej sieti Zen, ak sa v nej nejaké nachádzajú a vy figurujete v sieti [ako administrátor](#)). Toto dialógové okno vám umožní [odstrániť zariadenia z vašej siete](#).



- kliknutím na možnosť **Online podpora** otvoríte [Centrum podpory AVG](#) vo svojom prehliadači. Ak potrebujete pomoc so svojím produktom AVG, táto rozsiahla internetová stránka je skvelým miestom, kde ju zistíte.
- kliknutím na možnosť **Pomocník** získate prístup do tohto pomocníka programu (okno pomocníka môžete tiež kedykoľvek otvoriť stlačením klávesu **F1**).
- Nakoniec môžete kliknúť na možnosť **Informácie AVG Internet Security**, kde nájdete informácie o svojom softvérovom produkte alebo si môžete prečítať Licenčnú zmluvu.

Tiež by vás mohli zaujímať tieto súvisiace témy:

- [Ako zmeniť názov alebo typ zariadenia?](#)
- [Ako odstrániť zariadenia zo svojej siete?](#)



2.2.8. Ikona v paneli úloh

Ikona v paneli úloh (v paneli úloh Windows v pravom dolnom rohu monitora) zobrazuje aktuálny stav produktu AVG Zen. Vždy sa nachádza v paneli úloh bez ohľadu na to, či je [používané rozhranie](#) AVG Zen otvorené alebo zatvorené.



innosti prístupné prostredníctvom ikony v paneli úloh

Ikony v paneli úloh môžete použiť aj na rýchle zobrazenie [používateľského rozhrania](#) AVG Zen. Stačí dvakrát kliknúť na ikonu. Kliknutím pravým tlačidlom myši na ikonu sa otvorí krátko kontextová ponuka, ktorá vám sprístupňuje niektoré z najdôležitejších funkcií:

- **Otvoriť AVG** – použijete toto tlačidlo na otvorenie [AVG Zen](#).
- **Skontrolovať teraz** – použijete toto tlačidlo na okamžité spustenie Kontroly celého počítača.
- **Ochrana** (aktivované /deaktivované ) – použijete tento prepínač, aby ste vyplisústali **AVG Internet Security**, ktoré zabezpečujú ochranu v reálnom čase. Potom budete mať možnosť určiť, ako dlho má byť ochrana **AVG Internet Security** neaktívna. Môžete sa tiež rozhodnúť, či sa má taktiež vypnúť súčasne Firewall. Ochranu **AVG Internet Security** môžete kedykoľvek znova aktivovať – jednoducho znova kliknite na prepínač.

2.3. Sprievodcovia krok za krokom

Táto kapitola obsahuje sprievodcov krok za krokom opisujúcich najbežnejšie inštalácie v prostredí produktu Zen.

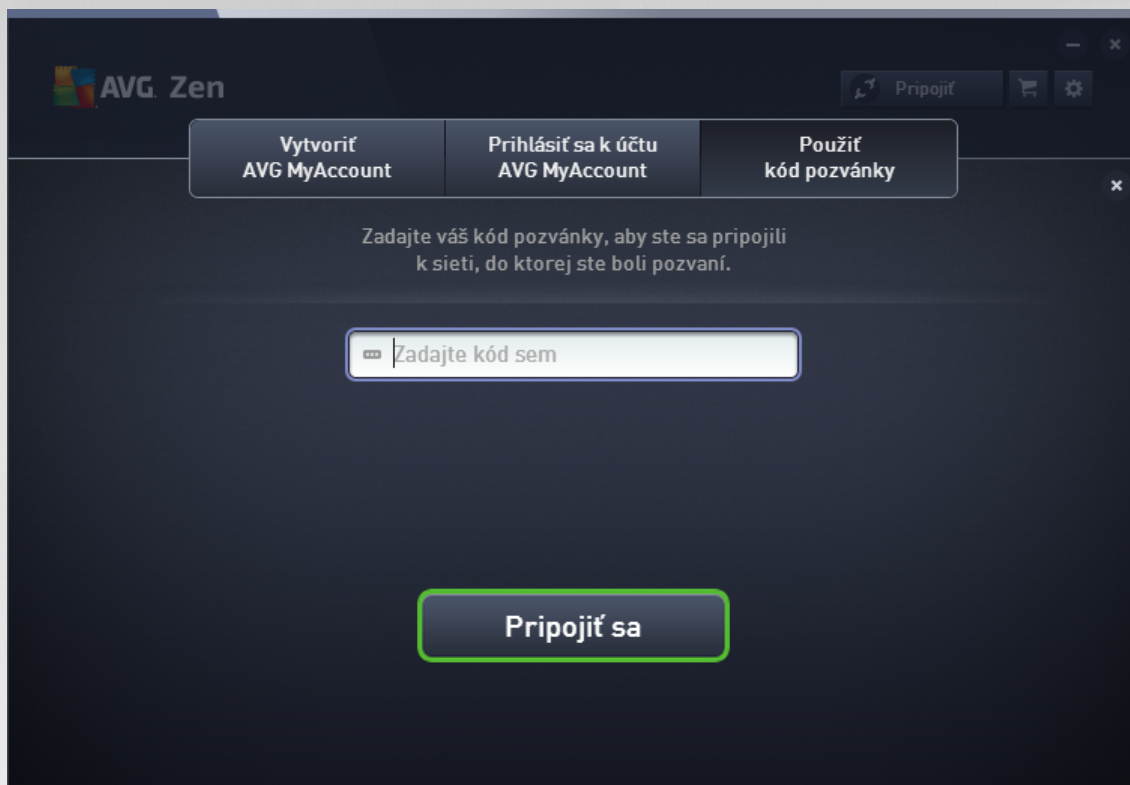
2.3.1. Ako prijať pozvánky?

Ak používate produkty AVG na viac ako jednom zariadení alebo ak nemáte dostatočné skúsenosti a chcete, aby niekto sledoval vaše produkty AVG a pomohol vám s riešením akýchkoľvek problémov, možno budete chcieť pridať svoj počítač alebo mobilné zariadenie s Androidom do existujúcej siete Zen. Najprv však musíte byť pozvaní administrátorom vašej budúcej siete. Musíte ho preto požiadať, aby vám poslal e-mail s pozvánkou. Keď dorazí, otvorte ho a nájdete v ňom **kód pozvánky**.

Ďalší postup závisí na tom, či chcete pridať počítač alebo prenosné zariadenie so systémom Android™:

Počítače:

1. Nainštalujte AVG Zen (ak ste to už neurobili).
2. Kliknite na [stavové tlačidlo](#) (s textom **Pripojiť**) a potvrdte kliknutím na položku **Pripojiť** v malom kontextovom dialógovom okne.
3. Vyberte panel **Použiť kód pozvánky** v novootvorenom dialógovom okne (je to tretia položka, úplne napravo).



4. Pomocou metódy kopírovať /vložiť skopírujte kód pozvánky z e-mailu do príslušného textového poľa v dialógovom okne Zen (alebo ho prepíšte ručne).

Metóda kopírovať /vložiť je bežný postup, ktorý vám umožní vložiť obsah kopírovaný (texty, obrázky atď.) do schránky Windowsu, a potom to vložiť inde. Funguje to takto:

- i. Označíte text, v tomto prípade kód pozvánky v e-maile. Môžete to urobiť podržaním ľavého tlačidla myši alebo klávesu Shift.
- ii. Stlačíte klávesovú skratku **Ctrl + C** na klávesnici (v tejto fáze nemáte viditeľné potvrdenie, že sa text podarilo skopírovať).
- iii. Prejdite na požadované miesto, v tomto prípade dialógové okno Pripojiť sa k sieti Zen, a kliknite na textové pole, do ktorého chcete vložiť text.
- iv. Stlačíte klávesovú skratku **Ctrl + V**.
- v. Zobrazí sa vložený text, v tomto prípade kód pozvánky. Hotovo.

5. Kliknite na tlačidlo **Pripojiť sa**. Po krátkej chvíli sa stanete členom siete Zen, ktorú ste si vybrali. Pre vás osobne sa v skutočnosti nič nezmení (iba text na [stavovom tlačidle](#) sa zmení na **Pripojené**). Vaše zariadenie však bude odteraz monitorované administrátorom siete, vďaka čomu bude môcť zistiť možné problémy a pomôže vám ich vyriešiť. Ak budete chcieť, môžete kedykoľvek jednoducho [opustiť túto sieť](#).

Prenosné zariadenia so systémom Android:

Na rozdiel od počítačov sa pripojenie do siete na prenosných zariadeniach so systémom Android vykonáva priamo z aplikácie:

1. Najprv musíte mať nainštalovanú jednu z mobilných aplikácií AVG, a teda by pripojenie k nejakej sieti Zen ([kliknite sem](#), aby ste zistili viac o pripojení mobilného zariadenia s Androidom k existujúcej sieti Zen). Prijatie pozvánky v mobilnom zariadení v skutočnosti znamená, že zariadenie prestane byť členom



aktuálnej siete Zen a stane sa sú časťou novej.


2. Otvorte aplikáciu a kliknite na **ikonu ponuky** (logo aplikácie) umiestnenú v ľavom hornom rohu hlavnej obrazovky.
3. Keď sa zobrazí ponuka, kliknite na možnosť **Spravova zariadenia**.
4. Kliknite na možnosť **Pripoji sa k inej sieti Zen** úplne na spodnej časti obrazovky. Potom zadajte kód pozvánky, ktorý vám predtým zaslal administrátor tejto siete. Kliknite na tlačidlo **Pripoji**.
5. Gratulujeme! Ste teraz súčasťou siete Zen. Keby ste však niekedy zmenili názor, môžete túto sieť jednoducho kedykoľvek [opustiť](#).

Zariadenia Mac:

Na rozdiel od počítačov sa pripojenie do siete na zariadeniach Mac vykonáva priamo z aplikácie:

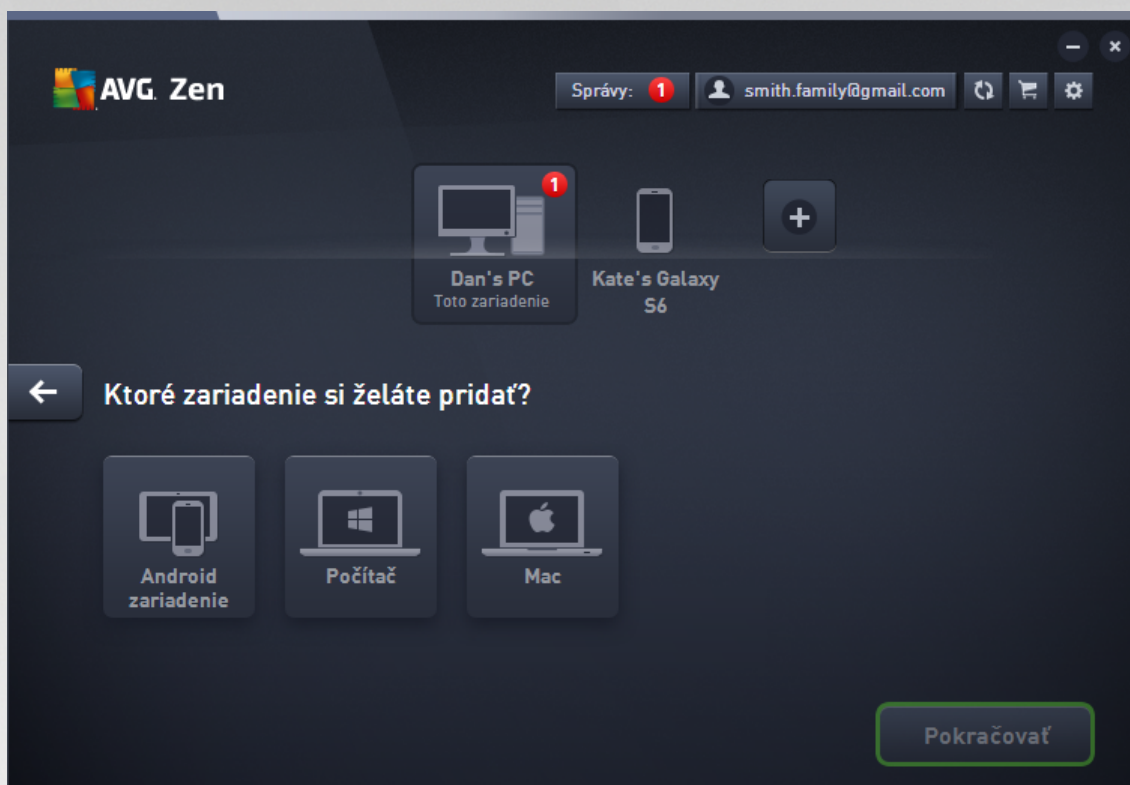
1. Najskôr musíte mať nainštalovanú jednu z aplikácií AVG pre Mac, a teda možno by už pripojení k nejakej sieti Zen ([kliknite sem](#), aby ste zistili viac o pripojení Macu k existujúcej sieti Zen). Ak ste pripojení, kliknite na tlačidlo v pravom hornom rohu obrazovky aplikácií (aktuálne uvádzajúcej stav „Pripojené“) a vyberte z rozbaľovacej ponuky možnosť **Opusti túto sieť**.
2. Tlačidlo v pravom hornom rohu obrazovky aplikácií teraz uvádza stav „Nepripojené“. Kliknite naň a vyberte z rozbaľovacej ponuky možnosť **Pripoji**.
3. V novootvorenom dialógovom okne kliknite na možnosť, ktorá sa nachádza najviac vpravo, **Použi kód pozvánky**.
4. Zobrazí sa textové pole umožňujúce vám zadať kód pozvánky, ktorý vám predtým zaslal administrátor tejto siete. Po zadaní tohto kódu kliknite na tlačidlo **Pripoji**.
5. Gratulujeme! Ste teraz súčasťou siete Zen. Ak keby ste niekedy zmenili názor, môžete túto sieť kedykoľvek [opustiť](#).

2.3.2. Ako pridať zariadenia do svojej siete?

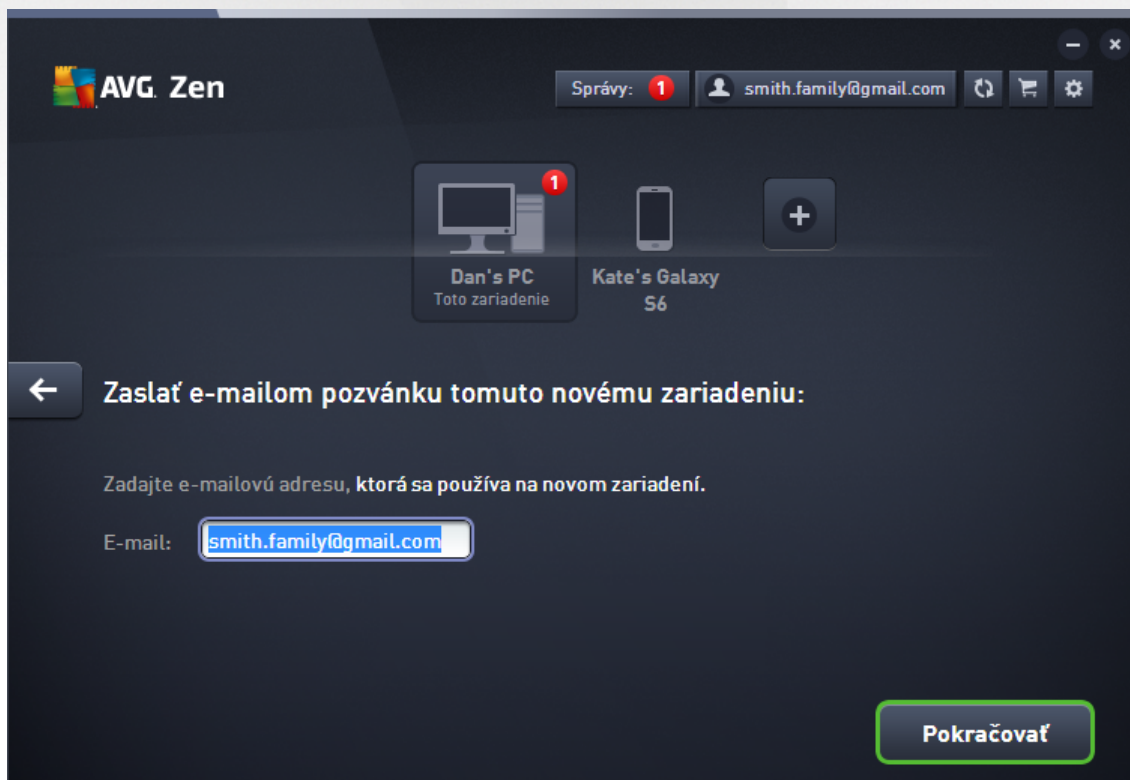
1. Keď chcete pridať zariadenie do svojej siete Zen, musíte zariadenie najprv pozvať. Toto vykonáte tak, že kliknete na tlačidlo  na pravej strane [pásu nástrojov Zariadenia](#).

Upozorujeme, že posielanie pozvánky a pridávanie zariadenia do sietí môžu iba administrátori. Ak nie ste pripojení do žiadnej siete Zen, pripojte sa alebo si vytvorte novú.

2. Zobrazí sa nové dialógové okno. Vyberte typ zariadenia, ktoré chcete pridať (t. j. počítač alebo prenosné zariadenie so systémom Android™) tak, že označíte príslušnú dlaždicu a kliknete na tlačidlo **Pokračovať**.

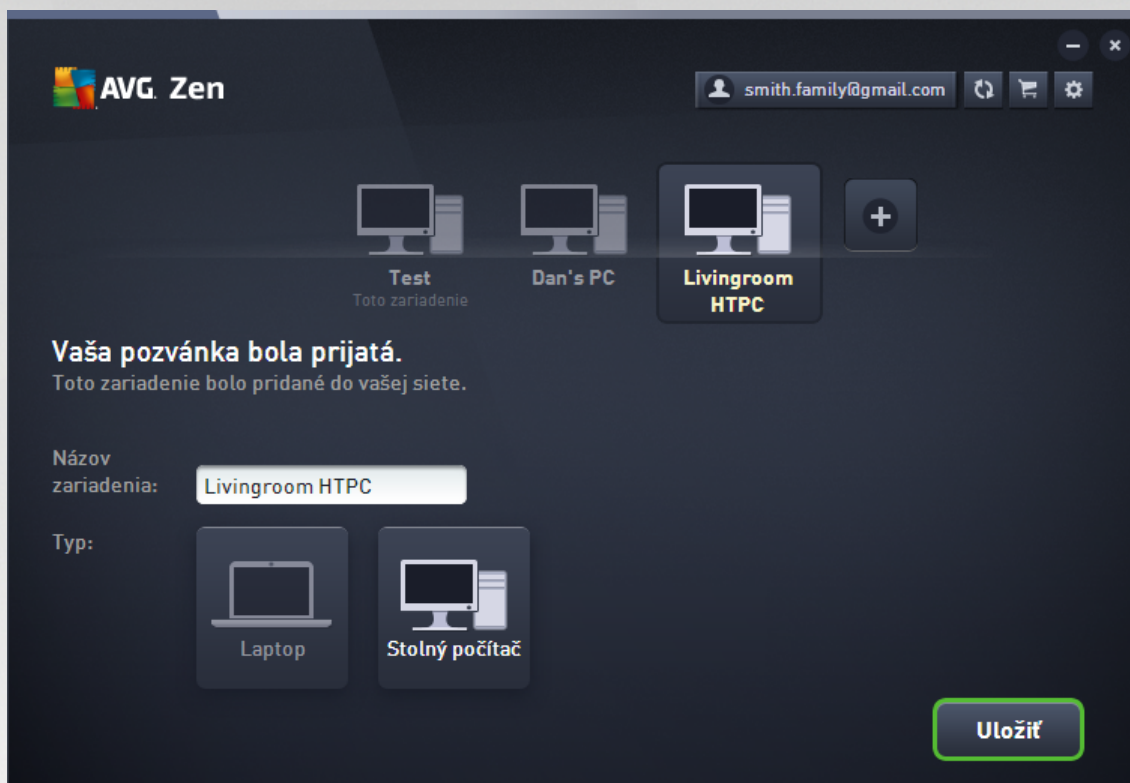


3. Zobrazí sa ďalšie dialógové okno. Zadajte e-mailovú adresu, ktorá sa používa na novom zariadení, a kliknite na tlačidlo **Pokračovať**.





4. E-mail s pozvánkou sa odošle. Zariadenie sa zobrazí v [páse nástrojov Zariadenia](#) ako „ aká sa“. Toto znamená, že sa aká na [prijatie](#) pozvánky.

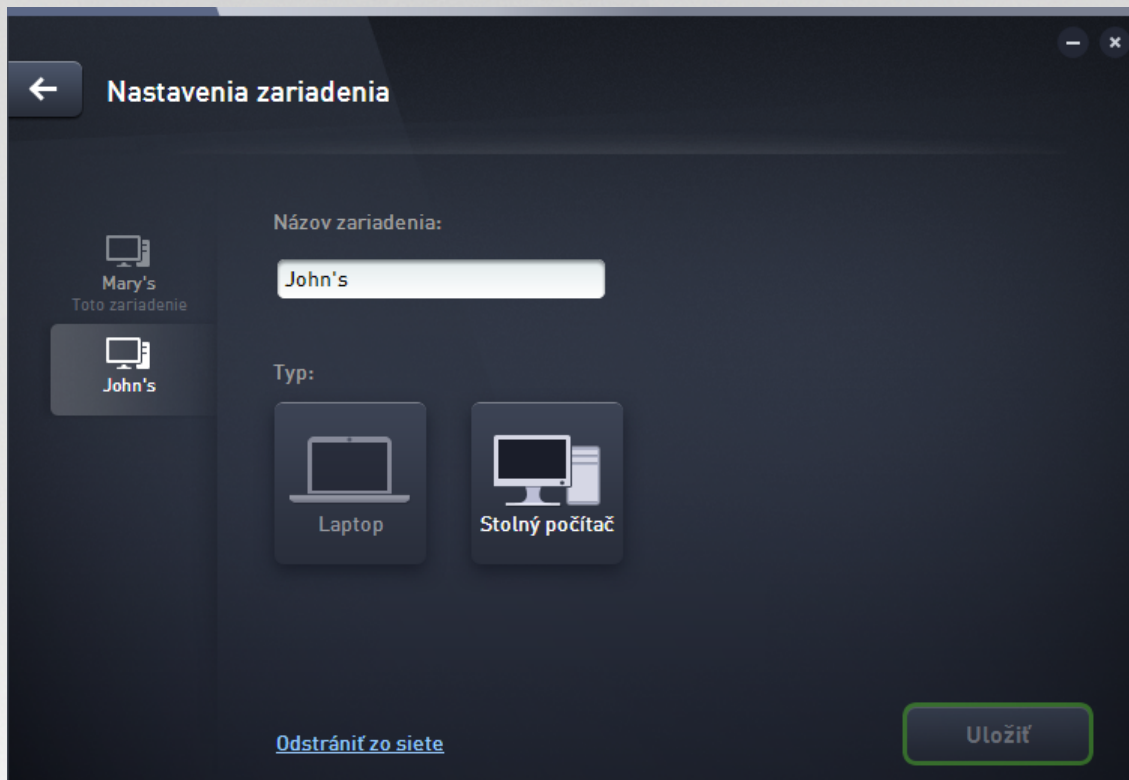


Kým je pozvánka v stave „ aká sa“, môžete **Znovu zasl** odkaz pozvánky alebo úplne **Zruši** pozvánku.

5. Hne po prijatí pozvánky môžete zmeni názov a typ zariadenia, ktoré sa pridalo (toto môžete samozrejme urobi kedyko vek v budúcnosti). Zariadenie je odteraz sú as ou vašej siete Zen a vy môžete na dia ku zobrazí stav produktov AVG, ktoré sú v om nainštalované. Gratulujeme, práve sa z vás stal naozajstný Zen administrátor!

2.3.3. Ako zmeniť názov alebo typ zariadenia?

1. Kliknite na [tlačidlo Nastavenia](#) a potom v kontextovom dialógovom okne vyberte položku **Nastavenia zariadenia**.



2. Zobrazené nastavenia sa týkajú zariadenia, ktoré máte vybrané. V strede s dlaždicami na ľavej strane dialógového okna Nastavenia zariadenia je zobrazený zoznam [zariadení aktuálne dostupných vo vašej sieti](#) (t. j. zariadení, ktoré prijali pozvánku). Medzi zariadeniami prepnete jednoduchým kliknutím na jednotlivé dlaždice.
3. Textové pole **Názov zariadenia** uvádza názov zariadenia, ktoré je aktuálne vybrané. Môžete ho vymazať a nahradiť akýmkoľvek iným názvom.
4. Nižšie môžete nastaviť **Typ** aktuálne vybraného zariadenia (telefón, tablet, notebook alebo stolný počítač). Jednoducho kliknite na príslušnú dlaždicu.
5. Potvrďte zmeny kliknutím na tlačidlo **Uložiť**.

Taktiež môžete kliknúť pravým tlačidlom myši na ktorúkoľvek z dlaždíc zariadení v páske nástrojov Zariadenia a vybrať z kontextovej ponuky buď možnosť **Premenovať**, alebo **Zmeniť ikonu** (tzn. typ).

2.3.4. Ako sa pripojiť k existujúcej sieti Zen?

Počiatočné:

1. Ak nie ste práve prihlásení ku žiadnemu účtu AVG MyAccount, kliknite na [stavové tlačidlo](#) (s nápisom **Pripojiť**) a potvrdte kliknutím na položku **Pripojiť** v malom kontextovom dialógovom okne.



Ak už ste prihlásení k nejakému účtu AVG MyAccount, musíte sa najprv odhlásiť, aby ste sa mohli pripojiť k inému. Kliknite na [stavové tlačidlo](#) (na ktorom je napísaný prihlásený účet AVG MyAccount) a potvrdíte kliknutím na tlačidlo **Odhlásiť sa** v malom dialógovom okne.

2. Vyberte panel **Prihlásiť sa do účtu AVG MyAccount** v novootvorenom dialógovom okne (je to položka v strede).

3. Zadajte svoje používateľské meno a heslo k účtu AVG MyAccount. Ak ešte nemáte účet AVG MyAccount, jednoducho [si vytvorte nový](#). Budete prihlásení ako [administrátor](#), takže si budete môcť zobrazovať produkty AVG na vzdialených zariadeniach v tejto sieti Zen (môžete sa však vždy neskôr odpojiť a zostať v sieti len ako [pripojený používateľ](#)).

Ak ste zabudli svoje heslo, kliknite na odkaz **Zabudli ste heslo?** (pod textovým polom hesla). Budete presmerovaní na webovú stránku, na ktorej môžete obnoviť svoje stratené heslo.

4. Kliknite na tlačidlo **Prihlásiť sa**. Proces pripojenia by sa mal dokončiť v priebehu niekoľkých sekúnd. Po úspešnom pripojení budete vidieť na [stavovom tlačidle](#) názov svojho účtu MyAccount.

Prenosné zariadenia so systémom Android:

Na rozdiel od počítačov sa pripojenie do siete na prenosných zariadeniach so systémom Android vykonáva priamo z aplikácie:

1. Ak chcete pripojiť mobilné zariadenie s Androidom do siete Zen, musíte si stiahnuť jednu z mobilných aplikácií AVG (t. j. AVG AntiVirus, AVG Cleaner a/alebo AVG PrivacyFix). Toto môžete urobiť jednoducho v obchode Google Play, kde sú k dispozícii na stiahnutie všetky tieto aplikácie zdarma. Aby spojenie



fungovalo správne, musíte mať nainštalovanú najnovšiu dostupnú verziu.

2. Aplikáciu AVG po nainštalovaní otvorte a kliknite na **ikonu ponuky** (logo aplikácie) umiestnenú v ľavom hornom rohu hlavnej obrazovky.
3. Keď sa zobrazí ponuka, kliknite na možnosť **Spravova zariadenia**.
4. Tu kliknite na kartu **Prihlásenie** a zadajte príslušné prihlasovacie údaje útu AVG MyAccount (t. j. vaše **používateľské meno** a **heslo**).
5. Gratulujeme! Ste teraz súčasťou siete Zen. Po kliknutí na ikonu ponuky by ste mali v hornej časti ponuky vidieť text **Pripojené ako:** spolu s názvom prihláseného útu AVG MyAccount. Ak keby ste niekedy zmenili názor, môžete túto sieť kedykoľvek [opustiť](#).

Zariadenia Mac:

Na rozdiel od počítačov sa pripojenie do siete na zariadeniach Mac vykonáva priamo z aplikácie:

1. Ak chcete pripojiť zariadenie Mac do siete Zen, musíte si stiahnuť jednu z mobilných aplikácií AVG (t. j. AVG AntiVirus a/alebo AVG Cleaner). Môžete to jednoducho vykonať napríklad v [Centre sťahovania AVG](#) alebo v obchode Mac App Store, odkiaľ je možné všetky tieto aplikácie stiahnuť a nainštalovať zadarmo. Aby spojenie fungovalo správne, musíte mať nainštalovanú najnovšiu dostupnú verziu.
2. Po nainštalovaní aplikácie AVG ju otvorte. V pravom hornom rohu obrazovky aplikácií uvidíte obdĺžnikové tlačidlo (teraz uvádza stav „Nepripojené“). Kliknite naň a vyberte z rozbaľovacej ponuky možnosť **Pripojiť**.
3. V novootvorenom dialógovom okne kliknite na možnosť v strede **Prihlásiť sa k útu AVG MyAccount** (mala by už byť predvolená).
4. Zadajte príslušné prihlasovacie údaje útu AVG MyAccount, teda vaše **používateľské meno** (e-mail útu MyAccount) a **heslo**.
5. Gratulujeme! Ste teraz súčasťou siete Zen. Tlačidlo v pravom hornom rohu uvádza teraz stav „Pripojené“. Ak naň kliknete, uvidíte, ku ktorej sieti ste práve pripojení. Keby ste niekedy zmenili názor, môžete túto sieť jednoducho kedykoľvek [opustiť](#).

2.3.5. Ako vytvoriť novú sieť Zen?

Aby ste mohli vytvoriť (a [spravovať](#)) novú sieť Zen, musíte najskôr vytvoriť svoj osobný účet AVG MyAccount. Existujú dva spôsoby: prostredníctvom webového prehliadača a alebo priamo z aplikácie AVG Zen.

Z prehliadača:

1. V prehliadači otvorte webovú stránku <https://myaccount.avg.com/>.
2. Kliknite na tlačidlo **Vytvoriť účet AVG MyAccount**.
3. Zadajte svoj prihlasovací e-mail, svoje heslo dvakrát a kliknite na tlačidlo **Vytvoriť účet**.
4. Pošleme vám odkaz na aktiváciu útu AVG MyAccount (na e-mailovú adresu zadanú v kroku 3). Pre dokončenie vytvárania útu MyAccount budete musieť kliknúť na tento odkaz. Ak tento e-mail nenájdete v doručenej pošte, môže byť medzi nevyžiadanými správami.



Od AVG Zen:

1. Ak nie ste práve prihlásení ku žiadnemu účtu AVG MyAccount, kliknite na [stavové tlačidlo](#) (s nápisom **Pripoji**) a potvrdíte kliknutím na položku **Pripoji** v malom kontextovom dialógovom okne.

Ak už ste prihlásení k nejakému účtu AVG MyAccount, musíte sa najprv odhlásiť, aby ste sa mohli pripojiť k inému. Kliknite na [stavové tlačidlo](#) (na ktorom je napísaný prihlásený účet AVG MyAccount) a potvrdíte kliknutím na tlačidlo **Odhlásiť sa** v malom dialógovom okne.

2. Ubezpečte sa, že je vybraný panel **Vytvoriť účet AVG MyAccount** v novootvorenom dialógovom okne (mal by byť už predvolene vybraný).

3. Zadajte svoj prihlasovací e-mail, nastavte si heslo a potom kliknite na tlačidlo **Vytvoriť účet**.
4. Po niekoľkých sekundách budete pripojení k novovytvorenej sieti s oprávneniami [administrátora](#). To znamená, že môžete [pridávať do svojej siete zariadenia](#), vzdialene zobrazovať produkty AVG, ktoré sú na nich nainštalované, a v prípade potreby [ich odstrániť](#) zo svojej siete (môžete sa však vždy neskôr odpojiť a zostať v sieti len ako [pripojený používateľ](#)).

2.3.6. Ako nainštalovať produkty AVG?

1. Pomocou aplikácie Zen môžete jednoducho nainštalovať produkty AVG. Toto vykonáte kliknutím na dlaždicu [Kategória](#) pod a vášho výberu (dlaždica bude sivá, čo znamená, že nie je ešte nainštalovaný žiadny produkt z danej kategórie; môže byť polovicou zelená, čo znamená, že máte produkt z tejto kategórie, ale existuje iný produkt, ktorý by ste mohli nainštalovať).



2. Ak chcete rovno spustiť inštaláciu produktu, stačí kliknúť na tlačidlo **Získajte ho BEZPLATNE**. Produkt sa potom nainštaluje automaticky s predvolenými nastaveniami.

Ak chcete sami prejsť inštaláciou nainštalovaným procesom, kliknite na malé tlačidlo so šípkou (na pravej strane tlačidla **Získajte ho BEZPLATNE**) a kliknite na položku **Vlastná inštalácia**. Takto uvidíte inštaláciu ako postupnosť dialógových okien a budete môcť zmeniť niektoré nastavenia, inštalované sú všetky a pod.

Inštalované procesy rôznych produktov spoločnosti AVG sú podrobne popísané v ďalšej časti tejto dokumentácie alebo dokonca v samostatných používateľských sprievodcoch. Týchto sprievodcov si môžete jednoducho stiahnuť z [webovej lokality spoločnosti AVG](#).

3. V priebehu inštalácie sa v dlaždici príslušnej [Kategórie](#) zobrazí zelený krúžok. Po úspešnom dokončení inštalácie sa zelený krúžok v dlaždici zmení na plný (v niektorých kategóriách nemusí byť úplný, čo znamená, že v tejto kategórii sú produkty, ktoré môžete nainštalovať). Tento krúžok (alebo neúplný krúžok) môže hneď po dokončení inštalácie zmeniť farbu (žltá alebo červená), čo znamená, že je potrebná vaša pozornosť na vyriešenie nejakého problému.
4. Zobrazí sa správa potvrdzujúca, že bola inštalácia dokončená úspešne (priamo pod dlaždicami [Kategórii](#)).

2.3.7. Ako opustiť sieť?

Počítač:

1. Ak ste členom nejakej siete Zen a chcete ju opustiť, je to veľmi jednoduché. Zaujmite tým, že kliknete na [stavové tlačidlo](#) (s nápisom **Pripojené**) a potom kliknete na tlačidlo **Opustiť túto sieť** v malom dialógovom okne.



2. Teraz musíte potvrdiť, že naozaj chcete opustiť sieť Zen. Toto vykonáte kliknutím na tlačidlo **Opustiť**.
3. Po niekoľkých sekundách sa od siete definitívne odpojíte. Administrátor opustenej siete už nebude môcť spravovať produkty AVG vo vašom počítači. Nápis na [stavovom tlačidle](#) sa zmení na **Pripojiť** (t.j. po iato nový stav).

Prenosné zariadenia so systémom Android:

Na rozdiel od počítačov sa pripojenie do siete na prenosných zariadeniach so systémom Android vykonáva priamo z aplikácie:

1. Otvorte aplikáciu AVG a kliknite na **ikonu ponuky** (logo aplikácie) umiestnenú v ľavom hornom rohu hlavnej obrazovky.
2. V hornej časti ponuky uvidíte text **Pripojené ako:** spolu s názvom vášho účtu AVG MyAccount. Vedľa neho je malá ikona dverí so šípkou ukazujúcou doprava. Kliknite na ňu.
3. Potvrďte, že naozaj chcete opustiť sieť Zen tak, že kliknete na tlačidlo **OK**.
4. Po niekoľkých sekundách sa od siete definitívne odpojíte. Administrátor opustenej siete už nebude môcť spravovať produkty AVG na vašom prenosnom zariadení so systémom Android™. Potom sa však môžete jednoducho pripojiť do tejto (alebo ktorejkoľvek inej) siete Zen znova – či už [priamo](#) alebo [prijatím pozvánky](#).

Zariadenia Mac:

Na rozdiel od počítačov sa pripojenie do siete na zariadeniach Mac vykonáva priamo z aplikácie:

1. Otvorte svoju aplikáciu AVG a kliknite na obdĺžnikové tlačidlo v pravom hornom rohu obrazovky aplikácií (teraz uvádzajúcej stav „Pripojené“).
2. V hornej časti rozbaľovacej ponuky uvidíte text **Ste pripojení k nasledujúcej sieti Zen:** spolu s názvom vášho účtu AVG MyAccount.
3. Priamo pod informáciami o sieti Zen sa nachádza možnosť **Opustiť túto sieť**. Kliknite na ňu.
4. Po niekoľkých sekundách sa od siete definitívne odpojíte. Administrátor opustenej siete už nebude môcť spravovať produkty AVG vo vašom zariadení Mac. Potom sa však môžete jednoducho pripojiť do tejto (alebo ktorejkoľvek inej) siete Zen znova – či už [priamo](#) alebo [prijatím pozvánky](#).

2.3.8. Ako odstrániť zariadenia zo svojej siete?

1. Ak nechcete, aby niektoré zariadenie bolo súčasťou vašej siete Zen, môžete ho jednoducho odstrániť. Kliknite na [tlačidlo Nastavenia](#) a potom v kontextovom dialógovom okne vyberte položku **Nastavenia zariadenia**.
2. Na ľavej strane dialógového okna Nastavenia zariadenia je uvedený zoznam [zariadení aktuálne dostupných vo vašej sieti](#), zobrazený ako špecifické dlaždice. Prepnite na zariadenie, ktoré chcete odstrániť – kliknite na dlaždicu s jeho názvom.
3. Pri dolnej hrane dialógového okna uvidíte odkaz **Odstrániť zo siete**. Kliknite na ňu.

Poznámka: pri zariadení, ktoré aktuálne používate takýto odkaz nie je uvedený. Toto zariadenie sa považuje



za hlavný prvok vašej siete, a preto ho nemôžete odstrániť .

4. Teraz musíte potvrdiť , že chcete toto zariadenie naozaj odstrániť zo siete Zen. Toto vykonáte kliknutím na tlačidlo **Odstrániť** .
5. Zariadenie bude za niekoľko sekúnd definitívne odstránené. Už nebudete môcť spravovať produkty AVG, ktoré sú v ňom nainštalované; odstránené zariadenie tiež zmizne z [pásu nástrojov Zariadenia](#) vo vašom používateľskom rozhraní.

alším spôsobom, ako odstrániť zariadenie, je kliknúť pravým tlačidlom myši na jeho dlaždicu v [páse nástrojov Zariadenia](#) a vybrať z kontextovej ponuky možnosť **Odstrániť zo siete**. Teraz musíte opäť potvrdiť , že chcete naozaj vykonať túto úlohu (t. j. kliknúť na tlačidlo **Odstrániť**).

2.3.9. Ako zobrazíť a/alebo spravovať produkty AVG?

Ak si chcete prezrieť a spravovať svoje vlastné zariadenie

Jediné, čo musíte urobiť je kliknúť na dlaždicu príslušnej [kategórie](#). Tým otvoríte používateľské rozhranie produktu AVG, v ktorom si môžete prezrieť a konfigurovať všetky možnosti. Napríklad kliknutím na dlaždicu **OCHRANA** otvoríte používateľské rozhranie aplikácie AVG Internet Security a pod. Ak je v kategórii viac produktov, po kliknutí na jej dlaždicu môžete vybrať z dlaždíc týchto produktov (napríklad AVG PrivacyFix v kategórii **SÚKROMIE A IDENTITA**).

Produkty spoločnosti AVG, ktoré si môžete prezrieť a spravovať prostredníctvom nástroja Zen, sú podrobne popísané v ďalšej časti tejto dokumentácie alebo aj v samostatných používateľských sprievodcoch. Môžete ich stiahnuť z webovej lokality [spoločnosti AVG](#).

V prípade, že existujú dôležité problémy vyžadujúce vašu pozornosť , môžete kliknúť na [tlačidlo Správy](#). Novootvorené dialógové okno zobrazuje zoznam problémov. Niektoré z nich sa dajú vyriešiť priamo v tomto dialógovom okne – v takom prípade sa vedľa nich zobrazí špeciálne tlačidlo.

Ak chcete prezrieť a spravovať vzdialené zariadenie (iba pre administrátorov)

Toto je tiež veľmi jednoduché. Z [pásu nástrojov Zariadenia](#) vyberte zariadenie, ktoré si chcete prezrieť a kliknite na [dlaždicu príslušnej kategórie](#). Následne sa otvorí nové dialógové okno zobrazujúce stručný prehľad stavov produktov AVG v tejto kategórii.



Ako [administrátor](#) môžete použiť viacero tlačidiel, aby ste vykonali rôzne činnosti vykonávané na diaľku v produktoch AVG vo vašej sieti Zen. Dostupné činnosti závisia od typu vášho zariadenia ([počítač](#), [Android](#) alebo [počítač Mac](#)) a [dlaždice kategórie](#), ktorú si aktuálne prezeráte. Upozorujeme, že niektoré činnosti (ako napríklad kontrola či aktualizácia) nemusia byť k dispozícii, ak už boli pomerne nedávno vykonané. Nižšie sú uvedené všetky dostupné činnosti vykonávané na diaľku pre produkty AVG:

TYP ZARIADENIA	DLAŽDICE KATEGÓRIÍ	DOSTUPNÉ ČINNOSTI VYKONÁVANÉ NA DIAĽKU
Počítač	OCHRANA (AVG Internet Security)	<ul style="list-style-type: none"> • Tlačidlo Skontrolovať teraz – kliknutím na ňu okamžite spustíte kontrolu, ktorá zistí, či sa na vzdialenom zariadení nenachádzajú vírusy a iný škodlivý softvér. Po dokončení kontroly budete okamžite informovaní o jej výsledkoch. Kliknite sem, aby ste sa dozvedeli viac o kontrole v rámci nástroja AVG Internet Security. • Tlačidlo Aktualizácia – kliknutím na ňu spustíte na vzdialenom zariadení proces aktualizácie nástroja AVG Internet Security. Všetky antivírusové aplikácie by mali vždy byť udržiavané aktuálne, aby ste zabezpečili maximálnu úroveň ochrany. Kliknite sem, aby ste sa dozvedeli viac o dôležitosti aktualizácií v rámci nástroja AVG Internet Security. • Tlačidlo Zobrazí podrobnosti – toto tlačidlo je k dispozícii len

TYP ZARIADENIA	DLAŽDICE KATEGÓRIÍ	DOSTUPNÉ FUNKCIE VYKONÁVANÉ NA ZARIADENÍ
		<p>ak existujú naliehavé problémy vyžadujúce si vašu pozornosť. Kliknutím na ikonu otvoríte dialógové okno Správy aktuálne vybraného zariadenia. Toto dialógové okno zobrazuje zoznam problémov zoradený podľa kategórie produktov. Niektorí z nich je možné ihneď vyriešiť kliknutím na tlačidlo Opraviť teraz. V nastroji AVG Internet Security môžete napríklad zapnúť predtým vypnuté služby ochrany.</p>
Počítač	VÝKON – AVG PC TuneUp	<ul style="list-style-type: none"> • Tlačidlo Spustiť údržbu – kliknutím na tlačidlo spustíte údržbu systému – súbor rôznych úloh vytvorených na optimalizáciu systému na vzdialenom zariadení, jeho zrýchlenie a optimalizáciu jeho výkonu. • Tlačidlo Aktualizácia – kliknutím na tlačidlo spustíte na vzdialenom zariadení proces aktualizácie nástroja AVG PC TuneUp. Je veľmi dôležité, aby ste udržiavali nástroj AVG PC TuneUp aktuálny, keďže jeho jednotlivé služby sa neustále rozširujú a prispôbujú tak, aby vyhovovali najnovším technológiám a boli opravené chyby. • Tlačidlo Zobrazí podrobnosti – toto tlačidlo je k dispozícii len ak existujú naliehavé problémy vyžadujúce si vašu pozornosť. Kliknutím na ikonu otvoríte dialógové okno Správy aktuálne vybraného zariadenia. Toto dialógové okno zobrazuje zoznam problémov zoradený podľa kategórie produktov. Niektorí z nich je možné ihneď vyriešiť kliknutím na tlačidlo Opraviť teraz.
Android	OCHRANA (AVG AntiVirus)	<ul style="list-style-type: none"> • Tlačidlo Skontrolovať teraz – kliknutím na tlačidlo okamžite spustíte kontrolu, ktorá zistí, či sa na vzdialenom zariadení so systémom Android nenachádzajú vírusy a iný škodlivý obsah. Po dokončení kontroly budete okamžite informovaní o jej výsledkoch. • Tlačidlo Aktualizácia – kliknutím na tlačidlo spustíte na vzdialenom zariadení so systémom Android proces aktualizácie nástroja AVG AntiVirus. Všetky antivírusové aplikácie by mali vždy byť udržiavané aktuálne, aby ste zabezpečili maximálnu úroveň ochrany. • Tlačidlo Zobrazí podrobnosti – toto tlačidlo je k dispozícii len ak existujú naliehavé problémy vyžadujúce si vašu pozornosť. Kliknutím na ikonu otvoríte dialógové okno Správy aktuálne vybraného zariadenia. Toto dialógové okno zobrazuje zoznam problémov zoradený podľa kategórie produktov. Toto dialógové okno však v prípade nástroja AVG AntiVirus pre Android obsahuje iba informácie a neumožňuje vykonanie žiadnej zmeny.
Mac	OCHRANA (AVG AntiVirus)	<ul style="list-style-type: none"> • Tlačidlo Aktualizácia – kliknutím na tlačidlo spustíte na vzdialenom zariadení Mac proces aktualizácie nástroja AVG AntiVirus. Všetky antivírusové aplikácie by mali vždy byť udržiavané aktuálne, aby ste



TYP ZARIADENIA	DLAŽDICE KATEGÓRIÍ	DOSTUPNÉ INNOSTI VYKONÁVANÉ NA DIAĽKU
		<p>zabezpečiť alebo maximálnu úroveň ochrany.</p> <ul style="list-style-type: none"> • Tlačidlo Zobrazí podrobnosti – toto tlačidlo je k dispozícii len ak existujú naliehavé problémy vyžadujúce si vašu pozornosť. Kliknutím naň otvoríte dialógové okno Správy aktuálne vybraného zariadenia. Toto dialógové okno zobrazuje zoznam problémov zoradený podľa kategórie produktov. V prípade nástroja AVG AntiVirus pre Mac môžete použiť tlačidlo Opraviť teraz, aby ste zapli predtým deaktivovanú ochranu v reálnom čase.

2.4. FAQ a podpora

Používate ská podpora programu AVG Zen je vám kedykoľvek k dispozícii. Stačí kliknúť na tlačidlo [Nastavenia](#) zvolí možnosť **Podpora**.

Vo vašom prehliadači sa otvorí stránka [AVG Support Center](#). Táto stránka vám sprístupní profesionálnu podporu používateľov spoločnosti AVG. Môžete sa opýtať otázky týkajúce sa licencií, inštalácie, vírusov a špecifických funkcií produktu. Ak potrebujete pomoc s produktom spoločnosti AVG, toto je to správne miesto, kde začať.

Ak chcete získať úplné informácie o AVG Zen, navštívte stránku www.avg.com/zen.

Ak ste off-line a máte problém s pripojením sa späť k internetu, kontaktujte oddelenie pomoci vášho poskytovateľa internetového pripojenia. Bez pripojenia k internetu nebude AVG Zen fungovať správne, a taktiež nebudú k dispozícii jeho možnosti podpory.



3. AVG Internet Security

Táto časť príručky podrobne dokumentuje produkt **AVG Internet Security**.

Môžete využiť aj ďalšie zdroje informácií:

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



3.1. Proces inštalácie AVG

Na nainštalovanie programu **AVG Internet Security** do počítača sa musí použiť najnovší inštalovaný súbor. Aby ste sa uistili, že inštalujete najnovšiu verziu aplikácie **AVG Internet Security**, odporúčame vám stiahnuť inštalovaný súbor priamo z webovej lokality spoločnosti AVG (<http://www.avg.com/>). V časti **Podpora** sa nachádza štruktúrovaný prehľad inštalovaných súborov pre každú z edícií AVG. Po stiahnutí a uložení inštalovaného súboru na váš 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. Okrem toho ale ponúkame podrobné vysvetlenia každého z dialógových okien:

3.1.1. Vitajte!

Proces inštalácie začína dialógovým oknom **Víta vás AVG Internet Security**:



Výber jazyka

V tomto dialógovom okne zvolíte jazyk, ktorý sa použije pri procese inštalácie. Kliknutím na rozbaľovacie pole pri možnosti **Jazyk** zobrazíte ponuku jazykov. Vyberte požadovaný jazyk a proces inštalácie bude pokračovať alej v jazyku podľa vášho výberu. Aplikácia bude taktiež komunikovať vo vybranom jazyku, pričom budete mať možnosť prepnúť do angličtiny, ktorá sa vždy inštaluje automaticky.

Licenčná zmluva s koncovým používateľom a Ochrana osobných údajov

Odporúčame vám, aby ste sa pred tým, ako budete pokračovať v procese inštalácie, zoznámili s dokumentmi **Licenčná zmluva s koncovým používateľom** a **Ochrana osobných údajov**. Prístup k obom dokumentom získate prostredníctvom aktívnych odkazov v spodnej časti dialógového okna. Kliknite na ktorýkoľvek z hypertextových odkazov, aby ste otvorili nové dialógové okno/nové okno prehliadača, v ktorom bude uvedené plné znenie príslušnej listiny. Pozorne si prečítajte tieto právne záväzné dokumenty. Kliknutím na tlačidlo **Pokračovať** potvrdíte, že súhlasíte s týmito dokumentmi.



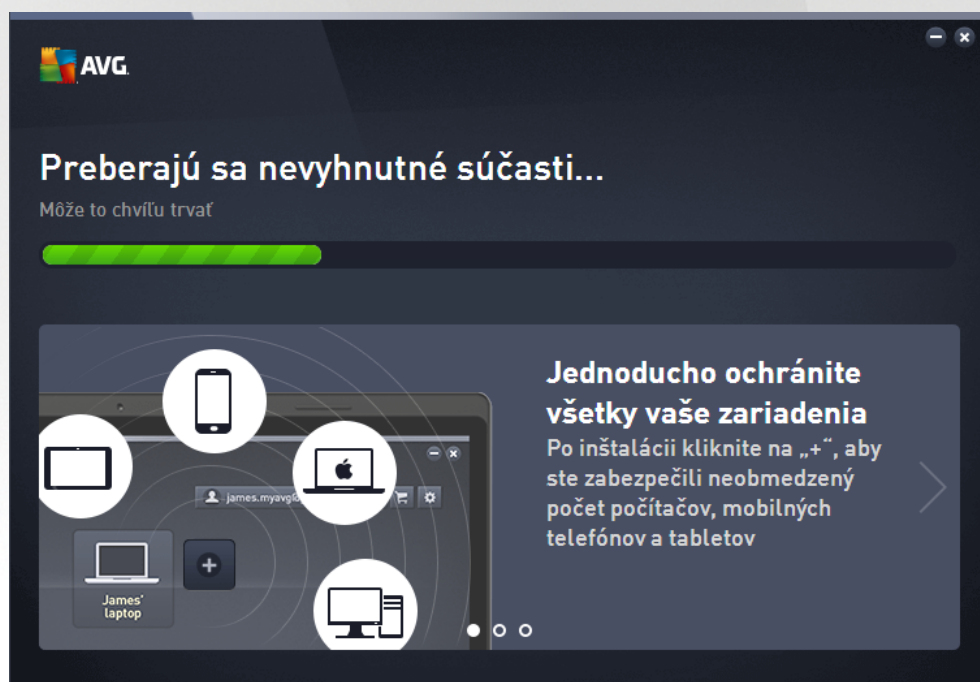
Pokračujte v inštalácii

Na pokračovanie inštalácie jednoducho kliknite na tlačidlo **Pokračovať**. Budete požiadaní o vaše licenčné číslo a potom bude inštalácia v plne automatickom režime. Pre vásinu používate sa odporúča, aby použili túto štandardnú možnosť inštalácie **AVG Internet Security**, v ktorej všetky nastavenia vopred definoval dodávateľ programu. Táto konfigurácia poskytuje maximálne zabezpečenie s optimálnym využitím zdrojov. Ak v budúcnosti budete potrebovať zmeniť konfiguráciu, vždy to bude možné priamo v aplikácii.

Prípadne máte k dispozícii možnosť **Vlastná inštalácia**, a to vo forme hypertextového odkazu umiestneného pod tlačidlom **Pokračovať**. Vlastnú inštaláciu by mali používať len skúsení používatelia, ktorí majú skutočný dôvod inštalovať aplikáciu s neštandardnými nastaveniami, napríklad na účely prispôbenia konkrétnym systémovým potrebám. Ak sa rozhodnete pre tento spôsob, po vyplnení licenčného čísla budete presmerovaní na dialógové okno **Prispôbiť inštaláciu**, kde môžete zadať svoje nastavenia.

3.1.2. Inštalácia AVG

Po potvrdení spustenia inštalácie v predchádzajúcom dialógovom okne sa spustí proces inštalácie v plne automatickom režime a nevyžaduje žiadne zásahy:



Po dokončení procesu inštalácie vám bude ponúknutá možnosť vytvoriť si svoj sieťový útvar – podrobnosti si pozrite v kapitole nazvanej **Ako vytvoriť novú sieť Zen?**

3.2. Po inštalácii

3.2.1. Aktualizácia vírusovej databázy

Upozorujeme, že po inštalácii (po reštarte počítača, ak sa vyžaduje) **AVG Internet Security** automaticky aktualizuje svoju vírusovú databázu a všetky súčasti a pripravuje ich na použitie. To môže trvať niekoľko minút. Keď proces aktualizácie prebieha, budete na to upozornení informáciou, ktorá sa zobrazí v hlavnom dialógovom okne. Počkajte chvíľu, pokiaľ neskončí proces aktualizácie a nebudete mať **AVG Internet Security** úplne spustený a pripravený na to, aby vás chránil!



3.2.2. Registrácia produktu

Po nainštalovaní produktu **AVG Internet Security** 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**. Označte položku [v hornom navigačnom pruhu Možnosti/Zaregistrujte teraz](#). Budete presmerovaní na stránku **Registrácia** na webovej lokalite AVG (<http://www.avg.com/>). Postupujte podľa pokynov na tejto stránke.

3.2.3. Otvorenie používateľského rozhrania

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

- dvakrát kliknite na ikonu AVG Internet Security v paneli úloh,
- dvakrát kliknite na ikonu AVG Protection na pracovnej ploche,
- z ponuky *Štart/Všetky programy/AVG/AVG Protection*.

3.2.4. Kontrola celého počítača

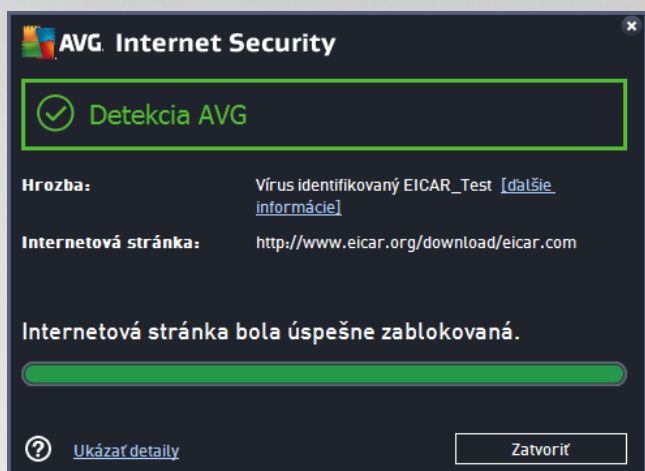
Existuje potenciálne riziko, že sa do vášho počítača dostal vírus ešte pred nainštalovaním produktu **AVG Internet Security**. Z tohto dôvodu by ste mali spustiť [Kontrolu celého počítača](#), aby sa vylúčila možnosť existencie infekcie v počítači. Prvá kontrola môže trvať (približne hodinu), no odporúčame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

3.2.5. Test EICAR

Pre potvrdenie správnej inštalácie **AVG Internet Security** môžete vykonať 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. Väšina produktov na ň reaguje ako keby išlo o vírus (aj keď ho obyčajne označujú jasným názvom, ako napríklad „EICAR-AV-Test“). Vírus EICAR si môžete stiahnuť na internetových stránkach EICAR na adrese www.eicar.com, kde nájdete aj všetky potrebné informácie o teste EICAR.

Stiahnite si súbor *eicar.com* a uložte ho na pevný disk počítača. Hneď po potvrdení stiahnutia testovacieho súboru **AVG Internet Security** na ň zareaguje varovaním. Zobrazenie tohto oznámenia znamená, že program AVG správne nainštalovaný v počítači.



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

3.2.6. Predvolená konfigurácia AVG

Predvolenú konfiguráciu, (t. j. nastavenie aplikácie bezprostredne po inštalácii) produktu **AVG Internet Security**, 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](#).

3.3. Používateľské rozhranie AVG

AVG Internet Security otvorí hlavné okno:



Hlavné okno je rozdelené na niekoľko častí:



- **Navigácia v hornom riadku** obsahuje štyri aktívne odkazy zoradené v hornej časti hlavného okna (*alšie produkty od AVG, Správy, Podpora, Možnosti*). [Podrobnosti >>](#)
- **Informácie o stave zabezpečenia** je časť so základnými informáciami o aktuálnom stave vášho **AVG Internet Security**. [Podrobnosti >>](#)
- **Prejsť na tlačidlo Zen** otvorí hlavné používateľské rozhranie aplikácie ZEN, kde môžete na jednom mieste spravovať ochranu, výkon a súkromie na všetkých elektronických zariadeniach, ktoré používate.
- **Prehľad nainštalovaných súčastí** nájdete vo vodorovnom pruhu blokov v strednej časti hlavného okna. Súčasti sú zobrazené ako zelené obdĺžniky s ikonou príslušnej súčasti. Poskytujú informácie o jej stave. [Podrobnosti >>](#)
- **Kontrola/Aktualizácia** sa nachádzajú v dolnom pruhu hlavného okna. Tieto tlačidlá umožnia okamžitý prístup k vášim najdôležitejším a najčastejšie používaným funkciám programu AVG. [Podrobnosti >>](#)

Okrem hlavného okna **AVG Internet Security** existuje ešte jedna kontrolná súčnosť, cez ktorú máte prístup k aplikácii:

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

3.3.1. Horný navigačný rad

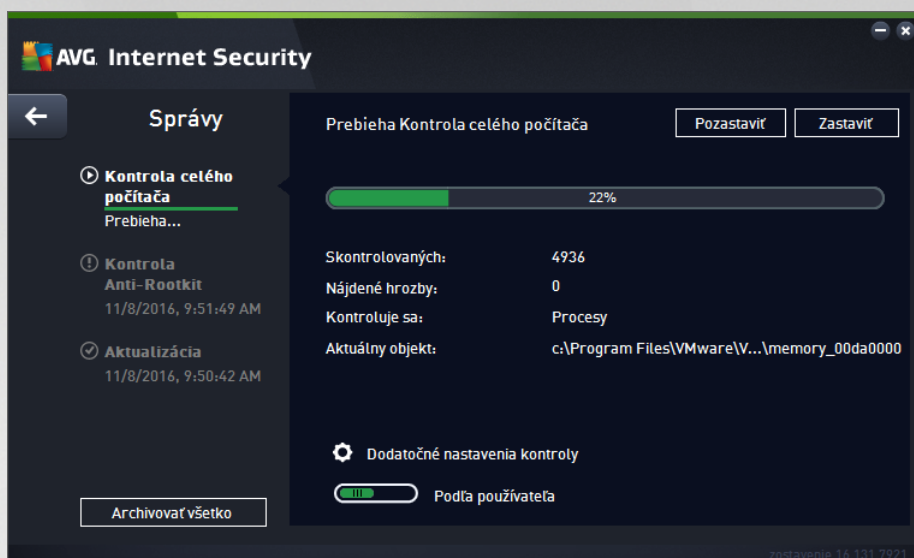
Horný navigačný rad sa skladá z radu viacerých aktívnych odkazov v hornej časti hlavného okna. Navigácia obsahuje tieto tlačidlá:

3.3.1.1. Ďalšie produkty od AVG

Jedným kliknutím na odkaz sa pripojíte ku webovej stránke AVG, kde nájdete všetky informácie o ochrane AVG pre vašu maximálnu bezpečnosť na internete.

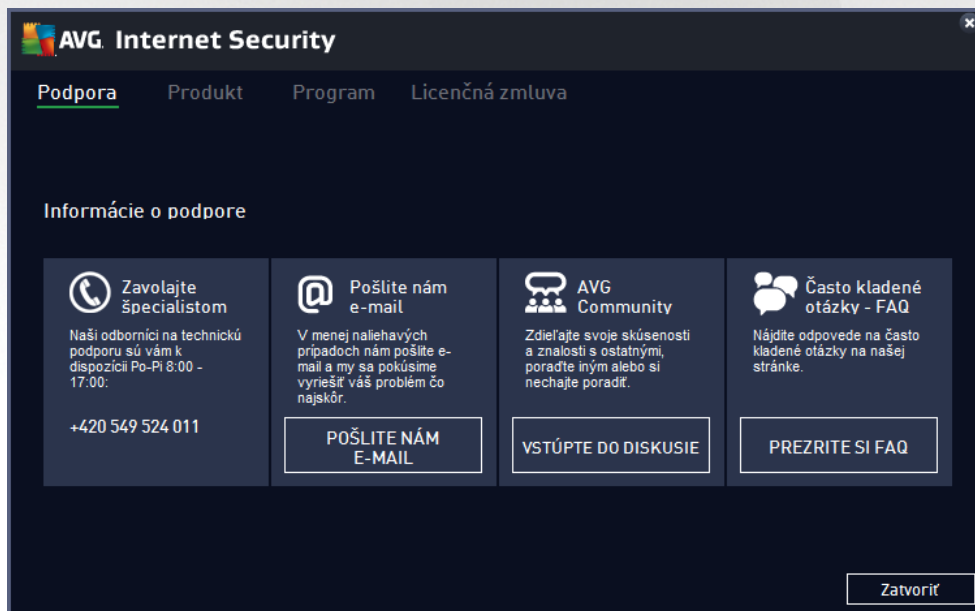
3.3.1.2. Správy

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:



3.3.1.3. Podpora

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



- **Podpora** – táto karta obsahuje prehľad a usporiadaný prehľad všetkých dostupných kontaktov na zákaznícku podporu.
- **Produkt** – na tejto karte sa nachádza prehľad najdôležitejších technických údajov **AVG Internet Security**, týkajúcich sa informácií o antivírusovom produkte, nainštalovaných sústaviach a nainštalovanej ochrane e-mailu.
- **Program** – na tejto karte nájdete podrobné technické informácie o nainštalovanom produkte **AVG**



Internet Security, ako napríklad číslo hlavnej verzie produktu a zoznam všetkých čísel verzií všetkých príslušných produktov (napr. *Zen*, *PC TuneUp at* ...). Ďalej sa na tejto karte uvádza prehľad všetkých nainštalovaných súčastí a konkrétne informácie o zabezpečení (číslo verzií vírusovej databázy, nástrojov *Link Scanner* a *Anti-Spam*).

- **Licenčná zmluva** – na tejto karte sa nachádza plné znenie licenčnej zmluvy medzi vami a spoločnosťou AVG Technologies.

3.3.1.4. Možnosti

Údržba **AVG Internet Security** je dostupná prostredníctvom položky **Možnosti**. Kliknutím na šípku otvoríte rozbaľovaciu ponuku:

- **Skontrolovať počítač** – spustí kontrolu celého počítača.
- **Skontrolovať vybraný priečinok...** – prepne na rozhranie kontroly AVG a pomocou stromovej štruktúry počítača umožní definovať, ktoré súbory a priečinky sa majú kontrolovať.
- **Skontrolovať súbor...** – umožní vám spustiť na požiadanie test jedného konkrétneho súboru. Kliknutím na túto možnosť sa otvorí nové okno so stromovou štruktúrou disku. Vyberte požadovaný súbor a potvrdíte spustenie kontroly.
- **Aktualizácia** – automaticky spustí proces aktualizácie **AVG Internet Security**.
- **Aktualizácia z adresára...** – spustí proces aktualizácie z aktualizovaných súborov, ktoré sa nachádzajú v určenom priečinku na miestnom disku. Túto možnosť vám však odporúčame použiť len ako núdzové riešenie, napr. v situáciách, keď nie je vytvorené pripojenie na internet (napríklad počítač je infikovaný a odpojený od internetu; počítač je pripojený k sieti bez prístupu na internet a pod.). V novo otvorenom okne zvolíte priečinok, do ktorého ste predtým uložili aktualizovaný súbor, a spustíte proces aktualizácie.
- **Vírusový trezor** – otvorí rozhranie úložiska karantény (Vírusový trezor), do ktorého AVG odstráni všetky zistené infekcie. V tejto karanténe sú infikované súbory izolované a je zaručená bezpečnosť vášho počítača. Zároveň sú infikované súbory uložené pre ich budúcu možnú opravu.
- **História** – ponúka ďalšie špeciálne možnosti podponuky:
 - **Výsledky kontroly** – otvorí dialógové okno s prehľadom výsledkov kontrol.
 - **Nálezy súčastí Rezidentný štít** – otvorí dialógové okno s prehľadom hrozieb detegovaných Rezidentným štítom.
 - **Nálezy súčastí Software Analyzer** – otvorí dialógové okno s prehľadom hrozieb detegovaných súčastí Software Analyzer.
 - **Nálezy súčastí Ochrana e-mailu** – otvorí dialógové okno s prehľadom príloh e-mailových správ označených súčastí Ochrana e-mailu ako nebezpečné.
 - **Nálezy súčastí Webový štít** – otvorí dialógové okno s prehľadom hrozieb detegovaných Webovým štítom.
 - **Protokol histórie udalostí** – otvorí rozhranie protokolu histórie s prehľadom všetkých zaznamenaných udalostí **AVG Internet Security**.



- o [Protokol sú asti Firewall](#) – otvorí dialógové okno s podrobným prehľadom o inosti sú asti Firewall.
- [Rozšírené nastavenia...](#) – otvorí dialógové okno s rozšírenými nastaveniami AVG, kde môžete upravi konfiguráciu **AVG Internet Security**. V zásade vám neodporúame meniť predvolené nastavenia aplikácie definované dodávateľom softvéru.
- [Nastavenia sú asti Firewall...](#) – otvorí samostatné dialógové okno s rozšírenou konfiguráciou sú asti Firewall.
- **Obsah pomocníka** – otvorí súbory pomocníka AVG.
- **Získajte podporu** – otvorí [dialógové okno podpory](#), ktoré poskytuje všetky dostupné kontakty a informácie podpory.
- **Vaša AVG webová stránka** – otvorí webovú stránku AVG (<http://www.avg.com/>).
- **O vírusoch a hrozbách** – otvorí online vírusovú encyklopédiu na webovej stránke AVG (<http://www.avg.com/>), v ktorej môžete vyhľadať podrobné informácie o identifikovanom víruse.
- **MyAccount** – spája so stránkou registrácie webovej stránky **AVG MyAccount** (<http://www.avg.com/>). Vytvorte si účet AVG, aby ste mohli jednoducho spravovať svoje zaregistrované produkty a licencie AVG, sledovať nové produkty, sledovať stav vašich objednávok a spravovať vaše osobné údaje a heslá. Vyplňte vaše registračné údaje; nárok na bezplatnú technickú podporu získajú len tí zákazníci, ktorí si produkt AVG zaregistrujú.
- **O AVG** – otvorí nové dialógové okno s tromi záložkami s údajmi o zakúpenej licencií a informáciami o dostupnej podpore, produkte a programe. Uvedené je tu tiež plné znenie licenčnej zmluvy. (Rovnaké dialógové okno môžete otvoriť pomocou odkazu [Podpora](#) v hlavnej navigácii.)

3.3.2. Informácie o stave zabezpečenia

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



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



– žltá ikona upozorňuje, že **jedna súčasta alebo niekto ko sú súčasti je nesprávne nakonfigurovaných** a treba venovať pozornosť ich vlastnostiam alebo nastaveniam. Neexistuje žiadny kritický problém s produktom **AVG Internet Security** a pravdepodobne ste sa rozhodli z nejakého dôvodu vypnúť 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 väčšine prípadov **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 nechcete nechať program **AVG Internet Security** v tomto stave a nechcete byť na to upozorňovaní. Môže sa vyskytnúť situácia, keď bude potrebné použiť túto možnosť; dôrazne vám však odporúčame, aby ste funkciu **Ignorovať chybný stav** o najskôr znova vyplili!



Žltá ikona sa zobrazí aj vtedy, ak **AVG Internet Security** 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!** Jedna alebo viac súčastí nefunguje správne a **AVG Internet Security** 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 nastavený tak, aby poskytoval optimálny výkon, ved a informácie o stave zabezpečenia sa zobrazí nové tlačidlo s názvom Kliknutím opraviť (alebo Kliknutím opraviť všetko, ak sa problém týka viacerých súčastí). Stlačením tlačidla spustíte automatický proces kontroly a konfigurácie programu. Je to jednoduchý spôsob nastavenia optimálneho výkonu AVG Internet Security a dosiahnutia maximálnej úrovne zabezpečenia.

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

Poznámka: Informáciu o stave produktu AVG Internet Security môžete zistiť kedykoľvek pomocou ikony v paneli úloh systému.

3.3.3. Prehľad súčastí

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

Presuňte kurzor myši nad súčasti. 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 **AVG Internet Security** v časti **Prehľad súčastí** sa nachádzajú informácie o nasledujúcich súčastiach:

- **Počítač** – tieto súčasti sa týkajú dvoch služieb: **AntiVirus Shield** deteguje vírusy, spyware, červy, trójske kone, neželané spustiteľné súbory a knižnice v systéme a chráni vás pred škodlivým adware. **Anti-Rootkit** kontroluje nebezpečné rootkity ukryté vnútri aplikácií, ovládačov alebo knižníc. [Podrobnosti >>](#)
- **Prezeranie webu** – chráni vás pred útokmi na webe pri vyhľadávaní a surfovaní na internete. [Podrobnosti >>](#)
- **Softvér** – táto súčasť spúšťa službu **Software Analyzer**, ktorá neustále chráni vaše digitálne aktíva pred novými a neznámymi hrozbami na internete. [Podrobnosti >>](#)
- **E-mail** – kontroluje prichádzajúce e-mailové správy, či neobsahujú nevyžiadajúcu poštu, a blokuje vírusy, phishingové útoky a iné hrozby. [Podrobnosti >>](#)
- **Firewall** – kontroluje komunikáciu na všetkých sieťových portoch, chráni pred útokmi a blokuje každý



pokus o prienik. [Podrobnosti >>](#)

Dostupné inosti

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

3.3.4. Kontrola /Aktualizovať rýchle odkazy

Rýchle odkazy sa nachádzajú v spodnom riadku tlačidiel [AVG Internet Security](#). 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 asti. Odkazom **Skontrolovať teraz** okamžite spustíte [Kontrolu celého počítača](#) a môžete sledovať jej priebeh a výsledky v automaticky otvorenom okne [Správy](#). Tlačidlo **Možnosti** otvorí dialógové okno **Možnosti kontroly**, kde môžete [spravovať naplánované kontroly](#) a upraviť parametre [Kontroly celého počítača/Kontroly súborov/priebehov](#). (Podrobnosti nájdete v kapitole [Kontrola AVG](#))
- **Opraviť výkon** – Týmto tlačidlom vstúpite do služby [PC Analyzer](#), vyspelého nástroja na podrobnú analýzu a opravu systému, ktorý sa používa na hľadanie možností, ako zvýšiť rýchlosť počítača a zlepšiť jeho celkový výkon.
- **Aktualizovať teraz** – stlačením tohto tlačidla okamžite spustíte aktualizáciu. O výsledkoch aktualizácie budete informovaní v oznámení nad ikonou AVG v paneli úloh. (Podrobnosti nájdete v asti [Aktualizácie AVG](#))

3.3.5. AVG Advisor

Súčasť **AVG Advisor** bola navrhnutá tak, aby detegovala problémy, ktoré môžu ohrozovať váš počítač a na odporúčanie akcií na riešenie daných situácií. **AVG Advisor** vidíte v podobe vysúvacieho kontextového okna nad panelom úloh. Služba deteguje pravdepodobnú **neznámu sieť so známym názvom**. To sa obvykle týka len tých používateľov, ktorí sa pripájajú k rôznym sieťam, obvykle pomocou prenosných počítačov. V prípade, že nová neznáma sieť má rovnaký názov ako dobre známa a často používaná sieť (napríklad *Doma alebo MojeWifi*), môže nastáť omyl a nechtiac sa môžete pripojiť do úplne neznámej a potenciálne nebezpečnej siete. **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 **AVG Advisor**, aby v budúcnosti nebola znovu nahlasovaná.

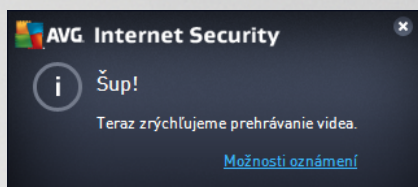
Podporované internetové prehliadače

Táto funkcia funguje v nasledujúcich internetových prehliadačoch: Internet Explorer, Chrome, Firefox, Opera, Safari.



3.3.6. AVG Akcelerátor

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



3.4. Súčasti AVG

3.4.1. Ochrana počítača

Súčasťou **Počítača** sa týka dvoch hlavných bezpečnostných služieb: **AntiVirus** a **Dátový trezor**.


- **AntiVirus** sa skladá z kontrolného jadra, ktoré stráži všetky súbory, systémové oblasti počítača a vymeniteľné médiá (*disk flash a pod.*) a kontroluje známe vírusy. 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 v pozadí“. Súčasťou AntiVirus používa tiež heuristickú kontrolu, pri ktorej sa v súboroch kontrolujú charakteristiky typické pre vírusy. To znamená, že súčasťou AntiVirus dokáže detegovať nový, neznámy vírus, ak tento nový vírus obsahuje isté typické vlastnosti existujúcich vírusov. **AVG Internet Security** dokáže tiež analyzovať a detegovať spustené aplikácie alebo knižnice DLL, ktoré by sa v systéme nemali nachádzať (rôzne typy spyware, adware a pod.). AntiVirus tiež kontroluje podozrivé záznamy v registri, dočasné internetové súbory a spracuje všetky potenciálne škodlivé položky rovnakým spôsobom ako každú inú infekciu.
- **Dátový trezor** vám umožňuje vytvárať bezpečné virtuálne trezory na uchovávanie citlivých údajov. Obsah Dátového trezora je šifrovaný a chránený heslom, ktoré si vyberiete, aby k údajom nikto nemal prístup bez povolenia.







Ovládacie prvky dialógového okna

Ak chcete prepínať medzi oboma stranami dialógového okna, stačí kliknúť kdekoko na príslušný servisný panel. Panel sa zvýrazní v svetlejšom odtieni modrej. V oboch stranách dialógového okna nájdete tieto ovládacie prvky. Ich funkcia je rovnaká bez ohľadu na to, do ktorej bezpečnostnej služby patria (*AntiVirus* alebo *Dátový trezor*):

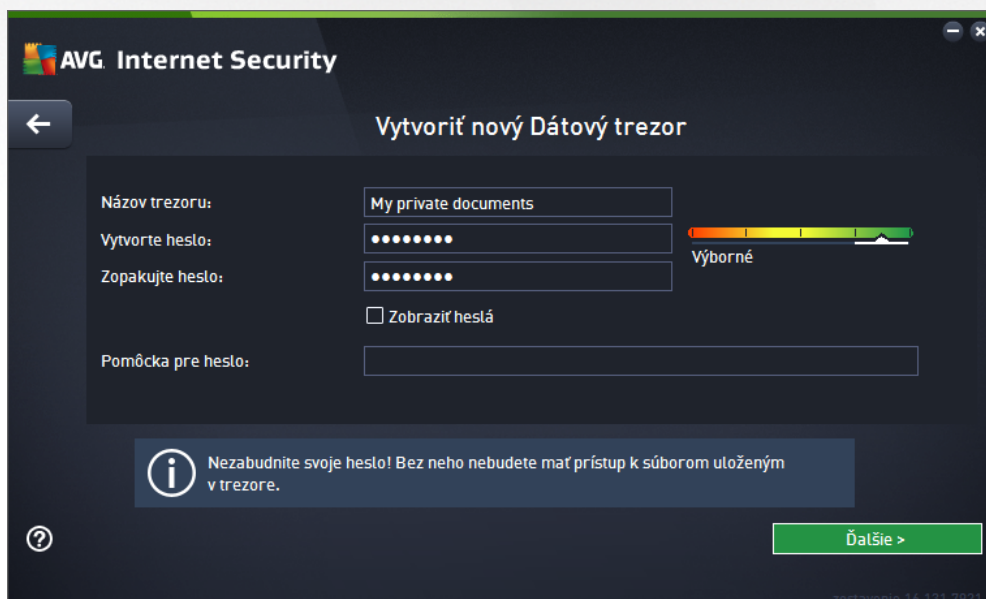
 **Zakázané/povolené** – tlačidlo môže pripomínať semafor vzhľadom aj funkciou. Kliknutím môžete prepínať medzi jeho dvomi polohami. Zelená farba symbolizuje stav **Povolené**, čo znamená, že bezpečnostná služba AntiVirus je aktívna a plne funkčná. Červená farba predstavuje stav **Zakázané**, t. j. služba je vypnutá. Ak nemáte dobrý dôvod na vypnutie služby, výrazne 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 upozornení na možné riziká červeným **varovným** nápisom a oznámením faktu, že momentálne nie ste úplne chránení. **Nezabudnite, že by ste službu mali znovu aktivovať o najskôr.**

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

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

Ako vytvoriť dátový trezor

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



Názov trezoru: My private documents

Vytvoríte heslo: Výborné

Zopakujte heslo:

Zobrazit heslá

Pomôcka pre heslo:

Nezabudnite svoje heslo! Bez neho nebudete mať prístup k súborom uloženým v trezore.

Ďalšie >

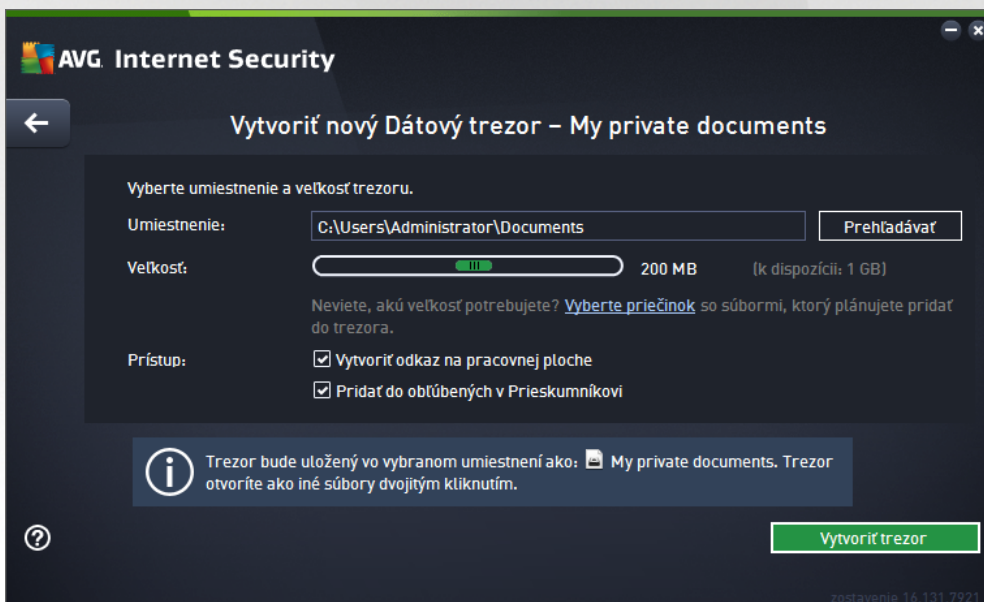
Zostavenie: 14.131.7921

Najprv je potrebné zadať názov trezora a vytvoriť silné heslo:



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

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



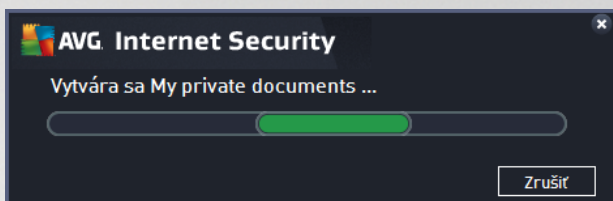
Toto dialógové okno poskytuje nasledovné možnosti konfigurácie:

- **Umiestnenie** uvádza, kde bude dátový trezor fyzicky umiestnený. Nájdite vhodné miesto na pevnom disku alebo ponechajte preddefinované umiestnenie v priečinku *Dokumenty*. Upozorujeme, že keď dátový trezor vytvoríte, jeho umiestnenie už nemôžete zmeniť.
- **Veľkosť** – môžete prednastaviť veľkosť dátového trezoru, čím sa vyhradí potrebné miesto na disku. Nastavená hodnota by nemala byť príliš malá (*nedostatočná pre vaše potreby*) ani príliš veľká (*aby trezor nezaberal zbytočne príliš veľa miesta na disku*). Ak už viete, čo chcete do dátového trezora umiestniť, môžete dať všetky príslušné súbory do jedného priečinka a potom pomocou odkazu **Vybrať priečink** automaticky vyplníť celkovú veľkosť. Veľkosť však môžete neskôr zmeniť podľa svojich potrieb.
- **Prístup** – zaškrtnutie políčok v tejto časti umožní vytvoriť pohodlné skratky k dátovému trezoru.



Ako používa dátový trezor

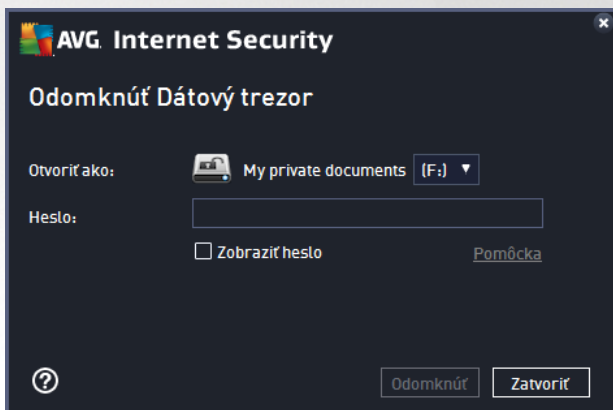
Ke budete s nastaveniami spokojní, kliknite na tlačidlo **Vytvori teraz**. Otvorí sa nové dialógové okno **Váš dátový trezor je teraz pripravený** a oznámi vám, že daný trezor je pripravený na ukladanie súborov. Práve teraz je trezor otvorený a môžete k nemu ihne pristupovať. Pri každom ďalšom pokuse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



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

Ako odomknú dátový trezor

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



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

3.4.2. Ochrana prezerania webu

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

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




v momente, keď je to najviac dôležité – v momente, keď sa chystáte kliknúť na odkaz. **LinkScanner Surf-Shield nie je určený 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 stiahnu do počítača. Webový štít zistí prítomnosť nebezpečného kódu JavaScript na stránke, ktorú sa práve chystáte navštíviť, a neumožní stránku zobraziť. Zároveň rozpozná škodlivý softvér, ktorý sa nachádza na tejto stránke, a ihneď zastaví jeho sťahovanie, aby sa nikdy nedostal do počítača. Táto unikátna ochrana zablokuje škodlivý kód každej webovej stránky, ktorú sa pokúšate otvoriť, a zabráni jeho stiahnutiu 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 zneužívané stránky môžu infikovať váš počítač už len tým, že ich navštívite. **Webový štít nie je určený na ochranu serverových platforiem!**



Ovládacie prvky dialógového okna

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

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

 **Nastavenia** – kliknutím na tlačidlo budete presmerovaní na rozhranie [rozšírených nastavení](#). Otvorí



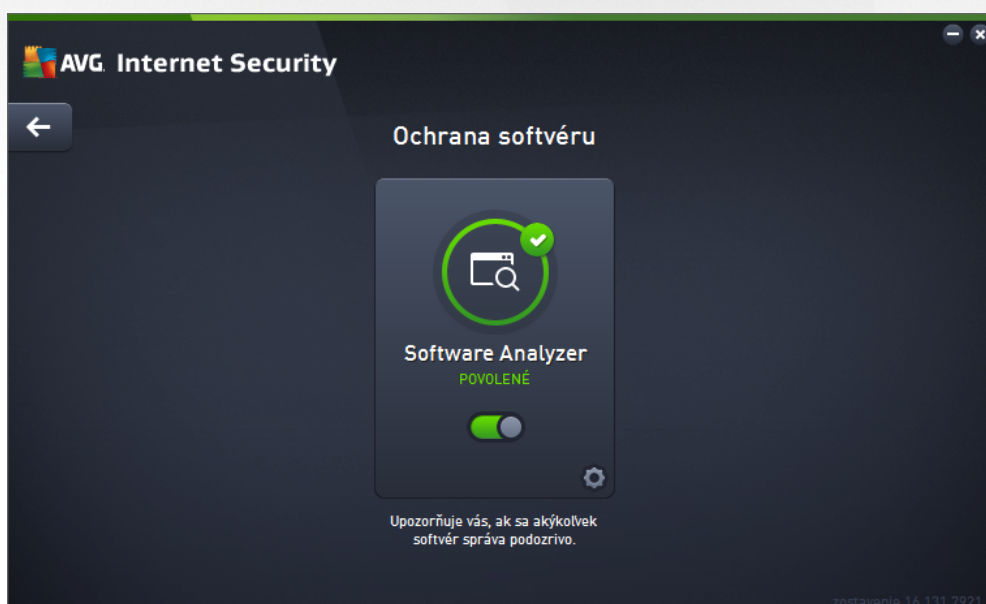
sa príslušné dialógové okno a budete môc nakonfigurova vybranú službu, t. j. [LinkScanner Surf-Shield](#) alebo [Webový štít](#). V rozšírených nastaveniach môžete upravi všetky konfigurácie každej bezpečnostnej služby **AVG Internet Security**, no akékoľvek nastavenie odporúame iba skúseným používateľom!

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

3.4.3. Software Analyzer

Súčasť **Software Analyzer** neustále chráni vaše digitálne aktíva pred novými a neznámymi hrozbami na internete:


- **Software Analyzer** je služba na ochranu pred malware, ktorá vás chráni pred všetkými druhmi malware (*spyware*, *softvérové roboty*, *krádež identity atď.*) s použitím technológií monitorovania správania a poskytuje okamžitú ochranu pred novými vírusmi. Identity Protection zabráňuje páchaťom po číslach tejto trestnej činnosti v oblasti odcudzenia identity, aby odcudzili vaše heslá, podrobnosti o bankových účtoch, čísla kreditných kariet a iné cenné osobné digitálne údaje zo všetkých druhov škodlivého softvéru (*malware*), ktorý útočí na váš počítač. Zabezpečuje správne fungovanie všetkých spustených programov na počítači alebo zdieľanej sieti. Software Analyzer neustále zaznamenáva a blokuje podozrivé správanie a chráni váš počítač pred každým novým malware. Software Analyzer chráni váš 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 počítači nevyskytuje nič škodlivé. Preto dokáže odhaliť hrozby, ktoré ešte nie sú opísané vo vírusovej databáze. Keď sa do počítača dostane neznámy kód, program ho ihneď začne sledovať z hardiskového správania. Ak sa súbor označí ako škodlivý, Software Analyzer presunie kód do [Vírusového trezora](#) a vráti späť všetky zmeny vykonané v systéme (*vloženia kódu, zmeny v registri, otvorenie portov a pod.*). Na dosiahnutie ochrany nemusíte spúšťať kontrolu. Technológia má voľne aktívny prístup, len zriedka sa musí aktualizovať a vždy je v strehu.







Ovládacie prvky dialógového okna

V tomto dialógovom okne nájdete nasledujúce ovládacie prvky:

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

 **Nastavenia** – kliknutím na tlačidlo budete presmerovaní na rozhranie [rozšírených nastavení](#). Otvorí sa príslušné dialógové okno a budete môcť nakonfigurovať vybranú službu, t. j. [Software Analyzer](#). V rozhraní rozšírených nastavení môžete upraviť všetky konfigurácie každej bezpečnostnej služby v **AVG Internet Security**, no akúkoľvek konfiguráciu odporúčame iba skúseným používateľom!

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

V **AVG Internet Security** nie je služba Identity Alert zatiaľ 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.

Berte, prosím, do úvahy, že aj v edíciách AVG Premium Security je služba Identity Alert momentálne dostupná iba vo vybraných oblastiach: USA, Spojené kráľovstvo, Kanada a Írsko.

3.4.4. Ochrana e-mailu

Súčasť **Ochrana e-mailu** obsahuje nasledujúce dve služby zabezpečenia: **Kontrola pošty** a **Anti-Spam** (služba Anti-Spam je dostupná len v edíciách Internet/Premium Security).

- **Kontrola pošty:** Jeden z najbežnejších zdrojov vírusov a trojských košov je e-mail. Ohrozenia typu phishing a spam ale zvyšujú riziko e-mailu. Bezplatné e-mailové úty sú náchylnejšie na prijímanie takýchto škodlivých e-mailov (pretože málokedy využívajú technológiu na ochranu pred nevyžiadanou poštou) 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 cez e-mail. Spoločnosť nosí obyčajne ajne využívajú hromadné emailové úty a používajú antispamové filtre, 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, ihne presunie správu do [Vírusového trezora](#). Táto súčasť dokáže zároveň filtrovať niektoré typy e-mailových príloh a pridať text certifikácie k správam bez infekcie. **Kontrola pošty nie je určená pre serverové platformy!**
- **Anti-Spam** kontroluje všetku prichádzajúcu poštu a nechcené správy označí ako spam (Spam označuje nevyžiadajúcu poštu, ktorá vám šíri propagáciu produktov a služieb a ktorá je hromadne zasielaná na veľké množstvo e-mailových adries súčasne. Podobné správy plnia poštové schránky prijemcov. Spam sa nevzťahuje na legálne komerčné e-maily, s ktorými zákazníci súhlasia.). Anti-Spam dokáže zmeniť predmet e-mailovej správy (ktorá bola označená ako nevyžiadaná pošta) pridaním špeciálneho textového reazca. Môžete filtrovať e-mailové správy v e-mailovom klientovi.





Sú as Anti-Spam používa niekoľko metód analýzy na spracovanie jednotlivých e-mailových správ a prináša najvyššiu možnú úroveň ochrany pred nevyžiadanými e-mailovými správami. 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](#) (nikdy neoznačíte ako spam) a [zoznamu blokových](#) (vždy označíte ako spam) adries.




Ovládacie prvky dialógového okna

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

 **Zakázané/povolené** – tlačidlo môže pripomínať semafor vzhľadom aj funkciou. Kliknutím môžete prepínať medzi jeho dvomi polohami. Zelená farba symbolizuje stav **Povolené**, čo znamená, že bezpečnostná služba je aktívna a plne funkčná. Červená farba predstavuje stav **Zakázané**, t. j. služba je vypnutá. Ak nemáte dobrý dôvod na vypnutie služby, výrazne odporúčame, aby ste ponechali predvolené nastavenia pre všetky konfigurácie zabezpečenia. Predvolené nastavenia 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 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. [Kontrola pošty](#) alebo [Anti-Spam](#). V rozšírených nastaveniach môžete upraviť všetky konfigurácie každej bezpečnostnej služby **AVG Internet Security**, no akékoľvek nastavenie odporúčame iba skúseným používateľom!

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



3.4.5. Firewall

Firewall je systém, ktorý presadzuje zásady riadenia prístupu medzi dvoma alebo viacerými sieťami blokovaním, resp. povolením prenosov. Firewall má skupinu pravidiel, ktoré chránia internú sieť pred útokmi zvonku (zvyčajne z internetu) a riadi komunikáciu na každom jednom sieťovom porte. Komunikácia sa vyhodnotí podľa zadaných pravidiel, a potom sa buď povolí alebo zakáže. Keď Firewall zistí pokus o preniknutie do systému, zablokuje ho a nedovolí narušiteľovi vstúpiť do počítača. Firewall je nastavený tak, aby umožňoval alebo blokoval internú alebo externú komunikáciu (oboma smermi, dnu aj von) na definovaných portoch a pre definované softvérové aplikácie. Firewall sa môže nastaviť napríklad tak, aby umožňoval tok webových dát smerom dnu a von, len keď sa používa Microsoft Explorer. Každý pokus o prenos webových dát iným prehliadačom sa zablokuje. Chráni informácie, ktoré vás môžu osobne identifikovať, pred odoslaním z vášho počítača a bez vášho povolenia. Kontroluje ako váš počítač vymieňa údaje s ostatnými počítačmi na Internete alebo v lokálnej sieti. V rámci organizácie Firewall chráni samostatné počítače pred útokmi interných používateľov na ostatné počítače v sieti.

V aplikácii **AVG Internet Security** kontroluje **Firewall** všetky prenosy na každom sieťovom porte počítača. 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 Firewall buď povolí, alebo zakáže komunikáciu na sieťových portoch. Ak je aplikácia neznáma (teda nemá žiadne zadané pravidlá Firewallu), súhlasí Firewall s vašim predvoleným spýtaním, či chcete blokovanie alebo povolenie tento pokus o komunikáciu.

Súhlasí AVG Firewall nie je určená na ochranu serverových platforiem!

Odporúčanie: Vo všeobecnosti sa neodporúča používať viac ako jeden firewall na tom istom počítači. Zabezpečenie počítača nie je vyššie, ak nainštalujete viac firewallov. Vzniká však vyššia pravdepodobnosť, že medzi týmito dvomi aplikáciami nastane konflikt. Preto vám odporúčame, aby ste používali len jeden firewall na počítači a vypli všetky ostatné, aby sa eliminovalo riziko vzniku konfliktu a súvisiacich problémov.



Poznámka: Po inštalácii AVG Internet Security môže súhlasí Firewall požadovať reštartovanie počítača. V tomto prípade sa zobrazí dialógové okno súhlasí s informáciou, že je potrebné reštartovanie. Priamo v dialógovom okne nájdete tlačidlo **Reštartovať teraz**. Až do reštartovania nebude súhlasí Firewall plne aktívna. Taktiež bude v dialógovom okne vypnutá možnosť úprav. Venujte varovaniu pozornosť a o najskôr reštartujte počítač!



Dostupné režimy Firewallu

Firewall vám umožní 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 Firewallu špecifickou konfiguráciou súčasti Firewall a môžete použiť nieko ko takýchto vopred definovaných konfigurácií.

- **Automaticky** – v tomto režime Firewall automaticky spracúva všetky sieťové prenosy. Z vašej strany nebudú požadované žiadne rozhodnutia. Firewall umožní pripojenie všetkých známych aplikácií a súhlasne s tým sa vytvorí pre aplikáciu pravidlo, ktoré určí, či sa aplikácia môže v budúcnosti kedykoľvek pripojiť. V prípade iných aplikácií Firewall podľa správania aplikácie rozhodne, či sa má pripojenie povoliť alebo zablokovať. 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 počítača. Firewall ich bude sledovať a upozorní vás na každý pokus o komunikáciu alebo prenos dát, čím vám umožní povoliť alebo zablokovať daný pokus, ako to uznáte za vhodné. Odporúča sa len pokročilým používateľom.
- **Blokovať prístup k internetu** – internetové pripojenie bude úplne zablokované, nebudete mať prístup k internetu a nikto zvonku nebude mať prístup k vášmu počítaču. Len pre zvláštne a krátkodobé použitie.
- **Deaktivovať ochranu súčasti Firewall (neodporujeme)** – vypnutím povolíte všetky sieťové prenosy z počítača. Učiníte ho tak zraniteľným voči útoku hackerov. Vo väčšine prípadov sú možnosti vždy starostlivo zvažované.

Upozorujeme na špeciálny automatický režim, ktorý je tiež k dispozícii v rámci Firewallu. Tento režim sa v tichosti aktivuje vtedy, ak sa [Počítač](#) alebo súčasti [Software Analyzer](#) vypnú, a počítač bude preto zraniteľnejší. V takých prípadoch Firewall automaticky povolí pripojenie iba známym a úplne bezpečným aplikáciám. Pri všetkých ostatných bude od vás vyžadované rozhodnutie. Cieľom je nahradiť deaktivované súčasti ochrany a udržať počítač v bezpečí.

Veľmi dôrazne vám odporujeme, aby ste Firewall úplne nevypínali. Ak však vyvstane potreba a súčasti Firewall musíte skutočne deaktivovať, môžete tak urobiť pomocou výberu režimu Vypnúť ochranu súčasti Firewall zo zoznamu dostupných režimov súčasti Firewall vyššie.

Ovládacie prvky dialógového okna

Dialógové okno obsahuje prehľad základných údajov o stave súčasti Firewall:


- **Režim súčasti Firewall** – poskytuje informácie o aktuálne zvolenom režime Firewallu. Tlačidlom **Zmeniť** vedľa uvedených údajov prepnete na rozhranie [nastavení súčasti Firewall](#), pokiaľ chcete zmeniť aktuálny režim na iný (*popis a odporúčanie týkajúce sa profilov Firewallu nájdete v predchádzajúcom odseku*).
- **Zdieľanie súborov a tlačiarňí** – informuje 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 vo Windowse 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 žela ni zdie a .

- **Pripojené k** – poskytuje údaje o názve siete, ku ktorej ste práve pripojení. Vo Windowse XP názov siete zodpovedá ozna eniu, ktoré ste pre u vybrali pri prvom pripojení k nej. Vo Windowse Vista a novšom sa názov siete preberá automaticky z Centra sietí a zdie ania.
- **Obnovi konfiguráciu** – stla ením tohto tlačidla sa prepíše používaná konfigurácia sú asti Firewall a obnoví sa predvolená konfigurácia na základe automatickej detekcie.

Toto dialógové okno pozostáva z nasledujúcich grafických ovládacích prvkov:

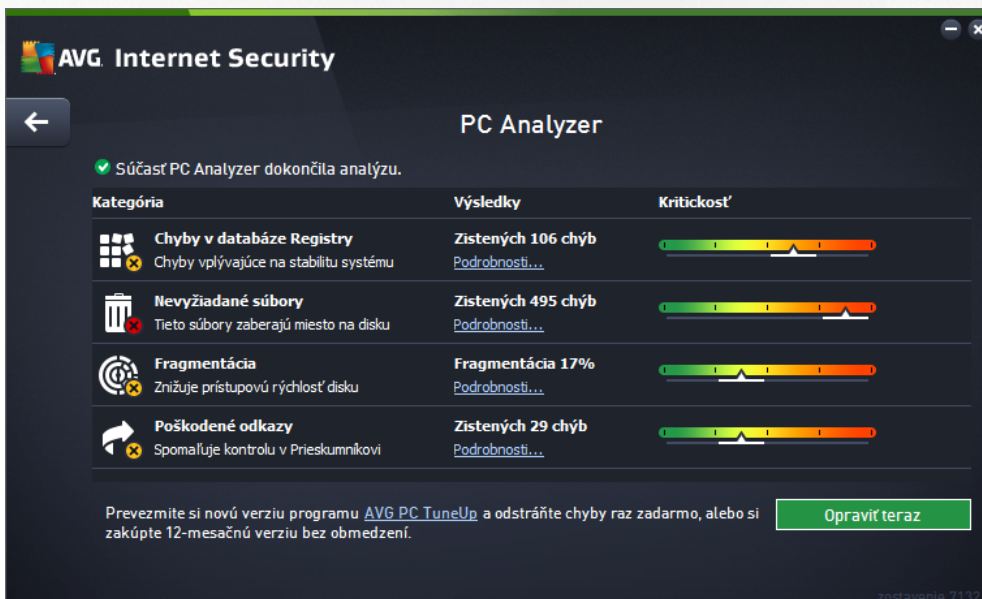
 **Nastavenia** – kliknutím na tlačidlo budete presmerovaní na kontextovú ponuku, ktorá ponúka dve možnosti:

- **Rozšírené nastavenia** – táto možnosť vás presmeruje na rozhranie [Nastavenia sú asti Firewall](#), kde môžete upravi celú konfiguráciu Firewallu. Pamätajte však na to, že akúkoľvek konfiguráciu by mali vykonáva len skúsení používatelia!
- **Odstráni ochranu sú as ou Firewall** – po výbere tejto možnosti bude odinštalovaná sú as Firewall, čo môže oslabi vašu bezpečnostnú ochranu. Ak chcete aj napriek tomu odstráni sú as Firewall, potv rte svoje rozhodnutie a sú as sa úplne odinštaluje.






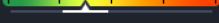


 **Šípka** – pomocou zelenej šípky v avej hornej asti dialógového okna sa vrátite naspä do [hlavného používate ského rozhrania](#) s preh adom sú astí.

3.4.6. PC Analyzer

PC Analyzer je vyspelý nástroj na podrobnú analýzu a opravu systému, ktorý sa používa na h adanie možností, ako zvýši rýchlosť počíta a a zlepši jeho celkový výkon. Otvára sa prostredníctvom tlačidla **Opravi výkon**, ktoré sa nachádza v [hlavnom dialógovom okne používate ského rozhrania](#) alebo prostredníctvom rovnakej možnosti uvedenej v kontextovej ponuke ikony AVG v paneli úloh. Potom si budete môc pozrie priebeh analýzy a výsledky priamo v tabu ke:



The screenshot shows the AVG Internet Security PC Analyzer window. At the top, it says "Súčasť PC Analyzer dokončila analýzu." Below this is a table with four rows of results:

Kategória	Výsledky	Kritickosť
 Chyby v databáze Registry Chyby vplývajúce na stabilitu systému	Zistených 106 chýb Podrobnosti...	
 Nevyžiadané súbory Tieto súbory zaberajú miesto na disku	Zistených 495 chýb Podrobnosti...	
 Fragmentácia Znižuje prístupovú rýchlosť disku	Fragmentácia 17% Podrobnosti...	
 Poškodené odkazy Spomaľuje kontrolu v Prieskumníkovi	Zistených 29 chýb Podrobnosti...	

At the bottom, there is a green button labeled "Opravi teraz" and a link to "Prevezmite si novú verziu programu AVG PC TuneUp a odstráňte chyby raz zadarmo, alebo si zakúpte 12-mesačnú verziu bez obmedzení." The version number "zostavenie 7132" is visible in the bottom right corner.



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

- **Chyby v databáze Registry** informujú o porušení chýb v databáze Registry operačného systému Windows, ktoré môžu spomaľovať vašu prácu alebo spôsobovať zobrazenie chybových hlásení.
- **Nevyžiadané súbory** informujú o porušení súborov, ktoré zaberajú miesto na disku, a ktoré sa pravdepodobne môžu vymazať. Zvyčajne ide o mnohé typy dočasných súborov a súborov 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.

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

Ovládacie tlačidlá

- **Zastaviť analýzu** (zobrazí sa počas spustenej analýzy) – stlačením tohto tlačidla sa ihneď preruší analýza počítača.
- **Inštalovať opravu** (zobrazí sa po dokončení analýzy) – utujeme, ale funkcia PC Analyzer v rámci **AVG Internet Security** je obmedzená na analýzu súčasného stavu vášho počítača. AVG však poskytuje vyspelý nástroj na podrobnú analýzu a opravu systému, ktorý sa používa na hľadanie možností, ako zvýšiť rýchlosť počítača a zlepšiť jeho celkový výkon. Kliknite na tlačidlo s logom a budete presmerovaní na vyhradenú webovú stránku pre ďalšie informácie.

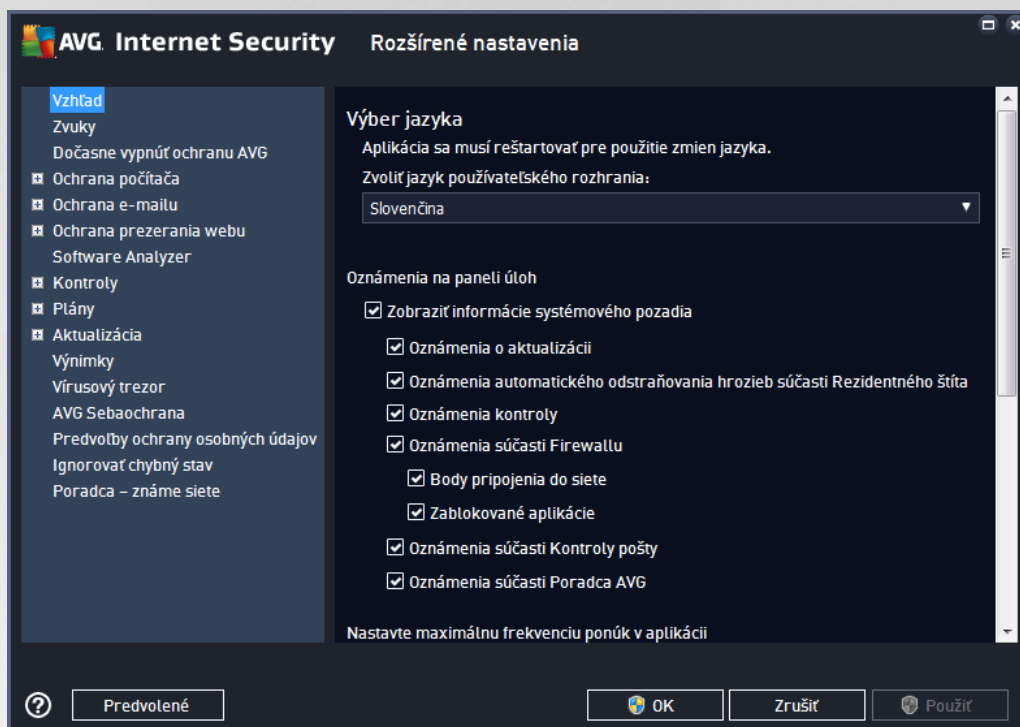
3.5. Rozšírené nastavenia AVG

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



3.5.1. Vzhľad

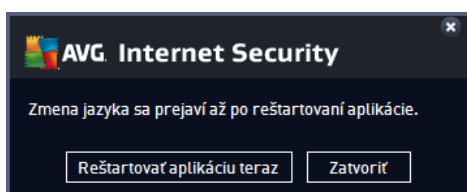
Prvá položka v navigačnej štruktúre, **Vzhľad**, sa týka všeobecných nastavení [používateľského rozhrania AVG Internet Security](#) a niektorých základných možností správania sa aplikácie:



Výber jazyka

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

- V rozba ovacej ponuke vyberte požadovaný jazyk aplikácie
- Potvr te výber stla ením tlačidla **Použi** (v pravom hornom rohu dialógového okna)
- Potvr te stla ením tlačidla **OK**
- Zobrazí sa nové dialógové okno s informáciami o zmene jazyka aplikácie a potrebe reštartova **AVG Internet Security**
- Stla ením tlačidla **Reštartova AVG teraz** súhlasíte s reštartovaním programu. Po kajte chví u, kým sa zmena jazyka prejaví:





Oznámenia na paneli úloh

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

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

- **Zobrazovanie oznámenia v paneli úloh (predvolene zapnuté)** – predvolene sa zobrazujú všetky oznámenia. Ak chcete úplne vypnúť zobrazovanie všetkých oznámení, zrušte začiarknutie tejto položky. Po zapnutí môžete tiež vybrať konkrétne oznámenia, ktoré sa majú zobrazovať:
 - **Oznámenia o aktualizáciách (predvolene zapnuté)** – rozhodnite sa, či sa majú zobrazovať informácie týkajúce sa spustenia, postupu a dokončenia procesu aktualizácie **AVG Internet Security**.
 - **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 (toto nastavenie sa zobrazuje, len keď je v súastí **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 súastí Firewall (predvolene zapnuté)** – rozhodnite sa, či by sa mali zobrazovať informácie súvisiace so stavom a procesmi súastí Firewall, ako sú upozornenia o zapnutí alebo vypnutí súastí, možné 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 súastí Firewall informuje o tom, či ide o známu sieť, a aké budú nastavenia zdieľania súborov a tlačeiarňí.
 - **Blokované aplikácie (predvolene zapnuté)** – ak sa do siete pokúša pripojiť neznáma alebo podozrivá aplikácia, súastí Firewall zablokuje tento pokus a zobrazí oznámenie. To je užitočné, aby ste boli informovaní, preto odporujeme nechať túto funkciu vždy zapnutú.
 - **Oznámenia Kontroly pošty (predvolene zapnuté)** – rozhodnite sa, či sa majú zobrazovať informácie po každej kontrole prichádzajúcich a odchádzajúcich e-mailových správ.
 - **Štatistické oznámenia (predvolene zapnuté)** – nechajte políčko začiarknuté, ak sa majú zobrazovať pravidelné štatistické prehľadové oznámenia v paneli úloh.
 - **Oznámenia AVG Advisor (predvolene zapnuté)** – rozhodnite sa, či sa informácie o aktivite [AVG Advisor](#) majú zobrazovať v paneli úloh.

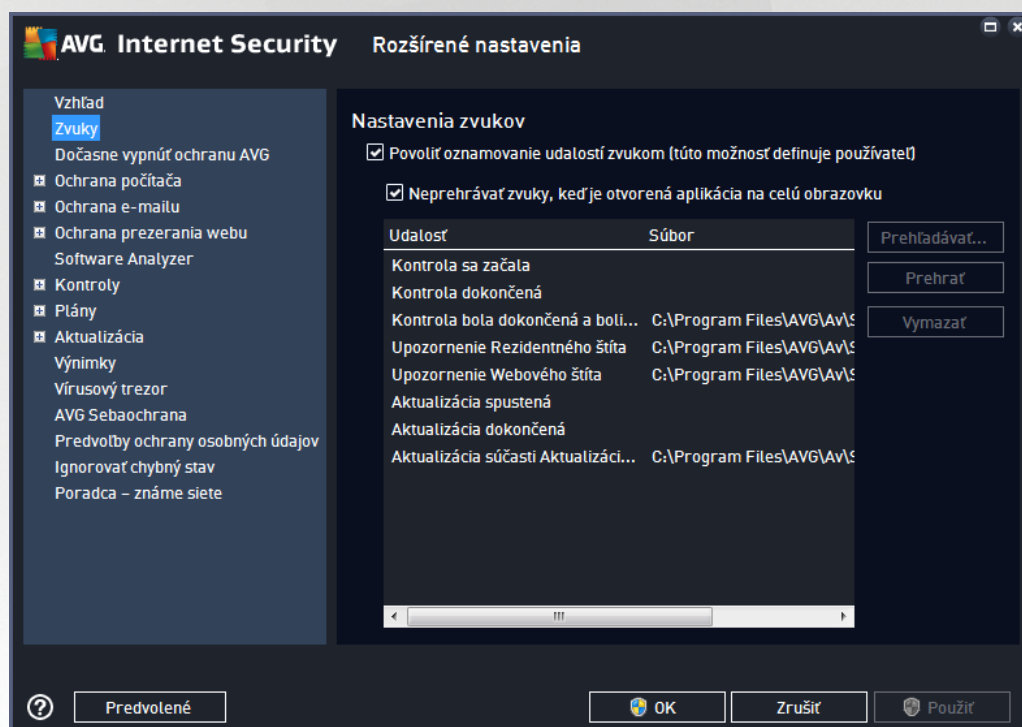


Režim hrania

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

3.5.2. Zvuky

Dialógové okno **Nastavenia zvukov** sa používa na zapnutie zvukových upozornení informujúcich o konkrétnych inostiach programu **AVG Internet Security**:



Tieto nastavenia sú platné len pre ú et aktuálneho používate a. To znamená, že každý používate na po íta i bude ma svoje vlastné nastavenia zvukov. Ak chcete povoliť zvukové oznamy, nechajte ozna enú možnosť **Povoliť oznamovanie udalostí zvukom** (táto možnosť je predvolene zapnutá), aby ste aktivovali zoznam všetkých dôležitých iností. alej môžete ozna i možnosť **Neprehráva zvuky, keď je aktívna aplikácia na celú obrazovku**, ak chcete potla i zvukové upozornenia v situáciách, keď by mohli vyrušova (pozrite si tiež as **Režim hry** v kapitole [Rozšírené nastavenia/Vzh ad](#) v tomto dokumente).

Ovládacie tlačidlá

- **Preh adáva ...** – po ozna ení príslušnej udalosti zo zoznamu pomocou tlačidla **Preh adáva** nájdete na disku požadovaný zvukový súbor, ktorý chcete udalosti priradiť. (Upozor ujeme, že v sú asnosti sú podporované iba zvuky vo formáte *.wav!)
- **Prehra** – ak si chcete vypo u zvolený zvuk, zvýraznite udalosť v zozname a stla te tlačidlo **Prehra**.

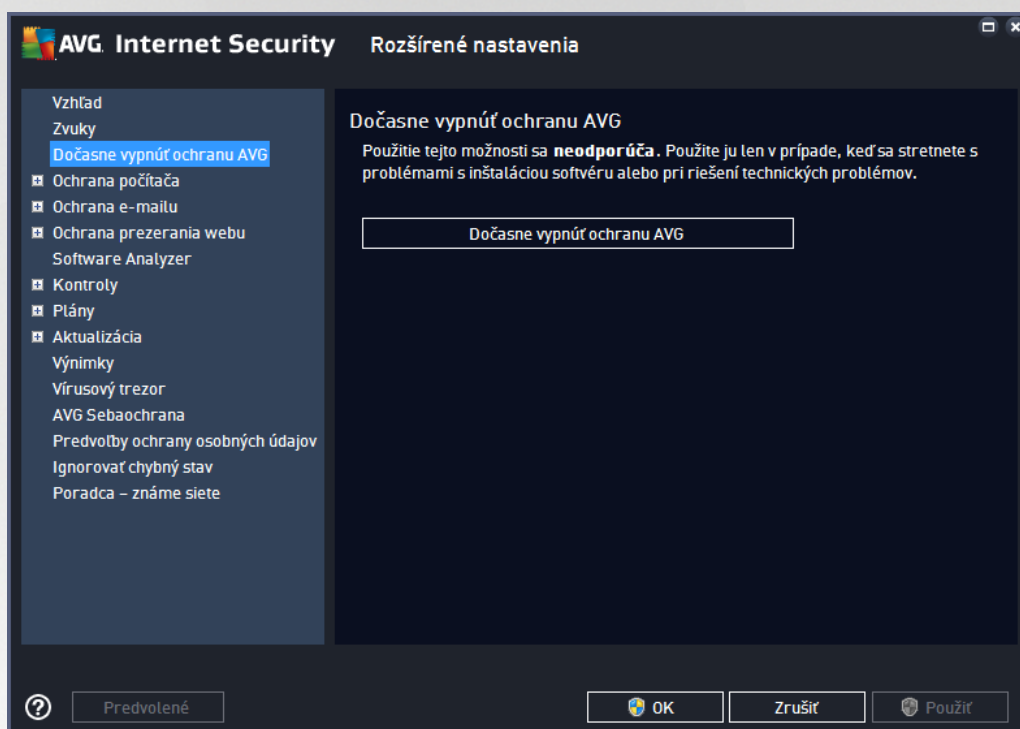


- **Vymaza** – na odstránenie zvuku priradeného ku konkrétnej udalosti použijete tlačidlo **Vymaza**.

3.5.3. Dočasne vypnúť ochranu AVG

Dialógové okno **Dočasne vypnúť ochranu AVG** umožňuje naraz vypnúť celú ochranu, ktorú zaisťuje **AVG Internet Security**.

Nepoužívajte túto možnosť, ak to nie je naozaj nevyhnutné!

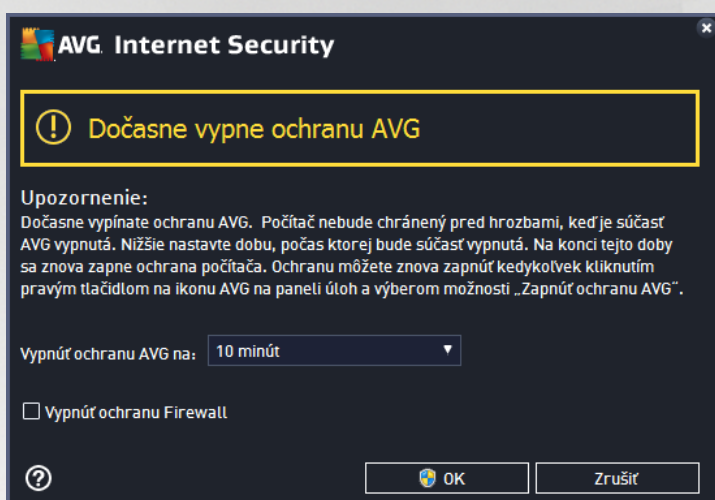


Vo väčšine prípadov **nie je potrebné** deaktivovať **AVG Internet Security** pred inštaláciou nového softvéru alebo ovládačov, a to ani v prípade, keď inštalovaný program alebo sprievodca inštaláciou softvéru odporúča, aby sa najskôr zatvorili spustené programy a aplikácie z dôvodu možného nežiaduceho prerušenia procesu inštalácie. Ak skutočne budete mať pri inštalácii problémy, pokúste sa najskôr [deaktivovať rezidentnú ochranu](#) (v dialógovom okne, do ktorého smeruje odkaz, zrušte začiarknutie položky **Povoliť rezidentný štít**). Ak musíte dočasne vypnúť ochranu **AVG Internet Security**, znova ju zapnite bezprostredne po dokončení úloh, pre ktoré ste ju vypli. Ak ste pripojení na internet alebo k sieti v momente, keď je antivírusový softvér vypnutý, váš počítač nie je chránený pred útokmi.



Ako vypnú ochranu AVG

Ozna te za iarkavacie polí ko **Do asne vypnú ochranu AVG** a potvr te vo bu stla ením tla idla **Použi** . V novom otvorenom dialógovom okne **Do asne vypnú ochranu AVG** zadajte as, na aký chcete vypnú ochranu **AVG Internet Security**. V predvolenom nastavení sa ochrana vypne na 10 minút, o by malo sta i na dokon enie bežných úloh, ako je inštalácia nového softvéru a pod. Môžete sa rozhodnú pre dlhší asový úsek, ale táto možnos sa neodporú a, ak to nie naozaj potrebné. Potom sa všetky vypnuté sú asti automaticky znovu aktivujú. Nanajvýš môžete vypnú ochranu AVG až do najbližšieho reštartovania počíta a. Samostatnú možnos vypnutia sú asti **Firewall** nájdete v dialógovom okne **Do asne vypnú ochranu AVG**. Ak tak chcete urobi , ozna te polí ko **Deaktívova ochranu sú as ou Firewall**.



3.5.4. Ochrana počítača

3.5.4.1. AntiVirus

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



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

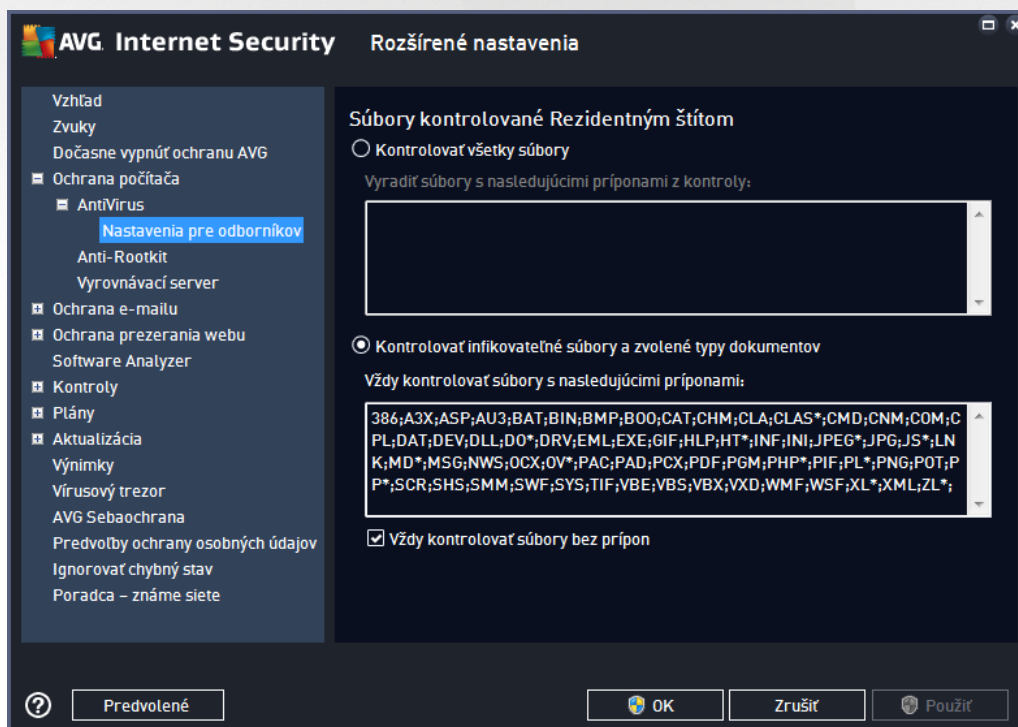
- **Opýtať sa ma pred odstránením hrozieb** (predvolene zapnuté) – za iarknite pre zabezpečenie, že Rezidentný štít nebude vykonávať žiadne akcie automaticky, a namiesto toho zobrazí dialógové okno popisujúce detegovanú hrozbu a umožní vám tak rozhodnúť sa, aká akcia by mala byť vykonaná. Ak ponecháte políčko neza iarknuté, **AVG Internet Security** bude automaticky liečiť infekcie, a ak to nebude možné, bude objekt premiestnený do [Vírusového trezora](#).
- **Nahlásiť potenciálne nežiaduce aplikácie a hrozby spyware** (predvolene zapnuté) – za iarknite toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu malware: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
- **Hlásí rozšírenú skupinu potenciálne nežiaducich programov** (predvolene 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 legítimne programy, a preto je táto funkcia predvolene vypnutá.
- **Kontrola súborov pri zatváraní** (predvolene vypnuté) – kontrola pri zatvorení zabezpečí, že AVG skontroluje aktívne objekty (napr. aplikácie, dokumenty, atď.), keď sa otvárajú alebo zatvárajú; táto funkcia pomáha chrániť počítač pred niektorými druhmi sofistikovaných vírusov.
- **Kontrola v bootovacom sektore odstrániteľných médií** (predvolene zapnuté) – označuje túto možnosť, ak sa majú kontrolovať zavádzacie sektory pripojených USB kúľov, externých diskových jednotiek a iných odstrániteľných médií z hľadiska výskytu hrozieb.



- **Použi heuristickú analýzu** (predvolene zapnuté) – na detekciu sa použije heuristická analýza (dynamická emulácia inštrukcií kontrolovaného objektu v prostredí virtuálneho počítača).
- **Kontrolova súbory uvedené v registroch** (predvolene zapnuté) – tento parameter určuje, že AVG bude kontrolovať všetky spustené súbory pridané do registra na spustenie pri štarte počítača, aby sa známa infekcia nemohla spustiť pri ďalšom spustení počítača.
- **Zapnú dôkladnú kontrolu** (predvolene vypnuté) – v určitých situáciách (napr. v stave mimoriadnej núdze) môžete zapnúť toto políčko aktivovať algoritmus najdôkladnejšej kontroly, ktorý skontroluje všetky možné nebezpečné objekty do hĺbky. Upozorujeme však, že tento spôsob je náročný na procesor.
- **Zapnú ochranu okamžitých správ a sťahovaní cez sieť P2P** (predvolene zapnuté) – zapnite toto políčko, ak chcete overiť, že komunikácie cez okamžité správy (t. j. AIM, Yahoo!, ICQ, Skype, MSN Messenger, atď.) a dáta stiahnuté 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.

Poznámka: Ak je AVG nainštalované vo Windows 10, nachádza sa v zozname jedna položka navyše, nazvaná **Aktivovať Windows Antimalware Scan Interface (AMSI) pre dôkladnejšie kontroly softvéru** – táto funkcia zlepšuje ochranu pred vírusmi, keďže umožňuje Windowsu a AVG užšie spolupracovať pri odhaľovaní škodlivého kódu, vďaka čomu je ochrana spoľahlivejšia a znižuje sa počet nesprávnych detekcií.

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



Označte príslušné zapínacie políčko podľa toho, či chcete použiť možnosť **Kontrolova všetky súbory** alebo **Kontrolova infikovateľné súbory a zvolené typy dokumentov**. Ak chcete urýchliť kontrolu

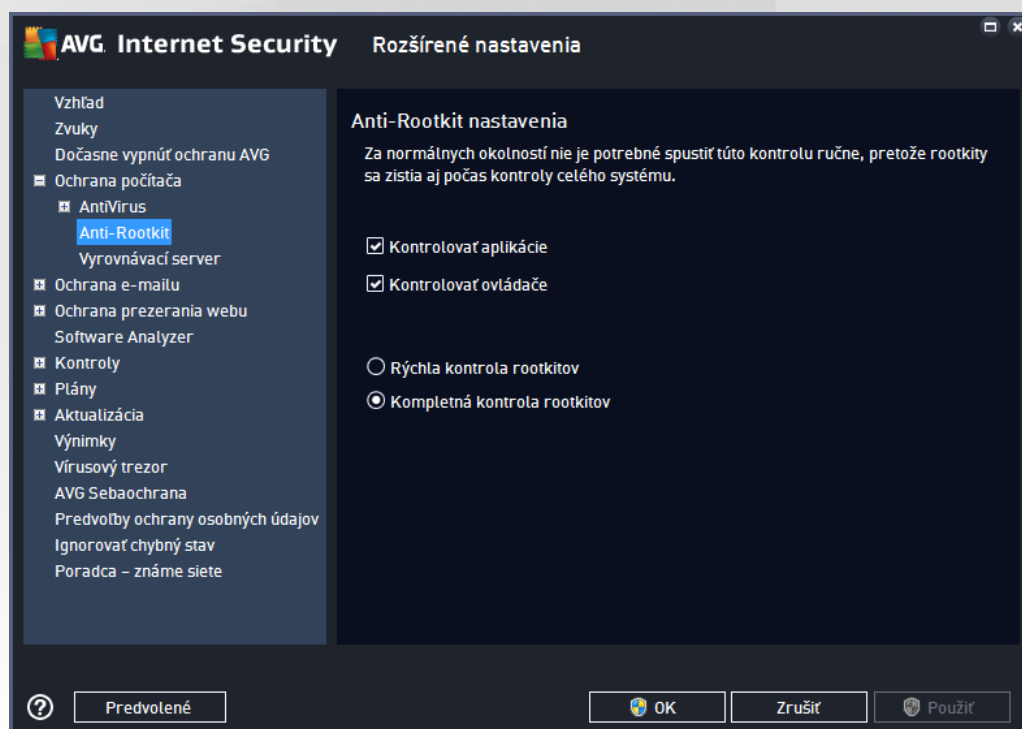


a sú asne zabezpe i maximálnu úrove ochrany, odporú ame zachova predvolené nastavenia. Takto sa budú kontrolova iba infikované súbory. V príslušnej asti dialógového okna nájdete aj upravený zoznam prípon súborov, ktoré sa majú za leni do kontroly.

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

3.5.4.2. Anti-Rootkit

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



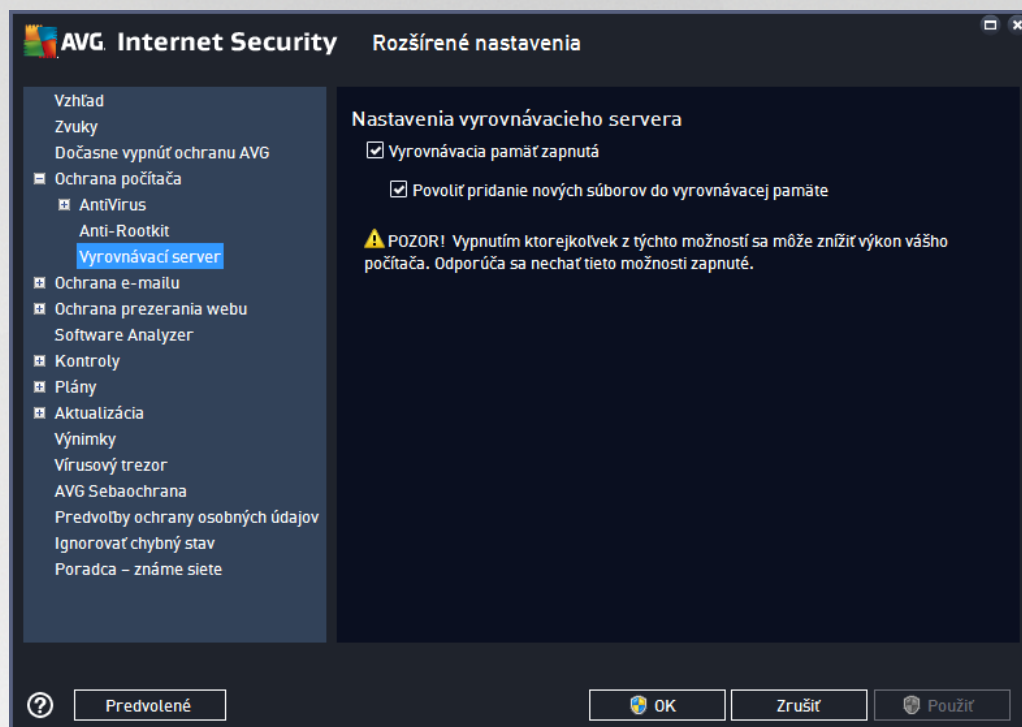
Možnosti **Kontrolova aplikácie** a **Kontrolova ovláda e** vám umož ňujú podrobne zada , o by malo by sú as ou kontroly Anti-Rootkit. Tieto nastavenia sú ur ené pre skúsených používateľov, odporú ame vám, aby ste nechali všetky možnosti zapnuté. Môžete tiež vybra režim kontroly rootkitov:

- **Rýchla kontrola rootkitov** – kontroluje všetky spustené procesy, zavedené ovláda e a systémový prie inok (zvy ajne *c:\Windows*)
- **Kompletná kontrola rootkitov** – kontroluje všetky spustené procesy, zavedené ovláda e, systémový prie inok (zvy ajne *c:\Windows*), a navyše všetky miestne disky (*vrátane pamä ových médií, nie však disketové jednotky/jednotky CD-ROM*)



3.5.4.3. Server vyrovnávacej pamäte

Dialógové okno **Nastavenia servera vyrovnávacej pamäte** sa týka procesu servera vyrovnávacej pamäte určeného na zrýchlenie všetkých typov kontrol **AVG Internet Security**:



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 nie je potrebné ich kontrolovať. Preto sa počas kontroly vynechávajú.

Dialógové okno **Nastavenie servera vyrovnávacej pamäte** ponúka nasledujúce možnosti konfigurácie:

- **Vyrovnávacia pamäť zapnutá** (*predvolene zapnuté*) – zrušením označenia tohto políčka sa vypne **server vyrovnávacej pamäte** a vyprázdni sa vyrovnávacia pamäť. Upozorujeme, že sa týmto môže spomaliť kontrola a zníži celkový výkon počítača, pretože každý jeden používaný súbor sa najskôr skontroluje, či neobsahuje vírusy a spyware.
- **Povoliť prídanie nových súborov do vyrovnávacej pamäte** (*predvolene zapnuté*) – zrušením označenia tohto políčka sa zastaví pridávanie ďalších súborov do vyrovnávacej pamäte. Všetky súbory už vložené do vyrovnávacej pamäte sa zachovávajú a budú sa používať do úplného vypnutia ukladania do vyrovnávacej pamäte alebo do ďalšieho aktualizovania vírusovej databázy.

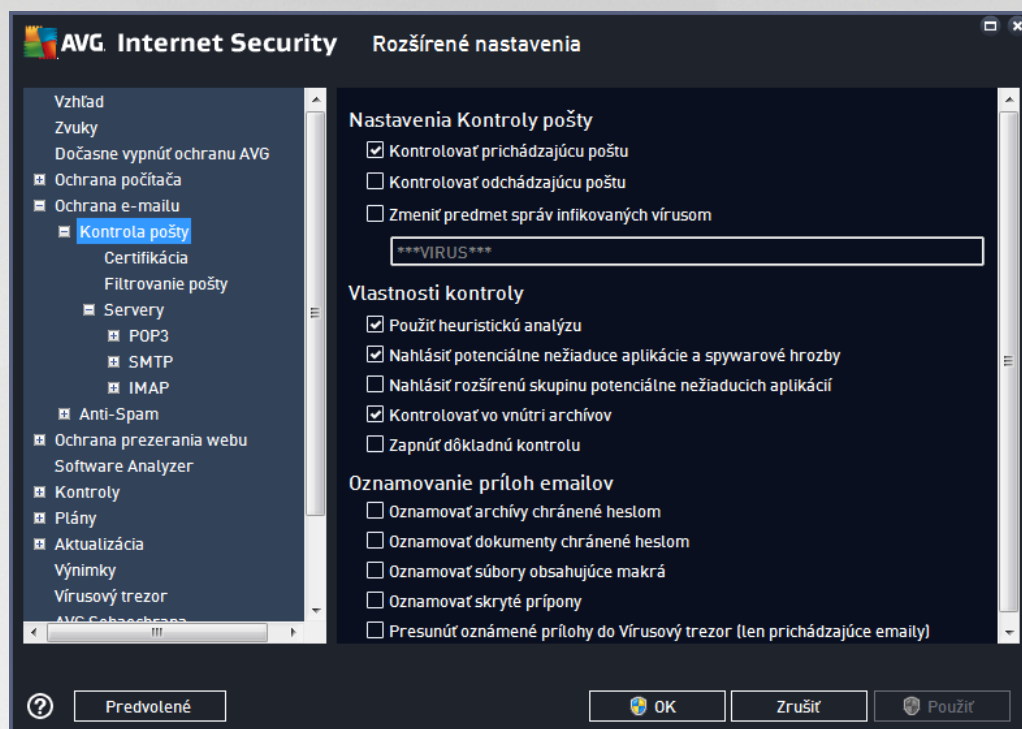
Ak nemáte oprávnený dôvod na vypnutie servera vyrovnávacej pamäte, dôrazne odporúčame zachovať predvolené nastavenia a nechať obe možnosti zapnuté. Inak môžete zaznamenať výrazné spomalenie rýchlosti a výkonu systému.

3.5.5. Kontrola pošty

V tejto časti môžete upraviť podrobnosti konfigurácie nástroja [Kontrola pošty](#) a [Anti-Spam](#):

3.5.5.1. Kontrola pošty

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



Kontrola pošty

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

- **Kontrola prichádzajúcu poštu** (predvolene zapnuté) – začiarknutím zapnete resp. vypnete funkciu na kontrolu všetkých e-mailových správ doručených do vášho e-mailového klienta
- **Kontrola odchádzajúcu poštu** (predvolene vypnuté) – začiarknutím zapnete resp. vypnete funkciu na kontrolu všetkých e-mailov poslaných z vašej poštovej aplikácie
- **Zmeni predmet správ infikovaných vírusom** (predvolene vypnuté) – ak chcete byť informovaní o detegovaní infekcie v prichádzajúcej 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 kontrolovať:

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



toto polí ko, ak chcete aktivova kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu malware: aj ke v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu by nainštalované úmyselne. Odporúame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.

- **Hlási rozšírenú skupinu potenciálne nežiaducich programov (predvolene vypnuté)** – začiarknite toto polí ko, 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 predvolene vypnutá.
- **Kontrola vo vnútri archívov (predvolene zapnuté)** – začiarknite toto polí ko, ak sa má kontrolovať obsah archívov priložených k e-mailovým správam.
- **Zapnú dôkladnú kontrolu (predvolene vypnuté)** – v určitých situáciách (napr. pri podozrení na infikovanie počítača a vírusom alebo zneužitím) môžete začiarknutím tohto polí ka 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.

Hlásenie príloh e-mailov

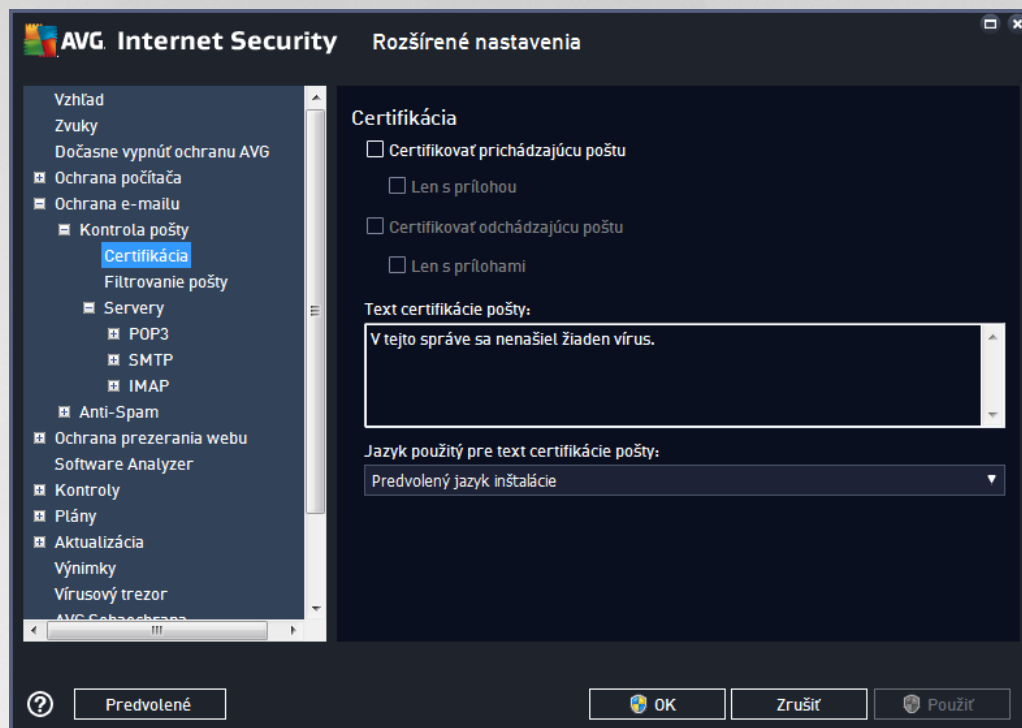
Táto časť umožňuje nastaviť ďalšie správy o súboroch, ktoré môžu by potenciálne nebezpečné alebo podozrivé. Nezobrazí sa žiadne dialógové okno, na koniec e-mailovej správy sa len pridá text certifikácie a všetky takéto správy budú uvedené v dialógovom okne [Nálezy súčasti Ochrana e-mailu](#):

- **Oznamova archívy chránené heslom** – archívy (ZIP, RAR, atď.) chránené heslom sa nedajú skontrolovať na prítomnosť vírusov; začiarknite toto polí ko, ak sa majú oznamovať tieto archívy ako potenciálne nebezpečné.
- **Oznamova dokumenty chránené heslom** – dokumenty chránené heslom sa nedajú skontrolovať na prítomnosť vírusov; začiarknite toto polí ko, ak sa majú oznamovať tieto dokumenty ako potenciálne nebezpečné.
- **Oznamova súbory obsahujúce makrá** – makro je vopred definovaný sled krokov, ktoré zjednodušujú konkrétne úlohy používateľovi (makrá používané v MS Word sú veľmi známe). Makro ako také môže obsahovať potenciálne nebezpečné inštrukcie, a preto je vhodné začiarknuť toto polí ko, aby sa súbory s makrami oznamovali ako podozrivé.
- **Oznamova skryté prípony** – skrytá prípona môže spôsobiť, že sa bude podozrivý spustiteľný súbor „nie o.txt.exe“ javiť ako neškodný jednoduchý textový súbor „nie o.txt“; začiarknite toto polí ko, 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 takáto správa identifikuje počas kontroly, uvedte, či sa má detegovaný infikovaný objekt presunúť do [Vírusového trezora](#).

V dialógovom okne **Certifikácia** môžete označiť konkrétne začiarkacie polí ka a určiť, či chcete certifikovať prichádzajúcu poštu (**Certifikovať prichádzajúcu poštu**) alebo odchádzajúcu poštu (**Certifikovať odchádzajúcu poštu**). Pri každej možnosti môžete alej určiť parameter **Len s prílohami**. Vtedy sa

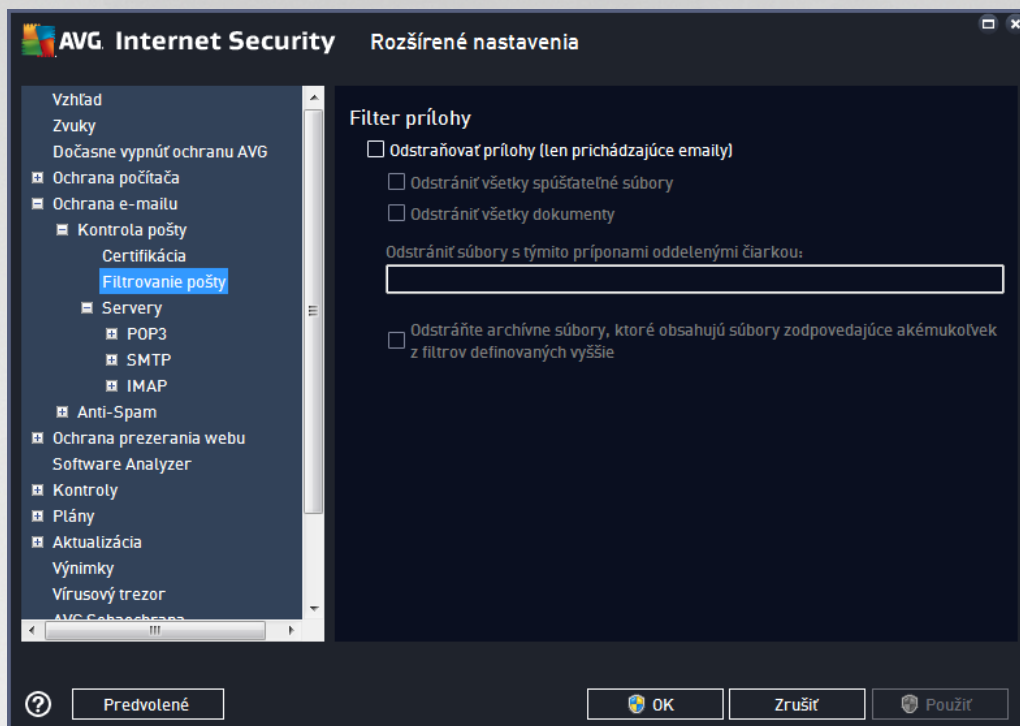


certifikácia bude týka iba e-mailových správ s prílohami:



Predvolene text certifikácie obsahuje iba základnú informáciu: *V tejto správe sa nenašiel žiadny vírus.* Tieto informácie však podľa potreby môžete rozšíriť alebo zmeniť: do políčka **Text e-mailovej certifikácie** napíšte požadovaný text certifikácie. V poli **Jazyk použitý pre text e-mailovej certifikácie** môžete tiež definovať, v akom jazyku sa má automaticky vytváraná certifikácia (*V tejto správe sa nenašiel žiadny vírus*) zobrazovať.

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



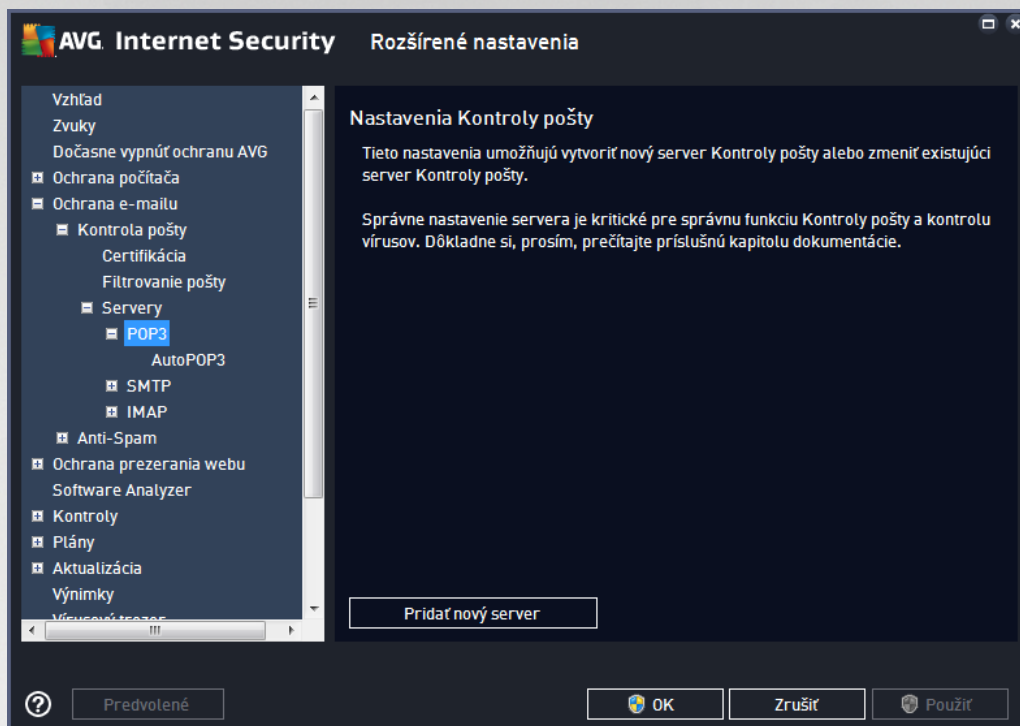
Dialógové okno **Filter príloh** vám umožní nastaviť parametre pre kontrolu príloh e-mailových správ. V predvolenom nastavení je možnosť **Odstrániť prílohy** vypnutá. Ak sa rozhodnete ju aktivovať, všetky prílohy e-mailových správ detegované ako infekcie alebo potenciálne nebezpečné programy sa automaticky odstránia. Ak chcete definovať konkrétne typy príloh, ktoré sa majú odstrániť, vyberte príslušnú možnosť:

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

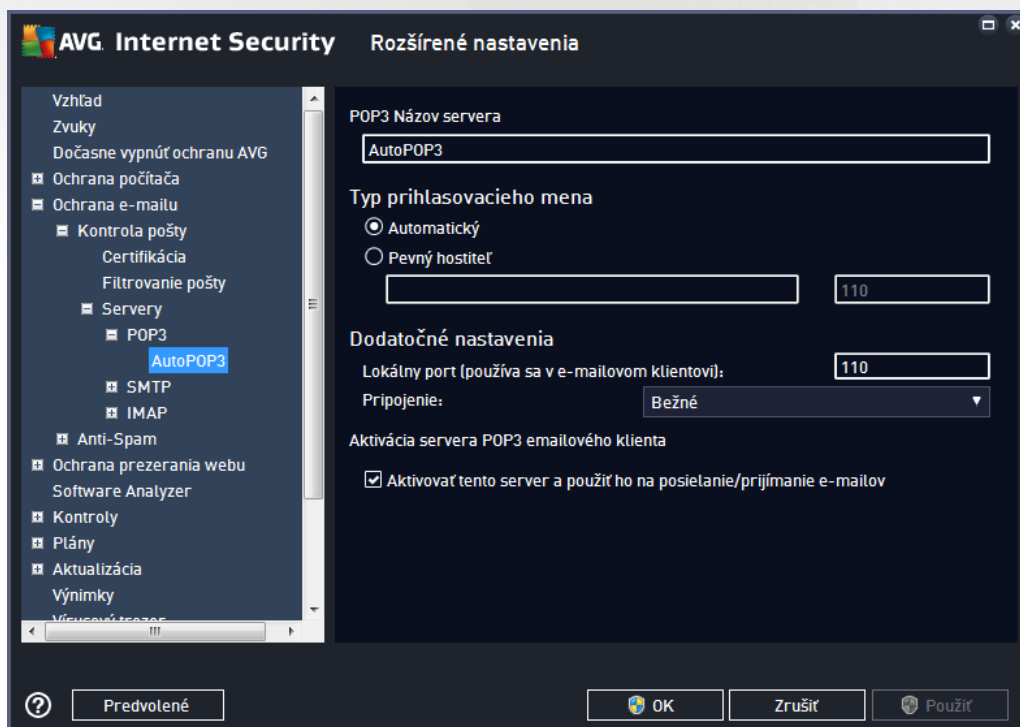
V časti **Servery** môžete upraviť parametre serverov súčasti [Kontrola pošty](#):

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

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



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

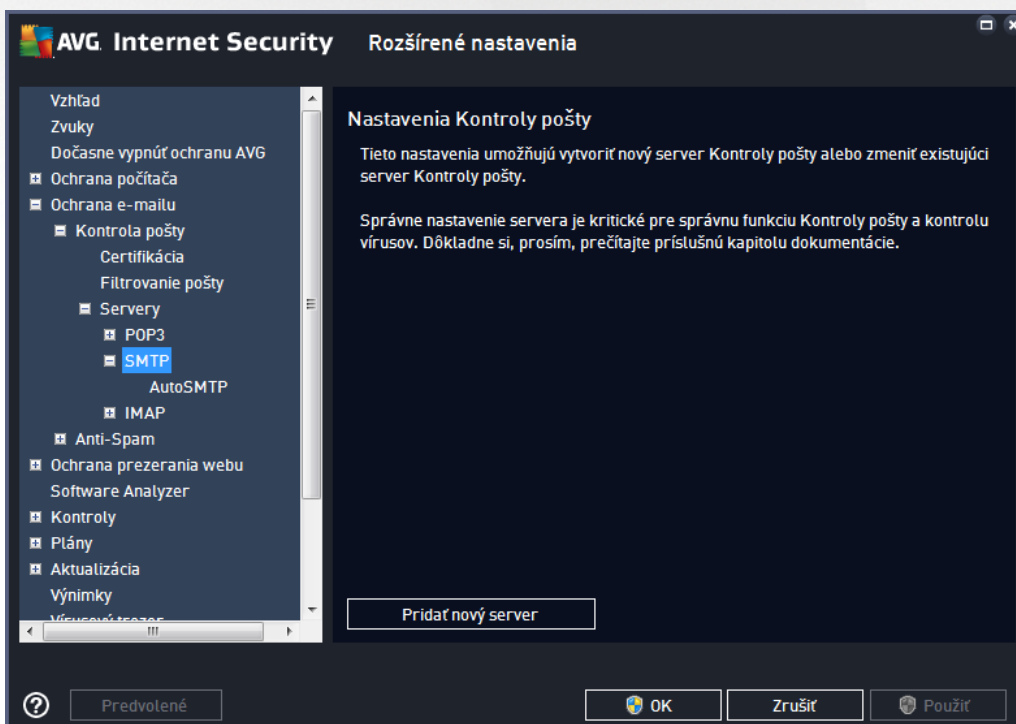


- **Názov servera POP3** – do tohto poľa môžete zadať názov novo pridaných serverov (na pridanie)



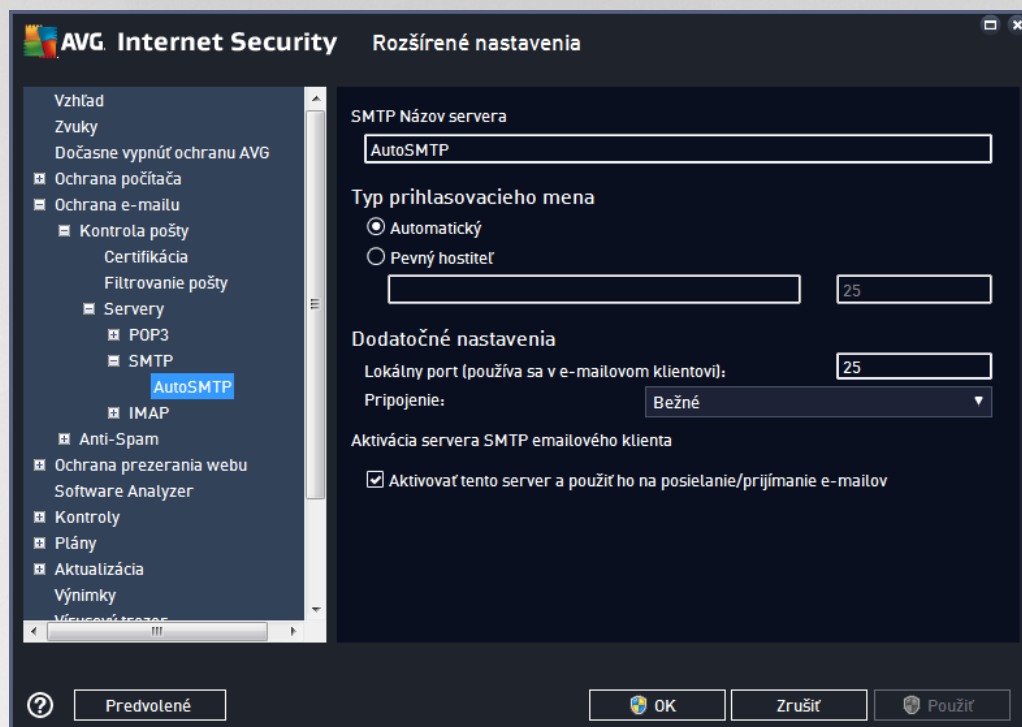
servera POP3 kliknite pravým tlačidlom myši na položku POP3 v akejkoľvek ponuke).

- **Typ prihlásenia** – určuje metódu určovania e-mailového servera, ktorý sa používa pre prichádzajúcu poštu:
 - **Automaticky** – prihlásenie sa uskutoční automaticky podľa nastavení vášho e-mailového klienta.
 - **Pevný hosť** – v tomto prípade program vždy použije server, ktorý je tu uvedený. Zadajte adresu alebo názov svojho emailového serveru. Prihlasovacie meno zostane nezmenené. Ako názov môžete použiť názov domény (napríklad *pop.acme.com*), ako aj adresu IP (napríklad *123.45.67.89*). Ak poštový server používa neštandardný port, môžete zadať tento port za názvom servera a použijete dvojbodku ako oddeľovací znak (napríklad *pop.acme.com:8200*). Štandardný port pre komunikáciu POP3 je 110.
- **Dodatkové nastavenia** – uvádza podrobnejšie parametre:
 - **Lokálny port** – uvádza port, na ktorom sa odohráva komunikácia 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, ak ju podporuje cieľový poštový server.
- **Aktivácia servera POP3 v e-mailovom klientovi** – označením/zrušením označenia tejto položky sa aktivuje, resp. deaktivuje uvedený server POP3





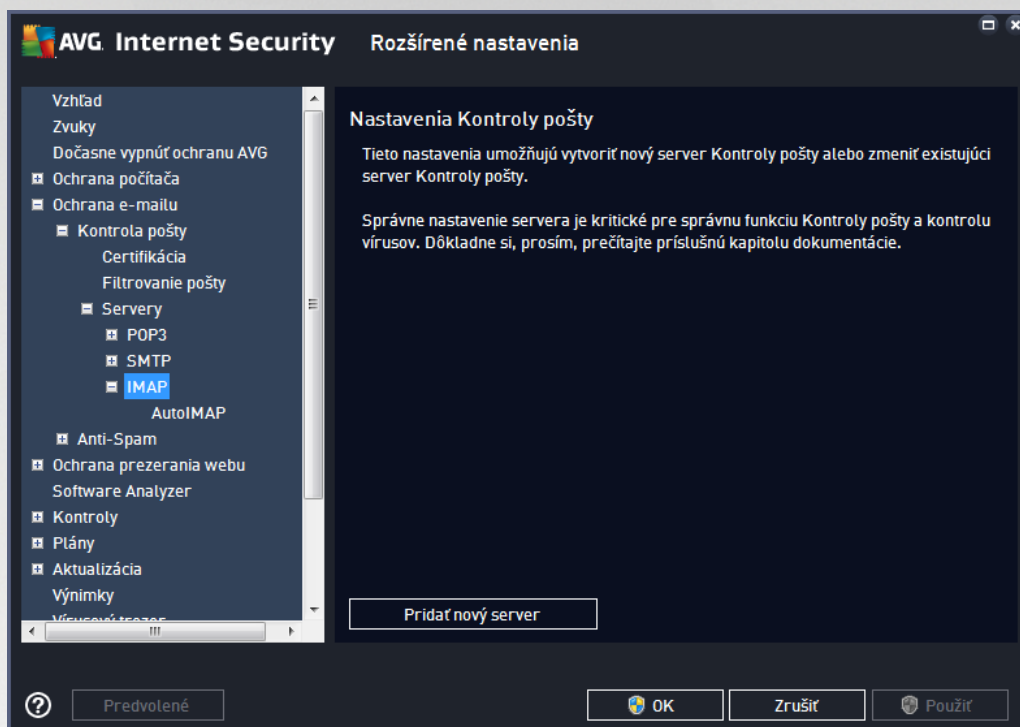
Toto dialógové okno umožňuje nastaviť pre súčasť s [Kontrolou pošty](#) nový server pomocou protokolu SMTP pre odchádzajúcu poštu:



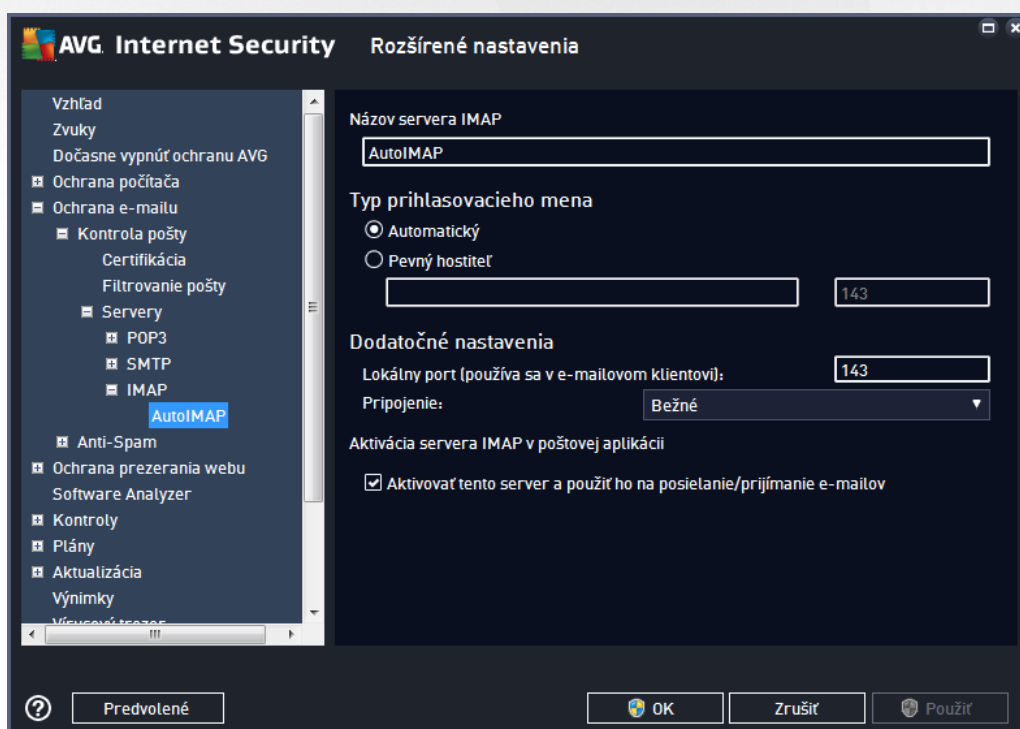
- **Názov servera SMTP** – do tohto poľa zadajte názov novo pridaných serverov (na pridanie servera SMTP kliknite pravým tlačidlom myši na položku SMTP v akejkoľvek navigačnej ponuke). Pre automaticky vytvorené servery „AutoSMTP“ je toto pole vypnuté.
- **Typ prihlásenia** – určuje spôsob zistenia poštového servera, ktorý sa používa pre odchádzajúcu poštu:
 - **Automaticky** – prihlásenie sa uskutočňuje automaticky podľa nastavení vášho e-mailového klienta
 - **Pevný hostiteľ** – v tomto prípade program vždy použije server, ktorý je tu uvedený. Zadajte adresu alebo názov svojho emailového serveru. 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 oddelovací znak použijete dvojbodku (napríklad *smtp.acme.com:8200*). Štandardný port pre komunikáciu SMTP je 25.
- **Dodatočné nastavenia** – uvádza podrobnejšie parametre:
 - **Lokálny port** – uvádza port, na ktorom sa uskutočňuje komunikácia 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/predvolené SSL*). Ak nastavíte pripojenie SSL, potom sa budú posielať dáta šifrované a žiadna tretia strana ich nebude môcť vypočítať ani monitorovať. Táto funkcia je dostupná len vtedy, keď ju podporuje cieľový poštový server.



- **Aktivácia servera SMTP v e-mailovom klientovi** – za iarknutím alebo zrušením za iarknutia tohto polí ka sa aktivuje, resp. deaktivuje vyššie uvedený server SMTP



Toto dialógové okno umož ňuje nastavi pre sú as [Kontrola pošty](#) nový server pomocou protokolu IMAP pre odchádzajúcu poštu:





- **Názov servera IMAP** – do tohto poľa a zadajte názov novo pridaných serverov (na pridanie servera IMAP kliknite pravým tlačidlom myši na položku IMAP v akejkoľvek ponuke).
- **Typ prihlásenia** – určuje spôsob zistenia poštového servera, ktorý sa používa pre odchádzajúcu poštu:
 - **Automaticky** – prihlásenie sa uskutočňuje automaticky podľa nastavení vášho e-mailového klienta
 - **Pevný hosť** – v tomto prípade program vždy použije server, ktorý je tu uvedený. Zadajte adresu alebo názov svojho emailového serveru. 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 dvojčiarok ako oddelovacieho znaku (napríklad *imap.acme.com:8200*). Štandardný port pre komunikáciu IMAP je 143.
- **Dodatkové nastavenia** – uvádza podrobnejšie parametre:
 - **Lokálny port používaný v** – určuje port, na ktorom sa má uskutočňovať 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/predvolené SSL). Ak si zvolíte pripojenie SSL, zaslané údaje budú zakódované bez rizika vystopovania alebo monitorovania treťou stranou. Táto funkcia je dostupná len vtedy, keď ju podporuje cieľový poštový server.
- **Aktivácia servera IMAP v e-mailovom klientovi** – za kliknutím alebo zrušením za kliknutia tohto poľa sa aktivuje, resp. deaktivuje vyššie uvedený server IMAP

3.5.5.2. Anti-Spam

V dialógovom okne **Nastavenia súčasti Anti-Spam** môžete za kliknutím alebo zrušením za kliknutia poľa **Zapnúť ochranu Anti-Spam** zapnúť, resp. vypnúť kontrolu e-mailovej komunikácie súčasti Anti-Spam. Táto možnosť je predvolene zapnutá a odporúčame vám, aby ste toto nastavenie nikdy nenechali, ak na to nemáte skutočný dôvod.

Okrem toho môžete nastaviť viac alebo menej agresívne hodnotenie skóre. Filter súčasti **Anti-Spam** pridelí každej správe skóre (t. j. v akej miere sa obsah správy podobá nevyžiadanej pošte) na základe niekoľkých dynamických metód kontroly. Môžete nastaviť položku **Označenie správ ako spam, ak je skóre vyššie ako** buď zadaním hodnoty, alebo presunutím posúvača doľava alebo doprava.

Rozsah hodnôt je obmedzený od 50 do 90. Toto je základný prehľad prahovej hodnoty skóre:

- **Hodnota 80 – 90** – budú sa filtrovať e-mailové správy, ktoré veľa pravdepodobne patria medzi nevyžiadajúcu poštu. Niektoré správy, ktoré nie sú nevyžiadajúcou poštou, sa môžu filtrovať nesprávne.
- **Hodnota 60 – 79** – považuje sa za celkom agresívnu konfiguráciu. E-mailové správy, ktoré môžu predstavovať nevyžiadajúcu poštu, sa budú filtrovať. Pravdepodobne sa zachytia aj správy, ktoré nie sú nevyžiadajúcou poštou.
- **Hodnota 50 – 59** – veľa agresívne nastavenie. E-mailové správy, ktoré nie sú nevyžiadajúcou poštou, sa pravdepodobne zachytia ako správy nevyžiadajúcej pošty. **Tento rozsah prahov sa neodporúča a na**



normálne použitie.

V dialógovom okne **Nastavenia sú astí Anti-Spam** môžete alej definova , ako sa bude zaobchádza s nájdenou nevyžiadanou poštou:

- **Premiestni správu do prie inka pre neželané správy** (len ako doplnok pre Microsoft Outlook) – za iarknite toto polí ko, ak sa má každá detegovaná správa nevyžiadanej pošty automaticky premiestni do konkrétneho prie inka pre spam v e-mailovom klientovi MS Outlook. V sú asnosti túto funkciu iní e-mailoví klienti nepodporujú.
- **Prida príjemcov poslaných e-mailov do zoznamu povolených príjemcov** – za iarknite toto polí ko, ak sa majú všetci príjemcovia odoslaných 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 nesprávneho detegovania** – ak ste po as procesu 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 zaradi do kategórie spamu.

V dialógovom okne **Nastavenia výkonu jadra** (otvára sa pomocou položky **Výkon** v ponuke na avej strane) sa nachádzajú výkonové nastavenia sú astí **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 nevyžiadanej pošty. Na identifikáciu sa použijú len tréningové údaje. Tento režim vám neodporú ame používa na bežné ú ely. Používajte ho len vtedy, keď má počíta ve mi slabý hardvér.
- **Drahší desktop** – v tomto režime sa bude využíva vä šie množstvo pamäte. Po as procesu preh adávania na zis ovanie prítomnosti spamu sa použijú nasledovné funkcie: pravidlá a vyrovnávacia pamä databázy nevyžiadanej pošty, základné a rozšírené pravidlá, adresy IP rozosielate ov nevyžiadanej pošty a databázy rozosielate ov nevyžiadanej pošty.

Položka **Povoli kontrolu on-line** je predvolene zapnutá. Má za následok presnejšiu detekciu nevyžiadanej pošty cez komunikáciu so servermi [Mailshell](#), t. j. preh adávané údaje sa porovnávajú s online databázami [Mailshell](#).

Oby ajne sa odporú a ponecha predvolené nastavenia a zmeni ich len vtedy, ak k tomu máte závažný dôvod. Zmeny konfigurácie odporú ame robi len skúseným používateľom!

Položka **Zoznam povolených odosielate ov** otvorí dialógové okno s názvom **Zoznam schválených odosielate ov e-mailov** s globálnym zoznamom povolených e-mailových adres odosielate ov a názvom domén, ktorých správy nebudú nikdy ozna ené 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 (napr. *avg.com*), o ktorých viete, že nevytvárajú správy nevyžiadanej pošty. 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 adres naraz.

Ovládacie tlačidlá

Sú dostupné nasledovné ovládacie tlačidlá:

- **Upraviť** – po stlačení tohto tlačidla sa otvorí dialógové okno, do ktorého môžete ručne zadať zoznam adres (môžete použiť aj metódu *kopírovať a prilepiť*). Do každého riadka vložte vždy jednu položku (odosielateľ, názov domény).
- **Exportovať** – ak sa z nejakého dôvodu rozhodnete exportovať záznamy, môžete tak urobiť stlačením 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 jednoducho 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 adres odosielateľov a názvov domén, ktorých správy sa vždy označia ako spam.

V rozhraní úprav môžete zostaviť zoznam odosielateľov, od ktorých odakávate nevyžiadané správy (spam). Zároveň môžete vytvoriť zoznam úplných názvov domén (napr. *spamingspolocnost.sk*), od ktorých odakávate alebo ste dostali nevyžiadajúcu poštu. Všetky emaily z uvedených adres/domén budú identifikované ako nevyžiadajúca pošta. 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 adres naraz.

Ovládacie tlačidlá

Sú dostupné nasledovné ovládacie tlačidlá:

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



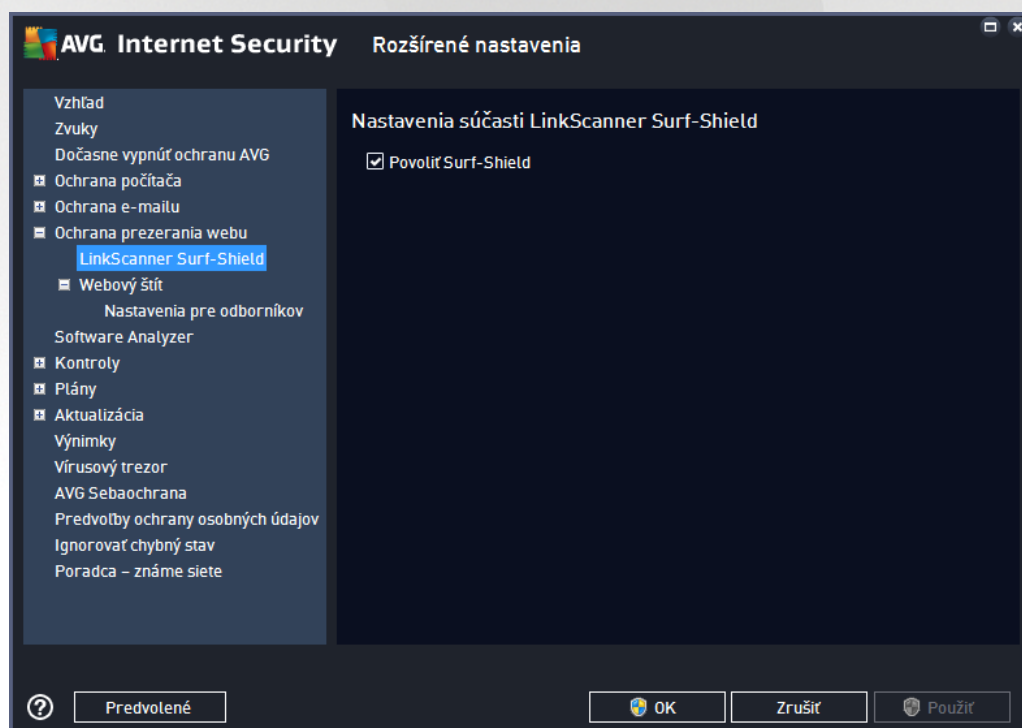
jednotlivé dialógové okná, ale v používateľskom rozhraní sa nachádza stručný opis každej príslušnej možnosti. Dôrazne odporúčame nenechať žiadne nastavenia, ak nie ste dokonale oboznámení s rozšírenými nastaveniami programu Spamcatcher (MailShell Inc.). Každá nevhodná zmena môže mať za následok zníženie výkonu alebo nesprávne fungovanie súčasti.

Ak sa aj napriek tomu rozhodnete zmeniť konfiguráciu súčasti Anti-Spam na vyššej 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.

3.5.6. Ochrana prezerania webu

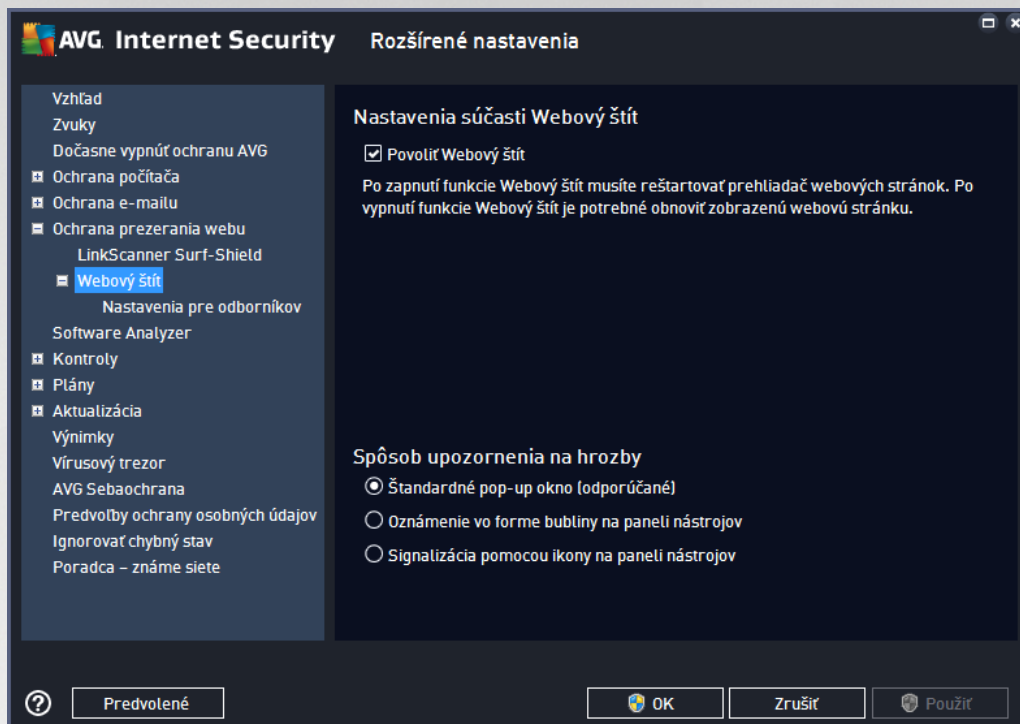
Dialógové okno s nastaveniami súčasti **LinkScanner** vám umožní zapnúť/vypnúť tieto funkcie:



- **Povolí Surf-Shield** – (predvolene 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).

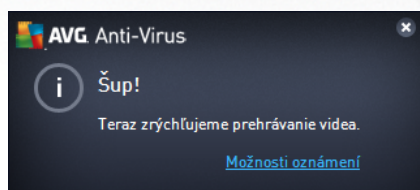


3.5.6.1. Webový štít



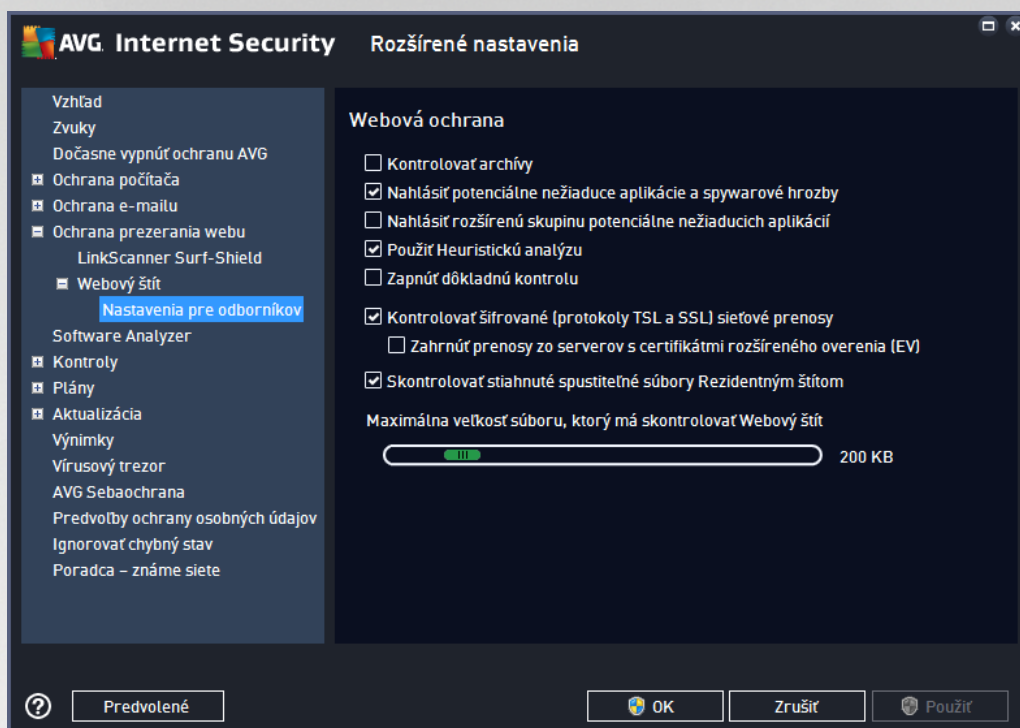
Dialógové okno **Webový štít** ponúka tieto možnosti:

- **Povoliť Webový štít** (predvolené zapnuté) – aktivuje/deaktivuje celú službu **Webový štít**. Ďalšie rozšírené nastavenia **Webového štítu** nájdete v nasledujúcom dialógovom okne s názvom [Webová ochrana](#).
- **Povoliť AVG Accelerator** (predvolené zapnuté) – aktivuje/vypne sa služba AVG Akcelerátor. AVG Akcelerátor umožňuje stabilnejšie prehrávanie on-line videa a ušetrí pamäť. Ďalšie s ohľadom na akceleráciu 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 informácie o nej ikony v paneli úloh.



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

- **Kontrolovať archívy** – (predvolene vypnuté): kontroluje obsah archívov, ktoré sa môžu nachádzať na otvorenej webovej stránke.
- **Nahlásiť potenciálne nežiaduce programy a spyware hrozby** – (predvolene zapnuté): zaškrtnite toto políčko, ak chcete aktívovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu malware: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
- **Nahlásiť rozšírenú skupinu potenciálne nežiaducich aplikácií** – (predvolene 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 počítača, ale môže blokovать dobré programy, a preto je táto funkcia predvolene vypnutá.
- **Použiť heuristickú analýzu** – (predvolene zapnuté): kontroluje obsah zobrazovanej stránky pomocou metódy heuristickej analýzy (dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí).
- **Zapnúť dôkladnú kontrolu** – (predvolene 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.
- **Kontrolovať šifrované (protokoly TSL a SSL) sieťové prenosy** – (predvolene zapnuté):



nechajte označené, aby ste umožnili AVG kontrolovať taktiež všetku šifrovanú sieťovú komunikáciu, teda spojenia prostredníctvom zabezpečených protokolov (SSL a jeho novšia verzia TLS). Týka sa to webových stránok používajúcich protokol HTTPS a pripojení e-mailových klientov používajúcich protokol TLS/SSL. Zabezpečené prenosy sa dešifrujú, skontrolujú, či neobsahujú malware, znova sa zašifrujú a bezpečne sa odošlú do počítača. V rámci tejto možnosti sa môžete rozhodnúť **Zahrnúť prenosy zo serverov s certifikátmi rozšíreného overenia (EV)** a kontrolovať taktiež šifrovanú sieťovú komunikáciu so servermi, ktoré sú certifikované pomocou certifikátu rozšíreného overenia. Vydanie certifikátu EV vyžaduje predloženie platnosti certifikátnym orgánom a webové stránky prevádzkované na základe certifikátu sú preto omnoho dôveryhodnejšie (*je menej pravdepodobné, že budú prenášať malware*). Z tohto dôvodu sa môžete rozhodnúť nekontrolovať prenosy z certifikovaných serverov EV, čo by malo mierne zrýchliť šifrovanú komunikáciu.

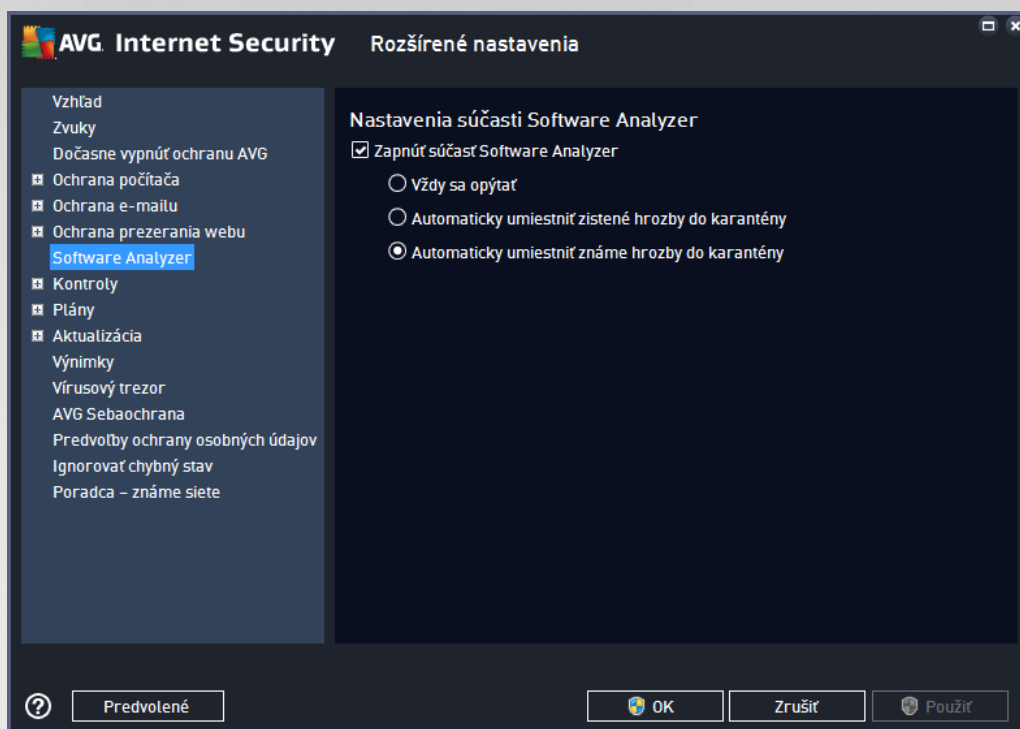
- **Skontrolovať stiahnuté spustiteľné súbory Rezidentným štítom** – (predvolene zapnuté): kontrolovať spustiteľné súbory (typicky prípony *exe, bat, com*) po ich stiahnutí. Rezidentný štít kontroluje súbory pred stiahnutím, aby zabezpečil, že sa žiadny škodlivý kód nedostane do vášho počítača. Táto kontrola je však obmedzená **Maximálnou iastkovou ve kosou kontrolovaného súboru** – pozrite si nasledujúcu položku v tomto dialógovom okne. Preto sú všetky súbory kontrolované po istých, a to isté platí aj pre váš šírku spustiteľných súborov. Spustiteľné súbory môžu vo vašom počítači vykonávať rôzne úlohy, a preto je nevyhnutne nutné, aby boli na 100 % bezpečné. To je možné zabezpečiť kontrolou súboru pred jeho stiahnutím a taktiež kontrolou ihneď po dokončení stiahnutia súboru. Odporúčame vám ponechať túto možnosť zaškrtnutú. Ak túto možnosť deaktivujete, stále môžete byť pokojní, že AVG nájde akýkoľvek potenciálne škodlivý kód. Len obvykle nebude schopný posúdiť spustiteľný súbor ako celok, takže môže ohlasovať nieko ko nesprávnych detekcií.

Posúvať v dolnej časti dialógového okna vám umožní určiť **Maximálnu iastkovú ve kosou kontrolovaného súboru** – ak sa priložené súbory nachádzajú na otvorenej stránke, potom sa ich obsah môže zároveň skontrolovať ešte predtým, než sa súbory stiahnu do počítača. Kontrola veľkých súborov však chvíľu trvá a stiahnutie z internetovej stránky sa môže výrazne spomaliť. Pomocou posúvať a môžete nastaviť maximálnu veľkosť súboru, ktorá sa má kontrolovať súčasne **Webový štít**. Aj keď je stiahnutý 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.

3.5.7. Software Analyzer

Software Analyzer je súčasťou na ochranu pred malware, ktorá vás chráni pred všetkými typmi malware (spyware, softvérové roboty, krádeže identity atď.). Používa behaviorálne technológie a poskytuje okamžitú ochranu pred novými vírusmi (podrobný popis funkcií tejto súčasti nájdete v kapitole [Software Analyzer](#)).

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



Aktívova Software Analyzer (predvolene zapnuté) – zrušením za iarknutia sa vypne sú as [Identita](#). **Odporú ame, aby ste tak u inili len v prípade, ak to je naozaj nevyhnutné!** Ke je sú as Software Analyzer aktivovaná, môžete nastavi , o sa má urobi pri detegovaní hrozby:

- **Vždy sa opýta** – pri detegovaní hrozby sa vás program opýta, i sa má hrozba premiestni do karantény, aby nedošlo k neželanému odstráneniu aplikácií, ktoré chcete používa .
- **Automatically umiestni zistené hrozby do karantény** – ozna te toto za iarkavacie polí ko, ak si želáte všetky potenciálne zistené hrozby ihne premiestni na bezpečné miesto vo [Vírusovom trezore](#). Ponechaním predvolených nastavení sa vás pri zistení hrozby program opýta, i sa má hrozba premiestni do karantény, aby nedošlo k neželanému odstráneniu aplikácií, ktoré chcete používa .
- **Automatically umiestni známe hrozby do karantény (predvolene zapnuté)** – nechajte toto za iarkavacie polí ko ozna éné, ak si želáte všetky aplikácie ozna éné ako potenciálne škodlivé automaticky a ihne premiestni do [Vírusového trezora](#).

3.5.8. Kontroly

Rozšírené nastavenia kontroly sú rozdelené na štyri kategórie pod a konkrétnych typov kontroly definovaných dodávate om softvéru:

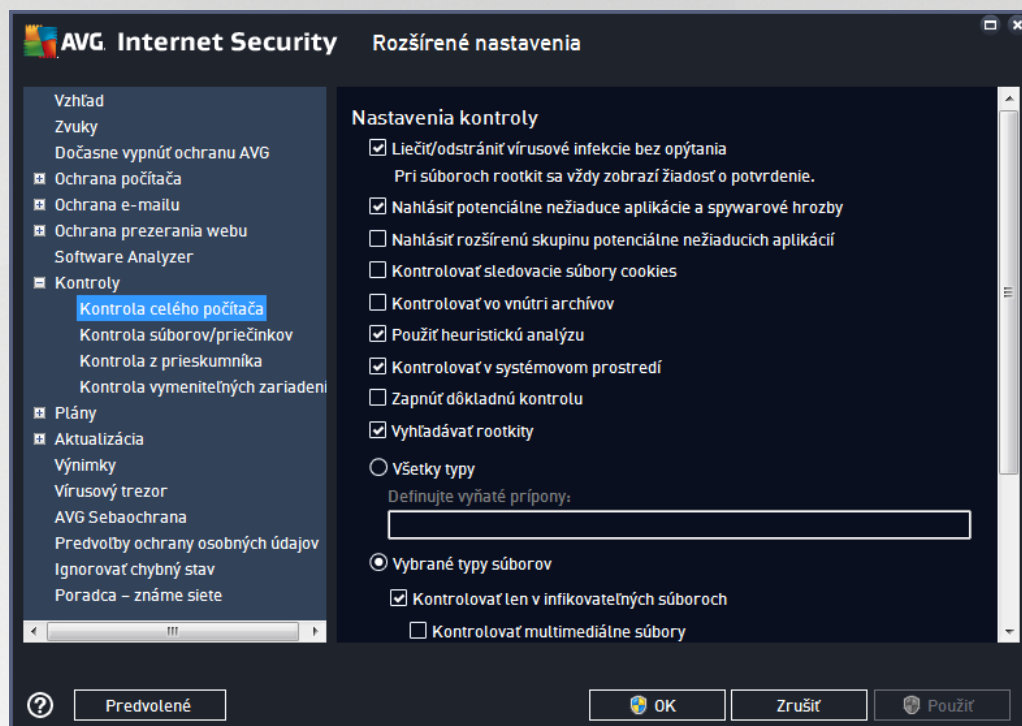
- [Kontrola celého počíta a](#) – štandardná vopred definovaná kontrola celého počíta a.
- [Kontrola súborov/prie inkov](#) – štandardná vopred definovaná kontrola vybraných oblastí počíta a.
- [Kontrola z prieskumnika](#) – špeciálna kontrola vybraného objektu priamo v prostredí programu Windows Explorer.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



po ťa a.

3.5.8.1. Kontrola celého počítača

Funkcia **Kontrola celého po ťa a** umož ťuje upravi parametre jednej z kontrol vopred definovaných výrobcem softvéru, [Kontrola celého po ťa a](#):



Nastavenia kontroly

V ťasti **Nastavenia kontroly** sa nachádza zoznam parametrov kontroly, ktoré sa dajú volite ne zapnú , resp. vypnú :

- **Lie i /odstráni vírusovú infekciu bez opýtania** (predvolene zapnuté) – ak sa po as kontroly nájde vírus, môže by automatickyylie ený, pokia je liek k dispozícii. Ak nie je možné infikovaný súborylie i automaticky, premiestni sa do [Vírusového trezora](#).
- **Nahlási potenciálne nežiaduce aplikácie a hrozby spyware** (predvolene zapnuté) – za iarknite toto polí ko, ak chcete aktivova kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu malware: 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 zabezpe enia po ťa a.
- **Hlási rozšírenú skupinu potenciálne nežiaducich programov** (predvolene vypnuté) – za iarknite toto polí ko, ak sa má detegova rozšírená skupina spywaru: programov, ktoré sú úplne v poriadku a neškodné, ke sa získajú priamo od výrobcu, ale neskôr sa dajú zneuži na škodlivé ú ely. Toto je alšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpe enia po ťa a, ale môže blokova dobré programy, a preto je táto funkcia predvolene vypnutá.
- **Kontrolova sledovacie súbory cookies** (predvolene vypnuté) – tento parameter sú ťasti zapína



detekciu súborov cookies; (súbory 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** (predvolene vypnuté) – tento parameter určuje, že sa majú po as kontroly preverovať všetky súbory uložené vnútri archívov, napr. ZIP, RAR, atď.
- **Použi heuristickú analýzu** (predvolene zapnuté) – heuristická analýza (dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom prostredí) bude jednou z metód, ktoré sa použijú na detekciu vírusov po as kontroly.
- **Kontrolova v systémovom prostredí** (predvolene zapnuté) – po as kontroly sa overujú systémové oblasti počítača.
- **Zapnú dôkladnú kontrolu** (predvolene 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 as.
- **Kontrolova rootkity** (predvolene zapnuté) – [Anti-Rootkit](#) skontroluje počítača a zisťuje prítomnosť potenciálnych rootkitov, t. j. programov a technológií, ktoré dokážu zakryť prítomnosť malwaru v počítači. Keď program deteguje rootkit, nemusí to nevyhnutne znamenať, že je počítač infikovaný. V niektorých prípadoch sa môžu určitým spôsobom ovládať alebo časti bežných aplikácií nesprávne označovať ako rootkity.

Mali by ste tiež určiť, čo chcete kontrolovať

- **Všetky typy súborov** s možnosťou definovať výnimky z kontroly vytvorením zoznamu súborov oddelených (uložením súborov s názvom *zoznam súborov*) prípon súborov, ktoré sa nemajú kontrolovať.
- **Vybrané typy súborov** – môžete nastaviť, aby sa kontrolovali len súbory, pri ktorých existuje pravdepodobnosť infikovania (súbory, ktoré nemôžu byť napadnuté infekciou, napríklad niektoré jednoduché textové súbory alebo niektoré nespustiteľné súbory, sa nebudú kontrolovať), vrátane mediálnych súborov (video, audio súborov – ak necháte toto políčko nezaškrtnuté, potom sa as kontroly skráti ešte viac, pretože tieto súbory sú často veľa väčšie, pričom pravdepodobnosť napadnutia vírusom je veľa menšia). Znova môžete definovať, pod aké prípony, ktoré súbory sa majú kontrolovať vždy.
- Alternatívne môžete rozhodnúť, že chcete **kontrolovať súbory bez prípony** – táto možnosť je predvolene zapnutá a odporúčame vám, aby ste toto nastavenie nikdy nemenili, ak na to nemáte skutočný dôvod. Súbory bez prípony sú skôr podozrivé a mali by sa vždy kontrolovať.

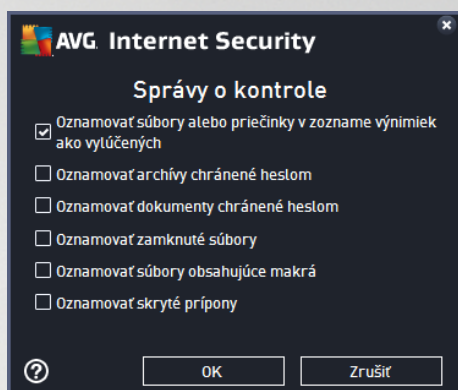
Nastaviť rýchlosť dokončenia kontroly

V časti **Nastaviť rýchlosť dokončenia kontroly** môžete alej nastaviť požadovanú rýchlosť kontroly v závislosti od využívania systémových zdrojov. Predvolene má tento parameter nastavenú úroveň automatického využívania zdrojov „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 využitie systémových zdrojov predĺžením doby trvania kontroly.



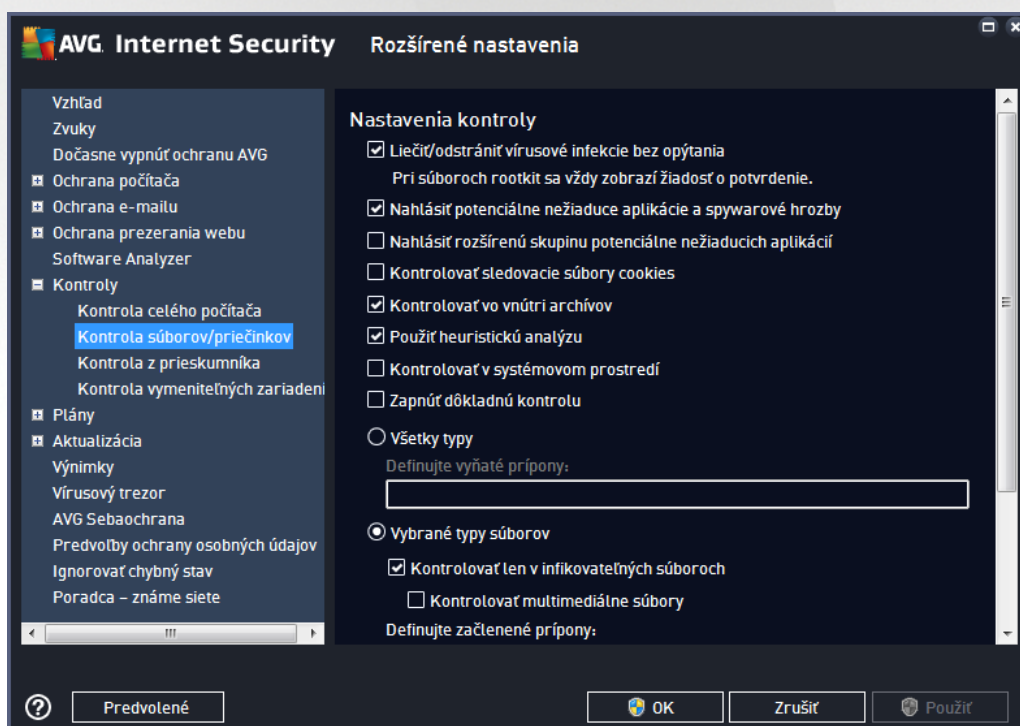
Vytvoriť ďalšie správy o kontrole...

Kliknutím na odkaz **Nastaviť dodatočné 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:



3.5.8.2. Kontrola súborov/priečinkov

Rozhranie editácie na **Kontrolu súborov/priečinkov** je takmer rovnaké ako dialógové okno editácie s názvom [Kontrola celého počítača](#), avšak predvolené nastavenia sú pre možnosť [Kontrola celého počítača](#) prísnejšie:



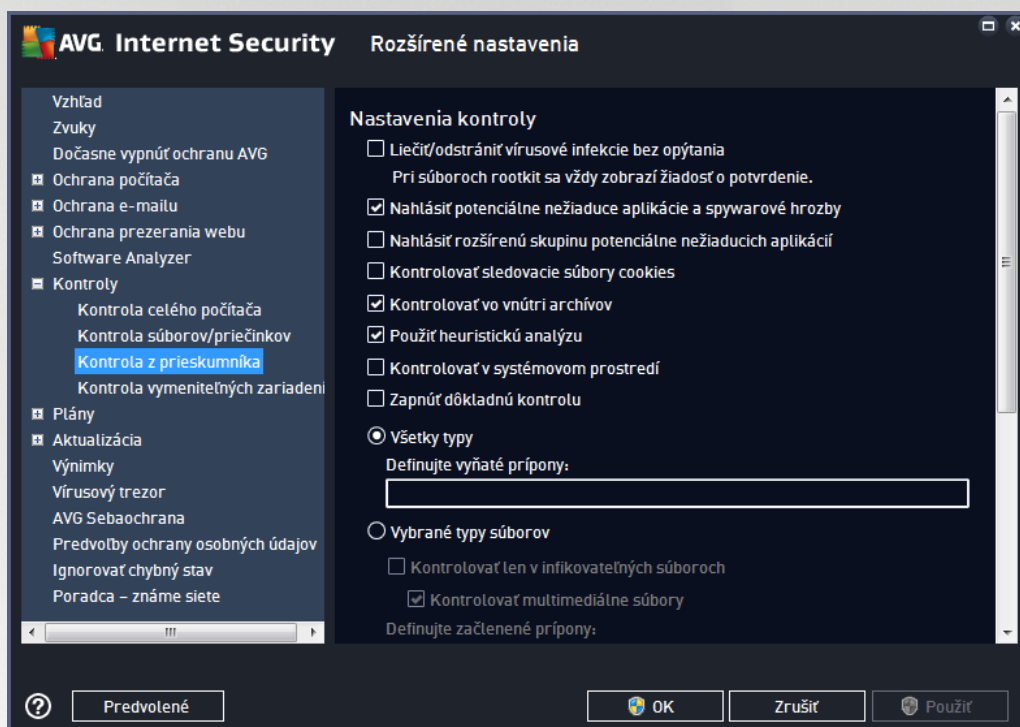
Všetky parametre nastavené v tomto dialógovom okne konfigurácie sa vzťahujú len na oblasti vybrané na kontrolu v dialógovom okne [Kontrola súborov/priečinkov](#)!

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



3.5.8.3. Kontrola z prieskumníka

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



Možnosti úpravy sú takmer rovnaké ako tie, ktoré sú k dispozícii pre možnosť [Kontrola celého počítača](#), avšak predvolené nastavenia sa líšia (napríklad *Kontrola celého počítača* predvolene nekontroluje archívy, ale kontroluje systémové prostredie, zatiaľ čo *Kontrola z prieskumníka* má presne opačné nastavenia).

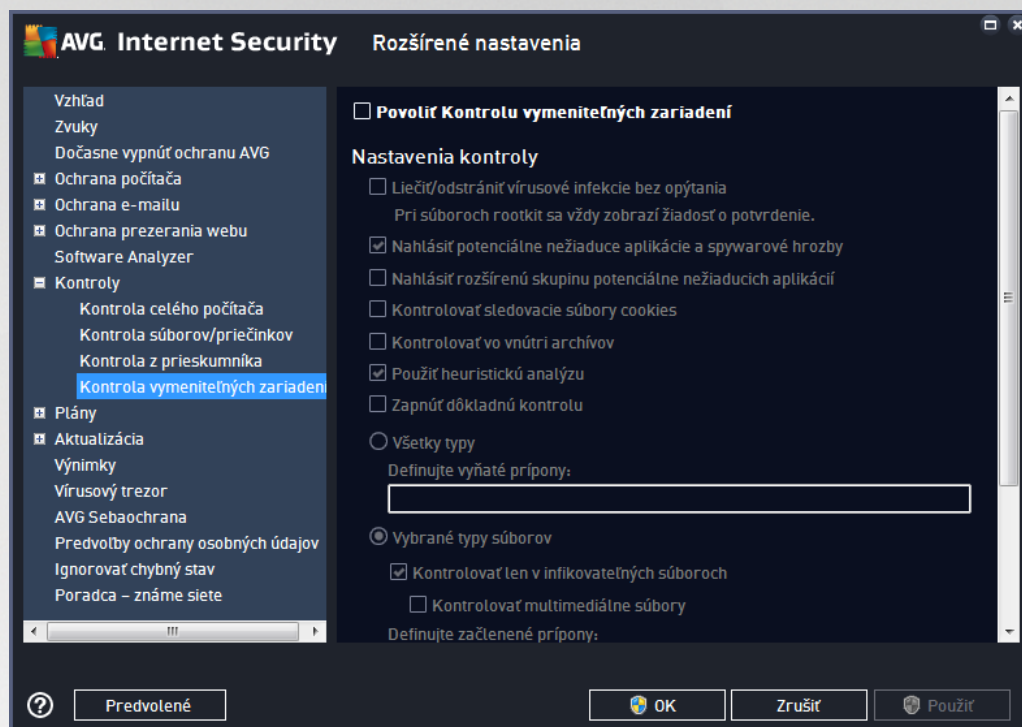
Poznámka: Informácie o konkrétnych parametroch nájdete v kapitole [Rozšírené nastavenia AVG/Kontroly/Kontrola celého počítača](#).

V porovnaní s dialógovým oknom [Kontrola celého počítača](#) sa v dialógovom okne **Kontrola z prieskumníka** nachádza aj časť s názvom **Zobrazenie postupu a výsledkov kontroly**, ktorá umožňuje nastaviť, či majú byť výsledky a priebeh kontroly prístupné v používateľskom rozhraní AVG. Zároveň umožňuje nastaviť, aby sa výsledky kontroly zobrazili len v prípade, keď sa počas kontrolovania deteguje infekcia.



3.5.8.4. Kontrola vymeniteľných zariadení

Rozhranie editácie **Kontrola vymeniteľných zariadení** je tiež veľmi podobné dialógovému oknu editácie [Kontrola celého počítača](#):



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

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

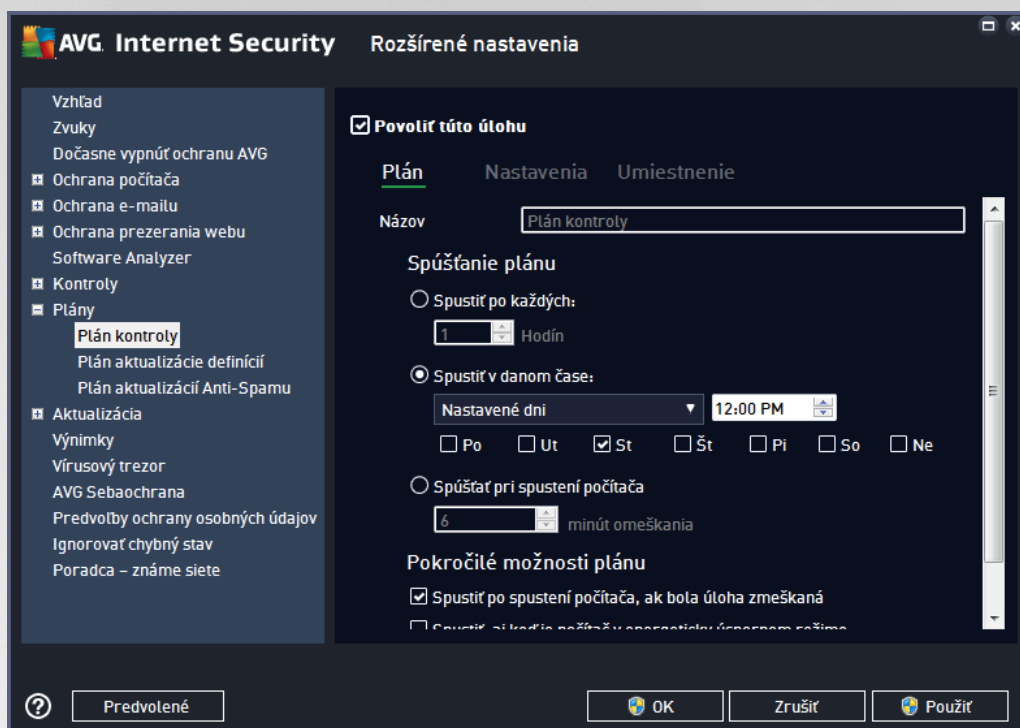
3.5.9. Plány

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

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

3.5.9.1. Plán kontroly

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



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

Napríklad: nie je vhodné nazývať kontrolu „Nová kontrola“ alebo „Moja kontrola“, pretože tieto názvy sa nevzťahujú na to, čo kontrola vlastne preveruje. Na druhej strane, príkladom dobrého opisného názvu je „Kontrola systémových oblastí“ a pod. 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 [kontrol vybraných súborov alebo priečinkov](#).

Toto dialógové okno umožňuje alej definovať tieto parametre prehadzovania:

Spúšťanie naplánovaných úloh

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

Rozšírené možnosti plánu

- **Spustiť po spustení počítača, ak bola úloha zmeškaná** – ak naplánujete úlohu, aby sa spustila v istom čase, táto možnosť zabezpečí, že sa následne vykoná kontrola v prípade, že sa počítač v naplánovanom čase vypne.
- **Spustiť, aj keď je počítač v energeticky úspornom režime** – úloha sa má vykonať v naplánovanom čase, aj keď je počítač v energeticky úspornom režime.



ase, aj keď je napájaný batériou.



V karte **Nastavenia** nájdete zoznam parametrov kontrolovania, ktoré sa dajú voliteľne zapnúť /vypnúť. Predvolené 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 vírusové infekcie bez opýtania** (predvolené zapnuté): ak počas kontroly identifikuje vírus, môže sa automaticky vylíčiť, ak je dostupná liečba. Ak nie je možné infikovaný súbor vylíčiť automaticky, premiestni sa do [Vírusového trezora](#).
- **Nahlásiť potenciálne nežiaduce aplikácie a spywarové hrozby** (predvolené zapnuté): zašiar kníte toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu malware: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporujeme vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
- **Nahlásiť rozšírenú skupinu potenciálne nežiaducich aplikácií** (predvolené vypnuté): zašiar kníte 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 predvolené vypnutá.
- **Kontrolovať sledovacie súbory cookies** (predvolené vypnuté): tento parameter súčasti zapína funkciu na detekciu súborov cookies počas kontroly; (súbory HTTP cookies sa používajú na overenie totožnosti, sledovanie a správu konkrétnych informácií o používateľoch, akými sú napr. preferencie stránok alebo obsah elektronických nákupných košíkov).
- **Kontrolovať vo vnútri archívov** (predvolené vypnuté): tento parameter určuje, že sa majú počas



kontroly preverova všetky súbory, aj keď sú uložené vo vnútri archívu, napr. ZIP, RAR, atď.

- **Použiť heuristickú analýzu** (predvolene zapnuté): heuristická analýza (dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí) bude jednou z metód, ktoré sa použijú na detekciu vírusov počas kontroly.
- **Kontrolovať v systémovom prostredí** (predvolene zapnuté): počas kontroly sa budú overovať aj systémové oblasti počítača.
- **Zapnúť dôkladnú kontrolu** (predvolene vypnuté): v určitých situáciách (podozrenie na infikovanie počítača) môžete touto možnosťou aktivovať najdôkladnejšie kontrolné algoritmy, ktoré pre istotu skontrolujú aj tie oblasti počítača, ktoré sa obyčajne vôbec neinfikujú. Upozorujeme však, že tento spôsob je náročný na procesor.
- **Kontrolovať rootkity** (predvolene zapnuté): Kontrola Anti-Rootkit kontroluje počítača a zisťuje prítomnosť potenciálnych rootkitov (programov a technológií, ktoré dokážu zakryť malwaru v počítači). Keď program deteguje rootkit, nemusí to nevyhnutne znamenať, že je počítač infikovaný. V niektorých prípadoch sa môžu určitým spôsobom ovládať alebo časti bežných aplikácií nesprávne označovať ako rootkity.

Mali by ste tiež určiť, čo chcete kontrolovať

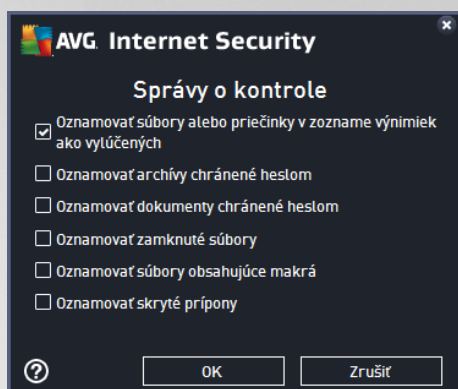
- **Všetky typy súborov** s možnosťou definovať výnimky z kontroly vytvorením zoznamu súborov oddelených (uložením súborov s názvom *zoznam súborov*) prípon súborov, ktoré sa nemajú kontrolovať.
- **Vybrané typy súborov** – môžete nastaviť, aby sa kontrolovali len súbory, pri ktorých existuje pravdepodobnosť infikovania (súbory, ktoré nemôžu byť napadnuté infekciou, napríklad niektoré jednoduché textové súbory alebo niektoré nespustiteľné súbory, sa nebudú kontrolovať), vrátane mediálnych súborov (video, audio súborov – ak necháte toto políčko nezaškrtnuté, potom sa počas kontroly skrátí ešte viac, pretože tieto súbory sú často veľa väčšie, pričom pravdepodobnosť napadnutia vírusom je veľa menšia). Znova môžete definovať, pod aké prípony, ktoré súbory sa majú kontrolovať vždy.
- Alternatívne môžete rozhodnúť, že chcete **kontrolovať súbory bez prípony** – táto možnosť je predvolene 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 využitie systémových zdrojov predĺžením doby trvania kontroly.

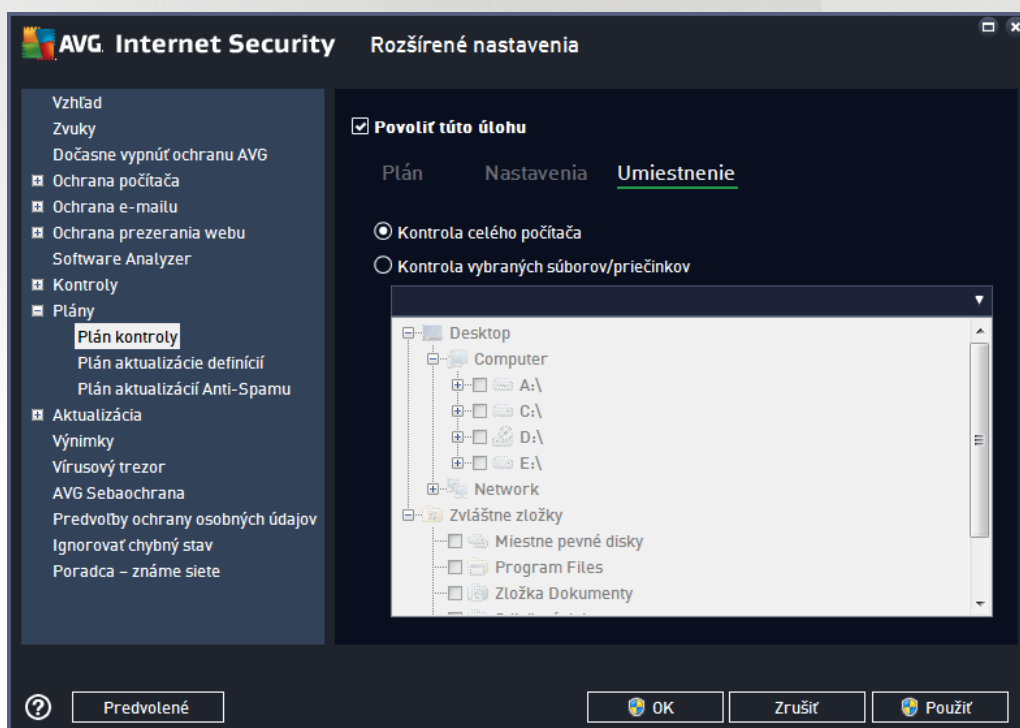
Vytvoriť ďalšie správy o kontrole

Kliknutím na odkaz **Nastaviť dodatočné 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 po íta a

Vasti **Možnosti vypnutia po íta a** môžete rozhodnú , i sa má po íta vypnú automaticky po dokon ení procesu kontroly. Po potvrdení tejto možnosti (**Vypnú po íta po dokon ení kontroly**) sa aktivuje nová možnosť , ktorá umožní vypnú po íta , aj ke je momentálne zablokovaný (**Vynútené vypnutie, ak je po íta zablokovaný**).

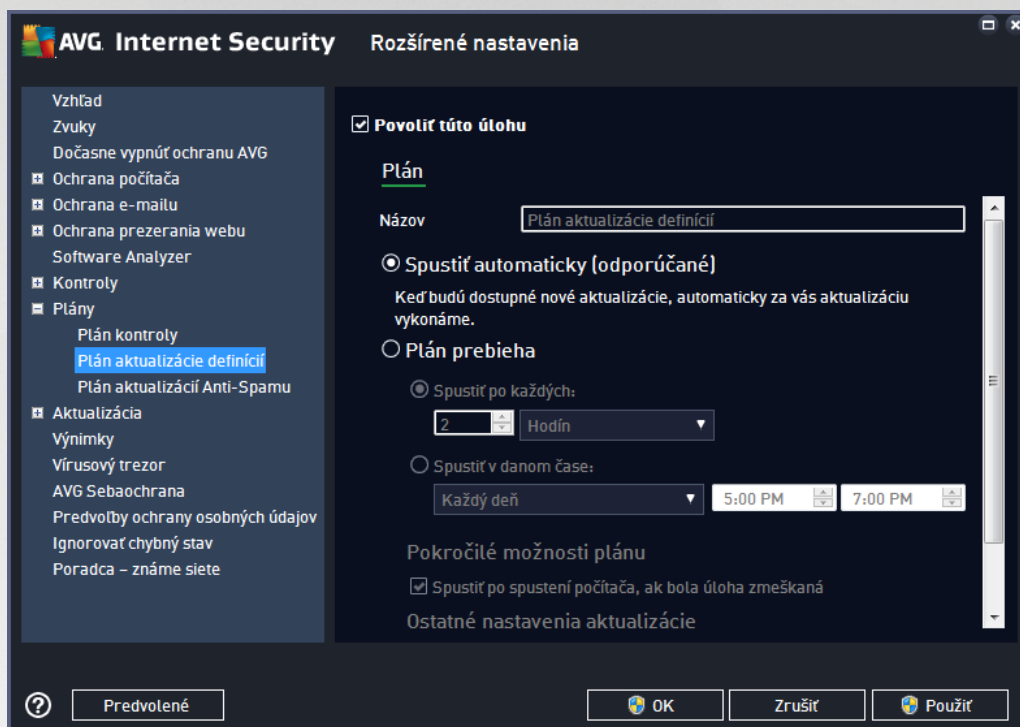


Na karte **Umiestnenie** môžete nastavi , i chcete naplánova [kontrolu celého po íta a](#) alebo [kontrolu súborov/prie inkov](#). V prípade, že zvolíte kontrolu súborov/prie inkov, v spodnej asti tohto dialógového okna sa aktivuje zobrazená stromová štruktúra a môžete ur i prie inky, ktoré sa majú kontrolova .



3.5.9.2. Plán aktualizácie definícií

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



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

Spúšanie naplánovaných úloh

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

Rozšírené možnosti plánu

Táto časť sa používa na definovanie podmienok, za akých sa má/nemá spustiť aktualizácia programu, ak je po ňom 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 ihne 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 dialógovom okne [Rozšírené nastavenia/Vzhľad](#)*).



3.5.9.3. Plán aktualizácie Anti-Spamu

Ak je to naozaj potrebné, zrušením začiarknutia možnosti **Povoli túto úlohu** môžete dočasne vypnúť naplánovanú aktualizáciu služby [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 definujete časové intervaly pre nové naplánované spúšťanie aktualizácie služby Anti-Spam. Načasovanie sa nastavuje buď ako opakované spúšťanie aktualizácie služby Anti-Spam po uplynutí určitého času (**Spusti po každých**), nastavením presného dátumu a času (**Spusti v konkrétnom ase**) alebo definovaním udalosti, s ktorou sa bude spájať spustenie aktualizácie (**Spusti pri spustení počítača**).

Rozšírené možnosti plánu

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

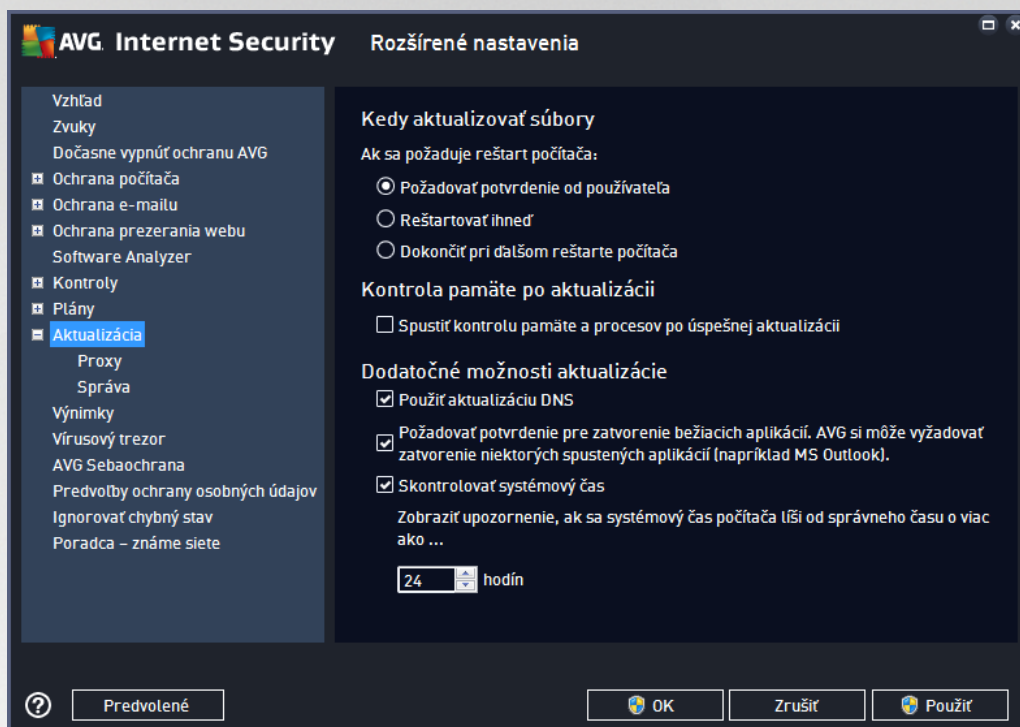
Ďalšie nastavenia aktualizácie

Označte možnosť **Spusti aktualizáciu znova po obnovení pripojenia k internetu**, ak sa má v prípade výpadku internetového pripojenia obnoviť postup aktualizácie služby Anti-Spam ihneď po obnovení pripojenia. Po spustení plánu kontroly v nastavenom ase 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](#)).



3.5.10. Aktualizácia

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



Kedy aktualizovať súbory

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

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

Kontrola pamäte po aktualizácii

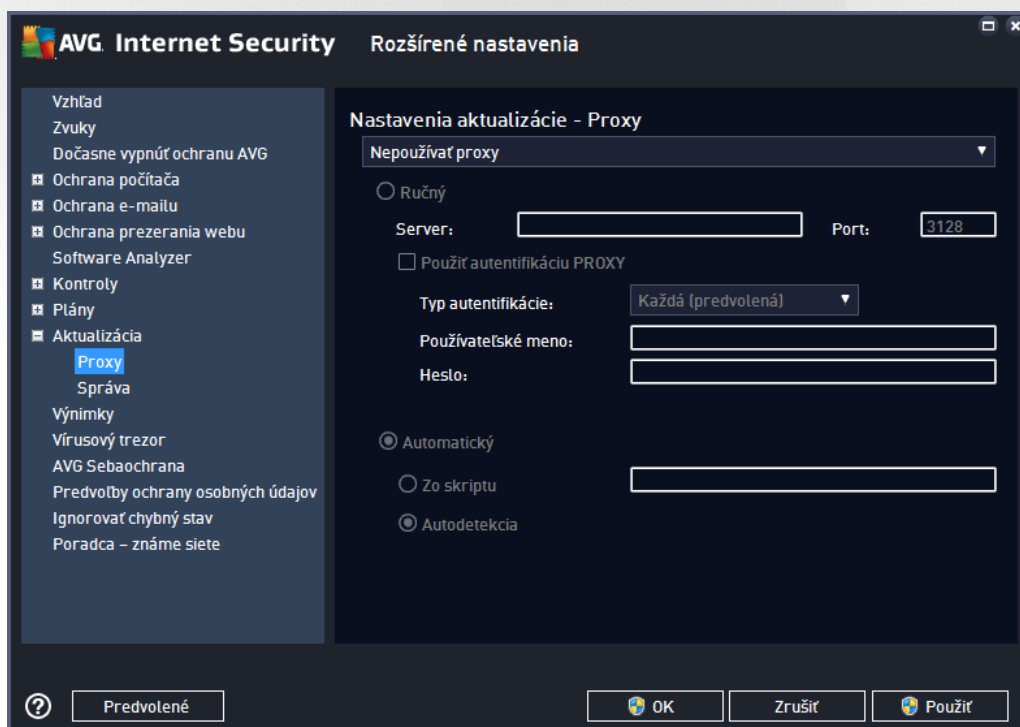
Označte toto začiarkavacie políčko, ak sa má nová kontrola pamäte spustiť po každej úspešnej aktualizácii. Najnovšia stiahnutá aktualizácia môže obsahovať nové definície vírusov, ktoré sa môžu ihneď použiť pri kontrole.



alšie možnosti aktualizácie

- **Vytvorí nový bod obnovy systému pri každej aktualizácii programu** (predvolene zapnuté) – pred každým spustením aktualizácie programu AVG sa vytvorí bod obnovy 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 vykonávané zmeny týchto nastavení sa odporúča len skúseným používateľom! Nechajte toto zaškrtnuté políčko označené, ak chcete používať túto funkčnosť.
- **Použije aktualizáciu DNS** (predvolene zapnuté) – ak je toto zaškrtnuté políčko označené, po spustení aktualizácie **AVG Internet Security** vyhľadá informácie o najnovšej verzii vírusovej databázy a najnovšej verzii programu na serveri DNS. Až potom sa stiahnu a nainštalujú najmenšie nevyhnutne potrebné aktualizované súbory. Týmto spôsobom sa minimalizuje celkový objem stiahnutých dát a zrýchli proces aktualizácie.
- **Požadová súhlas so zatvorením spustených aplikácií** (predvolene zapnuté) – postará sa o to, aby sa žiadna spustená aplikácia nezatvorila bez vášho súhlasu, ak to je potrebné na dokončenie procesu aktualizácie.
- **Skontroluje systémový čas** (predvolene zapnuté) – zaškrtnite túto možnosť, ak chcete byť informovaní v prípade, keď sa systémový čas líši od skutočného času o viac, ako je stanovený počet hodín.

3.5.10.1. Proxy



Server proxy je samostatný server alebo služba spustená na počítači, ktorá zabezpečí bezpečnejšie pripojenie do internetu. Podľa zadovaných pravidiel siete potom môžete prísť k Internetu buď priamo alebo cez proxy server, môžete využiť aj obidve možnosti zároveň. Potom v prvej položke dialógového okna **Nastavenia**



aktualizácie – Proxy musíte nastaviť v ponuke, ak ich chcete:

- **Nepoužíva proxy** – predvolené nastavenia
- **Použi proxy**
- **Pokúsi sa pripoji pomocou 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 manuálne alebo automaticky.

Ručná konfigurácia

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

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

Proxy server môže mať tiež nakonfigurované špecifické pravidlá pre každého používateľa. Ak je server proxy nastavený týmto spôsobom, zvoľte možnosť **Použi autentifikáciu PROXY** na overenie, či sú vaše používateľské meno a heslo platné na vytvorenie pripojenia na internet cez server proxy.

Automatická konfigurácia

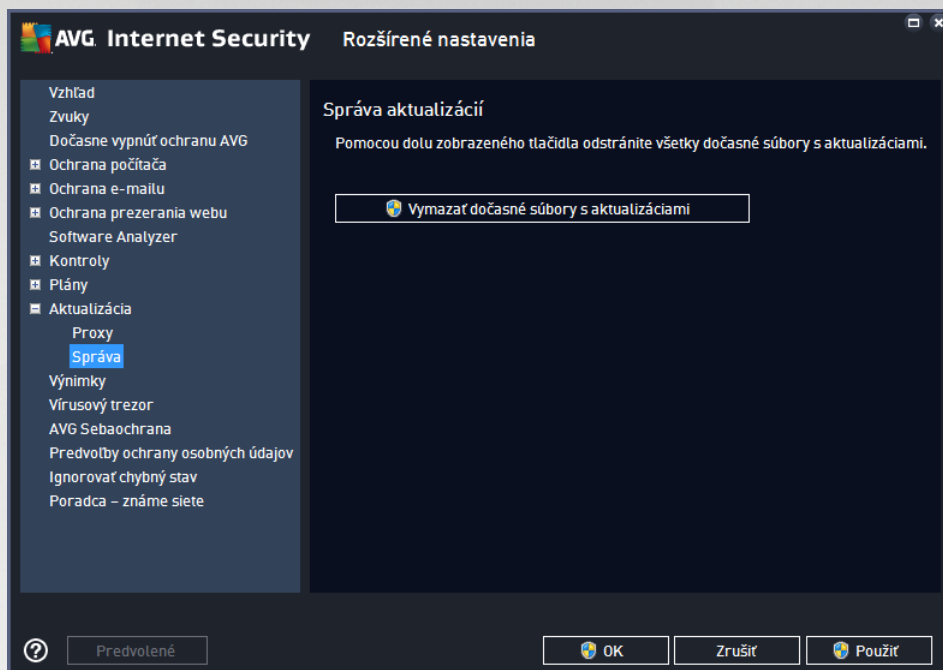
Ak sa rozhodnete pre automatickú konfiguráciu (zvoľte možnosť **Automatická na aktivovanie príslušnej asti dialógového okna**), nastavte, odkiaľ sa má stiahnuť konfigurácia servera proxy:

- **Z prehliadača** – konfigurácia sa načítava z predvoleného internetového prehliadača
- **Zo skriptu** – konfigurácia sa prečítava zo stiahnutého skriptu s funkciou, ktorá vráti adresu proxy
- **Autodetekcia** – konfigurácia sa bude detegovať automaticky priamo zo servera proxy



3.5.10.2. Správa

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

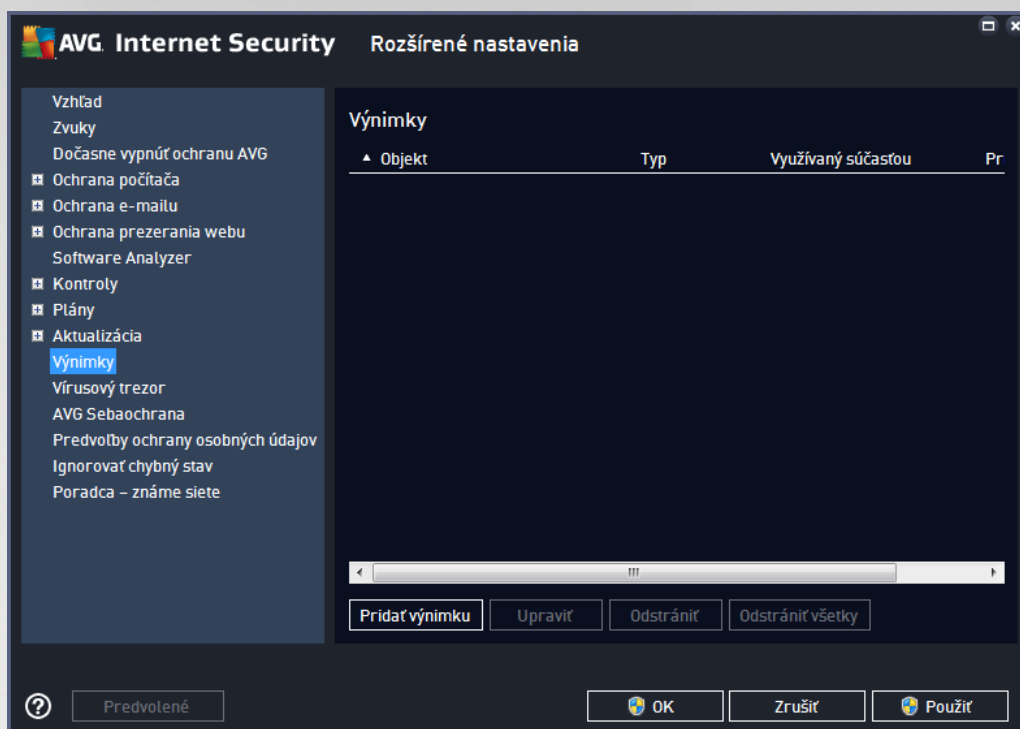


- **Vymazať dočasné súbory s aktualizáciami** – stlačením tohto tlačidla sa vymažú všetky nepotrebné súbory aktualizácie z pevného disku (v predvolenom nastavení zostanú tieto súbory uložené 30 dní)
- **Vrátiť sa na predchádzajúcu verziu databázy vírusov** – stlačením tohto tlačidla sa vymaže najnovšia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

3.5.11. Výnimky

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

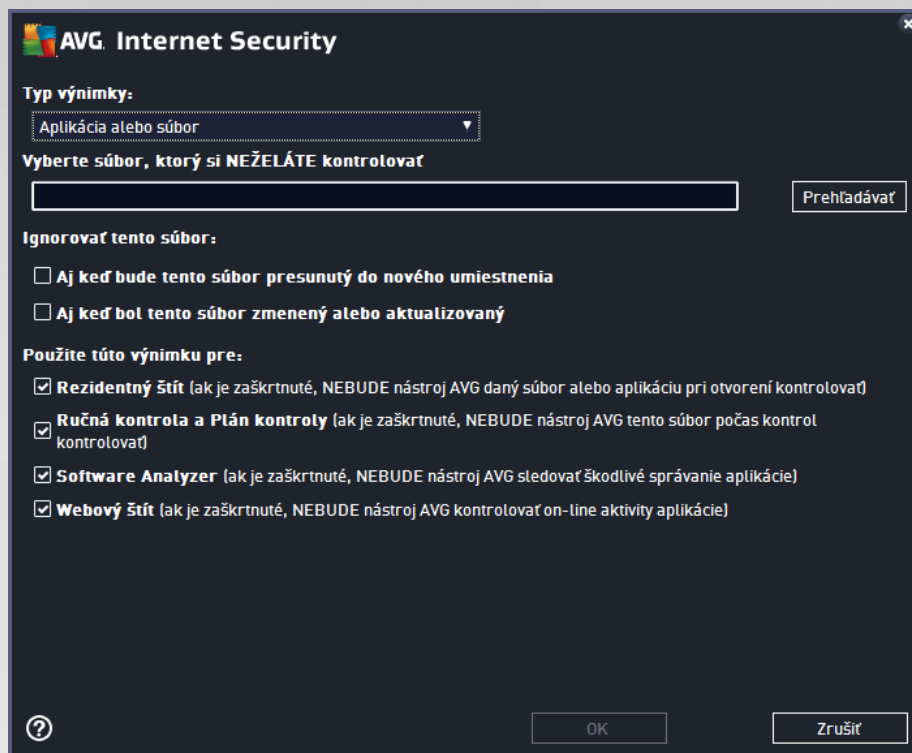
Vždy sa uistíte, že daný súbor, program alebo stránka sú úplne bezpečné!



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, aby sa položky zoradili podľa príslušného kritéria.

Ovládacie tlačidlá

- **Pridať výnimku** – kliknutím otvoríte nové dialógové okno, kde môžete zadať položku, ktorá sa má vynechať z kontroly AVG:

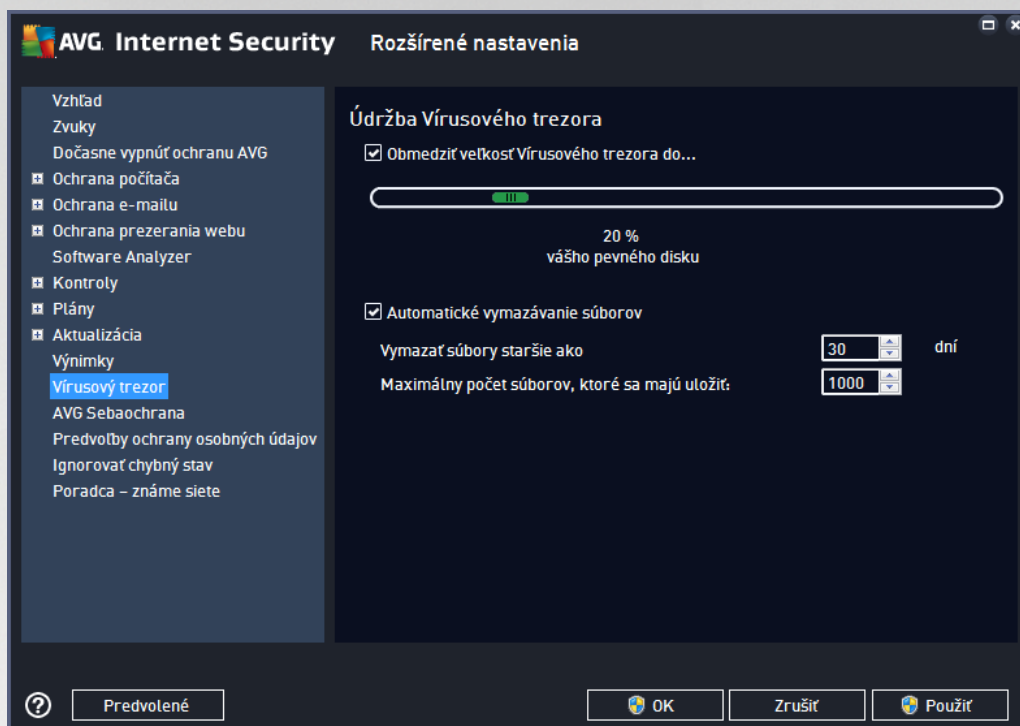


Najskôr budete vyzvaní na zadanie typu objektu, t. j. či ide o aplikáciu alebo súbor, pričom môžete vybrať aj typ certifikátu. Potom na disku nájdete cestu k príslušnému objektu alebo napíšete URL. Nakoniec môžete zvoliť, ktoré funkcie AVG by mali vybraný objekt ignorovať (Rezidentný štít, Ručná kontrola a Plán kontroly, Software Analyzer, Webový štít a Windows Antimalware Scan Interface).

- **Upraviť** – toto tlačidlo je aktívne iba vtedy, ak už sú nadefinované nejaké výnimky a 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 AVG príslušný súbor, pričom i adresu URL opäť kontrolovať. Upozorujeme, že bude odstránená len výnimka, nie súbor alebo príloha samotný!
- **Odstrániť všetky** – použijete toto tlačidlo na vymazanie všetkých výnimiek definovaných v zozname.



3.5.12. Vírusový trezor

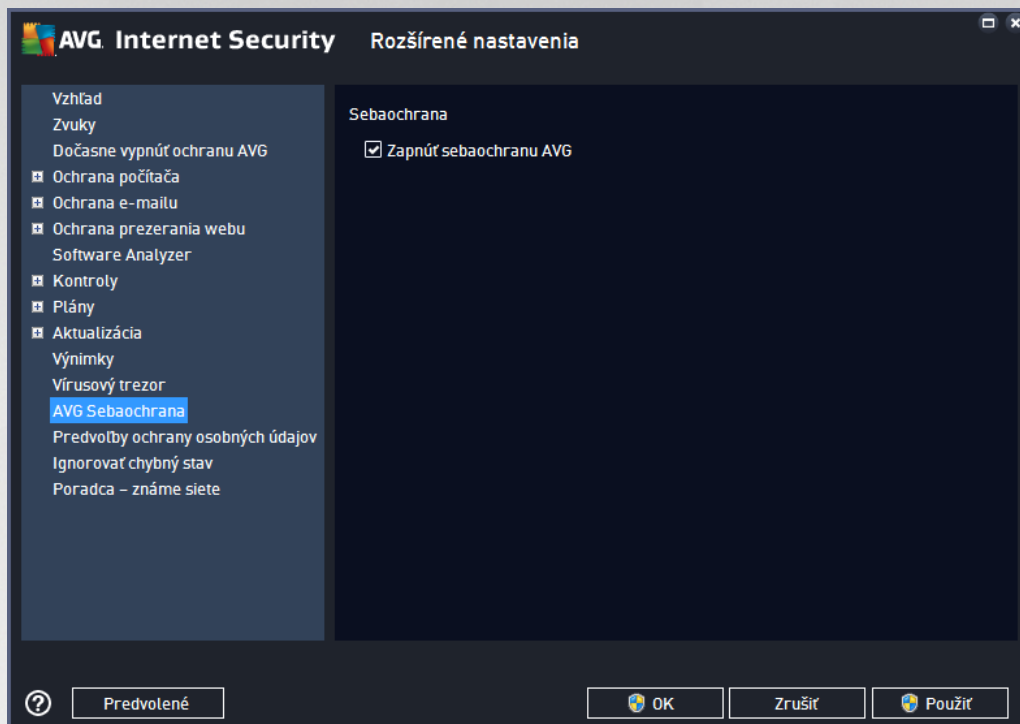


Dialógové okno **Správa Vírusového trezora** vám umožňuje zdefinovať niektoré parametre ohľadom administrácie objektov uložených vo [Vírusovom trezore](#):

- **Obmedziť veľkosť Vírusového trezora** – použijete posúvač na nastavenie maximálnej veľkosti [Vírusového trezora](#). Táto veľkosť sa uvádza úmerne v porovnaní s veľkosťou vášho miestneho disku.
- **Automatické vymazávanie súborov** – v tejto časti môžete stanoviť maximálny časový úsek, počas ktorého by mali byť objekty uložené vo [Vírusovom trezore](#) (**Vymazať súbory staršie ako ... dní**), a maximálny počet súborov, ktoré budú uložené vo [Vírusovom trezore](#) (**Maximálny počet uložených súborov**).



3.5.13. AVG Sebaochrana

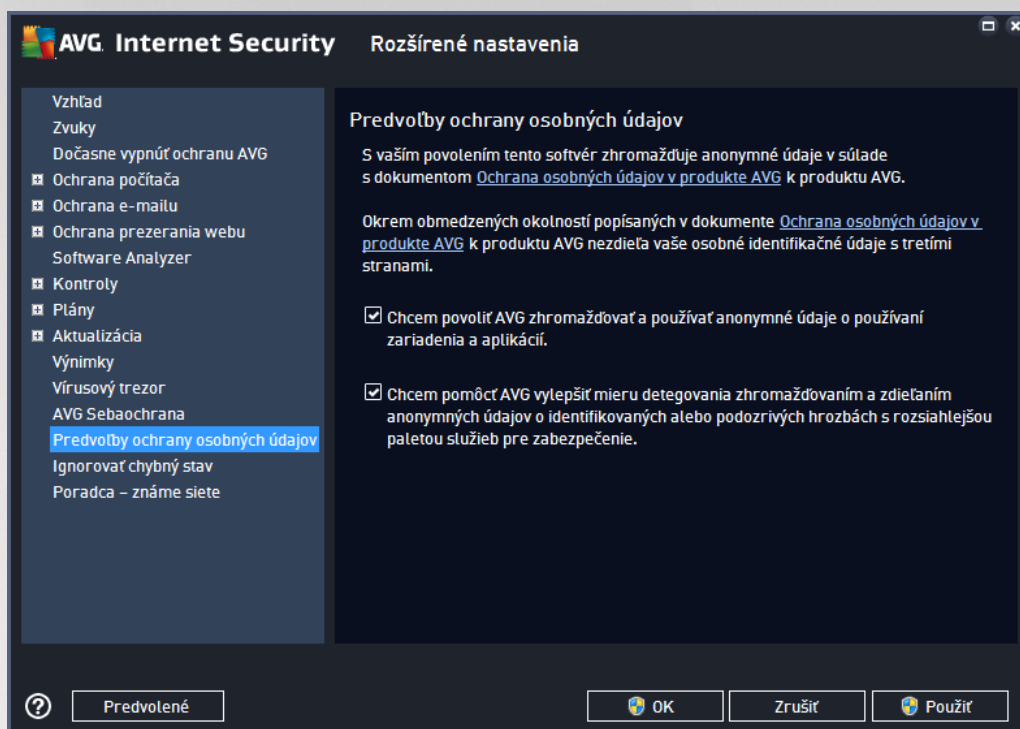


Funkcia **AVG Sebaochrana** umožňuje **AVG Internet Security** chrániť svoje vlastné procesy, súbory, záznamy v registri a ovládať ich pred zmenou alebo deaktiváciou. Hlavným dôvodom pre tento druh ochrany je, že niektoré sofistikované hrozby sa snažia vypnúť antivírusovú ochranu, a potom nerušené poškodzujú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

Odporúčame vám túto funkciu ponechať zapnutú!

3.5.14. Preferencie ochrany osobných údajov

Dialógové okno **Preferencie ochrany osobných údajov** vám ponúka 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 ústníkov 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:

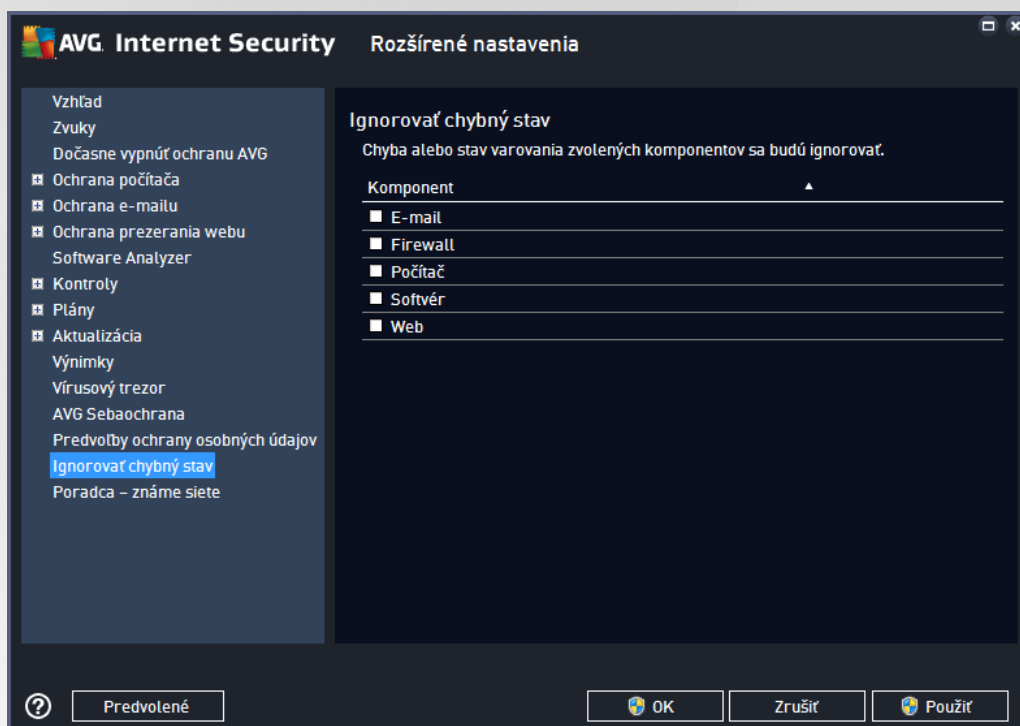
- **Želám si pomôcť spoločnosti AVG zlepšovať jej produkty a chcem sa zúčastniť Programu zlepšovania produktov AVG (predvolené zapnuté)** – ak nám chcete pomáhať v ďalšom zlepšovaní produktu **AVG Internet Security**, nechajte toto políčko začiarknuté. Táto funkcia zapne oznamovanie všetkých zaznamenaných hrozieb do spoločnosti AVG a umožní nám zhromažďovať najnovšie informácie o malware od všetkých používateľov z celého sveta a zlepšovať ochranu pre každého jednotlivca. Oznamovanie prebieha automaticky, preto vás nijako nezaťažuje, a v správach nie sú uvedené žiadne osobné údaje.
 - **Povolí posielanie informácií o nesprávne identifikovaných e-mailoch po potvrdení používateľa** (predvolené zapnuté) – zasiela informácie o e-mailových správach, ktoré boli nesprávne označené ako nevyžiadaná pošta, alebo správach nevyžiadanej pošty, ktoré služba Anti-Spam nedetegovala. Pred poslaním tohto druhu informácií vás program požiada o potvrdenie.
 - **Povolí posielanie anonymných informácií o identifikovaných alebo podozrivých hrozbách** (predvolené zapnuté) – zasiela informácie o podozrivom alebo pozitívne nebezpečnom kóde alebo vzore správania (môže ísť o vírus, spyware alebo škodlivé internetové stránky, ktoré sa pokúšate otvoriť) detegovanom na vašom počítači.
 - **Povolí posielanie anonymných informácií o používaní produktu** (predvolené zapnuté) – odosielanie základných štatistík o používaní aplikácie, ako je počet nájdených hrozieb, spustených kontrol, úspešné a neúspešné kontroly a pod.
- **Zapnúť overovanie detekcií pomocou cloud computingu** (predvolené zapnuté) – detegované hrozby sa budú overovať, a sú naozaj infikované, aby sa vylúčili nesprávne detekcie.
- **Želám si, aby sa produkty AVG prispôbili mojej práci zapnutím funkcie AVG Personalizácia**



(predvolene vypnutá) – táto funkcia anonymne analyzuje správanie programov a aplikácií vo vašom počítači. Na základe tejto analýzy vám môže spoločnosť AVG ponúkať služby na mieru vašich potrieb, aby vám zabezpečila maximálnu bezpečnosť.

3.5.15. Ignorovať chybový stav

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



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

- ikona v paneli úloh – ak všetky súčasti aplikácie AVG fungujú správne, ikona je zobrazená v štyroch farbách; ak sa však vyskytne chyba, ikona sa zobrazí so žltým výkričníkom,
- textový popis existujúceho problému v súčasti [Informácie o stave zabezpečenia](#) v hlavnom okne AVG

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

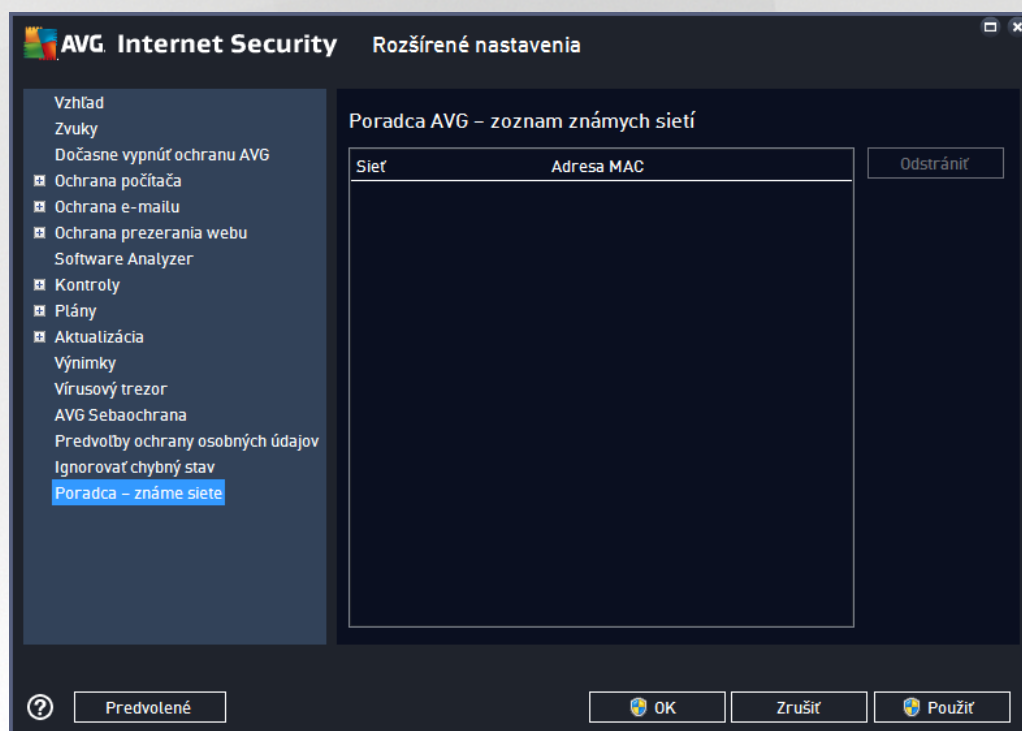
V tejto situácii môžete v dialógovom okne **Ignorovať chybný stav** vybrať súčasti, o ktorých prípadnom chybnom stave (alebo vypnutí) si neželáte byť informovaní. Kliknutím na tlačidlo **OK** potvrdíte zmeny.



3.5.16. Advisor – známe siete

[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 AVG Advisor nie je podporovaná v 64-bitových systémoch Windows XP.

3.6. Nastavenia súčasti Firewall

Konfigurácia súčasti [Firewall](#) sa otvorí v novom okne, kde môžete vo viacerých dialógových oknách nastaviť všetky parametre komponentu. Konfigurácia súčasti Firewall sa otvorí v novom okne, kde môžete upraviť rozšírené parametre v niekoľkých 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 tlačiarň](#)



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

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

3.6.1. Všeobecné

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

Dodávateľ softvéru nastavil všetky súčasti produktu AVG Internet Security tak, aby dosahovali optimálny výkon. Nemajte predvolenú konfiguráciu, ak na to nemáte oprávnený dôvod. Akékoľvek zmeny nastavení by mali vykonať len skúsení používatelia!



Firewall vám umožní vydefinovať 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 Firewallu špecifickou konfiguráciou súčasti Firewall a môžete použiť niekedy takýchto vopred definovaných konfigurácií:

- **Automaticky** – v tomto režime Firewall automaticky spracúva celú prevádzku v sieti. Z vašej strany nebudú požadované žiadne rozhodnutia. 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. V prípade iných aplikácií Firewall podľa správania aplikácie rozhodne, či sa má pripojenie povoliť alebo zablokovat. 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 váš počítač.**

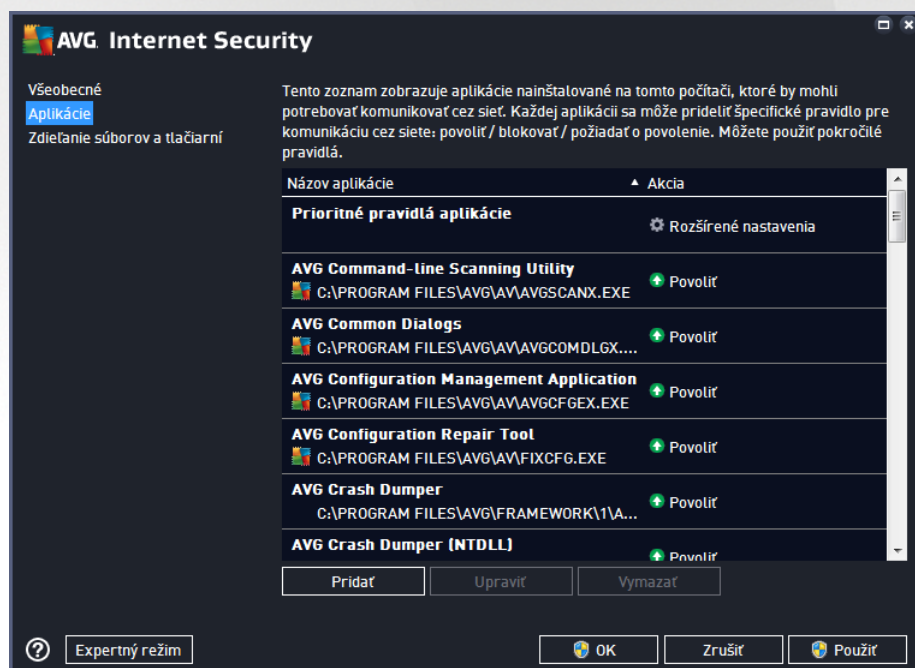


- **Interaktívny** – tento režim je praktický, ak si želáte kontrolovať všetky sieťové prenosy z a do vášho počítača. Firewall ich bude sledovať a upozorní vás na každý pokus o komunikáciu alebo prenos dát, čím vám umožní povoliť alebo zablockovať daný pokus, ako to uznáte za vhodné. Odporúčame sa len pokročiť, ak ho používate.
- **Blokovať prístup na internet** – internetové pripojenie bude úplne zablockované, nebudete mať prístup na internet a nikto zvonku nebude mať prístup do vášho počítača. Len pre zvláštne a krátkodobé použitie.
- **Vypnúť ochranu súčasnou Firewall** – deaktivovaním Firewallu povolíte všetky sieťové prenosy z a do vášho počítača. Uistite sa, že sa neobráti na útok hackerov. Vo väčšine prípadov je táto možnosť vždy starostlivo zvážte.



Upozorujeme na špeciálny automatický režim, ktorý je tiež k dispozícii v rámci Firewallu. Tento režim sa v tichosti aktivuje vtedy, ak sa počítač alebo súčasná **Software Analyzer** vypnú, a počítač bude preto zraniteľnejší. V takých prípadoch Firewall automaticky povolí pripojenie iba známym a úplne bezpečným aplikáciám. Pri všetkých ostatných bude od vás vyžadovať rozhodnutie. Cieľom je nahradiť deaktivované súčasti ochrany a udržať počítač v bezpečí.

3.6.2. 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 sieťoch
-  – blokuje komunikáciu



-  – definované rozšírené nastavenia

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

Samozrejme, že pravidlá pre novú aplikáciu môžete definovať aj hneď: v tomto dialógovom okne stlačte tlačidlo **Pridať** a vyplňte podrobnosti 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. **Ďalšie aplikácie a pravidlá** (v spodnej časti zoznamu) sa použijú ako „posledná možnosť“ v prípade, keď sa nepoužijú konkrétne pravidlá pre aplikácie, ako sú napríklad neznáme a nedefinované aplikácie. Vyberte akciu, ktorá sa má spustiť, keď sa táto aplikácia pokúsi komunikovať v sieti: **Blokovať** (komunikácia sa vždy zablokuje), **Povoliť** (komunikácia sa povolí cez akúkoľvek sieť), **Spýtať sa** (budete požiadaní o rozhodnutie, či danú komunikáciu povoliť, alebo blokovat). **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:

- **Pridať** – otvorí prázdne dialógové okno na definovanie nových aplikačných pravidiel.
- **Upraviť** – otvorí to isté dialógové okno, ktoré sa používa na zmenu existujúcej skupiny aplikačných pravidiel.
- **Vymazať** – odstráni vybranú aplikáciu zo zoznamu.

3.6.3. Zdieľanie súborov a tlačiarňí

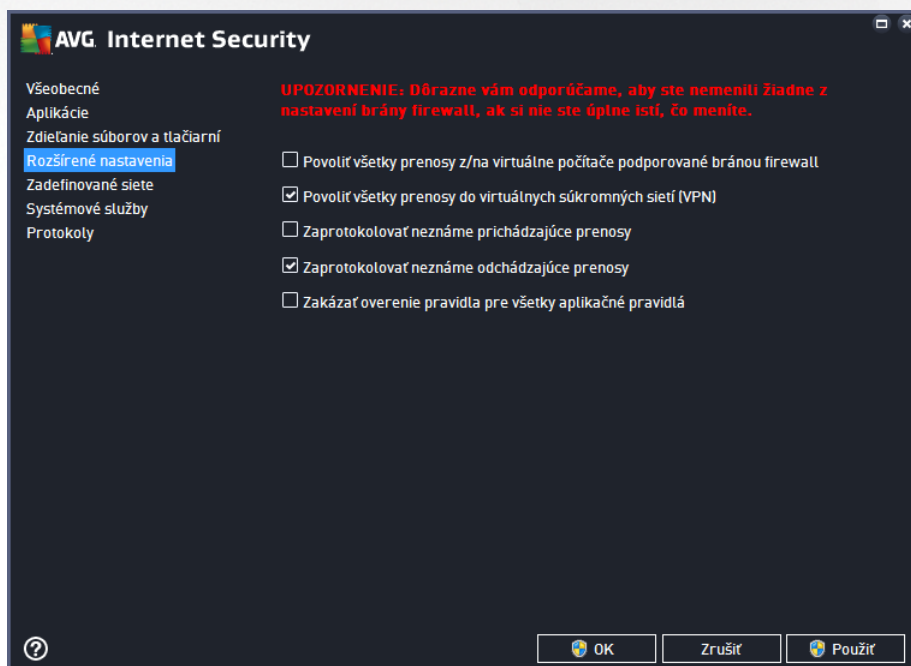
Zdieľanie súborov a tlačiarňí v podstate znamená zdieľanie akýchkoľvek súborov alebo priečinkov, ktoré ste označili vo Windows ako „Zdieľané“, spoločných diskových jednotiek, tlačiarňí, skenerov a všetkých podobných zariadení. Zdieľanie takýchto položiek je želané len v rámci sietí, ktoré môžu byť považované 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 zdieľanie želáť. AVG Firewall môže jednoducho blokovat alebo povoliť zdieľanie a umožní vám uložiť si svoju voľbu pre už navštívené siete.



V dialógovom okne **Zdieľanie súborov a tlačiarň** môžete upraviť konfiguráciu zdieľania súborov a tlačiarň a aktuálne pripojených sietí. Vo Windowse XP názov siete zodpovedá označeniu, ktoré ste predtým vybrali pri prvom pripojení k nej. Vo Windowse Vista a novšom sa názov siete preberá automaticky z Centra sietí a zdieľania.

3.6.4. 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 ku vzdialeným počítačom).
- **Zaprotokolovať neznáme prichádzajúce/odchádzajúce prenosy** – všetky pokusy o komunikáciu (prichádzajúce/odchádzajúce) od neznámych aplikácií budú zaznamenané v [Protokole súasti Firewall](#).
- **Deaktivovať overovanie pravidiel pre všetky aplikácie** – Firewall neustále sleduje všetky súbory, ktorých sa každé aplikácie pravidlo týka. Ak nastane zmena binárneho súboru, Firewall znovu vykoná pokus o potvrdenie dôveryhodnosti danej aplikácie pomocou štandardných spôsobov, napríklad overením jej certifikátu, jej vyhlásením v [databáze dôveryhodných aplikácií](#) atď. Ak aplikáciu nie je možné považovať za bezpečnú, Firewall bude s ňou zachádzať v súlade s [vybraným režimom](#):
 - ak je Firewall spustený v [Automatickom režime](#), aplikácia bude v predvolenom nastavení povolená,
 - ak je Firewall spustený v [Interaktívnom režime](#), aplikácia bude blokována a zobrazí sa dialógové okno so žiadosťou, aby používateľ rozhodol, ako by sa malo s aplikáciou zaobchádzať.

Želaný postup určujúci spôsob, akým sa má zaobchádzať s konkrétnou aplikáciou, môžete samozrejme stanoviť samostatne pre každú aplikáciu v dialógovom okne [Aplikácie](#).



3.6.5. Zadefinované siete

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

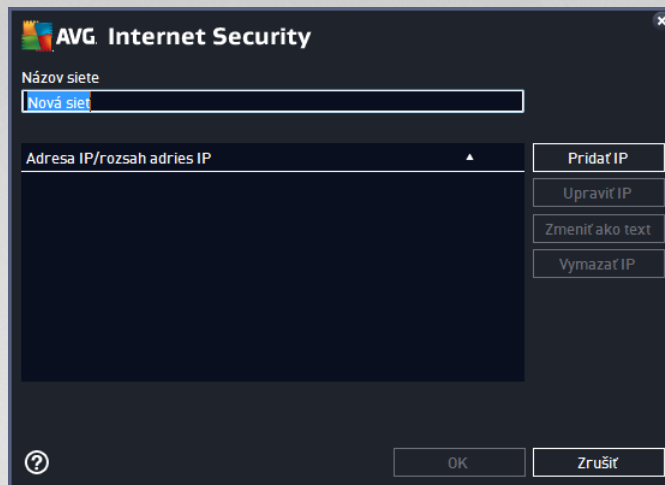


V dialógovom okne **Zadefinované siete** sa nachádza zoznam všetkých sietí, ku ktorým je počítač pripojený. V zozname sú uvedené nasledujúce informácie o každej zistenej sieti:

- **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

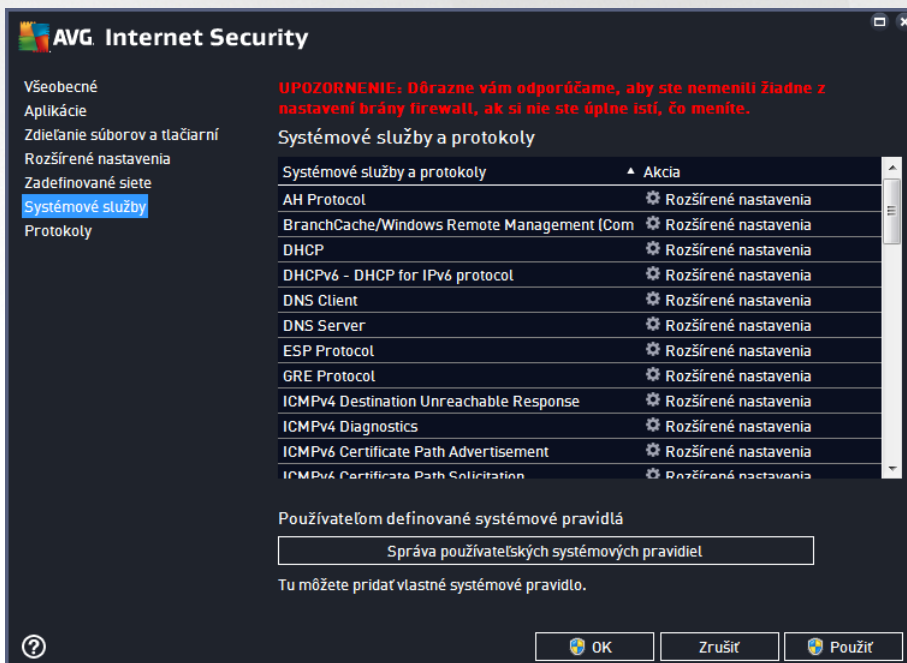
- **Pridať sieť** – otvorí nové dialógové okno, kde môžete upraviť parametre novo definovanej siete, t. j. zadať **názov siete** a **rozsah IP adresy**.



- **Upravi sie** – otvorí dialógové okno **Vlastnosti siete** (pozrite 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.

3.6.6. 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:

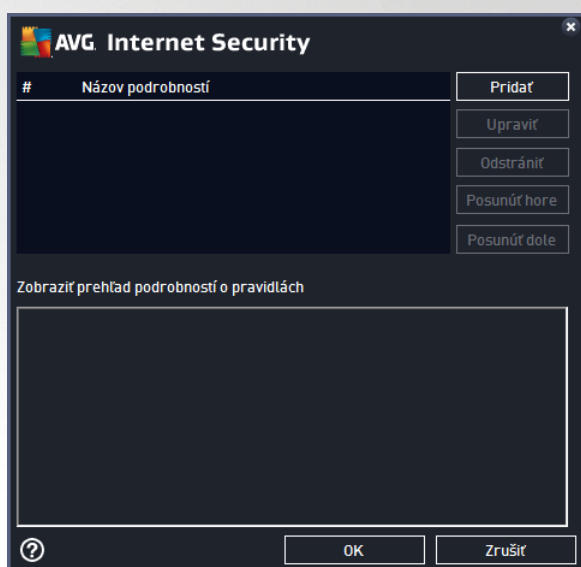


- **Systémová služba a protokoly** – v tomto stpci je uvedený názov príslušnej systémovej služby.
- **Akcia** – tento stpec zobrazuje ikonu pridelenej akcie:
 - Umožni komunikáciu pre všetky siete
 - Blokuje komunikáciu

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

Používateľom definované systémové pravidlá

Ak chcete otvoriť nové dialógové okno na definovanie vlastného pravidla pre systémovú službu (*pozri obrázok nižšie*), stlačte 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 časti tohto dialógového okna sa nachádza prehľad všetkých podrobností o práve editovanom systémovom pravidle, v dolnej časti sa nachádzajú zvolené informácie. Príslušným tlačidlom môžete podrobnosti o pravidle upravi, pridať alebo vymazať:



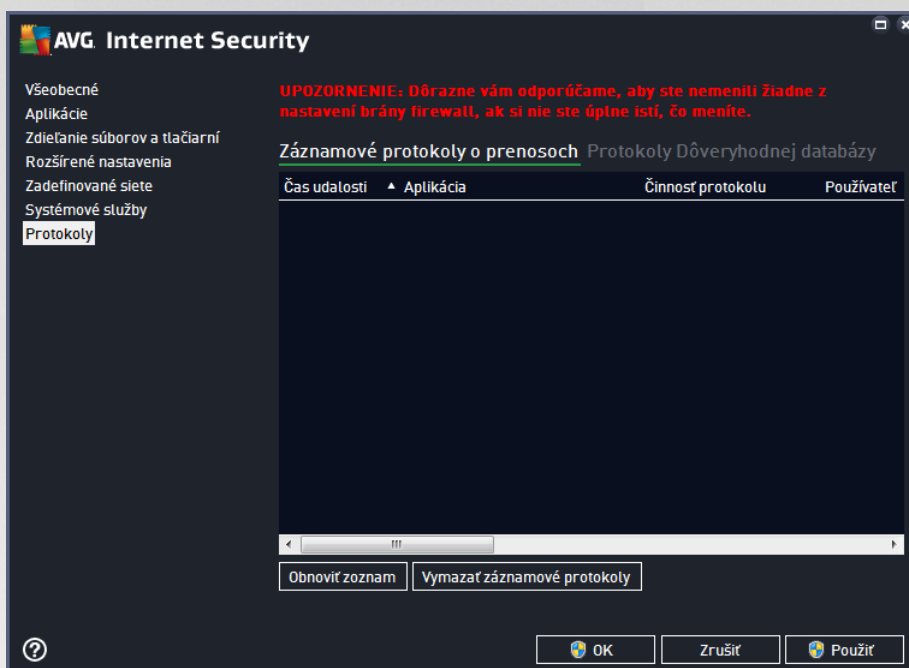
Nezabudnite, že podrobné nastavenie pravidiel je pokrivená funkcia určená najmä pre správcov siete, ktorí potrebujú mať úplnú kontrolu nad konfiguráciou Firewallu. Ak nie ste oboznámení s typmi komunikačných protokolov, s listami sieťových portov, definíciami adries IP a pod., nemeňte tieto nastavenia!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

3.6.7. Protokoly

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

Dialógové okno **Protokoly** vám umožní skontrolovať zoznam všetkých zaprotokolovaných činností a udalostí súvisiacich s Firewallom s podrobným popisom príslušných parametrov zobrazenom na dvoch kartách:

- **Záznamové protokoly o prenosoch** – na tejto karte nájdete informácie o aktivitách všetkých aplikácií, ktoré sa pokúsili pripojiť do siete. Pre každú položku tu sú uvedené údaje o dате udalosti, názve aplikácie, príslušnej zaprotokolovanej činnosti, mene používateľa, PID, smere prenosu, type protokolu, pošte vzdialených a miestnych portov a o miestnych a vzdialených adresách IP.



- **Protokoly Dôveryhodnej databázy** – Dôveryhodná databáza je interná databáza AVG, ktorá zhromažďuje informácie o certifikovaných a dôveryhodných aplikáciách, ktorým sa môže vždy povoliť komunikácia online. Pri prvom pokuse novej aplikácie o pripojenie do siete (t. j. ak doposiaľ nebolo vytvorené pravidlo pre firewall súvisiace s touto aplikáciou) je potrebné zistiť, či sa má povoliť sieťová komunikácia príslušnej aplikácie. AVG najskôr prehľadá Dôveryhodnú databázu a ak je v nej aplikácia uvedená, potom sa jej automaticky povolí prístup k sieti. Až potom, v prípade, 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.



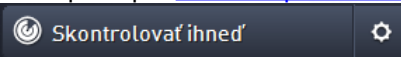
Ovládacie tlačidlá

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

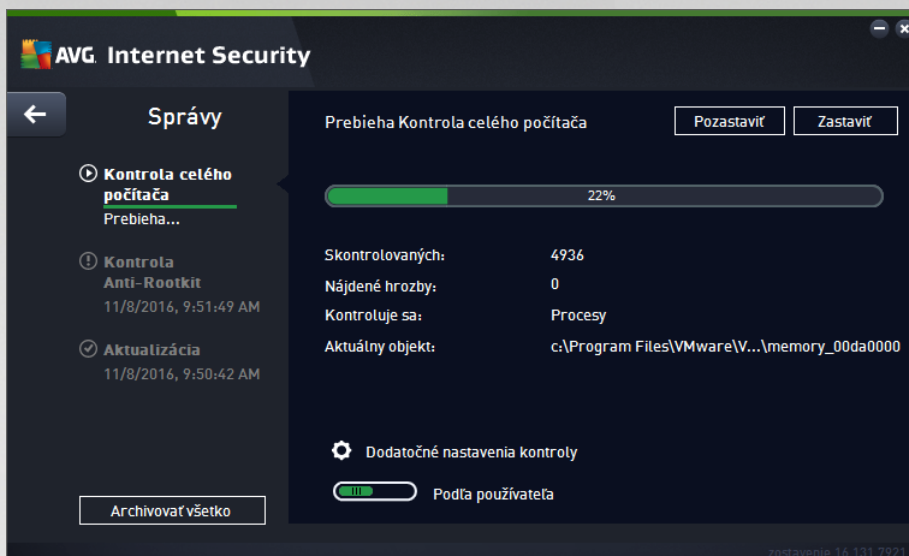
3.7. Kontrola AVG

V predvolenom nastavení **AVG Internet Security** nespúšťa žiadnu kontrolu, pretože po úvodnej kontrole (*zobrazí sa vám návrh na jej spustenie*) by ste mali byť dokonale chránení rezidentnými sústavami **AVG Internet Security**, 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 AVG máte prístup z [hlavného používateľského rozhrania](#) prostredníctvom tlačidla graficky

rozdeleného na dve časti: 

- **Skontrolovať teraz** – stlačením tohto tlačidla pre okamžité spustenie [Kontroly celého počítača](#) a sledujte jej priebeh a výsledky v automaticky otvorenom okne [Výsledky](#):



- **Možnosti** – vyberte toto tlačidlo (graficky zobrazené ako tri vodorovné čiary v zelenom poli), ktorým otvoríte dialógové okno **Možnosti kontroly**, kde môžete [upravi naplánované kontroly](#) a parametre [Kontroly celého počítača/Kontroly súborov/priečinkov](#).



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

- **Upravi naplánované kontroly** – kliknutím na túto možnosť sa otvorí nové [dialógové okno s prehľadom všetkých naplánovaných kontrol](#). Než zadefinujete vlastné kontroly, zobrazí sa v tabu len iba jeden plán kontroly, ktorý vopred definoval dodávateľ softvéru. Táto kontrola je predvolene vypnutá. Ak ju chcete zapnúť, kliknite na tlačidlo na pravom tlačiteli a v kontextovej ponuke vyberte možnosť *Povoli úlohu*. Po povolení plánu kontroly môžete [upravi jej konfiguráciu](#) tlačidlom *Upravi plán kontroly*. Taktiež môžete kliknúť na tlačidlo *Prida plán kontroly*, aby ste vytvorili nový vlastný 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 **Nastavenia** sa zobrazí [konfiguračné okno, kde môžete nastaviť parametre kontroly celého počítača](#).

- o **Kontrola súborov/priebehov/Nastavenia** – tlačidlo je opäť rozdelené na dve časti. Kliknutím na možnosť **Kontrola súborov/priebehov** okamžite spustíte kontrolu vybraných oblastí počítača (*podrobnosti o kontrole súborov a priebehov nájdete v príslušnej kapitole s názvom [Vopred definované kontroly/Kontrola súborov/priebehov](#)*). Kliknutím na **Nastavenia** sa zobrazí [konfiguračné okno, kde môžete nastaviť parametre kontroly súborov a priebehov](#).
- o **Skontrolovať počítač na prítomnosť rootkitov/Nastavenia** – avšak oboje tlačidlá označujúce **Skontrolovať počítač na prítomnosť rootkitov** sa spustí okamžitá kontrola anti-rootkit (*podrobnosti o kontrole rootkitov nájdete v príslušnej kapitole pod názvom [Preddefinované kontroly/Skontrolovať počítač na prítomnosť rootkitov](#)*). Kliknutím na **Nastavenia** sa zobrazí konfiguračné okno, kde môžete [nastaviť parametre kontroly rootkitov](#).

3.7.1. Vopred definované kontroly

Jednou z hlavných funkcií programu **AVG Internet Security** 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.

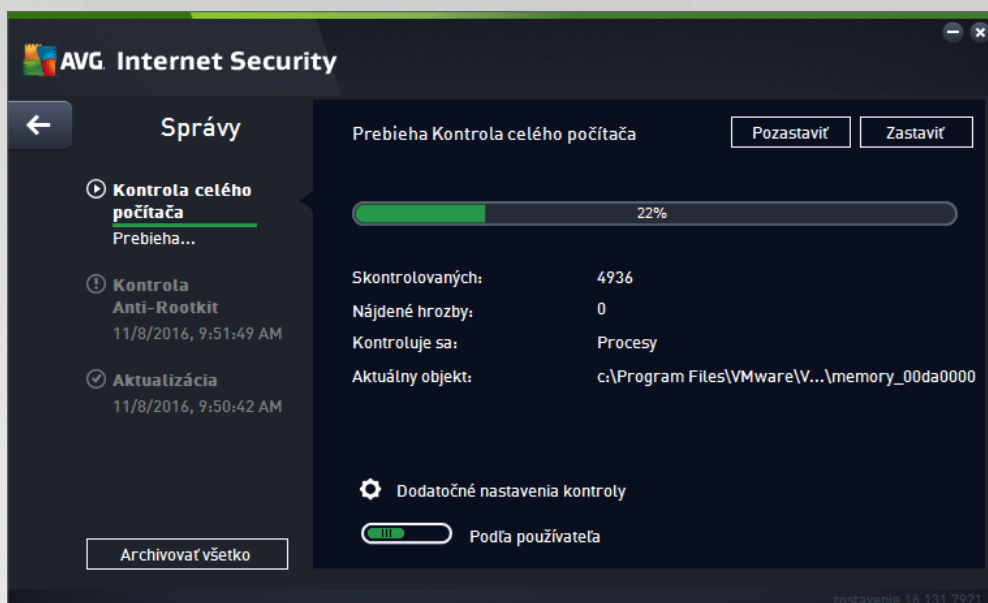
V produkte **AVG Internet Security** sa nachádzajú tieto typy kontrol vopred definované dodávateľom softvéru:

3.7.1.1. Kontrola celého počítača

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

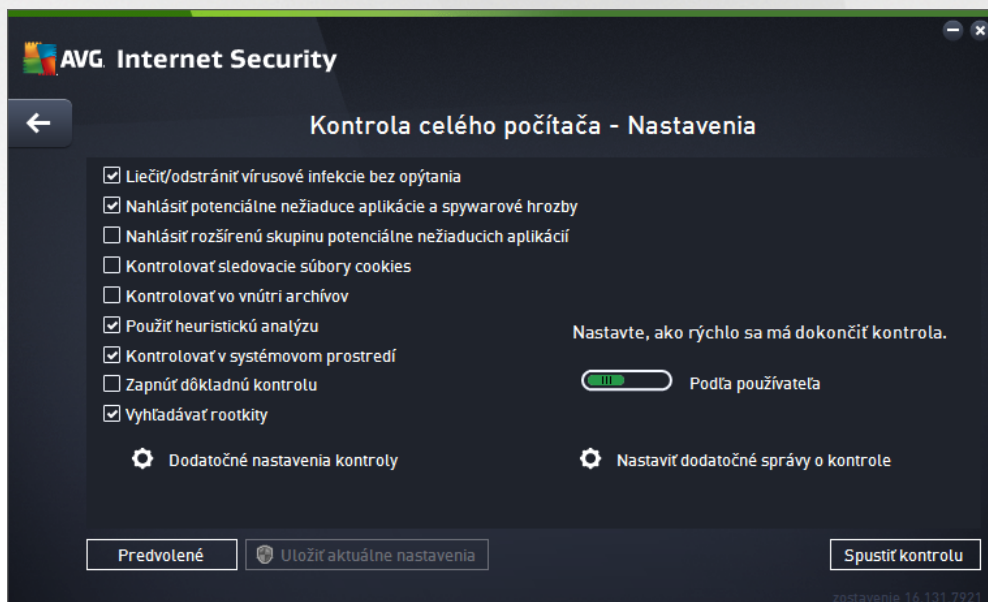
Spustenie kontroly

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



Zmena konfigurácie kontroly

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



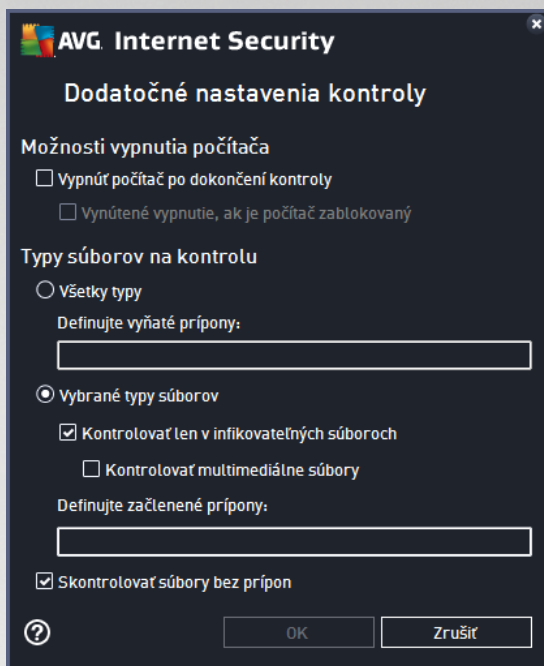
V zozname parametrov kontroly môžete zapnúť /vypnúť špecifické parametre podľa potreby:

- **Liečiť /odstrániť vírusovú infekciu bez opýtania** (predvolené zapnuté) – ak sa počas kontroly nájde vírus, môže byť automaticky vyliečený, pokiaľ je liek k dispozícii. Ak nie je možné infikovaný súbor vyliečiť automaticky, presunie sa do [Vírusového trezora](#).
- **Nahlásiť potenciálne nežiaduce aplikácie a hrozby spyware** (predvolené zapnuté) – zhlásiť toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu



malware: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.

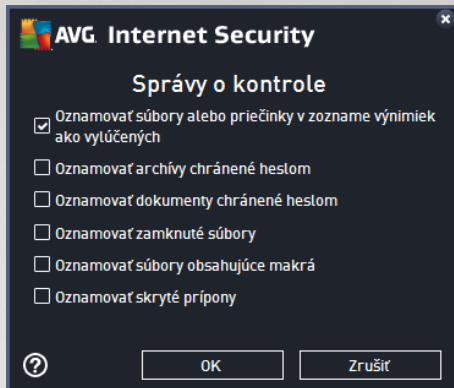
- **Hlási rozšírenú skupinu potenciálne nežiaducich aplikácií** (predvolene vypnuté) – zaškrtnite toto políčko, ak sa má detegovať rozšírená skupina spywaru: programov, ktoré sú úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpečenia počítača, ale môže blokovать dobré programy, a preto je táto funkcia predvolene vypnutá.
- **Kontrolova sledovacie súbory cookies** (predvolene vypnuté) – tento parameter zapína funkciu na detekciu súborov cookies (cookies protokolu HTTP sa používajú na overenie totožnosti, sledovanie a uchovávanie konkrétnych informácií o používateľoch, akými sú napríklad preferencie alebo obsah elektronických nákupných košíkov).
- **Kontrolova vo vnútri archívov** (predvolene vypnuté) – tento parameter určuje, že sa majú poas kontroly preverovať všetky súbory uložené vnútri archívov, napr. ZIP, RAR, atď.
- **Použi heuristickú analýzu** (predvolene zapnuté) – heuristická analýza (dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí) bude jednou z metód, ktoré sa použijú na detekciu vírusov poas kontroly.
- **Kontrolova v systémovom prostredí** (predvolene zapnuté) – poas kontroly sa budú overovať aj systémové oblasti počítača.
- **Zapnú dôkladnú kontrolu** (predvolene vypnuté) – v určitých situáciách (podozrenia na infikovanie počítača) môžete zaškrtnúť túto možnosť, aby ste aktivovali najdôkladnejšie kontrolné algoritmy, ktoré pre úplnú istotu skontrolujú aj tie oblasti počítača, ktoré sa obyčajne vôbec neinfikujú. Upozorujeme však, že tento spôsob je náročný na as.
- **Kontrolova rootkity** (predvolene zapnuté) – zahrnie kontrolu prítomnosti rootkitov do kontroly celého počítača. [Kontrolu anti-rootkit](#) možno spustiť aj samostatne.
- **Dodatné nastavenia kontroly** – tento odkaz otvorí nové dialógové okno Dodatok nastavenia kontroly, ktoré sa používa na nastavenie nasledujúcich parametrov.



- **Možnosti vypnutia počítača** – rozhodnite, či sa má po skončení kontroly vypnúť počítač automaticky po dokončení procesu kontroly. Po potvrdení tejto možnosti (**Vypnúť počítač po dokončení kontroly**) sa aktivuje nová možnosť, ktorá umožní vypnúť počítač, aj keď je momentálne zamknutý (**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 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 predvolene 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 pod a používate a. Prípadne môžete spustiť procesy kontroly pomalšie, čím sa minimalizuje využívanie počítačových zdrojov (užitočné vtedy, keď potrebujete pracovať na počítači, ale nezaujímajú vás, ako dlho bude kontrola trvať), alebo rýchlejšie s vyššou mierou využívania počítačových zdrojov (napríklad, keď sa počítač dočasne nepoužíva).
- **Vytvoriť ďalšie správy o kontrole** – odkaz otvorí nové dialógové okno **Správy o kontrole**, v ktorom



môžete určiť, aké typy možných nálezov sa majú hlásiť :



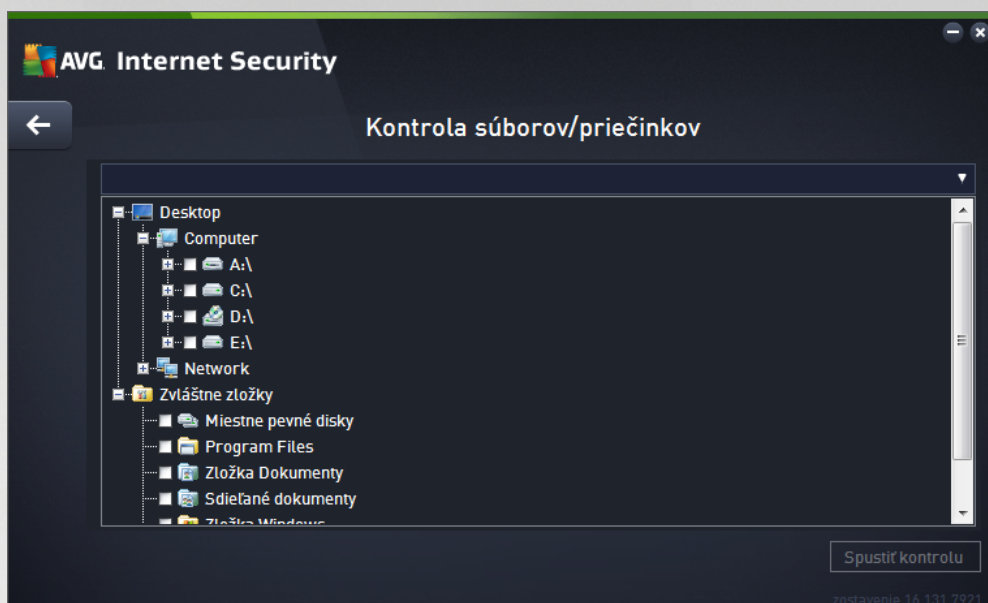
Varovanie: Tieto nastavenia kontroly sa zhodujú s parametrami novo definovanej kontroly; pozrite informácie [v kapitole Kontrola AVG/Plánovanie kontroly/Ako kontrolovať](#). Ak sa rozhodnete zmeniť predvolenú konfiguráciu funkcie **Kontrola celého počítača**, svoje nové nastavenie môžete uložiť ako predvolenú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

3.7.1.2. Kontrola súborov/priečinkov

Kontrola súborov/priečinkov – kontrolujú sa 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.

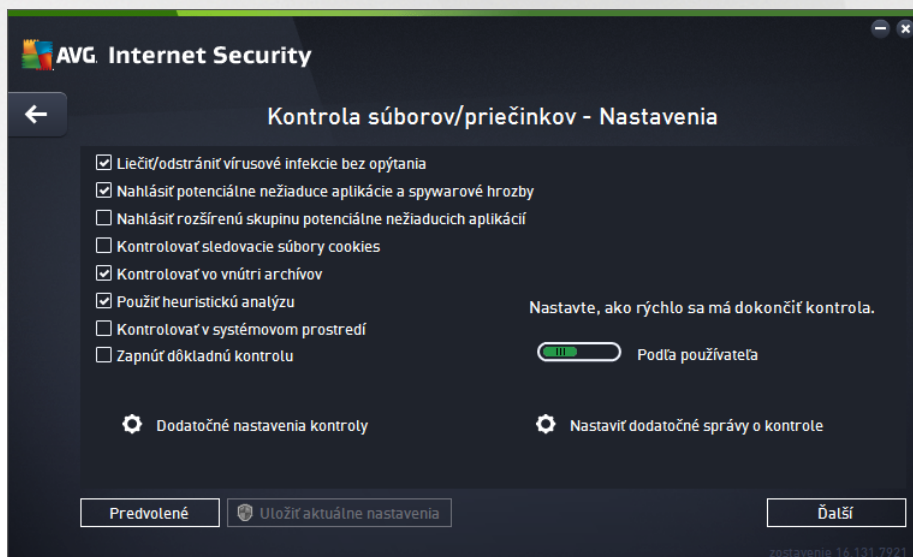
Spustenie kontroly

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



Zmena konfigurácie kontroly

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



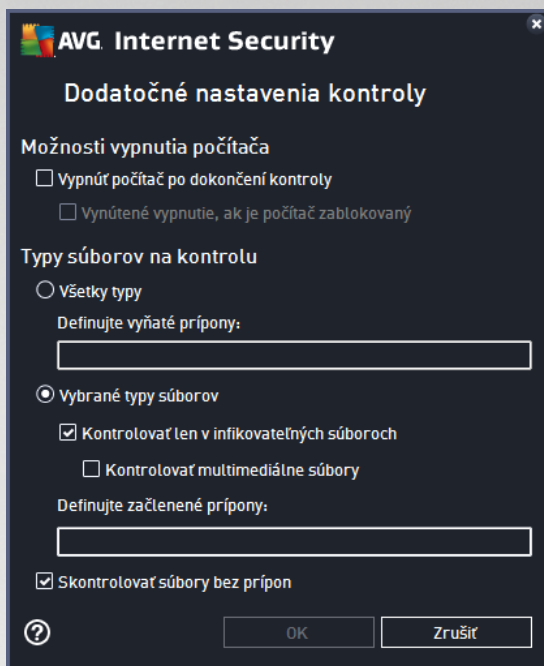
V tomto zozname parametrov kontroly môžete podľa potreby vypnúť alebo zapnúť konkrétne parametre:

- **Liečenie/odstránenie vírusových infekcií bez opýtania** (predvolené zapnuté): Ak sa počas kontroly identifikuje vírus, môže sa automaticky vylíčiť, ak je dostupná liečba. Ak nie je možné infikovaný súbor vylíčiť automaticky, premiestni sa do [Vírusového trezora](#).
- **Nahlásenie potenciálne nežiaducich aplikácií a spywarových hrozieb** (predvolené zapnuté): Zaujímať sa o toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu malware: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu



by nainštalované úmyselne. Odporujeme vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.

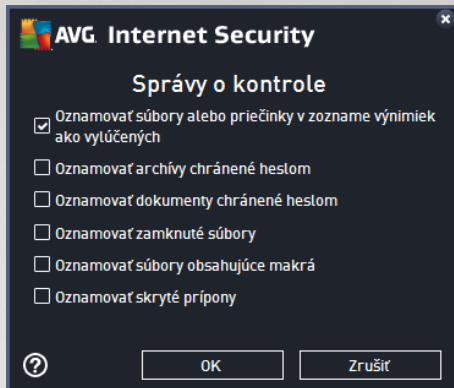
- **Nahlási rozšírenú skupinu potenciálne nežiaducich aplikácií** (predvolene vypnuté): Zaujímať sa môžete o toto políčko, ak sa má detegovať rozšírená skupina spywaru: programov, ktoré sú úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpečenia počítača, ale môže blokovать dobré programy, a preto je táto funkcia predvolene vypnutá.
- **Kontrolova sledovacie súbory cookies** (predvolene vypnuté): Tento parameter súvisí s zapínaním funkcie na detekciu súborov cookies (súbory 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** (predvolene zapnuté): Tento parameter definuje, že počas kontroly by sa mali kontrolovať všetky súbory, aj tie, ktoré sa nachádzajú vo vnútri archívov, napr. ZIP, RAR, atď.
- **Použi heuristickú analýzu** (predvolene zapnuté): Heuristická analýza (dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí) bude jednou z metód, ktoré sa použijú na detekciu vírusov počas kontroly.
- **Kontrolova v systémovom prostredí** (predvolene vypnuté): Počas kontroly sa budú kontrolovať aj systémové oblasti vášho počítača.
- **Zapnú dôkladnú kontrolu** (predvolene vypnuté): V určitých situáciách (podozrenie na infikovanie počítača) môžete touto možnosťou aktivovať najdôkladnejšie kontrolné algoritmy, ktoré pre istotu skontrolujú aj tie oblasti počítača, ktoré sa obyčajne vôbec neinfikujú. Upozorujeme však, že tento spôsob je náročný na procesor.
- **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 po skončení kontroly vypnúť počítač automaticky po dokončení procesu kontroly. Po potvrdení tejto možnosti (**Vypnúť počítač po dokončení kontroly**) sa aktivuje nová možnosť, ktorá umožní vypnúť počítač, aj keď je momentálne zablokovaný (**Vynútené vypnutie, ak je počítač zablokovaný**).
- **Typy súborov na kontrolu** – mali by ste tiež určiť, čo chcete kontrolovať:
 - **Všetky typy súborov** s možnosťou definovať výnimky z kontroly vytvorením zoznamu 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 súborov – ak necháte toto políčko nezaujaté, 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 predvolene 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 kontroly pomalšie, čím sa minimalizuje využívanie počítačových zdrojov (*užitočné vtedy, keď potrebujete pracovať na počítači, ale nezaujíma vás, ako dlho bude kontrola trvať*), alebo rýchlejšie s vyššou mierou využívania počítačových zdrojov (*napríklad keď sa počítač dočasne nepoužíva*).
- **Vytvoriť ďalšie správy o kontrole** – odkaz otvorí nové dialógové okno **Správy o kontrole**, ktoré vám



umožní nastavi , ktoré typy možných nálezov sa majú hlási :



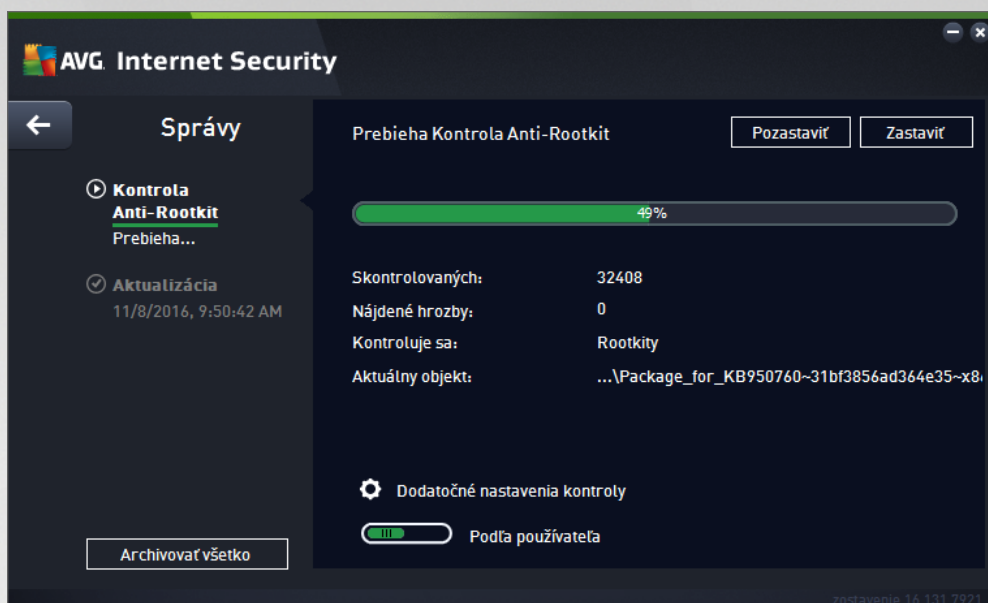
Varovanie: Tieto nastavenia kontroly sa zhodujú s parametrami novo definovanej kontroly; pozrite informácie v kapitole [Kontrola AVG/Plánovanie kontroly/Ako kontrolova](#) . Ak sa rozhodnete zmeni predvolenú konfiguráciu funkcie **kontrola súborov/prie inkov**, svoje nové nastavenie môžete potom uloži ako predvolenú konfiguráciu, ktorá sa použije pre všetky alšie kontroly konkrétnych súborov alebo prie inkov. Táto konfigurácia sa zároveň použije ako šablóna pre všetky vami novo naplánované kontroly ([všetky nastavené kontroly vychádzajú zo sú asnej konfigurácie kontroly vybraných súborov alebo prie inkov](#)).

3.7.1.3. Skontrolovať počítač na prítomnosť rootkitov

Kontrola po íta a na prítomnos rootkitov deteguje a ú inne odstra uje nebezpe né rootkity, t. j. programy a technológie, ktoré dokážu zamaskova prítomnos škodlivého softvéru vo vašom po íta i. Rootkit je program ur ený na to, aby sa zmocnil základnej kontroly nad po íta ovým systémom bez povolenia vlastníka systému a jeho právoplatných správcov. Kontrola dokáže zisti prítomnos rootkitov pomocou vopred definovanej skupiny pravidiel. Ak sa nájde rootkit, nemusí to nevyhnutne znamena , že je infikovaný. Programy rootkit sa niekedy používajú ako ovláda e, príp. tvoria sú as správnych aplikácií.

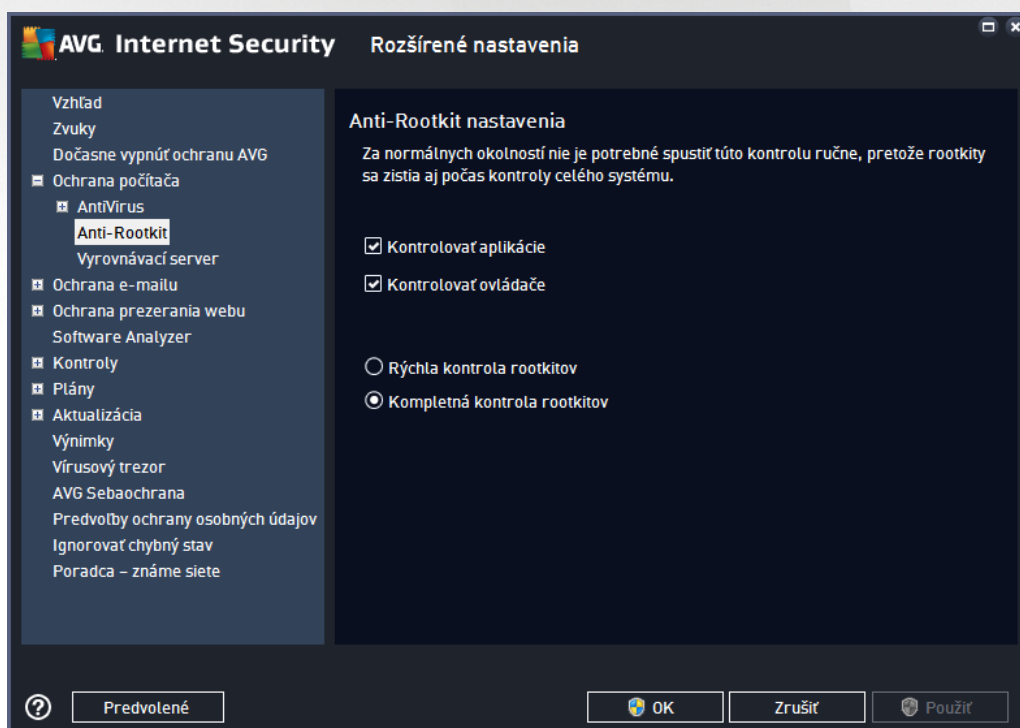
Spustenie kontroly

Kontrola po íta a na prítomnos rootkitov môže by spustená priamo z dialógového okna [Možnosti kontroly](#) kliknutím na tlačidlo **Kontrola po íta a na prítomnos rootkitov**. Otvorí sa nové dialógové okno s názvom **Priebeha kontrola Anti-Rootkit**, v ktorom sa zobrazuje priebeh spustenej kontroly:



Zmena konfigurácie kontroly

Konfiguráciu kontroly Anti-Rootkit môžete upraviť v dialógovom okne **Nastavenia nástroja Anti-Rootkit** (dialógové okno je prístupné cez odkaz **Nastavenia pre Kontrolu počítača** a na prítomnosť rootkitov v rámci dialógového okna [Možnosti kontroly](#)). **Odporúčame ponechať predvolené nastavenia, ak nemáte závažný dôvod ich meniť !**



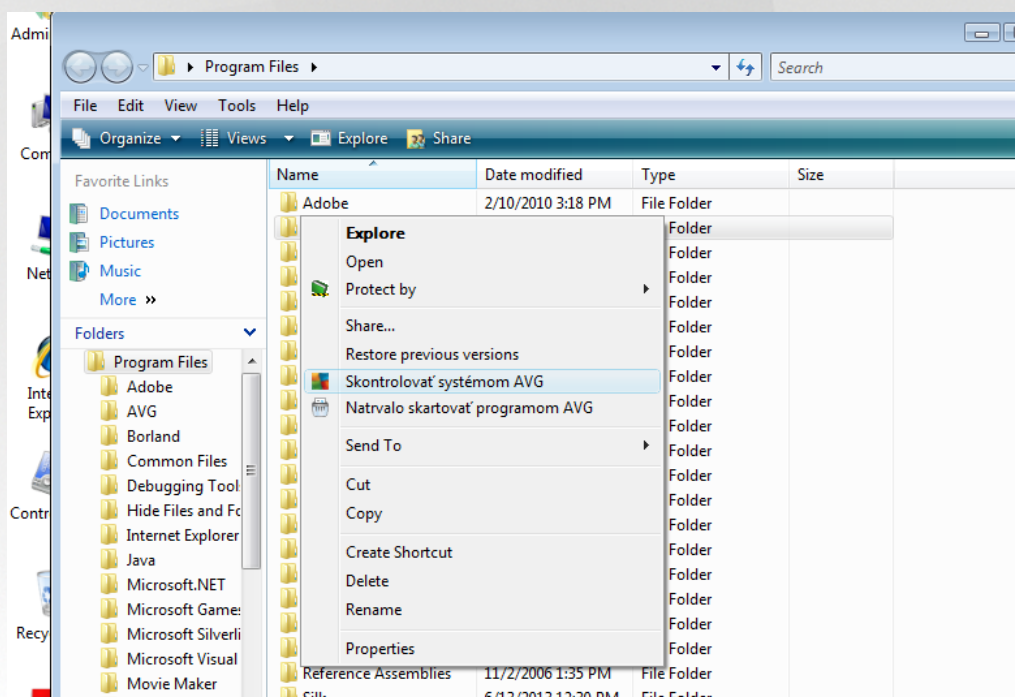
Možnosti **Kontrolovať aplikácie** a **Kontrolovať ovládače** vám umožnia podrobne nastaviť, čo by malo byť súčasťou kontroly Anti-Rootkit. Tieto nastavenia sú určené pre skúsených používateľov, odporúčame vám, aby ste nechali všetky možnosti zapnuté. Môžete tiež vybrať režim kontroly rootkitov.



- **Rýchla kontrola rootkitov** – kontroluje všetky spustené procesy, zavedené ovládače, a taktiež systémový priečinok (väšinou *c:\Windows*)
- **Kompletná kontrola rootkitov** – kontroluje všetky spustené procesy, zavedené ovládače a taktiež systémový priečinok (väšinou *c:\Windows*), a navyše všetky miestne disky (vrátane pamäťových médií, nie však disketové jednotky/jednotky CD)

3.7.2. Kontrola z prieskumníka

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



- V aplikácii Windows Explorer označte súbor (alebo priečinok), ktorý chcete skontrolovať.
- Kliknutím pravým tlačidlom myši na objekt otvorte kontextovú ponuku.
- Výberom možnosti **Skontrolovať programom AVG** skontrolujte súbor programom **AVG Internet Security**

3.7.3. Kontrola z príkazového riadka

V **AVG Internet Security** sa nachádza možnosť spustenia kontroly 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 väšinou parametrov, ktoré sa nachádzajú aj v grafickom používateľskom rozhraní AVG.

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



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

3.7.3.1. 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:**

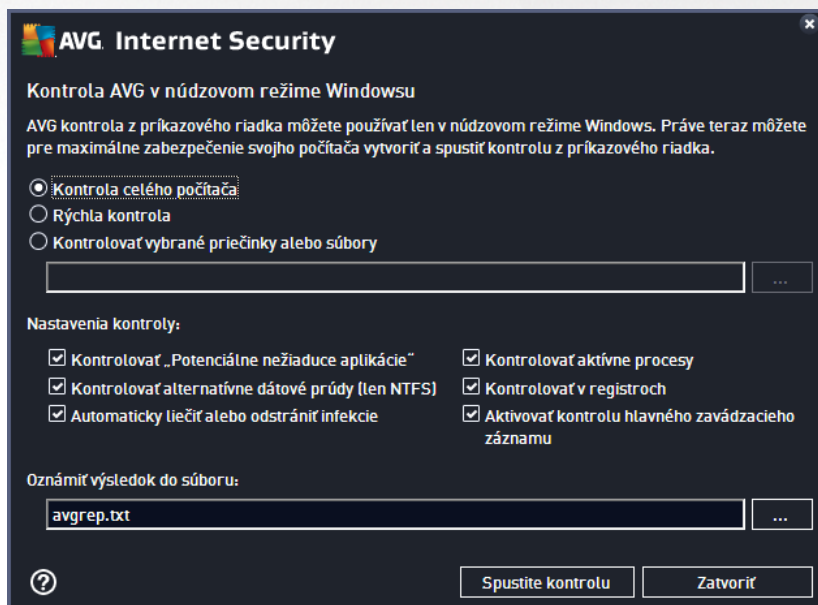
3.7.3.2. Parametre kontroly

Ak chcete zobraziť úplný prehľad použitých parametrov, zadajte príslušný príkaz spolu s parametrom **/?** alebo **/HELP** (napr. **avgscanx /?**). Jediný povinný parameter je **/SCAN**, ktorý definuje oblasti počítača, ktoré sa majú prehľadávať. 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**.

3.7.3.3. Kontrola z príkazového riadka spustená z grafického rozhrania

Keď je počítač spustený v Núdzovom režime, máte možnosť spustiť kontrolu pomocou príkazového riadka z grafického používateľského rozhrania:



V Núdzovom režime sa samotná kontrola spustí z príkazového riadka. Toto dialógové okno vám len umožňuje špecifikovať parametre kontroly v pohodlnom grafickom rozhraní.



Najskôr vyberte oblasti vášho počítača, ktoré chcete skontrolovať. Môžete sa rozhodnúť buď pre vopred definovanú [Kontrolu celého počítača](#), alebo pre možnosť [Skontrolovať vybrané priečinky](#). Tretia možnosť, **Rýchla kontrola**, spustí špeciálnu kontrolu vytvorenú na použitie v Núdzovom režime, ktorá kontroluje všetky dôležité oblasti potrebné na spustenie vášho počítača.

Nastavenia kontroly v ďalšej časti vám umožnia zadať podrobné parametre kontroly. V predvolenom nastavení sú všetky zaškrtnuté. Odporúčame vám ponechať ich takto označené a zaškrtnutie konkrétneho parametra zrušiť len v prípade, že na to máte konkrétny dôvod:

- **Kontrolovať „Potenciálne nežiaduce aplikácie“** – kontroluje spyware okrem vírusov
- **Kontrolovať alternatívne dátové prúdy (len pre NTFS)** – kontrola alternatívnych dátových prúdov NTFS, tzn. funkciu Windowsu, ktorú môžu zneužiť hackeri na skrývanie údajov, najmä škodlivého kódu
- **Automaticky liečiť alebo odstrániť infekcie** – všetky možné detekcie budú automaticky vyliečené alebo odstránené z vášho počítača
- **Kontrolovať aktívne procesy** – kontrola procesov a aplikácií načítaných do pamäte vášho počítača
- **Kontrolovať register** – kontrola registra Windows
- **Aktivovať kontrolu hlavného zavádzacieho záznamu** – kontrola tabuľky oblastí a zavádzacieho sektora

A nakoniec, v spodnej časti tohto dialógového okna môžete určiť názov a typ súboru správy o kontrole.

3.7.3.4. Parametre kontroly z príkazového riadka

Nasleduje zoznam všetkých dostupných parametrov pre kontrolu z príkazového riadka:

- /? Zobrazí pomoc k tejto téme
- /@ Súbor s príkazmi /názov súboru/
- /ADS Kontrolovať alternatívne dátové prúdy (len NTFS)
- /ARC Kontrolovať archívy
- /ARCBOMBSW Hlásí opakovane komprimované archívne súbory
- /ARCBOMBSW Hlásí archívne bomby (opakovane komprimované archívy)
- /BOOT Povolí kontrolu MBR/BOOT
- /BOOTPATH Spustí rýchlu kontrolu
- /CLEAN Automaticky vyčistiť
- /CLOUDCHECK Kontrola nesprávnych pozitívnych detekcií
- /COMP [Kontrola celého počítača](#)



- /COO Kontrolova súbory cookies
- /EXCLUDE Cesty alebo súbory, ktoré sa majú vynechať z kontroly
- /EXT Kontrolova tieto prípony (*napríklad EXT=EXE,DLL*)
- /FORCESHUTDOWN Vypnú počítač po dokončení kontroly
- /HELP Zobrazí pomocníka pre túto tému
- /HEUR Použije heuristickú analýzu
- /HIDDEN Hlásia súbory so skrytými príponami
- /IGNLOCKED Ignorovať zamknuté súbory
- /INFECTABLEONLY Kontrolovať len súbory s infikovateľnými príponami
- /LOG Generovať súbor s výsledkami kontroly
- /MACROW Hlásia makrá
- /NOBREAK Nepovolí prerušenie klávesmi CTRL-BREAK
- /NOEXT Nekontrolovať tieto prípony (*napríklad NOEXT=JPG*)
- /PRIORITY Nastaví prioritu kontroly (*nízka, automatická, vysoká* – pozrite sa [Rozšírené nastavenia/Kontroly](#))
- /PROC Kontrolovať aktívne procesy
- /PUP Hlásia potenciálne nežiaduce aplikácie
- /PUPEXT Hlásia rozšírenú skupinu potenciálne nežiaducich aplikácií
- /PWDW Hlásia súbory chránené heslom
- /QT Rýchly test
- /REG Kontrolovať register
- /REPAPPEND Pripojiť k súboru s hlásením
- /REPOK Hlásia neinfikované súbory so značkou OK
- /REPORT Hlásia do súboru (*názov súboru*)
- /SCAN [Kontrola súborov/priečinkov](#) (*SCAN=cesta;cesta* – napr. */SCAN=C:\;D:*)
- /SHUTDOWN Vypnú počítač po dokončení kontroly
- /THOROUGHSCAN Zapnúť dôkladnú kontrolu

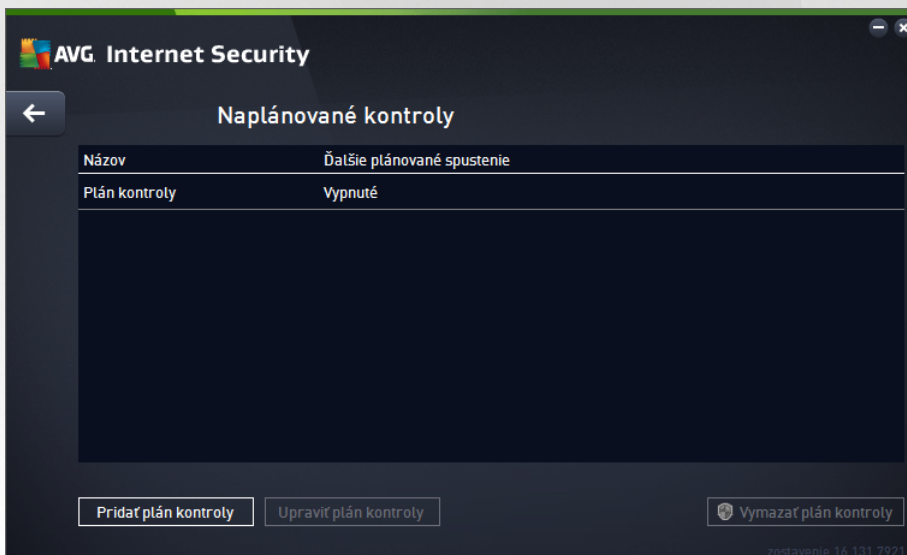


- /TRASH Presunú infikované súbory do [Vírusového trezora](#)

3.7.4. Plánovanie kontrol


Pomocou **AVG Internet Security** môžete spustiť kontrolu na požiadanie (*napríklad, keď máte podozrenie, že sa do počítača dostala infekcia*) alebo na základe vytvoreného plánu. Odporúčame spustiť kontroly na základe plánov. Týmto spôsobom môžete zabezpečiť, že je váš počítač chránený pred možnou infekciou a nebudete si musieť robiť starosti s tým, kedy a či vôbec máte spustiť kontrolu. Odporúčame vám, aby ste pravidelne, najmenej raz za týždeň, spustili [Kontrolu celého počítača](#). Podľa možnosti však kontrolu celého počítača spustíte každý deň v predvolenej konfigurácii plánu kontroly. Ak je počítač „stále zapnutý“, 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 kontrol**, ktoré zobrazíte tlačidlom **Správa plánu kontroly** v dialógovom okne [Možnosti kontroly](#). V novom dialógovom okne **Plán kontroly** môžete zobraziť prehľad všetkých naplánovaných kontrol:

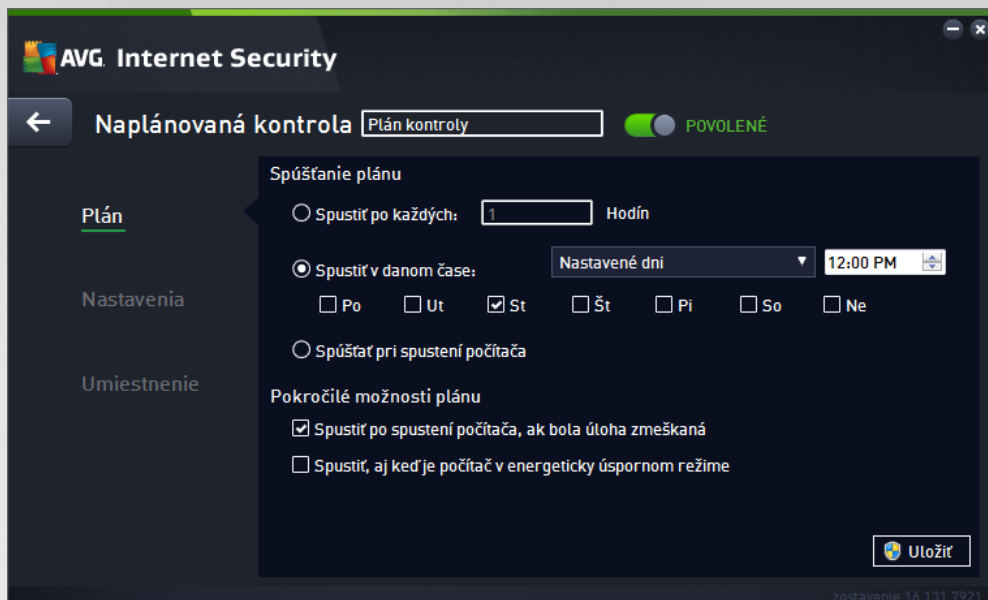


V dialógovom okne môžete zadať svoje vlastné kontroly. Pomocou tlačidla **Pridať plán kontroly** si môžete vytvoriť nový plán kontroly. Parametre plánu kontroly sa dajú upraviť (*alebo sa dá nastaviť nový plán*) v troch kartách:

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

Na každej karte môžete jednoducho zapnúť tlačidlo „semafor“ , aby ste dočasne deaktivovali naplánovaný test a znovu ho podľa potreby zapli.

3.7.4.1. 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 nezdajú na to, čo kontrola vlastne preveruje. Na druhej strane, príkladom dobrého opisného názvu je „Kontrola systémových oblastí“ a pod.

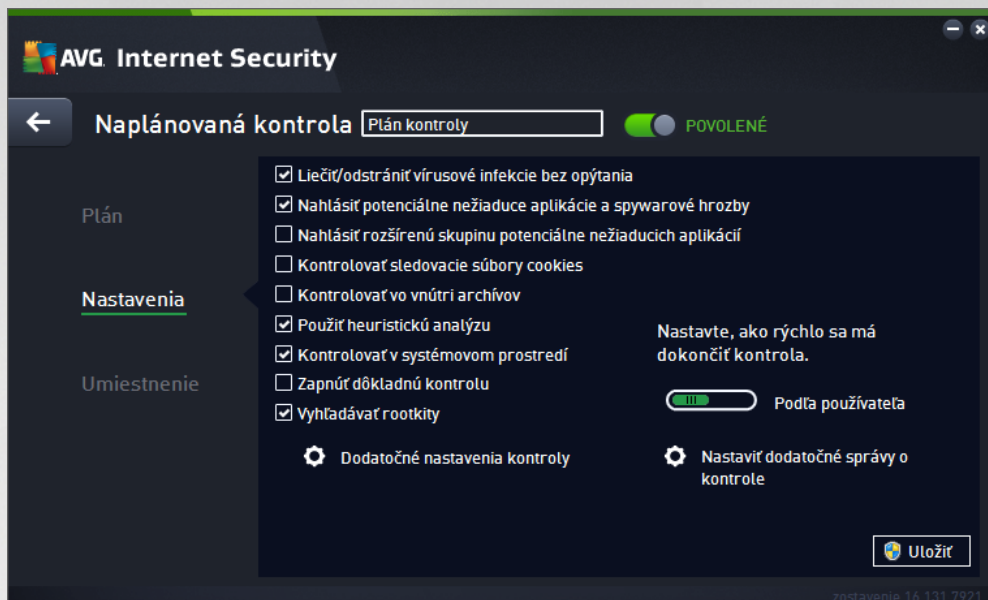
Toto dialógové okno umožňuje alej definovať tieto parametre kontroly:

- **Naplánovaná spúšťanie** – tu môžete nastaviť časové intervaly pre spustenie novo naplánovanej kontroly. Čas spúšťania sa definuje ako opakované spúšťanie kontroly po uplynutí určitého času (*Spustiť po každých ...*), definovaním presného dátumu a času (*Spustiť v konkrétnom čase*), prípadne definovaním udalosti, s ktorou sa bude spájať spustenie kontroly (*Spustiť pri spustení počítača*).
- **Možnosti pokročilého plánu** – táto časť vám umožní zadať podmienky, za akých podmienok by sa kontrola mala/nemala spustiť, ak je počítač v úspornom režime alebo celkom vypnutý. Keď sa spustí plán kontroly vo vami 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 zmení 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 [Plánu 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 [Plánu kontrol](#).

3.7.4.2. 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 voliť na zapnuté/vypnuté. **Ak nemáte závažný dôvod meniť tieto nastavenia, odporujeme vám ponechať vopred definovanú konfiguráciu:**

- **Liečiť/odstrániť vírusové infekcie bez opýtania** (predvolene zapnuté): ak sa počas kontroly identifikuje vírus, môže sa automaticky vylíčiť, ak je dostupná liečba. Ak nie je možné infikovaný súbor vylíčiť automaticky, premiestni sa do [Vírusového trezora](#).
- **Nahlásiť potenciálne nežiaduce aplikácie a spywarové hrozby** (predvolene zapnuté): začiarknite toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu malware: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporujeme vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
- **Nahlásiť rozšírenú skupinu potenciálne nežiaducich aplikácií** (predvolene 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 predvolene vypnutá.
- **Kontrola sledovacích súborov cookies** (predvolene vypnuté): tento parameter súčasně zapína funkciu na detekciu súborov cookies počas kontroly; (súbory 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** (predvolene vypnuté): tento parameter určuje, že sa majú počas

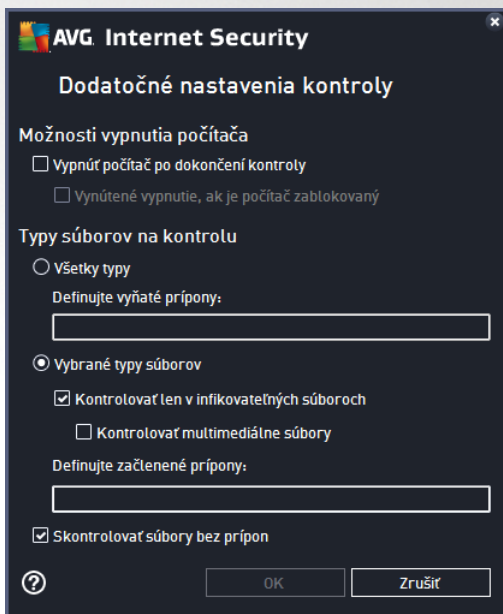


kontroly preverova všetky súbory, aj ke sú uložené vo vnútri archívu, napr. ZIP, RAR, at .

- **Použi heuristickú analýzu** (predvolene zapnuté): heuristická analýza (dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí) bude jednou z metód, ktoré sa použijú na detekciu vírusov počas kontroly.
- **Kontrolova v systémovom prostredí** (predvolene zapnuté): počas kontroly sa budú overovať aj systémové oblasti počítača.
- **Zapnú dôkladnú kontrolu** (predvolene vypnuté): v určitých situáciách (podozrenie na infikovanie počítača) môžete touto možnosťou aktivovať najdôkladnejšie kontrolné algoritmy, ktoré pre istotu skontrolujú aj tie oblasti počítača, ktoré sa obyčajne vôbec neinfikujú. Upozorujeme však, že tento spôsob je náročný na procesor.
- **Kontrolova rootkity** (predvolene zapnuté): Kontrola Anti-Rootkit kontroluje počítača a zisťuje prítomnosť potenciálnych rootkitov (programov a technológií, ktoré dokážu zakryť existenciu malwaru v počítači). Keď program deteguje rootkit, nemusí to nevyhnutne znamenať, že je počítač infikovaný. V niektorých prípadoch sa môžu určití ovládacie alebo časti bežných aplikácií nesprávne označovať 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 odkazov



oddelených prípon súborov, ktoré sa nemajú kontrolovať.

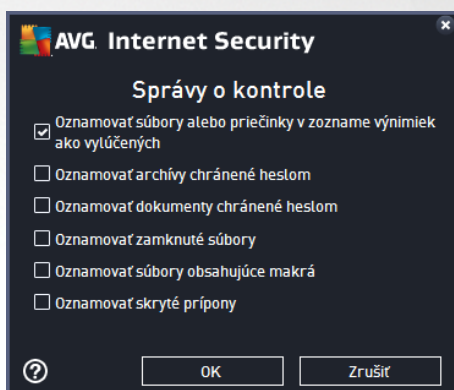
- o **Vybrané typy súborov** – môžete nastaviť, aby sa kontrolovali len súbory, pri ktorých existuje pravdepodobnosť infikovania (súbory, ktoré nemôžu byť napadnuté infekciou, napríklad niektoré jednoduché textové súbory alebo niektoré nespustiteľné súbory) vrátane mediálnych súborov (video, audio súborov – ak necháte toto políčko nezaškrtnuté, potom sa čas kontroly 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.
- o Alternatívne môžete rozhodnúť, že chcete **kontrolovať súbory bez prípony** – táto možnosť je predvolene 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 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 pred začatím doby trvania kontroly.

Vytvoriť ďalšie správy o kontrole

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

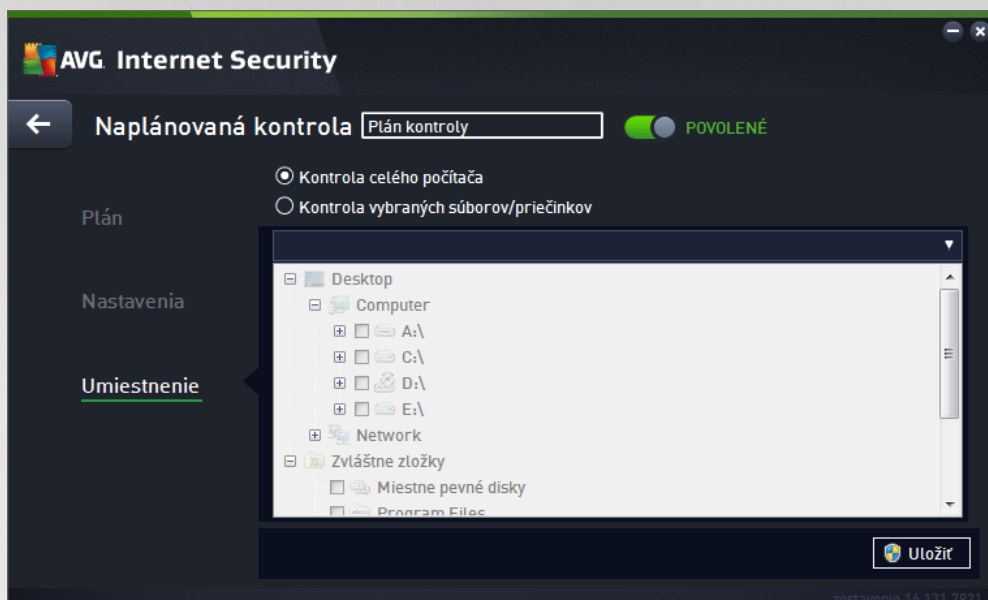


Ovládacie prvky dialógového okna

- **Uložiť** – uloží všetky zmeny, ktoré ste vykonali v tejto karte alebo v inej karte tohto dialógového okna a prepne naspäť do prehľadu [Plánu 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 [Plánu kontrol](#).



3.7.4.3. Umiestnenie



Na karte **Umiestnenie** môžete nastaviť, či chcete naplánovať [kontrolu celého počítača](#) alebo [kontrolu súborov/priečinkov](#). Keď vyberiete kontrolu súborov/priečinkov, potom sa v spodnej časti tohto dialógového okna aktivuje zobrazená stromová štruktúra, v ktorej môžete nastaviť priečinky, ktoré sa majú kontrolovať (rozbaťte položky kliknutím na uzol so znakom plus a vyberte priečinku, ktorú chcete kontrolovať). Zauklíknutím príslušných polí okna 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 za iarkavacieho políka:

- **Miestne pevné disky** – všetky pevné disky vášho počítača
- **Programové súbory**
 - C:\Program Files\
 - v 64-bitovej verzii C:\Program Files (x86)
- **Priečinku Moje dokumenty**
 - vo Windows XP: C:\Dokumenty a nastavenia\Predvolený používateľ\Moje dokumenty\
 - vo Windows Vista/7: C:\Používateľia\používateľ\Dokumenty\
- **Zdieľané dokumenty**
 - vo Windows XP: C:\Dokumenty a nastavenia\Všetci používatelia\Dokumenty\
 - vo Windows Vista/7: C:\Používateľia\Verejné\Dokumenty\

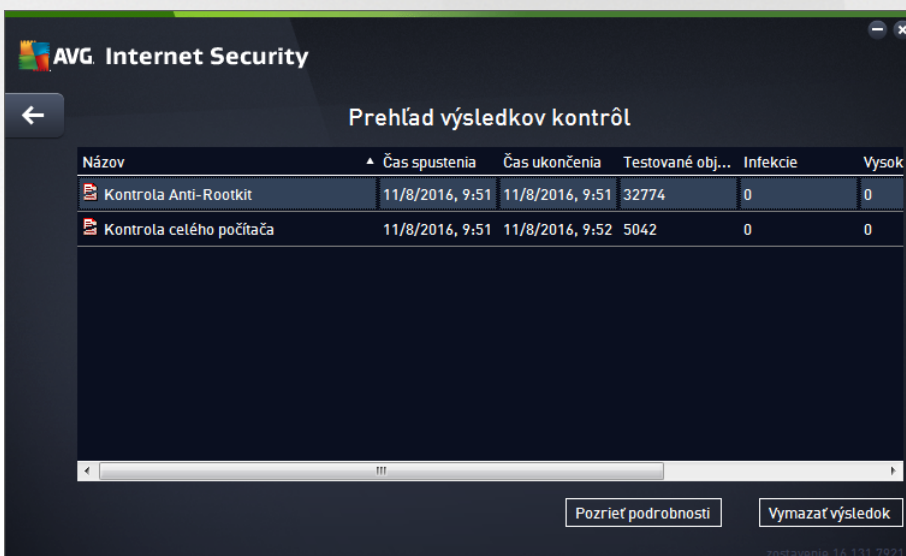


- **Prie inok Windows** – C:\Windows\
- **Iné**
 - **Systémový disk** – pevný disk, na ktorom je nainštalovaný operačný systém (zvyčajne C:)
 - **Systémový prie inok** – C:\Windows\System32\
 - **Prie inok Do asné súbory** – C:\Dokumenty a nastavenia\Používateľ\Miestne (Windows XP) alebo C:\Používateľia\používateľ\AppData\Local\Temp\ (Windows Vista/7)
 - **Do asné internetové súbory** – C:\Dokumenty a nastavenia\Používateľ\Miestne nastavenia\Do asné internetové súbory\ (Windows XP) alebo C:\Používateľia\používateľ\AppData\Local\Microsoft\Windows\Do asné internetové súbory (Windows Vista/7)

Ovládacie prvky dialógového okna

- **Uloži** – uloží všetky zmeny, ktoré ste vykonali v tejto karte alebo v inej karte tohto dialógového okna a prepne naspäť do prehľadu [Plánu 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 [Plánu kontrol](#).

3.7.5. Výsledky kontrol



Dialógové okno **Prehľad výsledkov kontrol** obsahuje zoznam výsledkov všetkých doterajších kontrol. Tabuľka obsahuje pre každý výsledok kontroly tieto údaje:

- **Ikona** – v prvom stĺpci sa zobrazuje informačná ikona popisujúca stav kontroly:
 - Nenašla sa žiadna infekcia, kontrola sa dokončila
 - Nenašla sa žiadna infekcia, kontrola sa prerušila pred dokončením



- Našli sa infekcie, ktoré neboli vyličené, kontrola sa dokončila
 - Našli sa infekcie, ktoré neboli vyličené, kontrola sa prerušila pred dokončením
 - Našli sa infekcie a všetky boli vyličené alebo odstránené, kontrola sa dokončila
 - Našli sa infekcie a všetky boli vyličené alebo odstránené, kontrola sa prerušila pred dokončením
- **Názov** – v stupci sa nachádza názov príslušnej kontroly. Buď je to jedna z dvoch [vopred definovaných kontrol](#), alebo váš vlastný [plán kontroly](#).
 - **as spustenia** – uvádza presný dátum a čas, kedy bola kontrola spustená.
 - **as 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 stupcoch je uvedený počet nájdených infekcií s vysokou, strednou a nízkou závažnosťou.
 - **Rootkity** – uvádza celkový počet [rootkitov](#) nájdených počas kontroly.

Ovládacie prvky dialógového okna

Pozrieť podrobnosti – kliknutím na tlačidlo zobrazíte [podrobné informácie o vybranej kontrole](#) (označené v tabuľke vyššie).

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

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

3.7.6. 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 karta poskytuje základné informácie o kontrole: či bola dokončená úspešne, či boli nájdené nejaké hrozby a čo sa s nimi stalo.
- **Podrobnosti** – táto karta 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 karta je zobrazená len v prípade, že boli počas kontroly detegované nejaké hrozby, a uvádza podrobné informácie o týchto hrozbách:



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

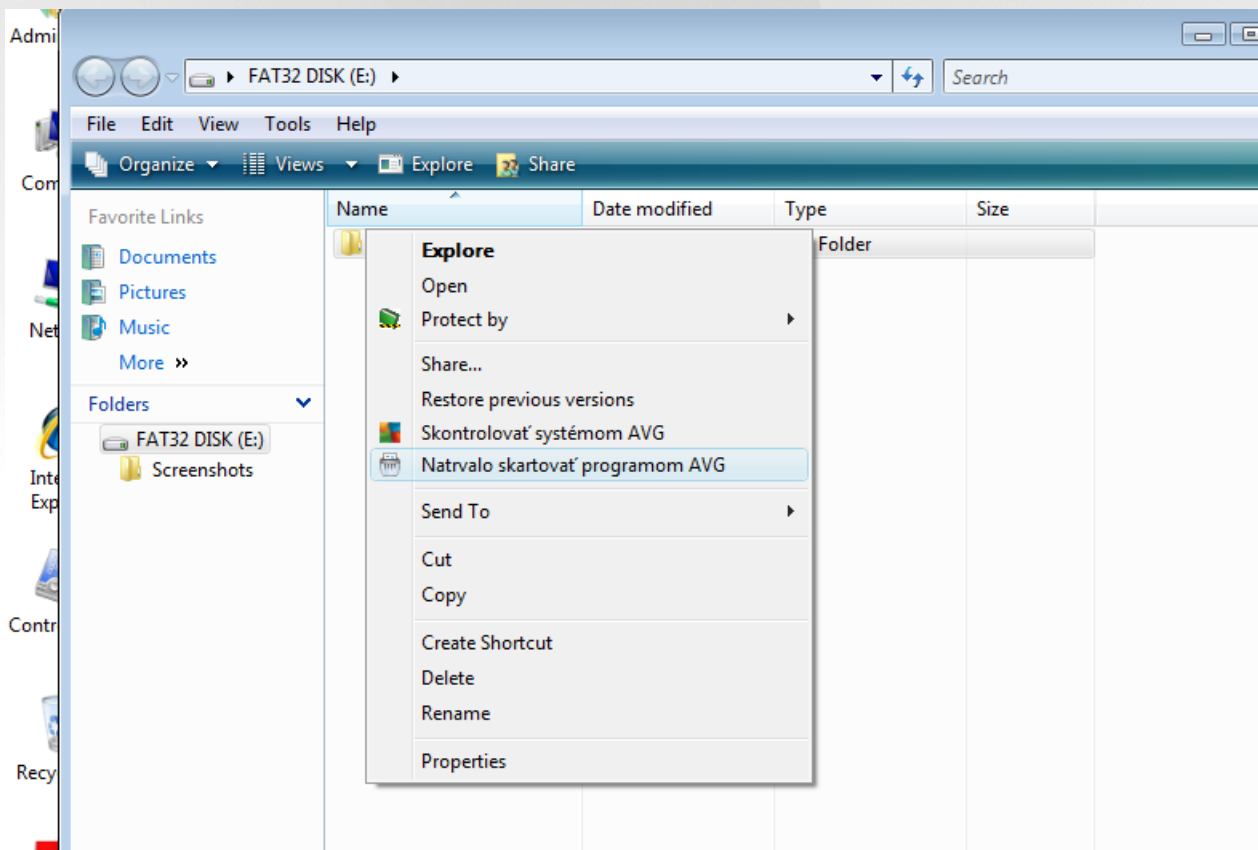
•• **Stredná závažnosť** : obvykle potenciálne nežiaduce aplikácie (ako napríklad adware) alebo sledovacie súbory cookies

••• **Vysoká závažnosť** : vážne hrozby, ako napríklad vírusy, trójske kone a zneužitia. Taktiež objekty detegované heuristickou metódou detekcie, teda hrozby, ktoré ešte nie sú popísané vo vírusovej databáze.

3.8. AVG File Shredder

AVG File Shredder bol navrhnutý na úplne bezpečné vymazávanie súborov, teda bez akejkoľvek možnosti ich obnovenia, dokonca ani s pokročilými softvérovými nástrojmi na to určenými.

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



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



3.9. Vírusový trezor

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

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

- **Pridaný dátum** – uvádza dátum a čas, kedy bol podozrivý súbor detegovaný a presunutý do Vírusového trezora.
- **Hrozba** – ak sa rozhodnete nainštalovať súčasný [Software Analyzer](#) v rámci **AVG Internet Security**, potom sa v tejto časti bude nachádzať grafické znázornenie úrovne závažnosti zisteného nálezku: od vyhovujúcej (*tri zelené bodky*) až po veľmi nebezpečnú (*tri červené bodky*). Taktiež zistíte informácie o type infekcie a jej pôvodnom umiestnení. Odkaz *Viac informácií* vás presmeruje na stránku v [online vírusovej encyklopédii](#) uvádzajúcu podrobné informácie o zistenej hrozbe.
- **Zdroj** – uvádza, ktorá súčasná **AVG Internet Security** zistila príslušnú hrozbu.
- **Oznámenia** – 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:

- **Obnovi** – odstráni infikovaný súbor naspäť na jeho pôvodné umiestnenie na vašom disku.
- **Obnovi ako** – premiestni infikovaný súbor do vybraného priežinku.
- **Zaslať na analýzu** – toto tlačidlo je aktívne len v prípade, že v zozname detekcií vyššie označíte objekt. V takomto prípade máte možnosť zaslať vybranú detekciu do vírusových laboratórií spoločnosti AVG na ďalšiu podrobnú analýzu. Upozorujeme, že táto funkcia by sa mala predovšetkým používať len na zasielanie súborov nesprávne detegovaných, t. j. súborov, ktoré program AVG označil ako infikované alebo podozrivé, ale o ktorých ste presvedčení, že sú neškodné.
- **Podrobnosti** – ak chcete zobraziť podrobné informácie o konkrétnej hrozbe vložennej do karantény vo **Vírusovom trezore**, označte vybranú položku v zozname a kliknutím na tlačidlo **Podrobnosti** otvoríte nové dialógové okno s popisom zistenej hrozby.
- **Vymazať** – dokonale a nenávratne odstráni infikovaný súbor z **Vírusového trezora**.
- **Vyprázdni trezor** – vymaže celý obsah **Vírusového trezora**. Odstránením z **Vírusového trezora** sa súbory úplne a nenávratne odstránia z disku (*nepremiestnia sa do Koša*).

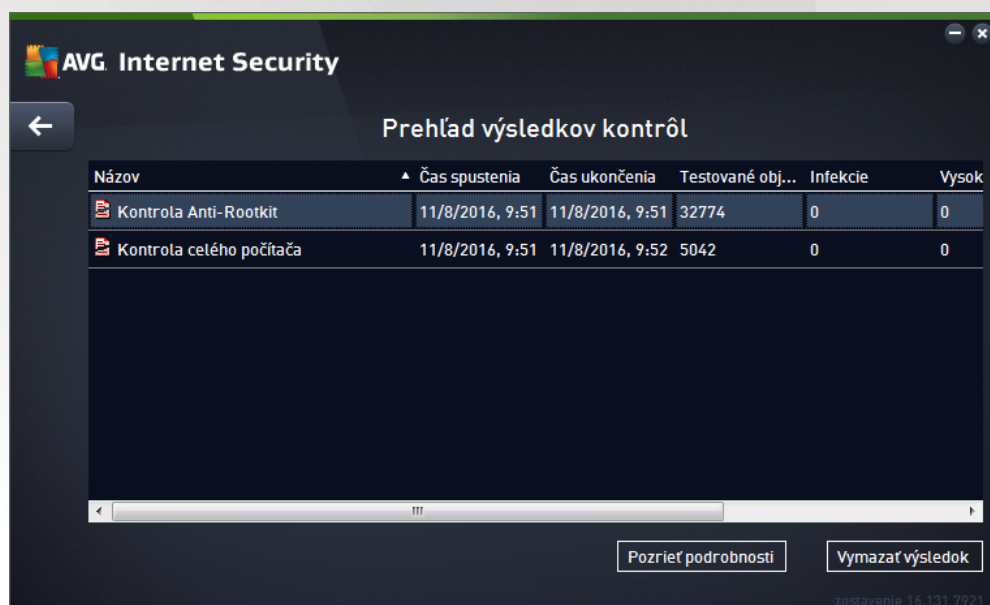


3.10. História

as **História** obsahuje informácie o všetkých udalostiach v minulosti (ako napríklad aktualizácie, kontroly, detekcie a pod.) a správy o týchto udalostiach. K tejto asťi sa dostanete z [hlavného používateľského rozhrania](#) prostredníctvom položky **Možnosti/História**. História všetkých zaznamenaných udalostí je rozdelená do nasledujúcich asťí:

- [Výsledky kontrol](#)
- [Nálezy sú asťi Rezydentný štít](#)
- [Nálezy sú asťi Ochrana e-mailu](#)
- [Nálezy sú asťi Webový štít](#)
- [História udalostí](#)
- [Protokol sú asťi Firewall](#)

3.10.1. Výsledky kontrol




Dialógové okno **Prehľad výsledkov kontrol** je prístupné prostredníctvom ponuky **Možnosti/História/Výsledky kontrol** v hornom navigačnom pruhu hlavného okna **AVG Internet Security**. 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 s označením výsledku 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 plná, alebo rozdelená na polovicu – plné ikony predstavujú dokončené a správne ukončené kontroly, ikony rozdelené na polovicu predstavujú 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** – v týchto stupňoch sa uvádza číslo odstránených/celkových infekcií nájdených pre každú z úrovní závažnosti (vysokú a strednú)
- **Info** – informácie súvisiace s priebehom a výsledkami kontroly (*obvyčajne s jej 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 výsledok** – stlačením tohto tlačidla sa zvolená položka odstráni z prehľadu výsledkov kontroly
-  – ak si želáte prepnúť späť na predvolené [hlavné dialógové okno AVG](#) (*prehľad súčasti*), použijete šípku v ľavom hornom rohu tohto dialógového okna

3.10.2. Nálezy súčasti Rezidentný štít

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

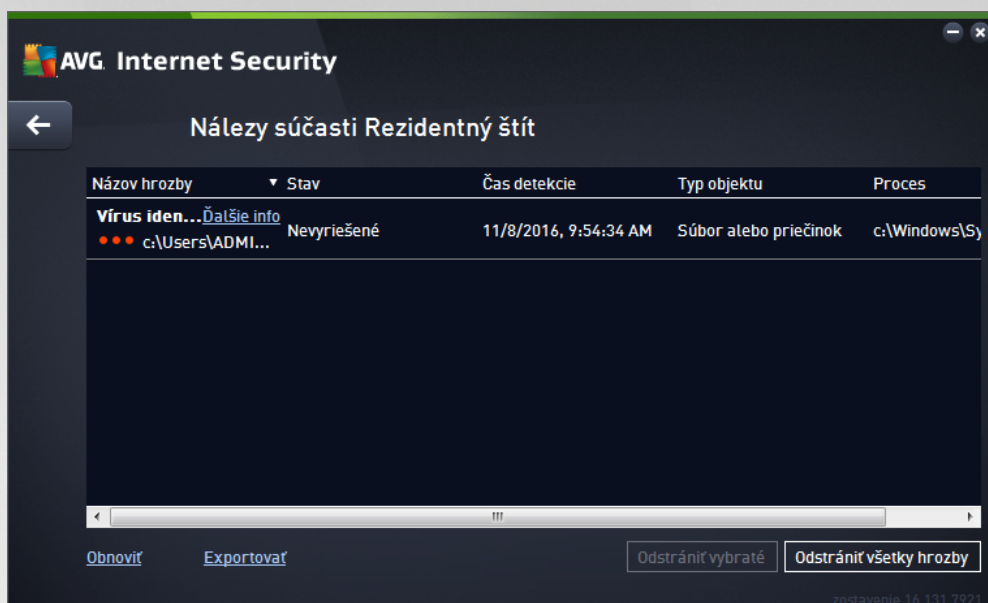


V tomto dialógovom okne s upozornením sa nachádzajú informácie o zistenom objekte, ktorý sa považuje za infikovaný (*Hrozba*), a kratší popis rozpoznanej infekcie (*Popis*). Odkaz *Viac informácií* vás presmeruje na stránku v [online vírusovej encyklopédii](#), uvádzajúcu podrobné informácie o zistenej hrozbe, ak sú tieto 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 vírus detegovaný objektom prejde 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 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 produktu AVG Internet Security](#). Toto dialógové okno obsahuje prehľad objektov detegovaných súčastou Rezidentný štít vyhodnotených ako nebezpečné, ktoré boli buď vyčistené, alebo premiestnené do [Vírusového trezora](#).



Pre každý detegovaný objekt sa zobrazia tieto informácie:

- **Názov hrozby** – popis (prípadne aj názov) zisteného objektu a jeho umiestnenie. Odkaz *Viac informácií* vás presmeruje na stránku v [online vírusovej encyklopédii](#) uvádzajúcu podrobné informácie o zistenej hrozbe.
- **Stav** – akcia vykonaná s detegovaným objektom
- **čas detekcie** – dátum a čas detegovania a zablokovania hrozby
- **Typ objektu** – typ detegovaného objektu.
- **Proces** – aká akcia sa vykonala na zavolaní potenciálne nebezpečného objektu, aby sa mohol detegovať

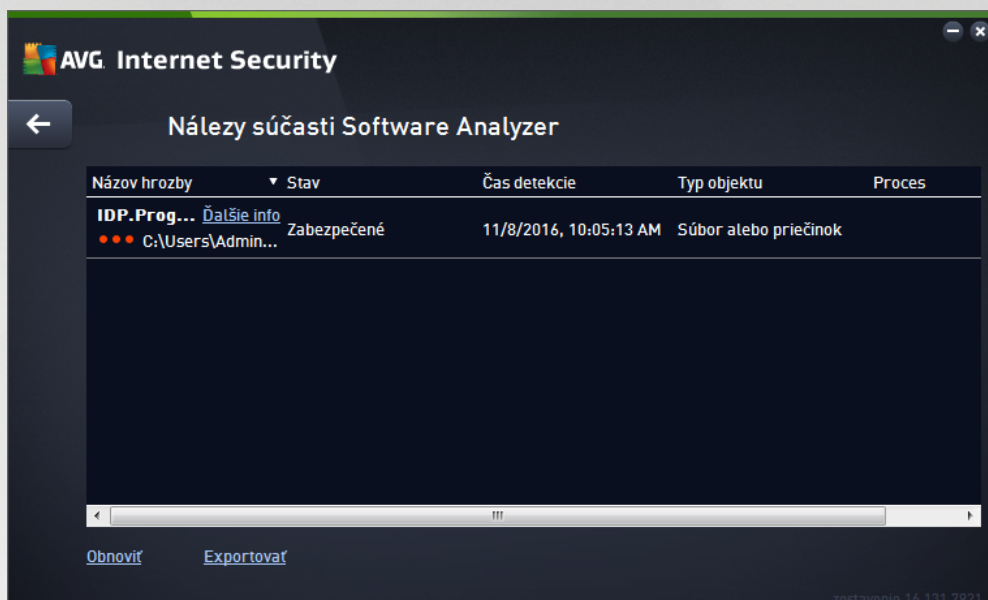
Ovládacie tlačidlá

- **Obnoviť** – aktualizuje sa zoznam nálezov zistených **Webovým štítom**
- **Exportovať** – exportuje celý zoznam zistených objektov do súboru
- **Odstrániť vybrané** – v zozname môžete označiť iba vybrané záznamy a týmto tlačidlom ich vymažete
- **Odstrániť všetky hrozby** – týmto tlačidlom vymažete všetky záznamy v tomto dialógovom okne
- **←** – ak si želáte prepnúť naspäť na predvolené [hlavné dialógové okno AVG](#) (prehľad súčastí), použijete šípku v ľavom hornom rohu tohto dialógového okna



3.10.3. Nálezy súčasti Identity Protection

Dialógové okno **Nálezy súčasti Software Analyzer** je dostupné prostredníctvom ponuky **Možnosti /História/ Nálezy súčasti Software Analyzer** v hornom navigačnom pruhu hlavného okna **AVG Internet Security**.



Toto dialógové okno obsahuje zoznam všetkých nálezov detegovaných súčastí **Software Analyzer**. Pre každý detegovaný objekt sa zobrazia tieto informácie:

- **Názov hrozby** – popis (prípadne aj názov) zisteného objektu a jeho umiestnenie. Odkaz *Viac informácií* vás presmeruje na stránku v [online vírusovej encyklopédii](#) uvádzajúcu podrobné informácie o zistenej hrozbe.
- **Stav** – akcia vykonaná s detegovaným objektom
- **čas detekcie** – dátum a čas detegovania a zablokovania hrozby
- **Typ objektu** – typ detegovaného objektu
- **Proces** – aká akcia sa vykonala na vyvolanie potenciálne nebezpečného objektu, aby sa mohol detegovať

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

Ovládacie tlačidlá

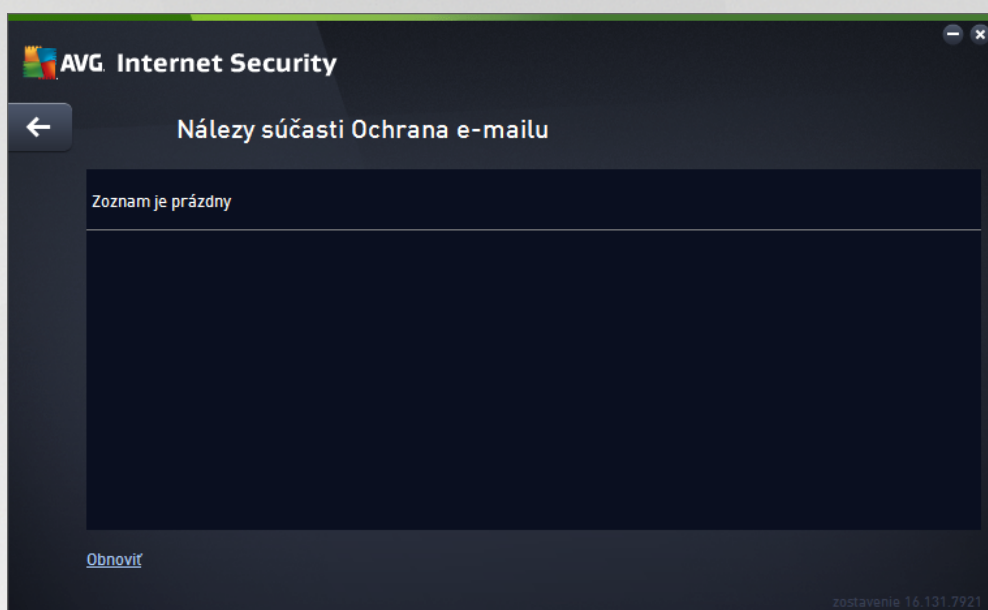
V rozhraní **Nálezov súčasti Software Analyzer** sa nachádzajú tieto ovládacie tlačidlá:

- **Obnoviť zoznam** – aktualizuje zoznam detegovaných hrozieb
- **←** – ak si želáte prepnúť naspäť na predvolené [hlavné dialógové okno AVG](#) (prehľad súčastí), použijete šípku v ľavom hornom rohu tohto dialógového okna



3.10.4. 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 produktu **AVG Internet Security**.



Toto dialógové okno obsahuje zoznam všetkých nálezov detegovaných súčasti **Kontrola pošty**. Pre každý detegovaný objekt sa zobrazia tieto informácie:

- **Názov detekcie** – popis (prípadne aj názov) detegovaného objektu a jeho zdroj
- **Výsledok** – akcia vykonaná na detegovanom objekte
- **čas detekcie** – dátum a čas detekcie podozrivého objektu
- **Typ objektu** – typ detegovaného objektu
- **Proces** – aká akcia sa vykonala na vyvolanie potenciálne nebezpečného objektu, aby sa mohol 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

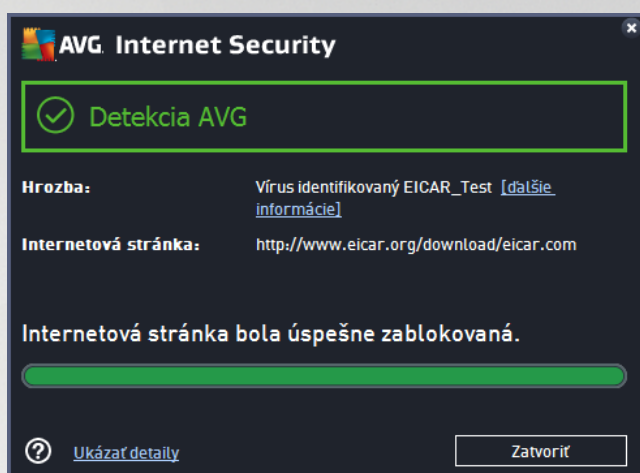
V rozhraní **Nálezy súčasti Kontrola pošty** sa nachádzajú nasledujúce tlačidlá:

- **Obnoviť zoznam** – aktualizuje zoznam detegovaných hrozieb
- **←** – ak si želáte prepnúť naspäť na predvolené **hlavné dialógové okno AVG** (prehľad súčasti), použijete šípku v ľavom hornom rohu tohto dialógového okna



3.10.5. Nálezy súčasti Webový štít

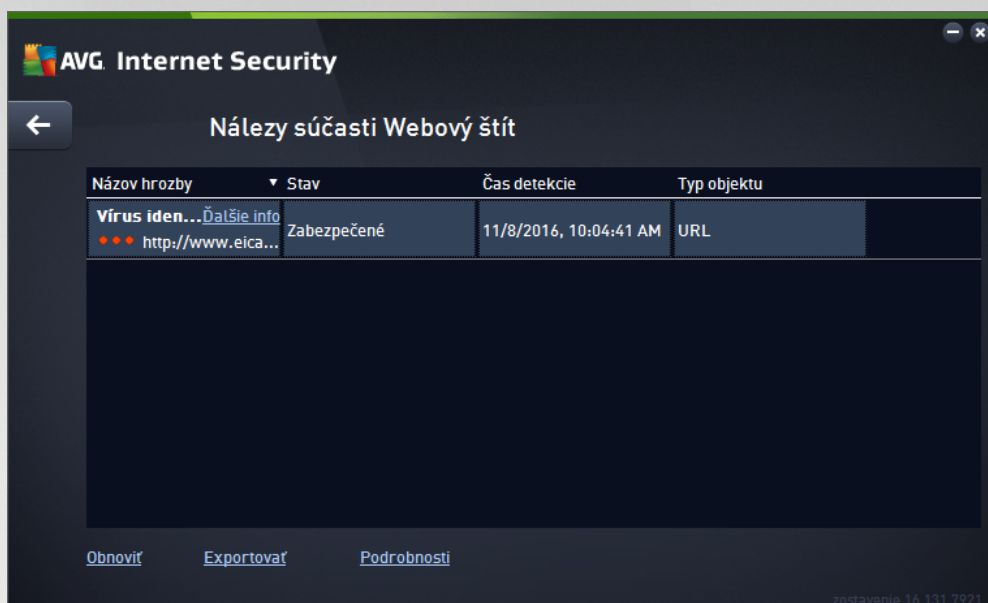
Webový štít kontroluje obsah navštívených internetových stránok a súborov, ktoré sa na nich môžu nachádzať, ešte predtým, než sa zobrazia v internetovom prehliadači alebo stiahnu do počítača. Pri detegovaní hrozby vás program ihneď upozorní otvorením tohto dialógového okna:



V tomto dialógovom okne s upozomením sa nachádzajú informácie o zistenom objekte, ktorý sa považuje za infikovaný (*Hrozba*), a kratší popis rozpoznanej infekcie (*Názov objektu*). Odkaz *Viac informácií* vás presmeruje na [online vírusovú encyklopédiu](http://www.eicar.org/download/eicar.com), 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 varovaním.

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



Pre každý detegovaný objekt sa zobrazia tieto informácie:

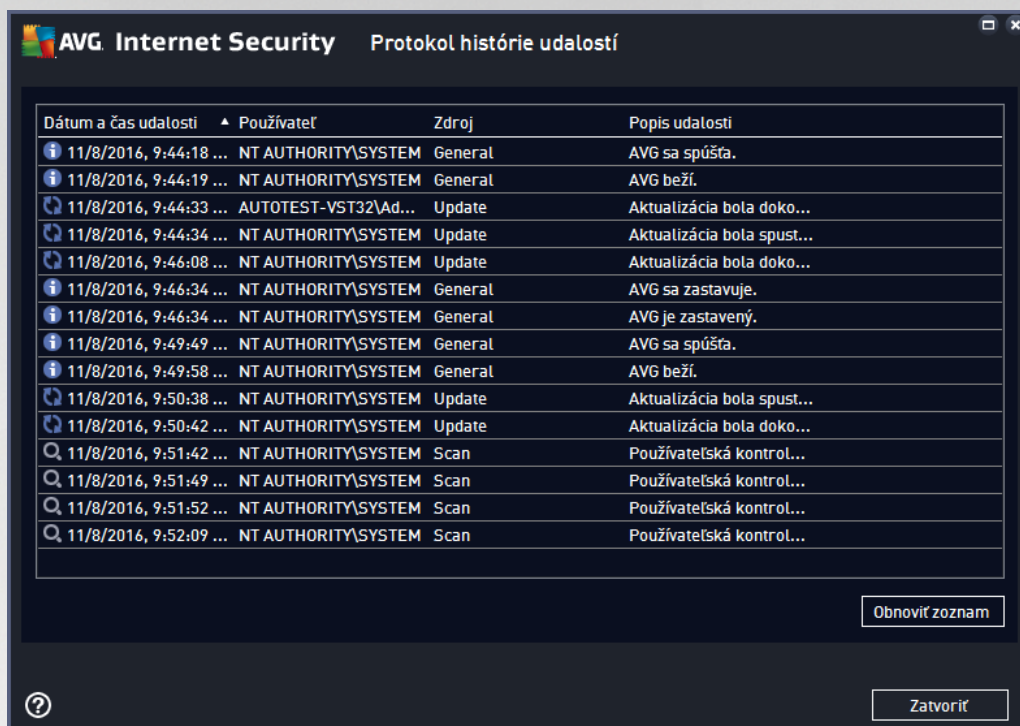
- **Názov hrozby** – popis (prípadne aj názov) zisteného objektu a jeho zdroj (webová stránka). Odkaz *Viac informácií* vás presmeruje na stránku v [online vírusovej encyklopédii](#), uvádzajúcu podrobné informácie o zistenej hrozbe.
- **Stav** – akcia vykonaná s detegovaným objektom
- **čas detekcie** – dátum a čas detegovania a zablokovania hrozby
- **Typ objektu** – typ detegovaného objektu.

Ovládacie tlačidlá

- **Obnovi** – aktualizuje sa zoznam nálezov zistených **Webovým štítom**.
- **Exportova** – exportuje celý zoznam zistených objektov do súboru.
- – ak si želáte prepnúť naspäť na predvolené [hlavné dialógové okno AVG](#) (prehľad súčastí), použijete šípku v ľavom hornom rohu tohto dialógového okna



3.10.6. Protokol histórie udalostí



Dialógové okno **História udalostí** sa nachádza v ponuke **Možnosti/História/História udalostí** v hornom navigačnom pruhu hlavného okna programu **AVG Internet Security**. V tejto časti nájdete zhrnutie významných udalostí, ktoré sa vyskytli počas prevádzky programu **AVG Internet Security**. 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 (či už **Rezidentným štítom** alebo **kontrolou**) vrátane miesta výskytu; a ďalšie dôležité udalosti.

Každá udalosť má uvedené tieto informácie:

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

Ovládacie tlačidlá

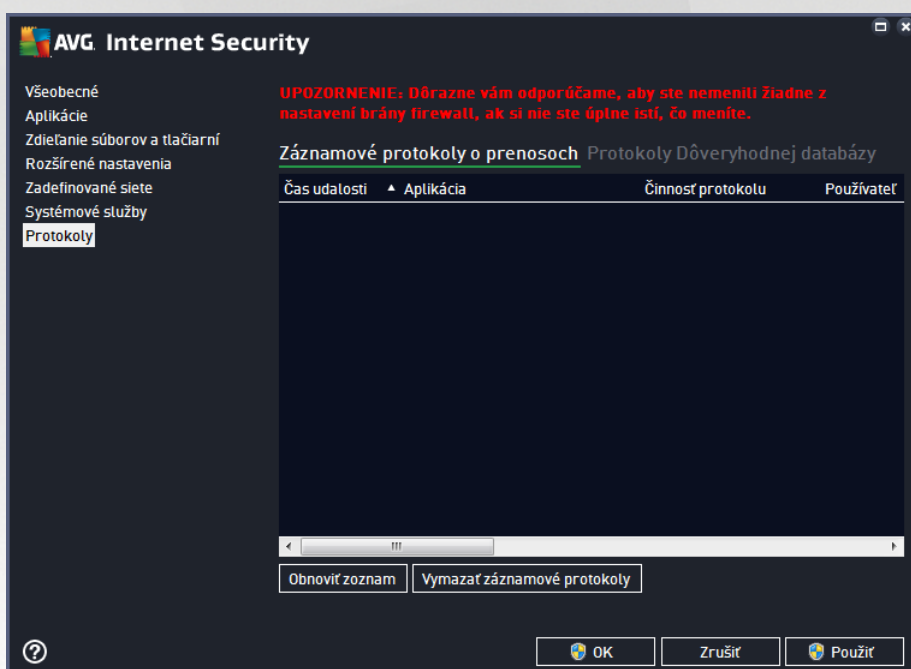
- **Obnoviť zoznam** – stlačením tohto tlačidla aktualizujete všetky položky v zozname udalostí.
- **Zatvoriť** – stlačením tohto tlačidla sa vrátite do hlavného okna **AVG Internet Security**.

3.10.7. Protokol súčasti Firewall

Toto dialógové okno je súčasťou expertných nastavení a odporúčame vám, aby ste si nezmenili žiadne nastavenia, ak si zmenou nie ste úplne istí!

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

- **Záznamové protokoly o prenosoch** – na tejto karte 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 zaprotokolovanej udalosti, mene používateľa, PID, smere prenosu, type protokolu, portoch vzdialených a miestnych a o miestnych a vzdialených adresách IP.



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

Ovládacie tlačidlá

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



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

Pravidelná aktualizácia 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.

V záujme maximálneho využitia dostupného zabezpečenia je **AVG Internet Security** predvolene nastavený tak, aby hľadal nové aktualizácie vírusovej databázy každé dve hodiny. Keďže sa aktualizácie AVG nezverejňujú pod a pevného harmonogramu, ale podľa potreby a závažnosti nových hrozieb, je táto kontrola veľmi dôležitá na zaistenie neustálej aktuálnosti vírusovej databázy AVG.

Ak chcete skontrolovať nové aktualizované súbory okamžite, môžete tak urobiť pomocou rýchleho odkazu [Aktualizovať teraz](#) v hlavnom používateľskom rozhraní. Tento odkaz sa nachádza v každom dialógovom okne [používateľského rozhrania](#). Keď spustíte aktualizáciu, AVG najskôr overí, či sú dostupné nové aktualizované súbory. Ak áno, **AVG Internet Security** ich začne sťahovať 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 a spúšťať a aktualizáciu aspoň raz denne!** Konfiguráciu môžete upraviť v sekcii [Rozšírené nastavenia/Plány](#), konkrétne v nasledovných dialógových oknách:

- [Plán aktualizácie definícií](#)
- [Plán aktualizácie Anti-Spamu](#)

3.12. Najčastejšie otázky a technická podpora

V prípade nákupných alebo technických problémov s aplikáciou **AVG Internet Security** 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 sekcii hlavného používateľského rozhrania*) obsahuje prepojenie **Podpora**, pomocou ktorého otvoríte nové dialógové okno so všetkými typmi údajov, ktoré môžete pri hľadaní pomoci potrebovať. Dialógové okno obsahuje základné údaje o nainštalovanom programe AVG (*verzia programu/databázy*), podrobnosti o 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** (*súbor pomocníka otvoríte stlačením klávesu F1 v niektorom z dialógových okien aplikácie*). V tejto sekcii nájdete zoznam najčastejších situácií,



v ktorých používate potrebuje vyh ada profesionálnu pomoc pre technický problém. Vyberte situáciu, ktorá najviac zodpovedá vášmu problému, a kliknutím zobrazte podrobné pokyny vedúce k riešeniu daného problému.

- **Webové stredisko podpory AVG** – riešenie problému môžete vyh ada aj na webovej lokalite AVG (<http://www.avg.com/>). V časti **Podpora** nájdete prehľad tematických skupín zaoberajúcich sa predajom aj technickými otázkami, štruktúrovanú časť otázo a všetky dostupné kontakty.
- **AVG ThreatLabs** – osobitná webová stránka spojená s programom AVG (<http://www.avgthreatlabs.com/website-safety-reports/>) venovaná problémom s vírusmi, ktorá poskytuje štruktúrovaný prehľad informácií súvisiacich s hrozbami on-line. Môžete tiež nájsť pokyny na odstránenie vírusov spyware a tipov na zachovanie ochrany.
- **Diskusné fórum** – môžete využiť aj diskusné fórum používateľov produktov AVG na adrese <http://community.avg.com/>.