AVG Internet Security 2012

Používateľská príručka

Revízia dokumentu 2012.20 (3/29/2012)

Obsah

1. Úvod

Táto príručka podrobne dokumentuje produkt **AVG Internet Security 2012**.

Produkt AVG Internet Security 2012 ponúka niekoľko vrstiev ochrany pre celú on-line činnosť, takže sa nemusíte obávať odcudzenia identity, vírusov ani otvorenia škodlivých lokalít. Súčasťou balíka sú AVG Protective Cloud Technology a AVG Community Protection Network, čo znamená, že zhromažďujeme informácie o najnovších hrozbách a zdieľame ich v rámci našej komunity, aby sme vám poskytli najlepšiu možnú ochranu:

- Bezpečne nakupujte on-line a používajte internetové bankovníctvo so súčasťami Firewall, Anti-Spam a AVG Identity Protection.
- Chráňte sa v sociálnych sieťach pomocou nástroja AVG Social Networking Protection.
- Surfujte a vyhľadávajte na internete s dôverou v ochranu v reálnom čase súčasťou LinkScanner.

2. Požiadavky na inštaláciu produktu AVG

2.1. Podporované operačné systémy

AVG Internet Security 2012 sa používa na ochranu počítačov s týmito operačnými systémami:

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

(a prípadne novšie balíky Service Pack pre konkrétne operačné systémy)

***Poznámka**: Súčasť ID Protection nepodporuje 64-bitové operačné systémy Windows XP. Produkt AVG Internet Security 2012 sa môže inštalovať pod týmto operačným systémom, ale bez súčasti IDP.*

2.2. Minimálne a odporúčané hardvérové požiadavky

Minimálne hardvérové požiadavky pre produkt **AVG Internet Security 2012**:

- Procesor Intel Pentium 1,5 GHz
- 512 MB pamäte RAM
- 1000 MB voľného miesta na pevnom disku (na účely inštalácie)

Odporúčané hardvérové požiadavky pre produkt **AVG Internet Security 2012**:

- Procesor Intel Pentium 1,8 GHz
- 512 MB pamäte RAM
- 1 550 MB voľného miesta na pevnom disku (na účely inštalácie)

3. Postup inštalácie produktu AVG

Kde získam inštalačný súbor?

Na nainštalovanie programu **AVG Internet Security 2012** do počítača sa musí použiť najnovší inštalačný súbor. Aby ste sa uistili, že inštalujete najnovšiu verziu aplikácie **AVG Internet Security 2012**, odporúčame vám prevziať inštalačný súbor priamo z webovej lokality spoločnosti AVG (http://www.avg.com/). V časti ***Centrum podpory/Na prevzatie*** sa nachádza štruktúrovaný prehľad inštalačných súborov pre každú z edícií AVG.

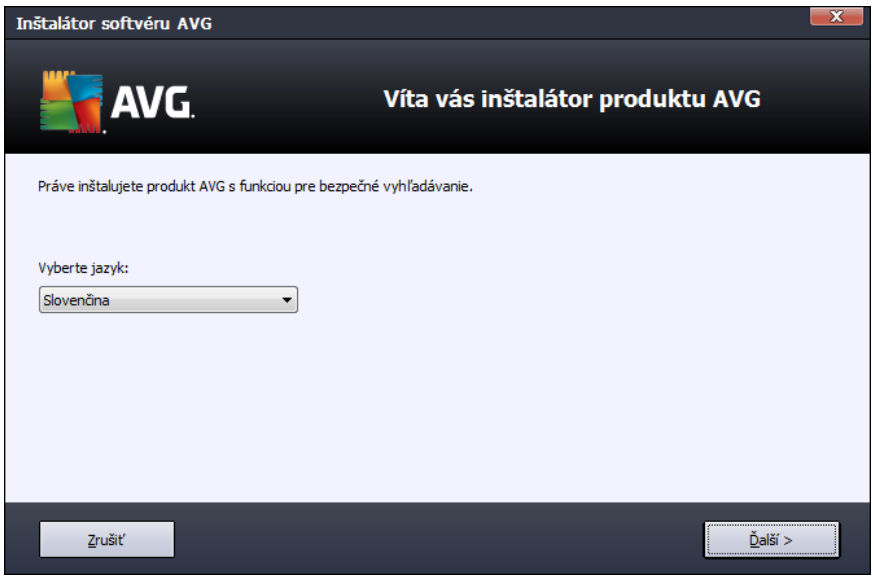
Ak neviete, ktoré súbory treba nainštalovať, môžete využiť službu ***Vybrať produkt*** v spodnej časti webovej lokality. Odpoviete na tri jednoduché otázky a služba vyberie súbory presne podľa vašich potrieb. Stlačením tlačidla ***Pokračovať*** budete presmerovaní na úplný zoznam súborov na prevzatie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

Ako vyzerá postup inštalácie?

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

3.1. Vitajte! Výber jazyka

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



V tomto dialógovom okne zvolíte jazyk, ktorý sa použije pri inštalácii. V pravom rohu dialógového okna kliknite na rozbaľovací zoznam. Rozvinie sa ponuka jazykov. Vyberte požadovaný jazyk a inštalácia sa posunie k výberu jazyka.

Pozor: Teraz vyberáte iba jazyk postupu inštalácie. Aplikácia AVG Internet Security 2012 sa nainštaluje vo zvolenom jazyku a v angličtine, v ktorej sa vždy inštaluje automaticky. Vždy je však možné nainštalovať viac jazykov a pracovať s aplikáciou AVG Internet Security 2012 v ktoromkoľvek z nich. V jednom z nasledujúcich dialógových okien Vlastné možnosti dostanete možnosť potvrdiť výber alternatívnych jazykov.

3.2. Vitajte! Licenčná zmluva

V ďalšom kroku dialógové okno ***Víta vás sprievodca inštaláciou AVG*** ponúkne úplné znenie licenčnej zmluvy AVG:

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

Zásady spoločnosti AVG týkajúce sa ochrany súkromia

Okrem licenčnej zmluvy sa v tomto dialógovom okne môžete podrobnejšie zoznámiť so zásadami spoločnosti AVG týkajúcimi sa ochrany súkromia. V ľavom dolnom rohu dialógového okna sa nachádza prepojenie ***Zásady spoločnosti AVG týkajúce sa ochrany súkromia***. Po kliknutí na uvedené prepojenie sa dostanete na webovú lokalitu spoločnosti AVG (http://www.avg.com/), kde nájdete celý text zásad spoločnosti AVG Technologies týkajúcich sa ochrany súkromia.

Ovládacie tlačidlá

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

- ***Verzia pre tlač*** – Kliknutím vytlačíte plné znenie licenčnej zmluvy AVG.

- ***Zamietnuť*** – Kliknutím na toto tlačidlo odmietnete podmienky licenčnej zmluvy. Inštalačný postup sa okamžite ukončí. Aplikácia **AVG Internet Security 2012** sa nenainštaluje!
- ***Späť*** – Kliknutím sa vrátite o jeden krok k predchádzajúcemu dialógovému oknu inštalácie.
- ***Prijať*** – Kliknutím na toto tlačidlo potvrdíte, že ste prečítali, pochopili a prijali podmienky licenčnej zmluvy. Inštalácia bude pokračovať a zobrazí sa ďalšie inštalačné dialógové okno.

3.3. Aktivujte si licenciu

V dialógovom okne ***Aktivovanie licencie*** zadajte licenčné číslo do príslušného textového poľa:

Kde nájsť licenčné číslo

Predajné číslo sa nachádza na obale disku CD v škatuli produktu **AVG Internet Security 2012**. Licenčné číslo sa nachádza v e-mailovej správe s potvrdením, ktorú ste dostali po zakúpení produktu **AVG Internet Security 2012** online. Číslo sa musí zadať presne tak, ako je uvedené. Ak máte k dispozícii licenčné číslo v digitálnej podobe (*v e-mailovej správe*), na jeho vloženie vám odporúčame použiť funkciu kopírovať a prilepiť.

Ako používať metódu Kopírovať a Prilepiť

Pomocou metódy ***Kopírovať a Prilepiť*** vložte licenčné číslo produktu **AVG Internet Security 2012** do programu. Tak zabezpečíte zadanie správneho čísla. Postupujte podľa nasledujúcich pokynov:

- Otvorte e-mail s licenčným číslom.
- Kliknite ľavým tlačidlom myši na začiatok licenčného čísla, podržte tlačidlo stlačené a presuňte kurzor myši na koniec čísla. Potom tlačidlo uvoľnite. Číslo by sa malo zvýrazniť.

- Stlačte a podržte kláves ***Ctrl*** a stlačte kláves ***C***. Tým číslo skopírujete.
- Nasmerujte kurzor a kliknite na miesto, kam chcete skopírované číslo vložiť.
- Stlačte a podržte kláves ***Ctrl*** a stlačte kláves ***V***. Tým prilepíte číslo na vybrané miesto.

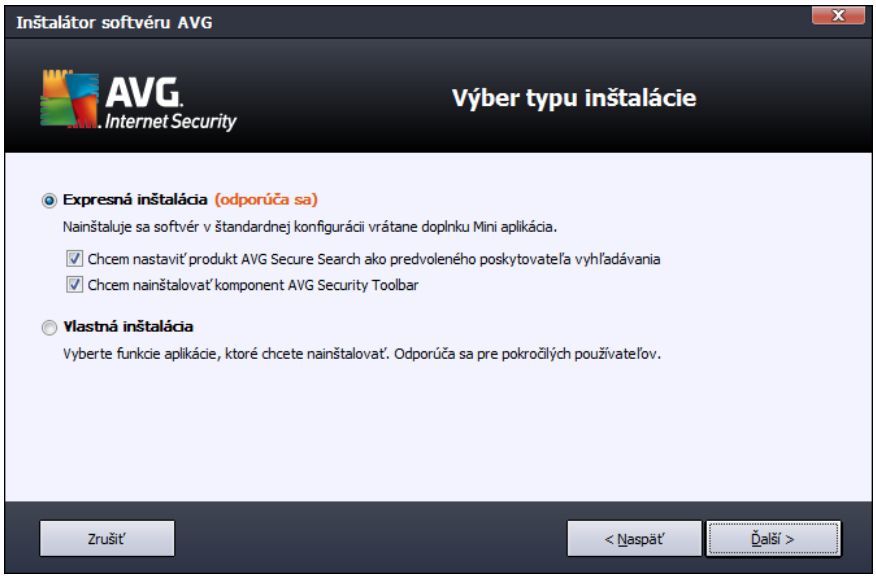
Ovládacie tlačidlá

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

- ***Zrušiť*** – Kliknutím okamžite ukončíte priebeh inštalácie. Aplikácia **AVG Internet Security 2012** sa nenainštaluje!
- ***Späť*** – Kliknutím sa vrátite o jeden krok k predchádzajúcemu dialógovému oknu inštalácie.
- ***Ďalej*** – Kliknutím posuniete priebeh inštalácie o krok ďalej.

3.4. Výber typu inštalácie

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



Expresná inštalácia

Väčšine používateľov odporúčame ponechať štandardnú ***expresnú*** inštaláciu, ktorá nainštaluje produkt **AVG Internet Security 2012** v úplne automatickom režime s nastaveniami vopred definovanými dodávateľom programu vrátane miniaplikácie AVG. Táto konfigurácia poskytuje maximálne zabezpečenie s optimálnym využitím zdrojov. Ak v budúcnosti budete chcieť zmeniť

konfiguráciu, vždy to bude možné priamo v aplikácii **AVG Internet Security 2012**.

Pri tejto možnosti sa nachádzajú dve označené políčka a dôrazne odporúčame, aby ste ich obe nechali označené:

- ***Chcem nastaviť produkt AVG Secure Search ako môj predvolený vyhľadávač*** – ponechaním tejto možnosti potvrdzujete, že chcete používať nástroj AVG Secure Search, ktorý úzko spolupracuje s komponentom Link Scanner a poskytuje vám tak maximálnu online
- ***Chcem nainštalovať panel nástrojov zabezpečenia AVG*** – určite si nainštalujte panel nástrojov zabezpečenia AVG, ktorý vás maximálne chráni pri surfovaní.

Stlačením tlačidla ***Ďalej*** prejdete k dialógovému oknu Inštalácia panelu nástrojov zabezpečenia AVG .

Vlastná inštalácia

Vlastnú inštaláciu by mali používať len skúsení používatelia, ktorí majú skutočný dôvod inštalovať produkt **AVG Internet Security 2012** s neštandardnými nastaveniami, napr. na účely prispôsobenia konkrétnym systémovým potrebám.

Ak sa rozhodnete pre túto možnosť, v dialógovom okne sa zobrazí nová časť s názvom ***Cieľový priečinok***. Tu môžete zadať umiestnenie, kam sa produkt **AVG Internet Security 2012** má nainštalovať. Produkt **AVG Internet Security 2012** sa štandardne inštaluje do priečinka Program Files na disku C:, ako je to uvedené v textovom poli dialógového okna. Ak si želáte zmeniť toto miesto, tlačidlom ***Prehľadávať*** otvorte prehľad diskových jednotiek a vyberte príslušný priečinok. Na obnovenie predvoleného umiestnenia nastaveného dodávateľom softvéru použite tlačidlo ***Predvolené***.

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

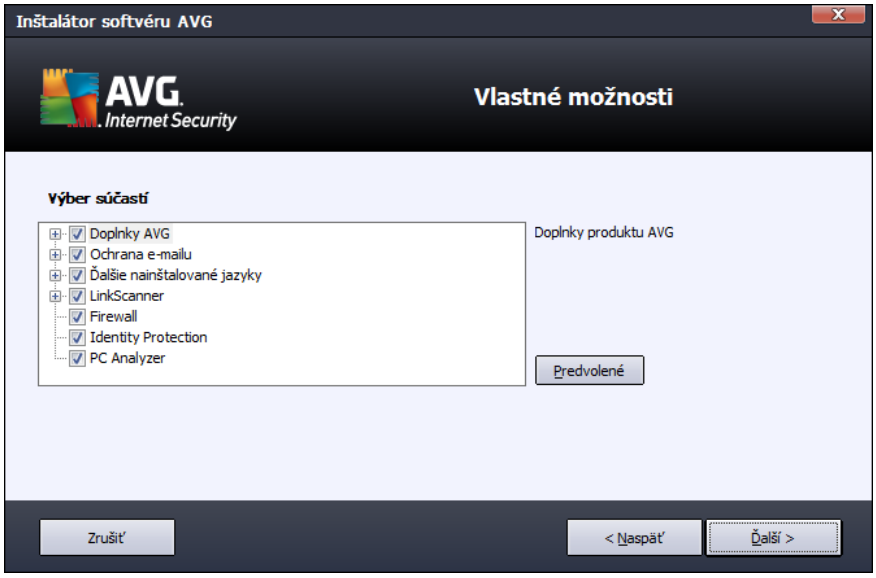
Ovládacie tlačidlá

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

- ***Zrušiť*** – Kliknutím okamžite ukončíte priebeh inštalácie. Aplikácia **AVG Internet Security 2012** sa nenainštaluje!
- ***Späť*** – Kliknutím sa vrátite o jeden krok k predchádzajúcemu dialógovému oknu inštalácie.
- ***Ďalej*** – Kliknutím posuniete priebeh inštalácie o krok ďalej.

3.5. Vlastné možnosti

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



V časti ***Výber súčastí*** sa nachádza prehľad všetkých súčastí programu **AVG Internet Security 2012**, ktoré je možné inštalovať. Ak vám predvolené nastavenia nevyhovujú, môžete odstrániť alebo pridať konkrétne súčasti.

Môžete však vybrať len tie súčasti, ktoré sú súčasťou edície AVG, ktorú ste si zakúpili!

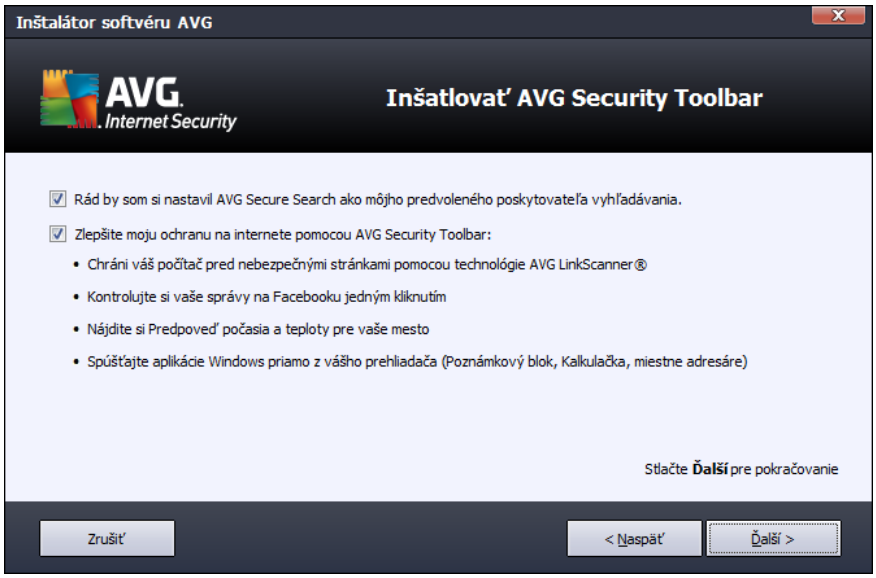
Zvýraznite položku v zozname ***Výber súčastí*** a na pravej strane v tejto časti sa zobrazia stručné informácie o príslušnej súčasti. Ďalšie informácie o funkcionalite jednotlivých súčastí sa nachádzajú v kapitole Prehľad súčastí v tejto dokumentácii. Na obnovenie predvolenej konfigurácie nastavenej dodávateľom softvéru použite tlačidlo ***Predvolené***.

Ovládacie tlačidlá

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

- ***Zrušiť*** – Kliknutím okamžite ukončíte priebeh inštalácie. Aplikácia **AVG Internet Security 2012** sa nenainštaluje!
- ***Späť*** – Kliknutím sa vrátite o jeden krok k predchádzajúcemu dialógovému oknu inštalácie.
- ***Ďalej*** – Kliknutím posuniete priebeh inštalácie o krok ďalej.

3.6. Inštalácia panela AVG Security Toolbar



V dialógovom okne ***Inštalácia súčasti AVG Security Toolbar*** nastavte, či sa má nainštalovať súčasť AVG Security Toolbar. Ak nezmeníte predvolené nastavenia, táto súčasť sa nainštaluje automaticky do internetového prehliadača (*v súčasnosti sú podporované prehliadače Microsoft Internet Explorer v. 6.0 a novšia a Mozilla Firefox v. 3.0 a novšia*) a postará sa o komplexnú ochranu počas surfovania na internete.

Zároveň môžete rozhodnúť, či sa má služba *AVG Secure Search (powered by Google)* nastaviť ako predvolený vyhľadávač. Ak ju chcete nastaviť ako predvolenú, nechajte príslušné začiarkovacie okienko označené.

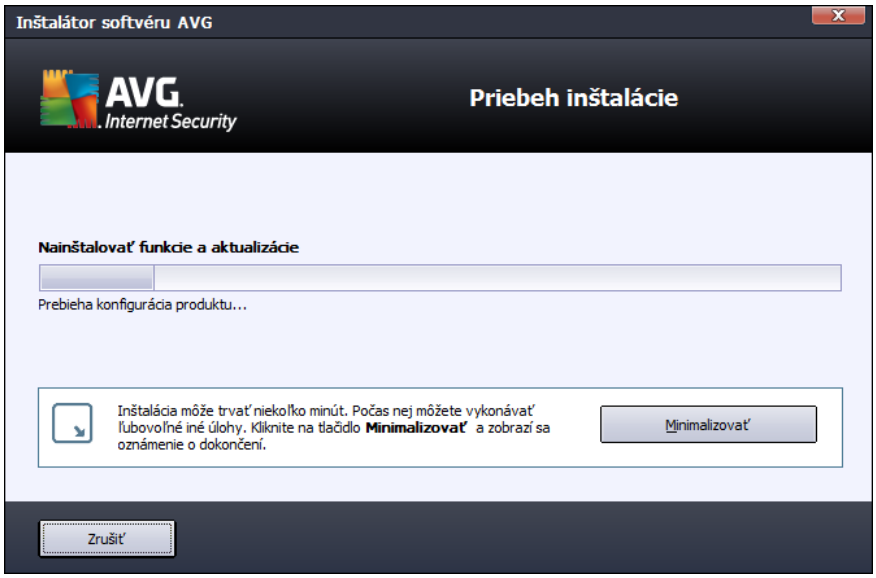
Ovládacie tlačidlá

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

- ***Zrušiť*** – Kliknutím okamžite ukončíte priebeh inštalácie. Aplikácia **AVG Internet Security 2012** sa nenainštaluje!
- ***Späť*** – Kliknutím sa vrátite o jeden krok k predchádzajúcemu dialógovému oknu inštalácie.
- ***Ďalej*** – Kliknutím posuniete priebeh inštalácie o krok ďalej.

3.7. Priebeh inštalácie

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



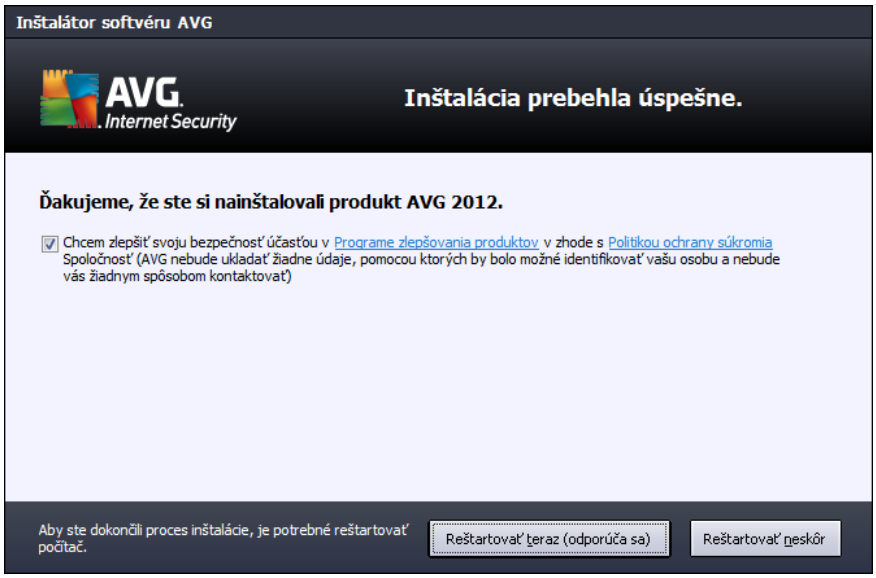
Po dokončení inštalácie sa automaticky otvorí ďalšie dialógové okno.

Ovládacie tlačidlá

V tomto dialógovom okne je dostupné len jedno ovládacie tlačidlo – ***Zrušiť***. Toto tlačidlo použite iba vtedy, keď chcete zastaviť postup inštalácie. Nezabudnite, že v takom prípade sa aplikácia **AVG Internet Security 2012** nenainštaluje!

3.8. Inštalácia prebehla úspešne

Dialógové okno ***Inštalácia prebehla úspešne*** potvrdí, že sa program **AVG Internet Security 2012** celý nainštaloval a nastavil:



Program zlepšovania produktov

Tu sa môžete rozhodnúť, či sa chcete podieľať na programe zlepšovania produktov (*podrobnosti nájdete v kapitole Rozšírenie nastavenia programu AVG/Program zlepšovania produktov*), ktorý zbiera anonymné informácie o zistených hrozbách s cieľom zvýšiť celkovú bezpečnosť na internete. Ak s tým súhlasíte, nechajte označenú možnosť ***Súhlasím s účasťou v programe webovej bezpečnosti aplikácie AVG 2012 a programe zlepšovania produktov ...*** *(možnosť je štandardne označená)*.

Reštartovanie počítača

Na dokončenie inštalácie je potrebné reštartovať počítač: rozhodnite, či chcete ***reštartovať teraz*** alebo neskôr – ***Reštartovať neskôr***.

4. Po inštalácii

4.1. Registrácia produktu

Po nainštalovaní produktu **AVG Internet Security 2012** zaregistrujte produkt on-line na webovej lokalite AVG (http://www.avg.com/). Registráciou získate úplný prístup k používateľskému účtu AVG, informáciám o aktualizáciách AVG a ďalším službám poskytovaným výhradne registrovaným používateľom.

Najjednoduchší spôsob registrácie je priamo z používateľského rozhrania aplikácie **AVG Internet Security 2012**. V hlavnej ponuke vyberte položku Pomocník/Registrovať. Budete presmerovaní na stránku ***Registrácia*** na webovej lokalite AVG (http://www.avg.com/). Postupujte podľa pokynov na tejto stránke.

4.2. Otvorenie používateľského rozhrania

Hlavné dialógové okno AVG sa otvára niekoľkými spôsobmi:

- Dvakrát kliknite na ikonu AVG na paneli úloh
- Dvakrát kliknite na ikonu AVG na pracovnej ploche.
- v ponuke ***Štart/Všetky programy/AVG 2012***

4.3. Kontrola celého počítača

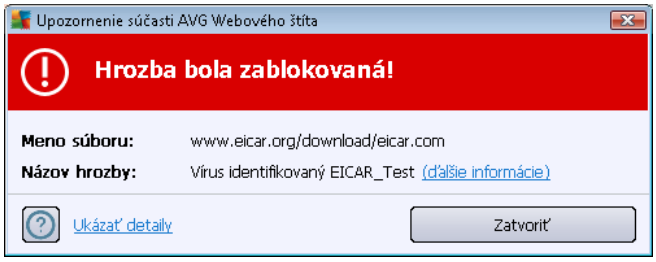
Existuje potenciálne riziko, že sa do vášho počítača dostal počítačový vírus ešte pred nainštalovaním produktu **AVG Internet Security 2012**. Z tohto dôvodu by ste mali spustiť Kontrolu celého počítača, aby sa vylúčila možnosť existencie infekcie v počítači. Prvá kontrola môže istý čas trvať *(približne hodinu)*, no odporúča sa ju nechať dokončiť, aby ste sa uistili že váš počítač nie je v ohrození. Pokyny na spustenie Kontroly celého počítača sa nachádzajú v kapitole Kontrola programom AVG.

4.4. Test EICAR

Na kontrolu, či sa program **AVG Internet Security 2012** nainštaloval správne, môžete použiť test EICAR.

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

Prevezmite si súbor ***eicar.com*** a uložte ho na pevný disk počítača. Okamžite po potvrdení prevzatia testovacieho súboru nástroj Online Shield (*časť súčasti LinkScanner*) reaguje upozornením. Zobrazenie tohto oznámenia znamená, že je program AVG správne nainštalovaný v počítači.



Na internetových stránkach http://www.eicar.com si môžete prevziať aj komprimovanú verziu „vírusu“ EICAR (*napr. s názvom eicar_com.zip*). Nástroj Online Shield umožní prevziať tento súbor a uložiť ho na pevný disk počítača, ale súčasť Resident Shield (*v rámci súčasti Anti-Virus*) zistí „vírus“ pri jeho rozbaľovaní.

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

4.5. Predvolená konfigurácia AVG

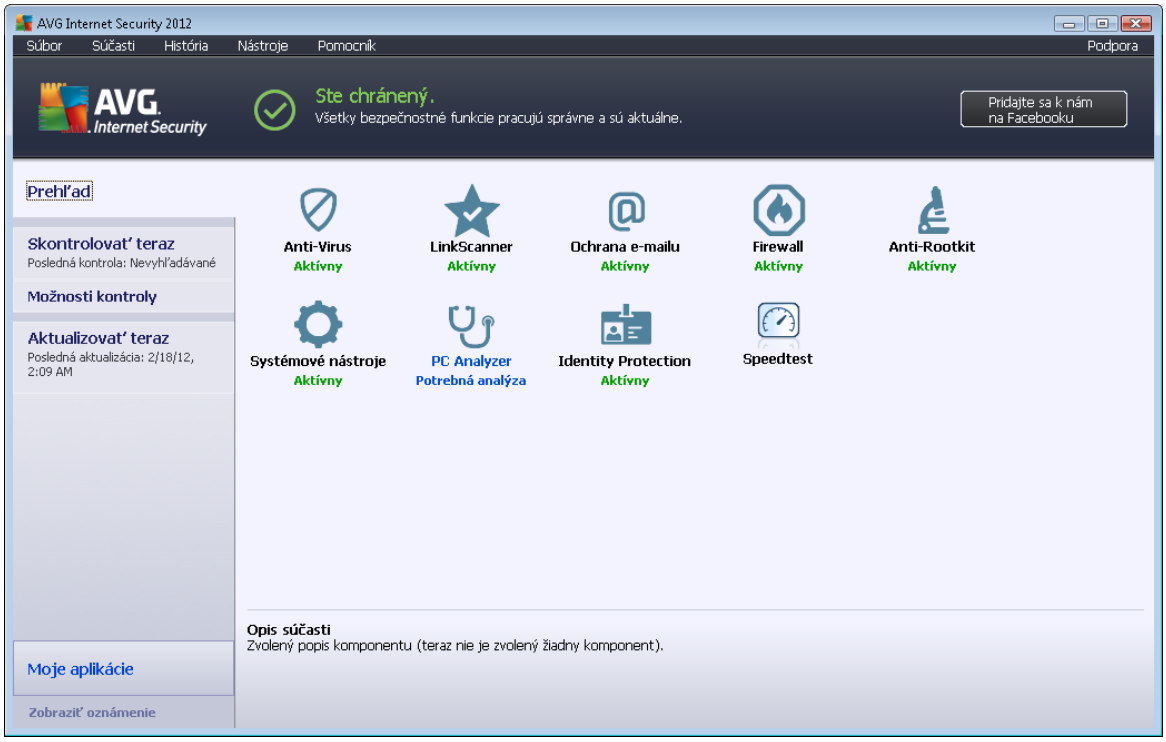
Predvolenú konfiguráciu (*t. j. nastavenie aplikácie bezprostredne po inštalácii*) produktu **AVG Internet Security 2012** nastavil dodávateľ softvéru tak, aby všetky súčasti a funkcie fungovali optimálnym spôsobom.

Nemeňte konfiguráciu AVG, ak na to nemáte vážny dôvod! Zmenu nastavení odporúčame robiť len skúseným používateľom.

Niektoré menšie zmeny nastavenia súčastí AVG je možné robiť priamo v používateľskom rozhraní konkrétnych súčastí. Ak máte pocit, že viete upraviť konfiguráciu programu AVG podľa svojich potrieb, prejdite do časti Rozšírené nastavenia programu AVG: vyberte položku systémovej ponuky ***Nástroje/Rozšírené nastavenia*** a upravte konfiguráciu v novootvorenom dialógovom okne Rozšírené nastavenia programu AVG.

5. Používateľské rozhranie AVG

AVG Internet Security 2012 sa otvára v hlavnom okne:



Hlavné okno je rozdelené na niekoľko častí:

- ***Systémová ponuka*** *(horný riadok v okne)* je štandardná štruktúrovaná ponuka, ktorá umožňuje prístup ku všetkým súčastiam, službám a funkciám produktu **AVG Internet Security 2012** – podrobnosti >>
- ***Informácie o stave zabezpečenia*** *(horná časť okna)* informuje o momentálnom stave nainštalovaného produktu **AVG Internet Security 2012** – podrobnosti >>
- ***Pridajte si nás na sieti Facebook*** *(časť okna vpravo hore) tlačidlom* sa môžete pridať do Komunity AVG na sieti Facebook. Tlačidlo sa však zobrazí iba vtedy, ak sú všetky komponenty plne funkčné a fungujú správne *(podrobnosti o stavoch komponentov AVG nájdete v kapitole Informácie o stave zabezpečenia)*
- ***Rýchle odkazy*** *(ľavá časť okna)* umožňuje rýchly prístup k najdôležitejším a najčastejšie používaným úlohám produktu **AVG Internet Security 2012** – podrobnosti >>
- ***Moje aplikácie*** *(ľavá dolná časť okna)* otvorí prehľad ďalších dostupných aplikácií **AVG Internet Security 2012**: LiveKive, Family Safety a PC Tuneup
- ***Prehľad súčastí*** *(stredná časť okna)* poskytuje prehľad všetkých nainštalovaných súčastí v produkte **AVG Internet Security 2012** – podrobnosti >>
- ***Ikona na paneli úloh*** *(pravý spodný roh monitora, na paneli úloh)* informuje o aktuálnom

stave produktu **AVG Internet Security 2012** – podrobnosti >>

- ***Mini-aplikácia AVG*** *(bočný panel systému Windows, v operačných systémoch Windows Vista/7)* umožňuje rýchly prístup ku kontrole a aktualizáciám produktu **AVG Internet Security 2012** – podrobnosti >>

5.1. Hlavná ponuka

Hlavná ponuka je štandardná ponuka, ktorá sa používa vo všetkých aplikáciách v operačnom systéme Windows. Je umiestnená horizontálne v hornej časti hlavného okna programu **AVG Internet Security 2012**. Hlavná ponuka sa používa na sprístupnenie konkrétnych súčastí, funkcií a služieb AVG.

Hlavná ponuka je rozdelená na päť hlavných častí:

5.1.1. Súbor

- ***Ukončiť***: Zatvorí používateľské rozhranie programu **AVG Internet Security 2012**. Aplikácia AVG sa však bude aj naďalej spúšťať na pozadí a počítač bude stále chránený!

5.1.2. Súčasti

Položka Súčasti v ponuke programu obsahuje odkazy na všetky nainštalované súčasti AVG, ktoré otvárajú hlavné dialógové okno v používateľskom rozhraní:

- ***Prehľad systému*** – používa sa na otvorenie hlavného používateľského rozhrania s prehľadom všetkých nainštalovaných súčastí a ich stavu
- ***Nástroj Anti-Virus*** odhaľuje v systéme vírusy, spyware, červy, trójske kone, nechcené spustiteľné súbory a knižnice a chráni pred škodlivými programami typu adware – podrobnosti >>
- ***Nástroj LinkScanner*** chráni pred útokmi na webe pri vyhľadávaní a surfovaní na internete – podrobnosti >>
- ***Nástroj Ochrana e-mailu*** kontroluje prichádzajúce e-mailové správy z hľadiska prítomnosti SPAMU a blokuje vírusy, phishingové útoky či iné hrozby – podrobnosti >>
- ***Nástroj Firewall*** kontroluje komunikáciu na všetkých sieťových portoch, chráni pred útokmi a blokuje každý pokus o prienik – podrobnosti >>
- ***Nástroj Anti-Rootkit*** hľadá nebezpečné programy rootkit ukryté v aplikáciách, ovládačoch alebo knižniciach – podrobnosti >>
- ***Systémové nástroje*** uvádza podrobný prehľad prostredia AVG a informácie o operačnom systéme – podrobnosti >>
- ***PC Analyzer*** poskytuje informácie o stave počítača – podrobnosti >>
- ***Nástroj Identity Protection*** nepretržite chráni digitálne aktíva pred novými a neznámymi hrozbami – podrobnosti >>

- ***Súčasť Remote Administration*** sa nachádza len v sieťových edíciách AVG Business Editions, a to len v prípade, ak ste ju nainštalovali počas inštalácie.

5.1.3. História

- Výsledky kontroly: Prepne sa testovacie rozhranie AVG, konkrétne na dialógové okno Prehľad výsledkov kontroly.

- Nálezy súčasti Rezidentný štít – Otvorí dialógové okno s prehľadom hrozieb detekovaných súčasťou Rezidentný štít

- Nálezy súčasti Kontrola pošty – Otvorí dialógové okno s prehľadom príloh e-mailových správ označených súčasťou Ochrana e-mailu ako nebezpečné.

- Nálezy súčasti Webový štít – otvorí sa dialógové okno s prehľadom hrozieb zistených súčasťou Webový štít v rámci súčasti LinkScanner.

- Vírusový trezor: Otvorí rozhranie úložiska karantény (Vírusový trezor), do ktorého AVG odstraňuje všetky zistené infekcie, ktoré sa z rôznych dôvodov nedajú automaticky vyliečiť. V tejto karanténe sú infikované súbory izolované, aby bolo možné garantovať bezpečnosť počítača. Infikované súbory sú zároveň uložené pre prípad, ak by sa dali v budúcnosti opraviť.

- Protokol histórie udalostí – otvára rozhranie protokolu histórie s prehľadom všetkých zaznamenaných činností aplikácie **AVG Internet Security 2012.**

- Protokol súčasti Firewall – otvára rozhranie s nastaveniami súčasti Firewall na karte Protokoly s podrobným prehľadom všetkých činností súčasti Firewall.

5.1.4. Nástroje

- Skontrolovať počítač – Spustí kontrolu celého počítača.

- Skontrolovať vybraný priečinok... – Otvorí rozhranie kontroly programom AVG a pomocou stromovej štruktúry počítača umožní definovať, ktoré súbory a priečinky sa majú kontrolovať.

- ***Skontrolovať súbor...*** – Umožní vám spustiť na požiadanie test konkrétneho súboru. Kliknutím na túto možnosť sa otvorí nové okno so stromovou štruktúrou disku. Vyberte požadovaný súbor a potvrďte spustenie kontroly.

- Aktualizácia – automaticky spustí aktualizácie produktu **AVG Internet Security 2012**.

- ***Aktualizácia z adresára...*** – Spustí aktualizáciu z aktualizačných súborov, ktoré sa nachádzajú v nastavenom priečinku na disku počítača. Túto možnosť vám však odporúčame použiť len ako núdzové riešenie, napr. v situáciách, keď nie je vytvorené pripojenie na internet (*napríklad počítač je infikovaný a odpojený od internetu; počítač je pripojený k sieti bez prístupu na internet a pod.*). V novo otvorenom okne vyberte priečinok, do ktorého ste predtým uložili aktualizačný súbor a spustite proces aktualizácie.

- Rozšírené nastavenia... – Otvorí dialógové okno Rozšírené nastavenia programu AVG, ktoré umožní upraviť konfiguráciu produktu AVG Internet Security 2012. Odporúčame vám, aby

ste nemenili predvolené nastavenia aplikácie definované dodávateľom softvéru.

- Nastavenia súčasti Firewall... – Otvorí samostatné dialógové okno s rozšírenou konfiguráciou súčasti Firewall .

5.1.5. Pomocník

- ***Obsah***: Otvorí súbory pomocníka AVG.
- ***Získajte podporu*** – Otvorí webovú lokalitu AVG (http://www.avg.com/) na stránke strediska podpory zákazníkov
- ***Webová lokalita AVG*** – Otvorí sa webová lokalita AVG (http://www.avg.com/)
- ***O vírusoch a hrozbách***: Otvorí on-line Vírusovú encyklopédiu, v ktorej si môžete vyhľadať podrobné informácie o identifikovanom víruse.
- ***Znova aktivovať*** – Otvorí dialógové okno ***Aktivácia produktu AVG*** s údajmi, ktoré ste vložili v dialógovom okne Prispôsobiť AVG v procese inštalácie. Toto dialógové okno sa používa na vloženie licenčného čísla, buď pri nahradení predajného čísla (*čísla, s ktorým ste nainštalovali produkt AVG*), alebo pri nahradení starého licenčného čísla (*napr. pri upgradovaní na nový produkt AVG*).
- ***Zaregistrovať*** – pripojí sa na registračnú stránku webovej lokality AVG (http://www.avg.com/). Vyplňte vaše registračné údaje; nárok na bezplatnú technickú podporu získajú len tí zákazníci, ktorí si produkt AVG zaregistrujú.

Poznámka**: Ak používate skúšobnú verziu produktu* **AVG Internet Security 2012**, *uvedené dve položky sa zobrazia v podobe* ***Kúpiť *a* ***Aktivovať*** *a umožnia vám zakúpiť úplnú verziu programu. Ak je produkt* **AVG Internet Security 2012** *nainštalovaný pomocou predajného čísla, položky sa zobrazia v podobe* ***Registrovať*** *a* ***Aktivovať***.

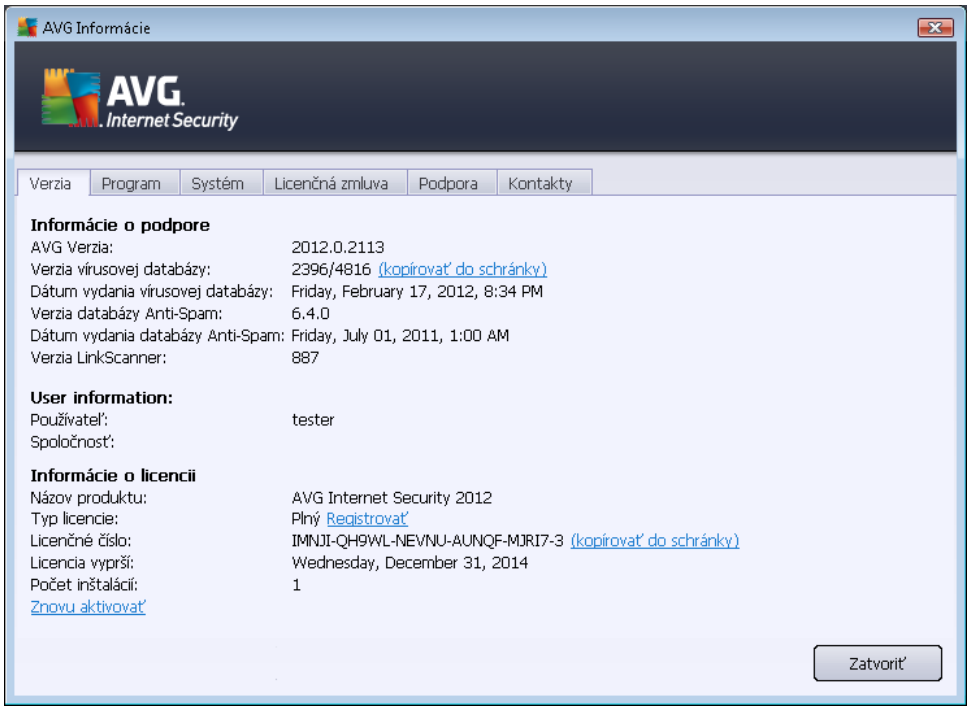
- ***O produkte AVG*** – Otvorí dialógové okno ***Informácie*** so šiestimi kartami, na ktorých sa nachádzajú informácie o názve programu, verzii programu a vírusovej databázy, systémové informácie, informácie o licenčnej zmluve a kontaktné informácie spoločnosti ***AVG Technologies CZ***.

5.1.6. Podpora

Prepojenie ***Podpora*** otvorí nové dialógové okno ***Informácie*** so všetkými typmi údajov, ktoré môžete potrebovať pri hľadaní pomoci. Dialógové okno obsahuje základné údaje o nainštalovanom programe AVG (*verzia programu/databázy*), podrobnosti o licencii a zoznam rýchlych prepojení na pomoc.

Dialógové okno ***Informácie*** je rozdelené na šesť častí:

Karta ***Verzia*** je rozdelená na tri časti:

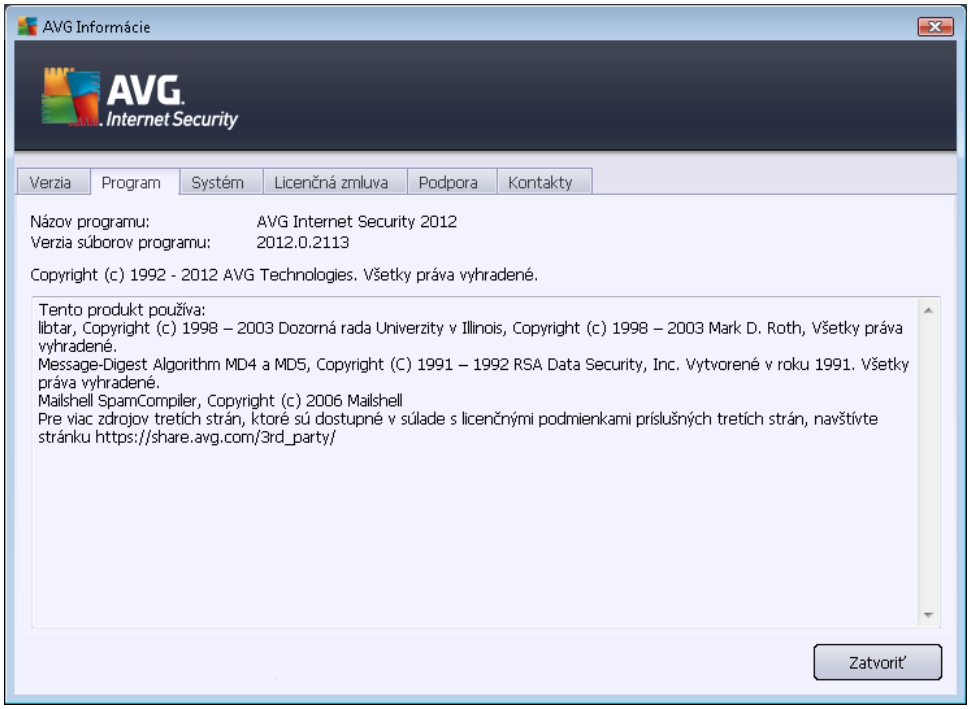


- ***Informácie o podpore*** – Obsahuje informácie o verzii produktu **AVG Internet Security 2012**, verzii vírusovej databázy, verzii databázy súčasti Anti-Spam a verzii súčasti LinkScanner.

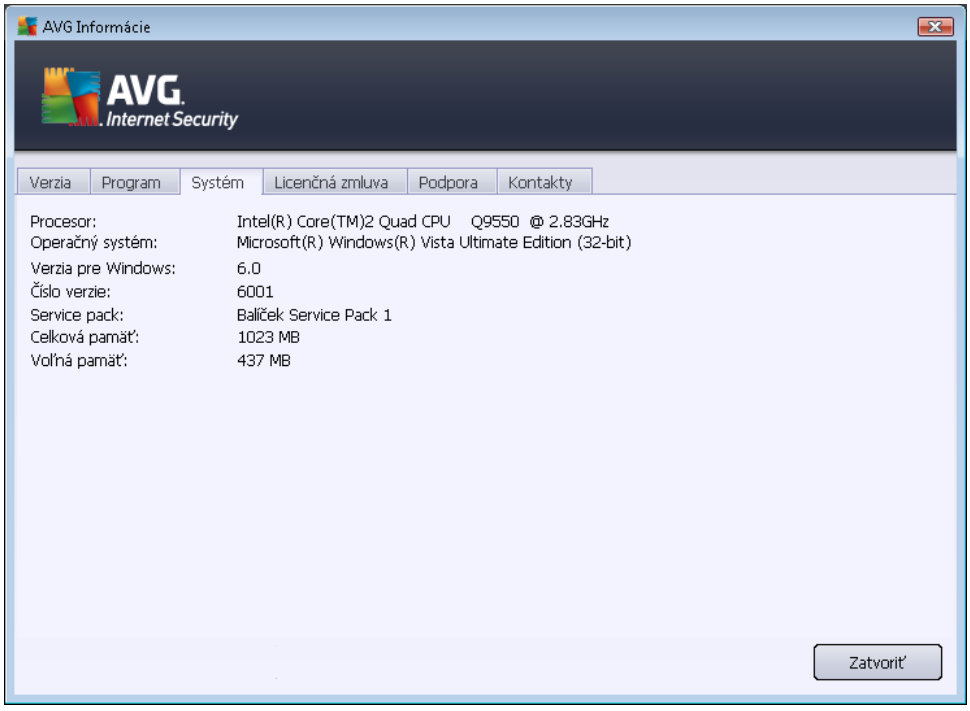
- ***Informácie o používateľovi*** – Obsahuje informácie o licencovanom používateľovi a spoločnosti.

- ***Podrobnosti o licencii*** – Obsahuje informácie o licencii*(názov produktu, typ licencie, číslo licencie, dátum ukončenia platnosti a počet inštalácií)*. V tejto časti môžete tiež využiť prepojenie ***Registrovať*** a zaregistrovať produkt **AVG Internet Security 2012** on-line. Tak budete môcť plne využiť technickú podporu AVG. Pomocou prepojenia ***Znova aktivovať*** otvoríte dialógové okno***Aktivovať AVG***: vyplňte číslo licencie do príslušného poľa, ak chcete nahradiť predajné číslo *(ktoré ste používali počas AVG Internet Security 2012 inštalácie)* alebo zmeniť aktuálne číslo licencie na iné *(napr. pri aktualizácii na vyšší produkt AVG).*

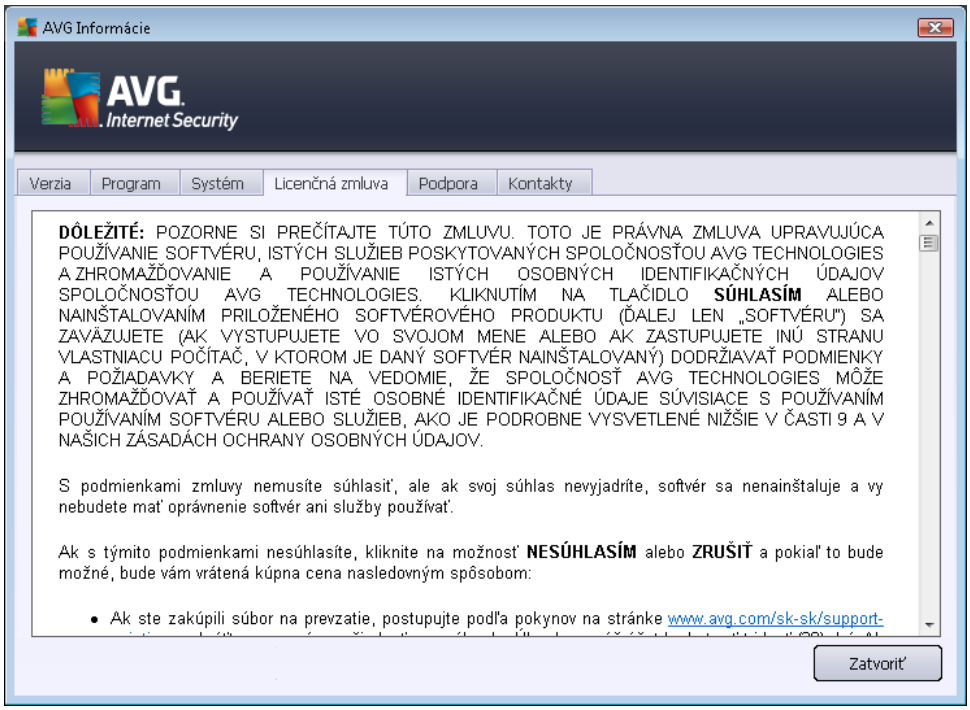
Na karte ***Program*** sa nachádzajú údaje o verzii súboru programu **AVG Internet Security 2012** a o kóde tretích strán, ktorý bol použitý pri tvorbe tohto produktu:



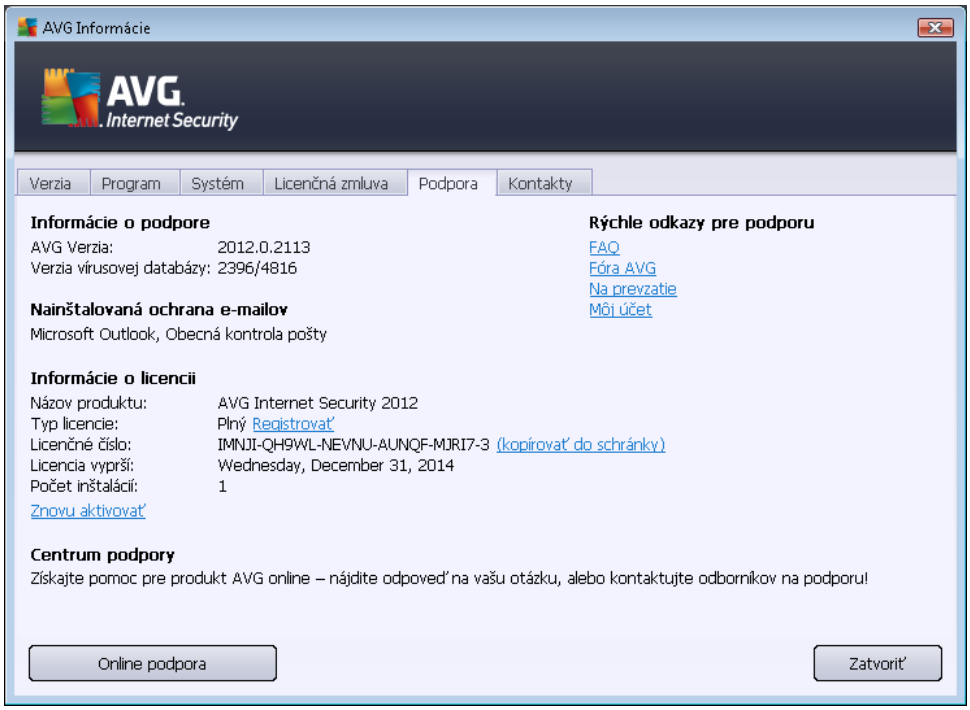
Na karte ***Systém*** sa nachádza zoznam parametrov operačného systému *(typ procesora, operačný systém a jeho verzia, číslo zostavy, použité opravné balíky, celkové množstvo pamäte a množstvo voľnej pamäte)*:



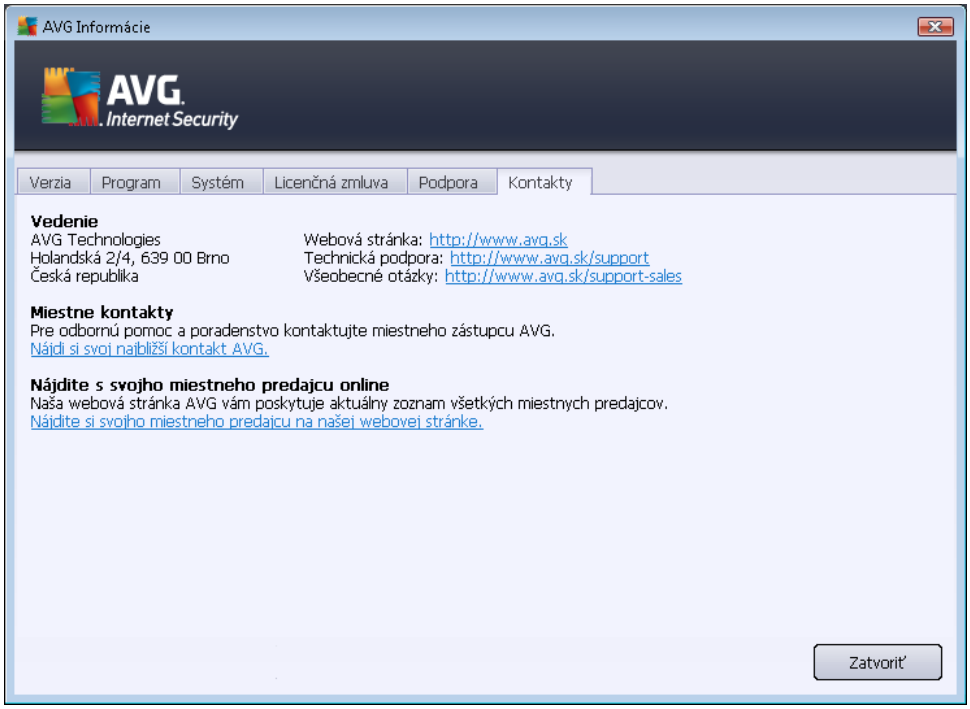
Na karte ***Licenčná zmluva*** si môžete prečítať úplné znenie licenčnej zmluvy medzi vami a spoločnosťou AVG Technologies:



Na karte ***Podpora*** sa nachádza zoznam všetkých možností kontaktovania zákazníckej podpory. Obsahuje aj prepojenia na webovú lokalitu AVG (http://www.avg.com/), fóra AVG, časté otázky... Ďalej tam nájdete informácie, ktoré môžete potrebovať pri komunikácii s tímom zákazníckej podpory:



Karta ***Kontakty*** obsahuje zoznam všetkých kontaktov na spoločnosť AVG Technologies a na miestnych zástupcov a predajcov značky AVG:



5.2. Informácie o stave zabezpečenia

Časť ***Informácie o stave zabezpečenia*** sa nachádza v hornej časti hlavného okna produktu **AVG Internet Security 2012**. V tejto časti sa vždy nachádzajú informácie o momentálnom stave zabezpečenia programom **AVG Internet Security 2012**. Pozrite si prehľad ikon, ktoré sa môžu nachádzať v tejto časti, a ich význam:

 – Zelená ikona informuje, že produkt ***AVG Internet Security 2012 je úplne funkčný***. Počítač je úplne chránený, aktualizovaný a všetky nainštalované súčasti fungujú správne.

 – Žltá ikona upozorňuje, že ***jedna súčasť alebo niekoľko súčastí je nesprávne nakonfigurovaných*** a treba venovať pozornosť ich vlastnostiam alebo nastaveniam. Nevyskytuje sa žiadny vážny problém s produktom **AVG Internet Security 2012** a pravdepodobne ste z nejakého dôvodu vypli niektorú súčasť. Stále ste chránení. Venujte však pozornosť nastaveniam problémovej súčasti! Jej názov bude uvedený v časti ***Informácie o stave zabezpečenia***.

Žltá ikona sa zobrazí aj vtedy, keď ste sa z nejakého dôvodu rozhodli ignorovať chybový stav súčasti. Možnosť ***Ignorovať stav súčasti*** je k dispozícii v kontextovej ponuke (*otvorte ju kliknutím pravým tlačidlom myši*) nad ikonou príslušnej súčasti v prehľade súčastí hlavného

okna aplikácie **AVG Internet Security 2012**. Túto možnosť vyberte vtedy, keď ste si vedomí chybového stavu súčasti, ale z nejakého dôvodu chcete nechať program **AVG Internet Security 2012** v tomto stave a nechcete byť informovaní prostredníctvom ikony na paneli úloh. Môže sa vyskytnúť situácia, keď bude potrebné použiť túto možnosť; dôrazne vám však odporúčame, aby ste funkciu ***Ignorovať stav súčasti*** čo najskôr znova vypli.

Žltá ikona sa zobrazí aj vtedy, ak produkt **AVG Internet Security 2012** vyžaduje reštart počítača (***Je potrebný reštart***). Venujte pozornosť tejto správe a reštartujte počítač pomocou tlačidla ***Reštartovať teraz***.

 – Oranžová ikona upozorňuje, že sa vyskytol vážny stav produktu ***AVG Internet Security 2012***! Jedna súčasť alebo viac súčastí nefunguje správne a produkt **AVG Internet Security 2012** nedokáže chrániť váš počítač. Venujte okamžitú pozornosť odstráneniu uvedeného problému. Ak nedokážete odstrániť chybu sami, kontaktujte tím technickej podpory AVG.

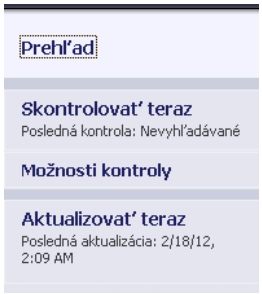
Ak nie je program AVG Internet Security 2012 nastavený tak, aby poskytoval optimálny výkon, vedľa informácie o stave zabezpečenia sa zobrazí nové tlačidlo s názvom Opraviť (alebo Opraviť všetko, ak sa problém týka viacerých súčastí). Stlačením tlačidla spustite automatický postup kontroly a konfigurácie programu. Je to jednoduchý spôsob nastavenia optimálneho výkonu programu AVG Internet Security 2012 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 2012 vám vždy poskytuje aj ikona na paneli úloh.*

5.3. Rýchle odkazy

Rýchle odkazy sa nachádzajú na ľavej strane používateľského rozhrania programu **AVG Internet Security 2012**. 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:



Rýchle odkazy sú graficky rozdelené na tri časti:

- ***Skontrolovať teraz*** – Štandardne toto tlačidlo ponúka informácie o poslednej spustenej kontrole *(t. j. typ kontroly a dátum posledného spustenia)*. Kliknutím na príkaz ***Skontrolovať teraz*** spustíte znovu rovnakú kontrolu. Ak chcete spustiť inú kontrolu, kliknite na prepojenie ***Možnosti kontroly***. Otvoríte rozhranie kontroly produktu AVG, v ktorom môžete spúšťať alebo plánovať kontroly, prípadne upraviť ich parametre. *(Podrobnosti nájdete v kapitole Kontrola aplikáciou AVG)*

- ***Možnosti kontroly*** – Tento odkaz použite na prepnutie z akéhokoľvek aktuálne otvoreného dialógového okna AVG na predvolené okno s prehľadom všetkých nainštalovaných súčastí. *(Podrobnosti nájdete v kapitole Prehľad súčastí)*

- ***Aktualizovať teraz*** – Odkaz poskytne dátum a čas spustenia poslednej aktualizácie. Stlačením tlačidla ihneď spustíte aktualizáciu a môžete sledovať jeho priebeh. *(Podrobnosti nájdete v kapitole Aktualizácie aplikácie AVG)*

Rýchle prepojenia sú dostupné z používateľského rozhrania AVG za všetkých okolností. Ak pomocou rýchleho prepojenia spustíte konkrétny postup, napríklad kontrolu alebo aktualizáciu, aplikácia sa prepne do nového dialógového okna, rýchle prepojenia však zostanú dostupné. Okrem toho sa spustený proces graficky zobrazí v navigácii, takže máte bezprostrednú kontrolu nad všetkými spustenými procesmi aplikácie **AVG Internet Security 2012** .

5.4. Prehľad súčastí

Časť Prehľad súčastí

Časť ***Prehľad súčastí*** sa nachádza v strednej časti používateľského rozhrania **AVG Internet Security 2012**. Táto časť je rozdelená na dve oblasti:

- ***Prehľad nainštalovaných súčastí*** sa skladá s grafických panelov pre každú z nainštalovaných súčastí. Každý panel je označený ikonou príslušnej súčasti a obsahuje informácie o tom, či je príslušná súčasť práve aktívna alebo neaktívna.

- ***V spodnej časti tohto dialógového okna sa nachádza opis súčasti***. Opis stručne vysvetľuje základnú funkciu súčasti. Obsahuje tiež informácie o aktuálnom stave vybranej súčasti.

Zoznam nainštalovaných súčastí

V programe **AVG Internet Security 2012** sa v časti ***Prehľad súčastí*** nachádzajú informácie o týchto súčastiach:

- ***Nástroj Anti-Virus*** odhaľuje v systéme vírusy, spyware, červy, trójske kone, nechcené spustiteľné súbory a knižnice a chráni pred škodlivými programami typu adware – podrobnosti >>

- ***Nástroj LinkScanner*** chráni pred útokmi na webe pri vyhľadávaní a surfovaní na internete – podrobnosti >>

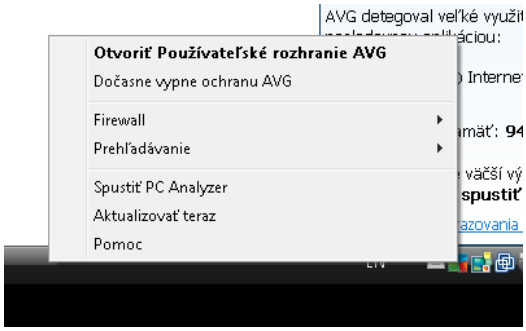
- ***Nástroj Ochrana e-mailu*** kontroluje prichádzajúce e-mailové správy z hľadiska prítomnosti SPAMU a blokuje vírusy, phishingové útoky či iné hrozby – podrobnosti >>
- ***Nástroj Firewall*** kontroluje komunikáciu na všetkých sieťových portoch, chráni pred útokmi a blokuje každý pokus o prienik – podrobnosti >>
- ***Nástroj Anti-Rootkit*** hľadá nebezpečné programy rootkit ukryté v aplikáciách, ovládačoch alebo knižniciach – podrobnosti >>
- ***Systémové nástroje*** uvádza podrobný prehľad prostredia AVG a informácie o operačnom systéme – podrobnosti >>
- ***PC Analyzer*** poskytuje informácie o stave počítača – podrobnosti >>
- ***Nástroj Identity Protection*** nepretržite chráni digitálne aktíva pred novými a neznámymi hrozbami – podrobnosti >>
- ***Súčasť Remote Administration*** sa nachádza len v sieťových edíciách AVG Business Editions, a to len v prípade, ak ste ju nainštalovali počas inštalácie.

Dostupné činnosti

- ***Presunutím kurzora myši nad ktorúkoľvek ikonu súčasti*** sa príslušná ikona zvýrazní v prehľade súčasti. V spodnej časti používateľského rozhrania sa zároveň zobrazí opis základných funkcií súčasti.
- ***Jedným kliknutím na ikonu súčasti*** otvoríte rozhranie konkrétnej súčasti so základnými štatistickými informáciami.
- ***Pravým tlačidlom kliknite na ikonu súčasti***. Rozbalí sa kontextová ponuka s niekoľkými možnosťami:
  - ***Otvoriť*** – Kliknutím na túto možnosť otvoríte vlastné dialógové okno súčasti *(podobne ako pri jednom kliknutí na ikonu komponentu)*.
  - ***Ignorovať stav tejto súčasti*** – Túto možnosť vyberte vtedy, ak ste si vedomí chybového stavu súčasti, ale z nejakého dôvodu chcete nechať program AVG v tomto stave a nemáte záujem o varovanie prostredníctvom ikony na paneli úloh.
  - ***Otvoriť v rozšírených nastaveniach ...*** – Táto možnosť je k dispozícii iba pri niektorých súčastiach, teda tých, ktoré poskytujú rozšírené nastavenia.

5.5. Ikona v paneli úloh

Ikona AVG v paneli úloh *(v paneli úloh systému Windows v pravom dolnom rohu monitora)* zobrazuje aktuálny stav produktu **AVG Internet Security 2012**. Vždy sa nachádza v paneli úloh bez ohľadu na to, či je používateľské rozhranie produktu **AVG Internet Security 2012** otvorené alebo zatvorené:



Zobrazenie ikony AVG v systémovom paneli úloh

- Úplne vyfarbená ikona bez ďalších prvkov znamená, že všetky komponenty aplikácie **AVG Internet Security 2012** sú aktívne a úplne funkčné. Takáto ikona sa však môže zobraziť aj vtedy, keď niektorá zo súčasti nie je úplne funkčná, ale používateľ sa rozhodol ignorovať jej stav. *(Ak ste potvrdili možnosť ignorovania stavu súčasti, potvrdzujete tým, že ste si vedomí chybového stavu súčasti, ale z nejakého dôvodu ju tak chcete ponechať a nechcete zobrazovať varovania týkajúce sa tejto situácie.)*

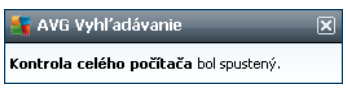
- Ikona s výkričníkom znamená, že súčasť *(alebo viac súčastí)* je v chybovom stave. Takýmto výstrahám vždy venujte pozornosť a snažte sa odstrániť problém konfigurácie súčasti, ktorá nie je nastavená správne. Ak chcete zmeniť konfiguráciu súčasti, dvakrát kliknite na ikonu v paneli úloh. Otvorí sa používateľské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

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

- Plnofarebné zobrazenie so šípkou znamená, že **AVG Internet Security 2012** práve prebieha kontrola.

Informácie ikony AVG v systémovom paneli úloh

Ikona AVG v paneli úloh ďalej obsahuje informácie o aktuálnej činnosti produktu **AVG Internet Security 2012** a možných zmenách stavu v programe (*napr. automatické spustenie naplánovanej kontroly alebo aktualizácie, Prepínač profilu brány firewall, zmeny stavu súčasti, výskytu chybového stavu, ...*) pomocou automaticky otváraného okna, ktoré sa otvorí v ikone v paneli úloh:



Činnosti prístupné prostredníctvom ikony AVG v paneli úloh

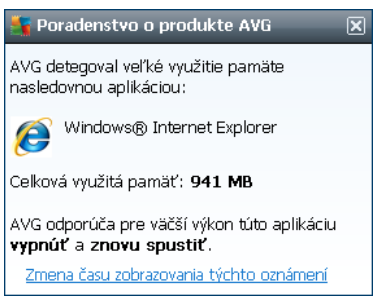
Ikonu AVG v paneli úloh môžete použiť aj na rýchle zobrazenie používateľského rozhrania

produktu **AVG Internet Security 2012**. Stačí dvakrát kliknúť na ikonu. Kliknutím pravým tlačidlom myši na ikonu sa otvorí krátka kontextová ponuka s týmito možnosťami:

- ***Otvoriť používateľské rozhranie*** – Kliknutím na túto položku sa otvorí používateľské rozhranie aplikácie **AVG Internet Security 2012**.
- ***Dočasne vypnúť ochranu AVG*** – Táto možnosť umožňuje vypnúť celú ochranu produktom **AVG Internet Security 2012** naraz. Nepoužívajte túto možnosť, ak to nie je naozaj nevyhnutné! Vo väčšine prípadov nie je potrebné vypnúť produkt **AVG Internet Security 2012** pred inštaláciou nového softvéru alebo ovládačov, a to ani v prípade, keď inštalačný program alebo sprievodca inštaláciou softvéru odporúča, aby sa najskôr zatvorili spustené programy a aplikácie z dôvodu možného nežiaduceho prerušenia procesu inštalácie. Ak musíte dočasne vypnúť ochranu **AVG Internet Security 2012**, znova ju zapnite bezprostredne po dokončení úloh, pre ktoré ste ju vypli. Ak ste pripojení na internet alebo k sieti v čase, keď je antivírový softvér vypnutý, počítač nie je chránený pred útokmi.
- ***Firewall*** – Kliknutím na túto možnosť sa otvára kontextová ponuka s možnosťami nastavenia súčasti Firewall, ktorá umožňuje editovať základné parametre: Stav súčasti Firewall (*Súčasť Firewall je zapnutá/Súčasť Firewall je vypnutá/Núdzový režim*), prepnutie režimu hry a profily súčasti Firewall.
- ***Kontroly*** – Kliknutím na túto možnosť otvoríte kontextovú ponuku vopred definovaných kontrol (*Kontrola celého počítača* a *Kontrola súborov/priečinkov*) a vyberte požadovanú kontrolu. Kontrola sa ihneď spustí.
- ***Kontroluje sa...*** – Táto položka sa zobrazí len v prípade, keď v počítači práve beží kontrola. Tejto kontrole môžete potom nastaviť prioritu, alebo ju môžete zastaviť alebo pozastaviť. Ďalej sa tu nachádzajú tieto funkcie: *Nastaviť prioritu pre všetky kontroly, Pozastaviť všetky kontroly* a *Zastaviť všetky kontroly*.
- ***Otvoriť PC Analyzer*** – Kliknutím na túto možnosť sa spúšťa súčasť PC Analyzer.
- ***Aktualizovať teraz*** – Spustí okamžitú aktualizáciu.
- ***Pomocník*** – Otvorí súbor pomocníka na úvodnej strane.

5.6. AVG Advisor

AVG Advisor je služba, ktorá sleduje všetky procesy spustené na počítači, či v nich nedochádza k problémom, a ponúka tipy na ich predchádzanie. ***AVG Advisor*** vidíte v podobe vysúvacieho kontextového okna na systémovom pozadí.



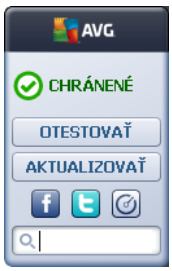
AVG Advisor sa môže zobraziť v týchto situáciách:

- Vášmu internetovému prehliadaču dochádza pamäť, čo môže spomaľovať prácu *(AVG Advisor podporujú iba prehliadače Explorer, Chrome, Firefox, Opera a Safari);*
- Proces spustený na počítači používa príliš veľa pamäte a spomaľuje jeho výkon;
- Počítač sa automaticky pripojí k neznámej sieti Wi-Fi.

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

5.7. Miniaplikácia AVG

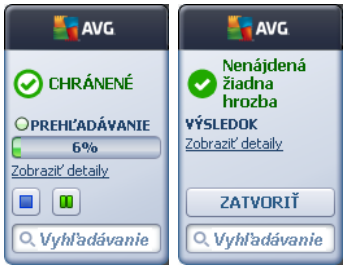
Mini-aplikácia AVG sa nachádza na pracovnej ploche operačného systému Windows (*bočnom paneli systému Windows*). Túto aplikáciu podporujú len operačné systémy Windows Vista a Windows 7. ***Mini-aplikácia AVG*** umožňuje okamžitý prístup k najdôležitejším funkciám programu **AVG Internet Security 2012**, t. j. kontrole a aktualizácii:



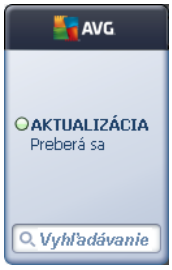
Rýchly prístup ku kontrole a aktualizácii

V prípade potreby môžete pomocou ***mini-aplikácie AVG*** okamžite spustiť kontrolu alebo aktualizáciu:

- ***Skontrolovať teraz*** – Kliknutím na odkaz ***Skontrolovať teraz*** sa priamo spustí kontrola celého počítača. Priebeh kontroly môžete pozorovať v prepínajúcom sa používateľskom rozhraní mini-aplikácie. Stručný štatistický prehľad informuje o počte skontrolovaných objektov a detekovaných a vyliečených hrozieb. Počas kontroly môžete vždy pozastaviť alebo zastaviť kontrolu. Podrobné informácie súvisiace s výsledkami kontroly sa nachádzajú v štandardnom dialógovom okne Prehľad výsledkov kontroly, ktoré sa otvára priamo v mini-aplikácii výberom možnosti ***Zobraziť podrobnosti*** *(príslušné výsledky kontroly budú uvedené pod položkou Kontrola z mini-aplikácie na bočnom paneli).*



- ***Aktualizovať teraz*** – Kliknutím na odkaz ***Aktualizovať teraz*** sa **AVG Internet Security 2012** aktualizuje priamo v miniaplikácii:



Prístup k sociálnym sieťam

Mini-aplikácia AVG ponúka tiež rýchle prepojenie na hlavné sociálne siete. Stlačením príslušného tlačidla sa pripojíte ku komunitám AVG na sieťach Twitter, Facebook alebo LinkedIn:

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

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

- ***LinkedIn*** – Táto možnosť je dostupná len v rámci sieťovej inštalácie (*t.j. pod podmienkou, že ste si produkt AVG nainštalovali pomocou licencie pre jednu z edícií AVG Business Edition*) a otvára internetový prehliadač na internetových stránkach ***AVG SMB***

Community v sociálnej sieti LinkedIn.

Ďalšie dostupné funkcie miniaplikácie

- ***PC Analyzer***  – Otvorí používateľské rozhranie súčasti PC Analyzer a priamo začne s analýzou.
- ***Vyhľadávacie políčko*** – Zadajte kľúčové slovo na okamžité zobrazenie výsledkov vyhľadávania v novom otvorenom okne v predvolenom internetovom prehliadači.

6. Súčasti AVG

6.1. Anti-Virus

Súčasť ***Anti-Virus*** je základom produktu **AVG Internet Security 2012** a spája niekoľko základných funkcií bezpečnostného programu:

- Kontrolovacie jadro
- Rezidentná ochrana
- Ochrana súčasťou Anti-Spyware

6.1.1. Kontrolovacie jadro

Kontrolovacie jadro, ktoré je základnou súčasťou nástroja ***Anti-Virus***, kontroluje všetky súbory a činnosti so súbormi *(otváranie/zatváranie súborov a pod.)*z hľadiska prítomnosti známych vírusov. Každý zistený vírus sa zablokuje, aby nemohol vykonávať žiadnu činnosť, a potom sa vymaže alebo sa premiestni do vírusového trezoru.

Dôležitá funkcia ochrany AVG Internet Security 2012 spočíva v tom, že v počítači nie je možné spustiť žiadny známy vírus!

Metódy zisťovania

Väčšina antivírusových softvérov používa aj heuristickú kontrolu, ktorá kontroluje typické vlastnosti vírusov v súboroch, tzv. vírusové signatúry. To znamená, že antivírusový program dokáže zistiť nový, neznámy vírus vtedy, keď obsahuje isté typické vlastnosti existujúcich vírusov. ***Súčasť Anti-Virus*** používa tieto metódy zisťovania:

- *Kontrolu* – vyhľadávanie reťazcov znakov, ktoré sú charakteristické pre daný vírus.
- *Heuristická analýza* – dynamická emulácia pokynov vyhľadávaných objektov vo virtuálnom prostredí počítača
- *Generická detekcia* – detekcia pokynov, ktoré sú charakteristické pre konkrétny vírus alebo skupinu vírusov

Ak s apoužije len jedna z uvedených technológií, zistenie či identifikácia vírusu sa nemusí podariť. Súčasť ***Anti-Virus*** využíva niekoľko technológií súčasne s cieľom zaručiť ochranu počítača pred vírusmi. Program **AVG Internet Security 2012** dokáže analyzovať a zistiť aj spustiteľné aplikácie a knižnice DLL, ktoré by mohli predstavovať potenciálne nežiaduce položky v systéme. Tieto hrozby nazývame potenciálne nežiaduce programy *(rôzne druhy spyware, adware atď.)*. Aplikácia **AVG Internet Security 2012** ďalej kontroluje podozrivé záznamy v databáze Registry, dočasné internetové súbory a sledovacie súbory cookies a spracuje všetky potenciálne škodlivé položky rovnakým spôsobom ako každú inú infekciu.

Produkt AVG Internet Security 2012 nepretržite chráni váš počítač.

6.1.2. Rezidentná ochrana

Aplikácia* AVG Internet Security 2012** poskytuje nepretržitú ochranu vo forme tzv. rezidentnej ochrany. ***Súčasť Anti-Virus prehľadáva jednotlivé súbory *(s určitými príponami alebo bez prípon)*, ktorý otvárate, ukladáte alebo kopírujete. Chráni systémové oblasti počítača a vymeniteľné médiá (*disky flash a podobne*). Keď zistí vírus v súbore, ktorý sa snažíte otvoriť, zastaví prebiehajúcu operáciu a nedovolí vírusu, aby sa aktivoval. Normálne tento proces ani nezbadáte, pretože rezidentná ochrana je „spustená na pozadí“. Uvidíte iba oznámenie o prípadnej zistenej hrozbe. Súčasť ***Anti-Virus*** zároveň zablokuje aktiváciu hrozby a odstráni ju.

Rezidentná ochrana sa zavedie do pamäte počítača počas zavádzania operačného systému a je dôležité, aby bola vždy zapnutá!

6.1.3. Ochrana súčasťou Anti-Spyware

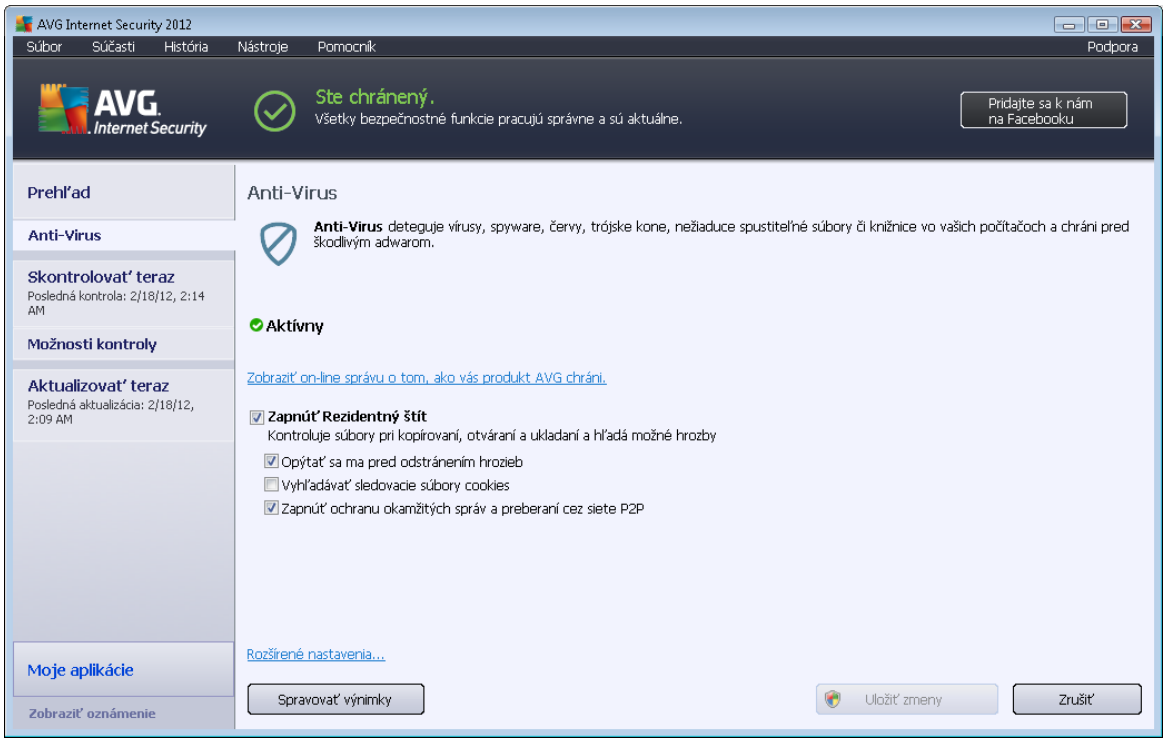
Súčasť Anti-Spyware sa skladá z databázy spyware, ktorá sa používa pri určovaní známych typov programov spyware. Odborníci spracujú identifikáciu a opis najnovších vzorov spyware bezprostredne po výskyte a ihneď pridajú definície do databázy spyware AVG. Prostredníctvom aktualizácie sa nové definície prevezmú do počítača, aby ste boli vždy spoľahlivo chránení aj pred najnovšími typmi programov spyware. ***Súčasť Anti-Spyware*** umožňuje komplexnú kontrolu počítača z hľadiska výskytu programov typu malware/spyware. Deteguje aj spiaci a neaktívny škodlivý softvér, t. j. taký, ktorý bol prevzatý do počítača, ale doposiaľ sa neaktivoval.

Čo je to spyware?

Spyware sa zvyčajne vymedzuje ako druh škodlivého softvéru, t. j. softvér, ktorý zhromažďuje informácie z počítača bez vedomia alebo súhlasu jeho používateľa. Niektoré aplikácie spyware môžu byť nainštalované aj zámerne a často obsahujú reklamy, kontextové okná alebo rôzne druhy nepríjemného softvéru. Najbežnejším zdrojom infekcie sú v súčasnosti webové stránky s potenciálne nebezpečným obsahom. Škodlivý kód sa šíri aj inými metódami prenosu, napr. e-mailom alebo červami a vírusmi. Základná ochrana spočíva v používaní kontrolných programov bežiacich na pozadí (tzv. ***Anti-Spyware***), ktoré fungujú ako rezidentný štít a kontrolujú aplikácie na pozadí, keď ich spúšťate.

6.1.4. Rozhranie súčasti Anti-Virus

Rozhranie súčasti ***Anti-Virus*** zobrazuje stručné informácie o funkcii súčasti, jej aktuálnom stave *(aktívna)* a možnostiach základnej konfigurácie:



Možnosti konfigurácie

Toto dialógové okno ponúka niekoľko základných možností konfigurácie funkcií súčasti ***Anti-Virus***. Nasleduje stručný opis:

- ***Zobrazenie on-line správy o ochrane aplikáciou AVG*** – Odkaz vás presmeruje na konkrétnu stránku na webovej lokalite AVG (http://www.avg.com/). Na tejto lokalite sa nachádza štatistický prehľad o všetkých **AVG Internet Security 2012** činnostiach vykonaných v počítači v stanovenom vymedzenom intervale a za celý čas.

- ***Povoliť súčasť Rezidentný štít*** – Pomocou tejto možnosti môžete vypnúť/zapnúť rezidentnú ochranu. Súčasť Rezidentný štít kontroluje súbory pri kopírovaní, otváraní alebo ukladaní. V prípade zistenia prítomnosti vírusu alebo akéhokoľvek druhu hrozby vás program ihneď upozorní. Štandardne je táto funkcia zapnutá a odporúčame vám, aby zostala aktívna. Po zapnutí rezidentnej ochrany môžete rozhodnúť, ako sa majú spracovať prípadné zistené infekcie:

  - ***Opýtať sa ma pred odstránením hrozieb*** – Túto možnosť nechajte označenú, ak chcete, aby sa vás program vždy pýtal pred presunutím nájdenej hrozby do Vírusového trezoru. Táto možnosť nemá žiadny vplyv na úroveň zabezpečenia a vyjadruje len vaše preferencie.

- ***Vyhľadávať sledovacie súbory cookies*** – Nezávisle od predchádzajúcich možností môžete rozhodnúť, či chcete vyhľadávať sledovacie súbory cookies. *(Cookies sú textové pakety posielané serverom do internetového prehliadača a následne posielané nezmenené späť z prehliadača pri každom sprístupnení príslušného servera. Súbory HTTP cookies sa používajú na autentifikáciu, sledovanie a zachovanie špecifických informácií o používateľoch, ako sú preferencie stránky alebo obsah ich elektronických nákupných vozíkov.)* V špecifických prípadoch môžete zapnúť túto možnosť, aby ste dosiahli maximálnu úroveň zabezpečenia, štandardne je však vypnutá.

- ***Zapnúť ochranu okamžitých správ a preberaní P2P*** – začiarknite túto položku, ak si želáte kontrolu, či sa v komunikácii pomocou okamžitých správ (*napr. ICQ, MSN Messenger...*) nenachádzajú vírusy.

- ***Rozšírené nastavenia***... – Po kliknutí na toto prepojenie sa v rámci Rozšírených nastavení produktu **AVG Internet Security 2012** zobrazí príslušné okno. V ňom môžete upraviť podrobnosti konfigurácie súčasti. Všimnite si však, že predvolená konfigurácia všetkých súčastí je nastavená tak, aby **AVG Internet Security 2012** poskytovala optimálny výkon a maximálne zabezpečenie. Ak nemáte na zmenu oprávnený dôvod, odporúčame vám zachovať predvolenú konfiguráciu!

Ovládacie tlačidlá

V dialógovom okne sú k dispozícii tieto ovládacie tlačidlá:

- ***Spravovať výnimky*** – Otvorí sa nové dialógové okno s názvom ***Súčasť Rezidentný štít – výnimky***. K dialógovému oknu na konfiguráciu výnimiek z kontroly rezidentného štítu máte prístup aj z hlavnej ponuky v poradí Rozšírené nastavenia/Antivírus/Resident Shield/ Výnimky *(pozrite si kapitolu s príslušnými informáciami)*. V tomto dialógovom okne môžete určiť súbory a priečinky, ktoré chcete vyňať z kontroly súčasťou Rezidentný štít. Odporúčame vám, aby ste nevylúčili žiadne položky, ak to nie je skutočne nutné. V tomto dialógovom okne sa nachádzajú tieto ovládacie tlačidlá:

  - *Pridať cestu* – Zadajte adresár *(alebo adresáre)*, ktoré sa majú vylúčiť z kontroly: postupne ich vyberte v navigačnej štruktúre lokálneho disku.

  - *Pridať súbor* – Zadajte súbory, ktoré sa majú vylúčiť z kontroly: postupne ich vyberte v navigačnej štruktúre lokálneho disku.

  - *Upraviť položku* – Umožňuje upraviť zadanú cestu k vybranému súboru alebo priečinku.

  - *Odstrániť položku* – Umožňuje odstrániť cestu k vybranej položke zo zoznamu.

  - *Upraviť zoznam* – Umožňuje upraviť celý zoznam definovaných výnimiek v novom dialógovom okne, ktoré sa správa ako štandardný textový editor.

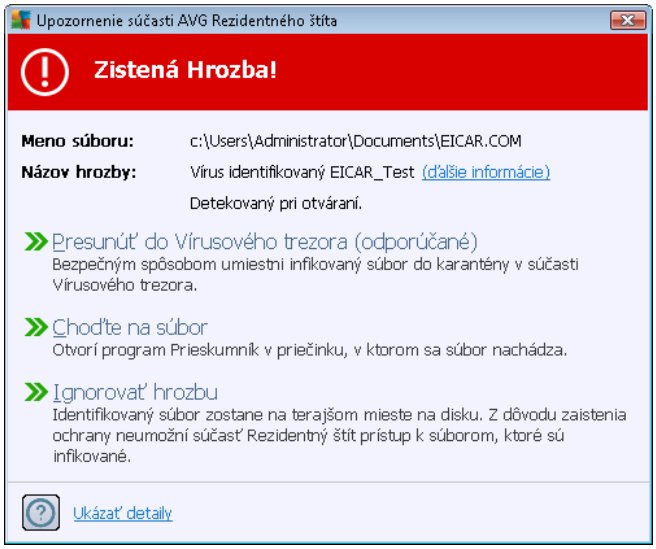
- ***Použiť*** – Všetky zmeny vykonané v tomto dialógovom okne sa uložia do nastavenia súčasti a vrátite sa späť do hlavného používateľského rozhrania produktu **AVG Internet Security 2012** (*prehľad súčastí*).

- ***Zrušiť*** – Všetky zmeny nastavení súčasti vykonané v tomto dialógovom okne sa zrušia. Zmeny sa neuložia. Vrátite sa do hlavného používateľského rozhrania produktu **AVG Internet Security 2012** (*prehľad súčastí*).

6.1.5. Nálezy súčasti Rezidentný štít

Zistená hrozba!

Rezidentný štít kontroluje súbory pri kopírovaní, otváraní a ukladaní. Pri detekovaní vírusu alebo akéhokoľvek druhu hrozby vás program ihneď upozorní zobrazením tohto dialógového okna:



V tomto dialógovom okne sa nachádzajú informácie o súbore, ktorý bol zistený a označený ako infikovaný (*Názov súboru*), názve rozpoznanej infekcie (*Názov hrozby*) a prepojenie na Encyklopédiu vírusov s podrobnými informáciami o zistenej infekcii, ak je známa (*Ďalšie informácie*).

Ďalej sa musíte rozhodnúť, akú akciu treba vykonať. K dispozícii je niekoľko alternatívnych možností. ***Upozorňujeme, že v určitých podmienkach (aký typ súboru bol infikovaný a kde sa nachádza) nie sú vždy k dispozícii všetky možnosti.***

- ***Vyliečiť*** – toto tlačidlo sa zobrazí, len keď je možné detekovanú infekciu vyliečiť. Odstráni infekciu a obnoví pôvodný stav súboru. Ak je však samotný súbor vírus, použite túto funkciu na jeho vymazanie (*t. j. odstránenie do Vírusového trezora*).
- ***Premiestniť do trezora (odporúča sa)*** – vírus sa premiestni do vírusového trezora
- ***Prejsť na súbor*** – táto možnosť vás presmeruje na presné umiestnenie podozrivého objektu (*otvorí nové okno programu Prieskumník*).
- ***Ignorovať hrozbu*** – odporúčame vám, aby ste túto možnosť NEPOUŽÍVALI, pokiaľ na to nemáte veľmi dobrý dôvod!

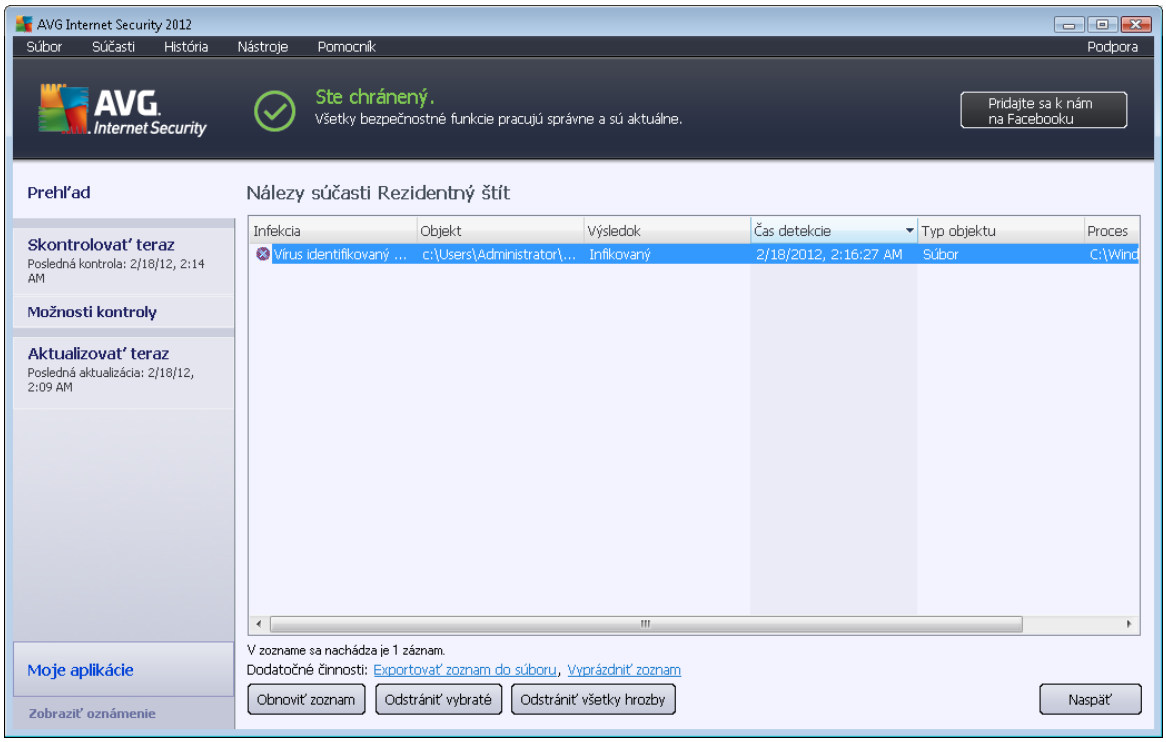
Poznámka: *Môže sa stať, že veľkosť detekovaného objektu prekročí veľkosť voľného miesta vo*

Vírusovom trezore. V tom prípade sa zobrazí upozornenie informujúce o probléme v súvislosti s premiestňovaním infikovaného súboru do Vírusového trezora. Veľkosť Vírusového trezora však môžete zmeniť. Je definovaná ako nastaviteľné percento skutočnej veľkosti vášho pevného disku. Na zväčšenie veľkosti Vírusového trezora otvorte dialógové okno Vírusový trezor v časti Rozšírené nastavenia programu AVG kliknutím na možnosť „Obmedziť veľkosť Vírusového trezora“.

V spodnej časti dialógového okna sa nachádza odkaz ***Zobraziť podrobnosti*** – kliknutím naň otvoríte automaticky otvárané okno s podrobnými informáciami o procese, ktorý bol spustený v čase zistenia infekcie, a identifikáciou procesu.

Prehľad nálezov súčasti Rezidentný štít

Celý prehľad všetkých hrozieb detekovaných súčasťou Rezidentný štít sa nachádza v dialógovom okne ***Nálezy súčasti Rezidentný štít***, ktoré sa otvára pomocou možnosti História/Nálezy súčasti Rezidentný štít v hlavnej ponuke programu:



Nálezy súčasti Rezidentný štít poskytuje prehľad objektov detekovaných súčasťou Rezidentný štít, vyhodnotených ako nebezpečné a buď vyliečených alebo premiestnených do Vírusového trezora. Pre každý detekovaný objekt sú k dispozícii tieto informácie:

- ***Infekcia*** – opis (prípadne aj názov) detekovaného objektu.
- ***Objekt*** – umiestnenie objektu.
- ***Výsledok*** – akcia urobená na detekovanom objekte.

- ***Čas detekcie*** – dátum a čas detekovania objektu.
- ***Typ objektu*** – typ detekovaného objektu.
- ***Proces*** – aká akcia sa vykonala na zavolanie potenciálne nebezpečného objektu, aby sa dal detekovať.

V spodnej časti dialógového okna pod zoznamom sa nachádzajú informácie o celkovom počte detekovaných objektov. Ďalej môžete exportovať celý zoznam detekovaných objektov do súboru (***Exportovať zoznam do súboru***) a vymazať všetky záznamy o detekovaných objektoch (***Vyprázdniť zoznam***). Tlačidlo ***Obnoviť zoznam*** aktualizuje zoznam hrozieb detekovaných súčasťou ***Rezidentný štít***. Tlačidlo ***Späť*** prepne späť na implicitné hlavné dialógové okno AVG (*prehľad súčastí*).

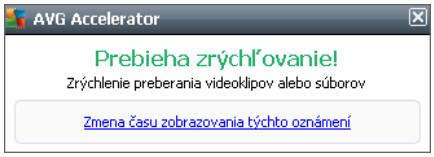
6.2. LinkScanner

LinkScanner 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 pozeráte, a stará sa o to, aby boli bezpečné práve v momente, keď je to najviac dôležité – v momente, keď sa chystáte kliknúť na odkaz.

Súčasť LinkScanner nie je určená na ochranu serverových platforiem.

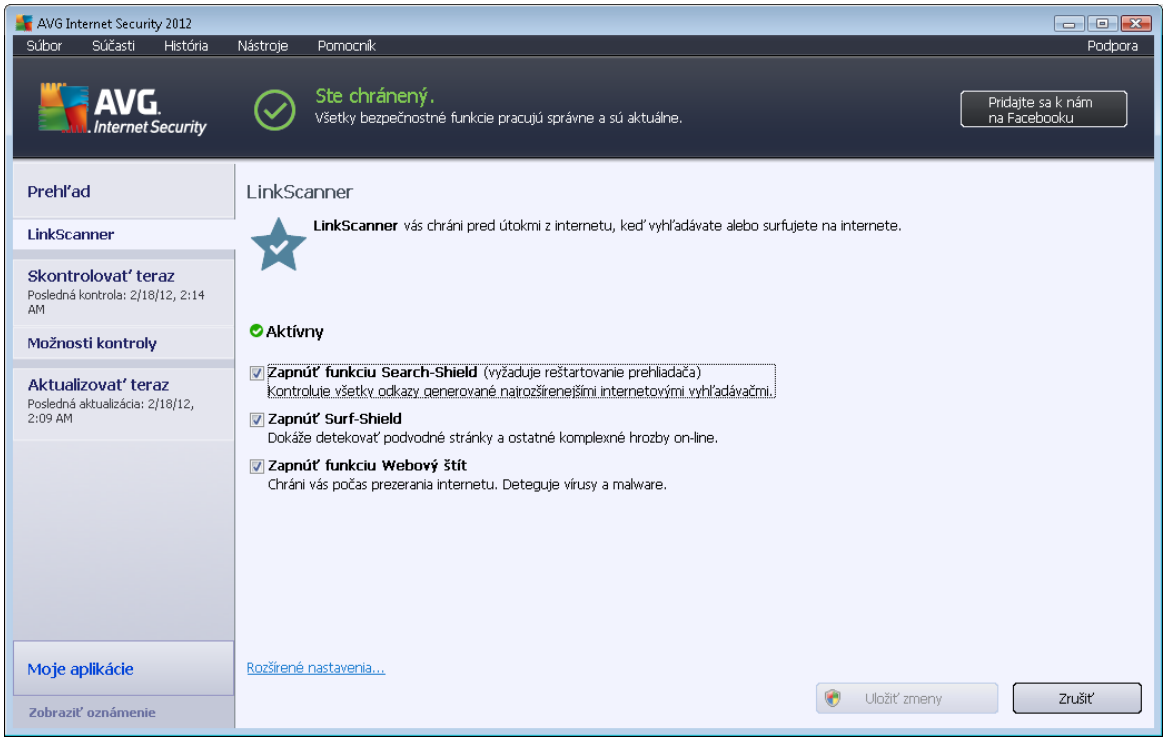
Technológiu ***LinkScanner*** tvoria tieto hlavné funkcie:

- Search-Shield používa zoznam internetových stránok *(adries URL)*, o ktorých je známe, že sú nebezpečné. Pri vyhľadávaní pomocou vyhľadávačov Google, Yahoo! JP, eBay, Twitter, Digg, SlashDot, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask a Seznam sa všetky výsledky vyhľadávania skontrolujú podľa tohto zoznamu a zobrazí sa ikona výsledku *(v súvislosti s výsledkami zistenými vyhľadávačom Yahoo! sa zobrazí len ikona výsledku „napadnuté webové lokality“)*.
- Surf-Shield kontroluje obsah navštívených webových lokalít bez ohľadu na ich internetovú adresu. Dokonca aj keď funkcia Search-Shield *nezachytí niektoré webové lokality (napr. keď sa vytvoria nové škodlivé webové lokality alebo keď pôvodne čisté lokality obsahujú škodlivý kód*), funkcia Surf-Shield ich zachytí a zablokuje v momente, keď sa ich pokúsite navštíviť.
- Webový štít funguje pri surfovaní na internete ako ochrana v reálnom čase. Skontroluje obsah navštívených webových lokalít (a možné súbory, ktoré sa tu nachádzajú) skôr, než sa zobrazia vašom webovom prehliadači alebo prevezmú do počítača. Webový štít zisťuje vírusy a spyware na stránke, ktorú chcete navštíviť, a okamžite zastaví preberanie, aby sa do počítača nedostali žiadne hrozby.
- ***Služba AVG Accelerator*** umožňuje stabilnejšie prehrávanie on-line videa a uľahčuje ďalšie preberania. Ak prebieha akcelerácia videa, v paneli úloh vás upozorní kontextové okno.



6.2.1. Rozhranie súčasti LinkScanner

V hlavnom dialógovom okne súčasti LinkScanner sa nachádza stručný opis funkcií súčasti a informácie o jej aktuálnom stave *(aktívna)*:



V spodnej časti dialógového okna môžete uskutočniť niektoré základné nastavenia súčasti:

- ***Povoliť súčasť Search-Shield*** – (*štandardne zapnuté*): Ak máte dostatočný dôvod vypnúť funkciu Search-Shield, zrušte označenie tohto políčka.
- ***Povoliť súčasť Surf-Shield*** – (*štandardne zapnuté*): Aktívna ochrana (*v reálnom čase*) pred nebezpečnými lokalitami, keď k nim pristupujete. Pripojenie k známym škodlivým lokalitám a ich nebezpečnému obsahu sa zablokuje pri otváraní v internetovom prehliadači (*alebo inej aplikácii, ktorá používa protokol HTTP*).
- ***Povoliť súčasť Webový štít*** – (*štandardne zapnuté*): Prehľadávanie webových lokalít, ktoré chcete navštíviť, v reálnom čase z hľadiska obsahu vírusov alebo spyware. Ak sa zistí ich prítomnosť, preberanie sa okamžite zastaví a do počítača sa nedostanú žiadne hrozby.

6.2.2. Nálezy súčasti Search-Shield

Ak vyhľadávate na internete so zapnutou funkciou ***Search-Shield***, všetky výsledky vyhľadávania v najrozšírenejších vyhľadávačoch (*Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg a SlashDot*) sú hodnotené z hľadiska nebezpečných a podozrivých odkazov. Kontrolou týchto odkazov a označením nevhodných prepojení vás súčasť LinkScanner upozorní skôr, než kliknete na nebezpečné, resp. podozrivé prepojenia, takže získate istotu, že navštevujete len bezpečné webové lokality.

Počas analyzovania odkazu sa na stránke s výsledkami vyhľadávania vedľa odkazu zobrazí značka, ktorá informuje o prebiehajúcej kontrole odkazu. Po dokončení procesu hodnotenia sa zobrazí príslušná informačná ikona:

Stránka odkazu je bezpečná.

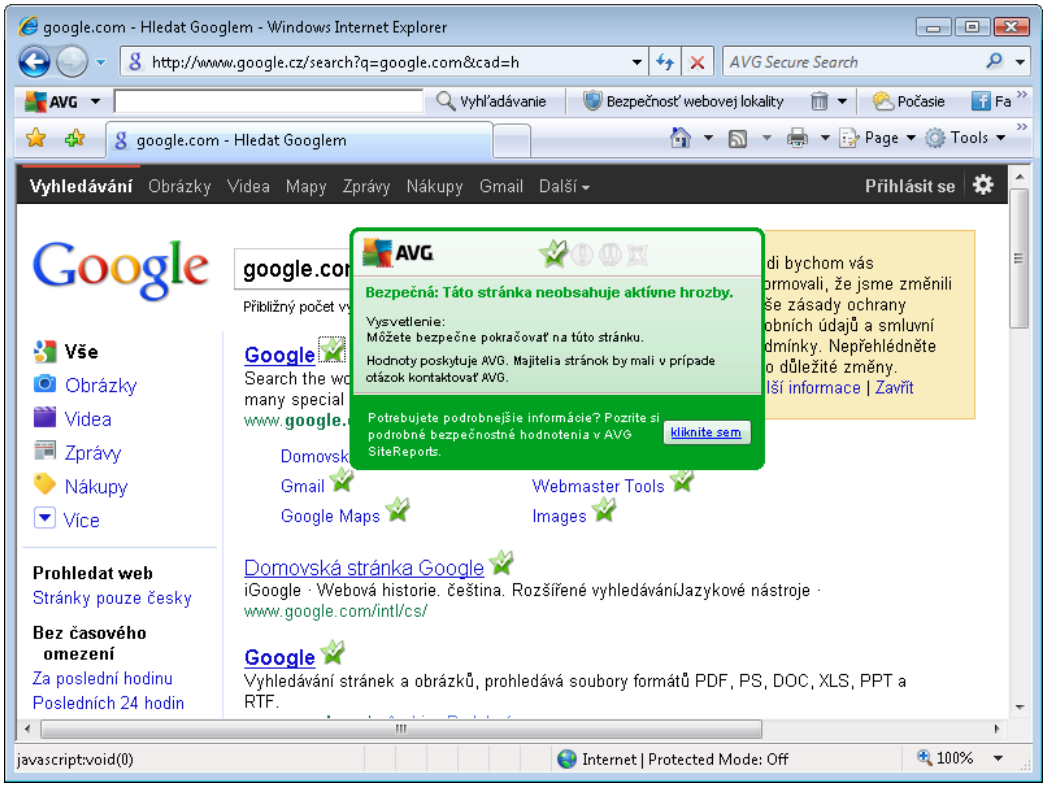
Na stránke odkazu sa nenachádzajú hrozby, ale je do istej miery podozrivá (*otázny pôvod alebo motív, a preto vám ju neodporúčame používať na internetové nakupovanie atď.*).

Stránka odkazu je buď bezpečná, ale zároveň sa na nej nachádzajú ďalšie odkazy na pozitívne nebezpečné stránky, alebo obsahuje podozrivý kód, hoci v tomto momente nepredstavuje žiadnu priamu hrozbu.

Na stránke odkazu sa nachádzajú činné hrozby! Pre vašu vlastnú bezpečnosť vám nebude umožnené navštíviť túto stránku.

Stránka odkazu nie je prístupná a nedala sa skontrolovať.

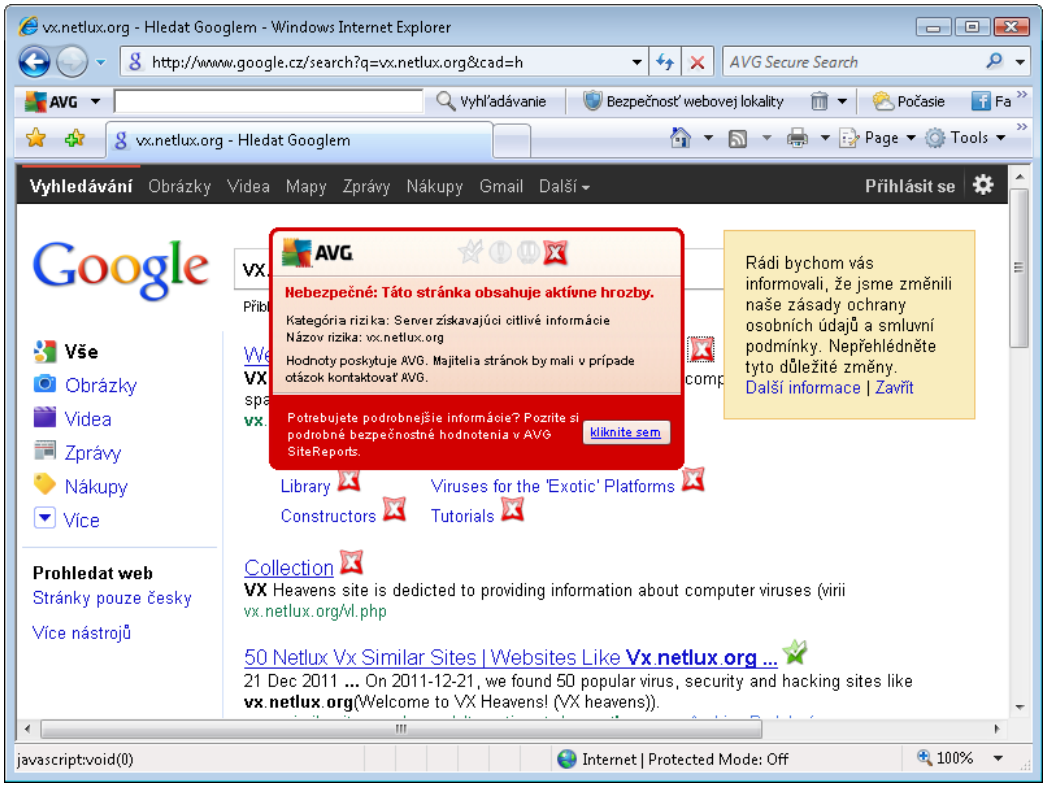
Nastavením kurzora nad jednotlivé ikony hodnotenia sa zobrazia podrobnosti o príslušnom odkaze. Informácie obsahujú ďalšie podrobnosti o hrozbe (*ak sú dostupné*):



6.2.3. Nálezy súčasti Surf-Shield

Táto účinná ochrana zablokuje škodlivý kód každej webovej stránky, ktorú sa pokúšate otvoriť a zabráni jeho prevzatiu do počítača. Ak je táto funkcia zapnutá a kliknete na odkaz alebo zadáte adresu URL nebezpečných stránok, funkcia automaticky zablokuje otvorenie týchto webových stránok, aby vás chránila pred náhodným infikovaním. Je dôležité mať na pamäti, že nebezpečné webové lokality môžu infikovať váš počítač tak, že ich navštívite. Keď sa teda pokúsite otvoriť nebezpečné webové lokality so škodlivým kódom a inými závažnými hrozbami, súčasť LinkScanner neumožní prehliadaču, aby tieto stránky zobrazil.

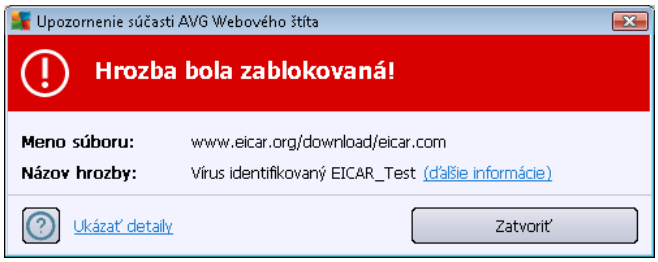
Ak narazíte na škodlivú webovú lokalitu, nástroj LinkScanner vás upozorní zobrazením podobnej obrazovky:



Otvorenie tejto webovej lokality predstavuje vysoké riziko a neodporúča sa!

6.2.4. Nálezy súčasti Webový štít

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

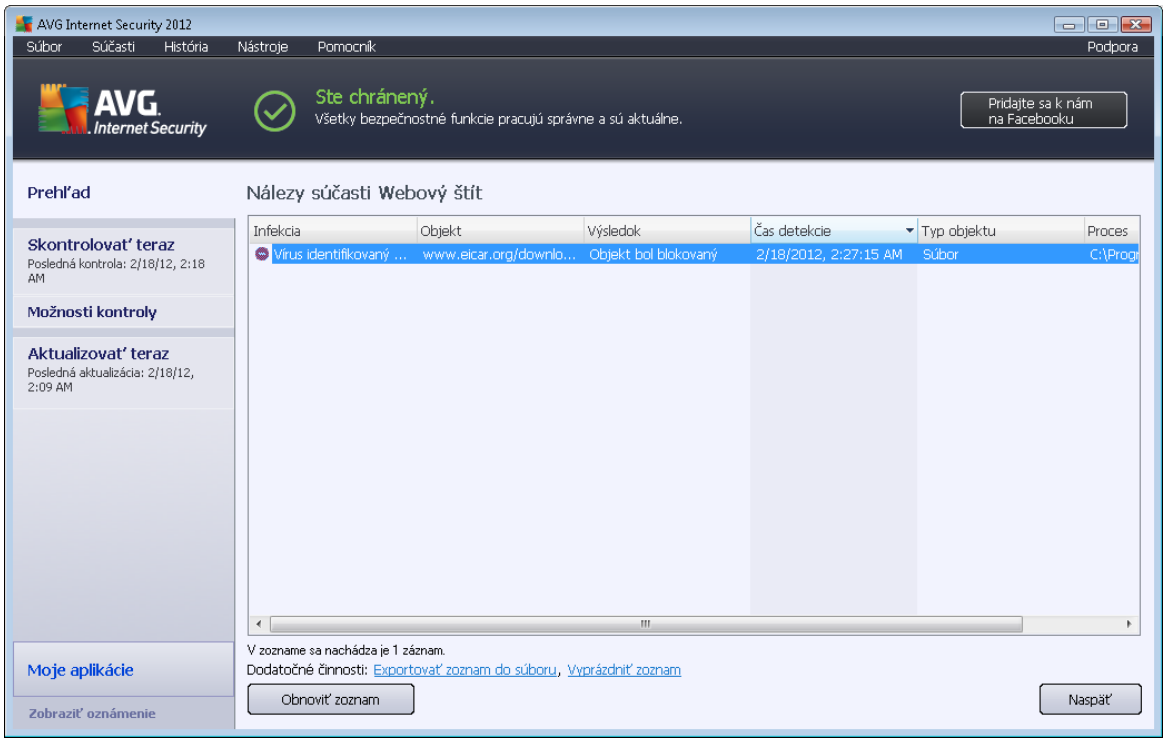


V tomto dialógovom okne sa nachádzajú informácie o súbore, ktorý bol zistený a označený ako infikovaný (*Názov súboru*), názov rozpoznanej infekcie (*Názov hrozby*) a odkaz na Encyklopédiu vírusov s podrobnými informáciami o zistenej infekcii, ak je známa (*Ďalšie informácie*). V tomto dialógovom okne sa nachádzajú tieto tlačidlá:

- ***Zobraziť podrobnosti*** – kliknutím na tlačidlo ***Zobraziť podrobnosti*** otvorte nové prekrývacie okno s informáciami o procese, ktorý bol spustený v čase detekovania infekcie, a identifikáciou procesu.

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

Podozrivá internetová stránka sa neotvorí a detekovaná hrozba sa zaznamená v zozname ***nálezov súčasti Webový štít*** – tento prehľad detekovaných hrozieb sa otvára v hlavnej ponuke História/ Nálezy súčasti Webový štít.



Pre každý detekovaný objekt sa zobrazia tieto informácie:

- ***Infekcia*** – opis (*prípadne aj názov*) detekovaného objektu.
- ***Objekt*** – zdroj objektu (*internetová stránka*).
- ***Výsledok*** – akcia urobená na detekovanom objekte.
- ***Čas detekovania*** – dátum a čas detekovania a zablokovania hrozby.
- ***Typ objektu*** – typ detekovaného objektu.
- ***Proces*** – aká akcia sa vykonala na zavolanie potenciálne nebezpečného objektu, aby sa dal detekovať.

V spodnej časti dialógového okna pod zoznamom sa nachádzajú informácie o celkovom počte detekovaných objektov. Ďalej môžete exportovať celý zoznam detekovaných objektov do súboru (***Exportovať zoznam do súboru***) a vymazať všetky záznamy o detekovaných objektoch (***Vyprázdniť zoznam***).

Ovládacie tlačidlá

- ***Obnoviť zoznam*** – Aktualizuje sa zoznam nálezov zistených súčasťou ***Webový štít***
- ***Späť*** – znovu otvorí implicitné hlavné dialógové okno programu AVG *(prehľad súčastí).*

6.3. Ochrana e-mailu

Jeden z najbežnejších zdrojov vírusov a trójskych koňov je email. Ohrozenia typu phishing a spam ďalej zvyšujú riziko emailu. Bezplatné e-mailové účty sú náchylnejšie na prijímanie takýchto škodlivých e-mailov (*pretože málokedy využívajú technológiu na ochranu pred spamom*) a domáci používatelia sa v pomerne veľkej miere spoliehajú na tieto e-mailové schránky. Domáci používatelia, ktorí surfujú po neznámych stránkach a do online formulárov vypĺňajú osobné údaje (*napr. e-mailové adresy*), sú vo zvýšenej miere vystavení útokom cez e-mail. Spoločnosti obyčajne využívajú hromadné emailové účty a používajú antispamové filtre, atď., aby toto riziko znížili.

Súčasť ***Ochrana e-mailu*** sa stará o kontrolu jednotlivých doručených alebo odoslaných e-mailových správ, a vždy, keď zistí prítomnosť vírusu, ihneď presunie správu do vírusového trezora. Táto súčasť dokáže zároveň filtrovať niektoré typy e-mailových príloh a priložiť text osvedčenia k správam bez infekcie. Funkciu ***Ochrana e-mailu*** tvoria dve hlavné funkcie:

- Kontrola pošty
- Anti-Spam

6.3.1. Kontrola pošty

Osobná Kontrola pošty automaticky kontroluje prichádzajúce a odchádzajúce e-maily. Môže sa používať s poštovými aplikáciami, ktoré nemajú vlastný zásuvný modul v programe AVG (*zároveň sa môže používať aj na kontrolu e-mailových správ v poštových aplikáciách, s ktorými AVG spolupracuje pomocou špeciálneho zásuvného modulu – napr. Microsoft Outlook, The Bat a Mozilla Thunderbird*). Primárne je určený pre poštové aplikácie ako sú Outlook Express, Incredimail atď.

Počas inštalácie programu sa vytvoria automatické servery na kontrolu e-mailov: jeden na kontrolu prichádzajúcich e-mailov a druhý na kontrolu odchádzajúcich e-mailov. Pomocou týchto dvoch serverov sa e-maily automaticky kontrolujú na portoch 110 a 25 (*štandardné porty pre posielanie a prijímanie e-mailov*).

Kontrola pošty pôsobí ako rozhranie medzi poštovou aplikáciou a poštovými servermi na internete.

- ***Prichádzajúca pošta:*** Počas prijímania správy zo servera testuje súčasť ***Kontrola pošty*** správu z hľadiska prítomnosti vírusov, odstráni infikované prílohy a pridá certifikáciu. Zistené vírusy sa ihneď uložia do karantény do vírusového trezora. Správa sa potom pošle do poštovej aplikácie.
- ***Odchádzajúca pošta:*** Správa sa pošle z poštovej aplikácie do súčasti Kontrola pošty, ktorá otestuje samotnú správu a jej prílohy z hľadiska výskytu vírusov, a potom ju pošle na server SMTP (*kontrola odchádzajúcich e-mailov je štandardne vypnutá a môže sa nastaviť ručne*).

Súčasť Kontrola pošty nie je určená pre serverové platformy.

6.3.2. Anti-Spam

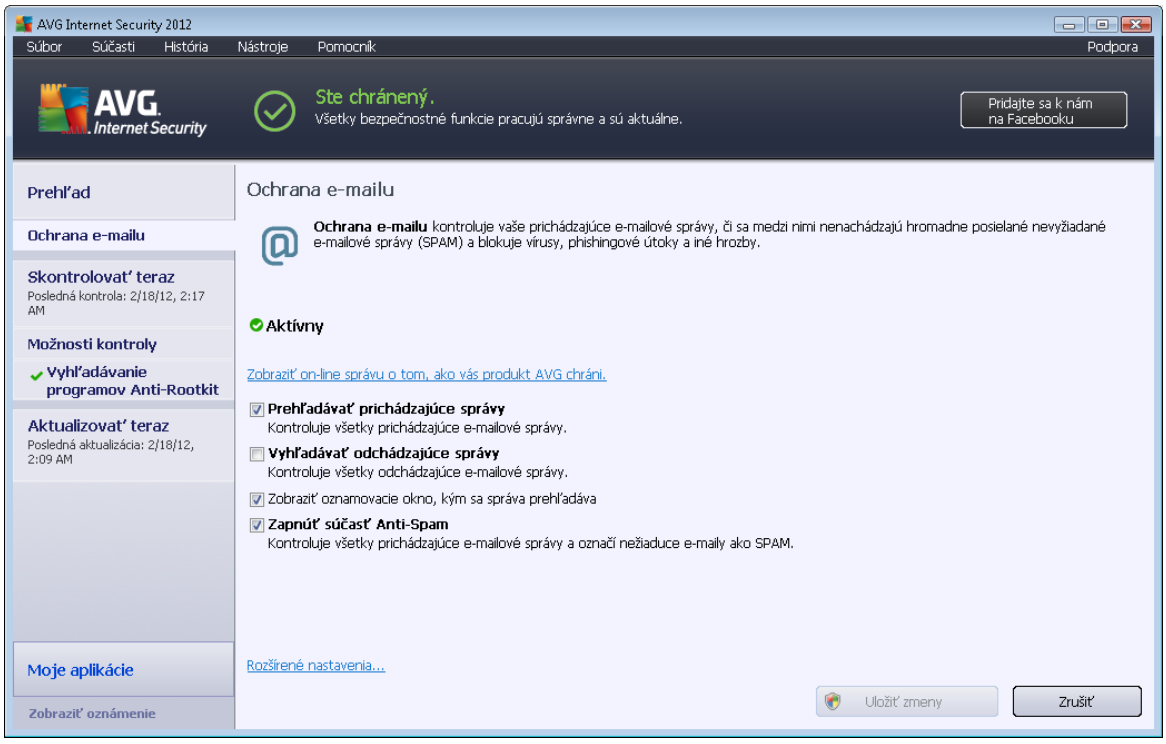
Ako funguje súčasť Anti-Spam?

Súčasť Anti-Spam kontroluje všetky prichádzajúce e-mailové správy a označí nežiaduce e-maily ako spam. ***Anti-Spam*** dokáže zmeniť predmet e-mailovej správy (*ktorá bola označená ako spam*) pridaním špeciálneho textového reťazca. Môžete filtrovať e-mailové správy v poštovej aplikácii. ***Súčasť Anti-Spam*** používa niekoľko metód analýzy na spracovanie jednotlivých e-mailových správ a prináša najvyššiu možnú úroveň ochrany pred nevyžiadanými e-mailovými správami. ***Súčasť Anti-Spam*** používa pravidelne aktualizovanú databázu na zisťovanie 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 neoznačiť ako spam*) a zoznamu blokovaných (*vždy označiť ako spam*) adries.

Čo je to spam?

Spam označuje nevyžiadané e-mailové správy, väčšinou propagujúce výrobok alebo službu, ktoré sa hromadne rozosielajú na veľký počet e-mailových adries a zapĺňajú poštové schránky prijímateľov. Spam neoznačuje legitímne komerčné e-maily, s ktorých prijímaním zákazníci poskytli súhlas. Spam je nielen otravný, ale niekedy môže byť aj zdrojom podvodov, vírusov alebo môže obsahovať urážlivé informácie.

6.3.3. Rozhranie súčasti Ochrana e-mailu



V dialógovom okne súčasti ***Ochrana e-mailu*** sa nachádza stručný text opisujúci fungovanie súčasti a informácie o jej aktuálnom stave (*aktívna).* Pomocou prepojenia ***Zobraziť on-line správu o ochrane aplikáciou AVG*** zobrazíte na príslušnej webovej lokalite (http://www.avg.com/) podrobnú štatistiku činnosti a zistenia aplikácie **AVG Internet Security 2012.**

Základné nastavenia súčasti Ochrana e-mailu

V dialógovom okne ***Ochrana e-mailu*** môžete upraviť ďalšie základné vlastnosti súčasti:

- ***Kontrolovať prichádzajúce správy*** *(štandardne zapnuté)* – Začiarknite toto políčko, ak sa má kontrolovať prítomnosť vírusov vo všetkých e-mailoch doručených do vašej e-mailovej schránky.
- ***Kontrolovať odchádzajúce správy*** *(štandardne vypnuté)* – Začiarknite toto políčko, ak sa má kontrolovať prítomnosť vírusov vo všetkých e-mailoch odoslaných z vášho e-mailového účtu.
- ***Zobraziť oznamovacie okno počas kontroly e-mailov*** *(štandardne zapnuté)* – Začiarknite túto možnosť, ak chcete byť informovaní otvorením oznamovacieho dialógového okna nad ikonou AVG na paneli úloh počas kontroly elektronickej pošty.
- ***Povoliť Anti-Spam*** *(štandardne zapnuté)* – Označením položky určíte, či chcete z prichádzajúcej pošty filtrovať nevyžiadané správy.

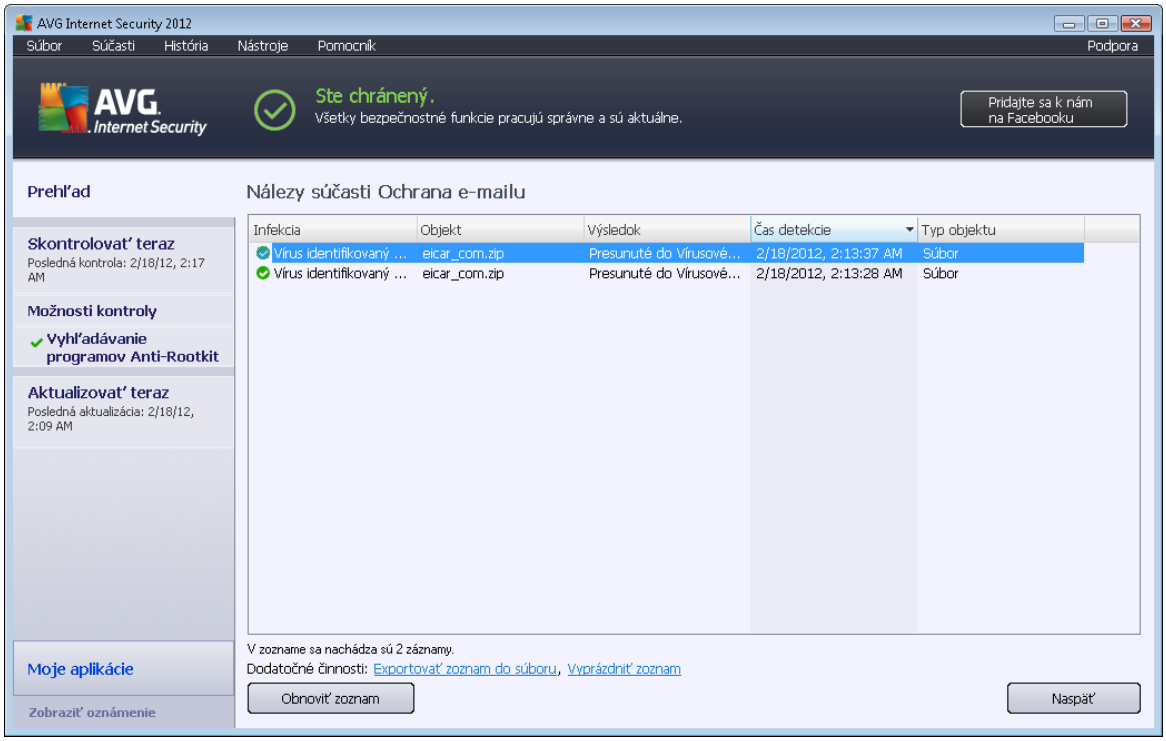
Dodávateľ softvéru nastavil všetky súčasti AVG tak, aby fungovali optimálnym spôsobom. Nemeňte konfiguráciu programu AVG, ak na to nemáte skutočný dôvod. Zmeny nastavení odporúčame robiť len skúseným používateľom. Ak chcete zmeniť konfiguráciu programu AVG, vyberte položku Nástroje/Rozšírené nastavenia v hlavnej ponuke programu a zmeňte konfiguráciu v novom dialógovom okne Rozšírené nastavenia programu AVG.

Ovládacie tlačidlá

V dialógovom okne ***Ochrana e-mailu*** sa nachádzajú tieto ovládacie tlačidlá:

- ***Uložiť zmeny*** – Stlačením tohto tlačidla sa uložia a použijú všetky zmeny uskutočnené v tomto dialógovom okne.
- ***Zrušiť*** – Stlačením tohto tlačidla sa znova otvorí implicitné hlavné dialógové okno AVG (*prehľad súčastí*)

6.3.4. Nálezy súčasti Kontrola pošty



V dialógovom okne ***Nálezy súčasti Kontrola pošty*** *(otvára sa pomocou možnosti História/Nálezy súčasti Kontrola pošty)* sa zobrazí zoznam všetkých hrozieb zistených súčasťou Ochrana e-mailu**.** Pre každý detekovaný objekt sú k dispozícii tieto informácie:

- ***Infekcia*** – opis (prípadne aj názov) detekovaného objektu.
- ***Objekt*** – umiestnenie objektu.
- ***Výsledok*** – akcia urobená na detekovanom objekte.
- ***Čas detekovania*** – dátum a čas detekovania podozrivého objektu.
- ***Typ objektu*** – typ detekovaného objektu.

V spodnej časti dialógového okna pod zoznamom sa nachádzajú informácie o celkovom počte detekovaných objektov. Ďalej môžete exportovať celý zoznam detekovaných objektov do súboru (***Exportovať zoznam do súboru***) a vymazať všetky záznamy o detekovaných objektov (***Vyprázdniť zoznam***).

Ovládacie tlačidlá

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

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

- ***Späť*** – Prepne sa späť na predchádzajúce dialógové okno.

6.4. Firewall

Firewall je systém, ktorý presadzuje zásady riadenia prístupu medzi dvoma alebo viacerými sieťami blokovaním resp. povolením prenosov. ***Firewall*** obsahuje súbor pravidiel, ktoré chránia internú sieť pred útokmi zvonku *(zvyčajne z Internetu)* a riadi komunikáciu na každom sieťovom porte. Komunikácia sa vyhodnotí podľa definovaných pravidiel a potom sa buď povolí, alebo zakáže. Keď brána ***Firewall*** zistí pokus o preniknutie do systému, zablokuje ho a nedovolí narušiteľovi vstúpiť do počítača.

Súčasť Firewall je nastavená tak, aby umožňovala alebo blokovala internú alebo externú komunikáciu (oboma smermi, dnu aj von) na definovaných portoch a pre definované softvérové aplikácie. Brána firewall sa môže nastaviť napríklad tak, aby umožňovala tok webových dát smerom dnu a von, len keď sa používa program Microsoft Explorer. Každý pokus o prenos webových dát iným prehliadačom sa zablokuje.

Brána ***Firewall*** bráni odoslaniu informácií, ktoré vás môžu osobne identifikovať, z počítača bez vášho povolenia. Kontroluje spôsob, akým si počítač vymieňa dáta s ostatnými počítačmi na internete alebo v miestnej sieti. V rámci organizácie brána ***Firewall*** chráni samostatné počítače pred útokmi interných používateľov na ostatné počítače v sieti.

Počítače, ktoré nie sú chránené bránou Firewall, bývajú ľahkým terčom počítačových hackerov a páchateľov trestnej činnosti v oblasti odcudzenia údajov.

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

6.4.1. Princíp fungovania súčasti Firewall

V aplikácii **AVG Internet Security 2012** ovláda súčasť ***Firewall*** celú aktivitu na každom sieťovom porte počítača. ***Súčasť 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. Pri každej z týchto aplikácií súčasť ***Firewall*** povolí alebo zakáže komunikáciu na sieťových portoch. Ak je aplikácia neznáma *(teda nemá žiadne vymedzené pravidlá súčasti Firewall)*, súčasť ***Firewall*** sa vás štandardne spýta, či chcete tento pokus o komunikáciu zablokovať alebo povoliť.

Súčasť AVG Firewall nie je určená pre serverové platformy!

Čo dokáže AVG Firewall:

- Povoliť alebo blokovať komunikačné pokusy známych aplikácií automaticky alebo vás požiadať o potvrdenie
- Použiť úplné profily s vopred definovanými pravidlami, podľa vašich potrieb.

- Prepnúť profily automaticky, keď sa pripájate na rôzne siete alebo používate rôzne sieťové karty.

6.4.2. Profily súčasti Firewall

Firewall umožňuje definovať konkrétne bezpečnostné pravidlá podľa toho, či sa počítač nachádza v doméne, alebo či ide o samostatný počítač alebo dokonca notebook. Každá z týchto možností si vyžaduje inú úroveň ochrany a jednotlivé úrovne patria do príslušných profilov. Povedané v skratke, profil súčasti Firewall je špeciálna konfigurácia súčasti Firewall a program umožňuje použiť niekoľko takýchto vopred definovaných konfigurácií.

Definované profily

- ***Povoliť všetky*** – Systémový profil súčasti Firewall, ktorý vopred nastavil výrobca, a ktorý je vždy prítomný. Keď je tento profil aktivovaný, celá sieťová komunikácia je povolená a neuplatňujú sa žiadne pravidlá bezpečnostnej politiky, ako keby bola ochrana Firewall vypnutá (t. j. všetky aplikácie sú povolené, ale pakety sa stále kontrolujú – na úplné vypnutie filtrovania je potrebné vypnúť súčasť Firewall). Tento systémový profil sa nedá kopírovať, odstrániť a jeho nastavenia sa nedajú meniť.

- ***Blokovať všetky*** – Systémový profil súčasti Firewall, ktorý vopred nastavil výrobca, a ktorý je vždy prítomný. Keď je tento profil aktivovaný, každá sieťová komunikácia sa zablokuje, počítač je nedostupný z vonkajších sietí ani nemôže komunikovať smerom von. Tento systémový profil sa nedá kopírovať, odstrániť a jeho nastavenia sa nedajú meniť.

- ***Vlastné profily*** – Vlastné profily umožňujú využívať výhody funkcie automatického prepínania profilov, ktorá je užitočná najmä v prípade, keď sa často pripájate k rôznym sieťam *(napr. s notebookom)*. Vlastné profily sa vytvárajú automaticky po inštalácii programu **AVG Internet Security 2012** a pokrývajú jednotlivé potreby z hľadiska pravidiel zásad súčasti Firewall. Dostupné sú tieto vlastné profily:

  - ***Priamo pripojené na internet*** – vhodné pre bežné domáce pracovné počítače alebo notebooky priamo pripojené na internet bez dodatočnej ochrany. Táto možnosť je vhodná aj vtedy, keď notebook pripájate k rôznym neznámym a potenciálne nebezpečným sieťam (*napr. v internetovej kaviarni, hotelovej izbe a pod.*). Najprísnejšie pravidlá politiky súčasti Firewall definované v tomto profile zaisťujú adekvátnu ochranu počítača.

  - ***Počítač s doménou*** – vhodné pre počítače v miestnej sieti, zvyčajne v škole alebo v zamestnaní. Predpokladá sa, že sieť je odborne spravovaná a chránená ďalšími prostriedkami, aby sa mohla použiť nižšia úroveň zabezpečenia ako v uvedených prípadoch a umožnil sa prístup ku zdieľaným priečinkom, diskom a pod.

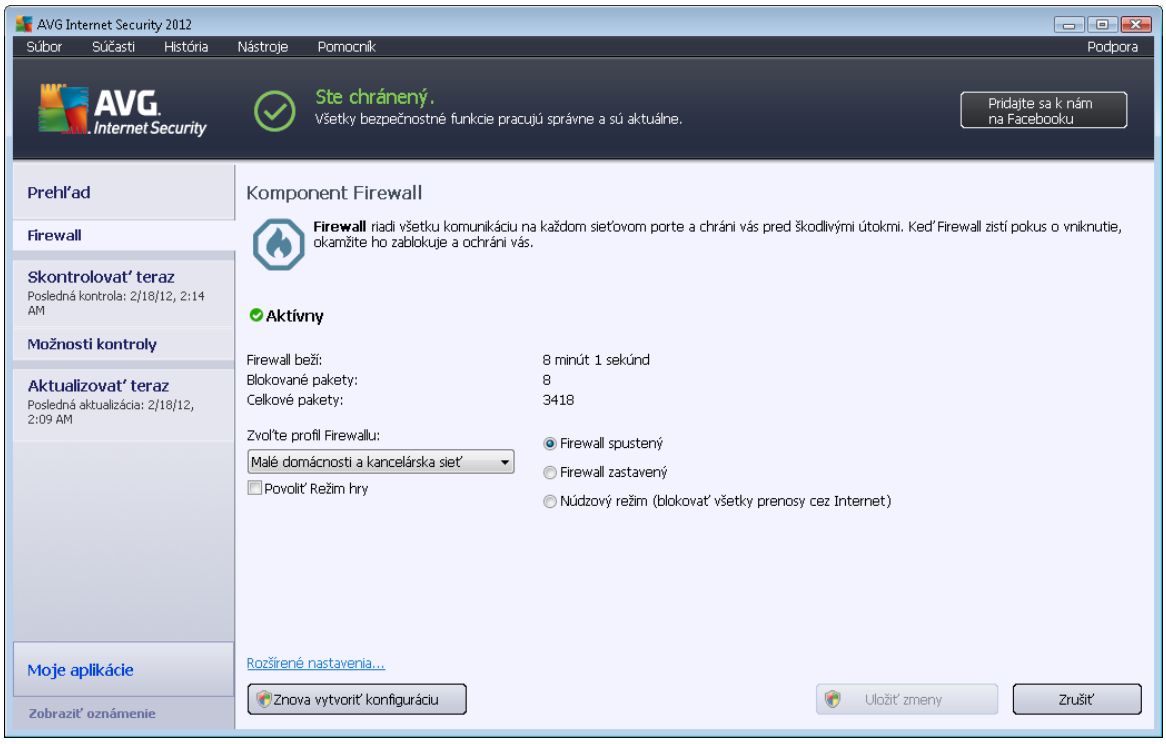
  - ***Malá domáca alebo kancelárska*** – vhodné pre počítače v malej sieti, napr. domácnosti alebo malom podniku. Takáto siete zvyčajne nemá žiadneho „centrálneho“ správcu a tvorí ju niekoľko prepojených počítačov, ktoré často využívajú spoločnú tlačiareň, skener alebo podobné zariadenie, čo musia pravidlá súčasti Firewall zohľadniť.

Prepínanie profilov

Funkcia Prepínanie profilov umožňuje súčasti Firewall automaticky prepnúť na definovaný profil pri použití konkrétnej sieťovej karty, alebo keď je počítač pripojený ku konkrétnemu typu siete. Ak nebol sieťovej oblasti doposiaľ pridelený žiaden profil, pri ďalšom pripojení k tejto oblasti otvorí súčasť Firewall dialógové okno, ktorým vás požiada o pridelenie profilu. Dialógové okno Profily oblastí a sieťových kariet umožňuje prideliť profily rozhraniam všetkých miestnych sietí alebo oblastí a definovať ďalšie nastavenia. Zároveň umožňuje vypnúť túto funkciu, keď ju nechcete používať (*potom sa pri každom type pripojenia použije predvolený profil*).

Túto funkciou používajú zvyčajne používatelia, ktorí vlastnia notebook a používajú rôzne typy pripojenia. Ak vlastníte stolový počítač a používate len jeden typ pripojenia (*napr. káblové pripojenie na internet*), nemusíte si robiť starosti s prepínaním profilov, pretože ho zrejme nikdy nevyužijete.

6.4.3. Rozhranie súčasti Firewall



Hlavné dialógové okno s názvom ***Komponent Firewall*** obsahuje niektoré základné informácie o funkcii komponentu, jeho stav *(aktívny)* a stručný štatistický prehľad o komponente:

- ***Súčasť Firewall je zapnutá*** – čas, ktorý uplynul od spustenia súčasti Firewall
- ***Blokované pakety*** – počet blokovaných paketov z celkového počtu kontrolovaných paketov.
- ***Celkové pakety*** – počet paketov skontrolovaných počas spustenia súčasti Firewall

Základné nastavenia súčasti Firewall

- ***Zvoľte profil brány Firewall*** – z rozbaľovacej ponuky vyberte jeden z definovaných profilov (*podrobný opis všetkých profilov a odporúčané použitie nájdete v kapitole Profily súčasti Firewall*)

- ***Zapnúť režim hrania*** – Toto políčko označte, keď chcete, aby v prípade otvorenia aplikácií na celú obrazovku (*(hier, prezentácií, filmov a pod.*), súčasť Firewall nezobrazovala dialógové okná s otázkou, či chcete povoliť alebo blokovať komunikáciu neznámym aplikáciám. Ak sa neznáma aplikácia pokúsi komunikovať v sieti v danom čase, súčasť Firewall automaticky povolí alebo zablokuje tento pokus podľa nastavení aktuálneho profilu. ***Poznámka:*** V režime hrania sa všetky naplánované úlohy (kontroly, aktualizácie) odložia do zatvorenia aplikácie.

- V tejto časti so základnými nastaveniami si môžete vybrať z troch alternatívnych možností určenia aktuálneho stavu komponentu Firewall:

    - ***Súčasť Firewall zapnutá*** *(štandardne)* – Túto možnosť vyberte, keď chcete povoliť komunikáciu tým aplikáciám, ktoré sú definované ako „povolené“ v skupine pravidiel definovaných vo vybranom profile súčasti Firewall.

    - ***Súčasť Firewall vypnutá*** – táto možnosť úplne vypne Firewall, všetky sieťové prenosy sa povolia, ale nebudú sa kontrolovať!

    - ***Núdzový režim (blokovať všetky internetové prenosy)*** – Túto možnosť vyberte na zablokovanie jednotlivých sieťových portov. Brána Firewall naďalej beží, ale všetky sieťové prenosy sú zastavené.

Poznámka: *Výrobca softvéru nastavil všetky súčasti produktu AVG Internet Security 2012 tak, aby dosahovali optimálny výkon. Nemeňte konfiguráciu AVG, ak na to nemáte skutočný dôvod. Vykonávať zmeny nastavení sa odporúčajú len skúseným používateľom. Keď potrebujete zmeniť konfiguráciu súčasti Firewall, vyberte položku* ***Nástroje/Nastavenia súčasti Firewall*** *v hlavnej ponuke programu a zmeňte konfiguráciu súčasti Firewall v novo otvorenom dialógovom okne Nastavenia súčasti Firewallu.*

Ovládacie tlačidlá

- ***Obnoviť konfiguráciu*** – stlačením tohto tlačidla sa prepíše používaná konfigurácia súčasti Firewall a obnoví sa predvolená konfigurácia na základe automatickej detekcie.

- ***Uložiť zmeny*** – Po stlačení tohto tlačidla sa uložia a uplatnia všetky zmeny, ktoré sa uskutočnili v tomto dialógovom okne.

- ***Zrušiť*** – Stlačením tohto tlačidla sa znova otvorí implicitné hlavné dialógové okno AVG (*prehľad súčastí*)

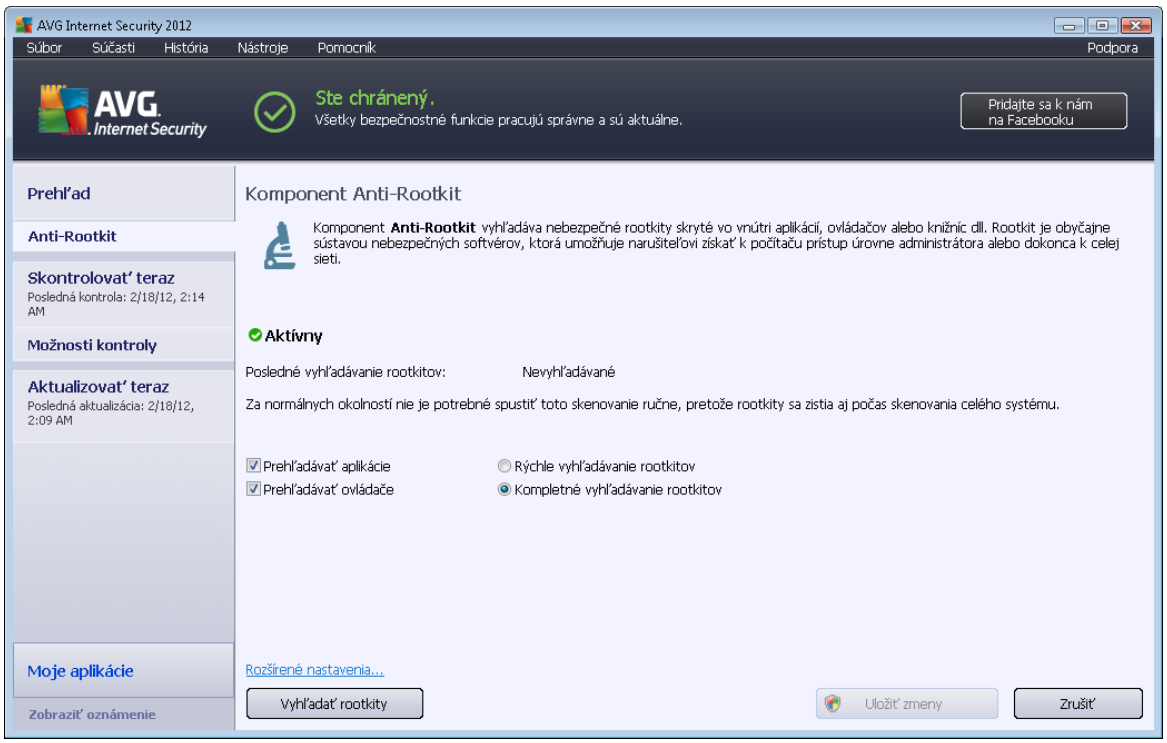
6.5. Anti-Rootkit

Anti-Rootkit je špeciálny nástroj, ktorý zisťuje a efektívne odstraňuje nebezpečné programy rootkit, teda programy a technológie, ktoré môžu zakrývať prítomnosť škodlivého softvéru v počítači. ***Súčasť Anti-Rootkit*** dokáže zistiť prítomnosť programov rootkit pomocou vopred definovanej skupiny pravidiel. Upozorňujeme, že súčasť zistí prítomnosť všetkých programov rootkit *(nielen infikovaných)* . Ak súčasť ***Anti-Rootkit*** nájde program rootkit, nemusí to nevyhnutne znamenať, že je tento program infikovaný. Programy rootkit sa niekedy používajú ako ovládače, príp. tvoria súčasť správnych aplikácií.

Čo je to rootkit?

Rootkit je program, ktorý sa používa na prevzatie základnej kontroly nad počítačovým systémom bez súhlasu vlastníka počítača a jeho právoplatných správcov. Prístup k hardvéru sa väčšinou nepožaduje, pretože účelom rootkitu je zmocniť sa kontroly nad operačným systémom spusteným na hardvéri. Rootkity zvyčajne maskujú svoju prítomnosť v systéme rozvratnou činnosťou, alebo vyhýbaním sa štandardným bezpečnostným mechanizmom operačného systému. Často ide aj o trójske kone, ktoré klamlivo presvedčia používateľov, že sa môžu bezpečne spustiť na počítači. Medzi metódy používané na dosiahnutie tohto cieľa patria utajenie spustených procesov pred sledovacími programami, alebo skrývanie súborov alebo systémových dát pred operačným systémom.

6.5.1. Rozhranie súčasti Anti-Rootkit



Dialógové okno súčasti ***Anti-Rootkit*** stručne opisuje fungovanie súčasti, informuje o momentálnom stave súčasti *(aktívny)*, ako aj o čase, kedy bol naposledy spustený test s nástrojom ***Anti-Rootkit*** (

posledné vyhľadávanie programov rootkit; test rootkitov je štandardný proces spustený v rámci Kontroly celého počítača). V dialógovom okne ***Anti-Rootkit*** sa ďalej nachádza odkaz na nástroje/rozšírené nastavenia. Použite odkaz na otvorenie prostredia s rozšírenou konfiguráciou súčasti ***Anti-Rootkit***.

Dodávateľ softvéru nastavil všetky súčasti AVG tak, aby fungovali optimálnym spôsobom. Nemeňte konfiguráciu AVG, ak na to nemáte skutočný dôvod. Zmenu nastavení by mali robiť len skúsení používatelia.

Základné nastavenia súčasti Anti-Rootkit

V spodnej časti dialógového okna môžete nastaviť niektoré základné funkcie vyhľadávania prítomnosti programov rootkit. Najskôr začiarknutím príslušných okienok definujte objekty, ktoré sa majú kontrolovať:

- ***Kontrolovať aplikácie***
- ***Kontrolovať ovládače***

Ďalej môžete vybrať režim vyhľadávania rootkitov:

- ***Rýchle vyhľadávanie programov rootkit*** – kontroluje všetky spustené procesy, zavedené ovládače a systémový priečinok (*zvyčajne c:\Windows*).
- ***Úplné vyhľadávanie programov rootkit*** – kontroluje všetky spustené procesy, zavedené ovládače, systémový priečinok (*zvyčajne c:\Windows*), ako aj všetky miestne disky (*vrátane pamäťových médií, nie však disketové jednotky/jednotky CD–ROM*).

Ovládacie tlačidlá

- ***Vyhľadávať programy rootkit*** – Keďže vyhľadávanie programov rootkit nie je integrovanou súčasťou funkcie Kontrola celého počítača, vyhľadávanie programov rootkit môžete spustiť priamo v rozhraní ***Anti-Rootkit*** pomocou tohto tlačidla.
- ***Uložiť zmeny*** – Stlačením tohto tlačidla sa uložia všetky zmeny uskutočnené v tomto rozhraní a otvorí sa implicitné hlavné dialógové okno AVG (*prehľad súčastí*).
- ***Zrušiť*** – Stlačením tohto tlačidla sa znova otvorí implicitné hlavné dialógové okno AVG (*prehľad súčastí*) bez uloženia uskutočnených zmien.

6.6. System Tools

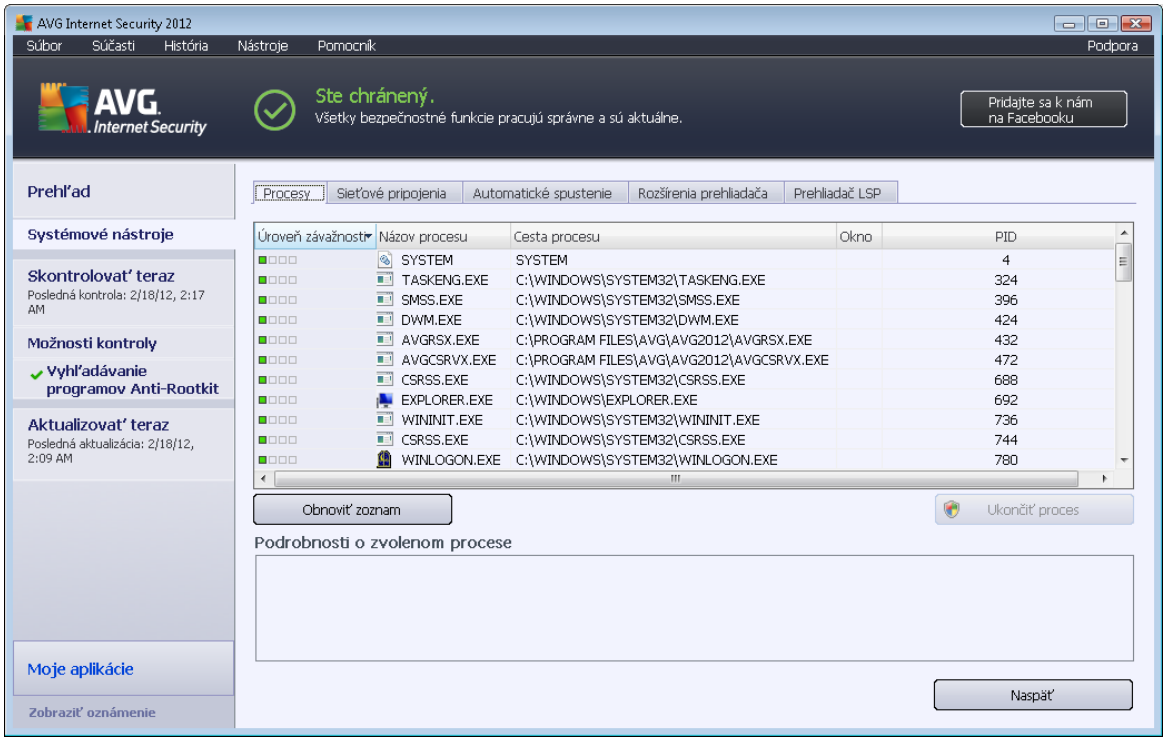
System Tools sú nástroje poskytujúce podrobný prehľad o prostredí produktu **AVG Internet Security 2012 a operačnom systéme.** V tejto súčasti sa nachádza prehľad týchto objektov:

- Procesy – zoznam procesov (*t. j. spustených aplikácií*), ktoré sú momentálne činné v počítači.

- Sieťové pripojenia – zoznam momentálne činných pripojení.
- Automatické spustenie – zoznam aplikácií, ktoré sa spúšťajú pri spustení systému Windows.
- Rozšírenia prehliadača – zoznam zásuvných modulov (*t. j. aplikácií*), ktoré sú nainštalované v internetovom prehliadači.
- Prehliadač LSP – zoznam ovládačov *LSP* (Layered Service Provider).

Jednotlivé prehľady sa dajú aj editovať; toto však odporúčame robiť len veľmi skúseným používateľom!

6.6.1. Procesy



V dialógovom okne ***Procesy*** sa nachádza zoznam procesov (*teda spustených aplikácií*), ktoré sú momentálne činné v počítači. Zoznam je rozdelený na niekoľko stĺpcov:

- ***Úroveň závažnosti*** – grafické znázornenie závažnosti príslušného procesu na stupnici so štyrmi úrovňami od najmenej významnej (■□□□) až po kritickú (■■■■).
- ***Názov procesu*** – názov spusteného procesu
- ***Cesta k procesu*** – fyzická cesta k spustenému procesu.
- ***Okno*** – ak existuje, uvádza názov aplikácie Windows
- ***PID*** – identifikačné číslo procesu je jedinečný interný identifikátor procesu operačného

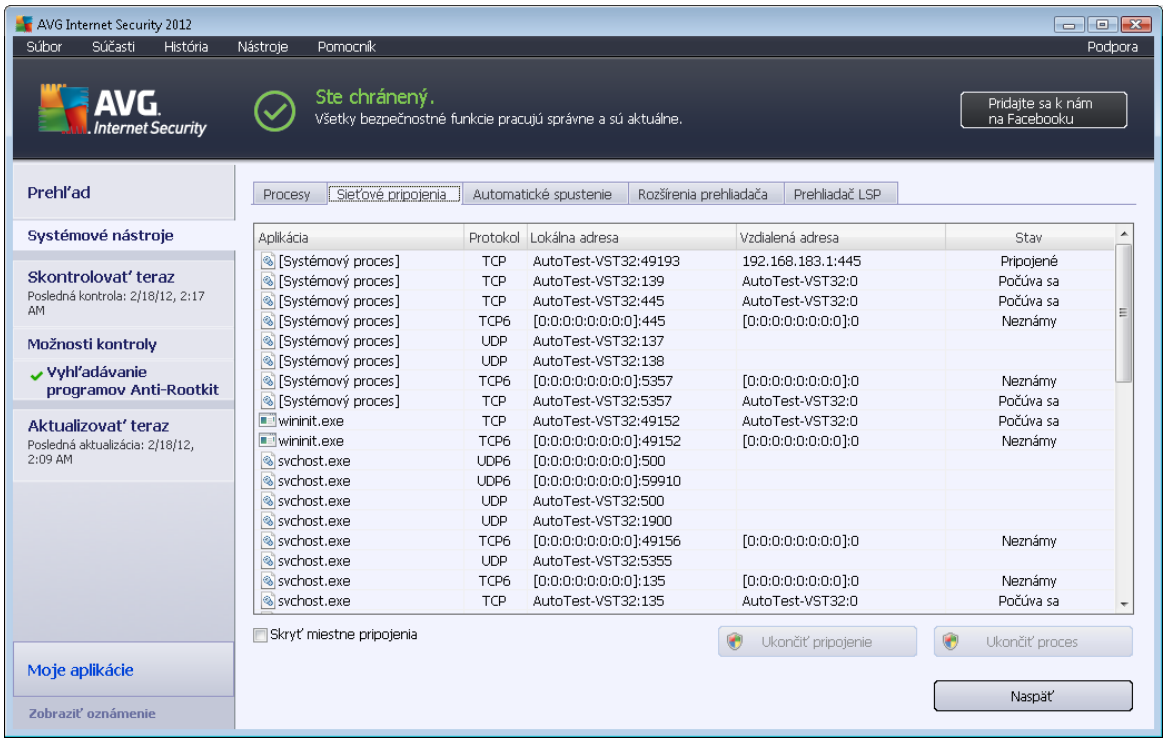
systému Windows.

Ovládacie tlačidlá

Na karte ***Procesy*** sú k dispozícii nasledujúce ovládacie tlačidlá:

- ***Obnoviť*** – aktualizuje zoznam procesov podľa momentálneho stavu.
- ***Ukončiť proces*** – môžete vybrať jednu alebo niekoľko aplikácií, a potom ich ukončiť stlačením tohto tlačidla. ***Odporúčame vám, aby ste neukončili žiadnu aplikáciu, ak si nie ste stopercentne istý, že predstavuje skutočnú hrozbu!***
- ***Späť*** – Vráti sa späť do implicitného hlavného dialógového okna AVG (*prehľad súčastí*).

6.6.2. Sieťové pripojenia



V dialógovom okne ***Sieťové pripojenia*** sa nachádza zoznam momentálne vytvorených pripojení. Zoznam je rozdelený na tieto stĺpce:

- ***Aplikácia*** – názov aplikácie súvisiacej s pripojením (*okrem operačných systémov Windows 2000, v ktorých tieto informácie nie sú k dispozícii*)
- ***Protokol*** – typ prenosového protokolu použitého na vytvorenie pripojenia:
  - TCP – protokol, ktorý sa používa spolu s internetovým protokolom (IP) na prenos informácií na internete.

- UDP – alternatíva protokolu TCP.

- ***Lokálna adresa*** – adresa IP lokálneho počítača a číslo použitého portu.
- ***Vzdialená adresa*** – adresa IP vzdialeného počítača a číslo portu, na ktorom je vytvorené pripojenie. Podľa možností sa vyhľadá aj hostiteľský názov vzdialeného počítača.
- ***Stav*** – informuje o najpravdepodobnejšom momentálnom stave (*Pripojené, Server sa musí odpojiť, Počúva, Aktívne zatvorenie dokončené, Pasívne zatvorenie, Aktívne zatvorenie*)

Ak chcete zobraziť len externé pripojenia, začiarknite začiarkovacie okienko ***Skryť miestne pripojenia*** v spodnej časti dialógového okna pod zoznamom.

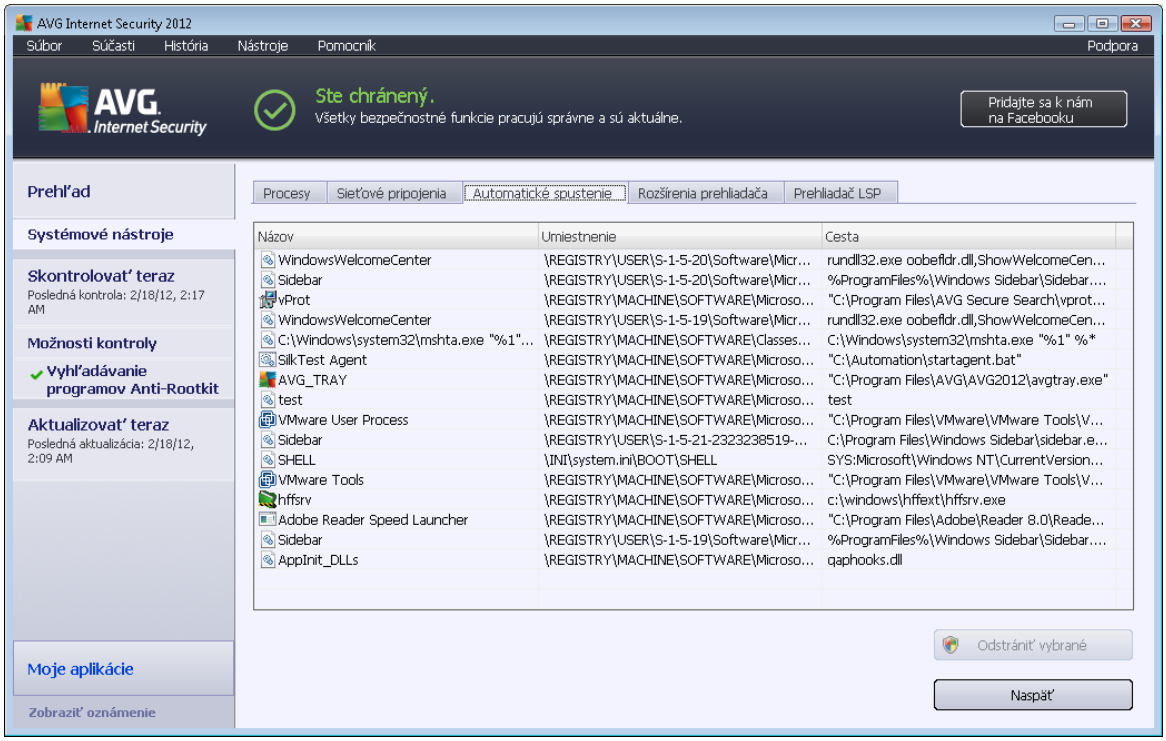
Ovládacie tlačidlá

Na karte ***Sieťové pripojenia*** sú k dispozícii tieto ovládacie tlačidlá:

- ***Ukončiť pripojenie*** – zatvorí jedno alebo viac pripojení vybraných v zozname.
- ***Ukončiť proces*** – zatvorí jednu alebo viac aplikácií súvisiacich s pripojeniami vybranými v zozname.
- ***Späť*** – znovu otvorí implicitné hlavné dialógové okno programu AVG (prehľad súčastí).

Niekedy vám program umožní ukončiť len tie aplikácie, ktoré sú práve pripojené. Odporúčame vám, aby ste neukončovali žiadne pripojenia, ak si nie ste stopercentne istý, že predstavujú skutočnú hrozbu!

6.6.3. Automatické spúšťanie



Dialógové okno ***Automatické spustenie*** zobrazuje zoznam aplikácií, ktoré sa spúšťajú pri spustení systému Windows. Často sa do spúšťacieho registra samovoľne pridá niekoľko aplikácií malware.

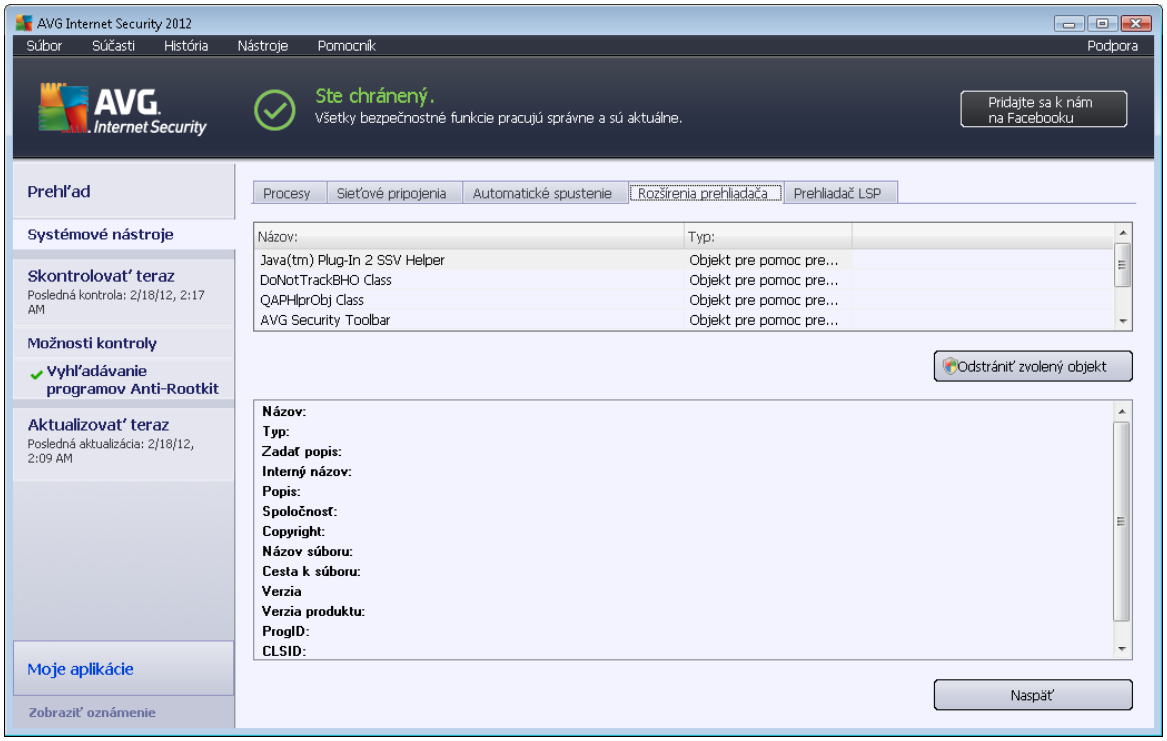
Ovládacie tlačidlá

Na karte ***Automatické spustenie*** sú k dispozícii nasledujúce ovládacie tlačidlá:

- ***Odstrániť označené*** – Stlačením tohto tlačidla odstránite označené položky.
- ***Späť*** – Vráti sa späť do implicitného hlavného dialógového okna AVG *(prehľad súčastí)*.

Odporúčame vám nevymazať žiadne aplikácie zo zoznamu, ak si nie ste stopercentne istí, že predstavujú skutočnú hrozbu!

6.6.4. Rozšírenia prehliadača



V dialógovom okne ***Rozšírenia prehliadača*** sa nachádza zoznam zásuvných modulov (*t. j. aplikácií*), ktoré sú nainštalované vo vašom internetovom prehliadači. V tomto zozname sa môžu nachádzať bežné aplikačné zásuvné moduly a rovnako aj potenciálne škodlivé programy. Po kliknutí na objekt v zozname sa v spodnej časti dialógového okna zobrazia podrobné informácie o vybranom zásuvnom module.

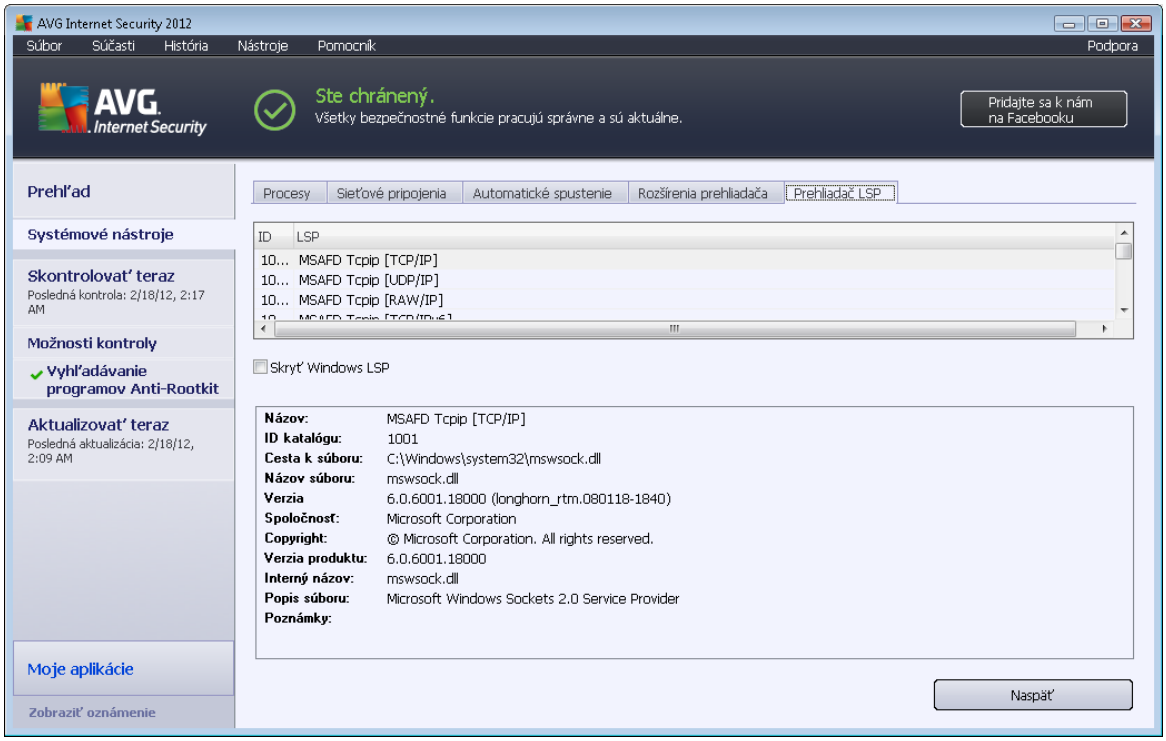
Ovládacie tlačidlá

Na karte ***Rozšírenia prehliadača*** sú k dispozícii tieto ovládacie tlačidlá:

- ***Odstrániť vybraný objekt*** – odstráni zásuvný modul, ktorý je momentálne zvýraznený v zozname. ***Odporúčame vám, aby ste nevymazali žiadne zásuvné moduly zo zoznamu, ak nie ste stopercentne presvedčený, že predstavujú skutočnú hrozbu!***

- ***Späť*** – Vráti späť do implicitného hlavného dialógového okna AVG *(prehľad súčastí).*

6.6.5. Prehliadač LSP



V dialógovom okne ***Prehliadač LSP*** sa nachádza zoznam ovládačov LSP (Layered Service Provider).

LSP (Layered Service Provider) je systémový ovládač, ktorý sa používa so sieťovými službami operačného systému Windows. Má prístup ku všetkým dátam, ktoré vstupujú do a vystupujú z počítača, a zároveň ich dokáže meniť. Niektoré LSP sú potrebné na to, aby umožnili systému Windows pripojiť sa k iným počítačom, vrátane pripojenia na internet. Niektoré škodlivé aplikácie sa však môžu tiež inštalovať ako LSP, a tak získať prístup ku všetkým dátam, ktoré váš počítač prenáša. Preto by vám tieto informácie mohli pomôcť pri kontrole všetkých možných hrozieb súvisiacich s LSP.

Za určitých okolností je možné opraviť poškodený ovládač LSP (*napríklad, keď sa súbor odstránil, ale záznamy databázy Registry zostali nedotknuté*). Keď sa zistí prítomnosť opraviteľného ovládača LSP, zobrazí sa nové tlačidlo, ktoré umožní problém odstrániť.

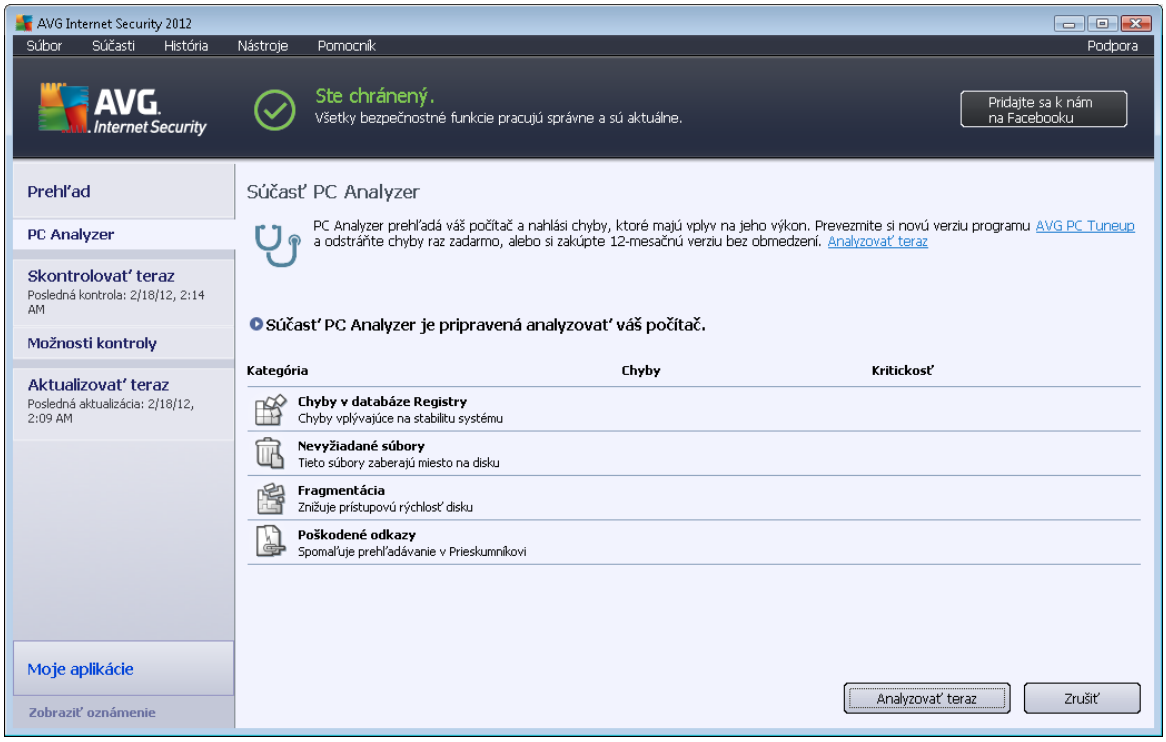
Ovládacie tlačidlá

Na karte ***Zobrazovač LSP*** sú k dispozícii tieto ovládacie tlačidlá:

- ***Skryť Windows LSP*** – Ak chcete vložiť do zoznamu Windows LSP, zrušte označenie tejto položky.
- ***Späť*** – Vráti sa späť do implicitného hlavného dialógového okna aplikácie (*prehľad súčastí*).

6.7. PC Analyzer

Súčasť ***PC Analyzer*** dokáže vyhľadať systémové problémy vášho počítača a zobrazí prehľad toho, čo môže zhoršovať celkový výkon počítača. V používateľskom rozhraní súčasti sa nachádza tabuľka rozdelená na štyri riadky podľa príslušných kategórií: chyby databázy Registry, nežiaduce súbory a poškodené odkazy:



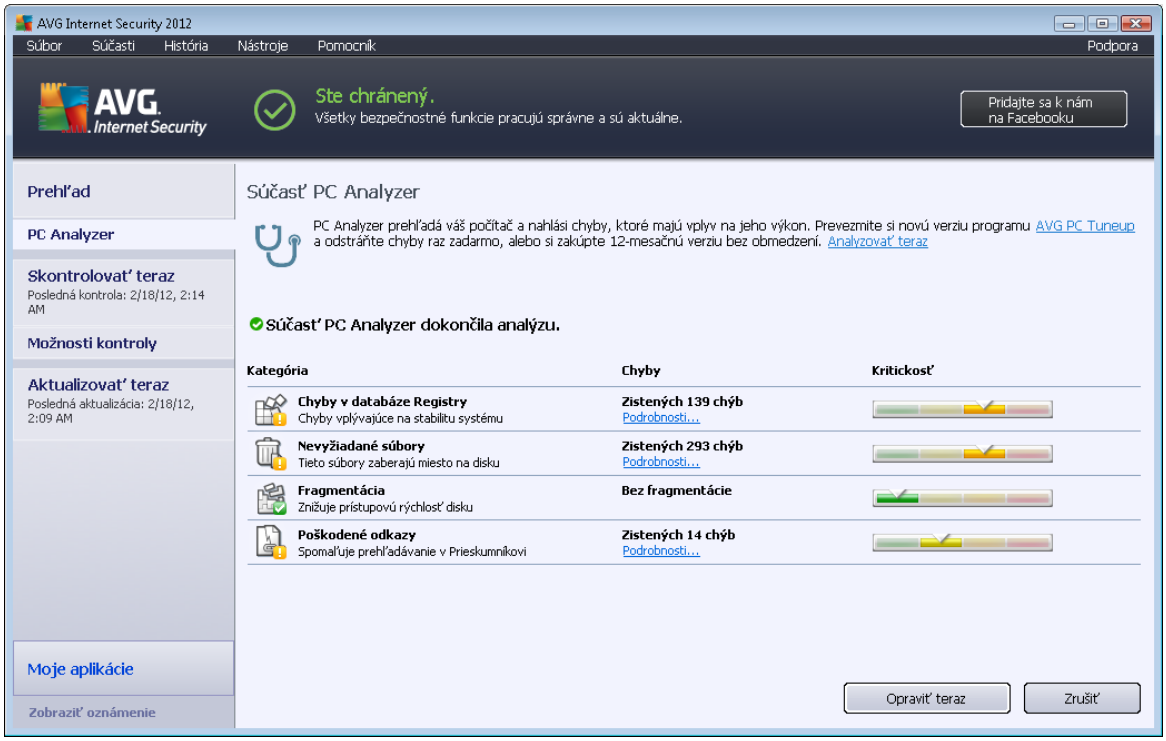
- ***Chyby databázy Registry*** informuje o počte chýb v databáze Registry operačného systému Windows. Keďže na opravenie databázy Registry sú potrebné vedomosti na pomerne vysokej úrovni, neodporúčame vám, aby ste sa ju pokúšali opraviť vlastnými silami.

- ***Nevyžiadané súbory*** informuje o počte súborov, bez ktorých sa s veľkou pravdepodobnosťou zaobídete. Zvyčajne ide o mnohé typy dočasných súborov a súbory v Koši.

- ***Fragmentácia*** vypočíta podiel pevného disku, ktorý je fragmentovaný, t. j. používal sa dlhý čas a väčšina súborov je umiestnená na rôznych miestach fyzického disku. Na odstránenie tohto problémy môžete použiť nástroj na defragmentáciu.

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

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



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

Ovládacie tlačidlá

- ***Analyzovať teraz*** (*zobrazí sa pred spustením analýzy*) – stlačením tohto tlačidla sa ihneď spustí analýza počítača.
- ***Opraviť teraz*** (*zobrazí sa po dokončení analýzy*) – Stlačením tohto tlačidla sa otvoria internetové stránky AVG (http://www.avg.com/) na stránke s podrobnými a najnovšími informáciami o súčasti ***PC Analyzer***.
- ***Zrušiť*** – Stlačením tohto tlačidla sa zastaví spustená analýza, resp. po dokončení analýzy sa otvorí implicitné hlavné dialógové okno aplikácie AVG (*prehľad súčastí*).

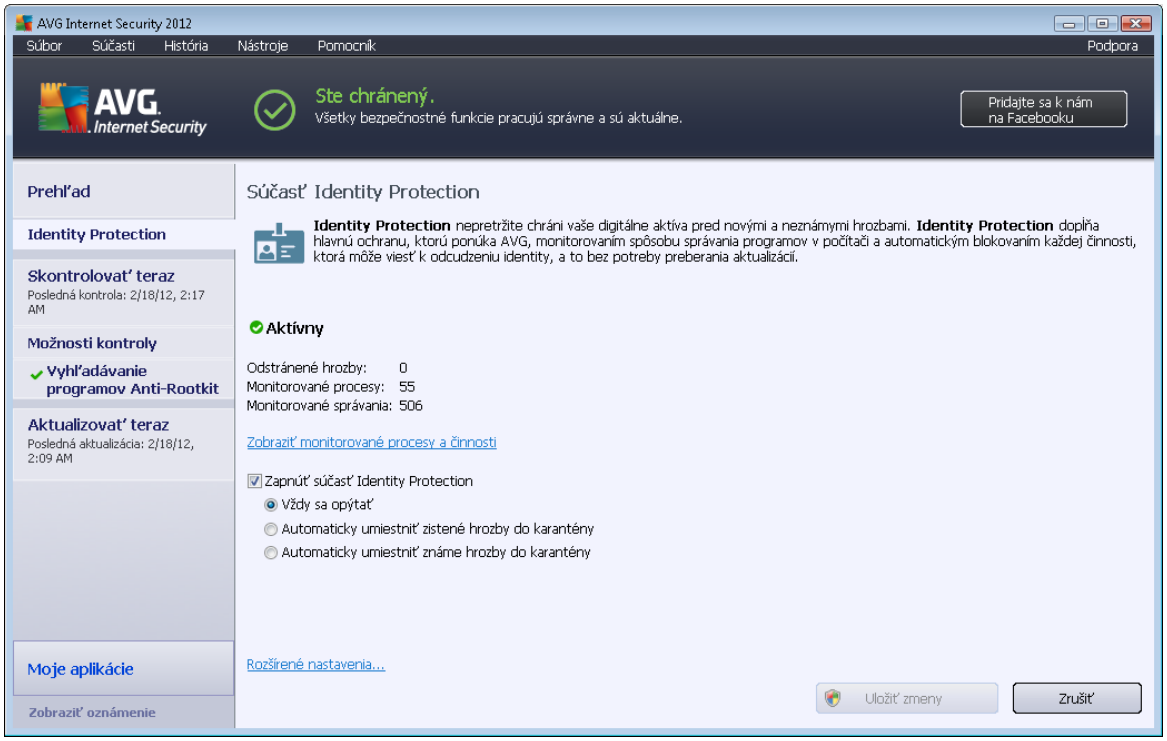
6.8. Identity Protection

Identity Protection je súčasť na ochranu pred malware, ktorá chráni pred všetkými druhmi malware (*spyware, softvéroví roboti, odcudzenie identity...*) pomocou technológií monitorovania správania a poskytuje okamžitú ochranu pred novými vírusmi. ***Identity Protection*** zabraňuje páchateľom počítačovej trestnej činnosti v oblasti odcudzenia identity, aby odcudzili vaše heslá, informácie o bankových účtoch, čísla kreditných kariet a iné cenné osobné digitálne údaje zo všetkých druhov škodlivého softvéru (*malware*), ktorý útočí na váš počítač. Zabezpečuje správne fungovanie všetkých spustených programov na počítači alebo zdieľanej sieti. ***Identity Protection*** zaznamenáva a blokuje podozrivé správanie a chráni počítač pred každým novým malware.

Súčasť Identity Protection chráni počítač pred novými a dokonca aj neznámymi hrozbami v reálnom čase. Monitoruje všetky procesy *(vrátane skrytých)* a viac ako 285 rôznych modelov správania a dokáže zistiť, či sa v počítači nevyskytuje niečo škodlivé. Preto dokáže odhaliť hrozby, ktoré ešte nie sú opísané vo vírusovej databáze. Keď sa do počítača dostane neznámy kód, program ho ihneď začne sledovať z hľadiska škodlivého správania. Ak sa súbor označí ako škodlivý, súčasť ***Identity Protection*** odstráni kód do Vírusového trezora a vráti späť všetky zmeny vykonané v systéme *(vloženie kódu, zmeny v databáze Registry, otvorenie portov a pod.)*. Na dosiahnutie ochrany nemusíte zapínať kontrolu. Technológia má veľmi aktívny prístup, len zriedka sa musí aktualizovať a vždy je v strehu.

Súčasť Identity Protection je doplnková ochrana nástroja Anti-Virus. Odporúčame vám nainštalovať oba komponenty, aby ste získali celkovú ochranu počítača.

6.8.1. Rozhranie súčasti Identity Protection



V dialógovom okne súčasti Identity Protection sa nachádza stručný prehľad základných funkcií súčasti, jej stavu *(aktívna)* a niektoré štatistické informácie:

- ***Odstránené hrozby*** – Informuje o počte odstránených aplikácií, ktoré boli označené ako malware
- ***Monitorované procesy*** – počet momentálne spustených aplikácií monitorovaných súčasťou IDP.
- ***Monitorované správania*** – počet konkrétnych činností spustených v rámci monitorovaných aplikácií.

Nižšie sa nachádza odkaz Zobraziť monitorované procesy a činnosti, ktorý otvára používateľské

rozhranie súčasti System Tools s podrobným prehľadom všetkých monitorovaných procesov.

Základné nastavenia súčasti Identity Protection

V spodnej časti dialógového okna môžete upraviť niektoré základné funkcie komponentu:

- ***Súčasť Identity Protection je zapnutá*** (*štandardne zapnuté*) – začiarknutím sa aktivuje súčasť IDP a otvoria sa ďalšie možnosti editovania.

  V niektorých prípadoch môže súčasť ***Identity Protection*** hlásiť, že je niektorý legitímny súbor podozrivý alebo nebezpečný. Keďže ***Identity Protection*** deteguje hrozby na základe ich správania, toto sa zvyčajne vyskytne v prípade, keď sa niektorý program pokúsi monitorovať kľúčové procesy, nainštalovať iné programy, alebo keď sa do počítača nainštaluje nový ovládač. Preto vyberte jednu z týchto možností, ktoré definujú správanie súčasti ***Identity Protection*** v prípade detekovania podozrivej činnosti:

  - ***Vždy sa opýtať*** – keď sa aplikácia označí ako škodlivá, potom sa vás program opýta, či ju chcete blokovať (*táto možnosť je štandardne zapnutá a odporúčame vám, aby ste toto nastavenie nemenili, ak na to nemáte skutočný dôvod*).
  - ***Automaticky umiestniť detekované hrozby do karantény*** – všetky aplikácie označené ako škodlivé sa budú automaticky blokovať.
  - ***Automaticky umiestniť známe hrozby do karantény*** – blokovať sa budú len aplikácie, ktoré sa so stopercentnou istotou detegujú ako škodlivé.

- ***Rozšírené nastavenia...*** – Po kliknutí na toto prepojenie sa v rámci Rozšírených nastavení produktu **AVG Internet Security 2012** zobrazí príslušné okno. V ňom môžete upraviť podrobnosti konfigurácie súčasti. Všimnite si však, že predvolená konfigurácia všetkých súčastí je nastavená tak, aby **AVG Internet Security 2012** poskytovala optimálny výkon a maximálne zabezpečenie. Ak nemáte na zmenu oprávnený dôvod, odporúčame vám zachovať predvolenú konfiguráciu!

Ovládacie tlačidlá

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

- ***Uložiť zmeny*** – stlačením tohto tlačidla sa uložia a použijú všetky zmeny urobené v tomto dialógovom okne.
- ***Zrušiť*** – Stlačením tohto tlačidla sa znova otvorí implicitné hlavné dialógové okno AVG (*prehľad súčastí*)

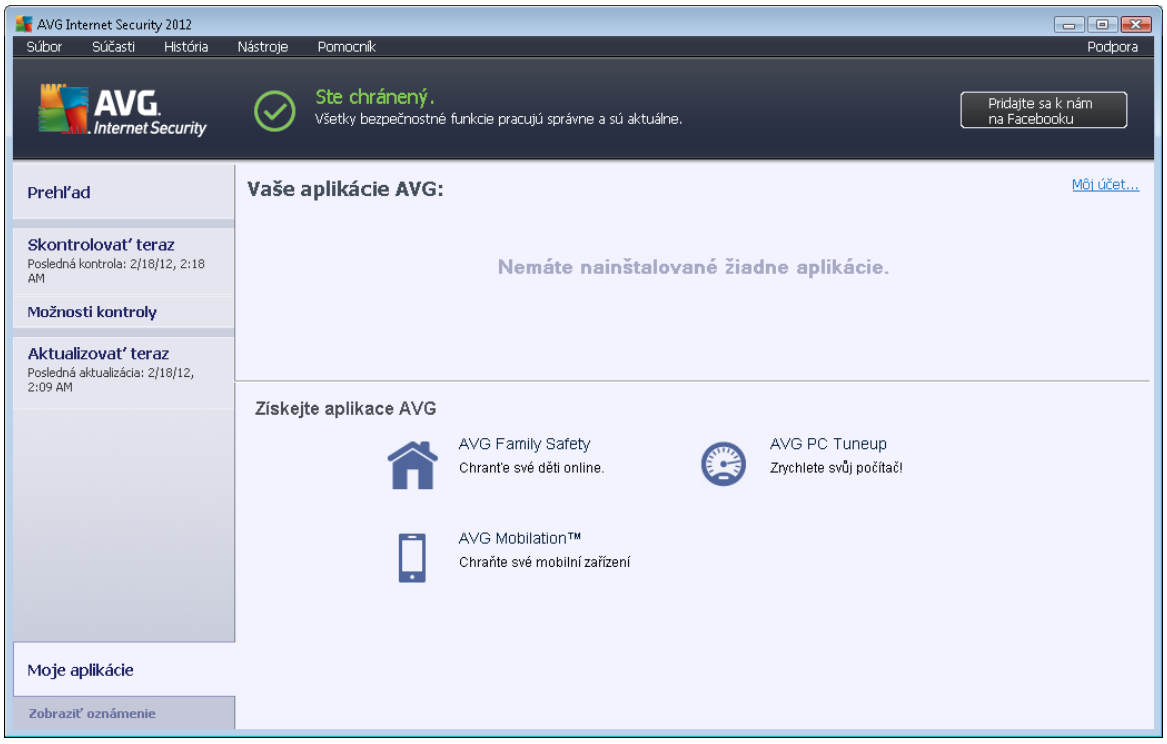
6.9. Remote Administration

Súčasť ***Vzdialená správa*** sa zobrazí v používateľskom rozhraní aplikácie **AVG Internet Security 2012** iba vtedy, ak máte nainštalovanú verziu Business Edition *(informácie o licencii použitej pri inštalácii nájdete na karte Verzia v dialógovom okne Informácie, ktoré otvoríte pomocou položky*

Podpora v systémovej ponuke.). Podrobný opis možností a funkcionality súčasti v systéme AVG Vzdialená správa sa nachádza v príslušnej dokumentácii vyhradenej špeciálne tejto téme. Túto dokumentáciu si môžete prevziať na webovej lokalite spoločnosti AVG (http://www.avg.com/) v časti ***Centrum podpory/Na prevzatie/Dokumentácia***.

7. Moje aplikácie

Dialógové okno ***Moje aplikácie*** *(dostupné priamo v hlavnom okne programu AVG pomocou tlačidla Moje aplikácie)* ponúka pohľad na samostatné aplikácie AVG, či nainštalované na počítači, alebo pripravené na voliteľné nainštalovanie:



Toto dialógové okno je rozdelené na dve sekcie:

- ***Vaše aplikácie AVG*** – ponúka prehľad všetkých samostatných aplikácií AVG, ktoré sa už nachádzajú na počítači;
- ***Získajte aplikácie AVG*** – ponúka prehľad samostatných aplikácií AVG, o ktoré by ste mohli mať záujem. Tieto aplikácie sú pripravené na inštaláciu. Ponuka sa dynamicky mení v závislosti od vašej licencie, polohy a iných faktorov. Podrobné informácie o týchto aplikáciách nájdete na webovej lokalite AVG (http://www.avg.com/).

Ďalej nájdete stručný popis všetkých dostupných aplikácií a krátke vysvetlenie ich funkcie:

7.1. AVG Family Safety

AVG Family Safety pomáha chrániť vaše deti pred nevhodnými internetovými stránkami, multimédiami a výsledkami vyhľadávania online a hlási vám ich aktivitu online. ***Aplikácia AVG Family Safety*** obsahuje technológiu sledujúcu stláčanie tlačidiel pri aktivitách vašich detí v chatovacích miestnostiach alebo v sociálnych sieťach. Ak zaregistruje slová, frázy alebo jazyk, ktoré sú typické pre šikanovanie detí online, okamžite vás upozorní pomocou správy SMS alebo e-mailom. V aplikácii môžete nastaviť vhodnú úroveň ochrany pre každé dieťa a sledovať deti individuálne pomocou jedinečných prihlasovacích údajov.

Podrobné informácie nájdete na príslušnej webovej lokalite AVG, z ktorej si môžete tiež okamžite súčasť prevziať. Kliknite na prepojenie AVG Family Safety v dialógovom okne Moje aplikácie.

7.2. AVG LiveKive

Súčasť ***AVG LiveKive*** sa používa výlučne na online zálohovanie dát na zabezpečených serveroch. ***AVG LiveKive*** automaticky zálohuje všetky vaše súbory, fotografie a hudbu na jednom bezpečnom mieste a umožňuje vám zdieľať tieto dáta s rodinou a priateľmi a získať k nim prístup z akéhokoľvek zariadenia s pripojením na internet, vrátane telefónov iPhone a zariadení s operačným systémom Android. ***Hlavné funkcie súčasti*** AVG LiveKive:

- bezpečnostné opatrenie pre prípad poškodenia počítača a/alebo pevného disku,
- prístup k dátam z akéhokoľvek zariadenia pripojeného na internet,
- jednoduchá organizácia,
- zdieľanie s každým, komu dáte povolenie.

Podrobné informácie nájdete na príslušnej webovej lokalite AVG, z ktorej si môžete tiež okamžite súčasť prevziať. Môžete tak urobiť pomocou odkazu PC LiveKive v dialógovom okne Moje aplikácie.

7.3. AVG Mobilation

AVG Mobilation chráni váš mobilný telefón pred vírusmi a softvérom malware a taktiež ponúka možnosť diaľkového sledovania smartfónu, pokiaľ by ste ho stratili. ***Hlavné funkcie súčasti*** AVG Mobilation:

- *File Scanner* (skener súborov) umožňuje bezpečnostnú kontrolu súborov na rôznych miestach;
- *Task Killer* (ukončenie úloh) ukončí aplikáciu, ak dôjde k spomaleniu zariadenia alebo zamrznutiu;
- *App Locker* (zámok aplikácií) vám umožní uzamknúť a chrániť heslom jednu alebo viac aplikácií a zabrániť tak ich zneužitiu;
- *Tuneup* zbiera rôzne parametre systému *(stav batérie, skladovanie, veľkosť a umiestnenie inštalácie aplikácie a pod)* a zobrazí ich do jedného súhrnného pohľadu, aby ste mohli ovládať výkon systému;
- *App Backup* (zálohovanie aplikácií) vám umožňuje zálohovať aplikácie na kartu SD a neskôr ich znovu použiť;
- *Spam and Scam* (Spam a podvody) vám umožňuje označiť správy SMS ako spam a nahlasovať webové lokality ako podvodné;
- *Vymazať osobné údaje* na diaľku v prípade odcudzenia telefónu;

- *Safe Web Surfing* (bezpečné surfovanie) poskytuje sledovanie navštevovaných webových stránok v reálnom čase.

Podrobné informácie nájdete na príslušnej webovej lokalite AVG, z ktorej si môžete tiež okamžite súčasť prevziať. Môžete tak urobiť pomocou odkazu AVG Mobilation v dialógovom okne Moje aplikácie.

7.4. AVG PC TuneUp

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

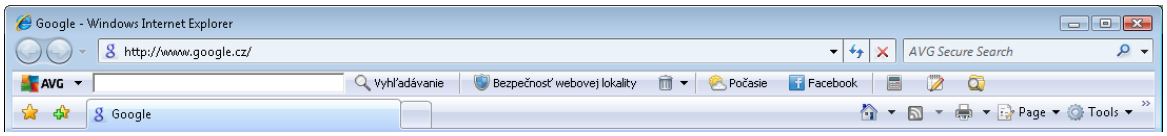
- *Nástroj Disk Cleaner* – Odstraňuje nežiaduce súbory, ktoré spomaľujú počítač.
- *Nástroj Disk Defrag* – Defragmentuje diskové jednotky a optimalizuje rozmiestnenie súborov.
- *Nástroj Registry Cleaner* – Opravuje chyby v registroch a zvyšuje tak stabilitu počítača.
- *Nástroj Registry Defrag* – Zhutní databázu Registry a znižuje tak zbytočné medzery, ktoré zaberajú pamäť.
- *Nástroj Disk Doctor* – Hľadá chybné sektory, stratené klastre, chyby v adresároch a opravuje ich.
- *Nástroj Internet Optimizer* – Prispôsobí všeobecné pripojenia konkrétnemu internetovému pripojeniu.
- *Nástroj Track Eraser* – Odstraňuje históriu počítača a používania internetu.
- *Nástroj Disk Wiper* – Vyčistí voľné miesto na disku, aby sa zabránilo obnoveniu citlivých údajov.
- *Nástroj File Shredder* – Vymaže vybrané súbory na disku alebo kľúči USB tak, že ich nebude možné obnoviť.
- *Nástroj File Recovery* – Obnoví nechcene vymazané súbory z diskov, kľúčov USB alebo fotoaparátov.
- *Nástroj Duplicate File Finder* – Pomáha hľadať a odstraňovať duplicitné súbory, ktoré zbytočne zaberajú priestor na disku.
- *Nástroj Services Manager* – Vypne nepotrebné služby spomaľujúce počítač.
- *Nástroj Startup Manager* – Umožňuje používateľovi spravovať programy, ktoré sa automaticky spúšťajú so systémom Windows.

- *Nástroj Uninstall Manager* – Úplne odinštaluje programy, ktoré už nepoužívate.
- *Nástroj Tewak Manager* – Umožňuje nastaviť na mieru stovky skrytých nastavení systému Windows.
- *Nástroj Správca úloh* – Zobrazí zoznam všetkých spustených procesov, služieb a zamknutých súborov.
- *Nástroj Disk Explorer* – Zobrazuje, ktoré súbory zaberajú najviac miesta v počítači.
- *Systémové informácie* – Obsahujú podrobné údaje o nainštalovanom hardvéri a softvéri.

Podrobné informácie nájdete na príslušnej webovej lokalite AVG, z ktorej si môžete tiež okamžite súčasť prevziať. Môžete tak urobiť pomocou odkazu AVG PC Tuneup v dialógovom okne Moje aplikácie.

8. Lišta nástrojov AVG Security

AVG Security Toolbar je nástroj, ktorý úzko spolupracuje so súčasťou LinkScanner a zabezpečuje maximálnu ochranu pri surfovaní. V produkte **AVG Internet Security 2012** je inštalácia súčasti ***AVG Security Toolbar*** voliteľná. Počas inštalácie sa môžete rozhodnúť, či chcete túto súčasť nainštalovať. K súčasti ***AVG Security Toolbar*** máte prístup priamo v internetovom prehliadači. V súčasnosti medzi podporované prehľadávače patrí Internet Explorer (*verzia 6.0 a novšia*) alebo Mozilla Firefox (*verzia 3.0 a novšia*). Iné prehliadače nie sú podporované *(ak používate alternatívny internetový prehliadač (napr. Avant Browser), môžete sa stretnúť s neočakávaným správaním)*.



Nástroj AVG Security Toolbar pozostáva z nasledujúcich častí:

- ***Logo AVG*** s rozbaľovacou ponukou:
  - ***Použiť funkciu AVG Secure Search*** – Umožní kontrolovať priamo z ***panela nástrojov zabezpečenia*** pomocou nástroja ***AVG Secure Search***. Všetky výsledky vyhľadávania priebežne kontroluje služba Search-Shield, preto sa môžete on-line cítiť absolútne bezpečne.
  - ***Aktuálna úroveň hrozieb*** – Otvorí webovú lokalitu vírusového laboratória s grafickým zobrazením momentálnej úrovne hrozieb na internete.
  - ***AVG Threat Labs*** – Otvorte konkrétnu webovú lokalitu ***AVG Threat Lab*** *(na adrese http://www.avgthreatlabs.com)*, kde nájdete informácie o bezpečnosti rôznych webových lokalít a aktuálnej hladine online hrozieb.
  - ***Pomocník pre panel nástrojov*** – Otvorí sa on-line pomocník s informáciami o funkciách nástroja ***AVG Security Toolbar***.
  - ***Poslať reakciu na produkt*** – Otvorí sa webová lokalita s formulárom, do ktorého môžete napísať svoje pocity a skúsenosti s nástrojom ***AVG Security Toolbar***.
  - ***O programe...*** – Otvorí sa nové okno s informáciami o verzii aktuálne nainštalovanej súčasti ***AVG Security Toolbar***.
- ***Pole vyhľadávania*** – Pri surfovaní s nástrojom ***AVG Security Toolbar*** ste absolútne chránení, pretože všetky zobrazené výsledky vyhľadávania sú stopercentne bezpečné. Do poľa vyhľadávania napíšte kľúčové slovo alebo frázu a stlačte tlačidlo ***Vyhľadať*** *(alebo Enter)*. Všetky výsledky vyhľadávania sa priebežne kontrolujú funkciou Search-Shield *(v rámci nástroja LinkScanner)*.

- ***Bezpečnosť stránky*** – Toto tlačidlo otvára nové dialógové okno obsahujúce informácie o aktuálnej úrovni hrozby *Aktuálne bezpečné*) internetovej stránky, na ktorej sa práve nachádzate. Toto krátke zhrnutie môžete rozbaliť a zobraziť všetky podrobnosti o všetkých bezpečnostných činnostiach týkajúcich sa internetovej stránky priamo v okne prehliadača (*Zobraziť úplnú správu*):

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

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

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

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

9. AVG Do Not Track

Aplikácia ***AVG Do Not Track*** pomáha identifikovať webové lokality, ktoré zhromažďujú údaje o vašej činnosti on-line. V prehľadávači sa zobrazí ikona upozorňujúca, že webová lokalita alebo reklamná služba zhromažďuje údaje o vašej aktivite, a máte možnosť povoliť alebo nepovoliť ich zhromažďovanie.

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

V súčasnosti je fungovanie aplikácie ***AVG Do Not Track*** podporované len v prehľadávačoch Mozilla Firefox, Chrome a Internet Explorer. *(V prehľadávači Internet Explorer je ikona aplikácie AVG Do Not Track umiestnená na pravej strane panelu príkazov. V prípade, že by ste zaznamenali problémy so zobrazením ikony aplikácie AVG Do Not Track v predvolenom nastavení internetového prehliadača, uistite sa, že máte zapnutý panel príkazov. Ak ikonu stále nevidíte, posuňte panel príkazov doľava, aby ste zobrazili všetky ikony a tlačidlá, ktoré sú na paneli nástrojov dostupné.)*

9.1. Rozhranie aplikácie AVG Do Not Track

Keď ste on-line, aplikácia ***AVG Do Not Track*** vás upozorní ihneď, ako zistí akúkoľvek činnosť zhromažďovania údajov. Zobrazí sa toto dialógové okno:

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

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

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

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

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

Dialógové okno obsahuje aj dve hypertextové prepojenia:

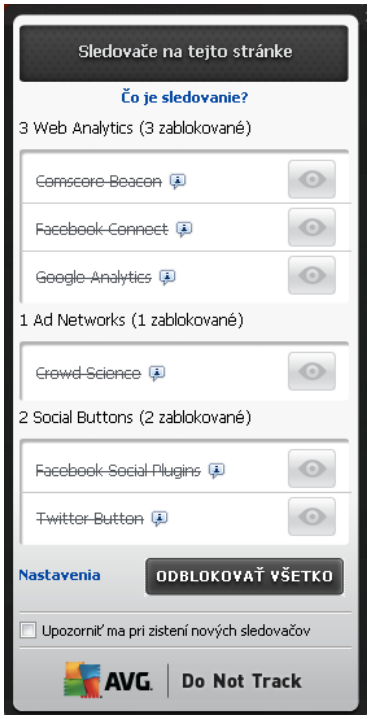
- ***Čo je sledovanie?*** – po kliknutí na toto prepojenie v hornej časti dialógového okna budete presmerovaní na špeciálnu webovú stránku s podrobným vysvetlením princípov sledovania a s popisom konkrétnych druhov sledovania.

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

9.2. Informácie o sledovacích procesoch

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

V spodnej časti informačnej bubliny môžete vidieť prepojenie ***Zásady ochrany osobných údajov***, ktoré vás prepojí na internetovú stránku venovanú zásadám ochrany osobných údajov príslušnej detegovanej služby.

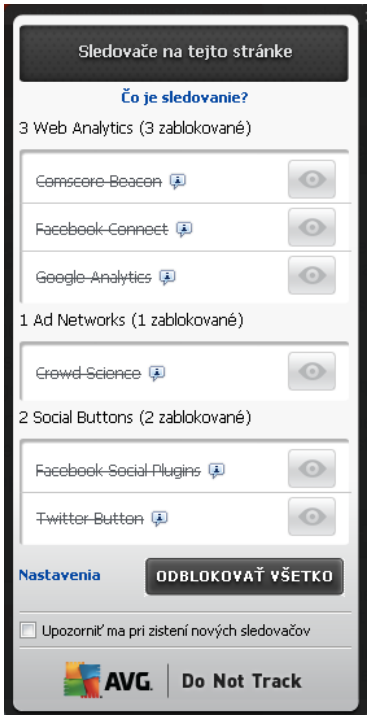


9.3. Blokovanie sledovacích procesov

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

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

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

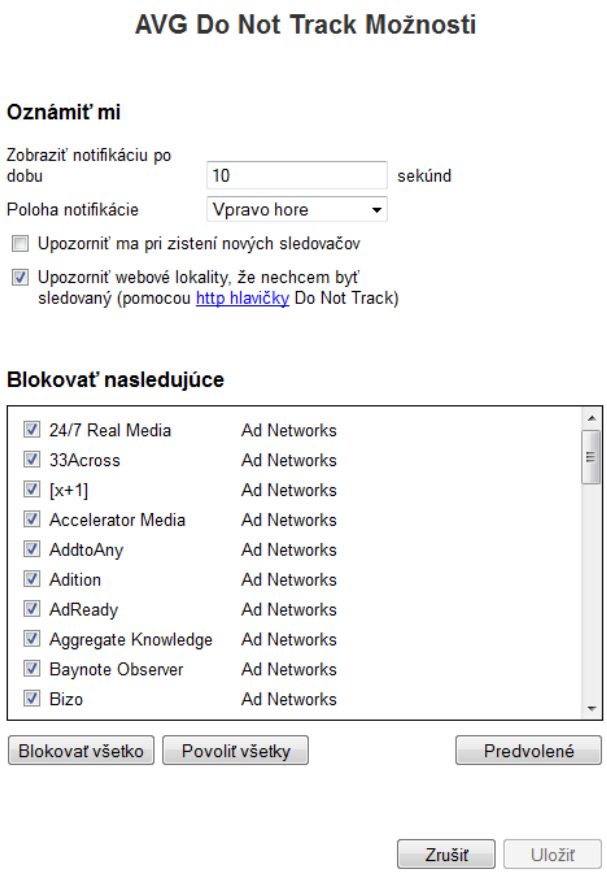


9.4. Nastavenia aplikácie AVG Do Not Track

Priamo v dialógovom okne aplikácie ***AVG Do Not Track*** sa nachádza iba jedna možnosť nastavenia: v spodnej časti môžete vidieť začiarkavacie políčko ***Upozorniť ma, keď sú detegované aktívne sledovacie služby***. V predvolenom nastavení táto možnosť nie je vybraná. Začiarknutím políčka potvrdíte, že chcete upozornenie zakaždým, keď prejdete na webovú stránku obsahujúcu novú službu zhromažďujúcu údaje, ktorá ešte nebola zablokovaná. Keď je políčko označené a

aplikácia ***AVG Do Not Track*** deteguje novú službu zhromažďujúcu údaje na stránke, na ktorej sa práve nachádzate, na obrazovke sa zobrazí dialógové okno s upozornením. V opačnom prípade si novú zistenú sledovaciu službu všimnete len tak, že ikona aplikácie ***AVG Do Not Track*** *(nachádza sa v paneli príkazov internetového prehľadávača)* zmení farbu zo zelenej na žltú.

V spodnej časti dialógového okna aplikácie ***AVG Do Not Track***však môžete nájsť prepojenie ***Nastavenia***. Kliknite priamo na toto prepojenie a presmerujete sa na špeciálnu internetovú stránku, na ktorej môžete spresniť možnosti aplikácie ***AVG Do Not Track***:



- ***Umiestnenie upozornenia*** *(v predvolenom nastavení pravý horný roh)* – Otvorte rozbaľovaciu ponuku a spresnite požadované umiestnenie dialógového okna aplikácie ***AVG Do Not Track*** na monitore.

- ***Dĺžka zobrazenia upozornenia****(v predvolenom nastavení 10 s)* – V tomto políčku sa rozhodnete, ako dlho *(v sekundách)* sa má upozornenie aplikácie ***AVG Do Not Track*** na obrazovke zobrazovať. Môžete určiť číslo 0 až 60 sekúnd *(ak je vybraná 0, upozornenie sa vôbec nezobrazí)*.

- ***Upozorniť ma, keď sú detegované aktívne sledovacie služby*** *(v predvolenom nastavení vypnuté)* - Ak si želáte byť upozornení vždy, keď navštívite internetovú stránku obsahujúcu novú službu zhromažďujúcu údaje, ktorá nebola ešte zablokovaná, označte toto

začiarkavacie políčko. Keď je políčko označené a aplikácia ***AVG Do Not Track*** deteguje novú službu zhromažďujúcu údaje na stránke, na ktorej sa práve nachádzate, na obrazovke sa zobrazí dialógové okno s upozornením. V opačnom prípade si novú zistenú sledovaciu službu všimnete len tak, že ikona aplikácie ***AVG Do Not Track*** *(nachádza sa v paneli príkazov internetového prehľadávača)* zmení farbu zo zelenej na žltú.

- ***Upozorniť internetové stránky, že si neželám sledovanie*** *(v predvolenom nastavení zapnuté)* – Túto možnosť nechajte začiarknutú vtedy, keď si želáte, aby aplikácia ***AVG Do Not Track*** informovala poskytovateľa služby zhromažďujúcej údaje, že nechcete, aby vás sledovala.

- ***Blokovať nasledujúce*** *(všetky služby zhromažďujúce údaje uvedené v zozname sú v predvolenom nastavení povolené)* – V tejto časti môžete vidieť políčko so zoznamom známych sledovacích služieb, ktoré môžu byť označené ako reklamné siete. V predvolenom nastavení služba ***AVG Do Not Track*** blokuje niektoré reklamné siete automaticky a od vás závisí, či budú blokované aj ostatné siete, alebo ich necháte povolené. Stačí, keď kliknete na tlačidlo ***Blokovať všetky*** pod zoznamom.

Ovládacie tlačidlá dostupné na stránke možností aplikácie ***AVG Do Not Track*** sú nasledovné:

- ***Blokovať všetky*** – Kliknite na úplné zablokovanie všetkých služieb uvedených v predchádzajúcom políčku, ktoré sú označené ako reklamné siete.

- ***Povoliť všetky*** – Kliknite na zrušenie zablokovania všetkých služieb uvedených v predchádzajúcom políčku, ktoré sú označené ako reklamné siete.

- ***Predvolené nastavenie*** – Kliknite na ukončenie prispôsobených nastavení a návrat do predvoleného nastavenia.

- ***Uložiť*** – Kliknite na použitie a uloženie vykonaného nastavenia.

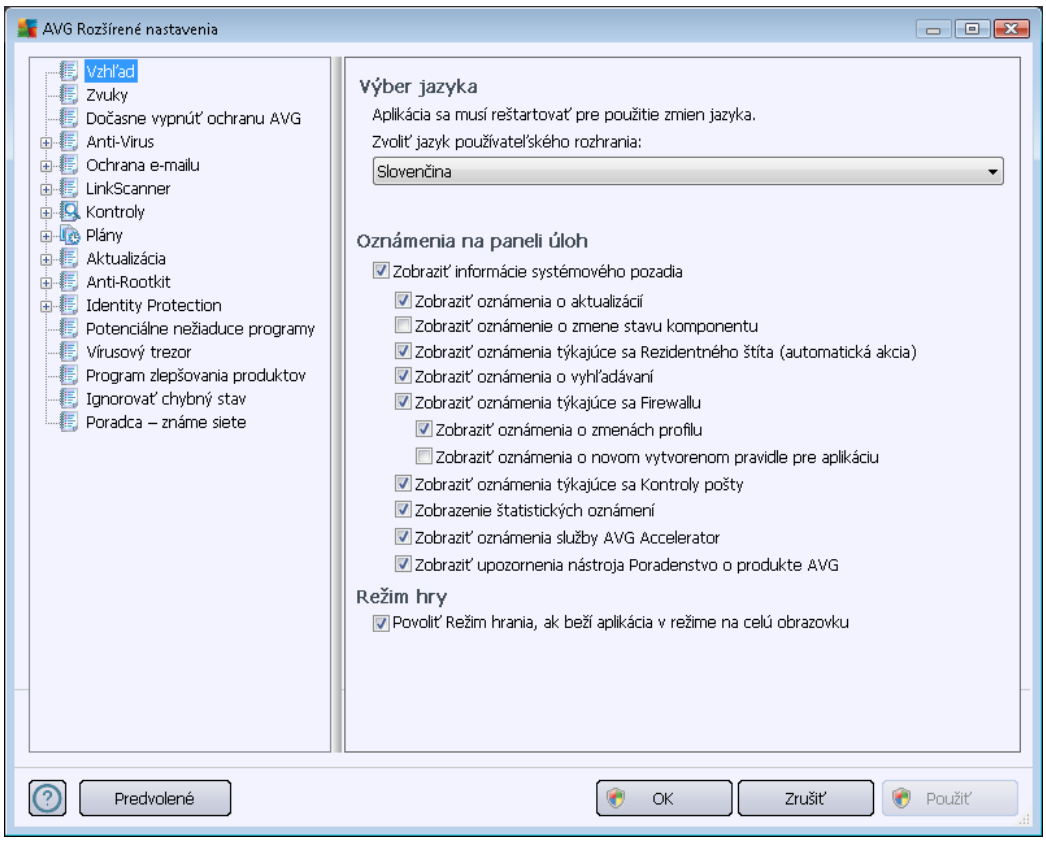
- ***Zrušiť*** – Kliknite na zrušenie všetkých predchádzajúcich nastavení.

10. Rozšírené nastavenia programu AVG

Dialógové okno s rozšírenou konfiguráciou produktu **AVG Internet Security 2012** 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 konkrétnu časť*), otvorte dialógové okno editovania v pravej časti okna.

10.1. Vzhľad

Prvá položka v navigačnej štruktúre, ***Vzhľad***, sa týka všeobecných nastavení používateľského rozhrania produktu **AVG Internet Security 2012** a niektorých základných možností správania sa aplikácie:

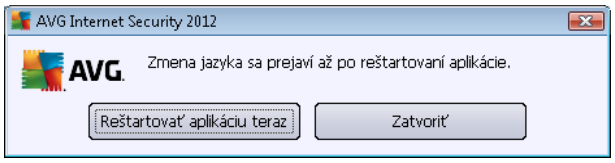


Výber jazyka

V časti ***Výber jazyka*** môžete v rozbaľovacej ponuke vybrať požadovaný jazyk. Vybraný jazyk sa potom použije pre celé používateľské prostredie produktu **AVG Internet Security 2012**. V rozbaľovacej ponuke sa nachádzajú len tie jazyky, ktoré ste už nainštalovali počas inštalácie (*pozri kapitolu Vlastné možnosti*) plus angličtina (*tá sa inštaluje štandardne*). Zmenu jazyka produktu **AVG Internet Security 2012** dokončíte reštartovaním aplikácie. Postupujte podľa nasledujúcich pokynov:

- V rozbaľovacej ponuke vyberte požadovaný jazyk aplikácie.

- Potvrďte výber stlačením tlačidla ***Použiť*** *(v pravom hornom rohu dialógového okna).*
- Potvrďte stlačením tlačidla ***OK.***
- Zobrazí sa nové dialógové okno s informáciami o zmene jazyka aplikácie a potrebe reštartovať **AVG Internet Security 2012**
- Stlačením tlačidla ***Reštartovať aplikáciu*** potvrďte súhlas s reštartovaním programu. Počkajte chvíľu, kým sa zmena jazyka prejaví:



Oznámenia v paneli úloh

V tejto časti môžete zrušiť zobrazovanie oznámení v paneli úloh o stave aplikácie **AVG Internet Security 2012**. Štandardne je zobrazovanie oznámení v paneli úloh povolené. Dôrazne odporúčame toto nastavenie nemeniť! Oznámenia v paneli úloh informujú napríklad o spustení vyhľadávania, spustení aktualizácie alebo o zmene súčasti **AVG Internet Security 2012**. Týmto oznámeniam by ste rozhodne mali venovať pozornosť.

Ak sa však z nejakého dôvodu rozhodnete tieto informácie nezobrazovať alebo ak chcete zobraziť iba niektoré oznámenia *(týkajúce sa konkrétnej súčasti AVG Internet Security 2012)*, môžete definovať a určiť vlastné predvoľby označením/zrušením označenia príslušných možností:

- ***Zobrazovať oznámenia v paneli úloh*** *(štandardne zapnuté)* – Štandardne sa zobrazujú všetky oznámenia. Ak chcete úplne vypnúť zobrazovanie všetkých oznámení, zrušte začiarknutie tejto položky. Po zapnutí môžete ďalej vybrať konkrétne oznámenia, ktoré sa majú zobrazovať:
  - ***Zobraziť oznámenia o aktualizácii*** *(štandardne zapnuté)* – Rozhodnite sa, či sa majú zobrazovať informácie **AVG Internet Security 2012**týkajúce sa spustenia aktualizácie, postupu a dokončenia.
  - ***Zobraziť oznámenia o zmene stavu súčasti*** *(štandardne vypnuté)* – Rozhodnite, či sa majú zobrazovať informácie týkajúce sa činnosti alebo nečinnosti súčasti, prípadne či sa majú zobrazovať informácie o možnom probléme. Táto možnosť má pri oznámení chybného stavu súčasti informačnú funkciu ikony na paneli úloh, ktorá informuje o probléme týkajúcom sa súčasti produktu **AVG Internet Security 2012**.
  - ***Zobraziť oznámenia súvisiace so súčasťou Resident Shield na paneli úloh (automatická akcia)****(štandardne zapnuté)* – Rozhodnite, či sa majú alebo nemajú zobrazovať informácie súvisiace s procesmi ukladania, kopírovania a otvárania súborov (*táto funkcia sa dá nastaviť, len keď je v súčasti Resident Shield zapnutá možnosť Liečiť automaticky*).
  - ***Zobraziť oznámenia o kontrole*** na paneli úloh *(štandardne zapnuté)* – Nastavte, či

sa majú zobrazovať informácie pri automatickom spustení naplánovanej kontroly, jej priebehu a výsledkoch.

- ***Zobraziť oznámenia súvisiace so súčasťou Firewall na paneli úloh*** *(štandardne zapnuté)* – Nastavte, či sa majú zobrazovať informácie súvisiace so stavom a procesmi súčasti Firewall, ako sú upozornenia o zapnutí alebo vypnutí súčasti, prípadne blokovaní prenosov atď . Na tomto mieste môžete určiť dve ďalšie možnosti *(podrobnejšie vysvetlenie každej z nich nájdete v kapitole Firewall v tomto dokumente)*:

  – ***Zobraziť oznámenia o zmenách profilu*** *(štandardne zapnuté)* – Upozorní vás na automatické zmeny profilov brány Firewall.

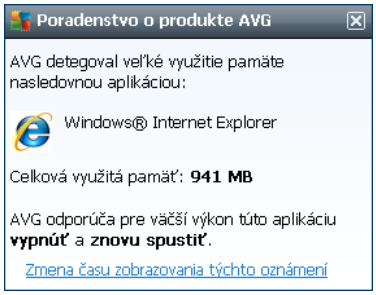
  – ***Zobraziť oznámenia o nových vytvorených aplikačných pravidlách*** *(štandardne vypnuté)* – Informuje o automatickom vytvorení pravidiel brány Firewall pre nové aplikácie na základe zoznamu bezpečných aplikácií.

- ***Zobraziť oznámenia súvisiace so súčasťou E-mail Scanner na paneli úloh*** *(štandardne zapnuté)* – Nastavte, či sa majú zobrazovať informácie po každej kontrole prichádzajúcich a odchádzajúcich e-mailových správ.

- ***Zobraziť štatistické oznámenia*** *(štandardne zapnuté)* – Nechajte políčko začiarknuté, ak sa majú zobrazovať pravidelné štatistické prehľadové oznámenia na paneli úloh.

- ***Zobraziť v paneli úloh oznámenia súčasti AVG Accelerator*** *(štandardne zapnuté)* – Môžete určiť, či sa majú zobrazovať informácie týkajúce sa činností súčasti ***AVG Accelerator***. ***Služba AVG Accelerator*** umožňuje stabilnejšie prehrávanie on-line videa a uľahčuje ďalšie preberania.

- ***Zobraziť v paneli úloh upozornenia týkajúce sa súčasti AVG Advice*** *(štandardne zapnuté)* – ***AVG Advice*** sleduje výkon podporovaných internetových prehliadačov *(Internet Explorer, Chrome, Firefox, Opera a Safari)* a informuje vás v prípade, že zaberajú nadmerné množstvo pamäte. Vtedy sa môže výrazne spomaliť výkon počítača. Služba vám poradí, aby ste reštartovali internetový prehliadač v záujme zrýchlenia chodu počítača. Ak chcete tieto informácie zobrazovať, nechajte možnosť ***Zobraziť v paneli úloh upozornenia týkajúce sa súčasti AVG Advice*** zapnutú.

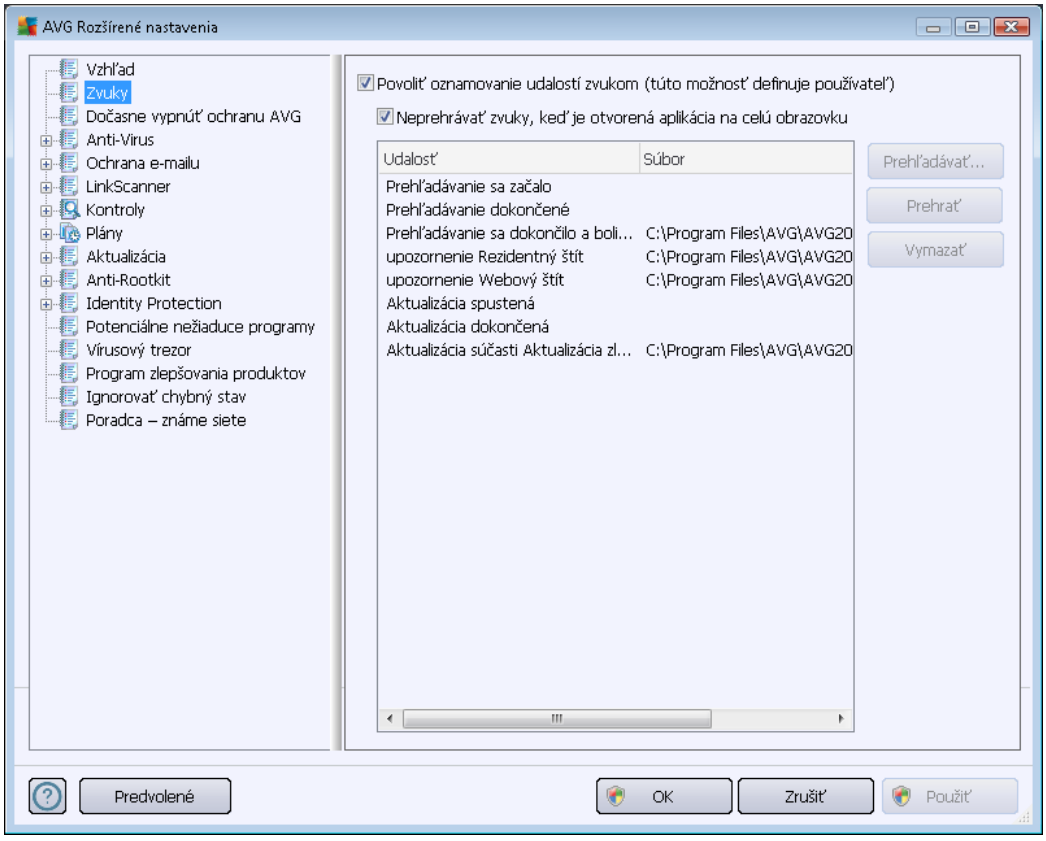


Režim hrania

Táto funkcia programu AVG sa používa v súvislosti s aplikáciami spustenými na celú obrazovku, ktorých spustenie by sa mohlo narušiť (*aplikácia by sa minimalizovala, alebo by sa porušila grafika*) zobrazením informačnej bubliny programu AVG (*ktorá sa zobrazí napr. pri spustení naplánovanej kontroly*). Ak sa chcete vyhnúť podobným situáciám, nechajte začiarkovacie okienko možnosti ***Zapnúť režim hrania, keď je spustená aplikácia v režime na celú obrazovku*** začiarknuté (*predvolené nastavenie*).

10.2. Zvuky

Dialógové okno ***Zvuky*** sa používa na zapnutie zvukových upozornení informujúcich o konkrétnych činnostiach programu **AVG Internet Security 2012**:



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

Ovládacie tlačidlá

- ***Prehľadávať*** – Po označení príslušnej udalosti zo zoznamu pomocou tlačidla ***Prehľadávať***

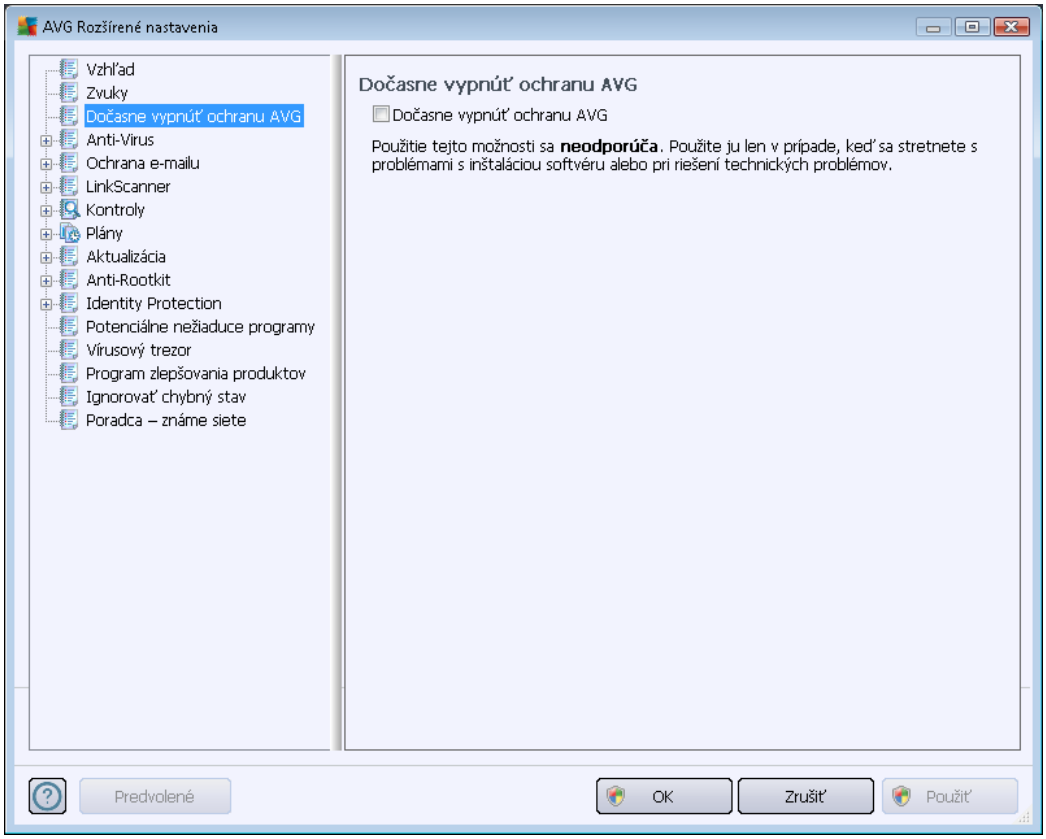
nájdete na disku požadovaný zvukový súbor, ktorý chcete činnosti priradiť. *(V súčasnosti sú podporované iba zvukové formáty *.wav!)*

- ***Prehrať*** – Ak si chcete vypočuť zvolený zvuk, zvýraznite udalosť v zozname a stlačte tlačidlo ***Prehrať***.
- ***Odstrániť*** – Na odstránenie zvuku prideleného konkrétnej udalosti použite tlačidlo ***Odstrániť***.

10.3. Dočasné vypnutie ochrany AVG

Dialógové okno ***Dočasné vypnutie ochrany AVG*** umožňuje naraz vypnúť celú ochranu zabezpečovanú programom **AVG Internet Security 2012**.

Nepoužívajte túto možnosť, ak to nie je naozaj nevyhnutné!

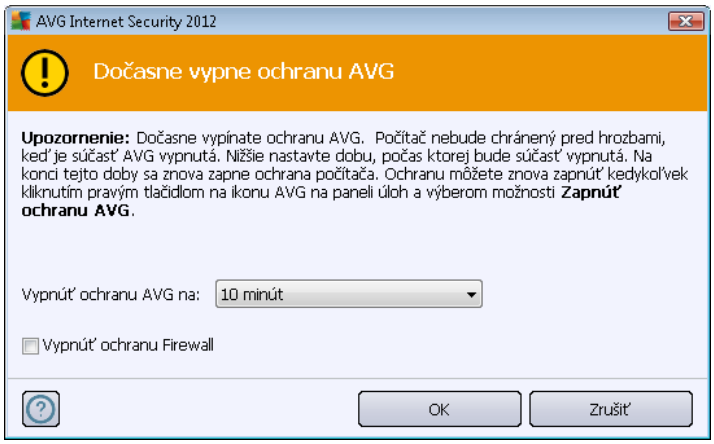


Vo väčšine prípadov ***nie je potrebné*** vypínať program **AVG Internet Security 2012** pred inštaláciou nového softvéru alebo ovládačov, a to ani v prípade, ak inštalačný program alebo sprievodca inštaláciou softvéru odporúča, aby sa najskôr zatvorili otvorené programy a aplikácie z dôvodu možného nežiaduceho prerušenia inštalácie. Ak sa počas inštalácie vyskytne problém, skúste najprv vypnúť rezidentnú ochranu (*Povoliť súčasť Resident Shield*). Ak musíte dočasne vypnúť ochranu **AVG Internet Security 2012**, znova ju zapnite bezprostredne po dokončení úloh, pre ktoré ste ju vypli. Ak ste pripojení na internet alebo k sieti v čase, keď je antivírový softvér vypnutý, počítač nie je chránený pred útokmi.

Ako vypnúť ochranu AVG

- Označte začiarkavacie políčko ***Dočasne vypnúť ochranu AVG*** a potvrďte voľbu stlačením tlačidla ***Použiť***

- V novom otvorenom dialógovom okne ***Dočasne vypnúť ochranu AVG*** zadajte čas, na aký chcete vypnúť aplikáciu **AVG Internet Security 2012**. Štandardne sa ochrana vypne na 10 minút, čo by malo stačiť na dokončenie bežných úloh, ako je inštalácia nového softvéru a pod. Prvý časový limit, ktorý je možné nastaviť, je 15 minút, a z bezpečnostných dôvodov sa nedá prepísať vlastnou hodnotou. Po uplynutí časového intervalu sa všetky vypnuté súčasti automaticky znovu aktivujú.

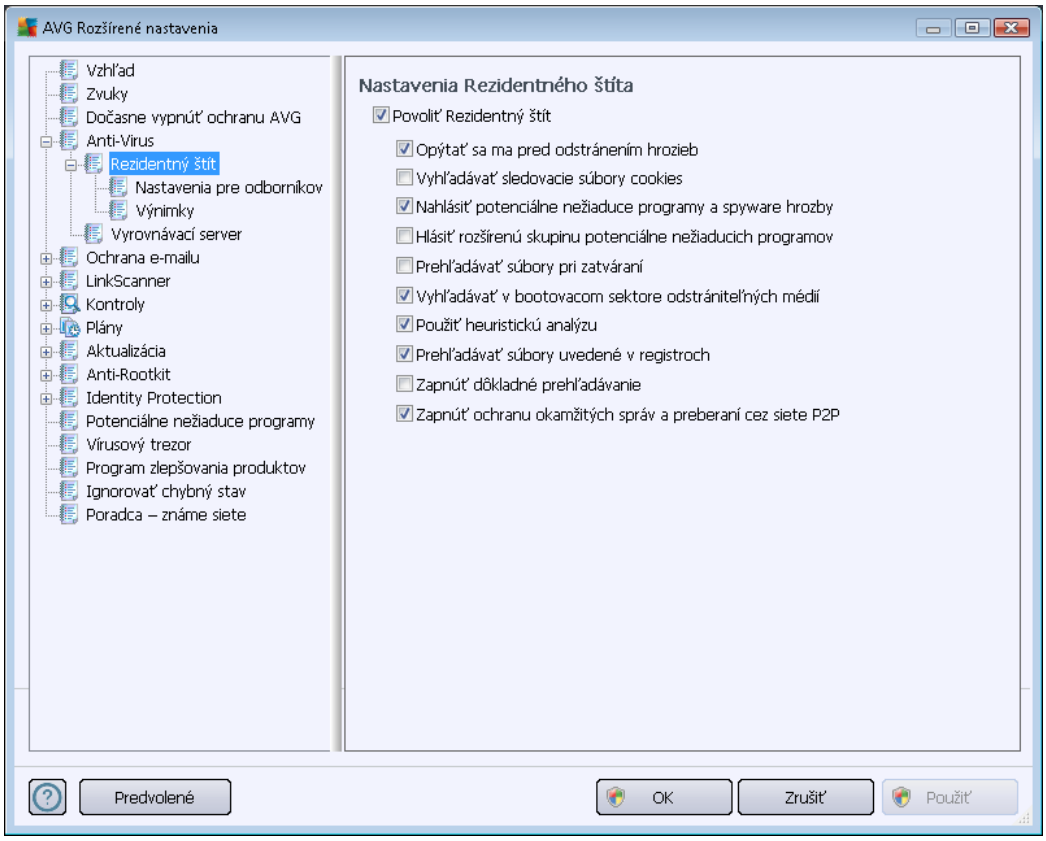


10.4. Anti-Virus

Súčasť ***Anti-Virus*** trvale chráni počítač pred všetkými známymi typmi vírusov a spywaru *(vrátane tzv. spiacich a neaktívnych programov malware, t.j. škodlivých programov prevzatých do počítača, ktoré sa zatiaľ neaktivovali).*

10.4.1. Rezidentný štít

Súčasť Rezidentný štít zabezpečuje živú ochranu súborov a priečinkov pred vírusmi, spyware a iným škodlivým softvérom.



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

- ***Spýtať sa pred odstránením hrozieb*** (*štandardne zapnuté*) – začiarknite pre zabezpečenie, že Rezidentný štít nebude vykonávať žiadne akcie automaticky a namiesto toho zobrazí dialógové okno popisujúce detegovanú hrozbu a umožní vám tak rozhodnúť sa, aká akcia by mala byť vykonaná. Ak ponecháte políčko nezačiarknuté, **AVG Internet Security 2012** bude automaticky liečiť infekcie, a ak to nebude možné, bude objekt premiestnený do Vírusového trezoru.

- ***Kontrolovať sledovacie súbory cookies*** (*štandardne vypnuté*) – Tento parameter určuje, že sa majú počas kontroly zisťovať aj súbory cookies. (*HTTP cookies sa používajú na autentifikáciu, sledovanie a zachovanie špecifických informácií o používateľoch, ako sú preferencie stránky alebo obsah ich elektronických nákupných vozíkov.*)

- ***Hlásiť potenciálne nežiaduce programy a hrozby spyware*** (*štandardne zapnuté*) – Začiarknite toto políčko, ak chcete zapnúť súčasť Anti-Spyware a kontrolovať spyware a vírusy. Spyware predstavuje pochybnú kategóriu škodlivého softvéru: hoci v bežných

situáciách predstavuje bezpečnostné riziko, niektoré takéto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.

- ***Hlásiť rozšírenú skupinu potenciálne nežiaducich programov*** (*štandardne vypnuté*) – Začiarknite, ak chcete zistiť rozšírenú skupinu programov spyware: programov, ktoré sú úplne v poriadku a neškodné pri získaní priamo od výrobcu, ale neskôr sa môžu zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré zvyšuje úroveň zabezpečenia počítača, ale môže blokovať zákonné programy, preto je táto funkcia štandardne vypnutá.

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

- ***Kontrola zavádzacieho sektora vymeniteľných médií*** (*štandardne zapnuté*)

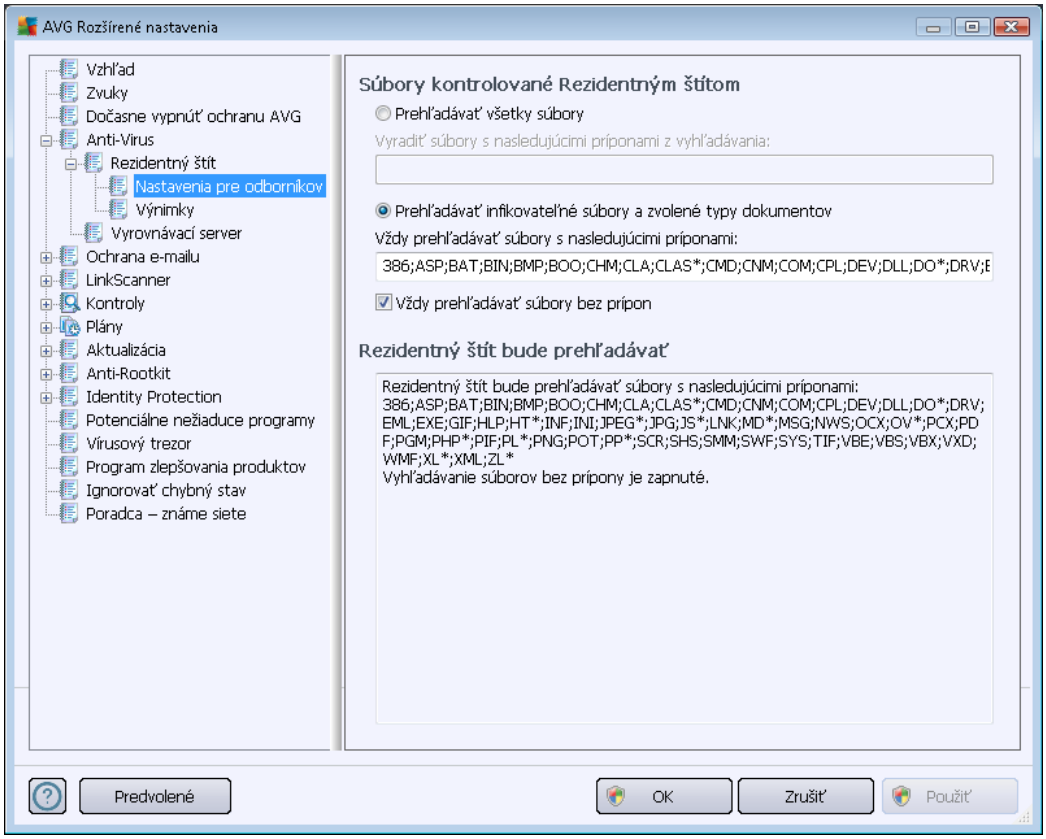
- ***Použiť heuristiku*** (*štandardne zapnuté*) – Na detekovanie sa použije heuristická analýza (*dynamická emulácia inštrukcií kontrolovaného objektu v prostredí virtuálneho počítača*).

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

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

- ***Zapnúť ochranu okamžitých správ a preberaní P2P*** (*štandardne zapnuté*) – Túto položku zapnite vtedy, ak chcete kontrolovať komunikáciu rýchlych správ (*napr. ICQ, MSN Messenger, ...*) a preberania P2P, či neobsahuje vírusy.

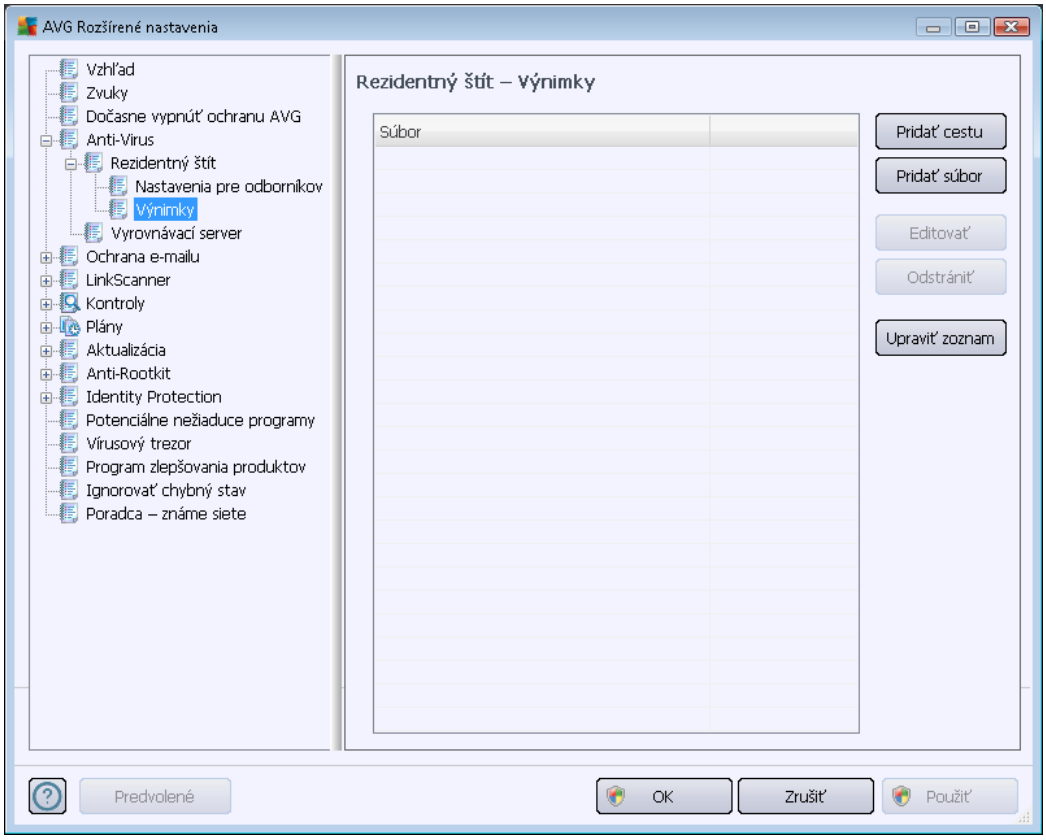
V dialógovom okne ***Súbory kontrolované súčasťou Rezidentný štít*** môžete nastaviť, ktoré súbory sa budú kontrolovať (*podľa konkrétnych prípon*):



Označte príslušné začiarkavacie políčko podľa toho, či chcete použiť možnosť ***Kontrolovať všetky súbory*** alebo ***Kontrolovať iba infikovateľné súbory a vybrané typy dokumentov***. Ak zvolíte druhú možnosť, môžete ďalej určiť prípony súborov, ktoré chcete vylúčiť z kontroly, ako aj zoznam prípon súborov, ktoré chcete kontrolovať za každých okolností.

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

V nasledujúcej časti s názvom ***Súčasť Rezidentný štít skontroluje*** sa nachádza prehľad momentálnych nastavení s podrobným prehľadom toho, čo bude súčasť ***Rezidentný štít*** skutočne kontrolovať.



Dialógové okno ***Rezidentný štít – Výnimky*** umožňuje definovať súbory alebo priečinky, ktoré sa vylúčia z kontroly súčasťou ***Rezidentný štít***.

Odporúčame vám, aby ste nevylúčili žiadne položky, ak to nie je nutné!

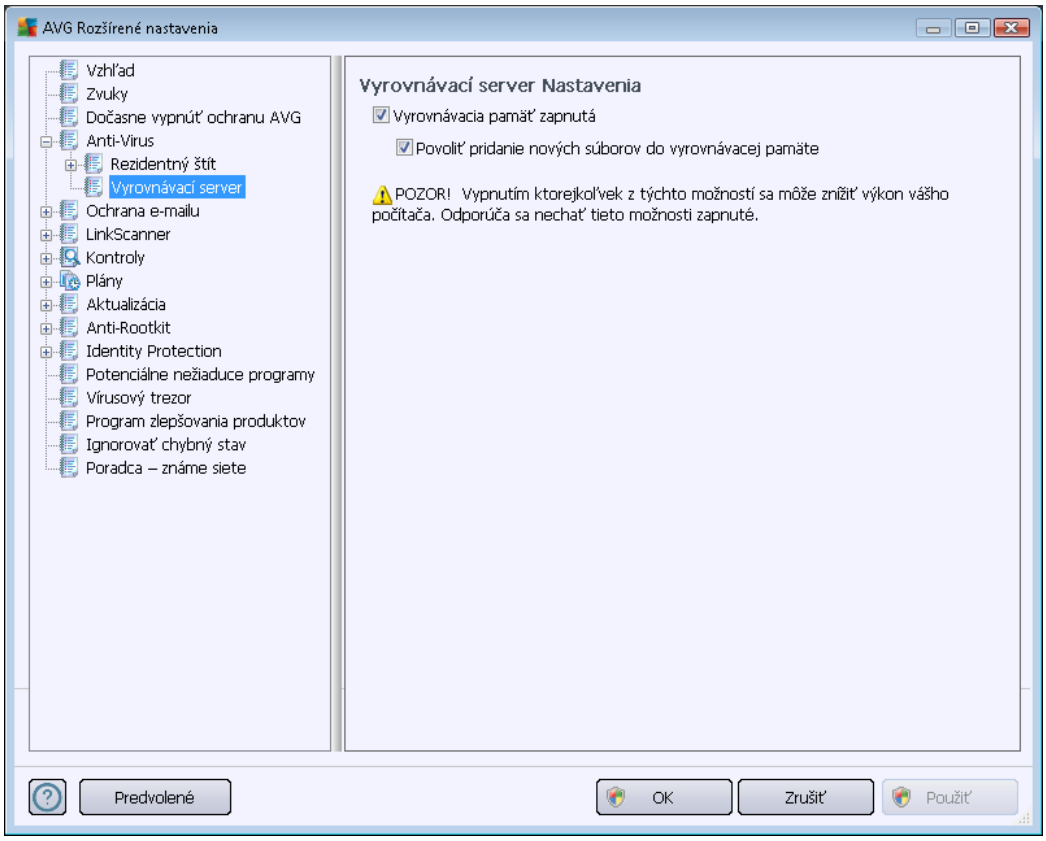
Ovládacie tlačidlá

V tomto dialógovom okne sa nachádzajú tieto ovládacie tlačidlá:

- ***Pridať cestu*** – uveďte adresáre, ktoré sa majú vylúčiť z kontroly, tak, že ich postupne vyberiete v navigačnej štruktúre lokálneho disku.
- ***Pridať súbor*** – uveďte súbory, ktoré sa majú vylúčiť z kontroly, tak, že ich postupne vyberiete v navigačnej štruktúre lokálneho disku.
- ***Editovať položku*** – umožňuje editovať zadanú cestu k vybranému súboru alebo priečinku.
- ***Odstrániť položku*** – umožňuje vymazať cestu k vybranej položke zo zoznamu.
- ***Upraviť zoznam*** – Umožňuje upraviť celý zoznam definovaných výnimiek v novom dialógovom okne, ktoré sa správa ako štandardný textový editor

10.4.2. Vyrovnávací server

Dialógové okno ***Nastavenie vyrovnávacieho servera*** sa týka procesu vyrovnávacieho servera určeného na zrýchlenie všetkých typov vyhľadávaní aplikácie **AVG Internet Security 2012**:



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

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

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

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

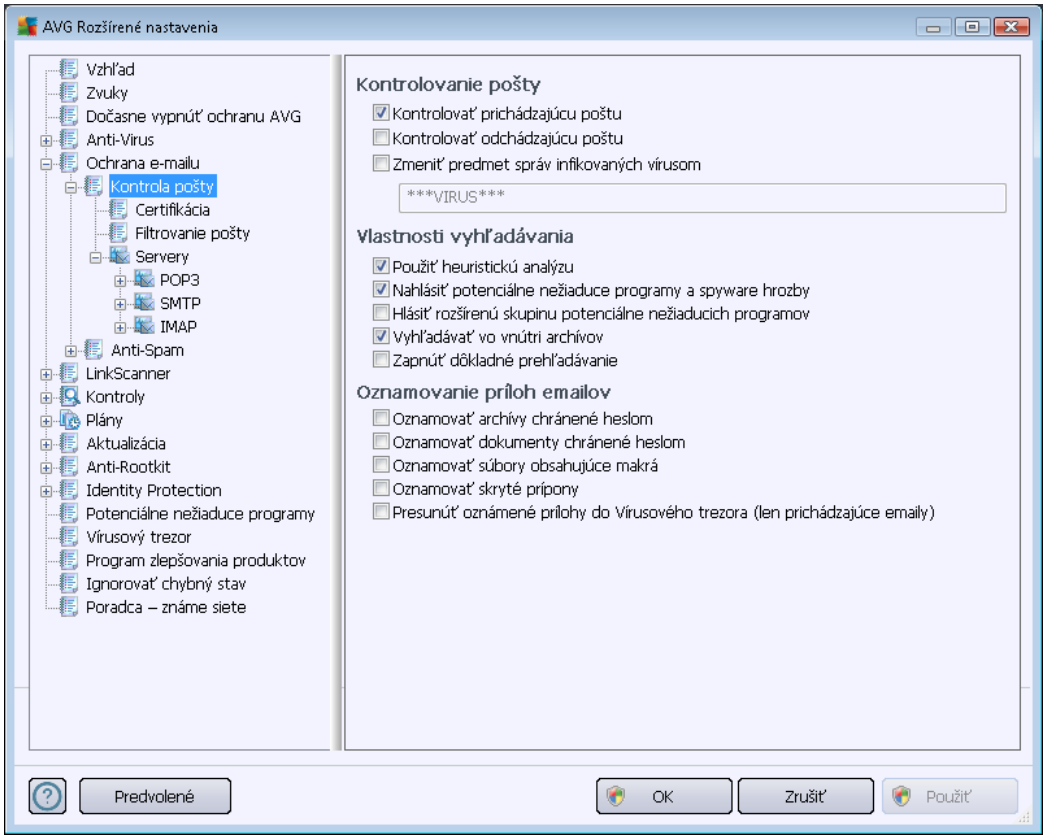
Ak nemáte oprávnený dôvod na vypnutie vyrovnávacieho servera, dôrazne odporúčame zachovať predvolené nastavenia a nechať obe možnosti zapnuté. Inak môžete zaznamenať výrazné spomalenie rýchlosti a výkonu systému.

10.5. Ochrana e-mailu

V časti ***Ochrana e-mailu*** môžete upraviť podrobnosti konfigurácie nástroja Kontrola pošty a Anti-Spam:

10.5.1. Kontrola pošty

Dialógové okno ***E-mail Scanner*** je rozdelené na tri časti:



Kontrola pošty

Táto časť umožňuje definovať tieto základné nastavenia pre prichádzajúce a/alebo odchádzajúce e-mailové správy:

- ***Kontrolovať prichádzajúce e-maily*** (*štandardne zapnuté*) – začiarknutím zapnite resp. vypnite funkciu na prehľadávanie všetkých e-mailových správ doručených do vašej poštovej aplikácie.
- ***Kontrolovať odchádzajúce e-maily*** (*štandardne vypnuté*) – začiarknutím zapnite resp. vypnite funkciu na prehľadávanie všetkých e-mailov poslaných z vašej poštovej aplikácie.
- ***Zmeniť predmet správ infikovaných vírusom*** (*štandardne vypnuté*) – ak chcete byť informovaný o detekovaní infekcie v prehľadanej e-mailovej správe, začiarknite túto položku a do textového poľa zadajte požadovaný text. Tento text sa potom pridá do poľa „Predmet“ každej detekovanej e-mailovej správy na účely jednoduchšej identifikácie a filtrovania.

Predvolená hodnota je ***VIRUS*** a odporúčame vám, aby ste ju nemenili.

Vlastnosti prehľadávania

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

- ***Použiť heuristiku*** (*štandardne zapnuté*) – začiarknite túto možnosť, ak chcete používať metódu heuristického detekovania pri prehľadávaní 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.

- ***Hlásiť potenciálne nežiaduce programy a hrozby spyware*** (*štandardne zapnuté*) – začiarknite toto okienko, ak chcete zapnúť súčasť Anti-Spyware a vyhľadávať spyware a vírusy. Spyware predstavuje pochybnú kategóriu škodlivého softvéru: hoci v bežných situáciách predstavuje bezpečnostné riziko, niektoré takéto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.

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

- ***Prehľadávať vo vnútri archívov*** (*štandardne zapnuté*) – začiarknite toto okienko, ak sa má prehľadávať obsah archívov priložených k e-mailovým správam.

- ***Zapnúť dôkladné prehľadávanie*** (*štandardne vypnuté*) – v určitých situáciách (*napr. pri podozrení na infikovanie počítača vírusom alebo zneužitím*) môžete začiarknutím tohto okienka zapnúť algoritmus najdôkladnejšieho prehľadávania, ktorý prehľadá aj tie oblasti počítača, ktoré bývajú infikované len vo výnimočných prípadoch – len pre istotu. Upozorňujeme však, že tento spôsob je náročný na čas.

Hlásenie príloh e-mailov

Táto časť umožňuje nastaviť ďalšie správy o súboroch, ktoré môžu byť potenciálne nebezpečné alebo podozrivé. Nezobrazí sa žiadne dialógové okno s upozornením, len sa pridá text certifikácie na koniec e-mailovej správy a všetky takéto správy sa uvedú v dialógovom okne Detekcia súčasti E-mail Scanner:

- ***Hlásiť archívy chránené heslom*** – archivačné súbory (*ZIP, RAR atď.*) chránené heslom sa nedajú prehľadávať z hľadiska prítomnosti vírusov; začiarknite toto okienko, ak sa majú hlásiť tieto archívy ako potenciálne nebezpečné.

- ***Hlásiť dokumenty chránené heslom*** – dokumenty chránené heslom sa nedajú prehľadávať z hľadiska prítomnosti vírusov; začiarknite toto okienko, ak sa majú hlásiť tieto dokumenty ako potenciálne nebezpečné.

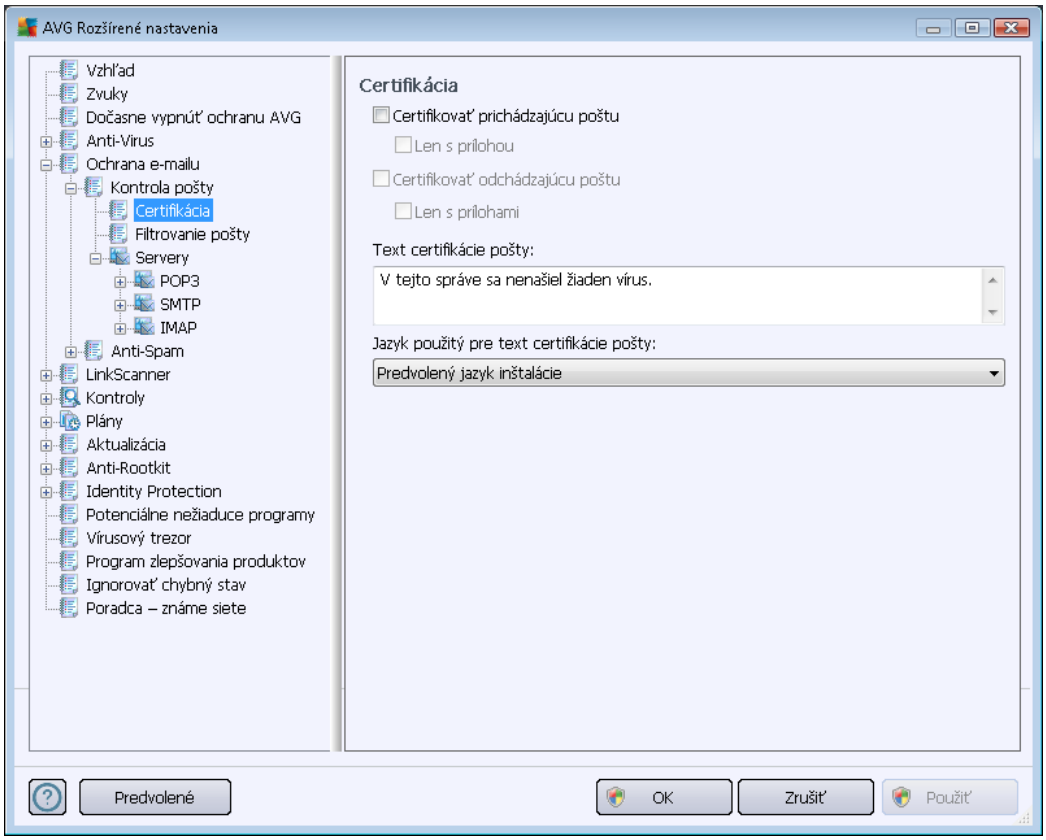
- ***Hlásiť súbory obsahujúce makrá*** – makro je vopred definovaný sled krokov, ktoré

zjednodušujú konkrétne úlohy používateľovi (*makrá sa bežne používajú v programe MS Word*). Makro, ako také, môže obsahovať potenciálne nebezpečné inštrukcie, a preto je vhodné začiarknuť toto okienko, aby sa súbory s makrami hlásili ako podozrivé.

- ***Hlásiť skryté prípony*** – skrytá prípona môže spôsobiť, že sa bude podozrivý spustiteľný súbor „niečo.txt.exe“ javiť ako neškodný jednoduchý textový súbor „niečo.txt“. Začiarknite toto okienko, ak majú byť hlásené ako potenciálne nebezpečné.

- ***Premiestniť hlásené prílohy do Vírusového trezora*** – nastavte, či si želáte byť informovaný e-mailom o archívoch chránených heslom, dokumentoch chránených heslom, súboroch s makrami alebo súboroch so skrytou príponou, ktoré boli detekované ako príloha prehľadávanej e-mailovej správy. Ak sa má táto správa zobraziť počas prehľadávania, potom nastavte, či sa má detekovaný infikovaný objekt premiestniť do Vírusového trezora.

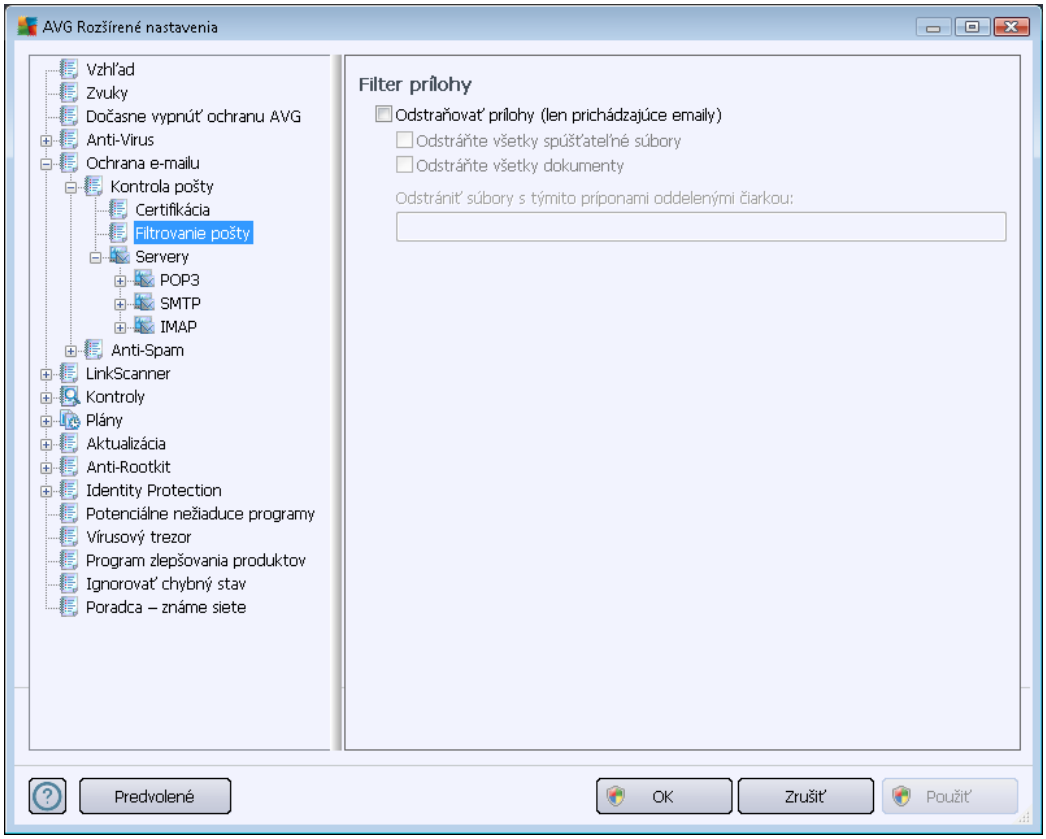
V dialógovom okne ***Certifikácia*** môžete označiť konkrétne začiarkavacie políčka a určiť, či chcete certifikovať prichádzajúcu poštu (***Potvrdiť prichádzajúcu poštu***) alebo odchádzajúcu poštu (***Potvrdiť odchádzajúcu poštu***). Pri každej možnosti môžete ďalej určiť parameter ***Len s prílohou***.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



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

sa nenašiel žiadny vírus) zobraziť.

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



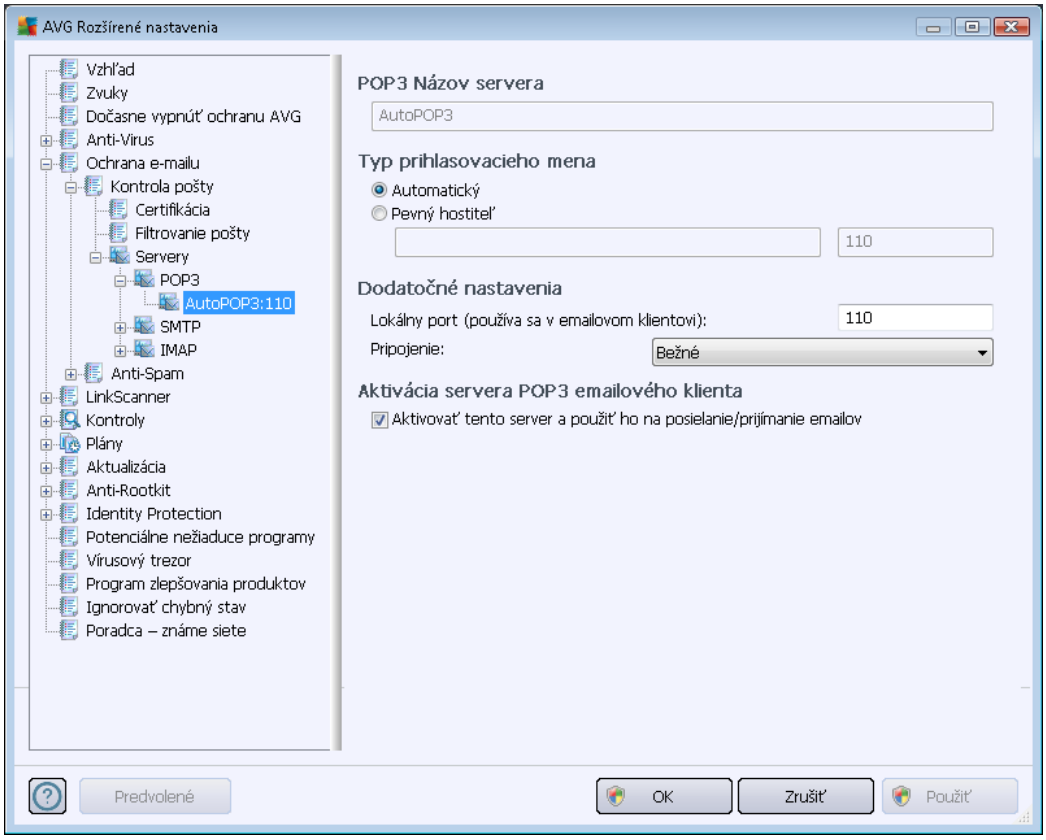
Dialógové okno ***Filter príloh*** umožňuje nastaviť parametre kontroly príloh e-mailových správ. Štandardne je možnosť ***Odstrániť prílohy*** vypnutá. Keď ju zapnete, potom sa všetky prílohy e-mailových správ detekované ako infekcie alebo potenciálne nebezpečné programy automaticky odstránia. Ak chcete definovať konkrétne typy príloh, ktoré sa majú odstrániť, vyberte príslušnú možnosť:

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

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

- Server POP3
- Server SMTP
- Server IMAP

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



Toto dialógové okno (*otvára sa v ponuke **Servery/POP3***) umožňuje nastaviť nový server súčasti E-mail Scanner pomocou protokolu POP3 pre prichádzajúcu poštu:

- ***Názov servera POP3*** – do tohto poľa zadajte názov novo pridaných serverov (*na pridanie servera POP3 kliknite pravým tlačidlom myši na položku POP3 v ľavej navigačnej ponuke*). Pre automaticky vytvorený server „AutoPOP3“ je toto pole vypnuté.
- ***Typ prihlasovacieho mena*** – určujte spôsob stanovenia poštového servera pre prichádzajúcu poštu:

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

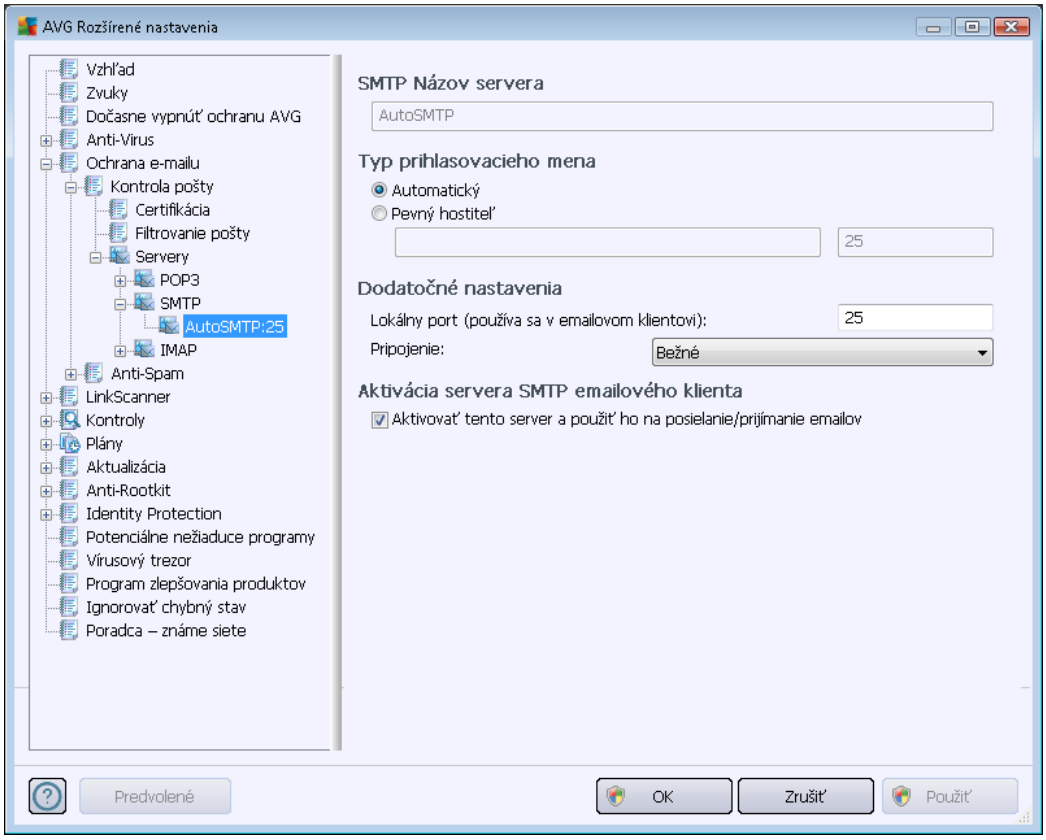
- ***Pevný hostiteľ*** – v tomto prípade program vždy použije server, ktorý je tu uvedený. Zadajte adresu alebo názov vášho poštového servera. Prihlasovacie meno zostane nezmenené. Ako názov môžete použiť názov domény (*napríklad pop.acme.com*) alebo adresu IP (*napríklad 123.45.67.89*). Ak poštový server používa neštandardný port, môžete zadať tento port za názvom servera a použite dvojbodku ako oddeľovací znak (*napríklad pop.acme.com:8200*). Štandardný port pre komunikáciu POP3 je 110.

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

  - ***Lokálny port*** – určuje port, na ktorom sa očakáva komunikácia prichádzajúca z vašej poštovej aplikácie. Potom musíte v poštovej aplikácii nastaviť tento port ako port pre komunikáciu POP3.

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

- ***Aktivovanie servera POP3 v poštovej aplikácii*** – začiarknutím alebo zrušením začiarknutia tejto položky sa aktivuje resp. deaktivuje uvedený server POP3.



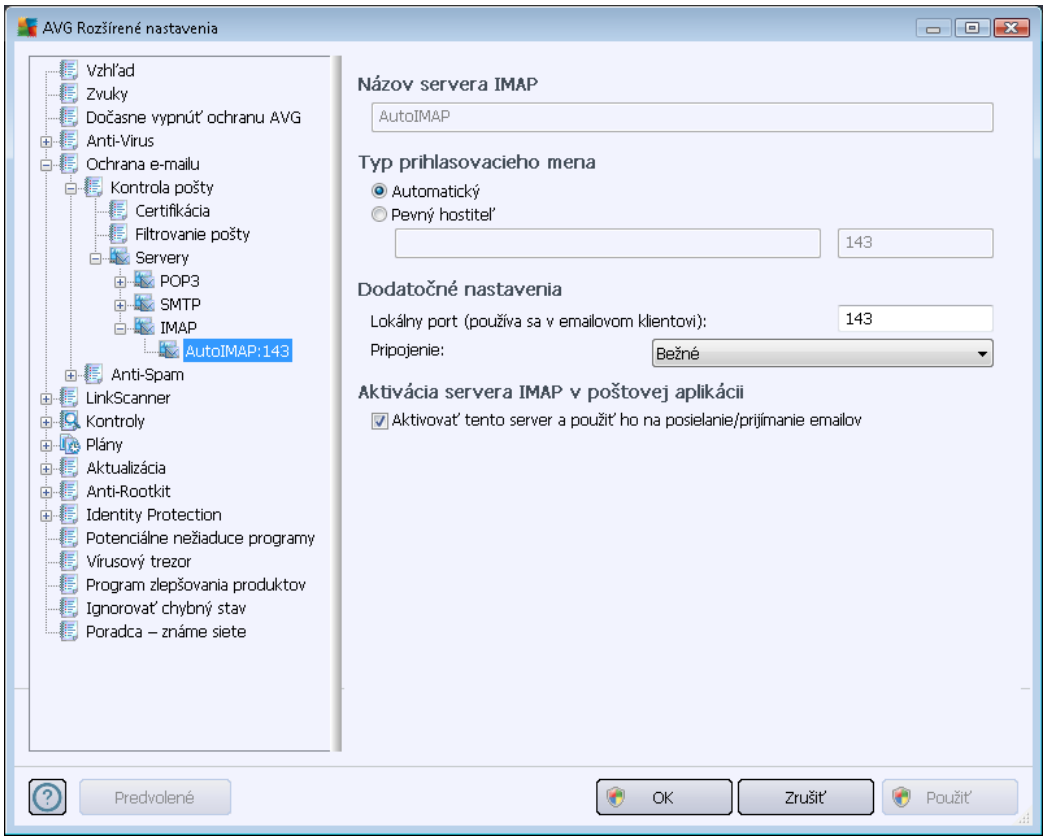
Toto dialógové okno (*otvára sa v ponuke **Servery/SMTP***) umožňuje nastaviť nový server E-mail Scanner pomocou protokolu SMTP pre odchádzajúcu poštu:

- ***Názov servera SMTP*** – do tohto poľa zadajte názov novo pridaných serverov (*na pridanie servera SMTP kliknite pravým tlačidlom myši na položku SMTP v ľavej navigačnej ponuke*). Pre automaticky vytvorený server „AutoSMTP“ je toto pole vypnuté.
- ***Typ prihlásenia*** – určuje spôsob zistenia poštového servera, ktorý sa používa pre prichádzajúcu poštu:
  - ***Automaticky*** – prihlásenie sa uskutoční automaticky podľa nastavení poštovej aplikácie.
  - ***Pevný hostiteľ*** – v tomto prípade program vždy použije server, ktorý je tu uvedený. Zadajte adresu alebo názov vášho poštového servera. Ako názov môžete použiť názov domény (*napríklad smtp.acme.com*) alebo adresu IP (*napríklad 123.45.67.89*). Ak poštový server používa neštandardný port, môžete zadať tento port za názvom servera. Ako oddeľovací znak použite dvojbodku (*napríklad smtp.acme.com:8200*). Štandardný port komunikácie SMTP je 25.
- ***Ďalšie nastavenia*** – používa sa na definovanie podrobnejších parametrov:
  - ***Lokálny port*** – určuje port, na ktorom sa očakáva komunikácia prichádzajúca z

vašej poštovej aplikácie. Potom musíte v poštovej aplikácii nastaviť tento port ako port pre komunikáciu SMTP.

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

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



Toto dialógové okno (otvára sa pomocou ponuky ***Servery/IMAP***) umožňuje nastaviť nový server typu E-mail Scanner pomocou protokolu IMAP pre odchádzajúcu poštu:

- ***Názov servera IMAP*** – do tohto poľa zadajte názov novo pridaných serverov (*na pridanie servera IMAP kliknite pravým tlačidlom myši na položku IMAP v ľavej navigačnej ponuke*). Pre automaticky vytvorený server „AutoIMAP“ je toto pole vypnuté.

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

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

- ***Pevný hostiteľ*** – v tomto prípade program vždy použije server, ktorý je tu uvedený. Zadajte adresu alebo názov vášho poštového servera. Ako názov môžete použiť názov domény (*napríklad smtp.acme.com*) alebo adresu IP (*napríklad 123.45.67.89*). Ak poštový server používa neštandardný port, môžete zadať tento port za názvom servera použitím dvojbodky ako oddeľovací znak (*napríklad smtp.acme.com:8200*). Štandardný port pre komunikáciu IMAP je 143.

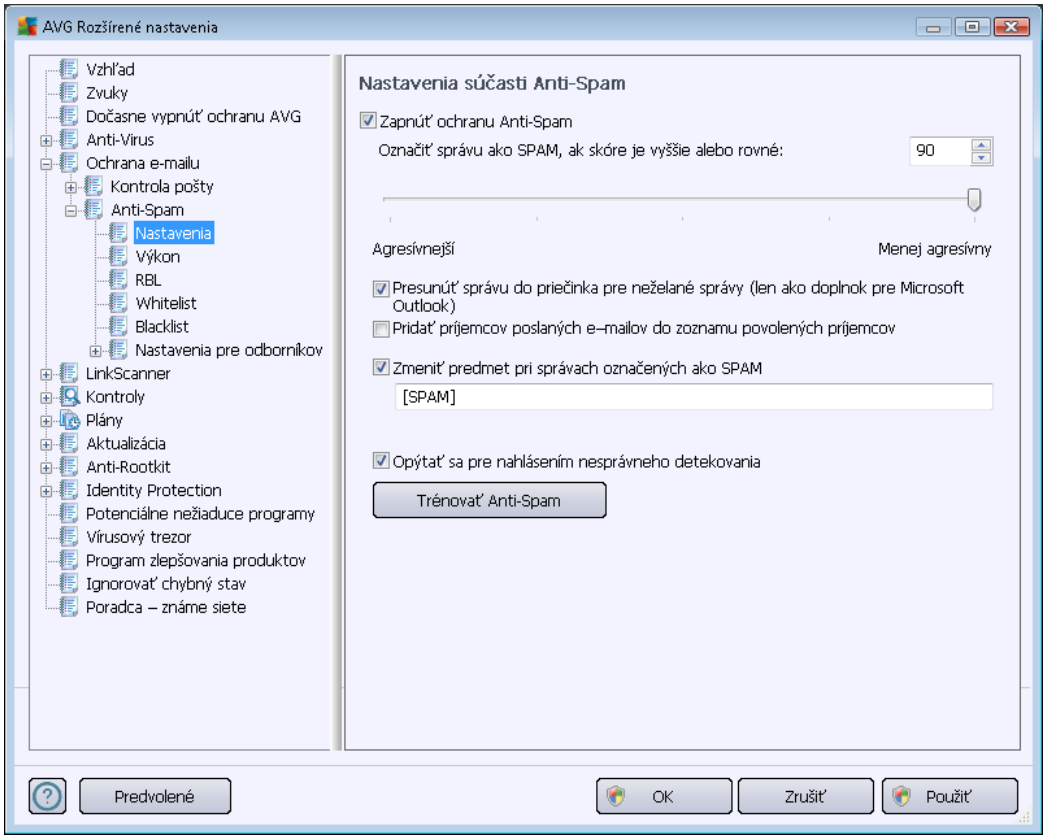
- ***Ďalšie nastavenia*** – používa sa na definovanie podrobnejších parametrov:

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

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

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

10.5.2. Anti-Spam



V dialógovom okne ***Nastavenia súčasti Anti-Spam*** môžete začiarknutím alebo zrušením začiarknutia políčka ***Zapnúť ochranu Anti-Spam*** zapnúť resp. vypnúť kontrolu e-mailovej komunikácie súčasťou Anti-Spam. Táto možnosť je štandardne zapnutá a odporúčame vám, aby ste toto nastavenie nikdy nemenili, ak na to nemáte skutočný dôvod.

Ďalej 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 SPAMU*) na základe niekoľkých dynamických metód kontroly. Hodnotu funkcie ***Označiť správu ako spam, keď je skóre vyššie ako*** môžete nastaviť buď zadaním hodnoty, alebo posunutím posúvača smerom doľava alebo doprava (*nastavené hodnoty môžu byť v rozsahu 50 – 90*).

Odporúčame vám, aby ste nastavili prahovú hodnotu v pásme 50 – 90, prípade ak máte naozaj pochybnosti ohľadne nastavenia, potom nastavte hodnotu 90. Toto je základný prehľad prahovej hodnoty skóre:

- ***Hodnota 80 – 90*** – Budú sa filtrovať tie e-mailové správy, ktoré veľmi pravdepodobne patria medzi nevyžiadanú poštu. Niektoré správy, ktoré nie sú spam, sa môžu filtrovať nesprávne.
- ***Hodnota 60 – 79*** – považuje sa za pomerne agresívne nastavenie. E-mailové správy, ktoré môžu predstavovať spam, sa budú filtrovať. Môžu sa zachytiť aj správy, ktoré nie sú spam.
- ***Hodnota 50 – 59*** – veľmi agresívne nastavenie. E-mailové správy, ktoré nie sú spam, sa pravdepodobne zachytia ako spamové správy. Neodporúčame vám používať toto nastavenie na normálne účely.

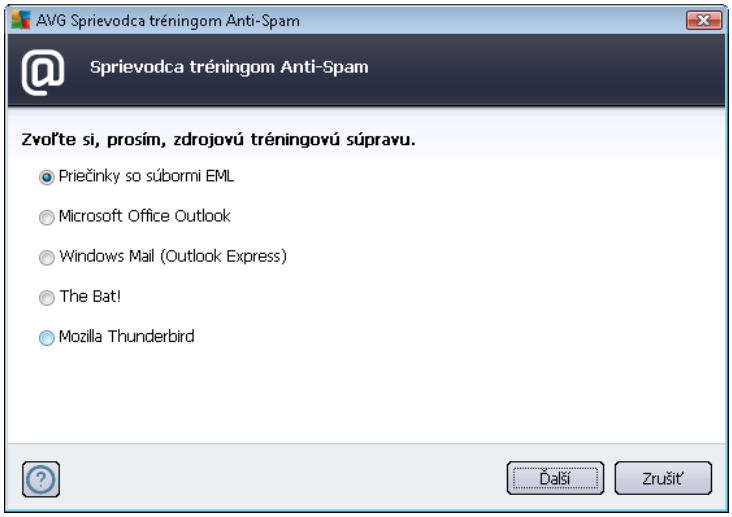
V dialógovom okne ***Nastavenia súčasti Anti-Spam*** môžete ďalej definovať, ako sa bude zaobchádzať s nájdeným spamom:

- ***Premiestniť správu do priečinka pre spam*** *(platí len pre zásuvný modul Microsoft Outlook)* – začiarknite toto políčko, ak sa má každý detegovaný spam automaticky premiestniť do konkrétneho priečinka pre spam v poštovej aplikácii MS Outlook. V súčasnosti túto službu iné poštové aplikácie nepodporujú.
- ***Pridať príjemcov poslaných e-mailov do zoznamu povolených*** – začiarknite toto políčko, ak sa majú všetci príjemcovia poslaných e-mailov považovať za dôveryhodných a aby bolo možné doručovať všetky e-mailové správy prichádzajúce z ich e-mailových schránok.
- ***Zmeniť predmet správ označených ako SPAM*** – Toto políčko označte vtedy,ak sa majú všetky správy označené ako spam označiť špecifickým slovom alebo znakom v riadku s predmetom e-mailu, pričom požadovaný text sa vkladá do zapnutého textového poľa.
- ***Opýtať sa pred hlásením nesprávnej detekcie*** – pod podmienkou, že ste počas inštalácie súhlasili s účasťou v programe zlepšovania produktov. V tom prípade ste povolili hlásenie zistených hrozieb spoločnosti AVG. Hlásenie sa uskutoční automaticky. Keď však začiarknete toto okienko, potom sa vás pred nahlásením detekovaného spamu do AVG program opýta, či sa má správa naozaj klasifikovať ako spam.

Ovládacie tlačidlá

Tlačidlo Trénovať Anti-Spam otvorí sprievodcu trénovaním súčasti Anti-Spam. Informácie o tomto sprievodcovi sa nachádzajú v ďalšej kapitole.

Prvé dialógové okno ***Sprievodcu trénovaním Anti-Spamu*** vás požiada, aby ste zvolili zdroj emailových správ, ktoré chcete použiť na trénovanie. Obyčajne budete chcieť použiť buď emaily, ktoré boli nesprávne označené ako SPAM alebo spamové správy, ktoré neboli rozpoznané.



Môžete si zvoliť z nasledujúcich možností:

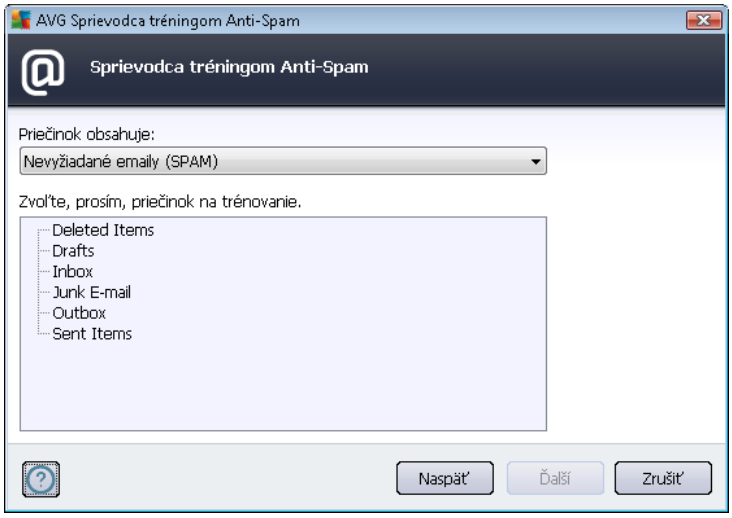
- ***Konkrétna poštová aplikácia*** – ak používate niektorú z uvedených poštových aplikácií (*MS Outlook, Outlook Express, The Bat!*), stačí, ak vyberiete príslušnú možnosť.
- ***Priečinok so súbormi EML*** – ak používate iný e-mailový program, najskôr si uložte správy do samostatného priečinka (*vo formáte eml*), alebo si zapamätajte umiestnenie priečinkov so správami, ktoré používa poštový klient. Potom zvoľte ***Priečinok so súbormi EML***, ktorý vám umožní lokalizovať želaný priečinok v ďalšom kroku

Pre rýchlejší a jednoduchší proces trénovania je dobré triediť emaily v priečinkoch vopred, takže priečinok, ktorý použijete na trénovanie, bude obsahovať len tréningové správy (či už chcené alebo nechcené). Nie je to však potrebné, keďže budete môcť filtrovať emaily neskôr.

Zvoľte vhodnú možnosť a kliknite na tlačidlo ***Ďalej*** pre pokračovanie sprievodcu.

Dialógové okno, ktoré sa otvorí v tomto kroku, závisí od výberu, ktorý ste urobili v predchádzajúcom kroku.

Priečinky so súbormi EML



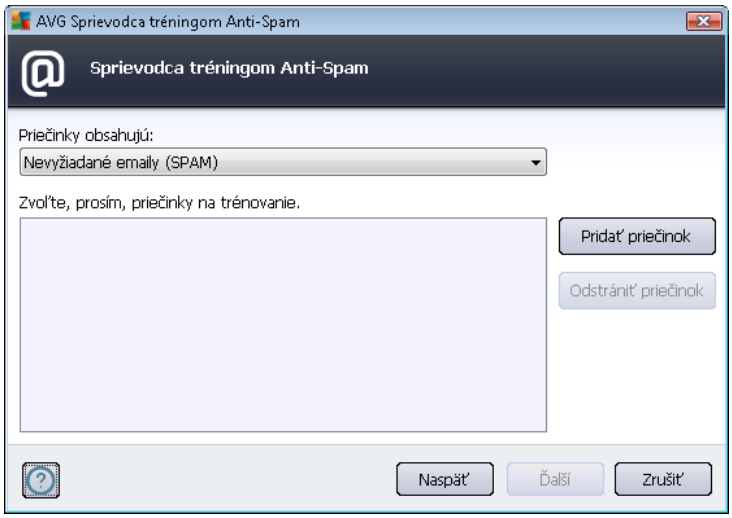
V tomto dialógovom okne vyberte priečinok so správami, ktorý chcete použiť na trénovanie. Stlačením tlačidla ***Pridať priečinok*** vyhľadajte priečinok so súbormi .eml (*uloženými e-mailovými správami*). Vybraný priečinok sa potom zobrazí v dialógovom okne.

V rozbaľovacej ponuke ***Priečinky obsahujú*** nastavte jednu z dvoch možností – či sa vo vybranom priečinku nachádzajú želané správy (*HAM*) alebo nevyžiadané správy (*SPAM*). V ďalšom kroku budete môcť správy filtrovať, takže priečinok nemusí obsahovať len trénovacie e-maily. Kliknutím na tlačidlo ***Odstrániť priečinok*** zároveň môžete odstrániť neželané vybrané priečinky zo zoznamu.

Nakoniec kliknutím na tlačidlo ***Ďalšie*** prejdite na možnosti filtrovania správ.

Výber poštovej aplikácie

Po potvrdení jednej z možností sa otvorí nové dialógové okno.

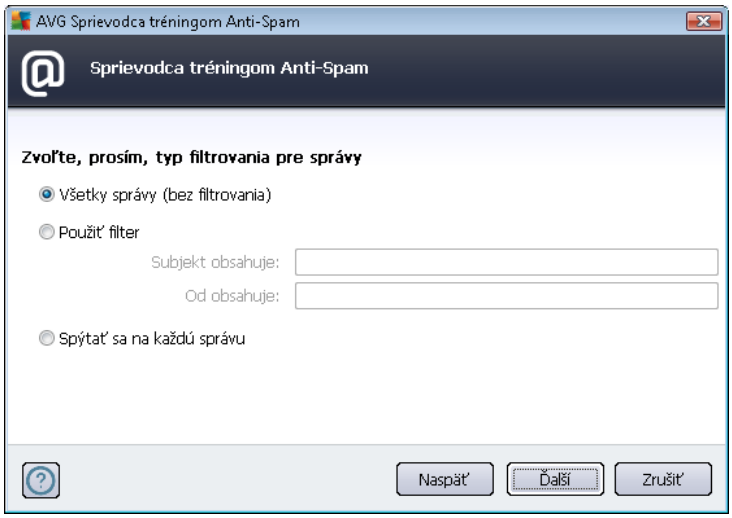


Poznámka: *Ak používate program Microsoft Office Outlook, program vás požiada, aby ste vybrali*

najskôr profil MS Office Outlook.

V rozbaľovacej ponuke ***Priečinky obsahujú*** nastavte jednu z dvoch možností – či sa vo vybranom priečinku nachádzajú želané správy (*HAM*) alebo nevyžiadané správy (*SPAM*). V ďalšom kroku budete môcť správy filtrovať, takže priečinok nemusí obsahovať len trénovacie e-maily. Navigačná štruktúra vybranej poštovej aplikácie je už zobrazená v hlavnej časti dialógového okna. Vyhľadajte želaný priečinok v navigačnej štruktúre a zvýraznite ho myšou.

Nakoniec kliknutím na tlačidlo ***Ďalšie*** prejdite na možnosti filtrovania správ.



Toto dialógové okno sa používa na nastavenie filtrovania e-mailových správ.

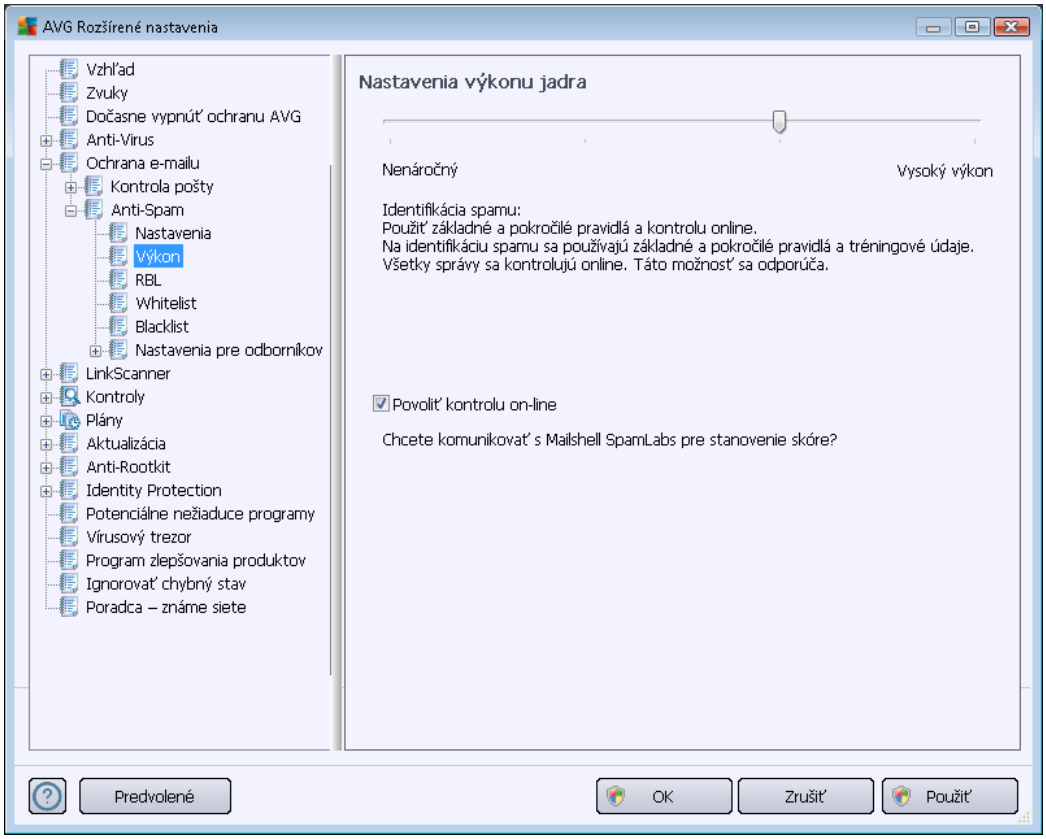
- ***Všetky správy (bez filtrovania)*** – Ak ste presvedčení, že sa vo vybranom priečinku nachádzajú len správy, ktoré chcete použiť na účely školenia, vyberte možnosť ***Všetky správy (bez filtrovania)***.

- ***Použiť filter*** – Ak chcete podrobnejšie filtrovať, vyberte možnosť ***Použiť filter***. Môžete doplniť slovo (*názov*), časť slova alebo vetu, ktorá sa má vyhľadať v predmete e-mailu alebo v poli odosielateľa. Všetky správy, ktoré sa presne zhodujú so zadanými kritériami, sa použijú na školenie bez zobrazenia ďalších otázok. Keď vyplníte obe textové polia, použijú sa aj adresy, ktoré sa zhodujú s jednou z dvoch uvedených podmienok!

- ***Spýtať sa na každú správu*** – Ak si nie ste istí správami v priečinku a chcete, aby sa vás sprievodca spýtal na každú správu *(aby ste mohli určiť, či sa má použiť na školenie alebo nie)*, vyberte možnosť ***Spýtať sa na každú správu***.

Po zvolení príslušnej možnosti kliknite na tlačidlo ***Ďalej***. Nasledujúce dialógové okno bude len informatívne, hovorí vám, že sprievodca je pripravený na spracovanie správ. Pre spustenie tréningu znovu kliknite na tlačidlo ***Ďalej***. Trénovanie sa potom začne podľa predtým zvolených podmienok.

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



Posunutím posúvača smerom doľava resp. doprava nastavte úroveň výkonu kontroly, od režimu ***Malé využitie pamäte*** po režim ***Vysoký výkon***.

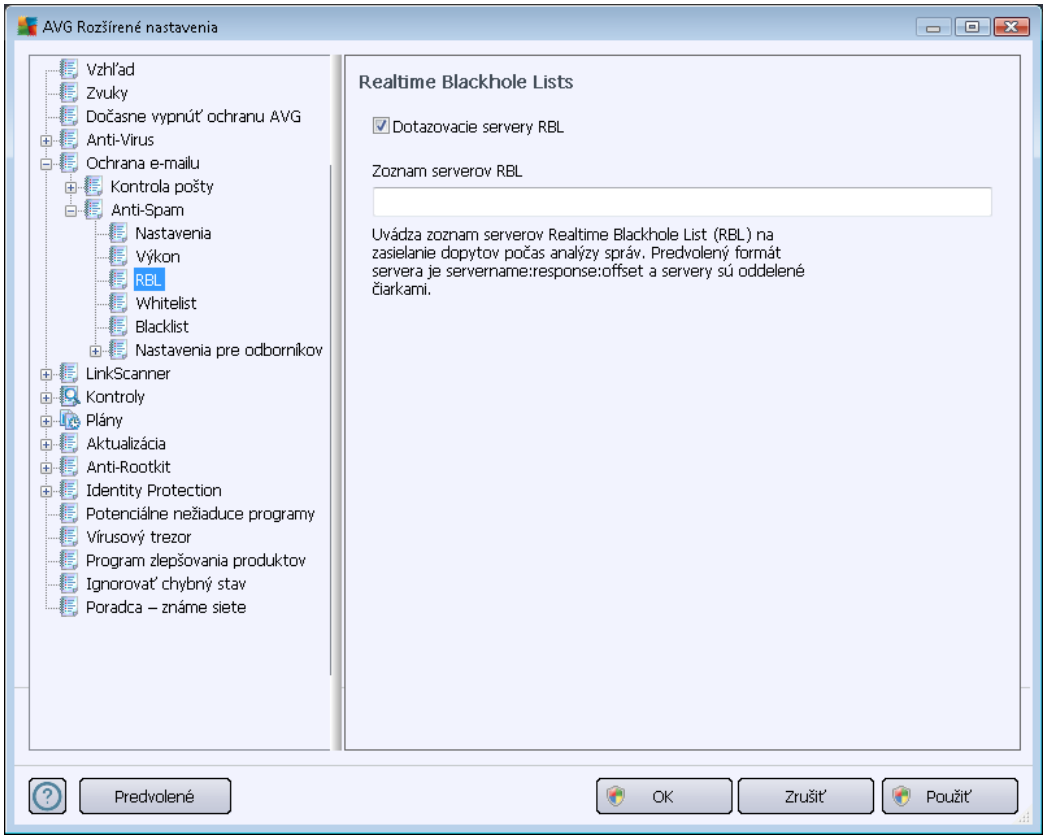
- ***Malé využitie pamäte*** – Pri kontrole sa nepoužijú žiadne pravidlá na identifikovanie spamu. Na identifikáciu sa použijú len tréningové údaje. Tento režim vám neodporúčame používať na bežné účely. Používajte ho len vtedy, keď má počítač veľmi slabý hardvér.

- ***Vysoký výkon*** – v tomto režime sa využíva veľké množstvo pamäte. Pri kontrole prítomnosti spamu sa použijú tieto funkcie: pravidlá a vyrovnávacia pamäť databázy spamu, základné a rozšírené pravidlá, adresy IP rozosielateľov spamu a databázy rozosielateľov spamu.

Položka ***Zapnúť on-line kontrolu*** je štandardne zapnutá. Používa sa na presnejšie zisťovanie spamu pomocou komunikácie so servermi Mailshell, t. j. kontrolované dáta sa porovnajú s on-line databázami Mailshell.

Odporúčame vám, aby ste zachovali predvolené nastavenia a zmenili ich len v prípade, keď na to máte vážny dôvod. Zmeny konfigurácie odporúčame robiť len skúseným používateľom!

Položka ***RBL*** otvorí dialógové okno na úpravy s názvom ***Realtime Blackhole Lists***, v ktorom môžete zapnúť alebo vypnúť funkciu ***Servery Query RBL***:

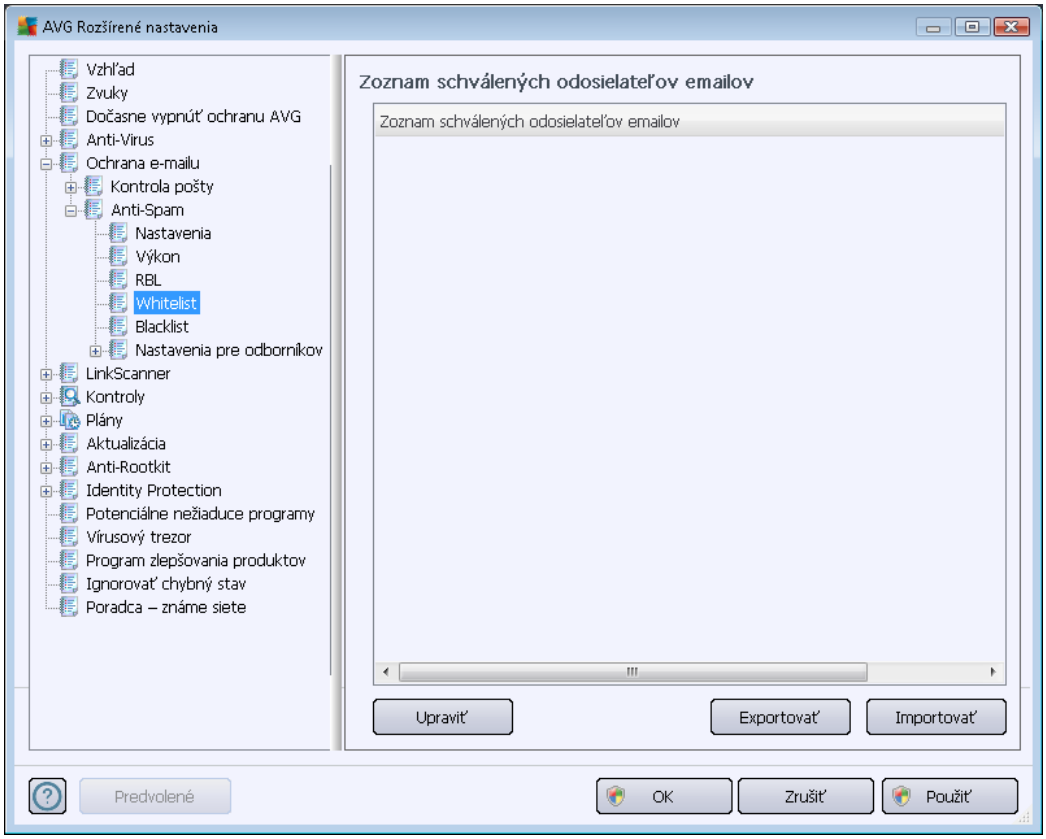


RBL (*Realtime Blackhole List*) server je DNS server s obsiahlou databázou známych odosielateľov spamov. Keď je táto funkcia zapnutá, všetky e-mailové správy sa porovnajú s databázou servera RBL a ak sa ich odosielateľ nachádza v databáze, označia sa ako spam. Databázy serverov RBL obsahujú najnovšie aktuálne hlavičky spamov, aby mohli poskytnúť tú najlepšiu a najpresnejšiu detekciu spamov. Táto funkcia je zvlášť užitočná pre používateľov, ktorí dostávajú veľké množstvo spamov, ktoré normálne zariadenie Anti-Spam nezistí.

Zoznam serverov RBL umožňuje definovať špecifické umiestnenia servera RBL (*povolením tejto možnosti sa v niektorých systémoch a pri určitých konfiguráciách môže spomaliť prijímanie e-mailov, pretože každá správa sa musí overiť podľa databázy servera RBL).*

Na server sa neposielajú žiadne osobné údaje!

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



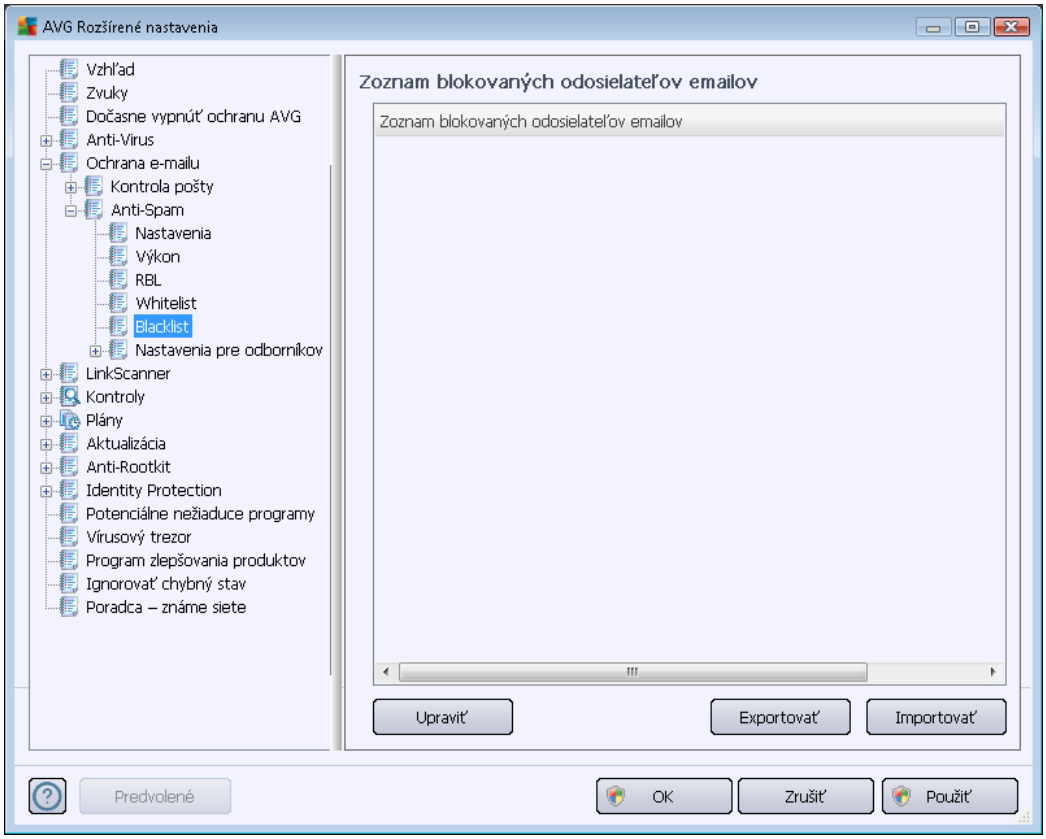
Editačné rozhranie umožňuje zostaviť zoznam odosielateľov, o ktorých ste presvedčený, že vám nikdy nepošlú nevyžiadané správy (spam). Zároveň môžete vytvoriť zoznam úplných názvov domén (*e.g. avg.com*), o ktorých viete, že nevytvárajú spamové správy. Keď máte zostavený takýto zoznam odosielateľov a/alebo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

Ovládacie tlačidlá

Sú dostupné nasledovné ovládacie tlačidlá:

- ***Editovať*** – po stlačení tohto tlačidla sa otvorí dialógové okno, do ktorého môžete ručne zadať zoznam adries (*môžete použiť aj metódu kopírovať a prilepiť*). Do každého riadka vložte vždy jednu položku (*odosielateľa, 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 emailovými adresami / názvami domén, môžete ho len importovať pomocou tohto tlačidla. Súbor môže obsahovať len jednu položku (*adresu, názov domény*) v každom riadku.

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



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

Ovládacie tlačidlá

Sú dostupné nasledovné ovládacie tlačidlá:

- ***Editovať'*** – po stlačení tohto tlačidla sa otvorí dialógové okno, do ktorého môžete ručne zadať zoznam adries (*môžete použiť aj metódu kopírovať a prilepiť*). Do každého riadka vložte vždy jednu položku (*odosielateľa, 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 emailovými adresami / názvami

domén, môžete ho len importovať pomocou tohto tlačidla.

Vo vetve Rozšírené nastavenia sa nachádzajú široké možnosti nastavenia súčasti Anti-Spam. Tieto nastavenia sú určené výhradne pre skúsených používateľov, zvyčajne správcov siete, ktorí potrebujú veľmi 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 vám odporúčame, aby ste nemenili žiadne nastavenia, ak nie ste dokonale oboznámený s rozšírenými nastaveniami programu Spamcatcher (MailShell Inc.). Každá nevhodná zmena môže mať za následok zníženie výkonu alebo nesprávne fungovanie aplikácie.

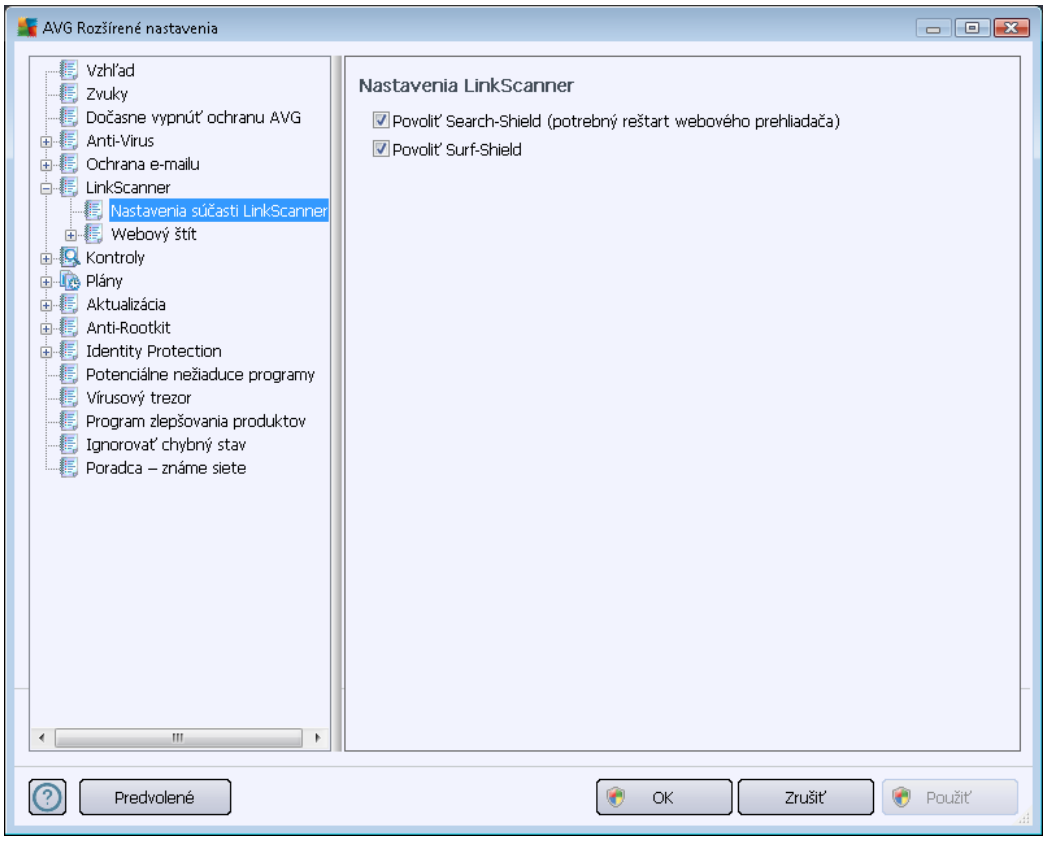
Ak sa aj napriek tomu rozhodnete zmeniť konfiguráciu súčasti Anti-Spam na veľmi podrobnej úrovni, postupujte podľa pokynov uvedených priamo v používateľskom rozhraní. V každom dialógovom okne sa bežne nachádza jedna konkrétna funkcia, ktorú môžete upraviť – jej opis sa vždy nachádza v samotnom dialógovom okne:

- ***Vyrovnávacia pamäť*** – odtlačok, názov domény, LegitRepute.
- ***Trénovanie*** – maximálny počet slov, prahová hodnota automatického trénovania, váhy.
- ***Filtrovanie*** – zoznam jazykov, zoznam krajín, povolené adresy IP, blokované adresy IP, blokované krajiny, blokované súbory znakov, nežiaduci odosielatelia.
- ***RBL*** – servery RBL, viacnásobné detekovanie, prahová hodnota, časový limit, maximálny počet adries IP.
- ***Internetové pripojenie*** – časový limit, server proxy, autentifikácia servera proxy.

10.6. LinkScanner

10.6.1. Nastavenia súčasti LinkScanner

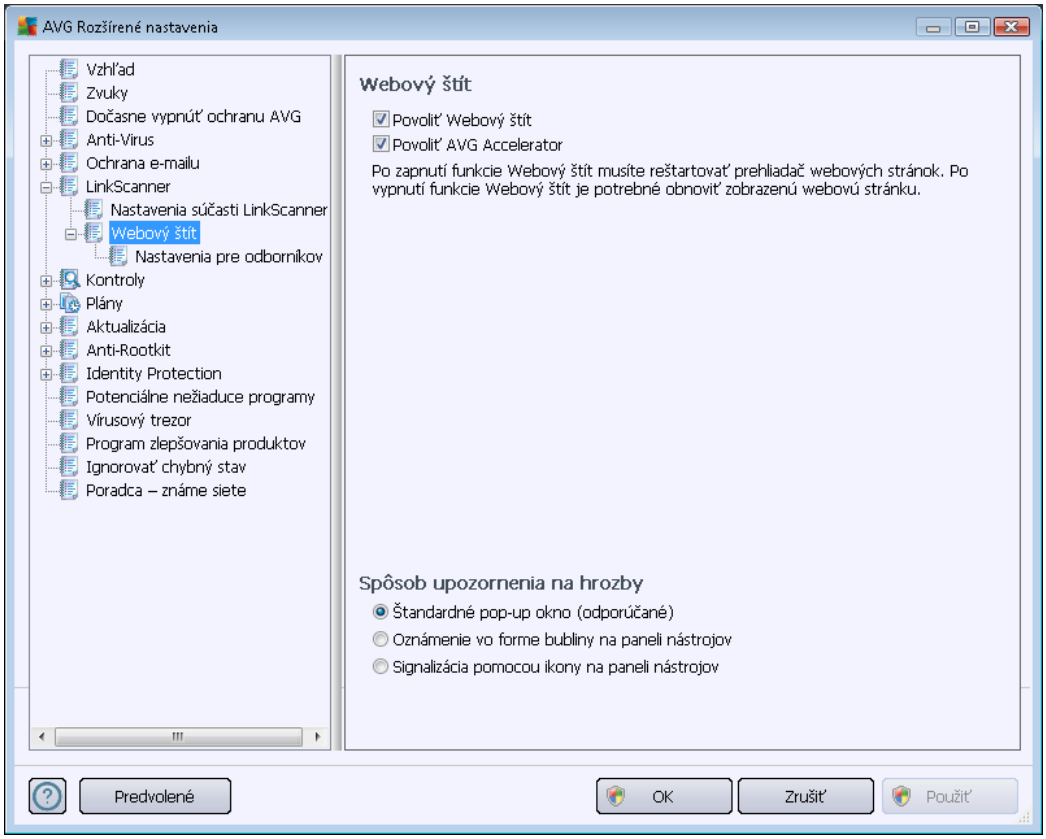
Dialógové okno ***Nastavenia súčasti LinkScanner*** umožňuje zapnúť a vypnúť základné funkcie súčasti LinkScanner:



- ***Zapnúť Search-Shield*** (*štandardne zapnuté*): informačné ikony s odporúčaniami pre výsledky vyhľadávania vo vyhľadávačoch Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg a SlashDot a vopred skontrolované.

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

10.6.2. Webový štít



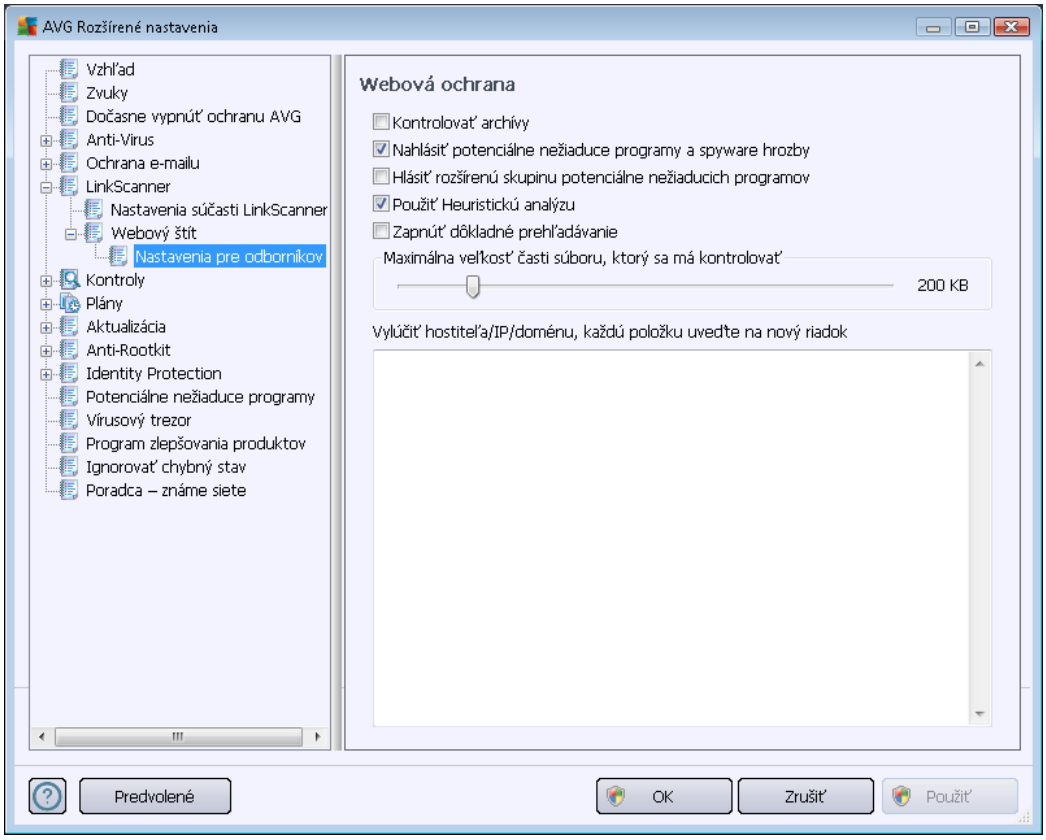
Dialógové okno ***Webový štít*** ponúka tieto možnosti:

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

- ***Povoliť AVG Accelerator*** *(štandardne zapnuté)* – Aktivuje/deaktivuje službu ***AVG Accelerator*** , ktorá umožňuje stabilnejšie prehrávanie on-line videa a uľahčuje ďalšie preberania.

Spôsob upozornenia na hrozby

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



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

- ***Zapnúť webovú ochranu*** – keď je táto funkcia zapnutá, potom bude súčasť ***Webový štít*** kontrolovať obsah internetových stránok. Keď je táto možnosť zapnutá (*štandardne*), môžete ďalej zapnúť alebo vypnúť tieto položky:
    - ***Kontrolovať archívy*** – (*štandardne vypnuté*): kontrolovať obsah archívov, ktoré sa môžu nachádzať na otvorenej internetovej stránke.
    - ***Hlásiť potenciálne nežiaduce programy a hrozby spyware*** – (*štandardne zapnuté*): označením aktivujete zariadenie Anti-Spyware, ktoré kontroluje spyware aj vírusy. Spyware predstavuje pochybnú kategóriu škodlivého softvéru: hoci v bežných situáciách predstavuje bezpečnostné riziko, niektoré takéto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
    - ***Hlásiť rozšírenú skupinu potenciálne nežiaducich programov*** – (*štandardne vypnuté*): začiarknite toto okienko, ak sa má detekovať rozšírená skupina spywaru: programov, ktoré sú úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpečenia počítača, ale môže blokovať dobré programy, a preto je táto funkcia štandardne vypnutá.

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

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

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

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

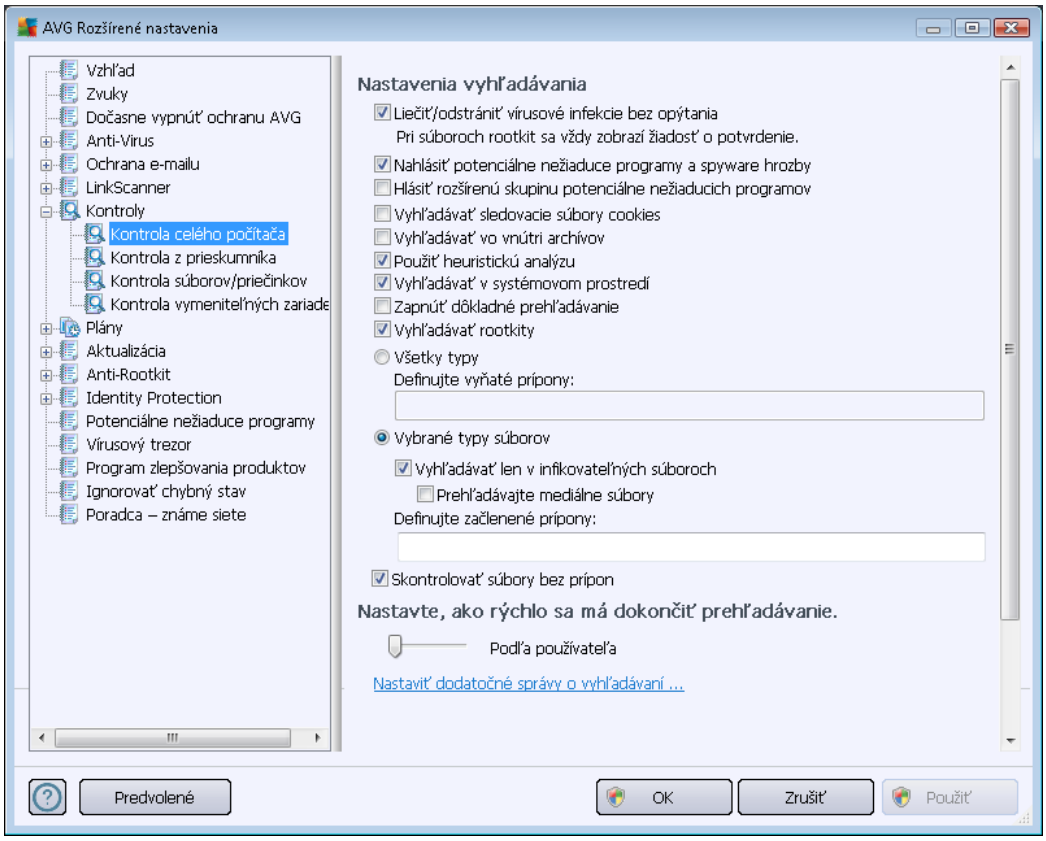
10.7. Kontroly

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

- ***Kontrola celého počítača*** – štandardné preddefinovaná kontrola celého počítača.
- ***Kontrola z prieskumníka*** – špeciálna kontrola vybraného objektu priamo v prostredí programu Prieskumník.
- ***Kontrola súborov/priečinkov*** – štandardná vopred definovaná kontrola vybraných oblastí počítača.
- ***Kontrola vymeniteľných zariadení*** – špeciálna kontrola vymeniteľných zariadení pripojených k počítaču.

10.7.1. Kontrola celého počítača

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



Nastavenia kontroly

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

- ***Liečiť/odstrániť infekciu bez opýtania*** (*štandardne zapnuté*) – Ak sa počas kontroly zistí prítomnosť vírusu, môže sa automaticky vyliečiť, ak je k dispozícii liečba. Ak nie je možné infikovaný súbor vyliečiť automaticky, premiestni sa do vírusového trezora.
- ***Hlásiť potenciálne nežiaduce programy a hrozby spyware*** (*štandardne zapnuté*) – Toto políčko označte, ak chcete zapnúť súčasť Anti-Spyware a kontrolovať spyware a vírusy. Spyware predstavuje pochybnú kategóriu škodlivého softvéru: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
- ***Hlásiť rozšírenú skupinu potenciálne nežiaducich programov*** (*štandardne vypnuté*) – Toto políčko začiarknite, ak sa má zistiť rozšírená skupina spyware – programov, ktoré sú

úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpečenia počítača, ale môže blokovať dobré programy, a preto je táto funkcia štandardne vypnutá.

- ***Kontrolovať sledovacie súbory cookies*** (*štandardne vypnuté*) – tento parameter súčasti Anti-Spyware zapína funkciu na detekovanie súborov cookies (*HTTP cookies sa používajú na overenie totožnosti, sledovanie a správu konkrétnych informácií o používateľoch, ako sú preferencie stránok alebo obsah elektronických nákupných košíkov*).

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

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

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

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

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

Ďalej rozhodnite, či chcete kontrolovať:

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

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

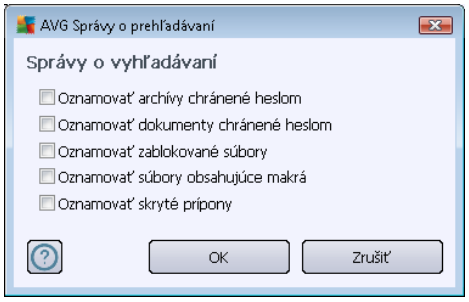
- Alternatívne môžete rozhodnúť, že chcete ***kontrolovať súbory bez prípony***. Táto možnosť je štandardne zapnutá a odporúčame vám, aby ste toto nastavenie nikdy nemenili, ak na to nemáte skutočný dôvod. Súbory bez prípony sú skôr podozrivé a mali by sa vždy kontrolovať.

Nastaviť rýchlosť dokončenia kontroly

V časti ***Nastaviť rýchlosť dokončenia kontroly*** môžete ďalej nastaviť požadovanú rýchlosť kontroly v závislosti od využívania počítačových zdrojov. Štandardne má tento parameter nastavenú úroveň automatického využívania zdrojov *„podľa používateľa*“. Ak chcete, aby kontrola prebiehala rýchlejšie, bude trvať kratšie, ale výrazne sa zvýši využitie systémových zdrojov a spomalia sa ostatné činnosti počítača (*táto možnosť sa môže použiť, keď je počítač zapnutý, ale nikto na ňom momentálne nepracuje*). Na druhej strane môžete znížiť využívanie počítačových zdrojov predĺžením doby trvania kontroly.

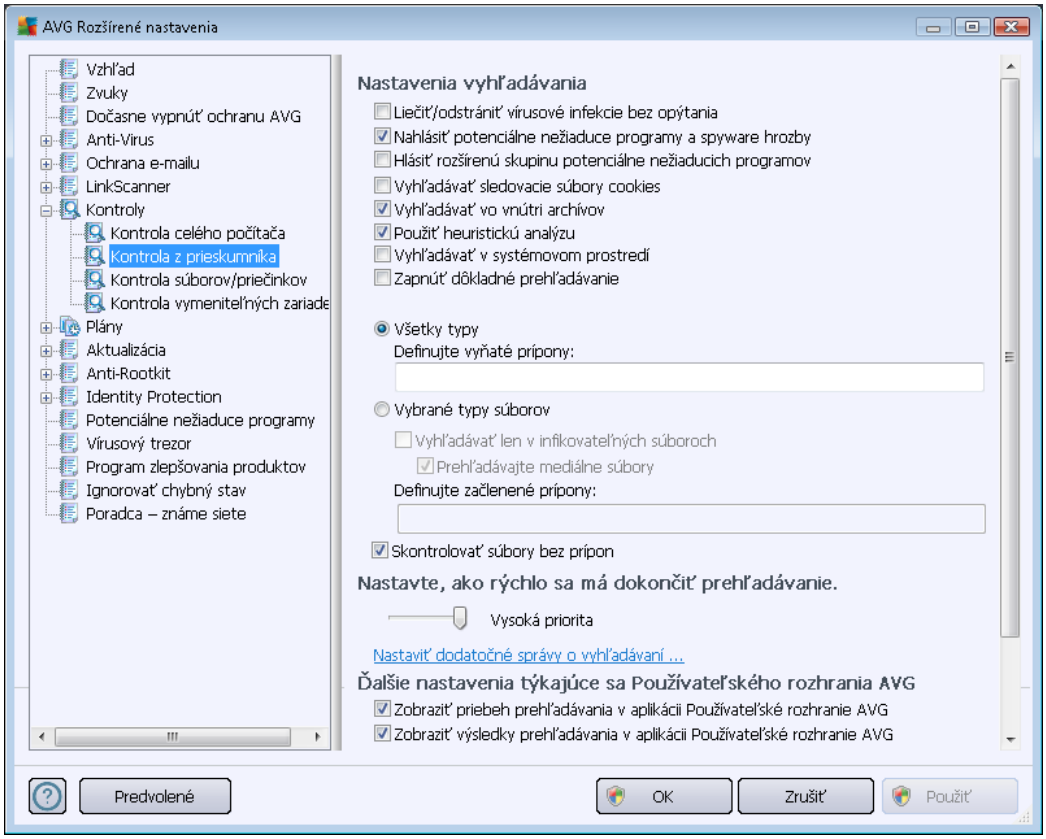
Vytvoriť ďalšie správy o kontrole...

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



10.7.2. 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 Prieskumník (*shell extension*), pozri kapitolu Kontrola z prieskumníka:



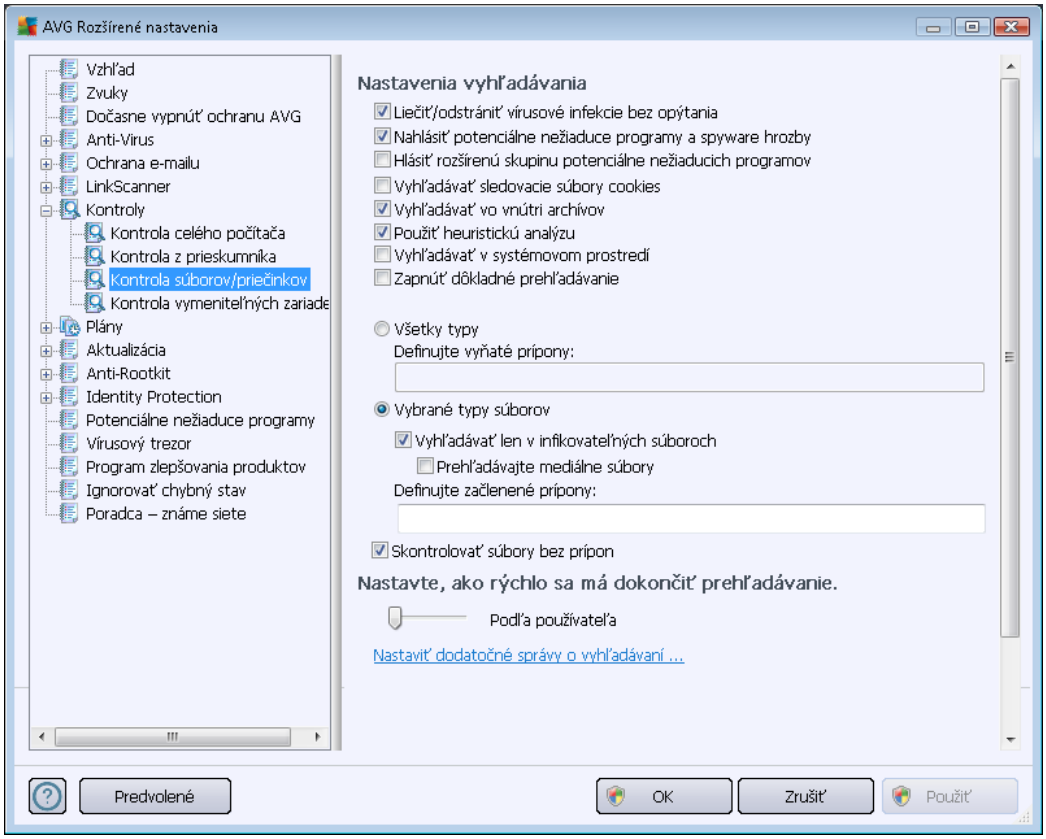
Zoznam parametrov je identický s parametrami použiteľnými pre kontrolu celého počítača. Predvolené nastavenia sa však líšia (*napríklad Kontrola celého počítača štandardne nekontroluje archívy, ale kontroluje systémové prostredie, zatiaľ čo Kontrola z prieskumníka má presne opačné nastavenia*).

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

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

10.7.3. Kontrola súborov/priečinkov

Rozhranie editácie na ***prehľadávanie konkrétnych súborov alebo priečinkov*** je rovnaké ako dialógové okno editácie s názvom Prehľadávať celý počítač. Všetky možnosti konfigurácie sú rovnaké, predvolené nastavenia sú však prísnejšie pri prehľadávaní celého počítača:

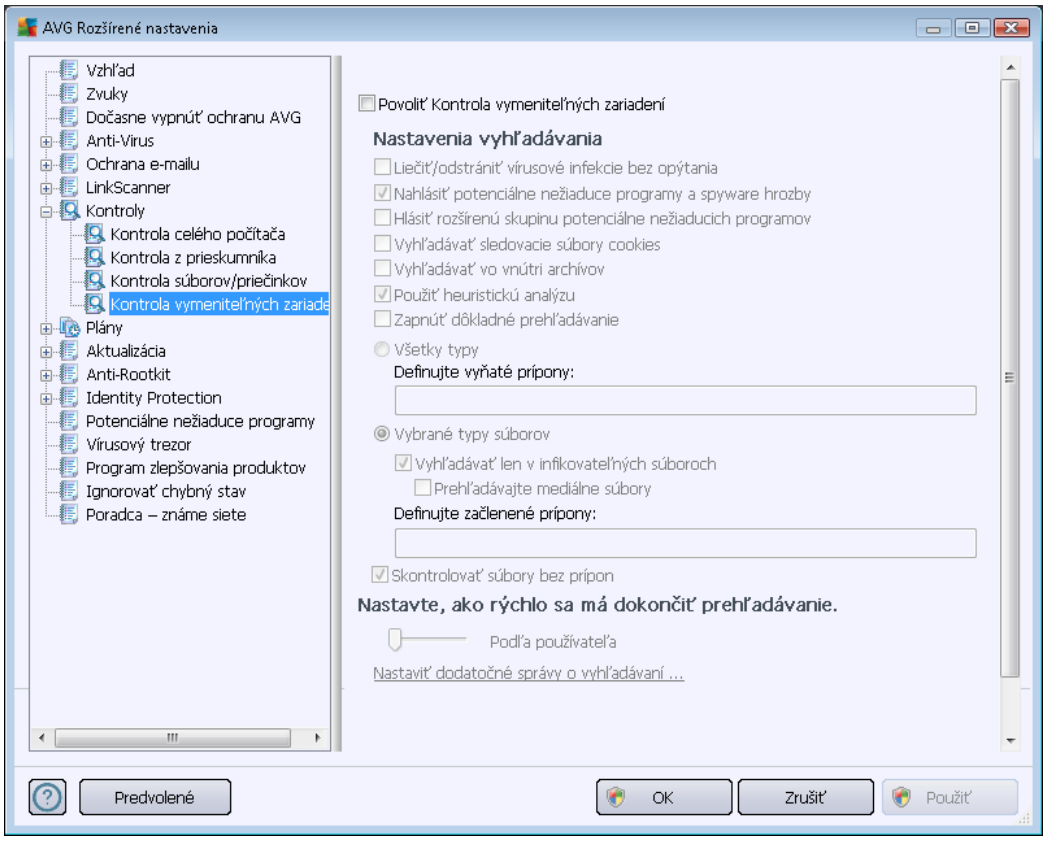


Všetky parametre nastavené v tomto dialógovom okne konfigurácie sa vzťahujú len na oblasti vybrané na prehľadávanie v dialógovom okne Prehľadávať konkrétne súbory alebo priečinky!

Poznámka: *Informácie o konkrétnych parametroch sa nachádzajú v kapitole Rozšírené nastavenia AVG/Prehľadávania/Prehľadávať celý počítač.*

10.7.4. Kontrola vymeniteľných zariadení

Rozhranie editácie ***prehľadávania vymeniteľný zariadení*** sa veľmi podobá dialógovému oknu editácie prehľadávania celého počítača:



Prehľadávanie vymeniteľných zariadení sa spustí automaticky po pripojení vymeniteľného zariadenia k počítaču. Toto prehľadávanie je štandardne vypnuté. Prehľadávanie vymeniteľných zariadení je však veľmi dôležité z hľadiska potenciálnych hrozieb, pretože tieto predstavujú zdroj infekcie. Ak chcete, aby bolo toto prehľadávanie pripravené a spustilo sa automaticky, keď je to potrebné, začiarknite možnosť ***Zapnúť prehľadávanie vymeniteľných zariadení***.

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

10.8. Plány

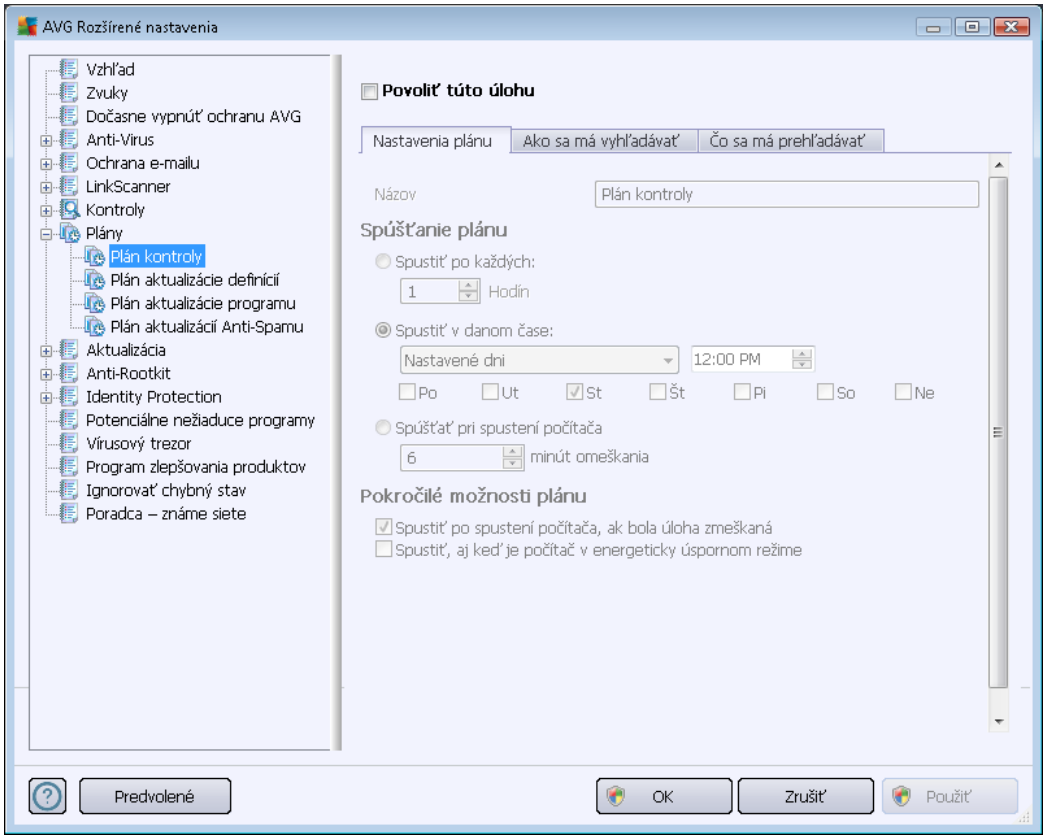
V časti ***Plány*** môžete upraviť predvolené nastavenia pre:

- Naplánované prehľadávanie
- Plán aktualizácie definícií
- Plán aktualizácie programu

- Plán aktualizácie súčasti Anti-Spam

10.8.1. Plánovaná kontrola

Parametre naplánovanej kontroly je možné editovať (*alebo nastaviť novú kontrolu*) na troch kartách. Na každej karte najskôr začiarknutím resp. zrušením začiarknutia položky ***Povoliť túto úlohu*** dočasne vypnite naplánovaný test a znova ho zapnite, keď je potrebný:



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

Príklad: *Nie je vhodné nazvať kontrolu „Nová kontrola“ alebo „Moja kontrola“, pretože tieto názvy nesúvisia s tým, čo kontrola vlastne kontroluje. 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 kontrolu vybraných súborov alebo priečinkov, pretože vaša vlastná kontrola bude vždy predstavovať špeciálnu verziu kontroly vybraných súborov alebo priečinkov.*

Toto dialógové umožňuje ďalej definovať tieto parametre kontroly:

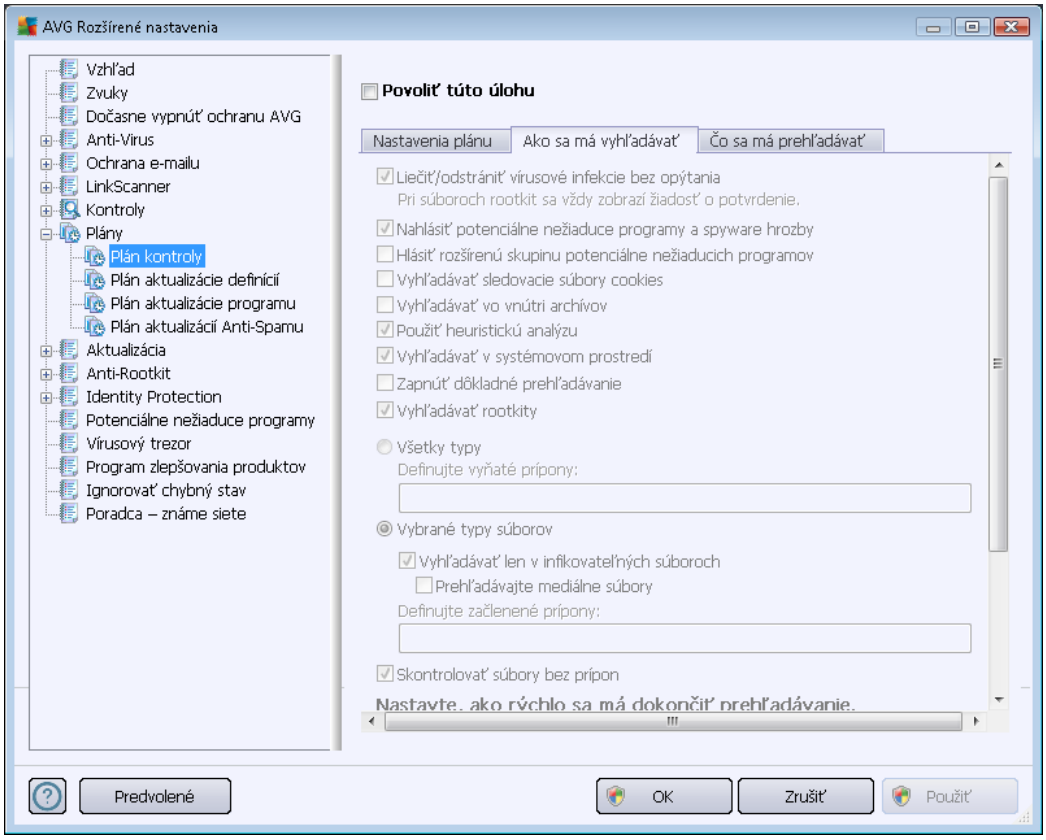
Spúšťanie naplánovaných úloh

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

Rozšírené možnosti plánu

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

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



Na karte ***Ako kontrolovať*** sa nachádza zoznam parametrov kontroly, ktoré sa dajú zapnúť resp. vypnúť. Štandardne je väčšina parametrov zapnutá a príslušná funkcia sa použije počas kontroly. ***Ak nemáte vážny dôvod meniť tieto nastavenia, potom vám odporúčame, aby ste zachovali preddefinovanú konfiguráciu***:

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

- ***Hlásiť potenciálne nežiaduce programy a hrozby spyware*** *(štandardne zapnuté):* začiarknite toto okienko, ak chcete zapnúť súčasť Anti-Spyware a kontrolovať spyware a vírusy. Spyware predstavuje pochybnú kategóriu škodlivého softvéru: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.

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

- ***Kontrolovať sledovacie súbory cookies*** (*štandardne vypnuté*): Tento parameter súčasti Anti-Spyware zapína funkciu na detekovanie súborov cookies počas kontroly; (*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 v archívoch*** (*štandardne vypnuté*): tento parameter určuje, že sa majú počas kontroly overovať všetky súbory, aj keď sú uložené vo vnútri archívu, napr. ZIP, RAR...

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

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

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

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

Ďalej rozhodnite, či chcete kontrolovať:

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

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

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

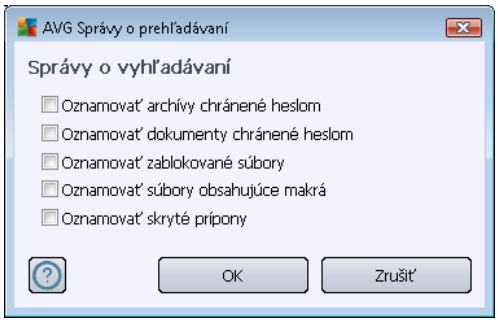
Nastaviť rýchlosť dokončenia kontroly

V časti ***Nastaviť rýchlosť dokončenia kontroly*** môžete ďalej nastaviť požadovanú rýchlosť kontroly v závislosti od využívania počítačových zdrojov. Štandardne má tento parameter nastavenú

úroveň automatického využívania zdrojov „*podľa používateľa*“. Ak chcete, aby kontrola prebiehala rýchlejšie, potom bude trvať kratšie, ale výrazne sa zvýši využívanie počítačových zdrojov a spomalia sa ostatné činnosti v počítači (*táto funkcia sa používa, keď je počítač zapnutý, ale nikto na ňom v danom momente nepracuje*). Na druhej strane môžete znížiť využívanie počítačových zdrojov predĺžením doby trvania kontroly.

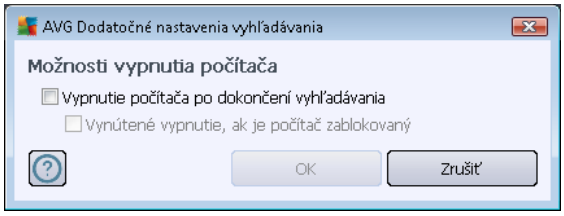
Vytvoriť ďalšie správy o kontrole

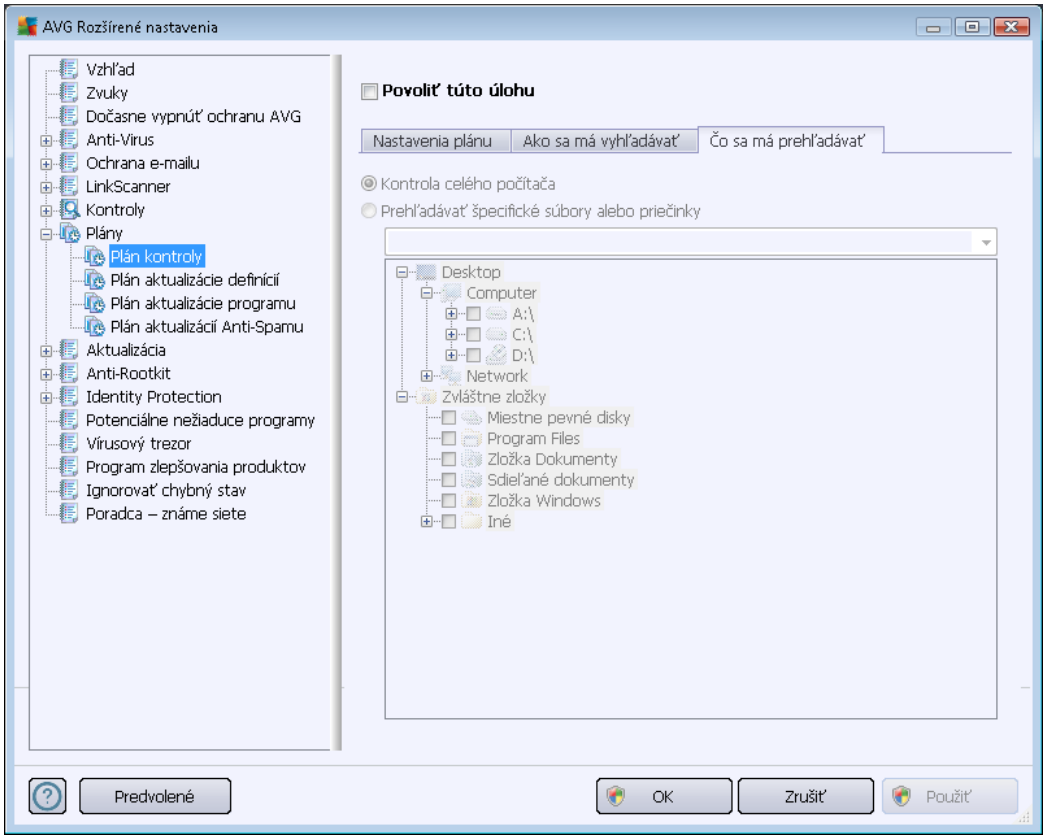
Kliknutím na odkaz ***Vytvoriť ďalšie správy o kontrole...*** otvorte samostatné dialógové okno s názvom ***Správy o kontrole***, v ktorom môžete začiarknutím konkrétnych položiek definovať, ktoré nálezy sa majú hlásiť:



Ďalšie nastavenia kontroly

Kliknutím na možnosť ***Ďalšie nastavenia kontroly...*** otvorte nové dialógové okno ***Možnosti vypnutia počítača***, ktoré vám umožní nastaviť, či sa má počítač automaticky vypnúť 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 počítača, keď je zamknutý***).

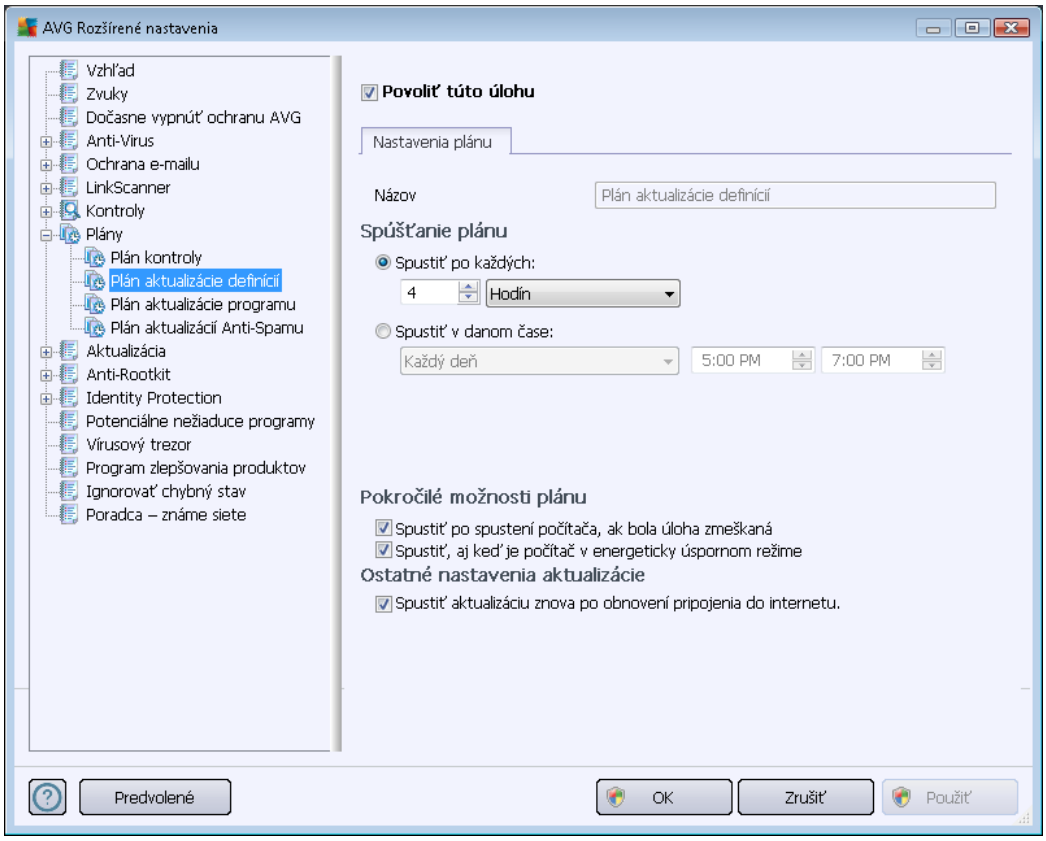




Karta ***Čo sa má prehľadávať*** umožňuje nastaviť, či chcete naplánovať prehľadávanie celého počítača alebo prehľadávanie konkrétnych súborov alebo priečinkov. V prípade, že zvolíte prehľadávanie špecifických súborov alebo priečinkov, v spodnej časti tohto dialógového okna sa aktivuje zobrazená stromová štruktúra a môžete uviesť priečinky, ktoré sa majú prehľadávať.

10.8.2. Plán aktualizácie definícií

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



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

Spúšťanie naplánovaných úloh

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

Rozšírené možnosti plánu

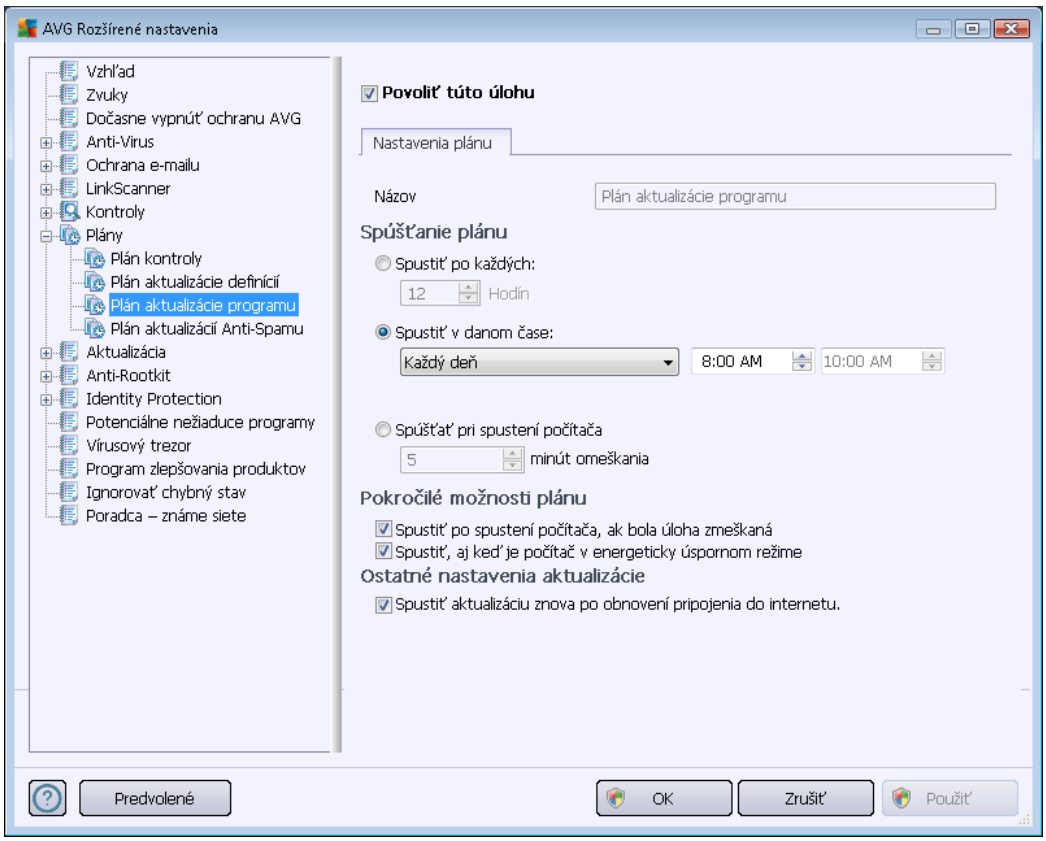
Táto časť sa používa na definovanie podmienok, v ktorých sa má/nemá spustiť aktualizácia definícií, keď je počítač v úspornom režime alebo úplne vypnutý.

Ďalšie nastavenia aktualizácie

Nakoniec označte možnosť ***Spustiť aktualizáciu znova hneď po obnovení internetového pripojenia***, ak sa má aktualizácia spustiť ihneď po obnovení po výpadku internetového pripojenia. Po spustení naplánovanej aktualizácie v nastavenom čase sa zobrazí informácia o tejto skutočnosti v automaticky otváranom okne nad ikonou AVG na paneli úloh (*pod podmienkou, že sa nezmenila predvolená konfigurácia v dialógom okne Rozšírené nastavenia/Vzhľad*).

10.8.3. Plán aktualizácie programu

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



V textovom poli s názvom ***Názov*** (*pole je neaktívne pre všetky predvolené plány*) sa nachádza názov, ktorý tomuto jedinečnému plánu pridelil výrobca programu.

Spúšťanie naplánovaných úloh

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

Rozšírené možnosti plánu

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

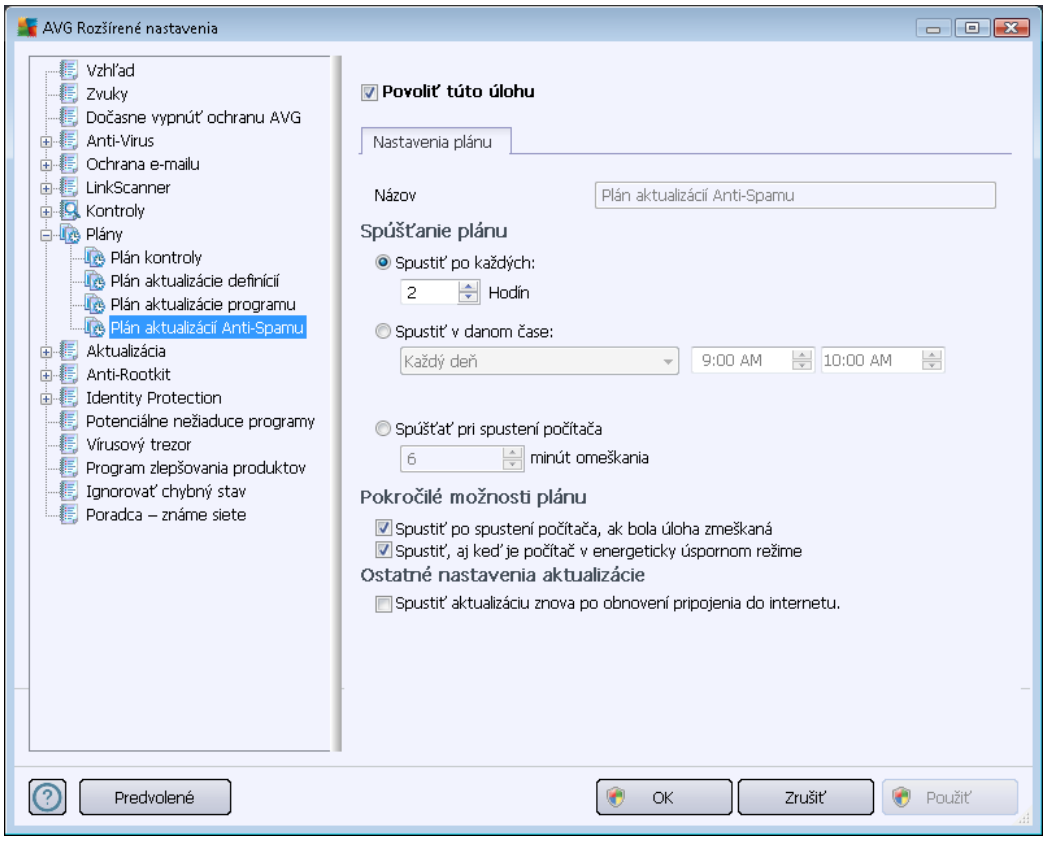
Ďalšie nastavenia aktualizácie

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

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

10.8.4. Plán aktualizácie súčasti Anti-Spam

Ak je to naozaj potrebné, zrušením začiarknutia možnosti ***Povoliť túto úlohu*** môžete dočasne vypnúť naplánovanú aktualizáciu súčasti Anti-Spam a neskôr ju znova zapnúť:



Toto dialógové okno sa používa na nastavenie niektorých podrobných parametrov plánu aktualizácie.

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

Spúšťanie naplánovaných úloh

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

Rozšírené možnosti plánu

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

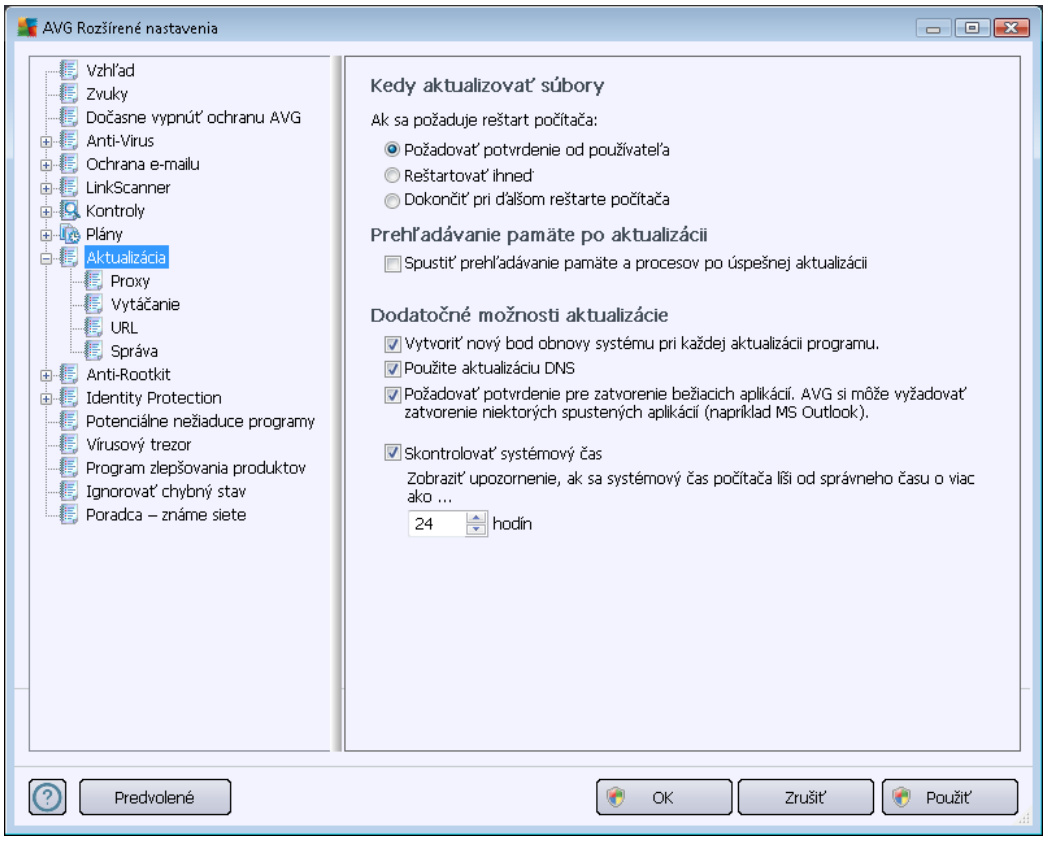
Ďalšie nastavenia aktualizácie

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

Po spustení naplánovanej kontroly v nastavenom čase sa zobrazí informácia v kontextovom okne nad ikonou AVG na paneli úloh (*pod podmienkou, že sa nezmenila predvolená konfigurácia v dialógom okne Rozšírené nastavenia/Vzhľad*).

10.9. Aktualizácia

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



Kedy aktualizovať súbory

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

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

Kontrola pamäte po aktualizácii

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

Ďalšie možnosti aktualizácie

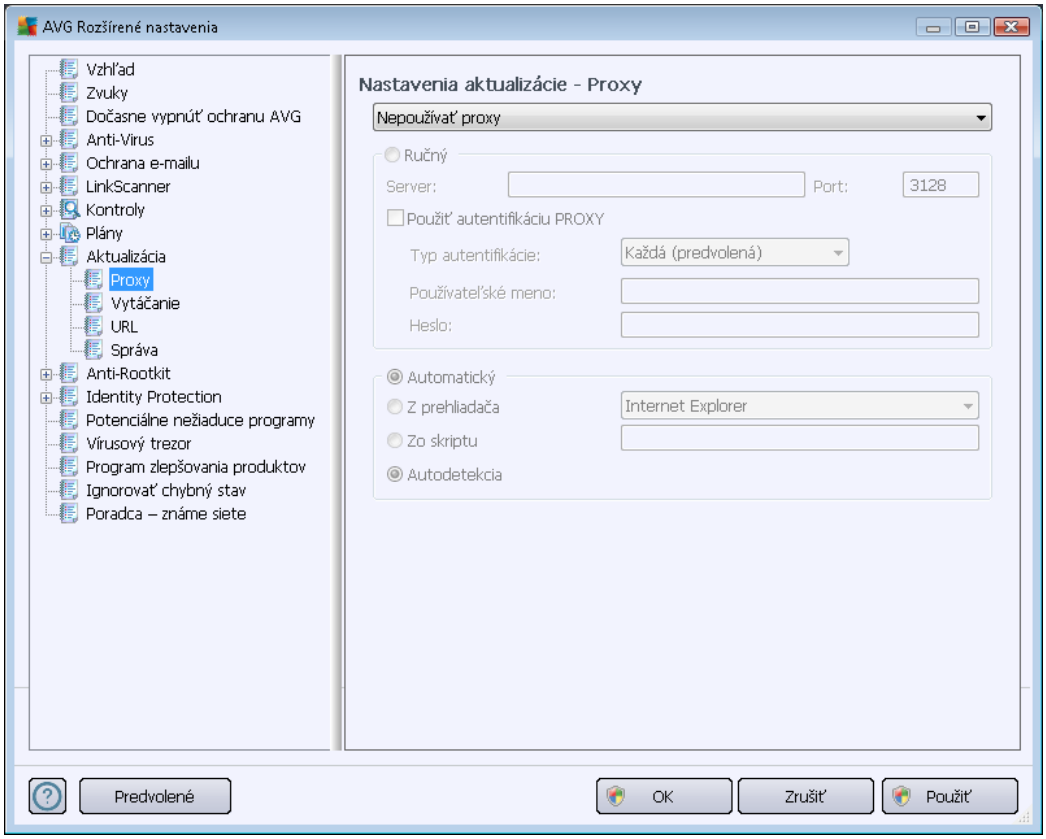
- ***Vytvoriť nový bod obnovenia systému počas každej aktualizácie programu*** – pred každým spustením aktualizácie programu AVG sa vytvorí bod obnovenia systému. Ak proces aktualizácie zlyhá a operačný systém spadne, potom vám tento bod obnovenia umožní obnoviť stav operačného systému s pôvodnou konfiguráciou. Táto funkcia sa otvára v ponuke Štart/Všetky programy/Príslušenstvo/Systémové nástroje/Obnovenie systému. Zmeny týchto nastavení však odporúčame robiť len skúseným používateľom! Nechajte toto začiarkovacie okienko začiarknuté, ak chcete používať túto funkcionalitu.

- ***Používať aktualizáciu DNS*** (*štandardne zapnuté*) – ak je toto začiarkovacie okienko označené, po spustení aktualizácie program **AVG Internet Security 2012** vyhľadá informácie o najnovšej verzii vírusovej databázy a najnovšej verzii programu na serveri DNS. Až potom sa prevezmú a nainštalujú najmenšie nevyhnutne potrebné aktualizačné súbory. Týmto spôsobom sa minimalizuje celkový objem prevzatých dát a zrýchli proces aktualizácie.

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

- ***Skontrolovať systémový čas*** – Toto políčko označte, ak chcete zobraziť oznámenie v prípade, že sa systémový čas líši od skutočného času o viac ako je nastavený počet hodín.

10.9.1. Proxy



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

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

Ak si zvolíte niektorú z možností používajúcich server proxy, budete musieť zadať ďalšie údaje. Nastavenia servera sa nastavujú buď ručne alebo automaticky.

Ručná konfigurácia

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

- ***Server***: Zadajte adresu IP servera alebo názov servera.

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

Server proxy môže mať tiež nastavené špeciálne pravidlá pre každého používateľa. Ak je server proxy nastavený týmto spôsobom, začiarknite možnosť ***Použiť autentifikáciu PROXY*** na overenie, či sú vaše používateľské meno a heslo platné na vytvorenie pripojenia na internet cez server proxy.

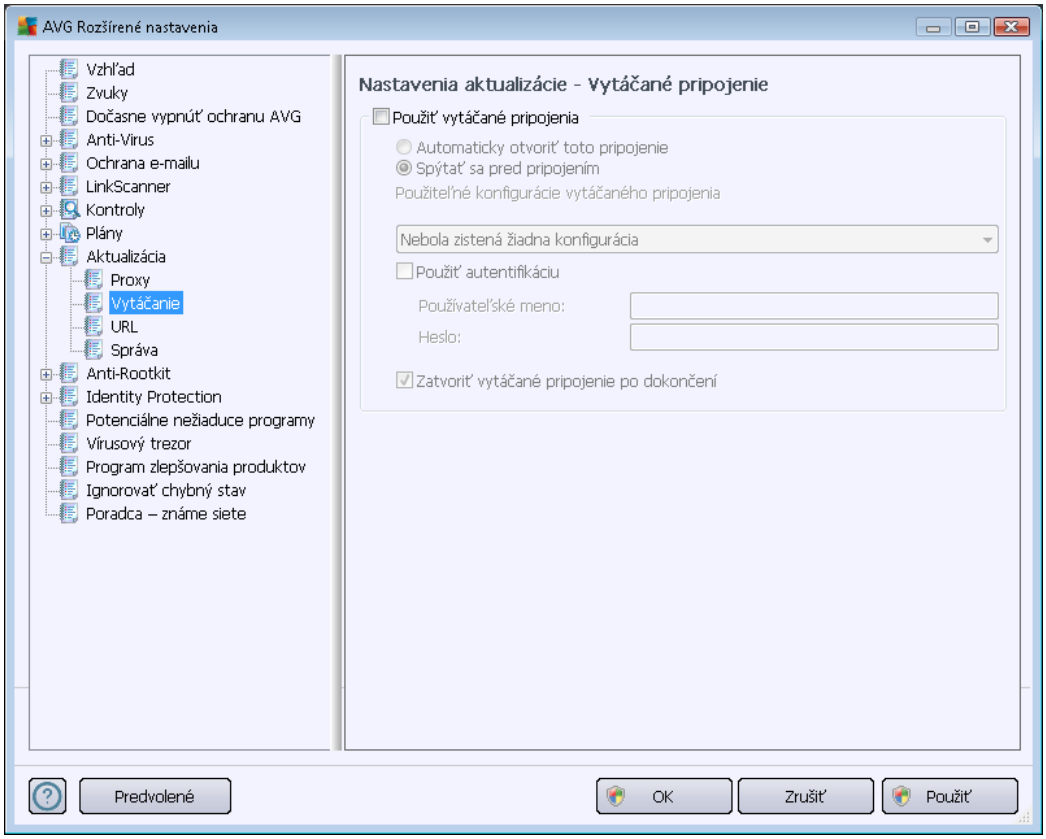
Automatická konfigurácia

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

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

10.9.2. Vytáčané pripojenie

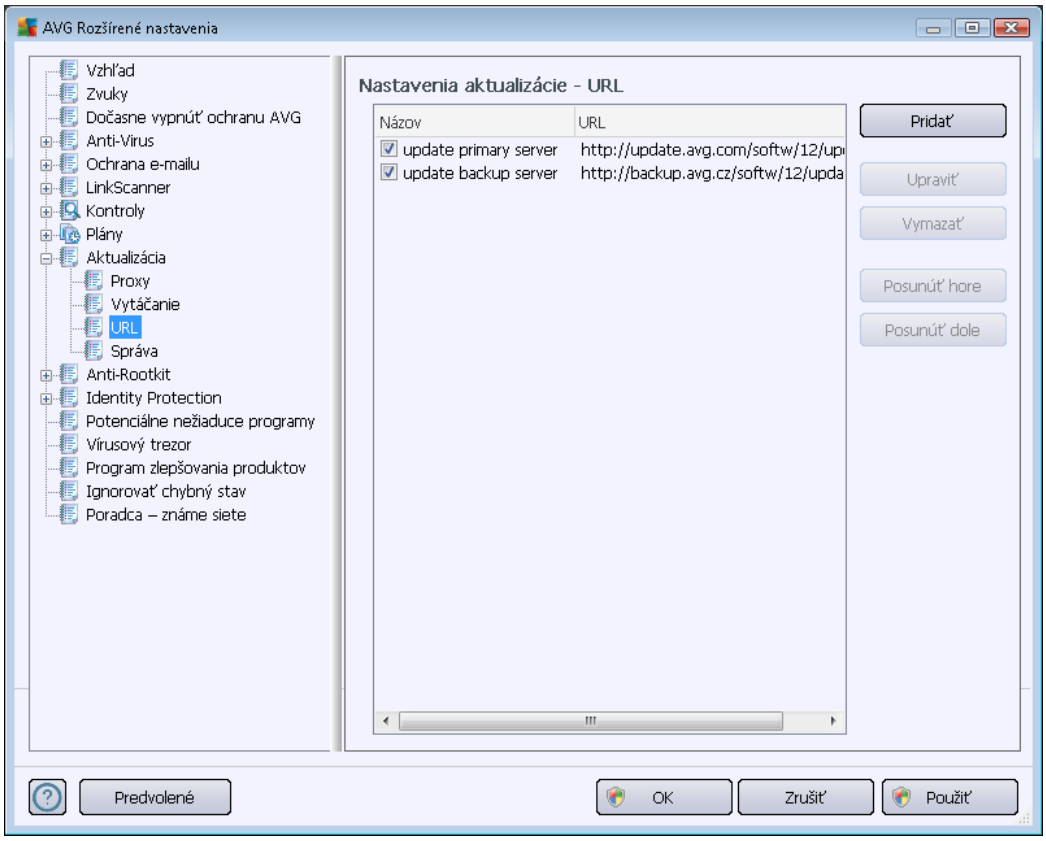
Všetky parametre voliteľne zadefinované v dialógovom okne ***Nastavenia aktualizácie – Vytáčané pripojenie*** sa vzťahujú na vytáčané pripojenie k Internetu. Polia v tomto dialógovom okne nebudú aktívne, kým neoznačíte možnosť ***Použiť vytáčané pripojenia***, potom sa polia aktivujú:



Zadajte, či sa chcete pripojiť k Internetu automaticky (***Automaticky otvoriť toto pripojenie***) alebo chcete každý krát potvrdiť toto pripojenie ručne (***Spýtať sa pred pripojením***). Pri automatickom pripojení by ste mali ďalej zvoliť, či sa má pripojenie zatvoriť po skončení aktualizácie (***Zatvoriť vytáčané pripojenie po dokončení***).

10.9.3. Adresa URL

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



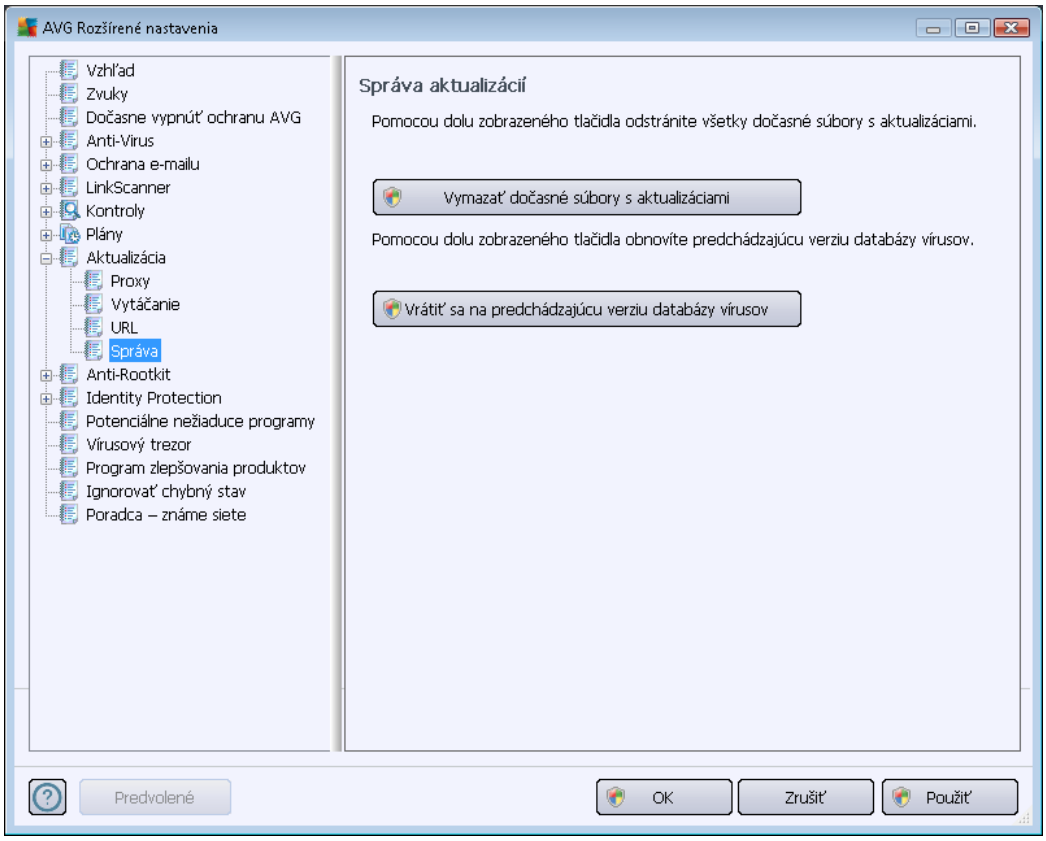
Ovládacie tlačidlá

Zoznam a jeho položky môžete zmeniť pomocou nasledujúcich ovládacích tlačidiel:

- ***Pridať*** – otvorí sa dialógové okno, kde môžete zadať novú URL adresu, ktorú chcete pridať do zoznamu
- ***Upraviť*** – otvorí sa dialógové okno, kde môžete upraviť parametre zvolenej URL adresy
- ***Vymazať*** – vymaže sa zvolená URL adresa zo zoznamu
- ***Posunúť hore*** – posunie zvolenú URL adresu o jednu pozíciu v zozname hore
- ***Posunúť dole*** – posunie zvolenú URL adresu o jednu pozíciu v zozname dole

10.9.4. Správa

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

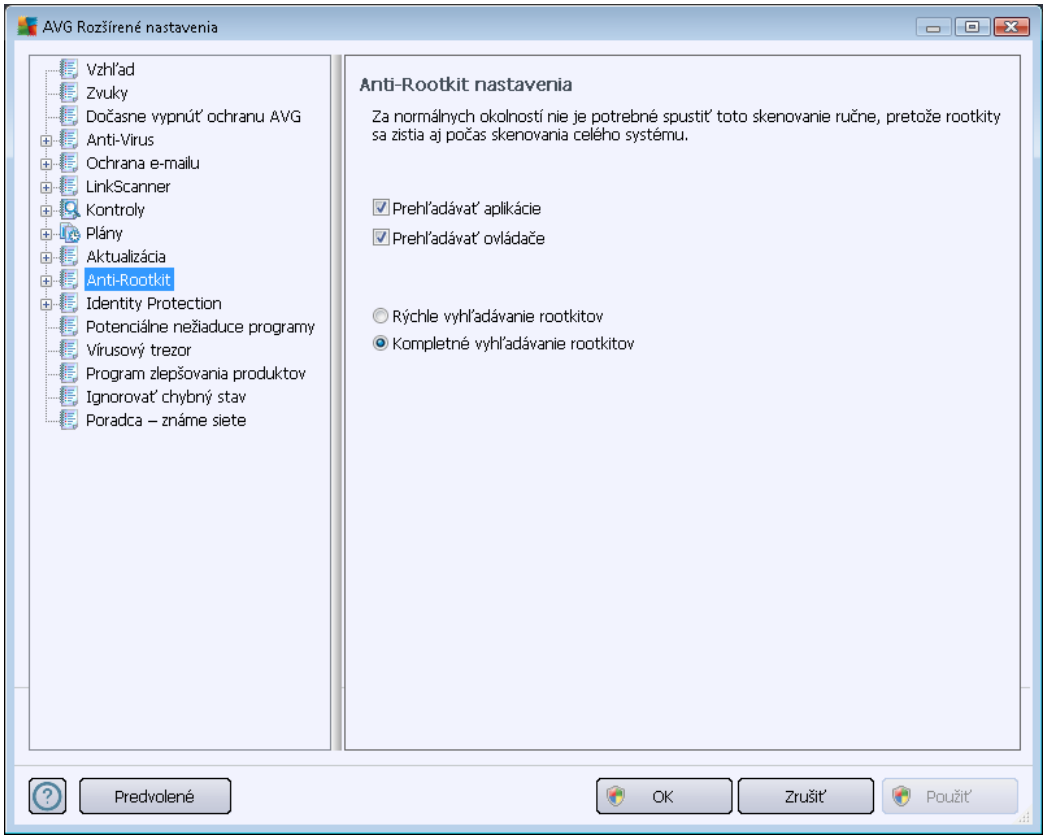


- ***Vymazať dočasné súbory aktualizácie***: Stlačením tohto tlačidla sa vymažú všetky redundantné súbory aktualizácie z pevného disku (*štandardne, tieto súbory zostanú uložené 30 dní*)

- ***Obnoviť 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*).

10.10. Anti-Rootkit

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



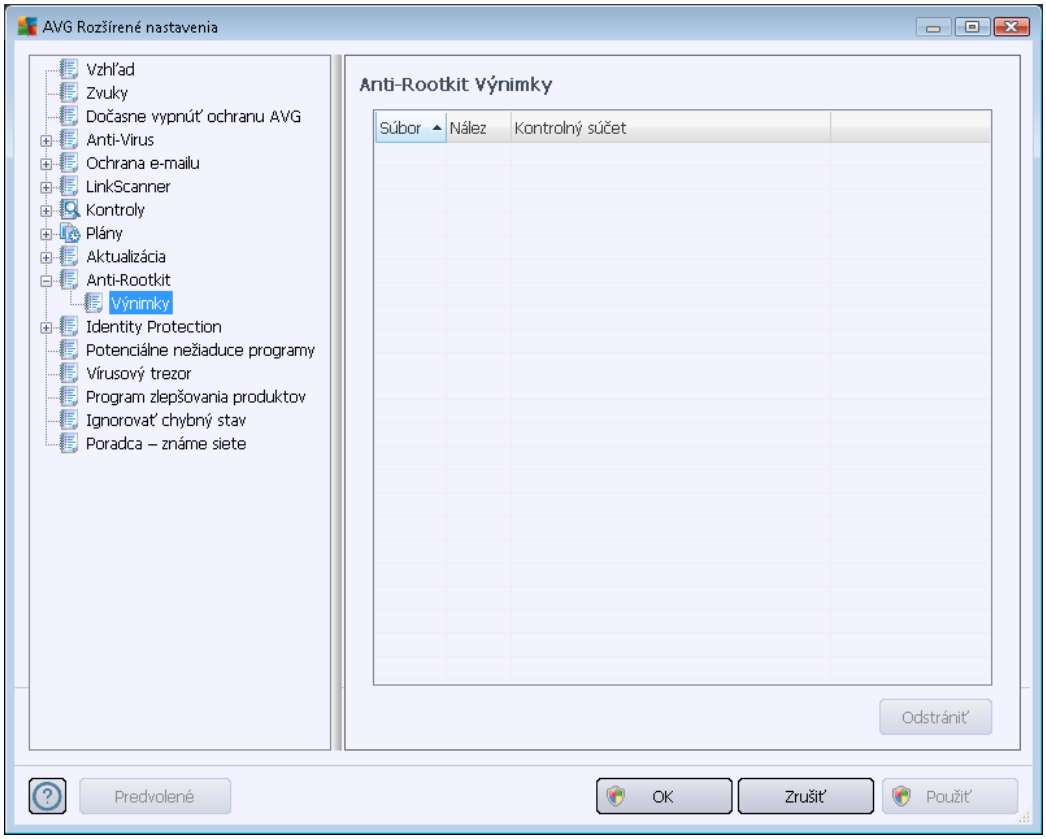
Úprava všetkých funkcií súčasti Anti-Rootkit, ktorú umožňuje toto dialógové okno, je možná aj priamo v rozhraní súčasti Anti-Rootkit.

Možnosti ***Kontrolovať aplikácie*** a ***Kontrolovať ovládače*** vám umožňujú podrobne zadať, čo by malo byť súčasťou kontroly Anti-Rootkit. Tieto nastavenia sú určené pre pokročilých používateľov; odporúčame ponechať všetky možnosti zapnuté. Ďalej môžete vybrať režim kontroly rootkitov:

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

10.10.1. Výnimky

V dialógovom okne ***Výnimky komponentu Anti-Rootkit*** môžete definovať konkrétne súbory *(napríklad niektoré ovládače, ktoré boli nesprávne zistené ako rootkit)*, ktoré by sa mali vyňať z kontroly:

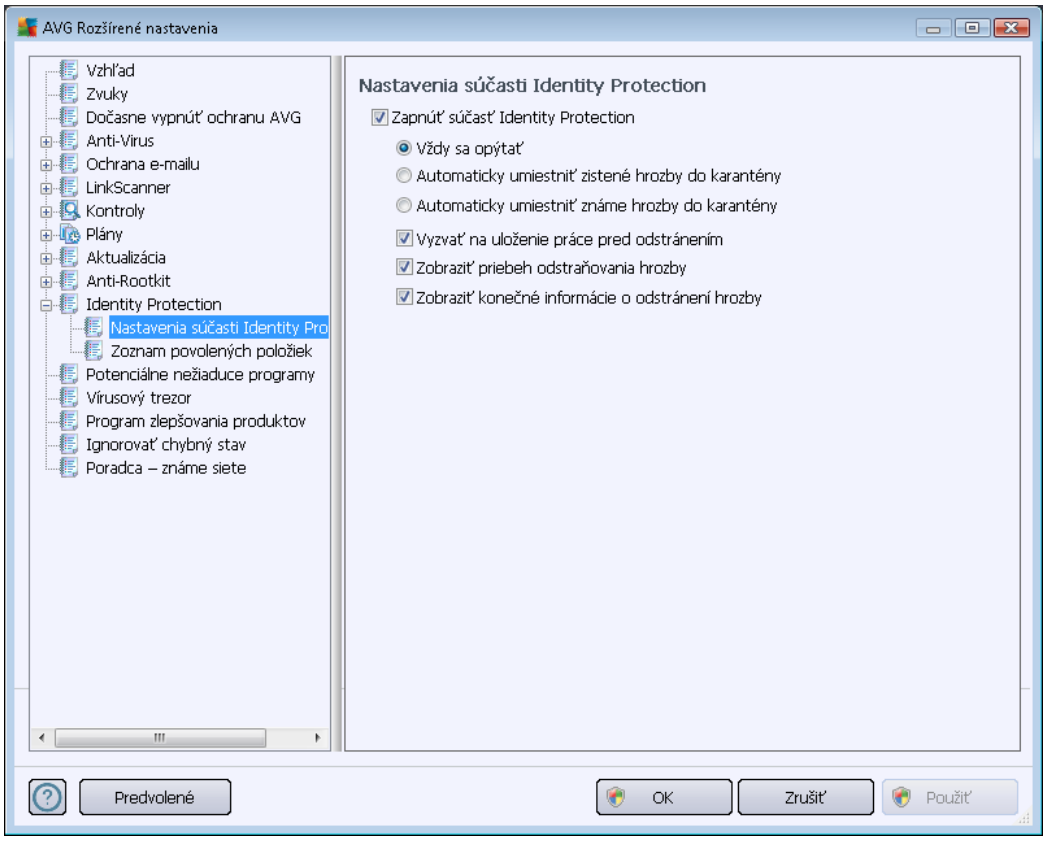


10.11. Identity Protection

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

10.11.1. Nastavenia súčasti Identity Protection

Dialógové okno ***Nastavenia súčasti Identity Protection*** sa používa na zapnutie a vypnutie dvoch základných funkcií súčasti Identity Protection:



Súčasť Identity Protection je zapnutá (*štandardne zapnuté*) – zrušením začiarknutia sa vypne súčasť Identity Protection.

Odporúčame vám, aby ste to urobili len v prípade, keď je to naozaj nevyhnutné!

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

- ***Vždy sa opýtať*** (*štandardne zapnuté*) – pri detekovaní hrozby sa vás program opýta, či sa má hrozba premiestniť do karantény, aby nedošlo k neželanému odstráneniu aplikácií, ktoré chcete používať.
- ***Automaticky umiestniť zistené hrozby do karantény*** – začiarknite toto začiarkovacie okienko, ak sa majú všetky potenciálne detekované hrozby ihneď premiestniť na bezpečné miest vo Vírusovom trezore. Keď zachováte predvolené nastavenia, potom sa vás program opýta pri detekovaní hrozby, či sa má táto hrozba premiestniť do karantény, aby nedošlo k odstráneniu aplikácií, ktoré chcete používať.
- ***Automaticky umiestniť známe hrozby do karantény*** – nechajte toto začiarkovacie okienko začiarknuté, ak sa majú všetky aplikácie detekované ako potenciálne škodlivé automaticky a ihneď premiestniť do Vírusového trezora.

Ďalej môžete nastaviť konkrétne položky a zapnúť ďalšie funkcie súčasti Identity Protection:

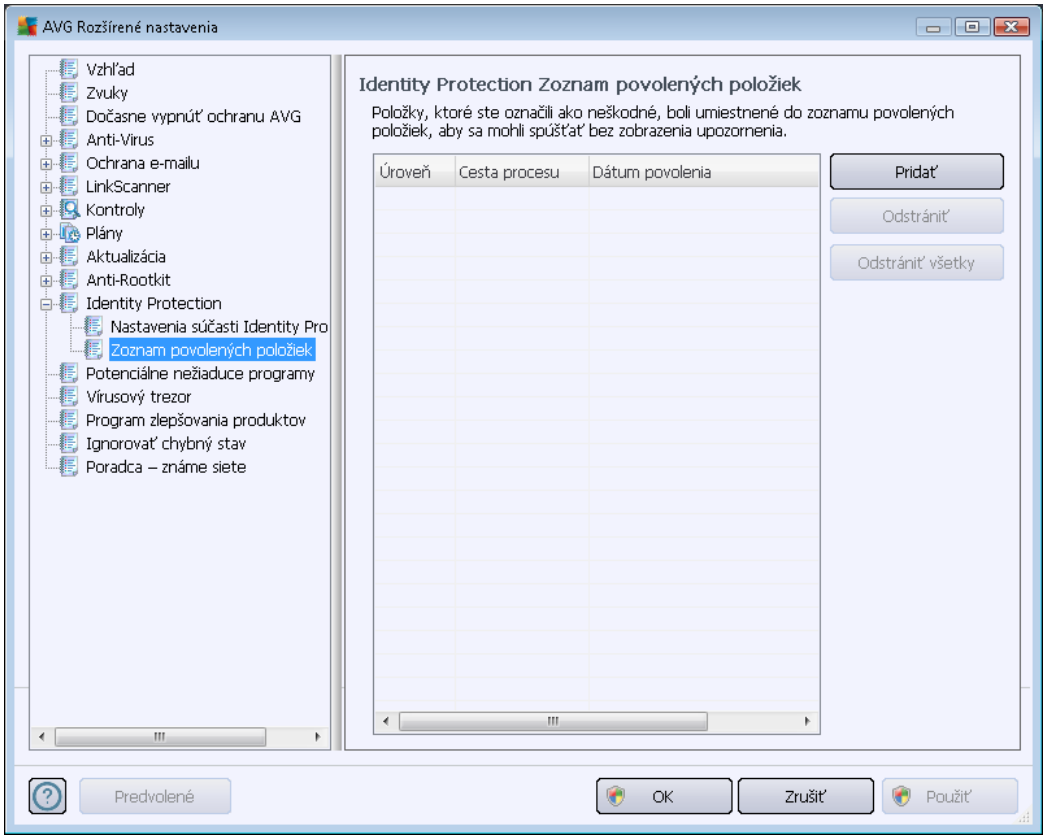
- ***Vyzvať na uloženie práce pred odstránením*** (*štandardne zapnuté*) – nechajte toto začiarkovacie okienko začiarknuté, ak chcete, aby sa pred premiestnením aplikácie detekovanej ako potenciálne škodlivá do karantény zobrazilo upozornenie. Ak práve pracujete s aplikáciou, projekt by sa mohol stratiť, a preto by ste ho mali najskôr uložiť. Táto možnosť je štandardne zapnutá a odporúčame vám, aby ste toto nastavenie nemenili.

- ***Zobraziť priebeh odstraňovania hrozieb*** - (*štandardne zapnuté*) – keď je táto funkcia zapnutá, potom sa po detekovaní potenciálneho škodlivého softvéru otvorí nové dialógové okno s priebehom premiestňovania škodlivého softvéru do karantény.

- ***Zobraziť konečné informácie o odstránení hrozieb*** - (*štandardne zapnuté*) – keď je táto funkcia zapnutá, potom súčasť ***Identity Protection*** zobrazí podrobné informácie o každom objekte premiestnenom do karantény (*úroveň závažnosti, umiestnenie atď.*).

10.11.2. Zoznam povolených

Keď máte otvorené dialógové okno ***Nastavenia súčasti Identity Protection*** a rozhodnete sa nechať položku ***Automaticky umiestniť detekované hrozby do karantény*** nezačiarknutú, potom sa vás pri každom detekovaní potenciálneho škodlivého softvéru program opýta, či ho chcete odstrániť. Ak potom označíte túto podozrivú aplikáciu (*rozpoznanú na základe jej správania*) za bezpečnú a potvrdíte, že sa má ponechať v počítači, aplikácia sa pridá do tzv. ***zoznamu povolených v súčasti Identity Protection*** a program ju už nebude označovať za potenciálne nebezpečnú:



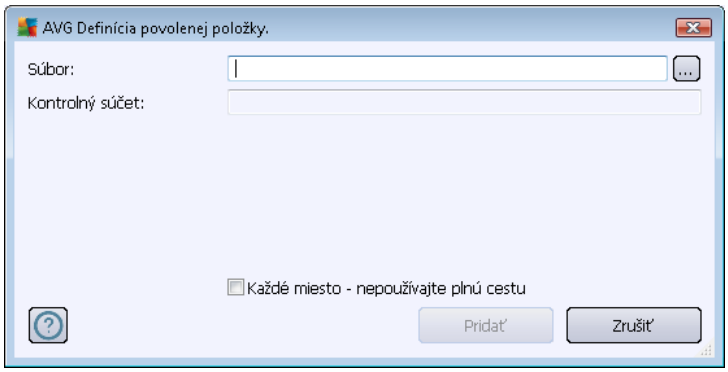
V ***zozname povolených v Identity Protection*** sa nachádzajú tieto informácie o každej aplikácii:

- ***Úroveň*** – grafické označenie závažnosti príslušného procesu na stupnici so štyrmi úrovňami od najmenej významnej (■□□□) až po kritickú (■■■■).
- ***Cesta procesu*** – cesta k umiestneniu spustiteľného súboru aplikácie (*procesu*).
- ***Dátum povolenia*** – dátum, keby bola aplikácia ručne označená za bezpečnú.

Ovládacie tlačidlá

V dialógovom okne ***Zoznam povolených v Identity Protection*** sa nachádzajú tieto ovládacie tlačidlá:

- ***Pridať*** – stlačením tohto tlačidla sa nová aplikácia pridá do zoznamu povolených. Otvorí sa toto prekrývacie okno:



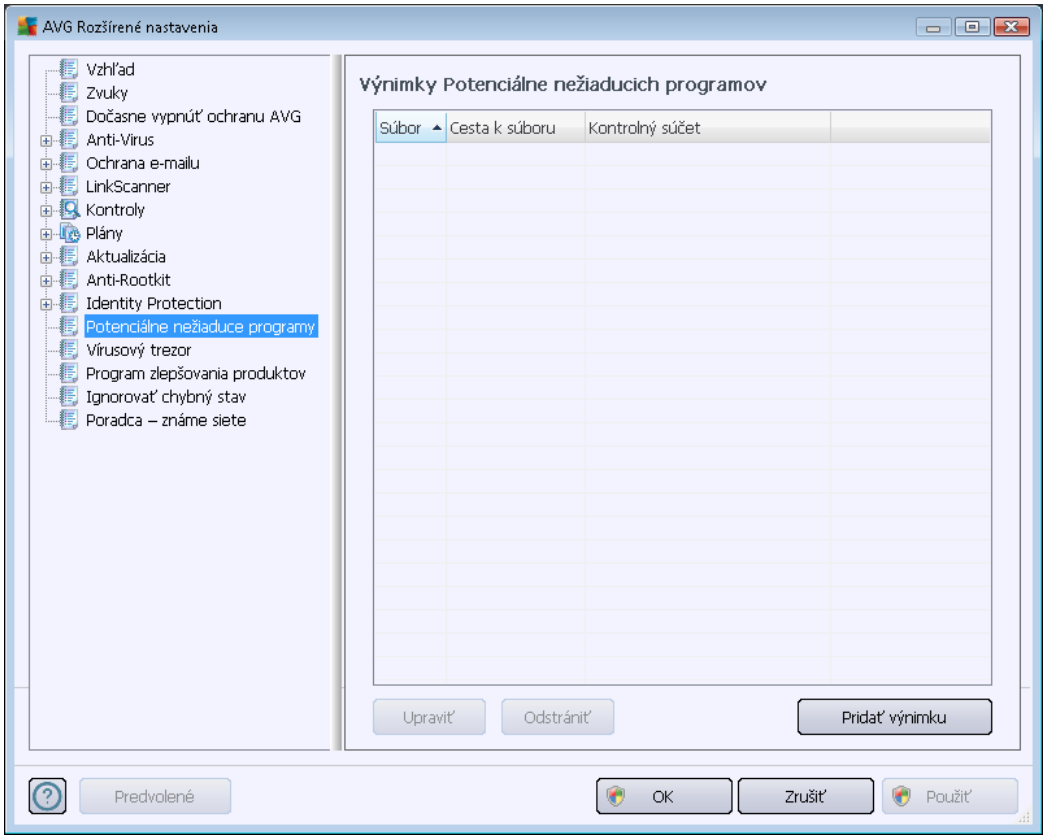
  - ***Súbor*** – zadajte úplnú cestu k súboru (*aplikácii*), ktorý chcete označiť ako výnimku.
  - ***Kontrolný súčet*** – uvádza jedinečnú „signatúru“ vybraného súboru. Tento kontrolný súčet je automaticky generovaný reťazec znakov, ktorý umožňuje programu AVG jasne odlíšiť vybraný súbor od ostatných súborov. Kontrolný súčet sa vygeneruje a zobrazí po úspešnom pridaní súboru.
  - ***Každé umiestnenie – nepoužívať úplnú cestu*** – ak chcete definovať tento súbor ako výnimku len pre konkrétne umiestnenie, nechajte toto okienko nezačiarknuté.

- ***Odstrániť*** – stlačením tohto tlačidla sa vybraná aplikácia odstráni zo zoznamu.
- ***Odstrániť všetky*** – stlačením tohto tlačidla sa odstránia všetky uvedené aplikácie.

10.12. Potenciálne nežiaduce programy

Program **AVG Internet Security 2012** dokáže analyzovať a zistiť spustiteľné aplikácie a knižnice DLL, ktoré by mohli predstavovať potenciálne nežiaduce položky v systéme. V niektorých prípadoch môže používateľ chcieť, aby niektoré nežiaduce programy zostali v počítači (programy, ktoré boli nainštalované zámerne). Programy, najmä bezplatné programy, obsahujú

adware. Takýto adware môže aplikácia **AVG Internet Security 2012** vyhodnotiť ako *potenciálne nežiaduci program*. Ak chcete ponechať tento program v počítači, nastavte ho ako výnimku z potenciálne nežiaducich programov:



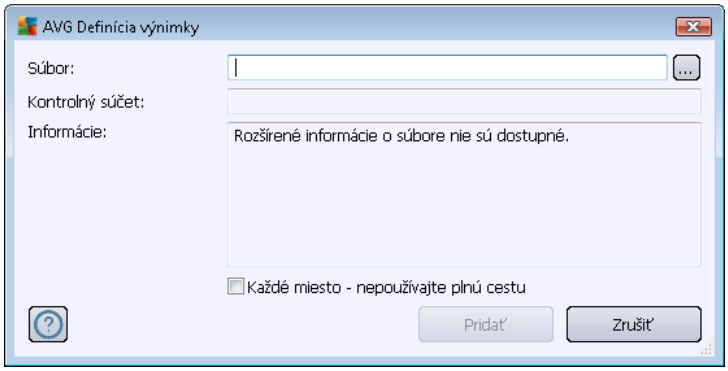
V dialógovom okne ***Výnimky z potenciálne nežiaducich programov*** sa nachádza zoznam už definovaných a momentálne platných výnimiek z potenciálne nežiaducich programov. Môžete editovať zoznam, vymazať existujúce položky, alebo pridať nové výnimky. V zozname sa nachádzajú tieto informácie o každej jednej výnimke:

- ***Súbor*** – Uvádza presný názov príslušnej aplikácie.
- ***Cesta k súboru*** – uvádza cestu k umiestneniu aplikácie.
- ***Kontrolný súčet*** – uvádza jedinečnú „signatúru“ vybraného súboru. Tento kontrolný súčet je automaticky generovaný reťazec znakov, ktorý umožňuje programu AVG jasne odlíšiť vybraný súbor od ostatných súborov. Kontrolný súčet sa vygeneruje a zobrazí po úspešnom pridaní súboru.

Ovládacie tlačidlá

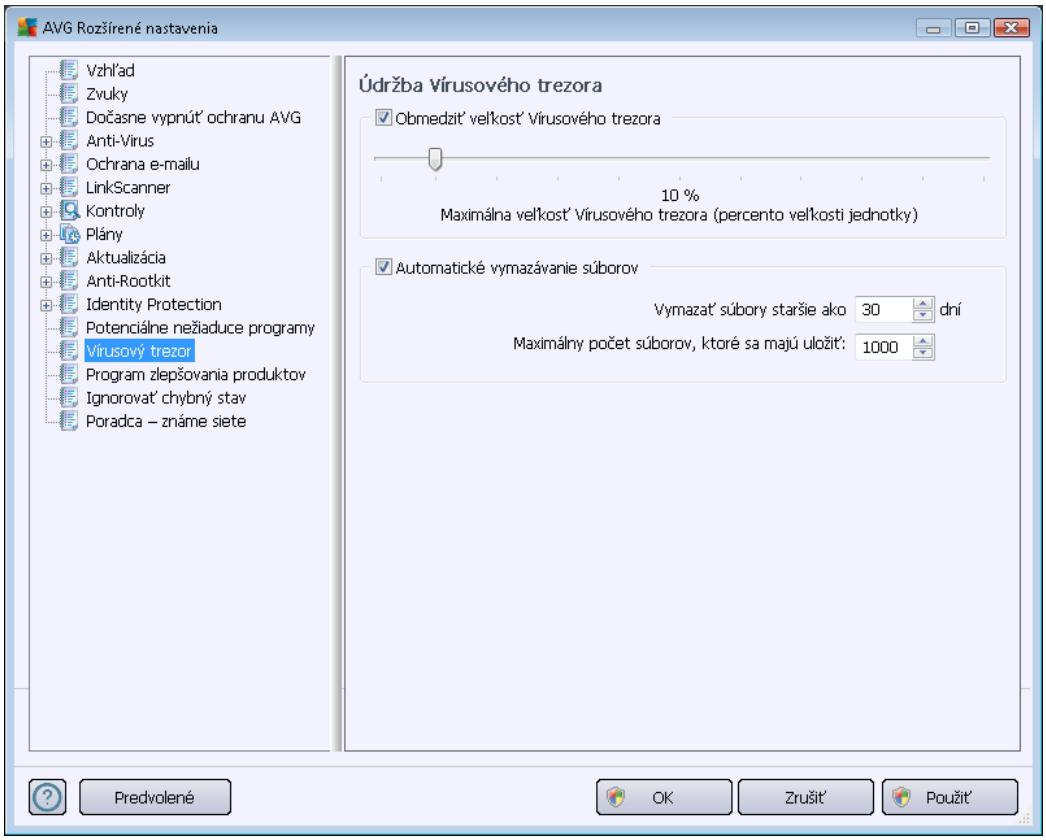
- ***Editovať*** – otvorí dialógové okno editovania (*je rovnaké ako dialógové okno definovania novej výnimky, pozri ďalej v texte*) už definovanej výnimky, v ktorom môžete zmeniť parametre výnimky.

- ***Odstrániť*** – vymaže vybranú položku zo zoznamu výnimiek.
- ***Pridať výnimku*** – otvorí dialógové okno editovania, ktoré umožňuje definovať parametre novej výnimky, ktorá sa má vytvoriť:



  - ***Súbor*** – zadajte úplnú cestu k súboru, ktorý chcete označiť ako výnimku.
  - ***Kontrolný súčet*** – zobrazí jedinečnú „signatúru“ vybraného súboru. Tento kontrolný súčet je automaticky generovaný reťazec znakov, ktorý umožňuje programu AVG jasne odlíšiť vybraný súbor od ostatných súborov. Kontrolný súčet sa vygeneruje a zobrazí po úspešnom pridaní súboru.
  - ***Informácie o súbore*** – Zobrazí všetky dostupné doplňujúce informácie o súbore *(informácie o licencii, verzii atď.)*
  - ***Každé miesto – nepoužívajte úplnú cestu*** – ak chcete definovať tento súbor ako výnimku len pre špecifické umiestnenie, nechajte toto políčko nezačiarknuté. Keď je toto začiarkavacie políčko začiarknuté, príslušný súbor je definovaný ako výnimka bez ohľadu na umiestnenie *(napriek tomu však musíte uviesť úplnú cestu k príslušnému súboru; súbor sa potom použije ako jedinečný príklad situácie, keď sa v počítači vyskytujú dva súbory s rovnakým názvom)*.

10.13. Vírusový trezor



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

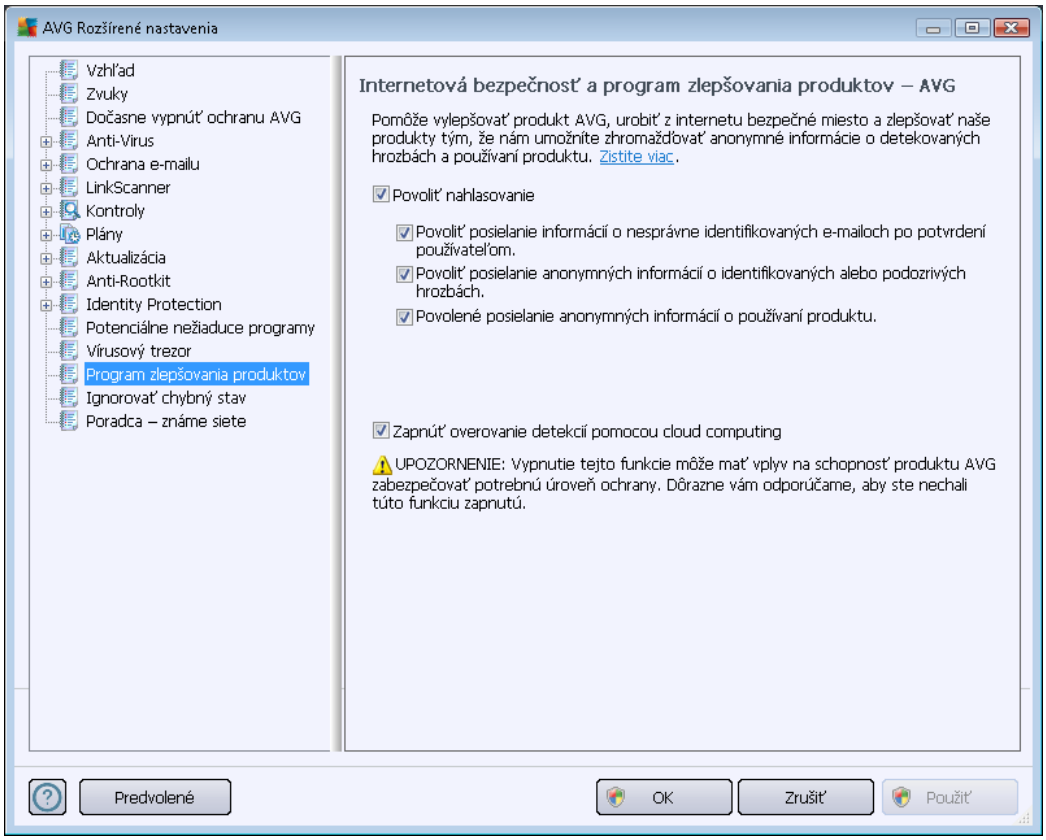
- ***Obmedziť veľkosť vírusového trezora*** – Použite posúvač na nastavenie maximálnej veľkosti vírusového trezora. Táto veľkosť sa uvádza úmerne k veľkosti lokálneho disku.
- ***Automatické odstraňovanie súborov*** – V tejto časti môžete stanoviť maximálny čas, kedy by objekty mali byť uložené vo vírusovom trezore (***Odstrániť súbory staršie ako ... dní***) a maximálny počet súborov, ktoré budú uložené vo vírusovom trezore (***Maximálny počet uložených súborov***).

10.14. Program zlepšovania produktov

Dialógové okno ***Internetová bezpečnosť a program zlepšovania produktov AVG*** vás pozýva, aby ste sa zúčastnili programu zlepšovania produktov AVG a pomohli nám zvýšiť celkovú úroveň zabezpečenia internetu. Nechajte možnosť ***Povoliť hlásenie*** označenú, aby bolo možné hlásiť zistené hrozby do laboratórií spoločnosti AVG. Táto funkcia nám pomáha zhromažďovať aktuálne informácie o najnovších hrozbách od účastníkov z celého sveta a umožňuje zlepšovať ochranu pre každého.

Hlásenie sa uskutoční automaticky a žiadnym spôsobom vás neobťažuje. 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:

- ***Povoliť oznamovanie*** *(štandardne zapnuté)* - Ak nám chcete pomôcť ďalej sa zlepšovať **AVG Internet Security 2012**, nechajte toto políčko označené. Táto funkcia zapne oznamovanie všetkých zaznamenaných hrozieb do spoločnosti AVG a umožní nám zhromažďovať najnovšie informácie o hrozbách od všetkých účastníkov z celého sveta a zlepšovať ochranu pre každého jednotlivca. Oznamovanie prebieha automaticky, preto vás nijako nezaťažuje a v správach nie sú uvedené žiadne osobné údaje.
    - ***Povoliť posielanie informácií o nesprávne identifikovaných e-mailoch po potvrdení používateľom*** *(štandardne zapnuté)* – posielať informácie o e-mailových správach, ktoré boli nesprávne označené ako spam, alebo spamových správach, ktoré súčasť Anti-Spam nedetegovala. Pred poslaním tohto druhu informácií vás program požiada o potvrdenie.
    - ***Povoliť posielanie anonymných informácií o identifikovaných alebo podozrivých hrozbách*** *(štandardne zapnuté)* – posielať informácie o podozrivom alebo pozitívne nebezpečnom kóde alebo priebehu správania *(môže ísť o vírus, spyware alebo škodlivé internetové stránky, ktoré sa pokúšate otvoriť)* detegovanom na počítači.

- ***Umožnite zasielať nám anonymné údaje o používaní produktu*** *(štandardne zapnuté)* – odosielanie základných štatistík o používaní aplikácie, ako je počet nájdených hrozieb, spustených kontrol, úspešné či neúspešné kontroly a pod.

- ***Zapnúť overovanie detekcií pomocou cloud computingu*** *(štandardne zapnuté)* – detegované hrozby sa budú overovať, či sú naozaj infikované, aby sa vylúčili nesprávne detekcie.

Najbežnejšie hrozby

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

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

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

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

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

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

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

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

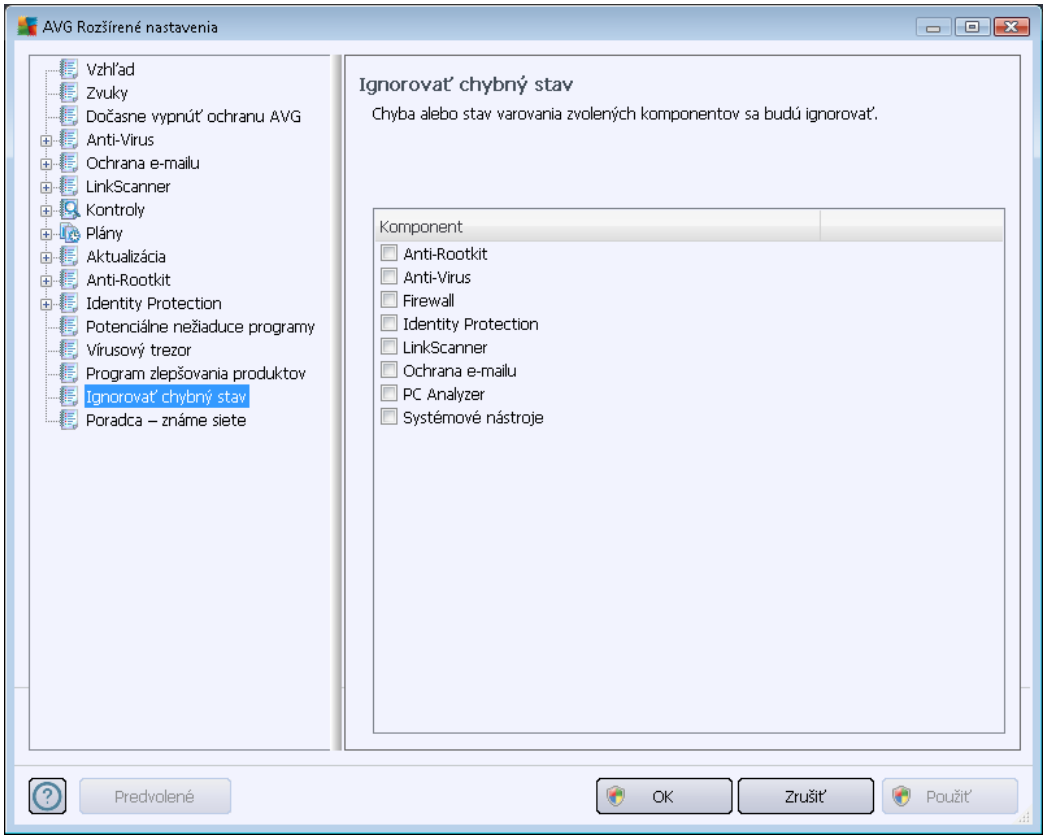
- ***Hoax*** je hromadný e-mail, ktorý obsahuje nebezpečné, alarmujúce alebo jednoducho len otravné a neužitočné informácie. Na šírenie väčšiny vyššie uvedených hrozieb sa používajú podvodné e-mailové správy typu hoax.

- ***Škodlivé internetové stránky*** sú napokon tie, ktoré úmyselne inštalujú škodlivý softvér do počítača a haknuté stránky robia to isté, ibaže ide o legitímne internetové stránky, ktoré boli zneužité na infikovanie počítača návštevníkov.

V záujme ochrany pred všetkými druhmi hrozieb produkt AVG Internet Security 2012 obsahuje špecializované komponenty. Ich stručný opis nájdete v kapitole Prehľad súčastí.

10.15. Ignorovať chybový stav

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



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

- Ikony na paneli úloh – keď všetky časti aplikácie AVG fungujú správne, potom má ikona štyri farby; keď sa však vyskytne chyba, ikona bude mať žltý výkričník.

- Textového opisu existujúceho problému v časti Informácie o stave zabezpečenia v hlavnom okne programu AVG.

Môže sa vyskytnúť situácia, keď bude potrebné z nejakého dôvodu súčasť dočasne vypnúť (*neodporúčame vám však, aby ste to robili; podľa možností nechajte všetky súčasti stále zapnuté a nemeňte predvolenú konfiguráciu*). V tom prípade ikona na 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 vo vyššie uvedenom dialógovom okne vybrať súčasti, o ktorých prípadnom chybovom stav (*alebo vypnutí*) si neželáte byť informovaný. Tá istá možnosť *(Ignorovať stav súčasti)* je dostupná aj pri špecifických komponentoch priamo v prehľade súčastí v hlavnom okne AVG.

10.16. Aplikácia Advisor – známe siete

AplikáciaAVG 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 sa k novej sieti môžete bezpečne pripojiť, môžete názov siete uložiť do zoznamu. Aplikácia AVG Advisor *si následne zapamätá parametre danej siete (konkrétne adresu MAC)* a upozornenie nabudúce nezobrazí.

V tomto dialógovom okne môžete skontrolovať, ktoré siete ste už uložili ako známe. Jednotlivé záznamy môžete vymazať stlačením tlačidla ***Odstrániť***; daná sieť bude následne opäť považovaná za neznámu a potenciálne nebezpečnú.

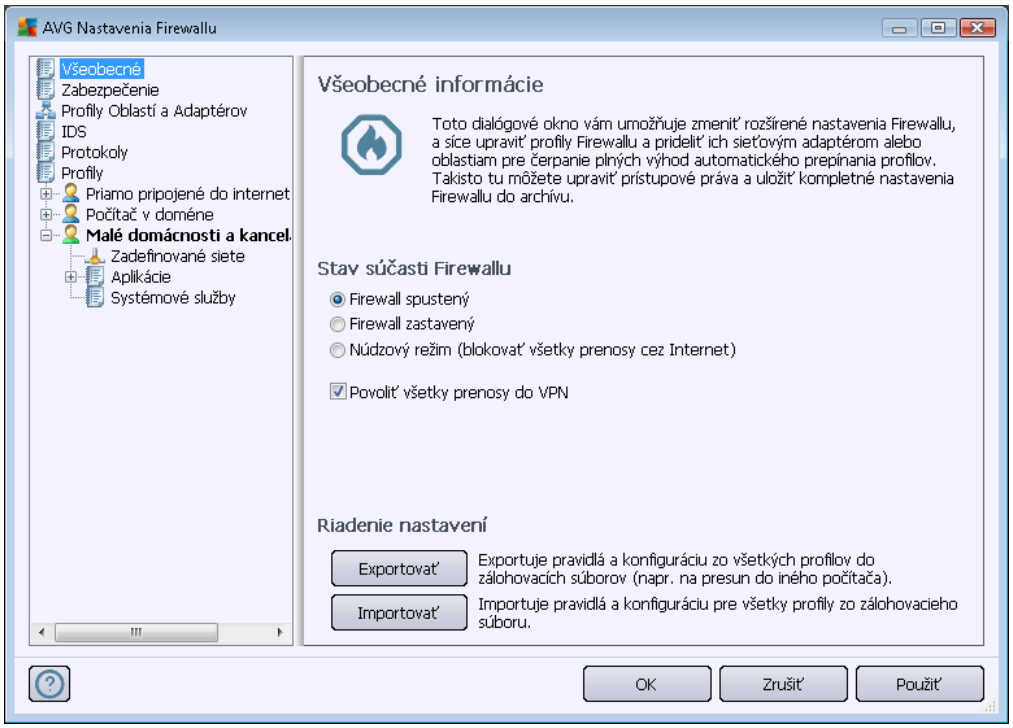
11. Nastavenia súčasti Firewall

Konfigurácia Firewallu sa otvorí v novom okne, kde môžete vo viacerých dialógových oknách nastaviť veľmi pokročilé parametre komponentu.

Výrobca softvéru nastavil všetky súčasti produktu AVG Internet Security 2012 tak, aby dosahovali optimálny výkon. Nemeňte predvolenú konfiguráciu, ak na to nemáte oprávnený dôvod. Odporúčame, aby nastavenia menil iba skúsený používateľ!

11.1. Všeobecné informácie

Dialógové okno ***Všeobecné informácie*** je rozdelené na dve časti:



Stav súčasti Firewall

Časť ***Stav súčasti Firewall*** umožňuje prepnúť stav súčasti Firewall vtedy, keď nastane potreba:

- ***Súčasť Firewall zapnutá*** – vyberte túto možnosť, ak chcete povoliť komunikáciu tým aplikáciám, ktoré sú nastavené ako „povolené“ v skupine pravidiel definovaných vo vybranom profile súčasti Firewall..
- ***Súčasť Firewall vypnutá*** – Táto možnosť úplne vypne bránu Firewall, všetky sieťové prenosy sa povolia, ale nebudú sa kontrolovať!
- ***Núdzový režim (blokovať všetky internetové prenosy)*** – Túto možnosť vyberte na zablokovanie jednotlivých sieťových portov. Brána Firewall naďalej beží, ale všetky sieťové

prenosy sú zastavené.

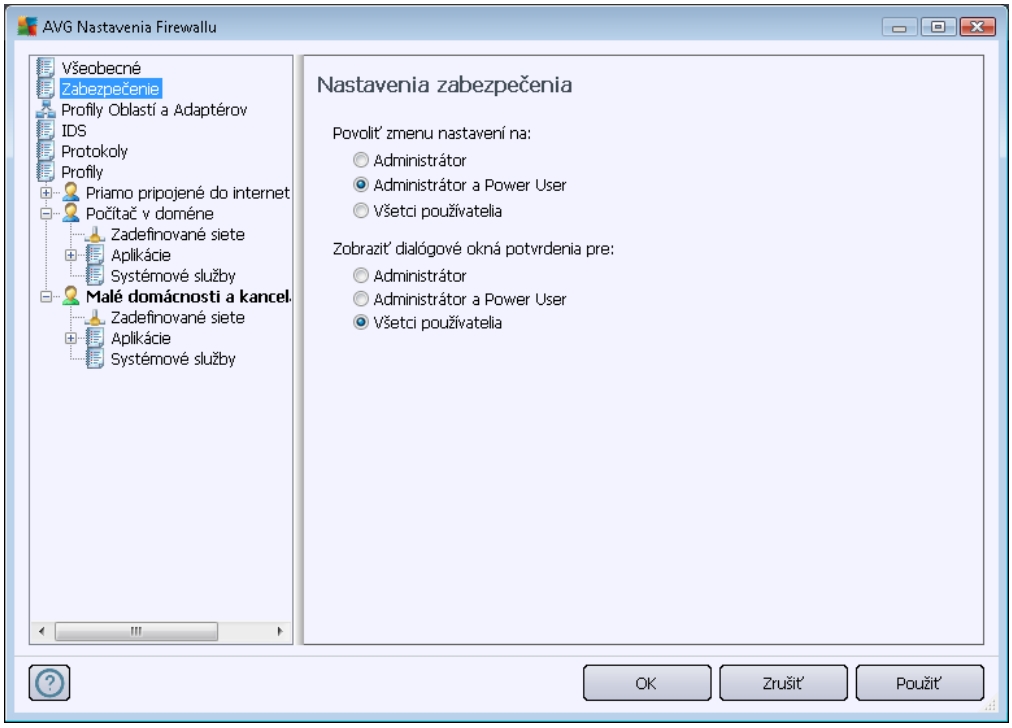
- ***Povoliť všetky prenosy do VPN*** *(štandardne zapnuté)* – Odporúčame vám označiť túto možnosť vtedy, keď používate pripojenie VPN *(virtuálna privátna sieť)*, napr. na pripojenie do kancelárie z domu. ***AVG Firewall*** automaticky preskúma vaše sieťové adaptéry a vyhľadá tie, ktoré sú používané pre pripojenie VPN, a umožní všetkým aplikáciám pripájať sa k cieľovej sieti *(platí len pre aplikácie bez prideleného špeciálneho pravidla súčasti Firewall)*. V štandardnom operačnom systéme s bežnými sieťovými adaptérmi, tento jednoduchý postup vám ušetrí prácu s nastavením podrobného pravidla pre každú aplikáciu, ktorú požívate v sieti VPN.

Poznámka: *Aby pripojenie VPN vôbec fungovalo, je potrebné povoliť komunikáciu na týchto systémových protokoloch: GRE, ESP, L2TP, PPTP. Robí sa to v dialógovom okne Systémové služby.*

Správa nastavení

Časť ***Riadenie nastavení*** umožňuje ***Export*** alebo ***Import*** konfigurácie súčasti Firewall, t. j. umožňuje exportovať definované pravidlá a nastavenia súčasti Firewall do zálohovacích súborov alebo importovať celý zálohovací súbor.

11.2. Zabezpečenie



V dialógovom okne ***Nastavenia zabezpečenia*** môžete zadefinovať všeobecné pravidlá správania Firewallu bez ohľadu na zvolený profil:

- ***Komu povoliť zmenu nastavení*** – Zadajte, kto má právo meniť konfiguráciu brány Firewall .

- ***Zobraziť dialógové okná potvrdenia pre*** – Zadajte, komu by sa mali zobrazovať dialógové okná potvrdenia *(dialógové okná vyžadujúce rozhodnutie v situácii, ktorú nerieši definované pravidlo brány Firewall)*.

V obidvoch prípadoch môžete prideliť špecifické právo jednej z nasledovných skupín používateľov:

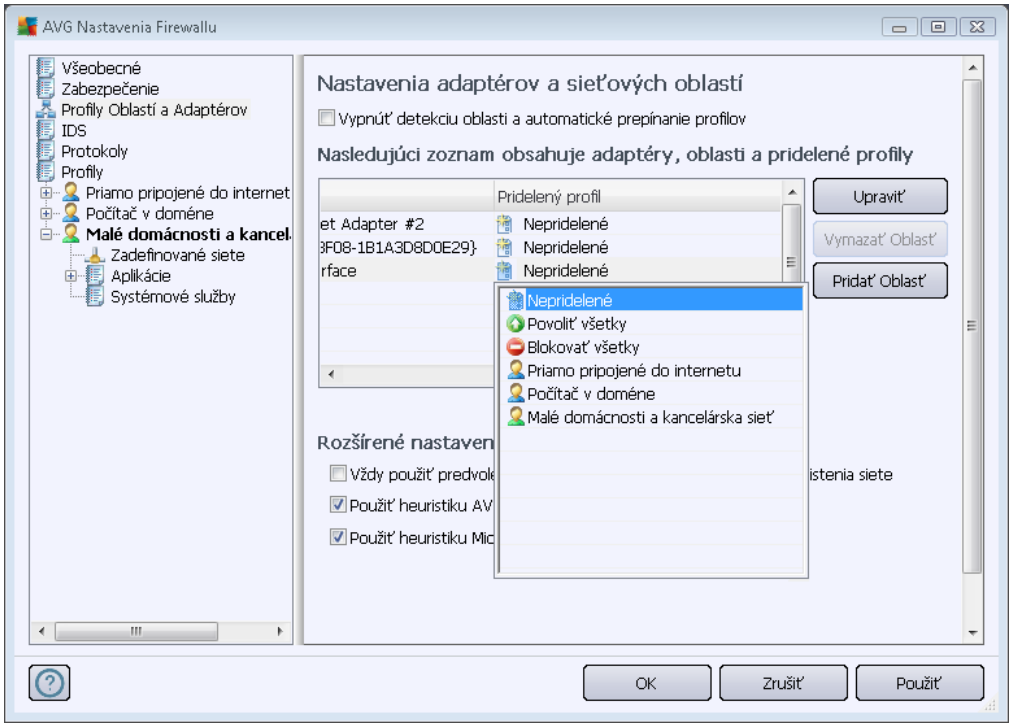
- ***Správca*** – riadi celý počítač a má právo zaradiť používateľov do skupín so špecificky definovanými oprávneniami

- ***Správca a oprávnený používateľ*** – Správca môže zaradiť používateľa do danej skupiny (*Oprávnený používateľ*) a definovať oprávnenia členov skupiny.

- ***Všetci používatelia*** – ostatní používatelia, ktorí nie sú zaradení do žiadnej skupiny

11.3. Profily oblastí a sieťových kariet

Dialógové okná ***Nastavenia sieťových kariet a sieťových oblastí*** sa používajú na zmenu nastavení súvisiacich s prideľovaním definovaných profilov konkrétnym sieťovým kartám a súvisiacim sieťam:



- ***Vypnúť zisťovanie oblastí a automatické prepínanie profilov*** *(štandardne vypnuté)* – Každému typu sieťového rozhrania, resp. každej oblasti, môžete prideliť jeden z definovaných profilov. Ak nechcete definovať konkrétne profily, potom sa použije jeden

spoločný profil. Ak sa však rozhodnete rozlišovať profily a prideliť ich konkrétnym sieťovým kartám a oblastiam a neskôr, z nejakého dôvodu, budete chcieť túto konfiguráciu dočasne prepnúť, označte možnosť ***Vypnúť detekciu oblastí a automatické prepínanie profilov***.

- ***Zoznam sieťových kariet, oblastí a pridelených profilov*** – V tomto zozname sa nachádza prehľad zistených sieťových kariet a oblastí. Každej položke môžete prideliť konkrétny profil z ponuky definovaných profilov. Ponuku otvoríte kliknutím ľavým tlačidlom myši na príslušnú položku v zozname adaptérov *(v stĺpci Pridelený profil)*, kde z kontextovej ponuky vyberiete príslušný profil.

Rozšírené nastavenia

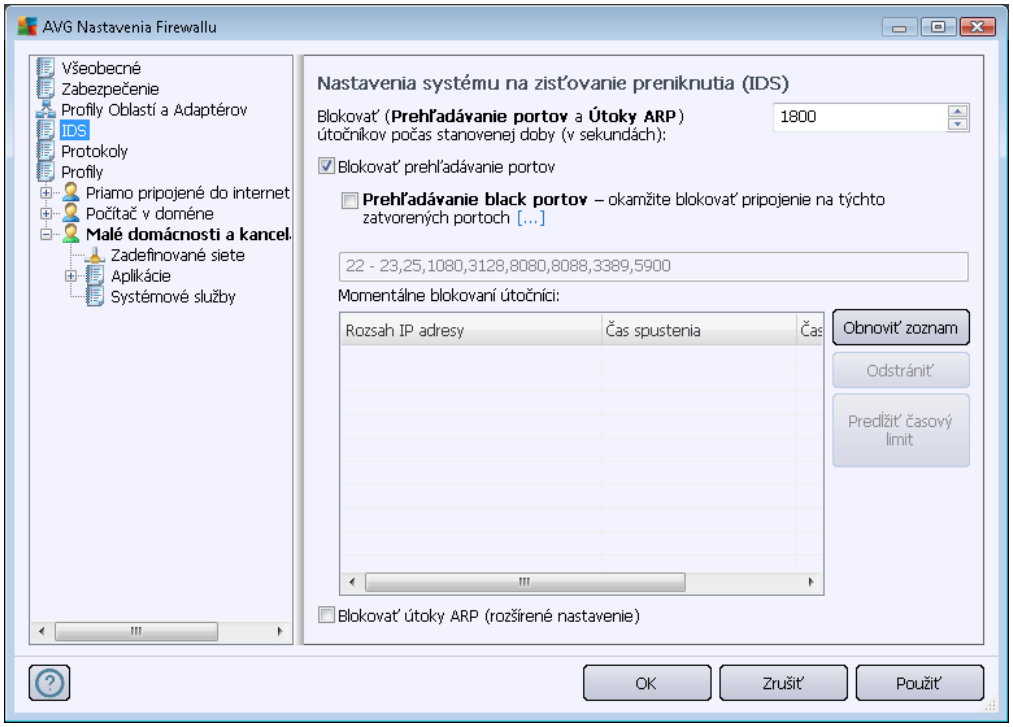
- ***Vždy použiť predvolený profil a neotvoriť okno zistenia novej sieťovej oblasti*** – Vždy, keď sa počítač pripojí k novej sieti, súčasť Firewall vás upozorní a otvorí dialógové okno, ktoré vám umožní vybrať typ sieťového pripojenia a prideliť jej profil súčasti Firewall. Ak si neželáte, aby sa toto dialógové okno otváralo, označte príslušné políčko.

- ***Používať heuristiku spoločnosti AVG na zisťovanie nových sietí*** – Zapína zhromažďovanie informácií o novej zistenej sieti pomocou vlastného mechanizmu produktu AVG (*táto možnosť je však dostupná len v operačných systémoch VISTA a novších systémoch*).

- ***Používať heuristiku spoločnosti Microsoft na zisťovanie nových sietí*** – Zapína zhromažďovanie informácií o novej zistenej sieti služby operačného systému Windows (*táto možnosť je dostupná len v operačnom systéme Windows Vista a novších systémoch*).

11.4. IDS

Systém na zisťovanie preniknutia je špeciálna funkcia na analýzu správania, ktorej účelom je identifikovať a blokovať podozrivé pokusy o komunikáciu na konkrétnych portoch počítača. Parametre IDS môžete nastaviť v dialógovom okne ***Nastavenia systému na zisťovanie preniknutia (IDS)***:



V dialógovom okne ***Nastavenia systému na zisťovanie preniknutia (IDS)*** sa nachádzajú tieto možnosti konfigurácie:

- ***Blokovať útočníkov (kontrola portov a útoky ARP) počas stanoveného času*** – Umožňuje nastaviť čas v sekundách, v ktorom bude port blokovaný vždy, keď sa na ňom zistí podozrivý pokus o komunikáciu. Štandardne je nastavený časový interval 1 800 sekúnd (*30 minút*).

- ***Blokovať kontrolu portov*** *(štandardne zapnuté)* – Začiarknutím tohto políčka sa zablokujú pokusy o komunikáciu na všetkých portoch TCP a UDP prichádzajúce do počítača zvonka. Pri každom takomto pripojení sa povolí päť pokusov a šiesty sa zablokuje. Možnosť je štandardne zapnutá a odporúčame ju takto ponechať. Ak necháte možnosť ***Blokovať kontrolu portov*** zapnutú, je možná ďalšia konfigurácia *(inak nasledujúce položky nebudú aktívne)*:

  - ***Kontrola čiernych portov*** – Začiarknutím tohto políčka sa okamžite zablokujú pokusy o komunikáciu na portoch uvedených v nasledujúcom textovom poli. Jednotlivé porty alebo intervaly portov sa musia oddeliť čiarkou. Program má preddefinovaný zoznam odporúčaných portov pre prípad, ak by ste chceli túto funkciu používať.

  - Momentálne blokovaní útočníci – V tejto časti sa nachádza zoznam pokusov o komunikáciu, ktoré sú momentálne blokované súčasťou Firewall. Celá história blokovaných pokusov sa nachádza v dialógovom okne Protokoly (*na karte Protokoly kontroly portov*).

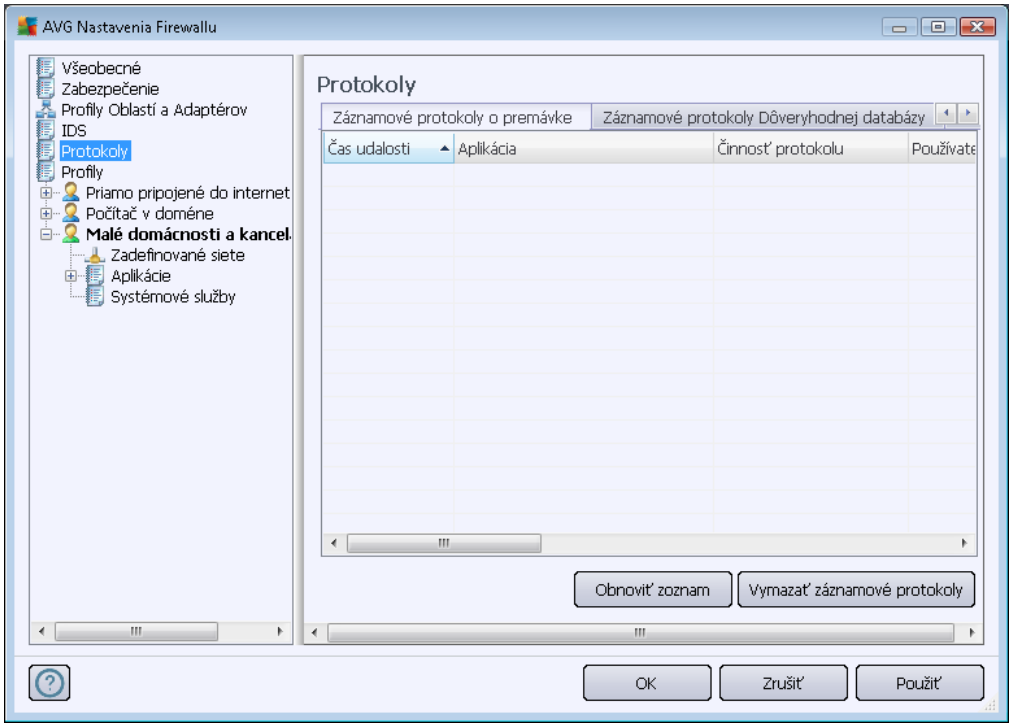
- ***Blokovať útoky ARP (rozšírené)*** *(štandardne vypnuté)* – Označením tejto možnosti aktivujete blokovanie špeciálnych typov pokusov o komunikáciu v miestnej sieti, ktoré

systém ***IDS*** vyhodnotil ako potenciálne nebezpečné. Použije sa čas nastavený v možnosti ***Blokovať útočníkov počas stanovenej doby***. Odporúča sa, aby túto funkciou používali len skúsení používatelia, ktorí sú oboznámení s typom a úrovňou rizika používanej miestnej siete.

Ovládacie tlačidlá

- ***Obnoviť zoznam*** – stlačením tohto tlačidla sa aktualizuje zoznam (*vrátane všetkých najnovších blokovaných pokusov*)
- ***Odstrániť*** – stlačením tohto tlačidla sa zruší vybrané blokovanie
- ***Predĺžiť časový limit*** – stlačením sa predĺži doba, počas ktorej sa vybraný pokus blokuje. Otvorí sa nové dialógové okno s rozšírenými možnosťami, ktoré umožňuje nastaviť konkrétny čas a dátum alebo neobmedzené trvanie.

11.5. Protokoly



Dialógové okno ***Protokoly*** umožňuje zobraziť zoznam všetkých zaznamenaných akcií a udalostí súčasti Firewall a obsahuje podrobný opis súvisiacich parametrov (*čas udalosti, názov aplikácie, príslušnú protokolovú činnosť, názov používateľa, PID, smer prenosu, typ protokolu, čísla vzdialených a miestnych portov a pod.*) na štyroch kartách:

- ***Protokoly prenosu*** – zobrazí informácie o činnosti všetkých aplikácií, ktoré sa pokúsili pripojiť k sieti.

- ***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 k sieti (*t. j. ak doposiaľ nebolo vytvorené pravidlo súčasti Firewall súvisiace s touto aplikáciou*) je potrebné zistiť, či sa má povoliť sieťová komunikácia príslušnej aplikácie. AVG najskôr nahliadne do *Dôveryhodnej databázy* a ak je v nej aplikácia uvedená, potom sa jej automaticky povolí prístup k sieti. Až potom, a pod podmienkou, že sa v databáze nenachádzajú informácie o tejto aplikácii, sa zobrazí dialógové okno, v ktorom sa vás program opýta, či chcete povoliť aplikácii prístup k sieti.

- ***Protokoly kontroly portov*** – Obsahujú záznamy o všetkých aktivitách Systému na detekciu preniknutia.

- ***Protokoly ARP*** – záznamy o blokovaní špeciálnych druhov pokusov o komunikáciu v miestnej sieti (možnosť *Blokovať útoky ARP*) detekovaných Systémom na detekciu preniknutia ako potenciálne nebezpečné.

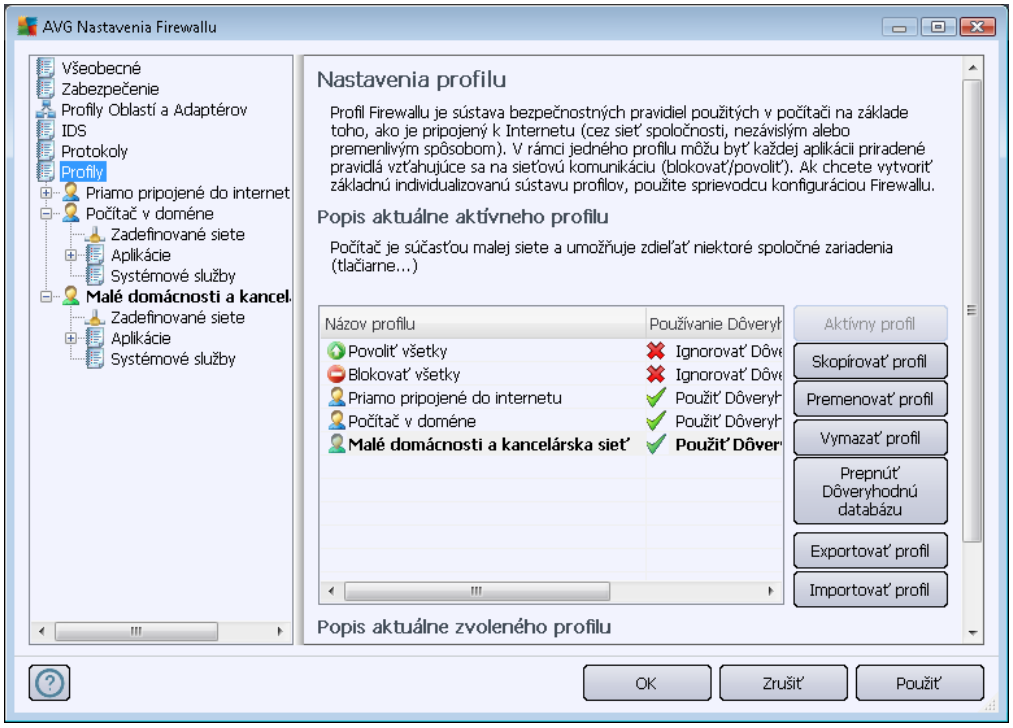
Ovládacie tlačidlá

- ***Obnoviť zoznam*** – Všetky zaprotokolované parametre môžete usporiadať podľa vybraného atribútu: chronologicky (*dátumy*) alebo podľa abecedy (*ostatné stĺpce*) – stačí kliknúť na hlavičku príslušného stĺpca. Použite tlačidlo ***Obnoviť zoznam*** na aktualizovanie práve zobrazených informácií.

- ***Odstrániť protokoly*** – Stlačením odstránite všetky položky v tabuľke.

11.6. Profily

V dialógovom okne ***Nastavenia profilu*** môžete nájsť zoznam všetkých dostupných profilov:



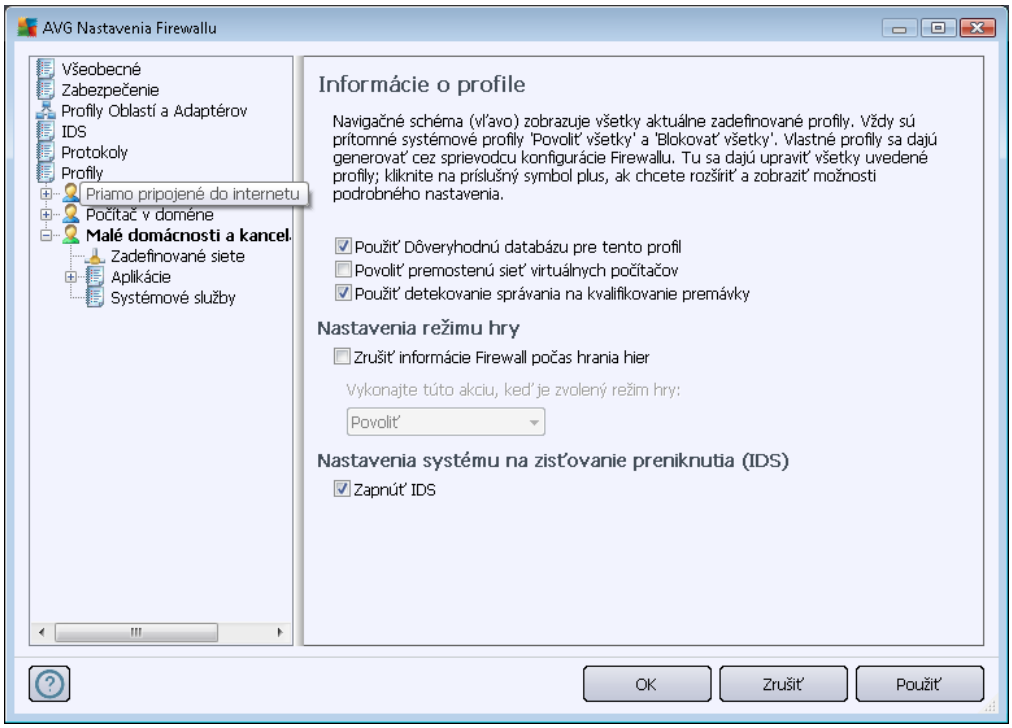
Systémové profily *(Povoliť všetky, Blokovať všetky)* nie je možné upraviť. Všetky vlastné profily *(Priamo pripojený k internetu, Počítač v doméne, Malá sieť v domácnosti alebo v kancelárii)* však môžete upraviť priamo v tomto dialógovom okne pomocou ovládacích tlačidiel:

- ***Aktivovať profil*** – Toto tlačidlo nastavuje zvolený profil ako aktívny, čo znamená, že konfiguráciu zvoleného profilu použije súčasť Firewall na ovládanie prenosov v sieti.
- ***Skopírovať profil*** – Vytvorí identickú kópiu zvoleného profilu; neskôr môžete kópiu upraviť a premenovať a vytvoriť nový profil na základe zvoleného pôvodného profilu.
- ***Premenovať profil*** – Umožňuje definovať nový názov vybraného profilu.
- ***Odstrániť profil*** – Odstráni zvolený profil zo zoznamu.
- ***Prepnúť na dôveryhodnú databázu*** – Môžete nastaviť, aby sa pre zvolený profil použili informácie *dôveryhodnej databázy* (*dôveryhodná databáza je interná databáza spoločnosti AVG zhromažďujúca informácie o dôveryhodných a certifikovaných aplikáciách, ktorým môže byť vždy povolené komunikovať on-line*).
- ***Exportovať profil*** – Zaznamená konfiguráciu zvoleného profilu do súboru, ktorý sa uloží pre prípadné budúce použitie.
- ***Importovať profil*** – Konfiguruje nastavenia zvoleného profilu na základe údajov exportovaných zo zálohovacieho súboru konfigurácie.

V spodnej časti tohto dialógového okna sa nachádza opis profilu, ktorý je momentálne vybraný vo vyššie uvedenom zozname.

Na základe počtu definovaných profilov, ktoré sa nachádzajú v zozname v dialógovom okne ***Profil***, sa zmení štruktúra ľavej navigačnej ponuky. Každý definovaný profil vytvorí špecifickú vetvu pod položkou ***Profil***. Jednotlivé profily sa potom dajú editovať v týchto dialógových oknách (*sú rovnaké pre všetky profily*):

11.6.1. Informácie o profile



Dialógové okno ***Informácie o profile*** je prvé dialógové okno časti, ktorá umožňuje zmeniť konfiguráciu každého profilu v samostatných dialógových oknách, ktoré sa týkajú konkrétnych parametrov profilu.

- ***Použiť dôveryhodnú databázu pre tento profil*** (*štandardne zapnuté*) – Označte túto možnosť, ak chcete používať *dôveryhodnú databázu* (*t. j. internú databázu spoločnosti AVG zhromažďujúcu informácie o dôveryhodných a certifikovaných aplikáciách komunikujúcich on-line. Ak konkrétna aplikácia nemá doposiaľ definované pravidlo, je potrebné zistiť, či sa jej môže povoliť prístup k sieti. AVG najskôr nahliadne do Dôveryhodnej databázy, a ak je v nej aplikácia uvedená, bude ju považovať za bezpečnú a umožní jej komunikovať v sieti. V opačnom prípade sa vás program opýta, či chcete aplikácii povoliť komunikáciu v sieti* v rámci príslušného profilu.

- ***Povoliť premostené sieťové spojenie virtuálnych počítačov*** (*štandardne vypnuté*) – Začiarknutím tejto možnosti sa povolí virtuálnym počítačom vo WMware, aby sa priamo pripojili do siete.

- ***Použiť zisťovanie správania na kvalifikovanie prenosu*** (*štandardne zapnuté*) –

Začiarknutím tejto možnosti sa povolí súčasti Firewall používať funkciu súčasti Identity Protection pri hodnotení aplikácie – Identity Protection dokáže zistiť, či sa aplikácia prejavuje podozrivým správaním alebo sa môže považovať za dôveryhodnú a môže sa jej povoliť komunikácia on-line.

Nastavenia režimu hry

Časť ***Nastavenia režimu hry*** umožňuje začiarknutím príslušnej položky nastaviť a potvrdiť, či sa majú zobrazovať informačné hlásenia súčasti Firewall aj vtedy, ak je v počítači spustená aplikácia na celú obrazovku (*zvyčajne ide o hry, ale platí to aj pre všetky aplikácie spustené na celú obrazovku, napr. prezentácie vo formáte PPT*), keďže informačné hlásenia môžu občas rušiť.

Ak začiarknete položku ***Vypnúť oznámenia súčasti Firewall počas hrania hry***, v rozbaľovacej ponuke potom nastavte, ktorá činnosť sa má vykonať v prípade, keď sa nová aplikácia bez definovaných pravidiel pokúsi komunikovať v sieti (*aplikácie, ktoré by normálne spôsobili otvorenie dialógového okna s otázkou*); všetky tieto aplikácie sa môžu buď povoliť alebo zakázať.

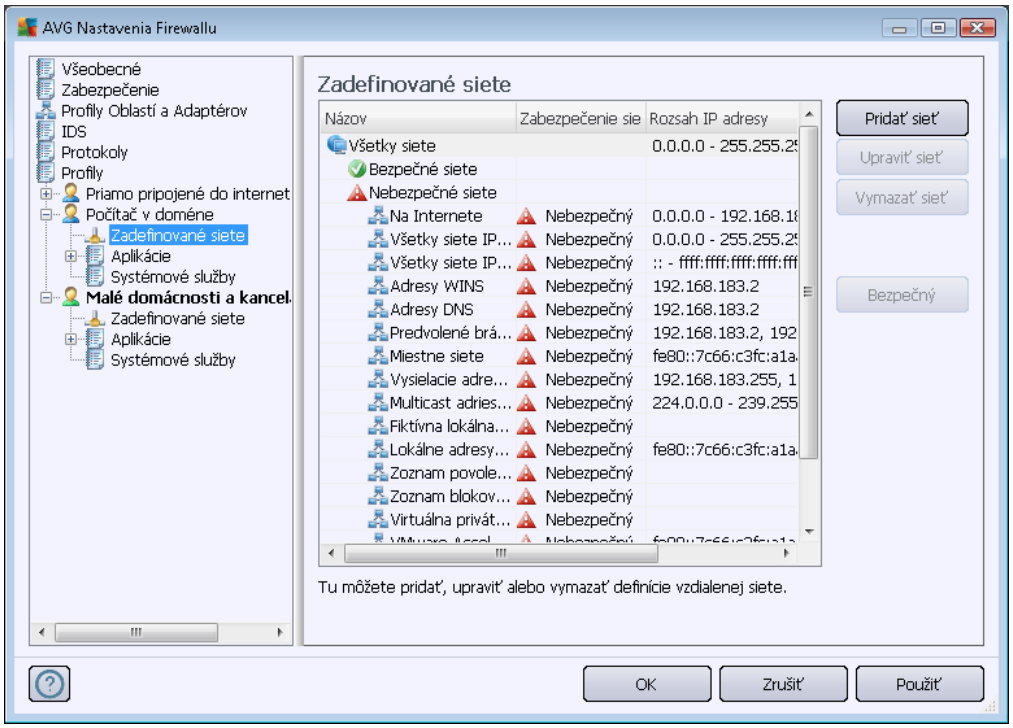
V režime hrania sa všetky naplánované úlohy (*kontrol, aktualizácie*) odložia do zatvorenia aplikácie.

Nastavenia systému na zisťovanie preniknutia (IDS)

Začiarknutím začiarkavacieho políčka ***Zapnúť IDS*** sa zapne špeciálna funkcia na analýzu správania, ktorej účelom je identifikovať a blokovať podozrivé pokusy o komunikáciu na konkrétnych portoch počítača *(podrobné informácie o nastaveniach tejto funkcie sa nachádzajú v kapitole IDS v tejto dokumentácii).*

11.6.2. Definované siete

V dialógovom okne ***Definované siete*** sa nachádza zoznam všetkých sietí, ku ktorým je váš počítač pripojený.

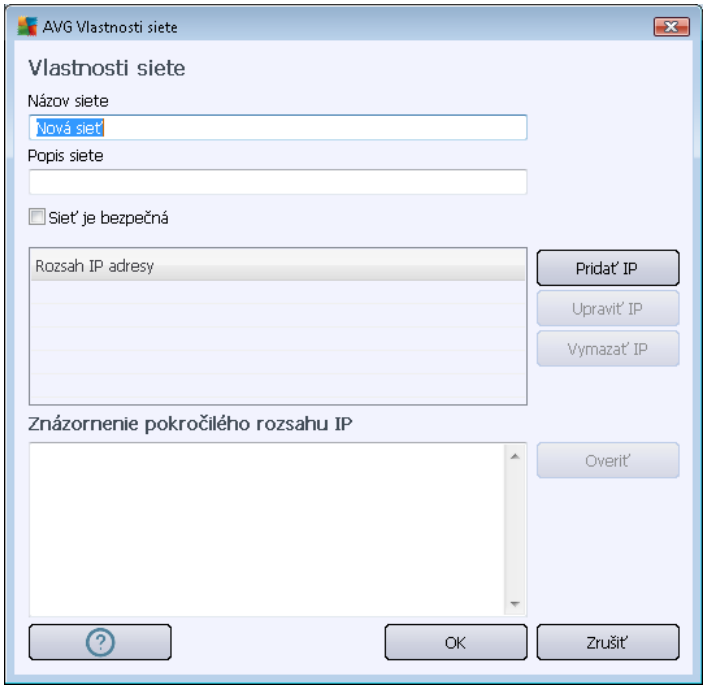


V zozname sú uvedené nasledujúce informácie o každej zistenej sieti:

- ***Siete*** – Obsahuje zoznam názvov všetkých sietí, ku ktorým je počítač pripojený.
- ***Zabezpečenie siete*** – Štandardne sa všetky siete považujú za nezabezpečené a len ak ste presvedčení, že je príslušná sieť bezpečná, povoľte ju (*kliknite na položku v zozname, ktorá odkazuje na príslušnú sieť a v kontextovej ponuke vyberte možnosť Bezpečná*). Všetky bezpečné siete sa potom pridajú do skupiny sietí, s ktorými môže aplikácia komunikovať podľa nastaveného pravidla aplikácie Povoliť pre bezpečné.
- ***Rozsah adries IP*** – Každá sieť sa automaticky zistí a definuje ako rozsah adries IP.

Ovládacie tlačidlá

- ***Pridať sieť*** – Otvorí dialógové okno ***Vlastnosti siete***, ktoré umožňuje editovať parametre novej definovanej siete:



V tomto dialógovom okne môžete definovať ***názov siete***, ***opis siete*** a prípadne nastaviť sieť ako bezpečnú. Novú sieť môžete potom definovať ručne v samostatnom dialógovom okne pomocou tlačidla ***Pridať adresu IP*** (prípadne ***Editovať adresu IP***/ ***Odstrániť adresu IP***). V tomto dialógovom okne môžete definovať sieť uvedením rozsahu adries IP alebo masky. Pri veľkom počte sietí, ktoré sa majú nastaviť ako súčasť novej vytvorenej siete, môžete použiť možnosť ***Podrobné definovanie rozsahu adries IP***. Do príslušného textového poľa zadajte zoznam všetkých sietí (*môžete použiť ľubovoľný štandardný formát*) a stlačením tlačidla ***Overiť*** skontrolujte, či je formát rozpoznateľný. Potom stlačením tlačidla ***OK*** potvrďte a uložte údaje.

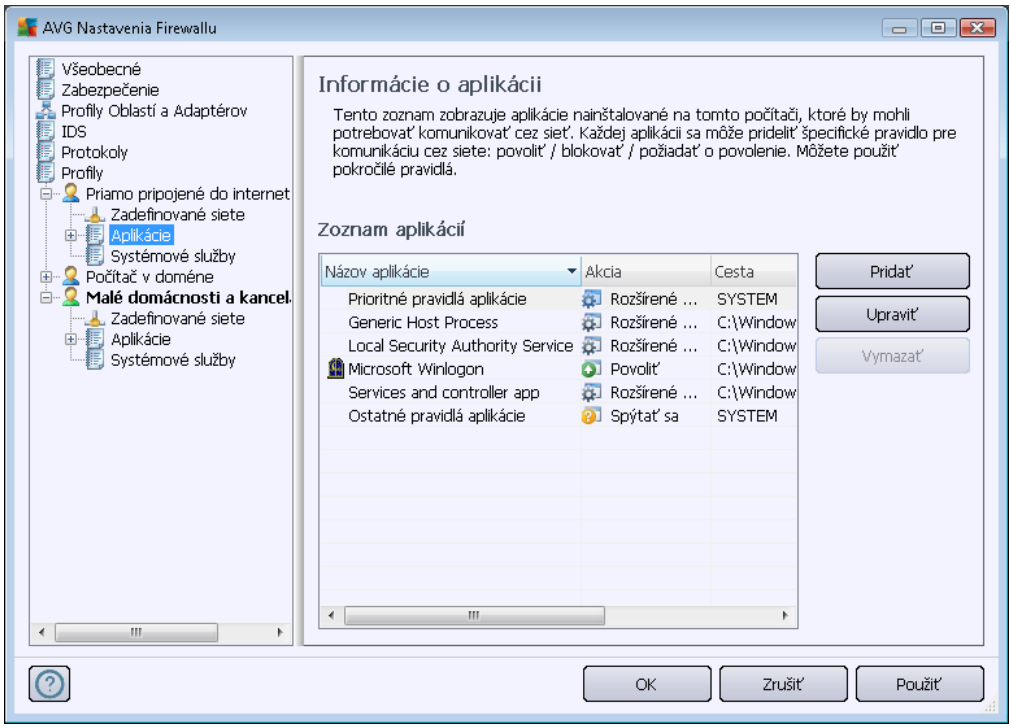
- ***Upraviť sieť*** – Otvorí dialógové okno ***Vlastnosti siete*** (*pozrite vyššie*), kde môžete upraviť parametre definovanej siete (*toto dialógové okno je rovnaké ako dialógové okno na pridanie novej siete, pozrite opis v predchádzajúcom odseku*).

- ***Odstrániť sieť*** – Odstráni záznam o sieti vybranej zo zoznamu sietí.

- ***Označiť ako bezpečnú*** – Štandardne sa všetky siete považujú za nezabezpečené a iba ak ste presvedčení, že je príslušná sieť bezpečná, použite toto tlačidlo a označte ju ako bezpečnú (*a naopak, po označení siete ako bezpečnej sa text tlačidla zmení na „Označiť ako nezabezpečenú“*).

11.6.3. Aplikácie

V informačnom dialógovom okne ***Aplikácie*** sa nachádza zoznam všetkých nainštalovaných aplikácií, ktoré pravdepodobne budú musieť komunikovať v sieti a ikony príslušnej akcie:



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

- – Povoliť komunikáciu vo všetkých sieťach
- – Povoliť komunikáciu v sieťach definovaných ako Len bezpečné
- – Blokovať komunikáciu
- – Zobraziť dialógové okno s otázkou (*Umožní vám rozhodnúť, či sa má povoliť alebo blokovať komunikácia, keď sa aplikácia pokúsi komunikovať v sieti.*)
- – Rozšírené nastavenia definované

Upozorňujeme, že program dokáže zistiť len prítomnosť nainštalovaných aplikácií, takže ak nainštalujete novú aplikáciu neskôr, budete pre ňu musieť definovať pravidlá bezpečnostnej brány firewall. Pri štandardnom nastavení, keď sa nová aplikácia pokúsi prvýkrát pripojiť v sieti, súčasť Firewall jej buď automaticky vytvorí pravidlo podľa dôveryhodnej databázy, alebo sa vás opýta, či chcete povoliť alebo blokovať komunikáciu. V druhom prípade budete môcť uložiť odpoveď ako trvalé pravidlo (ktoré sa potom zobrazí v tomto dialógovom okne).

Samozrejme, že pravidlá pre novú aplikáciu môžete definovať aj hneď: v tomto dialógovom okne stlačte tlačidlo ***Pridať*** a vyplňte informácie 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 pravidlá pre aplikácie*** (*v spodnej časti zoznamu*) sa použijú ako „posledná možnosť" v prípade, keď sa nepoužijú konkrétne pravidlá pre aplikácie, ako sú neznáme a nedefinované aplikácie. Vyberte akciu, ktorá sa má spustiť, keď sa táto aplikácia pokúsi komunikovať v sieti:
  - *Blokovať* – komunikácia bude vždy blokovaná.
  - *Povoliť* – komunikácia bude povolená v každej sieti.
  - *Spýtať sa* – budete musieť rozhodnúť, či má byť komunikácia povolená alebo zakázaná.

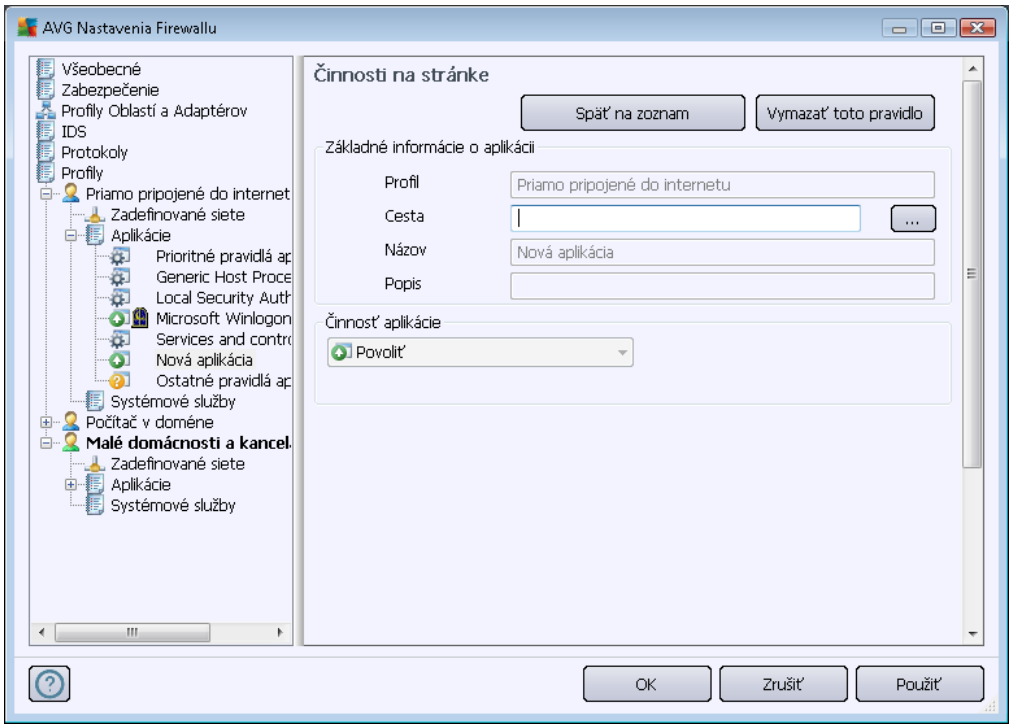
Tieto položky majú nastavené iné možnosti než bežné aplikácie a sú určené len pre skúsených používateľov. Odporúčame vám, aby ste nemenili tieto nastavenia!

Ovládacie tlačidlá

Na vykonanie zmien v zozname sa používajú tieto ovládacie tlačidlá:

- ***Pridať*** – Otvorí sa prázdne dialógové okno Akcie na stránke, ktoré sa používa na definovanie nových pravidiel pre aplikáciu.
- ***Upraviť*** – Otvorí sa to isté dialógové okno Akcie na stránke, ktoré sa používa na zmenu existujúcej skupiny pravidiel pre aplikáciu.
- ***Odstrániť*** – Odstráni zvolenú aplikáciu zo zoznamu.

V dialógovom okne ***Akcie na stránke*** môžete definovať podrobné nastavenia pre príslušnú aplikáciu:



Ovládacie tlačidlá

V hornej časti dialógového okna sa nachádzajú dve ovládacie tlačidlá:

- ***Späť na zoznam*** – Stlačením tlačidla zobrazíte prehľad všetkých definovaných pravidiel pre aplikácie.
- ***Odstrániť toto pravidlo*** – Stlačením tohto tlačidla odstránite aktuálne zobrazené pravidlo aplikácie. ***Tento krok nie je možné vrátiť späť!***

Základné informácie o aplikácii

V tejto časti vyplňte ***názov*** aplikácie a prípadne aj ***opis*** (*krátku poznámku pre vašu informáciu*). V poli ***Cesta*** zadajte úplnú cestu k aplikácii (*spustiteľnému súboru*) na disku; prípadne stlačte tlačidlo „ ***...***“ a ľahko vyhľadajte aplikáciu v stromovej štruktúre.

Akcia pre aplikáciu

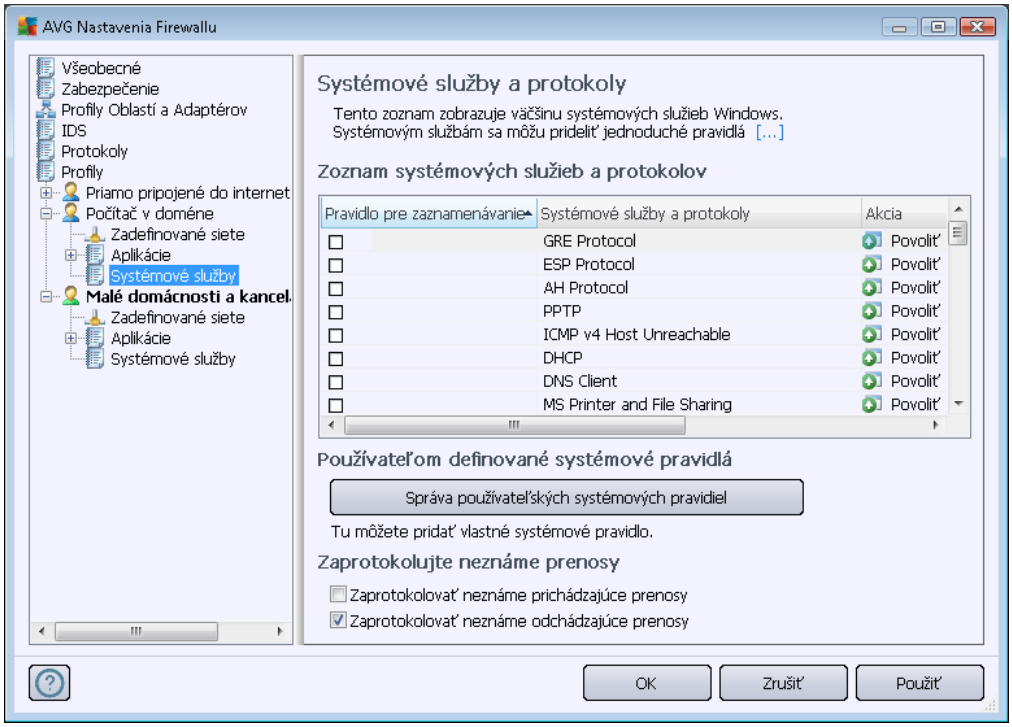
Rozbaľovacia ponuka umožňuje vybrať pravidlo súčasti Firewall pre aplikáciu, t. j. čo má Firewall urobiť, keď sa aplikácia pokúsi komunikovať v sieti:

- ***Povoliť pre všetky*** – Umožní aplikácii komunikovať vo všetkých definovaných sieťach a adaptéroch bez obmedzení.
- ***Povoliť pre bezpečné*** – Umožní aplikácii komunikovať len v sieťach označených ako bezpečné *(dôveryhodné)*.
- ***Blokovať*** – Automaticky zakáže komunikáciu; aplikácia sa nebude môcť pripojiť k žiadnej sieti.
- ***Opýtať sa*** – Otvorí sa dialógové okno, ktoré vám umožní rozhodnúť, či sa má povoliť alebo blokovať pokus o komunikáciu v danom momente.
- ***Rozšírené nastavenia*** – Zobrazia sa ďalšie rozšírené a podrobné možnosti nastavenia v spodnej časti dialógového okna v časti ***Podrobné pravidlá pre aplikácie***. Nastavenia sa použijú v uvedenom poradí, takže ich môžete ***posúvať hore*** resp. ***posúvať dole*** v zozname podľa požadovaného poradia. Po kliknutí na konkrétne pravidlo v zozname sa v spodnej časti dialógového okna zobrazia podrobné informácie o pravidle. Jednotlivé modré podčiarknuté hodnoty môžete zmeniť po kliknutí v príslušnom dialógovom okne nastavení. Ak chcete vymazať zvýraznené pravidlo, kliknite na tlačidlo ***Odstrániť***. Ak chcete definovať nové pravidlo, kliknutím na tlačidlo ***Pridať*** otvorte dialógové okno ***Zmena pravidla*** a definujte všetky potrebné parametre.

11.6.4. Systémové služby

Zmeny v dialógovom okne Systémové služby a protokoly odporúčame 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:



Zoznam systémových služieb a protokolov

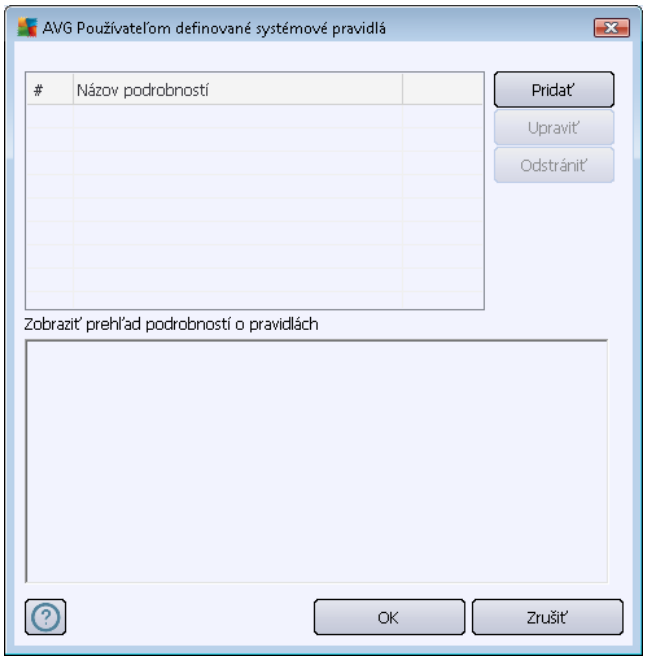
Tabuľka má tieto stĺpce:

- ***Zaznamenať činnosti pravidla*** – Používa sa na zapnutie funkcie na zaznamenania každého použitia pravidla v protokoloch.
- ***Systémová služba a protokoly*** – V tomto stĺpci je uvedený názov príslušnej systémovej služby.
- ***Akcia*** – V tomto stĺpci sa nachádza ikona pridelenej akcie:
  - Povoliť komunikáciu pre všetky siete
  - Povoliť komunikáciu pre siete definované ako Len bezpečné
  - Blokovať komunikáciu
- ***Siete*** – Tento stĺpec informuje o tom, ktorej konkrétnej siete sa systémové pravidlo týka.

Ak chcete zmeniť nastavenia položky v zozname (*vrátane pridelených akcií*), kliknite pravým tlačidlom myši na položku a vyberte možnosť ***Editovať***. ***Zmenu systémových pravidiel by však mali robiť 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***. V hornej časti dialógového okna ***Používateľom definované systémové pravidlá*** sa nachádza prehľad všetkých informácií o práve editovanom systémovom pravidle, v dolnej časti sa nachádzajú vybrané informácie. Na editovanie, pridanie resp. vymazanie používateľom definovaného pravidla sa používa príslušné tlačidlo; výrobcom definované pravidlá sa dajú len editovať:



Podrobné nastavenie pravidiel je pokročilá funkcia určená najmä pre správcov siete, ktorí potrebujú mať úplnú kontrolu nad konfiguráciou súčasti Firewall. Ak nie ste oboznámený s typmi komunikačných protokolov, číslami sieťových portov, definíciami adries IP a pod., nemeňte tieto nastavenia! Ak naozaj potrebujete zmeniť konfiguráciu, postupujte podľa pokynov v príslušných súboroch pomocníka.

Zaznamenať neznáme prenosy

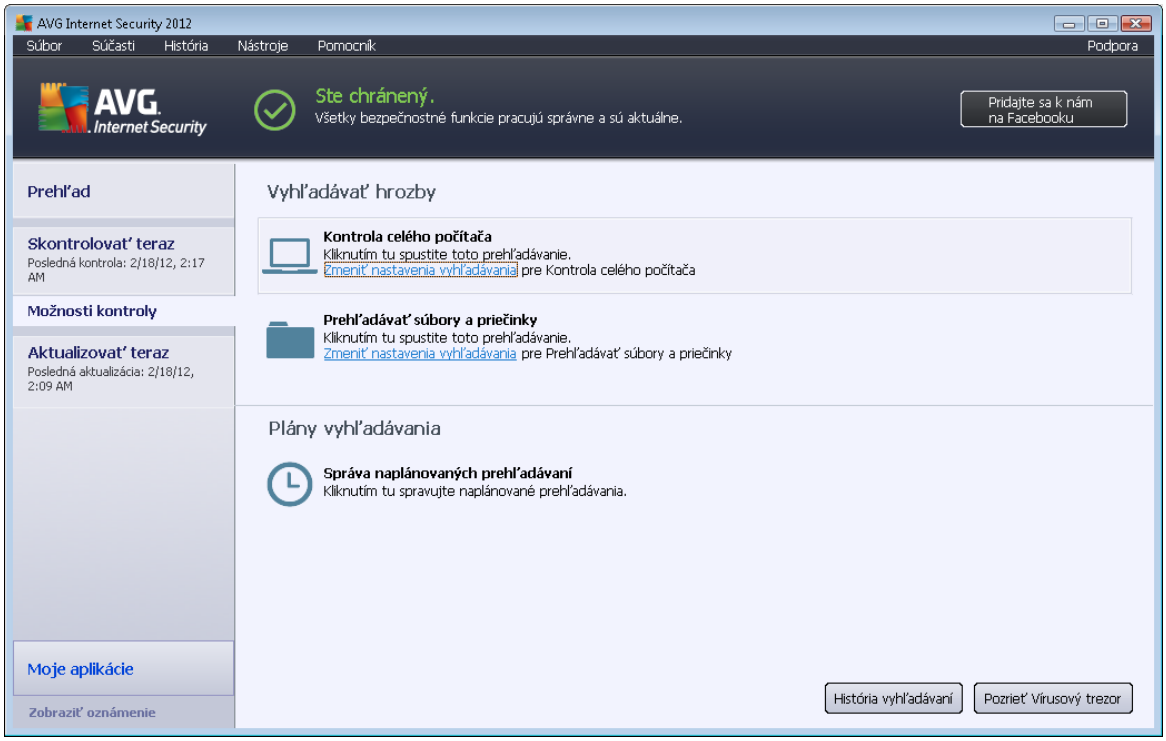
- ***Zaznamenať neznáme prichádzajúce prenosy*** *(štandardne vypnuté)* – Toto políčko začiarknite, ak sa protokoloch má zaznamenať každý neznámy pokus o pripojenie k počítaču zvonka.

- ***Zaznamenať neznáme odchádzajúce prenosy*** *(štandardne zapnuté)* – Toto políčko začiarknite, ak sa v protokoloch má zaznamenať každý neznámy pokus o pripojenie počítača k vonkajšej adrese.

12. Kontrola AVG

Štandardne aplikácia **AVG Internet Security 2012** nespúšťa žiadnu kontrolu, pretože po úvodnej kontrole by ste mali byť dokonale chránení rezidentnými súčasťami produktu **AVG Internet Security 2012**, ktoré sú vždy na stráži a nedovolia žiadnemu škodlivému kódu preniknúť do počítača. Samozrejme, že môžete naplánovať kontrolu, ktorá sa bude spúšťať v pravidelných intervaloch alebo manuálne kedykoľvek spustiť kontrolu podľa vlastných potrieb.

12.1. Rozhranie kontroly



Rozhranie kontroly programom AVG sa otvára rýchlym odkazom ***Možnosti kontroly***. Kliknutím na tento odkaz otvorte dialógové okno ***Kontrola hrozieb***. V tomto dialógovom okne sa nachádzajú tieto položky:

- prehľad preddefinovaných kontrol – tri druhy kontrol definované dodávateľom softvéru sú pripravené na použitie okamžitým výberom alebo ako naplánované:
  - Kontrola celého počítača
  - Kontrola špecifických súborov alebo priečinkov
- Časť Naplánovať prehľadávania – umožňuje definovať nové testy a vytvoriť nové harmonogramy podľa potreby.

Ovládacie tlačidlá

V testovacom rozhraní sa nachádzajú tieto tlačidlá:

- ***História kontrol*** – otvorí dialógové okno Prehľad výsledkov kontrol s celou históriou kontrol.
- ***Otvoriť Vírusový trezor*** – otvorí nové okno s Vírusovým trezorom, t. j. miesto, na ktorom sú uložené v karanténe detekované infekcie.

12.2. Preddefinované kontroly

Jednou z hlavných funkcií produktu **AVG Internet Security 2012** je kontrola na požiadanie. Testy na požiadanie sú určené na kontrolu rôznych častí počítača pri každom podozrení na možný výskyt vírusovej infekcie. Odporúčame vám, aby ste robili tieto testy pravidelne, aj keď si myslíte, že sa v počítači nenájde žiaden vírus.

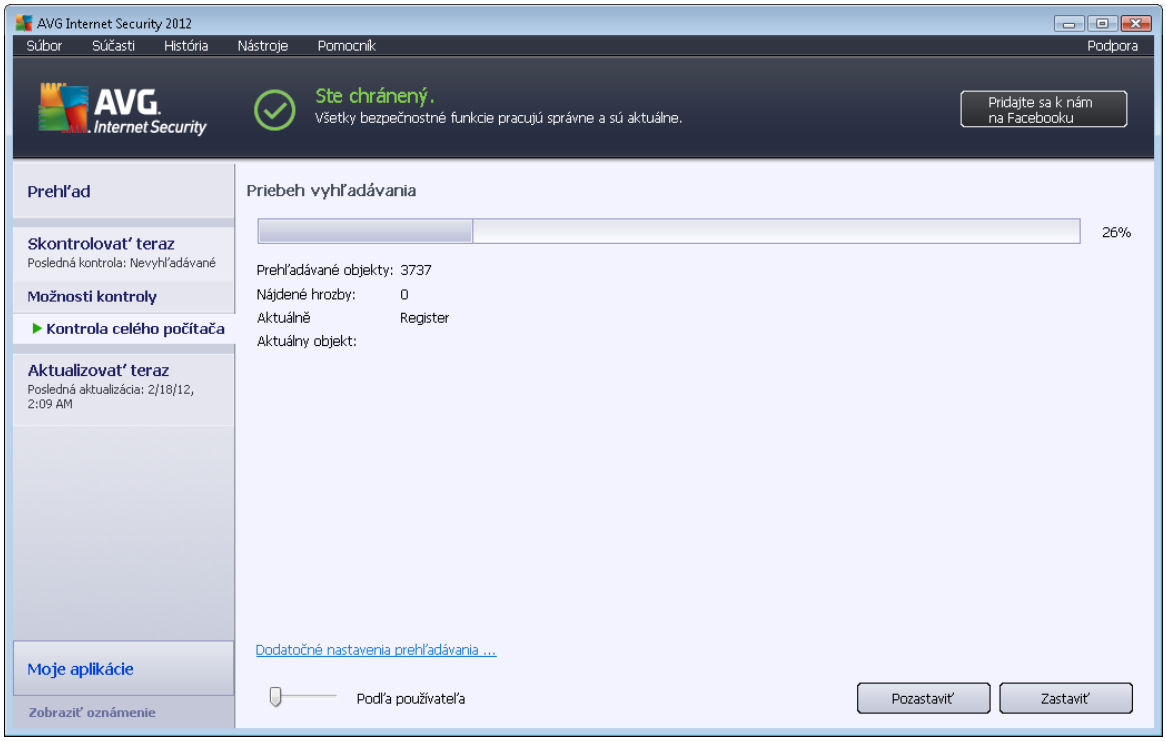
V produkte **AVG Internet Security 2012** sa nachádzajú tieto typy kontrol prednastavené dodávateľom softvéru:

12.2.1. Kontrola celého počítača

Kontrola celého počítača – skontroluje možné infekcie resp. potenciálne nežiaduce programy v celom počítači. Tento test bude kontrolovať všetky pevné disky počítača, deteguje vírusy a vylieči všetky nájdené vírusy alebo ich odstráni do Vírusového trezora. Odporúčame vám, aby ste naplánovali program takým spôsobom, aby sa kontrola celého počítača spustilo najmenej raz za týždeň.

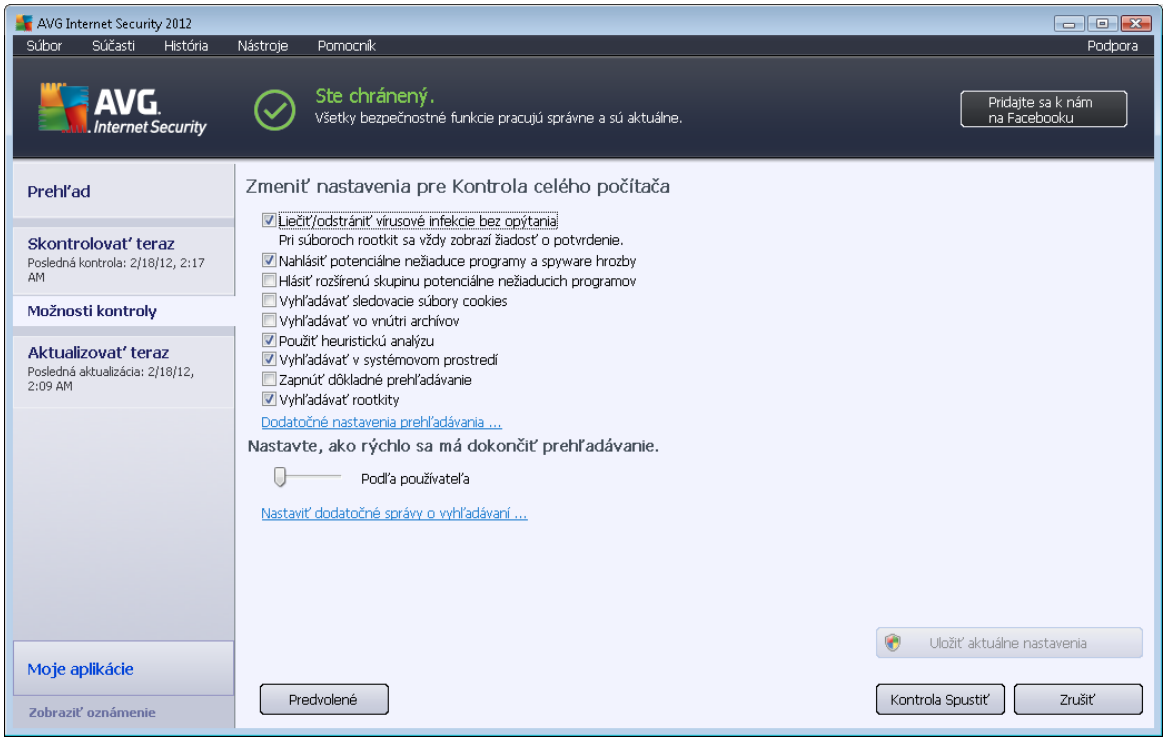
Spustenie kontroly

Kontrola celého počítača sa spúšťa priamo v rozhraní kontroly kliknutím na ikonu kontroly. Pre tento typ kontroly nie je potrebné konfigurovať žiadne ďalšie konkrétne nastavenia, kontrola sa spustí ihneď v dialógovom okne ***Prebieha kontrola*** (*pozri snímku obrazovky*). V prípade potreby môžete kontrolu dočasne prerušiť (tlačidlo ***Pozastaviť***) alebo zrušiť (tlačidlo ***Zastaviť***).



Zmena konfigurácie kontroly

Program umožňuje editovať vopred definované predvolené nastavenia funkcie ***Kontrola celého počítača***. Kliknutím na odkaz ***Zmeniť nastavenia kontroly*** otvorte dialógové okno ***Zmena nastavení kontroly celého počítača*** *(otvára sa v rozhraní kontroly pomocou odkazu Zmeniť nastavenia kontroly funkcie Kontrola celého počítača)*. ***Odporúčame vám, aby ste zachovali predvolené nastavenia, ak nemáte vážny dôvod na ich zmenu!***



- ***Parametre kontroly*** – v zozname parametrov kontroly môžete zapnúť alebo vypnúť konkrétne parametre podľa potreby:

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

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

    - ***Hlásiť rozšírenú skupinu potenciálne nežiaducich programov*** (*štandardne vypnuté*) – Začiarknite, ak chcete zistiť rozšírenú skupinu programov spyware: programov, ktoré sú úplne v poriadku a neškodné pri získaní priamo od výrobcu, ale neskôr sa môžu zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré zvyšuje úroveň zabezpečenia počítača, ale môže blokovať zákonné programy, preto je táto funkcia štandardne vypnutá.

    - ***Kontrolovať sledovacie súbory cookies*** (*štandardne vypnuté*) – tento parameter súčasti Anti-Spyware zapína funkciu na detekovanie súborov cookies (*HTTP cookies sa používajú na overenie totožnosti, sledovanie a správu konkrétnych informácií o používateľoch, ako sú preferencie stránok alebo obsah elektronických nákupných košíkov*).

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

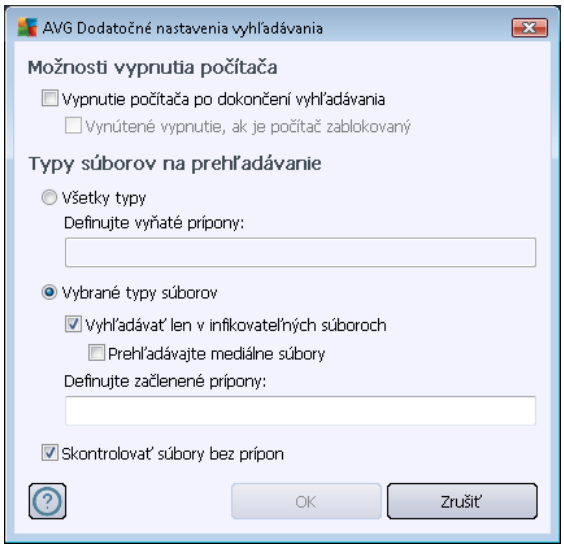
- ***Používať heuristiku*** (*štandardne zapnuté*): heuristická analýza (*dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí*) bude jedna z metód, ktoré sa použijú na detegovanie vírusov počas kontroly.

- ***Kontrolovať systémové prostredie*** (*štandardne zapnuté*) – počas kontroly sa budú kontrolovať aj systémové oblasti počítača.

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

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

- ***Ďalšie nastavenia kontroly*** – tento odkaz otvorí nové dialógové okno ***Ďalšie nastavenia kontroly***, ktoré sa používa na nastavenie týchto 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 zamknutý (***Vynútené vypnutie počítača, keď je zamknutý***).

- ***Typy súborov na kontrolu*** – Ďalej môžete rozhodnúť, či sa majú kontrolovať:

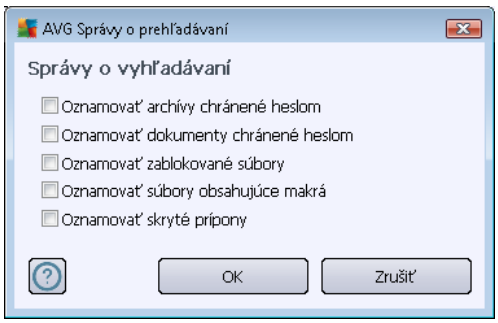
- ***Všetky typy súborov*** s možnosťou definovať výnimky kontroly vytvorením zoznamu čiarkou oddelených prípon súborov, ktoré sa nemajú kontrolovať.

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

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

- ***Nastaviť rýchlosť dokončenia kontroly*** – pomocou posúvača zmeňte prioritu procesu kontroly. Štandardne má tento parameter nastavenú úroveň automatického využívania zdrojov „*podľa používateľa*“. Prípadne môžete spustiť procesy kontroly pomalšie, čím sa minimalizuje využívanie počítačových zdrojov (*toto nastavenie je užitočné vtedy, ak potrebujete pracovať na počítači, ale nezaujíma vás, ako dlho bude kontrola trvať*), alebo rýchlejšie s vyššími nárokmi na využívanie počítačových zdrojov (*napr. keď sa počítač dočasne nepoužíva*).

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



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

12.2.2. Kontrola súborov/priečinkov

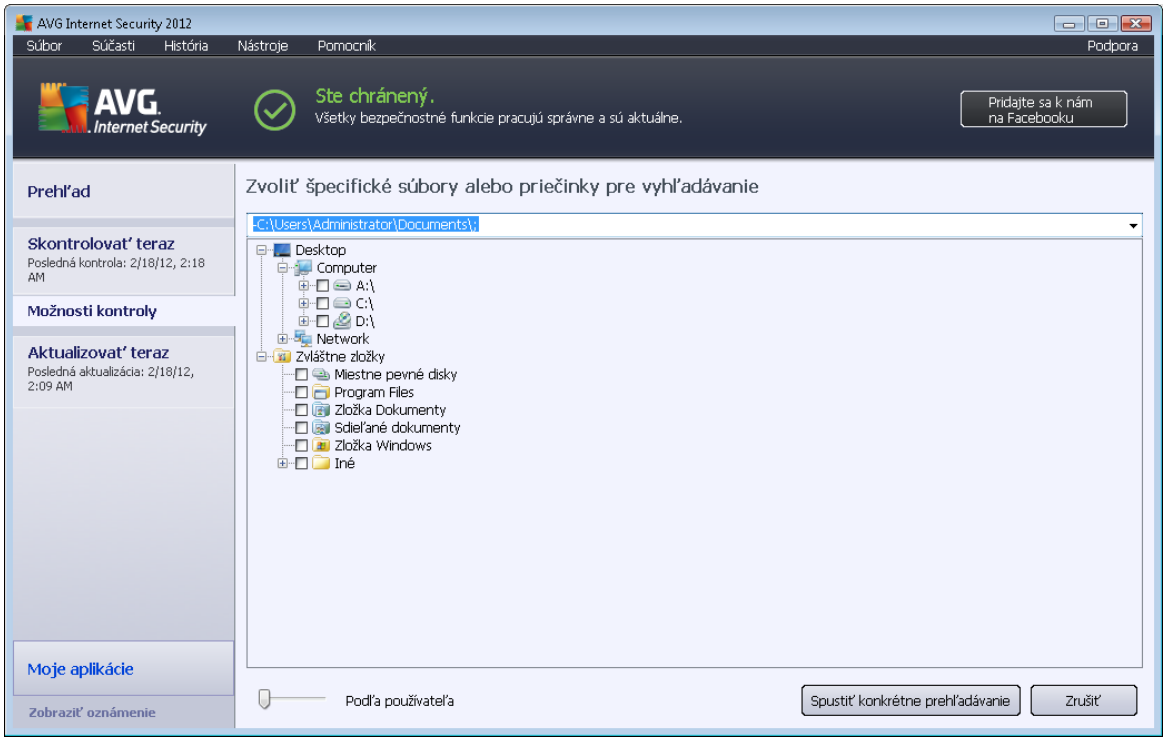
Kontrola súborov/priečinkov – kontrolovať sa budú len vami vybrané oblasti počítača (*vybrané priečinky, pevné disky, diskety, disky CD a pod.*). Priebeh kontroly pri detekovaní vírusu a jeho liečba sú rovnaké ako pri kontrole celého počítača: všetky nájdené vírusy sa vyliečia alebo odstránia do Vírusového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

Spustenie kontroly

Kontrolu vybraných súborov alebo priečinkov môžete spustiť priamo v rozhraní kontroly kliknutím na ikonu kontroly. 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 vybranému priečinku sa vygeneruje automaticky a objaví sa v textovom okne v hornej časti tohto dialógového okna.

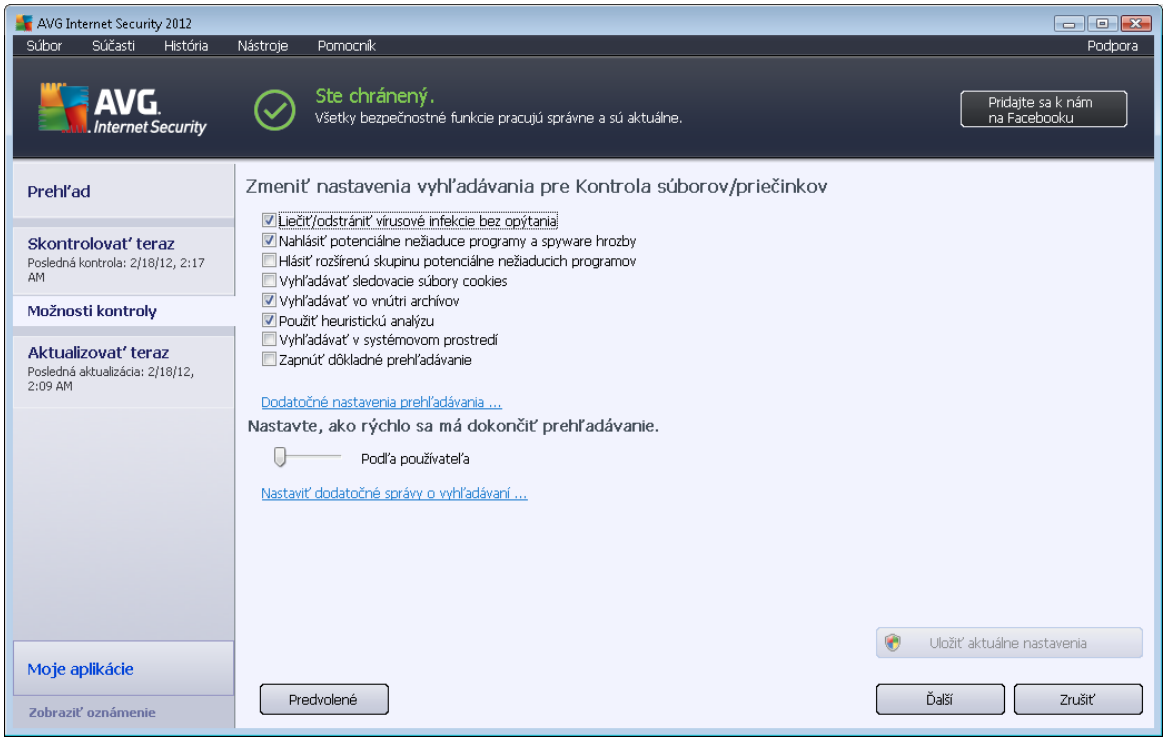
Rovnako môžete nastaviť kontrolu konkrétneho priečinka a zároveň vylúčiť všetky jeho podpriečinky z kontroly; v tom prípade vložte znak mínus „**-**“ pred automaticky vygenerovanú cestu (*pozri snímku obrazovky*). Na vylúčenie celého priečinka z kontroly použite parameter „**!**“.

Napokon, ak chcete spustiť kontrolu, stlačte tlačidlo ***Spustiť kontrolu***; samotný proces kontroly sa v podstate zhoduje s kontrolou celého počítača.



Zmena konfigurácie kontroly

Program umožňuje zmeniť preddefinované predvolené nastavenia funkcie na ***kontrolu konkrétnych súborov alebo priečinkov***. Kliknutím na odkaz ***Zmeniť nastavenia kontroly*** otvorte dialógové okno ***Zmena nastavení kontroly konkrétnych súborov alebo priečinkov***. ***Odporúčame vám, aby ste zachovali predvolené nastavenia, ak nemáte vážny dôvod na ich zmenu!***



- ***Parametre kontroly*** – v zozname parametrov kontroly môžete zapnúť alebo vypnúť konkrétne parametre podľa potreby:

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

    - ***Hlásiť potenciálne nežiaduce programy a hrozby spyware*** (*štandardne zapnuté*) – začiarknite toto okienko, ak chcete zapnúť súčasť Anti-Spyware a kontrolovať spyware a vírusy. Spyware predstavuje pochybnú kategóriu škodlivého softvéru: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.

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

    - ***Kontrolovať sledovacie súbory cookies*** (*štandardne vypnuté*) – tento parameter súčasti Anti-Spyware zapína funkciu na detekovanie súborov cookies (*HTTP cookies sa používajú na overenie totožnosti, sledovanie a správu konkrétnych informácií o používateľoch, ako sú preferencie stránok alebo obsah elektronických nákupných košíkov*).

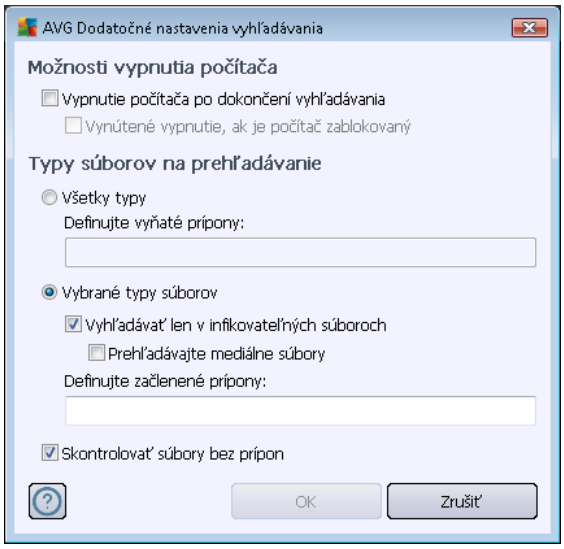
- ***Kontrolovať vo vnútri archívov*** (*štandardne zapnuté*) – tento parameter určuje, že sa majú počas kontroly overovať všetky súbory uložené vo vnútri archívov, napr. ZIP, RAR...

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

- ***Kontrolovať systémové prostredie*** (*štandardne vypnuté*) – počas kontroly sa budú overovať aj systémové oblasti počítača.

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

- ***Ďalšie nastavenia kontroly*** – tento odkaz otvorí nové dialógové okno ***Ďalšie nastavenia kontroly***, ktoré sa používa na nastavenie týchto 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 zamknutý (***Vynútené vypnutie počítača, keď je zamknutý***).

  - ***Typy súborov na kontrolu*** – Ďalej môžete rozhodnúť, či sa majú kontrolovať:

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

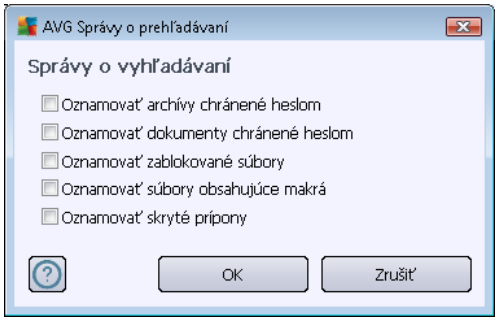
    - ***Vybrané typy súborov*** – môžete nastaviť, aby sa kontrolovali len súbory, pri ktorých existuje pravdepodobnosť infikovania (*súbory, ktoré nemôžu byť napadnuté infekciou, napríklad niektoré jednoduché textové súbory alebo*

niektoré nespustiteľné súbory), vrátane mediálnych súborov (*video, audio súborov – ak necháte toto okienko nezačiarknuté, potom sa čas kontroly skráti ešte viac, pretože tieto súbory sú často veľmi veľké, pričom pravdepodobnosť napadnutia vírusom je veľmi malá*). Znova môžete nastaviť (podľa prípony), ktoré súbory sa majú kontrolovať vždy.

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

- ***Priorita procesu kontroly*** – použite posúvač na zmenu priority procesu kontroly. Štandardne má tento parameter nastavenú úroveň automatického využívania zdrojov „*podľa používateľa*“. Prípadne môžete spustiť procesy kontroly pomalšie, čím sa minimalizuje využívanie počítačových zdrojov (*toto nastavenie je užitočné vtedy, ak potrebujete pracovať na počítači, ale nezaujíma vás, ako dlho bude kontrola trvať*), alebo rýchlejšie s vyššími nárokmi na využívanie počítačových zdrojov (*napr. keď sa počítač dočasne nepoužíva*).

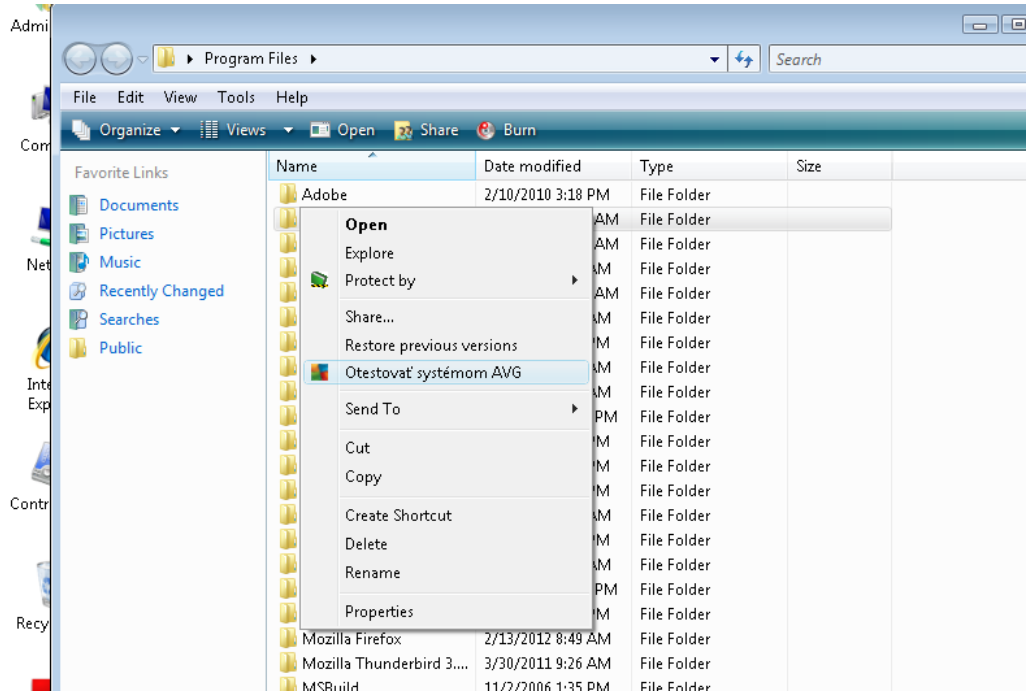
- ***Vytvoriť ďalšie správy o kontrole*** – odkaz otvorí nové dialógové okno ***Správy o kontrole***, ktoré umožňuje nastaviť typy možných nálezov, ktoré sa majú hlásiť:



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

12.3. Kontrola z prieskumníka

Okrem vopred definovaných kontrol spustených pre celý počítač alebo jeho vybrané oblasti, **AVG Internet Security 2012** 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 2012**

12.4. Kontrola z príkazového riadka

Program **AVG Internet Security 2012** ponúka možnosť spustiť kontrolu z príkazového riadka. Túto funkciu môžete použiť napríklad na serveroch, alebo keď vytvárate dávkový skript, ktorý sa bude spúšťať automaticky po zavedení operačného systému. Príkazový riadok umožňuje spustiť kontrolu s väčšinou parametrov, ktoré sa nachádzajú aj v grafickom používateľskom rozhraní AVG.

Na spustenie kontroly programom AVG z príkazového riadka spustite tento príkaz v priečinku, v ktorom je nainštalovaný program AVG:

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

Syntax príkazu

Toto je syntax príkazového riadka:

- ***avgscanx /parameter*** ... napr. ***avgscanx /comp*** na kontrolu celého počítača

- ***avgscanx /parameter /parameter*** ... Ak použijete niekoľko parametrov, zoraďte ich za sebou a oddeľte ich medzerou a lomkou.

- Ak sa musí uviesť konkrétna hodnota pre parameter (napr. parameter ***/scan***, ktorý si vyžaduje informáciu o tom, ktoré oblasti počítača sa majú kontrolovať, a je potrebné uviesť presnú cestu k vybranej časti), potom sa hodnoty oddelia bodkočiarkou, napríklad: ***avgscanx /scan=C:\;D:***

Parametre kontroly

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

Na spustenie kontroly stlačte kláves ***Enter***. Počas kontroly môžete zastaviť proces stlačením kombinácie klávesov ***Ctrl+C*** alebo ***Ctrl+Pause***.

Kontrola z príkazového riadka spustené z grafického rozhrania

Ak používate operačný systém Windows a počítač je v núdzovom režime, môžete spustiť kontrolu z príkazového riadka z grafického používateľského rozhrania. Samotná kontrola sa spustí z príkazového riadka, dialógové okno ***Command Line Composer*** umožňuje zadať väčšinu parametrov kontroly len pomocou praktického grafického rozhrania.

Keďže sa dá toto dialógové okno otvoriť, len keď je počítač s operačným systémom Windows v núdzovom režime, na zobrazenie podrobných informácií o tomto dialógovom okne použite súbor pomocníka, ktorý sa otvára priamo v dialógovom okne.

12.4.1. Parametre kontroly z príkazového riadka

Nasledujúce je zoznam všetkých parametrov použiteľných pri kontrole z príkazového riadka:

- ***/SCAN*** Kontrola súborov/priečinkov /SCAN=path;path *(napr. /SCAN=C:\;D:\)*
- ***/COMP*** Kontrola celého počítača
- ***/HEUR*** Použiť heuristickú analýzu
- ***/EXCLUDE*** Vylúčiť cestu alebo súbory z kontroly
- ***/@*** Súbor s príkazmi /názov súboru/
- ***/EXT*** Kontrolovať tieto prípony /napríklad EXT=EXE,DLL/
- ***/NOEXT*** Nekontrolovať tieto prípony /napríklad NOEXT=JPG/
- ***/ARC*** Kontrolovať archívy

- ***/CLEAN*** Automaticky vyčistiť
- ***/TRASH*** Premiestniť infikované súbory do Vírusového trezora
- ***/QT*** Rýchly test
- ***/LOG*** Generovať súbor s výsledkami kontroly
- ***/MACROW*** Hlásiť makrá
- ***/PWDW*** Hlásiť súbory chránené heslom
- ***/ARCBOMBSW*** Hlásiť opakovane komprimované archívne súbory
- ***/IGNLOCKED*** Ignorovať zamknuté súbory
- ***/REPORT*** Hlásiť do súboru /názov súboru/
- ***/REPAPPEND*** Pripojiť k súboru so správou
- ***/REPOK*** Označiť neinfikované súbory slovom OK
- ***/NOBREAK*** Nepovoliť prerušenie klávesmi CTRL-BREAK
- ***/BOOT*** Povoliť kontrolu MBR/BOOT
- ***/PROC*** Kontrolovať aktívne procesy
- ***/PUP*** Hlásiť Potenciálne nežiaduce programy
- ***/PUPEXT*** Hlásiť rozšírenú skupinu Potenciálne nežiaducich programov
- ***/REG*** Kontrolovať databázu Registry
- ***/COO*** Kontrolovať súbory cookies
- ***/?*** Zobraziť pomocníka pre túto tému
- ***/HELP*** Zobraziť pomocníka pre túto tému
- ***/PRIORITY*** Nastaviť prioritu kontroly /nízka, automatická, vysoká/ *(pozri časť Rozšírené nastavenia/Kontroly)*
- ***/SHUTDOWN*** Vypnúť počítača po dokončení kontroly
- ***/FORCESHUTDOWN*** Vynútené vypnutie počítača po dokončení kontroly
- ***/ADS*** Kontrolovať alternatívne dátové prúdy *(len pre NTFS)*
- ***/HIDDEN*** Hlásiť súbory so skrytou príponou

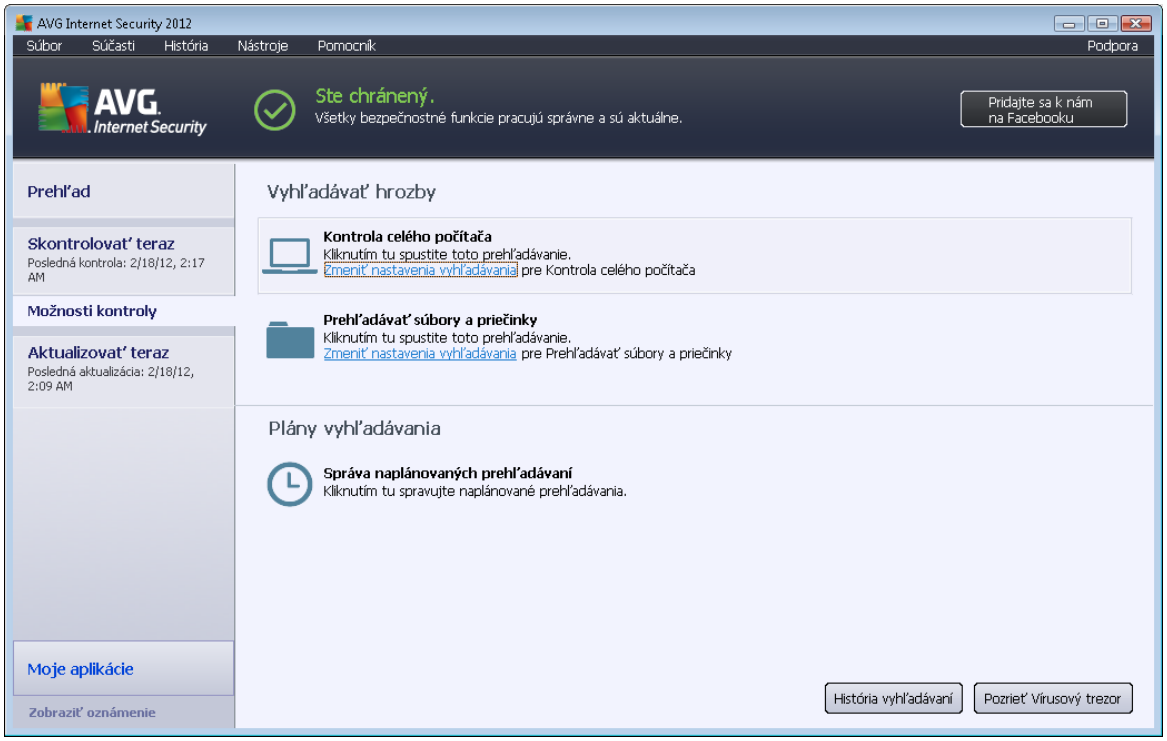
- ***/INFECTABLEONLY*** Kontrolovať len súbory s infikovateľnými príponami
- ***/THOROUGHSCAN*** Zapnúť dôkladnú kontrolu
- ***/CLOUDCHECK*** Kontrola nesprávnych pozitívnych detekcií
- ***/ARCBOMBSW*** Hlásiť opakovane komprimované archivačné súbory

12.5. Plánovanie kontroly

AVG Internet Security 2012 umožňuje spustiť kontrolu na požiadanie (napríklad, keď máte podozrenie, že sa do počítača dostala infekcia) alebo na základe vytvoreného plánu. Odporúčame vám, aby ste spúšťali kontroly podľa plánov: týmto spôsobom sa zabezpečí, že bude počítač chránený pred infikovaním a nebudete si musieť robiť starosti s tým, kedy a či vôbec máte spustiť kontrolu.

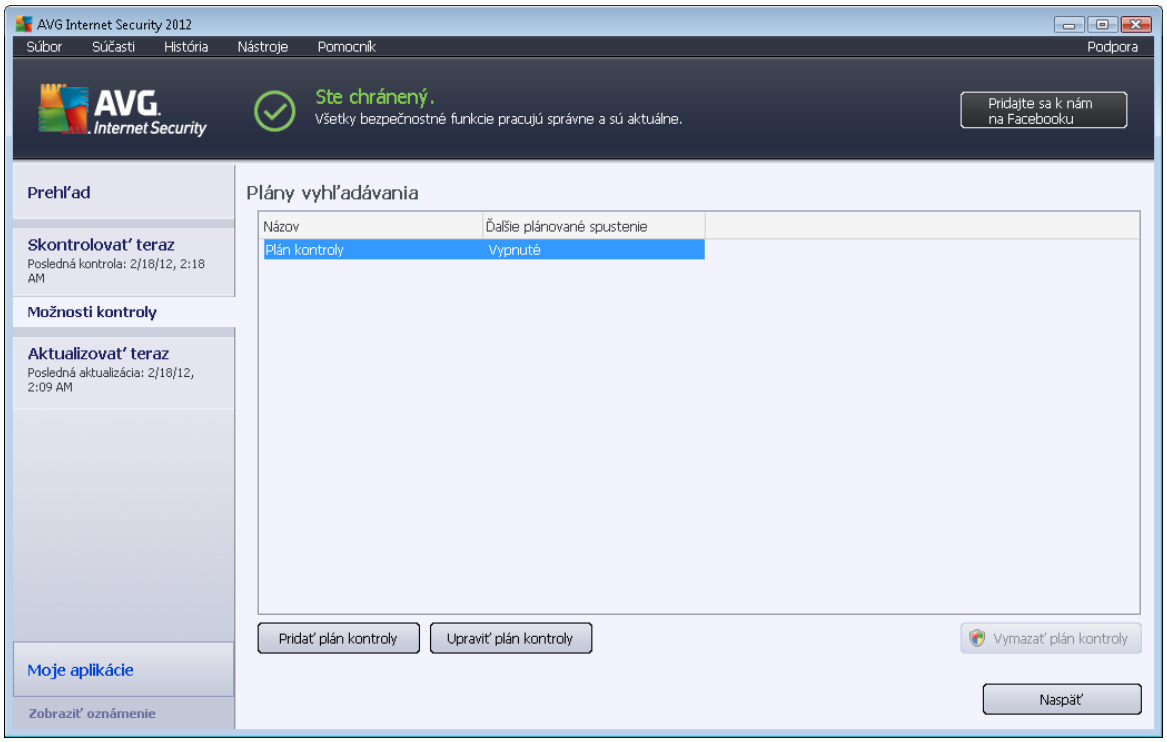
Odporúčame vám, aby ste pravidelne, najmenej raz za týždeň, spustili kontrolu celého počítača. Podľa možností však spúšťajte kontrolu celého počítača každý deň – tak, ako je nastavené v predvolenej konfigurácii plánu kontroly. Ak je počítač „stále zapnutý“, potom môžete naplánovať kontrolu na čas, keď sa počítač nepoužíva. Ak je počítač v tomto čase vypnutý, potom sa zmeškaná naplánovaná kontrola spustí pri spustení počítača.

Ak chcete vytvoriť nový plán kontroly, otvorte rozhranie kontroly programom AVG a prejdite na spodnú časť s názvom ***Naplánovať kontroly***:



Naplánovať kontroly

Kliknutím na grafickú ikonu v časti ***Naplánovať kontroly*** otvorte nové dialógové okno ***Naplánovať kontroly*** so zoznamom všetkých momentálne naplánovaných kontrol.

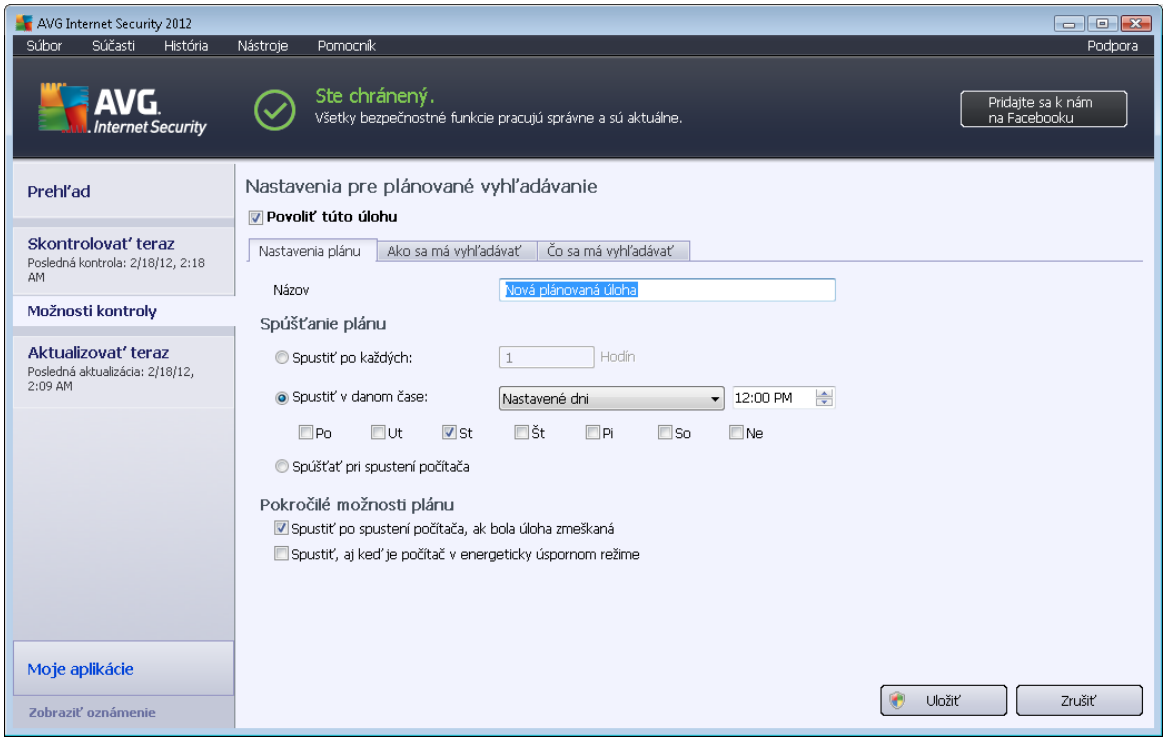


Umožňuje editovať a pridať kontroly pomocou týchto ovládacích tlačidiel:

- ***Pridať plán kontroly*** – toto tlačidlo otvorí dialógové okno ***Nastavenia naplánovanej kontroly***, kartu Nastavenia plánu. V tomto dialógovom okne nastavte parametre novo definovaného testu.
- ***Editovať plán kontroly*** – toto tlačidlo je použiteľné len v prípade, ak ste už predtým vybrali existujúci test v zozname naplánovaných testov. V tom prípade sa tlačidlo použiteľné – kliknutím naň sa otvorí dialógové okno ***Nastavenia plánovanej kontroly***, kartu Nastavenia plánu. Parametre vybraného testu sú tu už nastavené a dajú sa editovať.
- ***Vymazať plán kontroly*** – toto tlačidlo je tiež použiteľné len v prípade, ak ste už predtým vybrali existujúci test v zozname naplánovaných testov. Tento test môžete potom vymazať zo zoznamu stlačením ovládacieho tlačidla. Môžete však odstrániť len vaše vlastné kontroly, ***plán kontroly celého počítača*** nastavený v predvolenej konfigurácii sa nedá nikdy vymazať.
- ***Naspäť*** – návrat na používateľské rozhranie AVG

12.5.1. Nastavenia plánu

Ak si želáte naplánovať nový test a jeho pravidelné spúšťanie, otvorte dialógové okno ***Nastavenia plánovaného testu*** (*kliknite na tlačidlo* ***Pridať plán kontroly*** *v dialógovom okne* ***Naplánovať kontroly***). Toto dialógové okno je rozdelené na tri karty: ***Nastavenia plánu*** *(pozri nasledujúci obrázok, predvolená karta, ktorá sa otvorí automaticky*), Ako kontrolovať a Čo kontrolovať.



Na karte ***Nastavenia plánu*** najskôr začiarknutím alebo zrušením začiarknutia položky ***Povoliť túto úlohu*** jednoducho dočasne vypnite naplánovaný test a znova ho zapnite v prípade potreby.

Potom uveďte názov vytváranej kontroly a plánu. Zadajte názov do textového poľa vedľa položky ***Názov***. Podľa možností použite stručné, opisné a vhodné názvy pre kontroly, aby sa neskôr dali ľahšie rozpoznať medzi ostatnými.

Príklad: *Nie je vhodné nazvať kontrolu „Nová kontrola“ alebo „Moja kontrola“, pretože tieto názvy nesúvisia s tým, čo kontrola vlastne kontroluje. 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 kontrolu vybraných súborov alebo priečinkov, pretože vaša vlastná kontrola bude vždy predstavovať špeciálnu verziu kontroly vybraných súborov alebo priečinkov.*

Toto dialógové umožňuje ďalej definovať tieto parametre kontroly:

- ***Spúšťanie naplánovaných úloh*** – nastavte časové intervaly spúšťania novo naplánovanej kontroly. Čas spúšťania sa definuje ako opakované spúšťanie kontroly po uplynutí určitého času (***Spustiť každých...***), definovaním presného dátumu a času (***Spúšťať v konkrétnom časovom intervale...***), prípadne definovaním udalosti, s ktorou sa bude spájať spustenie kontroly (***Činnosť pri spustení počítača***).

- ***Rozšírené možnosti plánu*** – táto časť sa používa na definovanie podmienok, pri ktorých sa má resp. nemá spustiť kontrola, keď je počítač v úspornom režime alebo úplne vypnutý.

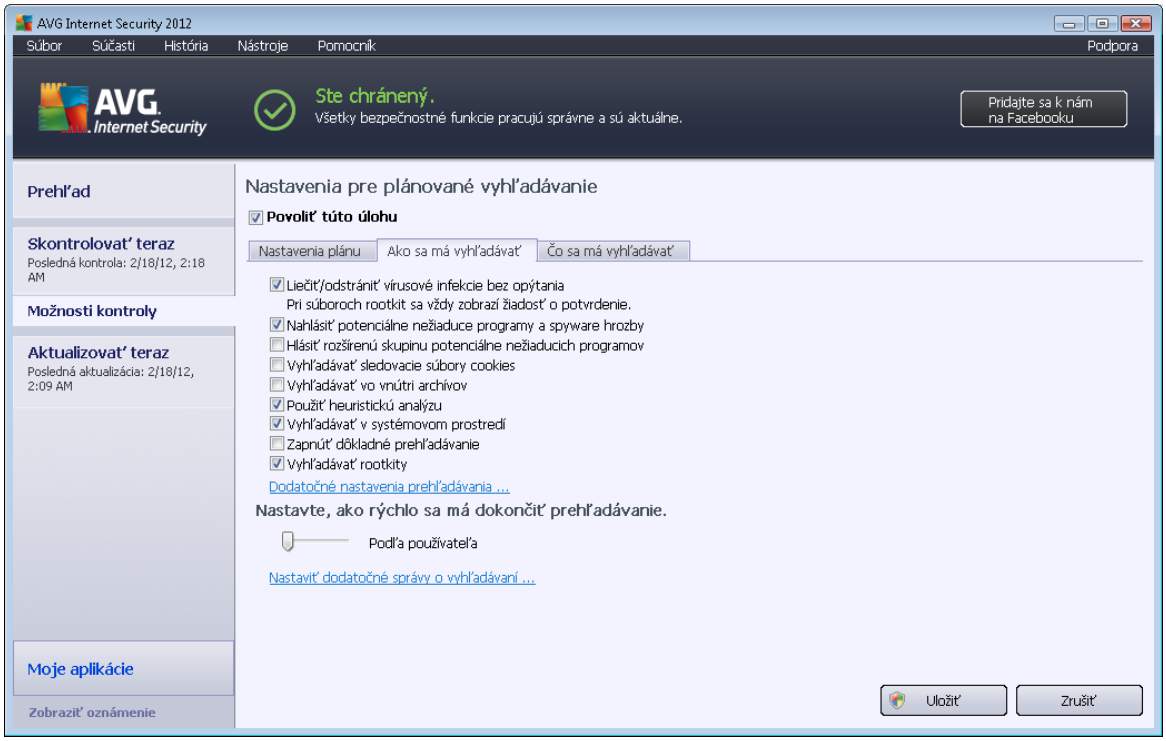
Ovládacie tlačidlá dialógového okna Nastavenia plánovanej kontroly

Na všetkých troch kartách dialógového okna ***Nastavenia naplánovanej kontroly*** *(Nastavenia plánu, Ako kontrolovať a Čo kontrolovať)* sa nachádzajú dve ovládacie tlačidlá, ktoré majú rovnakú funkciu bez ohľadu na to, ktorá karta je práve otvorená:

- ***Uložiť*** – uloží všetky zmeny, ktoré ste urobili na tejto karte alebo na inej karte tohto dialógového okna a prepne naspäť na hlavné dialógové okno s rozhraním kontroly programom AVG. Preto, ak chcete nastaviť parametre testu na všetkých kartách, stlačením tohto tlačidla ich uložte až po nastavení všetkých potrebných možností.

- ***Zrušiť*** – zruší všetky zmeny, ktoré ste urobili na tejto karte alebo na inej karte tohto dialógového okna a prepne naspäť na hlavné dialógové okno s rozhraním kontroly programom AVG.

12.5.2. Ako kontrolovať



Na karte ***Ako kontrolovať*** sa nachádza zoznam parametrov kontroly, ktoré sa dajú zapnúť resp. vypnúť. Štandardne je väčšina parametrov zapnutá a príslušná funkcia sa použije počas kontroly. Ak nemáte vážny dôvod meniť tieto nastavenia, potom vám odporúčame, aby ste zachovali prednastavenú konfiguráciu:

- ***Liečiť/odstrániť vírusovú infekciu bez opýtania*** (*štandardne zapnuté*): ak sa počas kontroly nájde vírus, môže byť automaticky vyliečený, pokiaľ je liek k dispozícii. Ak sa infikované súbory nedajú vyliečiť automaticky, alebo keď sa rozhodnete vypnúť túto funkciu, potom sa po detekcii vírusu zobrazí upozornenie a budete musieť rozhodnúť, čo sa má urobiť s detekovanou infekciou. Odporúčame vám, aby ste infikovaný súbor odstránili do Vírusového trezora.

- ***Hlásiť potenciálne nežiaduce programy a hrozby spyware*** (*štandardne zapnuté*):

začiarknite toto okienko, ak chcete zapnúť súčasť Anti-Spyware a kontrolovať spyware a vírusy. Spyware predstavuje pochybnú kategóriu škodlivého softvéru: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.

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

- ***Kontrolovať sledovacie súbory cookies*** (*štandardne vypnuté*): tento parameter súčasti Anti-Spyware zapína funkciu na zisťovanie prítomnosti súborov cookies počas kontroly (*HTTP cookies sa používajú na overenie totožnosti, sledovanie a správu konkrétnych informácií o používateľoch, ako sú preferencie stránok alebo obsah elektronických nákupných košíkov*).

- ***Kontrolovať v archívoch*** (*štandardne vypnuté*): tieto parametre určujú, že sa majú počas kontroly overovať všetky súbory, aj keď sú zabalené vo vnútri určitých typov archívov, ako sú ZIP, RAR...

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

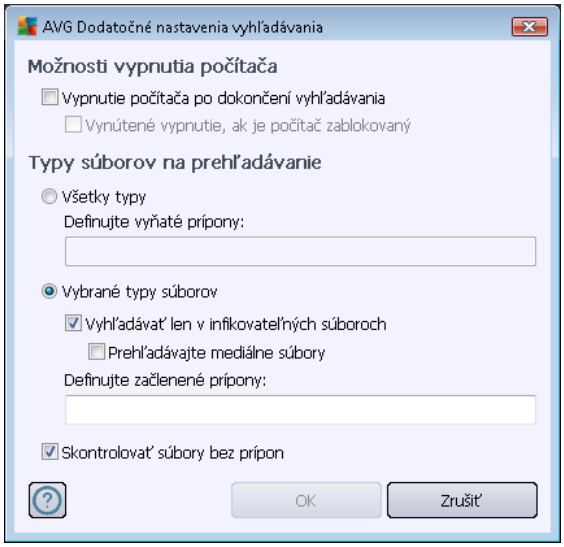
- ***Kontrolovať systémové prostredie*** (*štandardne zapnuté*): počas kontroly sa budú overovať aj systémové oblasti počítača.

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

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

Potom môžete zmeniť konfiguráciu kontroly podľa tohto postupu:

- ***Ďalšie nastavenia kontroly*** – tento odkaz otvorí nové dialógové okno ***Ďalšie nastavenia kontroly*** ktoré sa používa na nastavenie týchto 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 zamknutý (***Vynútené vypnutie počítača, keď je zamknutý***).

- ***Typy súborov na kontrolu*** – Ďalej môžete rozhodnúť, či sa majú kontrolovať:

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

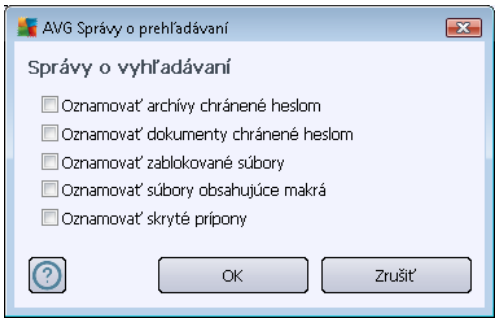
  - ***Vybrané typy súborov*** – môžete nastaviť, aby sa kontrolovali len súbory, pri ktorých existuje pravdepodobnosť infikovania (*súbory, ktoré nemôžu byť napadnuté infekciou, napríklad niektoré jednoduché textové súbory alebo niektoré nespustiteľné súbory*), vrátane mediálnych súborov (*video, audio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

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

- ***Nastaviť rýchlosť dokončenia kontroly*** – pomocou posúvača zmeňte prioritu procesu kontroly. Štandardne má tento parameter nastavenú úroveň automatického využívania zdrojov „*podľa používateľa*“. Prípadne môžete spustiť procesy kontroly pomalšie, čím sa minimalizuje využívanie počítačových zdrojov (*toto nastavenie je užitočné vtedy, ak potrebujete pracovať na počítači, ale nezaujíma vás, ako dlho bude kontrola trvať*), alebo rýchlejšie s vyššími nárokmi na využívanie počítačových zdrojov (*napr. keď sa počítač dočasne nepoužíva*).

- ***Vytvoriť ďalšie správy o kontrole*** – odkaz otvorí nové dialógové okno ***Správy o kontrole***,

v ktorom môžete určiť, aké typy možných nálezov sa majú uviesť v správach:



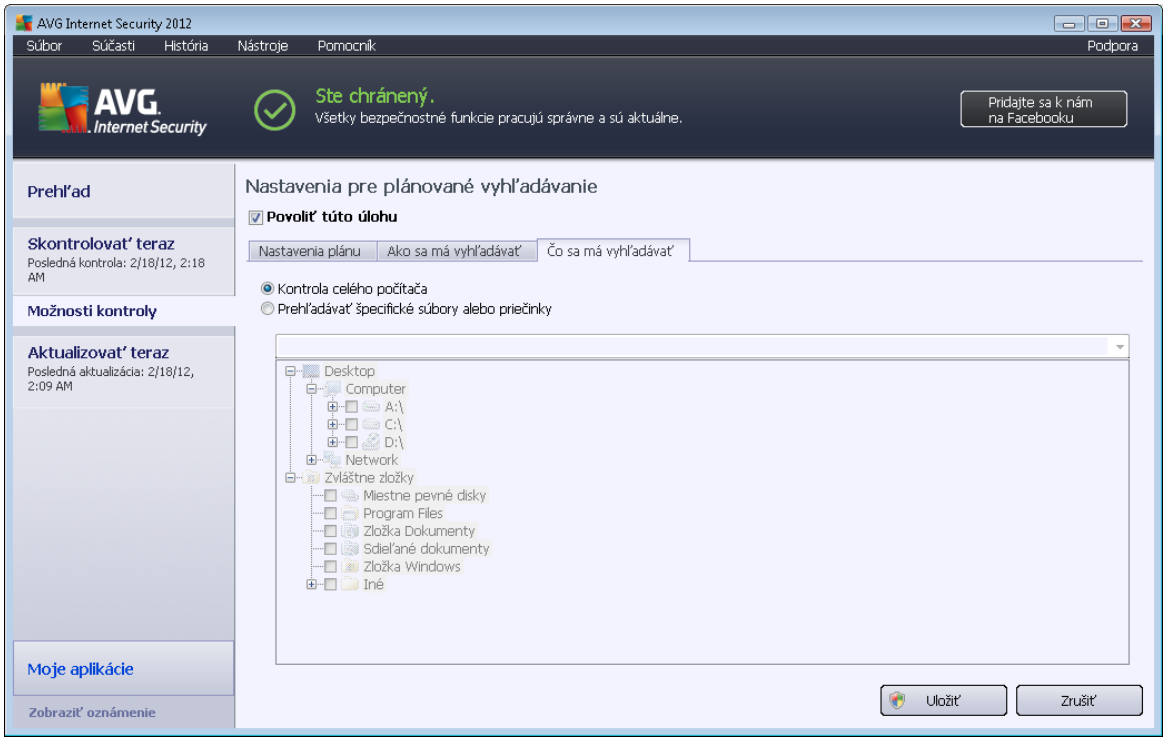
Ovládacie tlačidlá

Na všetkých troch kartách dialógového okna ***Nastavenia naplánovanej kontroly*** (*Nastavenia plánu*, *Ako kontrolovať* a *Čo kontrolovať*) sa nachádzajú dve ovládacie tlačidlá, ktoré majú rovnakú funkciu bez ohľadu na to, ktorá karta je práve otvorená:

- ***Uložiť*** – uloží všetky zmeny, ktoré ste urobili na tejto karte alebo na inej karte tohto dialógového okna a prepne naspäť na hlavné dialógové okno s rozhraním kontroly programom AVG. Preto, ak chcete nastaviť parametre testu na všetkých kartách, stlačením tohto tlačidla ich uložte až po nastavení všetkých potrebných možností.

- ***Zrušiť*** – zruší všetky zmeny, ktoré ste urobili na tejto karte alebo na inej karte tohto dialógového okna a prepne naspäť na hlavné dialógové okno s rozhraním kontroly programom AVG.

12.5.3. Čo kontrolovať



Na karte ***Čo kontrolovať*** môžete nastaviť, či chcete naplánovať kontrolu celého počítača alebo kontrolu vybraných súborov alebo priečinkov.

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

V stromovej štruktúre môžete zároveň vyhľadať vetvu s názvom ***Špeciálne umiestnenia***. Toto je zoznam umiestnení, ktoré sa skontrolujú po začiarknutí príslušného začiarkovacieho okienka:

- ***Pevné disky počítača*** – všetky pevné disky počítača
- ***Programové súbory***
  - C:\Program Files\
  - *v 64-bitovej verzii* C:\Program Files (x86)
- ***Priečinok Moje dokumenty***

- *vo Win XP:* C:\Documents and Settings\Default User\Moje dokumenty\
- *vo Windows Vista/7*: C:\Users\používateľ\Dokumenty\

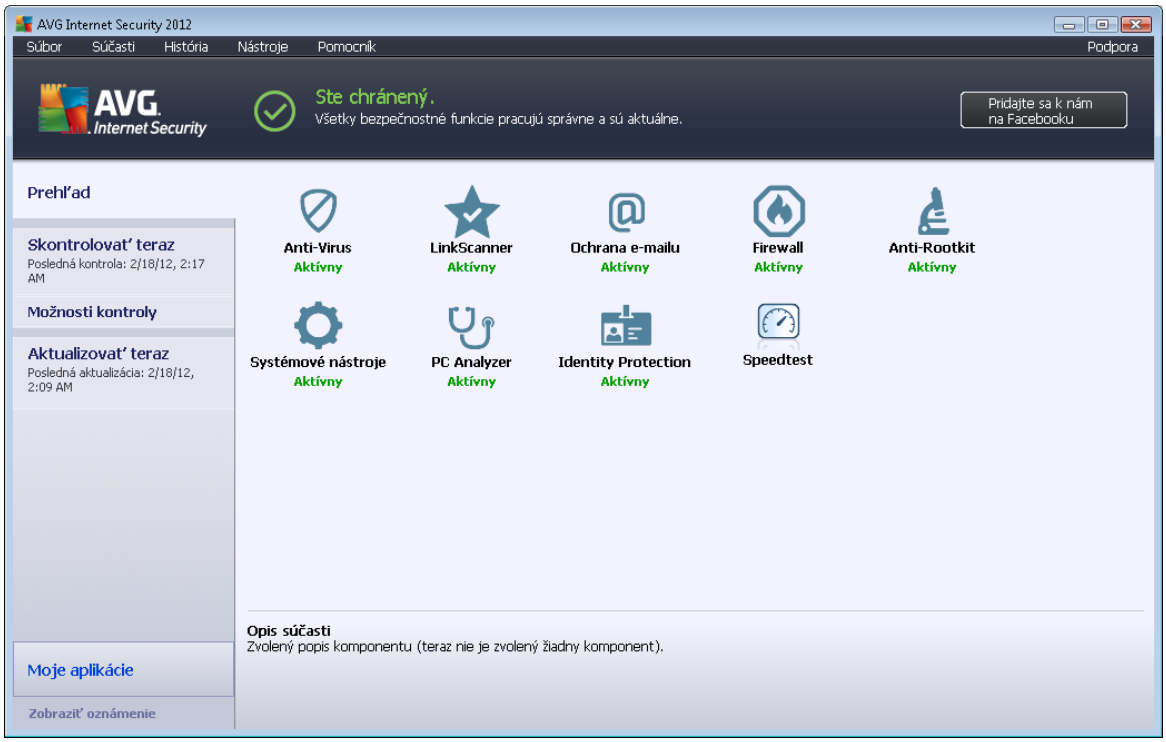
- ***Zdieľané dokumenty***
  - *vo Win XP*: C:\Documents and Settings\All Users\Dokumenty\
  - *vo Windows Vista/7*: C:\Users\Public\Dokumenty\
- ***Adresár Windows*** – C:\Windows\
- ***Iné***
  - *Systémový disk* – pevný disk, na ktorom je nainštalovaný operačný systém (zvyčajne C:).
  - *Systémový priečinok* – C:\Windows\System32\
  - *Priečinok Temporary Files* – C:\Documents and Settings\User\Local\ (*Windows XP*) alebo C:\Users\používateľ\AppData\Local\Temp\ (*Windows Vista/7*)
  - *Temporary Internet Files* – C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (*Windows XP*) alebo C: \Users\používateľ\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

Ovládacie tlačidlá

Na všetkých troch kartách dialógového okna ***Nastavenia plánovaných kontrol*** *(Nastavenia plánu, Ako kontrolovať a Čo kontrolovať) sa nachádzajú dve rovnaké ovládacie tlačidlá*:

- ***Uložiť*** – uloží všetky zmeny, ktoré ste urobili na tejto karte alebo na inej karte tohto dialógového okna a prepne naspäť na hlavné dialógové okno s rozhraním kontroly programom AVG. Preto, ak chcete nastaviť parametre testu na všetkých kartách, stlačením tohto tlačidla ich uložte až po nastavení všetkých potrebných možností.
- ***Zrušiť*** – zruší všetky zmeny, ktoré ste urobili na tejto karte alebo na inej karte tohto dialógového okna a prepne naspäť na hlavné dialógové okno s rozhraním kontroly programom AVG.

12.6. Prehľad výsledkov kontroly



Dialógové okno ***Prehľad výsledkov prehľadávania*** sa otvára v rozhraní prehľadávania programom AVG pomocou tlačidla ***História prehľadávaní***. V dialógovom okne sa nachádza zoznam všetkých doposiaľ spustených prehľadávaní a informácie o ich výsledkoch:

- ***Názov***: Označenie vyhľadávania; buď môže ísť o názov niektorého z vopred definovaných prehľadávaní alebo o názov, ktorý ste priradilo vlastnému naplánovanému prehľadávaniu. Každý názov obsahuje ikonu označujúcu výsledok prehľadávania:

  – Zelená ikona informuje, že počas prehľadávania nebola detekovaná žiadna infekcia.

  – Modrá ikona informuje, že počas prehľadávania bola detekovaná infekcia, ale infikovaný objekt bol automaticky odstránený.

  – Červená ikona upozorňuje, že počas prehľadávania bola detekovaná infekcia, ktorá sa nedala odstrániť!

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

  Poznámka: *Podrobné informácie o každom prehľadávaní sa nachádzajú v dialógovom okne Výsledky prehľadávania, ktoré sa otvára pomocou tlačidla Zobraziť podrobnosti (v spodnej časti tohto dialógového okna).*

- ***Čas spustenia***: Dátum a čas, kedy bolo prehľadávanie spustené.
- ***Čas skončenia***: Dátum a čas, kedy sa prehľadávanie skončilo.
- ***Testované objekty***: Počet objektov, ktoré sa skontrolovali počas prehľadávania.
- ***Infekcie***: Počet detekovaných/odstránených vírusových infekcií
- ***Spyware***: Počet detekovaných/odstránených programov typu spyware
- ***Upozornenia***: Počet detekovaných podozrivých objektov
- ***Rootkity***: Počet detekovaných rootkitov
- ***Informácie záznamového protokolu prehľadávania***: Informácie súvisiace s priebehom a výsledkami prehľadávania (obyčajne s jeho dokončením alebo prerušením).

Ovládacie tlačidlá

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

- ***Zobraziť podrobnosti***: Stlačením tohto tlačidla sa otvorí dialógové okno Výsledky prehľadávania s podrobnými informáciami o zvolenom prehľadávaní.
- ***Vymazať výsledky***: Stlačením tohto tlačidla sa zvolená položka odstráni z prehľadu výsledkov prehľadávania.
- ***Naspäť***: Prepne naspäť na hlavné dialógové okno rozhrania prehľadávania programom AVG

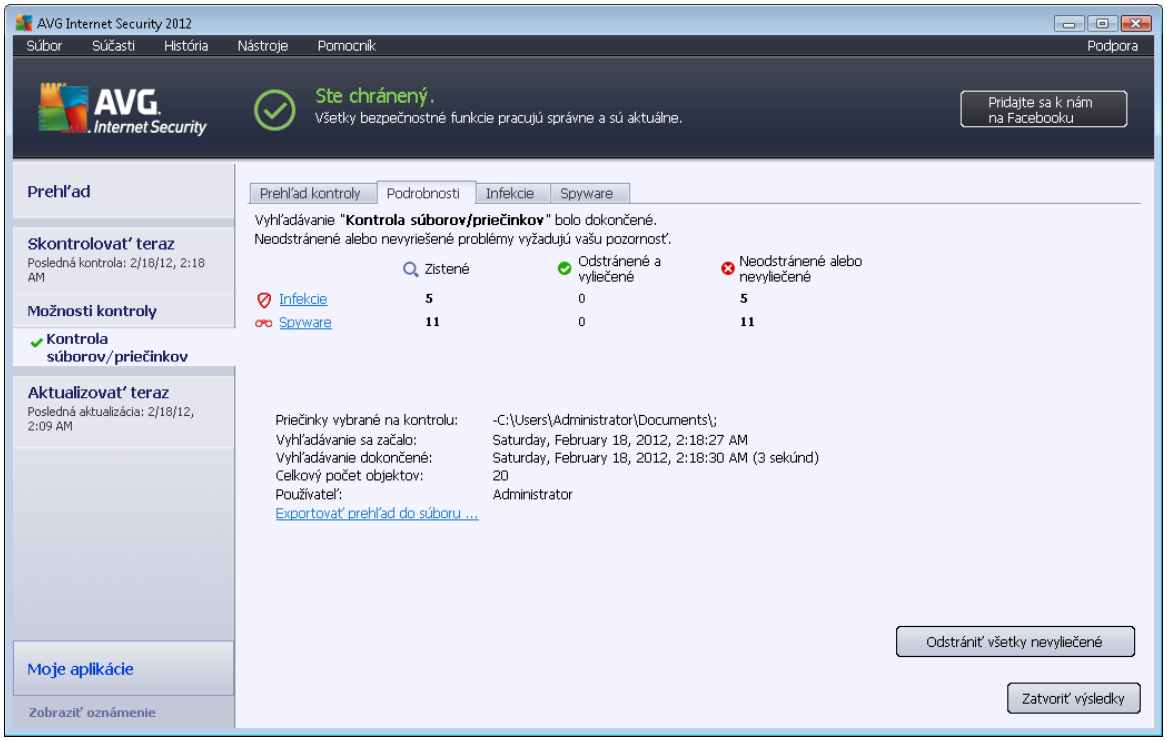
12.7. Podrobné výsledky kontroly

Ak v dialógovom okne Prehľad výsledkov kontroly zvolíte konkrétnu kontrolu, môžete kliknutím na tlačidlo ***Zobraziť podrobnosti*** otvoriť dialógové okno ***Výsledky kontroly*** s podrobnými informáciami o priebehu a výsledkoch zvolenej kontroly. Toto dialógové okno je rozdelené na niekoľko kariet:

- Prehľad výsledkov: Táto karta sa tu nachádza vždy a poskytuje štatistické informácie o priebehu kontroly.
- Infekcie: Táto karta sa tu nachádza len vtedy, ak sa počas kontroly zistila vírusová infekcia
- Spyware: Táto karta sa tu nachádza len vtedy, ak sa počas kontroly zistil spyware
- Upozornenia: Táto karta sa tu nachádza len vtedy, ak sa počas kontroly zistili súbory cookies.
- Rootkit: Táto karta sa tu nachádza len vtedy, ak sa počas kontroly zistili programy rootkit
- Informácie: Táto karta sa tu nachádza len vtedy, ak sa zistili niektoré potenciálne hrozby, ktoré sa však nedajú zaradiť do žiadnej z uvedených kategórií; na karte sa potom zobrazí

upozornenie súvisiace s nálezom. Nachádzajú sa tu aj informácie o objektoch, ktoré nie je možné skontrolovať *(napr. archívy chránené pomocou hesla)*.

12.7.1. Karta Prehľad výsledkov



V karte ***Výsledky vyhľadávania*** môžete nájsť podobnú štatistiku s informáciami o:

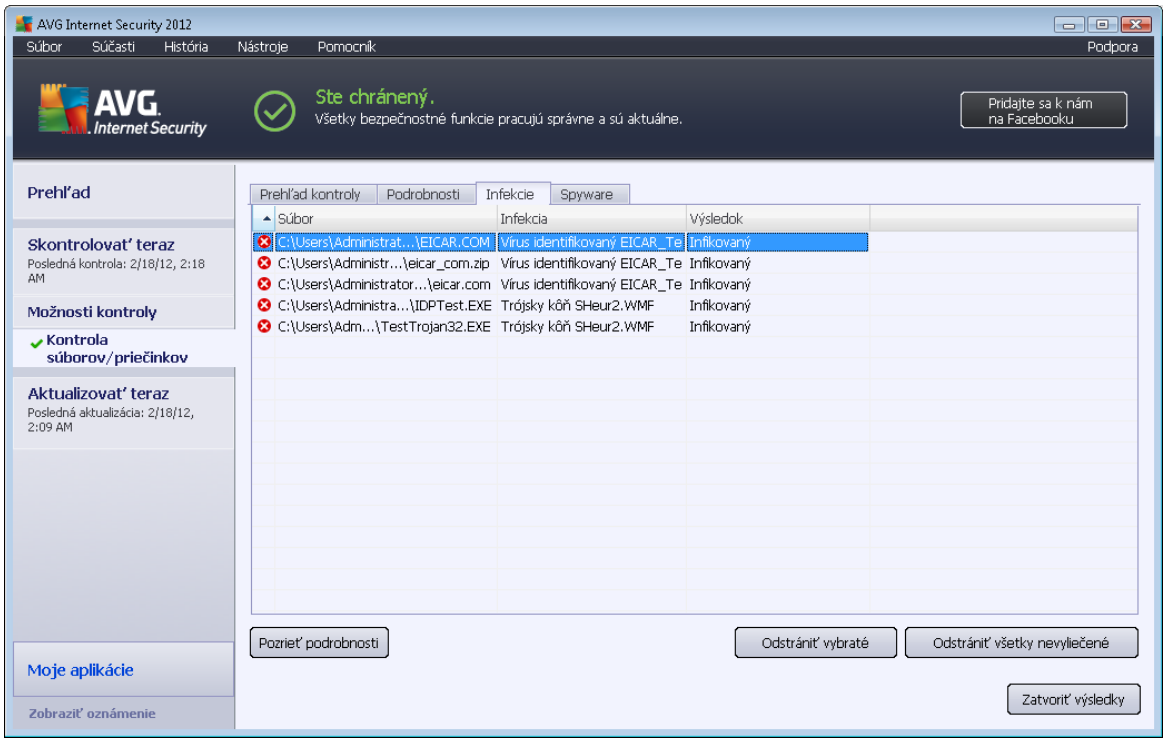
- zistených vírusových infekciách/spyware,
- odstránených vírusových infekciách/spyware,
- počte vírusových infekcií/spyware, ktoré sa nedajú odstrániť alebo vyliečiť.

Okrem toho nájdete informácie o dátume a presnom čase spustenia kontroly, o celkovom počte skontrolovaných objektov, o trvaní vyhľadávania a o počte chýb, ktoré sa vyskytli počas vyhľadávania.

Ovládacie tlačidlá

V tomto dialógovom okne je dostupné len jedno ovládacie tlačidlo. Tlačidlo ***Naspäť*** sa vráti do dialógového okna Prehľad výsledkov vyhľadávania.

12.7.2. Karta Infekcie



Karta ***Infekcie*** sa nachádza v dialógovom okne ***Výsledky kontroly*** len v prípade, ak sa počas kontroly detekovala vírusová infekcia. Táto karta je rozdelená na tri časti, na ktorých sa nachádzajú tieto informácie:

- ***Súbor*** – úplná cesta k pôvodnému umiestneniu infikovaného objektu.
- ***Infekcie*** – názov detekovaného vírusu (*podrobnosti o konkrétnych vírusoch sa nachádzajú online vo Vírusovej encyklopédii*).
- ***Výsledok*** – informuje o momentálnom stave infikovaného objektu, ktorý sa detekoval počas kontroly:
    - ***Infikovaný*** – infikovaný objekt bol detekovaný a ponechal sa na pôvodnom mieste (*napríklad ak ste vypli funkciu na automatické liečenie v nastavení konkrétnej kontroly*).
    - ***Vyliečený*** – infikovaný objekt sa automaticky vyliečil a ponechal na pôvodnom mieste.
    - ***Premiestnený do Vírusového trezora*** – infikovaný objekt sa premiestnil do karantény vo Vírusovom trezore
    - ***Vymazaný*** – infikovaný objekt sa vymazal.
    - ***Pridaný k výnimkám PUP*** – nález bol zhodnotený ako výnimka a pridaný do

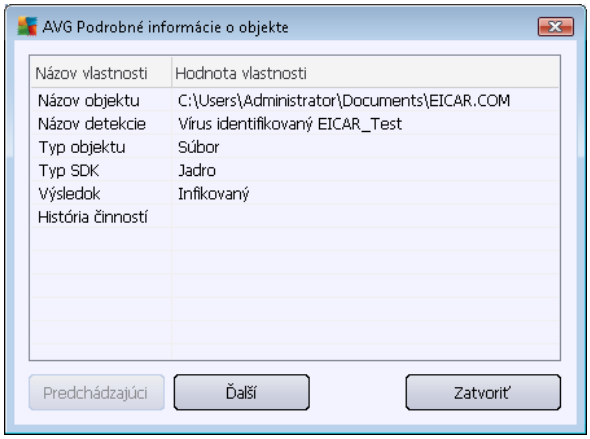
zoznamu výnimiek PUP *(konfigurovaný v dialógovom okne Výnimky PUP pokročilých nastavení)*

- ***Zamknutý súbor – netestovaný*** – príslušný objekt je zamknutý a program AVG ho preto nedokáže skontrolovať.
- ***Potenciálne nebezpečný objekt*** – objekt bol označený ako potenciálne nebezpečný, nie však infikovaný (*môže obsahovať napríklad makrá*); informáciu považujte len za upozornenie.
- ***Vyžaduje sa reštart na dokončenie akcie*** – infikovaný objekt sa nedá odstrániť, na jeho úplné odstránenie musíte reštartovať počítač

Ovládacie tlačidlá

V tomto dialógovom okne sa nachádzajú tri ovládacie tlačidlá:

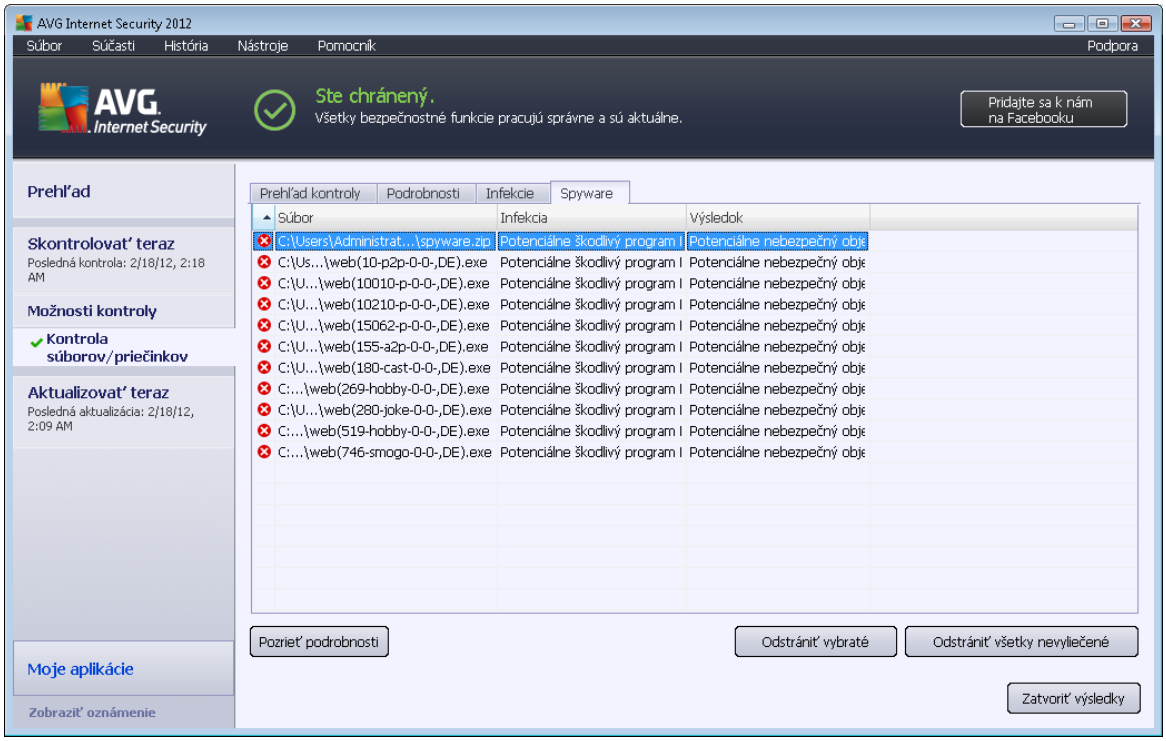
- ***Zobraziť podrobnosti*** – toto tlačidlo otvorí nové dialógové okno s názvom ***Podrobné informácie o objekte***:



V tomto dialógovom okne sa nachádzajú podrobné informácie o detekovanom infikovanom objekte (*napr. názov a umiestnenie infikovaného objektu, typ objektu, typ SDK, výsledky detekcie a história akcií súvisiacich s detekovaným objektom*). Tlačidlá ***Predchádzajúce***/***Ďalšie*** sa používajú na zobrazenie informácií o konkrétnych nálezoch. Tlačidlo ***Zatvoriť*** sa používa na zatvorenie tohto dialógového okna.

- ***Odstrániť vybrané*** – toto tlačidlo sa používa na premiestnenie vyberaného nálezu do Vírusového trezora
- ***Odstrániť všetky nevyliečené*** – toto tlačidlo vymaže všetky nálezy, ktoré sa nedajú vyliečiť alebo premiestniť do Vírusového trezora
- ***Zatvoriť výsledky*** – zatvorí prehľad a otvorí pôvodné dialógové okno Prehľad výsledkov kontroly.

12.7.3. Karta Spyware



Karta ***Spyware*** sa nachádza v dialógovom okne ***Výsledky kontroly***, len ak sa počas kontroly zistil spyware. Táto karta je rozdelená na tri časti, na ktorých sa nachádzajú tieto informácie:

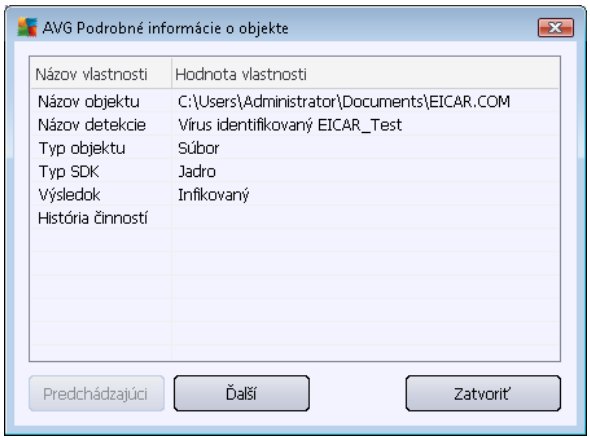
- ***Súbor*** – úplná cesta k pôvodnému umiestneniu infikovaného objektu.
- ***Infekcie*** – Názov zisteného spywaru *(podrobnosti o konkrétnych vírusoch sa nachádzajú v on-line Encyklopédii vírusov)*
- ***Výsledok*** – Informuje o momentálnom stave infikovaného objektu, ktorý sa zistil počas kontroly:
    - ***Infikovaný*** – *Zistený infikovaný objekt sa ponechal na pôvodnom mieste (napríklad ak ste vypli automatické liečenie v nastavení konkrétnej kontroly).*
    - ***Vyliečený*** – Infikovaný objekt sa automaticky vyliečil a ponechal na pôvodnom mieste.
    - ***Premiestnený do vírusového trezora*** – Infikovaný objekt sa premiestnil do karantény vo vírusovom trezore.
    - ***Odstránený*** – Infikovaný objekt sa odstránil.
    - ***Pridaný k výnimkám PUP*** – Nález bol vyhodnotený ako výnimka a pridaný do zoznamu výnimiek PUP *(konfigurovaný v dialógovom okne Výnimky PUP rozšírených nastavení).*

- ***Zamknutý súbor – netestovaný*** – príslušný objekt je zamknutý a program AVG ho preto nedokáže skontrolovať.
- ***Potenciálne nebezpečný objekt*** – objekt bol označený ako potenciálne nebezpečný, nie však infikovaný (môže obsahovať napríklad makrá); informácie považujte len za upozornenie.
- ***Vyžaduje sa reštart na dokončenie akcie*** – infikovaný objekt sa nedá odstrániť, na jeho úplné odstránenie musíte reštartovať počítač

Ovládacie tlačidlá

V tomto dialógovom okne sa nachádzajú tri ovládacie tlačidlá:

- ***Zobraziť podrobnosti*** – toto tlačidlo otvorí nové dialógové okno s názvom ***Podrobné informácie o objekte***:



  V tomto dialógovom okne sa nachádzajú podrobné informácie o detekovanom infikovanom objekte (*napr. názov a umiestnenie infikovaného objektu, typ objektu, typ SDK, výsledky detekcie a história akcií súvisiacich s detekovaným objektom*). Tlačidlá ***Predchádzajúce***/***Ďalšie*** sa používajú na zobrazenie informácií o konkrétnych nálezoch. Pomocou tlačidla ***Zatvoriť*** zatvorte toto dialógové okno.

- ***Odstrániť vybrané*** – toto tlačidlo sa používa na premiestnenie vyberaného nálezu do Vírusového trezora
- ***Odstrániť všetky nevyliečené*** – toto tlačidlo vymaže všetky nálezy, ktoré sa nedajú vyliečiť alebo premiestniť do Vírusového trezora
- ***Zatvoriť výsledky*** – Zatvorí podrobný prehľad a otvorí pôvodné dialógové okno Prehľad výsledkov kontroly.

12.7.4. Karta Upozornenia

Karta ***Varovania*** zobrazuje informácie o "podozrivých" objektoch (*obyčajne súboroch*) detekovaných počas vyhľadávania. Po detekcii súčasťou Resident Shield sa tieto súbory zablokujú, aby k nim nebol možný prístup. Typické príklady týchto druhov nálezov sú: skryté súbory, cookies, podozrivé kľúče registrov, heslom chránené dokumenty alebo archívy, atď. Tieto súbory nepredstavujú priamu hrozbu pre váš počítač ani bezpečnostnú hrozbu. Informácie o týchto súboroch majú význam hlavne v prípade, ak sa zistí prítomnosť škodlivého softvéru typu adware alebo spyware v počítači. Ak výsledky testu obsahujú iba varovania aplikácie **AVG Internet Security 2012**, nie je potrebná žiadna činnosť.

Toto je stručný popis najbežnejších príkladov takýchto objektov:

- ***Skryté súbory*** – skryté súbory sú štandardne neviditeľné v operačnom systéme Windows a niektoré vírusy alebo iné hrozby sa môžu pokúsiť vyhnúť detekovaniu tým, že svoje súbory uložia s týmto atribútom. Ak program **AVG Internet Security 2012** nájde skrytý súbor a máte podozrenie, že je škodlivý, môžete ho premiestniť do vírusového trezora.
- ***Cookies*** – cookies sú jednoduché textové súbory, ktoré používajú webové stránky na ukladanie špecifických informácií o používateľovi, ktoré sa neskôr použijú na načítanie vlastného rozloženia webovej stránky, automatické vyplnenie mena používateľa a pod.
- ***Podozrivé kľúče registrov*** – niektorý škodlivý softvér ukladá svoje informácie do registrov operačného systému Windows, aby sa zabezpečilo jeho načítanie pri spustení operačného systému, alebo rozšíril jeho vplyv v operačnom systéme.

12.7.5. Karta Rootkity

Na karte ***Rootkity*** sa nachádzajú informácie o rootkitoch detegovaných počas kontroly súčasťou Anti-Rootkit v rámci Kontroly celého počítača.

Rootkit je program, ktorého cieľom je zmocniť sa základnej kontroly nad počítačom bez súhlasu vlastníka počítača a jeho legitímnych správcov. Prístup k hardvéru sa väčšinou nepožaduje, pretože účelom rootkitu je zmocniť sa kontroly nad operačným systémom spusteným na hardvéri. Rootkity zvyčajne maskujú svoju prítomnosť v systéme rozvratnou činnosťou, alebo vyhýbaním sa štandardným bezpečnostným mechanizmom operačného systému. Často ide aj o trójske kone, ktoré klamlivo presvedčia používateľov, že sa môžu bezpečne spustiť na počítači. Medzi metódy používané na dosiahnutie tohto cieľa patria utajenie spustených procesov pred sledovacími programami, alebo skrývanie súborov alebo systémových dát pred operačným systémom.

Štruktúra tejto karty je v podstate zhodná so štruktúrou karty Infekcie a karty Spyware.

12.7.6. Karta Informácie

Karta ***Informácie*** obsahuje údaje o takýchto "nálezoch" , ktoré sa nedajú hodnotiť ako infekcie, spyware, atď. Nedajú sa pozitívne označiť ako nebezpečné, zasluhujú si však vašu pozornosť. Aplikácia **AVG Internet Security 2012** dokáže pri kontrole zisťovať súbory, ktoré nemusia byť infikované, ale sú podozrivé. Informácie o týchto súboroch sa zobrazia buď ako Upozornenie alebo ako Informácia.

Informácia o závažnosti sa zobrazí pri výskyte ktorejkoľvek z nasledujúcich udalostí:

- ***Komprimovaný za chodu*** – Súbor bol komprimovaný jedným z menej bežne používaných komprimačných programov, čo môže naznačovať pokus o zabránenie kontrole tohto súboru. Nie každá takáto informácia však znamená výskyt vírusu.

- ***Komprimovaný za chodu rekurzívny*** – Podobné ako predchádzajúce, ale súbor bol komprimovaný menej často používaným softvérom spomedzi bežných programov. Tieto súbory sú podozrivé a je potrebné zvážiť možnosť odstrániť alebo poslať ich na analýzu.

- ***Archív alebo dokument chránený pomocou hesla*** – Aplikácia **AVG Internet Security 2012** nedokáže kontrolovať súbory chránené pomocou hesla (*v podstate žiadny program na zisťovanie malware*).

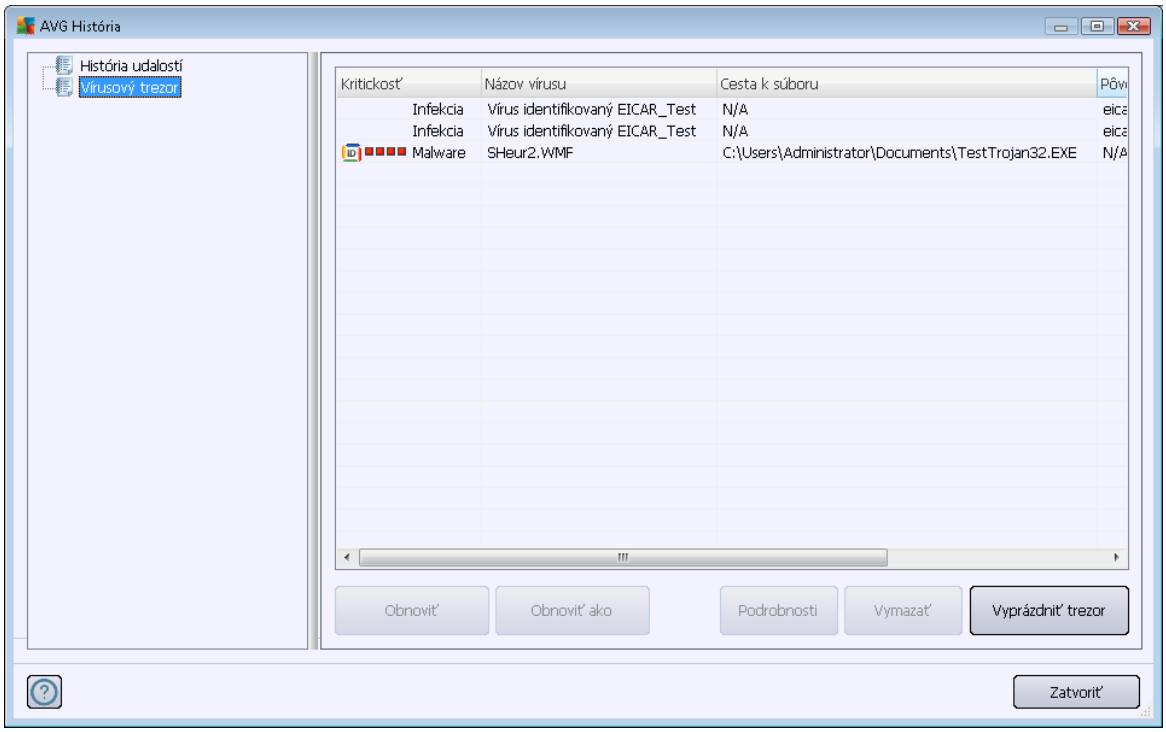
- ***Dokument obsahujúci makrá*** – Nahlásený dokument obsahuje makrá, ktoré môžu byť škodlivé.

- ***Skrytá prípona*** – Súbory so skrytou príponou sa môžu javiť napr. ako obrázky, ale v skutočnosti predstavujú spustiteľné súbory (*napr. obrazok.jpg.exe*). Druhá prípona nie je pri štandardnom nastavení operačného systému Windows viditeľná a program **AVG Internet Security 2012** upozorní na tieto súbory, aby zabránil ich náhodnému otvoreniu.

- ***Nesprávna cesta k súboru*** – Ak sa niektorý dôležitý systémový súbor spustí z iného ako štandardného umiestnenia (*napr. súbor winlogon.exe spustený z iného priečinka ako Windows*), program na túto nezrovnalosť upozorní. **AVG Internet Security 2012** V niektorých prípadoch vírusy používajú názvy štandardných systémových procesov, aby ich prítomnosť v systéme bola menej nápadná.

- ***Zamknutý súbor*** – Identifikovaný súbor je zamknutý, preto ho aplikácia **AVG Internet Security 2012** nemôže skontrolovať. Spravidla to znamená, že určitý súbor je neustále používaný systémom (*napr. swapový súbor*).

12.8. Vírusový trezor



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

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

- ***Úroveň závažnosti***: Ak sa rozhodnete nainštalovať súčasť Identity Protection do programu **AVG Internet Security 2012**, v tejto časti sa bude nachádzať grafické znázornenie úrovne závažnosti zisteného nálezu na stupnici so štyrmi úrovňami, od vyhovujúcej (■□□□) až po veľmi nebezpečnú (■■■■); a informácie o type infekcie (*na základe úrovne infikovateľnosti – všetky uvedené objekty môžu byť pozitívne alebo potenciálne infikované*).

- ***Názov vírusu*** – uvádza názov detekovanej infekcie podľa Encyklopédie vírusov *(online)*

- ***Cesta k súboru*** – úplná cestá k pôvodnému umiestneniu detekovaného infikovaného súboru.

- ***Pôvodný názov objektu*** – všetky detekované objekty uvedené v tabuľke boli označené štandardným názvom prideleným programom AVG počas procesu kontroly. Ak mal objekt

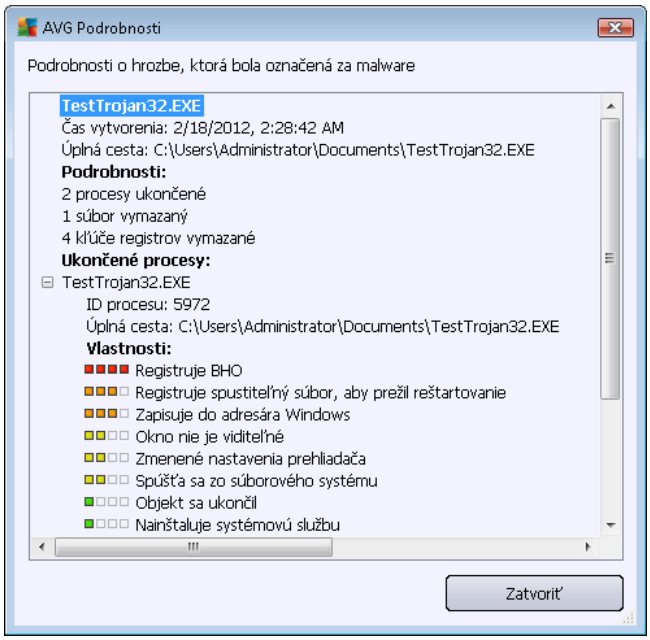
pridelený konkrétny pôvodný názov, ktorý je známy (*napr. názov prílohy e-mailu, ktorý nezodpovedá skutočnému obsahu prílohy*), bude uvedený v tomto stĺpci.

- ***Dátum uloženia*** – dátum a čas, kedy bol podozrivý súbor detekovaný a premiestnený do Vírusového trezora

Ovládacie tlačidlá

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

- ***Obnoviť*** – premiestni infikovaný súbor naspäť do pôvodného umiestnenia na disku.
- ***Obnoviť ako*** – premiestni infikovaný súbor do vybraného priečinka
- ***Podrobnosti*** – toto tlačidlo sa používa len v súvislosti s hrozbami detekovanými súčasťou Identity Protection. Po kliknutí sa zobrazí súhrnný prehľad informácií o hrozbe (*ktoré súbory alebo procesy boli ovplyvnené, vlastnosti procesov atď.*). Upozorňujeme, že pre všetky ostatné položky (okrem detekovaných súčasťou Identity Protection) je toto tlačidlo sivé a neaktívne!



- ***Vymazať*** – dokonale a nenávratne odstráni infikovaný súbor z ***Vírusového trezora***.
- ***Vyprázdniť trezor*** – dokonale vymaže celý obsah ***Vírusového trezora***. Odstránením z ***Vírusového trezora*** sa súbory úplne a nenávratne odstránia z disku (*nepremiestnia sa do Koša*).

13. Aktualizácie AVG

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

Vzhľadom na všetky nové počítačové hrozby a rýchlosť, akou sa šíria, je mimoriadne dôležité pravidelne aktualizovať produkt **AVG Internet Security 2012**. Najlepším riešením je ponechať predvolené nastavenia programu, v ktorých sú nastavené pravidelné aktualizácie. Nezabudnite, že bez aktuálnej vírusovej databázy programu **AVG Internet Security 2012** nemôže aplikácia zistiť najnovšie hrozby!

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

13.1. Spustenie aktualizácie

V záujme maximálneho využitia dostupného zabezpečenia je aplikácia **AVG Internet Security 2012** štandardne nastavená tak, aby hľadala nové aktualizácie každé štyri hodiny. Keďže spoločnosť AVG nezverejňuje aktualizácie podľa pevného harmonogramu, ale podľa počtu a závažnosti nových hrozieb, je veľmi dôležité dbať na aktuálnosť vírusovej databázy AVG.

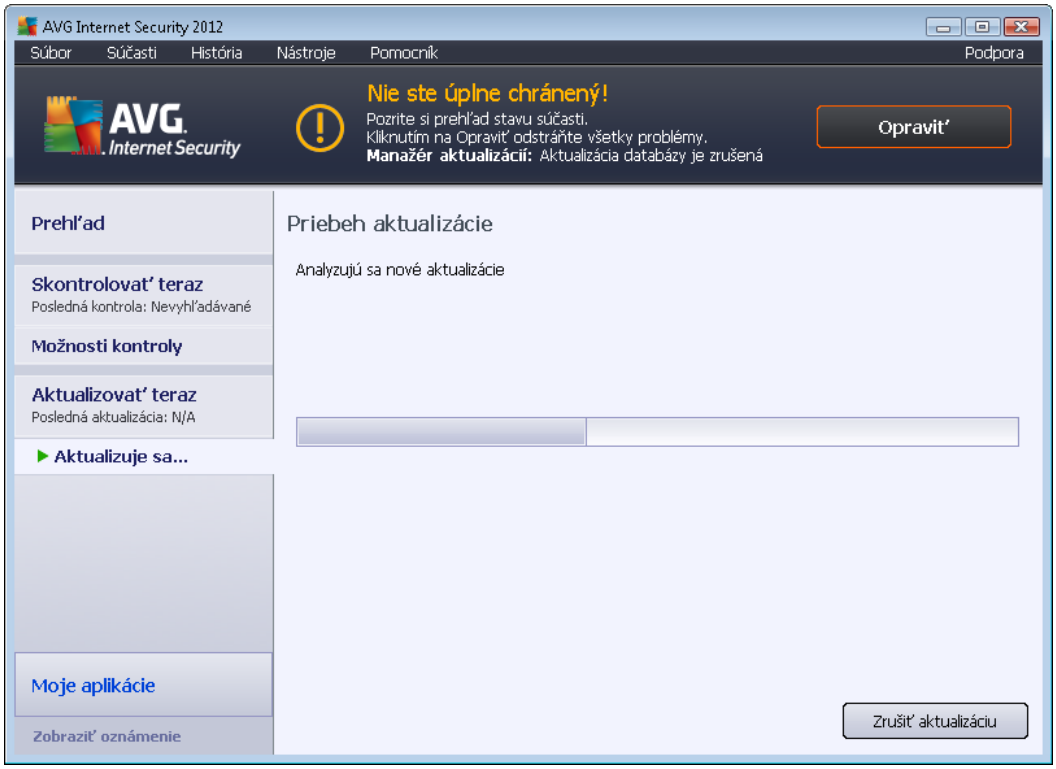
Ak chcete znížiť počet spustení aktualizácie, môžete tak urobiť pomocou vlastných parametrov spúšťania aktualizácie. Dôrazne sa však odporúča aktualizovať aspoň raz denne! Konfiguráciu môžete upraviť v časti Rozšírené nastavenia/plánovania, konkrétne v týchto dialógových oknách:

- Plán aktualizácie definícií
- Plán aktualizácie programu
- Plán aktualizácie súčasti Anti-Spam

Ak chcete skontrolovať novú aktualizáciu okamžite, môžete tak urobiť pomocou rýchleho prepojenia Aktualizovať teraz v hlavnom používateľskom rozhraní. Toto prepojenie sa nachádza v každom dialógovom okne používateľského rozhrania.

13.2. Postup aktualizácie

Po spustení aktualizácie program AVG najskôr skontroluje, či sú k dispozícii nové aktualizačné súbory. Ak **AVG Internet Security 2012** zistí prítomnosť nových aktualizačných súborov, začne ich preberať a spustí samotný proces aktualizácie. Počas procesu aktualizácie budete presmerovaní na rozhranie ***Aktualizácia*** , kde si môžete pozrieť napredovanie procesu v grafickom znázornení, ako aj prehľad príslušných štatistických parametrov (*veľkosť aktualizačného súboru, prijaté údaje, rýchlosť sťahovania, uplynutý čas...)*:



***Poznámka**: Pred spustením aktualizácie programu AVG sa vytvorí bod obnovy systému. Ak sa aktualizácie nepodarí a operačný systém spadne, bod obnovenia umožní obnoviť stav operačného systému s pôvodnou konfiguráciou. Táto možnosť je dostupná z ponuky systému Windows: Štart / Všetky programy / Príslušenstvo / Systémové nástroje / Obnovovanie systému. Odporúča sa len skúseným používateľom!*

13.3. Úrovne aktualizácie

Aplikácia **AVG Internet Security 2012** ponúka na výber dve úrovne aktualizácie:

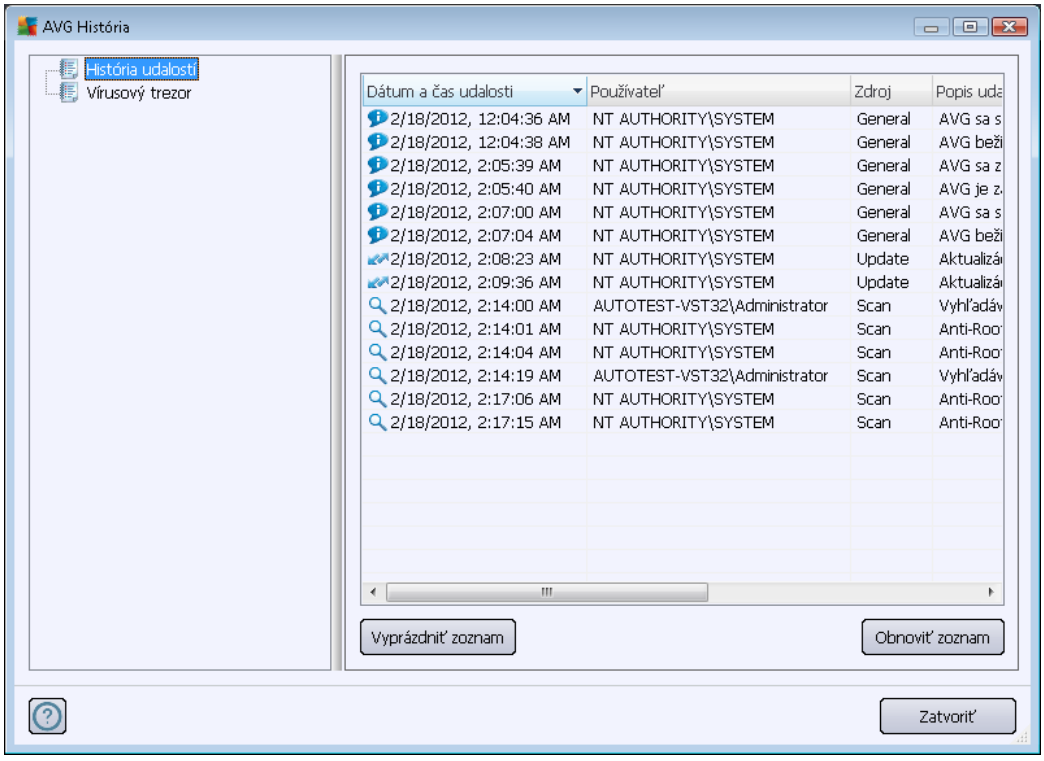
- ***Aktualizácia definícií*** obsahuje zmeny potrebné na dosiahnutie spoľahlivej ochrany pred vírusmi, spamom a škodlivým softvérom. Zvyčajne neobsahuje žiadne zmeny kódu a aktualizuje len databázu definícií. Táto aktualizácia by sa mala použiť čo možno najskôr.
- ***Aktualizácia programu*** obsahuje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

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

- Plán aktualizácie definícií
- Plán aktualizácie programu

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

14. História udalostí



Dialógové okno ***História udalostí*** sa otvára v ponuke programu kliknutím na položku ***História/ Protokol histórie udalostí***. V tomto dialógovom okne sa nachádza prehľad významných udalostí, ktoré sa vyskytli v čase, keď bol program **AVG Internet Security 2012** spustený. ***História*** zaznamenáva tieto typy udalostí:

- Informácie o aktualizáciách aplikácie AVG
- Informácie o spustení, ukončení a zastavení kontroly (*vrátane automaticky vykonávaných testov*)
- Informácie o udalostiach spojených so zisťovaním vírusov (*súčasťou Resident Shield alebo kontrolou*) vrátane miesta výskytu
- Iné významné udalosti

Každá udalosť má uvedené tieto informácie:

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

Ovládacie tlačidlá

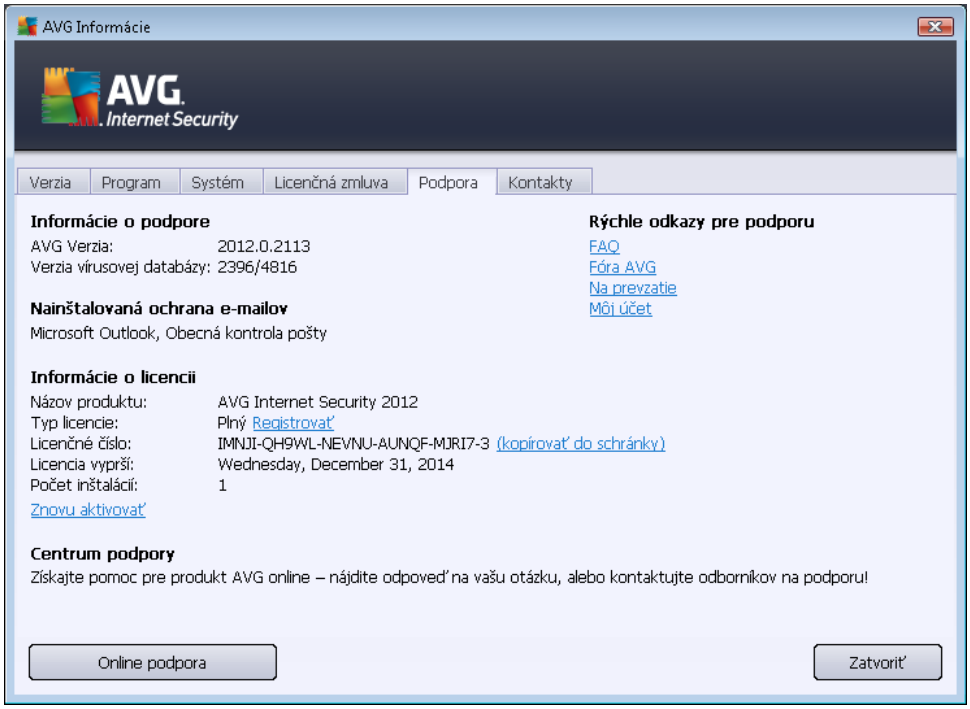
- ***Vymazať zoznam*** – Stlačením tohto tlačidla odstránite všetky položky v zozname udalostí
- ***Obnoviť zoznam*** – Stlačením tohto tlačidla aktualizujete všetky položky v zozname udalostí

15. FAQ a technická podpora

V prípade nákupných alebo technických problémov s aplikáciou **AVG Internet Security 2012** existuje niekoľko spôsobov, ako nájsť pomoc. Vyberte si z týchto možností:

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

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



- ***Riešenie problémov v súbore pomocníka***: Nová časť ***Riešenie problémov*** je k dispozícii priamo v súbore pomocníka v produkte **AVG Internet Security 2012** *(súbor pomocníka otvoríte stlačením klávesu F1 v niektorom z dialógových okien aplikácie)*. V tejto časti nájdete zoznam najčastejších situácií, v ktorých používateľ potrebuje vyhľadať profesionálnu pomoc pre technický problém. Vyberte situáciu, ktorá najviac zodpovedá vášmu problému, a kliknutím zobrazte podrobné pokyny vedúce k riešeniu daného problému.

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

- ***Časté otázky***: Na webovej lokalite AVG (http://www.avg.com/) môžete nájsť aj jednotlivé

dôkladne rozčlenené časté otázky. K tejto časti sa dostanete prostredníctvom ponuky ***Centrum podpory/FAQ***. Všetky otázky sú opäť prehľadne rozdelené do kategórií podľa toho, či sa problém týka nákupu, vírusov alebo ide o technickú otázku.

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

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