



AVG 9 Anti-Virus plus Firewall

Prírucka pre používateľa

Revízia dokumentu 90.21 (3.2.2010)

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

Tento produkt používa algoritmus MD5 Message-Digest spoločnosti RSA Data Security, Inc., Copyright (C) 1991-2, RSA Data Security, Inc. spoločnosť bola založená v roku 1991.

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

Tento produkt používa knižnicu kompresie zlib, Copyright (c) 1995-2002 Jean-loup Gailly a Mark Adler.
Tento produkt používa knižnicu kompresie libbzip2, Copyright (c) 1996-2002 Julian R Seward.

Obsah

1. Úvod	7
2. Požiadavky inštalácie AVG	8
2.1 Podporovaný operačný systém	8
2.2 Minimálne a odporúčané hardvérové nároky	8
3. Možnosti inštalácie produktu AVG	9
4. AVG Download Manager	10
4.1 Výber jazyka	10
4.2 Kontrola pripojenia	11
4.3 Nastavenia proxy	12
4.4 Prevzatie súborov na inštaláciu	13
5. Proces inštalácie AVG	14
5.1 Spustenie inštalácie	14
5.2 Licenčná zmluva	15
5.3 Kontrola stavu systému	15
5.4 Výber typu inštalácie	16
5.5 Aktivovanie licencie AVG	16
5.6 Používateľská inštalácia - Cielový priecinok	18
5.7 Používateľská inštalácia - Výber komponentu	19
5.8 AVG Security Toolbar	20
5.9 Zatvorte otvorené aplikácie	21
5.10 Prebieha inštalácia produktu AVG	22
5.11 Naplánovať pravidelné prehľadávania a aktualizácie	23
5.12 Výber spôsobu používania počítača	23
5.13 Pripojenie vášho počítača na internet	24
5.14 Konfigurácia ochrany AVG je dokončená.	25
6. Po inštalácii	26
6.1 Optimalizácia prehľadávania	26
6.2 Registrácia produktu	26
6.3 Prístup k Používateľskému rozhraniu	26
6.4 Prehľadávanie celého počítača	27
6.5 Test EICAR	27

6.6 Predvolená konfigurácia AVG	28
7. Používateľské rozhranie AVG	29
7.1 Systémová ponuka	30
7.1.1 Súbor	30
7.1.2 Komponenty	30
7.1.3 História	30
7.1.4 Nástroje	30
7.1.5 Pomoc	30
7.2 Informácie o stave zabezpečenia	33
7.3 Rýchle odkazy	34
7.4 Prehľad komponentov	35
7.5 Štatistika	36
7.6 Ikona systémového pozadia	36
8. Komponenty AVG	38
8.1 Anti-Virus	38
8.1.1 Anti-Virus Princípy	38
8.1.2 Rozhranie Anti-Virus	38
8.2 Anti-Spyware	40
8.2.1 Anti-Spyware Princípy	40
8.2.2 Rozhranie Anti-Spyware	40
8.3 Anti-Rootkit	42
8.4 Firewall	42
8.4.1 Princípy Firewallu	42
8.4.2 Profily Firewallu	42
8.4.3 Rozhranie Firewallu	42
8.5 Kontrola pošty	47
8.5.1 Princípy Kontroly pošty	47
8.5.2 Rozhranie Kontroly pošty	47
8.5.3 Detekcia Kontroly pošty	47
8.6 Licencia	51
8.7 Link Scanner	52
8.7.1 Pravidlá pre Link Scanner	52
8.7.2 Rozhranie Link Scanner	52
8.7.3 Štít vyhľadávania AVG	52
8.7.4 Aktívny štít surfovania AVG	52
8.8 Webový štít	56

8.8.1	Princíp fungovania súcasti Webový štít	56
8.8.2	Rozhranie súcasti Webový štít	56
8.8.3	Detegovanie súcastou Webový štít	56
8.9	Rezidentný štít	62
8.9.1	Rezidentný štít Princípy	62
8.9.2	Rozhranie Rezidentného štítu	62
8.9.3	Detekcia Rezidentného štítu	62
8.10	Manažér aktualizácií	67
8.10.1	Princípy Manažéra aktualizácií	67
8.10.2	Rozhranie Manažéra aktualizácií	67
9.	Panel nástrojov zabezpečenia AVG	70
9.1	Panel nástrojov zabezpečenia AVG Rozhranie	70
9.2	Možnosti panela nástrojov AVG Security Toolbar	72
9.2.1	Karta Všeobecné	72
9.2.2	Karta Užitočné tlačidlá	72
9.2.3	Karta Zabezpečenie	72
9.2.4	Karta Rozšírené možnosti	72
10.	Pokročilé nastavenia AVG	77
10.1	Vzhľad	77
10.2	Zvuky	80
10.3	Ignorovať chybný stav	81
10.4	Vírusový trezor	83
10.5	Výnimky PUP	84
10.6	Webový štít	86
10.6.1	Webová ochrana	86
10.6.2	Štít okamžitých správ	86
10.7	Kontrola odkazov	90
10.8	Vyhľadávania	91
10.8.1	Prehľadávať celý počítač	91
10.8.2	Prehľadávať v prieskumníkovi	91
10.8.3	Prehľadávať špecifické súbory alebo priecinky	91
10.8.4	Prehľadávanie vymeniteľných zariadení	91
10.9	Plány	98
10.9.1	Plánované vyhľadávanie	98
10.9.2	Plán aktualizácie vírusovej databázy	98
10.10	Kontrola pošty	110

10.10.1	Certifikácia	110
10.10.2	Filtrovanie pošty	110
10.10.3	Protokoly a Výsledky	110
10.10.4	Servery	110
10.11	Rezidentný štít	120
10.11.1	Pokročilé nastavenia	120
10.11.2	Výnimky adresára	120
10.11.3	Vylúčené súbory	120
10.12	Vyrovňovací server	125
10.13	Anti-Rootkit	127
10.14	Aktualizácia	128
10.14.1	Proxy	128
10.14.2	Vytácanie	128
10.14.3	URL	128
10.14.4	Správa	128
10.15	Vzdialená správa	135
11.	Firewall nastavenia	137
11.1	Všeobecné	137
11.2	Zabezpečenie	138
11.3	Profily Oblastí a Adaptérov	139
11.4	Protokoly	140
11.5	Profily	142
11.5.1	Informácie o profile	142
11.5.2	Zadefinované siete	142
11.5.3	Aplikácie	142
11.5.4	Systémové služby	142
12.	Vyhľadávanie AVG	154
12.1	Rozhranie vyhľadávania	154
12.2	Vopred zadefinované vyhľadávania	155
12.2.1	Prehľadávať celý počítač	155
12.2.2	Prehľadávať špecifické súbory alebo priecinky	155
12.3	Vyhľadávanie vo Windows Exploreri	163
12.4	Vyhľadávanie v Príkazovom riadku	164
12.4.1	Parametre vyhľadávania CMD	164
12.5	Plánovanie vyhľadávanií	167
12.5.1	Nastavenia plánu	167

12.5.2 Ako sa má vyhľadávať	167
12.5.3 Co sa má prehľadávať	167
12.6 Prehľad výsledkov vyhľadávania	178
12.7 Podrobnosti výsledkov vyhľadávania	180
12.7.1 Karta Prehľad výsledkov	180
12.7.2 Karta Infekcie	180
12.7.3 Karta Spyware	180
12.7.4 Karta Upozornenia	180
12.7.5 Karta Rootkity	180
12.7.6 Karta Informácie	180
12.8 Vírusový trezor	188
13. Aktualizácie AVG	190
13.1 Úrovne aktualizácie	190
13.2 Typy aktualizácie	190
13.3 Proces aktualizácie	191
14. História udalostí	192
15. Casto kladené otázky a technická podpora	194



1. Úvod

Táto príručka podrobne dokumentuje produkt **AVG 9 Anti-Virus plus Firewall**.

Blahoželáme vám k zakúpeniu produktu AVG 9 Anti-Virus plus Firewall!

AVG 9 Anti-Virus plus Firewall je jeden z ocenených produktov AVG, ktorých účelom je priniesť pokoj na mysl a úplné zabezpečenie vášho počítača. Rovnako ako všetky produkty AVG, aj program **AVG 9 Anti-Virus plus Firewall** je úplne pretvorený od základov a prináša osvedčenú a povestnú ochranu produktov AVG v ľahšie ovládateľnej a účinnejšej podobe.

Váš nový produkt **AVG 9 Anti-Virus plus Firewall** má zjednodušené rozhranie a používa agresívnejšie a rýchlejšie prehľadávanie. Automatizovali sme pre vás viacero funkcií zabezpečenia a vytvorili sme nové inteligentné používateľské nastavenia, aby ste si mohli prispôsobiť funkcie zabezpečenia svojmu zabehnutému životnému štýlu. Už žiaden kompromis medzi použiteľnosťou a zabezpečením!

Produkty AVG boli navrhnuté a vyrobené s cieľom chrániť váš počítač a vašu sieť. Používajte úplnú ochranu od AVG.



2. Požiadavky inštalácie AVG

2.1. Podporovaný operacný systém

AVG 9 Anti-Virus plus Firewall sa používa na ochranu počítačov s nasledujúcimi operacnými systémami:

- Windows 2000 Professional SP4 + Update Rollup 1
- 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 operacné systémy)

2.2. Minimálne a odporúčané hardvérové nároky

Minimálne hardvérové požiadavky pre produkt **AVG 9 Anti-Virus plus Firewall**:

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

Odporúčané hardvérové požiadavky pre produkt **AVG 9 Anti-Virus plus Firewall**:

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



3. Možnosti inštalácie produktu AVG

AVG umožňuje inštaláciu buď z inštalacného súboru, ktorý sa nachádza na inštalacnom disku CD, alebo prevzatím najnovšieho inštalacného súboru z webových stránok AVG (<http://www.avg.com/>).

Pred začatím inštalácie programu AVG vám odporúčame navštíviť webové stránky AVG (<http://www.avg.com/>) a vyhľadať nový inštalacný súbor. Prevzatím tohto nového inštalacného súboru sa zabezpečí nainštalovanie najnovšej ponúkanej verzie programu AVG 9 Anti-Virus plus Firewall.

Odporúčame vám použiť náš nový nástroj [AVG Download Manager](#), ktorý vám pomôže nastaviť správny jazyk pre inštalacný súbor!

Počas procesu inštalácie vás program požiada, aby ste vložili licenčné/predajné číslo. Pripravte si ho, prosím, ešte pred spustením inštalácie. Predajné číslo nájdete na obale CD. Ak ste si zakúpili svoju kópiu AVG online, vaše licenčné číslo vám bolo doručené emailom.

4. AVG Download Manager

AVG Download Manager je jednoduchý nástroj, ktorý vám pomôže zvoliť správny inštalacný súbor pre skúšobnú verziu produktu AVG. Na základe vložených údajov, program zvolí konkrétny produkt, druh licencie, požadované súčasti a jazyk. **AVG Download Manager** nakoniec prevezme súbor a spustí správny [proces inštalácie](#).

Upozornenie: Upozorňujeme, že program *AVG Download Manager* nie je vhodný na preberanie sieťových edícií a edícií SBS a funguje len pod nasledujúcimi operačnými systémami: Windows 2000 (s opravným balíkom SP4 + SRP), Windows XP, Windows Vista a Windows 7.

AVG Download Manager si môžete prevziať na webových stránkach AVG (<http://www.avg.com/>). Dolu uvádzame stručný opis každého jednotlivého kroku vykonaného programom **AVG Download Manager**:

4.1. Výber jazyka



V tomto prvom kroku programu **AVG Download Manager** zvolte jazyk inštalácie v rozbalovacej ponuke. Upozorňujeme, že výber jazyka sa týka len procesu inštalácie; po nainštalovaní programu budete môcť zmeniť jazyk priamo v nastaveniach programu. Potom pokračujte stlačením tlačidla **Dalšie**.

4.2. Kontrola pripojenia

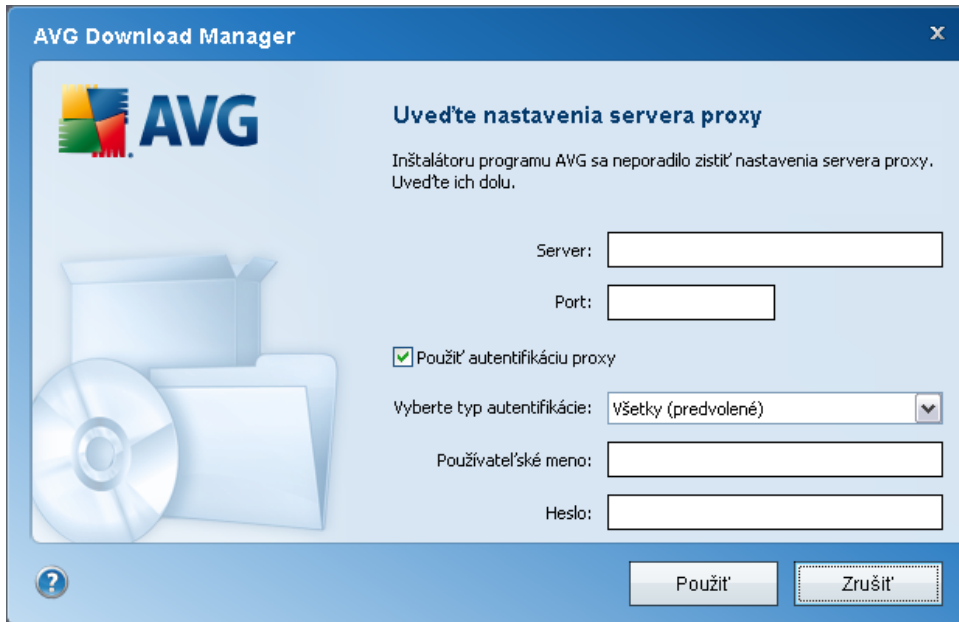
V ďalšom kroku sa program **AVG Download Manager** pokúsi vytvoriť pripojenie na internet, aby mohol vyhľadať aktualizácie. Nebudete môcť pokračovať v procese prevzatia až do momentu, keď program **AVG Download Manager** dokončí test pripojenia.

- Ak test nepotvrdí vytvorené pripojenie, skontrolujte, či je počítač naozaj pripojený na internet. Potom kliknite na tlačidlo **Skúsiť znova**.



- Ak používate pripojenie na internet cez server proxy, kliknite na tlačidlo **Nastavenia proxy** a zadajte [informácie o serveri proxy](#):
- Ak kontrola prebehla úspešne, pokračujte stlačením tlačidla **Ďalšie**.

4.3. Nastavenia proxy

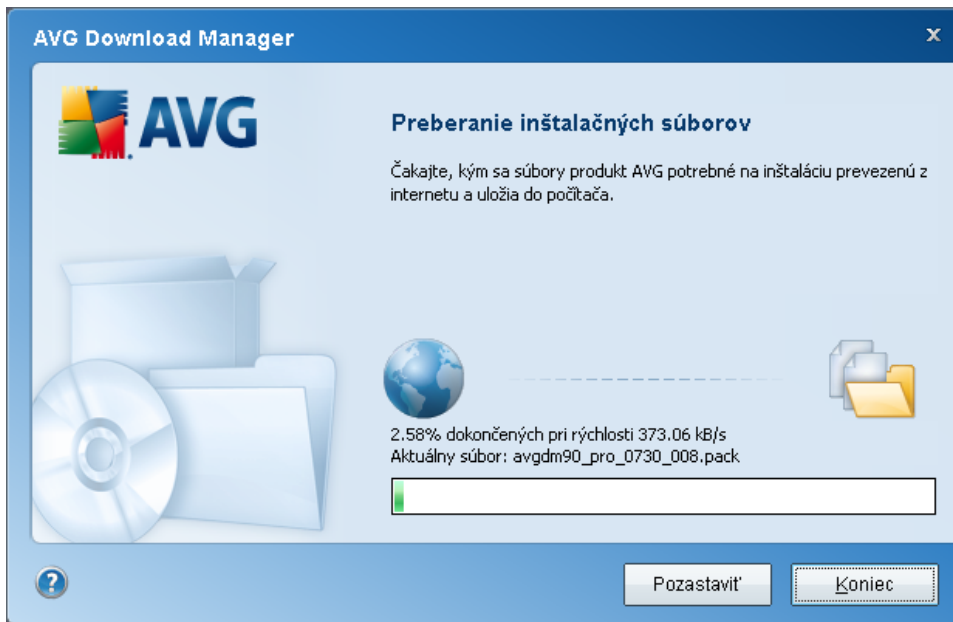


Ak sa programu **AVG Download Manager** nepodarilo zistiť nastavenia servera proxy, musíte ich definovať ručne. Vyplňte nasledujúce údaje:

- **Server:** Zadáajte platný názov alebo adresu IP servera proxy.
- **Port:** Zadáajte číslo príslušného portu.
- **Používať autentifikáciu proxy:** Označte toto zaciarkovacie políčko, ak server proxy vyžaduje overenie totožnosti.
- **Výber autentifikácie:** V rozbalovacej ponuke zvolte typ overenia totožnosti. Veľmi vám odporúčame ponechať predvolenú hodnotu (*server proxy vám potom automaticky oznámi svoje požiadavky*). Skúsení používatelia však môžu použiť aj možnosť Základné (*povinná pre niektoré servery*) (*povinná pre všetky servery ISA*). Potom vložte platné **používateľské meno** a **heslo** (voliteľné).

Stlačením tlačidla **Použiť** potvrdíte nastavenia a prejdete na ďalší krok v programe **AVG Download Manager**.

4.4. Prevzatie súborov na inštaláciu



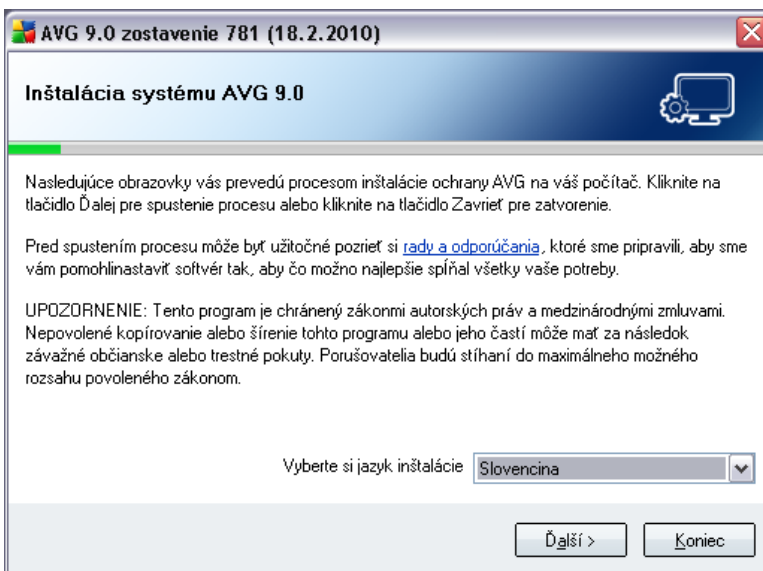
Teraz ste poskytli všetky informácie, ktoré program **AVG Download Manager** potrebuje na začatie preberania inštalacného balíka a spustenie procesu inštalácie. Potom prejdite na [proces inštalácie programu AVG](#).

5. Proces inštalácie AVG

Na nainštalovanie programu **AVG 9 Anti-Virus plus Firewall** do počítača sa musí použiť najnovší inštalčný súbor. Môžete použiť inštalčný súbor z CD, ktorý je súčasťou vašej krabicovej edície, tento súbor však môže byť zastaralý. Preto odporúčame stiahnuť si najnovší inštalčný súbor online. Súbor sa nachádza na webových stránkach AVG (<http://www.avg.com/>) v časti **Stredisko podpory/Na prevzatie**. Alebo môžete použiť náš nový nástroj **AVG Download Manager**, ktorý vám pomôže vytvoriť a prevziať potrebný inštalčný balík a spustiť proces inštalácie.

Proces inštalácie je tvorený sledom dialógových okien so stručným opisom toho, čo sa má v každom kroku urobiť. V nasledujúcej časti sa nachádza vysvetlenie každého dialógového okna:

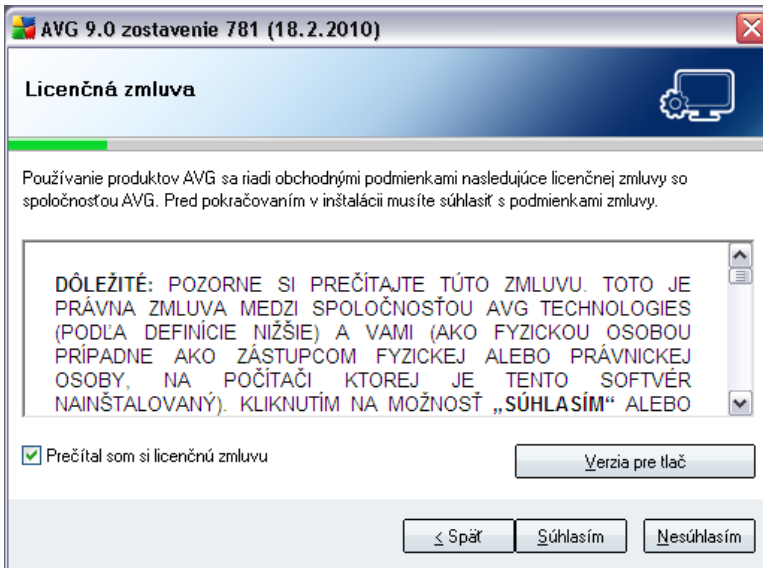
5.1. Spustenie inštalácie



Proces inštalácie začína oknom **Vitajte v inštalčnom programe AVG**. Tu zvolíte jazyk, ktorý sa použije pri procese inštalácie. V spodnej časti tohto dialógového okna nájdete položku **Zvoliť jazyk inštalácie** a zvolíte želaný jazyk vo vysúvacej ponuke. Potom stlačením tlačidla **Dalej** potvrdíte a prejdete na ďalšie dialógové okno.

Upozornenie: Tu si vyberáte jazyk len pre proces inštalácie. Nevyberáte si jazyk pre aplikáciu AVG – ten nastavíte neskôr počas procesu inštalácie!

5.2. Licenčná zmluva



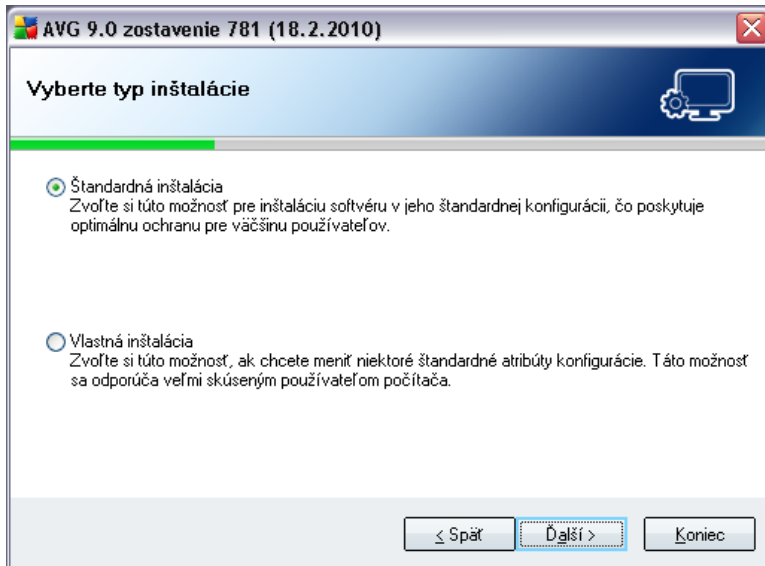
Dialógové okno **Licenčná zmluva** poskytuje kompletne znenie licenčnej zmluvy AVG. Dôkladne si ju prečítajte a označením zaciarkovacieho políčka **Prečítal/-s som si licenčnú zmluvu** a stlačením tlačidla **Súhlasím** potvrdte, že ste si prečítali a pochopili zmluvu a súhlasíte s jej obsahom.

Ak nesúhlasíte s licenčnou zmluvou, stlačte tlačidlo **Neprijat** a proces inštalácie sa ihneď ukončí.

5.3. Kontrola stavu systému

Po potvrdení licenčnej zmluvy budete presmerovaný na dialógové okno **Kontrola stavu systému**. Toto dialógové okno nevyžaduje žiadny zásah, váš systém bude skontrolovaný predtým, ako inštalácia AVG bude môcť začať. Pockajte, prosím, kým sa proces ukončí, potom bude automaticky pokračovať do nasledujúceho dialógového okna.

5.4. Výber typu inštalácie



Dialógové okno **Výber typu inštalácie** ponúka na výber dve možnosti inštalácie: **štandardnú** a **vlastnú** inštaláciu.

Väčšine používateľov odporúčame použiť **štandardnú inštaláciu**, ktorá nainštaluje program AVG v úplne automatickom režime s nastaveniami vopred definovanými výrobcou programu. Táto konfigurácia poskytuje maximálne zabezpečenie spolu s optimálnym využívaním zdrojov. V budúcnosti, ak bude potrebné zmeniť konfiguráciu, vždy budete mať možnosť urobiť tak priamo v aplikácii AVG.

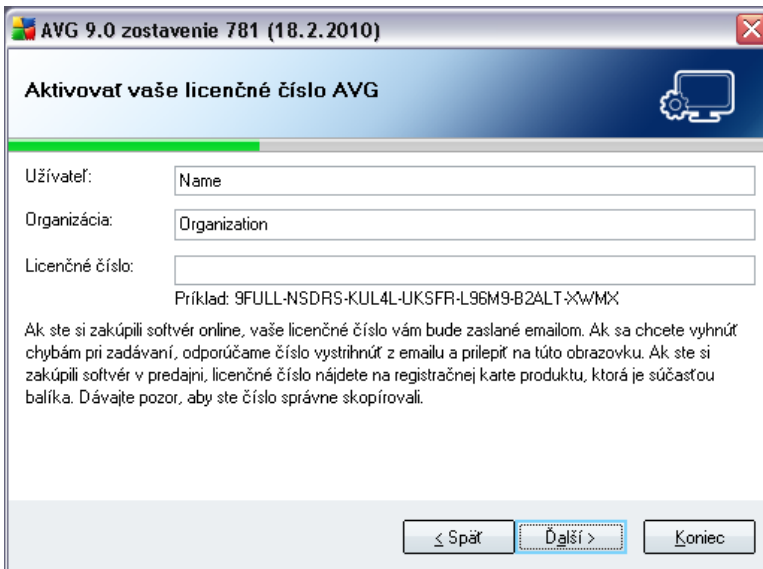
Vlastnú inštaláciu odporúčame používať len skúseným používateľom, ktorí majú skutočný dôvod inštalovať program AVG s neštandardnými nastaveniami, napr. na účely prispôsobenia konkrétnym systémovým požiadavkám.

5.5. Aktivovanie licencie AVG

V dialógovom okne **Aktivovanie licencie AVG** musíte vyplniť svoje registracné údaje. Zadáajte svoje meno (v poli **Meno používateľa**) a názov organizácie (v poli **Názov spoločnosti**).

Potom zadajte licencné/predajné číslo do textového pola **Licencné číslo**. Predajné číslo sa nachádza na obale disku CD v škatuli produktu **AVG 9 Anti-Virus plus Firewall**. Licencné číslo sa nachádza v e-mailovej správe s potvrdením, ktorú ste dostali po zakúpení produktu **AVG 9 Anti-Virus plus Firewall** online. Číslo sa musí

zadat 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.



AVG 9.0 zostavenie 781 (18.2.2010)

Aktivovať vaše licenčné číslo AVG

Užívateľ:

Organizácia:

Licenčné číslo:

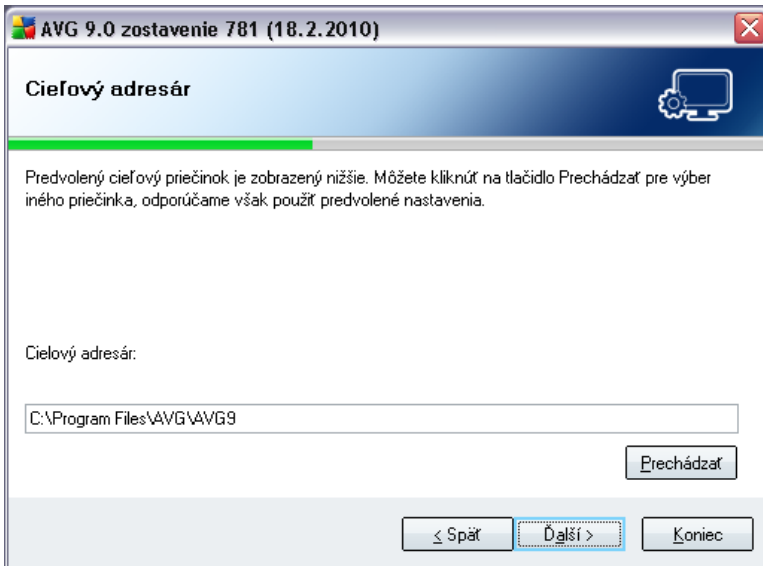
Príklad: 9FULL-NSDRS-KUL4L-UKSFR-L96M9-B2ALT-XWMX

Ak ste si zakúpili softvér online, vaše licenčné číslo vám bude zaslané emailom. Ak sa chcete vyhnúť chybám pri zadávaní, odporúčame číslo vystrihnúť z emailu a prilepiť na túto obrazovku. Ak ste si zakúpili softvér v predajni, licenčné číslo nájdete na registračnej karte produktu, ktorá je súčasťou balíka. Dávajte pozor, aby ste číslo správne skopírovali.

Pokračujte v procese inštalácie stlačením tlačidla **Dalšie**.

Ak ste v predchádzajúcom kroku zvolili štandardnú inštaláciu, otvorí sa priamo dialógové okno **AVG Security Toolbar**. Ak ste zvolili vlastnú inštaláciu, otvorí sa dialógové okno **Cielový priecinok**.

5.6. Používateľská inštalácia - Cieľový priečinok

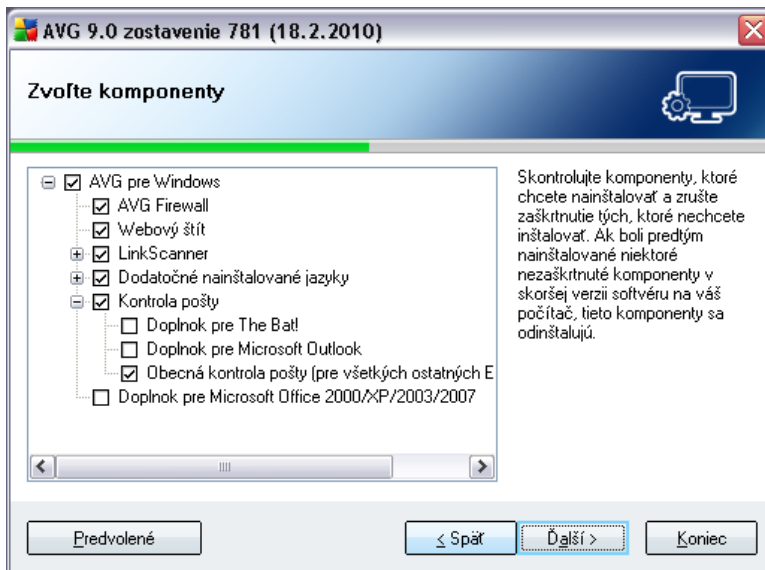


Dialógové okno **Cieľový priečinok** vám umožní nastaviť umiestnenie, do ktorého sa nainštaluje program **AVG 9 Anti-Virus plus Firewall**. Štandardne sa AVG nainštaluje do priečinka Program files na disku C:. Ak priečinok neexistuje, dialógové okno sa vás opýta, či súhlasíte s tým, aby ho program AVG teraz vytvoril.

Ak chcete toto umiestnenie zmeniť, použijete tlačidlo **Prehľadávať** na otvorenie prehľadu diskových jednotiek a zvolíte príslušný priečinok.

Potvrďte stlačením tlačidla **Dalšie**.

5.7. Používateľská inštalácia - Výber komponentu



V dialógovom okne **Výber súčastí** sa zobrazí prehľad všetkých súčastí programu **AVG 9 Anti-Virus plus Firewall**, ktoré je možné nainštalovať. Ak vám predvolené nastavenia nevyhovujú, môžete odstrániť/pridať konkrétne súčasti.

Môžete však nainštalovať len súčasti, ktoré sú súčasťou vašej zakúpenej edície AVG. Dialógové okno Výber súčastí vám ponúkne inštaláciu len týchto súčastí!

- **Výber jazyka**

V zozname inštalovaných súčastí môžete nastaviť jazyky, ktoré sa majú nainštalovať spolu s programom AVG. Oznacte položku **Dalšie nainštalované jazyky** a v príslušnej ponuke zvolte požadované jazyky.

- **Zásuvné moduly súčasti E-mail Scanner**

Kliknutím na položku **E-mail Scanner** otvorte a zvolte zásuvný modul, ktorý sa má nainštalovať na kontrolu elektronickej pošty. Ako predvolený sa nainštaluje zásuvný modul **Plugin for Microsoft Outlook**. Ďalšiu konkrétnu možnosť predstavuje zásuvný modul **Plugin for The Bat!** Ak používate inú poštovú aplikáciu (*MS Exchange, Qualcomm Eudora...*), použite možnosť **Personal E-mail Scanner** na automatické zabezpečenie e-mailovej komunikácie bez ohľadu na používanú aplikáciu.

Pokračujte stlačením tlačidla **Dalšie**.

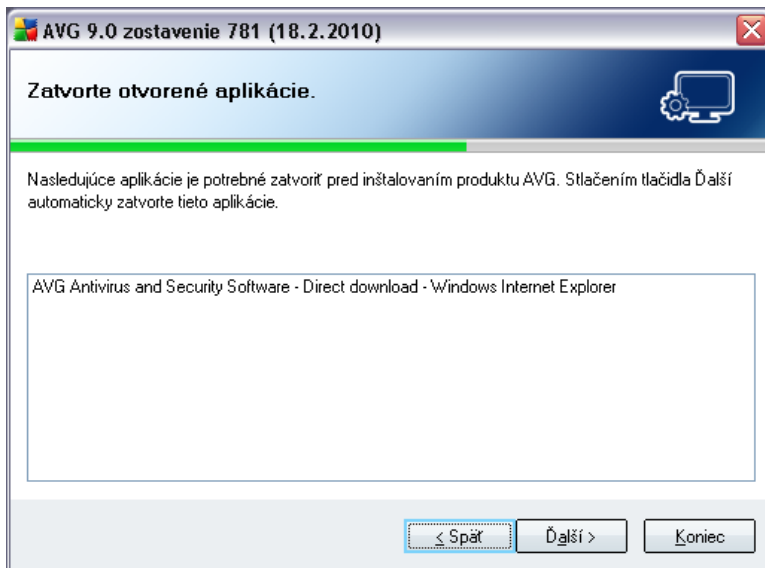
5.8. AVG Security Toolbar



V dialógovom okne **AVG Security Toolbar** nastavte, či chcete nainštalovať funkciu **AVG Security Toolbar** (overovanie výsledkov vyhľadávania v podporovaných internetových vyhľadávacoch). Ak nezmeníte predvolené nastavenia, táto súčasť sa nainštaluje automaticky do internetového prehliadača (v súčasnosti sú podporované prehliadače Microsoft Internet Explorer v. 6.0 a novšie a Mozilla Firefox v. 2.0 a novšie), aby vám zabezpečila komplexnú ochranu počas surfovania na internete.

Zároveň môžete rozhodnúť, či sa má Yahoo! nastaviť ako predvolený vyhľadávač. Ak ho chcete nastaviť ako predvolený, označte príslušné zaciarkovacie políčko.

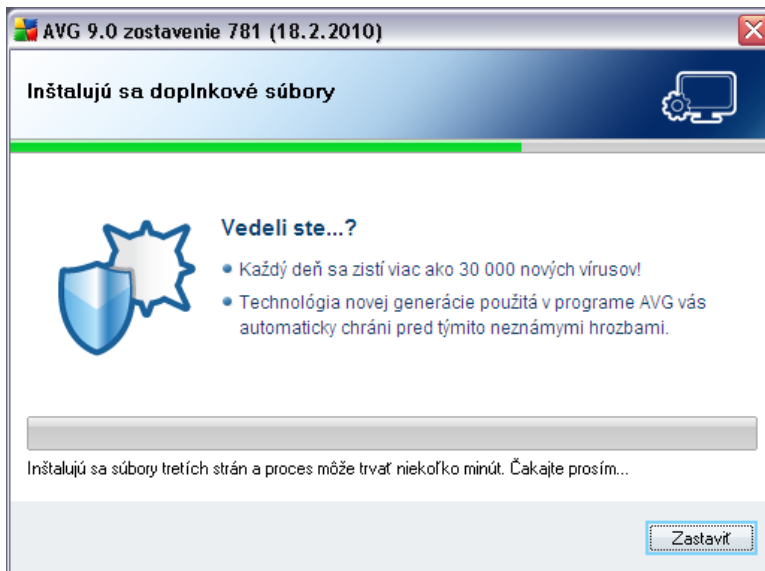
5.9. Zatvorte otvorené aplikácie



Dialógové okno **Zatvorte otvorené aplikácie** sa otvorí počas procesu inštalácie len v prípade, ak sú v tomto momente spustené v počítači programy, ktoré znemožňujú dokončenie inštalácie. Potom sa zobrazí zoznam programov, ktoré je potrebné zatvoriť na úspešné dokončenie procesu inštalácie. Stlačením tlačidla **Dalšie** potvrdíte, že súhlasíte so zatvorením uvedených aplikácií a prejdete na ďalší krok.

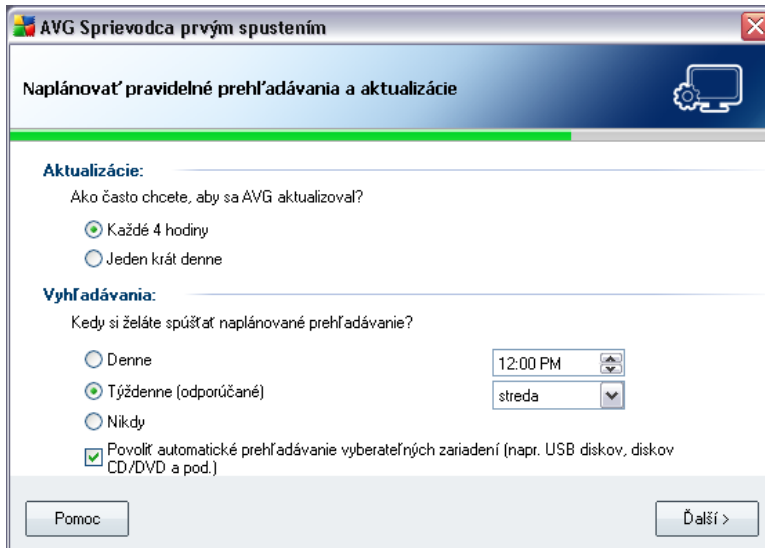
5.10. Prebieha inštalácia produktu AVG

V dialógovom okne **Prebieha inštalácia programu AVG** sa zobrazuje priebeh procesu inštalácie a okno nevyžaduje žiaden úkon zo strany používateľa:



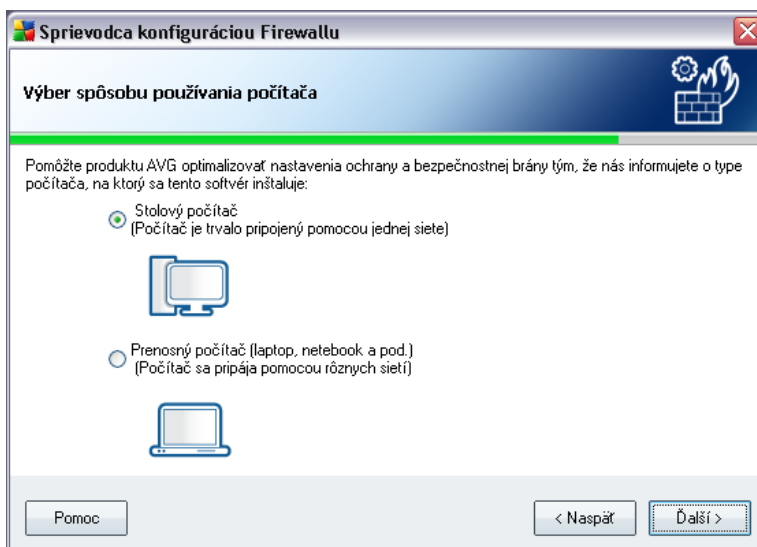
Po dokončení inštalácie sa automaticky otvorí ďalšie dialógové okno.

5.1.1. Naplánovať pravidelné prehľadovania a aktualizácie



V dialógovom okne **Naplánovať pravidelné vyhľadovania a aktualizácie** nastavte interval pre kontrolu dostupnosti nových aktualizacných súborov a zadefinujte čas, kedy sa má plánované vyhľadovanie spustiť. Odporúča sa ponechať predvolené hodnoty. Pokračujte stlačením tlačidla **Dalej**.

5.1.2. Výber spôsobu používania počítača



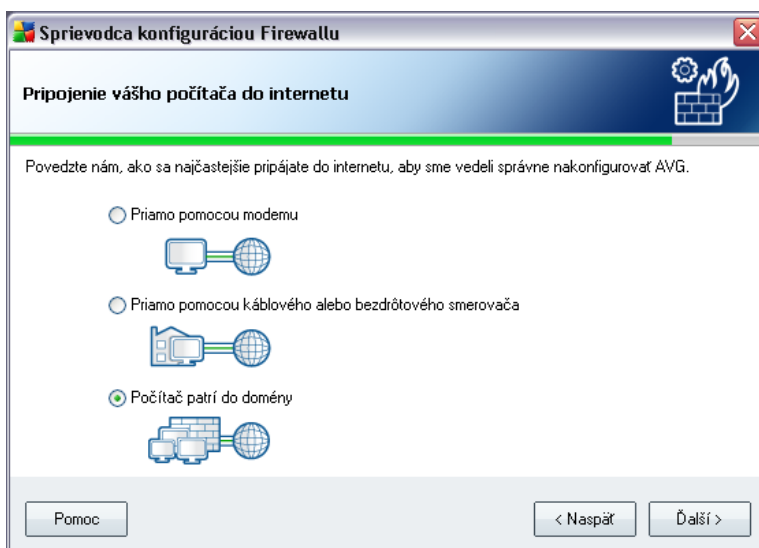
V tomto dialógovom okne sa vás **sprievodca konfiguráciou súčast Firewall** opýta, aký typ počítača používate. Napríklad notebook, s ktorým sa pripájate na internet na rôznych miestach (*letiskách, hotelových izbách a pod.*), vyžaduje prísnejšie bezpečnostné pravidlá než počítač v doméne (*podnikovej sieti a pod.*). Na základe zvoleného druhu použitia počítača sa nastaví predvolené pravidlá pre súčast **Firewall** s rôznou úrovňou zabezpečenia.

Program ponúka na výber z dvoch alternatívnych možností:

- **Stolový počítač**
- **Prenosný počítač**

Stlačením tlačidla **Dalšie** potvrdíte voľbu a otvorte ďalšie dialógové okno.

5.13. Pripojenie vášho počítača na internet



V tomto dialógovom okne sa vás **Sprievodca konfiguráciou Firewallu** spýta, ako je váš počítač pripojený k Internetu. Na základe zvoleného typu pripojenia sa predvolené pravidlá **Firewallu** zdefinujú s inou úrovňou zabezpečenia.

Máte na výber z troch alternatívnych možností:

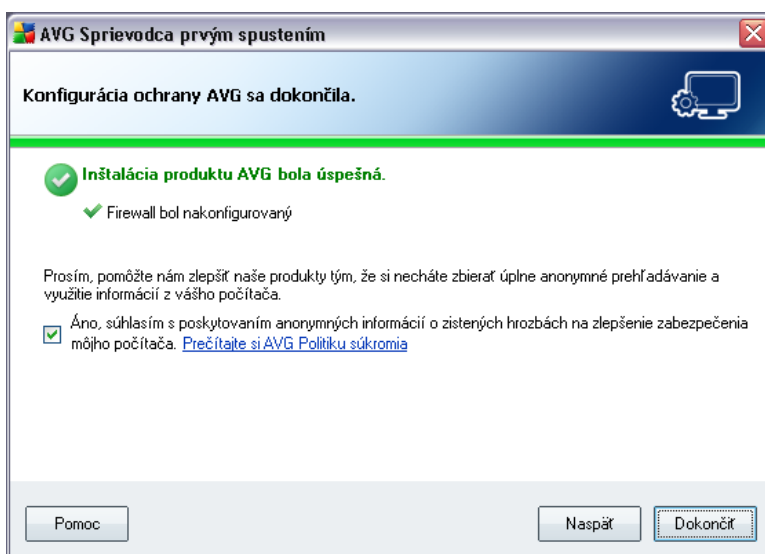
- **Priamo pomocou modemu**
- **Priamo pomocou káblového alebo bezdrôtového smerovaca**

- **Počítač patrí do domény**

Zvoľte typ pripojenia, ktorý najlepšie zodpovedá pripojeniu vášho počítača na internet.

Potvrďte svoj výber stlačením tlačidla **Dalej**, aby ste mohli pokračovať na nasledujúce dialógové okno.

5.14. Konfigurácia ochrany AVG je dokončená.



Váš produkt **AVG 9 Anti-Virus plus Firewall** je teraz nakonfigurovaný.

V tomto dialógovom okne nastavte, či chcete povoliť anonymné hlásenie hrozieb a zlých stránok do vírusového laboratória spoločnosti AVG. V prípade kladnej odpovede označte možnosť **Áno, súhlasím s poskytovaním ANONYMNÝCH informácií o zistených hrozbách na zlepšenie zabezpečenia môjho počítača.**

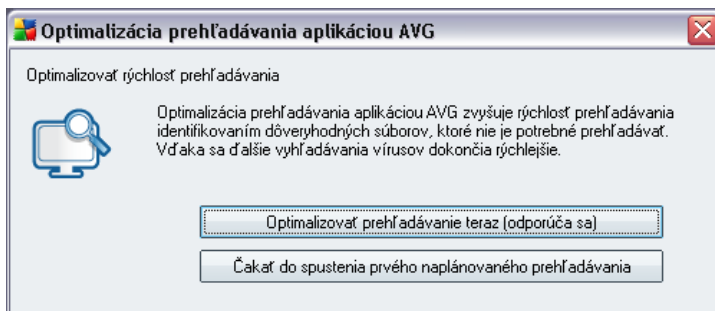
Nakoniec stlačte tlačidlo **Dokončiť**. Pred používaním produktu AVG bude pravdepodobne potrebné reštartovať počítač.

6. Po inštalácii

6.1. Optimalizácia prehľadovania

Funkcionalita procesu optimalizácie prehľadovania prehľadá priečinky *Windows* a *Program files*, v ktorých deteguje určité súbory (*momentálne súbory s príponami exe, dll a sys*) a uloží informácie o týchto súboroch. Pri neskoršom získaní prístupu sa tieto súbory nebudú znova prehľadávať, čím sa výrazne skráti doba prehľadovania.

Po dokončení procesu inštalácie sa otvorí nové dialógové okno, ktoré vám odporučí urobiť optimalizačné prehľadovanie:



Odporúčame vám použiť toto tlačidlo a spustiť proces optimalizácie prehľadovania stlačením tlačidla **Optimalizovať prehľadovanie teraz**.

6.2. Registrácia produktu

Po dokončení inštalácie produktu **AVG 9 Anti-Virus plus Firewall** si zaregistrujte produkt online na webových stránkach AVG (<http://www.avg.com/>) na stránke **Registrácia** (*postupujte podľa pokynov uvedených priamo na tejto stránke*). Registráciu získate úplný prístup k vášmu používateľskému kontu AVG, informáciám o aktualizáciách AVG a ďalším službám poskytovaným výhradne registrovaným používateľom.

6.3. Prístup k Používateľskému rozhraniu

Používateľské rozhranie AVG je dostupné niekoľkými spôsobmi:

- dvakrát kliknite na ikonu AVG na systémovom pozadí
- dvakrát kliknite na ikonu AVG na pracovnej ploche

- otvorením ponuky **Štart/Programy/AVG 9.0/Používateľské rozhranie AVG**

6.4. Prehľadávanie celého počítača

Existuje potenciálne riziko, že sa do vášho počítača dostal počítačový vírus ešte pred nainštalovaním produktu **AVG 9 Anti-Virus plus Firewall**. Z tohto dôvodu by ste mali spustiť [prehľadávanie celého počítača](#), aby sa vylúčila možnosť existencie infekcie v počítači.

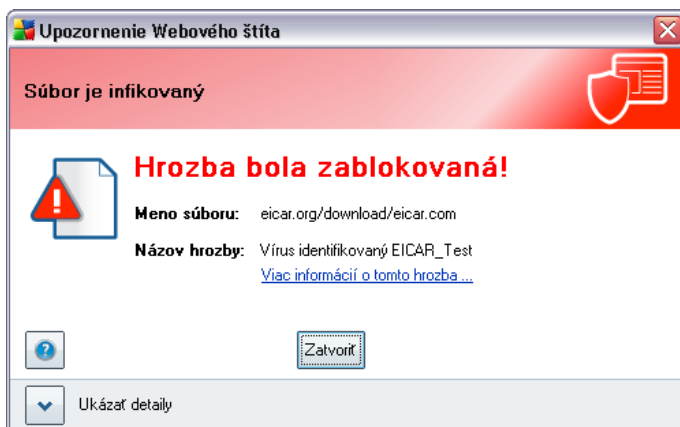
Pokyny na spustenie [prehľadávania celého počítača](#) sa nachádzajú v kapitole [Prehľadávanie programom AVG](#).

6.5. Test EICAR

Na kontrolu, či sa program **AVG 9 Anti-Virus plus Firewall** 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 nan reaguje ako na vírus (aj keď ho obvyčajne označí jednoznačným názvom, ako napríklad „EICAR-AV-Test“). Vírus EICAR si môžete prevziať na webových 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. Ihned po potvrdení preberania testovacieho súboru, [Webový štít](#) zobrazí upozornenie na túto skutočnosť. Zobrazenie tohto oznámenia znamená, že program AVG je správne nainštalovaný v počítači.





Na webových stránkach <http://www.eicar.com> si môžete prevziať aj komprimovanú verziu „vírusu“ EICAR (napr. s názvom *eicar_com.zip*). **Webový štít** vám umožní prevziať tento súbor a uložiť ho na pevný disk počítača, ale súčasť **Rezidentný štít** deteguje „vírus“, keď sa ho pokúsite rozbaľiť. **Ak sa programu AVG nepodari identifikovať testovací súbor EICAR ako vírus, skontrolujte ešte raz konfiguráciu programu!**

6.6. Predvolená konfigurácia AVG

Predvolenú konfiguráciu (t. j. spôsob nastavenia aplikácie bezprostredne po inštalácii) produktu **AVG 9 Anti-Virus plus Firewall** nastavil dodávateľ softvéru takým spôsobom, aby všetky súčasti a funkcie fungovali optimálne.

Nemete 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 je potrebné zmeniť konfiguráciu AVG takým spôsobom, aby bola lepšie prispôbená vašim potrebám, otvorte [rozšírené nastavenia AVG](#): zvolte položku v systémovej ponuke **Nástroje/Rozšírené nastavenia** a zmeňte konfiguráciu AVG v novo otvorenom dialógovom okne [Rozšírené nastavenia AVG](#).

7. Používateľské rozhranie AVG

AVG 9 Anti-Virus plus Firewall sa otvára v hlavnom okne:



Hlavné okno je rozdelené na niekoľko častí:

- **Systemová ponuka** (horný riadok v okne) je štandardná navigačná štruktúra, ktorá ponúka prístup ku všetkým súčastiam, službám a funkciám AVG – [podrobnosti >>](#).
- **Informácie o stave zabezpečenia** (horná časť okna) poskytuje informácie o aktuálnom stave nainštalovaného programu AVG – [podrobnosti >>](#)
- **Rýchle odkazy** (ľavá časť okna) umožňuje rýchly prístup k najdôležitejším a najčastejšie používaným úlohám programu AVG – [podrobnosti >>](#)

- **Prehľad súčastí** (*stredná časť okna*) poskytuje prehľad všetkých nainštalovaných súčastí AVG – [_podrobnosti >>](#)
- **Štatistika** (*ľavá spodná časť okna*) poskytuje všetky štatistické údaje o fungovaní programu – [_podrobnosti >>](#)
- **Ikona na paneli úloh** (*pravý spodný roh monitora, na paneli úloh*) informuje o aktuálnom stave programu AVG – [_podrobnosti >>](#)

7.1. Systémová 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 9 Anti-Virus plus Firewall**. Hlavná ponuka sa používa na sprístupnenie konkrétnych súčastí, funkcií a služieb AVG.

Hlavná ponuka je rozdelená na päť hlavných častí:

7.1.1. Súbor

- **Ukončiť:** Zatvorí používateľské rozhranie programu **AVG 9 Anti-Virus plus Firewall**. Aplikácia AVG sa však bude aj naďalej spúšťať na pozadí a počítač bude stále chránený!

7.1.2. Komponenty

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](#).
- **Anti-Virus:** Otvorí hlavnú stránku súčasti [Anti-Virus](#)
- **Anti-Rootkit:** Otvorí hlavnú stránku súčasti [Anti-Rootkit](#)
- **Anti-Spyware:** Otvorí hlavnú stránku súčasti [Anti-Spyware](#)
- **Firewall:** Otvorí hlavnú stránku súčasti [Firewall](#)
- **Link Scanner:** Otvorí hlavnú stránku súčasti [Link Scanner](#)
- **E-mail Scanner:** Otvorí hlavnú stránku súčasti [E-mail Scanner](#)
- **Licencia:** Otvorí hlavnú stránku súčasti [Licencia](#)

- **Webový štít:** Otvorí hlavnú stránku súcasti [Webový štít](#)
- **Rezidentný štít:** Otvorí hlavnú stránku súcasti [Rezidentný štít](#)
- **Update Manager:** Otvorí hlavnú stránku súcasti [Update Manager](#)

7.1.3. História

- **Výsledky prehľadovania:** Prepne sa testovacie rozhranie AVG, konkrétne na dialógové okno [Prehľad výsledkov prehľadovania](#).
- **Detegovanie súcastou Rezidentný štít:** Otvorí dialógové okno s prehľadom hrozieb detegovaných súcastou [Rezidentný štít](#)
- **Detegovanie súcastou E-mail Scanner:** Otvorí dialógové okno s prehľadom príloh e-mailových správ označených súcastou [E-mail Scanner](#) ako nebezpečné.
- **Nálezy súcasti Webového štítu:** Otvorí dialógové okno s prehľadom hrozieb zistených súcast [Webový štít](#)
- **Vírusový trezor:** Otvorí rozhranie úložiska karantény ([Vírusový trezor](#)), do ktorého AVG odstraňuje všetky detegované infekcie, ktoré sa z rôznych dôvodov nedajú automaticky vyliečiť. V tejto karanténe sú infikované súbory izolované, aby sa dala garantovať bezpečnosť počítača. Uložené súbory sa prípadne môžu neskôr opraviť.
- **História udalostí:** Otvorí rozhranie histórie udalostí s prehľadom všetkých zaznamenaných akcií programu **AVG 9 Anti-Virus plus Firewall**.
- **Firewall:** Otvorí rozhranie Nastavenia súcasti Firewall na karte [Záznamové protokoly](#) s podrobným prehľadom všetkých akcií súcasti Firewall.

7.1.4. Nástroje

- **Prehľadovať počítač:** Prepne na [rozhranie prehľadovania programom AVG](#) a spustí prehľadovanie celého počítača.
- **Prehľadovať zvolený priečinok:** Prepne na [rozhranie prehľadovania programom AVG](#) a pomocou stromovej štruktúry počítača umožní definovať, ktoré súbory a priečinky sa majú prehľadávať.
- **Prehľadovať súbor:** Používa sa na skontrolovanie jedného súboru zvoleného v stromovej štruktúre disku.

- **Aktualizácia**: Automaticky spustí proces aktualizácie programu **AVG 9 Anti-Virus plus Firewall**
- **Aktualizovať z adresára**: Spustí proces aktualizácie z aktualizacných súborov, ktoré sa nachádzajú v nastavenom priečinku na vašom lokálnom disku. Túto možnosť 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 na sieť bez prístupu na internet atď.*). V novo otvorenom okne zvolte priečinok, kde ste predtým vložili aktualizacný súbor a spustíte proces aktualizácie.
- **Rozšírené nastavenia**: Otvorí dialógové okno **Rozšírené nastavenia programu AVG**, ktoré vám umožní editovať konfiguráciu produktu **AVG 9 Anti-Virus plus Firewall**. Odporúča vám nemeniť predvolené nastavenia aplikácie definované výrobcom softvéru.
- **Nastavenia súčasti Firewall**: Otvorí samostatné dialógové okno s rozšírenou konfiguráciou súčasti **Firewall**.

7.1.5. Pomoc

- **Obsah**: Otvorí súbory pomocníka AVG.
- **Získať pomoc online**: Otvorí webové stránky AVG (<http://www.avg.com/>) na stránke strediska podpory zákazníkov.
- **Webové stránky vášho produktu AVG**: Otvorí webové stránky AVG (<http://www.avg.com/>).
- **O vírusoch a hrozbách**: Otvorí online **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 **Prispôbiť AVG** v **processe inštalácie**. Toto dialógové okno sa používa na vloženie licencného čísla, buď pri nahradení predajného čísla (*čísla, s ktorým ste nainštalovali AVG*), alebo pri nahradení starého licencného čísla (*napr. pri upgradovaní na nový produkt AVG*).
- **Registovať teraz**: Vytvorí pripojenie na registracnú stránku na webových stránkach AVG (<http://www.avg.com/>). Vyplňte svoje registracné údaje; nárok na bezplatnú technickú podporu získajú len zákazníci, ktorí si svoj produkt AVG zaregistrujú.

Poznámka: Ak používate skúšobnú verziu produktu **AVG 9 Anti-Virus plus Firewall**, uvedené dve položky sa zobrazia v podobe **Kúpiť teraz** a **Aktivovať** a

umožnia vám ihneď zakúpiť úplnú verziu programu. Ak je produkt **AVG 9 Anti-Virus plus Firewall** nainštalovaný pomocou predajného čísla, položky sa zobrazia v podobe **Registrovat a Aktivovat**. Ďalšie informácie sa nachádzajú v časti [Licencia](#) v tejto dokumentácii.

- **O produkte AVG:** Otvorí dialógové okno **Informácie** s piatimi 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**.

7.2. Informácie o stave zabezpečenia

Časť **informácie o stave zabezpečenia** sa nachádza v hornej časti hlavného okna AVG. V tejto časti sa vždy nachádzajú informácie o aktuálnom stave zabezpečenia vytváraného programu **AVG 9 Anti-Virus plus Firewall**. Pozrite si prehľad ikon, ktoré sa môžu nachádzať v tejto časti, a ich význam:



Zelená ikona informuje, že program AVG je úplne funkčný. Počítač je úplne chránený, aktualizovaný a všetky nainštalované súčasti fungujú správne.



Oranžová ikona upozorňuje, že jedna alebo viac súčastí je nesprávne nakonfigurovaných a je potrebné venovať pozornosť ich vlastnostiam/nastaveniam. Nevyskytuje sa žiaden kritický problém v programe AVG a pravdepodobne ste sa z nejakého dôvodu rozhodli niektorú súčasť vypnúť. Stále ste chránení programom AVG. Venujte však pozornosť nastaveniam problémovej súčasti! Jej názov bude uvedený v časti **Informácie o stave zabezpečenia**.

Táto ikona sa zobrazí aj vtedy, ak sa z nejakého dôvodu rozhodnete [ignorovať chybový stav súčasti](#) (možnosť „Ignorovať stav súčasti“ sa nachádza v kontextovej ponuke, ktorá sa otvára kliknutím pravým tlačidlom myši na ikone príslušnej súčasti v prehľade súčastí v hlavnom okne programu AVG). Môže sa vyskytnúť situácia, keď bude potrebné použiť túto možnosť; dôrazne vám však odporúčame, aby ste funkciu „**Ignorovať stav súčastí**“ čo najskôr znova vypli.



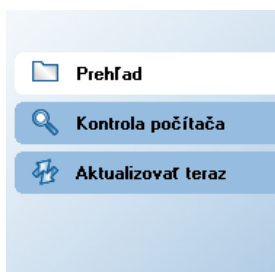
Červená ikona informuje, že sa vyskytol kritický stav programu AVG! Jeden alebo viacero komponentov nefunguje správne a AVG nemôže chrániť váš počítač. Venujte, prosím, pozornosť oprave uvedeného problému. Ak nedokážete odstrániť chybu sami, kontaktujte tím [technickej podpory AVG](#).

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

Poznámka: Informáciu o stave programu AVG získate kedykoľvek pohľadom na [ikonu na paneli úloh](#).

7.3. Rýchle odkazy

Rýchle odkazy (v ľavej časti [používateľského rozhrania AVG](#)) umožňujú okamžitý prístup k najdôležitejším a najčastejšie používaným funkciám programu AVG:



- **Prehľad:** Tento odkaz sa používa na prepnutie práve otvoreného rozhrania AVG na hlavné rozhranie s prehľadom všetkých nainštalovaných súčastí – pozri kapitolu [Prehľad súčastí >>](#)
- **Kontrola počítača:** Tento odkaz sa používa na otvorenie rozhrania prehľadávania programom AVG, ktoré umožňuje priamo spustiť testy, naplánovať prehľadávanie resp. editovať jeho parametre – pozri kapitolu [Prehľadávanie programom AVG >>](#)
- **Aktualizovať teraz:** Tento odkaz otvorí rozhranie aktualizácií a ihneď spustí proces aktualizácie programu AVG – pozri kapitolu [Aktualizácie programu AVG >>](#)

Tieto odkazy sa vždy nachádzajú v používateľskom rozhraní. Ak použijete rýchly odkaz na spustenie konkrétneho procesu, v grafickom používateľskom rozhraní sa otvorí nové dialógové okno, ale rýchle odkazy budú stále prístupné. Okrem toho sa prebiehajúci proces znázorní aj v grafickej podobe.

7.4. Prehľad komponentov

Časť **Prehľad súčastí** sa nachádza v strede [používateľského rozhrania AVG](#). Táto časť je rozdelená na dve oblasti:

- Prehľad všetkých nainštalovaných súčastí, ktorý je tvorený panelom s ikonami súčastí a informáciou o tom, či je príslušná súčasť zapnutá alebo vypnutá.
- Popis zvolenej súčasti

V programe **AVG 9 Anti-Virus plus Firewall** sa v časti **Prehľad súčastí** nachádzajú informácie o nasledujúcich súčastiach:

- **Anti-Virus** chráni pred vírusmi, ktoré sa pokúšajú preniknúť do vášho počítača – [podrobnosti >>](#).
- **Anti-Spyware** prehľadáva aplikácie na pozadí, keď ich spúšťate – [podrobnosti >>](#)
- **Firewall** kontroluje, akým spôsobom si počítač vymieňa dáta s ostatnými počítačmi na internete alebo v miestnej sieti – [podrobnosti >>](#)
- **Link Scanner** kontroluje výsledky vyhľadávania zobrazené v internetovom prehliadači – [podrobnosti >>](#)
- **Anti-Rootkit** deteguje programy a technológie, ktoré sa pokúšajú zamaskovať škodlivý kód – [podrobnosti >>](#)
- **E-mail Scanner** kontroluje všetky prichádzajúce a odchádzajúce správy, či neobsahujú vírusy – [podrobnosti >>](#)
- **Licencia** informuje o čísle, type a dátume expirácie licencie – [podrobnosti >>](#)
- **Webový štít** kontroluje všetky dáta prevzaté internetovým prehliadačom – [podrobnosti >>](#)
- **Rezidentný štít** beží na pozadí a prehľadáva kopírované, otvárané a ukladané súbory – [podrobnosti >>](#)
- **Update Manager** riadi všetky aktualizácie programu AVG – [podrobnosti >>](#)

Jedným kliknutím na ikonu ktorejkoľvek súčasti zvýrazníte súčasť v prehľade súčastí. Zároveň sa objaví popis základných funkcií komponentu v spodnej časti používateľského rozhrania. Dvakrát kliknite na ikonu pre otvorenie vlastného rozhrania

komponentu so zoznamom základných štatistických údajov.

Kliknutím pravým tlačidlom na ikonu súcasti otvorte kontextovú ponuku; okrem toho, že sa otvorí grafické rozhranie súcasti, môžete použiť aj možnosť **Ignorovať stav súcasti**. Zvoľte túto možnosť, ak ste si vedomý [chybového stavu súcasti](#), ale z nejakého dôvodu si želáte nechať program AVG v tomto stave a nechcete byť informovaný pomocou [ikony na paneli úloh](#).


7.5. Štatistika

Časť **Štatistika** sa nachádza v ľavej spodnej časti [Používateľského rozhrania AVG](#). Uvádza informácie o činnosti programu:

- **Posledné vyhľadávanie** - poskytuje dátum, kedy bolo vykonané posledné vyhľadávanie
- **Posledná aktualizácia** - uvádza dátum, kedy bola spustená posledná aktualizácia.
- **Vírusová databáza** - informuje vás o aktuálne nainštalovanej verzii vírusovej databázy
- **Verzia AVG** - informuje vás o nainštalovanej verzii AVG (*číslo je v tvare 9.0.xx, kde 9.0 je verzia línie produktov a xx predstavuje číslo buildu*)
- **Licencia končí** - poskytuje dátum ukončenia vašej licencie AVG

7.6. Ikona systémového pozadia

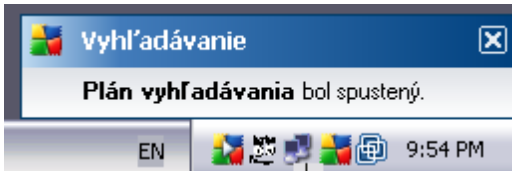
Ikona na paneli úloh (na paneli úloh operačného systému Windows) informuje o aktuálnom stave produktu **AVG 9 Anti-Virus plus Firewall**. Vždy sa nachádza na paneli úloh bez ohľadu na skutočnosť, či je hlavné okno programu AVG otvorené alebo zatvorené.

Farebná  **ikona na paneli úloh**) informuje, že všetky súcasti AVG sú zapnuté a úplne funkčné. Ikona AVG na paneli úloh je farebná aj v prípade, ak je program AVG v chybovom stave, ale tejto situácii ste si vedomý a vedome ste sa rozhodli [ignorovať stav súcasti](#).

Ikona s výkřičníkom  informuje o výskyte problému (*vypnutá súcast, chybový stav a pod.*). Dvojitým kliknutím na **ikonu na paneli úloh** otvorte hlavné okno, ktoré vám umožní zmeniť nastavenia súcasti.

Ikona na paneli úloh ďalej informuje o prebiehajúcich aktivitách produktu AVG a

možných zmenách stavu programu (napr. automatickom spustení naplánovaného prehľadávania alebo aktualizácie, prepnutí profilu súčasti Firewall, zmene stavu súčasti, výskyte chybového stavu...) pomocou prekrývacieho okna, ktoré sa otvorí na ikone AVG na paneli úloh:



Ikona na paneli úloh sa môže použiť aj ako rýchly odkaz na sprístupnenie hlavného okna programu AVG – dvakrát kliknite na túto ikonu. Kliknutím pravým tlačidlom myši na **ikonu na paneli úloh** sa otvorí krátka kontextová ponuka s nasledujúcimi možnosťami:

- **Otvoriť používateľské rozhranie AVG:** Kliknutím na túto položku sa otvorí [používateľské rozhranie AVG](#)
- **Aktualizovať:** Spustí okamžitú [aktualizáciu](#)

8. Komponenty AVG

8.1. Anti-Virus

8.1.1. Anti-Virus Princípy

Zariadenie na vyhľadávanie antivírusového softvéru prehľadáva všetky súbory a aktivitu súborov (otváranie/zatváranie súborov, atď.) a hľadá známe vírusy. Každý detekovaný vírus sa zablokuje, aby nemohol vykonávať žiadnu činnosť, a potom sa vymaže alebo sa dostane do karantény. Väčšina antivírusových softvérov takisto používa heuristické vyhľadávanie, kedy sa v súboroch vyhľadávajú typické vlastnosti vírusov, takzvané vírusové podpisy. To znamená, že antivírusová kontrola dokáže detekovať nový, neznámy vírus, ak tento nový vírus obsahuje isté typické vlastnosti existujúcich vírusov.

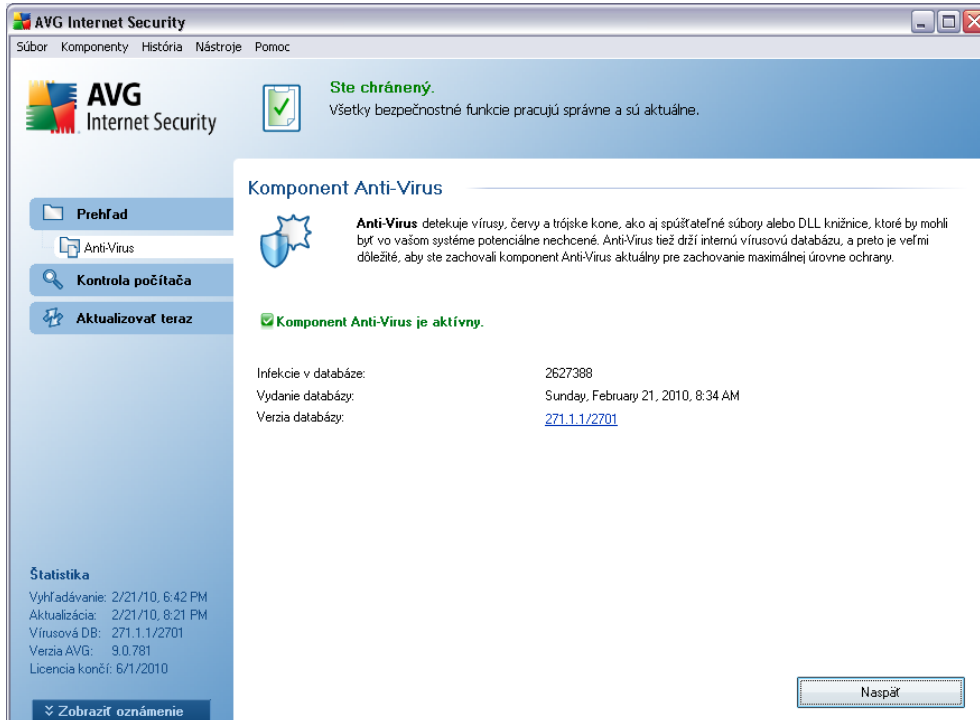
Dôležitou funkciou antivírusovej ochrany je, že sa v počítači nemôže spustiť žiadny známy vírus!

Kedže len jedna jediná technológia by mohla zabrániť detekcii alebo identifikácii vírusu, **Anti-Virus** spája viacero technológií pre zabezpečenie ochrany vášho počítača pred vírusmi:

- Vyhľadávanie – hľadanie špecifických reťazcov, 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 daný vírus / danú skupinu vírusov

AVG dokáže tiež analyzovať a detekovať spúšťateľné aplikácie alebo knižnice DLL, ktoré by mohli byť v systéme potenciálne nechcené. Takéto hrozby nazývame Potenciálne nežiaduce programy (rôzne druhy spywaru, adwaru, atď.). AVG ďalej vyhľadáva podozrivé položky v systémových registroch, dočasné internetové súbory a sledovacie súbory cookies a umožňuje vám spracovať všetky potenciálne škodlivé položky rovnako ako každú infekciu.

8.1.2. Rozhranie Anti-Virus



Rozhranie súčasti **Anti-Virus** poskytuje niektoré základné informácie o funkciách súčasti, aktuálnom stave súčasti (*Súčasť Anti-Virus je aktívna.*) a základnú štatistiku súčasti **Anti-Virus**:

- **Definície infekcií** – Číslo uvádza počet vírusov definovaných v aktuálnej verzii vírusovej databázy.
- **Najnovšia aktualizácia databázy** – Informuje, kedy a v akom case sa vírusová databáza naposledy aktualizovala.
- **Verzia databázy** – Uvádza číslo najnovšej verzie vírusovej databázy a toto číslo narastá s každou aktualizáciou vírusovej databázy.

V rozhraní tejto súčasti sa nachádza len jedno ovládacie tlačidlo (**Naspäť**) – Stlačením tohto tlačidla sa vrátite na základné [používateľské rozhranie AVG](#) (prehľad súčastí).

Poznámka: Dodávateľ softvéru nastavil všetky súčasti AVG takým spôsobom, aby fungovali optimálne. Nemente konfiguráciu AVG, ak k tomu nemáte závažný dôvod. Všetky zmeny nastavení by mali vykonávať len skúsení používatelia. Ak chcete zmeniť

konfiguráciu programu AVG, zvolte položku v ponuke programu **Nástroje/Rozšírené nastavenia** a zmente konfiguráciu v novo otvorenom dialógovom okne [Rozšírené nastavenia AVG](#).

8.2. Anti-Spyware

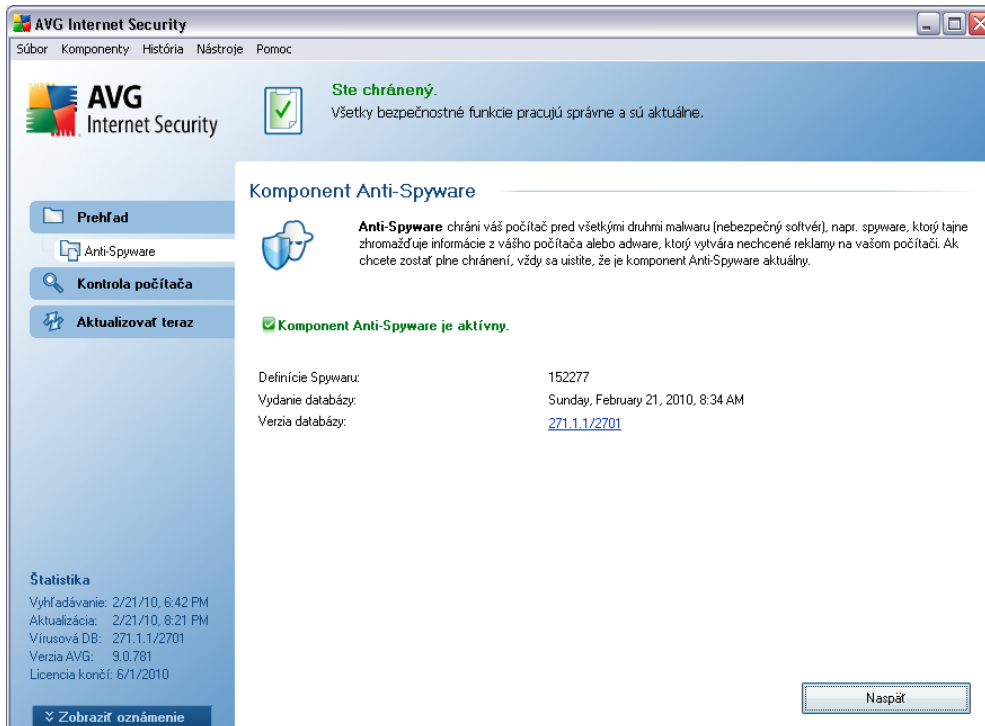
8.2.1. Anti-Spyware Princípy

Základná definícia spywaru: Spyware je druh škodlivého softvéru, t. j. softvér, ktorý zhromažďuje informácie z počítača bez vedomia alebo súhlasu jeho používateľa. Niektoré aplikácie typu spyware môžu byť nainštalované aj zámerne a často zobrazujú reklamu, prekryvacie okná, alebo obsahujú rôzne druhy nepríjemného softvéru.

Najbežnejším zdrojom infekcie sú v súčasnosti webové stránky s potenciálne nebezpečným kódom. Škodlivý kód sa šíri aj inými metódami prenosu, napr. cez e-mail alebo pomocou červov a vírusov. Základná ochrana spočíva v používaní prehľadávacích programov bežiacich na pozadí (tzv. **Anti-Spyware**), ktoré fungujú ako rezidentný štít a prehľadávajú aplikácie na pozadí, keď ich spúšťate.

Existuje aj potenciálne riziko, že sa škodlivý program dostal do vášho počítača pred nainštalovaním programu AVG, resp. že ste zabudli nainštalovať [najnovšiu databázu a programové aktualizácie](#) používaného programu **AVG 9 Anti-Virus plus Firewall**. Z tohto dôvodu vám AVG umožňuje vykonať kompletne vyhľadávanie programov malware/spyware vo vašom počítači s použitím funkcie vyhľadávania. Detekuje aj spiace a neaktívny malware, teda malware, ktorý bol stiahnutý, ale ešte nebol aktivovaný.

8.2.2. Rozhranie Anti-Spyware



Rozhranie súčasti **Anti-Spyware** poskytuje stručný prehľad funkcií súčasti, informácie o aktuálnom stave súčasti (*Súčasť Anti-Spyware je aktívna.*) a základnú štatistiku súčasti **Anti-Spyware**:

- **Definície spywaru** – Číslo informuje o počte vzoriek spywaru definovaných v najnovšej verzii databázy spywaru.
- **Najnovšia aktualizácia databázy** – Informuje, kedy a v akom case bola databáza spywaru aktualizovaná.
- **Verzia databázy** – Informuje o čísle najnovšej verzie databázy spywaru a toto číslo rastie s každou aktualizáciou vírusovej databázy.

V rozhraní tejto súčasti sa nachádza len jedno ovládacie tlačidlo (**Naspät**) – Stlačením tohto tlačidla sa vrátite na základné [používateľské rozhranie AVG](#) (prehľad súčastí).

Poznámka: Dodávateľ softvéru nastavil všetky súčasti AVG takým spôsobom, aby fungovali optimálne. Nemente konfiguráciu AVG, ak k tomu nemáte závažný dôvod. Všetky zmeny nastavení by mali vykonávať len skúsení používatelia. Ak chcete zmeniť

konfiguráciu programu AVG, zvolte položku v ponuke programu **Nástroje/Rozšírené nastavenia** a zmeníte konfiguráciu v novo otvorenom dialógovom okne [Rozšírené nastavenia AVG](#).

8.3. Anti-Rootkit

Rootkit je program, ktorý sa používa na prevzatie základnej kontroly nad počítačovým systémom bez povolenia vlastníka systému a jeho právoplatných správcov. Prístup k hardvéru sa väčšinou nepožaduje, pretože rootkit je určený na to, aby sa zmocnil kontroly nad operačným systémom spusteným na hardvéri. Rootkity sa obvyčajne snažia zakrývať svoju prítomnosť v systéme formou nižšej verzie alebo únikom pred štandardnými bezpečnostnými mechanizmami operačného systému. Často ide aj o Trójske kone, ktoré mýlia používateľov a tí si myslia, že je spúšťanie systému bezpečné. Metódy používané na splnenie tejto úlohy zahŕňajú utajenie bežiacich procesov pred sledovacími programami alebo skrývanie súborov alebo systémových údajov pred operačným systémom.

8.4. Firewall

Firewall je systém, ktorý vynucuje politiku riadenia prístupu medzi dvomi alebo viacerými sietami blokovaním/povolením prenosov. Každý firewall obsahuje sadu pravidiel, ktoré chránia internú sieť pred útokmi zvonka (obvyčajne z Internetu) a riadi komunikáciu na každom sieťovom porte. Komunikácia sa vyhodnotí podľa zadefinovaných pravidiel, a potom sa buď povolí alebo zakáže. Ak firewall zistí nejaké pokusy o vniknutie do systému, zablokuje tento pokus a nedovolí narušiteľovi vstúpiť do počítača.

Súčasť Firewall je nastavená takým spôsobom, aby umožňovala alebo blokovala internú/externú komunikáciu (oboma smermi, dnu aj von) na definovaných portoch a pre definované softvérové aplikácie. Napríklad, bezpečnostná brána firewall sa môže nastaviť tak, aby umožňovala tok webových dát dnu a von len pri použití programu Microsoft Explorer. Každý pokus o prenesenie webových dát iným prehliadacom bude zablokovaný.

Firewall chráni informácie, ktoré vás môžu osobne identifikovať, pred odoslaním z vášho počítača bez vášho povolenia. Kontroluje ako váš počítač vymieňa údaje s ostatnými počítačmi na Internete alebo v lokálnej sieti. V rámci organizácie Firewall takisto chráni samostatné počítače pred útokmi interných používateľov na ostatné počítače v sieti.

Odporúčanie: Vo všeobecnosti sa neodporúča používať viac ako jednu bezpečnostnú bránu firewall na tom istom počítači. Zabezpečenie počítača nie je vyššie, ak nainštalujete viac firewallov. Pravdepodobnejšie je skôr to, že medzi týmito dvomi aplikáciami sa vyskytne nejaký konflikt. Preto vám odporúčame používať len jeden firewall na vašom počítači a deaktivovať všetky ostatné firewally, čím sa eliminuje

riziko možného konfliktu a s tým spojených problémov.

8.4.1. Princípy Firewallu

V AVG komponent **Firewall** riadi všetky prenosy na každom sieťovom porte vášho počítača. Na základe zadefinovaných pravidiel **Firewall** vyhodnocuje aplikácie, ktoré sa buď spúšťajú na vašom počítači (a chcú sa pripojiť k Internetu/lokálnej sieti) alebo aplikácie, ktoré sa približujú k vášmu počítaču zvonku a snažia sa na váš počítač pripojiť. Pri každej z týchto aplikácií **Firewall** potom buď povolí alebo zakáže komunikáciu na sieťových portoch. Ak je aplikácia neznáma (teda nemá žiadne zadefinované pravidlá **Firewall**), **Firewall** sa vás štandardne spýta, či chcete blokovat alebo povoliť tento pokus o komunikáciu.

Poznámka: AVG Firewall nie je určený pre serverové platformy!

Co dokáže AVG Firewall:

- Povolit alebo blokovat komunikacné pokusy známych [aplikácií](#) automaticky alebo vás požiadať o potvrdenie
- Použiť úplné [profily](#) s vopred definovanými pravidlami, podľa vašich potrieb.
- [Prepnúť profil](#) automaticky, keď sa pripájate na rôzne siete alebo používate rôzne sieťové karty.

8.4.2. Profily Firewallu

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 súčasťou **Firewall** je špeciálna konfigurácia súčasťou **Firewall** a program umožňuje použiť niekoľko takýchto vopred definovaných konfigurácií.

Definované profily

- **Povolit všetky:** Systémový profil súčasťou **Firewall**, ktorý vopred nastavil výrobca, a ktorý je vždy prítomný. Ak tento profil je aktivovaný, všetka sieťová komunikácia je povolená a nie sú uplatňované žiadne pravidlá bezpečnostnej politiky, rovnako ako keby ochrana pomocou **Firewallu** bola vypnutá (t. j. všetky aplikácie sú povolené, ale pakety sú stále kontrolované – na úplné vypnutie filtrovania je potrebné vypnúť bezpečnostnú bránu firewall).

Tento systémový profil sa nedá kopírovať, vymazať a jeho nastavenia sa nedajú meniť.

- **Blokovať všetky:** Systémový profil súčasťou **Firewall**, ktorý vopred nastavil výrobca, a ktorý je vždy prítomný. Keď je tento profil aktivovaný, všetka sieťová komunikácia sa zablokuje a počítač nie je dostupný z vonkajších sietí, ani nemôže komunikovať smerom von. Tento systémový profil sa nedá kopírovať, vymazať a jeho nastavenia sa nedajú meniť.
- **Vlastné profily:**
 - **Priamo pripojený na internet:** Nastavenie vhodné pre bežné domáce stolové počítače pripojené priamo na internet, alebo notebooky pripájajúce sa na internet mimo zabezpečenej podnikovej siete. Zvoľte túto možnosť, ak sa pripájate z domu, alebo ste pripojení do malej podnikovej siete bez centrálného riadenia. Túto možnosť zvoľte aj v prípade, ak cestujete a s notebookom sa pripájate z rôznych neznámych a prípadne nie zabezpečených miest (*internetovej kaviarne, hotelovej izby a pod.*). Vytvorí sa prísnejšie pravidlá, keďže sa predpokladá, že tieto počítače nepoužívajú žiadnu ďalšiu ochranu, a preto vyžadujú maximálnu ochranu.
 - **Počítač v doméne:** Nastavenie vhodné pre počítače v miestnej sieti, napr. škole alebo podnikovej sieti. Predpokladá sa, že sieť je chránená ďalšími prostriedkami, aby sa mohla použiť nižšia úroveň zabezpečenia ako pri samostatnom počítači.
 - **Malé domáce alebo kancelárske siete:** Možnosť vhodná pre počítače v malej sieti, napr. domácnosti alebo malom podniku, obvyčajne ide len o niekoľko vzájomne prepojených počítačov bez „centrálného“ správcu.

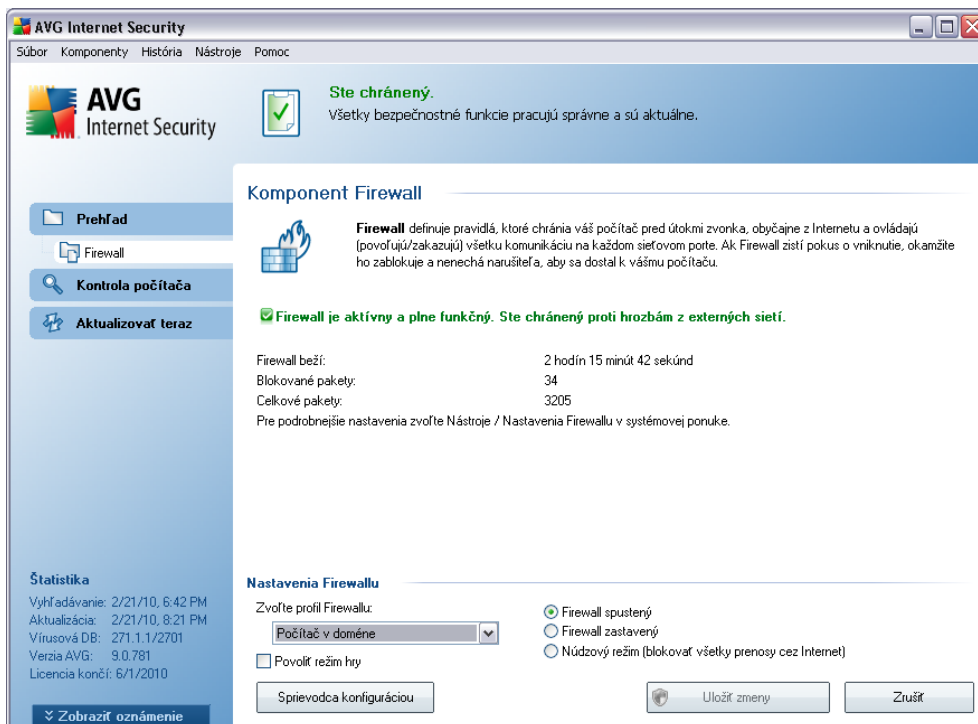
Prepínanie profilov

Funkcia Prepínanie profilov umožňuje automaticky prepnúť súčasť **Firewall** na definovaný profil pri použití konkrétnej sieťovej karty, alebo keď je počítač pripojený na konkrétny typ siete. Ak neboli sieťovej oblasti doposiaľ pridelené žiadne profily, pri ďalšom pripojení do tejto oblasti súčasť **Firewall** otvorí dialógové okno, ktoré vás požiada, aby ste pridelili profil.

Dialógové okno **Profily oblastí a sieťových kariet** vám umožní prideliť profily rozhraniám všetkých miestnych sietí alebo oblastí a zadať ďalšie nastavenia. Zároveň vám umožní túto funkciu aj vypnúť, ak ju nechcete používať (*potom sa pri každom type pripojenia použije predvolený profil*).

Túto funkciu používajú obyčajne 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 pravdepodobne nikdy nevyužijete.

8.4.3. Rozhranie Firewallu



Rozhranie súčasti **Firewall** poskytuje niektoré základné informácie o jej funkcionalite a stručný prehľad štatistických informácií o činnosti **bezpečnostnej brány**:

- **Súčasť Firewall bola zapnutá:** Čas uplynutý od spustenia súčasti Firewall.
- **Blokovane pakety:** Počet blokovanych paketov z celkového množstva skontrolovaných paketov.
- **Celkové pakety:** Počet všetkých paketov skontrolovaných počas zapnutia súčasti Firewall.

Základná konfigurácia súčastí

- **Zvolit profil súcasti Firewall:** V rozbalovacej ponuke zvolte jeden z uvedených profilov – dva profily sú použiteľné vždy (*predvolené profily s názvom **Povolit všetky** a **Blokovať všetky***), ostatné profily boli pridané ručne pri zmene profilu v dialógovom okne **Profily** v časti **Nastavenia súcasti Firewall**.
- **Povolit režim hrania:** Označte túto možnosť, aby počas spúšťania aplikácií na celú obrazovku (hier, prezentácií v programe PowerPoint atď.) súcast **Firewall** nezobrazila dialógové okná s otázkou, či chcete povoliť alebo blokovat komunikáciu pre neznáme aplikácie. V prípade, že sa neznáma aplikácia pokúsi komunikovať v sieti v danom case, **Firewall** automaticky povolí alebo zablokuje tento pokus podľa nastavení v aktuálnom profile.
- **Stav súcasti Firewall:**
 - **Súcast Firewall zapnutá:** Zvolte túto možnosť, ak chcete povoliť komunikáciu tým aplikáciám, ktoré sú nastavené ako „povolené“ v skupine pravidiel definovaných vo zvolenom profile súcasti **Firewall**.
 - **Súcast Firewall vypnutá:** Táto možnosť úplne vypne **Firewall**, všetky sieťové prenosy sa povolia, ale nebudú sa kontrolovať!
 - **Núdzový režim (blokovat všetky prenosy v internete):** Zvolte túto možnosť, ak chcete blokovat prenosy na všetkých sieťových portoch; **Firewall** stále beží, ale všetky prenosy v sieti sú zastavené.

Poznámka: Dodávateľ softvéru nastavil všetky súcasti AVG takým spôsobom, aby fungovali optimálne. Nemente konfiguráciu AVG, ak k tomu nemáte závažný dôvod. Všetky zmeny nastavení by mali vykonávať len skúsení užívatelia. Ak potrebujete zmeniť konfiguráciu súcasti Firewall, zvolte položku **Nástroje/Nastavenia súcasti Firewall** v hlavnej ponuke programu a zmeňte konfiguráciu súcasti Firewall v novo otvorenom dialógovom okne **Nastavenia súcasti Firewallu**.

Ovládacie tlačidlá

- **Sprievodca konfiguráciou:** Stlačením tohto tlačidla sa otvorí príslušné dialógové okno (*používa sa v rámci procesu inštalácie*) s názvom **Výber spôsobu používania počítača**, ktoré umožňuje definovať konfiguráciu súcasti **Firewall**.
- **Uložiť zmeny:** Stlačením tohto tlačidla sa uložia a použijú všetky zmeny urobené v tomto dialógovom okne.

- **Zrušit:** Stlačením tohto tlačidla sa vrátite na hlavné [používateľské rozhranie AVG](#) (prehľad súčastí)

8.5. Kontrola pošty

Jeden z najbežnejších zdrojov vírusov a trójskych konov 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 vyplňajú osobné údaje (*napr. e-mailové adresy*), sú vo zvýšenej miere vystavení útokom cez e-mail. Spoločnosti obvyčajne využívajú hromadné emailové účty a používajú antispamové filtre, atď., aby toto riziko znížili.

8.5.1. Princípy Kontroly pošty

Súčasť **E-mail Scanner** automaticky kontroluje prichádzajúce/odchádzajúce e-maily. Môže sa používať s poštovými aplikáciami, ktoré nemajú vlastný zásuvný modul v programe AVG (*napr. Outlook Express, Mozilla, Incredimail a pod.*).

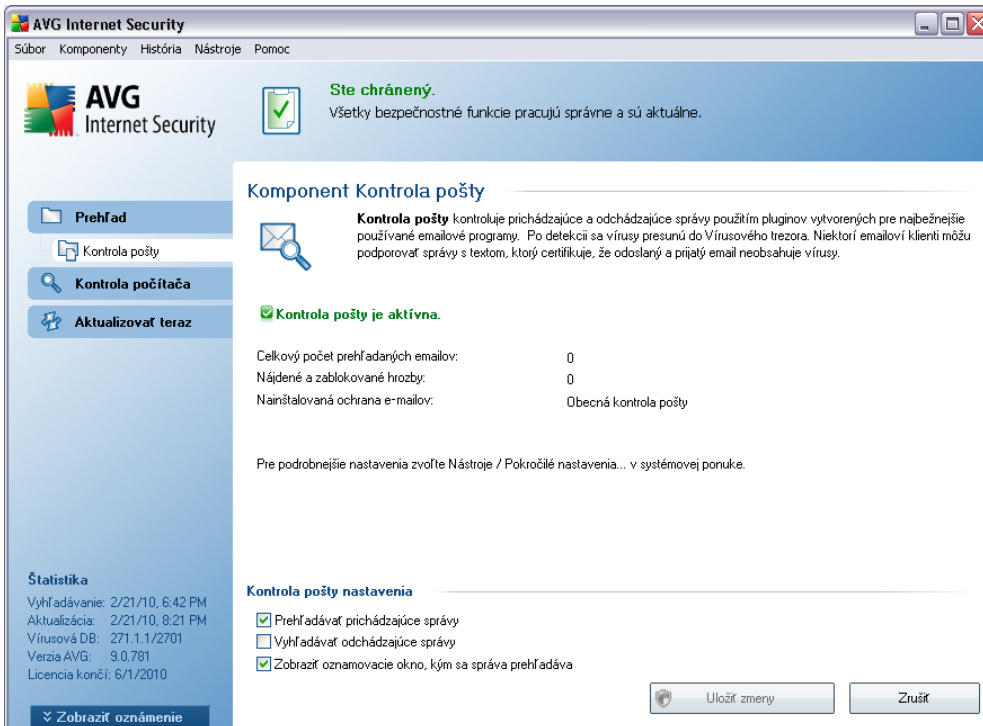
Pocas [inštalácie programu AVG](#) sa vytvoria automatické servery na kontrolu e-mailov: jeden na kontrolu prichádzajúcich e-mailov a druhý na kontrolu odchádzajúcich e-mailov. Pomocou týchto dvoch serverov sa e-maily automaticky kontrolujú na portoch 110 a 25 (*štandardné porty pre posielanie/prijímanie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

E-mail Scanner pôsobí ako rozhranie medzi poštovou aplikáciou a poštovými servermi na internete.

- **Prichádzajúca pošta:** Pocas prijímania správy zo servera, súčasť **E-mail Scanner** otestuje správu z hľadiska prítomnosti vírusov, odstráni infikované prílohy a pridá certifikáciu. Zistené vírusy sa ihneď uložia do karantény do [vírusového trezora](#). Potom sa správa prepošle do emailového klienta.
- **Odchádzajúca pošta:** Správa sa pošle z poštovej aplikácie do súčasti E-mail Scanner, 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*).

Poznámka: Súčasť AVG E-mail Scanner nie je prispôsobená na použitie so serverovými platformami!

8.5.2. Rozhranie Kontroly pošty



V dialógovom okne súčasti **E-mail Scanner** sa nachádza stručný text opisujúci funkcionálnosť súčasti, informácie o jej aktuálnom stave (*Súčasť E-mail Scanner je zapnutá.*) a nasledujúca štatistika:

- **Celkový počet prehládaných e-mailov:** Kolko e-mailových správ sa prehládalo od posledného spustenia súčasti **E-mail Scanner** (v prípade potreby túto hodnotu môžete vynulovať; napr. na štatistické účely – Vynulovať hodnotu).
- **Nájdene a zablokované hrozby:** Informuje o počte infekcií zistených v e-mailových správach od posledného spustenia súčasti **E-mail Scanner**.
- **Nainštalovaná ochrana e-mailov:** Informácie o konkrétnom zásuvnom module na ochranu e-mailov v predvolenej nainštalovanej poštovej aplikácii.

Základná konfigurácia súčastí

V spodnej časti tohto dialógového okna sa nachádza časť s názvom **Nastavenia**

súcasti E-mail Scanner, kde môžete zmeniť niektoré základné funkcie súcasti:

- **Kontrolovať prichádzajúce správy:** Označte túto možnosť, ak sa majú kontrolovať prítomnosť vírusov vo všetkých e-mailoch doručených do vašej e-mailovej schránky. Táto možnosť je štandardne zapnutá a odporúčame vám nemeniť toto nastavenie!
- **Kontrolovať odchádzajúce správy:** Označte túto možnosť, ak sa má kontrolovať prítomnosť vírusov vo všetkých e-mailoch poslaných z vašej e-mailovej schránky. Možnosť je štandardne vypnutá.
- **Zobraziť oznamovaciu ikonu počas kontroly e-mailov:** Označte túto možnosť, ak chcete byť informovaný zobrazením oznamovacieho dialógového okna nad ikonou AVG na paneli úloh počas kontroly pošty súcastou **E-mail Scanner**. Táto možnosť je štandardne zapnutá a odporúčame vám nemeniť toto nastavenie!

Rozšírená konfigurácia súcasti **E-mail Scanner** sa otvára výberom položky **Nástroje/Rozšírené nastavenia** v ponuke programu; odporúča sa však, aby rozšírenú konfiguráciu používali len skúsení používatelia!

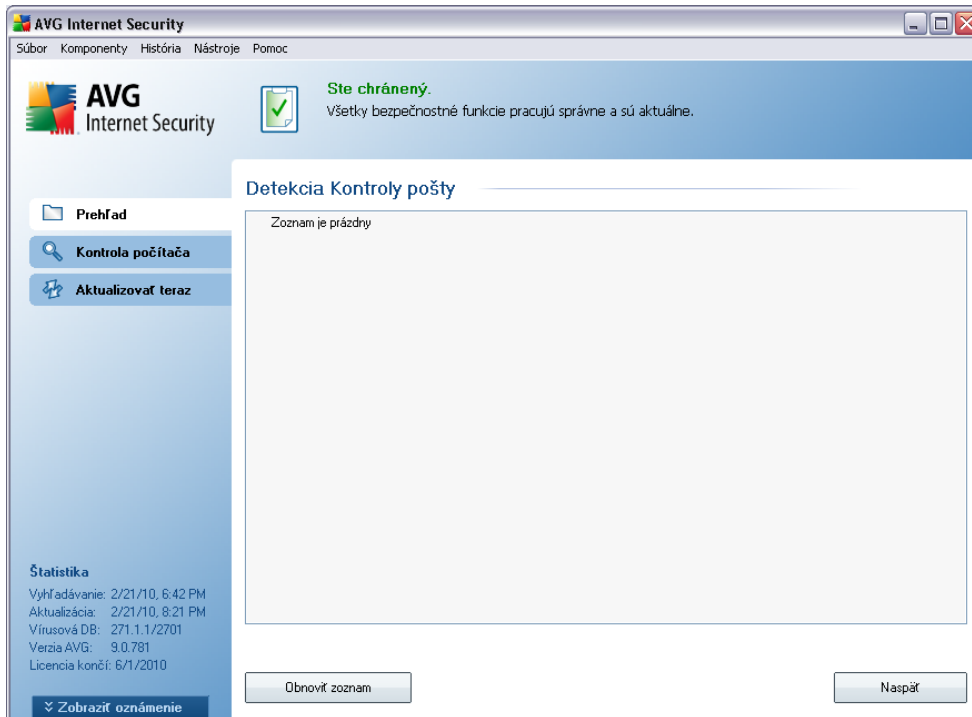
Poznámka: Dodávateľ softvéru nastavil všetky súcasti AVG takým spôsobom, aby fungovali optimálne. Nemente konfiguráciu AVG, ak k tomu nemáte závažný dôvod. Všetky zmeny nastavení by mali vykonávať len skúsení používatelia. Ak chcete zmeniť konfiguráciu programu AVG, zvolte položku v ponuke programu **Nástroje/Rozšírené nastavenia** a zmeňte konfiguráciu v novo otvorenom dialógovom okne **Rozšírené nastavenia AVG**.

Ovládacie tlačidlá

V rozhraní súcasti **E-mail Scanner** sa nachádzajú nasledujúce 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 hlavné [používateľské rozhranie AVG](#) (prehľad súcastí).

8.5.3. Detekcia Kontroly pošty



V dialógovom okne **Detegovanie súčasťou E-mail Scanner** (otvára sa pomocou možnosti *História/Detegovanie súčasťou E-mail Scanner*) sa zobrazí zoznam všetkých hrozieb zistených súčasťou **E-mail Scanner**. Pre každý detegovaný objekt sú k dispozícii nasledujúce informácie:

- **Infekcia**: Opis (prípadne aj názov) detegovaného objektu.
- **Objekt**: Umiestnenie objektu.
- **Výsledok**: Akcia urobená na detegovanom objekte.
- **Cas detegovania**: Dátum a čas detegovania podozrivého objektu.
- **Typ objektu**: Typ detegovaného objektu.

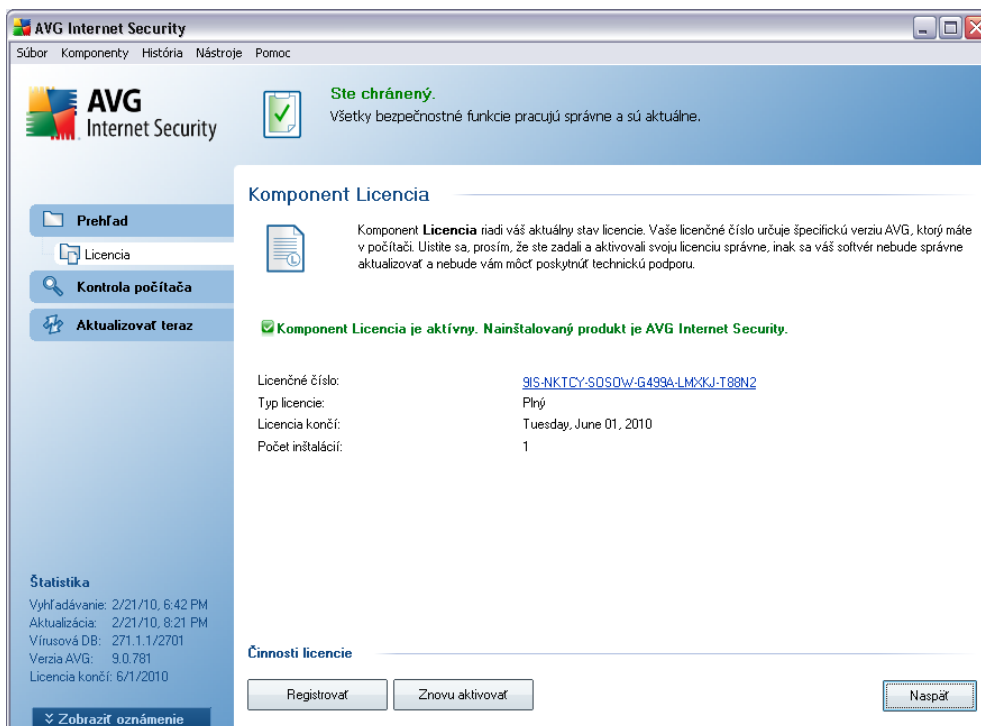
V spodnej časti dialógového okna pod zoznamom sa nachádzajú informácie o celkovom počte detegovaných objektov. Ďalej môžete exportovať celý zoznam detegovaných objektov do súboru (**Exportovať zoznam do súboru**) a vymazať všetky záznamy o detegovaných objektoch (**Vyprázdniť zoznam**).

Ovládacie tlačidlá

V rozhraní **Detegovanie súcastou E-mail Scanner** sa nachádzajú nasledujúce tlačidlá:

- **Obnovit zoznam:** Aktualizuje zoznam zistených hrozieb.
- **Naspät:** Prepne naspät na hlavné [používateľské rozhranie AVG](#) (prehľad súcastí).

8.6. Licencia



V rozhraní súcasti **Licencia** sa nachádza stručný prehľad funkcionality súcasti, informácie o jej aktuálnom stave (*Súcast Licencia je zapnutá.*) a nasledovné informácie:

- **Licenčné číslo:** Presné znenie vášho licenčného čísla. Licenčné číslo sa musí zadať úplne presne a tak, ako je uvedené. Preto vám odporúčame vždy použiť metódu „kopírovať a prilepiť“ pri každej manipulácii s licenčným číslom.

- **Typ licencie:** Informuje o type nainštalovaného produktu.
- **Platnosť licencie vyprší:** Tento dátum informuje o dobe platnosti vašej licencie. Ak chcete aj naďalej používať **AVG 9 Anti-Virus plus Firewall** aj po tomto dátume, musíte si obnoviť licenciu. [Obnovenie licencie môžete urobiť online](http://www.avg.com/) na webových stránkach AVG (<http://www.avg.com/>).
- **Pocet inštalácií:** Na koľko počítačov sa môže produkt **AVG 9 Anti-Virus plus Firewall** nainštalovať.

Ovládacie tlačidlá

- **Registrovať:** Program sa pripojí na registracnú stránku na webových stránkach AVG (<http://www.avg.com/>). Vyplňte svoje registracné údaje; nárok na bezplatnú technickú podporu získajú len zákazníci, ktorí si svoj produkt AVG zaregistrujú.
- **Znovu aktivovať:** Otvorí dialógové okno **Aktivácia produktu AVG** s údajmi, ktoré ste zadali v dialógovom okne **Prispôbiť AVG** v **processe inštalácie**. Toto dialógové okno sa používa na vloženie licencného čísla, buď pri nahradení predajného čísla (*čísla, s ktorým ste nainštalovali AVG*), alebo pri nahradení starého licencného čísla (*napr. pri upgradovaní na nový produkt AVG*).

Poznámka: Ak používate skúšobnú verziu produktu **AVG 9 Anti-Virus plus Firewall**, tlačidlá sa zobrazia v podobe **Kúpiť teraz** a **Aktivovať** a umožnia vám ihneď zakúpiť úplnú verziu programu. Ak je produkt **AVG 9 Anti-Virus plus Firewall** nainštalovaný pomocou predajného čísla, tlačidlá sa zobrazia v podobe **Registrovať** a **Aktivovať**.

- **Naspät:** Stlačením tohto tlačidla sa otvorí hlavné [používateľské rozhranie programu AVG](#) (prehľad súčastí).

8.7. Link Scanner

8.7.1. Pravidlá pre Link Scanner

Súčasť **LinkScanner** poskytuje ochranu pred webovými stránkami, ktoré sa snažia nainštalovať škodlivý softvér do počítača cez webový prehliadač a jeho zásuvné moduly. Súčasťou technológie **LinkScanner** sú dve funkcie, [AVG Search-Shield](#) a [AVG Active Surf-Shield](#):

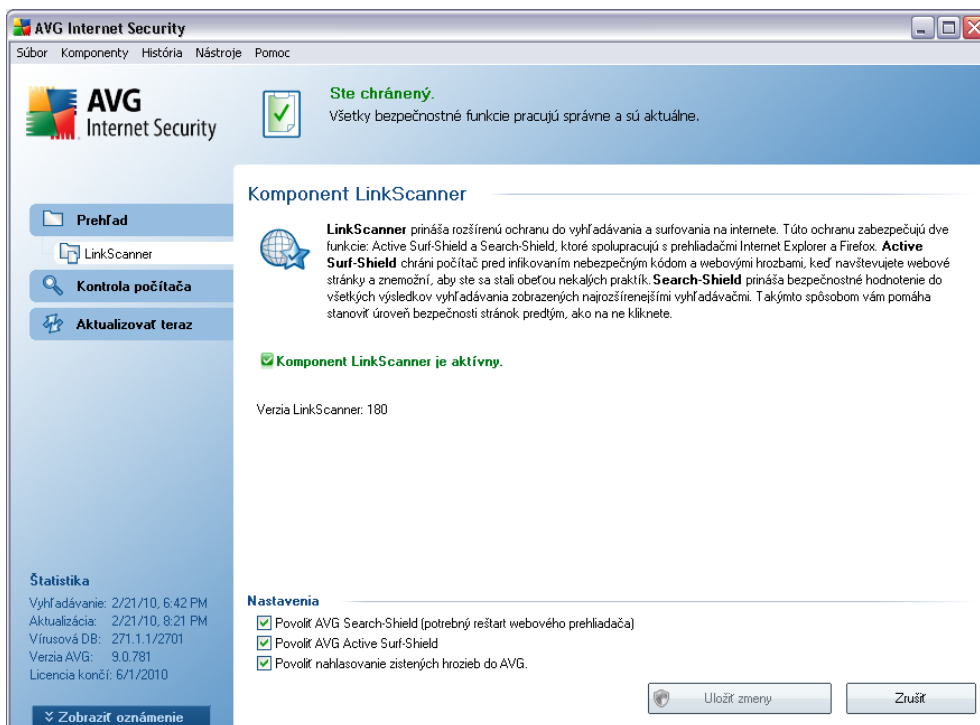
- **AVG Search Shield** používa zoznam webových stránok (*adres URL*), ktoré boli označené za nebezpečné. Pri vyhľadávaní pomocou vyhľadávacov Google, Yahoo!, Bing, Baidu, Altavista alebo Yandex sa všetky výsledky vyhľadávania skontrolujú podľa tohto zoznamu a zobrazí sa ikona verdiktu (*v súvislosti s výsledkami zistenými vyhľadávacom Yahoo! sa zobrazí len ikona verdiktu „škodlivé webové stránky“*). Rovnako ak napíšete adresu priamo do prehliadaca, kliknete na odkaz na webové stránky alebo napr. v e-mailovej správe, automaticky sa skontroluje a v prípade potreby zablokuje.
- **AVG Active Surf-Shield** prehľadáva obsah navštívených webových stránok bez ohľadu na ich adresu. Dokonca aj keď **AVG Search Shield** nezachytí niektoré webové stránky (*napr. ak sa vytvorí nové škodlivé webové stránky, alebo ak pôvodne čisté webové stránky teraz obsahujú škodlivý kód*), **AVG Active Surf-Shield** ich zachytí a zablokuje v momente, keď sa ich pokúsite navštíviť.

Poznámka: Súčasť AVG Link Scanner nie je prispôsobená na použitie so serverovými platformami!

8.7.2. Rozhranie Link Scanner

Súčasť **LinkScanner** pozostáva z dvoch častí, ktoré môžete zapnúť/vypnúť v rozhraní **súčasťi LinkScanner**:

V rozhraní súčasti **LinkScanner** sa nachádza stručný opis funkcionality súčasti a informácie o jej aktuálnom stave (*Súčasť LinkScanner je zapnutá.*). Ďalej sa v nom nachádzajú informácie o čísle najnovšej verzie databázy súčasti **LinkScanner** (*Verzia databázy LinkScanner*).




V spodnej časti dialógového okna môžete zmeniť niekoľko nastavení:


- **Zapnúť súčasť *AVG Search-Shield* (štandardne zapnuté):** Informačné ikony s odporúčaniami pre výsledky vyhľadávania zistené vyhľadávacom Google, Yahoo!, Bing, Baidu, Yandex a Altavista a vopred skontrolované.
- **Zapnúť *AVG Active Surf-Shield* (štandardne zapnuté):** Zapnúť ochranu (v *reálnom case*) pred webovými stránkami s nebezpečným obsahom pri ich otvorení. Pripojenie na známe nebezpečné stránky a ich nebezpečný obsah sa zablokuje pri sprístupňovaní pomocou webového prehliadača (alebo inej aplikácie, ktorá používa protokol HTTP).
- **Zapnúť oznamovanie zistených hrozieb do AVG:** Označte túto položku, ak chcete povoliť oznamovanie hrozieb a zlých stránok nájdených používateľmi buď pomocou funkcie **Safe Surf** alebo **Safe Search** do databázy zhromažďujúcej informácie o škodlivých aktivitách na webe.


8.7.3. Štít vyhľadávania AVG


Ked vyhľadáte na internete so zapnutou funkciou **AVG Search-Shield**, pri všetkých výsledkoch vyhľadávania v najrozšírenejších vyhľadávacoch, akými sú napr. je Yahoo!, Google, Bing, Altavista, Yandex a pod., sa zobrazí hodnotenie úrovne nebezpečnosti resp. podozrivosti odkazov. Kontrolou týchto odkazov a oznacením zlých odkazov vás súčasť **AVG Link Scanner** upozorní ešte predtým, než kliknete na nebezpečné resp. podozrivé odkazy, takže získate istotu, že navštévujete len bezpečné webové stránky.

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

 Stránka s odkazom je bezpečná (ak použijete vyhľadávac Yahoo!, v súčasti [AVG Security Toolbar](#) sa táto ikona nezobrazí!).

 Na stránke s odkazom sa nenachádzajú hrozby, ale je do istej miery podozrivá (otázny pôvod alebo motív, a preto vám ju neodporúčame použiť na internetové nakupovanie atd.).


 Stránka s odkazom 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 s odkazom sa nachádzajú aktívne hrozby! Pre vašu vlastnú bezpečnosť vám nebude umožnené navštíviť túto stránku.

 Stránka s odkazom nie je prístupná a nedala sa prehľadať.

Nastavením kurzora nad jednotlivé ikony hodnotenia sa zobrazia podrobnosti o príslušnom odkaze. V texte sa nachádzajú ďalšie informácie o prípadnej hrozbe, adresa IP odkazu a kedy bola stránka prehľadaná programom AVG:



AVG    

Bezpečná: Táto stránka neobsahuje aktívne hrozby.

Vysvetlenie:
Môžete bezpečne pokračovať na túto stránku.
IP Adresa: 92.122.212.211
Prehľadané dňa: 02/21/10 20:02:39
(0.04 sekundy pre prehľadávanie tejto stránky)

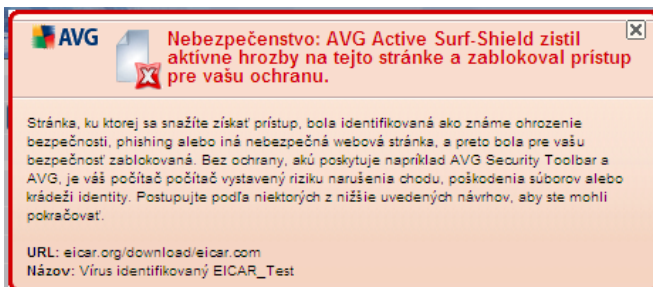
Hodnoty poskytuje AVG. Majitelia stránok by mali v prípade otázok kontaktovať AVG.

Držite krok s vývojom vďaka aktualizáciám a novinčkám o produkte AVG. Navštívte stránku produktu AVG. [Kliknite sem](#)

8.7.4. Aktívny štít surfovania AVG

Táto účinná ochrana zablokuje škodlivý kód každej webovej stránky, ktorú sa pokúšate otvoriť a zabráni jeho prevzatíu do počítača. Ak je táto funkcia zapnutá a kliknete na odkaz alebo zadáte adresu URL nebezpečných stránok, funkcia automaticky zablokuje otvorenie týchto webových stránok, aby vás chránila pred náhodným infikovaním. Je dôležité mať na pamäti, že nebezpečné webové stránky môžu infikovať váš počítač jednoducho tak, že navštívite príslušné stránky a z tohto dôvodu, keď sa pokúsíte otvoriť nebezpečné webové stránky so škodlivým kódom a inými závažnými hrozbami, súčasť **AVG Link Scanner** neumožní prehliadacu, aby tieto stránky zobrazil.

Ak narazíte na škodlivé webové stránky, **AVG Link Scanner** vás upozorní pomocou zobrazením podobnej obrazovky:



Otvorenie týchto webových stránok predstavuje vysoké riziko a neodporúča sa!

8.8. Webový štít

8.8.1. Princíp fungovania súčasti Webový štít

Webový štít je druh rezidentnej ochrany fungujúcej v reálnom čase; prehliadáva obsah navštívených webových stránok (a súborov, ktoré sa na nich môžu nachádzať) ešte predtým, než sa zobrazia vo webovom prehliadači alebo prevezmú do počítača.

Webový štít zistí prítomnosť nebezpečného kódu JavaScript na stránke, ktorú sa práve chystáte navštíviť, a zabráni zobrazeniu tejto stránky. Zároveň rozpozná škodlivý softvér, ktorý sa nachádza na tejto stránke, a ihneď zastaví jeho preberanie, aby sa nikdy nedostal do počítača.

Poznámka: Súčasť AVG Webový štít sa nemôže používať na serverových platformách!

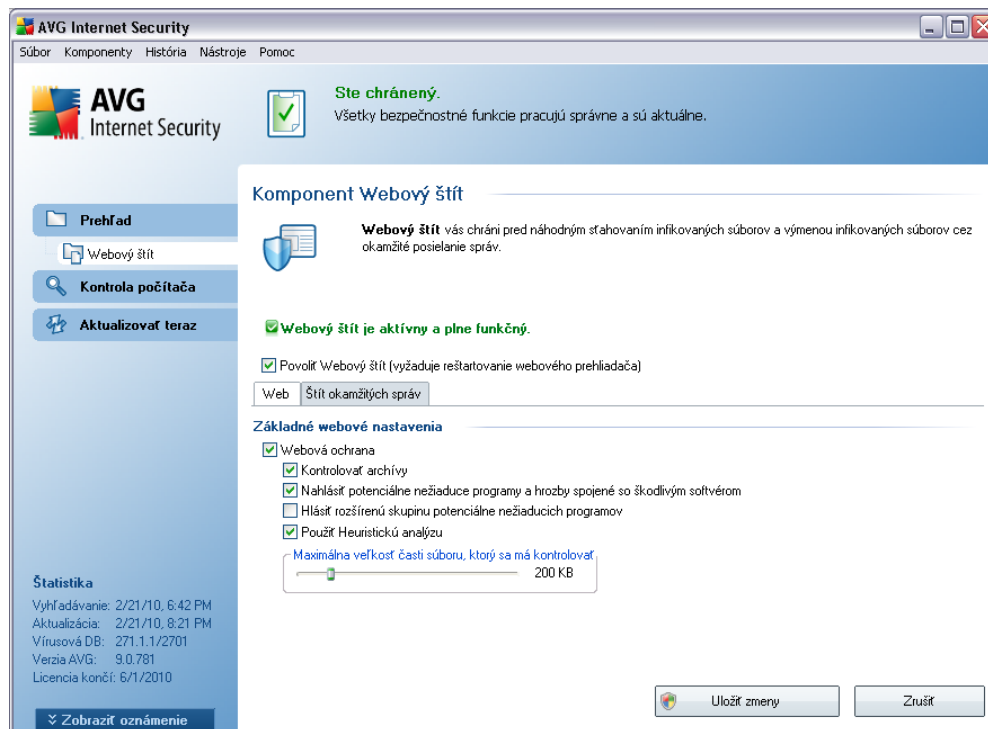
8.8.2. Rozhranie súčasti Webový štít

V rozhraní súčasti **Webový štít** sa nachádzajú informácie o správaní tohto typu ochrany. Dalej sa tam nachádzajú informácie o aktuálnom stave súčasti (*Súčasť Webový štít je zapnutá a úplne funkčná.*). V spodnej časti dialógového okna sa potom nachádzajú základné možnosti editovania funkcionality tejto súčasti.

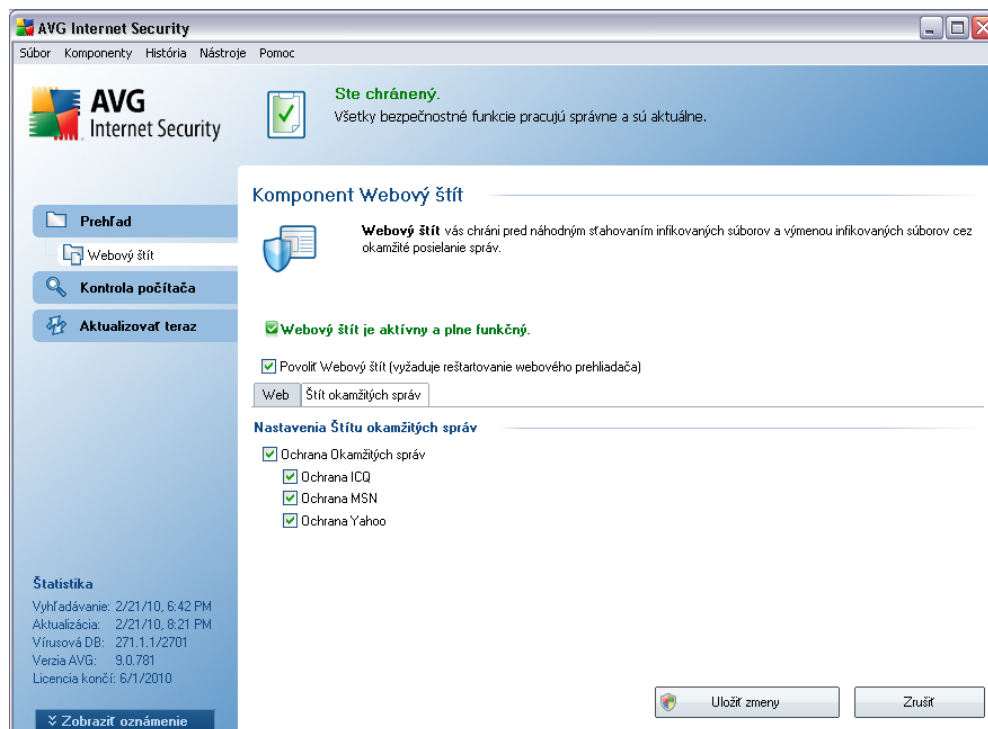
Základná konfigurácia súčasti

V prvom rade máte možnosť okamžite zapnúť/vypnúť **Webový štít** zaciarknutím položky **Zapnúť Webový štít**. Táto možnosť je štandardne povolená a súčasť **Webový štít** je zapnutá. Ak však nemáte dobrý dôvod meniť tieto nastavenia, odporúčame vám nechať súčasť zapnutú. Ak je táto položka zaciarknutá a súčasť **Webový štít** je spustená, k dispozícii sú ďalšie možnosti konfigurácie, ktoré môžete editovať na dvoch kartách:

- **Web:** Umožňuje editovať konfiguráciu súčasti z hľadiska prehľadávania obsahu webových stránok. Editacné rozhranie umožňuje nastaviť nasledujúce základné možnosti:



- **Webová ochrana:** Ak je táto funkcia zapnutá, súčasť **Webový štít** bude prehľadávať obsah webových stránok. Ak je táto možnosť zapnutá (štandardne), môžete ďalej zapnúť/vypnúť tieto položky:
 - **Kontrolovať archívy:** Zapne prehľadávanie obsahu archívov, ktoré môžu byť súčasťou zobrazovanej webovej stránky.
 - **Hlásiť potenciálne nežiaduce programy a hrozby spyware (štandardne zapnuté):** Označíte túto možnosť, ak chcete zapnúť súčasť **Anti-Spyware** a vyhľadávať spyware a vírusy. **Spyware** predstavuje pochybnú kategóriu škodlivého softvéru: Aj keď obvyčajne predstavujú bezpečnostné riziko, niektoré takéto programy môžu byť nainštalované úmyselne. Odporúčame vám nechať túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
 - **Hlásiť rozšírenú skupinu potenciálne nežiaducich programov:** Ak je zapnutá predchádzajúca možnosť, môžete označiť aj toto zaciarkovacie políčko, a tým povoliť detegovanie rozšírenej skupiny **spywaru**: programov, ktoré sú úplne v poriadku a neškodné, ak sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje zabezpečenie vášho počítača, ale môže blokovat dobré programy, a preto je táto funkcia štandardne vypnutá.
 - **Použiť heuristickú analýzu:** Zapne prehľadávanie obsahu zobrazovanej stránky pomocou metódy heuristickej analýzy, t. j. simulácie a hodnotenia inštrukcií prehľadávaného objektu vo virtuálnom počítačovom prostredí. Preto dokáže detegovať aj škodlivý kód, ktorý doposiaľ nie je opísaný vo vírusovej databáze (*pozri časť [Princíp fungovania súčasti Anti-Virus](#)*).
 - **Minimálna veľkosť súboru, ktorá sa má prehľadávať:** Ak sa priložené súbory nachádzajú na zobrazovanej stránke, ich obsah sa môže zároveň skontrolovať ešte predtým, než sa súbory prevezmú do počítača. Prehľadávanie veľkých súborov však chvíľu trvá a preberanie z webovej stránky sa môže výrazne spomaliť. Pomocou posúvaca môžete nastaviť maximálnu veľkosť súboru, ktorý sa má prehľadať súčasťou **Webový štít**. Aj keď je prevzatý súbor väčší než nastavená hodnota, a z tohto dôvodu ho súčasť **Webový štít** neskontroluje, váš počítač je stále chránený: ak je súbor infikovaný, súčasť **Rezidentný štít** ho ihneď deteguje.
- **Okamžité správy:** Umožňuje zmeniť nastavenia súčastí, ktoré sa týkajú prehľadávania okamžitých správ (*napr. v programoch ICQ, MSN Messenger, Yahoo...*).



- Ochrana okamžitých správ: Oznacte túto možnosť, ak chcete, aby súčasť Webový štít kontrolovala, či sa v online komunikácii nenachádzajú vírusy. Ak táto možnosť je zapnutá, môžete ďalej nastaviť, ktorú aplikáciu na posielanie okamžitých správ chcete kontrolovať – **AVG 9 Anti-Virus plus Firewall** momentálne spolupracuje s aplikáciami ICQ, MSN a Yahoo.

Poznámka: Výrobca softvéru nastavil všetky súčasti AVG takým spôsobom, aby fungovali optimálne. Nemente konfiguráciu AVG, ak k tomu nemáte závažný dôvod. Všetky zmeny nastavení by mali vykonávať len skúsení používatelia. Ak chcete zmeniť konfiguráciu programu AVG, zvolte položku v ponuke programu **Nástroje/Rozšírené nastavenia** a zmeňte konfiguráciu v novo otvorenom dialógovom okne [Rozšírené nastavenia programu AVG](#).

Ovládacie tlačidlá

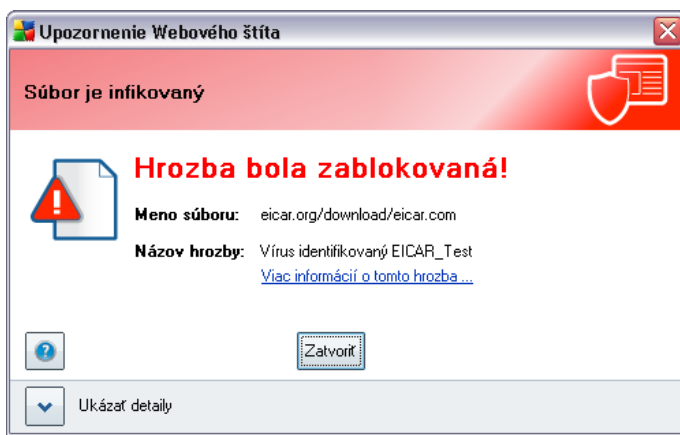
V rozhraní súčasti **Webový štít** sa nachádzajú nasledujúce ovládacie tlačidlá:

- **Uložiť zmeny:** Stlačením tohto tlačidla sa uložia a použijú všetky zmeny urobené v tomto dialógovom okne.

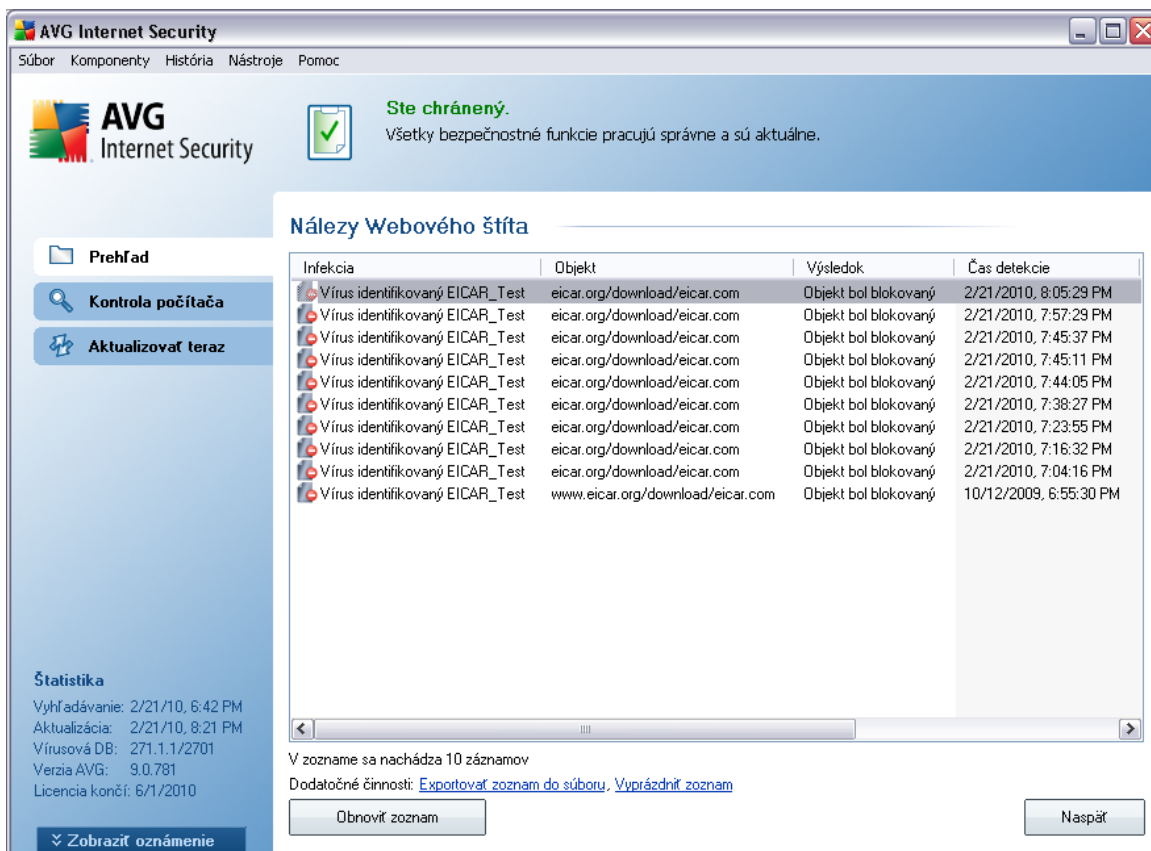
- **Zrušit:** Stlačením tohto tlačidla sa vrátite na hlavné [používateľské rozhranie AVG](#) (prehľad súčastí)

8.8.3. Detegovanie súčastou Webový štít

Webový štít prehľadáva obsah navštívených webových stránok a súborov, ktoré sa na nich môžu nachádzať, ešte predtým, než sa zobrazia vo webovom prehliadači alebo prevezmú do počítača. Pri zistení hrozby vás program ihneď upozorní zobrazením nasledujúceho dialógového okna:



Podozrivá webová stránka sa neotvorí a zistená hrozba sa zaznamená do zoznamu **nálezov súčasti Webový štít** – tento prehľad zistených hrozieb sa otvára pomocou hlavnej systému [História/Nálezy súčasti Webový štít](#).



The screenshot shows the AVG Internet Security application window. At the top, it says "Ste chránený." (You are protected) and "Všetky bezpečnostné funkcie pracujú správne a sú aktuálne." (All security functions are working correctly and are up to date). The main section is titled "Nálezy Webového štíta" (Web Shield Findings) and contains a table with the following data:

Infekcia	Objekt	Výsledok	Čas detekcie
Vírus identifikovaný EICAR_Test	eicar.org/download/eicar.com	Objekt bol blokováný	2/21/2010, 8:05:29 PM
Vírus identifikovaný EICAR_Test	eicar.org/download/eicar.com	Objekt bol blokováný	2/21/2010, 7:57:29 PM
Vírus identifikovaný EICAR_Test	eicar.org/download/eicar.com	Objekt bol blokováný	2/21/2010, 7:45:37 PM
Vírus identifikovaný EICAR_Test	eicar.org/download/eicar.com	Objekt bol blokováný	2/21/2010, 7:45:11 PM
Vírus identifikovaný EICAR_Test	eicar.org/download/eicar.com	Objekt bol blokováný	2/21/2010, 7:44:05 PM
Vírus identifikovaný EICAR_Test	eicar.org/download/eicar.com	Objekt bol blokováný	2/21/2010, 7:38:27 PM
Vírus identifikovaný EICAR_Test	eicar.org/download/eicar.com	Objekt bol blokováný	2/21/2010, 7:23:55 PM
Vírus identifikovaný EICAR_Test	eicar.org/download/eicar.com	Objekt bol blokováný	2/21/2010, 7:16:32 PM
Vírus identifikovaný EICAR_Test	eicar.org/download/eicar.com	Objekt bol blokováný	2/21/2010, 7:04:16 PM
Vírus identifikovaný EICAR_Test	www.eicar.org/download/eicar.com	Objekt bol blokováný	10/12/2009, 6:55:30 PM

Below the table, it indicates "V zozname sa nachádza 10 záznamov" (10 records in the list) and provides options to "Exportovať zoznam do súboru" (Export list to file) and "Vyprázdiť zoznam" (Clear list). There are also buttons for "Obnoviť zoznam" (Refresh list) and "Naspäť" (Back).

Pre každý detegovaný objekt sa zobrazia nasledujúce informácie:

- **Infekcia:** Opis (prípadne aj názov) detegovaného objektu.
- **Objekt:** Zdroj objektu (webová stránka).
- **Výsledok:** Akcia urobená na detegovanom objekte.
- **Cas detegovania:** Dátum a čas detegovania a zablokovania hrozby.
- **Typ objektu:** Typ detegovaného objektu.
- **Proces:** Aká akcia sa vykonala na zavolanie potenciálne nebezpečného objektu, aby sa dal detegovať.

V spodnej časti dialógového okna pod zoznamom sa nachádzajú informácie o celkovom počte detegovaných objektov. Ďalej môžete exportovať celý zoznam zistených

objektov do súboru (**Exportovať zoznam do súboru**) a vymazať všetky položky zistených objektov (**Vyprázdniť zoznam**). Tlačidlo **Obnoviť zoznam** aktualizuje zoznam nálezov detegovaných súčastou **Webový štít**. Tlačidlo **Naspäť** otvorí hlavné [používateľské rozhranie programu AVG](#) (prehľad súcastí).

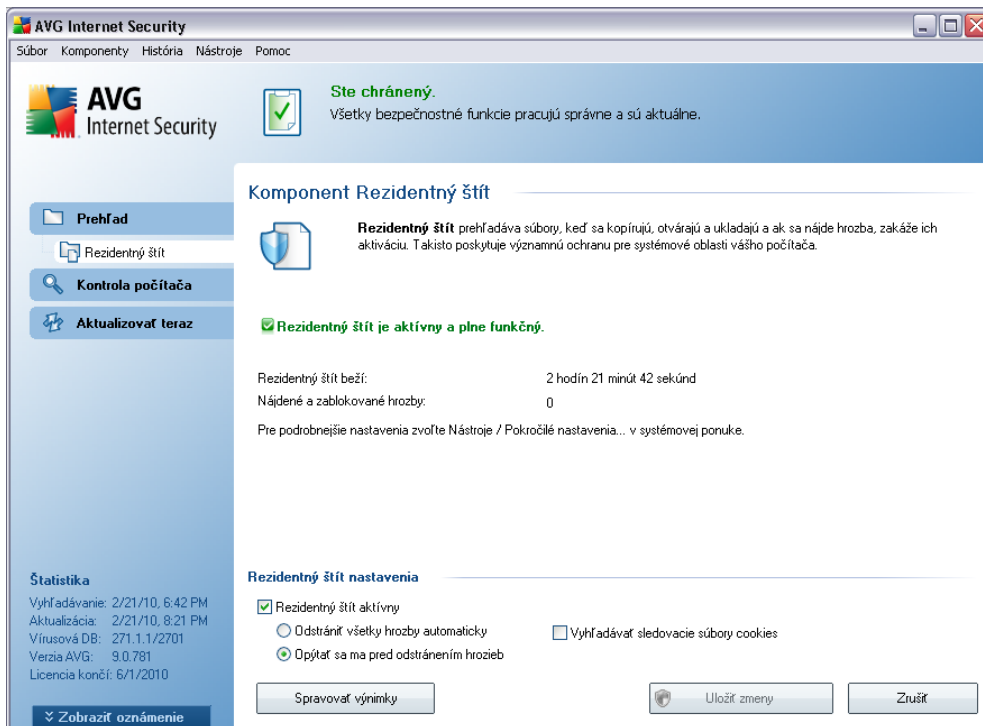
8.9. Rezidentný štít

8.9.1. Rezidentný štít Princípy

Súcast **Rezidentný štít** zabezpečuje neustálu ochranu vášho počítača. Prehľadáva každý jeden otváraný, ukladaný a kopírovaný súbor a chráni systémové oblasti počítača. Keď **Rezidentný štít** odhalí vírus v súbore, ktorý sa snaží sprístupniť, zastaví práve prebiehajúcu operáciu a nedovolí vírusu, aby sa aktivoval. Tento proces si normálne ani nevšimnete, pretože beží „na pozadí“ a budete informovaný len pri zistení hrozby a **Rezidentný štít** zároveň zablokuje aktivovanie hrozby a odstráni ju. **Rezidentný štít** sa nacíta do pamäte počítača počas zavádzania systému.

Upozornenie: Súcast Rezidentný štít sa nacíta do pamäte počítača počas spustenia systému a je dôležité, aby zostala stále zapnutá!

8.9.2. Rozhranie Rezidentného štítu



Vedľa prehľadu najdôležitejších štatistických údajov a informácií o aktuálnom stave súčasti (*Súčasť Rezidentný štít je zapnutá a úplne funkčná*), rozhranie súčasti **Rezidentný štít** poskytuje aj niektoré základné možnosti nastavenia súčasti. Štatistika vyzerá nasledovne:

- **Súčasť Rezidentný štít je zapnutá:** Informuje o case uplynutom od posledného spustenia súčasti.
- **Nájdene a zablokované hrozby:** Počet detegovaných infekcií, ktorých spusteniu/otvoreníu program zabránil (v prípade potreby sa dá táto hodnota vynulovať; napr. na štatistické účely – Vynulovať hodnotu).

Základná konfigurácia súčasti

V spodnej časti dialógového okna sa nachádza časť s názvom **Nastavenia súčasti Rezidentný štít**, ktorá umožňuje editovať niektoré základné nastavenia funkcionality súčasti (*podrobná konfigurácia ako pri všetkých ostatných súčastiach sa otvorí kliknutím na položku Nástroje/Rozšírené nastavenia v hlavnej ponuke programu*).

Možnosť **Súčasť Rezidentný štít je zapnutá** sa používa na rýchle zapnutie/vypnutie rezidentnej ochrany. Táto funkcia je štandardne zapnutá. So zapnutou rezidentnou ochranou sa môžete ďalej rozhodnúť, ako sa majú spracovať (odstrániť) pravdepodobne detekované infekcie:

- o buď automaticky (**Odstrániť všetky hrozby automaticky**),
- o alebo až po súhlase používateľa (**Opýtať sa pred odstránením hrozieb**).

Táto možnosť nemá žiaden vplyv na úroveň zabezpečenia a odzrkadľuje len vaše preferencie.

V oboch prípadoch môžete zvoliť, či chcete **odstrániť sledovacie súbory cookies automaticky**. V špecifických prípadoch môžete túto možnosť zapnúť na dosiahnutie maximálnej úrovne zabezpečenia, štandardne je však vypnutá. (Cookies sú textové pakety posielané serverom do internetového prehliadača a následne posielané naspäť nezmenené z prehliadača pri každom prístupe na daný server. HTTP cookies sa používajú na autentifikáciu, sledovanie a zachovanie špecifických informácií o používateľoch, akými sú napr. preferencie stránok alebo obsah elektronického nákupného košíka).

Poznámka: Výrobca softvéru nastavil všetky súčasti AVG takým spôsobom, aby fungovali optimálne. Nemente konfiguráciu AVG, ak k tomu nemáte závažný dôvod. Všetky zmeny nastavení by mali vykonávať len skúsení používatelia. Ak chcete zmeniť konfiguráciu programu AVG, zvolte položku v ponuke programu **Nástroje/Rozšírené nastavenia** a zmeňte konfiguráciu v novo otvorenom dialógovom okne [Rozšírené nastavenia AVG](#).

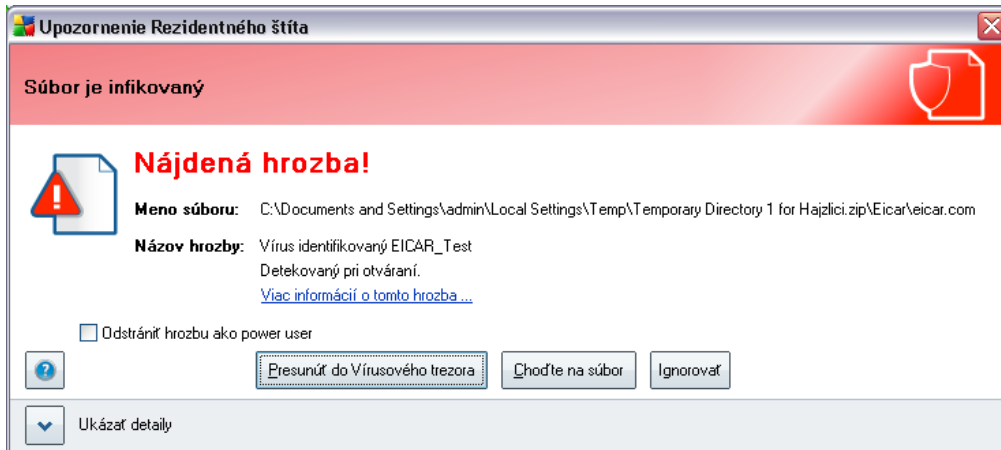
Ovládacie tlačidlá

V rozhraní súčasti **Rezidentný štít** sa nachádzajú nasledujúce ovládacie tlačidlá:

- **Správa výnimiek:** Otvorí dialógové okno [Rezidentný štít – Vylúčené adresáre](#), ktoré umožňuje definovať pricinky, ktoré sa majú vynechať z prehľadávania súčastou [Rezidentný štít](#).
- **Uložiť zmeny:** Stlačením tohto tlačidla sa uložia a použijú všetky zmeny urobené v tomto dialógovom okne.
- **Zrušiť:** Stlačením tohto tlačidla sa znova otvorí hlavné [používateľské rozhranie AVG](#) (prehľad súčastí).

8.9.3. Detekcia Rezidentného štítu

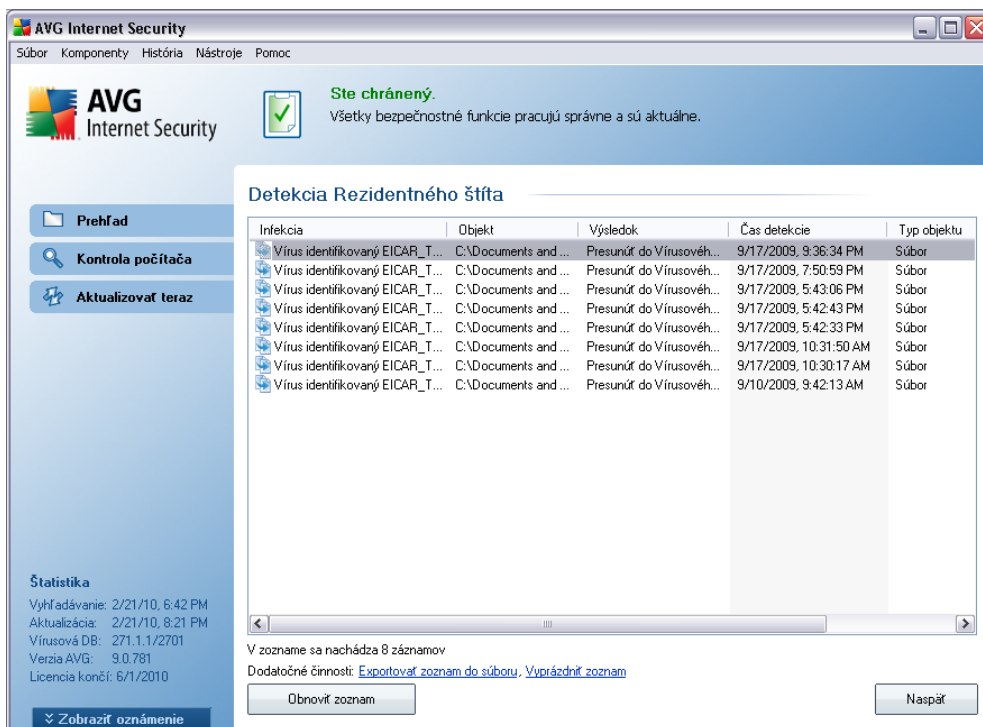
Rezidentný štít prehľadáva súbory pri kopírovaní, otváraní alebo ukladaní. Pri zistení vírusu alebo akéhokolvek druhu hrozby vás program ihneď upozorní zobrazením nasledujúceho dialógového okna:



V dialógovom okne sú uvedené informácie o zistenej hrozbe a okno vám zároveň umožní rozhodnúť o opatrení, ktoré sa má prijať:

- **Vyliečiť** – ak je k dispozícii prostriedok na vyliečenie, program AVG automaticky vylieci infikovaný súbor; táto možnosť predstavuje odporúčané opatrenie.
- **Premiestniť do trezora** – vírus sa premiestni do [vírusového trezora AVG](#).
- **Íst na súbor** - táto možnosť vás presmeruje na presné umiestnenie podozrivého objektu (otvorí nové okno programu *Windows Explorer*).
- **Ignorovať** – veľmi vám odporúčame, aby ste túto možnosť NEPOUŽÍVALI, pokiaľ na to nemáte veľmi dobrý dôvod!

Celý prehľad všetkých hrozieb zistených súčasťou **Rezidentný štít** sa nachádza v dialógovom okne **Detekcia súčasťou Rezidentný štít**, ktoré sa otvára pomocou možnosti v ponuke systému [História/zistenia Rezidentného štítu](#):



Detekcia Rezidentného štítu poskytuje prehľad objektov, ktoré detegoval **Rezidentný štít**, zhodnotených ako nebezpečné a buď vyliečené alebo presunuté do **Vírusového trezora**. Pri každom detekovanom objekte sa poskytujú nasledovné informácie:

- **Infekcia** - opis (prípadne aj názov) detegovaného objektu.
- **Objekt** - umiestnenie objektu
- **Výsledok** - vykonaná činnosť s detekovaným objektom
- **Cas detekcie** - dátum a čas detegovania objektu.
- **Typ objektu** - typ detekovaného objektu
- **Proces** - aká činnosť bola vykonaná pre vyvolanie potenciálne nebezpečného objektu tak, aby sa dal detekovať

V spodnej časti dialógového okna pod zoznamom nájdete informácie o celkovej počte detekovaných objektov. Ďalej môžete exportovať celý zoznam zistených objektov do súboru (**Exportovať zoznam do súboru**) a vymazať všetky položky zistených

objektov (**Vyprázdniť zoznam**). Tlačidlo **Obnoviť zoznam** aktualizuje zoznam hrozieb zistených **Rezydentným štítom**. Tlačidlo **Naspäť** vás vráti späť na predvolené **[používateľské rozhranie AVG](#)** (prehľad súčastí).

8.10. Manažér aktualizácií

8.10.1. Princípy Manažéra aktualizácií

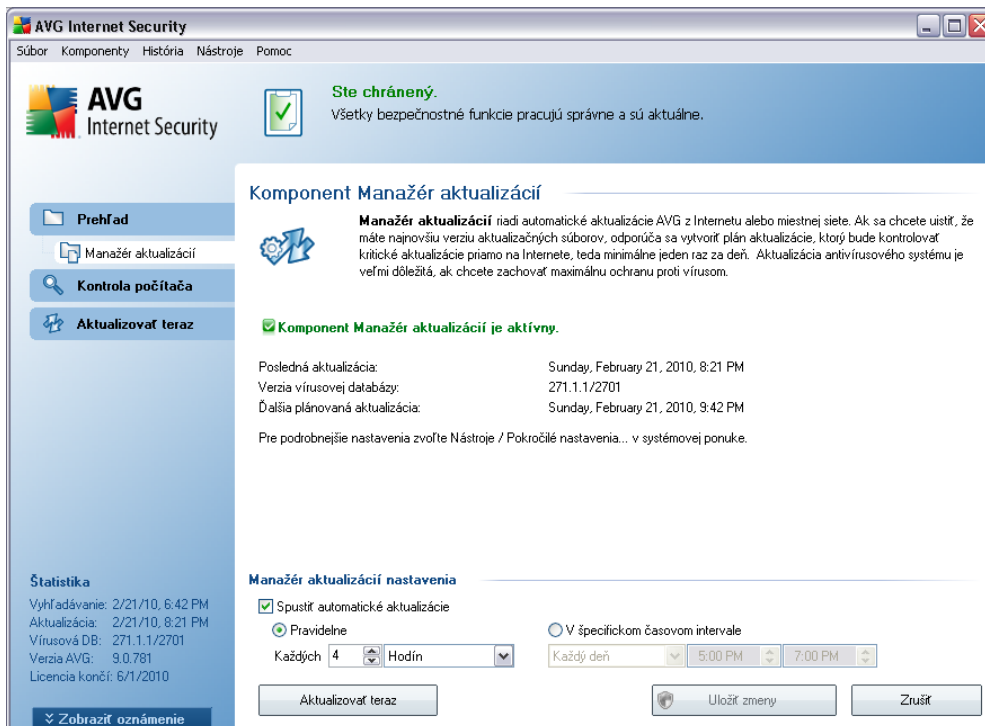
Žiaden bezpečnostný softvér nedokáže zaručiť skutocnú ochranu pred rôznymi typmi hrozieb, ak sa pravidelne neaktualizuje! Autori vírusov stále hľadajú nové trhliny, ktoré by mohli využiť, či už v softvéri alebo v operačných systémoch. Nové vírusy, nový malware, nové útoky hackerov sa objavujú denne.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

Pravidelná aktualizácia programu AVG je nevyhnutná!

Update Manager uľahčuje správu pravidelných aktualizácií. Súčasť umožňuje naplánovať automatické prevzatie aktualizacných súborov buď z internetu alebo z lokálnej siete. Dôležité aktualizácie vírusových definícií by sa mali robiť denne, ak to je možné. Menej urgentné programové aktualizácie sa môžu robiť raz za týždeň.

Poznámka: Venujte pozornosť kapitole **[Aktualizácie programu AVG](#)**, v ktorej sa nachádzajú ďalšie informácie o typoch a úrovniach aktualizácie!

8.10.2. Rozhranie Manažéra aktualizácií



V rozhraní súčasti **Update Manager** sa nachádzajú informácie o funkciách súčasti a jej aktuálnom stave (*Súčasť Update Manager je zapnutá.*) a súvisiace štatistické údaje:

- **Posledná aktualizácia:** Informuje, kedy a v akom case sa databáza aktualizovala.
- **Verzia vírusovej databázy:** Uvádza číslo najnovšej verzie vírusovej databázy a toto číslo narastá s každou aktualizáciou vírusovej databázy.
- **Nasledujúca naplánovaná aktualizácia:** Uvádza, na kedy a na aký cas je naplánovaná ďalšia aktualizácia databázy.

Základná konfigurácia súčasti

V spodnej časti tohto dialógového okna sa nachádza časť s názvom **Nastavenia súčasti Update Manager**, ktorá umožňuje urobiť zmeny pravidiel spustenia procesu aktualizácie. Umožňuje nastaviť, aby sa aktualizacné súbory preberali automaticky (

Spustit automatické aktualizácie), alebo len na požiadanie. Štandardne je možnosť **Spúšťať automatické aktualizácie** zapnutá a odporúčame vám nemeniť toto nastavenie! Pravidelné preberanie najnovších aktualizacných súborov je rozhodujúce na správne fungovanie každého bezpečnostného softvéru!

Dalej môžete nastaviť, kedy sa má aktualizácia spúšťať:

- o **Pravidelne**: Nastavte časový interval.
- o **V nastavenom case**: Nastavte presný den a čas.

Štandardne je aktualizácia nastavená na každé 4 hodiny. Odporúčame vám toto nastavenie nemeniť, ak na to nemáte vážny dôvod!

Poznámka: Výrobca softvéru nastavil všetky súčasti AVG takým spôsobom, aby fungovali optimálne. Nemente konfiguráciu AVG, ak k tomu nemáte závažný dôvod. Všetky zmeny nastavení by mali vykonávať len skúsení používatelia. Ak chcete zmeniť konfiguráciu programu AVG, zvolte položku v ponuke programu **Nástroje/Rozšírené nastavenia** a zmeňte konfiguráciu v novo otvorenom dialógovom okne [Rozšírené nastavenia AVG](#).

Ovládacie tlačidlá

V rozhraní súčasti **Update Manager** sa nachádzajú nasledujúce ovládacie tlačidlá:

- **Aktualizovať teraz**: Spustí [okamžitú aktualizáciu](#) na požiadanie.
- **Uložiť zmeny**: Stlačením tohto tlačidla sa uložia a použijú všetky zmeny urobené v tomto dialógovom okne.
- **Zrušiť**: Stlačením tohto tlačidla sa znova otvorí hlavné [používateľské rozhranie AVG](#) (prehľad súčastí).

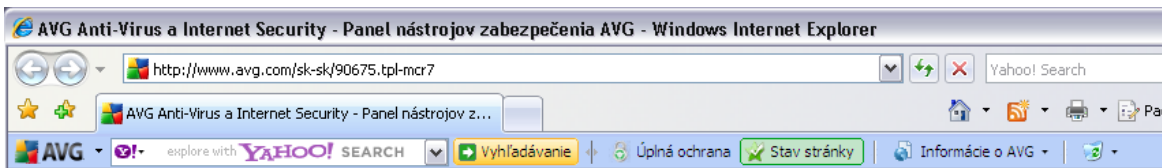
9. Panel nástrojov zabezpečenia AVG

AVG Security Toolbar je nový nástroj, ktorý spolupracuje so súčasťou **AVG Link Scanner** a kontroluje výsledky vyhľadávania v podporovaných internetových vyhľadávacoch (*Yahoo!*, *Google*, *Bing*, *Altavista*, *Baidu*). **AVG Security Toolbar** sa používa na ovládanie funkcií súčasti **AVG Link Scanner** a nastavenie jej správania.

Ak si zvolíte inštaláciu panela nástrojov počas inštalácie programu **AVG 9 Anti-Virus plus Firewall**, automaticky sa pridá do internetového prehliadaca. Ak používate alternatívny internetový prehliadac (*napr. Avant Browser*), môžete sa stretnúť s neocakávaným správaním.

9.1. Panel nástrojov zabezpečenia AVG Rozhranie

Súčasť **AVG Security Toolbar** spolupracuje s programami **MS Internet Explorer** (verzia 6.0 alebo novšia) a **Mozilla Firefox** (verzia 2.0 alebo novšia). Keď sa rozhodnete nainštalovať súčasť **AVG Security Toolbar** (pocas [procesu inštalácie produktu AVG](#) sa vás program opýta, či si želáte súčasť nainštalovať), súčasť sa bude nachádzať v internetovom prehliadaci hneď pod riadkom s adresou:



Poznámka: Súčasť **AVG Security Toolbar** nie je určená pre serverové platformy!

AVG Security Toolbar pozostáva z nasledujúcich častí:

- **Logom AVG:** Umožňuje prístup ku všeobecným položkám panela nástrojov. Kliknutím na tlačidlo s logom otvorte webové stránky AVG (<http://www.avg.com/>). Po kliknutí na kurzor vedľa ikony AVG sa otvorí nasledujúce:
 - **Informácie o paneli nástrojov:** Odkaz na domovskú stránku súčasti **AVG Security Toolbar** s podrobnými informáciami o ochrane poskytovanej panelom nástrojov.
 - **Spustiť AVG 9 Anti-Virus plus Firewall:** Otvorí používateľské rozhranie produktu **AVG 9 Anti-Virus plus Firewall**.
 - **Možnosti:** Otvorí dialógové okno konfigurácie, ktoré vám umožní prispôbiť nastavenia súčasti **AVG Security Toolbar** vašim potrebám (pozri ďalšiu kapitolu [Možnosti súčasti AVG Security Toolbar](#)).

- **Vymazať históriu:** Umožní vám *vymazať celú históriu* súčasti AVG Security Toolbar, resp. *vymazať históriu hľadania, vymazať históriu prehliadaca, vymazať históriu prevzatých súborov a vymazať súbory cookies*.
- **Aktualizovať:** Vyhladá nové aktualizácie pre súčast **AVG Security Toolbar**
- **Pomocník:** Umožní vám otvoriť súbor pomocníka, poslať spätnú väzbu na produkt a zobraziť informácie o aktuálnej verzii panela nástrojov.
- **Vyhľadávacie pole:** Zadajte slovo alebo slovné spojenie do vyhľadávacieho pola. Stlačením tlačidla **Hľadať** spustíte vyhľadávanie pomocou nastaveného vyhľadávaca (v časti [Rozšírené možnosti v súčasti AVG Security Toolbar](#) môžete zvoliť požadovaný vyhľadávac, buď Yahoo!, Wikipedia, Baidu, WebHľadani alebo Yandex), bez ohľadu na práve otvorenú stránku. Okienko pre vyhľadávanie uvádza aj vašu históriu vyhľadávania. Vyhľadávania vykonané cez okienko pre vyhľadávanie sa analyzujú pomocou ochrany Štitu vyhľadávania AVG.
- **Úplná ochrana:** Toto tlačidlo sa zobrazí v podobe **Úplná ochrana/Obmedzená ochrana/Žiadna ochrana** v závislosti od **AVG 9 Anti-Virus plus Firewall** konfigurácie
- **Stav stránky:** Priamo na paneli nástrojov sa pomocou tohto tlačidla zobrazí hodnotenie práve nahratej webovej stránky v závislosti od kritérií nastavených v súčasti **AVG Search-Shield** (*stránka je bezpečná/podozrivá/pozitívne nebezpečná/obsahuje hrozby/nedá sa prehľadať*). Kliknutím na tlačidlo otvorte informacný panel s podrobnými informáciami o konkrétnej webovej stránke.
- **Informácie o AVG:** Zobrazí odkazy na dôležité bezpečnostné informácie na webových stránkach AVG (<http://www.avg.com/>).
 - **Informácie o paneli nástrojov:** Odkaz na domovskú stránku súčasti **AVG Security Toolbar** s podrobnými informáciami o ochrane poskytovanej panelom nástrojov.
 - **O hrozbách:** Otvorí webovú stránku AVG s informáciami o súčasných vírusoch a hrozbách na internete.
 - **Novinky od AVG:** Otvorí webovú stránku s najnovšími tlačovými správami súvisiacimi s produktmi a spoločnosťou AVG.
 - **Súčasná úroveň hrozieb:** Otvorí webovú stránku vírusového laboratória

s grafickým zobrazením súčasnej úrovne hrozieb na webe.

- o **Encyklopédia vírusov**: Otvorí stránku s encyklopédiou vírusov, na ktorej môžete vyhľadať konkrétne vírusy podľa názvu a získať podrobné informácie o každom z nich.

9.2. Možnosti panela nástrojov AVG Security Toolbar

Všetky konfiguračné parametre panela **AVG Security Toolbar** sa sprístupňujú priamo na paneli **AVG Security Toolbar**. Editacné rozhranie sa otvára pomocou položky v ponuke panela nástrojov **AVG/Možnosti** v novom dialógovom okne s názvom **Možnosti panela nástrojov**, ktoré je rozdelené na tri časti:

9.2.1. Karta Všeobecné



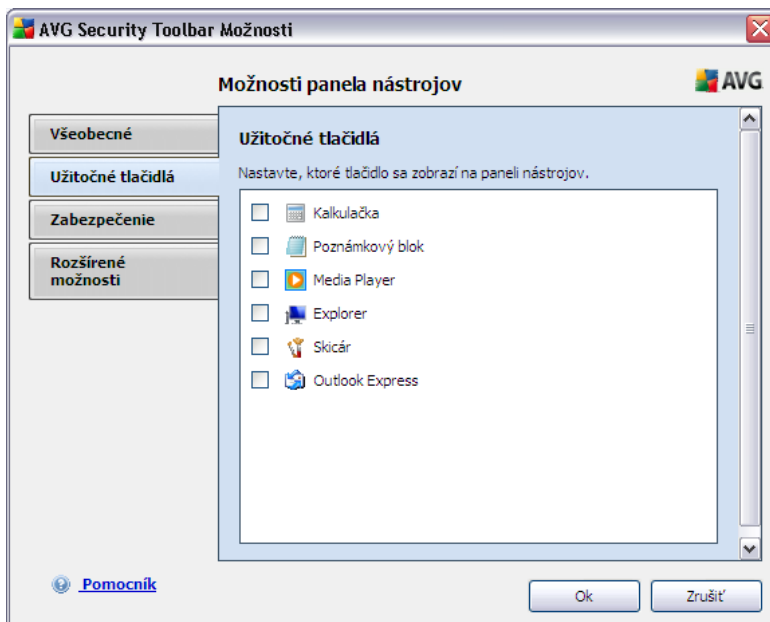
Táto karta umožňuje nastaviť, ktoré ovládacie tlačidlá sa majú zobrazit resp. skryt na paneli **AVG Security Toolbar**. Označte ľubovoľnú možnosť podľa toho, ktoré tlačidlá chcete zobrazit. Nasledujúce je prehľad funkcionality jednotlivých tlačidiel na paneli nástrojov:

- **Tlačidlo Novinky od AVG**: Otvorí webovú stránku s najnovšími tlačovými správami súvisiacimi s produktmi a spoločnosťou AVG.
- **Tlačidlo Novinky**: Otvorí štruktúrovaný prehľad aktuálnych správ z dennej

tlace.

- **Tlačidlo Informácie o AVG:** Toto tlačidlo zobrazí informácie o paneli nástrojov AVG, aktuálnych hrozbách a závažnosti internetových hrozieb, otvorí encyklopédiu vírusov a zobrazí ďalšie správy súvisiace s produktmi AVG.
- **Tlačidlo Vymazať históriu:** Toto tlačidlo sa používa na vymazanie celej histórie resp. vymazanie histórie hľadania, vymazanie histórie prehliadaca, vymazanie histórie prevzatých súborov a vymazanie súborov cookies priamo na paneli AVG Security Toolbar.

9.2.2. Karta Užitocné tlačidlá








Karta **Užitocné tlačidlá** umožňuje zvolit aplikácie v zozname a zobrazit ich ikonu v rozhraní panela nástrojov. Ikona sa potom používa ako skratka umožňujúca ihneď spustiť príslušnú aplikáciu.

9.2.3. Karta Zabezpečenie



Karta **Zabezpečenie** je rozdelená na dve časti, **AVG Browser Security** a **Hodnotenia**, kde môžete označením konkrétnych zaciarkovacích polícok pridelit panelu **AVG Security Toolbar** funkcionality, ktorú chcete používať:

- **AVG Browser Security**: Pomocou tejto položky sa zapínajú a vypínajú služby **AVG Search-Shield** a **AVG Active Surf-Shield**.
- **Hodnotenia**: Zvolte grafické symboly používané na hodnotenie výsledkov prehľadávania súčasťou **AVG Search-Shield**, ktoré chcete používať:
 -  stránka je bezpečná
 -  stránka je do istej miery podozrivá
 -  na stránke sa nachádzajú odkazy na pozitívne nebezpečné stránky
 -  na stránke sa nachádzajú aktívne hrozby
 -  stránka nie je prístupná a nemožno ju skontrolovať

Oznacením príslušnej možnosti potvrdte, že chcete byť informovaný o tejto konkrétnej úrovni hrozby. Zobrazenie červenej značky pridelenej stránkam obsahujúcim aktívne a nebezpečné hrozby však nie je možné vypnúť. **Znova vám odporúčame ponechať predvolenú konfiguráciu nastavenú výrobcom programu, ak nemáte skutočný dôvod meniť ju.**

9.2.4. Karta Rozšírené možnosti



Na karte **Rozšírené možnosti** najskôr zvolte, ktorý vyhľadávac chcete používať ako predvolený. Na výber máte nasledujúce možnosti: *Yahoo!*, *Baidu*, *WebHledani* a *Yandex*. Po zmene predvoleného vyhľadávaca reštartujte prehliadač, aby sa zmena prejavila.

Karta ďalej umožňuje zapnúť resp. vypnúť ďalšie nastavenia súvisiace s panelom nástrojov **AVG Security Toolbar**:

- **Nastaviť a ponechať Yahoo! ako predvolený vyhľadávac pre riadok s adresou** (štandardne zapnuté): Ak je táto možnosť oznacená, umožňuje zadať hľadaný výraz priamo do riadka s adresou v internetovom prehliadači a služba Yahoo! sa automaticky použije na vyhľadanie príslušných webových stránok.
- **Umožniť programu AVG zobrazit odporúčania pri zobrazení chyby navigácie v prehliadači (404/DNS)** (štandardne zapnuté): Ak počas vyhľadávania na internete narazíte na neexistujúcu stránku, alebo stránku,

ktorú nie je možné zobrazit (chyba 404), program automaticky otvorí webovú stránku, ktorá vám umožní urobiť výber v prehľade alternatívnych stránok súvisiacich s hľadanou problematikou.

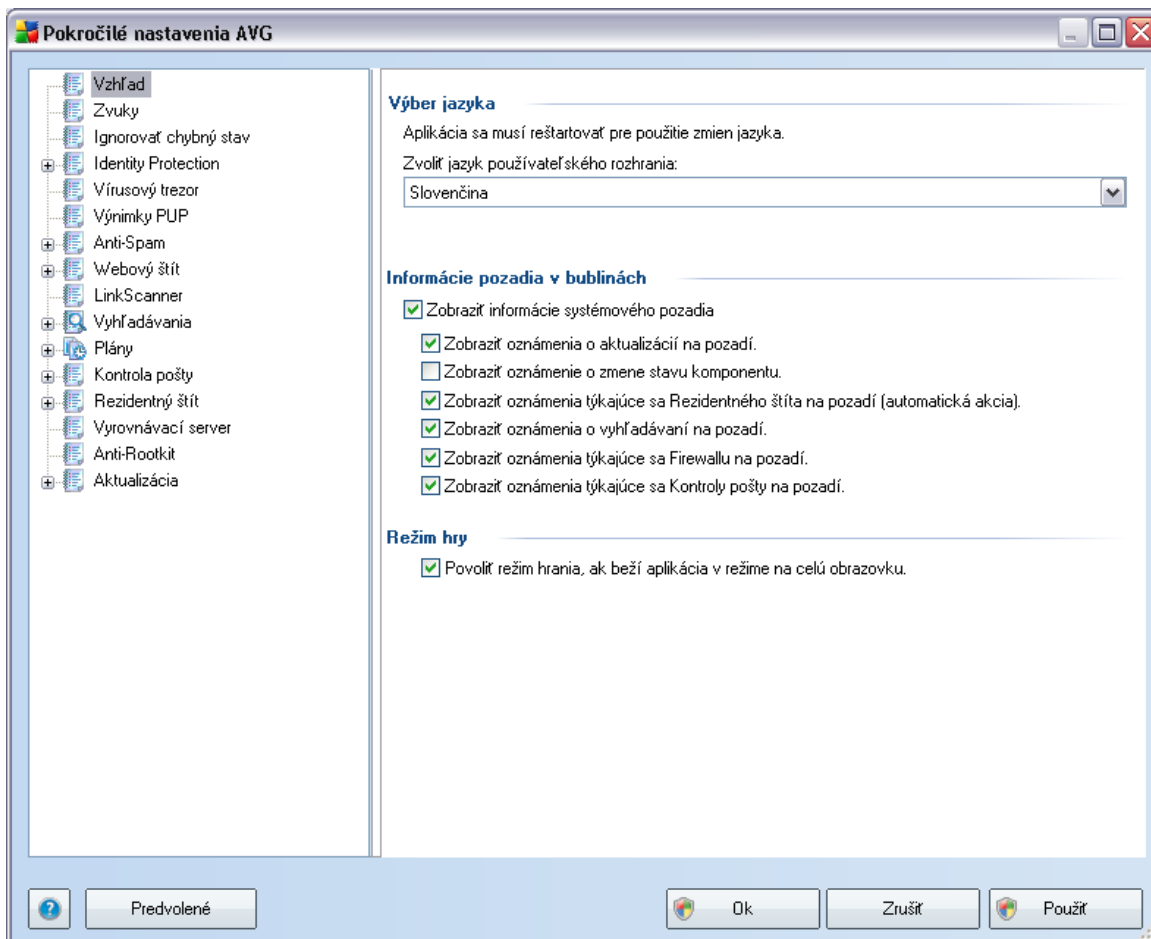
- **Nastaviť a ponechať Yahoo! ako vyhľadávac v prehliadaci** (štandardne vypnuté): Yahoo! je predvolený vyhľadávac na paneli nástrojov AVG Security Toolbar a zapnutím tejto možnosti sa zároveň nastaví ako predvolený vyhľadávac vo vašom internetovom prehliadaci.
- **Znova zobrazit panel nástrojov AVG Security Toolbar, ak je skrytý (týždenne)** (štandardne zapnuté): Táto možnosť je zapnutá štandardne a ak nechcete skryťe **AVG Security Toolbar**, znova sa zobrazí po uplynutí jedného týždňa.

10. Pokročilé nastavenia AVG

Dialógové okno s rozšírenou konfiguráciou produktu **AVG 9 Anti-Virus plus Firewall** 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

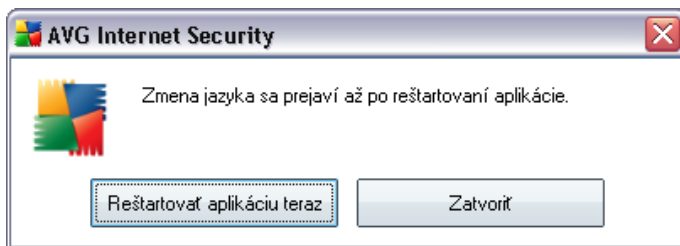
Prvá položka v stromovej štruktúre, **Vzhľad**, súvisí so všeobecnými nastaveniami [používateľského rozhrania AVG](#) a používa sa na nastavenie zopár základných možností správy aplikácie:



Výber jazyka

Časť **Výber jazyka** sa používa na nastavenie požadovaného jazyka pomocou rozbalovacej ponuky; jazyk sa potom použije pre celé [používateľské rozhranie AVG](#). V rozbalovacej ponuke sa nachádzajú len tie jazyky, ktoré ste nainštalovali počas [procesu inštalácie](#) (pozri kapitolu [Vlastná inštalácia – Výber súčastí](#)). Aby sa zmena jazyka prejavila, je potrebné reštartovať používateľské rozhranie; postupujte podľa nasledujúcich pokynov:

- Zvoľte požadovaný jazyk aplikácie a potvrdte výber stlačením tlačidla **Použiť** (v pravom spodnom rohu).
- Potvrdte stlačením tlačidla **OK**.
- Zobrazí sa nové dialógové okno, ktoré informuje, že na zmenu jazyka používateľského rozhrania AVG je potrebné reštartovať aplikáciu:



Informačné bubliny na paneli úloh

Táto časť umožňuje zrušiť zobrazovanie informačných bublín na paneli úloh informujúcich o stave aplikácie. Zobrazovanie informácií v bublinách je štandardne povolené a odporúča sa túto konfiguráciu ponechať! Informácie v bublinách obvyčajne informujú o zmene stavu niektorých komponentov AVG a mali by ste im venovať pozornosť!

Ak sa však z nejakého dôvodu rozhodnete, že nechcete, aby sa tieto informácie zobrazovali, alebo chcete, aby sa zobrazovali len niektoré informácie (súvisiace s konkrétnou súčasťou AVG), môžete definovať a zadať vlastné preferencie zaciarknutím/zrušením zaciarknutia nasledujúcich možností:

- **Zobrazit informácie na paneli úloh** – Táto položka je štandardne zaciarknutá (*zapnutá*) a zobrazujú sa informácie. Zrušte zaškrtnutie tejto položky, aby ste celkom vypli zobrazovanie všetkých informácií v bublinách. Po zapnutí môžete

ďalej zvolit, aké špecifické oznámenia by sa mali zobrazovať:

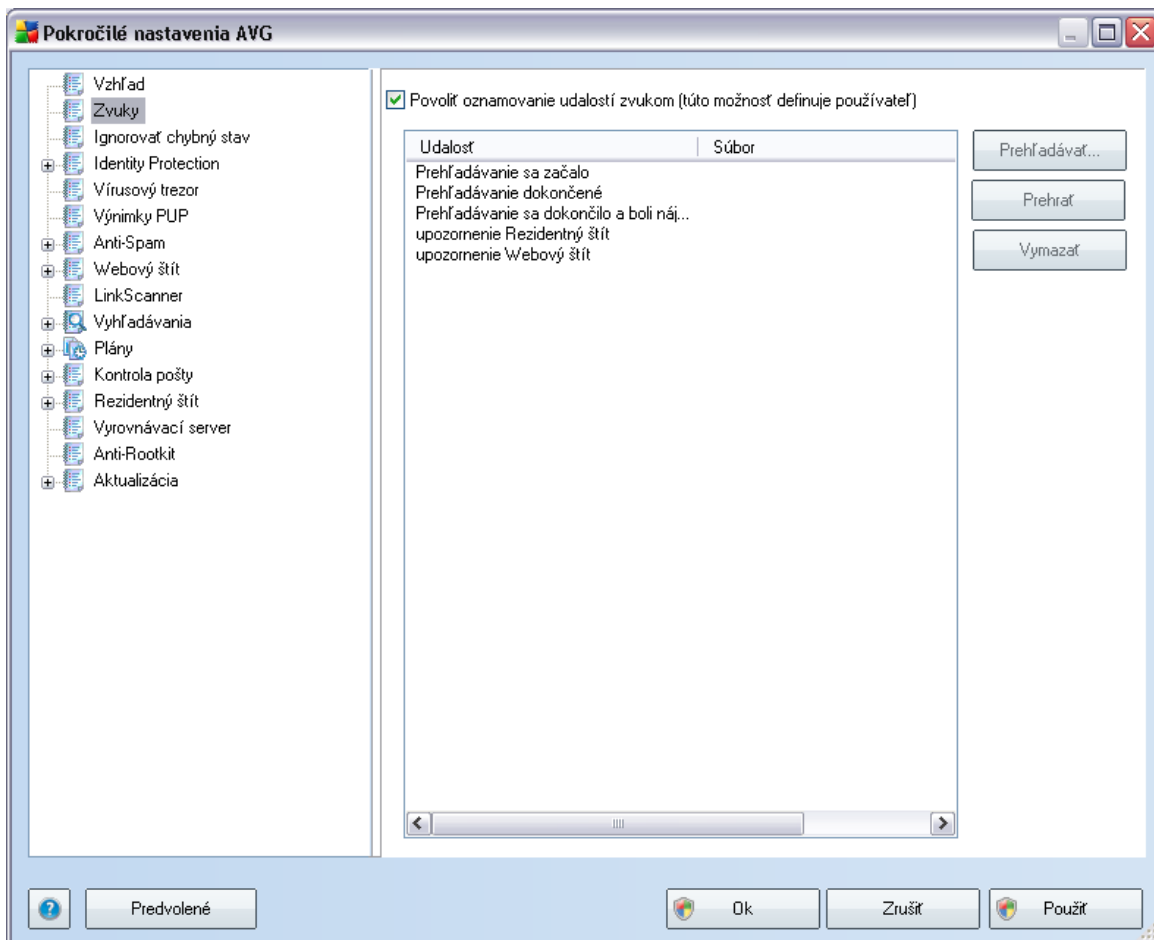
- **Zobraziť oznámenia o aktualizácii** na paneli úloh – Nastavte, či sa majú zobrazovať informácie súvisiace so spustením procesu aktualizácie programu AVG, jeho priebehom a dokončením.
- **Zobraziť oznámenia o zmene stavu súčasti** – Nastavte, či sa majú zobrazovať informácie súvisiace s aktivitou/necinnosťou súčasti, prípadne či sa majú zobrazovať informácie o možnom probléme. Pri oznamovaní chybového stavu súčasti táto možnosť zodpovedá informacnej funkcii [ikony na paneli úloh](#) (zmena farby), ktorá informuje o probléme jednotlivých súčastí AVG.
- **Zobraziť oznámenia súvisiace so súcastou Rezidentný štít na paneli úloh** – Nastavte, či sa majú alebo nemajú zobrazovať informácie súvisiace s procesmi ukladania, kopírovania a otvárania súborov (*táto funkcia je aktívna, len ak je zapnutá možnosť [Liecť automaticky](#) v súčasti Rezidentný štít*).
- **Zobraziť oznámenia o prehľadávaní** na paneli úloh – Nastavte, či sa majú zobrazovať informácie pri automatickom spustení naplánovaného prehľadávania, informácie o jeho priebehu a výsledkoch.
- **Zobraziť oznámenia súvisiace so súcastou Firewall na paneli úloh** – Nastavte, či sa majú zobrazovať informácie súvisiace so stavom a procesmi súčasti Firewall, napr. upozornenia o zapnutí/vypnutí súčasti, prípadne blokovanie prenosov atď.
- **Zobraziť oznámenia súvisiace so súcastou E-mail Scanner na paneli úloh** – Nastavte, či sa majú zobrazovať informácie po prehľadaní prichádzajúcich a odchádzajúcich e-mailových správ.

Režim hrania

Táto funkcia programu AVG sa používa v súvislosti s aplikáciami bežiacimi na celú obrazovku, ktorých chod by mohlo narušiť (*aplikácia by sa minimalizovala, alebo by sa porušila grafika*) zobrazenie informacnej bubliny programu AVG (*ktorá sa zobrazí napr. pri spustení naplánovaného prehľadávania*). Ak sa chcete vyhnúť podobným situáciám, nechajte zaciarkovacie políčko možnosti **Povolit režim hrania, ak beží aplikácia v režime na celú obrazovku** označené (*predvolené nastavenie*).

10.2. Zvuky

Dialógové okno **Zvuky** sa používa na zapnutie zvukových upozornení informujúcich o konkrétnych činnostiach programu AVG. Ak chcete túto funkciu zapnúť, označte možnosť **Povolit oznamovanie udalostí zvukom** (štandardne vypnuté), ktorá aktivuje zoznam činností programu AVG:

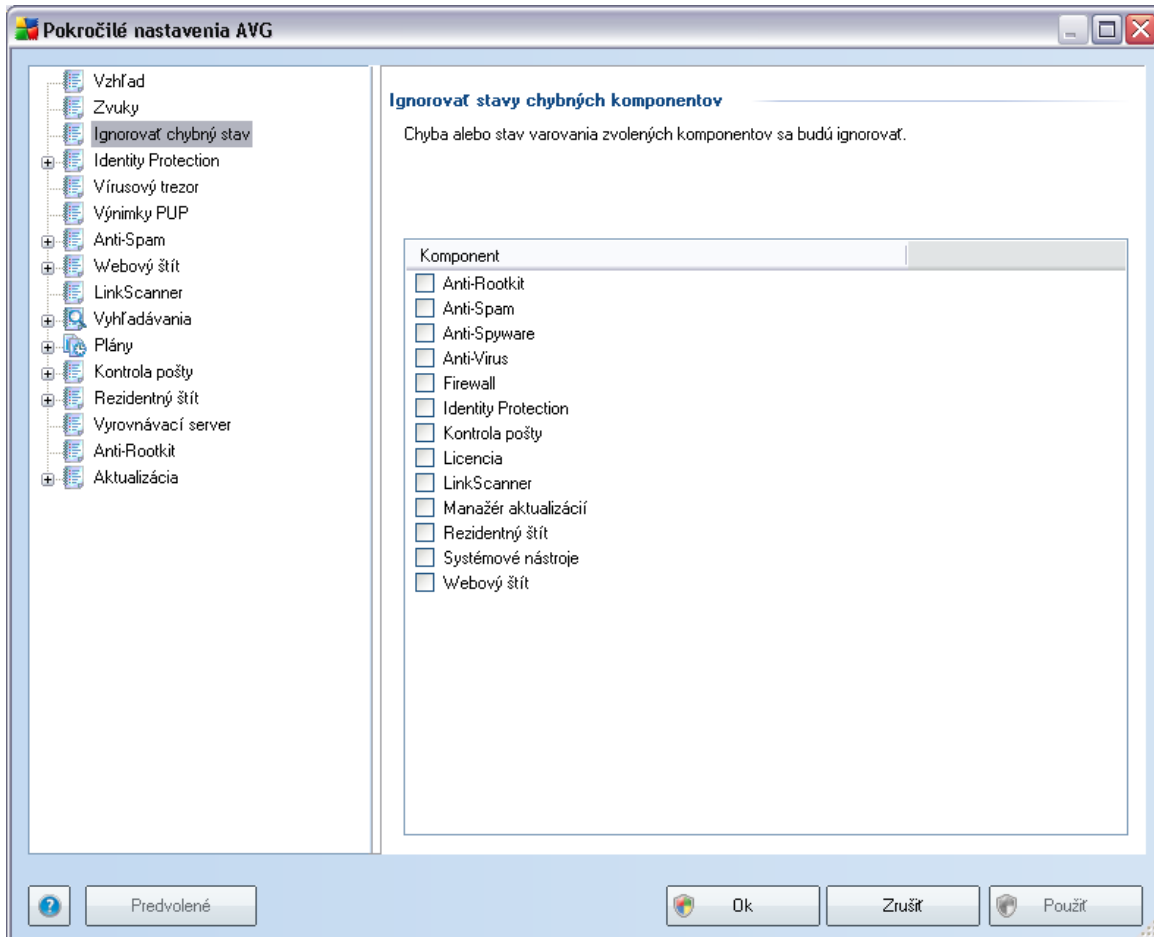


Potom zvolte požadovanú udalosť v zozname a na disku vyhladajte (tlacidlo **Prehľadávať**) vhodný zvuk, ktorý chcete pridelit tejto udalosti. Ak si chcete vypocut zvolený zvuk, zvýraznite udalosť v zozname a stlačte tlačidlo **Prehrať**. Na odstránenie zvuku prideleného konkrétnej udalosti použite tlačidlo **Vymazať**.

Poznámka: Použiť sa môžu len zvuky vo formáte *.wav.

10.3. Ignorovať chybný stav

Dialógové okno **Ignorovať chybový stav súčastí** vám umožní označiť tie súčasti, o ktorých nechcete byť informovaný:



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

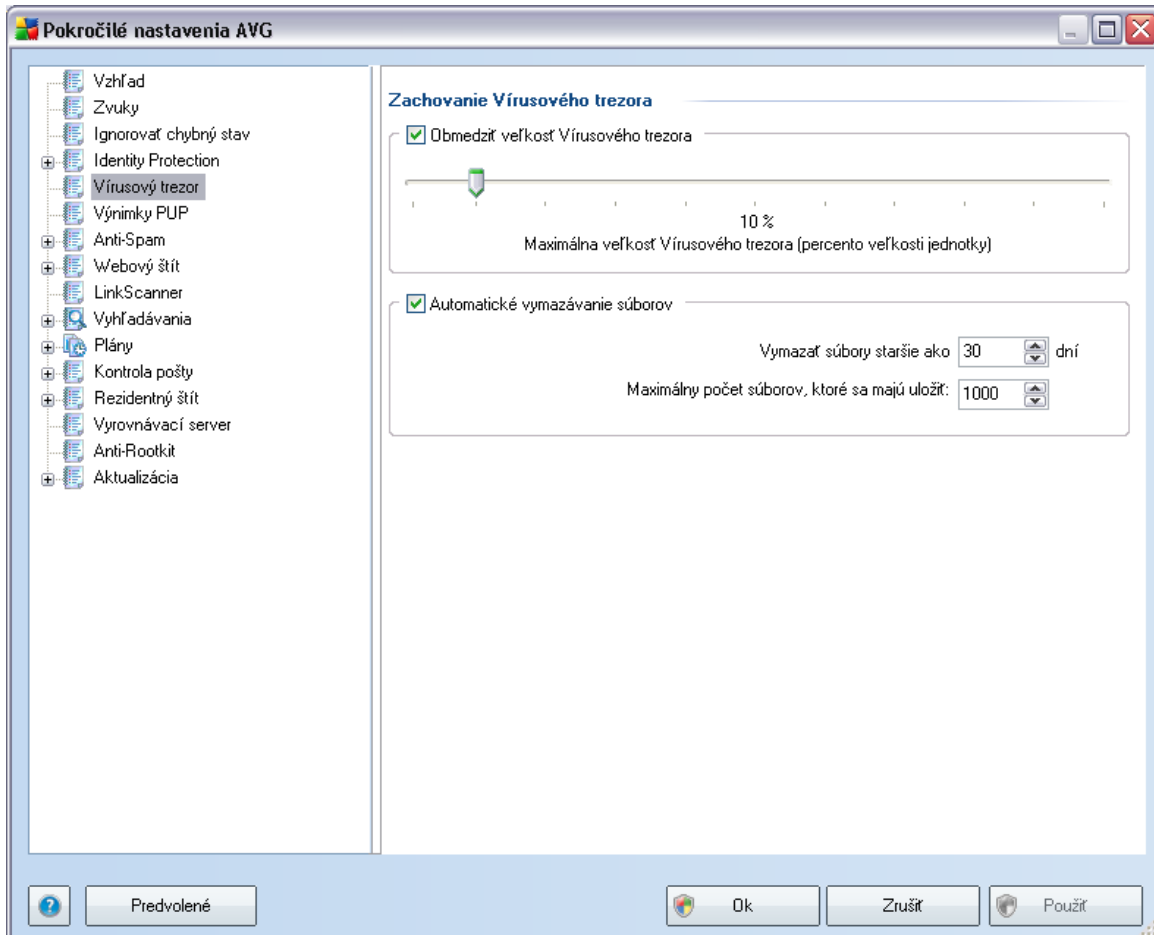
- **Ikony na paneli úloh:** Ak všetky časti aplikácie AVG fungujú správne, ikona je zobrazená v štyroch farbách; ak sa však vyskytne chyba, ikona sa zobrazí so žltým výkričníkom.
- Textového opisu existujúceho problému v časti **Informácie o stave**

zabezpečenia v hlavnom okne programu AVG.

Môže sa vyskytnúť situácia, keď bude potrebné z nejakého dôvodu súčast dočasne vypnúť (*neodporúčame vám to však; podľa možností nechajte všetky súčasti stále zapnuté a nemente predvolenú konfiguráciu*). V tom prípade ikona na systémovom pozadí automaticky oznámi chybový stav komponentu. V tomto konkrétnom prípade však nemôžeme hovoriť o skutočnej chybe, pretože ste ju vyvolali úmyselne a ste si vedomý potenciálneho rizika. A zároveň, keď je ikona zobrazená šedou farbou, ikona nemôže vlastne oznámiť žiadne ďalšie prípadné chyby, ktoré by sa mohli objaviť.

V tejto situácii môžete vo vyššie uvedenom dialógovom okne zvoliť súčasti, o ktorých prípadnom chybovom stav (*alebo vypnutí*) si neželáte byť informovaný. Tá istá možnosť **Ignorovať chybový stav** sa môže použiť pre konkrétne súčasti aj priamo v [prehlade súčastí v hlavnom okne programu AVG](#).

10.4. Vírusový trezor



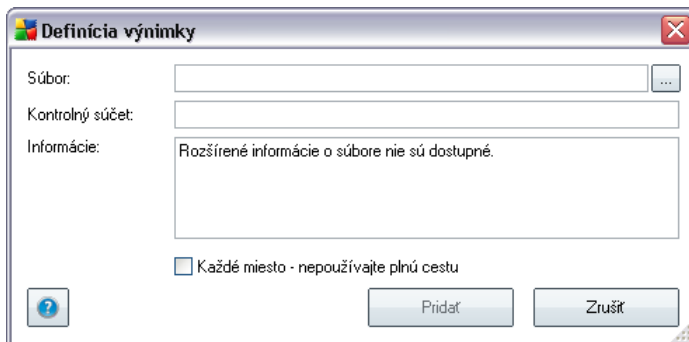
Dialógové okno **Zachovanie Vírusového trezora** vám umožňuje zdefinovať niekoľko parametrov ohľadom administrácie objektov uložených vo **Vírusovom trezore**:

- **Obmedziť veľkosť vírusového trezora** - použite posúvac na nastavenie maximálnej veľkosti **vírusového trezora**. Táto veľkosť sa uvádza úmerne v porovnaní s veľkosťou vášho lokálneho disku.
- **Automatické vymazávanie súborov** - v tejto časti môžete zdefinovať maximálnu dĺžku času, počas ktorého by mali byť objekty uložené vo **Vírusovom trezore** (**Vymazať súbory staršie ako ... dní**) a maximálny počet súborov, ktoré budú uložené vo **Vírusovom trezore** (**Maximálny počet uložených súborov**)

- **Súbor:** Uvádza názov príslušnej aplikácie.
- **Cesta k súboru:** Uvádza cestu k umiestneniu aplikácie.
- **Kontrolný súčet:** Uvádza jedinečný „podpis“ zvoleného súboru. Tento Kontrolný súčet je automaticky generovaný retazec znakov, ktorý umožňuje programu AVG jasne odlíšiť zvolený súbor od ostatných súborov. Kontrolný súčet sa generuje a zobrazí po úspešnom pridaní súboru.

Ovládacie tlačidlá

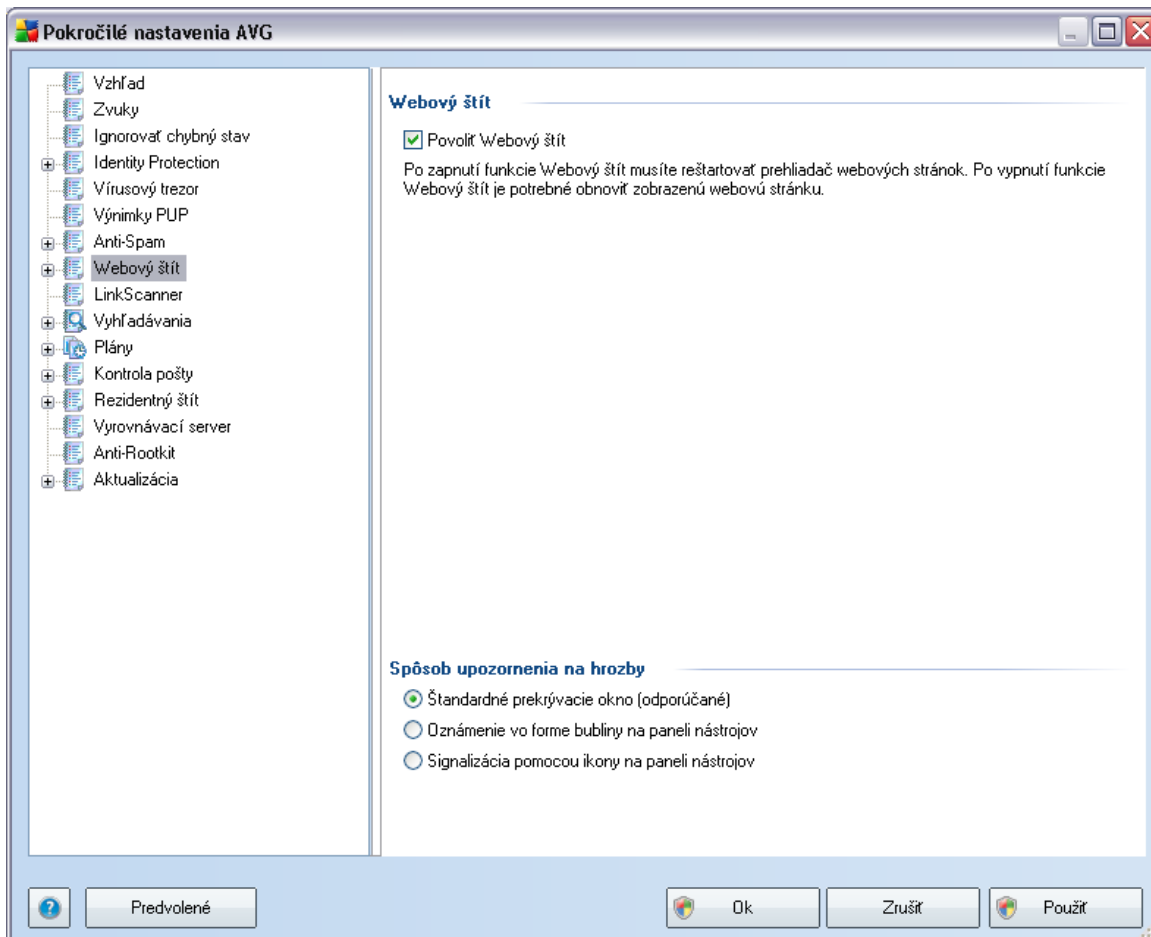
- **Editovať:** Otvorí dialógové okno editovania (*zhodné s dialógovým oknom na definovanie novej výnimky, pozri ďalej v texte*) už definovanej výnimky, v ktorom môžete zmeniť parametre výnimky.
- **Odstrániť:** Vymaže zvolenú položku zo zoznamu výnimiek.
- **Pridať výnimku:** Otvorí dialógové okno editovania, ktoré vám umožní definovať parametre novej výnimky, ktorá sa má vytvoriť:



- **Súbor:** Zadajte úplnú cestu k súboru, ktorý chcete označiť ako výnimku.
- **Kontrolný súčet:** Zobrazí jedinečný „podpis“ zvoleného súboru. Tento Kontrolný súčet je automaticky generovaný retazec znakov, ktorý umožňuje programu AVG jasne odlíšiť zvolený súbor od ostatných súborov. Kontrolný súčet sa generuje a zobrazí po úspešnom pridaní súboru.
- **Informácie o súbore:** Zobrazí všetky dostupné doplnujúce informácie o súbore (*informácie o licencií/verzii atď.*).
- **Každé umiestnenie – nepoužívať úplnú cestu:** Ak chcete definovať

tento súbor ako výnimku len pre konkrétne umiestnenie, nechajte toto okienko neoznačené.

10.6. Webový štít



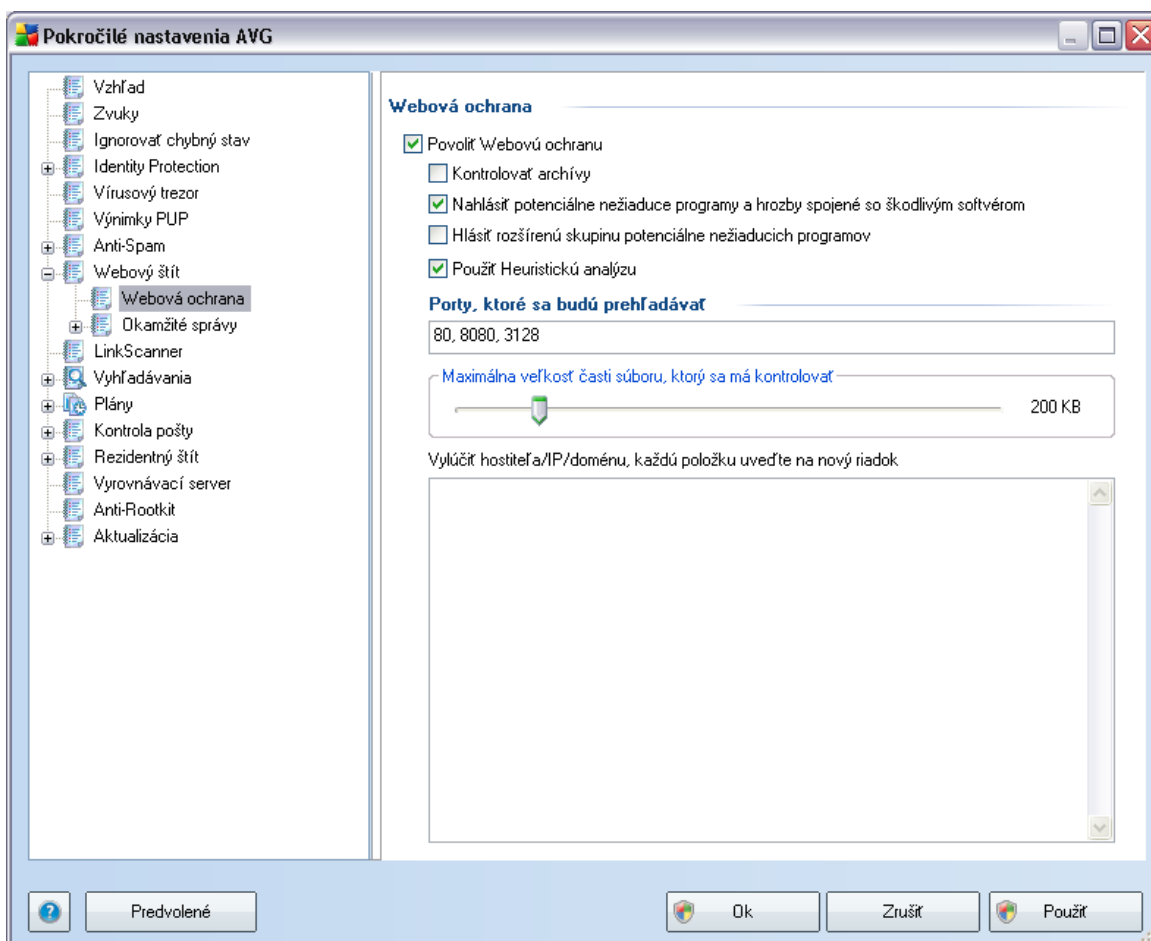
Dialógové okno **Webová ochrana** umožňuje zapnúť/vypnúť celú súčasť **Webový štít** pomocou možnosti **Zapnúť súčasť Webový štít** (štandardne zapnuté). Ak chcete prispôbiť ďalšie rozšírené nastavenia tejto súčasti, prejdite na nasledujúce dialógové okná uvedené v stromovej štruktúre:

- [Webová ochrana](#)
- [Okamžité správy](#)

Spôsob upozornenia na hrozby

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

10.6.1. Webová ochrana

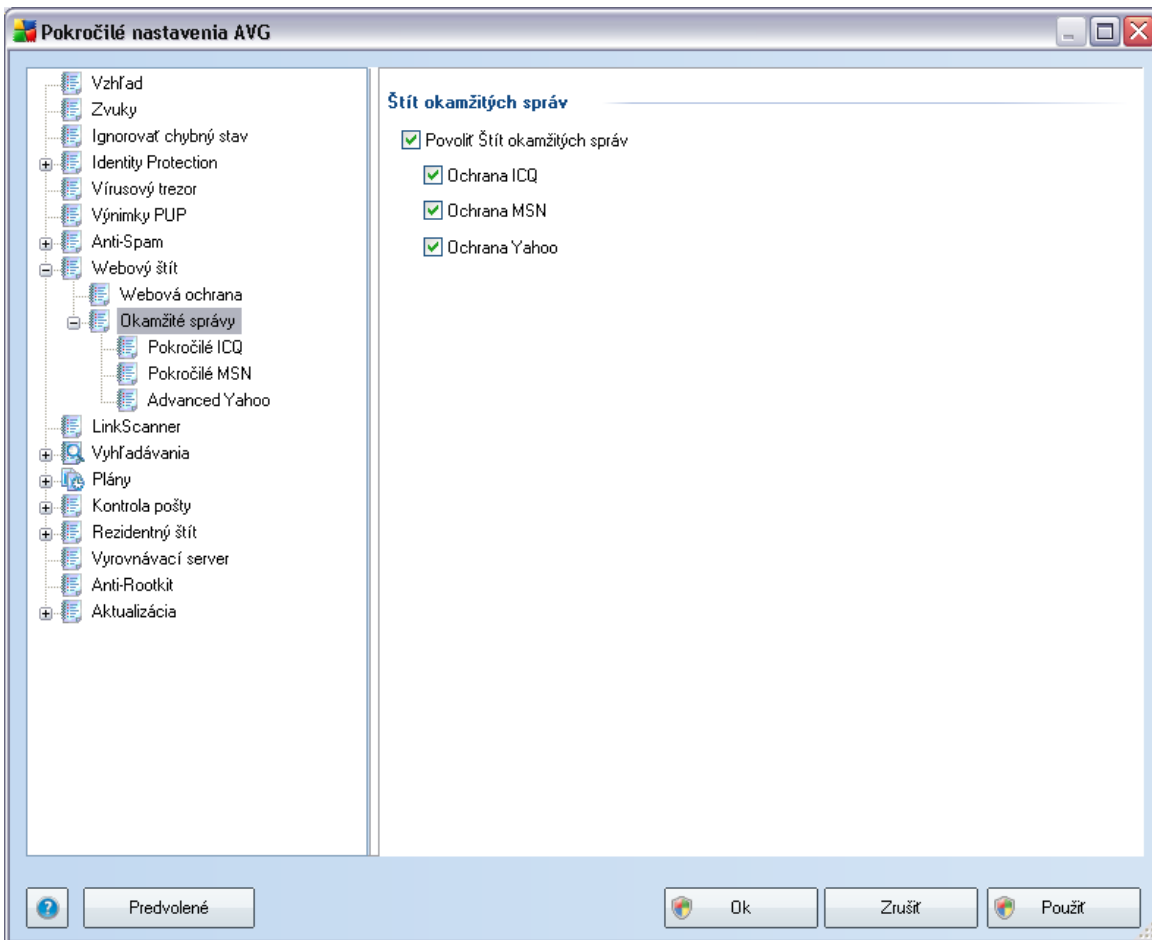


Dialógové okno **Webová ochrana** umožňuje editovať konfiguráciu súčasti z hladiska prehľadávania obsahu webových stránok. Editacné rozhranie umožňuje nastaviť nasledujúce základné možnosti:

- **Zapnúť webovú ochranu:** Ak je táto funkcia zapnutá, súčasť [Webový štít](#) bude prehľadávať obsah webových stránok. Ak je táto možnosť zapnutá (štandardne), môžete ďalej zapnúť/vypnúť tieto položky:
 - **Kontrolovať archívy:** Zapne prehľadávanie obsahu archívov, ktoré môžu byť súčasťou zobrazovanej webovej stránky.
 - **Hlásiť potenciálne nežiaduce programy a hrozby spyware (štandardne zapnuté):** Oznacíte túto možnosť, ak chcete zapnúť súčasť [Anti-Spyware](#) a vyhľadávať spyware a vírusy. [Spyware](#) predstavuje pochybnú kategóriu škodlivého softvéru: Aj keď obvyčajne predstavujú bezpečnostné riziko, niektoré takéto programy môžu byť nainštalované úmyselne. Odporúčame vám nechať túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
 - **Hlásiť rozšírenú skupinu potenciálne nežiaducich programov:** Ak je zapnutá predchádzajúca možnosť, môžete oznáčiť aj toto zaciarkovacie políčko, a tým povoliť detegovanie rozšírenej skupiny [spywaru](#): programov, ktoré sú úplne v poriadku a neškodné, ak sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje zabezpečenie vášho počítača, ale môže blokovat dobré programy, a preto je táto funkcia štandardne vypnutá.
 - **Použiť heuristickú analýzu:** Zapne prehľadávanie obsahu zobrazovanej stránky pomocou metódy [heuristickej analýzy](#) (dynamická emulácia inštrukcií prehľadávaného objektu vo virtuálnom počítačovom prostredí).
 - **Kontrolované porty:** V tomto poli sa nachádza zoznam štandardných čísiel komunikačných portov HTTP. Ak používate počítač s inou konfiguráciou, podľa potreby môžete zmeniť čísla portov.
 - **Maximálna čiastková veľkosť prehladávaného súboru:** Ak sa priložené súbory nachádzajú na zobrazovanej stránke, ich obsah sa môže zároveň skontrolovať ešte predtým, než sa súbory prevezmú do počítača. Prehľadávanie veľkých súborov však chvíľu trvá a preberanie z webovej stránky sa môže výrazne spomaliť. Pomocou posúvaca môžete nastaviť maximálnu veľkosť súboru, ktorý sa má prehľadať súčasťou [Webový štít](#). Aj keď je prevzatý súbor väčší než nastavená hodnota, a z tohto dôvodu ho súčasť Webový štít neskontroluje, váš počítač je stále chránený: ak je súbor infikovaný, súčasť [Rezidentný štít](#) ho ihneď deteguje.
 - **Vylúčiť hosťiteľa/adresu IP/doména:** Do textového poľa zadajte presný názov servera (hosťiteľa, adresu IP, adresu IP s maskou alebo

adresu URL) alebo doménu, ktorú súčasť **Webový štít** nemá prehľadávať. Preto vylúčte len hostitela, o ktorom ste si absolútne istý, že by nikdy neposlal nebezpečné dáta.

10.6.2. Štít okamžitých správ



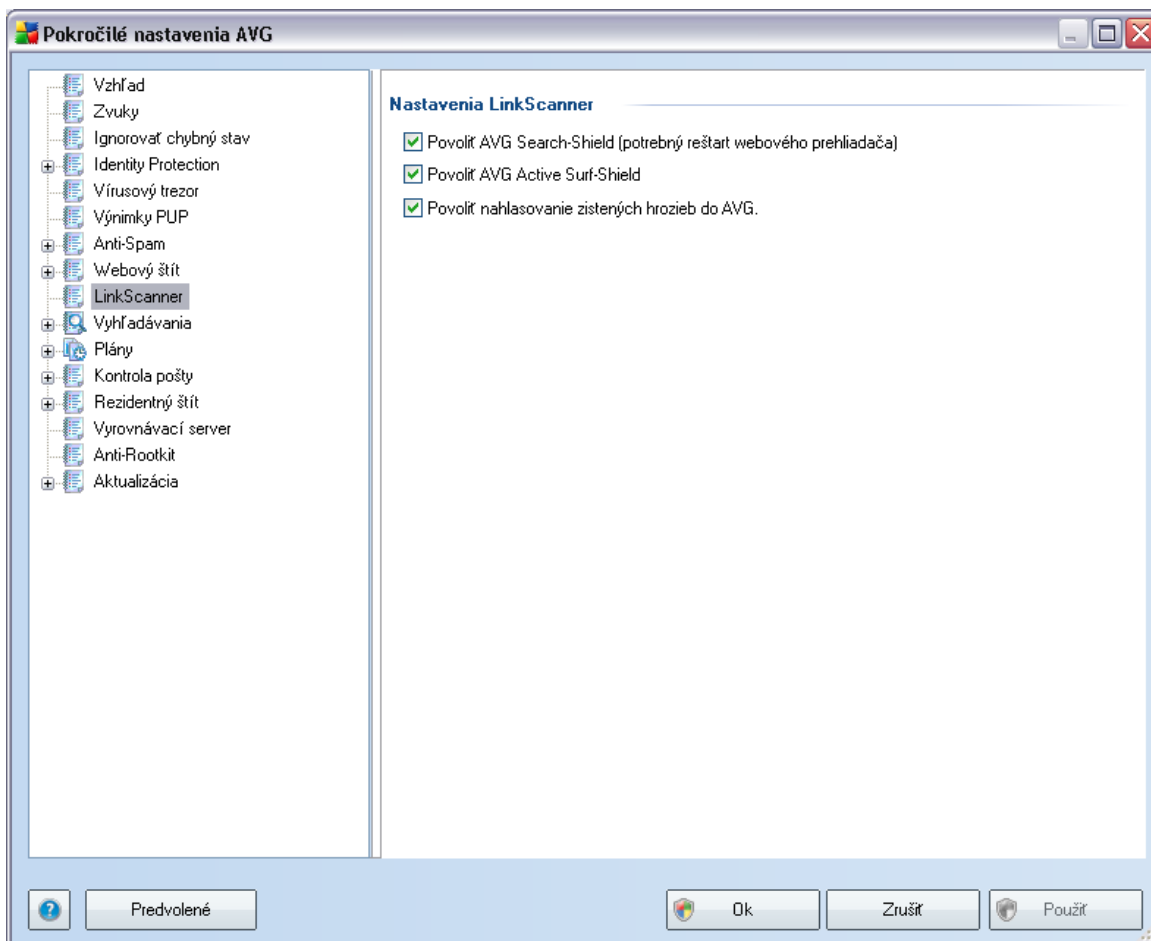
Dialógové okno **Štít okamžitých správ** umožňuje editovať nastavenia súčasti **Webový štít**, ktoré súvisia s prehľadávaním okamžitých správ. Aplikácia v súčasnosti podporuje nasledujúce tri programy pre okamžité správy: **ICQ**, **MSN** a **Yahoo** – označte príslušnú položku pre každý z týchto programov, ak chcete, aby súčasť **Webový štít** kontrolovala, či online komunikácia neobsahuje vírusy.

Ak chcete ďalej definovať povolených/blokovaných používateľov, otvorte príslušné dialógové okno (**Rozšírené ICQ**, **Rozšírené MSN**, **Rozšírené Yahoo**) a upravte jeho nastavenia a definujte **zoznam povolených používateľov** (zoznam používateľov,

ktorí s vami budú môcť komunikovať) a **zoznam blokových používateľov** (používateľov, ktorí budú blokovaní).

10.7. Kontrola odkazov

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



- **Zapnúť AVG Search-Shield** (štandardne zapnuté): Informačné ikony s odporúčaniami pre výsledky vyhľadávania zistené službou Google, Yahoo, Bing, Yandex, Altavista a Baidu a skontrolované predtým, ako sa obsah nájdených stránok zobrazí v prehliadaci.
- **Povoliť AVG Active Surf-Shield** (štandardne zapnuté): Používa sa na zapnutie

ochrany (v *reálnom case*) pred webovými stránkami s nebezpečným obsahom pri ich sprístupnení. Pripojenie na známe nebezpečné stránky a ich nebezpečný obsah sa zablokuje pri sprístupňovaní pomocou webového prehliadaca (*alebo inej aplikácie, ktorá používa protokol HTTP*).

- **Zapnúť oznamovanie zistených hrozieb do AVG** (štandardne zapnuté): Označením tejto položky povolíte oznamovanie hrozieb a zlých stránok zistených používateľmi buď pomocou funkcie **AVG Active Surf-Shield** alebo **AVG Search-Shield** do databázy nebezpečných aktivít na webe.

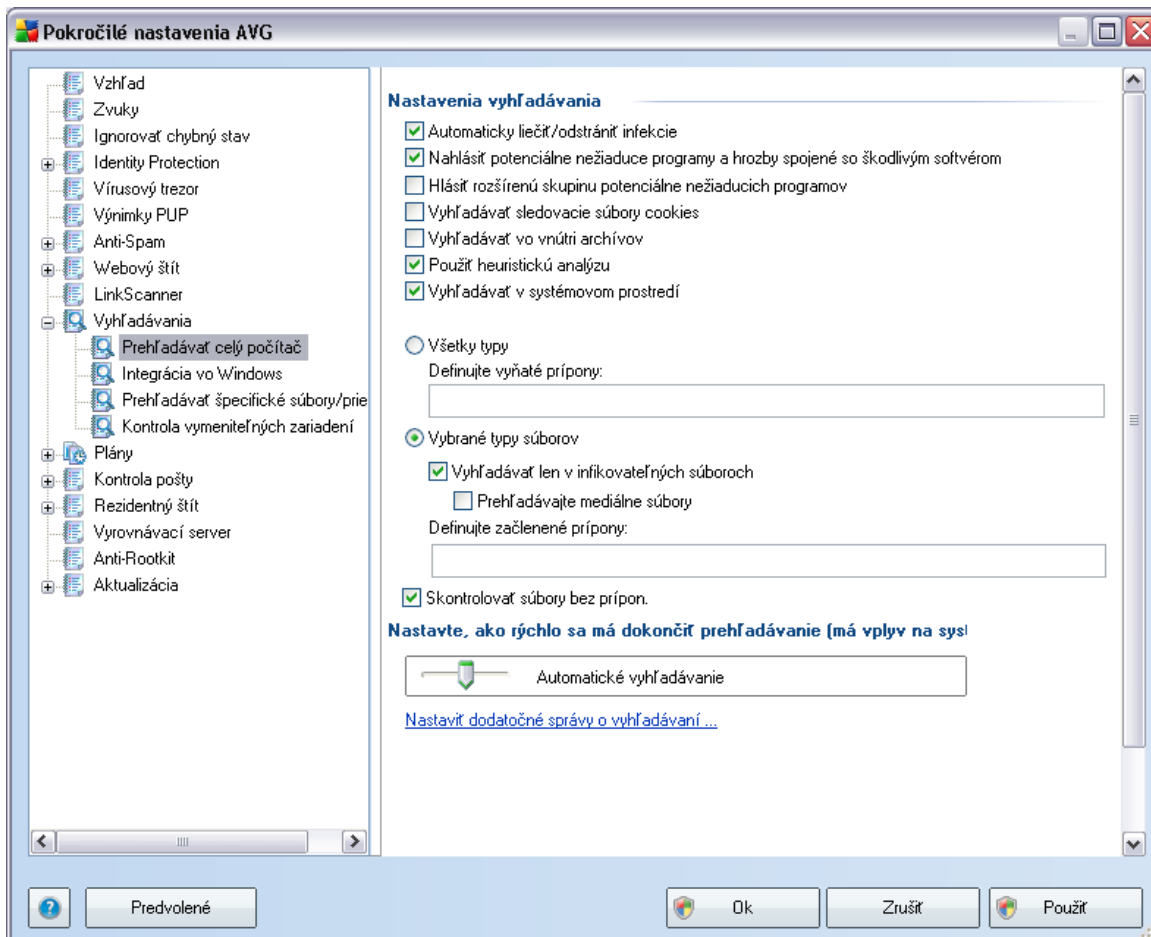
10.8. Vyhľadávania

Pokročilé nastavenia vyhľadávania sú rozdelené na tri kategórie, ktoré sa vzťahujú na špecifické typy vyhľadávania podľa definície predajcom softvéru:

- **Prehľadávať celý počítač** - štandardné vopred zadané prehľadávanie celého počítača
- **Prehľadávať v prieskumníkovi** - špeciálne prehľadávanie vybraného objektu priamo v prostredí programu Windows Explorer.
- **Prehľadávať špecifické súbory alebo priecinky** - štandardné vopred definované prehľadávanie vybraných oblastí počítača.
- **Prehľadávať vymeniteľné zariadenia** - špeciálne prehľadávanie vymeniteľných zariadení zapojených do počítača.

10.8.1. Prehľadávať celý počítač

Funkcia **Prehľadávať celý počítač** umožňuje editovať parametre jedného z prehľadávaní vopred definovaných výrobcov softvéru, **Prehľadávať celý počítač**:



Nastavenia prehľadávaní

V časti **Nastavenia prehľadávaní** sa nachádza zoznam parametrov prehľadávania, ktoré sa dajú voliteľne zapnúť/vypnúť:

- **Automatically detect/remove infection:** Ak sa počas vyhľadávania identifikuje vírus, môže sa automaticky vyliečiť, ak je k dispozícii liečba. Ak infikovaný súbor nie je možné vyliečiť automaticky, premiestni sa do **Vírusového trezora**.

- **Hlásit potenciálne nežiaduce programy a hrozby spyware** (štandardne zapnuté): Označte túto možnosť, ak chcete zapnúť súčasť [Anti-Spyware](#) a vyhľadávať spyware a vírusy. [Spyware](#) predstavuje pochybnú kategóriu škodlivého softvéru: Aj keď obvyčajne predstavujú bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporúčame vám nechať túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
- **Hlásit rozšírenú skupinu potenciálne nežiaducich programov**: Ak je zapnutá predchádzajúca možnosť, môžete označiť aj toto zaciarkovacie políčko, a tým povoliť detegovanie rozšírenej skupiny [spywaru](#): programov, ktoré sú úplne v poriadku a neškodné, ak sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje zabezpečenie vášho počítača, ale môže blokovat dobré programy, a preto je táto funkcia štandardne vypnutá.
- **Vyhľadávať sledovacie súbory cookies**: Tento parameter súčasť [Anti-Spyware](#) zapína funkciu zisťovania prítomnosti súborov cookies; (*HTTP cookies sa používajú na overenie totožnosti, sledovanie a správu konkrétnych informácií o používateľoch, akými sú preferencie stránok alebo obsah elektronických nákupných košíkov*).
- **Prehľadávať vo vnútri archívov**: Tento parameter stanovuje, že počas prehľadávania sa majú kontrolovať všetky súbory, aj keď sú uložené vo vnútri archívu, napr. ZIP, RAR...
- **Použiť heuristiku**: Heuristická analýza (*dynamická emulácia inštrukcií prehľadávaného objektu vo virtuálnom počítačovom prostredí*) bude predstavovať jednu z metód použitých na detegovanie vírusov počas prehľadávania.
- **Prehľadávať systémové prostredie**: Pocas prehľadávania sa budú kontrolovať aj systémové oblasti počítača.

Dalej rozhodnite, či chcete prehľadávať:

- **Všetky typy súborov** s možnosťou definovať výnimky prehľadávania vytvorením zoznamu ciarkou oddelených (*uložením sa ciarky zmenia na bodkociarky*) prípon súborov, ktoré sa nemajú prehľadávať.
- **Zvolené typy súborov**: Môžete nastaviť, že chcete prehľadávať len súbory, pri ktorých existuje pravdepodobnosť infikovania (*súbory, ktoré nemôžu byť napadnuté infekciou, napríklad niektoré jednoduché textové súbory, alebo niektoré nespustiteľné súbory*), vrátane mediálnych súborov (*video, audio súborov – ak necháte toto políčko neoznačené, čas prehľadávania sa skrúti 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 prehľadávať vždy.

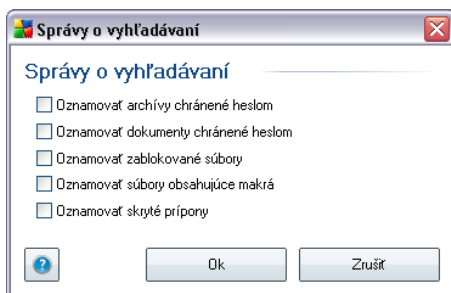
- Alternatívne môžete rozhodnúť, že chcete **prehľadávať súbory bez prípony**. Táto možnosť je štandardne zapnutá a odporúčame vám nikdy nemeniť túto konfiguráciu, ak na to nemáte skutočný dôvod. Súbory bez prípony sú skôr podozrivé a mali by sa vždy prehľadávať.

Priorita procesu prehľadávania

V časti **Priorita procesu prehľadávania** môžete ďalej špecifikovať želanú rýchlosť prehľadávania v závislosti od využitia systémových zdrojov. Štandardne je táto možnosť nastavená na strednú úroveň automatického využívania zdrojov. Ak chcete, aby prehľadávanie prebiehalo rýchlejšie, bude trvať kratšie, ale výrazne sa zvýši využitie systémových zdrojov a spomalia sa ostatné činnosti v počítači (*táto možnosť sa môže použiť, keď je počítač zapnutý, ale nikto na ňom momentálne nepracuje*). Na druhej strane môžete znížiť využitie systémových zdrojov predĺžením doby trvania prehľadávania.

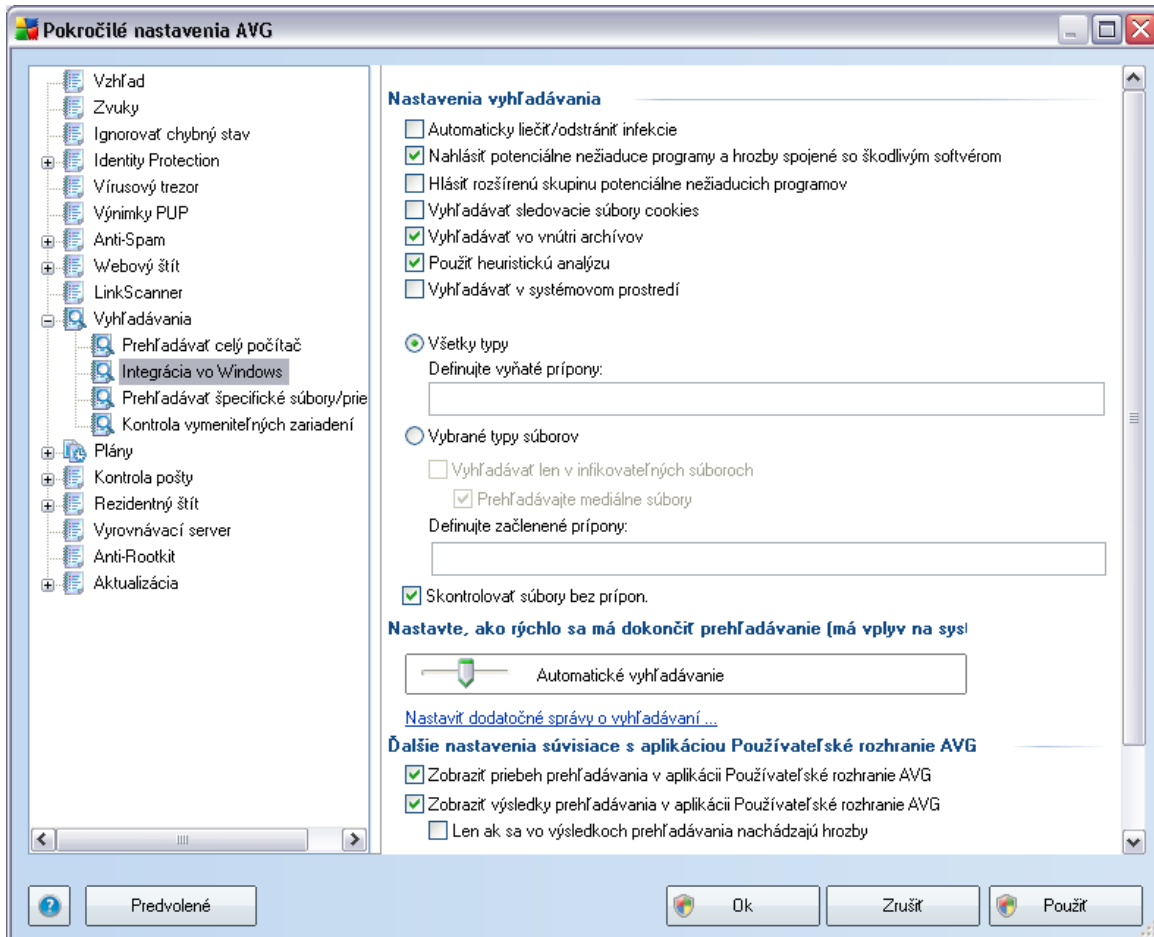
Vytvoriť ďalšie správy o prehľadávaní...

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



10.8.2. Prehľadávať v prieskumníkovi

Rovnako ako predchádzajúca funkcia **Prehľadávať celý počítač**, aj táto funkcia s názvom **Prehľadávať shell extension** ponúka niekoľko možností na editovanie prehľadávania definovaného výrobcom softvéru. V tomto prípade konfigurácia súvisí s [prehľadávaním konkrétnych objektov spustených v prostredí programu Prieskumník \(shell extension\)](#), pozri kapitolu [Prehľadávanie v programe Prieskumník](#):

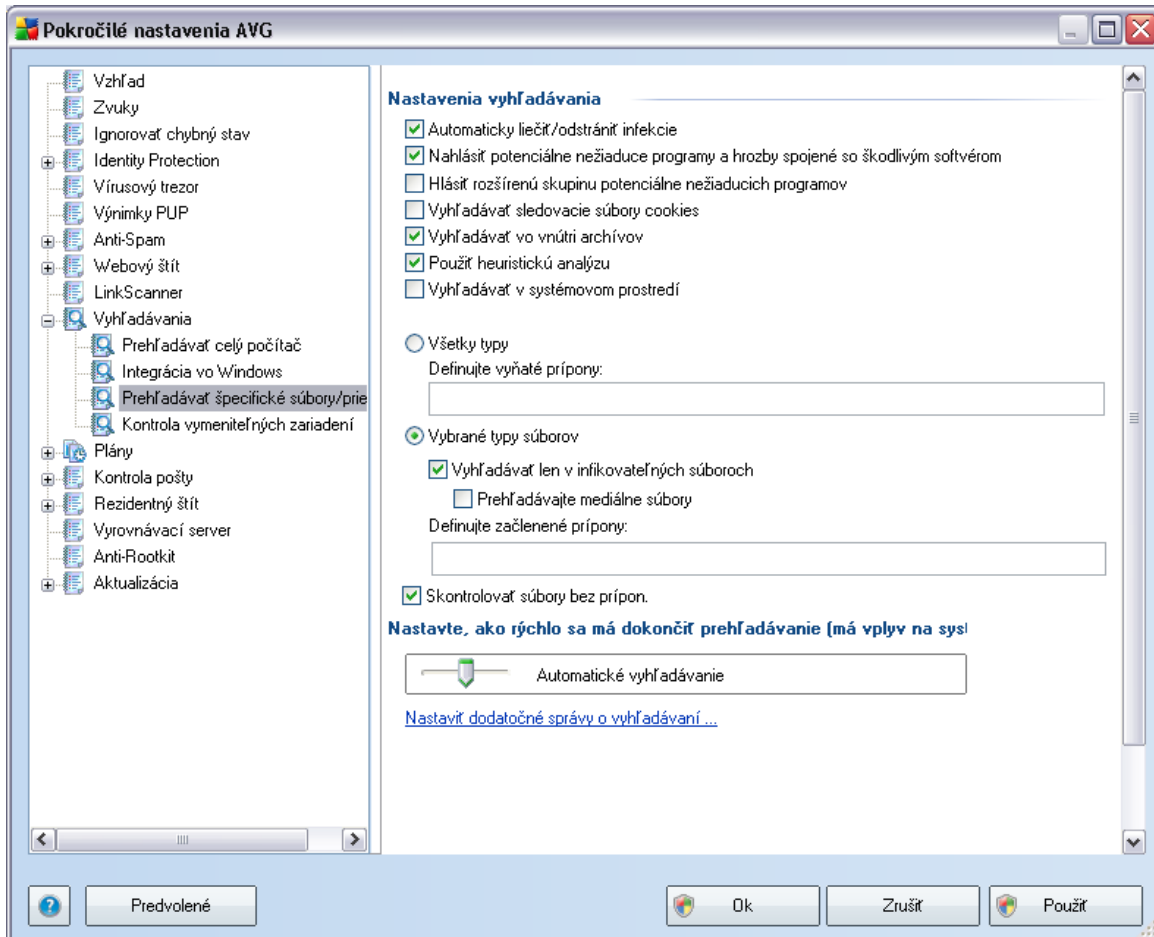


Zoznam parametrov je identický s parametrami použiteľnými pre [prehľadovanie celého počítača](#). Predvolené nastavenia sa však líšia: **prehľadovanie celého počítača** používa väčšinu parametrov, zatiaľ čo pri **prehľadávaní v rozšíreniach shell extension** ([Prehľadovanie v programe Prieskumník](#)) sú zapnuté len súvisiace parametre.

Poznámka: Informácie o konkrétnych parametroch sa nachádzajú v kapitole [Rozšírené nastavenia AVG/Prehľadovania/Prehľadávať celý počítač](#).

10.8.3. Prehľadávať špecifické súbory alebo priecinky

Rozhranie úprav pre **Prehľadovanie špecifických súborov alebo priecinkov** je rovnaké ako dialógové okno úprav [Prehľadávať celý počítač](#). Všetky možnosti konfigurácie sú rovnaké, predvolené nastavenia sú však prísnejšie pri [Prehľadávaní celého počítača](#):

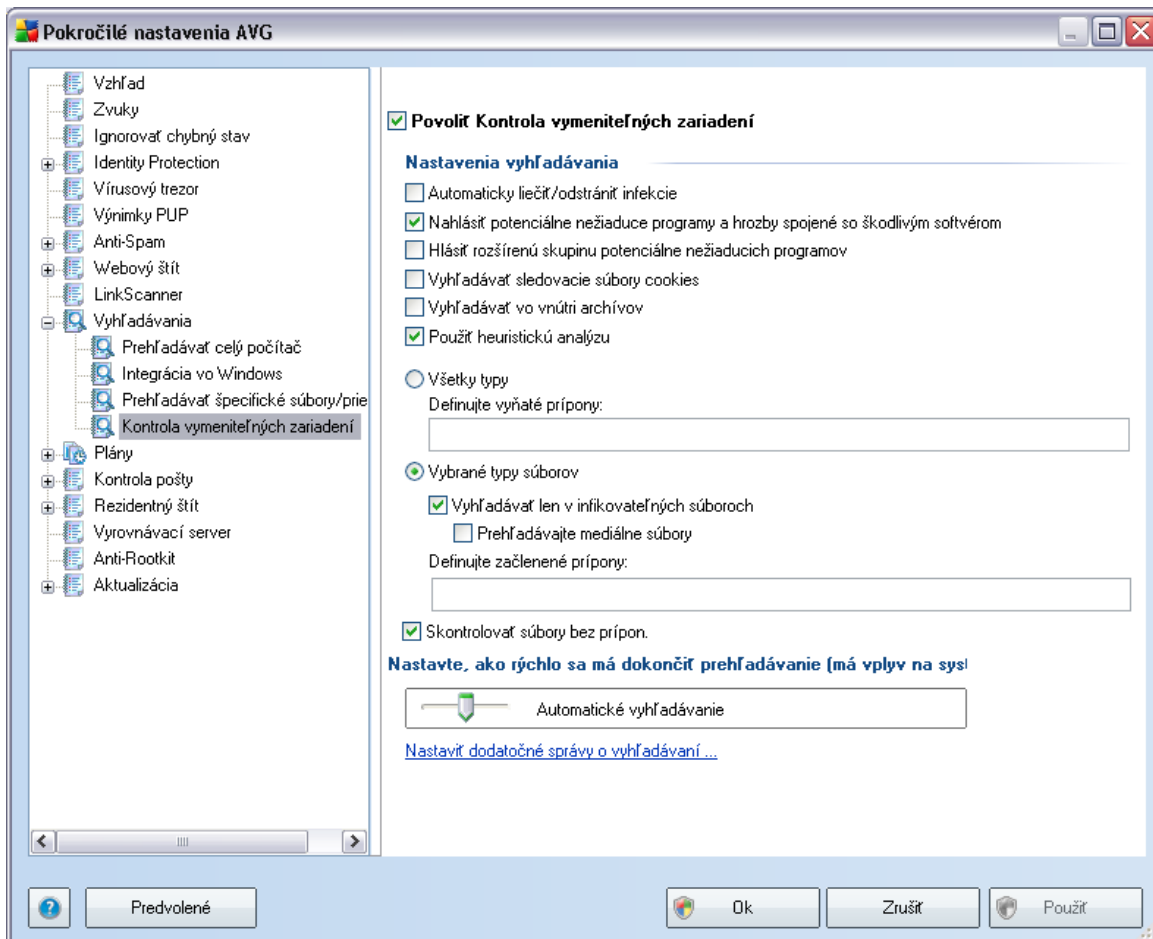


Všetky parametre nastavené v tomto dialógovom okne konfigurácie sa vzťahujú len na oblasť zvolenú pre vyhľadávanie v dialógovom okne **[Prehľadávať špecifické súbory alebo priecinky!](#)**

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

10.8.4. Prehľadovanie vymeniteľných zariadení

Editovateľné rozhranie pre **Prehľadovanie vymeniteľných zariadení** sa tiež veľmi podobá editovateľnému dialógovému oknu [Prehľadovať celý počítač](#):



Prehľadovanie vymeniteľných zariadení sa spustí automaticky po zapojení vymeniteľného zariadenia do počítača. Toto prehľadovanie je štandardne vypnuté. Prehľadovanie vymeniteľných zariadení je však veľmi dôležité z hľadiska potenciálnych hrozieb, pretože tieto predstavujú zdroj infekcie. Ak chcete, aby toto prehľadovanie bolo pripravené a spustilo sa automaticky v prípade potreby, oznacíte možnosť **Povolit prehľadovanie vymeniteľných zariadení**.

Poznámka: Informácie o konkrétnych parametroch sa nachádzajú v kapitole [Rozšírené nastavenia AVG / Prehľadovania / Prehľadovať celý počítač](#).

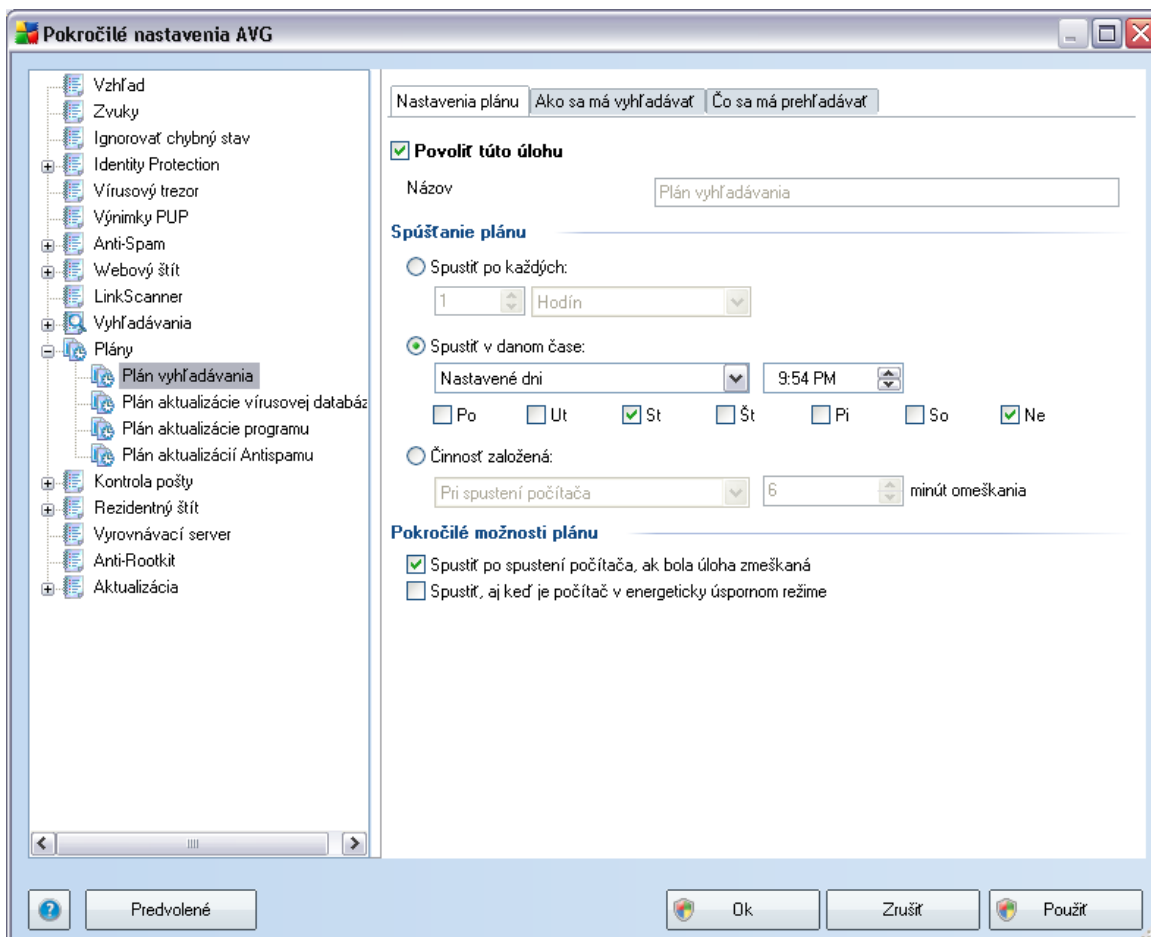
10.9. Plány

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

- [Plán prehľadávania celého počítača](#)
- [Plán aktualizácie vírusovej databázy](#)
- [Plán aktualizácie programu](#)

10.9.1. Plánované vyhľadávanie

Parametre plánovaného vyhľadávania sa dajú upraviť (*alebo sa dá nastaviť nový plán*) v troch kartách:



Na karte **Nastavenia plánu** najskôr oznacením/zrušením oznacenia položky **Povolit túto úlohu** jednoducho dočasne vypnete naplánovaný test a znova ho zapnete v prípade potreby.

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

Príklad: Nie je vhodné nazvať prehľadávanie „Nové prehľadávanie“ alebo „Moje

vyhľadávanie", pretože tieto názvy nesúvisia s tým, čo sa prehľadávanie vlastne kontroluje. Na druhej strane, príkladom dobrého opisného názvu je „Prehľadávanie systémových oblastí“ a pod. Takisto nie je potrebné zadať do názvu prehľadávania, či ide o prehľadávanie celého počítača alebo prehľadávanie zvolených súborov alebo priečinkov, pretože vaše vlastné prehľadávania budú vždy predstavovať špeciálnu verziu [prehľadávania zvolených súborov alebo priečinkov](#).

Toto dialógov umožňuje ďalej definovať nasledujúce parametre prehľadávania:

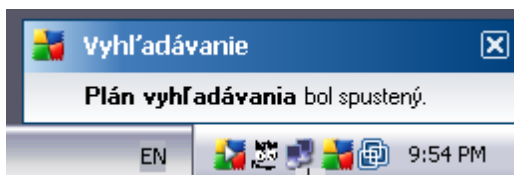
Spúšťanie naplánovaných úloh

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

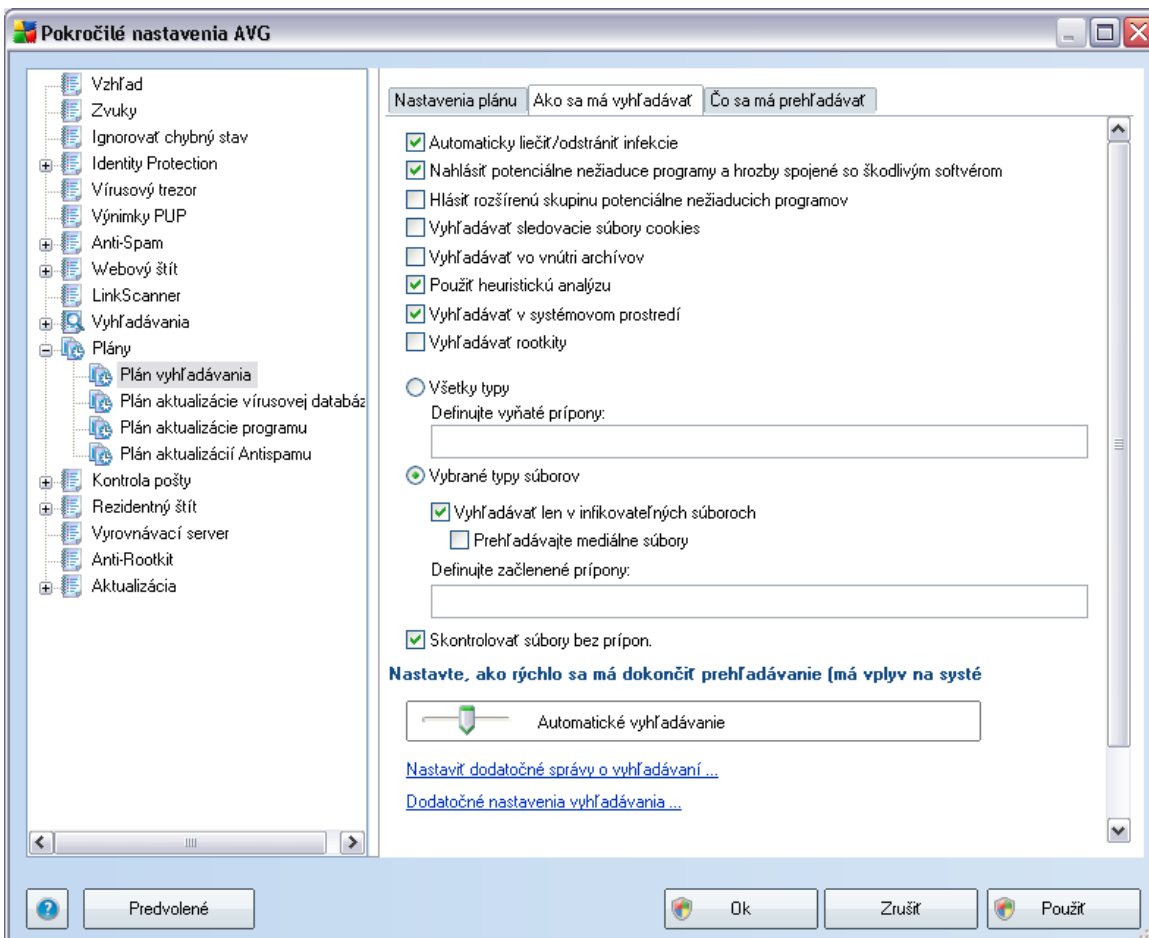
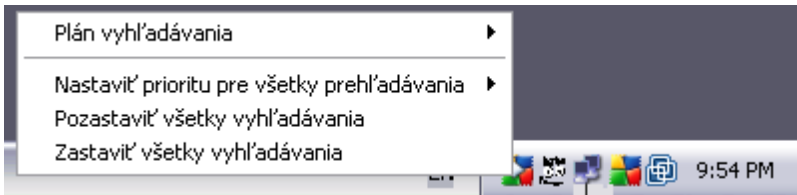
Rozšírené možnosti plánu

Táto časť sa používa na definovanie podmienok, pri ktorých sa má/nemá spustiť prehľadávanie, ak je počítač v úspornom režime alebo úplne vypnutý.

Keď sa spustí naplánované prehľadávanie v nastavenom čase, budete o tejto skutočnosti informovaný pomocou prekryvacieho okna, ktoré sa otvorí nad [ikonou AVG na paneli úloh](#):



Potom sa objaví nová [ikona AVG na paneli úloh](#) (farebná s bielou šípkou – pozri obrázok vyššie), ktorá informuje o tom, že prebieha naplánované prehľadávanie. Kliknutím pravým tlačidlom myši na ikonu AVG prebiehajúceho prehľadávania otvoríte kontextovú ponuku, ktorá vám umožní pozastaviť alebo dokonca zastaviť prebiehajúce prehľadávania:



Na karte **Ako sa má prehľadávať** sa nachádza zoznam parametrov prehľadávania, ktoré sa dajú zapnúť resp. vypnúť. Štandardne je väčšina parametrov zapnutá a daná funkcia sa počas vyhľadávania uplatní. Ak nemáte závažný dôvod meniť tieto nastavenia, odporúčame vám ponechať vopred nastavenú konfiguráciu:

- **Automaticky liečiť/odstrániť infekciu:** Ak sa počas vyhľadávania identifikuje

vírus, môže sa automaticky vyliečiť, ak je k dispozícii liečba. Ak infikovaný súbor nie je možné vyliečiť automaticky, premiestni sa do [Vírusového trezora](#).

- **Hlásit potenciálne nežiaduce programy a hrozby spyware** (štandardne zapnuté): Označíte túto možnosť, ak chcete zapnúť súčasť [Anti-Spyware](#) a vyhľadávať spyware a vírusy. [Spyware](#) predstavuje pochybnú kategóriu škodlivého softvéru: Aj keď obvyčajne predstavujú bezpečnostné riziko, niektoré takéto programy môžu byť nainštalované úmyselne. Odporúčame vám nechať túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
- **Hlásit rozšírenú skupinu potenciálne nežiaducich programov**: Ak je zapnutá predchádzajúca možnosť, môžete označiť aj toto zaciarkovacie políčko, a tým povoliť detegovanie rozšírenej skupiny [spywaru](#): programov, ktoré sú úplne v poriadku a neškodné, ak sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje zabezpečenie vášho počítača, ale môže blokovat dobré programy, a preto je táto funkcia štandardne vypnutá.
- **Vyhľadávať sledovacie súbory cookies** (štandardne zapnuté): Tento parameter súčasť [Anti-Spyware](#) zapína funkciu zisťovania prítomnosti súborov cookies počas prehľadávania; (*HTTP cookies sa používajú na overenie totožnosti, sledovanie a správu konkrétnych informácií o používateľoch, akými sú napr. preferencie stránok alebo obsah elektronických nákupných košíkov*).
- **Prehľadávať vo vnútri archívov**: (štandardne zapnuté): Tento parameter stanovuje, že počas prehľadávania sa majú kontrolovať všetky súbory, aj keď sú zabalené vo vnútri archívu, napr. ZIP, RAR...
- **Použiť heuristiku** (štandardne zapnuté): Heuristická analýza (*dynamická emulácia inštrukcií prehľadávaného objektu vo virtuálnom počítačovom prostredí*) bude predstavovať jednu z metód použitých na detegovanie vírusov počas prehľadávania.
- **Prehľadávať systémové prostredie** (štandardne zapnuté): Pocas prehľadávania sa budú kontrolovať aj systémové oblasti počítača.
- **Vyhľadávať rootkity**: Označíte túto položku, ak chcete zahrnúť zisťovanie prítomnosti rootkitov do kontroly celého počítača. Funkcia zisťovania prítomnosti rootkitov sa nachádza aj samostatne v súčasť [Anti-Rootkit](#).

Dalej rozhodnite, či chcete prehľadávať:

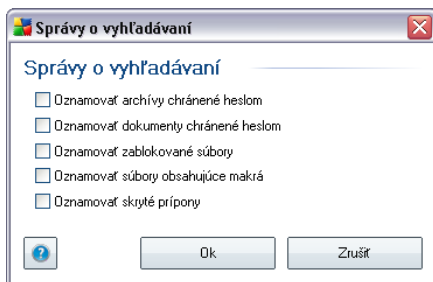
- **Všetky typy súborov** s možnosťou definovať výnimky prehľadávania vytvorením zoznamu ciarkou oddelených (*uložením sa ciarky zmenia na bodkociarky*) prípon súborov, ktoré sa nemajú prehľadávať.

- **Zvolené typy súborov:** Môžete nastaviť, že chcete prehľadávať len súbory, pri ktorých existuje pravdepodobnosť infikovania (súbory, ktoré nemôžu byť napadnuté infekciou, napríklad niektoré jednoduché textové súbory, alebo niektoré nespustiteľné súbory), vrátane mediálnych súborov (video, audio súborov – ak necháte toto políčko neoznačené, čas prehľadávania sa skrúti 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 prehľadávať vždy.
- Alternatívne môžete rozhodnúť, že chcete **prehľadávať súbory bez prípony**. Táto možnosť je štandardne zapnutá a odporúčame vám nikdy nemeniť túto konfiguráciu, ak na to nemáte skutočný dôvod. Súbory bez prípony sú skôr podozrivé a mali by sa vždy prehľadávať.

Priorita procesu prehľadávania

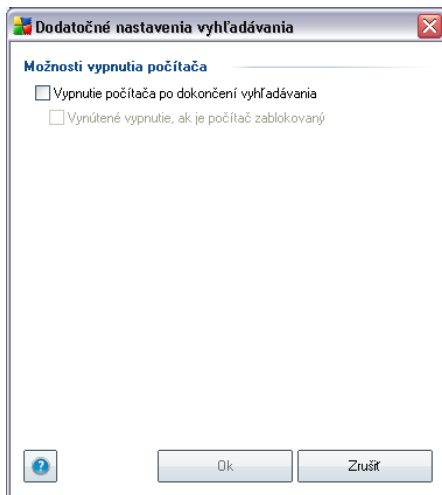
V časti **Priorita procesu prehľadávania** môžete ďalej špecifikovať želanú rýchlosť prehľadávania v závislosti od využitia systémových zdrojov. Štandardne je táto možnosť nastavená na strednú úroveň automatického využívania zdrojov. Ak chcete, aby prehľadávanie prebiehalo rýchlejšie, bude trvať kratšie, ale výrazne sa zvýši využitie systémových zdrojov a spomalí sa ostatné činnosti v počítači (táto možnosť sa môže použiť, keď je počítač zapnutý, ale nikto na ňom momentálne nepracuje). Na druhej strane môžete znížiť využitie systémových zdrojov predĺžením doby trvania prehľadávania.

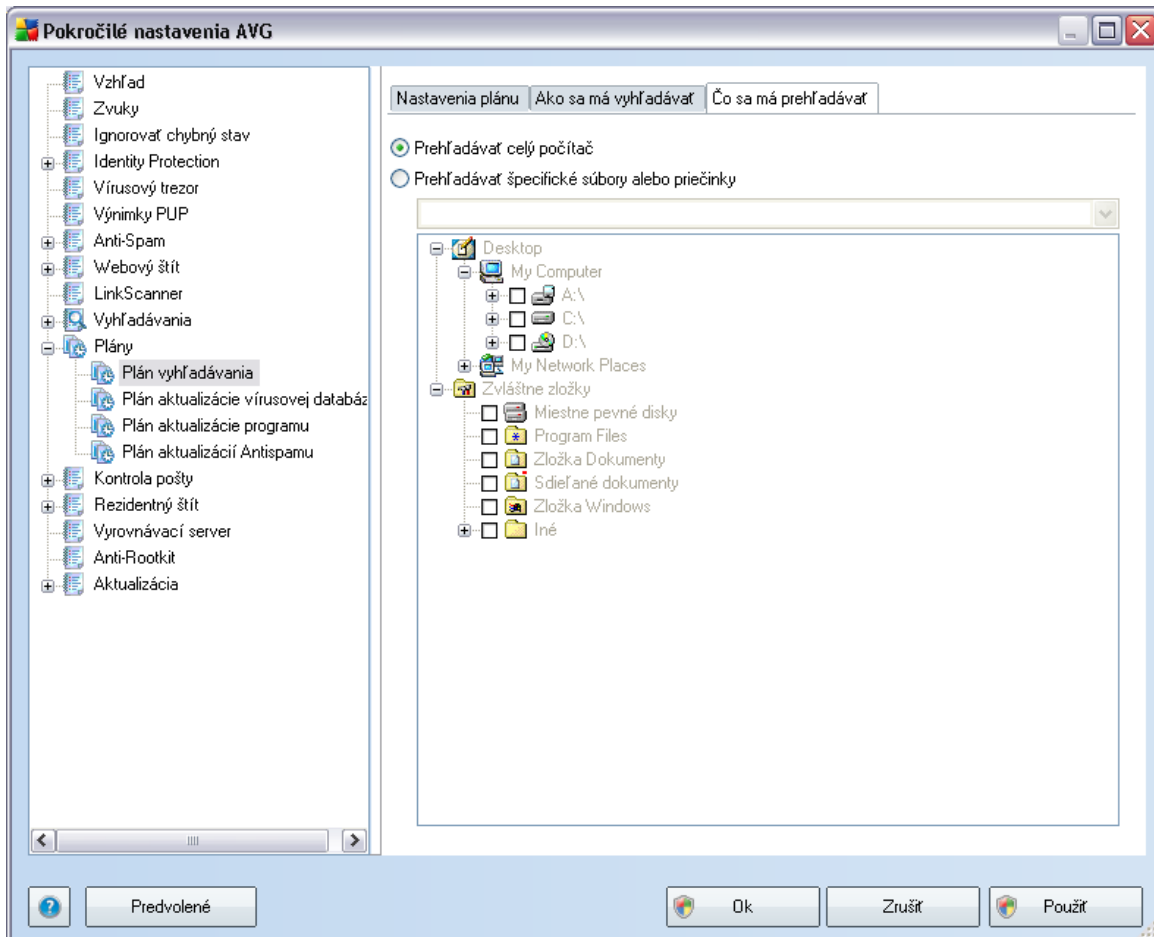
Kliknutím na odkaz **Vytvoriť ďalšie správy o prehľadávaní...** otvorte samostatné dialógové okno s názvom **Správy o prehľadávaní**, v ktorom môžete zaciarknutím konkrétnych položiek definovať, ktoré nálezy sa majú hlásiť:



Kliknutím na možnosť **Ďalšie nastavenia prehľadávania...** otvorte nové dialógové okno **Možnosti vypnutia počítača**, ktoré vám umožní nastaviť, či sa má počítač automaticky vypnúť po skončení procesu prehľadávania. Po potvrdení tejto možnosti (**Vypnúť počítač po dokončení prehľadávania**) sa aktivuje nová možnosť, ktorá umožní vypnúť počítač, aj keď je momentálne zamknutý (**Vynútiť vypnutie počítača**,

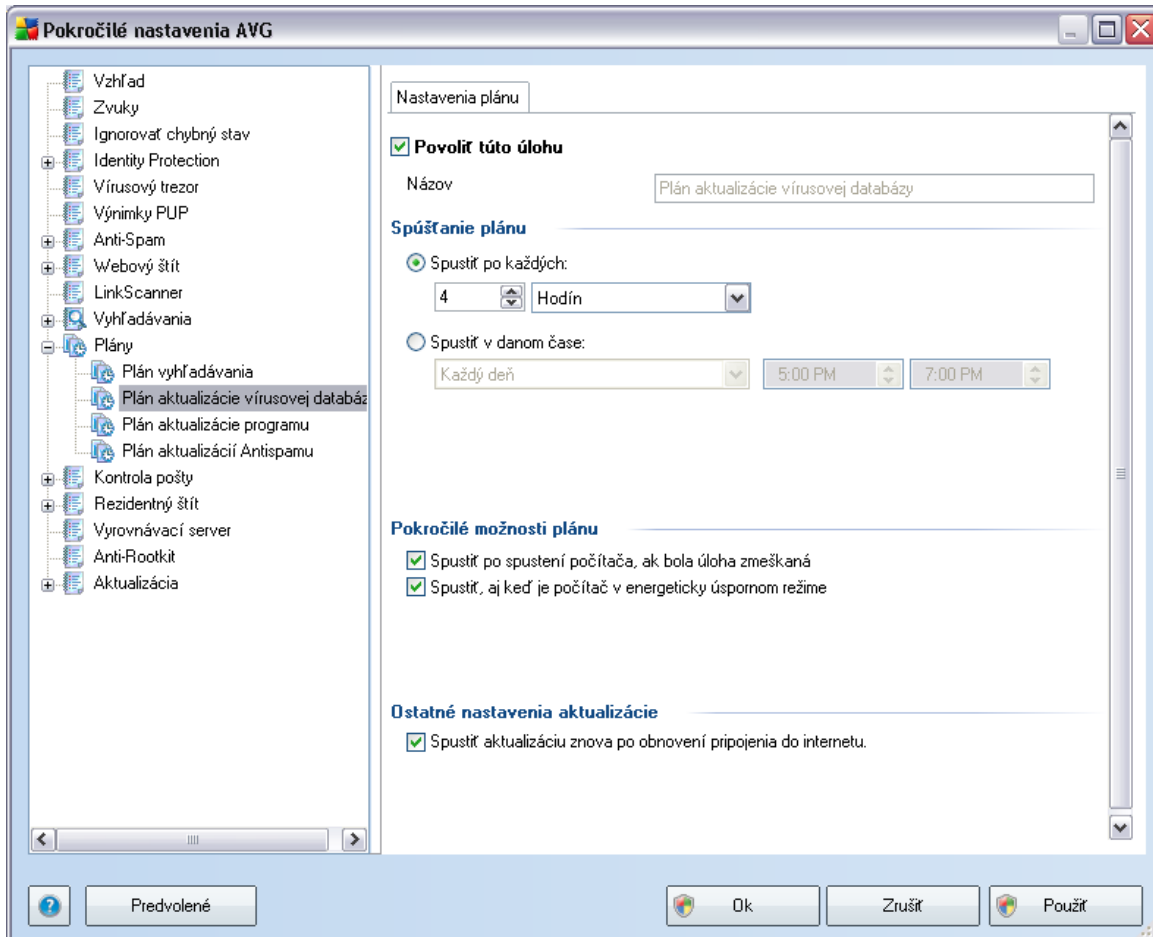
ked je zamknutý).





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.

10.9.2. Plán aktualizácie vírusovej databázy



Na karte **Nastavenia plánu** najskôr oznacenie/zrušením oznacenia položky **Povolit túto úlohu** jednoducho dočasne vypnete naplánovanú aktualizáciu databázy vírusov a znova ju zapnete v prípade potreby. Základný plán aktualizácie databázy vírusov je nastavený v súčasti **Update Manager**. Toto dialógové okno umožňuje nastaviť niektoré podrobné parametre plánu aktualizácie databázy. 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 novo naplánovanej aktualizácie



databázy vírusov. Casovanie sa definuje ako opakované spúšťanie aktualizácie po uplynutí určitého času (**Spustiť po každých...**) alebo nastavením presného dátumu a času (**Spúšťať v konkrétnom case...**).

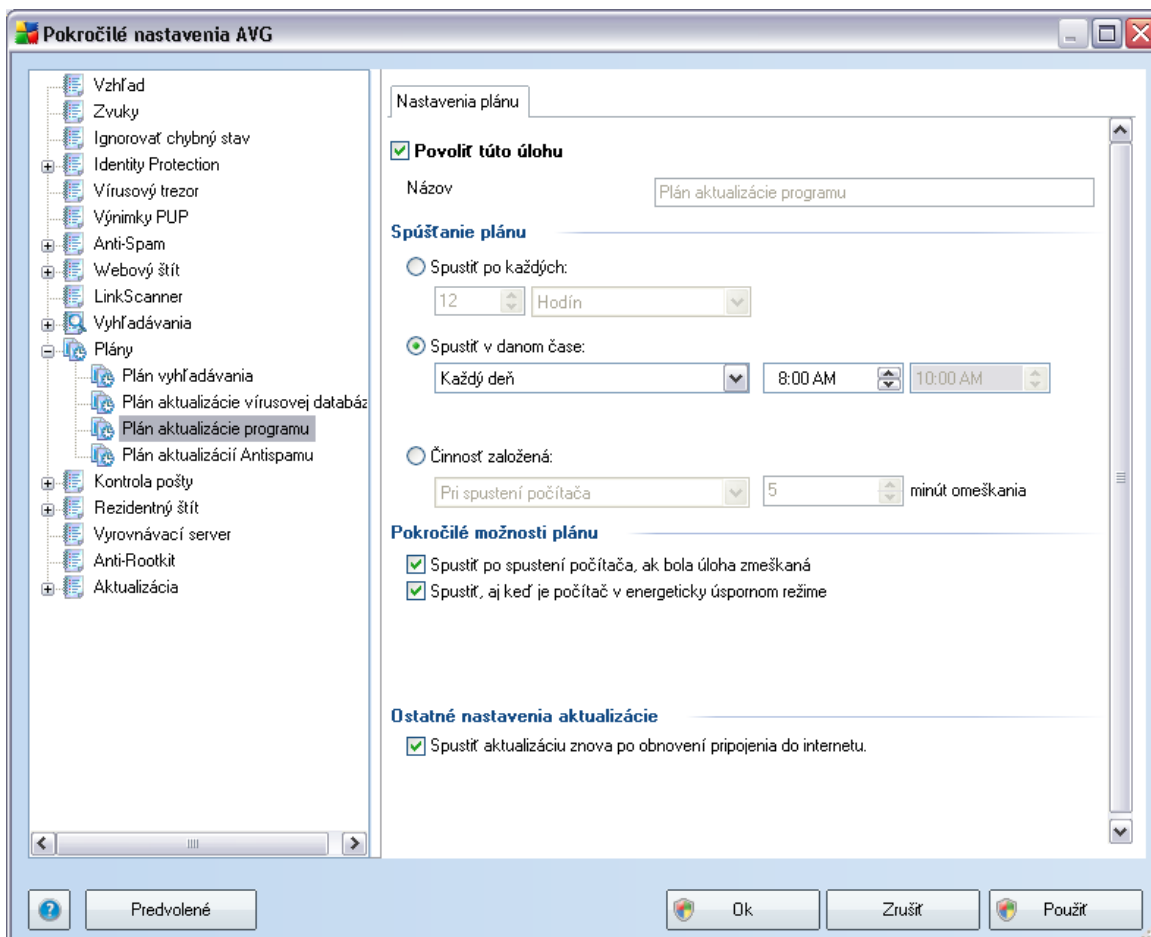
Rozšírené možnosti plánu

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

Dalšie nastavenia aktualizácie

Nakoniec oznacte možnosť **Spustiť aktualizáciu znova hneď po obnovení internetového pripojenia**, ak sa má v prípade výpadku internetového pripojenia obnoviť proces aktualizácie hneď po jeho obnovení.

Po spustení naplánovanej aktualizácie vo vami nastavenom case sa zobrazí informácia o tejto skutočnosti v prekrývacom okne nad [ikonou AVG na paneli úloh](#) (pod podmienkou, že sa nezmenila predvolená konfigurácia v dialógovom okne [Rozšírené nastavenia/Vzhlad](#)).



Na karte **Nastavenia plánu** najskôr oznacením/zrušením oznacenia položky **Povolit túto úlohu** jednoducho dočasne vypnete naplánovanú aktualizáciu programu a znova ju zapnete v prípade potreby. 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. Nacaso vanie sa definuje ako opakované spúšťanie aktualizácie po uplynutí určitého času (**Spustiť po každých...**), definovaním presného dátumu a času (**Spúšťať v konkrétnom case...**), prípadne definovaním udalosti, s ktorou sa bude spájať



spustenie aktualizácie (***Cinnost 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.

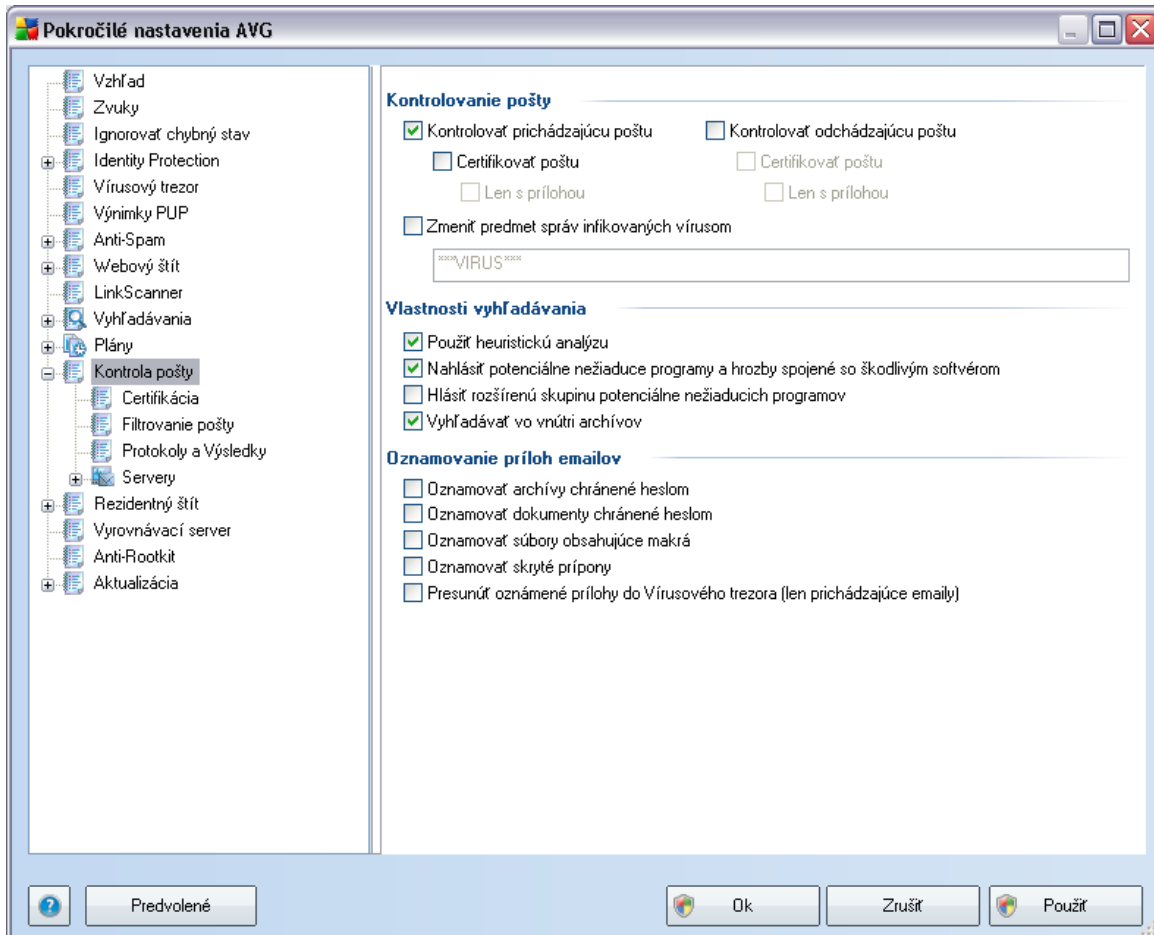
Dalšie nastavenia aktualizácie

Oznacujte možnosť ***Spustiť aktualizáciu znova ihneď po obnovení internetového pripojenia***, ak sa má v prípade výpadku internetového pripojenia obnoviť proces aktualizácie ihneď po jeho obnovení.

Po spustení naplánovanej aktualizácie vo vami nastavenom čase sa zobrazí informácia o tejto skutočnosti v prekrývacom okne nad [ikonou AVG na paneli úloh](#) (pod podmienkou, že sa nezmenila predvolená konfigurácia v dialógovom okne [Rozšírené nastavenia/Vzhlad](#)).

Poznámka: Ak sa čas naplánovanej aktualizácie programu náhodou prekrýva s naplánovaným prehliadaním, proces aktualizácie má vyššiu prioritu a prehliadanie sa preruší.

10.10. Kontrola pošty



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

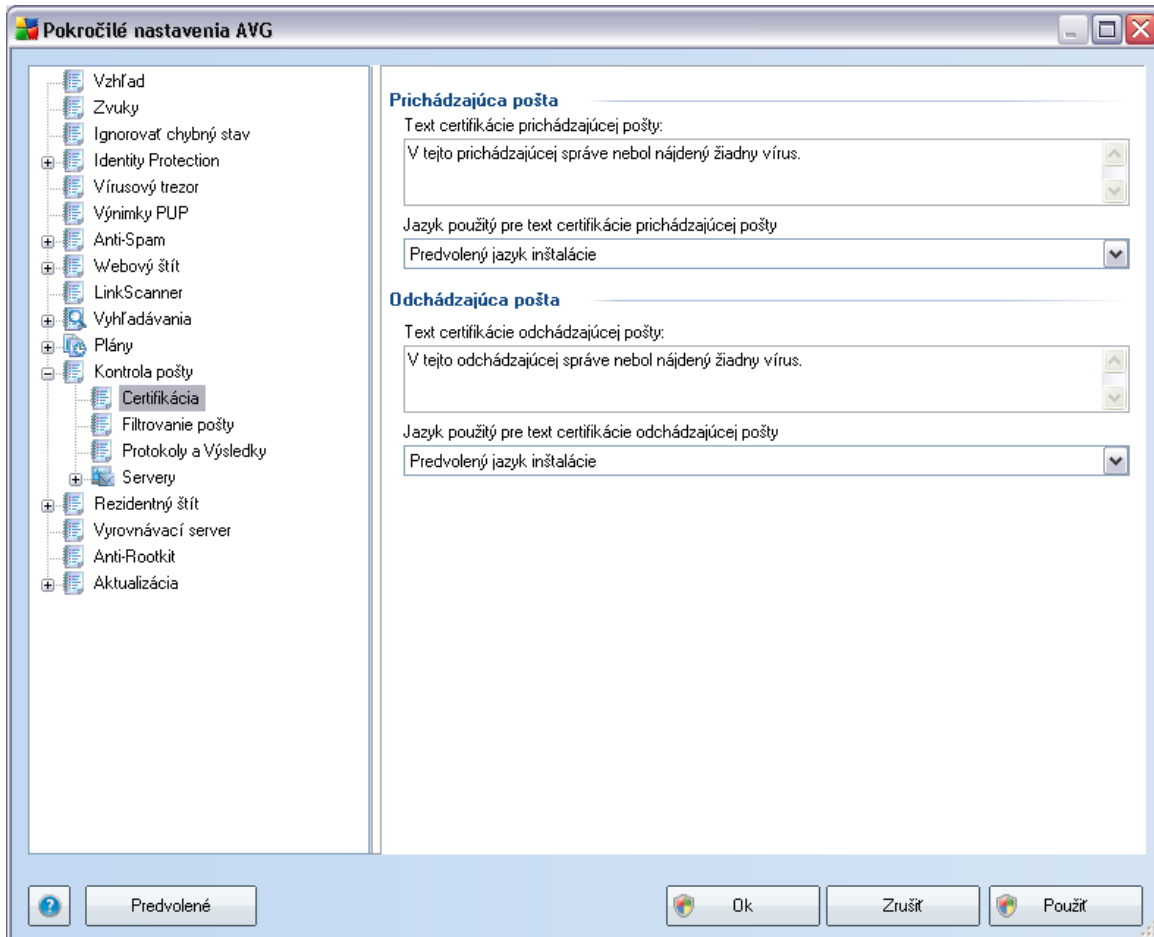
- **Kontrola pošty:** Táto časť umožňuje definovať tieto základné nastavenia pre prichádzajúce a/alebo odchádzajúce e-mailové správy:
 - Ci sa majú v e-mailových správach vyhľadávať vírusy.
 - Ci sa má na koniec každej správy pridať text certifikácie, ktorý informuje, že správa neobsahuje žiadne vírusy. Na prispôsobenie textu použite dialógové okno [Certifikácia](#).
 - Ci sa má text certifikácie pridať len do správ s prílohou.

Ak chcete **zmeniť predmet správ infikovaných vírusom**, zaciarknite toto políčko a do textového pola vložte požadovaný text. Potom sa pridá do pola predmetu každej infikovanej emailovej správy pre jednoduchšiu identifikáciu a filtrovanie. Predvolená hodnota je *****VIRUS*****, ktorú odporúčame ponechať.

- **Vlastnosti prehladávaní:** Táto časť umožňuje nastaviť spôsob, akým sa budú e-mailové správy prehladávať:
 - **Použiť heuristiku:** Oznacíte túto možnosť, ak chcete použiť [metódu heuristického detegovania](#) pri prehladávaní e-mailových správ. Keď je táto možnosť zapnutá, môžete filtrovať prílohy emailov nielen podľa prípony, ale aj podľa skutočného obsahu danej prílohy. Filtrovanie sa dá nastaviť v dialógovom okne [Filtrovanie pošty](#).
 - **Hlásiť potenciálne nežiaduce programy a hrozby spyware:** (štandardne zapnuté): Oznacíte túto možnosť, ak chcete zapnúť súčasť [Anti-Spyware](#) a vyhľadávať spyware a vírusy. [Spyware](#) predstavuje pochybnú kategóriu škodlivého softvéru: Aj keď obvyčajne predstavujú bezpečnostné riziko, niektoré takéto programy môžu byť nainštalované úmyselne. Odporúčame vám nechať túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
 - **Hlásiť rozšírenú skupinu potenciálne nežiaducich programov:** Ak je zapnutá predchádzajúca možnosť, môžete oznáčiť aj toto zaciarkovacie políčko, a tým povoliť detegovanie rozšírenej skupiny [spywaru](#): programov, ktoré sú úplne v poriadku a neškodné, ak sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje zabezpečenie vášho počítača, ale môže blokovat dobré programy, a preto je táto funkcia štandardne vypnutá.
 - **Prehladávať vo vnútri archívov:** Oznacíte túto položku, ak chcete prehladávať obsah archívov priložených k e-mailovým správam.
- **Hlásiť prílohy e-mailov:** Táto časť umožňuje nastaviť ďalšie správy o súboroch, ktoré môžu byť potenciálne nebezpečné alebo podozrivé. Nezobrazí sa žiadne dialógové okno s upozornením, na koniec e-mailovej správy sa len pridá text certifikácie a všetky takéto správy sa uvedú v dialógovom okne [Detegovanie súcastou E-mail Scanner](#):
 - **Hlásiť archívy chránené heslom** - archivacie súbory (ZIP, RAR a pod.), ktoré sú chránené heslom, sa nedajú prehladávať z hľadiska prítomnosti vírusov; zaciarknite toto políčko, ak chcete hlásiť tieto archívy ako potenciálne nebezpečné.

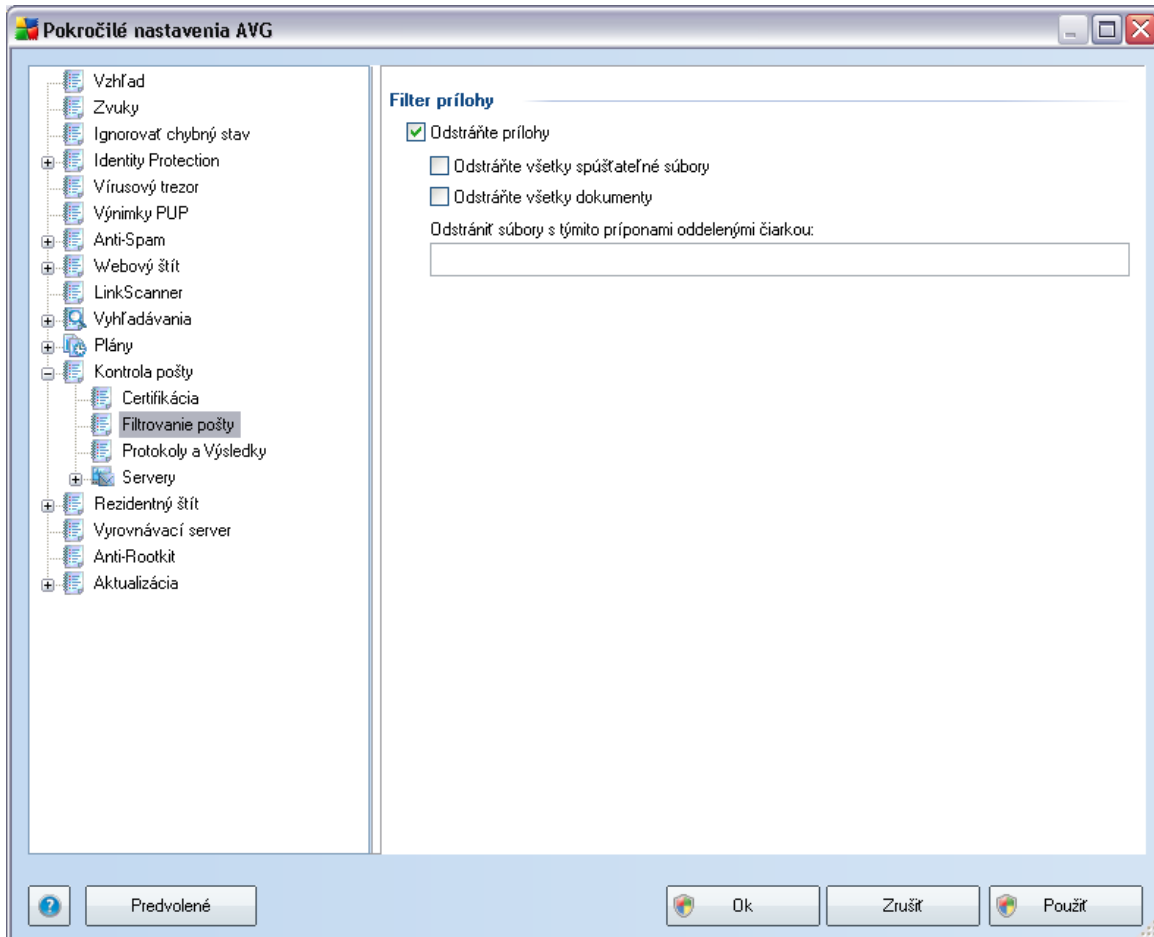
- **Hlásit dokumenty chránené heslom** - dokumenty chránené heslom sa nedajú prehľadávať z hľadiska prítomnosti vírusov; zaciarknite toto políčko, ak chcete hlásiť tieto dokumenty ako potenciálne nebezpečné.
- **Hlásit súbory obsahujúce makrá** - makro je vopred definovaný sled krokov, ktoré zjednodušujú konkrétne úlohy používateľovi (makrá sa bežne používajú v programe MS Word). Makro, ako také, môže obsahovať potenciálne nebezpečné inštrukcie, a preto je vhodné označiť toto políčko, aby sa súbory s makrami hlásili ako podozrivé.
- **Hlásit skryté prípony**: Skrytá prípona môže spôsobiť, že podozrivý spustiteľný súbor „nieco.txt.exe“ sa bude javiť ako neškodný jednoduchý textový súbor „nieco.txt“; zaciarknite toto políčko, ak ich chcete hlásiť 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 detegované ako príloha prehľadávanej e-mailovej správy. Ak sa má táto správa zobrazovať počas prehľadávania, nastavte, či sa má detegovaný infikovaný objekt premiestniť do [Vírusového trezora](#).

10.10.1. Certifikácia



V dialógovom okne **Certifikácia** môžete zadať, aký text by mala certifikácia presne obsahovať a v akom jazyku. Toto by ste mali zadať samostatne pre **Prichádzajúcu poštu** a **Odchádzajúcu poštu**.

10.10.2. Filtrovanie pošty

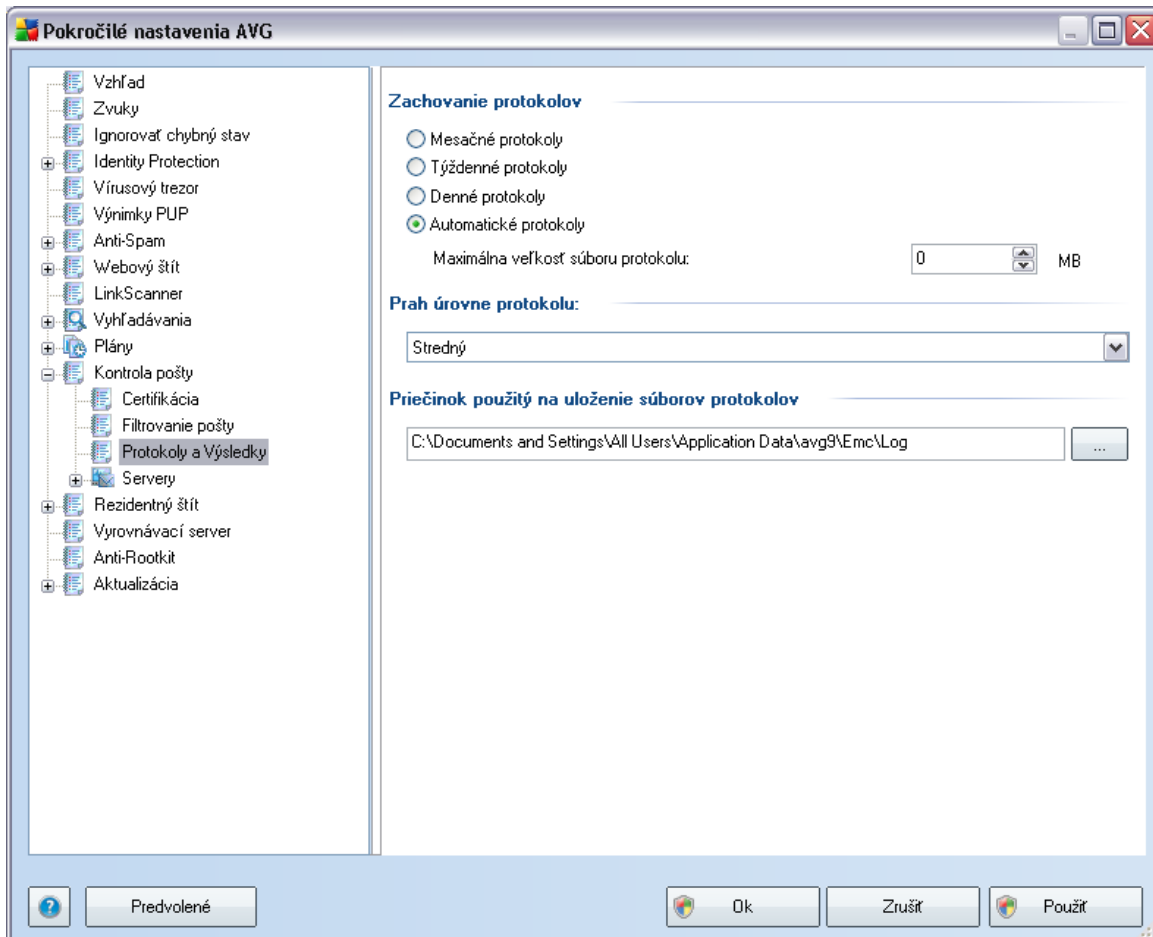


Dialógové okno **Filter príloh** umožňuje nastaviť parametre pre prehľadávanie príloh e-mailových správ. Štandardne je možnosť **Odstrániť prílohy** vypnutá. Ak sa rozhodnete ju aktivovať, všetky prílohy emailových správ detekované ako infekcie alebo potenciálne nebezpečné programy sa automaticky odstránia. Ak chcete zdefinovať špecifické typy príloh, ktoré sa majú odstrániť, zvolte 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.

10.10.3. Protokoly a Výsledky



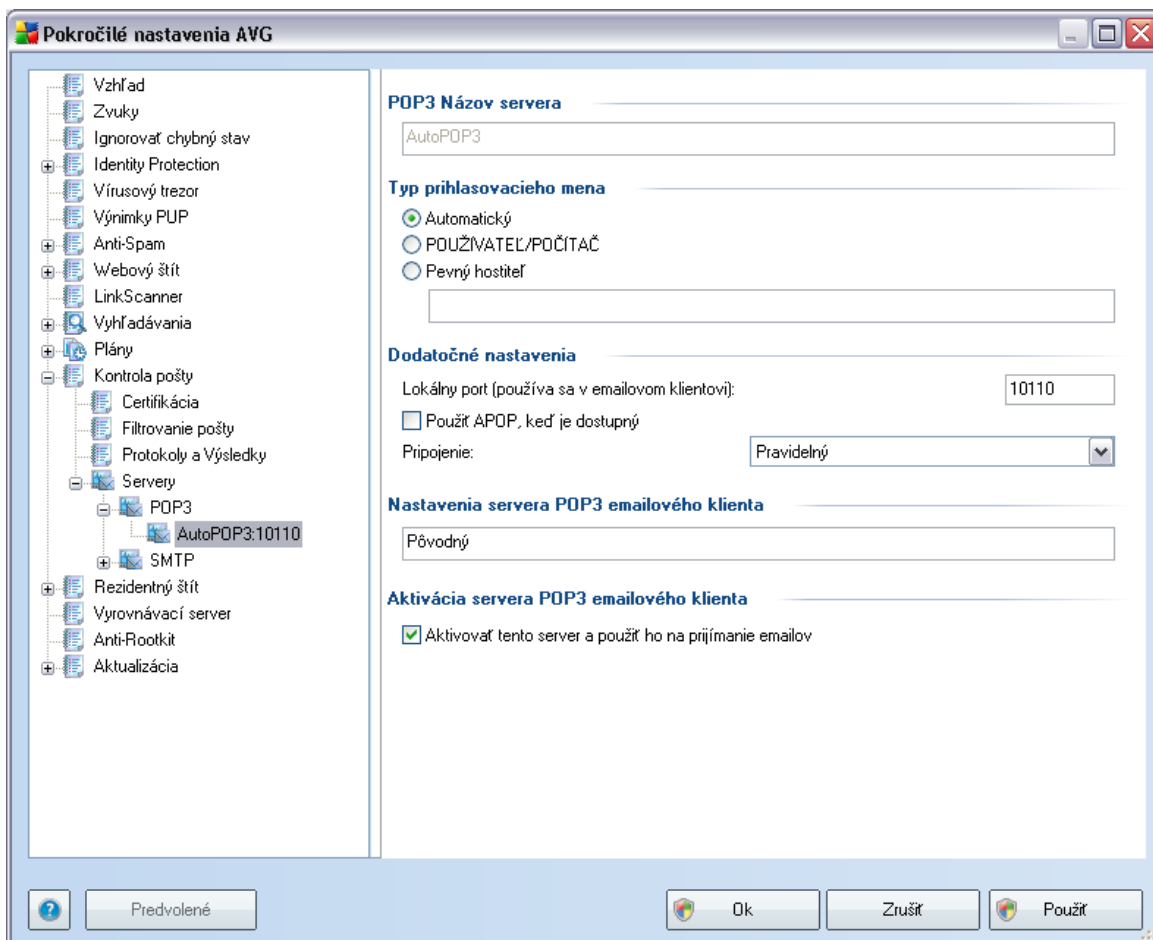
Dialógové okno otvorené cez navigačnú položku **Protokoly a výsledky** vám umožňuje zadať parametre pre zachovanie výsledkov vyhľadávania. Toto dialógové okno je rozdelené na niekoľko častí:

- **Zachovanie protokolov** - uveďte, či chcete dostávať informácie o protokoloch kontroly pošty denne, týždenne, mesačne, ... a zároveň zadajte maximálnu veľkosť súboru protokolu (v MB)
- **Prah úrovne protokolu** - stredná úroveň je nastavená štandardne - môžete si zvoliť nižšiu úroveň (*protokolovanie základných informácií o pripojení*) alebo vyššiu úroveň (*protokolovanie všetkých prenosov*)

- **Priecinok používaný na ukladanie súborov protokolu** - uvedte, kde sa má súbor protokolu uložiť

10.10.4. Servery

V časti **Servery** môžete zmeniť parametre pre servery komponentu **Kontrola pošty**, alebo nastaviť nový server stlačením tlačidla **Pridať nový server**.



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

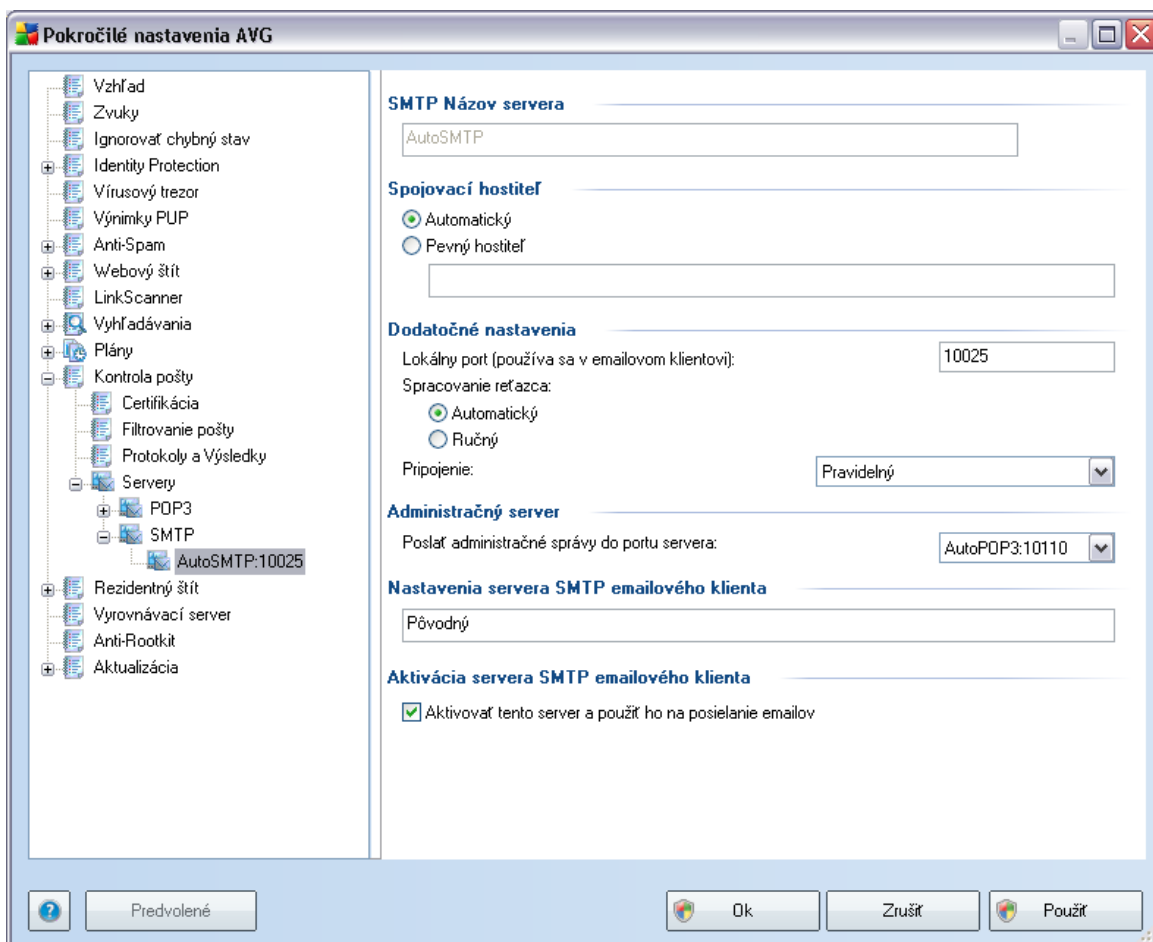
- **Názov servera POP3:** Zadajte názov servera alebo ponechajte predvolený

názov AutoPOP3

- **Typ prihlasovacieho mena:** Stanovuje metódu urcenia poštového servera pre prichádzajúcu poštu:
 - **Automaticky:** Prihlásenie sa uskutoční automaticky podľa nastavení poštovej aplikácie.
 - **POUŽÍVATEL/POCÍTAC:** Najjednoduchší a najcastejšie používaný spôsob stanovenia cieľového poštového servera je metóda proxy. Ak chcete použiť túto metódu, zadajte názov alebo adresu (alebo aj port) ako súčasť prihlasovacieho mena používateľa pre daný emailový server a oddelte ich znakom /. Napríklad pri účte user1 na serveri pop.acme.com a porte 8200 by ste zadali user1/pop.acme.com:8200 pre prihlasovacie meno.
 - **Pevný hosť:** V tomto prípade program vždy použije server, ktorý je tu uvedený. Zadajte adresu alebo názov svojho emailového servera. Prihlasovacie meno zostane nezmenené. Pre meno môžete použiť názov domény (napríklad pop.acme.com), ako aj IP adresu (napríklad 123.45.67.89). Ak emailový server používa neštandardný port, môžete zadať tento port za názvom servera použitím dvojbodky ako vymedzovaca (napríklad pop.acme.com:8200). Štandardný port pre komunikáciu POP3 je 110.
- **Dalšie nastavenia:** Používa sa na definovanie podrobnejších parametrov:
 - **Lokálny port:** Definuje port, na ktorom sa očakáva komunikácia z vašej poštovej aplikácie. Potom musíte vo svojej poštovej aplikácii nastaviť tento port ako port pre komunikáciu POP3.
 - **Použiť APOP, ak je k dispozícii:** Táto možnosť predstavuje vyššiu úroveň zabezpečenia pri pripájaní na poštový server. Tým zabezpečíte, že bude **AVG Osobná kontrola pošty** používať alternatívnu metódu preposielania hesla používateľského účtu pre prihlasovacie meno, pre posielanie hesla na server, ktoré nie je v otvorenom, ale zakódovanom formáte pomocou reťazca premenných prijatého zo servera. Táto funkcia je samozrejme dostupná len vtedy, keď ju podporuje cieľový emailový server.
 - **Pripojenie:** Táto rozbalovacia ponuka sa používa na nastavenie druhu pripojenia, ktoré sa má použiť (bežné/SSL/predvolené SSL). Ak si zvolíte pripojenie SSL, zaslané údaje budú zakódované bez rizika vystopovania alebo monitorovania tretou stranou. Táto funkcia je

dostupná len vtedy, keď ju podporuje cieľový emailový server.

- **Nastavenia servera POP3 v poštovej aplikácii:** Poskytuje stručné informácie o konfiguračných nastaveniach, ktoré sú potrebné na správne nastavenie poštovej aplikácie (aby súčasť **E-mail Scanner** kontrolovala všetky prichádzajúce správy). Toto je prehľad vychádzajúci z príslušných parametrov uvedených v tomto dialógovom okne a ďalších súvisiacich dialógových oknách.
- **Aktivovanie servera POP3 v poštovej aplikácii:** Označením/zrušením označenie tejto položky sa aktivuje resp. deaktivuje uvedený server POP3.



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

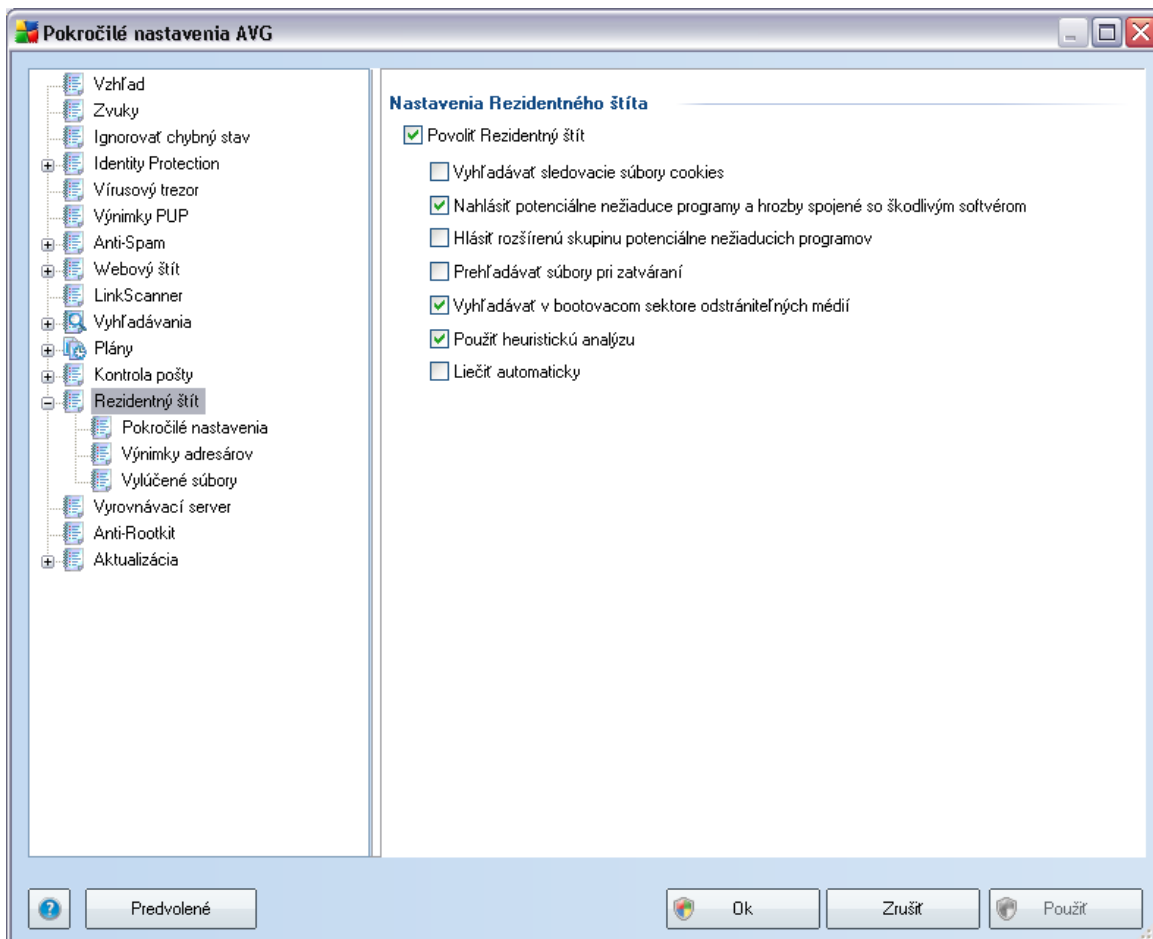
- **Názov servera SMTP** : Zadajte názov servera alebo ponechajte predvolený názov AutoSMTP
- **Spojovací hostiteľ** : Stanovuje metódu určenia poštového servera používaného pre odchádzajúcu poštu:
 - **Automaticky** : Prihlásenie sa uskutoční automaticky podľa nastavení poštovej aplikácie.
 - **Pevný hostiteľ** : V tomto prípade program vždy použije server, ktorý je tu uvedený. Zadajte adresu alebo názov svojho emailového servera. Môžete použiť názov domény (napríklad smtp.acme.com), ako aj IP adresu (napríklad 123.45.67.89) pre daný názov. Ak emailový server používa neštandardný port, môžete zadať tento port za názvom servera použitím dvojbodky ako vymedzovaca (napríklad smtp.acme.com:8200). Štandardný port pre komunikáciu SMTP je 25.
- **Dalšie nastavenia** : Používa sa na definovanie podrobnejších parametrov:
 - **Lokálny port** : Definuje port, na ktorom sa očakáva komunikácia z vašej poštovej aplikácie. Potom musíte vo svojej poštovej aplikácii zadať tento port ako port pre komunikáciu SMTP.
 - **Spracovanie frontu** : Rozhoduje o správaní súčasti **E-mail Scanner** pri spracovaní požiadaviek na poslanie e-mailových správ:
 - Automaticky: Odchádzajúce správy sa okamžite doručia (pošlú) na cieľový poštový server.
 - Rucne: Správa sa vloží do frontu odchádzajúcich správ a pošle sa neskôr.
 - **Pripojenie** : Táto rozbalovacia ponuka sa používa na nastavenie typu pripojenia, ktoré sa má použiť (bežné/SSL/predvolené SSL). Ak si zvolíte pripojenie SSL, zaslané údaje budú zakódované bez rizika vystopovania alebo monitorovania tretou stranou. Táto funkcia je dostupná len vtedy, keď ju podporuje cieľový emailový server.
- **Administratívny server** : Uvádza číslo portu servera, ktorý sa použije na spätné doručenie administratívnych správ. Tieto správy sa vygenerujú napríklad vtedy, keď cieľový poštový server odmietne odchádzajúcu správu, alebo keď nie je dostupný.
- **Nastavenia servera SMTP v poštovej aplikácii** : poskytuje stručné informácie o tom, ako nakonfigurovať poštovú aplikáciu na klientskom počítači

takým spôsobom, aby sa odchádzajúce správy kontrolovali pomocou práve nastaveného servera na kontrolu odchádzajúcej pošty. Tento prehľad vychádza z príslušných parametrov uvedených v tomto dialógovom okne a ďalších súvisiacich dialógových oknách.

- **Aktivovanie servera SMTP v poštovej aplikácii:** Označením/zrušením označenia tohto políčka sa aktivuje resp. deaktivuje uvedený server SMTP.

10.11. Rezidentný štít

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



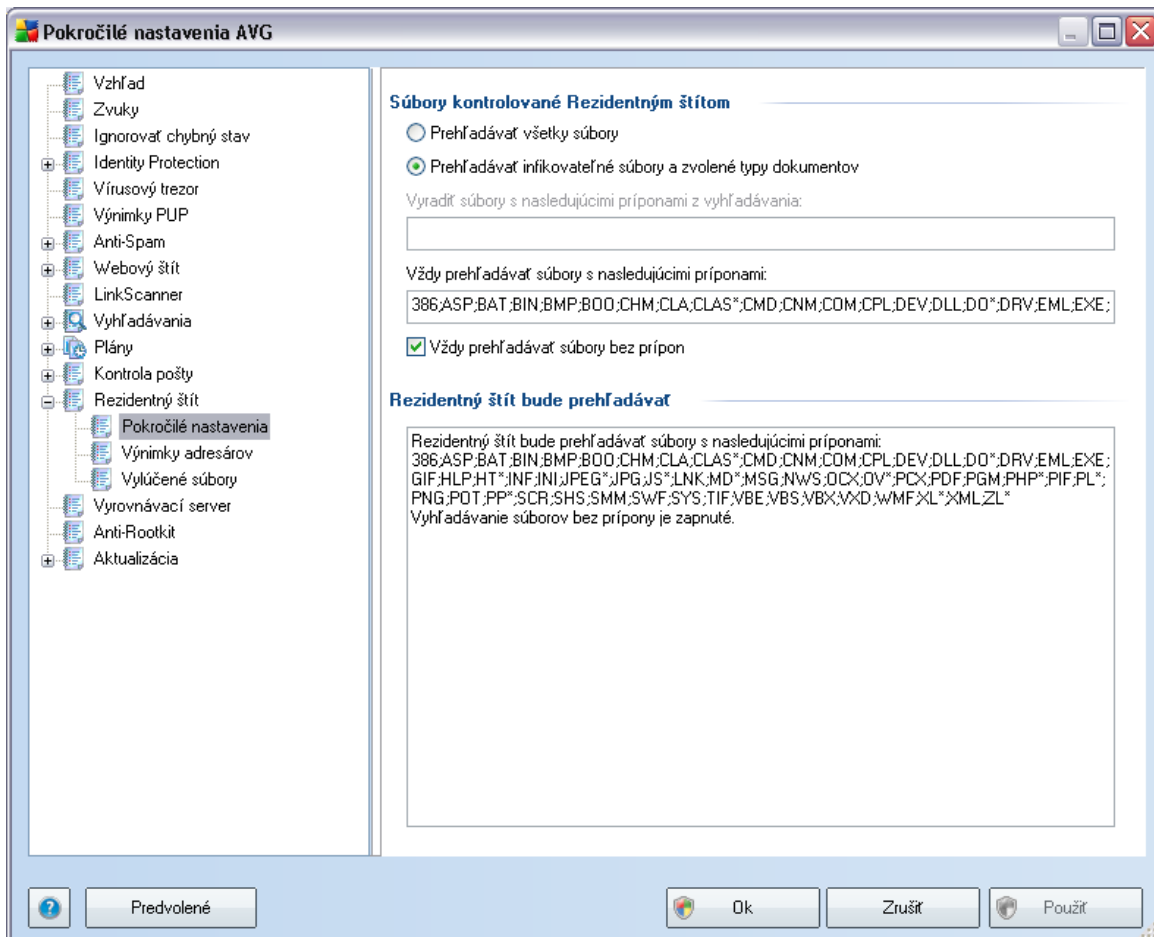
Dialógové okno **Nastavenia súčasti Rezidentný štít** umožňuje kompletne zapnúť alebo vypnúť ochranu zabezpečenú súčasťou **Rezidentný štít** zaciarknutím/

zrušením zaciarknutia položky **Zapnúť Rezidentný štít** (táto funkcia je štandardne zapnutá). Okrem toho môžete zvolit, ktoré funkcie súčasti **Rezidentný štít** sa majú zapnúť:

- **Vyhľadávat sledovacie súbory cookies:** Tento parameter definuje, že počas prehľadávania sa má zisťovať aj prítomnosť súborov cookies. (*HTTP cookies sa používajú na autentifikáciu, sledovanie a uchovanie konkrétnych informácií o používateľoch, ako sú preferencie stránok alebo obsah elektronických nákupných košíkov.*)
- **Hlásit potenciálne nežiaduce programy a hrozby spyware** (štandardne zapnuté): Označte túto možnosť, ak chcete zapnúť súčast **Anti-Spyware** a vyhľadávat spyware a vírusy. **Spyware** predstavuje pochybnú kategóriu škodlivého softvéru: Aj keď obvyčajne predstavujú bezpečnostné riziko, niektoré takéto programy môžu byť nainštalované úmyselne. Odporúčame vám nechať túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
- **Hlásit rozšírenú skupinu potenciálne nežiaducich programov:** Ak je zapnutá predchádzajúca možnosť, môžete označiť aj toto zaciarkovacie políčko, a tým povoliť detegovanie rozšírenej skupiny **spywaru**: programov, ktoré sú úplne v poriadku a neškodné, ak sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje zabezpečenie vášho počítača, ale môže blokovat dobré programy, a preto je táto funkcia štandardne vypnutá.
- **Prehľadávat súbory pri zatvorení:** Prehľadávanie pri zatvorení zabezpečí, že AVG prehľadá aktívne objekty (napr. aplikácie, dokumenty...), keď sa otvárajú alebo zatvárajú; táto funkcia pomáha chrániť počítač pred niektorými typmi sofistikovaných vírusov.
- **Prehľadávat zavádzací sektor vyberateľných médií** (štandardne zapnuté)
- **Použiť heuristiku** (štandardne zapnuté): **Na detegovanie sa použije heuristická analýza** (dynamická emulácia inštrukcií prehľadávaného objektu v prostredí virtuálneho počítača).
- **Liečiť automaticky:** Každá detegovaná infekcia sa automaticky vylieci, ak je k dispozícii liečba.

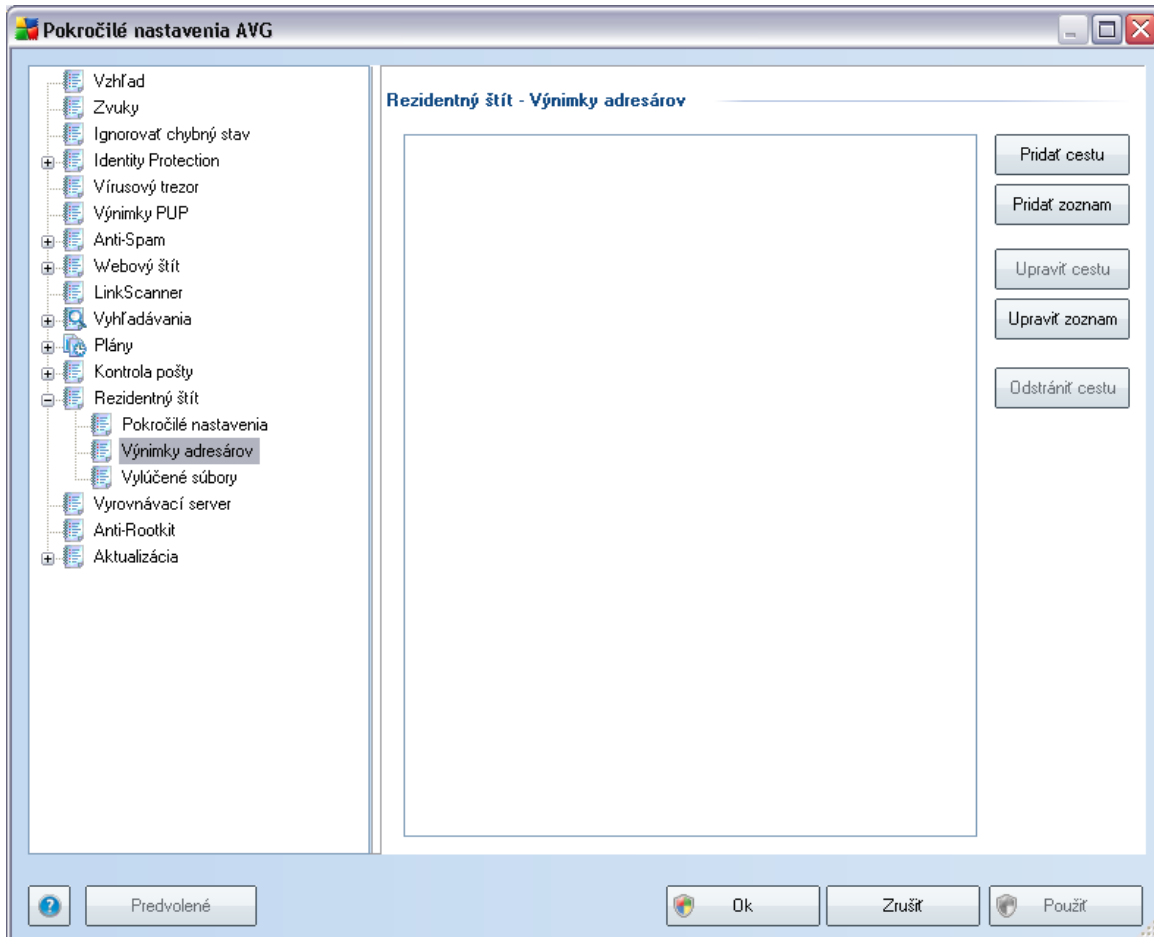
10.11.1. Pokročilé nastavenia

V dialógovom okne **Súbory prehladané Rezidentným štítom** môžete nastaviť, ktoré súbory sa budú prehladávať (podľa špecifických príloh):



Rozhodnite sa, či chcete prehladávať všetky súbory alebo len indikovatelné súbory v tom prípade môžete ďalej zadať zoznam prípon, ktoré definujú súbory, ktoré by sa mali vylúčiť z vyhľadávania a tiež zoznam prípon súborov, ktorý definuje súbory, ktoré sa budú vyhľadávať za každých okolností.

10.11.2. Výnimky adresára



Dialógové okno **Residentný štít - Výnimky adresárov** ponúka možnosť zdefinovať pricinky, ktoré by sa mali vylúčiť z vyhľadávania **Residentného štítu**.

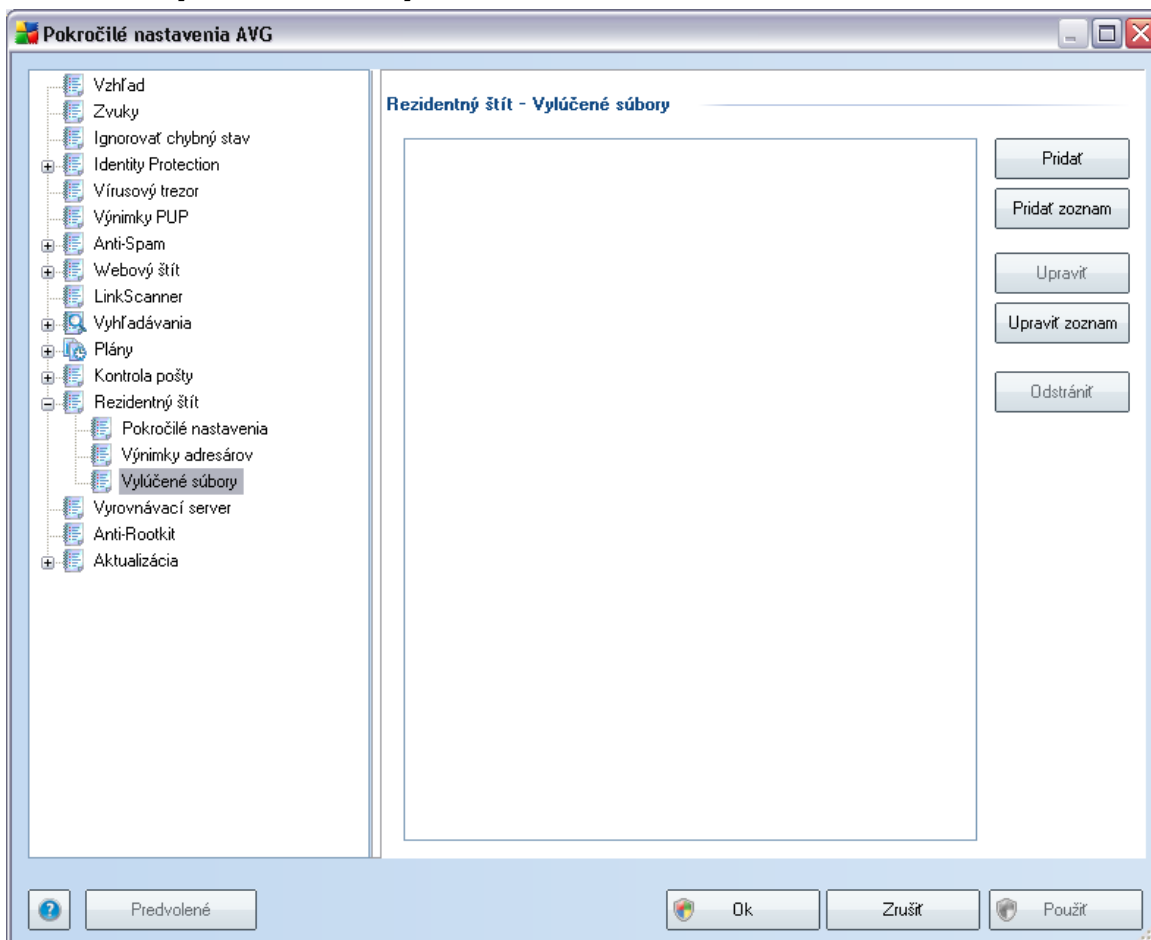
Ak to nie je nutné, odporúčame ponechať všetky adresáre!

V tomto dialógovom okne sa nachádzajú nasledovné ovládacie tlačidlá:

- **Pridať cestu**- zadajte adresáre, ktoré sa majú vylúčiť z prehľadávania ich postupným zvolením v navigacnej schéme lokálneho disku
- **Pridať zoznam**- umožňuje vám zadať celý zoznam adresárov, ktoré sa majú vylúčiť z prehľadávania **Residentným štítom**.

- **Upraviť cestu**- umožňuje vám upraviť zadanú cestu k zvolenému priečinku
- **Upraviť zoznam**- umožňuje vám upraviť zoznam priečinkov
- **Odstrániť cestu**- umožňuje vám vymazať zadanú cestu k zvolenému priečinku zo zoznamu

10.11.3. Vylúčené súbory



Dialógové okno **Rezidentný štít – Vylúčené súbory** sa správa rovnako ako predchádzajúce uvedené okno **Rezidentný štít – Vylúčené adresáre**, ale namiesto priečinkov teraz môžete definovať konkrétne súbory, ktoré sa majú vylúčiť z prehľadávania súčasťou **Rezidentný štít**.

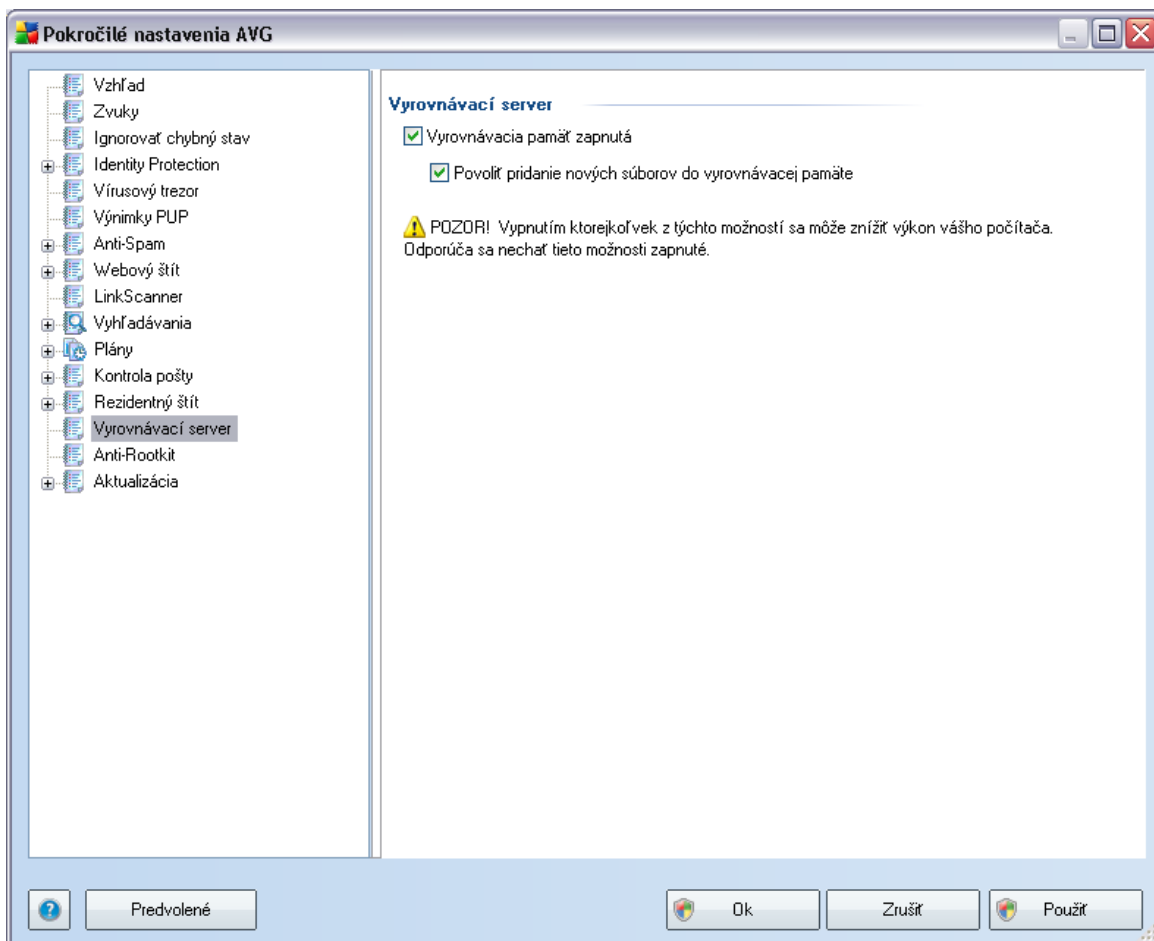
Ak to nie je nevyhnutné, odporúčame nevylúčiť žiadne súbory!

V tomto dialógovom okne sa nachádzajú nasledujúce ovládacie tlačidlá:

- **Pridat:** Definujte súbory, ktoré sa majú vylúčiť z prehľadávania ich postupným zvolením v navigacnej štruktúre lokálneho disku.
- **Pridat zoznam:** Umožňuje zadať celý zoznam súborov, ktoré sa majú vylúčiť z prehľadávania súčasťou [Rezidentný štít](#).
- **Editovat:** Umožňuje zmeniť zadanú cestu k zvolenému súboru.
- **Editovat zoznam:** Umožňuje editovať zoznam súborov.
- **Odstrániť:** Umožňuje vymazať cestu k zvolenému súboru zo zoznamu.

10.12. Vyrovnávací server

Vyrovnávací server je proces, ktorý sa používa na skrátenie doby prehľadávania (*prehľadávania na požiadanie, naplánovaného prehľadávania celého počítača, prehľadávania súčasťou [Rezidentný štít](#)*). Zhromažďuje a uchováva informácie o dôveryhodných súboroch (*systémových súboroch s digitálnym podpisom a pod.*): Tieto súbory sa potom považujú za bezpečné a počas prehľadávania sa vynechajú.

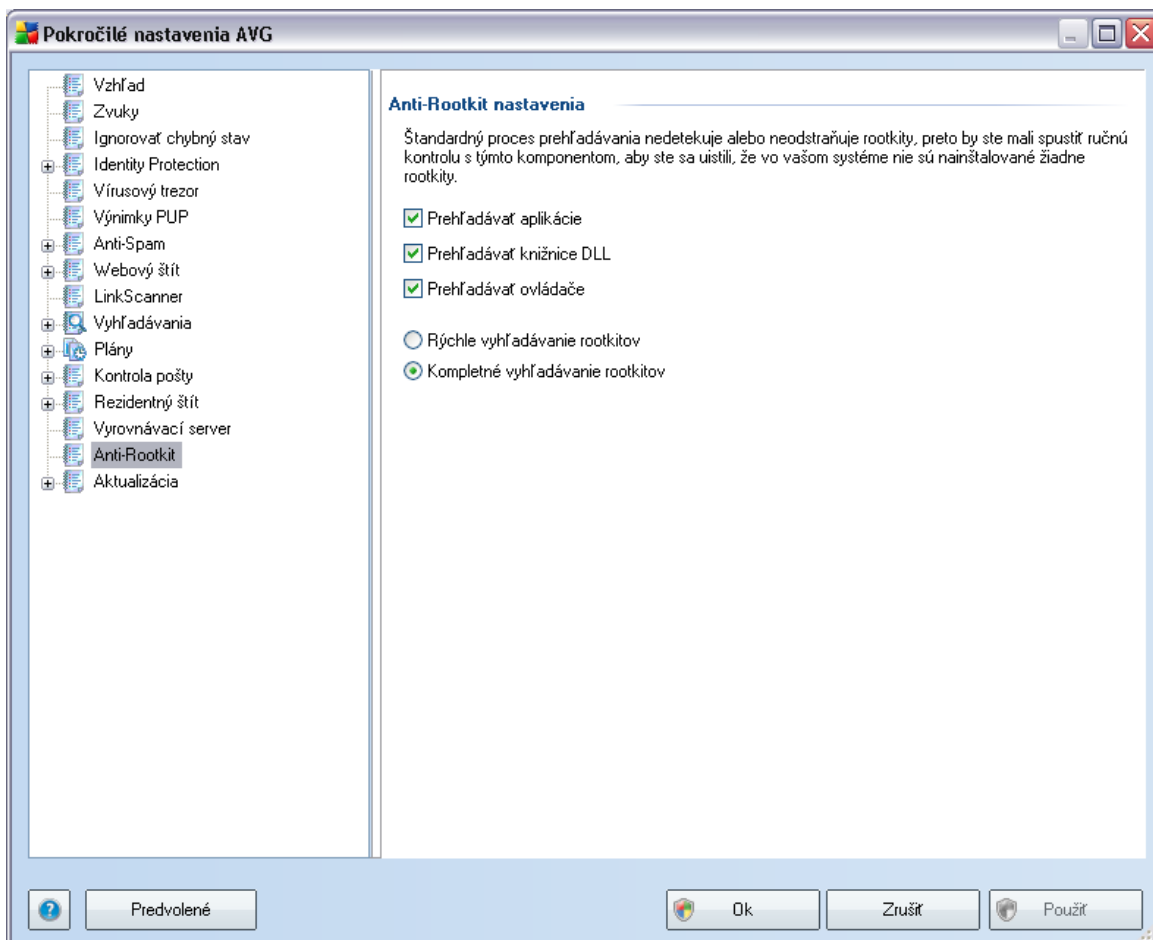


Dialógové okno s nastaveniami ponúka na výber z dvoch možností:

- **Vyrovňavacia pamäť zapnutá** (štandardne zapnuté): Zrušením označenia tohto políčka sa vypne **vyrovňavací server** a vyprázdni sa vyrovnávacia pamäť. Upozorňujeme, že týmto sa môže spomaliť prehľadávanie a znížiť celkový výkon počítača, pretože každý jeden používaný súbor sa najskôr skontroluje z hľadiska prítomnosti vírusov a spywaru.
- **Povolit 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 zachovávajú a budú sa používať do úplného vypnutia funkcie vyrovnávacej pamäte, resp. do ďalšieho aktualizovania vírusovej databázy.

10.13. Anti-Rootkit

Toto dialógové okno sa používa na zmenu konfigurácie súčasti **Anti-Rootkit**:



Editovanie všetkých funkcií súčasti **Anti-Rootkit**, tak ako sú uvedené v tomto dialógovom okne, je možné robiť aj priamo v **rozhraní súčasti Anti-Rootkit**.

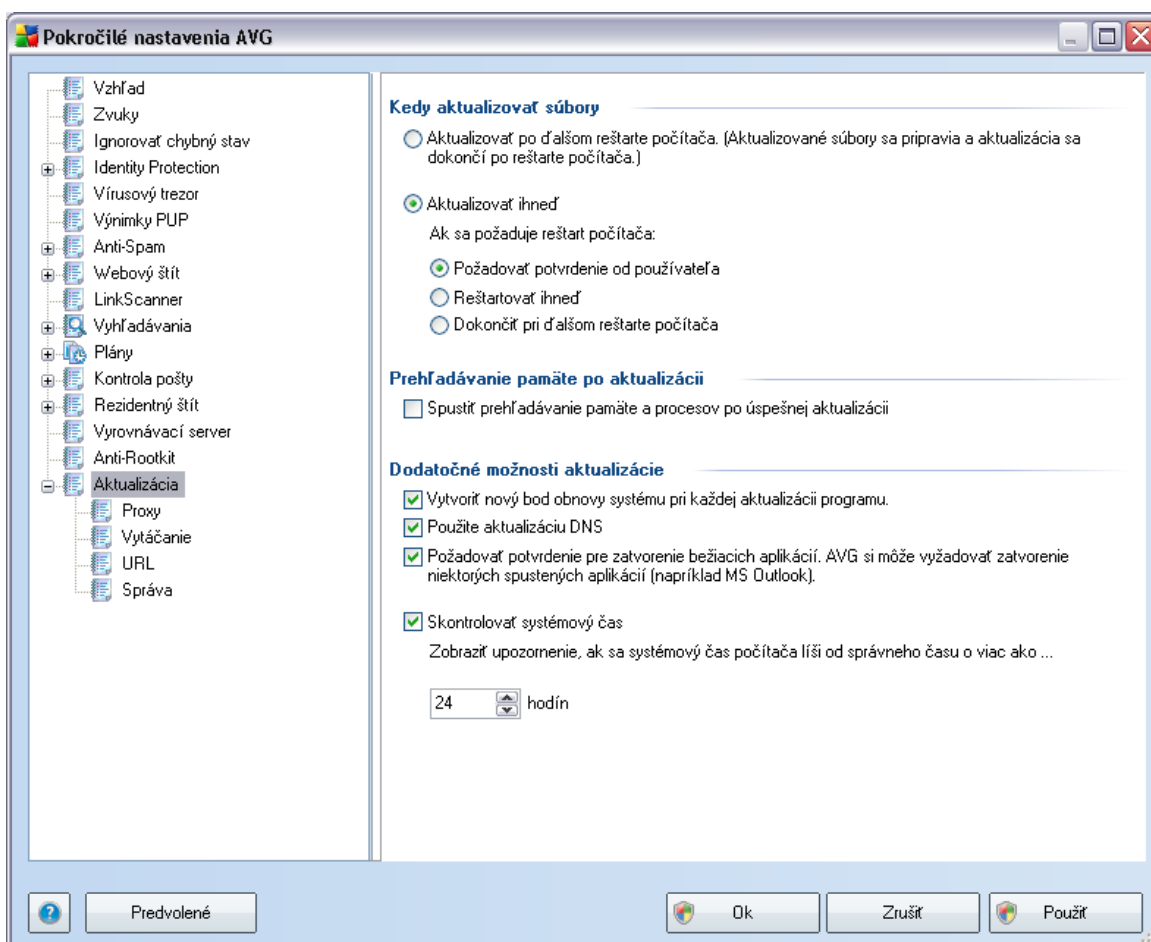
Zaciarknutím príslušných polícok definujete objekty, ktoré sa majú prehľadávať:

- **Prehľadávať aplikácie**
- **Prehľadávať knižnice DLL**
- **Prehľadávať ovládače**

Dalej môžete zvoliť režim vyhľadávania rootkitov:

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

10.14. Aktualizácia



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

Kedy aktualizovať súbory

Táto časť umožňuje zvoliť jednu z dvoch alternatívnych možností: naplánovať [aktualizáciu](#) pri ďalšom reštartovaní počítača, alebo spustiť [aktualizáciu](#) hneď. Štandardne je zvolená možnosť aktualizovať ihneď, pretože takto dokáže AVG zabezpečiť maximálnu úroveň ochrany. Plánovanie aktualizácie pri ďalšom reštarte počítača sa dá odporučiť len vtedy, ak ste si istý, že pravidelne reštartujete počítač, minimálne raz denne.

Ak sa rozhodnete zachovať predvolenú konfiguráciu a spustiť proces aktualizácie hneď, môžete definovať okolnosti, za ktorých sa má prípadné reštartovanie vykonať:

- **Požadovať potvrdenie od používateľa:** Operacný systém vás požiada o udelenie súhlasu s reštartovaním počítača, ktorý je potrebný na dokončenie [procesu aktualizácie](#)
- **Reštartovať hneď:** Počítač sa reštartuje automaticky hneď po dokončení [procesu aktualizácie](#) a nepožiada vás o udelenie súhlasu.
- **Dokončiť pri ďalšom reštartovaní počítača:** Dokončenie [procesu aktualizácie](#) sa odloží až do ďalšieho reštartovania počítača; túto možnosť vám odporúčame použiť len v prípade, ak ste presvedčený, že sa počítač pravidelne reštartuje, najmenej raz za deň.

Prehľadávanie pamäte po aktualizácii

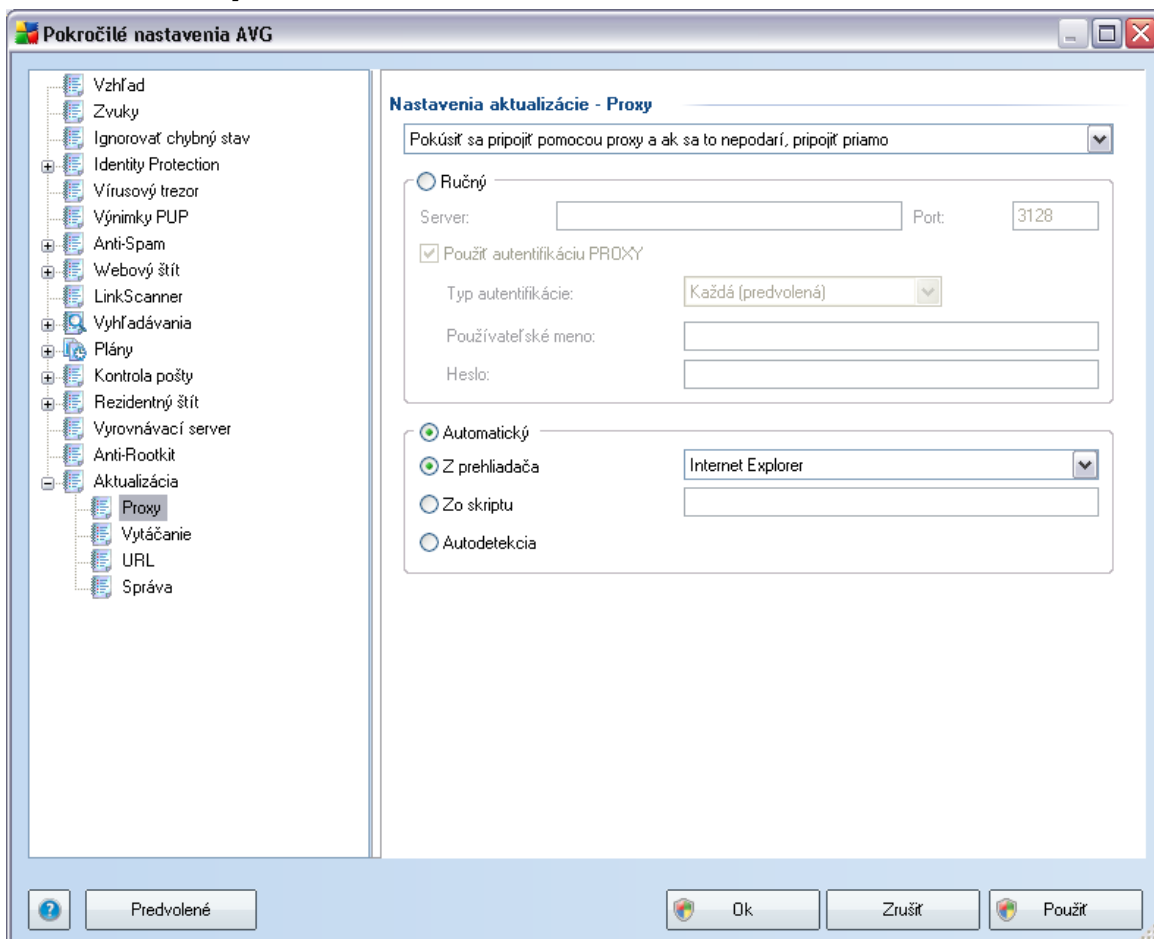
Oznacíte toto zaciarkovacie políčko, ak chcete, aby sa po každom úspešnom aktualizovaní spustilo nové prehľadávanie pamäte. Najnovšia prevzatá aktualizácia môže obsahovať nové definície vírusov, ktoré sa môžu ihneď použiť pri prehľadávaní.

Dalšie možnosti aktualizácie

- **Vytvoriť nový bod obnovenia systému po každej aktualizácii programu:** Pred každým spustením aktualizácie programu AVG sa vytvorí bod obnovenia systému. Ak proces aktualizácie zlyhá a operacný systém spadne, tento bod obnovenia umožní obnoviť stav operacného systému s pôvodnou konfiguráciou. Prístup k tejto možnosti je cez ponuku Štart/Všetky programy/Príslušenstvo/Systémové nástroje/Obnovenie systému. Zmeny týchto nastavení však odporúčame robiť len skúseným používateľom! Nechajte toto zaciarkovacie políčko označené, ak chcete používať túto funkčnosť.

- **Používať aktualizáciu DNS:** Onacte toto zaciarkovacie políčko, ak chcete používať metódu vyhľadania nových súborov aktualizácie, ktorá znižuje objem dát prenášaných medzi aktualizacným serverom a nainštalovaným programom AVG.
- **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 procesu aktualizácie.
- **Skontrolovať systémový čas:** Označte túto možnosť, ak chcete byť informovaný v prípade, ak sa systémový čas líši od skutočného času o viac ako je nastavený počet hodín.

10.14.1. 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 server 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 (zaciarknite 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, zaciarknite možnosť **Použiť autentifikáciu PROXY** na overenie, či sú vaše používateľské meno a heslo platné na vytvorenie pripojenia na internet cez server proxy.

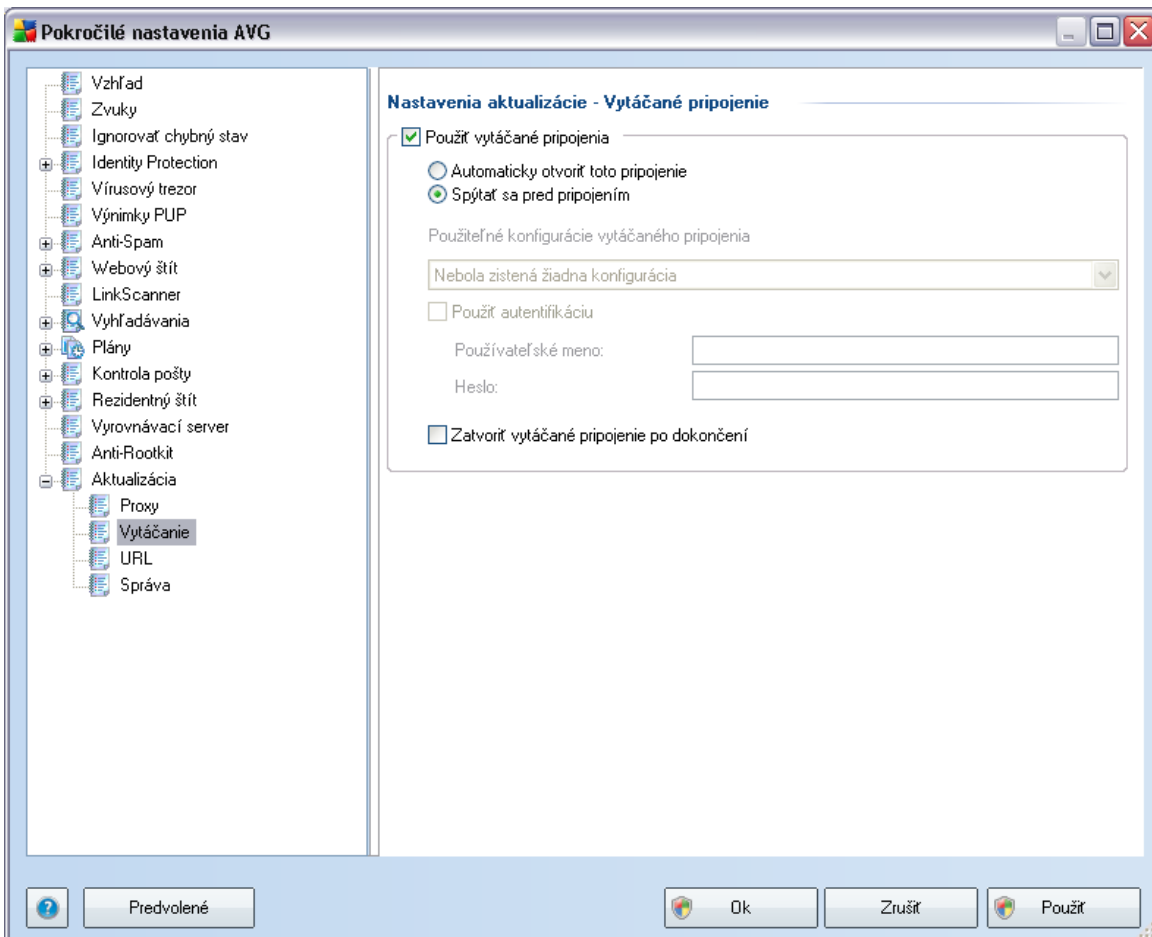
Automatická konfigurácia

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

- **Z prehliadaca:** Konfigurácia sa načíta z predvoleného internetového prehliadaca.
- **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.

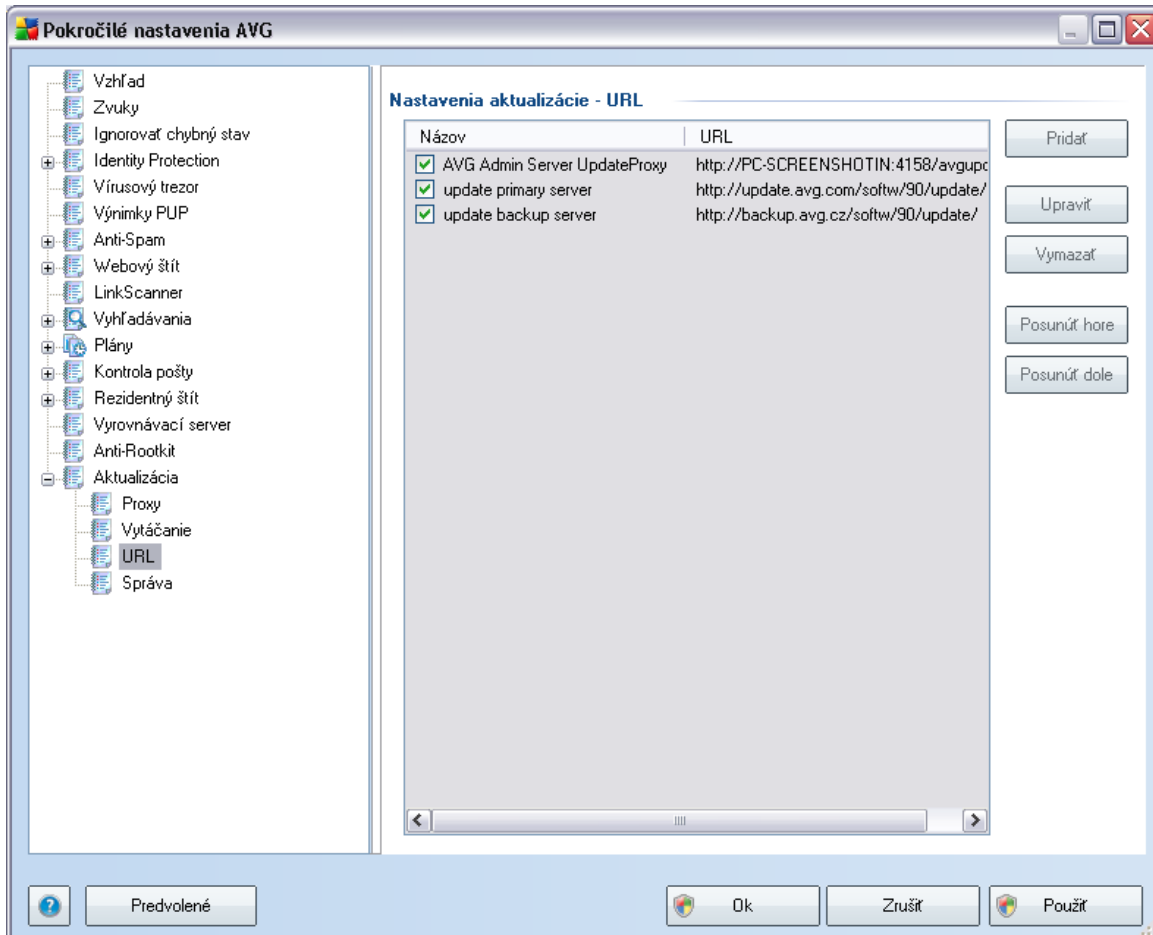
10.14.2. Vytáčanie



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 neoznacíte možnosť **Použiť vytáčané pripojenie**, 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**).

10.14.3. URL



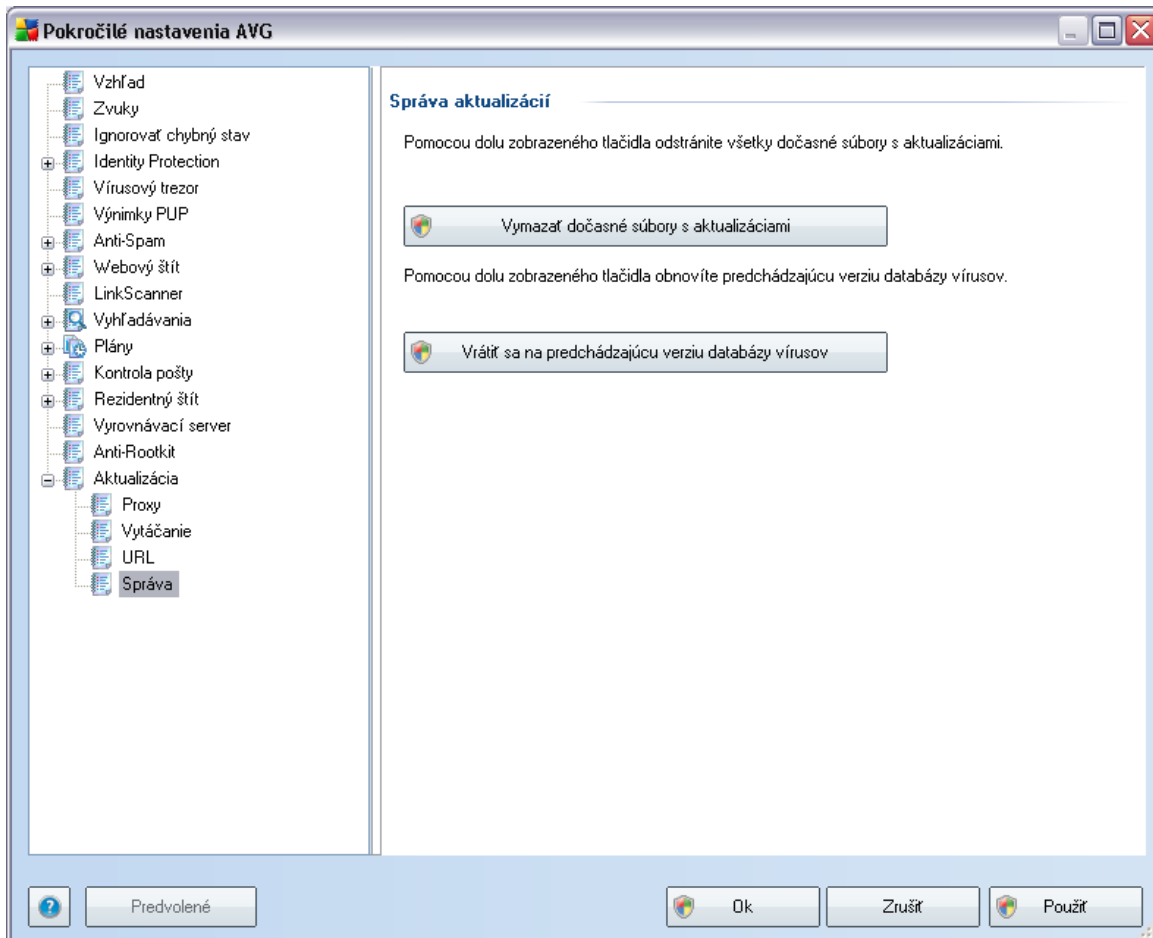
Dialógové okno **URL** uvádza zoznam internetových adries, odkiaľ si môžete prevziať aktualizacné súbory. Zoznam a jeho položky môžete zmeniť pomocou nasledujúcich ovládacích tlačidiel:

- **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

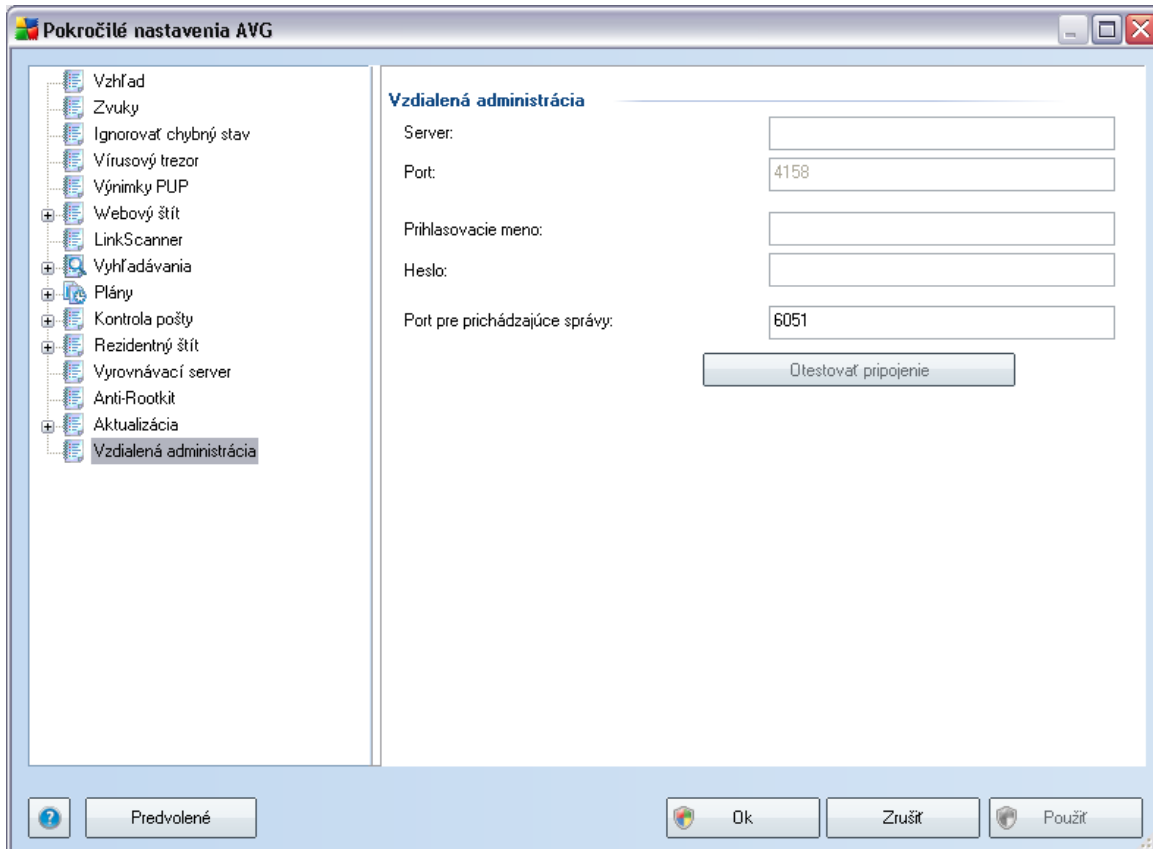
10.14.4. Správa

Dialógové okno **Správa** 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*).

10.15. Vzdialená správa



Nastavenia **Vzdialenej administrácie** sa vzťahujú na pripojenie stanice klienta AVG k systému diaľkovej administrácie. Ak plánujete pripojiť príslušnú stanicu k vzdialenej administrácii, uveďte, prosím, nasledujúce parametre:

- **Server** - názov servera (alebo IP adresa servera), kde je nainštalovaný AVG Admin Server
- **Port** - poskytuje číslo portu, na ktorom klient AVG komunikuje s AVG Admin Server (*port číslo 4158 sa považuje za predvolený - ak používate toto číslo portu, nemusíte ho výslovne uvádzať*)
- **Prihlasovacie meno** - ak je komunikácia medzi klientom AVG a AVG Admin Serverom definovaná ako zabezpečená, uveďte svoje meno používateľa ...
- **Heslo** - ... a svoje heslo



- **Port pre prichádzajúce správy** - číslo portu, na ktorom klient AVG prijíma prichádzajúce správy z AVG Admin Servera

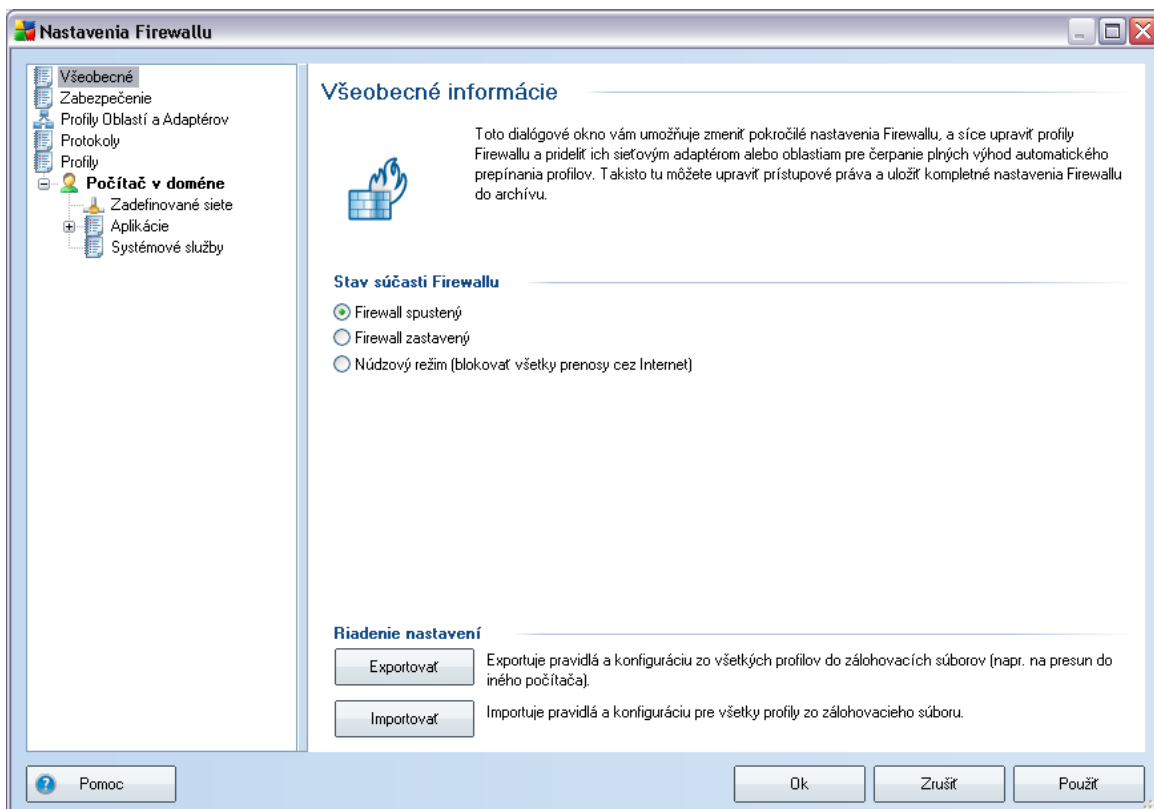
Tlačidlo **Otestovať pripojenie** vám pomáha overiť, či sú všetky vyššie uvedené údaje platné a či sa dajú použiť na úspešné pripojenie k DataCenter.

Poznámka: Podrobný popis vzdialenej administrácie nájdete v dokumentácii k Sietovej edícii AVG.

11. Firewall nastavenia

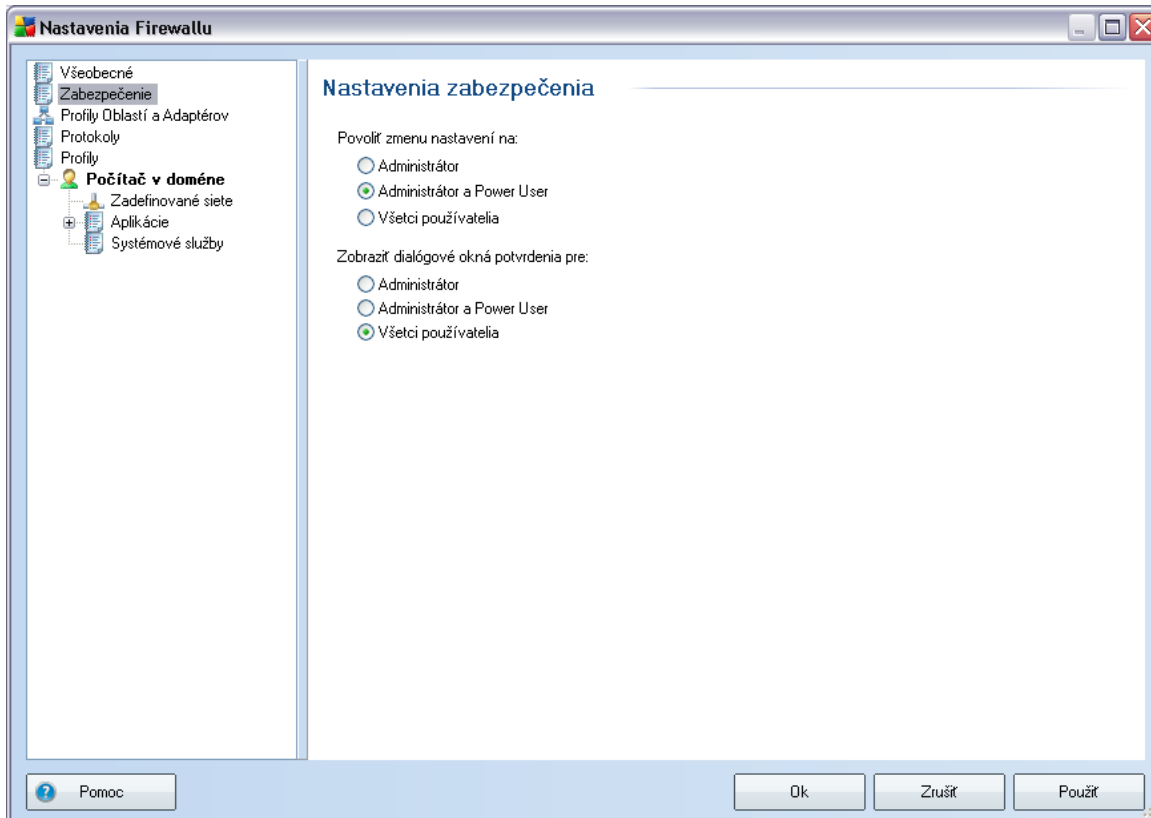
Konfigurácia **Firewallu** sa otvorí v novom okne, kde môžete vo viacerých dialógových oknách nastaviť veľmi pokročilé parametre komponentu. **Zmena rozšírenej konfigurácie je však určená len pre odborníkov a skúsených používateľov.**

11.1. Všeobecné



Ponuka **Všeobecné informácie** umožňuje **exportovať/importovať** konfiguráciu súčasti **Firewall**, t. j. exportovať definované pravidlá a nastavenia súčasti **Firewall** do zálohovacích súborov, alebo importovať celý zálohovací súbor.

11.2. Zabezpečenie



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

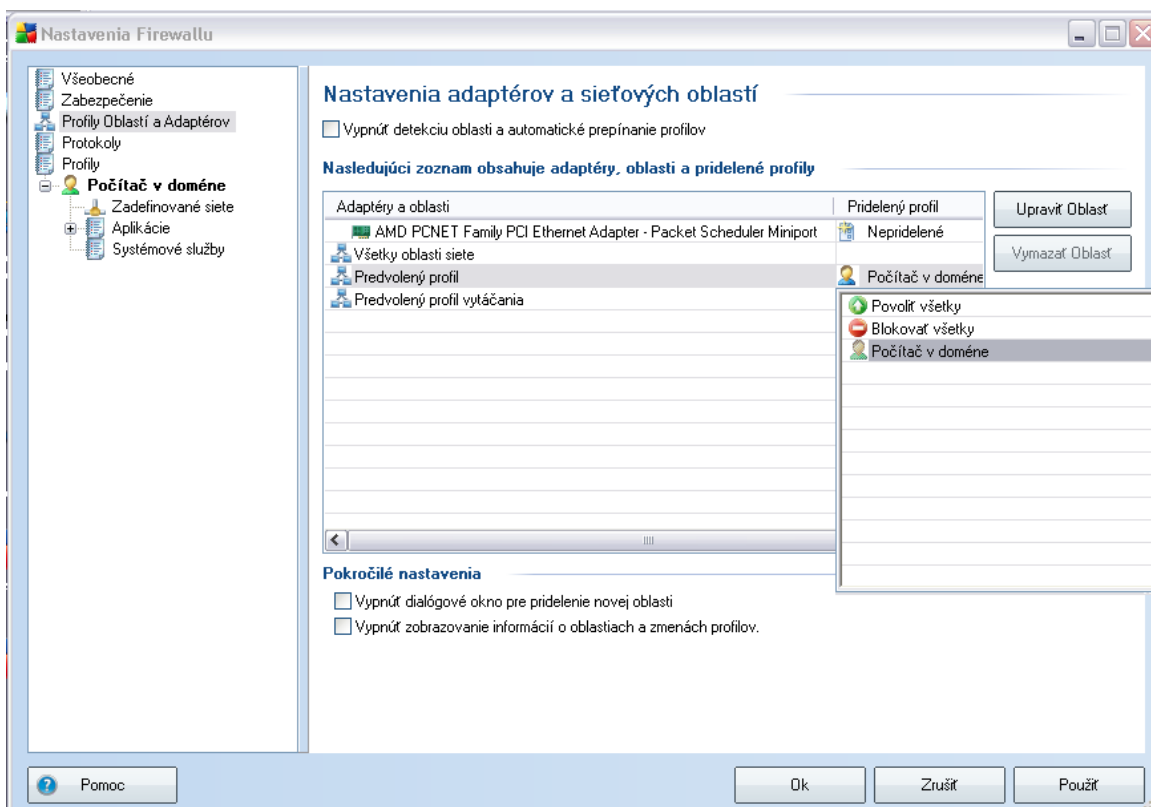
- **Povoliť zmenu nastavení komu** - zadajte, kto má právo meniť konfiguráciu **Firewallu**
- **Zobraziť dialógové okno potvrdenia pre** - zadajte, komu by sa mali zobrazovať dialógové okná potvrdenia (*dialógové okná, ktoré si vyžadujú rozhodnutie v situácii, ktorá nie je pokrytá zadaným pravidlom **Firewallu***)

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

- **Administrátor** - kompletne riadi počítač a má právo zaradovať používateľov do skupín so špecificky zadanými oprávneniami

- o **Administrátor a Power User** - administrátor môže zaradiť používateľa do danej skupiny (*Power User*) a zdefinovať oprávnenia členov skupiny
- o **Všetci používatelia** - ostatní používatelia, ktorí nie sú zaradení do žiadnej skupiny

11.3. Profily Oblasťí a Adaptérov



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

- **Vypnúť detegovanie oblastí a automatické prepínanie profilov** – Každému typu sieťového rozhrania, resp. každej oblasti môžete pridelit jeden z definovaných profilov. Ak nechcete definovať konkrétne profily, použijte sa jeden spoločný profil definovaný na základe [používania počítača](#) a [sieťového pripojenia počítača](#) zvoleného počas [procesu inštalácie](#). Ak sa však rozhodnete rozlišovať profily a pridelit ich konkrétnym adaptérom a oblastiam a

názov používateľa, PID, smer prenosu, typ protokolu, čísla vzdialených a miestnych portov a pod.) na dvoch kartách:

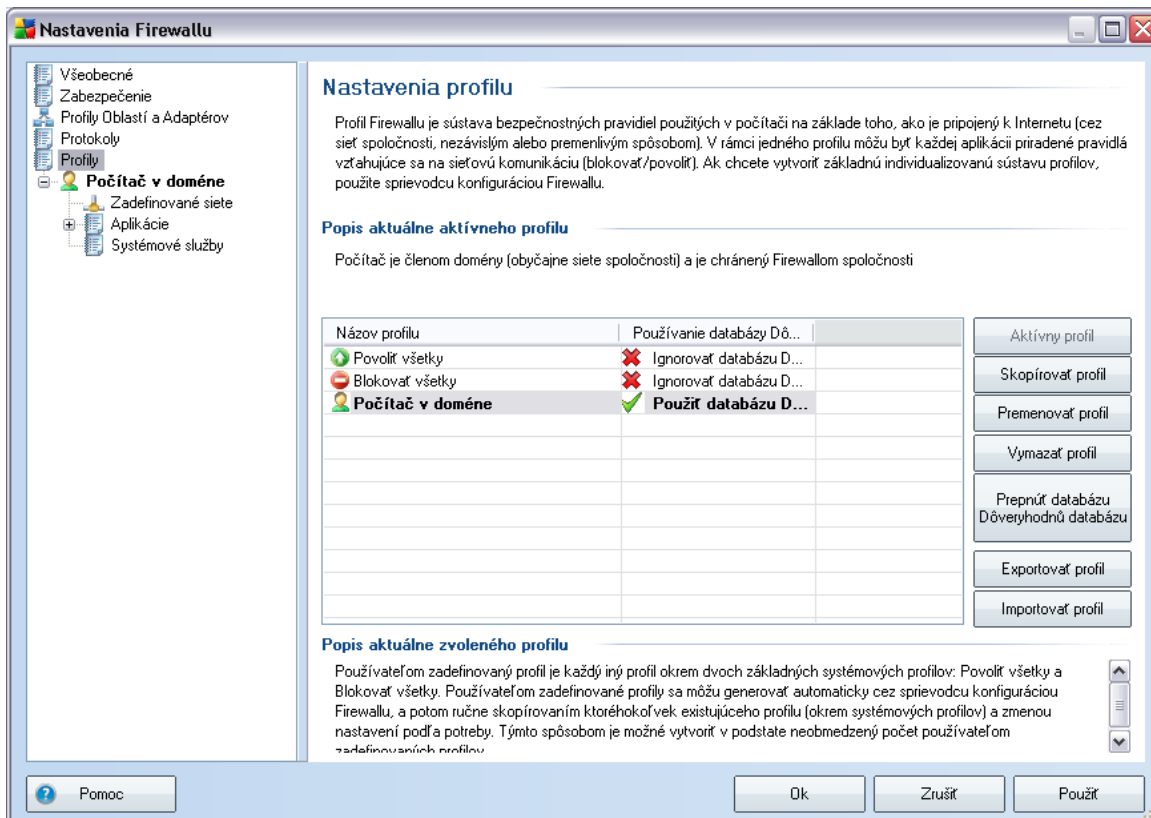
- **Záznamové protokoly o prenose:** Zobrazí informácie o činnosti všetkých aplikácií, ktoré sa pokúsili pripojiť na sieť.
- **Záznamové protokoly dôveryhodnej databázy:** Dôveryhodná databáza je interná databáza spoločnosti AVG zhromažďujúca informácie o certifikovaných a dôveryhodných aplikáciách, ktorým môže byť vždy povolené komunikovať online. Pri prvom pokuse novej aplikácie o pripojenie do siete (t. j. ak doposiaľ nebolo vytvorené pravidlo pre bezpečnostnú bránu firewall súvisiace s touto aplikáciou), je potrebné zistiť, či sa má povoliť sieťová komunikácia príslušnej aplikácie. AVG najskôr nahliadne do dôveryhodnej databázy a ak je v nej aplikácia uvedená, automaticky sa jej povolí prístup do siete. Až potom, a pod podmienkou, že v databáze sa nenachádzajú informácie o tejto aplikácii, sa zobrazí dialógové okno, v ktorom sa vás program opýta, či chcete povoliť aplikácii prístup do siete.

Ovládacie tlačidlá

- **Pomocník:** Otvorí súbory pomocníka pre toto dialógové okno.
- **Obnoviť zoznam:** Všetky zaznamenané parametre sa dajú usporiadať podľa zvoleného atribútu: chronologicky (*dátumy*) alebo abecedne (*ostatné stĺpce*) – stačí kliknúť na hlavičku príslušného stĺpca. Použite tlačidlo **Obnoviť zoznam** na aktualizovanie práve zobrazených informácií.
- **Vyprázdniť zoznam:** Vymaže všetky položky v tabuľke.

11.5. Profily

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



Všetky ostatné [profily](#) sa potom dajú upraviť priamo v tomto dialógovom okne pomocou nasledujúcich ovládacích tlačidiel:

- **Aktivovať profil** - toto tlačidlo nastavuje zvolený profil ako aktívny, čo znamená, že konfiguráciu zvoleného profilu použije **Firewall** na ovládanie prenosov v sieti
- **Skopírovať profil** - vytvorí identickú kópiu zvoleného profilu; neskôr môžete upraviť a premenovať kópiu pre vytvorenie nového profilu na základe zvoleného pôvodného profilu
- **Premenovať profil** - umožnuje vám zadanovať nový názov pre zvolený profil

- **Vymazať profil** - vymaže zvolený profil zo zoznamu
- **Prepnúť na dôveryhodnú databázu** - môžete rozhodnúť, že pre zvolený profil sa použijú informácie z *dôveryhodnej databázy* (*dôveryhodná databáza je interná databáza spoločnosti AVG zhromažďujúca informácie o dôveryhodných a certifikovaných aplikáciách, ktorým môže byť vždy povolené komunikovať online.*)
- **Exportovať profil** - zaznamená konfiguráciu zvoleného profilu do súboru, ktorý sa uloží pre možné budúce použitie
- **Importovať profil** - konfiguruje nastavenia zvoleného profilu na základe údajov exportovaných zo zálohovacieho súboru konfigurácie
- **Pomoc** - otvorí súbor pomoci dialógového okna.

V spodnej časti tohto dialógového okna nájdete popis profilu, ktorý je momentálne zvolený vo vyššie uvedenom zozname.

Na základe počtu zadaných profilov, ktoré sú uvedené v zozname v dialógovom okne **Profil** sa zmení lavá štruktúra navigačnej ponuky. Každý zadaný profil vytvorí špecifickú vetvu pod položkou **Profil**. Špecifické profily sa potom dajú upraviť v nasledujúcich dialógových oknách (*ktoré sú rovnaké pre všetky profily*):

11.5.1. 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):
Oznacíte túto možnosť, ak chcete používať *dôveryhodnú databázu* (t. j. *internú databázu spoločnosti AVG zhromažďujúcu informácie o dôveryhodných a certifikovaných aplikáciách komunikujúcich online*. Ak pre konkrétnu aplikáciu nebolo doposiaľ definované pravidlo, je potrebné zistiť, či sa aplikácii môže povoliť prístup do siete. AVG najskôr nahliadne do dôveryhodnej databázy a ak je v nej aplikácia uvedená, bude sa považovať za bezpečnú a umožní sa jej komunikovať v sieti. V opačnom prípade sa vás program opýta, či chcete aplikácii povoliť komunikáciu v sieti.) pre príslušný profil.
- **Povoliť mostové prepojenie virtuálnych počítačov** (štandardne vypnuté):
Oznacením tejto možnosti sa povolí virtuálnym počítačom vo VMware vytvoriť

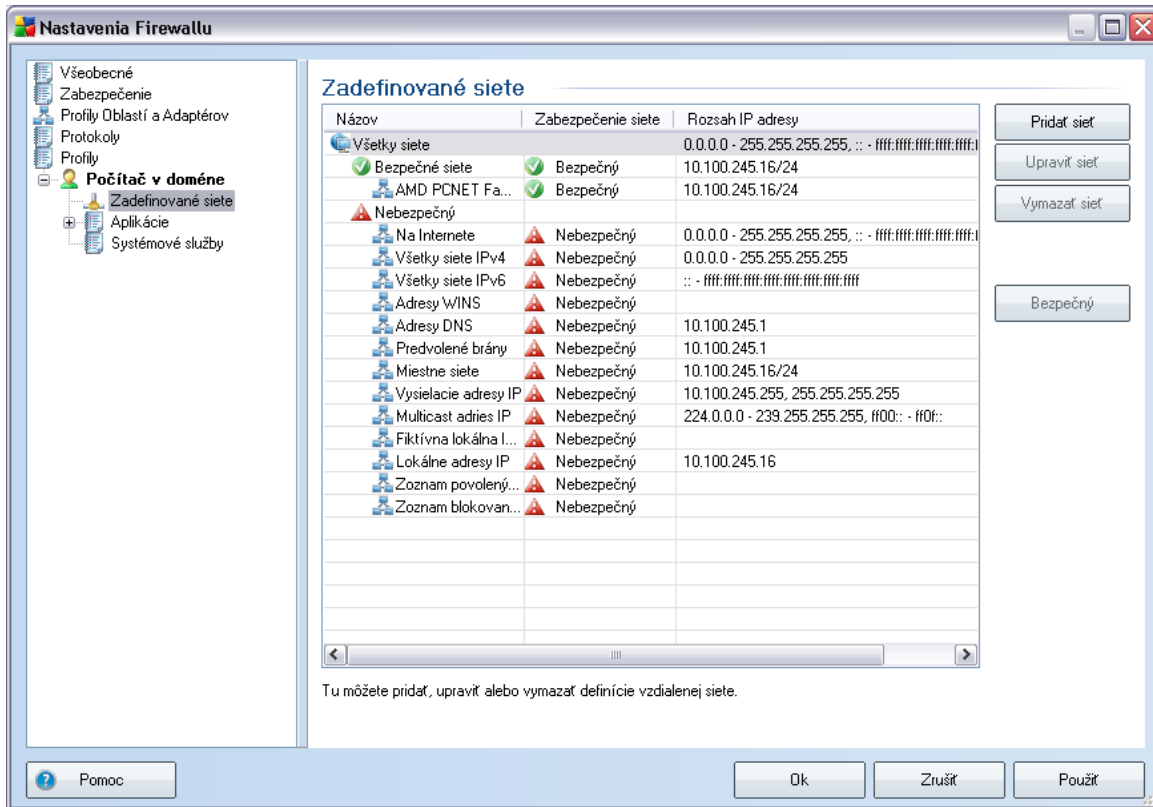
priame pripojenie na siet.

Nastavenia režimu hrania

Cast **Nastavenie režimu hrania** vám umožní nastaviť a potvrdiť, zaciarknutím príslušnej položky, podľa toho, či sa majú zobrazovať informácie správy súčasti **Firewall** aj vtedy, keď je na počítači spustená aplikácia na celú obrazovku (*obvyčajne ide o hry, ale vzťahuje sa to na všetky aplikácie spustené na celú obrazovku, napr. prezentácie vo formáte PPT*), keďže informácie hlásenia môžu byť do istej miery rušivé.

Ak označíte položku **Vypnúť oznámenia súčasti Firewall počas hrania hry**, v rozbalovacej ponuke potom nastavíte, ktorá činnosť sa má vykonať v prípade, ak 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.

11.5.2. Zadefinované siete

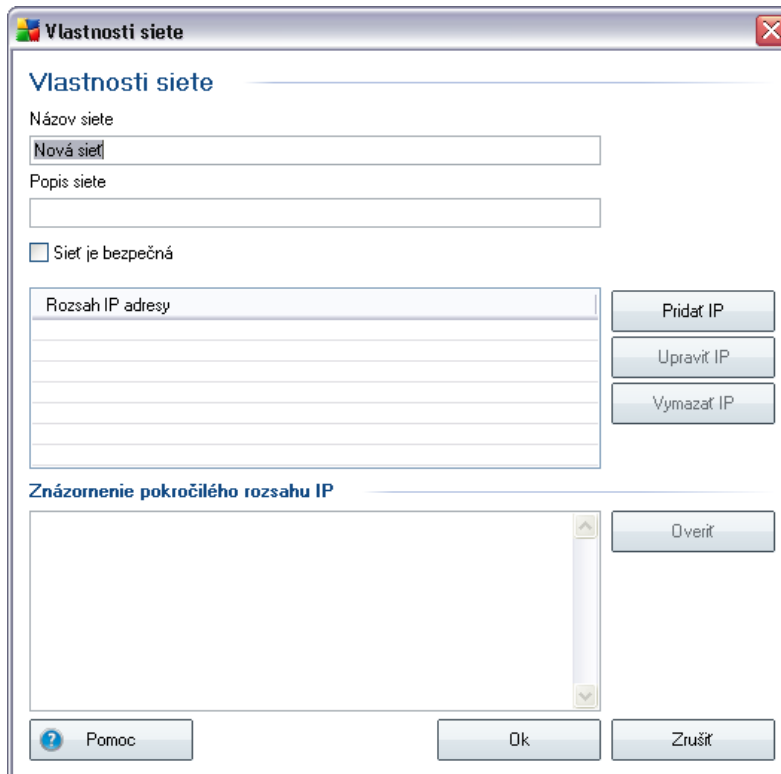


V dialógovom okne **Definované siete** sa nachádza zoznam všetkých sietí, do ktorých je váš počítač pripojený. Pre každú detegovanú sieť sa zobrazia nasledujúce informácie:

- **Siete:** Zoznam názvov všetkých sietí, do ktorých je počítač pripojený.
- **Zabezpečenie siete:** Štandardne sa všetky siete považujú za nezabezpečené a len ak ste presvedčení, že je príslušná sieť bezpečná, povolte ju (*kliknite na položku v zozname, ktorá odkazuje na príslušnú sieť a zvolte možnosť Zabezpečená v kontextovej ponuke*), aby sa pridala do zoznamu sietí, v ktorých aplikácia môže komunikovať, a ktoré majú nastavené aplikačné pravidlo Povolit pre bezpečné siete
- **Rozsah adres IP:** Každá sieť sa automaticky deteguje a definuje ako rozsah adres IP.

Ovládacie tlačidlá

- **Pridat sieť:** Otvorí dialógové okno **Vlastnosti siete**, kde môžete zmeniť parametre novo definovanej siete:

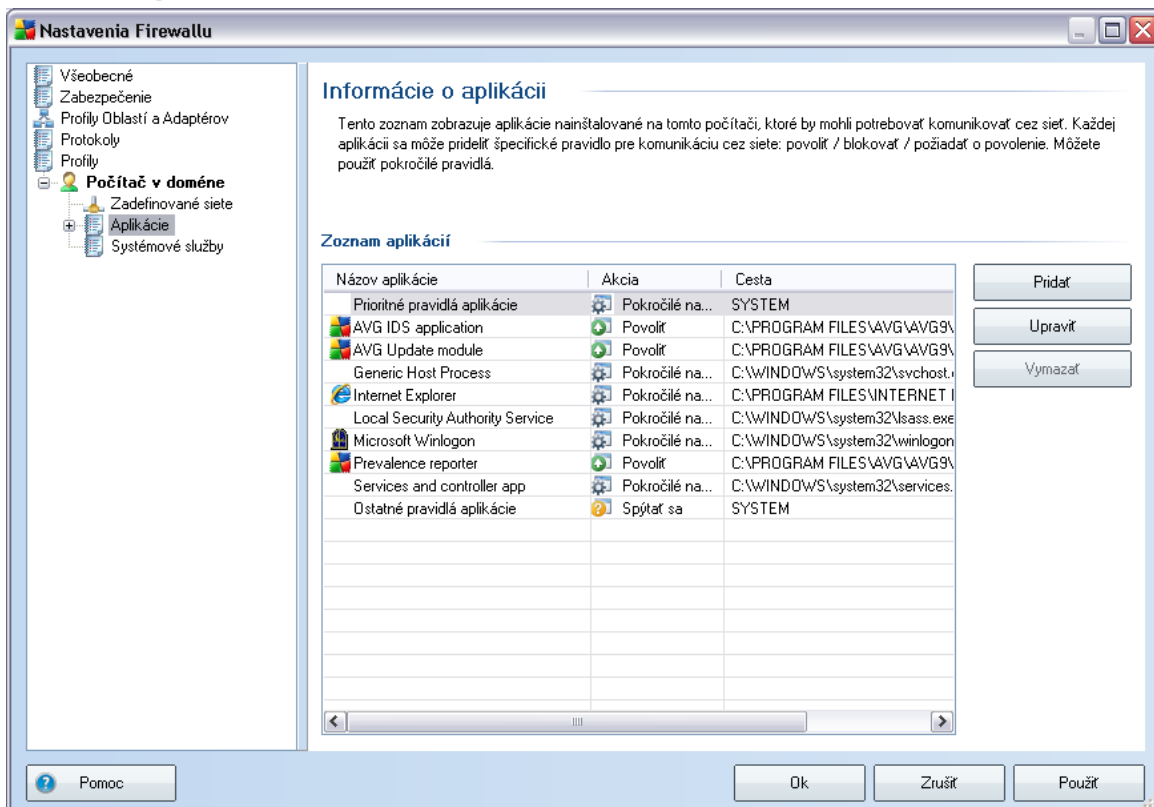


V tomto dialógovom okne môžete definovať **názov siete**, **opis siete** a prípadne nastaviť sieť ako bezpečnú. Novú sieť môžete definovať buď ručne v samostatnom dialógovom okne, ktoré sa otvára pomocou tlačidla **Pridať adresu IP** (prípadne **Editovať adresu IP/Vymazať adresu IP**), alebo v tomto dialógovom definovaním rozsahu adres IP alebo masky.






Pri veľkom počte sietí, ktoré sa majú nastaviť ako súčasť novo vytvorenej siete, môžete použiť možnosť **Podrobné definovanie rozsahu adres IP**; zadajte zoznam všetkých sietí do príslušného textového pola (*môžete použiť ľubovoľný štandardný formát*) a stlačením tlačidla **Overiť** skontrolujte, či je formát rozpoznateľný. Potom stlačením tlačidla **OK** potvrdíte a uložíte údaje.

- **Editovať sieť:** Otvorí dialógové okno **Vlastnosti siete** (pozri vyššie v texte), v ktorom môžete zmeniť parametre definovanej siete (toto dialógové okno je rovnaké ako dialógové okno pre pridanie novej siete; pozri informácie v predchádzajúcom odseku)
- **Vymazať sieť:** Odstráni záznam o zvolenej sieti zo zoznamu sietí.
- **Oznáčiť ako bezpečnú:** Štandardne sa všetky siete považujú za nezabezpečené a iba ak ste presvedčený, že je príslušná sieť bezpečná, môžete ju pomocou tohto tlačidla oznáčiť za bezpečnú (a naopak, po oznáčení siete za bezpečnú sa text tlačidla zmení na „Oznáčiť ako nezabezpečenú“).
- **Pomocník:** Otvorí súbor pomocníka v dialógovom okne.

11.5.3. Aplikácie



V informacnom dialógovom okne **Aplikácie** sa nachádza zoznam všetkých nainštalovaných aplikácií, ktoré pravdepodobne budú musieť komunikovať v sieti a ikony pre príslušnú akciu:

-  Povolit komunikáciu pre všetky siete
-  Povolit komunikáciu pre siete definované ako Len bezpečné
-  Blokovat komunikáciu
-  Zobrazit dialógové okno s otázkou (*umožní vám rozhodnúť, či sa má povoliť alebo blokovat komunikácia*)
-  Rozšírené nastavenia definované

Bud počas prehľadávania [Sprievodcom konfiguráciou súčasti Firewall](#) alebo neskôr, pri výskyte neznámej alebo novo nainštalovanej aplikácie, bola v počítači zistená prítomnosť aplikácií zo zoznamu (*a boli im pridelené príslušné akcie*).

Poznámka: Upozornujeme, že program deteguje len aplikácie, ktoré sú už nainštalované, takže ak neskôr nainštalujete novú aplikáciu, budete musieť pre ňu definovať pravidlá v súčasti Firewall. Pri štandardnom nastavení, ak sa nová aplikácia pokúsi prvýkrát pripojiť v sieti, súčast Firewall bud pre ňu automaticky vytvorí pravidlo podl a dôveryhodnej databázy, alebo sa vás opýta, či chcete povoliť alebo blokovat komunikáciu. V druhom prípade budete môcť uložiť odpoveď ako trvalé pravidlo (ktoré sa potom zobrazí v tomto dialógovom okne).

Samozrejme, že pravidlá pre novú aplikáciu môžete definovať aj hneď: v tomto dialógovom okne stlačte tlačidlo **Pridat** a vyplňte informácie o aplikácii.

Okrem aplikácií sa v zozname nachádzajú aj dve špeciálne položky:

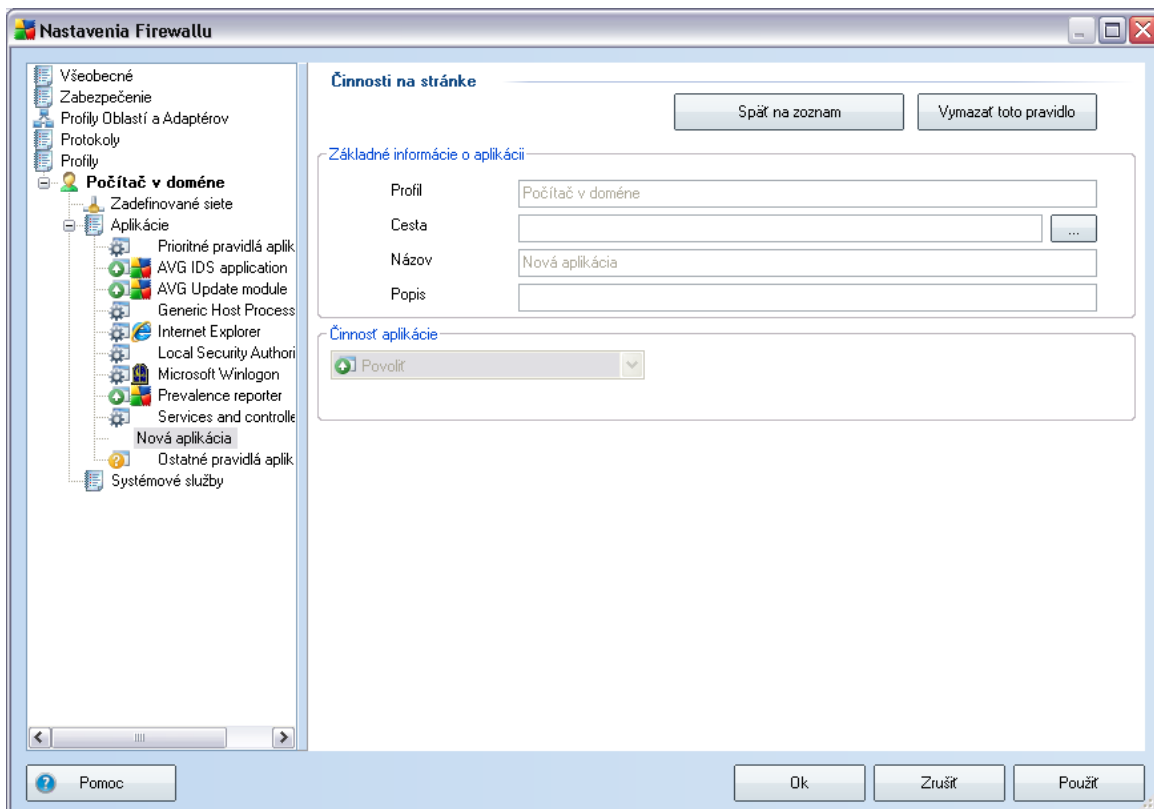
- **Prioritné pravidlá pre aplikácie** (v hornej časti zoznamu) sú prednostné a vždy sa použijú pred pravidlami jednotlivých aplikácií.
- **Dalšie pravidlá pre aplikácie** (v spodnej časti zoznamu) sa použijú ako „posledná možnosť“ v prípade, keď sa nepoužijú konkrétne pravidlá pre aplikácie, napr. pre neznáme a nedefinované aplikácie.

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 editovanie zoznamu sa používajú nasledujúce ovládacie tlačidlá:

- **Pridat** – Otvorí prázdne dialógové okno **Cinnosti na stránke**, ktoré sa používa na definovanie nových pravidiel pre aplikáciu.
- **Editovat** – Otvorí to isté dialógové okno **Cinnosti na stránke**, ktoré sa používa na editovanie existujúcej skupiny pravidiel pre aplikáciu.
- **Vymazat** – Odstráni zvolenú aplikáciu zo zoznamu.
- **Pomocník** – Otvorí dialógové okno s pomocníkom.



Toto dialógové okno sa používa na podrobné definovanie nastavení pre príslušnú aplikáciu.

Cinnosti na stránke






- Τλαϋδλο **Spät na zoznam** zobrazí prehľad všetkých definovaných pravidiel pre aplikácie.
- Τλαϋδλο **Vymazať toto pravidlo** vymaže práve zobrazené pravidlo pre aplikáciu. Upozornujeme, že 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 vyhladaťte aplikáciu v stromovej štruktúre.

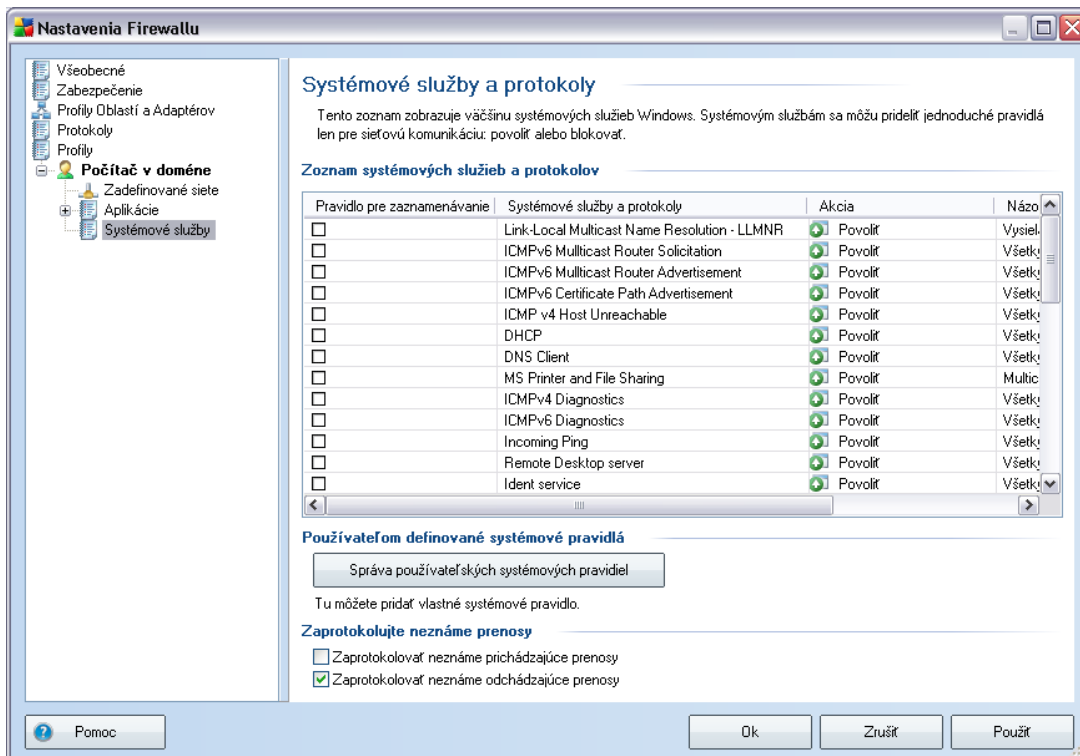
Akcia pre aplikáciu

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



-  **Povolit pre všetky** umožní aplikácii komunikovať vo všetkých definovaných sieťach a pomocou všetkých definovaných sieťových kariet bez obmedzení.
-  **Povolit pre bezpečné** umožní aplikácii komunikovať len v sieťach definovaných ako bezpečné (dôveryhodné).
-  **Blokovat** automaticky zakáže komunikáciu; aplikácia sa nebude môcť pripojiť na žiadnu sieť.
-  **Spýtat sa** zobrazí dialógové okno, ktoré vám umožní rozhodnúť, či sa má povolit alebo blokovat pokus o komunikáciu v danom momente.
-  **Μο~voσε Rozšírené nastavenia** zobrazí ďalšie rozšírené a podrobné možnosti nastavenia v spodnej časti dialógového okna v časti **Pravidlá pre aplikácie**. Nastavenia sa použijú v uvedenom poradí, takže ich môžete **posúvat hore** resp. **posúvat 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.

11.5.4. Systémové služby

Zmeny v dialógovom okne *Systémové služby a protokoly* odporúčame robiť **LEN skúseným používateľom!**



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

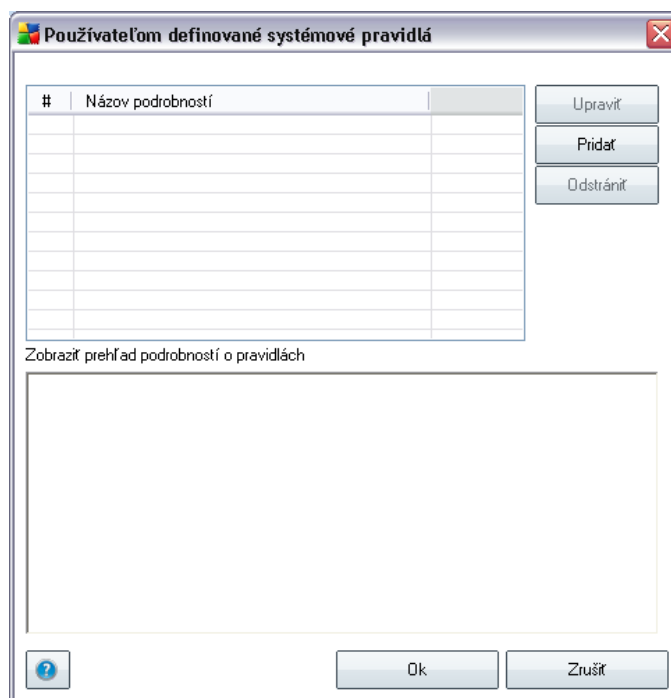
- **Zaznamenať cinnosti pravidla:** Používa sa na zapnutie funkcie zaznamenania každého použitia pravidla v záznamových protokoloch.
- **Systémová služba a protokoly:** Tento stĺpec uvádza názov príslušnej systémovej služby.
- **Akcia:** V tomto stĺpci sa nachádza ikona pridelenej akcie:
 -  Povolit komunikáciu pre všetky siete
 -  Povolit komunikáciu pre siete definované ako Len bezpečné

-  Blokovat komunikáciu

- **Siete:** Tento stlpec informuje, ktorej konkrétnej sieti sa systémové pravidlo týka.

Na editovanie zoznamu (*vrátane pridelených akcií*) sa používajú nasledujúce ovládacie tlačidlá:

- Ak chcete zmeniť nastavenia položky v zozname (*vrátane pridelených akcií*), kliknite pravým tlačidlom myši na položku a zvolte možnosť **Editovať**.
- Ak chcete otvoriť nové dialógové okno na definovanie vlastného pravidla pre systémovú službu (*pozri nasledujúci obrázok*), 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 zvolené informácie. Na editovanie, prídanie resp. vymazanie používateľom definovaného pravidla sa používa príslušné tlačidlo; výrobcom definované pravidlá sa dajú len editovať:



Upozornenie: Upozorňujeme, že nastavenia pravidiel sú podrobné a primárne určené pre správcov siete, ktorí potrebujú mať úplnú kontrolu nad konfiguráciou súčasti Firewall. Ak nie ste oboznámený s typmi komunikačných protokolov, číslami sieťových portov, definíciami adres IP a pod., nemente tieto nastavenia! Ak naozaj potrebujete zmeniť konfiguráciu, postupujte podľa pokynov v príslušných súboroch pomocníka.

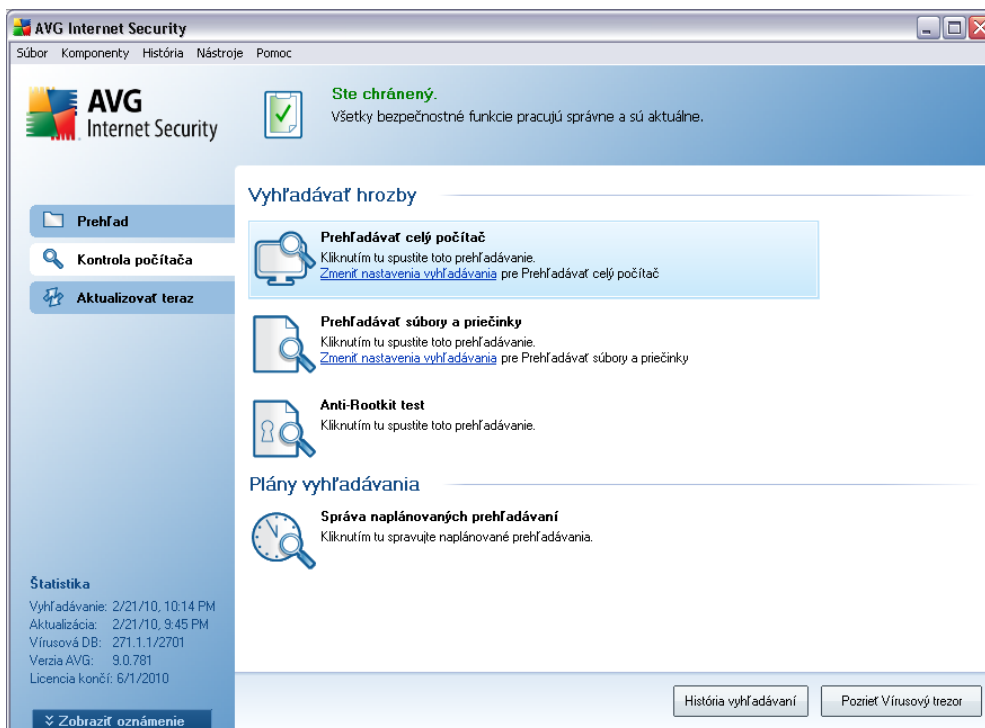
Zaznamenať neznáme prenosy

- **Zaznamenať neznáme prichádzajúce prenosy:** Zaciarknite toto políčko, ak chcete zaznamenať zo záznamových protokolov každý neznámy pokus o pripojenie do počítača zvonka
- **Zaznamenať neznáme odchádzajúce prenosy:** Zaciarknite toto políčko, ak chcete zaznamenať zo záznamových protokolov každý neznámy pokus o pripojenie počítača na vonkajšiu adresu

12. Vyhľadávanie AVG

Prehľadávanie predstavuje rozhodujúcu časť funkcionality produktu **AVG 9 Anti-Virus plus Firewall**. Umožňuje spúšťať testy na požiadanie a [naplávať ich pravidelné spúšťanie](#) vo vhodnom case.

12.1. Rozhranie vyhľadávania



Rozhranie vyhľadávania AVG je dostupné cez rýchly odkaz **Kontrola počítača*****. Kliknite na tento odkaz pre prepnutie na dialógové okno **Vyhľadávať hrozby**. V tomto dialógovom okne nájdete nasledujúce položky:

- prehľad [vopred definovaných prehľadávaní](#) - tri druhy prehľadávania definované dodávateľom softvéru sú pripravené na použitie okamžitým výberom alebo ako naplánované:
 - [Prehľadávať celý počítač](#)
 - [Prehľadávať konkrétne súbory a priečinky](#)
 - **Vyhľadávanie programov Anti-Rootkit**

- [cast plánovanie vyhľadávania](#) - kde môžete zadefinovať nové testy a vytvoriť nové plány podľa potreby.

Ovládacie tlačidlá

Ovládacie tlačidlá dostupné v testovacom rozhraní sú nasledovné:

- **História vyhľadávanií** - zobrazí dialógové okno [Prehľad výsledkov vyhľadávania](#) v celej histórii vyhľadávania
- **Pozriete Vírusový trezor** - otvorí nové okno s [Vírusovým trezorom](#) - miesto, kde sa detekované infekcie uložia do karantény

12.2. Vopred zadefinované vyhľadávania

Jednou z hlavných funkcií produktu **AVG 9 Anti-Virus plus Firewall** je prehľadovanie na požiadanie. Testy na požiadanie sú určené na vyhľadávanie v rôznych častiach počítača pri každom podozrení možného výskytu vírusovej infekcie. Odporúča sa vykonávať takéto testy pravidelne, aj keď si myslíte, že sa vo vašom počítači nenájde žiadny vírus.

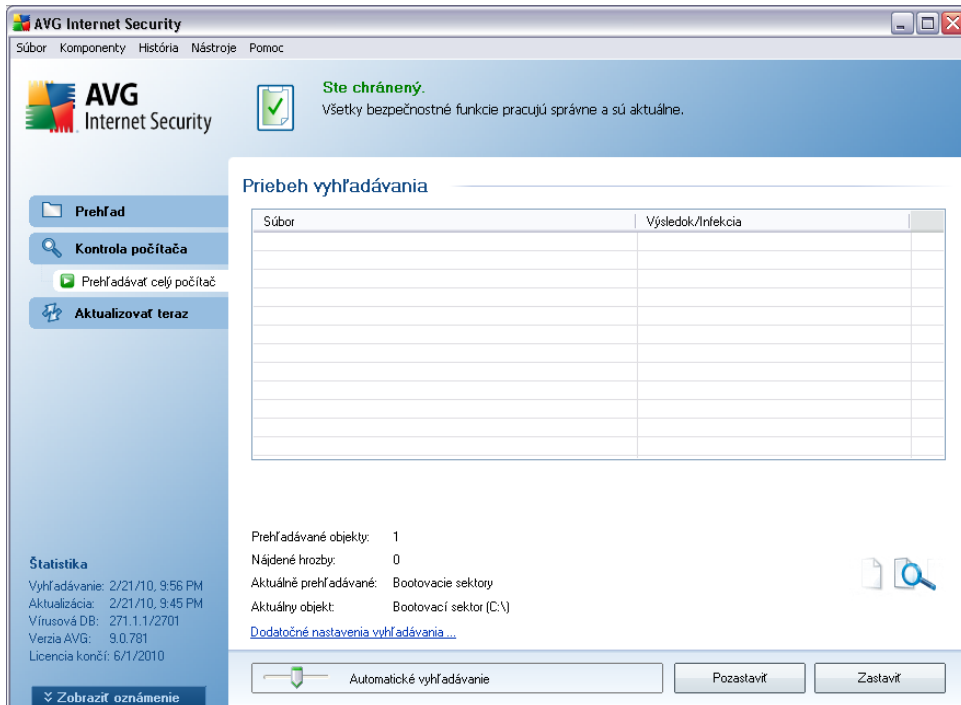
V produkte **AVG 9 Anti-Virus plus Firewall** sa nachádzajú dva typy prehľadávaní nastavené výrobcami softvéru:

12.2.1. Prehľadávať celý počítač

Prehľadávať celý počítač: Vyhľadáva možné infekcie resp. potenciálne nežiaduce programy v celom počítači. Tento test bude prehľadávať všetky pevné disky počítača, deteguje vírusy a vylicí všetky nájdené vírusy alebo ich odstráni do [Vírusového trezora](#). Odporúčame vám naplánovať program takým spôsobom, aby sa prehľadávanie celého počítača spustilo najmenej raz za týždeň.

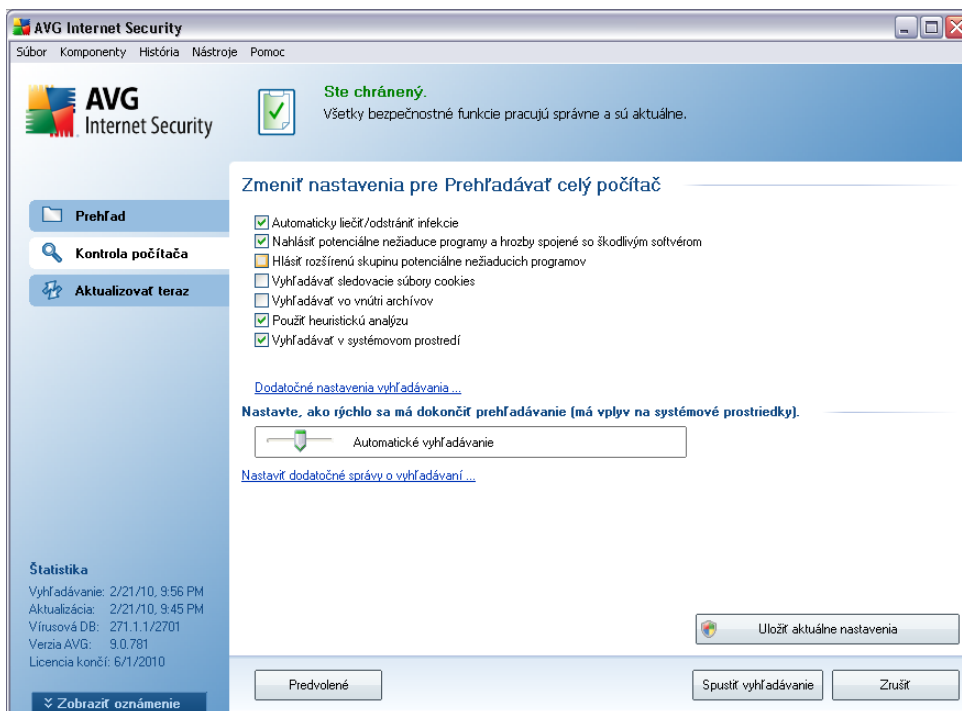
Spustenie prehľadávania

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

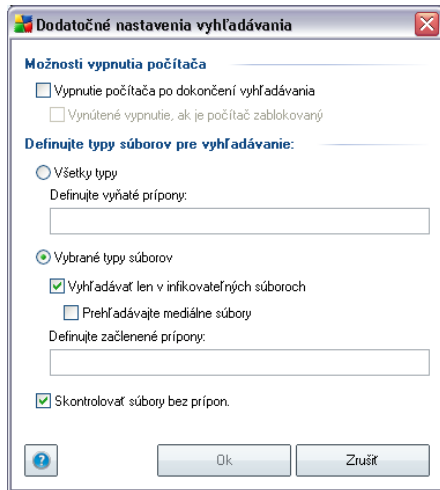


Zmena konfigurácie prehľadávania

Program umožňuje editovať vopred definované predvolené nastavenia **prehľadávania celého počítača**. Kliknutím na odkaz **Zmeniť nastavenia prehľadávania** otvorte dialógové okno **Zmeniť nastavenia prehľadávania pre funkciu prehľadávania celého počítača**. **Odporúčame vám ponechať predvolené nastavenia, ak nemáte vážny dôvod na ich zmenu!**

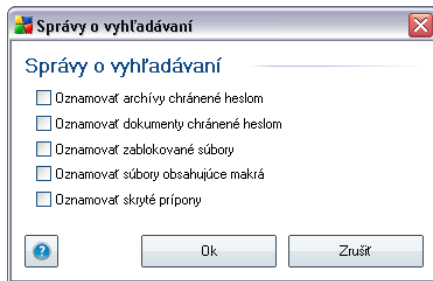


- **Parametre prehľadávania:** V zozname parametrov prehľadávania môžete podľa potreby zapnúť/vypnúť konkrétne parametre. Štandardne je väčšina parametrov zapnutá a tieto parametre sa použijú automaticky počas prehľadávania.
- **Dalšie nastavenia prehľadávania:** Tento odkaz otvorí nové dialógové okno **Dalšie nastavenia prehľadávania**, ktoré sa používa na nastavenie nasledujúcich parametrov:



- **Možnosti vypnutia počítača:** Rozhodnite, či sa má počítač vypnúť automaticky po dokončení procesu prehľadávania. Po potvrdení tejto možnosti (**Vypnúť počítač po dokončení prehľadávania**) sa aktivuje nová možnosť, ktorá umožní vypnúť počítač, aj keď je momentálne zamknutý (**Vynútiť vypnutie počítača, keď je zamknutý**).
- **Definovať typy súborov pre prehľadávanie:** Ďalej môžete rozhodnúť, či sa majú prehľadávať:
 - **Všetky typy súborov** s možnosťou definovať výnimky prehľadávania vytvorením zoznamu čiarkou oddelených prípon súborov, ktoré sa nemajú prehľadávať.
 - **Zvolené typy súborov:** Môžete nastaviť, že chcete prehľadávať len súbory, pri ktorých existuje pravdepodobnosť infikovania (*súbory, ktoré nemôžu byť napadnuté infekciou, napríklad niektoré jednoduché textové súbory, alebo niektoré nespustiteľné súbory*), vrátane mediálnych súborov (*video, audio súborov – ak necháte toto políčko neoznačené, čas prehľadávania sa skrúti 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 prehľadávať vždy.
 - Alternatívne môžete rozhodnúť, že chcete **prehľadávať súbory bez prípony**. Táto možnosť je štandardne zapnutá a odporúčame vám nikdy nemeniť túto konfiguráciu, ak na to nemáte skutočný dôvod. Súbory bez prípony sú skôr podozrivé a mali by sa vždy prehľadávať.

- **Priorita procesu prehládavania:** Použijte posúvac na zmenu priority proces prehládavania. Štandardne je priorita nastavená na strednú úroveň (*Automatické vyhľadávanie*), ktorá optimalizuje rýchlosť procesu vyhľadávania a využívanie systémových zdrojov. Prípadne môžete spustiť procesy vyhľadávania pomalšie, čím sa minimalizuje zataženie systémových zdrojov (*užitočné vtedy, keď potrebujete na počítači pracovať, ale nezaujíma vás, ako dlho bude vyhľadávanie trvať*) alebo rýchlejšie so zvýšenými požiadavkami zataženia systémových zdrojov (*napr. keď je počítač dočasne nepoužívaný*).
- **Vytvoriť ďalšie správy o prehládavaní:** Odkaz otvorí nové dialógové okno **Správy o prehládavaní**, v ktorom môžete zvolit, aké typy možných nálezov sa majú uviesť v správach:



Upozornenie: Tieto nastavenia prehládavania sa zhodujú s parametrami novo definovaného prehládavania; pozri informácie v kapitole [Prehládávanie programom AVG/Plánovanie prehládavania/Ako sa má vyhľadávať](#). Ak sa rozhodnete zmeniť predvolenú konfiguráciu funkcie **Prehládavať celý počítač**, svoje nové nastavenie môžete uložiť ako predvolenú konfiguráciu, ktorá sa použije pre všetky ďalšie prehládavania celého počítača.

12.2.2. Prehládavať špecifické súbory alebo priecinky

Prehládavať konkrétne súbory alebo priecinky: Prehládavať sa budú len vami zvolené oblasti počítača (zvolené priecinky, pevné disky, diskety, disky CD a pod.). Priebeh prehládavania pri detegovaní vírusu a jeho liečba sú rovnaké ako pri prehládavaní celého počítača: [všetky nájdené vírusy sa vyliečia alebo odstránia do Vírusového trezora](#). Prehládávanie konkrétnych súborov alebo priecinkov môžete použiť na nastavenie vlastných testov a ich plánov v závislosti od konkrétnych potrieb.

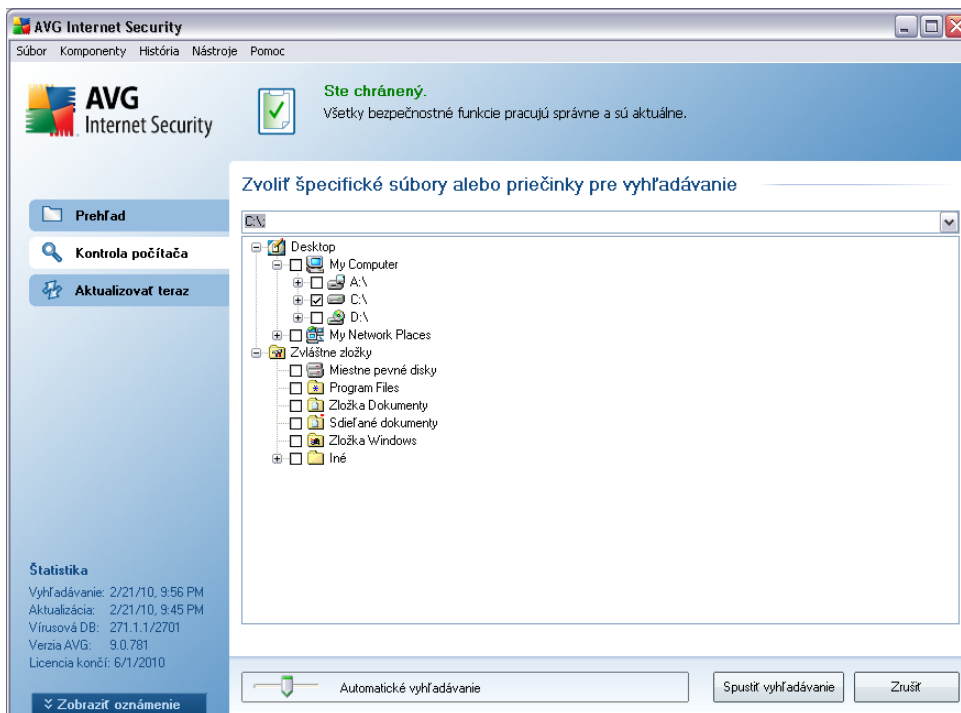
Spustenie prehládavania

Prehládávanie konkrétnych súborov alebo priecinkov môžete spustiť priamo z [rozhrania prehládavania](#) kliknutím na ikonu prehládavania. Otvorí sa nové dialógové

okno s názvom **Výber konkrétnych súborov alebo priečinkov na prehľadávanie**. V stromovej štruktúre počítača zvolte tie priečinky, ktoré chcete prehľadávať. Cesta ku každému zvolenému priečinku sa vygeneruje automaticky a objaví sa v textovom okne vo vrchnej časti tohto dialógového okna.

Rovnako môžete nastaviť prehľadávanie konkrétneho priečinka, ktorého vnorené priečinky sa vylúčia z tohto prehľadávania; v tom prípade vložte znak mínus „-“ pred automaticky vygenerovanú cestu (*pozri snímku obrazovky*). Ak chcete vylúčiť z vyhľadávania celý priečinok, použite „!“ parameter.

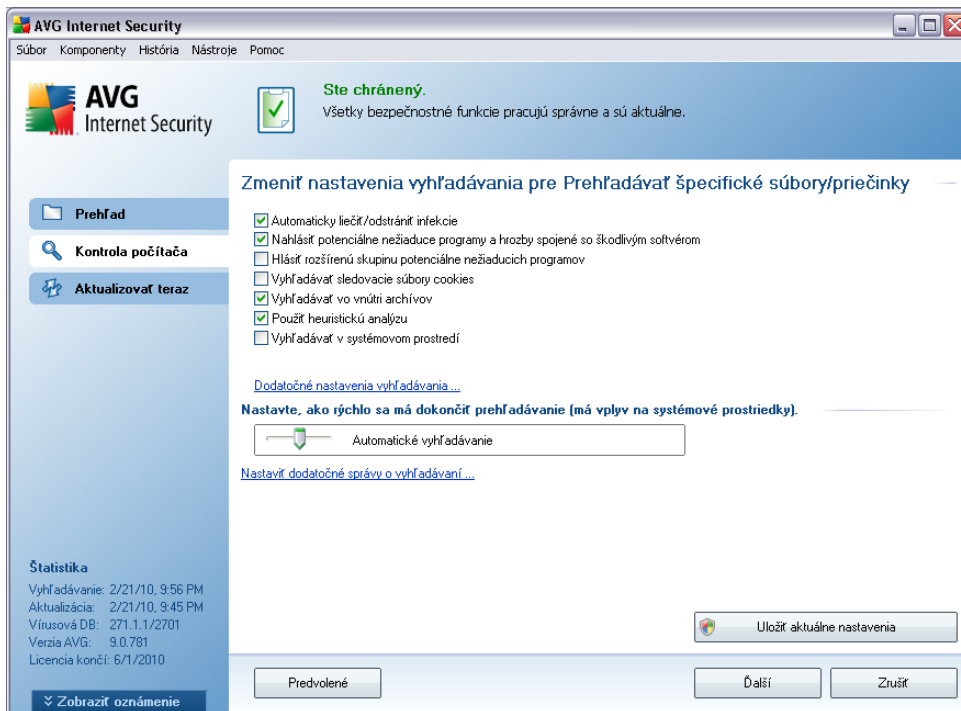
Napokon, ak chcete spustiť prehľadávanie, stlačte tlačidlo **Spustiť prehľadávanie**; samotný proces sa v podstate zhoduje s [prehľadávaním celého počítača](#).



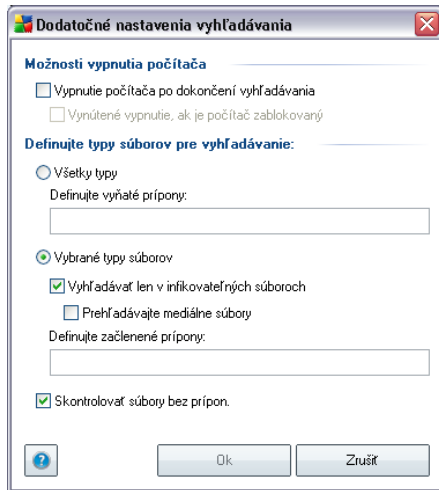
Zmena konfigurácie prehľadávania

Program umožňuje zmeniť vopred definované predvolené nastavenia pre funkciu **prehľadať konkrétne súbory alebo priečinky**. Kliknutím na odkaz **Zmeniť nastavenia prehľadávania** otvorte dialógové okno **Zmena nastavení prehľadávania pre prehľadávanie konkrétnych súborov alebo priečinkov**. **Odporúčame vám ponechať predvolené nastavenia, ak nemáte vážny dôvod na**

ich zmenu!

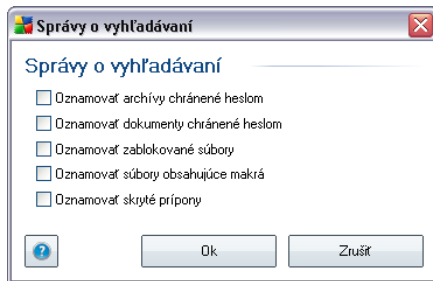


- **Parametre prehl adávania:** V zozname parametrov prehľadávania môžete podľa potreby zapnúť/vypnúť konkrétne parametre (*podrobné informácie o týchto nastaveniach sa nachádzajú v kapitole [Rozšírené nastavenia AVG/Prehľadávania/Prehľadávať konkrétne súbory alebo priečinky](#)*).
- **Dalšie nastavenia prehl adávania:** Tento odkaz otvorí nové dialógové okno Ďalšie nastavenia prehľadávania, ktoré sa používa na nastavenie nasledujúcich parametrov:



- **Možnosti vypnutia počítača:** Rozhodnite, či sa má počítač vypnúť automaticky po dokončení procesu prehľadávania. Po potvrdení tejto možnosti (**Vypnúť počítač po dokončení prehľadávania**) sa aktivuje nová možnosť, ktorá umožní vypnúť počítač, aj keď je momentálne zamknutý (**Vynútiť vypnutie počítača, keď je zamknutý**).
- **Definovať typy súborov pre prehľadávanie:** Ďalej môžete rozhodnúť, či sa majú prehľadávať:
 - **Všetky typy súborov** s možnosťou definovať výnimky prehľadávania vytvorením zoznamu čiarkou oddelených prípon súborov, ktoré sa nemajú prehľadávať.
 - **Zvolené typy súborov:** Môžete nastaviť, že chcete prehľadávať len súbory, pri ktorých existuje pravdepodobnosť infikovania (*súbory, ktoré nemôžu byť napadnuté infekciou, napríklad niektoré jednoduché textové súbory, alebo niektoré nespustiteľné súbory*), vrátane mediálnych súborov (*video, audio súborov – ak necháte toto políčko neoznačené, čas prehľadávania sa skrúti 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 prehľadávať vždy.
 - Alternatívne môžete rozhodnúť, že chcete **prehľadávať súbory bez prípony**. Táto možnosť je štandardne zapnutá a odporúčame vám nikdy nemeniť túto konfiguráciu, ak na to nemáte skutočný dôvod. Súbory bez prípony sú skôr podozrivé a mali by sa vždy prehľadávať.

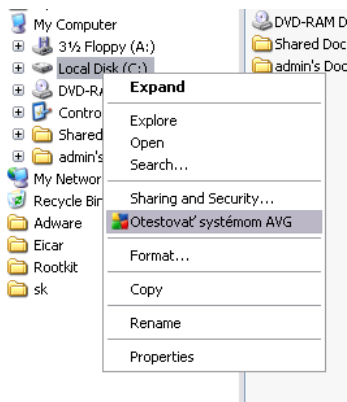
- **Priorita procesu prehládavania:** Použijte posúvac na zmenu priority proces prehládavania. Štandardne je priorita nastavená na strednú úroveň (*Automatické vyhľadávanie*), ktorá optimalizuje rýchlosť procesu vyhľadávania a využívanie systémových zdrojov. Prípadne môžete spustiť procesy vyhľadávania pomalšie, čím sa minimalizuje zataženie systémových zdrojov (*užitočné vtedy, keď potrebujete na počítači pracovať, ale nezaujíma vás, ako dlho bude vyhľadávanie trvať*) alebo rýchlejšie so zvýšenými požiadavkami zataženia systémových zdrojov (*napr. keď je počítač dočasne nepoužívaný*).
- **Vytvoriť ďalšie správy o prehládavaní:** Odkaz otvorí nové dialógové okno **Správy o prehládavaní**, ktoré vám umožní nastaviť, ktoré typy možných nálezov sa majú hlásiť:



Upozornenie: Tieto nastavenia prehládavania sa zhodujú s parametrami novo definovaného prehládavania; pozri informácie v kapitole [Prehládávanie programom AVG/Plánovanie prehládavania/Ako sa má vyhľadávať](#). Ak sa rozhodnete zmeniť predvolenú konfiguráciu funkcie **prehládávať konkrétne súbory alebo priečinky**, svoje nové nastavenie môžete potom uložiť ako predvolenú konfiguráciu, ktorá sa použije pre všetky ďalšie prehládavania konkrétnych súborov alebo priečinkov. Táto konfigurácia sa zároveň použije ako šablóna pre všetky vami novo naplánované prehládavania ([všetky nastavené prehládavania vychádzajú zo súčasnej konfigurácie prehládavania zvolených súborov alebo priečinkov](#)).

12.3. Vyhľadávanie vo Windows Exploreri

Okrem vopred definovaných prehládavání spustených pre celý počítač alebo jeho zvolené oblasti, **AVG 9 Anti-Virus plus Firewall** zároveň umožňuje rýchlo prehládávať konkrétny objekt priamo v prostredí programu Windows Explorer. Ak chcete otvoriť neznámy súbor a nemôžete si byť istý jeho obsahom, možno budete chcieť skontrolovať ho na požiadanie. Postupujte podľa týchto krokov:



- V programe Windows Explorer zvýraznite súbor (alebo priečinok), ktorý chcete skontrolovať.
- Kliknite pravým tlačidlom myši na objekt otvorte kontextovú ponuku.
- Výberom možnosti **Prehľadávať programom AVG** prehladájte súbor programom AVG.

12.4. Vyhladávanie v Príkazovom riadku

Program **AVG 9 Anti-Virus plus Firewall** ponúka možnosť spustiť prehľadávanie z príkazového riadka. Túto možnosť môžete použiť napríklad pri serveroch alebo keď vytvárate batchový skript, ktorý sa bude spúšťať automaticky po naboťovaní počítača. Z príkazového riadka môžete spustiť vyhľadávanie s väčšinou parametrov, ako je to uvedené v grafickom používateľskom rozhraní AVG.

Na spustenie prehľadávania programom AVG z príkazového riadka spustíte nasledujúci príkaz v priečinku, v ktorom je nainštalovaný program AVG:

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

Syntax príkazu

Nasledujúce je syntax príkazového riadka:

- **avgscanx /parameter ...** napr. **avgscanx /comp** pre prehľadávanie celého počítača

- **avgscanx /parameter /parameter** ... pri použití viacerých parametrov parametre zoradte za sebou a oddelte ich medzerou a lomkou
- ak sa pre parameter musí uviesť konkrétna hodnota (napr. parameter **/scan**, ktorý vyžaduje informáciu o tom, ktoré oblasti počítača sa majú prehľadávať a je potrebné uviesť presnú cestu k zvolenej časti), hodnoty sa oddelia bodkociarkou, napríklad: **avgscanx /scan=C:\;D:**

Parametre prehladávaní

Ak chcete zobrazit 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 prehľadávať. Podrobnejšie informácie o možnostiach sa nachádzajú v [prehlade parametrov príkazového riadka](#).

Na spustenie prehladávaní stlačte kláves **Enter**. Pčas prehladávaní môžete zastavit proces stlačením kombinácie klávesov **Ctrl+C** alebo **Ctrl+Pause**.

Prehladávanie z príkazového riadka spustené z grafického rozhrania

Ak používate operacný systém Windows a počítač je nastavený do núdzového režimu, môžete spustiť prehladávanie z príkazového riadka z grafického používateľského rozhrania. Samotné prehladávanie sa spustí z príkazového riadka, dialógové okno **Command Line Composer** umožňuje zadat väčšinu parametrov prehladávaní len pomocou praktického grafického rozhrania.

Kedže toto dialógové okno je možné otvoriť, len keď je počítač s operacným systémom Windows nastavený do núdzového režimu, na zobrazenie podrobných informácií o tomto dialógovom okne použite súbor s pomocníkom, ktorý sa otvára priamo z dialógového okna.

12.4.1. Parametre vyhladávaní CMD

Nasledujúce je zoznam všetkých parametrov použiteľných pri prehladávaní z príkazového riadka:

- **/SCAN** [Prehľadávať konkrétne súbory alebo priecinky](#) /
SCAN=path;path (napr. /SCAN=C:\;D:\)
- **/COMP** [Prehľadávať celý počítač](#)
- **/HEUR** Použiť [heuristickú analýzu](#)

- **/EXCLUDE** Vylúčiť cestu alebo súbory z prehľadávania
- **/@** Súbor s príkazmi /názov súboru/
- **/EXT** Prehľadávať tieto prípony /napríklad EXT=EXE,DLL/
- **/NOEXT** Neprehľadávať tieto prípony /napríklad NOEXT=JPG/
- **/ARC** Prehľadávať archívy
- **/CLEAN** Automaticky vycistiť
- **/TRASH** Premiestniť infikované súbory do [Vírusového trezora](#)
- **/QT** Rýchly test
- **/MACROW** Oznamovať makrá
- **/PWDW** Oznamovať súbory chránené heslom
- **/IGNLOCKED** Ignorovať zamknuté súbory
- **/REPORT** Oznamovať do súboru /názov súboru/
- **/REPAPPEND** Pripojiť k súboru so správou
- **/REPOK** Označiť neinfikované súbory slovom OK
- **/NOBREAK** Nepovolit prerušenie klávesmi CTRL-BREAK
- **/BOOT** Povolit kontrolu MBR/BOOT
- **/PROC** Prehľadávať aktívne procesy
- **/PUP** Oznamovať „[potenciálne nežiaduce programy](#)“
- **/REG** Vyhladávať v registroch
- **/COO** Prehľadávať súbory cookies
- **/?** Zobrazit pomocníka pre túto tému
- **/HELP** Zobrazit pomocníka pre túto tému
- **/PRIORITY** Nastaviť prioritu prehľadávania /nízka, automatická,

vysoká/ (pozri časť [Rozšírené nastavenia/Prehľadávania](#))

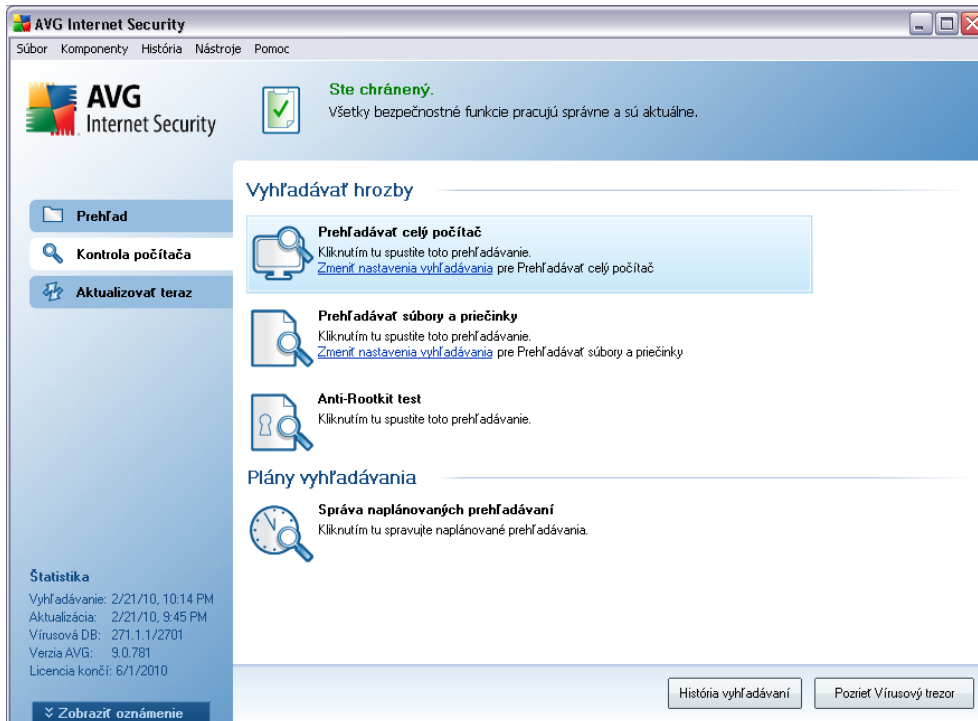
- **/SHUTDOWN** Vypnúť počítač po dokončení prehľadávania
- **/FORCESHUTDOWN** Vynútené vypnutie počítača po dokončení prehľadávania
- **/ADS** Prehľadať alternatívne dátové prúdy (len pre NTFS)

12.5. Plánovanie vyhľadávanií

AVG 9 Anti-Virus plus Firewall umožňuje spustiť prehľadávanie na požiadanie (napríklad, keď máte podozrenie, že sa do počítača dostala infekcia) alebo na základe vytvoreného plánu. Odporúčame vám spúšťať prehľadávanie podľa plánov: týmto spôsobom sa zabezpečí, že počítač bude chránený pred infikovaním a nebudete si musieť robiť starosti s tým, kedy a či vôbec máte spustiť prehľadávanie.

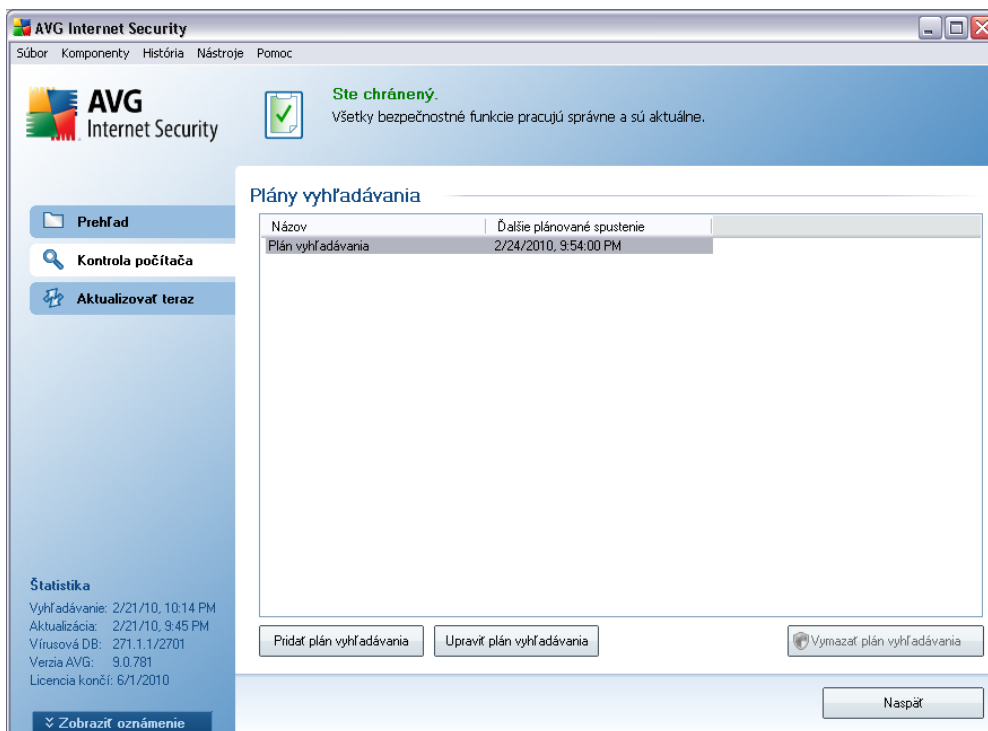
Odporúčame vám, aby ste najmenej raz za týždeň spustili [prehľadávanie celého počítača](#). Podľa možnosti však prehľadávanie celého počítača spúšťajte každý deň predvolenej konfigurácie plánu prehľadávania. Ak je počítač „stále zapnutý“, potom môžete naplánovať prehľadávanie na čas, keď sa počítač nepoužíva. Ak je počítač v tomto čase vypnutý, zmeškané naplánované prehľadávanie sa potom spustí [pri spustení počítača](#).

Ak chcete vytvoriť nový plán prehľadávania, otvorte [rozhranie vyhľadávania programom AVG](#) a prejdite na spodnú časť s názvom **Naplánovanie prehľadávania**:



Naplánovanie prehľadávania

Kliknutím na grafickú ikonu v časti **Naplánovanie prehľadávania** otvorte nové dialógové okno **Naplánovanie prehľadávania** so zoznamom všetkých momentálne naplánovaných prehľadávanií.

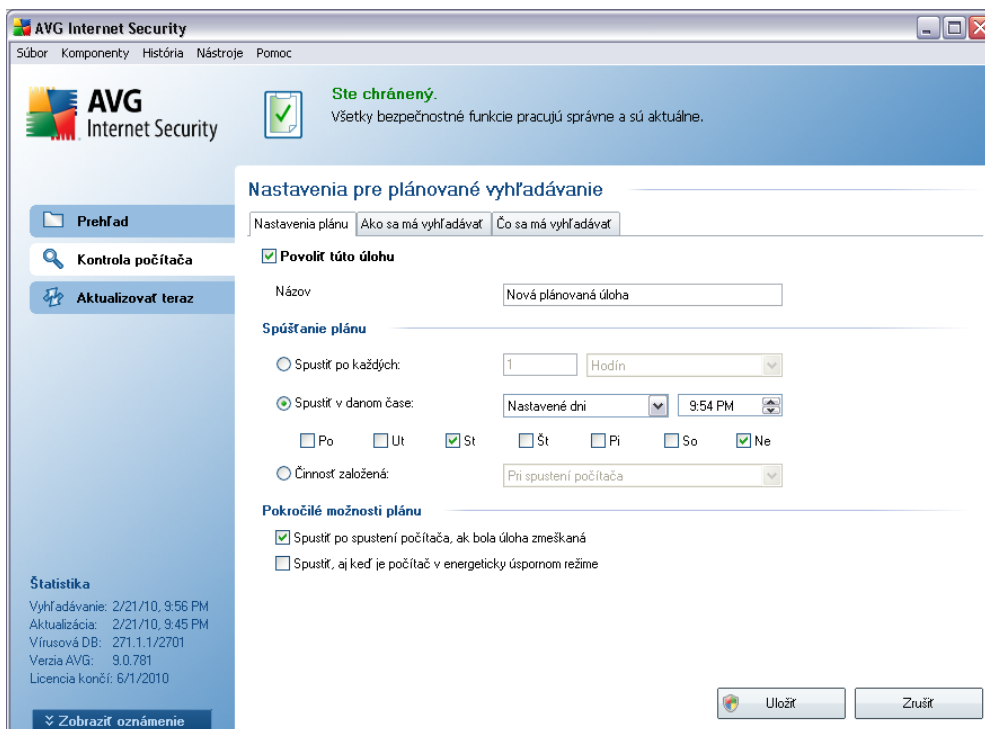


Umožňuje editovať/pridať prehľadávania pomocou nasledujúcich ovládacích tlačidiel:

- **Pridať plán prehľadávania:** Toto tlačidlo otvorí dialógové okno **Nastavenia naplánovaného prehľadávania**, kartu **Nastavenia plánu**. V tomto dialógovom okne nastavte parametre novo definovaného testu.
- **Editovať plán prehľadávania:** Toto tlačidlo je aktívne len v prípade, ak ste už predtým zvolili existujúci test v zozname naplánovaných testov. V tomto prípade sa toto tlačidlo objaví ako aktívne a môžete naň kliknúť pre prepnutie na dialógové okno **Nastavenia pre plánované vyhľadanie**, kartu **Nastavenia plánu**. Parametre zvoleného testu sú tu už uvedené a dajú sa upraviť.
- **Vymazať plán prehľadávania:** Toto tlačidlo je tiež aktívne len v prípade, ak ste už predtým zvolili existujúci test v zozname naplánovaných testov. Tento test môžete potom vymazať zo zoznamu stlačením ovládacieho tlačidla. Môžete však odstrániť len svoje vlastné testy, vopred zadaný **Plán prehľadávania celého počítača** v rámci predvolených nastavení 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 naplánovaného testu** (kliknite na tlačidlo **Pridať plán prehľadovania** v dialógovom okne **Naplánovanie prehľadovania**). Dialógové okno je rozdelené na tri karty: **Nastavenia plánu**: Pozri nasledujúci obrázok (predvolená karta, ktorá sa otvorí automaticky), **Ako sa má prehľadovať** a **Co sa má prehľadovať**.



Na karte **Nastavenia plánu** najskôr oznacím/zrušením oznacenia položky **Povolit túto úlohu** jednoducho dočasne vypnite naplánovaný test a znova ho zapnite v prípade potreby.

Potom uveďte názov vytváraného prehľadovania a plánu. Zadať názov do textového poľa vedľa položky **Název**. Podľa možností použite stručné, opisné a vhodné názvy pre prehľadovania, aby sa neskôr dali ľahšie rozpoznať medzi ostatnými.

Príklad: Nie je vhodné nazvať prehľadovanie „Nové prehľadovanie“ alebo „Moje vyhľadavanie“, pretože tieto názvy nesúvisia s tým, čo sa prehľadovaním vlastne kontroluje. Na druhej strane, príkladom dobrého opisného názvu je „Prehľadovanie systémových oblastí“ a pod. Takisto nie je potrebné zadať do názvu prehľadovania, či ide o prehľadovanie celého počítača alebo prehľadovanie zvolených súborov alebo

priecinkov, pretože vaše vlastné prehľadávania budú vždy predstavovať špeciálnu verziu [prehľadávania zvolených súborov alebo priecinkov](#).

Toto dialógov umožňuje ďalej definovať nasledujúce parametre prehľadávania:

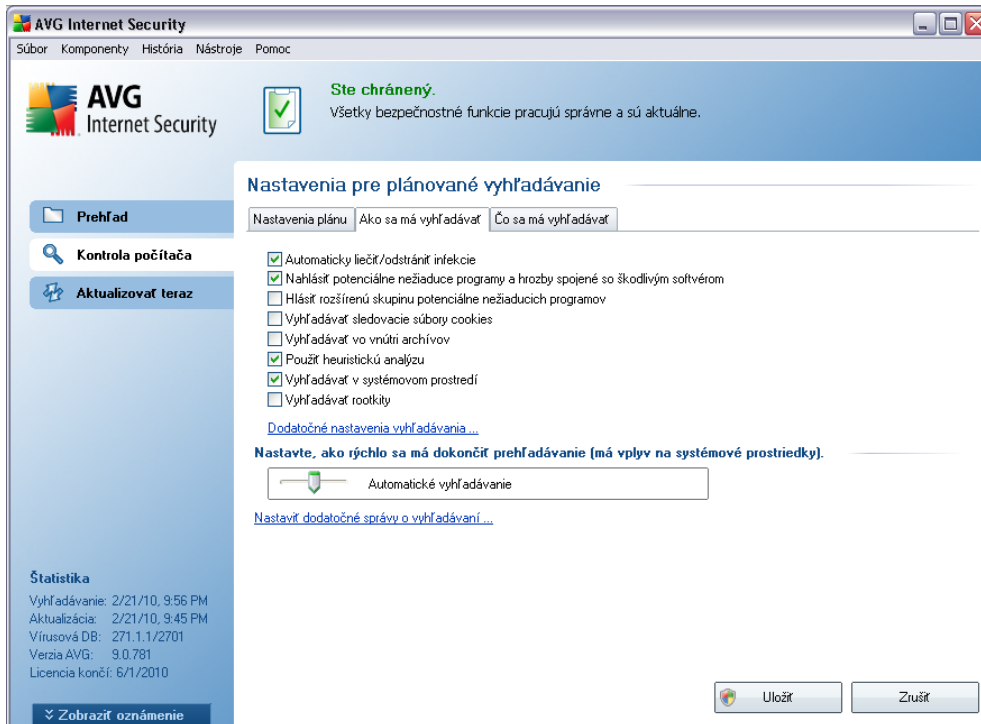
- **Spúšťanie naplánovaných úloh:** Nastavte časové intervaly pre spustenie novo naplánovaného prehľadávania. Casovanie sa definuje ako opakované spúšťanie prehľadávania po uplynutí určitého času (**Spustiť po každých...**), definovaním presného dátumu a času (**Spúšťať v konkrétnom časovom intervale...**), prípadne definovaním udalosti, s ktorou sa bude spájať spustenie prehľadávania (**Cinnosť pri spustení počítača**).
- **Rozšírené možnosti plánu:** Táto časť sa používa na definovanie podmienok, pri ktorých sa má/nemá spustiť prehľadávanie, ak je počítač v úspornom režime alebo úplne vypnutý.

Ovládacie tlačidlá dialógového okna Nastavenia naplánovaného prehľadávania

Na všetkých troch kartách dialógového okna **Nastavenia naplánovaného prehľadávania** (**Nastavenia plánu**, **Ako sa má preadávať** a **Co sa má prehladávať**) 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 prehľadávania programom AVG](#). Preto, ak chcete nastaviť parametre testu na všetkých kartách, stlačením tohto tlačidla ich uložte až po nastavení všetkých požadovaných 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 prehľadávania programom AVG](#).

12.5.2. Ako sa má vyhľadávať



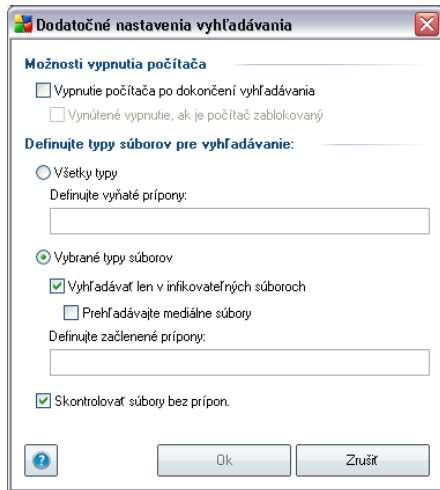
Na karte **Ako sa má prehľadávať** sa nachádza zoznam parametrov prehľadávania, ktoré sa dajú zapnúť resp. vypnúť. Štandardne je väčšina parametrov zapnutá a daná funkcia sa počas vyhľadávania uplatní. Ak nemáte závažný dôvod meniť tieto nastavenia, odporúčame vám ponechať vopred nastavenú konfiguráciu:

- **Automaticky liečiť/odstrániť infekciu** (štandardne zapnuté): Ak sa počas prehľadávania identifikuje vírus, môže sa automaticky vyliečiť, ak je k dispozícii liečba. V prípade, že sa infikované súbory nedajú vyliečiť automaticky alebo ak sa rozhodnete vypnúť túto funkciu, po detekcii vírusu dostanete oznámenie a budete sa musieť rozhodnúť, čo robiť s detekovanou infekciou. Odporúčanou činnosťou je odstrániť infikovaný súbor do [Vírusového trezora](#).
- **Hlásiť potenciálne nežiaduce programy a hrozby spyware** (štandardne zapnuté): Označte túto možnosť, ak chcete zapnúť súčasť [Anti-Spyware](#) a vyhľadávať spyware a vírusy. [Spyware](#) predstavuje pochybnú kategóriu škodlivého softvéru: Aj keď obvyčajne predstavujú bezpečnostné riziko, niektoré takéto programy môžu byť nainštalované úmyselne. Odporúčame vám nechať túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.

- **Hlásit rozšírenú skupinu potenciálne nežiaducich programov:** Ak je zapnutá predchádzajúca možnosť, môžete označiť aj toto zaciarkovacie políčko, a tým povoliť detegovanie rozšírenej skupiny [spywaru](#): programov, ktoré sú úplne v poriadku a neškodné, ak sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje zabezpečenie vášho počítača, ale môže blokovat dobré programy, a preto je táto funkcia štandardne vypnutá.
- **Vyhľadávať sledovacie súbory cookies (štandardne zapnuté):** Tento parameter súčasťou [Anti-Spyware](#) určuje, že sa má zisťovať prítomnosť súborov cookies počas prehľadávania (*cookies HTTP sa používajú na overenie totožnosti, sledovanie a správu konkrétnych informácií o používateľoch, akými sú nastavenia alebo obsah elektronického nákupného košíka*).
- **Vyhľadávať vo vnútri archívov (štandardne zapnuté):** Tento parameter určuje, že počas prehľadávania sa majú kontrolovať všetky súbory, aj keď sú zabalené vo vnútri ľubovlného typu archívu, napr. ZIP, RAR...
- **Použiť heuristiku (štandardne zapnuté):** Heuristická analýza (*dynamická emulácia inštrukcií prehľadávaného objektu vo virtuálnom počítačovom prostredí*) bude predstavovať jednu z metód použitých na detegovanie vírusov počas prehľadávania.
- **Prehľadávať systémové prostredie (štandardne zapnuté):** Počas prehľadávania sa budú kontrolovať aj systémové oblasti počítača.

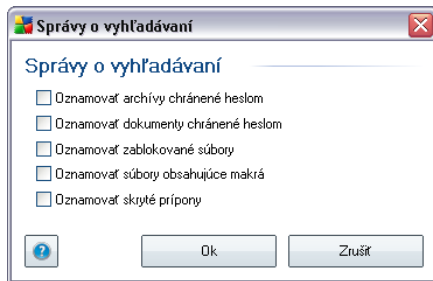
Potom môžete zmeniť konfiguráciu prehľadávania podľa nasledujúceho postupu:

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



- **Možnosti vypnutia počítača:** Rozhodnite, či sa má počítač vypnúť automaticky po dokončení procesu prehľadávania. Po potvrdení tejto možnosti (**Vypnúť počítač po dokončení prehľadávania**) sa aktivuje nová možnosť, ktorá umožní vypnúť počítač, aj keď je momentálne zamknutý (**Vynútiť vypnutie počítača, ak je zamknutý**).
- **Definovať typy súborov pre prehľadávanie:** Ďalej môžete rozhodnúť, či sa majú prehľadávať:
 - **Všetky typy súborov** s možnosťou definovať výnimky prehľadávania vytvorením zoznamu čiarkou oddelených prípon súborov, ktoré sa nemajú prehľadávať.
 - **Zvolené typy súborov:** Môžete nastaviť, že chcete prehľadávať len súbory, pri ktorých existuje pravdepodobnosť infikovania (*súbory, ktoré nemôžu byť napadnuté infekciou, napríklad niektoré jednoduché textové súbory, alebo niektoré nespustiteľné súbory*), vrátane mediálnych súborov (*video, audio súborov – ak necháte toto políčko neoznačené, čas prehľadávania sa skrúti ešte viac, pretože tieto súbory sú často veľmi veľké, pričom pravdepodobnosť napadnutia vírusom je veľmi malá*). Znova môžete definovať, podľa prípony, ktoré súbory sa majú prehľadávať vždy.
 - Alternatívne môžete rozhodnúť, že chcete **prehľadávať súbory bez prípony** – táto možnosť je štandardne zapnutá a odporúčame vám nikdy nemeniť túto konfiguráciu, ak na to nemáte skutocný dôvod. Súbory bez prípony sú skôr podozrivé a mali by sa vždy prehľadávať.

- **Priorita procesu prehládavania:** Použijte posúvac na zmenu priority proces prehládavania. Štandardne je priorita nastavená na strednú úroveň (*Automatické vyhľadávanie*), ktorá optimalizuje rýchlosť procesu vyhľadávania a využívanie systémových zdrojov. Prípadne môžete spustiť procesy vyhľadávania pomalšie, čím sa minimalizuje zataženie systémových zdrojov (*užitočné vtedy, keď potrebujete na počítači pracovať, ale nezaujíma vás, ako dlho bude vyhľadávanie trvať*) alebo rýchlejšie so zvýšenými požiadavkami zataženia systémových zdrojov (*napr. keď je počítač dočasne nepoužívaný*).
- **Vytvoriť ďalšie správy o prehládavaní:** Odkaz otvorí nové dialógové okno **Správy o prehládavaní**, v ktorom môžete zvoliť, aké typy možných nálezov sa majú uviesť v správach:



Poznámka: Konfigurácia prehládavania je štandardne nastavená na dosahovanie optimálneho výkonu. Ak nemáte závažný dôvod meniť nastavenia, odporúčame vám ponechať predvolenú konfiguráciu. Všetky zmeny konfigurácie by mali vykonávať len skúsení používatelia. Ďalšie možnosti konfigurácie prehládavania sa nachádzajú v dialógovom okne **Rozšírené nastavenia**, ktoré sa otvára pomocou položky v hlavnej ponuke programu **Súbor/Rozšírené nastavenie**.

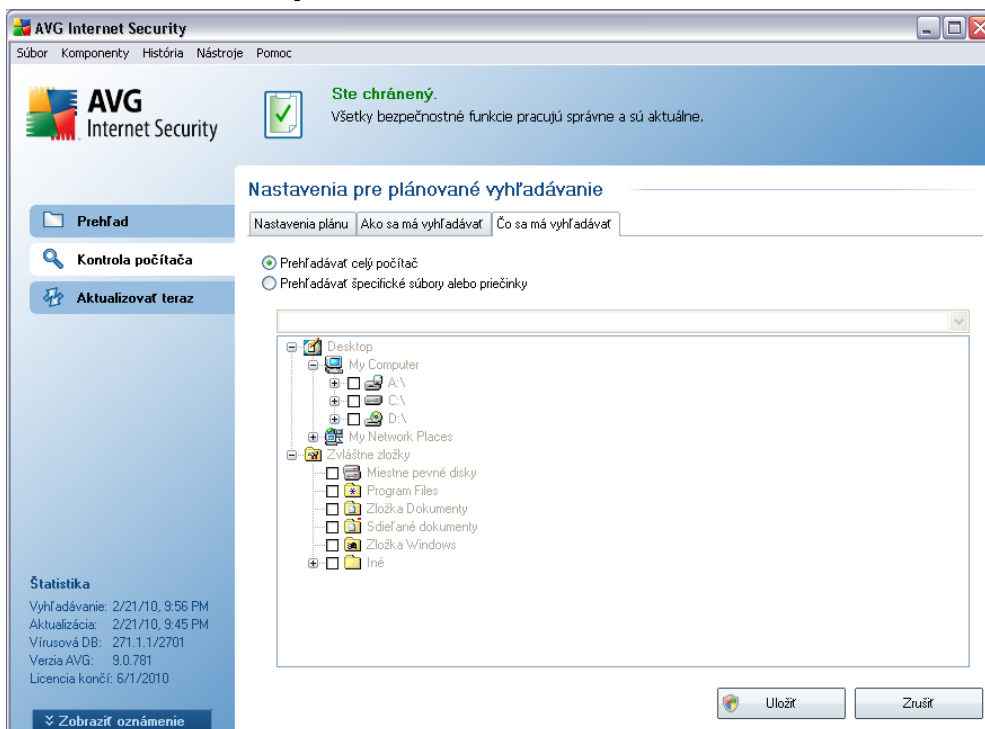
Ovládacie tlačidlá

Na všetkých troch kartách dialógového okna **Nastavenia naplánovaného prehládavania** (**Nastavenia plánu**, **Ako sa má preadávať** a **Co sa má prehládavať**) 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 prehládavania programom AVG](#). Preto, ak chcete nastaviť parametre testu na všetkých kartách, stlačením tohto tlačidla ich uložte až po nastavení všetkých požadovaných možností.
- **Zrušiť:** Zruší všetky zmeny, ktoré ste urobili na tejto karte alebo na inej karte

tohto dialógového okna a prepne naspät na [hlavné dialógové okno s rozhraním prehľadávania programom AVG](#).

12.5.3. Co sa má prehľadávať



Karta **Co sa má prehľadávať** umožňuje nastaviť, či chcete naplánovať [prehľadávanie celého počítača](#) alebo [prehľadávanie konkrétnych súborov alebo priečinkov](#).

Ak zvolíte prehľadávanie konkrétnych súborov alebo priečinkov, v spodnej časti tohto dialógového okna sa aktivuje zobrazená stromová štruktúra, v ktorej môžete nastaviť, ktoré priečinky sa majú prehľadávať (*rozbalte položky kliknutím na uzol so znakom plus a vyhladať priečinok, ktorý chcete prehľadávať*). Zaciarknutím príslušných polícok môžete zvoliť viac priečinkov. Zvolené priečinky sa zobrazia v textovom poli v hornej časti dialógového okna a do prekryvajúcej ponuky sa uloží história vami zvolených prehľadávaní pre neskoršie použitie. Úplnú cestu k požadovanému priečinku môžete zadať aj ručne (*ak zadáte viac ciest, musíte ich oddeliť bodkoviarkou bez medzier*).

V stromovej štruktúre môžete zároveň vyhľadať vetvu s názvom **Špeciálne umiestnenia**. Nasledujúce je zoznam umiestnení, ktoré sa prehľadávajú po označení príslušného zaciarkovacieho políčka:

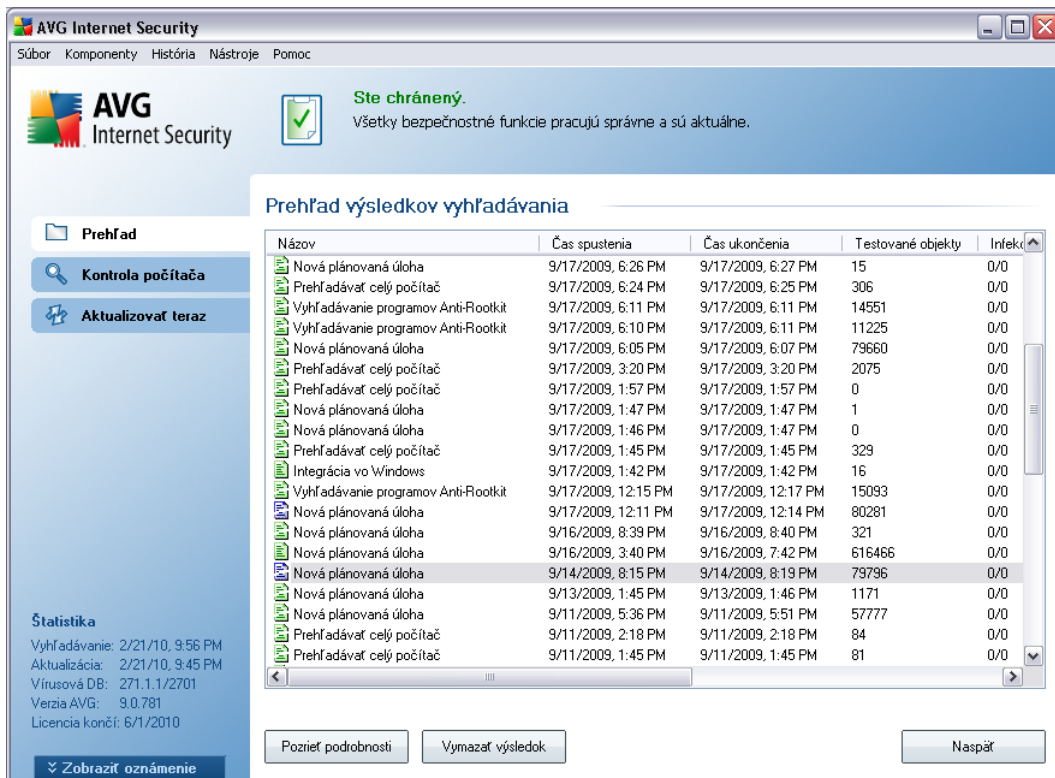
- **Pevné disky počítača:** Všetky pevné disky vášho počítača.
- **Programové súbory:** C:\Program Files\.
- **Priecinok Moje dokumenty:** C:\Dokumenty a nastavenia\Používateľ\Moje dokumenty\
- **Zdieľané dokumenty:** C:\Dokumenty a nastavenia\All Users\Documents\
- **Adresár Windows:** C:\Windows\
- **Iné**
 - **Systémový disk:** Pevný disk, na ktorom je nainštalovaný operacný systém (obvyčajne C:).
 - **Systémový priecinok:** Windows/System32
 - **Priecinok s dočasnými súbormi:** Dokumenty a nastavenia/Používateľ/Local Settings/Temp
 - **Dočasné internetové súbory:** Dokumenty a nastavenia/Používateľ/Local Settings/Temporary Internet Files

Ovládacie tlačidlá dialógového okna Nastavenia naplánovaného prehľadávania

Na všetkých troch kartách dialógového okna **Nastavenia naplánovaného prehľadávania** (**Nastavenia plánu**, **Ako sa má prehľadávať** a **Co sa má prehľadávať**) 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 prehľadávania programom AVG](#). Preto, ak chcete nastaviť parametre testu na všetkých kartách, stlačením tohto tlačidla ich uložte až po nastavení všetkých požadovaných 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 prehľadávania programom AVG](#).

12.6. Prehľad výsledkov vyhľadávania






Prehľad výsledkov vyhľadávania

Názov	Čas spustenia	Čas ukončenia	Testované objekty	Infekcia
Nová plánovaná úloha	9/17/2009, 6:26 PM	9/17/2009, 6:27 PM	15	0/0
Prehľadávať celý počítač	9/17/2009, 6:24 PM	9/17/2009, 6:25 PM	306	0/0
Vyhľadávanie programov Anti-Rootkit	9/17/2009, 6:11 PM	9/17/2009, 6:11 PM	14551	0/0
Vyhľadávanie programov Anti-Rootkit	9/17/2009, 6:10 PM	9/17/2009, 6:11 PM	11225	0/0
Nová plánovaná úloha	9/17/2009, 6:05 PM	9/17/2009, 6:07 PM	79660	0/0
Prehľadávať celý počítač	9/17/2009, 3:20 PM	9/17/2009, 3:20 PM	2075	0/0
Prehľadávať celý počítač	9/17/2009, 1:57 PM	9/17/2009, 1:57 PM	0	0/0
Nová plánovaná úloha	9/17/2009, 1:47 PM	9/17/2009, 1:47 PM	1	0/0
Nová plánovaná úloha	9/17/2009, 1:46 PM	9/17/2009, 1:47 PM	0	0/0
Prehľadávať celý počítač	9/17/2009, 1:45 PM	9/17/2009, 1:45 PM	329	0/0
Integrácia vo Windows	9/17/2009, 1:42 PM	9/17/2009, 1:42 PM	16	0/0
Vyhľadávanie programov Anti-Rootkit	9/17/2009, 12:15 PM	9/17/2009, 12:17 PM	15093	0/0
Nová plánovaná úloha	9/17/2009, 12:11 PM	9/17/2009, 12:14 PM	80281	0/0
Nová plánovaná úloha	9/16/2009, 8:39 PM	9/16/2009, 8:40 PM	321	0/0
Nová plánovaná úloha	9/16/2009, 3:40 PM	9/16/2009, 7:42 PM	616466	0/0
Nová plánovaná úloha	9/14/2009, 8:15 PM	9/14/2009, 8:19 PM	79796	0/0
Nová plánovaná úloha	9/13/2009, 1:45 PM	9/13/2009, 1:46 PM	1171	0/0
Nová plánovaná úloha	9/11/2009, 5:36 PM	9/11/2009, 5:51 PM	57777	0/0
Prehľadávať celý počítač	9/11/2009, 2:18 PM	9/11/2009, 2:18 PM	84	0/0
Prehľadávať celý počítač	9/11/2009, 1:45 PM	9/11/2009, 1:45 PM	81	0/0

Štatistika
 Vyhľadávanie: 2/21/10, 9:56 PM
 Aktualizácia: 2/21/10, 9:45 PM
 Vírusová DB: 271.1.1/2701
 Verzia AVG: 9.0.781
 Licencia končí: 6/1/2010

Dialógové okno **Prehľad výsledkov prehľadávania** sa otvára v [rozhraní prehľadávania programom AVG](#) pomocou tlačidla **História prehľadávání**. V dialógovom okne sa nachádza zoznam všetkých doposiaľ spustených prehľadávání a informácie o ich výsledkoch:

- **Názov:** Označenie vyhľadávania; buď môže ísť o názov niektorého z [vopred definovaných prehľadávání](#) alebo o názov, ktorý ste priradilo [vlastnému naplánovanému prehľadávaniu](#). Každý názov obsahuje ikonu označujúcu výsledok prehľadávania:
 -  – Zelená ikona informuje, že počas prehľadávania nebola detegovaná žiadna infekcia.
 -  – Modrá ikona informuje, že počas prehľadávania bola detegovaná infekcia, ale infikovaný objekt bol automaticky odstránený.
 -  – Červená ikona upozorňuje, že počas prehľadávania bola detegovaná

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).

- **Cas spustenia:** Dátum a čas, kedy bolo prehľadávanie spustené.
- **Cas skoncenia:** Dátum a čas, kedy sa prehľadávanie skončilo.
- **Testované objekty:** Počet objektov, ktoré sa skontrolovali počas prehľadávania.
- **Infekcie:** Počet detegovaných/odstránených [vírusových infekcií](#)
- **Spyware:** Počet detegovaných/odstránených programov typu [spyware](#)
- **Upozornenia:** Počet detegovaných [podozrivých objektov](#)
- **Rootkity:** Počet detegovaných [rootkitov](#)
 - **Informácie záznamového protokolu prehľadávania:** Informácie súvisiace s priebehom a výsledkami prehľadávania (obvyčajne 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.
- **Naspät:** Prepne naspät na hlavné dialógové okno [rozhrania prehľadávania](#)

[programom AVG](#)

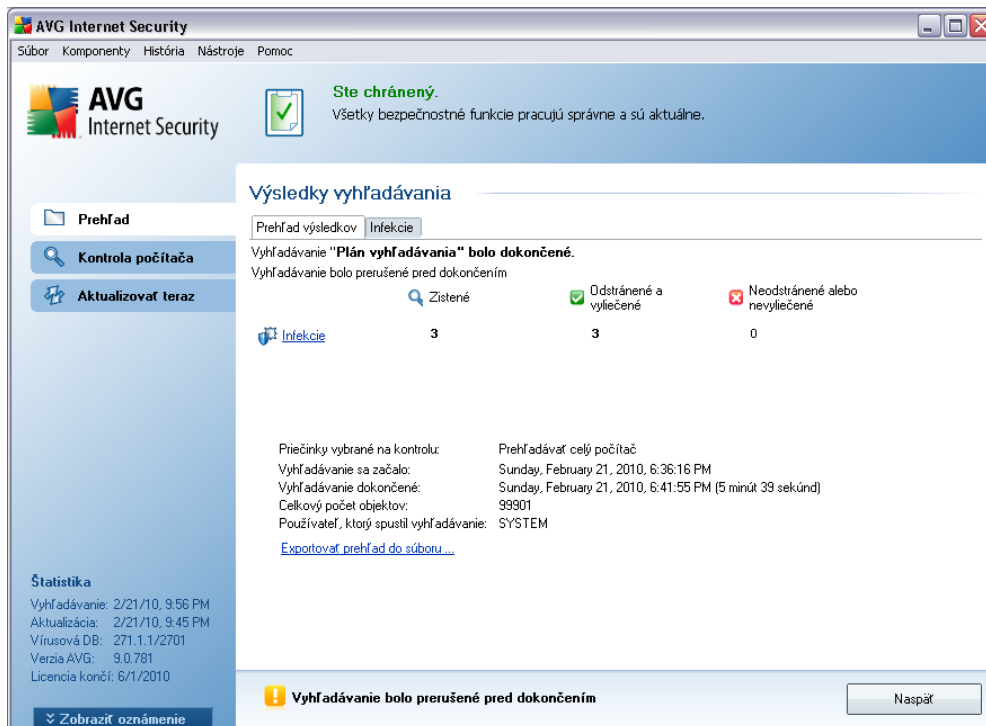
12.7. Podrobnosti výsledkov vyhľadávania

Ak v dialógovom okne **Prehľad výsledkov prehľadávania** zvolíte konkrétne prehľadávanie, potom môžete kliknutím na tlačidlo **Zobrazit podrobnosti** otvoriť dialógové okno **Výsledky prehľadávania** s podrobnými informáciami o priebehu a výsledkoch zvoleného prehľadávania.

Toto dialógové okno je rozdelené na niekoľko kariet:

- **Prehľad výsledkov:** Táto karta sa tu nachádza vždy a poskytuje štatistické informácie o priebehu prehľadávania.
- **Infekcie:** Táto karta sa tu nachádza len vtedy, ak sa počas prehľadávania detegovala [vírusová infekcia](#)
- **Spyware:** Táto karta sa tu nachádza len vtedy, ak sa počas prehľadávania detegoval [spyware](#)
- **Upozornenia:** Táto karta sa tu nachádza len vtedy, ak sa počas prehľadávania detegovali súbory cookies.
- **Informácie:** Táto karta sa tu nachádza len vtedy, ak sa detegovali niektoré potenciálne hrozby, ktoré sa však nedajú zaradiť do žiadnej z vyššie uvedených kategórií; na karte sa potom zobrazí upozornenie súvisiace s nálezom. Nachádzajú sa tu aj informácie o objektoch, ktoré nie je možné prehľadať (napr. heslom chránené archívy).

12.7.1. Karta Prehľad výsledkov



V karte **Výsledky vyhľadávania** môžete nájsť podobnú štatistiku s informáciami o:

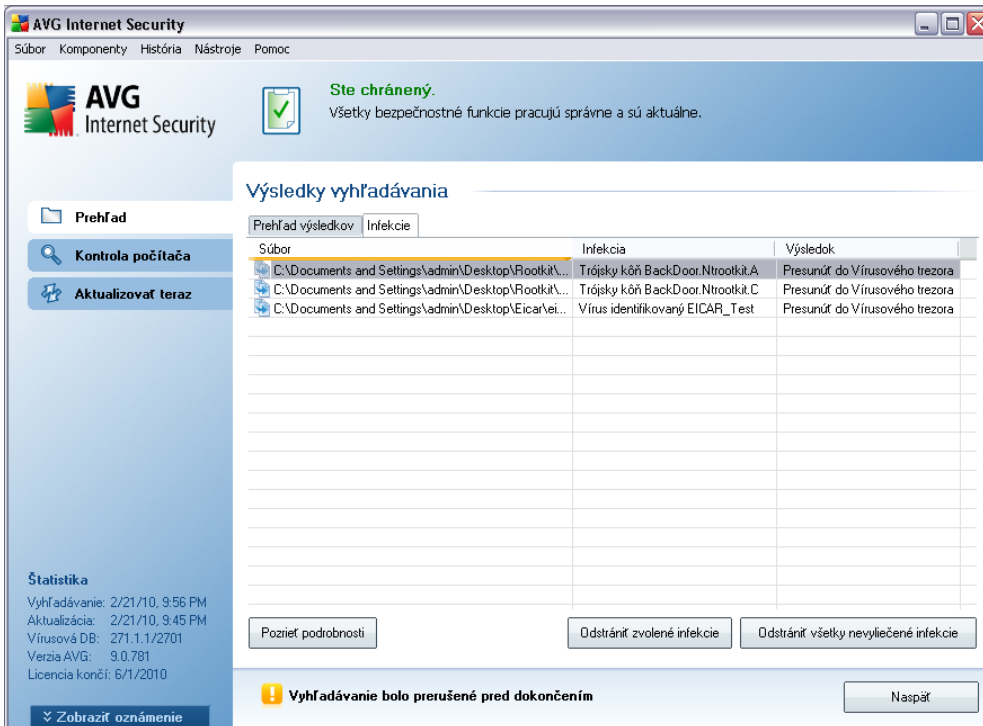
- detekovaných [vírusových infekciách](#) / [spyware](#)
- odstránených [vírusových infekciách](#) / [spyware](#)
- počte [vírusových infekcií](#) / [spyware](#), ktoré sa nedajú odstrániť alebo vyliečiť

Okrem toho nájdete informácie o dátume a presnom čase spustenia vyhľadávania, o celkovej počte prehľadaných 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 prehľadovania** len v prípade, ak sa počas prehľadovania zistila prítomnosť [vírusovej infekcie](#). Táto karta je rozdelená na tri časti, na ktorých sa nachádzajú nasledovné informácie:

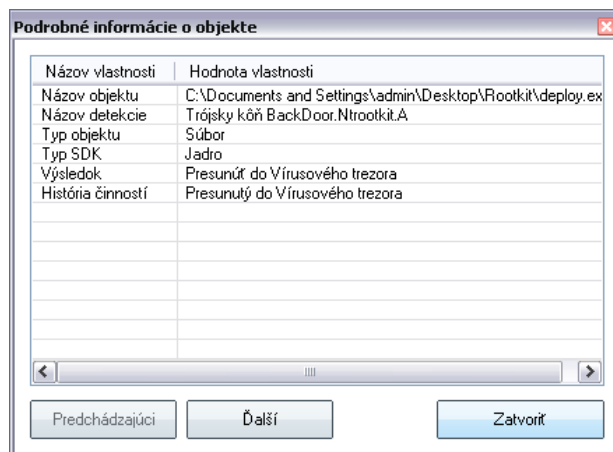
- **Súbor:** Úplná cesta k pôvodnému umiestneniu infikovaného objektu.
- **Infekcie:** Názov detegovaného [vírusu](#) (podrobnosti o konkrétnych vírusoch sa nachádzajú online vo [Vírusovej encyklopédii](#)).
- **Výsledok:** Definuje aktuálny stav infikovaného objektu, ktorý sa zistil počas prehľadovania:
 - **Infikovaný:** Infikovaný objekt bol detegovaný a ponechaný na pôvodnom mieste (napríklad ak ste [vypli možnosť automatického liečenia v nastavení konkrétneho prehľadovania](#)).
 - **Vyliečený:** Infikovaný objekt sa automaticky vyliečil a nechal na pôvodnom mieste.

- **Premiestnený do Vírusového trezora:** Infikovaný objekt sa premiestnil do karantény [Vírusového trezora](#)
- **Vymazaný:** Infikovaný objekt bol vymazaný.
- **Pridaný do výnimiek PNP:** Zistený program bol označený ako výnimka a pridaný do zoznamu výnimiek PNP (*nastavuje sa v dialógovom okne [Výnimky PNP](#) v rozšírených nastaveniach*)
- **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.
- **Požaduje 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 výsledkoch prehľadávania:**



V tomto dialógovom okne sa nachádzajú informácie o umiestnení detegovaného infikovaného objektu (**Názov vlastnosti**). Tlačidlá

Predchádzajúce/Nasledujúce použite na zobrazenie informácií o konkrétnych nálezoch. Tlačidlo **Zatvoriť** sa používa na zatvorenie tohto dialógového okna.

- **Odstrániť zvolené infekcie:** Toto tlačidlo sa používa na premiestnenie zvoleného nálezu do [Vírusového trezora](#)
- **Odstrániť všetky nevylicené infekcie:** Toto tlačidlo vymaže všetky nálezy, ktoré sa nedajú vylicit alebo premiestniť do [Vírusového trezora](#)
- **Zatvoriť výsledky:** Zatvorí prehľad a otvorí pôvodné dialógové okno [Prehľad výsledkov prehľadávania](#)

12.7.3. Karta Spyware

Karta **Spyware** sa nachádza v dialógovom okne **Výsledky prehľadávania**, len ak sa počas prehľadávania detegoval [spyware](#). Táto karta je rozdelená na tri časti, na ktorých sa nachádzajú nasledovné informácie:

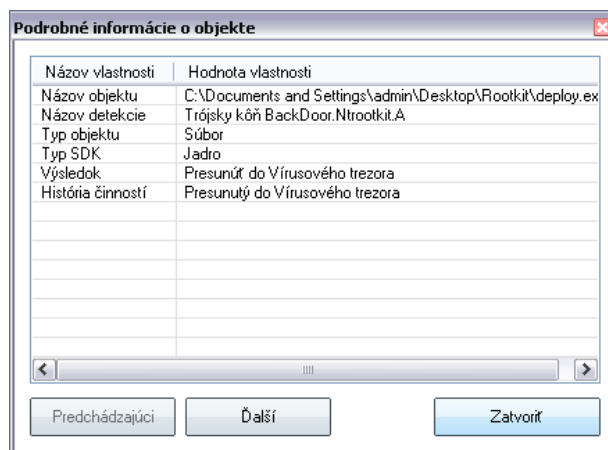
- **Súbor:** Úplná cesta k pôvodnému umiestneniu infikovaného objektu.
- **Infekcie:** Názov detegovaného [spywaru](#) (*podrobnosti o konkrétnych vírusoch sa nachádzajú v online [Vírusovej encyklopédii](#)*).
- **Výsledok:** Definuje aktuálny stav infikovaného objektu, ktorý sa zistil počas prehľadávania:
 - **Infikovaný:** Detegovaný infikovaný objekt bol ponechaný na pôvodnom mieste (napríklad ak ste [vypli možnosť automatického liečenia](#) v nastavení konkrétneho prehľadávania).
 - **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 bol vymazaný.
 - **Pridaný do výnimiek PNP:** Nález bol označený ako výnimka a pridaný do zoznamu výnimiek PNP (*nastavuje sa v dialógovom okne [Výnimky PNP](#) v rozšírených nastaveniach*).
 - **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.
- **Požaduje 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 výsledkoch prehľadovania:**

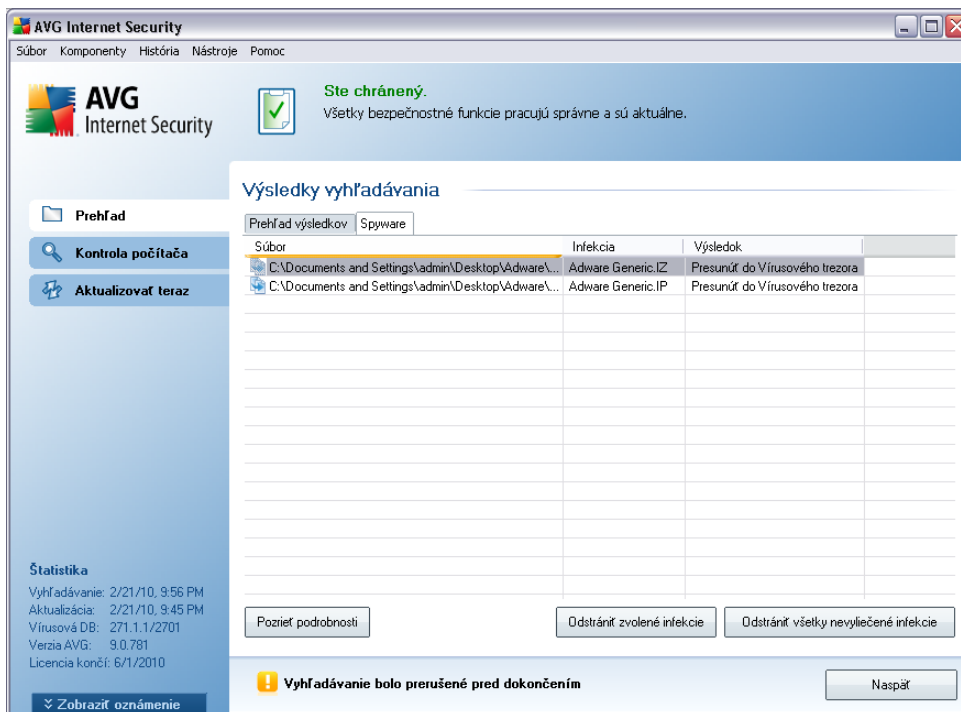


V tomto dialógovom okne sa nachádzajú informácie o umiestnení detegovaného infikovaného objektu (**Názov vlastnosti**). Tlačidlá **Predchádzajúce/Nasledujúce** použité na zobrazenie informácií o konkrétnych nálezoch. Pomocou tlačidla **Zatvoriť** zatvorte toto dialógové okno.

- **Odstrániť zvolené infekcie:** Toto tlačidlo sa používa na premiestnenie zvoleného nálezu do [Vírusového trezora](#)
- **Odstrániť všetky nevylicené infekcie:** Toto tlačidlo vymaže všetky nálezy, ktoré sa nedajú vylicit alebo premiestniť do [Vírusového trezora](#)
- **Zatvoriť výsledky:** Zatvorí prehľad a otvorí pôvodné dialógové okno [Prehľad výsledkov prehľadovania](#).

12.7.4. Karta Upozornenia

Karta **Varovania** zobrazuje informácie o "podozrivých" objektoch (*obycajne súboroch*) detekovaných počas vyhľadávania. Po detekcii **Rezidentným štítom** sa tieto súbory zablokujú, aby k nim nebol možný prístup. Typické príklady týchto druhov nálezov sú: skryté súbory, cookies, podozrivé klúče registrov, heslom chránené dokumenty alebo archívy, atd. 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 sa zobrazujú len upozornenia týkajúce sa prípadov zistených počas testu AVG, nie je potrebné prijať žiadne opatrenie.



Toto je stručný popis najbežnejších príkladov takýchto objektov:

- **Skryté súbory** - skryté súbory sú štandardne neviditeľné v operacnom systéme Windows a niektoré vírusy alebo iné hrozby sa môžu pokúsiť vyhnúť detegovaniu tým, že svoje súbory uložia s týmto atribútom. Ak program AVG nájde skrytý súbor a máte podozrenie, že je škodlivý, môžete ho premiestniť do **Vírusového trezora AVG**.
- **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 klúče registrov** - niektorý škodlivý softvér ukladá svoje informácie do registrov operacného systému Windows, aby sa zabezpečilo jeho načítanie pri spustení operacného systému, alebo rozšíril jeho vplyv v operacnom systéme.

12.7.5. Karta Rootkity

Na karte **Rootkity** sa nachádzajú informácie o rootkitoch zistených počas prehľadávania, ak ste spustili **prehľadávanie súčastou Anti-Rootkit**, alebo ručne pridali možnosť prehľadávania súčastou Anti-Rootkit do **prehľadávania celého počítača** (táto možnosť je štandardne vypnutá).

Rootkit je program, ktorého cieľom je zmocniť sa základnej kontroly nad počítačom bez súhlasu vlastníka počítača a jeho právoplatných správcov. Prístup k hardvéru sa väčšinou nepožaduje, pretože rootkit je určený na to, aby sa zmocnil kontroly nad operacným systémom spusteným na hardvéri. Rootkity sa obvyčajne snažia zakrývať svoju prítomnosť v systéme formou nižšej verzie alebo únikom pred štandardnými bezpečnostnými mechanizmami operacného systému. Často ide aj o Trójske kone, ktoré mýlia používateľov a tí si myslia, že je spúšťanie systému bezpečné. Metódy používané na splnenie tejto úlohy zahŕňajú utajenie bežiacich procesov pred sledovacími programami alebo skrývanie súborov alebo systémových údajov pred operacným 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. Programom AVG dokáže pri vyhľadávaní zistiť prítomnosť súborov, ktoré nemusia byť infikované, ale sú podozrivé. Informácia o týchto súboroch sa zobrazí 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 komprimacných 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 heslom** - Program AVG (a v podstate ani žiaden program na kontrolu výskytu škodlivého kódu) nedokáže prehľadávať súbory chránené heslom.
- **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 viditeľná pod operačným systémom Windows a AVG upozorní na tieto súbory, aby zabránil ich náhodnému spusteniu.
- **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 AVG upozorní na túto nezrovnalosť. V niektorých prípadoch vírusy používajú názvy štandardných systémových procesov, aby ich prítomnosť v systéme bola menej nápadná.
- **Zamknutý súbor** - Identifikovaný súbor je zamknutý, a preto ho AVG 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/infikovaných objektov detegovaných počas testov vykonaných programom AVG. Ak sa počas prehľadávania deteguje podozrivý objekt a aplikácia AVG ho nedokáže automaticky vyličiť, program sa vás opýta, čo sa má s podozrivým objektom urobiť. Odporúčame vám premiestniť objekt do **Vírusového trezora** pre prípad, ak ste s ním chceli pracovať v budúcnosti. Hlavným účelom **Vírusového trezora** je uložiť všetky vymazané súbory počas určitej doby, aby ste mali čas uistiť sa, že súbor naozaj nepotrebuje. 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:** informácie o type infekcie (na základe úrovne infikovateľnosti – všetky uvedené objekty môžu byť pozitívne alebo potenciálne infikované).
- **Názov vírusu:** Uvádza názov detegovanej infekcie podľa [Vírusovej encyklopédie](#) (online)
- **Cesta k súboru:** Úplná cesta k pôvodnému umiestneniu detegovaného infikovaného súboru.
- **Pôvodný názov objektu:** Všetky detegované objekty uvedené v tabulke boli označené štandardným názvom pridelených programom AVG počas procesu prehľadávania. 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 detegovaný a premiestnený do **Vírusového trezora**

Ovládacie tlačidlá

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

- **Obnovit:** Odstráni infikovaný súbor naspäť do jeho pôvodného umiestnenia na disku.
- **Obnovit ako:** Ak sa rozhodnete premiestniť detegovaný infikovaný objekt z **Vírusového trezora** do zvoleného priečinka, použijete toto tlačidlo. Podozrivý a detegovaný objekt sa uloží pod pôvodným názvom. Ak pôvodný názov nie je známy, použije sa štandardný názov.
- **Podrobnosti:** Toto tlačidlo sa používa len v súvislosti s hrozbami detegovanými súčasťou **Identity Protection**. Po kliknutí sa zobrazí súhrnný prehľad informácií o hrozbe (ktoré súbory/procesy boli ovplyvnené, vlastnosti procesov atd.). Upozorňujeme, že pre všetky ostatné položky (okrem detegovaných 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 súborov z Vírusového trezora sa tieto súbory úplne a nenávratne odstránia z disku (nepremiestnia sa do Koša).

13. Aktualizácie AVG

Zachovanie aktuálnosti programu AVG je dôležité z dôvodu čo najskoršieho detegovania novo objavených vírusov.

Pocas [procesu inštalácie programu AVG](#) môžete nastaviť, ako často si želáte aktualizovať nainštalovaný program AVG. Ponúkané možnosti sú **Každé 4 hodiny** a **Každý den** (pozri dialógové okno [Naplánovanie pravidelného prehladávanía aktualizácie](#)). Keďže aktualizácie pre programy AVG sa nevydávajú podľa pevne stanoveného harmonogramu, ale skôr v reakcii na množstvo a závažnosť nových hrozieb, odporúčame robiť aktualizáciu najmenej raz za den. Kontrolovaním nových aktualizácií každé 4 hodiny sa zaručí aktuálnosť programu **AVG 9 Anti-Virus plus Firewall** aj počas dňa.

13.1. Úrovne aktualizácie

AVG poskytuje dve úrovne aktualizácií, z ktorých si môžete vybrať:

- **Aktualizácia definícií** obsahuje zmeny potrebné na dosiahnutie spoľahlivej ochrany pred vírusmi. Obvyčajne 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](#) môžete nastaviť, ktorú úroveň priority chcete prevziať a použiť.

Poznámka: Ak sa čas naplánovanej aktualizácie programu náhodou prekrýva s naplánovaným prehladávaním, proces aktualizácie má vyššiu prioritu a prehladávanie sa preruší.

13.2. Typy aktualizácie

Rozlišujeme dva typy aktualizácie:

- **Aktualizácia na požiadanie** je okamžitá aktualizácia programu AVG, ktorú je možné spustiť vždy, keď je to potrebné.
- **Naplánovaná aktualizácia:** Program AVG zároveň umožňuje [vopred nastaviť plán aktualizácie](#). Plánovaná aktualizácia sa potom bude vykonávať pravidelne podľa konfigurácie nastavenia. Keď sa na uvedenom mieste nachádzajú nové aktualizčné súbory, stiahnu sa buď priamo z Internetu alebo zo sieťového adresára. Keď nie sú dostupné žiadne nové aktualizácie, nič sa nestane.

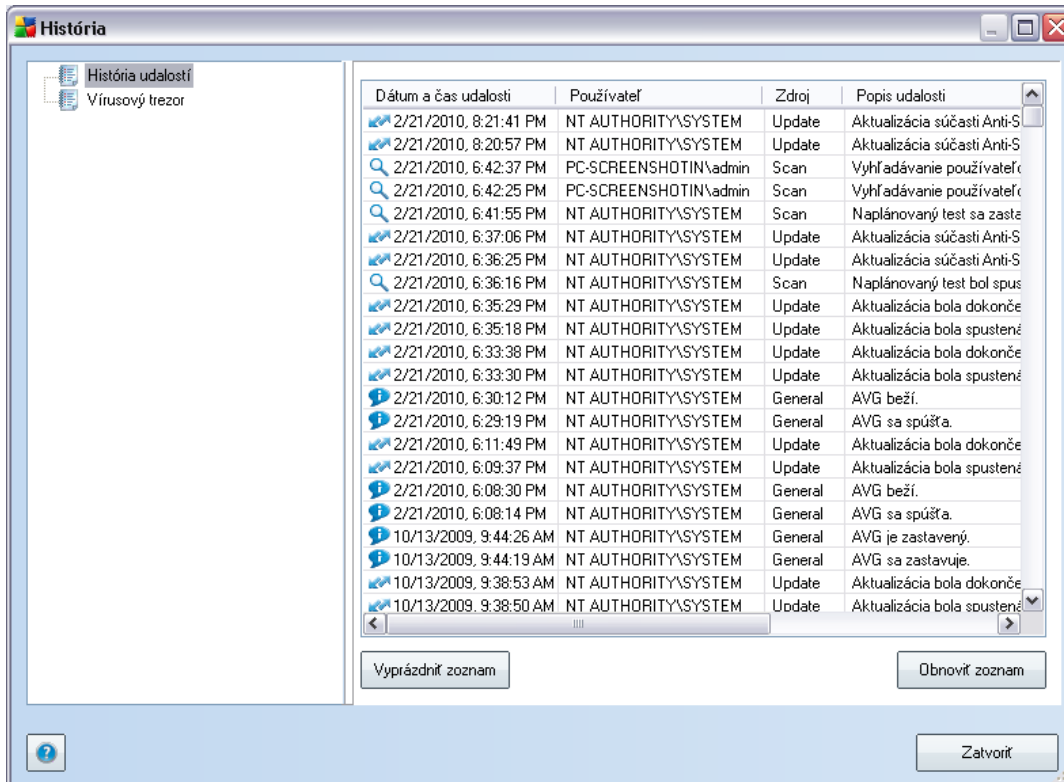
13.3. Proces aktualizácie

Proces aktualizácie môžete spustiť kedykoľvek podľa potreby kliknutím na odkaz **Aktualizovať teraz*****. Tento odkaz sa vždy nachádza v každom dialógovom okne [používateľského rozhrania AVG](#). Napriek tomu vám však odporúčame robiť aktualizácie pravidelne podľa plánu aktualizácie, ktorý sa nastavuje v súčasti [Update Manager](#).

Po spustení aktualizácie program AVG najskôr skontroluje, či sú k dispozícii nové aktualizacné súbory. Ak nájde nové aktualizácie, začne ich preberať a spustí samotný proces aktualizácie. Počas procesu aktualizácie sa otvorí rozhranie **aktualizácie**, ktoré informuje o priebehu procesu v grafickej podobe, a v ktorom sa zároveň nachádza prehľad súvisiacich štatistických parametrov (*veľkosť aktualizacného súboru, prijaté dáta, rýchlosť preberania, uplynutý čas...*).

Poznámka: *Pred spustením aktualizácie programu AVG sa vytvorí bod obnovenia systému. Ak proces aktualizácie zlyhá a operacný systém spadne, tento bod obnovenia umožní obnoviť stav operacného systému s pôvodnou konfiguráciou. Prístup k tejto možnosti je cez ponuku Štart/Programy/Príslušenstvo/Systémové nástroje/Obnovenie systému. Zmeny týchto nastavení odporúčame robiť len skúseným používateľom!*

14. História udalostí



Dialógové okno **História udalostí** sa otvára pomocou [hlavnej ponuky programu](#) kliknutím na položku **História/Záznamový protokol histórie udalostí**. V tomto dialógovom okne sa nachádza prehľad významných udalostí, ktoré sa vyskytli počas chodu programu **AVG 9 Anti-Virus plus Firewall**. **História udalostí** zaznamenáva nasledujúce typy udalostí:

- Informácie o aktualizáciách aplikácie AVG
- Spustenie, ukončenie a zastavenie prehľadávania (vrátane automaticky vykonávaných testov).
- Udaloosti spojené s detegovaním vírusov (súčasťou [Rezidentný štít](#) alebo počas [prehľadávania](#)), vrátane miesta výskytu).
- Dalšie dôležité udalosti.

Ovládacie tlačidlá

- **Vyprázdniť zoznam:** Vymaže všetky položky zo zoznamu udalostí.
- **Obnoviť zoznam:** Aktualizuje všetky položky v zozname udalostí.



15. Často kladené otázky a technická podpora

Ak narazíte na problémy s programom AVG, či už obchodné alebo technické, nahliadnite do časti **FAQ** na webových stránkach AVG (<http://www.avg.com/>).

Ak ani tu nenájdete pomoc, kontaktujte oddelenie technickej pomoci e-mailom. Použite, prosím, kontaktný formulár dostupný v systémovej ponuke cez **Pomoc/Získať pomoc online**.