AVG 8.5 Email Server Edice

Uživatelský manuál

Verze dokumentace 85.4 (30.4.2009)

Obsah

1. Úvod

Tento uživatelský manuál je kompletní dokumentací programu ***AVG 8.5 Email Server***.

AVG 8.5 Email Server je jedním z produktů nové řady oceňovaného bezpečnostního software AVG, jež byl navržen pro klid vaší duše a stoprocentní bezpečnost vašeho PC. Stejně jako všechny produkty nové řady AVG byl i ***AVG 8.5 Email Server*** kompletně a od základů přestavěn tak, aby nadále dostál své pověsti uznávaného bezpečnostního programu a současně nabídl svým uživatelům zcela nové, efektivnější a uživatelsky přívětivé rozhraní.

Nový ***AVG 8.5 Email Server*** přináší moderní grafické rozhraní v kombinaci s agresivnějším a rychlejším testováním. Pro větší pohodlí přináší více procesů v plně automatickém režimu a nabízí nové 'inteligentní' uživatelské možnosti, které se přesně přizpůsobí vašim potřebám.

2. Podmínky instalace

2.1. Podporované operační systémy

AVG 8.5 Email Server je určen k ochraně e-mail serverů s těmito operačními systémy:

- Windows 2008 Server (x64 a x86)
- Windows 2003 Server (x86, x64 a Itanium) SP1
- Windows 2000 Server SP4 + Update Rollup 1

(a všechny případné vyšší servisní balíky pro jednotlivé operační systémy)

2.2. Podporované e-mail servery

Podporovány jsou následující e-mail servery:

- ***MS Exchange Server 2000***

  Poznámka: *Pro Exchange 2000 Server je nutné před použitím testovacího jádra AVG nejprve instalovat servisní balík 1 (nebo vyšší); AVG pro Exchange 2000/2003 Server používá rozhraní aplikace VSAPI 2.0 (nebo 2.5 pro Exchange 2003 Server), jež je obsaženo v tomto servisním balíku.*

- ***MS Exchange Server 2003***
- ***MS Exchange Server 2007***
- ***AVG pro Kerio MailServer*** – verze 5.x/6.x a vyšší

2.3. Minimální hardwarové požadavky

Minimální hardwarové požadavky pro ***AVG 8.5 Email Server*** jsou tyto:

- Intel Pentium CPU 1,2 GHz
- 70 MB volného místa na pevném disku (z instalačních důvodů)
- 256 MB RAM paměti

2.4. Odinstalujte předchozí verze

Máte-li nainstalovanou starší verzi ***AVG Email Serveru***, je nutné ji před zahájením instalace ***AVG 8.5 Email Server*** odinstalovat. Odinstalaci je třeba provést ručně pomocí standardních funkcí Windows:

- V nabídce ***Start/Nastavení/Ovládací panel/Přidat nebo odebrat programy*** zvolte příslušný program.

  Poznámka*: Věnujte zvýšenou pozornost volbě správného AVG programu ze seznamu instalovaných programů! Nejprve musíte odinstalovat AVG Email Server Edici a teprve poté AVG File Server Edici.*

- Po odinstalaci ***AVG Email Server Edice*** přistoupíte k odinstalaci předchozí verze ***AVG File Server Edice***. Tuto akci provedete snadno z nabídky ***Start/ Programy/AVG/Odinstalovat AVG.***

2.5. MS Exchange Service pack

Jelikož ***AVG pro MS Exchange 2000/2003 Server*** užívá virové testovací rozhraní VSAPI 2.0/2.5, je pro instalaci ***MS Exchange 2000 Serveru*** nutné, abyste měli na svém systému aplikován servisní balík 1 (nebo vyšší). Nejnovější servisní balík pro ***MS Exchange 2000 Server*** najdete na adrese:

http://www.microsoft.com/technet/prodtechnol/exchange/downloads/2000/sp3/default.mspx

Pro instalaci ***MS Exchange 2003 Serveru*** není nutná instalace žádných dodatečných balíků, ale v každém případě doporučujeme, abyste se snažili udržovat svůj systém v co možná nejaktuálnějším stavu a a průběžně instalovali nové servisní balíky a záplaty, aby bylo dosaženo nejvyšší možné úrovně bezpečnosti.

Servisní balík pro ***MS Exchange 2003 Server*** (instalace je volitelná) najdete na adrese:

http://www.microsoft.com/exchange/evaluation/sp2/overview.mspx

Při zahájení instalace budou prověřeny všechny verze systémových knihoven. Bude-li nutné doinstalovat novější knihovny, instalátor označí zastaralé knihovny koncovkou *.delete*. Takto označené knihovny pak budou odstraněny při restartu systému.

3. Instalační proces AVG

Pro instalaci AVG na váš počítač potřebujete aktuální instalační soubor. Instalační soubor najdete na CD, které bylo součástí zakoupeného balení AVG, ale tento soubor může již být zastaralý.

Doporučujeme vám proto navštívit web AVG:

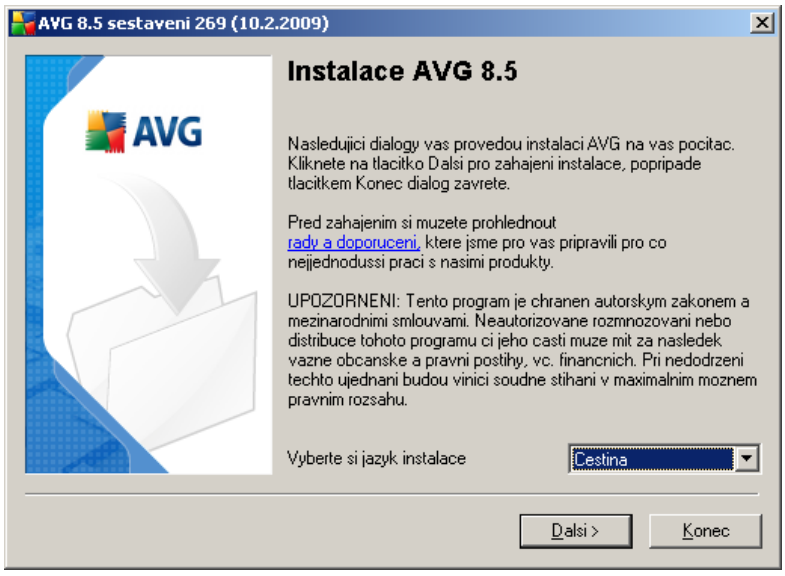
http://www.avg.cz/stahnout?prd=msw

a nejnovější instalační soubor si odtud stáhnout.

Během instalace budete požádáni o své licenční/prodejní číslo. Ujistěte se proto prosím, že jej máte k dispozici. Prodejní číslo najdete na CD v prodejním balení AVG. Pokud jste AVG zakoupili on-line, vaše licenční číslo vám bylo doručeno e-mailem.

Instalace probíhá ve sledu dialogových oken, z nichž každé vysvětluje, co je třeba v konkrétním kroku provést. Popis jednotlivých oken nyní nabízíme:

3.1. Spuštění instalace



Instalační proces je zahájen otevřením dialogu ***Instalace AVG***. V tomto dialogu máte možnost zvolit jazyk, v němž bude instalační proces probíhat. V dolní části okna u položky ***Vyberte si jazyk instalace*** zvolte z rozbalovacího menu jazyk, v němž chcete komunikovat, a volbu potvrďte stiskem tlačítka ***Další***.

Upozornění: *Tato volba se týká pouze instalačního procesu. Nevybíráte tedy jazyk samotného programu AVG, ale pouze jazyk instalačního procesu. Jazyk, v němž bude AVG instalován, můžete zvolit později během instalace!*

3.2. Licenční ujednání

V dialogu ***Licenční ujednání*** najdete plné znění závazné licenční smlouvy AVG. Text si přečtěte a svůj souhlas s licenčním ujednáním potvrďte stiskem tlačítka ***Souhlasím***. Pokud s licenční smlouvou nesouhlasíte a stisknete tlačítko ***Nesouhlasím***, instalace bude okamžitě ukončena.

3.3. Zjišťování stavu

Po potvrzení licenčního ujednání přejdete do dialogu ***Probíhá zjišťování stavu***. Tento dialog nevyžaduje žádný váš zásah; po dobu jeho zobrazení probíhá kontrola stavu vašeho systému před zahájením instalace AVG. Vyčkejte prosím dokončení tohoto procesu a budete automaticky přesměrováni do následujícího dialogu.

3.4. Zvolte operaci

Dialog ***Zvolte typ instalace*** vám dává na výběr mezi ***standardní*** a ***uživatelskou*** instalací.

Většině uživatelů doporučujeme použít ***standardní instalaci***, kdy bude AVG nainstalován zcela automaticky s nastavením definovaným výrobcem. Toho nastavení zaručuje maximální úroveň bezpečnosti a optimální využití zdrojů. Pokud se v budoucnu vyskytne potřeba některé konkrétní nastavení změnit, budete mít vždy možnost editovat konfiguraci AVG přímo v aplikaci.

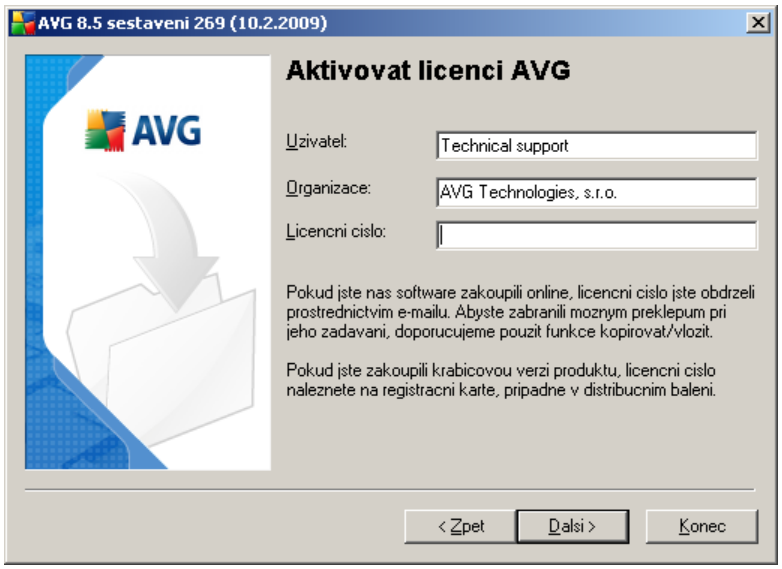
Uživatelská instalace je vhodná pouze pro pokročilé a znalé uživatele. Doporučit ji lze v případě, že máte skutečný důvod instalovat AVG s nestandardním nastavením tak, aby vyhovovalo specifickým požadavkům vašeho systému.

3.5. Aktivovat licenci AVG

V dialogu ***Aktivovat licenci AVG*** je třeba vyplnit vaše registrační údaje.

Vepište své jméno (pole ***Uživatel***) a název vaší organizace (pole ***Organizace***). Do položky ***Licenční/Prodejní číslo*** pak zadejte své licenční číslo. Toto číslo najdete buďto na registrační kartě v krabicovém balení AVG, anebo v potvrzovacím emailu, který jste obdrželi při zakoupení AVG on-line. Licenční číslo musí být zadáno naprosto přesně ve tvaru, jak je uvedeno, proto prosím věnujte velkou pozornost

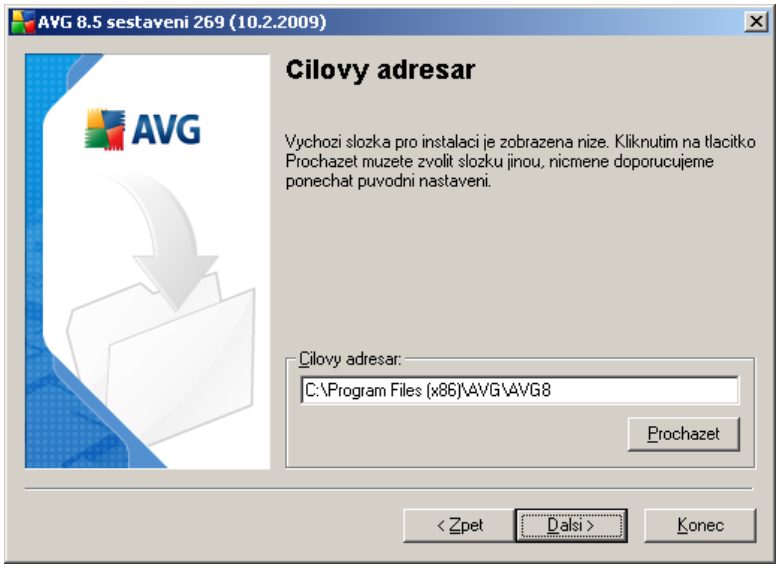
jeho přepisu. Pokud máte číslo k dispozici v digitální formě, doporučujeme jej do příslušného pole zkopírovat (metodou kopírovat a vložit).



V instalaci pokračujte stiskem tlačítka ***Další***.

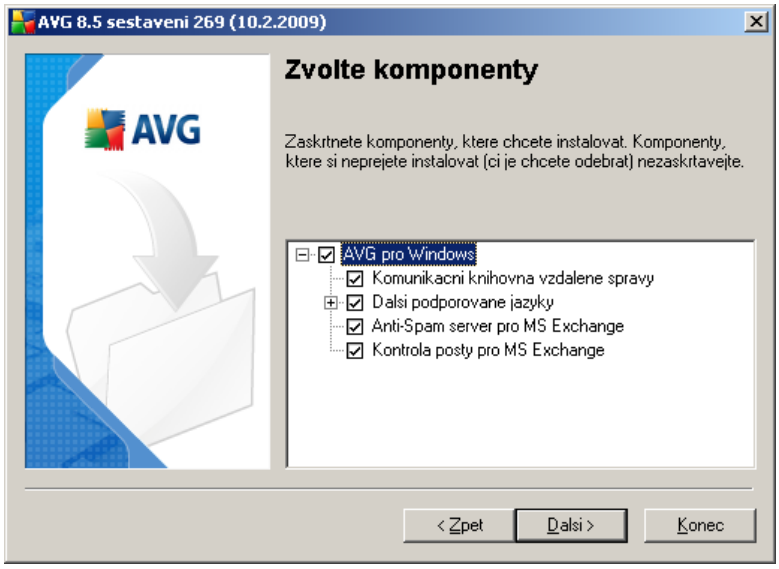
Pokud jste v předchozím kroku zvolili standardní instalaci, přejdete rovnou do dialogu ***Potvrzení instalace***. Při volbě uživatelské instalace budete pokračovat dialogem ***Cílový adresář***.

3.6. Uživatelská instalace - Cílový adresář



Dialog ***Cílový adresář*** vám dává možnost určit, kam má být program AVG instalován. Ve výchozím nastavení bude program instalován do adresáře programových souborů umístěném typicky na disku C:. Pokud si přejete toto umístění změnit, pomocí tlačítka ***Procházet*** zobrazte strukturu vašeho disku a zvolte adresář, kam má být AVG instalován. Svou volbu potvrďte stiskem tlačítka ***Další***.

3.7. Uživatelská instalace - Zvolte komponenty



V dialogu ***Zvolte komponenty*** je zobrazen přehled komponent AVG, které můžete nainstalovat. Pokud vám výchozí nastavení nevyhovuje, máte možnost jednotlivé komponenty odebrat/přidat.

Volit můžete pouze z těch komponent, které jsou zahrnuty ve vámi zakoupené licenci AVG. Pouze tyto komponenty vám také budou v dialogu nabídnuty!

- ***Komunikační knihovna vzdálené správy*** - pokud budete chtít tuto instalaci spravovat vzdáleně, zaškrtněte tuto volbu.

  Poznámka: *Ne všechny e-mail servery lze spravovat prostřednictvím Vzdálené správy!*

- ***Další podporované jazyky*** - zvolte si jazyky uživatelského rozhraní, které chcete nainstalovat.

- ***Anti-Spam Server (pro e-mail server)*** - zvolte, pokud si přejete nainstalovat Anti-Spam ochranu pro váš e-mail server.

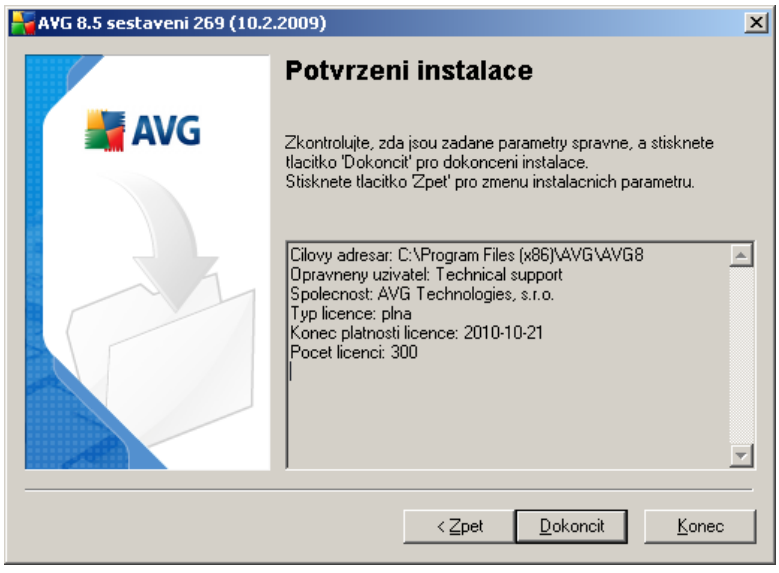
- ***Kontrola pošty (pro e-mail server)*** - zvolte, pokud si přejete nainstalovat anti-virus/anti-malware ochranu pro váš e-mail server.

Pokračujte stiskem tlačítka ***Další***.

3.8. Uživatelská instalace - DataCenter

Pokud jste v průběhu volby komponent vybrali ***Komunikační knihovnu vzdálené správy***, můžete v tomto dialogu zadat připojovací řetězec pro spojení s vaším AVG DataCenter.

3.9. Potvrzení instalace



Dialog ***Potvrzení instalace*** shrnuje všechny dosud zadané parametry instalace. Prosím, zkontrolujte, že vše je zadáno správně a podle vašich požadavků. Pokud je tomu tak, pokračujte stiskem tlačítka ***Dokončit***. V opačném případě máte možnost se pomocí tlačítka ***Zpět*** vrátit do příslušného dialogu a zadání opravit.

3.10.Probíhá instalace

Potvrzením předchozího dialogu dojde ke spuštění samotného procesu instalace, jehož průběh můžete sledovat v dialogu ***Probíhá instalace***. Tento dialog je také pouze informativní a nevyžaduje žádný váš zásah:

Počkejte prosím na dokončení instalace, poté budete přesměrováni do následujícího dialogu ***Instalace dokončena***.

3.11.Instalace dokončena

Dialog ***Instalace dokončena*** je posledním krokem instalačního procesu AVG. Nyní je AVG instalován na vašem počítači a plně funkční. Program běží ve výchozím nastavení na pozadí a nevyžaduje vaši pozornost.

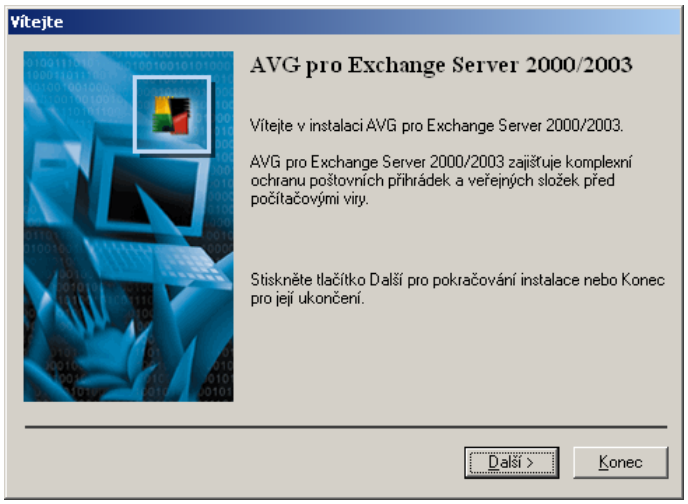
V závislosti na nainstalovaném e-mail serveru se objeví další instalační dialog (viz níže).

4. AVG E-mail servery - instalace

Jakmile dokončíte úspěšně instalaci AVG, spustí se instalace zvoleného e-mail serveru:

Poznámka: *Mechanismus antivirové ochrany je pro Kerio MailServer integrován přímo v aplikaci Kerio. Více informací naleznete v kapitole AVG pro Kerio Mailserver.*

4.1. Spuštění instalace



Instalační proces zahájíte v uvítacím dialogu tlačítkem ***Další***.

4.2. Licenční ujednání

V dialogu ***Licenční ujednání*** najdete plné znění závazné licenční smlouvy AVG. Text si přečtěte a svůj souhlas s licenčním ujednáním potvrďte stiskem tlačítka ***Souhlasím***. Pokud s licenční smlouvou nesouhlasíte a stisknete tlačítko ***Nesouhlasím***, instalace bude okamžitě ukončena.

4.3. Cílový adresář

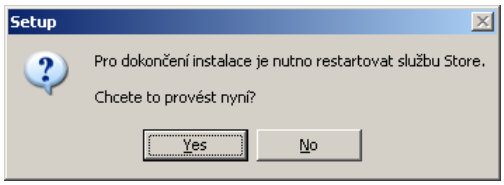
V dalším dialogu budete vyzváni, abyste zvolili cílový adresář. Stiskem tlačítka ***Procházet*** otevřete stromovou strukturu vašeho počítače a zvolte nové umístění cílového adresáře, pokud k tomu máte důvod. Jestliže skutečný důvod nemáte, doporučujeme ponechat výchozí nastavení. Pokračujte stiskem tlačítka ***Další***.

4.4. Kopírování souborů

V dalším dialogu setupu budete vyzváni, abyste před dokončením instalace spustili kopírování instalačních souborů. Potvrďte tento krok stiskem tlačítka ***Další***.

4.5. Restartování služby Store

Během instalace nebo po ukončení dialogu setupu budete vyzváni k restartu služby ***Exchange Message Store*** v ***MS Exchange Serveru***:

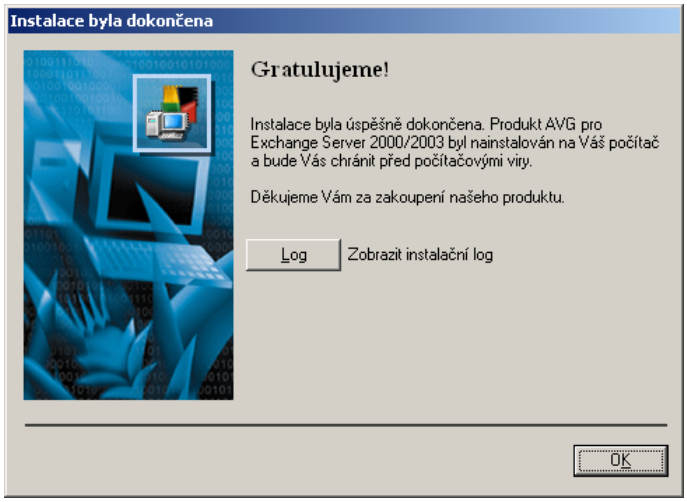


Stiskem tlačítka ***Yes*** tuto službu restartujte spolu se všemi obsaženými komponentami ***AVG pro MS Exchange***. Pak můžete produkt začít používat.

Poznámka: *Restart služby Exchange Message Store způsobí, že server bude po nějakou dobu nedostupný. Před restartem je tedy vhodné informovat všechny uživatele serveru, protože všichni uživatelé aktuálně připojení k serveru budou automaticky odpojeni.*

4.6. Instalace dokončena

Jakmile instalační průvodce zkopíruje všechny potřebné soubory na váš pevný disk, instalace bude dokončena.



Stiskem tlačítka ***Log*** můžete otevřít instalační protokol.

Protokol instalace si můžete prohlédnout také kdykoliv později - najdete jej jako soubor *setup.log* v dočasném systémovém adresáři.

Stiskem tlačítka ***OK*** v dialogu Instalace dokončena zavřete aktuální okno a ukončíte instalaci.

Po dokončení instalace se automaticky spustí ***Průvodce prvním spuštěním AVG*** a provede vás procesem konfigurace. Je samozřejmě možné nastavit požadovanou konfiguraci jednotlivých komponent AVG později, ale doporučujeme využít nabídky průvodce – tak nastavíte všechny základní parametry snadno, správně a k plné funkčnosti aplikace. Postupujte podle kroků popsaných v jednotlivých dialozích průvodce.

Pro nastavení ochrany pro váš e-mail server zvolte odpovídající kapitolu:

- ***AVG pro MS Exchange Server 2007***
- ***AVG pro MS Exchange Server 2000/2003***
- ***AVG pro Kerio MailServer***

5. AVG pro MS Exchange Server 2007

5.1. Konfigurace

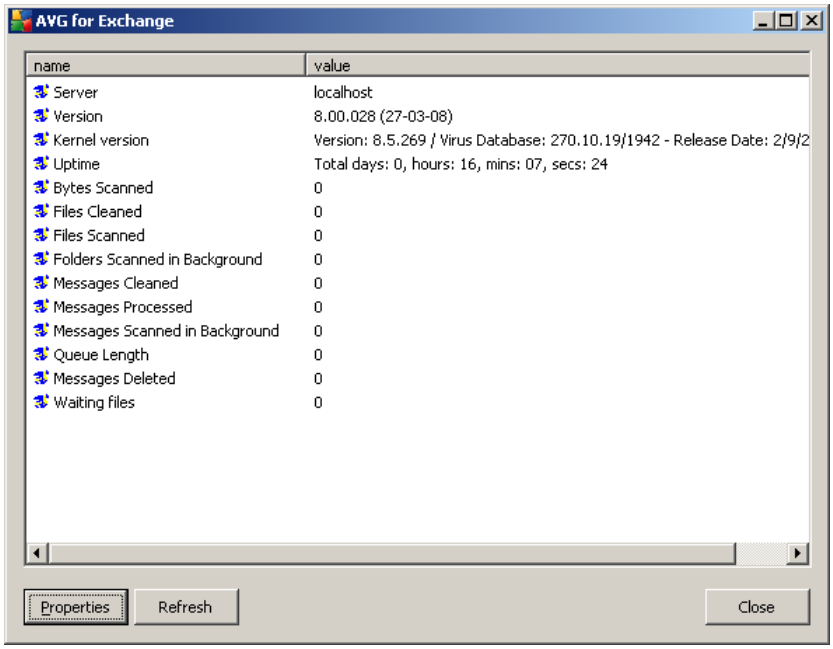
Po restartu služby ***Exchange Server Store*** a při instalovaném ***AVG pro MS Exchange Server*** už není zapotřebí žádné další konfigurace a můžete produkt spustit.

5.1.1. Stav

Pro zjištění stavu či konfiguraci AVG E-mail serveru je potřeba nejrpve spustit aplikaci AVG for Exchange administration. Tuto naleznete v instalačním adresáři, kterým je ve výchozím nastavení:

C:\AVG4ES2K

Otevřete tento adresář a spusťte soubor ***avg4es2kadm.exe***. Otevře se nové okno s informacemi o provozu serveru.



Informace zobrazené v tomto okně zahrnují jméno serveru, verzi aplikace, verzi databáze, verzi kernelu a celkovou dobu, po kterou je program spuštěn od

posledního restartu. Dále zde najdete informace o průběhu antivirové ochrany.

AVG pro MS Exchange Server testuje všechny zprávy v databázích soukromých a veřejných adresářů. Pokud detekuje přítomnost viru, napíše ***AVG pro MS Exchange Server*** zprávu do protokolovacího souboru AVG a také do protokolu událostí.

5.1.2. VSAPI 2.0

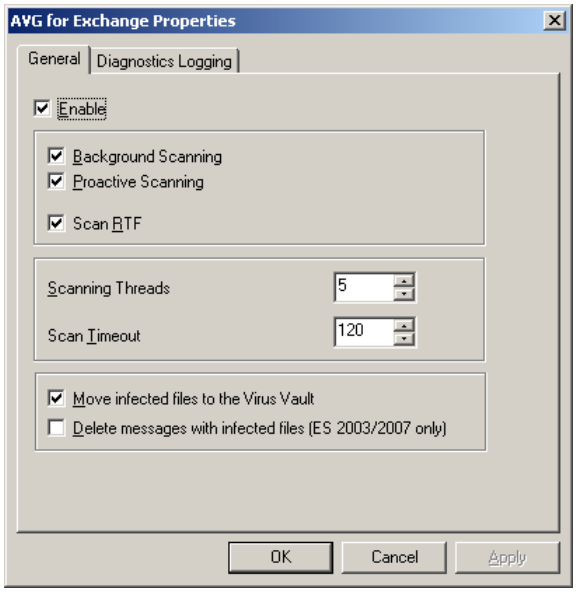
Virové testování ***API 2.5*** (*VSAPI 2.5 jako součást MS Exchange 2003 Serveru*) mazání infikovaných zpráv povoluje. Tuto funkci lze nastavit v konfiguračním dialogu ***AVG pro MS Exchange Server***.

5.1.3. Záložka General

Konfigurační dialog ***AVG for Exchange Server 2007*** lze otevřít kliknutím na tlačítko ***Properties***.

Konfigurační dialog vlastností ***AVG pro Exchange*** je tvořen dvěma záložkami. Na nich můžete editovat parametry testování pošty a protokolování.

Záložka General (Obecné)



Na záložce ***General*** najdete několik přednastavených možností vztahujících se k nastavení testovacích schopností ***AVG pro MS Exchange 2007 Serveru***:

- Položka ***Enable*** – zde lze povolit nebo zakázat kontrolu pošty.

- Položka ***Background Scanning*** – zde můžete povolit nebo zakázat proces kontroly existujícího obsahu databáze na pozadí. Kontrola uložené pošty na pozadí je jedním z prvků rozhraní VSAPI 2.0/2.5. Antivirová kontrola probíhá pro každou databázi na serveru zvlášť; vždy jsou testovány zprávy i přílohy.

  Pro každou databázi je zároveň použito jedno vlákno (*thread*) s nízkou prioritou, což znamená, že ostatní úlohy, jako například ukládání e-mail zpráv do Microsoft Exchange databáze dostane vždy přednost. Kontrola pošty na pozadí je aplikována pro tabulku se složkami v rámci Exchange úložiště. Složka, která již byla na pozadí jednou zkontrolována, bude znovu zkontrolována až při opětovném spuštění rozhraní. Změny jednotlivých zpráv ve složkách jsou zpracovávány proaktivní kontrolou (*proactive scanning*)

- Položka ***Proactive Scanning*** – zde můžete povolit nebo zakázat funkci proaktivní kontroly z VSAPI 2.0/2.5. Tato funkce spočívá v dynamické správě priorit položek v testovací frontě. Objekty s nižší prioritou nejsou testovány, dokud neproběhla kontrola všech položek s vyššími prioritami. Priorita objektu se nicméně může dynamicky měnit - vzrůstá ve chvíli, kdy se uživatel snaží daný objekt použít. Pořadí objektů ve frontě se tedy může dynamicky měnit podle aktivity připojených uživatelů.

- Položka ***Scan RTF*** – zde je možné určit, zda má ***AVG pro Exchange 2007 Server*** provádět také kontrolu těl zpráv ve formátu RTF (neboť tyto mohou také obsahovat viry).

- Položka ***Scanning Threads*** – proces antivirové kontroly je implicitně rozdělen do několika vláken kvůli zvýšení celkového testovacího výkonu zavedením určité úrovně paralelismu. V tomto poli můžete změnit počet těchto vláken. Implicitní hodnota počtu vláken je určena vztahem 2-krát ‘počet_procesorů’ + 1.

- Položka ***Scan Timeout*** – maximální souvislý interval (*v sekundách*), po který může jedno vlákno přistupovat k právě testovanému objektu.

- ***Move infected files to the Virus Vault*** – pokud je tato funkce zapnuta, každá infikovaná zpráva bude přesunuta do karanténního prostředí Virového trezoru.

- ***Delete messages with infected files*** (*ES 2003/2007 only*) – pomocí této položky je možno zapnout nebo vypnout možnost mazání infikovaných zpráv. Pokud je tato možnost zapnuta, takové zprávy jsou automaticky mazány. Pokud tomu tak není, zpráva je doručena adresátovi, infikovaná příloha je

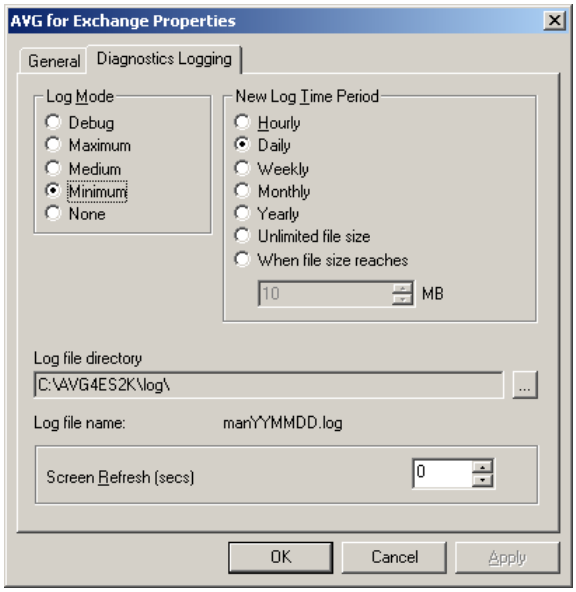
ovšem nahrazena textovým souborem s informací o vymazání viru. Tato možnost je dostupná pouze s pomocí VSAPI 2.5 v Exchange 2003 Serveru.

Všechny prvky na této záložce obecně tvoří uživatelské rozšíření aplikačního rozhraní Microsoft VSAPI 2.0/2.5. Pokud se chcete blíže informovat o tomto rozhraní, následujte tyto odkazy:

- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k – popis principů spolupráce Exchange s antivirovými programy
- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166 – informace o doplňcích ve VSAPI 2.5 v aplikaci Exchange 2003 Server

Poznámka: *Vlastnosti testování se řídí z aplikace AVG E-mail Server. V horním menu aplikace zvolte Nástroje/Pokročilé nastavení (viz kapitola Kontrola pošty).*

5.1.4. Záložka Diagnostics Logging



Na této záložce můžete nastavit parametry protokolování zpráv a akcí ***AVG pro Exchange 2007 Server***. Na záložce je několik samostatných skupin:

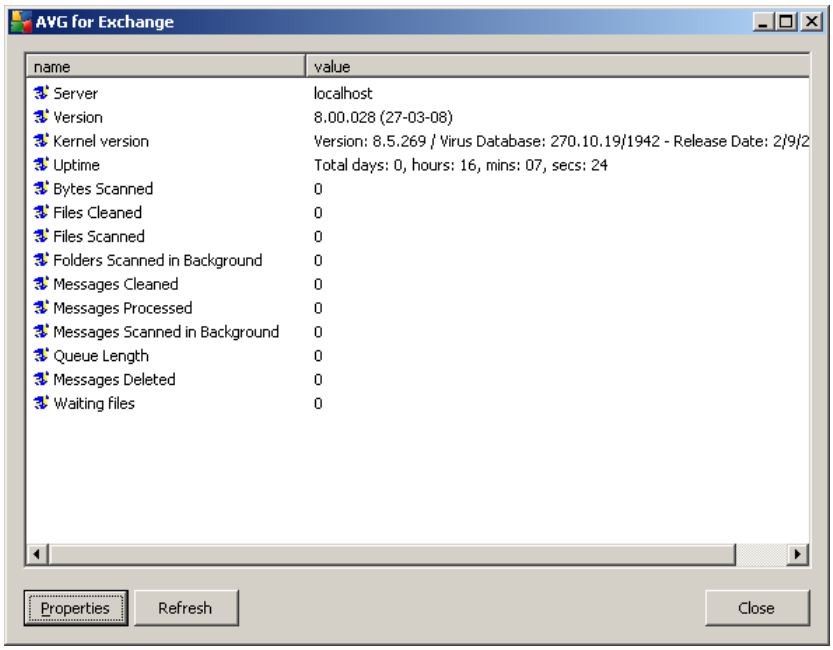
- ***Log Mode*** – toto nastavení reguluje množství a podrobnost zapisovaných zpráv

- ***New Log Time Period*** – zde nastavíte frekvenci vytváření nového souboru zpráv
- ***Log file directory*** – v tomto poli lze změnit implicitní nastavení umístění log souboru
- ***Log file name*** – zde je zobrazena implicitní maska jména souboru zpráv
- ***Screen Refresh*** – nastavení času obnovování monitorovacího okna *(zobrazeného v informačním okně **AVG pro Exchange 2007 Server**)* v sekundách

5.2. Monitorování serveru

5.2.1. Online Monitoring

V hlavním informačním okně AVG pro Exchange 2007 Server je zobrazeno několik polí:



V prvních čtyřech položkách jsou zobrazeny obecné informace o stavu serveru a modulu ***AVG pro Exchange 2007 Server***:

- ***Server*** – jméno serveru
- ***Version*** – verze ***AVG pro Exchange 2007 Server***
- ***Kernel version*** – verze testovacího jádra AVG a interní virové databáze
- ***Uptime*** – čas uplynulý od posledního restartu ***Exchange 2007 Serveru***

Ostatní položky představují jednotlivé monitorovací čítače výkonu, nabízené rozhraním VSAPI 2.0/2.5 serveru Exchange 2007. Popis čítačů je uveden v následujícím seznamu:

- ***Bytes Scanned*** – počet bytů zpracovaných antivirovým scannerem
- ***Files Cleaned*** – celkový počet souborů léčených antivirovým programem
- ***Files scanned*** – celkový počet souborů testovaných antivirovým programem
- ***Folders Scanned in Background*** – celkový počet složek testovaných v průběhu analýzy na pozadí (background scanning)
- ***Messages Cleaned*** – celkový počet zpráv nejvyšší úrovně léčených antivirovým programem
- ***Messages Quarantined*** – celkový počet zpráv přesunutých do karantény
- ***Messages Processed*** – počet zpráv nejvyšší úrovně, zpracovaných antivirovým programem
- ***Messages Scanned in Background*** – celkový počet zpráv zpracovaných pomocí kontroly na pozadí
- ***Messages Deleted*** – celkový počet smazaných podezřelých zpráv (dostupný pouze ve VSAPI 2.0/2.5)
- ***Queue Length*** – aktuální počet požadavků, čekajících zpracování antivirovým programem
- ***Waiting Files*** – počet souborů, čekajících na antivirový test

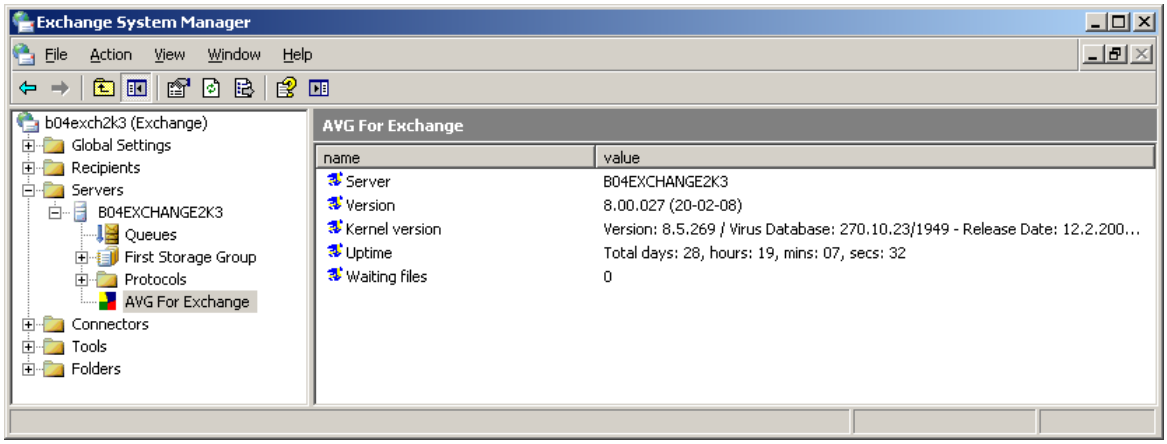
6. AVG pro MS Exchange Server 2000/2003

6.1. Konfigurace

Po restartu služby ***Exchange 2000/2003 Server Store*** a při instalovaném ***AVG pro MS Exchange 2000/2003 Server*** už není zapotřebí žádné další konfigurace a můžete produkt spustit.

6.1.1. Stav

Abyste zjistili, jaký je stav ***AVG***, spusťte aplikaci ***MS Exchange System Manager***. Ve větvi navigační stromové struktury označené ***Servers*** (*v levé části hlavního okna*) zvolte konkrétní server. Položkou této kategorie je také ***AVG pro Exchange***. Označte tuto větev a otevřete tak informační okno s přehledem různých relevantních dat.



Informace zobrazené v tomto okně zahrnují jméno serveru, verzi aplikace, verzi databáze, verzi kernelu a celkovou dobu, po kterou je program spuštěn od posledního restartu. Dále zde najdete informace o průběhu antivirové ochrany.

AVG pro MS Exchange 2000/2003 Server testuje všechny zprávy v databázích soukromých a veřejných adresářů. Pokud detekuje přítomnost viru, napíše ***AVG pro MS Exchange 2000/2003 Server*** zprávu do protokolovacího souboru AVG a také do protokolu událostí.

6.1.2. VSAPI 2.0

Virové testování ***API 2.0*** (*VSAPI 2.0 jako součást MS Exchange 2000 Serveru*) nepovoluje mazání infikovaných e-mailů. Jelikož tedy nelze odstranit přílohy infikovaných e-mailů, změní se jejich jméno: ***AVG pro Exchange 2000/2003 Server*** k původnímu jménu přidá koncovku *.virusinfo.txt*. Obsah souboru je přepsán zprávou o detekovaném viru. Jestliže je virus detekován přímo v samotné e-mailové zprávě, je celá zpráva přepsána informací o tom, že uvnitř e-mailu byl nalezen virus.

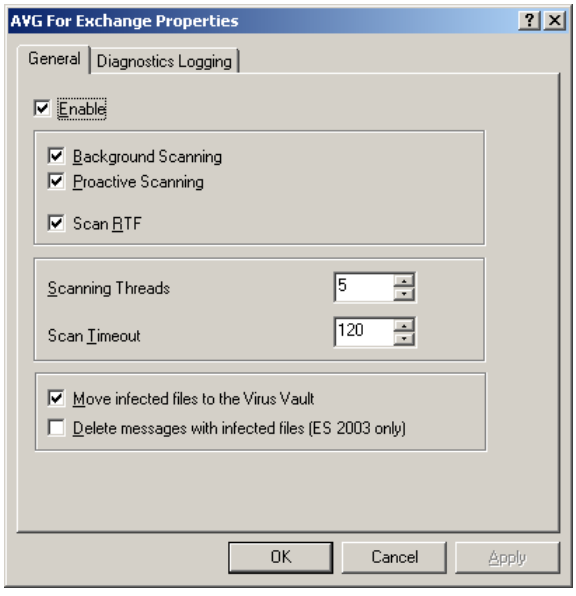
Virové testování ***API 2.5*** (*VSAPI 2.5 jako součást MS Exchange 2003 Serveru*) mazání infikovaných zpráv povoluje. Tuto funkci lze nastavit v konfiguračním dialogu ***AVG pro MS Exchange 2000/2003 Server***.

6.1.3. Záložka General

Konfigurační dialog ***AVG for Exchange 2000/2003 Server*** lze otevřít kliknutím pravého tlačítka myši na větvi ***AVG pro Exchange*** a volbou položky ***Properties*** (Vlastnosti). Dialog můžete také otevřít přes tlačítko ***Action*** v horním menu.

Konfigurační dialog vlastností ***AVG pro Exchange*** je tvořen dvěma záložkami. Na nich můžete editovat parametry testování pošty a protokolování.

Záložka General (Obecné)



Na záložce ***General*** najdete několik přednastavených možností vztahujících se k

nastavení testovacích schopností ***AVG pro MS Exchange 2000/2003 Serveru***:

- Položka ***Enable*** – zde lze povolit nebo zakázat kontrolu pošty.

- Položka ***Background Scanning*** – zde můžete povolit nebo zakázat proces kontroly existujícího obsahu databáze na pozadí. Kontrola uložené pošty na pozadí je jedním z prvků rozhraní VSAPI 2.0/2.5. Antivirová kontrola probíhá pro každou databázi na serveru zvlášť; vždy jsou testovány zprávy i přílohy. Pro každou databázi je zároveň použito jedno vlákno (*thread*) s nízkou prioritou, což znamená, že ostatní úlohy, jako například ukládání e-mail zpráv do Microsoft Exchange databáze dostane vždy přednost. Kontrola pošty na pozadí je aplikována pro tabulku se složkami v rámci Exchange úložiště. Složka, která již byla na pozadí jednou zkontrolována, bude znovu zkontrolována až při opětovném spuštění rozhraní. Změny jednotlivých zpráv ve složkách jsou zpracovávány proaktivní kontrolou (*proactive scanning*).

- Položka ***Proactive Scanning*** – zde můžete povolit nebo zakázat funkci proaktivní kontroly z VSAPI 2.0/2.5. Tato funkce spočívá v dynamické správě priorit položek v testovací frontě. Objekty s nižší prioritou nejsou testovány, dokud neproběhla kontrola všech položek s vyššími prioritami. Priorita objektu se nicméně může dynamicky měnit - vzrůstá ve chvíli, kdy se uživatel snaží daný objekt použít. Pořadí objektů ve frontě se tedy může dynamicky měnit podle aktivity připojených uživatelů.

- Položka ***Scan RTF*** – zde je možné určit, zda má ***AVG pro Exchange 2000/2003 Server*** provádět také kontrolu těl zpráv ve formátu RTF (neboť tyto mohou také obsahovat viry).

- Položka ***Scanning Threads*** – proces antivirové kontroly je implicitně rozdělen do několika vláken kvůli zvýšení celkového testovacího výkonu zavedením určité úrovně paralelismu. V tomto poli můžete změnit počet těchto vláken. Implicitní hodnota počtu vláken je určena vztahem 2-krát ‘počet_procesorů’ + 1.

- Položka ***Scan Timeout*** – maximální souvislý interval (*v sekundách*), po který může jedno vlákno přistupovat k právě testovanému objektu.

- ***Move infected files to the Virus Vault*** – pokud je tato funkce zapnuta, každá infikovaná zpráva bude přesunuta do karanténního prostředí Virového trezoru.

- ***Delete messages with infected files*** (*ES 2003 only*) – pomocí této položky je možno zapnout nebo vypnout možnost mazání infikovaných zpráv. Pokud je tato možnost zapnuta, takové zprávy jsou automaticky mazány. Pokud tomu

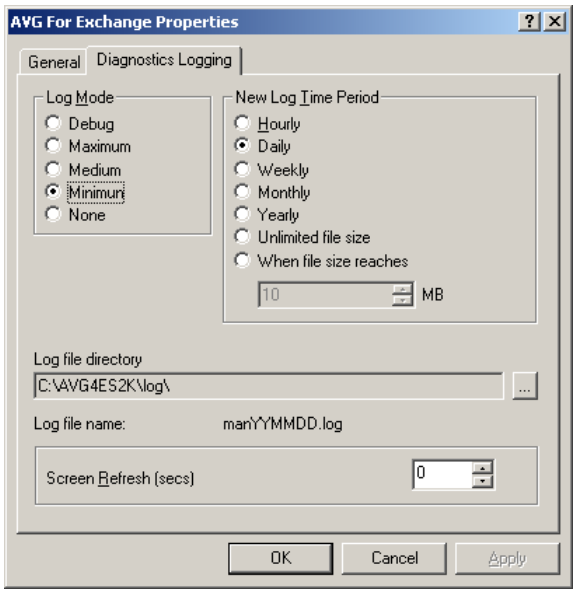
tak není, zpráva je doručena adresátovi, infikovaná příloha je ovšem nahrazena textovým souborem s informací o vymazání viru. Tato možnost je dostupná pouze s pomocí VSAPI 2.5 v Exchange 2003 Serveru.

Všechny prvky na této záložce obecně tvoří uživatelské rozšíření aplikačního rozhraní Microsoft VSAPI 2.0/2.5. Pokud se chcete blíže informovat o tomto rozhraní, následujte tyto odkazy:

- http://support.microsoft.com:80/support/kb/articles/Q285/6/67.ASP – obecné informace o VSAPI 2.0 v Service Pack 1 pro Exchange 2000 Server
- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k – popis principů spolupráce Exchange s antivirovými programy
- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166 – informace o doplňcích ve VSAPI 2.5 v aplikaci Exchange 2003 Server

Poznámka: *Vlastnosti testování se řídí z aplikace AVG E-mail Server. V horním menu aplikace zvolte Nástroje/Pokročilé nastavení (viz kapitola Kontrola pošty).*

6.1.4. Záložka Diagnostics Logging



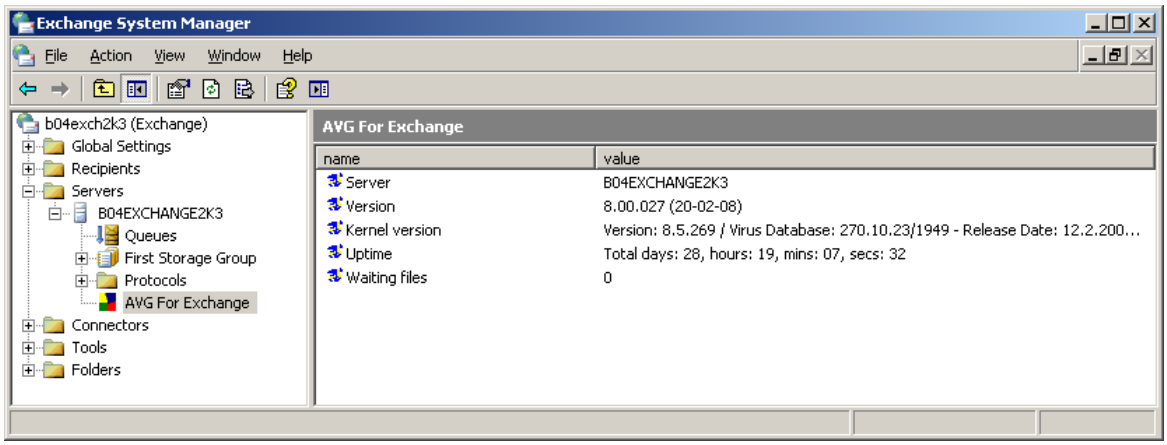
Na této záložce můžete nastavit parametry protokolování zpráv a akcí ***AVG pro Exchange 2000/2003 Server***. Na záložce je několik samostatných skupin:

- ***Log Mode*** – toto nastavení reguluje množství a podrobnost zapisovaných zpráv
- ***New Log Time Period*** – zde nastavíte frekvenci vytváření nového souboru zpráv
- ***Log file directory*** – v tomto poli lze změnit implicitní nastavení umístění log souboru
- ***Log file name*** – zde je zobrazena implicitní maska jména souboru zpráv
- ***Screen Refresh*** – nastavení času obnovování monitorovacího okna (zobrazeného v informačním okně AVG pro Exchange 2000/2003 Server) v sekundách

6.2. Monitorování serveru

6.2.1. Online Monitoring

V hlavním informačním okně AVG pro Exchange 2000/2003 Server je zobrazeno několik polí:



V prvních čtyřech položkách jsou zobrazeny obecné informace o stavu serveru a modulu ***AVG pro Exchange 2000/2003 Server***:

- ***Server*** – jméno serveru

- ***Version*** – verze ***AVG pro Exchange 2000/2003 Server***
- ***Kernel version*** – verze testovacího jádra AVG a interní virové databáze
- ***Uptime*** – čas uplynulý od posledního restartu ***Exchange 2000/2003 Serveru***
- ***Waiting Files*** – počet souborů, čekajících na antivirový test

Ostatní položky představují jednotlivé monitorovací čítače výkonu, nabízené rozhraním VSAPI 2.0/2.5 serveru Exchange 2000/2003 a nemusí být vždy k dispozici. Popis čítačů je uveden v následujícím seznamu:

- ***Bytes Scanned*** – počet bytů zpracovaných antivirovým scannerem
- ***Files Cleaned*** – celkový počet souborů léčených antivirovým programem
- ***Files Cleaned/sec*** – rychlost, jakou jsou jednotlivé soubory léčeny
- ***Files Quarantined*** – celkový počet souborů přesunutých do karantény
- ***Files Quarantined/sec*** – rychlost, jakou jsou soubory přesouvány do virové karantény
- ***Folders Scanned in Background*** – celkový počet složek testovaných v průběhu analýzy na pozadí (background scanning)
- ***Messages Cleaned*** – celkový počet zpráv nejvyšší úrovně léčených antivirovým programem
- ***Messages Cleaned/sec*** – rychlost, jakou jsou zprávy nejvyšší úrovně léčeny antivirovým programem
- ***Messages Quarantined*** – celkový počet zpráv přesunutých do karantény
- ***Messages Quarantined/sec*** – rychlost, jakou jsou zprávy přesouvány do virové karantény
- ***Messages Processed*** – počet zpráv nejvyšší úrovně, zpracovaných antivirovým programem
- ***Messages Processed/sec*** – rychlost, jakou jsou zprávy zpracovávány antivirovým programem

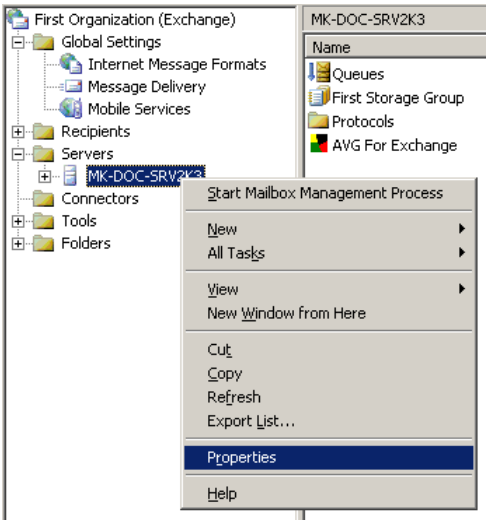
- ***Messages Scanned in Background*** – celkový počet zpráv zpracovaných pomocí kontroly na pozadí
- ***Messages Deleted*** – celkový počet smazaných podezřelých zpráv (dostupný pouze ve VSAPI 2.0/2.5)
- ***Messages Deleted/sec*** – rychlost, jakou jsou mazány podezřelé zprávy (dostupný pouze ve VSAPI 2.0/2.5)
- ***Queue Length*** – aktuální počet požadavků, čekajících zpracování antivirovým programem

6.2.2. Protokol událostí operačního systému

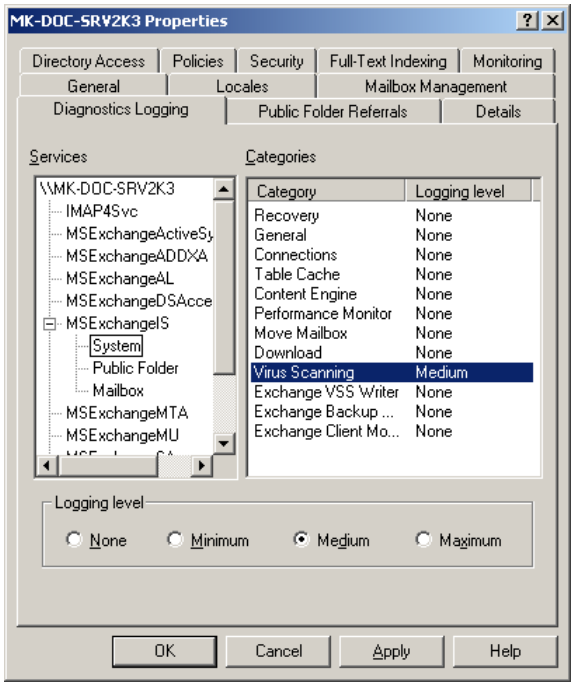
Mimo online sledování výkonu systému lze také nastavit zaznamenávání zpráv souvisejících s činností ***AVG pro Exchange 2000/2003 Server*** do protokolu událostí operačního systému Windows. Dostupné události zahrnují množství informací o událostech, jako jsou například nahrávání knihoven, nalezení viru, zprávy a varování o možných problémech apod.

Úroveň podrobnosti těchto zpráv můžete nastavit v hlavním okně aplikace Exchange System Manager:

- poklepejte na větev ***Servers*** v hlavním kontrolním stromě
- vyberte odpovídající server (na obrazovce pod tímto textem vidíte příklad zvýrazněného vybraného serveru)
- stiskněte pravé tlačítko myši na ikoně tohoto serveru a zvolte položku ***Properties*** *(Vlastnosti)* z nabídnutého kontextového menu



- otevře se následující okno vlastností serveru:



- přejděte na záložku ***Diagnostics Logging***
- ve stromě ***Services*** vyberte složku ***MSExchangeIS / System***

- v panelu ***Categories*** vyberte položku ***Virus Scanning*** a zvolte požadovanou úroveň podrobnosti zápisu zpráv do protokolu událostí. K dispozici jsou tyto úrovně:
    - ***None*** (žádné zprávy)
    - ***Minimum*** (minimální úroveň)
    - ***Medium*** (střední úroveň)
    - ***Maximum*** (maximální úroveň)

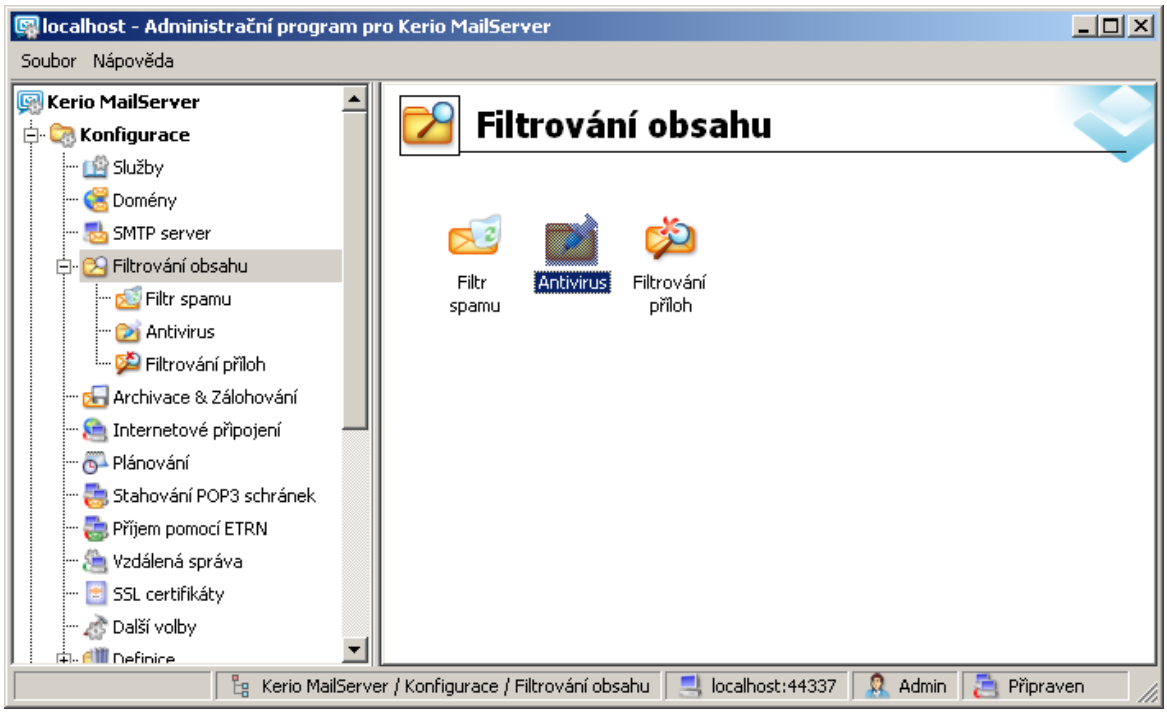
Poznámka: *Kompletní popis událostí aplikačního rozhraní pro kontrolu pošty Microsoft VSAPI 2.0/2.5 (v angličtině) najdete na stránce:*

http://support.microsoft.com/default.aspx?scid=kb;EN-US;294336.

7. AVG pro Kerio MailServer

7.1. Konfigurace

Mechanismus antivirové ochrany je integrován přímo v aplikaci ***Kerio MailServer***. Abyste aktivovali antivirovou ochranu ***Kerio MailServeru*** pomocí testovacího jádra AVG, spusťte administrační konzoli programu Kerio. V navigační struktuře na levé straně okna této aplikace zvolte položku ***Filtrování obsahu*** ve větvi ***Konfigurace***.

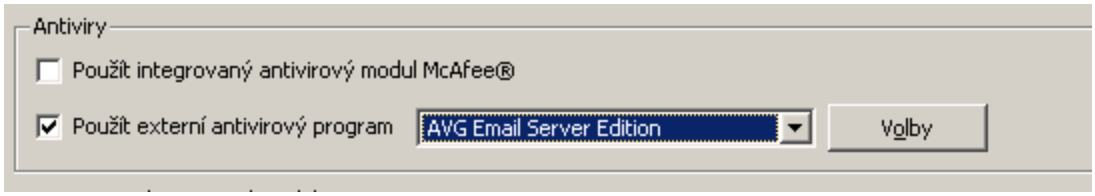


Na hlavním panelu aplikace se zobrazí dialogové okno ***Filtrování obsahu***. V rámci tohoto okna je možné volit ze tří nabídek:

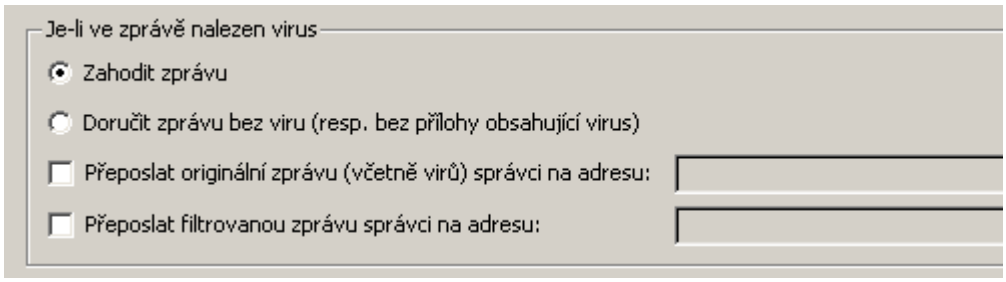
- ***Filtr spamu***
- ***Antivirus***
- ***Filtrování příloh***

7.1.1. Antivirus

Na této záložce můžete zapnout nebo vypnout antivirovou kontrolu pomocí ***AVG pro Kerio MailServer***. Pro aktivaci aplikace zvolte položku ***Použít externí antivirový program*** a vyberte možnost ***AVG E-mail Server*** z menu externího softwaru:

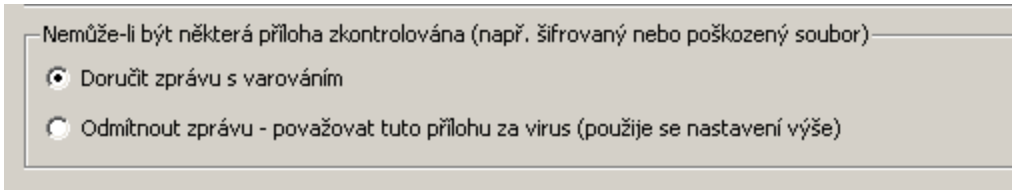


V následující části můžete specifikovat pravidla pro akce provedené v rámci detekce infikované zprávy nebo filtrování příloh:



Umožňuje definovat akce provedené při detekci viru nebo v rámci procesu filtrování příloh:

- ***Zahodit zprávu*** – pokud je tato možnost zvolena, infikovaná/filtrovaná zpráva je zamítnuta.
- ***Doručit zprávu bez viru*** – pokud je tato možnost vybrána, infikovaná/filtrovaná zpráva bude zbavena přílohy a doručena adresátovi.
- ***Přeposlat originální zprávu (včetně virů) správci na adresu*** – zapnutí/vypnutí možnosti přeposílání infikovaných zpráv na adresu zadanou v příslušném textovém poli.
- ***Přeposlat filtrovanou zprávu správci na adresu*** – zapnutí/vypnutí možnosti přeposílání filtrovaných (bez těchto příloh) zpráv na adresu zadanou v příslušném textovém poli.

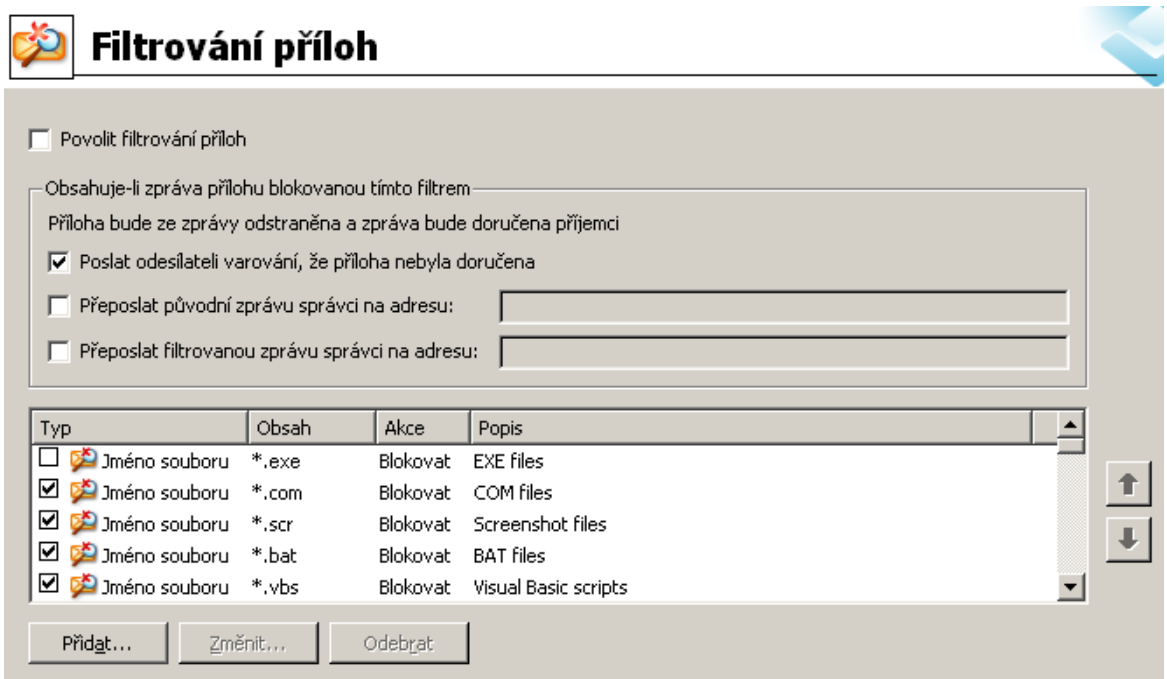


Umožňuje specifikovat akce pro soubory příloh, které nemohou být z jakéhokoli důvodu přečteny a otestovány:

- ***Doručit zprávu s varováním*** – zpráva (včetně přílohy) bude doručena nezkontrolovaná. Ke zprávě bude připojeno varování a uživatel bude upozorněn na to, že zprávu nebylo možno zkontrolovat, a že může obsahovat viry.
- ***Odmítnout zprávu*** – se zprávou bude naloženo, jako by příloha byla infikována.

7.1.2. Filtrování příloh

V nabídce ***Filtrování příloh*** je seznam s definicemi příloh pro jejich filtrování:



Filtr příloh lze zapnout nebo vypnout pomocí položky ***Povolit filtrování příloh***.

Volitelně lze upravit také následující nastavení:

- ***Poslat odesílateli varování, že příloha nebyla doručena*** - odesílateli bude ***Kerio Mailserverem*** zasláno varování, že odeslal zprávu s infikovanou nebo nepovolenou přílohou.

- ***Přeposlat původní zprávu správci na adresu*** - zpráva bude přeposlána v původním tvaru, tedy i s infikovanou nebo zakázanou přílohou, na zadanou emailovou adresu. Nezáleží na tom, zda bude uvedena lokální nebo externí adresa.

- ***Přeposlat filtrovanou zprávu správci na adresu*** - zpráva bez infikované nebo zakázané přílohy bude, kromě níže vybraných akcí, také přeposlána na zadanou emailovou adresu. Toho lze využít například pro ověření správné funkce antivirové kontroly a filtru příloh.

V seznamu přípon/příloh jsou u každého prvku obsažena čtyři pole:

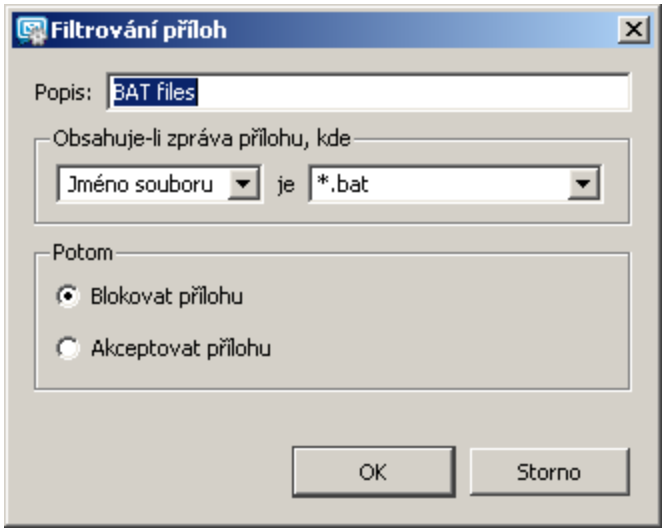
- ***Typ*** – specifikace druhu přílohy dané příponou zadanou v poli ***Obsah***. Možné typy jsou *File name* nebo *MIME type*. V příslušném poli můžete také zahrnout/vyloučit daný typ přílohy do/z filtru.

- ***Obsah*** – zde můžete definovat příponu filtrovaných příloh. Pro zápis lze využít wildcard znaků operačního systému (*například řetězec '*.doc.*' pro jakýkoli soubor s příponou .doc a libovolnou další za ní*).

- ***Akce*** – definice akce, která má být provedena s danou přílohou. Možné akce jsou ***Akceptovat*** (*přijmout přílohu*) a ***Blokovat*** (*blokovat přílohu podle pravidel definovaných na záložce Akce*).

- ***Popis*** – krátký popis dané přílohy.

Položka seznamu může být odstraněna pomocí tlačítka ***Odebrat***. Přidání položky je možné po stisku tlačítka ***Přidat...*** Stejně tak lze editovat existující záznam po stisku tlačítka ***Změnit...*** Objeví se toto okno:



- V poli ***Popis*** zadejte krátký popis druhu dané přílohy.
- V poli ***Obsahuje-li zpráva přílohu, kde*** můžete vybrat typ přílohy (*Jméno souboru nebo MIME typ*). V dalším poli také můžete zvolit příponu z připravené nabídky, nebo zadat přímo vlastní.

V poli ***Potom*** můžete rozhodnout, zda danou přílohu blokovat nebo přijmout.

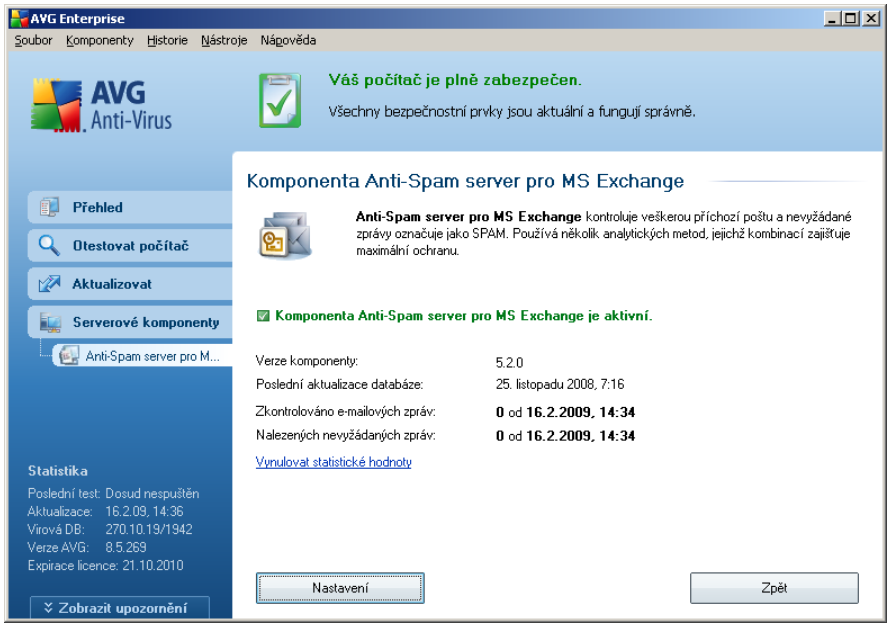
8. Nastavení komponenty Anti-Spam

8.1. Anti-Spam princip

Termínem *spam* označujeme nevyžádanou elektronickou poštu, převážně reklamního charakteru, jež je jednorázově hromadně rozesílána obrovskému počtu adresátů, čímž zahlcuje jejich poštovní schránky. Termín *spam* se nevztahuje na oprávněný e-mail komerčního charakteru, k jehož přijetí dal zákazník svůj souhlas. Spam je nejen nepříjemný a obtížný, ale je také častým zdrojem virů nebo distributorem textu urážlivého charakteru.

Komponenta ***Anti-Spam*** kontroluje veškerou příchozí poštu a nežádoucí zprávy označuje jako *spam*. K detekci spamu v jednotlivých zprávách používá několika analytických metod a zaručuje tedy maximální úroveň ochrany proti nevyžádané poště.

8.2. Anti-Spam rozhraní

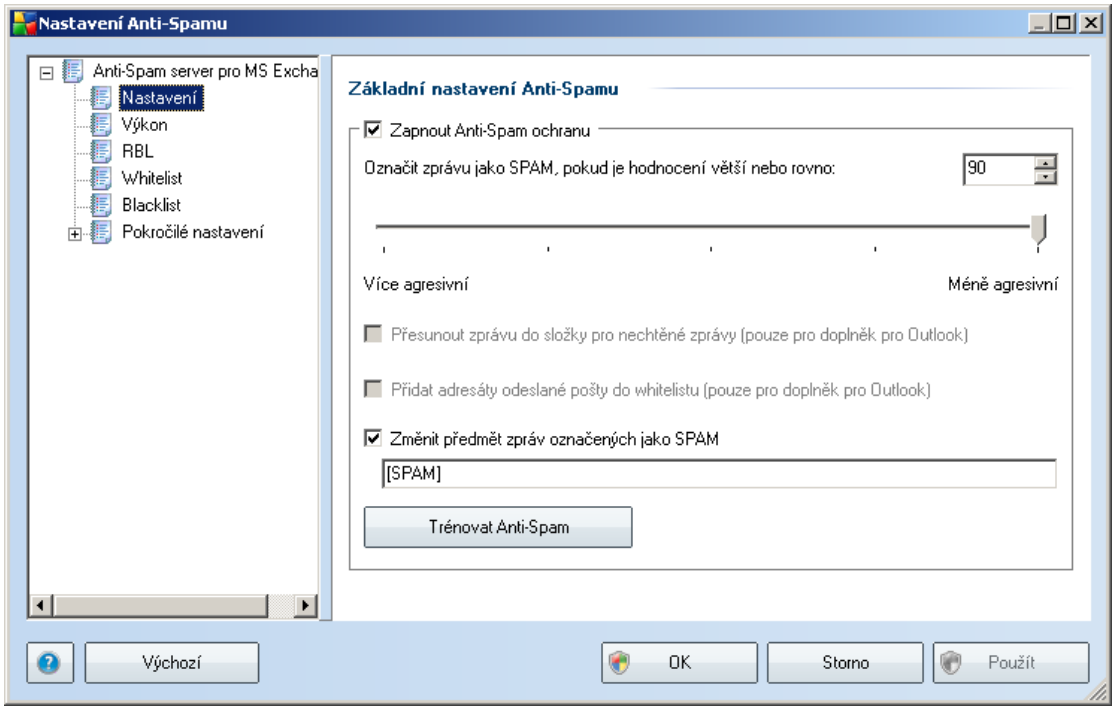


V dialogu komponenty ***Anti-Spam*** najdete kromě popisu funkce komponenty a informace o jejím aktuálním stavu (*Komponenta Anti-Spam je aktivní*) také běžnou statistiku.

V rozhraní jsou k dispozici tato ovládací tlačítka:

- ***Nastavení*** - otevře nastavení komponenty Anti-Spam.
- ***Zpět*** - vrátí vás do výchozího uživatelského rozhraní AVG (přehled komponent).

8.3. Anti-Spam nastavení



V dialogu ***Základní nastavení Anti-Spamu*** můžete označením položky ***Zapnout Anti-Spam ochranu*** celkově povolit či zakázat funkci komponenty ***Anti-Spam***.

V tomto dialogu také můžete definovat, jak chcete nastavit úroveň ochrany proti spamu - více či méně agresivní. Na základě několika dynamických testovacích technik pak filtr komponenty ***Anti-Spam*** přiřadí každé zprávě určité skóre (například podle toho, nakolik se obsah zprávy blíží textu, který lze považovat za spam). Hodnotu úrovně citlivosti pro označení spamu lze nastavit buď přímo vepsáním číselné hodnoty (*0 až 100*) do příslušného pole nebo pomocí posuvníku, který však pokrývá pouze rozsah hodnot 50-90.

Obecně doporučujeme nastavit úroveň citlivosti na spam v rozmezí 50-90.

Následuje přehled úrovní ochrany, jež odpovídají jednotlivým hodnotám:

- ***Hodnota 90-99*** - Většina příchozí pošty bude normálně doručena, aniž by byla označena jako spam. Snadno identifikovatelný spam bude odfiltrován, ale poměrně velká část spamových zpráv se přesto do vaší schránky dostane.

- ***Hodnota 80-89*** - E-mailové zprávy, u nichž se dá předpokládat charakter spamu, budou odfiltrovány. Je možné, že omylem dojde i k odfiltrování některých zpráv, jež nejsou spamového charakteru.

- ***Hodnota 60-79*** - Toto nastavení je již považováno za poměrně agresivní konfiguraci. E-mailové zprávy, které mohou být považovány za spam, budou odfiltrovány. Současně však dojde k poměrně velkému odchytu zpráv, které nejsou spamového charakteru, ale na základě určitých znaků mohou být takto vyhodnoceny.

- ***Hodnota 1-59*** - Velmi agresivní konfigurace. Nespamové e-mailové zprávy budou ve větší míře odfiltrovány spolu se zprávami pozitivně detekovanými jako spam. ***Tato konfigurace už není doporučeným nastavením pro běžné uživatele.***

- ***Hodnota 0*** - V tomto režimu vám budou doručeny pouze zprávy uživatelů uvedených na seznamu ***Whitelist***. Všechny ostatní zprávy budou automaticky považovány za spam. Tato konfigurace rozhodně není doporučeným nastavením pro běžné uživatele.

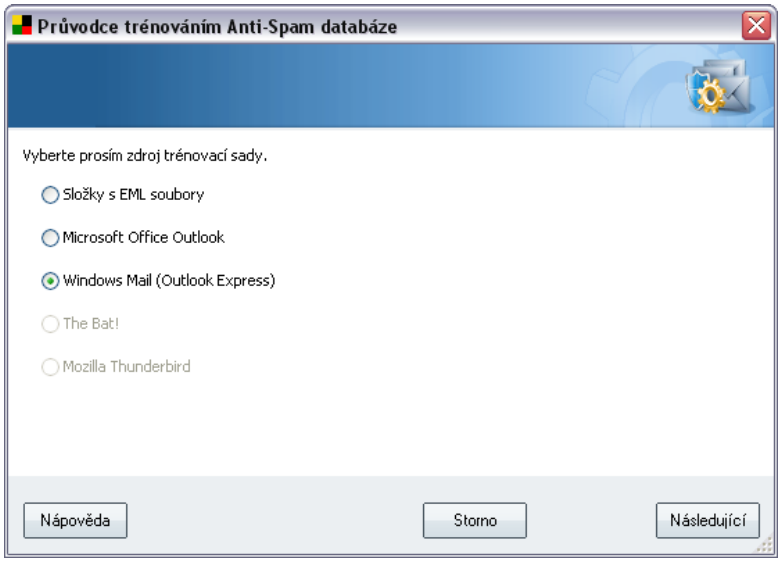
V dialogu ***Nastavení výkonu jádra*** můžete dále nastavit, jak se má zacházet s e-mailovými zprávami pozitivně detekovanými jako spam:

- ***Změnit předmět zprávy u zpráv označených jako spam*** - označením této položky zvolíte aktivujete textové pole, v němž máte možnost editovat text, kterým si přejete označovat zprávy detekované jako spam - tento text pak bude automaticky vepsán do předmětu každé detekované e-mailové zprávy

Tlačítko ***Trénovat Anti-Spam*** otevírá ***Průvodce trénováním Anti-Spam databáze***. Popis jednotlivých kroků průvodce najdete v samostatné kapitole.

8.3.1. Průvodce trénováním Anti-Spam databáze

V prvním dialogu ***Průvodce trénováním Anti-Spam databáze*** je nutno vybrat zdroj e-mailových zpráv, které chcete pro trénink použít. K trénování se obvykle používají zprávy, které byly anti-spamovou ochranou mylně označeny jako spam, nebo naopak nevyžádané zprávy, které prošly anti-spamovou ochranou bez povšimnutí.



Na výběr jsou následující možnosti:

- ***Konkrétní e-mailový program*** - pokud používáte některý z uvedených e-mailových programů (*MS Outlook, Outlook Express, The Bat!, Mozilla*), jednoduše vyberte příslušnou možnost

- ***Složky s EML soubory*** - používáte-li jiný e-mailový program, než které jsou v dialogu uvedeny, pak je vhodné nejdříve požadované zprávy uložit do nějakého adresáře na disk (*ve formátu .eml*), nebo se ujistit, že víte, kam váš e-mailový program zprávy ukládá. Poté zvolte možnost ***Složky s EML soubory***; v dalším kroku budete moci zadat umístění těchto složek.

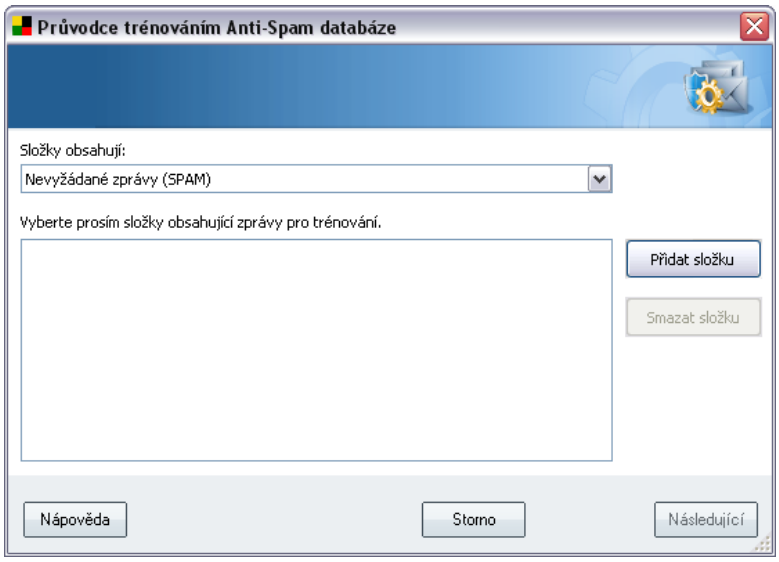
Chcete-li průběh trénování co nejvíce urychlit a zjednodušit, doporučujeme e-mailové zprávy dopředu vytřídit tak, aby ve zvolené složce byly umístěny pouze ty zprávy, které chcete použít pro trénink - žádané a nevyžádané zvlášť. Nicméně není to nutné, protože před zahájením samotného trénování budete mít možnost zprávy filtrovat.

Jakmile je zvolena požadovaná možnost, stiskněte tlačítko ***Následující*** a přejděte k dalšímu kroku.

8.3.2. Výběr složky se zprávami

Zobrazení dialogu v tomto kroku průvodce závisí na vaší předchozí volbě.

Volba složky s EML soubory



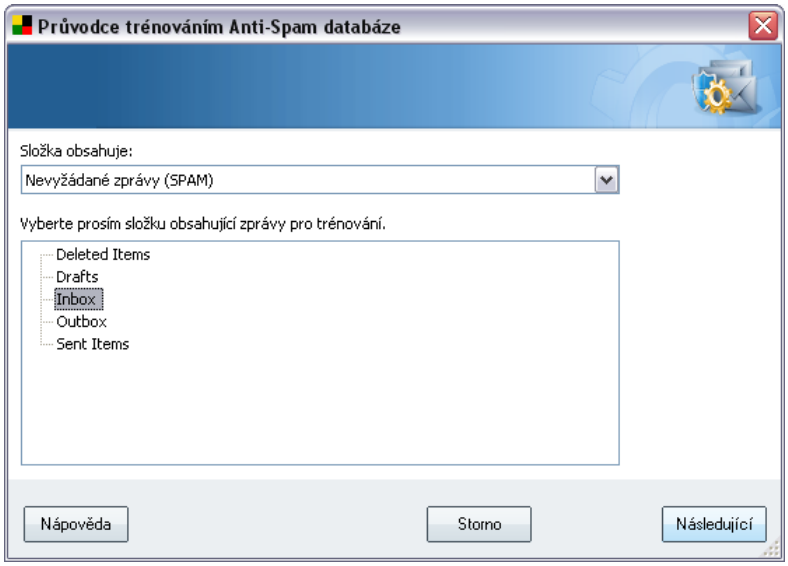
V tomto dialogu volíte složku se zprávami, které chcete pro trénování použít. Stiskněte tlačítko ***Přidat složku*** a určete umístění adresáře s .eml soubory (uloženými e-maily). Cesta k vybranému adresáři pak bude zobrazena v dialogu. Pro odebrání složky ze seznamu použijte tlačítko ***Smazat složku*** po jejím označení.

V rozbalovací nabídce ***Složka obsahuje*** zadejte, jaké zprávy se ve vybrané složce nacházejí - zda vyžádané (*tzv. HAM*), nebo nevyžádané (*SPAM*). V dalším dialogu budete moci zprávy ve složce filtrovat, takže složka nemusí obsahovat pouze e-maily určené k trénování.

Chcete-li pokračovat, stiskněte tlačítko ***Následující*** a pokračujte k části ***Způsob filtrování zpráv***.

Volba konkrétního e-mailového programu

Pokud jste vybrali některý e-mailový program, zobrazí se nový dialog se složkami.

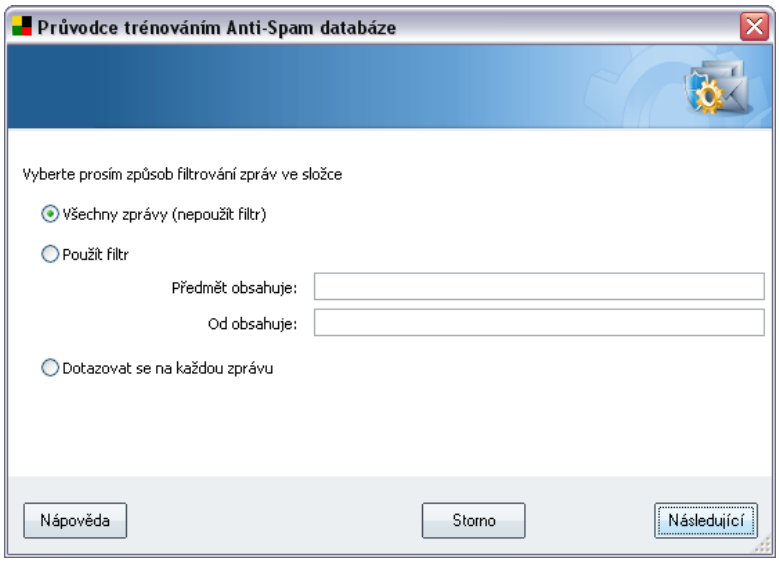


Poznámka: *V případě Microsoft Office Outlook bude nejprve potřeba zvolit MS Office Outlook profil.*

V rozbalovací nabídce ***Složka obsahuje*** zadejte, jaké zprávy se ve vybrané složce nacházejí - zda vyžádané (*tzv. HAM*), nebo nevyžádané (*SPAM*). V dalším dialogu budete moci zprávy ve složce filtrovat, takže složka nemusí obsahovat pouze e-maily určené k trénování. V hlavní sekci dialogu je zobrazen navigační strom příslušného e-mailového programu. Vyberte složku obsahující e-maily k trénování a označte ji.

Stiskem tlačítka ***Následující*** pokračujte k části ***Způsob filtrování zpráv***.

8.3.3. Způsob filtrování zpráv



V tomto dialogu můžete zvolit možnosti filtrování zpráv ve vybrané složce:

Jste-li si jisti, že složka obsahuje pouze zprávy, které chcete použít k trénování, a žádné další, zvolte možnost ***Všechny zprávy (nepoužít filtr)***.

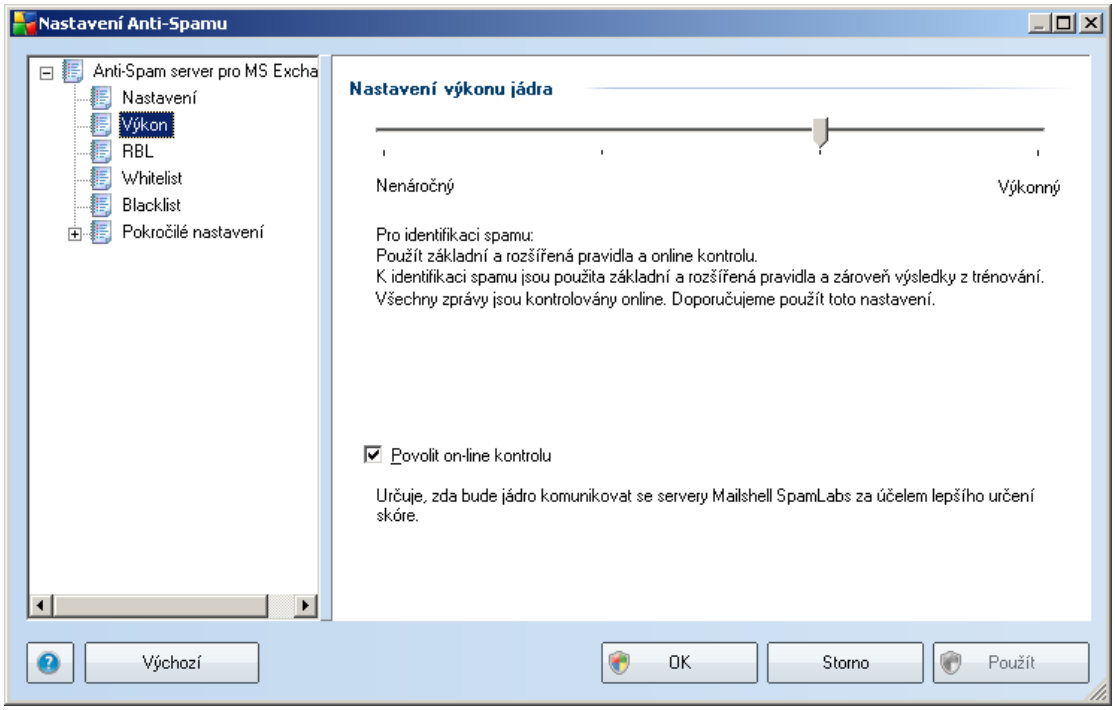
Pokud si nejste jisti, jaké zprávy složka obsahuje, a chcete, aby se průvodce u každé z nich zeptal, zda ji chcete nebo nechcete použít k trénování, pak zvolte možnost ***Dotazovat se na každou zprávu***.

Chcete-li zprávy filtrovat pokročilejším způsobem, zvolte položku ***Použít filtr***. Do textových políček pak můžete doplnit slovo (*jméno*), část slova nebo více slov, která se mají vyhledávat v polích "*Odesílatel*" a "*Předmět*" v hlavičce zprávy. Všechny e-maily, které budou těmto kritériím přesně vyhovovat, budou bez dalších dotazů použity k trénování.

Pozor: *Vyplníte-li obě textová pole (Předmět obsahuje: a Od obsahuje:), budou k trénování použity i zprávy, které vyhoví jen jedné z obou podmínek!*

Jakmile máte vybránu příslušnou možnost filtrování, stiskněte tlačítko ***Následující***. V následujícím informativním dialogu potvrďte svou volbu opět tlačítkem ***Následující***. Poté bude zahájeno trénování zpráv podle zvolených kritérií.

8.4. Výkon



Dialog ***Nastavení výkonu jádra*** (*odkazovaný položkou* ***Výkon***) nabízí možnost konfigurace parametrů výkonu komponenty ***Anti-Spam***. Polohou posuvníku určete úroveň testovacího výkonu na ose ***Nenáročný*** / ***Výkonný*** režim.

- ***Výkonný režim*** spotřebuje velký objem paměti. Během testovacího procesu budou k identifikaci spamu použity následující parametry: pravidla a spamové databáze, základní a pokročilé nastavení, IP adresy spammerů a spamové databáze.

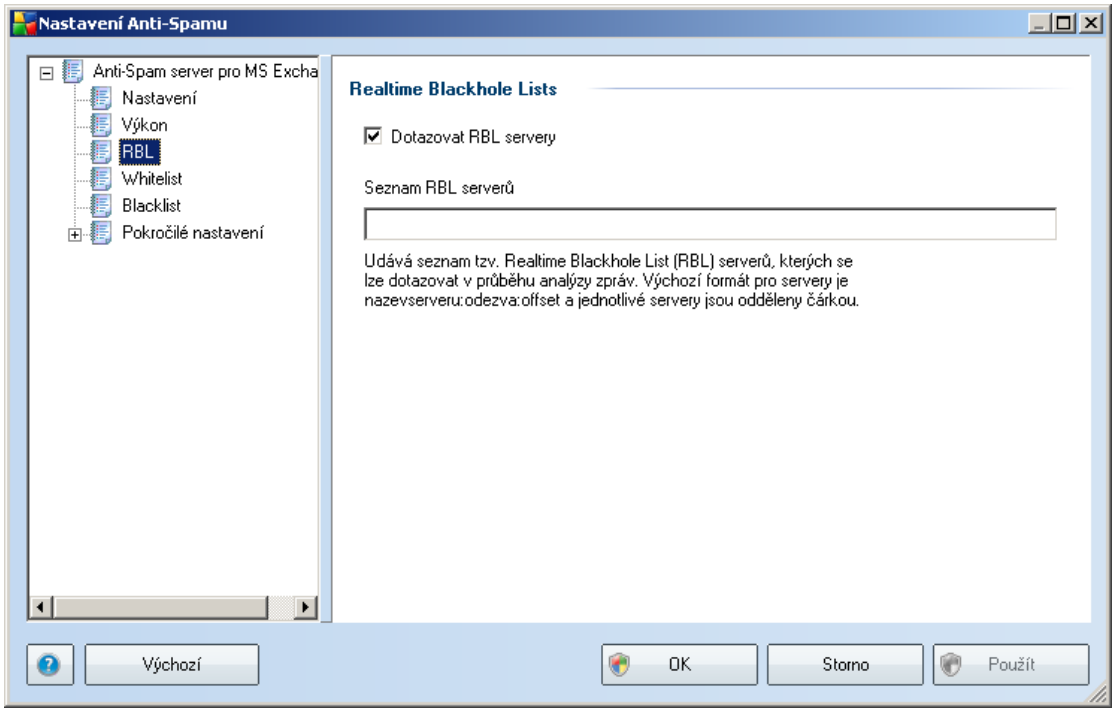
- ***Nenáročný režim*** znamená, že během testovacího procesu nebudou k identifikaci spamu použita žádná pravidla. Identifikace spamu bude založena výhradně na porovnání s testovacími daty. Tento režim pro běžné používání nedoporučujeme, nastavení lze doporučit výhradně u počítačů s velmi nízkou úrovní hardwarového vybavení.

Položka ***Povolit on-line kontrolu*** je ve výchozím nastavení označena a určuje, že pro přesnější detekci spamu bude k testování použita i komunikace se servery společnosti Mailshell, a během testování budou testovaná data porovnávána s databází této společnosti v online režimu.

Obecně doporučujeme podržet výchozí nastavení, pokud nemáte skutečný důvod tuto konfiguraci měnit. Změnu parametrů nastavení výkonu jádra lze doporučit výhradně znalým a zkušeným uživatelům!

8.5. RBL

Položka ***RBL*** otevírá editační dialog ***Realtime Blackhole Lists***:



V tomto dialogu máte možnost povolit funkci ***Dotazovat RBL servery***.

RBL (*Realtime Blackhole List*) server je DNS server s rozsáhlou databází známých odesilatelů spamu. Při zapnutí této funkce budou všechny příchozí zprávy v reálném čase porovnávány s RBL databází a při nalezení shody označeny jako spam.

Databáze RBL serverů obsahují skutečně nejnovější a nejaktuálnější záznamy o existujících centrech spamu a díky porovnávání e-mailových zpráv proti těmto databázím lze dosáhnout maximální úrovně ochrany před nevyžádanou poštou. Tato vlastnost se hodí zejména pro uživatele, kteří dostávají velké množství spamových zpráv, jež nemohou být detekovány pouze na základě pravidel definovaných jádrem komponenty Anti-Spam.

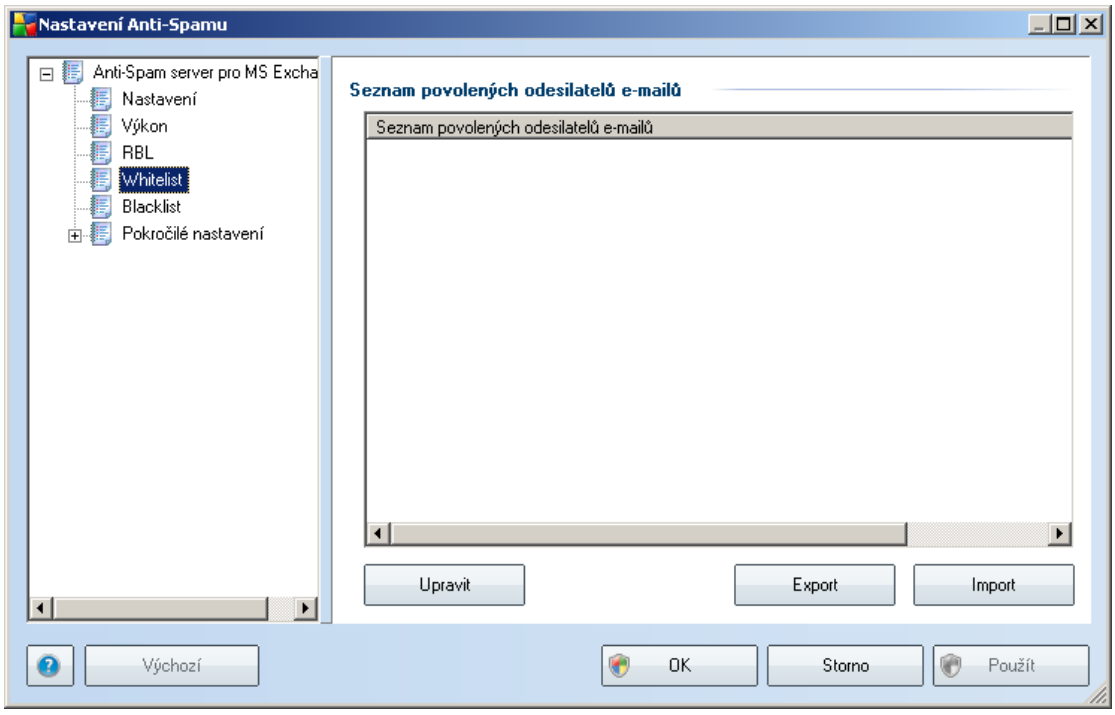
Položka ***Seznam RBL serverů*** vám dále umožní nastavit adresy konkrétních serverů, na nichž jsou tyto spamové databáze umístěny. Ve výchozím nastavení budou zprávy kontrolovány proti databázím na dvou RBL serverech. Doporučujeme ponechat toto nastavení, pokud nemáte skutečný důvod jej měnit - editace konfigurace RBL je vhodná jen pro skutečně znalé uživatele!

Poznámka: *Zapnutí této služby může na některých operačních systémech a konfiguracích zpomalit proces příjmu pošty, protože každá jednotlivá zpráva musí být prověřena proti databázi RBL serveru.*

Touto službou nedochází k odesílání žádných osobních nebo citlivých dat!

8.6. Whitelist

Položka ***Whitelist*** otevírá dialog se seznamem emailových adres a doménových jmen, u nichž víte, že pošta z těchto adres/domén doručená nikdy nebude mít charakter spamu:



V editačním rozhraní máte možnost sestavit seznam odesilatelů, u nichž předpokládáte, že vám nikdy nepošlou poštu, kterou lze považovat za spam (nevyžádanou poštu). Můžete také sestavit seznam kompletních doménových jmen

(například *avg.com*), o nichž víte, že negenerují nevyžádanou poštu.

Jakmile budete mít připraven tento seznam adres a domén, můžete je zadat do ***Whitelistu*** dvěma způsoby: přímým vložením jednotlivých adres nebo jednorázovým importem celého seznam. K dispozici jsou vám tato ovládací tlačítka:

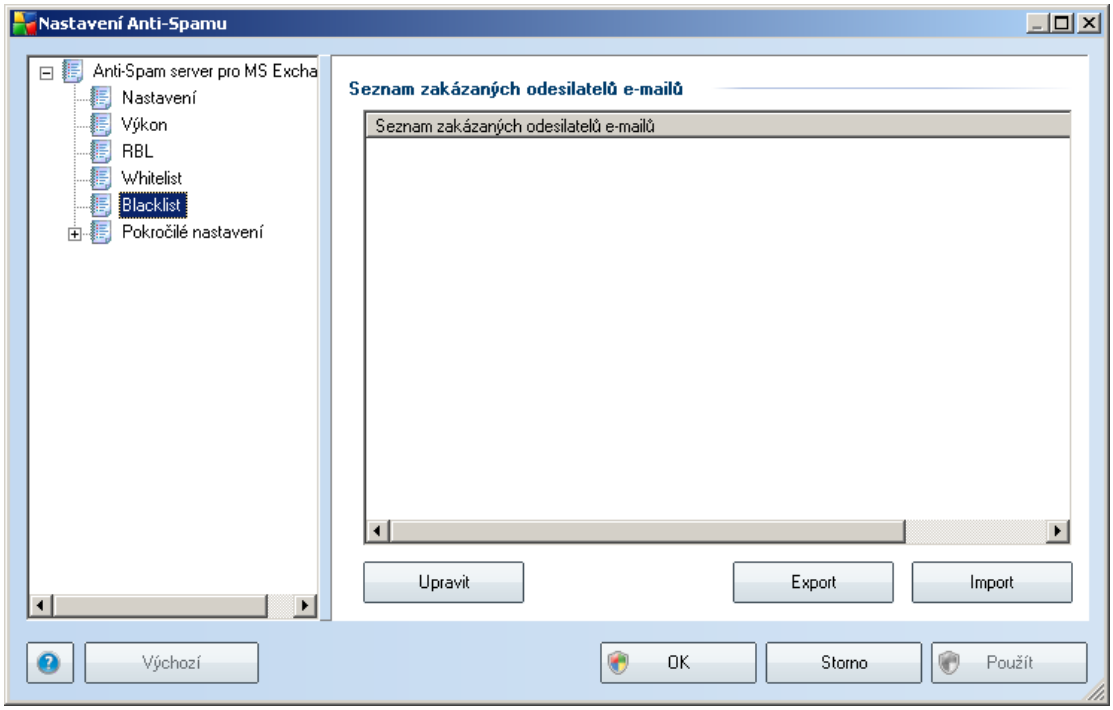
- ***Upravit*** - stiskem tohoto tlačítka otevřete dialog, v němž můžete manuálně přidávat adresy ze seznamu (můžete také použít jednorázově metodu *"kopírovat a vložit"*). Adresy/doménová jména vkládejte po jednom na každý řádek.

- ***Import*** - pokud již máte seznam adres/doménových jmen uložený v textovém souboru, můžete jej snadno importovat za použití tohoto tlačítka. Soubor, z nějž import provádíte, musí být ve formátu prostého textu a obsah musí být rozdělen tak, že každý řádek obsahuje pouze jedinou položku (adresu nebo doménové jméno).

- ***Export*** - pokud budete z libovolného důvodu chtít seznam adres/doménových jmen exportovat, můžete export provést pomocí tohoto tlačítka. Veškeré záznamy budou uloženy ve formátu prostého textu.

8.7. Blacklist

Položka ***Blacklist*** otevírá dialog se seznamem emailových adres a doménových jmen, která mají být zablokována pro příjem jakékoliv pošty. To znamená, že pošta odeslaná z kterékoliv uvedené adresy nebo domény bude vždy označena jako spam :



V editačním rozhraní máte možnost sestavit seznam odesilatelů, u nichž předpokládáte, že poštu, kterou vám posílají, lze považovat za spam (nevyžádaná pošta). Můžete také sestavit seznam kompletních doménových jmen (například *spammingcompany.com*), u nichž je předpoklad, že budou generovat nevyžádanou poštu. Pošta odeslaná z kterékoliv uvedené adresy bude pak detekována jako spam.

Jakmile budete mít připraven tento seznam adres a domén, můžete je zadat do ***Blacklistu*** dvěma způsoby: přímým vložením jednotlivých adres nebo jednorázovým importem celého seznam. K dispozici jsou vám tato ovládací tlačítka:

- ***Upravit*** - stiskem tohoto tlačítka otevřete dialog, v němž můžete manuálně přidávat adresy ze seznamu (můžete také použít jednorázově metodu *"kopírovat a vložit"*). Adresy/doménová jména vkládejte po jednom na každý řádek.

- ***Importovat*** - pokud již máte seznam adres/doménových jmen uložený v textovém souboru, můžete jej snadno importovat za použití tohoto tlačítka. Soubor, z nějž import provádíte, musí být ve formátu prostého textu a obsah musí být rozdělen tak, že každý řádek obsahuje pouze jedinou položku (adresu nebo doménové jméno).

- ***Export*** - pokud budete z libovolného důvodu chtít seznam adres/doménových jmen exportovat, můžete export provést pomocí tohoto tlačítka. Veškeré záznamy budou uloženy ve formátu prostého textu.

8.8. Pokročilé nastavení

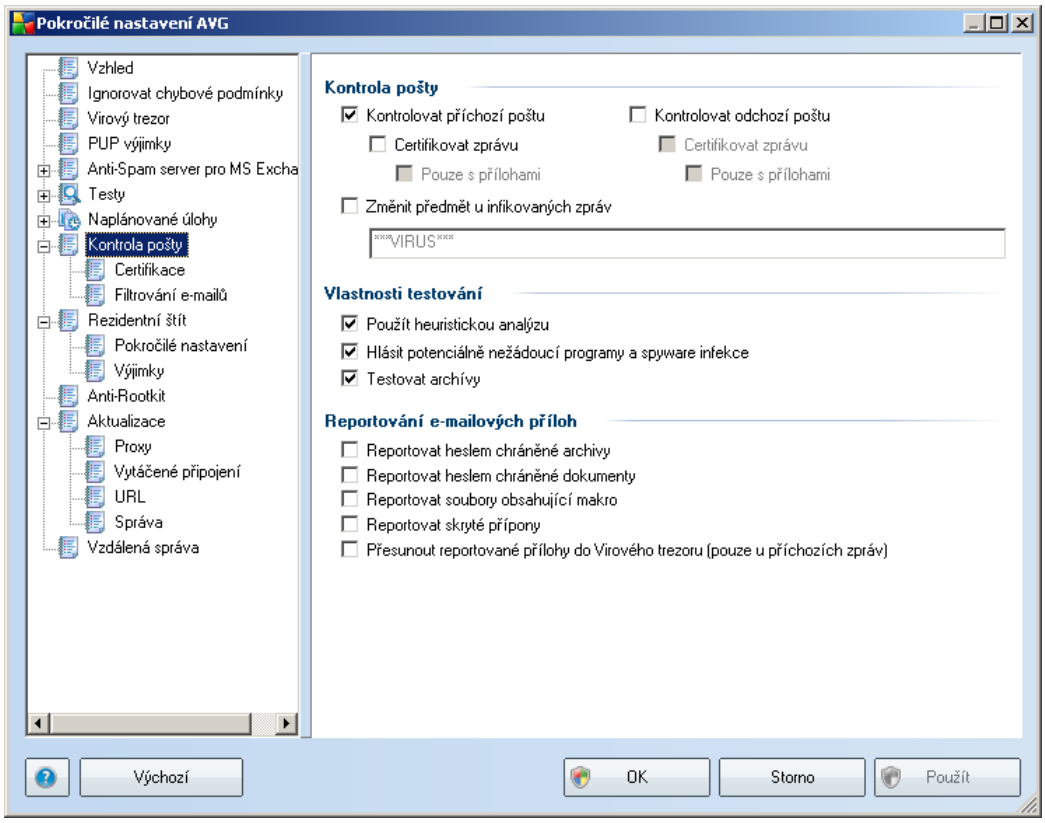
Obecně doporučujeme podržet výchozí nastavení, pokud nemáte skutečný důvod tuto konfiguraci měnit. Změnu parametrů nastavení výkonu jádra lze doporučit výhradně znalým a zkušeným uživatelům!

Pokud se přesto domníváte, že je nutné měnit konfiguraci komponenty Anti-Spam na úrovní vysoce pokročilého nastavení, pokračujte prosím podle instrukcí uvedených přímo v uživatelském rozhraní. Obecně platí, že v každém dialogu máte možnost zapnout jednu konkrétní funkci komponenty Anti-Spam a její popis je uveden přímo v dialogu:

- ***Paměť*** - fingerprint, reputace domén, LegitRepute
- ***Trénování*** - slovní nastavení, historie skóre, vyrovnávání skóre, počet slovních záznamů, práh pro samotrénování, váha, zápisový buffer
- ***Filtrování*** - seznam jazyků, seznam zemí, povolené IP adresy, blokované IP adresy, blokované země, blokované znakové sady, falešní odesilatelé
- ***RBL*** - RBL servery, multidetekce, práh, časový limit, maximum IP adres
- ***Internetové připojení*** - časový limit, ...

9. Kontrola pošty

Konfigurace komponenty ***Kontrola pošty*** se provádí z prostředí ***AVG***. V hlavním menu aplikace zvolte položku systémového menu ***Nástroje/Pokročilé nastavení***. V nabídce v levé části dialogu pak vyberte položku ***Kontrola pošty***:



Dialog ***Kontrola pošty*** je rozdělen do tří sekcí:

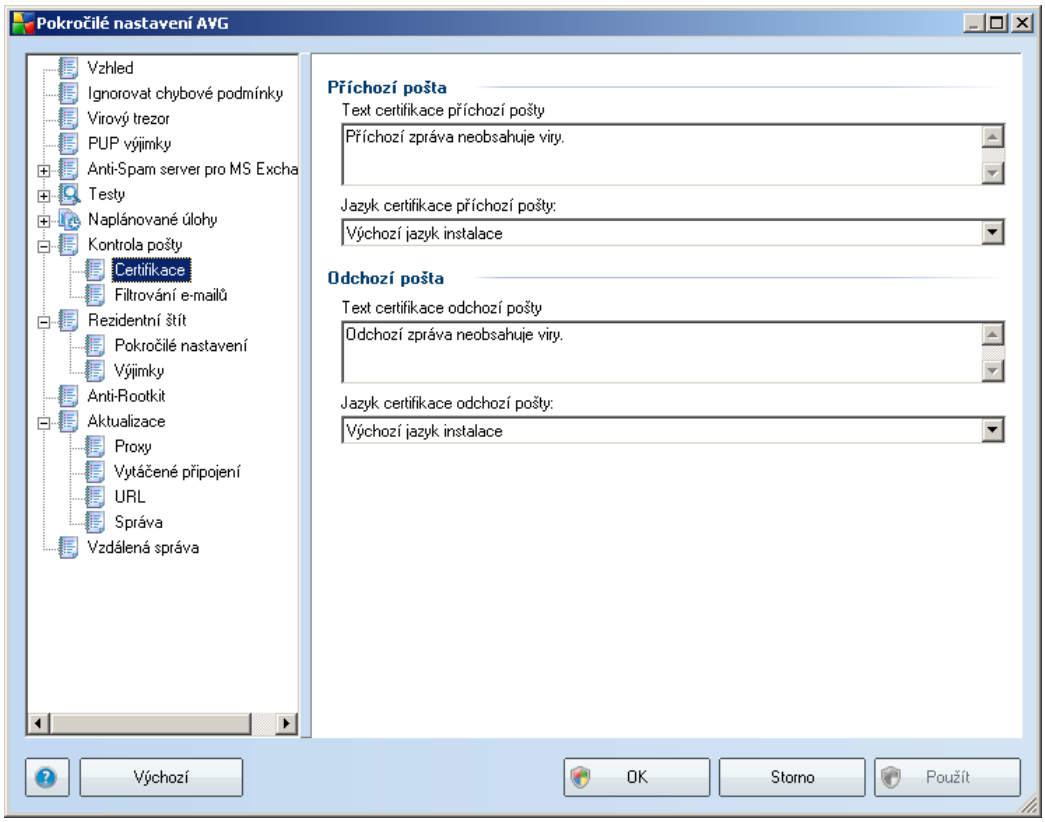
- ***Kontrola pošty*** - v této sekci zvolte, zda chcete kontrolovat příchozí/odchozí poštu a zda má být pošta certifikována vždy nebo jen pošta s přílohami (AVG necertifikuje e-mailové zprávy ve formátu HTML a RTF). Dále máte možnost rozhodnout se, zda si přejete, aby AVG automaticky změnilo předmět e-mailové zprávy, která pravděpodobně obsahuje virus. V takovém případě označte položku ***Změnit předmět u infikovaných zpráv*** a zvolte text, kterým má být zpráva označena (*standardně bude předmět zprávy změněn na text ***VIRUS****).

- ***Vlastnosti testování*** - rozhodněte, zda má být během testování elektronické

pošty použita metoda heuristické analýzy (***Použít heuristickou analýzu***), zda chcete testovat příchozí i odchozí poštu na přítomnost potenciálně nežádoucích programů (***Kontrolovat potenciálně nežádoucí programy***) a zda se mají kontrolovat i archivy (***Testovat archivy***).

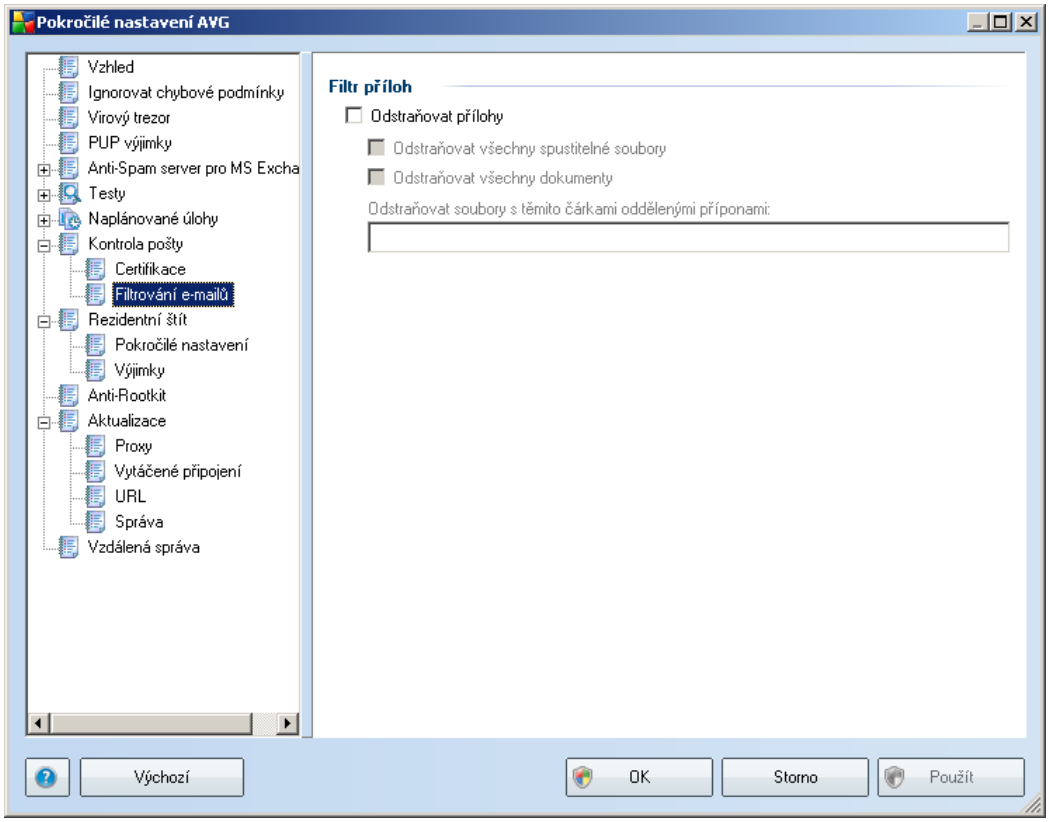
- ***Reportování e-mailových příloh*** - určete, zda si přejete být vyrozuměni o detekci heslem chráněných archivů, heslem chráněných dokumentů, souborů obsahujících makro a/nebo souborů se skrytou příponou nalezených v příloze testované e-mailové zprávy. Pokud bude taková zpráva při kontrole pošty zachycena, rozhodněte, zda má být detekovaný infikovaný objekt přesunut do ***Virového trezoru***.

9.1. Certifikace



V dialogu ***Certifikace*** můžete nastavit text certifikace a jazyk, v němž má být certifikace zobrazena. Toto nastavení se může lišit pro ***Příchozí poštu*** a ***Odchozí poštu***.

9.2. Filtrování e-mailů



Dialog ***Filtrování příloh*** umožňuje nastavení parametrů pro testování příloh e-mailových zpráv. Ve výchozím nastavení je možnost ***Odstraňovat přílohy*** vypnuta. Pokud se rozhodnete pro její aktivaci, budou automaticky odstraněny všechny přílohy zpráv, které byly detekovány jako infikované nebo potenciálně nebezpečné. Chcete-li blíže určit, které typy příloh mají být v případě pozitivní detekce odstraněny, označte příslušnou volbu:

- ***Odstraňovat všechny spustitelné soubory*** - odstraněny budou všechny pozitivně detekované přílohy s příponou .exe
- ***Odstraňovat všechny dokumenty*** - odstraněny budou všechny pozitivně detekované přílohy s příponou .doc
- ***Odstraňovat soubory s těmito příponami*** - odstraněny budou všechny pozitivně detekované přílohy s příponami, které sami definujete

10. FAQ a technická podpora

V případě problémů s AVG se pokuste vyhledat řešení na webu AVG (www.avg.cz) v sekci ***FAQ***.

Pokud na svůj dotaz nenajdete uspokojivou odpověď, obraťte se prosím na oddělení technické podpory AVG prostřednictvím kontaktního formuláře dostupného ze systémového menu volbou položky ***Nápověda / Odborná pomoc online***.